報道資料

令和７年１０月２３日
国家サイバー統括室
警察庁

国際文書「最新の防御可能なアーキテクチャのための基礎」への共同署名について

令和７年１０月２３日、国家サイバー統括室及び警察庁は、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「最新の防御可能なアーキテクチャのための基礎（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。

本件文書は、豪州のインシデント対応やセキュリティテスト実施等の経験等を踏まえ、各組織が、サイバー脅威に対応したシステムの構築、維持、更新、強化のために役に立つアプローチを提供するものです。

本件文書は、「最新の防御可能なアーキテクチャのための基礎」、「上級意思決定者向けの最新の防御可能なアーキテクチャ」及び「最新の防御可能なアーキテクチャへの投資」と題する３つのガイダンスから構成されています。

本件文書の目的である、各組織におけるサイバー脅威に対応したシステムの構築、維持、更新、強化の促進は、我が国のサイバーセキュリティ環境の向上にも資することから、共同署名に加わることとしました。

本件文書に共同署名した国は、豪州、日本の他、ドイツ、カナダ、ニュージーランド、韓国、チェコの計７か国です。

１．本件文書の概要

(1) 背景・目的

本文書は、豪州のインシデント対応やセキュリティテスト実施等の経験等を踏まえ、各組織が、サイバー脅威に対応したシステムの構築、維持、更新、強化のために役に立つアプローチを提供する。

(2) 最新の防御可能なアーキテクチャを導入するための１０の原則

- 一元管理された企業 ID：ID を一元管理することで可視性と正確性を向上させ、ID 侵害の可能性と影響を軽減する。

- 高い信頼性の認証：強力で信頼性の高い認証方法を使用し、認証の不正利用等を防止する。

- 文脈に沿った承認：アクセスの認証に際し、ユーザーとシステムとの継続的なやりとり、前後関係や文脈に沿った認証を行うことで、より信頼性のある正確な認証が可能となる。

- 信頼性ある資産一覧：一元的な資産一覧により、エンドポイント、ネットワーク、アプリケーション、暗号資産、保存データ等の組織が所有する資産の完全かつ包括的な知識を得る。

- 安全なエンドポイント：検証された強靭なエンドポイントを用いるこ

とで、サイバー攻撃の影響を制限する。

- 制限された攻撃経路：攻撃経路を制限することで、正しい場所における、より質の高い緩和策を講じることが可能になる。

- 強靭なネットワーク：障害耐性があり、サイバー攻撃に対して強靭で、横展開や縦移動の制限を通じて、データを保護するためのネットワークを実現する。

- セキュア・バイ・デザインのソフトウェア：ハードウェア・ソフトウェアが、セキュリティ第一の原則等を通じて設計等され、プライバシーとデータを保護し、セキュリティの維持を確保する。

- 包括的な保障と管理：セキュリティ対策について、緩和策とビジネスの双方の有効性が確保されるよう検証する。

- 継続的かつ実行可能なモニタリング：リアルタイムで自動化された監視を通じて、組織の環境等に対する行動を可視化する。

２．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】

国家サイバー統括室
国際ユニット国際戦略班
Tel：03-6277-7071