報道資料

令和７年５月２７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「SIEM 及び SOAR プラットフォームに関するガイダンス」への共同署名について

１．概要

令和７年５月２７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 SIEM 及び SOAR プラットフォームに関する一連のガイダンス（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、英国、カナダ、ニュージーランド、シンガポール、韓国及びチェコの計９か国です。

本件文書は、SIEM 及び/又は SOAR の調達を検討している又は運用している組織を対象に、これらの定義、ありうる利点や課題、調達・設置・保守に関するベストプラクティス等を提供するものです。本件文書は、幹部向けガイダンス（Executive Guidance）、実務者向けガイダンス（Practitioner guidance）及び実務者向け優先ログガイダンス(Priority logs for SIEM ingestion - Practitioner guidance)の３つに分かれています。

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 SIEM 及び SOAR プラットフォームに関するアドバイスを参照することは、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

実務者向けガイダンスでは、SIEM 及び/又は SOAR プラットフォームの調達を検討又は運用している組織を対象に、以下４点についてガイダンスを提供する。

(2) ４点の概要

ア　SIEM 及び SOAR の定義：SIEM は、ネットワーク内の複数のソースからログデータを収集、一元化及び分析するソフトウェアプラットフォームまたは機器の一種。SOAR は、ネットワーク上で検出された異常なアクティビティへの対応を自動化する一連のソフトウェアプラットフォーム。

イ　SIEM 及び/又は SOAR のありうる利点：ログの収集、一元化、ダッシュボード・報告の作成によるネットワーク内の可視性(Visibility)の強化、通常ではない活動に対する早期警報発出等インシデント検出の強化、SIEM のログ収集、一元化、早期警報及び SOAR の自動対応機能による対応の強化。

ウ　SIEM 及び/又は SOAR を実装する際の課題：効果的なログ分析の実現の

ためには SIEM を組織固有の IT 環境にあわせて設定することが必要、SOAR の設定には専門的なスキルを有する一定のスタッフが必要、実装には多大な継続コストが必要といった課題が存在。

エ　SIEM 及び/又は SOAR を実装するためのベストプラクティス原則:調達、設置及び保守の各段階について、技術面、人的資源面まで幅広い範囲にわたる、参照可能なベストプラクティスを提供。

※「実務者向け優先ログガイダンス」では、実務者が収集すべき具体的なログのデータソースが優先順位に沿って分類されており、我が国企業等にとって有用な情報となっている。

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