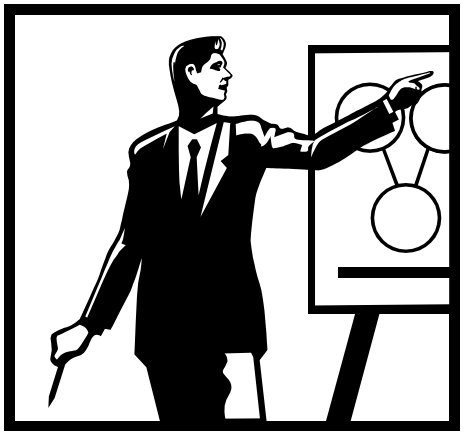
制御システム
セキュリティ評価ツールの紹介

2010年 2月9日

JPCERT コーディネーションセンター
情報流通対策グループ
成田　広樹

本日のアジェンダ

- SSAT (SCADA Self Assessment Tool) の紹介
- CSET (Cyber Security Evaluation Tool) の紹介
- SSAT と CSET の比較
- 質疑応答

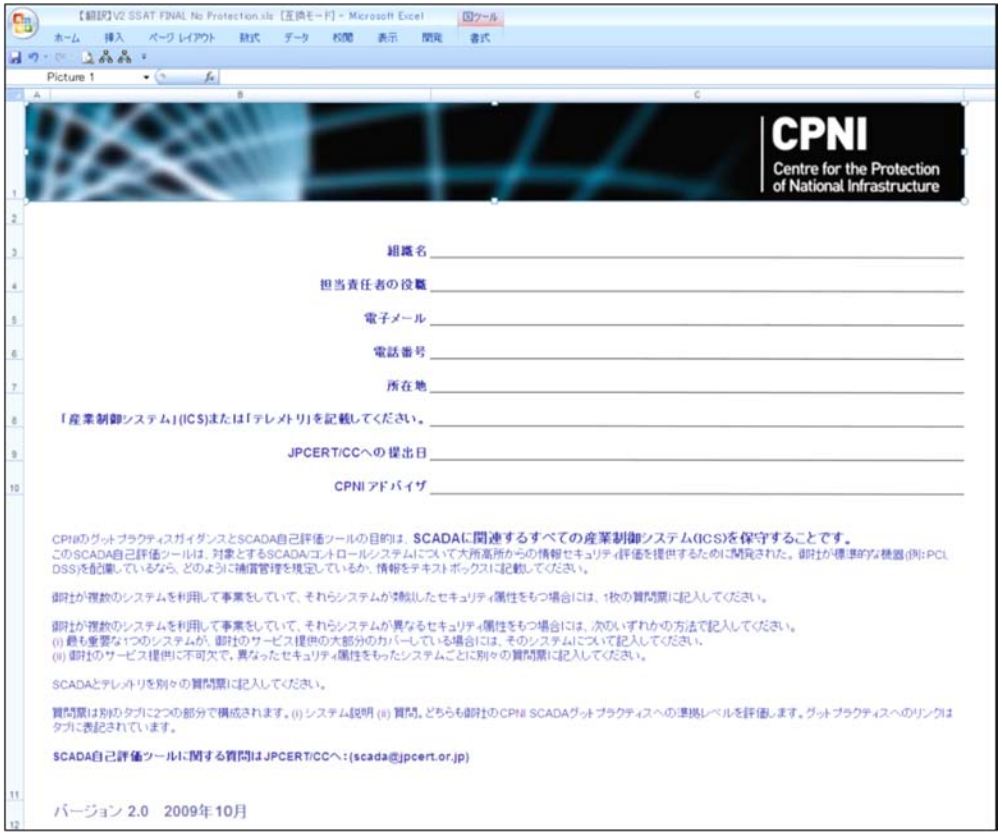


SSAT (SCADA Self Assessment Tool)

JPCERT CC®

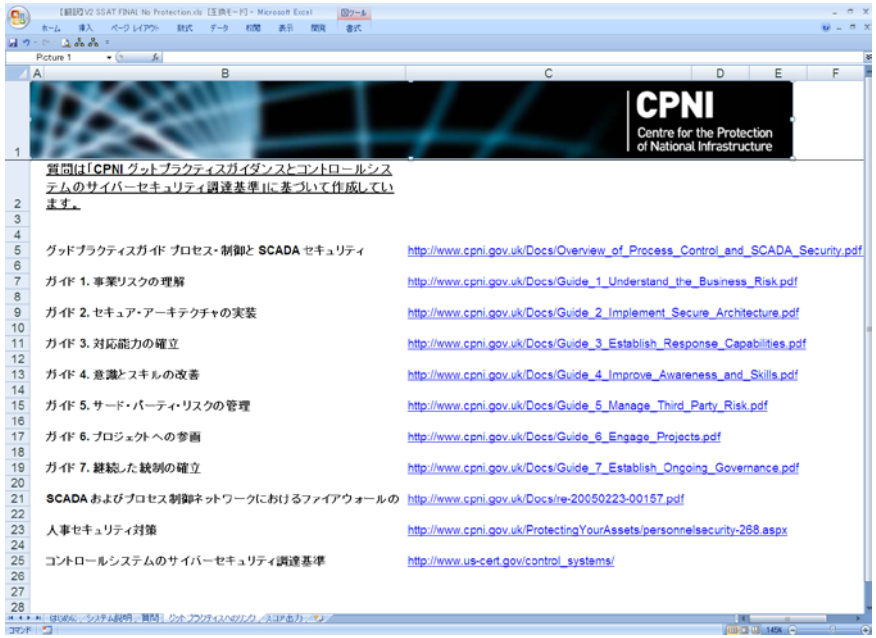
- **SSAT とは？**
  - CPNI が開発した SCADA を導入している制御システム向けの自己評価ツール

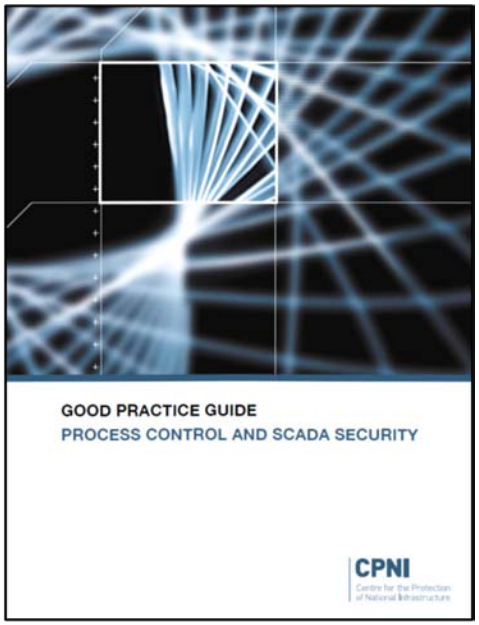
- **特徴は？**
  - SCADA に特化している評価ツール
  - 導入・操作が容易
  - 評価は短期間で実施可能
  - 和訳参考資料が豊富



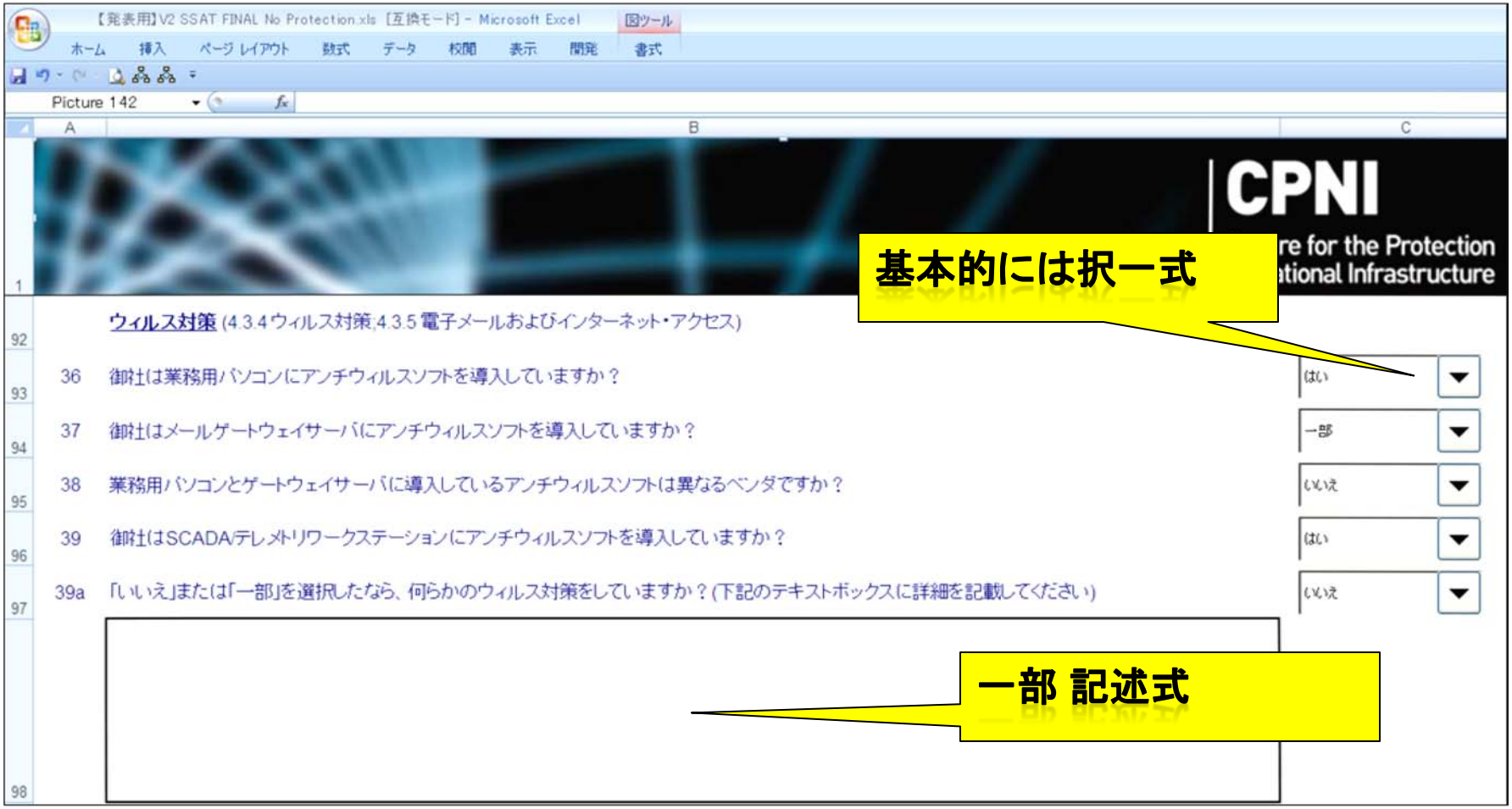
SSAT (SCADA Self Assessment Tool)

- **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





SSAT (SCADA Self Assessment Tool)



質問の紹介1

- 択一式（はい、いいえ、一部　など）
  - SCADA/テレメトリシステムからの、電子メールやインターネット・アクセスは、どのような要件でも禁止していますか?
  - 御社はSCADA/テレメトリワークステーションにアンチウィルスソフトを導入していますか？
- 記述式
  - 「いいえ」または「一部」を選択したなら、何らかのウィルス対策をしていますか？

質問の紹介2

- 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？
  - 機器を SCADA ネットワークに接続する前に、それらがウィルスやワームに感染していないことを確認する手順を文書化していますか？
- 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)

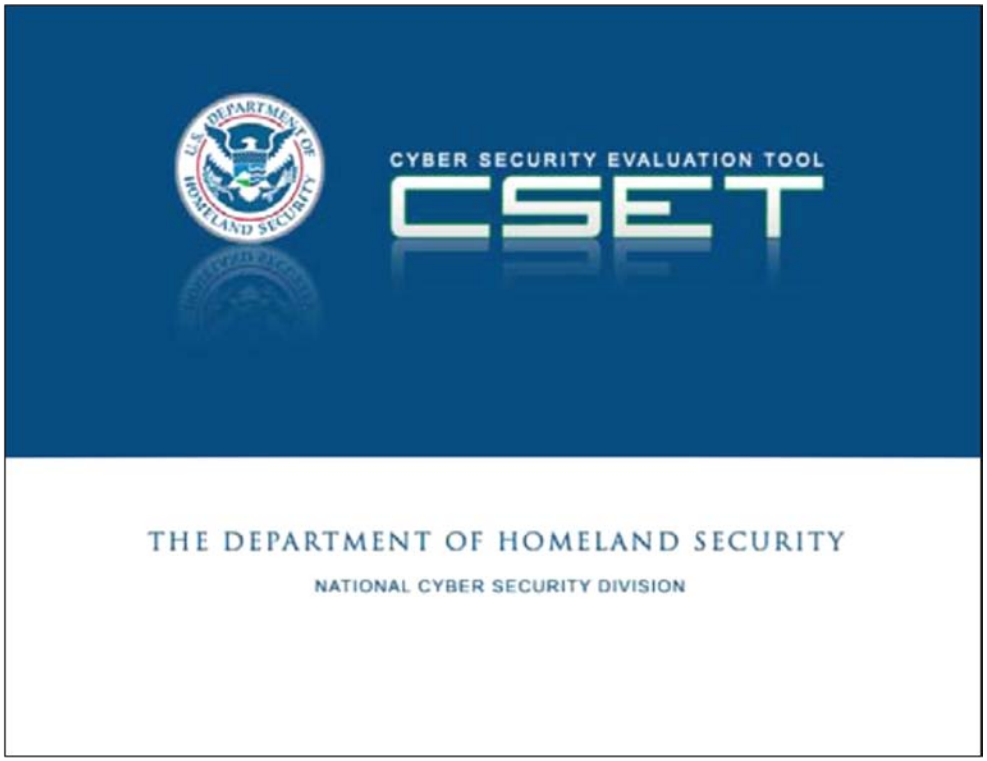
- **評価結果**
  - グットプラクティスガイドの準拠率を3段階で評価
  - 関連資料の URL を用意

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/

CSET (Cyber Security Evaluation Tool)

JPCERT CC®

- **CSETとは？**
  - DHS と INL が共同開発した制御・情報システムのサイバーセキュリティ自己評価ツール

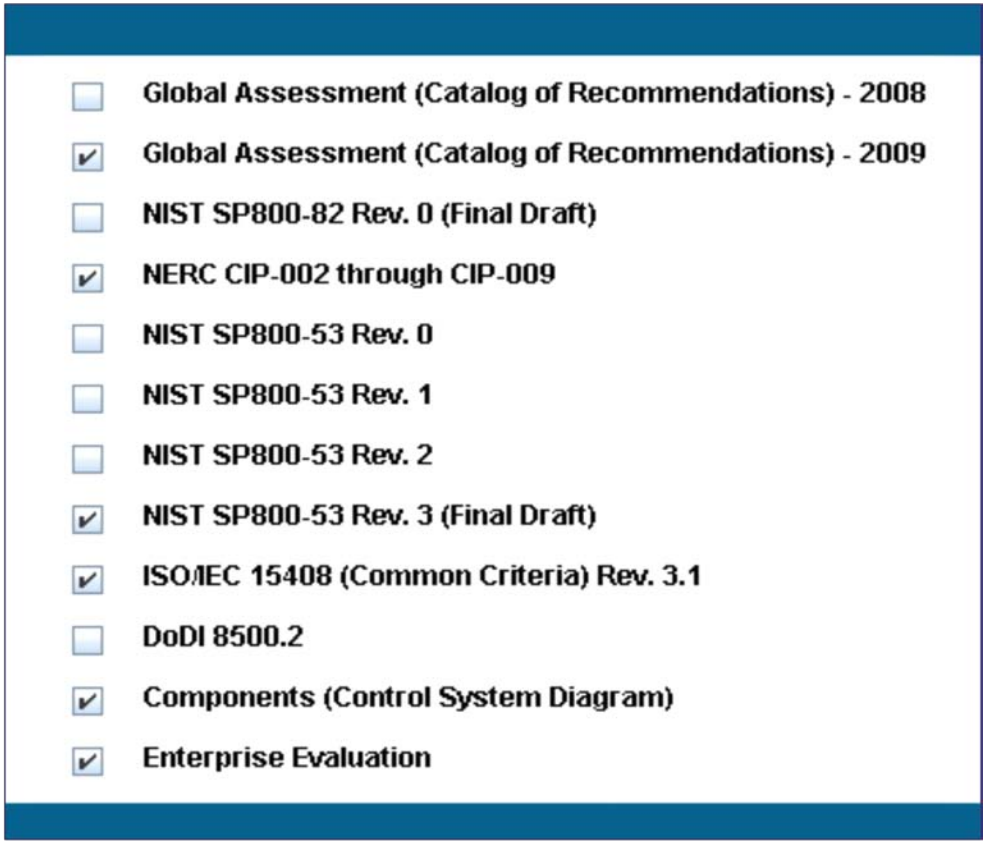


- **特徴は？**
  - 制御・情報システムの自己評価ツール
  - 複数のセキュリティ基準をサポート
  - ネットワーク構成図を基にした評価
  - Windows アプリケーション

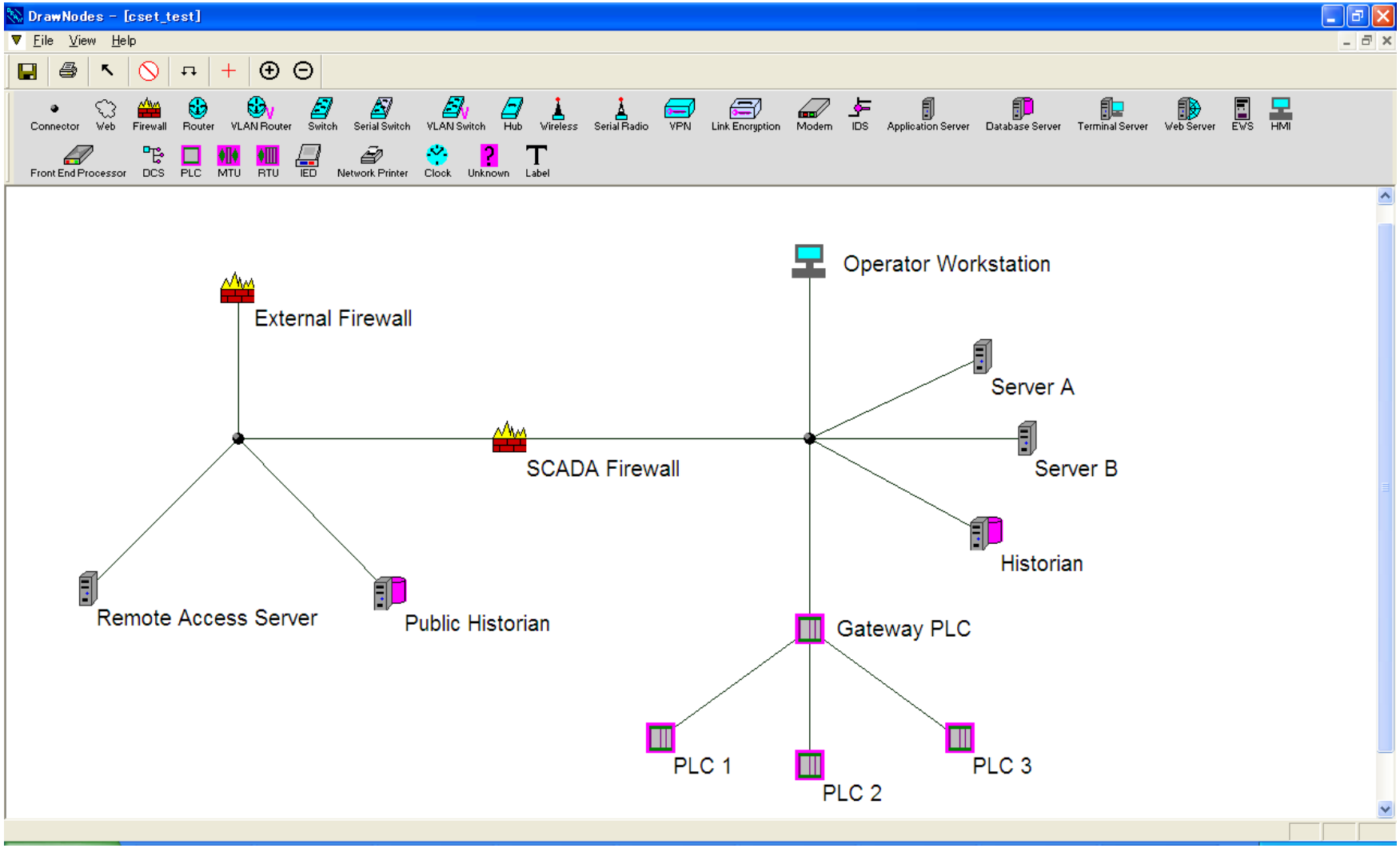
CSET (Cyber Security Evaluation Tool)

JPCERT CC®

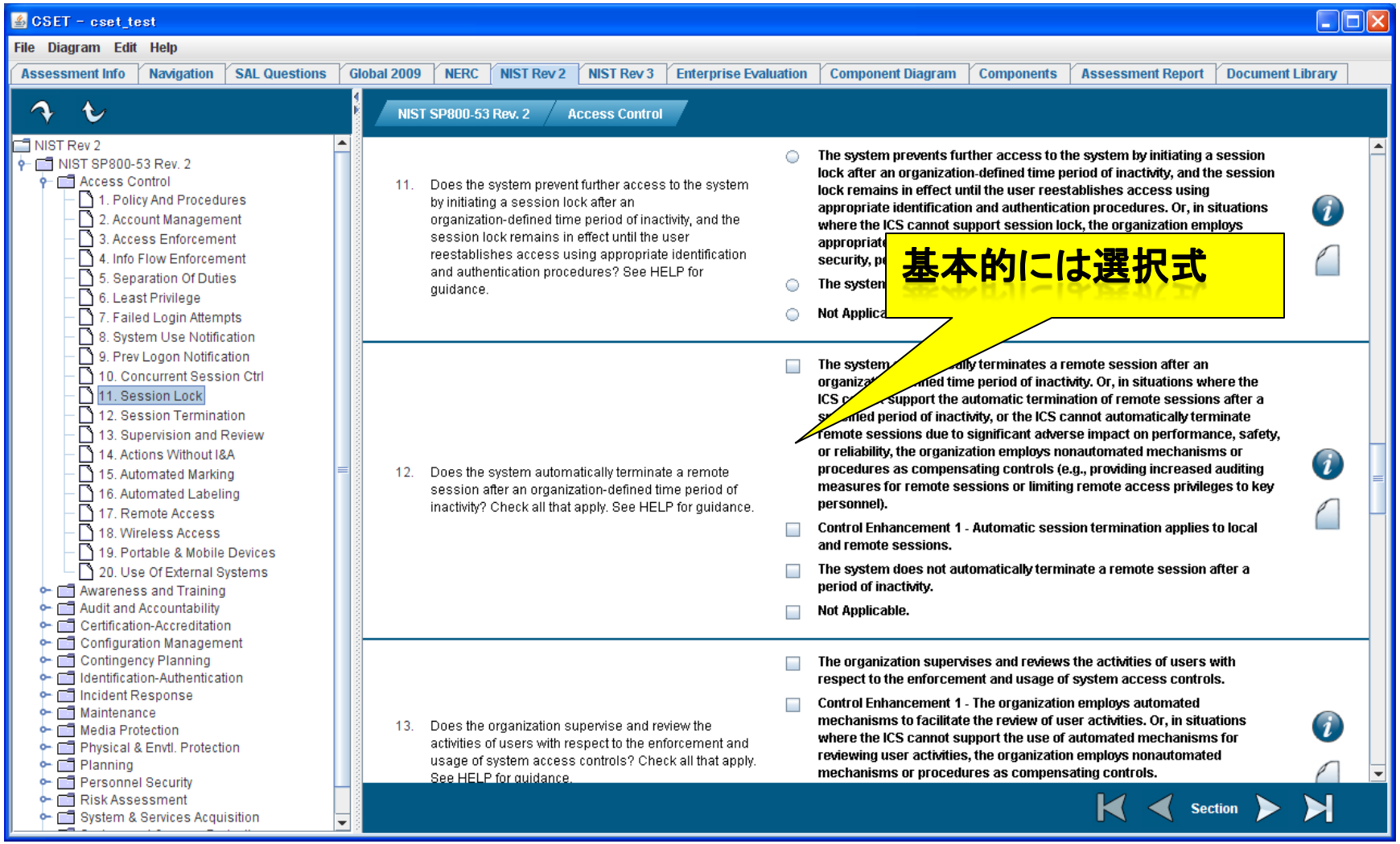
- **複数のセキュリティ基準をサポート**
  - NERC CIP-002 - 009
  - NIST SP800-53 Rev.0 - 3
  - NIST SP800-82 Rev.0
  - ISO/IEC 15408 Rev.3.1
  - DoDI 8500.2
  - Global Assessment
  - Enterprise Evaluation



CSET (Cyber Security Evaluation Tool)



CSET (Cyber Security Evaluation Tool)



質問の紹介1

以下の項目で、どのファイアウォールイベントログを記録していますか？
あてはまるすべてをチェックしてください。

- □ファイアウォールの起動時と停止時
- □ファイアウォールの故障時
- □ログイン時
- □セキュリティ要件の変更時
- □内部時間の変更時
- □設定の変更、変更違反、許可されていないコマンド実行時
- □特に記録していない

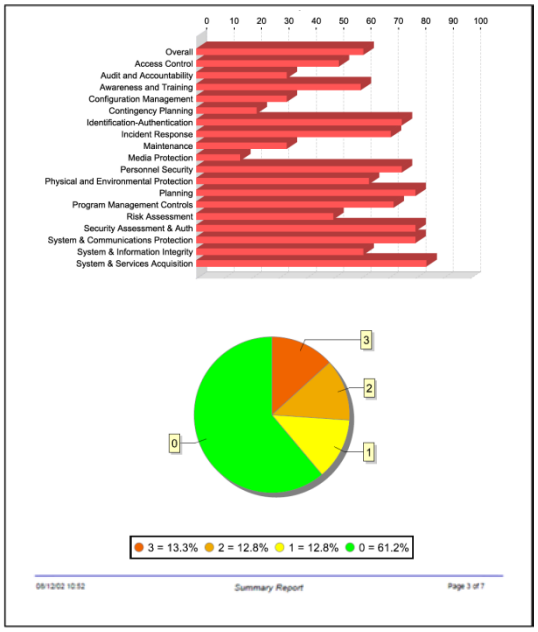
質問の紹介2

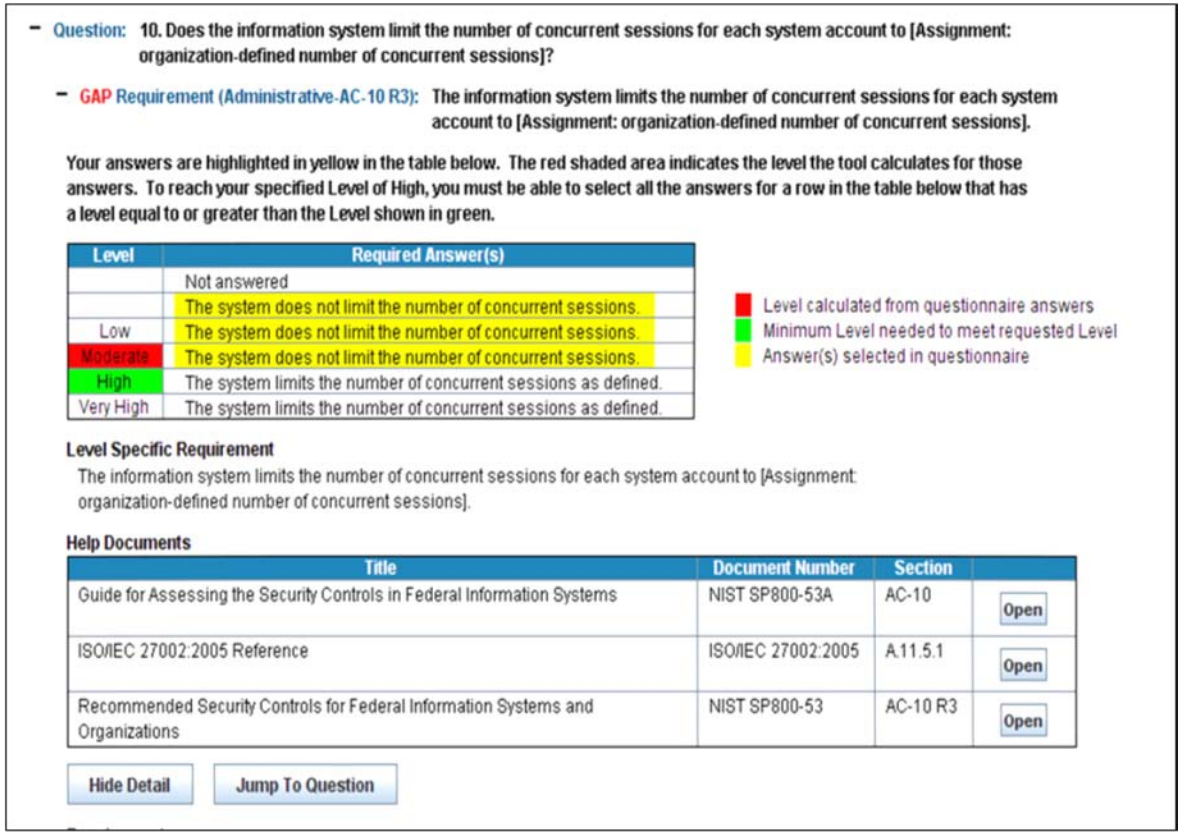
- データベースサーバのセキュリティ管理を行うユーザに許可されている、業務を選んでください。 あてはまるすべてをチェックしてください。

  - ☐データへのアクセス業務
  - ☐システム構成業務
  - ☐生成機能検査
  - ☐認証業務
  - ☐プロトコルセキュリティ業務
  - ☐暗号業務
  - ☐上記のどれも担っていない

評価結果

- 回答と改善案の表示
- 関連資料へのリンク
- 評価結果をレポート出力





SSATとCSETの比較

SSAT	比較内容	CSET
SCADA システムの自己評価	目的	制御システム全般の自己評価
CPNI のセキュリティ基準のみ	セキュリティ基準	複数のセキュリティ基準を用意
Excel の導入	導入	複数のアプリケーション導入
使い・見慣れたフォーム	操作性	独自のフォーム
和訳されているものが多い	資料	和訳されているものが少ない
短期間	評価期間	長期間
簡素な結果	結果	詳細な結果
粗い	評価の粒度	細かい

質疑応答