20th Anniversary

JPCERT CC®

制御システムセキュリティアセスメント

一般社団法人JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
落合 一郎

目次

- 様々な「アセスメント」
- 制御システムセキュリティアセスメントに使える基準とツール
- JPCERT/CCの制御システムセキュリティアセスメント
- 実施実績と効果 (速報)

様々な「アセスメント」

内部・外部アセスメント

- 内部アセスメント
  - セルフ
  - 社内監査部門
- 外部アセスメント
  - セキュリティ専門会社
  - 監査専門会社
  - ベンダ
  - 公的機関

内部・外部アセスメント

	内部アセスメント	外部アセスメント
誰が行う	組織内の担当者 組織内の監査部門	組織外の専門家 JPCERT CC®
利点	・重要な問題を深堀りできる ・普段から気になっている問題点をもれなくカバーできる	・内部の者が気づきにくい問題点に光を当てられる ・脅威や対策の相場観を適切に判断できる
欠点	・手前味噌の評価で終り重要な問題点を見過ごす可能性がある	・組織の内部事情への配慮の過剰や不足が結果が歪むことがある

監査・アセスメント

- 監査とアセスメント

  道具立てと実施手順は似通っている

  大きな相違は実施目的

  —批判的監査
    - 合格か不合格かを判定し
      その結果を第三者に知らしめる

  —指導的監査
    - 必要ないし望ましい改善点を見つけ出す

  —アセスメント
    - プロジェクトの方向性を決めるための予備的調査

監査・アセスメント

	批判的監査	指導的監査	アセスメント
何のため	第三者に問題が無いことを示す 適合性の認証	改善すべき点の発見	プロジェクトの細目を決めるための情報収集
基準の選択	制度ごとに決められている	改善を意図している者が選ぶ	収集すべき情報に応じて選ぶ
結果や指摘事項の扱い	合格するためには是正処置が必要	マネジメントの中で参考情報として活用	プロジェクト計画の中に反映

制御システムセキュリティ
アセスメントに使える基準とツール

様々なツール(チェックリストとして使える基準)

- J-CLICS
  Check List for Industrial Control Systems of Japan
- SSAT（CPNI）
  SCADA Self Assessment Tool
- NIST
  SP800-53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産業用制御システム(ICS)セキュリティガイド
- CSET (ICS-CERT)
  Cybersecurity Evaluation Tool
- CSMS（IEC62443）
  Cyber Security Management System
- 業界安全基準

様々なツール

- ネットワーク試験ツール
  - —Nmap等
- 脆弱性スキャナー
- ペネトレーション試験ツール
  - — Metasploit等

※ JPCERT/CCのアセスメントでは使用いたしません

JPCERT/CCの
制御システムセキュリティ
アセスメント

目的

- 目的

本アセスメントは、経済産業省からの委託事業として、日本の企業・組織の現状把握、関係構築を目的として実施し、アセスメントによって得られた結果や知見は匿名化したうえで、広く制御システム利用者の注意を喚起するためなどに活用する。

※個別の標準規格に基づいた評価や、発見された問題点や課題の具体的な改善策の提示などが必要な場合には専門のアセスメント・コンサルティングサービスの利用を推奨

概要

- アセスメント基準（ベースラインアプローチ）
  英国政府機関のCPNI (Centre for the Protection of National Infrastructure) が開発したSSAT を翻訳および日本向けに修正を行った日本版SSAT、または制御システムセキュリティのガイドラインとして用いられる米国のNIST文書に基づいたアセスメント

- オンサイトアセスメント
  JPCERT/CCの担当者がアセットオーナのサイトを訪れ、ヒアリングを行い、可能な範囲で証跡の確認を行う。
  その後、結果をまとめレポートとして提出

- 対象
  制御システムを利用する国内のアセットオーナ

- メリット
  現状のセキュリティの評価が行え、第3者評価による気付きを得ることができる。

2種類のアセスメント（SSATとTR）

■**SSAT**：SCADA Self Assessment Tool

導入から運用までの全般のアセスメント

■**TR**： Technical Review

ファイアウォールの設定内容等の技術面の詳細なアセスメント

	SSAT	TR
アプローチ	ベースライン	ベースライン
基準	日本版SSAT	NIST SP800-53 NIST SP800-82
分野	全般（デザイン、購買、導入、運用）	技術的（設計、運用）

NIST SP800-53 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
NIST SP800-82 産業用制御システム(ICS)セキュリティガイド

SSAT詳細

- リスクと脅威の理解
- 継続した統制の確立
- セキュア・アーキテクチャーの実装
- 意識とスキルの改善
- 対応能力の確立
- サードパーティリスクの管理
- プロジェクト参画
- 調達

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

安全・安心なIT社会のための、国内・国際連携を支援する

1) 事業リスクの理解 (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 - セクション 3.1 または ガイド 1 を参

事業リスクの要素は脅威、影響、脆弱性です。事業リスクをよく理解することで、初めて情報に基づいたセキュリティの適切なレベルはどのくらいか、改善すべき作業実施方法はどういったものかを判断できるようになります。

システムとビジネスリスクを理解する (3.4.1 システムの理解; 3.4.2 事業リスクの評価)

1	安全管理責任者はSCADA/遮隔監視ネットワークの棚卸監査と評価を実施し、最新の状態を管理していますか？（例: どんなシステムが存在しているか、機能は、重要な 業務/安全性は、設置場所は、所有者の明示、サポート担当者は誰か）	一部
1a	「はい」を選択したなら、それは過去12ケ月以内に見直し、監査結果報告書を作成していますか？	いいえ
2	安全管理責任者はシステムの事業リスクを、定められた手順に則って評価していますか？（例:リスクの発生の可能性と、リスクが発生した結果として予想できる影響でリスクを表します）	一部

脅威を理解する (3.4.3 脅威の理解)

3	安全管理責任者はSCADA/遮隔監視システムに起こりうる脅威を特定し、脅威評価に着手していますか？（例: DoS 攻撃、ネットワーク侵入、ウイルス、ワーム感染）	はい
3a	「はい」を選択したなら、それは過去12ケ月以内に見直していますか？	いいえ
4	安全管理責任者は特定のシナリオを考慮した、脅威評価に着手していますか？（例: 特定のOSを搭載したコンピュータシステムにおける攻撃被害や障害、EthernetIP ネットワークにおける攻撃被害や障害など）	いいえ
4a	「はい」を選択したなら、それは過去12ケ月以内に見直していますか？	いいえ

影響を理解する (3.4.4 影響の理解)

5	安全管理責任者はSCADA/遮隔監視システムで脅威が実際に起こった際の、プロセス制御システムへの影響と結果を文書化していますか？（例: ブランドへの影響、規定違反、業務目標の達成不能、財政上の損失）	いいえ

アセスメント項目（SSAT) 1/2

- リスクと脅威の理解
- 統制
- ネットワークアーキテクチャー
- ファイアウォール
- リモートアクセス
- 侵入検知
- 侵入テスト
- ワイヤレス
- ウイルス対策
- セキュリティパッチ
- システム強化
- パスワードとアカウント

アセスメント項目（SSAT) 2/2

- 転入・転出の管理
- 接続手順
- バックアップ
- 物理セキュリティ
- 意識とスキルの改善
- 対応能力の確立
- サードパーティリスク管理
- プロジェクト参画
- 調達

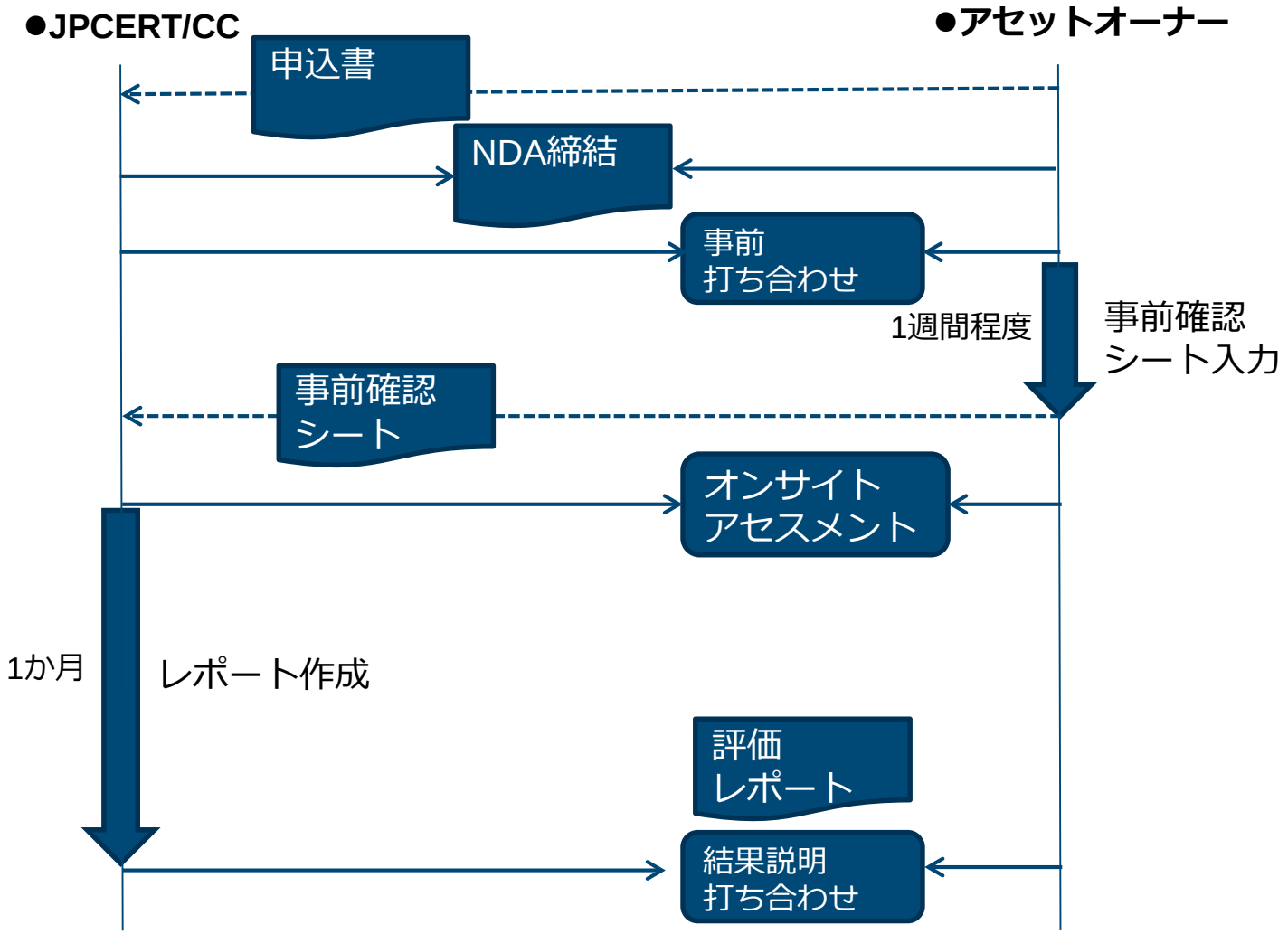
TR 詳細

- NIST SP800-53 技術管理策
  - AC(20) アクセス制御(Access Control)
  - AU(11) 監査および責任追跡性(Audit and Accountability)
  - IA(7) 識別および認証(Identification and Authentication)
  - SC(23) システムおよび通信の保護(System and Communications Protection)
- NIST SP800-82 産業制御システム(ICS)セキュリティ
  - ネットワークアーキテクチャー
  - セキュリティ管理策

アセスメント項目（TR）

- オフィスネットワークとの接続
- ファイアウォール・DMZ
- ネットワーク機器
- セキュリティ対策
- データヒストリアン
- ベンダ向けリモートアクセス
- バックアップ
- アクセス制御
- ログ監視
- 構成管理
- システムハードニング

アセスメントの流れ



評価レポートイメージ

JPCERT CC®

制御システムセキュリティ
アセスメントレポート

基本情報

御社名：
サイト：
システム名：
アセスメント実施日：

アセスメント手法：日本版 SSATによるオンサイトアセスメント

アセスメント結果サマリー

スコア（グッド・プラクティスの準拠率）

アセスメント結果詳細

1) 事業リスクの理解
   発見事項はありませんでいした。
2) 継続した統制の確立
   発見事項はありませんでした。
3) セキュア・アーキテクチャの実装
   ネットワークアーキテクチャ

発見事項	１つの PC によるデュアルホーム接続により、制御ネットワーク上の２つのシステムが接続されていました。
懸念事象	いずれか一方のシステムが侵害を受けた場合、容易にもう１つのシステムにも侵害が及ぶ可能性があります。
推奨対策	ファイアウォールによるネットワークの隔離が望まれます。

4) 意識とスキルの改善

発見事項	注意喚起プログラム活動計画、セキュリティ技術を習得する計画・措置などが現状とくに存在していませんでした。
懸念事象	組織としての対応能力向上が見込まれません。
推奨対策	何らかの意識とスキル向上の施策が望まれます。

5) 対応能力の確立
   発見事項はありませんでした。
6) サード・パーティ・リスクの管理
   発見事項はありませんでした。
7) プロジェクトへの参画
   発見事項はありませんでした。
8) 調達
   発見事項はありませんでした。

全体を通じた所感

オフィスネットワークとの接続は無いとのことで、「Air Gapl の対策がなされていることが確認できました。しかし、「Air Gapl によって守られた制御ネットワークでもマルウエアに感染する事故が起こっています。ウイルス対策ソフトは一部導入されていますが、セキュリティパッチに関しても、定期メンテナンスのタイミング等で適用が推奨されます。

JPCERT/CCの
制御システムセキュリティ
アセスメントの実績と効果 (速報)

2016年度実施状況

- 実施済：3社（SSAT×２、TR × １）

PA系

- 年度末までに実施予定：4社

PA系、BA系

発見事項例（１）：SSAT・TR

- ファイアウォール
  - —アセスメント結果
    - ファイアウォールを使用されている組織がありました。
    - データは中継サーバ経由でオフィスネットワーク側に送られている組織がありました。
    - ファイアウォールの設定・運用は外部ベンダに委託して実施されている組織がありました。

発見事項
・DMZが作られていない組織がありました。
・委託している外部ベンダの運用状況が確認されていない組織がありました。

発見事項例（２）：SSAT

- 物理セキュリティ
  - —アセスメント結果
    - 制御室への入退室制限は、問題なく行われている事が確認できました。

発見事項
・入退室の記録／監査は行っていない組織がありました。

発見事項例（３）：SSAT

- 対応能力の確立
  - ―アセスメント結果
    - CSIRTを作って組織的な対応ができている組織がありました。

発見事項
・どのような手順書が必要なのか不明との組織がありました。

よくできていた項目-運用・ポリシー：SSAT

- 統制

  セキュリティのポリシーは、全社的、または事業所向けとして定められていた組織がありました。

- 意識とスキルの改善

  Eラーニングを用意し、制御システムに関わる管理職、新人に対する教育を実施している組織がありました。

よくできていた項目-技術的：SSAT・TR

- ファイアウォールの設置

  制御ネットワークとオフィスネットワークは接続され、運転データの転送が行われていましたが、制御ネットワークとの境界にはファイアウォールが設置されている組織がありました。

- リモート接続の管理

  リモート接続の存在と目的等は文書化され、また必要な時にのみ接続する運用がされている組織がありました。

よくできていた項目-全般：SSAT

- 組織的なセキュリティ運用体制

  制御システムセキュリティに関して全社的な取り組みが行われ、制御システムも理解したITの責任者が全体の責任者となり、ポリシーから手順書等、CSIRT活動含めた施策が非常によくできていた組織がありました。

アセスメントを受けていただいた組織の所感

- 客観的な評価が得られて良かった。
- 大きな問題がないことが確認できて良かった。
- 普段、意識していなかったが、指摘により必要性を理解できた項目があった。
- 社外の専門組織によるアセスメントを受けることにより、関係者の情報セキュリティの意識高揚ができた。
- 今後、多くの組織でアセスメントを実施していただき、統計データはベンチマーク評価のデータとして提供していただきたい。

今後も、実施実績を増やし、
より有効なものとしていきます

アセスメントを受けていただいた組織の所感

- 施設の現状を考えると、あまり必要性を感じない要求事項があった。

このような点を考慮した
評価レポートをご提供いたします

- 情報系の技術を適用することが評価の前提となっているようなので、より制御系の制約に適合する評価がされるとよりよいと思われる。

制御系の制約を考慮した評価レポートをご提供するとともに、今後要求事項の改善をしていきます

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form

ご静聴ありがとうございました