White Paper

ビジネスに必要不可欠な安全なエンドポイント

Sponsored by: Apple

Tom Mainelli　　Michael Suby
September 2023

IDC の見解

IT 意思決定者（ITDM：IT Decision Makers）の安眠を妨げるものは何か。それは、もちろんセキュリティである。賢明な ITDM は、ビジネスがどれほど安定しようが、製品やサービスがどれほど評価されていようが、セキュリティが機能しなくなれば、ビジネス全体が一夜にして危険にさらされる可能性があることを知っているからである。

そして、残念なことに、世界は少しも安全になってはいない。テクノロジーに関して言えば、産業スパイ、ならず者国家、組織犯罪、そして日常的な窃盗でさえ、レベルアップしているのである。攻撃者に先んじるために、IT 部門は常に警戒を怠らず、新しいベンダーやテクノロジーを積極的に取り入れ、従業員、顧客、データの安全を守らなければならない。

IT 部門が直面するセキュリティ上の課題は多岐に渡っており、エンドポイント（コンピューター）を始め、データセンター、すべてを接続するネットワーク、そしてそれらすべてを動かすソフトウェアに至るまで、あらゆるものが関わっている。本調査レポートでは、エンドポイントをセキュアに保つことの重要性に焦点を合わせている。結局のところ、エンドポイントが安全でなければ、他のすべての分野のセキュリティはほとんど無意味となるためである。

エンドポイントのセキュリティ確保に関する重要な課題の一つは、従来、エンドポイントが安全であるとは、取り扱いの面倒なロックダウンデバイス（自由度を抑え安全性を優先したデバイス）を導入して、安全と引き換えにエンドユーザーに貧弱なエクスペリエンスを強いる場合が多いことである。一度そうなると、セキュリティスキームにおけるもう一つの主な弱点であるユーザーは、仕事を完了させたい一心で、しばしばそのセキュリティを巧みに回避する方法を見つけ出す。セキュリティがユーザーにとって目障りなものとなった瞬間、セキュリティはもはやその目的を果たすことはない。

テクノロジーの進歩によって、セキュリティを高く保ちながらユーザーエクスペリエンスについても高品質を維持する可能性は高まっている。マルウェア検出、データ保護、認証、そしてチップとソフトウェアの融合の進歩は、現在のエンドポイントがセキュリティ強化のために生産性を犠牲にする必要がないことを意味している。

調査方法

IDC は 2023 年 7 月に、米国とカナダの ITDM（n = 513）を対象にオンライン調査を実施し、セキュリティ全般に関する見解と、特にコンピューターエンドポイントのセキュリティ確保の重要性についてたずねた。回答者は、さまざまな業種の従業員規模 500 人以上の企業を対象としている。これらの ITDM は、Microsoft Windows、Apple macOS、Google ChromeOS など、さまざまなコンピューターのオペレーティングシステムをサポートしている。ITDM は、自社でセキュリティソフトウェアを選択、購入、導入しているか、それらの実施担当者を統括する立場にある。

概況

セキュリティは依然として経営陣の責務である。先進的な企業では、優れたセキュリティを「あればよい」ものではなく、組織的で資金力のある攻撃者によって絶えず進化する脅威の中でビジネスを健全に展開し、事業を成功させるための必須要件と認識している。

IDC が 2023 年の 3 月に従業員規模 500 人以上の企業の ITDM を対象に実施した「*Future Enterprise Resiliency and Spending Survey（FERS）*」では、調査対象となった世界中の企業の 50%以上が、過去 12 か月間にビジネスを妨害するランサムウェア攻撃を受けていた。そのグループの 3 分の 1 以上が、攻撃によって 1 週間以上の業務中断が発生したと回答している。大企業はより強固なセキュリティプロトコルを備えていることは間違いないにもかかわらず、このような攻撃を免れているとは言い難い。実際、ランサムウェアによる業務妨害を受けた割合が最も高かったのは、従業員規模 1,000～2,499 人のカテゴリー（71%）、2,500～4,999 人のカテゴリー（72%）、5,000～9,999 人のカテゴリー（70%）の企業であった。つまり、規模には関係なく、このような攻撃を免れる企業はないということである。

同調査では、ランサムウェア攻撃の主な侵入口はエンドポイントであると指摘している。さらに侵害の最初の発生箇所として、Web 閲覧（21%）、リムーバブルメディア（18%）、電子メールの添付ファイル（17%）、サプライチェーン（17%）、電子メール内の URL（14%）、内部アクセス（8%）が挙げられている。

ハイブリッドやリモート環境で働く従業員の増加は、IT 部門にとって、ランサムウェアやその他のセキュリティリスクに関する困難を積み上げるばかりである。IDC が 2022 年 12 月に実施したユーザー調査「*Endpoint Security Survey*」では、97%以上の企業で、従業員の誰かはリモートで勤務している。この数字は今後 1 年間で多少減少すると予測されるが、当面は非常に高い水準で推移するであろう。

企業が従業員の大規模なリモートワークによる持続的な課題に取り組む中で、ゼロトラスト戦略を導入する企業が増えている。ベストプラクティスの重点分野として、セキュリティコントロールのベースラインの確立、エンドポイントの高度なセキュリティ防御、デバイス認証（ネットワークに接続するデバイスが正規のものであることの確認）、強力なユーザー認証などが挙げられる。

以上を考慮すると、Figure 1 で示すように、IDC の調査で回答者が IT の最優先事項として、「データセキュリティ全体の向上」と「コンピューターの安全性確保」を上位の 2 項目として選択したのも当然のことである。

下図（Figure 1）で、IT にとって 3 番目に重要なトピックが、「より適切なデバイスによる従業員の生産性向上」であったことは注目に値する。一方、回答者に全体的なトピックの上位 3 つを選んでもらったところ、「より適切なデバイス」という選択肢が最も多く選ばれた。このことは、IT に関する忘れてはならない重要なメッセージを突きつけている。つまり、セキュリティは重要であるが、従業員の生産性を犠牲にはできない。最高のデバイスは、高いセキュリティと、そのセキュリティによって妨げられることのないエンドユーザーの満足度を兼ね備えているのである。

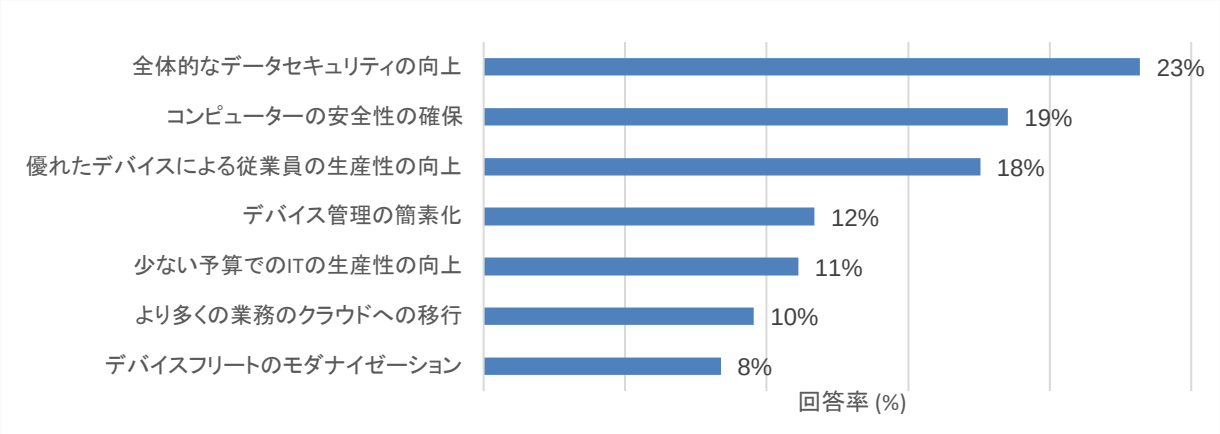
ITDM に、コンピューターベンダーの選定に関して、次に選ぶ際に最も決め手となる要因をたずねたところ、パフォーマンス、既存のアプリケーションのサポート、既存の IT インフラストラクチャとの統合を抑えて、セキュリティが 1 位となった。最も注目すべきは、仕様（スペック）に関する選択肢がその回答の最下位近くに見られたことであろう。

IT の最優先事項については、Figure 1 を参照のこと。コンピューターベンダー選択の際の最優先事項については Figure 2 を参照のこと。

FIGURE 1

IT の最優先課題：データとエンドポイントのセキュリティ

Q. 現在、貴社にとって優先順位の高い IT トピックは次のうちのどれですか？



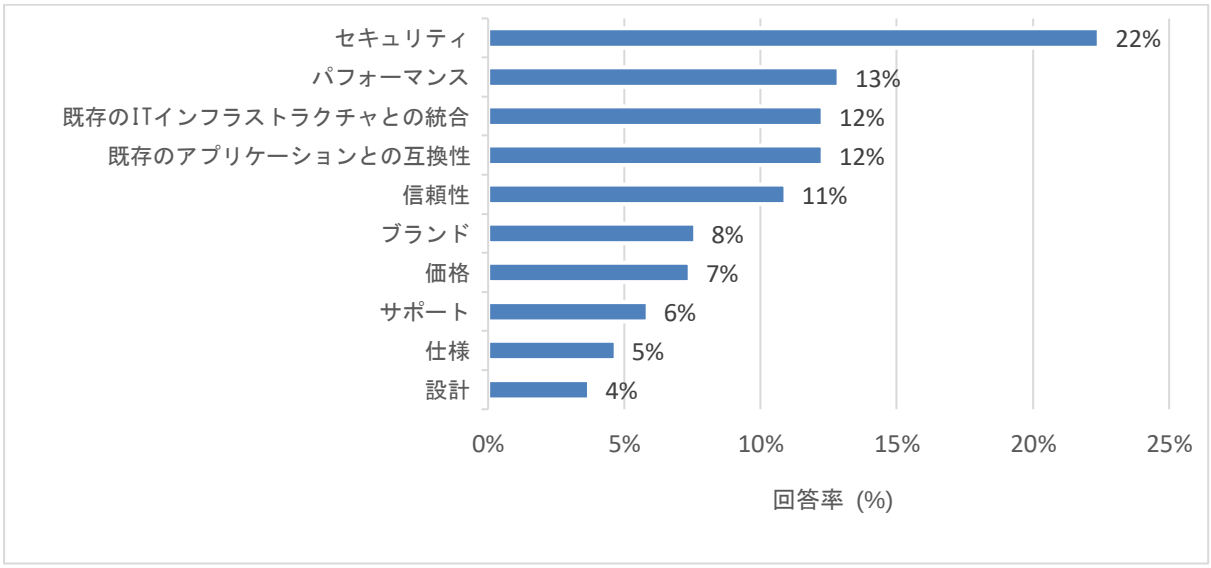
Note: データにはそれらのランキングの最も重要なランク（1 位）を含む

Source: IDC's Secure Endpoint Survey, n = 513

FIGURE 2

コンピューターベンダーの選択における最も重要な要因

Q. 貴社でコンピューターを選ぶ際に、最大の決め手となる要因は何ですか？



Note: データにはそれらのランキングの最も重要なランク（1 位）を含む

Source: IDC's Secure Endpoint Survey, n = 513

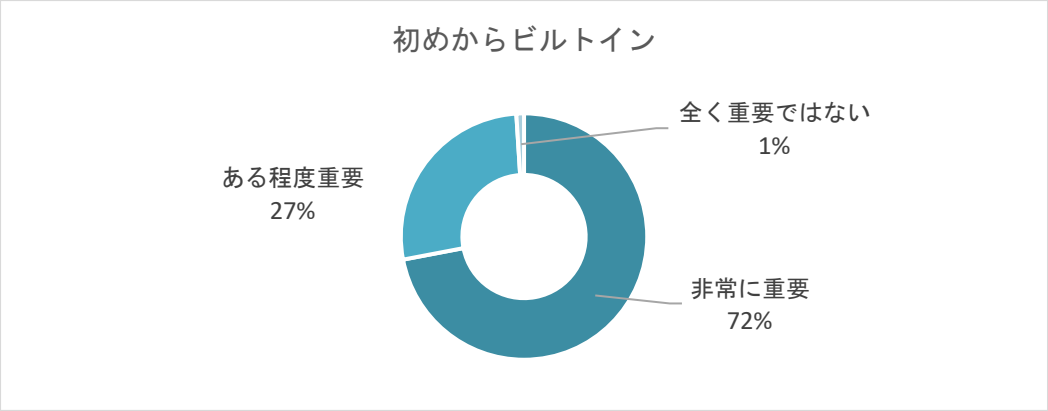
回答者の反応が最も強く表れたコンセプトは、ビルトインセキュリティと統合型データ保護の2つであった。「コンピューターを現在の、そして将来の予想される脅威から守るために、チップ、ファームウェア、OS を含め、コンピューターにセキュリティが最初から組み込まれていることは、

どの程度重要であると思いますか？」とたずねたところ、肯定的な回答が非常に多く、72%が「非常に重要」、27%が「ある程度重要」と答えた。「まったく重要ではない」と答えたのはわずか1%であった。データを詳しく見ると、医療機関や金融機関のITDMは、「非常に重要」と回答した割合がさらに高い（それぞれ84%と75%）結果となったことは注目に値する。統合型データ保護というコンセプトも同様に高い割合であった。「コンピューターのハードウェアにデータ暗号化機能が統合されていることは、どの程度重要であると思いますか？」との質問に対して、71%が「非常に重要」、29%が「ある程度重要」と答え、「重要ではない」と回答したのは0%であった。ビルトインセキュリティと統合型データ暗号化の詳細については、Figure 3 を参照のこと。

FIGURE 3

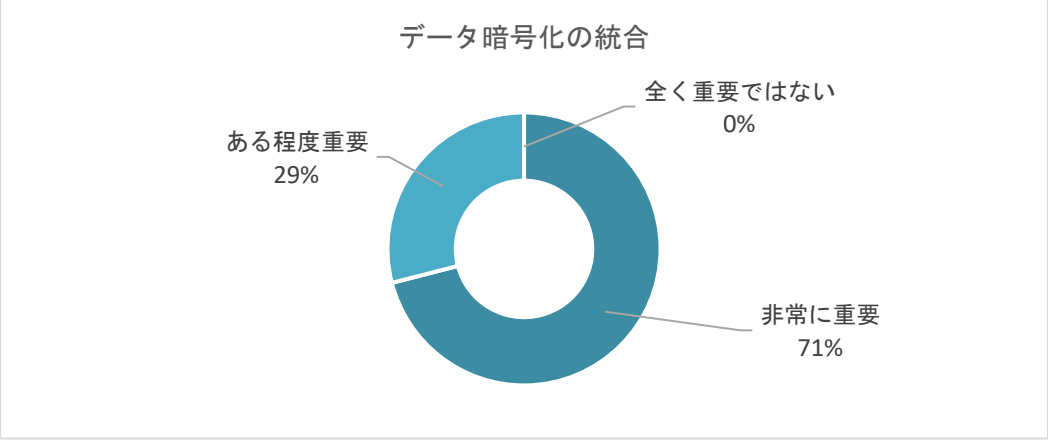
ビルトインセキュリティとデータ暗号化の統合の重要性

Q　コンピューターを現在の、そして将来の予想される脅威から守るために、チップ、ファームウェア、OSを含め、コンピューターにセキュリティが最初から組み込まれていることは、どの程度重要であると思いますか？



Source: IDC's Secure Endpoint Survey, n = 513

Q.　コンピューターのハードウェアにデータ暗号化機能が統合されていることは、どの程度重要であると思いますか？



Source: IDC's Secure Endpoint Survey, n = 513

最初からセキュリティが組み込まれたハードウェアは重要であり、データ暗号化の統合は重要な要件であるが、セキュリティの専門家は、どのようなセキュリティチェーンであっても、ウィーケストリンク（weakest link）は一般的にエンドユーザー自身であることを承知している。だからこそ、ユーザー認証は非常に重要であり、テクノロジーベンダーは認証の在り方を進化させるために努力してきたのである。しかし、残念ながら、この分野では多くの企業が後れを取っていることが IDC の調査で明らかになっている。

肯定回答が多かった項目としては、回答者の 68%が自社で複雑なパスワードを要求していると回答し、63%が 2 要素認証を使用していると回答していることが IDC の調査で明らかになった。肯定回答が比較的少ない項目としては、SSO（Single Sign-On：シングルサインオン）テクノロジーを使用しているのはわずか 23%で、生体認証セキュリティ（指や顔の認証など）を使用しているのはわずか 20%であった。回答者の中で、生体認証の方がパスワードよりもはるかに安全であると答えたのは 56%、いくらか安全であると答えたのは 35%、同程度であると答えたのは 9%であったが、安全性が低いと答えた回答者はいなかった（0%）ことには注目すべきである。

最近導入されている重要な新しい認証テクノロジーはパスキーである。パスキーは、パスワードよりもはるかに安全なソリューションを提供する 1 つのキーペアを活用したデジタル認証である。このテクノロジーは新しいため、自社で使用していると答えた回答者はわずか 14%にすぎないが、賢明な ITDM は、現在このテクノロジーに注目しているはずである。ユーザー認証の使用状況については、Figure 4 を参照のこと。

FIGURE 4

ユーザー認証方法

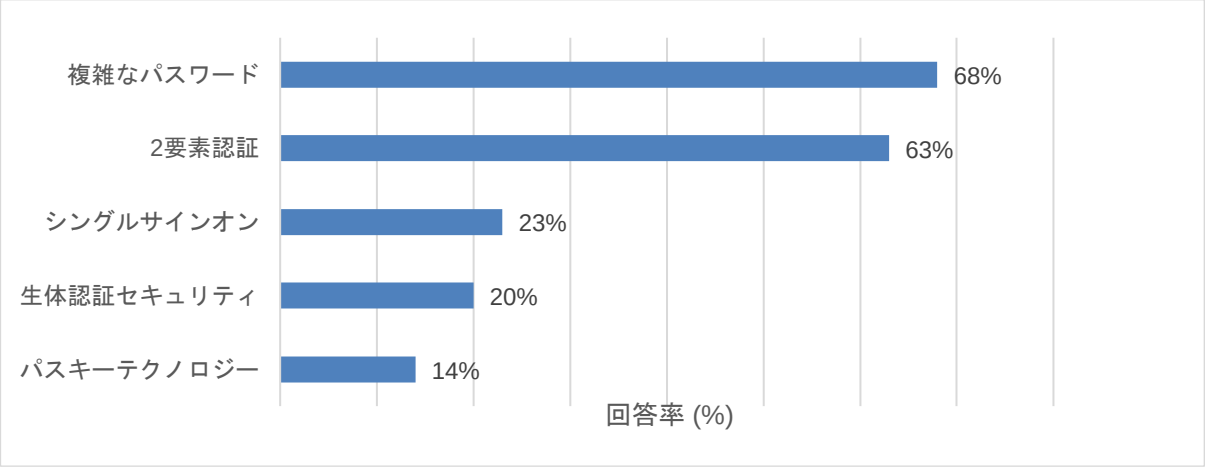
Q1. 貴社では、従業員がコンピューターにログインする際に、複雑なパスワードを使用することを義務づけていますか？

Q2. 貴社では、指スキャンなどの生体認証セキュリティ対策に対応したコンピューターを導入していますか？

Q3. 貴社では、パスキーテクノロジーを使用するベネフィットについて検討を始めましたか？

Q4. 貴社では 2 要素認証を義務づけていますか？

Q5. 貴社では SSO 機能を活用していますか？（はい／いいえ）



Note: データは、「はい」と答えた割合を示している

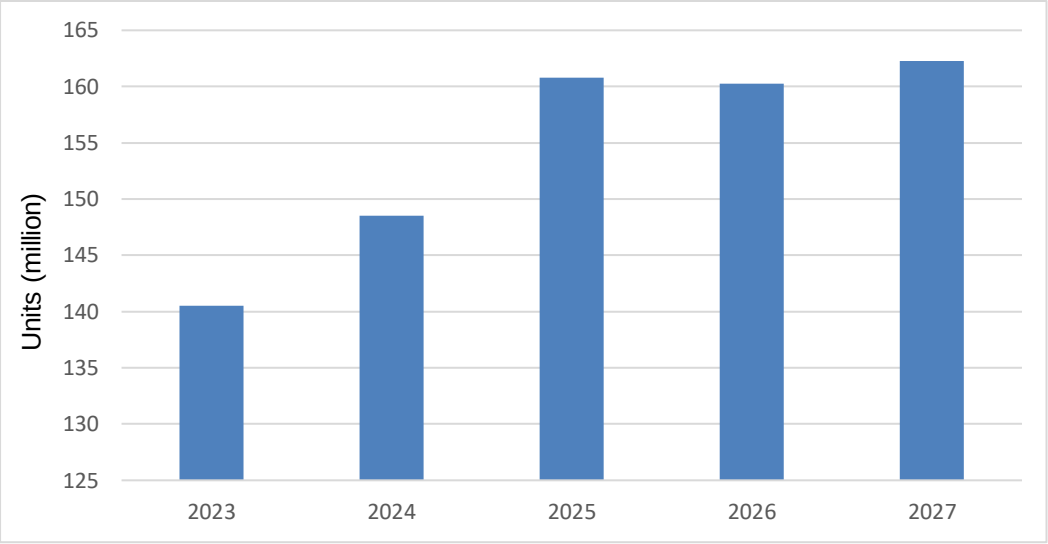
Source: IDC's Secure Endpoint Survey, n=513

回答者の中で、複雑なパスワード（32%）や2要素認証（37%）という基本的な認証プロトコルの実装にさえ失敗している割合が驚くほど高い。**取り組む価値があるベストプラクティス**は、企業全体で一貫した認証形式を確実に導入することである。このベースラインを確立した後に、強力なマスター認証プロトコルと組み合わせた SSO 機能を検討し始めるべきである。最後に、次回のハードウェア更新を行う際には、最高レベルの認証、すなわち生体認証セキュリティとパスキーテクノロジーをサポートできるコンピューターに関して、より詳しく検討すべきである。生体認証とパスキーの実現は、従業員が迅速かつ安全にコンピューターにログインし、そこからすぐにアプリケーションや Web サイトにアクセスできる未来を示している。

このセクションを締めくくる最後のポイントとして、「次回のハードウェア更新」に言及する。多くの企業は、老朽化し、交換が必要なコンピューターを稼働させている。つい最近のことと思える 2020 年に、新規のエンドポイントとしてかなりの割合で購入していたとしても、それらのコンピューターはもう間もなく 4 年が経過することになる。その間に、ハードウェアセキュリティは、現場の脅威に合わせて進化し続けてきた。おそらく同様に重要なことであるが、これらの製品のほとんどは、リモートワークやハイブリッドワークへの移行が広まる前に出荷されているため、現在では従業員にとって日常的な Web 会議アプリやコラボレーションアプリに不可欠な高品質のカメラ、マイク、スピーカーが搭載されていない。IDC の調査データ「*Personal Computing Device Tracker*」は、数年間出荷台数が伸び悩んだ後の数年間はこのカテゴリーが成長すると予測している。なお、法人向け出荷台数は、消費者以外、つまり企業によって購入された出荷台数を指す。IDC の消費者向け／法人向けコンピューターの予測については、Figure 5 を参照のこと。

FIGURE 5

世界法人向けコンピューター市場 出荷台数予測、2023 年～2027 年



Source: IDC PCD Tracker, August 2023

企業は、市場における競争力を維持し、優秀な人材を確保し、維持するために、従業員のコンピューターニーズを継続的に再評価する必要がある。かつて IT 部門は、セキュリティと従業員の満足度の間でかなりの妥協を迫られていたが、現在は適切なベンダーが妥協のないソリューションの推進を支援してくれる。最後に、**もう一つのベストプラクティス**として、次のハードウェア導入時にゼロトラストアクセス原則の適用を検討すべきである。この戦略は、デバイスが企業のリソースにアクセスを試みるときは常に、認証されるまでそのデバイスを信頼すべきではないとい

う考えである。ゼロトラストでは、（チップから重要な IT およびセキュリティアプリケーションに至るまで最適な）デバイスのセキュリティ状態、接続ネットワーク（公衆 Wi-Fi とプライベートネットワークなど）、ユーザーID を認証する技術とプロセスを採用している。

Mac in the Enterprise の検討

現在、より多くの IT 部門が Mac をサポートしており、IDC の調査ではその主な理由を指摘している。インストールベースでさまざまなオペレーティングシステムを導入している回答者のうち、76%が「Mac は他のコンピューターよりも安全であると考えている」と答えている。また、今後 1 年以内にさらに Mac を導入する理由の 1 位は「Mac の方が安全であると思うから」（47%）で、次いで僅差で「導入や管理が簡単であるから」（36%）であった。

アップルは、ソフトウェアを通じて Apple シリコンにセキュリティを組み込むことで、セキュリティを高めつつ、優れたユーザーエクスペリエンスを提供することに注力している。その一例が、アップルのビルトイン生体認証機能、Touch ID である。Apple シリコンは Secure Enclave を備えており、Touch ID のデータを保護するため使用されているパスコードを暗号化して保護する。

Apple の顧客の Spotlight

「Apple 製品の本当に重要な特徴の一つは、プライバシーとセキュリティが製品そのものに実際に組み込まれていることです。それらの機能は後付けではないため、非常に高く評価している部分です」 – Linda Jojo、エグゼクティブバイスプレジデント兼チーフカスタマーズオフィサー、United Airlines

OS とブートシーケンスが侵害されるリスクに対処するため、Mac には Secure Boot と Signed System Volume が組み込まれている。Secure Boot は、起動時に macOS の暗号論的に認証されたバージョンのみから確実に起動するように設定され、Signed System Volume は、実行中の OS の完全性を保護している。また、アップルはソフトウェアのアップデート版のエンドツーエンドの配布とインストールを自動化し、安全性を確保することで、古いソフトウェアがサイバーリスクになることを最小限に抑えている。

従業員の生産性を高めるには、優れたサードパーティ製のソフトウェアが不可欠であるが、そのソフトウェアもマルウェアに感染していないことが必要である。アップルは、マルウェア対策として多層的なアプローチを採用している。アップルの Mac App Store では、マルウェア対策としてすべてのアプリをスキャンしている。Mac のソフトウェアは Web からもダウンロードできるため、アップルは開発者に対し、マルウェア対策としてスキャンも行っているアップルの公証サービスにアプリを提出するよう求めている。macOS に含まれるアップルの Gatekeeper は、公証をチェックし、署名されていないアプリの実行を防ぐ。さらに、アップルのマルウェア対策ツールである XProtect は、既知のマルウェアをブロックして削除する。

データは、企業にとって最も価値の高い資産であり、相応に保護されなければならない。チップで強化された FileVault 暗号化、アップルがサポートする VPN プロトコル、アップルのサービス（iMessage や iCloud など）におけるエンドツーエンドの暗号化を組み合わせることで、データは保存時、転送時、使用時に確実に保護される。

ソーシャルエンジニアリングは脅威行為者の熟練したスキルの一つであるため、エンドユーザーは、用心深く行動して、阻止しなければならない。重い責任ではあるが、アップルは Safari Fraudulent Website Warning でサポートしている。さらに、脅威行為者が認証情報を盗み出すことが多い中、アップルのパスキーサポートは、この場合もやはり有意義なエンドユーザーエクスペリエンスを犠牲にすることなく、企業が認証方法をモダナイズするプロセスを簡素化できる。

高いセキュリティは、しっかりとしたデバイス管理と連携している。そのため、アップルは MDM（Mobile Device Management）を備えたビルトイン管理フレームワークを含む、さまざまなデバイス管理を提供している。Apple Business Manager は、ゼロタッチ導入と MDM ソリューションへのリンクを可能にし、Endpoint Security APIs for Mac は、開発者が、セキュリティ上の脅威を監視、分析、

対応するためのソリューションを構築できるようにする。また、アップルは、最新の IdP（Identity Provider：アイデンティティプロバイダー）と連携するビルトイン SSO フレームワークと ID の統合も提供している。

最後の話題となるが、アップルは macOS と共に、ソフトウェアのメジャーおよびマイナーアップデートを含むこれらのセキュリティ機能を、企業や消費者といった顧客に追加費用なしで提供している。

課題と機会

常に進化し続ける脅威環境にもかかわらず、IT 部門は、より少ない費用、より少ない IT スタッフ、より少ないリソースでより多くの課題に取り組みという状況に直面している。すべての企業が直面する継続的なセキュリティリスクに対処するだけでなく、多くの IT 企業もまた、導入するハードウェア、ソフトウェア、サービスを通じて、従業員の生産性と満足度を目に見える形で向上させることを求められている。セキュリティの向上と従業員の生産性／満足度の向上という 2 つの課題を同時に達成することは、困難なことのように思えるかもしれない。しかし、これは IT 部門にとって重要な機会でもある。購入するハードウェア、ソフトウェア、サービス、購入先のベンダー、そしてハイブリッド化が進む従業員への導入方法を再評価する機会である。さらに、現在の企業がどのようにテクノロジーを購入し、使用しているかをより適切に反映するために、総所有コスト（TCO：Total Cost of Ownership）モデルを再計算する時期であることは明らかである。

結論

IT 部門にとって、セキュリティは最大の関心事であり、今後もそうあり続けるであろう。IT 予算は逼迫し、ハードウェアの大規模な更新が控えている今、今後どのベンダーに予算を投じるかを再検討することは理に適っている。認証やゼロタッチ導入に関するベストプラクティスの実践を検討し、こうした移行を実現できるハードウェアを購入すべきである。セキュリティと有益なユーザーエクスペリエンスの両方を実現するために、ビルトインセキュリティとデータ暗号化を組み込んだコンピューターを提供できる頼れるベンダーが存在するのであれば、生産性や従業員の満足度よりもセキュリティを優先してはならない。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com