JPCERT/CCの新たな展開

JPCERT/CC 代表理事
山口英

JPCERT/CC概要、経緯

- これまでの経緯
  - 1992年：ボランティアベースの活動開始
  - 1996年8月：当時通産省から設立資金と当初2年間の運転資金を受け、正式にコンピュータ緊急対応センターとして発足。
  - 1996年10月：業務開始
- 現在は経済産業省、文部科学省から運転資金の支援
- 非営利の民間組織
- 日本におけるNational CSIRT(国際CSIRT間の連携業務におけるコンタクトポイント)
- 1998年から日本初のFIRST(Forum of Incident Response and Security Team)フルメンバ として活動
- 2002年からAPSIRC主催
- 2003年、APCERT(Asia Pacific Computer Emergency Response Team) 設立、SC メンバ、事務局運営

なぜ法人化か

National CSIRTに求められる要素を高める目的

- 機動性
  - 意思決定から実施までの迅速化
- 独立性
  - 集められた機密性を含む情報等の一元管理
- 中立性
  - 情報のコーディネーション、組織調整を中立な立場から行う

JPCERT/CC従来からの業務

JPCERT/CCの業務

- コンピュータセキュリティインシデント対応
  - 関連サイトへのコーディネーション
  - 国外サイトから、.jpサイトへの連絡仲介
  - 技術アドバイス
- セキュリティ認識啓発プログラム
  - JPCERT/CCメーリングリスト
    - 1996年からセキュリティ警告情報
    - 2001年からウィークリーメールマガジン
    - 技術メモ
  - セミナー、国際会議開催
- 国際地域活動（FIRST、APCERT、APECTEL）
  - 海外途上国CSIRT支援
- 日本のセキュリティ関係者のフォーラム
- JVN (JPCERT/CC Vendors States Notes)

法人化に伴う新たな事業展開

- 定点観測事業
  - Scan Probe自動ログデータ収集システムの開発
  - 協力組織との報告様式のデータフォーマットの標準化
  - 標準報告様式仕様に従った自動観測システムの開発
  - 協力組織との実施調整
  - 目標
    - 自動収集したログデータの分析をもとに、迅速な状況把握を行い、その関連情報は重要インフラを中心とする協力組織に発信、インシデント発生前に徹底したネットワーク防御策を呼びかける。
    - アジア太平洋地域で、既にスタートしている定点観測システム(オーストラリア、韓国)とのデータの統合、分析により、地域レベルのインシデント発生状況把握を実施。
- IODEF 実装運用事業
  - IODEF(インシデントオブジェクト記述交換フォーマット) を実装したツール、データベースの開発、運用
  - IETF INCH WGにて進行している、IODEF仕様標準化プロセスへの働きかけ
    - キャラクターセットの問題を解決し、アジア太平洋地域での普及目指す
  - 目標
    - インシデント情報の交換を、標準フォーマットで統一することで、国、産業ドメイン、組織をまたがっての情報交換を効率化させる。
    - セキュリティに関わる全ての現象を、標準化されたコモンランゲージ、フォーマットでやり取りすることで、常に共通の認識を確保する。
    - 開発したIODEFツール、データベースは、アジア太平洋地域のCSIRTを中心に、オープンソースで提供。特に途上国CSIRTのインシデント対応ツールの支援プログラムとして普及目指す。

新体制のJPCERT/CCは

- 日本におけるインシデント、脆弱性情報受信のコンタクトポイントとして、日本国内の、ドメイン、組織を越えた協力体制を強化する。
- セキュリティ関連情報を、効率化した方法により、迅速にコーディネーションする。
- そのために開発する、インシデント、また関連情報の交換、ハンドリング技術は、日本国内、国際地域枠に対して普及啓発する。
- インシデントを未然に防ぐ対策の徹底啓発。インシデント発生時の迅速な対応を目指す。
- 業務拡大に伴う、スタッフの増員、組織の拡張を行う。
- 24時間365日体制での情報収集業務を目指す。

なにとぞより一層のご支援
**　ご厚情をお願い申しあげます。**

山口　英　(suguru@jpcert.or.jp)
JPCERT**コーディネーションセンター**(JPCERT/CC)