JNSA 2014年度活動報告会
社会活動部会（BoF）

「IT環境の変化に対応していくインシデント対応の模索」パネリスト資料

一般社団法人 JPCERTコーディネーションセンター
常務理事
有村　浩一

2015年6月9日

自己紹介をかねつつ

一般財団法人　日本データ通信協会　テレコム・アイザック推進会議
- 国内主要通信事業者が主体会員となった連携活動
- 活動主体の特徴　　同業他社
- 2002年7月～【在籍期間：2002年～2011年】

活動の姿勢・意義
健全なセキュリティは高邁なコラボレーションから

一般社団法人 JPCERT コーディネーションセンター
- パートナー：企業【重要インフラ事業者、多数の会員を擁するサービスを行う事業者】
- パートナーの特徴：多種多様
- 1996年～【在籍2012年～】

活動の姿勢・意義
Our security depends on your security

設立の経緯：「JPCERT/CC 立ち上げのころの話」
https://www.jpcert.or.jp/magazine/10th/beginning.html

Telecom-ISAC Japanの概要

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

https://www.telecom-isac.jp/

- 2002年7月に日本で最初のISACとして発足
- 通信事業者の商用サービスの安全かつ安心な運用の確立を目的に、テレコム通信事業者を含む会員が関連情報を共有分析し、業界横断的な問題に対してタイムリーな対策をとる場を提供する活動を行う
- 世界に広がるサイバー空間の中で、「日本(jpドメイン)」が消失しないようサイバー脅威からネットワークを守る
- 単独では手に負えない大規模なサイバー脅威に共同で立ち向かう「互助会型」の通信事業者連携
- ビジネス競合関係にある国内大手ISPが会社の壁を越えて協力,連携するための会費会員制の民間組織

会員企業（平成27年4月現在）

赤文字はISP or 通信事業者を示す

会長：	飯塚　久夫
副会長：	NTT コミュニケーションズ株式会社、ニフティ株式会社、一般財団法人日本データ通信協会
会員企業：(19)	日本電気株式会社 、NTTコミュニケーションズ株式会社 、KDDI株式会社 、株式会社NTTドコモ、株式会社インターネットイニシアティブ 、ニフティ株式会社、株式会社日立製作所、沖電気工業株式会社 ソフトバンクモバイル株式会社、東日本電信電話株式会社、西日本電信電話株式会社、日本電信電話株式会社 株式会社KDDI研究所 、ビッグローブ株式会社 、富士通株式会社 、インターネットマルチフィード株式会社 NTTコムセキュリティ株式会社 、エヌ・ティ・ティ・データ先端技術株式会社 、ソネット株式会社
アライアンスメンバー：(11)	株式会社ラック 、日本アイ・ビー・エム株式会社、トレンドマイクロ株式会社 マイクロソフト株式会社 、株式会社サイバーディフェンス研究所 株式会社FFRI、株式会社情報通信総合研究所 一般社団法人日本ネットワークインフォメーションセンター 、BBIX株式会社 日本インターネットエクスチェンジ株式会社、NRIセキュアテクノロジーズ株式会社
オブザーバー：(5)	総務省、国立研究開発法人　情報通信研究機構(NICT)、 一般社団法人　日本インターネットプロバイダ協会（JAIPA） 一般社団法人　テレコムサービス協会、一般社団法人電気通信事業者協会（TCA）

Telecom-ISAC JapanのWG/SiGの設置状況

WG (11)

1-1) ACCESS-WG　2007年4月設置
インターネットアクセスNWサービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換

1-2) SoNAR-WG　2007年12月設置
ネットワークを利用した不正・不法行為対応(ABUSE対応)に関する情報の共有。インシデントの拡大を抑止するフレームワークの策定

1-3) DoS攻撃即応-WG　2011年10月設置
DoS攻撃への迅速な対応と複数事業者による協調対処の仕組みの検討。日本国内におけるDoS攻撃発生の、予測、早期検出、迅速かつ適切な対応の実現を目指す。

1-4) ルータ脆弱性問題-WG　2012年07月設置
危険な脆弱性を保有する特定ルータに対する具体的な対応の検討と調査を実施

1-5) 脆弱性保有ネットワークデバイス調査-WG　2013年05月設置
国内IPに接続されたネットワークデバイスの脆弱性保有状況の全容把握と調査を実施

1-6) サイバー攻撃等への適正な対策方法検討-WG（通秘-WG）　2013年12月設置
電気通信事業の業務を整理し通信の秘密に代表される法的な整理を行うことを目的とする

3-1) 経路情報共有-WG　2005年7月設置
ISP間の経路情報の共有、経路情報異常時の迅速な対応。および経路奉行システムの運用

4-1) サイバー攻撃即応スキーム検討WG（国際サイバーWG）　2011年12月設置
マルウェアやDDoSなどの様々なサイバー攻撃情報をISP間およびセキュリティ関連機関と共有し、予知・即応可能なサイバー攻撃対応スキームを検討

4-2) ACTIVE業務推進-WG　2013年07月設置
総務省ACTIVEプロジェクトの施策推進。マルウェアの感染防止、駆除を推進し、より安心・安全なインターネットの実現を目指す

4-3) WiFiリテラシー向上-WG　2013年09月設置
電波の有効利用（オフロード推進）を目的に、WiFiの利用および設置・運営において障壁となる情報セキュリティ課題の検討、対策の実施

6-1) サイバー攻撃対応演習-WG(CAE-WG)　2009年5月設置
電気通信事業者等の参加する、サイバー攻撃を想定した対応演習の企画、実施

SiG (1)

DNS運用者連絡会-SiG　2008年6月設置
DNSに関わる、脆弱性対応・情報の共有、DNSSEC化に備えた情報交換

※SiG：Special interest Group

JPCERT/CCとは

一般社団法人JPCERTコーディネーションセンター

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

- 1996年10月設立
- セキュリティインシデントに際し、その対応をはじめとする、国内外のCSIRTや関係団体、重要インフラ組織に対して技術的なサポートをするコーディネーションセンター
- ①コンピュータセキュリティインシデントへの対応、②国内外にセンサをおいたインターネット定点観測やインターネット上で発生する脅威・事故・問題点などに関する情報収集、③ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- 経済産業省からの委託事業として、業務を遂行

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

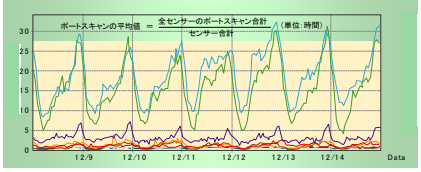
脆弱性情報ハンドリング

- 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
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

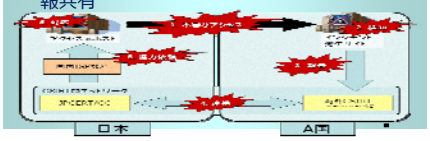
情報収集・分析・発信
定点観測（TSUBAME）

- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング（インシデント対応調整支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

JPCERT業務における現在の主要課題

① 高度標的型攻撃対応支援における課題
　関連技術の高度化
　長期戦化

② 「攻撃対象や問題の多様化」への対応における課題
　制御システム、IoT、組込ソフト、オリパラ・・・
　技術面、社会面、制度面