2006 年 3 月 17 日

參考文件

立法會資訊科技及廣播事務委員會

資訊保安

目的

本文件的目的，是就傳媒報道最近有資訊於網上外泄的背景下，向委員會簡述本港資訊保安的現況。

政府就資訊保安所持的立場

2. 政府非常重視資訊保安和保護政府的資訊及電腦資產。在數碼 21 資訊科技策略下，建立一個穩妥的環境，是推動資訊及通訊科技在本港發展的重要一環。政府已就資訊保安採取不同措施，以提高社會各界對進行電子交易的信心，藉以促進電子政府及電子商貿的發展。過去數年，我們推行多項與資訊保安有關的計劃，以建立發展電子商貿所需的公共資訊保安基建，並已取得實質進展。

3. 政府亦以身作則，率先採用國際認同的良好作業模式及標準，以保護內部的資訊系統。此外，政府又透過不同渠道，向工商業及市民大力推廣，以提高社會各界對資訊保安的認知。

香港與資訊保安有關的法律架構

4. 香港有一套全面的法律架構，以防範和處理電腦相關罪行及個人資料的濫用。此架構包括：

(a)《刑事罪行條例》（第 200 章）- 擴大“財產”的含意，以涵蓋電腦所載的任何程式或數據；擴大“對財產的刑事損壞”的含意，以涵蓋不當使用電腦程式數據；

(b) 《電訊條例》（第 106 章）- 禁止藉電訊而在未獲授權下取用電腦資料；

(c) 《盜竊罪條例》（第 210 章）- 擴大“盜竊罪”的含意，以涵蓋非法使電腦作非原來設定的用途及修改、刪除或增加電腦程式或數據；擴大“偽造帳目”的含意，以涵蓋毀壞、塗改、隱瞞或竄改電腦所存的記錄；

(d) 《個人資料（私隱）條例》（第 486 章）- 保護與在世個人相關的個人資料的私隱；適用於規管個人資料收集、儲存、處理或使用，包括電子形式的個人資料；

(e) 《專利條例》（第 514 章）及商標條例（第 43 章） - 就獲認可類別的文學作品、戲劇作品、音樂作品和藝術作品，以及影片、電視廣播、有線傳播節目和互聯網傳送的版權作品，提供全面的保護；以及

(f) 《電子交易條例》(第 553 章) - 爲推動本港電子商務的發展訂立明確的法律架構；賦予電子紀錄及簽署跟對同的紙張文件上的紀錄和簽署同等的法律地位；爲核證機關及由其發出的數據證書設立自願認可計劃，以加強社會人士對電子交易的信心。

5. 爲遏制濫發電子訊息的問題，政府現正擬備《未經收訊人許可而發出的電子訊息條例草案》，並會於本年稍後時間提交立法會審核。

公共資訊保安基建

6. 除法律架構外，香港的資訊保安基建還包括其他重要組成部分。在 2000 年，政府資訊科技總監辦公室[1]成立核證機關認可辦公室，以支援在《電子交易條例》下推行核證機關自願認可計劃。爲配合計劃的推行，政府推出了公匙基建。這是一套由技術機制、程序及政策組成的架構，以應付電子交易對數據機密性、真確性、完整性及不可否定性的需求。

7. 在 2001 年，政府提供撥款在香港生產力促進局下成立香港電腦保安事故協調中心。在發生保安事故時，中心會扮演中央聯絡協調的角式，負責收集本地公司及互聯網用戶就電腦及網絡保安事故提交的資料並作出回應。此外，中心平時還會就防範保安受威脅的措施向

[1] 政府資訊科技總監辦公室於 2004 年 7 月 1 日成立，由通訊及科技局通訊及科技科轄下與資訊科技工作有關的部別與前資訊科技署合併而成。

各界提供意見，以及就資訊保安有關課題舉辦研討會和培訓課程。

8. 自 2003 年 6 月起，入境事務處開始向全港市民發出多用途智能身分證，並隨證附加啓用認可數碼證書的選擇。這項公共基建提供了一個易於使用的共用平台，方便工商界、公共團體及政府部門以穩妥方式提供電子服務。

9. 在 2005 年年中，香港銀行公會及香港金融管理局宣布就高風險零售網上銀行交易，引入雙重認證。這種認證方式混合使用雙重準則以核實用戶的身分，例如數碼證書、保安顯示器發出只用一次的密碼，以及手機短訊發出只用一次的密碼等。

政府的內部資訊保安架構

10. 政府制訂了一套全面的資訊保安政策及指引，以供決策局及部門（各局／部門）採用。此外，我們還設有管理架構、技術保安措施及其他保安機制，以監察、偵察及堵截電腦系統和網絡可能受到的入侵。

資訊保安管理架構

11. 除技術措施外，政府資訊科技總監辦公室已制訂一套完善的資訊科技保安政策、程序及有關指引，當中包括基準資訊科技保安政策、資訊科技保安指引、保安風險評估及審核指引及資訊保安事故處

理指引。這些程序和指引是參考國際間良好的作業模式及專業資源而制訂，並會不時更新以反映技術和保安威脅的轉變。它們在組織、管理及程序各方面提供相當詳盡的資料，讓各局／部門可按之自行建立資訊保安架構和作業模式。這些指引所涵蓋的一些課題列具於本文附件。各局／部門除了須採用上述指引外，還須遵守政府《保安規例》的規定。在《保安規例》的條文當中，有一條專爲資訊系統及資料的儲存、處理及傳送而設，所針對的課題包括機密資料、密碼匙管理、實體保安及妥善銷毀機密資料。

12. 爲監管和執行政府內部的資訊保安，資訊保安管理委員會於2000 成立，其核心成員包括保安局及政府資訊科技總監辦公室的代表。此外，爲了在行政上支援該委員會，政府成立資訊保安工作小組，負責在各局／部門推行及監察資訊保安政策及指引的實施。

保安威脅警報及事故回應

13. 除中央資訊保安管理架構外，政府資訊保安事故應變辦事處(GIRO) 於 2001 年成立，統籌和協助各部門處理政府資訊保安事故。爲支援 GIRO 的運作，政府資訊科技總監辦公室 成立常設辦公室，二十四小時無間斷地監察電腦病毒及資訊保安事故，以及密切注視在全球各地爆發的病毒及有關警報。在有需要時，辦公室會知會保安架構中的有關單位，而當確定保安問題事態嚴重，則會立即向各部門發出病毒或保安警報。各主要政府基建系統的管理人員每週均須就系統的保安狀況及其他涉及資訊保安事宜，向政府資訊科技總監辦公室提交報告，以供管理監察及控制之用。

14. 在部門層面，政府另設有管理架構以推行不同的保安措施，以保護政府的資訊系統。所有部門均須委任一位高級人員，充當部門資訊科技保安主任(DITSO)，負責該部門的整體資訊保安管理及運作。此外，各部門須設立資訊保安事故應變小組 (ISIRT)，以處理日常保安事故的報告及回應。視乎部門的大小及業務的複雜性，各部門的 DITSO 人選及 ISIRT 的安排可能會有差別。

資訊保安的保護措施及方法

15. 爲防範電腦蠕蟲和病毒、黑客入侵、濫發訊息及電腦罪行等不同的威脅，政府採用“防護、檢測、反應及恢復”的原則，並推行所需的措施，以確保業務交易和資訊安全。我們採用了各種尖端科技，包括防火牆、抗禦電腦病毒軟件、入侵偵察系統及其他防禦機制，以監測、偵察和堵截政府電腦網絡及系統可能受到的入侵。我們並會不時安裝所需的修補及糾正程式，以確保系統能應付最新的威脅。

16. 此外，政府還會就保安措施及程序，定期進行檢討和審核，以確保有關措施及程序能緊貼日新月異的科技、業界和國際間良好作業模式的發展，以及系統、網絡或組織環境的轉變。政府資訊科技總監辦公室已就資訊保安專業服務設立常備協議，以便各局／部門借助外間機構制訂保安政策和程序，以及進行系統保安檢討及評核。在 2002 年至 05 年期間，各局／部門透過中央統籌的合約，曾使用這類服務約 140 次，涉及總開支約 4,500 萬元。

政府的整體資訊保安狀況

17. 過去數年，政府在內部事務及公共服務的提供上大力引入資訊科技，而資訊保安架構及爲此動用的資源亦呈現相應的增長。我們就建立一個全面的資訊保安系統所作的努力，已取得令人鼓舞的成果。根據 GIRO 接獲的報告，在過去五年，保安事故的次數顯示持續偏低和逐步減少的趨勢。舉例說，經證實的事故已由 2002 年的 9 宗減少至 2005 年的 3 宗，當中更沒涉及數據／資訊的流失。這趨勢可歸功於各局／部門對保安管理日益關注，以及更嚴格遵守保安政策和指引。在世界貿易組織第六次部長級會議去年十二月在本港舉行之前，政府增強了各局／部門的資訊保安措施。結果，我們在會議期間並無接獲任何有關保安事故的報告。我們當然不會因此而自滿，反之我們會繼續爲系統和數據提供最高水平的防護。

政府就社會採取的資訊保安措施

18. 政府致力令香港成爲一個着着領先的電子商務社群和數碼城市，而資訊保安是香港發展電子商務環境的重要支柱。

業界支援及聯絡

19. 政府鼓勵業界、學術界及有關團體進行研究，以推動知識型社會在本港的發展，並爲此提供所需的資助。爲應付科技罪行，警方

已設立設施和培育包括電腦資料鑑證方面的人才。因此，近年多宗網上罪案得以成功偵破。在 2001 年成立的香港電腦保安事故協調中心，增強了本港就保安事故作出應變的能力。在 2005 年，政府資訊科技總監辦公室成立互聯網基建聯絡小組（IILG）[2]，協助本地的互聯網機構交換資訊和共同處理網上事故。此外，政府又成立資訊保安專責小組，成員包括政府資訊科技總監辦公室、警務處、教育統籌處，數碼 21 策略諮詢委員會，以及資訊保安業界機構的代表，專責研究有助增強本港整體資訊保安水平的具體課題。

市民在資訊保安方面的認知及教育

20. 在 2002 年，政府資訊科技總監辦公室推出「資訊安全網」網站（www.infosec.gov.hk），方便市民透過這個一站式的入門網站，取得資訊保安各方面的最新資訊。此外，我們還在該網站發布廣爲科技先進國家採用的國際良好作業模式及標準。同時，政府資訊科技總監辦公室定期製作電台節目及電視特輯，以提高市民對資訊保安的認知、推廣作業操守、以及向各界灌輸有關防止電腦罪行及熱門資訊保安課題（例如濫發訊息）的最新資訊。我們又透過不同途徑（例如社區中心、圖書館及學校）及舉辦各種活動（例如展會、會議及研討會），以派發資訊小冊子。

21. 在 2003 年，保安局向本地的專業機構和工商業協會發出資訊文件，與各方分享有關國際訊保安標準的最新資訊。此外，又邀請各

[2].IILG 的成員包括香港互聯網交換中心、香港域名註冊有限公司、香港電腦保安事故協調中心、香港互聯網供應商協會、警務處、電訊管理局及政府資訊科技總監辦公室。

團體考慮爲其所屬行業訂立資訊保安標準和評審機制，以滿足不同行業的具體需要。

22. 在地區層面方面，政府資訊科技總監辦公室是亞太經合會電訊暨資訊工作小組的成員，該小組對電子商貿、數碼隔膜及有關問題，尤其是資訊科技保安及電腦緊急應變方面的問題，正日益關注。政府資訊科技總監辦公室一向都有積極參與小組的事務，包括小組就資訊保安進行的開發工作。透過此等參與，我們的目標是要提高政府在收集情報、交換資訊，以及區內一旦發生重要保安事故採取應變措施的能力。

2006-07 年度的計劃項目

23. 資訊科技保安仍然是政府重點工作項目之一。當局會繼續推行一連串的工作，向政府內部及社會各界推廣和灌輸資訊保安的認知，以及提高他們處理資訊保安問題的應變能力。

政府內部

24. 於2006-07年度，政府資訊科技總監辦公室將會-

(a) 在2006 年第2 季度內完成修訂政府資訊科技保安有關的規例、政策及指引，以靠貼日新月異的科技及國際／ 業界作業模式的發展；

(b) 加強各局／ 部門資訊保安的管理、監察、威脅預警和保安事故應變措施的機制， 以及與警務處、香港電腦保安事故協調中心和互聯網基建組織等有關團體保持緊密合作；

(c) 搜集資訊保安的科研發展和有關資料， 並公布預防的指引， 供各局／ 部門參考； 以及

(d) 爲各局／ 部門的管理及技術人員舉辦培訓班／ 研討會，並盡量以時下關注的資訊科技保安課題及國際認同的良好作業模式爲主題（例如反濫發訊息及採用資訊保安標準）來提高資訊保安的效應。

25. 在2006-07 年度的預算開支爲130萬元，並不包括爲各局／部門進行資訊保安覆檢及審核的費用。各局／部門須根據有關項目的規模，以部門營運開支支付所需費用，或向基本工程儲備基金總目710 電腦化計劃申請撥款。

社區各界

26. 於2006-07年度，當局會繼續向各界推廣和灌輸有關更廣泛應用資訊科技和資訊保安的知識-

(a) 當局會加強對弱勢社群和各行業的中小企的推廣工作， 以提高他們對資訊科技的認知和應用。由於資訊保安及資訊科

技應用相關的新知是重要的一環， 我們會繼續向社會各界灌輸在這方面的認知， 例如參照良好作業模式， 作爲防範和應付電腦相關罪行、電子商務詐騙及濫發訊息， 與及工商機構採用合適的國際標準來保護資訊資產。

(b) 此外，我們會繼續透過「資訊安全網」網站，提供一站式的資料參考和專業意見給市民及各界參閱。我們會與業界合作， 就公眾關注的課題如反濫發訊息等協辦展覽會和研討會。我們會尋求與專業協會和有關組織合作的機會， 開設短期課程給市民進修， 以增強公眾對資訊保安的認知。我們還會製作一個新系列的電台節目， 向市民灌輸保護資訊資產和防範電腦罪行的知識。

27. 以上在社區推廣資訊保安的預算開支爲100 萬元。

徵詢意見

28. 謹請議員察悉本文的內容。

工商及科技局

政府資訊科技總監辦公室

2006 年 3 月

資訊科技專業人員 有用指引及標準

English 简体版

- 資訊科技專業人員專欄
- 保安貼士
- 技術參考資料
- 有用指引及標準
- 資訊保安管理
- 相關條例
- 公共服務
- 電腦病毒
- 消息及活動
- 詞彙表
- 下載區
- 有用連結

為協助你為公司制訂資訊保安管理計劃，我們點出一些被推薦為有效保安作業實務的有用指引及資訊保安國際認可標準以供參考。

- 資訊科技保安政策及指引
- 資訊保安標準
- 資訊科技保安參考資料

(以下文件是PDF格式，你需要使用Adobe Acrobat Reader來閱覽及列印，請按此處下傳。 Get Adobe Acrobat Reader)

資訊科技保安政策及指引

香港特別行政區政府向各決策局和部門提供了基準資訊科技保安政策及一系列與資訊科技保安有關的指引以給各決策局和部門在保護政府資訊系統時提供有關的技術建議及指引。有關的指引可透過以下超連結獲取。用戶須留意這些指引只供一般參考用途，用戶在使用這些指引前須自行對所提供的資料作出評估及徵詢獨立意見。

- **基準資訊科技保安政策**-本文件就政府各政策局及部門在資訊科技保安規格訂定基礎標準。它述明那些保安事宜，對政策局及部門至為重要。
- **資訊科技保安指引**-這份指引概述與資訊科技保安有關的理念，並就《基準資訊科技保安政策》作出闡釋。
- **互聯網通訊閘保安指引**-這是《資訊科技保安指引》的補充文件，就互聯網通訊閘的保安提供指引。
- **保安風險評估及審查指引**-這是《資訊科技保安指引》的補充文件，概述適用於保安風險評估及審計的參考模型。
- **資訊保安事故處理指引**-這是《資訊科技保安指引》的補充文件，有助於制定處理保安事故的規劃措施，而文件並可用作預防、偵測及應付保安事故的參考資料。

- 頁首 -

資訊保安標準

- **ISO 17799** - 爲資訊保安管理而設的業務守則
- **ISO 7498，開放式系統連結標準** - ISO/IEC 7498保安結構，第二部分(已被以下標準所取代：ISO/IEC 10745和ITU-T X.803"上層保安標準"、ISO/IEC 13594和ITU-T X.802"下層保安標準"，以及ISO/IEC 10181-1和ITU-T X.810"保安架構，第一部分：概覽")
- **BS 7799** - 以商業爲先制定的資訊保安管理最佳作業實務
- **可信賴系統評估準則(TCSEC)或稱爲「橘皮書」** - 基於政府及軍事機關大部分操作系統的功能評估、有效性及保證性評估而進行的保安要求分類。TCSEC於1985年面世，並於2000年廢除。
- **彩虹系列(The Rainbow Series)** - 這系列叢書把「橘皮書」的涵蓋範圍延伸至資訊保安的其他方面。例如：
    - 可信賴網絡詮釋(TNI)或稱「紅皮書」- 爲保護不同類型的網絡及網絡環節提供架構。
- **資訊技術保安評估準則(ITSEC)** - 由歐洲國家爲評估電腦系統保安屬性而制訂的首個單一標準，只用於歐洲。
- **通用條件(Common Criteria)** - 透過加拿大、法國、德國、荷蘭、英國及美國的國家保安標準組織協作努力，結合並劃一現有及演變中的評估條件。URL://csrc.nist.gov/cc/Documents/CC%20v2.1%20-%20HTML/CCCOVER.HTM

- 頁首 -

資訊科技保安參考資料

- **Establishing a Computer Security Incident Response Capability**，NIST (National Institute of Standards and Technology)特刊800-3，1991年11月
- **Sample Incident Handling Procedures**，來自SANS (System Administration, Networking, and Security Institute)，1998年4月
- **RFC 2196 Site Security Handbook**，來自IETF (The Internet Engineering Task Force)
- **RFC 2350 Expectations for Computer Security Incident Response**，來自IETF (The Internet Engineering Task Force)
- **Responding to Computer Security Incidents: Guidelines for Incident Handling**, University of California Lawrence Livermore National Laboratory，1990年7月
  [Source: The U.S. Department of Energy's Computer Incident Advisory Capability (CIAC)]
- **SANS/FBI Top 20 Most Critical Internet Security Vulnerabilities List**
  該表列出了20個漏洞，並分成三類：影響所有系統的漏洞、影響視窗系統的漏洞、影響Unix系統的漏洞。

- **國際資訊系統審計協會標準、指引及程序**
  國際資訊系統審計協會制訂了一系列的資料系統審計標準、指引及程序。

- 頁首 -

修訂／檢視日期：二零零六年三月

政府資訊科技總監辦公室

基準資訊科技保安政策

[S17]

第2.3版

二零零四年十一月
香港特別行政區政府

目錄

政府資訊科技總監辦公室

資訊科技保安指引

[G3]

第 4.3 版

二零零四年十一月
香港特別行政區政府

目錄

附錄

政府資訊科技總監辦公室

保安風險評估及審計指引

[G51]

第 2.1 版

二零零四年七月
香港特別行政區政府

目錄

政府資訊科技總監辦公室

資訊保安事故處理指引

[G54]

第 2.2 版

二零零四年九月
香港特別行政區政府

目錄

附錄