

政府資訊科技總監辦公室

互聯網通訊閘保安指引

**[G50]**

第 4.0 版

二零零九年十二月  
香港特別行政區政府

## 版權公告

© 2009 香港特別行政區政府

除非另有註明，本出版物所載資料的版權屬香港特別行政區政府所有。在符合下列條件的情況下，這些資料一般可以任何格式或媒介複製及分發：

- (a) 有關資料沒有特別註明屬不可複製及分發之列，因此沒有被禁止複製及分發；
- (b) 複製並非為製造備份作售賣用途；
- (c) 必須準確地複製資料，而且不得在可能誤導他人的情況下使用資料；以及
- (d) 複製版本必須附上“經香港特別行政區政府批准複製／分發。香港特別行政區政府保留一切權利”的字眼。

如須複製資料作上述核准用途以外的用途，請聯絡政府資訊科技總監辦公室尋求准許。

## 目錄

<b>1. 目的</b> .....	<b>1-1</b>
<b>2. 範圍</b> .....	<b>2-1</b>
2.1 資訊科技保安文件概覽 .....	2-2
<b>3. 參考資料</b> .....	<b>3-1</b>
3.1 標準及指引 .....	3-1
3.2 其他參考資料 .....	3-1
<b>4. 定義及慣用詞</b> .....	<b>4-1</b>
4.1 定義 .....	4-1
4.2 慣用詞 .....	4-1
<b>5. 互聯網通訊閘概覽</b> .....	<b>5-1</b>
5.1 網絡互連 .....	5-1
5.2 建議採用的保安措施 .....	5-1
5.3 互聯網通訊閘架構示例 .....	5-3
<b>6. 防火牆</b> .....	<b>6-1</b>
6.1 防火牆配置 .....	6-1
6.2 防火牆管理 .....	6-2
<b>7. 路由器</b> .....	<b>7-1</b>
<b>8. 郵件通訊閘保安</b> .....	<b>8-1</b>
8.1 郵件伺服器設計及配置 .....	8-1
8.2 電郵轟炸、濫發電郵及電郵仿冒 .....	8-1
8.3 接達控制 .....	8-2
<b>9. 網站保安</b> .....	<b>9-1</b>
9.1 網站伺服器配置及管理 .....	9-1
9.2 接達控制 .....	9-1
9.3 網站內容管理 .....	9-2
9.4 共用網間連接界面腳本及應用程式界面程式 .....	9-2
9.5 認證 .....	9-3
9.6 網路瀏覽器 .....	9-3
9.7 主動式內容及COOKIE .....	9-3
<b>10. 遠程接達伺服器及調解器群</b> .....	<b>10-1</b>
<b>11. 領域名稱伺服器</b> .....	<b>11-1</b>
<b>12. 入侵偵測及監察</b> .....	<b>12-1</b>
<b>13. 其他保安考慮事項</b> .....	<b>13-1</b>
13.1 實體保安 .....	13-1
13.2 記錄 .....	13-1
13.3 備份及復原 .....	13-1
13.4 防範電腦病毒及惡意程式碼 .....	13-1

---

13.5	操作系統保安 .....	13-2
13.6	保安審計 .....	13-3
13.7	系統管理及操作 .....	13-3

**附錄**

A	— 建議就互聯網通訊閘保安採用的保護措施清單 .....	A-1
---	------------------------------	-----

## 1. 目的

本文件為互聯網通訊聞保安提供一般指引。這些指引針對互聯網公開平台，是控制保安風險於可接受水平的最佳作業實務。這份文件專為參與互聯網通訊聞操作及技術工作的人員而制訂。

由於本文件所載為一般性資料，不是為任何特定的電腦平台而編製，讀者應衡量個別環境考慮以選擇適用的資料。讀者如需要其他技術方面的意見，可聯絡政府資訊科技總監辦公室資訊科技保安小組。

## 2. 範圍

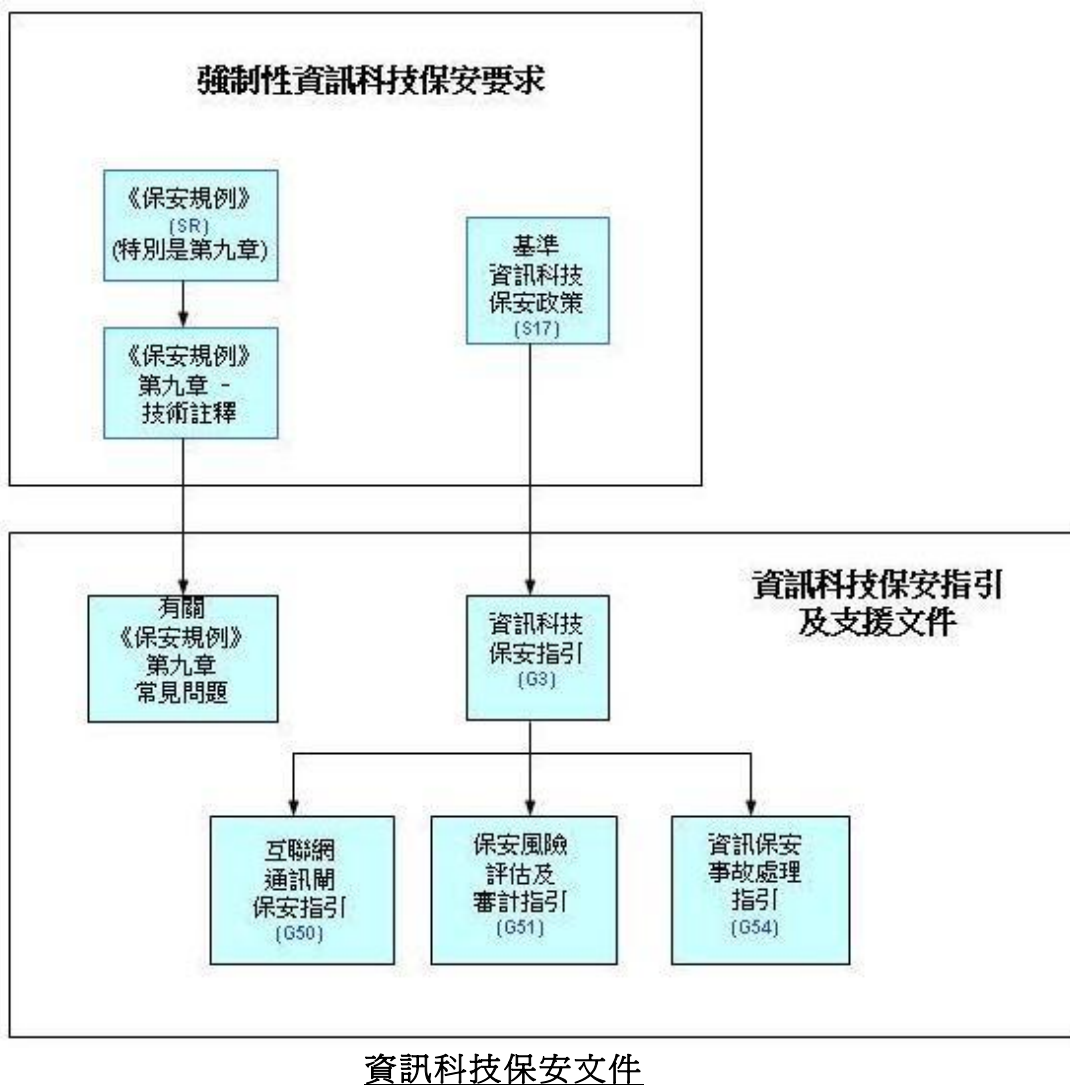
本文件就下列主要保安範疇提出指引：

- 互聯網通訊閘概覽
- 防火牆
- 路由器
- 郵件通訊閘保安
- 網站保安
- 遠程接達伺服器及調解器群
- 領域名稱伺服器
- 入侵偵測及監察
- 其他保安考慮事項

本文件旨在提供有關互聯網通訊閘最佳作業實務的資料，應與既定的保安規例、資訊科技保安政策、指引及程序一併使用。

## 2.1 資訊科技保安文件概覽

下圖所示為政府內部各資訊科技保安文件之間的關係：



五份核心資訊科技保安文件的目的及概要簡述如下：

- 《基準資訊科技保安政策》：**  
**(S17)**
- 最高層次的指令文件，為全體政策局／部門制訂保安規格必須達到的最低標準。這份文件列明了對政策局／部門至關重要的保安工作領域。《基準資訊科技保安政策》可視為必須遵守的強制性基準規例，此外，各政策局／部門亦可採取其他適當的措施加強保安。
- 《資訊科技保安指引》：**  
**(G3)**
- 介紹資訊科技保安的一般概念，並對《基準資訊科技保安政策》作出詳細詮釋。這份文件為制訂保安要求提供了指引和應予考慮的事項。
- 《互聯網通訊閘保安指引》：**  
**(G50)**
- 《資訊科技保安指引》的補充文件，為互聯網通訊閘保安提供一般指引。這些指引是針對互聯網公開平台，將保安風險控制在可接受水平的最佳作業實務。這份文件專為參與互聯網通訊閘操作及技術工作的人員而制訂。
- 《保安風險評估及審計指引》：**  
**(G51)**
- 《資訊科技保安指引》的補充文件，介紹資訊科技保安風險評估及保安審計的通用模型。這份文件的重點並非介紹如何進行保安風險評估或審計的詳情，而是提供一個參考模型，以確保由獨立保安顧問或審計師提供的服務，在範圍、方法及成品方面有所參照。
- 《資訊保安事故處理指引》：**  
**(G54)**
- 《資訊科技保安指引》的補充文件，為管理、行政及其他技術和操作人員提供參考，以便制訂保安事故處理計劃。此外，亦可用作資訊保安事故防範、偵測及應變的參考資料。

### 3. 參考資料

#### 3.1 標準及指引

- a) 《資訊科技保安指引》(G3)  
(<http://www.ogcio.gov.hk/chi/prodev/csecpol.htm>)

#### 3.2 其他參考資料

- a) 香港特別行政區政府《保安規例》
- b) 香港特別行政區政府——《公開資料守則》
- c) Site Security Handbook, Internet Engineering Task Force (IETF) – RFC2196  
(<http://www.ietf.org/rfc/rfc2196.txt>)
- d) The World Wide Web Security FAQ  
(<http://www.w3.org/Security/Faq/www-security-faq.html>)

## 4. 定義及慣用詞

### 4.1 定義

無

### 4.2 慣用詞

無

## 5. 互聯網通訊閘概覽

互聯網通訊閘是互聯網專用連接的界面。不論界面與部門或政府內部網絡是否有連接，互聯網通訊閘提供了與互聯網的連接點。安全的互聯網通訊閘可收緊控制，並建立更具成本效益和安全的操作環境。

由於互聯網屬於開放性平台，加上複雜的網絡服務和應用系統發展迅速，通訊閘缺乏保安措施可能令內部網絡容易遭受攻擊。因此，互聯網通訊閘的配置必須恰當，並應採取適當的保安措施以保護通訊閘免被攻擊。

### 5.1 網絡互連

互聯網通訊閘往往與內部網絡互連，使內部網絡能夠接達通訊閘服務。然而，在互連網絡時必須加倍小心，以確保**網絡互連不會降低或削弱現有保安水平至無法接受的程度，也不會損害所處理資料的安全性**。因此，互連各方必須：

- 維持在自有網絡、主機和系統所實施的特定保安防衛措施
- 維持本身的保安政策和指引，但這些政策和指引應配合互聯網通訊閘的有關政策和指引
- 建立嚴格的互聯網通訊閘邏輯接達控制
- 為互聯網接達和服務制訂保安事故處理和報告程序
- 提醒並教育用戶遵守及遵從相關的保安政策、指引和程序。

### 5.2 建議採用的保安措施

僅提供互聯網接達服務的安全互聯網通訊閘必須具備以下保安功能：

- 防火牆（接達控制）
- 小包過濾路由器（通訊路由和小包過濾）
- 入侵偵測系統（記錄、監察及偵測攻擊）
- 防範電腦病毒（偵測及預防電腦病毒）

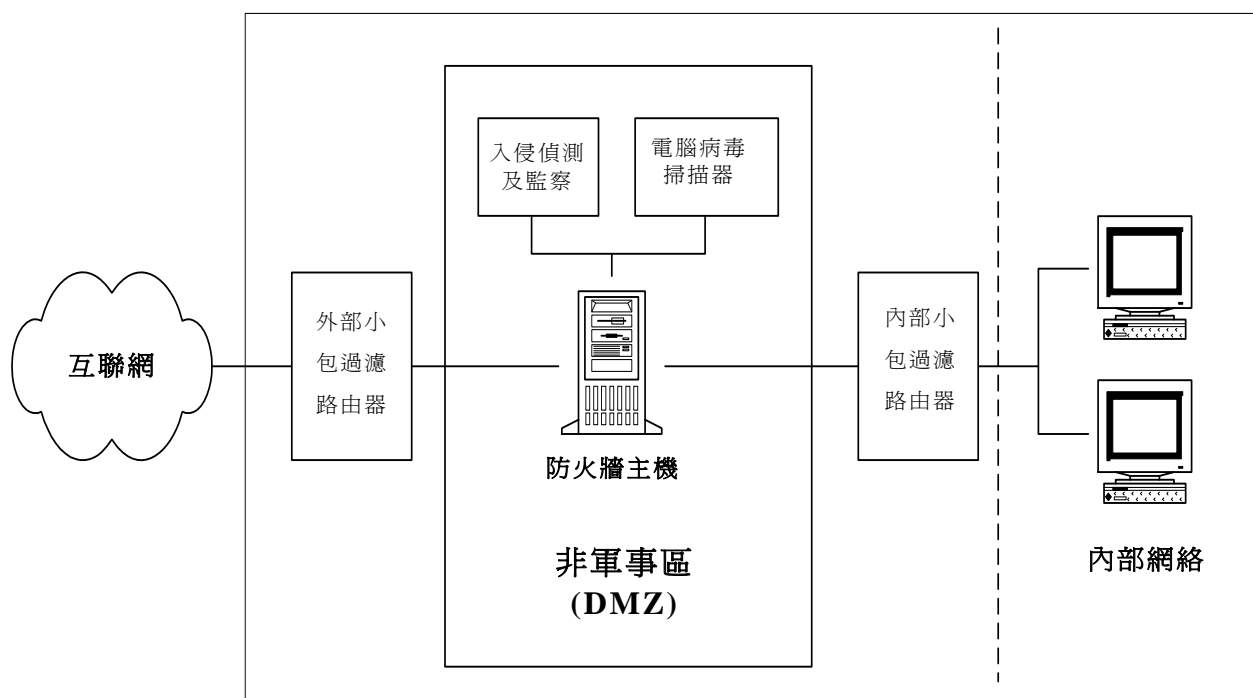


圖 1 — 具備建議保安保護措施的互聯網通訊閘

上圖所示是建議採用的互聯網通訊閘保安保護措施，互聯網通訊閘在毋需託管任何網站伺服器或郵件伺服器的情況下，提供了內部接達互聯網的途徑。非軍事區(DMZ)是保安措施所在的區域。

值得注意的是防火牆並非解決所有保安問題的方案。防火牆無法抵禦：

- 拒絕服務攻擊，也無法保證數據的完整性
- 用戶的意外攻擊
- 電腦病毒或惡意程式碼的攻擊

這些都是防火牆應與其他保安功能（例如入侵偵測與監察及電腦病毒掃描）一併使用的原因。然而，防火牆製造商不斷加強防火牆的功能（例如虛擬私有網絡、加密等），使防火牆與其他保安措施的分別日趨模糊。

兩部小包過濾路由器（外部及內部路由器各一部）從外部或內部網絡，過濾和引入經挑選的通訊至防火牆。為連接互聯網，路由器（即外部小包過濾路由器）是必需的設施。內部路由器則用來將非軍事區部分（下文將作詳細說明）與內部網絡隔開。與防火牆不同，這些路由器一般被視為具增值保安功能的網絡設備，而不是保安產品。

上文所述泛指可提供入侵偵測及監察功能的任何方法，可以是工具或程序，而不一定是實體裝置。使用入侵偵測系統工具有助將入侵偵測及監察程序自動化、加快和促進入侵偵測及監察程序。入侵偵測系統工具的實際使用仍須視乎個別要求而定，但通訊閘至少應提供一種偵測和監察入侵的程序機制。

此外，為控制和監察互聯網通訊閘，還應制訂一系列保安政策和程序。定期或在實施互聯網通訊閘前進行保安審計，可確保互聯網通訊閘是按照保安政策適當地設置。即使在沒有內部網絡的情況下，亦宜採取上文建議的保安保護措施。

附錄 A 列表所載為建議就互聯網通訊閘保安採取的一些保安措施。

### 5.3 互聯網通訊閘架構示例

下圖所示是互聯網通訊閘的邏輯網絡圖示例。各部門可根據個別需要、所提供的服務和現行的網絡結構，按下圖所示調整網絡架構。網絡構件的相對位置可能需要作出調整。

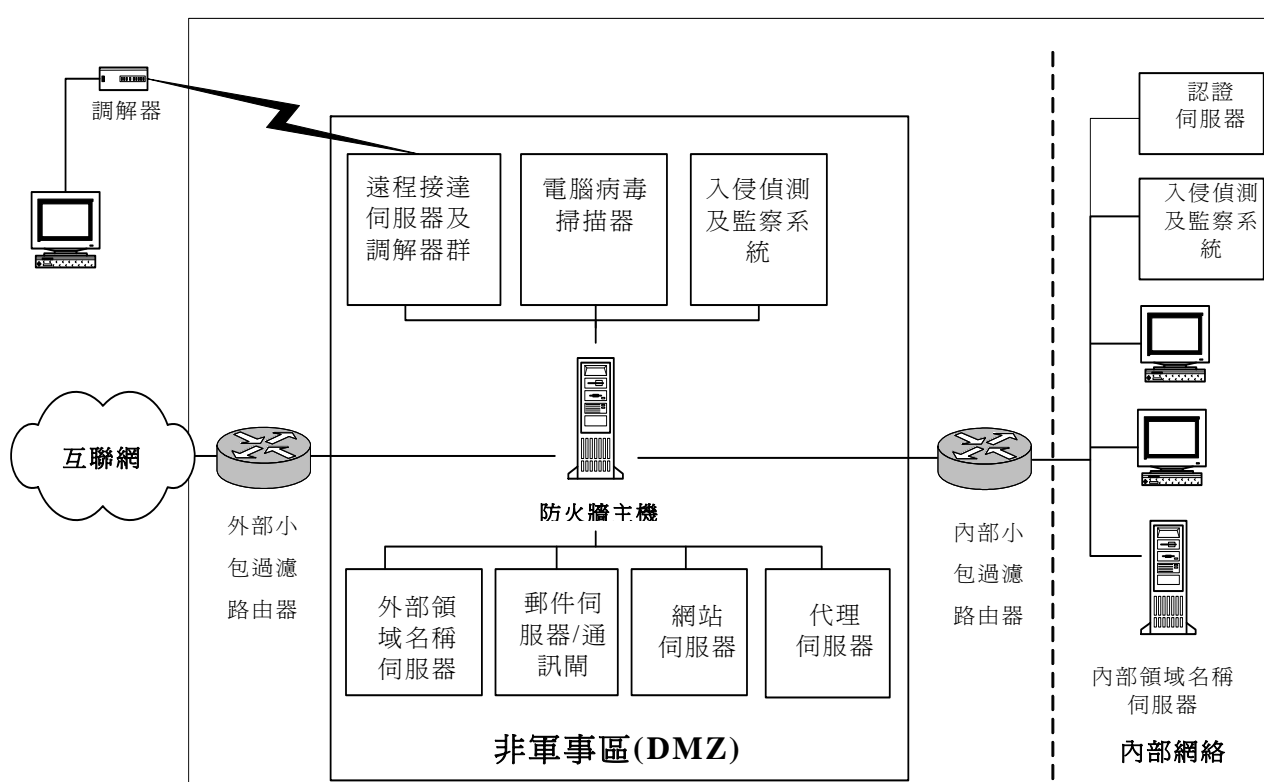


圖 2 — 具備非軍事區(DMZ)的互聯網通訊閘示例

網絡架構應保留防火牆系統、入侵偵測機制和電腦病毒掃描工具，為互聯網接達服務提供保安保護措施。因應通訊閘所提供的服務，可考慮納入下列網絡設備：

- 認證伺服器（用戶識別及接達控制）
- 遠程接達伺服器及調解器群（供遠程撥號接入及接達）
- 領域名稱伺服器（供主機名稱及地址映射）
- 簡單郵遞傳送規約（SMTP）通訊閘及郵件伺服器（供互聯網郵遞）
- 網站伺服器（供發佈資訊）
- 代理伺服器（供快取記憶、隱藏網址、接達控制）

下文將闡述適用於上述各構件的保安指引，以強調這些構件所需要的保安措施。

互聯網通訊閘架構可將內部網絡與外部網絡隔開，從而隱藏有關內部網絡的資料。非軍事區內可劃分個別的區段，以實施更有效的接達控制和保護。

事實上，提供不同服務的互聯網通訊閘架構都須要因應網絡基建、所提供的服務、性能、操作模式、成本等多種因素作出特定的調整。

### 5.3.1 網站伺服器

- 如須向內部和外部用戶提供不同資料，便應使用不同的網站伺服器以限制接達。
- 網站伺服器可置於內部網絡裏面或外面。放置在內部網絡裏面的網站伺服器一般用來向內部用戶提供資料，而放置在內部網絡外面的伺服器則用來向公眾或外部用戶發佈資料。所有放置在內部網絡外面的網站伺服器須與非軍事區內的防火牆連接，以隔開網絡界面。
- 網站伺服器、郵件伺服器或任何關鍵服務均應使用專用主機，以備一旦遭受攻擊，可減輕對其他服務的影響。

### 5.3.2 領域名稱伺服器

- 儲存在外部領域名稱伺服器中的所有主機名稱和網址，原則上可向公眾公開。因此，外部領域名稱伺服器不應儲存與內部網絡相關的任何資料。外部領域名稱伺服器亦可由互聯網服務供應商託管。
- 不應在互聯網披露內部領域資料，應儲存在內部設置的獨立領域名稱伺服器，並放置在內部網絡內。

### 5.3.3 入侵偵測及監察

如上所述，入侵偵測及監察功能可以以人手或一些自動操作的入侵偵測系統工具執行。如選擇以人手執行，必須妥善備存、覆檢和分析所有關鍵構件的系統及應用系統記錄。應適當地制訂及遵從覆檢和監察程序。

如選擇自動操作模式，可使用網絡入侵偵測系統或入侵防禦系統。

入侵偵測系統監聽及檢查網絡內部的小包，以被動的方式監察網絡通訊，並將已知的攻擊活動識別碼與通訊模式作比較，在比對吻合時發出警報。

入侵防禦系統較入侵偵測系統更積極阻截外來入侵，因為此系統可予以配置以發現及阻止損毀或刪除目標系統數據的入侵。與防火牆類似，入侵防禦系統可阻截及傳送小包，從而即時阻止攻擊。

這些基於網絡或主機的工具可偵測任何可疑的活動，並監察網絡通訊或系統活動。下文列出設置入侵偵測系統的一些建議：

- 入侵偵測系統／入侵防禦系統應置於非軍事區內，以偵測外來攻擊。額外的入侵偵測系統／入侵防禦系統可設置於內部網絡內，以在有需要時偵測內部攻擊。
- 應儘可能隱蔽入侵偵測系統／入侵防禦系統的運作。防火牆系統應掩護和保護入侵偵測系統／入侵防禦系統，以防止該系統受到攻擊。
- 不應單單依賴入侵偵測系統／入侵防禦系統保護網絡。入侵偵測系統／入侵防禦系統只是在發生異常或可疑活動時向用戶發出警報的實時偵測工具。最重要的措施仍是適當地配置網絡，並確保已採取所需的保安機制。此外，亦應密切監察及定期覆檢整個網絡，以儘早發現保安漏洞或配置不當之處。

#### 5.3.4 防火牆

根據用戶的保安要求，串列使用兩部或以上的防火牆或路由器有助加強防衛水平。舉例來說，兩部串列的防火牆（一部內部連接內部路由器，另一部則外部連接外部路由器）可提供不同的保護措施。如果有一部遠程接達伺服器與非軍事區連接，並設置於內部及外部防火牆之間，外部防火牆可用來堵截互聯網用戶的通訊，而內部防火牆則可堵截內部網絡用戶及遠程接達伺服器的遠程接達用戶的通訊。

如果是出於平衡負荷或性能的理由而平行使用多部防火牆，各部防火牆的配置必須互相配合。

#### 5.3.5 防範電腦病毒及惡意程式碼

- 應設置獨立主機與防火牆連接，以便在數據經過防火牆時，檢驗其中是否存有任何電腦病毒及惡意程式碼。此配置可中央控制個別電腦病毒及／或惡意程式碼的識別碼的更新，以防電腦病毒或惡意程式碼進入網站或郵件伺服器。
- 可在不同的位置（如郵件伺服器或網站伺服器）安裝抗電腦病毒及惡意程式碼偵測及修復軟件。
- 安裝抗電腦病毒軟件或惡意程式碼偵測及修復軟件的位置取決於網絡性能、須予防範的電腦病毒／惡意程式碼及須達到的防範水平等多個因素。在大多數情況下，因許多電腦病毒／惡意程式碼都是以電郵附件的形式入侵系統，因此郵件伺服器應裝入抗電腦病毒軟件或惡意程式碼偵測及修復軟件。

#### 5.3.6 遠程接達伺服器及調解器群

遠程接達伺服器是支援遠程或流動資訊處理的特定網絡互連設備。

- 獲授權用戶希望能夠使用撥號功能，即在沒有互聯網上網設備的情況下，遠距離登上互聯網。這種功能可能存在保安漏洞，所以實施和管理相關的服務，必須加倍小心。
- 宜採用中央調解器群，以達到方便管理及有效控制的目的。
- 應運用認證機制控制遠程或撥號接達。

### 5.3.7 代理伺服器

代理伺服器是指運行簡單程式或程序檢驗小包的伺服器。代理伺服器一般被視為加強性能的設備，為內部網絡用戶提供增值保安服務。代理伺服器擔當了在通訊兩方（例如客戶和伺服器）之間調解通訊及確定通訊方向的中介角色。換言之，各方均與代理伺服器通訊，而不是直接與另一方連接。至於代理伺服器的配置，除只應提供已獲授權的服務外，亦應限制用戶接達未經授權之目的地。代理伺服器還提供其他支援服務，例如快取記憶最近登入的網頁、接達控制、記錄、內容過濾，甚至是隱藏網址。

圖 2 所示的代理伺服器協助內部用戶控制互聯網接達。

部分防火牆可加強代理伺服器最常提供的服務，例如 TELNET、檔案傳送規約（FTP）、超文本傳輸規約（HTTP）及簡單郵遞傳送規約（SMTP），以防止未經過應用系統層調解的通訊穿過防火牆。

### 5.3.8 認證伺服器

防火牆和代理伺服器在某程度上具備用戶身分鑑定功能。用戶還可考慮使用被稱為「認證伺服器」的中央數據庫，以作中央記錄及儲存鑑定用戶身分及授權用戶所需的所有資料，例如用戶密碼和接達權限。此外，這些認證伺服器還支援更有效的認證模式，例如運用權標、智能卡等，而代理伺服器不一定支援這些認證模式。

舉例來說，遠程接達撥號用戶服務（RADIUS）和終端機存取控制器控制系統（TACACS+）是常見的遠程認證模式。圖 2 所示的認證伺服器可在遠程撥號用戶獲授權接達網絡前，用來鑑定遠程撥號用戶的身分。

- 儲存在認證數據庫內的資料應經過加密，而且應受到嚴密保護，以免被未獲授權接達或竄改。
- 應使用獨立及專用的電腦，並將此機放置在安全的地方。
- 應適當配置伺服器，以記錄管理事項、帳戶使用資料及認證事項，例如錯誤的登入。
- 如果使用一部或以上的認證伺服器如用以作備用，應確保儲存在認證數據庫內的資料已傳送到所有其他備用伺服器。
- 應定期審閱系統記錄檔案以發現任何未獲授權建立帳戶或權限修改。

在制定電子政府服務的電子認證要求時，政策局／部門亦應遵從《電子認證風險評估參考架構》的指引。該參考架構旨在提供一個統一的方法給政策局

---

／部門在制定其電子政府服務的認證方法時作為參考，務求令市民／僱員於使用有類似認證要求的電子政府服務時會有一致的經驗及介面。有關該架構的詳細資料，請參閱「電子認證架構」主題專頁。

## 6. 防火牆

防火牆可視為防止入侵者侵入，以保護機構資源的保安措施。防火牆是保安基礎設施的重要部分。在探討防火牆的設計前，須徹底了解防火牆的特點、功能、限制，以及與傳輸控制規約／聯網規約相關的保安威脅和漏洞。

防火牆應安裝在內部網絡（例如部門網絡）與外部網絡（例如互聯網）之間的所有網絡接口，以及須檢驗、限制、過濾或重新引導數據流的任何網絡點。

市場上提供多種防火牆產品。在選擇防火牆產品時，應考慮以下主要標準：

- 產品功能
- 性能／處理能力
- 與現有網絡的互用性
- 可靠性
- 備用支援能力
- 管理的便利程度
- 供應商的支援
- 產品核證(例如 EAL)
- 認證服務的支援(例如遠程接達撥號用戶服務)
- 系統容量
- 記錄
- 價格
- 客戶參考
- 所需的技術人員
- 保安要求

最為重要的，仍是適當配置及管理防火牆。

### 6.1 防火牆配置

防火牆須經適當配置，以過濾通訊、轉換 IP 地址、控制接達和過濾數據內容。防火牆配置不當或有誤可能導致保安錯覺，而保安錯覺比沒有設置防火牆更為危險。

以下列舉一些配置防火牆時應注意的事項，以供參考：

- 必須以防火牆為進出互聯網的唯一通道，強制所有傳入及發出的互聯網通訊經過防火牆。
- 從保守的防火牆保安政策做起，即「除明確獲准的服務外，拒絕所有服務」。用戶不宜盲目遵從防火牆預設的設定。
- 審慎規劃和評估獲准經過防火牆的所有服務。
- 配置防火牆時應啟動網路位址轉換，儘可能隱藏地址等內部網絡資料。
- 配置防火牆時應啟動掃描通訊內容、電腦病毒及惡意程式碼的功能。

- 必須適當配置防火牆，以使用互聯網規約層的過濾功能。
- 配置防火牆時應堵截不使用的埠和過濾不必要的通訊，例如不需要的傳入或發出的互聯網控制信息規約(ICMP)通訊。
- 必須確保防火牆本身的實體安全。
- 防火牆政策必須富彈性，以配合未來發展和適應保安要求的改變。
- 正確設定和編配防火牆檔案權限。必須儘可能限制系統檔案權限。
- 必須徹底測試防火牆，在投入運作前必須適當地檢驗防火牆配置。
- 在防火牆每次重大改動或升級後，必須進行測試。
- 在必要時，容許內部部門網絡內發出的 FTP 或 TELNET 可經過防火牆進入互聯網。
- 定期以修補程式和錯誤修補程式修改及更新在防火牆安裝的所有軟件，以確保使用的軟件版本恰當。
- 必須為緊急事故設定實時警報機制。

## 6.2 防火牆管理

- 應妥善記錄防火牆配置、管理及操作程序。
- 平行使用多部防火牆的配置必須完全一致。
- 在可行的情況下，應以檢驗和檢查防火牆配置檔案的完整性。
- 應定期記錄及覆檢防火牆的記錄。
- 為防火牆系統和配置檔案備份。
- 妥善備存用戶帳目十分重要。只有防火牆管理員和備份管理員可獲發防火牆用戶帳目。對操作人員應實施嚴格的接達控制，操作人員只可操作履行職務的必要功能。
- 為防火牆管理員提供持續培訓亦至關重要。
- 應指派至少兩名防火牆管理員（一名專責管理員，另一名為輔助管理員）維持防火牆的運作。
- 防火牆管理在保安事故處理中應佔一席位。
- 如果由不同的人擔任局部區域網絡管理員和防火牆管理員，兩者之間應建立有效的溝通渠道。
- 定期進行防火牆審計。主機系統亦應定期進行掃描和檢查，以偵測常見的配置漏洞和錯誤。

## 7. 路由器

路由器最常用來連接兩個或以上的網絡。路由器可過濾通訊，並限制接達到伺服器或網絡構件，例如應用系統代理伺服器。

在配置及管理網絡路由器時，應遵守以下指引：

- 與防火牆類似，路由器亦應妥善配置，除明確獲准的服務外，拒絕所有服務。應關閉源路由功能。
- 如同防火牆的配置及管理一般，應妥善進行記錄、備份和其他管理工作。
- 在實際運作前應進行徹底測試。
- 如果路由器與防火牆一併使用，則路由器應符合防火牆政策。

## 8. 郵件通訊閘保安

建立安全的郵件通訊閘，應遵守和遵從下列指引。

### 8.1 郵件伺服器設計及配置

- 郵件伺服器應由防火牆系統作掩護，防火牆系統可以限制對郵件伺服器的接達，並提供各種保安保護措施。
- 適當配置防火牆或路由器，以攔截不必要的通訊（例如由某個已知濫發電郵者的 IP 地址所發出的通訊）進入郵件伺服器或通訊閘。
- 電郵系統只應提供能夠從外部接達的電郵地址，而不應包含內部網絡或系統的名稱或 IP 地址。
- 如技術上和運作上可行，電郵的標題應避免透露一些內部系統及配置的資料，以防止系統資料外泄。
- 內部電郵地址目錄不應對外公開。
- 郵件通訊閘應具備龐大和足夠的記錄功能，以記錄交換電郵事項作審計之用。郵件通訊閘應提供電郵如何、何時及何地寄入或發出等資料。
- 如發現有任何電郵轟炸或濫發電郵等情況，應嘗試找出電郵的來源或真正源頭，然後配置路由器或防火牆，以防止進一步發生電郵轟炸或濫發電郵情況。
- 應關閉為未獲授權用戶傳遞郵件功能。

### 8.2 電郵轟炸、濫發電郵及電郵仿冒

電郵轟炸是指向某個電郵地址發出相同的電郵。濫發電郵是指向無數不希望收到電郵的用戶發出電郵，以致互聯網因不必要的垃圾電郵泛濫而癱瘓。

電郵轟炸和濫發電郵都能夠劫持毫無防範的郵件伺服器，並利用這些伺服器進一步傳播電郵。這些被劫持的郵件伺服器充當了第三者郵件傳遞，為非局部用戶（不論是作為發件人，或是收件人）處理電郵，從而導致電郵仿冒。

郵件伺服器如未能適當配置，把第三方電郵傳遞功能關閉，伺服器便可能受到上述電郵攻擊。電郵系統的所有資源被濫發電郵者竊取後，可能因而癱瘓、超負荷，甚至遺失資料。復原正常服務的代價可能十分高昂。

受到電郵攻擊的跡象如下：

- 拒絕服務，例如磁碟已滿或系統關閉
- 在極短時間內，由同一發件人發出大量寄入／發出的電郵
- 從失效的來源地址收取大量寄入電郵或向無法回覆的地址發出大量電郵
- 由已知的濫發電郵者寄入／發出的電郵
- 聲稱由管理員發出，要求用戶寄出其密碼或其他敏感資料複本的電郵
- 要求用戶將密碼改為某指定值或字串的電郵

- 引導接收者至看似合法機構的欺詐性網站，以欺騙用戶提供個人身分資料及私人資料（例如信用卡資料）。

以下是防範電郵轟炸、濫發電郵及電郵仿冒的一些提示：

- 移除不用的電郵伺服器程式，例如 `sendmail`；如果需要使用這些程式，應確保使用最新的版本。
- 開啓記錄功能，以記錄及偵測任何可疑的活動，例如留意同一名寄件人在極短時間內寄入／發出大量電郵，或記錄仿冒電郵訊息的寄件人資料和標題。使用入侵偵測系統工具是有助偵測電郵轟炸的另一個辦法。
- 適當配置防火牆和路由器，限定外來的簡單電子郵件傳輸協定（SMTP）連接只能接到一台指定的郵件閘道或伺服器，以集中記錄和通訊控制。
- 必須堵截來至未獲授權或不存在的網址使用郵件傳遞，例如郵件伺服器只容許一些指定的內部 IP 地址或已獲授權內部用戶使用郵件傳遞，但外部用戶除外。
- 必須適當地配置電郵伺服器程式或電郵傳遞軟件所配備的過濾無效訊息功能。此功能可阻擋一些未獲授權網址所發出的電郵，或一些沒有有效「寄件人」或「收件人」地址的電郵、沒有有效回郵地址的郵件，以及由已知濫發電郵者發出的垃圾郵件。
- 限定每個電郵郵件大小上限，或可傳遞郵件數量上限，以免網絡資源或磁碟容量因電郵泛濫而癱瘓。
- 定期更新濫發電郵者名單。
- 在電郵伺服器與互聯網連接之間設置濫發電郵阻截系統，藉以過濾不必要的電郵。此濫發電郵阻截系統可發揮郵件通訊閘的功能，按照多項標準(例如電郵標題、內容、濫發電郵黑名單、濫發電郵白名單及反向領域名稱系統查詢等)在電郵進入電郵伺服器之前篩除濫發電郵。

### 8.3 接達控制

- 只有獲授權的用戶可使用電郵服務。
- 利用密碼或數碼簽署等認證模式以認證電郵，數碼簽署在傳遞電郵過程中可確保郵件的來源和完整性。
- 限制獲准連接電郵伺服器的用戶人數。
- 郵件只可儲存在具有適當接達控制及安全的目錄。小心處理郵件，確保其保密性。

## 9. 網站保安

網站保安是保護網站伺服器、網站用戶及內部網絡的一系列程序、作業實務和技術。網站伺服器及其組件如網站伺服器操作系統、網絡、應用程式／軟件等，以及儲存於網站內的資料都很容易招致攻擊。

由於網站伺服器完全暴露於互聯網，所以必須採取嚴密的主機和網絡保安防護措施。本節所述的網站保安指引，應予嚴格遵守和遵從。

### 9.1 網站伺服器配置及管理

網站伺服器軟件是在主機系統上運作，向用戶提供資料的應用程式，網站伺服器往往與互聯網連接。設計和配置對架設一個安全的網站伺服器，至為重要。

- 如果在非軍事區內提供郵件通訊閘服務，應配置網站伺服器使其不能提供任何簡單郵遞傳送規約（SMTP）服務，以免外部用戶利用網站伺服器傳遞郵件。
- 不應以管理員、超級用戶或「根」權限運行任何伺服器軟件和應用程式。所有伺服器軟件和應用程式的運行必須符合「最小權限」原則。
- 為網站伺服器內的目錄、檔案和網頁制訂適當的接達權限。
- 除超文本傳輸規約（HTTP）外，原則上禁止在網站伺服器運行任何網絡服務、應用程式或互聯網規約。如確有需要，應取得明文批准。
- 禁止在網站伺服器運行其他服務，例如郵件傳遞。
- 考慮關閉任何源自伺服器端有潛在危險的可執行程式碼，例如 Cookie 和微應用程式。
- 在可行的情況下，為網站伺服器另行開立獨立的工作目錄，以便在執行檔案時建立工作檔案。
- 網站伺服器管理工具只限在獲授權系統成功通過認證程序的獲授權管理員接達。重要的配置檔案只限管理員負責更新。
- 作為日常例行工作，應密切監察網站的完整性和可用性。管理員應利用系統實用程式、入侵偵測系統或入侵防禦系統，以掌握未獲授權竄改或接達的最新情況。
- 停用所有不使用的帳戶，包括用戶帳戶和預設帳戶。
- 移除網站伺服器軟件上的所有預設檔案或示範檔案。
- 對網路爬蟲程式施加限制，以免公眾搜尋器搜尋到和儲存不打算公開的內容。
- 定期更換這些管理工具的認證密碼，並禁止重覆使用相同的密碼。不要使用這些管理工具的預設密碼。

### 9.2 接達控制

- 為防止互聯網規約（IP）仿冒攻擊，應一併使用 IP 地址限制和用戶身分鑑定功能。

- 禁止匿名或未獲授權用戶更新目錄或數據檔案。
- 除已登記用戶外，其他人並無接達權限。可供登入伺服器的帳戶數目應予限制。很少使用服務的用戶應予刪除。
- 關閉所有不必要的帳戶，尤其是訪客帳戶。
- 閱讀記錄必須符合適當的管理程序／帳戶。
- 必要時可採取強化的加密和認證措施，保護儲存在外部網站伺服器的資料。

### 9.3 網站內容管理

- 在實際運作前徹底測試和檢查所有網站和網頁。
- 應實施控制以確保除獲委託及獲授權人士外，其他人無權在生產環境張貼和更新網頁。
- 如果不同的組別，甚至不同部門須共用網站伺服器，各組別、部門應使用不同的網站內容目錄或子目錄，這些目錄必須實施嚴格的接達控制，以限制接達、執行和儲存有關的網站應用程式。
- 網站應用程式不得設置通往儲存於指定網站目錄以外內部檔案的連結。
- 不得授權網站內容開發人員管理操作系統和網站伺服器。
- 為在網站伺服器張貼或更新網頁和應用程式，制定網站內容管理程序。
- 至於那些接受用戶數據輸入的網頁表單或應用系統，所有輸入的數據在進入後端應用系統前，必須先進行適當的核對及驗證，使任何預期以外的輸入都能被妥善地處理，不會成為攻擊應用系統的途徑。預期以外的輸入驗證包括過於長的輸入、不正確的數據種類、以及預期以外的負數、數據範圍或字符，如那些被應用系統用作分隔所輸入的字符串的字符。
- 須移除生產伺服器內不需要的內容，如顯示於系統橫幅的平台資料、說明數據庫、聯機軟件手冊及預設或示範檔案等，以免在不必要情況下披露系統資料。

### 9.4 共用網間連接界面腳本及應用程式界面程式

共用網間連接界面腳本（CGI Scripts）及應用程式界面程式（API Programs）常用來擴充網站伺服器，以加強性能。與網站伺服器一併供應的預設共用網間連接界面腳本可能在無意中提供了接達網站內容（包括電郵檔案）的「後門」。腳本可有意無意洩漏有關主機系統的資料，而且很容易招致攻擊。此外，共用網間連接界面腳本往往允許用戶輸入數據。

為加強保安，應遵守和遵從的項目如下：

- 適當設計、測試和檢查共用網間連接界面腳本和應用程式界面程式，確保腳本和應用程式界面程式只能夠提供所需的功能。除非預設或特製共用網間連接界面腳本已經過徹底測試和驗證，否則不得保留在伺服器內。
- 應在受限制的環境（例如在單一獨立目錄）中運行及儲存這些程式，以限制接達，同時可便於進行維修。

- 共用網間連接界面腳本只可獲授權執行，但並無閱讀或寫入權限。對系統資源的使用應予限制，例如中央處理器時間、超時時間和磁碟使用情況。適當限制共用網間連接界面腳本接達其他數據檔案或資料。
- 編譯程式、解譯程式、介殼程式及腳本引擎等程式不應放置在共用網間連接界面腳本內。這些程式應安全地放置在適當的目錄，如果不再需要這些程式，應徹底將程式從網站伺服器移除。
- 若用戶所輸入這些共用網間連接界面腳本的數據可能用於指令行功能，應在傳送到伺服器軟件或相關操作系統前適當地檢查。

## 9.5 認證

- 在可行的情況下，遠程管理控制應採用數碼證書、智能卡和權標等強化認證模式，這些強化認證模式亦可用於關鍵應用系統、伺服器和客戶的認證和識別程序。
- 可考慮在傳輸重要資料時，採用保密插口層（SSL）連接或安全超文本傳輸規約。

## 9.6 網路瀏覽器

應適當地配置網路瀏覽器。以下是配置網路瀏覽器的一些建議：

- 應通過獲授權通訊渠道，例如互聯網通訊閘接達互聯網。
- 最有效的方法是關閉電郵應用系統／瀏覽器的啓動動態內容的任何選項，例如 Java、JavaScript 和 ActiveX，與可信賴來源通訊則除外。
- 在開啓任何下載檔案前先行掃描電腦病毒及惡意程式碼。
- 使用最新版本的瀏覽器，並採用最新的保安修補程式。
- 關閉自動輸入密碼／密碼記憶功能。
- 除非所連接的網站可信賴，否則須啓動攔截彈出視窗功能。
- 定期移除瀏覽器內的快取檔案或臨時檔案，以保障資料私隱。
- 關閉自動安裝插件、附加程式或軟件的功能。

## 9.7 主動式內容及COOKIE

主動式內容使提供資訊的伺服器能夠裁製在用戶端瀏覽器顯示的執行腳本，例如 Java 微應用程式和 ActiveX。

Cookie 是伺服器與用戶端瀏覽器以無狀態的超文本傳輸規約連接時，用來掌握用戶狀態資料的一種機制。

### 9.7.1 Java微應用程式

Java 微應用程式是通常嵌入網站內超文本標示語言網頁的程式。用戶端的瀏覽器可能會自動下載 Java 微應用程式以便執行，但 Java 系統並不提供審計功能，而

且其中更存在不少保安漏洞。舉例來說，雖然 Java 限制其微應用程式只可進行一部分安全操作，使這些微應用程式無法破壞檔案系統或電腦的開機磁區，但 Java 對可用性攻擊的防備卻極度不足。在發展 Java 微應用程式時，發展人員應限制 Java 微應用程式只可接達指定的目錄、檔案和操作系統。

在用戶端運行 Java 微應用程式時，亦應考慮以下事項：

- 收緊對 Java 編譯程式、解譯程式及生成程式的保安控制。
- 了解有關 Java 微應用程式保安漏洞的最新資料，並採用最新的修補程式。
- 如若無需運行 Java 微應用程式，在瀏覽器選擇「關閉 Java」功能，禁止在電腦系統上運行 Java 微應用程式。

### 9.7.2 ActiveX

ActiveX 是軟件下載和執行所發展的軟件控件。ActiveX 控件編譯成在各個操作系統上執行，並嵌入在網頁內，但對於 ActiveX 所能夠進行的操作卻並無限制。ActiveX 控件可留駐在系統，甚至刪除數據或寫入本機硬磁碟。而且瀏覽器也無法記錄這些控件在用戶端電腦進行過的操作。

軟件編寫者可於 ActiveX 控件採用已取得核證機關認證的數碼簽署技術。這樣，用戶可在決定接受還是拒絕控件前根據編寫者身分檢驗簽署。

所以 ActiveX 的保安有賴於用戶的個人判斷。數碼簽署只能夠顯示 ActiveX 控件由何人編寫，但不能協助用戶決定控件是否可以信賴。用戶應認真考慮，而且只接受來自可信賴來源的控件。

### 9.7.3 Cookie

Cookie 是用於伺服器上的機制，可將資料儲存在用戶端以供伺服器提取。Cookie 向伺服器提供如網址、用戶電郵地址和資料等用戶狀態資料。攻擊者可仿冒伺服器接收來自客戶的 Cookie。

系統發展人員應注意讓 Cookie 儲存過多私人資料並不恰當。應儘可能避免在 Cookie 儲存純文本的用戶名稱和密碼。如果 Cookie 必須儲存認證資料，應對整個 Cookie 進行加密。系統設計人員還可加入一些控制資料，例如到期日、限制 Cookie 有效期的時間，以減低 Cookie 的潛在危害。

## 10. 遠程接達伺服器及調解器群

遠程接達是指在沒有直接連接網絡的遠程地點使用網絡資源。遠程接達有很多不同的方式。最常見的方式是使用兩部調解器和一條通訊鏈路將遠程用戶的個人電腦與網絡連接。因此，在遠程接達過程中有三方面需要保護：即遠程用戶、網絡資源和通訊鏈路。

- 明確制訂和設計規劃哪些用戶可獲准使用遠程接達服務，以及向這些用戶提供哪些服務。
- 只有明確獲授權的用戶可遠程接達網絡。
- 適當配置防火牆系統，以限制遠程接達。
- 確保遠程接達伺服器和調解器群的實體安全。
- 必須利用認證機制識別遠程接達用戶。
- 在進行遠程登入時，不應以純文字形式傳輸用戶名稱和密碼。
- 應以日誌記錄遠程接達伺服器的運作，例如記錄開始及結束登入狀態、開始及結束連接時間，以及在遠程接達伺服器加入或刪除用戶帳戶。
- 在可行的情況下，應運用加密保護在這些鏈路傳輸的數據。
- 攻擊者重覆撥號也可能令撥號服務陷於癱瘓。超時時間計時器或撥號時間上限可限制供用戶使用的資源，從而減低服務癱瘓的機會。

## 11. 領域名稱伺服器

領域名稱系統（DNS）提供領域名稱與 IP 地址映射的支援。領域名稱系統可提供不同資料，例如在指定領域內所有主機的 IP 地址清單、IP 地址轉為主機名稱的映射及用戶電郵地址等。如果領域名稱伺服器被破解或仿冒，儲存在領域名稱伺服器的資料便會失效。

為保障領域名稱伺服器的安全，應遵守和遵從下列指引：

- 使用最新的領域名稱系統版本或服務套裝軟件。
- 對領域名稱系統採取保安保護措施，例如收緊領域名稱系統數據庫檔案的接達權限，使用強化加密系統。
- 在可能的情況下，配置領域名稱伺服器，使伺服器為每一名客戶進行額外的領域名稱系統查詢，例如在 IP 地址轉換為主機名稱後，然後再將主機名稱換回 IP 地址，作為覆檢。
- 記錄 IP 地址的賦值資料，例如主機位置和主機資料。這些記錄可作為領域名稱伺服器遭攻擊時的備份、檢驗和審計清單。

## 12. 入侵偵測及監察

要維持互聯網通訊閘的安全，需要持續及全面的系統操作、支援和監察，以對不當、異常或可疑的活動或事故，作出防範、偵測、應變和升級處理。通過適當的人手操作程序，如覆檢和分析記錄，並在已覆檢的記錄或統計數字上簽名，便可達到上述目的。

在可能的情況下，可在策略性位置使用及安裝入侵偵測系統工具，不斷收集及檢查可疑活動的資料。應一併使用基於網絡和基於主機的入侵偵測系統工具。前者負責檢查在網絡傳輸的網絡小包，後者則負責偵測主機操作系統。

**不當配置和使用不當工具可導致向攻擊者泄露資料，並造成安全假象。**

- 使用入侵偵測系統工具鑑別網絡和主機的可疑活動，尤其是網站伺服器和郵件伺服器。
- 設置由電郵或流動傳呼自動發出警告或警報的功能，在偵測到攻擊跡象時向系統管理員發出警報。
- 在可行的情況下，採用能夠針對可疑網絡活動作出應變的精密系統或功能，以中斷或堵截可疑網絡活動的連接，並作記錄以供事後分析。
- 在使用入侵偵測工具前必須適當地測試和檢驗這些工具。
- 妥善控制和限制入侵偵測工具的使用和管理。
- 適當配置防火牆系統，儘可能保護和隱藏這些工具。
- 確保使用最新的入侵識別數據和攻擊識別碼檔案。
- 就使用入侵偵測工具制訂適當的操作、管理和監察程序。

## 13. 其他保安考慮事項

除上述特定的網絡構件外，任何網絡構件都可能涉及保安問題而須予以一般性的考慮。

政府資訊科技總監辦公室文件《資訊科技保安指引》(G3) 為整體保安考慮事項提供了較詳盡的資料，以下探討其中的一些相關內容。

### 13.1 實體保安

- 確保所有通訊閘構件的實體安全，所有構件應放置在受管制的地點。
- 放置這些設備的電腦室必須具備完善的設施，以防範實體或自然災害。
- 使用可上鎖的儲物架，以存放這些構件。
- 定期監察及覆檢現有的實體保安情況，例如檢查場地的出入口或接達記錄、檢查是否有任何未獲授權竊聽線路、檢查儲物架的門鎖和粘貼標籤。
- 在棄置儲存媒體前，移除及刪除所有資料，尤其是有關系統配置的資料。

### 13.2 記錄

- 在可行的情況下，應開啓防火牆、路由器、操作系統、網站伺服器 and 郵件伺服器的記錄功能。
- 備存誤差記錄、系統記錄、接達記錄、網站伺服器記錄和郵件伺服器記錄。應設法記錄以下資料，例如無效帳戶登入、在網站進行濫用、非法或未獲授權活動、向用戶提供的互聯網規約服務、管理行動、更新配置行動或具體資料要求（例如資料要求者的 IP 地址、主機名稱、URL 以及接達檔案的名稱）。
- 定期覆檢記錄，並將記錄存放在安全的地方不少於一星期。可使用唯讀光碟或磁帶等一次性寫入設備記錄這些檔案。
- 永久保留載有入侵和攻擊資料的記錄，以供調查和記錄。
- 在設計記錄功能前應考慮私隱權問題。

### 13.3 備份及復原

- 制訂並妥善記錄正式的備份及復原程序。
- 應定期為所有通訊閘構件的配置、記錄檔案、系統檔案、程式、數據和系統的其他資料作備份。若有需要或在更改配置時，亦要為這些資料作備份。必要時可將備份資料加密。
- 備份複本應存放在安全的地方。系統配置宜備存兩份備份複本，一份放置於場內，另一份則存放在場外。

### 13.4 防範電腦病毒及惡意程式碼

- 安裝聯機抗電腦病毒軟件，不斷對經過防火牆或個別資料伺服器的檔案、電郵或數據進行實時檢查，並自動清除電腦病毒和惡意程式碼。
- 為使防範工作更有效，安裝內容過濾及／或惡意程式碼偵測及修復軟件，以掃描所有輸入或輸出信息／檔案是否含有惡意內容。配置通訊閘時應過濾含有惡意內容的信息或檔案，隔離／刪除有關信息／檔案，並建立審計記錄以供日後參考。
- 應定期更新電腦病毒識別碼及惡意程式碼定義。宜配置為自動更新，且至少應每日更新一次。
- 倘若無法進行自動更新（例如並非經常接達網絡的流動電腦），則至少須每週手動更新一次。
- 用戶亦須注意，突發性及嚴重的電腦病毒會不時爆發。如果發生上述情況，用戶應遵循有關指示，並即時更新最新的病毒識別碼及惡意程式碼定義，以防範電腦病毒爆發。
- 定期為安裝資料伺服器的主機進行電腦病毒及惡意程式碼掃描。

### 13.5 操作系統保安

由於網絡應用軟件均在操作系統上運作，所以選擇操作系統時必須慎重考慮保安要求。保安漏洞往往源自操作系統的漏洞，而不是應用軟件的問題。

在選擇操作系統時，尤其是防火牆和關鍵伺服器，應挑選安全的操作系統平台。在各種操作系統中，宜選擇具備下列功能的操作系統：

- 多重同步程序
- 安全檔案接達權限和控制
- 能否追究用戶和系統行動的責任，並對此進行審計，例如具備詳盡的事件記錄
- 對系統的所有用戶進行識別和認證
- 資源隔壁，例如控制重新使用系統物件（已刪除的檔案、配置記憶）

不同的操作系統有不同的方式令配置更為安全。以下所列舉的示例可供一般操作系統參考。

- 移除或關閉所有非必要服務或程序，尤其是不再使用的預設操作服務和程序。
- 在可能的情況下移除非必要預設帳戶，或以強化密碼作為所有預設帳戶的密碼。
- 高權限操作程序的數目應減至最低。嚴格分配操作權限。
- 為預設檔案權限設定限定預設值。
- 系統管理員帳戶應儘可能使用難以猜測的名稱，避免使用“Administrator”或“Root”。
- 規範操作系統版本和軟件，並將操作系統版本和軟件的數目減到最低，以便安裝和維修。

- 定期安裝操作系統更新程式，並採用最新的操作系統修補程式，尤其是與保安問題相關的修補程式。

## 13.6 保安審計

應定期、在重大變更後及運作前進行保安審計。保安審計宜每年進行一次。保安審計的目的在於覆檢現行的保安措施、找出任何潛在的保安漏洞，並確保目前的保安保護機制符合現行的保安政策。

保安審計可以是對現行保安政策的一般覆檢，也可以是利用各種保安評估工具進行的技術覆檢。這些工具可用來掃描主機系統和網絡，以找出保安漏洞。在使用這些工具時應保持審慎態度。

- 明確界定審計範圍和目標，確保審計已涵蓋所有目標網絡構件。
- 在運作前必須進行技術審計覆檢。通訊閘內的各個主機都需要進行基於主機的掃描，尤其是操作服務和檔案權限。
- 徹底審計防火牆政策的規則及獲准的服務。
- 檢查密碼機制。
- 從網絡構件移除審計測試結果和數據，有關結果和數據必須存放在安全的地方。
- 必須控制掃描工具的使用，以防止未獲授權人士使用。
- 儘快處理審計建議。

## 13.7 系統管理及操作

- 因應人員調遷離職等情況妥善管理及備存用戶帳戶。
- 未經部門主管正式批准，禁止用戶或人員安裝或運作外部網站伺服器、郵件伺服器或防火牆以接達互聯網。
- 明確界定和分派全體系統管理人員的職務和職責。
- 應妥善制訂互聯網通訊閘程序，並嚴格遵守有關程序，例如更改管理控制程序（尤其是防火牆）、備份及復原程序、系統構件配置程序、網站內容管理程序和其他相關程序。
- 必須在主機安裝和運作安全版本的程式或軟件，並安裝修補程式或更新程式。
- 關鍵構件應由局部連接的終端機直接管理，或採用權標、智能卡、質疑／應答或一次性密碼等強化認證工具。
- 定期檢查聯機保安訊息或檔案，例如技術建議和保安事故或漏洞。
- 覆檢和修改配置，以適應更改要求、保安威脅或漏洞等環境轉變。
- 系統所顯示的歡迎登入、問候或錯誤信息可能會泄露系統資料。適當時應關閉這些信息功能。
- 在可能的情況下，安裝管理工具或使用服務，例如使用全場安裝修補程式軟件，集中系統管理和安裝工作。

\*\*\*完\*\*\*

## 附錄 A — 建議就互聯網通訊閘保安採用的保護措施清單

項目	建議的保護措施
防火牆	防火牆配置
	傳入／發出的所有通訊必須經過防火牆
	以「除明確獲准的服務外，拒絕所有服務」的防火牆政策為基礎
	審慎規劃和評估獲准的服務
	開啓網路位址轉換（NAT）功能
	開啓內容過濾，電腦病毒及惡意程式碼掃描功能
	適當配置 IP 層過濾
	制訂富彈性的防火牆政策，以備未來發展
	正確設定和編配防火牆檔案權限
	在運作前和每次重大變更後徹底測試防火牆
	確保防火牆安裝的所有軟件均為恰當版本的軟件
	設定實時警報機制
	如非必要，否則禁止由防火牆所發的 FTP 或 TELNET 通訊傳送到內部網絡
	保障安裝防火牆的操作系統的安全
	防火牆管理
	妥善記錄防火牆配置、管理及操作程序
	平行使用多部防火牆的配置必須完全一致
	檢查配置檔案的完整性，例如運用檢驗和
	定期記錄和覆檢防火牆記錄
定期為系統和配置檔案備份	
妥善備存用戶帳目	
為防火牆管理員提供持續培訓	
指派至少兩名防火牆管理員	
列防火牆管理成為保安事故處理的一部分	
與局部區域網絡管理員之間建立有效的溝通渠道	
定期進行保安審計	
入侵偵測及監察	操作控制
	制訂人手操作控制程序
	定期覆檢及分析記錄
	監察及分析用戶及系統活動
	在覆檢後的記錄上簽署
	入侵偵測系統工具（如已使用）
	網絡和主機都需要使用入侵偵測系統工具，尤其是網站或郵件伺服器

項目	建議的保護措施
	設置自動發出警告或警報功能
	採用能夠針對可疑活動而作出應變的精密功能，例如中斷或堵截連接
	在使用前適當測試和檢驗入侵偵測系統工具
	控制和限制入侵偵測工具的使用
	適當配置防火牆以保護及隱藏這些工具
	確保使用最新的入侵識別數據和攻擊識別碼檔案
	為使用這些工具制定操作、管理及監察程序
<b>防範電腦病毒及惡意程式碼</b>	偵測及防範電腦病毒及惡意程式碼
	安裝抗電腦病毒軟件及內容過濾通訊閘，以掃描所有輸入或輸出信息／檔案是否含有惡意內容。配置通訊閘時應過濾含有惡意內容的信息或檔案，隔離／刪除有關信息／檔案，並建立審計記錄以供日後參考
	定期使用最新的病毒識別碼及／或惡意程式碼定義
	定期進行電腦病毒及／或惡意程式碼掃描
	開發中或用作測試的電腦設備或軟件亦應遵守相關的資訊保安考慮事項及程序
	在電腦接達政府網絡之前，對電腦進行全面掃描
	第三方供應商應在安裝新機、維修服務和安裝軟件後以最新的病毒識別碼進行電腦病毒掃描
<b>保安政策、指引及標準</b>	制訂及執行保安政策
	制訂自身的互聯網通訊閘保安政策
	制訂相關的操作程序，例如更改管理控制程序、備份及復原程序、網站內容管理程序
	制訂保安事故處理和報告程序
	分派和界定系統管理及維修人員的職務和職責
	提醒並教育用戶遵守及遵從政策
<b>保安審計</b>	進行保安審計
	定期（至少每年一次）進行保安審計
	在運作前和重大變更後進行保安審計
	明確界定保安審計的範圍和目標
	由第三者進行保安審計
	審計防火牆政策
	檢查密碼機制
	保障審計結果和數據的安全
	控制對審計工具（如有）的使用
	儘快處理審計建議

