攻めの
デジタル・フォレンジック
と法

石井　徹哉

tedie@faculty.chiba-u.jp

CHIBA UNIVERSITY

CHIBA UNIVERSITY

フォレンジックの変容

- フォレンジック：裁判等における証拠能力を想定
  - 法令等に従った証拠化
  - 法令遵守がデジタル・フォレンジックの基本
- サイバー攻撃への対応、攻撃者への積極的な対抗措置の必要性
  - 具体的な技術的手法の法令適合性の検討の必要性
    - 法制度に不案内なことによる萎縮効果

CHIBA UNIVERSITY

ボットのパケット解析

- 通信の秘密の侵害のおそれ？
  - ハニーポットによる分析
  - シンクホールによる調査
- 組織の内側から外へ流れるもの
  - 就業規則その他内部ルールの策定により実施可能
  - proxyによる遮断

CHIBA UNIVERSITY

通信の秘密侵害罪

- 通信の秘密の侵害⇒外形的アクセスのみで足りる
- 通信事業者による侵害
  - 業務上必要なものは、正当業務行為として違法性を阻却（刑法35条）
  - 何が正当業務行為となるかは不明確
    - ガイドラインによる不処罰の拡張

CHIBA UNIVERSITY

正当業務行為

- 行為の目的、手段の相当性、法益侵害の比較、あるいは政策的な配慮などを総合考慮し、社会通念上許容し得る場合、あるいは法秩序全体の見地から許容し得る場合に違法性を阻却
- ルーティング等
  - 自動的、機械的またはこれらに準じた態様において実施する措置は、自動的または機械的であるがゆえに通信の秘密を侵害する虞が少なく、かつ、電気通信役務の円滑、適切な実施、通信の公平な取扱という電気通信役務の公共性を促すものであって、そのため電気通信事業に対する信頼を害するものではない
- 輻輳等の回避
  - 輻輳の原因を探索し、これを突き止める行為は、現に通信の秘密が侵されてはいるが、輻輳の原因を追及しない限り、円滑かつ適正な通信状態の復旧が望めないのであって、通信当事者の私的領域に踏み込むことはあっても、通信の安定性の確保を図るという点で通信事業の公共性に適合するものであり、通信状態の復旧こそが通信事業に対する信頼を確保することにつながる

CHIBA UNIVERSITY

C&Cサーバ、ボットのテイクダウン

- たとえ攻撃者の管理するものであっても、テイクダウンすることは、器物損壊罪や電子計算機損壊等業務妨害罪になるのではないか
  - ましてや、一般の人の管理するものがマルウエアの感染によりボット化している場合、問題はより深刻になりうる

C&Cサーバへの通信の遮断

- 自組織の機器からの通信を遮断することは、組織内のシステムのセキュリティ確保の目的から許容される
  - ただし、法的な整理は、あいまいなまま
- 通信事業者の顧客からの通信の場合、直ちに遮断できるわけではない
  - 顧客の代行をしている場合は可能
  - 同意？

不正アクセス禁止法

- 対象となるアクセス行為は、識別符号によるアクセス制御がなされているものに対するものだけに限定される
- ネットワーク上の機器（テレビ会議システム、ビデオカメラ、複合機等）へのアクセス
  - 管理権限のID・パスワードが初期設定のまま
  - そもそも管理者権限についてアクセス制御がない

識別符号によるアクセス制御がない

- 悪意ある者が行っても、調査する側が行っても、不正アクセス行為となり得ないのではないか
- さらに攻撃活動を停止する措置を行ったり、通信を遮断、または感染したマルウエアの除去を行うことは可能か
  - ここでも、器物損壊罪や電子計算機損壊等業務妨害罪が成立する可能性が残るのではないか

ハックバック、ビーコンファイル

- ビーコンファイルによる相手方の通信の監視は、通信の秘密の侵害となるのではないか
  - そもそも、ビーコンファイルの作成、蔵置行為が、不正指令電磁的記録作成罪、保管罪等を構成するのではないか
- ハックバックは、不正アクセス行為等に該当するのではないか

問題は、どのような行為がどのような状況において必要となり、そのために抵触しうる法令等を精査することがまず出発点として必要ではないか