

金融機構資訊系統安全基準



中華民國銀行商業同業公會全國聯合會

中華民國一〇五年九月修訂版

金融機構資訊系統安全基準

版權所有請勿翻印

中華民國銀行商業同業公會全國聯合會

中華民國一〇五年九月修訂版

金融機構資訊系統安全基準

目 錄

壹、總則

- (壹) 安全基準之意義
- (貳) 基準之組成
- (參) 基準之施行
- (肆) 基準之適用機構
- (伍) 基準之主要用語
- (陸) 安全對策基準一覽表

貳、基準

- (壹) 設備基準
- (貳) 營運基準
- (參) 技術基準

參、附則

- (壹) 本基準之「使用說明」，如另冊附件。
- (貳) 本基準由財政部訂頒各金融機構遵行。

壹、總則

(壹) 安全基準之意義

我國金融機構之電腦連線作業，已朝向大網路型態逐年迅速發展，而此種新服務系統之營運成效影響各業界經濟活動及國民生活至大。

金融主管當局有鑑於此，對於提高電腦系統穩定性已列作金融業務自動化應加強措施之一。爰為確保金融機構電腦系統之安全及穩定運作，分別就資訊中心及營業單位連線作業有關之防災、防犯（註一）及其他安全措施，按環境、設備、軟體、系統開發、運作管理及教育訓練等各項目，參酌國內外若干實施先例訂定本基準，俾作具體實施安全預防、偵測、處理及檢討上之指針。

（註一）本基準內所稱防犯，係指防止各種人為犯罪行為，例如：侵入、破壞、舞弊等犯罪行為。

(貳) 基準之組成

一、 內容

本基準的內容，是金融機構等為達到下列目標，配合各機構的實態，所必須採取的安全對策：

- (一) 因天然災害、機器的故障、非法使用行為等所引起的金融機構等資訊系統事故等之發生，
- (二) 萬一發生事故時，將影響降至最低
- (三) 維護個資之安全，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

二、 組成

本基準的內容，由設備基準、營運基準、技術基準等三個部份組成其內容分別如下：

(一) 設備基準

為保護安置資訊系統的建築物、設備等，不受天然災害、非法行為等之危害，在設備面應考慮的對策。

(二) 營運基準

為提升資訊系統的可用性、完整性、機密性、來源辨識性、不可重複性及不可否認性，在開發、營運管理上之對策。

(三) 技術基準

為提升資訊系統的可用性、完整性、機密性、來源辨識性、不可重複性及不可否認性，在系統硬體及軟體等技術面之對策。

（參）基準之施行

一、金融機構之施行

顧及電腦系統具有整體性、動態性之本質，本基準在諸多靜態基準外，在確立管理體制上，對於資訊中心、營業單位各須建立之防災組織及防犯組織，亦有所規範；惟為進一步發揮總體施行效果，金融機構總行（處）宜定期召開「電腦作業安全對策會報」，由總務、稽核、會計、安全及資訊等各部門主管參加討論：

（一）審議電腦安全對策提案及預算。

（二）審議稽核部門抽查各單位施行本基準情形報告，如有缺失事項，應督導各單位研擬並執行改善措施，或依組織相關章程懲處之。

（三）全盤檢討評估：

1、系統使用率。

2、設備障礙發生率。

3、未成功交易發生比率。

4、其他防災、防犯已發生案件之處理情形。

5、資訊安全通報事件統計。

（四）建立資訊安全通報機制及制訂資訊安全緊急應變處理程序，並定期演練及檢討改善。

（五）指派專責單位辦理執行風險評估、安全分級及系統安全控管措施。

（六）制訂企業永續運作管理相關辦法。

（七）資訊安全政策之研擬及定期檢討。

二、主管機關實施進度之訂定

主管機關得視實際情況訂定本基準之實施進度，並督導金融機構切實依照進度施行。

三、 實施層次

本安全基準中每一細項，均依實施順序以 A、B、C 區分為三種層次，即：

(A) 表示必須符合之基本基準

(B) 表示應該達到之加強基準

(C) 表示較高目標水準之基準

(肆) 基準之適用機構

凡金融機構（含基層金融機構）及金融機構之共同利用中心等機構均得適用之。

(伍) 基準之主要用語

一、本基準中「重要的」之意義

在本基準中，出現的「重要的本體裝置」或「重要的資料」等，以「重要的……」方式記述時，此「重要的……」之意義，是表示下列的情況：

- (一) 「當該 ……… 發生時，在提供金融服務的功能面（如提領現金、資金調撥等）上，對多數客戶發生影響，同時可以假設為不易有替代方案的情況」
- (二) 「當該 ……… 發生被破壞或篡改時，對資訊系統的運轉有極大的影響」
- (三) 「客戶資料本身」

二、本基準內所使用之主要用語之定義及其範圍

經營階層	經營主管（總經理、董事會）等
密碼	金融卡之密碼或簽入系統之密碼
空調設備	在資訊系統機房用以調整室內溫濕度用之設備，包含壓縮機、冷卻水塔等附屬設備
客戶資料	為業務需要所蒐集、處理、利用之客戶相關資料 資料的範圍包含保有之所有個人資料（姓名、出生年月日、交易內容等）及法人資料（負責人、清算內容、交易內容等，依個人資料保護法定義之得以直接或間接方式識別該個人之資料）
自動化服務區	在營業廳場所設置 ATM 等，提供服務之角落
週邊設備	以電腦主機為中心之系統，磁碟、半導體磁碟、磁帶機、系統控制臺等之總稱，在以伺服器為中心之系統，印表機等之總稱
可攜式電腦設備	攜帶式端末、攜帶型個人電腦、 <u>行動裝置設備</u> 、可攜式端末等，主要由外務人員攜帶，在營業廳外使用之電腦設備
端末設備	連接於電腦系統，為櫃臺用機器、自動化機器、工作站、個人電腦等設備之總稱
端末系統設備	端末設備、可攜式電腦設備及其控制設備等之總稱
通訊設備	以電腦主機為中心之系統，如通訊控制裝置等設備 以伺服器為中心的系統，如路由器設備
合作通路	應用轉帳卡或在便利超商之 ATM 等之總稱
電源設備	為使電腦系統能正常運轉之電力設備、定電壓定周波數裝置等設備，及其附屬之設備
電子簽章	為確保電子資料的真實性的一種技術，目前，以利用公開基碼亂碼方式處理之數位簽章方式為主流，電子簽章，不僅可以確認本人身分，同時具有防止篡改、防止否認交易等之功能。在電子簽章法所提之電子簽章，並不侷限於數位簽章
非法存取	利用不正當的手法，非使用者對系統資訊或設備所執行的存取

	行為，或使用者使用系統超越其使用權限者
硬體設備·····	以電腦主機為中心的系統，是指中央處理機、主記憶體裝置、輸出入通道等之總稱，以伺服器為中心之系統，是指伺服器本身
總行、營業單位等 ····	資訊系統中心以外的總行單位（具體上，指系統開發業務、營業單位支援等執行內部庶務的組織、庶務處理中心、區域中心等）或提供客戶服務之店舖（包含下列之「無人化服務區」或「企業內分行」等）之總稱
無人化服務區 ·····	僅設置 ATM 等自動化設備之店舖
行外收付處 ·····	設置於購物中心或超級商場等店舖內之金融機構營業單位
開放網路 ·····	以網際網路為代表，不特定多數使用者能自由連接通訊之網路
電腦操作人員 ·····	在資訊系統中心之電腦系統操作人員
主從架構系統 ·····	與以電腦主機為中心的中央集中型系統不同，利用區域網路等互相連結，以伺服器為中心之系統，共用資源而分散處理的非集中型電腦系統
便利超商 ATM ·····	金融機構等設置於便利超商之 ATM
電腦 ·····	大型主機系統、伺服器、工作站、個人電腦等之總稱
資訊系統 ·····	電腦、端末機器、週邊裝置、通信系統、通信線路以及軟體程式等全部或部分所構成，為處理資料的系統
電腦機房 ·····	設置資訊系統的機房或房間
資訊中心 ·····	為運轉資訊系統而設置電腦系統的建築物或組織
伺服器 ·····	在利用區域網路連接的系統中，用以共同利用其週邊裝置、群組軟體（Groupware）或資料庫（Database）之主要電腦系統
系統管理者 ·····	為使用電腦系統正常運轉，而統籌控管其維護、運作之管理者
安控管理者 ·····	全盤控管資訊安全的管理者
資訊安全政策 ·····	為能適切的保護資訊資產，公司（或組織）對安控對策訂定的方針
直接連接通路 ·····	利用開放型網路之網路銀行或行動銀行等金融服務商品，未經由營業單位等，而直接對客戶提供服務的方法之總稱
資料 ·····	適合由電腦系統處理之格式化資料
資料管理者 ·····	對於保有之資訊，統籌控管之管理者，主要職掌為對資料使用狀況之管理、資料存取權限之核可等
媒體儲存室 ·····	保管儲存資料、程式等記錄媒體的房間
轉帳卡 ·····	能提供將消費金額由客戶之帳戶即時扣除，並直接轉入特約商店帳戶的即時清算卡片服務
文件 ·····	電腦系統之開發、設計、撰寫、營運等相關記錄之文書
網路管理者 ·····	對網路系統之運用、安全管理、故障排除等統籌控管網路及其相關設備之管理者
套裝軟體 ·····	由其他廠商購入之業務處理用軟體 包含以個人電腦處理之泛用軟體
檔案 ·····	記錄媒體、或記錄於記憶裝置之資料或程式

行動交易	利用行動電話等設備，由金融機構等提供之銀行交易、證券交易、人壽保險或產物保險等金融服務之總稱
IDF	在線路進入機房樓層之最初場所，所設置之樓層配線盤裝置 (Intermediate Distributing Frame 之簡稱)
MDF	在線路進入建築物之最初場所，所設置之主配線盤裝置 (Main Distributing Frame 之簡稱)
UPS	當市電短暫中斷時，仍能由蓄電池供電，維持電腦系統之持續運轉之裝置 (不停電電源裝置 = Uninterruptible Power Supply 之簡稱)

(陸) 安全基準一覽表

設備基準

[一、 資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 建築物								
設 1		1. 環境	避免設置於容易發生各類災害、事故之區域		○				C
設 2		2. 周圍	檢討因所在地之環境變化，可能發生之災害與事故，並訂定對策		○				A
設 3			建地應確保必要的通道		◎				A
設 4			最好與鄰近建物保持充分之間隔		○				B
設 5			建立圍牆或隔柵以及加裝錄影監視設備防止侵入之設施		○				B
設 6			不可將招牌等懸掛在外面		○				A
設 7			建築物應安裝避雷設備及設備獨立接地系統		○				A
設 8			建築物應為資訊系統相關業務專用，或在建築物內區隔資訊系統相關業務專用之獨立區域		○				A
設 9			建地內通訊與電力線路要有防止切斷、延燒措施及雙迴路管線		○				A
設 10		3. 結構	應依據消防署規定之防火建築物		◎				B
設 11			具安全性之結構		◎				B
設 12			外牆、屋頂部份應有充分之防水性能		◎				A
設 13			外牆部份應具足夠之強度		○				B
設 14		4. 門窗	門窗應有防火措施		◎				B
設 15			應有防犯措施		◎				A
設 16			平常使用之進出口僅限一處，並設置進出管制裝置、防犯設備等		○				B
設 17			應設置緊急安全門		◎				A
設 18			應施以防水措施		○				A
設 19			進出門窗應具有充分之強度，並需隨時加鎖		◎				B
設 20		5. 內部裝潢	應使用具不燃性或耐燃性之材料		◎				A
設 21			對於因地震等裝潢之震落或損壞應有預防措施		○				B

設備基準

[一、資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(二) 電腦機房、媒體儲存室								
設 22		1. 位置	應設置於不易受到災害的位置		◎				A
設 23			應設置於不易由外部進入之位置		◎				A
設 24			不可懸掛室名等標示牌		◎				A
設 25			確保必要之維修空間		◎				A
設 26			應為獨立之專用房間		◎				A
設 27		2. 門窗	平時使用之進出口，應僅限設置一處，並須設置等候室		○				A
設 28			出入口之門窗，應具有足夠之強度，並須加鎖		◎				A
設 29			窗口應設置防火、防水、防止破壞等措施，並須設置由外部無法窺視機器設備之裝置		◎				B
設 30			緊急安全門、避難器具、指示燈、停電照明等設置		◎				A
設 31		3. 結構、內部裝潢	應為獨立之防火區域		◎				A
設 32			應設置防止漏水之對策		◎				A
設 33			應設置消除靜電之設備		◎				B
設 34			內部裝潢應使用不燃性材質或具防火性能之材料		◎				A
設 35			對於地震等內部裝潢之震落、損壞，應有預防措施		◎				A
設 36			高架地板應具有在地震時不會損壞之構造		◎				A
設 37		4. 設備	應設置自動火災檢知警報裝置		◎				A
設 38			應設置火災等緊急事故警示及緊急連絡裝置		◎				A
設 39			應設置滅火設備		◎				A
設 40			纜線之耐火及防止延燒之措施		◎				B
設 41			應設置排煙設備		◎				A
設 42			應設置緊急照明設備與攜帶式照明設備		◎				A
設 43			不可裝設一般用水的設備		◎				A
設 44			應安裝地震感應器		○				C
設 45			於機房進出口設置進出管制與防犯設備		○				A
設 46			應設置溫濕度自動記錄裝置或溫濕度警報裝置		◎				A

設備基準

[一、 資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 47		5. 資訊系統設備、其他各項設備及備用物品	應設有預防蟲鼠害之措施		○				A
設 48			各類雜項設備及備用品，應具有防火性能		◎				B
設 49			應設置防止靜電之措施		◎				C
設 50			各類雜項設備及備用品應具有耐震措施		◎				B
設 51			搬運車等應安裝固定裝置		◎				A
	(三) 電源室、空調室								
設 52			應設置於不易受到災害之位置		◎				B
設 53			應確保維修保養時必要的空間		◎				A
設 54			應為專用之獨立房間		○				B
設 55			門窗應加鎖，最好不要設置窗戶		◎				A
設 56			應採用耐火結構		◎				A
設 57			應安裝自動火災警報設備		◎				A
設 58			應安裝氣體滅火設備		○				A
設 59			空調設備應設有防止漏水的措施		◎				A
設 60			電纜線、各類導管導線等，應設有防止延燒的措施		◎				B
	(四) 電源設備								
設 61			電源設備之容量，應保持充裕有餘		◎				A
設 62			應以多重迴路引入電源		○				C
設 63			應設置能提供良質電力之供電設備		◎				A
設 64			應設置自備發電機設備及蓄電池設備		◎				A
設 65			電源設備應設置避雷裝置		◎				A
設 66			電源設備應具有耐震措施		◎				B
設 67			由配電盤至送至資訊系統設備之電源配線應為專屬專用電纜線		◎				A
設 68			應避免與負載變動激烈的機器設備共用電纜線		◎				A
設 69			資訊系統設備之接地線，應為專用之地線		◎				A
設 70			應設有預防措施，以避免因過大電流、漏電等事故，造成設備故障		◎				A

設備基準

[一、 資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 71			應設置防災、防犯用備用電源		◎				A
(五) 空調設備									
設 72			空調設備，應保持充分寬裕之容量		◎				A
設 73			空調設備，應具有穩定調節空氣之功能		◎				A
設 74			電腦機房之空調設備，應為獨立使用及維修		◎				A
設 75			應設置備援之空調設備		○				A
設 76			空調設備應安裝自動控制裝置、異常警報裝置等		◎				A
設 77			空調設備應具有預防入侵、破壞等措施		◎				A
設 78			空調設備應具有耐震之措施		◎				B
設 79			空調設備隔熱材料、排吸氣口應採用耐火材料		◎				A
(六) 監視控制設備									
設 80			應安裝監視控制設備		◎				B
設 81			宜設置中央監控室		○				B
(七) 數據線路相關設備									
設 82			數據線路相關設備，應上鎖		◎				A
設 83			數據線路相關設備之安裝場所，不可附加標示		◎				A
設 83-1			數據線路相關設備，應備有專用之配線空間		◎				C

設備基準

[二、總行、營業單位]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 建築物								
設 84		1. 周圍	建地內之通訊線路、供電纜線等，應具有防止被切斷、延燒之措施			○			A
設 85		2. 結構	應為耐火之建築物			○			C
設 86			建築物應具有安全性之結構			◎			B
設 87			建築物外牆與屋頂應具充分的防水性能			◎			A
設 88			建築物外牆應確保其強度			○			A
設 89			3. 門窗	窗戶應具有防火措施			◎		
設 90		門窗應有防犯措施				◎			A
設 91		出入口的門，應有足夠之強度，同時應加裝門鎖				◎			B
設 92		非營業時間之出入口應設置進入者識別用裝置				◎			B
設 93		進出口應具有防水措施				○			A
設 94		4. 內部裝潢	天花板及牆壁應具有隔熱、吸音之功能			○			C
設 95			應具有預防措施，以防止因地震而造成內部裝潢震落或損壞			◎			A
設 96			地板面應採用不易積存灰塵或產生靜電的材質			○			C
設 97			端末設備之通訊線路及電源線路，應具有防止被切斷的措施			◎			A
設 98			端末設備之通訊線路、電源線等，應有防止被漏水浸滲的措施			○			A
設 99		5. 設備	應安裝自動火災警報及滅火器等設備			◎			A
設 100			各類設備宜有耐震措施			○			B
設 101			應安裝耐火金庫或耐火庫房			◎			A
設 102	應安裝避雷裝置				○			A	
設 103	應安裝防犯措施				◎			A	
設 104	6. 線路相關設備	不可標示通訊線路相關設備安裝場所			◎			A	
設 105		易為外界碰觸之通訊線路相關設備等最好上鎖			◎			A	
設 106		連結端末機器設備之線路，最好有備援線路			○			A	

設備基準

[二、總行、營業單位]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 107		7. 電源設備	應注意電源線之配置，以確保端末設備之正常作業			◎			A
設 108			防災、防犯設備應安裝備用電源			◎			A
設 109			宜安裝自用發電設備			○			C
設 110		8. 空調設備	應設置空調設備			◎			A
設 111		9. 自動化服務區	應安裝直接通話設備			◎			A
設 112			應安裝緊急通報裝置			◎			B
設 113			宜安裝防犯措施			◎			A
設 114			應設置照明設備及緊急照明設備			◎			A
設 115			自動化服務區的門，應有部分為透明透光者			◎			A
設 116			自動化服務機器之裝填現金及設備維護作業應確保必要的空間			○			A
設 117			安裝自動運作設備			○			B
設 118		10. 端末設備	端末設備應設有耐震措施			○			B
設 119			機器設備之地線，應確實安裝			◎			A
設 120			端末設備應有保護措施，不受漏水或塵埃的侵害			○			B
		(二) 伺服器安裝場所							
設 121		1. 位置	伺服器設備應設置於較不易受到災害的位置			○			A
設 122			伺服器設備應設置於不易由外部進入的位置			○			A
設 123			設置伺服器設備的位置，不得張貼具室名等標示之招牌			○			A
設 124			設置伺服器設備的位置，應為專用之隔間			○			B
設 125		2. 結構・內部裝潢	應設置於具防火能力之隔間內			○			A
設 126			應具防止漏水的對策			○			A
設 127			高架地板應具有耐震之措施			○			B
設 128		3. 設備	應具有滅火設備			○			A
設 129			宜設置地震感應器			○			B

設備基準

[二、總行、營業單位]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 130			在設置伺服器的房間進出，應設置進出管理設備、防犯設備等			○			A
設 131			應設置溫濕度自動記錄裝置或溫濕度警報裝置等			○			A
設 132			應設置空調設備			○			A
設 133			應有防止鼠害的措施			○			A
設 134			應有防止電源插頭由插座鬆落的措施			◎			A
	(三) 行外收付處								
設 135			應有防止由其他區域入侵的措施			◎			A
設 136			配合使用商店設備之狀況，應有適當的補強對策			◎			A

設備基準

[三、 與流通業、零售店合作之合作通路]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 便利超商之 ATM								
設 137			應有防犯措施				◎		A

營運基準

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 確立管理體制								
運 1		1. 資訊安全管理與責任之明確化	應編製資訊安全管理辦法相關文件	◎					A
運 2			具體實施資訊安全管理標準之文件，應進行評估及修訂作業	◎					A
運 3			建立 資訊安全管理體制	◎					A
運 4			建立 系統管理體制	◎					A
運 5			建立資料管理體制	◎					A
運 6			建立網路管理體制。	◎					A
運 7		2. 組織及分工制衡	設置防災小組		◎	◎			A
運 8			設置防犯小組		◎	◎			A
運 9			確立分工體制		◎	◎			A
運 10		3. 各種規章之訂定	訂定各種規章	◎					A
運 10-1	4. 安控規章遵守狀況之確認	確認對安控規定之遵守狀況	◎					A	
	(二) 進出管理								
運 11		1. 門禁管理	實施人員資格限制及門禁識別工具管理		◎	◎			A
運 12			實施中心門禁管理		◎				A
運 13			實施電腦機房及媒體儲存室之門禁管理		◎	◎			A
	(三) 營運管理								
運 14		1. 手冊之建立	訂定日常作業手冊	◎					A
運 15			訂定故障或災害發生時相關作業之操作手冊	◎					A
運 16		2. 存取權限之管理	明確訂定各種資源、系統等之存取權限	◎					A
運 17			採取防止密碼、 作業憑證 等外洩之措施	◎					A
運 18			明確訂定存取權限之授予及評估等作業程序	◎					A
運 19		3. 操作管理	值勤操作人員之確認		◎				A
運 20			明確規定操作之申請及核可 程序		◎				A
運 21			明確規定操作之執行規範		◎				A
運 22			確認執行結果，並留存操作紀錄		◎				A

營運基準

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
運 23			辦理主從架構系統 (Client Server System) 之作業管理		○	○			A
運 24		4. 資料輸入管理	辦理資料輸入之管理		◎	◎			A
運 25		5. 資料檔案管理	規定資料授受及保管方法	◎					A
運 26			訂定資料檔案之修改管理方法	◎					A
運 27			確保資料檔案之備份作業	◎					A
運 28		6. 程式檔案管理	明確規定程式檔案之管理方法	◎					A
運 29			確保程式檔案之備份作業	◎					A
運 30		7. 電腦病毒之對策	應明確規定因應電腦病毒之對策	◎					A
運 31		8. 網路設定資訊之管理	應落實網路設定資訊之管理	◎					A
運 32			應落實網路設定資訊之備份作業	◎					A
運 33		9. 文件管理	明確訂定文件管理辦法	◎					A
運 34			確保文件之備份作業	◎					A
運 35		10. 傳票帳冊管理	明確訂定未使用之重要空白傳票帳冊管理辦法	◎					A
運 36			明確訂定已印製之重要傳票帳冊處理辦法	◎					A
運 37		11. 資料輸出管理	重要資料之編製、輸出處理等，應具有防止非法使用及保護機密之措施	◎					A
運 38		12. 交易管理	明確訂定各類交易之操作權限		◎	◎			A
運 39			操作人員作業卡之管理		◎	◎			A
運 40			記錄並驗證交易之操作內容		◎	◎			A
運 41			問題帳戶之管理	◎					A
運 42			事先明確告知客戶，使用電子儲值媒體應有之責任及潛在風險損失	◎					A
運 43		13. 金鑰之管理	應明確訂定金鑰使用及管理之辦法	◎					A
運 44		14. 實施嚴謹的身份確認	網路銀行之身分確認			◎			A
運 45		15. 無人化服務區之管理	訂定營運管理辦法			◎	◎		A
運 46			訂定監視機制			◎			A
運 47			明訂防犯措施			◎			A
運 48			訂定故障及災害發生時之因應措施			◎			A
運 49			備妥相關手冊			◎			A

營運基準

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
運 50		16. 可攜式電腦設備管理	明確訂定可攜式電腦設備管理辦法			◎			A
運 51		17. 各類卡片管理	明確訂定卡片管理辦法		◎	◎	◎		A
運 52			明確訂定對特定帳戶卡片交易之監視辦法		◎	◎	◎		A
運 53		18. 客戶資料保護	具有保護客戶資訊的措施	◎					A
運 54		19. 資源管理	掌握各種資源之能力及使用狀況	◎					A
運 55		20. 外部連接管理	明確訂定連接契約之內容	◎					A
運 56			應明確訂定與外部連接之營運管理辦法	◎					A
運 57		21. 機器設備之管理	應明確訂定資訊設備管理辦法		◎	◎			A
運 58			保護通訊網路相關設備之措施		○	○	○		A
運 59			明確訂定設備維護辦法		◎	◎			A
運 60		22. 營運監視	建置完善之監視體制	◎					A
運 61		23. 電腦機房、資料儲存室之管理	嚴密管理進入後之作業		◎	◎			A
運 62		24. 故障災變之因應對策	明確訂定相關人員之聯絡程序	◎					A
運 63			明確訂定故障災變時之復原作業程序	◎					A
運 64			調查、分析發生故障之原因	◎					A
運 65		25. 制定災變備援計畫	制定災變備援計畫	◎					A
(四) 系統開發、變更									
運 66		1. 硬體、軟體之管理	應實施硬體、軟體之管理	◎					A
運 67		2. 系統開發・變更之管理	明確訂定開發、變更之作業程序	◎					A
運 68			建立測試環境	◎					A
運 69			明確規定轉入正式作業之轉換程序	◎					A
運 70		3. 文件管理	格式之標準化	◎					A
運 71			明確規定管理辦法	◎					A
運 72		4. 套裝軟體之引入	套裝軟體之評估制度	◎					B
運 73			明確訂定使用、管理之方法	◎					A

營運基準

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
運 74		5. 系統之廢棄	擬定報廢計畫、作業程序	◎					A
運 75			應具有防止資料外洩之措施	◎					A
(五) 各項設備管理									
運 76		1. 維修管理	明確規定管理辦法		◎	◎			A
運 77			明定維護管理辦法		◎	◎			A
運 78		2. 資源管理	確認設備之容量、性能及使用狀態		◎	◎			A
運 79		3. 監視	建立監控機制		◎	◎			B
(六) 教育訓練									
運 80		1. 教育訓練	實施資訊安全教育	◎					A
運 81			實施提升技巧與熟練度訓練	◎					A
運 82			實施系統操作訓練	◎					A
運 83			實施事故應變操作訓練	◎					A
運 84			實施防災、防犯演練	◎					A
(七) 人員管理									
運 85		1. 人員管理	實施適當人事管理	◎					A
運 86			實施人員健康管理	◎					B
(八) 委外管理									
運 87		1. 委外計劃	系統開發、營運等委外處理，應事先明確訂定作業目標及範圍	◎					A
運 87-1			以明確之程序選擇委外廠商	◎					A
運 88			委託契約內容應包含安全政策相關事項	◎					A
運 89		2. 業務委外管理	規定委外廠商之從業人員應遵守事項並加以管理及檢核	◎					A
運 90			委外業務組織之建立、業務之管理及檢核之執行	◎					A
(九) 系統稽核									
運 91			系統稽核之體制	◎					A
(十) 行外收付處									
運 92			收付處設置地點之選擇基準，應事先明確訂定			◎			A

營運基準

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(十一) 便利超商 ATM								
運 93			設置地點之選擇基準，應事先明確訂定				◎		A
運 94			對於裝填現金等維護作業，應有防犯對策				◎		A
運 95			應明確訂定故障、災害發生時之因應對策				◎		A
運 96			對於網路相關設備，應制定資料傳輸之安全政策				◎		A
運 97			應確立與設備所在地之警察機關、保全公司等相關機構之聯絡體制				◎		A
	(十二) 轉帳卡 (Debit Card)								
運 99		1. 確保轉帳卡服務之安全性	應有轉帳卡服務之安全政策				◎		A
運 100			應確保帳號、密碼之安全性				◎		A
運 101		2. 客戶之保護	客戶使用轉帳卡應有客戶保護措施				◎		A
	(十三) 利用開放網路之金融服務								
運 103		1. 網路銀行、行動銀行	防範不當使用				◎		A
運 104			早期發現非法使用				◎		A
運 105			應公開安全政策相關資訊				○		A
運 106			應明確訂定營運管理辦法				◎		A
運 107		2. 電子郵件	應明確訂定電子郵件之應用方針				◎		B

技術基準

[一、提升系統可靠性]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
(一) 提升硬體設備之可靠性									
技 1		1. 預防硬體設備故障之對策	應實施預防保養		◎	◎			A
技 2		2. 備用硬體設備	設置主機裝置之備用設備		◎	◎			A
技 3			設置週邊設備之備援設備		◎	◎			A
技 4			設置通訊設備之備援設備		◎	◎			A
技 5			設置備用之通訊線路		○	○			A
技 6			端末系統設備之備用設備		◎	◎			A
(二) 提昇軟體系統之可靠性									
技 7		1. 提升開發品質	應確認系統開發設計與中長期計劃的整合性	◎					A
技 8			納入必要的安全控管機能	◎					A
技 9			在設計階段確保軟體之品質	◎					A
技 10			在程式撰寫階段，確保軟體的品質	◎					A
技 11			在程式測試階段，確保軟體的品質	◎					A
技 12			程式派送至使用單位時，應確保軟體的可靠性	◎					A
技 13			外購套裝軟體時，應確保軟體的品質	◎					A
技 14		2. 提升維護品質	確保定型化變更作業的正確性	◎					A
技 15			應確保功能變更、新增作業時的品質	◎					A
(三) 提升營運可靠性之對策									
技 16		1. 提升營運可靠性之對策	力求系統操作之自動化及簡易化	○					B
技 17			系統操作之檢核功能	◎					A
技 18			加強對系統負荷狀態之監控	◎					A
技 19			<u>加強 ATM 之異常偵測能力</u>		◎	◎	◎		B

技術基準

[一、 提升系統可靠性]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
(四) 故障之早期發現、早期復原									
技 20		1. 故障之早期發現	設置系統運轉狀況的監視功能	◎					A
技 21		2. 故障之早期復原	設置故障偵測及將故障部位隔離的機制	◎					A
技 22			應設置發生故障時，能縮小範圍並重組系統的功能	◎					A
技 23			具有限制交易的功能	◎					A
技 24			具有系統復原的功能	◎					A
(五) 災變對策									
技 25			具備災變備援中心		○				A

技術基準

[二、安全性侵害之對策]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 資料保護								
技 26		1. 防止洩漏	具備密碼隱密性之維護措施	◎					A
技 27			應具有識別、確認對方端末設備的功能	○					A
技 28			具有防止儲存資料外洩的功能	○					A
技 29			具有防止資料在傳輸中外洩的功能	○					A
技 30		2. 防止破壞、篡改	檔案存取應具有排他控制（Exclusive Control）的功能	◎					A
技 31			檔案應設置存取控制（Access Control）的功能	◎					A
技 32			加強對不當資料之檢查功能	◎					A
技 33		3. 檢測對策	具備偵測資料傳輸中被篡改的檢測對策	○					A
技 34			具備檔案相互勾核的功能	◎					A
	(二) 防止非法使用								
技 35		1-1. 預防對策（1） 存取權限確認	具備確認使用者身分的功能	◎					A
技 36			具備防止非法使用 ID 的功能	◎					A
技 37			管理系統的歷史資料	◎					A
技 38		1-2. 預防對策（2） 應用範圍之限制	設置限制端末機器、作業與交易範圍的功能	◎					A
技 39			設置在發生事故時能停止交易的功能	◎					A
技 40		1-3. 預防對策（3） 防止非法、偽造對策	具有防止卡片被偽造的對策		○	○	○		A
技 41			對於電子儲值應有檢測非法行為的保護功能機制	○					A
技 42			以電子式儲存基碼值之機器、媒體或軟體，應具有保護基碼值功能	◎					A
技 42-1			對於電子郵件的收發、首頁的瀏覽等，應具有防止非法使用的功能	○					A
技 43		2. 限制外部網路存取	具有防止外部網路非法入侵的功能	◎					A
技 44			由外部網路可以存取的機器設備應維持在最少的數量	◎					A
技 45		3. 偵測對策	設置監視非法存取的功能	◎					A
技 46			設置監視非法交易的功能	○					A
技 47			設置異常交易的監視功能	◎					A

技術基準

[二、安全性侵害之對策]

項目編號	大項目	中項目	小項目	適用性分類					基準等級
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
技 48		4. 因應對策	應備有因應非法存取與復原的對策	◎					A
(三) 防止非法程式									
技 49		1. 防禦對策	具有對電腦病毒等非法程式的防禦對策	◎					A
技 50		2. 偵測對策	應設置偵測電腦病毒等非法軟體的功能	◎					A
技 51		3. 復原對策	具有被電腦病毒等非法程式感染受害時之因應對策	◎					A

貳、基準篇

設備基準

一、資訊中心

(一) 建築物

資訊中心之建築物，對於各類災害及事故等應具有充份之預防措施，萬一發生災變或事故時，亦應有緊急應變措施，將災害減至最低之範圍，並儘速恢復正常運作。

資訊中心之建築物，應依其所在環境、建築物及其周圍等場所，分別預設可能發生的災害、事故等異常情況，應訂定適當之因應措施。

1、環境

設 1、避免設置於容易發生各類災害、事故之區域。

為了降低災害事故對資訊中心之影響，最好避免設置於容易發生各類災害或引起事故之地區。為避免資訊中心之建築物因所在地發生災難而造成不可復原的損壞，危及企業持續營運的能力，得考慮於適當距離外設置異地備援中心。

2、周圍

設 2、檢討因所在地之環境變化，可能發生之災害與事故，並訂定對策。

為降低資訊中心因災害所受影響，應檢討資訊中心隨自然環境、地區環境之變化而可能發生之災害與事故，並訂定防範對策。

設 3、建地應確保必要的通道。

建地應依建築法規之規定，確保必要的通道，以便發生火災時，容易進行滅火作業及避難工作。

設 4、最好與鄰近建物保持充分之間隔。

為防止延燒或滅火工作順利進行，最好能與鄰近建物保持充分之間隔。

設 5、建立圍牆或隔柵以及加裝錄影監視設備防止侵入之設施。

如在建地邊境實施進出管理時，儘可能建立圍牆或隔柵，必要時安裝防止侵入之設施，以防止不法入侵對建物之破壞行為。

設 6、不可將招牌等懸掛在外面。

為能事先預防由外部之侵入、破壞等行為，顯示資訊中心等所在地之標示板、招牌等不宜懸掛在外面。

設 7、建築物應安裝避雷設備及設備獨立接地系統。

在周圍沒有較高之建築物，或在雷擊較多之地區，應於建築物上安裝避雷設備，以防止因雷擊造成故障或事故。

設 8、建築物應為資訊系統相關業務專用，或在建築物內區隔資訊系統相關業務專用之獨立區域。

為了徹底實施安全管制，建築物應闢為資訊系統相關業務專用，或是在建築物內區隔資訊系統相關業務專用之獨立區域。

設 9、建地內通訊與電力線路要有防止切斷、延燒措施及雙迴路管線。

建地內數據通信線路與電力輸送纜線要有預防措施，以避免因施工或外部侵入，而發生切斷、延燒等之事故。

3、結構

設 10、應依據消防署規定之防火建築物。

資訊中心之建築物，應為建築相關法規規定之防火建築物。

設 11、具安全性之結構。

為防止造成資訊系統的事故，應具有建築基準法規訂定之結構安全性。

設 12、外牆、屋頂部份應有充分之防水性能。

外牆、屋頂部份應有防止漏水之措施，以避免長年使用後，因防水、排水性能降低而發生漏水現象，造成資訊系統之故障或事故。

設 13、外牆部份應具足夠之強度。

為防禦資訊系統與相關設備破壞，面臨街道之外牆部份，應具有足夠之強度。

4、門窗

設 14、門窗應有防火措施。

為防止延燒，有延燒可能性之門窗，應有防火措施。

設 15、應有防犯措施。

為防止對資訊中心建築物之不法入侵，對於容易由外部接

近或入侵的一樓等門窗，應有防犯措施。

設 16、平常使用之進出口僅限一處，並設置進出管制裝置、防犯設備等。

為確實辦理進出中心之管理、防止不法的入侵及不明物品的搬進搬出，平時使用之進出口，應僅限一處，並設置進出管制裝置、防犯設備等。

設 17、應設置緊急安全門。

在適當之位置設置緊急安全門，當遭遇災難時能順利避難，並在必要時能疏散各種物件。

設 18、應施以防水措施。

為防止因浸水或漏水造成資訊系統設備之故障，在進出口、門窗、機器設備搬運進出口等之開口部，應施以防水措施。

設 19、進出門窗應具有充分之強度，並需隨時加鎖。

為防犯、防災，進出口之門窗應具充分之強度，並需隨時加鎖。

5、內部裝潢

設 20、應使用具不燃性或耐燃性之材料。

內部裝潢等依建築法規應使用不燃性材料，並依消防法規之規定，使用具備防火性能之材料，以保護內部工作人員及資訊系統之安全。

設 21、對於因地震等裝潢之震落或損壞應有預防措施。

為確保內部工作人員及資訊系統不受到損傷，對於因地震等可能造成裝潢之震落或損壞，應有預防措施。

（二）電腦機房、媒體儲存室

電腦機房或媒體儲存室，多安置連線作業所需之系統及網路中樞設備，或存放重要資料儲存媒體。為了能確保其安全性，對於防止由於發生自然災害及不當行為等造成之損害，設備面應全盤留意。

1、位置

設 22、應設置於不易受到災害的位置。

為了避免資訊系統受到地震、火災或水患之影響，設備應設置於不易受到上述災害之位置。

設 23、應設置於不易由外部進入之位置。

為了預防入侵、破壞、機密外洩，應避免設置於接近進出口、電梯或樓梯等能夠直接進入之位置。

設 24、不可懸掛室名等標示牌。

為了預防入侵、破壞、機密外洩，應避免懸掛電腦機房、媒體儲存室等室名之標示牌。

設 25、確保必要之維修空間。

為設備之維修、人員避難等，應確保必要之空間。

設 26、應為獨立之專用房間。

為徹底執行安全控管，機房應為獨立之專用房間。

2、門窗

設 27、平時使用之進出口，應僅限設置一處，並須設置等候室。

為了確實實施進出機房之管制，平時使用之出入口，應僅限設置一處。同時，為確保安全性，防止外部的熱氣、濕氣、塵埃等侵入，在平時使用之出入口處，最好另設置等候室。

設 28、出入口之門窗，應具有足夠之強度，並須加鎖。

出入口門窗應具有足夠強度，並應予以加鎖，以利防犯、防災。

設 29、窗口應設置防火、防水、防止破壞等措施，並須設置由外部無法窺視機器設備之裝置。

為防犯、防災，設置窗口時，應設置防火、防水、防止破壞等措施、防止窗口玻璃破損措施，更應設置由外部無法窺視機器設備之裝置。

設 30、緊急安全門、避難器具、指示燈、停電照明等設置。

電腦機房應在適當部位開設緊急安全門，並放置避難器具，以便在遇到災難時，能順利避難及疏散各種物件，並應設置引導至緊急安全門的指示燈或方向指標及停電照明等之設置。

3、結構、內部裝潢

設 31、應為獨立之防火區域。

為防止火苗向建築物內其他地區延燒，電腦機房、媒體儲

存室應依建築基準法之規定設置獨立的防火區域。

設 32、應設置防止漏水之對策。

為防止建築物、設備等損傷，以及對資訊系統設備造成故障，屋頂、牆壁、地板等處，應施以防止漏水之措施。

設 33、應設置消除靜電之設備。

為防止靜電對資訊系統之不良影響，電腦機房的地板表面材料等，應施以防止靜電產生及預防帶電等特殊處理。

設 34、內部裝潢應使用不燃性材質或具防火性能之材料。

為保護室內工作人員及資訊設備的安全，內部裝潢應依建築法規之規定，使用不燃性材質，或依消防法規使用具防火性能的材料。

設 35、對於地震等內部裝潢之震落、損壞，應有預防措施。

為保護室內工作人員及資訊設備的安全，房間隔牆、天花板、照明器具等，對於地震有震落、損壞可能性的內部裝潢，應有預防震落、損壞之措施。

設 36、高架地板應具有在地震時不會損壞之構造。

高架地板應具有耐震措施，以免因地震發生而損壞。

4、設備

設 37、應設置自動火災檢知警報裝置。

萬一發生火災時，為能早期發現、發出警報、並啟動初期滅火及避難通報作業，機房內應設置適當的自動火災檢知通報裝置。

設 38、應設置火災等緊急事故警示及緊急連絡裝置。

火災等緊急事故警示及連絡裝置包含警鈴、警報器、緊急廣播設備、緊急電話等。

設 39、應設置滅火設備。

為了避免損及電器系統之安全，電腦機件之滅火劑宜採用氣體類滅火劑，而最好使用能在一定時間內，把滅火所需濃度的滅火劑平均充滿在防火區內的全域噴出型設備。除設置氣體類滅火設備外，亦可加裝自動灑水設備。為撲滅局部火災，應設置如二氧化碳滅火器之類之氣體類滅火器。

設 40、纜線之耐火及防止延燒之措施。

為防止電纜線的燃燒、延燒，電纜線應具耐火措施。對於在牆面電纜線貫穿部分，應有防止延燒的措施。

設 41、應設置排煙設備。

為預防火災之災害，應設置排煙設備。

設 42、應設置緊急照明設備與攜帶式照明設備。

為於火災發生時，人員能即時安全避難，電腦機房內，應設置緊急照明設備及準備攜帶式照明設備。

設 43、不可裝設一般用水的設備。

為防止因漏水造成對資訊系統的嚴重影響，在電腦機房、媒體儲存室內不可設置一般用水設備。

設 44、應安裝地震感應器。

電腦機房儘可能設置地震感應器。

設 45、於機房進出口設置進出管制與防犯設備。

為防止非法入侵，電腦機房、媒體儲存室等出入口，應設置能夠記錄進出狀況之管制設施。另外，儘可能安裝防範歹徒的防犯設備。

設 46、應設置溫濕度自動記錄裝置或溫濕度警報裝置。

為預防資訊系統的故障發生，並能在故障時分析其發生故障的原因，應設置溫濕度自動記錄裝置或溫濕度警報裝置。

設 47、應設有預防蟲鼠害之措施。

設有預防蟲鼠害的措施，以防止電纜線遭蟲、鼠咬損。

5、資訊系統設備、其他各項設備及備用物品

設 48、各類雜項設備及備用品，應具有防火性能。

為防止引火及擴大火災之災害，各類雜項設備及備用品，應使用類似鋼製品等具有防火性能的設備。

設 49、應設置防止靜電之措施。

為防止靜電對資訊系統產生不良影響，對於資訊系統設備、各類雜項設備及備用品，應具有防止靜電的預防措施。

設 50、各類雜項設備及備用品應具有耐震措施。

地震發生時，為不影響工作人員及資訊系統設備，機器設備及各類雜項設備應具耐震措施。

設 51、搬運車等應安裝固定裝置。

地震發生時，為不會傷害工作人員及資訊系統設備，磁帶、磁碟等媒體之搬運車等，應安裝煞車或固定裝置。

(三) 電源室、空調室

電源室內設置之電源設備，是為了對資訊系統供應穩定的電力，空調室內設置之空調設備，也是為了維持、管理機房穩定的溫濕度。這些房間平時都是在無人的狀態下運作，因此應在這些房間，設置能及早發現事故，將災害降至最低範圍的必要裝置。

設 52、應設置於不易受到災害之位置。

為了防止對資訊系統作業的影響，應設置於不易受到地震、火災、水患等災害的位置。

設 53、應確保維修保養時必要的空間。

為機器、設備等之維修保養及工作人員在災難時之避難疏散，應確保必要的空間。

設 54、應為專用之獨立房間。

為了易於維護、管理，並防止災害的擴大，應考量與其他各室分隔專用之獨立房間

設 55、門窗應加鎖，最好不要設置窗戶。

為防止由外部的入侵，並達到防火、防水的目標，最好不要設置窗戶，並在進出的門口設置門禁管控。

設 56、應採用耐火結構。

應採用耐火結構，以防止火災。

設 57、應安裝自動火災警報設備。

為早期發現火災，應安裝自動火災警報設備。

設 58、應安裝氣體滅火設備。

為能因應火災時迅速滅火，應安裝全域放出型之氣體滅火設備。

設 59、空調設備應設有防止漏水的措施。

避免因漏水造成系統的事故，冷卻水應設有防止漏水的措施，以預防冷卻水外漏及凝結等情況發生。

設 60、電纜線、各類導管導線等，應設有防止延燒的措施。

為避免延燒情況發生，應設有防止由電纜線、導管管線等引起延燒的措施。

（四）電源設備

電源設備應隨時供應穩定必要的電力，應避免因停電、異常電壓、異常周波數、電源的瞬斷、過大電流、漏電及電源設備本身的故障等，而影響到資訊系統的正常運作。

設 61、電源設備之容量，應保持充裕有餘。

為能穩定供應資訊系統設備必要的電力，電源設備應備有充裕的容量。

設 62、應以多重迴路引入電源。

為了預防受變電設備發生故障，電源應以多重迴路引進。

設 63、應設置能提供良質電力之供電設備。

為使資訊系統設備能穩定運作，應設置能提供良質電力之

供電設備。

設 64、應設置自備發電機設備及蓄電池設備。

為能在停電期間，維持資訊系統設備之正常運作，應設置自備發電機設備及蓄電池設備。

設 65、電源設備應設置避雷裝置。

為預防因雷擊造成的災害，電源設備最好能設置避雷裝置。

設 66、電源設備應具有耐震措施。

為預防因地震造成電源設備的位移、損傷等，電源設備應具有耐震措施。

設 67、由配電盤至送至資訊系統設備之電源配線應為專屬專用電纜線。

為使資訊系統受到的影響最小，對電腦系統供電之電源纜線，應為專屬專用電纜線。

設 68、應避免與負載變動激烈的機器設備共用電纜線。

為能對資訊系統設備供應穩定的電力，資訊系統設備與負載變動激烈的機器設備應分別配置供電之電源纜線。

設 69、資訊系統設備之接地線，應為專用之地線。

為防止電源設備或其他電氣設備等之不良影響，資訊系統設備的接地線，應為專屬專用之接地線。

設 70、應設有預防措施，以避免因過大電流、漏電等事故，造成設備故障。

應設置預防過大電流、漏電等事故之措施，以免造成各類機器設備之故障。

設 71、應設置防災、防犯用備用電源。

為在停電期間，防災、防犯設備能正常運作，應設置防災、防犯用備用電源。

(五) 空調設備

空調設備應能供給穩定之清淨空氣及適當之溫濕度。

空調設備之一部分機件設備，應安裝於建築物外部，因此應因應來自戶外之雜物侵入及嚴酷氣候條件之對策。

設 72、空調設備，應保持充分寬裕之容量。

空調設備，應保持充分寬裕之容量，以能適當調節電腦機房之溫濕度，並維持資訊系統之持續正常運轉。

設 73、空調設備，應具有穩定調節空氣之功能。

空調設備，應具有穩定調節空氣之功能，以維持資訊系統之正常運轉。

設 74、電腦機房之空調設備，應為獨立使用及維修。

為能確實控制電腦機房之溫濕度，空調設備應避免與其他各室共用。

設 75、應設置備援之空調設備。

空調設備之主要機器設備，應有備援措施，以備故障時能自動切換運轉。

設 76、空調設備應安裝自動控制裝置、異常警報裝置等。

為確保空調設備之正常運轉，除需安裝各種自動控制裝置之外，亦應安裝異常警報裝置，以便能迅速檢知異常狀況，發出警報告知。

設 77、空調設備應具有預防入侵、破壞等措施。

為確保資訊系統作業不受影響，空調設備應具有預防入侵、破壞等措施。

設 78、空調設備應具有耐震之措施。

為能防止地震引起之位移、損傷等影響，空調設備應具有耐震之措施。

設 79、空調設備隔熱材料、排吸氣口應採用耐火材料。

空調設備管道等隔熱材料及排吸氣口應採用耐火材料，以防止火災損害空調設備。

（六）監視控制設備

監視控制裝置，應具有電源、空調、防災、防犯等設備之管理中樞功能，同時具有發生故障之早期發現、通報、復原之功能。

設 80、應安裝監視控制設備。

為能及早發現故障之發生，電源、空調、防災、防犯等設備應安裝監視控制設備。

設 81、宜設置中央監控室。

為使電源設備、空調設備、防災設備、防犯設備等能順利運作管理，並有效發揮功能，宜設置中央監控室，將這些設備予以集中監視控管。

(七) 數據線路相關設備

數據線路相關設備，是指與通訊數據電路之接點，應具有防止非法接觸之措施。

設 82、數據線路相關設備，應上鎖。

為防止不正當之觸動、破壞等非法行為，安裝在電腦機房外之數據線路相關設備機架等，應上鎖。

設 83、數據線路相關設備之安裝場所，不可附加標示。

為避免讓外部人員知道數據線路相關設備之安裝場所不可附加標示。

設 83-1、數據線路相關設備，應備有專用之配線空間。

為防護數據線路故障或犯罪之破壞，並為防止其他電源線等雜訊的混入，應備有專用之配線空間。

二、總行、營業單位

(一) 建築物

總行、營業單位，設置各種端末設備、伺服器、ATM 等自動化服務機器，利用連線通訊網路，與資訊中心連接。為使整體資訊作業穩定運作，總行、營業單位之設備，也應講求安全對策。尤其自動化服務機器設備，在無人化環境（包含設置行外之自動化機器）作業時，應具備適合該環境之防犯、防災措施。

1、周圍

設 84、建地內之通訊線路、供電纜線等，應具有防止被切斷、延燒之措施。

為防止資訊系統作業之中斷，建地內之通訊線路、供電纜線等，應具有防止被切斷、延燒之措施。

2、結構

設 85、應為耐火之建築物。

為預防火災，建築物應為符合建築法規定之耐火建築物。

設 86、建築物應具有安全性之結構。

為確保建築物應有之安全性結構，建築物應依建築法規之規定建造。

設 87、建築物外牆與屋頂應具充分的防水性能。

為防止漏水發生，應具有充分之防水性能措施。

設 88、建築物外牆應確保其強度。

為防禦破壞與入侵，面向公共道路等外牆，應具有足夠之強度。

3、門窗

設 89、窗戶應具有防火措施。

為防止延燒，有延燒可能性之窗戶，均應具有防火措施。

設 90、門窗應有防犯措施。

為防止非法入侵，由外部容易接近、入侵之門窗等，應有防犯措施。

設 91、出入口的門，應有足夠之強度，同時應加裝門鎖。

為防犯、防災，出入口應設置具有足夠強度之門，同時應加裝門鎖。。

設 92、非營業時間之出入口應設置進入者識別用裝置。

為防止非法入侵，營業時間外之出入口應設置如對講機等，能由內部確認對方之識別用裝置。

設 93、進出口應具有防水措施。

為防止雨水等入侵，進出口應具有防水措施。

4、內部裝潢

設 94、天花板及牆壁應具有隔熱、吸音之功能。

為使端末設備運轉正常，發揮功能，天花板及牆壁應具有隔熱、吸音之功能。

設 95、應具有預防措施，以防止因地震而造成內部裝潢震落或損壞。

天花板、牆壁、照明器具等，應有防止震落或損壞的措施，以免傷及工作人員及端末設備等。

設 96、地板面應採用不易積存灰塵或產生靜電的材質。

地板面應採用不易積存灰塵或產生靜電的材質，以減少端末設備發生故障。

設 97、端末設備之通訊線路及電源線路，應具有防止被切斷的措施。

端末設備之通訊線路及電源線路，應設置於適當位置，最好地板下有預留管道，若不得已，需經人員通道，應具有防止不易被切斷的措施。

設 98、端末設備之通訊線路、電源線等，應有防止被漏水浸滲的措施。

對連接於端末設備之通訊線路、電源纜線等，應有防止被漏水浸滲的措施，以避免因事故引起的漏水，造成設備故障、系統停頓。

5、設備

設 99、應安裝自動火災警報及滅火器等設備。

應安裝煙霧感知器之自動火災警報及滅火器等設備，以便萬一發生火災時，能早期發現、發出警報，

以從事初步滅火工作及避難作業。

設 100、各類設備宜有耐震措施。

地震時，所有會影響端末設備之各類雜項設備、物品等，宜有防止掉落、移位或翻倒之耐震措施。

設 101、應安裝耐火金庫或耐火庫房。

應安裝耐火金庫或整室採用耐火材質之庫房，以備火災發生時，能保護災後系統復原所需要之媒體及資料等，以將災害的影響降至最低程度。

設 102、應安裝避雷裝置。

較高之建築物或內部電腦、電源設備等應安裝避雷裝置，以防止因雷擊造成資訊系統故障、室內工作人員觸電死傷、引起火災等事故。

設 103、應安裝防犯措施。

應安裝防犯攝影機、緊急通報裝置等防犯措施，以防範犯罪於未然。

6、線路相關設備

設 104、不可標示通訊線路相關設備安裝場所。

不可標示通訊線路相關設備安裝場所，以防範歹徒。

設 105、易為外界碰觸之通訊線路相關設備等最好上鎖。

容易被非相關人員接觸之通訊線路等相關設備，最好上鎖，以防誤觸或非法行為。

設 106、連結末端機器設備之線路，最好有備援線路。

末端機器設備之線路故障時，為求迅速回復，最好有備援線路。

7、電源設備

設 107、應注意電源線之配置，以確保末端設備之正常作業。

為確保末端機器設備正常作業，電源線應由配電盤直接配置到末端機器設備上，並避免與其他機器設備共用。

設 108、防災、防犯設備應安裝備用電源。

防災、防犯及緊急照明等設備，應安裝備用電源，以備停電時仍能正常運作。

設 109、宜安裝自用發電設備。

儘可能安裝自用發電設備，以因應停電時之需，避免作業中斷。

8、空調設備

設 110、應設置空調設備。

為防止溫濕度失調，致使末端設備異常，應配合末端機器的數量，設置適當的空調設備。

9、自動化服務區

設 111、應安裝直接通話設備。

自動化服務區應裝設電話、對講機等通話裝備，以便在發生故障時與營業廳通話。無人化運作時，應能與中央監控室等單位連線通話。

設 112、應安裝緊急通報裝置。

應安裝緊急通報裝置，以便在緊急時，向營業廳或中央監控室等地方通報。

設 113、宜安裝防犯措施。

應配合自動化服務區之機器配置與周圍環境，綜合考慮自動化服務區及該區機器本身之防犯設備，明訂防犯對策。

設 114、應設置照明設備及緊急照明設備。

應安裝亮度充足的照明設備，以便從室外確認室內的狀況。又為因應停電狀況，儘可能安裝緊急照明設備。

設 115、自動化服務區的門，應有部分為透明透光者。

為防範犯罪於未然，自動化服務區之門，應可由外部看到內部的情況，故門應有部分為透明的。

設 116、自動化服務機器之裝填現金及設備維護作業應確保必要的空間。

為能安全裝填現金及維護自動化服務機器，應於自動化服務機器後面確保必要的空間。

設 117、安裝自動運作設備。

為能適切的執行無人運作，應設置自動運轉設備。

10、端末設備

設 118、端末設備應設有耐震措施。

為防止移位、翻倒等造成端末設備之故障或破損，
同時能保護工作人員，應具防止移位、翻倒等措施。

設 119、機器設備之地線，應確實安裝。

為保護機器設備之安全，對需要安裝地線的設備，
應確實安裝地線，並拉至配電盤上。

設 120、端末設備應有保護措施，不受漏水或塵埃的侵害。

為避免受到漏水或塵埃的侵害，端末設備應備有防
水、防塵套等必要的措施。

（二） 伺服器安裝場所

安裝於資訊中心機房以外（總行、營業單位）之資訊系統設備，
多採用伺服器為主的系統架構，但其使用的形態及服務的內容，
依各金融機構有很大的差異。

本大項中，依各金融機構設置伺服器時，在安全措施上應注意的
事項，分成小項目，分別說明。至於是否實施，由各金融機構依
其資訊系統作業所提供之功能、需要保護的資料及連線服務持續
之重要性等因素，自行判斷決定。

1、位置

設 121、伺服器設備應設置於較不易受到災害的位置。

伺服器設備應設置於較不易受到災害的位置。

設 122、伺服器設備應設置於不易由外部進入的位置。

為防止入侵、破壞、資料外洩等，伺服器設備設置位置應避免接近進出門口、電梯、樓梯等之位置。

設 123、設置伺服器設備的位置，不得張貼具室名等標示之招牌。

為防止入侵、破壞、資料外洩等，設置伺服器設備的位置，不應張貼具室名等標示之招牌。

設 124、設置伺服器設備的位置，應為專用之隔間。

為徹底執行安全管理，設置伺服器設備的位置，應為專用之隔間。

2、結構、內部裝潢

設 125、應設置於具防火能力之隔間內。

為防止因建築物其他地區所發生的火災引起的延燒，設備應依照國內建築技術規則規定設置於防火隔間內，並與其他各室分隔；資料保管室未用防火隔間時，應使用耐火金庫。

設 126、應具防止漏水的對策。

為防止因漏水造成伺服器的損壞，應具備預防天花板、牆壁、地板等地方發生漏水時之因應對策。

設 127、高架地板應具有耐震之措施。

為避免高架地板板面在地震時受到損壞，高架地板應具有耐震之措施。

3、設備

設 128、應具有滅火設備。

為避免因火災造成伺服器的損壞，應設置必要的滅火設備。

設 129、宜設置地震感應器。

安裝伺服器的場所，宜設置地震感應器的裝置，以作為伺服器是否繼續作業之判斷依據。

設 130、在設置伺服器的房間進出，應設置進出管理設備、防犯設備等。

為防止非法入侵，在設置伺服器設備的房間進出門，應設置進出管理設備、防犯設備等。

設 131、應設置溫濕度自動記錄裝置或溫濕度警報裝置等。

為預防電腦系統的故障，維持正常運轉，同時在發生故障時，能分析故障原因，應設置溫濕度自動記錄裝置或溫濕度警報裝置等。

設 132、應設置空調設備。

為確保電腦機房適切的溫濕度，應設置專屬的空調設備。

設 133、應有防止鼠害的措施。。

為能防止因鼠害造成電纜線之破損，應有適當的防範措施。。

設 134、應有防止電源插頭由插座鬆落的措施。

為防止電源插頭輕易的鬆脫，電源插座應有防止脫落的措施。

(三)行外收付處

行外收付處可能會利用駐外營業場所既有的設備，營業時間可能與駐外地點商店的營業時間不同，或與總行、營業單位等營業時間不同。因此其設備應加強防犯措施，防止破壞、入侵情況發生。

設 135、應有防止由其他區域入侵的措施。

為防止入侵、破壞的情況發生，行外收付處之作業區域，應與其他商店區域劃分為獨立的防犯區域。

設 136、配合使用商店設備之狀況，應有適當的補強對策。

為防止入侵、破壞的情況發生，若行外收付處之商店既有設施與金融機構的要求不符時，在設備補強及作業應用面，應有適當的因應對策。

三、與流通業、零售店合作之合作通路

(一) 便利商店之 ATM

安裝於便利超商之 ATM，與設置於自動化服務區的 ATM 不同，便利超商係多數不特定的人物進出往來的場所，亦未設置自動化服務區域或機械室等，多僅單獨設置自動化服務的機器設備。因此，與設置於總行、營業單位自動化服務區之 ATM 設備比較，應有較強化之防犯對策。

設 137、應有防犯措施。

為確保設置於便利超商 ATM 之安全，應配合設置形態、週邊環境，對防犯設備及 ATM 本身之防犯措施，作一適切的組合，建立必要的防犯對策。

營運基準

(一) 確立管理體制

1、資訊安全管理與責任之明確化

設置於電腦機房中央集權型之主機系統，其存放系統內之資料，基於主要建築物之結構及進出機房管理等物理上之安全對策，已有必要之最低要求保護機能。但利用主從架構之系統（Client/Server System）或連結在網際網路之系統，在資料處理環境與作業目標，有多種型態，依過去之物理性安全對策，並不足以保護系統。資料之保護，不僅需要使用者具備安控管理之意識，同時對於資訊保護不是依賴使用者個人之裁量判斷，而應為整個機構安控理念之統一所制定之資訊安全政策。

本基準所謂資訊安全政策，是指機構（或是組織）為適切的保護其資訊資產，在機構內部整合之基本方針。在此，應明確化之內容，是指必須要保護之重要資訊資產到底是什麼，為什麼需要保護這些資訊，對這些資訊之保護責任又如何等內容。為能適當的實施安控管理，應先行訂定包含：資訊安全政策（基本方針）、資訊安全管理之標準（機構本身訂定之安控對策基準）、手冊或程序說明書等說明安控管理具體方法之相關文件，確實實施資訊系統之安控對策。

運 1、應編製資訊安全管理辦法相關文件。

為能適切執行安控管理，應事先編製文件，明確記載安控管理之具體程序、責任劃分等。

運 2、具體實施資訊安全管理標準之文件，應進行評估及修訂作業。

為能建置最適切的資訊安全管理標準，編製完成的文

件，應定期評估及檢討，對現行業務的狀況是否相宜，必要時應予以修訂。

運 3、建立資訊安全管理體制。

為能適切實施資訊安全管理，應指定資訊安全管理負責人，明確訂定其職務範圍、權限及應負之責任。

運 4、建立系統管理體制。

為能順利運用資訊安全管理並防止非法行為，應訂定系統管理程序，建立管理之體制。

運 5、建立資料管理體制。

為維護資料安全，並防止非法行為導致資料損毀或洩露，應訂定資料管理程序，建立管理之體制。

運 6、建立網路管理體制。

為能有效運用網路系統，並防止非法存取行為，應訂定網路管理程序，建立管理之體制。

2、組織及分工制衡

為保護金融機構資訊系統，使其能安全、順利運轉，並避免其受到災害、故障、入侵或犯罪等事故之重大影響，於發生事故時，能將受災程度減至最低、及早復原，應設置相關組織及訂定權責。

運 7、設置防災小組。

為預防災害並減輕受害程度，應設置防災小組，並明確指定負責人。

運 8、設置防犯小組。

為防止犯罪發生，應設置防犯小組，並明確指定負責人。

運 9、確立分工及代理體制。

為使資訊系統順利運轉，並防止非法事件發生，應有適當之職務分工，明確劃分業務範圍及責任、權限，以確立相互制衡體制。

3、各種規章之訂定

為使資訊系統順利運轉，應明確訂定劃分責任與權限之規章。

運 10、訂定各種規章。

為使資訊系統順利運轉及管理，對於防災、防犯小組及分工體制應明確訂定劃分責任與權限之規章。

4、安控規章遵守狀況之確認

為確保資訊系統順利運轉，應確認對於資訊安控相關規章所定各事項之遵守狀況。

運10-1、確認對安控規章之遵守狀況。

應確認對安控規章之遵守狀況，全體員工(包含駐外人員)及委外人員應對資訊安全政策確實認知，並努力提升機構之安全層次。

(二) 進出管理

1、門禁管理

為防止非法入侵、攜入危險物品、非法攜出物品等，對進出資訊中心或電腦機房等重要房間(館或室)之人、物，應加以管制。

運 11、實施人員資格限制及門禁識別工具管理。

為防止非法侵入，人員進入資訊中心、電腦機房、媒體儲存室、程式開發場所及電腦相關設備房應實施資格限制，鑰匙、門禁磁卡、識別碼等，應確實管理。

運 12、實施中心門禁管理。

為防止非法之侵入、危險物品之攜入及物品之非法攜出等，對進出人員應確認其身分，實施資訊中心之門禁管理。

運 13、實施電腦機房及媒體儲存室之門禁管理。

為防止非法之侵入、危險物品之攜入及物品之非法攜出等，對於電腦機房、媒體儲存室及中央監控室等重要區域，應實施進出管理。

(三) 營運管理

1、手冊之建立

為能正確安全運用資訊系統，日常各種作業處理程序等應標準化，並備妥完整之作業手冊。同時，對於系統故障或災害發生時，為使對系統之影響減至最小，並能在最短時間內復原系統，應明確訂定故障或災害發生時之系統操作程序，整理完整之作業手冊。

運 14、訂定日常作業手冊。

為正確且安全運轉資訊系統，應規定日常各種程序之

作業手冊。

運 15、訂定故障或災害發生時相關作業之操作手冊。

為減低故障、災害發生所導致資訊系統之影響並能及早復原，同時總行、營業單位能持續營運，應訂定故障、災害發生時之備援措施、復原程序等相關作業之操作手冊。

2、存取權限之管理

為防止資訊系統、檔案等各種資源遭非法使用或破壞，應依系統重要程度設定其存取使用權，並加以管理。

運 16、明確訂定各種資源、系統等之存取權限。

為防止非授權人員存取使用資訊系統及其重要檔案，應限定使用者之存取權限。

運 17、採取防止密碼、作業憑證等外洩之措施。

為防止密碼、作業憑證等之外洩，除應加強保護外，應宣導使用者落實管理。

運 18、明確訂定存取權限之授予及評估等作業程序。

管理各種資源、系統等存取權限之授予，應明確訂定其作業程序。同時，為維持存取權限之妥適性，應明確訂定定期評估之作業程序。

3、操作管理

為防止電腦系統之非法使用，並求運轉順利，有關操作應實施申請、核可、執行、記錄、結果之確認等管理。

運 19、值勤操作人員之確認。

為防止電腦系統之非法使用，應確認是否為值勤操作人員。

運 20、明確規定操作之申請及核可程序。

為防止電腦系統之非法或不當使用，應明確規定操作之申請及核可程序。

運 21、明確規定操作之執行規範。

為防止操作錯誤或違規使用，應明確規定操作之執行規範。

運 22、確認執行結果，並留存操作紀錄。

為驗證操作之正確性，應確認執行結果，並留存操作紀錄。

運 23、辦理主從架構系統（Client Server System）之作業管理。

為防止對主從架構系統（Client Server System）之非法使用，應明確訂定作業申請、核准等之程序，並有適切之執行、記錄機制。

4、資料輸入管理

為能確保輸入資料之安全性及完整性，應建立資料輸入之作業程序，並要求相關部門落實此作業程序。

運 24、辦理資料輸入之管理。

為保障資料之正確及防止非法作業，應訂定資料輸入

之作業程序。

5、資料檔案管理

為防止資料檔案之不當使用、篡改、毀損或遺失等，應由專人按規定方法執行資料檔案授受及保管作業。同時為預防資料檔案毀損、故障等情形，應確實執行檔案備份作業，以備資料檔案遭破壞或事故時之需。

運 25、規定資料授受及保管方法。

為防止資料檔案之不當使用、篡改、毀損及遺失等，其授受及保管，應由專人按規定辦理。

運 26、訂定資料檔案之修改管理方法。

為防止非法使用或篡改，凡資料檔案之修改，應先取得部門負責人之核准後按規定辦理，並驗證其辦理之結果。資料檔案修改紀錄，亦應依重要程度規定其保存期限。

運 27、確保資料檔案之備份作業。

為防範重要資料檔案發生毀損或故障等事故，應製作備份檔案及制定復原程序，明確規定管理方法。

6、程式檔案管理

為防止程式被篡改或破壞等，程式檔案應由專人按規定管理。並確實執行程式檔案之備份作業。

運 28、明確規定程式檔案之管理方法。

為防止程式被篡改或破壞等，應由專人按規定方法執行程式檔案入出庫管理及保管作業。

運 29、確保程式檔案之備份作業。

為防範程式檔案發生毀損或故障等事故，應製作備份程式及制定復原程序，並明確規定管理方法。

7、電腦病毒之對策

為預防非法篡改或破壞程式之電腦病毒，應明確規定防止電腦病毒入侵之對策，或遭入侵時之檢測對策。同時為預防被入侵感染，應明確規定檔案備份作業、系統復原作業等程序。

運 30、應明確規定因應電腦病毒之對策。

為預防電腦病毒入侵或感染，應明確訂定偵測、防禦、復原等作業程序。

8、網路設定資訊之管理

為預防網路設定資訊被非法篡改，應妥善管理上述設定資訊。同時，為預防上述設定資訊遭破壞或發生故障，應落實檔案備份作業。

運 31、應落實網路設定資訊之管理。

為預防電腦系統網路設定資訊被篡改，應強化網路設備管理人員帳號密碼保護機制，落實網路設定資訊之管理。

運 32、應落實網路設定資訊之備份作業。

為預防電腦系統網路設定資訊被非法篡改或因應故障發生，應明確訂定備份檔案之取得作業程序及管理辦法。

9、文件管理

為預防文件之不當使用或遺失等，應由專人按規定辦法管理之。另外，發生故障或災害時，為復原作業所需文件，應明確訂定取得備份文件及管理之辦法。

運 33、明確訂定文件管理辦法。

為預防文件不當使用、篡改或遺失，文件應依照規定辦法管理。

運 34、確保文件之備份作業。

為因應災害發生時之復原作業，應明確訂定所需文件備份之取得及管理辦法。

10、傳票帳冊管理

為預防傳票帳冊不當使用或資料內容外洩等，應明確訂定重要傳票帳冊之管理辦法及報廢程序等。

運 35、明確訂定未使用之重要空白傳票帳冊管理辦法。

為防止不當使用，未使用之重要空白傳票帳冊，其庫存管理及報廢，應依照規定辦理。

運 36、明確訂定已印製之重要傳票帳冊處理辦法。

為防止非法使用，已印製之重要傳票帳冊，其保管、交接或報廢應依照規定辦理。

11、資料輸出管理

為預防輸出資料不當使用或資料內容外洩，及保護資料的機密性、隱私權等，應明確訂定輸出資料之管理規則。

運 37、重要資料之編製、輸出處理等，應具有防止非法使用及保護機密之措施。

為防止重要輸出資料遭篡改、竊取、洩漏等，在編製及輸出處理過程，應有防止非法使用及保護機密之對策。

1 2、交易管理

為預防端末機器遭非法使用、啟動不當交易等，除應有操作人員身份識別及權限管理外，同時應詳細記錄交易的操作內容，並加以檢核。

運 38、明確訂定各類交易之操作權限。

為防止利用利用端末設備從事不正當交易，應依照交易內容，分別訂定端末設備操作者所能操作之權限範圍。

運 39、操作人員作業卡或使用者帳號之管理。

為防止利用端末設備從事不正當交易，應指派專人負責管理操作人員作業卡或使用者帳號。

運 40、記錄並驗證交易之操作內容。

為防止利用端末設備從事不正當交易，應建立可由交易明細表、端末設備操作紀錄等驗證交易內容之制度。

運 41、問題帳戶之管理。

為防止利用事故從事非法交易，對於掛失止付等問題帳戶，應規定事故申報處理之管理方法。

運 42、事先明確告知客戶，使用電子儲值媒體應有之責任及潛在損失風險。

為提醒客戶注意，利用電子儲值媒體（卡）或通訊等機器設備遭竊、破損時，客戶可能遭受損失，以及應由客戶承擔之責任等，應事先有明確的提示告知客戶。

1 3、金鑰之管理

金融機構在管理金鑰時，為預防資訊之洩露及非法使用，應明確訂定登錄、變更之程序，並嚴格管理。

運 43、應明確訂定金鑰使用及管理之辦法。

為防止非法使用，應明確訂定金鑰之產生、遞送、使用及管理等相关作業程序，同時相關文件，應由專人嚴格管理。

1 4、實施嚴謹的身份確認

網路銀行服務等是利用通訊網路提供銀行業務交易。此業務係以非面對面之方式執行，對於新開戶交易，客戶本人身份之確認是非常重要的。

運 44、網路銀行之身份確認。

網路銀行等以非面對面之方式辦理開戶手續時，應有適當之方法，確認本人身份。

1 5、無人化服務區之管理

為能使 ATM 及無人銀行能順利運轉，並符合安全政策，在發

生犯罪、故障或災害時，應有明確的因應辦法。此處所稱之「無人銀行」是指利用 ATM 等提供無人化服務之營業據點。

運 45、訂定營運管理辦法。

為確保 ATM 及無人化服務區之安全性與順利運作，應訂定營運管理辦法。

運 46、訂定監視機制。

為發現無人化服務區之異常情況，應明確訂定監視機制。

運 47、明訂防犯措施。

為防止於無人化服務區發生犯罪行為，應明確訂定預防及發生時之因應措施。

運 48、訂定故障及災害發生時之因應措施。

為使無人化服務區能順利運作，應明確訂定故障及災害發生時之因應措施。

運 49、備妥相關手冊。

無人化服務區相關手冊，應依總行、資訊中心、管制中心、營業單位、保全公司等分別編製，遇有變動應即時更新。

1 6、可攜式電腦設備管理

為確保安全性並順利處理業務，可攜式電腦設備應依規定管理。同時，為預防可攜式電腦設備不當使用、破壞、遺失或被竊等，應有具體之因應對策。

運 50、明確訂定可攜式電腦設備管理辦法。

為防止可攜式電腦設備之不當使用，應明確訂定可攜式電腦設備管理辦法。

1 7、各類卡片管理

為防止各類卡片遭非法使用，卡片之發卡、保管以及遞送等，應依規定程序執行。同時，應對特定帳戶之卡片進行交易時提供監視之功能。另外，對於金錢支付用、簡易貸款用、收受資訊用等各種不同名稱卡片，亦應遵守本基準項目之規定。

運 51、明確訂定卡片管理辦法。

為確保安全性及卡片之發卡、保管、遞送、回收以及作廢等作業順利，應明確訂定卡片管理辦法。

運 52、明確訂定對特定帳戶卡片交易之監視辦法。

為防止非法使用，應明確訂定在必要時對特定帳戶卡片交易之監視辦法。

1 8、客戶資料保護

金融機構應謹慎及適當的保護處理客戶個人資料資訊。

運 53、具有保護客戶個人資料資訊的措施。

為保護及適當使用客戶資訊，應訂定處理客戶個人資料之管理辦法。

1 9、資源管理

為避免由於各種資源（構成電腦系統之硬體、系統軟體、應用軟體及各類檔案）之性能或容量極限所引起之事故或處理能力之下降，應實施各種資源之管理。

運 54、掌握各種資源之能力及使用狀況。

掌握各種資源之能力及使用狀況，並研擬適當之因應措施。

20、外界連接管理

為安全及正確執行與外界之連接，並防止資料之洩露或遭非法使用等，凡有關透過連線而與顧客做資料授受者，應有確認連接對方為合法者之功能，並實施適當的管理。

運 55、明確訂定連接契約之內容。

為正確及安全執行與外界之連接，凡透過連線執行資料授受有關之契約，應在契約中明確訂定連接方法、資料格式及資料內容等。

運 56、應明確訂定與外部連接之營運管理辦法。

為防止資料外洩、非法存取等，應明確訂定與外部連接之營運管理辦法，並確實執行確認連接對象身分、確認連接條件(如登錄密碼等)及變更之管理。

21、機器設備之管理

為使構成資訊系統之各種機器故障減至最低程度，並防止非法使用或遭破壞，應訂定機器管理及維護方法，並明確規定管理負責人之權責。

運 57、應明確訂定資訊設備管理辦法。

為防止資訊系統之各種設備發生故障、非法使用、破壞、遭竊等，應明確訂定資訊設備管理辦法。

運 58、保護通訊網路相關設備之措施。

為防止設備之非法使用、破壞、遭竊等，對於構成處理重要資料之系統通訊網路設備應有適當之保護措施。

運 59、明確訂定設備維護辦法。

為防止資訊系統之各類機器設備發生故障，應確實執行維修保養作業，並確實掌握維修之內容及結果。

2 2、營運監視

為能早期發現異常狀態，應經常監視系統運轉之狀況。

運 60、建置完善之監視體制。

為能早期發現系統之異常狀況，應訂定包含監視對象、監視內容及監視方法等相關機制。

2 3、電腦機房、媒體儲存室之管理

為防止非法入侵、攜入危險物品、非法攜出物品等，應嚴密管理電腦機房、媒體儲存室等重要房間之進出。

運 61、嚴密管理進入後之作業。

為防止非法入侵、攜入危險物品、非法攜出物品等，應嚴密管理電腦機房或媒體儲存室等重要房間之進出。

2 4、故障災變之因應對策

為將資訊系統故障與災變對顧客、總行、營業單位之影響降至最低，同時儘早完成復原作業，應訂定故障災變之因應對策。

運 62、明確訂定相關人員之聯絡程序。

在故障、災變發生時，為迅速確實聯絡相關人員，應事先訂定人員聯絡之作業程序。

運 63、明確訂定故障災變時之復原作業程序。

應明確訂定因故障或災變，造成資訊系統無法正常運作時之復原作業程序，此復原程序應與災變備援計畫之內容具相容整合性。

運 64、調查、分析發生故障之原因。

為迅速回復資訊系統之作業功能，應調查、分析發生故障之原因。同時，應記錄故障原因，作為故障原因之統計分析，以避免再次發生問題。

2 5、制定災變備援計畫

於資訊系統發生故障或災害時，為使相關業務能在短時間內回復正常運作，應以假設事件為基礎，擬定災害備援作業計畫（緊急應變計畫）。

運 65、制定災變備援計畫。

對於無法預測之事故、災變及重大損害等，造成業務執行之困難時，為將損害範圍及對業務之影響降至最低，並能儘速復原，應事先制定災變備援計畫（緊急應變計畫）。

（四）系統開發、變更

1、硬體、軟體之管理

為能確實對應系統結構之變更，安裝建置之硬體設備及軟體

組成等，應以資產清冊等加以管理。

運 66、應實施硬體、軟體之管理。

為能確實執行系統之安裝建置、變更、報廢等，應實施硬體、軟體之組成架構、版本數量等之管理。

2、系統開發、變更之管理

為確保系統開發及其內容變更之正確性，兼顧系統之安全性，應明確訂定系統開發、變更之作業程序、測試環境之建置等整合性之管理機制。

運 67、明確訂定開發、變更之作業程序。

為確保系統開發、變更內容之正確性，應明確訂定開發、變更之作業程序。

運 68、建立測試環境。

為確保正式作業系統之安全性，應建立對正式作業系統不會造成影響之測試環境。尤其測試大型系統時，應制訂包括相關人員在內之測試制度。

運 69、明確規定轉入正式作業之轉換程序。

確保正式作業系統之安全，轉入正式作業時應明確規定其轉換程序。

3、文件管理

為使開發、變更作業順利進行，並防止篡改或不當使用等，應訂定有關系統開發及變更文件之管理方法。

運 70、格式之標準化。

為使開發及變更作業順利，應將在系統開發及變更各階段所使用之文件格式予以標準化。

運 71、明確規定管理辦法。

為防止篡改及不當使用等，應訂定規格書等設計文件之保管方法。

4、套裝軟體之引入

引進套裝軟體時，為能順利進行系統開發、修改等，應建立套裝軟體適用性之評估制度，並明確訂定套裝軟體之應用及管理。

運 72、套裝軟體之評估制度。

引進套裝軟體時，為能順利進行系統開發、修改等，應由系統開發部門及使用部門（營業單位）等單位共同評估。

運 73、明確訂定使用、管理之方法。

為順利辦理套裝軟體引進後對應事故或擴充功能，應明確訂定套裝軟體之使用與管理方法。

5、系統之廢棄

系統報廢時，對機密資料的保護、隱私權的保護、防止非法行為等，應確實遵守報廢計畫及相關作業程序等之規定。

運 74、擬定報廢計畫、作業程序。

為使系統報廢能順利、確實且安全，應擬定包含防範非法行為與保護機密等措施之計畫與作業程序。

運 75、應具有防止資料外洩之措施。

為保護機密或個人資料，防止非法行為，在系統報廢時，應有防範由機器設備洩漏資料之措施。

（五） 各項設備管理

1、維修管理

為使資訊系統順利運轉，應明確訂定電源、空調、供/排水、防災、防犯、監視、通訊線路等相關設備之管理及維護辦法。

運 76、明確規定管理辦法。

為使資訊系統運轉順利，應明確規定管理辦法，指定設備管理負責人員，依規定管理設備。同時，對於發生故障災變時之因應對策亦應明確規定。

運 77、明定維護管理辦法。

為使資訊系統運轉順利，應確實進行保養維護，並掌握維護結果。

2、資源管理

為使資訊系統順利運轉，應掌握各項設備之容量、性能及使用狀態。

運 78、確認設備之容量、性能及使用狀態。

應掌握各項設備之容量、性能極限，及其使用狀態，以早期發現異常情況。

3、監控

為及早發現異常情況，應隨時監控影響資訊系統運作之各項設備之運轉情況。

運 79、建立監控機制。

為早期發現異常情況，應建立監控機制，訂定監控標準的及監控方法等。

(六) 教育訓練

1、教育訓練

為能安全並順利運轉資訊系統，應對相關人員實施資訊安全教育訓練。並明訂教育訓練之目的、訓練計畫及實施辦法等。

運 80、實施資訊安全教育。

為提升全體員工（包含駐外人員）對資訊安全之認識，充分了解相關法令（如個人資料保護法）規定、組織之資訊安全政策及具體資訊安全措施，應配合業務實施相關教育訓練。

運 81、實施提升技巧與熟練度訓練。

為提升對系統及業務相關之知識及技能，應對系統開發人員施以必要訓練。

運 82、實施系統操作訓練。

為使人員能熟練營業單位資訊系統操作，以順利處理日常業務，應實施系統操作訓練。

運 83、實施事故應變操作訓練。

為期事故發生時，仍能維持作業，平常應演練應變作業。

運 84、實施防災、防犯演練。

為預防緊急狀況發生，應實施防災、防犯演練。

(七) 人員管理

1、人員管理

為使資訊系統能安全平順運轉，對系統開發、維護及操作人員，應適切實施人事管理及健康管理。

另外，對於人員的配置，應充分瞭解、評估每一員工的能力，確實區分職掌、權限等，以明確賦予適當的職責。

運 85、實施適當人事管理。

為使系統順利運轉，人員配置、代理人員等之人事管理應適切的實施。

運 86、實施人員健康管理。

建立完善之作業環境，定期的健康檢查等，以適切實施人員的健康管理。

(八) 委外管理

1、委外計畫

金融機構近年來對於資訊系統的開發、營運等，包含執行業務所必要的管理，委外處理或將某些業務完全委外之情況漸增。

委外作業之主要型態，也自委託給子公司，逐漸轉移為委託電腦廠商或資訊處理公司。

再者，多家金融機構共用資訊系統的「共用中心」也有增加的趨勢。

如上所述，金融機構的資訊系統開發、營運等，委外處理的範圍逐漸擴大，其內容也多樣化，在這種情況下，資訊系統策略的擬定，有關委外處理的事項，應經過充分的研究及檢

討。

因此，在個別系統的開發或營運上，委外處理的計畫、實施等，應以資訊系統策略為基礎，在決定委外處理的目的、範圍及風險管理上，應有具體措施。

除上述問題外，對於委外處理相關之安全與保密對策亦需一併考慮。

運 87、系統開發、營運等委外處理，應事先明確訂定作業目標及範圍。

系統開發、營運等委外處理，應事先明確訂定作業目標及其範圍。

運 87-1、以明確之程序選擇委外廠商。

在選擇委外廠商時，其選擇程序應明確而客觀，並應將選定結果呈報主管核准。

運 88、委託契約內容應包含安全政策相關事項。

為確保安全性，在委託契約內，應包含保密、安全與稽核條款。

2、業務委外管理

運 89、規定委外廠商之從業人員應遵守事項並加以管理及檢核。

應對委外廠商之從業人員實施適當安控管理，依委外業務內容及作業範圍等，訂定應遵守安全政策及相關各種規定，並進行教育訓練及監督稽核等。

運 90、委外業務組織之建立、業務之管理及檢核之執行。

為確認委外處理之業務內容，得配合調整業務組織，並依委外契約內容，執行業務管理及檢核工作。

（九）系統稽核

為確保資訊系統之開發、變更及系統營運之有效性、效率性、信賴性、遵守性與安全性，應具備完備之系統稽核體制。

運 91、系統稽核之體制。

為全面掌握並評估資訊系統及其管理之有效性、效率性、信賴性、遵守性及安全性，應建立系統稽核之體制。

（十）行外收付處

行外收付處多為開放式之擺設(Layout)，並以少數人員從事營運之據點，與一般總行、營業單位等，在營運上有差異。為確保行外收付處之安全性，據點之設置地點及商店之選擇基準，應事先明確訂定。

運 92、收付處設置地點之選擇基準，應事先明確訂定。

為確保行外收付處之安全性，選擇設置地點之基準應事先明確訂定。

（十一）便利超商 ATM

設置於便利超商之 ATM 與設置於自動化服務區之 ATM 不同，便利超商為不特定之多數人員進出之場所，且無法區隔設置自動化服務區及機械室等，而是機器設備單獨設置之服務區域。因此，設置於便利超商之 ATM 營運應考慮使用及維護人

員之安全。

運 93、設置地點之選擇基準，應事先明確訂定。

為確保便利超商ATM使用者之安全，設置地點與便利超商之選擇基準，應事先明確訂定。

運 94、對於裝填現金等維護作業，應有防犯對策。

為確保便利超商ATM維護作業之安全，應明確訂定防犯體制及防犯辦法。

運 95、應明確訂定故障、災害發生時之因應對策。

裝置於便利超商之ATM發生故障、災害時，為能迅速因應，應明確訂定因應程序。

運 96、對於網路相關設備，應制定資料傳輸之安全政策。

為確保資料傳輸之安全性、信賴性，並防止非法之使用、破壞、篡改，對於網路相關設備應有適當之保護措施以及資料傳輸之安全政策。

運 97、應確立與設備所在地之警察機關、保全公司等相關機構之聯絡體制。

為在發生犯罪行為時，迅速聯絡通報相關單位，應確立與設備所在地之警察機關、保全公司等相關機構之聯絡體制，並經常演練。

(十二) 轉帳卡(Debit Card)

為確保轉帳卡(DebitCard)服務之安全性，顧客(帳戶所有人)、發行卡片之金融機構等、加盟店金融機構、加盟店等，應共同協力維持系統之安全。此處所提之轉帳卡服務之安全

對策，是記述金融機構等應特別注意之事項。

1、確保轉帳卡服務之安全性

為確保轉帳卡服務之安全性，提供服務之金融機構與資料處理之相關單位應共同研訂實施相關安全政策。

運 99、應有轉帳卡服務之安全政策。

為確保轉帳卡服務之安全性，提供服務型態的金融機構與資訊處理中心、加盟店等，應有共同之安全對策。

運 100、應確保帳號、密碼之安全性。

為確保帳號、密碼之安全性，依照金融機構等所提供之服務形態、資料處理中心及加盟店等，應有共同之安全對策。

2、客戶之保護

為確保客戶在使用轉帳卡時之安全性，應有適當之客戶保護措施。

運 101、客戶使用轉帳卡應有客戶保護措施。

為確保使用轉帳卡之安全性，應有適當之客戶保護措施。

(十三) 利用開放網路之金融服務

1、網路銀行、行動銀行

為保障客戶得交易安全，對於開放網路上種種安全之威脅，應有安全對策。

在開放網路上執行業務之安全威脅，如竊聽、偽裝他人、資訊竄改、非法入侵、竄改置換首頁內容等。為因應這些威脅，

資訊系統應實施安全對策。

同時，對於發生故障之對應方法，事故之免責範圍等，應明確訂定記載。

運 103、防範不當使用。

為確保利用開放網路之金融服務安全性，應有能確認連接對象確實是客戶本人，或限制使用權限等之檢知對策，以防止非法使用系統。

運 104、早期發現非法使用。

為防範使用者非法使用，應設置使用者本身能確認使用狀態之機制。

運 105、應公開安全政策相關資訊。

為讓使用者能適當選擇往來之金融機構或服務，應公開有關安全政策之資訊。

運 106、應明確訂定營運管理辦法。

在利用網路銀行、行動銀行等執行銀行交易、證券交易、人壽保險、產物保險等之交易時，為保護使用者，確保交易安全，並使作業順利進行，應明確訂定營運管理辦法。

2、電子郵件

利用電子信箱，向使用者提供交易明細、金融商品相關資訊以及回覆問題諮詢時，應考慮電子郵件之特性，判斷對象業務之應用方針應予以明確化。

運 107、應明確訂定電子郵件之應用方針。

關於電子郵件之運用，為確保其信賴性及安全性，其應用方針應明確化。

技術基準

一、系統可靠性之提升對策

(一) 提升硬體設備之可靠性

若要提升資訊系統可靠性，首先需要提升構成系統要素之硬體設備之可靠性。這是指應極力減少資訊系統本身及其週邊相關連設備發生故障。

其次，當構成硬體設備要素之一部分發生故障時，應有避免影響整個系統的因應措施，這些措施，應依各個硬體設備之特性及其重要性，分別實施。

1、預防硬體設備故障的對策

技 1、應實施預防保養。

預防硬體設備的故障，應依據裝置的特性及其重要性，定期實施預防保養作業，必要時應隨時加強保養。

2、備用硬體設備

技 2、設置主機裝置之備用設備。

重要之主機設備應設置備援設備。

技 3、設置週邊設備之備援設備。

重要之週邊裝置應設置備援設備。

技 4、設置通訊設備之備援設備。

重要的通訊裝置應設置備用的設備。

技 5、設置備用之通訊線路。

重要的通訊線路應設置備用線路。

技 6、端末裝置之備用設備。

端末系統裝置應設置備援設備。

(二) 提昇軟體系統之可靠性

若要提升資訊系統可靠性，應提升軟體系統之可靠性。由技術面來看，在市面上提出的提升軟體系統可靠性之方法論及工具為數不少，在實際應用上，系統開發的各階段中，應採用那一種方法或工具，或採用這些方法或工具的目的，應明確訂定於系統開發設計的計劃內。同時，為能達到開發作業之標準化及作業的自動化，如何提升軟體系統可靠性的對策，是非常重要的。

其次，使用套裝軟體時，應注意與現運轉中的系統之整合性。在總行、營業單位之使用者，自行開發之作業，應注意參考系統開發部門的規範，以確保其可靠性。

1、提昇開發品質

技 7、應確認系統開發設計與中長期計劃的整合性。

為提升資訊系統整體的的可靠性，系統的開發設計與中長期計劃應具整合性。

技 8、納入必要的安全控管機能。

為確實實施安全控管，在系統計劃階段就應將必要的安全控管機制納入，並使其明確化。

技 9、在設計階段確保軟體之品質。

為在設計階段提升軟體的可靠性，開發前提應明確化，同時考量具可靠性設計、採標準化之設計作業等，確保軟體的品質。

技 10、在程式撰寫階段，確保軟體的品質。

依據程式規格書撰寫程式時，應實施程式撰寫的標準化、自動化、安全性等，以能在程式撰寫階段，確保軟體的品質及減少程式的安全漏洞。

技 11、在程式測試階段，確保軟體的品質。

為在程式測試階段，提升軟體的可靠性，應擬定測試計劃、準備測試環境與測試體制、並活用支援測試的功能，在測試階段實施各種管理，以確保軟體的品質。

技 12、程式派送至使用單位時，應確保軟體的可靠性。

為確保程式派送至使用單位時的可靠性，應確認軟體與發送之使用單位作業環境之整合性。

技 13、外購套裝軟體時，應確保軟體的品質。

為確保外購套裝軟體的品質，應事先確認該軟體之功能以及與機構內現有系統之整合性。

2、提升維護品質

技 14、確保定型化變更作業的正確性。

為確保新設營業單位或新增機器設備之定型化變更作業的正確性，應有變更作業合理化之對策。

技 15、應確保功能變更、新增作業時的品質。

在功能變更、新增作業時，為能確保程式的品質，應比照開發時提升品質之對策。

(三) 提升營運可靠性之對策

為提升資訊系統可靠性，除應提升硬體設備、軟體系統等之可靠性之外，人工操作也是提升作業可靠性之重要因素。

為提升營運之可靠性，除系統操作之自動化、簡易化等對策之外，如何充實妥適性、正當性的檢核功能，亦是非常重要的。

1、提升營運可靠性之對策

技 16、力求系統操作之自動化及簡易化。

為提升營運作業的可靠性，系統操作應力求自動化及簡易化。

技 17、系統操作之檢核功能。

為防止系統操作之失誤，應充實系統操作之檢核功能。

技 18、加強對系統負荷狀態之監控。

為使資訊系統穩定運轉，應監視系統負荷狀況，以免超過各類資源之能力或容量限制，必要時應有控制機制。

技 19、加強ATM之異常偵測能力。

為使自動化服務區之ATM穩定運轉，應集中監視其營運狀況，並應加強異常偵測之能力。

(四) 故障之早期發現、早期復原

在系統發生故障時，能即時偵測故障狀況，將其影響降至最低，並迅速採取系統復原的措施。

1、故障之早期發現

技 20、設置系統運轉狀況的監視功能。

為能及早發現及復原，應設置能監視資訊系統使用狀況（運轉狀態、停止狀態、錯誤狀態等）的機制。

技 21、設置故障偵測及將故障部位隔離的機制。

為迅速復原發生故障的系統，應設置能確實偵測資訊系統發生的各種故障，必要時並能夠將故障部位予以隔離。

2、故障之早期復原

技 22、應設置發生故障時，能縮小範圍並重組系統的功能。

發生故障時，除一部分的處理中斷外，為使系統繼續運轉，不致整體停頓，應具有縮小機能並重組系統的功能。

技 23、具有限制交易的功能。

為使檔案故障或軟體錯誤所造成的影響降至最低，應視情況，備有以檔案別或以科目別之交易限制功能。

技 24、具有系統復原的功能。

在發生故障時，為迅速回復系統，繼續執行業務處理，應建置系統復原的功能。

(五) 災變對策

為預防因資訊中心發生災變，致使資訊系統完全無法運作，同時為分散風險，應設置異地備援中心。

1、備援中心

技 25、具備災變備援中心。

為預防資訊中心本身因災變等的發生，造成系統功能完全喪失，應備有災變備援中心。

二、安全性侵害之對策

(一) 資料保護

機密資料或重要資料之外洩、破壞、篡改等，以及存取這些資料所需的密碼外洩時，均會對企業造成重大影響，因此，應重視對這些資料的保護對策。

1、防止洩漏

資料依其重要性，在儲存、傳送的作業上，應有適當的防止洩漏的對策。

技 26、具備密碼隱密性之維護措施。

為防止密碼洩漏，應採取不以明碼顯示；若以紙本印錄應採取必要之保護措施。。

技 27、應具有識別、確認對方端末設備的功能。

經由開放網路，為防止錯誤的情況發生，對可自動接收訊息的端末設備輸出/入資料時，應依設備功能設置確認對方端末設備身分之機制。

技 28、具有防止儲存資料外洩的功能。

為防止檔案遭複製或竊取等資料外洩，應對重要資料採用亂碼化處理。保存個資之載具或系統，應定期維護與更新。

技 29、具有防止資料在傳輸中外洩的功能。

為防止資料在傳輸中被竊聽而外洩，對於重要的資料，應有資料亂碼化的措施。

2、防止破壞、篡改

為防止因程式非法存取，造成資料被破壞、篡改，應有適當的防範對策。

技 30、檔案存取應具有獨占模式管控（Exclusive Control）的功能。

為防止檔案內容產生矛盾，檔案存取應具有獨占模式管控（Exclusive Control）的功能。

技 31、檔案應設置存取控制（Access Control）的功能。

為保護資料不被非法存取，對於使用者、程式與檔案等，應設有檢核存取權限的功能。

技 32、加強對不當資料之檢查功能。

為防止不當資料混入系統，應加強對不當資料之檢查及剔除的功能。

3、檢測對策

為早期發現資料之非法破壞或篡改，應有適當的檢測對策。

技 33、具備偵測資料傳輸中被篡改的檢測對策。

在傳輸重要的資料時，為偵測檢知是否被篡改，應有適當的方法與對策。

技 34、具備檔案相互勾核的功能。

為早期發現因故意或疏失而造成檔案間資料內容不一致，對於帳務主檔、交易日誌資料檔案、彙總清算檔案等，應有適當的檔案間相互勾核的機制。

（二） 防止非法使用

由於網路範圍的擴大，由各種端末設備存取系統的可能性增加，由無使用權限的使用者造成的非法存取、資料及軟體程式遭篡改等可能性大增。因此，應有確認系統使用權限、限制系統利用範圍等功能對策。

對於防止非法存取系統的對策，各金融機構應配合所使用的主機系統、端末設備、用途等，將非法存取系統的方式加以分類，擬定應檢核的項目。

1、預防對策

為防止對資訊系統的非法使用，如何確認本人身分、端末設備、媒體正當性、存取權限等，是非常重要的。若對存取權限的檢核確認作業實施不完整時，會增加系統遭非法存取的危險性。因此應充分講究系統存取權限及使用範圍的確認作業。

另外，為防止利用卡片的犯罪行為，提供安全的卡片交易服務，應有防止利用偽造卡片的措施。同時，對於電子式有價資料或密碼等資料之保護或偽造、篡改之防範與偵測，亦需有確實的對策。

1－1、預防對策（1）存取權限確認

技 35、具備確認使用者身分的功能。

為防止非法使用，配合業務內容及連接方法等，應確認連接對象的使用者身分以及是否為正當的端末設備，以及是否符合被允許的使用權限。。

技 36、具備防止非法使用 ID 的功能。

為防止非法存取系統及資料，應具備防止非法使用ID的功能。

技 37、管理系統的歷史資料。

為管理系統的狀況，對於使用系統或存取資料的歷史記錄應保管一段期間，以作為監查追蹤的依據。

1－2、預防對策（2）應用範圍之限制

技 38、設置限制端末設備、作業與交易範圍的功能。

為防止非法使用系統，對於端末交易，應依照使用的設備、媒體的種類、設置場所及用途等，設置限制交易內容的功能機制。

技 39、設置在發生事故時能停止交易的功能。

為因應發生遺失金融卡、存摺、印鑑等事故的處置，應有對該帳戶之對應媒體設定停止交易的功能。同時，行外之可攜式端末設備遭竊、遺失等事故發生時，亦應有對該端末設備停止交易的功能。

1－3、預防對策（3）防止非法、偽造對策

技 40、具有防止卡片被偽造的對策。

為防止非法使用，應具有防止卡片被偽造的對策。

技 41、對於電子儲值應有檢測非法行為的保護功能機制。

為因應電子儲值的複製、重複使用等非法行為，系統應建置保護資料，檢測非法行為的功能機制。

技 42、以電子式儲存基碼值之機器、媒體或軟體，應具有保護基碼值功能。

為防止基碼值外洩而引起非法行為，機器設備、媒體與使用之軟體系統應設置保護機碼值的功能。

技 42-1、對於電子郵件的收發、首頁的瀏覽等，應具有防止非法使用的功能。

對於電子郵件的收發、首頁的瀏覽等，應具有防止非法使用的對策。

2、限制外部網路存取

資訊系統連接到開放式網路等外部網路時，為防止經由網路之非法入侵及非法使用資訊系統，應限制外部的存取動作。

技 43、具有防止外部網路非法入侵的功能。

為防止非法入侵，處理重要資料及執行程式的系統在與外部網路（開放式網路、遠端存取等）連接的部分，應具有的防止非法入侵的適當對策。

技 44、由外部網路可以存取的機器設備應維持在最少的數量。

為防止非法入侵資訊系統，由外部網路可以存取的通訊路徑與通訊相關機器等應維持在最少的數量，不必要的機器設備不可連上網路。

3、偵測對策

為早期發現非法存取，應設置可以監視非法存取及異常交易的功能。同時，為防止非法交易的發生，應有能偵測非法交易的功能。

技 45、設置監視非法存取的功能。

為早期發現非法存取，應設置監視存取失敗或非法存取的功能。

技 46、設置偵測非法交易的功能。

為防止因非法交易造成的損害，應設置偵測非法交易的功能。

技 47、設置異常交易的監視功能。

為早期發現非法存取，應設置監視異常交易的功能。

4、因應對策

偵測到非法存取或非法使用時，應迅速調查可能受到損害的範圍，防止受損範圍的擴大，必要時需執行系統的復原作業。因此應事先備有因應策略。另外，應有受損狀況、原因等的調查分析與防止再次發生的措施。

技 48、應備有因應非法存取與復原的對策。

當偵測發現非法存取時，為防止非法存取擴大的因應對策與系統復原作業程序應明確訂定。偵測到非法存取時，不論是否有蒙受損害，應有防止非法存取行為擴大的因應對策與復原對策，同時，在分析非法存取的原因後，應有防止再發生的對策。

（三） 防止非法之程式

在講究資訊系統安全性之入侵對策時，防止非法程式侵入系統或安裝的對策也是非常重要的。

1、防禦對策

資訊系統遭到非法程式的侵入時，可能會造成機密資訊（密碼、重要檔案內容等）之外洩、或系統遭到破壞（如檔案之破壞、系統功能之破壞等）、甚至故意侵害系統的安全性等，因應這些事故，應有綜合性的考量，訂定整體性的因應策略。

技 49、具有對電腦病毒等非法程式的防禦對策。

為防止系統開發、維護、營運中遭受電腦病毒等非法程式的入侵、或非法存取而遭受損害，應有適當的防禦對策。

2、偵測對策

應能夠偵測電腦病毒或非法軟體的入侵，使用者或系統管理者能立即採取適當必要的措施。

技 50、應設置偵測電腦病毒等非法軟體的功能。

為確保並維持系統的可靠性，應設置能偵測檢查是否有被電腦病毒等非法軟體入侵或感染之對策。

3、復原對策

應準備電腦病毒受損系統之復原作業程序，同時應有防止再發生的因應對策。

技 51、具有被電腦病毒等非法程式感染受害時之因應對策。

被電腦病毒等不當程式感染時，為將受害的範圍縮至最小，應有由發現病毒感染到系統復原的因應對策。

**銀行公會金融業務電子化委員會資訊安全組
標準暨審查分組組員名單**

台灣土地銀行	畢海珊	處長
台灣銀行	許文隆	中專
華南商業銀行	許銘勳	副科長
台灣土地銀行	許珍蘭	科長
第一商業銀行	林志鑫	經理
彰化商業銀行	蔡江河	組長
合作金庫銀行	林文彬	科長
兆豐國際商業銀行	蘇家涵	高級專員
中國信託商業銀行	郭桂棻	經理
玉山商業銀行	陳思良	技術副理
台新銀行	林美惠	協理
台北富邦銀行	林世哲	協理
永豐商業銀行	彭勝寶	資深副理
國泰世華銀行	張俊銘	專案經理
金融聯合徵信中心	沈柏村	組長
陽信商業銀行	田凱元	副理
財金資訊公司	黃偉倫	組長

金融機構資訊系統安全基準 使用說明

中華民國銀行商業同業公會全國聯合會

中華民國一〇五年九月修訂版

金融機構資訊系統安全基準 使用說明

版權所有請勿翻印

2003 年 10 月日文原版
2005 年 03 月中文修訂一版
2011 年 08 月中文修訂二版
2016 年 09 月中文修訂三版

日本財團法人 金融資訊系統中心 原著
中華民國銀行商業同業公會全國聯合會 編修

安全基準索引

設備基準

[一、 資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 建築物								
設 1		1. 環境	避免設置於容易發生各類災害、事故之區域		○				5
設 2		2. 周圍	檢討因所在地之環境變化，可能發生之災害與事故，並訂定對策		○				8
設 3			建地應確保必要的通道		◎				9
設 4			最好與鄰近建物保持充分之間隔		○				10
設 5			建立圍牆或隔柵以及加裝錄影監視設備防止侵入之設施		○				11
設 6			不可將招牌等懸掛在外面		○				13
設 7			建築物應安裝避雷設備及設備獨立接地系統		○				14
設 8			建築物應為資訊系統相關業務專用，或在建築物內區隔資訊系統相關業務專用之獨立區域		○				15
設 9			建地內通訊與電力線路要有防止切斷、延燒措施及雙迴路管線		○				16
設 10		3. 結構	應依據消防署規定之防火建築物		◎				18
設 11			具安全性之結構		◎				19
設 12			外牆、屋頂部份應有充分之防水性能		◎				20
設 13			外牆部份應具足夠之強度		○				22
設 14		4. 門窗	門窗應有防火措施		◎				23
設 15			應有防犯措施		◎				24
設 16			平常使用之進出口僅限一處，並設置進出管制裝置、防犯設備等		○				25
設 17			應設置緊急安全門		◎				28
設 18			應施以防水措施		○				29
設 19			進出門窗應具有充分之強度，並需隨時加鎖		◎				30
設 20		5. 內部裝潢	應使用具不燃性或耐燃性之材料		◎				31
設 21			對於因地震等裝潢之震落或損壞應有預防措施		○				32

設備基準

[一、資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(二) 電腦機房、媒體儲存室								
設 22		1. 位置	應設置於不易受到災害的位置			◎			34
設 23			應設置於不易由外部進入之位置			◎			35
設 24			不可懸掛室名等標示牌			◎			37
設 25			確保必要之維修空間		◎				38
設 26			應為獨立之專用房間		◎				39
設 27		2. 門窗	平時使用之進出口，應僅限設置一處，並須設置等候室		○				40
設 28			出入口之門窗，應具有足夠之強度，並須加鎖		◎				41
設 29			窗口應設置防火、防水、防止破壞等措施，並須設置由外部無法窺視機器設備之裝置		◎				42
設 30			緊急安全門、避難器具、指示燈、停電照明等設置		◎				43
設 31		3. 結構、內部裝潢	應為獨立之防火區域		◎				45
設 32			應設置防止漏水之對策		◎				46
設 33			應設置消除靜電之設備		◎				47
設 34			內部裝潢應使用不燃性材質或具防火性能之材料		◎				48
設 35			對於地震等內部裝潢之震落、損壞，應有預防措施		◎				49
設 36			高架地板應具有在地震時不會損壞之構造		◎				50
設 37		4. 設備	應設置自動火災檢知警報裝置		◎				53
設 38			應設置火災等緊急事故警示及緊急連絡裝置		◎				55
設 39			應設置滅火設備		◎				56
設 40			纜線之耐火及防止延燒之措施		◎				60
設 41			應設置排煙設備		◎				62
設 42			應設置緊急照明設備與攜帶式照明設備		◎				63
設 43			不可裝設一般用水的設備		◎				64
設 44			應安裝地震感應器		○				65
設 45			於機房進出口設置進出管制與防犯設備		○				66
設 46			應設置溫濕度自動記錄裝置或溫濕度警報裝置		◎				67

設備基準

[一、 資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 47		5. 資訊系統設備、其他各項設備及備用物品	應設有預防蟲鼠害之措施		○				68
設 48			各類雜項設備及備用品，應具有防火性能		◎				69
設 49			應設置防止靜電之措施		◎				70
設 50			各類雜項設備及備用品應具有耐震措施		◎				71
設 51			搬運車等應安裝固定裝置		◎				75
	(三) 電源室、空調室								
設 52			應設置於不易受到災害之位置		◎				78
設 53			應確保維修保養時必要的空間		◎				79
設 54			應為專用之獨立房間		○				80
設 55			門窗應加鎖，最好不要設置窗戶		◎				81
設 56			應採用耐火結構		◎				82
設 57			應安裝自動火災警報設備		◎				83
設 58			應安裝氣體滅火設備		○				84
設 59			空調設備應設有防止漏水的措施		◎				85
設 60			電纜線、各類導管導線等，應設有防止延燒的措施		◎				86
	(四) 電源設備								
設 61			電源設備之容量，應保持充裕有餘		◎				88
設 62			應以多重迴路引入電源		○				90
設 63			應設置能提供良質電力之供電設備		◎				93
設 64			應設置自備發電機設備及蓄電池設備		◎				95
設 65			電源設備應設置避雷裝置		◎				96
設 66			電源設備應具有耐震措施		◎				97
設 67			由配電盤至送至資訊系統設備之電源配線應為專屬專用電纜線		◎				98
設 68			應避免與負載變動激烈的機器設備共用電纜線		◎				99
設 69			資訊系統設備之接地線，應為專用之地線		◎				100
設 70			應設有預防措施，以避免因過大電流、漏電等事故，造成設備故障		◎				101

設備基準

[一、 資訊中心]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 71			應設置防災、防犯用備用電源		◎				102
(五) 空調設備									
設 72			空調設備，應保持充分寬裕之容量		◎				104
設 73			空調設備，應具有穩定調節空氣之功能		◎				105
設 74			電腦機房之空調設備，應為獨立使用及維修		◎				107
設 75			應設置備援之空調設備		○				108
設 76			空調設備應安裝自動控制裝置、異常警報裝置等		◎				109
設 77			空調設備應具有預防入侵、破壞等措施		◎				110
設 78			空調設備應具有耐震之措施		◎				111
設 79			空調設備隔熱材料、排吸氣口應採用耐火材料		◎				112
(六) 監視控制設備									
設 80			應安裝監視控制設備		◎				114
設 81			宜設置中央監控室		○				115
(七) 數據線路相關設備									
設 82			數據線路相關設備，應上鎖		◎				117
設 83			數據線路相關設備之安裝場所，不可附加標示		◎				118
設 83-1			數據線路相關設備，應備有專用之配線空間		◎				119

設備基準

[二、總行、營業單位]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 建築物								
設 84		1. 周圍	建地內之通訊線路、供電纜線等，應具有防止被切斷、延燒之措施			○			121
設 85		2. 結構	應為耐火之建築物			○			122
設 86			建築物應具有安全性之結構			◎			123
設 87			建築物外牆與屋頂應具充分的防水性能			◎			124
設 88			建築物外牆應確保其強度			○			125
設 89			3. 門窗	窗戶應具有防火措施			◎		
設 90		門窗應有防犯措施				◎			127
設 91		出入口的門，應有足夠之強度，同時應加裝門鎖				◎			128
設 92		非營業時間之出入口應設置進入者識別用裝置				◎			129
設 93		進出口應具有防水措施				○			131
設 94		4. 內部裝潢	天花板及牆壁應具有隔熱、吸音之功能			○			132
設 95			應具有預防措施，以防止因地震而造成內部裝潢震落或損壞			◎			133
設 96			地板面應採用不易積存灰塵或產生靜電的材質			○			134
設 97			端末設備之通訊線路及電源線路，應具有防止被切斷的措施			◎			135
設 98			端末設備之通訊線路、電源線等，應有防止被漏水浸滲的措施			○			136
設 99		5. 設備	應安裝自動火災警報及滅火器等設備			◎			137
設 100			各類設備宜有耐震措施			○			139
設 101			應安裝耐火金庫或耐火庫房			◎			140
設 102	應安裝避雷裝置				○			141	
設 103	應安裝防犯措施				◎			142	
設 104	6. 線路相關設備	不可標示通訊線路相關設備安裝場所			◎			143	
設 105		易為外界碰觸之通訊線路相關設備等最好上鎖			◎			144	
設 106		連結端末機器設備之線路，最好有備援線路			○			145	

設備基準

[二、總行、營業單位]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 107		7. 電源設備	應注意電源線之配置，以確保端末設備之正常作業			◎			146
設 108			防災、防犯設備應安裝備用電源			◎			148
設 109			宜安裝自用發電設備			○			149
設 110		8. 空調設備	應設置空調設備			◎			150
設 111		9. 自動化服務區	應安裝直接通話設備			◎			151
設 112			應安裝緊急通報裝置			◎			152
設 113			宜安裝防犯措施			◎			153
設 114			應設置照明設備及緊急照明設備			◎			156
設 115			自動化服務區的門，應有部分為透明透光者			◎			157
設 116			自動化服務機器之裝填現金及設備維護作業應確保必要的空間			○			158
設 117			安裝自動運作設備			○			159
設 118		10. 端末設備	端末設備應設有耐震措施			○			162
設 119			機器設備之地線，應確實安裝			◎			165
設 120			端末設備應有保護措施，不受漏水或塵埃的侵害			○			166
(二) 伺服器安裝場所									
設 121		1. 位置	伺服器設備應設置於較不易受到災害的位置			○			168
設 122			伺服器設備應設置於不易由外部進入的位置			○			169
設 123			設置伺服器設備的位置，不得張貼具室名等標示之招牌			○			170
設 124			設置伺服器設備的位置，應為專用之隔間			○			171
設 125		2. 結構・內部裝潢	應設置於具防火能力之隔間內			○			172
設 126			應具防止漏水的對策			○			173
設 127			高架地板應具有耐震之措施			○			174
設 128		3. 設備	應具有滅火設備			○			175
設 129			宜設置地震感應器			○			176

設備基準

[二、總行、營業單位]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
設 130			在設置伺服器的房間進出，應設置進出管理設備、防犯設備等			○			177
設 131			應設置溫濕度自動記錄裝置或溫濕度警報裝置等			○			178
設 132			應設置空調設備			○			179
設 133			應有防止鼠害的措施			○			180
設 134			應有防止電源插頭由插座鬆落的措施			◎			181
	(三) 行外收付處								
設 135			應有防止由其他區域入侵的措施			◎			183
設 136			配合使用商店設備之狀況，應有適當的補強對策			◎			184

設備基準

[三、 與流通業、零售店合作之合作通路]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 便利超商之 ATM								
設 137			應有防犯措施				◎		186

營運基準

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 確立管理體制								
運 1		1. 資訊安全管理與責任之明確化	應編製資訊安全管理辦法相關文件	◎					193
運 2			具體實施資訊安全管理標準之文件，應進行評估及修訂作業	◎					195
運 3			建立 資訊安全管理體制	◎					197
運 4			建立 系統管理體制	◎					198
運 5			建立資料管理之體制	◎					199
運 6			建立網路管理之體制	◎					200
運 7		2. 組織及分工制衡	設置防災小組		◎	◎			201
運 8			設置防犯小組		◎	◎			204
運 9			確立分工體制		◎	◎			207
運 10		3. 各種規章之訂定	訂定各種規章	◎					209
運 10-1	4. 安控規章遵守狀況之確認	確認對安控規定之遵守狀況	◎					212	
	(二) 進出管理								
運 11		1. 門禁管理	實施人員資格限制及門禁識別工具管理		◎	◎			214
運 12			實施中心門禁管理		◎				216
運 13			實施電腦機房及媒體儲存室之門禁管理		◎	◎			217
	(三) 營運管理								
運 14		1. 手冊之建立	訂定日常作業手冊	◎					219
運 15			訂定故障或災害發生時相關作業之操作手冊	◎					221
運 16		2. 存取權限之管理	明確訂定各種資源、系統等之存取權限	◎					223
運 17			採取防止密碼、 作業憑證等 外洩之措施	◎					224
運 18			明確訂定存取權限之授予及評估等作業程序	◎					225
運 19		3. 操作管理	值勤操作人員之確認		◎				228
運 20			明確規定操作之申請及核可 程序		◎				229
運 21			明確規定操作之執行規範		◎				230
運 22			確認執行結果，並留存操作紀錄		◎				232

營運基準

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
運 23			辦理主從架構系統 (Client Server System) 之作業管理		○	○			233
運 24		4. 資料輸入管理	辦理資料輸入之管理		◎	◎			235
運 25		5. 資料檔案管理	規定資料授受及保管方法	◎					238
運 26			訂定資料檔案之修改管理方法	◎					240
運 27			確保資料檔案之備份作業	◎					241
運 28		6. 程式檔案管理	明確規定程式檔案之管理方法	◎					243
運 29			確保程式檔案之備份作業	◎					244
運 30		7. 電腦病毒之對策	應明確規定因應電腦病毒之對策	◎					246
運 31		8. 網路設定資訊之管理	應落實網路設定資訊之管理	◎					248
運 32			應落實網路設定資訊之備份作業	◎					249
運 33		9. 文件管理	明確訂定文件管理辦法	◎					251
運 34			確保文件之備份作業	◎					252
運 35		10. 傳票帳冊管理	明確訂定未使用之重要空白傳票帳冊管理辦法	◎					254
運 36			明確訂定已印製之重要傳票帳冊處理辦法	◎					255
運 37		11. 資料輸出管理	重要資料之編製、輸出處理等，應具有防止非法使用及保護機密之措施	◎					257
運 38		12. 交易管理	明確訂定各類交易之操作權限		◎	◎			261
運 39			操作人員作業卡之管理		◎	◎			262
運 40			記錄並驗證交易之操作內容		◎	◎			263
運 41			問題帳戶之管理	◎					264
運 42			事先明確告知客戶，使用電子儲值媒體應有之責任及潛在風險損失	◎					265
運 43		13. 金鑰之管理	應明確訂定金鑰使用及管理之辦法	◎					267
運 44		14. 實施嚴謹的身份確認	網路銀行之身分確認			◎			269
運 45		15. 無人化服務區之管理	訂定營運管理辦法			◎	◎		271
運 46			訂定監視機制			◎			273
運 47			明訂防犯措施			◎			274
運 48			訂定故障及災害發生時之因應措施			◎			275
運 49			備妥相關手冊			◎			276

營運基準

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
運 50		16. 可攜式電腦設備管理	明確訂定可攜式電腦設備管理辦法			◎			278
運 51		17. 各類卡片管理	明確訂定卡片管理辦法		◎	◎	◎		280
運 52			明確訂定對特定帳戶卡片交易之監視辦法		◎	◎	◎		282
運 53		18. 客戶資料保護	具有保護客戶資訊的措施	◎					284
運 54		19. 資源管理	掌握各種資源之能力及使用狀況	◎					286
運 55		20. 外部連接管理	明確訂定連接契約之內容	◎					289
運 56			應明確訂定與外部連接之營運管理辦法	◎					291
運 57		21. 機器設備之管理	應明確訂定管理辦法		◎	◎			294
運 58			保護通訊網路相關設備之措施		○	○	○		296
運 59			明確訂定設備維護辦法		◎	◎			297
運 60		22. 營運監視	建置完善之監視體制	◎					300
運 61		23. 電腦機房、資料儲存室之管理	嚴密管理進入後之作業		◎	◎			303
運 62		24. 故障災變之因應對策	明確訂定相關人員之聯絡程序	◎					305
運 63			明確訂定故障災變時之復原作業程序	◎					307
運 64			調查、分析發生故障之原因	◎					308
運 65		25. 制定災變備援計畫	制定災變備援計畫	◎					310
(四) 系統開發、變更									
運 66		1. 硬體、軟體之管理	應實施硬體、軟體之管理	◎					314
運 67		2. 系統開發・變更之管理	明確訂定開發、變更之作業程序	◎					317
運 68			建立測試環境	◎					319
運 69			明確規定轉入正式作業之轉換程序	◎					321
運 70		3. 文件管理	格式之標準化	◎					324
運 71			明確規定管理辦法	◎					325
運 72		4. 套裝軟體之引入	套裝軟體之評估制度	◎					327
運 73			明確訂定使用、管理之方法	◎					329

營運基準

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
運 74		5. 系統之廢棄	擬定報廢計畫、作業程序	◎					331
運 75			應具有防止資料外洩之措施	◎					332
(五) 各項設備管理									
運 76		1. 維修管理	明確規定管理辦法		◎	◎			335
運 77			明定維護管理辦法		◎	◎			337
運 78		2. 資源管理	確認設備之容量、性能及使用狀態		◎	◎			339
運 79		3. 監視	建立監控機制		◎	◎			341
(六) 教育訓練									
運 80		1. 教育訓練	實施資訊安全教育	◎					344
運 81			實施提升技巧與熟練度訓練	◎					346
運 82			實施系統操作訓練	◎					347
運 83			實施事故應變操作訓練	◎					348
運 84			實施防災、防犯演練	◎					350
(七) 人員管理									
運 85		1. 人員管理	實施適當人事管理	◎					352
運 86			實施人員健康管理	◎					353
(八) 委外管理									
運 87		1. 委外計劃	系統開發、營運等委外處理，應事先明確訂定作業目標及範圍	◎					355
運 87-1			以明確之程序選擇委外廠商	◎					356
運 88			委託契約內容應包含安全政策相關事項	◎					357
運 89		2. 業務委外管理	規定委外廠商之從業人員應遵守事項並加以管理及檢核	◎					359
運 90			委外業務組織之建立、業務之管理及檢核之執行	◎					360
(九) 系統稽核									
運 91			系統稽核之體制	◎					363
(十) 行外收付處									
運 92			收付處設置地點之選擇基準，應事先明確訂定			◎			365

營運基準

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(十一) 便利超商 ATM								
運 93			設置地點之選擇基準，應事先明確訂定				◎		367
運 94			對於裝填現金等維護作業，應有防犯對策				◎		368
運 95			應明確訂定故障、災害發生時之因應對策				◎		369
運 96			對於網路相關設備，應制定資料傳輸之安全政策				◎		370
運 97			應確立與設備所在地之警察機關、保全公司等相關機構之聯絡體制				◎		371
	(十二) 轉帳卡 (Debit Card)								
運 99		1. 確保轉帳卡服務之安全性	應有轉帳卡服務之安全政策				◎		373
運 100			應確保帳號、密碼之安全性				◎		374
運 101		2. 客戶之保護	客戶使用轉帳卡應有客戶保護措施			◎			376
	(十三) 利用開放網路之金融服務								
運 103		1. 網路銀行、行動銀行	防範不當使用				◎		378
運 104			早期發現非法使用				◎		380
運 105			應公開安全政策相關資訊				○		381
運 106			應明確訂定營運管理辦法				◎		382
運 107		2. 電子郵件	應明確訂定電子郵件之應用方針				◎		385

技術基準

[一、提升系統可靠性]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
(一) 提升硬體設備之可靠性									
技 1		1. 預防硬體設備故障之對策	應實施預防保養		◎	◎			391
技 2		2. 備用硬體設備	設置主機裝置之備用設備		◎	◎			392
技 3			設置週邊設備之備援設備		◎	◎			396
技 4			設置通訊設備之備援設備		◎	◎			398
技 5			設置備用之通訊線路		○	○			400
技 6			端末系統設備之備用設備		◎	◎			403
(二) 提昇軟體系統之可靠性									
技 7		1. 提升開發品質	應確認系統開發設計與中長期計劃的整合性	◎					405
技 8			納入必要的安全控管機能	◎					406
技 9			在設計階段確保軟體之品質	◎					407
技 10			在程式撰寫階段，確保軟體的品質	◎					409
技 11			在程式測試階段，確保軟體的品質	◎					411
技 12			程式派送至使用單位時，應確保軟體的可靠性	◎					415
技 13			外購套裝軟體時，應確保軟體的品質	◎					416
技 14		2. 提升維護品質	確保定型化變更作業的正確性	◎					417
技 15			應確保功能變更、新增作業時的品質	◎					418
(三) 提升營運可靠性之對策									
技 16		1. 提升營運可靠性之對策	力求系統操作之自動化及簡易化	○					421
技 17			系統操作之檢核功能	◎					424
技 18			加強對系統負荷狀態之監控	◎					426
技 19			<u>加強 ATM 之異常偵測能力</u>		◎	◎	◎		428

技術基準

[一、 提升系統可靠性]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
(四) 故障之早期發現、早期復原									
技 20		1. 故障之早期發現	設置系統運轉狀況的監視功能	◎					430
技 21		2. 故障之早期復原	設置故障偵測及將故障部位隔離的機制	◎					432
技 22			應設置發生故障時，能縮小範圍並重組系統的功能	◎					433
技 23			具有限制交易的功能	◎					434
技 24			具有系統復原的功能	◎					435
(五) 災變對策									
技 25			具備災變備援中心		○				438

技術基準

[二、安全性侵害之對策]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
	(一) 資料保護								
技 26		1. 防止洩漏	具備密碼隱密性之維護措施	◎					441
技 27			應具有識別、確認對方端末設備的功能	○					442
技 28			具有防止儲存資料外洩的功能	○					443
技 29			具有防止資料在傳輸中外洩的功能	○					444
技 30		2. 防止破壞、篡改	檔案存取應具有排他控制（Exclusive Control）的功能	◎					446
技 31			檔案應設置存取控制（Access Control）的功能	◎					448
技 32			加強對不當資料之檢查功能	◎					449
技 33		3. 檢測對策	具備偵測資料傳輸中被篡改的檢測對策	○					452
技 34			具備檔案相互勾核的功能	◎					453
	(二) 防止非法使用								
技 35		1-1. 預防對策（1） 存取權限確認	具備確認使用者身分的功能	◎					455
技 36			具備防止非法使用 ID 的功能	◎					457
技 37			管理系統的歷史資料	◎					458
技 38		1-2. 預防對策（2） 應用範圍之限制	設置限制端末機器、作業與交易範圍的功能	◎					460
技 39			設置在發生事故時能停止交易的功能	◎					462
技 40		1-3. 預防對策（3） 防止非法、偽造對策	具有防止卡片被偽造的對策		○	○	○		463
技 41			對於電子儲值應有檢測非法行為的保護功能機制	○					464
技 42			以電子式儲存基碼值之機器、媒體或軟體，應具有保護基碼值功能	◎					465
技 42-1			對於電子郵件的收發、首頁的瀏覽等，應具有防止非法使用的功能	○					466
技 43		2. 限制外部網路存取	具有防止外部網路非法入侵的功能	◎					469
技 44			由外部網路可以存取的機器設備應維持在最少的數量	◎					471
技 45		3. 偵測對策	設置監視非法存取的功能	◎					473
技 46			設置監視非法交易的功能	○					474
技 47			設置異常交易的監視功能	◎					475

[二、安全性侵害之對策]

項目編號	大項目	中項目	小項目	適用性分類					頁次
				全面適用	資訊中心	總行、營業單位	流通業、零售業等合作通路	直接連接通路	
技 48		4. 因應對策	應備有因應非法存取與復原的對策	◎					477
	(三) 防止非法之程式								
技 49		1. 防禦對策	具有對電腦病毒等非法程式的防禦對策	◎					480
技 50		2. 偵測對策	應設置偵測電腦病毒等非法軟體的功能	◎					484
技 51		3. 復原對策	具有被電腦病毒等非法程式感染受害時之因應對策	◎					487

設 備 基 準

設備基準概要

- 1、設備基準是針對「資訊中心」、「總行、營業單位」及「合作通路」等之建築物、設備、相關週邊設備，為防範各種災害、入侵破壞等不法行為、機器設備故障等事件，所訂定的具體預防及緊急應變措施。
- 2、「資訊中心」是針對建築物內之電腦機房、媒體儲存室、電源室、空調室、監視控制設備及線路相關設備等，於資訊系統營運上必要之空間及設備等所訂定之措施。
- 3、「總行、營業單位」是針對營業場所、資訊設備設置場所、設置 ATM 等設備之自動化服務區、電源設備、空調設備、線路相關設備等，於資訊系統營運上必要之空間及設備等所訂定之措施。
- 4、自動化設備等提供無人化服務之特定措施，包含在自動化服務區的項目中。對於安裝於企業內或行外之 ATM 等，可依使用狀況，由營業單位自動化服務區的項目中抽出適宜之項目，訂定適合之措施。
- 5、考慮對行外收付處或超市等外派據點等特殊環境，並為防範破壞入侵等，應另訂定與現有總行、營業單位不同之設備補強措施。
- 6、「合作通路」是針對無法如總行、營業單位等具有設置 ATM 之自動化設備機房、機械室等設備之便利超商等所訂定加強防犯之措施。
- 7、本設備基準係針對「資訊中心」、「總行、營業單位」及「合作通路」等實施對象，依其所在環境、建築物、各類空間、設備等整理訂定。因此，若實際運用上有困難時，可變更實施對象之措施。

一、資訊中心

（一）建築物

資訊中心之建築物，對於各類災害及事故等應具有充份之預防措施，萬一發生災變或事故時，亦應有緊急應變措施，將災害減至最低之範圍，並儘速恢復正常運作。

資訊中心之建築物，應依其所在環境、建築物及其周圍等場所，分別預設可能發生的災害、事故等異常情況，應訂定適當之因應措施。

建築物
環境

適用性分類			
中心	總行	合作	直接
○			

設	1	避免設置於容易發生各類災害、事故之區域。
---	---	----------------------

為了降低災害事故對資訊中心之影響，最好避免設置於容易發生各類災害或引起事故之地區。

- 1、各類災害或事故是指火災、颱風、土石流、落雷、滿潮、水災、地震、電場、磁場等事故、空氣污染、鹽鹼侵蝕災害、振動等。
- 2、建置資訊中心時，應避免設置於容易發生各類災害或引起事故的地區。若資訊中心已建置於容易發生各類災害或引起事故的地區，或不得已應建置於容易發生各類災害或引起事故的地區時，應訂定對應各類災害或事故之適當應變措施。

3、火災

容易發生火災的地區，是指如下地區：

- (1) 木造建築物密集的地區。
- (2) 處理大量易燃物的設施或地區。
- (3) 儲存爆炸性危險物品的地區。

4、颱風

颱風是一種劇烈的熱帶氣旋，也就是在熱帶海洋上發生的低氣壓。在四周氣壓較高處的空氣向氣壓較低處流動時形成「風」，而風速超過每秒 17.2 公尺就稱為颱風。颱風通常挾帶狂風暴雨，造成停電、洪水及土石流等災情，造成人員及建築物之損傷。

臺灣全島各地皆為颱風可能侵襲之地點，資訊中心的設置應能預防颱風所引起之各種災害。

5、土石流

大量水分之碎屑物搬運流動，如有一半以上的固體材料顆粒大小超過沙粒大小或含大量粗礫的岩石碎屑，則稱為岩屑流，在台灣稱為土石流。通常山崩

落石造成大大小小的石塊、泥土，如果雨水降臨，與之混合後，順著地表斜坡下滑移動或流動，滾滾土石流常造成嚴重威脅，只要土石流經過的地方，無一倖免，是目前威脅台灣山區的天然災害。

6、雷擊

在金融機構資訊中心引起系統事故之天然災害，雷擊是發生次數最多的災害。在檢討設置場所時，應參考公告之年度雷雨日數等資料及建築物本身（避雷針接地系統、設備接地系統）確實測量安裝。

7、滿潮

滿潮是由於颱風或強烈低氣壓造成海面異常上升，隨著強風，海水擁向陸地的現象，在V字型或U字形海灣，容易發生這種現象。

8、水災

容易發生水災的地區，是指下列地區：

- (1) 急速都市化的丘陵地、臺地或較低窪地區
- (2) 地層下陷地區、海拔零公尺地區、填土開墾地。
- (3) 河川匯流點附近、彎曲凹岸地區、鄰近堤岸而有水池的地區。

9、地震

可能因地震受到災害的地區，是指下列地區：

- (1) 過去發生過大地震，而最近不曾發生大地震的地區
- (2) 在過去曾因地震，發生過斷層或地層運動的地區
- (3) 有活潑的地殼活動的地區

另外，在地震災區可能會擴大災情的因素是地層液狀化之現象。所謂地層液狀化現象，是由於地殼震動，引起地層水壓上升，而噴出砂或水的情形，尤其在對水份含有量接近飽和狀態之砂層，會引起砂粒子浮游在水中的現象，形成地盤液化，容易使建築物下沉的狀態（表 1）。

10、電場、磁場之事故

有可能發生電場、磁場事故的地區，是指電塔、電波塔或微波等輸送線之附近，會發出強烈的電場與磁場，而對電腦系統會產生影響的地區。

11、空氣污染

由於空氣污染，有可能造成災害的地區，是指下列地區空氣中含有多量污

染物（如工廠產生的有毒氣體或含硫磺氣體）的地區。

火山地帶、含塵量高的礦場、砂石土儲存場等附近地區。

表 1 液狀化之可能性與地形

液狀化的可能性	依地形的判斷	依液狀化歷史的判斷
(A) 可能性高	<ul style="list-style-type: none">• 填土區域、水面填土地區• 舊、現有河道• 緩慢形成的天然堤防• 砂丘與低窪地之境界• 砂丘間的低窪地區	有液狀化歷史地點
(B) 依情況有可能性	除上述以外的低窪地區	無液狀化歷史地點
(C) 可能性低	<ul style="list-style-type: none">• 臺地• 丘陵• 山地	

12、鹽鹼侵蝕災害

鹽鹼侵蝕的地區，是指近海岸的地區。

鹽鹼侵蝕災害是指傳輸電線或通訊線路的絕緣體，由於風雨帶來的鹽份及塵埃附著其上，而變成帶有導電性質的情況，容易造成線路短路之事故。

13、振動

因振動可能造成災害的地區，是指接近鐵路軌道沿線、交通幹道沿線等地區。

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設	2	檢討因所在地之環境變化，可能發生之災害與事故，並訂定對策。
---	---	-------------------------------

為降低資訊中心因災害所受影響，應檢討資訊中心隨自然環境、地區環境之變化而可能發生之災害與事故，並訂定防範對策。

- 1、資訊中心所在地之產業、都市、住宅、交通等周圍環境繼續不斷的變化，因而發生災害與事故的起因、場所、影響範圍等也不斷地隨著變化、多樣化。因此，應注意資訊中心所在地周圍之自然環境、地理環境等各種變化，及其所帶來的災害或事故發生的可能性，並訂定因應對策，於災變未發生之前，防止災害於未然。
- 2、因環境變化而可能發生的災害，雖依地理環境之不同而異，但大致可列舉如下：
 - (1) 由於都市化的進展，使雨水的排放率、排放速度發生變化，可能引起淹水、河川氾濫之害。
 - (2) 因挖土、填土所發生的地表滑動、崩落、砂土流失等砂土災害。
 - (3) 地下水系統的變化，引起基礎地盤結構的變化。
 - (4) 鄰近地區有存放危險物品的設施、危險結構之建築物。
 - (5) 因鄰近地區之輸電鐵塔、電波塔等之設立，引起電場、磁場之干擾事故。
 - (6) 因建設會排放有毒氣體的工廠或火山活動活絡等所引起之空氣污染。
 - (7) 建設鐵路、地下鐵、高速公路等所引起的振動災害事故。

建築物
周圍

適用性分類			
中心	總行	合作	直接
◎			

設	3	建地應確保必要的通道。
---	---	-------------

建地應依建築法規之規定，確保必要的通道，以便發生火災時，容易進行滅火作業及避難工作。

- 1、為滅火作業及避難，應依建築法規之規定，確保必要的通道。
- 2、通道最好能向兩方向避難，同時應設置標誌、照明等設備，以利在夜間安全避難。緊急出口及避難通道，需經常整理維持暢通，不得放置會阻礙滅火作業或避難行動的物品。

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設 4	最好與鄰近建物保持充分之間隔。
-----	-----------------

為防止延燒或滅火工作順利進行，最好能與鄰近建物保持充分之間隔。

建物有延燒可能的部份，應依本國建築法規，與鄰近建築物之間預留充分之間隔距離。

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設	5	建立圍牆或隔柵以及加裝錄影監視設備防止侵入之設施。
---	---	---------------------------

如在建地邊境實施進出管理時，儘可能建立圍牆或隔柵，必要時安裝防止侵入之設施，以防止不法入侵對建物之破壞行為。

1、在建地邊界實施進出管理，乃為輔助在建地內建築物中實施進出管理之措施。

2、圍牆或隔柵

在建立圍牆或隔柵時，應留意是否與周圍環境調和，高度應在兩公尺以上，以防止外部之閒雜人越牆而入，並應採用堅固結構之物體，以防止遭到破壞。惟周圍狀況無閒人擅進之虞時，不在此限。

3、防止入侵之設施

防止入侵之措施，可分為配置警衛人員與安裝防止入侵之設備兩種方式。防止侵入之設備，有下列方式：

(1) 紅外線感應裝置

在一邊設置紅外線投光器，另一邊設置受光器，當侵入者遮斷紅外線光束時，會引起反應作用。惟因其警戒範圍僅為一條線，故能以發射兩條光束的方式，會更加有效。這種裝置最大的感應距離可達數百公尺，惟在設置時，需注意只能安裝於沒有樹木、造形物體等遮蔽物體而視野寬闊的場所（參照圖1）。

(2) 格柵警報器（Trap Sensor）

安裝在圍牆、鐵絲網格柵上，以檢測警告攀越、切斷或衝破等情況之發生（參照圖2）。

4、照明設備

設置照明設備時，應留意下列事項：

(1) 對於建築物周圍之建地、由地面至二樓之牆面、及緊急逃生梯等有可能入侵之場所，在夜間應設置能確保充分明亮度之照明設備（參照圖3）。

(2) 照明設備本身亦需加以保護，以免遭投石等之破壞。

5、錄影監視設備CCTV

(1) 在各重要出入口架設錄影監視設備以防止外人侵入破壞。

(2) 錄影監視設備需具備「移位偵測、事件感應警報記錄儲存、夜視、NAS Network Attached Storage儲存機能」等各項功能。

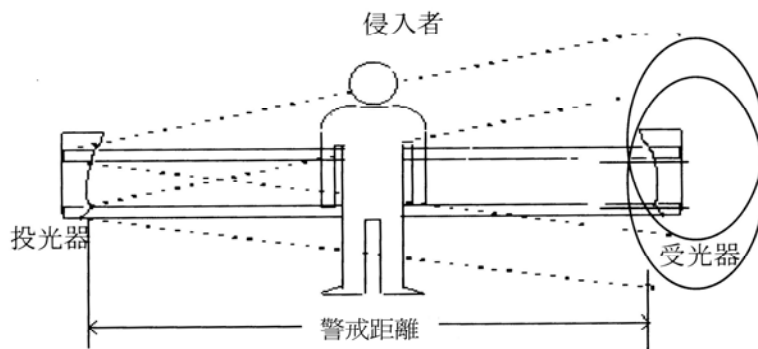


圖 1 紅外線感應設備

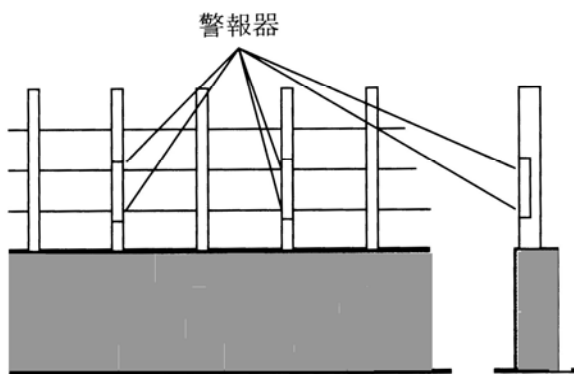


圖 2 格柵警報器

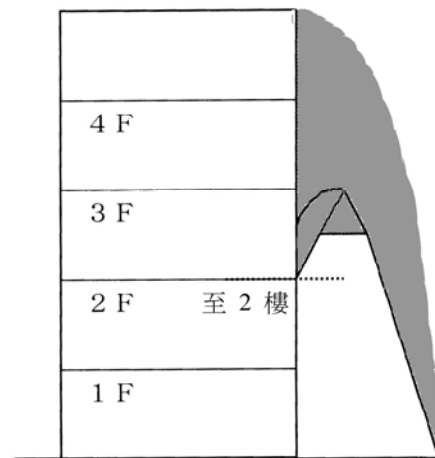


圖 3 照明設備

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設	6	不可將招牌等懸掛在外面。
---	---	--------------

為能事先預防由外部之侵入、破壞等行為，顯示資訊中心等所在地之標示板、招牌等不宜懸掛在外面。

- 1、此處所指，係如○○資訊中心、※※銀行資料處理中心等，顯示資訊中心等之所在地之標示板、招牌等。
- 2、在與其他機構共用的大樓中，也不要設置電腦系統或與其相關設備的場所，懸掛容易察知之標示板、招牌等標誌（參照【設 24】）。

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設	7	建築物應安裝避雷設備及設備獨立接地系統。
---	---	----------------------

在周圍沒有較高之建築物，或在雷擊較多之地區，應於建築物上安裝避雷設備，以防止因雷擊造成故障或事故。

- 1、避雷設備之安裝，是將雷擊產生之大電流安全地放流至大地（接地），不僅可以避免資訊系統造成故障，同時可以防止內部人員因觸電之傷亡、建築物之損壞、火災等。
- 2、設備需安裝獨立接地系統
設備接地不得與避雷針接地並接以防止電流回衝導致設備損壞。
- 3、避雷設備及設備接地系統，應為國家所指定符合台灣工業規格之製品。

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設	8	建築物應為資訊系統相關業務專用，或在建築物內區隔資訊系統相關業務專用之獨立區域。
---	---	--

為了徹底實施安全管制，建築物應闢為資訊系統相關業務專用，或是在建築物內區隔資訊系統相關業務專用之獨立區域。

- 1、將建築物闢為資訊系統相關業務專用，或是在建築物內區隔資訊系統相關業務專用之獨立區域，其目的如下：
 - (1) 由於資訊中心之值勤狀態異於總行或營業單位，可藉此要求營運時之徹底實施安全管制。
 - (2) 可以徹底實施進出樓（室）之管理。
 - (3) 對於各種設備之保護與安全，可以徹底實施運用管理。
 - (4) 客觀環境有變化時，較易採取快速而適當之應變對策。
- 2、資訊中心與其他機構共用同一大樓時，為徹底實施安全管制，在設備、營運作業各方面，應注意之事項，應與專用一棟建築物的狀況相同。

建築物
周圍

適用性分類			
中心	總行	合作	直接
○			

設 9	建地內通訊與電力線路要有防止切斷、延燒措施及雙迴路管線。
-----	------------------------------

建地內數據通信線路與電力輸送纜線要有預防措施，以避免因施工或外部侵入，而發生切斷、延燒等之事故。

- 1、資訊中心建地內數據通信線路與電力輸送線等，常因自來水管、瓦斯管等之施工或外部侵入，而發生切斷、延燒等事故。為確保資訊系統之安全，應有預防措施。
- 2、一般來說，至資訊中心建築物內之數據通信線路、電力輸送纜線，多以地下電纜管線引入，資訊中心建地內部的各種管道，多為金融機構的設施，前述纜線則由電信公司或電力公司負責施工。因此在施工時，應依各種設計圖事先協調，採取預防切斷、延燒之措施。另電力管線引進施工時可要求電力公司採雙迴路供電以確保不會斷電。
- 3、建地內之數據通信線路、電力輸送纜線之施工方法，舉例如下：
 - (1) 室內之數據通信線路、電力輸送纜線，宜採地下管線方式。
 - (2) 地下電纜管線，應使用耐燃電纜線，或以不燃性材料覆蓋電纜線。
 - (3) 地下纜線如使用套管或暗渠方式引進時，應使用堅固耐重壓，且不易浸水之套管或暗渠。
 - (4) 地下纜線如採用直接埋設方式引進時，在可能會受壓之地段，應埋設於離地面深度 1.2 公尺以上的地方，其他地段亦應埋設在深度 60 公分以上的地方。
 - (5) 使用套管等物引入的高壓或特別電壓的電源纜線，應每隔 2 公尺左右設置標籤，註明物件名稱、管理者姓名、電壓、埋設日期等資料。
 - (6) 地下電力輸送線纜與地下之數據通信線路之間應有充分之間隔距離，以避免因電流之漏電或誘導感應作用，引起通信干擾現象。
 - (7) 地下電力輸送纜線與地下之數據通信線路相互接近或交錯之地段，若纜

線之間的距離，低壓或一般高壓纜線在 30 公分以下，特別高壓在 60 公分以下時，其纜線間應設置堅固耐火之隔牆，或將纜線收入堅固不燃性、難燃性的套管中，並避免直接接觸纜線。

- (8) 選擇路徑時，應考慮將來的擴建、裝修、鋪路時，不受其影響。

建築物
結構

適用性分類			
中心	總行	合作	直接
◎			

設 10	應依據消防署規定之防火建築物。
------	-----------------

資訊中心之建築物，應為建築相關法規規定之防火建築物。

1、建築物採用防火建築之結構，不僅可以獲得防火功能，同時更可以具有防止犯罪、進出管制與高效率空調的效果。因此，今後要建置之資訊中心建築物，應依建築相關法規之規定，其結構應為耐火建築物。

2、耐火建築物

- (1) 所謂耐火建築物，是指牆壁、樑柱、屋頂等主要結構部份為防火結構之建築物，在外牆開口部份，若有延燒的可能性時，應配合法令之規定，採用防火門的結構，且需配置其他防火設備。
- (2) 所謂防火結構，係指鋼筋混凝土、磚造等結構，並具有法令規定之防火性能與時效之結構。

建築物
結構

適用性分類			
中心	總行	合作	直接
◎			

設 11	具安全性之結構。
------	----------

為防止造成資訊系統之事故，應具有建築基準法規訂定之結構安全性。

- 1、對於建築物本身重量、承載負荷、風壓以及地震等震動與衝擊，建築物在其結構上應具安全性，因而使資訊系統不致發生災害與事故。
- 2、現行之建築基準法規，依其施行或適用上，對現存之建築物，若有無法符合現行建築基準法規所規定之部份存在時，則該部份可不適用其規定。若資訊中心建築物係依照舊建築基準法規設計時，應儘可能對於耐震安全性，咨請公設機構予以診斷或判斷，在結構安全性上有問題時，應加強耐震之補強，以確保能符合現行法規所定之結構安全性基準。
- 3、建築基準法規規定之承載負荷為 300 kg/m^2 以上，但依電腦系統廠商所建議之設備安裝基準，載負荷應為 500 kg/m^2 以上。

建築物
結構

適用性分類			
中心	總行	合作	直接
◎			

設 12	外牆、屋頂部份應有充分之防水性能。
------	-------------------

外牆、屋頂部份應有防止漏水之措施，以避免長年使用後，因防水、排水性能降低而發生漏水現象，造成資訊系統之故障或事故。

- 1、外牆、屋頂部份因長年使用後，防水、排水性能降低，或遭遇超越排水能力之豪雨，或因排水口被垃圾阻塞而發生漏水現象時，可能造成資訊系統之故障或事故。為避免前述情況發生，應有防止漏水之措施。
- 2、實施防止漏水之措施，應留意下列事項：

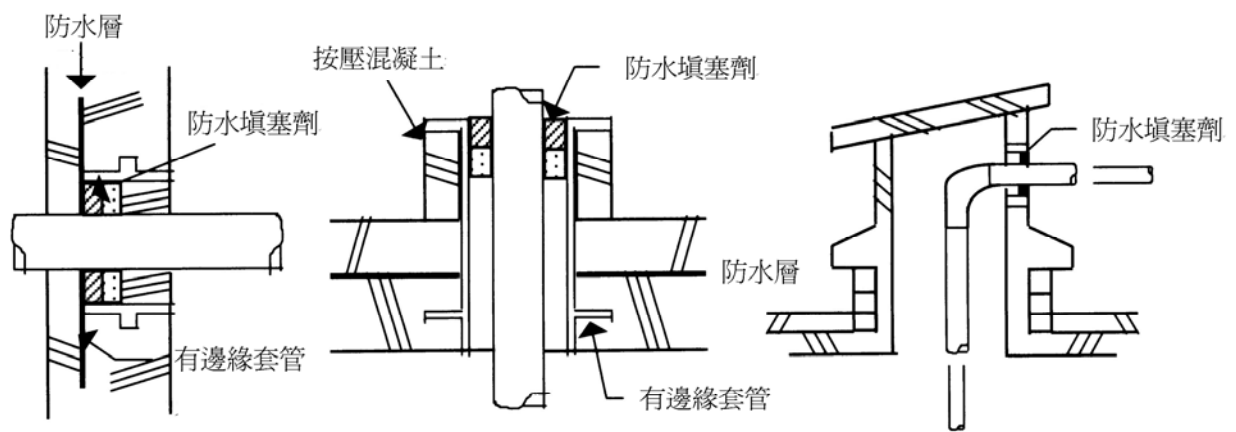
(1) 屋頂、外牆

屋頂、屋頂平臺、護牆、混凝土接縫部份的損傷，或防水層的退化、破損，以及混凝土龜裂等之進行。

(2) 應注意屋頂平臺上之扶手、吊環、高架水塔、冷卻水塔、廣告塔等設備，有無造成防水層之損傷。

(3) 貫通屋頂、外牆之部份

應注意貫通屋頂、外牆防水層的吸排氣口、風管、配管、配線等之防水性保護施工事項（參照圖 1）。另外，熱水、蒸氣等配管易受熱度之影響，風管亦易受風力的影響，以致防水層的剝離、斷裂等。



例 1 防水牆的情形

例 2 防水地板的情形

例 3 貫通屋頂時

圖 1 貫通防水層之配管例圖

建築物
結構

適用性分類			
中心	總行	合作	直接
○			

設 13	外牆部份應具足夠之強度。
------	--------------

為防禦資訊系統與相關設備破壞，面臨街道之外牆部份，應具有足夠之強度。

可以防禦破壞行為之外牆，有鋼筋混凝土造之外牆、具有相當強度之窗簾式牆壁(Curtain Wall)等。窗簾式牆壁是一種對於建築物無載重功能之薄牆，其材料有金屬板、鋼筋混凝土板等多種，一般都在工廠依規格生產之牆板。另玻璃板得在厚玻璃板中，夾入格子形狀金屬網之防火、防犯用網狀玻璃。

建築物
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 14	門窗應有防火措施。
------	-----------

為防止延燒，有延燒可能性之門窗，應有防火措施。

- 1、有延燒可能性之門窗，是指窗與鄰接境界線、道路中心線或同一建地內之兩棟以上建築物相互外牆間之中心線間的距離，在一層樓相距 3 公尺以下，在二層樓相距 5 公尺以下之情況。
- 2、對防火建築物或次防火建築物，有延燒之虞的外牆開口部份，應設置防火門窗或裝置防火設備。若門窗在一層樓之 3 公尺以內或在二層樓以上之 5 公尺以內有鄰接境界線、道路中心線等之情況時，應設置能隔離之防火或次防火之防火結構外牆、防火牆或其他類似之防火設備。
- 3、防火門窗有甲種與乙種防火門窗兩種，耐火性較高之甲種防火門窗，其規格如下：
 - (1) 骨架為鋼鐵製造，兩面鋪上厚度為 0.5 公厘以上之鋼板。
 - (2) 鐵製，鐵板厚度 1.5 公厘以上。
 - (3) 鋼筋混凝土製，厚度 3.5 公厘以上。
 - (4) 經由政府認可而與上述規格具有同等防火性能之產品。
- 4、與甲種防火門窗具有同等防火性能之設備，有水幕式防火設備。
水幕式防火設備是設置於外牆或門窗，為防止由鄰近建築物之延燒，可以噴出水幕，遮斷火災及其幅射熱等之設備。

建築物
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 15	應有防犯措施。
------	---------

為防止對資訊中心建築物之不法入侵，對於容易由外部接近或入侵的一樓等門窗，應有防犯措施。

1、門窗之防犯措施有下列數種：

- (1) 強化玻璃或夾網玻璃。
- (2) 可以開關之鐵製方格窗或鐵捲門。
- (3) 門窗的開閉，可以感應磁場動作之電磁開關（參照圖 1）。
- (4) 能感應在破壞玻璃時所產生的特定高周波之振動感應器（參照圖 1）。

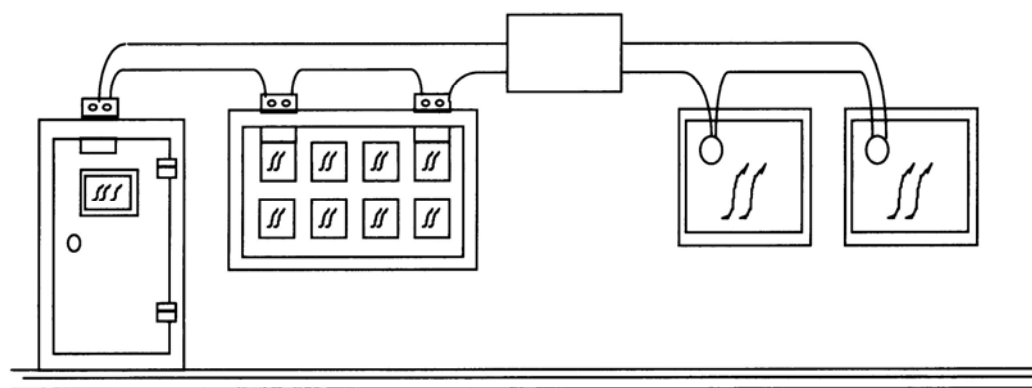


圖 1 電磁開關 (左)、嵌死窗戶用振動感應器 (右) 之例圖

2、若在建築物周圍，設有廣告招牌、建築物、人行陸橋或兩層樓以上的階梯，處於容易入侵之環境時，各個門窗亦應設置防犯措施。

建築物
門窗

適用性分類			
中心	總行	合作	直接
○			

設 16	平常使用之進出口僅限一處，並設置進出管制裝置、防犯設備等。
------	-------------------------------

為確實辦理進出中心之管理、防止不法的入侵及不明物品的搬進搬出，平時使用之進出口，應僅限一處，並設置進出管制裝置、防犯設備等。

1、平時使用之進出口所設置之進出管制裝置，可以採取下列之方式：

(1) 收發櫃臺

由警備人員識別進出之人員身分，除事先允許進入之人員外，應辦理手續之後再行進入。

(2) 開閉裝置

利用開閉裝置，識別事先予以設定之進出資格，經識別、記錄之後，控制進出門之開關。

- a. 磁卡進出管理裝置 …………… 將磁卡插入讀卡機查驗（參照圖 1）。
- b. 卡片感應裝置 …………… 將卡片接近感知器查驗。
- c. I C 卡、光卡進出管理裝置 … 將 I C 卡、光卡插入讀卡機查驗。
- d. 暗碼輸入裝置 …………… 輸入暗碼查驗。
- e. 掌形、掌紋識別裝置 …………… 利用光學原理，讀取掌形、掌紋查驗。
- f. 指紋比對裝置 …………… 利用光學原理，讀取指紋查驗。
- g. 視網膜形狀辨識裝置 …………… 利用光學原理，讀取視網膜形狀查驗。
- h. 簽字即時識別裝置 …………… 感知簽字時之筆壓、時間、筆跡等查驗。
- i. 聲紋認知裝置 …………… 讀取聲紋比對查驗。

2、平時使用之進出口所設置之防犯設備，可以採取下列之方式：

- (1) 對講機 …………… 在不開門的情況下，直接與內部人員對話，確認身分。
- (2) 防犯錄影機 ……… 利用錄影機設備，攝影記錄進出口、前面房間之狀態。
- (3) 防犯攝影機 ……… 利用攝影機設備，攝影記錄進出口、前面房間之狀態。

(4) 防犯警報裝置 … 在特定場所裝置、感應是否有人接近或通過，在異常時會啟動警報。

3、平時使用之進出口有兩個以上時，每一個進出口均需嚴格實施進出管制，否則應指定其中之一個進出口為平時使用之進出口，另一進出口則加上鑰匙關閉。

若大樓係共同使用之大樓，致無法將進出口限定為一處時，則應在設置資訊中心之樓層與資訊中心進出口處，辦理同樣之進出管制措施。

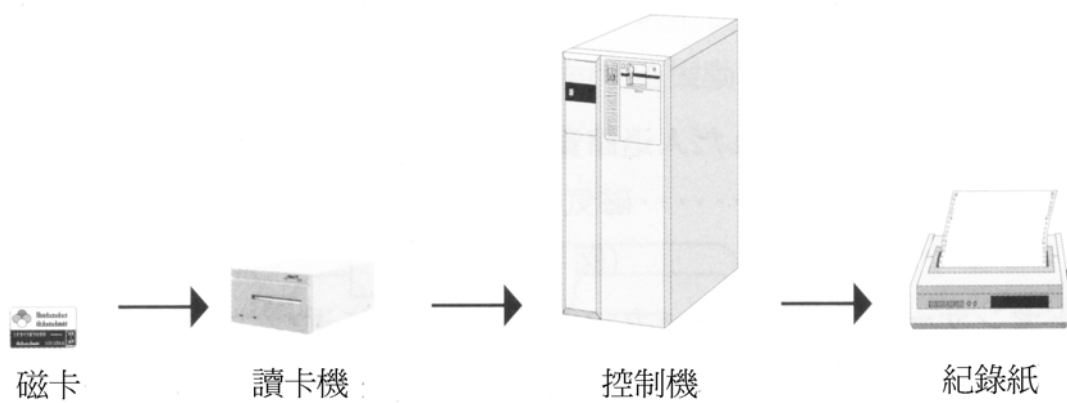
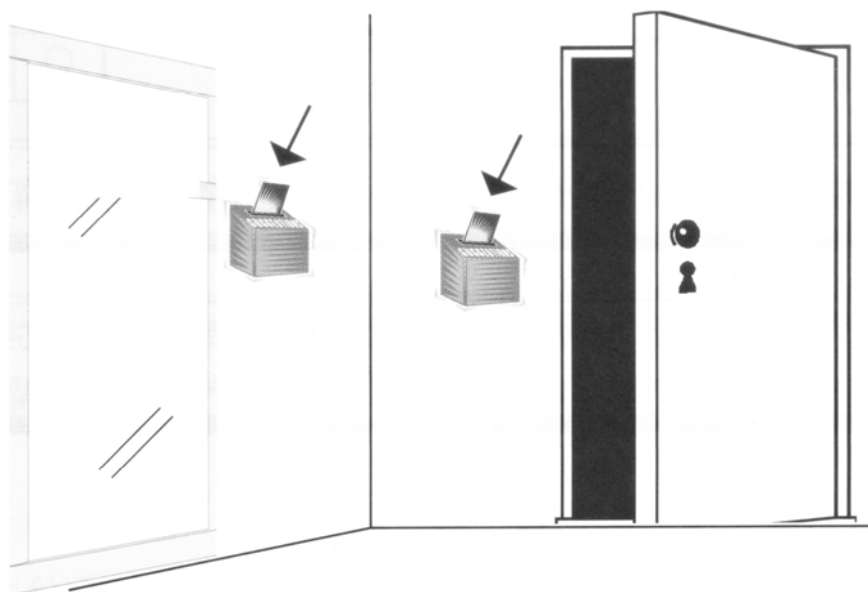


圖 1 磁卡進出管理裝置圖例

建築物
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 17	應設置緊急安全門。
------	-----------

在適當之位置設置緊急安全門，當遭遇災難時能順利避難，並在必要時能疏散各種物件。

- 1、緊急安全門是指當火災發生時，能由資訊中心順利避難之緊急出口。緊急安全門及通到緊急安全門通路，均應設置於能由建築物之任何位置雙向避難之位置。
- 2、緊急安全門，應在不使用鑰匙之情況下，由室內直接開啟。
- 3、緊急安全門如加裝門禁磁卡設備，在緊急狀況發生時可由室內直接開啟。

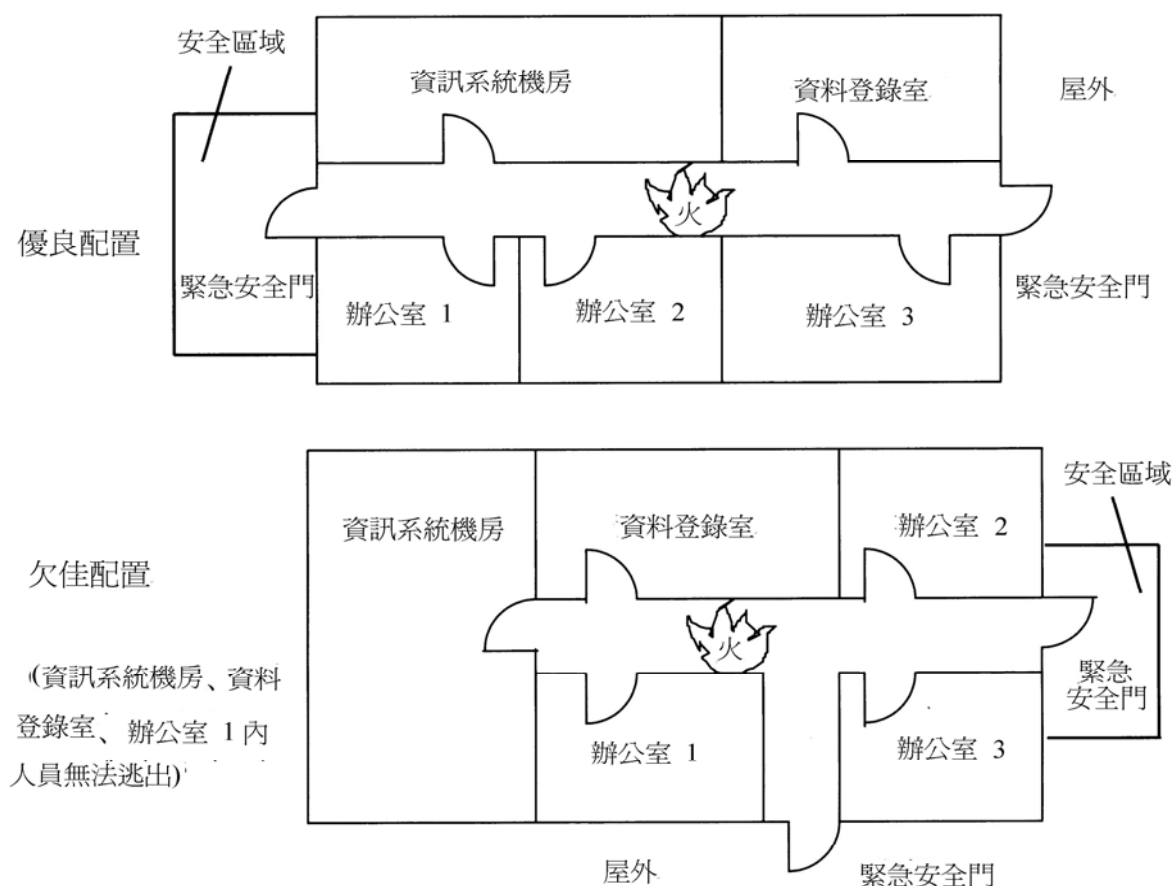


圖 1 緊急安全門及至緊急安全門之避難通路之實例

建築物
門窗

適用性分類			
中心	總行	合作	直接
○			

設 18	應施以防水措施。
------	----------

為防止因浸水或漏水造成資訊系統設備之故障，在進出口、門窗、機器設備搬運進出口等之開口部，應施以防水措施。

1、在進出口等開口部份實施之防水措施，可以採取下列之方式：

- (1) 對進出口門、鐵捲門、旋轉門等，加強防水。
- (2) 設置排水溝、防水堤、擋水板、防水門等。
- (3) 準備防水用砂袋。

2、在建築時，將建築物之進出口設於高出地面的地方，對於進出道路，則設置階梯或斜坡，是防止水患的措施之一。

建築物
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 19	進出門窗應具有充分之強度，並需隨時加鎖。
------	----------------------

為防犯、防災，進出口之門窗應具充分之強度，並需隨時加鎖。

- 1、進出口之門窗，應使用具有足夠強度之甲種防火門窗或鐵捲門（甲種防火規格），以防止非法入侵、投入危險物品或延燒等。
- 2、進出口門窗應加鎖，在緊急情況或作業結束下班後能夠上鎖。
- 3、進出口門窗之鑰匙，應採在緊急時不須使用鑰匙即可由內部直接開啟之結構。另外使用自動門時，應採用停電時亦能由內部直接開啟的結構。

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 20	應使用具不燃性或耐燃性之材料。
------	-----------------

內部裝潢等依建築法規應使用不燃性材料，並依消防法規之規定，使用具備防火性能之材料，以保護內部工作人員及資訊系統之安全。

- 1、不燃性材料，是指在一般的火災中被加熱時，不會引火燃燒或發生對救火有害之變形、熔解、龜裂或其他損傷，同時不會產生煙霧或有毒氣體。依建築法規，不燃性材料是指混凝土、磚、瓦、石棉板、鋼鐵、鋁板、玻璃、灰泥（mortar）、石灰牆或其他類似的建材。政府認可之不燃性建材如下：石膏板與石牆（Rock-Wall）之組合等。至於石棉建材，在拆除建築物時，需預防石棉粉末飛散措施等規定，應事先與建商討論。
- 2、依消防法規之規定，具有防火性能之窗簾、地毯等，均有如圖 1 之標示，雖有防火處理，並不是非燃性，只是在點燃後不會引發大火。因此，在電腦機房，最好使用金屬百葉窗等不燃性之窗簾。

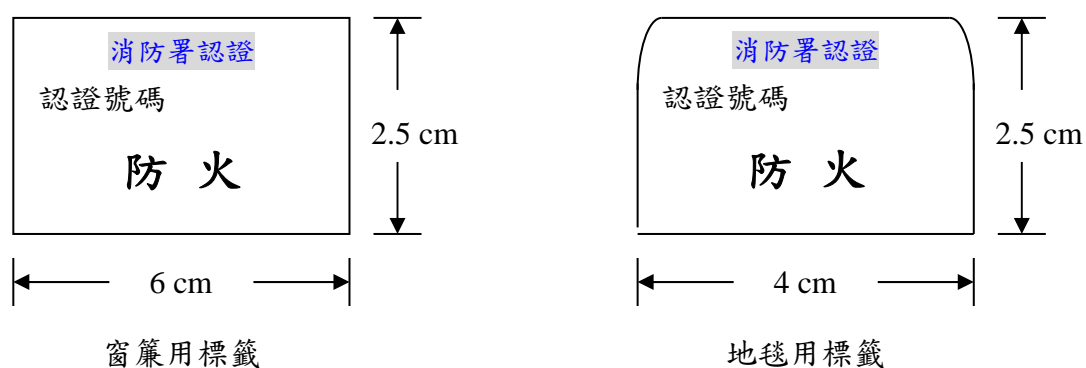


圖 1 防火標籤

- 3、夾板、纖維板、壁紙等裝潢材料，請使用具有我國工業規格等防火性能標示之材料。

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
○			

設 21	對於因地震等裝潢之震落或損壞應有預防措施。
------	-----------------------

為確保內部工作人員及資訊系統不受到損傷，對於因地震等可能造成裝潢之震落或損壞，應有預防措施。

- 1、以鋼骨建造之建築物，為維護其建築結構之耐火性能，樑柱等部份應以不燃性材料覆蓋。在覆蓋不燃性材料時，應要有預防因地震震落或損壞之措施。
- 2、若因地震發生配管之損傷，而造成漏水時，應事先訂定局限漏水範圍之檔水牆、排水溝、漏水監測系統預防措施。
- 3、請參照【設 35】

一、資訊中心

(二)電腦機房、媒體儲存室

電腦機房或媒體儲存室，多安置連線作業所需之系統及網路中樞設備，或存放重要資料儲存媒體。為了能確保其安全性，對於防止由於發生自然災害及不當行為等造成之損害，設備面應全盤留意。

電腦機房、媒體儲存室
位置

適用性分類			
中心	總行	合作	直接
◎			

設 22	應設置於不易受到災害的位置。
------	----------------

為了避免資訊系統受到地震、火災或水患之影響，設備應設置於不易受到上述災害之位置。

1、電腦機房、媒體儲存室等，應設置在建築物內不易受到地震、火災、水患等災害之位置，以防止系統受到影響；如不得已而設置在可能受到災害之位置時，應對各種災害，實施必要之防範措施。

另外，電腦機房、媒體儲存室等，應設置於不易受到電磁場影響的位置；如不得已而設置在可能受到影響的位置時，應實施電磁場隔離之措施。

2、在建築物內，受到災害影響較少的位置，舉例如下：

(1) 地震

- a. 鋼骨結構之建築物或地震之震動較少的低樓層。
- b. 如需放置重型設備時，放置樓面需加裝 H 形鋼材橫跨樑柱以加強樓地板安全承載。
- c. 在直接的上方層樓，不得有巨大重量之設備。
- d. 在鄰近位置，避免設置使用火之餐廳或茶室等。

(2) 火災

- a. 避免在鄰室、上下樓層設有易爆或易燃之鍋爐間、燃料儲存室等。
- b. 避免在鄰室設置儲存大量易燃性之文書保管倉庫、物品倉庫等。

(3) 水患

- a. 二樓以上無水患之虞的位置。
- b. 在鄰室或直接上方樓層，無用水設備的位置。
- c. 無屋頂漏水之虞之非頂樓的位置。

(4) 瓦斯滯留等

可燃性或腐蝕性氣體、蒸氣、粉塵、鹽分等較少侵入或滯留的位置。

電腦機房、媒體儲存室
位置

適用性分類			
中心	總行	合作	直接
◎			

設 23	應設置於不易由外部進入之位置。
------	-----------------

為了預防入侵、破壞、機密外洩，應避免設置於接近進出口、電梯或樓梯等能夠直接進入之位置。

- 1、設置電腦機房、媒體儲存室時，為了預防入侵、破壞、機密外洩等，應避免設置於接近進出口、電梯或樓梯等能夠直接進入之位置，而應設置於不易由外部直接進入之位置。
- 2、若不得已，電腦機房、媒體儲存室應設置於接近進出口、電梯或樓梯等能夠直接進入之位置時，應事先實施如下之預防措施：
 - (1) 為圖 1 所示，在進出口前設置等候室，避免直接入房。
 - (2) 在房間進出口設置進出管制設備。
 - (3) 以具足夠強度之牆壁等遮蔽房間。

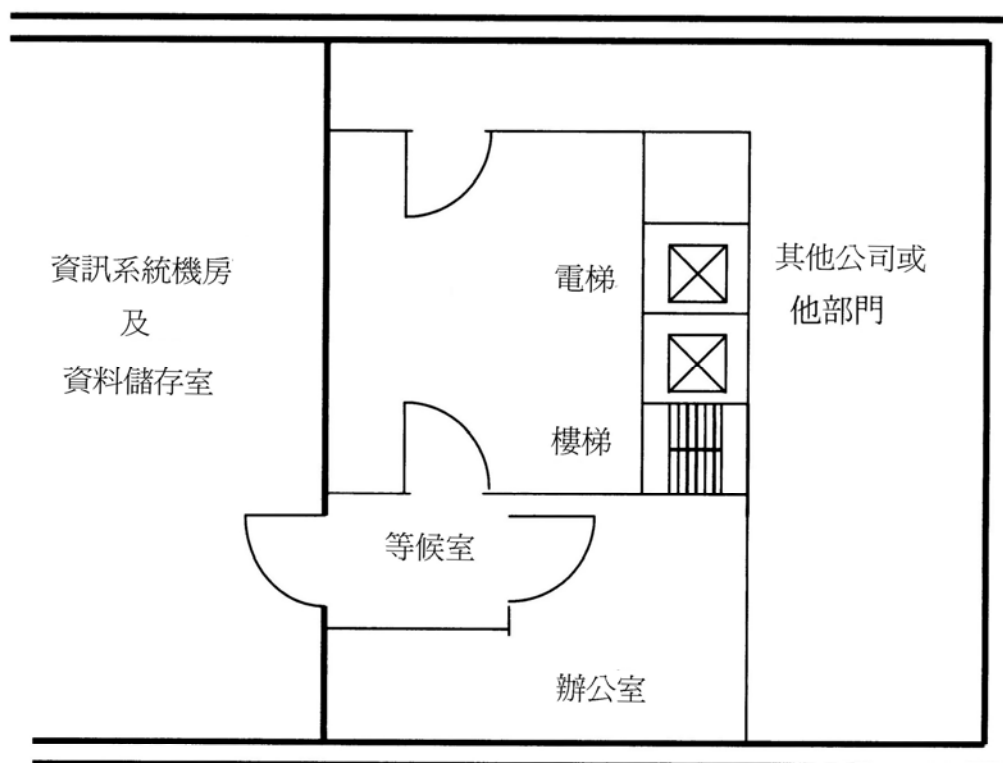


圖 1 資訊系統機房及資料儲存室之位置實例

電腦機房、媒體儲存室
位置

適用性分類			
中心	總行	合作	直接
◎			

設 24	不可懸掛室名等標示牌。
------	-------------

為了預防入侵、破壞、機密外洩，應避免懸掛電腦機房、媒體儲存室等室名之標示牌。

- 1、資訊中心之建築物內，為了預防入侵、破壞、機密外洩，應避免懸掛電腦機房、媒體儲存室等室名之標示或導引之招牌。
- 2、為能對消防人員明示電腦機房、媒體儲存室之位置，在建築物入口或管制中心等不易被外部人員看到的地方，保管電腦機房、電腦機房的平面配置圖。

電腦機房、媒體儲存室
位置

適用性分類			
中心	總行	合作	直接
◎			

設 25	確保必要之維修空間。
------	------------

為設備之維修、人員避難等，應確保必要之空間。

- 1、電腦機房內各項設備之配置，應預先保留設備操作、維修所需空間。同時為確保緊急情況發生時，能儘速到達緊急安全門等安全地點，應保留最短距離之避難空間。
- 2、維修所需之空間，大致以不移動機器設備，就能開關電腦設備及其週邊設備之機門為度。
- 3、為了資訊系統正常運轉，電腦機房會儲存報表等作業所需消耗品、雜項設備等物件，但平時應勤加整理整頓，不要將物品堆積在設備維修或人員避難所需之空間，也不要使通道變得狹窄。

電腦機房、媒體儲存室
位置

適用性分類			
中心	總行	合作	直接
◎			

設 26	應為獨立之專用房間。
------	------------

為徹底執行安全控管，機房應為獨立之專用房間。

1、電腦機房、媒體儲存室應採用獨立之專用房間其目的為：

- (1) 較易採取防火、防震對策。
- (2) 能實施進出管制，防止非法入侵或破壞行為。
- (3) 能防止機密資料之外洩。
- (4) 可以確實處理溫濕度之控管及調整。

2、若是把電腦機房的一個角落，供作媒體儲存室、辦公室、程式設計室或消耗品倉庫等共用時，在運用管理上，將會發生無法徹底實施進出管理等問題，同時容易發生機密資料外洩等不法行為或事故，應予以避免。

電腦機房、媒體儲存室
門窗

適用性分類			
中心	總行	合作	直接
○			

設 27	平時使用之進出口，應僅限設置一處，並須設置等候室。
------	---------------------------

為了確實實施進出機房之管制，平時使用之出入口，應僅限設置一處。同時，為確保安全性，防止外部的熱氣、濕氣、塵埃等侵入，在平時使用之出入口處，最好另設置等候室。

- 1、電腦機房、媒體儲存室等平時使用之出入口，應儘可能只限設置一處。若出入口有兩處以上時，應與只有一處出入口的情況相同，對每一個出入口，均須確實執行進出管制。同時，對於等候室內之入室者，應確實執行身分確認，並要注意防止熱氣、濕氣、塵埃等，由外部侵入。
- 2、電腦機房等候室之設置實例，如圖 1 所示
- 3、請參照【設 16】

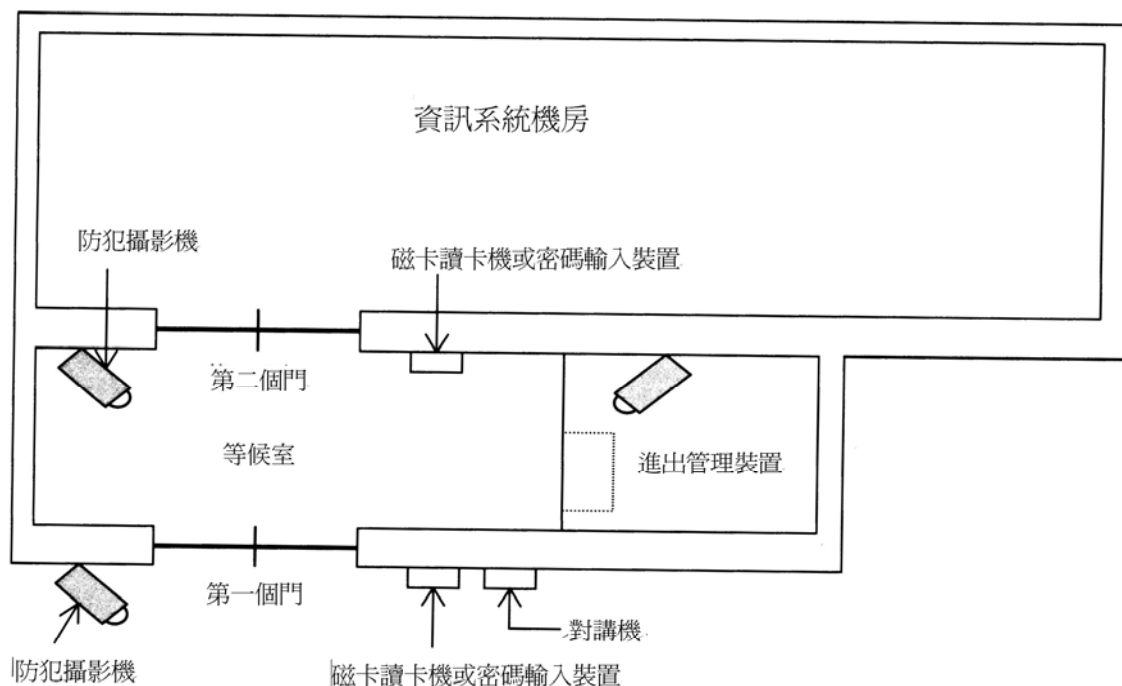


圖 1 資訊系統機房等候室之例圖

電腦機房、媒體儲存室
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 28	出入口之門窗，應具有足夠之強度，並須加鎖。
------	-----------------------

出入口門窗應具有足夠強度，並應予以加鎖，以利防犯、防災。

- 1、電腦機房、媒體儲存室之出入口門窗，最好使用甲種防火門以上具有足夠強度之門窗，並須加裝鑰匙，以防止非法入侵、投入危險物品與延燒等。
- 2、門鎖在緊急時，應不用鑰匙就可以從內部開啟。若出入門使用自動門時，即使在停電的情況下，亦須能即時開啟避難。
- 3、關於甲種防火門，請參照【設 14】。

電腦機房、資料儲存
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 29	窗口應設置防火、防水、防止破壞等措施，並須設置由外部無法窺視機器設備之裝置。
------	--

為防犯、防災，設置窗口時，應設置防火、防水、防止破壞等措施、防止窗口玻璃破損措施，更應設置由外部無法窺視機器設備之裝置。
--

- 1、如必須在電腦機房、媒體儲存室等開設窗口，其窗口應施以防火、防水、防犯措施，並須實施防止窗口玻璃破損等措施。同時，為防止由外部窺視室內之資訊系統設備、資料儲存保管設備等，應以窗簾、百葉窗等遮蔽。如果為了參觀、見習等目的，設置玻璃隔間時，應考慮安全管理上之必要措施。
- 2、防止玻璃窗口破損，可以採取下列措施：
 - (1) 窗戶玻璃使用夾網玻璃等材料。
 - (2) 在普通玻璃上加貼防止玻璃破碎飛散之透明膠片。
- 3、若電腦機房、媒體儲存室要設置在容易由外部接近的一樓等位置時，面臨外部之牆壁，應儘量採取無窗戶的結構。牆壁無窗戶的結構，能夠防止如下列的災害：
 - (1) 火災的延燒。
 - (2) 外部的入侵、破壞。
 - (3) 雨水等引起之漏水。
 - (4) 直射日光造成對機器設備之損傷。
- 4、依建築法規、消防法規之規定，若未設置有避難或滅火活動上有效開口部之樓層，則均視為無窗戶樓層，應設置滅火器、自動灑水裝置、自動火災警報設備、避難器具、排煙設備等都要設置齊全，不得在避難或滅火作業上，發生任何問題。

電腦機房、媒體儲存室
門窗

適用性分類			
中心	總行	合作	直接
◎			

設 30	緊急安全門、避難器具、指示燈、停電照明等設置。
------	-------------------------

電腦機房應在適當部位開設緊急安全門，並放置避難器具，以便在遇到災難時，能順利避難及疏散各種物件，並應設置引導至緊急安全門的指示燈或方向指標及停電照明等之設置。

1、緊急安全門

- (1) 安全門應設置在房內避難通路上，並設置二處以上。若電腦機房面積很大，應將機房劃分為數個區域，依個別區域訂定避難通路，並設置指示燈與方向指標，指示通到緊急安全門的通道(各緊急避難通路應加裝停電照明以利逃生)。
- (2) 為防止外人入侵，緊急安全門之構造，應為無法由外部開啟之結構。如應加裝門鎖，應該自室內無需使用鑰匙，即可直接開啟安全門。同時，在安全門附近容易看到的地方，標示開啟安全門的方法。

2、避難器具

- (1) 避難器具是指在發生火災，無法利用樓梯等避難設施逃生時，所利用的避難逃生器具。依消防法規規定，大樓需依樓層設置避難器具的種類如表 1。若在無窗戶之房間，設置避難器具無實質意義時，得不設置該項設備。

(表 1)

	地下樓層	三層樓	四層、五層	六層～十層
避難安全梯	○	○	○	○
避難用扶梯	○	○	—	—
滑梯	—	○	○	○
緩降機	—	○	○	○
避難橋	—	○	○	○
救助帶	—	○	○	○

(2) 安裝避難器具，須注意下列各點：

- 避難器具應安裝於避難時容易接近之場所，並固定設置於其窗口部位。
- 放置避難器具的窗口，每一樓層之位置不可以同一垂直線上。
- 避難器具安置場所，應設置記載避難器具使用方法之標示。

3、指示燈

- 指示燈如圖1所示，有指示避難出口之綠色「避難出口指示燈」及指示避難出口方向之白色「避難方向指示燈」兩種。避難方向指示燈，應懸掛於走道、室內及樓梯間。避難出口指示燈應懸掛於避難出口。
- 避難出口指示燈及避難方向指示燈之構造及性能，已於標示燈之基準規定內詳細訂定。



圖 1 避難出口指示燈



圖 2 避難方向指示燈

4、引導方向指標

引導方向指標是明確指示避難方向之不附燈光的標示牌，應裝置在眾人可以看到的位置。如裝置有指示燈時，在指示燈有效範圍內，可以不裝置引導方向指標。

電腦機房、媒體儲存室
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 31	應為獨立之防火區域。
------	------------

為防止火苗向建築物內其他地區延燒，電腦機房、媒體儲存室應依建築基準法之規定設置獨立的防火區域。

- 1、若因建築物之結構，媒體儲存室無法設置於獨立的防火區域時，在火災發生時，為能在一定時間內保護磁性媒體之資料，磁性媒體應存放在耐火之金庫或鐵櫃中。
- 2、分散存放在媒體儲存室之外的各類資料，尤其重要資料媒體，應存放在耐火之金庫或鐵櫃中保管。

電腦機房、媒體儲存室
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 32	應設置防止漏水之對策。
------	-------------

為防止建築物、設備等損傷，以及對資訊系統設備造成故障，屋頂、牆壁、地板等處，應施以防止漏水之措施。

- 1、若在電腦機房、媒體儲存室之隔鄰，設有用水的空間或設備時，應採取下列因應措施：
 - (1) 將機房之地板升高，使其高出其他地區。
 - (2) 在預設可能漏水地點或配置水管附近，應設置漏水偵測設備或接水容器，以防漏水。
 - (3) 設置防水堤，防止漏水流入。
 - (4) 設置抽水裝置、排水溝、排水桶等。
 - (5) 抽水裝置須加裝緊急供電系統以防止停電時無法使用。
 - (6) 在配水管直接貫穿機房之前，於可能安裝之位置上安裝止水閥。
 - (7) 配水管上應使用能吸收地震等振動之伸縮接管。
- 2、若在電腦機房、媒體儲存室之緊鄰上層樓設有用水的空間或設備時，應採取下列因應措施：
 - (1) 在上層樓的地板，應施以塗布柏油等防水工程。
 - (2) 在上層樓的地板，應鋪設大尺寸的塑膠布。
- 3、若在緊鄰上層樓無法執行防水施工時，應採取下列因應措施：
 - (1) 準備防水覆蓋物。
 - (2) 在天花板設置接水的盤狀裝置。
 - (3) 在天花板設置漏水偵測設備。

電腦機房、媒體儲存室
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 33	應設置消除靜電之設備。
------	-------------

為防止靜電對資訊系統之不良影響，電腦機房的地板表面材料等，應施以防止靜電產生及預防帶電等特殊處理。

防止靜電的產生或預防帶電，應採取下列措施：

- (1) 電腦機房內部的濕度低於 30 % 時，容易產生靜電，而造成系統之事故。
因此機房內應隨時維持適合機器設備之空調條件（正常情況為 40~60%）。
- (2) 電腦機房的地板材質，應使用能消除靜電並防止帶電的高架地板或良好的接地裝置。
- (3) 使用添加導電劑的塑膠地板、高壓薄板或防止帶電的地毯等。
- (4) 在地板表面塗上防止靜電的蠟或靜電防止劑。請注意，前述靜電防止劑的有效期限會依人員步行頻率而改變。

電腦機房、媒體儲存室
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 34	內部裝潢應使用不燃性材質或具防火性能之材料。
------	------------------------

為保護室內工作人員及資訊設備的安全，內部裝潢應依建築法規之規定，使用不燃性材質，或依消防法規使用具防火性能的材料。

- 1、天花板、牆壁等內部裝潢材料或窗簾等，應經過不燃性或難燃性處理，在發生煙霧或火災擴大時，才能保護室內工作人員及資訊設備的安全。
- 2、依建築基準法規之規定，天花板、牆壁等內部裝潢材料，應使用不燃性的材質，另外，依消防法規的規定，窗簾、地毯等，應使用具防火性能的材料。
- 3、高架地板的主要部份（地板、支架、固定框體），應使用不燃性材質。
- 4、有關不燃性材料或防火性能等，請參照【設 20】。

電腦機房、媒體儲存室
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 35	對於地震等內部裝潢之震落、損壞，應有預防措施。
------	-------------------------

為保護室內工作人員及資訊設備的安全，房間隔牆、天花板、照明器具等，對於地震有震落、損壞可能性的內部裝潢，應有預防震落、損壞之措施。

- 1、在室內空間安置之可移動隔牆、高架地板、天花板等固定物，在地震發生時，很容易受損。防止損壞的措施如下：
 - (1) 隔牆上部，不要固定於天花板，應固定於上層建築物的樓板上，下部不要固定於高架地板上，應固定於建築物的樓板上。
 - (2) 柱與牆壁間，應以固定之補強材料連接。
 - (3) 使用玻璃材質時，為防止破損及碎片飛散，應使用挾網玻璃或貼上防止飛散的膠膜。
- 2、天花板通常使用懸吊鐵絲與骨架懸吊於上層的樓板，天花板應以螺絲釘等固定於樓板上，以免因地震震落。
- 3、防止照明器具掉落之措施，舉例如下：
 - (1) 照明器具應懸吊於上層樓板或固定於天花板之骨架上。
 - (2) 懸吊型照明器具及金屬附件等，容易震落，應使用直接固鎖的照明器具。
 - (3) 具有燈罩的照明器具，應注意其燈罩的掉落。
 - (4) 燈管、燈泡要有防止掉落、破碎及碎片飛散之措施。

電腦機房、媒體儲存室
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
◎			

設 36	高架地板應具有在地震時不會損壞之構造。
------	---------------------

高架地板應具有耐震措施，以免因地震發生而損壞。

1、高架地板是配合資訊系統設備必要之配線及空調通路，多安置於樓板支撐的承柱上，高架地板嵌板與活動面板相似，非常容易拆卸，因此地震發生時，亦容易受損破壞。因此應有適當之措施，加強耐震性能，以免地震時，發生地板滑動或掉落，以及承柱翻倒的情形。

2、高架地板加強耐震性能，具體實例如下：

(1) 承柱

一般來說，承柱對於垂直方向的負荷能力非常強，但對於水平方向的承受力則非常弱。要補強承柱對水平方向的支撐強度，應有下列的措施：

- 各個承柱間，應以角鋼或固定架框連接。(圖 1、2)
- 承柱與建築物樓板連接處，應以螺絲釘固定。
- 承柱與建築物樓板連接處，應以黏着劑施工固定。

(2) 高架地板面

高架地板之板面，由鄰接之地板相互支撐，故若有部分板面鬆脫或掉落時，則可能會引起整個高架地板崩潰。固定高架地板的方式，有下列之措施，但這些措施可不必對每一塊地板實施，僅對機器設備底下及其附近、通道附近等，作重點性之實施即可。

- 對固定用之金屬板以螺絲栓緊固定。(圖 3)
- 利用金屬卡榫固定。
- 使用附有鉤爪的地板塊或承柱。

(3) 切割之高架地板開口處

移除地板作為高架地板之空調出風口部份，應套上鋼製網架等固定之，

以免周圍的地板滑動。(圖 4)另外，切除地板作為纜線配線出口部份，應套上補強框(圖 5)、補助承柱、止動器(圖 6)等，以免設備滑動掉落。注意，高架地板板面的切割，以必要之最小範圍來執行。

3、在建築物及牆壁間裝置彈簧等緩衝器來吸收地震之震動或使用免震結構之地板等，應檢討下列事項：

- (1) 會受到資訊系統設備及其相關週邊設備(分電盤、端子盤等)等設置位置之影響及限制。
- (2) 在地板底下之佈線，常受底下空間之限制。
- (3) 設置資訊系統設備之有效空間減少。
- (4) 纜線與固定地板間之接點，有磨損消耗之可能。

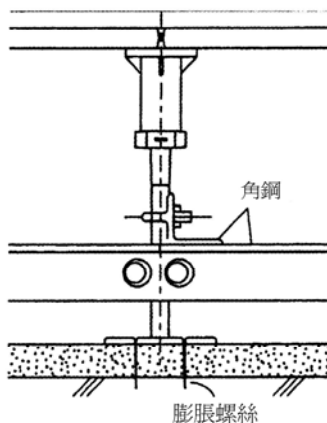


圖 1 利用角鋼之補強例

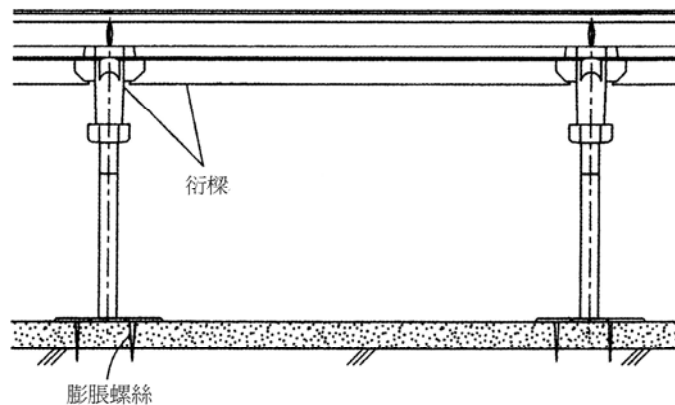


圖 2 利用固定架框之補強例

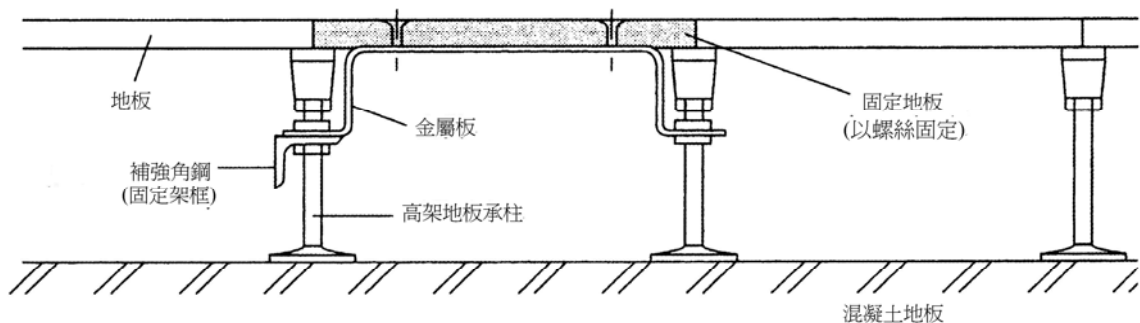


圖 3 固定地板之實例

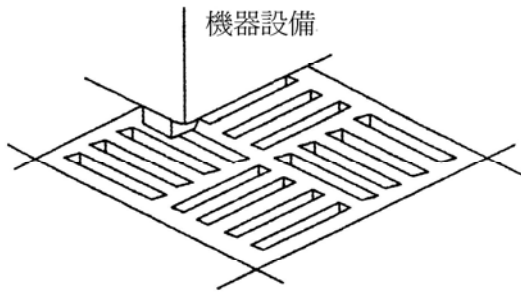


圖 4 鋼製蜂巢板例圖

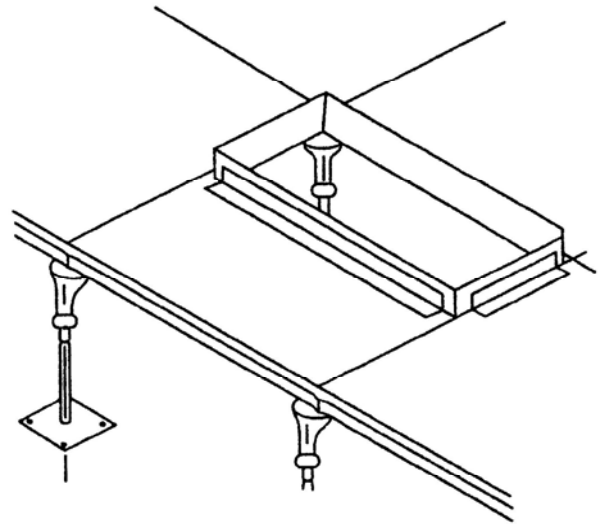


圖 5 開口部補強架框之安裝例圖

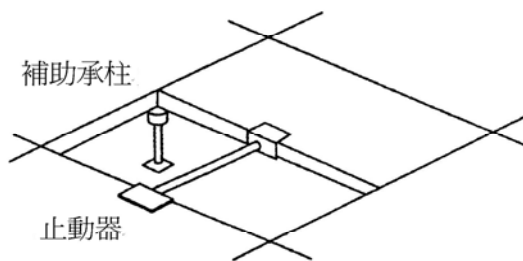


圖 6 補助承柱與止動器例圖

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

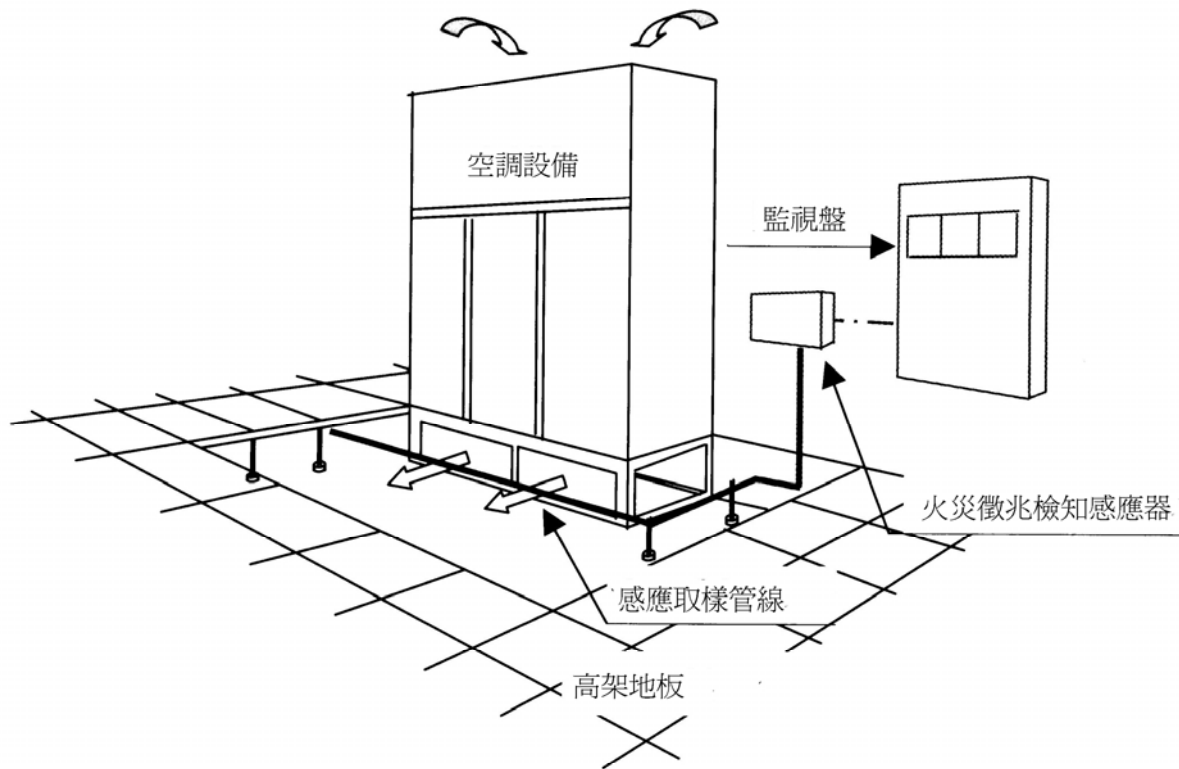
設 37	應設置自動火災檢知警報裝置。
------	----------------

萬一發生火災時，為能早期發現、發出警報、並啟動初期滅火及避難通報作業，機房內應設置適當的自動火災檢知通報裝置。

- 1、電腦機房、媒體儲存室多存放著容易受高溫或煙霧損傷的機器設備及磁性媒體，而平時只有少數的系統操作人員在室內。因此應設置能早期發現火災、發出警報之自動火災檢知通報裝置。
- 2、自動火災檢知通報裝置，分為火災感知器及將感應狀態通報各處之受信裝置兩部份。火災感知器有利用各種原理及構造的多種裝置，大致上可分為熱感應器、煙感應器及火感應器。一般煙感應器能較早期發現火災，故多被廣泛使用。自動火災檢知通報裝置的設置，應選擇最適合的設備，必要時可以使用不同架構的組合設備。自動火災檢知通報裝置，應配置備用電源，以備一般市電停電時，仍能正常運作。
- 3、安裝感應器的位置與數量，是依使用的感應器種類而定。在高架地板底下，通訊線、電源線密布，容易發生火災的地方，最好也能裝置感知器。

(參考)

電腦機房內，為能充分冷卻機器設備，在室內隨時都有大量的空調氣流循環，因此火災發生時所產生的煙霧，會被稀釋並擴散至整個機房，火災不易被早期發現。在這種情況下，最好能夠裝置對室內環境的變化能敏感察知，預先檢出火災徵兆的感應系統。



火災徵兆檢知系統設置例

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 38	應設置火災等緊急事故警示及緊急連絡裝置。
------	----------------------

火災等緊急事故警示及連絡裝置包含警鈴、警報器、緊急廣播設備、緊急電話等。

- 1、設置警鈴、警報器或緊急廣播設備之擴音器、緊急電話等裝置，以便於遇火災等緊急事故時，可以向機房、媒體儲存室之人員警示，並接受初步之滅火、避難等適當的指示。緊急聯絡裝置應配合電腦機房、媒體儲存室之狀況，選用一種或數種適當裝置組合。
- 2、設置緊急電話，於發生火災等緊急事故時，能迅速向中央監控室（防災中心等）安全負責人通報。緊急電話為防災專用，應事先將「緊急專用電話」及「緊急時連絡電話號碼」等明確標示。另外，緊急連絡電話，最好與資訊系統發生故障時之連絡用熱線電話，分別裝設。
- 3、緊急通報、緊急廣播設備之設置點，應以能迅速傳達通報內容、引導避難等為考量，例如經常有管理建築物值勤的地方，或是中央監控室等地方。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 39	應設置滅火設備。
------	----------

為了避免損及電器系統之安全，電腦機件之滅火劑宜採用氣體類滅火劑，而最好使用能在一定時間內，把滅火所需濃度的滅火劑平均充滿在防火區內的全域噴出型設備。除設置氣體類滅火設備外，亦可加裝自動灑水設備。為撲滅局部火災，應設置如二氧化碳滅火器之類之氣體類滅火器。

- 1、實際發生火災時，除能迅速滅火外，未罹災部分所安裝的電腦系統各機器與保管中之資料希望能不受損害，且在滅火後儘速再使用。因此電腦機房、媒體儲存室之滅火設備，應採用滅火後給機器之損害較少的氣體類滅火設備。
- 2、在電腦機房的氣體滅火設備，最好採用全區域噴射方式的滅火設備。全區域噴射方式的滅火設備，是指對使用耐火性材料來區隔的室內，能由噴氣頭對全室噴出滅火氣體的裝置。其設備的組成如圖 1 所示，由噴氣頭、起動裝置、音響警報裝置、配管、電源、自動火災通報裝置之感應器等構成。
- 3、氣體滅火劑，於海龍系統因環保因素停止使用後，替代的系統大體上包括鹵化烷化合物氣體（如 FM200、FE-13 等），以及非活性氣體（如氮氣、二氧化碳、IG-541、IG-55 等）。在設置氣體滅火裝置時，應與設備廠商等充分討論溝通後再決定最適當的設備。
- 4、在設置氣體滅火裝置時，應注意下列各事項：
 - (1) 考慮滅火劑對人體的影響，決定使用的場所及使用的方法。
 - (2) 為了警示氣體噴出時的危險性，在機房進出口處，應設置氣體噴出指示燈。
 - (3) 為了能在滅火後，對人不發生影響之情況下換氣，換氣設備之開關，應

能由室外操作。

- (4) 有減低滅火效果之虞的通風管，應設置通風管自動關閉裝置，以免在滅火氣體噴出前，降低滅火效果。

5、自動灑水滅火裝置

設置自動灑水滅火裝置時，儘可能採用前置動作方式（Pre-action）的裝置。前置動作方式的自動灑水滅火裝置具有防止因錯誤動作（如噴嘴前端不慎破損）引起的灑水滅火。如圖 2 所示，裝置是由閉鎖式灑水頭、與火災警報器連動之前置動作閥（Pre-action valve）、主立管等構成。平時，前置動作閥與灑水噴嘴之間的配管不注水，因此即使灑水頭誤動作也不會灑水，同時若火災警報器發生誤動作，而開啟動作閥時，因由於採用閉鎖型頭而不致於灑水。

6、設置自動灑水滅火裝置時，應注意下列各事項：

- (1) 為避免水害擴大，應在高架地板下設置排水溝。
- (2) 應有消防水之排水與室內烘乾功能。
- (3) 淋濕之機器需要相當時間之維修，因此要徹底考慮安裝機器之位置與方式，例如將平時使用機器與備援機器隔離安裝，以便遇到萬一狀況，亦能在短時間內開始運轉主要系統。

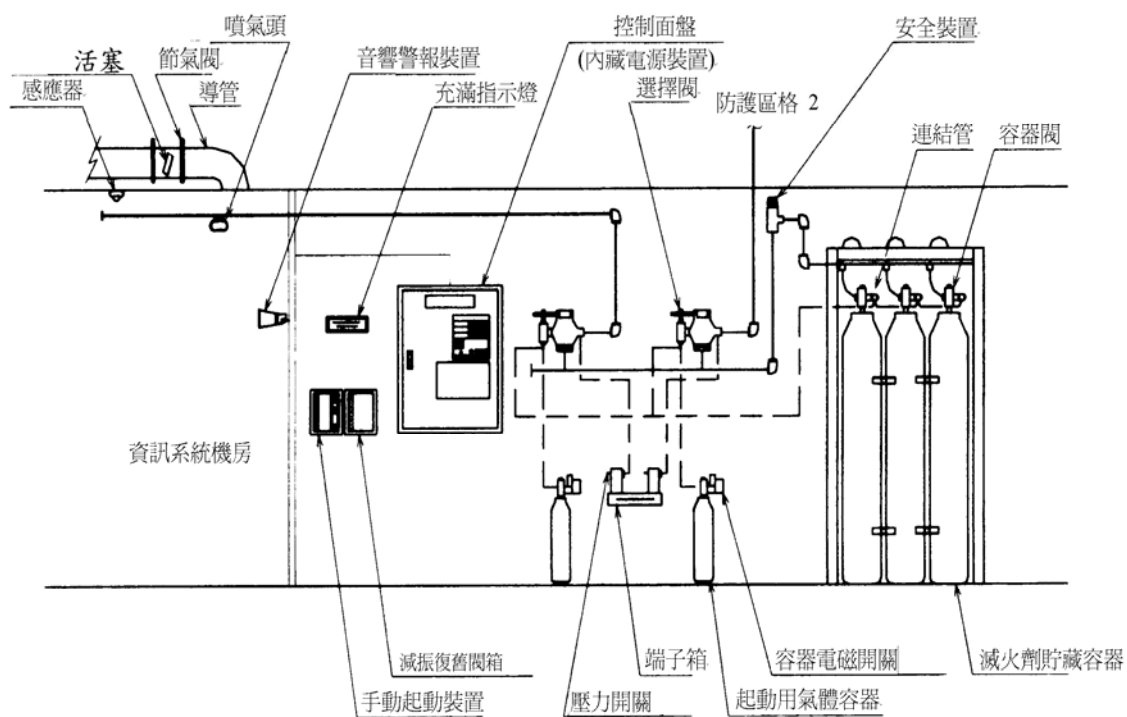


圖 1 氣體式滅火裝置

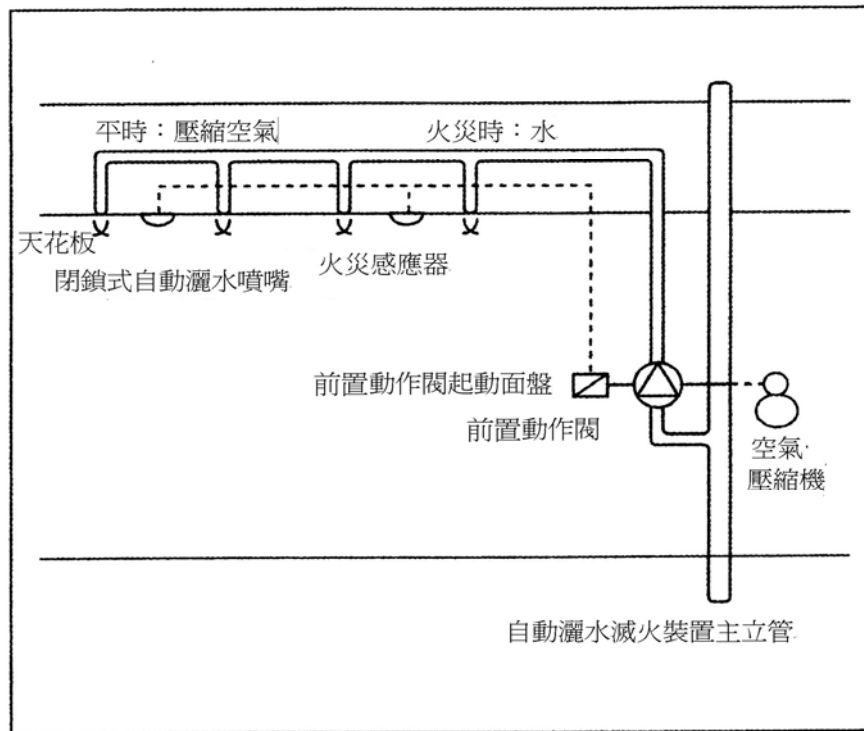


圖 2 預備動作方式的自動灑水滅火裝置之實例

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 40	纜線之耐火及防止延燒之措施。
------	----------------

為防止電纜線的燃燒、延燒，電纜線應具耐火措施。對於在牆面電纜線貫穿部分，應有防止延燒的措施。

- 1、電纜線絕緣體容易因過大電流、周圍火災等而著火燃燒，萬一著火時，其燃燒力強，也會產生具腐蝕性之有毒氣體。同時電纜線所產生的有毒氣體可能在未受火災危害地區，造成二次災害。因此，應儘可能在電纜線上採用耐火處理，在牆壁面電纜線貫穿部分，亦應有防止延燒的措施。
- 2、使用難燃性電纜線或塗布延燒防止劑，是有效的防火措施。延燒防止劑有防止電纜線着火與延燒之塗料，以及填塞於電纜線貫穿耐火結構牆壁部分之防火油灰等物質，應使用政府機構所認可的材料。
- 3、電纜線貫穿耐火結構之地板或牆面時，為防止因火災產生的煙霧侵襲及延燒，如圖 1 所示，應在貫穿部分的空隙裏填塞灰泥、石棉、防火油灰等耐火材料，施以適當的延燒防止措施。同時，當電纜線貫穿耐火結構牆等壁面時，其貫穿部分及貫穿部周圍兩側一公尺以內部分，應使用耐火材料覆蓋。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 41	應設置排煙設備。
------	----------

為預防火災之災害，應設置排煙設備。

- 1、設置排煙設備之目的，係在發生火災時，能將煙霧排出屋外，以抑止煙霧擴散至避難通道等其他區域，以利安全避難與進行消防工作，同時也能防止資訊系統設備、資料媒體等之污染破壞。
- 2、排煙設備，應依照我國建築相關法規之規定設置。
- 3、排煙設備有自然排煙方式與機器排煙方式兩種。自然排煙方式是在屋頂或外壁上開設有排煙效果的窗口，利用煙本身的浮力排煙。對於自然排煙方式的排煙窗，有其位置、大小、操作方法等規定。機械排煙方式則由排煙機、通風管、排煙口、電源等構成，在火災發生時，以人工起動裝置或自動起動裝置起動排煙機，將煙排到屋外。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 42	設置緊急照明設備與攜帶式照明設備。
------	-------------------

為於火災發生時，人員能即時安全避難，電腦機房內，應設置緊急照明設備及準備攜帶式照明設備。

- 1、緊急照明設備應具有必要的構造及性能，舉例如下：
 - (1) 照明應為直接照明，地板表面的亮度要在1勒克司以上。
 - (2) 照明器具之主要部份，應使用不燃性材料製造或覆蓋。
 - (3) 應設置備用電源。
- 2、緊急照明設備之備用電源，分為放置於照明器具內部之內建型電池，及將大型電池集中放在另外一處的電源另置型。電池內建型之備用電源，多使用於小規模之建築物內，另置大型備用電池的方式，則多使用於較大規模建築物中。
- 3、攜帶用照明器具，是指可以攜帶之手電筒等照明器具。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 43	不可裝設一般用水設備。
------	-------------

為防止因漏水造成對資訊系統的嚴重影響，在電腦機房、媒體儲存室內不可設置一般用水設備。

- 1、為防止漏水，不可設置洗手檯、茶水供應裝置等用水設備。同時為預防由牆壁、天花板、緊鄰上層樓地板滲水，應採取防水措施，並於必要時在配水管線周圍，裝置漏水偵測裝置，以利即時發現漏水現象。
- 2、若於電腦機房應設置用水裝置（例如水冷式電腦系統之冷卻裝置、空調系統之冷卻設備等）時，用水裝置周圍應設置漏水偵測裝置、漏水接盤、防水堤、排水溝、配水管及防止漏水的措施。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
○			

設 44	應安裝地震感應器。
------	-----------

電腦機房儘可能設置地震感應器。

- 1、利用地震感應器之震度顯示，可以作為防災行動判斷基準。在地震之後，依震度來判斷及決定設備檢查維修的程度。因此最好能在電腦機房設置地震感應器。
- 2、地震感應器應具有依設定地震規模大小，以音響、燈號等發出警報的功能。依警報或顯示之地震震度，如要以手動方式停止作業時，需訂定判斷基準，依既定的作業程序辦理。
- 3、若與地震感應器連動，以自動方式控制資訊系統作業之運作時，須留意下列事項：
 - (1) 若與地震感應器連動，自動控制電腦系統、電源、空調設備等運轉或執行資料媒體的保護動作時，應確保電腦系統軟體、硬體等整體的關連性體制。
 - (2) 地震感應器應設置於電腦機房或其附近相關地點。
 - (3) 地震感應器應配合資訊系統的可信賴度，選用適當品質的設備，不能因操作錯誤造成系統作業之停頓。
 - (4) 自動運轉控制裝置，應具備良好的耐震性。
 - (5) 電腦系統、電源、空調設備等系統，在停止運作後之復原作業，應簡單容易執行。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
○			

設 45	於機房進出口設置進出管制與防犯設備。
------	--------------------

為防止非法入侵，電腦機房、媒體儲存室等出入口，應設置能夠記錄進出狀況之管制設施。另外，儘可能安裝防範歹徒的防犯設備。

1、電腦機房應設置進出管制設施，以及防止非法入侵設備機制。

2、進出管制設施，舉例如下：

(1) 受理申請設備。

(2) 開關裝置：

a. 磁卡進出管理裝置。

b. 讀卡裝置。

c. IC 卡、光卡進出管理裝置。

d. 密碼輸入裝置。

e. 掌形、掌紋識別裝置。

f. 指紋比對裝置。

g. 視網膜形狀辨認裝置。

h. 簽字立即辨認裝置。

i. 聲紋認知裝置。

3、防犯設備：

(1) 對講機。

(2) 防犯電視攝影機。

(3) 防犯照相機。

(4) 防犯歹徒警報裝置。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
◎			

設 46	應設置溫濕度自動記錄裝置或溫濕度警報裝置。
------	-----------------------

為預防資訊系統的故障發生，並能在故障時分析其發生故障的原因，應設置溫濕度自動記錄裝置或溫濕度警報裝置。

- 1、溫濕度自動記錄裝置，是自動檢測電腦機房及媒體儲存室的溫濕度，並予記錄之裝置。溫濕度警報裝置於機房內溫溼度超過原先設定之範圍時，會發出警報以引起注意，以儘速採取適當處理之裝置。與溫濕度自動控制裝置連動的溫濕度自動記錄裝置，可以保持電腦機房及媒體儲存室之溫濕度在規定的範圍內，也可以提供資料以分析故障原因。
- 2、測定溫濕度的位置，應避免設置於機器設備出風口、空調設備之出風口等直接接受風的位置，亦應避免設置於機房出入口、溫濕度變化大的場所。

電腦機房、媒體儲存室
設備

適用性分類			
中心	總行	合作	直接
○			

設 47	應設有預防蟲鼠害之措施。
------	--------------

設有預防蟲鼠害的措施，以防止電纜線遭蟲、鼠咬損。

- 1、要防止因老鼠及蟑螂侵入、築窩而發生數據電路、電源電纜之漏電、接觸不良、腐蝕、斷線等以致引起電腦系統之故障，因此儘可能要有防止蟲鼠害之措施。
- 2、防止蟲鼠害的措施，舉例如下：
 - (1) 堵塞因配管或配線等工程而在牆壁上造成的空隙。
 - (2) 在下水道、排水溝、通風口等地方，以鐵絲或金屬網隔絕。
 - (3) 在電纜線、牆壁面等處塗抹環乙烯等驅鼠劑。
 - (4) 使用有混摻驅鼠劑的電纜。
- 3、若在大樓裏設有廚房、飲食店等適合老鼠棲身的場所時，鼠害會隨之增加，因此應考慮使用食品之完全收藏、廚房廢棄物完全處理等有關設備。

電腦機房、媒體儲存室
資訊系統設備、其他各項設備及備用物品

適用性分類			
中心	總行	合作	直接
◎			

設 48	各類雜項設備及備用品，應具有防火性能。
------	---------------------

為防止引火及擴大火災之災害，各類雜項設備及備用用品，應使用類似鋼製品等具有防火性能的設備。

- 1、在電腦機房、媒體儲存室使用之各類雜項設備及備用用品，應使用火災時不產生有害氣體與煙霧的鋼鐵、鋁等不燃材料製品，儘量少用可燃性椅子等物品。
- 2、電腦機房、媒體儲存室所使用的消耗品與文書，其收放方式應注意防火安全。萬一發生火災時，文書等可燃物如收放在防火鋼製書櫃等箱櫃裏，則比露出在桌上較能延緩火災之進行速度，因此較能獲得初步滅火或避難所需之時間。

電腦機房、媒體儲存室
資訊系統設備、其他各項設備及備用物品

適用性分類			
中心	總行	合作	直接
◎			

設 49	應設置防止靜電之措施。
------	-------------

為防止靜電對資訊系統產生不良影響，對於資訊系統設備、各類雜項設備及備用品，應具有防止靜電的預防措施。

防止靜電產生及帶電的措施，舉例如下：

- (1) 電腦機房的濕度降到 30 % 以下時，容易產生靜電，進而造成系統故障等事故，機房的空調應維持在系統所能容許的條件(一般情況為 40 ~ 60 %)。
- (2) 為抑止電腦機房工作人員產生靜電，工作人員宜穿着防止帶電之導電性纖維工作服及導電性橡膠鞋。
- (3) 機房應設置接地線之接頭，以便隨時連接地線，將多餘的靜電導至地下。
- (4) 可移動式設備（如磁帶、磁碟之搬運車等物）儘可能採用不銹鋼等不產生靜電材質的製品。

電腦機房、媒體儲存室
資訊系統設備、其他各項設備及備用物品

適用性分類			
中心	總行	合作	直接
◎			

設 50	各類雜項設備及備用品應具有耐震措施。
------	--------------------

地震發生時，為不影響工作人員及資訊系統設備，機器設備及各類雜項設備應具耐震措施。

1、防止機器設備之移位、翻倒而發生故障或破壞的措施，舉例如下：

(1) 固定於建築物結構體

- a. 以耐震角架固定。
- b. 以防止移動之金屬固定器具、橡膠腳墊等固定(如圖 1、圖 2)。
- c. 以翻倒防止框固定(如圖 3)。

(2) 以防震結構支撐

- a. 收藏於防震建築物中。
- b. 收藏於耐震建築物中。
- c. 將設備安置於防震基礎上。
- d. 將整個機器設備以防震結構支撐

(3) 將放置於桌上的機器設備，以防止滑落金屬固定器具、金屬皮帶等固定(如圖 4、圖 5)。

(4) 設置於機架上之數據機等設備，應以防止滑落金屬固定器具、金屬皮帶等固定。

2、在地震時會移動或翻倒，而使系統受到影響的雜項設備等，應具有防止移位、翻倒的措施，舉例如下：

(1) 放置式之雜項設備、備用品及資料保管設備等

- a. 以金屬固定器具固定於地板、牆壁或天花板上(如圖 6・例 1)。
- b. 具間隔空隙之備用設備，上部以不銹鋼管等連結器具相連結(如圖 6・例 2)。

- c. 背部相靠之備用設備，上部或下部相互連結（如圖 6・例 3）。
- d. 桌上之備用設備，固定於桌面上，或安裝於防止滑落的框上。
- e. 備用品之開口門或抽屜，應上鎖。
- f. 沒有設置門的開放式棚架型資料保管設備，應加裝防止滑落之止落器，以防磁性媒體滑落。

(2) 移動式雜項設備、備用品及資料保管設備等

- a. 在鐵軌上之移動式機架，應加裝防止脫軌之裝置。
- b. 臺車、椅子等有滑輪等設備，應加裝腳輪止滑制動器。

3、防止電腦機器設備之滑動、翻倒之耐震施工，依設備之重量、形狀、安裝場所等不同，廠商提供的建議施工方式亦不相同，請與設備廠商、建築業者討論協調後，再行施工。

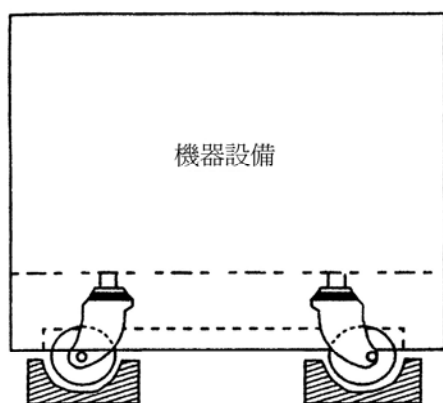


圖 1 腳輪固定器之實例

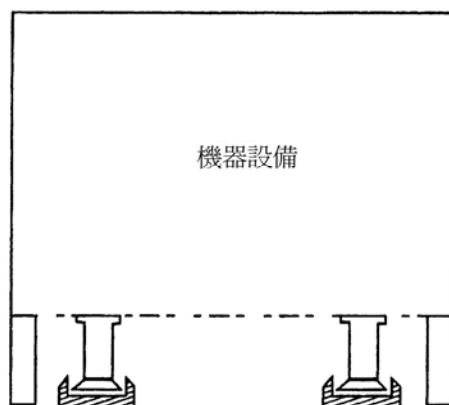


圖 2 橡膠腳墊之實例

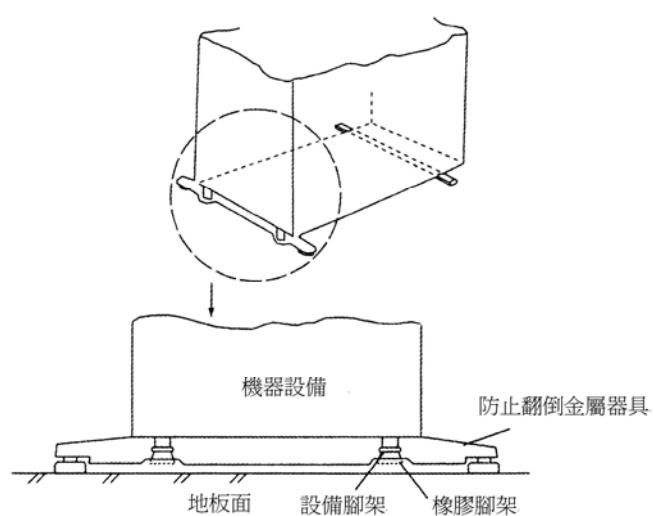


圖 3 翻倒防止框之安裝實例

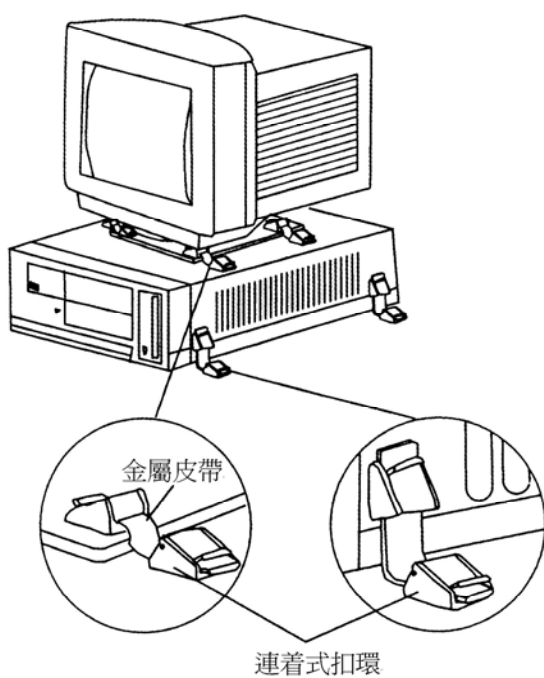


圖 4 以耐震金屬皮帶固定之實例

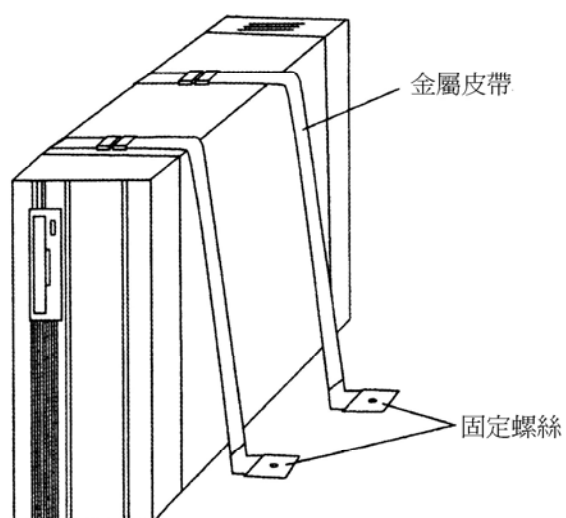
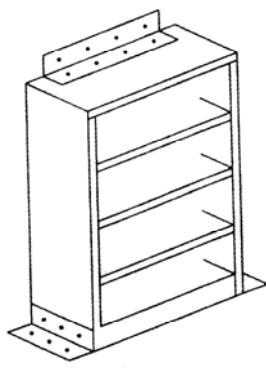
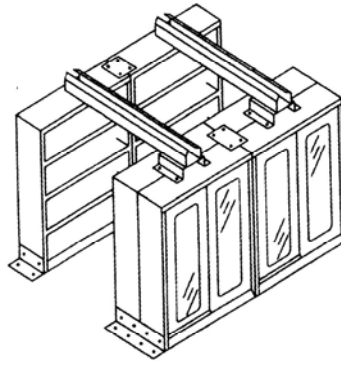


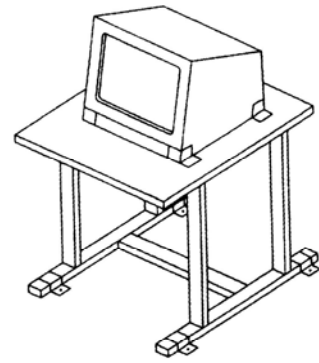
圖 5 耐震金屬皮帶設置例



例 1



例 2



例 3

圖 6 固定雜項設備例圖

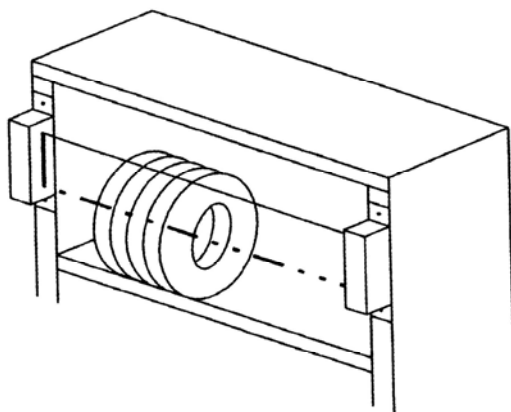
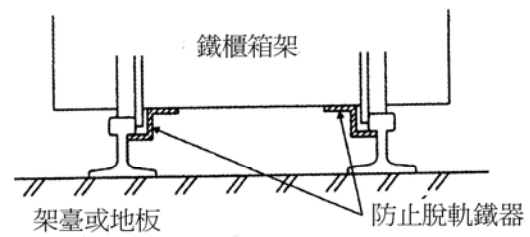
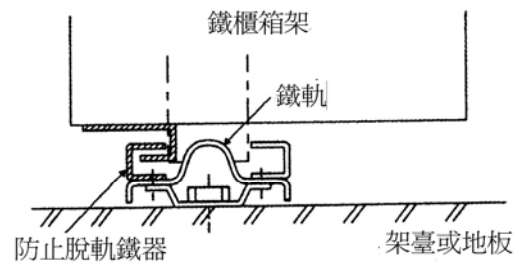


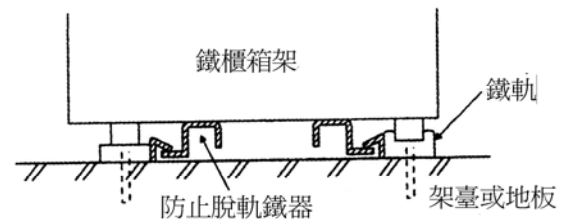
圖 7 防止滑落止落器例圖



例 1



例 2



例 3

圖 8 固定移動保管庫例圖

電腦機房、媒體儲存室
資訊系統設備、其他各項設備及備用物品

適用性分類			
中心	總行	合作	直接
◎			

設 51	搬運車等應安裝固定裝置。
------	--------------

地震發生時，為不會傷害工作人員及資訊系統設備，磁帶、磁碟等媒體之搬運車等，應安裝煞車或固定裝置。
--

搬運車等之煞車裝置或固定裝置，舉例如下：

(1) 在車輪上安裝腳輪制動器或煞車裝置(如圖 1、圖 2)。

(2) 利用鋼索或鑰匙等固定(如圖 3)。

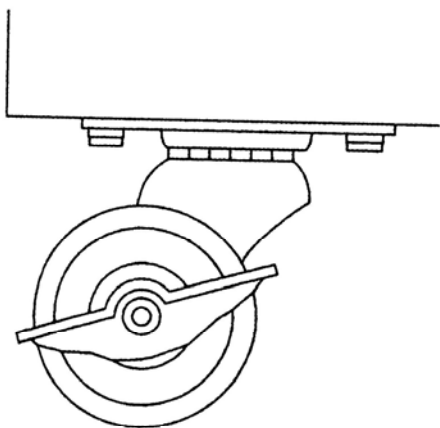


圖 1 腳輪制動器例圖

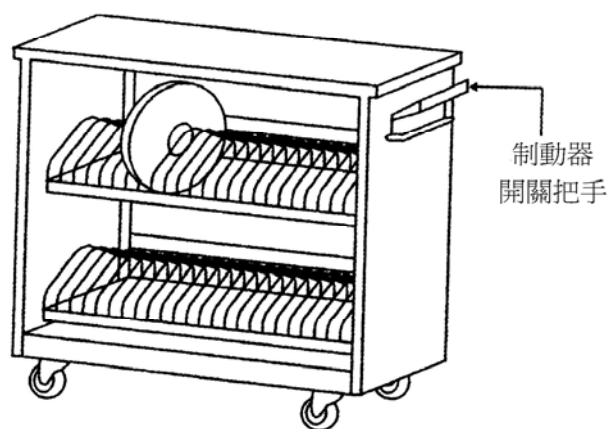


圖 2 放開把手會自動煞車的搬運車

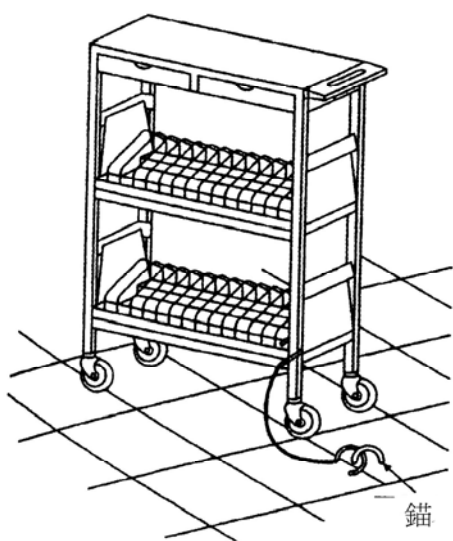


圖 3 高架臺例圖

一、資訊中心

(三) 電源室、空調室

電源室內設置之電源設備，是為了對資訊系統供應穩定的電力，空調室內設置之空調設備，也是為了維持、管理機房穩定的溫濕度。這些房間平時都是在無人的狀態下運作，因此應在這些房間，設置能及早發現事故，將災害降至最低範圍的必要裝置。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 52	應設置於不易受到災害之位置。
------	----------------

為了防止對資訊系統作業的影響，應設置於不易受到地震、火災、水患等災害的位置。

在建築物內，不易受到各類災害，可以作為設置電源室、空調室的場所，舉例如下。若不得已應將電源室、空調室設置於有可能遭受各種災害的位置時，應對各類災害，採取必要的因應措施。

- (1) 地震時，震動程度較小的位置。
- (2) 較少受到火災危害的位置。
- (3) 較少淹水或水分滲透的位置。
- (4) 遠離危險物品儲藏或危險物品處理場所等，應在對危險物品之傷害較少的地區。
- (5) 較少產生可燃性或具腐蝕性蒸氣、氣體或粉塵等的位置。
- (6) 溫度不會過高或過低的位置。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 53	應確保維修保養時必要的空間。
------	----------------

為機器、設備等之維修保養及工作人員在災難時之避難疏散，應確保必要的空間。

在電源室、空調室內設置機器設備時，應在設備間確保相關法規規定的空間。

(參考)

變電設備之應保持間隔距離，如下列 表1 所示

表 1 變電設備應保有之間隔距離

須確保間隔距離的部分		應確保的距離
配電盤	操作面	(1) 1.0 公尺以上 (2) 1.2 公尺以上：操作面盤互相面對面時。
	維修設備之面 有通風口之面	0.6 公尺 0.2 公尺
變壓器、電容器、 其他屬於此類的機器設備	維修設備之面	(1) 0.6 公尺以上 (2) 1.0 公尺以上：操作面盤互相面對面時。
	其他面	0.1 公尺

電源室、空調室

適用性分類			
中心	總行	合作	直接
○			

設 54	應為專用之獨立房間。
------	------------

為了易於維護、管理，並防止災害的擴大， <u>應考量</u> 與其他各室分隔 <u>專用之獨立房間</u> 。

- 1、電源室、空調室最好與其他各室分離，成為專用之獨立房間，其目的除為了易於維修管理之外，尚為能防止由電源室、空調室發生之災害擴大到其他地區。
- 2、所謂專用之獨立房間，是指電源室、空調室不與電腦機房、資料保管室、辦公室等共用房間。室內安裝型之電源設備及空調設備等若不安裝於獨立之電源室、空調室時，應採取防水、防火的措施。
- 3、電源室、空調室，通常不會有人員常駐，應設置門禁管理，非維修管理或操作等相關人員，應無法進入。
- 4、為能對消防人員明示電源室、空調室的位置，應將兩個房間的相關位置平面圖，標示於建築物內部、中央管理室等不易由外部看到的地方。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 55	門窗應加鎖，最好不要設置窗戶。
------	-----------------

為防止由外部的入侵，並達到防火、防水的目標，最好不要設置窗戶，並在進出的門口設置門禁管控。

- 1、通常，電源室、空調室均無人員常駐，僅在一定時間由維護人員巡視檢查。
因此，電源室、空調室最好不要設置窗戶，並在進出的門設置門禁管控，以防止由外部的入侵，並達到防火、防水的目標。
- 2、進出門口應使用防火門，並應有充分的強度。
- 3、電源室、空調室之出入門口，應限設置一處，如有兩處以上時，其管理規定應與僅有一個出入門的管理方式相同。
- 4、電源室、空調室若設置窗戶、換氣口等時，應具有防災、防犯的措施。
- 5、請參照【設 29】之說明。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 56	應採用耐火結構。
------	----------

應採用耐火結構，以防止火災。

- 1、依建築相關法規之規定，電源室、空調室應採用耐火結構。
- 2、電源纜線等應貫穿電源室、空調室之耐火結構牆壁面時，應採取防止延燒的措施。
- 3、請參照【設 31】之說明。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 57	應安裝自動火災警報設備。
------	--------------

為早期發現火災，應安裝自動火災警報設備。

- 1、通常，電源室、空調室均無人員常駐，當火災發生時，為能早期發現火災，並向中央管理室通報，迅速採取初步滅火工作，應安裝自動火災警報設備。
- 2、採用之感應器，可分為熱感應器、火燄感應器及煙霧感應器，在電源室、空調室使用之感應器，以煙霧感應器較為適合。
- 3、請參照【設 37】之說明。

電源室、空調室

適用性分類			
中心	總行	合作	直接
○			

設 58	應安裝氣體滅火設備。
------	------------

為能因應火災時迅速滅火，應安裝全域放出型之氣體滅火設備。

- 1、通常，電源室、空調室均無人員常駐，應安裝能全域放出型之氣體滅火設備。
- 2、若因電源室、空調室之結構問題，無法安裝全域放出型之氣體滅火設備時，應設置可以移動之二氧化碳型滅火器等氣體滅火裝置。設置滅火器的位置，應為火災發生時，能迅速取用的位置，如在電源室、空調室之出入口等位置。
- 3、請參照【設39】之說明。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 59	空調設備應設有防止漏水的措施。
------	-----------------

避免因漏水造成系統的事故，冷卻水應設有防止漏水的措施，以預防冷卻水外漏及凝結等情況發生。

- 1、空調室內部，空調設備之周邊及其正下方，應設置如接水盤、防水堤、排水口等防止漏水的設施，以預防冷卻水外漏、凝結以及因灰塵阻塞排水孔等情況發生。
- 2、在外牆上設置之進氣口、排氣口等，均需採取避免雨水侵入的防水結構。

電源室、空調室

適用性分類			
中心	總行	合作	直接
◎			

設 60	電纜線、各類導管導線等，應設有防止延燒的措施。
------	-------------------------

為避免延燒情況發生，應設有防止由電纜線、導管管線等引起延燒的措施。

- 1、為能避免火災延燒情況發生，在牆壁面上電纜線、導管管線等貫穿部分，應設有防止延燒的措施。
- 2、請參照【設 40】之說明。

一、資訊中心

(四) 電源設備

電源設備應隨時供應穩定必要的電力，應避免因停電、異常電壓、異常周波數、電源的瞬斷、過大電流、漏電及電源設備本身的故障等，而影響到資訊系統的正常運作。

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 61	電源設備之容量，應保持充裕有餘。
------	------------------

為能穩定供應資訊系統設備必要的電力，電源設備應備有充裕的容量。

- 1、此處所稱電源設備的容量，是指電源變壓器的額定容量、發電機的定額輸出容量以及配電纜線的容許電流容量等。
- 2、為了使電源設備具有充裕的容量，應注意下列事項：
 - (1) 電源設備之容量，應依據建築物的規模、資訊系統機房的規模、設置於各房間之機器設備的用電量，並檢討各房間的使用目的或使用條件等，加上未來必要之寬裕容量來估算電力的需求。
 - (2) 電腦系統及各周邊設備多裝有電容器及電動馬達等，因此電源的容量應能容納開機時之瞬間起動電流，以免引起電源跳電。
 - (3) 電源纜線之選擇與佈線，應考慮電源電壓瞬間變動、配線距離導致之電壓下降等情況，避免對電腦系統及其周邊設備造成可能的影響。
 - (4) 應採用高可靠性及容易維修的產品。
 - (5) 配合未來有增加用電負荷之可能性，應保留增加配線的空間，在電源室內應保留增加設備或提升設備所需之空間。
- 3、在不影響電源設備的情況下，需在電腦系統所使用之三相電源上，連接使用單相電源的設備時，其欠相率應不超出 30 %。
 - (1) 欠相率是指各線間連接的使用單相電源之機器設備，其負載總設備容量 (VA) 之最大與最小值之差額，與總負載設備容量 (VA) 之平均值之比 (%)，以下列公式表示之：

$$\text{欠相率} = \frac{\text{各線間連接之單相設備負載總設備容量最大最小值之差}}{\text{總負載設備容量之 } 1/3} \times 100$$

- (2) 欠相率之計算，是以電源設備至電腦系統為止的範圍為對象。因此電腦系統各機器設備間，不論其內部迴路是單相或三相迴路，應以整個設備為計算整體總負載之設備容量。

電源設備

適用性分類			
中心	總行	合作	直接
○			

設 62	應以多重迴路引入電源。
------	-------------

為了預防受變電設備發生故障，電源應以多重迴路引進。

- 1、為能在受變電設備發生故障時，仍能供應穩定的電源給電腦系統設備，由電力公司之受電設備，應以多重迴路引入電源。
- 2、多重迴路受電的方法，舉例如下：
 - (1) 以正線與備用線兩迴路受電(如圖 1)。
 - (2) 串聯 (Loop)受電。
 - (3) 並聯 (Spot network)受電。

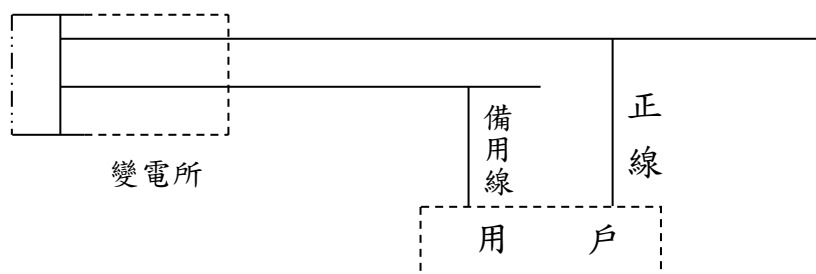


圖 1 正線、備用線，兩迴路受電實

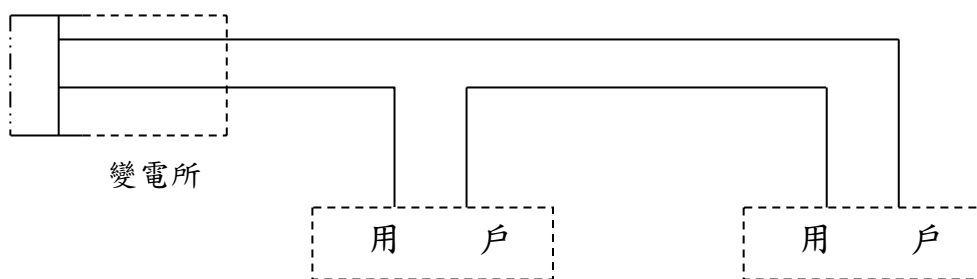


圖 2 串聯迴路受電實例

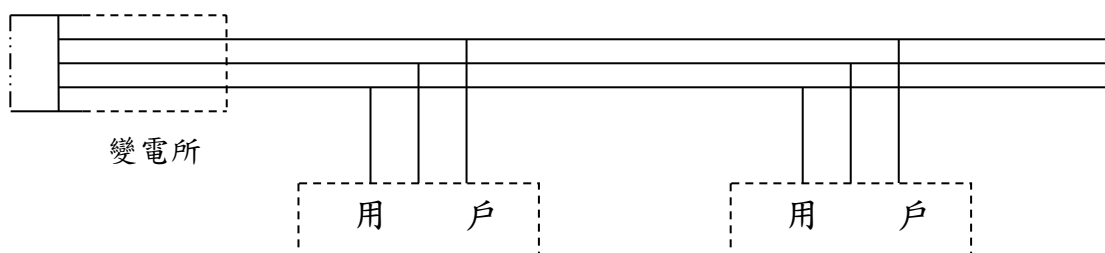


圖 3 並聯迴路受電實例

(參考)

依不同地區，當變電所發生故障而停電時，有些地區會自動切換輸電路由，由其他地區供電，請先與當地電力公司確認。

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 63	應設置能提供良質電力之供電設備。
------	------------------

為使資訊系統設備能穩定運作，應設置能提供良質電力之供電設備。

- 1、為使資訊系統能長期穩定運作，供電設備應設置具 CVCF (Constant Voltage Constant Frequency Power Supply：定電壓定周波數之穩壓穩頻設備)裝置。CVCF 裝置是一種不受輸入電源的變動或輸出負載變動，能確保對電腦系統供應之電力維持一定的電壓及周波數。
- 2、為避免因電源瞬斷或停電造成的資訊系統作業停頓，應設置 UPS (Uninterruptible Power Supply：不斷電電源設備)。UPS 是指當市電電源發生短暫時間的停電時，能由其蓄電池供應電力，使資訊系統持續作業的裝置。同時，當市電電源在長時間停電時，為使資訊系統能持續作業，UPS 裝置應能接受由自備發電機供應的電力，持續運轉作業。為達到這個目標，應在 CVCF 裝置上附加蓄電池、充電器等設備。不停電的電力供應系統，有下列幾種：

(1) CVCF + 蓄電池方式(如圖 1)

(2) CVCF + 蓄電池 + 自備發電機方式(如圖 2)

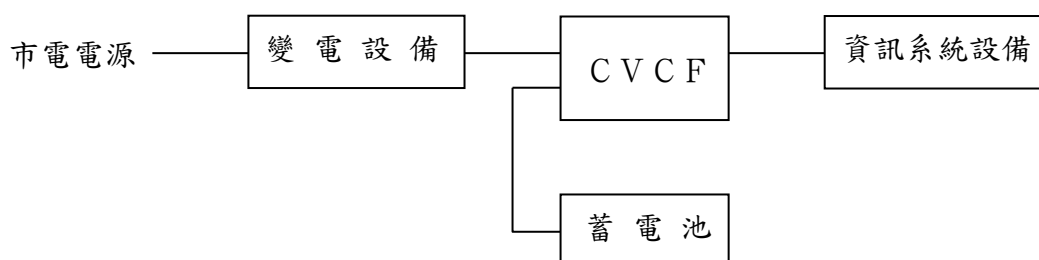


圖 1 CVCF + 蓄電池方式之實例

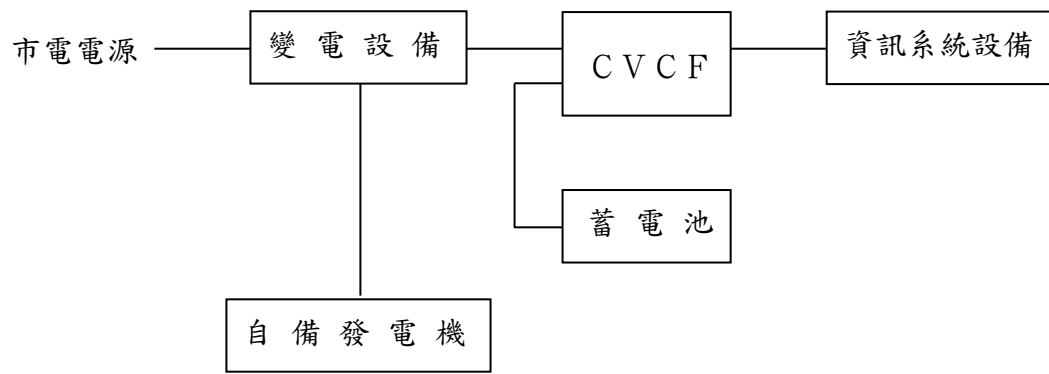


圖 2 C V C F + 蓄電池 + 自備發電機方式之實例

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 64	應設置自備發電機設備及蓄電池設備。
------	-------------------

為能在停電期間，維持資訊系統設備之正常運作，應設置自備發電機設備及蓄電池設備。

- 1、自備發電機設備，在電力公司提供之市電停電時，由柴油引擎或氣體渦輪機等動力推動發電機，自行發電，並於達到必要之電壓時，自動切換供電之電源設備。自備發電機設備之構造、性能等，應於市電停電時，自動啟動發電，確保必要的電壓後，切換並取代市電供電。
- 2、蓄電池設備由蓄電池與充電器組成，當市電停電時，自動切換為由蓄電池供電，並於市電回復正常時，能自動切換回復由市電正常供電的裝置。
- 3、為能使自備發電機設備所供應電力維持一定的電壓及周波數，應設置 CVCF 裝置。有關 CVCF 裝置，請參照【設 63】之說明。
- 4、資訊系統運作所需之照明及空調用電，最好也能由自備發電機供應。
- 5、為能確保在緊急狀況下，自備發電機設備與蓄電池設備能正常動作，應定期維護這些設備。

(1) 自備發電機設備：

- a. 燃料油的容量（運轉可能時間、油料補充程序等之確認等）。
- b. 冷卻水
- c. 運轉動作之確認

(2) 蓄電池設備：

- a. 蓄電池容量
- b. 蓄電池更換時間

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 65	電源設備應設置避雷裝置。
------	--------------

為預防因雷擊造成的災害，電源設備最好能設置避雷裝置。

- 1、因雷擊可能在輸電線之纜線上引發巨大的誘導感應電壓，電源設備之絕緣破壞，造成資訊系統設備之事故，為避免前述事故的發生，最好能在接近電源引入的纜線地方設置避雷裝置。
- 2、避雷裝置的種類有，在高壓電源使用之避雷器、在低壓電源使用之避雷器、保護電源用之保安器及以異常電壓吸收裝置等。

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 66	電源設備應具有耐震措施。
------	--------------

為預防因地震造成電源設備的位移、損傷等，電源設備應具有耐震措施。

- 1、地震發生時，由於電源設備之位移或損傷、配線之短路、切斷等，造成對資訊系統設備之故障，為防止上述事故的發生，電源設備應具有耐震措施。
- 2、電源設備之耐震措施，舉例如下：
 - (1) 加強安裝部位的強度。
 - (2) 配管、配線等應固定於天花板、地板下或牆壁上。
 - (3) 機器之電源連接部應使用防震軟管 (Flexible Pipe)，室內的纜線，應從寬佈設以備有緩衝的空間。
 - (4) 較重的機器設備，應在建築物地板結構體上，加裝耐震制動器，以防止機器設備之位移或翻倒。
 - (5) 較輕的機器，則應固定於地板、牆壁或柱子上。
- 3、蓄電池設備應設置於加強的電池架上，並固定在地板或牆壁上，以防止設備翻倒或損壞。
- 4、為防止地震時電源設備等各機器停止其運作機能，在機器設備之設置條件或運轉條件最好能考慮使用具有耐震設計的物件。

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 67	由配電盤至送至資訊系統設備之電源配線應為專屬專用電纜線。
------	------------------------------

為使資訊系統受到的影響最小，對電腦系統供電之電源纜線，應為專屬專用電纜線。

- 1、當電腦系統以外之機器設備供電之電源配線，因短路、漏電、斷線等事故發生時，為使電腦系統及通訊相關設備所受影響降至最低，由配電盤至電腦系統及通訊設備之電源纜線之配管與配線，應與其它設備之電源線分開配置，即須為專屬專用電纜線。在必要時，不僅對每一臺電腦系統需要獨立的專用線路，對輸出入裝置，亦需依其種類配置獨立的專用電源線。
- 2、由電源室至配電盤的電纜幹線，應為獨立專屬之幹線，同時為防止火災、磁場誘導感應等之影響，施工時，應使用金屬溝、金屬導管或金屬軟管等防護措施。另外，在維護保養時，為對系統之影響降至最低，由電源室至配電盤之幹線，最好配置複數的纜線迴路。
- 3、為了避免配電盤或電腦系統等之配線所產生的磁場，與資訊系統機房內其他設備之配線相互干擾影響，應施以具防磁效應之措施。
- 4、資訊系統設備之配電盤最好為專用設備，應裝置於電腦機房內部，配電盤外露之通電部份，應以鐵板覆蓋並加鎖，以防外部無關人員之碰觸。
- 5、在資訊系統機房使用日光燈、小型吸塵器等電氣機器時，應注意上述機器產生的雜訊(Noise)對電腦系統的影響，在設備維修時使用之電源插座的配線，亦應與電腦系統之配線分別配置。

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 68	應避免與負載變動激烈的機器設備共用電纜線。
------	-----------------------

為能對資訊系統設備供應穩定的電力，資訊系統設備與負載變動激烈的機器設備應分別配置供電之電源纜線。
--

- 1、若資訊系統設備與負載變動激烈的機器設備共用同一供電之電源纜線，有可能無法對資訊系統設備供應穩定的電力，而造成系統之不穩定。故應避免將負載變動激烈的機器設備與資訊系統設備的電源線連接在同一變壓器上。
- 2、此處所謂的負載變動激烈的機器設備，是指如電梯、空調設備等，電源啟動與停止的動作頻率高、消耗電力大的機器設備。

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 69	資訊系統設備之接地線，應為專用之地線。
------	---------------------

為防止電源設備或其他電氣設備等之不良影響，資訊系統設備的接地線，應為專屬專用之接地線。

為防止由電源設備或其他電氣設備等發生之雜訊對資訊系統設備產生不良的影響，如圖 1，資訊系統設備的接地線，應為專用之接地線，直接連結於配電盤上。依電腦系統廠商之設計不同，接地線之連接方式亦不相同，請與電腦廠商協商連接及安裝方式。

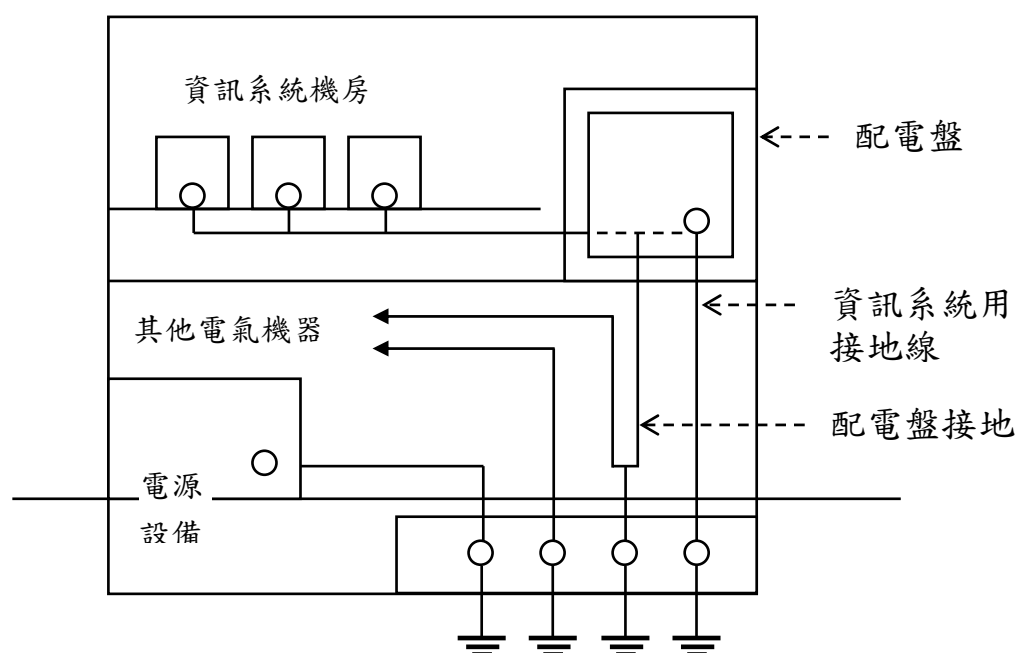


圖1 資訊系統接地線例圖

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 70	應設有預防措施，以避免因過大電流、漏電等事故，造成設備故障。
------	--------------------------------

應設置預防過大電流、漏電等事故之措施，以免造成各類機器設備之故障。

- 1、當資訊系統的迴路發生漏電或短路時，為防止發生觸電、火災等事故，應在配電盤的各迴路，分別安裝漏電斷路器或漏電警報器。惟安裝方式依電腦廠牌的不同而異，因此應與電腦廠商協商安裝的方式。
- 2、當空調設備的迴路發生漏電或短路時，為防止發生觸電、火災等事故，應在配電盤的各迴路，分別安裝漏電斷路器或漏電警報器。
- 3、當資訊系統的低頻濾波器流過容許值以上的透過電流時，可安裝絕緣變壓器，以非接地方式配電，但應與廠商協商後，採取適當的措施。

<p>(參考)</p> <p>低頻濾波器，是為防止因外來之電氣雜訊，造成機器設備異常動作，而安裝於機器設備電源端之裝置。由消除雜訊的立場而言，低頻濾波器的容量最好大一點，但容量大時，因其透過電流量增加，會妨礙真正漏電的檢知，而有發生觸電的危險。</p>
--

電源設備

適用性分類			
中心	總行	合作	直接
◎			

設 71	應設置防災、防犯用備用電源。
------	----------------

為在停電期間，防災、防犯設備能正常運作，應設置防災、防犯用備用電源。

- 1、當地震或火災發生造成市電停止供應時，為能確保工作人員之安全避難及對資訊系統之影響減至最低，防災、防犯設備能正常運作，應設置防災、防犯用備用電源。此處所謂備用電源是指當供應防災、防犯用的市電停止供應時，為確保上述防災、防犯設備能在指定時間內正常運作，所需之電力供應設備，如自備發電機或蓄電池設備等。
- 2、為防止火災時，防災、防犯設備之電源纜線燒斷，應使用耐火、耐熱之電線，或在電源纜線上加裝耐熱保護裝置。

一、資訊中心

（五）空調設備

空調設備應能供給穩定之清淨空氣及適當之溫濕度。

空調設備之一部分機件設備，應安裝於建築物外部，因此應因應來自戶外之雜物侵入及嚴酷氣候條件之對策。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 72	空調設備，應保持充分寬裕之容量。
------	------------------

空調設備，應保持充分寬裕之容量，以能適當調節電腦機房之溫濕度，並維持資訊系統之持續正常運轉。

空調設備，應具有充分寬裕之容量，對於設置於電腦機房內之各類資訊設備，維持適當之溫濕度作業環境，以防止資訊系統發生故障。

為使空調設備具有充分寬裕之容量，適切調整電腦機房之溫濕度，應注意下列各事項：

- (1) 安裝設備時，應考量其耐久性及維修管理之容易性。
- (2) 應檢討建築物結構、機房規模、各室所設置機器設備之發熱量與各室使用目的及使用條件等，估計最大負載熱量來決定空調設備之容量。
一般來說，電腦機房、辦公室、電源室、空調室等，應儘可能分別設定其空調條件。
- (3) 空調設備之機能應具有相當之彈性，以因應電腦機房、辦公室隔間等變更或其他對空調條件之變動。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 73	空調設備，應具有穩定調節空氣之功能。
------	--------------------

空調設備，應具有穩定調節空氣之功能，以維持資訊系統之正常運轉。

- 1、空調設備為防止污氣或塵埃等雜物混入，應在外氣吸入口或外氣與再循環空氣混合處，設置過濾網或集塵器等除塵裝置，採取適當之措施。
- 2、空調設備使用之補給水，應使用具良好水質之用水，並定期檢驗水質，若發現水質惡化時，應加裝適當之水質處理裝置。
- 3、在寒冷地帶或在冬季，為防止冷卻水塔內之循環水凍結，應加裝電力加熱裝置，以便檢知溫度低於預設之溫度時，能自動加溫。若加裝上述加溫裝置，則應具有適當之措施，以防止加熱器加熱時，因水量減少而發生過熱之現象。
- 4、空調設備之外氣吸入口、排氣口、煙囪出煙口、冷卻水塔等位置，應注意其風向等因素，以免進氣、排氣相互短路干擾，以致降低其效能。
- 5、在冬季使用空調設備時，應注意下列事項：
 - (1) 水冷式空調設備，為調節冷卻水水溫，應安裝冷卻水水溫控制裝置。
 - (2) 氣冷式空調設備，為防止因外界低溫，造成效率降低，應安裝風量控制裝置及風壓調整裝置。
- 6、空調設備之排水裝置，宜採用彎曲 U 型管水封，以防止惡臭及污染空氣侵入。其排水作用是利用空調設備與外部之壓力差來進行。為能獲得穩定之空氣調節，排水管內部應平滑，不易沾上污物，並應易於檢修、清潔，其構造宜簡單。
- 7、空調設備之運轉，會伴隨振動，因此各種機器組件、通風導管、配管等，

應視安裝場所之需要，採用防止振動之結構。

- 8、若利用高架地板下吹式空調之電腦機房，其空調氣流迴路，有可能會受電纜線、管線等重疊而受阻，影響調節效率，宜多加注意。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 74	電腦機房之空調設備，應為獨立使用及維修。
------	----------------------

為能確實控制電腦機房之溫濕度，空調設備應避免與其他各室共用。

- 1、電腦機房內之空調設備，應能精確地維持一定之溫度與濕度範圍，以適合電腦設備之運作。因此除了製造熱源之部分外，不可跟辦公室等其他各室共用空調設備。空調設備應為電腦機房獨立使用之設備。如此，維修管理也較容易方便。
- 2、若電腦機房專用之空調設備故障停用，仍有能力將其他各室所使用之空調設備，移作電腦機房使用。
- 3、若萬不得已，機房之空調設備應與其他各室共用時，應考慮並注意下列事項：
 - (1) 共用之空調設備發生故障時，不可影響電腦機房內溫濕度之適切調節功能，應設置備援空調設備。請參照【設 75】。
 - (2) 如與共用空調設備之房間，有通風導管等相連通時，應有防止電腦機房受到延燒之措施。同時，對共用之房間，應施以與電腦機房同一水準之防火措施。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 75	應設置備援之空調設備。
------	-------------

空調設備之主要機器設備，應有備援措施，以備故障時能自動切換運轉。

- 1、空調設備之主要機器設備，應設置多部以為備援。當一部設備發生故障時，能自動切換運轉，以維持電腦機房適切的溫濕度調節。同時，由於設置多部設備，也有可能如【設 72】之說明，有能力讓空調設備具有充分之空調餘力。
- 2、空調設備之主要機器組件，有下列幾項：
 - (1) 熱源裝置 …………… 冷凍壓縮機、鍋爐等
 - (2) 熱交換裝置 …………… 冷卻水塔、空氣調節機（冰水機）
 - (3) 搬運裝置 …………… 抽水機、送風機

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 76	空調設備應安裝自動控制裝置、異常警報裝置等。
------	------------------------

為確保空調設備之正常運轉，除需安裝各種自動控制裝置之外，亦應安裝異常警報裝置，以便能迅速檢知異常狀況，發出警報告知。

- 1、空調設備之自動控制裝置，能夠對溫濕度的變動，作出正確之反應，因此能夠隨時監視室內之溫濕度及空調設備運轉情況，並集中遙控操作，對空調設備作最佳之控制。
- 2、為能自動控制空調設備冷卻水之溫度、壓力及壓縮機冷媒之壓力等，並隨時確認設備運轉狀態，在抽水泵浦、熱源裝置或熱交換裝置之吸入口、吐出口，均須設置壓力計、溫度計等計測裝置。
- 3、空調設備之儲水槽、加濕器、排水接水盤等部分，應安裝異常警報裝置，以防範異常增水或缺水而引起火災、機房漏水等事故。
- 4、自動控制裝置發生故障時，應有適當之措施，能夠由自動控制切換為手動控制，繼續運轉空調設備。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 77	空調設備應具有預防入侵、破壞等措施。
------	--------------------

為確保資訊系統作業不受影響，空調設備應具有預防入侵、破壞等措施。

- 1、安裝在大樓頂樓、建地內部等建築物外部之空調設備，應具有預防閒人入侵、破壞等措施，以免影響資訊系統作業之正常運轉。
- 2、防止外部之入侵、破壞之對策，舉例如下：
 - (1) 到空調設備之通路、門戶等應上鎖，限制非特定人物之進出。
 - (2) 空調設備之周圍，應以鐵絲網等物做柵欄，柵欄進出門口應上鎖。
 - (3) 空調設備之蓋子、維護保養口等處，應上鎖。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 78	空調設備應具有耐震之措施。
------	---------------

為能防止地震引起之位移、損傷等影響，空調設備應具有耐震之措施。

- 1、為使資訊系統作業影響降至最低，空調設備應具有耐震措施，以防止地震造成設備之損壞。
- 2、空調設備之耐震措施，舉例如下：
 - (1) 空調設備應固定於地板、牆壁、天花板等處，以免地震時發生設備之位移、翻倒等情況。
 - (2) 在電腦機房之高架地板上，安裝箱型空調設備時，高架地板應予以加強耐震措施，或固定於建築物或牆壁上（如圖 1）。
 - (3) 安裝在屋頂上之空調設備，應使用防震管接頭、耐震支撐等材料，以提高對地震之抗震能力（如圖 2、3）。
 - (4) 為吸收空調設備之振動而加裝防振裝置時，應另外加裝止動器，以免地震時發生超出平時運轉之振幅而移位（如圖 4、5）。
- 3、配管、通風導管等之耐震措施，舉例如下：
 - (1) 使用能吸收移位變形之接頭，以避免因地震震動與建築物移位等事故所引起之損傷。
 - (2) 沿著牆壁、地板、天花板等安裝之配管、通風導管等，應予適當間隔，施以防止動搖用之耐震支撐裝置（如圖 6）。

空調設備

適用性分類			
中心	總行	合作	直接
◎			

設 79	空調設備隔熱材料、排吸氣口應採用耐火材料。
------	-----------------------

空調設備管道等隔熱材料及排吸氣口應採用耐火材料，以防止火災損害空調設備。

- 1、為防止火災發生時，由隔熱材料或由排吸氣口發生煙霧造成設備損害，空調設備導管等隔熱材料，應使用不會燃燒、不會因火災而發生變形、熔解、龜裂等損害之不燃性材料。
- 2、空調設備之導管需貫穿防火區域時，貫穿部分或其附近應安裝防火擋板。同時，通風導管之排氣口與吸氣口，也要使用不燃性材料。
- 3、空調設備之配管、接頭、閥及伸縮接頭，為防止因受熱變形而產生之壓力變化，或火災損及機器設備，應使用有良好耐火性，且具有充分強度之金屬性材料製品。
- 4、若使用箱型空調設備，風扇、濾網等組件部分，應使用不燃性材料製造或經過防燃處理之製品。

一、資訊中心

（六）監視控制裝置

監視控制裝置，應具有電源、空調、防災、防犯等設備之管理中樞功能，同時具有發生故障之早期發現、通報、復原之功能。

監視控制設備

適用性分類			
中心	總行	合作	直接
◎			

設 80	應安裝監視控制設備。
------	------------

為能及早發現故障之發生，電源、空調、防災、防犯等設備應安裝監視控制設備。

- 1、為使資訊中心複雜之各種設備能順利運轉，並早期發現故障，應於電源、空調、防災、防犯等設備安裝監視控制設備。同時為能將這些監視設備集中在同一個地方操作，最好設置集中監視控制之裝置。
- 2、需要設置監視控制裝置之設備，說明如下：
 - (1) 電源設備：受電變電設備、自備發電設備、蓄電池設備、穩壓定頻率裝置 (CVCF) 等。
 - (2) 空調設備：熱源設備、空調機設備等。
 - (3) 防災設備：自動火警通報設備、瓦斯洩漏警報器、漏電火災警報設備、地震檢知器、緊急狀況通報裝置、緊急廣播裝置、滅火設備、排煙設備、換氣設備、漏水檢知器等。
 - (4) 防犯設備：進出監視設備、防犯管制中心等。
 - (5) 其他：電梯運作設備等。

監視控制設備

適用性分類			
中心	總行	合作	直接
○			

設 81	宜設置中央監控室。
------	-----------

為使電源設備、空調設備、防災設備、防犯設備等能順利運作管理，並有效發揮功能，宜設置中央監控室，將這些設備予以集中監視控管。

- 1、中央監控室為資訊中心平時及緊急狀況時之監控中樞，監控室本身應具有防災措施及進出管理等防犯措施。
- 2、依資訊中心之結構與中央監控室之運用型態，有時會將管理之機能，分為管理電源設備、空調設備等之中央監控室與管理防災設備、防犯設備等防災中心等。最好能配合各單位之特性，選定設置場所，並訂定防災、防犯措施。
- 3、依建築法規，建築物應設置避難樓梯，同時在其大樓之上層樓或下層樓設置中央監控室。依建築法規及消防法規，在中央監控室集中管理之設備，有下列各項：
 - (1) 機械換氣設備。
 - (2) 中央控制之空調設備。
 - (3) 排煙設備。
 - (4) 能向消防機關通報之自動火警報知設備。
 - (5) 裝置自動灑水設備之自動警報。
 - (6) 自動火警報知設備之受訊機。
 - (7) 瓦斯洩漏火警報知設備之受訊機。
 - (8) 漏電火警報知之音響裝置。
 - (9) 緊急警報之廣播擴大器及操作面盤。

有關集中監控之對象設備，請參照 【設 80】 之說明。
- 4、上述設備之設置場所、結構、機能等，應依火災防治條例配合規定辦理。

一、資訊中心

(七) 數據線路相關設備

數據線路相關設備，是指與通訊數據電路之接點，應具有防止非法接觸之措施。

數據線路相關設備

適用性分類			
中心	總行	合作	直接
◎			

設 82	數據線路相關設備，應上鎖。
------	---------------

為防止不正當之觸動、破壞等非法行為，安裝在電腦機房外之數據線路相關設備機架等，應上鎖。

- 1、為防止不正當之觸動、破壞等非法行為，安裝在電腦機房外之 MDF、IDF、數據機等數據線路相關設備，如有被閒人觸動之虞，應上鎖保護。
- 2、安裝在電腦機房內之數據機等數據線路相關設備等，由於電腦機房已有進出管制，故已有與上鎖相同之效果。

數據線路相關設備

適用性分類			
中心	總行	合作	直接
◎			

設 83	數據線路相關設備之安裝場所，不可附加標示。
------	-----------------------

為避免讓外部人員知道數據線路相關設備之安裝場所不可附加標示。

為防止外部閒雜人等破壞設備，並確保資訊通訊網之安全，對於數據線路相關設備等，不可懸掛標示或指示板等，明示設備位置。

數據線路相關設備

適用性分類			
中心	總行	合作	直接
◎			

設 83-1	數據線路相關設備，應備有專用之配線空間。
--------	----------------------

為防護數據線路故障或犯罪之破壞，並為防止其他電源線等雜訊的混入，應備有專用之配線空間。

1、數據線路應備有專用配線空間，舉例如下：

- (1) 區域網路等之通訊線路，宜利用金屬管、金屬導管或配線溝槽佈線。
- (2) 宜導入整合配線系統。

整合配線系統：將原來分別配置之「資訊線路」與「電話線路」等，整合於同一種電纜線（雙絞纜線）上之配線方法。

一般辦公室，多採用「資訊線路、電話線路分配盤」，一元化管理通訊線路。當辦公室之配置變動時，只需將電話機或公用設備，連接到最近之 OA 插座上，再切換線盤端子即可。

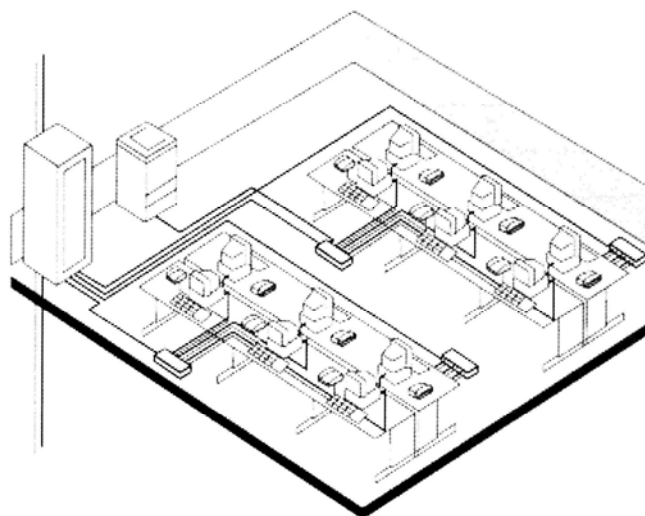


圖 1 整合配線系統之配線例圖

二、總行、營業單位

（一）建築物

總行、營業單位，設置各種端末設備、伺服器、ATM 等自動化服務機器，利用連線通訊網路，與資訊中心連接。為使整體資訊作業穩定運作，總行、營業單位之設備，也應講求安全對策。尤其自動化服務機器設備，在無人化環境（包含設置行外之自動化機器）作業時，應具備適合該環境之防犯、防災措施。

建築物

適用性分類			
中心	總行	合作	直接
	◎		

設 84	建地內之通訊線路、供電纜線等，應具有防止被切斷、延燒之措施。
------	--------------------------------

為防止資訊系統作業之中斷，建地內之通訊線路、供電線纜等，應具有防止被切斷、延燒之措施。

- 1、總行、營業單位建地內鋪設之通訊線路、供電線纜等，為防止因瓦斯、自來水等管線埋設工程、高架配線工程或外部入侵等造成破壞，應有防止被切斷、延燒等措施。
- 2、配設通訊線路、供電線纜等，應事先與電信公司及電力公司協商討論預防切斷、延燒之措施。
- 3、請參照【設 9】之說明。

建築物
結構

適用性分類			
中心	總行	合作	直接
	◎		

設 85	應為耐火之建築物。
------	-----------

為預防火災，建築物應為符合建築法規定之耐火建築物。

- 1、總行、營業單位之建築物結構，由耐火性能與安全性之觀點來看，應為耐火建築物之結構。
- 2、請參照【設 10】之說明。

建築物
結構

適用性分類			
中心	總行	合作	直接
	◎		

設 86	建築物應具有安全性之結構。
------	---------------

為確保建築物應有之安全性結構，建築物應依建築法規之規定建造。

- 1、結構安全，是指建築物對於其本身之重量、承載重量、積雪、風壓等，再加上因地震等震動引起之衝擊，能符合現行之建築法規定結構安全要求。
- 2、現行建築法規時，若現存之建築物發現有無法符合之部分，可引視為不適用該規定。現存總行、營業單位，有結構安全問題時，應考慮配合現行建築法規，以確保結構安全。
- 3、依相關法規之規定，若屬於特定建築物時，應申請耐震診斷測試，必要時應實施耐震補強作業。
- 4、請參照【設 11】之說明。

建築物
結構

適用性分類			
中心	總行	合作	直接
	◎		

設 87	建築物外牆與屋頂應具充分的防水性能。
------	--------------------

為防止漏水發生，應具有充分之防水性能措施。

- 1、外牆、屋頂等因長年使用，其防水、排水性能會下降，若遇到超過排水能力之豪雨或排水口阻塞等情形所引起之漏水，可能造成或電腦系統故障，應有防止漏水之因應措施。
- 2、請參照【設 12】之說明。

建築物
結構

適用性分類			
中心	總行	合作	直接
	◎		

設 88	建築物外牆應確保其強度。
------	--------------

為防禦破壞與入侵，面向公共道路等外牆，應具有足夠之強度。

- 1、面向公共道路之外牆，須具足夠強度，以保護建築物內部之資訊系統相關設備，不受罪犯等破壞。
- 2、可以防禦破壞行為的外牆，有鋼筋混凝土造的外牆、具有相當強度之窗簾式牆壁(Curtain Wall)等。窗簾式牆壁是一種對於建築物無載重功能的薄牆，其材料有金屬板、鋼筋混凝土板等多種，一般都是在工廠依規格生產的牆板。玻璃板則有在厚玻璃板中，夾入格子形狀金屬網之防火、防犯用網狀玻璃。

建築物
門窗

適用性分類			
中心	總行	合作	直接
	◎		

設 89	窗戶應具有防火措施。
------	------------

為防止延燒，有延燒可能性之窗戶，均應具有防火措施。

- 1、對防火建築物或次防火建築物，有延燒之虞之外壁開口部份，應設置防火門窗等防火設備。以防火門窗為例，窗框以不燃性材料之鋼材窗框或鋁製窗框製造，並鑲入夾入網狀玻璃金屬網之厚玻璃。
- 2、請參照【設 14】之說明。

建築物
門窗

適用性分類			
中心	總行	合作	直接
	◎		

設 90	門窗應有防犯措施。
------	-----------

為防止非法入侵，由外部容易接近、入侵之門窗等，應有防犯措施。

- 1、對於容易由外部接近或入侵之一樓等門窗，應有防犯措施，以防止不法入侵。
- 2、門窗之防犯措施有下列數種：
 - (1) 防犯用強化玻璃或夾網玻璃。
 - (2) 可以開關之鐵製方格窗或鐵捲門。
 - (3) 利用感應磁場動作，可以偵測門窗開閉之電磁開關。
 - (4) 可以感應在破壞玻璃時所產生特定高周波振動感應器。
 - (5) 設置於門內外側之紅外線斷電器警報裝置。
 - (6) 防犯攝影機、防犯錄影機。
- 3、請參照【設 15】之說明。

建築物
門窗

適用性分類			
中心	總行	合作	直接
	◎		

設 91	出入口的門，應有足夠之強度，同時應加裝門鎖。
------	------------------------

為防犯、防災，出入口應設置具有足夠強度之門，同時應加裝門鎖。

- 1、除火災等緊急狀況或營業時間外，出入口之門應能緊閉上鎖之防火結構，以防止延燒、不法入侵或被投入危險物品等。
- 2、出入口的門應為具有足夠強度之防火門或具防火規格之鐵捲門。
- 3、門宜考慮設置多重鎖。
- 4、請參照【設 19】之說明。

建築物
門窗

適用性分類			
中心	總行	合作	直接
	◎		

設 92	非營業時間之出入口應設置進入者識別用裝置。
------	-----------------------

為防止非法入侵，營業時間外之出入口應設置如對講機等，能由內部確認對方之識別用裝置。

- 1、為防止外人入侵營業櫃臺內部，破壞端末設備等，在營業時間外需進入室內時，應在門口設置對講機、防犯攝影機或錄影機等確認進入者之識別用裝置。
- 2、非營業時間出入口之管理辦法，舉例如下：
如圖 1，利用設置於非營業時間出入口之對講機及防犯攝影機等，由室內人員確認欲進入者之身分，再由內部開鎖放行。

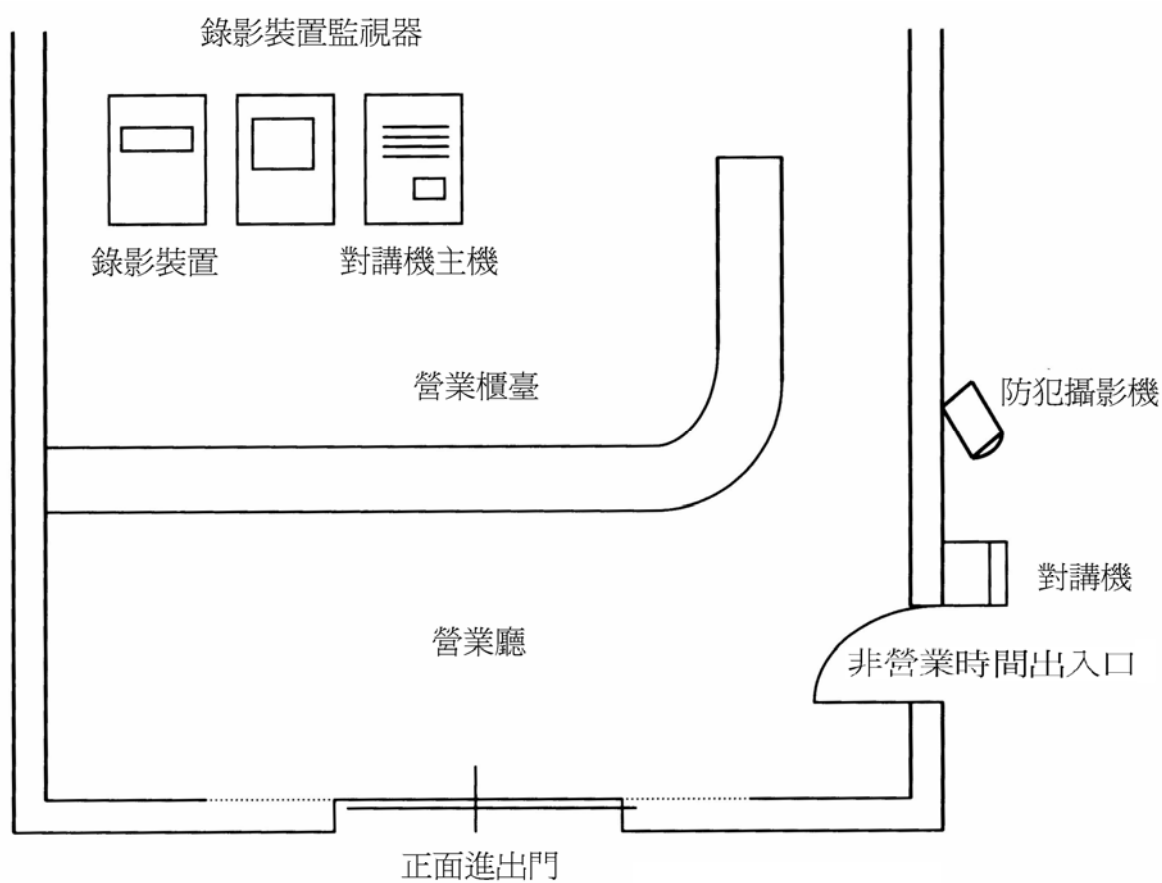


圖 1 非營業時間出入口之識別裝置、防犯設備例圖

建築物
門窗

適用性分類			
中心	總行	合作	直接
	◎		

設 93	進出口應具有防水措施。
------	-------------

為防止雨水等入侵，進出口應具有防水措施。

- 1、為防止雨水入侵，營業櫃臺出入口應具有防水措施，以免端末設備遭受損壞，影響作業。
- 2、為預防伴隨強風之降雨，營業櫃臺出入口應實施防水措施，舉例如下：
 - (1) 強化進出門口、鐵捲門、迴轉門等防水功能。
 - (2) 設置排水溝、防水堤、擋水板及防水門等。
 - (1) 設置防水沙袋。
- 3、有淹水危險性之區域，除上述防水措施之外，應假設營業櫃臺會遭受水患，對於端末設備、重要文件等，事先要有預防浸水之措施。

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
	○		

設 94	天花板及牆壁應具有隔熱、吸音之功能。
------	--------------------

為使端末設備運轉正常，發揮功能，天花板及牆壁應具有隔熱、吸音之功能。

- 1、天花板及牆壁應具有隔熱、吸音之功能，以維持穩定的空氣調節，並吸收端末設備之噪音。
- 2、所謂隔熱功能，是指能防止室內冷暖氣不易散出室外，以維持端末設備必要的作業環境。隔熱材料如：保麗龍發泡保溫板、石板牆保溫板、玻璃纖維保溫板等。
- 3、所謂吸音功能，是指能吸收端末設備所產生的噪音。吸音材料如：玻璃纖維吸音板、石板牆吸音板、吸音甘蔗板等。

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
	◎		

設 95	應具有預防措施，以防止因地震而造成內部裝潢震落或損壞。
------	-----------------------------

天花板、牆壁、照明器具等，應有防止震落或損壞的措施，以免傷及工作人員及端末設備等。

- 1、天花板、隔間分隔壁、照明器具、屏風等，應有防止地震震落或損壞的措施。
- 2、若有設置時鐘、防犯攝影機、公告欄、裝飾品等，應避開工作人員必經的通道或設置端末設備之上方，或是安裝須有足夠的強度，以防止其落下。
- 3、請參照【設 35】之說明。

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
	○		

設 96	地板面應採用不易積存灰塵或產生靜電的材質。
------	-----------------------

地板面應採用不易積存灰塵或產生靜電的材質，以減少端末設備發生故障。

- 1、地板面最好採用不易積存灰塵或產生靜電之塑膠地磚、高壓合板、地毯等材質。
- 2、為防止靜電的產生，可採用添加導電劑之塑膠地磚、高壓合板、防止帶電之地毯等材質。若在地板上塗有防止靜電產生之臘、靜電防止劑時，應注意行走頻度會改變有效期限。
- 3、若需安裝伺服器設備時，請依照【設 33】之準則，施以防止靜電產生措施。

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
	◎		

設 97	端末設備之通訊線路及電源線路，應具有防止被切斷的措施。
------	-----------------------------

端末設備之通訊線路及電源線路，應設置於適當位置，最好地板下有預留管道，若不得已，需經人員通道，應具有防止不易被切斷的措施。

- 1、端末設備之通訊線路或電源線等配線，最好佈設在低架地板下或地板之配線溝等。如使用扁平電纜線，最好能通過地毯底下。
- 2、若不得已，纜線會露出地板面時，須選擇適當位置，才不會因人員走動或物品移動等，造成纜線受損或中斷，最好加裝保護線匣等保護措施為宜。保護線匣，是指能將通訊線路或電源線固定於地板或牆壁，以保護線路之金屬製或塑膠製的角型或半圓型導管（圖 1）。

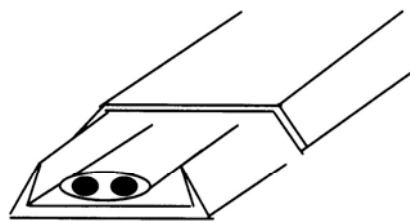


圖 1 保護線夾例圖

建築物
內部裝潢

適用性分類			
中心	總行	合作	直接
	○		

設 98	端末設備之通訊線路、電源線等，應有防止被漏水浸滲的措施。
------	------------------------------

對連接於端末設備之通訊線路、電源纜線等，應有防止被漏水浸滲的措施，以避免因事故引起的漏水，造成設備故障、系統停頓。

- 1、應有防止被漏水浸滲的措施，以免端末設備之通訊線路、電源纜線等發生故障。
- 2、有關防止被漏水浸滲的措施，舉例如下：
 - (1) 對空調設備、飲水機等排水，應有防漏措施，避免流至設有端末設備或管線之場所。
 - (2) 使用地板下之配線溝時，應考慮萬一浸水時之排水方式。
 - (3) 清掃時，應注意端末設備之通訊線路、電源纜線等，勿被水、清潔劑、地板臘等接觸。

建築物
設備

適用性分類			
中心	總行	合作	直接
	◎		

設 99	應安裝自動火災警報及滅火器等設備。
------	-------------------

應安裝煙霧感知器之自動火災警報及滅火器等設備，以便萬一發生火災時，能早期發現、發出警報，以從事初步滅火工作及避難作業。

- 1、當端末設備發生火災時，應使用對端末設備影響最少的二氧化碳滅火器等氣體型滅火器。
- 2、配合滅火對象，應設置乾粉滅火器、泡沫滅火器等設備。為避免緊急時誤用，應在滅火設備之適當位置，貼上對應的「適用火災標示」。

「適用火災標示」有下列三種：

- (1) 適用於 A 火災（一般火災）的標示：圓形標示，白底黑字「普通火災用」。
- (2) 適用於 B 火災（油火災）的標示：圓形標示，黃底黑字「油火災用」。
- (3) 適用於 C 火災（電氣火災）的標示：圓形標示，藍底白字「電氣火災用」。



底色：白



底色：黃



底色：欄

- 3、主要滅火器種類，應貼之「適用火災標示」說明如下：

- (1) 乾粉滅火器

利用高壓粉末噴出滅火之滅火器。依乾粉成分，而有不同之適用，例如僅適用火災 A 或 B 或 C，也有 ABC 三種火災皆適用，或不適用 A 火災之 B C 滅火器。

- (2) 泡沫滅火器

利用高壓泡沫噴出滅火之滅火器。主要適用於B(油)火災，也可用在A(一般)火災，但不適用C(電氣)火災。

(3) 二氧化碳滅火器

利用高壓二氧化碳氣體噴出滅火之滅火器。可適用於B(油)火災及C(電氣)火災。

(4) 海龍化合物滅火器

舊海龍化合物已於 1994 年 1 月 1 日全面停產。

- 4、安裝滅火器時，應注意設置的位置，研究各類滅火器的優缺點，再決定使用何種滅火器及應該安置於何處。
- 5、應於滅火器明顯處標示有效期限並定期檢查效期，若有逾期應即汰換。
- 6、有關自動火災警報設備，請參照【設 37】之說明。

建築物
設備

適用性分類			
中心	總行	合作	直接
	○		

設 100	各類設備宜有耐震措施。
-------	-------------

地震時，所有會影響端末設備之各類雜項設備、物品等，宜有防止掉落、移位或翻倒之耐震措施。

- 1、端末設備、線路設備及週邊的雜項設備、備用物品等，宜有耐震措施，以免其掉落、移位或翻倒，而造成系統服務中斷。
- 2、各類雜項設備、備用物品之耐震措施，舉例如下：
 - (1) 利用 L 型角鋼或錨釘，固定於地板、柱或牆壁上。
 - (2) 不會翻倒的設備或物品，可用 L 型角鋼，防止移位。
 - (3) 附有車輪之椅子或臺車等：
 - a. 以鑰匙或繩索連結固定。
 - b. 安裝制動器或煞車等裝置。
 - (4) 為防止放在桌上的機器、備用物品等掉落，桌面宜設置防落框或固定在桌上。
 - a. 設備或物品宜放置於移位防止框內。
 - b. 以耐震皮帶固定。
 - c. 以黏膠膠帶固定。
- 3、有關端末設備之耐震措施，請參照【設 118】之說明。

建築物
設備

適用性分類			
中心	總行	合作	直接
	◎		

設 101	應安裝耐火金庫或耐火庫房。
-------	---------------

應安裝耐火金庫或整室採用耐火材質之庫房，以備火災發生時，能保護災後系統復原所需要之媒體及資料等，以將災害的影響降至最低程度。

- 1、儘可能安裝整個庫房本身為具耐火結構之耐火庫房。
- 2、金庫或庫房中，應優先考慮存放不易修復或復原因難之媒體及資料。
- 3、依耐火金庫的種類及性能，其耐火時間有所差異，應依保管之內容物品、滅火設備之能力等狀況，選擇不同的耐火金庫。
- 4、磁性媒體對熱、濕度相當敏感，保存管理時，最好能存放磁性媒體專用之耐火金庫內。
- 5、耐火庫房之照明電源配線，應避免貫穿牆壁的直接供電方式，而應採用插電方式，由庫門附近供電，或採用庫門開關方式。
- 6、在租用大樓安裝金庫房時，若不適用混凝土施工法者，應注意金庫房四周牆板裝置之堅固及耐火性，例如可以金庫房常用的特殊鋼板為芯，兩面覆以耐火材質，再以金屬板做表面來裝配。

建築物
設備

適用性分類			
中心	總行	合作	直接
	○		

設 102	應安裝避雷裝置。
-------	----------

較高之建築物或內部電腦、電源設備等應安裝避雷裝置，以防止因雷擊造成資訊系統故障、室內工作人員觸電死傷、引起火災等事故。

- 1、總行、營業單位應視其周圍的情況，就所設置資訊系統設備之重要性，安裝避雷裝置。若是在容易發生雷擊地區，更應預防由電力輸送線路傳導之雷擊，在電腦、電源設備等應設置接地線等避雷措施。
- 2、請參照【設 7、設 65】之說明。

建築物
設備

適用性分類			
中心	總行	合作	直接
	◎		

設 103	應安裝防犯措施。
-------	----------

應安裝防犯攝影機、緊急通報裝置等防犯措施，以防範犯罪於未然。

- 1、應安裝防犯錄影機、防犯攝影機、防犯感應器、緊急呼叫按鈴及可攜式緊急呼叫按鈴等防犯設備，並對犯案情景予以記錄，以為追蹤之有效線索。
- 2、應安裝緊急連線通報裝置至警察局等治安單位，並做定期測試。

建築物
線路相關設備

適用性分類			
中心	總行	合作	直接
	◎		

設 104	不可標示通訊線路相關設備安裝場所。
-------	-------------------

不可標示通訊線路相關設備安裝場所，以防範歹徒。

不可標示 MDF、IDF、數據機等通訊線路相關設備之安裝場所，以免遭受非法存取或破壞，以保護資訊系統設備之安全。

建築物
線路相關設備

適用性分類			
中心	總行	合作	直接
	◎		

設 105	易為外界碰觸之通訊線路相關設備等最好上鎖。
-------	-----------------------

容易被非相關人員接觸之通訊線路等相關設備，最好上鎖，以防誤觸或非法行為。

- 1、通訊線路等相關設備，如安裝在外人易接觸之場所，最好上鎖，以防止不小心或惡意接觸，造成設備故障等事故。
- 2、若通訊線路等相關設備不易上鎖時，應於設備上加裝遮蔽物或移至外人不易接觸的場所。

建築物
線路相關設備

適用性分類			
中心	總行	合作	直接
	○		

設 106	連結端末設備之線路，最好有備援線路。
-------	--------------------

端末設備之線路故障時，為求迅速回復，最好有備援線路。

端末設備之重要線路，最好有備援線路，以便萬一發生線路中斷時，能迅速切換線路，及時回復正常作業。請參照【技 5】之說明。

建築物
電源設備

適用性分類			
中心	總行	合作	直接
	◎		

設 107	應注意電源線之配置，以確保末端設備之正常作業。
-------	-------------------------

為確保末端設備正常作業，電源線應由配電盤直接配置到末端設備上，並避免與其他機器設備共用。

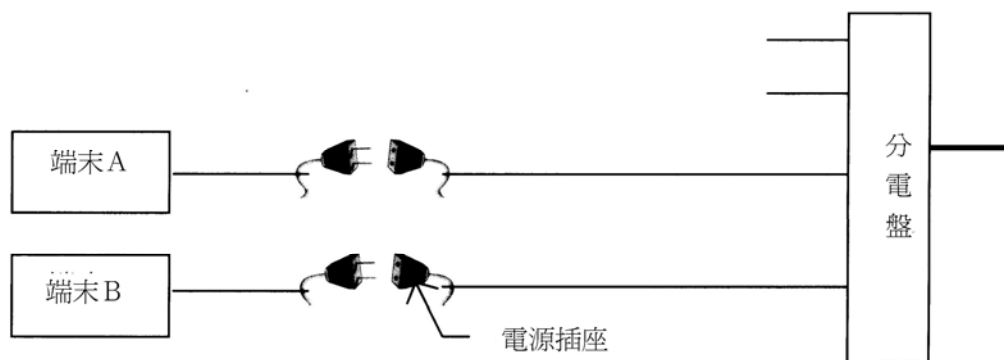
1、電源線的佈設應注意下列事項：

- (1) 電源線應選擇易於維護的路徑佈設。
- (2) 電源線佈設，應對過載或短路有安全保護功能。
- (3) 電源線佈設，應避免鄰近或平行佈設，以免造成雜訊等干擾。

2、避免干擾之電源線佈設方法，舉例如下：

- (1) 直接由分電盤接線到末端設備，如圖 1 之例 1。
- (2) 配線應視所接的末端設備，配予充分之容量。如圖 1 之例 2：a 點之配線容量應考慮末端設備 A 與 B 的容量且配電盤之保險絲容量，應考慮末端機器設備 A 與 B 的容量。

<例 1>



<例 2>

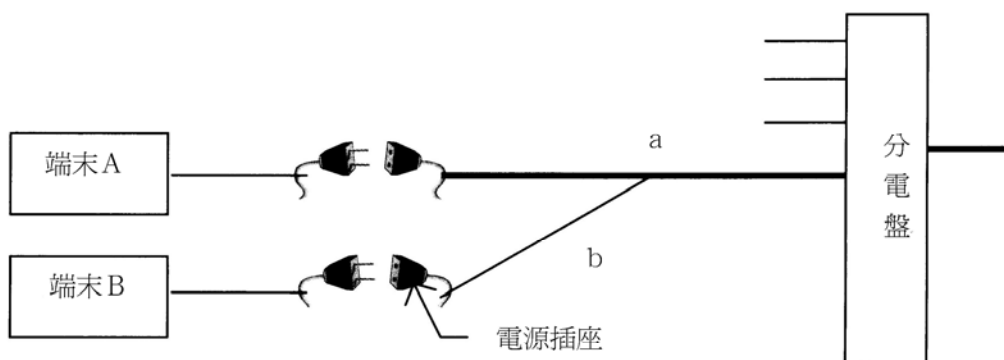


圖 1 電源電纜線佈線例圖

建築物
電源設備

適用性分類			
中心	總行	合作	直接
	◎		

設 108	防災、防犯設備應安裝備用電源。
-------	-----------------

防災、防犯及緊急照明等設備，應安裝備用電源，以備停電時仍能正常運作。

- 1、安裝備用電源，使防災、防犯設備，在發生地震、火災等原因造成停電時，仍能正常運作，讓工作人員能安全避難，且對資訊系統設備之影響降至最低。
- 2、無人銀行自助區之緊急照明裝置，應安裝備用電源，以確保該區之安全。
- 3、請參照【設 71】之說明。

建築物
電源設備

適用性分類			
中心	總行	合作	直接
	○		

設 109	宜安裝自用發電設備。
-------	------------

儘可能安裝自用發電設備，以因應停電時之需，避免作業中斷。

- 1、為防止因長時間停電，造成連線作業之中斷，應儘可能設置自用發電設備。
- 2、如果因營業單位之規模、建築物產權情況等關係，而無法設置固定式發電機時，可採取設置移動電源車或使用小型發電裝置等方法。
- 3、為預防因停電造成資料之損毀，重要伺服器設備等，宜裝設不停電裝置（UPS）。

建築物
空調設備

適用性分類			
中心	總行	合作	直接
	◎		

設 110	應設置空調設備。
-------	----------

為防止溫濕度失調，致使末端設備異常，應配合末端機器的數量，設置適當的空調設備。

- 1、安裝空調設備時，應視末端設備之機種、數量等，來安裝適當的空調設備。
- 2、營業廳的溫濕度，如超過末端設備運轉之容許限度時，末端設備可能會發生異常動作，因此應使用空調設備，使溫濕度不超過末端設備運轉時的容許限度。
- 3、位在日夜溫差極大的之營業單位，應了解劇烈的溫差容易使末端設備內部結露，造成末端設備的故障，故應十分注意空調之設定條件。
- 4、自動化服務區，一般多為與營業廳隔離、分開之獨立房間，該區機器產生之熱氣，也會提升室內的溫度，故應安裝空調設備。

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	◎		

設 111	應安裝直接通話設備。
-------	------------

自動化服務區應裝設電話、對講機等通話裝備，以便在發生故障時與營業廳通話。無人化運作時，應能與中央監控室等單位連線通話。

- 1、應在自動化服務設備附近，顧客容易看到的位置，設置電話、對講機等通話裝置，以便萬一機器故障或顧客有任何疑問時，能讓顧客立即與營業櫃檯或中央監控室之客服人員聯繫或通報。
此處所謂中央監控室，是指集中監控遠端行外自動化服務設備的中心、或委外業者之中央監控室。
- 2、若為完全無人化作業時，與中央監控室之通話裝置是必要的設備。
- 3、在自動化服務區內，自動化服務機器發生故障時之通知連絡方法，應明確標示於指引說明看板上，該看板應黏貼於自動化服務機器附近容易看到的地方。
- 4、請參照【設 117】之說明。

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	◎		

設 112	應安裝緊急通報裝置。
-------	------------

應安裝緊急通報裝置，以便在緊急時，向營業廳或中央監控室等地方通報。

- 1、在營業單位，自動化服務區發生的緊急狀態，應能立即通知營業櫃臺或中央監控室，該緊急通報裝置應設置於靠近自動化服務機器，容易被顧客看到的位置，並清楚標示該設備為「緊急通報裝置」。同時，營業櫃臺亦需裝設能確認緊急通報動作的裝置。
- 2、機器室（機器維護、現金裝填空間）也應裝設緊急通報裝置。該緊急通報裝置應裝設於維修人員容易看到的位置，並清楚標示該設備為「緊急通報裝置」。
- 3、無人化自動化服務區，應裝設能向中央監控室通報緊急狀況的通報裝置。
- 4、自動化服務區，對於發生緊急狀態時之通知連絡方法，應明確標示於指引說明看板上，該看板亦應黏貼於自動化機器附近容易看到的地方。
- 5、應定期檢視緊急通報裝置之有效性。
- 6、請參照【設 117】之說明。

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	◎		

設 113	宜安裝防犯措施。
-------	----------

應配合自動化服務區之機器配置與周圍環境，綜合考慮自動化服務區及該區機器本身之防犯設備，明訂防犯對策。

1、一般自動化服務區多稍離營業櫃臺，因此須有適當的防犯措施。而其防犯措施應作適當組合實施，例如：強化框體直接保護自動化服務機器，以預防不當使用、強盜行為等對端末設備惡意破壞；另外配合加裝防犯錄影機監視自動化服務區，以備萬一發生事故時，其記錄能作為追蹤的線索。

2、自動化服務區之防犯設備，舉例如下：

(1) 防犯攝影機或防犯錄影機：

- 如圖 1，利用防犯錄影機(攝影機)，將出入口、自動化服務區、機械室等之狀況隨時錄影，記錄於錄影裝置。
- 設置靜態影像傳送裝置，利用彩色靜態影像傳送裝置，能監視畫面之細部，具較高的識別能力。
- 能夠監視與錄影，能記錄使用者上半身的影像。當異常情況發生時，最好能自動切換為高解像度模式。考慮使用數位式解像度功能。
- 小型輕量化的攝影機不易發現安置的位置，對防犯效益較高。

(2) 防犯感應器：

- 非營業時間，對自動化服務區、機械室等之進出感應用裝置，紅外線感應器、焦熱電紅外線感應器、玻璃破壞感應器、門戶開關感應器、鐵捲門感應器、熱切割感應器等。
- 對破壞自動化服務設備之感應器，有振動衝擊感應器、熱切割感應器、破門感應器等。

(3) 緊急警報按鈕

應設置在緊急時，能直接將異常現象直接通報保全公司或金融機構中央監控室的通報裝置，最好能具備集音及影像傳送等功能。

設置的位置，應考慮在發生犯罪行為時，最容易通報的位置。

(4) 緊急鈴聲

一按按鈕，警鈴大作，不僅將異常情況告知周圍人員，同時具威嚇犯人的功能。

(5) 安裝多重鎖

機械設備室的進出門，宜安裝多重鎖，以防止非法入侵。

3、自動化機器設備之防犯措施

採用強化框體之自動化服務機器，或安裝自動化服務機器框體強化用品，可防止破壞行為。

4、營業廳外之崗亭 (Booth)

營業廳外設置自動化服務機器之崗亭，有屋外獨立型、鄰接店舖型、屋內獨立型、膠囊 (Capsule) 型等形態。

(1) 在設置營業廳外之崗亭時，應考慮之防犯措施，舉例如下：

- a. 加增防盜鑰匙。
- b. 門鎖前面部分的補強。
- c. 牆壁與門板間以邊條 (Mesh stick) 補強。
- d. 蝴蝶紋鏈部分以凸樺補強。

(2) 營業廳外之崗亭，應設置於重型建設機器不易進入的場所。

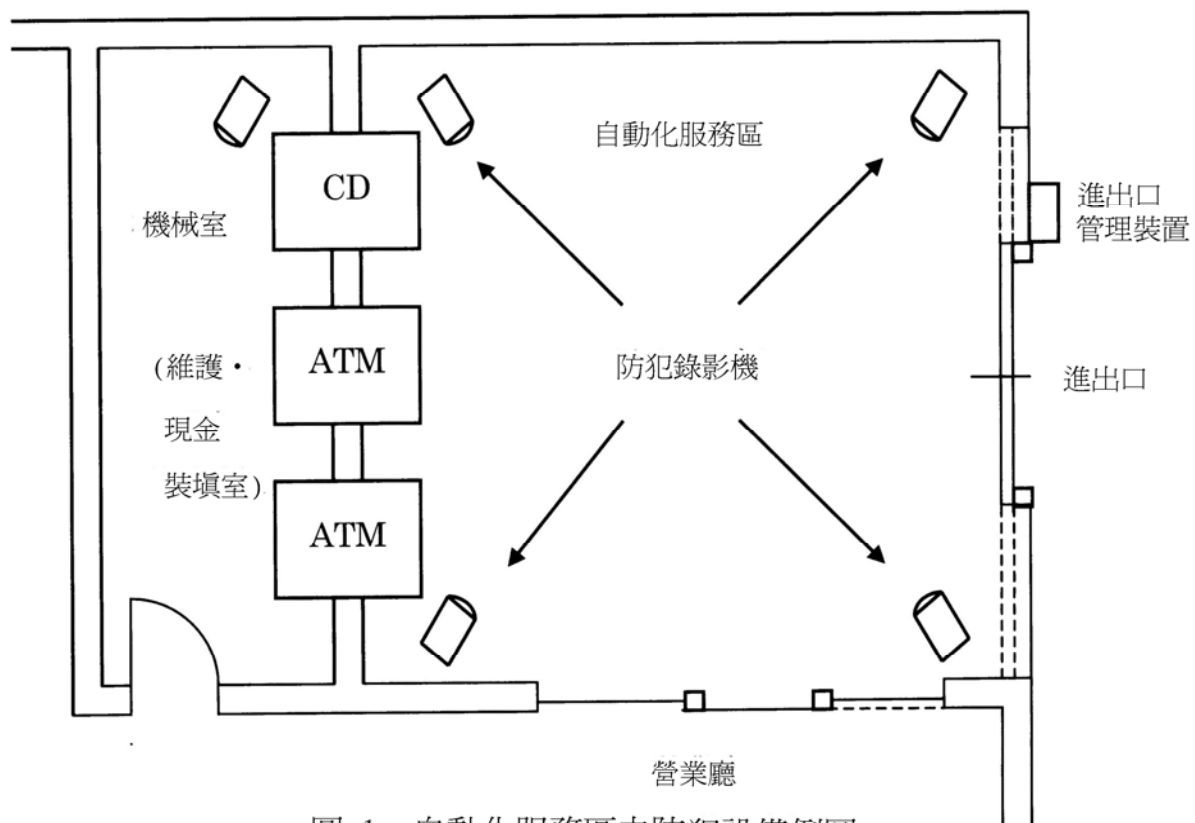


圖 1 自動化服務區之防犯設備例圖

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	◎		

設 114	應設置照明設備及緊急照明設備。
-------	-----------------

應安裝亮度充足的照明設備，以便從室外確認室內的狀況。又為因應停電狀況，儘可能安裝緊急照明設備。

- 1、自動化服務區多半的時間都在無人環境中作業，為對各種犯罪能防範於未然，應設置足夠亮度的照明設備。
- 2、無人運轉的自動化服務區，為在停電時仍能確保其安全，應設置緊急照明設備。
- 3、營業廳外設置自動化服務機器之崗亭，為防範犯罪於未然，應配合周遭環境的情況設置必要的夜間照明裝置。

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	◎		

設 115	自動化服務區的門，應有部分為透明透光者。
-------	----------------------

為防範犯罪於未然，自動化服務區之門，應可由外部看到內部的情況，故門應有部分為透明的。

- 1、自動化服務區之門，除中央部分之外，其上下部分，應透明透光，以便可以由外部看到自動化服務區內部的狀況。
- 2、ATM 等自動化服務機器，宜避免陽光直接照射。

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	○		

設 116	自動化服務機器之裝填現金及設備維護作業應確保必要的空間。
-------	------------------------------

為能安全裝填現金及維護自動化服務機器，應於自動化服務機器後面確保必要的空間。

1、為自動化服務機器之裝填現金及設備維護作業，在自動化服務機器後面應保留作業室的空間。

機械室的架構，請參照【設 113】圖 1 之說明。

2、進出作業室應採取適當的安全措施，舉例如下：

- (1) 窺視用小孔。
- (2) 防犯攝影機或防犯錄影機。
- (3) 防犯感應器。
- (4) 利用鑰匙或密碼等設置門禁安全對策。
- (5) 緊急呼叫按鈕。

3、若無法確保作業室的空間時，則應設置隔間等，防止外部人員進入的措施。

4、自動化機器的現金裝填、維護作業等所需要的空間大小，依不同機種而異，請與機器設備廠商討論之後再作決定。

建築物
自動化服務區

適用性分類			
中心	總行	合作	直接
	○		

設 117	安裝自動運轉設備。
-------	-----------

為能適切的執行無人運作，應設置自動運轉設備。

1、自動運轉設備

此處所謂自動運轉設備，是指依照預設系統運轉的程式或程序，控制自動化服務區內各類裝置的自動啟動、停止等功能，能夠實現上述自動啟動、停止功能的設備如下：

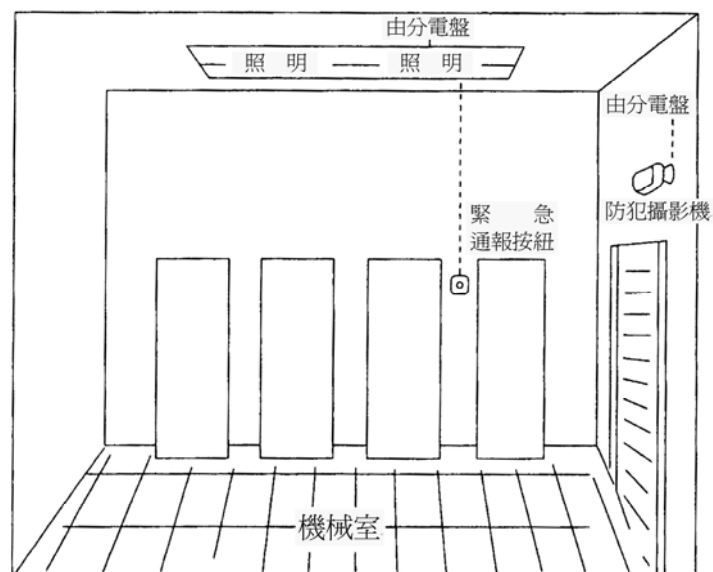
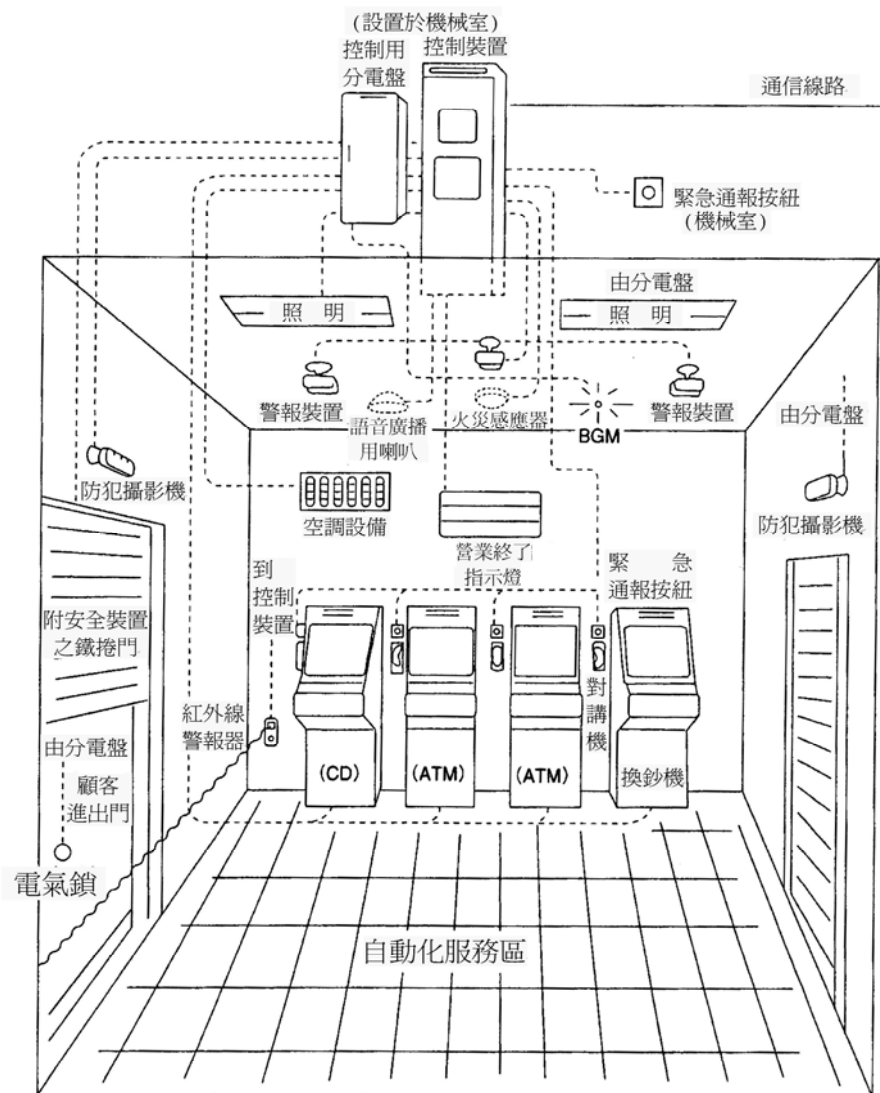
區 分	設備、機器名稱	功 能 等
自動運轉管理	自動運轉設備主機	由年度作業程序部分、程序控制部分、語音產生部分、顯示部分、手動操作部分、電源部分、端子部分、輸出入部分等構成，利用預設程式，執行自動化服務區內部各類設備之自動啟動、停止作業。
與電源設備相關部分	電磁開關控制部分及配電盤	依自動運轉設備的命令，具有執行對各類設備之電源ON/OFF 之功能，以及對其負載控制及確認負載狀態信號之功能。
與通訊設備相關部分	送信機	將自動運轉資訊及其他相關資訊傳送監控中心，同時接收由監控中心送達之控制資料。
	自動撥接通話設備	在營業時間連接到營業櫃臺、營業時間外或無人作業時，則連接到監控中心，作為緊急通話之用，上述通話對象之切換，由自動運轉設備執行。
	靜態畫面電傳裝置	自動化機器的監視。

與防犯相關 連之設備	防犯攝影機、防犯 錄影機	取得自動化服務區內之影像記錄。
	防犯感應器	紅外線感應器、感應墊片、鐵捲門感應器、門開關感應器等。 自動化服務區入侵檢測器、語音指引及防犯錄影機啟動感應裝置等。
	電鎖	自動化服務區進出門之自動開鎖上鎖裝置。 能夠監視開鎖上鎖，由內部可以自由外出。 對已安裝的門口，可用簡易式電鎖。
	鐵捲門安全裝置	自動運轉鐵捲門下降時之安全系統。
	喇叭	發出各類聲音的導引說明。
提供服務的 設備	空調設備	必要時，調和室內的空氣。
	照明設備	必要時，提供室內的照明。
	自動化服務機器	自動化服務機器、數據機等。

2、遠端監視設備

提供無人自動化服務時，為能監視運轉情況，應在監控中心等地，設置遠端監視設備，以對應顧客之呼叫、中心對顧客之連絡、故障時遙控復原等。

【自動運轉設備之設置例圖】



建築物
端末設備

適用性分類			
中心	總行	合作	直接
	○		

設 118	端末設備應設有耐震措施。
-------	--------------

為防止移位、翻倒等造成端末設備之故障或破損，同時能保護工作人員，應具防止移位、翻倒等措施。

防止端末設備之移位、翻倒等措施，舉例如下：

(1) 設置於地板上的機器設備

- a. 使用腳輪固定器、橡膠腳墊、翻倒防止墊等（如圖 1、圖 2、圖 3）。
- b. 固定於建築物的地板（如圖 4）。
- c. 將機器相互聯接並固定。

(機器設備設置於地板上時的固定方式)

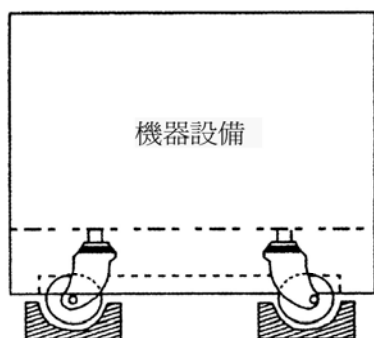


圖 1 腳輪固定器

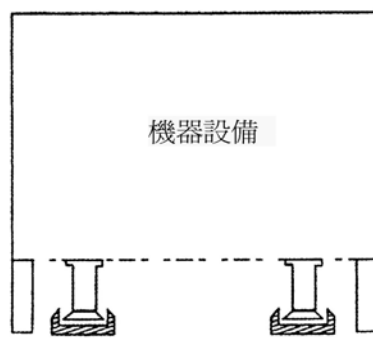


圖 2 橡膠腳墊

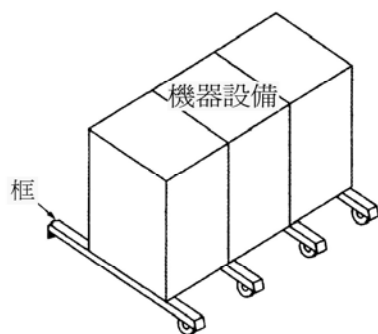


圖 3 翻倒防止框

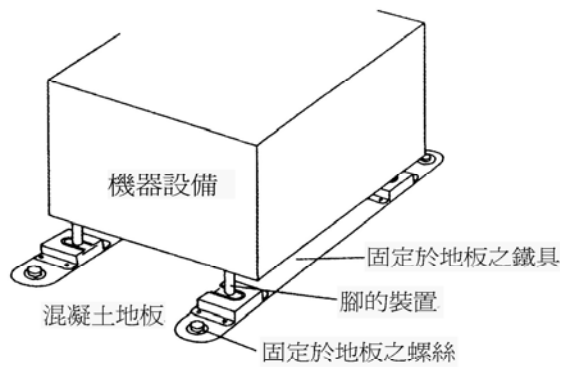


圖 4 固定在地板上之例圖

(2) 設置於桌上的機器設備

- 使用固定鐵器，將機器設備固定於桌上。
- 利用橡膠腳墊，將機器設備固定於桌上。
- 加裝防止桌上機器設備移位掉落之制動器 (Stopper)。

(機器設備設置於桌上時的固定方式)

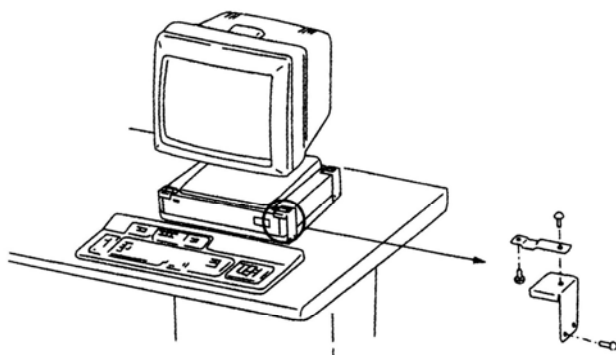


圖 5 固定鐵器之例圖

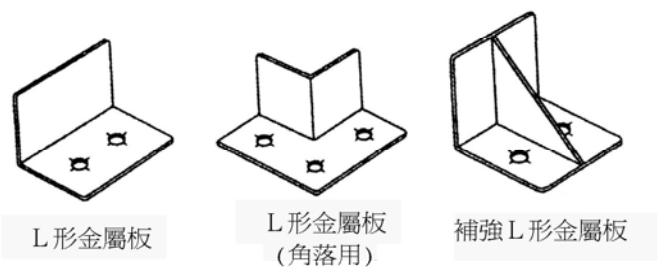


圖 6 防止移位型制動器圖例

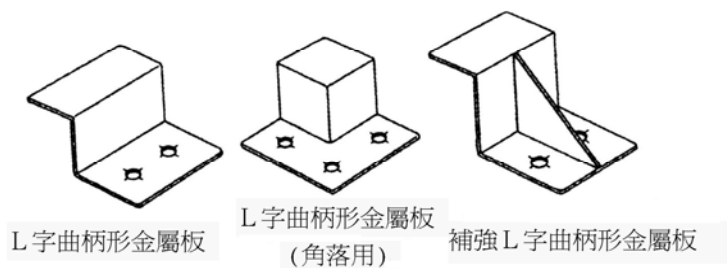


圖 7 防止移位・翻倒型制動器圖例

建築物
端末設備

適用性分類			
中心	總行	合作	直接
	◎		

設 119	機器設備之地線，應確實安裝。
-------	----------------

為保護機器設備之安全，對需要安裝地線的設備，應確實安裝地線，並拉至配電盤上。

- 1、對於設備安裝說明書上要求應安裝地線之端末設備等，應確實安裝地線。若未接上地線，在如空調設備等用電量大的設備啟動時，容易造成端末設備之 IC 晶片受損或保存的資料遭到破壞等。
- 2、接地線的連接方式，最好使用附加接地線之電源插座或電源延長接線。在新佈設電源線時，應要求附加接地線。附加接地線之插座，如圖 1 所示。



圖 1 附接地線之插座例圖

建築物
端末設備

適用性分類			
中心	總行	合作	直接
	○		

設 120	端末設備應有保護措施，不受漏水或塵埃的侵害。
-------	------------------------

為避免受到漏水或塵埃的侵害，端末設備應備有防水、防塵套等必要的措施。

- 1、 為防止端末設備受漏水、塵埃或煙霧的影響而損壞，端末設備在停止運轉時，應使用防水、防塵套，並在必要時，備有空調設備。
- 2、 保護端末設備，不受漏水、煙霧等損害，應嚴禁在機器四周抽煙或飲食等，並訂定使用機器設備的規則等，並確實執行。

二、總行、營業單位

（二）伺服器（Server）安裝場所

安裝於資訊中心機房以外（總行、營業單位）之資訊系統設備，多採用伺服器為主的系統架構，但其使用的形態及服務的內涵，依各金融機構有很大的差異。

本大項中，依各金融機構設置伺服器時，在安全措施上應注意的事項，分成小項目，分別說明。至於是否實施，由各金融機構依其資訊系統作業所提供之功能、需要保護的資料及連線服務持續之重要性等因素，自行判斷決定。

伺服器安裝場所
位置

適用性分類			
中心	總行	合作	直接
	○		

設 121	伺服器設備應設置於較不易受到災害的位置。
-------	----------------------

為防止資訊系統受到影響，其設備應設置於不易受到地震、火災、水災等災害影響的位置。

- 1、在建築物內，設置伺服器的位置，應安置於不易受到地震、火災、水災等災害影響的位置，以防止資訊系統受到影響，造成作業停頓。
若不得已應安置於容易受到災害的位置時，應考慮預防各種災害的對策。
- 2、在建築物內，不易受到災害的位置，請參照【設 22】之說明。

伺服器安裝場所
位置

適用性分類			
中心	總行	合作	直接
	○		

設 122	伺服器設備應設置於不易由外部進入的位置。
-------	----------------------

為防止入侵、破壞、資料外洩等，伺服器設備設置位置應避免接近進出門口、電梯、樓梯等之位置。

- 1、設置伺服器的位置，為防止入侵、破壞、資料外洩等，應避免接近進出門口、電梯、樓梯等容易直接進入的位置，應設置於不易由外部進入的位置。
- 2、若不得已應安置於容易進入之進出門口、電梯、樓梯等附近位置時，請參照【設 23】之說明，設置預防措施。

伺服器安裝場所
位置

適用性分類			
中心	總行	合作	直接
	○		

設 123	設置伺服器設備的位置，不得張貼具室名等標示之招牌。
-------	---------------------------

為防止入侵、破壞、資料外洩等，設置伺服器設備的位置，不應張貼具室名等標示之招牌。

- 1、在總行、營業單位等建築物內，為防止入侵、破壞、資料外洩等，設置伺服器設備的位置，不應張貼具室名等標示之招牌。
- 2、為能對消防人員明示伺服器設備的位置，應將房間的相關位置圖，設置於建築物內部，不易由外部看到的地方。

伺服器安裝場所
位置

適用性分類			
中心	總行	合作	直接
	○		

設 124	設置伺服器設備的位置，應為專用之隔間。
-------	---------------------

為徹底執行安全管理，設置伺服器設備的位置，應為專用之隔間。

- 1、須將安裝伺服器的場所，分隔為專用隔間的原因，請參照【設 26】之說明。
- 2、若不得已，應將伺服器安裝於與其他場所公用的地方，可以參考下列實例：
 - (1) 利用隔間屏風，分隔區域。
 - (2) 在出入口處加鎖。
 - (3) 在伺服器本身加鎖。

伺服器安裝場所
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
	○		

設 125	應設置於具防火能力之隔間內。
-------	----------------

為防止因建築物其他地區所發生的火災引起的延燒，設備應依照國內建築技術規則規定設置於防火隔間內，並與其他各室分隔；資料保管室未用防火隔間時，應使用耐火金庫。

為使安裝伺服器的場所，在建築物內其他地區發生火災時，受到的影響降至最低，應將設備安裝於依建築技術規則規定，具防火能力之隔間內。

伺服器安裝場所
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
	○		

設 126	應具防止漏水的對策。
-------	------------

為防止因漏水造成伺服器的損壞，應具備預防天花板、牆壁、地板等地方發生漏水時之因應對策。

- 1、安裝伺服器的場所，應設置於具防止漏水措施的場所，漏水防止措施請參照【設 32】之說明。
- 2、連接於伺服器之通訊線路、電源纜線等，亦應具防止漏水之措施，請參照【設 98】之說明。

伺服器安裝場所
結構、內部裝潢

適用性分類			
中心	總行	合作	直接
	○		

設 127	高架地板應具有耐震之措施。
-------	---------------

為避免高架地板板面在地震時受到損壞，高架地板應具有耐震之措施。

設置伺服器設備之場所，若使用高架地板時，應依照【設 36】之說明，具有耐震之措施。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	○		

設 128	應具有滅火設備。
-------	----------

為避免因火災造成伺服器的損壞，應設置必要的滅火設備。

- 1、設置伺服器的場所，多集中放置機器設備，且通常都在無人的情況下作業，應特別留意火災的發生。尤其在選擇滅火器時，應由對電腦設備之污損及安全性的觀點考量選擇。
- 2、設置於伺服器設備安裝場所之滅火設備，舉例說明如下：

具體實施之措施需依伺服器設備之重要性，將這些設備作適當的組合運用，以達最適宜的效果。

 - (1) 自動火災警報設備
請參照【設 37、設 99】之說明。
 - (2) 緊急連絡裝置
請參照【設 38】之說明。
 - (3) 滅火設備
請參照【設 39、設 99】之說明。
 - (4) 電纜線等之耐燃性、延燒防止對策
請參照【設 40】之說明。
 - (5) 其他（攜帶用照明設備、排煙設備等設置）
請參照【設 41、設 42】之說明。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	○		

設 129	宜設置地震感應器。
-------	-----------

安裝伺服器的場所，宜設置地震感應器的裝置，以作為伺服器是否繼續作業之判斷依據。

- 1、為防止因地震引起之資料損毀或電氣火災等二次災害，安裝伺服器的場所，宜設置地震感應器，以作為伺服器是否繼續作業之判斷依據。
地震感應器，需配合所安裝伺服器的重要性、數量、設置狀況等，裝設必要功能與數量之感應器。
- 2、關於地震感應器應注意事項，請參照【設 44】之說明。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	○		

設 130	在設置伺服器的房間進出，應設置進出管理設備、防犯設備等。
-------	------------------------------

為防止非法入侵，在設置伺服器設備的房間進出門，應設置進出管理設備、防犯設備等。

有關進出管理設備、防犯設備等，請參照【設 45】之說明。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	○		

設 131	應設置溫濕度自動記錄裝置或溫濕度警報裝置等。
-------	------------------------

為預防電腦系統的故障，維持正常運轉，同時在發生故障時，能分析故障原因，應設置溫濕度自動記錄裝置或溫濕度警報裝置等。

- 1、溫濕度自動紀錄裝置，是自動測量及紀錄電腦機房、資料保管室之溫溼度裝置。溫溼度警報裝置是房內溫濕度超過原來所設定範圍時，會發出警報以引起注意，並儘速採取適當處理之裝置。與溫濕度自動控制裝置連動的溫濕度自動紀錄裝置，可以保持電腦房、資料保管室之溫濕度在規定的範圍內，也可以提供資料以分析故障原因。
- 2、設置溫濕度自動記錄裝置或溫濕度警報裝置等設備時，位置最好避開下列溫濕度變化大的場所，如電腦設備之排氣口、空調設備之冷氣吹出口等直接受風的位置或房間之進出門口附近等。
另外，在設置溫濕度自動記錄裝置或溫濕度警報裝置時，應配合伺服器的重要性、設置的數量、安裝情況等作適當的配置。
- 3、請參照【設 46】之說明。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	○		

設 132	應設置空調設備。
-------	----------

為確保電腦機房適切的溫濕度，應設置專屬的空調設備。

- 1、應設置專屬的空調設備，同時為能確保穩定的空調效果，應確保機房的溫濕度，能適合伺服器的正常運轉條件，若必須安裝專屬空調設備時，應確保穩定的電源供應。
- 2、關於空調設備的安裝，請參照【設 72 ～ 設 79】之說明。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	○		

設 133	應有防止鼠害的措施。
-------	------------

為能防止因鼠害造成電纜線之破損，應有適當的防範措施。

- 1、老鼠的入侵、築巢，容易造成通訊線路、電源纜線等漏電、接觸不良、腐蝕、斷線等，引起電腦系統的故障。為避免上述故障的發生，通訊線路、電源纜線等，應有防止鼠害的措施。
- 2、若在大樓內有廚房、飲食商店等老鼠適於棲身的場所時，容易發生因老鼠引起的災害，應在設備面考慮將食品完全收藏、廚餘殘渣等完全處理的能力。
- 3、防止鼠害的措施實例，請參照【設 47】之說明。

伺服器安裝場所
設備

適用性分類			
中心	總行	合作	直接
	◎		

設 134	應有防止電源插頭由插座鬆落的措施。
-------	-------------------

為防止電源插頭輕易的鬆脫，電源插座應有防止脫落的措施。

- 1、伺服器系統及週邊機器設備之電力，若由電源插座供應時，由於不注意，可能造成電源插頭由插座鬆落的情況發生，應有防止脫落的措施。
- 2、加設防止鬆脫的電源插座，舉例如下：
 - (1) 防止脫落的插座。
 - (2) 附掛勾的插座。

二、總行、營業單位

（三）行外收付處

行外收付處可能會利用駐外營業場所既有的設備，營業時間可能與駐外地點商店的營業時間不同，或與總行、營業單位等營業時間不同。因此其設備應加強防犯措施，防止破壞、入侵情況發生。

行外收付處

適用性分類			
中心	總行	合作	直接
	◎		

設 135	應有防止由其他區域入侵的措施。
-------	-----------------

為防止入侵、破壞的情況發生，行外收付處之作業區域，應與其他商店區域劃分為獨立的防犯區域。

- 1、行外收付處的作業區域，應與商店其他區域分隔為獨立區域。防止由商店內其他區域入侵的因應對策，舉例如下：
 - (1) 利用鐵捲門隔離。
 - (2) 利用防犯感應器檢測，請參照【設 113】。
 - (3) 利用防犯攝影機或防犯錄影機監視，請參照【設 113】。
- 2、行外收付處所在地之商店或商店內之其他承租者，其營業日或營業時間可能互不相同。若在商店內其他區域之營業時間內，銀行駐外據點沒有營業時，在考慮商店整體視覺觀感下，應採用網狀鐵捲門等防犯措施。
- 3、行外收付處之現金、傳票帳冊等保管方法之訂定，應考慮該營業場所係，不特定多數閒雜人物進出場所。

行外收付處

適用性分類			
中心	總行	合作	直接
	◎		

設 136	配合使用商店設備之狀況，應有適當的補強對策。
-------	------------------------

為防止入侵、破壞的情況發生，若行外收付處之商店既有設施與金融機構的要求不符時，在設備補強及作業應用面，應有適當的因應對策。

- 1、商店既有的設施與金融機構要求的基準不符時，在設備補強及作業應用面，應有適當的因應對策。
- 2、依行外收付處所在商店既有設備的狀況，在設備面的因應對策，舉例如下：
 - (1) 若側壁與天花板之間有空隙未連接時，處理現金或傳票帳冊的辦公場所，應設置網狀天花板。
 - (2) 若側壁之強度不足，應加以補強。
- 3、依照行外收付處所在之商店狀況，應於應用面上加以檢討的對策，舉例如下：
 - (1) 增設防犯感應器，補強側壁等防止入侵的對策，請參照【設 113】。
 - (2) 實施利用防犯攝影機、防犯錄影機之監視作業，請參照【設 113】。

三、 與流通業、零售店之合作通路

(一) 便利超商之 ATM

安裝於便利超商之 ATM，與設置於自動化服務區的 ATM 不同，便利超商係多數不特定的人物進出往來的場所，亦未設置自動化服務區域或機械室等，多僅單獨設置自動化服務的機器設備。因此，與設置於總行、營業單位自動化服務區之 ATM 設備比較，應有較強化之防犯對策。

便利超商之 ATM

適用性分類			
中心	總行	合作	直接
		◎	

設 137	應有防犯措施。
-------	---------

為確保設置於便利超商 ATM 之安全，應配合設置形態、週邊環境，對防犯設備及ATM 本身之防犯措施，作一適切的組合，建立必要的防犯對策。

- 1、相較原設置於總行、營業單位等自動化服務區之 ATM，應有強化之防犯對策。
- 2、在便利超商使用 ATM 時，應考慮由背後或周圍窺視金融卡密碼的因應對策。
- 3、在便利超商使用 ATM 時，由背後或周圍窺視金融卡密碼之因應對策舉例如下：
 - (1) 在便利超商設置 ATM 的場所，應避免靠近銷售雜誌等客人會久留的場所。
 - (2) 在便利超商設置 ATM 的場所，若必須靠近銷售雜誌等客人久留的場所時，應設置防窺視的裝置。
- 4、在便利超商使用 ATM 時，預防由背後或周圍窺視金融卡密碼之設備舉例如下：
 - (1) 利用隔間屏風，分隔區域。
 - (2) ATM 顯示螢幕（螢幕顯示的視角限制、畫面顯示的角度、字型的大小及顯示的內容等）。
 - (3) 輸入操作之隱密裝置。
- 5、在便利超商的 ATM，其防犯設備舉例如下：
 - (1) 防犯攝影機及防犯錄影機

能夠監視與錄影，最少應能攝錄使用者之上半身影像。當異常情況發

生時，應能隨同警報，自動將攝錄功能切換為高解析度模式。

(2) 緊急呼叫按鈕

應設置於緊急時能夠直接向保全公司或金融機構之監控中心通知緊急狀況的裝置。設置位置，應考慮在客戶使用中發生緊急犯罪情況下，容易通報之位置與高度。

客戶在使用中可能發生的犯罪行為如下：

- a. 由後方攻擊。
- b. 由旁邊搶奪現金。
- c. 利用催淚噴霧劑等各類兇器。

(3) 緊急鈴聲

應裝置警鈴，當按下緊急呼叫按鈕，讓警鈴大鳴，不僅能對周圍的人通報異常情況的發生，同時可以威嚇犯人。

(4) 防犯感應器

檢知安裝於便利超商之 ATM 是否被破壞，有衝擊感應器、燒切感應器、破門感應器等不同之感應設備。

(5) 集音麥克風

利用集音麥克風，掌握現場的狀況。

6、在便利超商的 ATM，本身之防犯措施舉例如下：

(1) 本身的強度

- a. 對利用手工具之破壞行為，其強度應能承受 25 分鐘以上的破壞 (Level 3)。
- b. 利用安裝框體強化裝置等，增強其強度。

(2) 本身的固定

- a. 將機體本身以螺絲固定於地板或牆壁上。
- b. 應能感知機體溫度之異常、機身之傾斜、振動等，並向保全公司或金融機構監控中心發出警報。
- c. 將便利超商的 ATM 收藏於保護用框體中，使機器本身不易被移動。

(3) 電源纜線及通訊線路

- a. 前述配線應無法由外部查覺。

b. 前述配線若能由外部看到時，應加強保護，防止其被切斷。

7、對於偽造的紙幣，亦應有適當的因應對策。例如，在交易取消前投入之現金，能將原紙鈔退還客戶等。

營 運 基 準

營運基準之概要

- 1、營運基準是針對「資訊中心」、「總行、營業單位」、「流通業、零售業等合作通路」及「電子銀行、開放網路管道」等，在電腦資料處理之安全控管方針、組織、責任制度、確認程序等，整理出來之基準。因各金融機構在組織結構上之不同，可能有不符實際需求之處，因此各機構應宜依本基準及各機構之實際狀況，整理出具有實效性之基準規定。另外，為能客觀評估分析安全對策之實施狀況，提升其時效性，應建置系統稽核制度。
 - 2、營運基準之項目，由資訊安全管理之程序規定、責任體制等之整理、遵守情況之確認、防災、防犯、業務組織之整編、規定之整理、進出門禁管制、資訊系統相關設備之營運管理、系統開發、變更相關之許可／確認程序、各種設備之管理、對整體營運所需之教育訓練、人員管理、委外管理、系統稽核、利用塑膠卡片及開放網路金融服務、行外收付處及安裝於便利超商之ATM 等構成。資訊系統相關機器設備之運作管理，由手冊之整理、使用權限之管理、操作管理、資料輸入管理、資料檔案管理、程式檔案管理、電腦病毒對策、網路參數設定管理、文件管理、傳票帳冊管理、資料輸出管理、交易資料管理、金鑰管理、嚴謹實施身分確認、卡片管理、客戶資料保護、資源管理、對外連結之管理、機器設備之管理、運轉監視、資訊系統機房、資料儲存室之管理、故障、災害發生時之對策、災變備援計畫之策劃等之項目。
- 另外，在總行、營業單位特有之項目，如 ATM 等無人化服務區之管理、駐外據點之端末系統管理等。
- 同時，在發生故障或災害時，其對安全控管之要求，與平時作業時之要求，宜維持完全相同之層次。

(一)確立管理體制

1、資訊安全管理與責任之明確化

設置於電腦機房中央集權型之主機系統，其存放系統內之資料，基於主要建築物之結構及進出機房管理等物理上之安全對策，已有必要之最低要求保護機能。但利用主從架構之系統（Client/Server System）或連結在網際網路之系統，在資料處理環境與作業目標，有多種型態，依過去之物理性安全對策，並不足以保護系統。資料之保護，不僅需要使用者具備安控管理之意識，同時對於資訊保護不是依賴使用者個人之裁量判斷，而應為整個機構安控理念之統一所制定之資訊安全政策。

本基準所謂資訊安全政策，是指機構（或是組織）為適切的保護其資訊資產，在機構內部整合之基本方針。在此，應明確化之內容，是指必須要保護之重要資訊資產到底是什麼，為什麼需要保護這些資訊，對這些資訊之保護責任又如何等內容。為能適當的實施安控管理，應先行訂定包含：資訊安全政策（基本方針）、資訊安全管理之標準（機構本身訂定之安控對策基準）、手冊或程序說明書等說明安控管理具體方法之相關文件，確實實施資訊系統之安控對策。

確立管理體制
資訊安全管理及責任之明確化

適用性分類				
共通	中心	總行	合作	直接
◎				

運 1	應編製資訊安全管理辦法相關文件。
-----	------------------

為能適切執行安控管理，應事先編製文件，明確記載安控管理之具體程序、責任劃分等。

1、為能適切的執行安控管理，保護機構（或組織）之資訊資產之「資訊安全政策（基本方針）」、說明推行資訊安全政策具體對策之「資訊安全管理標準（機構內部安控對策基準）」及「執行手冊」或「作業程序」等與安控管理相關文件，都應事先整理編製。安控管理相關連之文件，分類如下：

(1) 資訊安全政策（基本方針）：

全機構統一之基本方針，訂定需要保護之資訊資產、保護之理由及責任劃分等。

(2) 資訊安全管理標準（機構內部安控對策基準）：

為確實執行「資訊安全政策（基本方針）」之具體對策，依機構內之部門別分別編製。

(3) 執行手冊或作業程序：

將資訊安全政策（基本方針）及資訊安全管理標準（機構內部安控對策基準）之內容，具體反應於業務處理之程序文件，也可以依機構內部部門別或依系統別分別編製。

請注意，對全機構（或全組織）安控管理之方針或對策有重大影響之安控管理相關文件之策劃、編製，應獲得經營階層認可。

2、安控相關文件，應對全體職員（包含駐外人員），依其在組織內對資訊安全政策之職掌與責任，作一適當告知及教育。有關安控教育，請參照【運 80】說明。

3、在「資訊安全政策」文件內，應訂定之重要事項如下：

- (1) 應保護之資訊資產。
- (2) 需要保護之理由。
- (3) 保護資訊資產之責任歸屬。

4、在編製整理安控相關文件時，應留意事項如下：

- (1) 安控管理實施計畫之訂定，應先判斷資訊系統所處理資訊之重要性，決定資訊系統所提供服務之優先順序。因此應先整理出目前處理之所有資訊型態，決定在機構（或組織）內資訊保護層級。
對於重要之資訊資產，應由資訊安全政策之原則、機密性、完整性、可用性觀點，依其重要性，實施適切之保護及管理。
另外，為確保安控所需手段，儘可能檢討是否適用投保方式。
- (2) 在新安裝或更新機器設備、軟體時，應確認其安控管理機能是否符合機構之資訊安全政策。
- (3) 為確保能達成安控管理要求，在系統規劃階段就需考慮是否能符合安控對策之要求。有關係統規劃時，應考慮之安控對策，請參照【技 8】說明。
- (4) 為能適切地實施安控管理，有關安控之法規亦需列入考慮。
- (5) 在制定資訊安全政策時，應掌握機構內各部門之意見、狀況，適切地反映在政策內。

- (註)・機密性 (Confidentiality) … 不允許無權限之人員，擷取相關資訊。
- ・完整性 (Integrity) … 保持資訊之完整，不允許被篡改。
 - ・可用性 (Availability) … 隨時保持可以使用之狀態。

確立管理體制
資訊安全管理及責任的明確化

適用性分類				
共通	中心	總行	合作	直接
◎				

運 2	具體實施資訊安全管理標準之文件，應進行評估及修訂作業。
-----	-----------------------------

為能建置最適切的資訊安全管理標準，編製完成的文件，應定期評估及檢討，對現行業務的狀況是否相宜，必要時應予以修訂。

1、為能適切實施安控管理，具體訂定管理作業辦法之資訊安全相關文件，應符合現行業務執行狀況。當有下列情況發生時，應重新檢討文件內容，必要時需修改其內容。

當資訊安全管理相關文件之修訂，足以影響整個機構（或全組織）之資訊安全管理方針或政策時，應事先獲得經營階層認可。

- (1) 組織之營運改變時。
- (2) 業務環境之變更。
- (3) 法令規章之制定、修訂。
- (4) 資訊與通訊技術之進步。
- (5) 業務組織及人員、就業環境之改變。
- (6) 所處理之資訊改變。
- (7) 有關資訊安全之事故或犯罪事件發生。
- (8) 資訊安全管理相關文件所訂定之規範遵行情況之檢查結果。

在此應注意，主管單位所修訂之規範，應對全機構公告，讓每一職員都能瞭解規範內容。

2、一般需要檢討修訂之文件如下，但於必要的情況下，資訊安全管理基礎之資訊安全政策（基本方針）亦有重新檢討之可能。

- (1) 安控標準（機構內部安控對策基準）。
- (2) 執行手冊或作業程序。

3、具有不同資訊安全政策之多個企業合併為一個企業時，在作系統整合之前，

應先確認與檢討所合併金融機構間，對資訊安全政策之差異點。

確立管理體制
資訊安全管理及責任的明確化

適用性分類				
共通	中心	總行	合作	直接
◎				

運 3	建立 資訊安全管理體制。
-----	---------------------

為能適切實施資訊安全管理，應指定資訊安全管理負責人，明確訂定其職務範圍、權限及應負之責任。

1、為確保全機構之資訊安全是否依照既定之方針、基準、指標或程序執行，應先確立適當之管理體制（組織、職責範圍、權限等）。

同時，應指定負責全機構資訊安全事宜之總負責人，以同一標準實施資訊安全管理。

對上述管理體制之確立，應獲得經營階層之認可。

2、在負責全機構資訊安全事宜之總負責人之下，依組織規模及體制，指定資訊安全管理人員前，應事先訂定資訊安全管理之整體體制。

為整頓資訊安全管理體制，並設置資訊安全管理人員等，請參照下列基準項目：

(1) 系統管理體制（系統管理人員），請參照【運 4】說明。

(2) 資料管理體制（資料管制人員），請參照【運 5】說明。

(3) 網路管理體制（網路管理人員），請參照【運 6】說明。

3、資訊安全管理人員之主要業務及職掌如下：

(1) 由系統規劃到開發、運作、維護、廢棄所有期間，對資訊安全之統籌管理。

(2) 對於重大故障、事故、犯罪等與資訊安全相關問題，應立即向負責全機構資訊安全事宜之總負責人或高階經營層提出報告。

(3) 對於資訊安全管理之阻礙、事故、犯罪等，應積極收集資訊、分析、評估，並應反映在資訊安全相關文件中。

(4) 委外處理之情況亦相同，對委外業務之資訊安全管理體制亦應建立備用。

確立管理體制
資訊安全管理及責任的明確化

適用性分類				
共通	中心	總行	合作	直接
◎				

運 4	建立 系統管理體制。
-----	-------------------

為能**有效**運用資訊安全管理並防止非法行為，應訂定系統管理程序，建立管理之體制。

- 1、訂定系統運作、管理及申請使用許可之手續等之管理程序，讓相關人員徹底瞭解，以確保系統運作能安全、順利進行。
- 2、為維持及管理硬體、軟體之狀態正常，使系統正常運作，應設置系統管理人員。
- 3、系統管理人員之職掌如下：
 - (1) 實施系統相關之資訊安全對策。
 - (2) 硬體、軟體之安裝設定、管理及維護。
 - (3) 系統組成之架構設定參數等之管理及維護。
 - (4) 確保系統之備援作業。
 - (5) 系統使用者 ID 之登錄。
 - (6) 系統使用狀況之管理。
 - (7) 電腦病毒等不正常程式之因應處理。
 - (8) 對違反資訊安全行為之因應處理，並向資訊安全管理人員提出報告。
 - (9) 系統故障、事故之因應處理。

另外，為防止系統管理人員之權限過於集中而發生非法行為，最好指定多位系統管理人員，並賦予不同之業務權限與責任，各金融機構應配合該機構之實際情況，適當分散權限，採行相互牽制的機能。
- 4、最好能與資料管制人員或網路管理人員適當的分散其職掌與權限。

確立管理體制
資訊安全管理及責任的明確化

適用性分類				
共通	中心	總行	合作	直接
◎				

運 5	建立資料管理體制。
-----	-----------

為維護資料安全，並防止非法行為，應訂定資料管理程序，建立管理之體制。

- 1、訂定資料管理程序及申請使用許可手續等之管理程序，應讓相關人員徹底瞭解，以確保資料安全管理能順利進行。
- 2、為能確保資料之機密性、完整性及可用性，應設置資料管制人員。
- 3、資料管制人員之職掌如下：
 - (1) 實施資料相關之資訊安全對策。
 - (2) 監督資料管理程序之遵守狀況。
 - (3) 資料使用相關之許可。
 - (4) 決定使用者對資料之存取權限。
 - (5) 資料使用狀況之管理。
 - (6) 對違反資料安控行為之因應處理，並向資訊安全管理人員提出報告。
 - (7) 故障、事故之因應處理。
- 4、最好能與系統管理人員或網路管理人員適當的分散其職掌與權限。

確立管理體制
資訊安全管理及責任的明確化

適用性分類				
共通	中心	總行	合作	直接
◎				

運 6	建立網路管理體制。
-----	-----------

為能有效運用網路系統，並防止非法存取行為，應訂定網路管理程序，建立管理之體制。

- 1、訂定網路管理程序及申請使用許可手續等管理程序，讓相關人員徹底瞭解以確保網路運作適切、有效及安全。
- 2、為管理網路運作狀況，並進行網路存取之控管及監視，須設置網路管理人員。
- 3、網路管理人員之職掌如下：
 - (1) 實施網路相關安控政策。
 - (2) 網路相關硬體、軟體之安裝設定、管理及維護。
 - (3) 網路組成之架構、設定參數等管理及維護。
 - (4) 網路設定參數等備援作業。
 - (5) 網路相關使用權限之設定登錄。
 - (6) 網路資料流量之管理。
 - (7) 網路存取狀況之管理。
 - (8) 對違反網路安控行為之因應處理，並向安控管理人員提出報告。
 - (9) 網路故障及事故之因應處理。

(一)確立管理體制

2、組織及分工制衡

為保護金融機構資訊系統，使其能安全、順利運轉，並避免其受到災害、故障、入侵或犯罪等事故之重大影響，於發生事故時，能將受災程度減至最低、及早復原，應設置相關組織及訂定權責。

確立管理體制
組織及分工制衡

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 7	設置防災小組。
-----	---------

為預防災害並減輕受害程度，應設置防災小組，並明確指定負責人。

- 1、為預防災害之發生，或發生災害時，能迅速因應災害，減輕受害程度，應設置防災小組；另外，為提升防災小組之有效性，應按分配工作類別明確指定負責人。防災小組實例如圖 1。
- 2、資訊中心與其他單位共用同一建築物時，除大樓整體之管理組織外，應另行設置以資訊中心為主之防災小組。
- 3、設置防災小組時，應注意事項如下

- (1) 設置防災小組，應確實通知相關部門，使其徹底瞭解。

有關防災小組之負責人、分工、避難路線等相關資訊，應確實通知相關部門人員。另外，對於派駐外地人員及其他公司派駐人員，在必要範圍內，亦應確實通知。

- (2) 為避免防災小組徒具形式，應定期檢討組織分工之妥適性並轉知相關部門，使其徹底瞭解該組織。

為使防災小組發揮功能，應定期確實檢討組織之妥適性，另負責人因人事異動變更或經辦員異動時，亦需再次徹底檢討並讓接任者認識該組織架構及其職務。

- (3) 在災害發生時，為能迅速確實連絡防災機構傳達正確受害情況，應明確訂定與防災機構之連繫方法及連繫內容。

此處所謂防災機構，係指消防隊等防災機構。

- (4) 建立災害發生時之緊急連絡網。：

應建立災害發生時之緊急連絡網，並定期檢討該連絡網之有效性。同時針對夜間或假日發生災害，亦應明確訂定相關人員緊急連絡體制。

- (5) 為利於發生地震及颱風等天然災害時採取因應措施，應隨時注意並收集災害預報資料。有關災害預報資料可由氣象局、電視、廣播電臺、地方政府機構發佈之警報或通報宣傳等獲知。

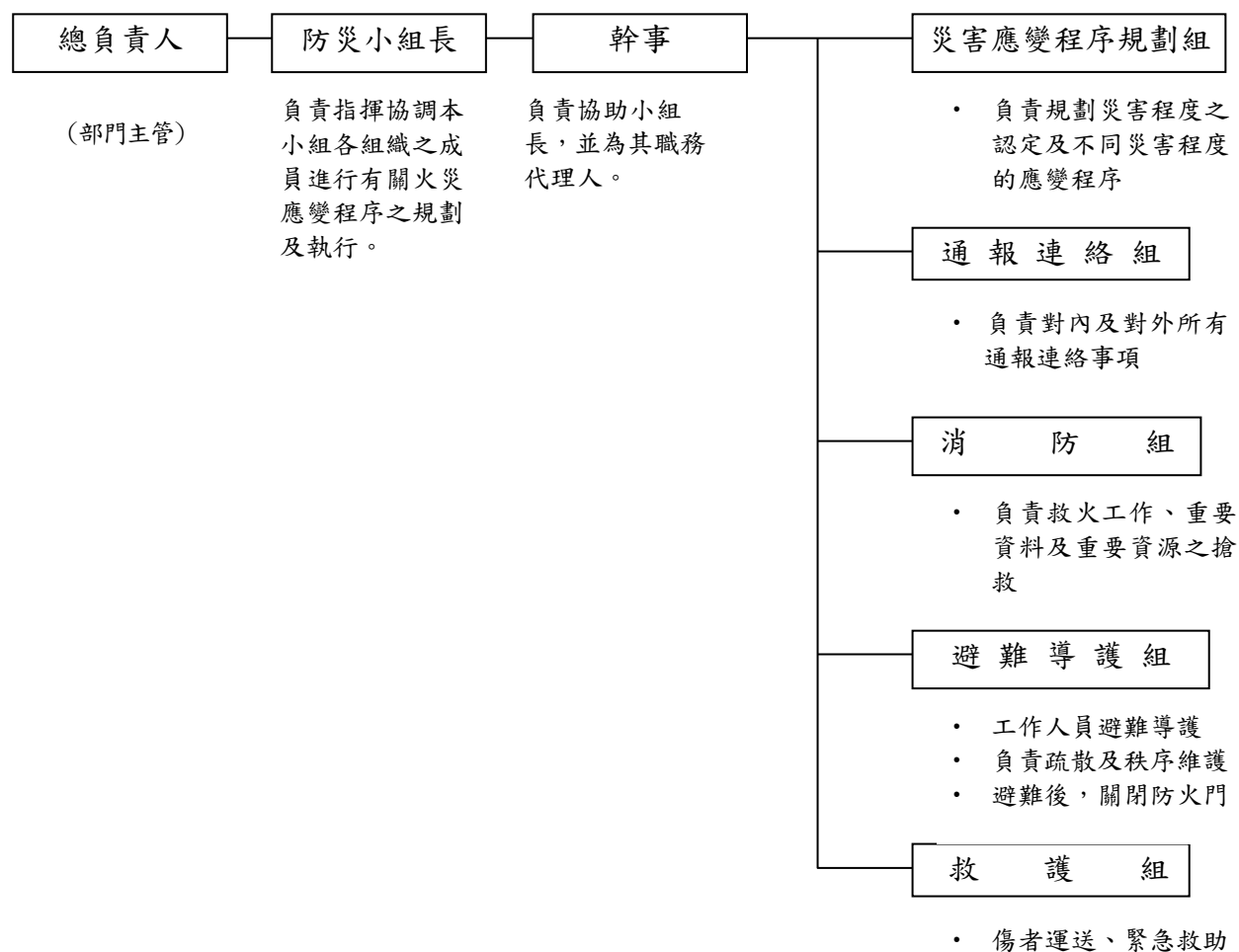


圖 1 防災小組例圖

確立管理體制
組織及分工制衡

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 8	設置防犯小組。
-----	---------

為防止犯罪發生，應設置防犯小組，並明確指定負責人。

- 1、為防止非法入侵、攜入危險物品及非法攜出物品等威脅或發生犯罪事件時，能迅速因應將災害降至最低，應設置防犯小組，並按分配工作類別明確指定負責人。防犯小組舉例如圖 1。
- 2、資訊中心與其他單位共用同一建築物時，除配合大樓整體之管理組織外，應另行設置以資訊中心為主之防犯小組。
- 3、設置防犯小組時，應注意事項如下：
 - (1) 設置防犯小組，應確實通知相關部門並使其徹底瞭解。
有關防犯小組相關之負責人、分工等，應使相關部門人員徹底瞭解。另外，對於保全公司、其他公司派駐人員及駐外之值勤人員等，在必要範圍內，亦應確實通知。
 - (2) 為避免防犯小組徒具形式，不僅需定期使相關部門徹底瞭解該組織，並為因應犯罪技巧之變化，應檢討組織架構與功能。尤其負責人因人事異動變更或經辦員異動時，亦需再次徹底檢討組織架構更須讓接任者認識該組織架構及其職務。
 - (3) 應明確訂定與防犯機關之連絡方法，以備發生犯罪行為時之需。此處所謂防犯機關，係指警察機關。
- 4、資訊中心之防犯對策，其設備基準如下：

(1) 資訊中心

項 目 內 容	相對應之項目編號
a. 建築物	
(a) 不可將招牌等懸掛在外面。	設 6
(b) 應有防犯措施。	設 15
(c) 平常使用之進出口僅限一處，並設置進出管制裝置、防犯設備等。	設 16
(d) 進出門窗應具有充分之強度，並需隨時加鎖。	設 19
b. 電腦機房、媒體儲存室	
(a) 應設置於不易由外部進入之位置。	設 23
(b) 不可懸掛室名等標示牌。	設 24
(c) 平時使用之進出口，應僅限設置一處，並須設置等候室。	設 27
(d) 出入口之門窗，應具有足夠之強度，並須加鎖。	設 28
(e) 應設置火災等緊急事故警示及緊急連絡裝置。	設 38
(f) 於機房進出口設置進出管制與防犯設備。	設 45
c. 電源室、空調室	
(a) 門窗應加鎖，最好不要設置窗戶。	設 55
d. 電源設備	
(a) 應設置防災、防犯用備用電源。	設 71
e. 空調設備	
(a) 空調設備應具有預防入侵、破壞等措施。	設 77
f. 監視控管設備	
(a) 應安裝監視控制設備。	設 80
(b) 宜設置中央監控室。	設 81
g. 數據線路相關設備	
(a) 數據線路相關設備，應上鎖。	設 82
(b) 數據線路相關設備之安裝場所，不可附加標示。	設 83
(c) 數據線路相關設備，應備有專用之配線空間。	設 83-1

(2) 總行、營業單位

項 目 內 容	相對應之項目編號
a. 門窗	
(a) 門窗應有防犯措施。	設 90
(b) 非營業時間之出入口應設置進入者識別用裝置。	設 92
b. 設備	
(a) 應安裝防犯措施。	設 103
c. 線路相關設備	
(a) 不可標示通訊線路相關設備安裝場所。	設 104
(b) 易為外界碰觸之通訊線路相關設備等最好上鎖。	設 105
d. 電源設備	
(a) 防災、防犯設備應安裝備用電源。	設 108
e. 自動化服務區	
(a) 應安裝緊急通報裝置。	設 112
(b) 宜安裝防犯措施。	設 113
(c) 應設置照明設備及緊急照明設備。	設 114
(d) 自動化服務區的門，應有部分為透明透光者。	設 115
f. 伺服器安裝場所	
(a) 伺服器設備應設置於不易由外部進入的位置。	設 122
(b) 設置伺服器設備的位置，不得張貼具室名等標示之招牌。	設 123
(c) 設置伺服器設備的位置，應為專用之隔間。	設 124
(d) 在設置伺服器的房間進出，應設置進出管理設備、防犯設備等。	設 130

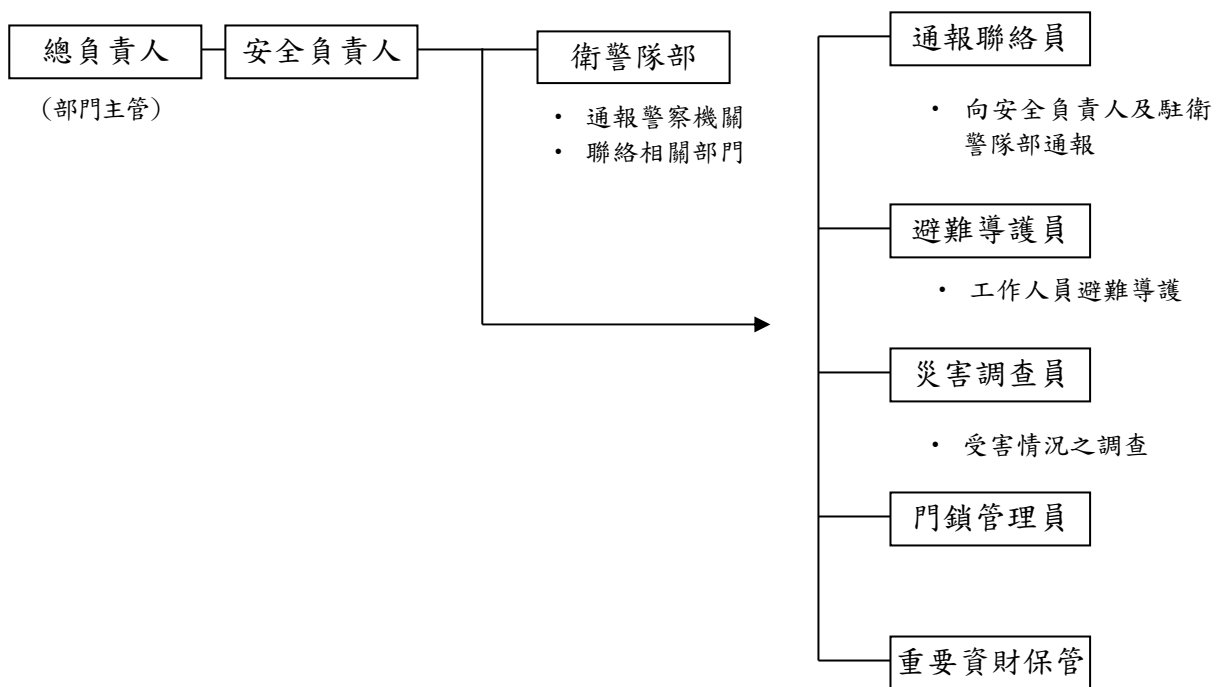


圖 1 防犯小組例圖

確立管理體制
組織及分工制衡

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 9	確立分工體制。
-----	---------

為使資訊系統順利運轉，並防止非法事件發生，應有適當之職務分工，明確劃分業務範圍及責任、權限，以確立相互制衡體制。

1、相互制衡體制係指為了要排除個人失誤或懷有惡意行為，而由第三者予以確認、驗證之體制。在執行資訊系統相關業務時，應明確劃分業務範圍、責任及權限，實施適切的業務組織分工，以有效發揮相互制衡體制之功能。

2、舉例如下：

(1) 業務組織之分工。

程式撰寫、資料輸入、資訊系統之操作、檔案管理等應分工擔任，以達相互制衡目的。

同時，依該業務規模及性質，可進一步考慮下列職務上之分工：

- a. 程式撰寫 …………… 設計者、程式撰寫者等。
- b. 資料輸入 …………… 開立傳票者、資料整理檢核者、資料登錄者等。
- c. 資訊系統之操作 … 電腦操作員、操作申請人、操作核准人、操作驗證人等。
- d. 檔案管理 …………… 程式檔案管理者、資料檔案管理者等。

(2) 明確規定業務處理權限並管理之。

對於上述工作劃分，應明確訂定其業務處理權限（如經辦部門之權限及分工範圍等）。

(一)確立管理體制

3、各種規章之訂定

為使資訊系統順利運轉，應明確訂定劃分責任與權限之規章。

確立管理體制
各種規章之訂定

適用性分類				
共通	中心	總行	合作	直接
◎				

運 10	訂定各種規章。
------	---------

為使資訊系統順利運轉及管理，對於防災、防犯小組及分工體制應明確訂定劃分責任與權限之規章。

1、在此處所稱之規章，係指對於防災、防犯小組及分工體制，明確訂定責任與權限，各項規章請參照如下所列項目：

- (1) 門禁管理。
- (2) 資訊系統於正常情況、發生故障時及發生災害時之運用。
- (3) 電腦處理之相關業務於正常情況、發生故障時及發生災害時之運用。
- (4) 資料、程式及文件管理。
- (5) 表單及磁卡管理。
- (6) 系統開發及變更。
- (7) 電源設備、空調設備、防災設備及防犯設備之管理。
- (8) 防犯、警備。
- (9) 監控。

2、關於資料、程式及文件管理，應視其重要性及機密性訂定必要之規章。

3、有關規章內容，請參照下列基準項目：

- (1) 門禁管理【運 11 ~ 13】。
- (2) 資訊系統於正常情況、發生故障時及發生災害時之運用
【運 14 ~ 24、運 31、運 32、運 54 ~ 65】。
- (3) 電腦處理相關業務於正常情況、發生故障時及發生災害時之運用
【運 37 ~ 50、運 53】。
- (4) 資料、程式及文件管理 【運 25 ~ 30、運 33 ~ 36】。
- (5) 表單及磁卡管理 【運 51、運 52】。
- (6) 系統開發及變更 【運 66 ~ 75】。

- (7) 電源設備、空調設備、防災設備、防犯設備之管理
【運 76 ~ 78】
- (8) 防犯、警備 【運 4 ~ 9】。
- (9) 監控【運 79】。

(一)確立管理體制

4、安控規章遵守狀況之確認

為確保資訊系統順利運轉，應確認對於資訊安控相關規章所定各事項之遵守狀況。

確立管理體制
安控規章遵守狀況之確認

適用性分類				
共通	中心	總行	合作	直接
◎				

運10-1	確認對安控規定之遵守狀況。
-------	---------------

應確認對安控規章之遵守狀況，全體員工(包含駐外人員)及委外人員應對資訊安全政策確實認知，並努力提升機構之安全層次。

- 1、為使資訊系統順利運轉，應確認對於資訊安控相關規章所定各事項之遵守狀況。全體員工(包含駐外人員)應對資訊安全政策確實認知，並努力提升機構之安全層次。
- 2、下列時點為對安控規章所訂定各事項之遵守狀況確認時機：
 - (1) 安裝新系統或新增服務項目時。
 - (2) 對既有舊系統或服務項目，定期或不定期實施。
 - (3) 變更或修改安控規定相關文件時。
 - (4) 人員組織配置異動時。
- 3、執行人員應藉由對內部環境之觀察檢查，以及與內部員工直接面談等，確認對安控對策及安控規章之遵守狀況。
- 4、應對安控規章所訂定各事項遵守狀況之確認結果進行評估，並對安控相關規章做必要修訂。 【運 2】
- 5、應對安控規章所訂定各事項遵守狀況之確認結果進行評估，並重新檢討安控教育訓練內容。 【運 80】

(二)進出管理

1、門禁管理

為防止非法入侵、攜入危險物品、非法攜出物品等，對進出資訊中心或電腦機房等重要房間(館或室)之人、物，應加以管制。

進出管理
門禁管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 11	實施人員資格限制及門禁識別工具管理。
------	--------------------

為防止非法侵入，人員進入資訊中心、電腦機房、媒體儲存室、程式開發場所及電腦相關設備房應實施資格限制，鑰匙、門禁磁卡、識別碼等，應確實管理。

1、此處所稱電腦相關設備房，是指下列場所：

- (1) 電源室。
- (2) 空調室。
- (3) 集中監控電源、空調、防災、防犯設備之中央監控室。

2、為管制資訊中心之人員進入電腦機房、媒體儲存室、程式開發等重要場所，應實施人員資格限制，舉例如下：

- (1) 常駐人員(資訊中心職員、其他公司值勤人員、與資訊中心業務關係密切之其他部門職員等，以下同)，發給貼有照片之出入許可證(以機器設備實施進出管理時，即指資格登錄，發行磁卡交付識別碼等)，及發給能夠辨別所屬單位與出入地點之識別證。至於列有所屬單位及出入地點之貼照片出入許可證，則可兼做識別證。

a. 如係根據本基準項目之宗旨，足以確認資格限制者，可視同此處所稱之貼照片出入許可證。

b. 此處所謂識別證是指名牌、徽章、臂章等，而能夠容易識別所屬單位、出入地點之方法，可考慮使用不同色別之識別證。

c. 此處所稱機器設備，係指識別事先設定之進出資格而做門窗之開關(上鎖、開鎖)之出入管理設備。請參照【設 16】。

- (2) 資格消失時，應收回出入許可證及識別證。

3、當限制資格時，應指定係進出電腦機房、媒體儲存室、電源室、空調室、亦或中央監控室。人員之資格限定如表 1 所示。同時對此處所示以外之人員，視其需要可准予進入，此時亦須明確規定資格限制之方法。

4、管理鑰匙、門禁磁卡、識別碼等，舉例如下：

- (1) 出入口之鑰匙，應保管於指定場所，並由專人管理。需複製鑰匙時，應依規定辦法辦理。
- (2) 記錄鑰匙授受人員之姓名及時間。記錄之目的在於明確登記鑰匙之交接，以表明責任所在，對於借出磁卡亦適用此項目。
- (3) 由專人執行磁卡之發行管理及識別代碼等之管理。
 - a. 門禁磁卡之發行管理，除應由專人按規定辦法辦理外，原具備資格者之資格消失時，亦須迅即收回磁卡。
 - b. 磁卡遺失時應即通知磁卡管理人予以註銷。
 - c. 進出管理用識別碼之登記、變更、註銷，除由專人按規定辦法辦理外，視需要情況應加以變更；至於在登記、變更進出管理用識別碼時，應選擇不易猜測之號碼。
 - d. 進出管理用數字鍵，應定期做清除或更換數字鍵保護蓋等，並研擬無法由外部窺視輸入密碼之措施。
 - e. 使用磁卡、識別碼、密碼以外之資格認定，參照【設 16】。

表 1 各房室可進出之人員舉例

房室	可進出人員
電腦機房	操作人員、系統程式人員
資料媒體儲存室	程式館管理人員、資料管制人員、程式文件管理人員
電源室	電源設備管理人員
空調室	空調設備管理人員
中央監控室	電源設備、空調設備及防災、防犯設備之管理人員

進出管理
門禁管理

適用性分類				
共通	中心	總行	合作	直接
	◎			

運 12	實施中心門禁管理。
------	-----------

為防止非法之侵入、危險物品之攜入及物品之非法攜出等，對進出人員應確認其身分，實施資訊中心之門禁管理。

1、資訊中心與其他單位共同使用同一大樓時，應實施其獨立之門禁管理。

2、相關做法舉例如下：

- (1) 對常駐人員，可由貼有照片之出入許可證(以機器設備實施進出管理時，則指磁卡、識別卡等)確認進出人員之資格，並要求在大樓內應佩戴識別證。
- (2) 對來訪者，於確認身分後，請其在訪客（來賓）登記簿上登記姓名、服務單位、電話號碼、目的、訪問對象、進入時間、來賓識別證號碼等之後，發給來賓識別證，要求其佩掛，於離去時收回，並登記離去時間。
- (3) 對來訪者以指定面談地點為原則，必要時得由被訪者帶領至其他地點。
- (4) 視需要情形，得對進出人員實施攜帶物品之檢查。
- (5) 資訊設備之攜入與攜出，均需符合組織之物品攜出入相關規定提出申請辦理，並由門禁管控人員（警衛）確認後放行。
- (6) 配置警衛人員。

3、對已具備進出資格之人員，其於下班後或假日進出時，仍須辦理進出登記。

進出管理
門禁管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 13	實施電腦機房及媒體儲存室之門禁管理。
------	--------------------

為防止非法之侵入、危險物品之攜入及物品之非法攜出等，對於電腦機房、媒體儲存室及中央監控室等重要區域，應實施進出管理。
--

- 1、除一般門禁管理外，對電腦機房及媒體儲存室等重要區域，應另訂更嚴謹之進出管理。
- 2、相關做法舉例如下：
 - (1) 進出電腦機房及媒體儲存室及中央監控室人員，可由機器或管制人員確認身分後，允許進入。
 - (2) 登記進出人員之姓名及進出時間。登記之目的在於明確表示滯留時間，使得發生事故或不當使用時，容易追究原因。另外，亦可考慮使用機器自動記錄。
 - (3) 攜入電腦機房之紙張等易燃物，要限於最低需要量。
 - (4) 除維護或施工外，危險物品或器具不得攜入電腦機房、媒體儲存室及中央監控室。
- 3、對所攜帶之物品，如屬可疑，仍須檢查其內容，並儘可能於重要地區裝設閉路電視等監視設備。

(三)營運管理

1、手冊之建立

為能正確安全運用資訊系統，日常各種作業處理程序等應標準化，並備妥完整之作業手冊。同時，對於系統故障或災害發生時，為使對系統之影響減至最小，並能在最短時間內復原系統，應明確訂定故障或災害發生時之系統操作程序，整理完整之作業手冊。

營運管理
手冊的建立

適用性分類				
共通	中心	總行	合作	直接
◎				

運 14	訂定日常作業手冊。
------	-----------

為正確且安全運轉資訊系統，應規定日常各種程序之作業手冊。

- 1、所謂日常作業手冊，是指資訊系統在日常作業時所必要之作業程序，或是機器設備之操作程序說明。
- 2、有關作業手冊中應訂定之事項，請參考下列基準項目：
 - (1) 使用權限之管理，請參照【運 16 ~ 18】。
 - (2) 操作管理，請參照【運 19 ~ 23】。
 - (3) 資料檔管理，請參照【運 25 ~ 27】。
 - (4) 程式管理，請參照【運 28、運 29】。
 - (5) 文件管理，請參照【運 33、運 34】。
 - (6) 表單管理，請參照【運 35、運 36】。
 - (7) 輸出資料管理，請參照【運 37】。
 - (8) 金融卡管理，請參照【運 51、運 52】。
 - (9) 資源管理，請參照【運 54】。
 - (10) 外界連接管理，請參照【運 55、運 56】。
 - (11) 機器之管理，請參照【運 57 ~ 59】。
 - (12) 運作狀況之監控，請參照【運 60】。
- 3、相關做法舉例如下：
 - (1) 平時即準備手冊，徹底通知相關部門遵守。
 - (2) 如有追加、變更等事項時，應依規定手續更新。
- 4、手冊涵蓋要項如下：
 - (1) 內容與項目：

手冊中應說明關於執行職務所需之基本事項，應載明其基準、程序等，

關於個別事務處理，應載明其具體流程、手續等，並應將作業方式具體簡明表達，使作業經辦員執行職務時易於遵循。其內容舉例如下：

- a. 名稱。
 - b. 修訂記錄。
 - c. 目錄。
 - d. 前言、總則(目的、宗旨、基本方針、適用範圍等)。
 - e. 本文。
 - f. 附則(適用之特例、實施日期、經過與措施等)。
 - g. 範例(範例、填寫說明等)。
 - h. 附表(參考資料及其他)。
- (2) 手冊之訂定與核定。
 - (3) 手冊之發佈與管理。
 - (4) 手冊修訂程序。
 - (5) 其他例外規定等。

營運管理
手冊的建立

適用性分類				
共通	中心	總行	合作	直接
◎				

運 15	訂定故障或災害發生時相關作業之操作手冊。
------	----------------------

為減低故障、災害發生所導致資訊系統之影響並能及早復原，同時總行、營業單位能持續營運，應訂定故障、災害發生時之備援措施、復原程序等相關作業之操作手冊。

1、故障、災害發生時之操作手冊修訂事項，請參考下列項目：

修訂故障、災害發生時之操作手冊，須與災變備援計畫整合，並定期檢討以維持最新狀態。

(1) 故障、災害發生時之對策，請參照【運 62 ~ 64】。

(2) 災變備援規劃，請參照【運 65】。

2、為維持總行、營業單位等能持續營運，於故障、災害發生時之操作手冊中，需包含下列內容。請參照【運 62 ~ 64】。

(1) 端末機器設備之處理。

(2) 業務處理程序。

(3) 資訊系統設備之處理。

(4) 網路通訊設備之處理。

(5) 機電設備之處理。

(三)營運管理

2、存取權限之管理

為防止資訊系統、檔案等各種資源遭非法使用或破壞，應依系統重要程度設定其存取使用權，並加以管理。

營運管理
存取權限之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 16	明確訂定各種資源、系統等之存取權限。
------	--------------------

為防止非授權人員存取使用資訊系統及其重要檔案，應限定使用者之存取權限。

- 1、此處所稱之資訊系統及其重要檔案，是指金融機構對客戶提供金融服務時，必要之資料及程式等。為防止被非法使用或篡改，應限定使用者之存取權限。亦可由下列各點執行：
 - (1) 防止非法使用重要原始帳冊。
 - (2) 防止系統開發、變更作業等相關測試資料外洩。
 - (3) 實施應用程式之管制，以防止利用程式更改或外洩資料內容。
 確認存取權限之機制，請參照【技 26、技 31、技 35、運 17】。
- 2、發生非法存取資料或檔案時，為能及早發現並追究原因，須能取得非法存取記錄。發現未授權存取資料時，應及時對當事人提出嚴重之警告。請參照【技 37】。
- 3、存取權限管理，具體注意事項，請參照【運 18】。

營運管理
存取權限之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 17	採取防止密碼、 <u>作業憑證等</u> 外洩之措施。
------	-----------------------------

為防止密碼、 <u>作業憑證等</u> 之外洩， <u>除應加強保護外</u> ， <u>應宣導使用者落實管理</u> 。

1、隨時對使用者宣導有關密碼之注意事項如下：

- (1) 不可使用容易被猜測之密碼。
- (2) 密碼不可外洩。
- (3) 不可使用他人之密碼。

2、容易被猜測之密碼如下列所示：

- (1) 位數短少之密碼。
- (2) 與身分證統一編號相同之密碼。
- (3) 出生年月日、電話號碼、自用車輛之牌照號碼等個人資料。
- (4) 自己或熟人（如配偶、朋友、寵物、名人等）之姓名或匿稱。
- (5) 如 123456 等單純之字串或僅使用純數字或純英文字。
- (6) 經常使用之英文單字。
- (7) 上述文數字之倒寫或組合。

3、公司內部使用之密碼，不可長期使用相同之密碼，須於適當之時機加以變更，必要時，得規定須定期變更，否則應設為失效。

4、密碼不為他人竊取之技術，請參照【技 26】。

另外，遇到登錄密碼或需列印時，不應列印在序時紙捲，而應分別列印或以密碼單列印並嚴密保管以達防止密碼外洩之目的。

營運管理
存取權限之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 18	明確訂定存取權限之授予及評估等作業程序。
------	----------------------

管理各種資源、系統等存取權限之授予，應明確訂定其作業程序。同時，為維持存取權限之妥適性，亦需明確訂定定期評估之作業程序。

- 1、存取權限之管理、設定等作業程序，應配合部門職責、部門配置，明確訂定由主管授予存取權限及審核等程序。存取權限之識別 ID 不可共用，須一人一個 ID 以明權責。
- 2、設定存取權限，可參考下列作業程序：
 - (1) 員工等使用者需要資料存取權限時，應申請辦理。
 - (2) 所屬主管，應確實審核是否為業務處理上必要之申請。
 - (3) 資料管理者，應依申請人所屬單位、職責、使用目的等，確實審核。

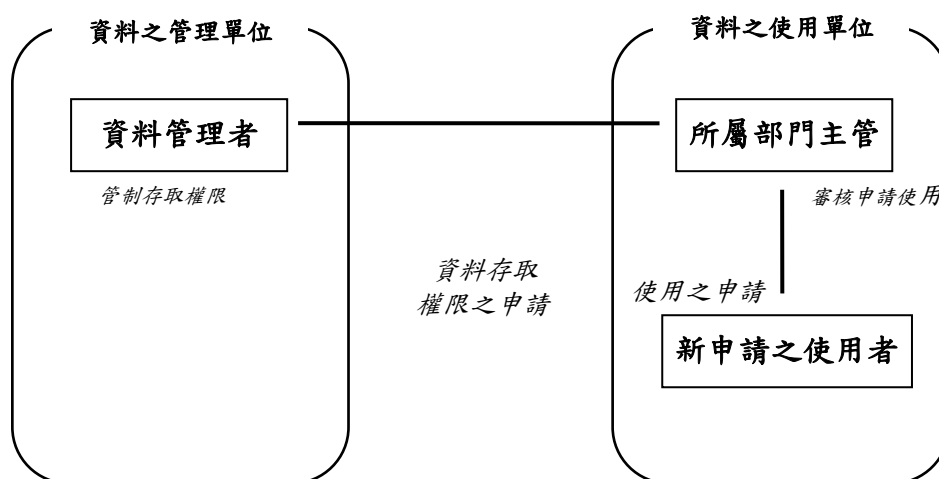


圖 1 申請資料存取權限之關係圖例

- 3、在人事異動時，存取權限之評估作業程序應明確訂定，同時，重新評估資料

存取權限之妥適性。

4、重新評估資料存取權限之時機如下：

- (1) 部門、職掌、組織等變動時。
- (2) 人員進用、離職時。
- (3) 長期出差、留學、停職等。
- (4) 新系統啟用時。
- (5) 經過一定時間後。

5、存取權限之管理，注意事項如下：

- (1) 明確訂定 ID 之登錄、變更等作業管理人員。
- (2) 明確訂定 ID 之申請、審核、設定等作業程序。
- (3) 使用者不再需要存取資料時，其存取權限應即時刪除。
- (4) 由廠商購置之套裝軟體、應用軟體等，在安裝啟用時，應刪除預設之存取權限。
- (5) 系統中，若有特權之 ID (Super User 等)，應嚴謹管制並評估予以刪除或變更名稱。
- (6) 授予存取權限得設定其有效期限，期滿後，再評估是否延長其有效期限。
- (7) 使用者密碼遺忘需修改及通知時，應確認使用者身分。

(三)營運管理

3、操作管理

為防止電腦系統之非法使用，並求運轉順利，有關操作應實施申請、核可、執行、記錄、結果之確認等管理。

營運管理
操作管理

適用性分類				
共通	中心	總行	合作	直接
	◎			

運 19	值勤操作人員之確認。
------	------------

為防止非法使用，應確認是否為值勤操作人員。

1、為防止因非法操作而發生資料洩露等事故，當操作電腦系統時，應經作業管理負責人確認操作人員之資格。

若因臨時狀況需要系統開發人員參與操作時，應經作業管理負責人核准，並依重要性會同處理。

2、資格確認舉例如下：

(1) 當操作人員執行操作時，作業管理負責人應根據執勤預定表等確認之。

(2) 電腦機房執勤之操作人員，除佩掛識別證，建議穿著制服。

營運管理
操作管理

適用性分類				
共通	中心	總行	合作	直接
	◎			

運 20	明確規定操作之申請及核可 <u>程序</u> 。
------	--------------------------

為防止電腦系統之非法或不當使用，應明確規定操作之申請及核可 <u>程序</u> 。

- 1、為防止電腦系統之非法或不當使用，應依規定程序申請作業。
- 2、如自動操作，應明確規定有關排程之編排與認可，以及登錄到自動排程程式等之作業程序。
- 3、對於臨時處理或由事故引起之例外處理等，都需要明確規定作業程序。

營運管理
操作管理

適用性分類				
共通	中心	總行	合作	直接
	◎			

運 21	明確規定操作之執行規範。
------	--------------

為防止操作錯誤或違規使用，應明確規定操作之執行規範。

1、此處所稱操作之執行規範，係指操作時之操作人員編組及操作程序。

2、有關操作之執行規範舉例如下：

(1) 根據操作申請單等，確認係已核可之作業申請。

(2) 設置專任操作人員，其專任之目的如下：

a. 明確責任。

b. 防止違規。

(3) 操作應由二人以上之操作員執行，其目的如下：

a. 透過操作員相互間的牽制效果以防止違規使用。

b. 緊急時之因應。

(4) 輸入重要指令時，實施相互確認。

輸入重要指令時實施相互確認之目的，在於防止操作錯誤導致發生故障，至於重要指令，舉例如下：

a. 連線開機處理。

b. 連線關機處理。

c. 故障設備之隔離(中央處理機、主記憶體設備、通道裝置、儲存體設備等)(參照【技 19】)。

d. 通訊電路之切換。

(5) 明確指定作業(Job)之執行人員。

明確指定作業之執行人員之目的，除了明確劃分責任外，發生事故時，容易追究原因。

至於此處所稱之作業執行人員，係指由主控台操作或對運行狀況加以確

認之操作人員或操作小組。

- 3、當發生故障狀況或意外事件時，應迅速向主管提出報告。
- 4、為防止操作錯誤導致電腦系統發生事故，以期業務進行順利，應訂定標準操作程序，並編寫成手冊：
 - (1) 各種機器之操作方法。
 - (2) 指令之使用方法。
 - (3) 電腦系統運轉程序。
- 5、機密性較高之作業，應特別指定作業人員。
- 6、有關操作之自動化與簡易化，參照【技 13】。

營運管理
操作管理

適用性分類				
共通	中心	總行	合作	直接
	◎			

運 22	<u>確認執行結果，並留存操作紀錄。</u>
------	------------------------

為驗證操作之正確性，應確認執行結果，並留存操作紀錄。

1、為確保操作之正確性，除確認操作執行時之運轉狀況外，應確認申請之操作是否已按指示處理完畢，並留存操作紀錄。

2、舉例如下：

(1) 編製確認運轉狀況之查核表 (Check List)。

可確認運轉狀況之查核表，舉例如下：

- a. 操作紀錄。
- b. 操作預定、實際比較表。
- c. 作業執行狀況表。

(2) 明確規定交接事項。

為防止交班時未處理及重複處理，應將交接事項明確交代，交接事項舉例如下：

- a. 工作處理狀況。
- b. 事故發生狀況。
- c. 其他聯絡事項。

(3) 留存操作紀錄，明確訂定驗證操作結果之制度。

驗證使用紀錄如下：

- a. 運轉狀況查核紀錄。
- b. 自動運轉檢核紀錄。

在檢核、確認過程，如發現重大過失時，應迅速向主管提出報告。

營運管理
操作管理

適用性分類				
共通	中心	總行	合作	直接
	○	○		

運 23	辦理主從架構系統 (Client Server System) 之作業管理。
------	--

為防止對主從架構系統 (Client Server System) 之非法使用，應明確訂定作業申請、核准等之程序，並有適切之執行、記錄機制。

操作管理的方法，舉例如下：

- (1) 依作業類別，指定系統操作人員及其作業，請參照 【運 21】。
 - a. 資料、程式檔案之備份作業。
 - b. 存取權限之登錄。
 - c. 系統之維護作業。
- (2) 應明確訂定作業申請、核准之程序，請參照 【運 20】。
- (3) 作業記錄，請參照 【運 22】。
 - a. 取得資料、程式檔案之備份檔。
 - b. 系統版本更新作業。

(三)營運管理

4、資料輸入管理

為能確保輸入資料之安全性及完整性，應建立資料輸入之作業程序，並要求相關部門落實此作業程序。

營運管理
資料輸入管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 24	辦理資料輸入之管理。
------	------------

為保障資料之正確及防止非法作業，應訂定資料輸入之作業程序。

- 1、為保障輸入資料之正確，確保其完整性與機密性，並防止非法使用，應訂定資料輸入之作業及核可程序，並確實遵守。
- 2、訂定資料輸入之作業程序，舉例如下：
 - (1) 設置資料管制負責人員，並明訂其職掌、責任。
 - (2) 輸入資料之製作：
 - a. 原始資料之製作要領。
 - b. 資料輸入之說明。
 - (3) 資料授受之輸入：
 - a. 作業程序名稱。
 - b. 負責人員。
 - c. 資料輸入記錄：
 - (a) 資料輸入人員。
 - (b) 日期。
 - (c) 資料件數。
 - (d) 資料格式（形式）與標籤內容。
 - (4) 明定重要資料、機密資料之處理人員及資料確認之時機。
 - (5) 輸入資料之確認。
 - (6) 資料輸入前後之確認。
 - (7) 資料之檢核：
 - a. 資料內容之確認。
 - b. 資料原始憑證與輸入資料之比對勾核。

- (8) 輸入資料之刪除、修改及追加。
- (9) 資料輸入紀錄之取得、管理及保存。

(三)營運管理

5、資料檔案管理

為防止資料檔案之不當使用、篡改、毀損或遺失等，應由專人按規定方法執行資料檔案授受及保管作業。同時為預防資料檔案毀損、故障等情形，應確實執行檔案備份作業，以備資料檔案遭破壞或事故時之需。

營運管理
資料檔案管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 25	規定資料授受及保管方法。
------	--------------

為防止資料檔案之不當使用、篡改、毀損及遺失等，其授受及保管，應由專人按規定辦理。

- 1、此處所稱資料檔案，係指存放於磁碟、磁片、光碟、磁帶、匣式磁帶、DAT(數位錄音帶)等媒體中之檔案。
- 2、資料檔案之授受及保管方法，舉例如下：
 - (1) 訂定資料檔案交接及報廢之處理方法，並明確指定負責人。
 - a. 在資料檔案之交接紀錄應包含下列各項目：
 - (a)使用目的。
 - (b)使用時間。
 - (c)使用者姓名。
 - (d)負責人之核可。
 - (e)進出庫時間。
 - (f)負責進出庫經辦人員姓名。
 - b. 以磁片、磁帶等與外界進行資料授受時，應訂定資料製作與交接辦法。
 - c. 因保存期限屆滿或讀寫錯誤等而報廢資料檔案時，為防止不當刪除或資料外洩等，應明確記載下列項目，並請參照 【運 74、運 75】：
 - (a)在檔案管理簿上記載保存期限。
 - (b)依資料檔之機密程度選用報廢方法（如消磁、裁剪裁斷等）。
 - (c)報廢理由。
 - (d)報廢日期。
 - (e)報廢作業負責人員姓名。
 - d. 由於磁碟故障，必須更換並報廢舊磁碟時，應有適當之防止資訊洩漏措施。請參照 【運 74、運 75】。

- (2) 需要複製資料檔案時，應按規定辦理。明確規定需要複製檔案時的申請、核准、複製手續及複製檔案之授受與報廢棄程序。
- (3) 檔案之保存期限應明確規定。
為防止資料檔案之不當刪除，應依其重要程度明確規定保存期限。
- (4) 使用檔案管理登記簿，實施檔案庫存管理。
為防止資料檔案之非法使用、遺失等，並及早發現上述問題，應使用檔案管理登記簿，定期或不定期實施檔案庫存管理作業。
- (5) 資料檔案應保管在資料保管室等指定場所。
- (6) 資料檔案標籤上之內容記載應使用代號。
為防止資料檔案之非法使用，資料檔案標籤上之內容記載，應使用代號，並以必要項目為限。

營運管理
資料檔案管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 26	訂定資料檔案之修改管理方法。
------	----------------

為防止非法使用或篡改，凡資料檔案之修改，應先取得部門負責人之核准後按規定辦理，並驗證其辦理之結果。資料檔案修改紀錄，亦應依重要程度規定其保存期限。

- 1、由於程式故障等原因，發現資料檔案不吻合時，應做資料檔案之修改，因資料檔案之修改異於正常之業務處理，應明確規定修改作業之申請、核准、及作業處理程序，同時應驗證其處理程序與結果。
- 2、驗證資料檔案修改之結果：
 - (1) 程序之合法性。
 - (2) 內容之正確性。
- 3、依資料檔重要程度之不同，規定文件(修改紀錄與修改申請書)之保存期限。

營運管理
資料檔案管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 27	確保資料檔案之備份作業。
------	--------------

為防範重要資料檔案發生毀損或故障等事故，應製作備份檔案，並明確規定管理方法。

- 1、重要資料檔案發生毀損或故障時，為能儘速復原毀損之檔案，應明確規定平時取得資料檔案備份、保存及管理之辦法，並以能與災變備援計畫整合為原則。
- 2、製作備份檔案時，應注意下列事項：
 - (1) 設定適當之版本階層管理（如二代制、三代制等）。
 - (2) 考量復原所需時間及復原作業期間之影響等，規定備份作業之週期。
 - (3) 應確認製作備份檔案過程正常結束（如結束代碼、件數等）。
- 3、檔案備份作業應依資料檔案種類、資料更新時機等，設定適當之備份作業及檔案保管之週期。有關備份檔案保管方法，舉例如下：
 - (1) 分散保管

將備份檔案保存在同一建築物內或較近距離的場所（對火災、區域性災害等較有效）。
 - (2) 異地保管

將備份檔案保存在較遠距離的場所（對地震、大規模的災害等有效）。

另外，檔案委外異地保管時，除考慮可靠性及安全性外、尚須考慮二十四小時隨時取用之可用性。

異地保管之資料（含代管資料）如須提早攜出時，應獲得主管之認可，且進出紀錄應依規定期限保存。
- 4、有關備份檔案的保管方法，請參照 【運 25】。
- 5、對於網路上傳輸的資料，亦需依其重要性執行資料備份作業。

(三)營運管理

6、程式檔案管理

為防止程式被篡改或破壞等，程式檔案應由專人按規定管理。並確實執行程式檔案之備份作業。

營運管理
程式檔案管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 28	明確規定程式檔案之管理方法。
------	----------------

<p>為防止程式被篡改或破壞等，應由專人按規定方法<u>執行程式檔案入出庫管理及保管作業</u>。</p>

- 1、此處所稱程式檔案，係指套裝軟體程式、自行開發的應用程式等之原始程式碼或執行模組(Load Module)。
- 2、對正式作業程式之上線或刪除，應由程式管理人員按規定方法管理，開發中或修改中之程式與正式作業程式應分開管理。
- 3、程式之管理方法，舉例如下：
 - (1) 設置程式管理登記簿。
管理內容請參照 【運 66】。
 - (2) 程式之上線作業，應按規定之作業程序辦理。
對正式作業程式之新增上線、修改後重新上線或刪除等，應根據上線申請單或刪除申請單由專人辦理，申請單之項目如下：
 - a. 程式編號或名稱。
 - b. 作業內容（新增、變更、刪除等）。
 - c. 作業理由（變更原因等）。
 - d. 版本編號（Version No.）。
 - e. 正式作業預定日期。
 - f. 經辦人員姓名。
 - g. 經有權人員核准。
 - (3) 實施程式、作業系統（OS）及編譯程式（Compiler）等之版本管理。

營運管理
程式檔案管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 29	確保程式檔案之備份作業。
------	--------------

為防範程式檔案發生毀損或故障等事故，應製作備份程式，並明確規定管理方法。

- 1、為預防電腦病毒等非法程式篡改或破壞程式，造成系統的故障，應明確訂定重要作業程式之備份檔案取得、保存與管理方法。
- 2、為了取得程式之備份檔案，並確保備份檔案的品質，應訂定適當的版本管理辦法（請參照【技 15】）。同時考慮系統復原所需時間及復原期間對作業之影響，應確實訂定備份作業之週期（請參照【運 27】）。

3、有關備份程式保管方法，舉例如下：

（1）分散保管

將備份程式保存在同一建築物內或較近距離的場所（對火災、區域性災等較有效）。

（2）異地保管

將備份程式保存在較遠距離的場所（對地震、大規模的災害等有效）。

另外，委外異地保管時，除考慮可靠性及安全性外、尚須考慮二十四小時隨時取用之可用性。異地保管之資料（含代管資料）如須提早攜出時，應獲得部門負責人之認可，且進出紀錄應依規定期限保存。

(三)營運管理

7、電腦病毒之對策

為預防非法篡改或破壞程式之電腦病毒，應明確規定防止電腦病毒入侵之對策，或遭入侵時之檢測對策。同時為預防被入侵感染，應明確規定檔案備份作業、系統復原作業等程序。

營運管理
電腦病毒之對策

適用性分類				
共通	中心	總行	合作	直接
◎				

運 30	應明確規定因應電腦病毒之對策。
------	-----------------

為預防電腦病毒入侵或感染，應明確訂定偵測、防禦、復原等作業程序。

為預防電腦病毒之入侵或感染，應明確訂定偵測、防禦、復原等作業程序。

- 1、對於電腦病毒等非法程式，應在事先防止其入侵。萬一已遭入侵時，應明確規定迅速偵測、發現之對策。
 - (1) 有關防禦對策，請參照 【技 49】。
 - (2) 有關偵測對策，請參照 【技 50】。
- 2、為預防萬一感染電腦病毒等非法程式，應事先訂定因應對策，以迅速完成復原作業。事前因應對策之舉例如下：
 - (1) 執行程式與資料檔案之備份作業，並將程式的原始檔案設定為唯讀檔案來保管。
 - (2) 應留存程式之異動紀錄。

請參照 【技 49】內「電腦病毒對策實例」。
- 3、當感染電腦病毒等非法程式時，為防止災害擴散，應執行系統復原及預防再次感染等因應對策。

復原對策請參照 【技 51】。
- 4、針對電腦病毒對資料、硬體及軟體之破壞所需之復原費用，及損失賠償責任等，得考慮保險賠償等方法。

(三)營運管理

8、網路設定資訊之管理

為預防網路設定資訊被非法篡改，應妥善管理上述設定資訊。同時，為預防上述設定資訊遭破壞或發生故障，應落實檔案備份作業。

營運管理
網路設定資訊之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 31	應落實網路設定資訊之管理。
------	---------------

為預防電腦系統網路設定資訊被篡改，應強化網路設備管理人員帳號密碼保護機制，落實網路設定資訊之管理。

1、路由器（Router）等通訊設備之設定及修改，應經由正式之變更程序。為預防這些設備之設定值被非法修改或因故障而造成損毀，有關通訊網路架構之設定值，應有適當之管理。

有關網路架構之管理，請參照相關之基準項目：

完整之網路管理體制，請參照 【運 6】。

2、對連接公眾網路（Frame Relay、ATM、ISDN 等）之通訊設備，應特別加以監視，實施適當之管理作業。

3、對於路由器之設定作業，應使用 ID 及密碼等保護功能，防止非法存取設定值之情形發生。

非法存取之對策，請參照下列基準項目：

(1) 應設置確認本人之機制。請參照 【技 35】。

(2) 應具有密碼不外洩之對策。請參照 【技 26】。

營運管理
網路設定資訊之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 32	應落實網路設定資訊之備份作業。
------	-----------------

為預防電腦系統網路設定資訊被非法篡改或因應故障發生，應明確訂定備份檔案之取得作業程序及管理辦法。

1、為預防路由器等通訊網路設備之設定值被非法篡改，或因故障而遭毀損，網路架構等資訊應明確落實資料備份作業。

設定值備份方法，請參照下列之基準項目：

- (1) 訂定交接、保管管理之辦法。請參照 【運 25】。
- (2) 訂定修改變更之辦法。請參照 【運 26】。
- (3) 落實備份作業。請參照 【運 27】。

(三)營運管理

9、文件管理

為預防文件之不當使用或遺失等，應由專人按規定辦法管理之。另外，發生故障或災害時，為復原作業所需文件，應明確訂定取得備份文件及管理之辦法。

營運管理
文件管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 33	明確訂定文件管理辦法。
------	-------------

為預防文件不當使用、篡改或遺失，文件應依照規定辦法管理。

- 1、此處所稱文件，係指資訊中心作業管理上所需要的操作流程、操作說明、系統相關資料及端末操作等之手冊。
- 2、文件之管理方法，舉例如下：
 - (1) 由系統開發部門移交新的業務處理作業時，應依照規定程序，辦理文件之交接。
 - (2) 文件新增或變更時，應依照規定程序辦理。
 - (3) 各種文件應設置登記簿管理之。
 - (4) 重要文件，應依規定程序，存放在加鎖之文書櫃中。
 - (5) 其他部門人員，需要調閱文件時，應依照規定程序辦理。
 - (6) 文件交接時，應依照規定程序辦理。
 - (7) 應依照文件類別，訂定保存期限。
- 3、對於非紙本文件（如電子媒體等），亦須遵照上述規定處理。
- 4、對於重要文件之影印、複製，應訂定管理辦法。

營運管理
文件管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 34	確保文件之備份作業。
------	------------

為因應災害發生時之復原作業，應明確訂定所需文件備份之取得及管理辦法。

1、為因應災害發生時之復原作業，復原作業所需各類文件，應明確訂定文件備份之取得及管理辦法。另外，有關備份文件之保管方法，舉例如下（備份週期，請參照 【運 27】）。

(1) 分散保管

將系統復原所須文件之備份文件，保存在同一建築物內或較近距離的場所（對火災、區域性災害等較有效）。

(2) 異地保管

將系統復原所需文件之備份文件，保存在遠距離的場所（對地震、大規模的災害等有效）。

對於在預定保管期間，如須提早攜出備份文件時，應獲得部門主管同意，並記載文件攜出紀錄，且攜出紀錄應依規定期限保存。

2、為因應災害發生時之復原作業，所需文件（紙本文件或類似磁片之文件）應考慮包含下列文件：

(1) 基本設計書、詳細設計書（應用程式流程圖、檔案格式、交易代碼、系統程式等之說明）。

(2) 操作指示文件。

(3) 使用者手冊。

(4) 作業系統之環境選項設定及變更項目。

(5) 系統架構（硬體架構及作業系統架構）。

(6) 網路架構。

(7) 災變備援作業計畫（緊急災變時因應計畫）。

(三)營運管理

10、傳票帳冊管理

為預防傳票帳冊不當使用或資料內容外洩等，應明確訂定重要傳票帳冊之管理辦法及報廢程序等。

營運管理
傳票帳冊管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 35	明確訂定未使用之重要空白傳票帳冊管理辦法。
------	-----------------------

為防止不當使用，未使用之重要空白傳票帳冊，其庫存管理及報廢，應依照規定辦理。

- 1、重要傳票帳冊，係指已蓋有公司印、總經理或董事長等公司負責人印之收據、支付通知書或有價證券等，可以直接領取現金或變現的傳票帳冊或與契約相關之傳票、帳冊、存摺、證書（存款證明等）之文件。
- 2、對於庫存管理或報廢作業，應管理使用張數及作廢張數。具體的管理方法，舉例如下：
 - (1) 重要傳票帳冊，應存放在加鎖之文書櫃中保管。
 - (2) 領取或繳回空白傳票帳冊時，應會同保管人員辦理，並登錄於登記簿。
 - (3) 印製後，應清點確認印製後庫存數量。

$$\text{印製後庫存數量} = \text{印製前庫存數量} - \text{印製數量} - \text{印製失敗數量} - \text{印表機送紙空白作廢數量}$$
 - (4) 應依據傳票帳冊庫存管理登記簿做庫存管理，同時應於適當時點做庫存清點，確認數量。
- 3、印製錯誤、印製不良等，或帳冊格式修訂而需要作廢時，應由負責人員確認後銷毀之。

營運管理
傳票帳冊管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 36	明確訂定已印製之重要傳票帳冊處理辦法。
------	---------------------

為防止非法使用，已印製之重要傳票帳冊，其交接或報廢應依照規定辦理。

- 1、此處所稱已印製之重要傳票帳冊，是指在【運 35】所提帳冊經由資訊中心處理結果並印錄包含各種資訊(如客戶資訊、交易明細資料等)之表報，以及由端末機器列印之傳票帳冊等，不論其媒體的種類，由資訊系統處理編製的文件均屬重要傳票帳冊。
- 2、為防止已印錄之重要傳票帳冊被非法使用，應由專人依規定辦理交接及報廢，並須經由主管負責人確認。
另外，在交接的過程中，如有需要短期的保管時，應嚴謹管理。
- 3、交接事宜
已印錄之重要傳票帳冊交接時，應根據交接用簽單、交接登記簿、發送登記簿、文件張數等逐一確認無誤。
- 4、管理事宜
傳票帳冊的保管，應存放規定的場所，發生故障或災害時所需的傳票帳冊，應存放在防加鎖之文書櫃中保管。
- 5、報廢事宜
對於已使用或回收的重要傳票帳冊，作廢時，應由負責人確認後銷毀之。

(三)營運管理

11、資料輸出管理

為預防輸出資料不當使用或資料內容外洩，及保護資料的機密性、隱私權等，應明確訂定輸出資料之管理規則。

營運管理
資料輸出管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 37	重要資料之編製、輸出處理等，應具有防止非法使用及保護機密之措施。
------	----------------------------------

為防止重要輸出資料遭篡改、竊取、洩漏等，在編製及輸出處理過程，應有防止非法使用及保護機密之對策。

1、重要輸出資訊編製、交接、保管、管理以及報廢等，應有防止被篡改、竊取、洩漏等的措施。

此處所稱輸出資料，係指由資訊系統處理結果所編製的資訊，與傳票帳冊、磁帶、磁片等媒體種類無關。

2、對策要點，舉例如下：

- (1) 輸出資料之編製程序，應包含防止非法使用措施。
- (2) 應有防止影印、複製等非法行為之措施。
- (3) 依輸出資訊之重要性，限制進出處理人員。

3、具體對策，舉例如下：

(1) 輸出資料之編製程序與處理

a. 對端末系統、個人電腦等之資訊輸出

- (a) 應確認操作者之存取權限，及設定使用機器及處理業務之權限。
- (b) 資料不得長時間顯示在畫面上。
- (c) 對設置於行外機器的資料輸出，其資料之應用應以契約或使用規定，明確訂定。

b. 在資訊系統中處理新增資料之輸出

- (a) 應依照操作程序處理。
- (b) 應由多位操作人員共同處理。
- (c) 應在操作日誌中記載作業處理之結果。
- (d) 為防止在處理過程中發生機密外洩或遺失，應限定使用之印表機或指定處理人員。

(2) 防止非法使用對策

a. 對端末機器或個人電腦之顯示畫面

(a)防止無權限者之操作、窺視畫面或取得複印文件等。

(b)不得長時間連續顯示資料於畫面上。

b. 輸出資料之列印

(a)限定印表機操作人員。

(b)限定資料的輸出量、輸出範圍等。

若份數或資料量超出輸出規定時，應有能發現並通報之機制。

(3) 對影印、複製之處理

重要資料之影印、複製，應留下記錄。

(4) 資料輸出之記錄

a. 有關資料輸出之資訊，應留下記錄。

b. 經由網路連接之端末機器或個人電腦，資料之傳輸應取得輸出記錄。

c. 編製資料輸出的記錄。記錄表單的內容項目，舉例如下：

(a)處理之業務。

(b)處理時間。

(c)處理結果（正常、異常）。

(d)處理人員。

(e)申請人員。

(f)資料輸出量。

(5) 輸出資料的檢核

a. 確認沒有發生處理錯誤的情況。

b. 確認項目內容，舉例如下：

(a)資料識別 ID。

(b)依密碼的資格確認。

(c)資料件數。

(d)資料項目之合計（檢核合計數）。

(6) 保管及報廢

a. 指定負責人。

b. 訂定保管場所及管理辦法。

c. 訂定報廢辦法。

請參照 【運 36】。

(三)營運管理

12、交易管理

為預防端末機器遭非法使用、啟動不當交易等，除應以操作人員識別卡管理外，同時應詳細記錄交易的操作內容，並加以檢核。

營運管理
交易管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 38	明確訂定各類交易之操作權限。
------	----------------

為防止利用利用端末設備從事不正當交易，應依照交易內容，分別訂定端末設備操作者所能操作之權限範圍。

- 1、為防止利用端末設備執行不正當交易，依交易重要程度，分別規範操作者所能操作之權限範圍，對於營業廳外可以單人獨立操作之端末設備等，更需明訂其操作權限。
- 2、特殊交易處理前，須獲該交易有權者之核可。

營運管理
交易管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 39	操作人員作業卡之管理。
------	-------------

為防止利用端末設備從事不正當交易，應指派專人負責管理操作人員作業卡。

- 1、操作人員作業卡為操作端末設備時，確認其操作權限之方法，涵蓋鑰匙、通行碼、識別碼等。
- 2、操作人員作業卡之管理，可考慮下列方法：
 - (1) 明確指派專人負責作業卡之管理，遇出借作業卡時應設簿登記加強控管。
 - (2) 處理特殊交易之主管卡，應由主管妥善保管，並留使用記錄。
- 3、通行碼等之管理，可考慮下列之方法：
 - (1) 明確訂定通行碼等登錄、變更與註銷之申請程序。
 - (2) 明確指定通行碼等登錄、變更與人員，並設專人妥善管理登記簿。
 - (3) 原有使用者於喪失使用權時，應儘速將其通行碼等註銷。

營運管理
交易管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 40	記錄並驗證交易之操作內容。
------	---------------

為防止利用端末設備從事不正當交易，應建立可由交易明細表、端末設備操作紀錄等驗證交易內容之制度。

1、應訂定以記錄交易內容之端末設備紀錄紙捲及資訊中心回傳之交易明細資料等，驗證交易內容之方法。

2、具體實例如下：

(1) 制訂記錄端末設備操作者之措施。

端末設備操作紀錄之內容，除交易本身內容之外，應考慮加入下列項目：

- a. 端末設備操作人員姓名。
- b. 端末設備編號。
- c. 處理序號。
- d. 處理時間。

端末設備操作紀錄是指在營業單位的交易傳票、端末機的時序紀錄、資訊中心或營業單位之交易時序紀錄檔案等。

(2) 由有權人員驗證特殊交易之交易紀錄，驗證方法舉例如下： 請參照【技 47】

- a. 列印交易明細資料。
- b. 連線查詢之方法。
- c. 使用監控專屬（指定）之端末設備。

(3) 依照端末設備操作紀錄規定之保存期限加以保存。

營運管理
交易管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 41	問題帳戶之管理。
------	----------

為防止利用事故從事非法交易，對於掛失止付等問題帳戶，應規定事故申報處理之管理方法。

- 1、為防止利用申報事故之帳戶不當使用，對提供客戶使用之設備、卡片等，經客戶申報遺失、被竊時，應依規定予以處理。
所謂「事故」是指金融機構提供給客戶使用之機器設備、IC 卡或磁條卡、存摺、印鑑、證明單據、有價證券等發生遭竊、遺失之問題。
- 2、受理事故申報時，除記錄受理時間外，應立即執行事故登錄。接到電話申報到收到書面申報之間，應有適當的處理規定。請參照 【技 39】。
- 3、夜間或假日僅提供 ATM 服務之時段，亦需由管制中心或服務中心等受理客戶申報掛失止付之事故處理。
- 4、解除已登錄之事故註記時，應依規定慎重處理並留存記錄。

營運管理
交易管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 42	事先明確告知客戶，使用電子儲值媒體應有之責任及潛在風險損失。
------	--------------------------------

為提醒使用者注意，利用電子儲值媒體（卡）或通訊等機器設備遭竊、破損時，使用者可能遭受損失，以及應由使用者承擔之責任等，應有簡單明確之提示。

電子儲值媒體（卡）等遺失、遭竊或破損時，客戶可能會遭受的損失及責任，應事先明確告知客戶。

提示之方式，舉例如下：

- (1) 於申請契約中規定。
- (2) 交易前以電子方式呈現或標示於媒體上。

提示之項目，舉例如下：

- (1) 有關電子式儲值之保證。
- (2) 遺失、遭竊、破損時之申報規定。
- (3) 遺失、被竊的媒體、機器設備等之損失及責任問題。

(三)營運管理

13、金鑰之管理

金融機構在管理金鑰時，為預防資訊之洩露及非法使用，應明確訂定登錄、變更之程序，並嚴格管理。

營運管理
金鑰之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 43	應明確訂定金鑰使用及管理之辦法。
------	------------------

為防止非法使用，應明確訂定金鑰之產生、遞送、使用及管理等相关作業程序，同時相關管理文件，應由主管嚴格管理。

- 1、金融機構對於金鑰之遞送、遺失、損壞回復、回收及有效期限等相关之作業程序，應事先明確訂定。
- 2、金融機構執行金鑰（對稱式金鑰或公開金鑰之私鑰）之產生、遞送、保管、失效、更新、廢止等相关作業時，為能順利正確完成，應事先訂定相關處理程序。同時，為防止非法惡意使用，相關作業紀錄等管理文件，應由主管嚴格管理。
另外，如有必要保存失效之金鑰時，亦需明訂保存之作業程序辦法，相關管理文件亦應由主管嚴格管理。
- 3、產生、遞送、保管、失效、更新、廢止等相关作業程序的之明確化，應注意下列事項：
 - (1) 作業應由經授權之指定人員執行。
 - (2) 作業之執行應事先獲得主管核准，為預防操作錯誤，應由多位有權處理之人員共同執行，以達相互牽制之功能。
 - (3) 作業應保存紀錄（包含作業人員姓名、作業日期、作業內容等），並保留一定期間備查。

(三)營運管理

14、實施嚴謹之身分確認

網路銀行服務等是利用通訊網路提供銀行業務交易。此業務係以非面對面之方式執行，對於新開戶交易，客戶本人身分之確認是非常重要的。

營運管理
實施嚴謹之身分確認

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 44	網路銀行之身分確認。
------	------------

網路銀行等以非面對面之方式辦理開戶手續時，應有適當之方法，確認本人身分。

- 1、在網路銀行服務等非面對面之交易型態中，辦理新開戶等作業時，為防止發生非法交易，應利用下列方式，確認客戶本人之身分：
 - (1) 交付具公證性之證明書正本或影本。
 - (2) 將交易相關文件（如金融卡等）以掛號信件直接寄送。
- 2、防止非法交易之對策，請參照 【運 103】。

(三)營運管理

15、無人化服務區之管理

為能使 ATM 及無人銀行能順利運轉，並符合安全政策，在發生犯罪、故障或災害時，應有明確的因應辦法。此處所稱之「無人銀行」是指利用 ATM 等提供無人化服務之營業據點。

營運管理
無人化服務區之管理

適用性分類				
共通	中心	總行	合作	直接
		◎	◎	

運 45	訂定營運管理辦法。
------	-----------

為確保ATM及無人化服務區之安全性與順利運作，應訂定營運管理辦法。

1、ATM等無人化服務區應訂定營運管理辦法，其具體內容可考慮下列項目：

- (1) 現金裝卸之作業程序。
- (2) ATM 操作記錄之保存期限。
- (3) 發生故障之因應方法。
- (4) 防犯監視之方法。

有關防犯監視之方法，請參照【設 113】、【設 137】、【運 47】。

2、行外ATM或無人化服務區應訂定營運管理辦法。

3、對於無人化服務區除訂定營運管理辦法並通告各相關人員外，應考慮下列事項：

- (1) 裝填適當數量之現金，避免現金不足。
- (2) ATM 等各種用紙，應充分裝填。
- (3) 提高自動化服務設備之可用性，應安裝一部以上機器設備，並張貼鄰近設備所在位置。

4、攝影、錄影等防犯監視設備之運用，及交易記錄紙捲等之使用，應明確訂定，其項目舉例如下：

- (1) 訂定交易記錄紙捲之保存期限及保存場所。
- (2) 負責人員。
- (3) 營運辦法。

5、防犯監視設備之營運管理方式，舉例如下：

- (1) 由金融機構自行管理。
- (2) 委託保全公司等委外機構管理。

(3) 安裝於便利超商之 ATM，亦可利用便利超商之防犯攝影機或錄影機，委由便利超商管理。

6、為防範客戶帳號等交易資訊之外洩，可考慮下列之措施：

- (1) 提醒客戶，ATM 之交易明細單據務必攜回。
- (2) 部份 ATM 交易，不列印交易明細單據（如查詢類交易）。
- (3) ATM 之交易明細單據，僅列印部份客戶帳號資料。
- (4) 安裝於便利超商之 ATM，若設紙屑箱應上鎖或附碎紙功能，其回收之客戶交易明細單據，應規定妥善之處理方式。

營運管理
無人化服務區之管理

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 46	訂定監視機制。
------	---------

為發現無人化服務區之異常情況，應明確訂定監視機制。

- 1、為使管制中心能監視無人化服務區之異常狀況，應考慮下列措施：
 - (1) 自動化服務設備故障、破壞等之連線監視。
 - (2) 利用通話設備指導客戶。
 - (3) 委託保全公司處理相關之事項，如顧客之因應或發生犯罪之對應等。
 - (4) 犯罪發生時，向治安機關通報。
 - (5) 故障、災害發生時，向銀行相關人員通報。
- 2、未設置管制中心時，可考慮委託保全公司定期巡邏，作為替代方案。
- 3、應於明顯位置標示受理客戶諮詢之連絡電話。

營運管理
無人化服務區之管理

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 47	明訂防犯措施。
------	---------

為防止於無人化服務區發生犯罪行為，應明確訂定預防及發生時之因應措施。

- 1、在無人化服務區，設備因易遭受破壞及發生盜取現金等非法行為，應明確訂定防犯之方法及犯罪發生時之因應方法。
 - (1) 具體防犯措施列舉如下：
 - a. 委託保全公司簽訂合約定期巡視。
 - b. 委託治安機關定期巡視。
 - c. 利用錄影設備監視。
 - (2) 發生犯罪行為時，具體因應對策列舉如下：
 - a. 由警報設備發出警報(如自動蜂鳴、遠端監視等鳴叫示警)。
 - b. 管制中心立即通報保全公司或治安機關處理。
 - c. 檢視監視錄影設備之記錄。
 - (3) 為防止遺失、遭竊卡片之非法使用，無人化服務區中應明顯標示受理掛失申請之二十四小時服務電話。
- 2、裝卸現金時，應二人以上會同辦理，並注意周遭環境安全，亦可委託保全人員代為處理。

營運管理
無人化服務區之管理

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 48	訂定故障及災害發生時之因應措施。
------	------------------

為使無人化服務區能順利運作，應明確訂定故障及災害發生時之因應措施。

1、無人化服務區設備發生故障時之因應措施舉例如下：

- (1) 明示故障時之連絡方法。
- (2) 明示卡片之返還程序。
- (3) 發生區域性故障，應引導客戶到其他地區進行交易。
- (4) 各相關人員（營業單位、總行、資訊中心、保全公司等）之連絡方法及職責分配。

2、對於災害發生時之因應措施，請參考上述方法訂定。

營運管理
無人化服務區之管理

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 49	備妥相關手冊。
------	---------

無人化服務區相關手冊，應依總行、資訊中心、管制中心、營業單位、保全公司等分別編製，遇有變動應即時更新。

相關手冊如下：

- 1、管制中心之監控手冊。
- 2、防犯手冊。
- 3、故障時處理手冊。
- 4、災害時處理手冊。
- 5、行外自動化服務設備管理手冊。
- 6、與保全公司、治安機關之連絡手冊。
- 7、現金、交易記錄紙捲等管理手冊。

(三)營運管理

16、可攜式電腦設備管理

為確保安全性並順利處理業務，可攜式電腦設備應依規定管理。同時，為預防可攜式電腦設備不當使用、破壞、遺失或被竊等，應有具體之因應對策。

營運管理
可攜式電腦設備管理

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 50	明確訂定可攜式電腦設備管理辦法。
------	------------------

為防止可攜式電腦設備之不當使用，應明確訂定可攜式電腦設備管理辦法。

- 1、此處所稱可攜式電腦設備係指手提端末、攜帶型個人電腦、口袋型電腦、攜帶式端末等可以搬移的端末設備。
- 2、每一部可攜式電腦設備均需訂定其識別用之 ID，並明確訂定該設備之使用者。
- 3、可攜式電腦設備，應存放於指定場所，並明確訂定管理方法。
- 4、應指定可攜式電腦設備之管理人員，並定期清點數量。
- 5、為預防可攜式電腦設備故障，應採取下列方法：
 - (1) 保管序時交易記錄之紙捲。
 - (2) 利用插槽式 IC 卡或記憶卡，儲存備份資料。
- 6、為預防可攜式電腦設備發生被竊或遺失，應有保護所儲存資料之措施，舉例如下：
 - (1) 啟動時需輸入識別碼及密碼，或以特殊的方法啟動設備等，以防止非法使用設備。
 - (2) 存放在可拆卸媒體上之資料檔案，應依其重要性採行適當防止外洩措施。請參照 【技 28】。
 - (3) 若資料檔案需要儲存於可攜式電腦設備，應依其重要性，明確訂定管理辦法。請參照 【運 25】。
- 7、為防止資料外洩、非法使用設備、電腦病毒等之入侵等，機構內部網路之連接或遠端連接運用等，應依規定程序辦理。
外部連接的運用管理，請參照 【運 56】。

(三)營運管理

17、各種卡片管理

為防止各類卡片遭非法使用，卡片之發卡、保管以及遞送等，應依規定程序執行。同時，應對特定帳戶之卡片進行交易時提供監視之功能。另外，對於金錢支付用、簡易貸款用、收受資訊用等各種不同名稱卡片，亦應遵守本基準項目之規定。

營運管理
各種卡片管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎	◎	

運 51	明確訂定卡片管理辦法。
------	-------------

為確保安全性及卡片之發卡、保管、遞送、回收以及作廢等作業順利，應明確訂定卡片管理辦法。

- 1、為防止非法行為，同時對非法行為產生嚇阻之效果，有關卡片的發卡（包含再發卡）、保管、遞送、回收以及作廢，應按規定辦理。
- 2、卡片之發卡、保管、遞送、回收以及作廢等均應指定負責人與經辦員。
- 3、發卡申請書上，若有記載密碼時，該申請書應由主管嚴加保管。
- 4、卡片發卡作業

- (1) 發卡作業中，應有防止密碼外洩之措施。
- (2) 依據發卡申請書內容，編製卡片資料時，其確認作業舉例如下：
 - a. 確認卡片發卡的正確性（包含磁條錄製資料及浮雕資料）。
 - b. 確認發卡數量與申請書張數是否相符。

5、卡片之保管

卡片之保管，應考慮下列項目：

- (1) 卡片（包含未使用、待發送、郵寄退回、待作廢等）應存放在金庫或可以加鎖之櫃中。
- (2) 應設登記簿管理未使用之卡片。
- (3) 卡片製卡後，應依下列方法確認庫存數量。

$$\text{目前庫存量} = \text{製卡前庫存量} - \text{製卡張數} - \text{製卡失敗張數}。$$
- (4) 測試用卡片，應由作業負責人員保管在可以加鎖之櫃中。

6、卡片之遞交方法

卡片遞交客戶時，原則上以掛號辦理，並在發送登記簿中記錄郵寄資料。若在營業單位外製作的卡片，需在營業單位直接面交客戶時，由製卡部門，利用內部掛號信件傳送辦法遞送，並由營業單位在確認本人並取得收據後，交

付客戶。

7、郵寄退回卡片之處理

以掛號信件郵寄的卡片被退回時，應依規定嚴加保管退回卡片，如利用保管登記簿，由主管或其指定代理人負責保管。

另外，若郵件退回的理由為「查無此人」時，原則上予以作廢。

8、廢卡之處理

因製卡失誤或設計變更等原因，無法再使用的卡片，或超過指定期間未領取的卡片或帳戶已銷戶而收回的卡片，應由負責人依規定程序銷毀之。

9、密碼之變更

提供客戶安全簡單之變更密碼方法，並於交付卡片時，詳細解說變更方法。密碼變更方法，舉例如下：

(1) 利用書面申請書，到總行、營業單位申請，經確認客戶本人身分後辦理。

(2) 利用總行、營業單位之 ATM 由客戶本人，直接操作機器設備變更密碼。

10、提醒客戶應注意事項

客戶申請卡片時，應告知客戶使用他人不易猜測的密碼。另外，在交付卡片給客戶時，應同時交付書面說明，以提醒客戶，不可將密碼輕易告訴他人，並應注意卡片、密碼等之保管。

營運管理
各種卡片管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎	◎	

運 52	明確訂定對特定帳戶卡片交易之監視辦法。
------	---------------------

為防止非法使用，應明確訂定在必要時對特定帳戶卡片交易之監視辦法。

- 1、此處所稱「特定帳戶卡片交易」係指與犯罪行為有關，以掌握罪犯所在地為目的，經由治安機關以書面申請的帳戶之卡片交易。
- 2、於監視時，能將該特定帳戶發生卡片交易時之自動化服務機器（ATM）編號顯示於監視設備上。
同時，應事先訂定連絡方法及連絡對象。
- 3、有關監視方法，請參照 【運 60】。
- 4、有關監視功能，請參照 【技 47】。

(三)營運管理

18、客戶資料保護

金融機構應謹慎及適當的保護處理客戶資訊。

營運管理
客戶資料保護

適用性分類				
共通	中心	總行	合作	直接
◎				

運 53	具有保護客戶資訊的措施。
------	--------------

為保護及適當使用客戶資訊，應訂定處理客戶資訊之管理辦法。

- 1、「客戶資訊」係指金融機構為業務上的需要，所收集儲存的客戶基本資料、交易往來明細資料及與客戶有關的所有資訊。
- 2、金融機構基於嚴守客戶資訊秘密的義務，對於客戶資訊的存取、管理負責人員以及資料處理方法等，應有適當的管理辦法。另外，對於客戶資訊管理，請參照【運 10、運 36、運 80、運 88】。
- 3、假設因非法存取等，致客戶資訊外洩，造成客戶蒙受損失的情況，考慮損失賠償責任等，應檢討如何適用保險賠償等之因應措施。

(三)營運管理

19、資源管理

為避免由於各種資源（構成電腦系統之硬體、系統軟體、應用軟體及各類檔案）之性能或容量極限所引起之事故或處理能力之下降，應實施各種資源之管理。

營運管理
資源管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 54	掌握各種資源之能力及使用狀況。
------	-----------------

掌握各種資源之能力及使用狀況，並研擬適當之因應措施。

1、為有效運用電腦資源，應隨時瞭解系統使用狀況，予以適當之調整（Tuning）。電腦資源列舉如下：

(1) 硬體資源

- a. 主機裝置（中央處理機、主記憶體等）。
- b. 週邊設備（磁碟機、磁帶機、印表機等）。
- c. 通訊設備（通訊控制機等）。

(2) 軟體資源

- a. 各種程式。
- b. 各種資料檔。

(3) 網路資源

2、管理資源時，應明定下列程序：

(1) 計畫

擬訂資源管理計畫，應包括資源項目、使用狀況及取樣頻率等。

(2) 實施

利用監控程式等以收集各種資源之使用率、使用容量等資料，並加以分析與評估。

(3) 檢討與改進

當發現系統運轉有阻礙之虞時，檢討資源能量設定參數及資源分配之妥當性，並研擬對策。

3、有關能量及使用狀況之檢討舉例如下：

- (1) 回應時間及批次處理時間是否在預期範圍內。

回應時間係指連線作業系統上處理一筆交易所需時間，而批次處理時間則指批次作業系統上，該工作從開始到結束止所需時間。

此外，對連線作業每一單位時間所能處理筆數，及因批次處理延誤影響次日連線作業開始時間等狀況亦須加以檢討。

- (2) 掌握各種機器之能量極限，定期實施使用狀況之確認。

應確認各種機器之使用狀況，並比較能量極限，事先考慮因應對策。

- (3) 掌握各種檔案可使用容量，定期實施使用狀況之確認。

- (4) 掌握各程式之使用頻率，依其高低檢討程式常駐或非常駐等設定之妥當性。

(三)營運管理

20、外界連接管理

為安全及正確執行與外界之連接，並防止資料之洩露或遭非法使用等，凡有關透過連線而與顧客做資料授受者，應有確認連接對方為合法者之功能，並實施適當的管理。

營運管理
外界連接管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 55	明確訂定連接契約之內容。
------	--------------

為正確及安全執行與外界之連接，凡透過連線執行資料授受有關之契約，應在契約中明確訂定連接方法、資料格式及資料內容等。

1、簽訂透過連線執行資料授受之契約時，應充分掌握契約內容，避免發生誤接情事。為此可考慮內容之標準化，如編製連接條件表格等。

2、在有關連接契約中，應明確劃分下列事項：

(1) 使用通訊線路

- a. 專用數據網路。
- b. 高速數位網路。
- c. 電信電話網路。
- d. 整體服務數位網路 (ISDN 網路)。
- e. 電路交換式數據網路。
- f. 分封交換式數據網路。
- g. 訊框通訊網路 (Frame Relay 網路)。
- h. ATM 通訊網路 (ATM 網路)。
- i. 網際網路通訊網路。
- j. 衛星通訊網路。

(2) 連接設備

- a. 電話。
- b. 語音儲存。
- c. 語音傳送。
- d. 傳真機。
- e. 電傳打字機。
- f. 電腦。

- g. 個人電腦。
- h. 其他。
- (3) 傳輸控制程序
 - a. 跨行系統通訊協定。
 - b. FTAM (OSI「開放系統間相互連接」中規定之檔案傳送國際標準規範)。
 - c. 其他。
- (4) 收發電信資料之格式 (Data Format)。
- (5) 資料內容
 - a. 薪資轉帳。
 - b. 綜合轉帳。
 - c. 公用事業費用。
 - d. 退休金給付。
 - e. 股息、股利配發。
 - f. 保險金、保險費用。
 - d. 其他。
- (6) 確認對方方法
 - a. 利用公共電路之傳真機及電話之連接：
 - (a) 首次申請及變更時以電話確認電話號碼。
 - (b) 首次申請及變更時以傳真確認電話號碼。
 - (c) 以回電方式確認連接之對方。
 - (d) 以通知服務方式確認連接之對方。
 - (e) 以密碼或識別號碼確認連接之對方。
 - b. 電腦、個人電腦、家庭用簡易端末等之連接：
 - 以確認對方專用代碼、通行碼或使用檔案基碼 (File Access Key)
 - 做連接對方之確認。
- (7) 無法傳輸時之對應方法。

營運管理
外界連接管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 56	應明確訂定與外部連接之營運管理辦法。
------	--------------------

為防止資料外洩、非法存取等，應明確訂定與外部連接之營運管理辦法，並確實執行確認連接對象身分、確認連接條件(如登錄密碼等)及變更之管理。

- 1、透過電路連接執行資料之授受時，應按契約所列的方法確認對方，並有適當的管理辦法。
- 2、特別對於透過網際網路或公眾通訊線路等之遠端存取應用，或具入侵機構內部網路之高危險性不特定多數使用者之網路連接時，應明確訂定網路連接相關營運之管理辦法。
- 3、營運管理辦法，舉例如下
 - (1) 連接對象之確認及限制
 - a. 在連接時，應確認對象之使用者身分及端末設備。確認的方法，請參照【技 27、技 35】。
 - b. 確認身分用的識別碼及密碼，其登錄、變更及檢核確認，應依規定程序辦理，其結果應經確認檢核。管理辦法，請參照【技 26、運 17】。
 - (2) 外部連接之應用管理

機構內部網路與網際網路的連接或由出差地點利用遠端連接狀況，應訂定下列各項目，並依作業情況，加以限制使用。

 - a. 有權使用者。
 - b. 可以使用的時段。
 - c. 使用的目的。
 - (3) 連接之監視

為防止非法存取或資訊外洩，應保存連接的記錄，並進行下列的監視作業。

 - a. 由外部對內部的連接。

b. 由內部對外部的連接。

監視的方法，請參照 【技 37、技 45】。

(4) 認證設備遺失時之對策

連接對方之確認身分用認證設備（如 Access token、IC 卡等）在遺失時之因應對策。

(5) 對安全漏洞的對應

對於與外部連接的伺服器或路由器所載入的軟體，應隨時蒐集其安全漏洞的資訊，並進行適當的軟體更新作業。

4、對於外部非法行為所造成的損失賠償責任、利益喪失、業務復原所需費用等，應研究採用保險或其他適當方式，以降低營運風險。

(三)營運管理

21、機器設備之管理

為使構成資訊系統之各種機器故障減至最低程度，並防止非法使用或遭破壞，應訂定機器管理及維護方法，並明確規定管理負責人之權責。

營運管理
機器設備之管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 57	應明確訂定資訊設備管理辦法。
------	----------------

為防止資訊系統之各種設備發生故障、非法使用、破壞、遭竊等，應明確訂定資訊設備管理辦法。

1、對於機器設備之管理，應指定管理負責人員，並依下列事項加以管理：

- (1) 除作業相關人員外，應不易接近機器設備。
- (2) 資料輸入設備（如端末機等）、輸出機器（如印表機等）重要之伺服器設備等，應限有權之作業人員來操作。
- (3) 對於系統之構成設備、使用型態、使用狀況、設備數量等，應隨時掌握。

2、前項事項之具體實施方法，請參照下列之實例：

- (1) 防止非相關人員接近設備：
 - a. 電腦機房及重要伺服器設備安裝場所，應確認進出人員資格，請參照【運 11】。
 - b. 上鎖之管理方法。請參照【運 11】。
- (2) 賦予機器設備操作之資格：
 - a. 機器設備操作者之資格確認。請參照【運 19】。
 - b. 利用交付 ID 或鑰匙，作為設備操作之權限賦予。請參照【運 16、18】。
 - c. 端末權限規範機制之設定。請參照【技 38】。
- (3) 容易攜出之設備，應注意預防盜竊：
 - a. 利用纜線等固定機器設備。
 - b. 收存於上鎖之機架。

3、機器設備為維修等，需攜出外部時，為防止資料之外洩，宜訂定設備送修

時之管理辦法。

- 4、因機器設備之非法使用、破壞、遭竊等所產生之損害或業務上喪失利益、業務上維持作業所需費用等，儘可能檢討投保理賠之適用性。

營運管理
機器設備之管理

適用性分類				
共通	中心	總行	合作	直接
	○	○	○	

運 58	保護通訊網路相關設備之措施。
------	----------------

為防止設備之非法使用、破壞、遭竊等，對於構成處理重要資料之系統通訊網路設備應有適當之保護措施。

- 1、在處理重要資料之系統中，通訊網路相關設備若發生非法使用、破壞、遭竊時，其影響非常重大。因此，通訊網路設備亦應比照伺服器等設備設置場所之管理辦法(請參照 【運 57】)管理之。
- 2、有關通訊網路之設定資訊，請參照 【運 31、32】。

營運管理
機器設備之管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 59	明確訂定設備維護辦法。
------	-------------

為防止資訊系統之各類機器設備發生故障，應確實執行維修保養作業，並確實掌握維修之內容及結果。

1、資訊系統設備之維護，分為定期維護及臨時維修，應考慮設備使用狀況、故障修復之急迫性及廠商維修之體制等，編製設備維護計畫，維護計畫之內容應事先擬定下列各事項。請參照【技 1】。

(1) 維護保養之設備名稱。

(2) 維護保養之週期。

(3) 維護保養之內容。

並在設備維護保養後，應掌握其內容及結果。

2、為避免機器設備遭竊、破壞及資訊之竊取等，機器設備依其重要性，應由管理該項設備之單位指派專人會同維護設備。

3、為能隨時聯絡廠商(包含專業維護公司)，有關廠商之公司名稱、維修作業負責人員姓名、電話號碼、負責維修範圍等，應確實掌握。

4、有關確保維護人員行蹤之方法如下：

(1) 需要時以電話等聯絡方式召集。

(2) 電腦廠商提供常駐維護人員。

5、關於維護保養，在管理運用上，建議注意下列事項：

(1) 建立報告維護內容之制度。

(2) 維護作業聯繫會議。

(3) 維護作業之統計分析。

(4) 訂定維護計畫。

(5) 前次維護作業後，設備故障、錯誤記錄(Error Log)之分析。

6、維護檢查之程序，應考慮下列各點：

- (1) 應調整相關設備（如空調設備、配電設備等）之維護檢查程序。
- (2) 應考慮 ATM 等機器假日營業與夜間營業等因素，調整維護檢查程序。

(三)營運管理

22、營運監視

為能早期發現異常狀態，應經常監視系統運轉之狀況。

營運管理
營運監視

適用性分類				
共通	中心	總行	合作	直接
◎				

運 60	建置完善之監視體制。
------	------------

為能早期發現系統之異常狀況，應訂定包含監視對象、監視內容及監視方法等相關機制。

1、為能早期發現系統之異常狀況以及非法使用系統，應明確訂定包含下列事項之監視機制。同時，對於發現異常狀況或非法使用時之因應辦法，亦需明確訂定。

(1) 監視對象、內容：

a. 為早期發現系統之異常狀況：

(a)連線作業營運狀況。

(b)中央處理器、輸出入通道裝置、檔案裝置等之運轉狀態。

(c)各業務連線作業相關通訊控制設備、通訊線路及營業單位端系統等之運轉狀況。

(d)ATM 等之運轉狀況。

(e)整批作業之進度與處理狀況。

b. 發現、防止非法使用之監視：

利用系統控制台記錄 (Console Log)、系統運轉記錄 (System Log) 等之分析及監視，應掌握下列各事項之狀態。

(a)確認作業處理狀況：

i. 確認是否有投入預先排定作業以外之其他作業。

ii. 利用系統操作指令，確認作業處理之狀態。

(b)確認系統使用時間或使用次數有無異常。

(c)確認對檔案之存取狀況：

i. 未經授權之使用者。

ii. 存取權限內檔案存取之狀況。

(2) 監視方法：

指定系統監視人員，利用集中監視之方式，一元化之監視作業。若系統操作係委外處理時，應事先訂定應提供定期報告及發現異常或非法使用情況時之即時報告等之作業辦法。

a. 系統異常狀況之早期發現：

(a)使用主控台 (Console) 或監控板。

(b)利用系統異常時之警示裝置監視。

(c)利用監視工具軟體。

(d)利用廠商提供之遠端監視系統。

b. 發現或防止非法使用之監視：

(a)使用監視工具軟體。

2、 有關監視機能，請參照 【技 18、技 20、技 45】。

3、 有關偵測故障功能，請參照 【技 21】。

4、 故障時、災害時之因應對策，請參照 【運 63、運 65】。

(三)營運管理

23、電腦機房、媒體儲存室之管理

為防止非法入侵、攜入危險物品、非法攜出物品等，應嚴密管理電腦機房、媒體儲存室等重要房間之進出。

營運管理
電腦機房、資料儲存室之管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 61	嚴密管理進入後之作業。
------	-------------

為防止非法入侵、攜入危險物品、非法攜出物品等，應嚴密管理電腦機房或媒體儲存室等重要房間之進出。

- 1、 電腦機房及媒體儲存室、中央控制室（中央監視室、防災中心）及設置重要伺服器之場所應經覆核主管核准後始得進入，人員進出應留下紀錄並嚴加管理後續之作業處理。
- 2、 人員進入後之作業管理具體實例，如下列所示：
 - （1）對重要房間，人員進入後之作業，應指派人員監視並陪同處理。
 - （2）除許可進入之區域之外，應限制其進入。
 - （3）未使用之區域應上鎖，並定期巡視確認。
 - （4）攝影機、錄影機、個人電腦等記錄用設備，未經許可不得使用。
- 3、 總行、營業單位等設置重要伺服器之場所，應比照上述之準則，對進入者之作業嚴加管理。

(三)營運管理

24、故障災變之因應對策

為將資訊系統故障與災變對顧客、總行、營業單位之影響降至最低，同時儘早完成復原作業，應訂定故障災變之因應對策。

營運管理
故障災變之因應對策

適用性分類				
共通	中心	總行	合作	直接
◎				

運 62	明確訂定相關人員之聯絡程序。
------	----------------

在故障、災變發生時，為迅速確實聯絡相關人員，應事先訂定人員聯絡之作業程序。

1、應事先訂定各種故障、災變發生時，必須聯絡召集之人員名單，並定期檢討其適宜性。同時，為預防聯絡不到相關人員，應指定正副兩名以上之人員，並應事先告知所有人員相關部署名單以及單位內部聯絡之作業程序等。另外，對於發生重大之故障、災變時，應向經營階層主管呈報。

(1) 資訊中心之相關人員：

- a. 資訊中心營運負責人員或管理人員。
- b. 系統負責人員或管理人員。
- c. 廠商維修部門之負責人員。
- d. 聯絡總行、營業單位之負責人員。
- e. 聯絡外部共用系統之負責人員。

(2) 總行、營業單位之相關人員：

- a. 總行、營業單位之負責人員。
- b. 向資訊中心聯絡之負責人員。
- c. 廠商維修部門之負責人員。
- d. 保全公司。
- e. 公關負責人。

2、同一人員應訂定一個以上之聯絡方法，其方式可參考下列所示：

- (1) 電話。
- (2) 呼叫器。
- (3) 傳真機。
- (4) 另外之連線系統，以廣播方式通報。

(5) 無線通訊。

(6) 個人電腦（利用網際網路等）。

(7) 語音信箱。

(8) 手機。

3、自動化服務機器等之故障可能發生於無人監視時段（夜間、星期假日、國定假日等），聯絡方法應另外訂定，並定期檢討適宜性。

4、為能對顧客提供正確之資訊，發佈新聞等應設置統一之窗口，並指定發言人提供各種資訊（系統故障狀況、復原資訊等）。

營運管理
故障災變之因應對策

適用性分類				
共通	中心	總行	合作	直接
◎				

運 63	明確訂定故障災變時之復原作業程序。
------	-------------------

應明確訂定因故障或災變，造成資訊系統無法正常運作時之復原作業程序，此復原程序應與災變備援計畫之內容具相容整合性。

1、故障災變之復原作業程序，是指因系統故障或災變，造成無法正常運作時，為復原資訊系統所需要之一連串作業程序，應事先明確訂定。

對於下列之故障，應事先編製資訊系統故障復原作業程序：

- (1) 資訊系統裝置之故障。
- (2) 端末機器設備之故障。
- (3) 相關週邊設備（電源、空調、給水排水設備等）之故障。
- (4) 通訊線路之故障。
- (5) 軟體系統之故障。

2、在明確訂定故障災變之復原作業程序時，應將下列事項納入考慮之要素：

- (1) 將影響縮小至局部化。
- (2) 切換備援系統。
- (3) 檔案完整性之確認程序。
- (4) 確定復原作業所需人員，並賦予必要之作業權限。
- (5) 對總行、營業單位之業務影響範圍及復原作業預估之聯絡程序。
- (6) 對外部系統影響程度之確認。

3、故障災變時使用之備援系統（包含備援中心之設置等）應定期確認是否能正常啟動營運。

4、有關故障災變時之復原作業，請參照 【技 22 ～ 24】。

營運管理
故障災變之因應對策

適用性分類				
共通	中心	總行	合作	直接
◎				

運 64	調查、分析發生故障之原因。
------	---------------

為迅速回復資訊系統之作業功能，應調查、分析發生故障之原因。同時，應記錄故障原因，作為故障原因之統計分析，以避免再次發生問題。

- 1、為迅速回復資訊系統之作業功能，應訂定故障原因之調查分析方法。具體之實例，請參照 【技 20、技 21】。
- 2、為能及時發現故障，或於故障發生後能及早掌握原因，可考慮安裝廠商提供之遠端診斷系統，以加速問題之排除。
- 3、為防止故障之發生，應收集、分析發生故障之各種資料，並調查發生之原因，作為制定故障對策之依據。

(三)營運管理

25、制定災變備援計畫

於資訊系統發生故障或災害時，為使相關業務能在短時間內回復正常運作，應以假設事件為基礎，擬定災害備援作業計畫（緊急應變計畫），另於設置之安全設備應定期檢查，並加強員工使用訓練；另應制訂資訊安全緊急應變處理等相關程序，並定期演練及檢討改善。

營運管理
制定災變備援計畫

適用性分類				
共通	中心	總行	合作	直接
◎				

運 65	制定災變備援計畫。
------	-----------

對於無法預測之事故、災變及重大損害等，造成業務執行之困難時，為將損害範圍及對業務之影響降至最低，並能儘速復原，應事先制定災變備援計畫（緊急應變計畫）。

- 1、災變備援計畫，是指金融機構之資訊系統因無法預測之事故、災變及重大損害等，造成業務執行困難時，為將損害範圍及對業務之影響降至最低，並能迅速有效回復業務處理，於事前制定之「緊急應變計畫」。
- 2、於設置之安全設備應定期檢查，並加強員工使用訓練。
- 3、應制訂資訊安全緊急應變處理等相關程序，並定期演練及測試。
- 4、對於無法預測之事故、災變及重大損害等，應事先假設數種可能發生之情況，擬定災變備援計畫，舉例如下：
 - (1) 資訊中心、總行、營業單位全部或部分受災。
 - (2) 資訊系統設備受到破壞或損壞。
 - (3) 端末機器設備受到破壞或損壞。
 - (4) 相關設備（電源、空調、給水排水設備等）受到破壞或損壞。
 - (5) 通訊線路中斷、通訊設備損壞。
 - (6) 公共基礎建設故障（停電、斷水、交通中斷等）。
 - (7) 軟體之故障。

另外，因天災造成交通中斷而發生員工無法上班執勤之情況，應由如何維持作業之觀點來考慮應變計畫。
- 3、在制定災變備援計畫時，應考慮之內容，列舉如下：
 - (1) 假設緊急情況之發生，評估機構內各種業務及設施所受到之影響程度。

- (2) 評估緊急狀況下，業務持續之優先順序。
- (3) 受災據點及災變處理總部在緊急狀況下臨時組織之編制（包含災變備援計畫啟動之權限）及成員等，應明確訂定。
- (4) 在緊急狀況發生時，確保顧客與員工之安全、保護資產、掌握受災情況等應變措施應明確訂定。
- (5) 業務、顧客服務中斷時，將中斷造成之損失降至最低，在業務無法正常持續之緊急情況下，對重要業務之臨時性處理措施應明確訂定。
- (6) 為儘速排除問題，回復正常營運，應明確訂定必要之措施。
- (7) 確立計畫之持續管理體制，實施定期之演練及訓練，須依演練之結果，檢討計畫內容，適時修正計畫內容，以符合實際需要。

4、在災變備援計畫制定後，應適時加以檢討修正。時機如下：

- (1) 重要業務處理內容有變更修改時。
- (2) 過去在災變備援計畫中未被重視之業務，對機構之重要性提升時。
- (3) 在執行上述業務之前提，組織、據點設施、基礎建設等條件發生變動時。

5、組織圖或緊急聯絡網等應隨時維持最新之狀態。

6、對於災變備援計畫或其他重要計畫內容之檢討修訂，應獲得經營層級主管之認可。

7、災變備援計畫應隨時保存於應變總部、各營業據點、災變備援中心等必要之場所。

8、發生故障、災害，必須執行系統復原或切換備援系統之作業時，有可能會造成安控層次之下降，因此在發生前述事件時，應注意系統安控應維持日常作業之水準。

9、在故障、災害發生時，可能產生之損失賠償責任、利益喪失、維持業務處理之費用等，儘可能檢討是否適用於投保理賠範圍。

10、設備及技術面之復原對策，以及預防故障、災害發生之應用訓練等，請參考下列之基準項目。

- (1) 環境 【設 1】。
- (2) 周邊 【設 2、設 3、設 4、設 7 ～ 9】。
- (3) 結構 【設 10 ～ 13、設 31 ～ 36】。

- (4) 門窗 【設 14、設 17 ～ 19、設 28 ～ 30】。
- (5) 內部裝潢 【設 20、設 21】。
- (6) 位置 【設 22、設 25 ～ 26】。
- (7) 設備 【設 37 ～ 44】。
- (8) 資訊設備、雜項設備、備品 【設 48、設 50 ～ 51】。
- (9) 電源室、空調室 【設 52、設 54 ～ 60】。
- (10) 電源設備 【設 62 ～ 71】。
- (11) 空調設備 【設 74 ～ 79】。
- (12) 監控設備 【設 80、設 81】。
- (13) 通訊線路相關設備 【設 82、設 83、設 83-1】。
- (14) 硬體設備之備份 【技 2 ～ 6】。
- (15) 故障之即時復原 【技 22 ～ 24】。
- (16) 教育、訓練 【運 80 ～ 84】。

(四)系統開發、變更

1、硬體、軟體之管理

為能確實對應系統結構之變更，安裝建置之硬體設備及軟體組成等，應以資產清冊等加以管理。

系統開發、變更
硬體、軟體之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 66	應實施硬體、軟體之管理。
------	--------------

為能確實執行系統之安裝建置、變更、報廢等，應實施硬體、軟體之組成架構、版本數量等之管理。

1、為能適當之管理資訊系統之硬體、軟體，應建置財產登記帳等。

2、應管理之項目，列舉如下：

(1) 硬體設備：

- a. 硬體設備名稱。
- b. 製造廠商及型號名稱（型號）。
- c. 識別用機器序號。
- d. 費用。
- e. 安裝日期。
- f. 資產管理編號或租賃契約編號。
- g. 最初安裝地點。
- h. 目前安裝地點。
- i. 負責保管人姓名。
- j. 維護廠商名稱。

(2) 軟體系統：

- a. 自行開發之軟體：
 - (a) 程式名稱。
 - (b) 最初開發日期。
 - (c) 最終更新日期。
 - (d) 使用單位名稱或使用人姓名。
- b. 購入之軟體：

- (a)軟體名稱。
- (b)製造廠商或契約代理商名稱。
- (c)購入或使用權契約之區分。
- (d)費用。
- (e)安裝日期。
- (f)資產管理編號。
- (g)版本編號。
- (h)序號。
- (i)使用單位名稱或使用人姓名。
- (j)維護廠商名稱。

- 5、資訊中心或系統主管單位，應收集廠商對作業系統等基本軟體所提供之版本及修訂資訊，以作為安裝最新修訂版本軟體之依據。
- 6、如個人電腦等，變更用途再利用時，應事先檢查是否有電腦病毒或非法軟體混入，以免發生問題。
 - (1) 電腦病毒等非法軟體之防禦對策，請參照 【技 49】。
 - (2) 電腦病毒等非法軟體之偵測對策，請參照 【技 50】。
- 7、硬體設備之損壞或軟體之錯誤（Software Bug）及非法軟體等，引起系統故障所造成之損害賠償責任、利益喪失、持續業務處理之費用等，儘可能檢討是否適用於投保理賠範圍。

(四)系統開發、變更

2、系統開發、變更之管理

為確保系統開發及其內容變更之正確性，兼顧系統之安全性，應明確訂定系統開發、變更之作業程序、測試環境之建置等整合性之管理機制。

系統開發、變更
系統開發、變更之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 67	明確訂定開發、變更之作業程序。
------	-----------------

為確保系統開發、變更內容之正確性，應明確訂定開發、變更之作業程序。

- 1、為提升系統可靠度，並確保內容之正確性，在系統開發、變更之各階段，其確認與驗證等應按規定程序辦理，開發及變更程序項目如下：
 - (1) 新系統之開發或既有系統之變更，其要件檢討、規劃之核可程序。
 - (2) 在設計、程式撰寫、測試等各階段之驗證及核可程序。
 - (3) 開發、變更作業完成後之驗證與核可程序。
 - (4) 對發生故障、災害時之因應程序等，亦需驗證與核可程序，請參照【運 15、運 65】。
- 2、為能適切管理系統開發工作，應明確指定專案負責人，訂定有效率開發程序，確實實施專案管理相關作業。
所謂專案管理，是指在系統之開發、變更作業所賦予的時間與資源（人、物、金錢等）範圍內，為求合理之推展，確實有效達成目標，依照規定之作業程序，充分掌握專案之進行狀態，適當採取因應措施。
- 3、為能提升系統之可靠度，提升軟體可靠度之對策是非常重要的。有關確保軟體品質之方法，請參照【技 7 ～ 15】。

(參考 1) 在開發各階段之管理要點，如下列所示：

1、系統要件之檢討、規劃

- (1) 在機構內設立組織橫向之審議部門，負責審議開發案件是否值得進行。
- (2) 以開發案件之驗證、核可規則評估資訊系統之投資效果及其風險，必要時應呈報經營階層主管。
- (3) 確認使用者之需求要件是否足夠，需求申請文件是否以登記簿管理。

2、系統設計

- (1) 在各階段編製之設計書等文件，其內容是否依照標準化規則編製。
- (2) 設計內容是否經過檢核。

3、程式撰寫

- (1) 程式撰寫作業若委外辦理時，是否明確規範詳細作業指示、文件交接、內容驗證、交付清單、交付文件等事宜。
- (2) 程式規格之驗證、核可等是否依照規定之程序，適切的執行。另外，對規格之變更，是否經由有權主管核定。

4、測試

- (1) 測試方法、確認之程序是否已明確訂定，並遵守辦理。
- (2) 對未解決之錯誤 (BUG)、問題、待決事項等等是否予以管理並訂定對策，如使用錯誤 (BUG) 管理表等。
- (3) 是否由使用部門參與製作測試資料、參加測試並認可。

5、系統運轉

- (1) 是否提供使用部門必要之手冊、辦理講習以及作業初期指導與問題之追蹤。
- (2) 是否備妥系統運作時之管理制度及系統管理文件。

(參考 2) 為系統開發之效率化，專案管理是非常重要的，其基礎程序之明確化，專案計劃與執行管理之成功導入，應對相關管理知識體系具相當認識。

系統開發、變更
系統開發、變更之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 68	建立測試環境。
------	---------

為確保正式作業系統之安全性，應建立對正式作業系統不會造成影響之測試環境。尤其測試大型系統時，應制訂包括相關人員在內之測試制度。

- 1、系統開發、變更相關之測試，應事前充分測試，以免影響正式作業。因此，正式作業之系統設備應與測試用之系統設備完全區隔。
- 2、建立測試環境之考慮事項如下：
 - (1) 測試環境之設定，不得影響正式作業環境。
 - a. 測試用檔案與正式作業用檔案要分開。
 - b. 應採取對策以防止自測試用端末機擷取正式作業資料。
有關防止非法存取系統及資料，請參照 【運 16 ～ 15】。
 - c. 應避免在正式作業系統中進行測試。
應儘量避免於正式作業系統中進行測試。必要時，應先評估測試之影響程度，依此設定測試限制。
 - d. 若使用正式作業機器測試時，應明定將機器轉回正式作業系統之程序，並確認有無對正式作業發生影響。
 - e. 須聯絡營業單位在業務處理方面應注意之事項。
如測試涉及營業單位時，為避免與現行系統發生關連而產生混亂，須聯絡辦理下列事項：
 - (a) 端末硬體、軟體之轉換。
 - (b) 使用表單等之管理。
 - (c) 業務處理程序、手冊類之管理。
 - (2) 為順利轉移至正式作業營運，應有能充分執行測試之測試用環境。
 - a. 應確保開發、測試用資源。

最好能確保足夠之開發、測試用電腦等資源，此時，應注意測試用之媒體或檔案未受到電腦病毒之感染。

b. 辦理外部系統（如跨行系統）之連接測試時，事先須就測試日程、測試內容、測試範圍與工作分配等做充分之聯繫與協調。

c. 正式作業之模擬測試環境。

有關測試之種類，請參照 【技 11】。

(3) 利用開放網路進行測試時，應注意之事項：

若測試之進行，需要與開放網路連接時，應設有防止非法入侵之功能。

請參照 【技 43】。

系統開發、變更
系統開發、變更之管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 69	明確規定轉入正式作業之轉換程序。
------	------------------

確保正式作業系統之安全，轉入正式作業時應明確規定其轉換程序。

- 1、為安全而確實辦理轉入正式作業，應明定轉換程序，以確保資訊中心與使用部門間之協調，防止發生事故。
- 2、移轉為正式作業之轉換程序應考慮事項，如下列所示：

(1) 轉換程序之明確化：

轉換作業程序以及切換點（Cutover）之判斷基準應明確。同時應考慮在轉換作業中發生問題時，能回復到原有之舊系統。

(2) 對營運部門與使用者之說明：

為轉換後能順利營運，應提供營運部門系統營運必要之文件手冊，並詳加說明。另外，對使用者應說明移轉之時間點、變更內容及限制事項等。

(3) 應實施轉換作業之排演：

對於系統之轉換，應依其必要性實施轉換作業之排演，以確認轉換作業能安全、確實進行，並明定轉換所需時間及其正確性，確認作業進行之檢測要項。

具體事項，可以考慮下列事項：

- a. 檔案移轉之確認測試。
- b. 轉換作業程序之確認測試。
- c. 通訊線路連接之確認測試。
- d. 操作程序之確認測試。
- e. 餘額查詢等之確認測試。

(4) 轉換作業之實施：

轉換作業小組依照轉換程序進行轉換作業。為防發生異常情況，應事先設定轉換作業中止、復原作業等之判斷點，以備必要時能迅速回復舊有系統。

(5) 最終之確認：

轉換後，應與使用部門會同辦理餘額核對、報表確認等事項。

(四)系統開發、變更

3、文件管理

為使開發、變更作業順利進行，並防止篡改或不當使用等，應訂定有關系統開發及變更文件之管理方法。

系統開發、變更
文件管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 70	格式之標準化。
------	---------

為使開發及變更作業順利，應將在系統開發及變更各階段所使用之文件格式予以標準化。

為使編製文件或驗證文件內容時，易於發現錯誤，同時提高系統之品質，應對系統開發及變更各階段所使用之文件格式予以標準化，應明確規定如下各點，並配合業務需求之變動隨時檢討：

- 1、 文件之名稱、格式、記述要項、範例。
- 2、 各文件之歸檔方法、保存方法、保管場所、保管者。
- 3、 各文件標準化之認可方法。

系統開發、變更
文件管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 71	明確規定管理辦法。
------	-----------

為防止篡改及不當使用等，應訂定規格書等設計文件之保管方法。

- 1、規格書等有關系統設計與管理等文件，為防止竄改及不當使用，其保管與變更等之管理應按規定程序辦理。
- 2、管理之具體實例，如下列所示：
 - (1) 各種文件使用應設簿登記並管理。
 - (2) 明確訂定各種文件別之保存期限。
 - (3) 有關文件之編寫、追加、變更及作廢等，應留存紀錄以利管理。
 - (4) 重要文件應保存於指定之場所（如能上鎖之保管室或櫃子）。
 - (5) 重要文件應限定可閱覽之人員，並訂有限制複印之措施。
 - (6) 轉交給使用部門時，按規定手續簽收，收回時亦同。
- 3、非紙本文件（存放電子媒體之文書檔案）之保管管理，亦應以相同之方式處理。

(四)系統開發、變更

4、套裝軟體之引進

引進套裝軟體時，為能順利進行系統開發、修改等，應建立套裝軟體適用性之評估制度，並明確訂定套裝軟體之應用及管理。

系統開發、變更
套裝軟體之引進

適用性分類				
共通	中心	總行	合作	直接
◎				

運 72	套裝軟體之評估制度。
------	------------

引進套裝軟體時，為能順利進行系統開發、修改等，應由系統開發部門及使用部門（營業單位）等單位共同評估。

- 1、引進套裝軟體時，應經系統開發部門、營運部門及使用單位（總行、營業單位等）之綜合評估。
- 2、引入套裝軟體時，評估之項目舉例如下：
 - (1) 套裝軟體本身之評估項目：
 - a. 業務需求之適應。
 - b. 效能（回應時間、處理時間等）。
 - c. 使用之難易度。
 - d. 文件完整性。
 - e. 擴充性。
 - f. 彈性。
 - g. 安全保護功能。
 - h. 套裝軟體供應者之支援能力。
 - i. 已使用單位之反應。
 - (2) 與現行系統整合性相關之評估項目：
 - a. O S 與 D B M S 、中介軟體（Middleware）之相容性：
 - (a) 能在現行作業平臺執行。
 - (b) 版本不符時，可能無法整合。
 - b. 輸出入規格：

資料輸入方法及輸出形式等（報表、存摺、傳票、檔案格式）。
 - c. 資料內碼體系：

中文內碼、字型、外字處理等。

- 3、為因應必要之客製化及未來需求，應確認廠商是否提供套裝軟體之程式原始碼。

系統開發、變更
套裝軟體之引進

適用性分類				
共通	中心	總行	合作	直接
◎				

運 73	明確訂定使用、管理之方法。
------	---------------

為順利辦理套裝軟體引進後對應事故或擴充功能，應明確訂定套裝軟體之使用與管理方法。

- 1、為使發生問題時之影響減至最低，應明定套裝軟體提供者之聯絡方式、維護程序及確認事項（如問題現象之掌握方法、緊急處置方法等）。
- 2、為防範非法使用，減少問題之發生，使用權之管理、軟體版本之管理體制應明確化。
- 3、為使系統能順利運作，軟體維護程序及套裝軟體廠商之支援體系，應明確化。
- 4、套裝軟體之教育訓練、諮詢等服務項目，應明確化。

(四) 系統開發、變更

5、系統之報廢

系統報廢時，對機密資料的保護、隱私權的保護、防止非法行為等，應確實遵守報廢計畫及相關作業程序等之規定。

系統開發、變更
系統之報廢

適用性分類				
共通	中心	總行	合作	直接
◎				

運 74	擬定報廢計畫、作業程序。
------	--------------

為使系統報廢能順利、確實且安全，應擬定包含防範非法行為與保護機密等措施之計畫與作業程序。

- 1、為能順利、確實、安全的進行系統報廢作業，應擬定報廢計畫與報廢作業程序。
- 2、資訊系統報廢前，應事先知會使用單位、系統資產管理單位及報廢作業相關單位等。
同時，在執行報廢作業之前，應先確認該系統作業已確實完全終止運作。
- 3、報廢計畫，應包含下列事項：
 - (1) 報廢目的。
 - (2) 報廢對象範圍。
 - (3) 報廢時間。
 - (4) 報廢方法。
 - (5) 會計帳資產之處分方法。
- 4、在報廢作業中，應有機密資料保護措施。請參照 【運 75】。

系統開發、變更
系統之報廢

適用性分類				
共通	中心	總行	合作	直接
◎				

運 75 應具有防止資料外洩之措施。

為保護機密或個人資料，防止非法行為，在系統報廢時，應有防範由機器設備洩漏資料之措施。

- 1、在系統報廢時，考慮該報廢系統的重要性，應有保護機密資料、隱私權以及防範非法行為的措施。
- 2、為確實執行報廢作業，報廢方法、報廢時間應明確，報廢作業完成後，應呈報報廢紀錄，並獲得負責人之核可。
- 3、硬體設備報廢時得採取之措施，列舉如下：

對於租賃契約期滿，需將設備退還租賃公司時，亦需參考下列方式處理。

 - (1) 移除軟體(Uninstall)。
 - (2) 刪除密碼等設定檔案。
 - (3) 徹底刪除硬碟上資料。
 - (4) 破壞 I C 卡等。
 - (5) 消磁。
- 4、報廢軟體系統或資料檔案時，得採取之措施，列舉如下：
 - (1) 由系統移除 (Uninstall)。
 - (2) 磁性媒體予以消磁或破壞。
 - (3) 燒毀或裁碎程式原始碼紙本。
- 5、報廢文件時得採取之措施，列舉如下：
 - (1) 燒毀或裁碎。
 - (2) 磁性媒體予以消磁或破壞。

6、若委託第三者銷毀時，應簽訂保密合約，依照上述方法辦理。

(五) 各種設備管理

1、維護管理

為使資訊系統順利運轉，應明確訂定電源、空調、供/排水、防災、防犯、監視、通訊線路等相關設備之管理及維護辦法。

各種設備管理
維修管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 76	明確規定管理辦法。
------	-----------

為使資訊系統運轉順利，應明確規定管理辦法，指定設備管理負責人員，依規定管理設備。同時，對於發生故障災變時之因應對策亦應明確規定。

1、為確保資訊系統（包含端末設備）之順利運轉，相關設備之電源、空調、供/排水、防災、防犯、監視及通訊線路等關連設備，應明確指定管理負責人員，依規定管理。

同時，為能將資訊系統受到的影響降至最低，對事故災變發生時之因應對策亦需明確訂定。

2、為確保端末設備、ATM 等自動化機器之順利運轉，應明確訂定電源設備、各種感應器、攝影機等防護設備之管理辦法。

同時，為確保災害發生時，防護設備能正常運作，滅火設備、監視設備等亦須適當管理。

另外，在增設OA機器、個人電腦等設備時，應掌握電源容量等相關設備的能力。

3、管理方法內容，舉例如下：

(1) 準備各類設備之操作手冊。

為防止各類設備之操作錯誤，以及在故障、災害發生時，能適當因應，迅速排除問題，應備有各類設備的操作手冊。

(2) 規定事故發生時，系統切換之程序。

(3) 規定事故發生時，系統維護相關人員之緊急召集體制。

(4) 規定在緊急情況時，相關人員之聯絡方法及聯絡內容等。

明確訂定資訊系統管理負責人員之聯絡方法及聯絡內容，以便迅速因應資訊系統事故。

(5) 應掌握在緊急時仍能運轉所需之燃料庫存。

故障、災害發生時，為使資訊系統作業仍能順利運轉，應適當管理各種設備所需使用之燃料、油、電力、水等。

(6) 擬定確認設備機能之定期測試/演練計畫，並確實執行。

例如，災變備援中心系統之切換、復原等大規模的故障災害測試演練、每月一次的發電機測試、備援空調設備的測試及絕緣測試等。

(7) 若相關設備機器的維護保養、運轉等，係委託外部廠商執行時，特別需要明確訂定管理責任，並貫徹安全指示。

(8) 夜間、假日等提供無人化服務所使用的設備，須訂定相關管理程序。

(9) 設備之操作應由負責管理人員執行。

(10) 行動電話等發射電磁波的機器設備，可能干擾資訊系統或相關設備之執行，在電腦機房或設置重要伺服器的機房得禁止或限制其使用。

(11) 掌握事故之原因，研擬對策，整理保存事故紀錄，分析事故發生原因，以改善問題。

各種設備管理
維修管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 77	明定維護管理辦法。
------	-----------

為使資訊系統運轉順利，應確實進行保養維護，並掌握維護結果。

1、為確保資訊系統（包含端末設備）能順利運轉，與設備相關之電源、空調、供/排水、防災、防犯、監視、通訊線路等相關設備之保養維護，應配合資訊系統運轉排程，明確訂定維護對象、維護期限與維護內容等。

同時，對於設備保養維護，應請廠商提供書面報告，維護內容應包含事前的作業內容及事後的作業結果，作為維護驗收紀錄留存。

2、對於防災設備的維護保養，應訂定規範，並定期實施。

有關防災設備，請參照【設 80】。

3、長時間停用之設備，於再啟動之前，應實施維護檢查作業。

4、常使用之備援設備，應定期檢查確認其可正常運轉。

5、維護設備時，維護人員與電腦操作人員，應密切連繫，以免影響系統的正常運作。

6、如電力裝置或空調設備等，對資訊系統有直接影響之設備，其維護作業應避免在連線作業時段進行。

7、如果必須在系統運轉中維護部份設備時，為不影響作業中之系統，應擬定作業程序，並會同該項設備負責人員辦理。

8、電源及監視設備之配線圖，在設備異動後，亦需配合更新。

（五）各種設備管理

2、資源管理

為使資訊系統順利運轉，應掌握各項設備之容量、性能及使用狀態。

各種設備管理
資源管理

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 78	確認設備之容量、性能及使用狀態。
------	------------------

應掌握各項設備之容量、性能極限，及其使用狀態，以早期發現異常情況。

1、為維持資訊系統穩定運轉，並早期發現各種設備之異常狀態，管理人員應掌握各項設備之容量及其性能，並注意下列各點：

(1) 資訊系統設備之擴增

檢討是否需要配合擴充或增設相關設備之容量。

(2) 機房設備配置變更

配置變更時，應確認有無確保通道與維修所需空間及地板加重後之安全性等。

2、所謂設備，係指下列各項：

(1) 配電設備（應注意與電力公司之契約容量）。

(2) 定電壓定周波數設備（CVCF）。

(3) 蓄電池設備。

(4) 自備發電設備。

(5) 水冷卻裝置。

(6) 空調設備。

(7) 給水、排水裝置。

(8) 消防設備。

(9) 監視設備。

(10) 通訊線路相關設備（含備援用網路等）。

(11) 緊急通訊設備（無線電、行動電話、衛星通訊等）。

(五) 各種設備管理

3、監控

為及早發現異常情況，應隨時監控影響資訊系統運作之各項設備之運轉情況。

各種設備管理
監控

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

運 79	建立監控機制。
------	---------

為早期發現異常情況，應建立監控機制，訂定監控標的及監控方法等。

1、為早期發現各項設備之異常狀況，減輕對資訊系統的影響，應建立包含監控標的、監控項目、以及監控方法等之監控機制。

(1) 對資訊中心之監控

a. 監控標的、項目

(a) 監控資訊系統是否正常運作

標的：電源、空調、給水、排水設備。

(b) 為防犯、防災的監視

標的：火災警報設備、感應器警報設備、進出門禁監視系統及遠端監視裝置等。

b. 監控方法

發現異常狀況的方法，舉例如下：

(a) 定期巡視時，需確認顯示操作面盤、閥等指示為正常值或正常位置。

(b) 利用警示燈或警示器，配合營運狀況，將異常狀況即時通報中央管理室等。

(c) 由中央管理室（中央監視室、防災中心）等，對電源、空調、給水、排水設備、防犯設備作集中監控。

(2) 總行、營業單位等之監控機制

設置於總行、營業單位之重要伺服器等，應配合營運狀況，與廠商協商討論，訂定最適當之監控方法。

2、發現異常狀況時之因應方法，應依設備分別明確訂定。

(1) 各種設備之容量以及其可能停用之時間，請參照 【設 61】。

(2) 決定因應對策，如是否有備援設備可用等。

（六）教育訓練

1、教育訓練

為能安全並順利運轉資訊系統，應對相關人員實施資訊安全教育訓練。並明訂教育訓練之目的、訓練計畫及實施辦法等。

教育訓練
教育訓練

適用性分類				
共通	中心	總行	合作	直接
◎				

運 80	實施資訊安全教育。
------	-----------

為提升全體員工（包含駐外人員）對資訊安全之認識，充分了解組織之資訊安全政策及具體資訊安全措施，應配合業務實施相關教育訓練。

- 1、組織規劃資訊安全教育訓練，應以資訊安全政策（基本方針）、資訊安全標準（機構內部安全對策基準）、相關手冊或作業程序說明、及資訊安全相關事故之緊急因應對策等為主要內容，對於責任、義務及懲罰等，亦應通告全體員工。
- 2、教育訓練應有計畫的實施。對新進員工或中途加入人員之教育訓練，亦應包括資訊安全教育。
- 3、教育訓練課程，應明確宣示下列事項的重要性：
 - （1）資訊系統所扮演的角色。
 - （2）機密之保護、客戶資訊的保護。
 - （3）有關係統安全運轉之對策。
- 4、教育的主題，舉例如下：
 - （1）資訊安全政策。
 - （2）資訊安全應遵循事項
特別是指：
 - a. 使用者帳號（User ID）、密碼（Password）之管理。
 - b. 使用權限之管理。
 - c. 文件及輸出物（報表、檔案）等之管理。
 - d. 發現異常狀況之因應處理。
 - （3）機密保護
 - （4）使用者之責任與義務。

- (5) 客戶資訊之保護。
- (6) 違反安控規定時之懲罰。
- (7) 電腦病毒之對策。
- (8) 非法存取系統之對策。
- (9) 作業系統軟體漏洞修復。
- (10) 社交工程 (Social Engineering) 對策。
- (11) 收發電子郵件、網際網路等之注意事項。
- (12) 重要法令宣導(如：個人資料保護法、著作權法、洗錢防治法等)。

教育訓練
教育訓練

適用性分類				
共通	中心	總行	合作	直接
◎				

運 81	實施提升技巧與熟練度訓練。
------	---------------

為提升對系統及業務相關之知識及技能，應對系統開發人員施以必要訓練。

1、對於參與資訊系統開發、建置及操作之人員（包含駐外人員）等，應配合其職掌、工作性質等，實施自辦訓練或參加外部機構訓練。

2、訓練具體實例如下：

（1）自辦訓練

- a. 系統技術訓練。
- b. 使用者訓練。
- c. 營運業務系統訓練。
- d. 營運業務相關知識訓練。
- e. 系統管理人員的研習。
- f. 資訊技術人員資格檢定訓練。
- g. 在職訓練（OJT）。

（2）參加外部機構訓練

- a. 廠商舉辦之訓練。
- b. 外部研討會、講習會。
- c. 其他機構舉辦之訓練。

3、教育訓練後，金融機構的教育負責人員，應向教育主辦單位取得受訓人員之研習結果，以掌握人員受訓狀況及成果。

教育訓練
教育訓練

適用性分類				
共通	中心	總行	合作	直接
◎				

運 82	實施系統操作訓練。
------	-----------

為使人員能熟練營業單位資訊系統操作，以順利處理日常業務，應實施系統操作訓練。

1、對於資訊系統操作的教育訓練，應注意下列事項：

- (1) 使用資訊系統處理日常作業（包含安裝自動執行作業的自動化系統）時，為能確實掌握系統處理狀況、迅速正確回應，使系統運轉順利進行，在新進人員報到、新系統安裝啟用或應用軟體變更時，應實施系統操作之教育訓練。實施教育訓練前，應先確定講師、訓練負責人員、訓練範圍、訓練內容、所需時間等事項。
- (2) 營業單位之端末系統操作，可指定負責人員，持續在新進員工報到或安裝新端末系統時，配合其工作性質辦理相關之教育訓練。

2、對訓練成果，應加以分析、評估，供下次訓練改進參考。

教育訓練
教育訓練

適用性分類				
共通	中心	總行	合作	直接
◎				

運 83	實施事故應變操作訓練。
------	-------------

為期事故發生時，仍能維持作業，平常應演練應變作業。

1、為使發生事故及災害時，系統得以快速回復運轉，應實施操作訓練演練，並分析及評核訓練結果後，作為下次訓練之參考。

在實施演練時，資訊中心與總行、各營業單位的連繫應作必要之溝通。

2、具體範例如下：

(1) 訓練範圍

依據系統操作負責人員（包含資訊中心及駐外人員）等之工作性質、職掌、工作經驗年資等，施以教育訓練。如有必要，總行、營業單位等之系統使用者亦需參加教育訓練。

(2) 訓練內容

- a. 連線作業之復原及重新啟動訓練。
- b. 備用機器、備用通訊線路等切換及切回的訓練。
- c. 連線作業離、斷線作業訓練。

(3) 所需時間

由於故障、災害發生時，需迅速執行復原行動，相關訓練應要求限時完成，同時應配合資訊系統運轉的時程加以調整。

3、訓練上應考慮的事項，列舉如下：

- (1) 為在故障、災害發生時，能迅速因應處理，在訓練時的作業環境，應儘可能與正式作業環境相同。但是，若在環境上無法配合時，亦可利用紙上作業之訓練方式，實施模擬演練之檢討。

(2) 配合作業負責人的變更或機器架構的改變實施訓練，以考核訓練的效果。

4、實施訓練時，應注意確認訓練當時與回復正式作業環境後，不致影響正式作業。

教育訓練
教育訓練

適用性分類				
共通	中心	總行	合作	直接
◎				

運 84	實施防災、防犯演練。
------	------------

為預防緊急狀況發生，應實施防災、防犯演練。

- 1、為使防災組織及防犯組織能充分發揮功能，應實施防災、防犯演練。
但是，若實施有困難時，亦可利用紙上作業之訓練方式，實施模擬演練。
- 2、防災、防犯訓練，應明確訂定訓練範圍、訓練內容、時間要求等內容。
 - (1) 訓練範圍
以資訊中心及總行、營業單位的執勤人員、外勤人員及相關人員為對象。
 - (2) 訓練內容
 - a. 防災、防犯設備之操作訓練。
 - b. 防災、防犯機關之聯絡訓練。
 - c. 緊急連絡網之功能訓練。
 - d. 避難訓練。
 - (3) 時間要求
災害、犯罪發生時，迅速因應的行動是非常重要的，因此應設定訓練結果之時間要求。
- 3、訓練實施結果應予分析、評估，作為規劃下一次訓練及修改災變備援作業計畫的參考。

（七）人員管理

1、人員管理

為使資訊系統能安全平順運轉，對系統開發、維護及操作人員，應適切實施人事管理及健康管理。

另外，對於人員的配置，應充分瞭解、評估每一員工的能力，確實區分職掌、權限等，以明確賦予適當的職責。

為確保各組織資訊系統之敏感性與機密性，各資訊安全管理人員(包括系統管理人員、資料管理人員、網路管理人員等)錄用及調派時，應進行適當之安全評估、品德、行為及家庭狀況考核，以降低資訊外洩之風險。

人員管理
人員管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 85	實施適當人事管理。
------	-----------

為使系統順利運轉，人員配置、代理人員等之人事管理應適切的實施。

- 1、資訊系統營運人員（包含兼職人員、外勤人員）的配置、調任等，應評估每一員工的能力、經驗年資、安控觀念與工作效率等。
- 2、應實施職務權限的分離，並對其被賦予的職責與能力，加以評估比較。
- 3、為確保各組織資訊系統之敏感性與機密性，各資訊單位人員錄用及調派時，應進行適當之安全評估、品德、行為及家庭狀況考核，以降低資訊外洩之風險。

人員管理
人員管理

適用性分類				
共通	中心	總行	合作	直接
◎				

運 86	實施人員健康管理。
------	-----------

建立完善之作業環境，定期的健康檢查等，以適切實施人員的健康管理。

- 1、對於資訊系統營運人員（包含兼職人員、外勤人員）的健康管理，應考量人員的勤務體制、作業內容、電腦機房環境，定期實施健康檢查或個別指導。
- 2、人員健康管理應注意事項，列舉如下：
 - （1）人員配置及交接班的適切性。
 - （2）加班、夜間值勤、假日出勤、休假狀況等勤務體制。
 - （3）由於業務壓力，可能造成之生理失調。
 - （4）維持並改善系統開發、業務營運等之作業環境。

(八) 委外管理

1、委外計畫

金融機構近年來對於資訊系統的開發、營運等，包含執行業務所必要的管理，委外處理或將某些業務完全委外之情況漸增。

委外作業之主要型態，也自委託給子公司，逐漸轉移為委託電腦廠商或資訊處理公司。

再者，多家金融機構共用資訊系統的「共用中心」也有增加的趨勢。

如上所述，金融機構的資訊系統開發、營運等，委外處理的範圍逐漸擴大，其內容也多樣化，在這種情況下，資訊系統策略的擬定，有關委外處理的事項，應經過充分的研究及檢討。

因此，在個別系統的開發或營運上，委外處理的計畫、實施等，應以資訊系統策略為基礎，在決定委外處理的目的、範圍及風險管理上，應有具體措施。

除上述問題外，對於委外處理相關之安全與保密對策亦需一併考慮。

委外管理
委外計畫

適用性分類				
共通	中心	總行	合作	直接
◎				

運 87	系統開發、營運等委外處理，應事先明確訂定作業目標及範圍。
------	------------------------------

系統開發、營運等委外處理，應事先明確訂定作業目標及其範圍。

- 1、系統開發或營運，若委外處理時，應事先明確訂定其目標及範圍。
- 2、委外處理時，應明確訂定的事項，舉例如下：
 - (1) 目的。
 - (2) 範圍。
 - (3) 形式。
 - (4) 期間。
 - (5) 費用分析。
 - (6) 風險評估。
 - (7) 評選條件。
 - (8) 雙方職責等。
- 3、在系統開發或營運計畫呈核時，有關委外作業部分，亦應一併呈報核准。

委外管理
委外計畫

適用性分類				
共通	中心	總行	合作	直接
◎				

運87-1	以明確之程序選擇委外廠商。
-------	---------------

在選擇委外廠商時，其選擇程序應明確而客觀，並應將選定結果呈報主管核准。

- 1、在選擇委外廠商時，其選擇程序應明確化。
- 2、委外廠商應有客觀的評估，評估的項目列舉如下：
 - (1) 穩定性（財務內容）、健全性。
 - (2) 信賴度及受託實績（例如系統開發實績、其他企劃案之評價等）。
 - (3) 技術層次（對業務內容的理解程度、業界相關知識、資訊收集能力、專案管理能力、安裝及支援能力）。
 - (4) 委外費用支付條件。
 - (5) 資訊安全政策的實施狀況。
 - (6) 問題發生時之因應能力。
 - (7) 維護體制。
 - (8) 是否取得各種公認的認證資格。
- 3、委外廠商的選定最終應獲得主管的核可。

委外管理
委外計畫

適用性分類				
共通	中心	總行	合作	直接
◎				

運 88	委託契約內容應包含安全政策相關事項。
------	--------------------

為確保安全性，在委託契約內，應包含保密、安全與稽核條款。

- 1、為了金融機構委外業務能安全執行，在與委外廠商簽定合約時，應包含保密、安全與稽核條款。
- 2、委外業務，舉例如下：
 - (1) 系統操作（包含備援中心的系統操作）。
 - (2) 系統開發、維護。
 - (3) 應用軟體的開發、維護。
 - (4) 硬體設備或通訊線路的設置、更換或撤除。
 - (5) 資料輸入(包含端末系統的操作)。
 - (6) 記錄媒體、文件以及傳票帳冊的編製、保管、配送、銷毀廢棄。
 - (7) 電腦機房、機構內部及營業廳等之警備。
 - (8) 電源、空調、防犯等設備之管理及維護。
 - (9) 集中監控（ATM 等）。
 - (10) ATM 之現金管理。
 - (11) 資訊系統完全委外。
- 3、委外作業形態，舉例如下：
 - (1) 由委託業者提供作業人員。
 - (2) 委外。
 - (3) 委任。
- 4、配合委外處理之業務種類及範圍，在安全政策上，應考慮下列事項，並納入契約條文中，特別是對於客戶資訊的處理以及資料保護等，應有嚴謹的管理。

在簽定合約時，應考慮的事項列舉如下：

- (1) 機密資料的保護。
- (2) 合約指定用途外使用之限制。
- (3) 作業時間及作業活動場所。
- (4) 轉包委託（轉包委託之責任歸屬應明確，應事先取得金融機構同意）。
- (5) 事故發生時的報告程序。
- (6) 產出之智慧財產之所有權、使用權等歸屬。
- (7) 期限、費用。
- (8) 損害賠償相關事項。
- (9) 對於作業指示的裁定。
- (10)品質/服務水準之保證及確認程序。
- (11)作業之報告方法及報告形式。
- (12)交貨項目、驗收條件與驗收程序、及權利移轉時機。
- (13)維護或故障時之復原作業。
- (14)有關當事人責任之裁決。
- (15)監察的權利（對委外廠商的稽核權或外部專業機關稽核的實施權等）。
- (16)契約修改時之程序。
- (17)雙方應遵守之法令規定、資訊安全政策等。
- (18)災變備援作業計畫（緊急時之對應計畫）。
- (19)委外業務發生問題時之解決對策及機制。
- (20)契約之解除（若委外廠商執行作業有問題時，可轉委託其他業者之權利等）。

5、金融機構與委外廠商之間，為能計算委外處理業務之達成程度，可考慮在契約內納入 SLA（Service Level Agreement）條文，請參照 **【運 90】**。

SLA 之應用，舉例如下：

- (1) 委託業務營運時：系統可使用率（Availability）之保證，連線系統營運起始時間的保證。
- (2) 委託開發業務時：開發所需要之人員、開發期間及期限之保證。

6、委外契約期間，應持續對委外廠商之作業情況進行考核。

委外管理
委外計畫

適用性分類				
共通	中心	總行	合作	直接
◎				

運 89	規定委外廠商之從業人員應遵守事項並加以管理及檢核。
------	---------------------------

應對委外廠商之從業人員實施適當安控管理，依委外業務內容及作業範圍等，訂定應遵守安全政策及相關各種規定，並進行教育訓練及監督稽核等。

- 1、委外廠商之從業人員執行委託業務時，應以金融機構之資訊安全政策為主，配合委託的業務內容，明確訂定相關規定，並嚴格要求遵守。為達上述要求，得採取下列措施：
 - (1) 要求委外廠商之從業人員遵守的規定，由金融機構明確提出，交委外廠商。尤其對於包含業務執行在內的委外作業，業務體制及稽核等安控要件，應於委外廠商同意之下，納入契約條文中，或明確條列於相關文件中，並告知業者應遵守的義務。
 - (2) 對於委外廠商之從業人員，應實施有關遵守規定的教育訓練。委外廠商之從業人員應遵守的規定，舉例如下：
 - a. 金融機構之資訊安全政策。
 - b. 電腦機房進出管理規定，設備管理規定。
 - c. 各種資訊存取權限管理規定（識別碼或密碼的賦予或刪除等規定）。
 - d. 開發工程中所編製文件或磁性媒體的管理程序。
- 2、賦予委外廠商之從業人員，對於金融機構之各種資源及系統的存取權限，應僅限於執行業務必要的範圍。
有關存取權限的檢討程序，請參照【運 18】。
- 3、金融機構為管理並檢核委外廠商是否遵守上述的規定，應依照委外業務的內容及作業範圍，稽核委外廠商的業務執行狀況，並接受委外廠商的業務執行報告，請參照【運 91】。

委外管理
委外計畫

適用性分類				
共通	中心	總行	合作	直接
◎				

運 90	委外業務組織之建立、業務之管理及檢核之執行。
------	------------------------

為確認委外處理之業務內容，得配合調整業務組織，並依委外契約內容，執行業務管理及檢核工作。

1、為使委外業務能順利正確營運，執行委外業務的業務組織（金融機構本身及委外廠商雙方所構成的組織）業務範圍及權責應明確訂定。有關組織的調整與相互牽制，請參照【運 9】。

2、具體範例如下：

(1) 可依下列方法掌握委外廠商之管理狀況：

- a. 聽取管理負責人員報告。
- b. 定期作業狀況之報告。
- c. 作業機密管理狀況報告。
- d. 相關重要變更事項(管理負責人交接、系統更新等)報告。
- e. 有關安控事故或犯罪之報告。

(2) 檢核委外廠商編製之系統設計書、程式等應執行的工作。

應檢核相關功能要件是否充足，確認標準化的遵守狀況，並執行例外處理之驗證測試。

(3) 委外業務結束之後，重要資料及相關文件的收回。

為保護機密資料及防止非法使用，在委外業務結束之後，委外廠商借出之相關重要資料、文件等以及其影印複製的文件，都應收回。

3、委外廠商之業務處理成果是否達到所要求的層次，金融機構應自行掌握。

為能計測業務成果，可以將 SLA (Service Level Agreement) 等，納入委

外契約中，並依據此合約，定期實施檢驗及評估，請參照【運 88】。
發現問題，應與委外廠商共同合作，儘速排除問題。

(九)系統稽核

為確保資訊系統之開發、變更及系統營運之有效性、效率性、信賴性、遵守性與安全性，應具備完備之系統稽核體制。

系統稽核
系統稽核

適用性分類				
共通	中心	總行	合作	直接
◎				

運 91	系統稽核之體制。
------	----------

為全面掌握並評估資訊系統及其管理之有效性、效率性、信賴性、遵守性及安全性，應建立系統稽核之體制。

- 1、為確保資訊系統之營運、系統開發及變更之有效性、效率性、信賴性、遵守性與安全性，應設置系統稽核人員(此稽核人員應與資訊系統部門分隔，能獨立作業)進行綜合性之監查、評估，並將檢查結果直接呈報經營階層主管。
- 2、上述系統稽核之實施，除內部稽核之外，應活用外部專門機構之稽核。
- 3、系統稽核之結果，若有發現缺失事項時，應由系統稽核部門與被稽核部門確認事實，並充分溝通交換意見，在確定問題之存在時，應立即執行適當之改善工作。
- 4、系統稽核部門之人員，應具備精通資訊系統之人才。

(十)行外收付處

行外收付處多為開放式之擺設(Layout)，並以少數人員從事營運之據點，與一般總行、營業單位等，在營運上有差異。為確保行外收付處之安全性，據點之設置地點及商店之選擇基準，應事先明確訂定。

行外收付處

適用性分類				
共通	中心	總行	合作	直接
		◎		

運 92	收付處設置地點之選擇基準，應事先明確訂定。
------	-----------------------

為確保行外收付處之安全性，選擇設置地點之基準應事先明確訂定。

- 1、行外收付處，多為開放式之擺設，並由少數人員從事營運之據點，與原有之總行、營業單位等，在營運上有差異。為確保行外收付處之安全性，據點之設置地點及商店之選擇基準，應事先明確訂定。
- 2、在設置行外收付處時，應注意預定設置地點之設備狀況。
- 3、對於行外收付處預定設置地點之設備狀況、行外收付處之工作人員之派遣，應有安全措施。有關行外收付處之安全措施，舉例如下：
 - (1) 利用防犯攝影機或防犯錄影機，請參照【設 113】。
 - (2) 設置緊急呼叫鈴、緊急呼叫按鈕等，請參照【設 113】。

(十一)便利超商 ATM

設置於便利超商之 ATM 與設置於自動化服務區之 ATM 不同，便利超商為不特定之多數人員進出之場所，且無法區隔設置自動化服務區及機械室等，而是機器設備單獨設置之服務區域。因此，設置於便利超商之 ATM 營運應考慮使用及維護人員之安全。

便利超商ATM

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 93	設置地點之選擇基準，應事先明確訂定。
------	--------------------

為確保便利超商ATM使用者之安全，設置地點與便利超商之選擇基準，應事先明確訂定。
--

- 1、為確保便利超商 ATM 及使用顧客之安全，設置地點與便利超商之選擇基準，應事先明確訂定。
- 2、明確之選擇基準，舉例如下：
 - (1) 便利超商之經營體質、警備保全方針。
 - (2) 自動櫃員機裝置時，應詳確評估其安全性，慎選設置地點，對非設置於營業處所之行外自動櫃員機，尤須考量管轄單位是否方便監督管理，並優先選擇有保全設備或有警衛、值勤人員巡守之處所。
 - (3) 自動櫃員機應裝置於明亮處所，以防歹徒覬覦或從容作案。
- 3、對於設置於便利超商之 ATM，應考慮該便利超商之設備狀況。
- 4、在便利超商之 ATM，應注意便利超商之設備狀況與對便利超商之店員之安全措施，自動櫃員機應裝置錄影監視系統，影像以彩色為主。

便利超商ATM

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 94	對於裝填現金等維護作業，應有防犯對策。
------	---------------------

為確保便利超商ATM維護作業之安全，應明確訂定防犯體制及防犯辦法。

- 1、便利超商 ATM 設置於開放之地點，因此在裝填現金等維護作業時，應有明確之防犯體制及防犯之辦法。
- 2、現金裝填作業應注意事項：
 - (1) 補鈔作業需兩人(含)以上共同執行。
 - (2) 補鈔時只更換鈔匣，不得在現場裝卸現金或點鈔。
 - (3) 現金運送及填補應委由合格且信譽良好之專業運鈔保全業者辦理。
 - (4) 設備應裝設自動報警、警報系統並與警察機關或保全公司連線。

便利超商ATM

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 95	應明確訂定故障、災害發生時之因應對策。
------	---------------------

裝置於便利超商之ATM發生故障、災害時，為能迅速因應，應明確訂定因應程序。

- 1、便利超商 ATM 發生故障、災害之因應程序應明確訂定。
- 2、銀行應於其所設置之自動化服務設備上明顯標示銀行名稱、緊急連絡電話及服務項目。
- 3、有關發生災害之對應方法，請參考故障發生時之因應程序，加以檢討、整理並訂定。

便利超商ATM

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 96	對於網路相關設備，應制定資料傳輸之安全政策。
------	------------------------

為確保資料傳輸之安全性、信賴性，並防止非法之使用、破壞、篡改，對於網路相關設備應有適當之保護措施以及資料傳輸之安全政策。
--

- 1、對於網路相關機器設備，應有適當保護措施，請參照【運 58】。
- 2、對於資料傳輸應有安全政策，通訊線路應使用與便利超商不同之線路。
- 3、資料傳輸之安全對策，列舉如下：
 - (1) 依傳輸資料之重要性，應有適當之防止洩漏對策，請參照【技 29】。
 - (2) 為早期發現傳輸資料遭非法破壞、篡改，應有適當之檢測措施，請參照【技 33】。

便利超商ATM

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 97	應確立與設備所在地之警察機關、保全公司等相關機構之聯絡體制。
------	--------------------------------

為在發生犯罪行為時，迅速聯絡通報相關單位，應確立與設備所在地之警察機關、保全公司等相關機構之聯絡體制，並經常演練。

- 1、自動櫃員機應週延裝設自動報警、警報系統，並與警察機關或保全公司連線。
- 2、前述報警及警報系統應加裝不斷電設備，以避免停電時失效，喪失警訊功能。
另為避免歹徒剪斷或破壞線路，應注意該系統電源開關及線路之隱密及安全性，以維報警、警報系統之暢通。
- 3、自動櫃員機置機或管轄單位應與轄區警察機關（委託辦理保全業務者含保全公司）保持密切聯繫，請其加強巡邏（必要時設置巡邏箱），以減少歹徒作案機會。
- 4、應於明顯處張貼警示標語，籲請自動櫃員機使用客戶留意交易之安全。並加強注意機器之維修與現鈔、紙卷之補充，以維持自動櫃員機之良好運作，降低故障發生頻率，俾減少客戶之情緒性破壞行為。

(十二)轉帳卡

為確保轉帳卡(DebitCard)服務之安全性，顧客(帳戶所有人)、發行卡片之金融機構等、加盟店金融機構、加盟店等，應共同協力維持系統之安全。此處所提之轉帳卡服務之安全對策，是記述金融機構等應特別注意之事項。

1、確保轉帳卡服務之安全性

為確保轉帳卡服務之安全性，提供服務之金融機構與資料處理之相關單位應共同研訂實施相關安全政策。

轉帳卡
確保轉帳卡服務之安全性

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 99	應有轉帳卡服務之安全政策。
------	---------------

為確保轉帳卡服務之安全性，提供服務型態的金融機構與資訊處理中心、加盟店等，應有共同之安全對策。

- 1、為確保轉帳卡服務之安全性，提供服務型態之金融機構與資訊處理中心、加盟店等，應有共同之綜合性安全對策。
- 2、依所提供服務之形態，應檢討之安全對策，舉例如下：
 - (1) 顧客資料之適切保護，請參照【運 53】：
 - a. 對於列印帳號等卡片資訊之印刷物品，應有適當之管理。
 - (2) 提醒顧客注意。
 - (3) 確保帳號、密碼等之安全性，請參照【運 100】。
 - (4) 防止轉帳卡被非法使用之對策：
 - a. 加盟店店員利用確認卡片，非法竊取卡片資料之檢知，請參照【技 40】。
 - b. 非法使用卡片交易等之檢知，請參照【技 46】。
 - (5) 應考慮轉帳卡在轉帳卡端末讀取資料時之安全對策：
 - a. 加盟店之店員在讀取卡片資料時，應在顧客可見之範圍內執行。
 - b. 由顧客本人親自操作，以讀取卡片資料。
 - (6) 應有抑制犯罪行為或能迅速識別犯罪者之措施：
 - a. 設定適當之使用額度，請參照【運 101】。
 - b. 在加盟店設置防犯攝影機。
 - c. 選擇正當之加盟店安裝轉帳卡之端末設備。
 - (7) 安控管理與責任之明確化，請參照【運 1～運 6】。
 - (8) 實施安全管理之教育訓練，請參照【運 80】。

轉帳卡
確保轉帳卡服務之安全性

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 100	應確保帳號、密碼之安全性。
-------	---------------

為確保帳號、密碼之安全性，依照金融機構等所提供之服務形態、資料處理中心及加盟店等，應有共同之安全對策。

- 1、為確保帳號、密碼之安全性，依照金融機構等所提供之服務形態、資料處理中心及加盟店等，應有共同之安全對策。
- 2、為確保帳號之安全性，可採取之對策如下：
 - (1) 防止由轉帳卡端末設備竊取之對策。
 - a. 在端末加強防破解性能(TamperResistant)來保護。
 - b. 卡片資訊亂碼化保護。
 - (2) 防止資料傳輸時之洩漏，請參照【技 29】。
 - (3) 防止由交易明細表等洩漏帳號等資訊：
 - a. 端末上，有關帳號等卡片資訊，僅列印部分或完全不列印。
 - (4) 防止轉帳卡被偽造之對策，請參照【技 40】。
- 3、為確保密碼之安全性，可採取之對策如下：
 - (1) 防止由轉帳卡端末竊取之對策：
 - a. 在端末加強防破解性能(TamperResistant)來保護。
 - b. 卡片資訊亂碼化保護。
 - (2) 防止資料傳輸時之洩漏，請參照【技 29】。
 - (3) 防止密碼被偷看：
 - a. 輸入密碼時所使用數字鍵盤之安裝位置。
 - b. 在加盟店設置防犯攝影機時，不可拍攝到顧客輸入密碼之手指。
 - (4) 應使用他人不易猜測之密碼，請參照【運 17】。
 - (5) 由顧客本人變更密碼，請參照【運 51、運 101】。

(十二)轉帳卡

2、客戶之保護

為確保客戶在使用轉帳卡時之安全性，應有適當之客戶保護措施。

轉帳卡
客戶之保護

適用性分類				
共通	中心	總行	合作	直接
			◎	

運 101	客戶使用轉帳卡應有客戶保護措施。
-------	------------------

為確保使用轉帳卡之安全性，應有適當之客戶保護措施。

- 1、為確保客戶在使用轉帳卡時之安全性，應有適當之客戶保護措施。
- 2、有關客戶在使用轉帳卡時，應有之客戶保護措施，如下列所示。
 - (1) 使用轉帳卡應注意事項，應明示並提醒客戶注意。
 - (2) 設定每日可利用之額度：
 - a. 統一設定可利用之額度。
 - b. 保留由客戶自行選擇、變更可利用額度之可能性。
 - (3) 保留由客戶自行選擇、變更轉帳卡使用之可能性。
 - (4) 發生轉帳卡遺失、遭竊、偽造等，對於客戶損失之補償，應有適當之對應措施。
 - (5) 保留客戶本人利用 ATM 自行變更密碼之可能性，請參照【運 51】。

(十三)利用開放網路之金融服務

1、網路銀行、行動銀行

為保障客戶得交易安全，對於開放網路上種種安全之威脅，應有安全對策。

在開放網路上執行業務之安全威脅，如竊聽、偽裝他人、資訊竄改、非法入侵、竄改置換首頁內容等。為因應這些威脅，資訊系統應實施安全對策。

同時，對於發生故障之對應方法，事故之免責範圍等，應明確訂定記載。

利用開放網路之金融服務
網路銀行、行動銀行

適用性分類				
共通	中心	總行	合作	直接
				◎

運 103	防範不當使用。
-------	---------

為確保利用開放網路之金融服務安全性，應有能確認連接對象確實是客戶本人，或限制使用權限等之檢知對策，以防止非法使用系統。

1、為防止非法使用，應嚴格實施確認本人之作業，尤其是資金移轉或預約交易等相關交易，應特別嚴格實施。

2、防止非法使用系統之策略，舉例如下：

(1) 預防對策：

- a. 代碼、密碼，請參照【技 35】。
- b. 代碼、密碼輸入錯誤次數之限制及監視，請參照【技 36】。
- c. 資金移轉及預約交易等交易時要求再次輸入密碼。
- d. 利用指紋等生物科技之技術，請參照【技 35】。
- e. 禁止同時簽入(Log-on)系統。
- f. 明示前次最後簽出(Log-off)之日期時間，請參照【技 36】。
- g. 一段時間未存取系統時，自動簽出系統，請參照【技 36、技 37】。
- h. 利用回撥(CallBack)方式，確認端末設備及本人，請參照【技 35】。
- i. 安裝 Client 認證技術，請參照【技 35】。
- j. 資料亂碼化，請參照【技 35】。
- k. 利用電子簽章，請參照【技 35】。

(2) 由外部網路存取系統之限制：

- a. 指定服務提供者，請參照【技 43】。
- b. 以數據專線連接服務提供者，請參照【技 43】。

(3) 檢知對策：

- a. 檢知非法入侵時，或檢知簽入失敗時，以蜂鳴器告知，請參照【技 45】。

b. 明示前次最後簽出之日期時間，請參照【技 45】。

c. 活用亂碼技術進行認證，或檢知資料是否遭竄改，請參照【技 33】。

3、在檢知並發現非法行為時，處理程序應事先訂定。

利用開放網路之金融商品
網路銀行、行動銀行

適用性分類				
共通	中心	總行	合作	直接
				◎

運 104	早期發現非法使用。
-------	-----------

為防範使用者非法使用，應設置使用者本身能確認使用狀態之機制。

- 1、未發現使用者代碼是否被非法使用，使用者本身應能自行確認使用狀態，尤其在資資金移轉或預約交易等交易，應能提供早期發現非法使用，以及確認交易處理結果之功能。同時，應隨時提醒使用者本身確認是否遭非法使用。
- 2、早期發現非法使用之對策，如下列所示：
 - (1) 顯示系統簽入與簽出之日期時間歷史資料，請參照【技 45】。
 - (2) 資金移轉、預約交易等，應顯示交易處理之結果。
 - (3) 資金移轉、預約交易之處理結果，利用郵寄或電子郵件寄送登錄之電子信箱。

利用開放網路之金融商品
網路銀行、行動銀行

適用性分類				
共通	中心	總行	合作	直接
				○

運 105	應公開安全政策相關資訊。
-------	--------------

為讓使用者能適當選擇往來之金融機構或服務，應公開有關安全政策之資訊。

- 1、為讓使用者能適當選擇往來之機構或金融服務，金融機構等之安控政策等資訊應公開明示。
- 2、公開明示之內容，如下列所示：
 - (1) 防止資料外洩之資料亂碼化。
 - (2) 防止偽裝他人之認證(代碼、密碼、電子認證等)。
 - (3) 依照個人資料保護法之規定及保密義務，保護客戶之個人資料。
- 3、公開明示之方法，如下列所示：
 - (1) 利用 DM 記載。
 - (2) 在店面或自動化服務設備前張貼海報。
 - (3) 金融機構之網頁公告。
 - (4) 新聞廣告。
- 4、對於資訊之公開明示，應利用圖文等讓使用者容易瞭解之方式。
- 5、應能因應客戶之諮詢與抱怨：
 - (1) 洽談窗口之設置。
 - (2) 在海報、首頁等明確記載連絡處所之資訊。

利用開放網路之金融商品
網路銀行、行動銀行

適用性分類				
共通	中心	總行	合作	直接
				◎

運 106	應明確訂定營運管理辦法。
-------	--------------

在利用網路銀行、行動銀行等執行銀行交易、證券交易、人壽保險、產物保險等之交易時，為保護使用者，確保交易安全，並使作業順利進行，應明確訂定營運管理辦法。

- 1、在利用網路銀行、行動銀行等執行銀行交易、證券交易、人壽保險、產物保險等交易時，應對使用者明示有關交易應注意事項，並實施適當之安全對策。
- 2、應對使用者公開明示之事項，舉例如下：
 - (1) 可使用之瀏覽軟體及其版本。
 - (2) 可使用之之機種。
 - (3) 可使用之時間區段、可使用之交易、上限金額、交易限額等之約定事項。
 - (4) 交易之操作方法。
 - (5) 密碼等使用者應自行管理之資料。
 - (6) 使用者在操作或交易之內容，需要諮詢時之連絡窗口。
 - (7) 若懷疑有非法使用時，向金融機構聯絡之方法及窗口。
 - (8) 金融機構等所實施之安全對策概要說明。
 - (9) 有關金融商品之說明、勸導方針及免責事項。
 - (10) 行動銀行因行動電話手機遭竊、遺失或變更電話號碼等，而終止契約之申請。
- 3、向使用者通報之方法，舉例如下：
 - (1) 契約簽定時之交易規定。
 - (2) 啟動交易畫面時，所顯示之同意事項及確認操作。
 - (3) 操作支援畫面之顯示。
- 4、金融機構等所實施之安全對策，舉例如下：
 - (1) 提供服務之系統，防止非法使用之對策，請參照【技 38～45】。
 - (2) 提供服務之系統，提升信賴度之對策，請參照【技 1～5、技 20～24】。

(3) 防止使用者操作錯誤之對策。

(4) 對可疑之違法性交易之監視。

(5) 防止鏈結之使用者誤認、混同之對策。

5、利用網路銀行、行動銀行等執行銀行交易、證券交易、人壽保險、產物保險等交易時，其安全對策，舉例如下：

(1) 利用認證機關發行之電子憑證實施認證作業。

(2) 資金移轉，應事先登錄，以防非法使用。

(3) 資金移轉交易或預約交易，另外設定專用之密碼。

(4) 交易確定前之確認畫面顯示，應有操作支援功能。

(5) 輸入錯誤之次數限制及監視。

(6) 歷史交易明細與交易處理結果，應能由使用者自行查核確認。

(7) 故障或交易取消時之顧客服務中心(CallCenter)支援體制。

(8) 與網際網路服務提供者(ISP)或行動電話中繼站之專線連接。

6、利用網路銀行、行動銀行等執行銀行交易、證券交易、人壽保險、產物保險等交易時，提升可用性之對策，舉例如下：

(1) 依預估之交易量，與網際網路服務提供者之間之通訊線路，應確保足夠之容量及備援線路，請參照【運 54】【技 5】。

(2) 依預估之交易量，安裝性能足夠維持之伺服器設備及設置備援系統，請參照【技 2~4】。

(3) 監視及控制系統運轉時之負荷狀態，設定交易量控制功能，請參照【技 18】。

(4) 利用推薦瀏覽軟體，確認作業之營運。

7、應明確訂定故障、災害發生時之因應作業程序，請參照【運 64】。

(十三)利用開放網路之金融商品

1、電子郵件

利用電子信箱，向使用者提供交易明細、金融商品相關資訊以及回覆問題諮詢時，應考慮電子郵件之特性，判斷對象業務之應用方針應予以明確化。

利用開放網路之金融商品
電子郵件

適用性分類				
共通	中心	總行	合作	直接
				◎

運 107	應明確訂定電子郵件之應用方針。
-------	-----------------

關於電子郵件之運用，為確保其信賴性及安全性，其應用方針應明確化。

- 1、利用電子信箱，對使用者提供交易通知、金融資訊或接洽事項等服務時，應考慮電子郵件之危險性。應考慮之電子郵件之危險性，舉例如下：
 - (1) 被竊聽或偽裝之可能性。
 - (2) 被利用來洩漏資訊之可能性。
 - (3) 送信端錯誤，誤送信件。
 - (4) 感染電腦病毒之可能性。
 - (5) 有可能傳送已感染電腦病毒之附加檔案之可能性。
 - (6) 郵件延遲或遺失之可能性。
 - (7) 對同一網路內使用之其他業務服務，有影響其反應時間之可能性。
 - (8) 因系統故障造成業務中斷之可能性。
- 2、考慮電子郵件之危險性，應用電子郵件之方針應明確訂定。明確之電子郵件應用方針，舉例如下：
 - (1) 防止非法存取之對策，請參照【運 17】【技 35】。
 - (2) 防止機密資料外洩之對策。
 - (3) 電腦病毒之檢查，請參照【技 49～51】。
 - (4) 附加檔案之處理方式。
 - (5) 收送信件容量之限制。
 - (6) 執行適當之內容過濾防護機制。**
- 3、利用電子郵件傳送交易通知、提供金融資訊、接洽事項時，電子郵件之應用方針應明確訂定如下：
 - (1) 交易資料之保護對策。

- (2) 交易等必要資訊之保管。
- (3) 收到訊息時之確認方法。
- (4) 故障發生時，對業務持續執行之對策。
- (5) 設施面之保護對策。

4、應用方針之管理體制，應明確化。

技 術 基 準

技術基準概要

技術基準應考慮技術的進展，而對策的內容則以功能為中心來顯現，實施各對策內容時，為實現其功能所必要的硬體設備、軟體系統等，應妥為建置並適切運用。

技術基準是為提升資訊系統的可靠性、安全性，其構成的要素之硬體設備、軟體系統等相關對策，是由系統可靠性之提升對策及安全性侵害之對策所構成。

一、系統可靠性之提升對策，是儘量避免資訊系統發生故障，萬一發生故障時，亦應將其影響降至最低，並迅速回復正常運轉。提升對策由下列的對策組成：

(一)提升硬體設備之可靠性：維護保養、備援用硬體設備等。

(二)提升軟體系統之可靠性：確保開發時之品質、確保維護時之品質等。

(三)提升營運可靠性之對策：系統操作自動化與簡易化、加強檢核功能、監視控管功能等。

(四)故障之早期發現、早期復原之對策：營運狀況的監視、故障的感應、檢出及隔離功能、故障時之退回及再建構的功能、系統復原功能等。

(五)災害對策：設置災害備援中心等。

二、安全性侵害之對策，由資料的保護、防止非法使用以及防止不正當程式等構成。

(一)資料的保護：防止外洩、破壞、篡改，以及偵測對策等。

(二)防止非法使用：預防對策、經由外部網路的系統存取限制、偵測及對應措施等。

(三)防止非法程式：防禦對策、偵測對策、復原對策構成。

一、系統可靠性之提升對策

(一)提升硬體設備之可靠性

若要提升資訊系統可靠性，首先需要提升硬體設備之可靠性。這是指應極力減少資訊系統本身及其週邊相關連設備發生故障。

其次，當構成硬體設備要素之一部分發生故障時，應有避免影響整個系統之因應措施，這些措施，應依各個硬體設備之特性及其重要性，分別實施。

提升硬體設備之可靠性
預防硬體設備故障之對策

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

技 1	應實施預防保養。
-----	----------

預防硬體設備的故障，應依據裝置的特性及其重要性，定期實施預防保養作業，必要時應隨時加強保養。

1、為提升資訊系統的可靠性，首先應提升硬體設備之可靠性，因此應實施預防保養作業，以極力減少硬體設備發生故障。

2、預防保養作業的具體實例，如下列所示。請參照【運 59】之說明。

(1) 定期保養維護

依據設備的特性及重要性，事先訂定應檢查維護的項目及週期，以防止發生故障於未然，而實施之保養維護作業，可分為下列兩種形態：

a. 整體的保養維護

停止系統整體的作業，進行綜合性的檢查維護。

b. 個別的保養維護

包含系統運轉期間，在不影響營運的範圍內，對個別的裝置，進行檢查維護。同時，系統操作人員在開機起始作業前之清潔工作也是非常重要的。

(2) 不定期保養維護

視情況需要分析個別設備之使用狀況，故障發生情形及相關之異常紀錄 (Error Log)，據以預測故障發生的可能性，防止故障發生於未然之保養維護作業。

3、需要長時間不中斷的作業，如 24 小時作業的系統，仍應衡酌該系統的機能及作業上的限制，實施適當的保養維護作業。

提升硬體設備之可靠性
備用硬體設備

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

技 2	設置主機裝置之備用設備。
-----	--------------

重要之主機設備應設置備援設備。

- 1、主機設備係中央處理器、主記憶體、輸出入通道設備等之總稱，在主從架構的系統，則指系統核心之伺服器。
- 2、依據系統使用目的及其重要性，應儘可能建置與正式作業主機設備處理能力相當之備援設備。尤其對於 24 小時運作的系統，因其需要長時間不中斷的作業，應配合該系統的機能及作業上的限制，設置備用的系統。
- 3、主機設備之備援方式，舉例如下：

(1) 雙工系統 (Duplex System)

當現行系統發生故障時，切換至備援系統，繼續進行業務處理作業。備援系統在待機期間，可以處理其他業務作業，但應具有與現行系統相同程度的處理能力（詳如圖 1）。

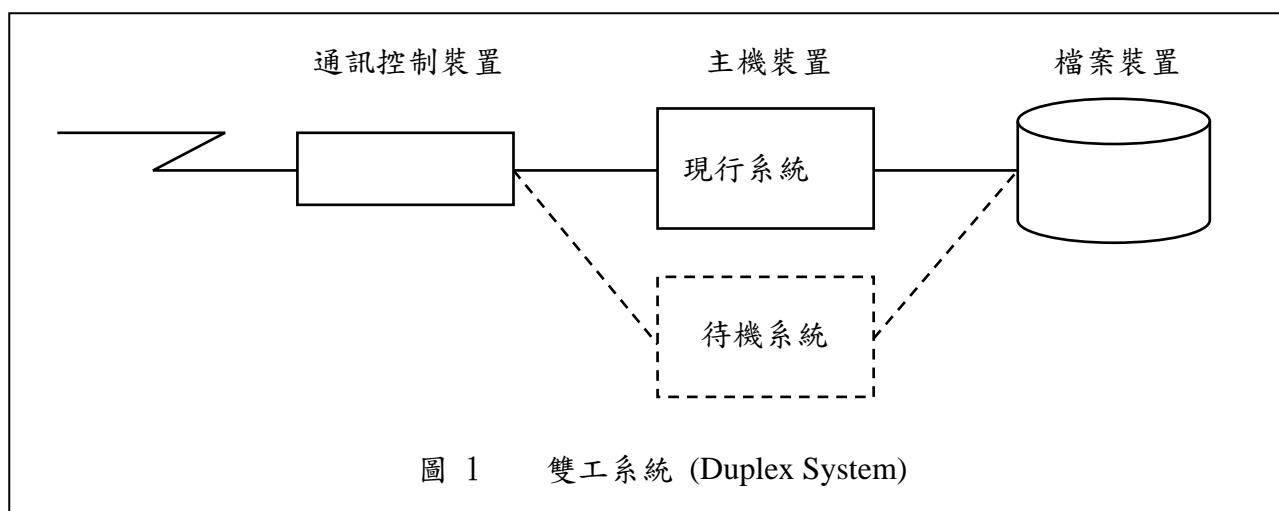
依備援系統的形態，可以分為下列數種方式：

a. 熱機即時備援方式 (Hot Standby)

事先將系統及應用程式等載入，完成大部分系統運轉必要的前置作業，當現行系統發生故障時，立即切換至備援系統，繼續處理業務。

b. 冷機非即時備援方式 (Cold Standby)

平時並不執行系統運轉必要的前置作業，但在現用系統發生故障時，須經必要之轉換程序(含必要之前置作業)後，方能接續處理業務。



(2) 負載平衡系統(load balance system)

兩組(含)以上的主機設備平常並列運轉，相互監視對方的運轉狀況，若有設備發生故障時，由其他存活系統繼續運轉。

(3) 容錯系統 (Fault Tolerant System)

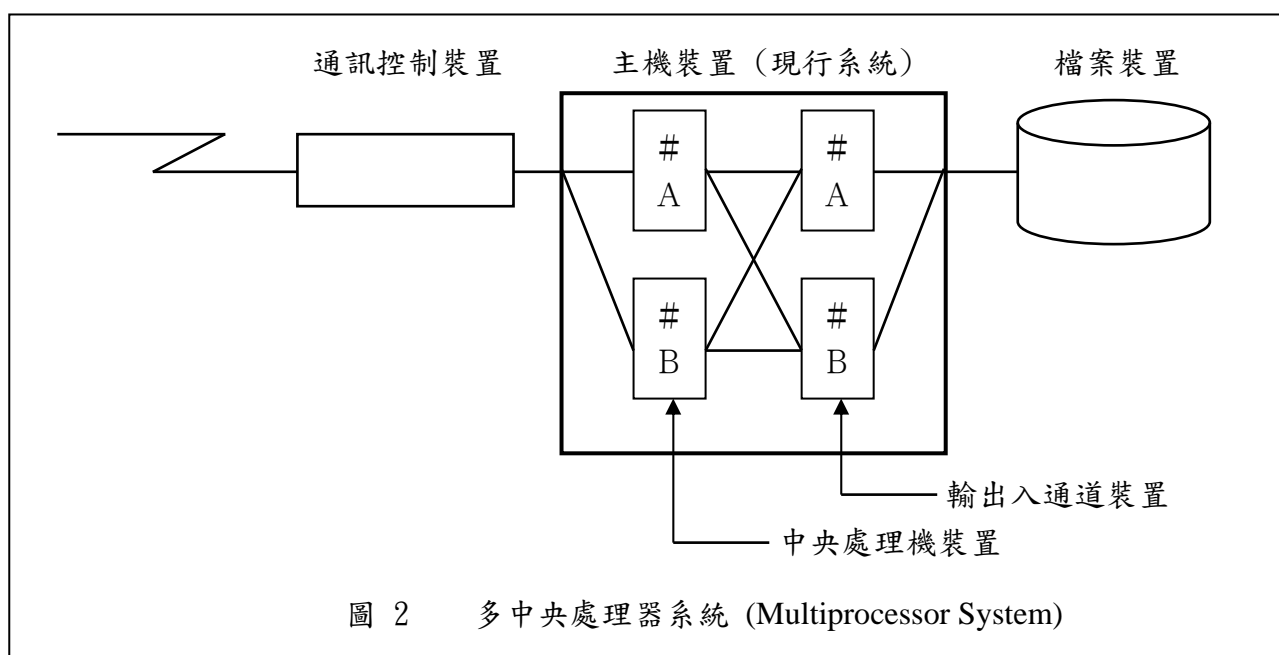
不論發生錯誤或故障，由外表來看，均具有能維持一定水準的處理能力的系統。

一般而言，系統中的主機裝置、磁碟裝置等主要的硬體設備均採多重化，整個系統架構為不停頓的設計，這種容錯系統架構多用於建構主機系統或伺服器系統。

(4) 多重處理機系統 (Multiprocessor System)

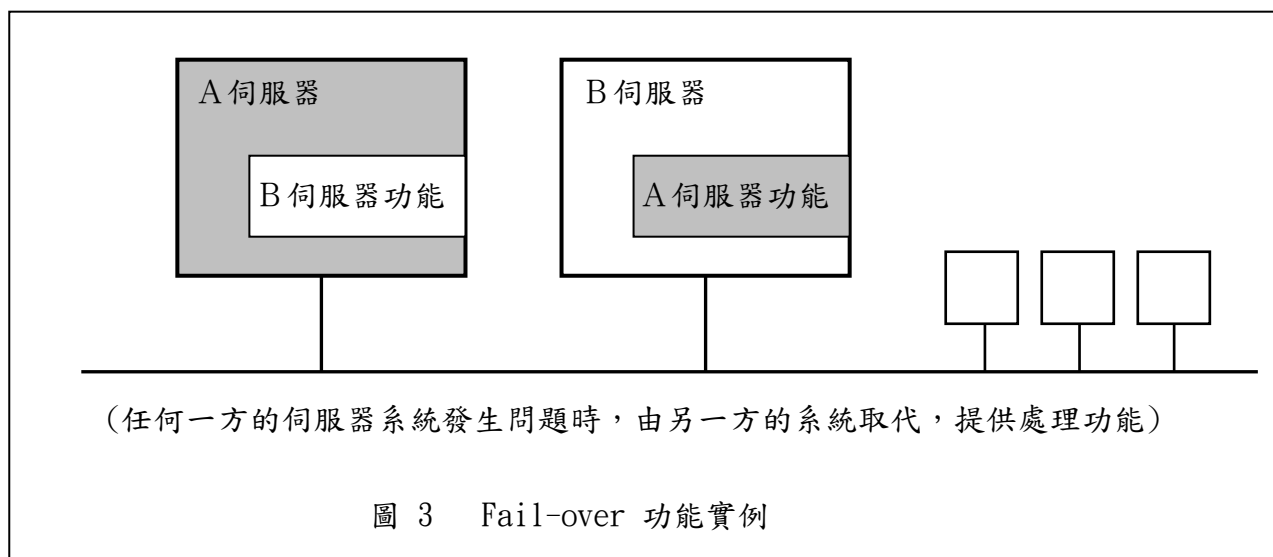
以提升性能與可靠性為目標，結合多部中央處理機 (Processor) 的系統。為提升其可靠性，若某一中央處理機發生故障時，系統具有切離故障的處理機，繼續作業的功能。

在切離故障的處理機而繼續作業的情況下，應仍能維持某一程度的處理能力，中央處理機裝置應有充裕的處理能力。(詳如圖 2)。



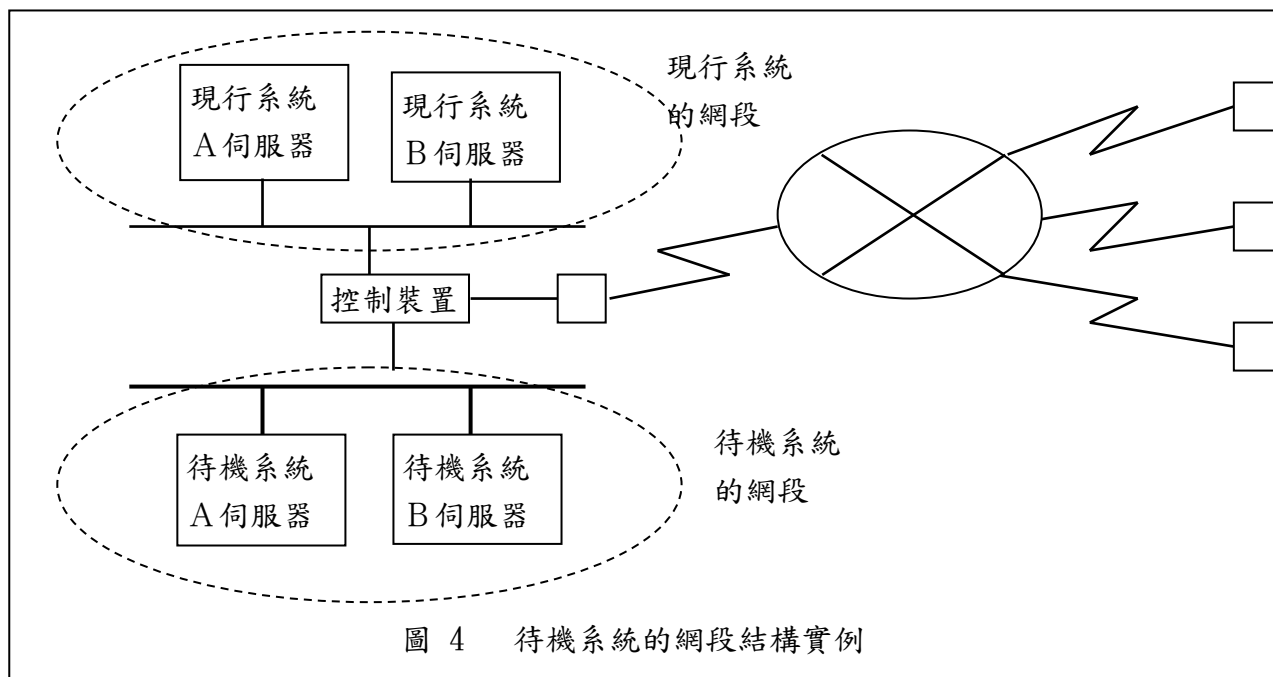
(5) Fail-over 功能

在主從架構的系統，當一個伺服器發生問題而停頓時，立即由另一個伺服器取代，處理作業的功能（詳如圖 3）。



(6) 待機系統之網段結構 (Replicate 結構)

在主從架構之系統，包含重要伺服器的區域網路架構應雙重化，並將其中一個網段作為待機備援用（詳如圖 4）。



提升硬體設備之可靠性
備用硬體設備

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

技 3	設置週邊設備之備援設備。
-----	--------------

重要之週邊裝置應設置備援設備。

1、週邊設備是指檔案設備(磁碟設備、半導體磁碟設備、光碟設備、磁鼓設備、磁帶設備等)、控制臺顯示器等設備。

(主從架構系統之伺服器系統，至於機架內部的磁碟設備，亦屬於週邊設備。)

2、重要週邊設備之備援或替代設備的設置方法，舉例如下：

(1) 以多部週邊設備，設置備用設備

一般情況，檔案設備之備援設備通常提供整批作業使用，連線作業設備發生故障時，始將其切換至連線作業使用，經檔案復原程序後，接續業務處理。另外，亦可利用設備多餘的空間作為備援。

(2) 裝置多部設備，以具備與備用設備相同的效果

(3) 利用異種設備替代

(4) 以網路上其他伺服器的檔案裝置替代

以網路上其他伺服器的檔案設備替代在主從架構之系統，可將網路上其他伺服器的檔案設備，作為本身之備用檔案裝置。

(5) 利用磁碟陣列設備(Disk Array) 作為檔案設備之備用設備

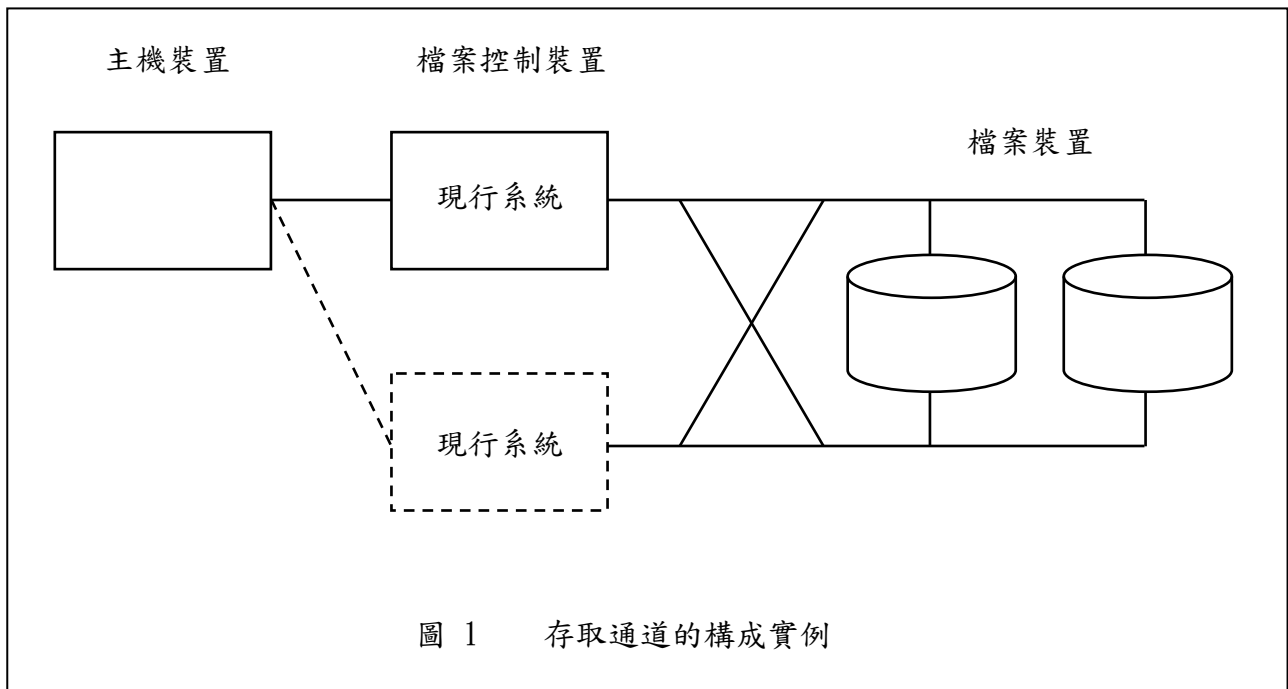
(註)磁碟陣列，是將資料加以分解，以平行方式對多部磁碟進行讀寫的動作的設備，具大容量、高性能、資料保護，以及能提供不中斷運轉可能的碟設備，稱為 RAID (Redundant Arrays of Inexpensive Disk)。

3、有關重要檔案設備與主機設備間的存取通道（連接路徑）

重要檔案設備應設置替代用通道，當正常存取通道發生故障時，可避免檔

案資料無法使用。

存取通道（Access Bus）的構成，如下列所示（圖 1）。



4、對於需要更高層次可靠性的檔案，應考慮雙重化儲存方式。需要雙重化的檔案，舉例如下：

- (1) 主要業務的主檔。
- (2) 作業日誌紀錄檔案。
- (3) 其他系統控制檔案。

提升硬體設備之可靠性
備用硬體設備

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

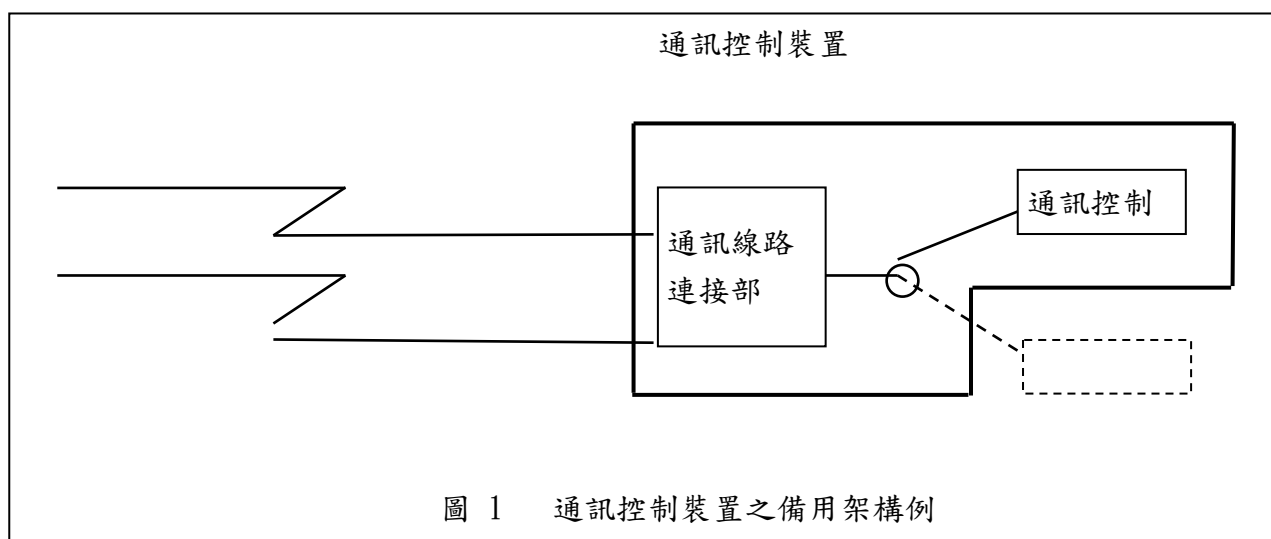
技 4	設置通訊設備之備援設備。
-----	--------------

重要之通訊裝置應設置備用設備。

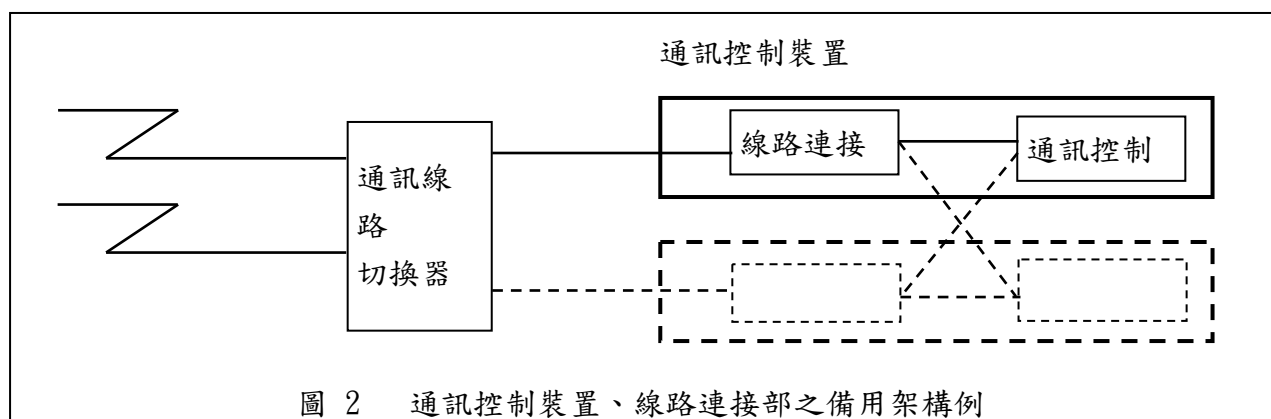
1、應設置備援設備之通訊設備，舉例如下：

(1) 通訊控制設備

a. 通訊控制設備之備援架構例（圖 1）



b. 通訊控制設備、線路連接部之備援架構例（圖 2）



亦可考慮多部通訊控制設備，每一裝置設置備援設備。至於線路切換設備，可依實際情況，檢討適合的切換方式。

(2) 數據機等

數據機設備亦同，對於重要線路，亦需要設置備用設備，在故障發生時，應能迅速對應處理。此處所謂數據機，包含分時多工設備 (Time Division Multiplexer)、數位傳輸終端裝置 (Digital Service Unit) 等。

(3) 路由器 (Router) 等

路由器或集線器 (HUB) 等發生故障時，應能迅速因應處理，對於重要線路，亦需要設置備用設備。

另外，設有網路過濾 (Filtering) 等網路設定參數之設備，除設備需要備用裝置之外，對於設定參數檔案，亦需有檔案備份及復原的作業程序，以提升設備之可靠性。請參照【運 31、運 32】之說明。

(4) 交換裝置

交換裝置發生故障時，應能迅速因應處理，對於重要線路，亦需要設置備用設備。此處所謂交換裝置，是指非同步傳送模式 (ATM) 裝置或訊框傳送裝置等。

(ATM: Asynchronous Transfer Mode)

2、準備數據機或路由器等之備用設備的方式，除機構自備之外，亦可利用與廠商的維護契約中，要求在必要時，隨時提供替代設備的條件，達到有效的準備備用設備。

提升硬體設備之可靠性
備用硬體設備

適用性分類				
共通	中心	總行	合作	直接
	○	○		

技 5	設置備用之通訊線路。
-----	------------

重要之通訊線路應設置備用線路。

1、有關通訊線路的備援線路，應注意下列事項：

- (1) 各地點之間（機構外面）的重要通訊線路，儘可能多重化，以建置備援線路。同時線路多重化時，應要求在實體上經由不同路徑（例如，經由不同的交換局等）。
- (2) 機構內部的線路，在資訊中心之內部配線或重要部門之區域網路線等，儘可能設置備用線路。

2、有關各地點之間（在機構外面的部分）之線路

(1) 備用線路的具體實例，舉例如下：

a. 通訊專線多重化的實例

- (a) 將端末系統設備分為兩個群組，分別以不同的通訊線路連接。
- (b) 兩條通訊線路之一設定為備用線路，並準備切換用裝置及切換程序備用。

b. 利用電話線路（包含 xDSL 線路）、ISDN 線路、通訊交換線路、封包交換線路、訊框（Frame Relay）線路、ATM 線路、衛星通訊線路、光纖通訊網路等，備用之通訊線路（詳如圖 1）。

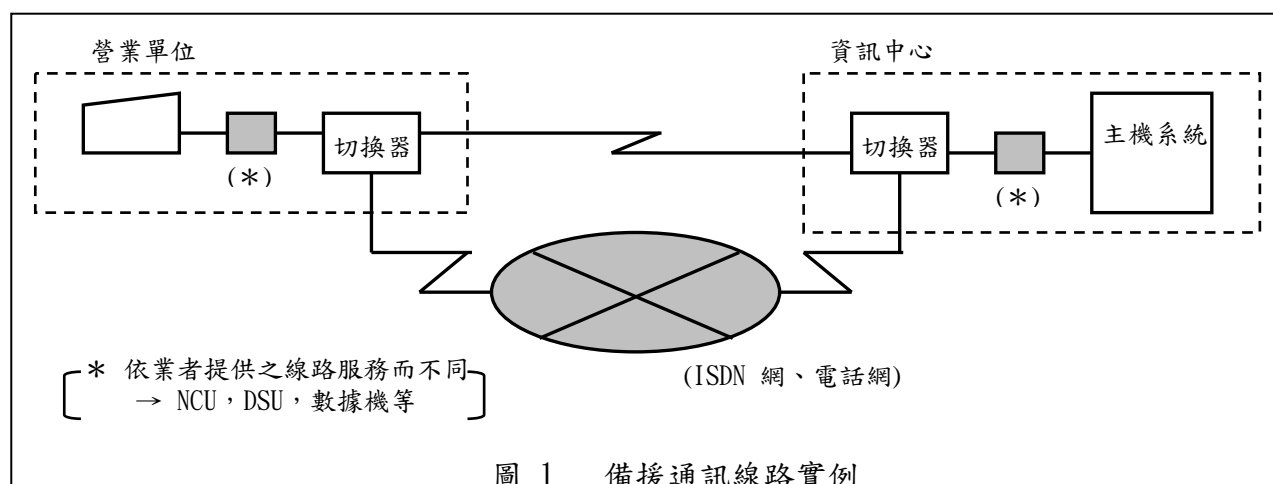
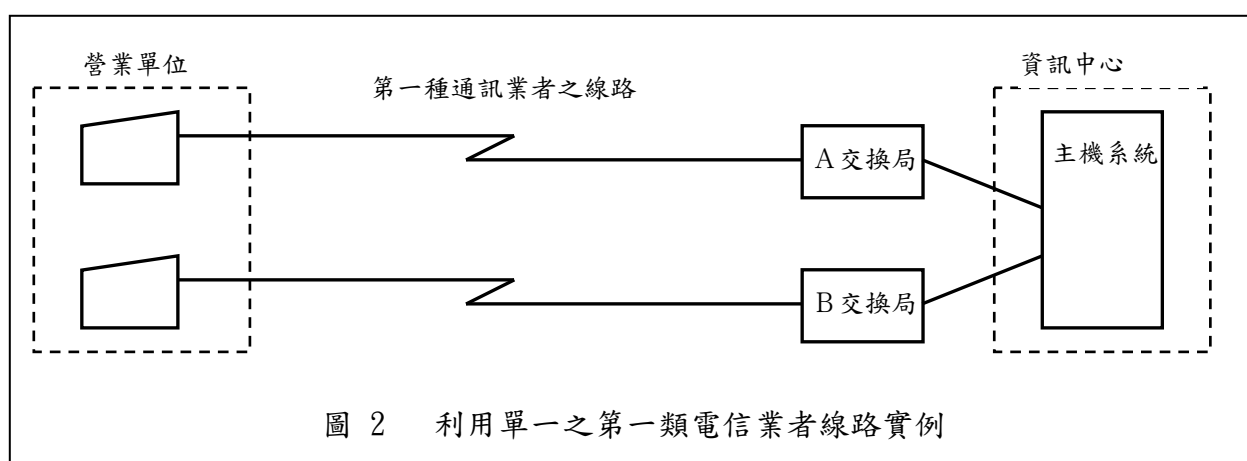


圖 1 備援通訊線路實例

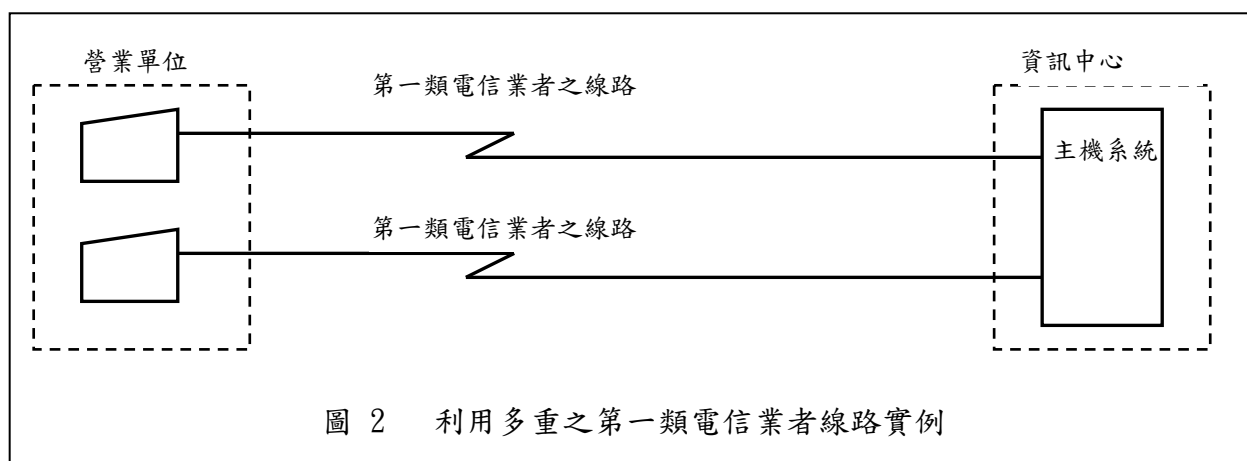
(2) 通訊線路之不同路徑

若通訊線路之路徑發生問題，全部的通訊線路都會中斷無法使用，為防止這類事情發生，應利用多重線路分別連接，以平行方式分散危險。利用單一之第一類電信業者之線路，要求經由不同的交換局（在實體線路上，經由不同的路徑），或利用多重第一類電信業者之線路的方法（詳如圖 2、圖 3）。

a. 利用單一第一類電信業者之線路



b. 利用多重之第一類電信業者之線路



3、機構內部通訊線路

(1) 資訊中心應注意事項

資訊中心通訊線路相關設備至各重要機器設備間的配線，應為雙重化的線路，尤其在建物外部的線路雙重化後，由 MDF 至通訊控制設備的各重要機器設備間的配線，應為雙重化的線路。

(2) 機構內部之區域網路線路

機構內部之區域網路線路，依其重要性，儘可能設置備用線路，備援線路之實例如下所示：

a. 區域網路幹線之多重化（詳如圖 4）

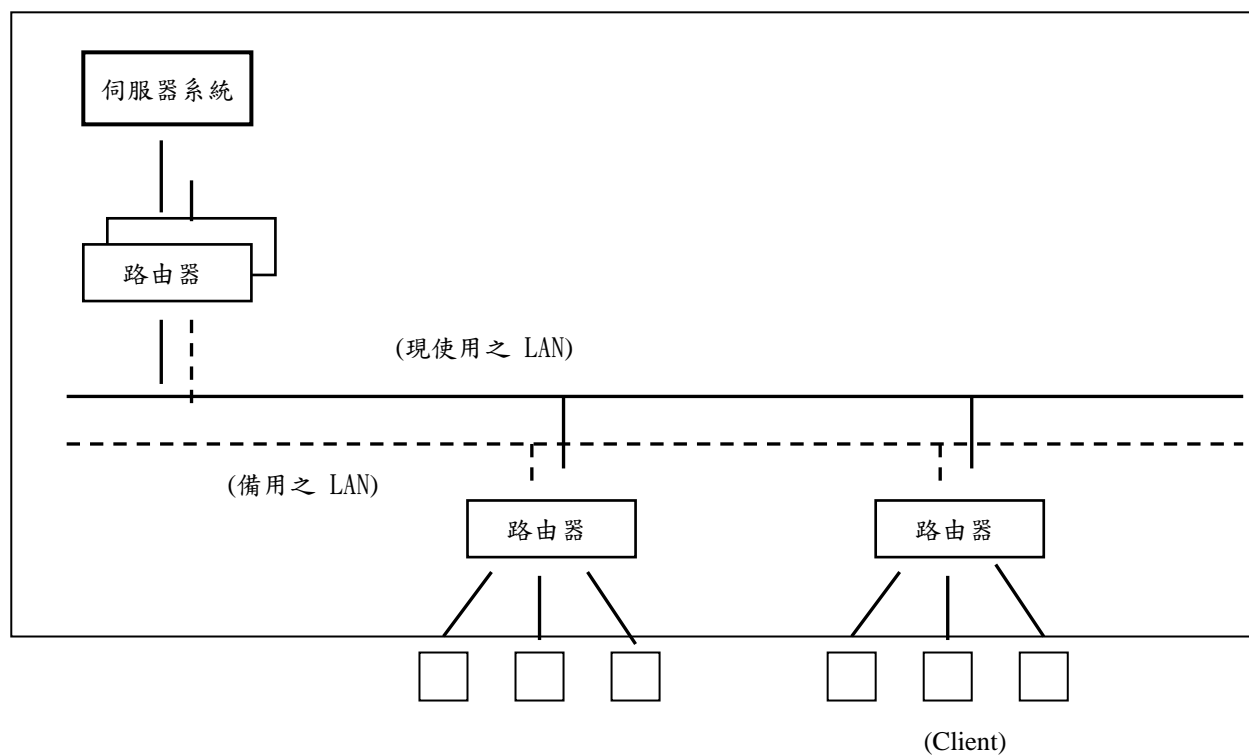


圖 4 LAN 之多重化之實例

提升硬體設備之可靠性
備用硬體設備

適用性分類				
共通	中心	總行	合作	直接
	◎	◎		

技 6	端末系統設備之備用設備。
-----	--------------

端末系統裝置應設置備援設備。

1、端末控制設備（TC 等）、端末設備、Client 設備等之備援設備或替代功能之設置方法，如下列所示：

- (1) 配合規模的大小，依地區別或主要營業單位別設置，或在資訊中心設置備援端末設備。
- (2) 設置多部設備，與設置備用系統具相同的功效。
- (3) 當端末控制設備發生故障，連接於該端末控制設備下的端末機，轉接到其他營業單位之端末控制設備上，繼續作業。
(若端末控制設備有存放該單位專屬的資料檔案 (Local File) 時，應事先研擬故障時檔案之復原對策，或保有備份檔案的方法)。
- (4) 與設備供應商簽定維護合約時，加列故障時，緊急提供備用設備之承諾。
- (5) 端末裝置發生故障時，以其他不同類形的端末設備，或利用其他業務在使用之端末，作為替代的端末裝置。
 - a. ATM、影像 OCR 等專屬端末裝置發生故障時，利用通用端末裝置替代。
 - b. 通用端末裝置發生故障時，利用行外端末設備，作為部分端末之備用設備。
 - c. 業務處理用與管理資訊用之端末設備，相互作為對方之備用端末設備。
- (6) 應事先設置能利用其他營業單位或資訊系統中心的端末設備，代為處理登錄作業的功能。

一、系統可靠性之提升對策

(二)提升軟體系統之可靠性

若要提升資訊系統可靠性，應提升軟體系統之可靠性。由技術面來看，在市面上提出的提升軟體系統可靠性之方法論及工具為數不少，在實際應用上，系統開發的各階段中，應採用那一種方法或工具，或採用這些方法或工具的目的，應明確訂定於系統開發設計的計劃內。同時，為能達到開發作業之標準化及作業的自動化，如何提升軟體系統可靠性的對策，是非常重要的。

其次，使用套裝軟體時，應注意與現運轉中的系統之整合性。在總行、營業單位之使用者，自行開發之作業，應注意參考系統開發部門的規範，以確保其可靠性。

提升軟體系統之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 7	應確認系統開發設計與中長期計劃的整合性。
-----	----------------------

為提升資訊系統整體的的可靠性，系統的開發設計與中長期計劃應具整合性。

- 1、資訊系統的開發，應與其它開發中的系統，在功能及作業上確實分攤，以發揮整體的系統功能，為達到這個目標，系統的開發計劃，應考慮中長期資訊系統化計劃，以獲整體的整合性。
- 2、為能廣泛的檢討資訊技術的適用性，擬定開發計劃，應調查內外部的資訊技術。若系統需要委外開發時，應請委外之廠商提出詳細說明，以分析判斷所採用技術之適當性。所需調查的重點，舉例如下：
 - (1) 技術的特徵，適用條件。
 - (2) 技術的性能評比。
 - (3) 費用效能比的評比。

提升軟體系統之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 8	納入必要的安全控管機能。
-----	--------------

為確實實施安全控管，在系統計劃階段就應將必要的安全控管機制納入，並使其明確化。

- 1、有關開發中的系統應具備的安全控管功能，或實現這些安控所需的技術等，應在系統規劃設計階段，即加以考慮。
- 2、安控對策應與整體系統開發計劃，取得整合性，依處理的業務或資料的重要性及風險性，決定其安控對策。

提升軟體系統之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 9	在設計階段確保軟體之品質。
-----	---------------

為在設計階段提升軟體的可靠性，開發前提應明確化，同時考量具可靠性設計、採標準化之設計作業等，確保軟體的品質。

1、為確保軟體系統的品質，設計階段要求高品質是非常重要的，為此應考慮的要項舉例如下：

(1) 應加入安控機制

為確保有關安控之品質，在設計階段即應加入安控的機制，請注意下列事項：

- a. 以安控政策為基準，應加入企業（或組織）視為必要的安控機制。
- b. 將安控機制列為使用者的需求要件。

(2) 活用提升品質的設計技巧及工具

設計的技巧及工具，是配合技術的進步，經常更新的方法或提案，應經過研究檢討，並建立組織體制、推展標準化、實施教育訓練等。

2、確保品質的具體實例，如下列所示：

(1) 系統開發的前提需求明確化

a. 安控需求的明確化

有關安控需求的明確化，應注意下列事項：

- (a) 應滿足安控政策。
- (b) 應滿足使用者需求要項的安控機制。
- (c) 開發新系統時，若發現已開發或安裝使用的系統有安全上的弱點，應一併解決問題。
- (d) 稽核軌跡（可以作為處理內容歷史的軌跡日誌記錄等）之建置功能等需求應明確化。

b. 使用者需求要項的明確化

開發中系統之使用者需求要項，如資料輸出入需求、主要功能需求（業務處理內容）、硬體設備需求等。

c. 設定開發目標

為確保安全性與軟體品質應根據使用者所提需求要項，從可靠性、功能、性能、操作性、擴充性、維護性等方面予以綜合考量，設定開發目標。

(2) 設計作業的標準化

設計作業標準化的對象，舉例如下：

a. 設計過程

設計過程中應執行的作業、內容、範圍等。

b. 文件

記述設計內容的文件內容、編製的程序等。

c. 檢核 (review)

檢核程序、實施基準等。

(3) 可靠性設計的考量

不僅需努力減少錯誤的發生率，同時在設計時應考慮可能發生的錯誤及避免的方法，舉例如下：

a. 錯誤侷限化的設計

若軟體發生錯誤，應能防止影響擴散，將錯誤的影響範圍侷限化。

b. 檢出異常情況，並加入其因應對策

檢出異常情況，並將其因應對策體制化。

(4) 實施檢核

檢核是指為提升系統之完成度，在系統開發的各階段，召開檢討會，請其他人員檢討檢核設計書等。同時，在實施檢核時，應從是否容易測試、文件可讀性、容易維護等各種觀點來檢討。

提升軟體設備之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 10	在程式撰寫階段，確保軟體的品質。
------	------------------

依據程式規格書撰寫程式時，應實施程式撰寫的標準化、自動化、安全性等，以能在程式撰寫階段，確保軟體的品質及減少程式的安全漏洞。

1、在程式撰寫階段，確保軟體品質的方法，以下是標準化、自動化之實例

(1) 標準化

a. 選擇適當的語言

考慮整體開發的效率，應適當的選擇語言，作為軟體開發的工具。

b. 程式驗證 (Inspection) 的規則化

撰寫完成的軟體，是否符合程式規格書所指定的內容，應經由他人的驗證。尤其以核心程式或是技術及標準化經驗尚淺之新進人員所撰寫的程式為對象，驗證方法規則化，能有效早期發現程式的錯誤。另外，依據驗證的結果，實施追蹤作業，對於減少往後的錯誤非常有效。

c. 模組化、定型化之有效運用

將經常使用的典型程式與使用頻率高的程式部份段落模組化並登錄，以便靈活運用。

d. 其他

(a) 程式撰寫規範的訂定

實施程式撰寫的標準化，以消除程式撰寫人員之個別差異，提高程式讀取的容易度，同時減少程式錯誤。

(b) 利用結構化程式的技巧

利用三種基本的控制結構（連續執行指令的單純結構、選擇執行指令的分歧結構、反覆執行指令之迴圈結構）或其組合，作成程式的一種技巧，可以減少程式錯誤的發生。

(2) 程式編製之自動化

a. 利用自動化程式編製工具

利用下列之自動化程式編製的工具，是一種有效的方法

(a)利用「規格記述語言」編製半成品程式。

(b)利用交談式的畫面定義編製程式。

(c)檢核設計規格與程式內容是否符合。

b. 活用文件編製工具

活用編製文件的工具，亦是有效的方法，例如，程式詳細處理流程說明書（流程圖等）的編製工具。

2、在程式撰寫階段，應預防電腦病毒等不正當程式的入侵。特別是在網路系統環境下開發程式時，在程式開發者之間的檔案共用，或使用市面販賣的套裝軟體等情形，電腦病毒入侵的機會非常多，應利用電腦病毒檢查軟體等作必要的監視。請參照【技 49、技 50】之說明。

3、在程式撰寫階段，將 OWASP 等常見的網站應用程式弱點納入軟體開發安全參考，避免產生類似弱點，並於程式開發階段執程式碼安全檢測，以減少程式的安全漏洞。

提升軟體設備之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 11	在程式測試階段，確保軟體的品質。
------	------------------

為在程式測試階段，提升軟體的可靠性，應擬定測試計劃、準備測試環境與測試體制、並活用支援測試的功能，在測試階段實施各種管理，以確保軟體的品質。

1、應能事先發現並剔除軟體內在的瑕疵，同時充分測試驗證軟體的正確性。

2、為確保軟體品質，應注意下列各事項：

(1) 擬定測試計劃書

隨著對系統需求的多樣化，需要開發的系統本身亦複雜化，因而評估可靠性之軟體品質測試作業亦隨之複雜，在這種情況下，最重要的就是能讓測試階段順利進行的測試計劃書。

在測試計劃書中，應明確訂定的項目，如下列所示：

a. 實施方針

測試分類與目的，測試完成的基準、測試時程等。

b. 實施體制

測試體制的工作職掌分攤及人員指派等（詳如下面所述）。

c. 實施方法

測試工具及其使用方法、驗證方法、作業申請方法等。

d. 實施之資源

測試環境、資源預估。

e. 實施管理

程式管理（程式庫管理、資源管理等）、問題管理、文件管理、進度管理、品質管理、委外管理等。

(2) 測試體制的建置

對於測試項目龐大的系統，為求測試作業的效率、確保軟體的品質，應成立執行測試的專責單位，分工合作。測試結果的收集，應由對內

容充分了解的人員負責。同時對於人員的指派，應請使用單位及營運部門的人員參與，提高測試的效果。

(3) 測試工作的分類

測試工作的分類，有種種方式可以考量，例如下列所示的方式：

a. 單元測試以程式模組為單位，測試驗證特定程式範圍的功能。

b. 連結測試

將程式模組結合（以程式為單位或以子系統為單位）進行功能之驗證測試。

c. 系統測試（整體測試、整體運轉測試）

在設計階段所計劃的系統需求功能，是否能依計劃的內容確實運作，可利用系統整體測試方式，進行功能驗證。

為驗證軟體的品質，除利用系統測試工具、超負載之壓力測試工具、異常情況測試工具等進行測試之外，亦應考慮以近似正式作業環境的系統測試。為驗證軟體品質，應做如下之測試：

(a)性能測試。

(b)例外處理測試。

(c)復原作業測試。

(d)系統使用者參與之模擬測試。

(e)邊際值測試。

(f)連接測試（包含通訊線路之連接、記錄媒體的交換作業等）。

(g)有關機密保護之安控功能測試。

(4) 各種測試工具的活用

為能有效率的實施測試工作，可以考慮使用種種的測試用工具，舉例如下：

a. 在單元測試、結合測試（整合測試）作業所使用的工具實例

(a)驅動程式（Driver，測試下層模組之工具）

執行編譯（Compile）時之最小模組的測試工具。

(b)中介模擬測試（Stub Simulator）（代替未完成模組的測試用工具程式）

在進行程式測試時，模擬未完成的下層模組功能之測試工具。

(c)除錯工具 (Debugger)

在進程式測試中，輔助程式除錯的工具。

(d)涵蓋率 (Coverage) (測試涵蓋範圍的管理工具)

在程式測試的全程，能夠管理已經測試了那些程式邏輯流程，其佔全部測試途徑的比率等之工具軟體，是了解測試工作是否充分進行的評估指標，也是測試進度管理的工具。

(e)測試資料產生器

為建立足夠大量的測試用資料，以雛型測試案例為基礎，自動產生詳細分類的大量測試資料的工具。

b. 系統測試 (整體測試、整體運轉測試) 作業之測試工具實例

(a)系統測試用工具

具備系統整體運轉、測試所需之測試環境，測試資料產生功能、記錄測試結果等功能等之工具。

(b)超負載壓力測試工具

備有能建置超負載作業環境的工具。

(c)異常情況測試用工具

備有能建置異常狀況的工具。

(5) 測試實施階段之各種管理實例

測試實施階段之各種管理實例，如下列所示。另外，在測試終了後，應編製測試結果的報告書，呈報開發負責人。

a. 程式管理

為使未來程式的編製、變更及刪除等容易進行，應進程式管理，管理內容如下：

(a)程式庫管理

在測試階段，測試、發現錯誤 (缺陷)、修改 (除錯) 程式等作業重複執行。為能有效執行這些作業，依照單元測試、整合測試、系統測試 (整合測試、整合運轉測試) 等作業別，或依業務別，對程式分成不同的程式庫分別管理。

(b)資料辭典 (Data Dictionary) 管理

程式所需參照的資料或程式相互間的關連等，作一統籌的管理，

以確保在測試階段，能周全的管理變更，而不致於遺漏。

(c)變更管理

對於新需求要項之追加、需求要項之變更，文件、程式等之修改變更管理，應明確訂定並加以管理，同時應通告所有相關人員。

b. 問題管理

分析了解問題的原因，並迅速確實修正解決該問題，掌握、管理發生問題的情況及趨勢，以防止相同、類似情況的再發生。

c. 文件管理

測試規格書（測試案例一覽表、測試項目等）、測試資料、測試結果報告書、測試範圍內涵報告書等測試文件，應於各測試階段整理完成，並加以管理。

d. 進度管理

為早期發現測試所發生的問題，並儘早規劃因應對策，應依照測試計劃，管理並控制測試作業的進行。

e 品質管理

根據測試的結果，驗證並管理是否滿足品質管理基準值。為防止測試環境（測試工具或測試用媒體）受電腦病毒等不正當軟體的入侵，也是這個階段的品質管理之一。

提升軟體設備之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 12	程式派送至使用單位時，應確保軟體的可靠性。
------	-----------------------

為確保程式派送至使用單位時的可靠性，應確認軟體與發送之使用單位作業環境之整合性。

1、主從架構的系統等，在派送業務用應用軟體時，程式開發測試的環境與正式作業的系統環境可能不盡相同，應事先確認其整合性。

應考慮注意的事項，如下列所示：

(1) 硬體環境（微處理器、記憶體容量等）之差異。

(2) 作業系統、中介軟體等之差異，以及這些軟體的版本差異等。

同時，應假設這些原因造成系統無法正常運作時之復原作業程序與軟體更新修正的作業程序。

2、利用電腦病毒檢查軟體，確保安全性。

為防止程式在開發測試時，混入電腦病毒等不正當的軟體，將程式散佈各單位之前，應先利用電腦病毒檢查軟體進行掃毒。

防止電腦病毒等不正當軟體之入侵，請參照【技 49、技 50】之說明。

提升軟體設備之可靠性
提升開發品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 13	外購套裝軟體時，應確保軟體的品質。
------	-------------------

為確保外購套裝軟體的品質，應事先確認該軟體之功能以及與機構內現有系統之整合性。

在外購業務系統之套裝軟體時，確保其品質的具體做法，舉例如下：

1、導入套裝軟體需求要項之明確化

(1) 使用者需求的明確化

要購入套裝軟體之使用單位的需求，有輸出入資料的需求要項、主要處理功能需求（業務處理內容），硬體需求要項等。

(2) 目標的設定

根據使用者的需求，有關安全性的確保及軟體品質的確保等，應設定可靠性、功能、性能、操作性、擴充性、維護性等目標。

2、記載相關功能之規格書、設計書、測試確認書等文件之確保

確保安全性、軟體品質以及軟體之維護作業，必要的文件。

3、自行於公司內測試

為確認功能、性能、操作性等之測試作業，請依照【技 11】之準則。

提升軟體設備之可靠性
提升維護品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 14	確保定型化變更作業的正確性。
------	----------------

為確保新設營業單位或新增機器設備之定型化變更作業的正確性，應有變更作業合理化之對策。
--

屬於定型之變更作業，如新設營業單位或新增機器設備等，為確保作業正確性，可執行的方法如下：

1、變更作業之合理化

(1) 定義之統一

將營業單位、機器設備等之定義資料，利用表格或資料庫予以整合統一，避免因單一項目的變更，導致多處皆須修改之情形。

(2) 變更程序之簡化

為提升變更作業的可靠性，對各相關之表格或資料庫的內容之修改、追加或刪除，簡化變更作業的程序。

2、變更內容及作業程序的文件化

伴隨定型變更的變動及測試所需的程式等，應維持在最新的狀態，同時應備妥記載變更處所、變更方法等文件。利用這種方法，可以確認變更作業是否有遺漏，以確保其正確性。

3、確立測試及驗證的程序

為確保變更作業之正確性，應建置變更結果的整合性及妥適性之檢核工具（變更部分的測試、副作用測試及檢核項目表等），作業程序亦需編製成手冊。

提升軟體設備之可靠性
提升維護品質

適用性分類				
共通	中心	總行	合作	直接
◎				

技 15	應確保功能變更、新增作業時的品質。
------	-------------------

在功能變更、新增作業時，為能確保程式的品質，應比照開發時提升品質之對策。

軟體功能的變更、新增作業，應檢討伴隨變更、新增可能所產生的影響，並將影響減至最低，舉例如下：

1、確認變更、追加之處

(1) 活用文件產生輔助工具

有效應用產生程式文件的輔助工具，利用文件檢核、確認變更之處。

(2) 活用新舊程式比較工具

比較變更、追加作業前後之程式，以確認是否按原訂目的修改變更，並確定不需修改的部分為被更動，以避免發生新的問題，或被編入非法的程式邏輯。

2、影響程度的驗證

(1) 建置測試環境及測試資料

利用變更前的測試資料，針對變動部分以外的部分，確認測試結果是否與變更前相同，這是活用測試環境與測試資料的方法。

(2) 活用影響程度的確認工具

編製程式與程式、程式與檔案、程式與資料之對照表（Cross Reference），以便確認功能之變更、新增等對那些程式或檔案發生影響。

3、功能變更、追加作業之故障對策

(1) 備份作業

在功能之變更、新增時，除致力於品質的確保外，在變更作業前，應事先完成系統之備份作業，以因應對變更、新增可能產生的故障。

(2) 訂定故障之復原程序

故障發生時復原作業程序，應事先研訂、測試、演練。

一、系統可靠性之提升對策

(三)提升營運可靠性之對策

為提升資訊系統可靠性，除應提升硬體設備、軟體系統等之可靠性之外，人工操作也是提升作業可靠性之重要因素。

為提升營運之可靠性，除系統操作之自動化、簡易化等對策之外，如何充實妥適性、正當性的檢核功能，亦是非常重要的。

提升營運可靠性之對策
提升營運可靠性之對策

適用性分類				
共通	中心	總行	合作	直接
○				

技 16	力求系統操作之自動化及簡易化。
------	-----------------

為提升營運作業的可靠性，系統操作應力求自動化及簡易化。

1、通用主機與伺服器的操作

為提升資訊中心或總行、營業單位等資訊系統操作之可靠性，利用自動化之硬體設備及軟體系統，力求系統操作自動化及簡易化是非常重要的，自動化的方法舉例如下：

(1) 資訊中心的系統操作

a. 自動化

建立並活用自動執行系統開啟或業務應用啟動、作業（Job）啟動與作業模組對應等，各種自動化營運的機制。或是依實際情形開發相關的功能，以增進資訊中心的作業自動化。

依據排程之作業群組（Job Group）及作業順序（Job Sequence）之作業自動啟動，或利用定時器按時啟動作業之自動化之外，有下列作業自動化方式：

- (a) 插上電源後，啟動電腦系統、開啟連線作業、開啟端末系統，到業務應用程式的運轉，一連串作業之自動化。
- (b) 依照平日、峰日、月底、週末等之型態，作業預先排程，並一起發送通報，將端末系統作業模式的變更自動化。
- (c) 交易日誌記錄檔案由整批作業承接的自動化。
- (d) 交易日制記錄檔案交由其他系統承接處理的自動化。
- (e) 端末系統關閉至連線作業結束之間，一連串作業之自動化。
- (f) 系統停止作業之自動化。
- (g) 磁帶裝卸作業之自動化。

關於自動運轉作業應注意的事項，當處理的順序或運轉狀況、條件發生變動時，為避免影響系統整體的作業運轉，應能變更自動化作業程序的功能，變更的內容，舉例如下：

- (a)一起發送通報或變更端末系統作業模式時間之變更。
- (b)系統的變更（由正式作業系統變更為備用系統，或其反向的變更）。
- (c)由自動運轉切換為人工操作的運轉。
- (d)作業網（Job Network）中，作業之追加、變更等。
- (e)模組之追加、變更。
- (f)執行 JCL（作業控制語言）的變更。

b. 簡易化

為求系統操作之單純、簡易化，應統一指令的體系，輸出的訊息文字，以及操作介面的平易化，同時將系統操作標準模式化，對需連續下達的指令，亦予以結合單純化，以下簡易化的實例：

- (a)輸入的指令儘量減少。
- (b)儘量減少磁帶的裝卸作業。
- (c)作業異常結束後之重新啟動，其操作應定型化。

c. 自動化簡易化應注意事項

資訊中心作業自動化之推進，對提升系統操作之可靠性是非常有效的，但過度的自動化，有可能會對阻礙到機械運作之安全性。在這種情況下，應提供訊息給系統操作人員，留給操作人員作判斷的餘地。對需要操作人員應答的訊息，或需提醒操作人員的注意訊息等，應能以高亮度或紅字等顯示，並發出聲音（在操作人員應答後自動復原），以預防操作人員不慎遺漏重要的訊息。

(2) 總行、營業單位之操作

總行、營業單位，重要伺服器的操作，應模仿資訊中心的操作自動化、簡易化。若在總行、營業單位無法配置具電腦系統專業知識與技能的人員時，自動化運轉，應有能由遠端遙控操作的功能。

a. 自動化

總行、營業單位，重要伺服器操作的自動化，舉例如下：

- (a)插上電源後，系統的開啟及應用程式的起動。
- (b)備份的取得及資料庫的更新程序。
- (c)故障發生時，資料之退回程序及系統關閉程序。

b. 簡易化

作業操作之簡易化，舉例如下：

- (a)操作用介面友善化（採用 User Friendly 的介面）。
- (b)將一連串的指令合併為一個，儘量減少指令的輸入動作。
- (c)系統異常終了時之重開動作單純化。

2、資料輸入作業（端末機的操作）

(1) 自動化

活用磁條讀取裝置、現金處理機、光學字體閱讀機等，以減少或取消人手輸入資料的操作。

(2) 簡易化

活用操作指引功能，以減少輸入之判斷，或利用代碼之輸入，使端末的操作簡單化。

提升營運可靠性之對策
提升營運可靠性之對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 17	系統操作之檢核功能。
------	------------

為防止系統操作之失誤，應充實系統操作之檢核功能。

1、主機、伺服器系統的操作

為防止操作的失誤，並早期發現錯誤，應充實操作檢核功能。

(1) 資訊中心的系統操作

資訊中心有關系統操作的檢核功能，舉例如下：

a. 輸入指令之再確認功能

在資訊中心，對於操作錯誤可能引起重大系統故障的指令，應設有再確認的功能。

b. 檢核妥適性的功能

作業處理的順序因營運狀況、條件（時段、星期別等）之不同，應具檢核輸入指令之妥適性的功能。

c. 使用磁帶檔案時，應有檢核磁帶標籤的功能

為檢核使用磁帶檔案之正確性，應有效活用作業（Job）與磁帶標籤（Tape Label）之對應檢核功能。

(2) 總行、營業單位的系統操作

總行、營業單位等重要伺服器系統的操作，應具備與資訊中心相同的指令檢核功能。

2、資料輸入作業（端末機之操作）

對於電腦系統之端末操作者所輸入的資料，應具有檢核的功能，舉例如下：

(1) 輸入資料之檢核功能

輸入資料項目檢核（如位數溢位的檢核，或應輸入資料欄位之檢核等），以及項目之間相互關連之檢核，帳號之檢查碼檢核功能等，應

具有充實的資料檢核功能。

(2) 各種合計欄之檢核功能

除各個輸入資料的檢核之外，對經由端末機輸入之交易，應具有勾核筆數及金額等合計數的功能（如精算櫃臺之日結數核對），請參照【技32】之說明。

提升營運可靠性之對策
提升營運可靠性之對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 18	加強對系統負荷狀態之監控。
------	---------------

為使資訊系統穩定運轉，應監視系統負荷狀況，以免超過各類資源之能力或容量限制，必要時應有控制機制。

1、對資訊系統負荷狀態的監視與控管的實例，舉例如下：

(1) 監視功能

a. 顯示負荷狀態功能

掌握中央處理機、輸出入通道裝置、檔案裝置、通訊控制裝置、通訊線路等負荷狀態之顯示功能。

b. 查詢使用狀況功能

掌握主記憶體、檔案裝置等資源使用狀況（緩衝區、檔案容量等）之查詢功能。

同時，當使用率接近容量之臨界值時，應設置發出警訊的功能。

c. 統計分析功能

具有收集各類資源的使用狀況，如平均值、最大值等功能，經統計分析並定期檢核，事先擬定因應對策。

(2) 資料流量（Traffic）控制功能

為維持系統的穩定運轉，應設置控制資料輸入的功能，以便控制訊息等待佇列或系統控制重要計數器等之使用容量不致超過臨界點。

另可利用作業的優先順序及處理之多重化等調整控制資料的流量。

2、配置於總行、營業單位的機器設備，利用遠端集中監視、控管的功能較為有效。至於分散環境的負荷狀態監視功能，可利用 SNMP（簡易網路管理協定）等通訊協定，定期收集各節點（Node）裝置的管理資訊資料庫（MIB），並於收集之資料超出臨界值時，自動送出警訊，以達遠端遙控節點裝置的

效果。

(SNMP : Simple Network Management Protocol)

(MIB : Management Information Base)

提升營運可靠性之對策
提升營運可靠性之對策

適用性分類				
共通	中心	總行	合作	直接
	◎	◎	◎	

技 19	加強ATM之異常偵測能力。
------	----------------------

為使自動化服務區之ATM穩定運轉，應集中監視其營運狀況，**並應加強異常偵測之能力。**

集中監控無人化服務區 ATM 之營運狀況，除考慮設備基準上的要求之外，在技術面亦需考慮實施安全對策。請參照【設 111～設 117】之說明。

- 1、應設置能偵測異常狀況（現鈔短缺、紙卷收據等之夾紙、機器設備之異常、通訊線路中斷等）之裝置。
- 2、偵測現鈔、交易紀錄紙卷等即將用罄情況，並採取適當處理。
- 3、偵測各設備運轉狀況（錯誤狀況的蒐集統計），並採取適當的預防作業。

一、提升系統可靠性的對策

(四)故障之早期發現、早期復原

在系統發生故障時，能即時偵測故障狀況，將其影響降至最低，並迅速採取系統復原的措施。

故障之早期發現、早期復原
故障之早期發現

適用性分類				
共通	中心	總行	合作	直接
◎				

技 20	設置系統運轉狀況的監視功能。
------	----------------

為能及早發現及復原，應設置能監視資訊系統使用狀況（運轉狀態、停止狀態、錯誤狀態等）的機制。

1、對於資訊系統運轉狀況，依系統之重要性，應有適當的監視能力。具體的監視功能，舉例如下：

(1) 利用軟體監視

定時存取系統裝置，以掌握系統運轉狀況。

(2) 透過控制台顯示系統狀態

由系統操作人員，利用查詢指令，顯示系統各項設備之運轉狀況。

(3) 透過遠端監視面板等之遠端監視功能

利用能顯示系統運轉狀況及錯誤訊息的顯示裝置，進行遠端監控作業。

(4) 利用服務處理機（Service Processor）之監視

使用維護診斷專用之獨立處理機，即時掌握系統的運轉狀態。

2、隨著系統規模的擴大，集中監控更加重要。具體的監視實例，舉例如下：

(1) 資訊系統的監視包含中央處理裝置、輸出入通道裝置、各種檔案裝置等運轉狀況之集中監視。

(2) 網路之監控包含通訊線路、多媒體變換裝置、分時多工裝置、數據機、路由器、HUB、端末設備等運轉狀況之集中監視。

3、其他

主從架構之系統，對設置於總行、營業單位之伺服器，應依其重要性設置監視機制。總行、營業單位若未配置具備資訊技術之人員，則除遠端集中監視機制外，亦應具備遠端控制功能，以協助處理困難或問題。例如：

(1) 伺服器的電源開關控制（遠端電源開關控制）。

(2) 對 DBMS 等中介軟體（Middleware）或業務處理軟體的啟動、結束及系

統環境最適化調整。

(3) 資料存取分散化及對交易處理優先順序 (Priority) 的調控。

故障之早期發現、早期復原
故障之早期發現

適用性分類				
共通	中心	總行	合作	直接
◎				

技 21	設置故障偵測及將故障部位隔離的機制。
------	--------------------

為迅速復原發生故障的系統，應設置能確實偵測資訊系統發生的各種故障，必要時並能夠將故障部位予以隔離。

能夠偵測系統故障，並將故障部位隔離的功能，舉例如下：

1、偵測異常狀況功能

為迅速進行故障回復，偵測異常狀況之功能舉例如下：

(1) 中央處理機、主記憶體、檔案設備、通訊線路、端末設備等之故障偵測功能。

(2) 程式故障偵測功能

2、系統紀錄 (Logging) 功能

為迅速隔離發生故障部位，須具備記錄功能，舉例如下：

(1) 記錄發生錯誤時，系統相關詳細資訊。

(2) 記錄系統主控制台訊息 (Console Message)。

(3) 記錄可供追蹤至故障發生前，系統運轉狀況的詳細資訊 (例如，輸出入追蹤資訊、程式模組追蹤資訊等)。

3、測試功能

為能迅速隔離發生故障部位，須具備測試功能，舉例如下：

(1) 為隔離發生故障部位所需之折返測試。

(2) 為隔離發生故障部位所需之診斷測試。

故障之早期發現・早期復原
故障之早期復原

適用性分類				
共通	中心	總行	合作	直接
◎				

技 22	應設置發生故障時，能縮小範圍並重組系統的功能。
------	-------------------------

發生故障時，除一部分的處理中斷外，為使系統繼續運轉，不致整體停頓，應具有縮小機能並重組系統的功能。

1、系統機能縮小、重組的功能，舉例如下：

(1) 封閉（停止）故障發生部位相關交易

(2) 將故障部位離線維修

在不影響連線處理作業的情況下，進行維修系統的作業。

(3) 以獲得正常架構運轉效果為目標的系統重組

故障修復後，隨時能重組系統，並回復為原來的系統架構。

2、組成要項，包含硬體設備及軟體系統，其中硬體設備之要項，如下列所示：

(1) 多重處理機系統之中央處理機。

(2) 主記憶體設備。

(3) 輸出入通道設備。

(4) 檔案設備。

(5) 通訊控制設備。

(6) 通訊線路、端末系統設備。

3、此外，縮小功能、重組系統的操作程序，應予定型化，儘量減少操作人員的介入。

故障之早期發現・早期復原
故障之早期復原

適用性分類				
共通	中心	總行	合作	直接
◎				

技 23	具有限制交易的功能。
------	------------

為使檔案故障或軟體錯誤所造成的影響降至最低，應視情況，備有以檔案別或以科目別之交易限制功能。
--

- 1、交易限制功能，是指為限制故障所造成的影響，視故障狀況，將部分交易從運轉中的系統予以隔離。
- 2、實際上可以限制交易的項目，舉例如下：
 - (1) 業務。
 - (2) 科目。
 - (3) 提供之服務、商品。
 - (4) 運轉中程式的控制單元。
 - (5) 營業單位或營業地區。
 - (6) 端末設備。
 - (7) 交易對象、交易帳戶。

故障之早期發現、早期復原
故障之早期復原

適用性分類				
共通	中心	總行	合作	直接
◎				

技 24	具有系統復原的功能。
------	------------

在發生故障時，為迅速回復系統，繼續執行業務處理，應建置系統復原的功能。

- 1、故障發生時，為縮短對業務的影響時間、減少對業務的障礙，系統應具有故障復原功能。
- 2、包含多部伺服器之分散處理系統等，應訂定不影響各電腦間的系統運作與整合之復原作業程序。
- 3、系統復原功能，舉例如下：
 - (1) 復原用日誌紀錄（Journal）功能
為有助於各類系統復原作業，詳細記錄資料處理過程。
 - (2) 設置檢核點（Check Point）
為迅速執行復原作業，應將存放在主記憶體之重要計數器或端末系統狀態表格等內容，每隔一定時間或每隔一定交易量，轉存於外部記憶體設備或儲存媒體上。
 - (3) 局部復原功能（Partial Recovery）
當程式（Program）或作業（Task）異常終止時，可根據日誌紀錄資料進行復原，而不致影響其他程式或交易之運轉（即不需中止系統之運轉）之功能。
 - (4) 整體系統復原（Down Recovery）功能
若發生整個系統故障中斷時，利用日誌紀錄資料，回復整個系統。
為達到這個目的，除需定義交易之完成基準外，重新開機時並須能確實判斷掌握最後完成的交易。

(5) 檔案復原功能

檔案發生故障時，利用前次的備份檔案及日誌紀錄等資料將檔案復原。為迅速完成檔案之復原作業，根據裝置的特性，以磁碟（Disk Unit）或是磁柱（Disk Cylinder）為單位，將復原範圍縮減至最小。

4、對於 24 小時連線作業的系統，應以不影響連線服務為原則，於連線系統營運中，取得復原所需之備份資料，這種連線取得備份資料的功能，舉例如下：

- (1) 檔案復原作業通常以原始帳務之備份檔案為起點，利用日誌紀錄資料進行復原，因此應有原始帳務之備份檔案，此備份檔案需在連線系統運轉中取得。
- (2) 在程式修改後，因程式內容的問題所引發之故障，應能在不中斷系統作業之下，完成程式修改作業。

分散處理系統之程式修改方法，有連線作業下之維護或在連線作業下之遠端維護。

一、提升系統可靠性的對策

(五)災變對策

為預防因資訊中心發生災變，致使資訊系統完全無法運作，同時為分散風險，應設置異地備援中心。

災變對策
備援中心

適用性分類				
共通	中心	總行	合作	直接
	○			

技 25	具備災變備援中心。
------	-----------

為預防資訊中心本身因災變等的發生，造成系統功能完全喪失，應備有災變備援中心。

1、為預防資訊中心本身因災變發生，造成系統功能完全喪失的情況，同時為分散系統風險，應設置異地備援中心，其型態舉例如下：

由於災變備援中心之設置需要資訊系統相關設備的大量投資，對於發生故障時的替代方法，有必要事先充分研究檢討。

(1) 自備備援中心

個別金融機構各自獨立設置之專用備援中心。

(2) 共同利用之備援中心

多家金融機構共同設置備援中心。

(3) 相互備援中心

利用同一金融機構（金融集團）不同地區的事業部門，在發生災變時相互備援。

提供備援設施的部門，在發生災變時，可能需要停止某些不太重要的業務處理；或可利用與其他金融機構或企業合作相互備援。

(4) 代理備援中心

委託第三者辦理備援作業，必要時能隨時使用。

2、若災變備援中心委外辦理時，為避免多家委託企業可能同時發生緊急狀況，都需使用備援中心設施的情況發生，應事先確認委辦備援中心之優先順序安排、最低的保證範圍等服務，同時配合業務處理量的變更，定期檢討調整備援作業的方式。

- 3、備援中心與正式的資訊中心不可有同一風險因素（如火災、地震、停電等）存在，同時應考慮發生災害時，必要人員移動所需時間等因素，作一綜合性的分析判斷，再進行備援機制的規劃。

二、安全性侵害之對策

(一)資料保護

機密資料或重要資料之外洩、破壞、篡改等，以及存取這些資料所需的密碼外洩時，均會對企業造成重大影響，因此，應重視對這些資料的保護對策。

1、防止洩漏

資料依其重要性，在儲存、傳送的作業上，應有適當防止洩漏的對策。

資料保護
防止洩漏

適用性分類				
共通	中心	總行	合作	直接
◎				

技 26	具備密碼隱密性之維護措施。
------	---------------

為防止密碼洩漏，應採取不顯示、不印錄等措施。

- 1、為避免由端末設備洩漏密碼，應採取不顯示、不印錄等措施。同時，儲存在媒體上的密碼應不可直接錄製。
- 2、密碼的安全對策，舉例如下：
 - (1) 密碼不得使用 Null 或位數很短的文數字。
 - (2) 設定密碼之使用期限，在有效期將屆時，應有要求變更的機制。
 - (3) 密碼變更應有不接受前次或之前幾次所使用密碼的機制。
 - (4) 避免使用容易猜測的密碼（如生日、自己公司的名稱）。
 - (5) 僅限使用動態（每次必須變更）密碼管理機制。
 - (6) 使用者在第一次簽入（Log-on）系統時，應有強制變更初始密碼之機制。
- 3、有關避免密碼外洩的管理對策，請參照【運 17】之說明。

資料保護
防止洩漏

適用性分類				
共通	中心	總行	合作	直接
<input type="radio"/>				

技 27	應具有識別、確認對方端末設備的功能。
------	--------------------

經由開放網路，為防止錯誤的情況發生，對可自動接收訊息的端末設備輸出/入資料時，應依設備功能設置確認對方端末設備身分之機制。

- 1、金融機構利用開放網路對客戶發送匯款入帳通知等金融訊息時，若係經由客戶的電傳或傳真等具自動收信功能的端末設備時，因無法依賴密碼等方式確認客戶身分，因此有可能因電話號碼登錄錯誤或撥號錯誤等，造成訊息誤傳。
- 2、如端末設備具有可確認對方端末設備之功能，應加設確認對方端末設備身分的功能，舉例如下：
 - (1) 利用電話之發話者資訊通知服務之功能。
 - (2) 利用傳真機端末之識別 ID。
 - (3) 利用電傳端末之回撥（Answer Back）功能。
- 3、利用開放網路對個人電腦或主機系統傳送各種資金調動或金融資訊訊息時，在連線時，應執行身分確認功能，先確認端末之識別 ID 或發信者身分。請參照【技 35】之說明。

資料保護
防止洩漏

適用性分類				
共通	中心	總行	合作	直接
○				

技 28	具有防止儲存資料外洩的功能。
------	----------------

為防止檔案遭複製或竊取等資料外洩，應對重要資料採用亂碼化處理。

- 1、檔案遭非法複製或竊取時，為使資料內容無法讀取或瞭解意義，對重要的資料應予以亂碼化處理。尤其對於利用電子交易所儲存的各類資料，應經由亂碼化處理。
- 2、亂碼化處理應選擇適當可靠的亂碼技術。惟亂碼技術的強度會隨資料處理技術的發展而改變，因此使用亂碼技術時，最好利用多種亂碼技術的組合。
- 3、IC 卡具有防止資料外洩的耐破壞（Tamper Resistant）強化特性，其他儲存媒體可採型資料亂碼化之類的防止外洩對策。儲存媒體的資料亂碼化程度如下列所示：
 - （1）將檔案中重要項目資料予以亂碼化
例：密碼及電子有價資訊等。
 - （2）對重要檔案所有項目資料予以亂碼化
例：密碼檔案、個人資料檔案及電子有價資訊檔案等。
- 4、為預防行外端末設備遭竊或遺失，若需在行外端末系統內儲存重要資訊時，應經過亂碼化處理。

資料保護
防止洩漏

適用性分類				
共通	中心	總行	合作	直接
○				

技 29	具有防止資料在傳輸中外洩的功能。
------	------------------

為防止資料在傳輸中被竊聽而外洩，對於重要的資料，應有資料亂碼化的措施。

- 1、為保護資料即使在傳輸中被竊聽，亦無法瞭解其內容意義，重要的資料應經由亂碼化處理。若需利用公眾網路或無線網路等傳輸資料時，應與通訊業者協力合作並將資料亂碼化，充分作好防止外洩的措施。對於開發時的文件、程式原始碼等，依其重要性考慮傳輸方法。
- 2、使用亂碼功能時，應選擇可靠且適當的亂碼技術。亂碼技術的強度會隨著資訊處理技術的進步而改變，因此在使用亂碼技術時，最好能應用多種亂碼技術，以適當的組合方式處理。
- 3、資料傳輸使用亂碼技術的實例，如下所示：
 - (1) 資料亂碼化程度及對象範圍
 - a. 傳輸資料部分亂碼化（例如：密碼、帳號、電子格式的有價資訊等）。
 - b. 傳輸資料全部亂碼化。
 - (2) 在傳輸線路上資料之亂碼化程度
 - a. 在傳輸之線路上亂碼化（例如：在傳輸線路的兩端，裝設亂碼、解碼用的裝置）。
 - b. 端末設備間之亂碼（例如：利用端末設備的亂碼化軟體，將端末設備間的傳輸資料加以亂碼化）。
 - (3) 組合(1)與(2)的亂碼化方式

例如：將密碼、帳號、電子格式等重要資料碼後，再利用亂碼技術或設備將資料再亂碼。

二、安全性侵害之對策

(一)資料保護

2、防止破壞、篡改

為防止因程式非法存取，造成資料被破壞、篡改，應有適當的防範對策。

資料保護
防止破壞、篡改

適用性分類				
共通	中心	總行	合作	直接
◎				

技 30	檔案存取應具有排他控制（Exclusive Control）的功能。
------	------------------------------------

為防止檔案內容產生矛盾，檔案存取應具有排他控制（Exclusive Control）的功能。
--

1、若同一檔案，由多個程式同時要求更新資料，資料內容容易造成衝突矛盾，造成檔案破壞。為防止這種情況，檔案存取應設置排他控制（Exclusive Control）功能。

2、同一系統下，多個程式共用同一檔案的情況

對同一檔案，可能會發生同時存取的情況，因此應具有排他控制的機制，也就是當一個程式在存取某一個檔案時，其他程式若同時需要存取同一檔案，則應等待原已存取檔案之程式結束存取動作，並釋放對該檔案的控制權時，其他程式才能存取。

對於檔案之排他存取控制的程度，舉例如下：

- (1) 以檔案為單位。
- (2) 以段（Block）為單位。
- (3) 以紀錄（Record）為單位。

3、多個系統間共用同一檔案的情況

在多個系統間共用同一檔案時，各系統應有能對該檔案啟動排他控制的對策。其實例如下：

- (1) 在各系統之間傳送、確認排他控制用資訊（檔案鎖定資訊）。
- (2) 利用檔案控制裝置的排他控制功能。

4、因鎖死（Dead Lock）引起等待（Wait）狀態的迴避對策

若對檔案加入排他控制功能時，就有可能會發生鎖死的情況。因此，應有迴避因鎖死引起等待（Wait）狀態的對策。其具體的實例，如下列所示：

(1) 鎖死狀態的檢測及解除。

檢查發現發生鎖死狀況時，先將引起鎖死的交易設為無效，以解除鎖死的狀態，再重新處理該交易。

(2) 訂定檔案存取順序之規則。

資料保護
防止破壞、篡改

適用性分類				
共通	中心	總行	合作	直接
◎				

技 31	檔案應設置存取控制（Access Control）的功能。
------	-------------------------------

為保護資料不被非法存取，對於使用者、程式與檔案等，應設有檢核存取權限的功能。
--

- 1、為預防因故意或疏失引起的檔案破壞或非法存取，對於重要的檔案，應設置檔案存取權限控管的功能。
- 2、檔案存取權限控管的方法，一般來說有下列數種方式：
 - (1) 利用 OS 內含的存取權限控管功能。
 - (2) 利用 DBMS 內含的存取權限控管功能。
 - (3) 利用控管存取權限專用軟體的方法。
- 3、為控制檔案存取的權限，在網路上加設存取控管亦是一種有效的方法。
利用網路設備、IP Address 或 Port Number 之過濾功能是網路上加設存取控管的實例。
- 4、存取控管具體實例如下：
 - (1) 程式對檔案之存取權限的檢核
賦予程式對檔案的存取權限（唯讀、更新等權限）並予以檢核，以保護檔案。
 - (2) 使用者（包含端末系統）對檔案之存取權限的檢核
賦予使用者對檔案的存取範圍及存取權限（唯讀、更新等權限），並予以檢核，以保護檔案。
 - (3) 使用者（包含端末系統）對程式之存取權限的檢核
賦予使用者對程式的存取範圍，並予以檢核，以間接保護檔案。

資料保護
防止破壞、篡改

適用性分類				
共通	中心	總行	合作	直接
◎				

技 32	加強對不當資料之檢查功能。
------	---------------

為防止不當資料混入系統，應加強對不當資料之檢查及剔除的功能。

1、偵測因故意或疏失所造成不當資料的對策，舉例如下：

(1) 輸入資料的檢核

篩檢輸入資料在邏輯上或格式上的不完整性之功能，舉例如下：

a. 格式的檢查

檢查資料各欄位是否符合其設定的性質：數字形式或文字形式、必要的欄位是否均已輸入資料。

b. 範圍的檢核

檢核各資料欄位的內容，是否符合各項目所指定的邏輯範圍。

c. 利用檢查碼（Check Digit）檢核

利用客戶代碼等附加的驗證數字，在輸入資料時，以預設檢核邏輯的計算結果相互勾核。

d. 妥當性檢核

從資料項目的組合及關聯性，檢核是否有不應出現的資料，或在邏輯上互相矛盾的資料存在。

e. 序號檢查

檢查附加的處理序號是否符合編排順序。

f. 與主檔之勾核

檢核輸入資料各欄位的內容是否與主檔內相關欄位的內容相符。

（註）這種檢核，只是針對資料邏輯、格式條件的檢查為主，對於資料內容在本質上的錯誤，仍有無法檢知的可能性，因此資料輸入前的檢驗與管理應用面等對策之並行是非常重要的。

(2) 保留稽核軌跡

對於在邏輯、格式條件的檢查上無法判別的不當資料之處理過程，應保留稽核軌跡，以供事後追查，這個功能對於連線的業務處理特別重要。一般而言，在日誌紀錄資料中，加入資料復原所需的資料處理日期時間、使用之端末機器、資料輸入者的識別碼等重要資料。同時，對於儲存這些處理過程的稽核軌跡，應有存取保護的機制。

有關保留稽核軌跡的存取保護機制，請參照【技 37】之說明。

二、安全性侵害之對策

(一)資料保護

3、檢測對策

為早期發現資料之非法破壞或篡改，應有適當的檢測對策。

資料保護
檢測對策

適用性分類				
共通	中心	總行	合作	直接
○				

技 33	具備偵測資料傳輸中被篡改的檢測對策。
------	--------------------

在傳輸重要的資料時，為偵測檢知是否被篡改，應有適當的方法與對策。

- 1、在傳送重要資料時，為檢測資料是否被篡改，應備有適當的方法與對策。
特別是經由開放式網路傳輸資料時，應具有檢測資料在傳送中是否被篡改的適當對策。
- 2、利用資料亂碼技術的認證功能，偵測資料是否遭篡改的功能，舉例如下：
 - (1) 訊息認證碼。
 - (2) 電子簽章。

資料保護
檢測對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 34	具備檔案相互勾核的功能。
------	--------------

為早期發現因故意或疏失而造成檔案間資料內容不一致，對於帳務主檔、交易日誌資料檔案、彙總清算檔案等，應有適當的檔案間相互勾核的機制。

- 1、為早期發現因故意或疏失造成的檔案間資料內容不一致或處理邏輯的錯誤，對於帳務主檔、交易日誌資料檔案、彙總清算檔案等，應事先建置檔案間內容的相互勾核驗證之功能。
- 2、檔案間內容不一致的原因，舉例如下：
 - (1) 資料遭篡改。
 - (2) 程式錯誤。
 - (3) 系統發生故障，復原作業不完整。
- 3、檔案間內容相互勾核、驗證的方法，例如合計數的檢核方法。
合計數檢核是利用帳務主檔及彙總清算檔案，分別統計其合計數，再相互勾核。若能再以帳務主檔及交易日誌資料檔案作進一步的勾核，則對提升檔案間的完整精確更有幫助。
- 4、採取分散處理的系統，因檔案係分散儲存，對於檔案間完整性的檢核，更需特別注意實施。

二、安全性侵害之對策

(二) 防止非法使用

由於網路範圍的擴大，由各種端末設備存取系統的可能性增加，由無使用權限的使用者造成的非法存取、資料及軟體程式遭篡改等可能性大增。因此，應有確認系統使用權限、限制系統利用範圍等功能對策。對於防止非法存取系統的對策，各金融機構應配合所使用的主機系統、端末設備、用途等，將非法存取系統的方式加以分類，擬定應檢核的項目。

3、預防對策

為防止對資訊系統的非法使用，如何確認本人身分、端末設備、媒體正當性、存取權限等，是非常重要的。若對存取權限的檢核確認作業實施不完整時，會增加系統遭非法存取的危險性。因此應充分講究系統存取權限及使用範圍的確認作業。

另外，為防止利用卡片的犯罪行為，提供安全的卡片交易服務，應有防止利用偽造卡片的措施。同時，對於電子式有價資料或密碼等資料之保護或偽造、篡改之防範與偵測，亦需有確實的對策。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 35	具備確認使用者身分的功能。
------	---------------

為防止非法使用，配合業務內容及連接方法等，應確認連接對象的使用者身分以及是否為正當的端末設備。

- 1、因為網路應用的擴增，各種不特定的端末設備及人員非法存取系統的可能性增加。為預防這些非法行為，應嚴格確認連接對象之人員及設備是否經正當授權。
- 2、經由網際網路進行電子式交易行為時，應特別注意偽裝他人的可能性，應嚴密確認通訊對方是否為擁有正當使用權限的使用者。
- 3、使用者身分確認的方法，舉例如下：
 - (1) 廣義的通行碼
 - a. 密碼 (Password)。
 - b. 使用者代號與密碼 (ID、Password)。
 - c. 動態密碼 (One Time Password)。
 - d. 詢問與回應 (Challenge、Response) 方式等。
 - (2) 亂碼技術
 - a. 對稱式金鑰。
 - b. 公開金鑰。
 - c. 電子簽章。
 - d. 使用憑證機關發行的電子憑證等。
 - (3) 生物科技 (利用個人身體的特徵作為識別的資訊，以確認本人的技術)
 - a. 指紋。
 - b. 聲紋。
 - c. 掌紋。

d. 眼底視網模紋路。

e. 虹膜。

f. 筆跡等。

(4) 所有物

a. 磁卡（金融卡、櫃員卡、主管卡等）。

b. I C 卡。

c. 存取符紀（Access Token）等。

(5) 以上方法並用。

4、確認端末的方式，舉例如下：

(1) 端末 ID 的確認。

(2) 電話號碼的確認。

(3) 回撥。

(4) 利用認證機構發行的憑證，由連接端伺服器檢核。

5、對確認使用者身分所使用技法的管理營運方法，請參照

【技 26、運 16、運 17、運 18、運 39、運 51】之說明。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 36	具備防止非法使用 ID 的功能。
------	------------------

為防止非法存取系統及資料，應具備防止非法使用ID的功能。

1、為預防系統及資料被非法存取及使用，應設置防止非法使用的功能。

2、具體的方法，舉例如下：

(1) 簽入系統作業的逾時 (Time-out) 控制

在簽入系統之後，經過一段時間未有任何操作動作時，由系統強制自動簽出。

(2) 未使用之 ID，應強制刪除

經過一段時間，一直未使用系統之 ID，應予以強制刪除。

(3) 向使用者提供簽入系統的歷史資料

當使用者簽入系統時，應由系統提供使用者下列資訊

a. 前次使用系統的日期、時間及狀態。

b. 自前次簽入系統後，若連續多次簽入失敗時，顯示其存取的狀態。

(4) 密碼輸入失敗的次數限制

密碼輸入失敗的次數超過一定次數之後，該 ID 應設定為暫停使用。

(5) 應具有防止他人知道密碼的對策

有關防止他人知道密碼的對策，請參照【技 26】之說明。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 37	管理系統的歷史資料。
------	------------

為管理系統的狀況，對於使用系統或存取資料的歷史記錄應保管一段期間，以作為監查追蹤的依據。

1、系統的歷史資料應保存一段時間以作為稽查追蹤的依據。同時，應定期分析使用歷史資料，以調查是否有非法使用系統的情形，這種分析調查的作業，應公告週知，以防止並牽制有心人士非法使用系統。

使用系統歷史資料，具體的內容，舉例如下

- (1) 簽入、簽出的狀態（使用的端末、時間、ID、通訊線路種類、使用的系統或資料以及執行的處理等）。
- (2) 非法的存取要求（使用端末、時間、ID）。
- (3) 使用系統認為已失效的 ID。
- (4) 對系統簽入後，一段時間未操作，而被強制簽出的 ID 等，有關非法使用之對策請參照以下的基準項目。
- (5) 設定確認本人身分的功能。請參照【技 35】之說明。
- (6) 應具有防止密碼被他人知道的對策。請參照【技 26】之說明。

2、根據稽查追蹤資料，分析未經授權使用系統情況，並提出報告。

3、為防止稽核軌跡、操作紀錄、系統營運紀錄等被篡改或非法存取，除擁有正當存取權限之使用者外，應有適當的保護功能。

具體的對策，舉例如下：

- (1) 利用亂碼化技術保護。
- (2) 儲存於無法覆寫的媒體上，並保管於受保護的場所。
- (3) 為防止經由網路的非法存取或篡改，應儲存於離線的媒體上。

4、為利於日後查閱使用歷史資料，各系統的時鐘應以標準時間為基準，所有系統時鐘應取得同步。

在分散系統之間，時間同步可以利用 NTP (Network Time Protocol) 的方法。

5、為防止他人非法使用網際網路的交易，以保護真正的使用者，系統應具備由使用者親自確認使用狀態（前次簽入日期、時間、交易歷史資料等）的功能。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 38	設置限制端末設備、作業與交易範圍的功能。
------	----------------------

為防止非法使用系統，對於端末交易，應依照使用的設備、媒體的種類、設置場所及用途等，設置限制交易內容的功能機制。

- 1、若存取系統的權限無法確實確認，或認為非法存取系統的危險性高時，對使用端末機器的交易，應具備能隨時依所使用的設備、媒體的種類、設置場所、用途等，對交易或業務內容加以設限的功能。同時，在設定對交易或業務內容的限制時，應仔細研究交易或業務內容的特徵，以保護客戶的觀點來訂定。
- 2、對對交易或業務內容設限的重要因素，舉例如下：
 - (1) 依照端末設備種類的業務限制
 - a. 開發用端末機。
 - b. 櫃台端末機。
 - c. ATM。
 - d. 行外端末機。
 - e. 提供行員使用之行動裝置。
 - (2) 依照端末設備設置場所的業務限制：
 - a. ATM。
 - b. 行外可攜式端末機。
 - c. 客戶、企業之端末機。
- 3、交易限制的內容，舉例如下：
 - (1) 交易金額的限制。
 - (2) 電子式儲值之可儲存金額限制。

- (3) 服務內容僅限定查詢業務。
- (4) 資金移轉交易，限定可以轉入的對象。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 39	設置在發生事故時能停止交易的功能。
------	-------------------

為因應發生遺失金融卡、存摺、印鑑等事故的處置，應有對該帳戶之對應媒體設定停止交易的功能。同時，行外之可攜式端末設備遭竊、遺失等事故發生時，亦應有對該端末設備停止交易的功能。

停止交易的具體實例，如下列所示：

在金融卡、存摺、印鑑等對應該帳戶之主檔上，或可攜式端末設備的端末 ID 主檔上，登錄事故內容、應注意的代碼或停止付款的記號，以因應遭竊、遺失等事故。請參照【運 41】之說明。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
	○	○	○	

技 40	具有防止卡片被偽造的對策。
------	---------------

為防止非法使用，應具有防止卡片被偽造的對策。

- 1、為防止卡片的犯罪行為，提供安全的卡片服務，應有防止卡片被偽造的對策。
- 2、防止卡片偽造的對策，舉例如下：
 - (1) 判別偽卡用的代碼，記錄在卡片的磁條上面。
 - (2) 客戶照片或親簽文件之版面印刷。
 - (3) 採用 I C 卡等高安全性的技術。
 - (4) 對卡片設定有效期限，或更新卡片資料等，應用等高安全性的技術。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
○				

技 41	對於電子儲值應有檢測非法行為的保護功能機制。
------	------------------------

為因應電子儲值的複製、重複使用等非法行為，系統應建置保護資料，檢測非法行為的功能機制。

- 1、電子儲值機器、媒體與所包含之軟體，應具備保護儲值資料的功能。
- 2、若未能設置上述功能時，應具有檢測防止電子儲值資料遭篡改、非法複製、重複使用的功能。
- 3、為確保安全性，應應用下列的方法，並以組合方式，建置整合性的因應方法。

同時，應隨時注意安控技術的最新動向，適切的評估其穩定性、互換性、安裝的容易性等，以決定是否採用這類的安控技術。

- (1) I C卡型電子錢包之耐破壞性 (Tamper Resistant) 之保護功能。
- (2) 設定 I C卡有效期限以抑制偽造。
- (3) 利用交易序號檢核非法交易。
- (4) 由驗證中心檢測。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
○				

技 42	以電子式儲存基碼值之機器、媒體或軟體，應具有保護基碼值功能。
------	--------------------------------

為防止基碼值外洩而引起非法行為，機器設備、媒體與使用之軟體系統應設置保護機碼值的功能。

1、儲存電子化之公開金鑰、私密金鑰之 I C 卡等機器設備、媒體與相關之軟體，應具有保護公開金鑰、私密金鑰的功能。

若利用個人電腦，公開金鑰與私密金鑰應分別以不同機器設備或媒體保存，在有需要時才將兩者連結使用。

2、將公開金鑰、私密金鑰儲存於個人電腦系統時，應具備他人無法解讀的預防措施。

3、為確保安全性，應應用下列的手法，並以組合方式，建置整合性的因應方法。

同時，應隨時注意安控技術的最新動向，適切的評估其穩定性、互換性、安裝的容易性等，以決定是否採用這類的安控技術。

(1) I C 卡之耐破壞性 (Tamper Resistant) 之保護功能。

(2) 利用 ID、密碼等之存取限制。

(3) 亂碼化處理後再儲存。

防止非法使用
預防對策

適用性分類				
共通	中心	總行	合作	直接
○				

技42-1	對於電子郵件的收發、首頁的瀏覽等，應具有防止非法使用功能。
-------	-------------------------------

對於業務需要以外之電子郵件的收發、首頁的瀏覽等，應具有防止非法使用的對策。

- 1、為能因應除業務需要以外之電子郵件的收發、首頁的瀏覽等，應具有與安控政策整合之防止非法使用的對策。
- 2、業務需要以外之電子郵件的收發、首頁的瀏覽等，有下列所示的類型：
 - (1) 電子郵件的收發
 - a. 與業務無關的私人資訊交換或連絡。
 - b. 超出業務適當範圍外的電子郵件，例如：不正當的郵件清單 (Mailing List) 或郵件雜誌 (Mail Magazine) 等。
 - c. 發送違反公共善良風俗的郵件。
 - (2) 首頁的瀏覽
 - a. 瀏覽與業務無關的首頁。
 - b. 在首頁上刊載超出業務適當範圍的信息（例如：公佈欄刊載違反公共善良風俗的信息等）。
- 3、對於業務需要以外之電子郵件收發、首頁瀏覽等之預防對策，舉例如下：
 - (1) 對於可能收發電子郵件或瀏覽首頁的人員應設定適當的範圍。請參照【運 16】之說明。
 - (2) 安裝電子郵件過濾軟體 (Mail Filtering)，利用判斷郵件內容的功能，防止不當郵件收發。針對收發不當電子郵件的人員，應予以適當的處置。
 - (3) 對發送至機構外部的電子郵件，自動轉送該員的主管。
 - (4) 安裝內容過濾軟體 (Contents Filtering)，利用判斷首頁內容的功

能，防止不當之首頁瀏覽。針對瀏覽不當首頁的人員，應予以適當的處置。

- 4、在運用面來說，應對全體員工實施資訊安全之教育訓練，詳細說明責任、義務及懲罰規定，已徹底瞭解安控相關規定。請參照【運 80】之說明。

二、安全性侵害之對策

(二) 防止非法使用

2、限制外部網路存取

資訊系統連接到開放式網路等外部網路時，為防止經由網路之非法入侵及非法使用資訊系統，應限制外部的存取動作。

防止非法使用
限制外部網路存取

適用性分類				
共通	中心	總行	合作	直接
◎				

技 43	具有防止外部網路非法入侵的功能。
------	------------------

為防止非法入侵，處理重要資料及執行程式的系統在與外部網路（開放式網路、遠端存取等）連接的部分，應具有的防止非法入侵的適當對策。

- 1、在此處所謂之外部網路，是指可能有不特定多數人存取之網路，主要有網際網路、公眾通訊網路等。利用數據專線，連接特定對方的網路，則不列入本項的對象。但是，對於只有中途部分使用數據專線，末端仍為不特定多數人連接的網路（例如與網際網路服務提供者，以數據專線連接的情況），仍應視為本項目之對象。
- 2、外部網路之連接對企業內部系統具有非法入侵的危險性。因此，執行程式處理重要資料的系統與外部網路連接時，應具有防止非法入侵的適當對策。
- 3、為防止外部網路非法入侵內部系統，並及早發現，應監視系統存取的狀況，檢核存取系統之歷史資料，並對伺服器實施安全漏洞相關的因應對策。請參照【技 37、技 45、運 56】之說明。

4、防止非法入侵的對策，舉例如下：

(1) 防火牆 (Firewall)

與網際網路連接時，應設置防火牆系統，以防範經由網際網路入侵企業內部的網路。

(2) 存取伺服器 (Access Server)

在撥接線路之遠端存取連接口，應設置存取伺服器設備。並利用回撥、存取權限認證等，確保其安全性。

(3) 非戰區 (DMZ : De-Militarized Zone)

在以防火牆設置的特別區域內，建置公開伺服器（向外部公開網頁的伺服器），以防止入侵企業內部網路。設置非戰區的目的是將內部網路隱藏起來，由外部無法看到內部網路，同時可以設定詳細的存取權

限。非戰區請參照圖 1 之實例。

(4) 其他

為早期檢測對提供服務者之阻斷服務攻擊 (Dos 攻擊：Denial of Service)，對網站之存取要求交易數量或客戶之正當性，應嚴加監視。

- 5、防火牆及存取伺服器等設備，應設置於資訊系統機房內，或與設置重要伺服器系統機房具同等基準的場所。
- 6、防火牆及存取伺服器等設備，應經由適當的評估，確認在安全性上的效果，並依據其結果，實施系統之維護作業。
- 7、連接外部與不連接外部網路之網路，其網路架構作應作物理上之分隔。
- 8、確認本人身分等系統存取權限確認功能與本項併用，可強化機能。請參照【技 35】之說明。
- 9、與網際網路連接之安控技術，應隨時注意最新技術的動向，適切的評估其穩定性、互換性、安裝的容易性等，以決定是否採用這類的安控技術。

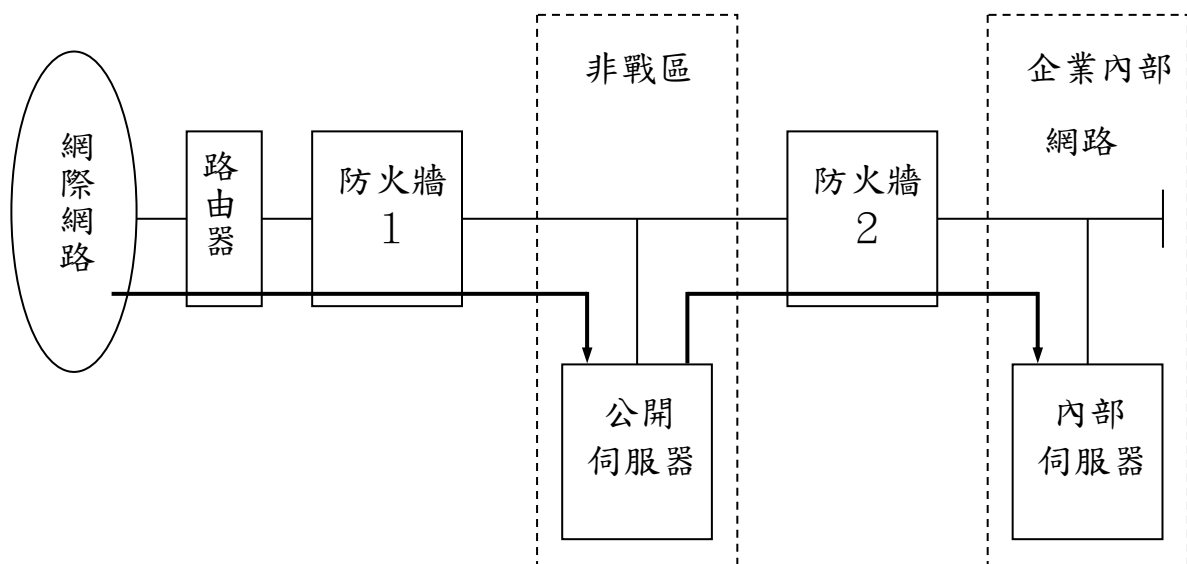


圖 1 非戰區的構成實例

防止非法使用
限制外部網路存取

適用性分類				
共通	中心	總行	合作	直接
◎				

技 44	由外部網路可以存取的機器設備應維持在最少的數量。
------	--------------------------

為防止非法入侵資訊系統，由外部網路可以存取的通訊路徑與通訊相關機器等應維持在最少的數量，不必要的機器設備不可連上網路。

1、為防止非法存取，由外部網路存取的路徑，應侷限於必要的最小量。如此才能限制入侵的路徑，並加以嚴密的管理與監視。

存取路徑維持在必要之最小量，舉例如下：

(1) 長期未使用的機器設備（電腦、數據機等），應由網路上切離
為防止非法使用，預防系統發生故障，應由網路上實體（物理上）切離，或關閉設備之電源。

(2) 未使用的通訊埠應封閉
未使用的通訊埠容易受到外部非法使用的威脅，因此應封閉。

2、連接外部網路的資訊系統，其安裝設定應考慮系統的安全性。

考慮系統安全性的設定，舉例如下：

(1) 選擇基本軟體所提供的功能
將基本軟體的安全漏洞維持在最小量，若基本軟體所提供之功能（如 Telnet、ftp、finger 等）有未使用的，應將其設定為停用或限制其使用。

(2) 限制安裝載入軟體
一般軟體都有發現安全漏洞的可能，連接於外部網路的電腦系統，非預先設定要使用的軟體，不應安裝載入於系統中。

二、安全性侵害之對策

(二) 防止非法使用

3、偵測對策

為早期發現非法存取，應設置可以監視非法存取及異常交易的功能。同時，為防止非法交易的發生，應有能偵測非法交易的功能。

防止非法使用
偵測對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 45	設置監視非法存取的功能。
------	--------------

為早期發現非法存取，應設置監視存取失敗或非法存取的功能。

1、監視存取失敗的功能，舉例說明設置的方法：

- (1) 設置記錄存取失敗明細資料之功能。
- (2) 對於連續數次的存取失敗，應設置能強制結束、停止交易等之功能。

2、監視非法存取的功能，舉例如下：

- (1) 利用個人電腦、按鍵式電話或端末機，辦理資金撥轉、餘額查詢等交易，所輸入密碼錯誤次數超過規定次數時，應立即自動禁止該交易之進行。
- (2) 對於利用 ATM 或金融卡端末設備進行資金撥轉、餘額查詢等交易所輸入密碼錯誤次數超過規定次數時，應立即停止往後磁卡交易之進行。
- (3) 安裝由行外端末執行遠端診斷用系統時，如非必要使用，應禁止連結。若需要執行遠端診斷時，亦應設定需要連結的時段，並檢查分析是否有非法存取資料的情形。系統存取的歷史資料應加以保存，供日後追查之用。
- (4) 為讓使用者明確瞭解並確認是否有被他人非法使用，應提供前次進入系統的日期時間等資訊，供客戶確認。
- (5) 若偵測出非法存取的情況時，應能自動通知安控管理者或事先指定的管理人員。
- (6) 若利用網頁等提供資訊時，應利用入侵偵測系統，自動監視首頁是否被篡改。同時，可以活用電子簽章的功能，早期偵測資訊是否遭篡改。

防止非法使用
偵測對策

適用性分類				
共通	中心	總行	合作	直接
○				

技 46	設置偵測非法交易的功能。
------	--------------

為防止因非法交易造成的損害，應設置偵測非法交易的功能。

1、為防止因非法交易造成的洗錢行為（Money Laundering），及非法使用卡片造成損害，進而防止損害擴散，應設置能偵測非法交易的功能。

2、應偵測的非法交易，列舉如下：

（1）疑似洗錢行為（Money Laundering）的交易

短期間頻繁發生的交易行為，且以現金或支票存取的總金額相當大，應偵測並通知相關人員。

（2）卡片之非法交易

a. 在平時不曾使用過的場所使用卡片交易，或在一定的短時間內，使用卡片的交易次數激增等情況。

b. 由同一連鎖店，同一張卡片在短時間內，發生多筆同一金額的交易等情況。

防止非法使用
偵測對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 47	設置異常交易的監視功能。
------	--------------

為早期發現非法存取，應設置監視異常交易的功能。

- 1、事故登錄之解除、存摺或存單之再發行、通行密碼的查詢等之特殊交易，除應經過主管覆核外，應設有主管覆核交易紀錄之確認核可機制。
 - (1) 利用原始憑證（如傳票）。
 - (2) 連線查詢。
 - (3) 利用主管專用（特別指定）端末機。
 主管覆核的功能，主要是為確認使用端末機的操作者為具有主管權限的人員。
- 2、對於特定帳戶的交易，設置包含端末機編號之監視功能。當某特定帳戶發生交易時，應有能立即輸出顯示啟動交易的端末機編號等資訊的功能。
- 3、關於由客戶端末、企業端末、外部中心等送來的異常交易，應有交易管理機制。

二、安全性侵害之對策

(二)防止非法使用

4、因應對策

偵測到非法存取或非法使用時，應迅速調查可能受到損害的範圍，防止特定受損範圍的擴大，必要時需執行系統的復原作業。因此應事先備有因應策略。另外，應有受損狀況、原因等的調查分析與防止再次發生的措施。

防止非法使用
因應對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 48	應備有因應非法存取與復原的對策。
------	------------------

當偵測發現非法存取時，為防止非法存取擴大的因應對策略與系統復原作業程序應明確訂定。偵測到非法存取時，不論是否有蒙受損害，應有防止非法存取行為擴大的因應對策與復原對策，同時，在分析非法存取的原因後，應有防止再發生的對策。

1、應事先明確訂定防止非法存取擴大的因應對策與系統復原對策，並能達到下列目標。同時，因應對策應與相關人員協力進行。

(1) 防止非法存取的擴大

多數的非法存取行為，係先行侵入一個機器設備或路徑，再經由該機器或路徑，向其週邊逐漸擴大範圍。當偵測到非法存取時的對應方法，舉例如下：

- a. 緊急停用被入侵的系統。
- b. 立即切斷被入侵網路的連結路徑。

(2) 針對非法存取損害的復原作業

- a. 針對非法存取損害的復原作業，應事先明確訂定作業程序。舉例如下：

- (a)阻斷服務攻擊（Dos 攻擊）等，造成通訊網路無法營運。
- (b)伺服器等特殊存取權限（如 Root 權限）被竊取。
- (c)發現伺服器開始出現不正常的處理。
- (d)發現伺服器有被入侵的跡象。
- (e)伺服器無法通訊。
- (f)發現網頁之內容被篡改。

對於事先無法完成對應復原程序的事件情況，應召集相關人員共同檢討復原對策。

- b. 復原作業所需的資料、檔案及程式檔案應確保備份的完整，以因應檔案被破壞的情況。

復原的因應作業，舉例如下：

(a)復原被刪除或破壞的檔案。

(b)調閱被入侵的系統及對其週邊設備的存取歷史記錄，以確認週邊其他系統是否有被入侵。

(c)確認是否有非法程式潛伏在系統內。

系統復原作業時，為追究分析非法存取的原因所必要的資料，應確實收集保存。

2、防止非法存取的行為再次發生，應有下列之因應對策：

(1) 掌握入侵路徑、入侵時點、受損害的範圍等狀況。

(2) 追究原因，並加以分析。

(3) 針對追究的原因，應擬定防止再次發生的因應對策防止再發生的對策，舉例如下：

a. 強化系統存取權限管制。

b. 被非法盜用之 ID 或其相關周圍之 ID 等的密碼全部更換。

c. 若發現系統內部有安全漏洞存在時，應立即修補。

二、安全性侵害之對策

（三）防止非法程式

在講究資訊系統安全性之入侵對策時，防止非法程式侵入系統或安裝的對策也是非常重要的。

1、防禦對策

資訊系統遭到非法程式的侵入時，可能會造成機密資訊（密碼、重要檔案內容等）之外洩、或系統遭到破壞（如檔案之破壞、系統功能之破壞等）、甚至故意侵害系統的安全性等，因應這些事故，應有綜合性的考量，訂定整體性的因應策略。

防止非法程式
防禦對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 49	具有對電腦病毒等非法程式的防禦對策。
------	--------------------

為防止系統開發、維護、營運中遭受電腦病毒等非法程式的入侵、或非法存取而遭受損害，應有適當的防禦對策。

1、為保護系統不受非法程式之侵犯，應防止電腦病毒的入侵及非法存取篡改系統內的程式，因此應有預防上述事項的對策。

另外，為防止在系統中被安裝非法程式，在安裝程式（包含自行開發的程式、委外開發的程式、套裝軟體程式或下載的程式等）時，應事前確實測試檢核。

2、電腦病毒入侵、程式篡改或安裝不當程式的方法，舉例如下：

(1) 電腦病毒的入侵

- a. 利用電子郵件的附加檔案。
- b. 利用網際網路下載的程式。
- c. 由套裝軟體入侵。
- d. 利用磁片（Floppy Disk）等資料媒體入侵。

(2) 非法存取竄改或程式被篡改

- a. 利用特洛伊木馬竄改程式。
- b. 篡改系統，跳過系統存取權限之檢核功能。
- c. 系統測試用功能等越權使用，以篡改系統。
- d. 由系統運轉紀錄檔案竊取或篡改系統之 ID 及通行密碼。
- e. 利用作業系統等之安全漏洞，突破及篡改系統。
- f. 利用端末系統測試功能，安裝程式等。
- g. 利用系統示範或研習用 ID，安裝程式等。

(3) 非法程式之安裝

- a. 對交易處理程式，增加不當處理的功能。
- b. 篡改內建於端末設備內的程式。
- c. 利用篡改個人電腦等之系統啟始程式。

3、防禦對策策略，舉例如下：

(1) 電腦病毒的入侵

a. 安裝防毒軟體

防毒軟體除安裝於端末、伺服器系統之外，同時應安裝於連接外部網路與內部網路之閘道器(Gateway) 等，資料在流經這些設備時，均應確實檢驗。

為有效應用防毒軟體，應隨時更新最新的病毒碼，當然應建置能自動更新的系統環境架構。

b. 實施檔案管理

不安裝來路不明的軟體，對網路下載的檔案及電子郵件附加檔案，應經過防毒軟體的檢驗，對原始程式檔案，應加入防寫控制等因應對策。

(2) 利用非法存取，篡改程式

a. 實施存取控管

對檔案設定存取權限的控管機制。請參照【技 31】之說明。

設定確認使用者身分的機制。請參照【技 35】之說明。

設定防止非法使用 ID 的機制。請參照【技 36】之說明。

b. 防止非法入侵的機制

設定防止由外部網路非法入侵的機制。請參照【技 43】之說明。

c. 去除非法存取的要因

(a)防止 ID 密碼之洩漏

暗碼、行密碼等不被他人知悉的對策。請參照【技 26】之說明。

防止儲存的資料外洩的對策。請參照【技 28】之說明。

防止資料在傳送中外洩的對策。請參照【技 29】之說明。

(b)因應作業系統等之安全漏洞的對策

(3) 不當程式之安裝

在開發的各階段，應經過充分的檢測驗證，應防止被不當程式的混入。

- a. 應內建必要的安控機制。請參照【技 8】之說明。
- b. 在程式設計的階段，即確保軟體的品質。請參照【技 9】之說明。
- c. 在程式撰寫的階段，即確保軟體的品質。請參照【技 10】之說明。
- d. 在測試的階段，即確保軟體的品質。請參照【技 11】之說明。
- e. 對於建置套裝軟體時，應確保軟體的品質。請參照【技 13】之說明。

4、關於作業系統等之安全漏洞，應隨時掌握最新的資訊，準備隨時防堵安全漏洞。

二、安全性侵害之對策

(三) 防止非法程式

2、偵測對策

應能夠偵測電腦病毒或非法軟體的入侵，使用者或系統管理者能立即採取適當必要的措施。

防止非法程式
偵測對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 50	應設置偵測電腦病毒等非法軟體的功能。
------	--------------------

為確保並維持系統的可靠性，應設置能偵測檢查是否有被電腦病毒等非法軟體入侵或感染之對策。

1、應具備能配合技術的進步、服務環境的變化及系統擴充或變更等而隨時確認有效的防禦政策，以防止非法行為的入侵。

為確保並維持軟體的可靠性，應有非法程式之偵測對策，以及驗證系統正當性的對策。

對於非法程式等之偵測，不是一種技術或軟體能涵蓋的，應依據偵測對象之程式、機器的結構、使用的作業系統等，分別訂定適當的因應對策。在擬定個別的對策時，應廣為收集已被發現或公告的非法行為（入侵或附加安裝的手法等）實例，這些資訊應對擬定編製防禦對策、偵測對策有所幫助，因此，這些記載、文獻或指南是有參考價值的。

2、偵測的對策，舉例如下：

（1）利用防毒軟體之偵測

對於電腦病毒，可以利用防毒軟體偵測，此時應注意應使用最新的病毒碼來偵測。

（2）利用存取歷史資料偵測

監視系統運轉的狀態，或檢視分析系統運轉的歷史記錄等，若發現系統運轉有異常現象或對重要檔案的異常存取、密碼錯誤的內容、次數等，可以發現非法行為。

應實施系統存取歷史資料的管理。請參照【技 37】之說明。

（3）利用資源管理之偵測

由系統資源（檔案容量、記憶體容量、CPU 使用時間等）的使用狀況，檢核偵測是否異常或特殊情況傾向發生，以偵測發現不當程式的入侵

或組裝。

(4) 利用程式庫的管理偵測

- a. 管理檔案更新歷史資料，能夠偵測非法程式的更新或新增。
- b. 原始程式庫之檔案（利用個人電腦開發的程式或購入的程式的原始檔等）及使用中的程式檔作比較，以偵測是否有不當程式的入侵或安裝。
- c. 利用文件製作支援工具，觀察偵測是否有非法情形。

二、安全性侵害之對策

(三) 防止非法程式

3、復原對策

應準備電腦病毒受損系統之復原作業程序，同時應有防止再發生的因應對策。

防止非法程式
復原對策

適用性分類				
共通	中心	總行	合作	直接
◎				

技 51	具有被電腦病毒等非法程式感染受害時之因應對策。
------	-------------------------

被電腦病毒等不當程式感染時，為將受害的範圍縮至最小，應有由發現病毒感染到系統復原的因應對策。
--

- 1、在偵測到電腦病毒的感染或發作時，或發現非法軟體時，應備有因應對策。
對於發生狀況的系統或網路，應立即終止所有處理作業，應用事先訂定的作業程序（不可由使用者個人判斷）啟動系統復原作業。
- 2、發現電腦病毒的感染或發作時，因應的作業程序，舉例如下：
 - (1) 立即隔離受感染的系統（或是端末裝置、個人電腦等）。
 - (2) 向有關人員通報。
 - (3) 檢查其他有可能被感染的系統。
 - (4) 移除電腦病毒。
 - (5) 重新安裝程式（依作業需要）。
 - (6) 重新載入備份磁帶的檔案（依作業需要）。
 - (7) 再次檢查該系統有無電腦病毒。
 - (8) 實施防止再發生的措施。
 - (9) 系統（或是端末裝置、個人電腦等）之再連結。
- 3、發生其他非法程式損害情形時，除須依照上述的處理原則辦理外，尚應注意証據之保留。

金融機構資訊系統安全基準修正對照表

修 正 條 文	現 行 條 文	說 明
<p>壹、總則</p> <p>(貳) 基準之組成</p> <p>二、組成</p> <p>本基準的內容，由設備基準、營運基準、技術基準等三個部份組成其內容分別如下：</p> <p>(一)設備基準</p> <p>為保護安置資訊系統的建築物、設備等，不受天然災害、非法行為等之危害，在設備面應考慮的對策。</p> <p>(二)營運基準</p> <p>為提升資訊系統的可用性、完整性、機密性、<u>來源辨識性</u>、<u>不可重複性及不可否認性</u>，在</p>	<p>壹、總則</p> <p>(貳) 基準之組成</p> <p>二、組成</p> <p>本基準的內容，由設備基準、營運基準、技術基準等三個部份組成其內容分別如下：</p> <p>(一)設備基準</p> <p>為保護安置資訊系統的建築物、設備等，不受天然災害、非法行為等之危害，在設備面應考慮的對策。</p> <p>(二)營運基準</p> <p>為提升資訊系統的可用性、完整性及機密性，在開發、營運管理</p>	<p>參考「金融機構辦理電子銀行業務安全控管作業基準」交易面之安全需求，於營運基準及技術基準之組成增列來源辨識性、不可重複性及不可否認性等安全性原則。</p>

修 正 條 文	現 行 條 文	說 明
<p>開發、營運管理上之對策。</p> <p>(三)技術基準</p> <p>為提升資訊系統的可用性、完整性、機密性、<u>來源辨識性</u>、<u>不可重複性及不可否認性</u>，在系統硬體及軟體等技術面之對策。</p>	<p>上之對策。</p> <p>(三)技術基準</p> <p>為提升資訊系統的可用性、完整性及機密性，在系統硬體及軟體等技術面之對策。(P.2)</p>	
<p>(伍)基準之主要用語</p> <p>二、本基準內所使用之主要用語之定義及其範圍</p> <p>可攜式電腦設備……攜帶式端末、攜帶型個人電腦、<u>行動裝置設備</u>、可攜式端末等，主要由外務人員攜帶，在營業廳外使用之電腦設備。</p>	<p>(伍)基準之主要用語</p> <p>二、本基準內所使用之主要用語之定義及其範圍</p> <p>可攜式電腦設備……攜帶式端末、攜帶型個人電腦、<u>口袋型個人電腦</u>、可攜式端末等，主要由外務人員攜帶，在營業廳外使用之電腦設備。(P.5)</p>	<p>因應消費性電子產品之演進，將可攜式電腦設備範圍中之「口袋型個人電腦」調整為「行動裝置設備」。</p>
<p>貳、基準篇</p> <p><u>設備基準</u></p>	<p>貳、基準篇</p> <p><u>設備基準</u></p>	<p>文字增補。</p>

修 正 條 文	現 行 條 文	說 明
<p>一、資訊中心</p> <p>(一)建築物</p> <p>1、環境</p> <p>設 4、 最好與鄰近建物保持充分之間<u>隔</u>。</p> <p>為防止延燒或滅火工作順利進行，最好能與鄰近建物保持充分之間隔。</p>	<p>一、資訊中心</p> <p>(一)建築物</p> <p>1、環境</p> <p>設 4、 最好與鄰近建物保持充分之間。</p> <p>為防止延燒或滅火工作順利進行，最好能與鄰近建物保持充分之間隔。(P. 30)</p>	
<p>(三) 電源室、空調室</p> <p>設 54、應為專用之獨立房間。</p> <p>為了易於維護、管理，並防止災害的擴大，<u>應考量</u>與其他各室分隔<u>專用之獨立房間</u>。</p>	<p>(三) 電源室、空調室</p> <p>設 54、應為專用之獨立房間。</p> <p>為了易於維護、管理，並防止災害的擴大，<u>最好是</u>與其他各室分隔<u>之專用獨立房間</u>。(P. 38)。</p>	文字調整。

<p>營運基準</p> <p>(一) 確立管理體制</p> <p>1、資訊安全管理與責任之明確化</p> <p>運 3、 建立資訊安全管理體制。</p> <p>為能適切實施資訊安全管理，應指定資訊安全管理負責人，明確訂定其職務範圍、權限及應負之責任。</p>	<p>營運基準</p> <p>(一) 確立管理體制</p> <p>1、資訊安全管理與責任之明確化</p> <p>運 3、 整頓資訊安全管理<u>之</u>體制。</p> <p>為能適切實施資訊安全管理，應指定資訊安全管理負責人，明確訂定其職務範圍、權限及應負之責任。 (P.56)</p>	<p>考量運 3-運 6 之一致性，進行標題及文字調整。</p>
<p>運 4、 建立系統管理體制。</p> <p>為能有效運用資訊安全管理並防止非法行為，應訂定系統管理程序，建立管理之體制。</p>	<p>運 4、 整頓系統管理<u>之</u>體制。</p> <p>為能順利運用資訊安全管理並防止非法行為，應訂定系統管理程序，建立管理之體制。(P.56)</p>	<p>考量運 3-運 6 之一致性，進行標題及文字調整。</p>
<p>運 5、 建立資料管理體制。</p> <p>為維護資料安全，並防止非法行為導致資料損毀或洩露，應訂定資料管理程序，</p>	<p>運 5、 建立資料管理<u>之</u>體制。</p> <p>為能順利維護資料安全，並防止非法行為導致資料損毀或洩露，應訂定資料管理程序，建立管理之體制。</p>	<p>文字調整。</p>

修 正 條 文	現 行 條 文	說 明
建立管理之體制。	(P. 56)	
<p>運 6、 建立網路管理體制。</p> <p>為能有效運用網路系統，並防止非法存取行為，應訂定網路管理程序，建立管理之體制。</p>	<p>運 6、 建立網路管理<u>之</u>體制。</p> <p>為能<u>順利</u>有效運用網路系統，並防止非法存取行為，應訂定網路管理程序，建立管理之體制。(P. 56)</p>	文字調整。
<p>2、組織及分工制衡</p> <p>為保護金融機構資訊系統，使其能安全、順利運轉，並避免其受到災害、故障、<u>入侵</u>或犯罪等事故之重大影響，於發生事故時，能將受災程度減至最低、及早復原，應設置<u>相關組織及訂定權責</u>。</p>	<p>2、組織及分工制衡</p> <p>為保護金融機構資訊系統，使其能安全、順利運轉，並避免其受到災害、故障或犯罪等事故之重大影響，於發生<u>上述</u>事故時，能將受災程度減至最低、及早復原，應設置<u>有關組織</u>。(P. 56)</p>	增列「入侵」為事故之類別，並進行文字調整。
<p>4、安控規章遵守狀況之確認</p> <p>運 10-1、確認對安控規章之遵守狀況。</p>	<p>4、安控規章遵守狀況之確認</p> <p>運 10-1、確認對安控規章之遵守狀況。</p>	增列「委外人員」為資訊安全政策認知之確認對象。

修 正 條 文	現 行 條 文	說 明
應確認對安控規章之遵守狀況，全體員工(包含駐外人員) <u>及委外人員</u> 應對資訊安全政策確實認知，並努力提升機構之安全層次。	應確認對安控規章之遵守狀況，全體員工(包含駐外人員)應對資訊安全政策確實認知，並努力提升機構之安全層次。(P.57)	
<p>(三) 營運管理</p> <p>2、存取權限之管理</p> <p>運 17、採取防止密碼、<u>作業憑證等</u>外洩之措施。</p> <p>為防止密碼、<u>作業憑證等</u>之外洩，除應加強保護外，應<u>宣導使用者落實管理。</u></p>	<p>(三) 營運管理</p> <p>2、存取權限之管理</p> <p>運 17、採取防止<u>密碼外洩</u>之措施。</p> <p>為防止<u>密碼</u>之外洩，應<u>隨時</u>宣導使用者加強<u>密碼之</u>保護，<u>注意其密碼不被他人竊取</u>。(P.59)</p>	增列「作業憑證」為存取權限管理之保護範圍，並進行文字調整。
<p>3、操作管理</p> <p>運 20、明確規定操作之申請及核可<u>程序</u>。</p> <p>為防止電腦系統之非法或</p>	<p>3、操作管理</p> <p>運 20、明確規定操作之申請及核可<u>手續</u>。</p> <p>為防止電腦系統之非法或</p>	文字調整。

修 正 條 文	現 行 條 文	說 明
不當使用，應明確規定操作之申請及核可 <u>程序</u> 。	不當使用，應明確規定操作之申請及核可 <u>手續</u> 。(P. 60)	
<p>運 22、<u>確認執行結果，並留存操作紀錄</u>。</p> <p>為驗證操作之正確性，應<u>確認執行結果，並留存操作紀錄</u>。</p>	<p>運 22、<u>辦理</u>操作之<u>登記及確認</u>。</p> <p>為驗證操作之正確性，應<u>辦理</u>操作之<u>登記及確認</u>。(P. 60)</p>	文字調整。
<p>運 27、確保資料檔案之備份作業。</p> <p>為防範重要資料檔案發生<u>毀損</u>或故障等事故，應製作備份檔案及制定復原程序，明確規定管理方法。</p>	<p>運 27、確保資料檔案之備份作業。</p> <p>為防範重要資料檔案發生<u>破損</u>或故障等事故，應製作備份檔案及制定復原程序，並明確規定管理方法。(P. 60)</p>	文字調整。
<p>運 28、明確規定程式檔案之管理辦法。</p> <p>為防止程式被篡改或破壞等，應由專人按規定方法<u>執</u></p>	<p>運 28、明確規定程式檔案之管理方法。</p> <p>為防止程式被篡改或破壞等，程式檔案應由專人按規</p>	明訂程式檔案之管理應包含程式檔案入出庫管理及保管。

修 正 條 文	現 行 條 文	說 明
<u>行程式檔案入出庫管理及保管作業。</u>	定方法 <u>管理</u> 。(P. 61)	
<p>8、網路設定資訊之管理。</p> <p>運31、應落實網路設定資訊之管理。</p> <p>為預防電腦系統網路設定資訊被篡改，應<u>強化網路設備管理人員帳號密碼保護機制</u>，落實網路設定資訊之管理。</p>	<p>8、網路設定資訊之管理。</p> <p>運 31、應落實網路設定資訊之管理。</p> <p>為預防電腦系統網路設定資訊被篡改，應落實網路設定資訊之管理。(P. 62)</p>	強化網路設備管理人員之帳號密碼保護，以降低未經授權竄改之風險。
<p>運32、應落實網路設定資訊之備份作業。</p> <p>為預防電腦系統網路設定資訊被非法篡改或因應故障發生，應明確訂定備份檔案之<u>取得作業程序</u>及管理辦法。</p>	<p>運32、應落實網路設定資訊之備份作業。</p> <p>為預防電腦系統網路設定資訊被非法篡改或因應故障發生，應明確訂定備份檔案之<u>取得</u>及管理辦法。(P. 62)</p>	明訂備份檔案之取得應有作業程序。
12、交易管理	12、交易管理	文字調整。

修 正 條 文	現 行 條 文	說 明
<p>運 38、明確訂定各類交易之操作權限。</p> <p>為防止<u>利</u>用端末設備從事不正當交易，應依照交易內容，分別訂定端末設備操作者所能操作之權限範圍。</p>	<p>運 38、明確訂定各類交易之操作權限。</p> <p>為防止<u>使</u>用端末設備從事不正當交易，應依照交易內容，分別訂定端末設備操作者所能操作之權限範圍。 (P. 64)</p>	
<p>17、各類卡片管理</p> <p>運 51、明確訂定卡片管理辦法。</p> <p>為確保安全性及卡片之發卡、保管、遞送、回收以及作廢<u>等作業順利，應明確訂定卡片管理辦法。</u></p>	<p>17、各類卡片管理</p> <p>運 51、明確訂定卡片管理辦法。</p> <p>為確保安全性及<u>作業處理順利</u>，卡片之發卡、保管、遞送、回收以及作廢<u>應按規定辦理。</u> (P. 67)</p>	<p>明訂卡片管理應訂定卡片管理辦法並進行文字調整。</p>
<p>21、機器設備之管理</p> <p>運 57、應明確訂定資訊設備管理辦法。</p> <p>為防止資訊系統之各種設</p>	<p>21、機器設備之管理</p> <p>運 57、應明確訂定資訊設備管理辦法。</p> <p>為防止資訊系統之各種設</p>	<p>文字調整。</p>

修 正 條 文	現 行 條 文	說 明
備發生故障、非法使用、破壞、遭竊等，應明確訂定資訊設備管理辦法。	備發生故障、非法使用、破壞、遭竊等，應明確訂定資訊設備管理辦法， <u>以為遵循</u> 。(P. 68)	
<p>運 75、應具有防止資料外洩之措施。</p> <p>為保護機密<u>或個人</u>資料，防止非法行為，在系統報廢時，應有防範由機器設備洩漏資料之措施。</p>	<p>運 75、應具有防止資料外洩之措施。</p> <p>為保護機密資料，防止非法行為，在系統報廢時，應有防範由機器設備洩漏資料之措施(P. 72)。</p>	配合個資法修訂，增列個人資料為防止資料外洩措施之保護範圍。
<p>技術基準</p> <p>一、系統可靠性之提升對策</p> <p>(二) 提昇軟體系統之可靠性</p> <p>1、提昇開發品質</p> <p>技 10、在程式撰寫階段，確保軟體的品質。</p>	<p>技術基準</p> <p>一、系統可靠性之提升對策</p> <p>(二) 提昇軟體系統之可靠性</p> <p>1、提昇開發品質</p> <p>技 10、在程式撰寫階段，確保軟體的品質。</p>	增列「減少程式的安全漏洞」為提昇軟體系統開發品質之要項。

修 正 條 文	現 行 條 文	說 明
依據程式規格書撰寫程式時，應實施程式撰寫的標準化、自動化、安全性等，以能在程式撰寫階段，確保軟體的品質 <u>及減少程式的安全漏洞</u> 。	依據程式規格書撰寫程式時，應實施程式撰寫的標準化、自動化、安全性等，以能在程式撰寫階段，確保軟體的品質。(P. 84)	
<p>(三) 提升營運可靠性之對策</p> <p>1、提升營運可靠性之對策</p> <p>技 19、<u>加強 ATM 之異常偵測能力</u>。</p> <p>為使自動化服務區之<u>ATM</u>穩定運轉，應集中監視其營運狀況，<u>並應加強異常偵測之能力</u>。</p>	<p>(三) 提升營運可靠性之對策</p> <p>1、提升營運可靠性之對策</p> <p>技 19、<u>設置 CD/ATM 之遠端遙控功能</u></p> <p>為使自動化服務區的<u>CD/ATM</u>穩定運轉，應集中監視其營運狀況，<u>必要時可設置遠端遙控功能</u>。(P. 85)</p>	<p>強化 ATM 之異常偵測需求，以提昇營運之可靠性。(本文件所有 CD/ATM 將全部修正為 ATM，不列於本對照表)</p>

金融資訊系統安全基準使用說明

修正條文對照表

修 正 條 文	現 行 條 文	說 明
<p>設備基準</p> <p>一、資訊中心</p> <p>(三) 電源室、空調室</p> <p>設 60、電纜線、各類導管導線等，應設有防止延燒的措施。</p> <p>為避免延燒情況發生，應設有防止由電纜線、導管管線等引起延燒的措施。</p> <p>1、 為能避免火災<u>延</u>燒情況發生，在牆壁面上電纜線、導管管線等貫穿部分，應設有防止延燒的措施。</p>	<p>設備基準</p> <p>一、資訊中心</p> <p>(三) 電源室、空調室</p> <p>設 60、電纜線、各類導管導線等，應設有防止延燒的措施。</p> <p>為避免延燒情況發生，應設有防止由電纜線、導管管線等引起延燒的措施。</p> <p>1、 為能避免火災<u>沿</u>燒情況發生，在牆壁面上電纜線、導管管線等貫穿部分，應設有防止延燒的措施。(P. 86)</p>	<p>文字勘誤。</p>

修 正 條 文	現 行 條 文	說 明
<p><u>營運基準</u></p> <p>(三) 營運管理</p> <p>15、無人化服務區之管理</p> <p>運 45、訂定營運管理辦法。</p> <p>為確保 <u>ATM</u> 及無人化服務區之安全性與順利運作，應訂定營運管理辦法。</p> <p>2、行外 <u>ATM</u> 或無人化服務區 <u>應</u> 訂定營運管理辦法。</p>	<p><u>營運基準</u></p> <p>(三) 營運管理</p> <p>15、無人化服務區之管理</p> <p>運 45、訂定營運管理辦法。</p> <p>為確保 <u>CD/ATM</u> 及無人化服務區之安全性與順利運作，應訂定營運管理辦法。</p> <p>2、行外 <u>CD/ATM</u> 或無人化服務區 <u>可考慮由管轄之分行</u> 訂定營運管理辦法。(P. 271)</p>	<p>明訂行外 ATM 無人化服務區應訂定營運管理辦法。</p>
<p>運 78、確認設備之容量、性能及使用狀態。</p> <p>2、所謂設備，係指下列各項：</p> <p>(10)通訊線路相關設備 (含備援用<u>網路</u>等)</p>	<p>運 78、確認設備之容量、性能及使用狀態。</p> <p>2、所謂設備，係指下列各項：</p> <p>(10)通訊線路相關設備 (含備援用<u>分封網</u></p>	<p>進行文字調整以擴大通訊線路相關設備之適用範圍。</p>

修 正 條 文	現 行 條 文	說 明
	<u>路、撥接網路</u> 等)(P. 339)	
<p>運 92、收付處設置地點之選擇基準，應事先明確訂定。</p> <p>3、對於行外收付處…</p> <p>(2) 設置緊急呼叫鈴、緊急呼叫按<u>鈕</u>等，請參照【設113】。</p>	<p>運 92、收付處設置地點之選擇基準，應事先明確訂定。</p> <p>3、對於行外收付處…</p> <p>(2) 設置緊急呼叫鈴、緊急呼叫按<u>紐</u>等，請參照【設113】。(P. 365)</p>	文字勘誤。
<p>(十三) 利用開放網路之金融商品</p> <p>1、電子郵件</p> <p>運 107、應明確訂定電子郵件之應用方針。</p> <p>2、考慮電子郵件之危險性，應用電子郵件之方針應明確訂定。明確之電子郵件應用方針，舉例如下：</p> <p><u>(6)執行適當之內容過</u></p>	<p>(十三) 利用開放網路之金融商品</p> <p>1、電子郵件</p> <p>運 107、應明確訂定電子郵件之應用方針。</p> <p>2、考慮電子郵件之危險性，應用電子郵件之方針應明確訂定。明確之電子郵件應用方針，舉例如下：(P. 385)</p>	增列「適當之內容過濾防護機制」為電子郵件之應用方針。

修 正 條 文	現 行 條 文	說 明
<u>濾防護機制。</u>		
<p>1、提昇開發品質</p> <p>技 10、在程式撰寫階段，確保軟體的品質。</p> <p>依據程式規格書撰寫程式時，應實施程式撰寫的標準化、自動化、安全性等，以能在程式撰寫階段，確保軟體的品質<u>及減少程式的安全漏洞。</u></p> <p><u>3、在程式撰寫階段，將 OWASP 等常見的網站應用程式弱點納入軟體開發安全參考，避免產生類似弱點，並於程式開發階段執行程式碼安全檢測，以減少程</u></p>	<p>1、提昇開發品質</p> <p>技 10、在程式撰寫階段，確保軟體的品質。</p> <p>依據程式規格書撰寫程式時，應實施程式撰寫的標準化、自動化、安全性等，以能在程式撰寫階段，確保軟體的品質。(P. 410)</p>	<p>將 OWASP 等常見的網站應用程式弱點納入軟體開發安全參考，避免產生類似弱點，並將程式碼安全檢測納入程式開發階段必要程序。</p>

修 正 條 文	現 行 條 文	說 明
<u>式的安全漏洞。</u>		
<p>技 38、設置限制端末設備、作業與交易範圍的功能。</p> <p>2、對交易或業務內容設限的重要因<u>素</u>，舉例如下：</p> <p>(1)依照<u>端末設備</u>種類的業務限制</p> <p>a. 開發用<u>端末機</u>。</p> <p>b. 櫃台<u>端末機</u>。</p> <p>c. <u>ATM</u>。</p> <p>d. 行外<u>端末機</u>。</p> <p><u>e. 提供行員使用之行動裝置。</u></p> <p>(2)依照<u>端末設備</u>設置場所的業務限制：</p> <p>a. <u>ATM</u>。</p> <p>b. 行外可攜式<u>端末機</u>。</p> <p>c. 客戶、企業之<u>端末機</u>。</p>	<p>技 38、設置限制端末設備、作業與交易範圍的功能。</p> <p>2、對交易或業務內容設限的重要因，舉例如下：</p> <p>(1)依照<u>端末機</u>種類的業務限制</p> <p>a. 開發用<u>端末機</u>。</p> <p>b. 櫃台<u>端末機</u>。</p> <p>c. <u>CD/ATM</u>。</p> <p>d. 行外<u>端末機</u>。(P. 460)</p> <p>(2)依照<u>端末機</u>設置場所的業務限制：</p> <p>a. <u>CD/ATM</u>。</p> <p>b. 行外可攜式<u>端末機</u>。</p> <p>c. 客戶、企業之<u>端末機</u>。</p>	<p>文字增補，並增列「行動裝置」為依照<u>端末設備</u>種類進行業務限制之考量對象。</p>