ファームウェアアップデート のベストプラクティス

はじめに

ファームウェアのアップデートを計画的に行うことは、信頼性の高いサイバーセキュリティのために不可欠な要素ですが、多くの企業にとっては困難なことです。本レポートでは、IT部門とセキュリティ部門のリーダーを対象に、ファームウェアのアップデート管理に関する考え方と、ベストプラクティスに関するガイダンスを提供します。

多くの企業のITおよびセキュリティチームは、オペレーティングシステム（OS）やアプリケーションを常に最新の状態に保ち、既知の脆弱性を排除することが非常に重要であることを理解しています。しかし、ソフトウェアのパッチ適用やアップデートには多大なリソースが費やされる一方で、システムハードウェアの基本的な動作を支えるファームウェアについては、同様のプロセスや厳格さが適用されていないことが少なくありません。多くの場合、機器のファームウェアは全く更新されないか、せいぜい緊急時にしか更新されない状況であります。

“2022年までに、ファームウェアのアップグレード計画が実施されていない組織の70%が、ファームウェアの脆弱性のために侵害されるでしょう。”

- Gartner、”How To Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds,”、Tony Harvey、2019年7月3日
（注：Gartnerのサブスクリプションが必要となります）

しかしながら、ファームウェア層は、攻撃者の企業への攻撃のターゲットの一部となっており、企業は、ファームウェアのセキュリティを無視することで、大きな代償を払うことになります。最近のランサムウェアは、ダメージを与えるためにファームウェアを標的にするだけでなく、マルウェアは他にも認証情報を盗むためにファームウェアをターゲットにして持続性、ステルス性を高め、システムを再イメージングしても脅威を維持します。また、重要なインフラを使用不能にするために、ファームウェアが攻撃されるケースもあります。攻撃者が無防備なファームウェア層を継続的に狙っていることから、企業はもはやファームウェアの脆弱性に目をつぶることができないことは明らかです。

リサーチおよびアドバイザリー会社のTAG Cyberの CEO であり、元 AT&T の CISO である Edward Amoroso博士によれば、世界レベルのファームウェアアップデート管理プロセスを構築する必要性は、もはやオプションではないといいます：
「ファームウェアのアップデート管理は、かつては、脆弱性に対処するための組織の計画において、必要不可欠な要素であると考えられていました」と説明し、加えて「今では、成功するセキュリティプログラムの中心的な要素の一つに発展しています」と言っています。

ほとんどの CISO とセキュリティチームは、ファームウェアのセキュリティ衛生状態を改善したいと考えていますが、現実にはさまざまな課題があります。ファームウェアのアップデートには、時間がかかり、リスクがあり、システムの再起動やダウンタイムが必要になることもあります。組織には、アップデートを安全にテストしてロールアウトするためのツールがないかもしれないし、自分たちの環境にどのようなファームウェアがあるのか、そもそもアップデートが可能なのかどうかを知ることすらできないかもしれないのです。

「ソフトウェアへのパッチ適用は、それほど大変なことではなく、より安全なことです。しかし、ソフトウェアとハードウェアの更新の適切なバランスを見極める必要があります。また、Infosecチームと緊密に協力して、ファームウェアの運用ポリシーを確立し、伝える必要があります」。

- ジョニー氏、大手ハイテク企業のシステムアーキテクト

このホワイトペーパーでは、ファームウェアアップデート管理の現状と、業界がどのように進化しているかを検証します。そして、組織のリスクおよび脆弱性管理戦略にファームウェアを統合する、安全で信頼できる プロセスを構築するために、セキュリティ・リーダーが取ることのできる具体的なステップを提案します。

文中のハイパーリンクは英文のリンクとなっております、日本語をご希望される方はブラウザの翻訳機能等をご使用ください。

ファームウェアの脅威と脆弱性の状況

ファームウェアの脆弱性を管理するプロセスに入る前に、そもそもなぜファームウェア層が攻撃対象となるのかを理解しておく必要があります。多くの時間が必要とされる中で、IT およびセキュリティグループは、企業に最大の影響を 与える仕事を優先しなければならない。そのため、なぜファームウェアがセキュリティ分野で最も重要な領域の1つに急速に発展したのかを認識することが重要です。

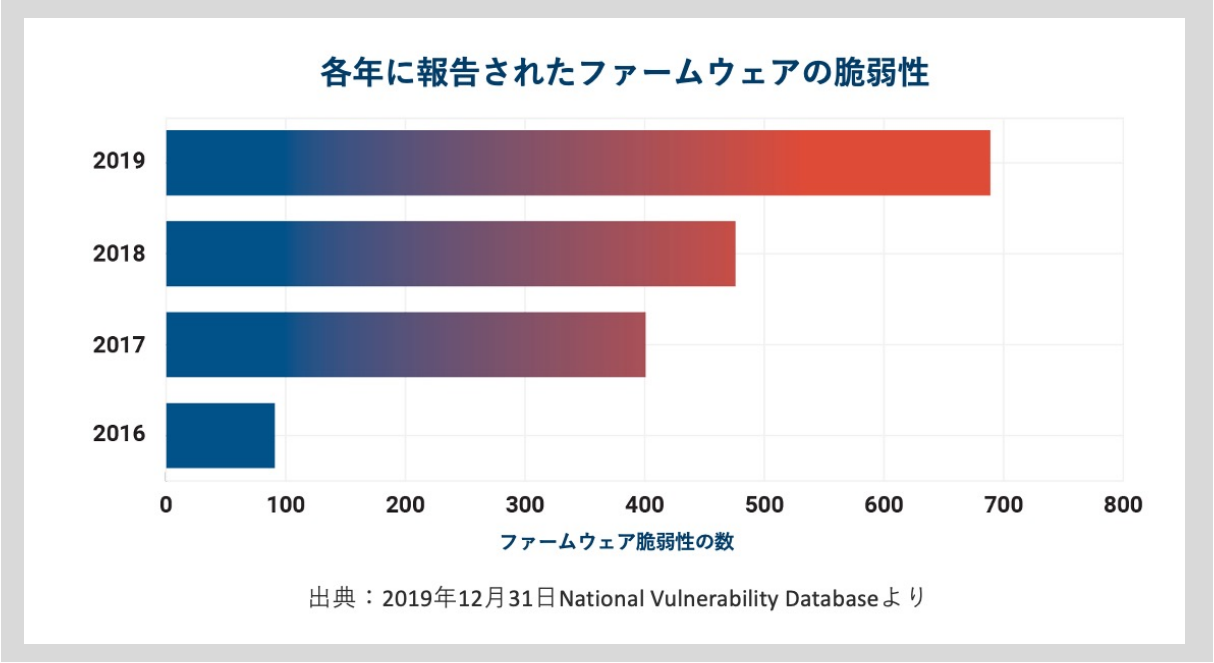
さまざまな要因がありますが、主な理由は3つに要約できます。

1. 確認されたファームウェアの脆弱性の数が増加していること。
2. 実際に確認されたファームウェアの脆弱性を狙った攻撃が増えていること。
3. これらの脆弱性が悪用されると、攻撃者は最高レベルの権限を与えられ、システムを制御することができます。攻撃者の動機やテクニックに関する追加情報は、当社のオンラインリソース「Anatomy of a Firmware Attack」に記載されています。

ファームウェアの脆弱性が急増

近年、ファームウェアの脆弱性の総数は急増しており、2016年以降の各年は、National Vulnerability Database (NVD)で追跡された脆弱性の総数でも年々増加の一途をたどっています。2019年は、これまでで最も多くの脆弱性が記録されたことに加え、2018年と比較して43%増加し、2016年からは7.5倍の増加となりました。

このような脆弱性の急増は、攻撃対象が急速に拡大していることを示すだけでなく、研究者と攻撃者の両方がファームウェアに注目するようになっていることを示しています。



出典：2019年12月31日National Vulnerability Databaseより

ファームウェアは実環境ですでに攻撃されています

このような機会と影響の組み合わせにより、実際にファームウェアを使用した攻撃が発生し、さらなる脆弱性が発見されています。最近のForrester社の調査では、“63%の企業が、ハードウェアまたはシリコンレベルのセキュリティの脆弱性が悪用されたことにより、過去12カ月以内にデータの漏洩または違反を経験している”という結果が出ています。同様に、エフセキュア社の分析によると、2019年上半期には、侵害されたファームウェアが3番目に多い感染ベクターであることがわかりました。

また、ファームウェアへの攻撃は数が増えている一方で、その手法は進化し、影響も変化しています。攻撃の内容は以下の通りです：

LoJaxは、ファームウェア構成の脆弱性を悪用してシステムのSPIフラッシュメモリにインストールするためにAPT-28によって使用されるUEFIルートキットです。 LoJaxは脅威システムの実態がファームウェア内に存在するため、Windowsの再インストールや、ハードドライブの交換などでは削除されません。

JungleSecは、セキュリティで保護されていないIPMI（Intelligent Platform Management Interface）コマンドを介して被害者のBMCに感染するランサムウェアです。 FBIは、ランサムウェアからの脅威への対応として、ファームウェアにパッチを適用するよう外部に促すアラートを公開しています。

ShadowHammerの場合は、正規ベンダーのASUS Live Updateユーティリティを介して配布され、数千台のAsusコンピューターにバックドアをインストールしました。その結果、バックドアにより、ハッカーはいつでも、誰にも知られることなく、被害者のコンピュータに自由にアクセスできるようになっていました。

APT-41によるスパイ活動とサイバー犯罪攻撃の波は、脆弱性を悪用し、CiscoおよびCitrixネットワークデバイスのファームウェア内にバックドアをインストールし、ROCKBOOT MBRベースのブートキットを使用してWindowsデバイスでの永続性を実現します。

ファームウェア攻撃は影響が大きい

攻撃者の視点から見ると、ファームウェアは、非常に価値の高い、戦略的なターゲットとなります。ファームウェアは攻撃者に、盗み出したり、身代金を要求したりできるデータへの深いレベルのアクセスを提供します。さらに、コンポーネントまたはデバイス全体を完全に無効にすることができます。また、ファームウェアは、企業に対する長期的な攻撃を実行するために、従来のセキュリティを弱体化させようとする攻撃者の企みを幇助します。そのモチベーションには具体的に以下のようなものがあります：

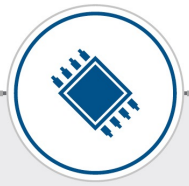
- 最高レベルの特権：ファームウェアは、オペレーティングシステムのカーネルの下にあります。ファームウェアを制御することで、攻撃者はカーネルを破壊し、デバイスの最高レベルの特権にエスカレートする可能性があります。

- 従来のセキュリティのバイパス：攻撃者は、システムの起動方法を制御するか、オペレーティングシステム自体にパッチを適用することで、オペレーティングシステムと仮想マシンのレイヤーで実行されるセキュリティ対策を回避できます。

- 永続性：ファームウェア内の悪意のあるコードは、当然、デバイスのハードウェアに関連付けられており、システムの完全な再イメージングを行っても攻撃者のコードを永続させる可能性があります。

- ステルス：侵害されたファームウェアにより、攻撃者は検出されずに重要な攻撃機能を実行することもできます。たとえば、攻撃者は、ホストベースのファイアウォールを回避するためのコマンドアンドコントロールチャネルとして、BMCおよびラップトップチップセットの帯域外管理機能を使用することが可能です。

- ダメージ：最後に、ファームウェアレイヤーへのアクセスにより、攻撃者はデバイスに決定的なダメージを与えることができます。攻撃者はファームウェア自体にダメージを与えることにより、デバイスを永続的に「ブリック（起動不可）」とすることも簡単に実現可能です。



ファームウェアベンダーの視点

ファームウェアレベルで実行されるマルウェアは持続的で、簡単には除去できません。洗練されたマルウェアは、ファームウェアを既知の正規バージョンにアップデートしようとする試みを妨害し、阻止することができます。ファームウェアレベルのマルウェアは、PCや同一ネットワーク上の他のデバイスに完全にアクセスすることができ、OSのカーネルにマルウェアを注入することができます。Hacking TeamのUEFI BIOSルートキットで実証されているように、一度マルウェアがインストールされると、ユーザーがハードディスクを再フォーマット（または新しいハードディスクへの入れ替え）して、システムをOSから再インストールしても、マルウェアは残ります。プライベートネットワーク上で感染したPCは、ハッカーが機密データを流出させたり、そのネットワーク上の他のPCやデバイスに感染させたりするのに使われます。ネットワークのどこか1箇所にでも脆弱性があると、ネットワーク全体が脆弱となります。

PC製品のメーカーは、脆弱性の公表を受けて、脆弱性を緩和するためのパッチを含むファームウェアのアップデートをお客様に提供しています。ファームウェアの脆弱性を最も効果的に回避するためには、セキュリティパッチが公開されたらすぐにインストールすることが重要です。また、PCを構成するハードウェアのソフトウェアや、プリンタなど同じネットワークに接続されている他の機器のファームウェアをアップデートすることも同様に重要です。

非常に多くの影響力の大きい脆弱性と現実の脅威が組み合わさることで、企業がリスクに晒されるため、積極的な管理が必要となります 。

ファームウェアアップデート プログラムの開発

脆弱性と資産の管理は、あらゆるセキュリティ・プログラムの基盤となる要素です。ファームウェアの重要性を考えれば、組織が、オペレーティング・システムに使用しているのと同 じレベルの管理ポリシーと頻度で、ファームウェアをアップデートすることは、理にかなっていると言えるでしょう。また、ファームウェアは、組織の全体的な脆弱性およびリスク管理プログラムの重要な構成要素として含まれるべきです。

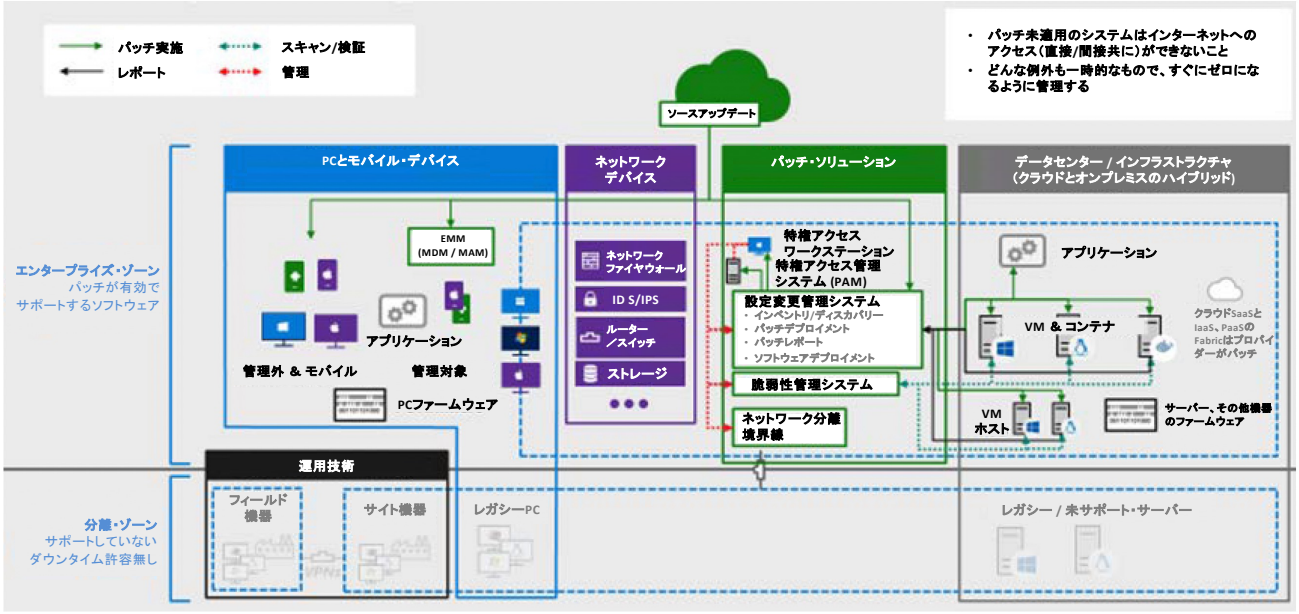
ファームウェアのパッチ、ファームウェアのアップデート、どっちをする？

“ ここで重要なことは、パッチとアップデートの違いを認識することです。’パッチ’ や ’パッチ・マネジメント’ という言葉は、既存のプログラムにコードを追加したり、その一部を変更したりする場合に使われますが、’アップデート’ は対象となるコードやプログラムを完全に置き換えることを指します。そのため、アプリケーションやOSはパッチを当てることが多く、ファームウェアはほとんどの場合アップデートされます。どちらの場合も、バグの修正や脆弱性の除去を目的とした新しいコードが提供されます。”

— Tim Lewis, CTO Insyde Software

現在進行中のNISTプロジェクト「Critical Cybersecurity Hygiene: Patching the Enterprise」では、ソフトウェアだけでなく、ファームウェアも最新の状態に保つことの重要性が強く訴えられています。このプロジェクトはまだ構築段階にありますが、現在のドキュメントでは、企業が様々なテクノロジーを最新の状態に保つための重要なステップが示されています。この文書では、PCおよびサーバのファームウェアとネットワークデバイスの両方を、常に最新の状態に保つ必要がある重要なコンポーネントとして挙げています。

NISTは今回の文書案で、ファームウェアの更新もサイバーハイジーンの必要かつ重要な要素とみなすことを提案しています。ファームウェアは、他のすべての技術やセキュリティ特性の基礎となるものであり、企業がオペレーティングシステムと同様の管理ポリシーと頻度でファームウェアを更新することは道理にかなっています。



セキュリティパッチリファレンスアーキテクチャ

出典：NIST、Critical Cybersecurity Hygiene：Patching the Enterprise

政府のコンピュータ・システムのセキュリティを確保するための包括的なフレームワークを規定しているFISMAも、同様に、基本的なセキュリティ管理の多くにおいて、ファームウェアを取り上げています。NISTのPlatform Firmware Resiliency Guidelines (SP 800-193)は、さらに進んでいて、攻撃に直面したときにデバイスの回復力を維持することができるファームウェアコンポーネントとセキュリティメカニズムの詳細な分析を提供しています。FISMAで義務付けられているファームウェア関連の問題にEclypsiumがどのように対処できるかについての詳細は、FISMAコンプライアンスのベストプラクティスとクイックリファレンスガイドを参照してください。

ファームウェアのアップデートプログラムを開発する上で、もうひとつ参考になるのが、ファームウェアとドライバーのメンテナンスに関する社内戦略を公開しているインテルITです。このドキュメント「**Developing a Gold Standard for Driver and Firmware Maintenance**」は、ファームウェアアップデートに対するインテルの完全なアプローチをカバーしています。この資料は、特に企業にとって重要なものです。なぜなら、ファームウェアのセキュリティの重要性を独自に理解している大企業が、ファームウェアのメンテナンスの課題にどのように取り組んでいるかについて、現実的な視点を提供しているからです。

特に、インテルの文書では、インテルが利用可能なすべてのファームウェアアップデートをインストールするわけではないという事実が報告されています。インテルは、ユーザーやシステムへの混乱の可能性と比較して、各アップデートの重要性と価値を評価しています。インテルは、特に重要なセキュリティフィックスを含むアップデートを優先し、そのアップデートが 1）環境のバグに対処しているかどうか、2）必要な新機能を導入しているかどうか、3）オペレーティングシステムのアップグレードの前提条件であるかどうかを判断しています。

また、ガートナー社は、レポート "How to Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds "の中で、インフラストラクチャーやオペレーションのリーダー向けに、ファームウェアのアップデートに関するガイダンスを提供しています。このレポートによると "データセンターのインフラを担当するI&Oのリーダーは、次のことを行う必要があります。

- 最高情報セキュリティ責任者（CISO）と協力して、新しいファームウェア脅威の検出およびスキャニング・ツールに投資し、業界のコンソーシアムやこの分野の専門家と連携することで、ファームウェアおよびハードウェアの脅威を理解するスキルをチーム内で開発する。
- ファームウェア・アップグレード・ポリシーを、データ・センターの標準的な手順に組み込むことで、アップデートを定期的に行い、緊急時の対策を講じる。
- ネットワークの分離、ユーザー・アクセス・コントロール、ロギング、およびベンダーのセキュア・ファームウェア機能を使用することにより、ファームウェア・アップデートへのアクセスを確保する。
- クラウド・ベンダーとオンプレミス・ベンダーの両方が、ベンダーのマネジメント・チームと協力して、安全なファームウェア・アップデート・プログラムを持っていることを確認する。*

*Gartner「How To Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds」Tony Harvey、2019年7月3日。

ファームウェアの更新戦略を考える

組織は、これらの概念やその他の概念を、脆弱性管理のための既存のプロセスに組み込むべきです。詳細は組織によって異なりますが、チームは、ファームウェアのアップデートの優先順位を決定するために使用する基準に関する戦略とポリシーを定義するべきです。また、更新を行わない正当なビジネス上の理由となり得る条件を決定するべきです。主なトピックは以下の通りです:

チーム間のコミュニケーションの確立: ファームウェアのアップデートは、当然ながら様々なチームに影響を与えます。アップデートの決定と手順は、組織全体で調整されることが不可欠です。例えば、セキュリティチームは重大な脆弱性のためにアップデートを必要とするかもしれませんが、その実施はITチームに任されます。同様に、組織全体で適切な判断を下すためには、アップデートによるビジネスへの影響を特定し、関連するチームと経営陣に情報を提供する必要があります。

更新の影響の理解: 組織は、アップデートがユーザや、影響を受けるハードウェアに依存するアプリケーションやサービスに与える影響を理解する必要があります。チームは、段階的な導入計画を策定し、本格的な導入の前に代表的なシステムが十分にテストされるようにする必要があります。これにより、システムやサービスの全体的な可用性を許容範囲内に維持することができます。

テスト、ロールバック、および段階的展開: チームは、ターゲット・システムへの潜在的な悪影響を特定するために、広範な展開の前にファームウェアのアップデートをテストするための、適切なシステムとツールを用意します。また、問題が発生した場合には、ファームウェアのロールバックとリカバリーをサポートするツールが必要となります。段階的な展開を計画することで、組織は、 1）より重要なシステムに影響を与える前に影響の低いシステムで問題を特定し、 2）アップデートによって一時的に利用できなくなったリソースを、柔軟性の高いアプリケーションで確実に補うことができます。

ITおよびセキュリティツール: 統制とれた規律あるファームウェア・アップデート・ポリシーの目標を達成するために、企業は、様々なサポート技術力を必要となります。それは、現在、持っているかどうかは別にして、様々な技術的能力をサポートするものです。これには、重要なデバイスのファームウェアを、システムの UEFI レベルとコンポーネント・レベルの両方で、確実に可視化することが含まれます。

ベンダーの選定: 新しいハードウェアやベンダーを評価する際には、ファームウェア・アップデートの品質と管理性を重要な要件とすべきです。これには、ベンダーがどのようにファームウェア・アップデートをサポートしているか？、どのようなツールが提供されているか？、カプセル化はサポートされているか？、ファームウェア・アップデートは適切に署名され、アップデート・プロセスは安全か？、などを理解することも含まれます。

Linuxベンダーファームウェアサービス（LVFS）からの視点

Linux Vendor Firmware Serviceを設立したRichard Hughes氏は、ファームウェアアップデートの実践に熱心に取り組んでいます。彼は、強力な公開鍵/秘密鍵の暗号を使ってファームウェアに署名するなど、基本的な原則に従わないベンダーがあまりにも多いと感じています。ファームウェアのアップデートに失敗してデバイスを「ブリック」するようなことは絶対にあってはならないと、OEMやODMメーカーに忠告しています。問題の原因が、予期せぬハードマシンのパワーダウンであっても、アップデートの途中でユーザーが物理的にプラグを抜いてしまっても、あるいは「有効な」ファームウェアイメージを間違ったデバイスにフラッシュしてしまっても、です。ファームウェアアップデート作業の進捗状況を報告するなどの簡単なステップを踏むことで、ユーザーがアップデートがインストールされたと勘違いしてコンピューターを再起動するのを防ぐことができます。

理想的なシナリオでは、ファームウェアのアップデートは、オペレーティング・システムやその他の重要なソフトウェアに適用されるのと同じプロセスで行われます。しかし、現実の世界では、さまざまな課題のために、そうなっていないことが多い。

今日のファームウェアアップデートの状況は、過去10～20年のソフトウェアやOSの状況に似ています。OSの自動アップデートは、徐々に企業に受け入れられてきましたが、ソフトウェアのアップデートの品質や、問題が発生した場合にシームレスにロールバックできる能力について、企業が必要な信頼を得るには、何十年もかかりました。

OSベンダー、コンポーネントを設計するODM（Original Design Manufacturers）、完成品を販売するOEM（Original Equipment Manufacturers）、そしてオープンソースプロジェクトは、ファームウェアの管理・保守方法を近代化するために取り組んでいます。しかし、これらの取り組みは、一夜にして実現するものではなく、最終的には、リスクを嫌うIT組織が信頼できる、強力で実証済みの実績を提供しなければなりません。

これらの課題のいくつかは、テクノロジー全体のサプライチェーンの一部として、ファームウェアがどのように開発され、提供されるかに起因する、業界全体の問題に根ざしている。他の課題は、ダウンタイムの可能性、テスト作業、ロールバックのシナリオなど、企業内の 運用上の課題とより密接に結びついている。しかし、ファームウェアには、いくつかのユニークな課題がある一方で、企業がこれらの課題に対処するために、業界ではさまざまな取り組みが行われています。

業界の課題

機能していないファームウェアのエコシステム

OSベンダーが、信頼性の高いOSアップデートのプロセスを開発し、企業のITチームとの信頼関係を築くまでには、20年以上の歳月が必要でした。それと比較して、ファームウェアの状況はさらに困難なものです。OSの市場は、Windows、Linux、Appleを中心に少数のコアベンダーとプロジェクトによって支配されています。これに対して、ファームウェアやファームウェアのアップデートは、数多くのソースから提供されています。ファームウェアは、コンポーネントベンダーによって開発される場合もあれば、サードパーティに委託される場合もあります。このファームウェアはOEMベンダーに渡され、そのまま使用されることもあれば、ニーズに応じて変更されることもあります。そのため、誰がファームウェアに責任を持っているのか、お客様がどこでアップデートを求めればよいのか、必ずしも明確ではない状況に陥る可能性があります。

ソリューションと推奨事項：企業は、コンポーネントや周辺機器に含まれるファームウェアを含め、デバイスに含まれるすべてのファームウェアに注意を払う必要があります。理想的には、チームは、ファームウェアのアップデートについて、上流のコンポーネント・ベンダーに注意を払うべきです。しかしながら実際には、これはより洗練された、十分な人員を擁する組織にとってのみ現実的なことかもしれません。また、購入を決定する際には、ベンダーが提供するファームウェ ア管理の質を強く考慮すべきです。さらに、すべてのファームウェアを自動的に監視し、アップデートが利用可能になったときに検出するツールへの投資を検討することも必要な事項です。

長期間放置されるファームウェアの問題

継続的に開発・更新が行われるソフトウェアとは異なり、ファームウェアの開発は断続的で、更新の間隔が数年に及ぶこともあります。その結果、ファームウェアのアップデートは、提供されるまでに時間がかかり、オリジナルのファームウェア開発者によるサポートも受けられないことが多いこともあります。多くのベンダーは、特定のインシデントや問題が発生しない限り、ファームウェアのアップデートを一切行わないことを想像してみてください。一方、攻撃者は、特定のデバイスが大量に出回るようになるまで、脆弱性の発見に注力しないかもしれません。そうなると、守備側は、ファームウェア層の可視化ができない、あるいは監視できないため、問題の存在を検知するのに長い時間を要することになります。何年も経ってから問題が発見された場合でも、メーカーが解決策を講じることになります。OEMはしばしばサプライヤーを変更するため、問題が発見された時点で、当初のファームウェア開発者がソリューションを提供できなくなっていることはよくあることで、さらに遅れが生じてしまいます。例えば、ThinkPwn UEFIの脆弱性の背景にある脆弱なファームウェアコードは、発見された時点ですでに2年前のものでした。同様に、Absolute社のLojackソフトウェアを不正に改変したバージョンは、悪意のあるコマンド＆コントロールドメインを含んでいることが判明するまで、何年もの間、フィールドに放置されていたのです。

ソリューションと推奨事項：企業は、強力なファームウェア管理機能と、下流のサプライヤーとの統合機能を備えたテクノロジー・ベンダーを選択すべきです。例えば、HP Support Assistant は、HP のデバイスに搭載されているコンポーネントのファームウェアを明確に把握することができ、また、アップデートがいつ利用可能になるかを知ることができます。組織は、ベンダーごとにファームウェアの可視性を個別に管理するのではなく、すべてのデバイスにおけるすべての企業のファームウェアの状態を追跡するツールを検討することが良い方策と言えます。

テクノロジーサプライチェーンにおける感染

テクノロジーOEMメーカーは、自社のファームウェアをサポートするために、複雑なサプライチェーンを構築しなければならない場合があります。これには、サードパーティからライセンスを受けたファームウェアや、ODMパートナーのコンポーネントに含まれるファームウェアが含まれます。攻撃者は、このサプライチェーンの中でファームウェアを侵害し、最終顧客に届けられる前にデバイスを感染させることができてしまいます。さらに悪いことに、アップデートのインフラ自体が危険にさらされる可能性もあります。例えば、ShadowHammerのケースでは、攻撃者はASUSに侵入し、ASUSの証明書で適切に署名され、公式のASUS Live Updateユーティリティーを通じて配信されたマルウェアをユーザーに届けることができてしまいました。

ソリューションと推奨事項：サプライチェーン攻撃に対する防御策は、サプライチェーンのどこで、どのように侵害されたかによって異なります。企業は、新たに入手したデバイスをスキャンして、ファームウェアがベンダーから提供されている既知の有効なファームウェアと一致していることを確認し、既知のファームウェア・インプラントの存在を検出する必要があります。新たに未知のファームウェアが埋め込まれた場合、あるいは、ベンダーからの有効なアッ プデートが侵害された場合、組織は、ファームウェアの異常な動作を監視する機能が必要となります。そのためには、多くの場合、このタスクに特化したセキュリティツールが必要となります。

ファームウェアの署名の未検証

最近の業界およびEclypsiumの調査によると、デバイスの中には、ファームウェアコードを更新または実行する前に、ファームウェアが適切に署名されているかどうかを検証しないコンポーネントが存在することが珍しくありません。つまり、これらのコンポーネントには、デバイスに読み込まれたファームウェアが本物であり、信頼すべきものであることを検証する手段がないということです。このため、攻撃者は、悪意のある、あるいは脆弱なファームウェア・イメージを挿入し、コンポーネントとしては、これを盲目的に信頼して実行するになってしまいます。

ソリューションと推奨事項：ファームウェアおよびアップデートは、強力な公開鍵/秘密鍵暗号方式を用いて、関連する技術提供者によって署名されなければなりません。また、秘密鍵は機器本体に保存してはならず、シリコン上で検証するか、共有フラッシュへの書き込みを担当するMCUで検証する必要があります。上記の要件はOEM/ODMの責任ですが、組織は、新しい技術の購入を検討する際には、デバイスやそのコンポーネントのファームウェアをスキャンし、脆弱なファームウェアや署名のないファームウェアがないかどうかを確認する必要があります。また、すべてのコンポーネントに署名されたファームウェアのみを使用するベンダーを選ぶべきです。

共通の脆弱性の分類法の欠如

ファームウェアを全体的な脆弱性管理プログラムに統合している組織は、ソフトウェアで利用可能 なツールや基準の多くが、ファームウェアでは利用できないことに気づくことが多くあります。脆弱性スキャンが、ファームウェアの脆弱性にまで及ぶことはほとんどありません。同じ問題が、業界自体を悩ませています。例えば、ファームウェアの脆弱性は、CVEに含まれていますが、開発者やセキュリティチームが脆弱性の根本的な弱点を理解するために使用するCWE（Common Weakness Enumeration）コードが割り当てられていないことが多いのです。インテルをはじめとする業界では、CWEの概念をハードウェアの問題にまで広げようとする動きが活発化しています。CWEコードは、開発者やセキュリティチームが脆弱性の根本的な弱点を理解するために使用します。標準化が進めば、研究者が研究成果を発表する際に役立
つだけでなく、組織が自社の環境における脆弱性の影響を理解し、情報に基づいて優先順位を決定するのにも役立ちます。

ソリューションと推奨事項：このような業界レベルの大きな課題には、当然ながら多くの組織やベンダーの協力が必要です。そのため、このような変化は、個々の企業の範疇を超えていると思われます。しかし、企業は、インテルのような業界への取り組みを支持し、他のベンダーに対して、ソフトウェアに使用されている既存の分類法にハードウェアおよびソフトウェアの脆弱性を含めるよう働きかけるべきです。

業界の課題

ファームウェアとハードウェアインベントリの欠如

ファームウェアやハードウェアの可視化は、組織にとって最も基本的な課題の一つです。どのようなファームウェアがデバイスに搭載されているのか、そのファームウェアに脆弱性が含まれているのか、アップデートがあるのか、といった基本的な情報がチームには不足していることが多くの場合あります。この問題は、ハードウェアの更新サイクルが段階的に行われ、複数の異なるハードウェアプラットフォームが使用されている組織であるほど、非常に大きくなります。

ソリューションと推奨事項：組織のファームウェアを検査し、インベントリを作成する能力は、優れたファームウェア管理のための前提条件となります。ファームウェアの可視性が高いメーカーもありますが、デバイスの種類、ベンダー、基盤となるコンポーネントが多様であるため、企業内のすべてのファームウェアを追跡することは、ほとんど不可能といえます。環境内のデバイスを集中的に、定期的にスキャンすることで、どのデバイスをアップデートする必要があるかを一貫して知ることができます。

難しい更新プロセス

従来、ファームウェアのアップデートは、ソフトウェアのアップデートに比べて、ITチームやセキュリティチームの手作業による作業が多く必要でした。そのため、アップデートに対する障壁が高くなり、結果的に無防備な攻撃対象となってしまう。さらに、ファームウェアのアップデートには、組織内の異なる機能別チーム間の調整が必要になることが多い。前述したように、セキュリティチームは重要な脆弱性に基づいてアップデートを提案するが、実際にアップデートを適用するプロセスはITチームが担当することがある。一方で、ファームウェアのアップデート時には、PCR0が変更されることでBitLockerの回復キーの入力を求められるなど、他の複雑な問題が発生する可能性があります。オペレーティングシステムやOEMの中には、アップデート中にBitLockerを一時停止するオプションを提供しているものもありますが、すべてではありません。

ソリューションと推奨事項：ファームウェアのカプセル化により、企業がオペレーティングシステムやソフトウェアのメンテナンスに使用するのと同じモデルに沿った、ファームウェアアップデートの自動化されたアプローチが可能になります。どのコンポーネントがカプセル化によってアップデート可能で、どのコンポーネントがより手動のアプローチを必要とするかを理解するためには、組織はデバイスを可視化する必要があります。いずれの場合でも、チームは、ファームウェアのアップデートをテストして、アップデートが広範囲に展開される前に、潜在的な問題を発見する準備をしなければならない。組織は、複数のファームウェア・アップデートをカプセル化するツールや機能を認識し、 それらをファームウェア管理戦略に統合し始めるべきである。また、ベンダーの選択プロセスにおいて、ファームウェアのカプセル化が可能であるかどうかを 検討するとよいだろう。最後に、ベンダーを評価する際には、アップデート中にBitLockerを一時停止するオプションを検討するとよいだろう。どのようなアップデートプロセスが利用できるかにかかわらず、組織は、ファームウェアに関連する多くの機能チーム間の明確なコミュニケーションと調整を確立する手順を確立する必要がある。

潜在的な悪影響

ファームウェアのアップデートに関して、企業が最も懸念していることの1つが、ファームウェアアップデート時の失敗によるリスクの可能性です。「ブリック」（デバイスを完全に使用不能にすること）を恐れるあまり、極端な状況を除いては、ファームウェアのアップデートを行わない企業もあります。幸いなことに、ファームウェアの自動ロールバックと手動ロールバックの両方のテストとサポートが強化されたことにより、ファームウェアのアップデートは、10年前、15年前に比べてはるかに安全になりました。特に、Intel、HP Enterprise、Dell、Lenovoなどの大手企業テクノロジーベンダーは、アップデートが失敗した場合に、既知の良好な状態のファームウェアに自動的にロールバックするツールの開発、提供をしています。具体的には、DellはBIOSリカバリーツールを提供し、HP EnterpriseはSmart Update Technologyの一部として自動ロールバック機能を備えています。

しかし、ファームウェアは、デバイスの動作温度を上げてしまったり、パフォーマンスに影響を与えたりするなど、簡単には認識できないような微妙な影響をデバイスに与える場合があります。また、アップデートによってデバイスの設定に影響を与え、セキュリティ機能やデバイスのセキュアブート機構を誤って無効にしてしまう可能性もあります。

ソリューションと推奨事項：多くのベンダーは、自動および手動のファームウェア・ロールバックの機能を大幅に向上させているが、多くのITチームは、これらの機能の向上を認識していない。チームは、これらの機能についてベンダーに質問し、調達の判断材料にするべきである。企業は、ファームウェアのアップデートを適切にテストし、アップデートのロールアウトを段階的に行い、問題が検出された場合にはロールバックとリカバリーのオプションをサポートするためのプロセスを構築し、ツールを開発する必要がある。同時に、組織は、ファームウェアのロールアウトをテストし、コントロールするための独自のプロセスを開発しなければならない。チームは、アップデートされたデバイスをスキャンして、セキュアブートやその他のセキュリ ティ設定がアップデート中に無効化されていないことを確認するツールを持つべきである。テストと手動によるロールバックのオプションも特に重要です。チームは、自動化されたロールバック機能をテストし、自動化された方法が失敗した場合に、既知の良好な状態にロールバックするためのバックアップ計画を持つ必要があります。

デバイスのダウンタイム

ファームウェアの管理における継続的な課題の一つは、アップデートの際にデバイスの再起動が必要になることです。つまり、たとえ最良の状況であっても、ファームウェアのアップデートには一定のダウンタイムが必要となるのです。この問題は、重要なアプリケーションをサポートするサーバーや、仮想化やコンテナ化された環境でホストされているさまざまな資産をアップデートする場合には、さらに深刻になります。さらに、短時間でもデバイスを停止させることに抵抗のあるITチームに、アップデートのプロセスを実行、または承認してもらう必要があるかもしれません。

ソリューションと推奨事項：ある程度のダウンタイムは避けられませんが、企業は、ファームウェア・アップデートのテスト、アップデートのスケジューリング、段階的なロールアウト・プロセスを通じて、少なくともその影響を最小限に抑えることができます。ターゲット・システムのテスト・バージョンに対して、ファームウェア・アップデートとロールバック・プロシージャをテストすることで、ITチームは、アップデートを適用する前に、実際に予想されるリソースのダウンタイムと、最悪のケースのダウンタイムを確実に知ることができます。この情報をもとに、アップデート・チームは、影響を受けるチームとコミュニケーションをとり、組織への影響を最小限に抑えるために適切なアップデート・ウィンドウを選択することができます。段階的なロールアウト・プランは、弾力性のあるアプリケーションやサービスをサポートするサーバを更新する際に特に有効です。インフラの更新を段階的に行うことで、アプリケーションの可用性を維持しながら、ハードウェアの更新を行うことができます。さらに、インテルのホワイトペーパーで紹介されているようなシステムの開発を検討することもできます。このシステムでは、IT部門を含むさまざまな機能チームからの意見を取り入れて、ファームウェアに対する標準的なアプローチを確立しています。

ベストプラクティスと推奨事項

1. ファームウェアアップデートに関する組織的な戦略と方針の確立

インテルのホワイトペーパーで確立されたものと同様の原則で、ファームウェアの更新に関するクロスファンクショナルなポリシーを策定します。その目的は、インテルの具体的なポリシーを再現することではなく、ファームウェアをいつ更新すべきかについて、合意された条件を確立することにあります。これらの条件は、アップデートしないことのリスク、新機能の必要性、ダウンタイムの潜在的なコストなどの要因を考慮し、アップデート・プロセスを適切に計画するものです。

- すべての関連チームおよび技術的な利害関係者からの賛同を得る。
- 重要なセキュリティ問題に必要な緊急アップデートのプロセスを確立する。
- ハードウェアおよびファームウェアの脆弱性に優先順位をつける際、CVSSスコアおよびリスクベースの脆弱性データを活用する。
- 定期的なアップデートについては、セキュリティへの影響、機能への影響、ダウンタイムのリスクなどに基づいて、アップデートを導入すべきかどうかを判断する基準を設ける。
- アップデートの決定を支援するために、ファームウェアを含めたリスクアセスメントを確立する。例えば、特定の脆弱性に関連する攻撃ベクターは何か？デバイスはそれらのベクターにさらされる可能性があるか？など。

2. ファームウェアの可視性を確立する

ファームウェアの可視化は、さまざまな方法で実現することができます。様々なコンポーネントのファームウェアのアップデートがいつ可能かを特定するという点で、プラットフォーム・ベンダーの機能を確認します。さらに、デバイスをスキャンして、使用されているファームウェア、その脆弱性、および利用可能なアップデートを特定することができるクロスプラットフォームのアプローチを検討します。これらの要件のいくつかを満たすためには、より多くのセキュリティ・ツールが必要になるかもしれません。

- UEFI、BIOS、統合されたコンポーネント、および周辺機器に対する可視性の確保。
- ラップトップ、サーバ、ネットワークインフラなど、サポートされているすべてのデバイスとプラットフォームの確実なカバー。
- 新たに発見された脆弱性を特定、追跡、管理する方法の導入。これには、セキュリティベンダーとの連携やオープンソースインテリジェンス（OSINT）へのアクセスなどを含む。
- ノートPC、サーバ、ネットワーク機器のファームウェアに存在する既知の脆弱性の定期的なスキャン。
- 設置デバイスのアップデートが利用可能かどうかの検出。
- ファームウェアのバージョン情報の可視性の維持。
- 現在インストールされているバージョンとターゲットバージョンのファームウェアの間で、中間的なアップデートが必要かどうかを確認する。
- ファームウェアアップデートの前後で、ファームウェアのコンフィギュレーションの可視性を維持する（例：USBは無効化されているか？SecureBootの状態はどうなっているか？SGXは有効か無効か？BIOSはパスワードで保護されているか）。
- 外部に接続されたデバイス（リムーバブルUSBドライブなど）をチェックし、ファームウェアのアップデートに互換性の問題がないかの確認。
- ベンダーのリソースからファームウェアを収集して監視し、安定性の問題やサプライチェーン攻撃の際にファームウェアが無効になっていないかの確認。

3. テスト、ロールアウト、ロールバックに必要なツールとスキルの開発

ファームウェアのテストと導入には、プロセスとツールの両方への投資が必要です。スタッフはトレーニングを受ける必要があり、テストはアップデートされるデバイスのタイプに応じてカスタマイズする必要があります。

- 様々なコンポーネントのファームウェアのアップデートに必要なプロセスの評価。
- どのコンポーネントをカプセル化してアップデートできるか、手動プロセスやその他の方法でアップデートできるかの判断。
- ファームウェアのアップデートに問題がないかを適切にテストするために、チームに適切なツールとリファレンス・システムの準備。
- ITスタッフやセキュリティ・スタッフなどの賛同者による初期テストを行い、段階的なロールアウト・プログラムの確立。サーバー・ファームやローカル・クラウドの資産のダウンタイムによる影響を最小限に抑えるためのアップデートの段階的な実施。大規模なデバイス群へのロールアウトを完了する前に、小規模なグループや価値の低い資産へのロールアウトの段階的な実施と追加テストの実施。
- 様々なベンダーの自動ロールバック・リカバリー機能をすべてテスト。
- 必要に応じて、問題無いことを確認済みのバージョンに手動でロールバックするためのツールとプロセスの開発。
- ファームウェアのロールバック対策が施されている機器に注意。ベンダーによっては、攻撃者が脆弱な初期バージョンのファームウェアにロールバックするのを防ぐために、初期バージョンのファームウェアへのダウングレードを禁止している。これは、保護レイヤを提供する一方で、ファームウェアの更新が悪影響を及ぼす場合に、デバイスを良好な状態に戻すことができないことを意味する場合がある。チームは、アップデートを決定する際に、このトレードオフを考慮に入れる必要がある。
- ファームウェアのバージョンが大きく変わると（例：バージョン1.xから6.xへ）、副作用が生じたり、システムが壊れたりする可能性があるため、注意が必要。
- アップデート後、ファームウェアが期待通りのバージョンに正常にアップグレードされているかどうかの確認。
- 構成を分析し、ファームウェアのアップデートによって、アップデート後に機密性の高い構成設定が変更されていないことの確認。
- ファームウェアアップデートの重要性と、アップデートプロセスに何を期待すべきかについて、エンドユーザーへの教育。

「私のサーバーを購入する際の判断基準は、セキュリティと、ハードウェアやファームウェアのアップデートを自動化するための最適な機能を備えているかどうかです」
— Alex, Fortune 500企業のパッチ管理、システムエンジニア

4. ハードウェア購入時にファームウェアサポートを優先

PC業界は分断されているため、ベンダーがファームウェアのセキュリティをどのように優先するかについては、大きなばらつきがあります。強力なセキュリティ対策は容易ではなく、ベンダーによっては、コストやオーバーヘッドを削減するために、優れたセキュリティを回避することもあります。しかし、ハードウェア・コストの小さな削減は、デバイスでサポートされていないファームウェアに手動で対処するために組織が満たさなければならない人手の必要性に比べて、しばしば矮小化されます。

- プラットフォームの評価の一環として、ファームウェアの更新プロセスを含める。
- 確立されたベンダーにとって重要な機能として、強力なファームウェアアップデート機能を要求。

結論

ファームウェアのアップデートは大変な作業ですが、企業は、過去にも同じような課題を克服してきたという事実に自信を持って対応すべきです。多くの点で、ファームウェアは、過去 20 年間にソフトウェア、およびOS ベンダーが経験したのと同じ成長の痛みを経験しています。適切な戦略、ツール、およびプロセスを構築し、ファームウェアの管理を優先するベンダーを選択することによって、企業は、ファームウェアのセキュリティへの確実な道を築くことができるのです。

単純な事実として、ファームウェアが企業の標的となる層が増えているため、組織は、セキュリ ティをより高めるための全体的なアプローチの一部として、ファームウェアのアップデートを含める必要があります。パッチマネジメントの基本的な目標の多くは、ファームウェアにも適用されますが、ファームウェアには、組織が準備しなければならないいくつかのユニークな課題があります。いくつかのベンダーは、ファームウェアのアップデート(およびロールバック)をより自動化するための努力をしていますが、その機能は、ベンダーによって大きく異なります。また、デバイスの中には、ファームウェアに依存するさまざまなコンポーネントが存在するため、問題はさらに複雑化しており、多くの組織にとっては、自分の環境にどのようなファームウェアが存在するのかを知ることさえ困難になっているのが実情ではないでしょうか。

これを補うためには、組織は、全体的なファームウェア戦略を策定するとともに、ファームウェアの更新というユニークな要件に合わせた新しいスキル、プロセス、ツールを開発する必要があります。他の多くのセキュリティ分野と同様に、可視性を確立することは、重要な要件です。チームは、組織のすべての重要なデバイスにおいて、どのようなファームウェアが使用されているかを、それらのデバイスの中にある多くのファームウェア依存のコンポーネントを含めて、 確認できる必要があります。チームは、ファームウェアのアップデートがいつ利用可能かを知る必要があり、また、いつアップデートを適用すべきかを判断するための基準を確立する必要もあるのです。

次に、ファームウェアをアップデートするために利用できるさまざまなメカニズムを知っておく必要があります。すべてのコンポーネントをカバーするためには、チームは複数のアップデート戦略をサポートする必要があり、これはアップデートに必要な時間と労力に影響を与える可能性があるのです。最後に、アップデートに関連する問題を検出するためには、ファームウェアのアップデートをテストし、段階的に展開するためのプロセスを確立する能力も必要となります。また、必要に応じてファームウェアをロールバックするプロセスも必要です。

当然のことながら、すべての組織は組織毎に独特な部分を持ち、それぞれの課題を持っています。ファームウェアアップデートプログラムの構築や、企業のファームウェアを一般的にモニターする方法については、Eclypsiumチーム(jp-info@eclypsium.com)までお気軽にお問い合わせください。

御礼

Eclypsiumは、本レポートにご協力いただいたCriteo社、Insyde Software社、Linux Foundation社、TAG Cyber社、Phoenix Technologies社のほか、匿名でご協力をいただいた数名の寄稿者とレビュアーの皆様に深く感謝いたします。

ECLYPSIUMについて

Eclypsiumは、業界をリードするエンタープライズファームウェア保護プラットフォームであり、ラップトップ、サーバー、およびネットワークデバイスをファームウェア攻撃から保護するための新しいセキュリティレイヤーを提供します。 Eclypsiumプラットフォームは、エンタープライズラップトップ、サーバー、およびネットワークデバイスのすべての主要コンポーネントで実行されているファームウェアを完全に可視化します。直感的に、ファームウェアにインプラントやバックドアがあるかどうか、既知の脅威に対して脆弱であるかどうか、または古くて更新が必要かどうかがわかります。脆弱性の重大度に関する専門家のガイダンスと最新のファームウェアアップデートへのリンクが提供されるため、脅威を軽減して資産を保護できます。Eclypsiumがファームウェアのセキュリティの向上にどのように役立つか、詳しい製品情報に関するお問い合わせについては、 jp-info@eclypsium.comまでお気軽にお問い合わせください。