立法會
Legislative Council

立法會CB(2)1779/2024(02)號文件

檔　號：CB2/BC/6/24

《保護關鍵基礎設施(電腦系統)條例草案》委員會

背景資料簡介

目的

本文件就《保護關鍵基礎設施(電腦系統)條例草案》("《條例草案》")提供背景資料，並概述保安事務委員會("事務委員會")就相關立法工作進行的討論。

背景

2. 現時，香港未有就針對保護關鍵基礎設施電腦系統作出任何法定要求。保安局於2021年10月向事務委員會簡介相關的政策措施時表示，因應近年網絡攻擊增加等情況，建議以立法方式清晰訂定關鍵資訊基礎設施的營運者的網絡安全責任。其後，行政長官在2022年10月發表的《施政報告》中宣布，會立法提升關鍵資訊基礎設施的網絡安全。按政府當局於2024年7月所述，考慮到香港的情況，並參考了其他司法管轄區的做法和吸納了不同持份者的意見，是次立法工作的政策目的，是加強關鍵基礎設施的電腦系統的保安能力，減低必要服務因網絡攻擊被干擾或破壞的可能，從而提升香港整體的電腦系統安全。香港網絡安全事故協調中心於2018年1月至2024年11月所接獲的事故報告數字載於**附錄1**。[1]

---

[1] 香港網絡安全事故協調中心由香港生產力促進局管理，為本地企業及互聯網用戶提供資訊保安事故的消息和防禦指引、事故回應及支援服務，及提高保安意識。

《保護關鍵基礎設施(電腦系統)條例草案》

3. 《條例草案》於2024年12月6日在憲報刊登，並於2024年12月11日的立法會會議上首讀。《條例草案》旨在：

(a) 保障香港關鍵基礎設施的電腦系統安全；

(b) 規管該等基礎設施的營運者；

(c) 就調查和應對該等電腦系統的電腦系統安全威脅及事故，訂定條文；及

(d) 就相關事宜，訂定條文。

4. 《條例草案》的立法建議重點，載於保安局於2024年12月4日發出的立法會參考資料摘要(檔號：SBCR 1/3231/2022 Pt. 5)第7至29段。

議員的意見及關注

立法框架

5. 委員提及包括低空飛行等新科技發展迅速，相關基礎設施日後或涉及提供日常生活必要的服務。就此，他們詢問立法框架如何**達至科技中性**，以應對科技的變化。政府當局表示，擬議規管當局[2]可就關鍵基礎設施營運者的責任發出實務守則。在制定和更新有關實務守則時，擬議規管當局將參照最新科技發展和國際標準，並按適當情況諮詢持份者，以應對日後可能出現的各類情況。

規管範圍和對象

6. 委員察悉，立法建議擬規管的關鍵基礎設施涵蓋兩大類別，即(a)在香港持續提供8個指明界別下的必要服務的基礎設施：能源、資訊科技、銀行和金融服務、陸上交通、航空交通、海運、醫護服務，及通訊和廣播服務；及(b)維持關鍵的社會和經濟活動的基礎設施。立法建議會以“機構為本”，而擬議規管當局會指定有關機構為關鍵基礎設施營運者(“指定營運者”)。

[2] 見下文第15段。

委員問及電子支付工具、即時通訊軟件、社交媒體平台、傳媒、電台、高等院校的科研設施，以及積金易平台是否屬擬議規管對象。對於政府當局表示絕大部分關鍵基礎設施由大機構營運，委員認為部分**中小型企業**(例如中小型數據中心和在港業務規模較小的航空公司)亦可能會成為指定營運者，但該等企業**或需要政府當局提供支援，以遵從立法建議下向關鍵基礎設施營運者所施加的責任**。

7. 政府當局表示，規管當局會考慮多項因素(例如有關設施一旦遭到破壞、喪失功能或數據洩漏可造成的影響)，以確定某基礎設施是否指明關鍵基礎設施。為免關鍵基礎設施成為攻擊目標，經參考其他司法管轄區的做法，擬議條例只會列出必要服務界別的名稱，關鍵基礎設施及關鍵基礎設施營運者的名單則不予公開。擬議條例通過後，規管當局會因應不同關鍵基礎設施的界別內可能被指明為關鍵基礎設施營運者的準備程度等情況，逐步分階段作出指明。此外，政府當局將繼續透過各項措施，加強中小型企業應對網絡攻擊的能力。

8. 委員詢問，政府當局有何措施防止公眾人士透過政府當局就立法建議下各項**涉及指定營運者的擬議罪行提出的檢控**，或**指定營運者**或其**第三方服務提供者的主動披露，得悉某機構為指定營運者**。政府當局表示，在提出相關檢控時會考慮需否向法庭申請在檢控程序中無需公開某些資料。而向關鍵基礎設施營運者發出的擬議實務守則，會訂有與保密責任相關的要求。

9. 委員提及內地的《關鍵信息基礎設施安全保護條例》涵蓋電子政務，他們要求政府當局說明**不擬將政府部門(特別是**負責**提供食水**等**必要服務**的政府部門)**納入規管**的**理據**。有意見認為，**至少應要求相關部門履行**類似立法建議下**事故通報和應對方面的責任**[3]。政府當局表示，各政府部門必須遵循數字政策辦公室制定的資訊科技保安政策及指引，該等政策及指引是參考國際標準和業界良好作業模式所訂定，與立法建議的要求相若。數字政策辦公室並會定期為各政策局及部門進行遵循審計。

10. 委員察悉，所有關乎關鍵基礎設施的核心功能屬必要的電腦系統會被指明為"關鍵電腦系統"，不論該等系統是否實際設置於香港。他們要求政府當局說明如何**規管設置於境外**

[3] 見下文第11段。

的電腦系統，以及**跟進**有關的**電腦系統安全事故**。政府當局表示，在立法建議下，如某關鍵電腦系統發生電腦系統安全事故，指定營運者有責任提供相關電腦系統(包括位處境外而可在香港或從香港接達的系統)的資料。

法定責任及罰則水平

11. 政府當局建議向指定營運者施加以下3類法定責任：架構的責任(第1類)、預防威脅及事故的責任(第2類)和事故通報及應對的責任(第3類)。就第2類責任，政府當局建議指明營運者必須**至少每年進行一次電腦系統安全風險評估**，以及**至少每兩年進行一次獨立電腦系統安全審核**，並提交報告。委員要求當局說明上述評估和審計的合規標準，以及規管當局會否就所接獲的報告進行抽查。他們關注到，本港**有否足夠的合資格資訊保安人才**，協助指定營運者履行相關法定責任，並建議當局**訂立進行上述審核的認可服務提供者名單**。政府當局表示，實務守則將述明有關評估和審計的標準，以及對審計人員資歷的要求。按其估算，本港現時約有3 000名合資格資訊保安人員可提供相關服務，如有需要，當局日後會考慮訂立認可服務提供者名單的可行性。

12. 就事故通報及應對的責任方面，委員關注到，就涉及**個人資料外洩的電腦系統安全事故**，指定營運者**是否**只需要按擬議條例下的機制通報，還是一如現行的做法，仍然**需要向個人資料(私隱)專員公署作出通報**。政府當局表示，擬議規管制度與其他現有法例或做法並非互相排斥，指定營運者應按個別監管機構的要求或建議，在事故發生後及時採取相應的跟進行動。就資料外洩事故而言，指定營運者可按個人資料(私隱)專員公署的建議，向其作出通報。

13. 委員察悉，政府當局建議參考其他司法管轄區的做法，就未盡應盡的努力或未有合理辯解(視乎所涉罪行而訂)而干犯擬議條例所訂的罪行，只會在機構層面向指定營運者處以最高罰款50萬至500萬元不等，並就持續罪行處以每日額外罰款。他們關注到，擬議罰則對指定營運者或其員工**是否有足夠的阻嚇力**。他們亦要求政府當局釐清，指定營運者在**委聘第三方服務提供者**設計或管理關鍵電腦系統時，相關營運者及第三方服務提供者各自**須承擔的法定責任**。政府當局表示，訂立相關罪行及罰的目的，是確保條例能有效實施及執行，其立法原意並非旨在懲罰營運者。考慮到香港的實際情況以及其他司法

管轄區的規定，政府當局認為擬議罰則水平合適。至於第三方服務提供者的責任方面，規管當局會參考其他司法管轄區的做法，在實務守則提供履行"盡責查證"及"合理努力"等或可視作合理辯解的指引，為指定營運者在聘用第三方服務提供者時訂定及履行合約提供參考。政府當局強調，若相關違規行為涉及其他刑事罪行(例如與詐騙相關的罪行)，涉事人員亦有機會要負上個人刑事責任。

14. 有委員認為，當局可考慮在擬議條例下設立賠償機制，**要求指定營運者在發生電腦系統安全事故後**，須**向受事故影響的人士作出賠償**。政府當局表示，受影響人士可按現時做法，按個別情況循民事訴訟程序索償。

規管當局及上訴機制

15. 委員察悉，在立法建議下，由行政長官所委任的一名專員及部分界別的指定當局[4]會作為規管當局。政府當局並建議成立一個隸屬保安局的專責辦公室，負責推行法定制度。委員要求政府當局說明，**專責辦公室**的擬議**人手編制**。政府當局表示，專責辦公室將由行政長官所委任的專員(首長級薪級第3點或第4點)帶領，並由2名副專員(首長級薪級第1點)提供支援。專責辦公室會有約40至50名非首長級人員，當中包括分別從數字政策辦公室及香港警務處科技罪案組借調的人員，以及法律專業人士和負責制訂政策的人員。

16. 委員察悉，因應部分擬規管的必要服務界別現已受其他法定行業監管機構的全面規管，在立法建議下，個別行業的監管機構會獲指明為指定當局，負責監管受其規管的指定營運者履行關於架構的責任和預防威脅及事故的責任。政府當局在現階段建議的指定當局為金融管理專員(相對的界別為銀行及金融服務界別)及通訊事務管理局(相對的界別為電訊及廣播服務界別)。至於監管所有指定營運者關於事故通報及應對的責任，則由專員全權負責。委員要求政府當局澄清，受指定當局規管的指定營運者未能履行關於架構的責任和預防威脅及事故的責任時，是否只會按指定當局的懲罰機制處理。政府當局表示，基本原則是按照指定當局的機制處理，例如指定當局可視乎情況，取消其發出的牌照。

---

[4] 見下文第16段。

17. 有委員關注**若干法定行業監管機構**(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)**未被指明為擬議條例下的指定當局**。政府當局表示，會因應相關行業及監管機制的發展，適時作出檢討。

18. 就於立法建議下成立、負責處理指定營運者就規管當局的若干決定所提出的上訴的上訴委員會，鑒於市場上電腦保安人才的供應或有限，委員對**上訴委員會的組成**及有何措施**避免委員出現利益衝突的情況**表示關注。政府當局表示，在擬議上訴機制下，行政長官會委任1名主席和2名副主席，以及至少8至10名人士作為委員，當中包括法律專業人士、資訊科技專業人士及其他社會人士。上訴委員會會按一貫處理利益衝突的方式行事。

相關文件

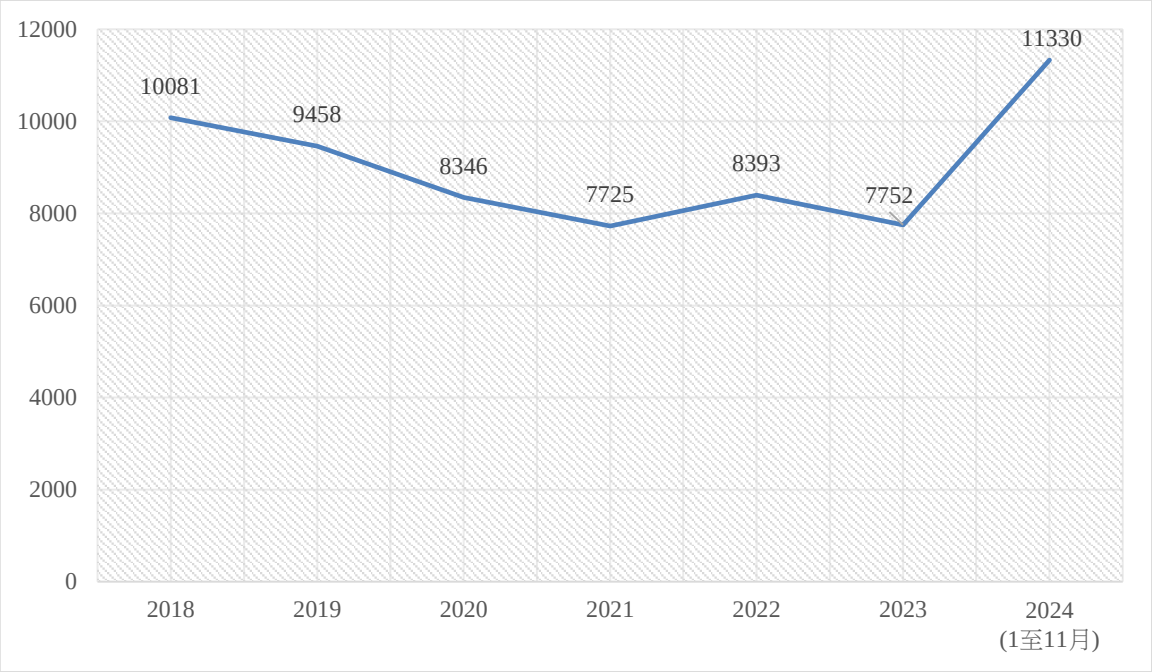
19. 相關文件一覽表載於**附錄2**，該等文件已登載於立法會網站。

立法會秘書處
議會事務部
2025年1月3日

附錄1

香港網絡安全事故協調中心
於2018年1月至2024年11月所接獲的事故報告數字

接獲的事故總數[1]



資料來源　：　香港網絡安全事故協調中心網頁，網址為：https://www.hkcert.org/tc/statistic

---

1　於2018年1月至2024年11月期間，香港網絡安全事故協調中心接獲最多的3類事故類別為：

(a)　殭屍網路(殭屍網路由一群殭屍電腦組成，而殭屍電腦大多數是一般電腦被惡意程式感染而成。當被感染後，惡意程式會用盡方法隱藏，連接到命令與控制服務器，得到黑客的指令，並進行攻擊)；

(b)　惡意軟件(惡意軟件是一個統稱，一些常見的類型有病毒、勒索軟件、蠕蟲、木馬、間諜軟件和廣告軟件等)；及

(c)　網絡釣魚(即透過冒充一個合法電郵或網站，以達到詐騙的目的)。

附錄2

《保護關鍵基礎設施(電腦系統)條例草案》

相關文件一覽表

委員會	會議日期	文件
保安事務委員會	2021年10月25日	議程第II項：保安局局長就行政長官2021年施政報告作出簡報 政策簡報會及會議紀要
	2022年2月8日	議程第III項：保安局局長就行政長官2021年施政報告作出簡報 政策簡報會及會議紀要
	2022年10月31日	議程第IV項：保安局局長就行政長官2022年施政報告作出簡報 政策簡報會及會議紀要
	2023年11月13日	議程第III項：保安局局長就行政長官2023年施政報告作出簡報 政策簡報會紀要
	2024年7月2日	議程第III項：加強保護關鍵基礎設施電腦系統安全 — 建議立法框架 會議紀要
	2024年10月2日*	政府當局就“加強保護關鍵基礎設施電腦系統安全 — 建議立法框架諮詢報告”提供的資料文件

* 發出日期

立法會秘書處
議會事務部
2025年1月3日