



標的型攻撃対応とリスク・ マネージメント

市川昌
(江戸川大学)

2015/8/30



標的型サイバー攻撃とは？

- 不正アクセスによる標的型サーバー侵入
- 少数の対象または特定範囲の情報窃取のための無差別攻撃。
- 遠隔操作によるPC乗っ取りによるサーバー侵入による情報窃取、被害範囲予想。
- 偽名なりすまし送信元、不正添付ファイルを開示させてウイルス汚染。
- サイバー攻撃の防御策としての情報資産の分散ネット管理、アクセス権の制限。



標的型攻撃としてのメール対策

- 不審なメールを開かない。
- 不審な添付ファイルを開かない。
- 不審なURLリンクを開かない。
- 不審なアプリケーションをインストールしない
- ウイルス対策ソフトを確認、最新化する。
- 通信ログ、端末操作ログの不審なアクセスを監視。
- アイコン偽装、フリーメールに注意。



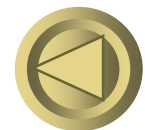
不正アクセス禁止法とは？

- 刑事法、平成11年8月公布、法律128号
 - インターネットなどネットワーク通信の不正アクセスの禁止と他人の識別番号の不正窃取、入力行為の刑事罰
 - アクセス制御機能をもつ他の電子計算機にアクセスして本来制限されている機能を利用可能行為の処罰。
 - アクセス管理者による防御処置義務の励行。
(識別番号の適切管理。アクセス制御機能の検証)
- フィッシングなど不正アクセス行為者の処罰
(違反者は1年以下の懲役または50万円以下の罰金)



特定電子メール送信適正化法 いわゆる迷惑メール禁止法

- 平成17年改正、偽装した広告、宣伝等スパムへの刑事罰。平成20年迷惑メールの罰則強化
- 送信者の表示義務の強化。送信者名の的確表示。
- 送信拒否者への再送信禁止。
- 多数架空メール送信の禁止。
- 行政処分と罰則：1年以下の懲役または100万円以下の罰金。法人は3000万円以下の罰金



情報犯罪の刑事罰の強化

- 情報価値は物品被害より大きい。
- 情報被害は事前防衛と事後調査の強化。
- 刑事罰は不正アクセス、サーバー侵入と共に個人情報保護法、著作権法、刑法、の民法などで複合適用で重罪とできる。

