MANDIANT
NOW PART OF Google Cloud

サイバー・スナップショット・レポート
第4号

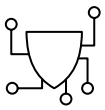
『防御側の優位性 - サイバー・スナップショット』では、サイバー攻撃の最前線でのMandiantの観測結果また現実世界での経験に基づき、重要性を増すサイバー防御のトピックに関する知見をお届けします。本号では、AIシステムにおけるセキュリティの構築、インシデント発生時の効果的なクライシス・コミュニケーションのベスト・プラクティス、IoTおよびエッジ・ネットワーク・インフラストラクチャに対する最新のリスク軽減策など、幅広いトピックを取り上げます。

人工知能システムの保護

人工知能（AI）は急速に進歩しており、効果的なリスク管理戦略も並行して進化させることが重要です。ネットワークとDevOpsを悩ませてきたボルトオン・セキュリティ・ソリューションを回避するには、最初からAIシステムにセキュリティを構築することが重要であるとMandiantは考えます。これを実現するべく、Googleは最近、安全なAIシステムの概念的フレームワークである Secure AI Framework（SAIF）を導入しました。

SAIFは、セキュリティ（アクセス管理、ネットワークとエンドポイントのセキュリティ、サプライ・チェーン攻撃など）、AI/MLモデルのリスク管理（モデルの透明性と説明責任、データ・ポイズニング、データ系列など）、プライバシーとコンプライアンス（データ・プライバシーと機密データの使用など）、人と組織（人材ギャップ、ガバナンス、取締役会への報告など）など、最重要懸念に対処するための実践的なアプローチを提供します。

SAIFには、組織が安全かつ責任ある方法でAIシステムを総合的に構築およびデプロイできるようにするための、核となる要素が6つあります。

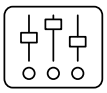


強力なセキュリティ基盤をAIエコシステムに拡大

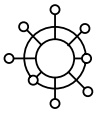
組織の脅威分野にAIを導入するための検知能力・対応能力の拡張

既存および新たな脅威に対応するための防御の自動化

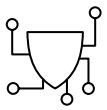
組織全体で一貫したセキュリティを実現するためのプラットフォーム・レベルの調和的対策



軽減策を調整し、AIデプロイメント時のフィードバック・ループを高速化するための対策



ビジネス・プロセス周りのAIシステム・リスクのコンテキスト化



強力なセキュリティ基盤をAIエコシステムに拡大

- **セキュリティ・ドメイン全体においてAIシステムに適用されている既存のセキュリティ対策を確認する**

  セキュリティ・ドメイン全体における既存のセキュリティ対策は、さまざまな形でAIシステムに適用されています。たとえば、データのセキュリティ対策で、AIシステムがトレーニングと運用に使用するデータを保護できます。ほかにも、アプリケーションのセキュリティ対策でAIシステムが実装されているソフトウェアを、また、インフラストラクチャのセキュリティ対策でAIシステムが依存している基盤のインフラストラクチャを保護できます。さらに、運用面でのセキュリティ対策によって、AIシステムを安全な方法で運用していることを確認できます。

  必要とされる具体的な対策は、AIの利用、個々のAIシステム、環境によって異なります。

- **使用可能なフレームワークで、AIの脅威とリスクに対する従来の対策の関連性を評価する**

  AIの脅威やリスクの中には、従来のセキュリティ対策が適切な場合もありますが、効果的に運用するには適応させる必要があったり、AI特有のリスクに対処する防御態勢へのレイヤーの追加が必要になったりする場合があります。たとえば、データの暗号化は、キーに対するアクセス権を特定のロールに制限することで、不正なアクセスからのAIシステム保護に利用できます。しかし、データの暗号化を利用して、盗難や改ざんからAIモデルとその基礎となるデータの保護が必要となる場合もあります。

- **分析を通じて、AIに特有な脅威や規制などの理由から、追加する必要のあるセキュリティ対策を特定する**

  チームを構成して、現在の対策がAIユースケースにどのように対応しているかを確認し、それら対策の目的適合性を評価して、ギャップ領域に対処する計画を立てます。これらをすべて完了したら、リスクが低減したかどうかや、意図したAI利用への対応具合に基づいて、それらの対策の有効性も測定します。

- **サプライ・チェーンの資産、コード、トレーニング・データの保存と追跡の準備をする**

  AIシステムを利用している組織は、サプライ・チェーンの資産、コード、トレーニング・データの保存および追跡を準備する必要があります。これには、すべての資産を識別・分類・保護して、不正アクセスまたは不正使用を監視することが含まれます。組織はこうした手順を踏むことで、AIシステムを攻撃から保護することができます。

- **データ・ガバナンスとライフサイクル管理が、スケーラブルでAIに適応していることを確認する**

  データ・ガバナンスには、そこで従う定義に応じて、次の最大6つの意思決定ドメインがあります。

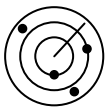
  - データの品質
  - データのセキュリティ
  - データのアーキテクチャ
  - メタデータ
  - データのライフサイクル
  - データの保存

  AIデータ・ガバナンスはこれまで以上に重要となるでしょう。たとえば、AIモデルの有効性の重要な基礎の1つに、データのトレーニング・セットがあります。データ・セットには、ライフサイクルの一環としてセキュリティを重視した、適切なライフサイクル管理システムが必要です（つまり、データの作成から最終的なデータ破棄までのライフサイクル全体に、セキュリティ対策を埋め込むということです）。データ系列も重要な役割を果たし、プライバシーと知的財産に関する問いに答えるのに役立ちます。データの作成者、データの出所、データ・セットの構成要素がわかっていると、前述のトピックに関する問いに答えることがずっと簡単になります。

  AIの導入が進むにつれ、組織の成功はそうした意思決定ドメインを迅速にスケーリングできるかどうかにかかってきます。こうした取り組みをサポートするには、部署横断的なチームでデータ・ガバナンス戦略を検討し、AIの進歩を確実に反映するように調整できることが重要です。

- **人材の定着と再トレーニング**

  これは、AIではなく、人についてです。多くの組織において、セキュリティやプライバシー、コンプライアンスの分野で適切な人材を見出すには、数年という時間がかかる場合があります。適切な人材を定着させる対策を講じることで、成功につながる場合があります。個々のAIの知識があっても習得に長い時間がかかる組織についての知識がない外部の人材を雇い入れるよりも、既にいる人材にAI関連のスキルを再トレーニングした方が短時間ですむかもしれません。



組織の脅威分野にAIを導入するための検知能力・対応能力の拡張

- **AI利用のシナリオにおいて問題となる脅威や利用するAIの種類などについての理解を深める**

  AIシステムを利用する組織は、個々のAI利用シナリオに関連する脅威を把握しておく必要があります。利用するAIの種類、AIシステムのトレーニングに使用するデータ、セキュリティ侵害の潜在的な結果について理解します。組織はこうした手順を踏むことで、AIシステムを攻撃から保護することができます。

- **AIに対する攻撃、AI出力によって起こる問題に対応する準備をする**

  AIシステムを利用する組織は、セキュリティ・インシデントの検知と対応の計画を立て、AIシステムが有害なまたは偏った意思決定をするリスクを低減する必要があります。そうした対策を講じることで、組織はAIシステムとユーザーを危険から守ることができます。

- **具体的には、生成AIの場合、AIの出力に焦点を当て、コンテンツの安全性に関するポリシー施行の準備をする**

  生成AIは、テキストから画像、動画まで、さまざまなコンテンツを作成するためのパワフルなツールです。ただし、悪用される可能性もあります。たとえば、生成AIはヘイト・スピーチまたは暴力的な画像など、有害なコンテンツの作成に使用されるリスクがあります。そうしたリスクを低減するには、コンテンツの安全性ポリシーを施行する準備をすることが重要です。

- **悪意のあるコンテンツの作成やAIのプライバシー侵害などのAI特有のインシデントの種類に応じて、悪用ポリシーやインシデントレスポンス・プロセスを調整する**
- AIシステムがより複雑となり、かつ普及する中、大切なのは、悪用ポリシーを調整して悪用ユースケースに対応するだけでなく、個々のAIインシデントの種類を考慮してインシデントレスポンス・プロセスの調整を行うことです。そうしたインシデントには、悪意のあるコンテンツの作成、AIのプライバシー侵害、AIによるバイアス、システムの一般的な悪用などがあります。

既存および新たな脅威に対応するための防御の自動化

- **AIシステムの保護、データ・パイプラインのトレーニングなどに焦点を当てたAIのセキュリティ対応能力をリストにまとめる**

  AIセキュリティのテクノロジーによって、データ漏えい、悪意のあるコンテンツの作成、AIのバイアスなどのさまざまな脅威からAIシステムを保護できます。そうしたテクノロジーには、従来のデータ暗号化、アクセス対策、AIで補強できる監査、またトレーニング・データやモデルを保護する新技術などがあります。

- **AIによる防御態勢でAIの脅威に対抗しつつ、意思決定には常に人間が関与する**

  データ漏えいや悪意のあるコンテンツの作成、AIによるバイアスなどのAIの脅威は、AIを使用して検知・対応することができます。しかしながら、脅威を構成するものの特定、その対応方法などの重要な意思決定には、常に人間が関与する必要があります。これは、AIシステムにはバイアスがかかったり間違いを犯す可能性があり、倫理的かつ責任ある方法でAIシステムを利用するには、人間の監視が必要なためです。

- **AIを通じて、時間がかかるタスクの自動化、仕事の削減、防御メカニズムの高速化を実現する**

  AIが作業を簡素化するように思いますが、実は、AIを利用して時間のかかるタスクを高速化することが、最終的には迅速に結果を出すことにつながります。たとえば、時間のかかる、マルウェアのバイナリのリバース・エンジニアリングに対して、AIは関連コードを素早く調べて、アナリストに実用的な情報を提供することができます。この情報を利用して、アナリストは必要なアクションを探すYARAルールを生成するようシステムに命じることができます。この例では、防御態勢のための仕事をただちに縮小し、迅速に結果へと繋げています。

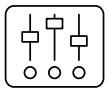
組織全体で一貫したセキュリティを実現するための プラットフォーム・レベルの調和的対策

- **AIの利用方法と、AIベース・アプリのライフサイクルを確認する**

  ステップ1で触れたように、AIの利用方法を把握することは重要な要素の1つです。組織でAIが広範に利用されるようになると、セキュリティ・リスクを特定・軽減するために、利用状況を定期的に確認するプロセスを実装する必要があります。このプロセスでは、利用中のAIモデルとアプリケーションの種類、AIモデルのトレーニングと実行に使用するデータ、AIモデルとアプリケーションを保護するために導入されているセキュリティ対策、AIセキュリティ・インシデントを監視・対応する手順、さらには全従業員に対するAIセキュリティ・リスクの認識向上とトレーニングの状況を確認します。

- **ツールとフレームワークの標準化を図ることで、対策のばらつきを防ぐ**

  前述のプロセスを導入すると、現在導入されている既存のツール、セキュリティ対策、フレームワークをより理解できるようになります。同時に、対策のばらつきを減らす上で、セキュリティとコンプライアンス対策に、異なるまたは重複するフレームワークがないかどうかを確認することが大切です。対策にばらつきがあると、複雑さが増したり、かなりの重複が生じたりします。ほかにも、コストが増加して、非効率となります。フレームワークと対策を調和させ、AI利用コンテキストへの適用性を把握することで、ばらつきを防ぎ、リスクを軽減する対策に「ピッタリ」のアプローチを見つけることができます。このガイダンスでは、主に既存の対策フレームワークと基準を取り上げていますが、同じ原則（全体の数をできる限り少なくする、など）は、新たなAIのフレームワークおよび基準にも該当します。



軽減策を調整し、AIデプロイメント時のフィードバック・ループを高速化するための対策

- **AIを活用した製品と対応能力の安全性とセキュリティを向上させるレッド・チーム演習を実施する**

  レッド・チーム演習はセキュリティ・テストの方法の1つで、倫理に従うハッカー・チームが組織のシステムやアプリケーションの脆弱性の悪用をテストするものです。組織はこの演習を通じて、悪意のある攻撃者がAI システムを悪用する前に、セキュリティ・リスクを特定・低減することできます。

- **プロンプト・インジェクションやデータ・ポイズニング、回避攻撃など、今までにない攻撃を乗り越える**

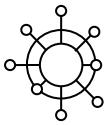
  そうした攻撃は、AIシステムの脆弱性を悪用して、機密データの漏えいや予測の誤り、あるいは業務中断などの害を及ぼす可能性があります。最新の攻撃手法を常に把握しておくことで、そうしたリスクを低減するための措置を講じることができます。

- **機械学習技術を適用して検知精度と速度を向上させる**

  AI利用に対する保護に注力することが重要である一方、AIはセキュリティの成果の大規模な実現にも利用できます。たとえば、AIが支援する検知および対応能力は、どのような組織にとっても重要な財産になります。同時に、関連するAIシステムやプロセス、意思決定の監視には、常に人間が関与することが不可欠です。こうした取り組みを通じて継続的な学習を促進することで、AIベースの保護、基礎モデル向けデータ・セットの更新トレーニングと微調整、および保護の構築に利用するMLモデルを改善することができます。このようにして、組織は脅威環境の進化に応じて、攻撃に戦略的に対応できるようになります。継続的な学習は、保護の精度の向上、遅延の短縮、効率性の向上にも重要です。

- **フィードバック・ループを構築する**

  前出の3つの要素の影響を最大化するには、フィードバック・ループを構築することが必要です。たとえば、レッド・チームがAIシステムの悪用を発見した場合、修復のみに焦点を当てるのではなく、その情報を組織にフィードバックすることで、防御の改善に役立てる必要があります。同様に、組織が新しい攻撃ベクトルを発見した場合は、継続学習の一環としてトレーニング・データ・セットにフィードバックする必要があります。フィードバックをうまく活用するには、さまざまな取り込み手段を検討し、保護にフィードバックを素早く反映させる方法をきちんと理解することが重要です。



ビジネス・プロセス周りのAIシステム・リスクのコンテキスト化

- **モデルとなるリスク管理フレームワークを確立して、AI関連リスクを把握するチームを作る**

  組織はAIモデルに関連するリスクを特定、評価、軽減するプロセスを策定する必要があります。チームは、AI、セキュリティ、リスク管理の専門家で構成します。

- **サードパーティのソリューションやサービスを利用する際、個々のユースケースと責任の分担に基づいて、AIモデルとそのリスク・プロファイルのインベントリを構築する**

  組織は、AIモデルの包括的なインベントリを構築し、サードパーティのソリューションやサービスを利用する際、個々のユースケース、データの機密性、責任の分担に基づいてリスク・プロファイルを評価する必要があります。これは、利用しているすべてのAIモデルを特定し、各モデルに関連する個々のリスクを把握して、そのリスクを軽減するセキュリティ対策を実装すると同時に、明確な役割と責任を割り当てることを意味します。

- **MLモデルのライフサイクル全体にデータ・プライバシー、サイバー・リスク、サードパーティ・リスクのポリシー、プロトコル、および対策を実装し、モデルの開発、実装、監視、検証を実施する**

  組織がモデルの開発、実装、監視、検証を実施するには、MLモデルのライフサイクル全体にデータ・プライバシー、サイバー・リスク、サードパーティ・リスクのポリシー、プロトコル、および対策を実装する必要があります。これは、MLモデルのライフサイクルの各段階に関連する各リスクに対処するポリシー、プロトコル、対策を開発し、実装することを意味します。対策のばらつきを防ぐには、常にフレームワークの4番目の要素に留意します。

- **AIの組織的利用を考慮したリスク評価を実施する**

  組織は、AIの利用に関連するリスクを特定、評価し、それらのリスクを低減するセキュリティ対策を実装する必要があります。組織は、モデル出力の説明可能性、ドリフトの監視など、対策の有効性を監視および検証するセキュリティ・プラクティスも含める必要があります。最初の2つの要素で触れたように、この取り組みを支援するには、部署横断的なチームを構成し、関連するユースケースの理解を深めることが重要です。組織はリスク評価に既存のフレームワークを使用して作業を進めることもできますが、アプローチを補強または適応し、新しいAIリスク管理フレームワークに対応する必要があります。

- **AIシステムの開発担当者、モデル・プロバイダーが開発したモデルのデプロイ担当者、モデルの調整担当者、あるいは既存のソリューションの利用に応じて、AIの保護責任を分担し、反映させる**

  AIシステムのセキュリティでは、それらのシステムの開発担当者、デプロイ担当者、ユーザーの間で責任を分担します。各当事者の具体的な責任は、AIシステムの開発とデプロイメントにおける役割によって異なります。たとえば、AIシステムの開発担当者は、設計上安全なAIシステムを開発する責任があります。この責任には、安全なコーディング・プラクティス、クリーンなデータでのAIモデルのトレーニング、AIシステムを攻撃から保護するセキュリティ対策の実装などがあります。

- **AIのユースケースをリスク許容度に一致させる**

  これは、各AIユースケースに関連する個々のリスクを把握して、そのリスクを低減するセキュリティ対策を実装することを意味します。たとえば、医療または金融など、人々の生活に重大な影響を与える可能性がある意思決定に役立てられるAIシステムでは、マーケティングまたは顧客サービスといった緊急性の低いタスクに使用されるAIシステムよりも安全性を厳格に確保する必要があります。

結論

AIは世界の人々の興味をかき立て、多くの組織がこの新しい技術を活用することで、創造性を高め、生産性を向上させる機会を見出しています。SAIFは、AIシステムの開発とデプロイ時のセキュリティ基準のレベルを高め、全体的なリスクを低減することを目的としてます。

サイバーセキュリティのクライシス・コミュニケーションの4つのフェーズ

クライシス発生時のコミュニケーションは、そうした事態に精通しており、十分に準備が整っている組織であっても対応が難しいと言えます。サイバー攻撃の独特な特性と攻撃者によるパブリック・ドメインの使用の増加は、被害組織がインシデント発生時に利害関係者とどのようにコミュニケーションするかが、技術的な修復の終了後も長期間にわたりブランドに影響を与える可能性があることを示しています。

対応をより複雑にするのは、サイバー・インシデントが発生し、組織が業務とネットワークを迅速に復旧しようとする際、コミュニケーション管理のプロセスにより、危機対応担当者と経営幹部の時間と注意の奪い合いが起こる可能性があることです。また、サイバーセキュリティのクライシス・コミュニケーションの範囲についても、しばしば混乱があります。メディア広報はコミュニケーション戦略の対応に関して目立つ活動ですが、相手は1人にすぎません。実際には、組織は社内外のすべての利害関係者に伝える包括的なコミュニケーション戦略を策定する必要があります。

特に一秒一秒が重要なストレスの多い時にコミュニケーション・ミスを避けるには、組織とその理事会が適切に対応できるよう、アドバイスや専門知識を提供するサイバーセキュリティのクライシス・コミュニケーションに精通した専門家がいることが役立ちます。セキュリティ脅威トレンドが進化し、攻撃者が新たな手法を取り入れる中、Mandiantは、インシデントレスポンス・チームとともにサイバーセキュリティのクライシス・コミュニケーション専門家を提供し、お客様によるインシデントの把握、ステークホルダーの関与の評価、関連するカスケード・コミュニケーションの戦略立案をサポートします。

サイバーセキュリティにおけるクライシス・コミュニケーションとは？

サイバーセキュリティに特有のクライシス・コミュニケーションとは、インシデントレスポンスと危機管理業務を組み合わせたコミュニケーションのことです。さまざまな利害関係者やチャネル向けにカスタマイズしたメッセージを策定し、複雑に計画されたタイミングでも配信できます。クライシス発生時には、コミュニケーション戦略において、業務への影響、リスク選好度、ブランドまたは評判悪化の可能性のほかにも、いくつかの要因を考慮する必要があります。たとえば、攻撃者の行動やインテリジェンスの傾向は、何をいつ、どのように伝えるかを決める際の重要な考慮事項です。特定のメッセージが攻撃者に漏れて、攻撃者の戦術、技術、手順の変更を引き起こす場合があるため、「戦略的非対応」が最善の対応となることもあります。

サイバー・インシデント中は特に、信頼とブランドの回復力が試される時ですが、その最中は信頼の構築を開始する時期ではありません。むしろ、クライシス・コミュニケーションへの組織のアプローチや、情報提供の失敗と透明性の欠如により、信頼がさらに損なわれることがあります。コミュニケーション・ミスは、組織全体の損失と業務への影響を悪化させます。このため、クライシス・コミュニケーションとは何か、クライシス発生時の対応に関するベスト・プラクティス、その時に備えた準備と計画をしっかりと理解しておくことは不可欠です。

サイバー・セキュリティクライシスの際、最善のクライシス・コミュニケーション対応を行うには？

Mandiantの経験からすると、侵害またはインシデント発生初日のかなり前から、準備を開始します。組織のインシデントレスポンスと事業継続計画の検討・分析・刷新の継続的サイクルの方が重要です。クライシス・コミュニケーションを特に取り上げ、サイバーセキュリティのクライシス・コミュニケーション計画に取り組む専門家が直接体験した中から学んだ教訓を紹介しましょう。こうした活動のサイクルは、戦略的なサイバー防御態勢の強化、保証、対応・インシデント後の精査の4つのフェーズに分類されます。

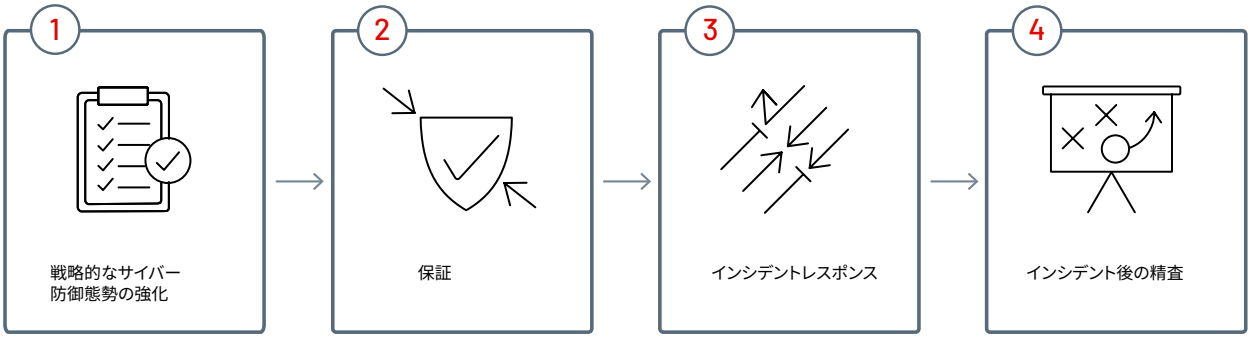
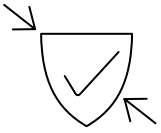


図1：サイバーセキュリティのクライシス・コミュニケーションの各フェーズ

第1フェーズ：戦略的なサイバー防御態勢の強化

最初のサイクルは、侵害前の「戦略的なサイバー防御態勢の強化」フェーズ、簡単に言うと計画段階のフェーズです。このフェーズは、規模や部署、場所に関係なく、どの組織においても基本的かつ不可欠です。組織に合わせてアプローチをカスタマイズし、役割と責任が明確に定義された書面による反復可能な計画、正式な意思決定の権限レベルがあるガバナンス構造、レスポンスのフレームワークを提供する必要があります。多くの運動競技のコーチと同様、対応担当者にとってこれは戦略であり、将来起こりうる活動に基づくものです。また、定期的に確認し、インシデント発生時に対応チームの一員となる個人と共有する、生きている文書としての役割も果たすものと考えてください。

役割と責任を明確に定義した適切なチームを常備しておくことが大切です。このチームは、組織全体の各部署（人事部、調達部、広報部、法務部、物流部、業務部など）の代表者で構成する必要があります。特に、ハードウェアのプロビジョニング、カスケード・コミュニケーションの伝達、洞察力に優れたデータの影響評価の実施に関しては、何が必要になるかは予測できません。また、チームは、職能的責任に沿った個々の作業グループとともに、ガバナンスと管理モデルを実装する必要もあります。計画フェーズ中に策定する成果物の1つが、インシデントレスポンス戦略の付随するクライシス・コミュニケーションです。この戦略は組織に固有のもので、インシデントとクライシス対応、仮説シナリオに基づく重要なメッセージ、利害関係者の特定とチャネル・マッピングに関するセクションを含める必要があります。もう1つ考慮すべき重要な点は、主となるコミュニケーション方法が侵害された場合のために、一般に「帯域外」通信と呼ばれる代替コミュニケーション・メカニズムを用意しておくことです。データ漏えいやサイバーセキュリティ・インシデントでは、攻撃者がネットワークに留まる場合があり、リーダーと対応担当者は代替のコミュニケーション方法を使用する必要があります。

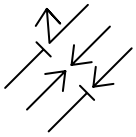


第2フェーズ：保証

第2フェーズは「保証」または演習フェーズで、侵害発生前のプロアクティブな対応の一部でもあります。このフェーズ中、企業は現実世界での攻撃とシナリオに基づき、チームの対応を演習する必要があります。一部の州では理事会の対応の一環として、これを義務付ける動きさえあります[1]。十分な訓練を受けた専門家を招いて、カスタマイズされた、現実的なシナリオに基づく演習を開発および促進する際に、こうした演習は必ず役に立つでしょう。演習では、チームは計画を実施し、戦略をテストして、修復のためのギャップを特定できます。また、チーム・メンバーは安全でストレスの少ない環境で、瞬発力を必要とする活動を訓練できます。本番が近づくにつれ、ミスの結果の重大性が増しますし、プレッシャーが大きくなると、ミスが起こる可能性は高くなります。実施と結果を予想しつつ、次に何が起こるかを予測できれば、落ち着いて冷静に対応することがずっと容易になります。

また、チームがアドバイスとフィードバックを受け入れることは、保証フェーズの一環として不可欠です。このフェーズはまた、経営幹部のリーダーシップ・チームや取締役会を超えたさまざまな職務内容とレベルの個人が組織全体から参加し、繰り返し行われる演習である必要があります。「ただ項目を読むだけ」の演習にするべきではありません。最後に、演習は「補強」チームまたはサージ・チームも対象にし、豊富な人材を揃えておく必要があります。対応チームは、少なくとも最初の30日間の持続的な取り組みと、人員のシフト体制を計画しておく必要があります。初期においては、たいてい24時間365日の対応となるでしょう。燃え尽きや極度の疲労を防ぐには、訓練を受けた救援対応者名簿を作成しておき、対応準備を整えておくことが大切です。事業継続計画やディザスタ・リカバリ計画、インシデントレスポンス計画に、コミュニケーションに関する付属文書またはセクションを設けておきましょう。

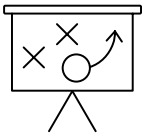
1. ニューヨーク州金融サービス局のDFS最高責任者、 アドリエンヌ・A・ハリス（Adrienne A. Harris）氏、サイバーセキュリティ規制の更新版を発表　2022年11月



第3フェーズ：インシデントレスポンス

第3フェーズは「インシデントレスポンス」の対応フェーズです。レスポンスの実行は、最初の2つのフェーズで導入された優先順位と重要度で決まります。時間の8割を計画、2割を実行に費やすべきと言われることがありますが、確かにこれは真実です。企業は、その日に備えて、チームを素早く立ち上げて対応できるようにしておくことが不可欠です。チームは自分たちの役割と責任を理解し、対応のための出動ガバナンス体制を整えておきます。重要な情報交換をまとめたり、アクション項目やタスクを追跡したりしておきます。利害関係者とのコミュニケーション・チャネルを開いておき、チャネルの準備態勢を素早く評価できるようにします。

最もスムーズかつ効果的に対応できる担当者は通常、十分な訓練を受け、十分な装備を備え、必要なツールを事前に準備している人です。彼らは、このフェーズが短距離走ではなくマラソンであることを自覚し、尊厳を備え、チームを尊重し、ペースを考えて対応します。意思決定の前には緊密に連携して情報を共有しますが、分析を邪魔することはありません。失敗したり、つまずいたりする組織は通常、アドバイスやフィードバックに耳を傾けることも、パフォーマンスの失敗の自覚もなく、対応とコミュニケーションの整理や調整がうまくできていません。



第4フェーズ：インシデント後の精査

感情と運用のどちらの観点からしても、侵害は管理が難しく、多くの人にとってインシデントの見直しは簡単ではありません。難しいかもしれませんが、最終フェーズである事後評価に進むことは大切です。このフェーズは、混乱が落ち着くとすぐに始まります。すなわち、調査が完了して、修復活動によって業務が回復し、規制当局または被害者への通知を終えた段階です。このフェーズは「行動後」または「教訓を学ぶ」フェーズとも呼ばれ、計画に次いで、徹底的に行われるべき、特に重要なフェーズの1つです。専門家はクライアントと連携することで、ギャップとソリューションを特定し、将来のインシデントの影響を低減することができます。

Mandiantの顧客事例から得たベスト・プラクティスには、事後評価で表面化したものもあります。インシデントと対応はさまざまです。出だしでつまずいて、後で盛り返すものもあれば、業界のベスト・プラクティスの模範となるものもあります。大切なことは、学んだ教訓を他の人の利益のために活かすことです。ウィンストン・チャーチルはこういっています。「歴史から学ばない者は、その過ちを繰り返す運命にある」と。

エスピオナージ・グループの標的となっているビジネスIoT

モノのインターネット（IoT）に接続するアクティブなデバイスの数は、2023年にはほぼ420億台に達すると予想されており[2]、スマート製造や小売在庫管理、デジタル決済、物理的なセキュリティと監視など、さまざまな業種にまたがるイノベーションと自動化の加速に貢献しています。さまざまなテクノロジーが進歩するにつれて、その副産物として、サイバー・リスクはあらゆる企業で起きること予想しておくべきです。

過去にMandiantは、IoTデバイス、スマート・デバイス、ルーターが侵害され、金銭を目的とした大規模なサイバー犯罪活動を実行するボットネットの作成に使用されているのを観測しています。 ボットネットは侵害されたデバイスのネットワークで、攻撃者はDDoS攻撃やマルウェアの配布など、さまざまな脅威活動の実行に使用できます。しかし、Mandiantは、国家とつながりのあるエスピオナージ・グループも複数の目的のためにボットネットを活用していると見ています（情報信頼度：中）[3]。こうした攻撃者の行動が明確に示すものは、グローバル企業から戦略的インテリジェンスや知的財産を得ようとする国家とつながりのある攻撃者にとって、IoTやスマート・デバイスの大規模な導入が攻撃の機会になるということです。

デジタル・トランスフォーメーションの継続、自動化の加速、新型コロナウイルス感染症パンデミックによる経済的影響後に失われたバリュー・チェーンの回復、あるいは5G接続ネットワークの展開を引き続き模索している組織[4]は、組織を保護できるよう、サイバーセキュリティ・チームと緊密に連携して、包括的なサイバー防御計画を策定しておくことが推奨されます。

活動の難読化の際に利用される、IoTデバイス、スマート・デバイス、ルーター・ボットネット

Mandiantは、当社とその他の民間および公共部門のセキュリティ研究者からの複数の活動観測から見て、国家とつながりのあるエスピオナージ・グループがIoTやスマート・デバイス、ルーターで構成されるボットネットを使用して、悪意のある活動を難読化させていると評価しています。侵害されたデバイスのボットネットをエスピオナージ・グループが使用した事例報告には、以下のようなものがあります。

- 2022年4月、Mandiant、QUIETEXITマルウェアを使用したコマンド＆コントロール（C2）活動の一環として、IoTカメラのボットネットを使用したAPT29による活動を報告[5]（図 2）。このC2活動で使用されたドメインは、感染したIoTデバイスの正規のトラフィックに溶け込むよう設計されており、明らかに、ログの確認担当者がこの行動に気づかないようにしています。

2. Frost and Sullivan、Internet of Things (IoT) Predictions Outlook、2022年11月
3. Mandiant、Espionage Actors Lurk in Compromised Device Botnets、2023 年 4 月
4. Frost and Sullivan、The Top Growth Opportunities for IoT in 2023、2023 年 3 月
5. Mandiant、https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

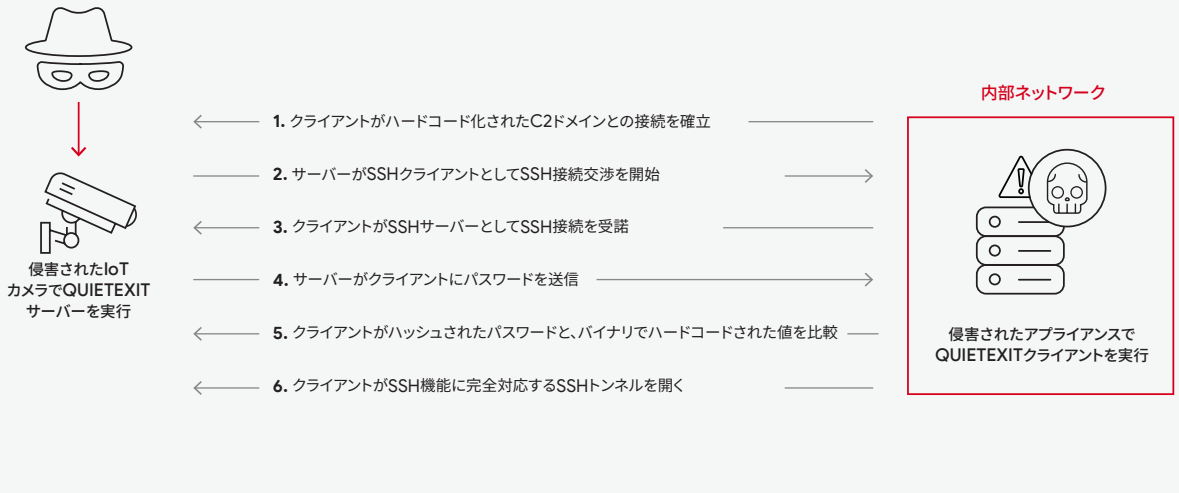


図2：QUIETEXITとIoTデバイスの連携

- フランス国家情報システム・セキュリティ庁（ANSSI、Agence nationale de la sécurité des systèmes d'information）が、2021年の報告書[6]で中国のグループ、APT31にリンクされた活動を詳細に報告。APT31は標的ネットワーク上の活動の難読化の目的で、ルーターのボットネットや、おそらくその他の小規模オフィスやホーム・オフィスのデバイスを使用するものと報じられています。
- 2022年、PricewaterhouseCoopersが、活動中に観測され「BPFDoor」と名付けられたマルウェアについて報告[7]。MandiantはこのマルウェアをAPT41と関連付けました。報告された活動では、このマルウェアは、台湾を拠点とする侵害を受けたルーターのネットワークによって制御された仮想プライベート・サーバー（VPS）からコマンドを受信していたとされています。
- 中国のセキュリティ企業、Antiyは2022年、侵害を受けたIoTデバイスとLinuxデバイスからなる大規模ネットワークが、C2サーバーとToriiマルウェア間のトラフィックをルーティングしていることを観測したと報告[8]。同社によれば、この行動はMandiantがAPT32と呼ぶOceanLotusによる可能性があるとのことでしたが、Mandiantはこの帰属を確認していません。
- 2018年、グローバルなネットワーク・デバイスとウクライナに過剰集中しているネットワーク接続ストレージ（NAS）デバイスをターゲットにした活動において、VPNFILTERマルウェアが使用されていると研究者が公式に報告[9]。一部サンプルには中間者攻撃（AiTM攻撃）と破壊的能力が統合されていると報告されていますが、これらのモジュールの目的は他にあった可能性があります。Mandiantは、このVPNFILTERの使用はロシアが支援するサイバー・エスピオナージ活動と同一のものであると見ています。

6. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-013/
7. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
8. https://mp.weixin.qq.com/s/2RluW4O56UWiNSQB2hQtGA
9. https://blog.talosintelligence.com/vpnfilter/
10. https://thehackernews.com/2018/06/vpnfilter-router-malware.html

公開レポートとMandiantの観察によると、一部の攻撃者が、他の攻撃者が作成した既存のボットネットを侵害または利用していることが示されています。この戦術がエスピオナージ・グループにとって有用となる状況は極めて限定されるため、将来的にこうした利用が大幅に増加することはないとMandiantは考えています。

- 2022年9月、Mandiant、Turlaチームとの関連が疑われるUNC4210による活動を発見[11]。この活動では、攻撃者らがANDROMEDAマルウェア・ボットネットに関連する少なくとも3つのC2ドメインをハイジャックしていました。このボットネットに関連するANDROMEDAのバージョンは、2013年に初めてVirusTotalにアップロードされ、感染したUSBキーから拡散していました。Turlaは期限切れのC2ドメインを再登録後、サーバーに接続した残りの感染を使用して、被害者のプロファイルと選択にアクセスできたようです（図3）。

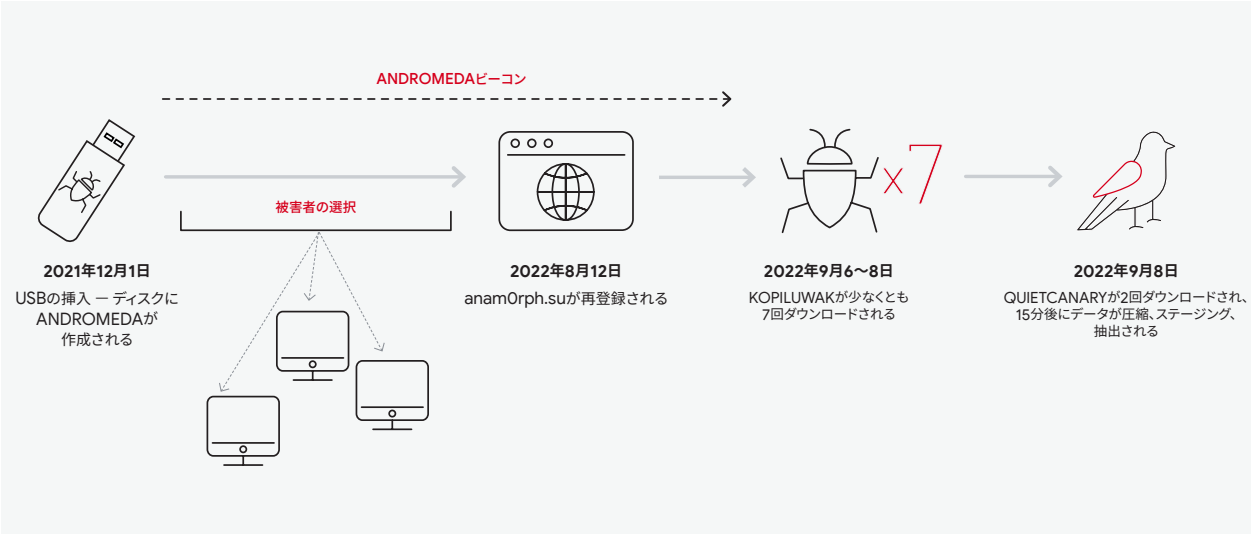


図3：ANDROMEDAからTurla侵入までのタイムライン

11. https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

IoTデバイスの保護

IoTやスマート・デバイスの設計は安全ではないことが多く、認証情報がハードコードされている、および/またはソフトウェアの脆弱性が発見された際に、パッチを適用することが困難または不可能である場合があります。そうしたデバイスを積極的にデプロイしている組織、またはデジタル・トランスフォーメーション計画にIoTを組み込んでいる組織は、デバイスが適切に保護されていること、不審な活動がないか定期的にチェック可能なことを確認する必要があります。図4は、資産所有者がそうしたデバイスのデプロイ計画と合わせて考慮すべき、IoTデバイスの製造と運用に関連するセキュリティ・リスクの概要を説明しています。

図4：IoTデバイス保護のための検討事項

デジタル・トランスフォーメーション中の組織にとっての意味

急速に普及しているIoTとスマート・デバイスは保護が不十分なことが多く、比較的少ない時間とリソースの投資で効果的な戦術的利点が攻撃者にもたらされます。このため、サイバー・エスピオナージ・グループは引き続き、この戦術を使用するものとMandiantは予想しています。また、IoTとスマート・デバイスの人気の高まりが続いており、特にそうしたデバイスを標的にしたツールが闇市場とオンラインで自由に入手できるようになる中、エスピオナージ・グループは、情報収集活動を無害または日和見的な金銭目的のサイバー犯罪を偽装する手段として、ボットネットの使用に関心を示す可能性があるとMandiantは推測しています。

エッジ・デバイス攻撃に対する回復力の確立

過去10年間にわたり、組織はデジタル環境全体における可視性を高めてきました。その結果、組織は多層防御スタイルのアーキテクチャに向けて移行を続け、攻撃者をより迅速に検知し[12]、パスワードの再利用や総当たり攻撃などの脅威から環境を積極的に保護するという面で著しく進歩しています。

この傾向は正しい方向に向かっており、多くの組織が、エンドポイント検出と対応（EDR）ソリューションが提供する可視性を軸とした検知および対応に注力しています。しかしながらEDRソリューションは、名前が示すように、エンドポイントにデプロイされるものです。つまり、ファイアウォール、IoTデバイス、VPN、ハイパーバイザー、その他の多くのデバイスは、通常、EDRでサポートされません。このため、一般的に「エッジ・デバイス」と呼ばれます。悪意のある攻撃者がエッジ・デバイスを標的にし始めたらどうなるでしょうか？

定義上、エッジ・デバイスはほとんどの組織の通常の検知範囲外にあるため、侵入時には攻撃者に多大な価値をもたらします。エッジ・デバイスは、方法が異なれど、常に攻撃者の標的になります。そうしたエッジ・デバイスは、内部セキュリティ・ツールの監視など、多くの貴重なサービスを組織に提供しますが、これまでEDRソリューションには対応しておらず、システム・レベルで監視されることもほとんどありませんでした。この種のシステム・レベルの監視は、コードが変更されているか、または対象のマルウェアがインストールされているかを割り出す場合に必要です。

エッジ・デバイスはセキュリティの追求と保護に利用されるものの、本質的にそれ自体は保護されません。端的に言えば、通常、ベンダーはユーザーのオペレーティング・システムまたはファイル・システムに直接アクセスできません。検知はそうしたエッジ・デバイスやシステムにまで拡張されないため、防御側が潜在的に異常な動作の根本的な分析を実行する能力は限られます。

12. M-Trends 2023、Mandiant、2023年4月

過去5年間、Mandiantは、国家の支援を受けた攻撃者がエッジ・デバイスを標的にしていることを示す証拠が増えていることを確認しています。こうしたエッジ・デバイスへのフォーカスは、攻撃者にとって有利になる一方、防御側にとっては懸念事項となります。エッジ・デバイスが悪意のある侵入の標的になり、標的環境において足場の獲得、または存在の維持ができる可能性が高くなります。エッジ・デバイスは、悪意のある攻撃者に単純な足場だけでなく、多くのメリットをもたらします。まず、エッジ・デバイスは環境内の可視性と権限を高め、ネットワークの監視または安全なアクセス・ポイントをもたらします。また、攻撃者はエッジ・デバイスにアクセスすることで、操作のタイミングを制御できるようになり、検出される機会が減る可能性があります。定義上、エッジ・デバイスはEDRソリューションから見えません。つまり、攻撃側にはこうしたすべての利点があると同時に、防御側から隠れ続ける可能性があります。

国家の支援を受けた攻撃者は、これまで知られていない脆弱性を特定し、悪用することを目的として、しばしば広範囲の研究や開発サイクルにかなりの時間と労力を費やします。中国とのつながりが疑われるグループがゼロデイ脆弱性を悪用し、カスタム・マルウェアをデプロイしてユーザーの認証情報を盗み、被害者環境への長期アクセスを維持する数十件の侵入を、Mandiantは長年にわたって調査してきました。たとえば、2022年、UNC3886はファイアウォールなどのエッジ・デバイスを標的にし、その後の攻撃ライフサイクルではハイパーバイザー・テクノロジーを標的にしていました。

UNC3886の事例研究

Fortinet[13]のエコシステムにある複数のコンポーネントは、VMWareインフラストラクチャへの水平展開を行う前にUNC3886の標的になっていました。侵害発生時の、それらコンポーネントとその関連するバージョンは以下のとおりです。

- **FortiGate: 6.2.7** – FortiGateユニットは、デバイスを通過するネットワーク・トラフィックの対策と監視ができるネットワーク・ファイアウォール・デバイスです。
- **FortiManager 6.4.7** – FortiManagerは、Fortinetデバイスを管理する一元型の管理プラットフォームです。
- **FortiAnalyzer 6.4.7** – FortiAnalyzerは、Fortinetデバイスの一元型ログ管理ソリューション、および報告用プラットフォームです。

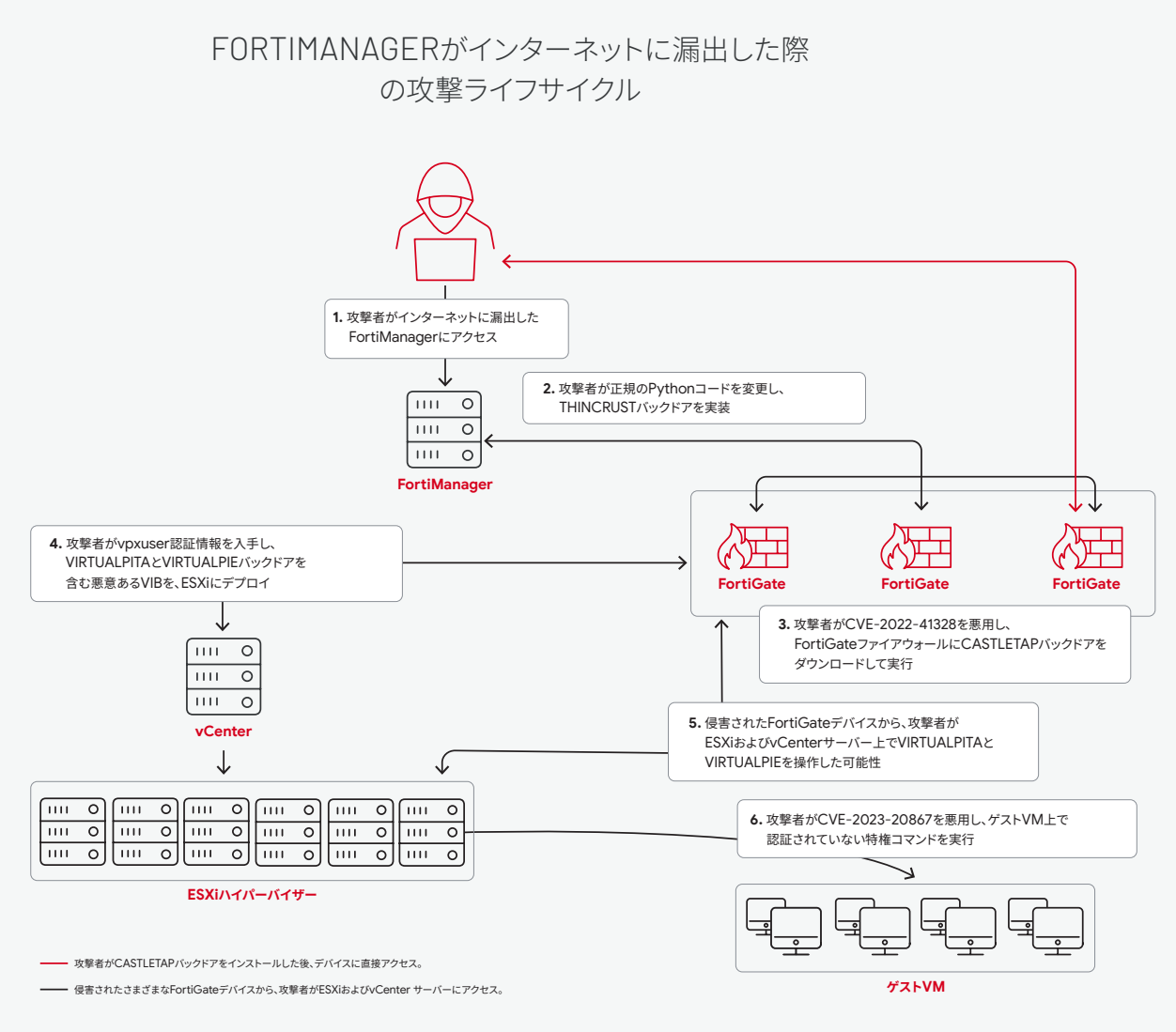


図5：FortiManagerにインターネット・アクセス制限が実装された後の動作

13. https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

2022年、Mandiantは中国とのつながりが疑われるグループ、UNC3886の追跡を開始しました。このグループは、特にFortinetのエコシステムを標的にしており、最終的にはターゲット環境内で水平展開し、VMWareインフラストラクチャにアクセスしました。このアクセス権を得るため、UNC3886には、FortiGate（ファイアウォール）、FortiManager（一元型管理ソリューション）、FortiAnalyzer（ログ管理、解析、報告用プラットフォーム）など、複数のFortinetソリューションに関する十分な知識があることが立証されました。UNC3886はこの知識を活用して、FortiManagerデバイスとFortiAnalyzerデバイスにバックドアをデプロイし、持続性を得ようとしました。Mandiantは、これらのイベントを**THINCRUST**として追跡しています。ほかにも、UNC3886はFortiManagerのネイティブ・スクリプトへのアクセスを利用してCVE-2022-41328を悪用し、FortiGateデバイスに別のバックドアである、**CASTLETAP**をダウンロードおよび実行して、環境内でのアクセス権を引き続き維持しようとしました。

Mandiantは、標的の環境内のFortinetデバイスからESXiサーバーへのSSH接続と、それに続く**VIRTUALPITA**と**VIRTUALPIE**バックドアを含むvSphereインストール・バンドル[14]がインストールされたことを観測しました。

FortiManagerがインターネットから制限された別のシナリオでは、UNC3886が以前に確立していたアクセス権を利用して、ネットワーク・トラフィック転送ユーティリティ（Mandiantでは**TABLEFLIP**として追跡）と**REPTILE**のリバース・シェル・バックドアの亜種をFortiManagerにインストールしました。このマルウェアの併用により、UNC3886は外部アクセスを制限するネットワーク・アクセス・コントロール・リスト（ACL）を回避できています。

これらのいずれのシナリオでも、UNC3886は正規のシステム・プロセスを使用して偵察コマンドの実行とデータの抽出を開始し、その後、Fortinetエコシステムと VMwareハイパーバイザーの両方が完全に侵害されて、悪意のある活動が展開されています。

この事例研究についての詳細は、ブログ「Fortinetのゼロデイ マルウェアとカスタム マルウェア、中国の攻撃者によるスパイ活動で使用された疑い」**を参照してください。**

CASTLETAPはパケットを受動的に待ち受け、ICMP Echoパケットを受信するとバックドア機能をアクティブ化するLinuxバイナリです。これらのパケット内で、マルウェアはSSLソケット経由で接続を回復できるC2サーバー情報も検索します。その機能としては、ファイルのアップロードとダウンロード、通常のシェルおよびビジーボックス・ベースのシェルの生成などがあります。

THINCRUSTは、HTTPリクエストでリモート・コマンドの実行、ファイルの読み取り、書き込みができるサードパーティのライブラリ・コードに埋め込まれたPythonのバックドアです。暗号化されたコマンドはHTTP Cookieに保存されます。

VIRTUALPITAは、ハードコードされたTCPまたはVMCIポート番号にリスナーを作成する、LinuxおよびVMware ESXiの64ビットのパッシブ・バックドアです。任意のコマンドの実行、ファイルのアップロードとダウンロード、vmsyslogdの開始と停止が可能です。

VIRTUALPIEは、ハードコードされたTCPポート上にデーモン化したIPv6リスナーを生成する、Pythonで作成されるバックドアです。ファイルの転送、任意のコマンド実行、リバース・シェル機能を持っています。このバックドアはカスタム・プロトコルで通信し、データはRC4を使用して暗号化します。

TABLEFLIPは、トラフィックを転送するユーティリティです。すべてのアクティブなインターフェイスで、特別なコマンド・パケットを受動的に待ちます。パケットには、iptableコマンドを使用してトラフィックを転送する、XORエンコード化されたIPアドレスとポート番号が含まれます。

REPTILEはC言語で書かれた、公開されているLinux rootkitです。ポートノッキングを介してICMP、UDP、またはTCPパケットでアクティブ化できるバックドア機能を持っています。その他の機能としては、リバース・シェルやファイル転送があります。

14. https://blogs.vmware.com/vsphere/2011/09/whats-in-a-vib.html

APT29の事例研究

さらにMandiantは、APT29のような国家の支援を受けた攻撃者が、新型のトンネラーで同様のタイプのエッジ・デバイス・アプライアンスを標的にしていることも観測しました。

2022年初め、APT29は標的の環境へのアクセス権を取得後、環境全体のエンドポイントに**QUIETEXIT**をデプロイしました。あるケースでは、APT29は正規のアプリケーション固有の起動スクリプトをハイジャックし、ネイティブな持続メカニズムがない**QUIETEXIT**を起動時に実行できるようにしました。**QUIETEXIT**はSSH機能を完全にサポートしており、APT29は標的環境へのSOCKSトンネルを利用します。このため、APT29は標的のコンピュータ上にほとんど証拠を残さず、データを盗むツールを実行できます。APT29は、バイナリ名になりすましてファイル・システム上の正規のファイルに紛れ込ませる、ネットワーク接続ストレージ（NAS）を標的にしていました。追加のアクセス権を維持するため、APT29はDMZ Webサーバー上に二次的なバックドア、**REGEORG** Webシェルをデプロイしました。これは、サポートされているウイルス対策ソリューションまたはEDRソリューションの欠如と相まって、滞留時間の長期化につながりました。

QUIETEXITは、リモートC2に接続するリバースSSHトンネラーですが、認証にはパスワードが必要です。QUIETEXITはSOCKSを介して、コマンドやプロキシ・トラフィックを実行できます。QUIETEXITは、オープンソースのDROPBEAR SSLクライアント・サーバー・ソフトウェアから派生します。

REGEORGは、Webシェル・トラフィックのトンネリングに使用されるオープンソース・ユーティリティです。

QUIETEXIT。Mandiantが観測したコマンド＆コントロール（C2）システムは主としてレガシーな会議室カメラ・システムで、QUIETEXITのサーバー・コンポーネントに感染している可能性がありました。これらの信頼できるシステムを標的にすることで、APT29は標的環境で少なくとも18か月間、検出されることはありませんでした。

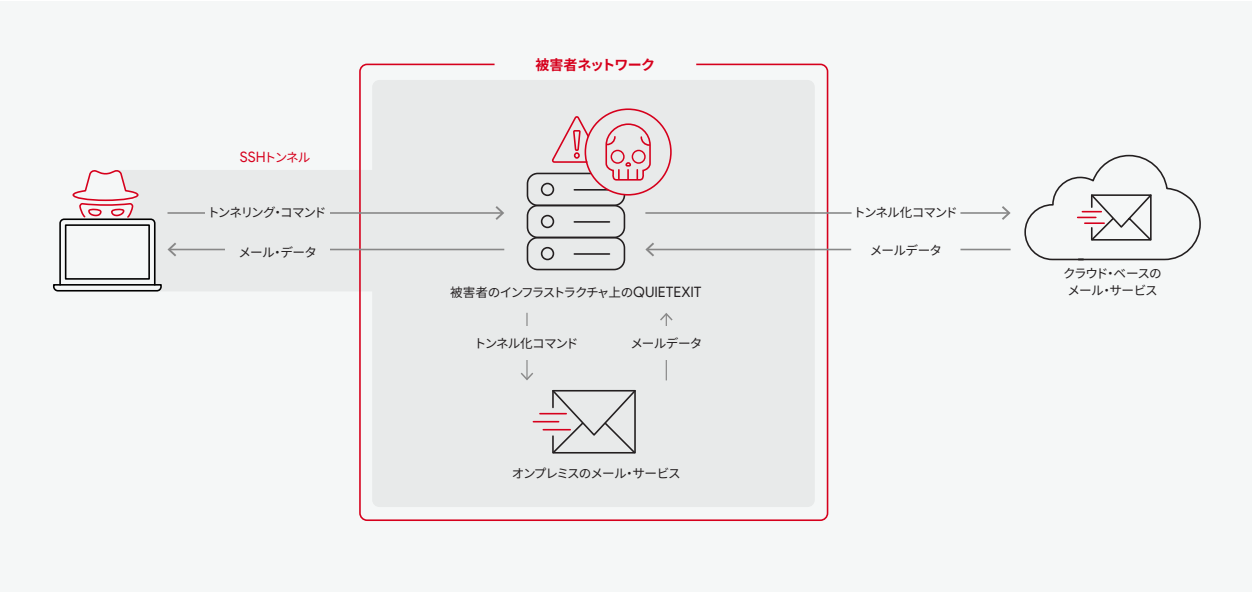


図6：QUIETEXITを使ったトンネリング

ミッションを完了したAPT29は、標的の電子メール環境への特権認証情報を得ることに成功し、企業開発、合併・買収に関与する経営陣や従業員、またはITセキュリティ・スタッフの情報搾取を集中的に行いました。いくつかのケースでは、APT29は、調査当局が対応の際に利用するプログラム化された検索および電子メール・データへのアクセスで使用するものと同じ、eDiscoveryとGraph APIツールを活用しています。これらのツールにより、APT29は大量の電子メールを漏出していました。

この事例研究についての詳細は、ブログ「Eye Spy on Your Email」を参照してください。

APT28の事例研究

2022年、MandiantはAPT28が過去の活動から逸脱していることを観測しました。このグループは、エッジのインフラストラクチャを侵害して、さまざまな作戦を実行する傾向を示しており、この手法は「Living on the Edge」と呼ばれています。ウクライナ戦争が始まって以来、GRUとして知られるロシア軍事諜報機関は、ウクライナ国内の主要サービスと組織に対して、連続的かつほぼ恒常的にサイバー・エスピオナージ活動と破壊活動を行っています。標的組織へのアクセスとそれに対する活動のバランスは、ルーターとその他のインターネット接続デバイスなどのエッジ・インフラの侵害によって異なります。

この事例研究についての詳細は、M-Trends 2023、「ウクライナ侵攻：戦時下のサイバーオペレーション」を参照してください。

主な教訓

これらの事例研究では、攻撃者は、設計上エッジ・ネットワークを標的にして、検出されないようにしており、攻撃者の侵入後の行動中に環境内で侵害の証拠が検出されました。調査中、Mandiantは影響を受けたシステムを徹底的に精査し、最初の侵入経路を特定しています。これらの事例には、エッジ・デバイスのIPアドレスまでのアクセスを遡って追跡できる証拠が存在していました。このため、調査当局はベンダーと協力することで証拠を遡り、それらデバイスのフォレンシック画像を収集し、分析を進めました。組織横断的なコミュニケーションとコラボレーションは、世に出回っている新しい攻撃手法を公開前にいち早くメーカーに通知し、それらの新しい攻撃をより詳しく解明する専門知識を調査当局に提供する際に重要な鍵となります。

エッジ・デバイス攻撃に対してできる対策

サイバー・エスピオナージ関連の攻撃者は、通常EDRをサポートしていないシステムに対するツールと悪用の研究および開発への投資を増大させています。これらのタイプのツールと悪用には、標的にされたオペレーティング・システムに関する深い理解が必要です。組織はセキュリティ・オペレーション・センター（SOC）の構築を続ける一方で、エンドポイントの検知以外にも可視性を継続的に拡大する必要があります。可視性のギャップにより、攻撃者は最小限の努力で検知を回避できます。こうした可視性のギャップを突き止めることが、組織のセキュリティを支援する効率的なSOCを構築するための次のステップです。組織はネットワーク上のデバイスのインベントリを作成し、それぞれに監視ツールが使用できるかを評価する必要があります。監視ツールをサポートしていない各デバイスには、個々のベンダーが適切なログ記録を行うための強化対策が求められます。組織は、そうした各ベンダーのログが中央のリポジトリに転送されるようにする必要もあります。それらデバイスからの出力トラフィックを制限または完全に禁止する、ネットワーク・アクセス対策の利用も評価しなければなりません。追加のネットワーク監視を実装し、エッジ・デバイスとその他の非EDR対応テクノロジー間の異常トラフィックを検知することで、上記のネットワーク対策が実現不可能な場合でも、さらなる検知能力を発揮できるようになります。

その他のリソースについては、以下を参照してください。

MandiantのMicrosoft 365強化ガイド

ESXiハイパーバイザー内の検知とハードニング

特権資産管理を実装する際の6つのヒント

クラウド・サービスやSaaSアプリケーションの導入が増えたことで、組織が運用および管理する必要があるアカウント数が飛躍的に増えています。たとえば、現在、従業員は平均して30の法人アカウントとアプリケーションにアクセスしています。ほかにも、マシンID、デジタル証明書、キーの数は現在、個人ID数の45倍[15]を上回ります。

不要なアカウントの削減や、必要のない個人やシステムに対する過剰な特権の削除に苦労している組織にとって、特権アクセス管理（PAM）の実装は有益です。

PAMは、以下によって企業内の資産に対するアクセス権を管理し、保護します。

承認ワークフローの作成

秘密の安全な保存と暗号化

特権アクセス・イベントの監査、監視、ログ記録

秘密管理のポリシーの設定（パスワードの変更など）

セッション・マネージャーを使った標的システムへのアクセスの保護と分離

従来、組織はPAMへのアプローチの主要テクノロジーとして多要素認証（MFA）ソリューションを採用してきました。しかしながら、MFAソリューションが適切に実装および維持されていないと、組織に意図しないリスクが生じる可能性があります。

15. 特権アクセス管理を優先する5つの理由、CyberArk、2022年

2017年	2019年	2021年	2022年
Equifax 約1億4,700万人の消費者の個人情報（PII）へのアクセス権が漏出。	**オーストラリア国立大学** 19年分にわたる職員と学生のPIIにアクセスされる。	**Verkada** サプライ・チェーン攻撃により、病院、学校、刑務所で利用されているVerkadaセキュリティ・カメラ・システムにアクセスされる。	**アメリカ合衆国退役軍人省** 医療記録を含むシステムへの機密資格情報がGitHubに漏出。

図7：攻撃者が特権アクセス管理ソリューションを悪用した際に発生する侵害のタイムライン

これまで、攻撃者はアクセス管理ソリューションの脆弱性を悪用し、高い成功を収めてきました。規模と範囲に関する注目すべきデータ漏えいでは、2017年にまで遡るEquifaxのPAM脆弱性が挙げられており、攻撃者は1億4,700万人の消費者の個人情報と特権情報へのアクセス権を得ました[16]。その後も、オーストラリア国立大学では、医療記録を含むシステムへの機密資格情報がGitHubに漏出しています[17]。2021年、物理的セキュリティ・ベンダー、Verkadaへのサプライ・チェーン攻撃で、病院や学校、刑務所で使用されているセキュリティ・カメラ・システムへのアクセス権が漏出しました[18]。2022年には、アメリカ合衆国退役軍人省が、請負業者による特権アカウントの認証情報のデータ漏洩の被害を受けました[19]。

Mandiantは、攻撃者が複数の事例でMFA対策の回避に成功していることを観測しています。ある事例では、ロシアを拠点とするAPT攻撃グループが、標的被害者の電子メールや電話、登録済みデバイスに二要素認証リクエストを繰り返しプッシュすることでMFA疲労攻撃[20]を実行し、電子メール・アカウントへのアクセス権を入手して、通信詐欺インシデントを行いました。

Mandiantはほかにも、APT29[21]が組織内のMFAの自己登録プロセスを利用しているのを観測しています。ユーザー名とパスワードがあれば、誰でもデバイスを登録できていました。APT29は、パスワード推測攻撃を実行して、デバイスが登録されていないアカウントを検索し、独自のアカウントを追加しようとしました。

組織の規模またはPAMプログラムの成熟度に関係なく、セキュリティ・リーダーはPAMを実装する際には、ビジネスの安全を確保するために時間をかけて、これら7つのヒントを確認する必要があります。

16. Wallix Cybersecurity、Equifax Breach: Preventing Data Breaches with Privileged Access Management
17. オーストラリア国立大学、Incident Report on the Breach of the Australian national Universities Administrative Systems、2019 年
18. Verkada、Summary: March 9, 2021 Security Incident Report、2021年
19. VA investigates breach after federal contractor publishes source code、2022年9月
20. Mandiant、Suspected Russian Activity Targeting Government and Business Entities Around the Globe、2021年12月
21. Mandiant、APT29、Microsoft 365を標的とした攻撃を継続、2022年8月

01

特権アカウントについて

セキュリティおよびITリーダーがよく尋ねられる質問に「特権アカウントとは何か？」があります。一般的な回答は「すべてのアカウントにあるレベルの権限のこと」ですが、より高い権限を提供するアカウントも存在し、そのカテゴリには以下のようなものがあります。

- **ドメイン管理者：**ドメインに対する完全な制御権を持つユーザー。
- **個人特権アカウント：**通常のユーザーより多くの権限があるユーザー・アカウント。ユーザーはケース・バイ・ケースで利用します。
- **デフォルトのアカウント：**システムまたはアプリケーションによって自動的に作成されるアカウント（SA、Root、mysql、ec2-userなど）。
- **サービス・アカウント：**マシンに割り当てられた、法人システム、サービス、アプリケーションへのアクセス権を提供するアカウント。
- **Root、スーパー管理者、またはグローバル管理者（クラウド）：**ユーザーにローカル・デバイスに対する完全な制御権を付与するその他のシステム管理者アカウント。
- **緊急アクセス用アカウント：**セキュリティ・インシデント発生時にシステムへのアクセスに使用するアカウント。
- **セキュリティ・アカウント：**セキュリティ担当者がシステムにアクセスし、セキュリティ監査と調査の実行に使用するアカウント。

特権アクセスを提供するアカウントの悪用にまつわるリスクを理解することは重要です。最小権限で開始し、各ユーザーがそれぞれの役割で定義されたアクションのみを実行できるようにします。

個人識別情報（PII）または知的財産（IP）にアクセスするロールには、特に注意してください。

取るべき対策

- **組織内の特権アクセスのリスク評価を実施する。個人とシステムの両方について、重要な資産と情報へのリスクとなるアカウントを特定する。インタラクティブなログオンなどの本人確認手順を含め、権限の種類を検討する。高リスクのPAMアカウントを優先する。**
- **上級管理者や経営幹部の同意を得ることで、組織内の全体的なリスクを低減するツールの実装を促進する。**
- **実装の際には必ずセキュリティ・チームと情報テクノロジー・チームと協力して、さまざまなユーザー・グループのニーズと、PAM実装に必要なコミュニケーションと変更管理に対応する。**
- **アカウントに割り当てられた権限の再証明と検証を実施する。このアカウントを維持する際、新しいユースケースがあり、適切な承認を得た後、適切なタイプのアカウントを作成するか、期間限定アクセス・ポリシーを付与するのでない限り、変更してはならない。**

02

アカウントの作成、検出、オンボーディングのための連続的なプロセスを確立する

PAMは環境全体に実装されるため、PAMチームは組織内のセキュリティ・ギャップにプロアクティブに対処する必要があります。この取り組みでは、アプリケーション・チームによって必要と判断されたアカウントのすべてを登録し、PAMソリューションでそれらアカウントを管理する理由についての理解が重要です。

必要なアカウントをすべて登録しないと、保護されていない特権アカウントが急増し、組織が脆弱なままとなります。攻撃者はそうしたアカウントを悪用してシステムにアクセスし、権限を引き上げ、水平展開し、持続性を確立できるようになります。

特権アカウントの安全性の問題は、新しいアカウントやサービスを環境に追加する場合には特に重大です。アカウントやサービスの追加により、特権アカウントの攻撃対象領域と検出範囲がさらに拡大し、セキュリティ侵害のリスクが増大します。

環境内の古いアカウントと新しいアカウントすべてを含んだインベントリを維持することで、組織はセキュリティ・インシデント中にどのアカウントが危険であるかを素早く特定できます。この対策は、アカウントを保護し、アクセス権を持っているシステムを特定し、重要な資産にアクセスするため、信頼できるルートを作成する上で役立ちます。そうすることで、セキュリティ・インシデントへの対応の際、セキュリティ・チーム、インシデント対応担当者、インシデント・マネージャーへのプレッシャーを軽減できます。

取るべき対策

- **アカウントの作成時に登録して、「検出範囲」の拡大を回避する。**
- **検出ツールを使用して漏れているアカウントを特定、登録し、アカウントのライフサイクルを管理する効果的な対策を実装する。**
- **特権アカウントの範囲を把握する。知的財産、PII、またはPHIの保存場所とアクセス方法を検討する。**
- **アカウント検出のための継続的なプロセスを確立する。チームと協力して、作成、検出、登録を自動化する。**
- **MITRE ATT&CK®フレームワークを利用して、敵対者が権限昇格攻撃の際によく使用するさまざまな悪用手法を精査する。**

03

PAM実装に対する適切なアクセス対策を徹底する

PAMの目的は、環境に入るための鍵を保護することにあります。特権ユーザー・アカウントとシステムが標的になり得るため、PAMソリューションへのアクセス権を管理する必要があります。

PAM管理に関する承認と保護対象のディレクトリをリンクさせてはいけません。そうしたアクセス権は、PAMツールのビルトイン・ディレクトリを使用して管理します。

また、承認のワークフローを検討します。この対策によって組織内部の脅威に対する防御力が向上し、PAMチームはPAM用に実装されたシステムの制御方法を理解することができます。

取るべき対策

- 特権付きアカウントを登録する。
  - PAMツール管理者
  - アプリケーション・アカウント
  - サーバー・アカウント
  - 自動化とスクリプト
- PAMソリューションを使用するためのアクセス・モデルを確認し、有害な特権の組み合わせを特定する。
- PAMソリューションの管理アカウントに適切に権限が付与されていることを確認し、アプリケーションが保護する認証情報へのアクセスを制限する。
- 承認とアクセスのワークフローを確立し、重要なアカウントを保護する。
- 重要なセキュリティの知識があるチームが、トレーニング、イネーブルメント、専門家からのサポートにより、組織のセキュリティ態勢を継続的に向上できるようにする。

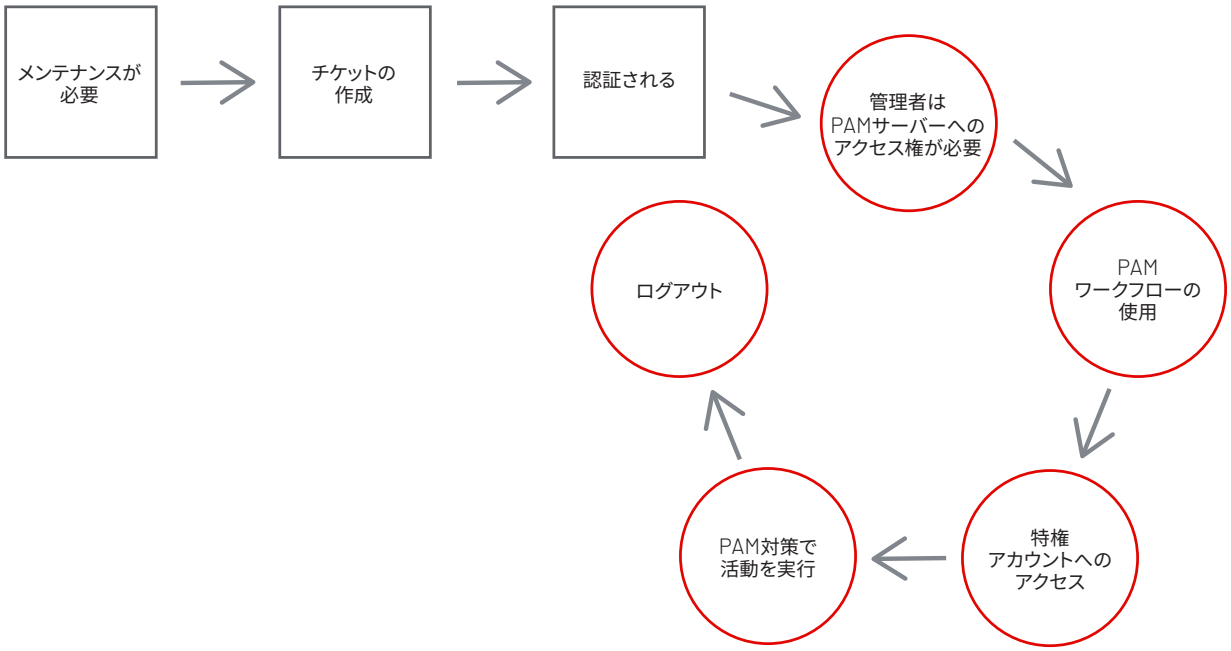


図8：PAM承認のワークフロー

04

アクセス・ルートのマップを作成して保護する

組織内の資産にアクセスする際、特権アクセス権の保護に重要となる取り組みがいくつかあります。取り組みの1つは、パスワードがエンドポイント・システムに漏出するのを防止することです。ユーザーと標的システムとの間で何が起きるかも検討します。

トラフィックの送信に信頼済みのパスが利用されているか？
そうしたパスを強制する方法は？

その他にも問うべきことは、

- 接続にWebリソースが必要か？
- そのWebリソースはワークステーションから直接接続しているか？
- 接続にはHTTPSが使用されているか？

標的へのフローとパスを把握することで、脅威のリスクの大きさがわかります。アプリケーションがシークレットにアクセスする方法、アプリケーションとサーバー間でそのシークレットが使用される方法についても検討する必要があります。

取るべき対策

環境内のアクセス・マップを作成し、PAMツールが提供するものにアーキテクチャがマッピングされていることを確認する。

- **使用する安全なプロトコルを決定し、セッション・マネージャーと標的へのアクセスに取るべきルートを決める。**
  - **RDPではなく、HTTPSで接続する**
  - **NACLをクリアな状態に保ち、送信アクセスのみを許可する場合は、リバース・リスナーの使用を検討する**
  - **認証情報とアクセス階層化モデルを確立する**
- **サードパーティが安全な認証メカニズムで保護され、承認が正しくプロビジョニングされていることを確認する。**
- **サードパーティが安全な方法で接続していることを確認する。**
- **アクセス・ルートの特定：**
  - **内部ネットワークとパブリック・ネットワークを経由するパス**
  - **クリーンなソース・システム**
  - **強力なアクセス階層**
  - **認証情報の保護**
  - **アクセス・ルートのテスト**

05

適切な設定でログ記録を実装する

ログを記録・監視することで、サイバー攻撃後に不可欠な貴重な情報を得ることができます。ログの記録と監視の目的は、サイバー・インシデントの範囲と影響を特定することにあります。フォレンジック調査では、ログのソースを使用することで、サイバー・インシデント中に生じる多くの問いに答えることができます。たとえば、フォレンジック調査はデータ漏出を特定する際、ファイアウォールやネット・フローのログ・データに大きく依存します。データ漏出やネットワークから漏出したデータ量に関する問いに対する答えが、こうしたログに含まれている場合があります。ほかにも、ユーザーの活動の追跡にも利用できます。特権アカウントが侵害された場合、ログ記録はそのユーザーが実行したアクションの追跡に役立ちます。

取るべき対策

- 組織全体で特権アカウントの活動を捕捉するログ記録と監視ソリューションを実装する。
- ログ記録を適切に設定する。ログに記録する必要がある活動のタイプとそれらログの保持についての概要を示す、ログ記録と監視ポリシーを策定する。
- 適切なシステムにログ・データを送信していることを確認する。データを組織内防御の強化に活用しているかどうかを確認することは、より重要。セキュリティ・チームは脅威解析を活用して、導入されている対策をさらに改善することも、あるいは攻撃者が環境内に侵入した指標として利用することもできる。
- システム・アクセスなど、ユーザー活動に異常がないか確認する。
- インシデント発生時のアクション計画を把握しておく。SIEMに保存しない場合は、監査ログとデータを確認する計画を作成する。

06

MFAを実装する

多要素認証（MFA）は、デジタルIDを証明し、単一のアクターまたはエンティティを介してシステムへの安全なアクセスを確立する上で重要です。

MFAでは、ユーザーは複数の認証要素を提供し、アプリケーションにアクセスする必要があります。最も一般的な2つのMFA形式は、ワンタイム・パスコード（OTP）とプッシュ通知です。OTPとは、ユーザーがMFAアプリケーション（Google Authenticatorなど）を介してモバイル・デバイスで受信するコードで、認証に利用できます。プッシュ通知は、ユーザーのモバイル・デバイスに通知を送信することで、ログインを承認/拒否できます。

いずれの方法も、フィッシング攻撃または中間者攻撃に対して脆弱です。最近の攻撃を見ると、MFAプッシュ通知またはSMS配信コードだけでは、アクセスの保護が十分とは言えません。たとえば、MFA疲労[22]攻撃は、攻撃者がユーザーにプッシュ通知を大量に送信し、ユーザーを苛立たせ、同意をクリックすることを期待するものです。

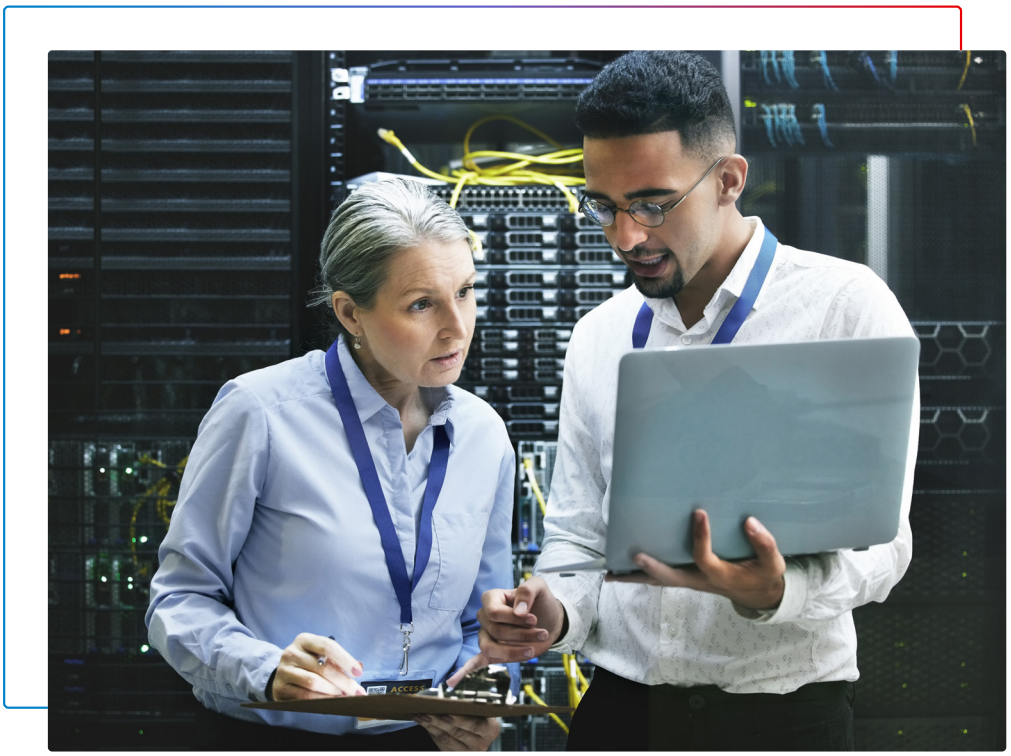
取るべき対策

- 強力でフィッシング耐性のあるMFAを実装する。
  - 生体認証あるいはハードウェアキー（YubiKeyなど）を使用したFIDO2認証
  - 単に受諾（番号一致）だけではないチャレンジ/レスポンスメカニズムの使用
- 従業員全体のトレーニングを実施して、従業員にMFAを正しく活用できる知識があることを確認する。
- 攻撃を受けていると思われるアカウントに対してアラートとリスク・ベースのタグを導入する。
  - 地理的位置
  - 異常なアクセス期間
  - MFAのチャレンジ/レスポンスでの過剰なリクエスト
- 使用されているオーセンティケーターの認証保証の確認
- アイデンティティに対する脅威ハンティングの実行

22. Mandiant、Suspected Russian Activity Targeting Government and Business Entities Around the Globe、2021年12月

結論

セキュリティ態勢の強化のためにPAMソリューションを実装する企業は増えていますが、そうしたツールを適切に構成して実装することが重要です。設定ミス、適切なアクセス管理不足、組み込みの機能の活用不足は、セキュリティに対する誤った認識をもたらす重要な要因の一部となり、場合によっては企業リスクの増大につながる可能性があります。



詳しくはwww.Mandiant.jpをご覧ください。

Mandiant

〒106-0032
東京都港区六本木6丁目10番1号
六本木ヒルズ森タワー
03-4577-4401
japan@mandiant.com

Mandiantについて

Mandiantは、ダイナミックなサイバー防御、脅威インテリジェンス、インシデントレスポンス・サービスのリーダーとして知られています。長年にわたり攻撃の最前線で得た豊富な経験を活かし、サイバー脅威に対する防御と対応においてお客様組織を支援します。Mandiant は現在、Google Cloudの一部です。

MANDIANT
NOW PART OF Google Cloud