# 日本發布關鍵基礎設施資訊安全對策第4次行動計畫

為了持續維持日本國內以及與東京奧運舉辦相關的關鍵基礎設施服務的安全性，日本內閣網路中心於2017年4月19日公布關鍵基礎設施資訊安全對策第4次行動計畫。

在第4次行動計畫，關鍵基礎設施防護目的主要是以關鍵基礎設施的功能保證為考量，盡量減少關鍵基礎設施IT故障的發生，並提升從事故中恢復的速度。因此，第4次行動計畫除持續檢討並改善第3次行動計畫原有政策外，較重要的變革為OT(Operation Technology)的重視與風險對應機制整備。在安全基準整備與落實情況方面，要求關鍵基礎設施產業須將OT的觀點融入人才培育。在資訊分享制度方面，分享的資訊範圍應包含IT、OT與IoT的資訊，並排除資訊分享的障礙。而在風險管理部分，日本從功能保證的觀點出發，新增風險情況對應準備的要求，包含事業持續計畫的提出與緊急應變措施的制定等。而在防護基礎強化上，該行動計畫認為關鍵基礎設施產業的IT、OT人員及法務部門必須依其內部資訊安全策略共同為關鍵基礎設施安全而跨組織合作。

另外，第4次行動計畫變更電力領域關鍵基礎設施的重要系統，從原有的運轉監視系統變更為智慧電表，以及新增化學、信用卡與石油三大關鍵基礎設施領域的業者、關鍵系統與因IT故障對關鍵基礎設施可能造成的危害影響。

## 相關連結

- 重要インフラの情報セキュリティ対策に係る 第４次行動計画，内閣サイバーセキュリティセンター
- 「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」に関する意見の募集について（終了しました），内閣サイバーセキュリティセンター

**蔡淑蘭**
法律研究員 編譯整理

**上稿時間：** 2017年06月

**資料來源：**
重要インフラの情報セキュリティ対策に係る 第４次行動計画，内閣サイバーセキュリティセンター，https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf（最後瀏覽日：2017/05/02）。
「重要インフラの情報セキュリティ対策に係る第４次行動計画（案）」に関する意見の募集について（終了しました），内閣サイバーセキュリティセンター，https://www.nisc.go.jp/active/infra/pubcom_ap4.html（最後瀏覽日：2017/05/02）。

文章標籤

資訊安全