政府电脑保安事故协调中心简介

1. 文件资料

本文件参照 RFC 2350[1]的要求，对政府电脑保安事故协调中心（下称「GovCERT.HK」）作出相关的描述。文件提供有关 GovCERT.HK 的基本资料，并载述其通讯渠道、角色、责任及服务。

1.1 最后更新日期

这是截至 2020 年 9 月 15 日的 1.4 版本。

1.2 分发通知的名单

本文件如有更新，将会通知 GovCERT.HK 的成员。

1.3 文件可供查阅的位置

本文件的现行版本载于 GovCERT.HK 网站。

1.4 认证本文件

本文件已加上由 GovCERT.HK 的 PGP 密钥所签发的数码签署（请参阅下文第 2.6 段）。

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

2. 联络资料

2.1 中心名称

政府电脑保安事故协调中心
简称：GovCERT.HK

2.2 地址

香港数码港道 100 号
数码港一座 6 楼
政府电脑保安事故协调中心

2.3 时区

香港（GMT +08:00）

2.4 传真号码

+852 2519 7320

2.5 电邮地址

所有给 GovCERT.HK 的通讯均应电邮至 cert@govcert.gov.hk。

中华人民共和国香港特别行政区政府（下称「政府」）各局和部门应通过内部电邮系统，汇报所有信息安全事故。

2.6 公开密钥及信息保密

GovCERT.HK 与各局和部门之间会以 S/MIME 传输敏感数据。

GovCERT.HK 备有 PGP 密钥（公开密钥识别码：0x7D779220, 公开密钥指纹：93A6 1508 500A 73F8 4817 9721 FA29 2F03 7D77 9220）。该密钥现于以下网站及公开密钥服务器提供：

- GovCERT.HK 网站（网址：www.govcert.gov.hk）
- PGP.com 密钥服务器（网址：keyserver.pgp.com）
- 麻省理工学院 PGP 公开密钥服务器（网址：pgp.mit.edu）
- SKS OpenPGP 密钥服务器（网址：keys.gnupg.net）

2.7 中心成员

GovCERT.HK 团队的负责人是数字政策办公室（下称「数字办」）的总系统经理（项目管理及网络安全）。该团队由数字办的信息技术安全专业人员组成。

2.8 其他资料

有关 GovCERT.HK 的一般资料，可浏览 www.govcert.gov.hk 网站。

2.9 联络方法

如欲与 GovCERT.HK 联络，应先电邮至 cert@govcert.gov.hk。如需向 GovCERT.HK 紧急求助，请在电邮主题注明[紧急]二字。

3. 约章

3.1 使命宣言

GovCERT.HK 的使命是支援政府的信息及网络安全工作。

GovCERT.HK 的工作包括发放安全警报及预警；发出有关安全措施的建议；协调安全事故的处理及复原工作；以及加强市民的信息安全认知和教育。为提升区内信息及网络安全的能力，GovCERT.HK 亦会与其他计算机紧急事故应变小组及服务提供商合作，以便有效应对计算机安全事故，并交流良好作业模式。

3.2 服务对象

GovCERT.HK 是政府的电脑保安事故应变小组，专责为政府协调处理信息及网络安全事故。GovCERT.HK 的服务对象包括政府的各局和部门。

3.3 资助及／或联系

GovCERT.HK 是数字办辖下的工作单位。该中心是负责国家或地区计算机安全事务的计算机安全事故紧急应变小组，由政府全资设立。

GovCERT.HK 与香港网络安全事故协调中心（HKCERT）紧密合作，亦通过加入电脑紧急事故应变小组统筹中心（CERT/CC）、全球保安事故协调中心组织（FIRST）及亚太区电脑保安事故协调组织（APCERT），与其他负责国家或地区计算机安全事务的计算机安全事故紧急应变小组建立紧密关系。

3.4 负责当局

GovCERT.HK 隶属数字办，属政府的计算机安全事故应变小组。

4. 政策

4.1 安全事故种类和支援水平

GovCERT.HK 会视乎安全事故的种类、严重性、程度和以下的缓急次序，按适合的支援水平妥善协调所提供的资源，以减轻安全事故带来的影响。

1. 构成人命和人身安全威胁。
2. 危及敏感或关键资源。
3. 遗失或损毁重要资料并造成严重损失。
4. 系统损坏并导致长时间故障及复原成本高昂。
5. 服务中断。
6. 相关的局和部门或整个政府的公众形象受损。

4.2 合作、交流和信息公开

GovCERT.HK 会与本地执法机构、其他计算机紧急事故应变小组和机构合作，分享有关安全警报及威胁的信息。GovCERT.HK 会遵从交通灯协议（Traffic Light Protocol）的规定，与其他计算机紧急事故应变小组或机构交换敏感信息。

GovCERT.HK 会以限阅方式处理安全事故和部分系统漏洞的信息。已获授权的 GovCERT.HK 成员、负责受影响信息系统的信息安全人员及参与鉴证调查的调查人员才可交换和传送这些信息。事故所得的经验可分享给服务对象和其他计算机紧急事故应变小组。

4.3 通讯与认证

GovCERT.HK 会依照政府的相关规例和政策保护敏感信息。

传输的敏感信息会以 S/MIME 或 PGP 加密及签署。

5. 服务

5.1 事故应变

GovCERT.HK 将在技术方面协助各局和部门处理安全事故，特别是就安全事故管理中以下几个方面提供协助及建议：

5.1.1 事故分流

- 评估在政府内发生的安全事故的影响及程度。

5.1.2 事故协调

- 协调处理在政府内发生的安全事故，并提供建议。
- 协调相关持份者，就声称及真实的网络攻击加强应对措施。

5.1.3 事故处理

- 在有需要时向相关的局和部门提供建议或协助，以采取适当行动控制安全事故所造成的损害。
- 与相关的局和部门跟进处理安全事故的进展。

5.2 积极进行的工作

GovCERT.HK 协调和提供下列服务：

- 发放安全警报、安全建议及相关信息；
- 通过举办研讨会及培训课程，提高政府及公众对信息安全的认知；
- 协调预防性的漏洞扫描工作及网络安全演习；以及
- 与相关机构合作，分享最新的安全威胁及信息。

6. 安全事故报告表

本网站及内联网上的《信息安全事故处理实务指南》(ISPG-SM02)载有信息安全事故初步报告及事故事后报告的样本，以供服务对象参考。

7. 免责声明

GovCERT.HK 在拟备信息、通知及安全警报时已设法核对有关资料，但若本网站所提供的资料有任何错漏，或有人因使用相关资料而蒙受损失，GovCERT.HK 概不承担任何责任。

完