政府資訊科技總監辦公室

資訊保安

資訊保安事故處理

實務指引

[ISPG-SM02]

第 1.4 版

2023 年 6 月

版權公告

修改記錄

修改次數	修改詳情	經修改頁數	版本編號	日期
1	G54 資訊保安事故處理指引第 5.0 版已轉換成資訊保安事故處理實務指引。修改報告可於政府內聯網「資訊科技情報網」查閱：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	增加關於資訊科技保安管理的新章節及與其他實務指引保持參考上的一致。	整份文件	1.1	2017 年 11 月
3	詳細解釋政府資訊系統的範圍，以及舉例說明對事故的評估和決定。報告機制的表格亦作出輕微修改。	第 6 頁、26 頁、附件 C	1.2	2021 年 6 月
4	如發現有跡象顯示可能發生資訊保安事故，政府部門可咨詢政府資訊保安事故應變辦事處常設辦公室的建議。	第 20 頁、26 頁、附件 F	1.3	2022 年 9 月
5	更新個人資料私隱專員公署的《資料外洩事故通報表格》的超連結。	第 28 頁	1.4	2023 年 6 月

目錄

1. 簡介

有效的資訊保安管理包括識別、防範、偵測、應變和復原的互相配合。除部署強而有力的保安保護措施外，決策局／部門還應具備事故應變能力，以備在發生資訊保安事故（以下簡稱為保安事故或事故）時啟動適當程序。適當及預早的計劃能確保人員知悉、協調及有系統地進行事故應變和復原活動。決策局／部門須建立、記錄、測試及維護一套本身資訊系統的保安事故應變／報告程序。

1.1 目的

本文件就資訊保安事故處理計劃的制訂，以及資訊保安事故的防範、偵測及應變，為管理、行政及其他技術和操作人員提供指導說明。由於不同資訊系統的資訊保安事故可能構成不同的影響和導致不同的後果，決策局／部門應根據其實際的操作需要，為本身的資訊系統制訂合適的資訊保安事故處理程序。

本文件旨在提供政府內部資訊保安事故處理的實際指引和參考，但並不包括對個別具體電腦硬件或操作系統平台的詳細技術描述。決策局／部門應就有關技術細節諮詢相關的系統管理員、技術支援人員和產品供應商。

1.2 參考標準

以下的參考文件為本文件在應用上的參考：

- 香港特別行政區政府《基準資訊科技保安政策》[S17]
- 香港特別行政區政府《資訊科技保安指引》[G3]
- Information technology - Security techniques - Information security management systems –Overview and vocabulary (fourth edition), ISO/IEC 27000:2016
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management, ISO/IEC 27035-1:2016
- Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response, ISO/IEC 27035-2:2016

1.3 定義及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用的及以下的定義及慣用詞。

縮寫及術語	
資訊保安事件	發生可能違反資訊保安或控制失效的情況。
資訊保安事故	會對政府資訊系統及／或數據資產造成傷害，或會損害其運作的一個或多個相關的及已證實資訊保安事件。

1.4 聯絡方法

1.4.1 一般聯絡

本文件由政府資訊科技總監辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@ogcio.gov.hk

Lotus Notes 電郵： IT Security Team/OGCIO/HKSARG@OGCIO

CMMP 電郵： IT Security Team/OGCIO

有關更多政府事故處理聯絡資料，請參閱政府內聯網「資訊科技情報網」的「資訊科技保安專題」網頁
(https：//itginfo.ccgo.hksarg/content/itsecure/sih/contacts.shtml)。

2. 資訊保安管理

資訊保安是關於保安控制和措施的規劃、實施和持續提升，以保護資訊資產的機密性、完整性和可用性，適用於資訊的存儲、處理或傳輸過程及其相關資訊系統中。資訊保安管理是一套有關規劃、組織、指導、控制的原則和應用這些原則的法則，來迅速有效地管理實體、財務、人力資源和資訊資源，以及確保資訊資產和資訊系統的安全。

資訊保安管理涉及一系列需要持續監測和控制的活動。這些活動包括但不限於以下的範疇：

- 保安管理框架與組織；
- 管治、風險管理和遵行要求；
- 保安操作；
- 保安事件和事故管理；
- 保安意識培訓和能力建立；和
- 態勢感知和資訊共享。

保安管理框架與組織

決策局／部門須根據業務需要和政府保安要求，制定和實施部門資訊保安政策、標準、指引和程序。

決策局／部門亦須界定資訊保安的組織架構，並為有關各方就保安責任提供清晰的定義和適當的分配。

管治、風險管理和遵行要求

決策局／部門須採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。

決策局／部門須定期和在必要時對資訊系統和生產應用系統進行保安風險評估，以識別與保安漏洞相關的風險和後果，並為建立具成本效益的保安計劃和實施適當的保安保護和保障措施提供依據。

決策局／部門亦須定期對資訊系統進行保安審計，以確保當前的保安措施符合部門資訊保安政策、標準和其他合約或法律上的要求。

保安操作

為保護資訊資產和資訊系統，決策局／部門應根據業務需要實施全面的保安措施，涵蓋業務上不同的技術領域，並在日常操作中採取「預防、偵測、應變和復原」原則。

- 預防措施避免或阻止不良事件的發生；
- 偵測措施識別不良事件的發生；
- 應變措施是指在發生不良事件或事故時，採取相應行動來遏制損害；和
- 復原措施是將資訊系統的機密性、完整性和可用性恢復到預期狀態。

保安事件和事故管理

在現實環境中，由於存在不可預見並致服務中斷的事件，故此保安事故仍可能會發生。若保安事件危及業務的連續性或引起數據保安風險，決策局／部門須啟動其常規保安事故管理計劃，以實時識別、管理、記錄和分析保安威脅、攻擊或事故。決策局／部門亦應準備與有關各方適當地溝通，透過分享對有關保安風險的應變以消除不信任或不必要的猜測。當制定保安事故管理計劃時，決策局／部門應規劃和準備適當的資源，並製定相關程序，以配合必要的跟進調查。

保安意識培訓和能力建立

因為資訊保安是每個人的責任，所以決策局／部門應不斷提升機構內的資訊保安意識，透過培訓及教育，確保有關各方了解保安風險，遵守保安規定和要求，並採取資訊保安的良好作業模式。

態勢感知和資訊共享

因應網絡威脅形勢不斷變化，決策局／部門亦應不斷關注由保安行業和政府電腦保安事故協調中心發布的現時保安漏洞訊息、威脅警報和重要通知。應將即將或已經發生具威脅的保安警報傳達及分享給決策局／部門內的負責同事，以便採取及時的應對措施來緩解風險。

決策局／部門可以利用網絡風險資訊共享平台接收和分享保安事務、保安漏洞和網絡威脅情報的訊息。

人員亦可以通過參與保安演習和參加研討會、展示會或瀏覽載有保安情報資訊（例如網絡風險資訊共享平台）和一般保安資訊（例如網絡安全資訊站、資訊安全網）的專頁來提高保安意識。

3. 保安事故處理簡介

在資訊保安管理中，「保安操作」職能範疇包括適當地部署保安保護和保安措施以降低成功攻擊的風險。但是，儘管採取了這些措施，保安事故仍會發生。故此，資訊保安事故處理計劃應預先準備，這是保安事件與事故管理下的一個主要範疇。一旦服務下降或暫停，這些計劃能幫助決策局／部門對事故做好應對和恢復服務的準備。應當委派適當的人員和各按其職、預留資源和規劃好處理程序，以應付保安事故。預先的準備將有助於回應保安事故，並能讓資訊系統以更有組織、有效率和有效地恢復。

3.1 資訊保安事故

保安威脅是指可能會為資訊資產、系統及網絡帶來負面影響（例如利用資訊系統或網絡的漏洞）的潛在事件或任何情況。資訊保安事件是指可能違反資訊保安或控制失效的事件。資訊保安事件的發生並不一定代表攻擊成功。不是所有資訊保安事件都會被分類為資訊保安事故。「資訊保安事故」一詞在本文件中指會對政府資訊系統（包括由政府提供和負責維護的資訊系統，不論該資訊系統是在政府內部或以外推行）及數據資產造成傷害，或會損害其運作的一個或多個相關的已證實資訊保安事件。例如，資訊保安事故可以是指不合乎政府利益的資料泄漏，或資訊系統及／或網絡內的負面事件，而且對電腦或網絡保安的機密性、完整性和可用性構成影響。本實務指引的重點是資訊保安相關的事故，自然災害、硬件／軟件故障、數據線故障、停電等負面事件並不包括在本實務指引範圍內。這些負面事件應通過相關系統維修和運作復原計劃處理。

常見的保安事故包括：拒絕服務攻擊、入侵資訊系統或數據資產、保密資料在電子形態下泄漏、惡意破壞或竄改數據、濫用資訊系統、大規模感染惡意軟件、網站遭塗改，以及影響聯網系統的惡意腳本程式。

下圖解釋威脅、保安事件及保安事故之間的關係：

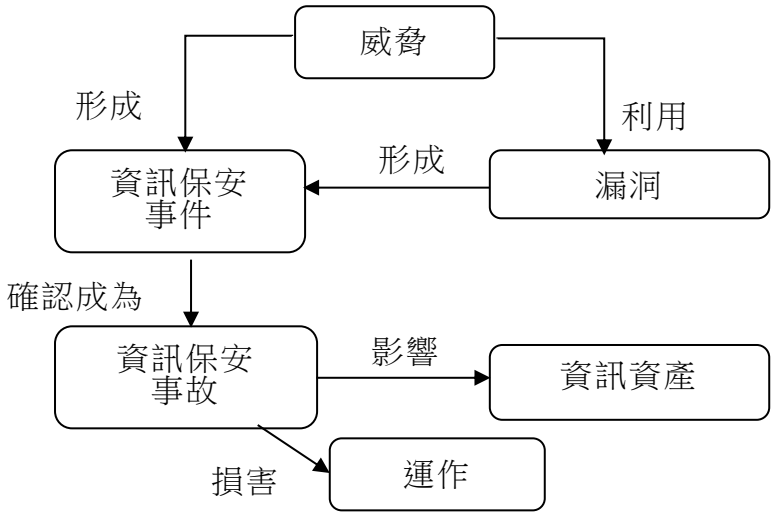


圖 3.1 保安事件及保安事故的關係

3.1.1 保安事故處理

保安事故處理是一系列持續進行的程序，規管保安事故發生前、發生時和發生後所採取的措施。

保安事故處理始於規劃和準備資源，以及制訂適當程序（例如升級處理和保安事故應變程序），以備日後遵照執行。

一旦保安事故被識別，負責保安事故應變的各方須按照預定程序實施應變。保安事故應變是指為處理保安事故並恢復系統的正常操作狀態，而進行的工作或採取的措施。

保安事故過後，應採取跟進行動對事故進行評估，並加強保安保護措施，以防止再度發生事故。應覆檢規劃和準備的工作，並作出相應的修訂，以確保有足夠的資源（包括人力資源、設備和技術知識）和有妥善制訂的程序處理日後的同類事故。

3.2 保安事故處理的目的

明確清晰的保安事故處理計劃對高效益及有效處理保安事故至為重要。它能於保安事故發生時減少影響和破壞，並有助迅速復原系統的運作。保安事故處理的主要目的如下：

- 確保具備處理事故所需的資源（包括人力資源、技術等）。
- 確保負責保安事故處理的各方明確了解，在發生保安事故時應按預定程序進行的工作。
- 確保事故應變有條不紊並具效益，而且能夠迅速復原受襲系統。
- 確保事故應變工作已獲確認和互相配合。
- 盡量減少泄漏資料、破壞資料和系統中斷等事故可能造成的影響。
- 在適當情況下，分享事故應變經驗。
- 防止受到進一步的攻擊和破壞。
- 處理相關的法律問題及在認為有需要時轉介警方作刑事調查。
- 若涉及個人資料，應向個人資料私隱專員公署報告。
- 在切實可行範圍內盡量保存資料作調查之用。

鑒於資訊科技在政府內部迅速發展，所有決策局／部門都必須制訂一套保安事故處理計劃，尤其是設有下列資訊系統的決策局和部門：

- 與外部（例如互聯網）連接的系統。
- 處理敏感數據和資料的系統。
- 關鍵任務系統。
- 任何可因保安事故的發生而受重大不良影響的系統。

3.3 披露事故資訊

除向負責處理保安事故及系統保安工作，或獲授權參與調查電腦罪行或濫用電腦事故的人士外，所有人員不得向任何人士披露有關電腦罪行及濫用電腦事故中的受害人、決策局／部門、受影響系統或造成該次事故的系統保安漏洞和入侵方法的資料。

披露任何事故資訊，包括被攻擊的方法、系統背景資料如實體位置或操作系統等，可能會鼓勵黑客入侵具有相同漏洞的其他系統，亦可能會影響警方偵查時的鑑證及檢控工作。但是，在事故事後分析之後，可能會得出防止類似保安事故的行動建議。如果建議內不包含個人、決策局／部門和系統發生事故的具體資訊，便可以在政府內分享，讓其他決策局／部門也可以防止類似的事故，並改善其保安處理程序。

4. 組織架構

下圖所示為政府內部保安事故應變組織架構的通用參考模型。

根據基準資訊科技保安政策，每個決策局／部門須成立一個資訊保安事故應變小組以協調處理與決策局／部門有關的資訊保安事故。政府資訊保安事故應變辦事處則集中統籌並支援各決策局／部門內部的資訊保安事故應變小組。各決策局／部門的資訊保安事故應變小組負責監督決策局／部門內部特定資訊科技系統、電腦服務或職能範圍的事故處理程序。

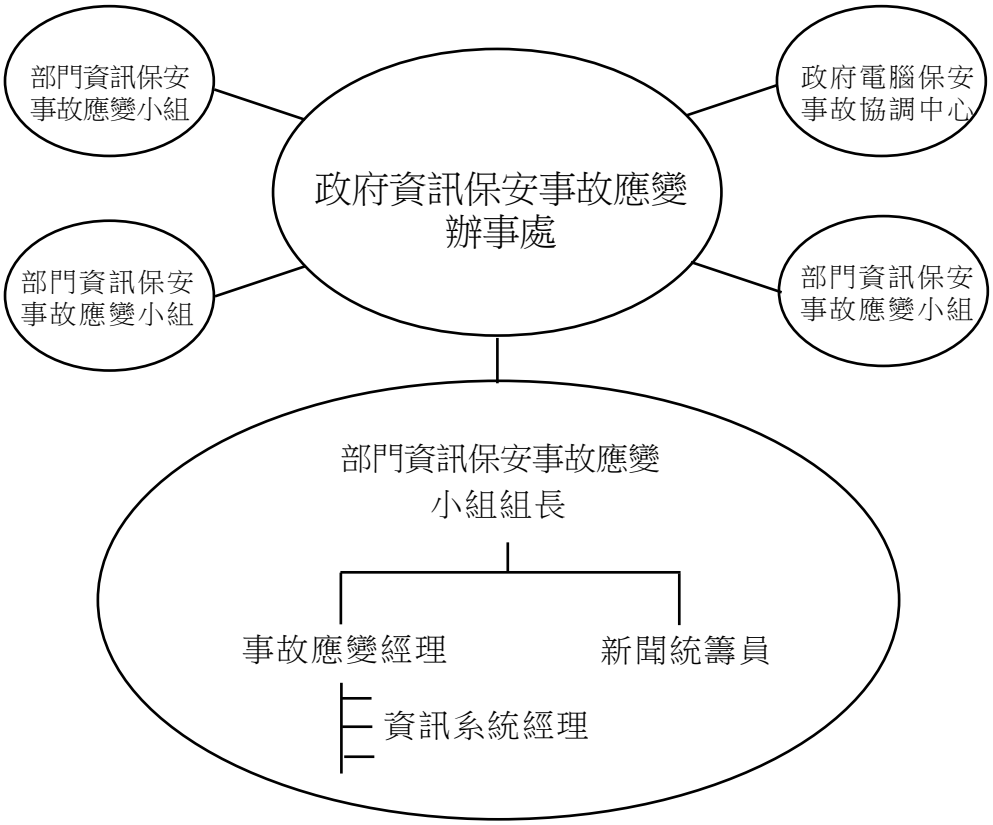


圖 4.1 參與保安事故處理的各方

本章闡述資訊保安事故處理的高層次組織架構和參與資訊保安事故處理工作各方的職務和職責。資訊保安事故應變小組及負責部門資訊系統的人員，應根據決策局／部門或相關系統的特殊業務需要和操作要求，制訂詳細的資訊保安事故處理程序。

4.1 政府資訊保安事故應變辦事處

政府資訊保安事故應變辦事處（GIRO）是為整個政府提供服務的組織，負責中央統籌及支援各個決策局／部門內的資訊保安事故應變小組，以處理資訊保安事故。

政府資訊保安事故應變辦事處常設辦公室扮演政府資訊保安事故應變辦事處的執行機構。政府資訊保安事故應變辦事處常設辦公室主要功能包括：

- 在資訊保安事故報告中扮演資訊保安事故應變小組組長的中心聯絡點，以及為可能涉及整個政府的資訊保安事故作應變協調。
- 就事故跟進進度，以及提醒相關的部門資訊保安事故應變小組提交事後報告及中期報告。
- 與政府電腦保安事故協調中心緊密合作，並在有需要時尋求對方建議。
- 若涉及刑事行為，與香港警務處網絡安全及科技罪案調查科緊密合作。

4.1.1 政府資訊保安事故應變辦事處的職能

政府資訊保安事故應變辦事處主要有以下職能：

- 設立中央數據庫，並監督政府內部對所有資訊保安事故的處理。
- 定期編製政府資訊保安事故統計報告。
- 充當中央協調辦事處，以應付多點保安攻擊（即不同的政府資訊系統同時遭受攻擊）。
- 促使決策局／部門的資訊保安事故應變小組互相分享和交流資訊保安事故處理的經驗和資料。

4.1.2 政府資訊保安事故應變辦事處的結構

政府資訊保安事故應變辦事處的核心成員包括來自下列決策局／部門的代表：

- 政府資訊科技總監辦公室
- 保安局
- 香港警務處

視乎不同保安事故的性質，必要時可能會邀請個別決策局／部門的資訊保安事故應變小組成員和其他專家，為政府資訊保安事故應變辦事處的運作提供協助。

政府資訊保安事故應變辦事處常設辦公室負責為政府資訊保安事故應變辦事處提供秘書處和職能方面的支援，並於應付可能影響整個政府的資訊保安事故時，擔任各部門資訊保安事故應變小組組長間的中心聯絡點，以收集資訊保安事故報告和統籌應變行動。

各決策局和部門須向政府資訊保安事故應變辦事處常設辦公室提供資訊保安事故應變小組組長的聯絡資料，如資料有任何更改，應向常設辦公室提供最新的資料，以確保資訊有效傳遞。部門資訊科技保安聯絡資料更新表載於**附件 A**。

政府資訊保安事故應變辦事處在必要時可成立特殊專責小組（例如在發生多點攻擊時），就影響遍及多個決策局／部門及／或政府整體運作和穩定的保安事故，協調應變工作。

4.2 政府電腦保安事故協調中心

政府電腦保安事故協調中心於 2015 年 4 月成立，與政府資訊保安事故應變辦事處常設辦公室合作，負責協調政府內部的資訊和網絡保安事故。該中心還與其他電腦應變小組合作共享事故資訊和威脅情報，並互相交流良好實踐及做法，以加強該地區的資訊和網絡保安能力。政府電腦保安事故協調中心具有以下主要功能：

- 就即將發生和實際威脅，向決策局／部門發出保安警報。
- 作為電腦保安事故協調中心與其他電腦應變小組合作在處理網絡保安事件時的橋樑。

4.3 部門資訊保安事故應變小組

根據基準資訊科技保安政策，各決策局／部門須成立資訊保安事故應變小組。該小組是決策局／部門內部負責協調、傳訊和採取保安事故處理行動的協調中心。資訊保安事故應變小組的規模應按不同決策局／部門資訊系統的規模和範圍、系統的敏感程度以及保安事故對決策局／部門的潛在影響，作出相應調整。

雖然政府資訊保安事故應變辦事處負責集中統籌資訊保安事故的報告，並為個別資訊保安事故應變小組提供協調和諮詢支援，但各決策局／部門的資訊保安事故應變小組，仍須在處理決策局／部門內發生的保安事故時，負責整體指揮和控制。

4.3.1 資訊保安事故應變小組的職能

資訊保安事故應變小組的主要職能應包括：

- 整體監督和協調決策局／部門內部所有資訊科技系統的保安事故處理。
- 在報告保安事故方面，與政府資訊保安事故應變辦事處合作，以便中央記錄和採取必要的跟進行動，例如報告警方作進一步罪案調查。
- 轉發政府資訊保安事故應變辦事處就即將發生及已經發生的事故所發放的警報，給決策局／部門內部負責有關工作的各方人士。
- 促進決策局／部門內部就保安事故處理，以及其他相關事務分享經驗和交流資訊。

4.3.2 資訊保安事故應變小組的結構

資訊保安事故應變小組是決策局／部門內協調所有資訊科技保安事故的中央聯絡點。決策局／部門首長應從高層管理人員中挑選一名人員，擔任資訊保安事故應變小組組長。組長應有權任命資訊保安事故應變小組的核心成員。

在籌組資訊保安事故應變小組時，部門資訊科技保安主任應給予建議和支持，以協助資訊保安事故應變小組組長為部門資訊系統制訂個別系統的特定保安政策和事故處理計劃，並制訂相關的後勤安排。部門資訊科技保安主任還須確保所在決策局／部門的所有資訊系統，已遵守和履行部門整體資訊科技保安政策的規定。

雖然資訊保安事故應變小組可根據決策局／部門的不同電腦設備情況，決定小組成員的實際組合，但資訊保安事故應變小組內也有一些必要的關鍵職務，包括資訊保安事故應變小組組長、事故應變經理、新聞統籌員和資訊系統經理等。這些職務可由多人或一人負責。

下文將詳述資訊保安事故應變小組內各項職務及職能。

4.3.3 資訊保安事故應變小組成員的職責

4.3.3.1 組長

組長的職責包括：

- 全面監督及協調處理決策局／部門內所有資訊系統的資訊保安事故。
- 根據事故應變經理提供的事故報告及分析，就控制損毀、系統復原、外部機構委聘及其所參與工作的程度，以及復原後恢復正常服務的後勤工作等關鍵事項作出決策。
- 因應事故對決策局／部門業務運作的影響，在適當情況下啟動部門的運作復原程序。
- 代表管理層批核為事故處理程序投放的資源。
- 代表管理層批核就事故的立場所作的公眾發布。
- 在報告資訊保安事故（特別是報告具有下列特點的資訊保安事故）方面，與政府資訊保安事故應變辦事處常設辦公室協調及合作，以便作中央記錄及採取必要的跟進行動：
  - (i) 直接提供公共服務的系統，而且系統故障可能導致服務中斷（例如向政府互聯網網站的拒絕服務攻擊）
  - (ii) 處理保密資料的系統
  - (iii) 支援關鍵任務操作的系統
  - (iv) 一旦發生保安事故，可能造成重大不良影響的系統，例如因網站遭塗改而使政府形象受損
- 促進決策局／部門內部互相交流和分享資訊保安事故處理及相關事宜的經驗和資料。
- 與調查機關協調及配合調查保安事故。

4.3.3.2 事故應變經理

事故應變經理負責監察決策局／部門內部的所有保安事故處理程序，並為處理事故程序尋求管理層提供資源和支持。事故應變經理的職責包括：

- 整體管理及監督決策局／部門內部與保安事故處理相關的所有事務。
- 在接獲影響部門資訊系統的保安事故報告後，通知資訊保安事故應變小組組長。
- 與資訊系統經理和有關方面跟進保安事故，彙編事故報告和進行分析。
- 向資訊保安事故應變小組組長匯報保安事故處理程序的進展情況。

- 在處理資訊事故時與警方、個人資料私隱專員公署、服務承辦商、服務支援供應商及保安顧問等外部機構和人士協調。
- 為事故處理工作，向資訊保安事故應變小組組長尋求提供所需的資源和支持。

4.3.3.3 新聞統籌員

新聞統籌員負責回覆公眾有關決策局／部門保安事故的查詢。新聞統籌員還負責整體控制和監督向公眾（包括傳媒）發布資訊的工作。

4.3.3.4 資訊系統經理

應撥出特定的資源來應付個別資訊系統、電腦服務或職能範圍可能發生的保安事故。

當處理資訊保安事故時，個別部門支援小組的規模和結構將視乎部門系統的範圍和性質而有所區別。舉例來說，就小型、非關鍵的內部系統而言，一人便已足以履行事故應變的職責。

對於個別部門的資訊系統，相關的部門資訊系統經理將監督整個系統保安事故處理流程或其職責範圍。經理應代表個別部門資訊系統下的支援小組，提供以下主要功能：

- 監督所負責職能範圍的保安事故處理程序。
- 事先制訂相關的事故處理程序和聯絡名單，以加快及推動處理程序。
- 提供直接接收可疑事故報告的途徑。
- 直接並即時回應可疑活動。
- 協助將破壞減至最少，並回復系統正常操作。
- 向服務承辦商、電腦產品供應商、警方或個人資料私隱專員公署等外部機構和人士尋求有關保安問題的意見。
- 與其他外部機構和人士協調相關資訊系統的保安事故處理工作。
- 就所負責職能範圍，對來自資訊保安事故應變小組和政府電腦保安事故協調中心的保安警報，進行影響分析。

如果資訊系統的部分操作或全部操作均已外判予外部服務供應商及／或已包括在其他政府部門提供的服務範圍內，則外判服務供應商及／或提供服務的部門亦應委任資訊系統經理及成立類似的支援小組以應對該特定的資訊系統，並提供與其職責相應的服務。

除提供以上主要功能，資訊系統經理應負責以下職務:

- 制訂及推行個別系統的保安事故應變程序。
- 遵守並遵從保安事故應變程序，向決策局／部門的資訊保安事故應變小組報告事故。
- 與服務供應商、承辦商和產品支援供應商等相關各方安排及協調，針對事故採取修正和復原行動。
- 向資訊保安事故應變小組報告保安事故，在資訊保安事故應變小組的管理支持下，於調查和收集證據的過程中對外尋求協調，例如尋求警方、個人資料私隱專員公署或香港電腦保安事故協調中心的協助。
- 掌握最新的資訊保安科技和技術，並了解與系統或所負責職能範圍相關的最新保安警報和保安漏洞。
- 利用保安工具／軟件及／或系統記錄並檢查審計追蹤記錄，找出可疑的攻擊或未獲授權的接達。
- 在診斷問題和復原系統過程中，提供有助於證據收集、系統備份和復原、系統配置和管理等技術支援。
- 為資訊系統安排定期保安評估、影響分析和覆檢。

5. 保安事故處理步驟概覽

保安事故處理共有 5 個主要步驟，有關概述見下文。各步驟所涉及的過程在相應章節會有更詳細描述。

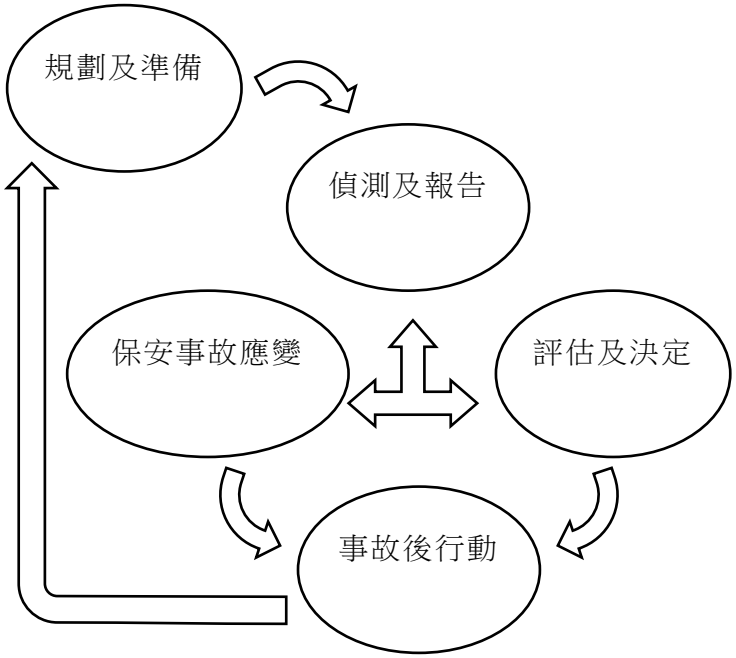


圖 5.1 保安事故處理的循環過程

A. 規劃和準備（第 6 章）

在這步驟中，決策局／部門應規劃和準備資源，並制訂適當程序，以備日後遵照執行。本步驟涉及的主要活動如下。

- 保安事故處理計劃
- 報告程序
- 升級處理程序
- 保安事故應變程序
- 培訓與教育
- 事故監察措施

B. 偵測及報告（第 7 章）

在這步驟中，決策局／部門應根據建立的檢測和監控機制檢測保安事件。決策局／部門也應遵循報告程序，使保安事件得到部門資訊保安事故應變小組的關注。這一步有兩個主要的活動：

- 偵測措施
- 報告

C. 評估及決定（第 8 章）

偵測到事件後，決策局／部門應確定是否真有事故發生。如果事件被識別為資訊保安事故，決策局／部門應確定事故的類型，並評估其範圍、損害和影響，以有效處理事故。決策局／部門還應遵循事先規劃的升級處理程序通知相關方面，並將事件升級到適當的級別。這步驟涉及的主要活動有：

- 事故評估
- 升級處理

D. 保安事故應變（第 9 章）

當識別到保安事故時，決策局／部門應遵循保安事故應變程序，採取行動處理保安事故，恢復系統正常運作。應變程序大致分為三個階段：

- 遏制
- 杜絕
- 復原

E. 事後跟進（第 10 章）

事故結束後，應採取後續行動對事故進行評估，加強保安防範，防止再次發生。主要後續行動如下：

- 事故事後分析
- 保安事故報告
- 保安評估
- 覆檢現行的保護措施
- 調查及檢控

6. 規劃和準備

適當的事先規劃可確保人員對應採取的事故應變及復原行動有所瞭解，使其能在互相配合及有條不紊的情況下執行。決策局／部門須備存最新資訊系統清單，當中附有保安事故處理的緊急聯絡點。及早計劃還有助決策局／部門在處理保安事故時作出適當和有效的決定，從而將保安事故可能造成的破壞減到最少。保安事故應變計劃包括加強保安保護措施、採取適當的事故應變、系統復原和其他跟進工作。

規劃和準備所涉及的主要工作如下：

- 保安事故處理計劃
- 報告程序
- 升級處理程序
- 保安事故應變程序
- 培訓與教育
- 事故監察措施

保安事故處理準備工作清單列於**附件 B**，以供參考。

6.1 保安事故處理計劃

保安事故處理計劃應符合基準資訊科技保安政策及資訊科技保安指引，一般應涵蓋以下幾個主要部分：

- 範圍
- 目標和優先處理事項
- 職務和職責
- 限制

6.1.1 範圍

這部分為界定保安事故應變小組的職能範圍。有關範圍既可包括整個決策局／部門（即資訊保安事故應變小組），亦可局限於決策局／部門內部的特定資訊系統或應用程式。

6.1.2 目標和優先處理事項

事先應明確制訂保安事故處理計劃的目標，並根據系統和管理需要為目標排列緩急次序。及後制訂的保安事故應變程序應配合這些預定的目標。

視乎不同系統和管理需要，事故處理的目標宜包括：

- 評估事故的影響和破壞
- 盡快使系統恢復正常操作
- 盡量減輕事故對其他系統的影響
- 避免發生同類事故
- 找出事故的根本成因
- 收集證據為日後的個案調查提供證明
- 有必要時更新政策和程序

部分事故的性質過於複雜或規模過大，以致難以在同一時間解決所有問題。為處理的事項訂定緩急次序便是一個關鍵步驟，讓事故應變人員可以聚焦先處理最關鍵事項。建議優先處理以下的事項：

- 保障生命和人身安全
- 保護關鍵資源
- 保護遺失或損毀後會造成較大損失的敏感或重要資料
- 防止停頓後會造成較大損失及復原成本較高的系統受到損壞
- 對服務中斷的影響減到最少
- 維護決策局／部門或政府整體的公眾形象

6.1.3 職務和職責

參與保安事故處理工作各方的職務和職責應明確界定。上述第 4 章為界定保安事故應變小組主要成員的職務和職責提供了參考模型。

6.1.4 限制

資源、科技和時間等限制因素應予考慮。這些限制可能影響保安事故處理工作的結果。舉例來說，決策局／部門如缺乏內部技術專才，便可能須委聘外部顧問或服務承辦商。這些準備工作應事先辦妥，確保在發生保安事故時能夠順利處理。

6.2 報告程序

應建立及記錄一套報告程序，清楚訂明任何可疑活動的報告步驟和程序，以便及時向有關各方作出報告。報告程序應列明詳盡的聯絡資料，例如電話號碼（包括辦公時間及非辦公時間內的聯絡電話號碼和流動電話號碼）、電郵地址和傳真號碼等，以確保負責人員之間能夠有效溝通。一些建議的報告機制載於**附件 C** 第 1 節，以供參考。

事先應制訂適當的報告程序，以便一旦發生保安事故，參與事故應變的全體人員知悉應向何人和以何種方式報告，以及應注意和報告的事項。

為有效執行報告程序，應注意以下幾點：

- 報告程序應載列明確的聯絡點，並制訂簡單但明確的步驟以便遵從。
- 向所有相關人員發布報告程序，以供參閱和參考。
- 確保所有相關人員熟習報告程序，並能夠立即報告保安事故。
- 編製保安事故報告表，以規範所收集的資料。
- 考慮是否需要在非辦公時間啟動報告程序，如確有需要，應制訂一份獨立的非辦公時間報告程序，並指定相關人員擔任非辦公時間聯絡人。
- 有關事故的資料應根據「有需要知道」原則披露，除資訊保安事故應變小組組長外，任何其他人士均無權閱覽，也不得授權他人將有關保安事故的資料與他人分享。

為改善資訊科技保安事故處理的效率和效益，當政府部門發現有跡象顯示可能發生資訊保安事故，可咨詢政府資訊保安事故應變辦事處常設辦公室的建議。**附件 F** 第 1 節載列了一些值得特別注意的典型事故跡象。

當證實發生資訊保安事故時，部門資訊保安事故應變小組需要：

- 於 **60 分鐘**內向政府資訊保安事故應變辦事處常設辦公室作電話滙報，並於 **48 小時**內提交完整的資訊保安事故初步報告表；
- 如保安事故牽涉關鍵電子政府服務、對保安有重大影響，或會引起傳媒注意，盡快向政府資訊保安事故應變辦事處常設辦公室分享以下資料：
  - (i) 事故類別及對事故範圍、破壞及影響的評估；
  - (ii) 為遏止破壞及修正問題而正在或將會採取的行動；
  - (iii) 若引起傳媒注意時的回應口徑；以及
  - (iv) 傳媒的查詢及回應建議（如有）。
- 每日向政府資訊保安事故應變辦事處常設辦公室更新受影響的關鍵電子政

府服務的修復狀況，直至服務恢復為止。

- 就任何已向香港警務處、個人資料私隱專員公署報告或向傳媒機構發布的保安事故，通知政府資訊保安事故應變辦事處常設辦公室。

應在解決事故後的 1 星期內，向政府資訊保安事故應變辦事處常設辦公室提交事故事後報告。對於需要較長時間完成調查的個案，有關的部門資訊保安事故應變小組需要就最新的修復情況及調查進度，每 3 個月向政府資訊保安事故應變辦事處常設辦公室提交中期報告：

- 於證實事故後 3 個月內向政府資訊保安事故應變辦事處常設辦公室提交第一份中期報告；以及
- 為令管理層獲悉狀況，每 3 個月向政府資訊保安事故應變辦事處常設辦公室提交事故調查進度，直到結案爲止。

6.3 升級處理程序

升級處理程序是指將事故上報管理層和有關方面，以確保立即作出重要決策的程序。

在發生事故時，往往需要處理大量緊急事項，所以很難找到適當人選處理林林總總的事項。為順利執行保安事故處理的各階段工作，應事先編備處理法律、技術和管理事項所需的重要聯絡名單。因此，制訂升級處理程序是準備和規劃階段的主要工作之一。

升級處理程序按事故的類別和影響的嚴重程度，載列內部和外部各級別人員的聯絡點及各聯絡點的聯絡資料。

就不同類別的事故，升級處理程序的聯絡點和跟進行動也可能有所區別。不同類別的事故涉及不同的專業知識或管理決策，所以應編備特定的聯絡名單以處理這些事故。

有關升級處理程序的建議和升級處理程序示例載於**附件 D**，以供參考。報告及升級處理政府資訊保安事故的工作流程示例載於**附件 E**，以供參考。

6.4 保安事故應變程序

保安事故應變程序界定了一旦發生事故應採取的步驟，其目的在於根據預定的目標和首要工作將破壞減至最少，杜絕事故的肇因，以及使系統恢復正常操作等。

須制訂及記錄保安事故應變程序，以便在事故處理程序中為保安事故應變小組提供指引。全體員工（包括管理層人員）均應知悉該程序，以作為參考和遵守的依據。這套程序應清晰明確而且容易理解，確保全體人員清楚了解應採取的行動。應變程序須定期進行測試和更新，以確保能迅速及有效地應對資訊保安事故。此外，演習須至少每兩年進行一次，最好每年進行一次，以評估程序的有效性。

有關事故應變演習流程及不同情景的行動卡詳情，請參閱政府內聯網「資訊科技情報網」的「資訊科技保安專題」網頁 (https://itginfo.ccgo.hksarg/content/itsecure/sih/actioncard/index.html) 。

第9章提供處理保安事故的參考模型，特別在遏制、杜絕和復原程序等方面。

6.5 培訓與教育

決策局／部門須確保全體員工均遵守及遵從保安事故的處理／報告程序。各人員應熟習由事故報告、確認、採取適當行動到恢復系統正常操作的處理事故程序。決策局／部門應定期舉行事故處理演習，使人員熟習有關程序。進行演習後，應對結果進行覆檢，並提出建議，以在適當情況下改善事故處理程序。

此外，為了加強系統或職能範圍的保安保護措施，並減低發生事故的機會，應向系統操作和支援人員提供足夠的培訓，使他們掌握有關保安預防的知識。由於終端用戶往往最先察覺問題發生，因此應鼓勵他們報告異常情況或涉嫌違反保安的情況。

6.6 事故監察措施

須採取足夠的事故監察保安措施以便在正常操作時保護系統，同時監察潛在的保安事故。所採取措施的程度和範圍則取決於系統、系統處理的資料及系統提供的功能的重要性和敏感程度。

下列是一些常見的保安事故監察措施：

- 安裝防火牆構件並採取認證和接達控制措施，以保護重要系統和數據資源。

- 安裝入侵偵測工具，主動監察、偵測並就系統入侵或黑客活動作出應變。
- 安裝抗惡意軟件和惡意軟件偵測及修復軟件，以偵測及清除惡意軟件，並防止惡意軟件影響系統操作。
- 定期利用保安掃描工具進行保安檢查，以找出目前存在的保安漏洞，並進行既定保安政策水平與實際保安工作環境之間的差距分析。
- 安裝內容過濾工具，以偵測電子郵件或網絡通訊的惡意內容或程式碼。
- 開啟系統及網絡審計記錄功能，以便偵測和追蹤未獲授權活動。
- 開發程式和腳本程式協助偵測可疑活動、監察系統和數據的完整性，以及分析審計記錄資料。
- 訂閱保安新聞、警示、漏洞資料、報告和其他有關資訊保安刊物，以提升對不斷湧現的保安威脅和相關風險的警覺。
- 維護及記錄漏洞管理機制，以識別、評估及減低保安風險。

7. 偵測及報告

7.1 偵測措施

決策局／部門應確保推行偵測及監察機制以偵測保安事件。決策局／部門應偵測資訊保安事件的發生，並輔以以下資料，就事件作出報告：

- 網絡監察裝置（例如防火牆、網絡流量分析工具或網頁過濾工具）的警示。
- 保安監察裝置（例如入侵偵測系統、入侵防禦系統、抗惡意軟件方案、記錄監察系統或保安資訊管理系統）的警示。
- 來自裝置、服務、主機及不同系統的記錄資料分析。
- 來自用戶或服務台的報告。
- 來自外來人士（例如其他資訊保安事故應變小組、電訊服務供應商、互聯網服務供應商、一般大眾、媒體或外聘服務供應商）的外部通知。

資訊保安事故應變小組應維護決策局／部門裡所有資訊保安事件的清單。

7.2 報告

人員應跟從報告程序，讓資訊保安事故應變小組注意有關保安事件。所有人員都須清楚知道及可以取得報告程序，以便報告不同種類的潛在資訊保安事件。下列資料應是報告資訊保安事件的依據：

- 偵測日期／時間
- 受影響系統
- 觀察
- 報告該保安事件人士的聯絡資料

8. 評估及決定

在發現可疑活動後，資訊系統的用戶、操作員或管理員應遵照既定的報告程序，向有關資訊系統經理報告事故。收集資料時可使用標準保安事故報告表，該報告表還可用作進一步調查和分析之用。另一方面，入侵偵測工具和系統審計記錄等監察工具亦可用來協助偵測未獲授權或異常活動。

在偵測到異常情況後，資訊系統經理應確認事故，此階段的工作包括以下步驟：

- 判斷是否發生事故，並進行初步評估
- 記錄事故
- 如有需要，記錄系統當前狀況

要決定是否發生事故，決策局／部門應考慮包括但不限於以下情況：

- 有關系統是否在政府內部推行；
- 如有關系統並非在政府內部推行，

(i) 該系統是否由政府提供和維護；以及

(ii) 事故是否由系統的保安漏洞或不受政府控制的因素造成；例如推行該系統的一方犯錯或違反政府的建議遺漏部分程序。

舉例來說，決策局／部門發現由其提供和維護的系統存在保安漏洞，而該系統並非在政府內部推行。其後，決策局／部門為保安漏洞提供修補程式，並通知推行該系統的用戶安裝。如果用戶沒有安裝，然後所推行的系統被黑客入侵，這通常不應視為政府保安事故。在類似情況下，如智能手機所安裝的流動應用程式已獲提供保安修補程式，但用戶沒有安裝該修補程式，該手機所發生的違反保安事件也不算保安事故。

8.1 事故評估

首先，資訊系統經理應判斷是否確實發生事故。然而，判斷所發現的異常情況是否就是發生事故的跡象往往十分困難。有些異常情況可能是由另外一些原因造成的（例如硬件故障或用戶操作錯誤）。

為判斷某種異常情況是系統問題還是真正事故所造成，資訊保安事故應變小組應收集有關資訊保安事件的資訊，並要求報告保安事件的人士作任何澄清。當政府部門發現有跡象顯示可能發生資訊保安事故，如有需要，可咨詢政府資訊保安事故應變辦事處常設辦公室的建議。**附件 F** 載列了一些值得特別注意的典型事故跡象、典型保安事故，以及決定事故範圍及影響時需考慮的因素，以供參考。

8.2 升級處理

在某事件被識別為資訊保安事故後，系統經理應判斷事故的類別、評估事故的範圍、破壞和影響，以便作出有效的應變。了解事故的類別有助確定處理事故的適當應變措施。此外，根據所造成的破壞和影響，還可立即採取一些預防或防衛措施。

相關的資訊系統經理與負責整體協調的資訊保安事故應變小組事故應變經理應通知適當人士，及跟從之前訂立的升級程序，將事故提升至適當級別。

在升級處理過程中，建議在描述事故時提供下列資料：

- 簡單描述事故：什麼事故、事故在何時發生、系統如何受到攻擊、所造成的破壞／影響。
- 說明攻擊者（如有）是否仍在系統中活動。
- 系統資料，例如系統名稱、功能，和主機名稱、互聯網規約地址、操作系統及版本等其他技術資料。
- 補充資料（如有需要），例如擷取的屏幕畫面、系統訊息等。

在升級處理過程中提供的資料應明確簡潔、準確而真實。提供不準確、誤導或不完整的資料可能會妨礙應變程序，甚至令情況惡化。決策局／部門還應考慮可否對外提供某些敏感資料。

如果決策局／部門確認有事故發生，有關資訊保安事故應變小組組長應在確認事故後的 60 分鐘內，向政府資訊保安事故應變辦事處常設辦公室報告事故。

為便於記錄和協調事故處理工作，資訊保安事故應變小組組長還應提供一份資訊保安事故初步報告（請參閱**附件 C** 第 2 節），向政府資訊保安事故應變辦事處常設辦公室報告，包括但不限於下列各類資訊保安事故（有關詳情，請參閱**附件 F** 第 3 節）。

- 濫用資訊系統
- 入侵資訊系統或數據資產
- 拒絕服務攻擊（包括中央或部門互聯網通訊閘、電郵系統、政府網站及／或向公眾提供電子服務的系統）
- 泄漏電子保密資料
- 遺失存有保密資料的流動裝置或抽取式媒體
- 偽冒
- 大規模惡意軟件感染
- 勒索軟件
- 網站遭塗改

與保安無關的事故（如下所列）無須向政府資訊保安事故應變辦事處常設辦公室報告，而應該按照現行系統管理及操作的準則和程序處理。

- 系統受颱風、水浸、火災等自然災害影響
- 硬件或軟件問題
- 數據／通訊線故障
- 停電
- 例行系統關閉或維修時間
- 因管理／操作錯誤導致的系統故障
- 因系統或人為錯誤遺失或損毀保密資料
- 不影響政府系統和數據的欺詐電郵或網站

如發生對政府服務及／或形象構成重大影響的嚴重事故，政府資訊保安事故應變辦事處常設辦公室與資訊保安事故應變小組組長會密切監察事態發展。如果事故是針對整個香港特別行政區政府的多點攻擊，常設辦公室會立即通知政府資訊保安事故應變辦事處並採取必要的行動。

在處理資料外泄事故時，決策局／部門宜考慮採取補救措施如下：

- 立即收集有關外泄事故的重要資料。
- 採取適當措施，制止資料外泄。
- 評估造成傷害的風險。
- 考慮發出有關資料外泄的通報。

如果保安事故涉及個人資料，決策局／部門應盡快向個人資料私隱專員公署報告，《資料外洩事故通報表格》可於個人資料私隱專員公署網站下載 (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/forms/files/DBN_c.pdf)。通報表格亦可以透過網上方式遞交 (https://www.pcpd.org.hk/tc_chi/enforcement/data_breach_notification/dbn_form.html) 。

決策局／部門應盡可能通知受影響人士。如基於合理原因而不作出通報，必須得到決策局局長／部門主管的批准方可。

如果決策局／部門懷疑發生電腦罪案，應聯絡香港警務處網絡安全及科技罪案調查科。在向警方報告案件前，應事先徵求資訊保安事故應變小組高級管理層的意見和批准。此外，如果需要向警方或個人資料私隱專員公署報告保安事故，決策局／部門應通知政府資訊保安事故應變辦事處常設辦公室，以便作中央記錄和協調。

有關升級處理程序示例和有關保安事故升級處理程序的其他相關資料，請參閱**附件 D**。政府保安事故報告及升級處理工作流程闡述於**附件 E**，以供參考。

8.3 記錄事故

應記錄所有保安事故、已採取的行動和相關的行動結果。這些記錄應以加密、上鎖或接達控制方法妥善儲存。這些記錄有助確認和評估事故，為檢控提供證據，並為及後的事故處理階段提供有用的資料。整個保安事故應變過程都應保留記錄。為事故設定編號有助在整個事故處理過程中作跟進和追蹤。

事故記錄最低限度必須包括以下資料：

- 系統事件和其他相關資料，例如審計記錄
- 已採取的所有行動，包括日期、時間和參與行動人員
- 所有對外通訊，包括日期、時間、內容及有關各方

8.4 記錄系統狀況

在偵測到可疑活動後應以最快速度，並在技術和操作上可行的情況下記錄受襲系統的狀況。這些資料可防止攻擊者銷毀證據，並為日後的個案調查（例如收集法證證據）提供了證據。所記錄的系統資料可包括下列項目：

- 伺服器記錄、網絡記錄、防火牆／路由器記錄、接達記錄等系統記錄檔案
- 仍在進行活動的系統登入或網絡連接，以及有關程序狀態的資料
- 受襲系統影像，以供調查，並作為日後採取跟進行動的證據

9. 保安事故應變

保安事故應變涉及制訂程序評估事故並作出應變，盡快將受影響的系統元件和服務恢復正常。有關程序大致可分為 3 個階段：即下圖 9.1 所示的*遏制*、*杜絕和復原*。認識各階段具體工作有利於制訂有效的保安事故應變程序。

應變程序無須依足 3 個階段的次序進行，決策局／部門可因應本身的實際需要自行制訂應變程序各階段的次序。

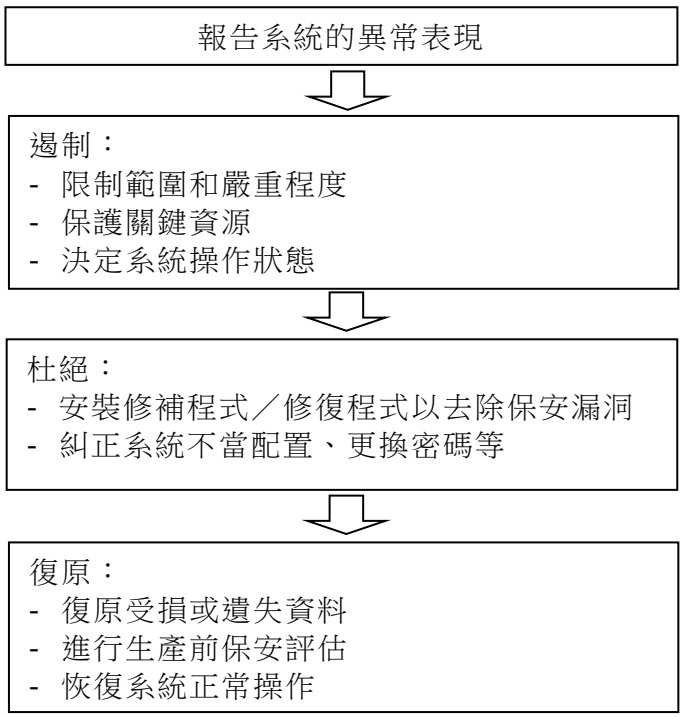


圖 9.1 保安事故應變的主要階段

9.1 遏制

事故應變的第一階段是遏制。遏制的目的是限制事故的範圍、嚴重程度和影響。有些事故，例如惡意軟件感染可迅速傳播，並造成大規模破壞。因此，在事故造成進一步破壞前，應限制事故的影響程度。

事先應清晰釐定並在保安事故應變程序中列明，針對不同的事故應採取哪種應變策略和程序，以及投入哪種資源。如果需要採取關鍵行動，便可能須要徵求資訊保安事故應變小組管理層的意見和批准（如有需要，資訊保安事故應變小組也可能須要諮詢政府資訊保安事故應變辦事處的意見）。

這一階段的工作宜包括：

- 評估事故對數據和資訊系統的影響，以確定有關的數據或資料是否已受事故破壞或感染。
- 保護敏感或關鍵資料和系統，例如將關鍵資料轉移至與受襲系統或網絡隔開的其他媒體（或其他系統）。
- 決定受襲系統的當前操作狀態。
- 複製受襲系統的當前映像，以供調查，並作為日後採取跟進行動的證據；
- 記錄這一階段採取的所有行動。
- 檢查共用網絡服務，或任何因可信賴關係而與受襲系統連接的系統。

9.1.1 決定受襲系統的當前操作狀態

有待作出的其中一項重要決定，是繼續還是終止受襲系統的操作和服務。這項決定在很大程度上取決於事故的類別和嚴重程度、系統要求、對公共服務和決策局／部門以至整個政府形象的影響，以及事故處理計劃內預定的目標和優先事項。

可採取的行動宜包括：

- 暫時關閉或隔離受襲的電腦或系統，以防止事故對互相連接的其他系統造成進一步破壞。這尤其是當事故會快速傳播時，當儲存敏感資料的電腦受到威脅時，又或是為了防止受襲系統被利用而向相連的系統發起攻擊。
- 終止受襲資訊系統的操作。
- 關閉系統的部分功能。
- 禁止用戶接達或登入系統。
- 繼續操作以收集有關事故的證據。該行動只適用於可承受某程度風險如服務中斷或數據受損的非關鍵任務系統，而且在處理時須格外小心，並加以嚴密監控。

9.2 杜絕

遏制後的下一個階段是杜絕。杜絕是指從系統清除導致事故的肇因，例如從受感染的系統和媒體清除惡意軟件。

在移除任何檔案或終止／刪掉任何程序前，宜收集所有必需的資料，包括所有記錄檔案、仍在進行活動的網絡連接及程序狀態資料。這將有助於為日後的調查收集證據，因為這些資料可能會在清理系統時被刪除或重新設定。

9.2.1 可杜絕事故的行動

在杜絕階段，決策局／部門宜根據事故的類別和性質及系統要求，採取以下行動：

- 終止或刪掉黑客在系統中產生或啟動的所有程序，以停止破壞及逼使黑客離開。
- 刪除黑客建立的所有偽冒檔案。系統操作員在刪除檔案前應將偽冒檔案作備分，以便日後調查。
- 清除黑客安裝的所有後門程式和惡意程式。
- 採用修補和修復程式修補在所有操作系統、伺服器和網絡設備等發現的保安漏洞。在系統恢復正常操作前，應徹底測試所採用的修補或修復程式。
- 糾正系統和網絡的不當設定，例如防火牆和路由器配置不當。
- 如發生惡意軟件事故，應遵照抗惡意軟件供應商的指引，在適當情況下，從所有受感染的系統和媒體清除惡意軟件。
- 確保備份未受感染，以免系統在下一階段利用備份復原系統時再度受到感染。
- 利用其他的保安工具，協助進行杜絕工作，例如利用保安掃描工具偵測入侵，並採用建議的解決方案。應確保使用具有最新檢測模式的保安工具。
- 更換所有可能被黑客接達的登入帳戶的密碼。
- 在某些情況下，支援人員可能須要將所有受感染的媒體重新格式化，並利用備份重新安裝系統和數據，尤其是在不確定事故對關鍵系統造成破壞的嚴重程度，或難以完全清理系統之時。
- 記錄已採取的所有行動。

以上所列只是在處理保安事故時常見的措施示例。杜絕行動視乎事故的性質及事故對受襲系統的影響而定。在某些情況下，決策局／部門可能須尋求外部機構（例如警方、個人資料私隱專員公署及／或外部服務供應商）的意見，並參考其他決策局／部門處理類似事故的經驗。此外，應尋求資訊保安事故應變小組和政府資訊保安事故應變辦事處的意見和協調。

9.3 復原

事故應變的最後階段是復原。本階段的目的在於恢復系統的正常操作。復原工作包括：

- 評估事故的破壞。
- 必要時從可信賴的來源取得檔案和資料，以重新安裝被刪除／遭破壞的檔案或整個系統。
- 在受控制的情況下，按照需求的緩急次序逐階段恢復功能／服務，例如可優先恢復最重要的服務或以大多數人為對象的服務。
- 檢驗復原操作是否成功，系統是否已恢復正常操作。
- 在恢復系統操作前，事先通知所有相關人士，如操作員、管理員、高級管理層和升級處理程序所涉及的其他人士等。
- 關閉不需要的服務。
- 記錄已採取的所有行動。

在系統恢復正常操作前，其中的一項重要工作是進行生產前保安評估，以確保受襲系統及其相關元件已安全。這項工作可能會運用到保安掃描工具，以確定事故的問題根源已清除，同時找出系統內任何可能存在的其他保安漏洞。視乎事故的嚴重程度和系統的服務水平要求，評估可集中處理某個領域，也可以涵蓋整個系統。

在進行一切復原工作前，須得到資訊保安事故應變小組高級管理層批准。如有需要，可尋求政府資訊保安事故應變辦事處的支持和意見。

10. 事故後行動

系統恢復正常操作並不代表保安事故處理程序的結束。採取必要的跟進行動是十分重要的。跟進行動包括評估事故所造成的破壞、改良系統以防止再度發生事故、更新保安政策和程序及為日後的檢控進行個案調查。

跟進行動可收以下效果：

- 改善事故應變程序。
- 改善保安措施，以保護系統日後免受攻擊。
- 向違法者提出檢控。
- 有助他人認識保安事故應變程序。
- 有助參與事故應變的各方人士汲取教訓。

跟進行動包括：

- 事故事後分析。
- 事故事後報告。
- 保安評估。
- 覆檢現行的保護措施。
- 調查及檢控。

10.1 事故事後分析

事故事後分析是對事故及事故應變措施的分析，以作為日後的參考。這項分析有助更深入地了解系統受到的威脅及可能存在的保安漏洞，以便採取更有效的保障措施。

分析的範圍包括：

- 防止再度受攻擊的建議行動。
- 迅速取得所需的資料及獲取有關資料的方法。
- 供偵測及杜絕程序所用或所需的額外工具。
- 準備和應變措施的足夠程度。
- 溝通的足夠程度。
- 實際困難。

- 事故的破壞，當中包括：
  (i) 處理事故所需的人力消耗
  (ii) 金錢成本
  (iii) 中斷操作的損失
  (iv) 遺失或遭破壞數據、軟件和硬件的價值，包括被泄露的敏感資料
  (v) 受託機密資料的法律責任
  (vi) 難堪或令信譽喪失
- 汲取的其他教訓。

10.2 事故事後報告

根據事故分析所編製的事故事後報告，應概述事故、應變、復原行動、破壞和汲取的教訓。相關資訊系統的經理負責編製報告，並提交資訊保安事故應變小組作參考，以便日後及時採取預防措施，避免其他系統和服務再度發生同類保安事故。

事故事後報告應包括下列項目：

- 事故的類別、範圍和程度。
- 事故的詳情：攻擊的來源、時間和可能方法，以及發現攻擊的方法等。
- 概述受攻擊的系統，包括系統範圍及功能、技術資料（例如系統硬件、軟件和操作系統，以及版本、網絡體系結構及程式編製語言等）。
- 事故應變及杜絕的方法。
- 復原程序。
- 汲取的其他教訓。

事故事後報告應在解決保安事故後的 1 週內提交予政府資訊保安事故應變辦事處。事故事後報告樣本載於**附件 C** 第 3.2 節，以供參考。

10.3 保安評估

可能受到保安風險威脅的系統宜定期進行保安風險評估和審計，尤其是曾經受保安事故影響的系統。保安覆檢及系統審計應持續進行，以便及時發現可能存在的保安漏洞及／或因應保安保護措施及攻擊／入侵科技的發展，而須作出的系統改善。

在發生保安事故時收集的資料亦有助於事後的保安評估，這對找出系統的保安漏洞和保安威脅尤其有用。

10.4 覆檢現行保護措施

根據事故事後分析與定期保安評估所得出的結果，可確認系統的保安政策、程序和保護機制中可改善的範圍。科技發展一日千里，所以必須定期更新保安相關政策、程序和保護機制，以確保整體保安保護措施對資訊系統的效用。在進行事故事後分析時，如有需要應覆檢和修訂政策、標準、指引和程序，以配合預防措施。

10.5 調查及檢控

在適當的情況下，還應對引起事故的個人採取個案調查、紀律處分或法律檢控等行動。

如經評估後，事故已構成刑事罪行，則應向香港警務處網絡安全及科技罪案調查科報告，以便展開個案調查和收集證據。在向警方報告案件前，應事先徵求資訊保安事故應變小組高級管理層的意見和批准。決策局／部門可能需要跟進法律程序及提供所需證據。

如果保安事故涉及個人資料，則決策局／部門應盡快向個人資料私隱專員公署報告。決策局／部門也應盡可能通知受影響的人。如基於合理原因而不作出通報，應得到決策局／部門主管的批准方可。

另外，對於向警方或個人資料私隱專員公署報告的任何保安事故，亦應通知政府資訊保安事故應變辦事處常設辦公室以進行中央記錄和協調支援。

完

附件 A：部門資訊科技保安聯絡人資料更新表

<table>
<tr><th colspan="2">決策局／部門名稱</th></tr>
<tr><td colspan="2"></td></tr>
<tr><th colspan="2">人員職務</th></tr>
<tr><td colspan="2">☐ 部門資訊科技保安主任
☐ 部門資訊科技保安副主任
☐ 部門資訊保安事故應變小組組長
☐ 部門資訊保安事故應變小組副組長</td></tr>
<tr><td colspan="2">更換人員:_____ (請為每位人員另備獨立表格)</td></tr>
<tr><th colspan="2">聯絡資料</th></tr>
<tr><td>姓名：</td><td>職位：</td></tr>
<tr><td>辦公室聯絡號碼：</td><td>流動電話號碼：
（作 7x24 緊急聯絡之用）</td></tr>
<tr><td colspan="2">電郵地址：</td></tr>
<tr><td colspan="2">收取資訊科技保安相關資料的其他電郵地址：</td></tr>
<tr><th colspan="2">遞交人</th></tr>
<tr><td>部門資訊科技保安主任／資訊保安事故應變小組組長* 姓名：</td><td>職位：</td></tr>
<tr><td>部門資訊科技保安主任／資訊保安事故應變小組組長* 簽署：</td><td>有效日期：</td></tr>
<tr><th colspan="2">送交政府資訊科技總監辦公室資訊科技保安小組</th></tr>
<tr><td colspan="2">請通過以下途徑向資訊科技保安小組遞交已填妥的表格：
電郵： it_security@ogcio.gov.hk
傳真號碼：2989 6073</td></tr>
</table>

**刪除不適用部分*

附件 **B:** 保安事故處理準備工作清單

B.1 保安事故處理準備工作清單樣本

	項目	詳情	進展情況
1	保安事故處理計劃	為保安事故處理制訂計劃	
2	報告程序	設計及準備報告機制	
		向全體人員頒布報告機制	
3	升級處理程序	收集需要聯絡／參與工作的全體人員（內部和外部）的聯絡資料	
		準備升級處理程序	
		向參與工作的全體人員頒布升級處理程序	
4	保安事故應變程序	準備保安事故應變程序	
		向參與工作的全體人員頒布保安事故應變程序	
5	培訓與教育	向操作及支援人員提供有關保安事故處理的培訓	
		確保各人員熟習事故應變程序	
6	事故監察措施	安裝防火牆設備和接達控制措施，以保護重要的系統和數據資源	
		安裝惡意軟件偵測及修復軟件，定期進行掃描並更新識別碼	
		安裝監察工具，例如入侵偵測系統	
		開啟系統及網絡設備的審計記錄功能	

附件 C: 報告機制

C.1 報告機制建議

電話熱線

這是最便利和快捷的報告事故途徑。部分系統可能已設有專門處理查詢及／或保安事故報告的電話熱線。

如果系統需要日夜不停運作，便可能需要提供 24 小時電話熱線服務。

電子郵件

通過電郵報告事故也是個有效的途徑。然而，如果發生屬於網絡攻擊或針對電郵系統的事故，以電郵報告的途徑便會受到影響。要解決這個問題，應採用其他的報告途徑，例如電話或傳真。

傳真號碼

通過傳真報告是一個補充機制，特別是當要提交可能無法通過電話清楚及準確地報告的詳細資訊。但是，透過傳真機報告事故應特別注意，最好由專人負責接收傳真。 此外，還應特別注意處理傳真報告，以防止向未經授權的人員披露事故。鑑於通過傳真報告的須留意這些額外的保安措施，為了更有效率和更具成本效益，通常會使用電子郵件來提交報告。

親身報告

這個辦法被認為沒有效率，而且還會構成不便。這只應用於，必須親身由報告事故的人員提供詳細資料或與報告事故的人員討論事故的情況，又或者事故地點與事故報告聯絡人的所在地十分接近，否則應避免採取親身報告的方式。

C.2 資訊保安事故初步報告

限 閱

事故參考編號： _____
（只供政府資訊保安事故應變辦事處常設辦公室填寫）

資訊保安事故初步報告

背景資料	
決策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
受影響系統的實體位置： ☐決策局／部門內部　☐ 外聘服務供應商設施 ☐中央服務：_____ **系統管理員／操作員：** ☐ 內部人員　☐ 終端用戶　☐ 外判服務供應商	
報告人資料	
姓名：	***職位：***
辦公室聯絡號碼：	***24 小時聯絡號碼：***
電郵地址：	***報告日期：***
事故詳情	
發生事故的日期／時間：	
發現事故的日期／時間：	**向政府資訊保安事故應變辦事處常設辦公室報告的日期／時間：**
事故說明： ***發生事情：*** _____	

初步調查結果（如有）：

發生經過：

_____

發生原因：

_____

已識別漏洞：

_____

類別：

☐ 濫用資訊系統
☐ 入侵資訊系統或數據資產
☐ 拒絕服務攻擊
☐ 泄漏電子保密資料
☐ 偽冒
☐ 遺失存有保密資料的流動裝置或抽取式媒體
☐ 大規模惡意軟件感染
☐ 勒索軟件
☐ 網站遭塗改
☐ 其他：_____

受影響組件／資產：

☐ 電郵系統
☐ 硬件
☐ 資料／數據
☐ 網絡
☐ 軟件
☐ 網站
☐ 其他：_____

受影響組件／資產詳情：

_____

影響：

☐ 機密性
☐ 完整性
☐ 可用性
☐ 政府形象
☐ 其他_____

請提供有關影響和中斷服務時間（如有）的詳情：

_____

事故有否涉及保密資料？

☐ 有，涉及 ☐限閱類別 ☐機密類別

☐ 沒有

請提供所涉及保密資料的詳情（例如數據是否加密、數據類型等）：

_____

事故有否涉及個人資料？

☐ 有，所涉及個人資料為：_____

☐ 沒有

已通知人士／單位：

☐ 資訊系統經理 ☐ 新聞統籌員

☐ 事故應變經理 ☐ 資訊保安事故應變小組組長

☐ 政府資訊保安事故應變辦事處常設辦公室 ☐ 其他：_____

已通知外部人士／單位（日期／時間）：

☐ 香港警務處網絡安全及科技罪案調查科：_____
檔案參考編號：_____

☐ 個人資料私隱專員公署：_____

☐ 其他：_____

為解決事故所採取的行動：

為解決事故所計劃的行動：

未進行的行動：

目前系統的狀況：

其他資料：

媒體／公眾查詢（如適用）	
媒體查詢數目：	**公眾查詢數目：**

C.3.1 事故中期報告

限 閱

事故參考編號：_____

（只供政府資訊保安事故應變辦事處常設辦公室填寫）

事故中期報告

背景資料	
決策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
受影響系統的實體位置： ☐ 決策局／部門內部　☐ 外聘服務供應商設施 ☐ 中央服務：_____ **系統管理員／操作員：** ☐ 內部人員　☐ 終端用戶　☐ 外判服務供應商	
報告人資料	
姓名：	***職位：***
辦公室聯絡號碼：	***24 小時聯絡號碼：***
電郵地址：	***報告日期：***
事故詳情	
發生事故的日期／時間：	
發現事故的日期／時間：	**向政府資訊保安事故應變辦事處常設辦公室報告的日期／時間：**
事故說明： ***發生事情***： _____	

調查結果：

發生經過：

_____

發生原因：

_____

已識別漏洞：

_____

最新狀況：

C.3.2 事故事後報告

限 閱

事故參考編號：_____

（只供政府資訊保安事故應變辦事處常設辦公室填寫）

事故事後報告

背景資料	
決策局／部門名稱：	
概述受影響的系統（例如功能、網址等）：	
受影響系統的位置： ☐ 決策局／部門內部 ☐ 外聘服務供應商設施 ☐ 中央服務：_____ **系統管理員／操作員：** ☐ 內部人員 ☐ 終端用戶 ☐ 外判服務供應商	
報告人資料	
姓名：	***職位：***
辦公室聯絡號碼：	***24 小時聯絡號碼：***
電郵地址：	***報告日期：***
事故詳情	
發生事故的日期／時間：	
發現事故的日期／時間：	**向政府資訊保安事故應變辦事處常設辦公室報告的日期／時間：**
事故說明： ***發生事情***： ––	

調查結果：

發生經過：

_____

發生原因：

_____

已識別漏洞：

_____

類別：

☐ 濫用資訊系統
☐ 拒絕服務攻擊
☐ 偽冒
☐ 大規模惡意軟件感染
☐ 網站遭塗改
☐ 入侵資訊系統或數據資產
☐ 泄漏電子保密資料
☐ 遺失存有保密資料的流動裝置或抽取式媒體
☐ 勒索軟件
☐ 其他：_____

受影響組件／資產：

☐ 電郵系統
☐ 資料／數據
☐ 軟件
☐ 硬件
☐ 網絡
☐ 網站
☐ 其他：_____

受影響組件／資產詳情：

_____

其他受影響場地／系統（如有）：

_____

影響：

☐ 機密性　　☐ 完整性

☐ 可用性　　☐ 政府形像

☐ 其他_____

請提供有關影響和中斷服務時間（如有）的詳情：

_____

已通知人士／單位：

☐ 資訊系統經理　　☐ 新聞統籌員

☐ 事故應變經理　　☐ 資訊保安事故應變小組組長

☐ 政府資訊保安事故應變辦事處常設辦公室　　☐ 其他：_____

已通知外部人士／單位（日期／時間）：

☐ 香港警務處網絡安全及科技罪案調查科：_____
檔案參考編號：_____

☐ 個人資料私隱專員公署：_____

☐ 其他：_____

香港警務處調查結果（如有）：

_____
_____

事件發生的次序：

日期／時間	*事件*

已採取的行動及結果：

目前系統的狀況：

參與人員：

姓名	*職位*	*電話號碼*	*電郵地址*	*職務*

肇事者（如有）詳情：

涉及的肇事者：

☐ 人　　☐ 組織

☐ 沒有肇事者　　☐ 不明

☐ 其他：_____

事故的懷疑動機：

☐ 經濟利益　　☐ 黑客攻擊

☐ 政治　　☐ 報復

☐ 不明　　☐ 其他：_____

惡意軟件（如有）詳情：

如事故涉及保密資料，請提供詳情（例如數據是否加密、數據類型等）：

保密資料：　☐限閱類別　☐機密類別

備註：

_____

_____

如事故涉及個人資料，請提供詳情（例如受影響人數、個人資料類別（如香港身份證號碼）、是否已通知受影響人士等）：

受影響人數：_____

（*內部人員和市民人數分項數字*）

個人資料類別：

_____

是否已通知受影響人士：是／否。 如否，原因： _____ 備註： _____
成本因素（包括因事故招致的損失和復原成本／人力資源）：
防止再度發生事故的建議行動：
汲取的教訓：

媒體／公眾查詢 （如適用）	
媒體查詢數目：	公眾查詢數目：

附件 **D:** 升級處理程序

D.1 需要通知的各方

升級處理程序內需要包括哪些人員，取決於事故的性質和嚴重程度，及系統要求。舉例來說，發生事故的初期可能只需要內部支援人員處理問題。其後可能需要通知高級管理層。如果問題仍無法解決，便可能需要視乎情況，尋求服務承辦商、產品供應商、警方及個人資料私隱專員公署等外部支援服務機構的意見。

應為各系統設定個別的升級處理程序和聯絡人，以滿足系統的特殊操作需要。

視乎系統受到的破壞或系統的敏感程度，在不同的階段可通知不同的人員。聯絡人包括，但不限於：

內部：

- 操作及技術支援人員
- 相關資訊系統的經理、資訊保安事故應變小組及政府資訊保安事故應變辦事處常設辦公室
- 其他受影響／有關聯的系統或功能操作人員
- 香港警務處網絡安全及科技罪案調查科
- 新聞統籌員，為準備對事故的立場和向傳媒發布的新聞稿

外部：

- 支援服務供應商，包括系統的硬件或軟件供應商、應用程式開發商和保安顧問等
- 服務供應商（例如電訊供應商、互聯網服務供應商）
- 個人資料私隱專員公署
- 受影響人士

D.2 聯絡名單

參與工作人員的聯絡名單應包括下列資料：

- 專責人員的姓名
- 職銜
- 電郵地址
- 聯絡電話號碼（按需要加入 24 小時聯絡號碼）
- 傳真號碼

D.3 升級處理程序示例

以下所列是資訊保安事故的升級處理程序示例。

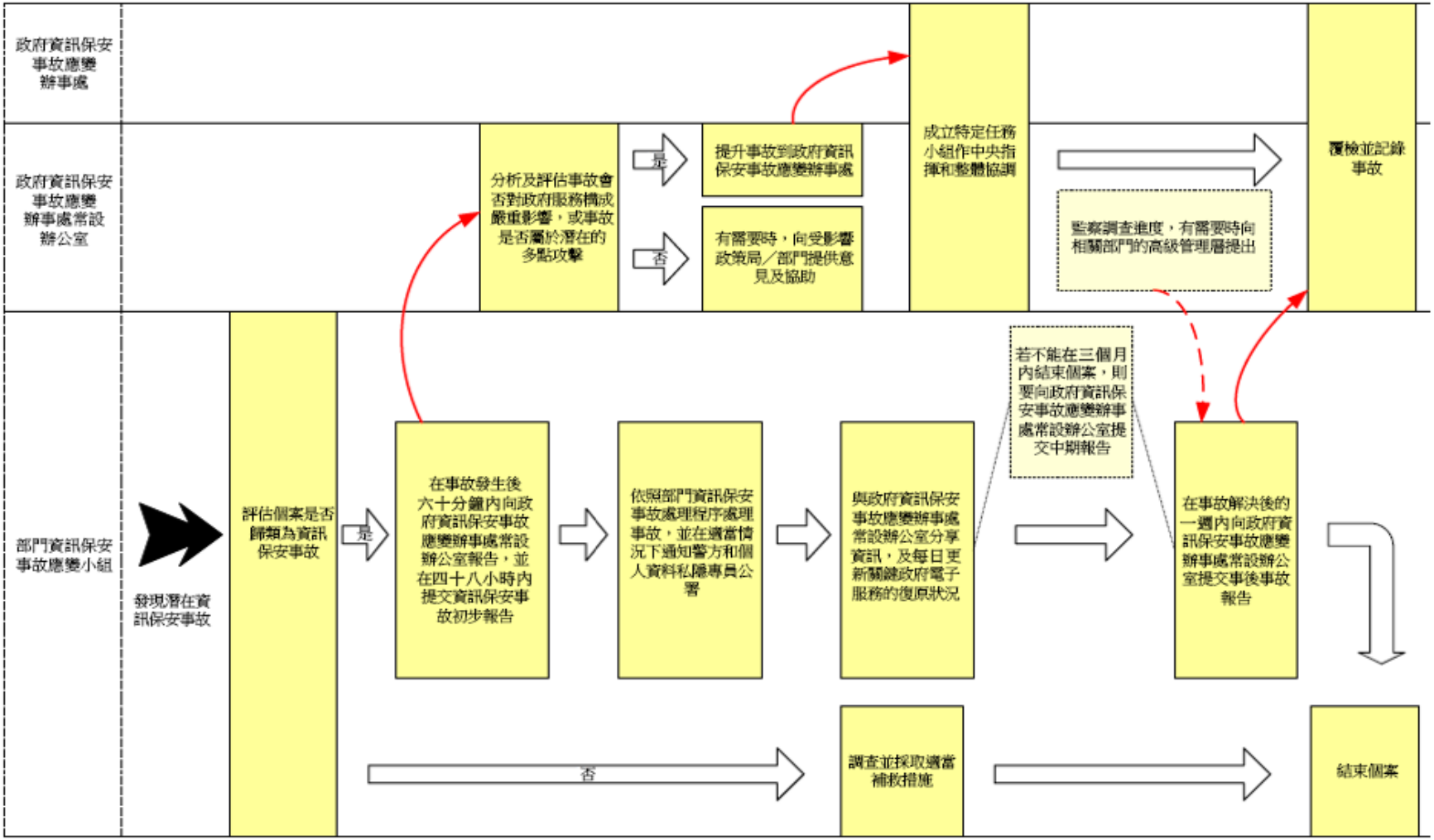
報告時限	**聯絡名單**	**聯絡方法**
事故發生後 15 分鐘內	有關的資訊系統經理、技術支援人員、提供支援的相關供應商和服務承辦商	*流動電話及供應商 24 小時電話熱線*
事故發生後 30 分鐘內	上述各人員及資訊保安事故應變小組的事故應變經理和新聞統籌員	*流動電話*
事故發生後 60 分鐘內	通知資訊保安事故應變小組組長	*流動電話*
事故發生後 60 分鐘內	資訊保安事故應變小組通知政府資訊保安事故應變辦事處 (及於事故發生後 48 小時內向政府資訊保安事故應變辦事處常設辦公室提供資訊保安事故初步報告)	*預設的電話熱線或電子郵件*
其後每 30 分鐘	向上述各人員匯報最新情況	*流動電話或電子郵件*
定期	資訊保安事故應變小組向政府資訊保安事故應變辦事處匯報事故的最新情況	*電子郵件*
系統復原後（1 星期內）	資訊保安事故應變小組向政府資訊保安事故應變辦事處遞交一份事故事後報告作記錄	*電子郵件*
如懷疑構成刑事犯罪，則由資訊保安事故應變小組決定	向警方舉報以調查案件	*預設的電話熱線*
如涉及個人資料	向個人資料私隱專員報告 （並盡可能通知受影響人士）	*預設的電話熱線或任何其他途徑*

報告應包括下列資料：

- 概括描述問題：發生何事、何時發生、如何發生及持續時間
- 表明系統是否受到攻擊
- 表明攻擊者（如有）是否仍在系統進行活動
- 表明攻擊是否來自本地
- 系統復原的最新進展情況

附件 E: 資訊保安事故應變機制的流程

下圖所示為政府保安事故報告及升級處理工作流程圖：



附件 F: 確認事故

F.1 保安事故的典型跡象

為判斷異常情況是由系統問題所造成，還是確實已發生事故，可留意保安事故一些特定跡象。保安事故的常見跡象包括下列任何或全部跡象：

與系統操作相關的跡象：

- 入侵偵測、抗惡意軟件或惡意軟件偵測工具所發出的系統警報或類似訊息
- 可疑的系統或網絡帳戶（例如用戶沒有經過正常程序而取得根接達權限）
- 帳戶資料錯漏
- 部分或全部系統記錄遺失或遭竄改
- 系統崩潰
- 系統性能突然大幅下降
- 未獲授權下執行程式
- 可疑的試探，例如多次的登入失敗
- 可疑的瀏覽活動，例如擁有根權限的帳戶接達不同用戶帳戶的多個檔案
- 系統時間出現預計以外的大幅偏差
- 網絡通訊量出現異常偏差（例如不尋常的網絡掃描活動）

與用戶帳戶相關的跡象：

- 預計以外的用戶帳戶之建立或刪除
- 以往使用頻率低的帳戶突頻繁使用
- 因帳戶遭竄改而無法登入
- 預計以外的用戶密碼更換
- 異常使用時間
- 對上一次登入或使用用戶帳戶的情況可疑
- 異常使用模式（例如沒有參與程式編製的用戶帳戶在編製程式）
- 電腦系統顯示奇怪的訊息
- 在無法解釋的情況下，不能接達電腦系統
- 大量載有可疑內容的回彈電郵
- 用戶報告收到恐嚇電郵訊息

與檔案及數據相關的跡象：

- 預計以外的檔案或數據之建立、竄改或刪除
- 陌生的檔案名稱
- 預計以外的竄改檔案大小或數據，尤其是系統的可執行檔案
- 預計以外的嘗試寫入系統檔案，或修改系統檔案
- 無法接達檔案和數據
- 在公開地方（例如打印機出紙口）發現無人看管的敏感資料

然而，單憑一種跡象未必可確定是否有事故發生。擁有豐富保安和技術知識的技術人員應參與判斷，以根據上述的一種或多種跡象確認事故。此外，在確認事故時，多人集思廣益作出的判斷往往優勝於一人作出的判斷。

F.2 為確認事故收集的資料

在確認事故時還應查閱下列資料：

- 系統記錄、防火牆／路由器記錄、伺服器記錄和入侵偵測系統記錄等審計追蹤或記錄檔案
- 仍在進行活動的網絡連接及系統程序狀態資料
- 有助調查人員更好地了解系統功能、網絡基本設施及對外連接情況的任何其他文件

F.3 事故類別

所有資訊保安事故都應予報告，下表列載一些保安事故的類別及其描述：

資訊保安事故	描述
濫用資訊系統	當有人利用資訊系統作非獲准用途，例如為資訊資產帶來負面影響，即已構成濫用。
入侵資訊系統或數據資產	在未得到系統擁有人批准的情況下，實體或邏輯接達整個或部分資訊系統及／或其數據。入侵可以經由不可信源頭的手動或透過自動化技術造成。
拒絕服務攻擊	蓄意或無意地妨礙使用資訊資源，以影響資訊資源的可用性。拒絕服務攻擊的例子包括 SYN 氾濫、致命小包和 Ping 氾濫，這些攻擊嘗試使資訊系統或網絡連接超出負荷，而無法向其用戶提供正常的服務。
泄漏電子保密資料	保密資料外泄，或被未獲授權人士接達。
遺失存有保密資料的流動裝置或抽取式媒體	流動裝置／抽取式媒體因意外或失竊而遺失。
偽冒	使用他人身份，以取得超出本身原有的資訊系統接達權限。
大規模惡意軟件感染	惡意軟件感染可以損毀檔案、刪改數據、加密檔案、秘密偷取數據、關閉硬件或軟件運作，或拒絕合法用戶接達等。決策局／部門須識別及評估是否對業務運作有嚴重影響。
勒索軟件	勒索軟件是一種通過加密以阻止和限制用戶接達其系統或檔案並要求付款解密的惡意軟件。
網站遭塗改	未獲授權竄改互聯網網頁的內容。

F.4 影響事故範圍和後果的因素

影響事故範圍和後果的因素包括：

- 事故的影響程度：影響單一系統還是多個系統
- 對公共服務及／或政府形象可能造成的影響
- 新聞媒體的介入
- 涉及犯罪活動
- 事故的潛在影響
- 是否涉及保密資料
- 事故的進入點，例如網絡、互聯網、電話線、局部終端機等
- 攻擊來自本地的可能性
- 預計事故後復原所需的時間
- 處理事故所需的資源，包括人員、時間和設備
- 造成進一步破壞的可能性