報道資料

令和７年２月４日
内閣官房 内閣サイバーセキュリティセンター

国際文書「エッジデバイスのための緩和戦略」への共同署名について

１．概要

令和７年２月４日、内閣サイバーセキュリティセンター（NISC）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「エッジデバイスのための緩和戦略」（“Mitigation strategies for edge devices”）（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、韓国、オランダ及びチェコの９か国です。

本件文書は、エッジデバイスを標的とした攻撃が増加していることを踏まえ、リスク緩和のための７つの戦略を提供するものです。重要インフラ事業者を始めとした我が国企業等が、本件文書で記載されたエッジデバイスに対するリスク緩和策を参照することは、我が国サイバーセキュリティ強化に大いに資することから、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

多くの悪意のあるアクターは、インターネットからアクセス可能なネットワーク等に対してスキャン・偵察を行い、パッチが適用されていない脆弱なエッジデバイスを侵害している。本文書は、サイバー脅威に対するセキュリティとレジリエンスの向上を目的にリスク緩和のための 7 つの戦略を提供する。

(2) ７つの戦略の概要

ア　エッジを知る：ネットワークの周辺がどこにあるかを理解し、その周辺に配置されているエッジデバイスを検査するよう努める。サポートが終了したデバイスを特定し、それらを取り外し、交換する。

イ　セキュア・バイ・デザイン機器を調達する：製品開発中にセキュア・バイ・デザインの原則に従っているメーカーからの調達を優先し、調達プロセスの一環として、メーカーに対し製品のセキュリティを明示的に要求する。

ウ　セキュリティ強化のガイダンス、更新及びパッチを適用する：特定のベンダーがセキュリティを強化するガイダンスを利用していることを検証して実装する。不正利用から保護するため、エッジデバイスに対するセキュリティパッチと更新の迅速な適用を確保する。

エ　強力な認証を実装する：不正利用から保護するため、エッジデバイス全体において、フィッシングに対する耐性のある多要素認証等の認証を実装する。

オ　不要な機能とポートを無効にする：組織において使用されていない、

エッジデバイスで利用可能なオプション機能を検査し、これを無効とすることで、機器の攻撃対象範囲を減少させる。また、開かれたポート数を減らす。

カ　管理インターフェイスを安全にする：管理インターフェイスをインターネットに直接接続しない。

キ　脅威検出のための監視を一元化する：インシデントの検出のため、イベントログの保存と完全性を保護する。ログへのアクセスの一元化を確保する。

３．関連リンク

【原文リンク】

【本報道発表に関する問い合わせ先】

内閣官房 内閣サイバーセキュリティセンター
国際ユニット国際戦略班
Tel：03-6277-7071