重要インフラシステムと情報セキュリティ

－制御監視系のシステムにおける脆弱性を取り巻く問題について－

有限責任中間法人 JPCERTコーディネーションセンター
早期警戒グループ
情報セキュリティアナリスト　不破　譲

目次

- JPCERT/CC概要
- 脆弱性情報ハンドリング
- JVNで公開した制御監視系関連製品の脆弱性
- 増加する制御監視系システム関連脆弱性
- 制御監視系システムに発見される脆弱性関連情報の取り扱いの現状課題
- 課題への取り組み
- 日本の状況

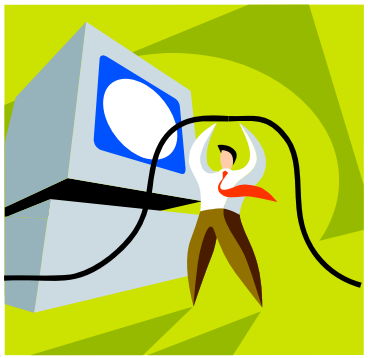
JPCERT/CC概要

Japan Computer Emergency Response Team Coordination Center
ジェーピーサートコーディネーションセンター

インターネットを介して発生する侵入やサービス妨害等の
コンピュータセキュリティインシデント*に関する以下のサービスを
技術的な立場から行っている組織です。

- インシデント関連情報の窓口対応および対応支援
  - インシデントハンドリング
  - 脆弱性情報ハンドリング
- 国内向け技術情報の配信
  - 注意喚起、調査結果、その他
  - インターネット定点観測システム(ISDAS)
- セキュリティインシデント対応体制の強化
  - 国内外の関連組織との連携および協業

*コンピュータセキュリティに関係する人為的事象で、意図的及び偶発的なもの



- 2004年経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」にて
  脆弱性情報流通調整機関に指定受け、脆弱性関連情報ハンドリング事業を展開

JPCERT/CCの活動

JPCERT CC®

インシデント予防

脆弱性情報ハンドリング

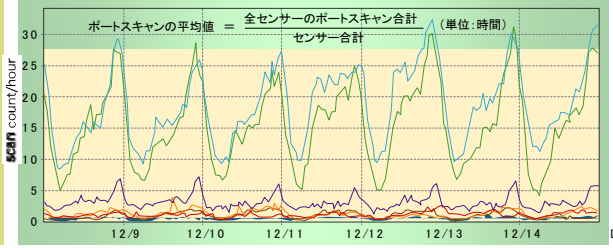
未公開の脆弱性関連情報を
製品開発者へ提供し対応依頼
国際的に情報公開日を調整

JVN
JP Vendor Status Notes

インシデントの予測と捕捉

定点観測（ISDAS）

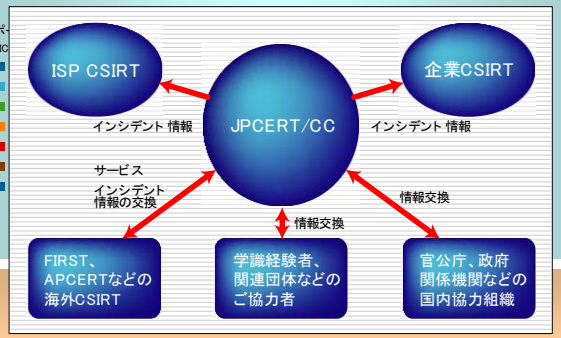
ネットワークトラフィック情報
の収集分析
定期的なセキュリティ予防情報の提供



発生したインシデントへの対応

インシデントハンドリング

インシデントレスポンスの時間短縮による
被害最小化
再発防止に向けた関係各関の情報交換
および情報共有



早期警戒情報

重要インフラ事業者等の特定組織向け情報発信

CSIRT構築支援

企業内のセキュリティ対応組織の構築支援

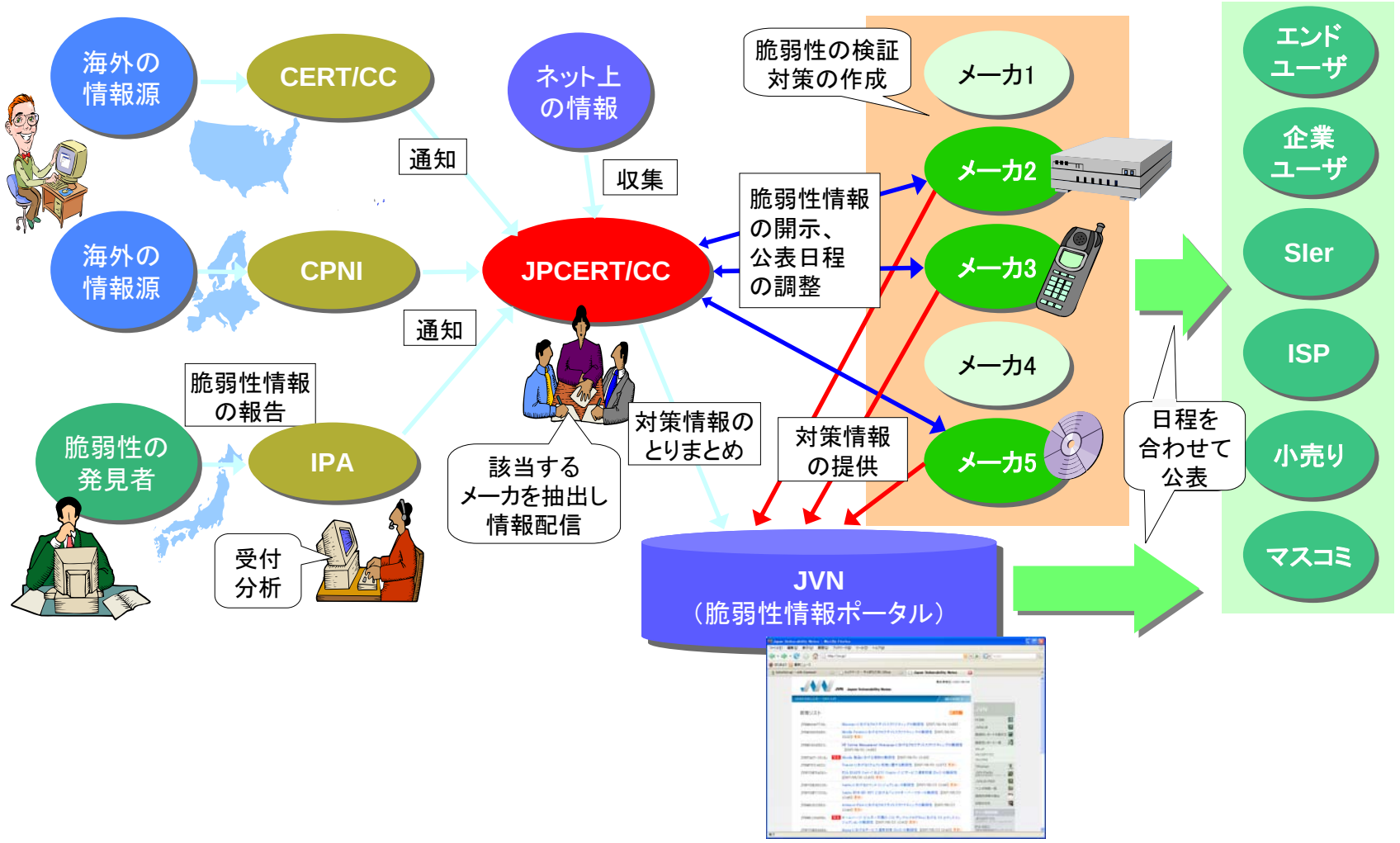
JPCERT/CCの脆弱性情報ハンドリング
情報セキュリティ早期警戒パートナーシップ

JPCERT CC®

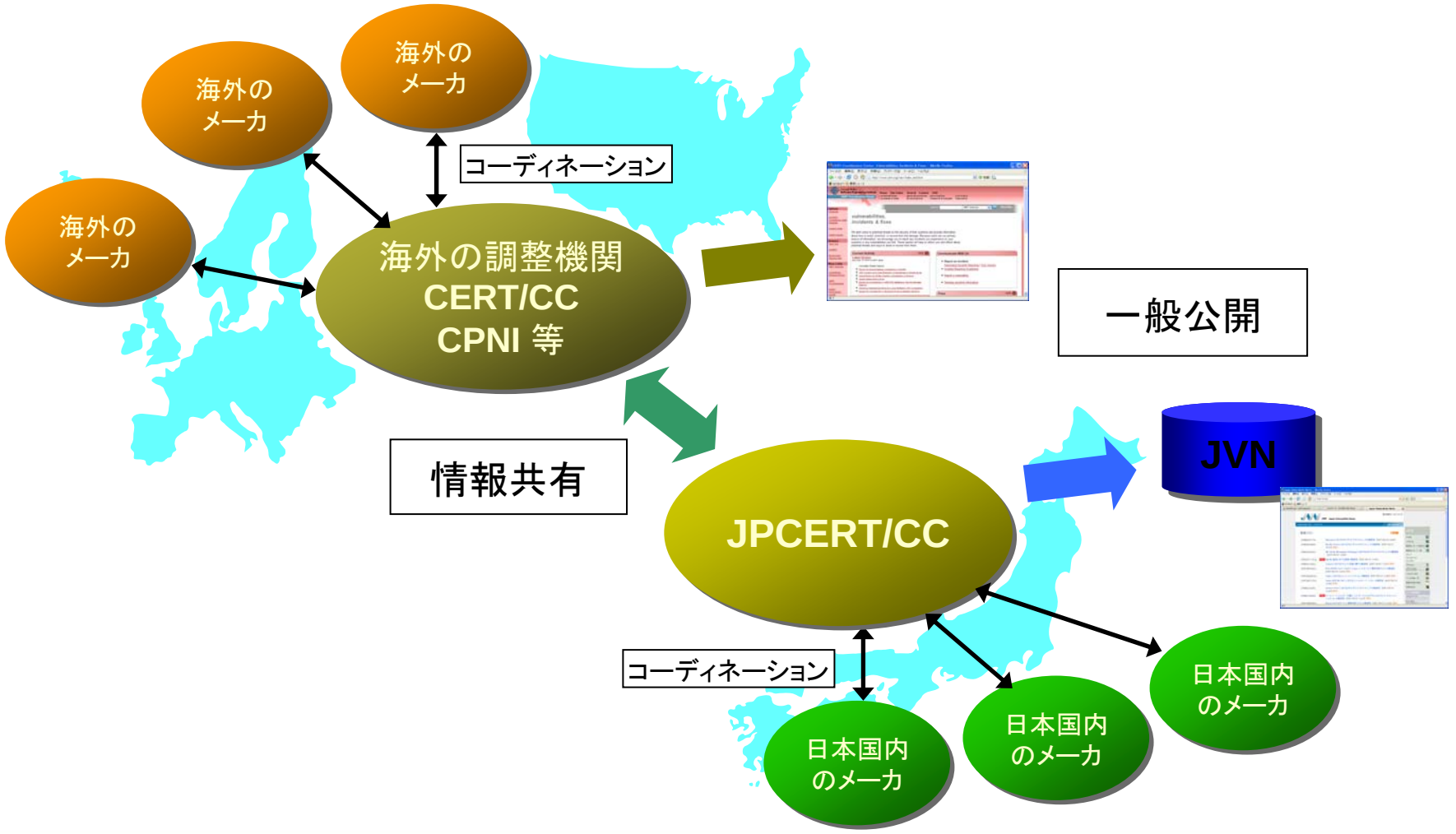
- 脆弱性関連情報を、適切な関係者へ事前に開示し、被害を最小限に食い止めるためのプロセス
  - 未公開脆弱性情報の受付 ⇒ 検証 ⇒ 製品開発者に開示
  - 国外の関係機関（CERT/CC、CPNI等）と連携し、国内外の製品開発者へ情報展開
  - 関係するすべての製品開発者が同時に情報公開するよう調整
  - 脆弱性情報ポータルサイト（JVN）を運営し、脆弱性情報と各社の対応を公開

- 経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づく活動
  - JPCERT/CCが調整機関として指定
  - JEITA、JNSA、JISA、CSAJ、IPA、JPCERT/CC が協同で「情報セキュリティ早期警戒パートナーシップ」ガイドラインを策定

JPCERT/CCの脆弱性情報ハンドリング
脆弱性情報流通の枠組み



JPCERT/CCの脆弱性情報ハンドリング国際的な枠組みについて



JPCERT/CCの脆弱性情報ハンドリング
脆弱性案件の種類

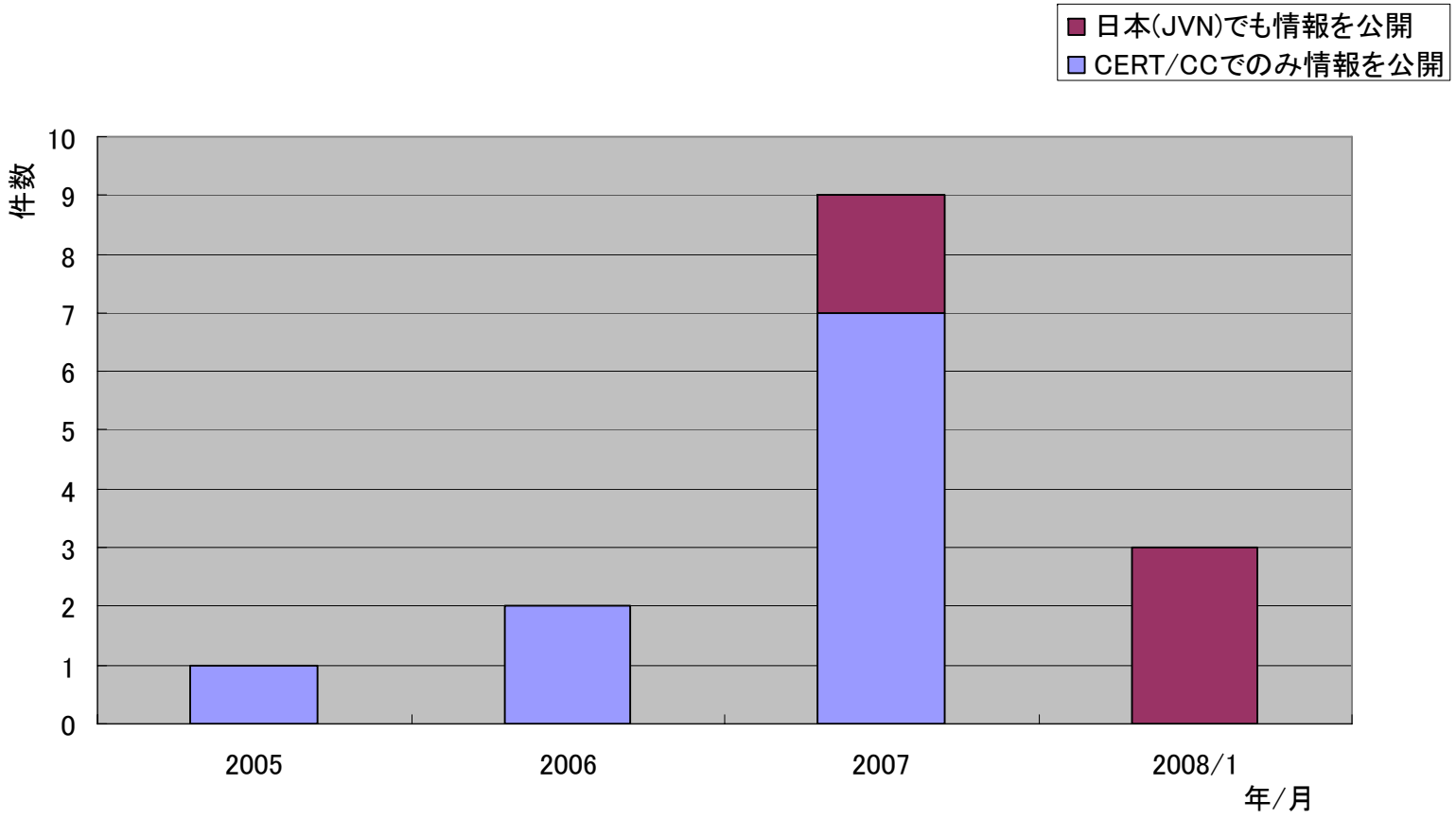
- 特定の製品開発者における特定の製品に関わる脆弱性
  - 例えば、“Microsoft Internet Explorer のxx機能の脆弱性”など
- 複数の製品開発者にまたがる、汎用技術の根本的な問題による脆弱性
  - 通信プロトコル
  - ライブラリ
  - その他
  - 制御監視系システムのプロトコル

JPCERT/CCが報告を受け調整しJVN※で公開した制御監視系関連製品の脆弱性

- 2007/03/22　JVNVU#296593:
  - NETxAutomation 社製 NETxEIB OPC Server にOPC server handle を適切に処理できない脆弱性
- 2007/03/19　JVN#83832818:
  - Interstage Application Server におけるクロスサイトスクリプティングの脆弱性
- 2007/03/16　JVNVU#202345:緊急
  - デバイスエクスプローラ MELSEC OPC サーバにバッファオーバーフローの脆弱性
- 2007/03/16　JVNVU#346577:緊急
  - デバイスエクスプローラ MODBUS OPC サーバにバッファオーバーフローの脆弱性
- 2007/03/16　JVNVU#347105:緊急
  - デバイスエクスプローラ HIDIC OPC サーバにバッファオーバーフローの脆弱性
- 2007/03/16　JVNVU#926551:緊急
  - デバイスエクスプローラ TOYOPUC OPC サーバにバッファオーバーフローの脆弱性
- 2007/03/16　JVNVU#907049:緊急
  - デバイスエクスプローラ FA-M3 OPC サーバにバッファオーバーフローの脆弱性
- 2007/03/16　JVNVU#581889:緊急
  - デバイスエクスプローラ SYSMAC OPC サーバにバッファオーバーフローの脆弱性
- 2008/01/28　JVNVU#308556:
  - GE Fanuc CIMPLICITY HMI にヒープバッファオーバーフローの脆弱性
- 2008/01/28　JVNVU#339345:
  - 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
- 2008/01/28　JVNVU#180876:
  - GE Fanuc Proficy Information Portal が認証情報を平文で送信する問題

※Japan Vulnerability Notes http://jvn.jp

増加する
制御監視系システム関連脆弱性



CERT/CCで公開された制御系システム関連脆弱性

なぜ制御監視系システムの脆弱性報告が増えてきているのか

- ベンダー固有の技術からオープン化へ
  - —通信のIP化、TCP/UDP、他（産業用Ethernet等）
  - —CC-Link 、FL-net（OPCN-2）
  - —汎用基本OSの採用
    - Windows,Linux,Solaris
    - Embedded OS(ITRON,Linux,RealTimeOS,Windows Emmbedded)

<u>オープン化されることで、プロトコル研究・脆弱性調査等の対象となってきている。</u>

制御監視系通信規格、プロトコル例（一部）

Foundation Fieldbus/H1	FL-net (OPCN-2)	JDDAC
Foundation Fieldbus/HSE	TCnet (Time-critical Control Network)	ICCP/TASE.2, IEC 60870-6
INTERBUS	SERCOS	IEC 60870-5 (101, 102, 103, 104)
Modbus	Data Highway DH, DH II, DH+	IEC 61850
Modbus Plus	GE CCM	IEC 62351
Modbus TCP	GE Series 90 Protocol (SNP) and SNP-X	DNP3
Profibus	GE Service Request Transfer Protocol (SRTP)	HNZ
Profinet	HART (Highway Addressable Remote Transducer)	GenLink
Common Industrial Protocol (CIP)	NetDDE, FastDDE	CIM / IEC 61970 and 61968
ControlNet	P-NET	UCA 2.0
DeviceNet	SINEC-H	OpenAMI
Ethernet/IP	SSCNET	SINAUT
MECHATROLINK	Vnet	Manufacturing Message Specification (MMS) ISO 9506
Omron Host Link	Vnet/IP	BACnet (ISO/IEC 16484-5)
Omron FINs	WorldFIP /EN50170	BACnet/IP
Actuator-Sensor (AS) Interface	EtherCAT (Ethernet for Control Automation Technology)	Home Bus System (HBS)
ARCNET	Ethernet Powerlink (EPL)	KNX, IEC 14543
Controller Area Network (CAN)	Zigbee	KNXnet/IP
CANopen	IEEE 802.15.4	LonTalk (Echelon) EIA-790.1
MELSECNET/H or /10	OPC	SISA/QD2
CC-Link	OPC UA	DF1

2000年以降の重要インフラのシステムに関連したインシデント

JPCERT CC®

- 海外）
  - 2001年9月11日　米国）同時多発テロ事件
  - 2003年8月　米国）北東部停電
  - 米国）揚水貯蔵ダム決壊
  - 豪）下水処理システム侵入・汚水流出
  - ルートDNSサーバーへのDDos攻撃
  - エストニア公共サービスWebサイトへのDDos攻撃
  - 電力システム脅迫
- 国内）
  - ファイル共有ネットワークへの情報漏洩

制御監視系システムに発見される脆弱性関連情報の取り扱いの現状課題

- 汎用ソフトウェアシステム業界で5年前に課題となっていたこと
  - 発見者が脆弱性情報を開発者に通知したくても、開発者への適切なパスがなかったり、受け付られなかったりすることがあり、発見者が情報を開示してしまったり、脆弱性の修正が遅れることがあった
  - 脆弱性関連情報、また修正情報の開示方針が定まらず、複数の実装に共通に影響を及ぼすような脆弱性の場合、情報開示に伴うリスクが高くなることがあった
- 上記の問題は、制御監視系システムの仕様に発見される脆弱性の修正、調整を行う関係者（発見者、調整機関、制御監視系システムベンダ等）が、同じく現在抱えている状況
- 脆弱性関連情報公開方針：ソフトウェア業界の解
  - 調整機関に対してベンダが脆弱性対応連絡窓口を登録、または一般に対して脆弱性情報の受付窓口を公開
  - 脆弱性情報を隠しておくのは得策ではない
    - 情報公開により、脆弱性によるリスクをユーザに適切に周知し、対策の適用を促す
    - いずれ悪意の第三者が脆弱性を発見し、攻撃に利用される可能性が高い
  - 中立な調整機関を通し、すべての関係者が同時に情報公開するよう日程調整する枠組みを構築した
  - 「公表日一致の原則」の遵守
    - 脆弱性情報と、対策情報を同時に公開する
    - 脆弱性の影響を受けるすべての製品開発者が同時に情報公開する

制御監視系システム関係者における この課題への取り組み

- 海外においては、制御監視系システム運用者、ベンダ、調整機関、関係政府機関が集まって脆弱性関連情報公開方針や各種課題について、再度議論の動きが活発化している
  - 必要だという意見と、汎用システムと同じく扱うべきという意見の調整が必要
- 米国
  - Process Control Security Forum (PCSF) と Control Systems Cyber Security Vendor Forum (CSCSVF) が合同でミーティング (2007)
    - https://www.pcsforum.org/library/files/1196793082-Vendor_Forum_Aligns_with_PCSF.pdf
- イギリス
  - CPNI (国家インフラ防御センター)は、制御監視系システムベンダと、制御監視系システム運用事業者 それぞれの情報共有グループを運用

日本の状況は？

日本の状況
1997　大規模プラントネットワークセキュリティ対策委員会　提言

制御監視系システムの変遷

第1 世代	1970 年代～ 1980 年代後半	● コンソール、コントローラともベンダ各社のOSを使用している。 ● 制御監視系システムと情報系システムとの通信は、回線容量 が小さく、1対1で接続されており、データ交換などの アプリケーション層の通信プロトコルはベンダ固有または接続の都度相互に決めて行われていた。
第2 世代	1980 年代後半 ～ 1990 年代前半	● コンソールのOSは主にUNIX、コントローラはベンダ独自のOSを使用している。Ethernet 接続は情報系LANや制御監視系情報LANの中 でもごく一部に限られており、パソコンのネットワーク はまだ普及しておらず、社外へのインターネットなどとのオープンな接続もほとんどない。制御LANはベンダ 固有の通信プロトコルを採用している。 ● UNIX系OSとTCP／IPプロトコルに精通した者であればコンソールまでの不正侵入は可能である。但しコントローラへのクラッキングは対象プラントの制御監視系システムの構造を充分に知らないと不可能である。
第3 世代	1990 年代後半	● コンソールのOSはUNIX系およびWindows NT等の汎用OSを使用している。コントローラはベンダ独自のOSを使用している。
	（最近）	● 汎用OSのネットワーク技術を活用することにより、オ ープン化が進んでいる。 ● 汎用OSのネットワーク技術に精通した者であれば、コ ンソールまでは比較的容易に侵入でき、パソコンを含む 社内、社外のネットワーク接続の普及により、クラッキングの脅威が高まりつつある。

制御監視系システムの今後の傾向

全社レベルの情報系システムとの接続	ERP(Enterprise Resource Planning) パッケージの適用、情報系既存システムとの情報共有、等
プラントの情報系システムとの接続、高度化、分散化、統合化	PIMS (Plant Information Management System) の適用
オープン化	汎用技術の採用（フィールドバス、TCP/IP）
汎用化	専用OSから汎用OSへのシフト

現在はどうなっただろうか？

大規模プラント・ネットワーク・セキュリティ対策委員会最終報告書より

日本の状況

- 制御監視系システム領域のセキュリティ
  - 「大規模プラント・ネットワークセキュリティ対策委員会」（1997、通商産業省）最終報告書策定から7年が経過。
    - 当時予測されたオープン化が進みつつある
    - 制御監視系システムに対する、脅威シナリオ、攻撃者の想定はサイバーテロを主眼にしている
      - 参考：米国NISTのSP800-82の脅威分析レポートにおいて想定される攻撃者は、（フィッシングやスパム送信行為、ボット運用等をする者が主な想定）、犯罪組織、マルウェア作成者、テロリスト、外国諜報機関、産業スパイ、内部犯行者等。
  - 脆弱性関連情報の届出は年々増加傾向にあり、ユーザー、製品開発者ともに対応の重要性が増している
  - 「重要インフラの情報セキュリティ対策に係る行動計画」（平成17年12月13日情報セキュリティ政策会議決定）

日本においても、新たな脅威に対応するための取り組みを再開する時期に来ているのではないか？

制御監視系システムのセキュリティに関するJPCERT/CCの近年の取り組み（主なもの）

- 2005年度
  - 重要インフラセキュリティセミナー開催
    - 制御監視系システムを運用する事業者に対しての普及・啓発を目的としたセキュリティセミナー
- 2006年度
  - 制御監視系システムプロトコルにおける脆弱性の調整・情報公開
    - JVNにて7件公開
  - 重要インフラセキュリティセミナー開催
  - CPNI（旧NISCC,UK):「Policy and Best Practices」 の翻訳公開
    （http://www.jpcert.or.jp/research/）
    - SCADAおよびプロセス制御ネットワークにおけるファイアーウォールの利用についてのグッドプラクティスガイド
    - グッド・プラクティス・ガイド　プロセス・制御と SCADA システム
    - 他、9シリーズ
  - 制御監視系システムに関するヒアリング・意見交換会
    - 制御系システム開発者、国内研究機関等
- 2007年度
  - 重要インフラセキュリティセミナー開催
  - 制御監視系システムプロトコルにおける脆弱性の調整・情報公開
    - JVNにて10件公開
  - 制御監視系システムに関するヒアリング・意見交換会
    - 業界団体、国内研究機関、大学、学会
  - 制御監視系システムプロトコル調査

脆弱性情報ハンドリングワークショップ（製品開発者ミーティング）

JPCERT CC®

3月26日（水）に脆弱性情報ハンドリングワークショップの開催を予定しています。

目的：脆弱性情報ハンドリングに参加する製品開発者が集まり、共通の課題を話し合う

参加ご希望の方はお問い合わせください
（JPCERT/CC製品開発者リストへの登録が必要です）

お問い合わせ先：　情報流通対策グループ　poc-vh@jpcert.or.jp

お願い

- 製品開発者のみなさま
  - JPCERT/CCの脆弱性情報ハンドリングの枠組みへご参加ください。
  - お問い合わせ先：　情報流通対策グループ
    poc-vh@jpcert.or.jp
    http://www.jpcert.or.jp/vh/
- 重要インフラ事業者のみなさま
  - 「早期警戒情報」のご利用のお問い合わせは下記まで
  - お問い合わせ先：　ww-info@jpcert.or.jp

ご清聴ありがとうございました