香港電腦保安事故應變中心服務
制度檢討報告

香港特別行政區政府

商務及經濟發展局

政府資訊科技總監辦公室

二零零八年十月

目錄

前言

政府資訊科技總監已就香港的電腦保安事故應變中心服務完成了制度檢討，並將檢討結果及建議編成報告。現邀請業界就訂定香港的電腦保安事故應變中心服務運作的優先次序、目標及服務水平的機制，提出意見。

請於**二零零八年十一月十四日**或之前，以下列其中一種方式，把意見書送交政府資訊科技總監：

郵遞：	香港數碼港道 100 號 數碼港 1 座 6 樓 政府資訊科技總監辦公室 政府資訊科技總監 (經辦人：系統經理 (E)21A)
傳真：	(852) 2989 6073
電郵：	cerc_review@ogcio.gov.hk

除非遞交意見書的人士提出要求，否則我們不會以保密形式處理意見書。我們或會以某種形式複製和公開意見書的全部或部分內容，以及採用、修改或演繹當中提出的任何建議，

但不會徵求遞交意見書人士的同意，也不會引述出處。

商務及經濟發展局

政府資訊科技總監辦公室

二零零八年十月

背景

隨着資訊科技和互聯網應用於電子商貿日趨普及，近年非法入侵電腦的情況亦急速增加。若要達到“數碼 21”資訊科技策略的目標，即在網絡相連的世界中把香港發展爲領先數碼城市，資訊保安是必須重視的課題。業界普遍認爲，應付及減少保安事故最重要的環節，是加深認知、保持警覺和採取防範措施。

2. 一九八八年十二月，Carnegie Mellon 大學在一次電腦保安事故發生後（這次事故引致大約百分之十的互聯網系統陷入停頓），爲美國國防部成立了電腦保安事故應變中心[1]。自此以後，該應變中心的工作逐漸擴展至包括向公眾發放有關保安威脅及事故的預警及警報，以達至減少這些事故所造成的破壞。

3. 鑑於社會對電腦系統及互聯網的保安威脅日益關注，多個海外經濟體系和部分大型機構都設立了電腦保安事故應變中心，統籌電腦保安事故的匯報，以及爲受網絡保安

[1] 美國電腦保安事故應變中心的詳盡資料，載於 http://www.cert.org 網站。

事故影響的當地企業和互聯網用戶提供應變措施。電腦保安事故應變中心一般統籌應變及復原行動、發布有關電腦保安的資訊、確認保安漏洞，以及採取相應的預防措施。此外，應變中心亦會舉辦有關推廣資訊保安的宣傳活動、訓練課程和會議，以及與當地及海外的相關機構保持密切聯繫。

4. 現時在 40 多個經濟體系中，大約有 200 間服務不同用戶羣及界別的相關機構提供電腦保安事故應變和有關服務。在本報告，這些服務統稱爲電腦保安事故應變中心服務。

5. 一般而言，世界各地有兩大類電腦保安事故應變中心相關的機構。其中一類的服務對象爲商界、學術界或政府機構，主要爲其特定用戶羣提供服務和支援，而另一類則是向當地整個社會不同界別提供服務。在本報告，我們着重於檢討本港在後一類電腦保安事故應變中心的制度。

資訊保安事故帶來的影響

6. 近年，互聯網的迅速發展令電子商貿在全球商業環境下快速增長。自二零零一年起，本港透過電子途徑售賣貨

品、服務或資料等有關的商業交易超過 1,950 億元。在二零零一至二零零七年期間，本港電腦保安事故的數目上升超過 7 倍；而在二零零四至二零零七年期間，仿冒詐騙事故的數目則上升超過 10 倍。自二零零一年起，本港電腦罪案引致的財政損失超逾 5,000 萬元。

7. 參照海外的經驗，單一的網絡事故也足以對社會造成重大影響。二零零七年四月，波羅的海國家愛沙尼亞經歷了嚴重的網上襲擊，受影響的單位包括政府部門、銀行、報界和政黨。有關網上襲擊影響全國多日的運作，受襲電腦約有 100 萬部，分布超過 50 個國家。此外，在二零零六年十二月，美國一間公營機構 TJX 報稱其電腦系統遭入侵，超過 4,500 萬張信用卡的資料被竊。預計 TJX 須耗資約 10 億美元，以解決事件帶來的後果。

8. 有鑑於電腦罪行帶來潛在的龐大財政損失，以及電子商貿可涉及大額交易，有必要提供一個穩妥可靠的網絡環境，以進行電子商貿。

香港的電腦保安事故應變中心服務

9. 在二零零一年，香港生產力促進局成立香港電腦保安事故協調中心（下稱“協調中心”）[2]，在電腦及網絡保安事故發生時實行中央統籌，收集本地公司（尤其中小型企業）及互聯網用戶就事故提交的資料，並協助作出應變。協調中心亦統籌匯報事故的應變及復原工作、協助監察及發布有關資訊保安的信息、就防範保安威脅的措施提供意見，以及舉辦資訊保安研討會和培訓課程。

電腦保安事故應變中心服務制度的檢討

10. 香港的電腦保安事故應變中心在協助本地提供可靠穩妥的營商環境上，扮演着重要的角色。因應互聯網環境的急速轉變，政府資訊科技總監檢討了香港的電腦保安事故應變中心服務，從而爲未來的服務確立方向，並作出長遠及可持續的安排。

11. 是項檢討參考了國際及地區的最新發展，以探究適用

[2] 香港電腦保安事故協調中心的詳盡資料，載於 http://www.hkcert.org 網站。

於香港電腦保安事故應變中心服務的長遠安排。檢討參考了八個經濟體系（包括: 澳洲、加拿大、中國、印度、日本、馬來西亞、新加坡及美國）的作業模式。有關這些經濟體系和香港現時的電腦保安事故應變中心服務的比較，載於附件一。

本港電腦保安事故應變中心的需要

12. 許多數碼領先的經濟體系均已建立其電腦保安事故應變中心。鑑於上文第 6 至第 8 段所述有關資訊保安事故所帶來的重大影響，我們認爲有需要爲本地企業及互聯網用戶提供電腦保安事故應變中心服務，以保持可靠穩妥的網絡環境。在資訊保安事故發生後，亦可幫助電腦用戶減少服務中斷及所蒙受的損失，並協助復原業務的運作。

成立電腦保安事故應變中心的安排

13. 在大部分的海外經濟體系,電腦保安事故應變中心都是由非牟利及中立的機構或其政府營運。香港亦會採用這個作業模式。作爲一個非牟利機構，香港生產力促進局將會繼

續營運協調中心，爲本港提供電腦保安事故應變中心服務。

財務安排

14. 爲提供穩定及中立的電腦保安事故應變中心服務，政府將資助協調中心的運作，以支援必要的服務。但是，協調中心仍可在政府認爲合適的個別情況下，提供其他收費的增值服務。

電腦保安事故應變中心服務的範圍

15. 爲保持可靠穩妥的網絡環境，以便在香港進行商貿活動，我們認爲下列電腦保安事故應變中心服務是必要的。這些服務可協助本地企業及互聯網用戶預防並減少服務中斷，以及免受網上襲擊：

- 事故處理、應變及協調
- 發布警報信息、預警及其他有關電腦保安的資訊
- 保安認知的建立和培訓
- 與不同單位合作，並協調保安防範措施

徵求業界意見

16. 香港生產力促進局已向政府建議二零零九至二零一零年協調中心的運作安排及往後的未來計劃。服務建議書的詳細內容，載於附件二。

17. 在管治及表現監察方面，香港生產力促進局建議，除了由其管理層監察協調中心的職能和運作，並督導中心的策略外，可加入以下的新機制：

(a) 協調中心會製作年報，闡述年內的工作表現。該年報將向政府資訊科技總監辦公室提交，及在香港生產力促進局的業界羣組中作簡報，並會張貼於協調中心的網站，讓公眾參閱。

(b) 協調中心的管理層每年與政府資訊科技總監辦公室會面兩次，討論有關協調中心的運作及活動，並商定中心未來的策略及計劃。該會議亦可加入評核協調中心工作表現的議題。

18. 歡迎業界就協調中心的管治及表現監察機制給予意見。業界亦可就訂定電腦保安事故應變中心服務運作的優先次序、目標及服務水平的機制提出建議。我們會考慮各界的意見，爲香港電腦保安事故應變中心的新制度定案。

附件一 – 香港和其他經濟體系的電腦保安事故應變中心服務

	香港 香港電腦保安事故協調中心	澳洲 AusCERT	加拿大 CCIRC	中國 國家計算機網絡應急技術處理協調中心	印度 CERT-In	日本 JPCERT/CC	馬來西亞 MyCERT	新加坡 SingCERT	美國 US-CERT
成立年份	2001	1993	2005	2000	2004	1996	1997	1997	2003
電腦保安事故應變中心服務 - 事故處理、應變及協調									
• 提供 24x7 電腦保安事故報告或應變服務	✓	✓	✓	✓	✓	✓	✓	✓	✓
• 與不同機構包括其他電腦保安事故應變中心合作	✓	✓	✓	✓	✓	✓	✓	✓	✓

	香港 香港電腦 保安事故 協調中心	澳洲 AusCERT	加拿大 CCIRC	中國 國家計算機 網絡應急 技術處理 協調中心	印度 CERT-In	日本 JPCERT/CC	馬來西亞 MyCERT	新加坡 SingCERT	美國 US-CERT
• 多種保安事故報告渠道 (例如：電郵、傳真、電話及短訊等)	✓	✓	✓	✓	✓	✓	✓	✓	✓
電腦保安事故應變中心服務 - 發布警報信息、預警及其他有關電腦保安的資訊									
• 公布電腦保安資訊(例如：保安警報、預警及漏洞)	✓	✓	✓	✓	✓	✓	✓	✓	✓
• 公布保安指引、報告、通訊及統計資料等	✓	✓	✓	✓	✓	✓	✓	✓	✓
• 多種資料發放渠道(例如：網站、短訊、簡易資訊聚合及電郵名單等)	✓	✓	✓	✓	✓	✓	✓	✓	✓

	香港 香港電腦 保安事故 協調中心	澳洲 AusCERT	加拿大 CCIRC	中國 國家計算機 網絡應急 技術處理 協調中心	印度 CERT-In	日本 JPCERT/CC	馬來西亞 MyCERT	新加坡 SingCERT	美國 US-CERT
電腦保安事故應變中心服務 - 保安認知的建立和培訓									
• 舉辦與電腦保安相關的講座、工作坊及培訓課程	✓	✓	✓	✓	✓	✓	✓	✓	✓
電腦保安事故應變中心服務 - 與不同單位合作，並協調保安防範措施									
• 與不同的機構合作 (例如：互聯網持份者、執法機關及產品供應商等)	✓	✓	✓	✓	✓	✓	✓	✓	✓
• 監測互聯網的保安威脅及狀況	有限服務	✓	✓	✓	資料不詳	✓	資料不詳	✓	✓
• 提供免費保安檢測服務	沒有提供	資料不詳	資料不詳	資料不詳	資料不詳	資料不詳	✓	資料不詳	資料不詳

	香港 香港電腦保安事故協調中心	澳洲 AusCERT	加拿大 CCIRC	中國 國家計算機網絡應急技術處理協調中心	印度 CERT-In	日本 JPCERT/CC	馬來西亞 MyCERT	新加坡 SingCERT	美國 US-CERT
• 參與國際及地區電腦保安事故應變中心有關的活動	✓	✓	✓	✓	✓	✓	✓	✓	✓
• 研究及分析有關電腦保安事故的議題	有限服務	✓	資料不詳	✓	✓	✓	✓	✓	✓
成立電腦保安事故應變中心的安排									
• 由政府成立	-	-	✓	✓	✓	-	✓	✓	-
• 由非牟利機構成立	✓	✓	-	-	-	✓ (有合法地位)	-	-	-
• 以公私營合夥形式成立	-	-	-	-	-	-	-	-	✓

	香港 香港電腦 保安事故 協調中心	澳洲 AusCERT	加拿大 CCIRC	中國 國家計算機 網絡應急 技術處理 協調中心	印度 CERT-In	日本 JPCERT/CC	馬來西亞 MyCERT	新加坡 SingCERT	美國 US-CERT
財務安排									
• 政府資助	✓	-	✓	✓	✓	✓	✓	✓	✓
• 自資	-	✓	-	-	-	-	-	-	-
詳細資料載於以下網站超連結									
	http://www.hkcert.org/chinese/home.html	http://www.auscert.org.au/index.html	http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx	http://www.cert.org.cn/index.shtml	http://www.cert-in.org.in/	http://www.jpcert.or.jp/english/	http://www.mycert.org.my/	http://www.singcert.org.sg/	http://www.us-cert.gov/

註：上述資料截至 2008 年 9 月。

附件二 –

香港生產力促進局提交的香港電腦保安事故協調中心服務建議書

Hong Kong
Productivity Council
香港生產力促進局

香港電腦保安事故協調中心

服務建議書

香港生產力促進局

二OO八年十月

Hong Kong Productivity Council
香港生產力促進局

目錄表

一、 目的

香港電腦保安事故協調中心 (Hong Kong Computer Emergency Response Team Coordination Centre，HKCERT) 於二OO一年由香港特別行政區政府創新科技基金撥款成立。中心由香港生產力促進局負責日常運作。主要服務對象爲本地企業，尤其是中小型企業及互聯網用戶。

中心成立的宗旨，包括：

甲) 集中處理香港的電腦保安事故及回應；

乙) 提高電腦保安的意識並提倡有關國際標準及實踐；

丙) 協助改善系統的保安及防範電腦保安事故的發生；

丁) 協助及協調電腦保安事故發生後的復修工作；

戊) 與國際上其他協調中心，包括 Forum of Incident Response and Security Team (FIRST) 的成員緊密聯繫，協調並合作處理保安事故。

二、 背景

HKCERT 是香港資訊基建極重要的一環。在本港，它集中對本地企業及互聯網用戶處理及協調電腦保安事故。在國際間，它被確認爲代表本港的電腦保安事故協調機構，協調並與其他協調中心合作處理資訊保安及電腦保安事故。過去幾年，HKCERT 已在香港及國際間成功建立它的專業技術水平，社會的認同及在處理保安事故上的信任。

成立以來，協調中心成功的處理香港一些重大的事故，包括：

甲) 在二OO三年及二OO四年爆發的 SQL Slammer 蠕蟲，Blaster 蠕蟲(衝擊波)及 Sasser 蠕蟲(震盪波)；

乙) 在二OO五年一些銀行客戶大規模感染的間諜程式；

丙) 在二OO五年世貿部長級會議、二OO六年國際電信聯盟會及二OO八年北京奧運會及殘奧會期間，密切注視互聯網上的異動及威脅；

丁) 在二OO八年協助香港域名註冊有限公司，識別及關閉在 .hk 域名上登記含惡意的域名；

戊) 從二OO八年起，主動尋找本地受惡意編碼入侵及遭塗改的網頁。

除了對電腦保安事故回應外，HKCERT 亦透過舉辦研討會等活動，提高市民對資訊保安、防範保安事故的認識。中心亦曾出版不少有關資訊保安的指引及手冊。包括：

甲) 中小型企業資訊保安指南；
乙) 預防間諜程式及其他不明軟件指南；
丙) 家用個人電腦保安基準自我檢查指引；
丁) 移除 "MarketScore" 的程序；
戊) 因蠕蟲引致電郵氾濫的處理方法；
己) 安全使用無線網絡 (Wireless LAN) 指南；
庚) 預防電腦病毒指南；
辛) Pretty Good Privacy (PGP) 指南。

HKCERT 亦經常參與政府設立的工作小組及委員會，例如互聯網基建聯絡小組 (Internet Infrastructure Liaison Group，IILG)，資訊保安專責小組 (Information Security Task Force)，無線網絡保安工作組。自二 OO 一年起，HKCERT 亦代表香港出席國際間的保安事故協調小組的會議。

隨著香港電子商貿活動的增加，HKCERT 已成爲在香港資訊基建重要的一環，協助香港建立一個安全的互聯網環境。

三、 二OO九至二O一O年度 HKCERT 的服務及運作

二 OO 九至二 O 一 O 年度的服務範疇與本年度的內容大致相同，工作內容包括：

甲) 事故報告及回應

- 本地事故報告(問題確認及解決)
  - 提供全年每天24小時電腦事故報告服務，包括感染惡意程式、黑客入侵、釣魚網站及電郵；
  - 透過電話、電郵或傳真接受報告；
  - 協助及協調電腦事故後的復修工作；
  - 在重大電腦保安事故，協調不同機構合作處理。
- 外地事故報告(協調本地及外地機構)
  - 協調及回應外地向香港報告的事故；
  - 與本地及外地機構溝通聯絡解決問題。
- 主動尋找本地被入侵及塗改的網站
  - 搜集入侵漏洞及惡意網站的資料；
  - 尋找受感染的 .hk 網站；

- 通知網站負責人有關事故，並協助復修工作；
- 跟進有關復修情況。

乙) 電腦保安警報及預警

- 資料搜集
  - 緊密監測有關電腦保安的資訊，例如電腦病毒、保安漏洞及對策。
- 發佈警報
  - 透過 HKCERT 網站、電郵、短訊及傳媒，向公眾發放有關電腦保安及事故的資訊。

丙) 出版

- 資訊保安月報
  - 每月出版「資訊保安報」，提供有關電腦及網絡保安最新資訊。
- 警報摘要
  - 每月兩次發表電腦保安警報摘要，內容包括保安警報及新聞。
- 保安指引及核對清單
  - 就有關電腦保安，出版電腦保安威脅及對策的指引。
- 保安文章及忠告

- 就電腦保安威脅、漏洞、防禦策略、襲擊預警等撰寫文章及忠告。

丁) 教育、培訓及推廣

- 全城電腦清潔日
  - 與政府資訊科技總監辦公室(OGCIO)及香港警務處合作在十一月至十二月期間，安排活動，提高公眾對電腦保安的認識。
- 擔任公開研討會的講者
  - 在公眾場合演講，提高公眾意識。
- 報刊與傳媒
  - 與報刊及傳媒溝通有關資訊保安的問題及事故。

戊) 聯繫與合作

- 本地的委員會及工作小組
  - 與政府資訊科技總監辦公室及香港警務處科技罪案組定期會面，並商討共同關注的議題及策略；
  - 參與香港特區政府機構，例如政府資訊科技總監辦公室及電訊管理局所組織有關資訊保安的工作小組及委員會。
- 互聯網供應商及香港域名註冊有限公司

- 與香港域名註冊有限公司及互聯網供應商(主要透過香港互聯網供應商協會)，解決有關資訊保安的問題。

- 資訊保安產品供應商
  - 與一般軟件及資訊保安產品及服務供應商保持聯繫，共同處理資訊保安問題。
- 海外的協調中心
  - 與國際及亞太區的協調中心保持聯繫，以解決資訊保安的問題及事故；
  - 參與國際及亞太區的協調中心倡議的活動，增強資訊交流及合作。

四、 資源及支出

本部分特意留空

五、 管治及表現

五/一) 管治

目前，香港生產力促進局的管理層負責管理 HKCERT 的運作，並設定其功能及監督發展策略。由於 HKCERT 的服務和功能比較獨特，其他本地機構或個人不一定具備相關的專業知識，充分了解一個協調中心不斷發展及改進的功能和運作。所以我們建議中心的監管模式透過下列兩項活動進行：

甲) HKCERT 將每年發佈一份年報，內容包括一年來的工作表現，所處理的事故及舉行的活動。報告將張貼於 HKCERT 的網站內，讓公眾可以瞭解 HKCERT 的工作及活動，並提供意見。報告亦將提交與政府資訊科技總監辦公室及在香港生產力促進局的業界羣組中作簡報。

乙) HKCERT 的管理層每年與政府資訊科技總監辦公室會面兩次，討論有關 HKCERT 的運作及活動並協議中心未來的發展方向、策略及活動等。

五/二) 表現

協調中心一般會根據資訊保安及襲擊的趨勢，快速回應及調整工作範圍和活動。加上協調中心的服務一般都是在應急情況下才發揮它的效用，故此在訂立表現度量及目標以評核一個協調中心的表現並不容易。使用中心的用戶包括本地及海外的用戶，加上解決事故牽涉的團體眾多，並不容易對中心提供的服務的滿意程度作出合適的評核。

我們建議在每半年和政府資訊科技總監辦公室的會面中，可以對中心的工作表現作客觀評核。

六、 未來計劃

六/一) 工作範圍

隨著惡意程式及釣魚網絡等活動日趨嚴重，世界各地的協調中心已逐步建立新的功能，分析惡意程式及主動監測互聯網上潛在的威脅。很多協調中心已擴充它們的工作範圍，加進惡意程式偵測和分析，網上威脅監測和增強與其他機構的聯繫等功能。HKCERT 亦需要增強它的功能和服務，以應付最新電腦保安事故的發展趨勢。

甲) 惡意程式偵測和分析

- 建立一個技術平台，偵測和分析惡意程式，尤其是針對本地機構的入侵程式；
- 與世界各地的協調中心聯繫，交流有關惡意程式的資訊，分享偵測和分析的技術和工具；
- 安裝 honeypots、honeynets 等技術，以偵測和分析潛在的攻擊。

乙) 與世界各地的協調中心進行有關惡意程式的資訊交流

丙) 成立「互聯網威脅監測及分析」系統

- 確立相關的方法、營運模式、工具、合作伙伴，以建立相關系統；
- 策劃及實施這系統；
- 根據研究結果提供預報及威脅分析。

丁) 和互聯網供應商、軟件供應商及資訊保安供應商建立合作關係

- 與互聯網供應商就事故報告及回應訂立程序，以縮短回應時間；
- 策劃及組織本地的事故回應演習。

戊) 改善事故回應系統及技巧

己) 加強宣傳 HKCERT 的服務

- 宣傳 HKCERT 的服務；
- 透過業界的商會提高資訊保安意識。

庚) 加強本港事故處理能力

- 協助本地大機構建立事故回應能力及設立機構內的協調中心；

- 擴展中心的聯繫範疇包括重要基建，並加強和這些機構在資訊保安、潛在威脅、事故回應及復修行動的溝通。

六/二) 資源及支出

本部分特意留空

- 完 -