HPE aruba networking

ビジネスホワイトペーパー

AI搭載のセキュリティファースト ネットワークによるNISTコンプライアンス

HPE Aruba Networkingで NISTコンプライアンスを推進

HPE GreenLake

目次

サイバーセキュリティとリスク管理のためのNISTフレームワーク

米国商務省の一部門であるアメリカ国立標準技術研究所（NIST）は、規制機関や企業が採用できる技術標準やガイドラインに関する推奨事項を公表しています。これらをグループにまとめたものはフレームワークと呼ばれます。

NISTフレームワークは、サイバーセキュリティとプライバシーに関する米国内、国際間、および業界固有のさまざまな規制の基盤となっているので、一部の公共機関や民間企業にとってNISTコンプライアンスが必須です。NISTガイドラインは、FedRAMP、連邦情報セキュリティマネジメント法（FISMA）、健康保険の携行性と責任に関する法律（HIPAA）といった法律や、Comply to Connect（C2C）のようなプログラムに組み込まれています。NIST標準はまた、ISO標準の要件や、カリフォルニア州消費者プライバシー法（CCPA）、EU一般データ保護規則（GDPR）といった法規にも対応付けられます。規制の対象ではない組織の間でも、NISTフレームワークをベストプラクティスとして自発的に採用する動きが広がっています[1]。

NISTの最も一般的な文書としては、次のものがあります。

- **NISTサイバーセキュリティフレームワーク（CSF）** ― 組織がビジネス要因に基づいてサイバーセキュリティリスクを管理するために使用できる標準、ガイドライン、手法[2]。
- **NIST SP 800-53: 情報システムおよび組織のためのセキュリティおよびプライバシー管理** ― 運用、アセット、人員をさまざま脅威やリスクから保護するための、ITシステム向けのセキュリティおよびプライバシー管理のガイドライン[3]。
- **NIST 800-207: ゼロトラストアーキテクチャー** ― 静的なネットワーク境界防御ではなく、ユーザー、アセット、リソースに焦点を絞ったサイバーセキュリティ戦略の定義と一般的な展開モデル[4]。なお、2021年5月に米国政府は、ゼロトラスト実装への基本的ステップとして、米国の連邦機関にNIST SP 800-207への準拠を義務付けた大統領令を発令しています[5]。

NISTコンプライアンスの課題

ゼロトラストのテクノロジーや手法を初めて導入する場合でも、業界や規制の要件の拡大に対応するため機能を追加する場合でも、NISTベストプラクティスへのコンプライアンスは、組織にとって困難な場合があります。

複数の領域にわたる要件 ― NIST標準に基づくコンプライアンスフレームワークは、多くの場合に組織内の複数のテクノロジー領域にまたがり、エッジからクラウドまでの手順やインフラストラクチャに影響を与えます。

機能の断片化 ― NISTフレームワークへの準拠に必要な機能は、時間とともに進化し、複数のテクノロジーソリューションにまたがることが多いため、ポイント製品のばらばらな採用につながることがあります。このセキュリティに対するつぎはぎのアプローチは、アーキテクチャーと運用の複雑さを増大させるだけでなく、組織をセキュリティギャップ、ポリシーと適用の不一致、潜在的なサイバーセキュリティリスクにさらすことになります。

チームのコラボレーション ― コンプライアンス要件を満たすイノベーションを成功させるには、多くの場合、ネットワークチームとセキュリティチームが協力して共通の目標と目的を追求し、ますます蔓延する高度化した攻撃から組織を守りながら、優れたエクスペリエンスを提供する必要があります。

[1]「General Perspectives（一般的観点）」、アメリカ国立標準技術研究所、https://www.nist.gov/cyberframework/general-perspectives、2021年12月。

[2]「Framework for Improving Critical Infrastructure Cybersecurity（重要なインフラサイバーセキュリティを改善するためのフレームワーク）」、バージョン1.1。アメリカ国立標準技術研究所、https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf、2018年4月。

[3]「Joint Task Force（ジョイントタスクフォース）」。「Security and Privacy Controls for Information Systems and Organizations（情報システムおよび組織のためのセキュリティおよびプライバシー管理）」、NIST Special Publication 800-53。アメリカ国立標準技術研究所、https://doi.org/10.6028/NIST.SP.800-53r5、2020年9月。

[4] Rose, S.、Borchert, O.、Mitchell, S.、Connelly, S.、「Zero Trust Architecture（ゼロトラストアーキテクチャー）」、NIST Special Publication 800-207。アメリカ国立標準技術研究所、https://doi.org/10.6028/NIST.SP.800-207、2020年8月。

[5] Biden, Jr., J.、「Executive Order on Improving the Nation's Cybersecurity（国家のサイバーセキュリティ向上に関する大統領令）」、ホワイトハウス、https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/、2021年5月。

地域や業界のサイバーセキュリティおよびデータプライバシー要件に違反すると、罰金やその他の罰則が科されることがあります。

NISTサイバーセキュリティベストプラクティスの採用のためのAI搭載のセキュリティファースト ネットワーク

HPE Aruba Networkingが提供するAI搭載のセキュリティファースト ネットワークを使えば、コンプライアンスを推進できます。ゼロトラストを基盤として構築されたHPE Aruba Networkingが提供するAI搭載のセキュリティファースト ネットワーキングソリューションは、ネットワーキングチームとセキュリティチームに共通の基盤を提供し、サイバーセキュリティ保護を犠牲にすることなく、独自のエクスペリエンスと革新的なビジネス成果を推進します。

HPE Aruba Networkingが提供するAI搭載のセキュリティファースト ネットワークは、組織がネットワークをセキュリティソリューションとして使用可能にすることで、サイバーセキュリティの標準および規制への準拠を容易にします。ネットワークは、単一のプラットフォームでより高度な可視性と洞察、一元的なポリシー管理、データ保護、脅威防御、アクセス制御を提供できるようになりました。こうした組み込みゼロトラストセキュリティ機能を使えば、ネットワーク自体が重要な防衛線となり、セキュリティ、データプライバシー、リスク管理の要件の充足に貢献するとともに、ばらばらな複数のツールのために複雑さが増加したり、既存のインフラストラクチャの完全な置き換えによって大きなコストや業務の中断が発生したりするおそれもなくなります。

AIを活用したネットワーキングは、組織の人的なパワーも倍増します。これは、規制の枠組みが拡大し、人材の不足が拡大し、サイバー脅威が増加する中で、重要な要素となります。HPE Aruba Networkingのセキュリティ優先のAI活用ネットワーキングにより、チームは手作業の削減、可視性と異常検出の向上、監視と診断の強化といったインテリジェントな自動化の恩恵を受けることができ、これらすべてによって組織が不必要なリスクにさらされないように図ることができます。

HPE Aruba Networkingによる主要なNIST要件の達成

NISTガイドラインは、サイバーセキュリティとビジネス回復力を高めることを目的としたさまざまな機能と要件にわたっています。ガイドラインには、サイバーセキュリティ戦略およびガバナンス、インシデントの検出と対応、インフラストラクチャおよびアプリケーションセキュリティに関する要件が含まれます。

サイバーセキュリティ

NISTのサイバーセキュリティフレームワークは、サイバーセキュリティリスクの管理と軽減に対する構造化されたアプローチを記述しています。NISTガイダンスには、進化するサイバーセキュリティリスクに対処するために運用できる機能的成果が含まれています[6]。

HPE Aruba Networkingソリューションは、以下のようなNISTサイバーセキュリティフレームワークをサポートします。

- 識別
- 保護
- 検出
- 対応
- リカバリ

ゼロトラストの原理

ゼロトラストセキュリティの原理は、最新のセキュリティアーキテクチャーに関する主要な留意事項の1つです。NIST Special Publication 800-207には、ゼロトラストアーキテクチャーの実装のためのさまざまな要件が記述されています[7]。ゼロトラストは境界ベースのセキュリティモデルからのパラダイムシフトであり、主体（ユーザーやデバイス）の物理的位置やネットワーク上の位置だけに基づく暗黙の信頼は存在しないと仮定します。その代わりに、主体には、その職務や機能の遂行に必要なリソースだけを対象とした最小権限のアクセスが許可されます。

[6]「Framework for Improving Critical Infrastructure Cybersecurity（重要なインフラストラクチャのサイバーセキュリティを高めるフレームワーク）」、バージョン1.1。アメリカ国立標準技術研究所、https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf、2018年4月。

[7] Rose, S.、Borchert, O.、Mitchell, S.、Connelly, S.、「Zero Trust Architecture（ゼロトラストアーキテクチャー）」、NIST Special Publication 800-207。アメリカ国立標準技術研究所、https://doi.org/10.6028/NIST.SP.800-207、2020年8月。

単一のベンダー、ソリューションが1つの組織に必要となるすべてのサイバー保護機能を提供することは不可能ですが、ゼロトラストセキュリティの組み込み型基盤を提供するネットワークから始めることで、重要なデジタルエントリーポイントでの保護を強化しながら、NISTガイドラインへの準拠が必要となるツールの数を軽減できます。

HPE Aruba Networking Edge Services Platform (ESP) は、エッジからクラウドまでのゼロトラストセキュリティの原理に基づいて設計されており、運用を簡素化しながら保護を強化することができます。HPE Aruba Networkingは、包括的な可視化、認証と承認、最小権限のアクセス制御といった重要なゼロトラスト機能に加えて、企業ネットワーク内外でのセキュリティエコシステム全体と連携した継続的な監視とポリシー適用も可能にします。

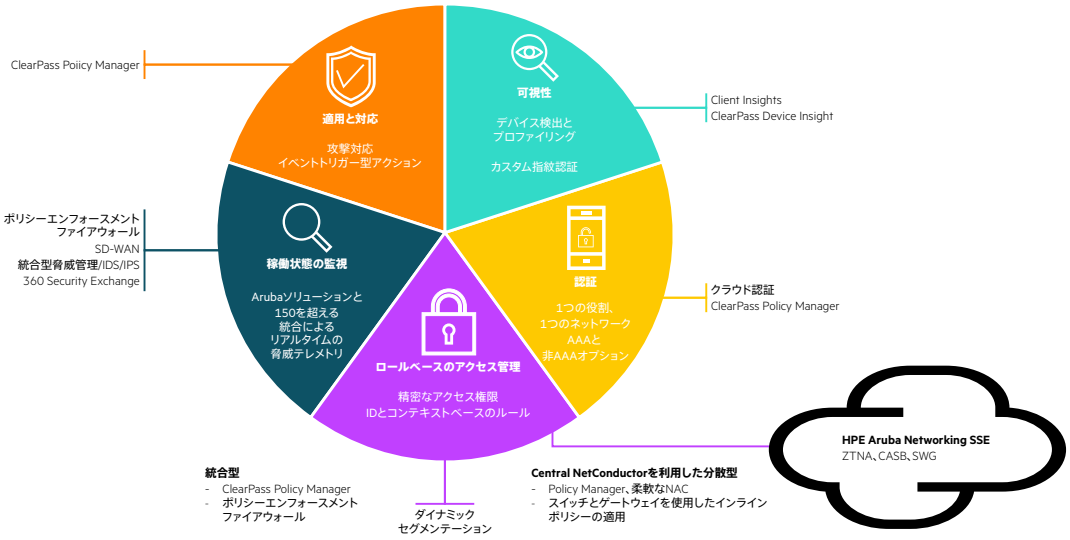

図1. HPE Aruba Networkingが提供する、ゼロトラストセキュリティの基盤

可視性: ユーザー、デバイス、アプリケーション

ゼロトラストセキュリティは、接続されているユーザーとデバイスを可視化することから始まります。クラウドベースのネットワーク管理ソリューション**HPE Aruba Networking Central**には、**Client Insights**が提供するAI搭載の可視化機能とプロファイリング機能が含まれています。Client Insightsは、アクセスポイント、スイッチ、ゲートウェイ、さらにはクライアントのネイティブなインフラストラクチャテレメトリを直接分析しますが、物理コレクターや物理エージェントをインストールする必要はありません。Client Insightsは、有線および無線インフラストラクチャ全体にわたるさまざまなIoTデバイスのセットを含む、ネットワークに接続するさまざまなエンドポイントにわたって、既知クライアントの最大99%のプロファイリング精度と、未知のクライアントの割合が5%未満の、正確なAI/MLデバイスプロファイリングを提供します[8]。クラウドベースのHPE Aruba Networking Centralやサードパーティのネットワークデバイスで管理されていない環境の場合、**HPE Aruba Networking ClearPass Device Insight**はクライアントのMLベースの識別とプロファイリングを提供します。

IoTを含むネットワーク接続デバイスで最大99%のプロファイリング精度を獲得

HPE Aruba Networking Centralの**アプリケーションの識別と分類**機能を使えば、組織内で使用されているアプリケーションに対する可視性が得られ、カスタム定義のリスクプロファイルに従ってアプリケーションを定義し、分類することもできます。ゲートウェイを使えば、リスクプロファイルに基づいてゲートウェイでトラフィックを監視することで、ネットワークチームとセキュリティチームが共通に使用できる、ネットワークのパフォーマンスと保護の最適化のための手法が得られます。

[8]「Aruba Helps Network Teams Overcome Scarce Staff Resources with First AIOps Solution that Combines Network and Security Insights for Improved IT Efficiency (Arubaは、ネットワークとセキュリティに関するインサイトを組み合わせることでIT効率を改善する初めてのAIOpsソリューションにより、ネットワークチームのスタッフリソースの不足解消に貢献)」、https://www.businesswire.com/news/home/20220726005426/en/Aruba-Helps-Network-Teams-Overcome-Scarce-Staff-Resources-with-First-AIOps-Solution-that-Combines-Network-and-Security-Insights-for-Improved-IT-Efficiency、「AI-powered Network Infrastructure: The answer to IT Efficiency (AI搭載のネットワークインフラストラクチャ：ITの効率性への答え)」、https://www.arubanetworks.com/resource/ai-powered-network-infrastructure-the-answer-to-it-efficiency/

認証と承認

ユーザー、デバイスの識別とプロファイリングが完了した後は、それらがネットワークに接続するたびにIDを認証します。**HPE Aruba Networking ClearPass**を使えば、Active Directoryなどのさまざまなソースに対してユーザーとデバイスを認証できます。正確なアクセス権限を可能にする豊富なポリシーエンジンを使用して、ClearPassはどのユーザー、またどのデバイスがどのリソースにアクセス可能かを制御します。ポリシーは、マルチベンダー環境内であっても、有線、無線、ワイドエリアネットワーク全体でユーザーとデバイスをシームレスに追跡します。**ClearPass OnGuard**を使えばエンドポイントポスチャの評価も可能なので、構成とコンプライアンスのガイドラインが満たされていることを確認し、準拠していないデバイスをネットワークから排除することができます。

HPE Aruba Networking Centralで管理されるネットワークでは、クラウドネイティブなネットワークアクセス制御（NAC）ソリューション**Cloud Auth**によって、MACアドレスベースの認証、またGoogle Workspace™やAzure Active Directoryなどの一般的なクラウドIDストアとの統合を通じて、エンドユーザーとクライアントデバイスをスムーズにオンボーディングし、適切なレベルのネットワークアクセスの自動割り当てが可能になります。

IDベースのアクセス

HPE Aruba Networkingの**ダイナミックセグメンテーション**は、IDおよび関連するアクセス許可に基づいてネットワークトラフィックを分離し、エッジからクラウドまでのアプリケーションとデータへの最小特権アクセスを適用します。ダイナミックセグメンテーションは統合型と分散型の適用モデルを複数サポートしており、IT部門は環境のニーズに応じてどちらか1つ、また両方のモデルを使用できます。一元的な適用は、HPE Aruba Networkingのネットワークインフラストラクチャに組み込まれている完全なアプリケーションファイアウォールである**ポリシーエンフォースメントファイアウォール**（PEF）によって提供されます。

ゲートウェイおよびスイッチングインフラストラクチャ内部でのインラインの分散型適用のために、**HPE Aruba Networking Central NetConductor**は、EVPN/VXLANなどの広く採用されているテクノロジーを使用して、分散型ネットワークオーバーレイを作成します。このフルスタックのソリューションには、シンプルなビジネスロジックインターフェイスによるグローバルポリシー管理およびネットワーク構成のためのクラウドネイティブセキュリティサービスと、ネットワークチームとセキュリティチームが、ゼロトラストアーキテクチャーの基盤であるきめ細かいセキュリティポリシーを定義して適用しながら、最適なネットワークパフォーマンスを実現するために使用できる直観的なワークフローが含まれています。

HPE Aruba Networking Central NetConductorは、きめ細かいL2 ～ L7アクセスポリシーをシンプルに定義し、ネットワーク全体に容易に伝播するための共通のツールセットを、ネットワークチームとセキュリティチームに提供します。**HPE Aruba Networking CX 6300および6400スイッチ**内部のステートフルなアプリケーション対応型ファイアウォール機能は、ビジネス目的に基づいてポリシーを適用することで、VLANやACLに関連する手動作業、不整合性、潜在的リスクを排除します。

組織は、**HPE Aruba Networking EdgeConnect SD-WAN**を使用して、組み込みのエンドツーエンドの次世代ファイアウォール機能（IDS/IPS、DDoS保護、企業全体のマイクロセグメント化が含まれる）により、WANとLANにまたがる一貫したセキュリティポリシーを適用することもできます。組み込みの次世代ファイアウォールサービスにより、組織はブランチ内の従来のファイアウォールとルーターを排除し、ブランチネットワークとセキュリティ機能を統合できます。

データセンター内では、**HPE Aruba Networking Fabric Composer**は、使いやすいポイントアンドクリックのユーザーインターフェイスでマイクロセグメンテーションプロセスを簡素化および自動化し、ゼロトラストセキュリティの実装を容易にします。**HPE Aruba Networking CX 10000スイッチ**は、分散型マイクロセグメンテーション、East-Westファイアウォール、暗号化、テレメトリサービスをすべてのポートにわたってインラインで提供し、重要なエンタープライズアプリケーション付近でのファイアウォールの追加が不要になります。

ハイブリッドユーザーとリモートユーザー、請負業者や派遣労働者などのサードパーティの場合、**HPE Aruba Networking SSEゼロトラストネットワークアクセス（ZTNA）**は、トラストブローカーを介して、単一のグローバルポリシーインターフェイスで定義済みのように、ユーザーが承認された特定のアプリケーションまたはマイクロセグメントのみにアクセスを制限します。継続的な監視により、ID、場所、デバイスの健全性の変化に基づいてポリシーが自動的に適応されるため、あらゆるアクセスイベントに対してゼロトラストの確実な適用が容易になります。

継続的監視、適用、対応

ネットワーク上のユーザーとデバイスの継続的な監視は、ゼロトラストセキュリティのもう1つのベストプラクティスです。HPE Aruba Networkingソリューションでは、**Aruba 360 Security Exchange**に含まれる150種類以上の最高水準のセキュリティソリューションとの統合により、複数のソースからリアルタイムの脅威テレメトリを入手して利用できます。ネットワークとセキュリティエコシステム全体との間の双方向通信により、ネットワークデータを利用して、ユーザーとデバイスの活動に対する可視性と制御性を得るだけでなく、投資の価値を高めることもできます。

リスク管理フレームワーク

NISTのリスク管理ガイダンスに含まれるNIST Special Publication 800-53は、情報を処理、保管、または伝送する組織やシステムのためのシステムと組織的制御を確立します[9]。制御は、適切なセキュリティおよびプライバシーリスク管理ポリシーの実装に関して組織をガイドするように設計されています[10]。要件は、インフラストラクチャのセキュリティに関するリスクを管理し、個人のプライバシーを保護するための、テクノロジー、運用、組織に関連する手段を対象としています[11]。

HPE Aruba Networkingは、リスク管理に関する次のようなNISTガイドラインを満たすために役立ちます。

- アウェアネスとトレーニング
- アクセス権と権限
- 事業継続性
- 構成管理
- インシデント処理
- セキュアソフトウェア開発
- サプライチェーンのセキュリティ
- システムおよびサービスの購入
- 脆弱性の報告と解決

セキュアソフトウェア開発

HPE Aruba Networkingは、セキュア開発プロセスを使用して、脆弱性を減らすとともに、ソリューションのコストと可用性を最適化します。**ソフトウェア開発ライフサイクルとセキュアソフトウェア開発フレームワーク**のベストプラクティスに従って製品を開発することにより、不要なリスクから組織を守ることができます。

- **要件分析 ー** セキュリティリスクを分析し、高レベルのセキュリティ要件を設定します。
- **定義 ー** セキュリティ脅威のモデリングと分析を行います。
- **設計 ー** 要件ごとにセキュリティリスクを軽減するための設計を行います。オープンソースとサードパーティのコンポーネントを特定します。
- **コーディング ー** セキュアなコンポーネントを再利用します。セキュアなコーディングプラクティスを実装します。コードをレビューし、静的なコード分析ツールを使用します。
- **テスト ー** セキュアな構成を実現するために、セキュリティスキャン、入力検証、侵入テストを実行してセキュリティ機能をテストします。
- **展開 ー** コードの完全性を検証するためにソフトウェアにデジタル署名（コード署名）を行います。マルウェアをスキャンし、オープンソースコードのレビューを行います。ソフトウェア部品表（SBOM）を提供します。
- **メンテナンス ー** HPE Aruba Networkingサポートポータルに投稿します。必要に応じて、リリースのパッチを提供し、メンテナンスを行います。

[9]「Joint Task Force（ジョイントタスクフォース）」。「Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy（情報システムと情報組織を対象としたリスク管理フレームワーク: セキュリティとプライバシーのためのシステムライフサイクルアプローチ）」、NIST Special Publication 800-53。アメリカ国立標準技術研究所、https://doi.org/10.6028/NIST.SP.800-53r5、2020年9月。

[10]「Joint Task Force（ジョイントタスクフォース）」。「Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy（情報システムと情報組織を対象としたリスク管理フレームワーク: セキュリティとプライバシーのためのシステムライフサイクルアプローチ）」、NIST Special Publication 800-53。アメリカ国立標準技術研究所、https://doi.org/10.6028/NIST.SP.800-53r5、2020年9月。

[11]「Joint Task Force（ジョイントタスクフォース）」。「Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy（情報システムと情報組織を対象としたリスク管理フレームワーク: セキュリティとプライバシーのためのシステムライフサイクルアプローチ）」、NIST Special Publication 800-53。アメリカ国立標準技術研究所、https://doi.org/10.6028/NIST.SP.800-53r5、2020年9月。

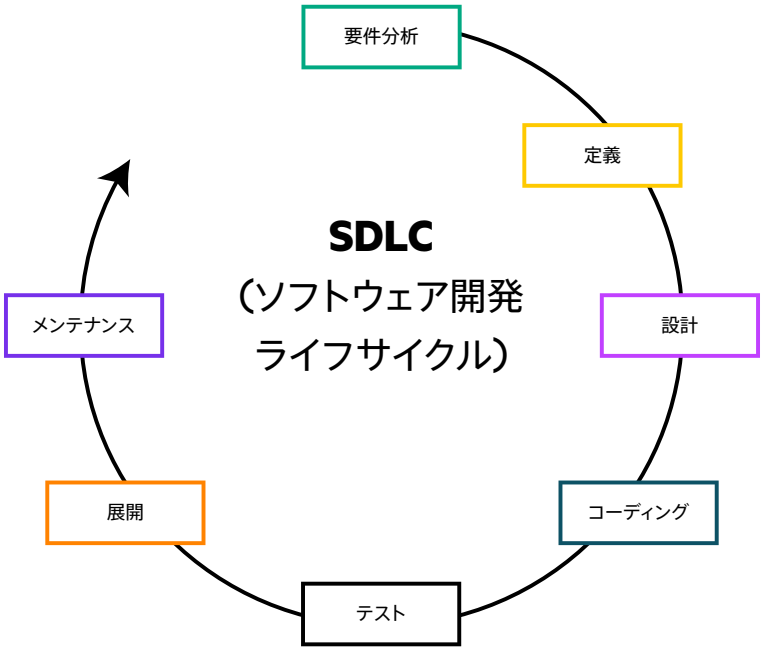

図2. ソフトウェア開発ライフサイクル（SDLC）

サプライチェーンのセキュリティ

HPEは、ICT業界でのサプライチェーンサイバーセキュリティをリードしています。HPE Aruba Networkingソリューションは、認定済みの**TAA準拠**SKUだけを使用しているので、製品のハードウェアおよびソフトウェアコンポーネントが敵対的な国の人物によって操作されている可能性を減らすことができます。製品がTAAに準拠するためには、米国またはTAA「指定国」で製造または「実質的に改造」されている必要があります[12]。

ソリューションには、ソフトウェアコンポーネントのリスク管理のための**ソフトウェア部品表**が付属します。サイバーセキュリティ脅威の進化に対応して、HPE Aruba Networkingは、サプライチェーン内部のサイバーセキュリティリスクを特定して軽減し、セキュアな製品を提供し続けることで、お客様がビジネス目標に集中できるようにします。

セキュアな基盤に構築

米国国家安全保障局（NSA）によって承認されたCommercial National Security Algorithm（CNSA）スイートは、非機密情報と大半の機密情報のための暗号の基盤となる公開アルゴリズムです。NSAは、異なる部門間での取り扱い注意のデータや機密データの共有を容易にし、商用のノートパソコン、タブレット、スマートフォンによるセキュアモビリティを可能にするため、CNSAの使用を承認しました。**HPE Aruba Networking Advanced Cryptography（ACR）モジュール**は、CNSA暗号化を提供することで、ユーザーのモビリティと、管理対象の非機密情報や機密情報を扱うネットワークへのセキュアなアクセスを可能にします。

HPE Aruba Networkingソリューションは、コモンクライテリア、FIPS-140、DoDIN-APL、USGv6といった米国のサイバーセキュリティ指令やプログラムに準拠した使用のために評価され、認定されています。このことは、最も厳格なセキュリティ要件を満たすソリューションであることを意味します。

[12] 連邦調達規則: 52.225-5貿易協定、https://www.acquisition.gov/far/52.225-5、米国政府。

HPE Aruba Networkingインフラストラクチャは、米国国防総省本部内の機密および非機密ネットワーク向けに採用され、毎日数万台以上のデバイスをサポートしています。さらに国防総省は、ネットワーク全体でセキュアなネットワークアクセス制御を実現するため、ClearPass Policy Managerの展開も拡大しています[13]。

悪意のあるブートコード、デバイス偽装攻撃を防ぐため、HPE Aruba Networkingの有線/無線ネットワーク ソリューションは、デバイスに暗号化キーを組み込んでハードウェアのセキュリティを確保するように設計され、耐タンパー性を備えたセキュアな暗号プロセッサーの国際標準である**Trusted Platform Module (TPM) テクノロジー**を使用します。製造中にインストールされるTPMチップテクノロジーによって、ゼロトラストおよびセキュアアクセスサービスエッジ (SASE) セキュリティの追加レイヤーの基盤となるセキュアな信頼の起点を確立できます。

承認されていない不正アクセスポイントがネットワークへのバックドアアクセスを獲得してユーザーデータを傍受するのを防ぐため、HPE Aruba Networking Centralは、高度な**ワイヤレス侵入防御**機能を提供しています。ネットワークチームやセキュリティチームは、固有のリスクしきい値に基づいて、不正アクセスポイント検出のためのカスタムルールを設定できます。

ソフトウェアアップデートとデバイス構成

HPE Aruba Networking Centralを使えば、管理者は複数のデバイスをグループにまとめることで、管理対象デバイスの構成ワークフローを簡素化できます。グループを使うことで、管理者は、UIベースの構成ワークフローまたはCLIベースの構成テンプレートを使用して、デバイスを効率的に管理できます。

HPE Aruba Networkingでは、賞を受けた**サポートポータル**を通じて、ソフトウェアのパフォーマンスおよびセキュリティアップデートを提供しています。

2023年度TSIA STAR Award: カスタマーポータル分野でのイノベーションを通じたデジタルカスタマーエクスペリエンスの向上に対して

脆弱性の報告と解決

HPE Aruba Networking Threat Labsは、HPE Aruba Networking製品内のセキュリティ脆弱性を管理し、軽減する役割を果たします。脆弱性の報告は、独立系セキュリティ調査機関、お客様、さらにHPE Aruba Networking従業員からも行われます。また、HPE Aruba Networkingは、脆弱性を迅速に発見するため、公開のバグ懸賞金プログラムも実施しています。

事業継続性

HPE Aruba Networkingのネットワークおよび管理プラットフォームは、さまざまな耐障害性機能を通じて、運用の中断を最小化し、ネットワークのアップタイムを改善します。例としては、ヒットレスフェイルオーバー、インサービスソフトウェアアップグレード、VSFによって強化されたソフトウェアアップグレード、ライブアップグレード、高可用性設計などがあります。

[13]「The Pentagon Modernizes Wired and Wireless Connectivity, Across All Classification Levels, with Aruba Infrastructure (国防総省はArubaインフラストラクチャによりあらゆる機密レベルでの有線および無線接続のモダナイゼーションを実現)」、https://www.businesswire.com/news/home/20201026005079/en/The-Pentagon-Modernizes-Wired-and-Wireless-Connectivity-Across-All-Classification-Levels-with-Aruba-Infrastructure、2020年10月。

HPE Aruba Networkingソリューションを補完するために、HPE GreenLakeのディザスタリカバリおよびバックアップサービスが利用できます。これは、暗号化されたバックアップを利用して、オンプレミスおよびクラウドネイティブのワークロードをランサムウェア攻撃から保護するものです。また、HPE Servicesを利用すれば、組織に合わせた情報システムのセキュリティ・リスクマネジメントのためのポリシーをセットアップできます。

まとめ

シンプル化とコラボレーションのための戦略的アプローチを採らない限り、サイバーセキュリティ、ゼロトラスト、リスク管理コントロールに関する包括的なNISTガイドラインの実装は困難です。HPE Aruba Networkingが提供するAI搭載のセキュリティファースト ネットワークを導入すれば、セキュリティ、プライバシー、コンプライアンスに関する全チーム共通の目的を達成するための組織の資産としてネットワークを活用できます。

詳細については、arubanetworks.com/products/security/をご覧ください

その他の関連情報

HPEサプライチェーンのセキュリティイノベーション: エッジからクラウドまでの信頼性と耐障害性を向上

製品のセキュリティインシデント対応ポリシー | HPE Aruba Networking

サイバーセキュリティ認定資格・トレーニング | HPE Services - 教育

お客様のニーズに最適な製品をお選びください。
HPEのプリセールススペシャリストにお問い合わせください。

お問い合わせ

ArubaNetworks.comにアクセス

BWP_NISTCompliance_RVK_020224 a00137586jpn

Hewlett Packard Enterprise