專題快訊
第 1 期

保護關鍵基礎設施電腦系統

立法會秘書處
議會事務部編製

2024 年
12 月

概覽

關鍵基礎設施涉及社會及經濟命脈，是**維持香港社會正常運作和維持市民正常生活**所必須的設施，例如銀行和金融機構、通訊網絡、供電設施、鐵路系統、醫療系統等。倘若其電腦系統受到惡意網絡攻擊而遭到破壞，或造成數據洩露，將影響該等設施的運作，甚至令整個社會停擺。

其他司法管轄區已訂立保障關鍵基礎設施電腦系統安全的**法規**。參考了其他司法管轄區的做法，香港政府建議就此訂立一條全新的法例，規定相關營運者必須履行有關架構、預防，及事故通報和應對的法定責任，確保各項重要服務的穩定運作。

本**專題快訊**簡介立法建議的原則和重點，並綜述當局因應諮詢期接獲的意見作出的回應，以及立法會的相關討論。

立法工作進程

2023 年：

- 政府當局聆聽持份者就初步建議立法框架的意見

2024 年：

- 7 月：政府當局就**建議立法框架**諮詢立法會保安事務委員會及**展開**為期 1 個月的**諮詢工作**
- 10 月：政府當局**向**立法會**保安事務委員會報告諮詢結果**，當局考慮議員及業界的意見後會敲定立法建議
- 12 月：政府當局向立法會提交**《保護關鍵基礎設施（電腦系統）條例草案》**，內務委員會同意**成立法案委員會**研究條例草案

2024 年若干關鍵基礎設施被網絡攻擊而對社會造成重大影響的事故

香港	有私營醫院的電腦系統被黑客用勒索軟件攻擊，導致電腦系統未能如常運作，影響部分醫療服務
瑞典	一所數據中心遭黑客攻擊，令政府及商戶的運作受到干擾
美國	有醫療保險公司受勒索軟件攻擊，部分醫療服務停頓，大量個人資料及醫療資訊有洩漏風險

立法建議的原則

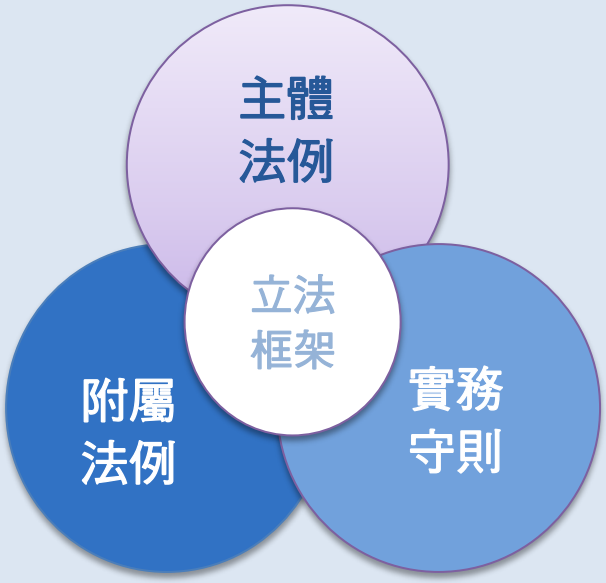
4 項原則

1 只涉及指定大型機構，**不影響個人或中小企**

2 只涵蓋香港設辦事處的營運者，**無域外效力**

3 索取資料以評估及應對事故，**不針對個人資料或商業機密**

4 以機構為單位，**無個人刑責**或監禁



訂明專員的權限或營運者法定責任和細節

訂明若干責任的建議標準，提供履行 3 類責任的實際指引

立法建議的重點

規管對象

- 維持香港社會必要服務，或重要的社會和經濟活動的**"關鍵基礎設施營運者"**及**其"關鍵電腦系統"**，規管對象以**機構為本**
- "關鍵基礎設施**營運者**"的**名單不會公開**，以免其成為網絡攻擊的目標
- **政府部門**必須嚴格遵循《保安規例》及《政府資訊科技保安政策及指引》，數字政策辦公室亦會定期為各部門進行遵循審核，故政府部門**無需納入規管**

被指定為"關鍵基礎設施"的 2 類設施

1. 在香港**提供必要服務**的基礎設施，涵蓋以下 **8 個界別**：

(1) 能源	(5) 航空交通
(2) 資訊科技	(6) 海運
(3) 銀行和金融服務	(7) 醫護服務
(4) 陸上交通	(8) 電訊和廣播服務

2. **維持關鍵的社會和經濟活動**的基礎設施，例如大型體育及表演場地、主要科技園等

被指定為“關鍵電腦系統”的電腦系統

- 可由“關鍵基礎設施營運者”在香港或從香港接達的電腦系統
- 關乎“關鍵基礎設施”核心功能的電腦系統

諮詢期接獲的意見：若因為關聯系統可能喪失功能而影響營運者提供必要服務而一併被指定為“關鍵電腦系統”，範圍會太廣

諮詢工作後的建議：由於“關聯”一詞未必能精準反映指定“關鍵電腦系統”的考慮因素，已刪除“關聯系統”的概念

監管及執行當局

- 由行政長官委任一名**專員**，帶領保安局轄下的**專責辦公室**執行擬議條例
- 指定有關行業監管機構為**“指定當局”**，包括**金融管理專員及通訊事務管理局**，負責監管相關界別內受其規管的“關鍵基礎設施營運者”履行**架構及預防的責任**
- 設立獨立的**上訴機制**，當機構不同意專責辦公室有關“關鍵基礎設施營運者”或“關鍵電腦系統”的決定，可提出上訴

議員齊發聲

立法會
相關文件

- 議員普遍**支持**政府當局提出的擬議**立法框架**。
- 議員認為擬議條例應達至**科技中立**。議員關注到部分規模較小的企業(例如數據中心)可能屬“關鍵基礎設施營運者”的**第三方服務提供者**，建議政府**當局協助該等企業履行**法例下的相關**法定責任**。
- 對於擬議條例並不適用於政府，議員建議**政府政策局**或**部門**，特別是涉及提供必要服務者(例如水務署)，必須符合類似擬議條例下有關**事故通報和應對**的**要求**。
- 議員建議政府當局因應日後的發展，**適時檢視其他法定行業監管機構**，例如負責規管保險業(屬擬議條例下的金融服務界別)的保險業監管局，**是否需要被指定為**擬議條例下的**指定當局**。

“關鍵基礎設施營運者”的3類責任

1 架構責任

- 在**香港持續**設有**辦事處**，以便營運者在香港履行有關預防和事故通報及應對的責任，並把地址通知專員或指定當局
- **通知**“關鍵基礎設施”**營運者**的**變更**，以便專員或指定當局了解其運作情況
- 設有**電腦系統安全管理單位**(可自設或外判)，確保有專責部門負責電腦系統保安及跟進專責辦公室的指示
- ✦ ***諮詢期接獲的意見***：機構(尤其是上市公司)難以就“擁有權”變更經常作出報告
- ✦ ***諮詢工作後的建議***：已刪除通報“擁有權”變更的要求

2 預防責任

- **報告**“關鍵電腦系統”在設計、配置、安全或運作等方面的**重大變化**
- 制定、實施及向專員或指定當局提交電腦系統**安全管理計劃**
- 進行電腦系統**安全風險評估**(至少每12個月一次)，並向專員或指定當局提交有關報告
- 進行獨立電腦系統**安全審核**(至少每24個月一次)，並向專員或指定當局提交有關報告

3 事故通報和應對責任

- 參與由專責辦公室舉行的**電腦系統安全演習**
- 制訂應對並妥善處理突發事件的**應急計劃**，並向專員提交計劃
- 在得悉“關鍵電腦系統”的電腦系統安全事故發生後的以下指明時限內，向專員作出通知，並在知悉有關事故當日後的14日內，向專員提交書面報告：
  - 嚴重事故[註]：**12小時內**
  - 其他事故：**48小時內**
- ✦ ***諮詢期接獲的意見***：機構難以按原建議的要求，在得悉嚴重電腦系統保安事故發生的2小時內，及時查證事故性質和成因，並向專員通報
- ✦ ***諮詢工作後的建議***：已放寬通報嚴重電腦系統保安事故的時限，由得悉後2小時放寬至12小時，而其他事故則由得悉後24小時放寬至48小時

註 指有關電腦系統安全事故已干擾，正干擾或相當可能將干擾有關“關鍵基礎設施”的核心功能

專員及指定當局的調查權力

- 專員可調查針對"關鍵電腦系統"的**安全威脅或事故**及**與**上述 **3 類責任相關的罪行**
- **調查權力**包括要求"關鍵基礎設施營運者"回答問題和提供資料、在裁判官手令下進入處所調查等，這與其他司法管轄區的做法一致，而每一項權力均有特定的條件、行使權力的程序或作出授權的機關等規範，以確保這些調查權力為最低限度而必要的

諮詢期接獲的意見：

(1) 擔心或涉及對境外的電腦系統執法

(2) 擔心擬議條例賦權專員在"關鍵電腦系統"接達設備或安裝程式，會影響系統的正常運作

諮詢工作後的建議：

(1) 擬議條例不具域外效力，專員要求的資料，只會為營運者可在香港或從香港取得的資料

(2) 只有發生嚴重事故而營運者不願意或未能自行應對事故等情況下，專員才會考慮向裁判官申請手令，接達有關系統，以應對事故。其他司法管轄區(如澳洲和新加坡)的相關監管機構也擁有類似的權力

罪行及罰則

- 除了在違反第 1 類、第 2 類和第 3 類責任或書面指示的情況中因"已盡應盡的努力"，以及在其他違法行為中因"合理辯解"而構成免責辯護外，違法行為將構成罪行
- 刑罰只會**以機構為單位**，不會在個人層面懲罰機構的主管或員工(除非違規行為涉及觸犯刑事法例(如提供虛假資料))
- 最高罰款港幣 50 萬元至 500 萬元不等；個別罪行也會就持續違法行為處以額外的每日罰款

議員齊發聲

- 議員對具備足夠**電腦保安專業知識人才**的**供應**表示關注，建議政府當局可考慮訂立電腦系統安全審核的認可服務提供者名單，以便利營運者聘請合適的人員。議員亦關注若干將載列於**《實務守則》**的**細節**，包括"關鍵基礎設施營運者"須進行的電腦系統安全風險評估和安全審核的合規標準。
- 議員建議政府當局**清楚界定**"關鍵基礎設施營運者"的**涉事員工**及**第三方服務提供者**需承擔的**法律責任**，以及確保擬議罪行的罰則具有足夠的阻嚇力。

立法所參考的其他司法管轄區有關保護關鍵基礎設施電腦系統安全的法例

中國內地

《中華人民共和國網絡安全法》

《關鍵信息基礎設施安全保護條例》

英國

《2018 年網絡與資訊系統規則》*(譯名)(只備英文本)*

澳門特別行政區

《網絡安全法》(2019 年)

美國

《2018 年網絡安全與基礎設施安全局法》*(譯名)(只備英文本)*

《2022 年關鍵基礎設施網絡事件報告法》

(譯名)(只備英文本)

新加坡

《2018 年網絡安全法》

(譯名)(只備英文本)

《2024 年網絡安全(修正)法案》

(譯名)(只備英文本)

歐盟

《2022 年於歐盟實施高度共通程度之網絡安全措施指令》

(譯名)(只備英文本)

澳洲

《2018 年關鍵基礎設施安全法》

(譯名)(只備英文本)

加拿大

正審議相關法案

當中所參考的部分事項

- 就**"關鍵基礎設施"**的定義**指明必要服務的界別**，其他司法管轄區的相關法例亦有類此做法，當中英國、澳洲、美國及歐盟的法例，亦有涵蓋維持關鍵社會和經濟活動的類似描述的基礎設施
- 採用**"機構為本"**的方式，以負責營運每個關鍵基礎設施的機構為一個單位，對其施加履行保障其電腦系統安全的責任，亦是英國、澳洲及歐盟的做法
- **不公開**關鍵基礎設施及"關鍵基礎設施營運者"的**名單**的做法，與英國及澳洲等司法管轄區的做法一致
- 將規管個別"關鍵基礎設施營運者"的責任交予**行業監管機構**的做法，亦見於英國、澳洲和美國的相關法例
- 不遵從擬議條例下的責任和規定所引致的罪行，其**罰則**只包含罰款的做法，亦見於英國及歐盟的相關法例

立法會秘書處

想進一步了解立法會相關討論

可從右方**二維碼**或**連結**瀏覽

立法會相關網站

保安事務委員會

《保護關鍵基礎設施(電腦系統)條例草案》委員會