制御システムセキュリティ
国際標準の現状と日本の取組み

2011年11月18日
独立行政法人 情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ技術ラボラトリー
ラボラトリー 長　小林 偉昭

講演目録

- 情報処理推進機構(IPA) について
  ◇組織のご紹介
  ◇IPAの取組み

- 制御システムセキュリティ
  ◇制御システムセキュリティの状況
  ◇経済産業省の国策とIPAの活動
  ◇標準規格：IEC62443のご紹介
    ・IEC62443全体概要と規格化状況
    ・IEC62443-2-1の概要
    ・IEC62443-3-3の概要
  ◇評価・認証の動向について

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報処理推進機構(IPA)について
～組織のご紹介～

<組織のご紹介>

IPAとは
(Information-technology Promotion Agency,Japan)

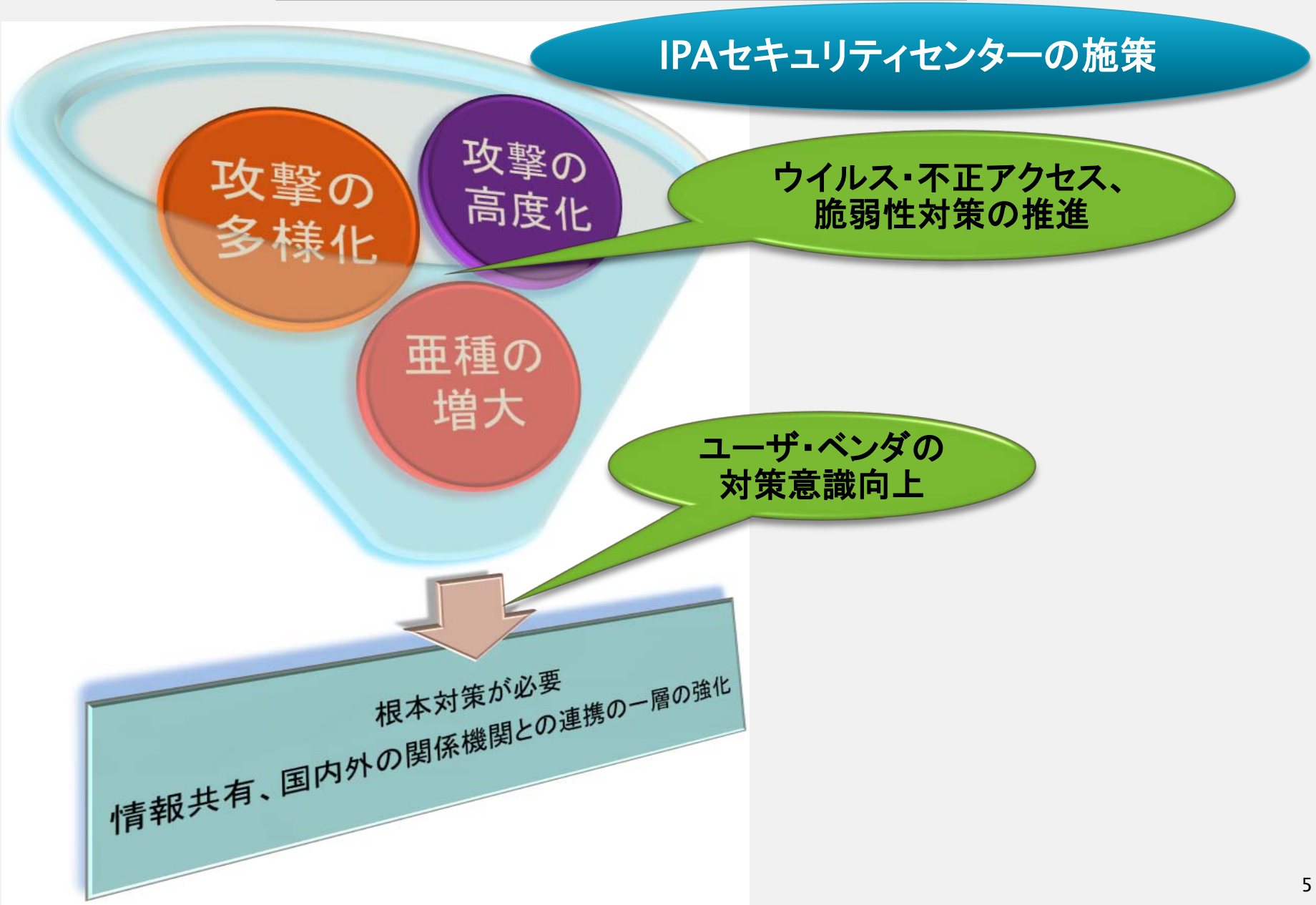
◇経済産業省所管の独立行政法人

◇IT産業の健全な発展を推進し、国民すべてにITのメリットが行き渡る社会の実現に向けた取組み

◇次の4つの柱がIPAの重点施策

<組織のご紹介>

日本の情報セキュリティ力の強化



IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

情報処理推進機構(IPA)について
～IPAの取組み～

技術本部セキュリティセンター施策
ウイルス・不正アクセス対策、脆弱性対策について

<＜IPAの取組み＞

脆弱性のない安全なシステムの開発、運用に向けたセキュリティセンターの主な活動

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

セキュリティ対策

- 調査、動向把握、開発方針・体制整備（ビジネスインパクト分析含む）
- セキュアプログラミング
- ソースコード検査
- テスト（ファジング他）
- 脆弱性診断（ペネトレーション）
- 運用時対策
- 脆弱性対策

システムライフサイクル

1. 企画 → 2. 設計 → 3. 実装 → 4. テスト → 5. 運用／利用 → 6. 廃棄

- 脅威、動向：1. 企画
- 脆弱性：2. 設計、3. 実装、4. テスト
- 攻撃：5. 運用／利用

IPAの活動・成果物

- 10大脅威
- 情報セキュリティ白書
- 知っていますか？脆弱性

＜調査・ガイド類＞
- 組込みシステム向け
- 情報家電向け
- 制御システム向け
- 自動車向け
- 生体認証導入、運用ガイド

- 安全なWebサイトの作り方
- 安全なSQLの呼び出し方
- セキュアプログラミング講座
- 開発者向け脆弱性実習ツール：AppGoat
- 「ソースコード検査ツール
- 「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

- TCP/IP 脆弱性検証ツール
- SIP 脆弱性検証ツール

- ウイルス対策のしおり
- Web攻撃検出ツールiLogScanner
- WAF読本
- 安全なWebサイト運営入門
- 5分でできる！情報セキュリティポイント学習

【届出制度／脆弱性／ウイルス】
- 脆弱性届出制度（PP/Web）
- JVN, JVN iPedia, MyJVN
- ウイルス、不正アクセス届出制度
- 安心相談窓口

IPAの取組み(1)～ウイルス・不正アクセス届出～

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ウイルス・不正アクセスの届出

IPAは、経済産業省の告示に基づき、コンピュータウイルス及び不正アクセスの届出を受付け、毎月国内の被害状況を統計データとして公表するとともに、被害の事例紹介や必要に応じて、注意喚起、緊急対策情報などを随時発信しています。

【届出】 http://www.ipa.go.jp/security/todoke/

【報告】 http://www.ipa.go.jp/security/txt/list.html

【注意喚起】 http://www.ipa.go.jp/security/announce/alert.html

「情報セキュリティ安心相談窓口」の開設

IPAは、コンピュータウイルスをはじめとする不正なプログラム(マルウェア)や不正アクセスに関する総合的な相談窓口を開設しています。

http://www.ipa.go.jp/security/anshin/

標的型サイバー攻撃に特化した特別相談窓口も設置

電話:03-5978-7509 (平日 10:00～12:00、13:30～17:00)

FAX:03-5978-7518 e-mail:anshin@ipa.go.jp

★ オペレータに、標的型攻撃メールと思われる不審メールを受け取ったと伝えてください

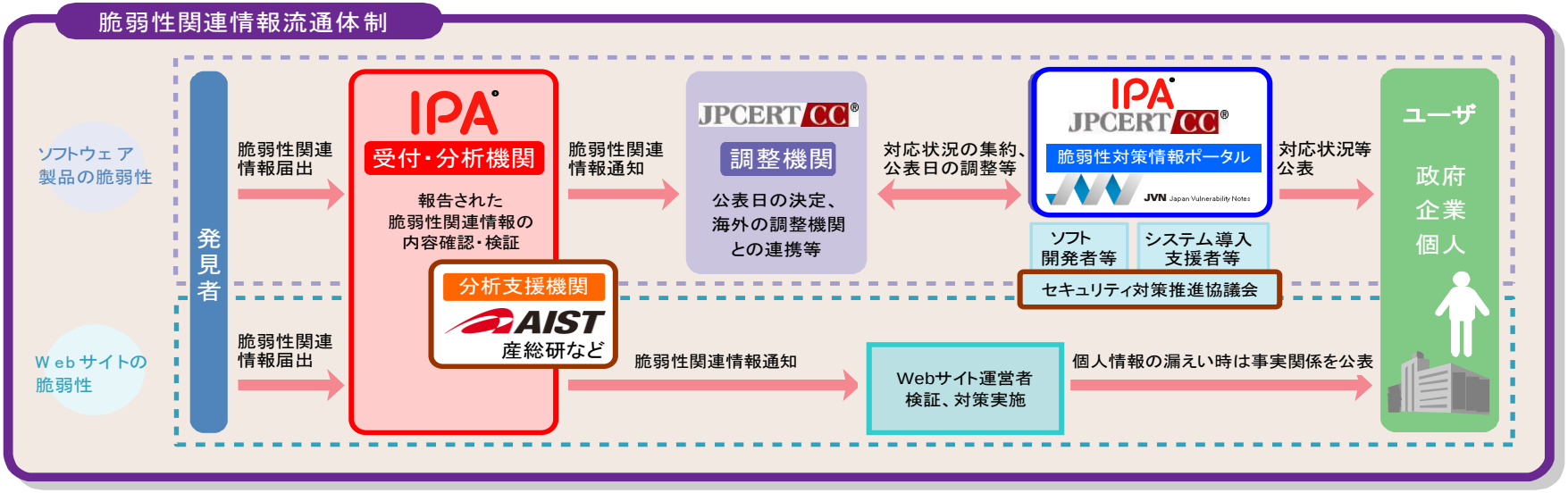
<＜IPAの取組み＞

IPAの取組み(2)~脆弱性対策~

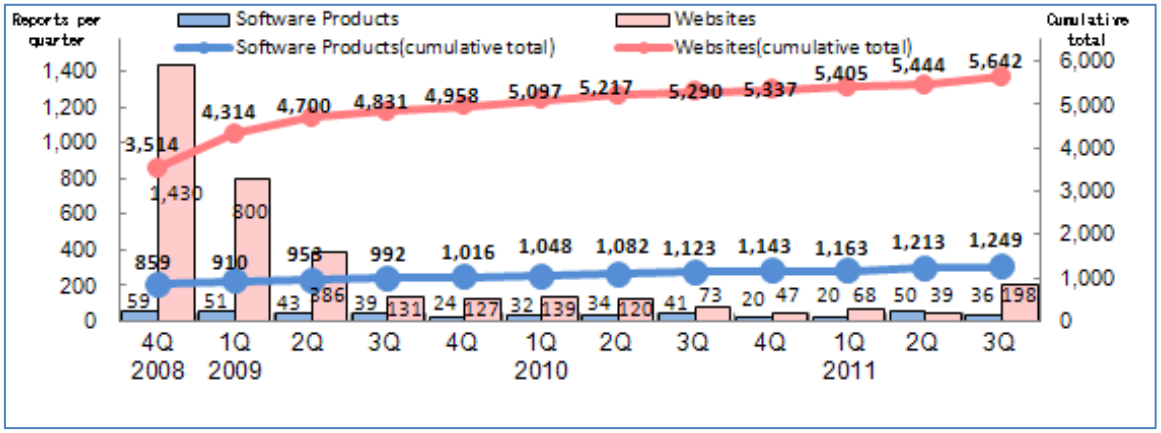
脆弱性関連情報の届出制度

http://www.ipa.go.jp/security/vuln/index.html

2004年7月に経済産業省が「ソフトウエア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）を公示し、「情報セキュリティ早期警戒パートナーシップガイドライン」に則り運用を行っている。



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：独立行政法人　産業技術総合研究所



2011 3Q(Jul-Sep)

分類	件数
ソフトウエア	1,249
ウェブサイト	5,642
累計	6,891

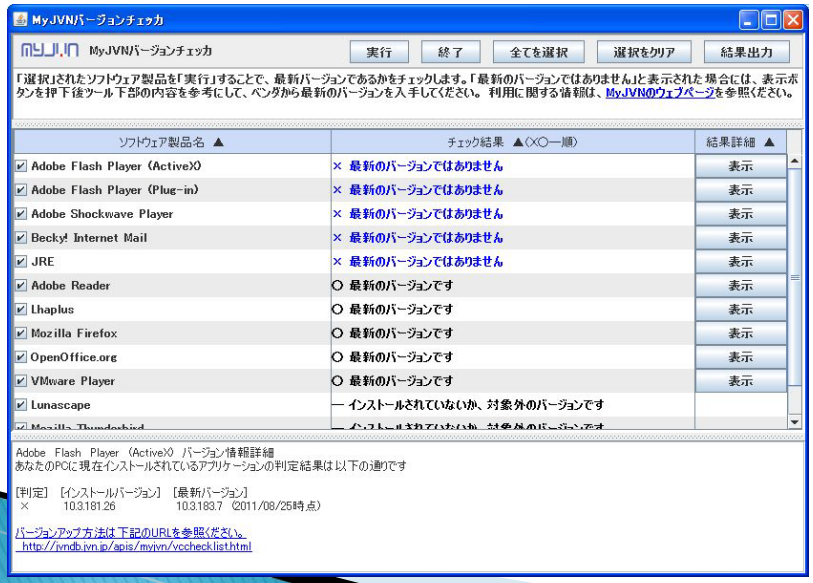
IPAの取組み(3)～脆弱性対策～

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

MyJVNバージョンチェッカ MyJVN
http://jvndb.jvn.jp/apis/myjvn/

MyJVNを利用して、使っているソフトウェアが最新か、確認をして下さい。

- 利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール
- チェックリストに基づき、バージョンが最新であるかどうかのチェックを手作業ではなく、ツールにより作業を自動化する。
- サーバOS（Win,Linux）上でサーバソフトウェアもチェック可能 【2011年8月】



CPE common platform enumeration
OVAL oval.mitre.org
XCCDF security benchmark automation

制御システム*セキュリティ

*ICS:Industrial Control Systems

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

制御システムセキュリティ
～制御システムセキュリティの状況～

迫りくる制御システムへのサイバー脅威

IPA INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

＜従来の制御システム＞

◇常時ネットワークにつながっていない

◇制御システムの仕様は事業者ごとに固有

・内部仕様を熟知していなければ、有効な攻撃は不可能

「一般的なPCが感染するウイルスや不正プログラムの影響を受けない」

制御システムの生産性・保守性等の利便性向上と引き換えにサイバー脅威が現実化

＜最近の制御システム＞

◇外部ネットワークと接続する傾向にある

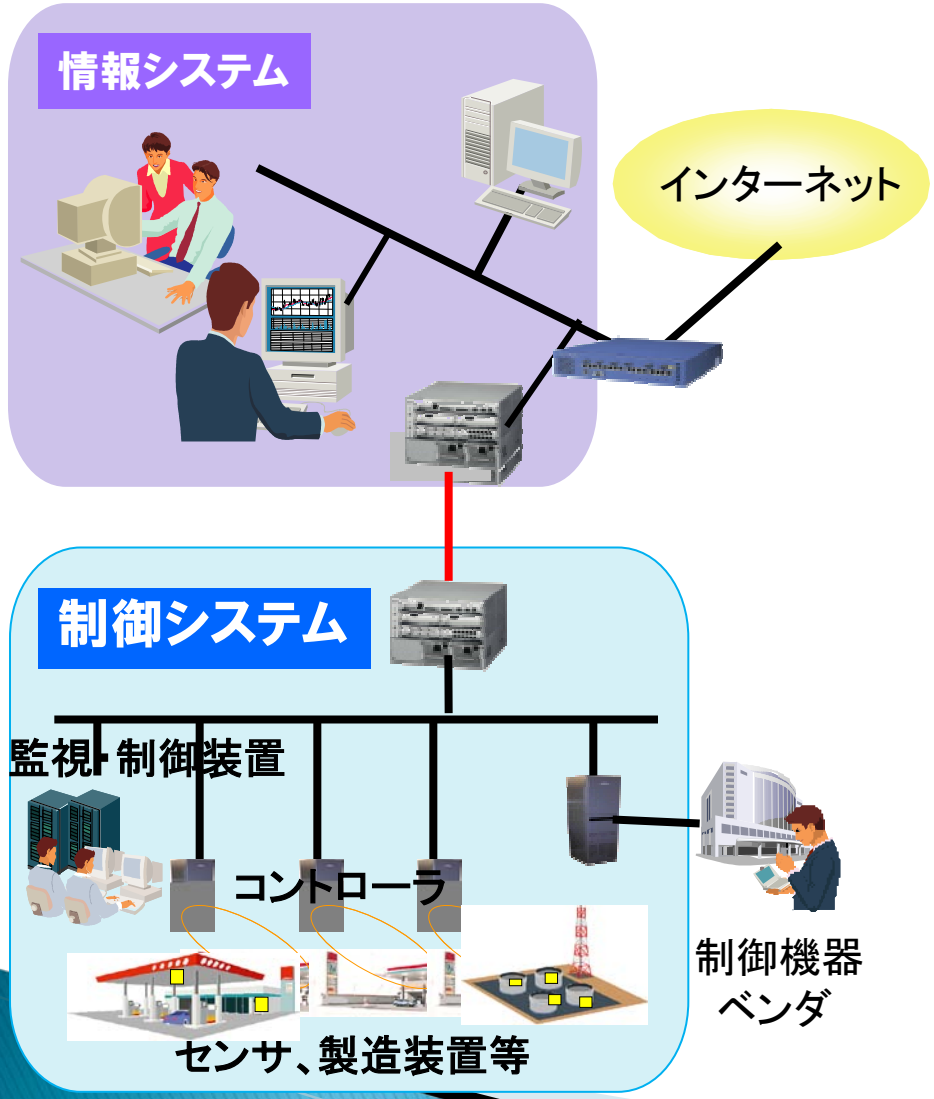
◇制御システムの仕様がオープン化(汎用製品及び標準プロトコル採用)

・WindowsやUnix系等、一般的な情報システムOSの利用が進んでいる

「一般的なPCと同様、ウイルスや不正プログラムの影響を受けやすい」

<制御システムセキュリティ>
制御システムセキュリティの状況

制御システムにおけるセキュリティの脅威



動向：

① 共通プラットフォームの利用
② 利便性からネットワークへの接続
③ 無線の利用

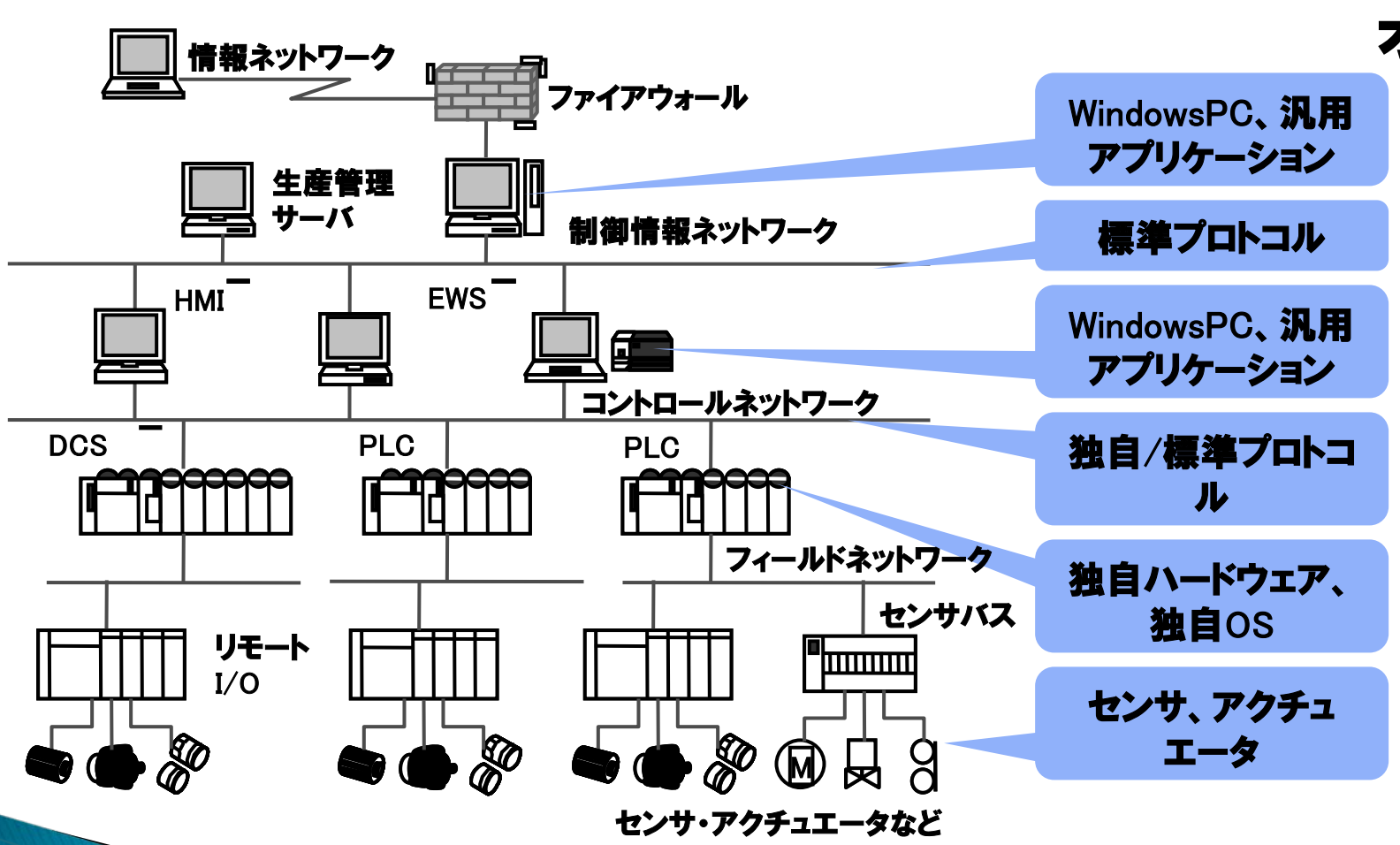
課題：

① 長期間利用（10年～20年）に耐えられる適切なセキュリティ対策
（脆弱性対策含む）
② 組織、社会に対する重大な影響
③ 準拠すべきセキュリティ基準、標準

<制御システムセキュリティ>
制御システムセキュリティの状況

制御システムの現状

「オープン化」:汎用製品＋標準プロトコル



各種製造装置における汎用IT技術の利用

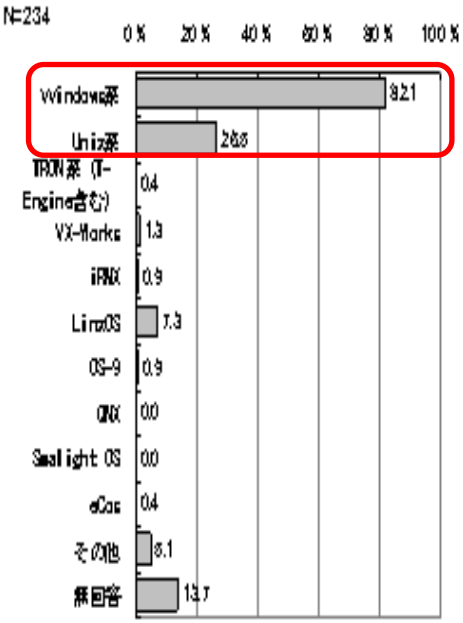


図 5.1-1 OSの利用状況（サーバ）

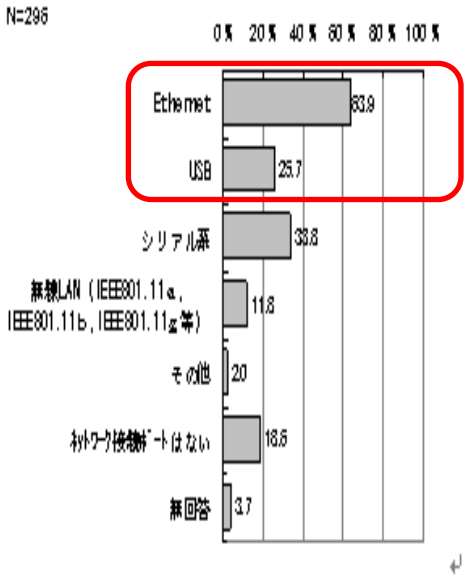


図 5.1-3 ネットワーク接続ポートの有無（サーバ）

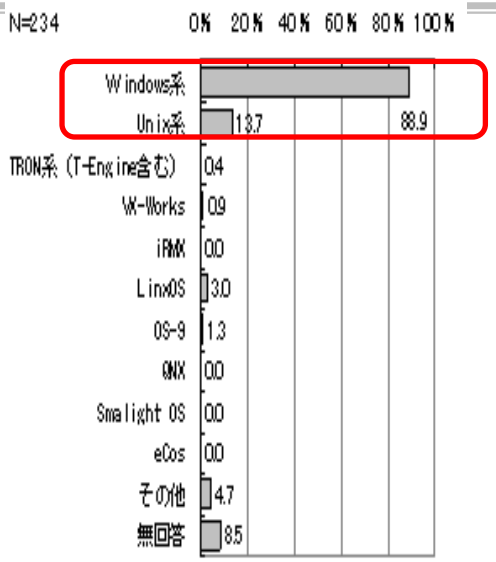


図 5.1-4 OSの利用状況（端末）

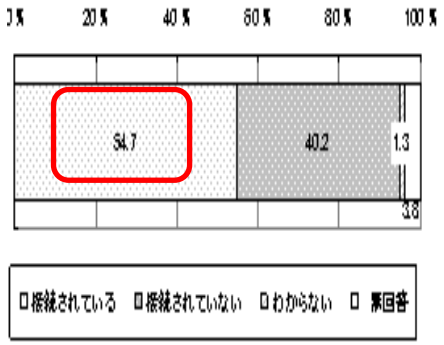


図 5.1-7 社内情報系システムとの接続

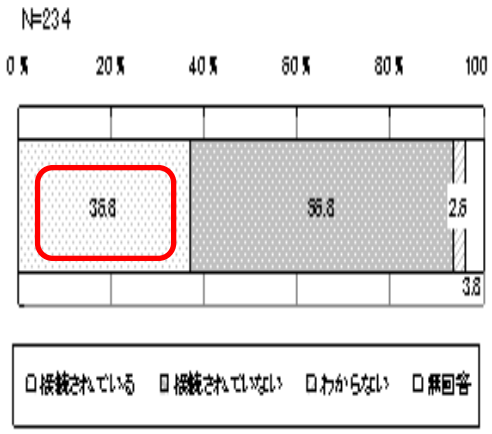


図 5.1-8 外部ネットワークとの接続

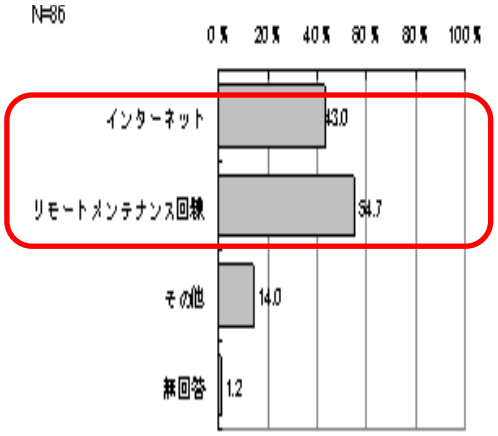


図 5.1-9 外部ネットワークとの接続先

出典：工業用装置等における汎用IT技術応用に起因する脅威と対策に関する実態調査事業　報告書(経済産業省)

制御システムのセキュリティ課題

【課題１：オープン化に伴う脆弱性リスクの混入】

・汎用製品、標準プロトコルネットワーク採用により、脆弱性リスク、ワームなどのウイルスの侵入や、機密情報漏えいのおそれがある。

【課題２：製品の長期利用に伴うセキュリティ対策技術の陳腐化】

・制御システムは通常10～20年使用。セキュリティ対策も最新ではない可能性がある。

【課題3：可用性重視に伴うセキュリティ機能の絞込み】

・可用性重視の観点から、一般的に、システム上の負荷となるウイルス監視やチェックプログラムの自動更新がない、または間隔が長い。

	制御システム	情報システム
セキュリティ優先順位	A.I.C（可用性重視）	C.I.A（機密性重視）
セキュリティの対象	モノ（設備、製品） サービス（連続稼動）	情報

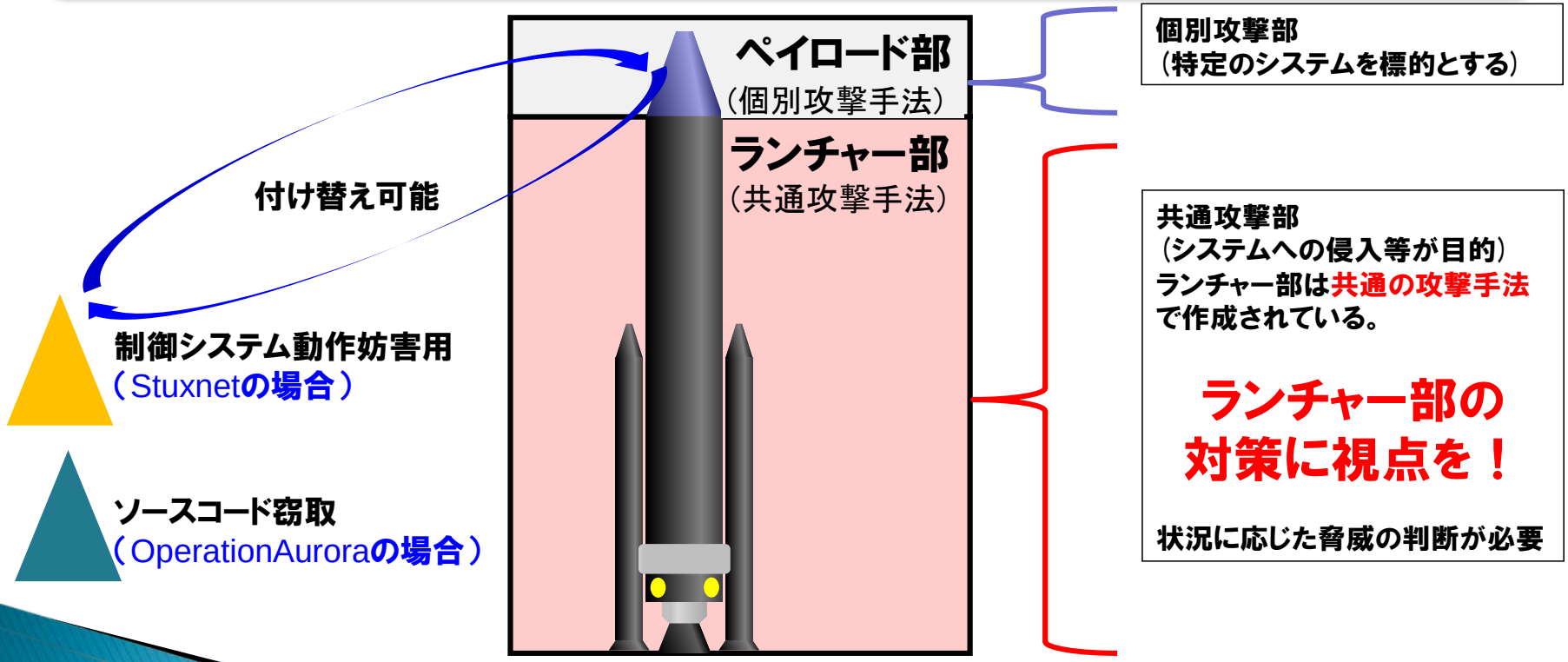
資料：IPA「重要インフラの制御システムセキュリティとITサービス継続に関する調査」より抜粋

新しいタイプの攻撃（APT）

APT：Advanced Persistent Threats

IPA INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

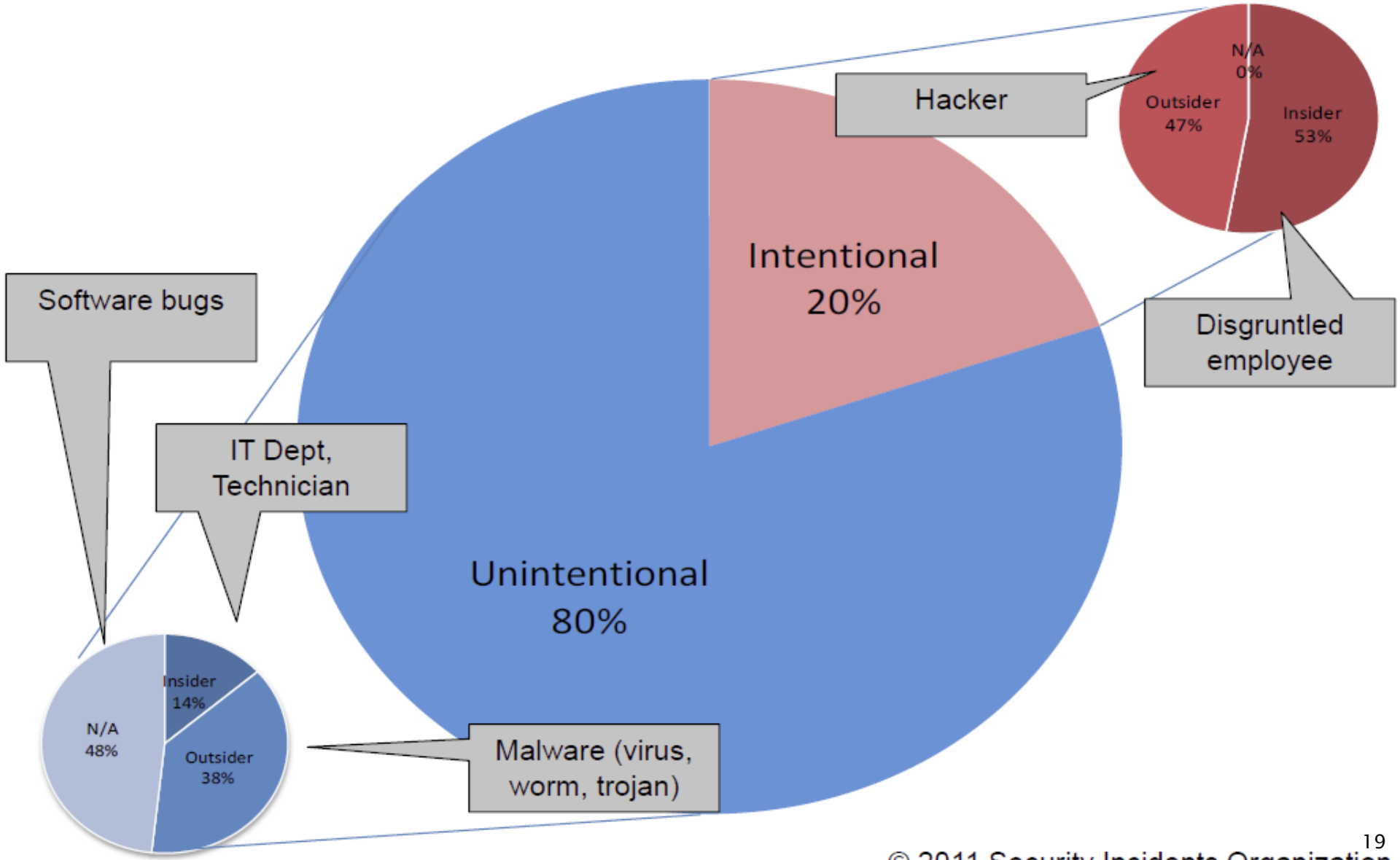
『新しいタイプの攻撃』をロケットの例で考えてみると、システムへの攻撃に特化したペイロード部と特定のシステムに侵入する為の共通仕様部分のランチャー部に分けることができる。



ネットワークに接続する以上、組込み機器にも情報セキュリティを要検討

セキュリティインシデントの各種分類・統計

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN



IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

重要インフラの制御システムの事故の例

原子力発電所の制御システムへのワーム侵入

- 発生した原因

◇VPN接続による内部感染

◇対象パッチの未更新

- 事件の影響

◇6時間の運用停止

2003 年1 月、オハイオ州Davis Besse 原子力発電所でマイクロソフトのSQL サーバを狙ったSlammer（読み方：スラマー）ワームがVPN（Virtual Private Network）接続を介して侵入・感染し、SCADA システムを約5 時間にわたって停止させた。同施設のプロセス・コンピュータも停止し、再運用までに約6 時間を費やしたほか、他の電力施設を結ぶ通信トラフィックも混乱し、通信の遅延や遮断に追い込まれた。感染したSlammer ワームに対するパッチは、その時点で公開されていたが、発電所のシステムには該当パッチがあてられていなかった。

Davis Besse 原子力発電所

重要インフラの制御システムの事故の例

- アンチウイルスソフトがシステムの安全停止を妨害

- 発生した原因
  ◇不正操作(過失)
- 業種
  ◇石油

TÜVが認証済のボイラー安全保護システムはPCワークステーション上で動作するMicroSoft Excelを使用していた。また、このワークステーションはノートン社製のアンチウイルスソフトを導入していた。このアンチウイルスソフトはPCと保護システムとの間の固有通信を妨害し、安全停止が実行されなかった。

重要インフラの制御システムの事故の例

- セキュリティ監査時にPLCが故障
- 発生した国
  ◇米国
- 業種
  ◇食品会社
- 事故原因
  ◇内部者(過失)
- 想定被害
  ◇$1M以上の損失

セキュリティコンサルタント は食品会社の事業とネットワークの脆弱性を監査した。一時的に妨害を行なうパケットを Ethernetでコントロールネットワークに流したため、複数のPLCに深刻な欠損が生じた。このパケットは4か、それ以上のICMPエコー要求を含むものであった。

Source: The Repository of Industrial Security Incidents (www.securityincidents.org)

制御システムにおける情報セキュリティ事故の被害例（海外）

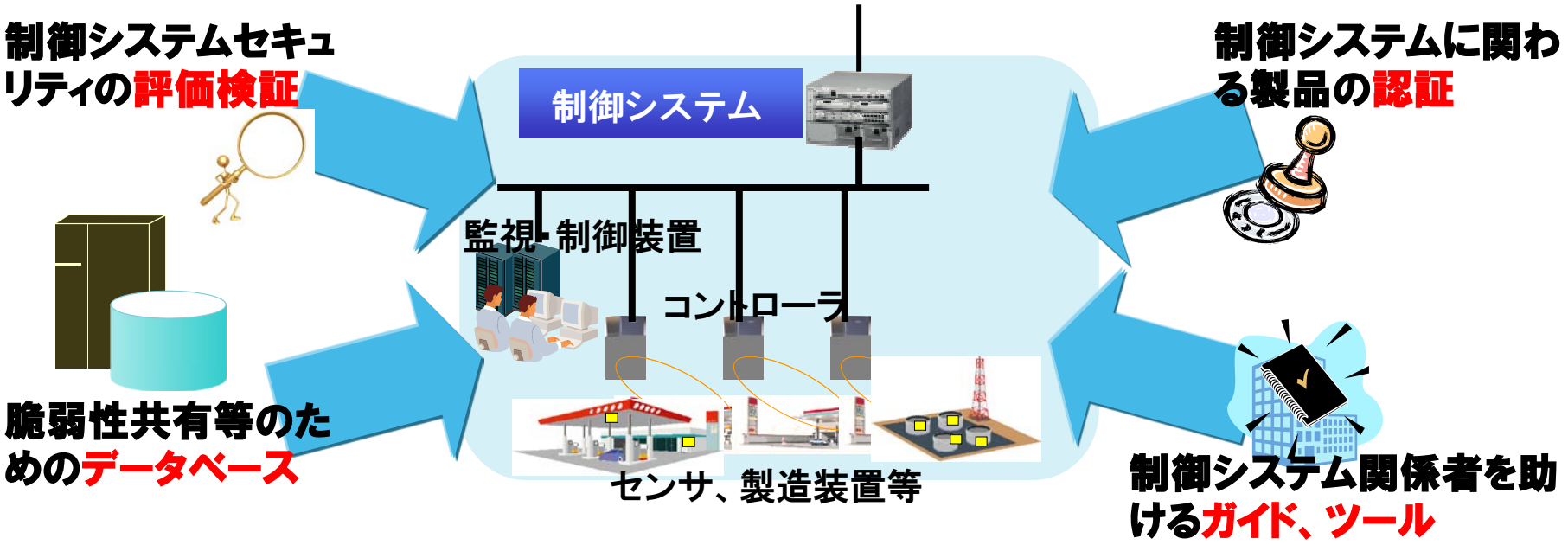
年	ウイルス名	ポイント	概要
2003	Slammer ワーム	原子力発電所の制御システムへのワーム侵入	米国の原子力発電所で、マイクロソフトSQLサーバを狙ったウィルスがVPN接続を介して侵入・感染。制御システムを約5 時間にわたって停止させた。他の電力施設を結ぶ通信トラフィックも混乱し、通信の遅延や遮断に追い込まれた。発電所のサーバはファイアウォールで外部ネットワークと遮断されていたが、ファイアウォール内部のネットワークに接続した、発電所のコンサルタント会社の端末が感染源となった。
2003	W32/ Blaster ワーム	鉄道の信号管理システムのウイルス感染による運行停止	米国東部の鉄道会社の信号管理システムがコンピュータウイルスに感染し、周辺の3 路線で朝から昼にかけて通勤および貨物列車が停止、ダイヤ乱れが発生。ウイルスによって、信号や配車のシステムなどの重要システムをつなぐネットワーク部分が、断絶したことが原因と判明。
2005	Zotob ワーム	ウィルスによる自動車工場の操業停止	米国大手輸送関連会社の米国にある複数の自動車工場において、ウィルスが制御システム内に入り込み、プラント中に広がり、操業停止となる事故が発生。Windows2000システムにパッチをあてることで生産を再開したが、部品サプライヤへの感染も疑われ部品供給の懸念も生じ、およそ1,400 万ドルの損害をもたらした。
2010	Stuxnet	システムの停止又は暴走・破壊	石油や天然ガスなどのパイプラインやウラン濃縮施設などで使用されている制御システムソフトウェアが乗っ取られたり、制御データが搾取される可能性があったことが判明。USB等の外部記録媒体を経由して、オフィスPCにウイルス感染させ、遠隔監視ソフトウェアの脆弱性を悪用し、PLCに悪質なコードを書き込み、制御システム上の装置に対して攻撃を実行した。イランのウラン濃縮施設では、約8,400台の遠心分離機全てが停止しており、これが本ウイルスによるものの疑いもある。

経済産業省「サイバーセキュリティと経済研究会中間とりまとめ」及びIPA報告書より一部抜粋

制御システムのセキュリティに関わる取組みのポイント

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

欧州や米国の制御システムセキュリティについて、四つの視点から調査を行い、日本の制御システムに必要とされる施策について提言。



取組み状況調査結果のまとめ

● 日米欧の取組み状況比較（１／２）

施策	欧州	米国	日本
ガイド・ツール	・推奨される プラクティス集を公開（英国CPNI、オラ ンダNICC/TNO水セクター向け） ・セキュリティ基準を策定（ドイツBSI standard 100-1～4） ・自己評価ツ ールを配布（英国CPNIのSSAT） ・情報共有の仕組みを整備（欧州のE-SCSIE、 英国CPNIのSCSIE、スウェ ーデンSEMAのFIDI-SC）	・推奨される プラクティス集を公開（DHS/CSSP） ・セキュリティ基準を策定中（NISTのSP800-82およびISA のISA99, 100、NERCのCIP002～008） ・自己評価ツ ールを配布（DHS/CSSPのCS2SATおよびその後継のCSET） ・情報共有の仕組みを整備（2008年までPCSF、2009年 よ りICSJWG（HSINサービス 開始））	・「重要インフラにおける情報セキュリティ確保に 係る『安全基準等』策定に当たっての指針」（2007年6月 情報セキュリティ政策会議）などに 基づき分野ごとに安全基準を設定 ・独自のツ ール類は少ない
評価・検証	・ヨーロ ピアンテストベッド取組みの一部 としてIPSCではSCADAテストベッドを 開設しセキュリティ検証を実施	・DOEがSCADAテストベッドを開設しセキュリティ技術の開発、検証を 実施 （INLのNSTBで検証実施）	・電力中央研究所で制御システムセキュリティの 評価・検証を 行っているが、事業者または制御 機器ベン ダー内で共通的に利用可能なセキュリ ティテスト環境は見つからない

取組み状況調査結果のまとめ

● 日米欧の取組み状況比較（2／2）

施策	欧州	米国	日本
データベース	・CPNIが制御システムセキュリティプロ グラ ムのひとつであるSCSIEを運営し ており、イ ンフラ運用者間での脆弱性 情報共有カ ンファレンスを定期的に実 施 ・制御機器ベンダーが脆弱性関連情報 をユーザグループに直 接 通 知 、対 策 し 、ユーザグループ内での解決を図る ・TNOがイ ンシデント情報のデータベー スを 構築	・US-CERTが制御システムの 脆弱性関連情報のデータ ベースを 持つが15～20件と 少数 ・RISIが制御システムのセキュ リティ事象データベースを運 用 ・制御機器ベンダーが脆弱性 関連情報を ユーザグループ に直接 通 知 、対 策 し 、ユ ー ザ グループ内での解決を図る	・JPCERT/CCが制御システムの脆弱性関連情報の収集、公開を実施。但し件数は少ない ・IPAが脆弱性対策情報DB（JVN iPedia）を運用
認証	・TUViTが複数の基準を 顧客要件によ り組み合わせ、制御システムの監査・ 認証を 実施	・ 製品認証機関（米国MuDynamics 社 、カナダWurldtech社）による認証製品を 利用することで、一定のセキュリティレベルが担保さ れている ことを確認、保証可 能（ISCIでの検証サービス）	・現状で特段の取組みは無い

調査分析結果を踏まえて(1/2)

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

● 欧米で脆弱性対策への取組みが拡大中

- ガイド・ツールに関しては、セキュリティ基準の策定、推奨プラクティス集の公開、自己評価ツールの配布を実施
- 評価・検証に関しては、SCADAテストベッドの開設によるセキュリティ検証を実施
- データベースに関しては、制御システムのインシデント情報のデータベース構築・公開を開始
- 認証に関しては、民間主導によるセキュリティ監査・認証サービスが行われており、ISA ISCIによる標準化が進展中
- 制御システムセキュリティ強化に向けた認識向上や関係者間の信頼関係構築により施策の普及を促進させるための、情報共有コミュニティを設置し運用

調査分析結果を踏まえて(2/2)

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

● 日本としても具体的な対策を進める必要性あり

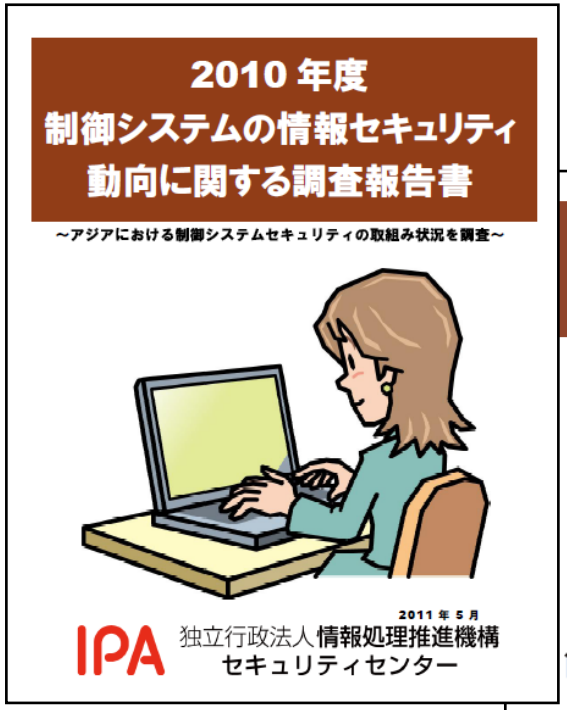
- 日本独自のガイド・ツール類の提供はまだ少なく、テスト環境も一部セクターのみ。脆弱性対策情報（JVN iPediaなど）のデータベースはあるがインシデンツを含む幅広い制御システムセキュリティの情報収集はこれから
- 制御システムのセキュリティ対策のあり方は日本と欧米とで必ずしも同一ではなく、日本の重要インフラにとっての優先度を判別した上で、最も効果のある課題から始めていくことが必要
- セキュリティ規格標準化の動向に関しては、産業の国際競争力強化の観点からも日本独自の規格ではなく、国際標準への対応を念頭に推進することが重要
- 欧米での制御システムセキュリティへの取組みも、まさに現在進行形であり、今後の動向を注視しながらアジアの展開も視野に幅広く対応
- 制御システムセキュリティの脆弱性対策においては、関係者の認識改善と対策の実効性向上の観点からも、官民連携による情報共有の仕組みづくりが鍵

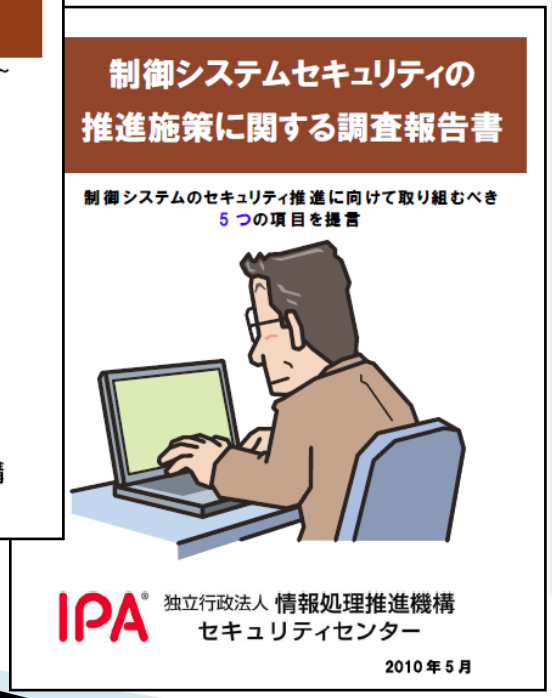
<制御システムセキュリティ>
制御システムセキュリティの状況

IPAの調査報告書

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

- 2010年度：アジアにおける制御システムセキュリティの取組み状況を調査
  http://www.ipa.go.jp/security/fy22/reports/ics_sec/index.html
- 2009年度：制御システムセキュリティの推進施策に関する調査報告書
  http://www.ipa.go.jp/security/fy21/reports/ics_sec/index.html





＜主なトピック＞

制御システムのセキュリティに係る現状
制御システムのインシデントの動向
具体的なインシデント例
その他の動向
米国における取組み
欧州における取組み
アジア各国における取組み
日本における取組み
スマートメータ周辺の制御システムの動向
スマートメータ周辺の制御システム
スマートメータ及び連携する構成要素
スマートハウスにおけるセキュリティ

制御システムセキュリティ
～経済産業省の国策とIPAの活動～

「サイバーセキュリティと経済研究会」での検討と制御システムセキュリティ検討タスクフォースの設置

サイバーセキュリティと経済研究会

(経済産業省)

＜概要＞

サイバー攻撃により、知的財産やライフラインを狙った事案や企業等の機密漏えいが多発している状況　から、ITの安全確保によって守るべき対象が経済活動や国民生活に直接関わる分野へ質的に変化して　いることを鑑み、経済の成長・安全保障の観点から、必要な情報セキュリティ政策を検討。

◇主な検討項目

- 標的型サイバー攻撃への対応
- **制御システムの安全性確保**
- 情報セキュリティ人材の育成

制御システムセキュリティ検討タスクフォース(経済産業省)

＜概要＞

左記研究会の検討に基づき、主に以下の2点における制御システムセキュリティについての施策の実施検討。

◇日本国内のICSセキュリティ確保
◇ICSの海外輸出のための評価認証

＜タスクフォースに配置するWG＞

- **標準化WG (IPA)**
- **評価・認証制度WG (IPA)**
- インシデントハンドリングWG
- テストベッドWG
- 人材育成WG
- 普及啓発WG

ICS：Industrial Control Systems

＜制御システム情報セキュリティ委員会＞『標準化WG、評価・認証制度WGについて』

経済産業省「サイバーセキュリティと経済研究会」での言及により、発足

経済産業省

制御システムセキュリティ検討TF（TaskForce）

ステアリングコミッティ

- インシデントハンドリングWG
- テストベッド検討WG
- 人材育成WG
- 普及啓発WG

①WGからTFへの原案の提案
②TFによるWG原案の承認

IPA 制御システム情報セキュリティ委員会

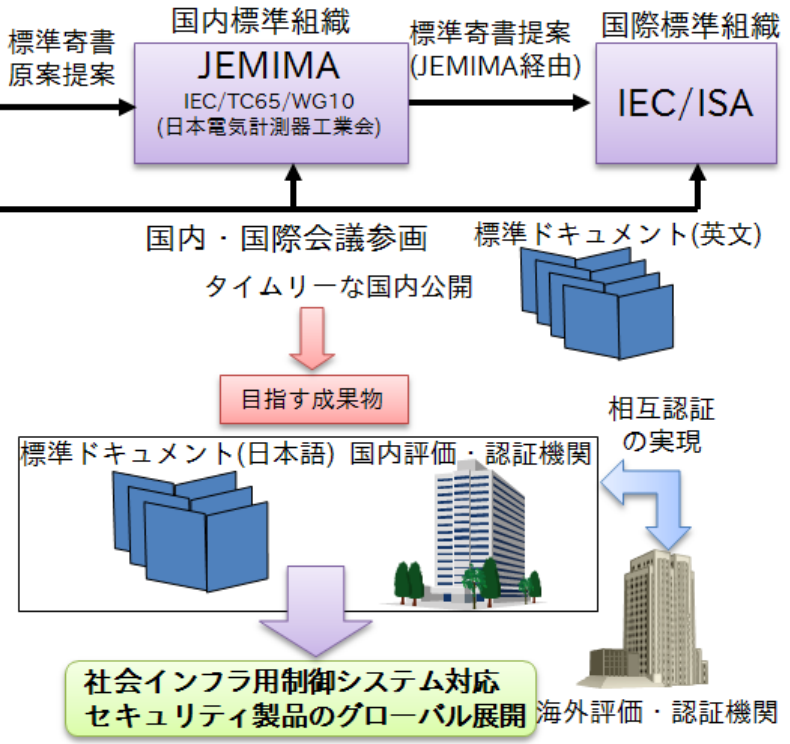
- 標準化WG
- 評価・認証制度WG

活動期間：2011/9-2012/11

本委員会の活動の活動内容

1)標準化WG
- 国際標準へ国内意見提案と国内へ国際標準の普及・展開
  対象標準規格：IEC62443 産業用制御システムセキュリティ
  IECにおける各規格の標準化状況に応じ、コメント案等を寄書

2)評価・認証WG
- 欧米で先行している評価・認証サービススキームの調査・検討
  主な調査対象：ISA/ISCI制御システム評価・認証スキーム(EDSA)
- 日本国内における評価・認証スキームの仕組みについて検討



JEMIMA:Japan Electric Measuring Instruments Manufacturers' Association
IEC:International Electrotechnical Commission
ISA:International Society of Automation
ISCI:ISA Security Compliance Institute
EDSA: Embedded Device Security Assurance

制御システムセキュリティ
～標準規格：IEC62443のご紹介～

IEC62443全体概要と規格化状況

<＜制御システムセキュリティ＞
IEC62443のご紹介>

制御システム分野における標準と認証、評価の位置づけ

標準化 *1)

事業者

インテグレータ

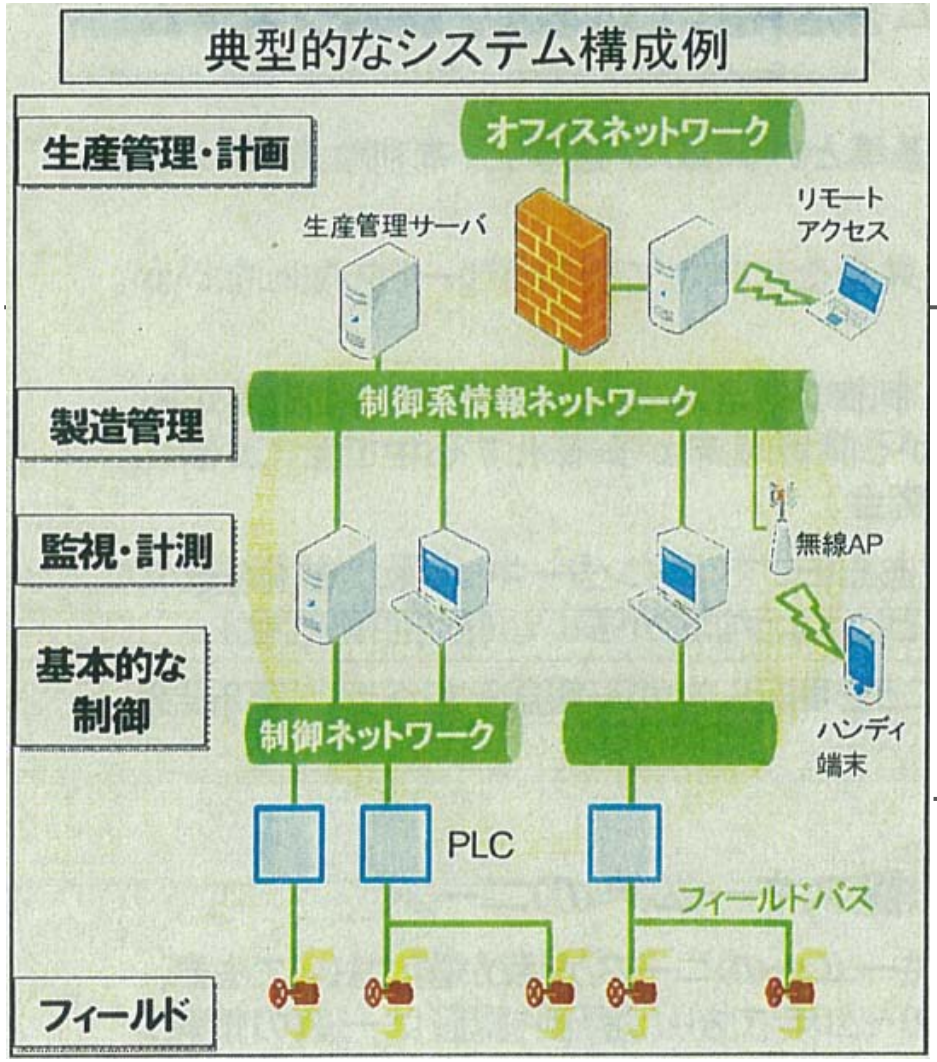
装置ベンダ

IEC62443-1

IEC62443-2
管理・運用・ﾌﾟﾛｾｽ

IEC62443-3
技術・システム

IEC62443-4
ｺﾝﾎﾟｰﾈﾝﾄ・ﾃﾞﾊﾞｲｽ



認証・評価

・WIB*2)
＜Wurldtec＞

＜評価事業者＞
・ISCI:ISASecure*3)
＜exida＞
・Wurldtec Achilles*4)
＜Wurldtec＞

*1) IEC62443のCyber securityの標準化作業は、IEC/TC65/WG10が担当。日本では、JEMIMAが対応（幹事：Yokogawa）。
*2) International Instrument User's Associations, 認証はWurldtech Achilles認証。IEC62443-2-4に取り込み。
*3) EDSA(Embedded Device Security Assurance) certification。ISA99標準仕様。IEC62443-4-1に相当。
*4) ﾈｯﾄﾜｰｸ接続装置（ｺﾝﾄﾛｰﾗ等）の信頼性認証（ﾍﾟﾈﾄﾚｰｼｮﾝ、ﾌｧｼﾞﾝｸﾞﾃｽﾄ）。調達要件に指定されている。

<＜制御システムセキュリティ＞
IEC62443のご紹介

IEC62443規格化の状況

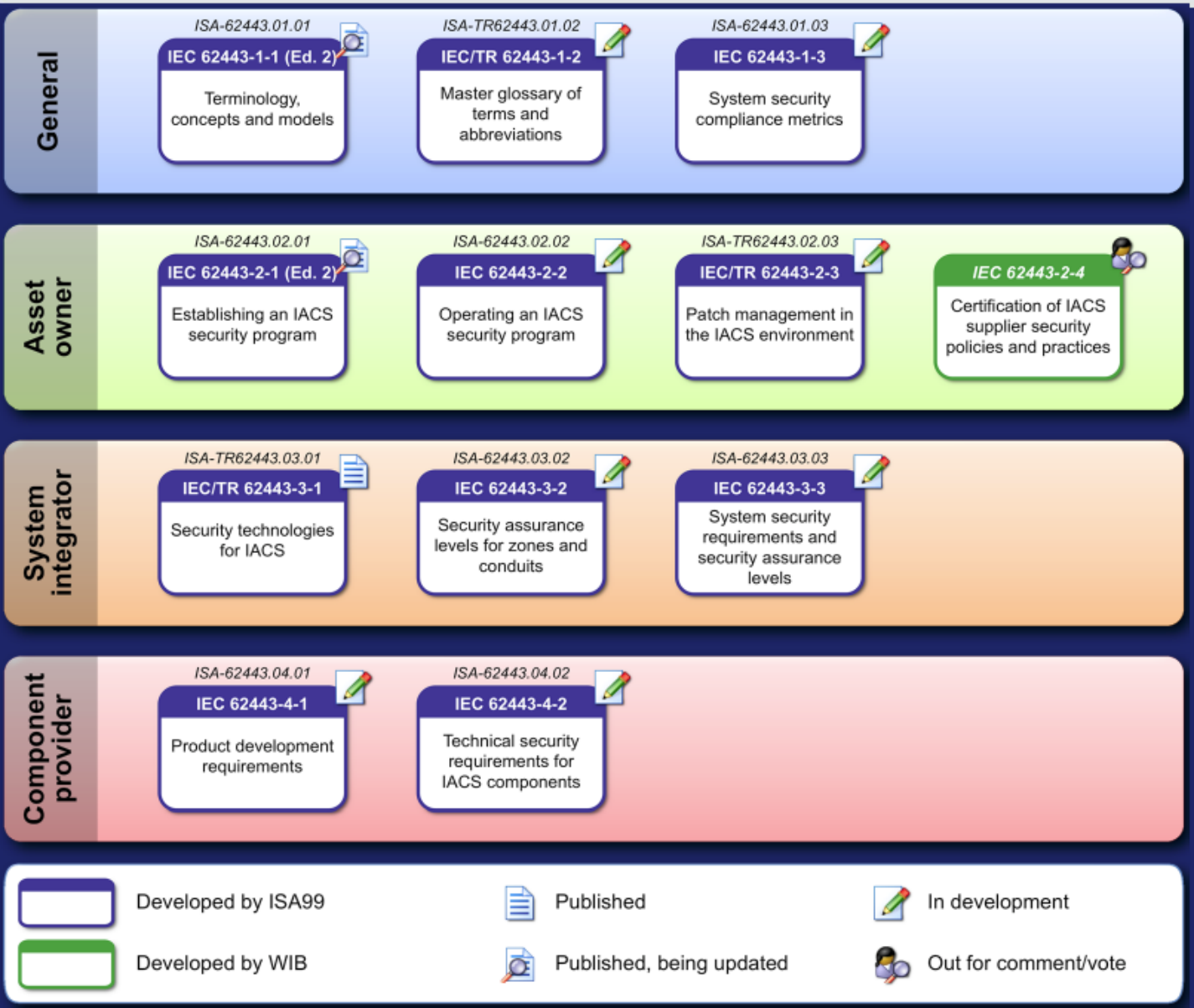
(2011年11月現在)

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

区分	主対象者	IEC	原本名及び概要	現状のステータス ドキュメントの状況，ドラフトの現状	現状のステータス 2012のTC65's Plenary meetingにDC提示予想	リリース予定 発行済み，DTR，Edition2など	詳細	評価認証機関 規格を利用した認証者
共通	全体	62443-1-1	Terminology, concepts and models ＜ｾｷｭﾘﾃｨ概念、Scadaﾓﾃﾞﾙｰ般論、本標準の用語統一と導入部分で認証に関わらない。＞	発行済み，アップデート中RR作成中	（済）	2009.07 Ed.2：1CDは21011Q4	・セキュリティ概念（目的、基本要件、体系、リスク分析、ポリシー、経路、ｿｰﾆﾝｸﾞ、ｾｷｭﾘﾃｨﾚﾍﾞﾙ、ﾗｲﾌｻｲｸﾙ） ・参照ﾓﾃﾞﾙ(5階層)、資産ﾓﾃﾞﾙ(参照ｱｰｷﾃｸﾁｬ)、ｿﾞｰﾝ&経路ﾓﾃﾞﾙ	認証対象外
		62443-1-2	master glossary of terms and abbreviations	テクニカルレポートとしてレビュー中	○	1DC：2012Q1 DTR：2012Q3		
		62443-1-3	System security compliance metrics	ドラフト執筆中	○	1DC：2011Q4 DTR：2013.02		
セキュリティプログラム	事業・運用者	62443-2-1	Establishing an IACS security program ＜事業者自体のｾｷｭﾘﾃｨﾏﾈｰｼﾞﾒﾝﾄｼｽﾃﾑ構築＞	発行済み，アップデート中、RR作成中	（済）	2010.10 Ed.2：CDVは2012Q4	CSMS（Cyber Security Management System）、ISMS（ISO27001）ICS版 ・リスク解析、リスク対応（ﾎﾟﾘｼｰ、組織、対策、実装）、ﾓﾆﾀﾘﾝｸﾞと改善 ・127要件（ISO17799：128、ISO27001：132） ・本文（38P），補足資料（121p）、ISO27001との対応表 ISMSと類似の認証は可能だが、ISMS認証の普及は日本が主。	
		62443-2-2	Operating an IACS security program	ドラフト執筆中	○	1DC：2012Q2 CDV：2013Q1		
		62443-2-3	Patch management in the IACS environment	ドラフト執筆中	○	1DC：2012Q4 DTR：2112Q3		
		62443-2-4	Certification of IACS supplier security policies and practices ＜事業者が制御システムのコンポーネントやシステムを調達する際のセキュリティ要件集＞	(9/19-22)IEC/TC65/WG10： 現CDへのコメントを受け、改訂案議論、2012.2調整予定。	（ほぼ済）	CD：2011.04 CDV：2011.10 ＜目標＞ ・2012.5 最終版CD予定	要件レベルが3段階（金、銀、銅）で構成。 製品のセキュリティ要件を、下記4層で明示的に既定 ・製造組織要件（3分類：10項目） ・セキュリティ機能要件（12分類：44項目） ・受入テスト要件（10分類：40項目） ・メンテ/保守要件（10分類：36項目） ・ISO/IEC 27002をベースとしているとの記載有。	（WIB：Wurldtech、exida）
技術・システム	SIer	62443-3-1	Security technologies for IACS ＜セキュリティ技術解説書で認証対象でない＞	発行済み RR作成中	（済）	2009.07	認証、ﾌｨﾙﾀﾘﾝｸﾞ/ﾌﾞﾛｯｷﾝｸﾞ/ｱｸｾｽ制御（FW，IDS、VLAN）、暗号/ﾃﾞｰﾀ保護、管理・監査・証跡、ｿﾌﾄ管理（脆弱性対応含）、物理ｾｷｭﾘﾃｨ、人的ｾｷｭﾘﾃｨ	認証対象外
		62443-3-2	Security assurance levels for zones and conduits	ドラフト執筆中	○	1DC：2012Q2 CDV：2013.02		
		62443-3-3	System security requirements and security assurance levels	ドラフトが75%完成済み	（ほぼ済）	1DC：2011.10 CDV：2012Q1		
部品	ベンダ	62443-4-1	prodauct development requirements	ドラフト執筆中	○	1DC：2012Q2 CDV：2013Q1	セキュアなコンポーネントを開発するための方法を規定。 ISASecureのEDSA（SDSA）をベースにしている。	（EDSA:exida） Wurldtech
		62443-4-2	technical security requirements for IACS components	ドラフト執筆中	○	1DC：2012Q1 CDV：2013Q1	デバイス、システムに搭載されるセキュリティ機能を規定。 ISASecureのEDSA（FSA）をベースにしている。	（EDSA:exida） Wurldtech

IEC: International Electrotechnical Commision　CD：Committee Draft 、CDV：Committee Draft for Vote、DC：Document for Comments　ISA: International Society of Automation
IACS: industrial Automation and Control Systems　DTR: Draft Technical Report 、NP：New Work Item Proposal 、RR:Review Report　WIB: international instrument User's Associations

IEC 62443, Security for industrial automation and control systems – Network and system security

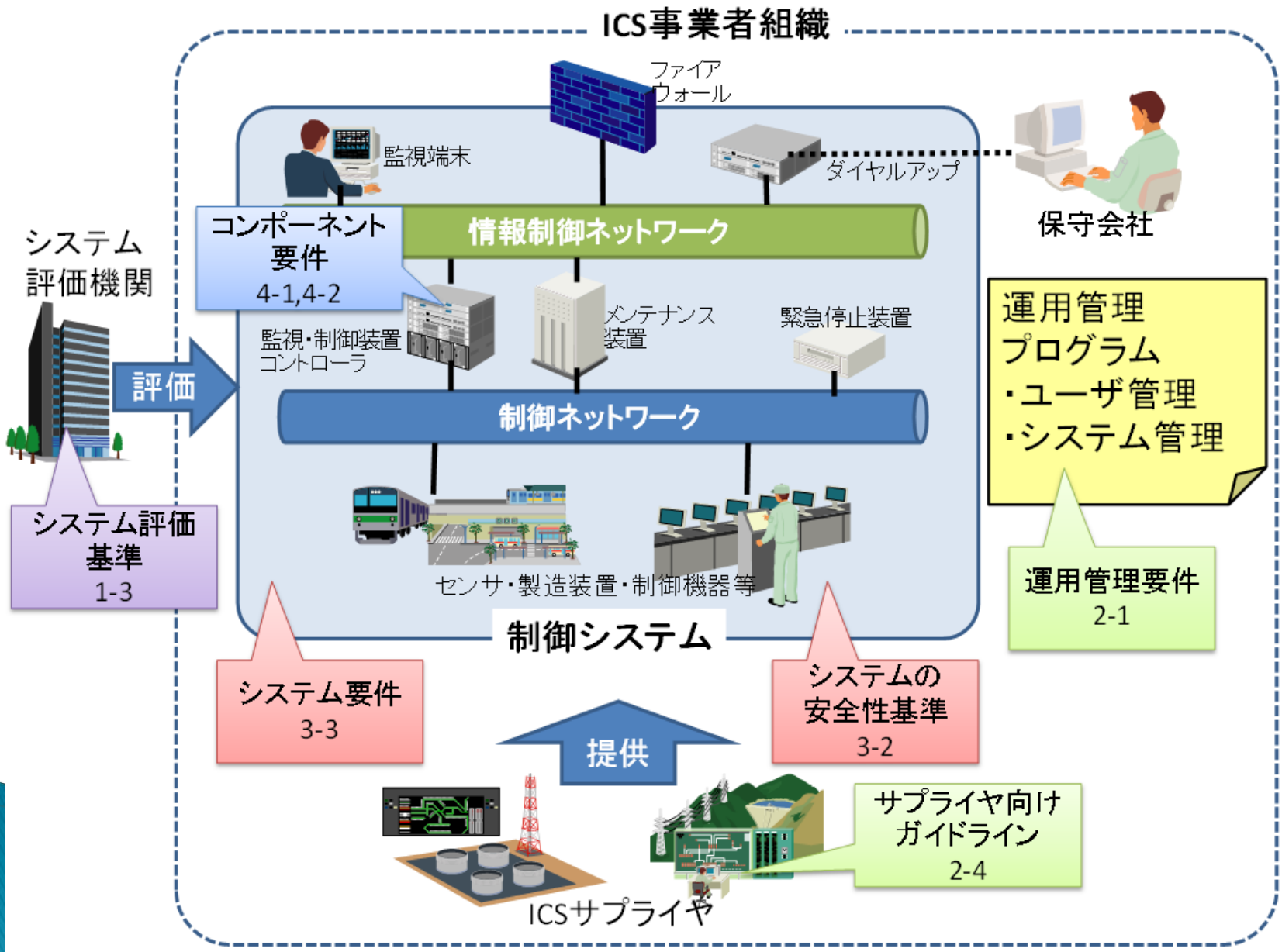


The IEC 62443 standards form four sub-series, aligned with the three previously identified classes of users.

The 1st sub-series provides general information relevant to the other three subseries.

※International Electrotechnical Commission

IEC62443の規格のマッピング



IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

制御システムセキュリティ
～ IEC62443のご紹介～

IEC62443-2-1の概要

IEC62443-2-1の概要
Establishing an IACS* security program

*IACS: Industrial Automation and Control Systems

- 概要

◇CSMS（Cyber Security Management System)と呼称
ISMS（ISO27001）のIACS版と考えられ、ほぼ同様の要求事項。

- CSMSの要件：全127要件

◇リスク分析(Risk analysis)
・リスクの識別、分類、評価等の要件

◇リスク対応(Addressing risk with the CSMS)
・セキュリティ基本方針、組織、対策、実装に関する要件

◇モニタリングと改善(Monitoring and improving the CSMS)
・適合性(監査実施)、監査結果評価による改善・維持等の要件

リスク分析(Risk analysis)

- Risk identification, classification and assessment

◇リスク識別、分類、及び評価

・リスク評価方法を選択
・IACSの識別
・IACSの全ライフサイクルでリスク評価
・リスク評価の文書化
・脆弱性評価記録の維持

リスク対応 (Addressing risk with the CSMS)

- Security policy, organization, and awareness
  ◇CSMSの対象範囲の定義
  ◇管理層を含むセキュリティ組織の確立・責任の定義
  ◇スタッフのトレーニングとセキュリティ認識
  ◇Business continuity plan(回復対象、チーム等)
  ◇セキュリティポリシーと手順
- Selected security countermeasures
  ◇要員や物理的環境的セキュリティ、アカウント制御
- Implementation
  ◇リスク管理と実行、システム開発とメンテナンス
- ◇情報・文書管理、インシデント対応計画

モニタリングと改善
(Monitoring and improving the CSMS)

- 適合性評価（Conformance）
  - ・監査プロセスの規定
  - ・定期的なIACS監査を実施
  - ・適合性測定法を確立
  - ・不適合時の罰則の定義
  - ・監査人の能力を保証
- CSMSのレビュー・維持改善
  - ・CSMSの管理、実行組織の割り当て
  - ・定期的なCSMS評価
  - ・業界のCSMS戦略を監視、評価

ISMSとCSMSの主な相違点

項　目		ISMS	CSMS
要員のトレーニング	トレーニング計画策定	○	○
	トレーニングの実施	○	○
	トレーニング結果の維持	○	○
	計画の妥当性の証明	△	○
	トレーニング計画の改善	△	○
内部監査	監査プロセスの規定	○	○
	監査人の能力保証	○	○
	不適合時の罰則	△	○

○：shall、△：should

制御システムセキュリティ
～ IEC62443のご紹介～

IEC62443-3-3の概要

IEC62443-3-3(案)の概要 System security requirements and security assurance levels

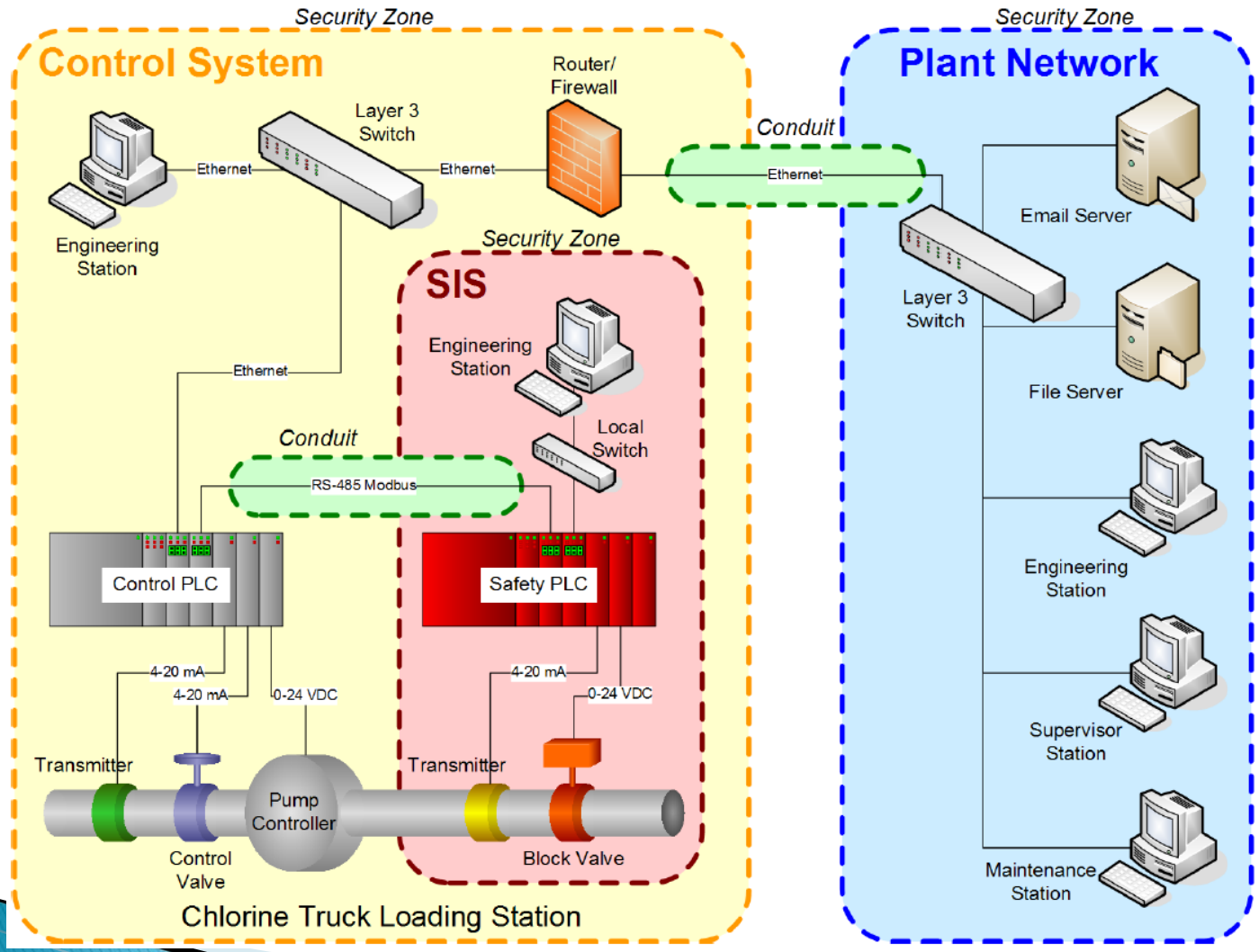
- 概要

◇扱う人、プロセス、デバイスの識別・認証、
及びそれらのアクセス制御(証跡記録)の要件を規定。
扱うデータの完全性・機密性、資源の可用性等の要件も含む。
◇7種の要件に4段階のセキュリティ保証レベルSAL(Security assurance levels)を規程。

- システムセキュリティ要件について：全94要件(7種の大項目)

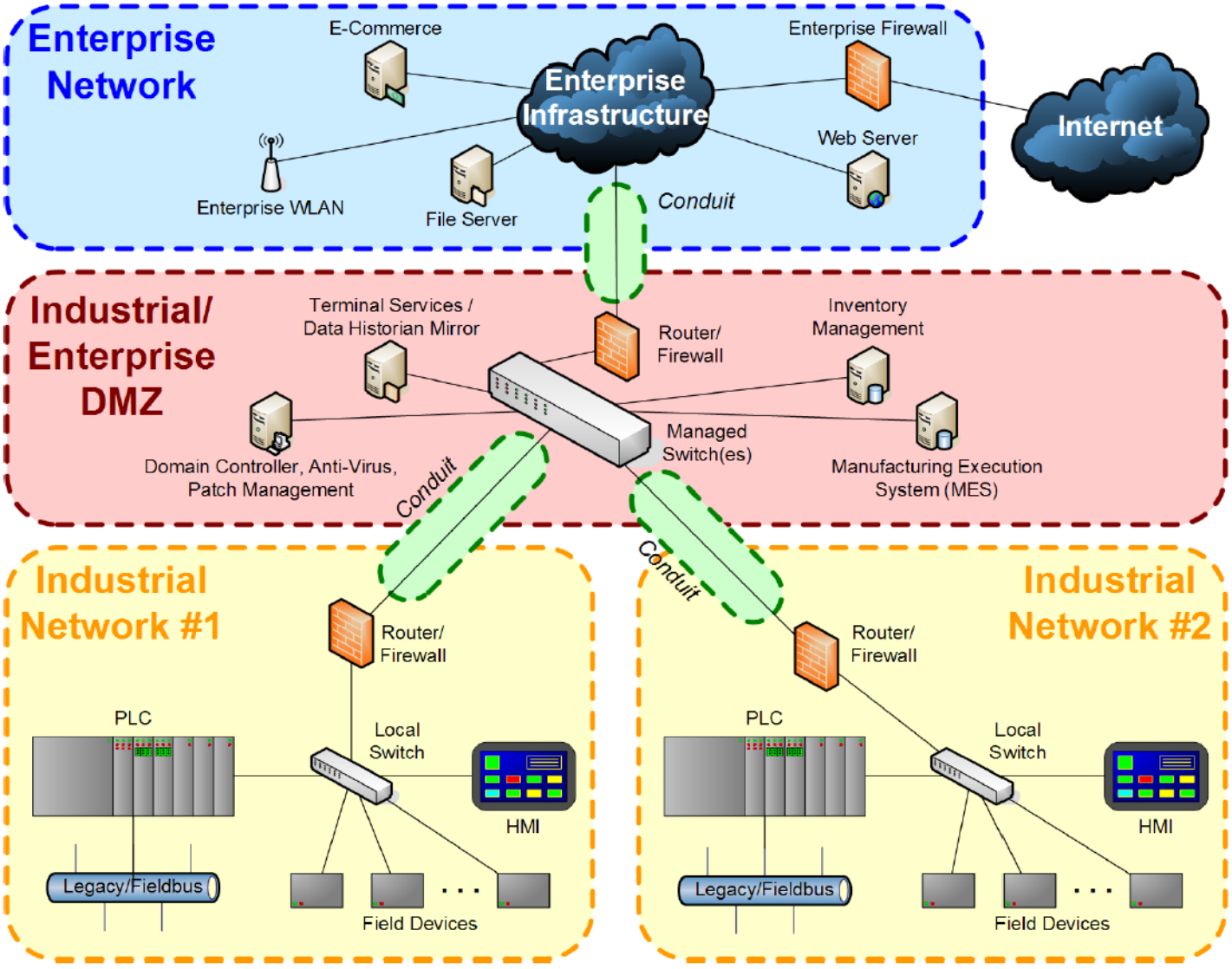
◇識別及び認証(Identification and authentication control)
・人、プロセス、デバイスの認証、パスワード強度等の要件
◇利用制御(Use control)
・適切な権限付与、証跡記録、ワイヤレスアクセス制御
◇データの完全性・機密性、資源の可用性要件
・通信完全性、暗号の利用、DoS対策やバックアップ等の要件

産業システムの構成


Security Zone
Control System
Router/
Firewall
Layer 3
Switch
Ethernet
Ethernet
Engineering
Station
Security Zone
SIS
Engineering
Station
Local
Switch
Ethernet
Conduit
RS-485 Modbus
Control PLC
Safety PLC
4-20 mA
4-20 mA
0-24 VDC
4-20 mA
0-24 VDC
Transmitter
Transmitter
Pump
Controller
Control
Valve
Block Valve
Chlorine Truck Loading Station
Conduit
Ethernet
Security Zone
Plant Network
Email Server
Layer 3
Switch
File Server
Engineering
Station
Supervisor
Station
Maintenance
Station

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

製造システム階層



識別及び認証
(Identification and authentication control)

- 人、プロセス、デバイスの認証
- アカウント管理
- パスワード認証の強度
- 公開鍵認証の強度
- デバイス認証

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

利用制御
(Use control)

- 適切な権限付与
- ワイヤレスアクセス制限
- 監査可能なイベント
- タイムスタンプ
- 監査情報の保護
- 否認防止

データの完全性・機密性、資源の可用性要件

- データの完全性
  - ◇通信完全性
  - ◇セキュリティ機能の検証
  - ◇入力正当化
  - ◇セッション完全性
- データの機密性
  - ◇情報永続性
  - ◇情報機密性
  - ◇暗号の使用
- 資源の可用性
  - ◇サービス妨害攻撃からの保護
  - ◇バックアップ
  - ◇回復と再構成

制御システムセキュリティ
～ 評価・認証の動向について～

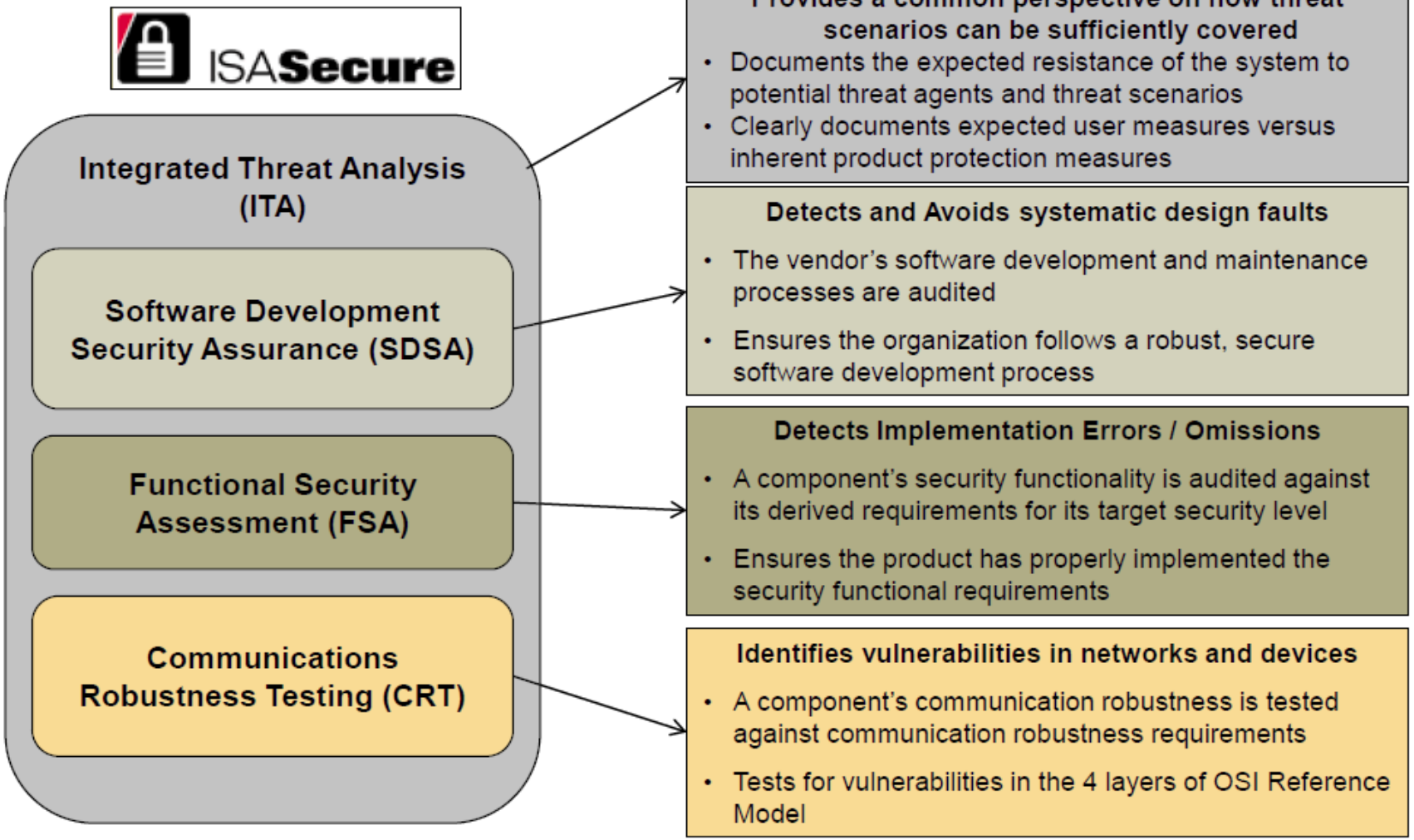
1. 制御システムの評価・認証に関する動向

IPA INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

- 現在は民間組織が主体の認証スキームが主流
  - 規格準拠評価型
    - ドイツTUViT社
      - Trusted Site Security SCADA Infrastructure
    - オランダWIB(International Instrument Users' Association)
  - ツール提供型
    - カナダWurldtech社
      - Achilles
    - アメリカMu Dynamics社
      - MUSIC(Mu Secure Industrial Control)　※現在は行われていない
- ISAが主体の認証スキームが登場
  - ISCI(ISA Security Compliance Institute)
    - ISASecure認証：EDSA(Embedded Device Security Assurance)

**国際標準(IEC62443)への組込みが見込まれており、
認証のスキームも綿密に組み立てられているため、
今後拡大してゆく可能性大**

Embedded Device Security Assurance Certification



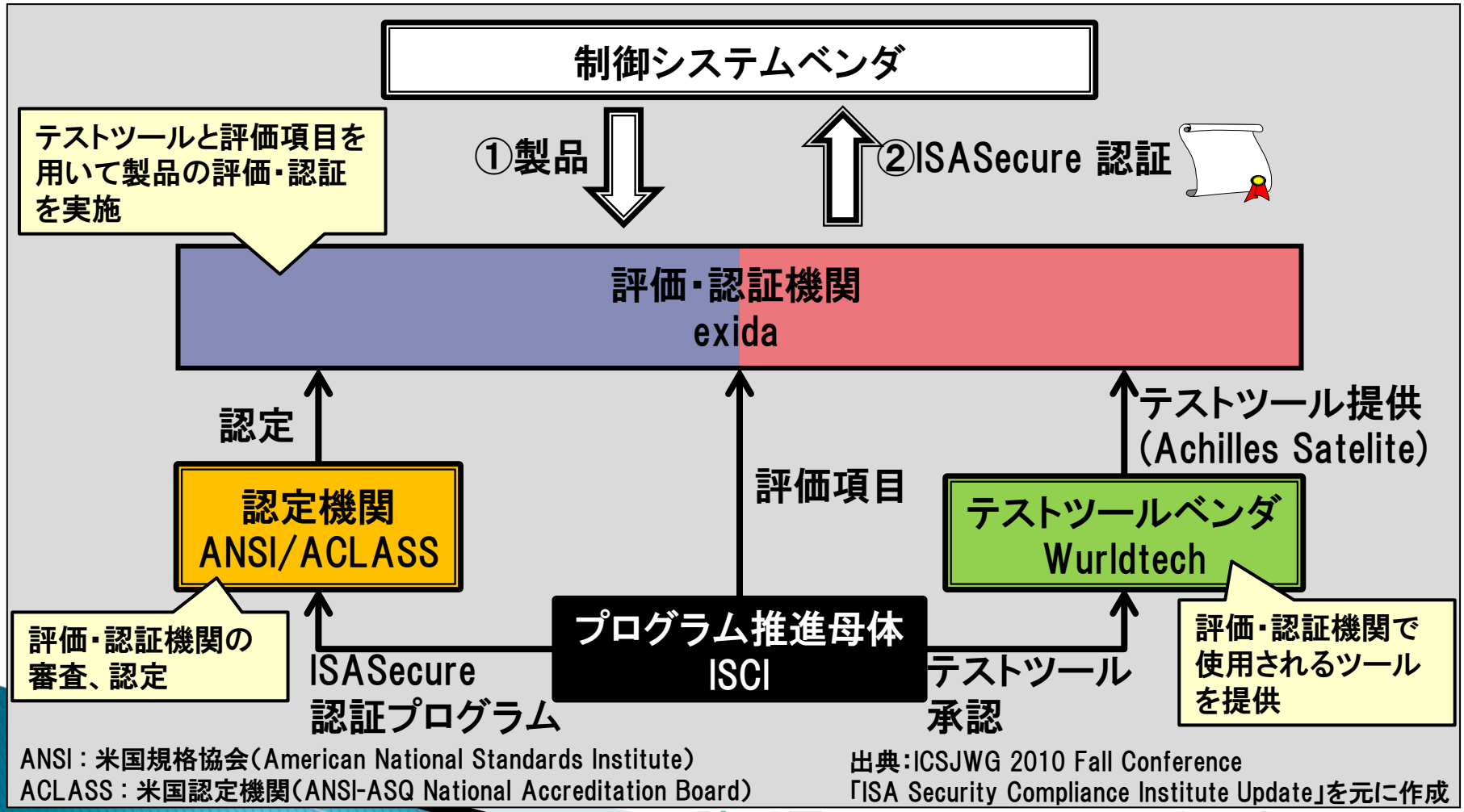
2. ISASecure認証(EDSA)

- コンポーネントの認証
- 3段階での評価
  - CRT(Communication Robustness Testing)
    - 通信レベルでの評価
  - FSA(Functional Security Assessment)
    - セキュリティ機能評価
  - SDSA(Software Development Security Assessment)
    - ソフト開発プロセス評価
- 評価項目の数によって3段階の認証レベルを規定
- Honeywell, RTP Corporationが認証を取得済

()内は要件数

3. ISASecure認証プログラム

■評価・認証機関：製品を評価し，ISASecure認証を発行する機関
■認定機関：評価・認証機関を審査し，認定する機関
■テストツールベンダ：評価・認証機関で使用されるツールを提供する企業

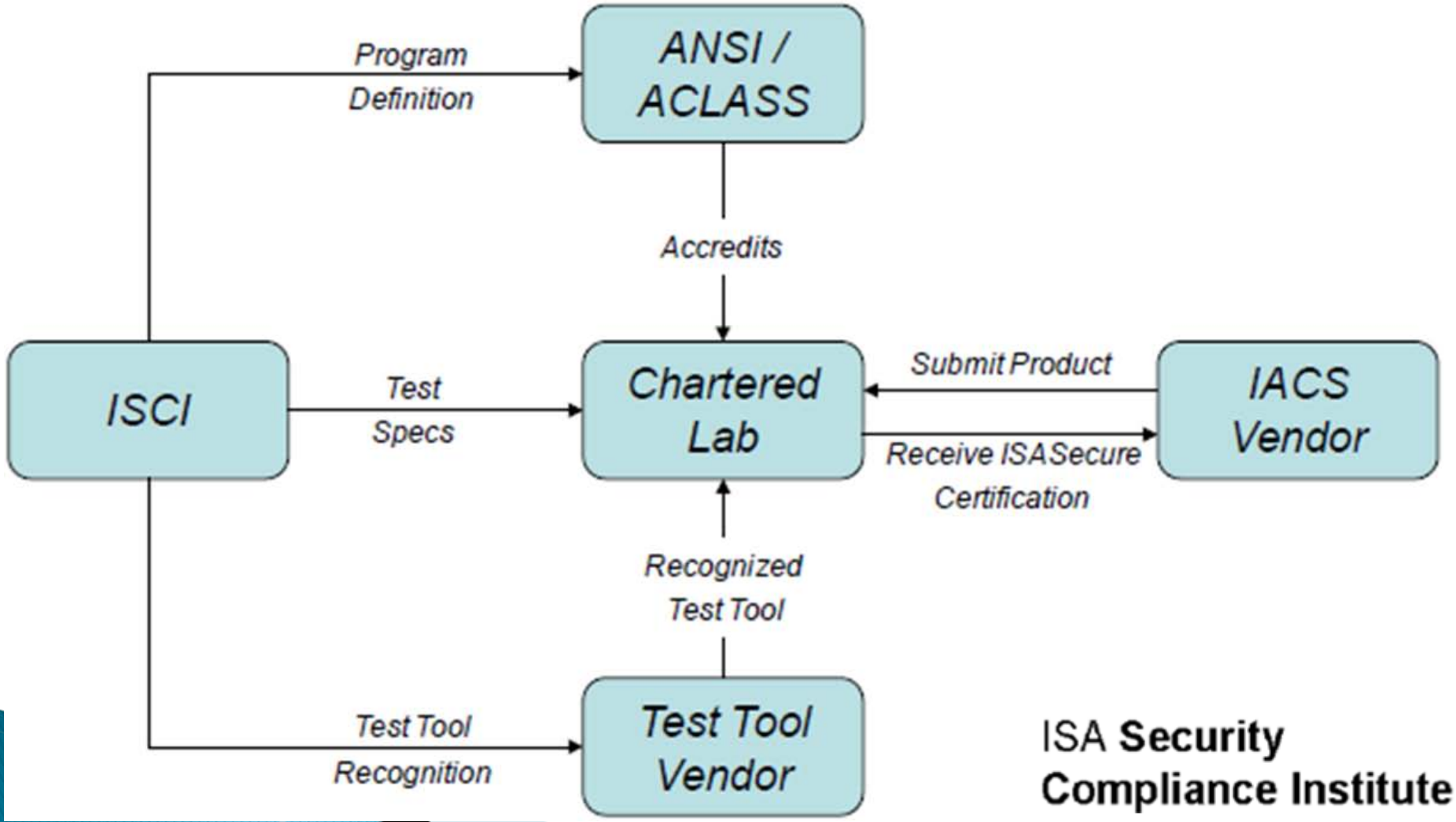


ANSI：米国規格協会(American National Standards Institute)
ACLASS：米国認定機関(ANSI-ASQ National Accreditation Board)

出典:ICSJWG 2010 Fall Conference
「ISA Security Compliance Institute Update」を元に作成

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

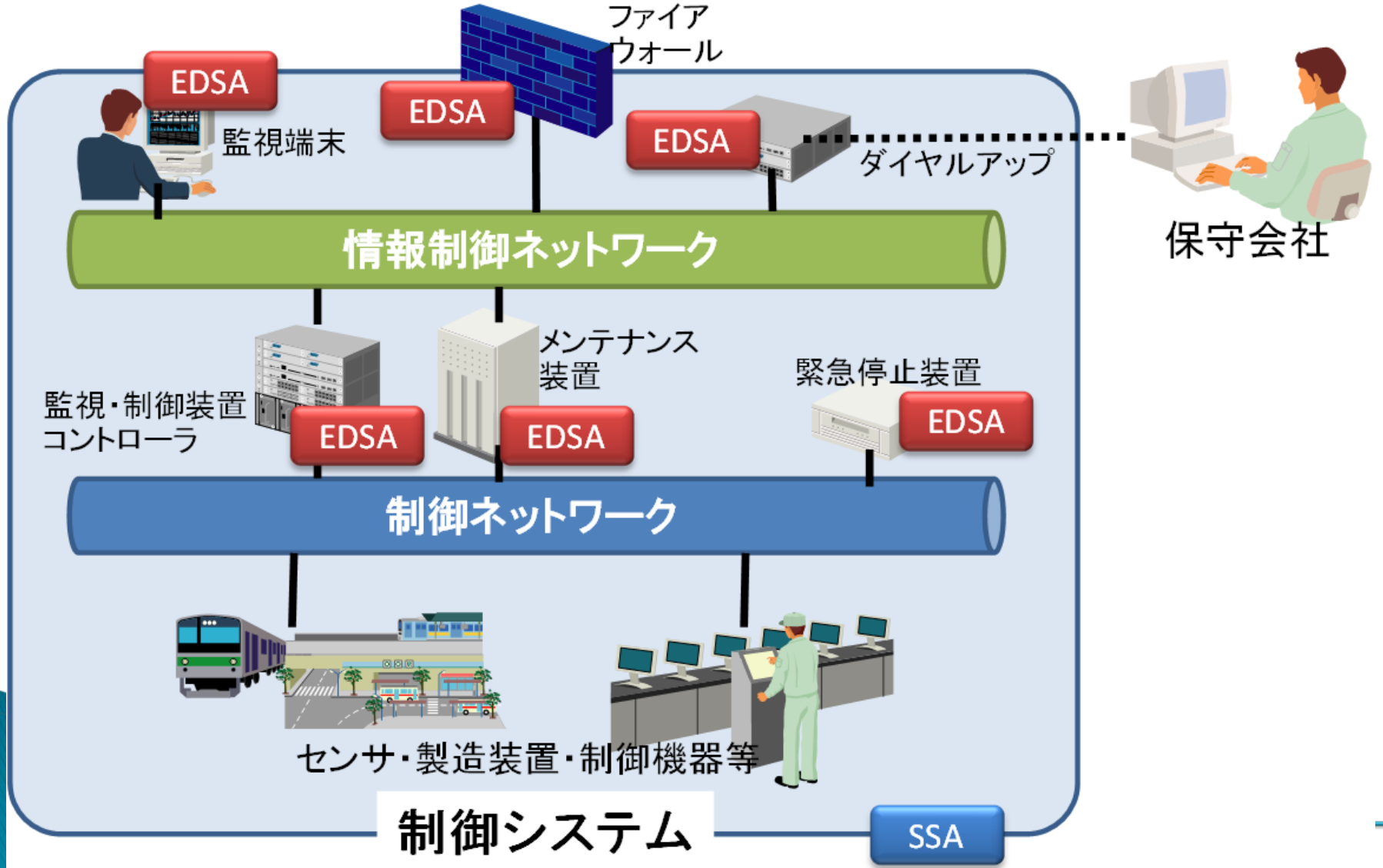
ISASecure認証の体制



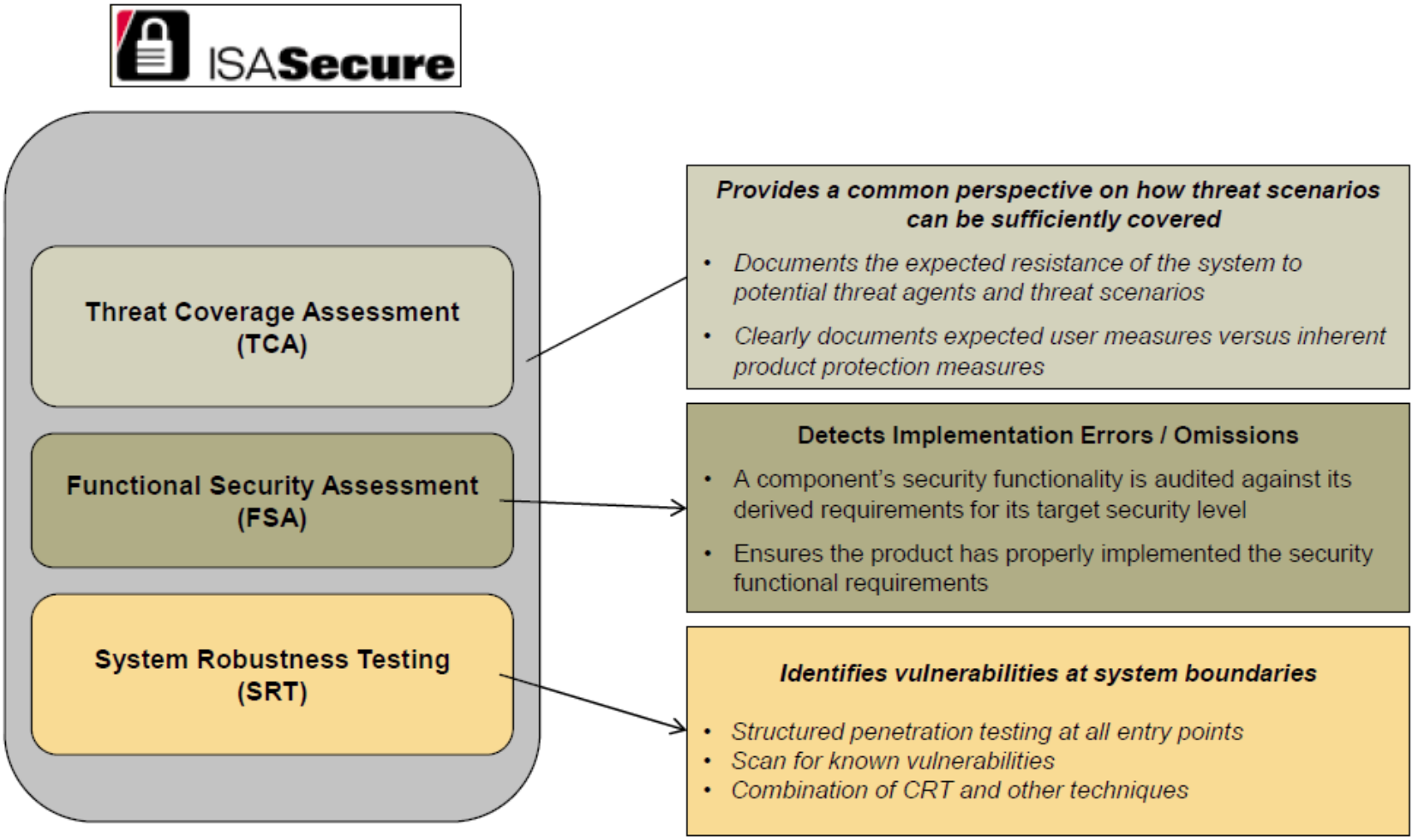
ISA Security
Compliance Institute

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

SSA
(System Security Assessment)



ISASecure System Security Assurance (*SSA*) Certification



ご清聴ありがとうございました！

本発表の中に引用した報告書はIPAのWebサイトでダウンロードする事ができますので、ご活用下さい。
http://www.ipa.go.jp/security/index.html

Contact：
IPA（独立行政法人 情報処理推進機構）
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー
TEL 03（5978）7527
FAX 03（5978）7518
電子メール　vuln-inq@ipa.go.jp