資訊產業 資訊安全管理工程師職能基準

1. 擬定安全方針				
編號	工作	達成指標	所需知識	所需技能
1-1	評估資訊資產	・透過實際面訪經營階層、資訊策略負責或承辦人員、資訊安全相關負責幹部及部門高級主管、資訊系統部門高級主管及企劃相關人員等，辨別該企業的資訊資產（資訊系統、資料、人員和文件紀錄）。 ・經過整理的資訊資產須從機密性、完整性和可用性等三方面去評估並整理其在經營上的重要程度及致命程度。 ・對已經整理並加以評估的資訊資產，應對經營階層、資訊安全相關負責幹部及企劃相關人員作說明，並且獲得認可。	・收集資訊的手法、順序和實行方面的知識。 ・相關法令知識（如公平交易法、著作權和專利權等）。 ・企業資訊資產相關的知識。 ・企業的資訊系統及網路建置相關等知識。 ・有關資訊資產的評估及量化等方面方法的知識。 ・有關作成書面資料的相關知識。	・在展開調查時具備設定目標及範圍的能力。 ・對企業的資訊資產具備足以觀察到細部的能力。 ・對企業內資訊資產的流向具備分析的能力。 ・有能力可以合理地整理資訊資產。 ・有能力可以對經營階層、資訊安全相關負責幹部及企劃相關人員作簡報。 ・對經評估過的資訊資產，有能力可以在公司內部進行交涉。
1-2	認識威脅	・調查資訊必須正確且完整。 ・對資訊來源及掌握要求須採用適切的方法論。 ・對目前構成威脅的相關資訊須多方面收集。 ・將收集到的資訊以竄改資訊、洩漏資訊、耗費資源、資源不當使用和人為過失等工作來進行分類。	・收集資訊的方法、順序和實行方面的知識。 ・與資訊資產有關的事件和事故等實際案例方面的知識。 ・有關評估風險的知識。 ・一般系統和網路的技術與運作的知識。 ・系統及網路架構、硬體與軟體相關的知識。	・在展開調查時具備設定目標及範圍的能力。 ・針對社會上所發生資訊系統的事件和事故，具備足以觀察到細部的能力。 ・具備持續收集資訊的能力。 ・具備掌握合理的威脅的能力。

1-3	辨識風險	・對經評估過的資訊資產，必須可以辨識目前的風險。 ・必須整理出可能發生風險的場所和發生時期。 ・能以實體環境因素、技術性因素和人為因素等將風險原因加以區分整理 。	・具備有關風險種類及發生原因的知識。 ・資訊資產相關的知識。 ・企業資訊系統及網路結構相關的知識。 ・系統及網路架構、硬體與軟體相關的知識。	・對企業資訊資產的風險及構成原因，具備足以觀察到細部的能力。。 ・有能力可以合理地了解資訊資產與風險之間的關係並作整理。
1-4	整理及調查對策	・對已經辨識出的風險須決定相關對策。 ・對決策目前執行狀況應加以調查並整理。	・具備風險對策相關的知識。 ・系統及網路架構、硬體與軟體相關的知識。 ・收集資訊的手法、順序和實行等方面的知識。	・對企業資訊資產的風險及構成原因，具備足以觀察到細部的能力。 ・具備整理出合理的風險及其對策的能力。 ・在展開調查時，具備設定目標及範圍的能力。 ・具備分析調查結果的能力。
1-5	評估風險	・對經過整理的風險，必須確定其發生機率。 ・必須估算發生風險時可能造成的損失總額。 ・對各項風險，研擬降低風險的對策並估算對策的成本。 ・對各項風險，考慮實際發生時，損失總額和對策成本之間的平衡關係。 ・評估可能遺留的風險。 ・對風險對策排定優先順序。	・對發生風險的機率，具備相關經驗資料的知識。 ・對發生風險的機率，具備一般常識的數字及統計的知識。 ・有關安全對策之估算成本相關的知識。	・對因風險所造成對資訊資產的損失(如損失的資產價值、了解原因的成本及修復費用、對社會說明的費用等)，具備估算和評估的能力。 ・針對社會上所發生的資訊系統安全事件和事故，具備足以觀察到細部的能力。 ・具備持續收集資訊的能力。

1-6	擬定安全方針	・在經營方針裡，明確提示必須研擬資訊安全對策。 ・方針的內容應該不能依賴所有的技術。 ・在安全對策中要明白記載有關目的、適用範圍、達成水準、對策基準方針、資訊安全負責人、經營幹部與員工遵守事項、組織或實施體制、運作、罰責、公開及重新檢討的內容等等。 ・應對經營階層、資訊安全相關負責幹部及企劃相關人員作說明，並且獲得認可。	・必須具備經營方針相關的知識。 ・有關作成書面資料的相關知識。。 ・有關擬定安全方針之方法的知識。	・在製作政策時，要具備充分應變能力，可以回溯到從評估資訊資產到評估風險的所有任何前置作業。 ・有能力以業務水準的詞彙來進行相關工作之記述。 ・具備撰文表達能力，闡述安全對策的持續性。 ・具備對經營階層、資訊安全相關負責幹部及企劃相關人員等作簡報之能力。

資訊產業 資訊安全管理工程師職能基準

2. 擬定安全基準				
編號	工作	達成指標	所需知識	所需技能
2-1	擬定一般企業活動的安全規範	・最少必須涵蓋研擬安全方針時所歸納整理的對策。 ・最少需對經營階層、資訊安全相關負責幹部及企劃相關人員等作說明，並且獲得認可。 ・依照分析風險所擬定的對策，可制定下列基準： （1）聘僱契約/職務規定 （2）機密/文件/資訊管理之規定 （3）資訊安全教育的規定 （4）罰責的規定 （5）對外說明的規定 （6）例外的規定 （7）更新規則的規定	・有關安全方針的知識。 ・有關安全基準之標準的知識。 ・有關法令及法律程序方面的知識。 ・有關聘僱契約方面的知識。 ・有關職務規定的知識。 ・有關保密義務協定方面的知識。 ・有關保護個人隱私相關的知識。 ・有關危機管理相關的知識。 ・有關洩漏機密方面的知識。 ・有關機密資訊之管理流程的知識。 ・有關安全事件和事故等實際案例方面的知識。 ・有關安全方面的外部教育服務方面的知識。 ・有關發布消息的知識。 ・有關擬定基準和更新基準方面的知識。 ・有關文件管理及變更文件手續等方面的知識。	・對制定基準，具備足以觀察到細部的能力。 ・具對經營階層、資訊安全相關負責幹部及企劃相關人員作簡報之能力。 ・擬定基準後，具對已經評估過的資訊資產，在公司內部進行交涉之能力。 ・對有關安全性的事件和事故的實際案例，具備持續收集資訊的能力。 ・具備靈活運作基準的能力。

2-2	擬定資訊系統的安全規範	・此規範必須涵蓋研擬安全方針時所歸納整理的對策。 ・此規範應對經營階層、資訊安全相關負責幹部及企劃相關人員作說明，並且獲得認可。 ・依據分析風險歸納的對策，可研擬出下列的基準。 （1）使用網路之規定 （2）針對網路中公用伺服器的設置及管理規定。 （3）公司內伺服器及用戶端的設置及管理規定。 （4）遠端存取點（remote access point）的設置及管理規定。 （5）應用程式安裝（application install）的規定 （6）資料管理的規定。 （7）運作電腦病毒對策的規定。 （8）緊急對應的規定。 （9）監查安全性的規定。 （10）資訊系統管理人員的規定。 （11）開發系統的規定	・具備安全方針方面的知識。 ・具備安全基準之標準的知識。 ・具備有關網路所上提供之服務、流行和犯罪案例等的知識。 ・具備網路存取技術及安全性工具相關的知識。 ・具備網路拓樸（TOPOLOGY）相關的知識。 ・具備防火牆方面的知識。 ・具備安裝及使用伺服器方面的知識。 ・具備安裝及使用運作遠端存取伺服器（remote access server）的知識。 ・具備有關應用軟體執照體系的知識。 ・具備有關洩漏機密的知識。 ・具備有關資訊密碼化技術的知識。 ・具備有關網路、硬體和軟體的知識。 ・具備有關社會工學的知識。 ・具備有關電腦病毒的知識。 ・具備有關電腦病毒應用軟體的知識。 ・具備有關危機管理的知識。 ・具備有關發表聲明的知識。 ・具備有關檢測事故的知識。 ・具備有關監控安全的知識。 ・具備有關職務規定的知識。 ・具備系統運作與管理方面的知識。 ・具備系統開發程序相關的知識。 ・具備外包契約的知識。	・對制定基準具備足以觀察到細部的能力。 ・有能力可以對經營階層、資訊安全相關負責幹部及企劃相關人員作簡報，而且具說服力。 ・在擬定基準後，有能力可以在公司內部進行交涉。 ・對有關網路上所提供之服務、流行等訊息，具備持續收集資訊的能力。 ・對有關資訊安全事件和事故的實際案例，具備持續收集資訊的能力。 ・能夠從事件及事故的案例中，分析對策。

3. 安全系統設計				
編號	工作	達成指標	所需知識	所需技能
3-1	認證及權限控制	・為達成安全基準須執行下列的系統設計： （1）密碼設計應避免選擇容易簡單推算的文字組合。 （2）須經研判後，始能決定是否採用生物辨識-依人體部位辨識功能（BIOMETRICS）或數位簽章（DIGITAL SIGNATURE）技術 （3）認證作業的設計不需超過實際所需，亦避免過於冗長，同時存取控制的設定要簡化、方便。 （4）可對存取權限進行管控，當有非法使用，闖入一個認證時，須使其無法存取進入其他部分。 （5）應設計可以記錄使用者的操作動作，並且當使用者對系統及資料發生不當存取，能夠及早發現的裝置。	・具備密碼學技術的知識。 ・具備認證技術的知識。 ・具備生物辨識（BIOMETRICS）技術方面的知識。 ・具備數位簽章方面技術的知識。 ・具備作業系統（OS）方面的知識。 ・具備網路、硬體、軟體及資料庫的知識。	・有能力可以從安全基準中導出有關認證及權限的系統條件。 ・有能力作認證及權限關係的整合， ・有能力可以從整體規劃的角度，將認證、密碼技術和數位簽章技術等相關資訊安全技術整合在一個系統裡。 ・能夠結合生物辨識（BIOMETRICS）技術和數位簽章技術，提出系統化的提案。

3-2	實體及環境安全控制	・為達成安全基準，必須執行以下的系統設計： （1）選擇合適的預防訊號洩漏之實體傳輸媒體。 （2）選擇在網路斷線事故時，受害範圍最小的網路拓樸 （3）確認具備實體隔離。 （4）決定實體裝置的配置，手動存取，以及使用環境的安全裝置等。	・具備從通訊電纜竊聽等方面的知識。 ・具備網路拓樸相關的知識。 ・具備網路硬體和軟體的知識。 ・具備有關資訊安全產品相關的知識。	・有能力可以從安全基準導出實體裝置上有關資訊安全的系統要件。 ・有能力依照風險分析所作的資訊資產評估，採用適切的實體安全方式。 ・能對實體上能隔離重要資訊資產的系統，進行整合的動作。 ・能夠實際到企業相關的組織，針對實現實體安全進行討論並說服他人。
3-3	邏輯安全性控制	・為達成安全基準，必須執行以下的系統設計： （1）理解網路設計，並能從資訊安全的觀點檢討問題對策。 （2）對網路存取控制，應明確要求。使經過認證的使用者能夠存取到適當的網路資產。	・具備網路架構的知識。 ・具備網路拓樸（TOPOLOGY）相關的知識。 ・具備網路過濾原理的知識。 ・具備有關 TCP/IP 的知識。 ・具備路由（Routing）的知識。	・有能力可以從安全基準導出有關邏輯安全性的系統要件。 ・具備將安全技術適用在系統設計的能力。 ・具備理解網路設計的能力。 ・有能力可以從安全系統的設計要件導出網路設計要件。

3-4	確保資料在網路傳輸上的可信度	・為達成安全基準，必須執行以下的系統設計： （1）決定是否安裝防火牆以限制、允許或拒絕流量。 （2）針對網路服務、協定及相關支援，設計相對的安全機制。 （3）網路架構中使用的重要資料流（如路由資訊的更新訊息），要設計成透過認證才可進行的方式。 （4）對重要資料在備份後傳送，如果發生失敗應該有重新傳送的功能。	・有關防火牆的知識。 ・有關網路架構的知識。 ・有關網路服務的知識。 ・有關路由技術的知識。 ・有關 TCP 協定的知識。 ・有關網路攻擊的知識。	・有能力可以從安全基準導出與資料整合性相關的系統要件。 ・具備能將安全技術適用在系統設計的能力。 ・能依據風險分析出來的系統重要性，決定適切的流量控制系統。 ・能收集 CERT/CC 和廠商提供有關網路服務的相關資訊，加以過濾後，依必要性將之套用在系統上。
3-5	資料機密的維持	・為達成安全基準，必須執行以下的系統設計： （1）透過風險分析，將非法使用時風險最大的資料加密。 （2）必須設計成只有在特殊情況下時才能執行金鑰回復的動作。 （3）在設計中，金鑰的管理須充分被保障。	・具備有關密碼學技術的知識。 ・具備運作密碼系統的知識。 ・具備金鑰管理方法的知識。	・具備從安全基準中，推導出維持資料機密的機制要件。 ・具備能將安全技術使用在系統設計上的能力。 ・具備判斷資料有否需加密的能力。 ・具備實作管理金鑰的能力。

3-6	研擬安全性的運作程序	・為達成安全基準，必須聽取使用者的意見，作成以下適切的運作內容及運作程序，並且取得單位組織的許可： （1）備份及重新架構的操作程序 （2）完成軟體的備份及資料的保管等程序 （3）對單位組織內的電腦及重要資料之攜離，應訂定嚴謹的程序。 （4）決定在監控安全時，所要收集資料的範圍。 （5）有關安全監控資料的保存管理程序。 （6）對涵蓋個人資訊的監控資料，應考慮個人隱私權的問題	・具備有關文件管理的知識。 ・具備有關儲存媒體的知識。 ・具備有關備份工具的知識。 ・具備有關機密洩漏的知識。 ・具備有關安全監查的知識。 ・具備有關保障隱私權的知識。 ・具備有關協助調查安全事故能力的知識。	・有能力可以從安全基準中導出有關備份機制等的相關要件。 ・有能力可以研擬一套完整的備份程序。 ・具備決定檢測資料範圍的能力，以檢測出安全事件或事故的發生。 ・對備份的資料和所監控安全的資料，具備保管方法的能力。 ・有能力可以從安全基準中，研擬出實際運作安全系統的操作流程 。 ・針對擬定的運作內容及流程，有能力可以在公司內部進行交涉。
3-7	對使用者啟蒙及教育訓練計劃	・為達成安全基準，必須執行以下的事項： （1）對持續執行資訊安全教育，須獲得經營高層的認同。 （2）為提昇安全意識，須執行安全相關的啟蒙教育。 （3）對經營階層和公司員工，須擬定教育訓練計劃，並持續執行資訊安全教育。	・具備有關資訊資產風險的知識。 ・具備有關公司內安全相關之規定及罰則規定等的知識。 ・具備一般有關資訊安全新領域方面的知識。	・具備說服經營階層持續實施安全教育的重要性。 ・能考量使用者的方便，擬定教育計劃。

4. 實作與檢查安全系統				
編號	工作	達成指標	所需知識	所需技能
4-1	安全性產品的選擇及導入	·選擇並導入適合企業網路架構的安全產品。 ·對導入產品的成本與實際發生風險所造成損失，須檢討其投資報酬率。 ·必須確認必要的安全機能是否有動作。 ·必須確認是否合乎國際標準。	·具備有關企業網路架構的知識。 ·具備有關資訊安全相關產品性能的知識。 ·具備有關 ISO15408 的知識。	·具備選擇實作安全系統的相關產品之能力。 ·具備在適當的投資報酬率下，挑選合適的資訊安全產品之能力。
4-2	安全系統的開發	·必須充分調查有無符合需求的安全性產品。 ·對開發產品的成本與實際發生風險所造成損失，應該檢討其投資報酬率。 ·必須確認必要機能的動作。	·具備有關資訊安全產品性能的知識。 ·具備有關電腦系統架構的知識。 ·具備有關網路系統架構的知識。 ·具備有關開發軟體方面的知識。	·具備可以明確定義安全機能要件的能力。 ·對已開發的系統，能夠檢測是否具備安全機能要件的要求。 ·具備了解電腦和網路作業系統運作模式的能力。
4-3	安全系統實作的確認	·須取得有關安全漏洞（SECURITY HALL）資訊、安全建議和安全修補（PATCH）等資訊的最新訊息。 ·對實際攻擊，需執行入侵檢查。 ·入侵檢查的內容須反映有關資資訊全的最新訊息。 ·一旦發現安全漏洞，必須儘速採取對策，並檢討日後可能的持續對策。	·具備有關安全漏洞方面的知識。 ·具備有關安全建議的知識。 ·具備有關檢視安全機能或檢查安全漏洞所需工具的知識。 ·具備有關電腦系統及網路系統架構的知識。 ·具備有關網路攻擊方面的知識。	·能持續收集有關安全漏洞及安全方面訊息的能力。 ·具備實作網路攻擊的能力。 ·具備得到公司內部信任的能力。

5. 安全系統的運作管理				
編號	工作	達成指標	所需知識	所需技能
5-1	實施安全運作的流程	·必須依據安全政策（安全方針及安全基準），實際運作，並發揮其機能。 ·執行過程中發生的問題，必須加以紀錄。	·有關在安全政策下，安全運作用流程方面的知識。 ·有關例外的運作流程相關的知識。	·具備製作一套可讓人完全遵循的運作流程。 ·能夠發現運作流程的隱藏問題，並加以阻止。
5-2	系統運作的監控與記錄	·須明確定義監控的對象與方法。 ·安全系統設計中決定的資料流，必須加以監控並記錄。 ·紀錄的資料必須妥善保存，並維持其可被分析的狀態。 ·一旦發現違反安全之狀況，必須依據既定的程序採取對應的步驟。	·有關安全運作流程方面的知識。 ·有關安全監控工具方面的知識。	·可以從些微的紀錄中，發現或預測重大的攻擊事實· ·能夠利用安全監控工具，發現安全漏洞及違反安全的狀況（此能力包含執行並管裡所用工具，以進行檢查的人力）。 ·對違反安全，能夠迅速處理對應。
5-3	系統保護	·取得有關安全漏洞的資訊、安全建議和安全修補程式等資訊的最新訊息。 ·評估檢討廠商所提供最新的安全修補程式，如有必要應該導入。	·有關安全漏洞的知識。 ·有關安全修補程式方面的知識。 ·有關網路系統的知識。 ·有關網路產品的知識。	·能夠選擇網路上所須的安全修補程式。 ·具備執行安全修補程式的能力（此能力包含執行並管理執行安全修補程式的人力）。
5-4	教育使用者	·必須確實達成教育計劃裡的機能。 ·須適時且持續對使用者進行安全相關教育。	·有關資訊安全事件及事故方面的知識。 ·有關資訊資產所可能產生的風險方面的知識。 ·有關公司內部規定與罰責方面的知識。	·能夠簡單明瞭解說安全性事件及事故。 ·具備說服使用者的能力。 ·具備簡報的能力。 ·具備與使用者的部門主管進行溝通的能力。

5-5	教育安全技術人員	·必須確實達到發揮教育計劃裡的機能。 ·安全技術人員的教育必須適時且持續地執行。 ·教育成果須應用在安全運作管理上。	·具備有關資訊安全外部服務的知識。 ·具備有關安全事件及事故的相關知識。 ·具備網路攻擊的相關知識。	·能讓人學到新技術資訊的能力。 ·能夠分析安全事件及事故的原因。 ·能夠將學到的技術，用在安全系統的運作管理上。

6.安全分析				
編號	工作	達成指標	所需知識	所需技能
6-1	檢測可能發生的事故	・充分掌握正常系統如何動作。 ・定期檢查日誌檔。 ・定期檢查系統的完整性。 ・可以利用自動啟動工具程式，檢測不當入侵。	・具備網路攻擊的知識。 ・具備檢測入侵方法的知識。 ・具備有關系統存取日誌檔相關的知識。 ・具備檢測不當入侵系統及其他自動工具程式等相關的知識。 ・具備外部監控服務內容相關的知識。	・具備持續監控的能力。 ・可以從些微的紀錄中發現或預測重大的攻擊事實・ ・對違反安全者能在不破壞人際關係的情況下給予警告。
6-2	事故初期的處理	・須將事故發生初期的對應處理程序作成書面資料。 ・須依照程序確實聯絡資訊系統負責人及相關部門。 ・須確定處理事故的優先順序。 ・須依據處理的優先順序進行處理，以避免受害範圍擴大。 ・對事故初期處理的紀錄，作成書面資料，同時提出報告。	・有關公司內部聯絡體制與責任體制等方面的知識。 ・有關事故的公布等方面知識。 ・有關安全政策方面的知識。 ・有關風險分析的結果與資訊資產重要性等方面的知識。 ・有關電腦系統與網路系統方面的知識。 ・有關系統運作方面的知識。	・具備在事故初期可以冷靜應對的能力。 ・能從資訊資產的重要性決定處理的優先順序。 ・能夠正確地轉述事實而不加入個人揣測意見。 ・能夠與 CERT/IPA 等單位取得聯繫，作適當的處理。
6-3	事故分析	・必須健全事故分析的體制。 ・必須辨識受害的範圍。 ・可以取得有關安全漏洞資訊、安全建議和安全修補程式等資訊的最新訊息。 ・須確定事故發生的原因。	・具備網路攻擊的知識。 ・有關電腦系統與網路系統的知識。 ・有關安全事件與事故的知識。 ・有關分析安全監控資料的知識。 ・有關調查事故原因處理程序的知識。	・能夠慎重地調查網路攻擊的狀況並加以分析。 ・能夠與 CERT/IPA 等單位取得聯繫，報告事故發生的原因，並且對事故客觀地分析。 ・能夠對事故內容作詳細的紀錄。

6-4	事故的修復	・發生事故後須儘速修復，若有必要需重新建置系統。 ・修復時應留下書面的詳細紀錄。 ・修復後，須通知資訊系統管理人員和使用者。 ・修復後須重新檢討安全性。	・具備有關安全漏洞、安全建議和安全修補程式等資訊的知識。 ・具備有關企業系統架構方面的知識。 ・具備有關備份程序與重新建置程序等方面的知識。	・能夠在短時間內判斷事故的緊急性和短期修復的對策，並加以應對處理。 ・具備正確紀錄並告知事實的能力。
6-5	實施預防措施	・必須擬定避免同樣事故再度發生的對策，若有必要需重新建置系統。・在擬定對策後須重新檢討安全性。	・具備有關安全安全漏洞、安全建議和安全修補程式等資訊的知識。 ・具備有關企業系統架構方面的知識。	・能夠從事故發生原因中，研判適當的處理方法並加以執行。 ・具備正確紀錄並告知事實的能力。
6-6	評估安全系統	・執行入侵檢查以評估其遵守安全政策的情形。 ・必須持續執行入侵檢查。 ・在入侵檢查中一旦發現缺陷，必須儘速採取對策。 ・利用安全性的評估資訊，重新檢討安全性。	・具備有關安全漏洞、安全建議和安全修補程式資訊的知識。 ・具備有關安全檢查工作項目的知識。 ・具備有關外部檢查服務的知識。 ・具備有關網路攻擊方面的知識。	・一旦發現安全漏洞，能夠儘速處理。 ・能夠持續實施安全對策。 ・能夠獲得公司內部的信任。 ・能夠使用各種攻擊工具。

7.重新檢視安全政策				
編號	工作	達成指標	所需知識	所需技能
7-1	收集技術資訊並做評估	·可以獲得有關安全漏洞、安全建議和分析安全修補程式等資訊的最新資料。 ·收集最新的有關安全技術方面的資訊，並評估是否適用於公司內的系統上。	·具備有關安全事件或事故的相關知識。 ·具備有關安全技術方面的知識。 ·具備企業系統架構和網路架構等相關的知識。 ·具備相關廠商資訊的知識。	·具備收集有關安全技術方面資訊的能力。 ·能夠對企業的資訊系統及網路相關之安全漏洞，以及安全技術方面資訊有去蕪存菁的能力。
7-2	整理運作上的問題點並作分析	·對使用者進行問卷調查或面訪，以收集並整理運作實施時的問題點。 ·要收集並整理違反情況較多的基準。 ·對於經過整理的問題點，須分析是否變更安全政策，同時重新檢討政策內容。 ·為避免同樣事故再度發生，因而實施相對的應對措施，應分析對安全性政策所造成之影響，並且重新檢討政策。	·具備有關收集資訊的方法、程序及實作等方面的資訊。 ·具備企業系統架構和網路架構等相關的知識。 ·具備企業系統和網路之運作的相關知識。	·在展開調查時具備設定目標及範圍的能力。 ·能從問卷調查的分析中，整理出系統和網路運作時的可能問題點。 ·對所分析的問題點，能夠重新檢討安全政策。 ·對所分析的問題點，能夠向經營階層報告經營上應對的方式。
7-3	整理技術上的問題點並作分析	·藉由開發新技術而了解安全性政策受影響的部位，並加以整理。 ·藉由安全性分析的評估結果，了解安全性政策受影響的部份，並加以整理。 ·對經過整理的問題點，分析是否變更安全性政策，同時重新檢討政策內容。	·具備有關安全技術方面的知識。 ·具備企業系統架構和網路架構等相關的知識。	·具備整理安全相關資訊的能力。 ·能從整理過的技術資料中，分析出安全性政策（方針與基準）的可能問題點。 ·能從所分析出的問題點中，重新檢討安全性政策。 ·對所分析的問題點，能夠向經營高層報告經營上應對的方式。

7-4	整理新的風險並作分析	・收集並整理新的風險。 ・藉由新的風險，了解安全性政策受影響的部位，並加以整理。 ・對經過整理的問題點，分析是否變更安全性政策，同時重新檢討政策內容。	・具備認知安全性的相關事件和事故的知識。 ・具備有關新的安全技術方面的知識。 ・具備企業系統和網路架構等的相關知識。	・收集有關安全性的相關事件和事故之實例並加以整理。 ・能夠從案例中鎖定安全相關事件及事故的發生原因並分析對策。 ・能從整理過的技術資料中，分析出安全性政策（方針與基準）的可能問題點。 ・能從分析出的問題點，重新檢討安全性政策。
7-5	更新安全政策	・須健全安全性政策更新的體制。 ・依分析結果對政策變更的部分，重新作風險分析並更新政策。 ・有關更新安全性政策，應該獲得經營階層、資訊安全相關負責人員及企劃相關人員的認可。 ・持續地重新檢討安全政策。	・有關變更安全性政策程序方面的知識。 ・有關安全性政策方面的知識。 ・有關擬定安全性政策(方針與基準)方法的知識。	・能夠持續地徹查安全性政策的內容。