政府電腦保安事故協調中心簡介

1. 文件資料

本文件參照 RFC 2350[1]的要求，對政府電腦保安事故協調中心（下稱「GovCERT.HK」）作出相關的描述。文件提供有關 GovCERT.HK 的基本資料，並載述其通訊渠道、角色、責任及服務。

1.1 最後更新日期

這是截至 2020 年 9 月 15 日的 1.4 版本。

1.2 分發通知的名單

本文件如有更新，將會通知 GovCERT.HK 的成員。

1.3 文件可供查閱的位置

本文件的現行版本載於 GovCERT.HK 網站。

1.4 認證本文件

本文件已加上由 GovCERT.HK 的 PGP 密碼匙所簽發的數碼簽署（請參閱下文第 2.6 段）。

[1] https://www.ietf.org/rfc/rfc2350.txt

2. 聯絡資料

2.1 中心名稱

政府電腦保安事故協調中心
簡稱：GovCERT.HK

2.2 地址

香港數碼港道 100 號
數碼港一座 6 樓
政府電腦保安事故協調中心

2.3 時區

香港（GMT +08:00）

2.4 傳真號碼

+852 2519 7320

2.5 電郵地址

所有給 GovCERT.HK 的通訊均應電郵至 cert@govcert.gov.hk。

中華人民共和國香港特別行政區（下稱「政府」）各局和部門應通過內部電郵系統，匯報所有資訊保安事故。

2.6 公開密碼匙及資訊保密

GovCERT.HK 與各局和部門之間會以 S/MIME 傳輸敏感數據。

GovCERT.HK 備有 PGP 密碼匙（公開密碼匙識別碼：0x7D779220, 公開密碼匙指紋：93A6 1508 500A 73F8 4817 9721 FA29 2F03 7D77 9220）。該密碼匙現於以下網站及公開密碼匙伺服器提供：

- GovCERT.HK 網站（網址：www.govcert.gov.hk）
- PGP.com 密碼匙伺服器（網址：keyserver.pgp.com）
- 麻省理工學院 PGP 公開密碼匙伺服器（網址：pgp.mit.edu）
- SKS OpenPGP 密碼匙伺服器（網址：keys.gnupg.net）

2.7 中心成員

GovCERT.HK 團隊的負責人是數字政策辦公室（下稱「數字辦」）的總系統經理（項目管理及網絡安全）。該團隊由數字辦的資訊科技保安專業人員組成。

2.8 其他資料

有關 GovCERT.HK 的一般資料，可瀏覽 www.govcert.gov.hk 網站。

2.9 聯絡方法

如欲與 GovCERT.HK 聯絡，應先電郵至 cert@govcert.gov.hk。如需向 GovCERT.HK 緊急求助，請在電郵主題註明[緊急]二字。

3. 約章

3.1 使命宣言

GovCERT.HK 的使命是支援政府的資訊及網絡保安工作。

GovCERT.HK 的工作包括發放保安警報及預警；發出有關保安措施的建議；協調保安事故的處理及復原工作；以及加強市民的資訊保安認知和教育。為提升區內資訊及網絡保安的能力，GovCERT.HK 亦會與其他電腦緊急事故應變小組及服務供應商合作，以便有效應對電腦保安事故，並交流良好作業模式。

3.2 服務對象

GovCERT.HK 是政府的電腦保安事故應變小組，專責為政府協調處理資訊及網絡保安事故。GovCERT.HK 的服務對象包括政府的各局和部門。

3.3 資助及／或聯繫

GovCERT.HK 是數字辦轄下的工作單位。該中心是負責國家或地區電腦保安事務的電腦保安事故緊急應變小組，由政府全資設立。

GovCERT.HK 與香港網絡安全事故協調中心（HKCERT）緊密合作，亦通過加入電腦緊急事故應變小組統籌中心（CERT/CC）、全球保安事故協調中心組織（FIRST）及亞太區電腦保安事故協調組織（APCERT），與其他負責國家或地區電腦保安事務的電腦保安事故緊急應變小組建立緊密關係。

3.4 負責當局

GovCERT.HK 隸屬數字辦，屬政府的電腦保安事故應變小組。

4. 政策

4.1 保安事故種類和支援水平

GovCERT.HK 會視乎保安事故的種類、嚴重性、程度和以下的緩急次序，按適合的支援水平妥善協調所提供的資源，以減輕保安事故帶來的影響。

1. 構成人命和人身安全威脅。
2. 危及敏感或關鍵資源。
3. 遺失或損毀重要資料並造成嚴重損失。
4. 系統損壞並導致長時間故障及復原成本高昂。
5. 服務中斷。
6. 相關的局和部門或整個政府的公眾形象受損。

4.2 合作、交流和資訊公開

GovCERT.HK 會與本地執法機構、其他電腦緊急事故應變小組和機構合作，分享有關保安警報及威脅的資訊。GovCERT.HK 會遵從交通燈協議（Traffic Light Protocol）的規定，與其他電腦緊急事故應變小組或機構交換敏感資訊。

GovCERT.HK 會以限閱方式處理保安事故和部分系統漏洞的資訊。已獲授權的 GovCERT.HK 成員、負責受影響資訊系統的資訊保安人員及參與鑑證調查的調查人員才可交換和傳送這些資訊。事故所得的經驗可分享給服務對象和其他電腦緊急事故應變小組。

4.3 通訊與認證

GovCERT.HK 會依照政府的相關規例和政策保護敏感資訊。

傳輸的敏感資訊會以 S/MIME 或 PGP 加密及簽署。

5. 服務

5.1 事故應變

GovCERT.HK 將在技術方面協助各局和部門處理保安事故，特別是就保安事故管理中以下幾個方面提供協助及建議：

5.1.1 事故分流

- 評估在政府內發生的保安事故的影響及程度。

5.1.2 事故協調

- 協調處理在政府內發生的保安事故，並提供建議。
- 協調相關持份者，就聲稱及真實的網絡攻擊加強應對措施。

5.1.3 事故處理

- 在有需要時向相關的局和部門提供建議或協助，以採取適當行動控制保安事故所造成的損害。
- 與相關的局和部門跟進處理保安事故的進展。

5.2 積極進行的工作

GovCERT.HK 協調和提供下列服務：

- 發放保安警報、保安建議及相關資訊；
- 通過舉辦研討會及培訓課程，提高政府及公眾對資訊保安的認知；
- 協調預防性的漏洞掃描工作及網絡安全演習；以及
- 與相關機構合作，分享最新的保安威脅及資訊。

6. 保安事故報告表

本網站及內聯網上的《資訊保安事故處理實務指引》(ISPG-SM02)載有資訊保安事故初步報告表及事故事後報告的樣本，以供服務對象參考。

7. 免責聲明

GovCERT.HK 在擬備資訊、通知及保安警報時已設法核對有關資料，但若本網站所提供的資料有任何錯漏，或有人因使用相關資料而蒙受損失，GovCERT.HK 概不承擔任何責任。

完