JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

生産制御システムセキュリティの技術動向

2010.10.7

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。

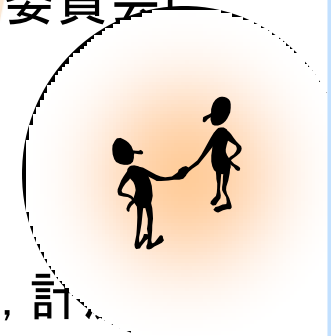
- 設立:2005年4月
- メンバ

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. ISA SP99　TR2を利用したセキュリティ対策の実践
    2. NIST 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
    5. セキュリティ評価ツールの調査

WGのご紹介

- 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）
  - IEC/TC65/WG10国内委員会にメンバ登録



- 広報活動
  - JEMIMA 委員会セミナー，計
  - JPCERT制御システムセキュリティカンファレンス
  - 制御技術会議
  - SICE Annual Conference

Agenda

PART1
生産制御システムセキュリティの現状

PART2
グッドプラクティスの検討

PART3
セキュリティ評価ツールの取り組み

JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

PART 1

生産制御システム セキュリティの現状

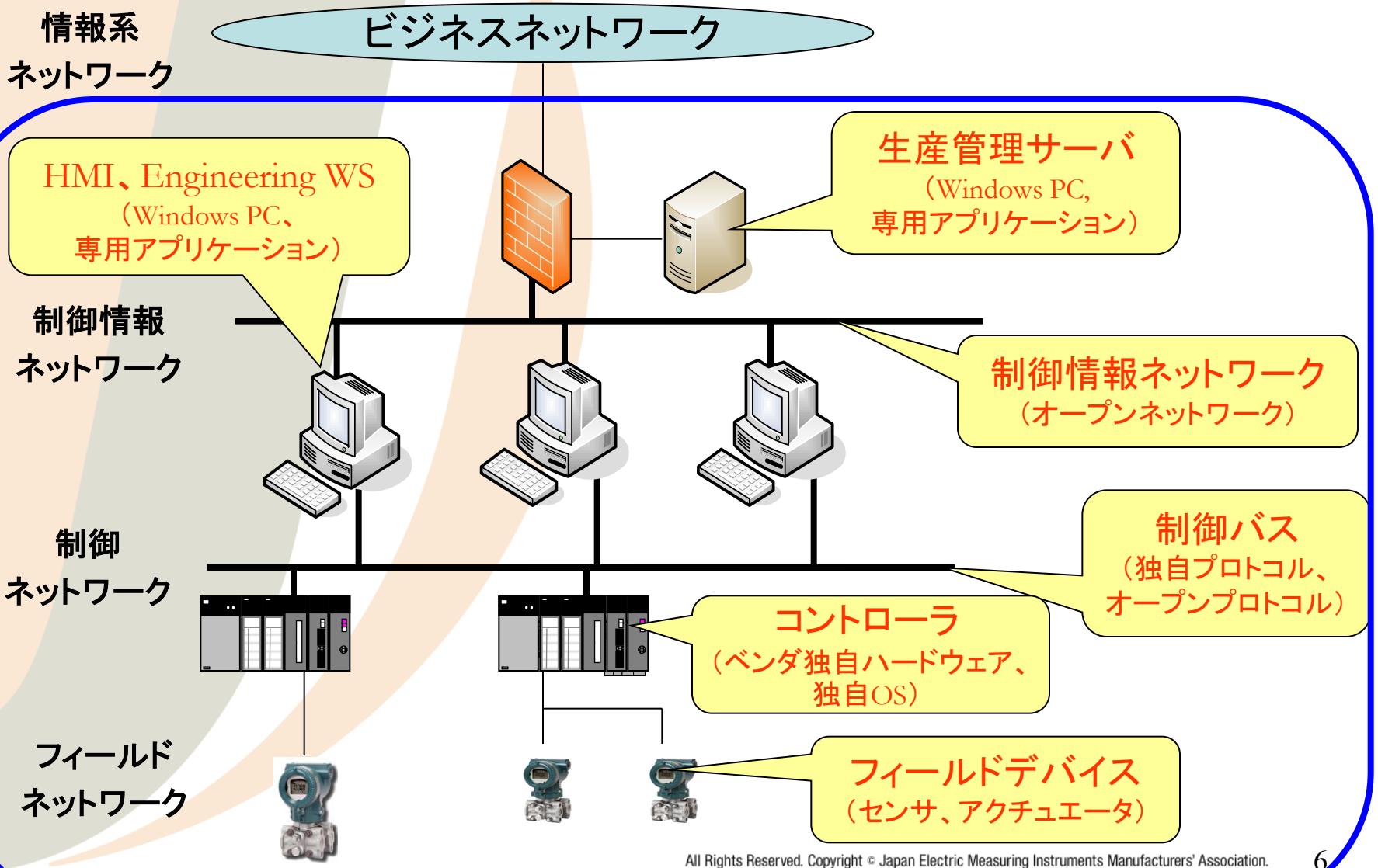
2010.10.7

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

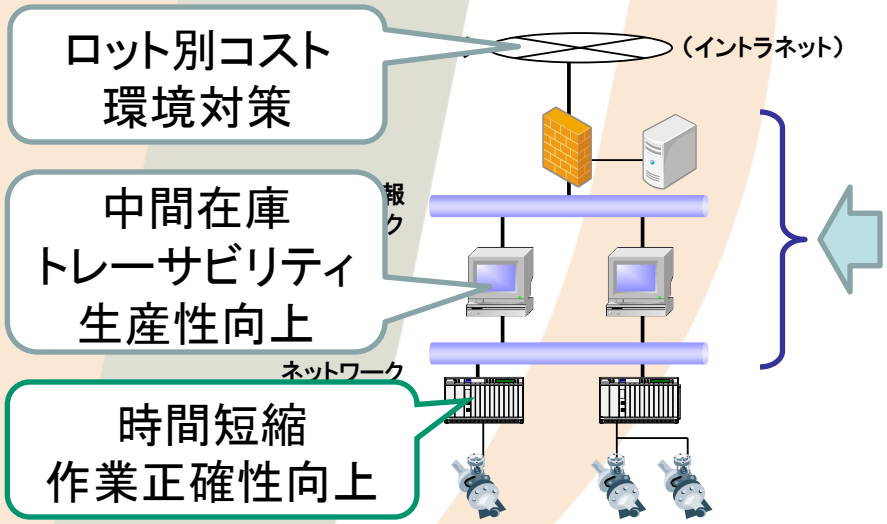
生産制御システム概要



生産制御システムセキュリティの背景

制御システムにおいて情報連携の重要性が高まる

見える化(経営，生産管理，操業) ＋ 技術の共通化の進展



- オープン技術
  - ハードウェア(x86, LAN用LSI)
  - OS(Windows, Linux)
  - ネットワーク(Ethernet, 無線LAN)
  - プロトコル(OPC, 産業用Ethernet)
  - アプリケーション(ﾃﾞｰﾀﾍﾞｰｽ, Web)
- マルチベンダ

外部からの干渉を受けやすくなる

⇒被害を受けないように防止することが必要になる

OPC：OLE for Process Control

現実化する脅威

セキュリティ事故事例：
オーストラリア下水システム侵入

- 2000年，マルーチー市の下水処理管理システムが不正に侵入され，河川や海に何百万リットルもの下水を流出
- 原因は退職エンジニアによる侵入
  - 市の下水システムを開発した会社に勤務していた
  - 市へ就職を希望したが，不採用で立腹
  - 2000年3月～4月で少なくとも46回侵入し，システムの制御権を奪取
- ノートPC＋無線を使い侵入
  ⇒逮捕・禁固2年

Maroochy by Google map

セキュリティ確保の3条件

- 第三者の悪意のある行為に対するシステムのセキュリティ確保には3つの条件があります

①機密性

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

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

情報や資源がいつでも利用できること

ITシステムと生産制御システムにおいては3条件の保護する優先度が異なります

ITシステムと生産制御システムの違い

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

ITシステムと生産制御システムの違い

JEMIMA

	内　容	生産制御 シ ス テ ム	IT　シ ス テ ム
1	性能要件	応答性能が重要。遅延は重大問題。	応答性能よりもスループットが要求される。
2	可用性	システムの再起動は許されない場合が多い。	運用上必要であればシステムの再起動が許容。
3	即時性	緊急処置に対する人間の操作を妨げてはならない。	即時性を要求する緊急処置は少ない。
4	ライフタイム	15-20年と長い。	システム、機器のライフタイムは3-5年が中心。
5	守るべき資産	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。	IT資産および情報を第一に保護している。
6	システム運用	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。	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。
7	リソース（メモリやディスク容量）	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。	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。
8	通信	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。	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。
9	サポート	サービスサポートは通常1ベンダーによる。	機器メーカーによる様々な支援体制がある。
10	危機管理	人、環境の安全性が第一、次がプロセスの保護である。	データ機密性及び完全性を第一に管理する。

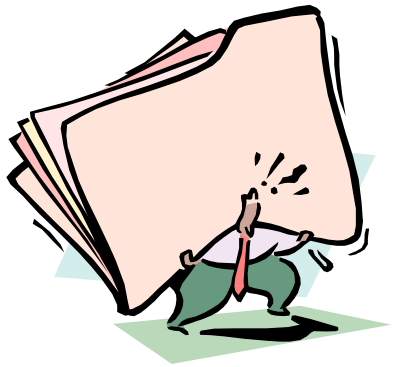
生産制御システムセキュリティの課題

出典：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」

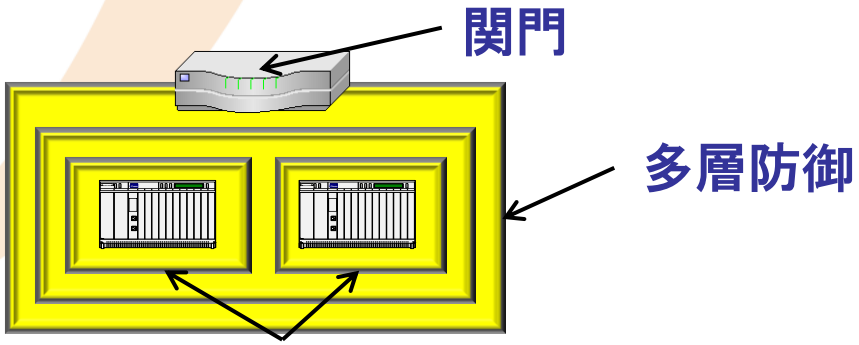
- 課題１：オープン化に伴う脆弱性リスクの混入
  - 汎用製品，標準ネットワークの採用
    ⇒ 脆弱性の課題も引き継ぐ（例：USBメモリ，ネットワーク侵入）
- 課題２：長期利用に伴うセキュリティ対策技術の陳腐化
  - １０～２０年の間に，対策が更新されない可能性あり
- 課題３：可用性重視に伴うセキュリティ機能の絞り込み
  - ウイルス検査プログラム負荷のシステムに対する影響
  - セキュリティパッチ導入によるシステム稼働率への影響

課題対策の現状

生産制御システムに対するセキュリティ対策：
　対策が必要であることは判っているが、何をどうすれば
　良いか判断がつけにくい。

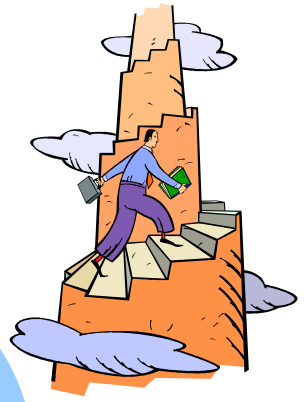


基本戦略：
- 独立した複雑なセキュリティシステムより，
  シンプルな対策を「重ねる」
- シンプル/安易なセキュリティはない
  繰り返して見直す，PDCAサイクルを回すことが重要



PDCAサイクルの具体策

	制御系セキュリティに使えるツール・規格 例
Plan	ISA-99 NIST SP800-53/82 各種Good Practice セキュリティ評価ツール
Do	ISA-99 脆弱性スキャナ 侵入検知システム（IDS）
Check	ログ監査 侵入検知システム（IDS） 脆弱性情報
Act	ISA-99 NIST SP800-53/82 各種Good Practice



WGメンバー

ISA-99

- 名称
  - “Security for Industrial Automation and Control Systems”
- 団体
  - ISA：International Society of Automation／国際計測制御学会
- 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，一部のメンバーは執筆に大きく貢献
  - システムベンダーもひと通り参加
- 内容
  - 生産制御システムへの電子的侵入を防ぐための指針の確立を目的としており、4つのパート(Part 1～4)で構成されている。

各文書は順次レリースされているが、現在作成中の文書もある。

NIST SP800

- 団体
  - NIST：National Institute of Standards and Technology
    ／米国国立標準技術研究所
- 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, …)
- 内容

SP800シリーズと名付けたコンピュータセキュリティに関する特別文書（Special Publications）が約100件公開されている。

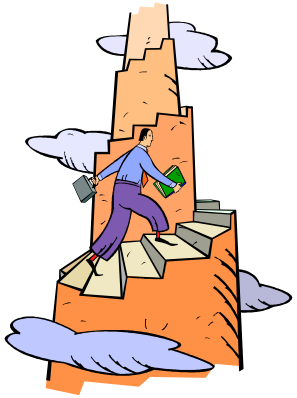
2つの文書が生産制御システムコミュニティに当てはまる。

SP800-53　Recommended Security Controls for Federal Information Systems
／連邦政府情報システムにおける推奨セキュリティ管理策

SP800-82　Guide to Industrial Control System Security
／産業用制御システムセキュリティのためのガイド

PDCAサイクルの具体策

	制御系セキュリティに使えるツール・規格 例
Plan	ISA-99 NIST SP800-53/82 各種Good Practice セキュリティ評価ツール
Do	ISA-99 脆弱性スキャナ 侵入検知システム（IDS）
Check	ログ監査 侵入検知システム（IDS） 脆弱性情報
Act	ISA-99 NIST SP800-53/82 各種Good Practice



・Good Practice の検討
・セキュリティ評価ツールの取組

WGメンバー

JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

PART 2

グッドプラクティスの検討

2010.10.7

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

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

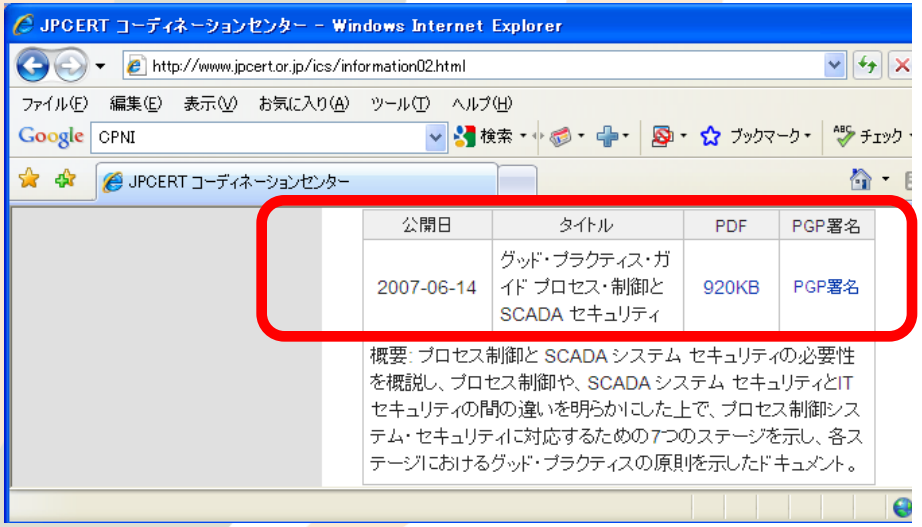
“グッドプラクティスの原則”

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

大項目

事例

4.3 グッド・プラクティスの原則

4.3.1 ネットワーク・アーキテクチャ

- 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

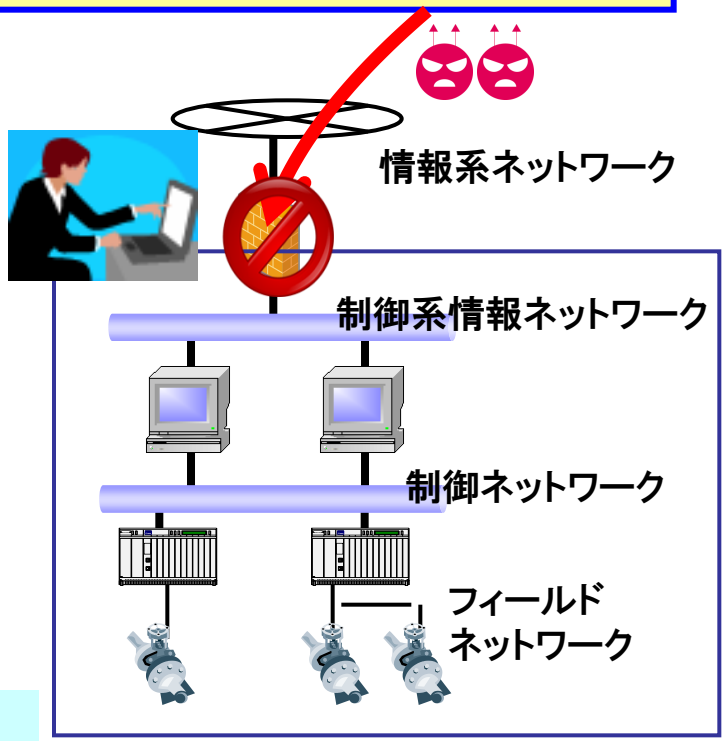
人的リソースがさけるか？
・膨大な通信量/ログ
・就業時間外/休日

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

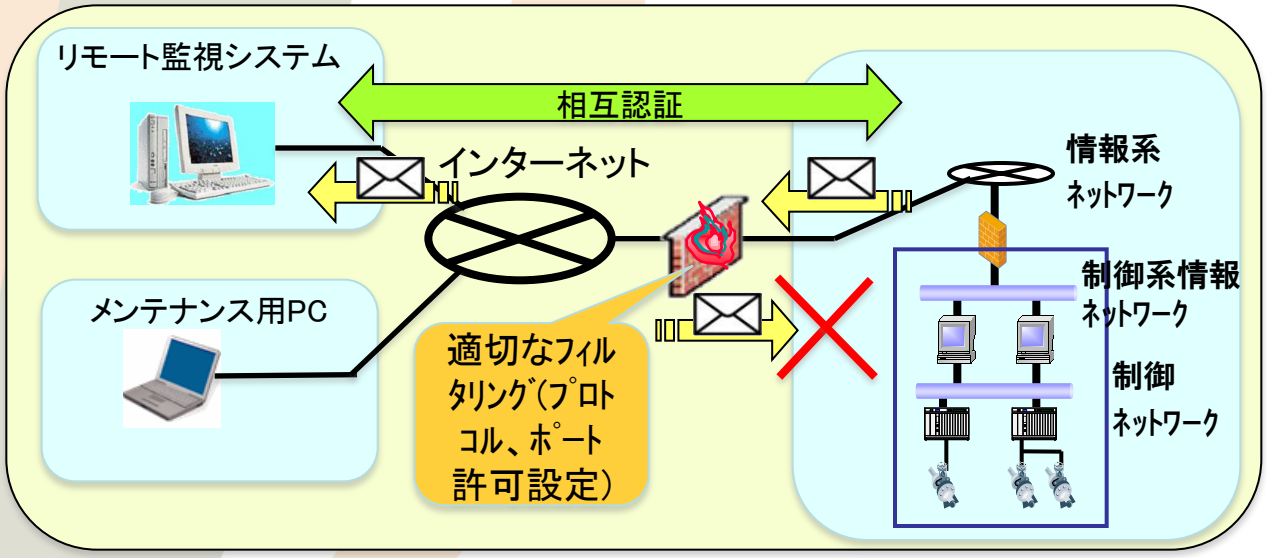


安全最優先

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**

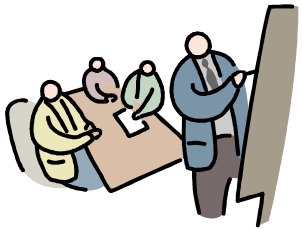
スパムメールによる異常負荷が想定されるため**メール受信は禁止**

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	セキュリティ機能の設計	機能を割当
・行為者は誰か ・守る資産は ・脅威は何か	・ウイルス対策 ・監査ログ記録 ・機能の維持	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

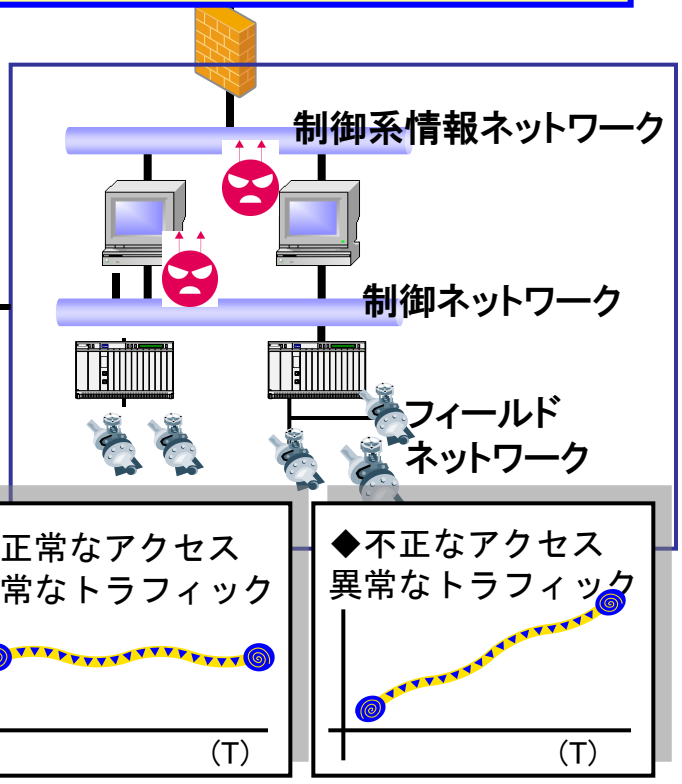
認証・ファイアウォール ⇒　「ユーザ権限管理，アプリが使う通信ポートの見極め」などの適切な設定を施さなければ効果なし

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。

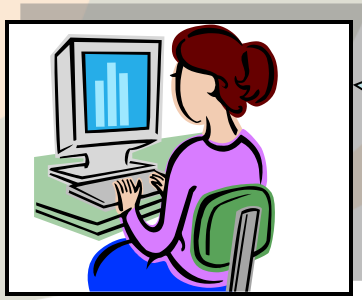
① リアルタイムで不正・異常動作を監査

⇒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

JEMIMA

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。

◆正規なアクセス

遠隔監視

リモートメンテナンス

インターネ

データ改竄/盗難
システム破壊/停止

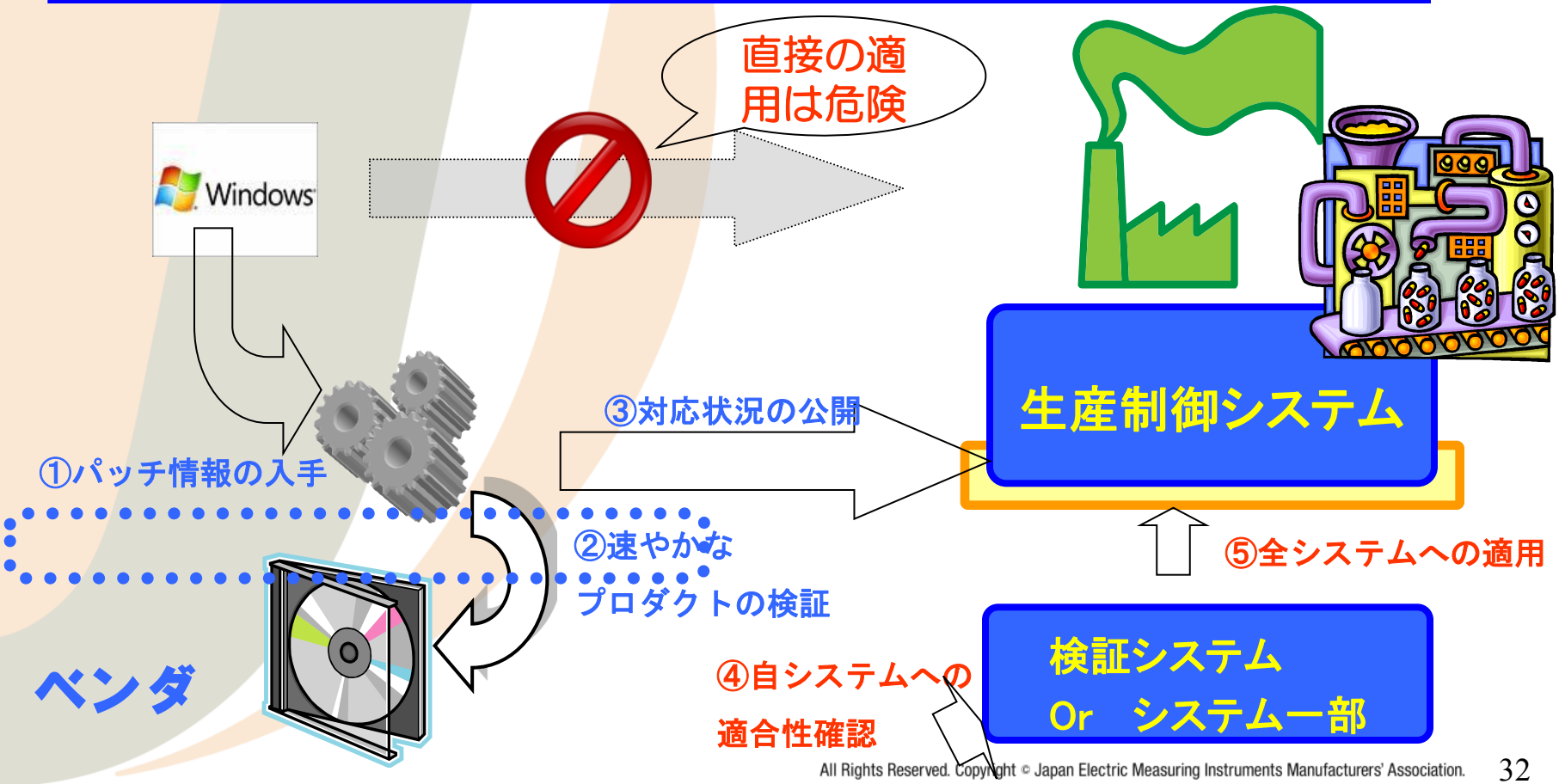
◆不正なアクセス

不正侵入者（成りすまし）

定期的なアクセスログの監査証跡
⇒不正なアクセスを検知
- 権限のないユーザのアクセス
- 異常に長時間のアクセス
- 深夜など通常と異なるアクセス

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。



PART2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。

JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

PART 3

セキュリティ評価ツールの取り組み

2010.10.7

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

概要

- 概要
  - 本WGでは、2010年度活動として「セキュリティ評価ツールSSAT」の評価を行なっている
  - これまでの活動の概要と今後の課題について紹介する

- 内容
  - モデルシステムのセキュリティ評価
    - 目的・方法
    - セキュリティ評価ツールSSATの紹介
    - 評価対象モデルシステムの紹介
    - 評価手順
    - 評価結果
  - 評価結果に基く改善試行
    - 改善案の作成
    - 改善後の評価結果
    - 改善試行のまとめ
  - セキュリティ評価ツールの感想・所見
  - まとめと今後の課題

モデルシステムのセキュリティ評価

モデルシステムのセキュリティ評価

- 目的
  - セキュリティ評価ツールSSATを評価する
    - 生産制御システムのセキュリティ向上への有用性は？
    - 設問の内容はわかりやすく回答しやすいか？
    - ブラッシュアップできる点はあるか？
  - モデルシステムのセキュリティ状況を確認する
    - セキュリティ評価ツールでの評価結果は？
    - セキュリティ上の問題点は？
- 方法
  - モデルシステムの想定に基いて各メンバーがセキュリティ評価ツールの設問に回答
    - 評価対象はWGメンバーが定義したモデルシステム(日本の標準的な生産制御システムを想定)
    - 評価にはSSAT日本語版(JPCERT/CC提供)を使用
    - セキュリティ評価ツールについて気が付いた点を指摘
      - 生産制御システム関係者が理解・回答できる設問内容か?
      - 現状と大きく乖離した設問はないか?
  - 各メンバーの回答内容を持ち寄りWGで検討
    - モデルシステムの想定に合った回答になるよう討議・調整
  - 検討後の回答をセキュリティ評価ツールで評価
    - モデルシステムのセキュリティ状況を確認

セキュリティ評価ツールSSAT

WGメンバーで検討

セキュリティ評価ツール SSATの紹介

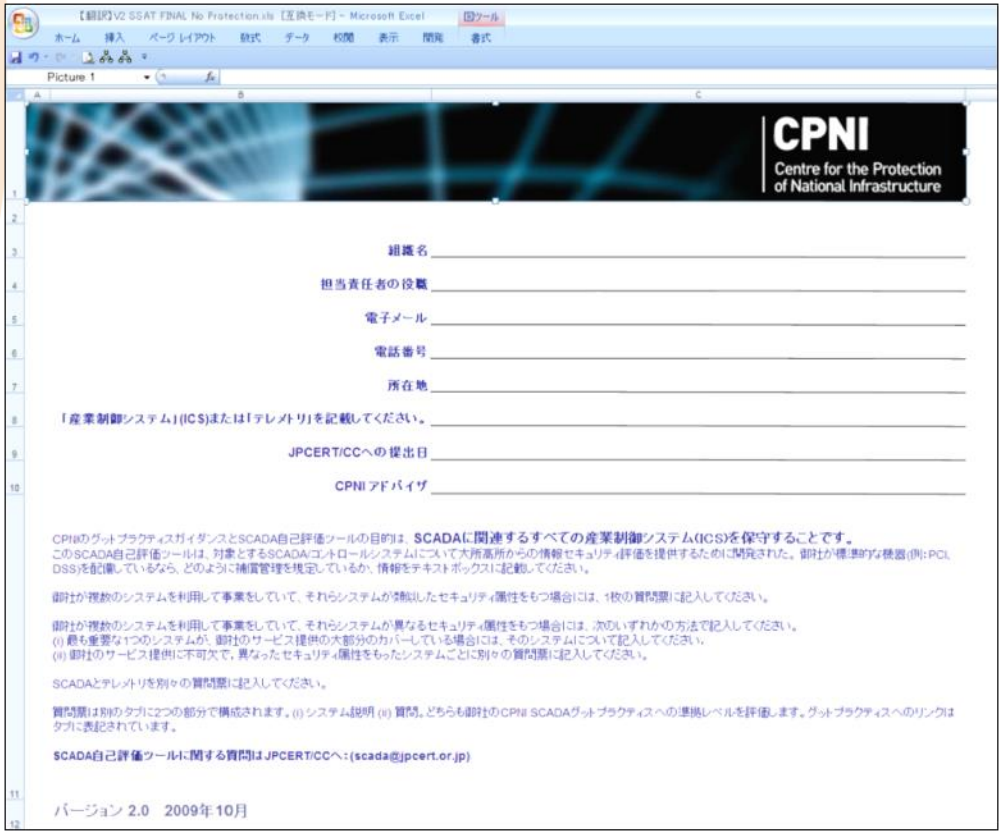
SSAT (SCADA Self Assessment Tool)

SSAT とは？

- CPNI が開発した SCADA を導入している生産制御システム向けの自己評価ツール

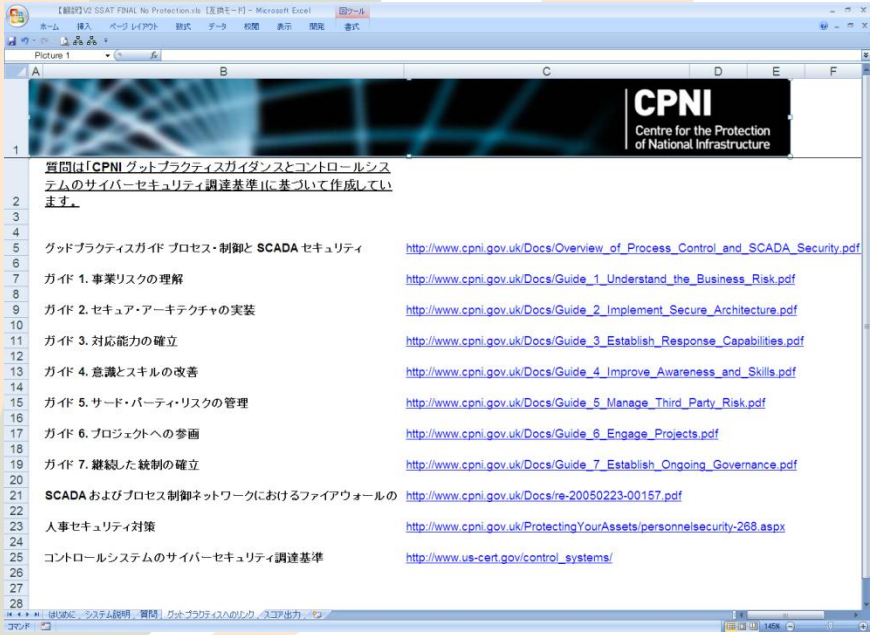
特徴は？

- SCADA に特化しているセキュリティ評価ツール
- 導入・操作が容易
- 評価は短期間で実施可能
- 和訳参考資料が豊富



SSAT (SCADA Self Assessment Tool)

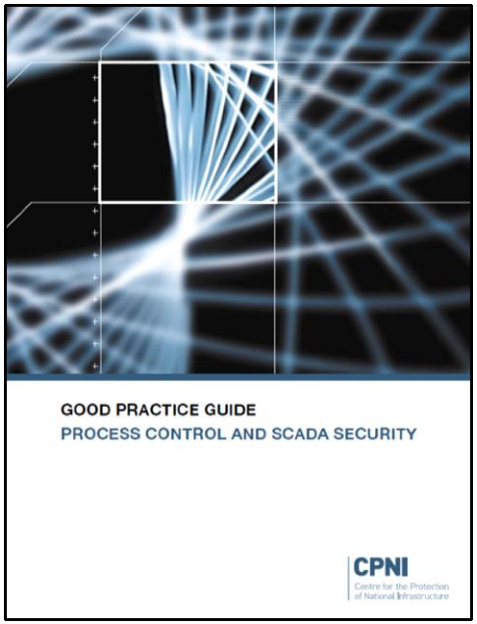
- **セキュリティ基準は CPNI が公開しているグッド・プラクティス・ガイド「 プロセス・制御と SCADA セキュリティ 」**
  - グッド・プラクティスはいくつかのガイドに分かれている
  - 最新版(2009/10 ver 2.0)はファイアウォールと人事セキュリティ基準を追加



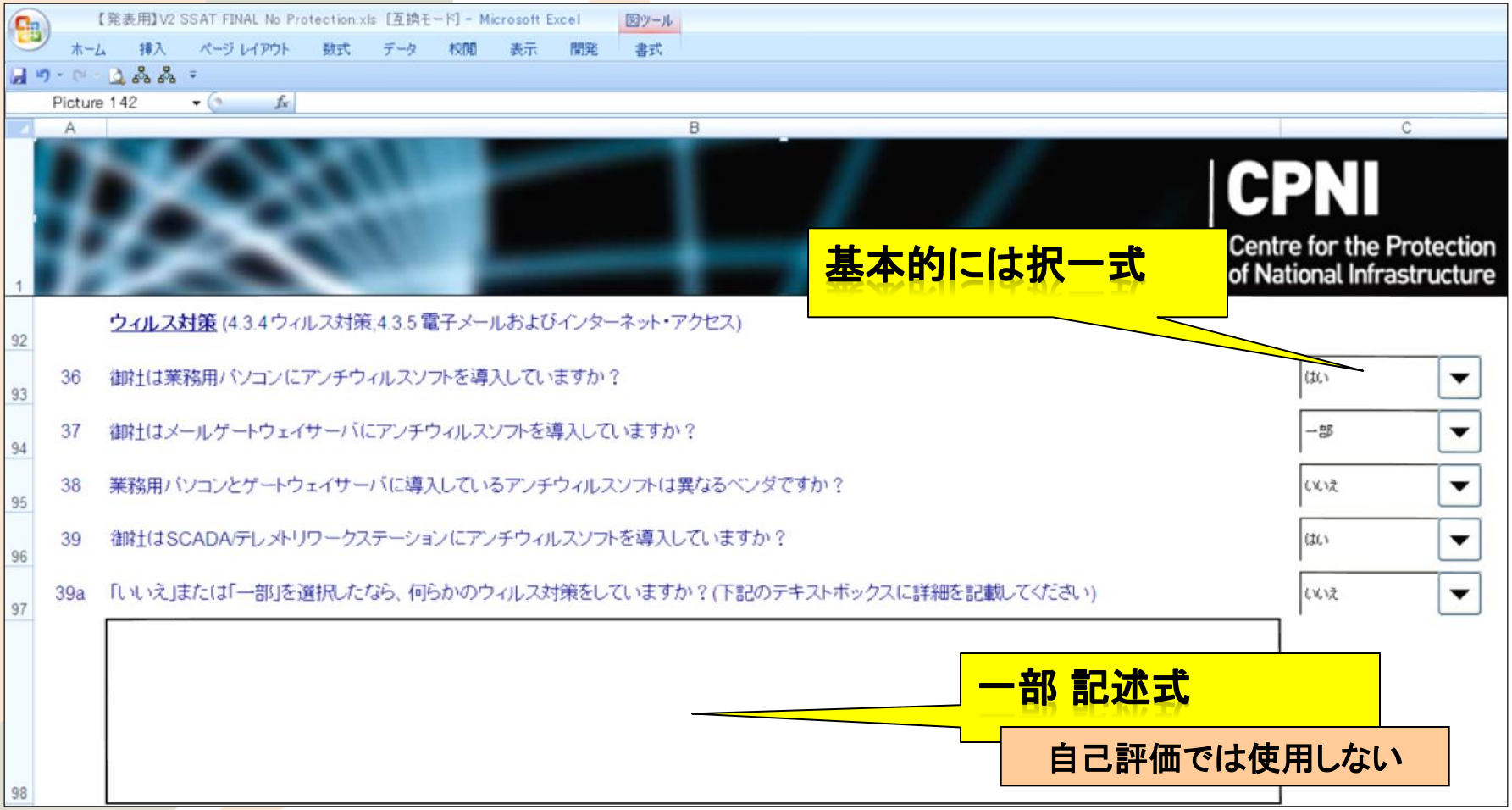
CPNI
Centre for the Protection of National Infrastructure

質問は「CPNI グッドプラクティスガイダンスとコントロールシステムのサイバーセキュリティ調達基準」に基づいて作成しています。

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.cpni.gov.uk/Docs/Overview_of_Process_Control_and_SCADA_Security.pdf
ガイド 1. 事業リスクの理解	http://www.cpni.gov.uk/Docs/Guide_1_Understand_the_Business_Risk.pdf
ガイド 2. セキュア・アーキテクチャの実装	http://www.cpni.gov.uk/Docs/Guide_2_Implement_Secure_Architecture.pdf
ガイド 3. 対応能力の確立	http://www.cpni.gov.uk/Docs/Guide_3_Establish_Response_Capabilities.pdf
ガイド 4. 意識とスキルの改善	http://www.cpni.gov.uk/Docs/Guide_4_Improve_Awareness_and_Skills.pdf
ガイド 5. サード・パーティ・リスクの管理	http://www.cpni.gov.uk/Docs/Guide_5_Manage_Third_Party_Risk.pdf
ガイド 6. プロジェクトへの参画	http://www.cpni.gov.uk/Docs/Guide_6_Engage_Projects.pdf
ガイド 7. 継続した統制の確立	http://www.cpni.gov.uk/Docs/Guide_7_Establish_Ongoing_Governance.pdf
SCADA およびプロセス制御ネットワークにおけるファイアウォールの	http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf
人事セキュリティ対策	http://www.cpni.gov.uk/ProtectingYourAssets/personnelsecurity-268.aspx
コントロールシステムのサイバーセキュリティ調達基準	http://www.us-cert.gov/control_systems/



SSAT (SCADA Self Assessment Tool)



SSAT (SCADA Self Assessment Tool)

- 質問例
  - 択一式（はい、いいえ、一部 など）
    - 御社は業務用パソコンにアンチウィルスソフトを導入していますか？
  - 記述式
    - システム/アプリケーションに最新のパッチを適用していないなら、何らかの対応をしていますか？

SSAT (SCADA Self Assessment Tool)

JEMIMA

評価結果

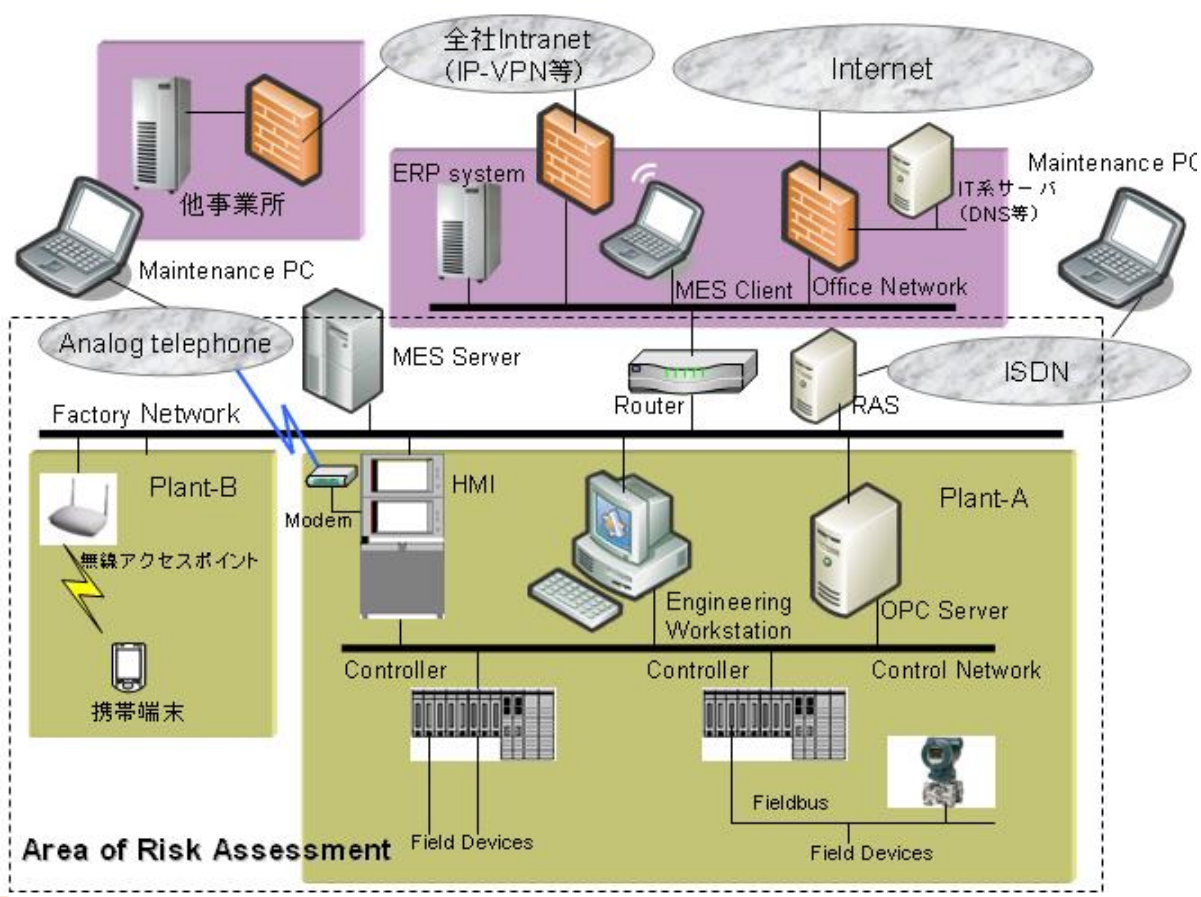
- グットプラクティスガイドの準拠率を3段階で評価
- 関連資料の URL を用意

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.cpni.gov.uk/Docs/Overview_of_F
ガイド 1. 事業リスクの理解	http://www.cpni.gov.uk/Docs/Guide_1_Unde
ガイド 2. セキュア・アーキテクチャの実装	http://www.cpni.gov.uk/Docs/Guide_2_Imple
ガイド 3. 対応能力の確立	http://www.cpni.gov.uk/Docs/Guide_3_Estab
ガイド 4. 意識とスキルの改善	http://www.cpni.gov.uk/Docs/Guide_4_Improve_Awareness_and_Skills.pdf
ガイド 5. サード・パーティ・リスクの管理	http://www.cpni.gov.uk/Docs/Guide_5_Manage_Third_Party_Risk.pdf
ガイド 6. プロジェクトへの参画	http://www.cpni.gov.uk/Docs/Guide_6_Engage_Projects.pdf
ガイド 7. 継続した統制の確立	http://www.cpni.gov.uk/Docs/Guide_7_Establish_Ongoing_Governance.pdf
SCADA およびプロセス制御ネットワークにおけるファイアウォールの	http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf
人事セキュリティ対策	http://www.cpni.gov.uk/ProtectingYourAssets/personnelsecurity-268.aspx
コントロールシステムのサイバーセキュリティ調達基準	http://www.us-cert.gov/control_systems/

評価対象のモデルシステム

評価対象のモデルシステム

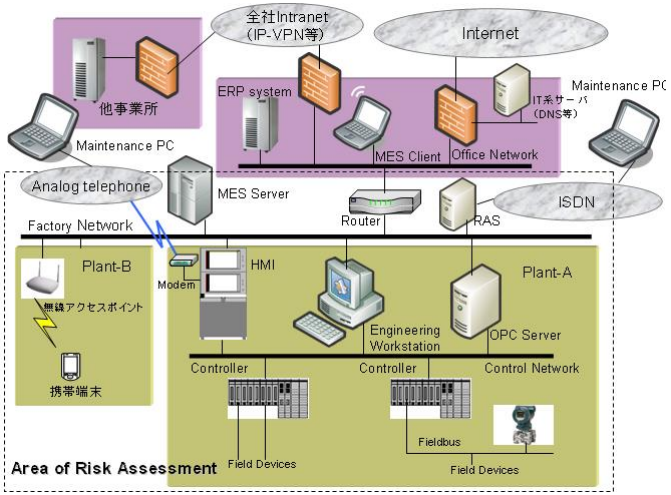
WGメンバーが検討し、今回ツールを適用した一般的な生産制御システム例



評価手順と評価結果

評価手順

- モデルシステムの想定に従いセキュリティ評価を試行
  - 設問は 8分野, 99問
    - 「はい」「いいえ」「一部」の選択式
  - 回答所要時間は4時間程度
    - 試行では確認作業が無いため短時間で完了
    - 実際の評価では1日～数日かかると思われる
  - 各メンバーの回答を持ち寄りWGで討議
    - メンバーは生産制御システム関係者が中心
    - モデルシステムの想定に合った回答を作成



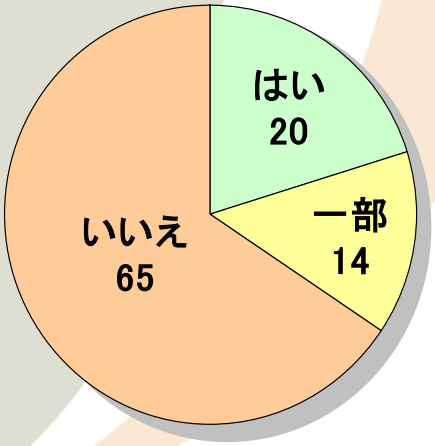
評価に用いたモデルシステム

	A	B	J	K	L	M	N
1	SSAT	回答リスト（全体）					
2		質問がわかりづらい場合や誤字・脱字がある場合にはその旨を備考欄に記載してください		A委員	A委員	B委員	B委員
3							
4	質問番号	質問	全体意見	回答 (改善しやすい質問項目に対して、改善前の評価と改善後の評価を記入する) 例：いいえ→はい	改善するための手段例 (これをやれば評価をアップすることができる例を記載)	回答 (改善しやすい質問項目に対して、改善前の評価と改善後の評価を記入する) 例：いいえ→はい	改善するための手段例 (これをやれば評価をアップすることができる例を記載)
102	物理的セキュリティ（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 - 4.3.8 物理的セキュリティ）						
103	64	御社はプロセス制御システムと関連するネットワーキング装置を、物理的攻撃や内部の不正アクセスから守るため、物理的なセキュリティ保護対策を講じていますか？	一部	一部	**難易度：中** 物理セキュリティ施策を実施する(セキュリティ区画およびラックの施錠など)	一部	
104	65	SCADA/テレメトリネットワークのサーバ・装置の専属スタッフがサポートするために訪問することはありますか？ また、サーバ・機器がIT企業の機器と同じセキュリティルームに設置してているのであれば、機器の違いはすべてのスタッフが理解していますか？	いいえ→はい ◇貼り紙をする	いいえ→はい	**難易度：低** SCADA関連装置など重要機器に**注意喚起の表示**を貼付する	いいえ	

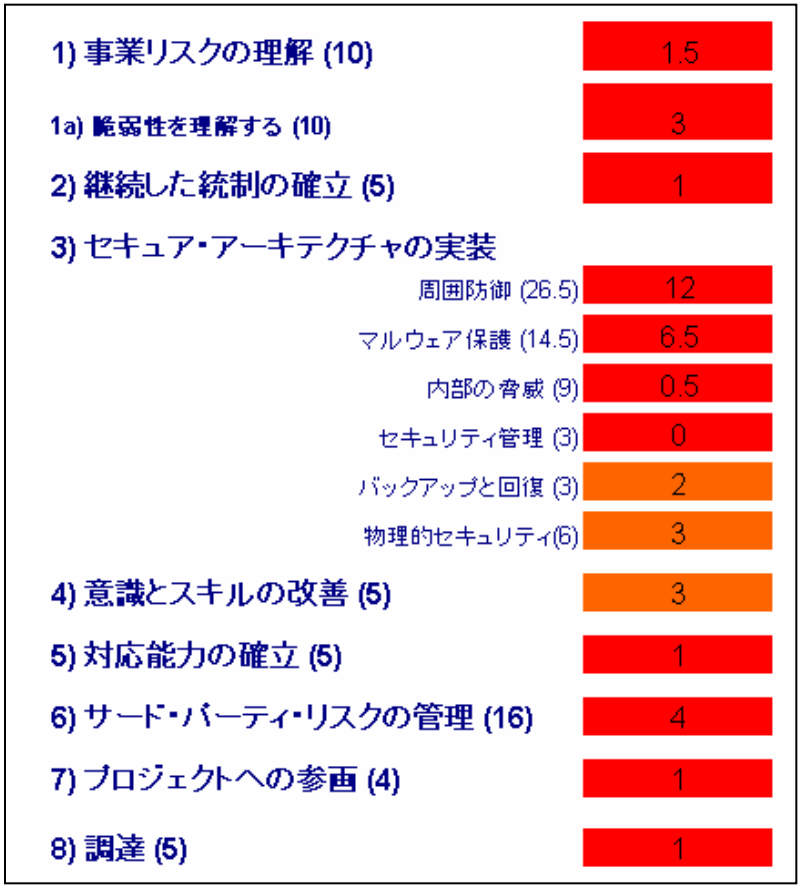
各メンバーの回答例

評価結果（概要）

- **評価基準**
  - 「はい」　→ 適切な状態
  - 「いいえ」　→ 不適切な状態
  - 「一部・時々」　→ 中間的な状態
- **モデルシステム評価結果**
  - 99問中「はい」が20個
    → セキュリティ上好ましくないという結果
  - 全体的に低いスコア

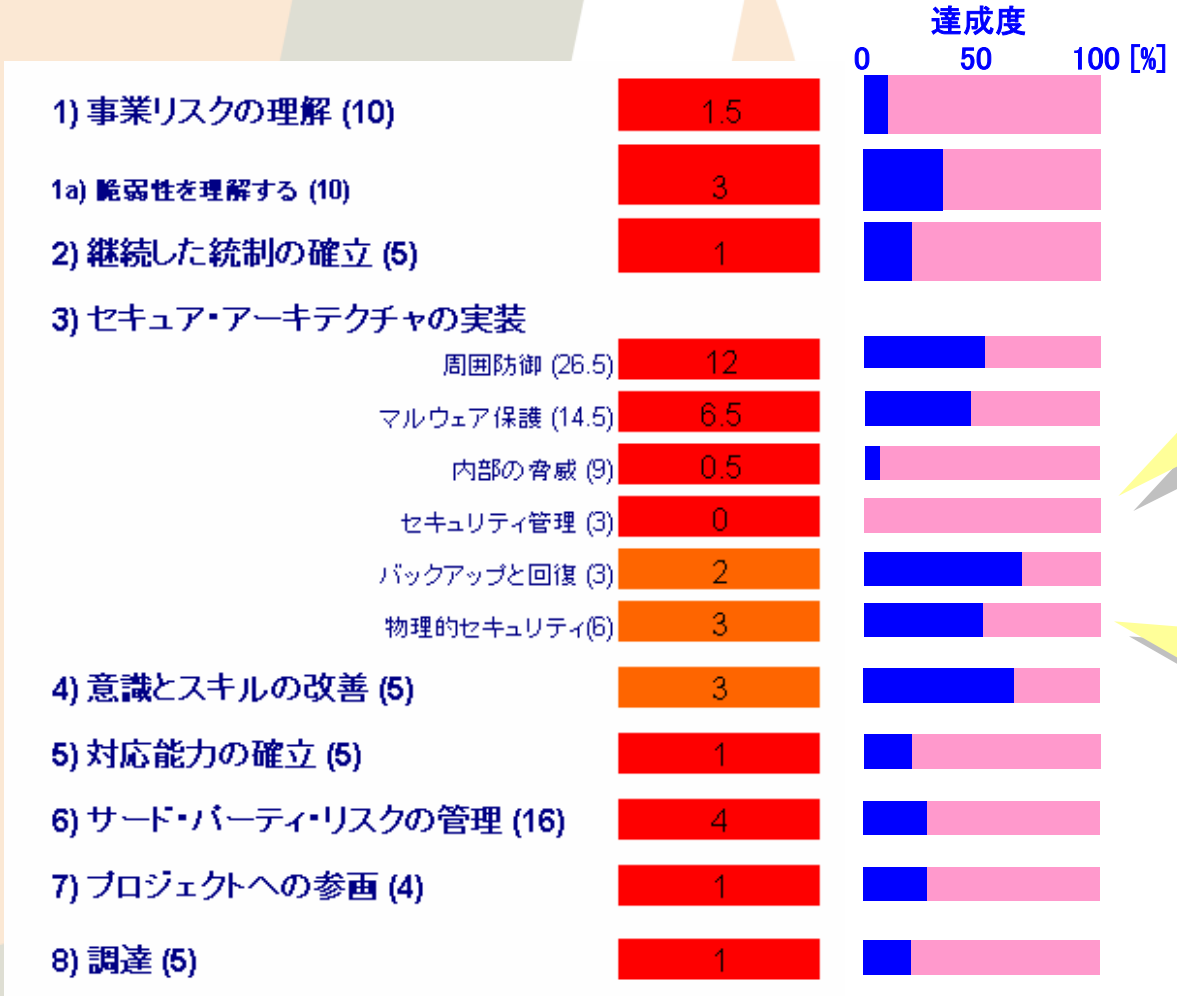


モデルシステム評価での回答（N=99）



SSAT評価結果出力

評価結果（分類別）



セキュリティ管理，
リスク評価
関係の項目は
達成度が低い

バックアップ，
マルウェア保護，
物理セキュリティ
関係の項目は
達成度が高い

SSAT評価結果と達成度

モデルシステム評価の感想・所見

- モデルシステム評価結果について
  - 99問中「はい」が20個 → セキュリティ上好ましくない
  - 簡単に改善できそうな項目もあった
    - 本来必要である文書・記録を整備すればよいもの
      - （例）「設問50. SCADA/テレメトリネットワークシステムのパスワードの強度と有効期限を含むパスワード・ポリシーは文書化されていますか」
    - 既存の組織・担当者に役割を追加すればよいもの
      - （例）「設問10. 御社はSCADA/テレメトリシテムのセキュリティに対して責任を持つ専用のチームまたは個人がいますか」
    - 本来必要である評価・確認を行えば良いもの
      - （例）「設問16. 過去12ヶ月以内にファイアウォールの設定を審査していますか」
    - 外部に依頼すれば済むもの
      - （例）「設問79. 御社は現在のセキュリティシステムに対するセキュリティ手引きと、将来のシステム開発対するセキュリティロードマップを提供するようにベンダに要求していますか」

簡単に改善できそうな項目に対応した場合、評価結果はどれくらい改善できるだろうか？
簡単に改善できない項目にはどのようなものがあるだろうか？
改善のためには何が必要となるのだろうか？

評価結果にもとづく改善

評価結果にもとづく改善

- 目的
  - セキュリティ向上のための改善方法を模索する
  - 簡単に改善できる項目がどれくらいあるのかを把握する
    - どうすれば改善できるのか改善方法の案を作成する
  - 簡単には改善できない項目がどれくらいあるのかを把握する
    - 何が改善の障害になっているのか検討する
- 方法
  - モデルシステム評価で「はい」以外の回答になった79項目の設問について各メンバーの改善案を持ち寄りWGで検討
  - 「簡単に改善できそうな」項目を抽出
    - 本来必要である文書・記録を整備すればよいもの
    - 既存の組織・担当者に役割を追加すればよいもの
    - 本来必要である評価・確認を行えば良いもの
    - 外部に依頼すれば済むもの
    - 低い金銭的・人的コストで改善できるもの
  - 改善方法の案を作成
  - 改善後にセキュリティ評価ツールで再評価し効果を確認

改善案の作成

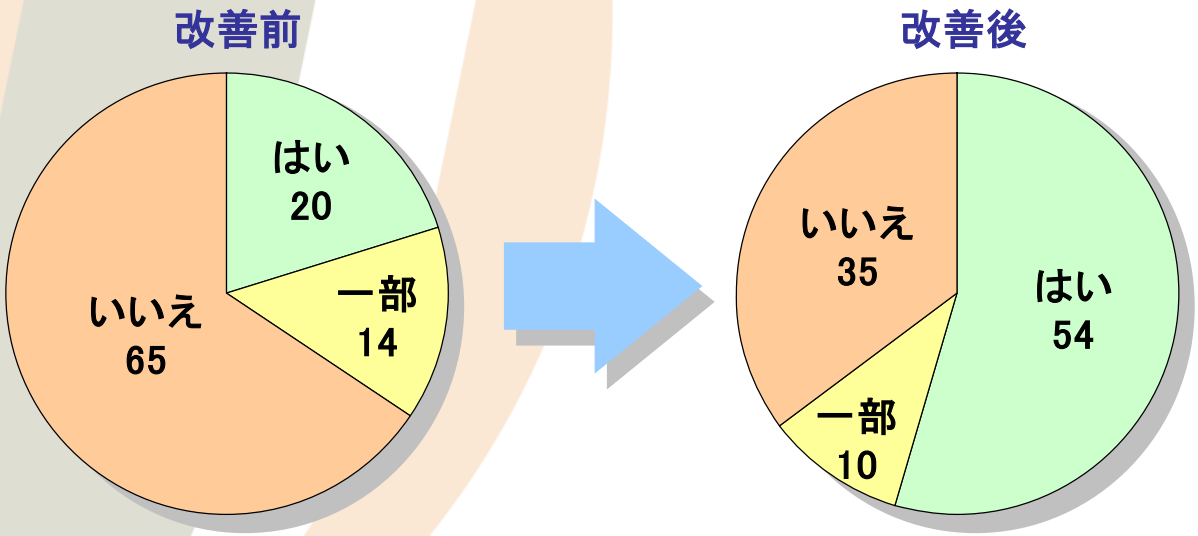
- モデルシステム評価で「はい」でなかった項目について
  - WGで改善できそうな項目を抽出して改善案を作成
  - 改善結果に基いて再評価を実施

2		質問がわかりづらい場合や誤字・脱字がある場合にはその旨を備考欄に記載してください		A委員	A委員	B委員	B委員
3 4	質問番号	質問	全体意見	回答 (改善しやすい質問項目に対して、改善前の評価と改善後の評価を記入する) 例: いいえ→はい	改善するための手段例 (これをやれば評価をアップすることができる例を記載)	回答 (改善しやすい質問項目に対して、改善前の評価と改善後の評価を記入する) 例: いいえ→はい	改善するための手段例 (これをやれば評価をアップすることができる例を記載)
102	物理的セキュリティ (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 - 4.3.8 物理的セキュリティ)						
103	64	御社はプロセス制御システムと関連するネットワーキング装置を、物理的攻撃や内部の不正アクセスから守るため、物理的なセキュリティ保護対策を講じていますか？	一部	一部	**難易度:中** 物理セキュリティ施策を実施する(セキュリティ区画およびラックの施錠など)	一部	
104	65	SCADA/テレメトリネットワークのサーバ・装置の専属スタッフがサポートするために訪問することはありますか？ また、サーバ・機器がIT企業の機器と同じセキュリティルームに設置してているのであれば、機器の違いはすべてのスタッフが理解していますか？	いいえ→はい ◇貼り紙をする	いいえ→はい	**難易度:低** SCADA関連装置など重要機器に**注意喚起の表示**を貼付する	いいえ	
104		いはすべてのスタッフが理解していますか？					

改善案検討例

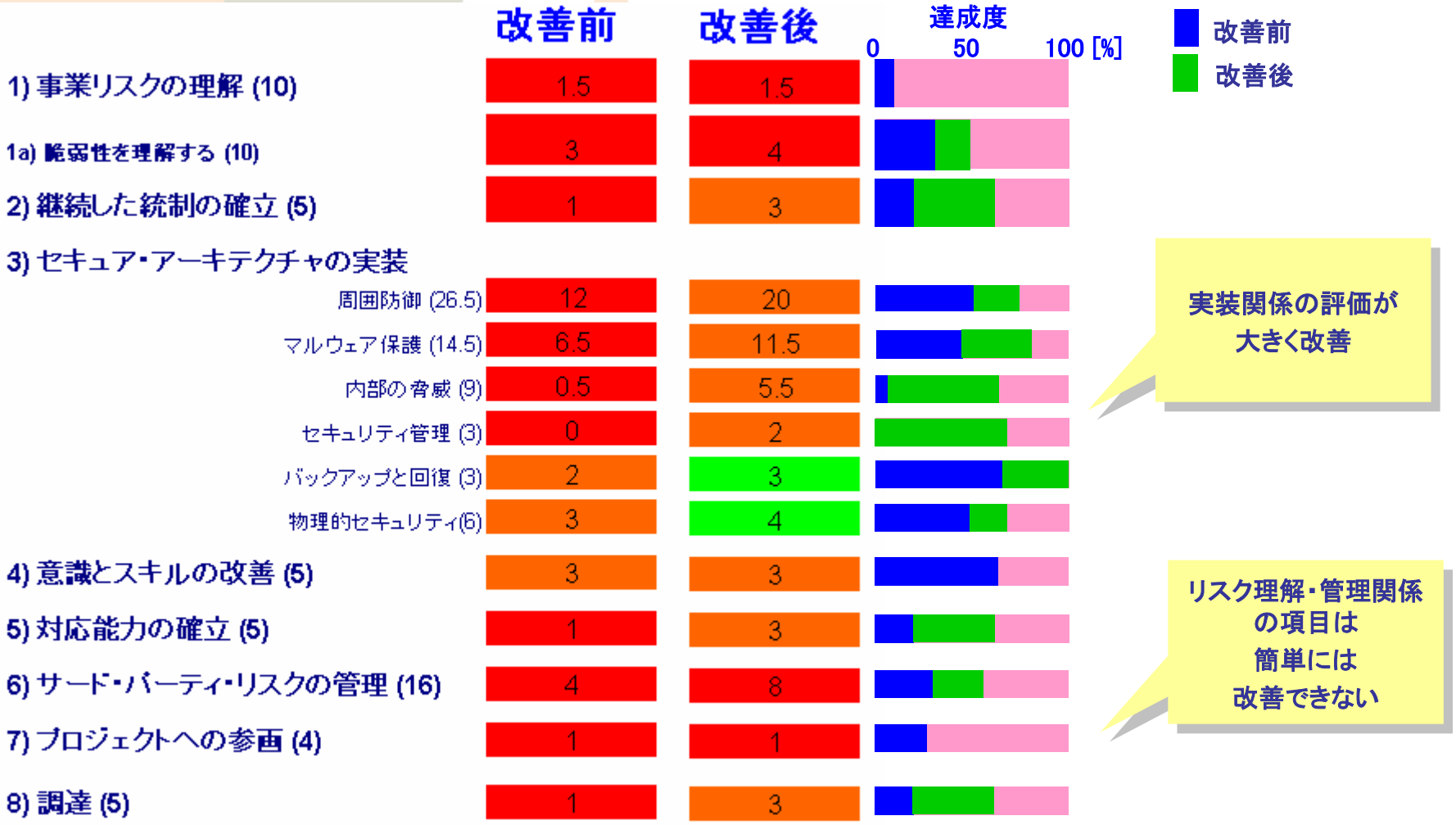
改善結果（概要）

- 改善結果
  - 「はい」以外の回答であった79項目のうち、34項目について改善案を作成した
  - 「はい」回答の数が、20項目から54項目に改善された



改善前と後の回答数

改善後の評価結果（分類別）



改善前と後の評価結果

改善案まとめ

- 簡単な改善で6割の要件を満たすことができた
  - 本来あるべき文書や手順をしっかり整備することが重要
- しかし4割の要件は満たすことができなかった
  - 改善の障害となる要因として、ユーザ側(内的要因)とSSAT側(外的要因)とがあった
- ユーザ側の要因（内的要因）
  - 関係者の協力を得るのが困難に思われた
    - （例）「設問89：御社はすべてのサポート組織に定期的なセキュリチェック・評価を実施していますか」
  - 人的・金銭的コストがかかるため簡単とは言えないと思われた
    - （例）「設問78a：脆弱性公開プロセスをベンダが提供しているなら、御社はこのプロセスに従う/情報提供を受けることを保証しますか」
  - 改善のためには施設や業務を大きく変更する必要があると思われた
    - （例）「設問35：御社はSCADA/テレメトリシステムでワイヤレスネットワーキングを展開しないことを定めていますか」
      → すでに使用している場合は大きな設備変更が必要
- SSAT側の要因（外的要因）
  - 難解な設問があった
    - （例）「設問8：上級管理者はSCADA/テレメトリセキュティに関する責任を経営陣による支援で確実なものとしていますか」
      → 具体的に何を行なっていれば「はい」と回答できるのかわからないと回答できない
  - 要件を満たすための具体的な施策内容がわからなかった
    - （例）「設問98：御社はすべてのサポート組織に定期的なリスク評価とセキュリティチェック・評価をしていますか」
      → 要件を満たすためには具体的に何をすれば良いのかわからない

残りの要件を満たすためにはどうするべきかを検討するのが今後の課題

セキュリティ評価ツールの感想・所見

セキュリティ評価ツールの感想・所見

- SSATについての感想
  - 手軽に評価ができた
    - 評価ツールや，資料となるグッドプラクティスともに日本語版が提供されている
    - 選択式で回答しやすく、設問数も99と少なめ
    - MS Excelのマクロですぐに結果が出る
  - 評価しながらグッドプラクティスでの要求事項が一覧できた
    - グッドプラクティスの概要を知るには良い資料
  - 網羅性がありバランスが良い設問内容だった
    - 管理やシステムを含む広範囲をカバーする設問
    - 偏りがちなセキュリティ施策のバランスをチェックするのにも有用
  - 難しい設問もあった
    - 用語の意味が難しい設問もあった
      - （例）「設問51. 御社は特殊なパスワードポリシーですか？」
→「特殊なパスワードポリシ」の意味がわからないと回答できない
    - 内容が抽象的で判定が難しい設問もあった
      - （例）「設問8. 上級管理者はSCADA/テレメトリセキュティに関する責任を経営陣による支援で確実なものとしていますか」
→ 具体的に何を行なっていれば「はい」と回答できるのかわからないと回答できない

セキュリティ評価ツールSSATは十分利用できる内容
表記の改善や説明を追加をすればより使いやすくなる

まとめと今後の課題

まとめと今後の課題

- まとめ
  - セキュリティ評価ツールは生産制御システムのセキュリティ向上に有用
    - セキュリティ上の問題点を手軽に抽出できる
    - 簡単に改善できる項目も多い　→　即効性がある！
    - バランスの良いセキュリティ施策の検討に使える

  セキュリティ評価ツールを生産制御システムのセキュリティ向上のために活用したい

- 今後の課題
  - 改善を支援するための施策を検討
    - セキュリティ評価ツールの改良提案
      - わかりやすい用語への置換
      - わかりやすい表現への置換
      - 解説・例示の追加
      - 改善案を日本語版提供元のJPCERT/CCへ提案
    - 改善ガイドの作成
      - 改善のため施策例を提案（本WGで提案した"Good Practice"を活用）
      - 改善のための参考資料を紹介

全体のまとめ

- セキュリティ評価ツールやガイドラインなどを活用して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。

参考情報

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/CC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

- SSAT和訳版 問い合わせ先（JPCERT/CC）：

  cs-security-staff@jpcert.or.jp