報道資料

令和６年８月２２日
内閣官房 内閣サイバーセキュリティセンター

# 豪州主導の国際文書「イベントログと脅威検知のためのベストプラクティス」への共同署名について

## １．概要

令和６年８月２２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「イベントログと脅威検知のためのベストプラクティス」（“Best practices for event logging and threat detection”）（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、シンガポール、韓国及びオランダの９か国です。

本件文書は、経営層の IT 責任者やネットワーク運用者等を対象として、イベントログと脅威検知に関する国際的なベストプラクティス集となっています。検知が困難とされるシステム内寄生（Living Off The Land）戦術への技術的な対策を示すことは、我が国のサイバーセキュリティ強化に資することから、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）システム内寄生戦術を使用した悪意のあるアクターの増加によって、イベントログの重要性が高まっている。本件文書は、クラウド、企業ネットワーク、エンタープライズモビリティ及び OT（Operational Technology：オペレーショナルテクノロジー）ネットワークのイベントログと脅威検知のためのベストプラクティスを説明。

（２）本件文書は、中規模から大規模の組織を対象としているところ、特に IT 及び OT に関する経営幹部、IT 及び OT オペレーター、ネットワーク管理者及び重要インフラ事業者向けに作成。

（３）イベントログのベストプラクティスとして、次のとおり記述。

（ア）イベントログポリシー

ログポリシーの作成に当たって考慮すべき事項として、イベントログに含めるべき詳細（保存すべきイベントログの詳細）、内容及びフォーマットの一貫性、タイムスタンプの一貫性、イベントログ保存（保存期間等）を列挙。

（イ）ログの収集と相関の一元化

企業ネットワーク、OT、エンタープライズモビリティ、クラウドについて、保存すべきログの優先順位付け（ログソースのリストを詳述）。

（ウ）安全な保存とイベントログの完全性

完全性確保のためのイベントログの保護とアクセス制限。

（エ）脅威に対する検知戦略

挙動異常の例を次のとおり列挙するとともに、挙動異常を自動検知できるようにすることを推奨。

- 通常とは異なる時間（勤務時間外、休日、休暇中等）にログインしたユーザー
- 通常はアクセスしないサービス（管理者や人事サービス等）にアクセスしたアカウント

- 通常と異なるデバイスを使用してログインしたユーザー
- 大量のアクセス試行
- 不可能な移動や複数の場所から同時にサインインがあった場合
- 大量のデータをダウンロード又はエクスポートした場合
- 定義されたコンピュータのアクセスや物理的なアクセスログの検証なくネットワークにログインした場合
- 単一の IP アドレスから、複数の異なるユーザーとして認証しようとした場合
- 特に管理者権限のあるアカウントが、ユーザーアカウントを作成又は無効化されたアカウントを再び有効化した場合
- あるデバイスが、通常は接続しない他の内部デバイスと通信していることを示すネットフローデータ
- 通常と異なるスクリプトの実行、ソフトウェアのインストール又は管理者ツールの利用
- 予期せぬログの消去
- 通常と異なる又は不審なパスからのプロセス実行
- Windows Defender 等のセキュリティソフトウェアやログ管理ソフトウェアの設定変更

## ３．関連リンク

豪州 ACSC ホームページ

【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:03-3580-3188