jamf

# 多層防御：

## ソリューションを多層的に統合して セキュリティギャップを解消

**デバイスやユーザ、データ、リソースを狙う高度な脅威から組織を守るには、サイバーセキュリティが必要不可欠です。**

これまで組織の対策は、ウイルス対策ツールやVPNクライアントなど、オフィス環境向けに設計された基本的な境界型セキュリティツールが一般的でした。しかし、企業ネットワークの枠を超えた働き方が主流となった今、従来のツールだけでは対応しきれなくなっています。現代のハイブリッドワーク環境では、プロアクティブな多層型対策により、デバイスとユーザがどこに存在しようと保護することが求められているのです。

本資料の主な内容：

- 進化し続ける脅威の現状
- あらゆるデバイスとオペレーティングシステムを保護することの重要性
- 最新の多層防御戦略を支える柱
- 統合型セキュリティが実現する、強固な防御とシンプルな管理

# 進化し続ける脅威の現状

今日、企業のITとセキュリティは大きな進歩を遂げています。モバイルテクノロジー、クラウドコンピューティング、モダンセキュリティフレームワークの発展のおかげで、事業運営の形そのものが変わり、従業員は時間も場所もデバイスも問わず働けるようになりました。しかし、このような進歩は企業だけにとどまりません。脅威アクターもまた進化し、新技術を悪用しこれまでと異なるデバイスを標的とするように戦術を変化させてきました。そのため、脅威は大幅に巧妙化しており、エンドユーザにとっては見抜きづらく、セキュリティ担当者にとっては対策の困難なものとなっています。

簡潔に言えば、今や脅威はあらゆる角度から攻めてきます。あらゆる種類のデバイスやオペレーティングシステム（OS）が標的となり、あらゆるネットワーク接続が侵入経路に使われています。

それは**なぜでしょう？かつてデータ/エンドポイントのセキュリティ対策として一応の成功を収めた境界型の「単一ソリューションによるセキュリティ戦略」では、このような脅威には対応できないからです。ネットワークの境界は、以下の要因により実質的に崩壊してしまいました。**

- クラウドベースのサービスやアプリへの移行
- リモートワーク/ハイブリッドワークへの移行
- 個人所有デバイスの業務利用
- 信頼できないネットワーク接続を用いた通信
- 共同作業用の共有ツールの利用

AIや機械学習といった技術がこの変化を一層加速させ、新たなリスクとチャンスを生み出しています。それに対応するには、進化する脅威に適応できるセキュリティ戦略が必要です。

ユーザの視点で見れば、上記の変化は新たな可能性を開きました。場所やインフラ、ソフトウェアを自由に選び、いつでも、どこからでも、好きなデバイスで任意のネットワークを介して働けるようになったのです。しかし、その一方で攻撃の標的となる対象も広がり、脅威アクターが悪用可能なベクトル（経路）も増加してしまいました。

以降のセクションでは、モバイルテクノロジーが発達し働く場所が分散する中で、脅威がどのように進化してきたのかを解説します。

## 持続的標的型攻撃、融合型脅威、攻撃の複雑化

現代の脅威はかつてないほど高度化し、適応性を増し、他の脅威との結びつきを強めています。悪意あるコードもいまだに攻撃手法として人気があり、アプリケーション内にラッパーとして仕込まれるか、侵害したウェブサイト経由で配布されています。結果はこれまでと同様で、デバイスを侵害し、攻撃者の指令を受けて操作を実行します。

過去の攻撃パターンに見られた単純さは、もうありません。今日の脅威は複雑化しており、複数の攻撃手法を組み合わせるか、間接的な侵入口（侵害したパートナーやサプライヤーなど）を使うことがほとんどです。このコンバージェンス（融合）により、攻撃の検出と防御は一層困難になりました。こうした巧妙な攻撃手法に関する過去数年の事例を以下に示します。

- わずか2年の間に発生した2件の攻撃によって、**1億人以上**の顧客の個人識別情報（PII）が侵害
- 2023年にサプライチェーン攻撃が3倍に増加し、既知の脆弱性が確認されているコンポーネント（修正バージョンが提供済み）のダウンロードが**21億件発生**
- カジノ・ホテル会社にソーシャルエンジニアリングキャンペーンを起点とするランサムウェア攻撃が仕掛けられ、業務の中断と顧客データの侵害の結果金銭的損害が発生
- ソーシャルメディアプラットフォームのAPIが侵害された結果、**540万ユーザ**のデータが漏洩し、さらに**4,000万ユーザ**の公開/非公開データがダークウェブ上で取引
- 国家によるスパイウェア「Pegasus」を使った攻撃により、重要人物の個人所有モバイルデバイスを不正に監視。深刻なプライバシー侵害が発生
- ある企業の最高財務責任者（CFO）の音声と画像がディープフェイクキャンペーンに悪用され、設計企業が2,500万ドルの詐欺被害に遭遇

## 融合型脅威

融合型脅威はサイバーフィジカル融合型とも呼ばれ、その由来はデジタル領域と物理領域がつながり合う性質にあります。これら2領域の見た目上の絡み合いが強まることでその境界線は曖昧になりつつあるため、片方の領域（サイバー）に対する脅威が、もう片方の領域（物理）にもきわめて現実的な影響を及ぼすようになっています。サイバー脅威の攻撃範囲の拡大により、物理的なシステム、プロセス、リソースの破壊だけでなくその波及効果も悪化しており、以下の攻撃による影響が増大しています。

- 持続性の確保
- 権限昇格
- ネットワーク内での横展開
- マルウェア展開
- データ流出

前述の脅威は、あらゆる業界の組織にとって現実のものとなっています。事業の継続という点でテクノロジーへの依存性が非常に強まっているため、1つのサイバー攻撃を受けるだけで業務が実質的に停止しかねません。例えば、メールへのアクセスが妨害されれば、アクセスが回復するまで業務を行えなくなります。そして対応が遅れてしまうと、業務への影響が製造ロスや収益の喪失などの重大な問題へと発展し、最終的には事業の閉鎖に追い込まれてしまいかねません。

このような事態は、既に実際に発生しています。有名な事例として、2021年にランサムウェア攻撃が発生し、攻撃から5日後に米国最大の石油製品用パイプラインが事業停止に至りました。被害が主要インフラに及んだため、運営企業は暗号化されたシステムとデータへのアクセスを取り返すために500万ドルの身代金を支払ったと報じられています。このインシデントを受け、様々な発展が見られました。米国司法省はランサムウェアネットワークを解体し首謀者を追求するため、取り組みの積極性を高めました。

それでも、脅威アクターの戦術は巧妙化しており、「攻撃の90%以上でもはや被害者のデバイスを暗号化するのではなく、ただデータを流出させ、あらゆる人を脅迫する」ようになっています。

## ソーシャルエンジニアリング

現代の脅威環境において、ソーシャルエンジニアリングを利用した脅威は際限なく増加しているように思われます。かつては、一般的なソーシャルエンジニアリングの問題といえば、企業の従業員になりすまそうとする攻撃者が時折出てくるか、あなたの銀行口座に自分の何百万ドルもの資産を預けたいと必死に申し出てくる、あの“心優しいが心配性の王子”からのメール程度のものでした。

しかし、時代は変わりました。

ソーシャルエンジニアリングは今や、階層的なフローチャートのように複雑化しており、その攻撃手法の種類はあまりに多く、すべてを列挙するのは不可能なほどです。その増大の様子は、新しいテクノロジーが公開されるたびに新しい手法が生まれているかのようです。おそらく、「すべてを統べる一つの指輪」がフィッシングで、他の手法はすべてそこから派生したものなのでしょう。

QRコードフィッシング（別名「クイッシング」）のように、新しい後継手法は出るたびに新たなセキュリティ用語を生み出していますが、現在のソーシャルエンジニアリングの進化は2つの次元で起きています。つまり、表に出てくる手法と、水面下に潜んでいる手法があるのです。前者の手法は検出が簡単です。企業の働き方に合わせてフィッシング攻撃を変化させたもので、以下の5件のなりすまし手法がよく見られます。

1. メールフィッシング
2. スピアフィッシング
3. ホエーリング
4. スミッシング/ビッシング
5. アングラーフィッシング

しかし、後者は本質的に、名前を付けられるようなものではありません。そのため、この種の新しい脅威はより一層危険であり、エンドユーザやIT部門・セキュリティ部門での検出が困難になっています。

最近、Jamf Threat Labsによってこうした脅威の例が2件発見されており、その概念実証型（PoC）の性質は現在、そして未来のモバイルセキュリティに衝撃をもたらしました。

### 偽の機内モード

ポストエクスプロイト永続化手法の一種で、機内モードのUIを偽装しながら悪意のあるアクティビティを陰で実行します。デバイスへの攻撃後、インターフェイス制御用のシステムファイルを改変し、攻撃者のアプリケーションだけはインターネットアクセスが有効な状態であるのにデバイスがオフライン状態のように見せかけるのです。このようなエクスプロイトは主に、ソーシャルエンジニアリングか不正なコンテンツによりユーザに悪意あるソフトウェアをインストールさせる形で配布されます。これにより、攻撃者は被害者にデバイスをオフライン状態にしたと思い込ませたまま、そのデバイスへのアクセスを確保（永続化）できます。

### 偽のロックダウンモード

前ページでは、国家がスパイウェア「Pegasus」を利用し重要人物の追跡を行った事例を紹介しました。国家主導／支援型の脅威については次セクションで詳しく解説しますが、こうした攻撃対象領域（アタックサーフェス）を減らすうえで重要な対策のひとつが、Appleの「ロックダウンモード」です。

たとえば、あなたのモバイルデバイスが侵害されたと感じたとき、さらなる被害を防ぐためにロックダウンモードを有効にするという判断は自然な対応でしょう。しかし、その“最後の防衛線”ともいえるモードを脅威アクターが巧みにすり抜け、デバイスが依然として脆弱なまま だとしたら…

これはソーシャルエンジニアリング攻撃の一種であり、ユーザにセキュリティは万全であると信じ込ませながら、モバイルデバイスへのアクセスを確保しコントロールします。

## 国家支援型攻撃／標的型攻撃

今日の世界は非常に多くのものがインターネットにつながっており、日常生活のほぼあらゆる場面にテクノロジーがかかわっています。身の回りにあるデバイスやネットワークを介して絶えずデータが収集、送信、保存されているので、どれほど注意深い人でもプライバシーのリスクは避けられません。

このような常時インターネットにつながる環境は、攻撃者に直接的に、あるいは付近の人物を標的とする形で脆弱性を悪用するチャンスをもたらしています。

国家主導/支援攻撃、または持続的標的型攻撃（APT）を行うグループがもたらす脅威は、特定の業界にとどまりません。現代の脅威事情を分析すると、APT攻撃がその対象範囲を従来の重要インフラから広げ、国家主体の利益につながるあらゆる人物、組織、地域を狙うようになっています。

**数字で見る国家主導/支援攻撃のデータ：**

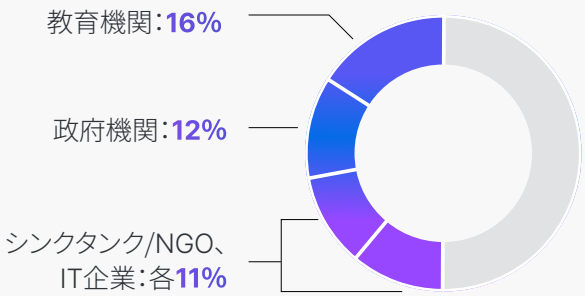
セキュリティアラートの**90%**は重要インフラ以外の分野から発生

**10社中9社**が、国家関連の脅威アクターから攻撃を受けた可能性があると回答

組織の平均被害額は**インシデント1件あたり160万ドル**

**5件のAPT攻撃**（現時点）でAIによる脅威の強化を確認

**世界的に狙われている分野トップ3：**




ほとんどの脅威アクターの動機の上位には金銭的利益があると考えて間違いないと思われますが、国家主導/国家関連の脅威アクターの主目的は盗んだデータにあります。だからといって、スパイ活動やネットワーク接続システム/サービスの破壊の優先順位が低いというわけではありません。現在の脅威事情の分析によれば、情報を収集し他の攻撃や社会的・政治的活動の妨害を行うための手段として機密データの流出が狙われるようになっています。

後者の場合はスパイ活動、特に重要人物狙いのモバイルマルウェアの増加と合わせて、モバイルデバイスに内蔵された無数のセンサーでユーザが不正に監視されるプライバシー上の問題も生じています。問題はこれにとどまらず、国家は収集したデータを基にジャーナリストや政治家、経営幹部などを標的としたさらなる攻撃を仕掛け、気づかれることなく無断でデバイスを侵害しています。この種のスパイウェアはステルス機能のようなものを備え、攻撃被害者のモバイルデバイスにリモートで展開されあらゆる種類のデータを流出させます。その多くはゼロクリックインストールやゼロデイエクスプロイトを利用し、標的のデバイスに感染します。

## 単一ソリューションでは対応が困難

第1セクションで解説したサイバー脅威の発展性に加え、前述の事項も現在の状況を招いた要因です。以下を守るように設計された従来のソリューションや手順、ワークフローは分岐点に立たされています。

- 企業所有のデスクトップコンピュータ
- サポート対象OSを実行するコンピュータ

**これはIT部門によって制限されており、以下のような対策が講じられています:**

- 使用できるソフトウェアを限定
- 業務目的から外れた操作の制限
- 「社内ネットワーク境界」という相対的に安全な環境内での運用
- ネットワークトラフィックはすべて社内ファイアウォールを経由
- マルウェア対策ソリューションによるデータ保護
- VPNによるリモートアクセスの安全なトンネリング

従来型の固定されたエンドポイントを保護するために開発されたレガシーなセキュリティソリューションでは、現在の脅威環境において十分なセキュリティ体制を確保することはできません。ましてや、変化の激しい働き方が常態化し、多様な要素を含む現代の企業環境においてはなおさらです。

最新のセキュリティ戦略には、強固さと柔軟性を両立できるメリットがあります。モバイルデバイスや特定のOS、私用デバイスの使用を禁止するという管理ポリシーを単に適用するだけでは、それらのハードウェアやソフトウェアに関連するリスクを十分に軽減することはできません。それどころか、こうしたポリシーは、ユーザが「制限対象エンドポイント」から企業リソースにアクセスする行為を止めることすらできません。こうしたユーザが社内ネットワークにリスクを招く可能性はきわめて現実的なもので、さらに悪いことに、管理者はインシデントが発生するまで状況を認識できません。

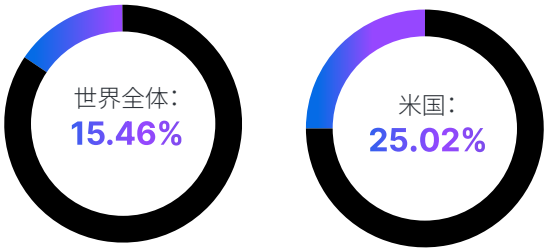
### では、最良の方針は?

IT部門とセキュリティ部門で最善のエンドポイント/セキュリティ管理を実現する鍵は、用途ごとに最適なソリューションを導入することです。こうした管理ソリューションとセキュリティソリューションは、対象のデバイスタイプとOSをネイティブにサポートするよう設計されています。そのため、ハードウェアとソフトウェアについて最高レベルの互換性を確保するだけでなく、IT部門とセキュリティ部門で社内インフラのエンドポイントを最適に管理・保護するためのツールも揃えられます。

#### 企業のmacOS導入状況

ここで、貴社の環境について考えてみてください。多くの企業ではWindowsベースの業務用デバイスを管理・運用されていると思いますが、macOSのデスクトップやノートパソコンについてはどのようにお考えでしょうか。CIO 300名を対象とした最近の調査では、米国のCIOの96%が、今後12ヶ月から24ヶ月の間に社内のMacデバイスが増大する見込みと回答しています。

詳細に触れる前に、2024年2月時点におけるmacOSの市場シェアを見てみましょう。




米国だけでも、macOSは市場の4分の1を占めており、半数以上のmacOSが企業で利用されています。つまり、macOSデバイスが企業内で利用されるのはもはや時間の問題であり、「そのときにどう守るか?」が今、問うべきテーマです。なぜなら、エンドユーザが業務の遂行にmacOSを多かれ少なかれ利用している可能性が高いと考えられるからです。それが、会社から正式に支給された業務用デバイスであっても、従業員選択制やBYOD (Bring Your Own Device) / COPE (Company Owned Personally Enabled) の取り組みの一環であっても、あるいは会社の承認を得ていない個人用デバイスであっても…

Macの導入は加速しているだけでなく、業務への活用にも影響を及ぼしています。どのハードウェアやソフトウェアにも言えることですが、IT部門やセキュリティ部門がWindowsベースのデバイスへの対応と同様に、Mac特有のニーズに合わせて設計された管理・セキュリティツールを用いて対処しなければ、将来的に企業のセキュリティに重大な被害が生じるでしょう。

## 見過ごされがちなリスク：モバイルデバイス

平均的なユーザが使用するコンピュータは1台だけですが、モバイルデバイスに関してはスマートフォンやタブレット、スマートウォッチなど、複数のタイプを利用する場合がほとんどです。実際、Statista社の調査によれば、世界全体におけるユーザ1人あたりのデバイスの平均台数は2023年に3.6台に達しています。

つまり、ユーザ1人あたりの攻撃経路が4倍になったということです。デスクトップOSベースのデバイスのセキュリティ対策が必要不可欠であることは、企業にとって言うまでもありません。しかし、モバイルデバイスの管理が不十分なままでは、従業員が生産性向上のために無防備なデバイスで社内ネットワークに接続し、業務データやリソースへアクセスすることが許容されてしまい、リスクを抱えることになります。。


### モバイルデバイス固有のリスクとは？

リスクの多くはデスクトップコンピュータのものと共通ですが、モバイルデバイス固有のファイルシステムを可視化する専用のエンドポイントセキュリティソフトウェアがなければ対応できません。

企業に影響しかねない一般的なモバイルデバイス固有のリスクとしては、以下のものが挙げられます。

- **不正アクセス：**ソーシャルエンジニアリングキャンペーンによりSMSおよびソーシャルメディア経由で被害者の認証情報が収集されると、脅威アクターに業務サービスへ不正にアクセスされてしまいます。
- **マルウェアの持ち込み：**非公式のアプリストアからダウンロード（サイドローディング）したアプリを起動すると悪意あるコードが実行され、業務データや個人データが損なわれます。
- **コンプライアンス違反：**ポリシーベースの適用を行わないと、デバイスがコンプライアンスに違反した際に組織に責任が生じます。規制の厳しい業界では被害が増大します。
- **データの流出：**業務データ、個人データ、プライバシーデータが盗まれると、機密データが脅威アクターの手に落ちてしまいます。
- **水平展開：**ネットワーク経由の攻撃は、侵害した認証情報を基にインフラ全体へ攻撃を拡大し、より多くのデータを漏洩させます。
- **対策の迂回：**セキュリティ設定やアプリ設定にミスがあると、脅威の攻撃対象の候補が増加し、デバイス上で無防備なままペイロードを実行されやすくなります。
- **権限昇格：**バージョンの古いソフトウェアに脆弱性があると、脅威アクターがそれを悪用してデバイス、さらには社内ネットワークへ侵入するおそれがあります。

## リソースを保護するだけでは不十分

セキュリティギャップの解消という観点でセキュリティ担当者が様々なリスク対策を考える場合、次のように思考を巡らせるものです。ソフトウェアやOSを最新状態に保ち、既知の脅威から保護する対策としては、パッチ管理プロセスの改善が一般的です。また、人工知能（AI）や機械学習（ML）ツールをセキュリティスタックに組み込んで、検出精度を高め、対応を早めるとともに、自動化に対応することも考えられます。しかし、AIおよびMLは最新のセキュリティ業務では標準的な存在になりつつあるものの、ほとんどの企業では状況に応じて判断を導き、これらテクノロジーの責任ある利用を徹底するため、人ありきの対応を継続しています。

こうした取り組みは、セキュリティギャップの解消という点でたしかに優れています。しかし一方で、デバイスやユーザ、データの保護を強化する対策の導入という枠を超えた、他の要素も存在します。こうした要素は基礎的なので、技術的/論理的対策の導入ほど派手で「楽しい」ものではないかもしれませんが、セキュリティ戦略の構成手順やプロセス、ツール、業務フローを効率化、自動化、整理統合して組織の価値を高めます。さらにこうした要素は、デバイス、ユーザ、データのコンプライアンス確保と生産性維持に責任を負うIT部門とセキュリティ部門を支えます。

このセクションでは、これらの要素について詳しく掘り下げ、「4つのC」と名付けて解説します。相互にどう連携し、組織全体のセキュリティ課題の解決にどのように貢献するのか、その相乗効果と実践的な価値に焦点を当ててご紹介します。

### 一貫性（Consistency）

企業が社内のセキュリティについて考える場合、仕事に使用され社内リソースに接続するあらゆるタイプのデバイスを（それらで実行される各種のOSも含めて）同様に扱わなければなりません。結局のところ、Windowsコンピュータを従業員に支給する企業が、その管理と保護用にエンドポイントセキュリティを導入したとしても、従業員の使用する未許可のモバイルデバイスから社内データを保護するモバイル脅威対策を導入していなければ、モバイルデバイス狙いのリスクに対しては無防備も同然であり、データ侵害を招きかねないからです。

Apple製デバイス（macOS、iOS、iPadOS）はセキュリティを念頭に設計され、かつAppleもセキュリティとプライバシーの強化を進めていますが、これらデバイスもWindowsやAndroidと同じく脅威アクターから定期的に攻撃を受けています。「一貫性」に伴う問題のポイントは、各OSどうしの相違点だけではなく、むしろ共通点にあります。デスクトップやノートパソコン、タブレット、スマートフォンはサイズこそ異なりますが、見た目上の違いの数よりも動作の核となる要素の共通点の方が多いコンピューティングツールの実例です。

これこそ、一貫性の問題です。以下の違いにとらわれることなく、社内リソースにアクセスするすべてのデバイスを同様に扱う必要があるのです。

- デバイスの種類
- サイズ・形状
- オペレーティングシステム
- アプリとサービス

## コンプライアンス

コンプライアンス（Compliance）

「コンプライアンス」の意味合いは、企業の属する業界によって異なります。規制の厳しい業界では、保護対象のデータタイプの漏洩を防止するため、データ、プロセス、ワークフローに講じるべきセキュリティ対策が法律で定められています。そうでない業界でも、企業によっては守るべきコンプライアンスレベルを定めているところもあります。その目的は、社内のビジネスポリシーに準拠するためか、事業運営上遵守すべき基準やフレームワークに適合するためか、あるいはその両方でしょう。

セキュリティギャップの解消という点では、コンプライアンスは次の2つの重要事項に対処することを意味します。

### ベースラインの活用

1番目の重要事項はベースライン、より具体的に言えば、社内インフラの正常な運用レベルの区分けを目的としたベースラインの策定です。設計上、ベースラインは管理者にとっての責任分界点にもなります。エンドポイントがベースラインに定める許容範囲から外れた際の警報となり、コンプライアンス違反の可能性を把握できるからです。

### 監査人への証拠の提出

内部監査人を任命しているにせよ、規制遵守の一環として独立した第三者による監査が義務付けられているにせよ、コンプライアンスの維持状況を示すには常になんらかの証拠が必要です。エンドポイントコンプライアンスの証明においては、監査人の経験則である「記録にないことは行われていないとみなす」が適用されます。

ベースラインの管理と監査用の証拠の収集では、テレメトリデータが鍵を握ります。このデータがあれば、管理者はエンドポイントの健全性を把握できます。さらに、社内データへのアクセス、処理、保存、変更、拡散、共有に使用されたデバイスが社内のセキュリティ計画や規制管理で定められたガイドラインまたは要件に準拠しているかをいつでも確認できるようになります。

## 統合（Consolidation）

3つ目の「C」こと「統合」は、ソリューションに関するものと間違われやすく、最も誤解されがちな「C」と言えます。

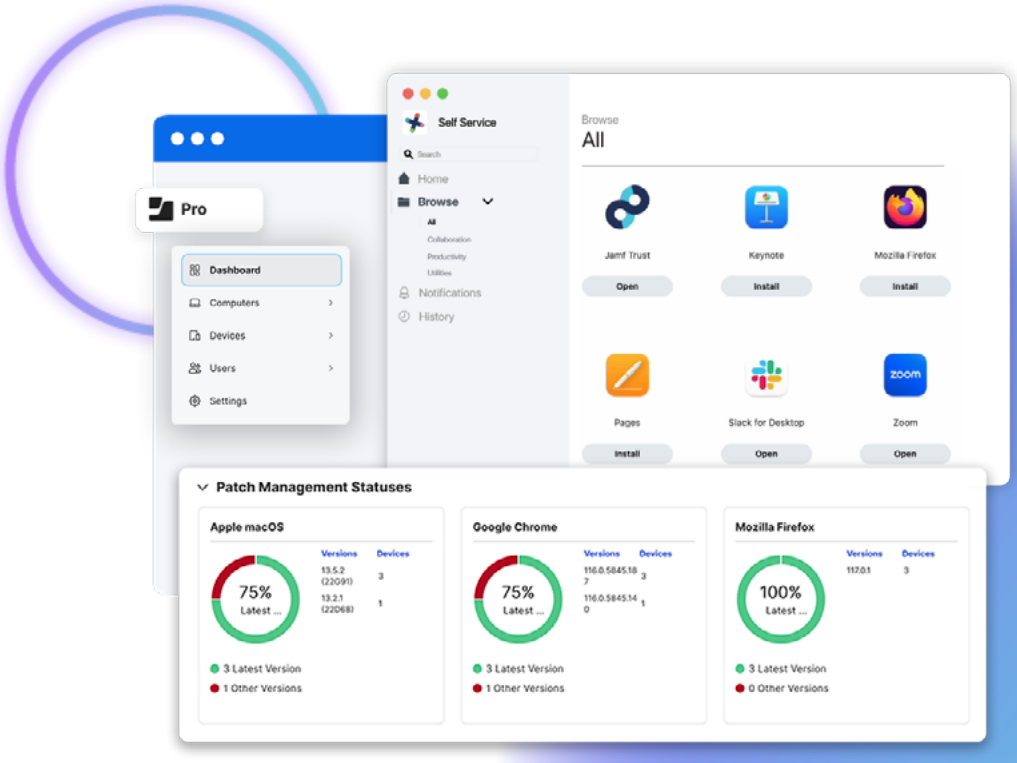
ここでの「統合」とは、IT担当者とセキュリティ担当者を1つのチームとして結束させることです。つまり、業務の性質がまったく異なる両部門を変革するのです。これらの部門は「情報テクノロジー」という言葉で括られているものの、ビジネス上の様々な理由から独立した業務体制を敷いていることがほとんどです。

現代の脅威状況を考えると、こうした業務方式の問題は、部門ごとに管理するソフトウェア、ベンダーパートナーシップ、プロセス、ポリシー、業務フローが異なることにあります。理論的に言えば、両部門の体制が分けられている理由は、デバイスおよび組織全体のセキュリティ状態を強化することです。しかし、ほとんどの場合、こうした構造は逆効果です。

効果的に統合を進めるには、以下の目的に合わせ、サイバーセキュリティのアーキテクチャとプロセスをモダナイズおよび統合することが求められます。

- 用途ごとのソリューションを一元化し、サポート対象プラットフォームをネイティブに管理する
- ベンダーやパートナーシップの数を減らす
- サイロ化を解消し、情報共有を強める
- ナレッジマネジメントの手順を確立して属人化を解消する
- 管理とセキュリティのアプローチを統合する
- 脅威防御を統合してインシデント対応を迅速化する
- 保護の範囲をインフラ全体に拡張する

企業の管理者は社内の機密データにアクセス・活用するデバイスやユーザを包括的なセキュリティ対策で保護する職務を負っていますが、セキュリティと管理の統合を進めることで、その対象を社内リソース全般に広げています。



## コスト削減（Cost savings）

IT部門とセキュリティ部門の統合と並行して、ROI（投資利益率）の重要性も考慮する必要があります。ROIで特に大きな手柄となるのは、組織固有のコンプライアンスニーズに一貫して対処するうえで「最適な」ソリューションを選択できた際に得られるコスト削減効果です。そのためには、ソリューションのコストに対する価値を把握するだけでなく、多層防御戦略関連のROIへ直接的に（および間接的に）影響するほかの要素のバランスを取ることも必要です。

ROIだけでなく包括的なセキュリティ戦略にも影響する直接的および間接的な要素としては、例えば以下のものがあります。

- 組織の様々なデバイスとOSをネイティブにサポートするだけでなく、1つに統合して総合的なソリューションを構成可能なツールを選択する
- 時間のかかる手作業に自動化を組み込んで効率を高め、管理者が価値を生むプロジェクトに専念する時間を確保する
- セキュリティ関連のプロセスや業務を効率化し、対象範囲をインフラ全体に拡大し最適化して多数のエンドポイントとアプリケーションを一括でサポートする
- ソリューションとインシデント対応間の複雑度を低減し、セキュリティインシデントの発見から修復までにかかる時間を最小化する（＝ダウンタイムを減らして生産性を高める）
- アクティブな監視・報告により管理者にリアルタイムで詳細なテレメトリデータを提供し、コンプライアンス面で被害を受ける前にリスクベクトルを検出/是正してコンプライアンス面で被害を受ける前にリスクベクトルを検出/是正する

コスト削減や現代の複雑化する脅威環境を考慮するうえで、従業員が自身の所有デバイスを業務に使用するという選択肢（BYOD）も、重要な要素となっています。今日では多数の組織がBYOD制を取り入れており、この傾向は従業員間のつながりとコラボレーション促進のためにリモート/ハイブリッド環境を導入している企業で特に顕著です。さらに、BYODが雇用主にもメリットをもたらすことは間違いないため、Zippia社によれば米国のIT部門の意思決定者のうち**70%**がBYOD制度を承認しています。

社内ネットワークに接続するモバイルデバイスの**96%**は従業員個人の所有物

上級管理職の**80%**はモバイルデバイスが従業員の業務に必須であると考えている

ウェアラブルデバイスを活用する従業員は**30%**増加する見込み

また、従業員選択制も組織に有益です。この制度では、生産性を最も高められるハードウェアやソフトウェアを従業員が購入費の負担なく選べるようにして、コンピュータだけでなく数百、数千、あるいは数万台のモバイルデバイスのインベントリを管理します。これには相当なメリットがあり、コスト削減効果もあります。

# 多層防御：複数層にわたる効果的なセキュリティ

米国立標準技術研究所（NIST）によれば、多層防御（DiD）とは「情報セキュリティ戦略の一種で、人、テクノロジー、業務機能を統合し組織の複数の層とミッションにわたって可変的な防御壁を築く」ものとされています。

この戦略をサイバーセキュリティ計画に組み込むと、セキュリティ対策を増やし、組織のセキュリティ状態を強化できます。しかし、この多層的な対策がもたらすものは、言うなれば「セーフティーネット」です。緊急時の対策を実装し、社内リソースを脅威から守るわけです。脅威がある層のセキュリティ対策をすり抜けても、攻撃経路上に次の対策があるので、脅威がコンプライアンスに影響するインシデントへと発展する前に補足して軽減できるのです。

**本セクションでは、次のような疑問を検討します。**

- 統合は全体として企業のサイバーセキュリティ計画にどのような影響をもたらすのか？
- DiDの実現に役立つ包括的なセキュリティ対策にはどのようなものがあるのか？
- サイバーセキュリティ計画にDiDを組み込むとコンプライアンス要件の遵守にどのようなメリットがあるのか？

## 管理 + ID + セキュリティ

本書の読者の多くは、管理やID、セキュリティといったデバイス管理の概念をご存知でしょう。これらの概念はそれ自体だけで基本要素とみなされており、注目すべきことに、以下の各カテゴリに関連するテクノロジーやベストプラクティス一式を生み出しています。

- **デバイス管理：**コンピュータやモバイルデバイスを管理することを指し、設定の管理、セキュリティ構成の導入、ソフトウェアのインストール、ポリシーの適用などを行います。
- **ID・アクセス管理：**複数のポリシーとテクノロジーから成るフレームワークで、保護対象リソースへのアクセスを、ユーザ認証とデバイス認可により権限を割り当てて管理します。
- **エンドポイントセキュリティ：**ソフトウェア中心のテクノロジーで、保護対象のリソースを守りながら、リスクを最小限に抑えデバイスとユーザを脅威や攻撃から保護します。

これら3つの基本要素を統合することで強固な多層型のサイバーセキュリティ計画を構築して、不正アクセスから社内リソースを守り、エンドポイントのリスクベクトルを最小限に抑え、ユーザのセキュリティと生産性を確保できます。

以下のセクションでは、この統合で実現できるテクノロジーについて解説するとともに、それらのテクノロジーがリスクの軽減、マルウェアの阻止、高度な脅威の検出と軽減にどのように役立つかをあわせて紹介します。

- ゼロタッチ導入
- 脅威ハンティング
- ゼロトラストネットワークアクセス（ZTNA）
- 高度な脅威対策

## ゼロタッチ導入：利用開始時からセキュリティを確保

多くの場合、セキュリティは受動的なものです。例えば「インシデント対応」という言葉には、脅威への対処にあたってまずその検出を待つという受動的な性質が表れています。これは、原因と結果のようなものです。

このような「因果関係」的性質を変えるために管理者ができることはほとんどありません。しかし、攻撃の対象領域を縮小させ、脅威がデバイスを襲う「方法」と「場所」をできる限り減らす方法はあります。

この対策を講じるタイミングとしては、デバイスの電源が初めてオンになった時が最も効果的です。これが、プロビジョニングとゼロタッチ導入の力です。特に、Appleデバイスの管理であれば簡単にゼロタッチ導入のメリットを活かせます。

なぜなら、企業用のゼロタッチ導入ソリューションでは、初期設定画面中に管理ワークフローとID・アクセス管理ワークフローをデバイスへプロアクティブに配信するからです。具体的には、ユーザが自社の認証情報を使用して認証を完了し、デバイスをモバイルデバイス管理（MDM）に登録して、管理プロファイルをインストールすると、これらワークフローが配信されます。その後、MDMが直ちにユーザの業務に必要なリソースすべてを展開し、組織の基準に沿ってデバイスを構成します。

このゼロタッチ導入のプロビジョニング段階で実施できる対策には、以下のものがあります。

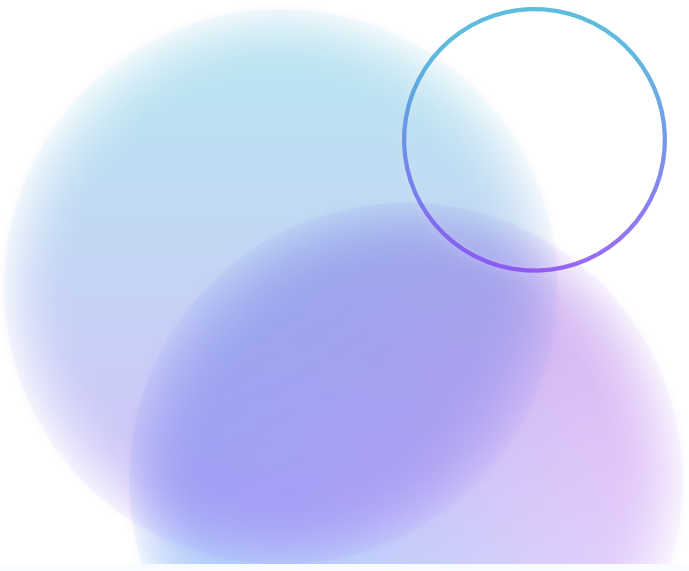
- デバイスセキュリティの強化
- 管理対象Appのインストール
- アプリケーション設定の構成
- ユーザアカウントの割り当て
- セルフサービスオプションの選別
- システムパッチのアップデート
- セキュリティソフトウェアの導入
- 実施ポリシーの設定

このように聞くと、会社所有のデバイスには適しているが、個人所有デバイスには向いていなさそうだと考える方もいるでしょう。

ゼロタッチワークフローは、個人所有デバイスを含むあらゆるオーナーシップモデルに対応しています。こうした状況のために、Appleでは、ユーザプライバシーと企業のセキュリティ対策を両立するユーザ登録機能を開発しています。

ユーザによる企業用MDMソリューションへの個人用デバイスの登録には、以下の特長があります。

- 社内リソースへのアクセスを保護する（メール、連絡先、予定表、Wi-Fi、暗号化ネットワーク接続など）
- 個人データは手つかずのままで、業務データだけがデバイス上の暗号化された個別ボリュームに保存される
- 2つのApple IDを併用できる（個人データと設定には個人用ID、業務データには管理対象IDを使用）
- 管理者が個人所有デバイスで閲覧、アクセス、削除できるのは業務データのみであり、個人データとプライバシーデータはアクセス・操作できない
- 企業全体のセキュリティ対策を標準化し、オーナーシップモデルを問わずすべてのデバイスに均一の保護を提供できる



## 脅威ハンティング：プロアクティブ（予防的）> リアクティブ（事後対応的）

管理担当者は様々な専門業務の中でも、特にインシデント対応を任されています。これは、管理者がエンドポイントセキュリティソフトウェアから悪意ある挙動や脅威に関する警告を受け取った場合に、潜在的な問題を検出しトリアージする作業です。問題を確認し、封じ込め、最終的に修復する作業は対応担当チームに任されます。

対応担当者にとって、既知の問題への対処は珍しいものではありませんが、管理ソリューションとセキュリティソリューションを統合してワークフローやプロセスを強化すると、このほぼ受動的なプロセスを能動的なものに変える要素を付加できます。

### セキュアなベースラインの確立

サイバーセキュリティの分野では、ベースラインとは企業のエンドポイントが正常に動作する状態を指します。ベースラインを確立するには、パフォーマンスを測定するだけでは足りません。ベースラインには安全な構成や設定、エンドポイントセキュリティソフトウェア、アプリ、サービスなど、ユーザが職務を安全に遂行するうえで必要なすべてのものが含まれるからです。これは、コンプライアンス要件の遵守や企業ポリシーとの合致も意味します。

### 既知の脅威の阻止

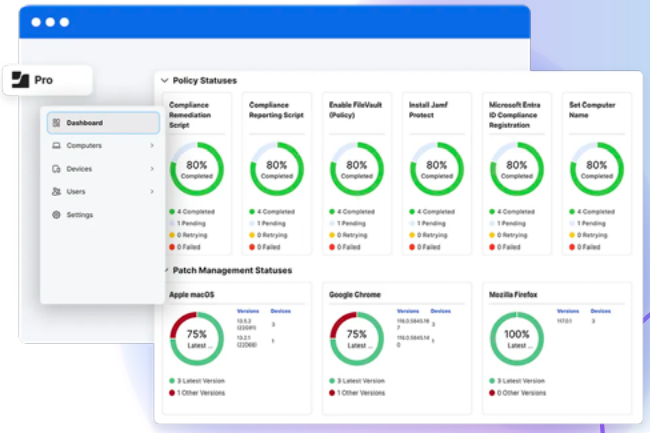
必須のパラメータをベースラインとして定めて収集すると、管理者がエンドポイントの健全性が許容範囲にあるかを判断しやすくなります。許容範囲から外れると、エンドポイントセキュリティソリューションから管理者に逸脱を知らせるアラートが送られ、手作業でリスクを軽減するチャンスが生じます。または、管理ソリューションとの統合を構成済みであれば、両ソリューション間でのテレメトリデータの共有をトリガーとして、インシデントを修復するための自動ワークフローが実行されます。

### 未知の脅威の検出

テクノロジーにおいては、「プロアクティブ（予防的）」か「リアクティブ（事後対応的）」かという視点が常に重要なテーマであり、脅威が複雑化・高度化する現在、エンドポイントの管理と保護を維持するうえで極めて重要です。プロアクティブな取り組みの代表例のひとつが「スレットハンティング（脅威ハンティング）」です。

### この作業を効果的に実施するために必要なもの：

- 環境に関するきわめて豊富なデータ
- 優れたデータ分析スキルとパターン認識スキル
- ハードウェアとソフトウェアに関する深い知識
- 高性能のセキュリティツールとその使用法
- 未知のものを調査できるだけの時間、忍耐力、勤勉さ



## ZTNA：絶対に信頼せず、必ず検証

かつては最先端とされていたテクノロジーであっても、時が経つにつれて旧式扱いとなり、時代遅れとされ、最終的には完全に廃止されて、他の高性能で速く強力なテクノロジーに置き換えられてしまうものです。VPNのような従来のテクノロジーは、現代の脅威環境がもたらす課題に対処するように設計されていません。ゼロトラストネットワークアクセスは、こうした課題に対処できるセキュリティモデルとして考案されました。

セキュリティ、ID、管理を統合するZTNA（ゼロトラストネットワークアクセス）が、サイバーセキュリティにおける新たな枠組みをどのように築いているのかをご紹介します。

### ネットワーク経由の脅威を阻止

技術者であれば、ファイアウォールを知らない人はいないでしょう。特に、その用途と機能は誰もがご存知のはずです。ファイアウォールはネットワークベースの攻撃に対して境界型のセキュリティを提供する強力な手段ですが、分散型ワークスタイルへの移行や、個人所有デバイスの業務利用が進む現在において、LANの境界を守るファイアウォールだけでは、リモート環境や管理されていないデバイスを使う従業員を保護するには十分とは言えません。ZTNAなら、脅威と攻撃に対してデバイス上およびネットワーク内にセキュリティを確立できます。さらに、その対象範囲は複数のプラットフォームに及ぶので、OSがmacOS、iOS、iPadOS、Windows、Androidのどれであってもコンピュータとモバイルデバイスに対して均一なセキュリティ対策を提供できます。

### 通信の分離と暗号化

またZTNAでは、あらゆるネットワーク接続上のトンネルを暗号化して保護します。この暗号化は常時有効であり、ユーザやマルウェアに無効化されても自動で再び有効化されます。さらに、ZTNAをIDベースのアクセス管理機能と統合して防御層を増設することも可能で、保護対象リソースへの接続が行われるたびに、対象のアプリまたはリソース専用のマイクロトンネルを生成できます。これは、公共のWi-Fiホットスポットを使う場合によくある中間者攻撃（MitM）を防ぐのはもちろん、マイクロトンネルどうしが分離されるのでネットワーク内の水平展開も阻止できます。さらには、最小権限の原則を適用し、ユーザの認証を必須にして、各自に割り当てられたリソースへのアクセスを明示的に付与できます。一度認証すればネットワーク全体へのアクセスが付与されるVPNとは異なり、ネットワークインフラの他のすべての要素はデフォルトでアクセスが拒否されます。

### エンドポイント健全性とアクセス要求の検証

ゼロトラストモデルでは、デバイスを暗黙的に「信頼」するのではなく、要求が行われるたびにエンドポイントと認証情報を必ず検証します。この検証では、検証時点のエンドポイントの健全性を組織で定めた許容状態と比較します。この2つのチェックポイントに合格すると、要求対象のリソースへのアクセスが付与されます。認証とデバイス健全性のどちらかに誤りがある場合、アクセスは拒否され（デフォルトの挙動）、逸脱を是正する修復ワークフローが実施されます。修復の実施後、両方のチェックポイントが再び実行されます。つまりZTNAでは、デバイスと認証情報の両方が検証に合格するまで、要求対象リソースへのアクセスが許可されることはないのです。

**モバイルデバイスが次のいずれであっても関係ありません。**

- 会社支給か個人所有か
- 接続先が社内ネットワークか公共Wi-Fiホットスポットか
- デバイスチェックポイントに合格したが認証情報チェックポイントに失敗した

**また、ユーザアカウントが次のいずれであるかも考慮されません。**

- 特定の職務に属するものである（幹部や管理職など）
- 認証に合格したのが1時間前であるか5分前であるか
- 認証情報チェックポイントに合格したがデバイスチェックポイントに失敗した

このように「絶対に信頼せず、必ず検証」の言葉どおり、デフォルトでアクセスを無効化します。要求が行われるたびに、デバイスと認証情報の検証が行われます。

## 高度な脅威対応：経営幹部向けの保護機能

今日では持続的標的型攻撃（APT）が急増し、世界中のあらゆる業界の組織が狙われています。

本セクションでは、セキュリティソリューションと管理ソリューションを統合する際に、管理者が導入可能な防御策について解説します。両ツールを統合し包括性を高め、各ツールで脅威インテリジェンスデータを収集し共有し合うことで、重要人物を狙う傾向が高まっている高度な脅威や重要人物（CEOなど）を狙う役職標的型サイバー攻撃を受けた場合でも、強固な脅威対応と修正を行えます。

高度な脅威によるリスクの対策として、セキュリティソリューションと管理ソリューションを統合する主なメリットは以下のとおりです。

**モバイルデバイス狙いの攻撃を可視化**

現在、モバイルデバイスを狙う攻撃が増加しています。現在の脅威環境はますます進化を続けており、その矛先は年々モバイルデバイスとその利用者に向けられています。

これは私たちだけの主張ではありません。裏付けとなる注目すべきデータをご紹介します。

- 侵害を受けたデバイスのうち（ジェイルブレイクやルート化にとどまらず）完全に悪用された割合は**43%**（前年比**187%**増加）
- フィッシングサイトの**80%**は、モバイルデバイスのみを標的としているか、デスクトップとモバイルデバイスの両方に対応
- 2022年に発見された重大な脆弱性のうちAndroidに関するものは**138%**増加。一方で、実際に悪用されたゼロデイ脆弱性のうち**80%**はApple iOSに関連していた
- モバイルアプリ上のクラウドストレージの設定ミスが攻撃対象として突出しており、iOSモバイルアプリの**±2%**、Androidモバイルアプリの**±10%**が危険なクラウドインスタンスにアクセスしていた
- モバイルマルウェアのユニークなサンプル数は前年比で**51%**増加し、サンプルの検出数は**920,000件**以上に増加

モバイルデバイス狙いの攻撃を把握する鍵は、アクティブな監視と可視化にあります。これらの対策は、こうした攻撃の特定だけでなく、社内リソースにアクセスするエンドポイントの健全性を把握し、脅威アクターに悪用される前にリスク要因を最小化することにもつながります。

これらタスクの完了後、エンドポイントセキュリティソリューションが脅威対策の結果を確認するためにデバイスを再スキャンします。対策が成功した場合、社内リソースへのアクセスが許可されます。失敗した場合、要求は拒否状態のままになり、場合によっては追加の修正措置が求められます。

**持続的標的型攻撃を阻止**

脅威の状況を正しく理解するには、脅威を未然に防ぐことが、対応するよりもはるかに重要であるという前提を持つことが必要です。とはいえ、現実には一部の脅威がデバイスに影響を及ぼし、ネットワークにも被害を与える可能性があることも、見落としてはなりません。持続的標的型攻撃（APT）を支える巧妙さを考えると、エンドポイントの侵害は「起きるかどうか」ではなく、「起きたらどうするか」を考えるべきものです。迅速に対応できるかどうかは、チームの準備状況にかかっています。そのため、APT対策の準備度合いが、APTの修復に使用するツールの機能とデータの品質に左右されることは間違いありません。

ここで重要になるのが、セキュリティと管理の連携です。この2つを組み合わせることで、次のような高度な手順やワークフローが実現します：

- 不審な挙動を検出する
- 管理者にインシデントを警告する
- 脅威のセキュリティ侵害インジケータ（IoC）または攻撃インジケータ（IoA）を評価する
- 複数の脅威インテリジェンスソースの所見を分析する
- 脅威が真陽性であるか検証する
- 軽減戦略を展開する
- 必要に応じて、修復作業を実行する
- デバイスをスキャンしコンプライアンス状態を検証する

脅威の重要度によっては、セキュリティソリューションと管理ソリューションの統合は、社内担当者による手作業でのインシデント対応プロセスを強化する効果も発揮します。これは、同プロセスを統合ソリューションプロバイダーが自動で実施する場合も同様です。

**数週間かかっていた調査を数分に短縮**

同じ脅威は一つとしてなく、直近の脅威や概念実証型（PoC）攻撃では巧妙さが一段と高まっていることから、対応部門や脅威ハンターが未知の脅威の影響を完全に把握するには、従来以上に深く徹底的に調査を行わなければなりません。これまで、脅威の重大性やその複雑さにもよりますが、調査の期間は数週間に及ぶこともありました。

脅威が高度化する今、モバイルデバイス上のインシデントや攻撃を効率的に検出し対応するには、ツールも高度なものにする必要があります。こうしたエンドポイントは「持ち運ばれる」ので、モバイルデバイス狙いの攻撃を検出、対応するにはインシデント対応をリモートで実施できなければなりません。これを実現する手段がデスクトップとモバイルデバイスのセキュリティの融合であり、以下の作業が可能になります。

- 詳細な分析でIoCを特定する
- 不審なイベントの時系列を分析し、デバイス侵害がいつどのように起きたかを明らかにする
- インシデントの概要をわかりやすく提示し、本来なら見逃されていた高度なゼロデイ攻撃を表面化
- APT（持続的標的型攻撃）には標準機能を使って対応し、脅威の監視と対処を継続的に実施

## まとめ

企業・組織のセキュリティ上の脆弱性を効果的に解消するためには、最新のサイバーセキュリティアプローチが必要です。具体的には、包括的なセキュリティ対策を重層的に展開し、インフラ全体を通じてデバイス、ユーザ、データの保護とプライバシーを実現することが求められます。そのためには、管理、ID、セキュリティを統合した、単一の強力な多層防御ソリューションが最適です。