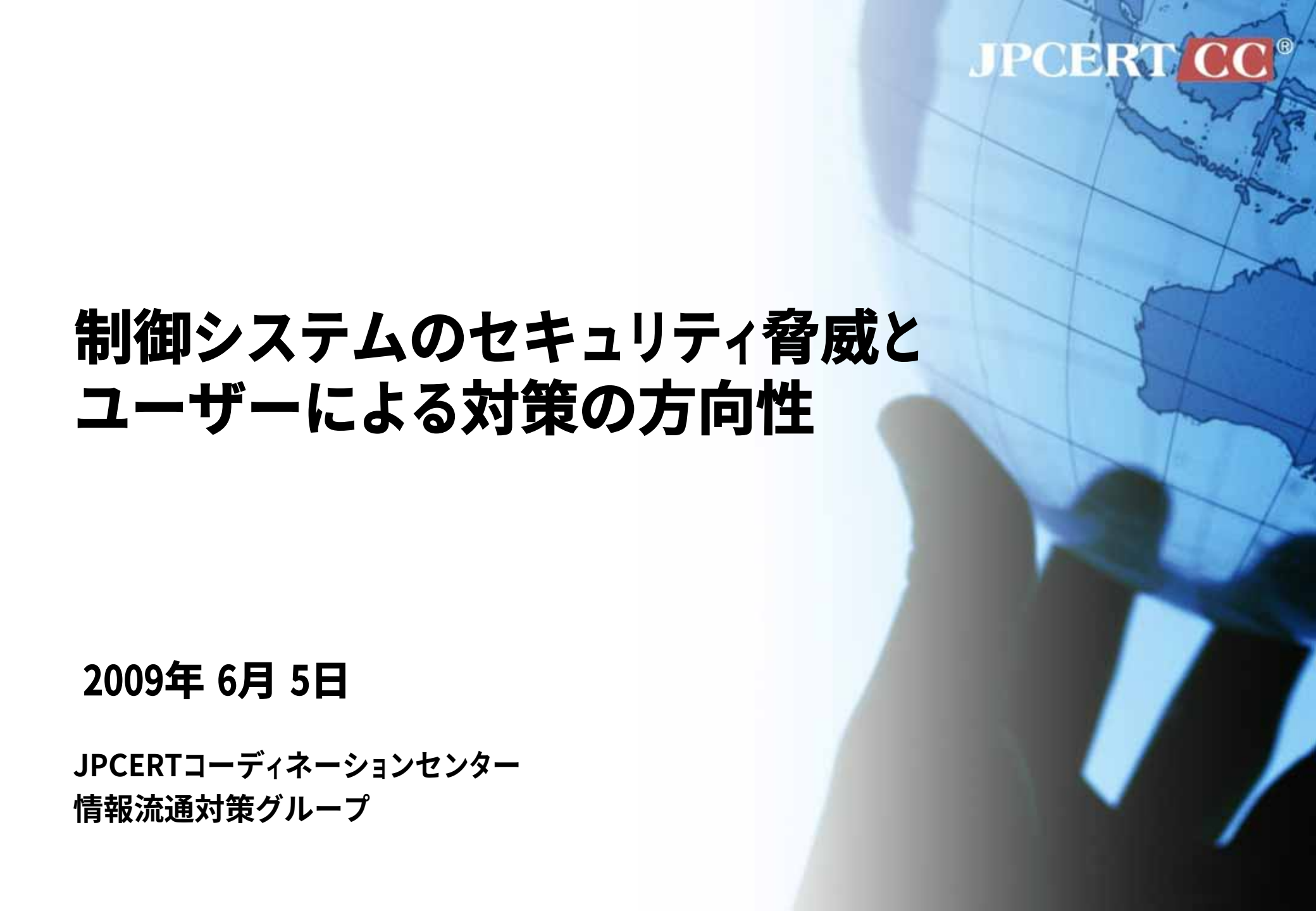


制御システムのセキュリティ脅威とユーザーによる対策の方向性

2009年 6月 5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

本日のアジェンダ

- 制御システムにおける脅威（事例）
- 制御システム関連ソフトウェアで報告された脆弱性
- 汎用IT系ソフトウェアで報告された脆弱性
- 対策が必要な理由
  - 制御システムにおける技術環境の変化
  - 制御システム＝価値ある情報資産
- ヒアリング結果から懸念される点
- 制御システムにおけるセキュリティ対策の方向性

制御システムにおける脅威（事例）

JPCERT CC®

- 事例1：ウイルス感染による制御システムの停止
  - メンテナンスのため外部よりPCを持ち込んで接続し、システムのPCにウイルス感染
  - システム停止には至らないが監視・制御機能を阻害
  - 大きな悪影響が無いと考え対策を取らずにトラブルを繰り返す場合も

- 事例2：システム内のプログラム／記録等の漏えい
  - 製造装置内の制御プログラムをリバースエンジニアリングされた疑い
  - 現場の機器から抜き出された可能性

制御システム関連ソフトウェアで報告された脆弱性 (2008年以後に国際的に周知された案件)

公開日	JVN における案件名
2009年 2月13日	GE Fanuc Proficy HMI/SCADA iFIX の認証機能における脆弱性
2009年 2月10日	AREVA e-terra habitat に複数の脆弱性
2009年 2月10日	GoAhead WebServer に情報漏えいの脆弱性
2009年 2月10日	Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge に URL リダイレクションの脆弱性
2009年 2月10日	Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge にクロスサイトスクリプティングの脆弱性
2008年 9月29日	ABB PCU400 にバッファオーバーフローの脆弱性
2008年 6月12日	Citect 社製 CitectSCADA におけるバッファオーバーフローの脆弱性
2008年 5月 7日	Wonderware SuiteLink における NULL ポインタ参照の脆弱性
2008年 1月28日	GE Fanuc Proficy Information Portal が認証情報を平文で送信する問題
2008年 1月28日	GE Fanuc CIMPLICITY HMI にヒープバッファオーバーフローの脆弱性
2008年 1月28日	GE Fanuc Proficy Information Portal が任意のファイルをアップロードおよび実行を許可する問題

汎用IT系ソフトウェアで報告された脆弱性 (2008年以後に国際的に周知された案件)

- 汎用IT系技術は、常に脅威にさらされている

- 著名な製品で公開された脆弱性の登録件数(※1)
  - Microsoft 製品
    - Windows XP：112件、IE：83件、Office：59件、 Excel：9件
  - Adobe 製品
    - Acrobat Reader：15件
  - Sun 製品
    - JAVA：7件
  - Linux 製品
    - Linux　オペレーティングシステム：49件

※1　NVD (National Vulnerability Database) で2008/1/1～2009/5/31の公開件数を検索

対策が必要な理由：
制御システムにおける技術環境の変化

JPCERT CC®

- 汎用IT技術が制御システムに導入され始めた
  - リアルタイム性が要求される個所が限定されてきた
    - 必要な機能を整理することで棲み分けが可能になってきた
  - 使い勝手がよい
    - 高性能･安価･入手が容易
    - 従来の製品に比べて扱い易く、種類も豊富
    - 省配線も実現できる
    - 遠隔からの確認や操作を行うのに便利
    - CSVデータ処理やPDFファイルの閲覧等のアプリ利用が利用できる
    - 開発環境も充実している
  - 制御システムと社内情報システムが強く連携
    - 制御情報ネットワークにおける現場のコンピューティング推進

対策が必要な理由：
制御システムにおける技術環境の変化

JPCERT CC®

- コスト削減が汎用IT技術の導入を促進する
  - ユーザ企業における導入費や保守費削減
  - 開発ベンダにおける開発コスト削減
  - 汎用IT技術を使いたくなくてもやむを得ない状況になりつつある

- そして脅威も付いてきた
  - 汎用IT技術の脅威は、外部のネットワークからの攻撃だけではない
  - PDFやオフィスファイル、メールを開くだけで発現する脅威もある
  - 外部のWebページ閲覧だけで呼び込む脅威もある
  - 個人レベルではどんなに注意していても、隣席のPCから始まる脅威もある
  - 脅威に備えて準備する手間が、結果的には不要なコストを削減する事になっていくだろう

対策が必要な理由：
制御システム＝価値ある情報資産

- 生産のノウハウは制御システム上に蓄積される
  - 工程、システム構成、個々の機器の設定、ログなど
  - 企業の価値につながっている情報
  - 攻撃者にも価値がある（ノウハウの転売を目的とする攻撃の可能性）

    （参考）：　装置として輸出されるシステムからのリバースエンジニアリング

    内部犯による技術情報の漏えい

- 制御システム自体を企業の情報資産として捉え、資産価値に見合った対策をとることが求められる

ヒアリング結果から懸念される点

- システムが外部と接続される機能･機会は以前より増えている
  - メンテナンス用PCの持込み／持出し
  - リムーバブルメディア（USBメモリー等）の運用時の利用
  - プログラム、設定等のネットワーク更新

- ネットワーク接続における懸念点
  - 攻撃のベクトルは外部からだけではなく、内側から取り込む事もある
  - オフィスと制御システム用PCやサーバがネットワークでつながる
  - 汎用ITのネットワーク機器の増加
    - 無防備なポートへの不用意な接続ひとつで対策がバイパスされてしまう可能性も

- 個人のスキルへの依存が低い場合の人の流動性も懸念点の一つ

ヒアリング結果から懸念される点

- 制御システムに関連するPCのセキュリティ対策は十分だろうか
- オペレータコンソール
  - 監視、制御等に用途が限定されたPC
    - 専用筐体に作りつけられていることも。「実は中身がPC」という機器も存在しうる
  - 多くの場合、構成や接続状況は構築時のまま変更されない
    - セキュリティ脆弱性を持ち続ける（特にOS）

ヒアリング結果から懸念される点

- 作業用PC（エンジニアリング用PCなど）
  - ウェブアクセス、メール、資料の閲覧、帳票への記入、プログラム作成 等
  - プライベートでも使い慣れたOSで提供される事も多い
    - 制御システム稼働後に変更が加えられることもある
    - 慣れからくる油断から、本来の用途以外で使われることもある
  - 社内LANと制御システムの橋渡しとして使われる事もある
    - 汎用の技術が使われており、専門知識を持たない者でも取り扱える

ヒアリング結果から懸念される点

- 無線LAN
  - ステータス確認や監視等、一部では既に利用されている
    - スマートフォン等の端末を利用したステータスの確認
      - スマートメータなど
  - 現状利用されているのは802.11xの技術が多い
    - 無線LANのパケットの採取は容易
    - 重要度によって解読されにくい暗号化は必須

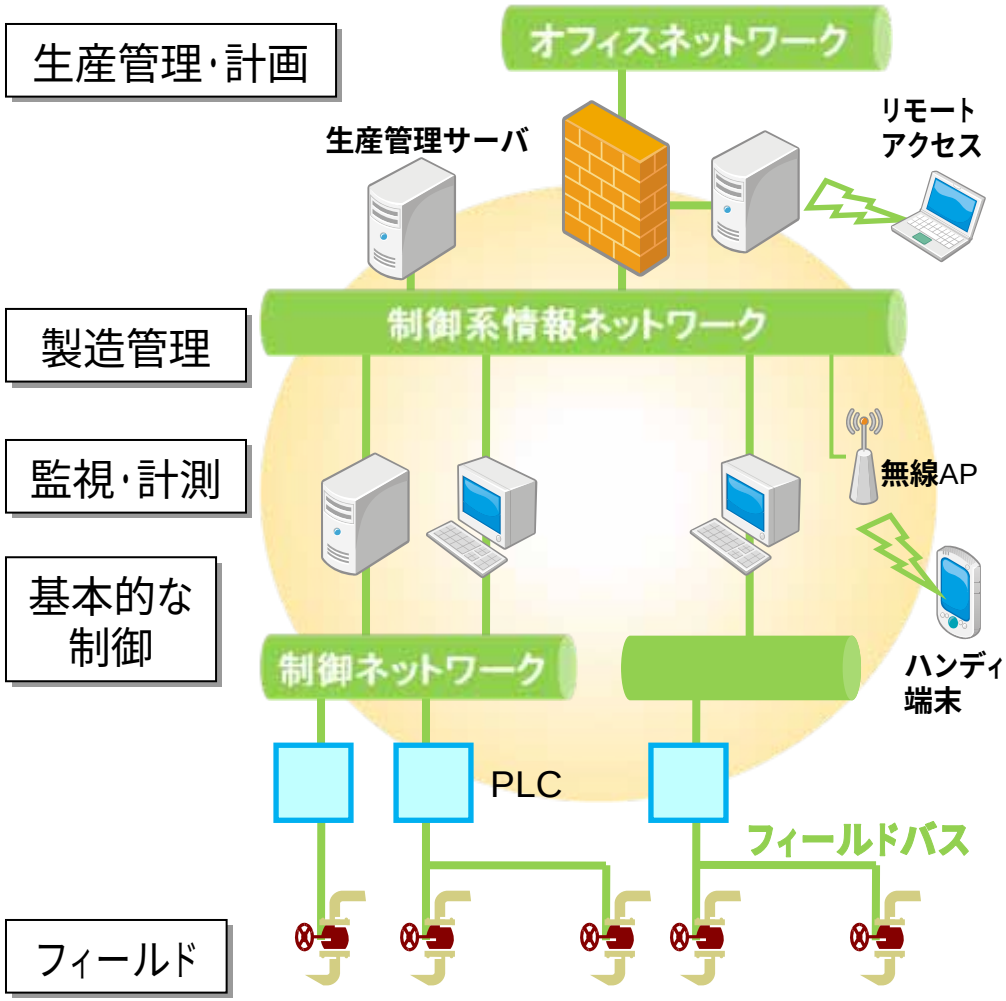
制御システムにおけるセキュリティ対策の方向性

- ユーザはセキュリティ対策を求めない？
  - 汎用IT技術の導入によってもたらされるセキュリティリスクについて、正しく理解しているユーザは多くはない
  - インターネットに繋がっていないから大丈夫、と考えるユーザは多く、コスト削減の対象とする傾向がみられる
  - セキュリティ対策が守るのは情報資産の安全だけではなく、サービス・事業の継続性である事の理解を求め、望まれるセキュリティ要件を抽出する事が必要となる

- セキュリティ対策の導入を望む場合でも・・・
  - 明確なセキュリティポリシーを提示できるユーザは少ない
  - 守るべきものは何かを明確に把握できなければ、必要な要件も定義できない
  - 制御システムと汎用IT技術の両方に知見のある人材がまだまだ少ない

制御システムにおけるセキュリティ対策の方向性

- ネットワークからの脅威への対策
  - 基本的なネットワーク構成を踏襲するだけでは、漏れてしまう盲点
    - ネットワークモデル図は、垂直型の外部からの攻撃に対して有効
    - 攻撃ベクトルは外部からだけではない。内側から取り込む脅威もある
    - 水平型の脅威（同一セグメント上のPCの汚染）は考慮されているか
    - IP等による論理的な接続を拒否する手段は有効
    - Firewall を過信していないか。配置やルールは適切か
    - 物理的な接続はどうか。無防備にさらされたポートから始まる脅威もある



制御システムにおけるセキュリティ対策の方向性

JPCERT CC®

- ユーザーに必要なセキュリティ体制
  - 構築段階、運用段階の両輪での取り組み
  - 何が守るべき対象か、それを守るために何をしなければならないかの把握
  - それを実現するためのシステムの構築、あるいは運用手段の導入
  - 運用実態を踏まえた包括的なポリシーやルールの整備
  - 構築後の適切な運用のために関係者を教育

制御システムにおけるセキュリティ対策の方向性

- セキュリティ体制構築で最低限考慮すべき事項
  - ソーシャルエンジニアリングを考慮した情報管理を行っているか
    - 管理者権限は適切に設定されているか。不適切な人に不要な権限を与えていないか
    - 情報の重要度は設定されているか。不適切な人に不要な情報を与えていないか
  - ネットワークの構成は正しいか、垂直・水平・論理・物理の安全は考慮されているか
    - 社外のネットワークにアクセスするリスクは管理しているか
    - 制御系情報ネットワークの水平位置につながる機器への不用意なUSB接続やアプリ・データ導入が行われないように管理しているか
    - Firewall があるという事実で満足していないか。都合のいい設定がされていないか
    - 制御ネットワークを構成するネットワーク機器が不用意に利用されないように、機器の物理的配置を考慮しているか
    - 無線LANは、適切な用途と暗号技術を選んでいるか
  - 機器を扱う作業者に、機器の取り扱いやセキュリティに関する教育を行っているか。
    - アプリやデータの導入、パッチの適用を行う際、それを事前にテストしているか
    - USB等の接続がもたらす問題の可能性について、きちんとした認識を持たせているか
    - Windows であっても、扱う機器が制御系システムの一部である事の認識をきちんと持たせているか。勝手に変更が加えられないように管理を徹底しているか

連絡先

- JPCERT コーディネーションセンター (代表)
  - Email: office@jpcert.or.jp
  - TEL: 03-3518-4600
  - URL: http://www.jpcert.or.jp/
- 制御システムセキュリティに関するお問合せ
  - Email: scada@jpcert.or.jp
  - TEL: 03-3518-4600