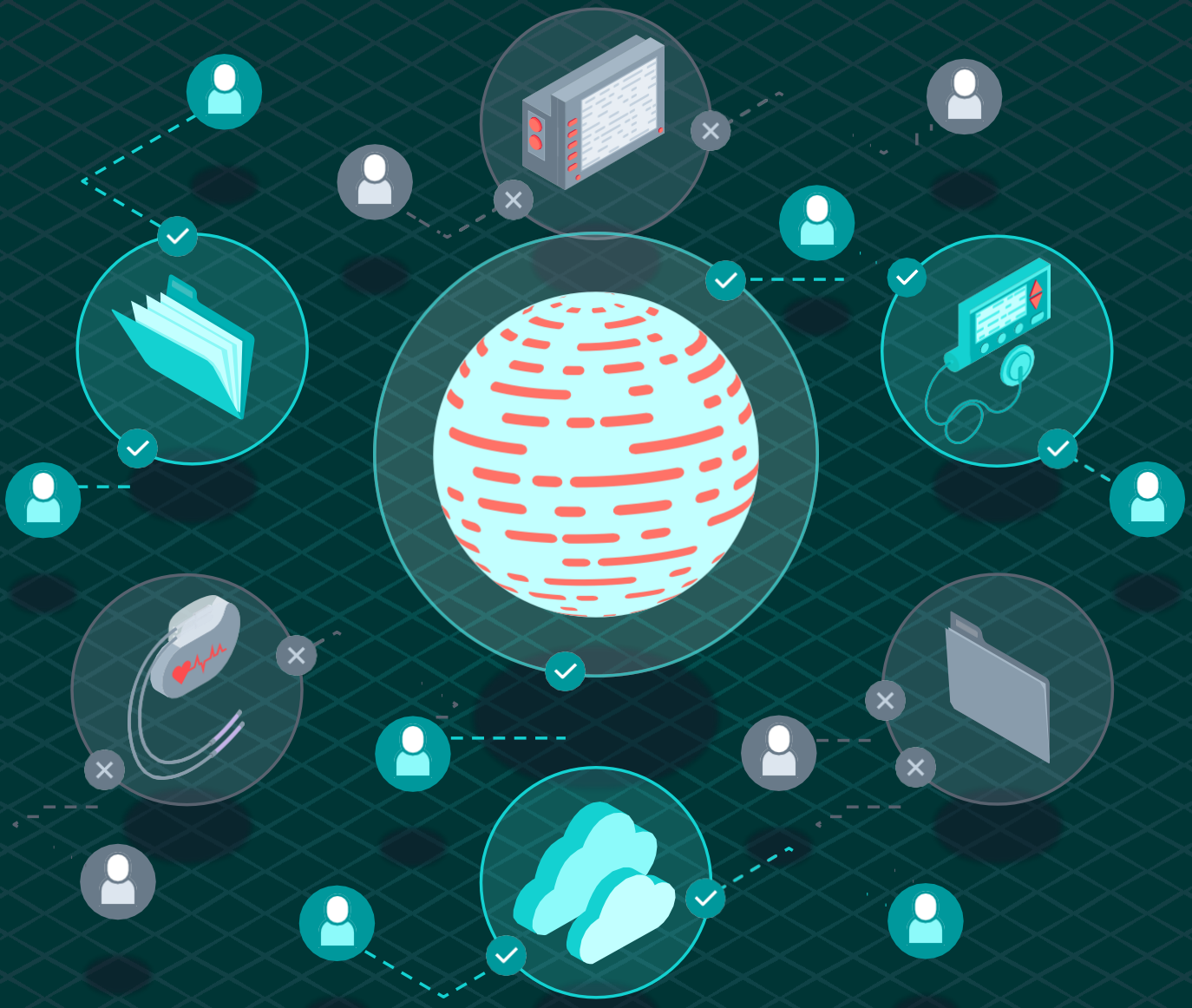
ゼロトラストアーキテクチャにおける医療機器



CSAJC cloud security alliance Japan Chapter

CSA cloud security alliance®

The permanent and official location for Health Information Management (HIM) Working Group is https://cloudsecurityalliance.org/research/working-groups/health-information-management/です。

Acknowledgments

Lead Author

Dr. James Angle

Contributors

Michael Roza
Wayne Anderson

Reviewers

Ashish Vashishtha
Jennifer Minella (jj)
David Nance
Shamik Kacker

CSA Staff

Alex Kaluza

The Health Information Management (HIM) Working Group aims to provide direct influence on how health information service providers deliver secure cloud solutions (services, transport, applications, and storage) to their clients, and foster cloud awareness within all aspects of healthcare and related industries.

日本語版提供に際しての告知及び注意事項

本書「ゼロトラストアーキテクチャにおける医療機器」は、Cloud Security Alliance (CSA)が公開している「Medical Devices in A Zero Trust Architecture」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2023年05月31日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。

(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3. 本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4. 原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5. その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「ゼロトラストアーキテクチャにおける医療機器」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

石井　英男
小田部　悟士
塩田　英二
満田　淳
諸角　昌宏

目次

内容

要約

ネットワークのセキュリティは、ユーザー、デバイス、アプリケーション、システム、そしてそれらがアクセスしようとするすべてのデータなど、ネットワークにつながるすべてのものを理解することから始まります。しかし、デバイスがユーザーである場合はどうなるのでしょうか。セキュリティは、脅威が最も発生しやすい場所に焦点を当てる必要があります。現在の医療機器はクラウドに接続することが多く、攻撃対象が拡大することでリスクが高まります。医療機器は、ネットワークと医療機関（HDO:Healthcare Delivery Organizations）の双方にとって重大なセキュリティリスクとなり、医療機関の業務や患者データを危険にさらす可能性があります[1]。その結果、セキュリティアーキテクトはアイデンティティの概念を再検討する必要に迫られています。基本的に、接続されたすべての医療機器にはIDがあり、ゼロトラストフレームワークの中で考慮する必要があります[2]。

はじめに

サイバー攻撃の著しい増加に伴い、医療業界はシステムや機器の安全性を確保する必要があります。HDOでは通常、数百、数千の医療機器が接続されており、それらはすべて複数の脆弱性を抱えています[3]。これらには、植込み型機器からサーバーベースのシステムまでが含まれます。HDOがこれらの機器のセキュリティ確保に取り組む中で、定着しつつあるのがゼロトラストアーキテクチャ（ZTA）の導入です。

医療分野は、日々発生するランサムウェア攻撃やデータ漏洩の件数に見られるように、セキュリティ上のリスクが極めて高い分野です。保護された医療情報（PHI: Protected Health Information）を含むシステム、医療機器、そして命を救う薬や治療薬を入れる冷蔵庫までもがHDOのネットワークに接続されています。ネットワークにインシデントが発生した場合、システム全体や患者さんに大きな影響を与えます[4]。

従来のネットワークセキュリティは、HDOが外側に強固なセキュリティ境界を構築し、境界の内側のネットワークトラフィックを信頼するという境界アプローチを採用していました。このアプローチは、HDOを脆弱にする可能性のある信頼レベルを想定しています。ゼロトラストネットワークは、今日のヘルスケア企業がレジリエンスを維持しなければならないという現実を受け入れています。壁を作るのではなく、ゼロトラストネットワークは5つの基本的な主張の上に成り立っています。

- ネットワークは常に敵対的であることが前提
- ネットワーク上には、常に外部と内部の脅威が存在する
- ネットワークのローカリティは、ネットワークの信頼性を決めるのに十分ではない

[1] Angle, J., 2020. Managing the Risk for Medical Devices Connected to the Cloud, Cloud Security Alliance, Retrieved from https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical-devices-connected-to-the-cloud/

[2] Kumar, S., 2021. Embracing Zero Trust for IoT and OT: A Fundamental Mind Shift, Retrieved from https://www.forescout.com/blog/embracing-zero-trust-for-iot-and-ot-a-fundamental-mind-shift/

[3] Lerman, L., 2021. Zero Trust Approach Can Defend Against IoMT Device Attacks for Healthcare Organizations, Retrieved from https://www.toolbox.com/tech/iot/guest-article/zero-trust-approach-can-defend-against-iomt-device-attacks-for-healthcare-organizations/.

[4] McKeon, J., 2021. Exploring Zero Trust Security in Healthcare, How It Protects Health Data, Retrieved from https://healthitsecurity.com/features/exploring-zero-trust-security-in-healthcare-how-it-protects-health-data

- すべてのデバイス、ユーザー、ネットワークフローが認証され、許可される。
- ポリシーは動的で、できるだけ多くのデータソースから算出する必要がある[5]。

境界線を採用するのではなく、ネットワーク上のすべての接続やイベントを悪意があり信頼できないものと見なします。つまり、すべてのネットワーク構成要素に「ゼロトラスト」が与えられるのです。本稿では、ゼロトラスト成熟度モデルに基づき、HDOが医療機器のゼロトラストを実現するための方法を検討します。

ゼロトラスト成熟度のための5つの柱は以下になります。

- アイデンティティ
- デバイス
- ネットワーク
- アプリケーション
- データ

ゼロトラスト成熟度モデルは、5つの柱からなる段階的な実装を表しており、最適化に向けて時間をかけて少しずつ前進させることができます。図1に描かれている柱は、アイデンティティ、デバイス、ネットワーク、アプリケーションワークロード、データです。各柱には、「可視化と分析」「自動化とオーケストレーション」「ガバナンス」に関する一般的な内容が含まれています。この成熟度モデルは、ゼロトラストへの移行をサポートするための多くの道のりのうちの一つです[6]。

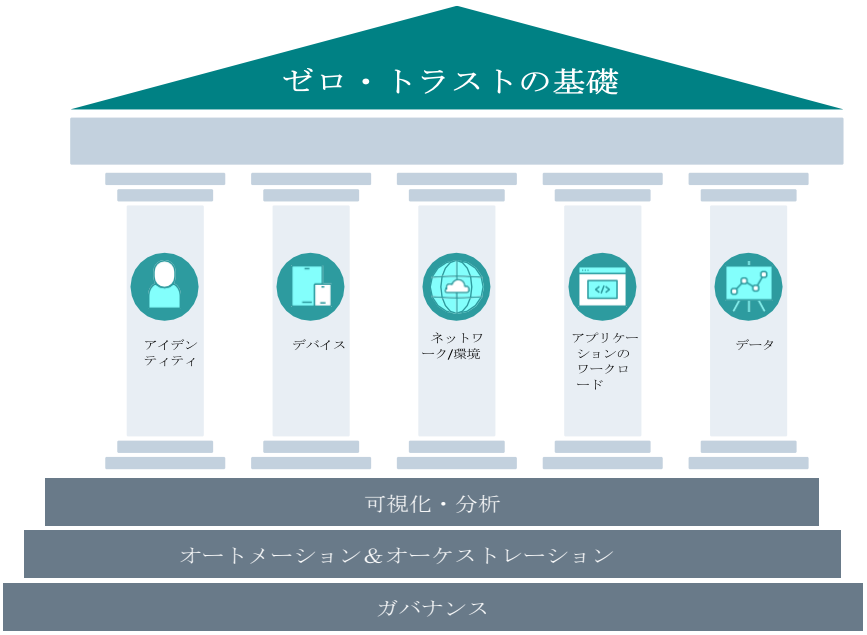


図1:ゼロトラストの基礎

[5] Gilman, E. & Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Trusted Networks, O'Reilly Media Inc. Sebastopol, CA.

[6] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

各ステージの説明は、ゼロトラストテクノロジーの柱ごとに成熟度を特定し、成熟度モデル全体に一貫性を持たせるために、以下のような説明を用いています。

- **従来**：手動による設定と属性の割り当て、静的なセキュリティポリシー、外部システムへの依存度が粗い柱レベルのソリューション、プロビジョニング時に確立された最小限の機能、独自の柔軟性のない柱によるポリシー実施、手動によるインシデント対応、軽減策の展開。
- **高度**：柱をまたいだ調整、集中的な可視化、集中的なID管理、柱をまたいだ入力と出力に基づくポリシー実施、事前に定義された緩和策へのインシデント対応、外部システムとの依存関係の詳細化、ポスチャーアセスメントに基づく最低限の権限変更など。
- **最適**：資産やリソースへの属性の完全自動割り当て、自動化/観察されたトリガーに基づく動的ポリシー、動的な最小権限アクセス（閾値内）のための自己列挙型依存関係を持つ資産、柱間の相互運用性のためのオープンスタンダードとの連携、状態をポイントインタイムで思い出すためのヒストリアンと集中的な可視化機能。

また、各柱には、その柱の「可視性と分析」「自動化とオーケストレーション」「ガバナンス」に関する一般的な詳細が記載されています[7]。

機能	従来	高度	最適
可視化・分析能力	エージェンシーは、基本属性と静的属性でユーザー活動の可視性をセグメント化します。	エージェンシーは、基本的な属性でユーザーの活動の可視性を集約し、手動で絞り込むための分析・報告を行います。	エージェンシーは、高忠実度の属性とユーザーおよびエンティティの行動分析（UEBA）により、ユーザーの可視性を一元化します。
自動化・オーケストレーション機能	エージェンシーは、IDおよびクレデンシャルを手動で管理し、オーケストレーション（複製）します。	エージェンシーは、基本的な自動オーケストレーションを使用して、ID をフェデレートし、ID ストア間の管理を許可します。	エージェンシーは、ID ライフサイクルを完全にオーケストレーションし、ダイナミックユーザープロファイリング、ダイナミック ID、グループメンバーシップ、およびジャストインタイムとジャストフットのアクセス制御を実装しています。

[7] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

ガバナンス・ケイパビリティ	エージェンシーは、クレデンシャル・ポリシー（複雑さ、再利用、長さ、クリッピング、MFAなど）の静的な 技術的実施を使用して、最初のプロビジョニング後にIDおよび権限を手動で監査します。	エージェンシーは、ポリシーに基づく自動アクセス取り消しを使用します。共有アカウントはありません。	エージェンシーは、ポリシーの技術的な実施を完全に自動化します。エージェンシーは、新しいオーケストレーションオプションを反映させるためにポリシーを更新します。

表1 例CISA成熟度モデル アイデンティティ・ピラー

医療機器のセキュリティを5つの柱を通して見ることで、HDOは医療機器のセキュリティポスチャを明確に把握すべきです[8]。

ゼロトラスト

クラウドコンピューティング、モバイルデバイス、IoMT（Internet of Medical Things:医療領域のIoT）デバイスの利用が進むにつれ、ネットワークの境界を定義した強固な境界防御という考え方は薄れてきています。
さらに、今日の労働力は分散しており、リモートワーカーはいつでもどこでも、どのデバイスからでもアクセスできることが求められています。HDOは、どこからでもすべてのリソースに安全にアクセスできるようにする必要があります。

ゼロトラストは、デバイス、主体、ネットワークに与えられている信頼の前提を取り除くものです。ゼロトラストは、リスクベースのアクセス制御を実施することで、ネットワークの場所、主体、資産に関係なく安全にアクセスすることを重視しています。厳格なアクセス制御とリクエストごとの特権を強制する際の不確実性を最小化するために設計されたコンセプトのコレクションを提供します。アクセスの決定は、情報システムやサービスが競合するネットワークに直面した際に行われます[9]。ユーザーは、組織のデジタル資産に対して厳格なアクセス権を与えられます[10]。ユーザーは、与えられたタスクを実行するためのインフラストラクチャーコンポーネントのみを見たりアクセスしたりすることができます。

ゼロトラストでは、デバイスの正常性の証明、データレベルの保護、堅牢なIDアーキテクチャ、組織のデジタルリソースの周囲にきめ細かい信頼ゾーンを作成するための戦略的マイクロセグメンテーションが必要です。ゼロトラストでは、アクセス要求や通信動作をオープンコネクトの長さでリアルタイムに評価します。アクセスは継続的かつ一貫してHDOのリソースに再調整されます。次の図は、米国国立標準技術研究所（NIST）による抽象的なゼロトラストアーキテクチャ

[8] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[9] Rose, S., 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. National Institute of Standards and Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf

[10] Kumar, S., 2021. Embracing Zero Trust for IoT and OT: A Fundamental Mind Shift, Retrieved from https://www.forescout.com/blog/embracing-zero-trust-for-iot-and-ot-a-fundamental-mind-shift/

です[11]。組織は、ゼロトラストを有効にするために、包括的な情報セキュリティとレジリエンスの実践を行う必要があります。既存のサイバーセキュリティポリシーやガイドライン、ID・アクセス管理、継続的なモニタリング、ベストプラクティスとバランスを取ることで、ZTAは一般的な脅威から保護し、リスク管理アプローチを用いて組織のセキュリティポスチャーを向上させることができます。

これは導入時、開発時のどちらでも提起可能です[12]。

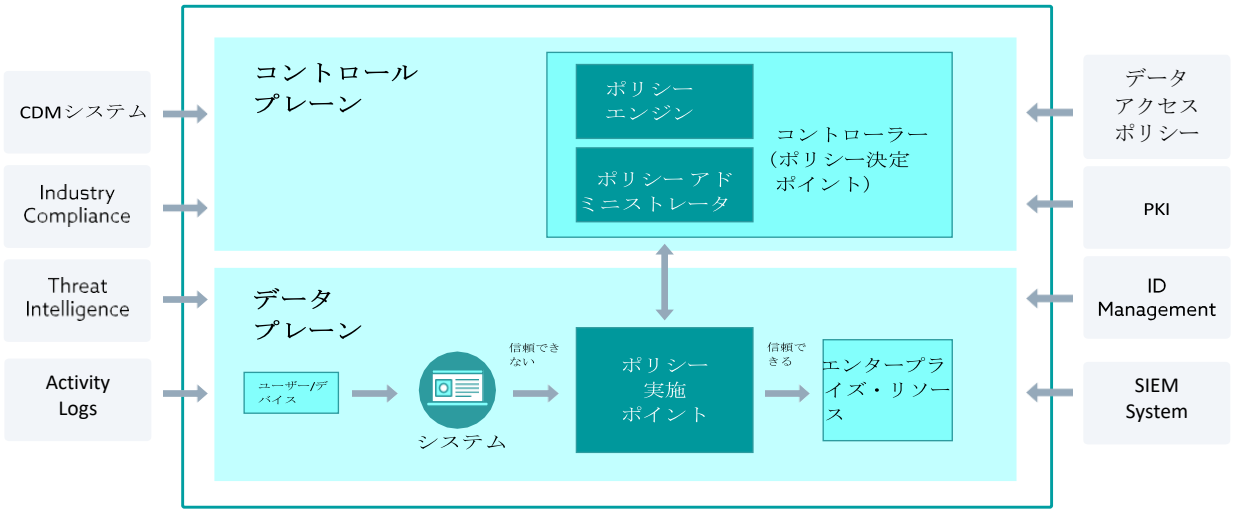


図 2: コア・ゼロ・トラスト論理構成要素

医療機器管理プログラム

医療機器のゼロトラストの実装について説明する前に、多くのHDOでは機器の数が多いため、手動で管理しようとすると非常に手間がかかることに留意しておく必要があります。HDOは、ネットワークのマイクロセグメンテーションを管理し、ポリシーを適用し、脆弱性を特定し、エンドポイントの検出と応答を提供するツールを必要としています。

さらに、すべてのデバイスを見ることができるようなプログラムが必要です。管理プログラムは、すべてのデバイスとその場所の完全なインベントリを提供する必要があります。インベントリには、リソース要求に対して効果的なほぼリアルタイムの承認決定を行うために、十分な具体性と詳細性を持つインベントリに指紋認証デバイスが含まれている必要があります。医療機器管理に特化した製品も多くあります。また、医療機器に関連する脆弱性やリスクを特定する製品もあります。HDOがどの製品を選択するかにかかわらず、そのツールは医療機器エコシステムの全体像を提供する必要があります。

[11] Rose, S., 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. National Institute of Standards and Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf

[12] https://doi.org/10.6028/NIST.SP.800-207

アイデンティティ

成熟度モデルの最初の柱は「アイデンティティ」です。アイデンティティ成熟度モデルの機能は、認証、アイデンティティ・ストア、およびリスク評価です。アイデンティティは、ゼロトラストアーキテクチャの中核をなすものです。成熟度モデルでは、単純なパスワードから複数の要素の組み合わせによる検証へ移行し、すべてのインタラクションを通じて継続的に検証を行います。アイデンティティとは、ユーザーまたはエンティティを一意に示す属性または属性のセットを指します。

HDOは、適切なユーザーとデバイスが適切なタイミングで適切なリソースにアクセスできることを保証し、実施する必要があります[13]。ゼロトラスト環境での検証の後、ネットワークに接続されたデバイスを信頼することが重要です。 IoMT デバイスには、他のネットワーク デバイスと同じ方法でデバイスを認証できない可能性があるという問題があります。HDOはコントロールプレーンと認証できない可能性があり、デバイスはTPM（Trusted Platform Module）を持っていない可能性があります。他のいくつかの方法として、デバイス[14]の信頼性のレベルを提供することができます。これについてはネットワークのセクションで説明します。

医療機器にゼロトラストポリシーを適用する前に、HDOはどのような機器が存在し、その機能、目的、場所を知っておく必要があります。HDOでは使用するデバイスの数が多いため、これは特に困難となる場合があります。多くの場合、HDOは各機器を特定のサブネットに属するIPアドレスとしてしか知らないかもしれません[15]。

HDOは、環境にあるすべての医療機器を発見し、分類し、インベントリ化する信頼性の高い方法を必要としています。このためには、可能な限りデバイスの種類、メーカー、機能、場所、アプリケーション/ポート、動作などを詳細に把握することが必要です。医療機器のセキュリティは、接続された機器を認証し、各機器が期待される動作をできるように、信頼できるかどうかにかかっています。

医療機器の通信は、そのほとんどが機器と機器の間で行われます。小型の携帯デバイスは、ドッキングステーションを使用してワークステーションに接続することが多く、その後ネットワーク接続を介してサーバーに接続されます。患者モニタリング装置は、ワークステーション/サーバーに接続します。機器のアイデンティティでは、一般的にユーザー管理をする際に使われる標準的な因子は利用できません。例えば、機器はトークンを持たず、覚えろと言われたものは必ず「覚え」ます（例えば、悪慣習であるパスワードの挿入やハードコーディングなど）。その結果、HDO環境は、認証・認可プロセスの一部として、安全に保存・挿入された認証情報および証明書などのメカニズムを使用する機器ベースの運用を行う必要があります。

セキュリティ運用環境は、医療機器の特性を利用して、環境の「信頼状態」の複合的なコンテキストを構築する必要があります。この信頼状態は動的であり、デバイス、動作環境、および現在の状態を強く識別することを組み合わせて使用します。

---

[13] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[14] Gilman, E. & Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Untrusted Networks, O'Reilly Media Inc. Sebastopol CA.

[15] Order White Paper,2022. 5 Steps to Zero Trust for Unmanaged and IoT Devices, retrieved from https://resources.ordr.net/whitepapers/5-steps-to-zero-trust-for-unmanaged-and-iot-devices

セキュリティ運用の意思決定において医療機器管理プログラムを使用することで、HDOは各医療機器に関するすべての関連情報を収集することができます。これには、各デバイスにどのようなポリシーを適用すべきかを判断するための情報が含まれます。このプログラムは、次の図に示すように、ゼロトラスト環境において、ネットワークのポリシー決定ポイント（PDP）として機能することができます。

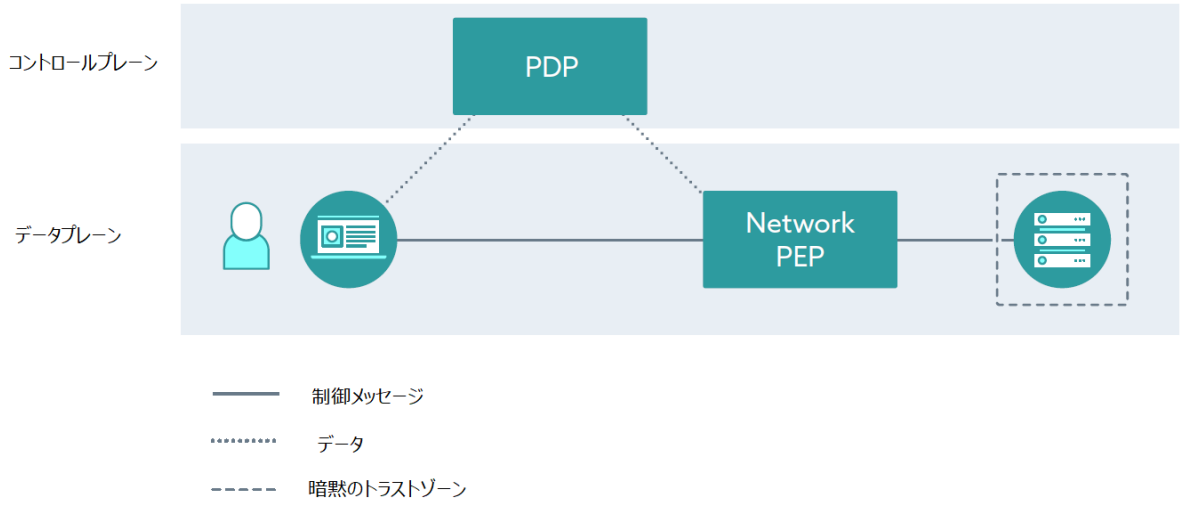


図3:ゼロトラストネットワークのデータフロー

デバイス

2つ目の柱は、デバイスです。デバイスとは、ネットワークに接続できるあらゆるハードウェア資産を指し、IoMTデバイスや関連する管理機能のエンドポイント、人間の対話型エンドポイントも含まれます。**デバイス成熟度**モデルの機能は、コンプライアンス・モニタリング、データアクセス、アセット・マネジメントです。HDOは、サービスやデータにアクセスするためのデバイスの整合性を確保する必要があります。
成熟度モデルは、ポリシーの実施をエッジに押しやり、従来の人間が操作するデバイスを経由せずに、ユーザーやデバイスが直接サービスやデータを利用できるようにする機会を増やします[16]。

接続された医療機器は、HDOが質の高い医療を提供する能力を高める一方で、患者やHDOを危険にさらすセキュリティ上の問題も抱えています。コネクテッドメディカルデバイスのセキュリティ管理には、以下のような課題があります。

- 医療機器に対する明確な可視性がなく、そのリスクエクスポージャーを明確に理解できていない。
- 目に見えない脆弱性がリスクを拡大させる
- 脅威はHDOの能力を凌駕している
- レガシーなセキュリティアーキテクチャがコンプライアンスを阻害している

[16] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

- IoMTデバイスは、権限のない個人が物理的にアクセスすることができ、機密データを取り出す目的でデバイスを改ざんしたり、盗んだりすることができる。
- IoMTデバイスは、一般的に脆弱性のアップデートやパッチを適用することができない
- IoMTデバイスは、最新の認証方式を取り込めない可能性がある

HDOは、医療機器の完全かつ正確なインベントリとリスクアセスメントを行うことで、これらの課題に対処することができます。

- 完全かつ正確なデバイスの発見とリスク評価
- 最小アクセスポリシーの推奨と実施
- 継続的な監視と脅威の防止[17]

ゼロトラストフレームワークにより、HDOは接続された臨床機器のセキュリティリスクを最小化することができます。以下の推奨事項は、HDOがゼロトラストによるデバイスセキュリティを実現するのに役立つものです。

- **オーケストレーションされた可視性：**包括的な可視化には、管理されている医療機器と管理されていない医療機器のすべてを完全にプロファイリングし、動的にリスクスコア化したインベントリが必要です。可視性とは、各デバイスのセキュリティ状況、ネットワークの状態、場所、デバイスの使用状況などを動画で確認できることです。特に、資産の不正な動作を検出するには、許可された動作を詳細に知る必要があるため、各機種の動作要件やワークフローをプロファイル化する必要があります。これが、包括的な視認性という意味です。正しいデータへの適切な変更を、正しいシステムやワークフローで即座に利用できるようにします。このような状況の中で、それは医療機器管理プログラムのデータ取得とオーケストレーションは、ネットワークトラフィックフローから受動的に取得する機器データに限定されないことを理解することが重要です。また、セキュリティオペレーション機能（潜在的にはエンドポイント検知・応答機能、またはコンテキスト処理と応答の他の手段を含む）のように、他のネットワーク化されたシステムで活発に捕捉・保持されるデータも含まれます。
- **XDR（Extended Detection and Response）：**XDRは、エンドポイントの検出と応答機能を拡張し、リアルタイムのマルチドメイン検出とオーケストレーションされた応答を提供します。HDO全体の脅威の可視化、セキュリティ運用の迅速化、リスクの低減を実現します。XDRは、一般的にクラウドインテリジェンスとコントロールの統合ツールで、セキュリティ製品やデータを統合してシンプルなソリューションにすることで、全体的に最適化されたセキュリティを提供します。XDRセキュリティは、予防、検知、調査、対応の効率的でプロアクティブなソリューションを提供し、可視化、分析、相関するインシデントアラート、自動応答を提供することで、データセキュリティの向上と脅威への対処を実現します。
- **ダイナミックセグメンテーション：**ネットワークセグメントへの侵入を防ぐには、適切なセキュリティポリシーの作成を迅速化し、展開前に検証を行うプロセスが必要です。医療機器管理プログラムでは、複雑すぎない合理的なセキュリティポリシーの作成が常に課題となっているため、ポリシーのベースラインを自動生成するようにしました。これらのプログラムは、各デバイスの動作要件（内部/外部接続要件、意図するワークフロ

[17] Palo Alto Networks, 2022. The Right Approach to Zero Trust for Medical IoT Devices, Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/right-approach-zero-trust-medical-iot

ーなど）を把握しているため、自動化が非常に効果的です。マイクロセグメンテーションによる有意義な統合により、管理者は以下のことが可能になります。

- デバイスのアイデンティティと既存の関係を理解する
- セキュリティポリシーの影響をバーチャルにシミュレート
- 基本的なポリシールールの影響をテストし、必要に応じて修正する。
- 臨床業務に支障をきたすことなく、セグメンテーション効果を検討[18]

ネットワーク

3つ目の柱は、ネットワークです。ネットワークとは、社内ネットワーク、無線、インターネットなど、オープンな通信媒体のことを指します。ネットワーク成熟度モデルの機能はセグメンテーション、脅威防御、暗号化です。HDOは、従来のネットワークセグメンテーションに内在する暗黙の信頼ではなく、アプリケーションワークフローのニーズに応じてネットワークのセグメンテーションと保護を調整する必要があります[19]。

医療機器がネットワーク化されていることこそが、セキュリティリスクを生みます。セキュリティはデバイスから始まりますが、HDOはネットワークのトポロジーに対処する必要があります。企業内LAN上の機器が他の機器と接続する必要がある場合、互いを識別するための規格が必要となります。規格はIEEE 802.1 X[20]です。802.1Xプロトコルを使用することで、医療機器のセキュリティが強化されます。IEEE 802.1Xは、IEEE 802.1Xワーキンググループによって定義された、有線および無線ネットワークの認証を採用したポートベースのアクセス制御を扱う規格です。RADIUSサーバーは、ユーザーの認証情報または証明書に基づいてIDを確認します。

図4に示すように802.1Xを理解するためには、3つの用語を理解する必要があります。

- **サプリカント**: 認証を受けたいユーザーまたはクライアント
- **認証サーバー(AS)**：認証を行う実際のサーバー（通常はRADIUSサーバー）
- **オーセンティケータ**：サプリカントと認証サーバーの間にある機器（無線アクセスポイントなど）。

802.1Xの利点の1つは、認証者が多くのメモリや処理能力を必要としないことです。このため、802.1Xは無線アクセスポイントに最適です[21]。

[18] Crowdstrike, 2022. Healthcare IoT Security Operations Maturity: A Rationalized Approach to a New Normal, Retrieved from, https://www.crowdstrike.com/resources/reports/healthcare-iot-security-operations-maturity/

[19] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[20] Study CCNA.com, 2022. Cisco CCNA Study Notes, Retrieved from https://study-ccna.com/802-1x-authentication/

[21] Fruhlinger, J. and Snyder, J., 2021. 802.1X: What you need to know about this LAN-authentication standard, Network World. Retrieved from https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html

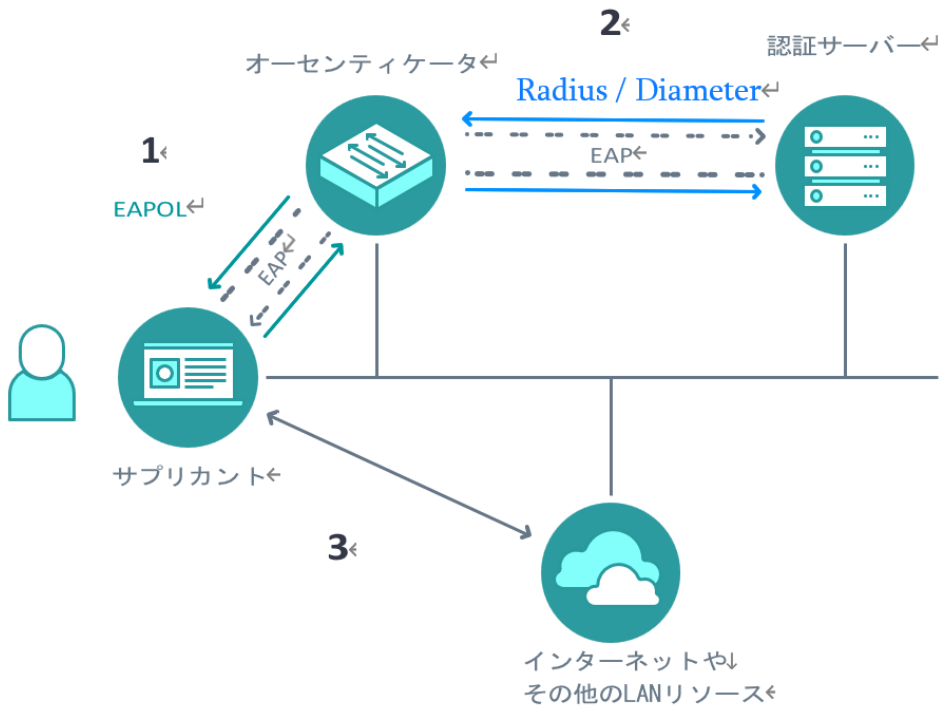


図4:CCNAスタディガイドに掲載されている共通EAPベース認証について

一般的なEAPベースの認証方式には、以下のものがあります。

- **Lightweight EAP(LEAP)**：認証プロセスは、クライアントがASにユーザー名やパスワードなどの認証情報を提供することです。
- **EAP Flexible Authentication by Secure Tunneling（EAP-FAST）**：ASとサプリカントの間でPAC（Protected Access Credential）を通過させる方法です。
- **Protected EAP（PEAP）**：内側と外側の認証を使用します。とはいえ、ASは外部認証でサプリカントとの認証のためにデジタル証明書を提示します。
- **EAP Transport Layer Security（EAP-TLS）**：ASとサプリカントが証明書を交換し、互いに認証することができます。EAP-TLSは、無線クライアントがデジタル証明書を受信して利用できる場合にのみ実用的です。医療機器などの多くの無線機器は、CAとのインタフェースや証明書を使用することができないOSを基盤としています[22]。

残念ながら、すべての医療機器が802.1Xで利用可能な安全な認証方法を使用できるわけではありません。アクセスエッジにおける最善かつ最も安全なソリューションは、ネットワークのインテリジェンスを利用することです。MAC認証バイパス（MAB）では、認証サーバーは、ここで説明したEAPOLの認証プロセスではなく、そのMACアドレスを使用してクライアントデバイスを認証することができます。MABは、MACアドレスを使用してネットワークアクセスレベルを決定します。MABは、IEEE 802.1XをサポートしないIoMTデバイスに対して、ネットワークエッジでの可視化とIDベースのアクセス制御を提供します。MAB対応ポートは、接続しようとする機器のMACアドレスに基づいて、動的に有効または無効にすることができます。
IEEE 802.1Xを使用する前と使用した後のDefault Network Accessを以下に示します。

[22] Study CCNA.com, 2022. Cisco CCNA Study Notes, Retrieved from https://study-ccna.com/802-1x-authentication/

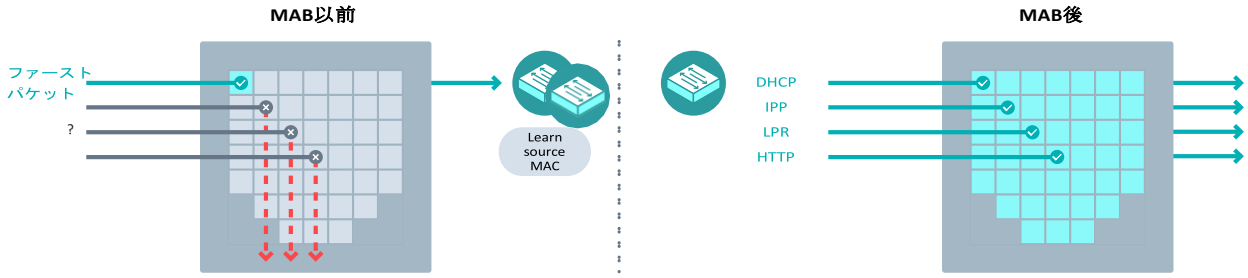


図5 MABの前と後（Ciscoより取得）

MAB認証前は、デバイスの身元が不明であり、トラフィックがブロックされます。スイッチは、1つのパケットを調べて、送信元MACアドレスを学習し、認証します。MABが成功すると、デバイスのIDが判明し、そのデバイスからのトラフィックが許可されます[23]。

MABはそれ以外をチェックすることはできません。そのため、MACアドレスのなりすましが容易であるため、安全な認証方法とは言えません。これをセキュアにするのは、医療機器管理プログラムの活用とマイクロセグメンテーションです。医療機器管理プログラムは、機器がどのセグメントにあるかを把握し、特定の機器からの送信であることを識別できるため、機器へのなりすましが難しくなります。

Cloud Security Allianceの論文「Managing the Risk for Medical Devices Connected to Cloud」では、医療機器をセグメント化して分離することの重要性が強調されています[24]。ゼロトラスト環境では、さらに一歩踏み込んでマイクロセグメンテーションを実施する必要があります。マイクロセグメンテーションは、セグメンテーションの些細な改良のように聞こえるかもしれませんが、実際には全体の焦点を大きく変えることを意味します。従来のネットワークセグメンテーションは、ネットワークの性能と管理に重点を置いていました。しかし、マイクロセグメンテーションは、セキュリティとビジネスアジリティに関する問題に対処するものです。マイクロセグメンテーションは、リスクを低減し、ダイナミックなIT環境にセキュリティを適応させるための強力なアプローチです。マイクロセグメンテーションは、IT環境を制御可能な区画に分割することで、横の動きを止めるという課題を解決します。セキュリティルールをアプリケーションの概念で表現し、アプリケーションやインフラストラクチャのコンポーネントが変更されたときに自動的に再構成できるようにすることで、セキュリティを動的なものにします[25]。

マイクロセグメンテーションは、クラウドやデータセンター環境全体でセキュアゾーンを作成し、ワークロードを互いに分離して個別に保護します。ファイアウォールポリシーは、ゼロトラストセキュリティアプローチに基づき、ワークロード間の東西トラフィックを制限して攻撃面を減らし、脅威のラテラルムーブメントを防いで侵害を封じ込めることができます。医療機器管理プログラムは、ポリシーを実施ポイントにプッシュし、動的な設定と実施を行うことができます。

---

[23] Cisco, 2011. MAC Authentication Bypass Deployment Guide, Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/MAB/MAB_Dep_Guide.html

[24] Angle, J., 2020. Managing the Risk for Medical Devices Connected to the Cloud, Cloud Security Alliance, Retrieved from https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical-devices-connected-to-the-cloud/

[25] Friedman, J., 2017. The Definitive Guide to Micro-Segmentation, Illumio. Retrieved from https://www.illumio.com/lp/definitive-guide-to-micro-segmentation

すべての医療機器のトラフィックは、医療機器管理プログラムとEDR、MDR、NDR、XDRなどのセキュリティ監視・応答ソフトウェアを使用して監視する必要があります。異常が確認された場合、HDOはラテラルムーブメントの動きを制限するポリシーを実施し、マルウェアや悪意のある活動の拡散を防止することができます。さらに、すべてのネットワークトラフィックを暗号化する必要があります。

アプリケーション

4つ目の柱は「アプリケーション」です。これには、オンプレミスやクラウドで実行するアプリケーションも含まれます。アプリケーション成熟度モデルの機能は、アクセス承認、脅威防御、アクセシビリティ、アプリケーションセキュリティです。HDOは、保護機能をアプリケーションのワークフローと密接に統合し、適切なセキュリティを提供するために必要な可視性と理解を保護機能が確保する必要があります[26]。

医療機器アプリケーションのセキュリティを確保することは、機器の侵害を防止する上で非常に重要です。ゼロトラストのセキュリティモデルはこれを実現することができますが、ゼロトラストは製品ではありません。その代わりに、安全なネットワークとアプリケーションのアーキテクチャに変換するアプローチであり、格言でもあるのです。基本的に、ネットワークの内外からどのユーザーやデバイスもデフォルトで信頼されないようにするために、ソリューションのエコシステムが連携しています。アプリケーションにアクセスする前に検証が必要です。医療機器アプリケーションを保護するために、以下のことが要求されます[27]。

- **アクセス前の認証**：これは、ゼロトラスト環境を構築し、内部および外部のユーザーが認可前にアクセスできないようにすることで、これらの要素が侵害される可能性を低減させるものです。
  最小特権アクセスモデル：最低限、デバイスの接続は最小特権に基づくポリシーを活用する必要があります。そのためには、HDOは、ユーザーが何を達成しようとしているのか、アクセスしようとしているサービスの種類、必要な通信プロトコルを特定する必要があります。一度決定すれば、現在の状況に基づいてアクセスを許可すべきかどうかを検証することができます。アクセスを許可する場合でも、必要な通信フローのみを許可し、それ以外は許可しないような方法でプロビジョニングする必要があります[28]。
- **マイクロセグメンテーション**：これにより、企業は物理的なネットワークを論理的なマイクロセグメントに分割するだけで保護され、アクセスを許可された人だけがデータを見ることができるようになり、リスクを軽減することができます。マイクロセグメンテーションは、不正なラテラルムーブメントを防ぎつつ、攻撃対象領域を可能な限り小さくすることを目的としています。アプリケーションのリクエストの送信元は、アクセス権のレベルや種類を計算する際に考慮される必要があります[29]。

[26] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[27] F5, 2022. Zero Trust in an Application-Centric World, Retrieved from https://www.f5.com/services/resources/use-cases/zero-trust-in-an-application-centric-world

[28] Bomba, M., 2021. Basic Zero Trust Principles for Application Security, Retrieved from https://kemptechnologies.com/blog/zero-trust-application-security

[29] Cigniti, 2022. Implement Zero Trust to secure your applications, Retrieved from

- **継続的な検証/モニタリング**：アプリケーションのアクセス権を特定のユーザーに対して特定の場所から特定のデバイスで提供した後、リスクレベルが変化した場合、リスクを最小化するために接続を停止できるよう、継続的な監視が必要です。医療機器管理プログラムとXDRは、異常の検出と対応の鍵となるネットワーク視点での監視を可能にします。

さらに、アプリケーションのセキュリティには、内部アクセスか外部アクセスかにかかわらず、移動中および保存中のデータの暗号化が不可欠です[30]。

データ

5つ目の柱は「データ」です。データは、デバイス、アプリケーション、ネットワークで保護する必要があります。データ成熟度モデルの機能は、インベントリ管理、アクセス判定、暗号化です。HDOは、セキュリティに対してデータ中心的なアプローチをとるべきです。HDOは、すべてのデータ資産を識別し、分類し、インベントリ化する必要があります[31]。

医療機器は、多くの目的を果たす電子的に保護された健康情報（ePHI）を大量に生成します。そのデータは、患者さんの診断、モニタリング、治療などに活用されます。これらの情報は、安全で効果的な医療を提供するために役立ちます。さらに、そのデータをビッグデータとして、ポピュレーションヘルスや予防分析に活用することも可能です。このデータは、移動中と保存中の両方で保護されなければなりません。ゼロトラスト環境では、機密データを特定し、すべてのデータフローをマッピングし、すべてのストレージを特定する必要があります。

ゼロトラストは、アクセス制御の実施粒度によってデータ利用が可能になります。ゼロトラスト・データ管理は、ゼロトラストの信条に根ざしたサイバーセキュリティの基礎となるデータ中心のアプローチに焦点を当てます。データの所在にかかわらず、データは保護されます。HDO個人へのアクセスリソースは、セッション単位でのみ発生します。動的なポリシーは、すべてのデータソースへのアクセスを制御することで、企業のプロセスを保護します。常にデータのアカウンティングを行い、場所、権限、アプリケーションの要件、行動に合わせて信頼ゾーンとアクセス制御を確立することで、すべてのデータの可視性を確保します。

ゼロトラストアーキテクチャ内の異常検知と機械学習を用いた予測分析は、すべてのアクセス試行を記録し、それらの試行が異常な行動や疑わしい活動であるかを分析します。システムが矛盾を認識し、アクセス要求を自動的に拒否し、警告を発するため、HDOは攻撃から積極的に保護することができます[32]。

ゼロトラスト環境では、データ利用を検討する段階が複数存在します。データは保存中、移動中、使用中のいずれでもあり得ます。これらの各段階では、データの管理とセキュリティに課題

https://www.cigniti.com/blog/zero-trustsecure-applications/

[30] Bomba, M., 2021. Basic Zero Trust Principles for Application Security Retrieved from https://kemptechnologies.com/blog/zero-trust-application-security

[31] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[32] Ross, J., 2022. The Zero Trust Approach to Data Management, Retrieved from https://thenewstack.io/the-zero-trustapproach-to-data-management/

があります。
データの保護は、アクセスのコントロールから始まります。アクセス制御は、誰がデータを見ることができるか、データに変更を加えることができるか、データを削除することができるかを決定し、実施する必要があります。しかし、その前に、保存中のデータを暗号化する必要があります。さらに、移動中のデータはすべて暗号化する必要があります。

HDOは、データ損失防止（DLP）ソリューションを採用する必要があります。DLPソリューションは、以下の要素に関する制御を提供します。

- **デバイス制御**：デバイスレベルでデータの利用方法を定義する手段
- **コンテンツアウェア制御**：データの内容に応じた制御の実施と調整
- **暗号化の実施**：保存中のデータを確実に暗号化する
- **データディスカバリー**：機密データを見つける手段を提供する

ゼロトラストでは、データは保護が必要なリソースです。つまり、すべてのデータアクセスはPDPとPEPを経由する必要があり、IDを中心としたセキュリティが実施されることを保証します[33]。

結論

医療機器の場合、ゼロトラストは少し難しいですが、適切に実施することで、HDOのデバイスセキュリティを強化することができます。医療機器管理プログラムを使用して、すべての機器を識別し、フットプリントを付けることで、HDOはPDPとしてプログラムを使用することができます。PDPはアクセス制御を支援することができ、正しいポリシーが適用されることを保証します。マイクロセグメンテーションにより、HDOはデータの流れを完全に制御することができ、疑わしい活動のラテラルムーブメントを防ぐことができます。エンドポイントプロテクションとXDRは、早期発見と対応を強化し、DLPは、データ損失の可能性を低減します。

これらのセキュリティツールに加え、HDOの現行のセキュリティツールにより、安全なゼロトラスト環境を提供します。この環境では、すべてのデバイスが識別され、すべてのアクセスが制限・制御されます。データはすべて暗号化され、その場所もわかります。アクセス制御、隔離、継続的な監視を組み合わせることで、脆弱性を特定し、デバイスを修復できるまで緩和的な制御が行われる環境を提供することができます。HDOはリスクを排除することはできませんが、ゼロトラストは現在最高のセキュリティを提供します。

[33] [1] Garbis, J. & Chapman J. W., 2021. Zero Trust Security: An Enterprise Guide, Apress Media, California.

参考文献

Angle, J., 2020. Managing the Risk for Medical Devices Connected to the Cloud, Cloud Security Alliance, Retrieved from https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medicaldevices-connected-to-the-cloud/

Bomba, M., 2021. Basic Zero Trust Principles for Application Security, Retrieved from https://kemptechnologies.com/blog/zero-trust-application-security

Cigniti, 2022. Implement Zero Trust to secure your applications, Retrieved from https://www.cigniti.com/blog/zero-trust-secure-applications/

Cisco, 2011. MAC Authentication Bypass Deployment Guide, Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/MAB/MAB_Dep_Guide.html

Crowdstrike, 2022. Healthcare IoT Security Operations Maturity: A Rationalized Approach to a New Normal, Retrieved from, https://www.crowdstrike.com/resources/reports/healthcare-iot-securityoperations-maturity/

Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

F5, 2022. Zero Trust in an Application-Centric World, Retrieved from https://www.f5.com/services/resources/use-cases/zero-trust-in-an-application-centric-world

Friedman, J., 2017. The Definitive Guide to Micro-Segmentation, Illumio. Retrieved from https://www.illumio.com/lp/definitive-guide-to-micro-segmentation

Fruhlinger, J. and Snyder, J., 2021. 802.1X: What you need to know about this LAN-authentication standard, Network World. Retrieved from https://www.networkworld.com/article/2216499/wirelesswhat-is-802-1x.html

Garbis, J. & Chapman J. W., 2021. Zero Trust Security: An Enterprise Guide, Apress Media, California. https://dio.org/10.1007/978-1-4842-6702-8

Gilman, E. & Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Trusted Networks, O'Reilly Media Inc. Sebastopol, CA.

Kumar, S., 2021. Embracing Zero Trust for IoT and OT: A Fundamental Mind Shift, Retrieved from https://www.forescout.com/blog/embracing-zero-trust-for-iot-and-ot-a-fundamental-mind-shift/

Lerman, L., 2021. Zero Trust Approach Can Defend Against IoMT Device Attacks for Healthcare Organizations, Retrieved from https://www.toolbox.com/tech/iot/guest-article/zero-trust-approachcan-defend-against-iomt-device-attacks-for-healthcare-organizations/

McKeon, J., 2021. Exploring Zero Trust Security in Healthcare, How It Protects Health Data, Retrieved from https://healthitsecurity.com/features/exploring-zero-trust-security-in-healthcare-how-itprotects-health-data

Order White Paper,2022. 5 Steps to Zero Trust for Unmanaged and IoT Devices, retrieved from https://resources.ordr.net/whitepapers/5-steps-to-zero-trust-for-unmanaged-and-iot-devices

Palo Alto Networks, 2022. The Right Approach to Zero Trust for Medical IoT Devices, Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/right-approach-zero-trust-medical-iot

Rose, S., 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. National Institute of Standards and Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf

Ross, J., 2022. The Zero Trust Approach to Data Management, Retrieved from https://thenewstack.io/the-zero-trust-approach-to-data-management/

Study CCNA.com, 2022. Cisco CCNA Study Notes, Retrieved from https://study-ccna.com/802-1xauthentication/