第43回電子化知的財産・社会基盤研究会（EIP）

「サイバー空間におけるリスクとは？」

～その脅威の最新動向～

2009年2月13日

（株）ラック
サイバーリスク総合研究所
村上　晃

ネットワークセキュリティ上の脅威（1）

脅威が様々な形で存在

- 不正アクセス（SQLインジェクション）
- 情報漏えい（Antinny）
- 踏み台
- 盗聴
- SPAM（迷惑メール）
- P2P（ファイル共有ソフトウェア）

1

Copyright ©2009 Akira Murakami

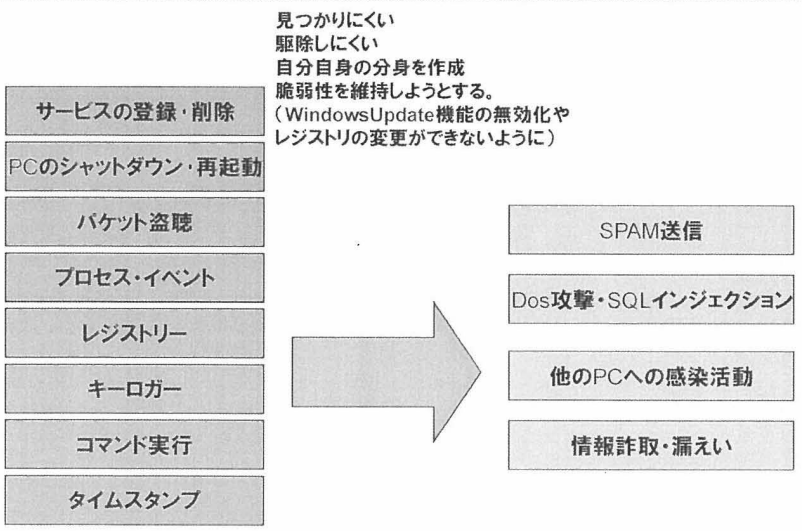
ネットワークセキュリティ上の脅威（2）

正常通信と不正通信が混在（見極めること）

過剰通信
ウイルス/ワーム
ボット
スパイウェア
Denial of Service（DoS）
詐欺・デマ
恐喝

Copyright © 2009 Akira Murakami

ボット・ボットネットの機能例と脅威



Copyright © 2009 Akira Murakami

共通・ 脆弱性

- **Webサイトに見かけられる脆弱性**
  - 推測されやすいセッションID
  - Cookieに重要情報を保存する
  - IIS標準エラーページの使用(エラー制御がされていない)
  - 入力チェック処理やエスケープ処理漏れ(テスト品質の問題)
- **緊急対応事例でよく見かける脆弱な部分**
  - 不適切なネットワーク設計
  - ファイアウォール運用が不適切
  - アクセス制御(ACL)などのポリシー設定が不適切。
  - 外部からの遮断だけで、内側から外への通信が無条件に許可
  - アプリケーションソースの構成管理、変更管理などの開発手法が未熟
  - セキュリティを考慮したプログラミングが行われていない

Copyright © 2009 Akira Murakami

セキュリティ対策としての取り組み

- **リスクを見える化する必要性**

① 経営者層の明確な姿勢
→従業員に対する意識付け

② リスクマネジメントに対する理解と実践

③ 情報の共有化(積極的な情報公開)

④ 失敗を隠さない企業風土つくり(ヒヤリハット)

⑤ 常にリスクを意識させる仕掛け作り

キーワード＝セキュリティ対策状況の把握・見える化

Copyright ©2009 Akira Murakami

・・・・・・対策計画業者・依頼・・・・・・・・

■ 正しい判断を養う目を持つことが重要

- 何でもできますセキュリティ対策を提案する営業には気をつけろ！
  何でもできるは、何にも出来ない。
- ・取り扱い製品の出来ないこと、出来ることを明確に提示できる。
  対策しなかったときのリスクや、懸念点も言える営業とは仲良くしましょう。
- 事業規模や、社風を考慮しないコンサルタント
  会社の事業規模や売り上げ高も知らずに、高額な提案をするコンサルタント(IT全般におけるセキュリティ対策への効果を提示できるか？)
- 基準や規格などを一般的なセキュリティ対策は運用が出来ないので破綻
  「今これが基準なので、これさえ満たせば、御社は基準を満たしていることになります。」(形式的セキュリティ対策でよければどうぞ)

運用が伴わないセキュリティ対策費用は無駄です。

Copyright ©2009 Akira Murakami

通信＆サーバー＆アプリで連携防御

■ 多層防御（Defense In Depth）・有効性

・・・・・暗号化・
・・・・・・・・F/W,IDS,IPS)
・・・・・・・・・・・・・・・・・・・・・・
・・・・・・・・・・WAF・・・・・・・・・・・・
物理・・・・・・・入退出管理・監視・・・・
人的・・・・・・・・・・・・・教育・研修・
■・・・・・・・防御・・・被害・最小限・・・・

Copyright ©2009 Akira Murakami

対策・・・・・・被害・最小限・・・・・・・

- ・クライアントPC、サーバの設定
  - アンチウイルスソフトの定義ファイルを最新に保つ
  - すべてのPC、およびサーバ上のアンチウイルスソフトの定義ファイルが最新に。
  - アカウント管理
- ・ネットワーク上の対策(多重防御で見える化を)
  - 組織内ネットワークやDMZ からの外向きの通信を監視
  - ネットワーク監視装置の導入
    - ファイアウォール、IDS/I PS 、他にアプリケーションファイアウォールの導入
- インシデント発生時の対応
  - インシデントの早期解決のために、異変に気付いた時点でのメモリダンプを取得
  - 異変(キータイプが遅い、Web カメラがよく点滅するなど)に気付いたら初動対応
  - 万一被害に遭った場合は感染PC のフォーマットおよび再インストール
- 組織内の連携と体制づくり
  - これらの脅威に対し、情報共有やインシデント早期発見のための組織内の連携が重要
    - その一例として、組織内CSIRT などを軸としたインシデント対応の準備

8

Copyright © 2009 Akira Murakami