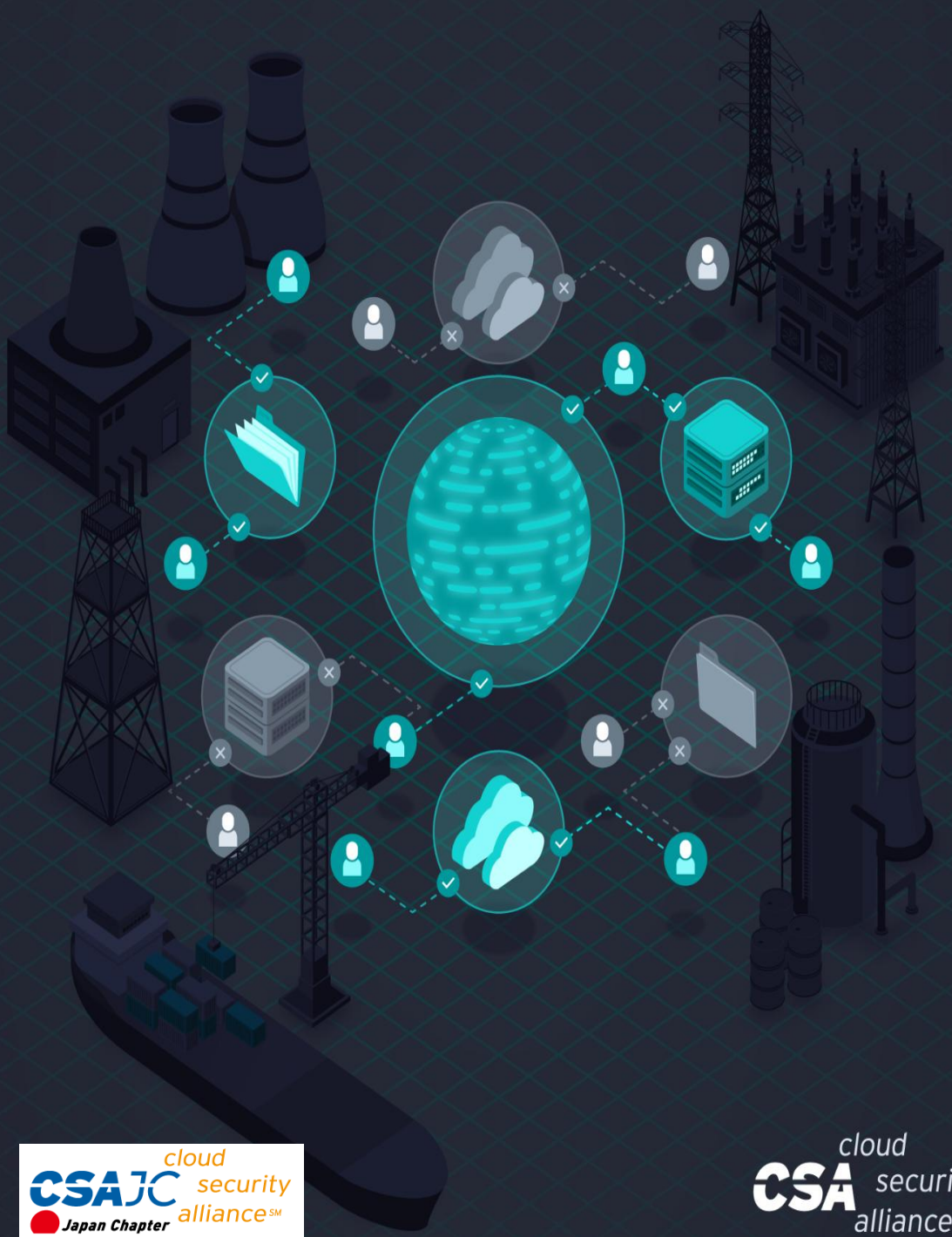
重要インフラのゼロトラスト・ガイダンス



CSAJC cloud security alliance Japan Chapter

cloud security alliance®

The permanent and official location for the CSA Zero Trust Working Group is
https://cloudsecurityalliance.org/research/working-groups/zero-trust/

日本語版提供に際しての告知及び注意事項

本書「重要インフラのゼロトラスト・ガイダンス」は、Cloud Security Alliance (CSA)が公開している「Zero Trust Guidance for Critical Infrastructure」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
2025年01月14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

「重要インフラのゼロトラスト・ガイダンス」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
井上　尚人
笠松　隆幸
諸角　昌宏
山﨑　英人
山下　亮一

Acknowledgments

ゼロトラストの研究とガイダンスの範囲は、必然的にクラウドとオンプレミス環境、モバイルエンドポイントを含み、モノのインターネット（IoT）と運用技術（OT）に適用されます。CSAゼロトラスト（ZT）ワーキンググループの目標は以下の通りです。

- 情報セキュリティ(InfoSec)に対する現代的で必要かつクラウドに適したアプローチとして、ゼロトラストのベストプラクティスを共同で開発し、認知度を高めます。
- ソートリーダーシップを発揮し、さまざまなZTアプローチの長所と短所について業界を啓蒙することで、組織がそれぞれのニーズと優先事項に基づいて十分な情報に基づいた意思決定を行えるようにします。
- 成熟したゼロトラスト実装のアーキテクチャと実装アプローチに関して、意図的に製品およびベンダーに中立的なアプローチを取ります。
- 製品およびベンダーに中立的でありながら、ゼロトラストに関する技術的に健全な立場を取り、擁護可能な提案を行います。
- 本ワーキンググループは、ゼロトラストの柱に沿った9つの異なる作業の流れで構成されています。
- この文書のリードワークストリームは、Jennifer "JJ" MinellaとJoshua Woodruffが率いるZT4 - Devicesです。

Lead Authors

Jennifer Minella
Joshua Woodruff

Contributors

Dr.Ron Martin
Mark Fishburn
Michael Roza
Philip Griffiths
Roland Kissoon
Anna Pasupathy
Shamik Kacker
Rajesh Murthy
Samia
Oukemeni
Gaurav
Agarwaal Shruti
Kulkarni Nathan
Moser

Reviewers

Erik Johnson
Jason Garbis
John Kindervag
Chandra Rajagopalan
Will Schmitt
Alex Sharpe
Karen Uttecht
Annie Weathers
Will Schmitt
Mike Vo
Matthew Rogers
Vaibhav Malik
Mehmet Yilmaz
Venkatesh
Gopal

CSA Global Staff

Erik Johnson
Stephen Smith

Additionally the CSA would like to thank the following valued collaboration partners for their interest in, contributions to and review of this document:

- US Department of Defense (DoD)
- US Cybersecurity and Infrastructure Security Agency (CISA)
- US National Security Agency (NSA)
- MIT Lincoln Labs
- Mitre Corporation
- Johns Hopkins University APL

目次

要旨

本書は、運用技術（OT）および産業制御システム（ICS）におけるゼロトラスト（ZT）原則の重要かつ包括的な適用について掘り下げます。これは、従来の情報技術（IT）セキュリティ手法と、重要インフラ（CI）分野におけるOT/ICS特有の要求とのギャップを埋めることを目的としています。本書では、これらの環境に固有の明確な課題とアーキテクチャを認識し、ZTの基本概念を明確にするだけでなく、これらの原則をOT/ICS環境で効果的に実施するためのロードマップを提供します。このロードマップは、「NSTAC Report to the President on Zero Trust and Trusted IdentityManagement」で概説されている 5 段階のプロセスに基づき、プロテクトサーフェスの定義から継続的なモニタリングと保守に至るまでの体系的なアプローチを採用しており、急速に進化するデジタルテクノロジーと脅威の状況の中で CI のレジリエンスとセキュリティを確保します。

対象読者

主な対象読者は、次のようなセキュリティの専門家です：サイバーセキュリティアーキテクト、セキュリティエンジニア、SOCアナリスト、ZTプラクティショナー、運用技術（OT）および産業制御システム（ICS）のオペレータおよびエンジニア、IT担当者、ZT戦略および/または運用技術を監督するエグゼクティブステークホルダー。

二次的な対象読者は、最高情報セキュリティ責任者（CISO）、脅威モデラー、インシデントマネージャー、監査役、ビジネスおよび運用システムオーナー、コンプライアンス責任者、リスクマネージャー、ネットワーク管理者、ITコンプライアンスアナリスト、データプライバシー専門家、およびこの分野のソリューションや技術を提供するベンダーです。

はじめに

目標

本書の目的は、対象読者に対して、運用技術（OT）と産業制御システム（ICS）に焦点を当て、重要インフラ（エネルギー、水、輸送、医療など）に対するZT原則の検討と適用について教育することです。このガイダンスは、サイバーセキュリティポリシーとコントロールを担当するチームと、OTとICSのシステム所有者とオペレータとの間のコミュニケーションとコラボレーションのためのツールとして機能すべきです。特にCI分野におけるOT/ICS資産のセキュリティ確保には、部門を超えたチーム間の教育と協力が必要です。

本書のスコープ

本書のスコープは、特に、運用技術（OT）及び産業制御システム（ICS）の領域におけるゼロトラストセキュリティフレームワークの運用を中心としたものです。本書は、CI環境に合わせた実践的な戦略と具体的な方法論を明らかにすることを目的としています。本書では、ネットワーク設計、デバイスの異種性、特定のセキュリティ要件などの側面に焦点を当て、従来のITシステムとOT/ICSシステムの本質的な違いを詳細に検証しています。その後、段階的な実施ガイドへと進み、これらのユニークな環境におけるZTモデルの展開の各段階について、実用的な洞察を示しています。これには、重要資産の特定、データフローのマッピング、ZTアーキテクチャ（ZTA）の構築、ポリシーの策定、OT/ICSコンテキスト内での継続的モニタリングの包括的な理解に関する具体的なガイダンスが含まれます。主にセキュリティアーキテクト、OT/ICSオペレータ、およびCIの意思決定者を対象とした本書は、セキュリティが最重要でありながら明らかな困難が伴うセクターにおいて、ZTの原則を適応・適用するための包括的なマニュアルとして機能します。

ゼロトラストとは何ですか？

いかなるユーザーや資産も暗黙のうちに信頼されるべきではないという考えを前提としたサイバーセキュリティ戦略です。情報漏洩がすでに発生している、または今後発生することを前提としています。したがって、企業の境界で実行される1回の検証でユーザーに機密情報へのアクセスを許可すべきではありません。その代わり、各ユーザー、デバイス、アプリケーション、およびトランザクションを継続的に検証する[1]必要があります。

従来の中央集権的で信頼に基づく「城と堀」のような物理的なネットワーク境界セキュリティアーキテクチャは、今日の分散化されたコンピューティング環境やリモートワークフォース環境ではますます効果がなくなっています。

インターネット接続を多用する、高度に分散した現代の企業ネットワークにおいて、技術的または人的な脆弱性をエクスプロイトすることに対して、洗練された脅威アクターの手口はますます巧妙になっています。

[1] NSTAC Report to the President on Zero Trust & Trusted Identity Management, pg.1 & CSA definition of Zero Trust

成功するサイバー攻撃は、一般的に何らかの方法で信頼をエクスプロイトします。このため、デジタルシステム内の「信頼」は、緩和・管理されるべき危険な脆弱性となります。ZTでは、すべてのネットワーク資産とパケットは暗黙のうちに信頼されず、システムを流れる他のすべてのパケットと同じように扱われます。信頼レベルはゼロと定義され、それゆえゼロトラストと呼ばれています。

ZTは、クラウド／マルチクラウド（あらゆるサービスモデル）、オンプレミス／ハイブリッドシステム、社内外のパートナー／関係者ユーザー（組織管理およびBYOD（Bring Your Own Device））のエンドポイントを包含し、運用技術（OT）、産業制御システム（ICS）、およびモノのインターネット（IoT）を含み、場合によっては物理的なセキュリティにまで及ぶ、拡張可能で全体的な企業セキュリティ戦略です。その結果、ZTは一歩ずつ登っていくべき山に例えられています[2]。これらの原則は、Cloud Security Alliance（CSA）のゼロトラスト（ZT）ガイダンスの共通テーマです。

エグゼクティブサマリー

ほとんどの国では、公共サービスの健全性は、セキュアでレジリエントな重要インフラ（CI）に依存しています。これらのインフラストラクチャは、その機能停止や破壊が国家の安全保障、経済、および社会福祉に深刻な影響を及ぼすことから、重要とみなされます。オペレーショナルテクノロジー（OT）システムは、世界中のCIのバックボーンとして機能しています。

「OTは、物理的環境と相互作用する（または物理的環境と相互作用するデバイスを管理する）プログラム可能なシステムまたはデバイスを幅広く包含します。これらのシステム/デバイスは、デバイス、プロセス、およびイベントを監視および/または制御することにより、直接的な変化を検出または引き起こします。例えば、産業制御システム（ICS）、ビルディングオートメーションシステム、輸送システム、物理アクセス制御システム、物理環境監視システム、および物理環境測定システムなど。」[3]

重要インフラセクター

エネルギー、交通、通信、水供給、およびヘルスケアに至るまで、CI部門は現代文明が依存する重要な枠組みを総合的に構成しています。

世界各国の政府は、情報通信が直面する多面的な脅威への警戒を強めています。このような意識の高まりは、実際の侵害だけでなく、「環境寄生型」テクニックを採用する洗練された脅威アクターの発見からも生じています。このような敵対者は、インフラストラクチャ自体の中にある正当なツールやプロセスをエクスプロイトするため、検知や緩和が特に難しくなります。このような手口は、従来のセキュリティ対策を超えた包括的な保護戦略の必要性を強調しています。

米国大統領科学技術諮問会議（United States President's Council of Advisors on Science and Technology（PCAST）)は、国家のサイバーフィジカルシステムを強化するための戦略をまとめた報告書を発表しまし

[2] CISA Zero Trust Maturity Model
[3] NIST Guide to Operational Technology (OT) Security: NIST SP 800-82r3

た[4]。

PCASTの提言は、CIのレジリエンスを強化するための包括的なアプローチを提示しています。彼らは、明確なパフォーマンス目標の設定、脆弱性に関する研究の強化、および脅威の先を行くための国による観測所の設立を提唱しています。報告書はまた、組織の縦割りを打破し、政府の支援を強化し、業界のリーダーたちに説明責任を果たさせることを強調しています。これらの提案は、自然災害やサイバー攻撃、人為的ミスに直面した場合でも、重要なサービスが逆境に耐え、円滑に稼働し続けることを保証することを目的としています。

グローバルの重要インフラセクターに関する調査

CIセクターは、国家安全保障、公衆衛生、安全、および経済的安定にとって重要であると認識されており、多様な産業を網羅しています。

米国では、CISA（Cybersecurity and Infrastructure Security Agency）が現在16のセクターを重要インフラとして認定しています[5]。世界各地で、政府や地域主体は、自分たちにとって最も意味のある方法でCIセクターを定義しています。これらの多くは、 International Critical Information Infrastructure Protection（CIIP）の報告書[66]で見ることができます。2008年に発行されたCIIPは、25カ国と7つの主要な国際機関のCIセクターを詳細に網羅した、他に類を見ないリソースです。その包括的な分析は、世界のCI保護に関する貴重な洞察を提供しています。

世界中で広くCIとみなされている一般的なセクターには、以下のようなものがあります（ただし、これらに限定されるものではありません）。

1. エネルギー（ガス、石油燃料、製油所、パイプライン、発電、配電・送電）
2. 水（給水、排水処理）
3. 銀行・金融（銀行、金融機関、取引所）
4. 緊急サービス（警察、消防、緊急対応）
5. ヘルスケア（病院、診療所、研究所）
6. 食料供給（生産、貯蔵、流通）
7. 通信（電気通信、電話、ファックス、インターネット、ニュースメディア）
8. 公共の場（スポーツアリーナ、スタジアム、集会所、礼拝所）
9. 輸送およびロジスティクス（航空、道路、鉄道、海上、船積み／貨物／郵便サービス）
10. 重要な製造業（自動車、化学、エレクトロニクス、製薬など）
11. 政府・行政（省庁、システム、施設など）
12. 教育（学校、大学）

これらは世界共通のセクターですが、米国においてCISAは以下のようなものも含めており、その多くに適用可能です。

1. 化学（基礎化学、特殊化学、農業化学、生活化学）

[4] PCAST Releases Report on Strategy for Cyber-Physical Resilience
[5] Critical Infrastructure Sectors | CISA
[6] International CIIP Handbook 2008/2009

2. 商業施設（娯楽・メディア、ゲーム、宿泊、野外イベント、集会、不動産、小売、スポーツリーグ）
3. ダム（水力発電、給水、灌漑、洪水調節、河川航行、産業廃棄物管理、レクリエーション）
4. 軍/国防部門と国防産業基盤（軍を可能にする世界的な産業サプライチェーン）
5. 情報技術（テクノロジーへの依存度が高まっているため、国家の安全保障、経済、公衆衛生・安全の中心的存在）
6. 原子炉、材料、廃棄物（発電炉、研究・試験炉、活動中の核燃料サイクル施設、および放射性線源の認可ユーザー）

2024年4月、バイデン米大統領は「National Security Memorandum on Critical Infrastructure Security and Resilience」 を発表し、これらの重要セクターを保護するための連邦政府の方針と責任を更新しました。

世界各国は、自然災害とテロやサイバー攻撃を含む人的脅威の両方から自国のCIを保護する責任を負っています。こうした重要な資産の所有モデルは世界的にさまざまで、公共と民間の利害関係者が混在しています。多くの国では、情報収集施設のかなりの部分が民間で所有・運営されており、保護活動に複雑さをもたらしています[7]。

CI および OT/ICS環境におけるZT

CIは、自然および人為的なさまざまな脅威に直面している地域社会の幸福を維持し、国家のレジリエンスを確保するために極めて重要です。そして今、社会がますます相互接続を深め、技術の進歩に依存するようになるにつれて、CIの保護は世界的な必須事項へと進化し、それに伴ってZTの必要性も高まっています。

CIは多くの場合、複雑で相互接続されたネットワークで構成されており、インターネットへの接続が進んでいるため、単純かつ巧妙なサイバー攻撃を受けやすくなっています。ZTのアプローチは、ユーザー、デバイス、アプリケーションから要求されたアクセスを承認し、すべてのインタラクションとアクセス要求が徹底的に認証され、コンテキストが検証されることを保証します。

残念ながら、多くのOTやICS環境はレガシーシステムや特殊なプロトコルに大きく依存しており、パッチやアップグレードが容易でないクローズドなシステムであることが広く知られています。また、多くの組織では、OT/ICS資産の正確なインベントリを把握しておらず、運用やセキュリティの担当者がOT/ICS資産を十分に理解していないことも少なくありません。

以下のセクションでは、OT/ICS 環境で ZT を実施する際に適用される主なテーマと傾向について説明します。

[7] Critical Infrastructure Protection: CISA Should Improve Priority Setting

重要インフラに固有の脅威ベクトル

数十年にわたるCIへの攻撃の歴史は、好奇心旺盛なティーンエイジャーからハクティビズム、さらには政治的動機による国家を標的にした攻撃まで多岐にわたり、これらの部門が直面する脅威の多様性と進化を浮き彫りにしています。例えば、多くのOTデバイスにはIPアドレスや標準オペレーティングシステムがないため、従来の脆弱性パッチ適用戦略が有効でなかったり、適用できなかったりします。

攻撃者の動機にかかわらず、CIセクターは地域社会や経済における重要な役割を担っているため、格好の標的となります。このような環境が悪意のある行為者を惹きつける主な理由は以下のとおりです。このリストは脅威のベクトルに焦点を当てていますが、OTのその他の課題については、「OTとITのアーキテクチャとテクノロジーの違い」のセクションでさらに詳しく説明しています。

- 規制とコンプライアンスの圧力：CIを管理する複雑な規制の状況は、意図せず脆弱性を生み出しかねません。コンプライアンス重視のセキュリティ対策は、必ずしも最も効果的なサイバーセキュリティの実践と一致するとは限らず、攻撃者が悪用できるギャップを残す可能性があります。
- インサイダーの脅威：従業員、請負業者、または内部情報に精通し、CIシステムにアクセスできるその他の個人は、特有のリスクをもたらします。悪意があろうと過失があろうと、内部関係者はセキュリティ対策を迂回し、重大な損害や混乱を引き起こす可能性があります。
- サプライチェーンの脆弱性：CIは多くの場合、ハードウェアとソフトウェアの両方のコンポーネントについて、複雑でグローバルなサプライチェーンに依存しています。サプライチェーンにおける侵害は、システムに脆弱性や悪意のある要素を持ち込む可能性があり、直接侵入することなくセクター全体に影響を及ぼす可能性があります。
- 大きな影響：CIを混乱させたり損傷させたりすることは、公共の安全、国家安全保障、経済に重大な影響を及ぼします。攻撃者は、広範囲に混乱を引き起こしたり、重要なサービスを中断させたりすることを目的としています。
- 相互接続と相互依存システム：CIセクターは相互の関連性が高く、しばしば相互依存しています。あるエリアでの侵害は、ラテラルムーブメントや相互依存的なつながりによって他のエリアに連鎖し、攻撃の影響を増幅させるドミノ効果をもたらします。
- 経済的動機：CIに対する攻撃の中には、金銭的な動機によるものもあります。攻撃者は、身代金を支払わなければ必要なサービスを停止させると脅すことで、組織や国家から金銭を脅し取ろうとする場合があります。
- サイバースパイ活動：国家やサイバー犯罪者は、スパイ活動の目的でCIを標的にすることがあります。産業システムに不正アクセスすることで、その国の能力、脆弱性、戦略的資産に関する情報を収集することができます。
- 政治的動機：CIへの攻撃は、政治的な動機で国家を不安定化させたり、特定の要求を満たすよう政府に圧力をかけたりすることがあります。その背景には、地政学的な緊張や紛争、イデオロギーの対立があるのかもしれません[8]。
- 攻撃されやすい：多くのCIシステムは、最新のサイバーセキュリティを考慮して設計されていない

[8] DoD Zero Trust Symposium 2024 - DAY 2 - Defense Acquisition University

レガシーテクノロジーを使用しています。これらのシステムには、攻撃者が悪用できる脆弱性がある可能性があり、セキュリティ対策や警告が限られています。

- 国家間のサイバー戦争：国家がサイバー戦争に関与する可能性があり、CIを戦略的な標的と見なします。敵のインフラを破壊することは、従来の軍事的手段に頼ることなく、紛争において戦略的優位に立つための手段となり得ます。
- 物理的なセキュリティ： OT/ICSは、その露出された、しばしばガードされていない性質により、悪意のある行為者を惹きつけ、物理的な脆弱性を悪用した直接的な改ざん、スパイ行為、妨害行為の機会を提供します。物理的なインフラへの攻撃は、最も簡単でありながら最も影響力のある攻撃[9]であることがよくあります。

ランサムウェアとデータ流出は、近年、CIに影響を与える攻撃として流行しています。しかし、新たなツールキットが導入され、脅威行為者の政治的動機が産業制御システム（ICS）を無効化または混乱させる目的で標的とするように進化するにつれて、この傾向は変化する可能性があります。また、ソーシャルエンジニアリング、物理的攻撃、カードリーダーやセキュリティカメラ・システムなどの脆弱な付帯サービスプロバイダーを利用した攻撃など、これらの部門は一般的に高度ではない攻撃の被害者となっています。

OT/ITとデジタルトランスフォーメーションの融合

近年の技術の進歩により、私たちの生産性と能力は向上していますが、脅威の状況も同様に進化しています。さまざまなセキュリティレベルや成熟度が異なるシステムが相互接続されている場合、それらのシステム間で適切かつ信頼性の高いセキュリティ管理を実施することは大きな課題となります。

特に、過去20年間におけるインターネット、クラウド、産業用 IoT（IIoT）の成長とユビキタス化、およびそれらの相互接続性により、重要システムへの多数のアクセスポイントが生まれ、以前はそれほど侵入されにくかった環境に複数の穴が開いてしまいました。デジタルトランスフォーメーションの導入を急ぐあまり、生産性、効率性、俊敏性を高めるためにこれらのシステムが相互接続され、これらのシステムをさらに無防備な状態にさせました。加えて、従来のサプライチェーンネットワークに内在していた弱点は、攻撃者が一旦侵入すると、より広範なアクセスを可能にする接続されたシステムによって更に悪化しました。

歴史的に、OTは他のネットワークから物理的に完全に切り離された「エアギャップ」でした。現在、エアギャップシステムは産業界ではほとんど見られません。最新のシステムは、多くの場合、内蔵ワイヤレスアクセス、クラウドやその他のインターネット接続サービス、SaaS（Software-as-a-Service）アプリケーションを介して相互接続されています。レガシーシステムでも、バックアップ、メンテナンスのアップグレードやパッチ、データ転送のために、メンテナンス用ノートパソコンやリムーバブルメディアとインターフェースをとります。セキュリティ制御を作成し適用する際には、こうしたエアギャップシステムから完全に統合されたネットワークへの移行と、それに伴うリスクを考慮しなければなりません。

ここでは、OT/ICS環境のセキュリティ確保に携わるITおよびセキュリティの専門家が考慮すべき重要な点をいくつか紹介します。

[9] Third North Carolina Power Substation Targeted by Gunfire as BPS Physical Security Concerns Mount

テクノロジーの進歩

テクノロジーの混乱により、こうしたシステムは変化を余儀なくされています。かつては隔離されていたエアギャップシステムも、今ではOT環境内で相互接続が進んでいます。シリアル接続からイーサネット接続への移行、OTコンポーネントへのワイアレスアダプタの組み込み、メンテナンス用デバイスとのインターフェースにより、接続された環境が生じていますが、潜在的に脆弱な状況を助長しています。かつては安定していたこれらのシステムも、今ではダイナミックに相互接続されたネットワークに接続されており、新たなリスクや課題への適応を余儀なくされています。

重要インフラの相互接続性

崩壊しつつある境界と高度に相互接続されたシステムにより、CIセクターは相互依存的で緊密に結合しています。1つの障害が連鎖反応を引き起こし、他の障害を引き起こす可能性があります。例えば、電力会社は他のほとんどのセクターに電力を供給しており、重要度の高い企業でさえ、バックアップ発電能力は限られています。水はサーバーの冷却、ミサイルの発射、産業プロセス用の蒸気生成に不可欠です。製油所はパイプラインシステムから原油を取得し、パイプラインシステムを通じて送り出します。これらのセクター間の依存関係は、それぞれ異なるエンティティ間のデータフローを含み、あるセクターへの攻撃が複数の業界や企業への連鎖的な混乱を引き起こす可能性がある複雑な相互関係の網を形成し、最初の標的をはるかに超えて影響が拡大する可能性があります。

OTとITの統合

OTとITシステムの統合は、リモートアクセス、システム監視・制御、データ集約・分析、レポート作成の必要性によって加速しています。インダストリー4.0に代表される統合とコンバージェンスは、単純なデータ収集にとどまらず、双方向の通信と制御を含みます。例えば、停電の通知や対応には、多くの場合、運用システムからのデータをIT管理の通信チャネルに取り込む OT/ITのシームレスな統合が必要です。

OTデータは、高度なモニタリングや分析を行うためにクラウドプラットフォームに送信されるケースが増えています。この傾向は、より洗練された双方向のデータフローへと進化しており、クラウドで処理された洞察に基づいてリアルタイムで調整できるようになっています。その代表的な例が、製造から輸送、流通に至る商品の追跡であり、特に食品業界や製薬業界では特に重要です。ここでは、データがOTシステム（生産ライン、輸送センサー）とITシステム（在庫管理、物流計画）の間を絶えず流れ、効率性とトレーサビリティを向上させるデジタルスレッドを作り出します。

この統合により、効率性の向上やデータに基づく意思決定など、大きなメリットがもたらされる一方で、接続性の向上や従来のOTとITの境界の曖昧さにより、新たな脆弱性も生じます。課題は、コンバージド・インフラストラクチャ全体で堅牢なセキュリティを維持しながら、これらの利点を活用することにあります。

全体として、企業はOT/ICSシステムの効率を高め、これらの資産をより広範なビジネス目的に活用しようと努めており、内部ネットワークと外部システムの両方への接続が必要です。このような状況において、ZTはビジネスの成長を安全に加速させるための大きな付加価値を提供します。ZTアプローチを採用することで、システムの安全性を確保し、監査、法律、コンプライアンス要件を満たし、サイバー攻撃から身を守ることができます。堅牢なセキュリティを維持しながら、刻々と変化する環境の中で迅速に目標を追求するこ

とができます。

重要なのは、ZTは新しい実装に限定されないということです。ゼロトラストアーキテクチャー（ZTA）の導入が成功すれば、当然、新規プロジェクトの「セキュア・バイ・デザイン」アプローチにつながりますが、既存のシステムを大幅に強化することもできます。ZTの原則を慎重に適用することで、組織はレガシーシステムの「セキュア・バイ・レトロフィット」を実現し、新規および既存のインフラストラクチャのセキュリティポスチャを強化することができます。この2つの適用可能性により、ZTはOT/ICS環境における包括的なセキュリティ向上のための強力な戦略となっています。

OT とITの目的の違い

OT/ICS環境がどのように、そしてなぜそのように動作するのかを十分に理解するには、従来のエンタープライズIT環境とは大きく異なる、これらのシステムの主要なビジネス目標と運用文化を理解することが不可欠です。

CIとそれに依存するOT/ICSシステムは、定義上、ミッションクリティカルです。サイバーセキュリティを重視したCIAトライアッド（機密性、完全性、可用性）を念頭に設計されることが多いITシステムとは異なり、OT/ICSシステムは主に信頼性と安全性を重視して設計されており、機密性と完全性はあまり重視されていません。この違いは、継続的かつ安全な運用を維持することが極めて重要であり、ダウンタイムが深刻な結果をもたらしかねないOT/ICS環境の運用に重点を置いていることに起因しています。これらのシステムでは、人命を守り、人と環境の両方への物理的な危害や損害を防ぐことに重点を置き、安全性が最優先されます。

ここでは、OT/ICS 環境を保護する専門家が考慮すべき関連事項をいくつか示します。

レジリエンス、アップタイム、安全性が第一目標

クリティカルなシステムでは、保守やメンテナンスの機会は限られています。新しいツールや技術を重要なシステムやレガシーシステムに導入するには、導入が安全性や運用に支障をきたさないことを確認するための慎重な評価とテストが必要です。サイバーセキュリティのインシデントが発生した場合、それ以上の被害や影響を防ぐには、これらの重要なサービスやシステムを停止させたり、オフラインにしたりする必要があります。

システムは静的、複雑、高価

CIシステムの特徴は、コストが高く、寿命が長く、設計が複雑であることです。これらの要素と、長い導入プロセスが相まって、その静的な性質を助長し、進化する脅威への適応性を低下させています。

多くの場合、資産は意図された寿命をはるかに超えて稼働し、時にはOEM（Origginal Equipment Manufacturer）のサポートサイクルを超えて稼働することもあります。これらのシステムの交換やアップグレードは、広範囲に及ぶ設計、エンジニアリング、調達、テストの各段階を含む複雑で時間のかかるプロセスです。これは、エラーが安全、健康、環境に重大な影響を与える可能性がある重要なアプリケーションで

は特に重要です。

その結果、古いシステムは、潜在的なセキュリティリスクにもかかわらず、慎重なリプレースプロセスが進行している間、インフラの寿命を延ばすために維持されることがよくあります。このため、業務継続と必要なセキュリティのアップグレードのバランスを取るという、独特の課題が生じます。

さらに問題を複雑にしているのは、多くのOTシステムが独自のプロトコルを使用しているため、定期的なアップデートが難しく、攻撃者が悪用できる脆弱性を生み出していることです。この複雑さが、OT/ICS環境のセキュリティ確保と近代化という課題を更に複雑化しています。

OT とITのアーキテクチャとテクノロジーの違い

OT/ICSとエンタープライズIT環境の全体的な目的の違いに加え、少なくともOT/ICSシステムの一部では、使用されるアーキテクチャやテクノロジーにも大きな違いがあります。 上記の「重要インフラに固有の脅威ベクトル」のセクションで述べたように 、これらの違い、OT/ICSに特有の更なる課題の詳細を提供します。

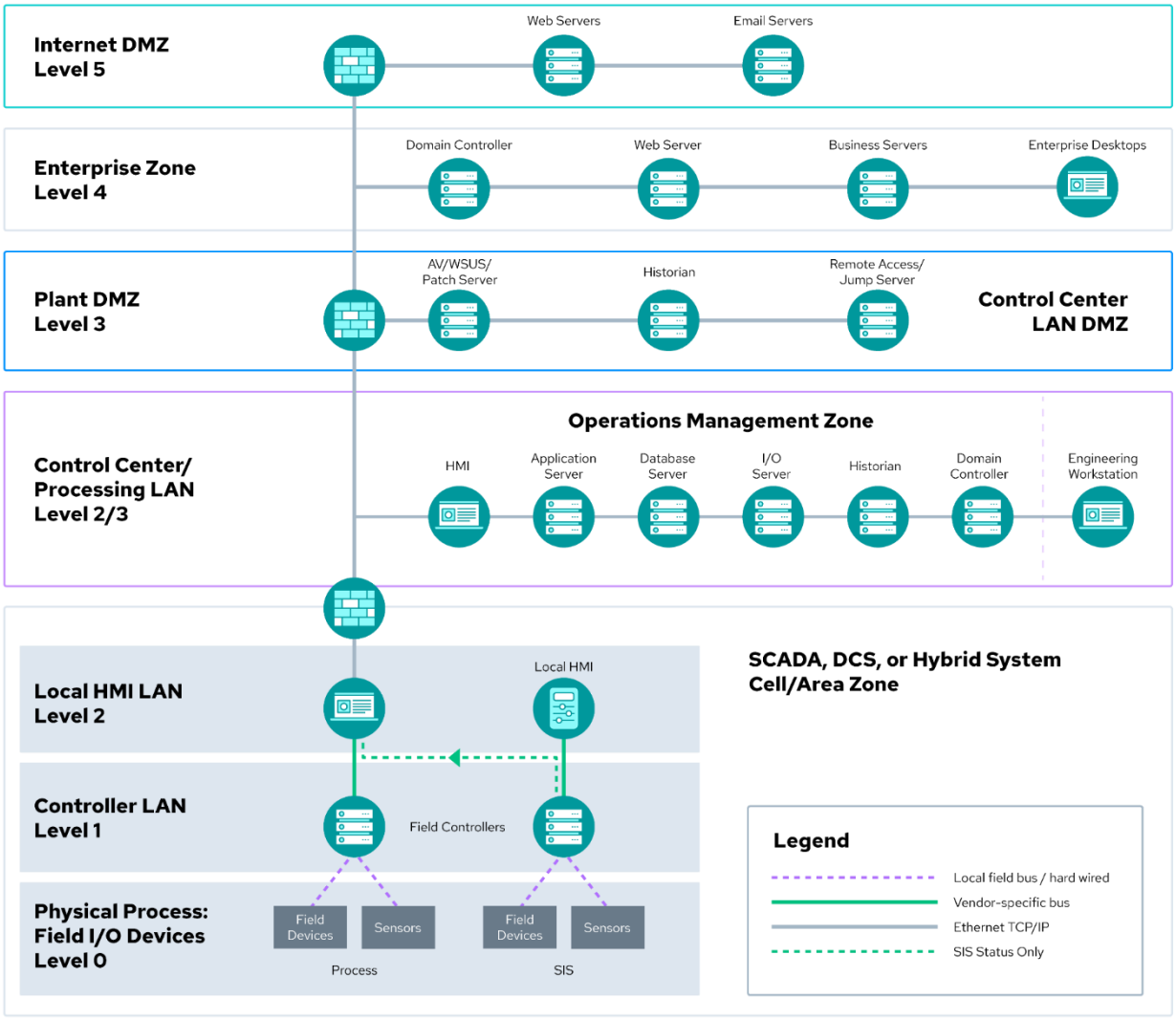
なぜなら、ZT のような包括的な概念はすべてのセグメントに適用できる（適用すべき）ものの、セキュリティポリシーの詳細や管理策の適用方法、運用方法は異なる可能性があるからです。

例えば、標準的な組織のITサイバーセキュリティポリシーでは、3回失敗したらユーザーをロックアウトすることが規定されています。しかし、OT/ICS環境では、人の安全が脅かされる緊急時に、システムオペレータがアクセスする必要のあるHMI（Human-Machine Interface）からシステムオペレータを閉め出すことは、最も避けたいことです。同様に、パッチ適用も企業ITの脆弱性管理の重要かつ一貫した部分です。対照的に、OT/ICS ネットワークでは、パッチを適用することが適切な緩和策となるケースは10%未満であることが多く、多くの報告では4%[10]とかなり低い数値となっています。

ここでは、IT またはサイバーセキュリティの専門家が、OT/ICS 環境のセキュリティを確保する際に直面する可能性のある考慮事項について説明します。

Purdue Model[11]は、OT/ICS 環境内のコンポーネントと接続を可視化するための共通参照モデルを提供します。最新のクラウドやSaaSに接続されたインフラストラクチャを扱うには不十分ですが、このモデルは本書で取り上げたいくつかの基本概念を伝えるツールとして十分に役立ちます。

[10] Dragos 2023 OT Cybersecurity Year in Review
[11] Cloud Industrial Internet of Things (IIoT) - Industrial Control Systems Security Glossary



Purdue Model *サンプル*

レガシーシステムとアプリケーションの普及

Purdue Model のサンプルを見てみると、資産がプロセス実行レベル（レベル0と1）に近ければ近いほど、使用されているシステムやプロトコルが独自性の高いものであることがわかります。しかし、プロセス制御、オートメーション、および管理（レベル2および3）に関わるシステムは、ほとんどの場合、さまざまな種類と世代のWindowsおよびLinuxオペレーティングシステムで構成されています。これらのシステムの多くは、時代遅れまたはベンダーが修正したバージョンのオペレーティングシステムを実行しており、パッチはほとんど適用されず、従来の企業ITシステムやエンドポイントとは異なるプロセスやサイクルに従って保守されています。

レガシーシステムの普及は、時代遅れのオペレーティングシステムやアプリケーションにとどまりません。世界の多くのCI環境では、それらを実行するOT/ICSシステムは、数年単位ではなく数十年単位で耐用年数が予想されるサイバーフィジカル資産で構成されています。

製造オートメーションシステムから発電、廃水処理プラントのポンプや流量センサーに至るまで、コンポーネントは10年、20年、さらには50年にわたり設置・保守される可能性があります。

毎年、OT/ICSネットワークに関する多くの報告書や調査が、これらの環境でレガシーシステムが使用され続けていることを証明しています。これらのシステムのほとんどは、基本的な保護さえ欠いています。例えば、ある報告書[12]はこう示しています：

- 71%が古いオペレーティングシステムを使用しています。
- 66%は自動ウイルス対策をしていません。
- 産業用施設の27%が、少なくとも1つのインターネットに直接接続しています。
- 54%は少なくとも1台のリモートアクセス可能なデバイスを持っています。
- 22%が脅威の指標を示しました。
- 64%が平文のパスワードを持っています。

独自のプロトコルと独自の構成

ITおよびサイバーセキュリティの専門家にとって、OT/ICSの世界をナビゲートすることは、新しいプロトコルを（少なくとも概念的に）理解し、新しい語彙を学び、新しいリスクを理解し、新しいスキルセットを開発することを意味します。

産業用制御プロトコル

OT/ICSデバイスとネットワークは、特に Purdue Model の下位レベルでは、環境に固有のプロトコル群を使用して動作します。例えば、Modbus、PROFIBUS、PROFINET、OPC、MQTT、EtherNet/IP、Fieldbus[13]、RS-485などの組み合わせがあります。

また、プロトコルは十分に文書化されたさまざまな業界標準を使用しているかもしれませんが、OT/ICS資産内の正確な構成は実装ごとに異なり、ベンダーやOTオペレータによって十分に文書化されていない可能性があります。例えば、Modbus は標準ですが、ベンダーやインストーラが特定の PLC の Modbus マッピングをどのようにプログラムしたかは異なる可能性があります。

このため、脆弱性や設定ミスを発見し、管理することが難しくなります。標準的なオペレーティングシステムを実行している資産とは異なり、これらのデバイスはカスタム化されたオペレーティングシステムを搭載していたり、オペレーティングシステムをまったく搭載していなかったりします。たとえあったとしても、稼働時間の制約やインストールができないなどの理由で、ダウンタイムはしばしば選択肢に入りません。

システムの古さと老朽化、そして古い技術によって、改善の余地が少なくなっています。多くの場合、コンポーネントは特定の機能を果たすように設計されており、設計上、機能が制限されています。そのため、計算資源の不足、機能の制限、メモリの制限などの制約により、新しいセキュリティ対策を更新したり追加したりする余地はほとんどまたはまったくありません。

[12] Global IoT-ICS Risk Report (2020)
[13] What Is Fieldbus? Learn the Basics of a Fieldbus Network

暗号化されていない通信

設計上、これらのプロトコルの多く（特にローカル・コントロール・プロセス・ゾーン内で実行するように設計されたもの）は暗号化されていません。OTシステムに暗号化がないため、重要な通信チャネルが傍受や操作にさらされることになります。この脆弱性により、悪意のある行為者は、機密の運用データを盗聴したり、偽のコマンドを注入したり、制御システムとフィールドデバイス間の通信を妨害したりすることができます。このような行為は、産業プロセスを不正にコントロールすることにつながり、操業の中断、機器の損傷、あるいは安全上の危険を引き起こす可能性があります。

しかし、これらのプロトコルの多くは暗号化されるようには設計されておらず、これらのプロトコルに暗号化をオーバーレイすると、リアルタイム通信に依存するOT/ICSシステムでは耐えられない遅延が発生したり、危険な状態になることさえあります。

例えば、暗号化を使用すると通信に遅延が生じ、ICS環境で重要なリアルタイムのオペレーションに影響を与える可能性があります。これらの遅延は、コマンドのタイムリーな実行やシステムの同期に影響を与え、制御プロセスの中断につながる可能性があります。極端な場合、特に発電や化学処理に見られるような緊密に連携したシステムでは、安全機構が遅れたり、意図したとおりに作動しなかったりするシナリオが生まれる可能性があります。

知識とスキルセット

OT/ICSにおける複数世代のハードウェア、アーキテクチャ、テクノロジーは、多方面にわたる幅広い知識を必要とします。OT と IT の間でチームメンバーをクロストレーニングし、常設の部門横断型チームを編成することは、多くの組織がOT/ICSサイバーセキュリティプラクティスを構築する際に成功を収めた戦略です。しかし、このような多様なスキルの統合は大きな課題であり、OTとITの伝統的な隔たりを埋めるには、慎重な計画、リソース、継続的な取り組みが必要です。

追加的な物理的露出

CIにおける重要かつ過小評価されがちな脆弱性は、多くの資産が物理的に露出していることです。安全なデータセンターに収容された従来のITシステムとは異なり、多数のOT/ICSコンポーネントはオープンでアクセス可能な環境に配備されています。風力タービン、電力変圧器、パイプラインのポンプ場、水処理施設などは、遠隔地や一般の人がアクセスできない場所にあることが多い重要資産のほんの一例です。

このような物理的な露出は、以下のような複数のリスクをもたらします。

1. 悪意のある行為者による直接的な改ざんや妨害行為
2. 自然災害や異常気象に対する脆弱性
3. 事故や人為的ミスによる不慮の損害の可能性
4. 敵が物理的な観察を通じて情報を収集する機会

これらの露出した資産を保護するには、物理的なセキュリティ対策と技術的な制御を統合した多層的なアプ

ローチが必要です。これには、境界セキュリティ、監視システム、アクセス制御メカニズム、強化された機器ハウジング、および定期的な物理的セキュリティ監査が含まれます。さらに、レジリエンス計画では物理的脅威とサイバー脅威の両方を考慮する必要があり、包括的なセキュリティ戦略は両領域に同時に対処するものであることを認識する必要があります。

OT/ICS における物理的セキュリティには特有の課題がありますが、本ガイダンスはその一助となります。これから説明するように、「DAAS の要素」として何があるのかを特定し、「ZTMM の柱」を使用してセキュリティ能力を測定し、改善することを含む、以下の 5 段階の実装プロセスを通じて、これらのコンポーネントのそれぞれを歩ませることで、ZT の旅の一部として、これらのコンポーネントのセキュリティを確保する漸進的な道筋ができます[14]。

モニタリングのニーズと課題

OT/ICS環境におけるモニタリングの歴史は古く、主にコンソールやフィールドのオペレータによって観測される運用上の問題に焦点が当てられてきました。しかし、脅威の状況は進化しており、特にサイバー関連インシデントに起因する可能性のある事象の検出において、モニタリング手法の転換が必要となっています。

重要な課題は、OTシステムにおける悪意のある活動に対する包括的なモニタリングの欠如にあります。運用データは注意深く監視されていますが、セキュリティに焦点を当てた監視は遅れをとることがよくあります。このギャップにより、サイバー関連の損害が信頼性の問題や設定ミスに起因すると誤認されることにつながり、セキュリティインシデントの真の性質と範囲を覆い隠してしまう可能性があります。

強化されたモニタリング機能を実装するには、独自の課題があります。ネットワーク監視に必要な新たな接続は、本質的に攻撃対象とデータ露出のリスクを増加させます。しかし、それ以上に懸念されるのは、重要なセキュリティデータがITチームとセキュリティチームによって効率的に収集、一元管理、相関化されていない場合が多いということです。

進めていくには微妙なバランスが必要です。OT環境は、運用の完全性を維持しながら継続的なセキュリティ監視を行うために、より新しいシステムに適応し、統合する必要があります。この進化は、従来のOT監視システムと最新のsecurity information and event management（SIEM）ツールとの相互運用性の向上を求めています。

サプライチェーンの課題

OT/ICS環境では、サプライチェーンセキュリティが大きな課題となります。その一部はITの世界と共通していますが、運用の文脈では増幅されることがよくあります。IT部門がサプライチェーンのセキュリティ問題に直面する一方で、OT部門のサプライヤーは通常、セキュリティよりもビジネス目標や業務機能を優先します。このため、OTのサプライチェーン全体にセキュリティ対策が組み込まれておらず、OT/ICSシステムのより深刻な脆弱性につながる可能性があります。この分野のベンダーは、IT部門ほど強固にセキュリティ問題を報告し、パッチを適用し、対処するプロセスを確立していない可能性があります。その結果、組織はOT/ICSサプライチェーンの細部に特に細心の注意を払う必要があり、IT部門に比べてセキュリティ情報やセ

[14] Zero Trust in the Real World - Physical Security

キュリティ慣行が入手しにくかったり、透明性が低かったりする状況を乗り切らなければなりません。

OT/ICS におけるサプライチェーンの脆弱性の潜在的な影響は、CI と業務の安全性に広範囲に及ぶ可能性があるため、このような監視の強化は極めて重要です[15]。

これらの課題は重大ですが、業界は進化する基準とベストプラクティスで対応しています。例えば、OT/ICSのサプライチェーンセキュリティに関連する規格は、サイバークリティカルなデバイス、ソフトウェア、アップグレードの正式な検証と妥当性確認（V&V）の要件をますます取り入れるようになっています。ISA/IEC 62443の産業用通信ネットワークセキュリティのような規格は、この傾向を象徴するもので、いくつかの制御目標にV&Vを規定しています。これらの新たな標準は、サプライチェーンの脆弱性に対処するための重要な一歩を示すものですが、その実施と有効性はOT/ICSの分野や地域によって異なります。サプライチェーンのセキュリティ強化を目指す企業は、ZTの取り組みと並行した包括的なリスク管理戦略の一環として、これらの標準に精通する必要があります。

その他の相違点と考慮点

企業の IT システムと OT/ICS システムの細かな技術的差異を挙げればきりがありませんが、OT/ICS のサイバーセキュリティを管理する IT およびセキュリティの専門家にとって斬新と思われる追加的な考慮事項には、次のようなものがあります。

- **リスク**： ITとOTの最大の違いの一つはリスクです。CIシステムの故障は、経済的損失や国家安全保障への影響など、ITシステムが経験する影響に加え、安全、健康、環境への影響につながる可能性があります。
- **規模**：これらのシステム（特に電力、電気通信、公共事業分野）は、地域、地方、国家、国際的な境界線にまたがる広い地理的範囲に広がっている可能性があります。技術的、運用的な違いだけでなく、法律や規制に関する独自の考慮事項が生じることもあります。
- **複雑さ**：OT/ICS環境は、その構成と運用の相互接続性により、事実上システム・オブ・システムであり、通常、OT/ICSシステムがIT監視制御サブシステムを持つ場合のように、それぞれが特定のタスクのために設計されたさまざまなサブシステムで構成されています。各サブシステムは、効果的に機能するために協調して動作する必要がある独自のハードウェア、ソフトウェア、および運用プロトコルを持っています。これらのサブシステムは独立したものではなく、互いに依存しあって機能しています。1つのシステムの故障や誤動作が他のシステムに連鎖的な影響を及ぼす可能性があるため、メンテナンスやトラブルシューティングが一層複雑になります。
- **長寿命**：OT/ICSインフラは、最新システムとレガシーシステムやコンポーネントが混在していることがよくあります。こうした構造は、時間の経過とともに出現し、変化していきます。このようなシステムが50年以上存続することも珍しくありません。部品の通常の寿命は10年から15年です。このようにシステムの寿命が延びることは、ビジネスにとって本質的なリスクと結果をもたらします。
- **所有権**： OT/ICSシステムの所有者や権限が1つであることはほとんどありません。公的所有と私的所有が混在している場合もあり、営利企業と非営利企業の両方がこれらのシステムを運営していま

[15] Pagers attack brings to life long-feared supply chain threat

す。これは、システムの最適化や更新を決定した場合に、新たな決定ポイントやプロセスを導入することになるため、注意が必要です。

CIセクター、OT/ICSの特徴的な課題、デジタルトランスフォーメーションがOTとITの融合に与える影響について検討した後、ZTの原則の適用に移ります。本ガイダンスでは、実績のある5つのステップのプロセスを活用して、ZT戦略を使用してOT/ICS環境を効果的に強化する方法について詳しく説明します。

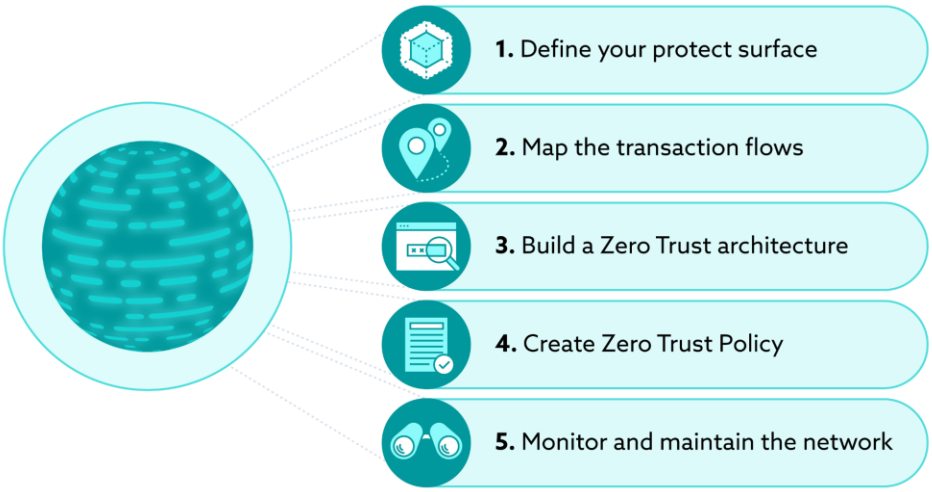
ゼロトラスト実施プロセス

5段階の実施プロセス

NSTAC Report to President on Zero Trust and Trusted Identity Management[16]は、CSA の Zero Trust 研究が活用され、連携された基礎的な参考文書です。本書は、優れた背景と概要を提供し、さまざまなZTの参考文献やアプローチを比較対照しています。また、段階的かつ反復的な実行に適した、技術にとらわれない再現可能な以下の5段階のZT実装プロセスも紹介しています。

1. プロテクトサーフェスの定義
2. トランザクションフローのマップ
3. ゼロトラストアーキテクチャの構築
4. ゼロトラストポリシーの策定
5. ネットワークの監視と保守

この文書では、スコープされたCI技術とセクターの文脈で、この5つのステップの旅について説明します。



[16] NSTAC Report to the President on Zero Trust and Trusted Identity Management

インクリメンタルと反復実行

5つのステップ・プロセスによって、ZTの旅でどのように即時の行動と継続的な改善が可能になるかを探ってみましょう。

ステップ**1**：プロテクトサーフェスを定義します：包括的な資産の発見

まず、組織全体にわたる事業資産と業務資産の棚卸しと評価を行います。この基本ステップにより、リスクに基づく優先順位付けが可能になり、的を絞ったZTの実施に向けた段階が整います。

ステップ**2-5**：焦点を絞った反復的な改良

特定されたプロテクトサーフェスごとに、手順2～5を繰り返します。この反復的なアプローチにより、洞察を得て戦略を洗練させながら、ZTのポスチャを継続的に強化することができます。

このプロセスにより、組織はすぐに着手して継続的に改善し、ZTの導入を進化する発見に適応させることができます。後ほど、「クロール、ウォーク、ラン」アプローチについて説明します。これは、組織が低リスクの部分から反復し始めて、徐々に複雑なシステムに取り組むことを可能にするものです。

これらのステップを OT/ICS 環境に適用するための詳細なガイダンスに入る前に、ZT の成熟度レベルを特定し、目標を設定するためのアプローチについて説明します。

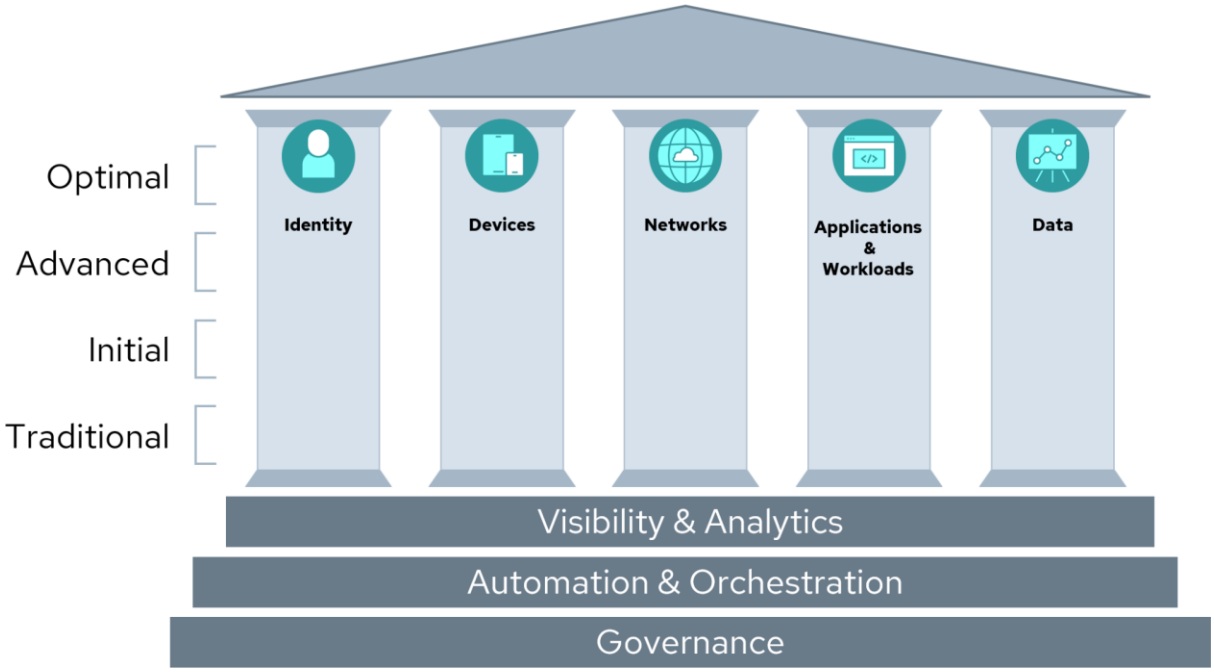
CISA ゼロトラスト成熟度モデル(ZTMM)

CISA（Cybersecurity and Infrastructure Security Agency）はZTMM（Zero Trust Maturity Model）[17]を発表しており、これは5つの柱にまたがる実装の段階を表し、時間の経過とともに 4 つの成熟段階を経て最適化に向けての進歩をめざします。

CISA ZTMMの柱

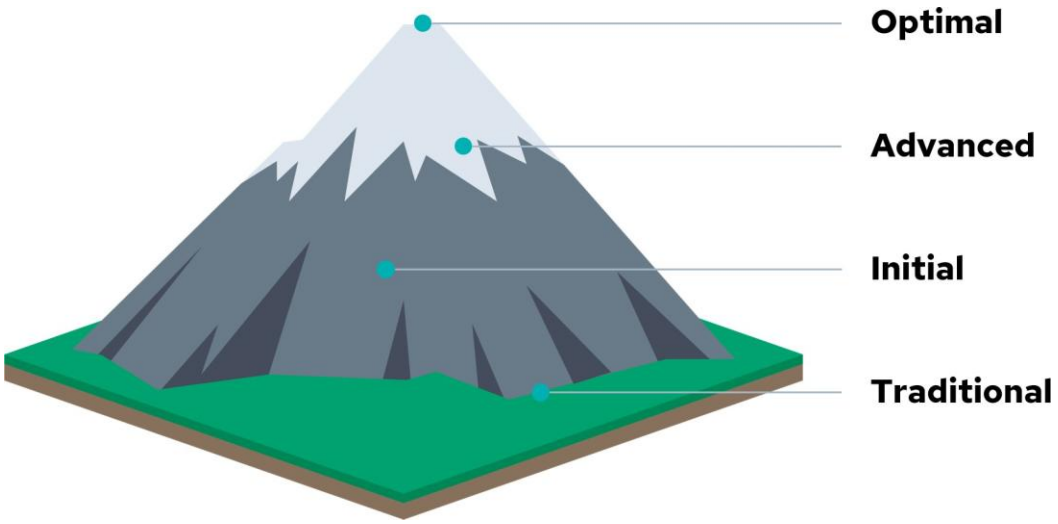
以下の5つの柱は、**アイデンティティ、デバイス、ネットワーク、アプリケーションとワークロード、データ**です。各柱には、次の横断的な能力に関する一般的な詳細が含まれています：**可視化と分析、自動化とオーケストレーション**、そして**ガバナンス**。

[17] Zero Trust Maturity Model Version 2.0



CISA ZTMMの成熟度レベル

ゼロトラスト成熟度モデル（ZTMM）の旅の段階は、以下に示すように、**従来**の出発点から、**初期**レベル、**高度**レベル、**最適**レベルへと進みます。各ステージでは、導入のための保護、自動化、詳細、複雑さのレベルが向上します。



元々は米国連邦政府機関向けのガイダンスとして発行されたものですが、このモデルは、公共および民間業界全体の主要な業界リファレンスとして機能しています。CSAは、IT環境とOT/ICS環境の両方において、ZTの旅の基礎となる重要なモデルとしてこれを使用しています。

アメリカ国防総省（DoD）は、同様の段階的なセキュリティ成熟度レベルを含む、独自のゼロトラスト参照アーキテクチャとゼロトラスト戦略を策定しました。注目すべきは、国防総省がオペレーショナルテクノロジーに特化した活動を取り入れるために、これらの枠組みを強化していることです。CISAとDoDのゼロトラスト成熟度へのアプローチを比較することに関心のある方向けに、CSAは、両組織のZTリーダーを招いた有益なウェビナー「Understanding the CISA Maturity Model and DoD's Zero Trust Strategy（CISAの成熟度モデルとDoDのゼロトラスト戦略を理解する）」を提供しており、この2つの影響力のあるモデルの類似点と相違点に関する貴重な洞察を提供しています。

OT/ICS の ZT 実施プロセス

ZTの5段階の導入プロセスは、OT/ICSの環境に適しています。実際、以下のセクションで示すように、5 つのステップはそれぞれ、NISTや国際自動制御学会（ISA）のガイダンスなど、OT/ICS や IT/OT のハイブリッド環境におけるサイバーセキュリティ管理のための確立されたアプローチに対応しています。

ステップ1：OT/ICSのプロテクトサーフェスの定義

CSAは、『Defining the Zero Trust Protect Surface（ゼロトラスト・プロテクトサーフェスの定義）』という出版物の中で、一般的なステップ1のガイダンスを作成しています。本セクションでは、このステップを OT/ICS 環境特有のニュアンスにどのように適用できるか、また、確立された OT/ICS ガイダンスとどのように整合させるかに焦点を当てます。

ゼロトラスト・プロテクトサーフェスの定義には、組織のビジネスシステム資産の強固で、理想的には動的に維持されるインベントリを作成することが含まれます。組織の資産目録は、次に説明するZT学習曲線で推奨されているように、ZT導入の優先順位付けに使用されます。

前述したように、ステップ1はZTの旅全体の基盤となり、ステップ2～5の反復プロセスの舞台を整えます。この包括的なインベントリにより、企業は、重要度、リスク、既存のセキュリティ対策のバランスを取りながら、戦略的にZTの導入に取り組むことができます。

ゼロトラストの学習曲線：クロール、ウォーク、ラン

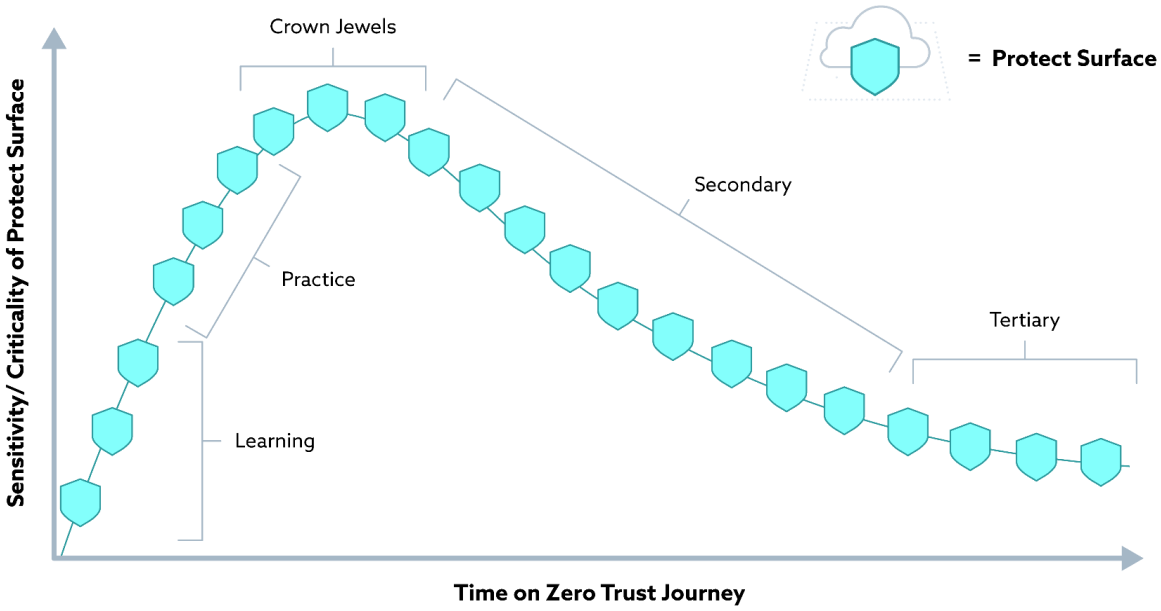
ZTの導入は、他の変革的戦略と同様、「クロール（這って）、ウォーク（歩いて）、ラン（走る）」と表現されるような、慎重かつ段階的なアプローチによってもたらされます。この方法論は、リスクが高く、混乱が深刻な結果をもたらす可能性があるOT/ICS環境において特に価値があります。完璧なコンディションを待ってから行動を起こすという、分析麻痺に陥りがちな落とし穴に対処します。その代わりに、このアプローチでは、低リスクの初期反復を通じて即時の進展を促し、リソースに負担をかけたり、重要な業務を中断させたりすることなく、セキュリティ強化への道筋をつけることができます。

組織は多くの場合、5つのステップの最初の反復のために、シンプルでリスクの低い「学習用」プロテクトサーフェスを特定することから始めます。この最初の反復作業（「クロール」）により、チームは、管理さ

れたノンクリティカルな環境で、ZT導入プロセスの5つのステップをたどり、実践的な経験を積むことができます。自信と専門知識が深まるにつれ、組織はプロテクトサーフェスの実践を繰り返しながら「ウォーク」することができるようになります。最後に、「ラン」段階では、最も重要で複雑なシステム、しばしば*クラウンジュエル*と呼ばれるシステムに取り組みます。

この戦略的で段階的なアプローチにより、ZTの導入プロセスを徐々に習得することができます。このプロセスで能力と信頼を築き、ミッションクリティカルなシステムに適用した場合、導入が効果的かつ継続的であることを保証します。組織が進歩するにつれて、ZTの原則を二次および三次システムに拡張し、最終的には包括的で全社的なZTAを達成することができます。

CSAは、新しいZTテクノロジーに投資する前に、既存のツールや機能を活用したプロテクトサーフェスの学習と実践を何度か繰り返すよう組織に助言しています。このアプローチは、具体的なニーズ、アーキテクチャ要件、統合ポイントに役立つ貴重な洞察をもたらします。このような学習段階を経ずに早すぎる調達を行った結果、基幹システムやより広範なアーキテクチャと互換性のないソリューションになってしまった事例を、私たちは目の当たりにしてきました。このような行き違いは、ZTの旅を著しく複雑にし、遅らせる可能性があります。即時の獲得よりも学習を優先させることで、企業はより多くの情報に基づいた意思決定を行うことができ、将来の投資が独自のZT要件や既存のインフラとシームレスに整合するようになります。



信頼ゼロの学習曲線ゼロトラストを一歩ずつ展開

OT/ICSにおけるプロテクトサーフェス

資産目録の作成とともに、プロテクトサーフェスを定義する最初のステップは、各資産とビジネスプロセスおよび価値の関係を特定する機会でもあります。例えば、製薬のような重要な業界では、低コストのOT/ICSコンポーネント1つでさえ、需要を満たし、収益性を維持するために極めて重要です。1,500ドルのロジック・コントローラーがサイバー攻撃を受ければ、数百万ドルの生産に影響を与え、救命薬へのアクセスに影響を与える可能性があります。

保護すべき組織資産を特定し、そのビジネス価値と関係を理解することで、組織はZTプロテクトサーフェスを定義することができます。私たちが保護しようとしているのは、一般的にDAAS要素と呼ばれるデータ、アプリケーション、資産、サービスです（詳しくは、 本書の 「Protect Surfaceを構成するDAAS要素」で説明します）。OT/ICS環境では、サイバーフィジカルな性質を反映し、デジタル資産と物理資産の両方がプロテクトサーフェスに含まれることがよくあります。オペレーショナルシステムは、特定のアウトプットを達成するために一体となって動作する、相互に接続された複数のサブシステムで構成されることがよくあります。

場合によっては、プロテクトサーフェスは、機械や関連制御システムなどの重要なシステムコンポーネントの集合体を包含することがあります。これらのDAAS要素やアセンブリを総称して、ZTプロテクトサーフェスやポリシーを説明する際に「資産」と呼ぶことがあります。

プロテクトサーフェスを定義する際には、幅広い範囲から始め、徐々に絞り込んでいくのが効果的です。ビジネス情報システムまたは業務システムを特定することから始め、それらをサブシステムに分解し、最後に個々のDAAS要素に分解します。この階層的アプローチは、OT/ICS環境の複雑で相互接続された性質によく合致しています。

この階層の各レベルは、組織のニーズやシステムの複雑さに応じて、それ自体がプロテクトサーフェスになる可能性があります。目標は、密接に連携した制御と最小限の特権ポリシーの実装を可能にする、最もきめ細かいプロテクトサーフェスを特定することです。

ISA/IEC 62443ゾーンとコンジットモデル

重要インフラ部門には、データの分類、セグメンテーション、リスク管理など、サイバーセキュリティに関する独自のガイダンスや規制があります。

すべての部門を横断する国際自動制御学会（ISA）は、OT/ICS（ISAはより広義にIACSと定義）のための一連の規格を維持しています。規格のリストの中には、ISA/IEC 62443があります。ISA/IEC 62443は、「世界で唯一のコンセンサスに基づくオートメーションおよび制御システムのサイバーセキュリティ規格」として宣伝されている一連の規格です。

ISA/IEC 62443 規格シリーズには、システム所有者、システムオペレータ、リスク専門家、製造業者向けに、OT/ICS のセキュリティを確保するための規範的なガイダンス（必要な活動）と有益なガイダンス

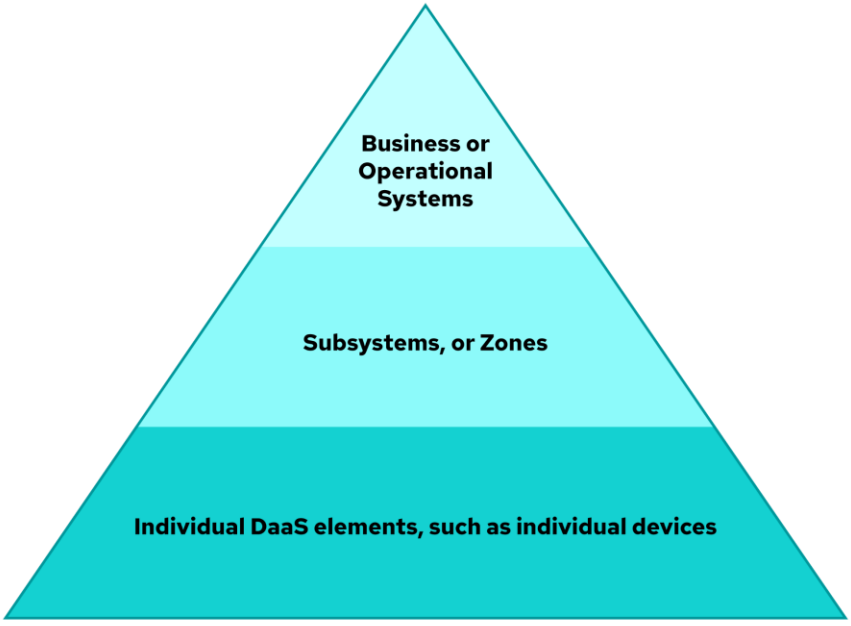
（役立つハウツー）の両方が含まれています。また、Purdue Modelに基づいたリファレンスアーキテクチャを使用し、セグメンテーションとアクセス制御に使用するゾーンとコンジットの概念も紹介しています。

ゾーンは、共有するセキュリティ要件[18]に基づいてシステムやコンポーネントをグループ化したもので、この階層におけるサブシステムに相当します。ゾーン間の通信経路であるコンジットについては、「ステップ2：OT/ICS の業務フローのマッピング」でさらに検討します。

ゾーンとコンジットモデルをすでに実装している場合、これらのゾーンはサーフェスを保護するための出発点となります。各ゾーン、またはサブシステムは、必要に応じてDAAS要素にさらに分解することができます。

プロテクトサーフェスを定義することは、反復的で、徐々に精巧になっていくプロセスであることを忘れないでください。5ステップの実装を進めるうちに、さらにサブシステム/ゾーンが特定されるかもしれません。その中には、別の保護対象として分割するのが理にかなっているものもあるかもしれません。このプロセスの洗練化は自然で意図された結果であり、ますます精密なセキュリティ管理を可能にします。

プロテクトサーフェスは、次のような階層構造で定義することができます。



[18] How to Define Zones and Conduits

プロテクトサーフェスを構成するDAASエレメント

このセクションでは、「プロテクトサーフェス」というコンセプトに基づいて、OT/ICS環境におけるサーフェスを構成する具体的なコンポーネントについて詳しく説明します。前述の通り、プロテクトサーフェスを構成するコンポーネントはDAASの要素：データ、アプリケーション、資産、サービスで構成されているとよく言われます。OT/ICSの文脈では、これらの要素がしばしばデジタルと物理の両方の領域にまたがることを認識することが重要です。このような包括的な視点により、ZTの原則を導入する際には、運用環境の重要な側面がすべて考慮されることになります。OT/ICSの設定に関連する具体的な例を挙げながら、これらの要素をそれぞれ詳しく探ってみましょう。

データ

OTおよびICS環境では、データには従来の機密情報だけでなく、産業プロセスの安全性、信頼性、効率性に直接影響する重要な運用データも含まれます。これには以下が含まれます。

- 制御信号、システム構成、プロセスパラメータ
- ヒストリアンデータ、P&ID、プロットプラン、機器図面、スペックシート
- 生産データ（シリアルデータ、材料調達データ、生産スケジュール）
- 知的財産と特許
- ビジネスデータ（出荷、請求、その他の分析）
- OTプログラム/ロジック構成ファイルを含む構成および設計データ
- ファームウェアファイルとパッチ適用およびアップデート用ソフトウェア
- 業界固有の規制で保護されたデータ（NERC CIP対象情報など）
- その他のビジネス、従業員、支払い、ベンダーのデータ

アプリケーション

アプリケーションは、重要なビジネス要件、機能要件、または運用要件を満たすソフトウェア、ハードウェア、およびインフラストラクチャの集合体です。データへの直接的または間接的なインターフェースを提供します。例えば、以下のようなものです。

- プロセスおよび生産アプリケーション（OPCアプリケーション、MES、SCADA、Historianなど）
- OT/ICS環境におけるハードウェアとソフトウェアのシステム管理アプリケーション
- IDおよびアクセス管理アプリケーション
- オペレータと機械やプロセスとのインタラクションのためのヒューマン・マシン・インターフェース（HMI）アプリケーション
- OT/ICS業務と連携する可能性のあるビジネス・プロセス・アプリケーション
- OT/ICSプロセスに対応するクラウドおよびSaaSアプリケーション

資産

資産とは、組織内でデータをホストしたり、重要な機能を果たすリソースのこと。OT/ICS環境では、ITとOTの両方のコンポーネントが含まれます。

- OT/ICS環境へのアクセスに使用されるコンピュータシステムおよび機器
- フィールドコントローラ（PLC、フィールドロジックデバイス）
- サービス提供の中核となるOT/ICS機器（製造プラント機器、発電機など）
- 物理的プロセスを実行する装置（ロボットアーム、コンベア、化学調整装置など）
- 重要なシステムへの入力を提供するセンサーと変換器
- OT/ICS内のネットワークインフラ（スイッチ、ルーター、ファイアウォール、無線アクセスポイント）
- 物理的な建物アクセス装置
- ユーザー（エンジニア、特定の知識/能力を持つアセットオペレーター）
- API、デバイスID、その他の非個人エンティティ

サービス

OT/ICS環境におけるサービスは、ビジネスおよび技術的な専門知識を応用して、情報および運用プロセスを作成、管理、最適化します。これには以下のようなものがあります。

- インテグラルサービス - プロテクトサーフェスの一部として含まれます。
    - ネットワークおよび通信サービス
    - OTの脆弱性管理と資産の健全性監視のための可視性と分析サービス
    - オートメーションとオーケストレーション・サービス
    - ICSおよびベンダー固有のプロトコル
- 外部サービスのサポート - サーフェス自体の保護
    - 遠隔監視・制御サービス（GE、シーメンス、SEなど）
    - ドメインネームサービス（DNS）
    - 公開鍵基盤および鍵管理サービス
    - アイデンティティサービス（IDaaS、FIDO/パスキー・サービスなど）
    - OT/ICSオペレーションをサポートするPaaSやSaaSのようなクラウドベースのサービス

プロテクトサーフェスをDAAS要素として定義することで、リスクを評価し、脆弱性を管理し、OT/ICS環境の最も重要な資産を保護することができます。定期的なアセスメントにより、進化する重要資産との整合性が確保されるため、CIの所有者および運営者は、攻撃成功のリスクを低減し、運用の完全性を維持することができます。

OT/ICSにおけるプロテクトサーフェスの例には、以下のようなものがあります。

ビジネス情報システム	データ	アプリケーション	資産	サービス（サポート）
産業制御システム	化学プラントの化学プロセス管理に使用される制御、センサー、プロセスデータ	生産化学プロセス制御アプリケーション	化学プラントのセンサーとPLC	暖房、換気、空調（HVAC）
スマートエネルギー計測・課金システム	電気消費量と顧客データ	顧客モニタリングと請求システム	システム監視と顧客課金をサポートするためにエネルギー信号を消費するスマートメーター	スマートメーター無線ネットワーク

ある組織のプロテクトサーフェスは不変かもしれませんが、それを構成するDAASの要素は、新しいテクノロジーが開発され、古いテクノロジーが陳腐化するにつれて常に変化しています。OT/ICSの所有者およびオペレータは、定期的にプロテクトサーフェスを評価し、重要な資産との整合性を確認することが重要です。

DAASの要素とZTMMの柱の関係

DAASの要素とCISAのゼロトラスト成熟度モデル（ZTMM）の柱は、どちらもZT戦略の構成要素ですが、導入プロセスにおける役割は異なります。

1. DAASの要素：これらは、組織がZT戦略の中で保護しようとする資産の目録を表しています。DAASの要素は、プロテクトサーフェスの定義に役立ち、セキュリティ保護が必要なものの包括的なビューを提供します。

2. CISA ZTMMの柱：5つの柱（アイデンティティ、デバイス、ネットワーク、アプリケーションとワークロード、データ）は、組織のインフラストラクチャのさまざまな側面にわたってZT機能を実装し、成熟させるためのフレームワークを提供します。組織のZT成熟度レベルを評価し、強化するための構造化されたアプローチを提供します。

DAASの要素とCISA ZTMMの柱による分類を理解することは、効果的なZTの計画と実施に役立ちます。

- DAASの要素は、重要な資産を目録化することによって、「我々は何を守っているのか？」という問いに答えます。

- ZTMMの柱は、インフラのさまざまなドメインやDAAS要素のタイプにわたって、「私たちの保護メカニズムがどの程度成熟しているか？」に対処します。

この2つのコンセプトを活用することで、組織は次のことが可能になります。

1. 重要な資産（DAAS要素）の包括的なインベントリに基づき、適切なサブシステム/ゾーンに分類されたプロテクトサーフェスを効果的に定義します。

2. ZTMMフレームワークを使用して、インフラストラクチャの関連するすべての側面にわたって、ZT機能の実装と成熟に優先順位を付けます。

3. 総合的なZTポスチャを段階的に強化する努力を優先します。

4. デジタルおよび物理的なインフラストラクチャのあらゆる側面に適切な保護を確実にします。

この統合されたアプローチにより、組織は、保護すべき特定の資産と、インフラのさまざまなドメインにわたる保護メカニズムの成熟度の両方に対処する、堅牢なZT戦略を策定することができます。これにより、より全体的なセキュリティの見方が可能になり、重要資産のインベントリが進化するにつれて、関連するすべての領域にわたるZT実装の成熟度も向上します。

OT/ICS環境におけるプロテクトサーフェス定義のヒント

OT/ICSでZTの旅に出る際には、以下のヒントを心に留めておいてください。ZT導入プロセスのその後の4つのステップは、この最初のステップで完了した発見と文書化によって決まることを忘れないでください。

利用可能なツールとデータから始めます

すべてのZTプログラムと同様、組織は「現在地から始める」ことが奨励されます。OT/ICS 環境で、堅牢な機能を備えた構成管理データベース（CMDB）アプリケーションなどのツールを利用できるのであれば、それは素晴らしいことです。しかし、在庫管理が行われていない、在庫が一部しかない、在庫が古い、あるいは紙や手動の在庫プロセスで運用されている、といった環境では、在庫管理から始めなければなりません。最初のタスクは、インベントリプロセスとツールを更新してZTプログラムを維持する方法を検討しながら、すぐに使用できるようにデータを集約することです。

インフラの運用に不可欠なすべての重要資産の特定します

組織にとって意味のある方法で資産を整理しましょう。これは、DAAS要素（データ、アプリケーション、資産、サービス）によって資産を分類すること、ゾーン/サブシステムを使用すること、またはその両方を混在させることを意味します。さらに、ビジネスプロセス、部門/チーム、地域、規制、重要度に基づいてサブグループ化することができます。

事業の重要性と影響における資産の役割を特定し文書化します

グループ分けに関係なく、プロテクトサーフェスを定義するには、ビジネス上の重要性におけるさまざまな資産の役割と、その資産またはシステムが事業運営や安全性に及ぼす可能性のある影響を特定するための発見と文書化が必要です。この段階では、リスク評価ではなく、ビジネスインパクト分析（BIA）を行うことが目的です。BIAを実施するための標準的なフレームワークやモデルは、NIST[19]、DHHS[20]、ISOをはじめ、OT/ICS向けのISA/IEC62443-3-2[21]のような業界や環境に特化したモデルなど、数多くあります。

資産の依存関係を特定し文書化します

この3つのヒントの最後の部分は、特定された資産の依存関係を詳述した文書を含めることです。この訓練は、BIAに最終的に影響を与える相互依存関係に基づいて、組織が個別の資産に重要度を適切に割り当てることを確実にします。この活動は、（ORFを活用した）より広範なレジリエンス・イニシアチブの一環であったり、災害復旧・事業継続計画（DR/BCP）を策定する取り組みであったりします。

先ほどの医薬品製造企業の例でいえば、プロテクトサーフェスを構成する構成資産を考慮せずに、システム（製造、組立、包装プロセスなど）の重要性を検討するのは得策ではありません。理想的なZTプランニングでは、プロテクトサーフェスは（資産のグループやシステムとしてではなく）個別に定義されます。産業環境では、このレベルの特定はより難しいかもしれませんが、可能であれば遵守すべきです。

[19] Business Impact Analysis (BIA) - Glossary | CSRC
[20] NIST Releases IR 8286D: Using Business Impact Analysis to Inform Risk Prioritization and Response
[21] Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2

可能であれば、ダイナミックでほぼリアルタイムの資産インベントリを維持します

ZTが成熟するにつれて、政策決定に必要な正確でリアルタイムのデータへの依存度が高まっています。この点で、資産目録は極めて重要です。組織は、すべての資産タイプにわたって、リアルタイムまたはほぼリアルタイムのデータによるインベントリの近代化を目指すべきです。

このタスクは従来、企業のIT環境だけでなく、OT/ICS資産を持つ産業環境においても（特に）課題でした。APIを通じて接続し、プッシュ、プル、ポーリングを行うことができるアプリケーションが望ましく、組織は戦略を通じて、または更新やアップグレードプロジェクトが発生したときに臨機応変に対応することができます。

あるいは、より一般的でアクセスしやすいdynamic inventoryソリューションは、システムを自動的に更新したり、変更に対して警告を発したりします。ソリューションによっては、（スパン/タップまたはネットワークデバイスを経由して）トラフィックを直接監視するものもあれば、適切なOT固有のプロトコルでデバイスに問い合わせるものもあります。半自動化ソリューションは、資産追跡を調達や変更管理のワークフローに組み込むことができます。

継続的なメンテナンス・タスクとしての再調査と更新を計画します

ZTAの維持には継続的な見直しが必要です。最終的には、ZTプログラムが成熟するにつれて、手作業によるレビューと保守作業は自動化されるべきです。ここでは、最新のインベントリを維持することに関連するものとして記載しましたが、追加情報は、ステップ5「継続的なモニタリングとメンテナンス」に記載されています。

対象範囲のシステムまたは環境に最も適したアプローチを使用します

エンタープライズ IT のプロセスやツールは、OT/ICS 環境にそのまま適用できるとは限らないことに留意してください。OT/ICSに特化したツール、ベンダー、プロセスを使用し、発見と分析を通じてシステムの信頼性と安全性を確保します。

例えば、先に言及したPurdueモデルのレベルを考慮すると、NMAPのような一般的なツールを実行しても、企業のITネットワーク上では無害かもしれませんが、Purdueモデルの下位レベル、特にサイバーフィジカル資産やフィールドデバイスに近づくにつれて、障害や不具合を引き起こす可能性があります。

OT/ICS資産の発見を任務とする企業のITおよびサイバーセキュリティの専門家は、OTエンジニアやシステムオペレータと緊密に連携する必要があり、またそれを望んでいます。新しいツールや技術は、非生産システムやネットワーク、あるいはデジタルツインでテストされるべきです。

これと同様に、OT/ICS ネットワークの監視、保守、インシデント対応に携わるベンダーやサードパーティは、これらのシステムに特化した専門知識を持つ必要があります。これについては、ステップ2、トランザクションフローのマッピング、ステップ5、継続的なモニタリングとメンテナンスで詳しく説明します。

各プロテクトサーフェスのメタデータ収集が不可欠です

各プロテクトサーフェスのメタデータの収集は、重要なコンセプトです。この情報には、データタイプ、プロトコル、システムのクリティカリティなどの詳細が含まれ、ZTの実装プロセス全体を通じて非常に重要です。フローのマッピングからアーキテクチャの設計、ポリシーの作成に至るまで、各ステップを進めるにつれて、このメタデータは絶えず進化し、拡張していきます。各ステージは、前のステージで収集されたメタデータを基に構築され、より正確でターゲットを絞ったセキュリティ対策を可能にする、より詳細な洞察を提供します。最終的には、このようなメタデータの蓄積が、各プロテクトサーフェス固有のニーズや特性にきめ細かく対応した、独自のZTポリシーの開発につながります。

プロテクトサーフェスに特化したセキュリティ対策を開発することは重要ですが、OT/ICS環境では、このタスクの重要性がさらに高まります。迅速なソリューション導入が可能なITとは異なり、産業部門は複雑です。この複雑さは、OTインフラや多様な通信プロトコルによるものだけでなく、エンジニアリングやオペレーションから、最高リスク責任者（CRO）やコントロールルームのスタッフ、多くのサードパーティの請負業者や専門家まで、幅広いステークホルダーが関わっていることに起因しています。各グループはそれぞれ独自の視点と目標を持っています。この複雑な検討の網は、カスタマイズされたZT戦略の必要性を浮き彫りにし、CI構成に固有の多面的なニーズと懸念を認識し、それに応えるように綿密に設計されたものです。

ステップ2：OT/ICS の業務フローのマッピング

業務フローのマッピングは、ZT 実装プロセスの5 つのステップの内、2 番目のステップです。ステップ 2 の目的は、プロテクトサーフェスへの、プロテクトサーフェスからの、および プロテクトサーフェス内の、情報フローをマッピングして、システムがどのように機能するかを理解することです。これには、さまざまな DAAS 要素が相互に、および他のリソースとどのように相互作用するかが含まれます。これらのフローを理解することで、適切な制御を配置する場所が直接わかります。

CSA は、ステップ 2 - トランザクションフローのマッピングのドキュメントでこのステップの一般的なガイダンスを提供していますが、OT/ICS コンテキストでは少し異なる視点が必要です。これらの環境では、「トランザクション」の概念はあまり重要ではありません。代わりに、業務フロー、プロセスフロー、および制御フローのマッピングに焦点を当てています。この用語の変更は、個別のトランザクションではなく、進行中のプロセスと制御操作に重点が置かれている OT/ICS システムの継続的で相互接続された性質をよりよく反映しています。

このマッピング情報により、セキュリティ制御、きめ細かいアクセス ポリシー、リソース割り当て、およびセキュリティポスチャの強化について、情報に基づいた決定が容易になります。

OT/ICSシステムにおけるフローのマッピング：戦略上の必要性

OT/ICS 環境における業務フローのマッピングは、システムがどのように相互作用するかを特定し、必要な制御を特定し、それらを防御するための堅牢な監視ポイントを確立するために不可欠なものです。IT システムとは異なり、OT システムでは、物理的および業務上の微妙な違いを考慮したマッピングアプローチが必要です。

可能な限り、各接続ポイントは、検証されるまで信頼できないものとして扱い、ZT 基本原則に従う必要があります。このアプローチは、脅威のラテラルムーブメントを防止するための基本です。これは、システムの相互接続性と特殊性が独自のセキュリティ上の課題をもたらす OT/ICS コンテキストでは特に重要な側面です。OT 内のシステムは複雑にリンクされており、従来の IT 環境とは異なるプロトコルで動作するため、脅威がネットワーク上を検知されずに移動するリスクが大幅に高まります。

OT/ICS サイバーセキュリティの分野では、産業オペレーションの理解が含まれます。プログラマブル・ロジック・コントローラー (PLC) の言語、監視制御およびデータ収集 (SCADA) システムのフロー、分散制御システム (DCS) のアーキテクチャに精通していると、そのメリットが得られます。この知識は、産業環境の独自の状況に合わせて調整された ZT 戦略を実装する際に役立ちます。

進化するインベントリ：業務フローマッピングの基礎

ステップ 1 で作成された資産インベントリは、OT/ICS 環境における業務フローマッピングの重要な基盤となります。ステップ 2 に進むにつれて、このインベントリを基にして改良し、OT 環境をより包括的かつ動的に理解できるようになります。

徹底した資産インベントリは、さまざまな資産間の依存関係、相互接続、アクセス関係の明確な文書化を促進します。この明確さは、業務フローマップの開発に役立ち、システム内のデータの移動と潜在的な脆弱性

を浮き彫りにします。フローをマッピングするプロセスでは、これまで見落とされていた資産や接続が明らかになることが多く、新しい要素、依存関係、データフロー情報で初期インベントリを充実させることができます。

重要なのは、ZTの旅の各ステップを進めるにつれて、見落とされていた要素が特定される可能性が高くなりますが、その量は減少します。この継続的な検出プロセスにより、定義されたプロテクトサーフェスやその優先順位が変更される可能性もあります。

多くの組織が依然として手動の方法でインベントリを管理していますが、このプロセスのデジタル化は ZT ロードマップの一部である必要があります。継続的に更新されるデジタルインベントリにより、OT 環境の進化に合わせて業務フローマッピングをリアルタイムで再評価および再調整できます。

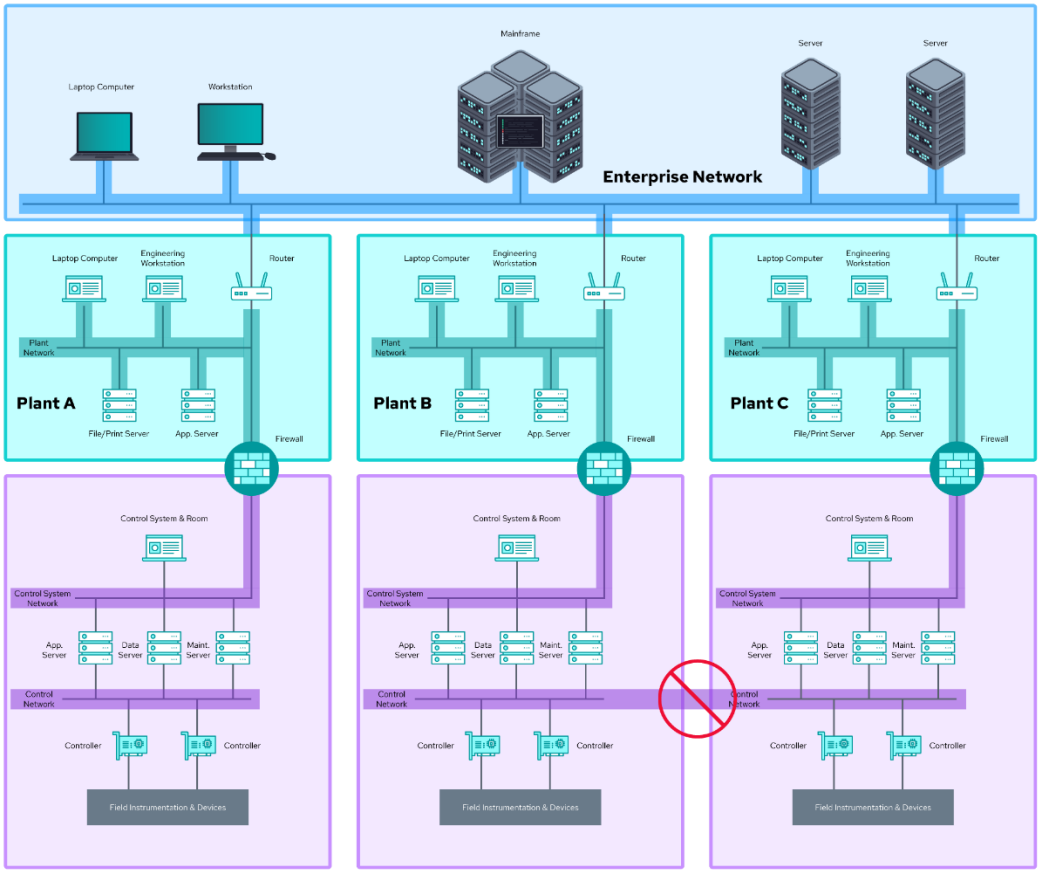
ISA/IEC 62443ゾーンとコンジットモデルを使用したフローのマッピング

前述のISA/IEC 62443規格を思い出してください。これらの標準は、OT/ICS 環境における業務フローのマッピングに役立つ参照モデルを提供します。
ゾーンとコンジットをモデル化する場合、専門家が考慮しなければならない一連の重要なルールがあります[22]。

- ゾーンはサブゾーンを持つことができます。
- 1つのゾーンに複数のコンジットがあってもかまいません。ゾーン内のサイバー資産は、1つ以上のコンジットを使って通信します。
- コンジットが複数のゾーンを横断することはできません。
- コンジットは、2つ以上のゾーンが互いに通信するために使用できます。

[22] How to Define Zones and Conduits

以下の図は、正しいゾーンとコンジット、間違ったゾーンとコンジットについて、ゾーンのアーキテクチャ例とコンジットのアーキテクチャ例を示しています。



ソースゾーンとコンジットの定義方法

上の図では、色分けされたボックスがゾーンを表し、その中の濃い網掛け部分がコンジットを表しています。

コンジットは、ゾーンを相互に接続できますが (north/south トラフィック)、単一のコンジットではゾーンを横断できません (east/west トラフィック)。これについては、以下の「コンジットを使用した業務フローのマッピング」セクションで詳しく説明します。

一般的なコンジットの種類

産業システムは、さまざまなプロトコルとメディアが利用されており、その種類、性質、機能も幅広い範囲を網羅しています。これらのプロトコルの膨大な数は、OT 環境に見られる複雑さと特殊性を反映しています。一般的なコンジットの種類には、次のようなものがあります。

- OPC を含むさまざまな産業プロトコルを使用した Ethernet ベースのプラントネットワーク
- 分散制御システムの制御ネットワーク (例: 横河 Centum VNet/IP)
- 産業フィールドネットワーク (例: Profibus DP、DNP3、HART7 など)

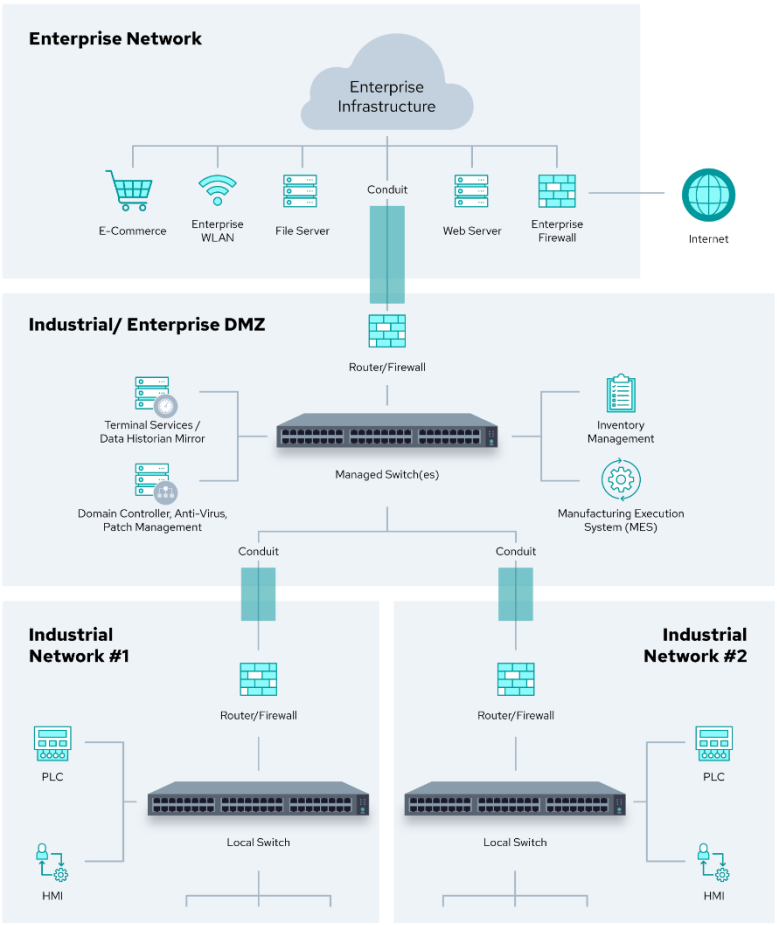
- ワイヤレスネットワーク: ISA100、ワイヤレス HART など
- 2 台のコンピュータ間の通信を可能にするシンプルな RS-232/422/485 シリアルケーブル

コンジットを使用した業務フローのマッピング

コンジットの構造は、ZT フローマッピングの原則と非常によく一致しています。

コンジットは、2 つ以上のゾーンを接続できる通信チャネルの論理的または物理的なグループです。コンジットは、セキュリティゾーンを接続し、OT/ICS ネットワーク内で必要な通信パスを明確に定義します。これにより、セグメンテーションとアクセス制御の要件が満たされます。

可能であれば、資産所有者は、余分で不要な複雑さを避けるために、ゾーンとコンジットをネットワークアーキテクチャと一致させるように努める必要があります[23]。



出典：ISA/IEC 62443のキーコンセプト：ゾーンとセキュリティレベル/Dragos
訳注）Dragos Inc とは、米国政府と米軍が2016年に設立し、政府や軍におけるOTの脅威から文明を守る使命を持った組織です。Dragos Platformは、最も効果的な産業用サイバーセキュリティテクノロジーを提供し、ICS/OT資産、脆弱性、脅威、および対応アクションを可視化します。

[23] Key Concepts of ISA/IEC 62443

OT/ICS 環境内の異なるゾーン間のデータフローとインタラクションを理解するには、コンジットを正確にマッピングすることが不可欠です。業務フローをマッピングする場合、正当なフローと不正な可能性のあるフローの両方を考慮することが不可欠です。これには、制御システム、フィールドデバイス、その他の業務コンポーネント間のデータ交換、および外部システムやネットワークとのインタラクションの調査が含まれます。これらのフローを徹底的にマッピングすることで、組織は潜在的な攻撃ベクトルを可視化し、ZT 原則を適用する必要がある領域を特定できます。

観察されたデータフローは、どの通信タイプがアクティブに発生し、おそらく許可されているかについて貴重な洞察を提供するということを覚えておいてください。ただし、ZT の原則では、デフォルト拒否モデルが推奨されています。したがって、アクティブなトラフィックを観察するだけにとどまらないことが重要です。コンジットとゾーン内ネットワーク構成、およびファイアウォールルールを評価して、すべての許可されたトラフィック （観察期間中にアクティブではなかった可能性のあるフローも含む） を特定します。次に、特定されたフローごとに、ZT ポリシーに基づいて許可するか拒否するかを決定します。

さらに、交換されるデータのタイプ、使用されるプロトコル、およびフローの業務プロセスに対する重要性など、各業務フローの性質と目的を文書化することが重要です。この情報（メタデータ) は、ZT 環境を設計し、これらの業務フローを管理および保護するための適切なポリシーを作成するという、その後の手順に情報を提供します。

重要な洞察は、マッピング演習中にフローのパターンまたはカテゴリを特定することです。これにより、エンタープライズセキュリティアーキテクチャの構成要素が明らかになり、ZTA を設計する次のステップをより適切に情報提供するのに役立ちます。

ゾーンとコンジットを超えて

ゼロ トラストのコアコンセプトは、最も細かいプロテクトサーフェスを特定し、密接に結びついた制御を実装し、正確にターゲットを絞った最小特権ポリシーを確保することです。ゾーンとコンジットを使用して業務フローをマッピングすることは、OT/ICS 環境内で非常に効果的ですが、ZT 実装を繰り返して成熟させるにつれて、より細かいコンポーネントを定義できるようになると、隔離によって脅威のラテラルムーブメントを防ぎ、影響範囲をさらに縮小することで、セキュリティポスチャをさらに強化できます[24]。

OT/ICSインフラ内のセグメンテーション

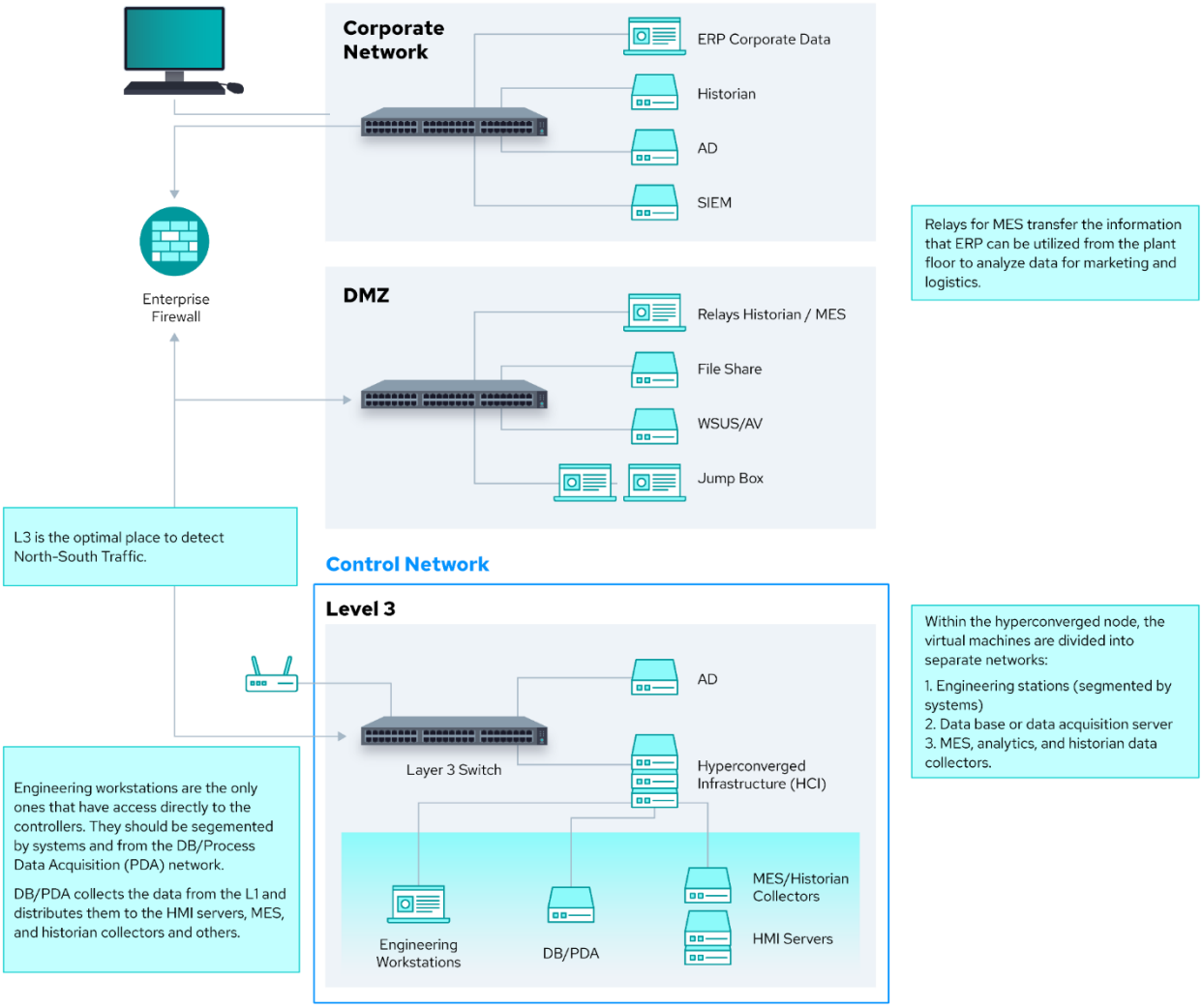
OT/ICS インフラストラクチャ内で DMZ を使用して IT と OT をセグメント化することは、通常 Purdue モデルのレベル 3 で、効果的な戦略となります。このホワイトペーパーの次のステップであるステップ 3 の ZTA の構築では、ZT のセグメンテーションについてさらに詳しく説明しますが、業務フローをマッピングする際には、いくつかの側面を考慮する価値があります。

多くの場合、Purdue モデルの下位レベルは、管理対象スイッチが十分にないフラットアーキテクチャのために監視されません。フラットネットワークでは、指定されたチョークポイントが不足します。これらのチョークポイントがないと、工場フロアからの大量のネットワークトラフィックを認識できないままになる可能性があります。その結果、追加のセンサーと監視機器を組み込む必要がある場合があります。以下のステップ 3 で説明するように、別のアプローチは、追加のセキュリティポリシーを適用するためにソフトウェアエージェントまたはレイヤー 7 (L7) コンポーネントを改造またはインストールすることです。

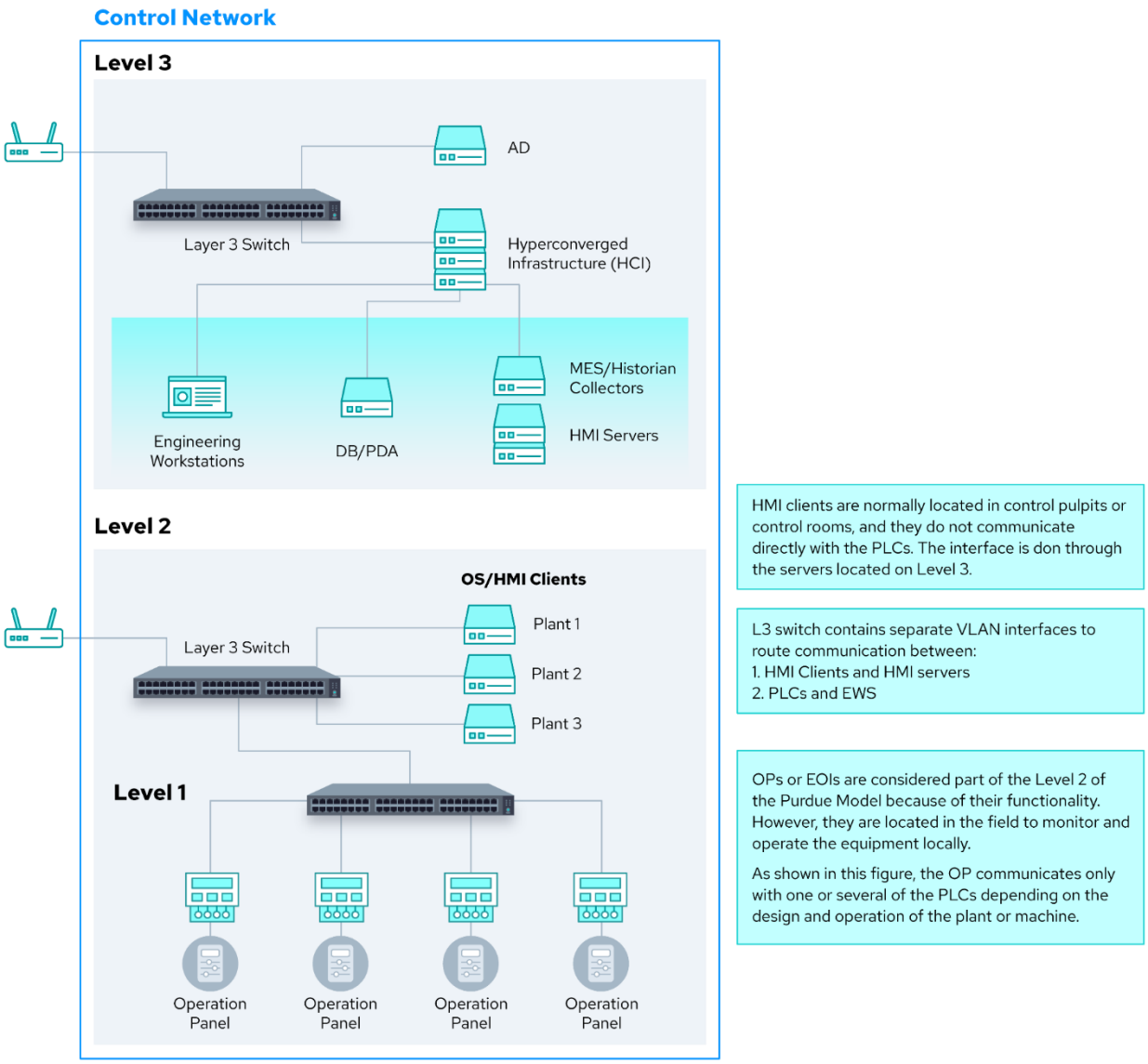
[24] For OT/ICS, it's not CIA, but AAA | OT Cybersecurity

マネージドスイッチ、センサー、エージェントを実装すると、業務フローを正確にマッピングする能力が大幅に向上します。これらのコンポーネントは、初期の ZT 実装サイクル (プロテクトサーフェスの学習または実践の反復など) の一部ではないかもしれませんが、将来の反復では貴重な考慮事項となります。5 ステップのプロセスを進める際には、これらの潜在的な機能強化を念頭に置いてください。これらは、再検討する設計要素のブックマークとして機能し、最終的には OT/ICS 環境でより包括的かつ正確な業務フローマッピングにつながります。

これを視覚的に理解しやすくするために、Dragos のホワイトペーパー「Network Segmentation Challengesand Solutions の図を以下に示します[25]。これらの図では、ERP (エンタープライズリソースプランニング) と MES (製造実行システム) について触れています。これらについては、Dragos のホワイトペーパーで詳しく読むことができます。これらの図をここに含めた目的は、業務フローのマッピングについて考えるきっかけとなるとともに、次のステップである ZTA の構築の入門書を提供することです。



[25] Whitepaper: Network Segmentation Challenges and Solutions



OT/ITの融合と業務フローのマッピング

前述のように、パンデミックによって特に加速したデジタルトランスフォーメーションの急速なペースにより、OT システムと IT システムの融合が強化されました。この変化により、従来の接続と最新の接続の両方を統合する必要があるため、業務フローのマッピングがさらに重要になり、プロトコルとテクノロジーの混合エコシステムを管理する必要性が強調されます。ベンダーが統合製品でこの融合を推進するにつれて、マッピング戦略がこれらの新しい相互接続を正確に反映することが不可欠です。

ビジネスとテクノロジーの進歩の急速なペースは、従来のセキュリティ対策を上回ることがよくあります。ZT 戦略は、このギャップに対処するのに最適であり、応答性と適応性に優れたセキュリティソリューションを提供します。この戦略の成功は、業務フローの包括的なマッピングにかかっています。これは、特にデジタルトランスフォーメーションに応じてデータパスが拡張または変更される場合、データパスを理解し、保護するために不可欠です。

・ **エアギャップはどうなったのでしょうか?**

OT システムと IT システムを分離する従来のエアギャップは減少しています。なぜでしょうか? 多くの場合、ビジネス上の意味があるからです。

・急速に変化する市場では、顧客への機敏な対応が求められ、ビジネスシステムと OT システムを接続して日常業務を強化する必要があります。

・食品メーカーは、Web アプリケーションと消費者の選択によって、工場の現場で特定の原材料の製造を直接推進したいと考えるかもしれません。ビジネスプロセスによって需要が促進されると、注文は OT に直接送信されて完了します。

・エネルギー消費を監視および制御する OT システムと IT システムをリンクしてエネルギー使用量を最適化し、需要、使用パターン、ユーティリティ料金に基づく自動調整によってリアルタイムのエネルギー管理とコスト削減を実現します。

・石油やガス、ユーティリティなどの業界では、IT と OT を統合することで、現場業務のリモート監視と制御が可能になります。この統合により、リアルタイムデータに基づく意思決定が容易になり、安全性と運用効率が向上します。

物理的なエアギャップがない場合、OT 環境は IT ネットワークに接続できます。その結果、インターネット経由の攻撃が OT デバイスに到達する可能性があり、ゼロ トラストが必須になります。

IT と OT の融合はイノベーションを推進しますが、OT ネットワーク内のシステムの特定の役割と相互作用を把握し、理解することが難しくなる傾向があります。そのため、業務フローのマッピングがますます重要になります。このプロセスでは、資産と既存のネットワーク接続間でデータがどのように移動するかを正確に概説し、可視性を高め、その結果としてセキュリティを強化する必要があります。場合によっては、ICS コンポーネントの改造が広く認識されることなく行われ、有効であると想定されていたエアギャップが無効になる可能性があることに注意してください。マッピングプロセスを実行するときは、これらの潜在的な「隠れた」改造に細心の注意を払ってください。

OT/ICSにおける業務フローをマッピングするためのヒント

役立つツールと技術

多くのベンダーが、パッシブおよびアクティブポーリング手法を含む、インベントリ検出と業務フローマッピングのための効果的なソリューションを提供しています。 Dragos Platform[26] 、Claroty[27] 、Nozomi Networks[28]、Armis Centrix[29]などのツールは、動的な資産検出を提供し、動的な業務フローマッピングを含むものもあり、ZT 実装プロセスの最初の 2 つの重要なステップを加速する可能性があります。 さらに、多くの OT プロトコル対応ファイアウォールベンダーが同様の可視性機能を提供しており、ラベル (メタデータ) に自動フラグを設定したり、サードパーティのメタデータを統合して動的なポリシーを作成したりできるも

[26] Asset Visibility for ICS environments | Dragos Platform
[27] Asset Inventory - Platform | Claroty
[28] OT Asset Inventory Management
[29] Full Asset Inventory and CMDB Enrichment | Armis

のもあります。

ただし、このようなソフトウェアの導入は必ずしも実行可能または許可されているわけではないことに注意することが重要です。船舶や海運などの重要な業界では、特定のツールの導入に関して規制上の制限を受ける場合があります。さらに、切断されたネットワークやシリアル接続されたネットワークでは、別のアプローチが必要になります。

自動化ツールを使用できる場合、継続的なネットワーク監視により、ネットワークの変更が迅速に認識、文書化、検証されるという信頼性が高まります。ソフトウェアの導入が制限されている環境では、セキュリティとリスク管理に対する代替の「システムベース」アプローチを検討してください。そのようなアプローチの **1** つが、**OT** 環境で高く評価されているフレームワークである、結果駆動型サイバー情報エンジニアリング**(**Consequence-driven Cyber-informed Engineering (CCE)**)**です。アイダホ国立研究所によって開発された **CCE** は、従来のソフトウェアソリューションが適用できないシナリオに貴重な洞察を提供します。

最終的には、ツールと方法論の選択は、特定の運用上の制約、規制要件、およびセキュリティ目標と一致する必要があります。自動化ツール、**OT** 対応ファイアウォール、手動プロセス、および **CCE**[30]などの革新的なフレームワークを組み合わせることで、多様な **OT/ICS** 環境でのインベントリとフローのマッピングに対する堅牢なアプローチを提供できます。

文化とコラボレーション

前述のように、OT/ICS 分野は IT とは大きく異なり、さまざまな機能構成要素が含まれます。多くの場合、OT 担当者と IT 担当者は、定期的にコミュニケーションをとりません。サイバーセキュリティ、IT、OT、ICS の専門家が協力して、業務フローのマッピングがこれらの環境に固有の複雑な相互作用と依存関係を正確に反映していることを確認します。この協力的なアプローチにより、データの潜在的な経路 (ひいては潜在的な攻撃ベクトル) がすべて考慮され、保護されます。

フローの文書化

検出、設計/アーキテクチャ、実装プロセスのあらゆる側面を文書化することは不可欠です。 文書化要件は、変更管理プロセスに組み込む必要があります。 これらの文書化要件には、資産インベントリ、ネットワーク図面、バックアップの更新、および更新されたトランザクションフローの検証を含める必要があります。

これにより、業務フローマッピングが適切に記録され、簡単に更新または参照できるようになります。業務フローをシステムとして表示して文書化し、それらの相互依存性を認識する必要があります。 この包括的な理解は、各プロテクトサーフェス用にカスタム構築された制御と環境を開発するために不可欠です。

ステップ**2**の締めくくり

ステップ 2 における業務フローのマッピングを、ゼロトラストの創始者である John Kindervag 氏の言葉を引用して締めくくりましょう[31]。「データを石油のように保護します。石油が精製されるにつれて価値が上がるのと同じように、データも価値が上がります。したがって、OT/ICS のトランザクションフローのマッピングには、変換と転送のあらゆる段階でデータを保護する厳格な対策が含まれ、貴重なリソースと同じレベルの保護で扱う必要があります。」

[30] Consequence-driven Cyber-informed Engineering
[31] Things Run Amok. Leveraging Zero Trust to protect IoT and OT assets.

業務フローのマッピングは、単なる手順タスクを超え、OT/ICS セキュリティの戦略的基礎へと進化します。このプロセスは、進化する脅威に対してシステムを強化するだけでなく、重要な操作とリモートアクセスに関する組織の理解を深めます。これらのフローを綿密に図表化することで、産業プロセスの中断を防ぎながら、新たなリスクに適応するレジリエンスのあるセキュリティの基盤を構築できます。最終的に、この演習により、セキュリティポスチャ全体が強化され、保護対策が OT/ICS 環境の複雑な現実に合わせられます。

ステップ3：OT/ICSにおけるゼロトラストアーキテクチャの構築

CSA は、Zero Trust Advancement Center (ZTAC) Resource Hubにある 5 つのステップの実装プロセスに関する一般的なガイダンスを提供しています。このセクションでは、OT/ICS 環境に固有のガイダンスを提供します。

ステップ 1「プロテクトサーフェスの定義」と、ステップ 2「業務フローのマッピング」の次は、ステップ 3「ゼロトラストアーキテクチャ (ZTA) の構築 (設計)」 です。これは、最初の 2 つのステップで収集された情報を使用して、アーキテクチャのどこで ZT ポリシーを適用できるかを特定する計画、およびドキュメント設計の段階です。

PurdueモデルとOSIモデル

このセクションでは、明確に異なる Purdue モデルのレベル (レベル 0 ～ 5) と OSI モデルのレイヤー (レイヤー 1 ～ 7) の両方を参照していることに注意してください。Purdue モデルは、このドキュメントでは OT/ICS ネットワークで一般的な資産のグループ化を説明する参照アーキテクチャとして参照されており、IT エンジニアと OT エンジニア間の議論のツールとなることを目的としています。OSI モデルは、ネットワークシステムの機能を説明するために使用される概念フレームワークです。Purdue モデルは産業用制御システムの階層構造を理解するのに役立ちますが、OSI モデルは、Purdue 階層のレベルに関係なく、その構造内のコンポーネント間でデータがどのように転送されるかを説明するために使用されます。

ポリシー実施ポイント

CI には、関係するシステムと資産のユニークな性質を考慮した、よく考えられたアーキテクチャ設計が必要です。これには、インフラストラクチャの重要なコンポーネントの徹底的な評価 (ステップ 1)、脅威の潜在的な侵入口の特定 (ステップ 2)、適切なセグメンテーションの決定 (ステップ 3) が含まれます。重要な資産の依存関係と相互作用を理解することで、レジリエンスのあるセキュアなアーキテクチャを構築できます。

これらは、ZT のポリシー実施ポイント (PEP) と呼ばれ、レイヤー 7 ポリシー制御用に細かく調整できるソフトウェア (エージェントなど) で保護されている場合、実施ポイントの計画は、はるかに簡単な作業になり、容易に導入できます。ヘッドレスデバイス (IoT など) やサイバーフィジカル資産、OT/ICSなどのレガシーデバイスが普及している環境では、この手順は少し複雑になる可能性があります。これについては、次のセクション「ポリシー実施ポイントの計画」で詳しく説明します。

計画が完了すると、ZTA設計によって、保護されたOT/ICS環境全体で均一で堅牢なセキュリティ対策が確保されます。

OT/ICSアーキテクチャの図解

環境を図式化することで、この段階でより直感的で綿密な計画を容易にする視覚的な表現が得られます。まだ図式化されていない場合は、対象範囲の OT/ICS 環境の図式を作成することが最も実用的な次のステップです。

図式は、複数の入力またはデータソースに基づいて手動で作成および更新できます。最終的には、理想的な ZT 環境には、このタスクを自動化するための統合と最新化が備わっているはずですが、ほとんどの組織はそこから始めていません。

この段階での一般的なオプションには、次の入力と方法の一部またはすべてが含まれます。

- ネットワーク図を手動で作成する (Microsoft Visio または同様のツールなど)
- サードパーティの検出およびインベントリツールを使用する (検出を自動化したり、ネイティブで視覚化を提供したり、視覚化ツールへの API 接続を提供したりできるツールが理想的)
- 検出およびインベントリ管理のためにマネージドサービスパートナーと契約する (Claroty、Dragos、Nazomi、Armis、Zscaler など)
- メーカーベンダー固有のツールを活用する (Siemens、Rockwell Automation、Emerson、Honeywell、Schneider Electric、Yokogawa など)

この図に含めることを検討すべき要素は次のとおりです。

- ステップ 1 で特定された各資産はプロテクトサーフェスを定義
- 論理接続とトポロジ (具体的には、ステップ 2 で特定された各業務フローのマッピング)
- 物理接続とトポロジ (OSI レイヤー 1 ネットワーク接続)
- ネットワーク接続とトポロジ (OSI レイヤー 2 およびレイヤー 3 ネットワーク接続)
- システムに保存されているデータまたはシステム内でアクセスされるデータの分類
- 保護された資産のビジネスへの影響
- 論理接続とネットワークルーティングに使用されているプロトコル
- 該当する場合は、その他の依存関係、ユーザー数、およびアクセスパラメータを詳述した関連メモ。

このホワイトペーパーで Siemens がさらに説明しているように、このドキュメントの前半で説明した ISA/IEC 62443 ゾーンとコンジットモデルは、ZTA にうまくマッピングされます。組織がすでに ISA/IEC 62443 ガイダンスに従っている場合や、ISA/IEC 62443 に基づくドキュメントや評価がある場合は、ZTA 計画に直接転送できる要素が多数あります。

セキュリティゾーンとゼロトラスト・プロテクトサーフェス

ISA/IEC 62443 セキュリティゾーンは、プロテクトサーフェスを定義する ZT タスクと相関しています。

ステップ 1 を思い出してください。セキュリティゾーンとは、共通のセキュリティ要件を共有する機能的、論理的、および物理的な関係に基づいてシステムとコンポーネントをグループ化したものです。プロテクトサーフェスを定義して業務フローをマッピングするステップ 1 と 2 の後、業務フローのマッピングの一部としてまだグループ化されていない場合は、資産をセキュリティゾーンにグループ化できます。

理想的な ZTA では、各資産は独自のプロテクトサーフェスであり、したがって独自のセキュリティゾーンです。ただし、出発点として、セキュリティゾーンに分類された資産のグループまたはビジネス運用システムを使用することは許容される、あるいは避けられない場合が多数です。これは、次のステップでポリシーを作成するために後で調整することができ、その時点で、可能であれば追加の粒度が適用されます。

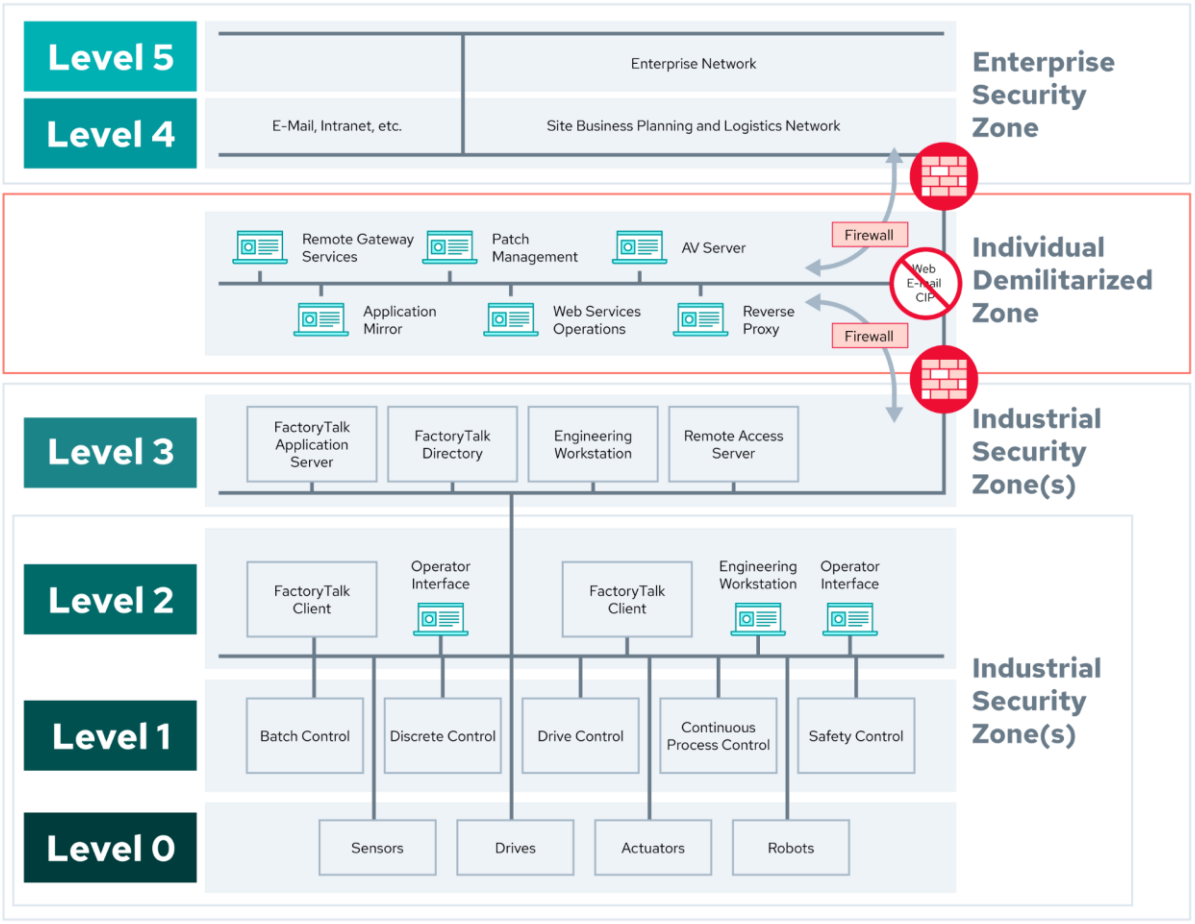
セグメンテーションとゼロトラスト実施ポイント

ISA/IEC 62443 内のセグメンテーション モデルは、ZT ポリシー実施ポイント (PEP) の配置とタイプと相関しています。

セグメンテーションの要件は、ゾーンとコンジットのビューで明らかになります。ここでは、どの資産が相互に通信する必要があるかが明確になります。追加のコンジットは、エンタープライズ IT ネットワークと OT ネットワーク間を通過するリモートアクセスまたはアクセスパスも定義します。

運用上、IT ネットワークと OT ネットワーク間のセグメンテーション、および OT ネットワーク内のセグメンテーションは、アーキテクチャと実装の両方においてエンタープライズ IT セグメンテーションとは異なります。具体的には、IT ネットワークでは、さまざまなネットワークやデバイスへのアクセスやそれらの通過を許可するためのファイアウォールとルールの中央セットが存在する場合があります。

OT ネットワークでは、理想的には、Purdue モデルレベル内で複数のホップを通過する単一のパスがあってはなりません。たとえば、企業の IT ネットワークまたはインターネット (Purdue モデル レベル 5) から HMI (Purdue モデル レベル 2 または 3) に直接 VPN またはアクセスパスを設計することはありません。代わりに、企業の IT ネットワーク (Purdue モデル レベル 4) から IT/OT DMZ (Purdue モデル レベル 3.5) への 1 つのホップ (またはコンジット) があり、その後、OT/ICS 管理 (Purdue モデル レベル 2 または 3) への別のホップ (コンジット) があります。



***Purdue**モデルのマルチホップ（出典: 産業用制御システム向け Purdue モデル)*

とはいえ、注目すべき例外がいくつかあります。

- OT 環境から (例) プロセスの監視やデータ収集/分析に送信される一方向のデータ。
- 接続された SaaS アプリケーションなど、一度に複数の境界を越える可能性のある OT 資産とのやり取り専用のアプリケーション。
- AI/ML などのクラウドテクノロジーを生産プロセスに導入したり、セルラー機能を導入したりすること。

さらに、さまざまな OT システム、IT システム、クラウドプラットフォーム間のシームレスなデータ交換と統合を促進する統合名前空間の概念は、複雑なソリューション処理のためのイベント駆動型アーキテクチャにより、注目を集めています。

ISA/IEC 62443 標準とゾーンとコンジットモデルは、参照モデルの唯一のオプションではありませんが、ほとんどの CI セクターで広く使用され、採用され、参照されているベンダーニュートラルの国際標準を提供します。このモデルは ZT 計画によく適合しており、計画を支援するリソースが多数用意されています。

OT/ICSにおける実施ポイント（PEP）の計画

ZTA を設計する際は、運用と保守の容易さの重要性、および進化するネットワークとビジネス要件に適応する柔軟性を考慮してください。ゼロトラストアーキテクチャ (NIST SP 800-207) で説明されているように、ポリシー実施ポイント (PEP) とポリシー決定ポイント (PDP) を含む、コントロールプレーンとデータプレーンの両方にわたる冗長性を確保することも同様に重要です[32]。

この冗長性により、単一障害点が排除され、重要なシステムの可用性と安全性が保護されます。このような包括的なアプローチにより、レジリエンスと適応性に優れた ZT フレームワークが保証され、効率性、俊敏性、中断のない運用で CI が保護されます。

CI、特に OT/ICS 環境では、ユーザー、デバイス、保護された資産間の情報の流れとやり取りを規制するためのきめ細かいアクセス制御が必要です。

ポリシー実施ポイント（PEP）の配置

ZTA の基礎となる目標は、実施ポイントを保護対象資産のできるだけ近くに配置することです。最新のアプリケーションとワークロードの場合、ソフトウェアベースの ZT エージェントを資産内または資産のすぐ前に追加するのは通常簡単です。これは、エンタープライズ IT ネットワーク (Purdue モデル レベル 4 以上)、IT ネットワークと OT ネットワーク間の DMZ の一部 (Purdue モデル レベル 3.5 前後)、および OT/ICS アプリケーションサーバー、データベース、データヒストリアン、エンジニアリングワークステーション、および HMI が存在する制御および処理ネットワーク (Purdue モデル レベル 2 および 3) に推奨される実装です。

Purdue モデルの下位 (レベル 0 および 1)、つまりフィールドデバイスに近い環境では、環境は多くの場合、レガシーまたは簡素化されたオペレーティングシステム、PLC、およびソフトウェアクライアントをサポートできないその他の資産で構成されます。

このようなシナリオでは、インフラストラクチャを改造してレイヤー 7 (アプリケーションレイヤー) でポリシーの実施を有効にするか、OSI モデルのレイヤー 2 (データリンクレイヤー) またはレイヤー 3 (ネットワークレイヤー) でネットワークベースの実施を実装する必要がある場合があります。この改造には、従来のソフトウェアクライアントが実行不可能な場合にセキュリティ対策を適用するために、レイヤー 7 ポリシーをサポートするネットワークルーターをインストールするなどの機能の追加が含まれる場合があります。

注: L7 ポリシーでは、アプリケーションレベルのトラフィックを詳細に検査する必要があり、多くの場合、このデータをプロキシするポリシー実施ポイント (PEP) が関係します。OT システムには特殊なプロトコルと多様なテクノロジーがあるため、ルーティングレイヤールールに重点を置いた L3 ポリシーを実装する方が実用的であることが多いです。このアプローチは、よりシンプルで邪魔にならないセキュリティ対策が望ましい OT システムの現実によく合致します。

OT/ICSの実施ポイントを計画する際の考慮事項は、以下の通りです。

- ISA/IEC 62443 ダイアグラム、ドキュメント、リスク評価、ゾーンとコンジットの計画、コンプライアンスレポートまたは監査からのドキュメント/証拠など、既存の作業を使用します。

[32] PDPは、ZTAの重要な概念であるコントロール プレーンのポリシー エンジンです。 詳細についてはNIST SP 800-207を参照

- 資産がソフトウェアエージェント/クライアントをサポートしている場合は、それをポリシー実施ポイントとして検討します (ゼロトラストネットワークアクセスソリューション、特権アクセス管理など)。
- 資産がソフトウェアエージェント/クライアントをネイティブにサポートできない場合は、それを拡張またはアップグレードしてサポートすることを検討します (資産を更新してソフトウェアをインストールするか、保護された資産の前にソフトウェアまたはハードウェアベースの実施ゲートウェイを追加するなど)。
- 資産がソフトウェアエージェント/クライアントをサポートできない場合は、次のようなネットワークベースの実施ポイントを計画します。
    - OT/ICS に適したファイアウォールを使用したレイヤー 3-7 セグメンテーション
    - SDN や VRF などの仮想ネットワークソリューションを使用したレイヤー 3-7 セグメンテーション
    - OT/ICS に適したルーターまたはルーティングスイッチを使用したレイヤー 2-4 セグメンテーション
    - 専用の LAN マイクロセグメンテーションゲートウェイを使用したレイヤー 2-3 セグメンテーション
    - 一方向ゲートウェイまたはデータダイオードを使用したレイヤー 1-2 セグメンテーション
- この機会を利用して、ステップ 5 で監視する必要があるもの、継続的な監視とメンテナンス、および監視の実現方法を特定します。

OT/ICS 環境の状況は急速に進化しており、レガシーデバイスやヘッドレスデバイスの課題に対処する革新的なソリューションが登場しています。たとえば、Siemens は「マシン用 ID カード」というコンセプトを導入し、SCALANCE-LPE 機器を開発しました。一方、Zscaler はゼロトラストセルラーエッジに接続する「ゼロトラスト対応 SIM カード」に取り組んでいます。これらの進歩により、従来は直接 PEP に対応できなかったデバイスに ZT の原則を適用する道が開かれています。このようなイノベーションにより、最新のセキュリティパラダイムとレガシーインフラストラクチャのギャップが埋められ、さまざまな OT/ICS 環境にわたってより包括的な ZTA が可能になります。

ステップ 1 と 2 で発見された情報の組み合わせは、全体的なアーキテクチャを計画し、段階的に実行されることが多い ZT 実装の優先順位を付ける優れた出発点となるはずです。

この段階での賢明な計画により、次のステップ (ステップ 4、ZT ポリシーの作成) で意図したポリシーを確実に実施できるようになり、より広範なポリシーステートメントから開始し、プログラムが成熟するにつれて詳細度を微調整する柔軟性が得られます。

ステップ4：OT/ICS におけるゼロトラストポリシーの作成

CSA には、ZTAC Resource Hubにある 5 段階の実装プロセスに関する一般的なガイダンスがあります。このセクションでは、OT/ICS 環境に特化したガイダンスを提供します。

ZTポリシーの作成は、最初の3つの計画ステップを終えた後の、最初の大きな「実行」ステップです。この段階で、ステップ3で設計した計画的なアクセス制御を実行し、ゼロトラストアーキテクチャを構築します。

アクセス権限を微調整し、定期的にアクセス権限を見直すことで、ユーザーが各自のタスクに必要な重要な資産や機能のみにアクセスできるようになります。最小特権の原則を採用し、アクセスは指定されたタスクに必要な最小限に制限されます。このアプローチは、潜在的な攻撃ベクトルや不正アクセスを効果的に最小化します。

OT/ICS環境におけるゼロトラストポリシーは、ISA 62443の通信経路に似たきめ細かな許可ルールが中心で、許可されたユーザーだけが指定されたアプリケーションを通じて特定のリソースにアクセスできるようにします。従来のIT環境では、アクティブなセッション中に動的なポリシー要素が変更された場合、ZTは通常アクセスの即時終了を義務付けていますが、OT/ICSではより微妙なアプローチが必要です。ゾーンの境界では、デフォルトで拒否(deny-by-default)するスタンスが依然として重要です。しかし、ゾーン内では、安全への配慮から、デフォルトで許可(allow-by-default)するアプローチが必要な場合があります。この適応は、産業環境において、セッションを突然終了させたり、重要なシステムへのアクセスを遮断したりすることの潜在的な危険性を認識するものであり、人命の安全を脅かす可能性があります。したがって、OT/ICSにおけるZTの適用には、安全で中断のないオペレーションを維持する必要性と、厳格なセキュリティ対策を天秤にかける、微妙なバランスが求められます。このアプローチは、産業環境特有の運用上の要求と安全要件を認識しながら、堅牢な保護を保証するものであり、IT中心のZT実装との重要な違いを示しています。

ゼロトラストポリシーの目標

ZTポリシーの作成で以下を可能にします。

1. **アプリケーション管理の簡素化：**CIオペレーションをサポートするために不可欠なアプリケーションに焦点を絞ることで、望ましくないアプリケーションをすべて特定してブロックするという継続的な作業を試みるよりも管理しやすくなります。
2. **セキュリティにフォーカス：**ほとんどの違反や悪意のある活動は許可ルールで発生することを認識し、このポリシーは許可されたトラフィックのセキュリティの取り組みに集中させ、正当なビジネス目的に厳密に必要なものだけを許可します。

ゼロトラストポリシー作成のための行動

プロテクトサーフェスと資産（ステップ1で特定）、マッピングされた業務フロー（ステップ2）、ZTA（ステップ3で設計/計画）に基づき、第4ステップで以下のアクションを行い、ZTポリシーを作成します。

ユーザーとデバイスの識別認証

OT/ICS環境において、主要なトランザクションポイントにおけるユーザーとデバイスの認証と認可を実装します。

- 厳格な本人確認と、重要なシステムへのタイムリーなアクセスの必要性のバランスをとること。
- 認証の失敗が業務の継続性と安全性に及ぼす潜在的な影響を検討。
- 戦略的に実施ポイントを配置することで、運用上のリスクを最小限に抑えつつ、セキュリティ上のメリットを最大化します。
- デバイスポスチャ、ユーザーの動作、アプリケーションの動作を常時監視し不正アクセスの試行を含むセキュリティイベントの迅速な特定を可能にします。

セキュリティポリシールール

CI要件を念頭に置いた包括的なセキュリティポリシールールが策定されます。これらのルールには以下が含まれます。

- **ネットワークセグメンテーション**：このアーキテクチャは、ネットワークをセグメント化し、アクセス権限を制限し、脅威のラテラルムーブメントを防ぐように設計します。
- **最小特権の原則**：アクセス権は最小特権の原則によって厳密に管理され、ユーザーが特定のタスクに必要なリソースにのみアクセスできるようにします。
- **トラフィックの検査と記録**：潜在的なセキュリティ上の脅威を特定し、対処するために、継続的なトラフィック検査を実施します。トラフィックの詳細なログは、セキュリティインシデントの調査に役立ちます。

セキュリティ基準の遵守

セキュリティポリシーのルールは、CIに特有の確立されたセキュリティ基準を厳守します。

ユニバーサル・ユーザー・フォローアップ

CIでは、ユーザー監視はシステムの能力によって異なります。個々のアカウンタビリティをサポートするシステム（Windowsマシンなど）では、ユーザーを継続的に監視・追跡し、一貫したセキュリティの実施を保証します。しかし、多くのOTシステムは、LDAPのような従来のユーザー管理技術をサポートしていません。このような場合は、以下のような別のモニタリング戦略を採用すべきです。

- 構成管理ツールを使用して、個人によるものでなくてもシステムの変更を検出します。
- 個別アカウントが不可能な場合はグループアカウントを導入し、デフォルトのパスワードを常に変更します。
- 物理的なアクセス制御を利用して、システムへのアクセスを制限し、監視します。
- 他の監視形態が不可能な場所にカメラを設置します。

このアプローチは、説明責任の必要性とOT環境の技術的限界のバランスをとり、多様なシステムにわたってセキュリティ警戒を維持します。

復号ポリシールール

必要に応じて、復号ポリシールールを使用してアプリケーショントラフィックを可視化し、セキュリティポリシールールでトラフィック内の潜在的な脅威を効果的に検査して識別できるようにします。

ゼロトラストポリシーにおける資産別セキュリティ境界

OT/ICSのZTAでは、「資産固有のセキュリティ境界」が「マイクロセグメンテーション」の概念を補完します。マイクロセグメンテーションが粒度の細かい分割によってネットワークトラフィックを効果的に制御するのに対して、資産固有のセキュリティ境界は、重要インフラ内の重要な資産のすぐ隣にセキュリティ制御を配置することに重点を置いています。これらの境界は、各プロテクトサーフェスを物理的または論理的に囲むことで、ZTの原理を拡張し、正確で特化したコントロールを実現します。この方法では、セキュリティ対策が保護する資産にできる限り近接し、内部のアタックサーフェスを最小限に抑え、厳格なアクセス制御を実施することで最小特権の原則に沿うようにします。

ZTのポリシールールは、このような資産固有のセキュリティ境界を定義し、いつ、どのような状況で、誰が、どのような資産と相互作用できるかを正確に制御します。業務の継続性と安全性が最優先されるOT/ICS環境では、このレベルの特殊性が不可欠です。マイクロセグメンテーションと資産固有のセキュリティ境界の両方を実装することで、企業は、ネットワークトラフィックを保護すると同時に物理資産の周辺を強化する、強固な多層防御戦略を実現することができます。

資産固有のセキュリティ境界をZTモデルに統合することで、OT/ICS特有の課題に適応する、より包括的なセキュリティフレームワークが可能になります。このようなセキュリティアーキテクチャは、多様な運用技術やさまざまなアクセス要件がある環境では特に有益です。資産固有のセキュリティ境界を導入することで、保護措置が保護する運用要素に近づくため、全体的なセキュリティポスチャが強化され、CI運用の即応性とレジリエンスが高まります。

ポリシー作成のためのキップリングメソッド

ZTポリシーは、ネットワークとそのポリシーの「誰が、何を、いつ、どこで、なぜ、どのように」の側面に対処するキップリングメソッドを使用して作成することができます。ポリシーの作成にキップリングメソッドを活用することで、きめ細かな制御が可能になり、既知の許可されたトラフィックと正当なアプリケーション通信のみがCIネットワーク内で許可されるようになります。この戦略的プロセスは、従来のポートベースのファイアウォールルールへの依存を最小限に抑えながら、アタックサーフェスを大幅に削減します。

キップリングメソッドを採用することで、OT/ICSネットワーク内のアクセス制御と通信について、正確なポリシーを定義することができます。次のようなポイントを押さえれば、簡単にポリシーが立てられます。

誰が（アイデンティティ）

CIリソースへのアクセスを許可されたユーザー、デバイス、およびエンティティを特定し、定義します。インフラストラクチャ内での責任とタスクに基づいて、さまざまな担当者の明確な役割と権限を確立します。

- *重要な質問*：誰がこのリソースにアクセスする必要がありますか？
- *考察*：
    - 許可されたユーザー、役割、エンティティの特定
    - 責任に応じたアクセス権限を設定し、その正当性を定期的に見直します。
    - フィッシングに強い多要素認証を導入し、セキュリティを強化します。
    - ユーザーのアクセス権を定期的に見直し、更新します。
    - 合理化された管理のための中央ユーザーアイデンティティリポジトリを維持します。

何を（アプリケーション）

承認されたアイデンティティが重要なリソースにアクセスするために使用できる承認済みのアプリケーションとサービスを決定します。セキュアで認可されたアプリケーションのみがインフラとやり取りできるようにします。

- *重要な質問*：どのようなアプリケーションが許可されていますか？
- *考察*：
    - 承認されたセキュアなアプリケーションの定義。
    - アプリケーションの許可リストと拒否リストの実装。
    - アプリケーションの使用状況を監視し、不正なソフトウェアを検出します。

いつ（タイミング）

重要なリソースへのアクセスを許可する条件を指定します。特定のアイデンティティが、いつ、どのような特定の状況下で資産やシステムと相互作用できるかを制御するアクセスルールを定義します。

重要なのは、緊急事態において、オペレータが重要なシステムから締め出されないようにすることです。

- *重要な質問*：アクセスはいつ可能ですか？
- *考察*：
    - 特定のアクセススケジュールとタイミングルールを設定します（緊急事態を考慮しながら）。
    - 重要なリソースに時間ベースのアクセス制御を導入します。
    - 一時特権のアクセス期限を設定します。

どこ（宛先）

認証されたアイデンティティ が通信を許可される CI 内の特定のサーバー、データベース、ネットワークセグメント、およびその他の資産を特定します。

- *重要な質問*：アクセスはどこでできますか？
- *考察*：
    - 許可された宛先またはエンドポイントを特定します。
    - 通信を制御するためのネットワークセグメントとサブネットを定義します。
    - 必要に応じて地理的制限を実施します。

なぜ（目的）

重要なリソースへの各アクセス要求の背後にある理由と目的を特定します。リクエストの正当なニーズに基づいてアクセスが許可されるように、データの分類とコンテキスト情報を適用します。

- *重要な質問*：なぜアクセスが必要なのですか？
- *考察*：
    - 各アクセス要求の理由と目的を文書化します。
    - 機密情報を区別するためにデータ分類を適用します。
    - アクセスの正当性を判断するためにコンテキスト情報を使用します。

どのように（アクセス方法）

認証されたアイデンティティ が重要なリソースにアクセスするために使用する方法とプロトコルを説明します。これには、許可される通信チャネル、認証メカニズム、暗号化標準の指定が含まれます。

- *重要な質問*：アクセス権はどのように付与されるのですか？
- *考察*：
    - 認証方法（ユーザー名/パスワード、トークンなど）を指定します。
    - データ伝送の暗号化

- 許可される通信プロトコル（HTTPS、SSHなど）を定義します。
- リモートアクセスには仮想プライベートネットワーク（VPN）またはその他の安全な経路を利用し、必要に応じてMFAを組み合わせます。

ステップ5：OT/ICSにおける継続的なモニタリングとメンテナンス活動

CSA には、ZTAC Resource Hubにある 5 段階の実施プロセスに関する一般的なガイダンスがあります。このセクションでは、OT/ICS 環境に特化したガイダンスを提供します。

CIにとって、継続的なモニタリングと分析は、潜在的な脅威を検知し、迅速に対応するために極めて重要です。ネットワークトラフィック、ユーザーの行動、デバイスのアクティビティをリアルタイムで分析することで、セキュリティチームは異常や潜在的なセキュリティ侵害を迅速に特定することができます。定期的なセキュリティ評価と侵入テストも実施し、脆弱性を特定し、プロアクティブに対処します。

OT/ICSのゼロトラストを継続的に支える活動

OT/ICS環境におけるZTプログラムには、最低でも以下の要素を含める必要があります。

OT/ICSのインシデント対応計画

チームがOT/ICS資産のインシデントレスポンス（IR）を任されている場合は、この活動のために専門家を招き、IR計画のOT/ICS部分を企業IT IR計画に組み込んで統合し、全体的なアプローチを行うことをお勧めします。

OT/ICS環境を専門としない企業ITサービスプロバイダーやIRチームには、このタスクに対応する能力はありません。専門のパートナーと協力し、サイバーセキュリティのインシデント発生中や発生後ではなく、早い段階でパートナーを特定し、確保します。そのパートナーは、ステップ1からステップ5まで、ZTプランニングの他の活動にも力を貸してくれるでしょう。

OT/ICS資産も狙われるかもしれませんが、近年、注目すべきCI攻撃は企業のITサイドから発生しています。これは、OTとITのIR計画に総合的に取り組むべきもう一つのケースです。ZTAは、保護対象資産、運用フロー、およびITネットワークとの間を含む依存関係を明確にします。

OT/ICSの可視化とモニタリング

OT/ICSネットワークへの可視性は、サイバーセキュリティ計画の重要な要素であり、ZTAの必須要素でもあります。監視が必要な資産とデータパスを特定し、適切なデータを収集し、適切なリポジトリに送信する計

画を立てていることを確認します。これには、集中型ロギング、OT/ICS SOCツール、ネットワークの監視を担当するメーカーまたはサードパーティパートナーのツールが含まれます。

また、これらの環境はOT/ICS環境に特化したプロトコルで通信しており、従来の企業ITツールはこのトラフィックに適さなかったり、認識していない可能性があることに留意してください。製造業者、設置業者/統合業者、または監視パートナーと協力し、OT/ICS 対応ツールが導入されていることを確認します。これにはおそらく、他のツールの中でもOT/ICS対応ファイアウォールが含まれるでしょう。

OT/ICSネットワーク（対ITネットワーク）の顕著な利点の1つは、よりきめ細かな可視性と高精度なアラートを提供できることです。このようなネットワークでは、ITネットワークで問題となるような継続的なチャッターや大量のデータやフローが発生しないため、ベースラインや異常の監視や特定が著しく容易になります。

OT/ICSにおける脆弱性管理

以前、「OT/ITのアーキテクチャの違い」の中で、OT/ICSネットワークにおいてパッチを適用することが適切である割合は4%から10%程度であることを説明しました。つまり、OT/ICSネットワークの脆弱性管理プログラムは、パッチ管理を中心に据えるべきではありません。その代わりに、コンテキストに基づく脆弱性評価を含み、可視化／モニタリングやその他の緩和策に大きく依存する必要があります。ZTポリシーが適切に実装されれば、OT/ICS 脆弱性管理プログラムにおける完璧な緩和コントロールとして機能します。

ネットワーク側では、SDP（Software-Defined Perimeter）やSPA（Single-Packet Authorization）[33] などの技術を使用して、未認証/未検証のエンティティから機器を見えないようにすることや、SPAによって導入されたネットワーク難読化の原則に基づきながら、エンドポイントやサービスの隠蔽のみに焦点を当てるのではなく、より広範なネットワークアーキテクチャレベルにこれらを拡張している新興技術のNHP（Network Hiding Protocol）[34] などを緩和策に含めることができます。

詳細な継続的ゼロトラストアーキテクチャの取り組み

ZTAの成長と進化に伴い、環境を保護し続けるZTAを維持するには、継続的な取り組みが必要です。このような取り組みは、サイバーセキュリティプログラムの成熟や、法律や業界規制の遵守を維持するための既存の取り組みと（重複しないように）整合させる必要があります。

理想的には、ZTAは、これらの継続的な活動を自動化し、手作業による文書化と報告を制限できる成熟度を満たしています。手動であれ自動であれ、ZTのライフサイクルと活動は、対象システムの寿命を通じて継続する必要があります。

これらの更新の周期は、データ収集がどの程度手作業か自動化されているか、また、地域やセクターにおけるサイバーセキュリティの取り組みについて、一般的なガイダンス、規制要件、または法律がどのような活動を指示しているかによって異なります。最低限、これらの活動を毎年繰り返すことをお勧めします。シス

[33] Software-Defined Perimeter (SDP) Specification v2.0 | CSA
[34] OpenNHP Documentation

テムと自動化が可能であれば、90日ごとまたは継続的な分析が望ましい。安全、健康、環境に影響を及ぼす可能性のある業界では、変更管理の一環として文書を見直し、更新する必要があります。

活動内容は以下の通りです。

ステップ1の再検討、資産の変化に伴うプロテクトサーフェスの定義を再検討

これは、OT/ICSネットワークの買収や移動、追加、変更に関する内部チケットと承認を、ZTAタスクに連携させることで対処できます。

ステップ2の再検討、アクセス要件の変更に伴う運用フローのマッピングを再検討

資産が一定期間固定されたままであっても、アクセス要件や運用フローのマッピングを更新する必要がある場合があります。例えば、OT/ICSネットワークへの追加リモートアクセスを必要とする、屋内退避命令などのパンデミック・シナリオが挙げられます。

ステップ3と4の再検討、ゼロトラストアーキテクチャの構築とポリシー作成を再検討

技術の進歩、資産の交換やアップグレード、アクセスシナリオの変更に伴い、ZTAとポリシーも更新されます。これらの活動には、アーキテクチャの文書化および図の維持、ZTポリシーの実施ポイントに対応するコントロールおよび製品または統合の更新が含まれます。

この活動の一環として、セキュリティベンダーやツールを定期的に再評価し、ロードマップの更新を依頼して、利用可能な新機能や統合機能を把握することもお勧めします。

ステップ5の再検討、インシデントレスポンス、モニタリング、脆弱性管理プロセスを再検討

ZTのロードマップ全体は、繰り返し行うワークフローであり、ステップ5の環境の継続的なケアとメンテナンスの詳細も例外ではありません。インシデント対応計画、監視ツール、分析、脆弱性管理は、継続的な評価と改善活動の一部であるべきです。

[33] Software-Defined Perimeter (SDP) Specification v2.0 | CSA
[34] OpenNHP Documentation

OT/ICS における SANS トップ 5 クリティカルコントロール

多くの場合、サイバーセキュリティの専門家は、しばしば矛盾し、重複するサイバーセキュリティのガイダンスに圧倒されています。ここでのガイダンスの目標は、OT/ICSのためのZT計画を提供し続けることであり、可能な限り既存のガイダンスや活動に関連付けることです。

SANS Institute（SysAdmin, Audit, Network, and Security：システム管理・監査・ネットワークセキュリティ研究所）は、脅威を考慮した活動に基づいて適切な投資を行うための指針として、OT/ICS システムに不可欠な 5 つの管理策を提示しています[35]。5つの実施ステップをすべて終えた今、ZT戦略がSANSの重要管理策をどのように強化しているかを振り返ることができます。これらは、ここで提案されているZTロードマップの活動の多くとよく一致しています。

1. ICSインシデントレスポンス
2. 防御可能なアーキテクチャ
3. 視認性モニタリング
4. 安全なリモートアクセス
5. リスクベースの脆弱性管理

ゼロトラストとOT/ICSのための5つの重要コントロール

OT/ICSにおける5つの重要な管理とZTAとの関係は以下の通りです。

ICSインシデントレスポンス

OT/ICS固有のインシデント対応計画は、ZTロードマップのステップ5、継続的なモニタリングとメンテナンスの一部です。また、世界中のほとんどのCI部門で必要とされています。

「OT/ITとデジタルトランスフォーメーションの融合」と「OT/ICSのインシデント対応計画」で述べたように、インシデントレスポンスは、専門的な注意を必要とする重要な分野として浮上しています。ICSインシデントレスポンスが最初の重要な管理項目として特定されたため、OT環境のレスポンス計画はIT環境のそれとは根本的に異なることを理解することが不可欠です。

ZT戦略を採用することは非常に重要ですが、OT部門に合わせて明確に調整する必要があります。ZTの核となる原則は一貫していますが、その適用には、各部門特有の課題や業務上のニュアンスに対応するための特別な調整が必要です。これにより、セキュリティ対策が効果的かつ適切なものとなり、ITとOTの融合が進む状況に対応できるようになります。

[35] The Five ICS Cybersecurity Critical Controls

防御可能なアーキテクチャ

SANSは、可視化、ログ収集、資産識別、セグメンテーションをサポートするアーキテクチャは防御可能であるとしています。つまり、攻撃を受けた場合でも防御可能ということです。本書で詳述するゼロトラスト5段階の実装は、防御可能なアーキテクチャを作成するためのプロセスを提供します。資産の特定から監視まで、ZTAは防御可能なアーキテクチャの各機能に対応しています。

システムが最新のパッチに対応していない可能性のあるOT環境では、「パッチよりも緩和」という原則が優先されます。このアプローチでは、頻繁な更新よりも緩和策を重視します。運用フローのマッピングでは、セグメンテーション、アクセス制御、継続的なモニタリングを通じて、レガシーシステム固有の脆弱性を補うことを優先します。「脆弱性管理」のセクションで述べた追加のテクニックを思い出して ください。

ICSネットワークの可視性監視

この重要なコントロールは、プロトコルに対応したツールセットによる OT/ICS 環境の継続的なネットワークセキュリティ監視を推奨しており、ステップ 5 の継続的な監視と保守に合致します。このアプローチにより、OT/ICSシステムの運用状態とセキュリティポスチャに対する包括的な可視性が確保されます。

OT/ICS環境では、可視性監視は主に内部変更に焦点を当てます。ZTの原則は、環境内の設定ファイルの変更を監視することの重要性を強調しています。これは、重要なシステムに対する潜在的なセキュリティ侵害や不正な変更を示す可能性があるためです。

この視点は、内部システムの変更に注意しながら、業務フローをマッピングするステップ2と一体であるべきです。

セキュアなリモートアクセス

セキュアなリモートアクセスには、リモート接続、パス、アクセス方法のインベントリが必要です。これらの項目は、ZTの導入プロセス全体を通じて定義されます。ステップ1のプロテクトサーフェスの定義に始まり、ステップ2の運用フローのマッピング、ステップ3と4のZTAの構築とポリシーの作成まで、ZTの導入プロセス全体を通じて定義されます。さらに、ステップ5の継続的なモニタリングにより、リモートアクセスが一元的に管理、制御され、悪用されていないことを確認します。

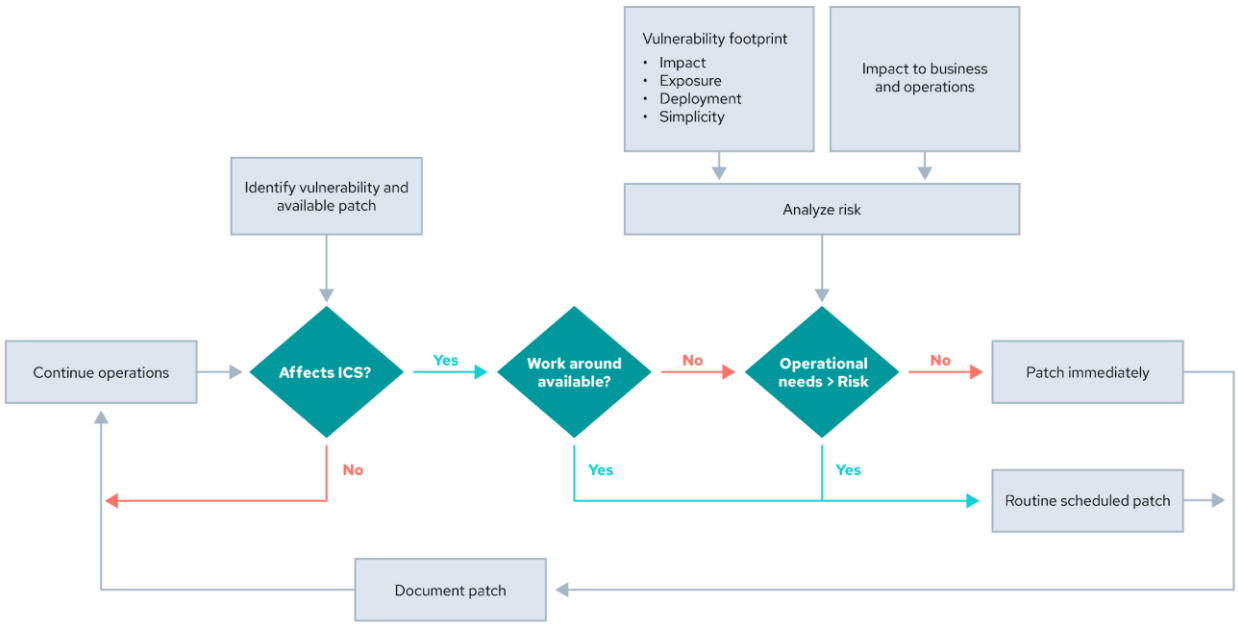
「ステップ 2 の締めくくり」で述べた、運用フローをマッピングすることの重要性を強調し、ステップ 2 を慎重に実施することで、セキュリティ確保の優先度が高いリモートアクセス通信経路、外部接続を特定することができ、多くのOTセキュリティインシデントがインターネットに接続したサービスから生じていることを認識できます。

リスクベースの脆弱性管理

OT/ICS 環境におけるリスクベースの脆弱性管理は、サイバーフィジカル資産、制御、および予想される運用条件を考慮します。ZTの導入プロセスでは、運用フローのマッピングを通じて重要なデータ経路を包括的に理解することで、このアプローチを強化します。この洞察は、セグメンテーション戦略に情報を提供し、効果的なリスク管理に不可欠なシステムの複雑さを簡素化します。

ZTの原則は、適切なパッチ適用を促進し、パッチ適用が不可能な場合の緩和策を導入し、継続的な監視を可能にすることで、この重要な制御をサポートします。このSANSのコントロールは、NISTサイバーセキュリティフレームワーク（CSF）[36]およびゼロトラストアーキテクチャ（ZTA）[37]と一致しており、デバイス、資産、アプリケーション、およびサービスのサイバーセキュリティを向上させる上で互いに補完し合っています。

重要なことは、OT/ICSにおける脆弱性管理は、特にスキャン、特定、およびパッチ適用プロセスにおいて、従来のIT慣行から逸脱していることです。CISAは、これらの環境における特有の課題を反映した、制御システムに特有のパッチ適用ワークフローを推奨しています[38]。



[36] NIST Cybersecurity Framework 2.0
[37] NIST Zero Trust Architecture
[38] Recommended Practice for Patch Management of Control Systems

新しいOTおよびICSシステムに関するガイダンス

本書は、既存の運用技術（OT）および産業制御システム（ICS）環境内でZTの原則を適用するためのガイダンスを提供することに重点を置いています。ここで説明する戦略と方法論は、組織が現在のインフラにZTセキュリティ対策を後付けできるように設計されています。これには、OT/ICSシステム固有の特性、課題、およびそのような制約がある中でZT機能を実装するための具体的な推奨事項についての詳細な検討が含まれます。

このガイダンスは一般的に既存の環境を対象としていますが、進化する脅威の状況とサイバーセキュリティ技術市場の両方を認識することが重要です。これには、特にCI組み込みの場合、技術が「セキュア・バイ・デザイン」であることを求める顧客と規制当局の要件の増加が含まれます。その結果、ベンダーやOEM (Original Equipment Manufacturers) は、一般的なサイバーセキュリティとZT機能を、新しいテクノロジーや既存製品の機能強化に組み込むことが増えています。このような一般的なサイバーセキュリティとZT機能のプロアクティブな統合は、設計によって新しいインフラをセキュアに調達・実装できるグリーンフィールドの展開において特に重要です。

最新のソリューションによるゼロトラストの加速

業界の進歩に伴い、多くのベンダー/OEMがZTの機能と性能を自社のソリューションに組み込み、ハードウェアベースのセキュリティモジュール、マシン・アイデンティティ、ZTネットワーキング・オーバーレイ、継続的認証、マイクロセグメンテーション、強化されたモニタリングなどの機能を組み込み機能として提供しています。これらの機能の中にはベンダーが開発したものもあれば、ホワイトラベルまたは明示的なパートナーシップとの提携によって実現されます。

Siemens、GE Vernova、Rockwell Automation、Schneider Electric などがその例です。これらの例のいくつかは、直接的な製品の機能であり、いくつかは産業用制御システムにおけるZTの推奨事項です。これらの技術革新は、特にレガシーシステムがないグリーンフィールドのシナリオにおいて、最新のセキュリティフレームワークをより簡単に実装できるため、ZTポスチャの導入を大幅に促進することができます。また、これらの機能の一部は、ベンダーのOEMがソフトウェアベースの機能を提供し、それを既存の製品や設置基盤に対してOTA（Over-the-Air）で更新可能な場合、ブラウンフィールドのシナリオにも適用できることに留意すべきです。たとえば、産業用ファイアウォールにファームウェアのアップデートを適用してZTオーバーレイ接続性を有効にする場合が挙げられます。

ZTは、様々な柱を統合し、自動化されたアプローチに依存するため、包括的なポートフォリオ、パートナーシップ、およびオープンAPIを介したサードパーティの統合を構築するOEMベンダーは、CI（OT/ICS）組織がZTの高い成熟度に到達するための最適な支援を提供できる立場にあります（本文書で前述したCISAのZero Trust Maturity Modelを参照）。この統合は、セキュリティポリシーのリアルタイムでの適用や、IT環境全体にわたるセキュリティポスチャの継続的な検証を可能にするため、極めて重要です。これらのプロセ

スを自動化することで、企業は迅速かつ効率的に脅威を検出して対応し、人為的ミスを最小限に抑え、セキュリティ対策を一貫して適用されるようにすることができます。

これらの最先端技術を活用することで、組織はより効率的に堅牢なZTAを実現することができます。このアプローチは、セキュリティを強化するだけでなく、進化する規制要件への準拠を保証し、ダイナミックな脅威の状況により容易に適応します。

ZTの原則を新規および既存のデプロイメントに組み込むことで、企業はレガシーシステムの改修に伴う複雑さや制約を回避することができます。本文書は、既存の OT/ICS 環境のセキュリティを確保するための基本的なガイドとなるものであり、同時に、本質的なセキュア・バイ・デザイン・テクノロジーを目指す動向を認識した内容となっています[39]。

[39] CISA Secure By Design

まとめ

今日の相互接続された世界において、CIセクターは、絶えず進化するサイバーおよび物理的な脅威に直面しています。これらのセクターがデジタルトランスフォーメーションを採用し、オペレーショナルテクノロジー（OT）とインフォメーションテクノロジー（IT）の融合を進める中で、堅牢で適応性の高いセキュリティ戦略の必要性はかつてないほど高まっています。ZTは、急速な技術進歩や脅威の進化に対応し、高度化する敵対勢力から重要なシステムを守るための強力な戦略を提供します。

本書では、OT/ICS環境にZTの原則を適用するための包括的なロードマップを提供します。反復可能な5段階のプロセスを実行することで、組織は効果的にリスクを軽減し、CIのレジリエンスを高めることができます。

1. プロテクトサーフェスの定義
2. 運用フローのマッピング
3. ゼロトラストアーキテクチャの構築
4. ゼロトラストポリシーの作成
5. モニタリングとメンテナンス

ここで紹介するガイダンスは、画一的な解決策ではなく、各セクターの固有の要件に合わせ、また新しいシステムにも既存のシステムにも適用できる、柔軟で拡張性のあるアプローチです。ISA/IEC 62443 などの既存の標準を活用し、SANS が概説する 5 つの重要な管理策と整合させるとともに、新しいシステムに対するセキュア・バイ・デザインの原則を採用することで、この ZT 戦略は、現在のベストプラクティスと統合しながら、継続的な改善のための将来を見据えた道筋を提供します。

組織のコラボレーションとコミットメント

最終的に、CIへのZT導入を成功させるには、リスク軽減に対する組織の強いコミットメントとともに、部門を超えた協力的な取り組みが必要です。そのためには、サイバーセキュリティの専門家の専門知識、OTエンジニアやシステム運用者の洞察力、OTソリューションプロバイダーのイノベーションとともに、経営陣のコミットメントが必要です。オープンなコミュニケーション、共通の理解、そしてあらゆるレベルでのセキュリティと安全性へのコミットメントを促進することで、世界中のCIセクターはZTの力を活用し、現代の生活を支えるシステムを保護することができます。これにより、自らの運用を守るだけでなく、絶えず変化する脅威の状況に直面する中で、物理的および経済的な安定性に不可欠なサービスの安全性、信頼性、レジリエンスを向上させ、国際社会の総体的なレジリエンス向上に貢献することができます。

役立つリソース

参考文献

1. 既存のCIとOTのガイダンスと規則
    a. Critical Infrastructure resources by sector at NIST CSF 1.1 Critical Infrastructure Resources | NIST
    b. SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC
    c. ISA/IEC 62443 Series of Standards
    d. The Five ICS Cybersecurity Critical Controls
    e. PCAST Releases Report on Strategy for Cyber-Physical Resilience
    f. US OMB Memo M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget
    g. National Security Memorandum on Critical Infrastructure Security and Resilience | The White House
    h. PCAST Strategy for Cyber-Physical Resilience Feb 2024
    i. DHS Offers WMD, Critical Infrastructure AI Guidance – MeriTalk
    j. Mitigating AI Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators
    k. MITRE ATT&CK ICS Matrix
    l. Top 20 Secure PLC Coding Practices
    m. OT Zero Trust Alliance
    n. Simplifying Adoption of ISA/IEC-62443 Using the Zero Trust Model for Operational Technology - Palo Alto Networks
    o. ISAGCA Whitepaper: Zero Trust Outcomes Using ISA/IEC 62443 Standards
    p. Zero Trust Whitepaper - Siemens Global
    q. CRITICAL INFRASTRUCTURE - CYBYR
    r. CISA Identifying and Mitigating Living Off the Land Techniques
    s. CISA Alert: Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means
    t. Principles of Operational Technology Cyber Security
2. 地域別重要インフラ部門
    a. UK: Critical National Infrastructure | NPSA
    b. EU: erncip
    c. US: Critical Infrastructure Sectors | CISA
    d. Singapore: Cybersecurity Act
    e. India: National Critical Information Infrastructure Protection Centre
3. CSAリソース
    a. CSA Zero Trust Resource Hub
    b. CSA Cloud Security Glossary
    c. CSA Defining the Zero Trust Protect Surface | CSA
    d. CSA Map the Transaction Flows for Zero Trust | CSA

e. CSA Zero Trust for Critical Infrastructure Presentation Recording of Dr. Ron Martin
f. CSA Zero Trust for OT & IoT - Zscaler CSA ZT WG Presentation Recording
g. CSA Agentless Network Microsegmentation - BYOS
h. CSA ZT Networking for difficult use cases - CI/OT/IoT, air gapped networks and more - NetFoundry

4. その他の参考文献
   a. NSTAC Report to the President on Zero Trust and Trusted Identity Management
   b. International CIIP Handbook 2008/2009
   c. CISA Zero Trust Maturity Model Version 2.0
   d. DoD Zero Trust Reference Architecture
   e. DoD Zero Trust Capability Execution Roadmap
   f. DoD Zero Trust Strategy
   g. DoD Zero Trust Symposium 2024 recordings - day 1, day 2
   h. CISA/NSA/FBI/ASD ACSC Guidance: Best Practices for Event Logging and Threat Detection
   i. Consequence-driven Cyber-informed Engineering (CCE) - Idaho National Laboratory

5. サービスプロバイダー
   a. Dragos
      i. Robert M. Lee on LinkedIn: The Evolution of Industrial Cyberthreats: Year in Review Report
      ii. Asset Visibility for ICS environments | Dragos Platform
      iii. Key Concepts of ISA/IEC 62443: Zones & Security Levels | Dragos
      iv. Whitepaper: Network Segmentation Challenges and Solutions
   b. Claroty Asset Inventory - Platform
   c. Nozomi Networks
      i. OT Asset Inventory Management
      ii. ISA/IEC 62443 Compliance Mapping Guide
   d. Armis Full Asset Inventory and CMDB Enrichment
   e. ICS Village
   f. SCYTHE
   g. Zscaler
      i. Building a resilient manufacturing environment through zero trust OT cybersecurity controls
      ii. Complete OT Security | Zscaler
      iii. Zero Trust for OT & IoT - Zscaler

h. Zero Trust Security — Massive Scale Consulting

本稿で使用する略語の定義

本稿では、CSA 用語集[40]で定義されている以下の略語を使用します：

1. Critical Infrastructure (CI)
2. Cybersecurity and Infrastructure Security Agency (CISA)
3. Cyber Physical Systems (CPS)
4. Data, Applications, Assets, and Services (DAAS)
5. Distributed Control System (DCS)
6. Human-Machine Interface (HMI)
7. Industrial Control System (ICS)
8. Industrial Internet of Things (IIoT)
9. Operational Technology (OT)
10. Programmable Logic Controller (PLC)
11. Policy Enforcement Points (PEPs)
12. Policy Decisions Points (PDPs)
13. SysAdmin, Audit, Network, and Security (SANS)
14. Safety Instrumented System (SIS)
15. Hardware Security Module (HSM)
16. Zero Trust (ZT)
17. Zero Trust Architecture (ZTA)
18. Zero Trust Advancement Center (ZTAC)
19. Zero Trust Maturity Model (ZTMM)

用語集

ゼロトラスト用語集の参考文献

- CSA Glossary (main/primary)
- On2IT ZT Glossary - Zero Trust Dictionary (John Kindervag)
- CSA SDP Glossary (Software Defined Perimeter)

[40] Cloud Security Glossary