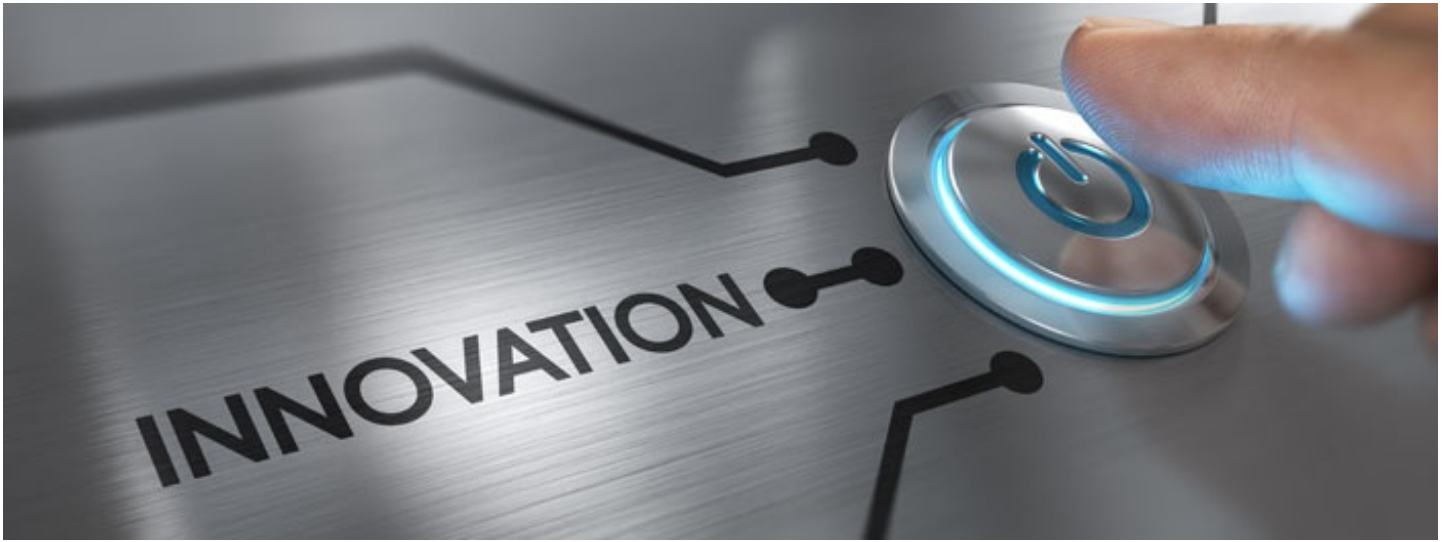


G7發布金融機關因應勒索軟體危脅之基礎要點



由於近年來勒索軟體對國際金融帶來重大影響，七大工業國組織G7成立網路專家小組CEG（Cyber Expert Group），並於2022年10月13日訂定了「金融機關因應勒索軟體危脅之基礎要點」（Fundamental Elements of Ransomware Resilience for the Financial Sector），本份要點是為因應勒索軟體所帶來之危脅，提供金融機關高標準之因應對策，並期望結合G7全體成員國已施行之政策辦法、業界指南以及最佳之實踐成果，建立處置應變之基礎，加強國際金融的韌性。該份要點內容著重於民營之金融機關（private sector financial entities），或關鍵之第三方提供商（critical third party providers），因其本身有遵守反洗錢和反恐怖主義之融資義務，但也可依要點訂定之原意，在減少自身受到勒索軟體之損害上，或在處置與應變上有更多的彈性。而日本金融廳於2022年10月21日公布該份要點之官方翻譯版本，要點所提列之重點如下：

1.網路安全策略與框架（Cybersecurity Strategy and Framework）：

將因應勒索軟體危脅之措施，列入金融機關整體的網路安全策略與框架之中。

2.治理（Governance）：

支付贖金本身可能於法不容許，也可能違背國家政策或業界基準，金融機關須在事件發生前，檢視相關法規，並針對潛在的被制裁風險進行評估。

3.風險及控制評估（Risk and Control Assessment）：

針對勒索軟體之風險，應建立控制評估機制並實踐之。因此可要求金融機關簽訂保險契約，填補勒索軟體造成的損害。

4.監控（Monitoring）：

針對潛在的勒索軟體，金融機關有監控其活動進而發現隱藏風險之義務，並向執法與資通安全機關提供該惡意行為之相關資訊。

5.因應處置、回覆（Response）：

遭遇勒索軟體攻擊之事件，就其處置措施，須依原訂定之計劃落實。

6.復原（Recovery）：

遭遇勒索軟體攻擊之事件，將受損之機能復原，須有明確的程序並加以落實。

7.資訊共享（Information Sharing）：

須與組織內外之利害關係人共享勒索軟體之事件內容、資訊以及知識。

8.持續精進（Continuous Learning）：

藉由過往之攻擊事件獲取知識，以提高應變勒索軟體之能力，建立完善的交易環境。

此要點並非強制規範，因此不具拘束力，且整合了2016年G7所公布的「G7網路安全文件之要素」（G7 Fundamental Elements of Cybersecurity document）之內容。綜上述CEG所提列重點，針對我國金融機關在抵禦網路攻擊之議題上，應如何完善資安體制，與日本後續因應勒索軟體之政策，皆值得作為借鏡與觀察。

相關連結

[〈G7サイバー・エキスパート・グループによるランサムウェア及びサードパーティのサイバーリスクマネジメントに関する基礎的要素の公表について〉](#)，日本金融庁ホームページ

[G7，〈Fundamental Elements of Ransomware Resilience for the Financial Sector〉](#)，Oct. 13, 2022

[日本金融庁，〈金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素（仮訳）〉](#)，令和4年10月21日

[〈金融セクターのサイバーセキュリティに関するG7の基礎的要素の公表について〉](#)，平成28年10月11日，日本金融庁ホームページ

[G7，〈G7 Fundamental Elements of Cybersecurity for the Financial Sector〉](#)，Oct. 11, 2016

[日本金融庁，〈金融セクターのサイバーセキュリティに関するG7の基礎的要素（仮訳）〉](#)，平成28年10月11日

你可能會想參加

- 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- 【已額滿】2023科技研發法制推廣活動－科專個資及反詐騙實務講座
- 供應鏈資安國際法制與政策趨勢分享會
- 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 商業服務業個資保護宣導說明會
- 【實體】2024科技研發法制推廣活動－科專個資及反詐騙實務講座
- 【直播】2024科技研發法制推廣活動－科專個資及反詐騙實務講座
- 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

陳政陽

副法律研究員 編譯整理

上稿時間：2023年02月

資料來源：

〈G7サイバー・エキスパート・グループによるランサムウェア及びサードパーティのサイバーリスクマネジメントに関する基礎的要素の公表について〉、日本金融庁ホームページ：<https://www.fsa.go.jp/inter/etc/20221021/contents.html>（最後瀏覽日：2023/1/15）。

G7、〈Fundamental Elements of Ransomware Resilience for the Financial Sector〉、Oct. 13, 2022、https://www.fsa.go.jp/inter/etc/20221021/ransom_fe.pdf（最後瀏覽日：2023/1/15）。

日本金融庁、〈金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素（仮訳）〉、令和4年10月21日、https://www.fsa.go.jp/inter/etc/20221021/ransom_kariyaku.pdf（最後瀏覽日：2023/1/15）。

〈金融セクターのサイバーセキュリティに関するG7の基礎的要素の公表について〉、平成28年10月11日、日本金融庁ホームページ：<https://www.fsa.go.jp/inter/etc/20161011-2.html>（最後瀏覽日：2023/1/15）。

G7、〈G7 Fundamental Elements of Cybersecurity for the Financial Sector〉、Oct. 11, 2016、<https://www.fsa.go.jp/inter/etc/20161011-2/3.pdf>（最後瀏覽日：2023/1/15）。

日本金融庁、〈金融セクターのサイバーセキュリティに関するG7の基礎的要素（仮訳）〉、平成28年10月11日、<https://www.fsa.go.jp/inter/etc/20161011-2/4.pdf>（最後瀏覽日：2023/1/15）。

文章標籤

推薦文章