THE POSSIBILITIES ARE INFINITE FUJITSU

セマンティックWebコンファレンス2010

オントロジを活用したマルウエア攻撃の見える化について

2010/3/5

株式会社富士通研究所
津田　宏, 小櫻　文彦, 鳥居　悟

ビジネス情報ナビゲーター

FUJITSU

I. 富士通研究所の開発したナレッジの見える化システム

II. 社内の様々なシステムに散在する、文書やDBなど様々な情報源から、ものごとの関係性を自動抽出し、RDFで統合・見える化することが可能。複数の情報源からの様々な関係を把握するのに役立ちます。

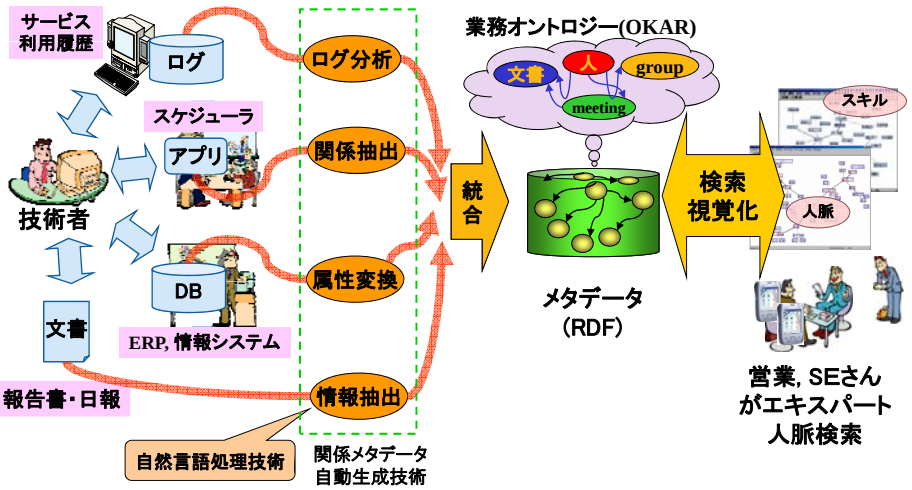
III. (例1) **富士通研究所**
研究員約1,000名のスキルや人脈を検索するKnowWho
（2004/11/19 日本経済新聞「特定分野に強い人材検索システム」）
(例2) **服薬指導支援**
薬や健康食品の飲み合わせチェック
（2006/10/9 第39回日本薬剤師会学術大会）
(例3) **地方銀行**
行内に散在する顧客間の関係を統合・見える化
（2008/5/7「滋賀銀行様においてビジネス情報ナビゲーションシステムが稼働」富士通プレスリリース）

ビジネス情報ナビゲーターの構成

FUJITSU

1. メタデータ自動生成
業務で使う様々な情報源(DB, テキスト、アプリ)から、人に関するメタデータを変換・統合

2. 関係を検索＋分析＋見える化
人のスキル・人脈を高速に検索し、関係をネットワーク分析（Know Who）



CCC DATAsetからのマルウエア分析

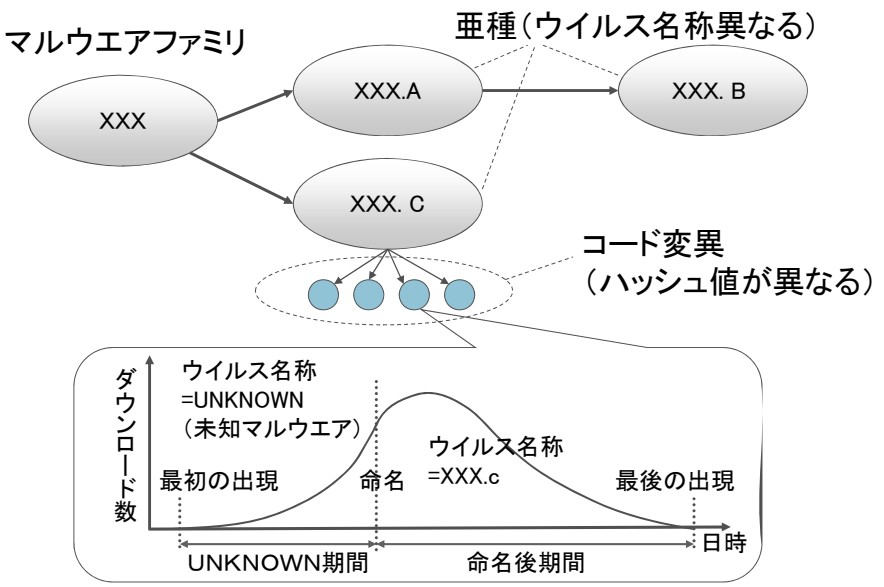
FUJITSU

- 研究用データセット　CCC DATAset 2008/2009
  - サイバークリーンセンター(https://www.ccc.go.jp/)で収集しているボット観測データ
  - マルウェア対策研究人材育成ワークショップ(MWS 2008,2009)にて、研究用データセットとして利用
  - 以下の3種類のデータ（CCC DATAset 2008の場合）
    - (1)マルウェア検体
      - ハニーポットで取得したマルウェア1検体のハッシュ値
    - (2)攻撃通信データ
      - ハニーポットで取得した通信のフルキャプチャデータ
      - 2台（WinXP、Win2000）の2日分、約2.8GB
      - FTTH、動的IPアドレス
    - (3)攻撃元データ
      - ハニーポットで取得したマルウェア取得時のログデータ
      - 時刻、ダウンロードホストIPアドレス、利用ポート番号／プロトコル、通信方向、ハッシュ値（SHA1）、ウイルス名称、ファイル名
      - ハニーポット112台、6ヶ月間、約294万レコード

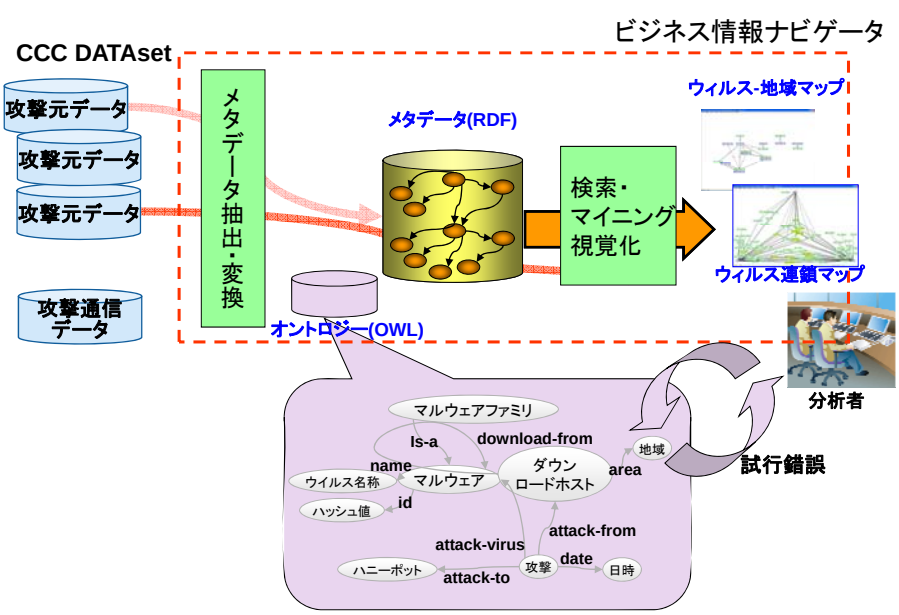
分析対象

(ハニーポット: マルウエア攻撃を受けるように設置されたPC)

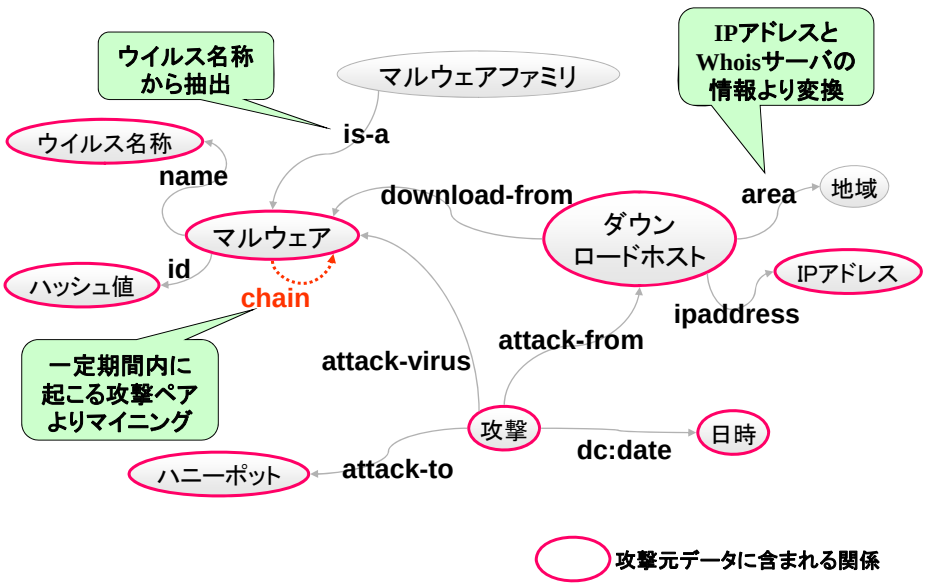
マルウエアのライフサイクル



マルウエア分析環境

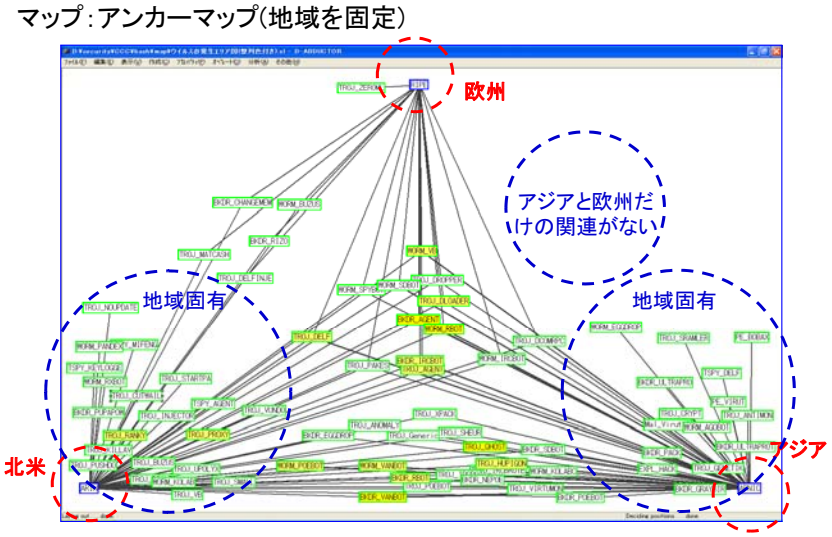


分析用メタデータ整備



(1) マルウエアファミリと地域の関連

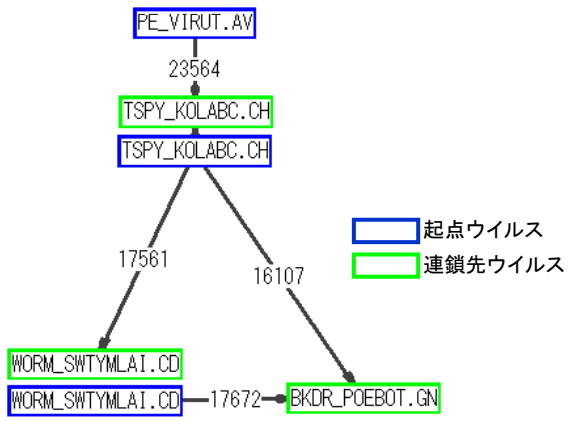
- ダウンロード時点では未知マルウエアだったものが、どこから攻撃されたか。命名後のマルウエアファミリと地域の関係を見える化。
- マップ：アンカーマップ(地域を固定)



(2) ウイルスの連鎖感染

FUJITSU

- マルウエア間の “chain” 関係のマイニング
  - 一定時間(5分)以内に、よく一緒に攻撃されるウイルス
  - (eg) KnowWhoにおける、共著者関係、同一会議への共出席関係



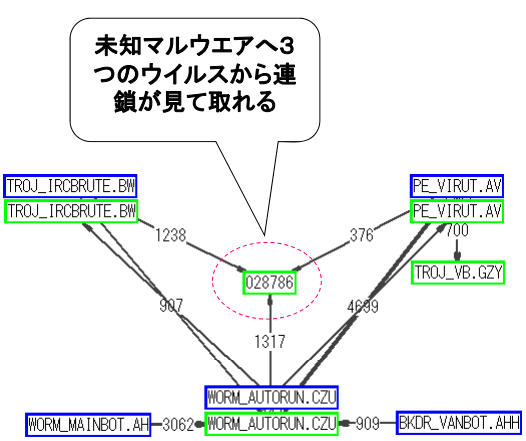
トレンドマイクロ社レポートにも、TSPY_KOLABC.CHが、WORM_SWTYMLAI.CDおよびBKDR_PEOBOT.GNを生成するという説明あり。

CCC DATAset2009におけるchain関係上位の見える化(一部)

(3) 未知マルウエアへの連鎖感染

FUJITSU

- 2009.4のchain関係の見える化

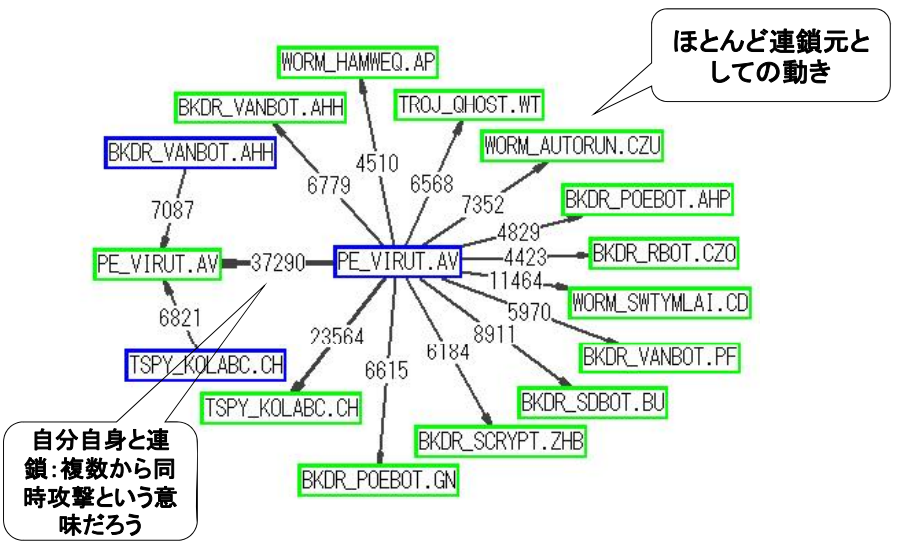


2009年4月サイバークリーンセンター活動実績でも、WORM_AUTORUN.CZUと未知検体への注意勧告がなされており、これに相当する

(4) 多くのマルウエアの連鎖元

FUJITSU

- PE_VIRUT.AV: CCC DATAset2009で攻撃数最多のマルウェア



まとめ

FUJITSU

- CCC DATAsetにおけるマルウエアのマクロな振る舞いを、セマンティックWebベースの見える化ツールで分析
  - 地域の関係、連鎖感染など、注意すべき関連性を相関マップにより分かりやすく見える化
- 可視化は単なる手段。ツールにデータを放り込めば終わりではない。どんな問題を解決するのに、何を見たいかを明らかにすることが必要
- オントロジー、メタデータにより一旦データを整理することで、こうした試行錯誤が見通し良くなる。
- 課題:さらに異種の情報源も加えた分析。LODで何か使えるものがあるか?

参考文献・リンク

FUJITSU

- 小櫻、津田、鳥居、”ウイルスのライフサイクルに着目した攻撃挙動の見える化”, MWS2008, 2008.10
- 小櫻、津田、鳥居、”ウイルスの時間的な関連性に注目した見える化”, MWS2009, 2009.10
- 松井,津田,片山, “ナレッジマネジメントツール:ビジネス情報ナビゲーター”, FUJITSU, pp.325-330, Vol.57, No.3, 2006
- 津田,ビジネスに生かすメタデータの統合・見える化技術, INTAPセマンティックWebコンファレンス, 2008
- W3C KnowWho, http://swada.w3.org/~htsuda/
- 滋賀銀行様においてビジネス情報ナビゲーションシステムが稼働～地域企業のビジネス相関図を見える化することで、地域密着型の提案を実現～, 富士通プレスリリース, 2008/5/7 http://pr.fujitsu.com/jp/news/2008/05/7.html
- 畑田他, “マルウエア対策のための研究用データセットとワークショップを通じた研究成果の共有”, MWS2009
- MWS2009, http://www.iwsec.org/mws/2009/
- サイバークリーンセンター https://www.ccc.go.jp/