デジタル･フォレンジックの動向と今後の趨勢および人材育成

RITSUMEIKAN

立命館大学
情報理工学部
情報システム学科
サイバーセキュリティ研究室
上原哲太郎
http://www.cysec.cs.ritsumei.ac.jp/

海外のデジタル･フォレンジック研究の歴史

- 1995～7年あたりにかけて“Computer Forensics” “Network Forensics”という言葉が使われ始める
  - “Computer Forensics: An Approach to Evidence in Cyberspace,” Mark Pollitt, 1995
  - “Network forensics and traffic monitoring,” Ranum, M J, 1997
  - 今でもWikipediaはComputer Forensics
    - こちらはシステム屋に好まれる用語
- 2000年前後にはDigital Forensicsという概念が生まれる
  - Information Forensicsとも言う
  - メディア処理研究者が多く参入

研究コミュニティの形成

- 2001年 Digital Forensics Research Workshop (DFRWS)開始　http://www.dfrws.org/
  - おそらく最古で今も一番活発
  - 「実学的」 “Forensic Challenge”などのコンテストも主催
  - HDDイメージの規格CDESFの提案WGなども
  - 論文誌Digital Investigationとタイアップ
- 2004年 IFIP（情報処理連合）のTC11（技術委員会）にWG11.9としてDigital Forensicsが発足
  - 毎年1月頃学会を主催（次は香港）　60～100名規模
  - DFRWSに比べると学術的
  - SpringerからAdvances in Digital Forensicsを毎年発行

4年前のコミュニティ2009にて さまざまな海外のコミュニティを紹介

- Digital Forensics Research Workshop (DFRWS)
- IFIP WG 11.9 Annual Conference on Digital Forensics
- Association on Digital Forensics, Security and Law (ADFSL)
- e-Forensics
- ARES Workshop on Digital Forensics (WSDF)
- IEEE Workshop on Information Forensics and Security (WIFS)
- IEEE COMPSAC Workshop on Computer Forensics in Software Engineering (CFSE)
- Systematic Approaches to Digital Forensic Enginnering (SADFE/IEEE)
- Forensics for Future Generation Communication (F2GC)

4年間のコミュニティの広がり

- e-Forensics以外のワークショップは存続
- さらにいろいろなコミュニティが産まれる
  (前回見落としも多少あり)
  - http://www.wikicfp.com/cfp/servlet/tool.search?q=forensics
  - この分野で年10～15程度の国際学会が常に開かれる状態に
- 米国中心の3大学会 (DFRWS, ADSFL, IFIP)
  のうちDFRWSは欧州に進出、ADFSLはアジア進出を企画
- だが日本は…？

論文検索をしてみる

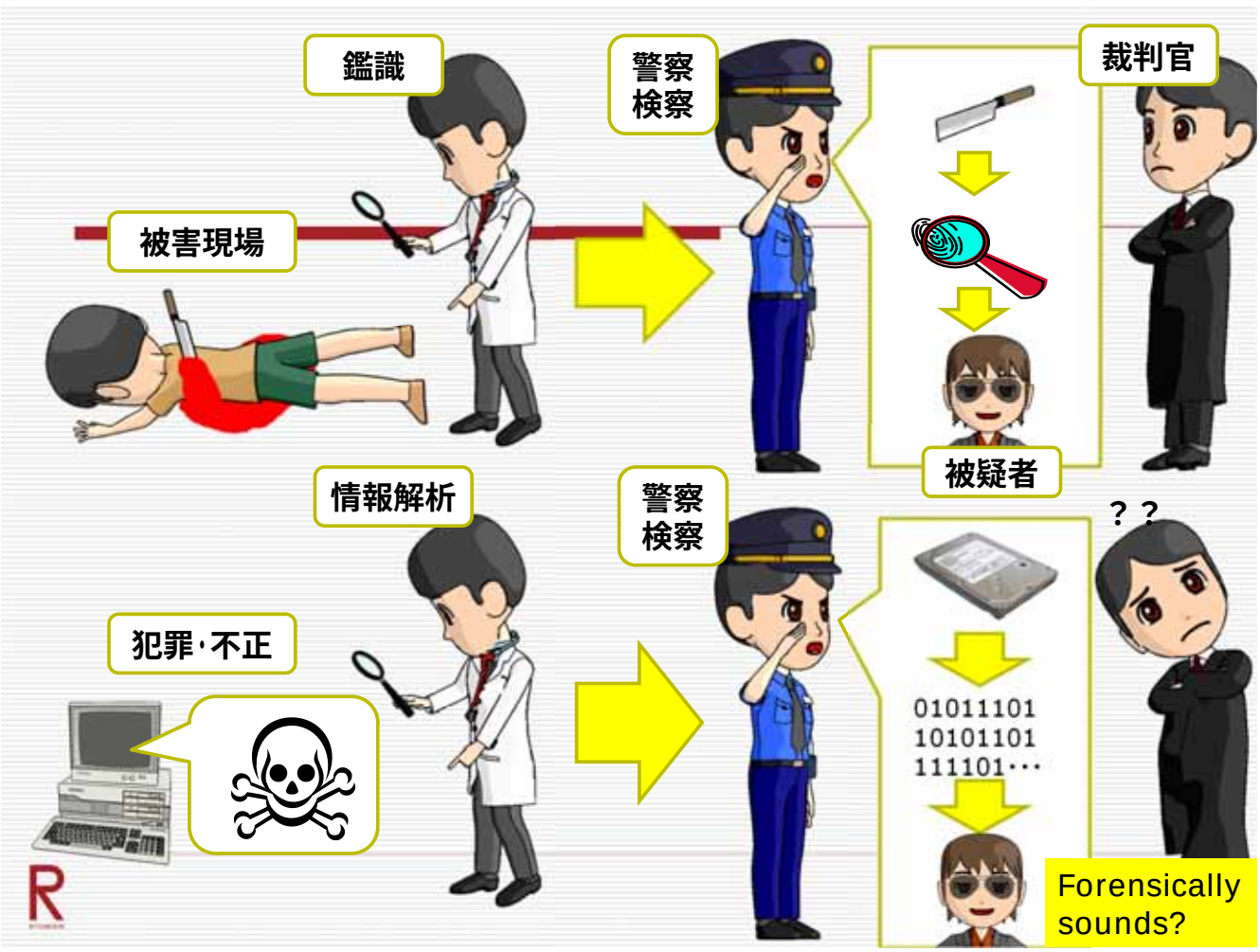
- Web of Scienceで
  “Digital forensics”
  or “Computer ～”
  を検索すると…
- 総数36.8万件
  2000年以降は
  毎年1.5～1.8万件

- CiNiiで
  “フォレンジック”を検索
- 文献は138件！

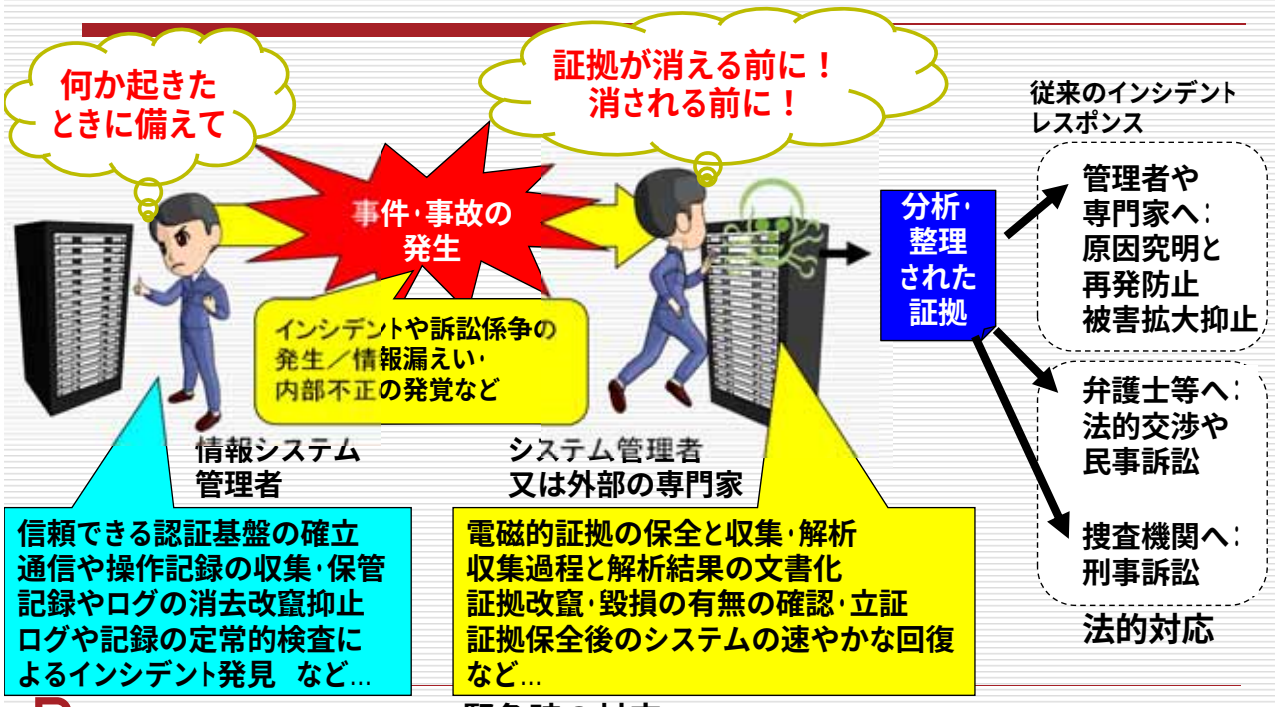
- J-Globalで
  “デジタル･フォレンジック”“コンピュータフォレンジック”および類語を全て検索
- 日本語の文献は7！

他のForensics的な分野は？

- CiNiiで検索
  - 「法医学」 6423
  - 「法科学」 2620
  - 「鑑識」 1077
  - 「科学捜査」 801
  - 「法化学」 299
  - 「インシデントレスポンス」 6
- J-Globalで検索
  - 「法医学」 20882
  - 「法科学」 5238
  - 「鑑識」 1426
  - 「科学捜査」 2940
  - 「法化学」 57
  - 「インシデントレスポンス」 3



警察だけのものではない：
インシデントレスポンスとして・・・



平時の対応　　緊急時の対応

情報科学の研究者にとっての
デジタル・フォレンジック

- 「犯罪や不正抑止のための
  電磁的記録の取り扱い」という視点で
  既存の技術を見直したもの
  - 要素技術の新規開発テーマは少ないが
    応用技術の方向性で勝負できる
- なので論文になりにくいというジレンマ
- しかし社会的要求は確実に上がった

研究分野を分類してみる

- 技術分野
  - 証拠保全技術
    - 事前処理（ログ記録・保管技術・・・）
    - 事後処理（正しい「証拠保全」のあり方）
  - 証拠収集技術
    - データ収集技術そのもの（含むファイル復活）
    - データ分析技術、検索技術
    - （場合によっては）暗号化解除技術
  - 証拠分析技術
    - 文書マイニング・画像映像解析・フォーマット解析
- 法曹分野
  - 技術の評価と法的位置づけの確立
  - 電子証拠収集プロセスの確立と評価

システム研究とメディア研究の2つの軸 今メディア優勢

システム寄りの主な研究（1）

- データ収集・保全技術関連
  - 伝統的外部記憶デバイスからのデータ取りだし
  - 主記憶からのデータ取り出し
  - 高度化・大容量化するRAIDへの対応
  - SSDなどフラッシュメモリへの対応
  - スマートフォン・タブレットのデータ取り出し
  - クラウドの取り扱い
- データ中の証跡の取り出し・検索関連
  - ファイルシステム・システムファイルの解析
  - 消去データ復元・破損データ修復・Carving
  - パスワード解析・暗号の解読・データハイディング対抗
  - 証跡の検索・マイニング関連（特に機械学習の応用）

システム寄りの主な研究(2)

- ネットワーク・フォレンジック関連
  - Web・メール・VoIP・P2Pの検出・監視・分析・・・
  - IDS／IPS関連技術
  - インターネットトレースバック
  - Botの検出・C&Cサーバ等の検出
  - 匿名性強化技術への対抗(P2P、Torなど)
  - SNS、クラウドストレージなど
    サービスに特化した分析
- マルウェアの解析関連技術
  - 解析の効率化

R

メディア処理関係技術

- 画像の分析、音声の分析
  - 大量データからの人の顔・音声の同定と抽出
    - さらに個人の同定
  - デジカメ画像からのカメラ機種推定・個体同定
    (Toolmarking)
  - 改竄の検知
- 電子メールや文書の分析
  - 筆者の推定(Authorship Attribution)
  - 文書作成に使ったソフトウェア・ツールの同定

R

画像の改ざんハードルが下がる

- Photoshopなどの
  「コンテンツに応じた塗り」により
  被写体の「自然な」改ざんが楽に
- どうやって見つけるか？
  - 周波数成分の解析で不連続性を検出など
- 音声に関しても同様

社会的ニーズは
インシデントレスポンス

- 2011年あたりが転機
  - ゲーム会社への侵入事件
  - 防衛産業へのサイバー攻撃
  - 衆参両院・各省庁…
- インシデントレスポンスのための人が
  足りない！

「遠隔操作事件」が明らかにした問題

- 捜査側のフォレンジック能力の限界
- トレーサビリティの問題
  - 敵失に頼るしかない
- 今後はさらにIPアドレスの追跡性が下がる
  - Large Scale NAT問題
  - IPv6問題
- これらに対応する「研究」が出来るか？

人材育成の動向

- 大学院の特別プログラム
  - 先導的ITスペシャリスト育成プログラム
    - IISEC「ISSスクエア」　奈良先端大「IT-Keys」
  - 分野・地域を越えた実践的情報教育協働
    - IISECなど「enPIT Security ： SECCAP」
- CTFなどコンテスト形式の人材育成
  - SECCON-CTF
  - Hardning
  - 白浜危機管理コンテスト

SECCAPの構造

- 情報セキュリティ大学院大学（IISEC）、東北大、北陸先端大、奈良先端大、慶応大の協働
- 内容を「参加大学」に広げていく仕組み

SECCAPでの提供科目

基礎知識学習	情報セキュリティ運用リテラシーⅠ・Ⅱ（共通科目） 所属大学指定科目（基礎科目）	所属大学指定科目（先進科目）	
実践セキュリティ演習 （演習）	理論系 情報セキュリティ演習	技術系 セキュリティ技術基礎演習 / ネットワークセキュリティ検査演習 Web アプリケーションセキュリティ検査演習 / デジタルフォレンジック演習 CTF 演習 / システム攻撃、防御演習 / 無線LAN セキュリティ演習 リスクマネジメント演習 / インシデント体験演習 / IT 危機管理演習 ネットワークセキュリティ実践 / ハードウェアセキュリティ演習	
	社会科学系 セキュリティマネジメント演習 インシデント対応マネジメント演習 事業継続マネジメント演習		
統合CBL （先進科目）	理論系 最新情報セキュリティ理論と応用	社会科学系 セキュア社会基盤論 情報セキュリティ法務経営論	技術系 情報セキュリティ技術特論 先進ネットワークセキュリティ技術
その他	セキュリティ分野シンポジウム	企業インターンシップ	交流ワークショップ

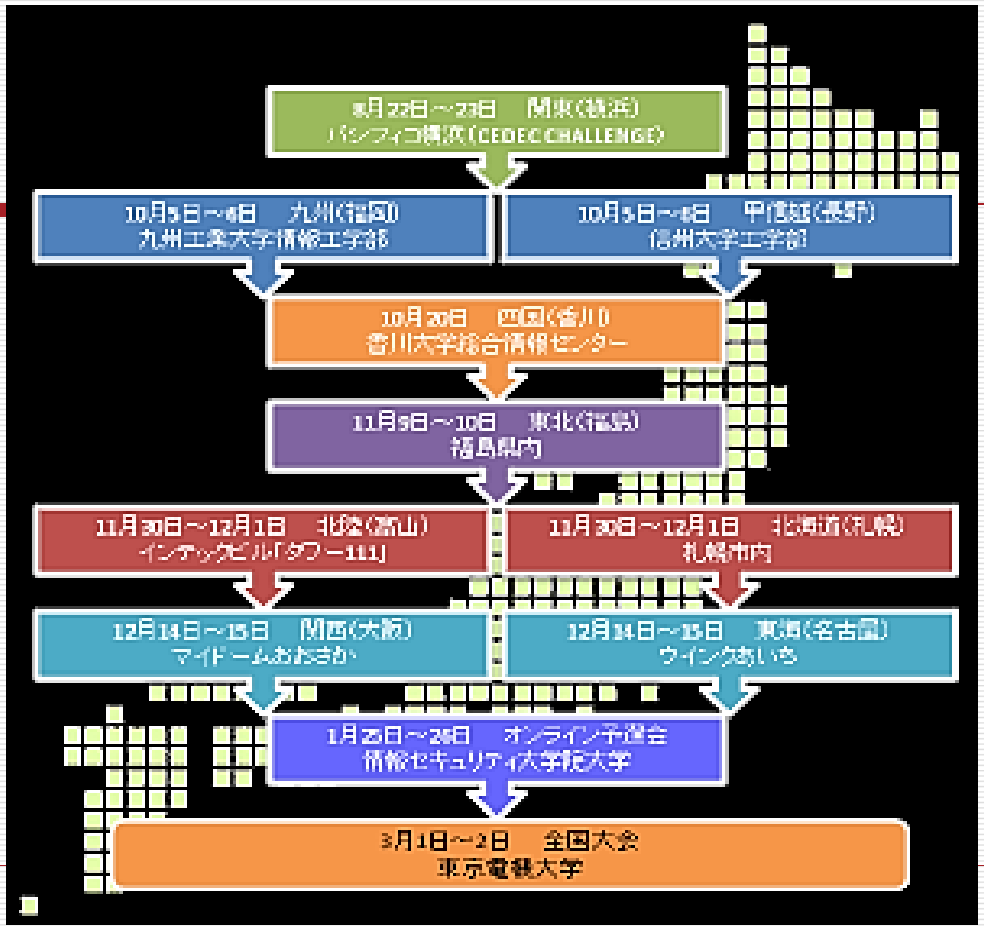
大学での人材育成の課題

- 大学側のリソース不足
  - システムセキュリティ研究者の不足
- 現場との乖離
  - 大学教員の限界
- 人材の「出口問題」
  - どのような場所でどのように働く人を？
    - インシデントレスポンスを「外部に」頼る需要は？
    - マネジメントとの関係

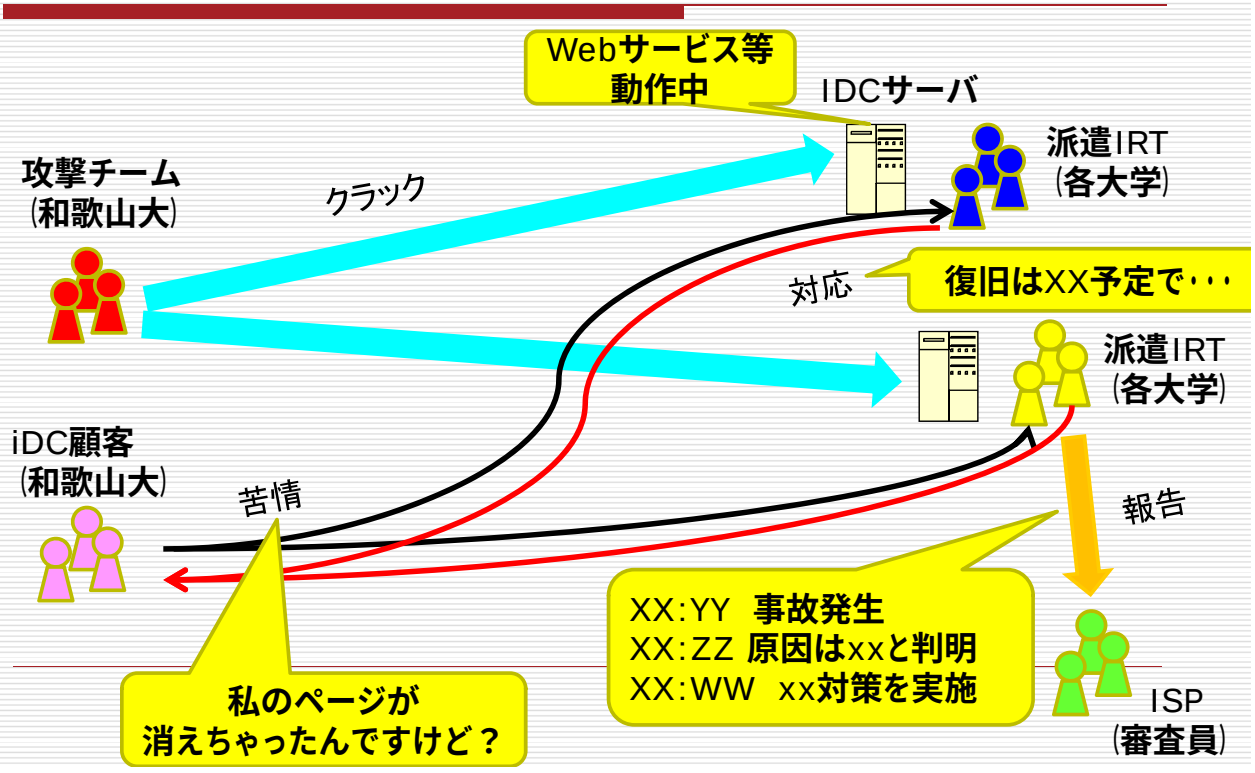
SECCON CTF

- JNSA主催　産官協働方式
  経産省「CTFチャレンジジャパン」と融合
- 地方大会→全国大会の形式
- 基本はクイズ形式（作業を含む）
  一部は攻防形式

- 技術者としての基礎体力を見る問題が多い



IT危機管理コンテスト



コンテスト方式の課題

- ミスマッチにならないか？
  - クイズはトリビアになりがち
    求める人材像にマッチしたクイズにする困難
  - ロールプレイはどれだけ実践的であるべきか
- 間接的影響であることの難しさ

終わりに

- デジタル・フォレンジック研究のありかた
  - なぜか情報科学の研究者は実学が苦手
    この壁をいかに乗り越えるか
  - 学際的研究に対する障壁
- フォレンジック人材育成のありかた
  - インシデントレスポンス人材だけでよいのか？
  - システム管理やマネジメント人材の育成