エンドポイントセキュリティのベストプラクティス

IIC:WHT:IN17:V1.0:PB:20180312

Steve Hanna, Srinivas Kumar, Dean Weber

本書では、インダストリアルインターネットセキュリティを広範なスコープでとらえ、産業アプリケーションにおけるエンドポイントセキュリティの[1]ベストプラクティスを提言します。適正な安全性、信頼性、強靭性、およびプライバシーを確保しながら、エンドポイントに求められるセキュリティレベルを達成するために必要な対応策を簡潔に説明しており、本書の対象読者は、既存のベストプラクティスをより容易に適用できるようになります。本書は、既存のさまざまな産業界向けガイダンスおよびコンプライアンスフレームワーク(IISF [IIC-IISF2016]、Industrie 4.0 [Ind4.0-ITSec]、IEC 62443 [IEC-62443-11]、および NIST SP 800-53 [NIST-800-53r4] [NIST-800-53r5])に関する詳細な分析に基づいています。今後の IIC ベストプラクティスに関する文書では、「インダストリアルインターネットセキュリティフレームワーク(IISF)」の 6 つのビルディングブロックに基づいて、インダストリアルインターネットセキュリティの別の側面についても述べていく予定です。なお、ここでは、危機の安全性やデータ プライバシーの側面は扱いません。

本書は、産業用機器メーカ、インテグレータ、産業用機器の所有者およびオペレータを対象にしています。それぞれのセキュリティレベルで一般的に推奨される対応策と制御についての明確な説明は、いずれの読者にとっても有益です。産業用機器メーカおよびインテグレータは、対象の製品、システム、およびソリューションをどのセキュリティレベルに対応しているのかを定義することができます。保険会社や政策立案者は、リスク分析、およびセキュリティ対策の実施と改善に有用な、共通のベンチマークを得ることができます。本書は、認証やチェックリストの基準となることは意図していませんが、認証組織が認証プログラムを開発した場合、本書に基づいた評価を行うことも可能でしょう。

本書の用途を図 1 に示します。

[1] IIC 用語集では、エンドポイントを「演算能力およびネットワーク接続を有するコンポーネント」と定義しています。したがって、エンドポイントには、エッジデバイス（例えば、組込みあるいは埋込医療機器、自動車制御システムのセンサやアクチュエータ、製造システムのポンプ、ヒータ、フローメータなど）、通信インフラ、クラウドサーバ、あるいはこれらの間に介在する機器が含まれます。

図 1　エンドポイントセキュリティベストプラクティスの用途

法令によってなんらかの組織をインダストリアルセキュリティの要求事項に従わせることもできますが、法令に拘束されない組織も注意が必要です。不十分なインダストリアルセキュリティは、安全性の問題、機器の損傷など直接的な負の効果だけでなく、顧客不満足度の増大、品質や信頼性の低下、負債の可能性、そして結果として利益が低減するなど間接的な負の効果をもたらします。これとは逆に、十分なセキュリティ対策は、コスト削減、安全性と信頼性の向上などの好循環をもたらします。

本書に示されているベストプラクティスは、製造や輸送など特定業界の具体的なニーズに特化したものではありません。本書の読者は、これらの事例を業界独自の要求事項や規制事項を反映するように適応させる必要があります。今後の改訂版には、各業界に対応したセクションが設けられるでしょう。本書は、前述の通り特定業界を対象としたものではありませんが、フィールドテストに基づく分野横断的に適用可能な助言を、慎重に実施したリスク分析と併せて、提供します。

セキュリティ向上のために、すでに展開されている既存のエンドポイントを修正（一部変更）することは難しく、本書では、基本的に新しいエンドポイントを対象としています。しかし、本書に示されているいくつかのコアコンセプト（例えば、耐タンパ対応変更制御）は、レガシーエンドポイントにとっても有効でしょう。エンドポイントにはセキュアな更新能力が必要ですが、年数が経過するとレガシーとなります。適正なセキュリティに対応できなくなったレガシーエンドポイントには、ネットワークセキュリティなど他のセキュリティ対策を導入しなければなりません。

他の IIC 文書との関係

「インダストリアルインターネットセキュリティフレームワーク（IISF）」は、システム設計者がセキュリティアーキテクチャおよびコンテキストの総合的な理解を深めることができるように、産業インターネットセキュリティのためのセキュア設計アーキテクチャを提供します。また、本書に加

え、データ保護、コミュニケーション、接続性など、他の IISF 関連文書に応じたセキュリティベストプラクティスについても公開予定です。

システム設計者は、本書に示されているエンドポイントセキュリティベストプラクティスを利用して、インダストリアル IoT（IIoT）エンドポイントシステムの構築やアップグレードの際に特定のセキュリティレベル（ベーシック、強化、重大）を達成するためには、どのような制御手法を適用すればよいか理解することができます。必要なセキュリティレベルはリスクのモデル化や脅威分析によって決定されます。

「セキュリティ成熟度モデル」は、組織がセキュリティ成熟度を分析するための別のアプローチです。セキュリティ成熟度が高い組織は、確立されたプロセスを使用してリスク分析と評価を行い、対応方法を決定します。そして、その組織、産業分野およびシステムに求められる適正なレベルのセキュリティメカニズムを適用します。このプロセスを通じて、脅威あるいは重大なリスクに晒されているシステムを特定し、より高度なセキュリティレベルで対応することができるようになるでしょう。本書に示されているベストプラクティスをガイドラインとして採用することにより、適切な対処方法を選択することが可能になります。

IIC 用語集 [IIC-IIV2017] では、本書および IIC が発行する他の文書で使用されている用語と定義を示します。頭字語ついては、すべて本書の最後にまとめてあり、該当個所の文字列には点線を引いてわかりやすくし、また、ハイパーリンクを設定してあります。[1]

セキュリティレベル

本書では 3 段階のセキュリティレベル:「ベーシック」、「強化」、および「重大」を定義しています。これらのセキュリティレベルは、産業分野で（今世紀初期に示された ISA99 のオリジナル文書にまで遡り）最も成熟したガイダンスおよびコンプライアンスフレームワークとして選択される IEC 62443 3-3 [IEC-62443-33]で定義されるセキュリティレベル 2、3 および 4 に相当します。IEC 62443-3-3 に示されているセキュリティレベル 0 およびセキュリティレベル 1 に関するベストプラクティスは、低レベルのセキュリティ環境に対応するものであり、インダストリアルインターネット環境には妥当ではないため、本書では説明していません。NIST SP 800-53r4 においても 3 段階のセキュリティレベルについて類似の定義がなされています。

[1]本書では、次のような一般に広く知られている標準化団体については、頭文字で表記しています。
International Organization for Standardization (ISO) 国際標準化機構、Institute of Electrical and Electronic Engineers (IEEE) 米国電気電子学会、International Electrotechnical Commission (IEC) 国際電気標準会議、
Internet Engineering Task Force (IETF) インターネット技術タスクフォース、および National Institute for Standards and Technology (NIST) 米国国立標準技術研究所。

セキュリティレベル「ベーシック」(SLB)では、通常のウィルスなど、「低レベルのリソースを使用した単純な方法による故意の侵害」に対する防衛対策を提供します。セキュリティレベル「強化」(SLE)では、産業用制御システム(ICS)ソフトウェアあるいはシステムの弱点（発見された脆弱性）を狙った「中レベルのリソースを使用した高度な方法による攻撃」に対応します。セキュリティレベル「重大」(SLC)では、防衛能力をさらに高め、カスタムゼロデイ攻撃を開発する能力を有するような「広範なリソースを使用した高度な方法による攻撃」に対応します。それぞれのエンドポイントにおいて、適正なセキュリティレベルの対策を講ずることが必要です。

オペレータは、慎重に実施したセキュリティリスクアセスメントに基づいて、どのセキュリティレベルで対応することが必要であるかを判断しなければなりません。本書の提言で使用する専門用語は、さまざまなコンプライアンスフレームワークの制御目標と同様ですので、後述するセキュリティ対策の提言は、コンプライアンスや規制に関する検討事項とほぼそのまま整合性がとれています。

脆弱性、脅威、およびリスクに関する説明は、いずれも共通の基盤に基づくものですが、コンプライアンスや規制の種類によって大きく異なります。脆弱性モデルおよび脅威モデルに関する議論は、NIST 800-82 *[NIST-800-82]*および IEC 62443 3-3 などの文書に示されています。

セキュリティは独立したものではなく、環境破壊やヒューマンエラー、システム障害、システムへの攻撃などに直面した場合の安全性、プライバシー、信頼性、あるいは、強靭性など、他のシステムの特性と相互に関連し、組み合わされています。トラストワージネスとは、これらの 5 つの観点（特性）において、システムが期待通りに運用されることをどの程度確信しているかということを示します。ある特性を達成すために選択された手段は、他の特性に影響しますので、総合的なトラストワージネスのゴールを達成するためには、ソリューションを、他の特性と協調させながら、反復的に検討し、策定する必要があります。

セキュリティアーキテクチャ

セキュリティレベルを向上させるためのエンドポイントセキュリティには、いくつかのフルスタックアーキテクチャがあります。そうしたアーキテクチャは、オープンスタンダードに準拠し、複数ベンダーの複数プラットフォームにおける（3 階層モデル、ゲートウエイを介して接続されるエッジ、多層データバスなど）さまざまなアーキテクチャパターンのエンドポイントの相互運用性を提供しています。採用するアーキテクチャパターンに関わらず、エンドポイントには、当該エンドポイントが晒されるリスクレベルに応じて、攻撃への耐性を備えることが必要です。

図 2、3 および 4 は、本書で定義している 3 段階のセキュリティレベル：「ベーシック」、「強化」、および「重大」に対して選択された対応策を示しています。それぞれのセキュリティレベルに対して選択された対応策に関する論理的根拠は、IEC 62443 および NIST SP 800-53 など既存の文書に示されています。

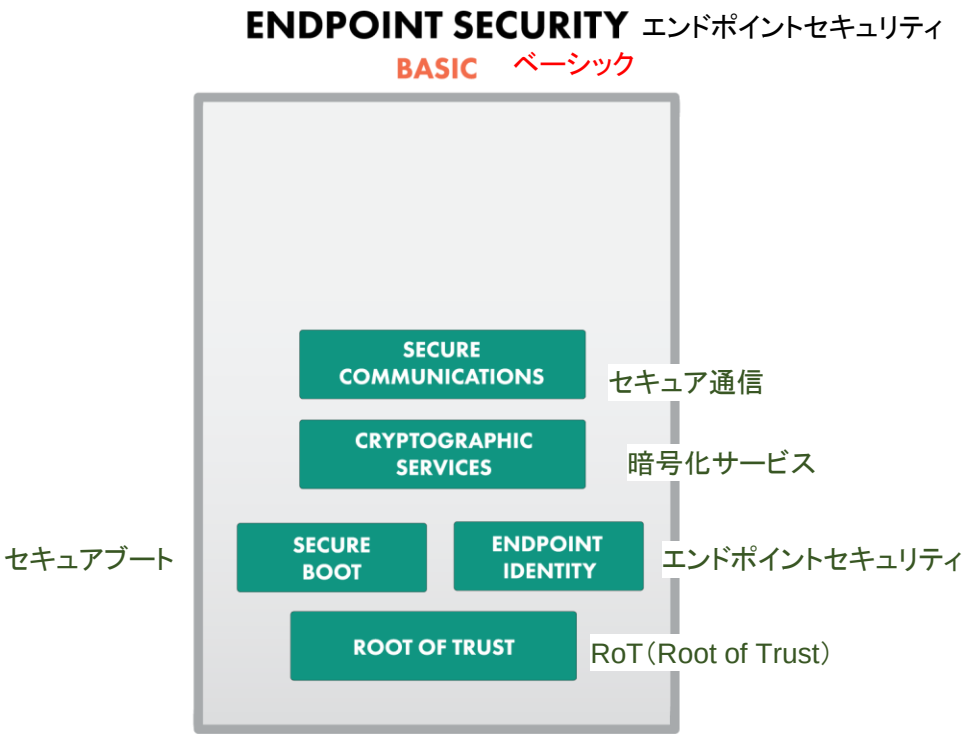

図 2 セキュリティレベル「ベーシック」

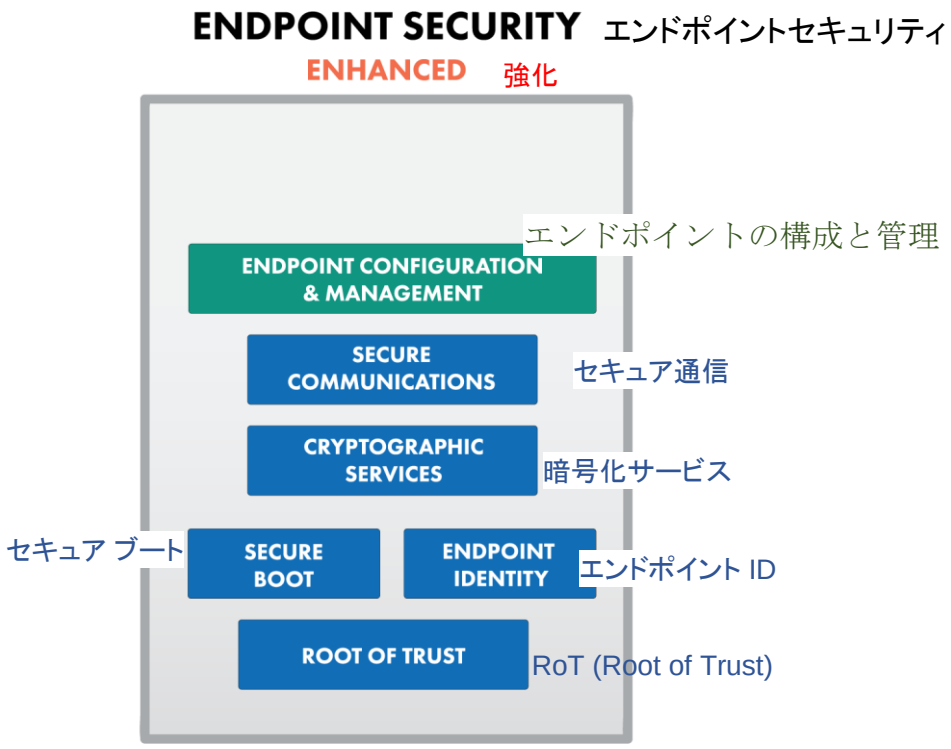

図 3 セキュリティレベル「強化」

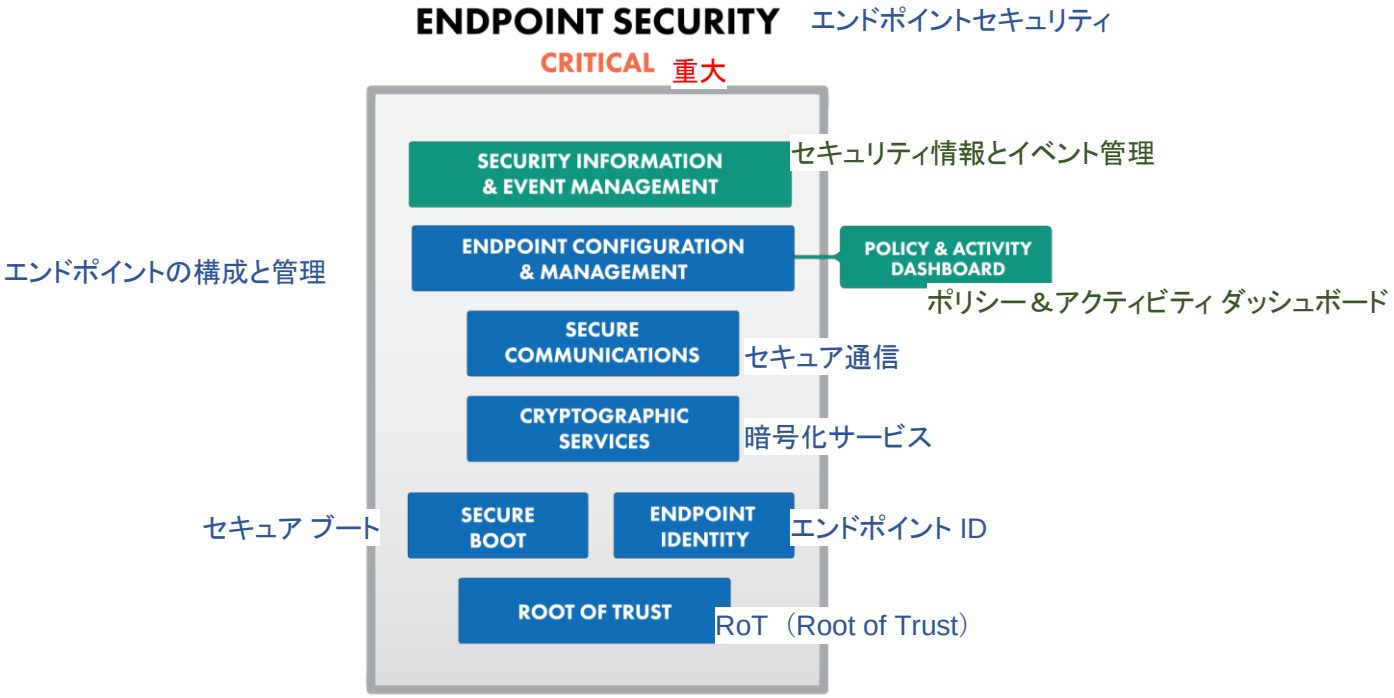

図 4 セキュリティレベル「重大」

次のセクションでは、アーキテクチャの各要素について詳述します。セキュリティ要求事項は、グレーでハイライトし、必要なセキュリティレベルをカッコ内に示しています。

ROOT OF TRUST　ROT （ROOT OF TRUST）

各エンドポイントには、エンドポイントセキュリティの基礎となる RoT（Root of Trust）が含まれ、次のような機能を提供します:

- エンドポイントアイデンティティ（「ベーシック」、「強化」、「重大」）[1]
- ソフトウェアおよびハードウェア ID 及び完全性の証明（「ベーシック」、「強化」、「重大」）[2]

RoT の強度は、当該機器の信頼性レベルを決定します。そして、その強度は、RoT をどのように実装したか（ソフトウェア、ハードウェアなど）に依存します。RoT は、シンプルでなければならず、また、完全性を確保するために危殆化から守られなくてはなりません。セキュリティレベル「強化」あるいは「重大」の場合、RoT はハードウェアで実行する必要があります（「強化」、「重大」）。[3] 物理的ハードウェアタンパリングに対する防衛策としては、一般的に、分散ハードウェアセキュリティチップ、あるいは耐タンパー性を備えた統合ハードウェアセキュリティブロックが必要になります。上述の「ソフトウェアおよびハードウェアの ID および完全性」とは、機器が、当該機器のハードウェアおよびソフトウェアのバージョン情報を、暗号化された形式で提供することを意味します。

エンドポイントアイデンティティ

エンドポイントアイデンティティは、ほとんどのセキュリティ対策において重要な役割を果たす、基本的なビルディングブロックです。公開鍵インフラストラクチャ(PKI)に対応することは、（必要に応じて、その他のオプションを使用することもできますが）セキュリティレベル「ベーシック」「強化」および「重大」において必須です。オープンスタンダード証明書管理プロトコル（例えば EST など）を使用して、内部あるいは外部認証機関によって発行された証明書の発行、更新、アップデート、あるいは失効処理を自動的に行います（「ベーシック」、「強化」、「重大」）。[4] エ

[1] NIST description https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust
NIST SP 800-147, IEC 62443-3-3 section 5.7.3.1
[2] NIST SP 800-155
[3] [IEC-62443-33]: 5.7.3, 5.7.4
[4] [IEC-62443-31]: 3.1.4, 3.1.5, 3.1.6, 3.1.25, 3.1.26, 3.1.34, 5.4, 5.7, 5.10
[IEC-62443-33] 5.10.4, 5.11.4, 7.6
NIST 800-53r5: AC-6, AC-20, IA-3, SC-2, SC-7, SC-14, SC-29, SC-30, SC-44, CM-3, CM-5, IA-5, IA-8, IA-9, MA-4, SC-12, SC-17, SC-23, SC-24, SI-7
NIST 800-125 supplemental virtualization guidance

ンドポイントの保証証明書からの一連の証明書チェインは、所有権をエンドポイント管理システムに移転するためのサプライチェーンの来歴を提供します。

セキュアブート

ファームウェアのセキュアブート構成証明（電源投入時に実行される改変不可のあるいは暗号化により保護されたブートストラップコード）および UEFI あるいは U-Boot ブートローダによるマルチステージブートには、公開鍵暗号化標準に基づく暗号技術的ハッシュ関数を使用することができます（「ベーシック」、「強化」、「重大」）。[1] これにより、ブートストラップから OS 起動まで、プラットフォームレベルの構成証明は拡張され、OTA またはネットワーク経由での、不正なファームウェア、ブートローダ、あるいはブートイメージの更新から保護されます。

暗号化サービス

包括的なエンドポイントセキュリティでは、転送プロトコル（移動中のデータ）、保存（保存データ）、およびアプリケーション（使用中のデータ）にわたって暗号化を適切に使用し、実行することが求められます（「ベーシック」、「強化」、「重大」）。[2] 以下事項に基づいて、機密性および完全性が保護されなければなりません:

- 公開鍵暗号化標準に基づく、適切な強度の非対称および対称暗号スイート、ハッシュ関数、および乱数生成器の採用[3]
- 米国標準技術研究所(NIST)／FIPS 標準規格に基づく、有効な暗号化アルゴリズムの実行
- 特に量子コンピューティングおよびポスト量子暗号進展下における、現場でのアップグレード機能を含む暗号化アルゴリズムの柔軟性
- 許容される暗号化アルゴリズムと暗号スイートに基づき、暗号化機能を用いたアプリケーション利用を動的に配信されるポリシーに基づいて制御すること、、および
- エコシステム内のセキュアな通信を可能にするために必要な、マルチベンダシステム間での暗号鍵方式および証明書の相互運用性

特定の環境においては、箇条書きで示した上述の提言の幾つかを採用しない理由（背景状況）も存在しえますが、異なる方向で対処する前に、全ての実装を十分に理解し、慎重に重要性を検討するする必要があります。

[1] NIST 800-147
NIST 800-53r5 SI-7
[2] [IEC-62443-33] 8.5
NIST Post-Quantum Initiatives NISTIR 8105
NIST 800-53r5 IA-3, SC-7, and throughout AC-x
[3] [NIST-800-57p1r4]

エンドポイントの構成と管理

ファームウェア、OS、構成、あるいはアプリケーションのリモートまたは自動更新は、何百万ものエンドポイントに対して、ブラックリストやホワイトリストに頼ることなく、スケーラブルに OT(運用・制御技術)の世界で検証できなければなりません。このためには、機密性と完全性を保持した更新ワークフローにおいてセキュアなエンドツーエンドのコンテンツ配信を実行するための、公開鍵暗号化標準に基づくデータの暗号化と、電子証明書による署名者（サプライチェーン来歴）と受信者（認証されたエンドポイント）の検証とが必要です。ファームウェアとソフトウェアの完全性をスケーラブルに検証するためには、エンドポイントからクラウドまでプラットフォーム全体にわたって整合性のあるリモート構成証明（TNC、TPM など）を実行することが必要です（「強化」、「重大」）。[1]

セキュア通信

セキュアなエンドツーエンド通信プロトコルスタックが求められる(「ベーシック」、「強化」、「重大」)[2] 。状況に応じて、以下事項が含まれます。

- 非否防止または認証に対応した、エンドポイントレベルでの拡張可能な認証プロトコル
- 必要ならば、暗号技術によって保護されたエンドからクラウドへの接続性のサポート
- 暗号技術によって保護されたエンドツーエンド接続性をサポート(例：鍵のライフサイクルマネージメントにグループ鍵 PKI 標準を用いたもの)
- セキュアな公開・プライベートの「鍵ペア」(PKI)、および最新の量子暗号耐性を持つ暗号スイートの使用による高信頼データ転送
- ネットワークのホワイトリスト管理および上り下り(イングレス／エグレス)フィルタによるアクセス制御のためのローカルエンドポイントファイアウォール
- ハードウェアによるセキュアな鍵保存
- (関連する RFC で示された仕様に基づく))マルチベンダシステムでの相互運用性
- 当該システムに関連する転送プロトコルの完全なスイート(例えば TLS, DTLS, SSH, IPsec, IKE, Wireless, GDOI など)、および
- 「インダストリアルインターネット接続性フレームワーク」[IIC-IICF2017]で定義される接続性に関するコアプロトコルで使用されるセキュリティメカニズムとの互換性(当該メカニ

[1] NIST 800-53r5 CM-x, PM-9, PS-8, SI-12
NIST SP 800-12, 800-30, 800-39, 800-100
[2] IEC 62443 3-3: 5.10
NIST 800-53r5 AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SC-8, SC-12, SC-13, SI-4

ズムがオープンソーススタックで実行されるか、クローズドソーススタックで実行されるかは問わない）

継続的な監視

次のような、エンドポイントのリアルタイムかつ継続的な監視が求められます（「重大」）[1] ：

- ファームウェア、OS あるいはインストール済みアプリケーションに対する不正な変更の検出および防止のための構成制御、および
- データの機密性や完全性を危険にさらす不正なアクティビティ（安全ではない暗号鍵やハッシュアルゴリズムの使用など）を検出および防止するためのアプリケーションレベルでの制御

ポリシーおよびアクティビティダッシュボード

遠隔・分散しているエンドポイントの可視化および制御のために、OT（運用・制御技術）オペレータおよび管理者には、以下の事項が求められます（「重大」）:[2]

- セキュリティ制御を定義するためのリモートポリシー管理
- 複数かつ分散したエンドポイントのセキュリティポリシーオーケストレーション、および
- インシデント対応のための、全体性、関連性、および適時性のあるコンテキストを提供するイベントデータ

システム情報およびイベント管理

インシデント対応および監査向けに、セキュリティリスクを継続的に測定および評価し、脅威を軽減するために使用し得る有用なインプットとして、イベントログが必要です（「重大」）[3]。そのために、次のような能力が求められます:

- ポリシーに基づくリスク監視プロファイルを提供する、
- オープンインタフェース、データモデルあるいは拡張可能なフォーマット（例えば REST APIs、JSON など）を使用して、さまざまな産業分野において、ルールを配布あるいは振舞い分析を管理する、
- イベントに関するコンテキストデータをもとに、ルールを起動し、振舞い分析の結果を提供する、そして

[1] NIST 80053r5: CA-7, CA-7, CM-5, CM-8, CM-9, CM-11, IA-3, PL-8, RA-5, SA-10, SA-12, SA-22, SC-37, SI-2, SI-3, SI-7

[2] NIST 800-53r5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-9, CM-5, IA-2, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, SC-7, SC-13, SC-37

[3] NIST 800-53r5: AU-3, AU-6, MP-6, RA-5

- 拡張可能なフォーマット（CEF、SNMP など）を用いて、生成したイベントログを「セキュリティ情報およびイベント管理(SIEM)」サービスやデータヒストリアンに記録する。

結論

合意されたセキュリティレベルにおける適切なインダストリアルセキュリティを実行するためのベストプラクティスを説明することにより、本ドキュメントはインダストリアルエコシステムの参加者の能力を向上させることができます。

- 自営業者は、必要なセキュリティを定義し、要求することができます。
- インテグレータは、顧客のセキュリティ要件を満たすシステムを効果的に構築することができます。
- 機器メーカは、必要なセキュリティ機能を提供する製品を効率的に製造することができます。
- 政府機関は、インダストリアルセキュリティのベストプラクティスの採用を促すことができます。
- 保険会社は、より強力なインダストリアルセキュリティに対してインセンティブを提供することができます。

ベストプラクティスを採用することにより、アドホックアプローチよりも大幅に低コストで、インダストリアルセキュリティの改善を達成することができます。

本書は、ベストプラクティスの改善に伴い、今後改訂されることがあります。

頭字語

CEF	Common Event Format　共通イベントフォーマット
DTLS	Datagram Transport Layer Security データグラムトランスポートレイヤーセキュリティー
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards　フィップス (連邦情報処理標準)
GDOI	Group Domain of Interpretation　グループドメイン オブ インタープリテーション
ICS	Industrial Control System　産業用制御システム
IEC	International Electrotechnical Commission　国際電気標準会議
IEEE	Institute of Electrical and Electronic Engineers　米国電気電子学会
IETF	Internet Engineering Task Force　インターネット技術タスクフォース
IISF	Industrial Internet Security Framework インダストリアルインターネットセキュリティフレームワーク
IKE	Internet Key Exchange　インターネット鍵交換
IPsec	Internet Protocol Security

ISA	International Society of Automation 国際計測制御学会
ISO	International Organization for Standardization 国際標準化機構
JSON	JavaScript Object Notation
OCSP	Online Certificate Status Protocol オンライン証明書状態プロトコル
NIST	National Institute for Standards and Technology 米国国立標準技術研究所
OS	Operating System オペレーティングシステム
OT	Operational Technology 運用・制御技術
PCR	Platform Configuration Register 特殊な更新操作でのみ書き換え可能な記憶領域
PKCS	Public Key Cryptography Standards 公開鍵暗号化標準
PKI	Public Key Infrastructure 公開鍵インフラストラクチャ
REST	Representational State Transfer
RFC	Request For Comment (a series of standards from IETF IETF におけるインターネットコミュニティの標準等の検討が公表される一連の文書)
RoT	Root of Trust
SIEM	Security Information and Event Management セキュリティ情報およびイベント管理
SLB	Security Level Basic セキュリティレベル「ベーシック」
SLC	Security Level Critical セキュリティレベル「強化」
SLE	Security Level Enhanced セキュリティレベル「重大」
SNMP	Simple Network Management Protocol
SSH	Secure Shell セキュアシェル
TLS	Transport Layer Security トランスポート層セキュリティ
TNC	Trusted Network Communications トラステッドネットワーク接続
TPM	Trusted Platform Module トラステッドプラットフォームモジュール
UEFI	Unified Extensible Firmware Interface

参考文献

[Ind4.0-ITSec]	IT Security in Industrie 4.0: Action fields for operators, November 2016, retrieved 2017-12-12 http://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/guideline-it-security-i40-action-fields.html
[IEC-62443-11]	International Electrotechnical Commission: IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009, retrieved 2016-09-02 https://webstore.iec.ch/publication/7029

[IEC-62443-31] International Electrotechnical Commission: IEC 62443-3-1:2013, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems, 2009, retrieved 2017-12-22 https://webstore.iec.ch/publication/7031

[IEC-62443-33] International Electrotechnical Commission: IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013, retrieved 2016-09-02 https://webstore.iec.ch/publication/7033

[IIC-IICF2017] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G5: Connectivity Framework, version 1.00, 2017-February-28, retrieved 2017-12-12 https://www.iiconsortium.org/IICF.htm

[IIC-IISF2016] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G4: Security Framework, version 1.00, 2016-September-26, retrieved 2017-12-12 https://www.iiconsortium.org/IISF.htm

[IIC-IIV2017] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G8: Vocabulary, version 2.00, 2017-July-19, retrieved 2017-12-12 https://www.iiconsortium.org/vocab

[NIST-800-53r4] National Institute of Standards and Technology (NIST): Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 2013 April, retrieved 2016-09-02 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[NIST-800-53r5] National Institute of Standards and Technology (NIST): Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5, 2017-August, retrieved 2017-12-22 https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[NIST-800-57p1r4] National Institute of Standards and Technology (NIST): Special Publication 800-57, Recommendation for Key Management Part 1: General Security, Revision 4, 2016-January, retrieved 2018-01-12 http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4

[NIST-800-82] National Institute of Standards and Technology (NIST): Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, revision 2, 2015-May, retrieved at 2016-09-02 http://dx.doi.org/10.6028/NIST.SP.800-82r2

著者および法律上の注意事項

本書は、Steve Hanna (Infineon) 、Srinivas Kumar (Mocana) および Dean Weber (Mocana) の執筆により、インダストリアルインターネットコンソーシアムのセキュリティ WG が発行しました。

The Endpoint Security Best Practices White Paper, published March 2018 and accessible here, https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf, is the definitive white paper publication. The publication date of this translated version is found in the footer of Page 1 of this document.