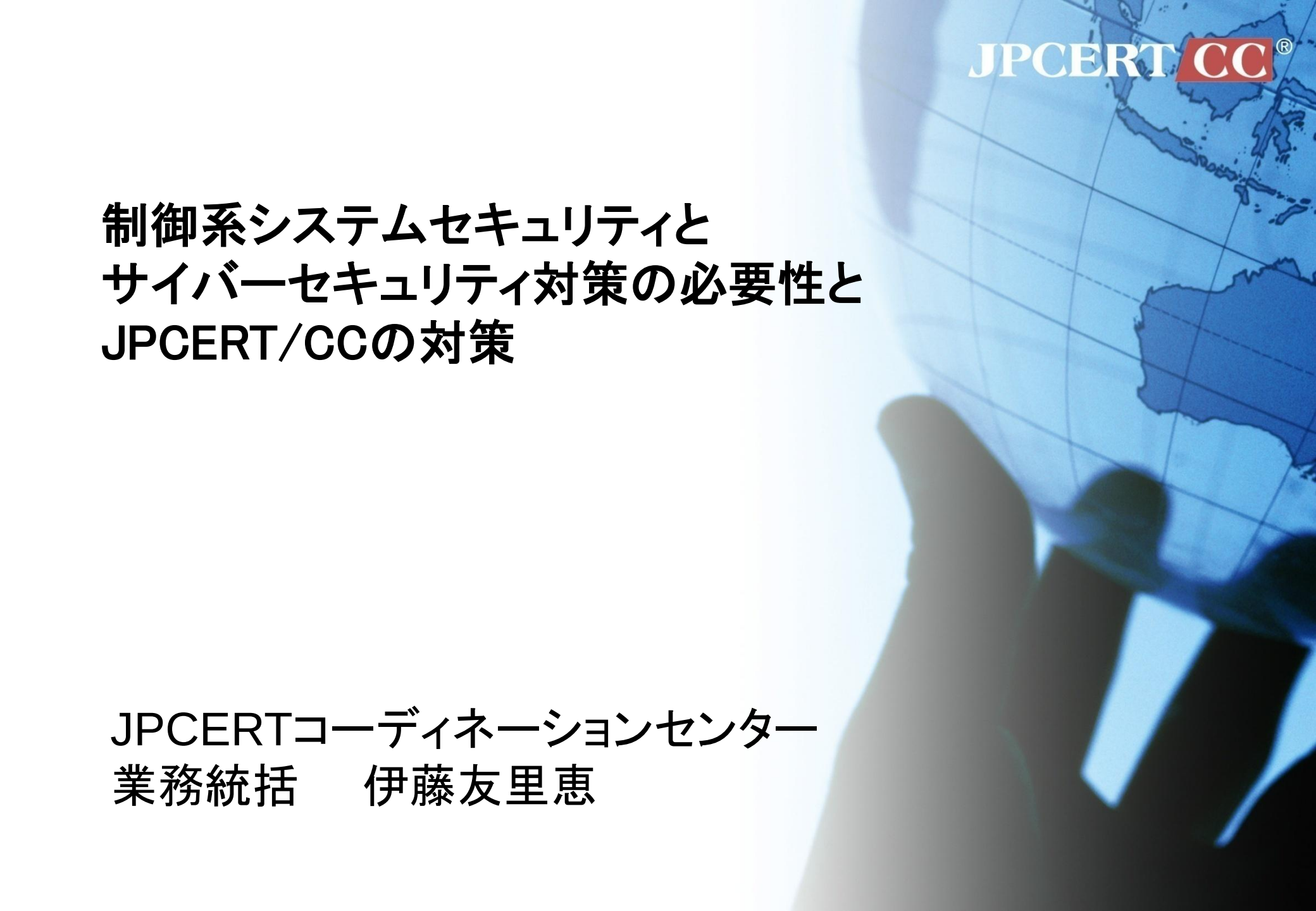


制御系システムセキュリティと サイバーセキュリティ対策の必要性と JPCERT/CCの対策

JPCERTコーディネーションセンター
業務統括　伊藤友里恵

制御系システムの脆弱性をつく侵入コードの一般公開まで

- **2008-01-30** : 発見者である研究者チーム(Core Technologies)が、ベンダーにコーディネーション開始
- **2008-06-11:** Security advisory CORE-2008-0125 published.
- **2008-06-12:** CERT、JPCERT/CC アドバイザリー公開
- **2008-09-05:** 当該脆弱性をつく、侵入コードがメタスプロイトで公開

キーポイント

- 制御系システムの脆弱性でも、情報は公開される
  - 検証コード
  - コーディネーション履歴

  ベンダーも、事業者も、脆弱性通知の連絡に対応できる体制の準備が必要

- メタスプロイトとは
  - フリーのオープンソース 侵入コード
  - 侵入テスト、ハッカーコミュニティに利用される

  ハッカーコミュニティが、制御系システムへの関心を高めている
  今後も、侵入コードは世の中に出回ることになる

制御系システムネットワークと、情報系ネットワーク

JPCERT CC®

- 制御系システムネットワークが、他のネットワークに接続する傾向が進んでいる
  - アプリケーション、PC、サーバーを汎用Unix、Windows OS上で稼動させる
  - データベース、ウェブアプリケーション、TCP/IP、Ethernet利用の増加
  - PLC、RTU、フィールドデバイスのほとんどの製品は、EtherNET、IEのインターフェースをオプションとして持つ
  - さらに多くの装置
  - 無線LAN、WANの増加

制御システムは、攻撃を受けやすくなり、脆弱なファクターも増加

情報系でオープン化と歩調を合わせてセキュリティが問題化したのと同様に、制御システムにおいても、オープン化の進行に伴って、セキュリティ問題が増大すると考えられる。

事業者における適切なセキュリティ対策が必要である

それでもまだ制御系システムがつながっていない!?
http://blog.wired.com/27bstroke6/2008/08/virus-infects-s.html

JPCERT CC®

Virus Infects Space Station Laptops (Again)

By Ryan Singel ✉ August 26, 2008 | 2:22:55 PM Categories: Hacks And Cracks

Viruses intended to steal passwords and send them to a remote server infected laptops in the International Space Station in July, NASA confirmed Tuesday.

And according to NASA, this wasn't the first infection.

"This is not the first time we have had a worm or a virus," NASA spokesman Kelly Humphries said. "It's not a frequent occurrence, but this isn't the first time."

That suggests that even in the future where space travel becomes an experience to complain about, rather than get dressed up for, computer viruses will still be tagging along uninvited.

NASA downplayed the news, calling the virus mainly a "nuisance" that was on non-critical space station laptops used for things like e-mail and nutritional experiments.

NASA and its par
now trying to figu
onboard and how
according to Hun

NASA declined to name the virus, but SpaceRef.com, which broke the story, reported

オープン化により制御系システムも、情報系と同じイーサネット上のIPで動作するものが増えており、たとえば、一時的に接続した保守用PCを介してマルウェアが侵入する可能性が現実のものになっている。

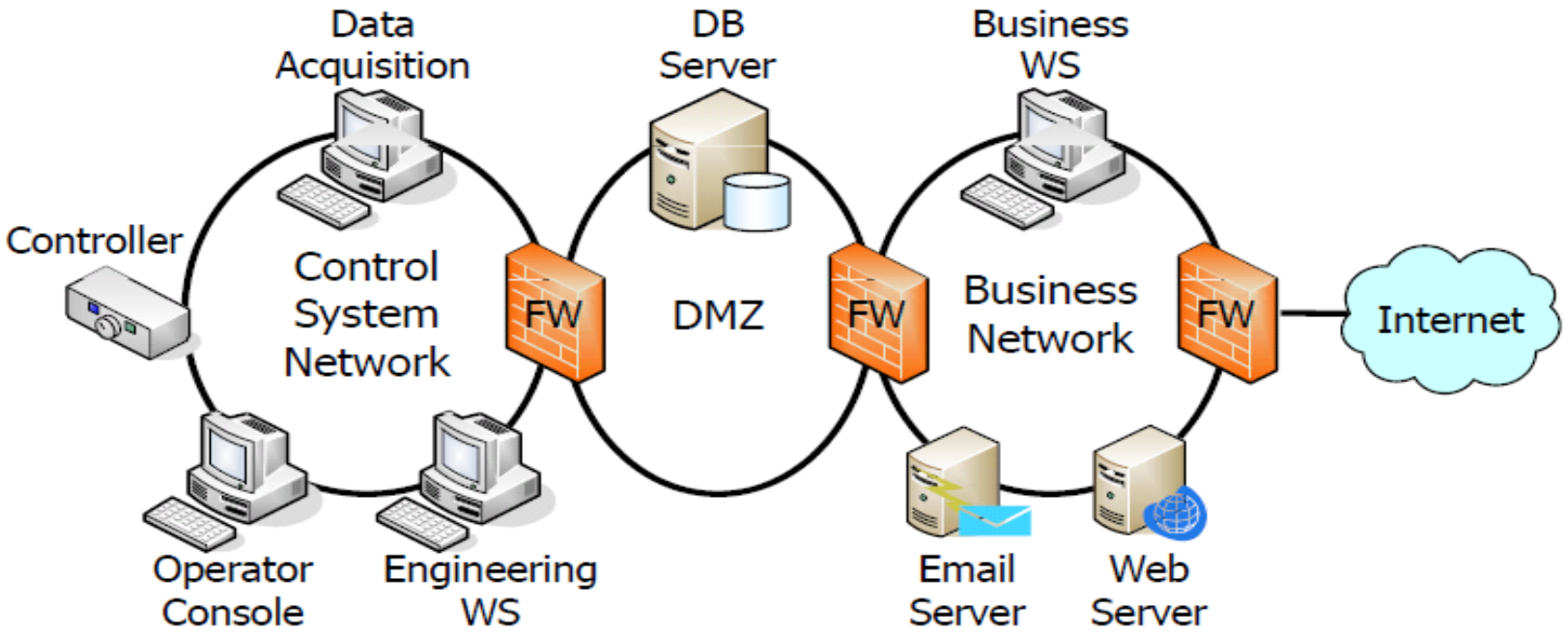
オープン化が進む理由

- システム的な要請：在庫の低減やエネルギー効率の向上のため、制御システムと情報システムを相互接続する要請が高まっている。

- 保守用などの一時的に接続される端末：ネットワーク基盤がイーサネット等の共通技術を利用したものになっていくため、通常のPCが保守用端末として制御システムに接続される機会が増える結果になっている。

ネットワーク境界セキュリティの穴

電中研の資料から：制御系システムの構築例の一つ



ファイヤーウォールによるネットワークセグメンテーション

JPCERT CC®

- **ベストプラクティス実装してますか?**
  - 3層ファイヤーウォールの実装
  - 最小特権の実装。全てを拒否するところから開始して、ファイヤーウォールの設定を行う。ファイヤーウォールに穴を開けるということは、その穴がセキュリティ上の攻撃ベクターになるということ。本当に必要なサービスかどうか確認。
  - 内側と、外側の直接のコネクションを絶対に許さないこと。全てのパスはDMZを介するように設定する
  - データはプッシュ型で
  - TCPはUDPよりベター
  - 最少数の穴をあけること、穴を空ける場合、それがまちがいなく必要な穴だということを評価すること。
  - ルールベースを定期的に見直す
  - システム構成上ひとつ以上のDMZを設置することを考慮し、その際はユーザーコミュニティの確認、承認レベル、許可する通信など、ポリシーをきちんと確認すること

- 旧来のシステムは「直接アクセスを制限されている」との前提から、ログイン認証や操作ログの機能を備えていないものが多いなど、オープン化に伴う脅威の増大に伴い、ほころびが露呈し始めている。

ネットワーク境界セキュリティの穴

- 完璧なファイヤーウォールを構築していても、全てのファイヤーウォールの穴は、攻撃ベクターである。
  - ファイヤーウォール越しに提供されるサービスに、侵入可能なバグがある場合、攻撃者はファイヤーウォールを通り抜けることができるから
- 多層防御は必要。ファイヤーウォールに全てを依存してはいけない。
  - AV、認証/承認、モニタリング、検知などを組み合わせる

- **JPCERT/CCからの脆弱性情報の通知を受け取れるようにすること。**

  JPCERTは、国際的なネットワークを通して、全世界から脆弱性情報の連絡、調整を行っています。ベンダのPOC、事業者のPOCを登録いただければ、情報展開することができます。

制御システムプロトコルスタックの脆弱性

制御システムプロトコルスタックの脆弱性

JPCERT CC®

- 多くの制御システムプロトコルスタックは脆弱
  - 意図されていないデータがデバイスやアプリケーションに送られてクラッシュ
  - 制御システムの一部か全体に影響を及ぼすことも
- 単純なポートスキャンが、制御システムをクラッシュさせるという事例は数多く見つかった。

ブラウンフェリー原子力発電所 の緊急停止

- 2006年8月16日、米国のブラウンフェリー原子力発電所のユニット3が緊急停止
- 冗長化してあるPLCの全てが同時に落ちたことによって緊急停止に至った。
- このPLCは、リアクターを冷やすための冷却水の循環を制御する装置として使われている
- ここでの問題でリアクターが冷却されなかったことによって緊急停止となった。
- 事故調査は、PLCのEthernetインターフェースに対して、想定以上のトラフィックが送られたことが原因だったと特定した。
- 直接的で意図的な攻撃のエビデンスは見られていない。
- ネットワーク上の他のデバイスがフェイルしてブロードキャストトラフィックを送信したことにより、PLCのプロトコルスタックが処理し切れなくなって、落ちたと検証された。

制御システムプロトコルスタックの脆弱性

- どんなトラフィックが制御ネットワークに流れるのか、制限、管理することが必須
- 攻撃トラフィックだけはなく、さらに第3者の開発したアプリケーションなども、きっちりとテストするまでネットワークにのせない
- セキュア制御システムプロトコル
  - 望ましくは、制御系システムの全てのリクエストと応答は、全てソースと、データの完全性を認証すべき。ただし、この機能は今日ないために、適切なクライアントソフトと、制御システムの知識があり、境界に侵入することができる能力の高い攻撃者は、送信中の全ての制御データを見て、プロセスを変更することができる。
  - 良いニュースは、セキュアDNP3、OPC UAとIEC62351-5 といった、プロトコルレベルでソースとデータの認証を行うものが出てきていること。
  - 製品として実装されるには、まだ時間がかかるものの、他のプロトコルにもこのような動きが始まることが期待される。

JPCERT・Digital Bond プロトコルセキュリティ調査

- 制御系プロトコル概要
  - プロトコルの典型的な利用シナリオ
  - 制御系プロトコルの典型的な使用シナリオについて、デバイスレベル、コントローラレベル、コントロールセンターレベルの制御系システムの階層別にまとめている。
  - 攻撃と脅威シナリオ

- 本調査で対象としているプロトコルは主として、Ethernet, IP, TCP/UDP ベースプロトコルを対象としているが、その理由をプロトコルへのアクセス、攻撃者のプロトコルに関する知識、攻撃用ツール、サードパーティ製品の脆弱性の影響それぞれのリスクといった側面からまとめている。

JPCERT・Digital Bond プロトコルセキュリティ調査

選定した10 の制御系プロトコルそれぞれについて、以下の項目について調査を実施。

* CC-Link IE
* DNP3
* EtherCAT
* EtherNet/IP
* FL-net
* Foundation Fieldbus HSE
* IEC 61850
* Modbus TCP
* OPC
* PROFINET

・歴史: 当該プロトコルの成り立ち、策定、標準化組織など
・用途: 当該プロトコルのシステム的な利用目的、利用されている分野、地理的な利用状況など
・機能: 当該プロトコルが持つ一般的な機能の特徴およびセキュリティ機能など
・プロトコル実装: 当該プロトコルの実装に関する情報
・他のプロトコルとの関連: 当該システムと他の制御系プロトコルとの関連性(同様なプロトコル、標準化との関連性などを含む)
・脆弱性: 当該プロトコルに関連して公開された脆弱性情報
・攻撃のシナリオと難易度: 当該プロトコルへの攻撃として考えられるリスク、攻撃者へのプロトコルの露出度および定性的な攻撃の難易度
・複雑さ: 当該プロトコルの仕様、実装に関する複雑さ

JPCERT/CCの取り組み： 脆弱性対応と、啓発活動

JPCERT CC®

JPCERT CC
有限責任中間法人 JPCERT コーディネーションセンター
一歩先の信頼と安全を提供するために

Japan Computer Emergency Response Team Coordination Center | English

Home > 公開情報 > 制御系システムセキュリティ > プロセス監視・制御系システム、SCADAセキュリティ

Contents

JPCERT/CCについて
- 代表理事あいさつ
- 組織概要
- JPCERT/CCに関するFAQ
- 活動概要
- 採用情報

インシデント対応
- フィッシング FAQ
- インシデント報告の届出
- PGP公開鍵 (http)
- PGP公開鍵 (https)

脆弱性情報ハンドリング
- 製品開発者リスト

プロセス監視・制御系システム、SCADAセキュリティ

最終更新: 2008-08-26

制御系システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学プラントの制御や、電力システムの監視制御、ダムや水供給システムの監視制御など国民生活の基盤サービスを提供する重要なシステムとして利用されています。その一方で、制御系システムに関連するソフトウエアに脆弱性が発見されるという事案も散見され始めています。

JPCERT/CC では、脆弱性関連情報調整機関として、プロセス監視・制御系システムにおける

開発者、研究者との情報共有タスクフォース (準備中)
脆弱性情報の通知、対策調整
脆弱性情報の情報公開
制御系プロトコルに関する脆弱性調査
プロセス監視・制御系システムセキュリティに関する各種情報収集
プロセス監視・制御系システム運用者への早期警戒情報発信 (準備中)

JPCERT/CCの取り組み： 脆弱性対応と、啓発活動

- 制御システムベンダーセキュリティ情報共有タスクフォースの発足、運営
  - 目的

    技術者間の、制御システムにおけるセキュリティ関連情報の対策の推進にご活用いただく情報の共有
  - 対象者

    制御システムおよび関連ソフトウェアの開発／構築に携わる技術者

    （制御システムベンダ、SI、研究者が対象）
  - 活動内容

    JPCERT/CCからのセキュリティ情報メールニュース、制御システムに関連するセキュリティ情報を配信

    関連テーマについて、イベント参加報告や、調査報告などの有益な情報共有を目的とした定期会合の開催

- セキュリティ啓発プログラムの実施
  - 制御システムセキュリティワークショップ・カンファレンスの継続的な開催

セキュリティ啓発を目的としたカンファレンスの開催

2009年2月18日（水）
「制御システムセキュリティワークショップ」開催
「制御システムベンダーセキュリティ情報共有タスクフォース」発足

2009年2月19日（木）
「制御システムセキュリティカンファレンス」開催

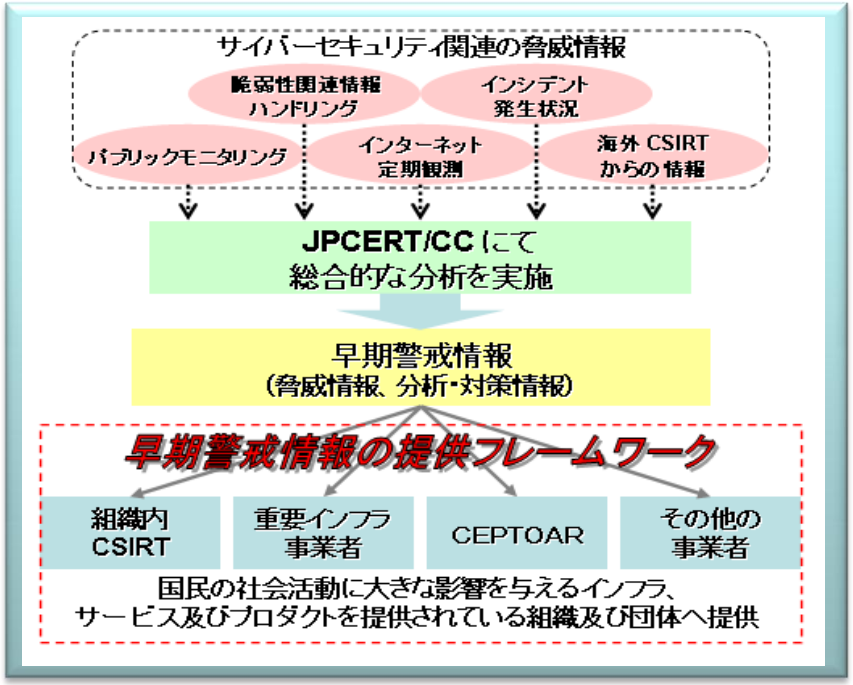
○ 主催
有限責任中間法人JPCERTコーディネーションセンター
（ソフトウエア等の脆弱性対策に関する経済産業省委託事業の一環として開催）

○ 協賛（申請中、順不同）
（社）計測自動制御学会（産業応用部門 計測・制御ネットワーク部会）
（社）日本電気計測器工業会（PA・FA計測制御委員会）
（社）電子情報技術産業協会（情報・産業システム部会 制御システム専門委員会）

JPCERT/CC が提供する早期警戒情報について

＜提供対象＞
国民の社会活動に大きな影響のある組織・団体等を対象に提供

＜提供タイミング＞
インシデントや脅威を極小化させるために、キャッチした情報を素早く提供



＜情報の信頼性＞
JPCERT/CC アナリストによる情報収集と各国CERTや、ベンダからの情報を収集して分析

＜安全な情報提供＞
各組織毎へ提供する専用ポータルサイト
クライアント証明書による安全な情報提供

＜提供情報の例＞
脅威度の高い未公開の脆弱性情報に関する回避策情報
大規模な範囲を対象とした攻撃予告に関する、注意喚起と対策情報
攻撃情報が一般に公開された脆弱性情報に関する、注意喚起と対策情報

＜お問い合わせ先＞
JPCERT/CC　早期警戒グループ　早期警戒情報登録受付窓　　Email：ww-info@jpcert.or.jp

お問い合わせ

- JPCERT コーディネーションセンター
  - Web. http://www.jpcert.or.jp/
  - Email. office@jpcert.or.jp
  - ML. http://www.jpcert.or.jp/announce.html
  - RSS. http://www.jpcert.or.jp/rss/jpcert.rdf
  - Tel. 03-3518-4600
  - Fax. 03-3518-4602

- インシデント報告の届出
  - Form. http://www.jpcert.or.jp/form/
  - Email. info@jpcert.or.jp

- 制御システムセキュリティに関するお問い合せ
  - Email. scada@jpcert.or.jp