ホワイトペーパー

Cisco public

産業用オートメーション および制御システムを保護する サイバーセキュリティ フレームワーク

ISA/IEC-62443-3-3

目次

概要 2

ISA/IEC 62443-3-3 セキュリティ原則 3

安全なコンポーネントの活用 5

ISA/IEC-62443-4-1：セキュアな製品開発ライフサイクル要件 5

ISA/IEC 62443-4-2：IACS コンポーネントの技術的なセキュリティ要件 6

ISA/IEC-62443-3-3 の基本要件 6

FR1：識別、認証制御、およびアクセス制御（AC） 7

FR2：使用制御（UC） 9

FR3：システムの完全性（SI） 11

FR4：データの機密性（DC） 12

FR5：データフローの制限（RDF） 13

FR6：イベントへのタイムリーな対応（TRE） 14

FR7：リソースの可用性（RA） 15

ISA/IEC-62443-3 準拠に向けた取り組みの開始 16

シスコ検証済みデザイン（CVD） 19

まとめ 21

リンクと参考資料 21

概要

産業組織にとって、産業用オートメーションおよび制御システム（IACS）をサイバー脅威から保護することは最優先事項です。しかし、頭ではわかっていても、いざ行動に移すとなるとこれは非常に困難なタスクです。IACS とその基盤ネットワークは非常に複雑で、旧式のテクノロジーが使われ、セキュリティ手順も不十分であることが多いため、何から着手すべきかわからずに頭を抱えることになりがちです。

幸い、国際自動制御学会（ISA）によって ISA99 標準規格および技術に関する報告書がまとめられています。国際電気標準会議（IEC）は ISA と協力して、これらの報告書の大部分を IEC 文書として公開し、補足的なパートを開発して共通の ISA/IEC-62443 シリーズに追加しています。

ISA/IEC-62443 シリーズ標準規格および技術報告書は、さまざまな目的と対象者に対応する 4 つのグループに分類されています。パート 3-3 にはシステムセキュリティ要件とセキュリティ機能レベルが定義されており、これに基づいて目標とするセキュリティレベルを満たす IACS を構築し、各要件に対する組織のプラクティスを評価できます。この文書は、IT チームと運用チームが連携して産業インフラストラクチャを構築して、サイバー脅威と偶発的イベントの両方から効果的に保護し、かつ継続的に改善するための共通の基盤を提供します。

シスコは、エンタープライズ ネットワークの構築とサイバーセキュリティ分野で最もよく知られています。しかし、15 年以上にわたって世界の産業組織におけるオペレーションのデジタル化に貢献してきたことはそれほど知られて

いません。シスコは製造業、エネルギーや水道の公益事業、鉱業、港湾、鉄道、道路交通網といった産業と連携してきました。実際、産業用ネットワークのあらゆる領域で、シスコはリーディングカンパニーなのです。

運用テクノロジー（OT）の要件を深く理解し、かつ最先端のサイバーセキュリティ ポートフォリオを提供しているシスコは、産業組織にとって、IACS の保護と ISA/IEC-62443-3-3 規格への準拠を支援できる理想的なパートナーです。この文書では、この規格に含まれている要件について解説し、シスコがどのような支援を提供できるのかについて説明します。

ISA/IEC 62443-3-3 セキュリティ原則

この標準規格のパート 3-3 には、パート 1-1 に定義されているサイバーセキュリティ原則に準拠するための基本要件（FR）から派生した、以下を含む重要なセキュリティ要件（システム要件（SR）と強化策（RE））が定義されています。

最小限の権限

この原則は、データやプログラムへの望ましくないアクセスを防ぎ、アカウントが侵害された場合に攻撃をブロックするか遅らせるために、ユーザーに作業の実行に必要な権限のみを与えるものです。

多層的な防御

この原則は、階層型の防御技術を使用して、産業用ネットワークにおけるサイバー攻撃を遅らせるか防止するものです。またこの標準は、システムを「ゾーン」と呼ばれるグループに分割し、ゾーン同士が「コンジット」と呼ばれる通信チャネルを介して物理的、電子的、またはプロセスベースで相互に通信できるようにすることをシステムに義務付けています。

リスク分析

重大度、可能性、および影響に基づくリスク分析の概念は、目新しいものではありません。製造インフラストラクチャ、製造能力（製造のダウンタイム）、人的影響（けが、死亡）、および環境（汚染）に関連するリスクに対処するために、すでに使用されています。ただし、産業情報システムに固有のリスクに対処するには、リスク分析をサイバーセキュリティにまで拡張する必要があります。ISA/IEC-62443-3-2 には、IACS 向けのセキュリティリスク評価方法が記述されています。

補完的なセキュリティ対策

多くの場合、IACS のコンポーネントは、特定のセキュリティレベルを満たすために必要な機能を提供しません。そのようなシナリオでは、技術的か手順型かを問わず、補完的なセキュリティ対策を使用することで、必要な機能を確保できます。セキュリティソリューションに見られる複数の技術の組み合わせは、そのような役割を果たすことを目的に設計されています。

ゾーンとコンジット

ISA/IEC-62443 は、これらの原則に基づいて、ISA95 で使用される Purdue 参照モデル（図 1）を活用し、これらの機能レベルをゾーンとコンジット（図 2）にセグメント化する産業用制御システムアーキテクチャを提案しています。セグメンテーションは、ISA/IEC-62443-3-2 に規定されているセキュリティリスク評価の結果生まれたものです。

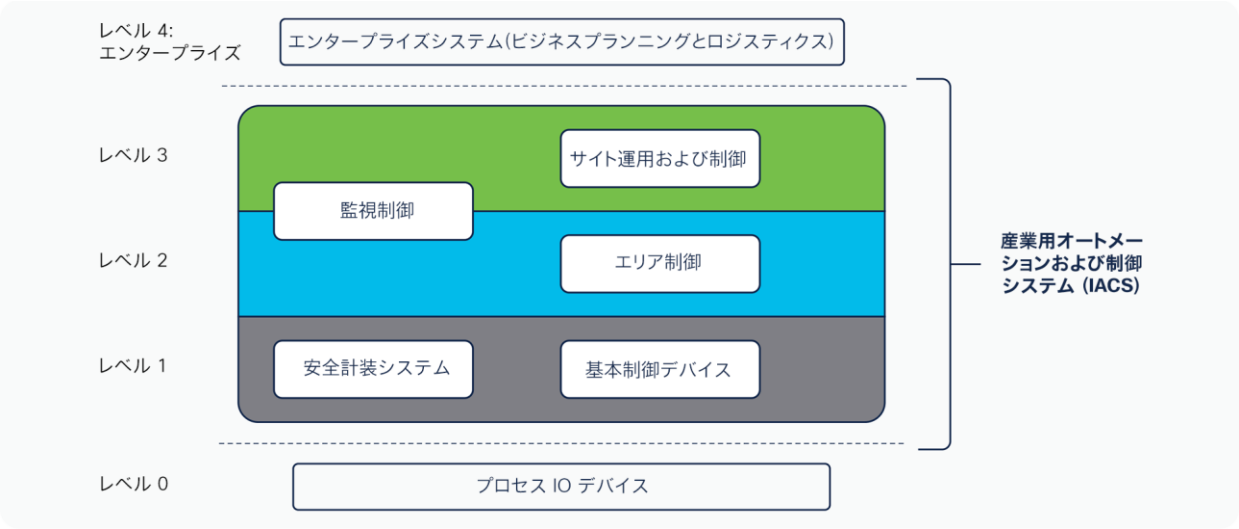

図 1.
ISA/IEC 62443 機能参照モデル（出典：IEC-62443-3-3 標準規格）

この規格によると、**ゾーン**とは、共通のセキュリティ要件を持つ、物理的または機能的に統合された資産の集合体です。これらのゾーンは、産業システム制御アーキテクチャの物理モデルと機能モデルに基づいて定義されます。IACS のすべての資産は、ゾーンに配置する必要があります。

コンジットは、ゾーン間の通信をサポートします。コンジットは、2 つ以上のゾーン間の通信チャネルの論理グループです。

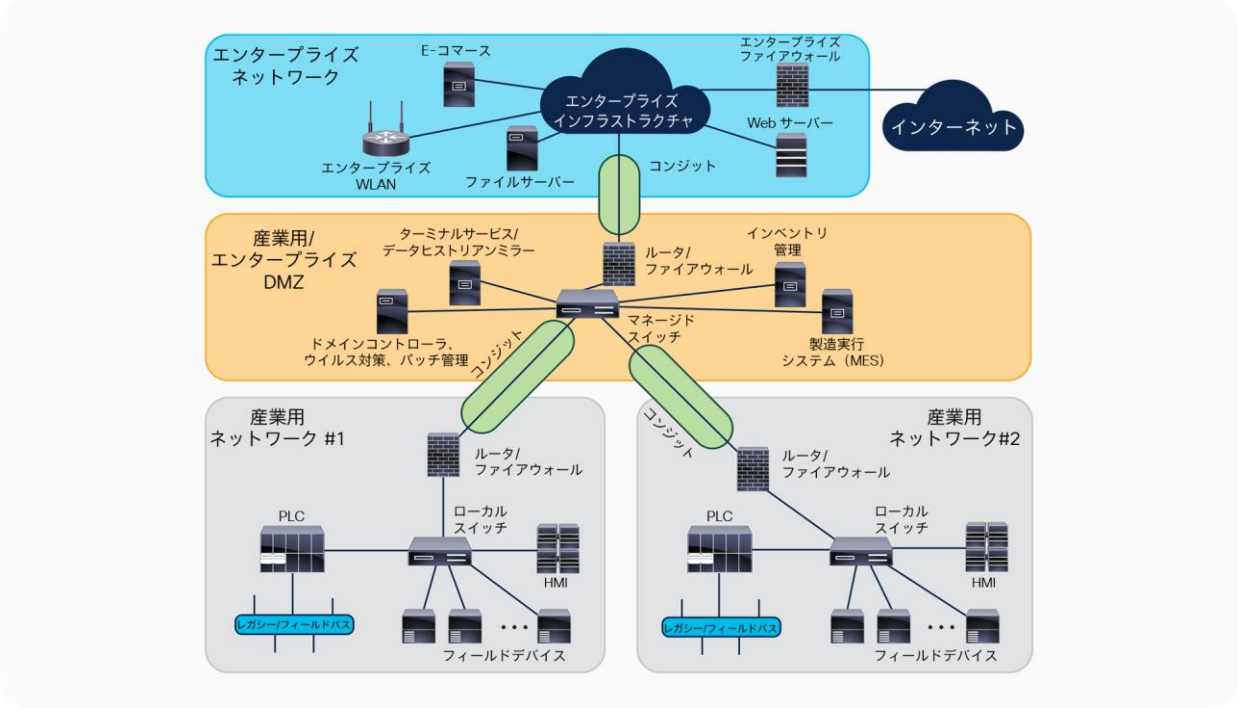

図 2.
産業用ネットワークゾーンとコンジットの例（出典：IEC 62443-3-3 標準規格）

安全なコンポーネントの活用

ISA/IEC-62443-3-3 は安全な IACS の原則に焦点を当てていますが、この標準規格シリーズの他のパートを活用します。たとえば、セキュリティプログラムが『IEC 62443-2-1：IACS 資産所有者のセキュリティプログラムの要件』に従って確立され、運用されることを前提としています。

また ISA/IEC-62443-3-3 は、安全なコンポーネントが展開されるか、追加の対策が実施されることも前提としています。これによってこの規格に規定されている要件を満たし、現在および将来の脆弱性や脅威の状況に対処することを想定しています。コンポーネントおよび開発の要件は、パート 4-2 および 4-1 に定義されています。これらの要件への対応は、コンプライアンスの達成に欠かせません。

ISA/IEC-62443-4-1：セキュアな製品開発ライフサイクル要件

ISA/IEC-62443 シリーズのこのパートは、IACS の構成に使用される製品を安全に開発するためのプロセス要件と、コンプライアンスのベンチマークを設定する成熟度レベルで構成されています。その内容は、要件、管理、設計、コーディングガイドラインの使用、実装、検証と確認、欠陥管理、パッチ管理、および製品サポートの終了のプロセスに関連しています。これらの要件は、コンポーネントのセキュリティ機能と IACS ソリューションの基盤となるセキュアバイデザイン（設計時にセキュリティを組み込む）アプローチにとってきわめて重要です。パート 4-1 の全体的な焦点は、製品の開発とリリースの高速化に対応するために不可欠な、継続的な改善です。

シスコのソフトウェアおよびハードウェア製品は、シスコセキュア開発ライフサイクル（Cisco SDL）に従って開発されているため、製品の計画からサポート終了にいたるまでセキュアバイデザインの考え方が徹底されています。シスコのすべての産業用製品の開発に適用される Cisco SDL は、IEC-62443-4-1 認定を取得しています。

ISA/IEC 62443-4-2：IACS コンポーネントの技術的なセキュリティ要件

このパートには、7 つの基本要件（FR）に関連する技術的な制御システムコンポーネントの要件が含まれています。このパートは、ISA/IEC-62443-3-3 に定義されているシステム要件（SR）および強化要件（RE）を、IACS 内に含まれるコンポーネント向けの一連のコンポーネント要件（CR）および関連する RE に拡張するものです。その目的は、IACS ソリューションを構築および統合するための制御システムコンポーネントの選択と調達を支援することです。

これに関して、この規格には、コンポーネントを特定のセキュリティレベル（SL）で IACS のシステム環境に統合するためのセキュリティ機能が規定されています。パート 4-2 には、ソフトウェア アプリケーション、組み込みデバイス、ホストデバイス、およびネットワークデバイスの 4 種類のコンポーネントについて、各資産の詳細に合わせて調整された要件が含まれています。要は、安全な IACS ソリューションを構築するには安全なコンポーネントをベースにし、必要に応じて補完的なセキュリティ対策を適用していく必要があるということです。

いくつかのシスコ製品は、すでに IEC-62443-4-2 認定を取得しています。シスコは、62443 認定を取得した開発プロセス（Cisco SDL）と併せて、重要なインフラストラクチャに IACS を展開するために不可欠な信頼性の高い通信製品を提供しています。

ISA/IEC-62443-3-3 の基本要件

この章では、各基本要件（FR）に関連して IEC-62443-3-3 に定義されているシステム要件（SR）と、これらに準拠するためにシスコがどのように役に立てるかについて詳しく説明します。FR 自体は、ISA/IEC 62443-1-1（用語、概念、モデル）に定義されています。

この標準規格の範囲によると、これらの要件は、IACS の構築と運用に使用されるすべてのコンポーネントに関連します。通常シスコは、資産所有者がネットワークおよびセキュリティのコンポーネントの要件と望ましいセキュリティレベルを満たすのを支援することができます。

この規格には、リスク分析の結果に応じて、組織がそれぞれの FR を達成するために選択できる 5 つの異なるセキュリティレベル（SL）が定義されています。

- **レベル 0：**特定の要件やセキュリティ保護の必要なし。
- **レベル 1：**偶発的イベントからの保護。
- **レベル 2：**悪意のあるユーザーによる、単純な手段、少ないリソース、一般的なスキルを使った、低モチベーションの意図的なイベントからの保護。
- **レベル 3：**悪意のあるユーザーによる、高度な手段、中程度のリソース、特定のスキルを使った中程度のモチベーションに基づく意図的なイベントからの保護。
- **レベル 4：**悪意のあるユーザーによる、高度な手段、広範なリソース、特定のスキルを使った高いモチベーションに基づく意図的なイベントからの保護。

組織はこれらのセキュリティレベルを使い、脅威の複雑さに応じたセキュリティ制御に必要な保護を定義できます。

FR1：識別、認証制御、およびアクセス制御（AC）

根拠

この規格のこのパートでは、産業用制御システムまたは特定のコンポーネントへのアクセスを許可する前に、ユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別および認証するための要件を説明しています。一部のコンポーネントには他のコンポーネントよりも強力な認証メカニズムが必要になる可能性があることを認識し、単一ゾーン内の制御を最小限に抑えることを推奨しています。

シスコが役に立てること

Cisco Identity Services Engine（ISE）は、有線および無線のネットワークデバイスと連携して、ユーザー、時間、場所、脅威、脆弱性、アクセスタイプなどの属性を使用した包括的なコンテキスト ID を作成します。これにより、ID が人間のものであるかどうかを問わず、ID のビジネス上の役割に合致する非常に安全なアクセスポリシーを適用できます。管理者はネットワーク上のエンドポイントで、誰が、何を、いつ、どこで、どのように許可するかを正確に制御できます。ISE は Microsoft Active Directory などの複数の外部 ID プロバイダーと統合できます。

さらに Cisco ISE は、容易に展開できる内部認証局を提供します。ISE はスタンドアロン展開および既存のエンタープライズ公開キーインフラストラクチャに認証局を統合する展開の両方をサポートしています。また、1 つまたは大量の証明書とキーのペアを手動で簡単に作成できるようにして、ネットワークに接続するデバイスに高度なセキュリティを提供できます。

人間のユーザーが工場フロアにある Windows ワークステーションにアクセスしたり、リモートでネットワークにアクセスしたりする場合、Cisco Duo により多要素認証（MFA）を実施し、アクセスを許可する前にユーザーの ID を確認できます。Duo Authentication for Windows Logon をインストールすると、インストーラで [RDP 経由のログイン時のみ Duo 認証を使用（Only prompt for Duo authentication when logging in via RDP）] オプションを選択しない限り、ローカルコンソールまたは Remote Desktop Protocol（RDP）のいずれを経由する場合も、すべての対話ユーザーによる Windows ログイン試行に MFA が追加されます。

Cisco Cyber Vision の主な機能は、資産インベントリの提供とフローデータの可視化です。クリアテキストプロトコルを使用して送信されたログイン情報の存在も検出できるため、管理者は中間者攻撃が発生する前に防御できます。

表 1. 識別、認証制御、アクセス制御のためのシステム要件

SR	説明	対応する製品機能
1.1	ユーザー（人）の識別と認証	• Cisco ISE は、有線ネットワークと無線ネットワークの両方でコンテキスト ID を提供します。 • Cisco Duo は、リモートアクセスユーザーの保護強化などの目的で、必要に応じて接続に MFA を提供します。
1.2	ソフトウェアプロセスとデバイスの識別と認証	• Cisco ISE は MAC 認証バイパス（MAB）を使用して、ネットワーク上のデバイスを MAC アドレスで認証します。 • Cisco Cyber Vision は IT および OT デバイスとそれらに関連するファームウェアを識別します。Cyber Vision によって構築されたデバイスインベントリは ISE と共有され、認証目的でも使用できます。
1.3	アカウント管理	• Cisco ISE は、スタンドアロンのアカウント管理ツールとして使用することも、Microsoft Active Directory と統合して個人アカウントとグループアカウント両方を管理することもできます。
1.4	識別子管理	• Cisco ISE は、ネットワーク内のすべての人とデバイスのポスチャを保存します。このポスチャで Cyber Vision を補完することで、デバイスの OT 固有の追加コンテキストを

SR	説明	対応する製品機能
		取得できます。

SR	説明	対応する製品機能
1.5	オーセンティケータ管理	• Cisco ISE はユーザーに最初のログイン後にパスワードを変更させ、それ以降は設定されたサイクルでパスワードを変更させることができます。 • Cyber Vision はクリアテキストプロトコルで送信されたパスワードを検出します。これにより、パスワードが中間者攻撃の対象であることを管理者に通知します。
1.6	無線アクセス管理	• Cisco ISE は有線ネットワークと無線ネットワークの両方に一貫した機能を提供します。
1.7	パスワードベース認証の強度	• Cisco ISE では、ユーザーがネットワークにログインするときに、最小長さやさまざまな文字タイプに基づいてパスワードの強度を設定できます。 • Cyber Vision はデフォルトのユーザーログイン情報とクリア（暗号化されていない）パスワードを検出します。
1.8	公開キーインフラストラクチャ（PKI）証明書	• Cisco ISE はデバイス間通信に対し、スタンドアロン PKI 展開および既存のエンタープライズ PKI と統合された認証局の展開の両方をサポートします。
1.9	公開キー認証の強度	• Cisco ISE は証明書を検証し、対応する秘密キーのユーザー制御を確立し、認証された ID をユーザーにマッピングする機能を提供します。
1.10	オーセンティケータのフィードバック	• シスコのネットワーク機器にログイン情報を提供する場合、パスワードは隠されます。
1.11	失敗したログインの試み	• Cisco ISE はすべてのネットワークログイン試行を、成功か失敗かにかかわらずログに記録します。 • Cisco Duo も、MFA を使用してアクセスを保護するときに、すべてのログイン情報をログに記録します。 • Cyber Vision は暗号化されていないプロトコルを使用している場合のログイン試行を識別し、ログに記録します。複数回の失敗を確認できます。
1.12	システム利用通知	• この要件は IACS 開発者に適用されます。
1.13	信頼されていないネットワーク経由のアクセス	• Cisco Secure Firewall は、Cisco AnyConnect クライアントと連携してリモートアクセス VPN 機能とポリシー適用機能を提供するため、信頼できないネットワークから境界を越えるトラフィックを制御できます。 • Cisco Secure Equipment Access は、Cisco Catalyst IR1101 高耐久性ルータなどのシスコの産業用ネットワーク機器に常駐する専用リモート アクセス アプリケーションで、個々の IACS デバイスへの安全なリモート接続を提供します。 • Cyber Vision は、信頼できないネットワークからのリモートアクセスを含むすべてのネットワーク通信をキャプチャします。

FR2：使用制御（UC）

根拠

この基本要件の目的は、不正なアクション（データの読み取り/書き込み、プログラムのダウンロード、構成の設定など）からコンポーネントを保護するために、識別および認証されたユーザー（人間、ソフトウェアプロセス、またはデバイス）に適切な特権を適用することです。また、ユーザーアクションの監視にも注意を払い、時刻、日付、場所、およびアクセス手段に基づいてユーザー権限を変更することを推奨しています。

シスコが役に立てること

Cisco Identity Services Engine（ISE）は、有線および無線の産業用ネットワークの両方でアクセス制御に使用される認証、許可、およびアカウンティング（AAA）サーバーです。認証はユーザーを識別する手段で、通常はユーザーが有効なユーザー名とパスワードを入力するとアクセスが許可されます。ただし、ネットワーク内のほとんどのデバイスは人間ではないため、ユーザー名やパスワードを提供することができません。

ISE には MAC 認証バイパス（MAB）を実行する機能が備わっており、デバイスの MAC アドレスに基づいて提供するネットワークアクセスレベルを決定できます。MAB の実行前はエンドポイントの ID が不明であるため、すべてのトラフィックがブロックされます。スイッチが単一のパケットを検査して送信元 MAC アドレスを学習および認証します。MAB が成功するとエンドポイント ID が認識され、エンドポイントからのトラフィックが許可されます。スイッチは送信元 MAC アドレスフィルタリングを実行し、MAB により認証されたエンドポイントのみがトラフィックを送信できるようにします。

認可は、ポリシーを適用し、ユーザーまたはデバイスにアクセスを許可するアクティビティ、リソース、サービスを決定するプロセスです。これらはすべて中央のロケーションからコントロールされ、Cisco ISE がネットワークおよびセキュリティ インフラストラクチャ全体に適用ポリシーを配信します。管理者は登録ユーザーからベンダーを区別するポリシーを一元的に定義し、最小限の特権に基づいてアクセスを許可できます。ISE は Downloadable Access Control Lists（dACL）、VLAN 割り当て、セキュリティグループタグ（SGT）、Cisco TrustSec など、さまざまなアクセス制御オプションを提供します。これらのテクノロジーについては、ネットワーク セグメンテーションに関連する FR5 でさらに詳しく説明されています。Cisco Secure Firewall は、読み取り/書き込みの適用などの機能について、ネットワーク境界をまたがるより詳細なポリシーを提供します。

アカウンティングは、アクセス時にユーザーが消費したリソースを測定します。対象には、システム時間や、セッション中にユーザーが送受信したデータ量などが含まれます。セッションの統計情報と使用状況情報を記録し、それらの情報を認可制御、リソース使用率分析、キャパシティプランニングなどのアクティビティに利用します。

Cisco Cyber Vision はネットワーク インフラストラクチャを通過するすべてのパケットを詳細に検査し、ネットワーク内のイベントを確認して OT 固有のデータを提供することで監査ログを保管します。

表 2. 使用制御のシステム要件

SR	説明	対応する製品機能
2.1	**認可の適用**	• Cisco ISE は有線ネットワークと無線ネットワークの両方でアクセスコントロールに使用される AAA サーバーです。 • Cisco Secure Firewall は、読み取り/書き込みの適用などの機能について、ネットワーク境界をまたがるより詳細なポリシーを提供します。
2.2	**無線利用制御**	• Cisco ISE はアクセステクノロジーに関係なく一貫した認可を適用します。 • Cyber Vision は無線ネットワークのアクティビティを（アクセスポイントレベルで）監視できます。
2.3	**ポータブルおよびモバイルデバイスの使用制御**	• Cisco ISE、Secure Firewall、および Duo はすべて、デバイスのタイプ、デバイスが管理対象かどうか、デバイスにリンクされたコンテキスト情報（例：ファームウェアバージョン）など、デバイスのポスチャに基づいてポリシーを適用できます。 • Cyber Vision は、新しく接続されたコンポーネント（ポータブルデバイスやモバイルデバイスなど）を検出し、警告を送信できます。
2.4	**モバイルコード**	• この要件は IACS 開発者に適用されます。
2.5	**セッションロック**	• ユーザーまたはデバイスにネットワークへの再認証を常に要求することは、可能ではありますが推奨されません。このシステム要件はアプリケーションアクセスのタイムアウトに適用され、シスコの対象範囲外です。 • ただし、重要なネットワーク用の安全なリモートアクセスツールである Cisco Secure Equipment Access は、指定されたエンドポイント（デバイスやアプリケーションなど）に、指定された時間のみアクセスを許可するように設定できます。
2.6	**リモートセッションの終了**	• Cisco Secure Firewall はネットワークへのリモートアクセス用 VPN コンセントレータで、アクティブなセッションを終了させてユーザーをネットワークから排除できます。

SR	説明	対応する製品機能
		• Cisco Secure Equipment Access は、リモートアクセスを指定された時間枠に制限する機能を提供し、いつでも強制終了できます。
2.7	同時セッション制御	• Cisco ISE はネットワーク上の特定のネットワークポートへの接続を単一の MAC アドレスにのみ制限するように設定できるため、不正なデバイスは正当なデバイスに代わってネットワークに接続できなくなります。 • Cyber Vision は、ネットワーク上のすべてのデバイスとの間の同時接続（フロー）を監視できます。
2.8	監査可能イベント	• Cisco ISE、Secure Firewall、Duo、および Cyber Vision はすべて、イベントのロギング、監査、およびエクスポート機能を提供します。
2.9	監査ストレージ容量	• このガイドに記載されているすべてのシスコ製品のログは製品内にアーカイブされ、標準形式を使用してエクスポートできます。保持ポリシーとストレージ容量は構成可能です。
2.10	監査処理の不備への対応	• この要件は IACS 開発者に適用されます。
2.11	タイムスタンプ	• すべてのシスコのログとアクティビティには、タイムスタンプが付けられています。
2.12	否認防止	• Cisco ISE を使用すると、セッションの統計情報と使用状況情報を記録するアカウンティングが実行され、それらの情報を認可制御、リソース使用率分析、キャパシティプランニングなどのアクティビティに利用できます。 • さらに Cisco Secure Firewall は ID を認識し、ファイアウォールを通過するアクティビティをログに記録するときにユーザー ID を含めることができます。

FR3：システムの完全性（SI）

根拠

この基本要件の目的は、コンポーネントのライフサイクル全体（テスト、運用、および非運用フェーズ中）にわたる不正な操作を防止することにより、IACS の各コンポーネントの完全性を確保することです。たとえばデータ転送の完全性も、測定値やコマンドパラメータの操作を防止するための重要な要件です。

シスコが役に立てること

特定の物理的および環境的影響に対処し、電磁波干渉（EMI）やその他の過酷な状況による影響を排除するためには、セキュリティ制御に加えて、強化された堅牢な機器が必要になります。これには、通信機器のケーブル配線、インターフェイス、および設計が含まれます。これに関連するよい例が、変電所に設置される機器向けの IEC-61850-3 標準規格です。変電所自動化ネットワークで使用されるシスコの高耐久性産業用スイッチはすべて、IEC-61850 パート 3 の認定を受けています。

また、データの高可用性を確保し、環境条件による影響を最小限に抑えるには、堅牢で信頼性が高く、場合によっては冗長化されたネットワークアーキテクチャが必要になります。

データ転送の完全性に関するインサイトを得られるように、シスコでは、エンドポイントソフトウェアと侵入検知システム（IDS）を使用して悪意のあるコードや不正なソフトウェアの影響を防止、検出、レポート作成、軽減することを推奨しています。Cisco Snort は、Cisco Secure Firewall と Cyber Vision の両方に統合されたオープンソースの IPS/IDS です。Cisco Secure Endpoint は、ワークステーション、Windows ベースのヒューマンマシン インターフェイス（HMI）、および産業用ネットワーク内で使用されるタブレット上のマルウェアを検出および防止できるエンドポイント保護ツールです。

表 3.　システムの完全性に関するシステム要件

SR	説明	対応する製品機能
3.1	通信の完全性	• Cyber Vision は、使用されているプロトコルを確認し、クリアテキストのフローと暗号化されたフローを区別できます。
3.2	悪意のあるコードからの保護	• Snort は、シスコが提供するオープンソースの IPS/IDS です。IP ネットワークでリアルタイムのトラフィック分析とパケットロギングが可能です。また、プロトコル分析とコンテンツの検索およびマッチングを実行できるほか、バッファオーバーフロー、ステルスポートスキャン、サーバーメッセージブロック（SMB）プローブ、OS フィンガープリントの試みなど、さまざまな攻撃とプローブの検出に使用できます。 • Snort IDS は Cyber Vision と統合されています。 • Snort IDS/IPS は Cisco Secure Firewall と統合されています。 • Cisco Secure Endpoint は、産業用ネットワーク内で使用されるデスクトップおよびモバイルエンドポイントでマルウェアを検出および防止できるエンドポイント保護ツールです。
3.3	セキュリティ機能の検証	• Cyber Vision はこの要件への対応だけでなく、ファイアウォール、ログシステム、バックアップソリューションといった他のセキュリティ機能の適切な動作を検証するのにも役立ちます。
3.4	ソフトウェアと情報の完全性	• Cyber Vision は、制御システムのアクティビティに関する運用上のインサイトを提供します。ネットワーク上で発生したすべての変更を検出してレポートします。 • 正しく設定されている場合、Cisco Secure Firewall と ISE は、ネットワークでの不正な変更の発生を阻止します。モニタリングにのみ使用する場合は、ファイアウォールと ISE のログはいずれも、ネットワークへの不正な変更にユーザーコンテキストを追加します。
3.5	入力の検証	• シスコはシスコツールの入力検証機能を提供していますが、この要件は主に IACS 開発者に適用されます。シスコは Snort ルールを活用して、定義されたフィールドタイプの範囲外の値を検出し、ネットワークを通過するデータの入力検証を実行できます。
3.6	確定的な出力	• この要件は IACS 開発者に適用されます。
3.7	エラー処理	• この要件は IACS 開発者に適用されます。
3.8	セッションの完全性	• この要件は IACS 開発者に適用されます。
3.9	監査情報の保護	• シスコは、シスコ独自のツールにおけるログの変更と削除を管理者アカウントに制限できますが、Security Information and Event Manager（SIEM）のすべてのログをバックアップすることをお勧めします。また、Cisco Secure Endpoint を使用すると、エンドポイントに監査ツールを常駐させて保護を強化できます。

FR4：データの機密性（DC）

根拠

この基本要件の目的は、データの送信中または保存中に、データを不正な開示から保護することです。この要件は、通信チャネルとストレージを保護する必要を示しているだけでなく、保護が必要なデータとそのデータにアクセスできるユーザーを定義することを組織に義務付けています。

シスコが役に立てること

MACsec は、2 台の MACsec 対応デバイス間のパケットの認証と暗号化に関する IEEE 802.1AE 規格です。たとえば、Cisco Catalyst IE3400 高耐久性 シリーズ スイッチは、スイッチと MACsec 対応ホストデバイス間の暗号化のために、スイッチからホストへのリンクで MACsec Key Agreement（MKA）による 802.1AE 暗号化をサポートします。このスイッチは、Cisco TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）、セキュリティ アソシエーション プロトコル（SAP）、および MKA ベースのキー交換プロトコルを使用したスイッチ間のセキュリティのために、MACsec 暗号化もサポートしています。

保管中のデータの保護はシスコの範囲外であるため、このデータを保護するにはさらに考慮が必要です。

表 4. データの機密性に関するシステム要件

SR	説明	対応する製品機能
4.1	情報の機密性	• Catalyst IE3400 などのシスコ産業用スイッチは、MACsec 対応ホストのために MACsec をサポートしています。 • Cyber Vision は、情報がクリアテキスト（またはバイナリ）として伝達されているか、暗号化された情報として伝達されているかをユーザーに通知します。 • Cisco Secure Firewall とシスコ産業用ルータはさらに、暗号化されたリンクを介したデータの送信をサポートします。
4.2	情報の永続性	• この要件は IACS 開発者に適用されます。
4.3	暗号化の使用	• Catalyst IE3400 などのシスコ産業用スイッチは、スイッチと対応ホストデバイス間の暗号化のために、スイッチからホストへのリンクで MKA を使用した 802.1AE 暗号化をサポートします。このスイッチは、Cisco TrustSec NDAC、SAP、および MKA ベースのキー交換プロトコルを使用したスイッチ間のセキュリティのために、MACsec 暗号化もサポートしています。

FR5：データフローの制限（RDF）

根拠

この基本要件の目的は、この規格で推奨されている最小特権の原則を実施するために、コンポーネント間のシームレスな通信を制限することです。通信を制限するには、IACS ネットワークをセグメント化し、組織のリスク評価および達成しようとするセキュリティレベルに基づいて定義されたゾーンとコンジットをサポートする必要があります。ネットワークのセグメンテーションは、制御システムがサイバー脅威にさらされる機会を減らし、攻撃の拡散を制限する効率的な方法として認められています。また、異なるネットワークセグメント間の接続を切断してインシデントに対応するためにも活用されます。

シスコが役に立てること

IDMZ（産業用緩衝ゾーン）は、重要な環境または製造現場システムとエンタープライズ ネットワークの間のバッファです。産業ゾーンとエンタープライズゾーンの間の共有サービスはすべて IDMZ に配置されます。シスコは、各セキュリティゾーンに出入りするトラフィックを検査できる Cisco Secure Firewall などの境界（「エッジ」）セキュリティアプライアンスに加え、セグメント化されたネットワークを維持しながら重要なネットワークとそれ以外のネットワーク間のギャップを埋めるために Cisco Telemetry Broker などのレプリケーションサービスも提供します。

プラント内部では、IEC 62443 で提示されるゾーン/コンジットモデルをサポートするために、Cisco ISE は TrustSec テクノロジーを使用して制御システムネットワークを論理的にセグメント化します。シスコのスイッチ、ルーティング、ワイヤレス LAN、およびファイアウォール製品には、Cisco TrustSec の分類およびポリシー適用機能が組み込まれています。ネットワーク アクセスポイントでは、通常はエンドポイントのユーザー、デバイス、およびロケーション属性に基づいて、セキュリティグループタグ（SGT）と呼ばれる Cisco TrustSec ポリシーグループがエンドポイントに割り当てられます。SGT はエンドポイントのアクセス権を示し、エンドポイントからのすべてのトラフィックが SGT 情報を伝達します。SGT は、スイッチ、ルータ、およびファイアウォールが転送の決定を行うために使用されます。SGT の割り当てによってビジネスの役割や機能を示すことができるため、基盤となるネットワークの詳細ではなく、ビジネスニーズに基づいて Cisco TrustSec の制御を定義できます。

Cisco Cyber Vision は、これらのビジネスの役割の定義に役立ちます。Cyber Vision は、パッシブ検出とアクティブ検出の独自の組み合わせを活用して、デバイスやプロセスに影響を与えることなくすべての資産を特定します。検出は産業用ネットワークによって実行されるため、検出用通信はファイアウォールやネットワークアドレス変換（NAT）境界によってブロックされません。その結果、100% の可視性が実現します。Cyber Vision により資産とその通信がマップに表示されるため、運用チームは自社の産業プロセスに容易に関連付けることができます。したがってチームは、資産をゾーン（生産セルなど）にグループ化し、ネットワーク セグメンテーション ロジックを定義できます。この情報が Cyber Vision により ISE と自動的に共有され、それに応じてセキュリティポリシーが構築されます。

コンプライアンス要件を満たすために、Cyber Vision は変数アクセスを含むすべてのイベントとアプリケーションフローの履歴を保持します。これによりフォレンジック調査を簡単に実行してレポートを作成できます。

表 5. データフロー制限のシステム要件

SR	説明	対応する製品機能
5.1	ネットワーク セグメンテーション	• Cisco Secure Firewall によりエンタープライズゾーンや産業ゾーンなどのネットワーク境界を表すセグメントを作成できます。IDMZ を通過するときの原則適用の主要なメカニズムです。 • プラント内部では、IEC 62443 で提示されるゾーン/コンジットモデルをサポートするために、Cisco ISE は TrustSec テクノロジーを使用して制御システムネットワークを論理的にセグメント化します。
5.2	ゾーン境界の保護	• Cyber Vision は、資産を論理ゾーンにグループ化し、コンジットを通過するデータを視覚化する機能を提供します。 • Cyber Vision で作成される論理的な区切りは ISE と共有され、リスクベースのゾーン/コンジットモデルに従って論理ゾーンの境界を越えて適用されるポリシーに影響を与えます。
5.3	一般的な目的の個人間通信の制限	• Cisco Secure Firewall は、産業ゾーンから電子メールサーバーへの接続やソーシャルメディアへの接続など、一般的な目的の個人間メッセージの使用を検出して防止します。
5.4	アプリケーションのパーティション	• この要件は IACS 開発者に適用されます。

FR6：イベントへのタイムリーな対応（TRE）

根拠

この基本要件の目的は、IACS コンポーネントを適切に監視することで、コンポーネントの安全性を確実に確保することです。これらの要件は、組織がフォレンジック調査に必要な証拠を収集し、セキュリティ違反に対応するために使用するツールと手順を実装できるように設計されています。5 つのセキュリティレベルによって、イベントがシステムのセキュリティに影響を与えた際に、適切な関係当局にいかに迅速に通知されるかについての異なる期待値が設定されています。

シスコが役に立てること

Cisco Cyber Vision はすべてのイベントとアプリケーションフローの履歴を保持します。これにより、現在のセキュリティステータスをすばやく把握し、異常と脆弱性を特定し、脅威に対応することができます。Cyber Vision はさまざまなダッシュボード、レポート、およびイベント履歴を提供するため、セキュリティの問題を簡単に特定できます。さらに、Cisco Talos 脅威インテリジェンスを活用した Snort IDS エンジンが統合され、マルウェアや悪意のあるトラフィックなどの既知の脅威と新たな脅威を検出します。

Cyber Vision は IBM QRadar や Splunk などの主要な SIEM および SOAR（Security, Orchestration, Automation, and Response）プラットフォームと事前に統合されており、syslog を使用して OT イベントとアラートを他のツールに転送できます。イベント疲れを回避するために、通知されるイベントタイプを選択することもできます。

Cisco SecureX は、シスコのセキュリティ製品とサードパーティのソースの両方からのインテリジェンスを集約し、ファイルハッシュ、IP アドレス、ドメイン、電子メールアドレスなどの監視対象が不審なものかどうかを識別します。調査を開始すると、シスコ統合セキュリティ製品からコンテキストが自動的に追加されているため、どのシステムが標的となり、どのような攻撃を受けたかを即座に把握できます。これにより、ナレッジがインテリジェンスソースとセキュリティ製品から返され、数秒で結果が表示されます。また、セキュリティ運用チームはカスタムワークフローをトリガーしてすぐに行動を起こしたり、提供されたツールを使用して調査を継続したりできます。

表 6. イベントへのタイムリーな対応のためのシステム要件

SR	説明	対応する製品機能
6.1	監査ログへのアクセス性	• Cyber Vision は役割ベースのアクセスに基づいて監査ログへの読み取り専用アクセスを提供します。 • Cisco Secure Firewall、Cyber Vision、および Duo を使用すると、管理者はログをエクスポートして、ツールへのアクセスを必要としないユーザーと共有できます。
6.2	継続的な監視	• Cisco Cyber Vision は、OT ネットワークアクティビティを継続的に監視して、新しい資産と変更された資産、通信パターン、および異常なイベントを識別するとともに、サポートされているハードウェアで IDS 監視を実行します。 • Cisco Secure Firewall を境界の選択した場所に展開することで、セキュリティ監視を追加できます。 • Cisco Secure Endpoint をエンドポイントに展開することで、それらのエンドポイントを継続的に監視し、疑わしいアクティビティに対応できます。

FR7：リソースの可用性（RA）

根拠

この基本要件の目的は、サービス拒否（DoS）攻撃の発生時のように機能が低下した環境で実行されているときでも、IACS コンポーネントが重要な機能の提供を継続し、安全な運用を確保できるようにすることです。つまり、ネットワークトラフィックの優先順位付け、ベースラインからの逸脱の検出、バックアップからのシステムの回復を実行できるようにします。これらすべてを実現可能にするには、すべての IACS コンポーネントの詳細なインベントリを維持する必要があります。

シスコが役に立てること

シスコの産業用セキュリティアーキテクチャの全体的な目的は、IACS リソースの完全性と可用性を確保することです。この目的は、以下の表に示すさまざまな手法によって実現されます。

さらに、シスコのネットワーク インフラストラクチャには、DoS 攻撃から保護するために Quality of Service（QoS）を設定する機能が備わっています。ユーザーは、特定のネットワークトラフィックを選択し、相対的な重要性に従って優先順位を付けることができます。ネットワークに QoS を実装すると、ネットワークパフォーマンスが予測しやすくなり、帯域幅の利用効率が向上します。ネットワークセグメントが侵害された場合でも、QoS によって、同じ物理インフラストラクチャ上の他のネットワークセグメントのリソース使用率に影響が及ぶのを回避できます。

表 7. リソースの可用性のシステム要件

SR	説明	対応する製品機能
7.1	DoS からの保護	• シスコは DoS からの保護機能を提供していますが、DoS 攻撃中の機能低下モードで実行するというこの要件は、IACS 開発者に適用されます。
7.2	リソース管理	• シスコは、重要なシステムがネットワーク内で常に優先され、ネットワーク インフラストラクチャを標的とする DoS 攻撃の影響を受けることがないように、ネットワーク インフラストラクチャで QoS ポリシーを使用することを推奨しています。
7.3	制御システムのバックアップ	• シスコは、Cisco DNA Center などの集中管理ツールの使用時に、ネットワーク構成をバックアップする機能を提供します。
7.4	制御システムの復旧と再構築	• Cyber Vision を使用すると、侵害されたシステムを検出し、IACS ネットワークの再構築に必要な時間を短縮できます。 • Cyber Vision は、回復後にシステムが既知の安全な状態に到達できたことを証明するのに役立ちます。
7.5	非常用電源	• シスコ産業用イーサネット（IE）スイッチは、非常用電源との間で切り替える機能を備えており、一次電源の障害時にネットワークの運用を確実に継続するのに役立ちます。
7.6	ネットワークとセキュリティの構成設定	• Cisco DNA Center がネットワーク構成を制御システム上でライブで確認し、推奨されるネットワークおよびセキュリティ構成と比較できます。
7.7	最小限の機能	• Cisco Secure Firewall を使用すると、ネットワークの境界を越えて不要な機能、ポート、プロトコル、サービスなどが使用されるのを禁止できます。 • Cisco ISE を使用すると、ACL や SGT を使用してネットワーク インフラストラクチャを通過する際に、同じサービスが横方向に移動するのを禁止できます。 • Cyber Vision は、禁止されているネットワーク通信や予期しないネットワーク通信（フロー、ポート、シャドウ通信、ネットワーク汚染など）の検出に役立ちます。
7.8	制御システムコンポーネントのインベントリ	• Cyber Vision は、インストールされているコンポーネントがネットワーク上で通信するたびに、そのコンポーネントとプロパティを受動的に検出します。 • Cyber Vision は、動作中のプロトコルのセマンティックスを使用してネットワーク上のコンポーネントにアクティブにクエリを実行し、コンポーネントの特性と構成に関する追加の詳細を収集する機能を備えています。

ISA/IEC-62443-3 準拠に向けた取り組みの開始

シスコは産業分野のユースケースに特化した、市場をリードするネットワーキング ポートフォリオを開発することによって、15 年以上にわたり世界中の産業組織の業務のデジタル化に貢献しています。OT 要件を深く理解すると同時に、包括的なサイバーセキュリティ ポートフォリオを提供しているシスコは、業界でも珍しい存在です。

シスコは、堅牢で柔軟なネットワークアーキテクチャこそが、堅牢なセキュリティの重要な成功基準であると考えています。ネットワーク設計が不十分だと大量の脆弱性を生み出し、セグメンテーションと拡張性の概念を妨げるだけでなく、サイバーセキュリティ制御と物理的セキュリティ対策の統合に支障をきたす可能性があります。

一方で、当社の経験から言えば、安全な産業用ネットワークの構築は一夜にして実現できるものではありません。確実な成功を支援するために、シスコは段階的なアプローチを推進しています。段階ごとに次の段階に向けた基盤を構築することで、お客様のペースに合わせてセキュリティ体制を強化し、この取り組みを開始するにあたりすべての利害関係者に価値を示すことができます。

シスコは、ISA/IEC-62443-3 のゾーン/コンジットの概念に基づいて、組織が規格に準拠しながら産業用制御システムを保護するために従うべきさまざまな手順を説明するリファレンスアーキテクチャを開発しました。シスコ産業用

セキュリティ検証済みデザイン（CVD）は、ISA/IEC-62443-3 で定義されている運用のニーズを満たしており、IT チームとセキュリティチームにはより馴染みのある NIST サイバーセキュリティ フレームワークも活用します。

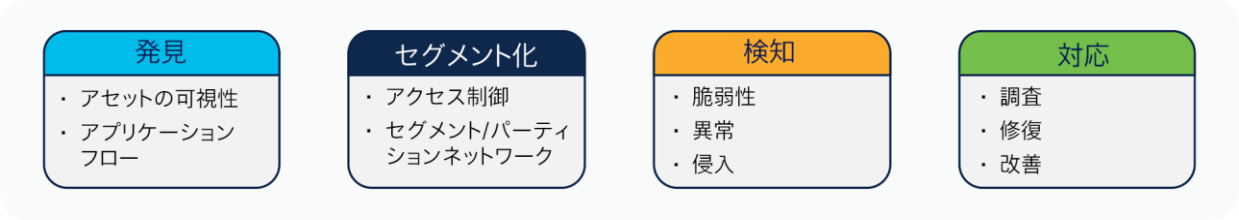

図 3.
NIST サイバーセキュリティ フレームワークの柱

発見

Cisco Cyber Vision はすべての産業用資産とそのアプリケーションフローの可視性を提供します。接続されているすべてのデバイスに関する詳細情報を含む動的なインベントリを作成し、通信アクティビティを追跡してゾーンとコンジットを監視します。またサイバー脅威にさらされている IACS を特定することでリスク評価にも役立ちます。Cyber Vision センサーは、セル/エリアネットワーク機器に組み込まれており、広域にわたる可視性を提供します。

セグメント化

産業用ネットワークは、Cisco Secure Firewall が配置する IDMZ（産業用緩衝ゾーン）によってエンタープライズネットワークからセグメント化されます。Cisco Secure Firewall は産業用ネットワークのさまざまな部分のセグメント化にも使用できます。各セグメントによって半自律的なゾーンが形成され、セキュリティインシデントをゾーン内に制限して封じ込めることができます。

より詳細なセグメンテーションと動的アクセス制御のために、Cisco Identity Services Engine（ISE）は、セキュリティポリシーをデバイスレベルで自動的に適用します。Cisco ISE は制御エンジニアによって Cyber Vision で構成されたゾーンを活用して、通信フローを適切に制限するようにネットワークに指示します。

Cisco ISE は、Cisco Secure Client（AnyConnect を含む）を使用して産業用ネットワークに VPN アクセスを行うリモートユーザーのアクティビティを制限することもできます。Cisco Secure Equipment Access は、もう 1 つのリモートアクセス ソリューションで、個々のデバイスに限定してアクセスを許可します。どちらのソリューションも、Cisco Duo を使用して MFA を活用できます。

検知

Cisco Cyber Vision は各 OT デバイスにパッチを適用する必要があるハードウェアとソフトウェアの脆弱性を管理者に警告します。また、Snort IDS エンジンを統合して侵入や悪意のあるトラフィックを検出します。OT ネットワークアクティビティに対するこの包括的な可視性により、通常の動作からの逸脱を検出するためのベースラインを構築できます。

Cisco Secure Network Analytics（旧称 Cisco Stealthwatch）も、ネットワークデバイスからテレメトリを収集し、ネットワークフローを監視することによって異常の検出に役立ちます。

Cisco Secure Firewall は Cisco Secure IPS、Secure Firewall Malware Defense、高度な分散型 DoS（DDoS）の軽減機能、および URL フィルタリング機能を統合して、包括的な侵入検出と保護を提供します。また、Talos シグネチャファイルを活用して脆弱性のエクスプロイトをブロックすることもできます。

Cisco Secure Endpoint は、さまざまなエンドポイント（ワークステーション、サーバー、ラップトップ、タブレットなど）にマルウェアからの高度な保護機能を提供する製品で、ネットワーク上で通信している保護対象エンドポイント上のプロセスを識別できます。

対応

Cisco SecureX は、複数のセキュリティテクノロジー（シスコおよびその他のベンダー）からの脅威インテリジェンスとデータを 1 つの統合ビューに集約することで調査を促進します。また、包括的なケース管理機能や特定の環境向けのカスタムプレイブックを提供して、修復の効率を高めます。

Cyber Vision やその他のセキュリティツールではログイベントを SIEM プラットフォームにエクスポートでき、より詳しい調査や関連付けで使用できます。

シスコ検証済みデザイン（CVD）

シスコ OT セキュリティ リファレンス デザインは、安全かつ堅牢で信頼性の高い産業用ネットワークのブループリントです。シスコの包括的なネットワーキングとセキュリティのテクノロジーを活用して、産業用資産の可視化、マクロ/ゾーンセグメンテーション、ゾーンアクセス制御、脅威検出および対応機能を提供します。このデザインでは、情報セキュリティとの調整を通じて、一貫性あるアクセスポリシー管理と、セキュリティ オペレーション センター（SOC）への産業セキュリティイベントの集約を実現できます。

図 4 に示すように、このデザインは Purdue/ISA95 モデルに従い、ISA/IEC-62443-3 に準拠するための詳細な設計および実装のガイドラインを提供します。

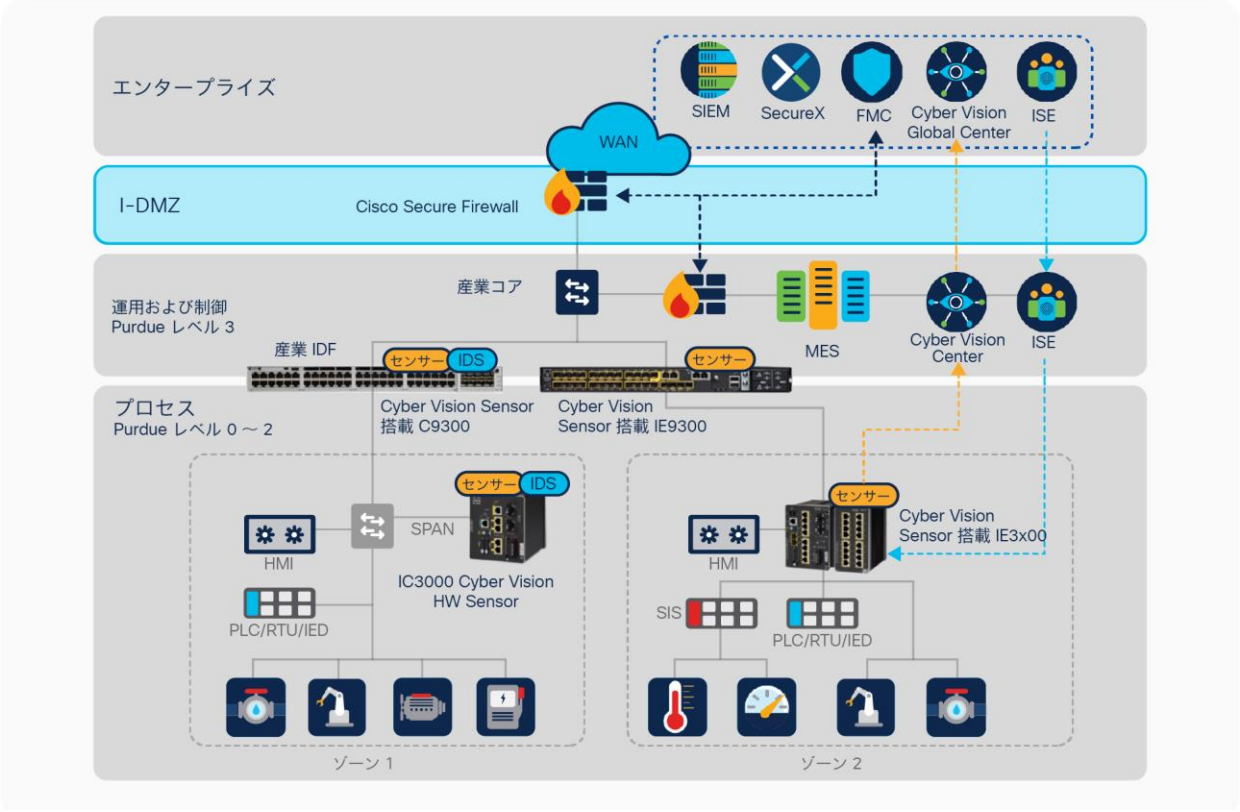

図 4.
シスコの産業用セキュリティアーキテクチャ（出典：シスコ OT セキュリティ検証済みデザイン）

まとめ

産業用オートメーションおよび制御システムの保護は、他のあらゆるセキュリティ対策と同様に、1 つの製品ではなく継続的なプロセスによって実現できるものです。このことはハードウェアとソフトウェアを含むコンポーネントの開発、運用、保守、および関連するその他のあらゆる活動に当てはまります。シスコはこの重要なパラダイムへの取り組みを、Cisco SDL に基づく製品開発に加え、シスコ検証済みデザインなどアーキテクチャおよび展開のリファレンスの改善も通じて行っています。

リンクと参考資料

- ISA99 標準委員会
- IEC62443-3-3 標準規格ダウンロード
- 産業用セキュリティ向けシスコ検証済みデザイン
- 産業用ネットワークを保護するための Cisco Industrial Threat Defense ソリューション
- シスコセキュア開発ライフサイクル（SDL）
- 産業用セキュリティのニーズについてご相談がある場合は、シスコにご連絡ください

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先
お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

0724-2022-000-X