IPA
Information-technology
Promotion
Agency, Japan

サイバー攻撃対策のための観測記述データ表記に関する検討

独立行政法人 情報処理推進機構（IPA）
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー
寺田真敏
2012年10月31日

目次

- 背景と目的
- 関連研究
  - サイバー攻撃対処モデル
  - サイバーセキュリティ情報交換仕様
- 観測記述データ表記に関する検討
  - 事例調査
  - 外部通信に着目した検討
- まとめ

背景と目的

- マルウェアの攻撃手法の多様化と巧妙化は進んでおり、活動形態にも大きな変化がみられる。
  - 1999年頃　メールを介したマルウェア（受動型感染）
  - 2001年頃　ネットワーク型ワーム（能動型感染）
  - 2004年頃　遠隔操作可能なボット（能動型感染）
  - 2008年頃　Web感染型マルウェア（受動型感染）
  - 2011年頃　メールと遠隔操作ツールの組合せ

- 機能面や実装面での変化を記録として残しつつ、その変化点を捉えて、効果的な対策につなげる。

背景と目的

- サイバー攻撃対処（脆弱性対策、インシデント対応）で活用できる仕様の整備が進んでいる。
  - ITU-T：サイバーセキュリティ情報交換フレームワーク（CYBEX）の標準化
  - 米国：サイバー攻撃対処（Cyber Kill Chain）モデルに基づいた情報交換仕様の検討

- JVN脆弱性対策機械処理基盤（JVN Security Content Automation Framework）などでの仕様活用を通して、地域性を考慮した機械処理基盤を整備する。

関連研究

- サイバー攻撃対処モデル
- サイバーセキュリティ情報交換仕様

サイバー攻撃対処モデル
新しいタイプの攻撃

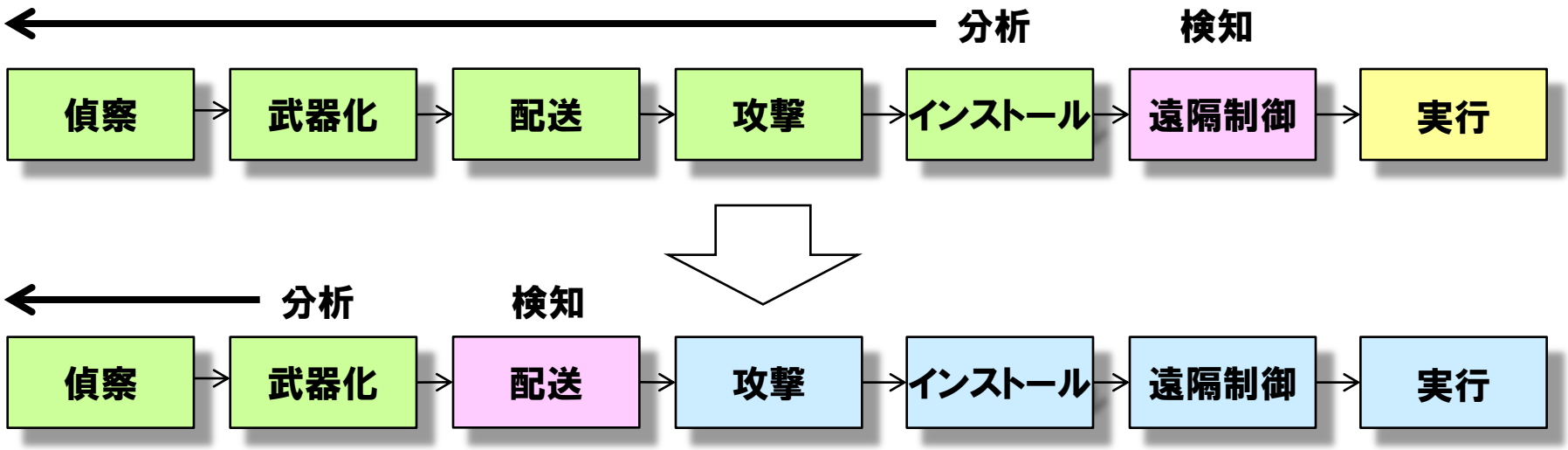
- 情報処理推進機構：『新しいタイプの攻撃』の対策に向けた設計・運用ガイド（2011年8月）
- 【モデル化で対象とする攻撃】
  入口での対策が効かない攻撃で、組織情報窃取や破壊を目的にする侵害活動で、従来の対策が効かないような共通攻撃手法と、組織に特化する攻撃である個別攻撃手法から構成される攻撃
- 【モデル】
  ① 攻撃準備段階
  ② 初期潜入段階
  ③ 攻撃基盤構築段階
  ④ システム調査段階
  ⑤ 攻撃最終目的の遂行段階

サイバー攻撃対処モデル
Intrusion Kill Chain (Cyber Kill Chain)

- Lockheed Martin: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (ICIW2011) (2011年3月)
- 【モデル化で対象とする攻撃】
  "Advanced Persistent Threat" (APT)
- 【モデル】
  - ① Reconnaissance (偵察)
  - ② Weaponization (武器化)
  - ③ Delivery (配送)
  - ④ Exploitation (攻撃)
  - ⑤ Installation (インストール)
  - ⑥ Command and Control (C2) (遠隔制御)
  - ⑦ Actions on Objectives (実行)

サイバー攻撃対処モデル
Intrusion Kill Chain (Cyber Kill Chain)

- 初期段階での分析ならびに検知へ（入口対策の強化）
  - 攻撃観測事象（Observable；攻撃によって観測された事象）、攻撃検知事象（Indicator；攻撃を検知するための事象）の活用



- 攻撃活動分析（Campaign Analysis）
  - 攻撃者のパタン、行動、TTP（Tactics, Techniques and Procedures：戦術、技術及び手順）を明らかにする。
  - 攻撃者の意図を明らかにする。

サイバーセキュリティ情報交換仕様 CYBEX

IPA

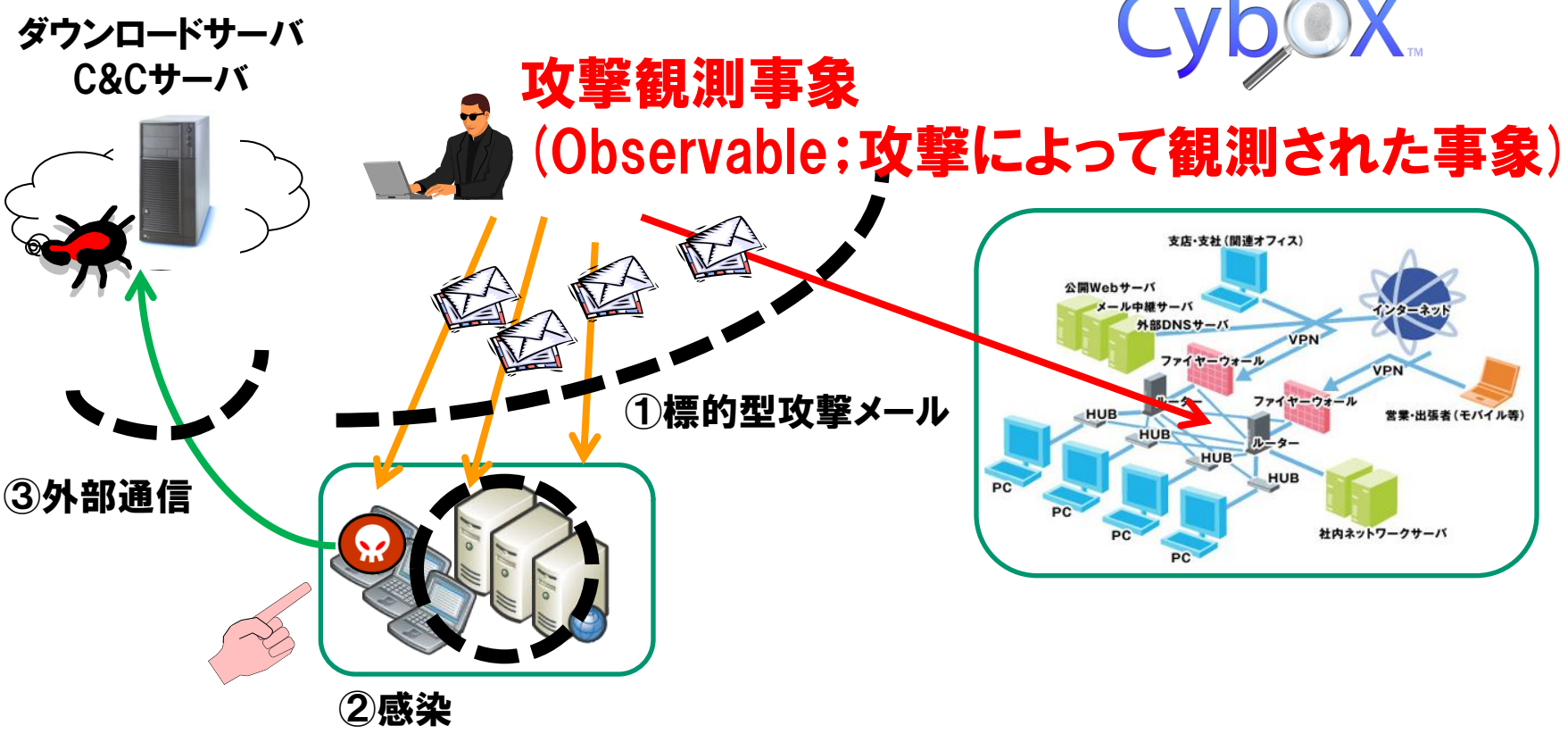
- ITU-T Q.4/17: X.cybex
  (Global Cybersecurity Information Exchange Framework；サイバーセキュリティ情報交換フレームワーク)
  - 共通仕様を用いて、グローバルかつタイムリーなサイバーセキュリティ情報の交換、活用ならびに、相互運用を実現するためのフレームワークを実現するため、脆弱性対策情報ならびにインシデント対応のフォーマット、番号体系などの技術仕様について標準化を進めている。
    脆弱性対策関連 (X.cpe、X.cce、X.cve、X.crf、X.oval、X.cwe、X.cvssなど) 、インシデント対応関連 (X.cee、X.iodef、X.capecなど) の共通仕様がある。

サイバーセキュリティ情報交換仕様
Cyber Kill Chain 関連活動

IPA

攻撃活動分析（Campaign Analysis） STIX™

CybOX™



サイバーセキュリティ情報交換仕様
Cyber Kill Chain 関連活動

- CybOX（Cyber Observable eXpression；サイバー攻撃観測記述形式）
  - MITREが中心となり仕様策定を進めてきたもので、サイバー攻撃活動によって観測された事象を記述するためのXML仕様 である。MandiantのOpenIOC（侵害を受けたシステムの痕跡(Indicator of Compromise)を記述する仕様)を踏まえた仕様となっている。
  - 経緯
    - 2009年9月: CAPECの延長で検討開始
    - 2010年6月: CAPEC、MAEC、CEEとの連携検討開始
    - 2010年12月: スキーマ V0.4完成(Mandiant OpenIOC連携)
    - 2011年5月: CEEとの連携、CybOXリリース
    - 2012年1月: CybOXスキーマ V0.7リリース(MAEC V2.0連携)
    - 2012年4月: CybOXスキーマ V1.0リリース

サイバーセキュリティ情報交換仕様
Cyber Kill Chain 関連活動

- Account
- Address
- API
- Code
- Device
- Disk
- Disk Partition
- DNS Cache
- DNS_Record
- Email Message
- File
- GUI
- GUI Dialog Box
- GUI Window
- Library
- Linux Package
- Memory
- Mutex
- Network Flow
- Network Packet
- Network Route Entry
- Network Route
- Network Subnet
- Pipe
- Port
- Process
- Product
- Semaphore
- Socket
- System
- Unix File
- Unix Network Route Entry
- Unix Pipe
- Unix Process
- Unix User Account
- Unix Volume
- URI
- User Account
- User Session
- Volume
- Win Computer Account
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Executable File
- Win File
- Win Kernel
- Win Kernel Hook
- Win Handle
- Win Mailslot
- Win Mutex
- Win Pipe
- Win Network Route Entry
- Win Network Share
- Win Pipe
- Win Prefetch
- Win Process
- Win Registry Key
- Win Semaphore
- Win Service
- Win System
- Win System Restore
- Win Task
- Win Thread
- Win User Account
- Win Volume
- Win Waitable Timer
- X509 Certificate

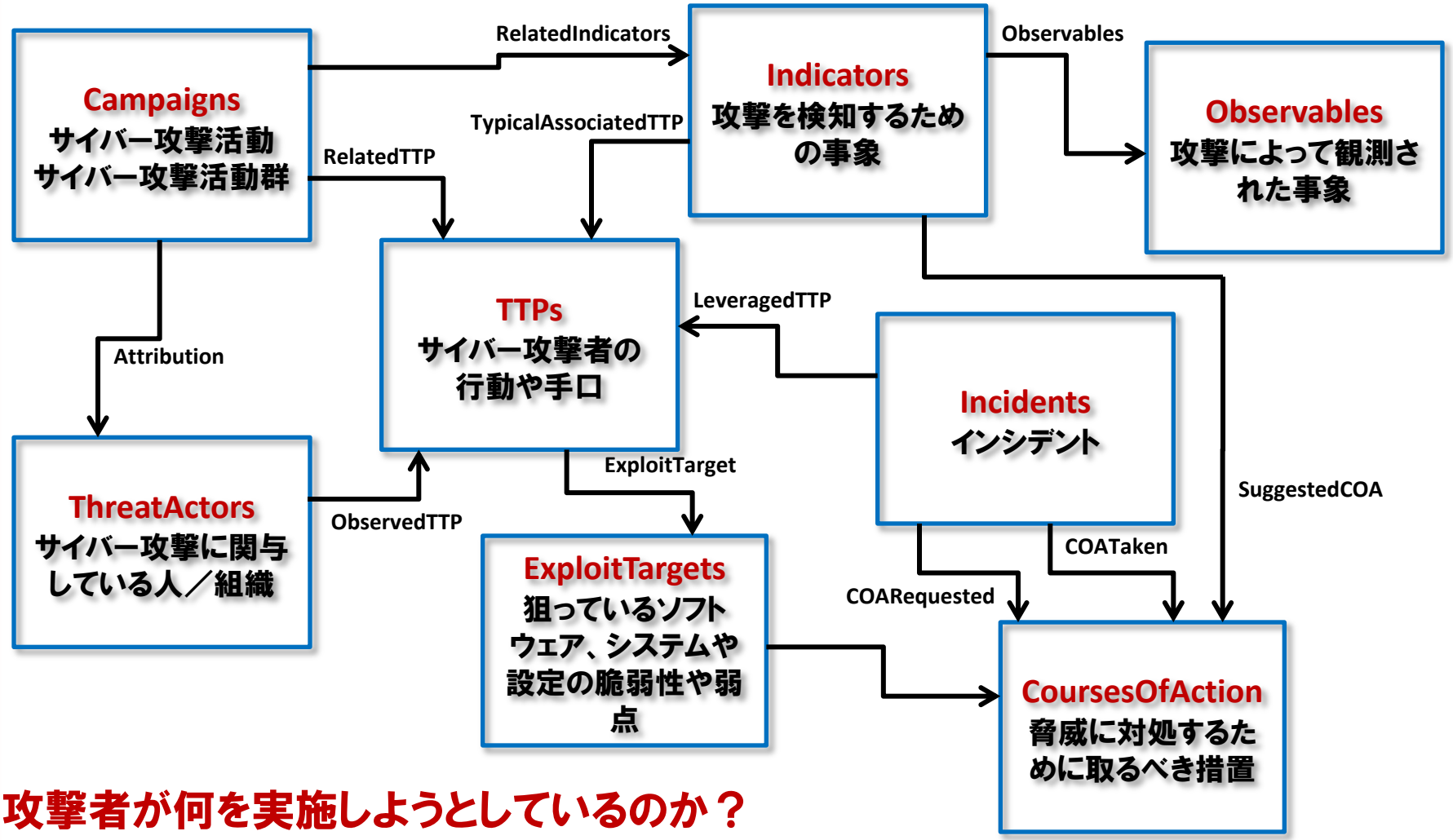
…

(more on the way)

サイバーセキュリティ情報交換仕様
Cyber Kill Chain 関連活動

- STIX（Structured Threat Information eXpression；脅威情報構造化記述形式）
  - MITREが中心となり仕様策定を進めてきたもので、サイバー攻撃（cyber threats；サイバー空間における脅威）の分析、サイバー攻撃を特徴付ける事象（indicator）の特定、サイバー攻撃対応の管理、サイバー攻撃に関する情報の共有などを目的としたXML仕様である。
  - 経緯
    - 2010年：US-CERTとCERT/CC、脅威情報の交換について検討開始⇒脅威情報を構造化したダイアグラムの作成
    - 2012年6月：STIXスキーマ V0.3リリース
    - 2012年8月：STIXスキーマ V0.5リリース

サイバーセキュリティ情報交換仕様
Cyber Kill Chain 関連活動



攻撃者が何を実施しようとしているのか？
どのように実施しようとしているのか？を特徴付けていくこと

観測記述データ表記に関する検討

- 事例調査
- 外部通信に着目した検討

事例調査

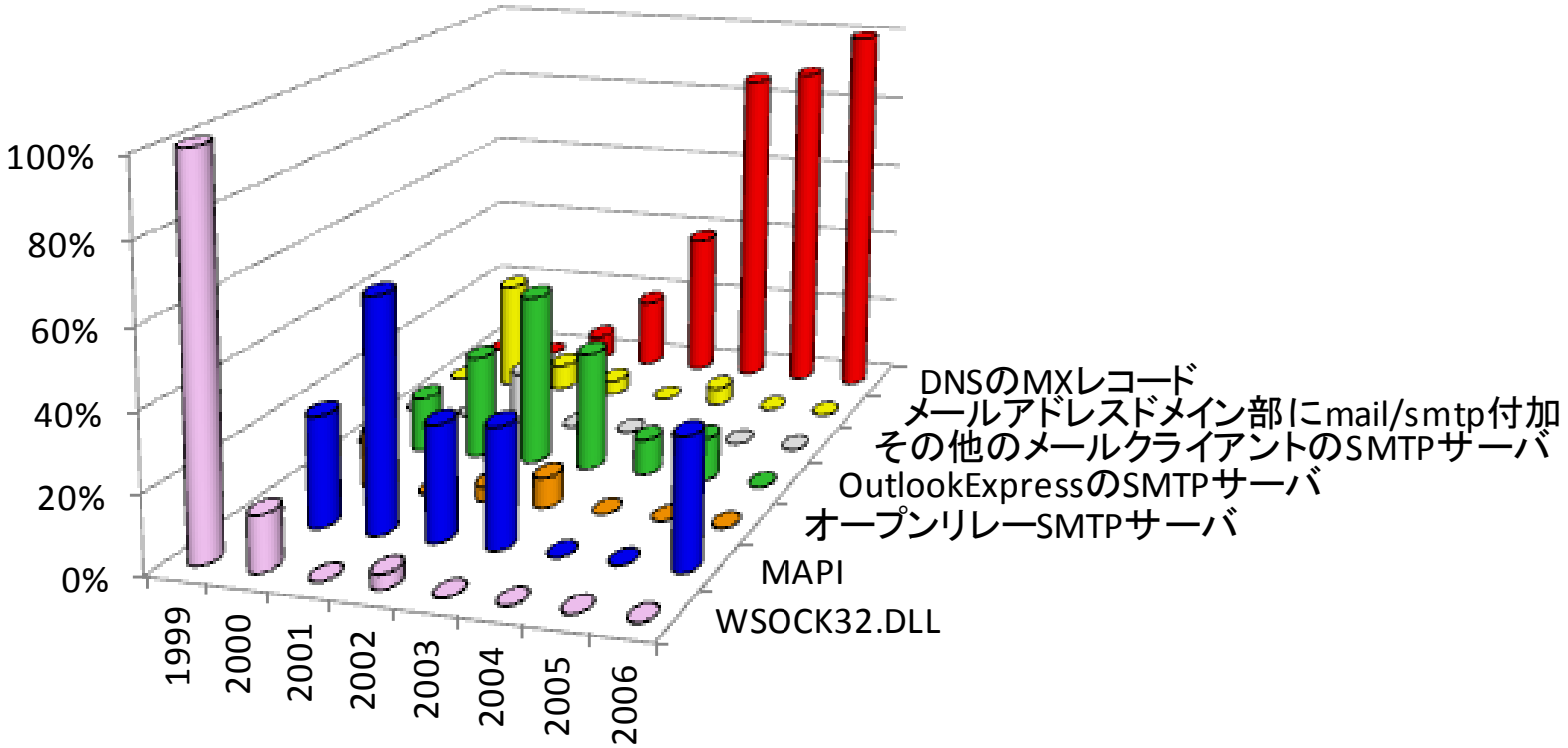
- メール型ワームを対象とした、機能面や実装面での変化の事例
  - マルウェアのメール送信方法
  - マルウェアのメールアドレス収集方法

事例調査

- メール送信方法に関する実装の分類
  - WSOCK32.DLL
  - MAPI
  - SMTP
    - 特定　　オープンリレーSMTPサーバ
    - 送信側　Outlook ExpressのSMTPサーバ
その他のメールクライアントのSMTPサーバ
    - 受信側　メールアドレスドメイン部にmail./smtp.付加
DNSのMXレコード

事例調査

- メール送信方法に関する実装の分類

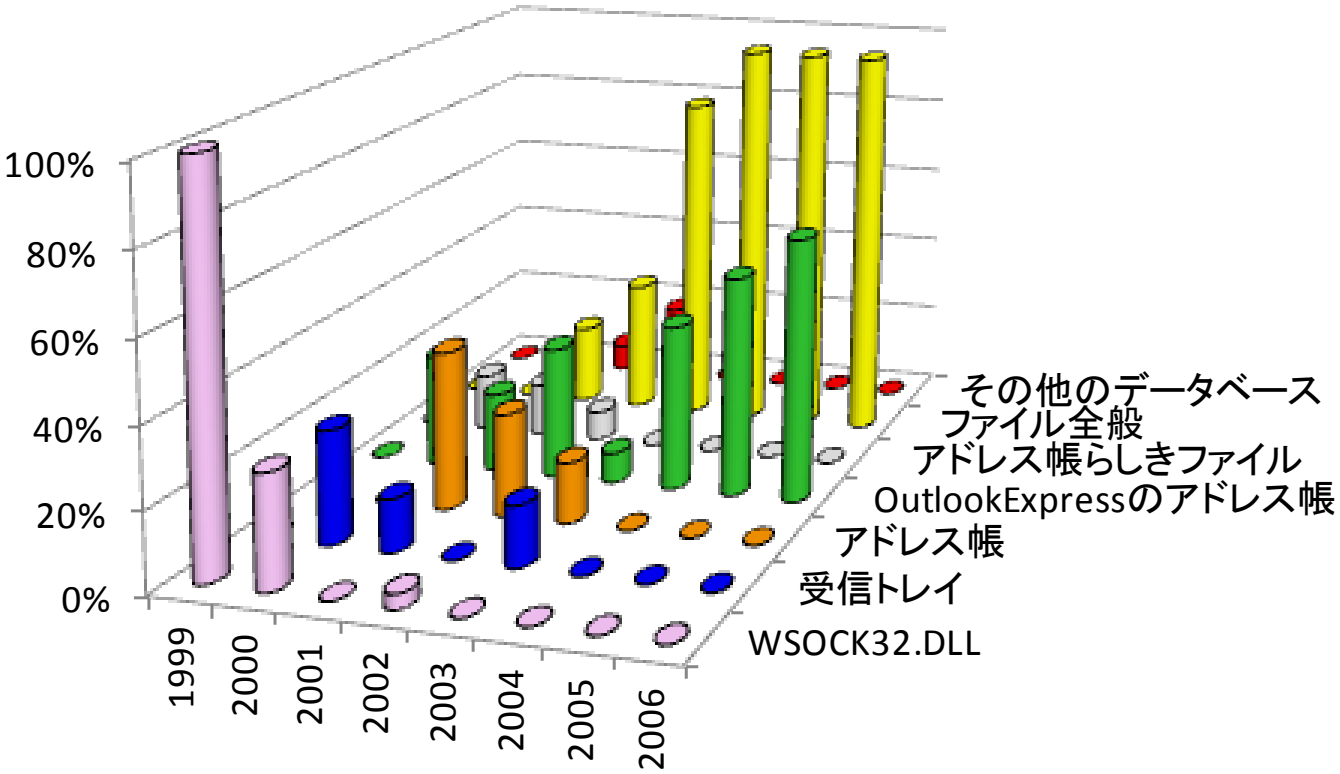


事例調査

- メールアドレス収集方法に関する実装の分類
  - WSOCK32.DLL
  - MAPI
    - 受信トレイ
    - アドレス帳
  - ファイル探索
    - Outlook Expressのアドレス帳
    - アドレス帳らしきファイル
    - ファイル全般
  - その他のデータベース

事例調査

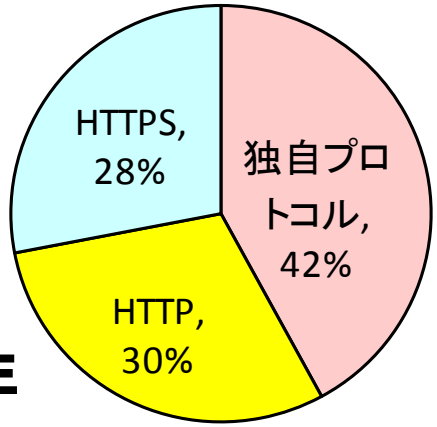
- メールアドレス収集方法に関する実装の分類



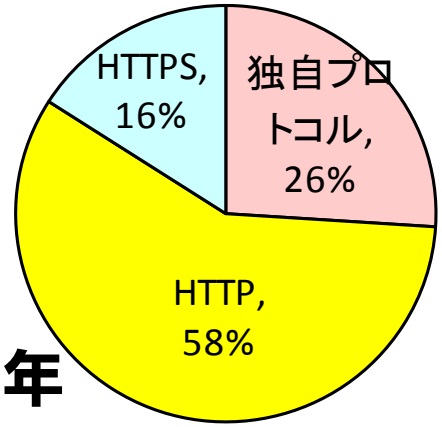
外部通信に着目した検討

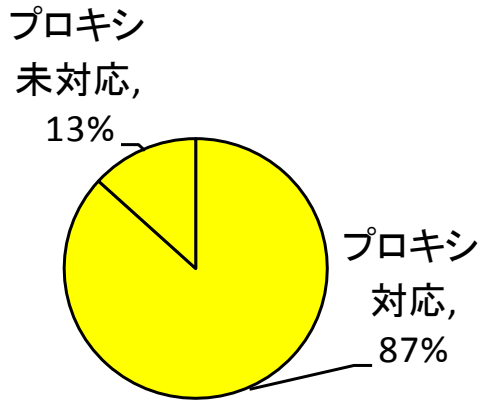
- 外部通信プロトコルの推移

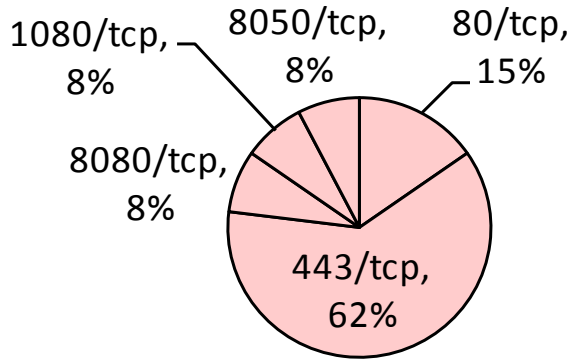
2011年



2012年



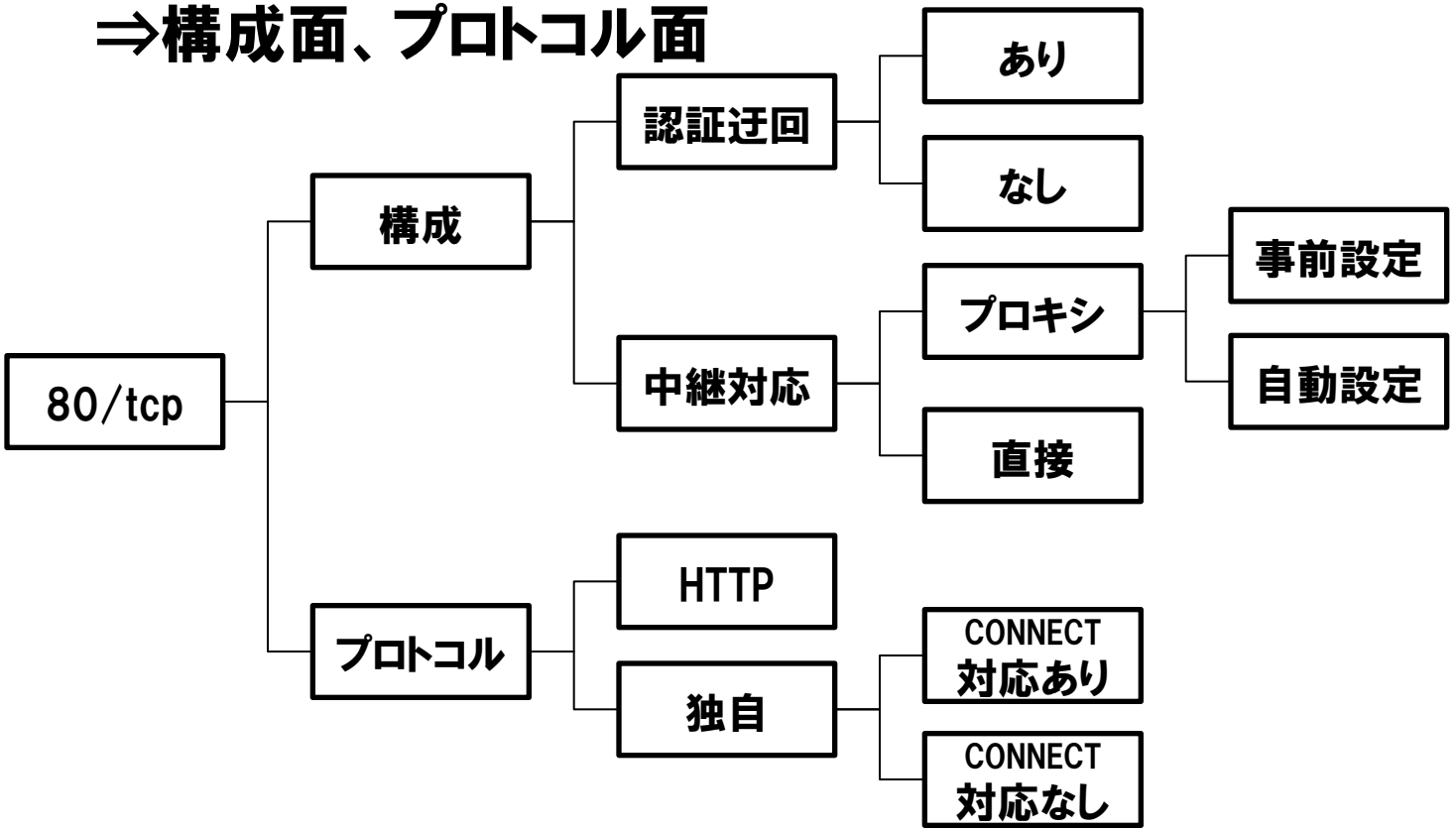




出典:トレンドマイクロ。2011年は2011年4月～10月に、国内で収集された標的型攻撃メールに添付されていたと思われるマルウェア50検体のバックドア通信を対象。2012年は文献[2]を参照。

外部通信に着目した検討

- 記録情報
  - 機能面や実装面での変化を記録として残しつつ、その変化点を捉えて、効果的な対策につなげる。
    ⇒構成面、プロトコル面



外部通信に着目した検討

- 記録情報のレベル分け
  - レベル1
    対策の一次情報として利用できるデータ
    マルウェアのハッシュ値、接続先IPアドレスなど
  - レベル2
    レベル1の補足情報や対策の阻害要因を示すデータなど
    プロキシ対応、認証迂回機能など
  - レベル3
    今後、対策の阻害要因になるかもしれない情報など
    マルウェア自身の防衛機能など

CybOX

外部通信に着目した検討
記録情報レベル1

IPA

- **標的型攻撃メールの記述例**

```
<?xml version="1.0" encoding="UTF-8" ?>
<cybox:Observables cybox_major_version="1" cybox_minor_version="0(draft)">
<cybox:Observable>
<cybox:Stateful_Measure>
        <cybox:Object id="cybox:email_attached" type="Email Message">
        <cybox:Defined_Object xsi:type="EmailMessageObj:EmailMessageObjectType">
                <EmailMessageObj:Attachments>
                        <EmailMessageObj:File>
                        <FileObj:File_Name datatype="String">malware_infected.zip</FileObj:File_Name>
                        <FileObj:Hashes>
                                <common:Hash>
                                <common:Type datatype="String">SHA1</common:Type>
                                <common:Simple_Hash_Value condition="Equals" datatype="hexBinary">
                                1aa7c9d7ef3.....2f733f01b35dca</common:Simple_Hash_Value>
                                </common:Hash>
                        </FileObj:Hashes>
                        </EmailMessageObj:File>
                </EmailMessageObj:Attachments>
                <EmailMessageObj:Header>
                        <EmailMessageObj:From category="e-mail">
                        <AddrObj:Address_Value datatype="String">attacker@example.com</AddrObj:Address_Value>
                        </EmailMessageObj:From>
                </EmailMessageObj:Header>
        </cybox:Defined_Object>
        </cybox:Object>
</cybox:Stateful_Measure>
</cybox:Observable>
</cybox:Observables>
```

添付ファイル

メール
ヘッダ

CybOX™

外部通信に着目した検討
記録情報レベル1

IPA

- **外部接続の記述例**

```
<?xml version="1.0" encoding="UTF-8" ?>
<cybox:Observables cybox_major_version="1" cybox_minor_version="0(draft)">
<cybox:Observable>
<cybox:Stateful_Measure>
        <cybox:Object id="cybox:mws2012.d3m.545e" type="File">
                <cybox:Defined_Object xsi:type="FileObj:FileObjectType">
                <FileObj:File_Name datatype="String">20110725.exe</FileObj:File_Name>
                <FileObj:Size_In_Bytes datatype="UnsignedLong">16896</FileObj:Size_In_Bytes>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
                <cybox:Related_Object idref="cybox:mws2012.d3m.545e.con2"
                type="URI" relationship="Connected_To" />
        </cybox:Related_Objects>
        </cybox:Object>
</cybox:Stateful_Measure>
</cybox:Observable>
<cybox:Observable>
<cybox:Stateful_Measure>
        <cybox:Object id="cybox:mws2012.d3m.545e.con2" type="URI">
        <cybox:Defined_Object xsi:type="URIObj:URIObjectType" type="URL">
        <URIObj:Value datatype="AnyURI" condition="Equals">xxx2wahaha.cn</URIObj:Value>
        </cybox:Defined_Object>
        </cybox:Object>
</cybox:Stateful_Measure>
</cybox:Observable>
</cybox:Observables>
```

ファイル属性
- ファイル名
- ファイルサイズ

接続先URL

CybOX™

まとめ

IPA

- マルウェアの機能面や実装面での変化を記録として残しつつ、その変化点を捉えて、対策につなげるためのアプローチについて示した。
  - 実装面での変遷として、2000年代前半に流布したメール型ワームの事例調査を通して、メール送信方法とメールアドレス収集方法のいずれにおいても、実装面での変化点があることを示した。
  - マルウェアの外部通信に着目し、対策にあたっては構成面、プロトコル面の双方から、どのような通信形態が増えてきたのかを捉えていくことと、変化として記録すべき情報を示した。
- 今後の課題
  - 3段階のレベル分けの実現方法として、特にレベル2、3の記録フォーマットなどの記録方法を具体化
  - 変化点を捉えるための事例収集