



## 新しい脅威の中で エンドポイントを保護する

テレワーク中に生産性を最大限に発揮できる柔軟性を従業員に提供する場合、従業員にテレワークできる柔軟性を与えつつ、拡大する脅威のランドスケープの防止、検出、対応を実現するためのエンドポイントセキュリティ対策を備えていることが重要になる。



ITリーダーは昨今の不安定な状況が与える影響を早く捉えようと情報の収集や分析を続けており、多くのリーダーは、テレワーク社員がこれまでにないほど増える中で、新しい標準を迎える予定を立てている。多くの企業と従業員が生産性の向上とより柔軟な働き方によるメリットを得ている一方で、保護の面では代償を払う必要がある。昨今の不安定な状況によるテレワークの急増で、エンドポイントの保護がさらに困難になっている。ITリーダーの84%は、テレワーク社員の保護が困難であると回答している。<sup>1</sup> 説得力のある説明の1つは、不安定な状況の中で世界中の組織に対するランサムウェア攻撃が148%増加していることだ。<sup>2</sup> これが深刻な統計である理由は、在宅勤務の従業員はEメールをビジネス コミュニケーションの主な手段として使用しており、それによってフィッシング攻撃が350%増加しているからだ。<sup>3</sup>

## 現在のサイバー セキュリティの動向

テレワークに突然に移行した裏で、多くの厄介なサイバー セキュリティの懸念があり、サイバー セキュリティの専門家の専門知識が必要になっている。なかでも次のような懸念が挙げられる。

1. BIOSレベルの攻撃：ハードウェアまたはシリコンの脆弱性を悪用される。BIOSが侵害された場合、通常、攻撃者は隠れたままで、デバイスの認証情報を使用してネットワークとデータにアクセスできる。63%の企業は、このような攻撃によるデータ侵害または侵害を経験している。<sup>4</sup>
2. 高度で持続的な脅威（APT）：多くの場合、高度な攻撃者は貴重なデータを吸い上げる前に、行動情報を収集しながら静かに潜伏する。被害者はサイレント攻撃が発生していることに長期間気付かないことがある。気付くまでに平均で108日かかっている。<sup>5</sup>
3. ファイルベースおよびファイルレス マルウェア
  - ・ファイルベースのマルウェア：通常は、従業員の業務で必要となるような使い慣れた拡張子（.DOCXや.PDFなど）を持つファイル タイプ。ユーザーがファイルを開くと、埋め込まれた悪意のあるコードが実行される。
  - ・ファイルレス マルウェア：通常は、PCに感染する正規プログラム。ユーザーがEメールからこのようなプログラムを起動すると、ファイルレス マルウェアはPCに感染し、さらにはネットワークに感染する可能性がある。これにより、多くのセキュリティ テクノロジーをすり抜けることができる。
4. 国家による攻撃：中国、北朝鮮、ロシア、イランからの攻撃が一般的。こうした国家の専門技術と財政的支援を受けている攻撃は、多くの場合、高度で非常に大きな損害を与える。しかし、これらの攻撃の多くは、最新のアップデートとパッチが適用されていないシステムを悪用するものである。FBIのCISA部門は定期的にアドバイザリーを送信している。



テレワークに突然に移行した裏で、多くの厄介なサイバー セキュリティの懸念があり、サイバー セキュリティの専門家の専門知識が必要になっている

1. 『The State of DLP 2020』、Tessian。

2. VMware Carbon Blackブログ、Patrick UpathamおよびJim Treinen、2020年4月15日。

3. PCMAG.comで引用されたGoogleレポート、2020年3月30日。

4. 『Match Present-Day Security Threats with BIOS-Level Control』、Dellの委託によるForrester Consulting Thought Leadership Paper、2019年6月。

5. 2018 U.S. State of Cybercrime調査。

5. クラウドベースの攻撃：デスクトップ アプリケーションに代わり、クラウドベースのコラボレーションおよび生産性アプリケーションが増加している。平均的な企業では、2,400以上のクラウド サービスを使用しており、93%の組織はクラウドのセキュリティについて、ある程度、または非常に懸念している。<sup>6</sup> 保護には、クラウドでのデータ ロス防止（DLP）と脅威に対する保護が含まれている必要がある。さらに、ユーザー認証ではなりすましから保護する必要があり、データはクラウドとの間で暗号化される必要がある。
6. コンプライアンス規制：個人を特定できる情報（PII）を保護することを目的としたもの。PIIが悪意を持った人の手に渡って最終的にIDの盗難に使用されないようにするため、一部の業種では厳しい罰則のある厳格な規制を採用している。これらには、医療機関におけるHIPAA、金融サービスおよび小売業におけるPCI-DSS、および欧州居住者とビジネスを行う企業を対象としたGDPRなどがある。
7. 壊滅的な影響が及ぶリスク：2021年にはサイバー犯罪による損失が6兆ドルにのぼると予測されており、2015年の3兆ドルから増加している。Cybersecurity Venturesによると、損失は、データの破損および破壊、資金の盗難、生産性の低下、知的財産の盗難、個人および財務データの盗難、攻撃後の業務の中断、評判の失墜などによるものだ。<sup>7</sup>



## エンドポイント セキュリティを再考

### エンドポイント セキュリティ：エンタープライズ セキュリティの一部

これまでになくテレワーク社員の人数が増え、その多くが業務で機密データを扱わなくてはならないため、ITリーダーは、組織のエンドポイント セキュリティの現状を評価する必要がある。しかし、エンドポイント セキュリティを単独で見るのではなく、多層型の保護を実装するエンタープライズ セキュリティに不可欠な部分として見るべきだ。また、エンドポイントだけでなく、ストレージ、ネットワーク、クラウドベースのサービスも含める必要がある。企業内で「信頼できるデバイス」を構築するための総合的なアプローチでは、次の要素を考慮する必要がある。

### 内蔵セキュリティ機能

エンドポイントを保護するためにソフトウェアだけに頼るのではなく、包括的なアプローチでは、信頼できるデバイス（デバイス自体にセキュリティを実装したエンド ユーザー コンピューティング デバイス）を使用することを提唱している。このようなデバイスは、デバイスが紛失または盗難に遭った場合に、PIIを保護し、法令遵守にあたって重要な役割を果たす。また、エンド ユーザー デバイスにはプライバシー スクリーン テクノロジーが搭載されている必要がある。これにより、同僚やオフィスの訪問者がPCの画面上の機密情報を閲覧することに歯止めがかかる。

ITリーダーは、エンドポイント セキュリティをエンタープライズ セキュリティに不可欠な部分として見るべきだ

6. 『Cybersecurity Insiders Cloud Security Reports』、2018年、2019年。

7. Cybersecurity Ventures、2020年。

## OSの上の層と下の層の保護

**OSの上の層**：IT部門は、可視性、モニタリング、およびデータセキュリティ、さらには、脅威に対する防御、検出、修復を必要としている。コンプライアンス要件を満たすためにはデバイスでの暗号化も非常に重要だ。ただし、それによってパフォーマンスが低下して、ユーザーの生産性が低下するようではいけない。

**OSの下の層**：ファームウェアとハードウェアに対する攻撃の頻度が高いため、IT部門はBIOSの保護とチップ認証を必要としている。BIOSが侵害されると、攻撃者は認証情報を含めエンドポイント上のすべてのデータにアクセスでき、組織のネットワーク内を移動し、より広範なITインフラストラクチャを攻撃することが可能になる。

## AIおよびML

今日のますます高度化する攻撃を考えると、エンドポイントの保護にとっては、検出と修復に人工知能と機械学習を使用することが欠かせない。AIおよびMLアルゴリズムは、行動パターンを観察することによって異常なアクティビティを検出し、侵害を知らせて防止できる。

## 安全なサプライチェーン

製造プロセスでは、不正行為者が侵害したコンポーネントを差し込んでバックドア攻撃を行えるようにした可能性がある。製造された製品にこのようなコンポーネントが組み込まれると、非常に損害の大きな侵害が可能になり、検出が困難だ。したがって、サプライヤーと製造元の両方が、サプライチェーンの重要なポイントで厳格なセキュリティ対策を実施することが重要だ。



## 信頼できるデル製デバイス

Dellは、次のテクノロジーを使用して各PCにセキュリティを組み込んでいます。

**SafeBIOS with BIOS Indicators of Attack (IoA)**：改ざんを防止するためにBIOSの変更を可視化する。保護されたイメージをDellがホスト外で管理し、BIOSの整合性を確認する。SafeBIOSは、VMware Carbon Black Audit and Remediationと統合された。これにより、自動レポートによって攻撃の可視性が向上し、リモートアクセスによってBIOSの破損を修復できる。

**SafeID**：チップベースの認証を提供する。エンドユーザーの資格情報は、安全性の低いソフトウェアに頼るのではなく、専用のセキュリティチップを使用して検証される。

**SafeScreen**：機密情報がオフィスの同僚、訪問者、メンテナンス作業員、その他の権限のない人物に漏洩する可能性がある画面を保護する。

**SafeGuard and Response**。VMware Carbon BlackとSecureworksのテクノロジーを活用したDellのポートフォリオには、次のものがある。

**VMware Carbon Black**：1つの軽量なエージェントと使いやすいコンソールを使用して、新しい脅威を寄せ付けないために必要なインテリジェントシステムハードニングと振る舞い防御を組み合わせ、クラウドネイティブのエンドポイント保護プラットフォーム。

信頼できるデバイスは、デバイスが紛失または盗難に遭った場合に、PIIを保護し、法令遵守にあたって重要な役割を果たす

**Secureworksマネージド サービス**：クラウド、ネットワーク、およびエンドポイントからのテレメトリーを収集して関連づけを行い、企業全体の脅威を特定する。業界をリードするインシデント対応を提供するSecureworksマネージド サービスは、VMware Carbon Blackプラットフォームやその他の多くのプラットフォームと統合されている。

**SafeData**。コラボレーションは、成功を収める企業で常に見られる特徴であり、テレワークが増える時代において重要性を増している。現代の従業員のコラボレーションでは、エンドユーザーの生産性が低下することがないように、デバイスとクラウドの両方でデータセキュリティを確保する必要がある。DellはNetskopeおよびAbsoluteとパートナー提携して、総合的なエンドポイントセキュリティを提供している。

**Netskope**。Netskopeテクノロジーは、データ中心のアプローチを取って、クラウドで作成および公開されたデータを保護する。NetskopeはIT部門にリアルタイムの可視性、クラウドへのアクセス、モニタリング、データロス防止機能を提供することで、クラウド、ネットワーク、およびデータセキュリティを新定義している。チームは、保護とスピードの最適なバランスを確保し、組織のデジタルトランスフォーメーションを確実に実現できる。

**Absolute**。Dellは、すべてのデバイスのファームウェアにAbsoluteテクノロジーを組み込み、すべてのエンドポイントにクラウドベースのAbsoluteダッシュボードへの自動修復リンクを提供する。これにより、管理者はネットワーク外にいても、エンドポイントとエンドポイント上のデータの追跡、管理、保護を行うことができる。Absoluteテクノロジーの特長：

- デバイスを検出して管理する。
- VPNおよびセキュリティソフトウェアの保全を実現する。
- エアギャップソリューションを実装して、攻撃からのリカバリーを可能にする。
- ソフトウェアデファインドまたはアプライアンスベースのいずれかにすることができるマルチクラウドデータ保護ソリューションを搭載している。

## まとめ

昨今の不安定な状況によるテレワークの急増で、すでに脅威にあふれたサイバーセキュリティの状況がさらに危険になっている。エンドポイント保護に対する新しい包括的なアプローチが必要だ。エンドポイント保護を再考するためには、まずOSの上と下の両方の層が保護された信頼できるデバイスから始めることだ。このような戦略では、エンドポイントにとどまらず、企業全体のサーバー、ネットワーク、クラウドベースのサービス、および法令遵守を含むサイバーセキュリティを見渡せる。Dellの信頼できるデバイスのポートフォリオは、このような包括的なアプローチを具現化したものだ。Dellのエンドポイント保護は、ソフトウェアデファインドまたはアプライアンスベースのソリューションとして提供可能なマルチクラウドデータ保護ソリューションを含めることができるような企業全体にわたる。さらに、Dellの信頼できるデバイスは、新しいテレワークのパラダイムの中でも、ますます高度化する攻撃から防御することで生産性を維持できるようになっている。

詳細については、こちらを参照していただきたい。

<https://www.delltechnologies.com/ja-jp/endpoint-security/index.htm>



現代の従業員のコラボレーションでは、エンドユーザーの生産性が低下することがないように、デバイスとクラウドの両方でデータセキュリティを確保する必要がある