jamf

新興テクノロジー活用戦略ガイド：現代の企業における管理・セキュリティ・スケーラビリティ

新興モバイルテクノロジーの発展と企業への影響

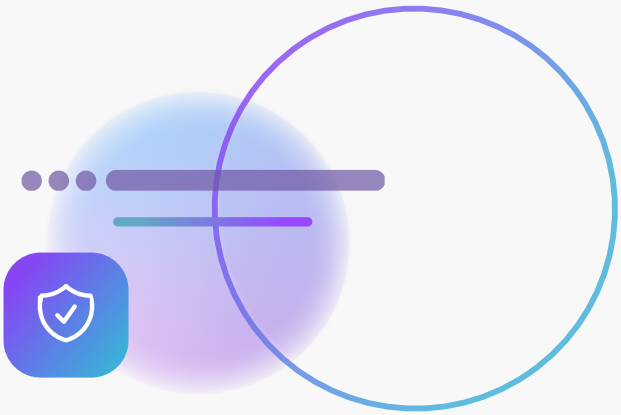
働く場所が変化してきたように、ウェアラブルデバイス、空間コンピューティング、AIといった新たなテクノロジーは、「働き方そのもの」に大きな変革をもたらしています。これらのテクノロジーは、ビジネスツールとしてユーザ体験を向上させ、生産性を革新し、業界を問わずグローバルなイノベーションを加速させています。

しかし同時に、こうしたテクノロジーの活用により、攻撃対象領域の拡大、可視性の断片化、運用リソースへの負荷増大といった新たなリスクも生まれています。そのため、企業のリーダーやIT/セキュリティ部門には、データを保護し、デバイスを包括的に管理しながら、組織全体の成長に柔軟かつ効率的に対応できるよう、エンドポイント戦略の再構築が求められています。

本書では、組織が管理を最新化すべき理由を概説するとともに、実際の状況に基づいた、強靭な基盤を構築・強化するための、プラットフォーム非依存のガイダンスを提供します。また、複雑さの軽減、可視性のギャップ解消、そしてハイブリッドコンピューティング時代への備えに向けた、実用的な対策も紹介しています。

本書の主なトピック：

- 新興テクノロジーに対応した管理・コンプライアンス戦略への適応方法
- 従来型のアプローチでは十分なセキュリティを確保できない理由
- 自動化と継続的なポリシー適用を中核とする戦略の活用
- ビジネス目標に沿った管理、ID、セキュリティ、コンプライアンスの確立
- ゼロトラストを現代のエンドポイントセキュリティの基本原則として導入する意義



概要

企業は今、ウェアラブルデバイス、IoT、AIといったハイブリッドコンピューティングモデルが急速に進化する時代の真っ只中にいます。これらの新興テクノロジーは、あらゆる業界でビジネスオペレーションを刷新し、イノベーションを加速させていますが、一方で複雑さや分断、新たなリスク要因も招いています。デバイスの多様化が進むにつれ、包括的な管理、コンテキストベースのアクセス制御ポリシー、継続的なセキュリティ状態の検証、そしてゼロトラストの導入がこれまで以上に求められるようになっています。ワークフローの自動化、高い可視性、ポリシーに基づいた制御に投資する組織は、データの保護、規制の変化への対応、新興テクノロジーのさらなる発展にも自信を持って効果的に対応できるでしょう。

重要なポイント：

- 堅牢型デバイスの年平均成長率（CAGR）予測 ー 2028年までに：**8.4%**
- スペーシャルコンピューティングのCAGR予測 ー 2030年までに：**33.16%**
- ハイブリッド型コンピューティングの企業導入率 ー 2028年までに：**40%**
- 顧客サービスの自動対応率 ー 2029年までに：**80%**
- ウェアラブルデバイスの出荷台数予測 ー 2025年：**5億9,070万台**

新興テクノロジー – 2026年以降

ウェアラブルデバイス、IoT、AIがパイロット導入を経て、ビジネス成果をもたらす本格的なエンタープライズツールへと進化し、コンピューティングの新時代が加速しています。これらのテクノロジーは、人々の働き方、学び方、関わり方を再定義し、現実世界とデジタルワークスペースの境界を曖昧にしながら、創造性、生産性、コラボレーション、洞察、そして自動化の新たなレベルを引き出しています。この変化の波に乗る組織は、戦略的に連携し、レジリエンスを高め、柔軟に拡張しながら、次のイノベーションを牽引するチャンスをつかめるでしょう。

空間コンピューティング

1990年代後半のゲームセンターに登場した『Virtual Reality（VR）Vortex』は、多くの人にとって初めての“仮想現実体験”でした。拡張現実（AR）やエクステンデッドリアリティ（XR）を含むこれらの技術は、今や複合現実（MR）へと進化し、現実世界とデジタル世界の理解の橋渡しをしています。

空間コンピューティングと総称されるこの技術は、学習と生産性の次なる進化の形であり、**年平均成長率（CAGR）は2030年までに33.16%に達すると推定**されています。

空間コンピューティングはまだ未成熟の段階ですが、この新興テクノロジーが秘める可能性は、教育、製造、医療など**世界中のさまざまな業界で**感じられ始めています。

空間コンピューティングが実際にどのように活用されているかがわかる事例をいくつかご紹介します。

- **オンボーディングの効率化：**新入社員が初日から職場に適応できるよう、見学・体験を通じた支援を行います。
- **ラピッドプロトタイピング：**エンジニアは製品を素開発・反復しながら、構造の整合性を検証し、リアルタイムで共同作業を行えます。
- **専門的なトレーニング：**外科医は、3Dオーバーレイによる没入型シミュレーションを通じて、現実に近い環境で手術手技を練習し、習熟と精度の向上を図ります。
- **顧客体験の強化：**小売業では、スマートフォンを活用して商品を自宅で確認・可視化したりバーチャルに試着することで、場所に縛られない顧客対応が可能になります。
- **ジャストインタイムのトラブルシューティング：**機械操作員はApple Vision Proを使用して問題を特定したり分析を実施したりして、製造現場で問題を解決できます。

ウェアラブルデバイス

信じられますか？Apple Watch には、かつて Pentium 4 クラスのデスクトップコンピュータにしか搭載できなかったハードウェアが小型化されて搭載されています。

ウェアラブルデバイスは、マルチコアプロセッサ、ニューラルエンジン、多数の微細なセンサーを搭載し、コンピューティングソースとして独立して動作でき、顔、手、指、手首に装着する高性能でエネルギー効率の良いデバイスとして、仕事に（遊びにも）申し分なく利用できます。

2025年に出荷された5億9,070万台のウェアラブルデバイスの活用事例をいくつかご紹介します。

- **腕時計：**GPS機能を搭載しモバイルデータ通信にも対応したスマートウォッチで旅行が（国内・海外を問わず）シンプルになります。面倒で高額なデータローミングプランで手を煩わせなくても、オフィスや大切な人といつでも連絡を取ることができます。
- **トラッカー：**最新の健康情報を確認しながら、バイタルサインを予防的にモニタリングし、目標達成までの進捗を把握。事故や体調の異変にもすばやく反応し、必要な救命医療につなげることができます。
- **イヤホン：**ノイズキャンセリングテクノロジーが外部からの雑音を抑えてくれるため、重要なことに集中できます。また、スマートフォンと連携させれば、複数の言語にリアルタイムで変換してくれるライブ翻訳機能も利用できます。
- **スマートグラス：**待ち合わせ場所への道順を確認したりしながら、急ぎのメッセージに返信する際に写真や動画を撮影するといったことが可能です。統合されたAIアシスタントにより、ハンズフリーで短時間により多くの作業をこなすことが可能です。

モノのインターネット（IoT）

効率化は事業継続の推進力です。自動化は効率化を実現する要素の一つなので、業務フローなどにおけるビジネスインテリジェンスの構築にIoTデバイスが使われるのは当然と言えます。事業運営を一元的に効率化する際に下す、データに基づく意思決定に大きなメリットをもたらすからです。

また、特定のビジネスモデルでは、センサーと自動化を組み合わせることで**約20〜30%のエネルギーコストを削減**できます。さらに、予知保全などへの戦略の転換を通して（事後対応型ではなく）予防型のアプローチで予定外のダウンタイムを削減することで、**保守コストを最大50%削減できる** 可能性もあります。

IoTが企業にメリットをもたらす事例をいくつかご紹介します。

- **資産トラッキングと物流ネットワーク：**在庫管理をシンプルにし、予測分析と組み合わせることで、キャパシティプランニングや在庫予測の精度を向上させます。
- **顧客体験のパーソナライズ：**一人ひとりのニーズに合わせた対応により、ブランドロイヤルティを強化し、サービス提供の質を向上させます。
- **建物や施設の管理：**冷暖房・空調（HVAC）、照明、セキュリティを自動化することで、エネルギー消費量を削減し、建物の機能効率を高められます。
- **高度なシステムの相互接続：**センサーとIoTを統合することで既存システムから付加価値を引き出し、新たなサービスや収益機会を創出できます。

人工知能（AI）

AIが持つ可能性は、企業ユーザと個人ユーザのどちらにも影響を与えています。世界中のさまざまな業界で活用されており、生成AIがビジネスにもたらす変革的なメリットには限りがないようです。

- **価値の拡大：**定型作業は自動化され、従業員は自身のスキルを戦略的な業務に注ぐことができます。
- **ROIの向上：**リソースの最適化と効率の向上によってプロセスが最適化され、運用コストが削減されるうえに、イノベーションと顧客体験の強化を通じて数字に表れないメリットも得られます。
- **プロセスの合理化：**コンセプトの可視化、コンテンツの要約、サンプルコードの迅速な開発を通じてリソースを最大限に活用できます。
- **分析の強化：**有益なインサイトを獲得し、トレンド評価を行い、データに基づいてプロアクティブな意思決定を下して、市場投入時間（GTM）を短縮できます。

さらに、エージェント型AI（人間が介入せずに意思決定を行うAI）には、上記のメリットをさらに広げる大きな利点があります。たとえば、Gartner社の調査によると、**2029年までにカスタマーサービスの一般的な課題の80%が自動で解決する**と予測されています。他にも、予防型アプローチ（脅威ハンティング）や適応型アプローチ（リアルタイム学習）といった機能も利用できます。企業の根幹をなすプロセスにエージェント型AIが変革をもたらす可能性を秘めている分野の一つが、サイバーセキュリティソフトウェアです。エージェント型AIをベースにしたセキュリティソリューションは、リスク要因を継続的に監視・評価し、人間が介入しなくても迅速に脅威を軽減する措置を講じて、対応までの時間を短縮し、レジリエンスを維持します。

ハイブリッドコンピューティング

世界中の企業が、業務効率やワークロード管理、リソースの確保・拡張、さらには法規制対応や資本支出といったさまざまな課題に直面しています。こうした課題は、オンプレミスやパブリック／プライベートクラウドといった従来のコンピューティングモデルだけでは、もはや十分に対応できません。エッジコンピューティングのようにデバイスに近い場所でデータを処理して工程を迅速化する低レイテンシモデルであっても、変化が急速なデジタル環境のすべての懸念に対処できるわけではありません。

ハイブリッドコンピューティングは、新興テクノロジーだけでなく既存のコンピューティングモデルを組み合わせる新たなパラダイムであり、前述の課題に次のような特性で対応します。

- **俊敏性：**組織は複数のコンピューティングモデルを活用することで、想定外のピーク時でも低コストでトラフィックの処理を最適化し、対応までの時間を短縮し、レイテンシを削減できます。
- **パフォーマンス：**AI活用型ツールと自動化を導入し、効率を最大限に高めた環境でワークロードをインテリジェントに分散することで、生産性を向上できます。
- **コンプライアンス：**ジオペイトリエーション（地理的データ管理）により、データやアプリケーションの保存場所を企業自身が管理できるようになり、プライバシー保護や規制要件への対応と同時に、データ主権も確保できます。
- **レジリエンス：**クラウド、オンプレミス、従来システムの統合を活用することで、事業継続を効率化し、障害発生時でも事業運営を継続できます。

Gartner社は、**ハイブリッドコンピューティング パラダイムアーキテクチャを重要なビジネスワークフローに導入するトップ企業は、現在の8%から大きく増加し、2028年までに40%を超える**と予測しています。

企業 IT を取り巻く課題

デバイスが管理の範囲から外れると、可視性にギャップが生じ、以下の点に支障がでます。

- セキュリティ状態の把握
- 脅威への迅速な対応
- データセキュリティの維持

多様なプラットフォームやデバイスに加え、所有モデルの違いやハイブリッドワーク環境が組織にもたらすさまざまな変数は、攻撃対象領域の拡大を引き起こしています。さらに、進化する脅威環境へのリスク対策を担っているチームには、これが一層の負担となっています。一方、AIとIoTをめぐる規制の変化と分断された基準によって、組織や業界全体に対するガバナンスと責任ある導入の重要性が世界規模で高まっています。

登録と初期設定

包括的な管理・セキュリティ戦略は、まずデバイスのエ登録から始まり、コンプライアンスの維持、データの保護、従業員の生産性確保に必要なツールや設定をデバイスに適切に配備できる能力が求められます。このようなベストプラクティスは包括的なITワークフローに組み込まれており、導入に関する多くの標準やフレームワークの対象にもなっています。

デバイスが管理スイートに登録されていなかったり、ユーザが業務の遂行に使用するツールが初期設定されていなかったりすると、じわじわと、しかし確実に支障が出始め、次の要素に対してリスクが生じます。

- デバイスの使い勝手
- データの機密性
- コミュニケーションの整合性
- ユーザプライバシー
- エンドポイントの可用性

個々のリスク要因がサービス品質やコンプライアンスに影響を与え、結果として事業継続への悪影響が連鎖的に拡大していきます。

ポリシーと可視性のギャップ

デバイスに関するインサイトは、あらゆるセキュリティ戦略にとって重要な基盤です。エンドポイントの状態を可視化・分析できない場合、IT部門やセキュリティ部門は、新興テクノロジーデバイスが企業インフラに接続・通信・リソースを利用する中で、内部で何が起きているかを正確に把握できません。

テレメトリの死角によって、管理者が把握できないまま潜在的な問題が数多く存在している可能性があります。脅威がどこにあるのか、限られたリソースや対応策の中で何を優先すべきかが見えなければ、こうした問題に効果的に対処することはできません。

可視性のギャップを引き起こす主な要因例：

- 複数のOSプラットフォーム
- 物理的な改ざん
- 所有モデルの混在
- サポート対象外のデバイスタイプ
- デバイスの設定ミス

脅威とリスクの軽減

ハードウェアやソフトウェアの脆弱性を狙う脅威アクターの存在は、サイバーセキュリティにおいて目新しいものではありません。しかし、ハイブリッド環境の普及や多様なデバイスの混在により、リスクの軽減は一層困難になっています。それぞれのデバイスは複数のソフトウェアプラットフォーム上で動作しており、組織に対して多様なリスクをもたらす要因となっています。

オープンソース、独自仕様システム、クローズドシステム、各種デバイスが混在する環境は、エンドポイントの管理と保護を担うITチームやセキュリティチームにとって大きな負担になっています。エンドポイントのセキュリティ状態を把握できないことや、大規模にデバイスを安全に構成する能力が限られていることが重なると、以下のような課題が企業リソースのセキュリティ維持をさらに困難にします。

- データのセキュリティ
- 脆弱性の悪用
- ネットワークのレジリエンス
- パッチ管理
- 攻撃対象エリアの拡大

規制およびコンプライアンス対応の圧力

新興テクノロジーは、既存のシステムやレガシーシステムとは異なり、多様で変化の速い数多くの課題を世界中で招いています。IoTのようなテクノロジーはその性質上分断されていることから、基準が統一されておらず、それによってデータセキュリティに関するさまざまな懸念が生じる場合があります。AIの活用によって得られる性能面でのメリットについては、多くの人が同意しています。しかし、その一方で、人間社会や環境に与える影響については、十分に理解されておらず、意見の一致も見られません。

こうした懸念の多くがリアルタイムで議論・対応されている一方で、すでに技術の進展に追いついた一部の法制度では、カリフォルニア州消費者プライバシー法（CCPA）や欧州一般データ保護規則（GDPR）といった厳格なデータ保護規制により、新たなテクノロジーの活用方法に対して非常に厳しい監視の目が向けられています。企業のリーダーが利用の可否や使用場所を判断するにあたって体系的評価が必要となる他の考慮事項には、以下のようなものがあります。

- データの格納場所
- 運用のレジリエンス
- 第三者によるリスク評価
- ガバナンス面の要因
- 倫理的な考慮事項

将来を見据えたソリューションとベストプラクティス

新たなテクノロジーを導入する際の課題に対応するには、リスクを最小限に抑えるための実績あるベストプラクティスを軸に、取り組みを構築することが重要です。このようなこうした体系的かつ実践的なアプローチは、エンドポイントの多様化や新たなユースケースの出現に対応しながら、スケーラブルで柔軟性の高いエンドポイント管理を実現します。それにより、成長するビジネスニーズにより的確に応えることが可能になります。

エンドポイントインベントリ

企業が包括的なリスク評価を行うには、まず自社のインフラの現状を把握する必要があります。その最善の方法は、すべてのハードウェア、ソフトウェア、サービス、プロセスを網羅したインベントリを作成することです。具体的には、以下の要素を詳しく把握します。

- すべてのデバイス
- その依存関係
- ワークフローとプロセス

各要素とその相互接続のあり方を洗い出すことで、インフラ全体、やりとりの方法、やりとりするデバイスを総合的に把握でき、企業は将来を見据えたソリューションを実装するための強固な基盤を築くことができます。

リスク評価

次のステップは、リスク要因を評価して、その重大度を判断することです。この段階での目的は、リスクの軽減だけでなく、各リスク要因を組織全体のリスク許容度やリスク選好度に見合ったものにすることです。

定性的な手法と定量的な手法を組み合わせることで、プログラミング的なサイバーリスク指標を策定し、以下に挙げるような主要な攻撃指標に基づいたデータ主体の概要を意思決定者に提供できます。

- **ベクトル**：攻撃を実行したりシステムを侵害したりするために使用される経路または手法。
- **複雑さ**：攻撃者が脆弱性を悪用するために必要なスキルとリソース。
- **影響**：攻撃が成功した場合のビジネス面や運用面の影響。
- **露出度**：環境を悪用されるおそれのある状態にする弱点やギャップ。
- **重大度**：脅威が発生する可能性と起こりうる被害の大きさを示す指標。
- **修復**：修正プログラムの有無、内容、導入に要する時間。

脅威モデリング

3つ目のステップは、デバイス、システム、アプリケーションにおけるリスクを特定して優先順位を付けるという予防的なアプローチです。具体的には、ペネトレーションテスト（次のセクションで詳しく説明します）の前に脅威モデリングを実施して、リスクを重大度の高いものから低いものへ優先順位付けすることが主な作業です。これには、デバイスリスクの軽減だけではなく、組織のセキュリティ状態を強化する効果もあります。

複数の脅威モデルがあり、特定の種類のリスクを評価したり、統合型のアプローチで脅威を体系的に検出して定量化したりすることができます。別の言い方をすれば、攻撃を軽減する最善の方法は、攻撃者のように考えることなのです。

一般的な脅威モデリング手法とその目的は、次のようなものです。

STRIDE：
Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Informative disclosure（情報漏洩）、Denial of service（サービス拒否（DoS）攻撃）、Elevation of privilege（権限昇格）。
概要：
内容に基づいてリスクを6つのカテゴリに分類します。

DREAD：
DREAD：Damage potential（潜在的な損害）、Reproducibility（再現可能性）、Exploitability（攻撃利用可能性）、Affected users（影響を受けるユーザ）、Discoverability（発見可能性）
概要：
5つの要素に基づいて平均スコアを算出し、リスクの重大度をランク付けします（多くの場合、STRIDEと組み合わせて使用し、高リスクの脅威の軽減策に優先順位を付けます）。

LINDDUN：
Linking（関連付け）、Identifying（識別可能性）、Non-repudiation（否認防止）、Detecting（検出可能性）、Data disclosure（情報漏えい）、Unawareness（利用者の不認知）、Non-compliance（法令・ポリシーの不遵守）

概要：
このモデルは、アプリケーションやシステム内におけるデータの流れを分析することで、プライバシーに関わる脅威を体系的に特定・軽減するための手法を提供します。

PASTA：
攻撃シミュレーションおよび脅威分析プロセス。
概要：
このモデルは、ビジネスインパクトを重視したリスク評価を行い、リスク軽減戦略の策定に向けた技術的要件（ビジネスの目的とスコープの定義、脆弱性の分析、攻撃シナリオのシミュレーションなど）を含む、体系的なプロセスを提供します。

OCTAVE：
業務上重要な脅威・資産・脆弱性の評価
概要：サイバーセキュリティ対策をビジネス目標と整合させながら、ビジネスリスクに焦点を当てる脅威モデリング手法です。このモデルでは、資産ベースの脅威プロファイルの構築、インフラにおける脆弱性の特定、リスク管理戦略の策定という3つのフェーズを通じて、リスクを体系的に評価・軽減していきます。。

ペネトレーションテスト

リスク評価において最も一般的なタスクはペネトレーションテストでしょう。これは多くの場合、デバイスやソフトウェアの脆弱性を発見して優先順位を付けるために行われます。この項目を最後に取り上げている理由は、前章で説明した脅威モデリングとの関係にあります。脅威モデリングの後にペネトレーションテストを実施することで、リスク評価プロセス全体の効率性と有効性が向上します。

効率性の向上：

- 脅威モデリングによって低リスクの脅威が事前に特定されているため、ペネトレーションテスト担当者はより深刻なリスクに集中できる
- IT部門が評価プロセスの早い段階でリスク軽減に着手できるようになる

有効性の向上：

- すでに実施された対策（リメディエーション）の有効性を検証できる
- これまで見逃されていた可能性のある脆弱性を発見するための、追加の検証レイヤーが加わる

デバイス状態とアイデンティティファーストアクセス（ゼロトラストに向けた取り組み）

新たなテクノロジーの導入が進む中で、IDを起点としたセキュリティ戦略と、デバイスのセキュリティ状態（デバイスポスチャ）の継続的な検証は不可欠です。多様化が進むデバイス群への対応を継続するには、管理の近代化が不可欠です。そのためには、ポリシーの適用を自動化し、運用負荷を軽減しながら、ゼロトラストをシームレスに拡張できる体制が求められます。

以下のソリューションは、新たなテクノロジーのライフサイクル管理を支援するために、IT部門に柔軟なツールを提供します。

- **モバイルデバイス管理（MDM）**：デバイス管理とID管理を統合し、エンドポイントセキュリティも包括的に提供します。**ゼロタッチ導入から安全な廃棄まで**、オンプレミス環境でもクラウド環境でも対応可能です。
- **統合エンドポイント管理（UEM）**：オンプレミス環境またはクラウド環境に対応し、複数のプラットフォームを横断的にサポートします。ただし、機能の幅広さよりも汎用性が優先される傾向があり、個々の機能は限定的な場合があります。
- **Amazon Web Services（AWS）：**IoTデバイスなど特定のテクノロジーに限定された管理とセキュリティを提供し、複数のベンダーをサポートするクラウドベースのモデルです。
- **自律型エンドポイント管理（AEM）：** クラウドベースのUEMの進化系であり、自動化によって運用コストを削減し、多様化するデバイス群にも柔軟に対応し、組織規模に応じてゼロトラストを実現します。具体的には、デバイスの状態（ポスチャ）を継続的に検証・修正することで、常に信頼できる状態を保ちます。

アプリとデータの制御

どのようなデバイスやOSであっても、本質的には扱うものは「データ」であるという点に変わりはありません。新興テクノロジーの管理・保護に関わるあらゆる施策や業務の根幹にあるのは、データを守るという目的です。

デバイスとデバイス内で処理・保存されるデータを保護する効果的な方法の一つが、構成の導入です。使える手法はOSプラットフォームによって大きく異なりますが、目的は同じで、標準やフレームワークなど、OSの垣根を越えて適用できるベストプラクティスに基づいてセキュアな構成を確立し、データの安全を守ることにあります。

セキュアな構成を作成するために使用されるツールの例：

- **Android：OEMConfig**、**Android Open Source Project**（AOSP）
- **Apple：Apple Configurator**、**Jamf Pro**、**宣言型デバイス管理**（DDM）
- **Linux：**Bashスクリプト、**SOTI MobiControl**、**Microsoft Intune**
- **独自仕様：**製造元のサポートサイトで、対象テクノロジーに特化したツールの入手場所に関する情報を確認してください。

監視と対応

エンドポイントの健全性の可視化は、予防型のサイバーセキュリティに欠かせない要素です。問題の特定が早ければ早いほど、インシデント対応でリスクの軽減や脅威の修復を実施するまでの時間を短縮できます。インフラ内のエンドポイントの積極的な監視は、強く推奨されるだけでなく、ゼロトラストアーキテクチャのきわめて重要な要素でもあります。

デバイス上の保護とネットワーク内の保護は、ゼロトラスト保護を構成する2要素です。デバイスの強固なセキュリティ態勢をインフラ全体で維持するうえで役立つ、エンドポイントを中心としたガイドラインを以下に示します（ネットワーク側については次のセクションで説明します）。

- デバイスの健全性テレメトリとコンプライアンスレベルを積極的に監視する
- 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、対応を自動化する
- リソースへのアクセスを許可する前にエンドポイントの健全性を検証するゼロトラストを実装する
- オペレーティングシステムのアップデート、セキュリティパッチ、アプリパッチを定期的に展開する

ネットワークセキュリティ

新興テクノロジーの進化のペースに標準の策定が追いつかないことが多く、特定のエンドポイントの管理が難しくなったり、ビジネス目標に合致しなくなったりしがちです。リスクの認識は主観的なものであるため、オールマイティなセキュリティ戦略というものはありません。より重点的に保護すべき対象は、エンドポイントのデータです。以下のソリューションは、単体で導入する場合でも、組み合わせて導入する場合でも、ローカル環境とクラウド環境全体でデータのセキュリティを最大限に高めるのに役立ちます。

- **非武装地帯（DMZ）**：IoTなどリスクの高いデバイスをセグメント化し、内部システムや外部ネットワークとの通信はポリシーに照らして制御されたものだけを許可します。
- **仮想ローカルエリアネットワーク（VLAN）**：ネットワークトラフィックを分離し、最小限のアクセスを適用して侵入拡大を抑制することで、IT部門がデバイスとミッションクリティカルなシステム間のトラフィックをきめ細かく制御できるようにします。
- **セキュリティ オーケストレーション オートメーション アンド レスポンス（SOAR）**：自動化を通じてセキュリティツールとワークフローを統合し、脅威の検出・対応・封じ込めを迅速化します。
- **ゼロタッチネットワークアクセス（ZTNA）**：継続的かつコンテキストに基づくデバイスの検証、接続要求ごとのマイクロトンネリング、およびヘルスチェックを適用し、準拠したデバイスのみが保護されたリソースにアクセスできるように制限します。

ベースラインとベンチマーク、標準とフレームワーク

各セクションは一方向に進むものではなく、継続的かつ繰り返し実行される循環的なプロセスとして理解することが重要です。ITとセキュリティのライフサイクルは、終わりのない反復的なプロセスです。過去の対応が次の判断に活かされ、継続的に最適化されていきます。これを踏まえたうえで、セキュリティを維持しながらテクノロジースタックに新興テクノロジーを組み込むためには、以下の各セクション間の相乗効果が非常に重要になります。

- **ベースライン：基本のセキュリティ状態を定義する**一連の対策とプロセス。
- **ベンチマーク：セキュリティのベストプラクティスへの準拠状況を測定する**ために使用されるパフォーマンス指標。
- **標準：特定の要件を満たす**ためにハードウェア、ソフトウェア、サービスのセキュリティを確保する方法を明確化した、世界的に認められているベストプラクティス。
- **フレームワーク：リスクを最小限に抑えて**セキュリティを最大限に高めるために、対策、ポリシー、プロセス、標準をどのように導入すべきかを詳述した体系的なガイドライン。

まとめ

新興テクノロジーの理解と、そのビジネスへの影響を踏まえた今、現行の管理およびセキュリティ戦略を、将来を見据えた実践的な方針へと移行すべき時が来ています。いち早く行動を起こすことで、組織は新たなリスクに先手を打ち、業務を効率化し、自信を持ってイノベーションの新時代を迎えることができるでしょう。

チェックリスト：ビジネスリーダーとIT管理者の次のステップ

1. ビジネスへの活用法を特定

- AI、IoT、空間コンピューティング、ウェアラブルなどの新興テクノロジーが、自社のビジネス目標とどのように一致しているかを見極める。
- 既存のワークフローに対する潜在的なROIと運用の改善点を特定する。
- 測定可能なビジネス成果とコンプライアンス対応を促進する取り組みの優先順位を付ける。

2. 部門横断的な評価チームの立ち上げ

- IT、セキュリティ、法務、業務の各関係者からなる委員会を編成する。
- リスク評価、コンプライアンスレビュー、ライフサイクル管理の責任者を任命する。
- 迅速なフィードバックとエスカレーションのためのコミュニケーションチャネルを決定する。

3. 資産および依存関係の包括的な棚卸しを実施

- インフラ内で使用されているすべてのデバイス、ソフトウェア、API、クラウドサービスを文書化する。
- ハイブリッド環境（クラウド、オンプレミス、エッジ）全体の統合依存関係を特定する。
- COBO/COPE/BYOD/CYODなどのデバイス運用モデルを明確にタグ付けし、可視性と責任の所在を確保する。

4. リスクと脅威の評価を実施

- リスク許容度と影響度を評価するために、定性的および定量的な手法の両方を活用する。
- 精度と一貫性を確保するために、モデルを使用して脅威をマッピングする。
- 脆弱性を、深刻度・悪用されやすさ・修正にかかる期間の観点からランク付けする。

5. 脅威モデリングの実施

- 承認された脅威モデリングフレームワークを使用して、潜在的な攻撃経路をシミュレートする。
- プライバシー、データフロー、運用面のセキュリティ露出点を特定する。
- 本番環境に導入する前に、リスク軽減の対策を文書化する。

6. コンプライアンスおよびガバナンス要件の確認

- 地域や業界固有の規制を調べる。
- データの格納場所、主権、サードパーティベンダーのリスク管理を確認する。
- AIとデータ駆動型テクノロジーに関する倫理的な考慮事項を組み込む。

7. デバイス登録およびプロビジョニングプロセスの定義

- すべてのデバイスタイプと所有モデルでオンボーディングワークフローを標準化する
- 構成、定期的なパッチ適用、アクセス制御を自動化し、手作業によるエラーを最小限に抑える。
- 安全な登録とIDベースの認証を使用してエンドポイントを検証する。

8. アイデンティティファーストのアクセス戦略を統合

- リソースにアクセスする前に認証情報とデバイス状態を継続的に検証することを義務付ける。
- エンドポイントとアプリケーション全体に最小権限の原則を適用する。
- ゼロトラストポリシーとコンテキストアウェアポリシーをアクセス制御システムに統合する。

9. セキュアな構成とデータ制御の確立

- セキュリティベースラインを定義して、構成とコンプライアンスの期待水準を設定する。
- 保存中と転送中の機密データを暗号化する。
- 分類、保存、共有のための詳細なデータポリシーを実装する。

10. ネットワーク通信のセグメント化と強化

- VLANとDMZを使用して、IoTやウェアラブルデバイスなどリスクの高いデバイスを分離する。
- マイクロセグメンテーションとゼロトラストネットワークアクセス（ZTNA）を適用して、適応性の高いネットワーク内セキュリティ対策を講じる。
- デバイスタイプ、所有モデル、OSプラットフォーム、ユーザの作業場所にかかわらず、データセキュリティをネットワークセキュリティの中心に据える。

11. 継続的な監視と自動対応のポリシーを実装する

- すべてのエンドポイントからテレメトリを収集し、リアルタイムの可視性と健全性に関するインサイトを取得する。
- 異常検出とインシデント対応のための自動ワークフローを導入する。
- アラートを一元的なツールにストリーミングし、脅威検出と修復のタスクを自動化する。

12. ベースラインとベンチマークの適用、および生産性指標の収集

- 企業全体の包括的なセキュリティを実現するためのベースライン構成の標準を適用する。
- ベンチマークを使用して、パフォーマンスとセキュリティ状態を測定する。
- KPIをレビューして、コンプライアンス状況を評価し、リスクの低減を実証する。

13. 定期的な検証（ペネトレーションテストや監査）の実施

- 導入後に行う定期的なペネトレーションテストと脆弱性スキャンの実施日を決める。
- 脅威モデリングで特定された修復策を検証する。
- 定評のあるベースラインに照らして調査結果を精査し、それに応じてポリシーを更新する。

14. ライフサイクル管理とポリシー適用の自動化

- 統合エンドポイント管理システムや自律型管理システムを活用して、コンプライアンスを維持する。
- パッチ適用プロセス、コンプライアンスポリシー、デバイス廃棄ワークフローを自動化する。
- 構成をフレームワークや標準の進化に合わせて継続的に調整する。

15. 調査結果の文書化と定期的なトレーニングの実施

- 新たな脅威と得られた教訓に関するフィードバックループを確立する。
- 管理者とユーザがリスクを認識できるようにトレーニングを継続的に提供する。
- テクノロジーと規制の変化に合わせて適合状況を再評価し、対策を継続的に改善する。