ファームウェアセキュリティを確保するための評価ガイド

セキュリティ責任者は、要求事項を丹念にチェックし、組織として追うべきコンプライアンスについて共有しなくてはなりません。最近、NIST 800-53 Rev. 5、PCI DSS、FedRAMP、NIST 800-171、セキュリティ成熟度モデル(CMMC: Cybersecurity Maturity Model Certification)などのコンプライアンス規格で、ファームウェアやハードウェアが紹介されていることに気付いたかもしれません。しかし、これは何を意味し、何を探せばよいのでしょうか。

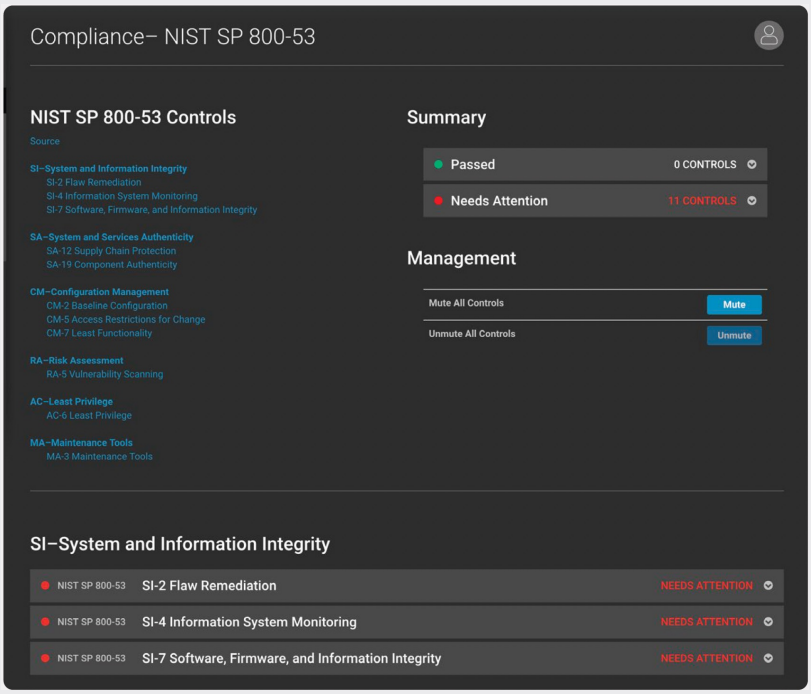
ファームウェアとハードウェアには、ソフトウェアと同じように多くのバグや脆弱性が存在します。リスクマネジメントのプロセスは、これらのレベルにまで及ぶべきです。これまでは、デバイスの多くのコンポーネントを列挙したり、ファームウェアの脆弱性を検査したり、不正な変更をチェックしたりするためのツールが特殊であったため、これらの実施が困難でした。ほとんどの企業は、ファームウェアの専門家チームを編成する余裕がないにもかかわらず、攻撃者はこのギャップを利用し続けている。セキュリティ責任者は、このようなギャップを特定し、攻撃される前に組織が解決できるよう支援することが必要です。

新しいツールが利用できるようになった今、セキュリティ責任者は、組織が、ファームウェアとハー ドウェアにおいて、オペレーティングシステムやアプリケーションと同レベルのコンプライアンス規律をどのように達成しているのかをすぐに確認しなくてはなりません。本ガイドは、NIST 800-53 Rev. 5に基づく監査時の質問の例と、組織がコンプライアンスの証明を行う方法について説明しています。

フレームワーク: 800-53 Rev.5	監査の質問	質問に対する確認すべき内容
CM-8 コンポーネント・インベントリ	各デバイスについて、どのコンポーネントが含まれていますか？ 重要機器に使用されているコンポーネントのメーカー、モデル、バージョンは？	組織の各部門またはチームからのデバイスおよび内部コンポーネント（CPU、BIOS、ストレージメディア、追加デバイスなど）のベンダー、モデル、バージョンを含む記録の確認。
CM-2 ベースラインコンフィグ	重要な機器に使用されているファームウェアのバージョンと構成オプションは？	ベースラインのシステム結果／レポートを調査し、ベースラインの一部であるバージョン、整合性、および構成設定を確認する。 不必要な機能は無効にし、デバイスのセキュリティ機能は有効／実行にしておく必要あり。この設定を最後に更新したのはいつか？
SI-2 欠陥の修復	各機器、コンポーネントについて、ファームウェアは ファームウェアは最新ですか？ そのモデル／バージョンには既知の脆弱性がありますか？	集めたバージョンをメーカーのウェブサイト、各機器／コンポーネントのCVEと比較する。 最新のファームウェアアップデートはいつ行われたか？
IR-4 インシデント・ハンドリング	どのようなプレイブック、ツール、あるいは能力が、侵害されたシステムのファームウェアをチェックするか？ チームは、ファームウェアの問題をトレーニングあるいは調査したか？	ファームウェアレベルの侵害を調査するためのプレイブック、トレーニング、または同様の文書の確保。 侵害されたシステムを調査するためのプレイブック、トレーニング、または同様の文書の確保。
RA-5 脆弱性スキャン	脆弱性スキャン機能は、ファームウェアの脆弱性を発見することができますか？	CPU、ME、TPM、BMC、ネットワークアプライアンスなどの脆弱性をスキャンした結果確認。これらのチェックは、最新の脆弱性を含むように定期的に更新されていることを確認する。
SI-2 フラウエイ・リメディエーション SI-4 情報システムの監視	ファームウェアの脆弱性やアップデートはどのように管理されていますか？ ファームウェア／ハードウェアの変更は監視によって検知されますか？	文書化されたリスク管理プロセスには、デバイスのファームウェア／ハードウェアの脆弱性が含まれていることの確認。 最新ではないデバイスには、不適切な正当性がないか。
MA-3 メンテナンスツール	ファームウェアを管理するために使用が承認されているメンテナンスツールは何ですか？	承認されたツールとそのバージョンの一覧を確認する。
SI-7 ソフトウェア、ファームウェア、及び情報の完全性	承認されていないファームウェアの変更または侵害の指標を検出するために、どのようなチェックが行われていますか？	デバイススキャンレポートには、ファームウェア の整合性と変更の検出状況が記載されていることの確認。
SR-9 耐タンパー性と 検知	脆弱なコンポーネントや不正なコンポーネントをどのようにして検出するのか？	ファームウェアの完全性と期待されるハードウェアをチェックするメカニズムの結果を確認する。 これらのチェックは、新しいコンポーネントや検出方法を含めるために定期的に更新されていること。

ツールは、デューデリジェンス（資産管理）の検証と、組織内でのコントロールの実施の両方において、大きな違いをもたらします。組織をコンプライアンスに適合させるためには、各エンドポイントにスキャンツールを導入することで、デバイスの詳細情報を一箇所に集めて分析することができます。その結果、インベントリが明確になり、脆弱性が特定され、改善策の優先順位が付けられ、脅威を炙り出すことに成功します。

また、質問に答えることで、企業がコンプライアンスを実現するために必要な次のステップがすぐにわかります。例えば、特定のネットワークカードやチップセットに重大な問題やバックドアが見つかった場合、組織は影響を受けるすべてのデバイスを見つけることができるでしょうか？OS やアプリケーションのアップデートを管理している場合、同じプロセスで BIOS やその他のコンポーネントのファームウェアも管理できるのか？ファームウェアレベルの改ざんや偽造を発見するためのチェックは行われているのか？これにより、セキュリティ管理者は今後の道筋を立て、コンプライアンスが満たされていることを確認することができます。



Eclypsiumは、企業全体でコンポーネントレベルのインベントリ、リスク管理、および脅威の検知を可能にします。発見された情報は、ファームウェアやハードウェアに関連するNIST Special Publicationsに自動的にマッピングされます。この情報は、環境における関連するコントロールの証拠となります。

Eclypsiumは、デバイスレベルの可視化、リスク管理、および高度な脅威の検知と防止を実現します。
詳細は jp-info@eclypsium.com までお問い合わせください。

エクリプシウムについて

米国オレゴン州ポートランドに本社を置くEclypsiumは デバイスの基盤に対する脅威を阻止することに特化した技術と専門知識の比類のない組み合わせを結集したスタートアップ・ベンダーです。2017年に設立された同社は、現在約60人以上の従業員を擁し、Fortune 50の金融サービス、データセンター事業者、政府などの顧客から信頼を得ています。政府機関のお客様のニーズをサポートするために、Eclypsiumは、ワシントンDC地域の専門家チームと、信頼できるパートナーのネットワークを結んでおります。Andreessen-Horowitz、Madrona Venture Group、Intel Capital、Ubiquity Venturesなどの一流の投資家の支援を得て、Eclypsiumは飛躍的な成長を続けています。2020年、Eclypsiumは、すべてのデバイスのファームウェアとハードウェアの基盤を守るというビジョンを実現し続けるために、さらに1,300万円の資金を調達しました。