Yahoo!BBにおけるインシデント対応フィルターについて

ソフトバンクBB株式会社
北谷忠士
tkitatan@softbank.co.jp

2003年インシデント対応フィルタ実施例

- CA-2003-04 :
  MS-SQL Server Worm
- CA-2003-15 :
  Cisco IOS Interface Blocked by IPv4 Packet
- CA-2003-17 :
  Exploit Available for the Cisco IOS Interface Blocked Vulnerabilities
- CA-2003-20 :
  W32/Blaster worm

フィルター適用時のユーザー対応内容

- **Web告知**
  ホームページへのインシデント情報の記載。
  フィルタ設定の告知。（特定通信の遮断）

- **メール通知**
  インシデント情報・対策方法などの配信。

- **サポート強化**
  コールセンターにて専用対策窓口の設置。

フィルター投入ポリシー

- インシデントによる「全サービス停止の可能性」と「特定サービスの遮断」をトレードオフした結果、フィルターを実施。

- フィルター実施の判断は、社内エンジニアやカスタマーサポートの意見を考慮して対策チームで対応。

SOFTBANK BB

ISPの足かせ

- **通信の内容把握**
  電気通信事業法 3条「検閲の禁止」
  電気通信事業法 4条「通信の秘密保護」
  憲法 21条2項「通信の秘密」により制限されている。

- **不正アクセス禁止法**
  ユーザ宅側機器の調査にはユーザの明示的な同意が必要。

- **コスト**
  対策には、どれも莫大なコストを要する。

積極的に行いたいアクション

- **ユーザ利用機器のPatch検査**
  Patchの適用が正しいか、対策済みのソフトウェアを利用しているかを検査。
  →未対策のユーザには個別対応。

- **インシデント発生元の特定**
  トラフィック監視の実施。(Honey Pot 等)
  →対象ユーザには個別対応。

- **ファイアウォール実装**
  モデムなどのユーザ宅機器への機能実装。

とどのつまり

- ISP単独での対応には限界がある。
- どこまでが法に触れるのかわからない。
- ユーザーの声はどこまで聞くべき？
- 総務省の見解はどうなの？