第14回
デジタル･フォレンジック･
コミュニティ2017 in TOKYO
資料

研究会2 「攻めのデジタル･フォレンジックを阻む法制度」
現実のサイバーセキュリティの現場から

佐藤 元彦

Who am I ?

- **佐藤 元彦**
- **伊藤忠商事株式会社**
  IT企画部 ITCCERT 上級サイバーセキュリティ分析官
- **(兼) 国立大学法人 千葉大学**
  准教授

- JPCERT/CC**専門委員**
- JASA**特任研究員**

My experience?

- **それなりに長い間、この業界で働かせていただいています**
  - **脆弱性検査**（NW・Web**アプリ**）
  - **情報セキュリティ監査・システム監査**
  - **政府の基準作り**（**情報セキュリティ管理基準等**）
  - ISO SC27**委員**
  - **セキュリティコンサルティング**（**方針策定・規程作り・体制整備・リスク分析**）
  - **インシデントレスポンス**（**複数の政府機関・民間事案をクローズ**）
  - **その他、情報セキュリティに関わる仕事**（**もちろん営業活動も**）

- **現在は伊藤忠商事に所属して、社内の**CSIRT**のチーム内で、インシデントを発生させないプロアクティブな防御活動や、日々のセキュリティイベントのトリアージや、必要に応じてインシデントレスポンス、さらには、全社・グループ会社のサイバーセキュリティ施策の企画・推進も行っています。**

Agenda

- **簡単に仕事内容の紹介**
- **現場がほしいものと専門家が売れるものとのギャップ**

- **リサーチャとしてのアクティビティ**
- **海外リサーチャの「情報」**
- **直面する問題**

- **日本は永遠のサイバーセキュリティ輸入国？**

簡単に仕事内容の紹介

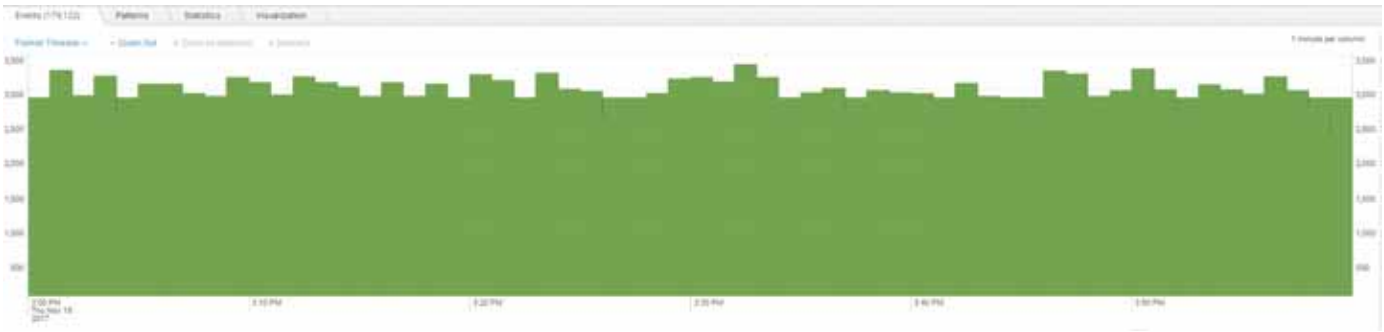
・<投影のみ>

現場がほしいものと専門家が売れるものとのギャップ

・<投影のみ>

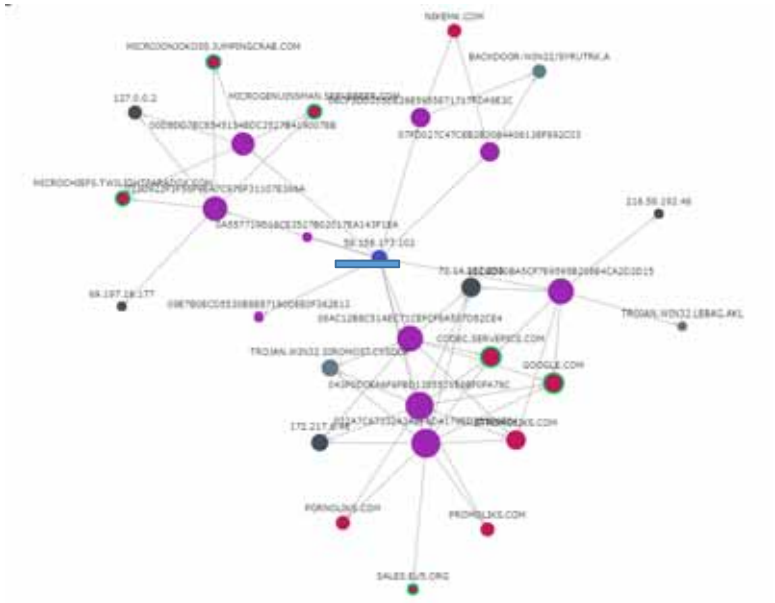
リサーチャとしてのアクティビティ（シンクホール）

・個人的にシンクホールを運用しています。
・ドメインは3年に渡って収集した2,000超のドメインを運用。
・標的型攻撃のドメインの保持数に限っては、世界で一、二を争う規模（と別のリサーチャ仲間に聞いています）



リサーチャとしてのアクティビティ（シンクホール）

・一日に100か国から430万の感染通信を捉えています。このデータからマルウェア通信の特徴を掴み、ログ分析のアラート作成をすると共に、感染組織が特定できた場合は、国内外の感染組織やNational CERTにIR対応依頼をコーディネーションしています。



リサーチャとしてのアクティビティ（犯人特定）

・<投影のみ>

海外リサーチャの「情報」

・<投影のみ>

直面する問題（シンクホール）

・<投影のみ>

直面する問題（犯人特定）

・<投影のみ>

日本は永遠のサイバーセキュリティ輸入国？

・日本が攻撃される（場合によっては被害を受ける）
・日本から攻撃情報がセキュリティ製品を経由して他国に渡る
・他国で攻撃情報が分析される
・日本に分析情報が高額で売られる

・これでよいのでしょうか？

・必要なのは「情報共有」？　でもないような。。。
・「国産製品」？　でもないような。。。

提起した問題（おさらい）

ありがとうございました