令和６年 10 月２日
内閣官房 内閣サイバーセキュリティセンター
警察庁

豪州主導国際文書「OT サイバーセキュリティの原則」への共同署名について

１．概要

令和６年 10 月２日、内閣サイバーセキュリティセンター（NISC）及び警察庁は、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）が策定した文書「OT サイバーセキュリティの原則」（“Principles of operational technology cyber security”）（以下「本件文書」という。）の共同署名に加わり、本件文書を公表しました。仮訳は追って公表予定です。

本件文書に共同署名し協力機関として組織名を列記した国は、豪州、日本の他、米国、英国、カナダ、ニュージーランド、ドイツ、オランダ及び韓国の９か国です。

本件文書は、重要インフラ組織は、不可欠なサービスを提供する物理的な機器やプロセスを制御･管理するため､オペレーショナル･テクノロジー(OT)に依存しているとして、重要インフラ組織が OT 環境の設計、実装及び管理に係る意思決定を行うことを支援する 6 つの原則を示しています。当該原則が我が国重要インフラ事業者において適用されることは、我が国サイバーセキュリティ強化にも資することから、共同署名に加わることとしました。

今後も、引き続き、サイバーセキュリティ分野での国際連携の強化に努めてまいります。

２．本件文書の概要

(1) 背景・目的

重要インフラ組織は、物理的な機器やプロセスを制御・管理するために OT に依存している。本文書は、重要インフラ組織の OT 環境の安心・安全の確保と重要なサービスの事業継続を可能すべく、組織が OT 環境の設計、実装及び管理に係る意思決定を行うことを支援するための原則を記述している。

(2) ６つの原則の概要

ア　原則１　安全が第一

〇考慮すべき事項：人命、プラント、設備及び環境の安全並びにサービスの信頼性・稼働時間

〇インシデント対応において問うべき事項:適切な職員の現場への派遣準備、バックアップの信頼性等

イ　原則２　ビジネスの知識が重要

〇ベースライン:重要なサービスの継続的な提供に不可欠なシステムの特定、OT システムのプロセス及びプロセスの各部分の重要性についての理解等

〇OT 固有のインシデント対応計画の BCP 等との統合、第三者の関与前・関与時における第三者に対する情報提供、OT の停止・サイバーセキュリティ侵害の影響・重要度の評価のための事業状況の理解、プラントの知識を有する OT サイバーセキュリティ職員の、物理的なプラントを担当する組織内職員との実務関係の維持

ウ　原則３　OT データは極めて重要であり、保護する必要あり
〇技術的構成データ（ネットワークダイヤグラム等）、電圧レベル等のより一時的 OT データ等の保護
〇OT データの機密性、整合性、可用性の保護以上の事項（OT データ漏洩との際の警告等）の実施
エ　原則４　OT を他の全てのネットワークから分離・隔離する
〇OT の他のネットワークからの分離・隔離
〇OT システムの管理・運用のインターフェイスの IT 環境からの分離・隔離
オ　原則５　サプライチェーンは安全でなければならない
〇ベンダーの規模や工学技術上の重要性に関係のない、監視が求められるとするシステムの範囲の再評価
〇ファームウェアのアップデートが可能なベンダーにデバイスが接続している場合、ファームウェアや設定が変更された場合のデバイスへの影響の検討
カ　原則６　OT のサイバーセキュリティには人材が不可欠
〇様々なスキル、知識、経験及びセキュリティ文化を備えた、異なる背景を持つ者の組み合わせ
〇重要インフラの OT 現場において、防御の最前線に立つのは OT サイバーセキュリティ専門家等でない者であることを踏まえた、サイバーセキュリティ意識の発展を現場の安全文化の中核的要素とすることの焦点化

３．関連リンク

豪州 ACSC ホームページ