JPCERT CC®

コーディネーションセンターから見た

情報セキュリティの最新動向と対応体制のベストプラクティスについて

2007.1.31（水）
JPCERT コーディネーションセンター

早期警戒グループ リーダ
情報セキュリティアナリスト名和 利男

JPCERT CC®

アジェンダ

- JPCERT/CC とは
- 最近のセキュリティ動向
  - トピック1 - Botnet
  - トピック2 – Phishing
  - トピック3 – 用語から見るセキュリティ動向
  - 最近の事象を 5W1H で整理
  - とらなければならない対策
- 対応対策のベストプラクティス：CSIRT
  - CSIRT とは
  - CSIRT の活用
  - 万が一のインシデント発生時に必要なこと

JPCERT/CC とは

JPCERT/CC とは

JPCERT コーディネーションセンター (**JPCERT/CC**) は、世界規模に進化するセキュリティインシデントに対応するため、我が国を代表する CSIRT (**Computer Security Incident Response Team**) として、国際連携 (**FIRST、APCERT**)、予防・対策・対処、モニタリングを行い、我が国の **CSIRT** 活動の推進を支援しています。

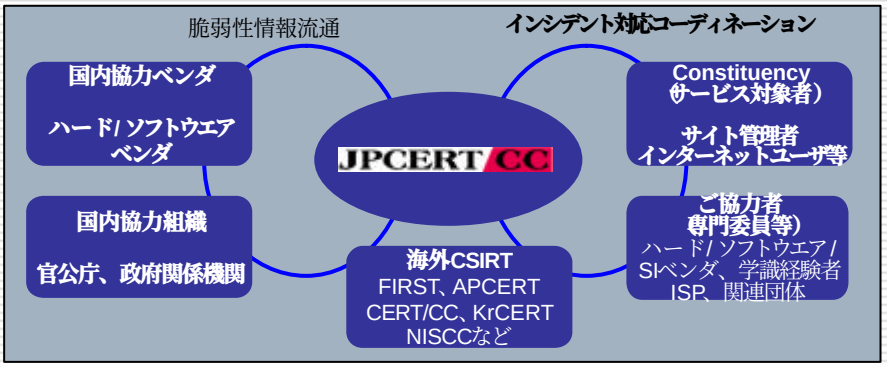
JPCERT/CC とは

- 沿革

1992年	ボランティアベースの活動開始 コンピュータセキュリティインシデント報告対応業務開始
1996年10月	任意団体として発足
1998年8月	CSIRTとして日本で最初にFIRSTに加盟 日本のPOC（窓口）CSIRTとして国際的に認知
2003年2月	APCERT（アジア太平洋コンピュータ緊急対応チーム）フォーラム発足
2003年3月	有限責任中間法人格取得
2003年12月	インターネット定点観測システム(ISDAS)公開
2004年7月	経済産業省告示にて「脆弱性情報流通調整機関」として指定
2005年8月	FIRST運営委員および理事就任
2005年10月	内閣官房情報セキュリティセンター重要インフラ専門委員有識者就任
2006年10月	JPCERT/CC 創立10周年

JPCERT/CC とは

- Japan Computer Emergency Response Team Coordination Center
  - コンピュータセキュリティインシデントの解決に向けた国内外の関係機関との調整ならびに連携などの活動を行っている
  - 緊急事態 (Emergency) への対応 (Response)

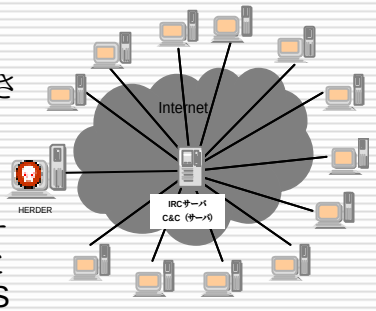


情報セキュリティの最新動向

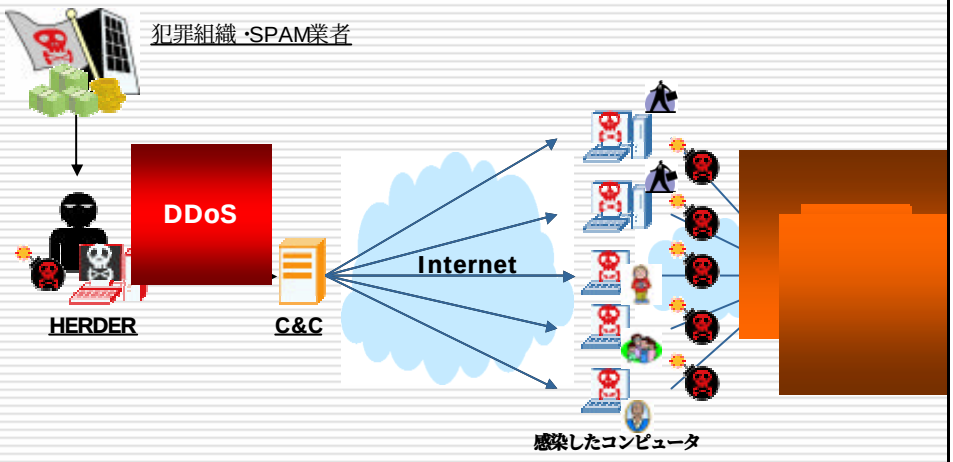
トピック１ Botnet

- Botnet とは
  Botnet とは、**Bot** と呼ばれるウイルスの一種に感染したコンピュータが構成するネットワークの総称であり、数百～数万台の規模で構成されている。 最近は、規模縮小化の傾向にある）

  Botnet は、通常のウイルスやワームとは異なり、**HERDER** (牧夫) と呼ばれる人間の指示により、DDoS 攻撃や SPAM メールの送信といった、さまざまな攻撃活動を行う。



トピック１ Botnet



トピック１ Botnet

- 攻撃者である Herder が出す命令の例
  - 脆弱性等を狙った感染活動
  - 機密情報（PC 内の価値ある情報）搾取
  - 指定サーバに対するパスワード総当り攻撃
  - 指定サーバに対するDDoS 攻撃
  - サーバソフト（HTTP や FTP 等）の起動
  - スニッフィング（盗聴行為）
  - （いわゆる）迷惑メールの送信や中継
  - スパイウェア等の不正なインストール

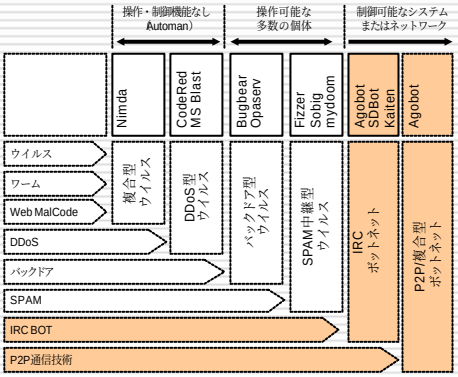
トピック１ Botnet

- ボット流行の背景
  - マルウェア作者の目的の変化
    - ウィルス、ワーム
      - 作者の売名、いたずら（愉快犯）と見られることが多かった
    - Botnet
      - ほとんどが金銭搾取の目的
      - 一部、恐喝や偏った思想も散見される

多くは金銭を得ることが目的のため、
必ずしも広く拡散する必要性はない。

トピック１ Botnet

- マルウェアの変化
  - DDoS機能
  - バックドア機能
  - SPAM メール中継機能



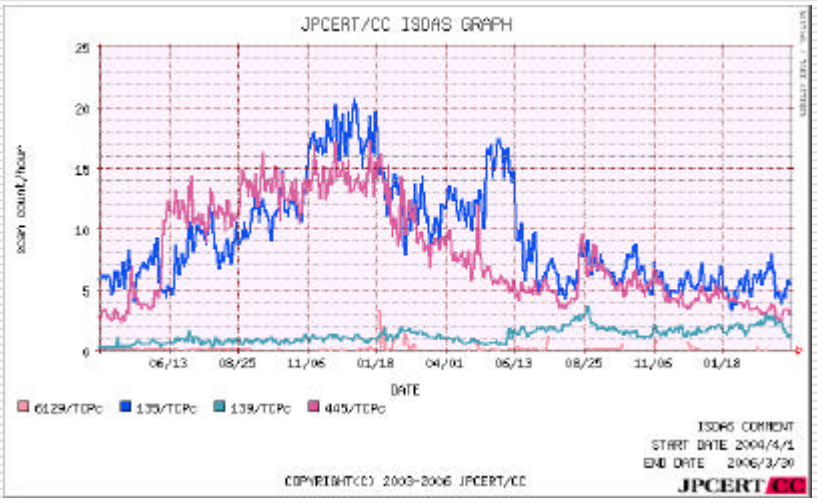
機能的には高度になったが、その制御に課題が出てきた。

行為者(HERDER)からの簡易な制御を可能とした。

トピック１ Botnet

- 脅威の変化
  - 攻撃者の目的の変化及び緻密な制御ができるようになった結果、マルウェアの活動が見えにくくなってきている。
  - 従来のウィルス、ワームの場合
    - 広域に拡散しようとした
    - 駆除されるまでに感染活動を継続していた。
      → 定点観測データに表れやすかった。
  - ボットの場合
    - 広域に拡散する必要がない。
    - HERDER からの指示で即起動、停止が可能。
      → 定点観測のデータに表れにくくなってきた。

トピック１ Botnet



トピック2 Phishing

- 2006年の世界的な Phishing 概要
  - 被害の拡大
    - オンライン犯罪グループの増加、100以上
    - 米国において、10月のある週だけで22,288 のユニークなフィッシングURL が発見された。
    - 米国でのフィッシングメールの2006年被害額が28億ドル
      - Gartner 調査 http://www.gartner.com/it/page.jsp?id=498245）
    - このような現状を受け、"phishing" はオックスフォード英語辞書に掲載されるほどにメジャーになった
  - 中国・ロシア・東欧からの攻撃が多い。
  - 送金などの手法が洗練されてきた

「2006 APWG General Meeting @ Orlando Florida（Nov 14-15 2006）」での報告より。

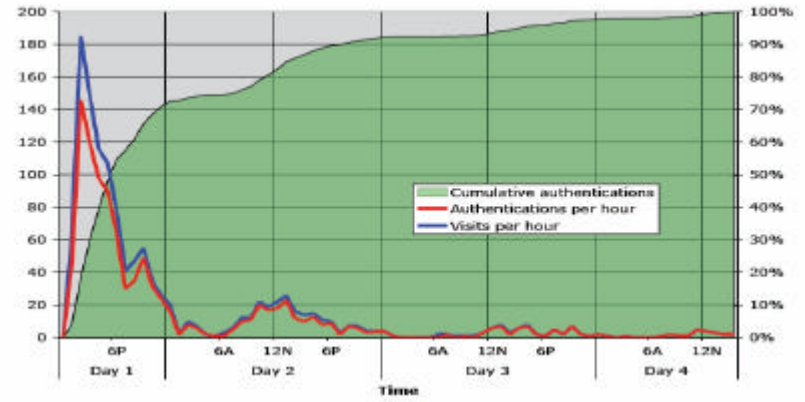
トピック2 Phishing

- オンライン詐欺の進歩
  - ワイルドカードDNS
    - http://<any junk you want here>.badguydomain.com
    - <>内がなんであろうと特定のIPを返す。DNSのログからどのドメインが「ヒット」したかを調査可能。
  - PHPを使ってIPを登録する
    - http://sample.xxxxx.xx.jp/login.php?id=238904389423423
    - URLに最初にアクセスしたリモートホストのIPを記録。URL中のIDとIPのテーブルを作成することで、以降別のIPからの接続を受け付けない。報告を受けた機関がサイトの生死を確認できない。
  - レジストラの営業時間を正確に把握する攻撃者

「2006 APWG General Meeting @ Orlando Florida（Nov 14-15 2006）」での報告より。

トピック２ Phishing

- サイト停止（TakeDown）だけでは難しい



出典元：Social Phising, Indiana University (Dec 12, 2005)
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

トピック２ Phishing

- 加害者は東欧やロシアの場合が多い。犯罪捜査に国際的な協力が必要になるが、国家間の関係からスムーズな捜査が行えないことが多い。
- 被害者がどこに通報するかが明確でない。
  - 消費者保護団体
  - シークレットサービス／FBI
  - 地方警察
  - CSIRT
- ISPや企業の担当者の連絡先の把握が困難。そのためサイト閉鎖などの対応の初動が遅れる

「2006 APWG General Meeting @ Orlando Florida（Nov 14-15 2006）」での報告より。

トピック２ Phishing

- レジストラ
  - 700語のキーワードリストを使って、ブランドネームが登録されないようにしている。（Godaddy.com ）
  - Phisher は同じユーザ名、同じクレジットカードで登録しているのではないか？それをレジストラ同士で共有できないか？
- Paypal,ebay

2006 APWG General Meeting @ Orlando Florida（Nov 14-15 2006）」での報告より。

トピック３ 用語から見るセキュリティ動向

- **Spear phishing**
- **ワンクリック詐欺とツークリック詐欺**
- **Vishing**
- **Piggy back**

トピック３用語から見るセキュリティ動向

- **Crimeware**
- **DUMP**
- **Carding**
- **Screen logger**
- **Money Mule**

最近の事象を 5W1H で整理

- **WHEN** – いつ発生？
  - 脆弱性が公表される前の攻撃が増加
    - ゼロディ攻撃
    - 対策方法が存在しない脆弱性への攻撃
- **HOW** – どんな手法？
  大規模に広がるワームはもう古い
  - ソーシャルエンジニアリング的な手法
    - 知人を騙ったメールや Phishing サイトへの誘導
  - 原始的なブルートフォース攻撃
    - SSHサーバへの攻撃
  - 高性能なアプリケーションの機能を利用した攻撃
    - 高性能ブラウザの便利な機能
    - オフィス系アプリケーションのマクロ機能

最近の事象を 5W1H で整理

- **WHAT** – どんな被害？
  - 金銭
  - 個人情報（IDやパスワード）
  - ビジネスの機密情報
  - 踏み台側は…
    - ネットワークリソースやコンピュータリソースの取得
  - オフィス系アプリケーションを対象としたものが目立つ
    - 高レイヤー化＝エンドユーザ化
    - アプリケーションレイヤを対象とした攻撃の増加
    - ネットワークレベルの攻撃はいまだに無くなってはいない
  - 日本語に特化したアプリケーションも対象になっている
  - 重要インフラのシステムも対象となる可能性がある
    - 世界中で重要インフラ保護の動きがある
    - インターネットのインフラであるDNSサーバへの攻撃

最近の事象を 5W1H で整理

- **WHERE** – どこが対象？
  - 攻撃対象の局所化（Targeted Attack）
    - 特定の組織を対象とした特定の攻撃
    - 一種類の攻撃手法を多くの組織に対して行ってしまうと検知・対策が容易にされてしまう
    - 検知しにくい、表面化しにくい、全体を把握しにくい
- **WHO** – いったい誰が？
  - 基本的には不明
    - 組織化されていることもある
    - 低年齢化の傾向も見られる
    - インターネットで調べると誰でもできるような環境

最近の事象を 5W1H で整理

- **WHY** – なぜ行う？
  - 以下のような情報や資産が取得できるから
    - 一般ホームユーザ
      - 個人情報（フィッシングなど）
      - 金銭取得（ワンクリック詐欺、フィッシングなど）
      - コンピュータ・ネットワークリソース
    - ビジネスユーザ
      - 機密情報
  - 最終的には、金銭の取得が目的の傾向が強い

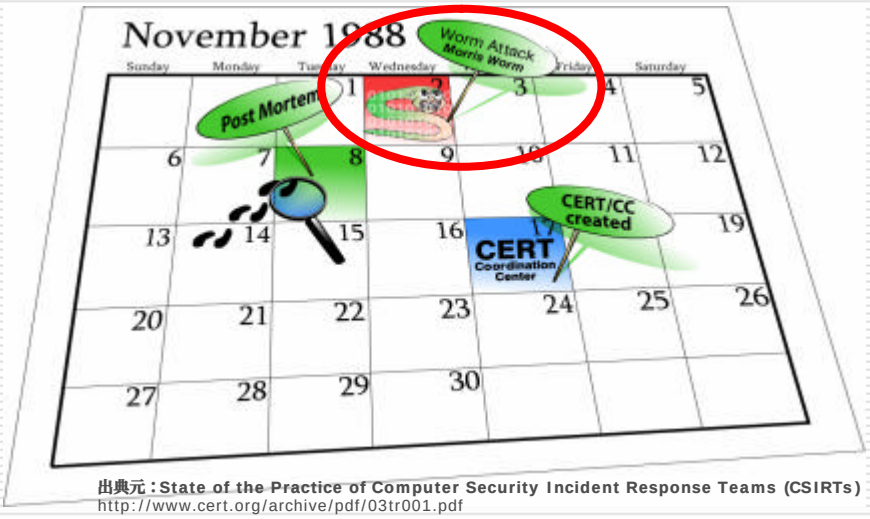
犯罪化

とらなければならない対策

- 犯罪者のリスクを底上げする
- 脆弱性の数を減らす
- 国境のないインターネットに必要な協調
  - 各レイヤーで国際的な協力関係が必要
    - 政府レイヤー
    - 法執行・法整備レイヤー
    - 技術レイヤー
      - インターネットは「技術」の集まり
  - すべてのレイヤーを繋ぐコーディネータとしてのCSIRTの活動を活発化させる必要がある。

対応体制のベストプラクティス :CSIRT

CSIRT とは

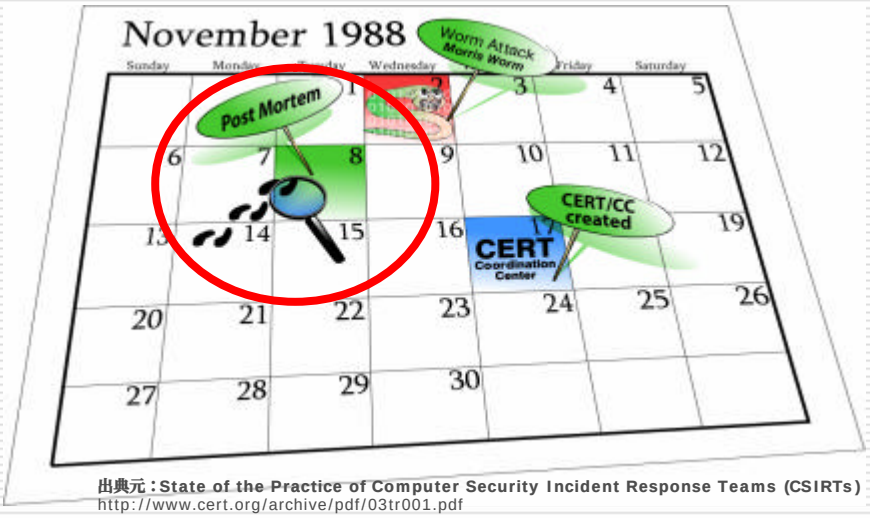


出典元：State of the Practice of Computer Security Incident Response Teams (CSIRTs)
http://www.cert.org/archive/pdf/03tr001.pdf

CSIRT とは

- モリスワーム発生！
  - 1988年11月2日発生
  - 米国の23歳の大学生が作成した不正プログラムで、さまざまな脆弱性を利用しながら、自発的に繁殖し、ARPANET の上の6,000～8,000のホスト（全体の約10%）に影響が出た
  - 対策として多くのホストが通信線を抜いたので、インターネットの通信リレーが機能しなくなった

CSIRT とは



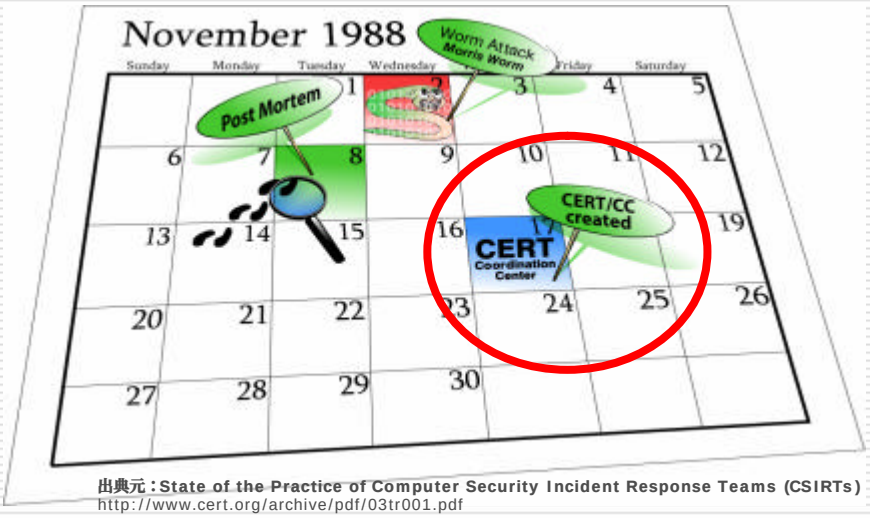
出典元：State of the Practice of Computer Security Incident Response Teams (CSIRTs)
http://www.cert.org/archive/pdf/03tr001.pdf

CSIRT とは

- モリスワーム対策会議にて
  - １９８８年１１月８日開催
    - Defense Advanced Research Projects Agency（DARPA）により構成
  - 不十分な協力体制
    - 研究機関やコンピューターセンターにおいて、それぞれ重複した分析作業をしていた
  - 連絡体制の未整備
    - 多くのサイトが最新の有効な対策情報をタイムリーに入手することができなかった

コンピュータインシデントの分析／対処をハンドリングする（取扱う）正式な手段がなかったという問題点が明確になる

CSIRT とは



出典元：State of the Practice of Computer Security Incident Response Teams (CSIRTs)
http://www.cert.org/archive/pdf/03tr001.pdf

CSIRT とは

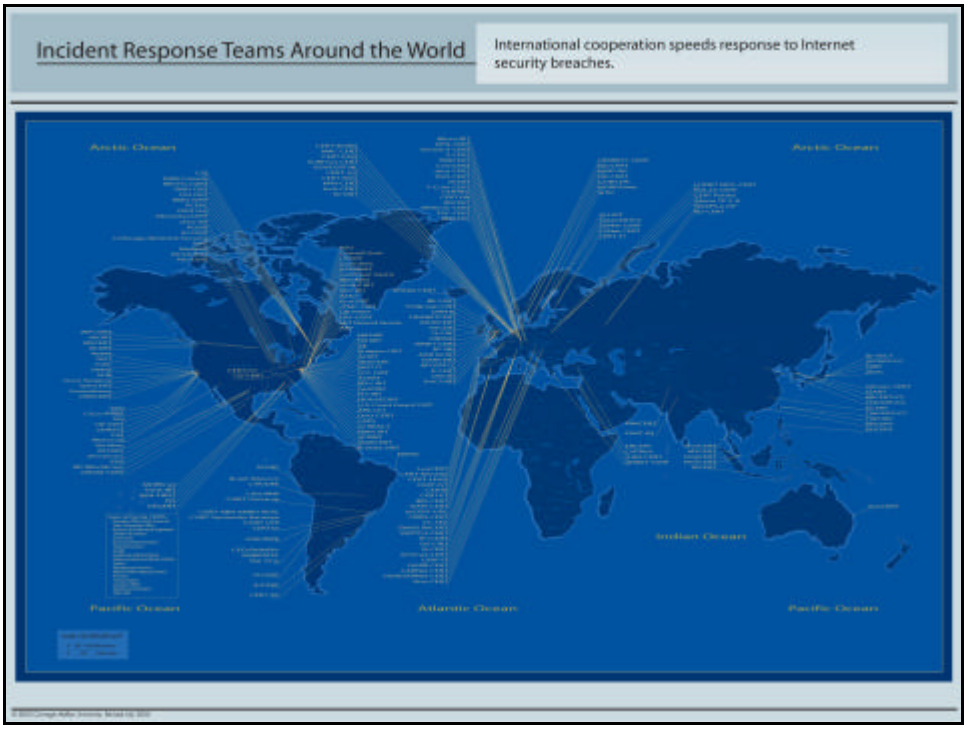
- 最初の CSIRT
  - 1988年11月17日、CERT/CC 発足
  - コンピュータ（Computer）の緊急事態に（Emergency）を対応（Response）する組織（Team）の構築へ
  - 単独の CSIRT のみで、すべての業種や組織体に対して対応をとることは大変難しいため、1989年以降、各政府機関においても同様な組織（チーム）が構築されていくことに

CSIRT とは

- CSIRT コミュニティ
  - 現在、JPCERT/CC のような、政府からも業界からも中立なインシデント対応調整組織は、世界中に存在
    - CERT/CC (米国)、KrCERT (韓国)、CNCERT(中国)、AusCERT (豪)など各国に存在
  - 政治的、市場からも独立した、テクニカルで、中立的な調整機関で、共通する方針を持って協力し、インシデント対応を行うコミュニティ
    - “My Security is Depending on your security”
    - “Web of Trust”
  - 実績と、信頼関係でつながるCSIRT
    - 繰り返し行うハンドリング手順によって、確実でスピードの速いインシデントを行う
    - 定期的な国際間インシデントハンドリングのドリル（訓練）の実施

CSIRT とは

- FIRST
  - http://www.first.org/
  - Forum of Incident Response and Security Teams
  - 1990年に CERT/CC などが中心となって設立
  - 世界中の CSIRT 同士の交流を目的にした組織
    - http://www.first.org/team-info/
    - 情報の共有
    - インシデント対応 (Incident Response) の国際協力
- APCERT
  - http://www.apcert.org/
  - Asia Pacific Computer Emergency Response Team
    - 2003年2月設立
    - アジア太平洋地域の CSIRT フォーラム、現13カ国20組織
    - 設立発起メンバ、現在はSecretariat & Steering Committee Member
    - 2006年3月北京で年次総会を開催



CSIRT とは

CSIRT のサービスの例

Reactive Service	Proactive Service	Security Quality Management Service
+アラート及び警告 +インシデントハンドリング - インシデント分析 - 現場でのｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ - ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽｻﾎﾟｰﾄ - インシデントレスポンス調整 +脆弱性ハンドリング - 脆弱性分析 - 脆弱性レスポンス - 脆弱性レスポンス調整 +アーティファクトハンドリング - アーティファクトレスポンス - ｱｰﾃｨﾌｧｸﾄﾚｽﾎﾟﾝｽ調整	○アナウンスメント ○技術動向監視 ○セキュリティ監査 或いはアセスメント ○調整、セキュリティツール／アプリケーションメンテナンス、インフラ整備 ○セキュリティツールの構築 ○不正検知サービス ○セキュリティ関連情報の提供	? リスク分析 ? 事業継続及び災害復旧計画 ? セキュリティコンサルタント ? セキュリティ意識啓発 ? 教育／トレーニング ? 製品の評価及び検証

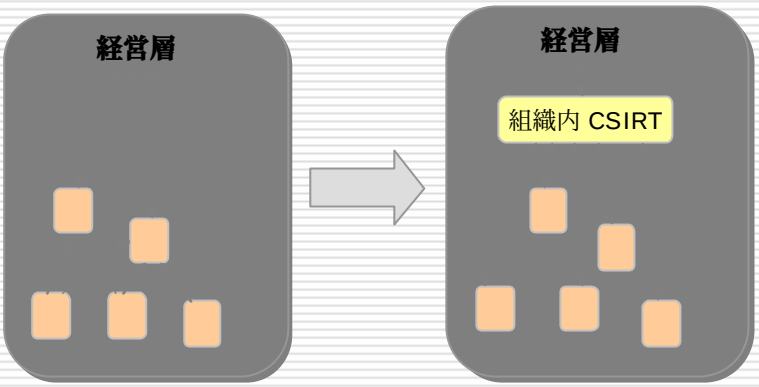
CSIRT とは

CSIRT の業務手順の例

1. 報告受け付けと評価（トリアージ）
2. 経過記録
3. 識別と分析
4. 告知 – 初度及び逐次
5. エスカレーション – インシデントタイプやレベルによる
6. 抑制措置
7. 証拠収集
8. 除去と復帰

CSIRT の活用

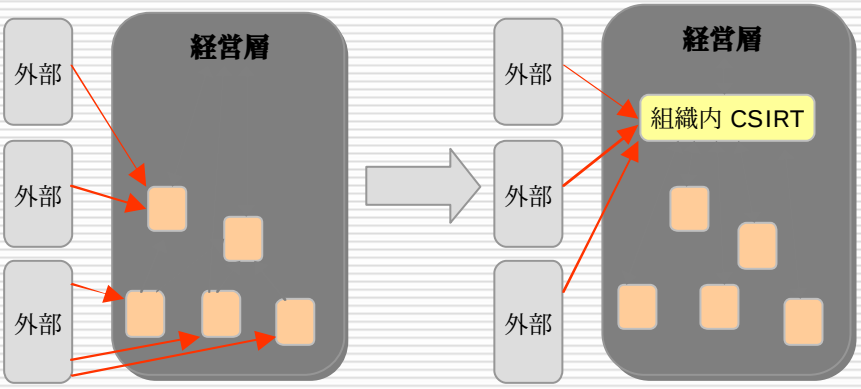
- 情報セキュリティのガバナンスとして



メリット：①社内セキュリティ情報の共有及び集中管理の実現
②セキュリティ対応にかかる指示系統の迅速化（ダイレクトリーチ）

CSIRT の活用

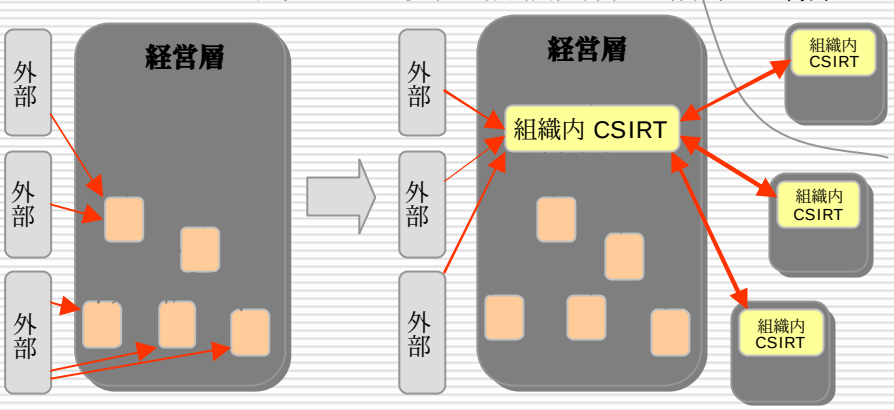
- 統一された窓口（POC）として



メリット：①外部に対する信頼性のある窓口先の提供
②外部からの情報の一元管理の実現

CSIRT の活用

- インシデント対応に必要な信頼関係の構築



メリット：①インシデントレスポンスに必要な情報量の向上
②想定外（予想外）のインシデントへの柔軟な対応

万が一のインシデント発生時に必要なこと

- 発生情報を ・・・・
  - 迅速かつ確実に！
  - 適切なところに！
- 現場は ・・・・
  - 「何を」しなければならないか！
  - 「誰が」意思決定するか！
  - 「どこまで」やるのか！
- 想定外（予想外）のインシデントには ・・・
  - 信頼でき、かつ、対応してくれる可能性のある組織に相談・依頼！
  - 日ごろからの情報蓄積と関係構築を！

万が一のインシデント発生時、みなさんは、どのくらいイメージできますか？

1988年からノウハウが蓄積された CSIRT の概念がベスト!

連絡先

- CSIRT構築のご相談
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp/

- インシデント報告
  - Email：info@jpcert.or.jp
    PGP Fingerprint：BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
  - インシデント報告様式
    http://www.jpcert.or.jp/form/

用語説明　(文責:SS研事務局)

【P.4】
FIRST : Forum of Incident Response and Security Teams
APCERT : Asia Paciffic Computer Emergency Response Team
　　アジア太平洋コンピュータ緊急対応チーム

【P.5】
POC : Point Of Contact 連絡窓口

【P.12】
DDos : Distributed Denial of Service
　DDos攻撃:攻撃の踏み台と呼ばれる複数のコンピュータが標的サーバ等に対して行う攻撃。

【P.16】
PHP : HTMLファイル内に記述するタイプのスクリプト言語のこと。
　「PHP:Hypertext Preprocessor」はオープンソースのソフトウエアの名称
レジストラ(registrar) : インターネット上の住所にあたるドメイン名の登録申請を受け付ける組織。

【P.18】
ISP : Internet Services Provider

【P.19】
Paypal : インターネットを利用した決済サービス
Ebay : アメリカに本部を置く世界最大規模のインターネットオークション会社

【P.20】
Spear phishing :
　特定の人物を狙い、偽のメールを送ったりウイルスを仕込んだりしてパスワードや個人情報などを搾取する詐欺
Vishing :
　VoIP Phishing IP電話経由で大量の電話番号へ録音されたメッセージを送り、偽造された発信者番号で安心させた上でクレジットカード番号を聞き出す詐欺
Piggy back : 正規のものの同伴者を装い侵入する行為

【P.21】
Crimeware :
　ユーザの個人情報を盗み、オンライン銀行から金銭を不正に引き出したりといった犯罪行為を行なう目的で作られた悪意のあるソフトウェア。
Dump : クレジット情報のこと。
Carding :
　カード不正利用ツールやクレジットカード情報(Dump)、さまざまな個人情報は、Cardingと呼ばれるsiteで売買されている。
Screen logger :
　ユーザ名やパスワードなど、画面に表示されていた個人情報や機密情報詐取プログラム
Money Mule :
　phisingや個人情報窃盗は世界中で盗まれたお金を洗浄するための悪意にうっかり荷担してしまった人(mule:麻薬の運び屋の意)。muleはメールで送られてくる求人募集に応募することで、不透明な商売や取引に巻き込まれるケースが多い。