アタックサーフェス　チェックリスト

近年の攻撃対象領域は、常に規模と複雑さが増しています。
新しいサイバー資産が増えるたびに、新しい攻撃ベクトルも導入されます。

以下のチェックリストを利用して、攻撃対象領域の各要素が十分に把握できているか、
または可視性に欠けている部分があるかを確認してください。各要素を次のように分類してください。

- 既知の既知：攻撃対象領域の一部であることが分かっているサイバー資産。
- 既知の未知：攻撃対象領域の一部であることは知っているが、
  可視化できていない、あるいは管理していないサイバー資産。
- 未知の未知：攻撃対象領域の一部であるかどうかが不明なサイバー資産。
- 該当なし：100%確実に攻撃対象外であるとわかっているサイバー資産。

チェックリストは、あなたのすべての回答を記録し、本書の最後にある1枚のシートにまとめています
(p. 11)ので、攻撃対象領域を一目で把握することができます。

ある種の資産は、複数のカテゴリーに分類される可能性があることにご留意ください（例えば、あるデバイスは、モバイルデバイスとエンドポイントデバイスの両方とみなされる可能性があります）。それで大丈夫です！ ここで目指すのは、可能な限り徹底すること - 盲点をなくすたびに、サイバー攻撃者が環境に侵入する機会がひとつ減ることになります。

エンドポイントデバイス

ネットワークに接続する、会社支給または従業員所有のデバイス（BYOD）。主にAndroid、ChromeOS、iOS、Linux、Mac、Windowsデバイスが含まれます。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- デスクトップPC
- ノートPC

管理ツール：

- IT資産の検出
- モダンデバイス管理 (MDM)
- 統合エンドポイント管理 (UEM)

モバイルデバイス

会社支給または従業員所有（BYOD）のエンドポイントデバイスで、通常はWi-Fi経由でネットワークに接続し、持ち運びが容易なように設計されています。主にアンドロイドとiOSデバイスが含まれます。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- スマートフォン
- スマートウォッチ
- タブレット

管理ツール：

- IT資産の検出
- モバイルデバイス管理 (MDM)
- モダンデバイス管理 (MDM)

堅牢なデバイス

建設現場、製造施設、倉庫などの標準的なモバイルデバイスが損傷を受けるような環境に耐えられる仕様に対応したモバイルデバイス。主にAndroid、iOS、Windowsデバイスが含まれます。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- 堅牢なモバイル・コンピュータ
- 堅牢なタブレット
- 堅牢なウェアラブル

管理ツール：

- IT資産の検出
- モバイルデバイス管理 (MDM)
- モダンデバイス管理 (MDM)

モノのインターネット（IoT）機器

非標準的なエンドポイントデバイスで、センサーやソフトウェアを搭載し、ネットワークや公共のインターネットを介して他のデバイスやシステムとデータを交換できるもの。使用ケースによっては、エンタープライズIoT（eIoT）、拡張版IoT（XIoT）、産業用IoT（IIoT）、医療向けIoT（IoMT）デバイスと呼ばれることもあります。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- 資産追跡装置（RFIDタグなど）
- 産業用センサー
- スマート家電（トースター、冷蔵庫、電球など）

管理ツール：

- IT資産の検出
- モダンデバイス管理 (MDM)
- 専用IoTセキュリティツール（多種多様）
- 統合エンドポイント管理 (UEM)

サイバーフィジカルシステム（CPS）

計算資源と物理資源を連携させ、顕密に調整してタスクを実行するシステム。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- ビル管理システム（BMS）
- 産業用制御システム（ICS）
- オペレーション・テクノロジー（OT）
- ロボティクス・システム

管理ツール：

- IT資産の検出
- サイバーフィジカルシステム（CPS）保護プラットフォーム
- モダンデバイス管理（MDM）

ネットワークデバイス

ネットワーク上の他のデバイスとの通信や相互作用をサポートするデバイス。ネットワークデバイスはネットワークインフラを構成します。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- ルーター
- スイッチ
- ファイアウォール

アクセスポイント管理ツール：

- ネットワーク検出ツール

サーバー/データセンターデバイス

データの処理、保存、配信をサポートするデバイス。メール通信やウェブサイトなどのサービスの基盤として考えられています。.

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- サーバー（電子メールサーバー、プリントサーバー、ウェブサーバーなど）
- ストレージシステム

管理ツール：

- IT資産の検出
- モダンデバイス管理 (MDM)
- 統合エンドポイント管理 (UEM)

固定機能デバイス

狭いユースケースを満たすために設計されたデバイス。多くの場合、顧客向けです。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- POSシステム
- セルフヘルプキオスク

管理ツール：

- IT資産の検出
- モダンデバイス管理 (MDM)
- 統合エンドポイント管理 (UEM)

クラウドサービス

クラウドコンピューティングは、インターネットを介してコンピューティングリソースへのオンデマンドアクセスを提供します。これらはプライベートクラウド（「内部クラウド」または「企業クラウド」とも呼ばれる）、パブリッククラウド、ハイブリッドクラウド、マルチクラウド環境を通じて調整されます。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- クラウドコンテナ
- クラウドデータストレージソリューション
- プライベートクラウドの基盤となるコンピュートリソース（例：CPUやストレージ）
- パブリッククラウドサービス（例：AWS、Google Cloud Platform、Microsoft Azure Cloud Services）

管理ツール：

- クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）
- クラウドセキュリティポスチャ管理（CSPM）
- クラウドワークロード保護プラットフォーム（CWPP）

SaaSアプリケーション

オンデマンドアプリケーションは、クラウドコンピューティングサービスモデルを介して展開され、サービスプロバイダーがすべての基盤となるインフラストラクチャを管理します。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- Microsoft 365
- Salesforce
- Slack

管理ツール：

- SaaSセキュリティポスチャ管理（SSPM）

コード

コンピュータに何をするべきかを指示するプログラミング言語で書かれた指示の集合。ソフトウェアの構成要素。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- 内部または顧客の利用のために開発されたカスタムソフトウェアのコード
- 商業販売のために開発された独自ソフトウェアのコード

管理ツール：

- コンテナスキャナー
- 動的アプリケーションセキュリティテスト（DAST）
- モバイルアプリケーションセキュリティテスト（MAST）
- オープンソースソフトウェア（OSS）スキャナー
- ソフトウェア構成分析（SCA）
- 静的アプリケーションセキュリティテスト（SAST

商用オフザシェルフ（COTS）ソフトウェアとアプリケーション

サードパーティから購入した、またはデバイスにプリインストールされている、組織が購入して使用するコンピュータプログラム。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- オペレーティングシステム（Windows、macOS、Linuxなど）
- 生産性向上スイート（Microsoft Officeなど）
- サードパーティ製アプリケーション（Zoomなど）

管理ツール：

- IT資産の検出
- パッチ管理

インターネットに面した資産

公共のインターネットから直接アクセスできるサイバー資産。これらの資産は、いわゆる”外部攻撃対象領域”を構成しています。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- 証明書／ドメイン
- 開発環境とQA環境（IPアドレス）
- ウェブサイト（ウェブサーバー）

管理ツール：

- 外部攻撃対象領域管理（EASM）

デジタル資産

通常のIT資産とは見なされないが、企業のブランド、評判、セキュリティに影響を及ぼす可能性のある資産の組み合わせ。例として、ダークウェブのデータやソーシャルメディアが挙げられます。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- オンライン・フォーラム
- ソーシャルメディア・アカウント

管理ツール：

- デジタルリスク保護 (DRP)

アイデンティティとアクセス

「アイデンティティ」は、企業に関連付けられた個人のデジタルアイデンティティを指します。具体的には、名前、役職、上司、直属の部下、電話番号などの情報が含まれます。「アクセス」は、その個人が役職やセキュリティクリアランスなどの要因に基づき、閲覧および/または編集する権限を持つリソースやデータを表します。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- ユーザーID
- アクセスレベル

管理ツール：

- アイデンティティおよびアクセス管理 (IAM)
- アイデンティティプロバイダ（IdP）

データ

計画、意思決定、日常業務の支援のために企業によって生成または収集された情報。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- 顧客のクレジットカード情報
- 知的財産（IP）
- 患者の医療記録
- 個人を特定できる情報（PII）
  （例：顧客の連絡先情報）

管理ツール：

- データ損失防止（DLP）
- データセキュリティポスチャ管理（DSPM）

アプリケーションプログラミングインターフェース（API）

異なるソフトウェアアプリケーションが互いに通信できるようにするための一連のルールおよびプロトコル。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- HubSpot APIs
- Salesforce APIs
- Slack APIs

管理ツール：

- API保護製品
- APIセキュリティ対策ツール

サードパーティ資産

現代の企業は、複数の外部組織と密接に連携しており、システムやデータを共有することがよくあります。二者がこれほど密接に関係するようになると、攻撃対象領域も連動するようになります。

既知の既知	☐
既知の未知	☐
未知の未知	☐
該当なし	☐

例：

- リセールパートナーのウェブサイト
- マーケティング会社のクラウドインフラストラクチャ
- サプライチェーンパートナーの開発環境

管理ツール：

- 外部攻撃対象領域管理（EASM）

	可視性			
資産カテゴリ	既知の既知	既知の未知	未知の未知	該当なし
エンドポイントデバイス	☐	☐	☐	☐
モバイルデバイス	☐	☐	☐	☐
堅牢なデバイス	☐	☐	☐	☐
モノのインターネット（IoT）機器	☐	☐	☐	☐
サイバーフィジカルシステム（CPS）	☐	☐	☐	☐
ネットワークデバイス	☐	☐	☐	☐
サーバー/データセンターデバイス	☐	☐	☐	☐
固定機能デバイス	☐	☐	☐	☐
クラウドサービス	☐	☐	☐	☐
サービスとしてのソフトウェア（SaaS）アプリケーション	☐	☐	☐	☐
コード	☐	☐	☐	☐
市販の商用ソフトウェアおよびアプリケーション	☐	☐	☐	☐
インターネットに面した資産	☐	☐	☐	☐
デジタル資産	☐	☐	☐	☐
アイデンティティとアクセス	☐	☐	☐	☐
データ	☐	☐	☐	☐
アプリケーションプログラミングインターフェース（API）	☐	☐	☐	☐
サードパーティとの関係	☐	☐	☐	☐

Ivanti について

Ivantiは、ITとセキュリティ部門間の障壁を取り除きEverywhere Work（場所にとらわれない働き方）を実現します。IvantiのCIOとCISO向けに特化したプラットフォームは、ITとセキュリティ部門へ組織のニーズに合わせて拡張できる包括的なソフトウェアソリューションを提供し、セキュアに従業員体験を向上させます。Ivantiプラットフォームは、クラウドスケールのインテリジェントなハイパーオートメーションレイヤーであるIvanti Neuronsを搭載しており、組織全体でプロアクティブな修復とユーザーフレンドリーなセキュリティを実現し、ユーザーが満足するような従業員体験を実現します。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む40,000社以上の顧客によって採用されています。Ivantiは、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来を実現するために取り組んでいます。詳細については、ivanti.com @GoIvantiをフォローしてください。

ivanti

詳細はivanti.com/ja
にお問い合わせください。