情報セキュリティ対策の国際的動向

伊藤友里恵
業務統括
JPCERT/CC

1. セキュリティ動向

経営トップの関与
CSIRT機能構築の傾向

- 経営トップが関与しないとインシデント対応しきれない。
  - 現場レベルではなく組織レベルでの対応が必須

- 組織CSIRT機能を構築する傾向
  - サイバーインシデント対応にトップの関与は必須
  - インシデントに対応する際の、意思決定プロセスが事前に必要
    - インシデント対応には、様々な意思決定が、タイムリーに必要

2. CSIRTとは

(Computer Security Incident Response Team)

CSIRTの基本的な役割
レスポンス（例）

消防署と消火活動

火事発生

↓

消防署に火事情報を報告

↓

現場に到着後、被害状況把握と火事の種類の見極め

↓

消火行動の決心

↓

火事の抑制と消火

CSIRTとインシデント報告

コンピュータに関するインシデント発生

↓

CSIRTにインシデント情報を報告／連絡

↓

インシデントの把握と分析

↓

被害抑制のための方策の決定

↓

問題解決に向けた行動

CSIRTの基本的な役割
事前行動（例）

消防署の事前行動

- 防火訓練
- 避難訓練
- 火災検知器の設置
- 非難設備（はしご）の設置

CSIRTの事前行動

- セキュリティ教育
- セキュリティコンサルティング
- 運用の維持管理
- 技術文書やアドバイザリーの提供

ＣＳＩＲＴの一般的な目的と活動

目 的

- セキュリティインシデントなどによる被害を抑制し、損害を最小限にすること
- 適切なレスポンスと有効な対策を提供すること
- 将来発生するインシデントに対する予防をすること

活 動

- 担当する対象範囲内のインフラなどに関する以下の情報を収集する
  - インシデント情報
  - セキュリティーホール情報
  - ソフトウェア及びシステムの脆弱性情報
- 配下のセキュリティー対策組織間の情報共有と連絡調整
- 他のCSIRTとの連携による情報共有と連絡調整

CSIRTの組織モデル

- Security Team
  - **セキュリティーチーム**
- Internal Distributed CSIRT
  - **内部における分配型**CSIRT
- Internal Centralized CSIRT
  - **内部における集中型**CSIRT
- Internal Combined Distributed and Centralized CSIRT
  - **内部における統合（分配/集中）型**CSIRT
- Coordinating CSIRT
  - **連絡調整としての**CSIRT

CSIRT 例
(FIRST メンバーリストから抜粋)

- Above Security Computer Emergency Response Team
- Army Emergency Response Team
- Accenture CIRT
- Apple Computer
- The American Red Cross Computer Emergency Response Team
- AT&T
- Bank One Computer Security Incident Response
- University of Wisconsin-Madison
- Boeing CERT
- British Telecommunications CERT Co-ordination Centre
- Brazilian Academic and Research Network CSIRT
- Croatian Academic and Research Network CERT
- Cable & Wireless Cyber Attack Team
- CERT Italiano
- Computer Emergency Response Team Polska
- US Department of Energy's Computer Incident Advisory Capability
- Citigroup CIRT
- Google Information Security Team
- Goldman, Sachs and Company
- JPMorgan Chase Computer Incident Response Team
- JPCERT/CC
- Motorola Cyber Emergency Response Team
- Merrill Lynch Computer Security Incident Response Team
- Nokia Incident Response Team
- NTT Computer Security Incident Response and Readiness Coordination Team
- Royal Bank of Scotland, Investigation and Threat Management
- United States Postal Service Computer Incident Response Team
- VISA-CIRT
- Wells Fargo Computer Security Incident Response Team

CSIRTコミュニティ

- 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、中立な調整機関間で、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対応を行う

CSIRTコミュニティにおける動向

- ユーザー側へのセキュリティサポートを重点化
  - 早期警戒情報発信サービス
    - CSIRT間国際ネットワークを通して様々な情報が集約される：脆弱性情報、インシデント情報、トラフィックモニタリング情報
    - 集約される情報を分析して、早期警戒情報を発信
    - JPCERT/CCにおいても早期警戒情報発信サービスを開始
  - 経営トップへの働きかけ
    - 世界的なCIO、CEOフォーラムの傾向
    - FIRST：Corporate Executive Programme (CEP)
      http://www.first.org/conference/2005/cep/index.html

CSIRTコミュニティにおける動向

- ユーザー側へのセキュリティサポートを重点化　(続)
  - サイバーセキュリティ演習の実施
    - インシデント対応、情報ハンドリングの専門組織として、これまでの実績や経験を基に、シナリオを作成したり、演習実施の実働部隊として機能
    - JPCERT/CCにおいても、サービスを開始
  - 脆弱性プライオリティの仕様作成
    - 脆弱性のシステムに対する脅威度は、ユーザーによって違う
      - Know your system.
    - CSIRT間にて、メトリック作成進めている

CSIRTコミュニティにおける動向（2）

- インシデント対応の為の情報共有には、重層的な協力関係が必要
  - インシデント対応、脆弱性対応するには、様々なプレーヤーとの情報共有が必須
  - 特に機密性の高い情報共有の難しさ
    - 政府機関と、民間
    - 異なる機能層－CSIRT、政策決定者、法執行機関
    - 競争関係
    - 国際間
  - CSIRTは、コミュニケーションが難しい当事者同士、プレーヤー間の情報連携を橋渡しする役目を担ってきた。
- CSIRTコミュニティとして、通信事業者だけでなく、インフラ事業者、経営者層、ベンダ、政府、司法機関含めた、さまざまなプレーヤーとのネットワーキングをはじめている。

まとめ

- 攻撃側は組織化、巧妙化、複雑化。
- 防御側も組織化して対応する必要がある。

- インターネットの保全は、全てのユーザー、プレーヤーの責任、各プレーヤー間の協力、連携によって実現する。
  - CSIRT、製品開発者、ユーザー、システム管理者、政府、ISP、メディア

お問い合わせ

- **伊藤友里恵**
  - JPCERT/CC
    - 03-3518-4600
    - office@jpcert.or.jp