JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

生産制御システムのセキュリティ

2009.11.18

PA･FA計測制御委員会

セキュリティ調査研究WG

社団法人 日本電気計測器工業会

WGのご紹介

- 目的:
  製造業分野におけるセキュリティ標準化動向、技術等の調査・研究活動を進め、会員企業、ユーザにフィードバックする。

- 設立:2005年4月
- メンバ

横河電機㈱ 、㈱山武、㈱東芝、富士電機ｼｽﾃﾑｽﾞ㈱
㈱日立ﾊｲﾃｸｺﾝﾄﾛｰﾙｼｽﾃﾑｽﾞ、㈱日立製作所

- 活動実績
  - 研究活動
    1. SP99　TR2を利用したセキュリティ対策の実践
    2. SPP-ICS ver1.0を利用したセキュリティ要件の分析および役割分担の明確化
    3. セキュリティ標準規格の調査
    4. CPNI グッドプラクティスの検討

WGのご紹介

- 広報活動
  - JEMIMA 委員会セミナー
  - 計測展
  - JEITA 制御システムフォーラム
  - SICE Annual Conference
- 団体との協力関係
  - SICE（計測・制御ネットワーク部会）
  - JEITA（制御システム専門委員会）
  - JPCERT/CC
  - IPA（独立行政法人情報処理推進機構）
- その他の活動
  - IEC/TC65/WG10国内委員会にメンバ登録

Agenda

PART1
　生産制御システムセキュリティの現状

PART2
　制御システムのセキュリティ規格化動向

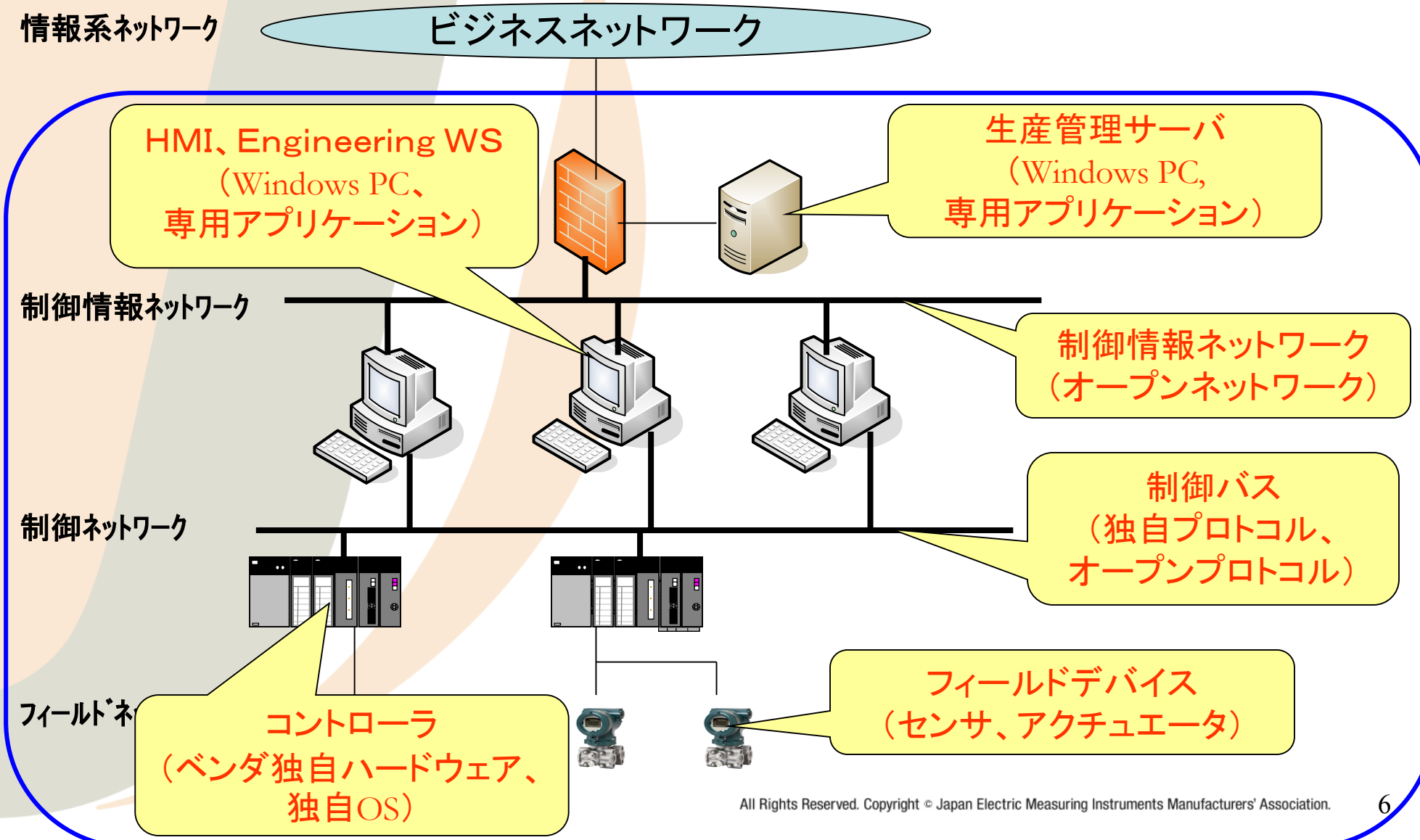
PART3
　グッドプラクティスの検討

PART1
生産制御システムセキュリティの現状

PART2
制御システムのセキュリティ規格化動向

PART3
グッドプラクティスの検討

生産制御システム概要



現実化する脅威

- 生産制御システム（M&CS）のネットワーク化
  - 個々の「島」→　垂直、水平方向へのネットワーク統合。

- 脅威が現実のものになってきている。
  - オーストラリア下水道
    - 元職員による汚水バルブの不正操作
  - オハイオ原発ネットワークダウン
    - ウイルスに感染したことによる
      ネットワーク停止

セキュリティへの脅威

- 第三者の悪意の行為に生じる現象

セキュリティの確保には下記3つの条件がある。

①機密性

ネットワーク上やコンピュータ内の情報を不適切な人間には決して見せないようにすること

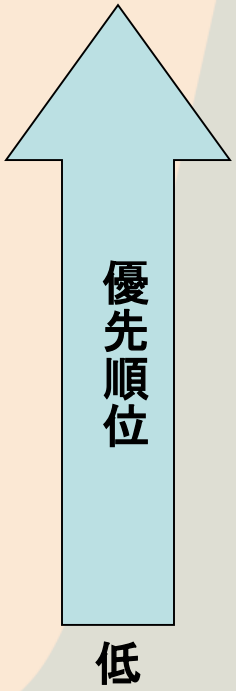
②完全性

ネットワーク上のコンピュータ内の情報が完全な形で保たれ、不正によって改ざんされたり破壊されないこと

③可用性

ネットワーク上のコンピュータ内の情報や資源がいつでも利用できること

セキュリティへの脅威



ITシステム

- **機密性**
- 完全性
- 可用性

●情報の保護が優先

生産制御システム

- **可用性**
- 完全性
- 機密性

●生産の継続が優先

M&CSセキュリティの課題

1. セキュリティパッチ適用時の脅威

Windowsなどの汎用OSや汎用ミドルウェア（データベースなど）を適用している制御システムの課題

1. パッチ適用時にウイルスが混入
2. パッチ適用によるソフトウェアレスポンスの低下、システム停止
3. 古いバージョンのOS等のセキュリティパッチ提供の停止
   （サポート期間が短い）

2. リムーバブルメディア利用による脅威

USBメモリやCD－R、DVD－Rなどのリムーバブルメディアの普及により、管理コンソールやオペレータコンソール（HMI）でメディアを利用する場合の課題

1. メディアからのウイルス感染
2. メディアを紛失することによる機密情報漏洩

M&CSセキュリティの課題

3. リモートメンテナンス時の脅威

インターネット回線等を利用するリモート監視システムの増加により、システム外部のコールセンターやリモート保守機器から保守を行う場合の脅威。

1. インターネット回線からの攻撃やウイルス感染

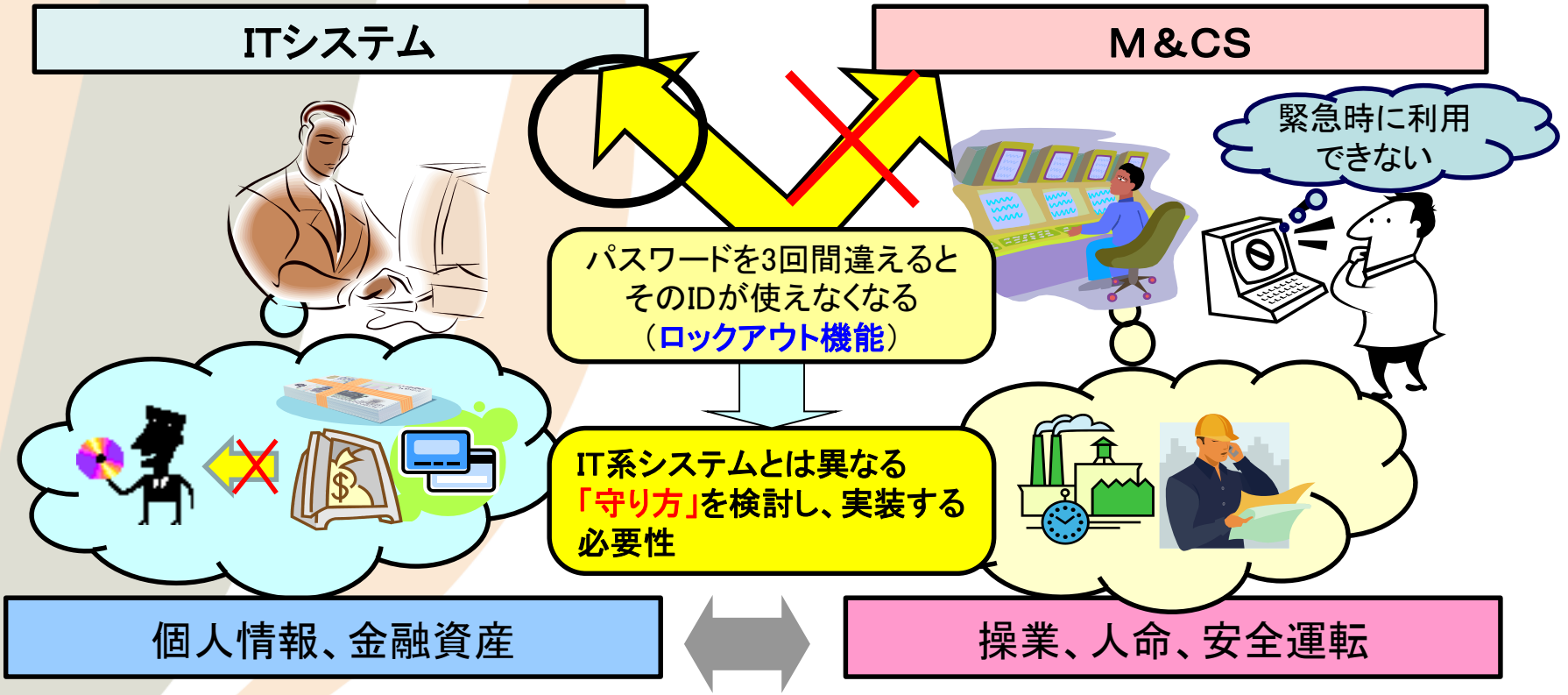
4. メンテナンス用機器など、新たな機器の接続による脅威

機器の増設やメンテナンス目的でシステム設計時に計画していなかった新たな機器を制御システムに接続するときに発生する脅威

1. 機器からのウイルス感染
2. 機器接続によるシステム構成異常

ITセキュリティとM&CSセキュリティ

● ユーザ認証

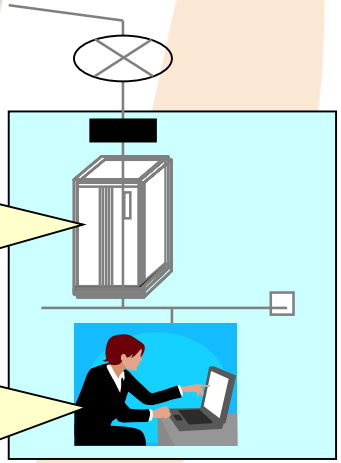


守るべき資産の違い

ITセキュリティとM&CSセキュリティ

●ウイルス対策

ITシステム

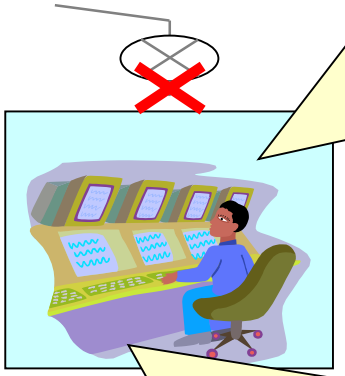


インターネットやイントラネットのパターン更新サーバと接続されている

ウイルス対策、管理されている保守用PCからネットワークを使用して保守を実施

常に高いセキュリティ対策レベルでの運用が可能

M&CS



孤立したネットワーク環境であるため、パターン更新などのセキュリティ対策は保守メンテ時にオフラインで実施。

（リアルタイムに最新パターンへ更新できない）

パッチ適用やモジュール更新は、USBメモリなどを利用してオフラインで実施する。

（紛失、ウイルス混入の危険性）

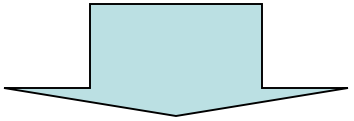
最新パターンで対策がされていない状態でのリムーバブル利用など、運用上考慮すべき課題が多い

ITセキュリティとM&CSセキュリティ

	内　容	IT 系 シ ス テ ム	M&CS シ ス テ ム
1	性能要件	応答性能よりもスループットが要求される。	応答性能が重要。遅延は重大問題。
2	可用性	運用上必要であればシステムの再起動が許容。	システムの再起動は許されない場合が多い。
3	即時性	即時性を要求する緊急処置は少ない。	緊急処置に対する人間の操作を妨げてはならない。
4	ライフタイム	システム、機器のライフタイムは3-5年が中心。	15-20年と長い。
5	守るべき資産	IT資産および情報を第一に保護している。	制御に直接関係する端末装置（プロセス制御装置のようなフィールド装置）を第一に保護。
6	システム運用	汎用OSを用いて設計されており、アップデートは自動化された仕組を利用でき容易である。	独自OSが多く、アップデートの自動化の仕組みが出来ていない。
7	リソース（メモリやディスク容量）	セキュリティ対策などのために、システムは十分なリソースを持っていることが一般的である。	最小メモリやその他リソースで生産プロセスを支援するように設計されており、セキュリティ機能もその範囲内で追加されている。
8	通信	ワイヤレスも含め、標準的な通信プロトコルが使用される。	標準プロトコルの他に専用プロトコル、通信設備が含まれるため、ネットワークは複雑となり、専門の技術者が必要。
9	サポート	機器メーカーによる様々な支援体制がある。	サービスサポートは通常1ベンダーによる。
10	危機管理	データ機密性及び完全性を第一に管理する。	人、環境の安全性が第一、次がプロセスの保護である。

セキュリティへの対応

- 制御システムもオープン化が進み、ウイルス感染や外部からの侵入による情報漏洩など、IT系システムと同様の**セキュリティ脅威**にさらされることが多くなっている
- 制御システムは**安全な運転とシステムの継続稼動を最優先**に運用管理しなければならないため、IT系システムと同じセキュリティ対策をそのまま実施することは、システム運用の妨げになる場合がある



制御システムとしてのセキュリティ標準化が必要

PART1
生産制御システムセキュリティの現状

PART2
制御システムのセキュリティ規格化動向

PART3
グッドプラクティスの検討

●制御システムのセキュリティ規格

2つの視点

マネージメント視点

- セキュリティ管理システム仕様
- 最適慣例集
  - 実施例の一覧

コンポーネント視点

- コンポーネントの情報セキュリティ機能評価基盤
  - セキュリティ機能要件定義
  - 評価・認証システムのフレームワーク

ITセキュリティの場合

マネージメント視点

- ISO/IEC 27001 情報セキュリティマネジメントシステム（ISMS）要求事項
- ISO/IEC 27002 ISMS 実践のための規範
- ISO/IEC 27005 情報システムのリスクマネージメント
- ISO/IEC 27006 認証/登録プロセスの要求仕様

以下予定。

- ISO/IEC27000 ISMS規格についての基本用語集
- ISO/IEC27003 ISMS実践ガイド
- ISO/IEC27004 情報セキュリティの測定、27007 ISMS監査の指針、27008、27011等・・・・・・・

コンポーネント視点

- ISO/IEC 15408: Information technology − Security techniques − Evaluation criteria for IT security
  （CC:Common Criteria）

M&CSセキュリティの場合

マネージメント視点

- ISA-99 (M&CSセキュリティ)
- IEC/TC65/WG10

  Industrial Process Measurement and Control – Net & System Security

コンポーネント視点

- PCSRF (Process Control Security Requirements Forum)
  - SPP-ICS

    (System Protection Profile - Industrial Control System)

ISA-99

- 名称
  - “Security for Industrial Automation and Control Systems”
- 目的
  - Manufacturing and Control Systems(以下M&CS)への電子的侵入を防ぐための指針を確立すること
- 参加メンバー
  - システムインテグレータ/コンサルタントが中心にリードしている
  - エンドユーザも参加しており，一部のメンバーはTRの執筆に大きく貢献
  - システムベンダーも一通り参加
- 活動内容
  - TR (Technical Report) を発行(2004年) 2007年改定版発行
    - ISA TR99.00.01: Security Technologies for Manufacturing and Control Systems (TR1)
    - ISA TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment (TR2)

ISA－99（4つのPartで構成）

- Part 1: ANSI/ISA-99.00.01-2007: Terminology, Concepts, and Models
  - 用語やモデルの定義
  - Part 2以下の基礎となる共通の理解をまとめる

- 策定中
  - Part 2: Establishing an Industrial Automation and Control System Security Program
    - M&CS情報セキュリティのビジネスケースを確立
    - 情報セキュリティ管理に必要な活動を挙げ，その詳細を記述
- 策定予定
  - Part 3: Operating an Industrial Automation and Control Systems Security Program
  - Part 4: Specific Security Requirements for Industrial Automation and Control

ISA-99としての主だった活動はなされておらず、IEC 62443（次ページ参照）との統合が進められている。

IEC 62443

- 2009年～2010年度規格化決定(2008年5月のTC65東京会議にて)

  現在部分的に順次決定、公開されている

- **公開済**
  - IEC/TR 62443-3-1 （2009年5月）
    - Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems
      （工業通信ネットワーク – ネットワーク及びシステムセキュリティ – 第3-1部：工業自動化及び制御システムのためのセキュリティ技術）
  - IEC/TS 62443-1-1 (2009年7月)
    - Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
      （工業通信ネットワーク – ネットワーク及びシステムセキュリティ – 第1-1部：用語，概念及びモデル）
  - IEC 62443-2-1・・・投票中(12月決定予定)
    - Industrial communication networks – network and system security – Part 2-1: Establishing an industrial automation and control system security program

IEC 62443(全体概要)

- IEC/TS62443−1(Part1)
  - Terminology, concepts and models
- IEC/TS62443−2(Part 2)
  - Establishing an industrial automation and control system security program
- IEC/TS62443−3(Part 3)
  - Operating an industrial automation and control system program
- IEC/TS62443−4(Part 4)
  - Specific security requirements for industrial automation and control system
- IEC/TR62443−5,(Part 5、ISA-99 TR00.01と同等)
  - Security technologies for industrial automation and control system

PCSRF

- 名称
  - Process Control Security Requirements Forum（発音: Pic-Surf）
- 位置付け
  - 米国商務省標準技術局:NIST（National Institute of Standards and Technology）の下部組織
- 目的
  - 産業用プロセス制御システム向けの情報セキュリティ要件を定義および適用することで，これらのシステムのセキュリティを強化すること。
  - ベースとして，ISO15408（Common Criteria for IT Security Evaluation）
- メンバー
  - 401の組織，32カ国(2008年10月現在)
  - 制御機器ベンダ(Rockwell, Honeywell,…)，ITベンダ(Cisco, SUN, …)，ユーザ(Exxon Mobil, BP, Dupont, …)，コンサルタント(KEMA, …)，公的機関(NSA, 経産省，…)

PCSRFの活動

- SCP (Security Capabilities Profile)
  - 脆弱性の解析を含めた制御システムのアーキテクチャの分析
  - 安全な制御システムに求められる機能を列挙
  - プロセス制御機器に今後求められるセキュリティ機能を，システムやコンポーネントのベンダに要求する手段とする
  - SPP-ICS作成の基礎とする
- SPP-ICS (System Protection Profile – Industrial Control System)の作成
  - ISO 15408 のPP (Protection Profile)をシステム向けに拡張
    - より特定されたシステム(SCADA, DCSなど)のPP
    - 具体的な制御システムのSST (System Security Target)の基礎
    - 各コンポーネント(コントローラの認証，センサの認証，など)のPP

数年改定されておらず、活動も休止状態。

Industrial Control Systems Joint Working Group (ICSJWG)として新たに活動を開始。

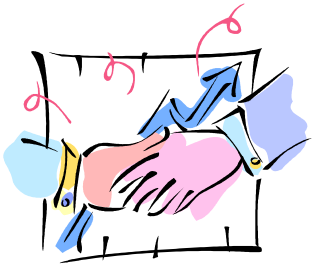
●制御システムセキュリティ俯瞰MAP

セキュリティ規格利用における課題

- セキュリティ規格、標準化団体は増えてきているが・・・
  - 現状
    - 欧米を中心に様々な規格、ガイドライン、団体が乱立している
    - 分野ごとに独自に作成され、互いに参照しあっているものもあるが、実際に適用する際に何を参照したら良いのか、どれが自分の目的に合致しているか判断できない
  - ベンダーの立場
    - 製品の設計や評価検証時にどの規格を採用したら良い？
  - ユーザーの立場
    - システムの検討フェーズや稼働中のシステムの運用時にやらなければならない事が不明
    - セキュリティに関する専門用語が難しい

解決策

- 利用者が、自身が必要な分野・開発フェーズ（ライフサイクル）から必要な規格を参照可能とするための俯瞰MAPを作成する



- 「制御システムセキュリティ俯瞰MAP」ドキュメント構成
  - 制御システムセキュリティ規格俯瞰MAP
  - 制御システムセキュリティ規格要約
  - 制御システムセキュリティ規格相関図

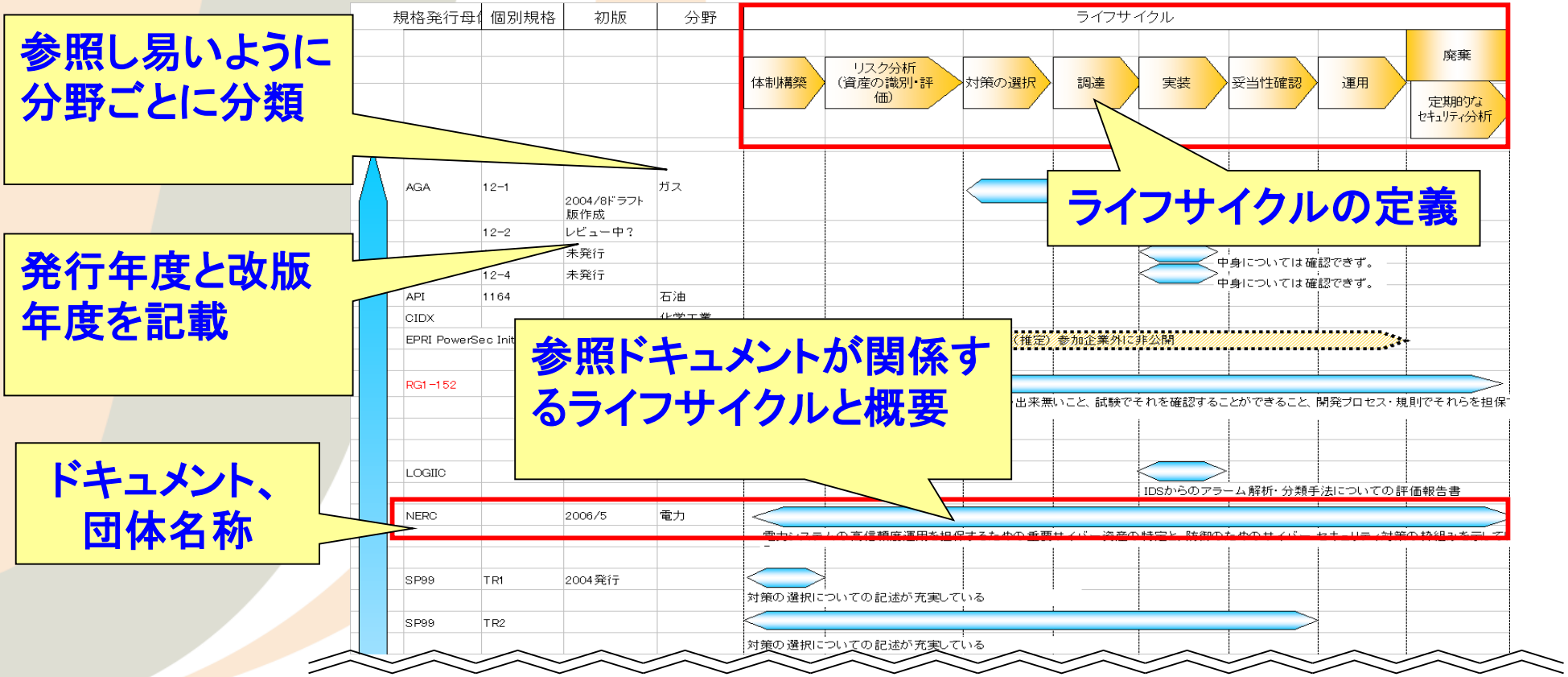
2008年度末に作成。以降、最新動向に合わせて改訂実施

俯瞰MAPの特長

- 各分野ごと(電力、ガス・石油)で取り組まれているセキュリティ規格、団体活動を整理
- 作成年度、更新年度を記載
  - 規格としての**「鮮度」**が重要
- 要約
  - 簡単に内容を理解できるように
- **システムのライフサイクル**に合わせて記載
  - 現在自分が担当している業務のフェーズから参照すべき規格が逆引きできる
- 情報系規格との関連を記載

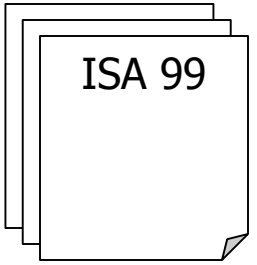
俯瞰MAPのレイアウト

- 参照するドキュメントが、どのライフサイクルの部分について書かれているかを容易に確認可能



セキュリティ規格の要約

- 1つの規格について1ページで要約されている
  - 策定団体、メンバー企業
  - 対象分野
  - 内容
  - 策定団体やドキュメントの参照URL
  - 発行年月日（ドラフト/初版/改版など）
    - 発行日や改訂状況などから**規格としての鮮度**を把握する
  - 対応するJIS規格



セキュリティ規格の要約

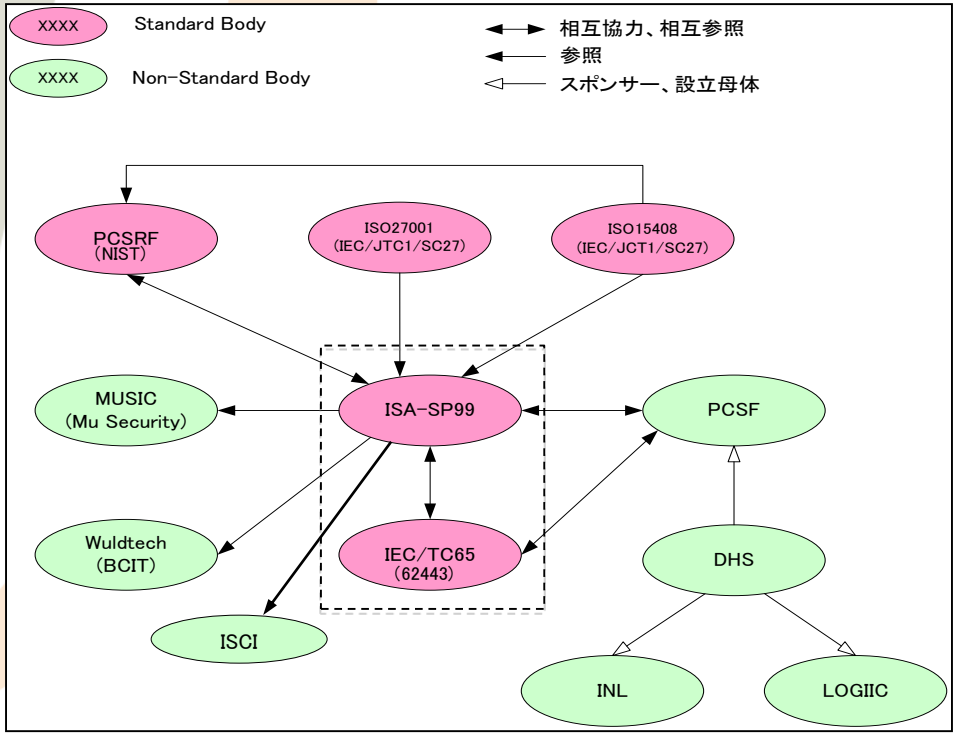
- 要約例

SP800-42 “Guideline on Network Security Testing"

- **策定団体：**
  アメリカ国立標準技術研究所(National Institute of Standards and Technology, NIST)
  http://www.nist.gov/
- **内容：**
  ネットワークセキュリティの検査ガイドライン。
  効果的なセキュリティテストプログラムの必要性を解説。目的は次の通り。
  (1) 最先端システムに存在する脆弱性と実運用のギャップを埋めるため
  (2) 組織のセキュリティ運用を理解，調整，記録するため
  (3) 組織の取り組みを改善するため
  セキュリティ開発ライフサイクルにおいて，実装と，妥当性検証，運用，定期的な監査に適用される。
- **発行年月日：**
  NIST Special Publication 800-42
  Guideline on Network Security Testing
  初版：2003 年 10 月
- **URL：**
  http://csrc.nist.gov/publications/PubsSPs.html
- **対応 JIS 規格：**
  なし

セキュリティ規格相関図

- 個々の規格、団体間の相関図
  - 各規格の関係、普及の度合いをわかりやすく整理



PART1
生産制御システムセキュリティの現状

PART2
制御システムのセキュリティ規格化動向

PART3
グッドプラクティスの検討

背景

1. 背景

■他システム、上位システムの連携を前提とした生産制御システムのセキュリティ対策どうすれば？

JEMIMAセキュリティ調査研究WG

生産制御システムとしてのセキュリティ・ガイド

プロセス・制御とSCADAセキュリティ

“グッドプラクティスの原則”

具体的なセキュリティ対策方法の事例検討

2. セキュリティ・ガイド

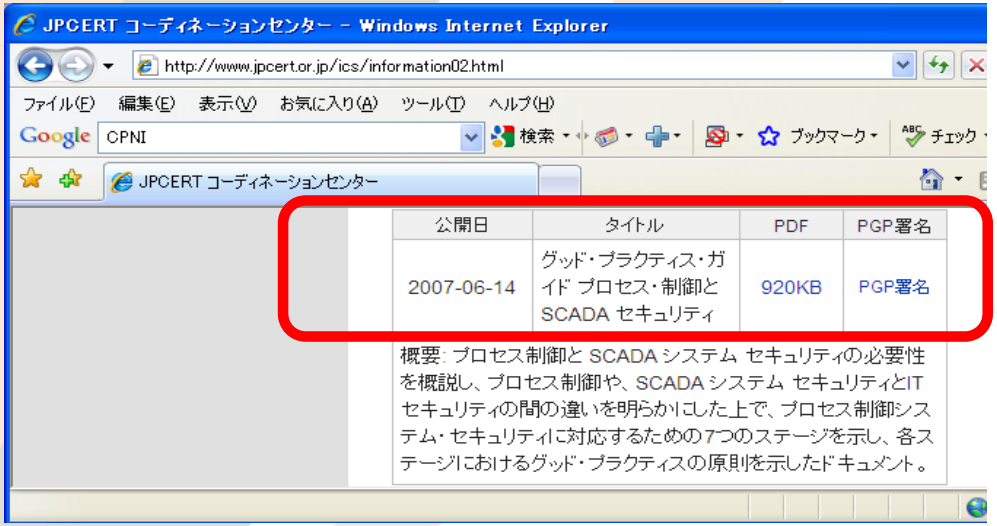
- 原版：“Good Practice Guide Process Control and SCADA Security”

  2005年10月：CPNI(英国)より初版発行

  2008年　6月：第2版発行

- 和訳版：“グッド・プラクティス・ガイド　プロセス・制御とSCADAセキュリティ”

  2007年6月：JPCERT/CCより発行



※CPNI = Centre for the Protection of National Infrastracture
JPCERT/CC = Japan Computer Emergency Response Team コーディネーションセンター

3. グッドプラクティスの原則

“グッドプラクティス”とは、

- 調査と評価により効果的であると示された、戦略、活動、方法等の最良の指針。

ただし、

- 環境や生産制御システムによっては、これらの原則のすべてを実施できない場合がありうる。
そのような場合には、他の防護手段を調査すべきである。

安全・安定稼動を最優先する制御システムに取り入れる際には、充分検討の上、実施する必要があります。

4. グッドプラクティスの事例

グッドプラクティス　対策事例

18項目　全55事例

大項目

事例

- 4.3.1 ネットワーク・アーキテクチャ(5)
- 4.3.2 ファイアウォール(7)
- 4.3.3 リモートアクセス(8)
- 4.3.4 ウィルス対策(2)
- 4.3.5 電子メールとインターネットアクセス(1)
- 4.3.6 システムの強化(2)
- 4.3.7 バックアップと回復(3)
- 4.3.8 物理的セキュリティ(1)
- 4.3.9 システム監視(5)
- 4.3.10 セキュリティ・パッチ(4)
- 4.3.11 要員の身元確認(1)
- 4.3.12 パスワードとアカウント(5)
- 4.3.13 文書セキュリティ・フレームワーク(3)
- 4.3.14 セキュリティ・スキャン(1)
- 4.3.15 転入者と転出者用のプロセス(2)
- 4.3.16 変更管理(2)
- 4.3.17 セキュリティ試験(2)
- 4.3.18 機器接続手順(1)

5. グッドプラクティスの事例

“グッドプラクティスの原則” 項目一例

4.3 グッド・プラクティスの原則

大項目

4.3.1 ネットワーク・アーキテクチャ

事例

- プロセス制御システムへのすべての接続を特定する。
- プロセス制御システムへの接続数を減らす。正当な事業上の理由がある接続だけを残す。
- できる限り、プロセス制御システムを他のネットワークから分離し、隔離する。
- 安全上重要なプロセス制御システムには専用のインフラストラクチャを用意する。
- できる限り、安全システム （例、緊急停止システム）とプロセス制御システムまたは他のネットワークの間で TCP/IP 接続を使わない。これが不可能な場合は、リスク分析を行うべきである。

4.3.2 ファイアウォール

- プロセス制御システムと他のシステムの間の接続は、ファイアウォールと非武装セグメント（DMZ）アーキテクチャを用いて保護する。[1]

6. 検討経過

大項目　グッドプラクティス事例　重要度　具体策

大項目	グッドプラクティス事例	○:ひとこと言いたい △:ほぼその通り □:その通り							制御システムとして、どのような具体策を講じることができるか？
		A委員	B委員	C委員	D委員	E委員	…	X委員	
4.3.2 ファイアウォール	ファイアウォールの管理と監視を 24 時間 365 日実施できる体制を築くべきである。	○	△	○	○	○	…	○	リアルタイムでの監視が必要。人力でのチェックは困難。機械化すべき。→ネットワークに対しての不正アクセスの検出を実施する。現時点ではIDSの設置による検出。検出時のアクションとして、該当システムのどこまでを止める（切り離す）ことが可能かを事前に決めておくことが必要。
4.3.5 電子メールとインターネット・アクセス	プロセス制御システムからの電子メールとインターネット・アクセスをすべて不可にする。	□	○	○	○	□	…	○	プロセス制御システムから電子メールを発信させる場合は適切な認証機能とファイアウォールによるフィルタリング機能を使用して外部からの不正アクセス対策を行う。受信はスパムメールによる異常負荷が想定されるため不可にする。 ブラウザなどによる外部サイトのアクセスは不正プログラムをダウンロードしてしまう可能性があるため、行わない事が望ましい。
4.3.6 システムの強化	すべての組み込まれたシステム・セキュリティ機能は有効にする。	○	△	○	△	△	…	△	全てのセキュリティ機能を有効にするのではなく、制御システムとしてセキュリティ機能の設計と割付を行った後，その実現手段として「組み込まれたシステムセキュリティ機能」を割り当てるようにすべき。
4.3.9 システム監視	電子的インシデントの結果と思われる異常動作（例、ネットワークのトラフィックが増えたのはワームに感染したからかもしれない）を検出するため、プロセス制御システムをリアルタイムで監視する。様々なパラメータを定義し、リアルタイムで監視し、異常動作検出のための正常動作基準と比較すべきである。	○	△	△	△	○	…	△	・定期監視（ログ監視）を実施する必要がある。制御システムでのサイトでの実施は現実的か？ ・実運用に関してはコスト、成果など課題は多い。
4.3.3 リモート・アクセス	不正なリモート・アクセス接続がないよう定期的に監査する。	△	△	○	△	△	…	△	アクセス記録の監視が必要。ファイアウォールと同様にリアルタイムな監視が必要。
4.3.11 セキュリティ・パッチ	このプロセスは、パッチ適用前にそのパッチに対するベンダの認定を受け、パッチをテストすること、および変更により支障が起こる危険を最小限にするために段階的に適用するプロセスを考慮すべきである。	△	△	○	△	△	…	△	制御システムベンダーとして、顧客のシステムの稼動とセキュリティの確保は必須と考えられる。ベンダーとしては供給製品に関する、セキュリティ確保のための情報提供及び、情報提供のための動作検証は、必須と考えられる。但し、セキュリティ確保のための作業及び導入の最終決定は、顧客依存と考えられる。

生産制御システムのセキュリティ対策としての重要度および適用する際の具体策を検討

事例紹介

4.3.2　ファイアウォール

ファイアウォールの管理と監視を 24 時間 365 日実施できる体制を築くべきである。

現実的な課題

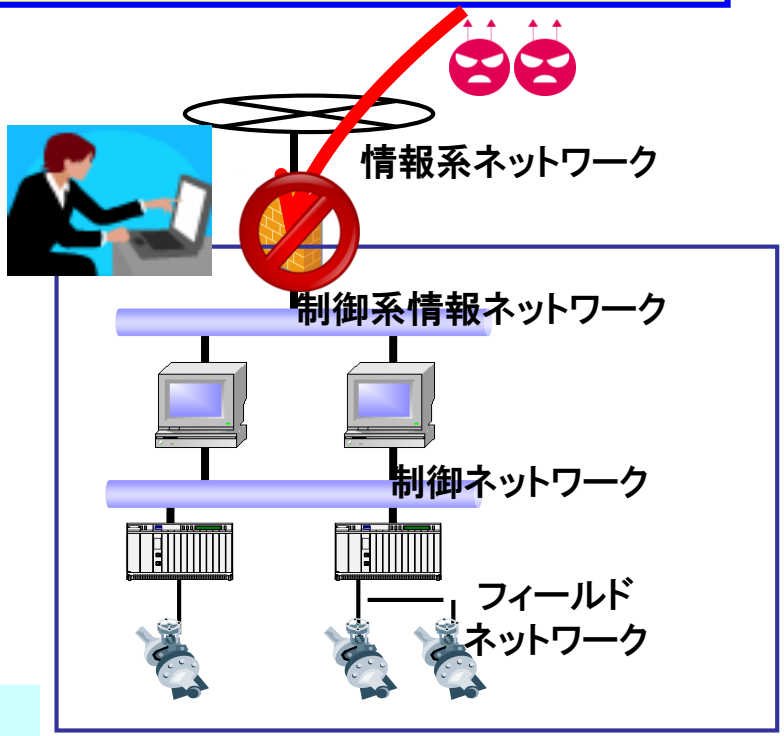
人的リソースがさけるか？
・膨大な通信量/ログ
・就業時間外/休日

手段

・不正検出自動化
（ログ解析および検出時のアラーム発報）
・IDS（侵入検知システム）の併用

不正検出時のアクション

・該当システムのどこまでを停める（切り離す）ことが可能かを事前に決めておくことが必要
・人命・安全にかかわる保護が最優先

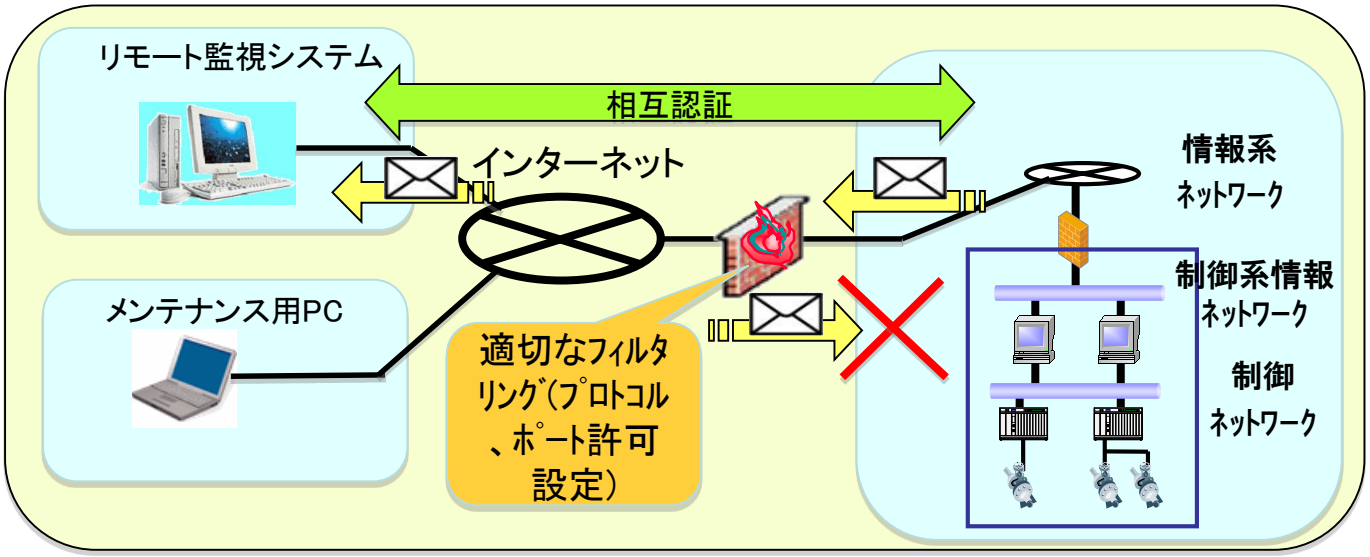


安全最優先

4.3.5　電子メールとインターネットアクセス

プロセス制御システムからの電子メールとインターネット・アクセスをすべて不可にする。

すべて不可が基本。メンテナンス等でやむをえずメール送信のためにインターネットに接続しなければならない場合、セキュリティ対策を充分に行う必要がある



適切な認証メール機能とファイアウォールによるフィルタリング機能を使用してメール発信のみ許可

スパムメールによる異常負荷が想定されるためメール受信は禁止

4.3.6　システムの強化
すべての組み込まれたシステム・セキュリティ機能は有効にする。

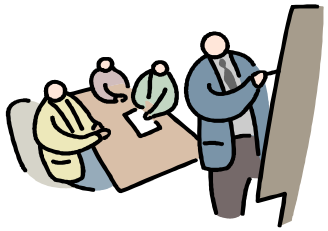
もう一歩踏み込んで考えると…

制御システムに必要なセキュリティ機能の設計をした後に
実現手段として「組み込まれたシステムセキュリティ機能」を割り当てるのが良い

リスク分析
・行為者は誰か
・守る資産は
・脅威は何か

セキュリティ機能の設計
・ウイルス対策
・監査ログ記録
・機能の維持

機能を割当
例えば…
・ウイルス検出ソフト
・ログ設定
・組込みファイアウォール



■セキュリティ機能を入れる場合の注意：

ウイルス検出ソフト　⇒　制御システムに影響を与えない範囲でのアップデートが重要

認証・ファイアウォール ⇒　「ユーザ権限管理，アプリが使う通信ポートの見極め」などの適切な設定を施さなければ効果なし

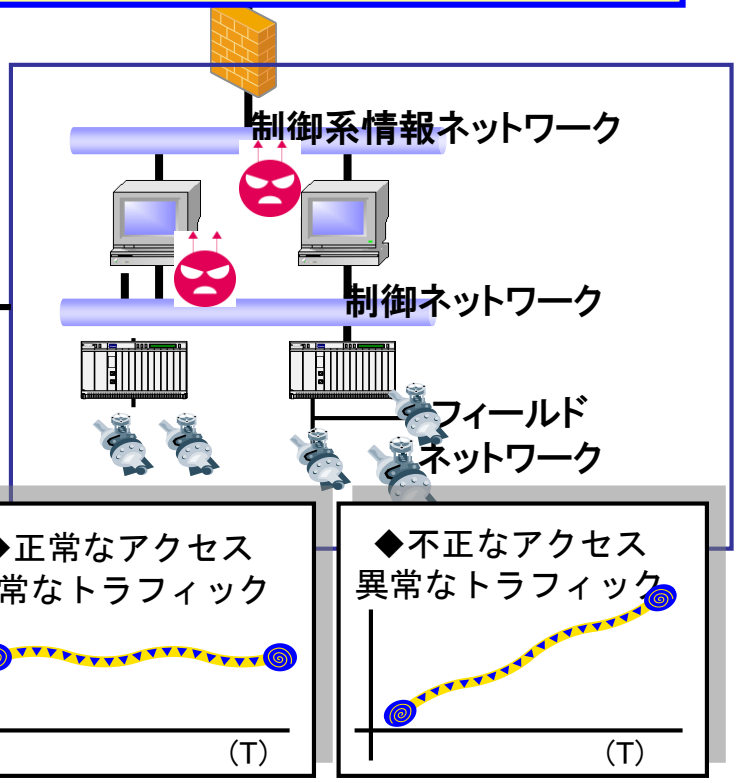
グッド・プラクティスの原則　　システム監視

4.3.9　システム監視

電子的インシデントの結果と思われる異常動作を検出するため、プロセス制御システムをリアルタイムで監視する。様々なパラメータを定義 し、リアルタイムで監視し、異常動作検出のための正常動作基準と比較すべきである。

① リアルタイムで不正・異常動作を監査

⇒IDSによるネットワークトラフィックの異常な増加や不正なアクセスの兆候を検知



IDS（Intrusion Detection System）：侵入検知システム

・不正検出：ユーザの行動やパケットのパターンチェック

・異常検出：通常と異なる“振る舞い”を検出

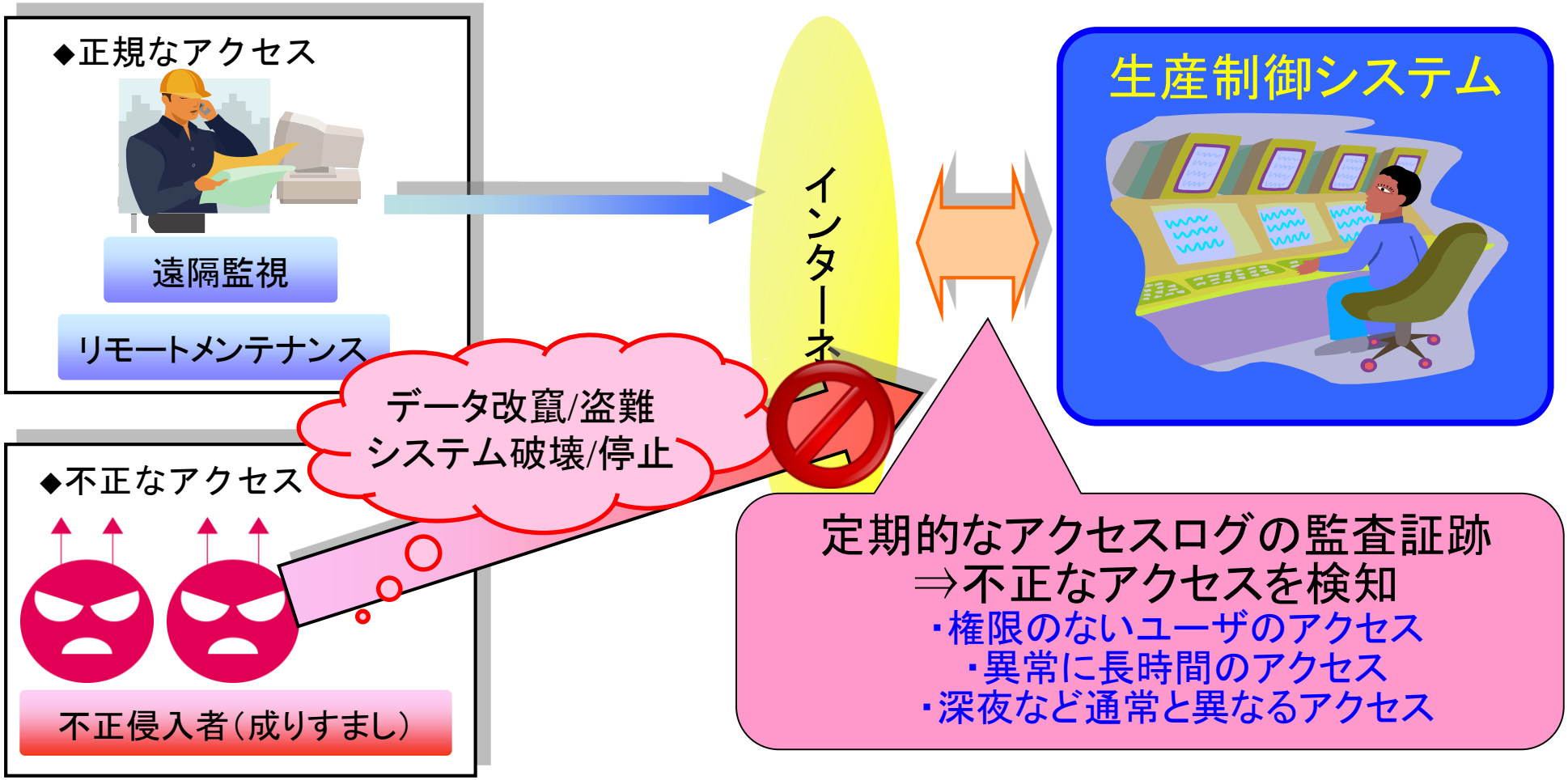
② ログ監視

⇒　定期的なログ監視の実施

グッド・プラクティスの原則　　リモート・アクセス

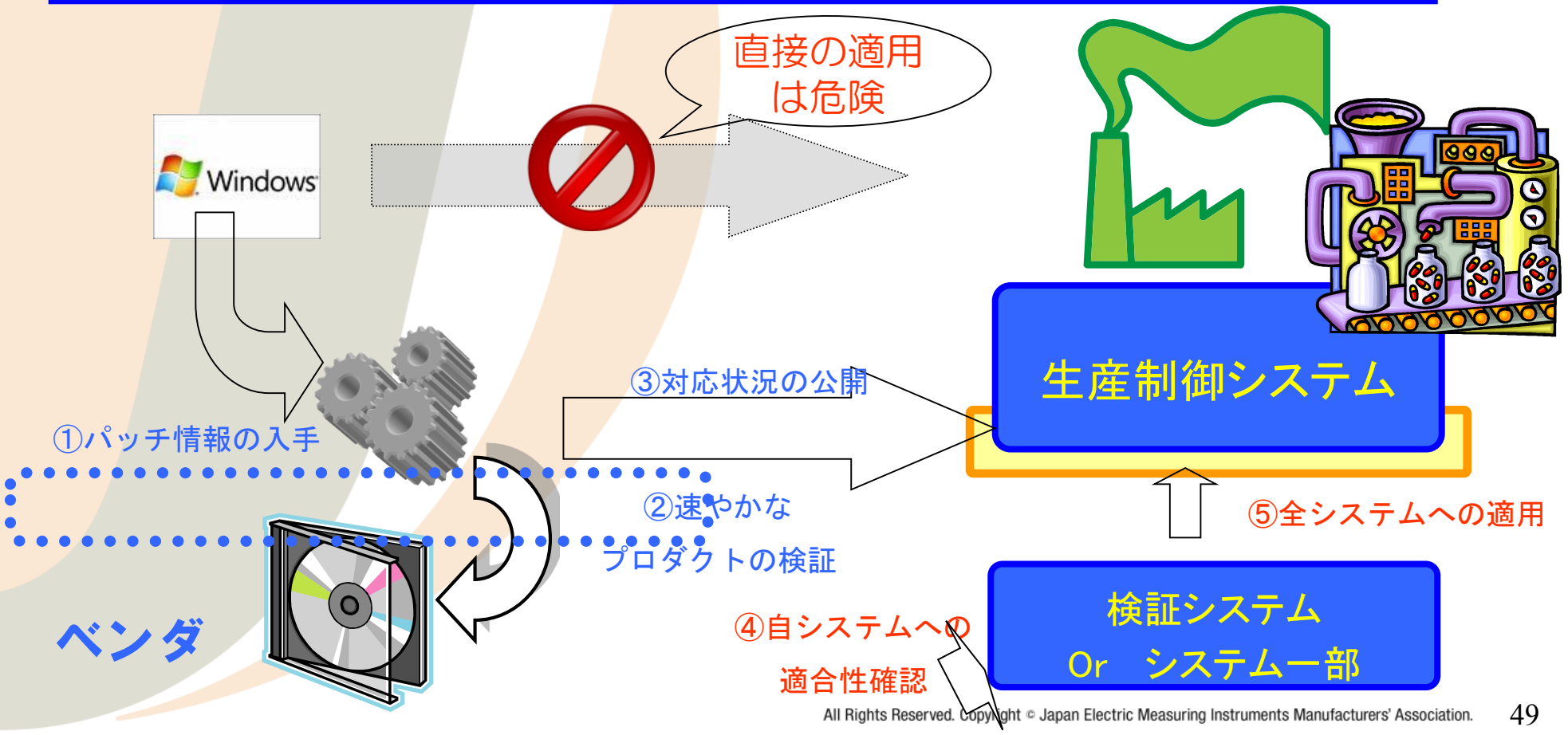
4.3.3　リモート・アクセス

不正なリモート・アクセス接続がないよう定期的に監査する。



4.3.11　セキュリティ・パッチ

生産制御システムは、パッチ適用前にそのパッチに対するベンダの認定を受け、パッチをテストすること、および変更により支障が起こる危険を最小限にするために段階的に適用するプロセスを考慮すべきである。



まとめ

全体のまとめ

- 今後、本グッドプラクティスをベースに、　セキュリティ対策に関する情報共有と　協力体制を関係者間で築いていきます。

参考URL

- CPNIガイドライン　オリジナル：

“Good Practice Guide Process Control and SCADA Security”

http://www.cpni.gov.uk/Products/guidelines.aspx

- JPCERT和訳版：

“グッド・プラクティスガイド　プロセス制御とSCADAセキュリティ”

http://www.jpcert.or.jp/ics/information02.html