IEC62443の実装

NEXTY Advanced Technology Company

- インダストリー4.0やインダストリアルIoTのおかげで、産業オートメーションおよび制御システム業界は絶好の機会を迎えていますが、このような機会とともに、セキュリティの脅威も出現します。産業界としては、増加するサイバー攻撃に備えて、設備の故障、停止、安全上の問題への対策が必須です。

- そこで、世界各国の産業セキュリティ専門家は、産業セキュリティに関する権威ある指針を作成しました。それが、**新しい国際的産業セキュリティ規格IEC 62443**です。この規格は、現在および将来の脅威から産業用ネットワークを守るための推奨事項を網羅した、一連の包括的な文書で構成されています。

- インダストリアルIoTに関連するあらゆる企業は、IEC 62443を使った利害関係の保護を検討するべきです。当社は、産業セキュリティのリーダーとして、IEC 62443の実装に関する有益な情報を提供し、システムインテグレータ、メーカー、資産所有者が、強固な産業セキュリティを実現できるように支援します。

セキュリティ世界標準の動向

NEXTY Advanced Technology Company

調達基準の厳格化

国際的な調達基準とユーザの関連性

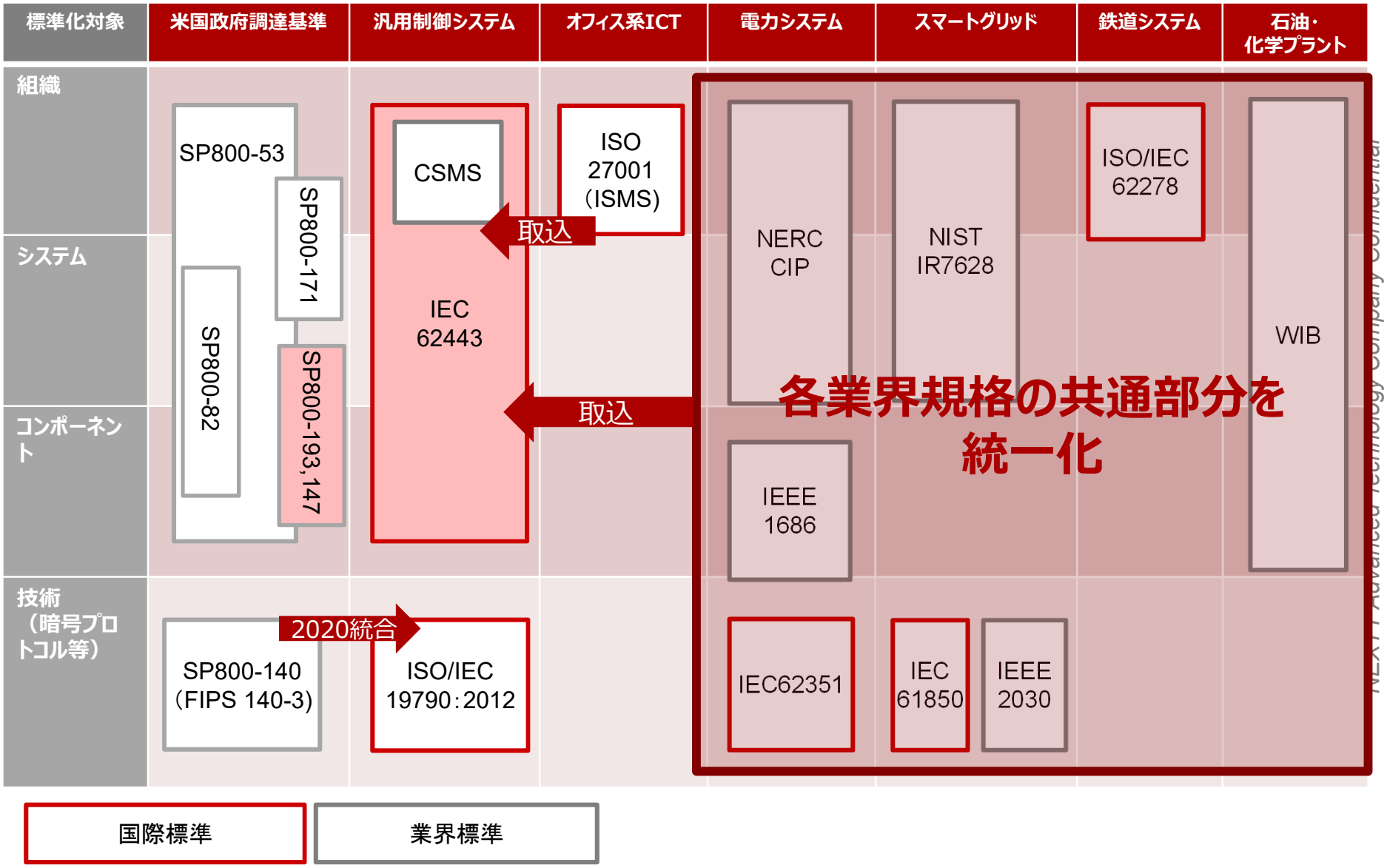
- NIST SP800-171（米国国防総省との取引企業が準拠を義務付けられているセキュリティ対策基準）
- 日本国内でもNIST SP800-171と同程度の新防衛調達基準の試行導入がスタート（2019年4月）
- 経団連もサイバーリスクに対処するためにNIST SP800-171を取り上げており、企業経営層に向けてサイバーセキュリティ対策を促している。

IEC62443と部品調達・機器製造の関連性

SP800とIEC 62443の関係性
＞米国政府の調達基準であるSP800シリーズと、
国際標準規格であるIEC62443は、対応範囲がほぼ同じであり、
下位の規格であるSP800-140とISO19790の
統合の動きに代表されるように、今後、相互補完・統合していくと予想します。

制御システムセキュリティにおけるIEC62443

NEXTY Advanced Technology Company



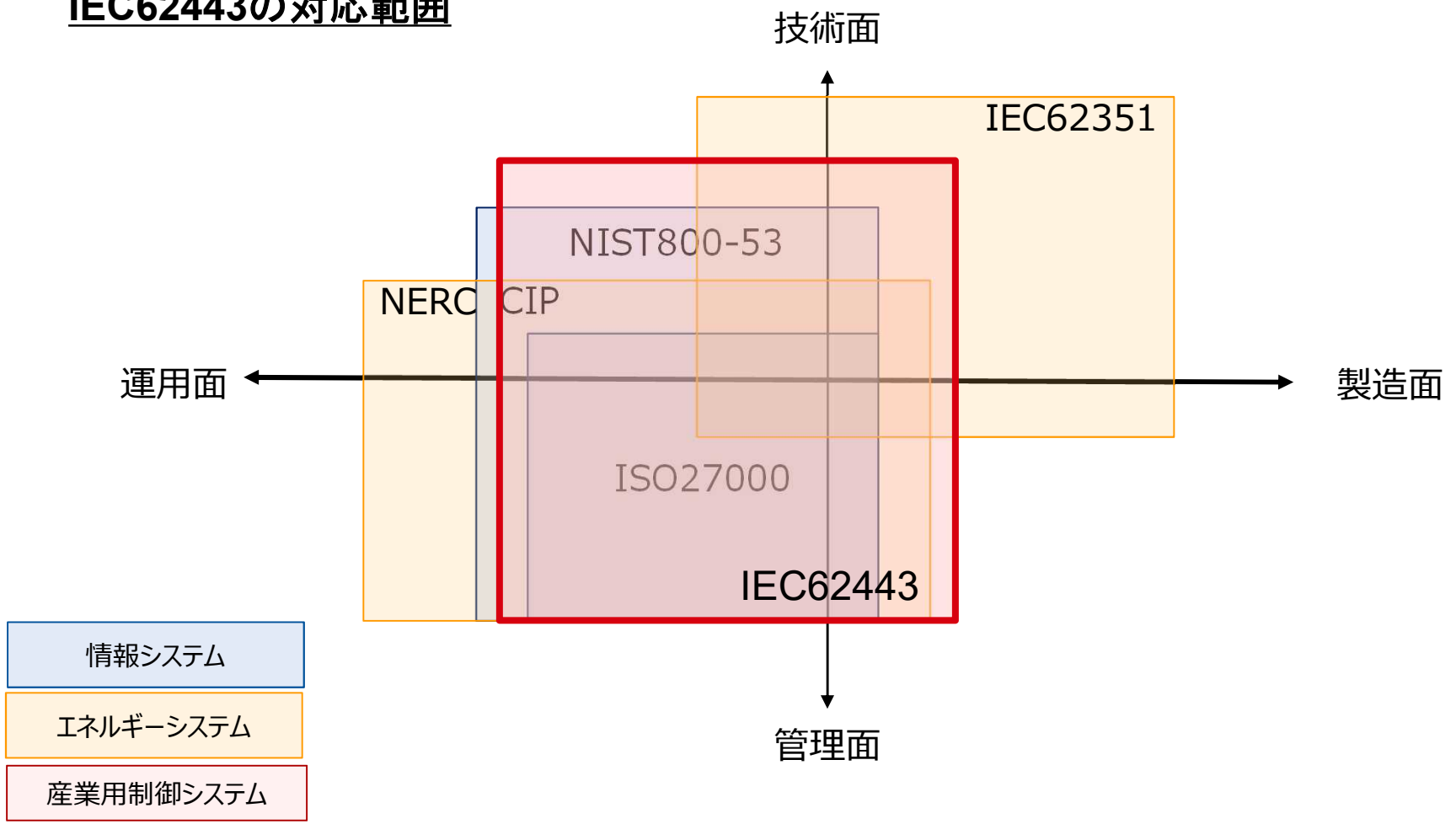
米国NISTの調達基準「SP800-53」をほぼ含有

NEXTY Advanced Technology Company

- 欧州・米国共通の標準規格

  ⇒技術・運用・製造・管理にてグローバルスタンダードになると予想

IEC62443の対応範囲



IEC62443の構成（4グループ･仕様）

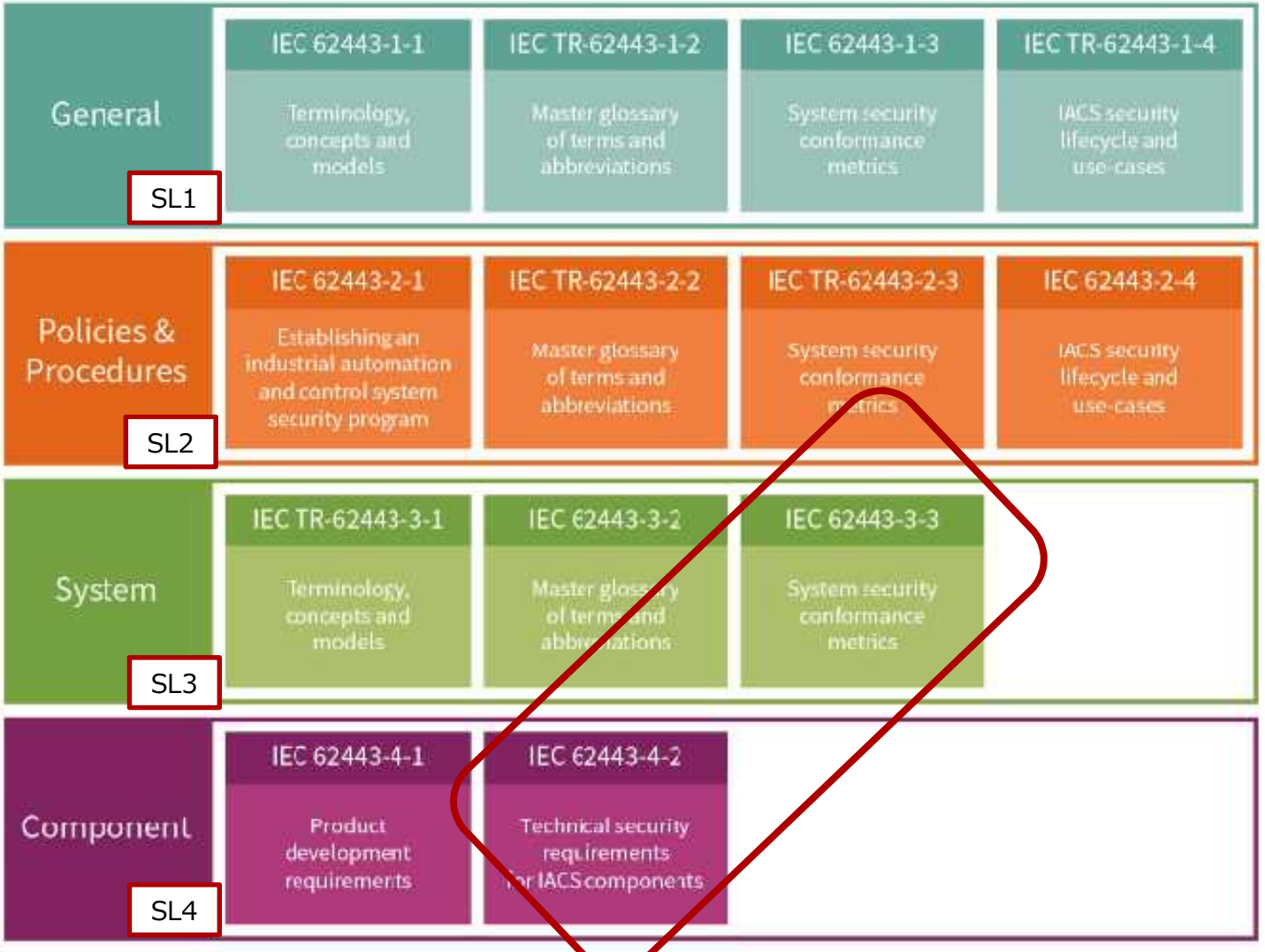
NEXTY Advanced Technology Company

<IEC62443取得者>

エンドユーザー様

システムインテグレーター様

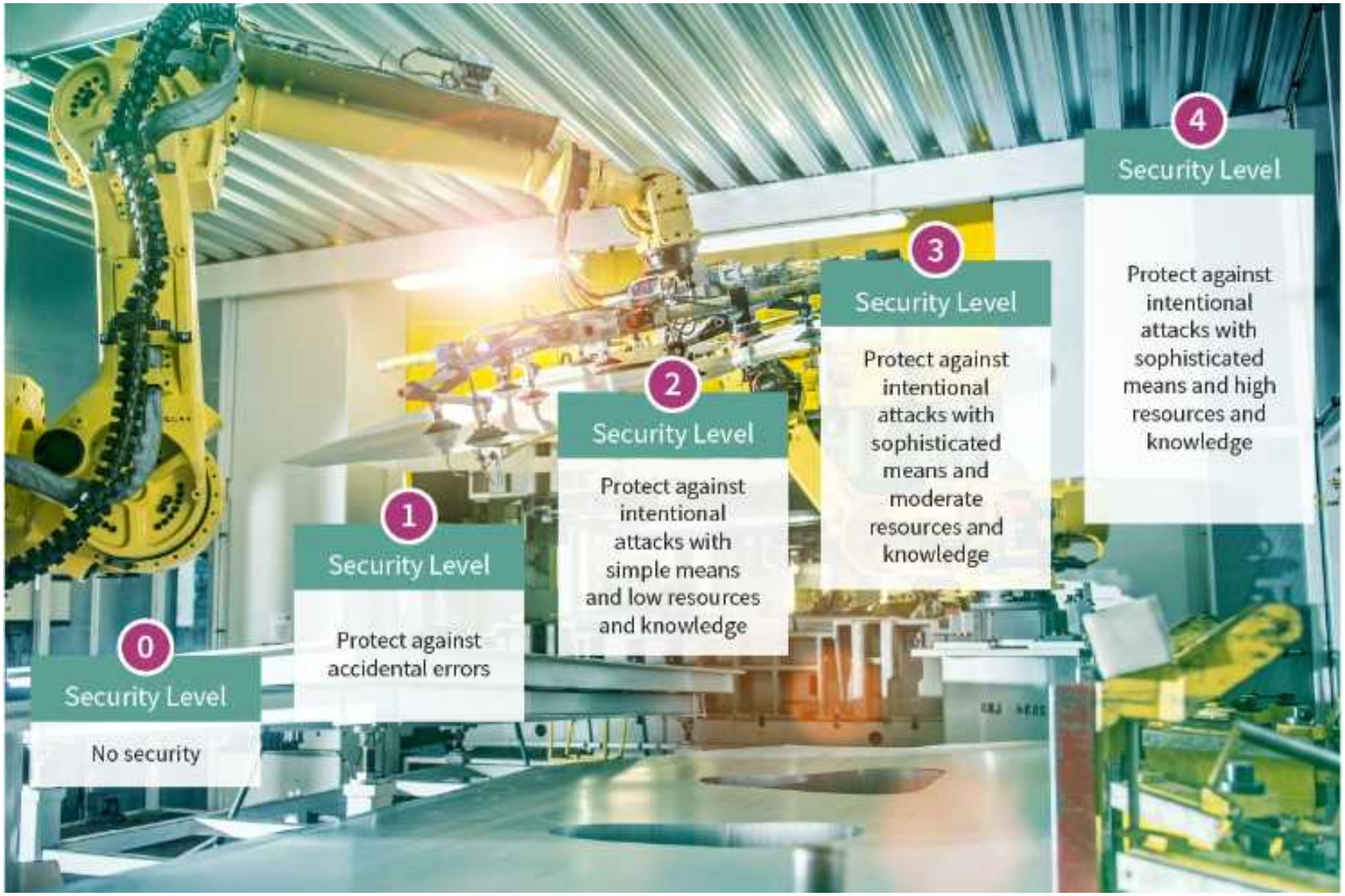
デバイスメーカー



デバイスメーカー側で4-2及び3-3で要求されているセキュリティレベルをシステムレベルで対応が必要

セキュリティレベル

NEXTY Advanced Technology Company



IEC62443-4-2 セキュリティ要件概要

NEXTY Advanced Technology Company

例えば、IEC62443-4-2には幾つかのFundamental Requirementが設定されていて、それぞれのFRに幾つかの項目が定義されています。

FR1	Identification and authentication control 識別および認証制御	人間、コンポーネント（デバイス、SWプロセス）の識別と認証要件を定義	SL3では「一意性と**HWによる識別子の保護**」、および、「**多要素認証**」が求められる
FR2	Use Control 利用制御	利用権限とアクセス制御、セッション管理、ロックアウト、監査要件を定義	OS／ネットワーク機能／アプリケーションを組合せて実現する必要がある
FR3	System Integrity システムの完全性	コンポーネント・通信の完全性、真正性検査、安全な更新、物理保護要件を定義	マルウェア対策、改ざん検知、侵入検知、**安全な更新**、物理防御、**RoTによるセキュアブート、データ保護**が必要
FR4	Data Integrity データの機密性	通信中および保持するデータの保護、解放／廃棄時の情報破棄要件を定義	SL3では廃棄時のデータ消去確認機能が必要
FR5	Restricted data flow データフロー制御	ネットワーク機器による通信制御とセグメント化の要件を定義	NW機器に対する要件。FWやルーティング制御により、NWをセグメント化する必要がある
FR6	Time Response to events イベントへのタイムリーな対応	監査ログのアクセス制限、インシデント監査、検出、報告要件を定義	監査ログへのアクセス制御機能、および、常時監視ツールの実装が求められる
FR7	Resource availability リソースの可用性	障害や災害、攻撃による停止、復旧、インベントリ報告の要件を定義	DOS対策、バックアップ、回復時の設定の維持、インベントリ報告機能の実装が求められる

FR1のセキュリティレベルにはSL1～4が定義されていて、このFRではSL3相当以上が必要と考えます。

セキュリティレベル定義： FR1の例

レベル	概要	対象（**弊社見解**）
SL 1	簡易な手法もしくは偶発的な不正アクセスから保護	
SL 2	少ない設備、汎用スキル、低モチベーションの単純な手段を使用した、意図的な不正アクセスから保護	コンシューマ機器等、安全性や機密性、プライバシーへの影響が少ない機器
SL 3	適度な設備、IACS固有のスキル、適度なモチベーションによる、意図的な不正アクセスから保護	産業機器や安全性・機密性・プライバシーを扱う機器
SL 4	大規模な設備とIACS固有のスキル、高いモチベーションによる、意図的な不正アクセスから保護	重要インフラ機器等

産業機器はSL3相当のセキュリティレベルが必要

- 機器を一意に識別
  - パスワード、共通鍵認証でも基準は満たすが、弊社としては、運用上の安全性、利便性を考えた場合、公開鍵/電子証明書による認証を推奨
  - 安全な鍵の管理、配付、書込み（＝プロビジョニング）、定期的な更新の仕組み
- ユーザを一意に識別
  - 多要素認証
  - 特権アカウントの設定
- 識別情報のHWによる保護
  - Root of Trustによる認証鍵、検証鍵、パスワード情報の保護
- システム、通信の完全性検証
  - Root of Trustによるセキュアブート
  - ソフトウェア、通信、バックアップの改ざん検知と通知機能
- 安全な更新機能
  - ソフトウェア更新時の改ざん検知、真正性（＝提供元）の検証

IEC62443-4-2のFR1を確認した場合に、システム上に「安全な鍵管理」や「Root of Trustによるセキュアブート」が要件として最終的に上がってくるので、それを実現するためにはセキュリティICは必要！

セキュリティICの必要性

NEXTY Advanced Technology Company

国際調達基準の導入が始まっている

国際調達基準の暗号技術は、今後の国際標準となる
IEC62443で包括される

IEC62443のコンポーネント/部品単位には
安全な鍵管理やセキュアブートの機能が要求される

これら要求を実現するためにはハードウエアのセキュリティICが必要

ハードウェアセキュリティのメリット

NEXTY Advanced Technology Company

- 問題提起
  - IEC 62443では、セキュリティレベル3および4に対して、ハードウェアセキュリティを要求しています。なぜハードウェアセキュリティが必要なのでしょうか？
  - ディスクリートのハードウェアセキュリティチップは、単なるソフトウェアセキュリティよりもはるかにセキュアです。ソフトウェアは、攻撃者に解析されて脆弱性を発見され、セキュリティが脅かされる攻撃を仕掛けられやすいと言えます。このような攻撃は、毎日起こっています。耐タンパ性を持つ(改ざん防止された)ハードウェアセキュリティチップは、そのような攻撃を効果的に阻止できます。

- 対策
  - 多くのハードウェアセキュリティチップは、独立したセキュリティ試験機関によって評価され、認証されています。この認証は、防御されたチップへの侵入に対して最も高度な障壁があることを証明しています。誰でもセキュリティ機能を提供していると公言することはできますが、重要なアプリケーションについては、独立した専門家の評価が必要です。
  - ハードウェアセキュリティは、設計およびサポートのコストを削減します。カスタムメイドのセキュリティは、開発費用が高価であり、常にメンテナンスが必要です。インフィニオンのセキュリティチップをお選びいただけば、当社の数十年にわたるセキュリティの専門知識を活用できます。

- まとめ
  - これらを含むさまざまな理由により、セキュリティ専門家の意見は、重要なシステムには耐タンパ性を持つ(改ざん防止された)セキュリティチップが最善のアプローチであるということで一致しています。だからこそ、IEC 62443ではハードウエアセキュリティチップを要求しているのです。