セキュリティ評価ツールの取り組み

2011.2.10

(社)日本電気計測器工業会
PA･FA計測制御委員会
セキュリティ調査研究WG
新井 貴之

セキュリティ調査研究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**
  ㈱東芝、㈱日立製作所、㈱日立ハイテクコントロールシステムズ
  ㈱富士電機システムズ、㈱山武、横河電機㈱（50音順）
- **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

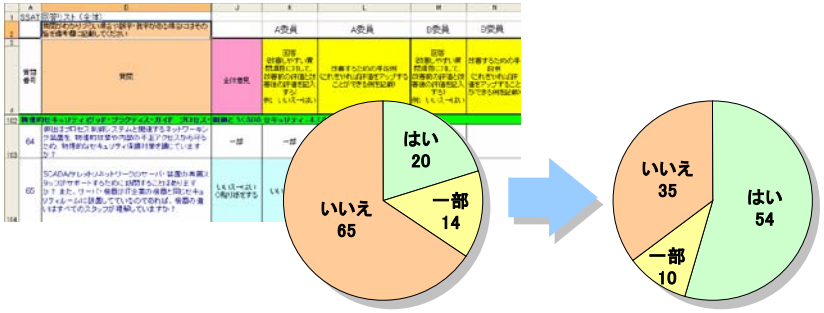
セキュリティ調査研究WGのご紹介

- **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国内委員会メンバ

- **広報活動**
  - JEMIMA 委員会セミナー，計測展
  - JPCERT制御システムセキュリティカンファレンス
  - 日本能率協会 計装制御技術会議
  - SICE Annual Conference

本日の内容

- 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
  - セキュリティ評価ツールの改良
    - 改良案の作成
    - 改良結果
  - 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検査

- 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？

セキュリティ評価ツールSSAT

- 方法
  - モデルシステムの想定に基いて各委員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?
  - 各委員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

WGメンバーで検討

セキュリティ評価ツール SSATの紹介

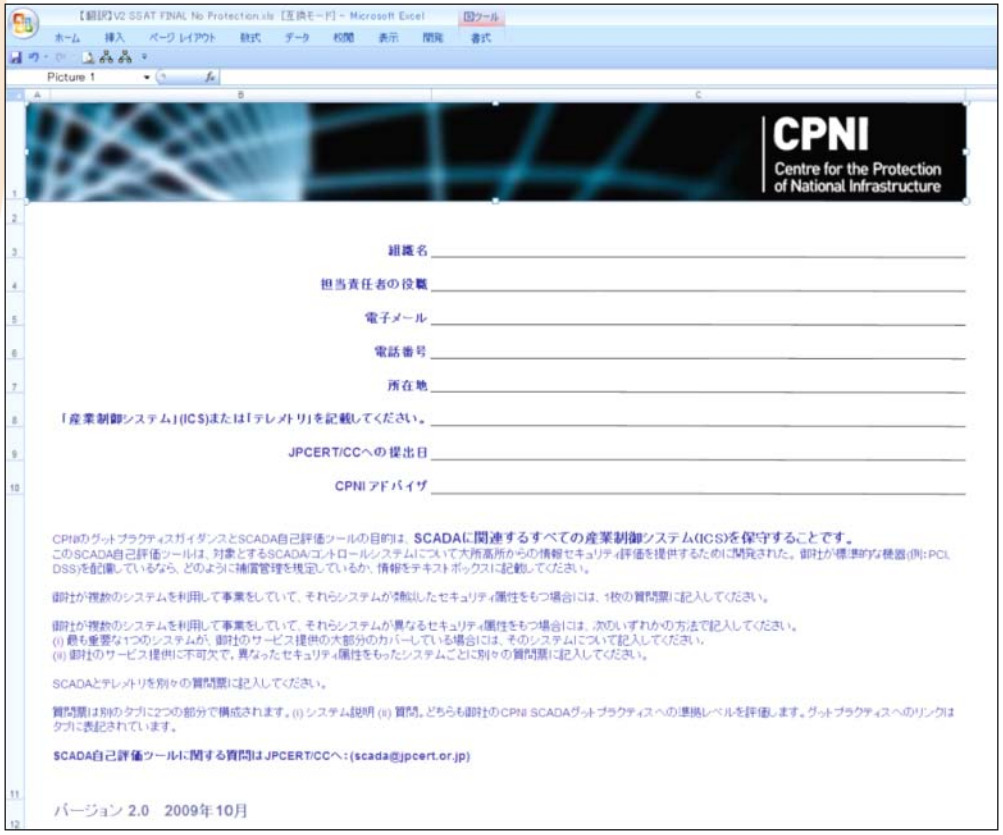
SSAT (SCADA Self Assessment Tool)

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

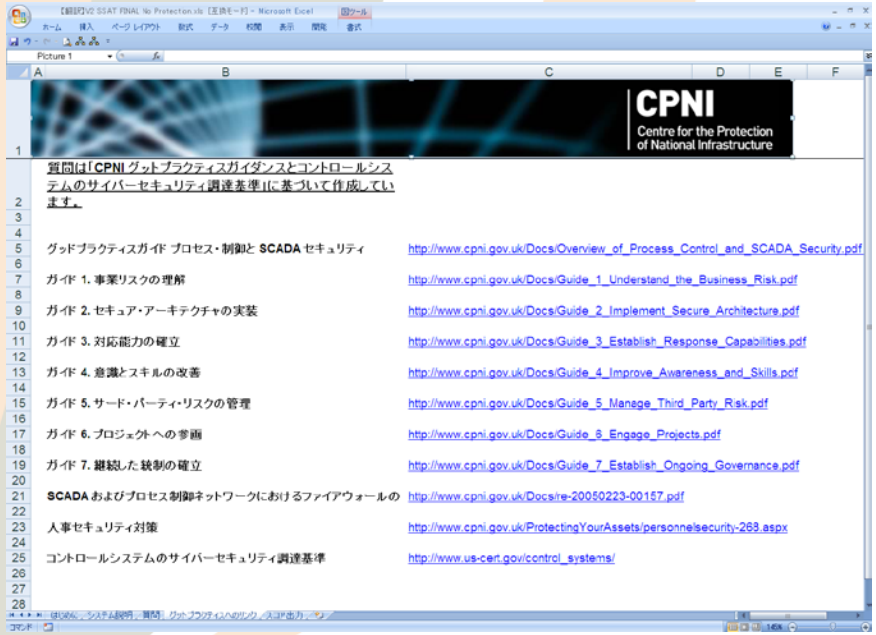
特徴は？

- 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)

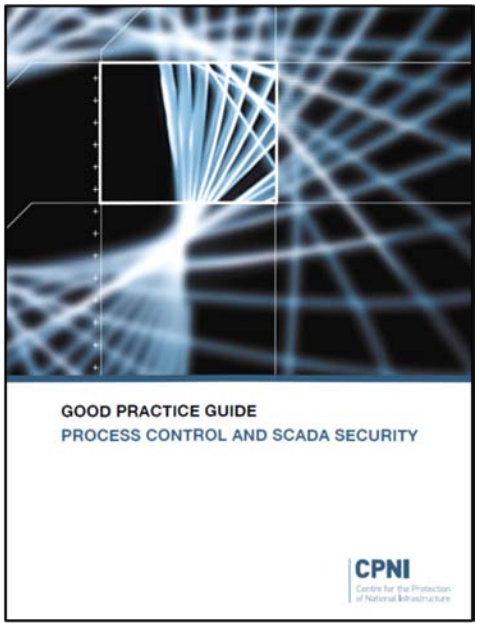
- **セキュリティ基準は CPNI が公開しているグッド・プラクティス・ガイド「 プロセス・制御と SCADA セキュリティ 」**
  - グッド・プラクティスはいくつかのガイドに分かれている
  - 最新版(2009/10 ver 2.0)はファイアウォールと人事セキュリティ基準を追加



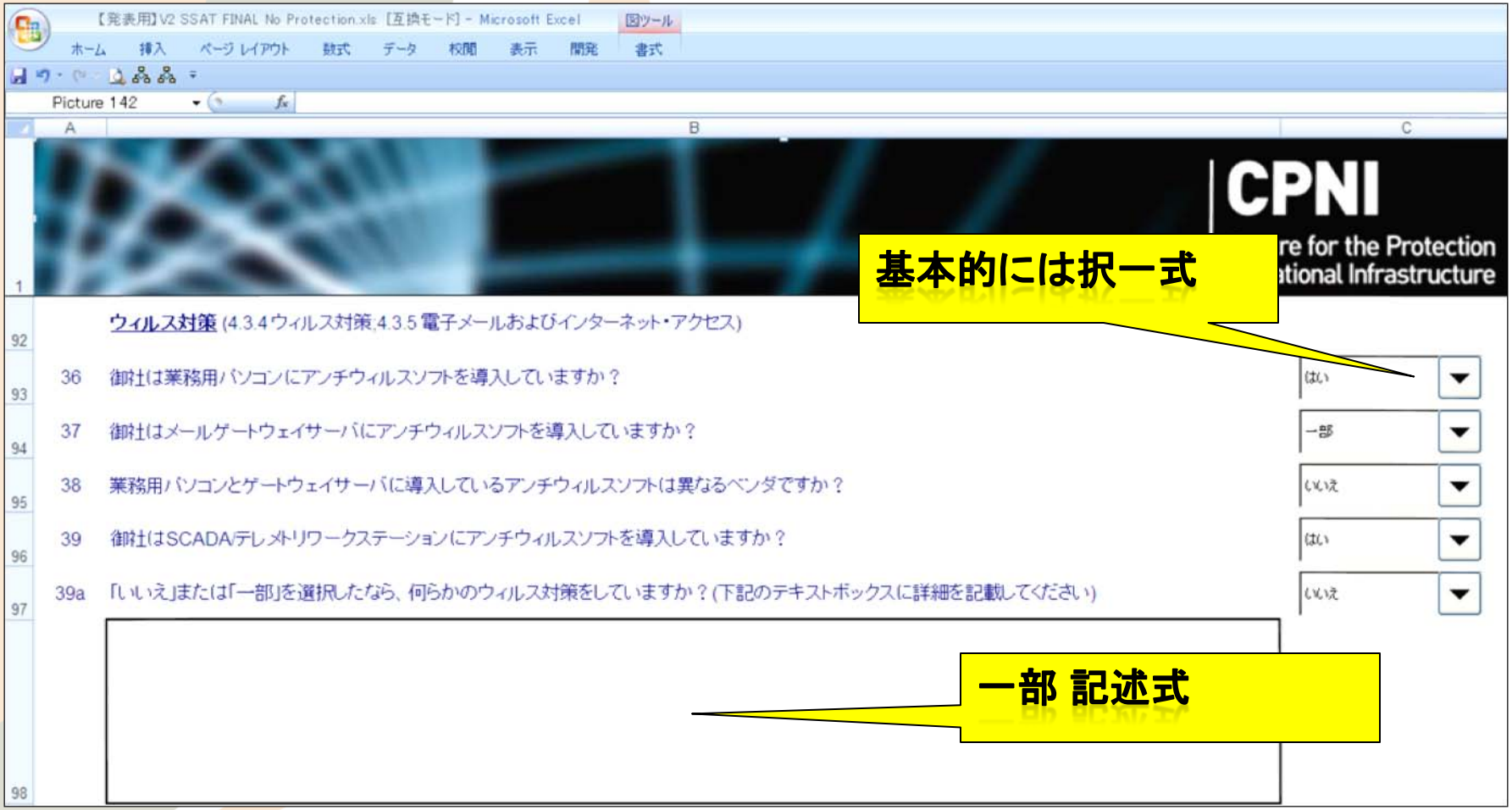
CPNI
Centre for the Protection of National Infrastructure

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)

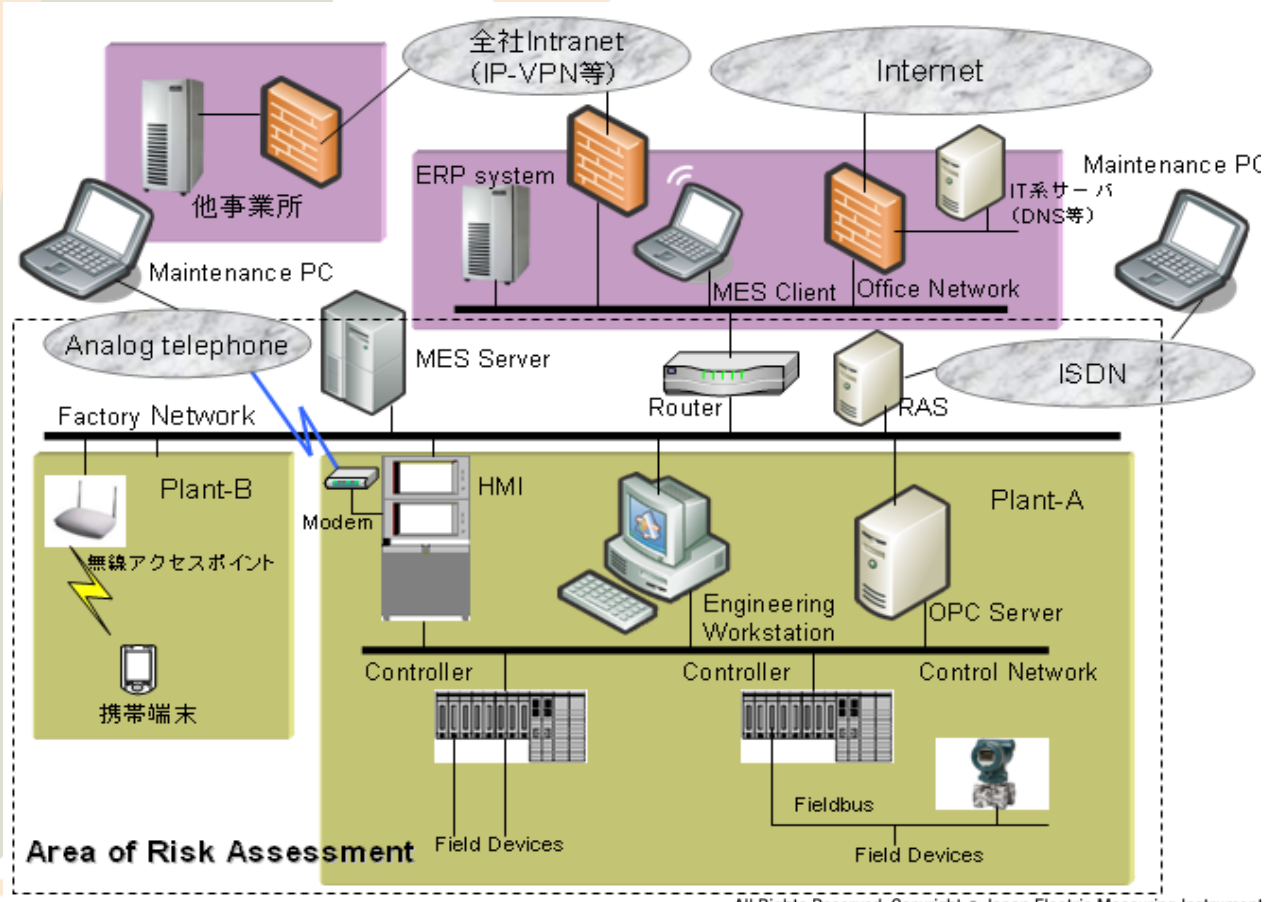
- **評価結果**
  - グットプラクティスガイドの準拠率を3段階で評価
  - 関連資料の URL を用意

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_Estal
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

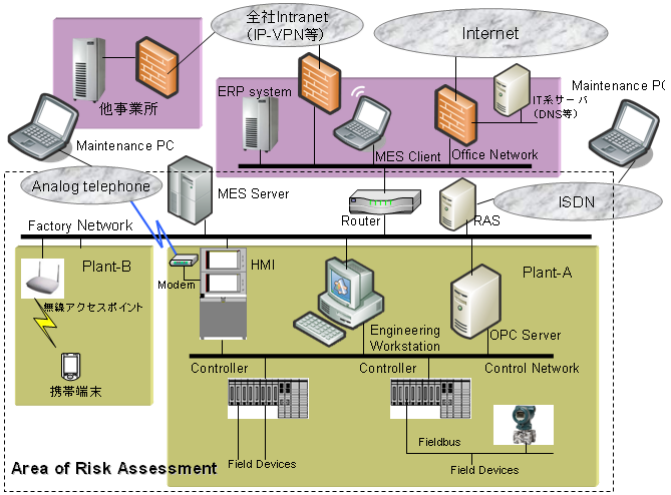
WGメンバーが検討し、今回ツールを適用した一般的な生産制御システム例



評価手順と評価結果

評価手順

- システムモデル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
    - 実際の検査では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



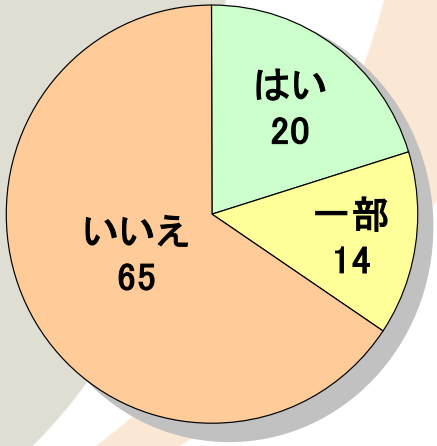
評価に用いたモデルシステム

	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	

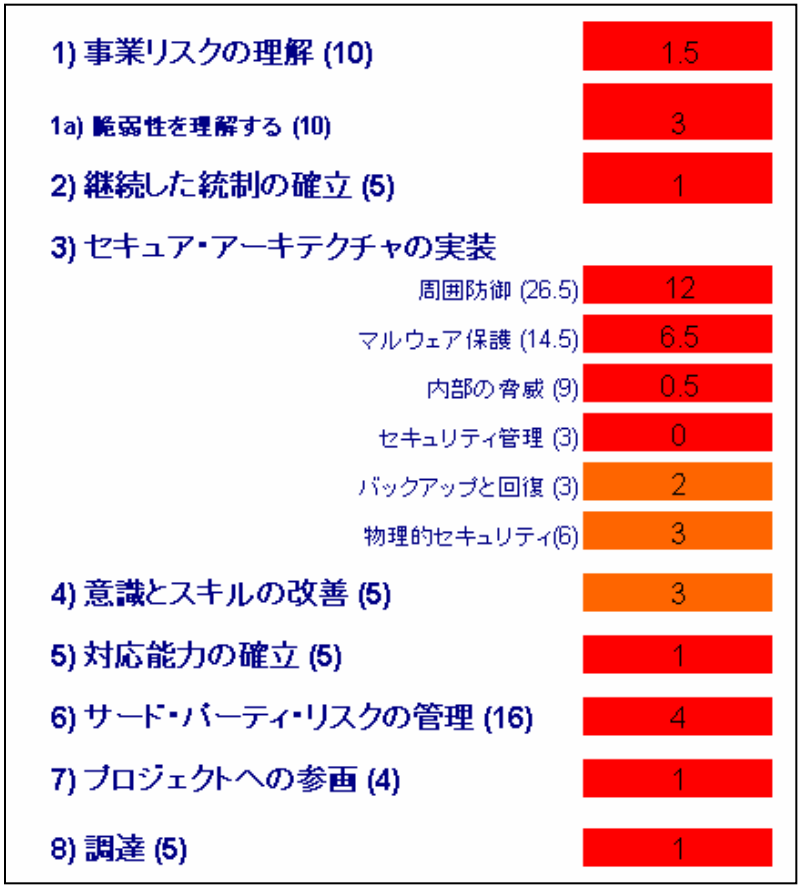
各委員の回答例

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
- 試行評価結果
  - 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

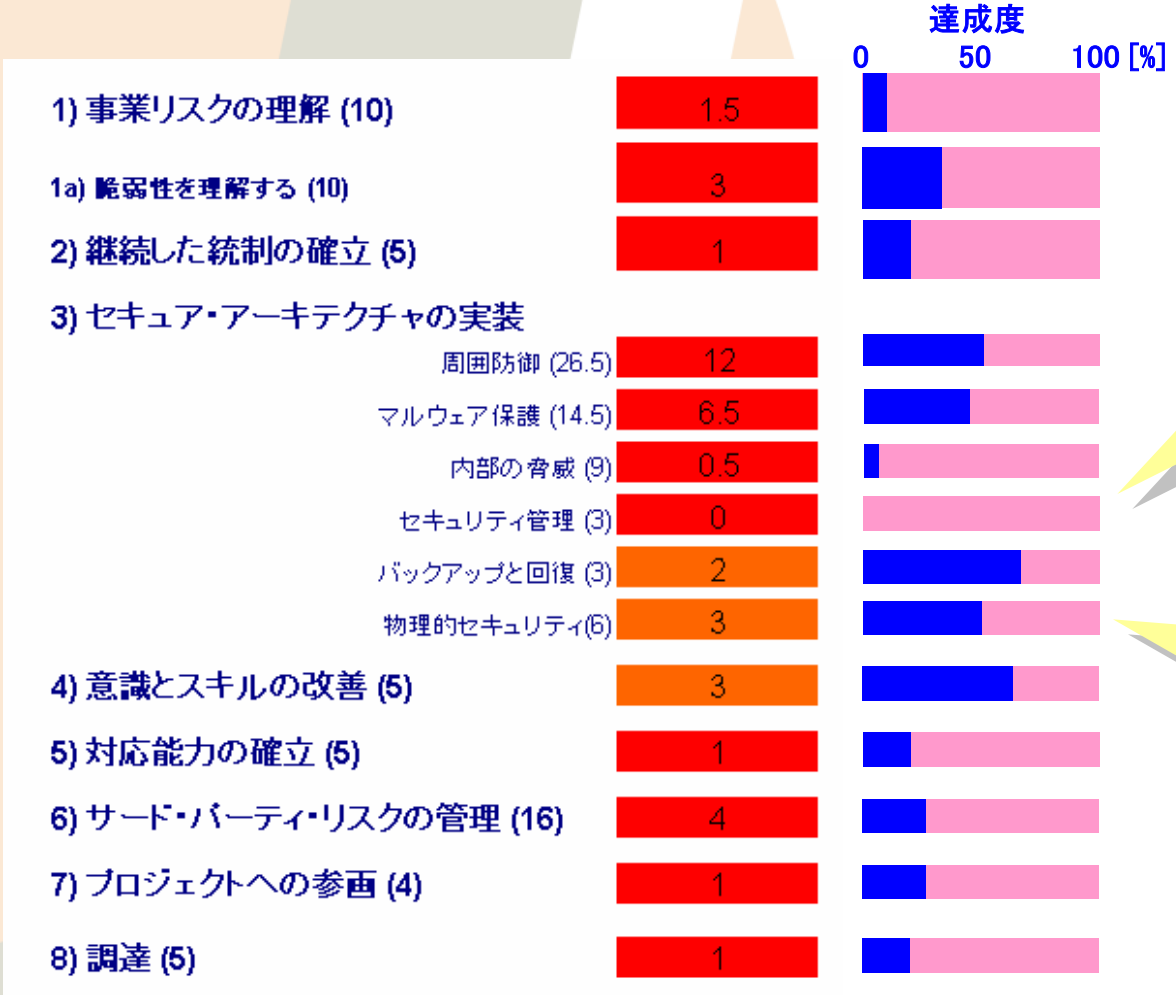


モデル評価での回答（N=99）



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

システムモデル評価の感想・所見

- システムモデル評価結果について
  - 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/テレメトリシス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」
    - 本来必要である検査・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
    - 本来必要である検査・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

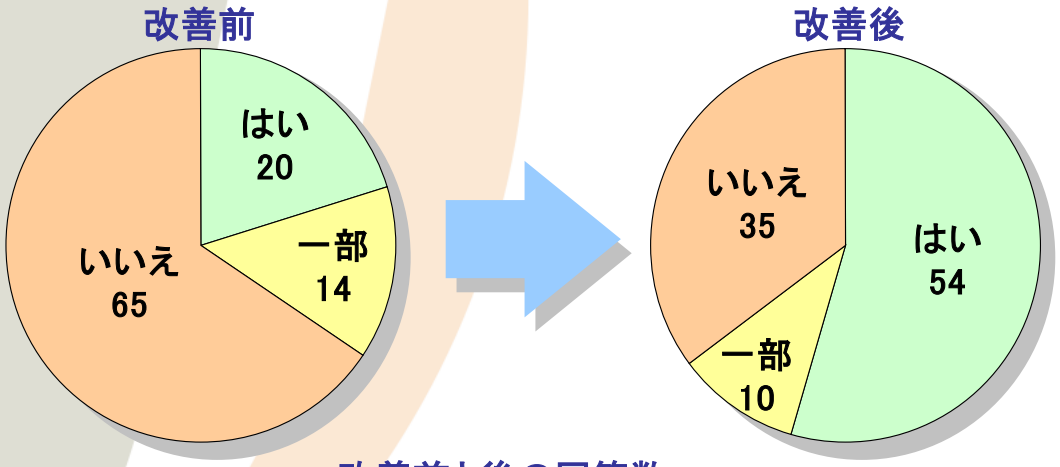
- システムモデル検査で「はい」でなかった項目について
  - WGで改善できそうな項目を抽出して改善案を作成
  - 改善結果に基いて再検査を実施

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

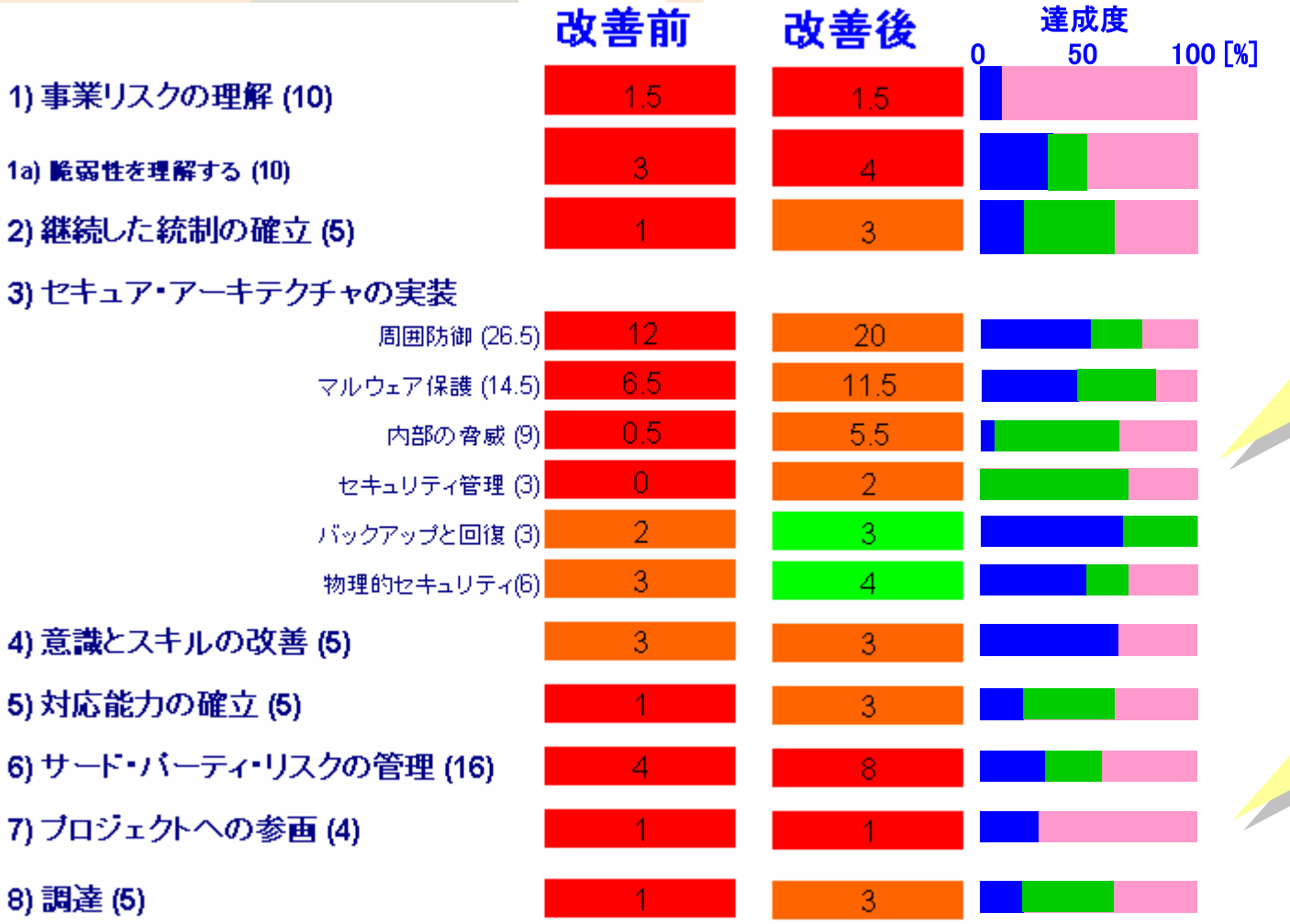
改善結果（概要）

- 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

改善後の検査結果（分類別）



実装関係の評価が
大きく改善

リスク理解・管理関係
の項目は
簡単には
改善できない

改善前と後の評価結果

改善できなかった項目の例

- 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・検査を実施していますか」
      → 全ての関係者にセキュリティチェックを行なうのは困難かも
  - 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」
      → 全てのサービスを受けるのは金銭的に困難かも
  - 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・検査をしていますか」
      → 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

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）
  - ユーザ側の都合で要件を満しづらいと思われる設問があった
    - 関係者の協力を得るのが困難に思われた
    - 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
    - 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
- SSAT側の要因（外的要因）
  - SSATの用語や表現が難しく「はい」と回答しづらいと思われる設問があった
    - 難解な設問があった
    - 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

設問の用語や表現を改良すれば、より多くの項目が改善できそう

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
  - 検査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）「御社は特殊なパスワードポリシーですか？」
    - 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」

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

セキュリティ評価ツールの改良提案

改良案の作成

- 目的
  - セキュリティ評価ツールSSATの用語や表現を改良してより使いやすくする
- 方法
  - 各委員がSSATの文面をチェックし改良点をリストアップ
    - 生産制御システムユーザやベンダの視点で用語や表現をチェック
  - 改良点を持ち寄り委員会で検討
    - 生産制御システムユーザやベンダの視点で内容を吟味
    - JPCERT/CC担当者も交えて検討
  - 改良案をJPCERT/CCに提案
  - JPCERT/CCでSSAT改訂版を作成
  - 改訂版を再検討

WGメンバーで検討

3 4	質問番号	質問	旧版への備考	V3の備考（A委員）	V3の備考（B委員）	V3の備考（C委員）	V3の備考（D委員）	V3の備考（E委員）
35	8	上級管理者はSCADA/テレメトリセキュリ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？	▼判定基準がわからない ▼文面がわかりづらいかも	上級管理者は経営陣の承認のもとでSCADA/テレメトリセキュリティに関する責任を明確にしていますか？	経営者は、SCADA/テレメトリセキュリティに関する安全管理責任者を任命し、確実に運営できるようにしているか？（意味通じる？）	上級管理者（プロジェクト責任者、施工管理者）	上級管理者　の範囲は？	
36	9	御社の経営者メンバーはSCADA/テレメトリセキュリティに関する日々の責任を明確にしていますか？	▼判定基準がわからない ▼文面がわかりづらいかも	▼明確にする＝文書化する？				

SSAT改良検討例

改良結果

- 結果
  - 検討→提案→改訂版検討のサイクルを4回実施
  - SSATの85%の設問について改良案を作成
    - わかりやすい用語への置換
      - （例）タンパー警報装置 → 侵入警報装置
    - わかりやすい表現への置換
      - （例）疑わしいセキュリティインシデント → セキュリティ上の異常と思われる事態
    - 「誰が」「何をする」の明確化
      - （例）御社は → 安全管理責任者は
    - 解説・例示の追加
      - （例）すべてのサードパーティー
        →すべてのサードパーティー（ベンダ、サポート組織、サプライチェーン内の他の関係者）
  - 改善例（設問61）
    - 完全復旧プロセスでバックアップの完全性をテストをしていますか？
      → 運用責任者はシステム機能の完全な回復を想定としたバックアップを行ない、
      定期的にバックアップデータの完全性テストを行なっていますか？

改良版セキュリティ検査ツールは「SSAT監修版」として
JPCERT/CCから生産制御システム関係者向けに近日公開予定
ぜひご利用ください！

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
  - 生産制御システムのセキュリティ改善を支援するための施策を検討
    - 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
    - セキュリティ関連規格/ガイドラインの調査
      - 「セキュリティ俯瞰マップ」の拡充

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

JEMIMA セキュリティ調査・研究WGは、
今後も生産制御システムのセキュリティを
どのようにして高めていくかを追い求め、
その結果が、ユーザ様、会員企業様のお
役に立つよう活動してまいります。

本日は、ありがとうございました。