制御システムセキュリティカンファレンス 2009
有限責任中間法人 JPCERT コーディネーションセンター (JPCERT/CC)

1.目的　近年、制御システム分野においても、一般の情報システムと同様に、情報セキュリティ対策の必要性が強く認識され始めています。制御システムに関わる技術者がセキュリティ関連情報を収集し対策を行う作業の負担を軽減し、セキュリティレベルの向上に必要な課題を効果的に解決するためには、製品ベンダー、ユーザー企業および情報セキュリティ分野の専門家による脅威や対策に関する情報の共有と連携が重要です。

そこで、JPCERT コーディネーションセンターは、経済産業省と共催で、制御システムに関するセキュリティ関連課題を共有し、解決に向けた関係者間のより強固な連携の構築に向け実りある議論を行い、ひいては国内における制御システムの情報セキュリティ対策の実効的推進に資することを目的として「制御システムセキュリティカンファレンス 2009」を開催します。

関係各位のご参加をお待ちしております。

目黒雅叙園 2階
2009年2月19日（木）

特別対談
制御システムセキュリティの課題と方向：これまでの取り組み、現状とこれから

電気通信大学 教授
新 誠一
帝京平成大学 教授
江木 紀彦
【聞き手】
JPCERTコーディネーションセンター 業務統括
伊藤 友里恵

大規模プラント・ネットワーク・セキュリティ
ー　重要システムのサイバーテロリズム、クラッキング対策　ー

PSEC　WG5　の発表（磯村論文）より引用

セイフティ『安全』 と　セキュリティ『安全保障』 の違いは何か

リスクの評価：脅威×脆弱性×資産価値　⟷　ROI　投資の価値

技術的

・サイバーテロの実体
・セキュリティ運用ガイドライン
・セキュリティ評価基準
・対サイバーテロ　コンティンジェンシープラン
・制御系システムのセキュリティ機能

非技術的

・情報セキュリティマネジメント：
　　ISO17799（BS7799　Part1相当）－2000年12月1日発行
　　GMITS（Guideline for the Management of IT Security)
・ソーシャルエンジニアリング
・ネットワークの安全性検証実験
・プラント・ネットワークのリスク分析

サイバー・テロリズム ⇒ 情報戦争（Information Warfare Class III)

国家レベル： 政府等国家に対する敵対行為

例 ・発電所の停止
・鉄道ネットワークへの妨害
・バンキングシステムへの妨害

企業レベル：

① 企業内情報システムの停止、攪乱
ネットワーク（経営情報、生産情報、配送管理）に障害を起こす

② 生産設備の停止
1．閉鎖的システム 自損事故のみか
2．オープン化システム
A 部分的妨害（情報系のみ）
B 生産管理への妨害

対策

脅威の分析　（枯れススキに怯えない）
脆弱性分析
経営者の自覚
セキュリティ技術者の養成

社会的には、不正アクセス、ウィルスの跋扈がある。

現状：　ウィルスの存在は当たり前
　　防御は個人の責任

PCの製造過程でウイルスの埋め込み有
（検査で使うメモリーにウイルス）

メモリスティックに感染（以前はFD）

プラントの制御系のオープン化により問題の拡大

システム化の程度により、蒙る被害は異なる

① プラントへのコンピュータ システムの導入
コンピュータ システムを全く使っていないプラントはあるか
たとえば、全て空気式、手動式のみなら安心である

② 情報系が活用されているプラント

データ処理系のみオープン化

運転指示・管理系までオープン化

遠隔地にあるプラントのリモート・オペレーション

③ 運転の妨害 （あるとすれば、侵入より潜入で時間をかけて行う）

A 遮断（停止）する	○
B 不良品を製造させる	△
C 災害を起こす	×

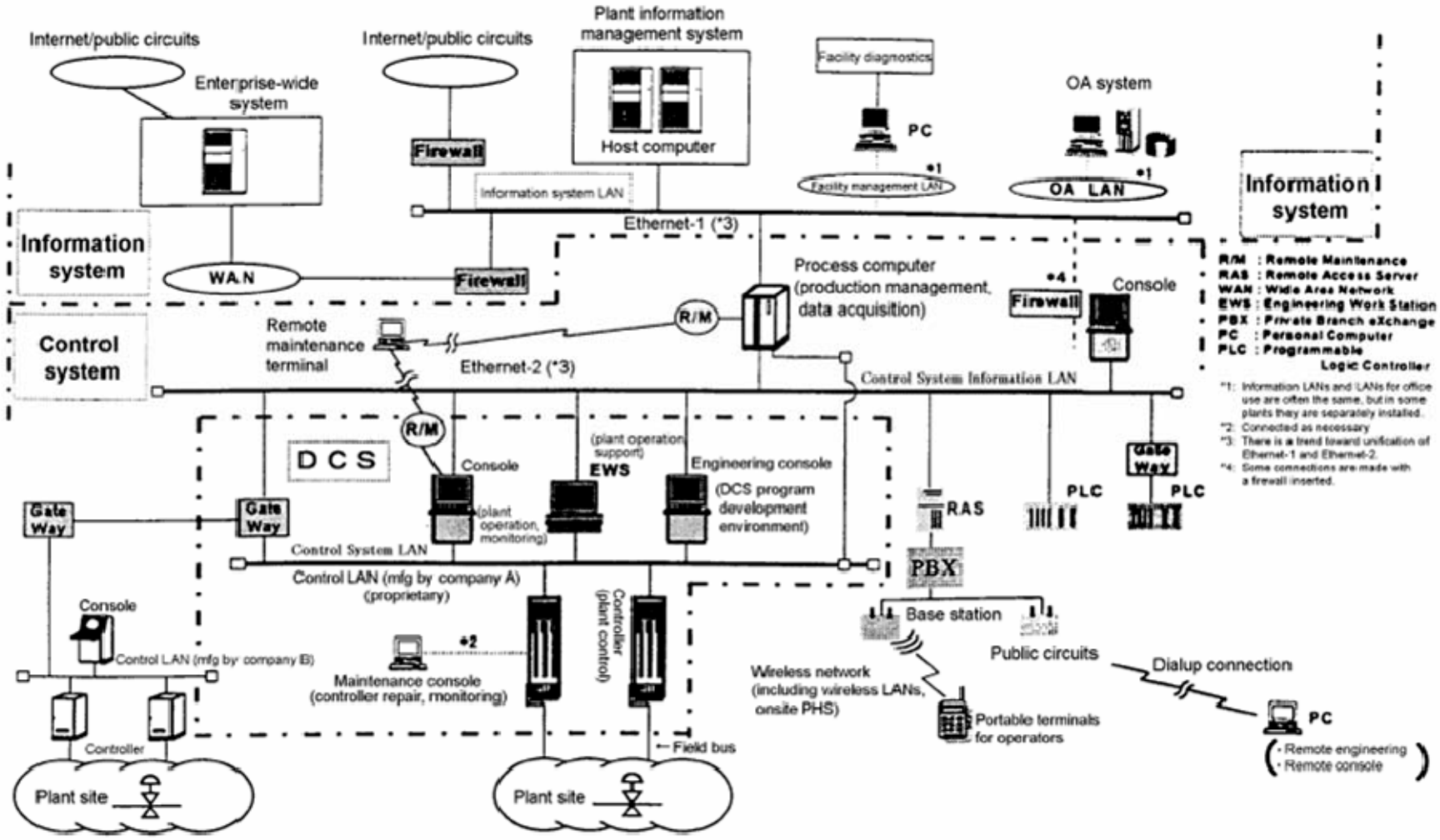
制御系のセキュリティ対策

1. 一般的でない（普及していない）ソフト（システム）の使用
   実時間対応なので、大体は一般的でないシステムを採用している
2. 汎用品の使用制限
   汎用品のソフト情報は公知である
3. ノウハウ保持の人材の管理　　労務管理　安易な解雇などは注意
4. 不用意な行動の絶滅（ウイルスの持込、感染の手伝い）
   個人所有のメモリー類の使用禁止
5. 成りすまし　の防止　　関係者の識別方法
6. Back　Door　作成の禁止
   保守（特にリモートメンテナンス）での注意

（関連メーカ、保守会社のセキュリティ対策）

ブログ炎上問題：　無責任な書き込み：無記名でできること

では、プラントの運転系で可能か？（面白半分でプラントを停止できるか）


Internet/public circuits
Enterprise-wide system
Internet/public circuits
Plant information management system
Host computer
Facility diagnostics
PC
OA system
Firewall
Information system LAN
Facility management LAN
OA LAN
*1
Ethernet-1 (*3)
Information system
Information system
WAN
Firewall
Process computer (production management, data acquisition)
*4
Firewall
Console
Control system
Remote maintenance terminal
R/M
Ethernet-2 (*3)
Control System Information LAN
R/M : Remote Maintenance
RAS : Remote Access Server
WAN : Wide Area Network
EWS : Engineering Work Station
PBX : Private Branch eXchange
PC : Personal Computer
PLC : Programmable Logic Controller
*1: Information LANs and LANs for office use are often the same, but in some plants they are separately installed.
*2: Connected as necessary
*3: There is a trend toward unification of Ethernet-1 and Ethernet-2.
*4: Some connections are made with a firewall inserted.
DCS
R/M
Console
(plant operation, monitoring)
(plant operation support)
EWS
Engineering console
(DCS program development environment)
Gate Way
Gate Way
Gate Way
RAS
PLC
PLC
Control System LAN
Control LAN (mfg by company A) (proprietary)
PBX
Console
Control LAN (mfg by company B)
*2
Maintenance console (controller repair, monitoring)
Controller (plant control)
Base station
Public circuits
Dialup connection
Wireless network (including wireless LANs, onsite PHS)
Portable terminals for operators
PC
(• Remote engineering • Remote console)
Controller
Field bus
Plant site
Plant site

情報系ＬＡＮ	Information System LAN
制御（系ＬＡＮ	Control System LAN
不正アクセス	Unauthorized access
侵入	Intrusion
	*(penetration, to break into)
なりすまし	Identity theft
破壊	Destruction
サービス妨害（業務妨害）	Denial of service (DoS)
脆弱性	Vulnerability
セキュリティホール	Security hole
識別	Identification
認証	Authentication
暗号化	Encryption
復号化	Decryption
不正操作	Unauthorized operation
停止（コンピュータ、システムの）	Shutdown
改ざん	Falsification
汎用ＯＳ	Open OS (Operating System)
暗号	Cryptograph
（独自、専用）カスタムＯＳ	Custom OS
オープンネットワーク	Open Network
プロコン	Process computer
エンコン	Engineering console
オペコン	Operator console

(*)シンポジウム(99/10/01)講演資料内で使用