

重要インフラセキュリティフォーラム
2010年1月25日

JPCERT **CC**®

重要社会インフラのための 制御システム・セキュリティ強化に 向けたガイド

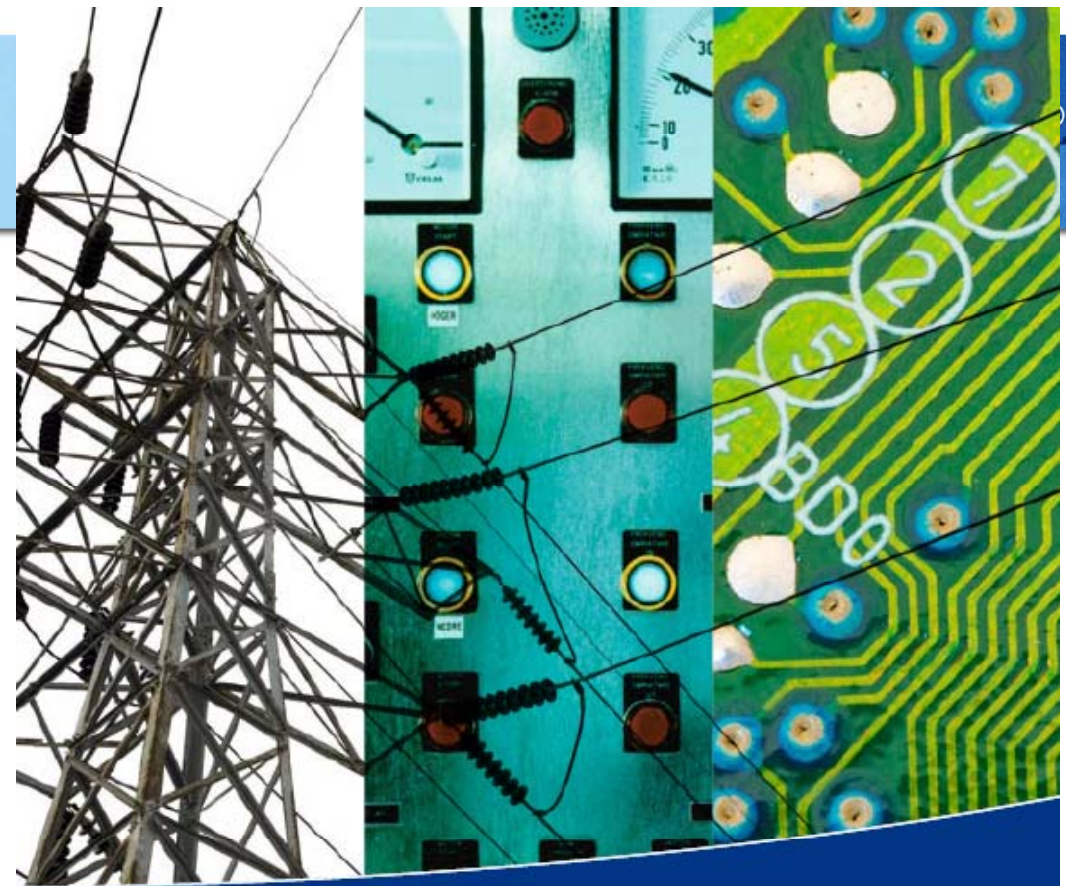
JPCERTコーディネーションセンター

目次

- 「重要社会インフラのための
制御システム(PCS)のセキュリティ強化ガイド」について
- プロセス制御システム(PCS; Process Control Systems)
 - PCSとは
 - ITシステムとPCSの比較
 - ITシステムとPCSの結合
 - PCSのセキュリティの重要性
- 推奨事項
 - 推奨事項の説明に関する基本方針
 - PCSのセキュリティ強化に関する推奨事項
 - まとめ

重要社会インフラのための 制御システム(PCS)の セキュリティ強化ガイド

- スウェーデンの緊急管理庁
が民間専門家の協力を得て
開発
 - 緊急管理庁(SEMA; KBM)は
その後、公衆非常庁(SCCV;
MSB)に移管統合された
- SCCV: Swedish Civil Contingencies
Agency
- MSB: Myndigheten för samhäll och
beredskap
- CPNI(英)の制御システム・ガ
イドラインがベース
 - NIST(米)のSP800-82
 - JPCERT/CCがSEMAの許可
を得て邦訳し公開



Guide to Increased Security in Process Control Systems for Critical Societal Functions

The Swedish forum for information
sharing concerning information
security – SCADA and process
control systems (FIDI-SC)



SWEDISH EMERGENCY
MANAGEMENT AGENCY

制御システムとは

(PCS; Process Control Systems)

PCSとは

- 重要社会インフラをはじめとする様々な分野では、コンピュータベースのシステムが物理的プロセスの監督・制御を行っている
- 上記のようなコンピュータベースのシステムを**PCS(プロセス制御システム)**という

使われている分野の例

電力, 鉄道, 航空, 水道, ガス,
農業, 製造業, 化学, 石油, etc.



ITシステムとPCSの比較

本ガイドの表1(経営管理用ITシステムとPCSとの重要な相違点)より抜粋、一部改訂

分類	ITシステム	PCS
パフォーマンスの要件	<u>非リアルタイム</u>	<u>リアルタイム</u>
リスクマネジメントの要件	<u>業務運営の中断が最大のリスク</u>	<u>人命、処理設備、操業能力の喪失にかかわる大きなリスクがある</u>
サービス稼働期間	<u>コンポーネントとシステムの稼働期間は短い(3~5年)</u>	<u>コンポーネントとシステムの稼働期間は長い(15~20年)</u>

両者は性質が違う

ITシステムとPCSの結合



PCSの世界にIT技術が導入されました

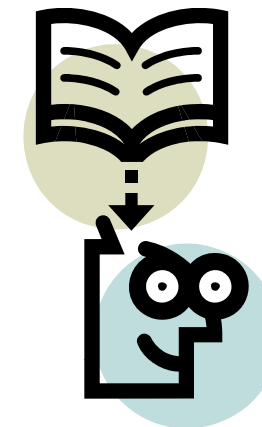
➡ コスト面、生産性が向上した

PCSの世界にIT技術を経由してサイバー攻撃がされはじめた

➡ PCSの運用に支障をきたすケースが発生した

PCSのセキュリティを考える理由

- PCSに対する**サイバー攻撃が脅威**となりつつあるから
 - ➔ サイバー攻撃による影響が運用上の不都合になる可能性がある
- PCSが**高可用性システム**であるから
 - ➔ 定常的に運用するため、運用中の設定変更や更新作業が避けられている
- PCSのセキュリティ要件の**検討作業**が必要であるから
 - ➔ IT技術のセキュリティとの間に文化的な摩擦が生じている



推奨事項

- CPNI(英国)などの国際的に認知されたガイドラインに整合
- 実践的なプロジェクトを通じて得られた経験を反映
- PDCAサイクル・モデルに関連付けて整理

PCSのセキュリティ強化に関する推奨事項 (1/4) (Plan:計画)

明確化・確立

1. PCSのセキュリティに関する**役割**と**責任範囲**を明確化せよ
2. PCSの調査と**リスク分析**の実施に関するプロセスを確立する
3. PCSの**変更管理**に関するプロセスを確立せよ
4. PCSの**緊急時対応計画**と**インシデント管理**に関するプロセスを確立せよ
5. PCSの**セキュリティ要件**を, すべての計画・調達作業に当初から定義し, 適用せよ



PCSのセキュリティ強化に関する推奨事項 (2/4) (Do:実行)

導入・実装

1. 良質のセキュリティ文化を醸成し、PCSにおける**セキュリティの必要性に関する意識**を向上せよ
2. PCS内に**複数の防護層**を形成せよ(多層防御)
3. ホスト型及びネットワーク型**侵入検知・インシデント監視手段**をPCSに24時間体制で導入せよ



PCSのセキュリティ強化に関する推奨事項 (3/4) (Check:評価)

分析・監査

1. PCSの**リスク**分析をシステム変更や環境の変化に合わせて実施する
2. PCS及び接続されたネットワークに対し、**技術的なセキュリティ**監査を定期的 to 実施する
3. PCSの**物理的なセキュリティ**を継続的に評価する



PCSのセキュリティ強化に関する推奨事項 (4/4) (Act:改善)

維持・是正

1. PCSで発生するインシデントの経過を追跡管理し、組織外で起きた**セキュリティ問題**の情報を収集分析する
2. ユーザグループや標準化機関等との間に、PCSのセキュリティ強化を目的とした**コミュニティ**を構築する
3. **PCSに対する接続のルール**を議論し、**安全な運用**を維持する
4. システムベンダの協力のもと、PCSを**堅牢化**及び**アップグレード**する



PCSのセキュリティに関する 役割と責任範囲を明確化する

失敗事例：

システムが悪意のあるコードに感染した。

しかし、その対応について誰にどのような権限が与えられているのかが分からなかったため、誰も何もできなかった。

その結果、被害の拡大防止措置が遅れ、運用に大規模な悪影響が出てしまった。

PCSの調査とリスク分析の 実施に関するプロセスを確立する

失敗事例：

リスクアセスメントを怠っていたため、重要なPCSが保護されていない状態に置かれたままだった。

他方で、重要ではない情報リソースの保護に必要以上のリソースが費やされていた

PCSの変更管理に関する プロセスを確立する

失敗事例：

ベンダがテスト・システム上でシステム変更の検証をしたが、そのテスト・システムの構成が実稼働環境と異なっていた。

後日、その変更を実稼働環境に適用すると、予期しない事態が発生してPCSが不安定になってしまった。

PCSの緊急時対応計画と インシデント管理に関する プロセスを確立する

失敗事例：

深刻な障害が発生し、PCSを完全に復旧せざるを得なくなかった。バックアップは定期的に実施されていたが、バックアップテープの取扱いが不適切で、復旧不可能なほどテープが劣化していた。また、障害に関する報告がなく、分析作業が行えなかった。

PCSのセキュリティ要件を、
このすべての計画・調達作業に
当初から定義し、適用する

失敗事例：

調達時にセキュリティ要件を考慮しなかったため、別の発注が必要になり、追加コストが発生した。加えて、導入後のセキュリティソリューションの品質が低く、複雑な設計となった。

良質のセキュリティ文化を醸成し、
PCSにおけるセキュリティの
必要性に関する意識を向上する

失敗事例：

定形的な運用状況下で、負荷が小さい時間帯に自分用のコンピュータを使ってスポーツ中継の視聴やチャットを行った。

その結果、そのコンピュータにスパイウェアが感染し、システムが使用不能になった。

PCS内に複数の
防護層を形成する
(多層防御)

失敗事例：

ファイアウォールを導入したが、別のセキュリティ保護のない接続を介してワークステーションをインターネットに接続した結果、侵入されてしまった。

ホスト型及びネットワーク型侵入
検知・インシデント監視手段を
PCSに24時間体制で導入する

失敗事例：

IDS(侵入検知システム)が、PCSで使われる特殊な通信プロトコルを理解するように設計されていなかったため、攻撃や攻撃試行の検知ができなかった

**PCSのリスク分析をシステム変更や
環境の変化に合わせて実施する**

失敗事例：

リスク分析の見直しを年に1回しか実施しなかったため、最近実施された大幅なシステム変更がリスク分析に反映されていなかった。このため、実際には変更後にミッション・クリティカルである制御システムのアクセス権限に対する要件が低いまま放置されていた。

PCS及び接続されたネットワークに対し、
技術的なセキュリティ監査を
定期的に実施する

失敗事例：

PLCのテストを実稼働環境内で実施した。

テストの影響で、装置の状態が不安定になり、制御コマンドを取りこぼしたり、正常に動作しなくなったりした。

PCSの物理的なセキュリティを 継続的に評価する

失敗事例：

PCS用のノートPCを無断で自宅に持ち帰った。
子供が、そのPCでオンラインゲームをした際に、
悪意のあるコードに感染した。
翌日、PCを検疫せずにPCSネットワークに接続
したため、ファイアウォールの内側で悪意のあ
るコードが感染を拡大してしまった。

PCSで発生するインシデントの
経過を追跡管理し, 組織外で
起きたセキュリティ問題の情報を
収集分析する

失敗事例：

インシデントの報告書がないため, セキュリティに関連する既存の作業の欠陥を見つけられなかった。その結果, ささいな誤操作がPCSの運用に被害や機能停止をもたらした。

ユーザグループや標準化機関等と、
PCSのセキュリティ強化を目的とし
たコミュニティを構築する

失敗事例：

標準化活動やセキュリティ対策活動が、ベンダやユーザの経験を反映させることなく進行したため、現場の実態から乖離したセキュリティ要件が策定された。

PCSに対する接続のルールを議論し、
安全な運用を維持する

失敗事例：

PCSとイントラネットの間に、公式には知られていない接続が存在した。

ある部門のコンピュータがワームに感染し、イントラネット上へ広がった際に、感染がPCSにまで広がり、運用が中断された。

システムベンダの協力のもと、
PCSを堅牢化及び
アップグレードする

失敗事例：

制御システムに精通していない人員にシステムの堅牢化を担当させた。

その結果、滅多に使われないが必要不可欠なコンポーネントが不用意に削除されてしまい、システムが不安定になった。

まとめ

- セキュリティ対策の考え方の基本は、情報システムにおける対策と同じ
- 制御システム固有の難しさを理解した上で、セキュリティ対策を検討することが必要
 - 制御システム担当部門とセキュリティ担当部門の交流を！
 - 制御システムまで情報セキュリティ・ポリシーと施策の拡大を！
- 制御システム(中身自体と他のシステムとの関係)の進化に注意
 - 定期的なリスク評価の見直しを！
 - 制御システム更改時にセキュリティ要件を織り込め！

ご清聴ありがとうございました

謝辞：

この講演資料は、中央大学大学院理工学研究科の巴洋一さんが「ISSスクエア」のインターンシップの活動の中で作成されたものをベースとしています。

Q & A

参考資料：

JPCERT/CCのウェブ・ページ(<http://www.jpCERT.or.jp/>)の「制御システムセキュリティ」のコーナーをご参照ください。