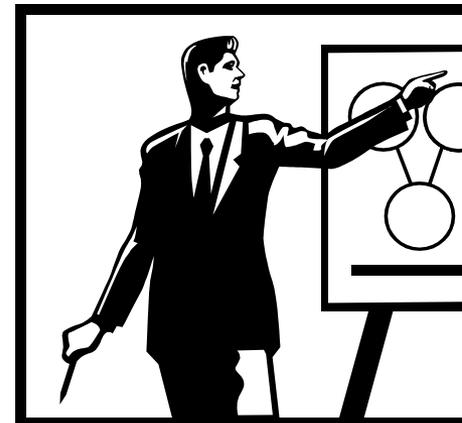


# 制御システム セキュリティ評価ツールの紹介

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

- 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

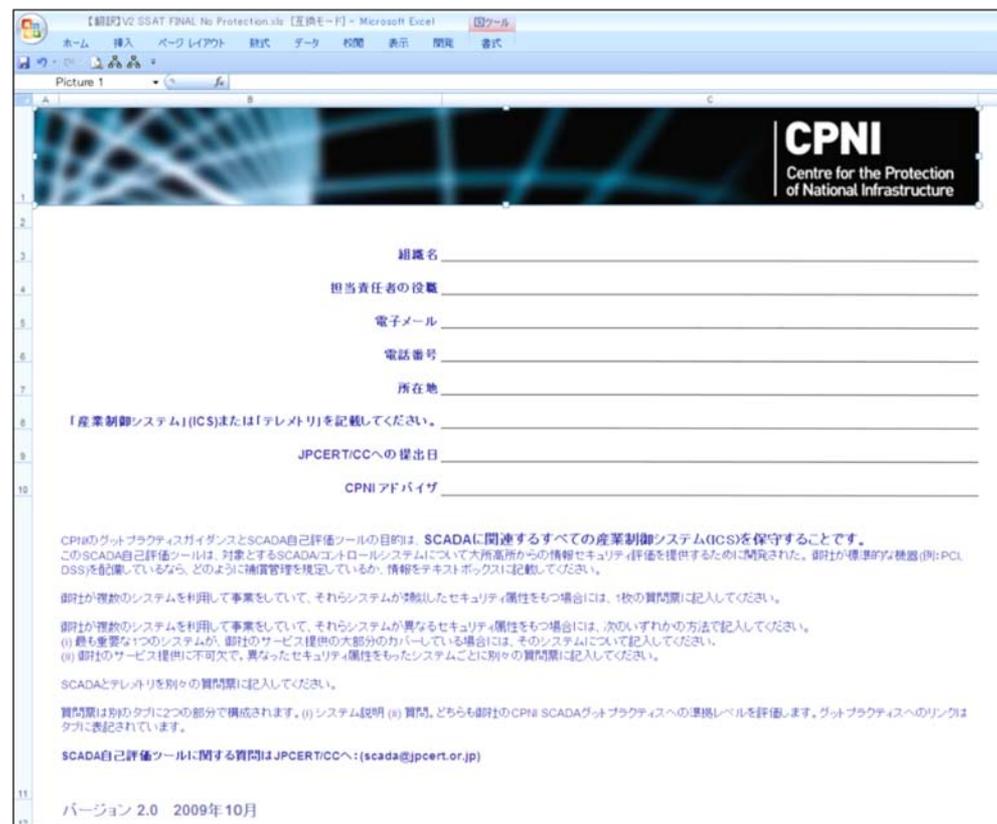


## ■ SSAT とは？

- 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



The screenshot shows a Microsoft Excel spreadsheet titled "【印刷用】SSAT FINAL No Protection.xls". The spreadsheet contains a form for the SSAT assessment. The form includes the following fields:

- 組織名
- 担当責任者の役職
- 電子メール
- 電話番号
- 所在地
- 「産業制御システム」(ICS)または「テレメトリ」を記載してください。
- JPCERT/CCへの提出日
- CPNI アドバイザ

Below the form, there is a section of Japanese text explaining the purpose of the tool and providing instructions for use. The text includes:

CPNIのグッドプラクティスガイダンスとSCADA自己評価ツールの目的は、SCADAに関連するすべての産業制御システム(ICS)を保守することです。このSCADA自己評価ツールは、対象とするSCADA/制御システムについて大所高所からの情報セキュリティ評価を提供するために開発された。御社が標準的な機器(例: PLC, DSS)を配備しているなら、どのように補償管理を規定しているか、情報をテキストボックスに記載してください。

御社が複数のシステムを利用して事業をしていて、それらシステムが異なるセキュリティ属性をもつ場合には、1枚の質問票に記入してください。

御社が複数のシステムを利用して事業をしていて、それらシステムが異なるセキュリティ属性をもつ場合には、次のいずれかの方法で記入してください。

- (i) 最も重要な1つのシステムが、御社のサービス提供の大部分のカバーしている場合には、そのシステムにのみ記入してください。
- (ii) 御社のサービス提供に不可欠で、異なるセキュリティ属性をもったシステムごとに別々の質問票に記入してください。

SCADAとテレメトリを別々の質問票に記入してください。

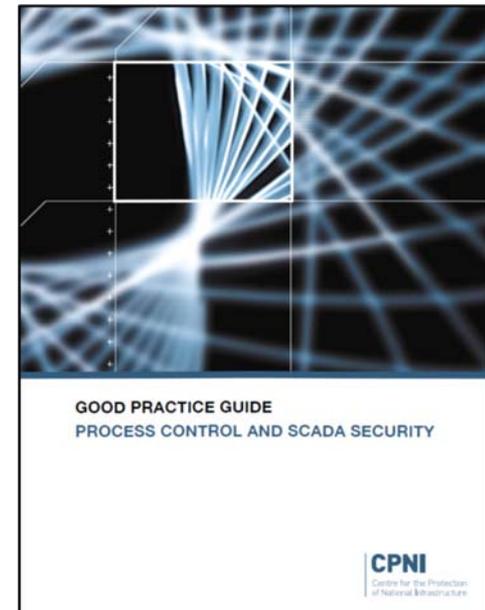
質問票は別のタブに2つの部分で構成されます。(i) システム説明 (ii) 質問。どちらも御社のCPNI SCADAグッドプラクティスへの準拠レベルを評価します。グッドプラクティスへのリンクはタブに表示されています。

SCADA自己評価ツールに関する質問はJPCERT/CCへ: (scada@jpcert.or.jp)

バージョン 2.0 2009年10月

## ■ 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 )

【宛表用】V2 SSAT FINAL No Protection.xls [互換モード] - Microsoft Excel

Picture 142

CPNI  
Center for the Protection of Critical National Infrastructure

**基本的には択一式**

ウイルス対策 (4.3.4ウイルス対策,4.3.5 電子メールおよびインターネット・アクセス)

36 御社は業務用パソコンにアンチウイルスソフトを導入していますか？

37 御社はメールゲートウェイサーバにアンチウイルスソフトを導入していますか？

38 業務用パソコンとゲートウェイサーバに導入しているアンチウイルスソフトは異なるベンダですか？

39 御社はSCADA/テレメトリワークステーションにアンチウイルスソフトを導入していますか？

39a 「いいえ」または「一部」を選択したなら、何らかのウイルス対策をしていますか？(下記のテキストボックスに詳細を記載してください)

**一部 記述式**

## ■ 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イ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イ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、それらがウイ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？

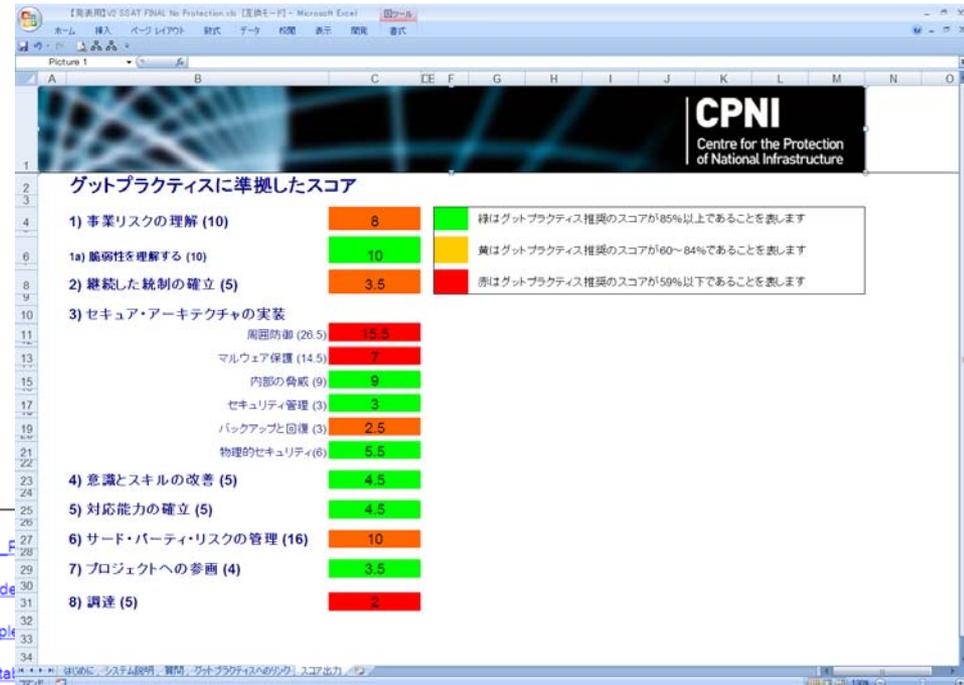
### ■ 記述式

- 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？



## ■ 評価結果

- ゲ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	<a href="http://www.cpni.gov.uk/Docs/Overview_of_F...">http://www.cpni.gov.uk/Docs/Overview_of_F...</a>
ガイド 1. 事業リスクの理解	<a href="http://www.cpni.gov.uk/Docs/Guide_1_Unde...">http://www.cpni.gov.uk/Docs/Guide_1_Unde...</a>
ガイド 2. セキュア・アーキテクチャの実装	<a href="http://www.cpni.gov.uk/Docs/Guide_2_Impl...">http://www.cpni.gov.uk/Docs/Guide_2_Impl...</a>
ガイド 3. 対応能力の確立	<a href="http://www.cpni.gov.uk/Docs/Guide_3_Esta...">http://www.cpni.gov.uk/Docs/Guide_3_Esta...</a>
ガイド 4. 意識とスキルの改善	<a href="http://www.cpni.gov.uk/Docs/Guide_4_Impr...">http://www.cpni.gov.uk/Docs/Guide_4_Impr...</a>
ガイド 5. サード・パーティ・リスクの管理	<a href="http://www.cpni.gov.uk/Docs/Guide_5_Man...">http://www.cpni.gov.uk/Docs/Guide_5_Man...</a>
ガイド 6. プロジェクトへの参画	<a href="http://www.cpni.gov.uk/Docs/Guide_6_Eng...">http://www.cpni.gov.uk/Docs/Guide_6_Eng...</a>
ガイド 7. 継続した統制の確立	<a href="http://www.cpni.gov.uk/Docs/Guide_7_Est...">http://www.cpni.gov.uk/Docs/Guide_7_Est...</a>
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	<a href="http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf">http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf</a>
人事セキュリティ対策	<a href="http://www.cpni.gov.uk/ProtectingYourAssets/personnelsecurity-268.aspx">http://www.cpni.gov.uk/ProtectingYourAssets/personnelsecurity-268.aspx</a>
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	<a href="http://www.us-cert.gov/control_systems/">http://www.us-cert.gov/control_systems/</a>

## ■ 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



## ■ 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

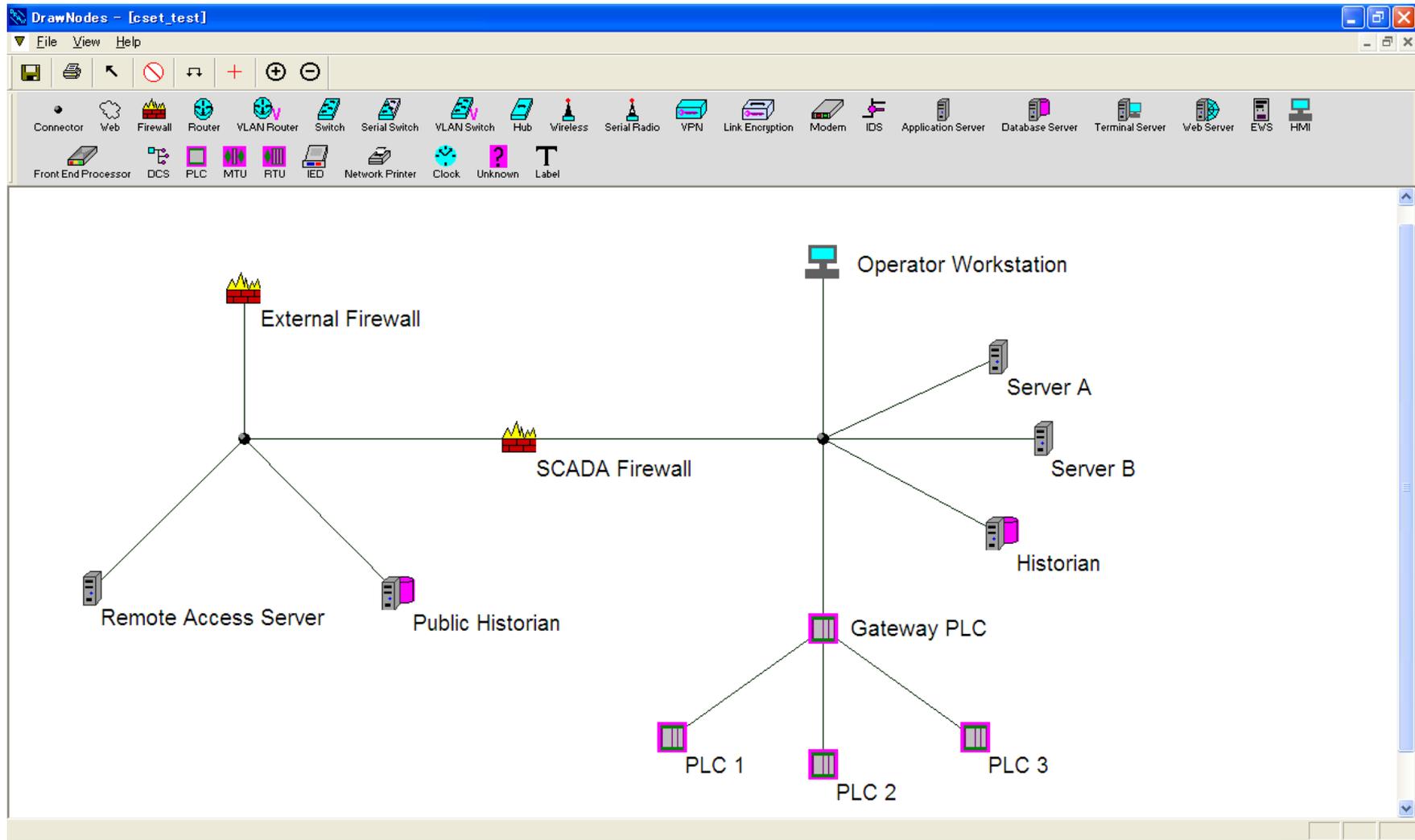
■ DoDI 8500. 2

■ Global Assessment

■ Enterprise Evaluation

- Global Assessment (Catalog of Recommendations) - 2008
- Global Assessment (Catalog of Recommendations) - 2009
- NIST SP800-82 Rev. 0 (Final Draft)
- NERC CIP-002 through CIP-009
- NIST SP800-53 Rev. 0
- NIST SP800-53 Rev. 1
- NIST SP800-53 Rev. 2
- NIST SP800-53 Rev. 3 (Final Draft)
- ISO/IEC 15408 (Common Criteria) Rev. 3.1
- DoDI 8500.2
- Components (Control System Diagram)
- Enterprise Evaluation

# CSET ( Cyber Security Evaluation Tool )



The screenshot shows the CSET - cset\_test application window. The menu bar includes File, Diagram, Edit, and Help. The toolbar contains Assessment Info, Navigation, SAL Questions, Global 2009, NERC, NIST Rev 2, NIST Rev 3, Enterprise Evaluation, Component Diagram, Components, Assessment Report, and Document Library. The main content area is titled 'NIST SP800-53 Rev. 2 / Access Control'. On the left, a tree view shows the hierarchy: NIST Rev 2 > NIST SP800-53 Rev. 2 > Access Control > 11. Session Lock. The main area displays three questions:

11. Does the system prevent further access to the system by initiating a session lock after an organization-defined time period of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures? See HELP for guidance.

- The system prevents further access to the system by initiating a session lock after an organization-defined time period of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Or, in situations where the ICS cannot support session lock, the organization employs appropriate security, p...
- The system
- Not Applicable

12. Does the system automatically terminate a remote session after an organization-defined time period of inactivity? Check all that apply. See HELP for guidance.

- The system automatically terminates a remote session after an organization-defined time period of inactivity. Or, in situations where the ICS cannot support the automatic termination of remote sessions after a specified period of inactivity, or the ICS cannot automatically terminate remote sessions due to significant adverse impact on performance, safety, or reliability, the organization employs nonautomated mechanisms or procedures as compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).
- Control Enhancement 1 - Automatic session termination applies to local and remote sessions.
- The system does not automatically terminate a remote session after a period of inactivity.
- Not Applicable.

13. Does the organization supervise and review the activities of users with respect to the enforcement and usage of system access controls? Check all that apply. See HELP for guidance.

- The organization supervises and reviews the activities of users with respect to the enforcement and usage of system access controls.
- Control Enhancement 1 - The organization employs automated mechanisms to facilitate the review of user activities. Or, in situations where the ICS cannot support the use of automated mechanisms for reviewing user activities, the organization employs nonautomated mechanisms or procedures as compensating controls.

A yellow callout box with the text '基本的には選択式' (Basically, it's a multiple-choice type) points to the radio button options for question 11. The bottom of the window features navigation arrows and a 'Section' label.

## ■ 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

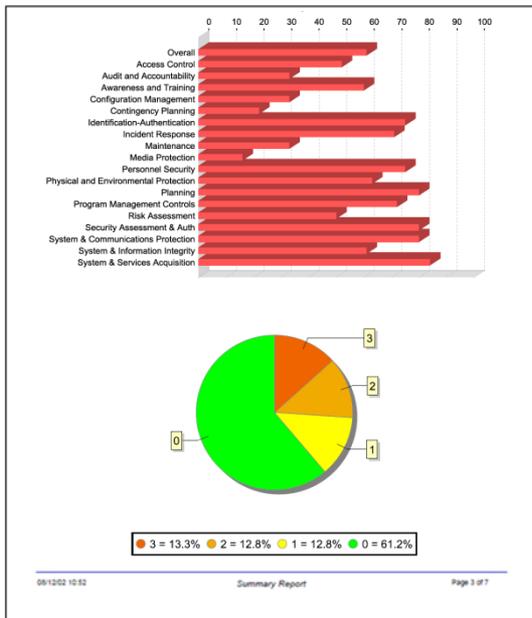
■ データベースサーバのセキュリティ管理を行うユーザに許可されている、業務を選んでください。 あてはまるすべてをチェックしてください。

- 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



- **Question:** 10. Does the information system limit the number of concurrent sessions for each system account to [Assignment: organization-defined number of concurrent sessions]?

- **GAP Requirement (Administrative-AC-10 R3):** The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number of concurrent sessions].

Your answers are highlighted in yellow in the table below. The red shaded area indicates the level the tool calculates for those answers. To reach your specified Level of High, you must be able to select all the answers for a row in the table below that has a level equal to or greater than the Level shown in green.

Level	Required Answer(s)
	Not answered
	The system does not limit the number of concurrent sessions.
Low	The system does not limit the number of concurrent sessions.
Moderate	The system does not limit the number of concurrent sessions.
High	The system limits the number of concurrent sessions as defined.
Very High	The system limits the number of concurrent sessions as defined.

- Level calculated from questionnaire answers
- Minimum Level needed to meet requested Level
- Answer(s) selected in questionnaire

### Level Specific Requirement

The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number of concurrent sessions].

### Help Documents

Title	Document Number	Section	
Guide for Assessing the Security Controls in Federal Information Systems	NIST SP800-53A	AC-10	<a href="#">Open</a>
ISO/IEC 27002:2005 Reference	ISO/IEC 27002:2005	A.11.5.1	<a href="#">Open</a>
Recommended Security Controls for Federal Information Systems and Organizations	NIST SP800-53	AC-10 R3	<a href="#">Open</a>

[Hide Detail](#)

[Jump To Question](#)

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