MSOffice1

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2008年2月20日

重要インフラ事業者への新たな見えない脅威

独立行政法人 情報処理推進機構
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

研究員 鵜飼裕司

MSOffice1 , 2008/01/29

はじめに

特定の企業・組織を標的とした標的型攻撃が深刻化

攻撃が見えにくくなっている
企業・組織は十分な情報や技術的解決策を得られない

詳細な挙動・仕組みはよく分かっていない
脅威を正確に把握できない

近年の標的型攻撃とそれがもたらす脅威について詳細な調査研究を行い
実態を正確に把握し、対策に結びつける

標的型攻撃と近年のマルウエア　1

標的型攻撃は・・・

- 近年のマルウエア攻撃の一形態
- 攻撃対象が限定的。攻撃発生前に情報を入手し対応を取る事が難しい
- ダウンローダ経由で設置する「シーケンシャルマルウエア」
- 脆弱性を利用することも
- 解析や検出を困難にするための手法が高度化

標的型攻撃と近年のマルウエア　2

アンチウイルスや侵入検知などが有効に機能しないケースも

従来型マルウエア

標的型攻撃と近年のマルウエア　3

アンチウイルスや侵入検知などが有効に機能しないケースも

シーケンシャルマルウエア

マルウエアの解析と脅威分析

近年のマルウエアは攻撃手順が複雑化、プログラムは肥大化
マルウエア対策では効率よくシグネチャを開発する事が重要

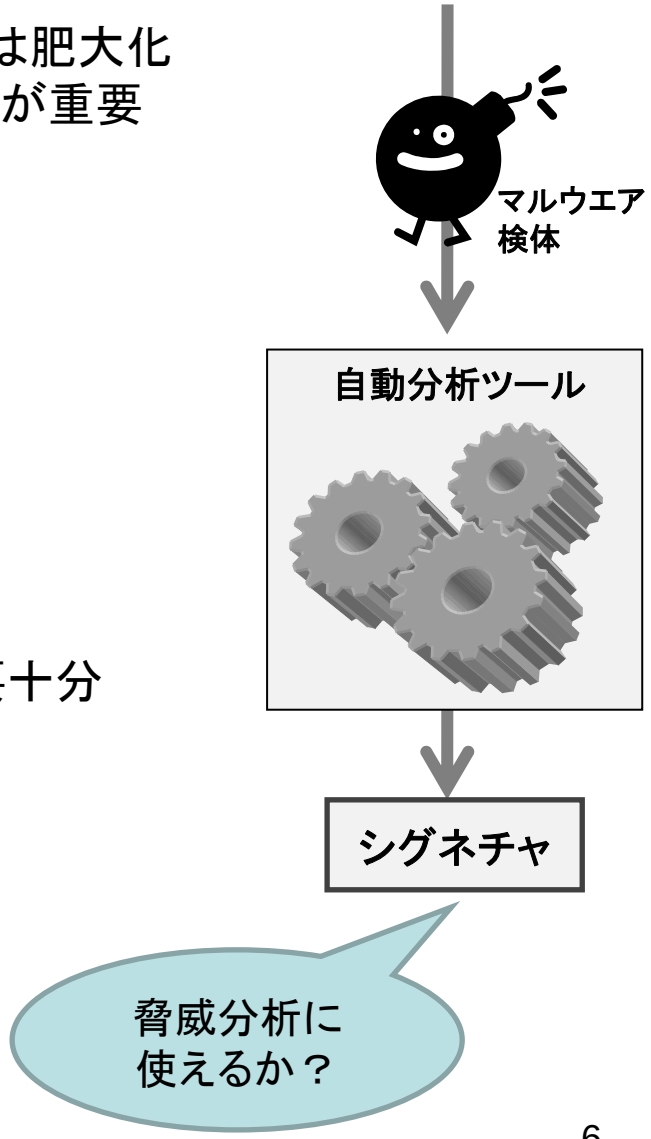
・API (Application Program Interface) トレース
・ファイルシステムやレジストリのモニタリング
・通信の分析、など

解析は自動化可能な所に限定

検出シグネチャを開発するという目的においては必要十分

しかし・・・
- アンチウイルス製品は脅威分析目的ではない
- マルウエアの感染の防止が目的

自動化された解析手法だけでは十分でない



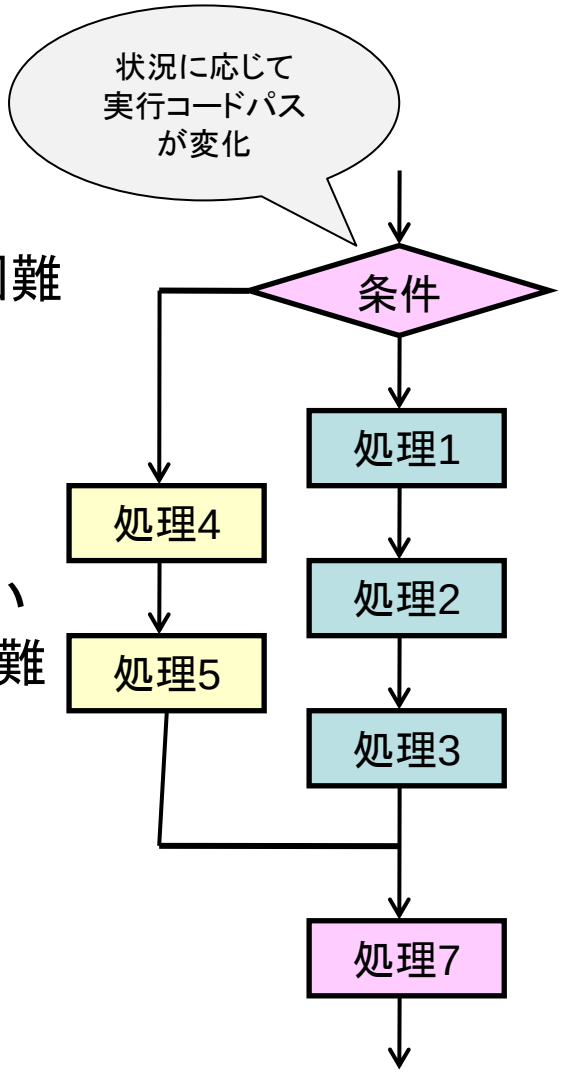
マルウエアの自動解析による脅威分析の問題点

マルウエアの自動解析では、

コードの詳細を把握できないため正確な挙動分析が困難

- 状況に応じて実行パスやコードが変化する可能性
- 分析時以外の状況で何が起こるのか予測不可
- トレースログから正確な全体フローの作成が困難
- 通信も暗号化し、送受信内容を正確に把握できない
- 攻撃者の指示や動作の可能性の網羅的分析が困難

正確な脅威分析には全コードの網羅的解析が必要



調査研究の概要

a.標的型攻撃用セキュリティ脆弱性の実態調査・傾向分析

b.標的型攻撃用セキュリティ脆弱性の分析

- アタックベクタ、脆弱性の性質、攻撃安定性、環境依存性などの観点から分析
- 今後の標的型攻撃に利用される可能性が高いソフトウエアの傾向を分析

c. 標的型攻撃用マルウエア実態調査・傾向分析

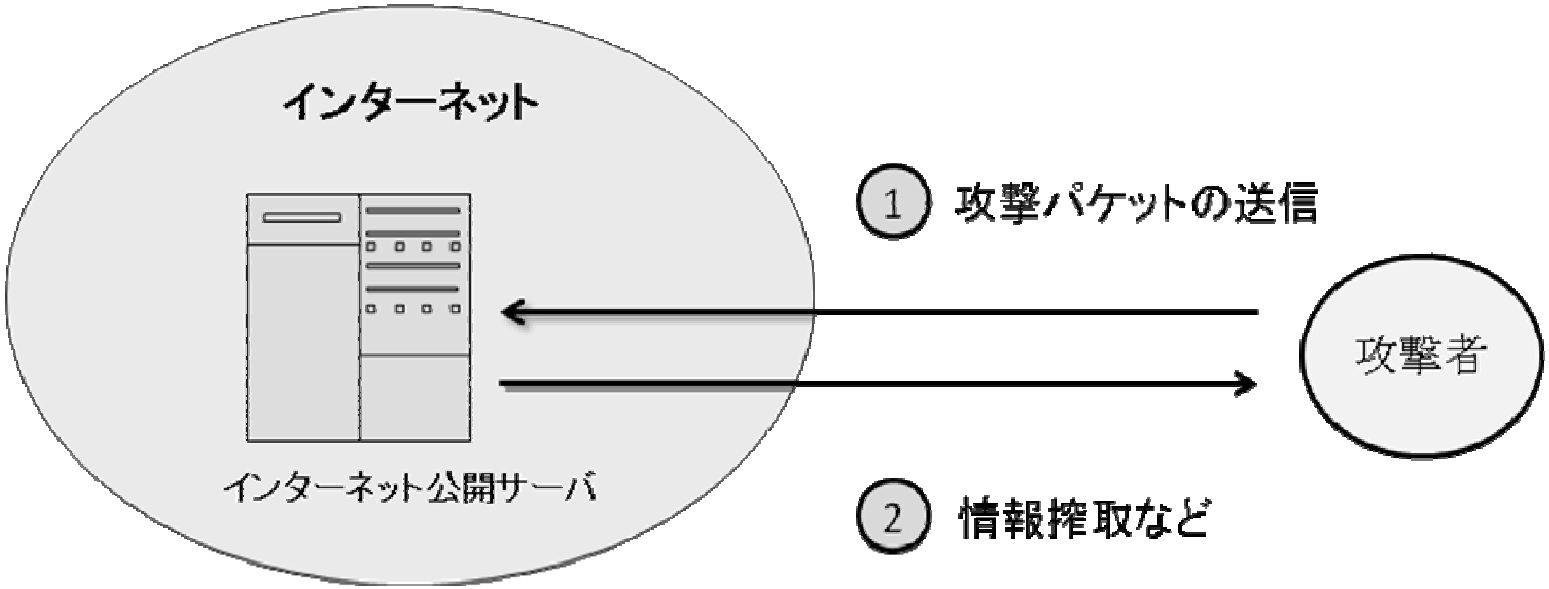
d. 標的型攻撃用マルウエア分析

- 静的・動的解析（構造と挙動、攻撃シーケンスを分析）
- シーケンシャルマルウエアの攻撃ダウンロードサイトの特徴分析・収集分析
- 一般に広く感染したマルウエアとの共通性分析
- 標的型攻撃の攻撃モデルの分析整理
- イントラ内に潜伏したマルウエアの検知手法の検討
- シーケンシャルマルウエア攻撃シーケンスに応じる動的解析手法の検討

標的型攻撃に利用される脆弱性のタイプ　1

対象はサーバではなく企業などのイントラネット内PC
外部から直接アクセス不可
受動的攻撃が主流

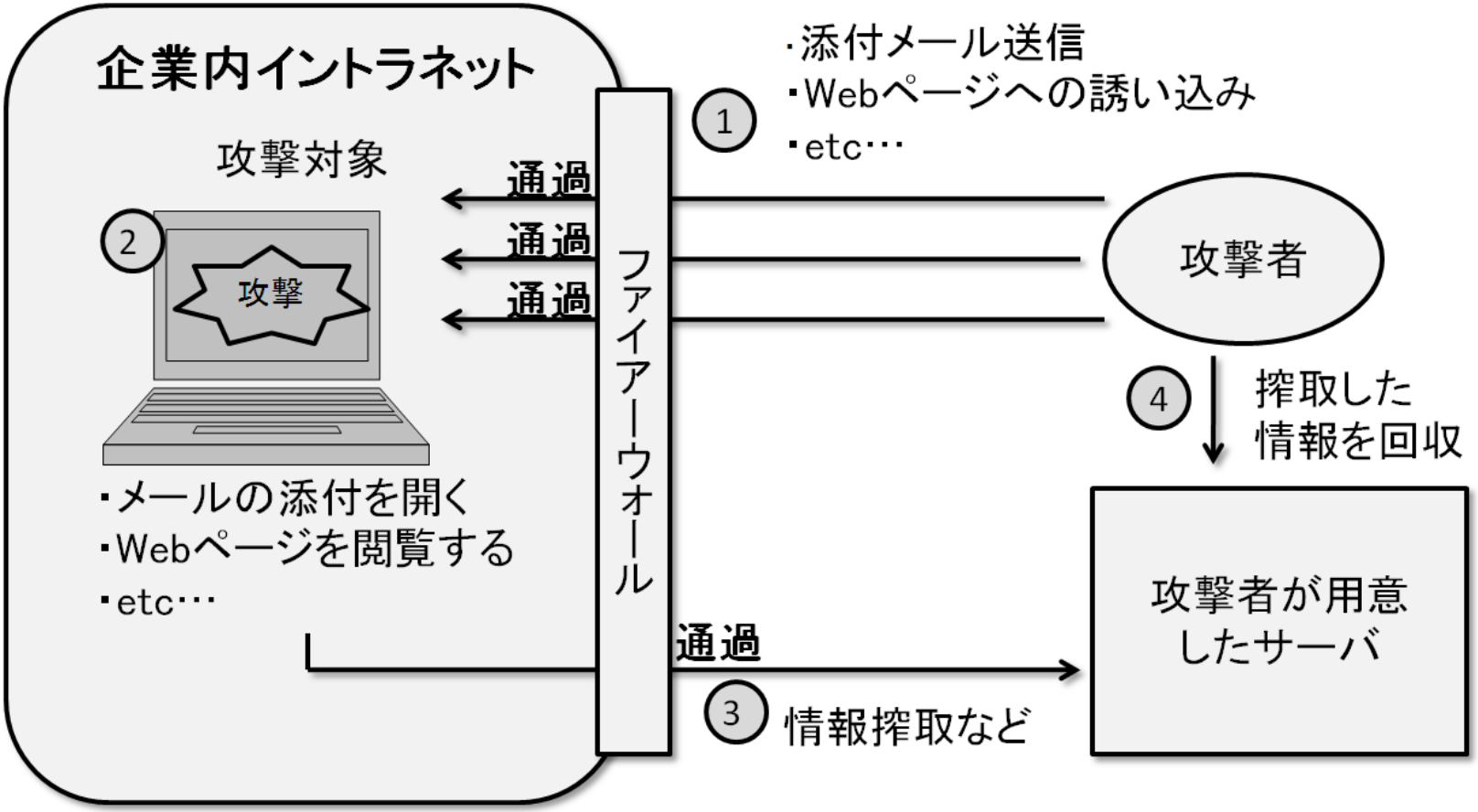
能動的攻撃　　・ネットワークサービスに直接攻撃
・ネットワーク的に到達可能が前提
・イントラネット内システムの攻撃は難しい



標的型攻撃に利用される脆弱性のタイプ　2

受動的攻撃

・攻撃対象ユーザーの何らかの操作が前提
・e-mailなどの手段で簡単に到達
・イントラネット内システムの攻撃に有利



代表的な標的型攻撃で利用された脆弱性　1

系列　MDropper 系	
名称	**脆弱性**
Trojan.Mdropper.A Trojan.Mdropper.B Trojan.Mdropper.D	Microsoft Word (MS03-050)
Trojan.Mdropper.C Trojan.Mdropper.F Trojan.Mdropper.G	Microsoft Office 製品(MS03-037)
Trojan.Mdropper.J	Microsoft Office 製品(MS06-037)
Trojan.Mdropper.H Trojan.Mdropper.I Trojan.Mdropper.K Trojan.Mdropper.Q Trojan.Mdropper.T Trojan.Mdropper.U Trojan.Mdropper.W Trojan.Mdropper.X	Microsoft Office(0-day、もしくは不明)
Trojan.Mdropper.L Trojan.Mdropper.P Trojan.Mdropper.S	Microsoft Word (MS06-027)
Trojan.Mdropper.N Trojan.Mdropper.R	Microsoft Office (MS06-047)
Trojan.Mdropper.Z	Microsoft Word (MS07-015)

代表的な標的型攻撃で利用された脆弱性　2

系列　PPDropper 系	
名称	**脆弱性**
Trojan.PPDropper Trojan.PPDropper.D Trojan.PPDropper.E	Microsoft Office 製品(MS06-012)
Trojan.PPDropper.B Trojan.PPDropper.C	Microsoft Power Point (0-day、もしくは不明)
Trojan.PPDropper.F	Microsoft Office 製品(MS06-058)
Trojan.PPDropper.G	Microsoft Office 製品(MS07-015)

代表的な標的型攻撃で利用された脆弱性　3

系列　Acdropper 系	
名称	**脆弱性**
Trojan.Acdropper Trojan.Acdropper.B	Microsoft Jet Database Engine (0-day、もしくは不明)
系列　Tarodrop 系	
名称	**脆弱性**
Troj_Tarodrop	一太郎 (0-day 詳細不明)
系列　解凍ソフト系	
名称	**脆弱性**
Exploit-LHAZ.a	Lhaz の脆弱性
Trojan.Radropper	WinRAR の脆弱性

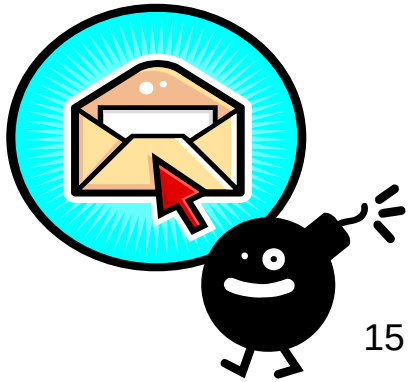
代表的な標的型攻撃で利用された脆弱性 2

脆弱性	概要
MS03-037	VBA(Visual Basic for Applications)の脆弱性の脆弱性により、任意のコードが実行される
MS03-050	Microsoft Word および Microsoft Excel の脆弱性により、任意のコードが実行される
MS06-012	Microsoft Office の脆弱性により、任意のコードが実行される
MS06-027	Microsoft Wordの脆弱性により、任意のコードが実行される
MS06-047	VBAの脆弱性の脆弱性により、任意のコードが実行される
MS06-058	Microsoft PowerPointの脆弱性により、任意のコードが実行される
MS07-015	Microsoft Office の脆弱性により、任意のコードが実行される
Lhaz の脆弱性	ZIPファイル処理における脆弱性により、任意のコードが実行される
WinRAR の脆弱性	LZHファイル処理における脆弱性により、任意のコードが実行される

狙われやすいソフトウエアと脆弱性

1. 多くのユーザーの間で「開いても安全」な認識が高いファイルを利用

- e-mailの添付ファイルや外部webサーバへのリンクが大半
- webブラウザやメーラーは安全性確認と脆弱性対応が進む
  簡単に悪用できる致命的脆弱性が少ない
- OSではなくアプリケーションの脆弱性が利用されるケースが多い
  → 文書処理ソフトウエア、アーカイバなど



狙われやすいソフトウエアと脆弱性

2. 著名なソフトウエアの脆弱性が標的型攻撃においてよく利用される

・対象システムで利用されているアプリケーションの推測が困難

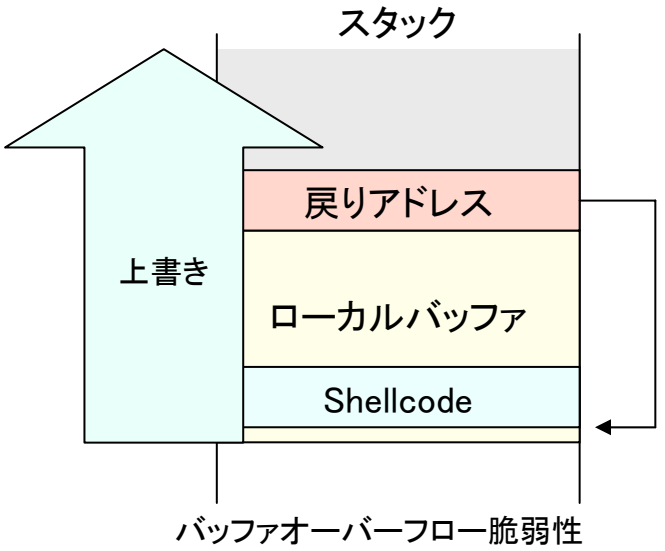
・アプリケーションの著名さは国ごとに異なるケースがある →
特定の地域や組織のみ利用されるソフトウエアの脆弱性も悪用

標的型攻撃に利用された脆弱性

TROJ_MDROPPER系およびPPDROP系

(1)アタックベクタ
- 両者ともMicrosoft Officeファイル
- e-mailに添付されて到達
- 脆弱性が攻略されマルウエアに感染

(2)脆弱性の性質
- 両者ともバッファオーバーフロー脆弱性

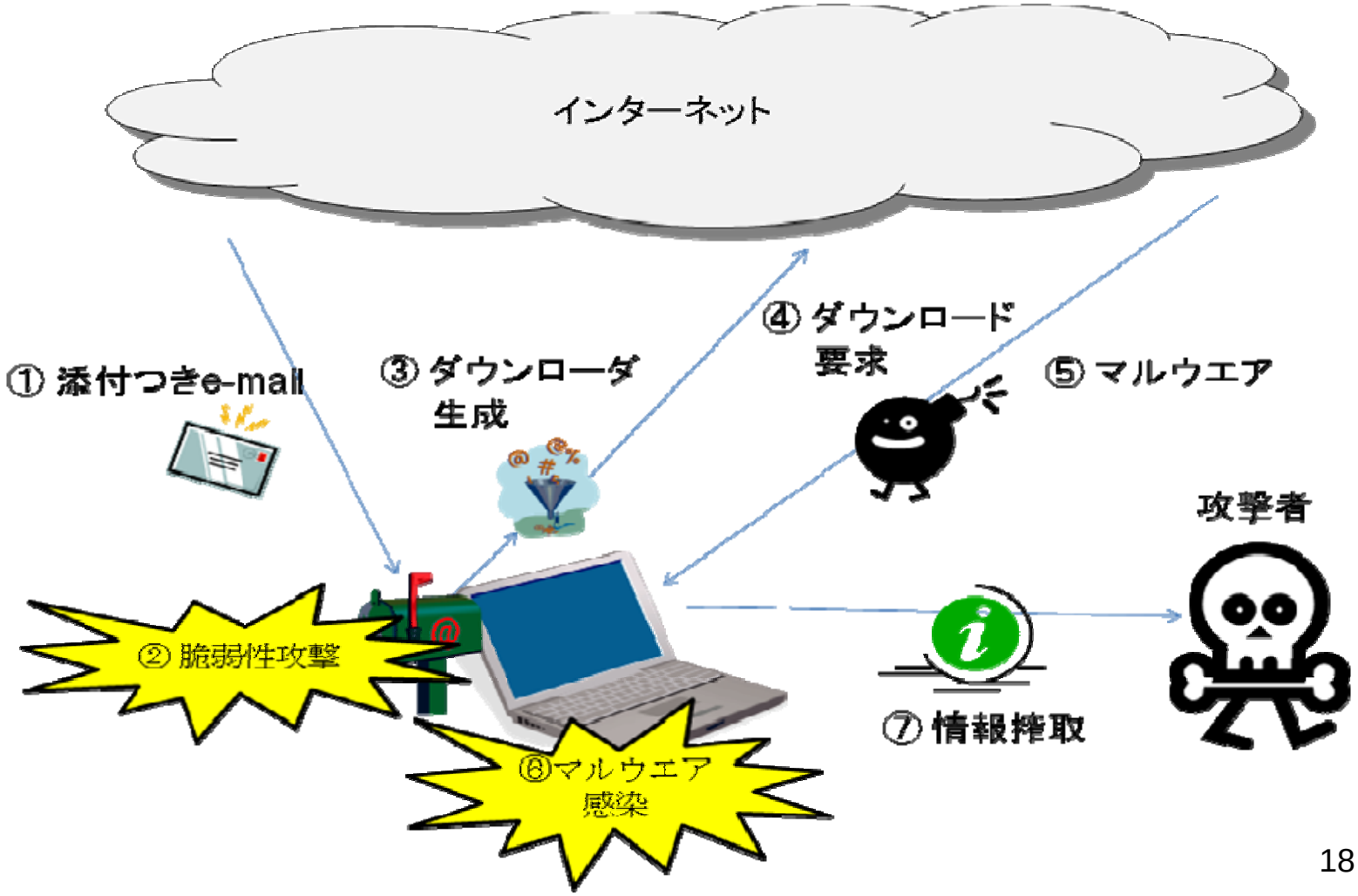


(3)攻撃安定性
- 両者とも非常に安定して攻撃できる脆弱性のみ利用
- 攻撃安定性が低い脆弱性は利用されていない

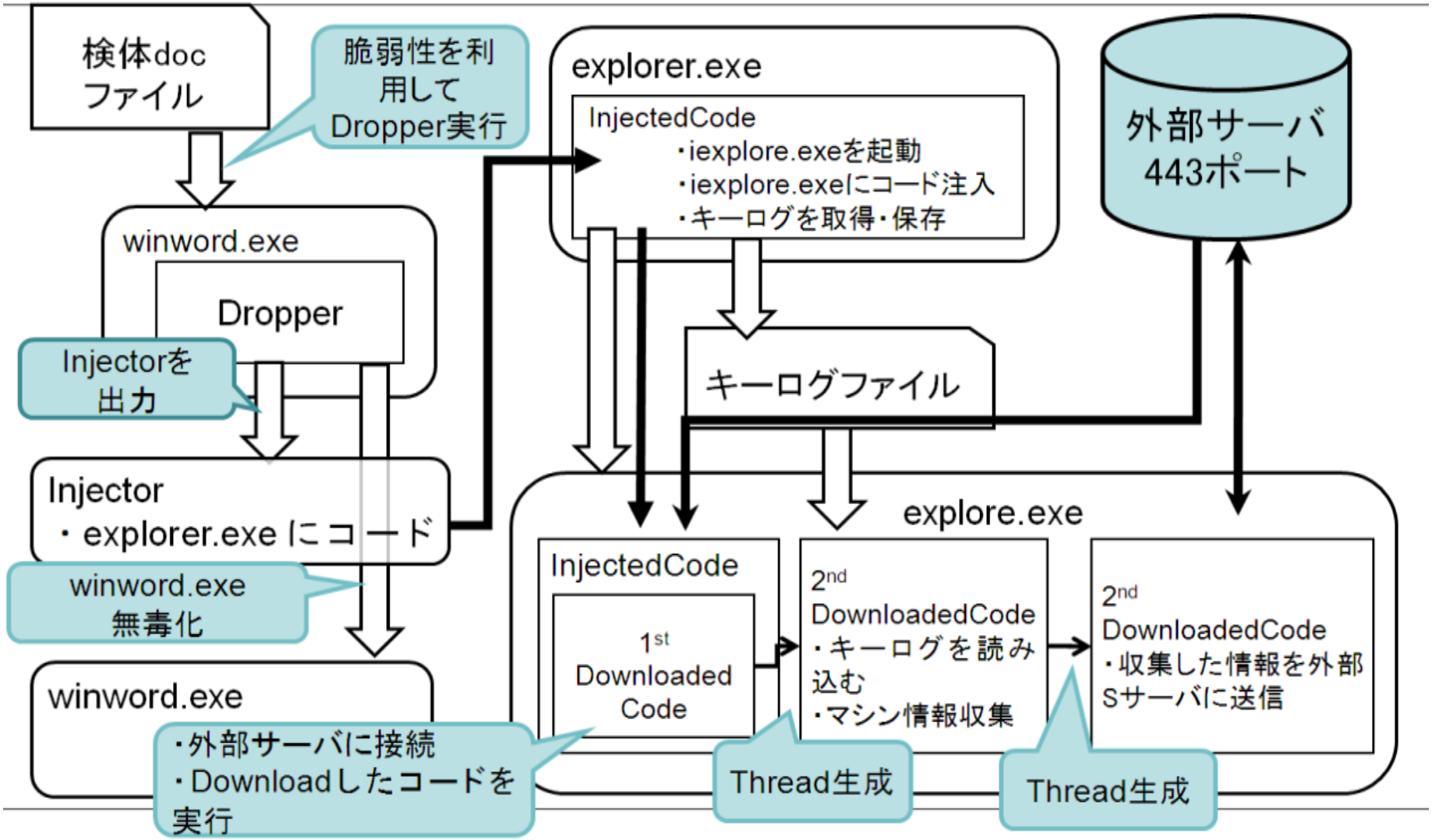
(4)環境依存性
- TROJ_MDROPPER系のExploitは環境依存性が高く発動せず
- 攻撃シーケンスは全体的に高度だが、重要要素のExploitingが非常に稚拙

近年の標的型攻撃で用いられるマルウエア

従来のように単体動作するのではなく、ダウンローダを介して設置される
シーケンシャルマルウエアが多い



TROJ_MDROPPER系の攻撃シーケンス

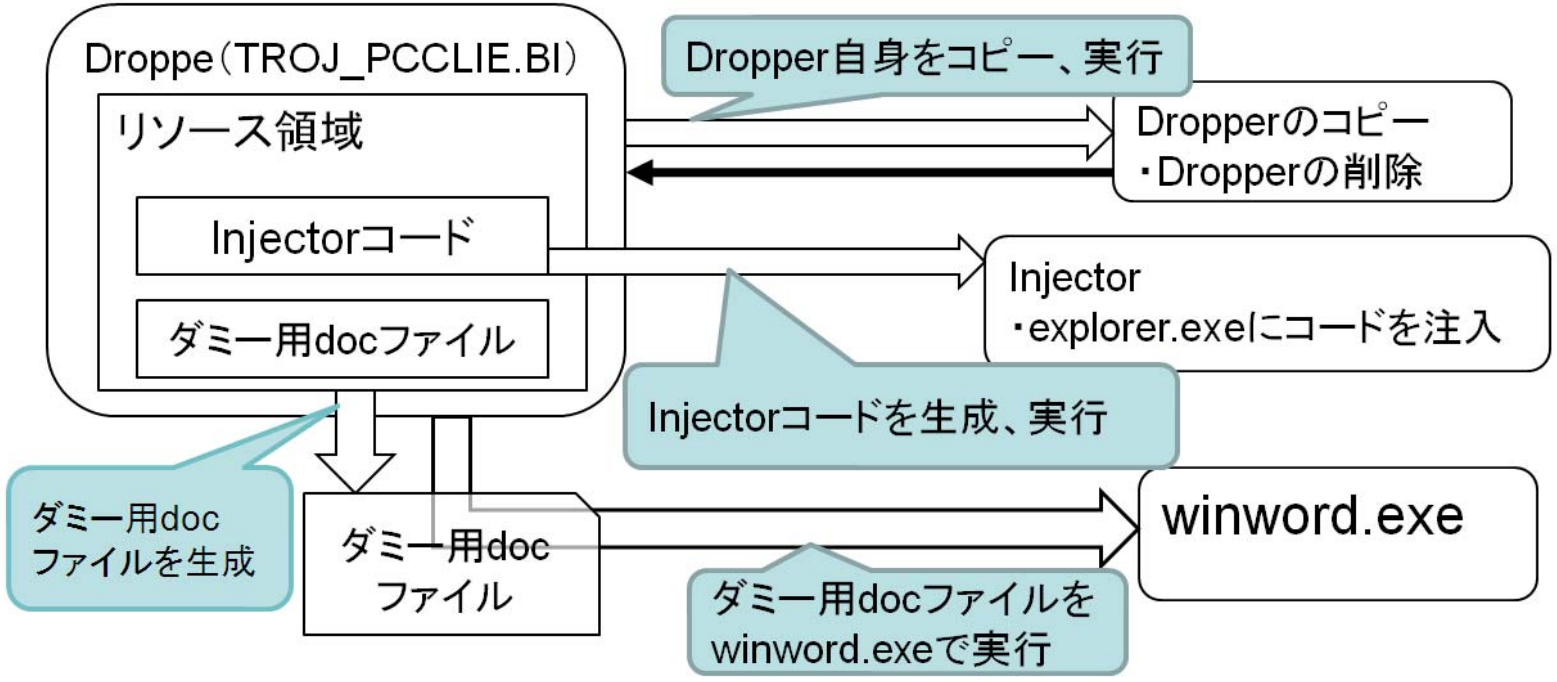


TROJ_PCCLIE系Dropper

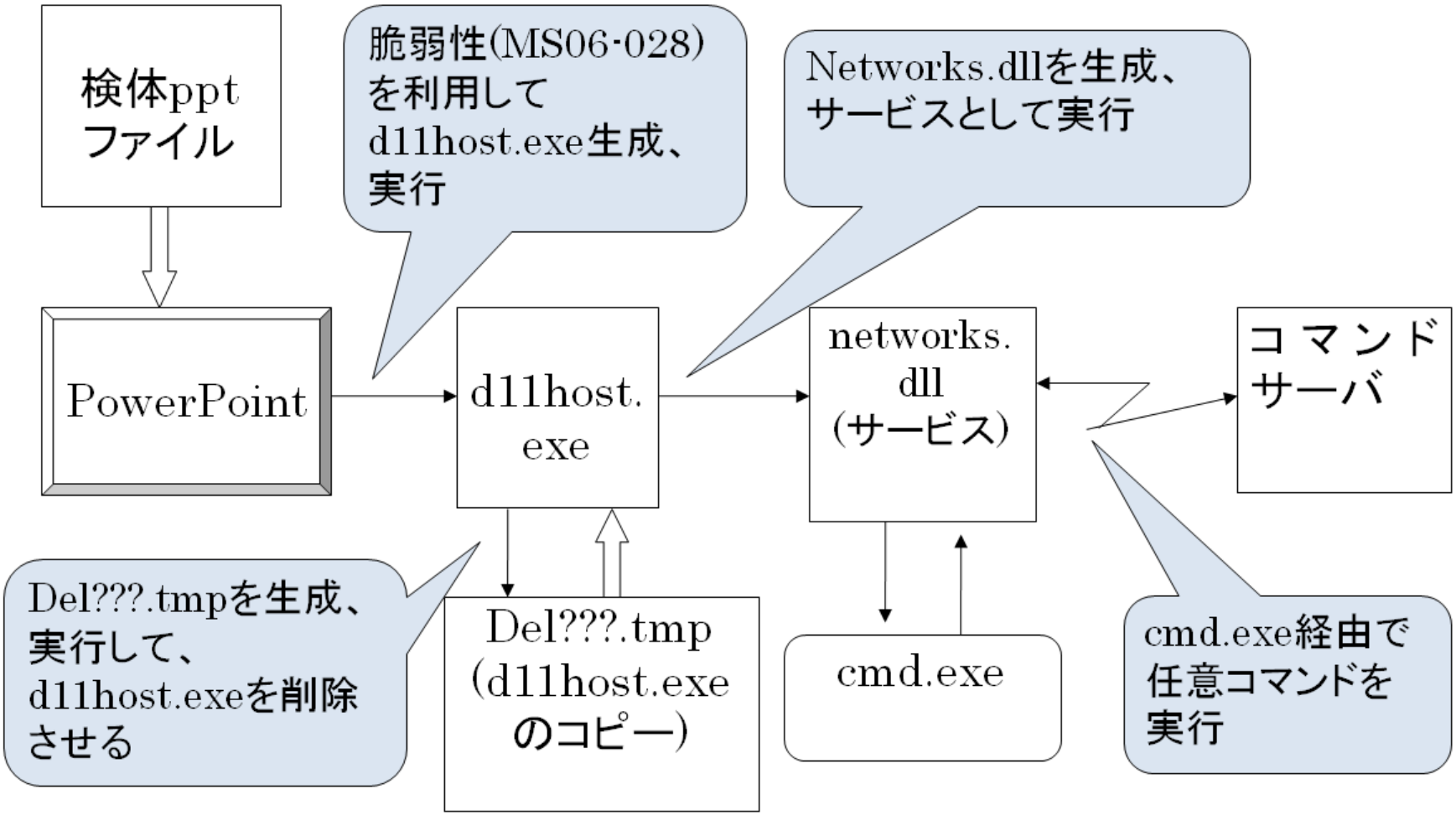
TROJ_MDROPPER系と同じ動作

相違点

- Dropper自身が実行ファイル(Wordの文書ファイルアイコン)
- 2種類の実行ファイルと文書ファイルを生成
  - Injector
  - 自身のコピー



TROJ_PPDROP系の攻撃シーケンス



TROJ_MDROPPER系攻撃サイトの特徴

TCP(Trasmission Control Protocol) のポート80番、および、443番を利用

しかし、

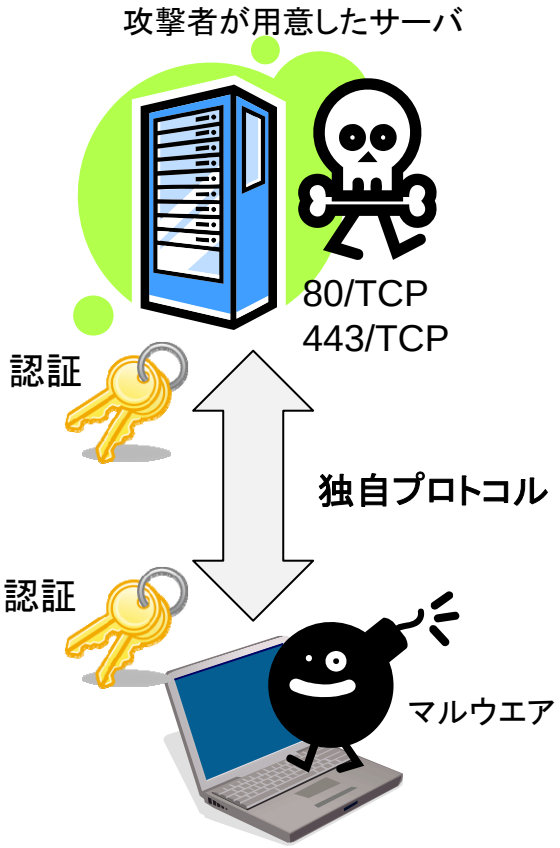
HTTP (Hyper Text Transfer Protocol)
HTTPS (Hyper Text Transfer Protocol over SSL)

のプロトコルに則っていない。全て独自のプロトコル

・攻撃者が用意したサーバ
・ Webサーバではない

さらに、

・ サーバ側、およびクライアント側の両方で認証
・ マルウエアにとって不正な接続を遮断



自動解析による脅威分析の問題点の例

TROJ_MDROPPER系

アンチウイルスベンダーのwebサイトにて以下のように解説

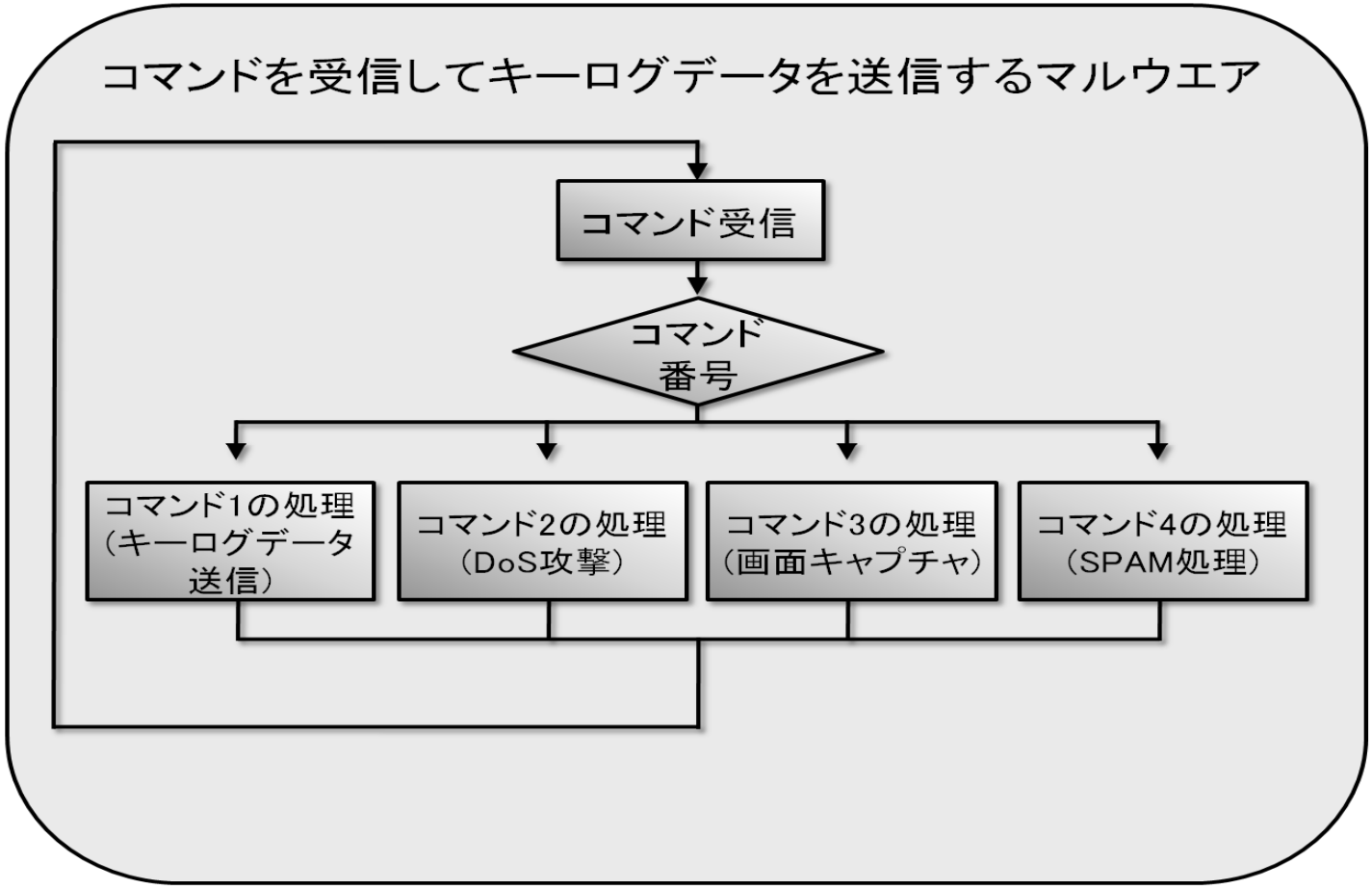
(a) explorer.exeプロセスのメモリに書き込む
(b) iexplorer.exeを起動してバックドアを開く
(c) コマンドを受信し盗み出した情報を送信する

- コマンドを受信するとあるが、実際に受信するのはコマンドではない
- コードそのもの
- ダウンロードしたコードは状況に応じて変化する可能性がある

自動的解析によるアプローチでは、その違いを把握する事が難しい

コマンド受信とコード受信　1

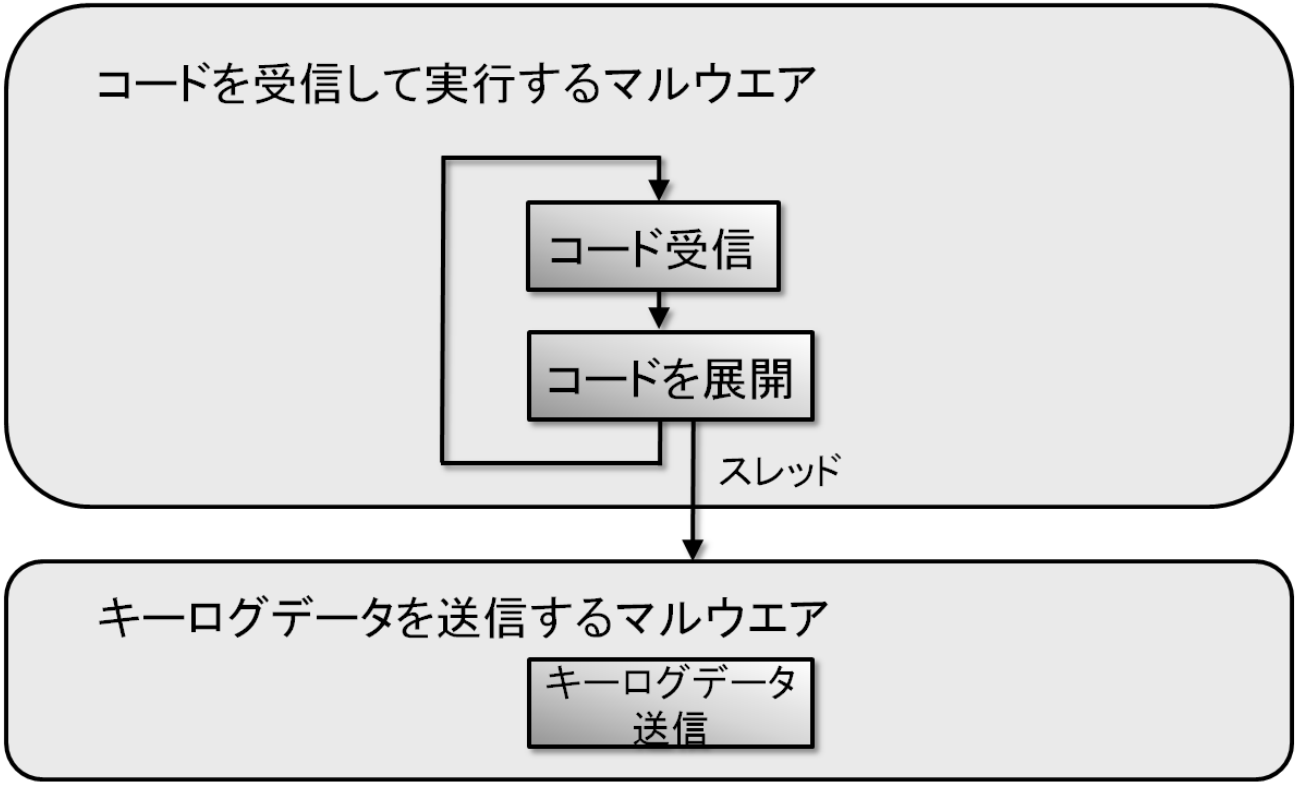
コマンド受信



コマンドで記述されている以上の事は行わない
もし全てのコマンドが自動解析で解析できれば正確に脅威分析できる

コード受信とコマンド受信　2

コード受信



新たにコードがダウンロードされる

何が起こるかは、攻撃者が用意したサーバに置いてある第2のマルウエアの実装による

自動解析では解析時の状況しか分からない

コード受信は第2次マルウエアの攻撃である

検証時は、攻撃者が用意したサーバから2つのコードがダウンロードされた
キーログデータの他に、ホスト情報やユーザー情報などが送信されていた

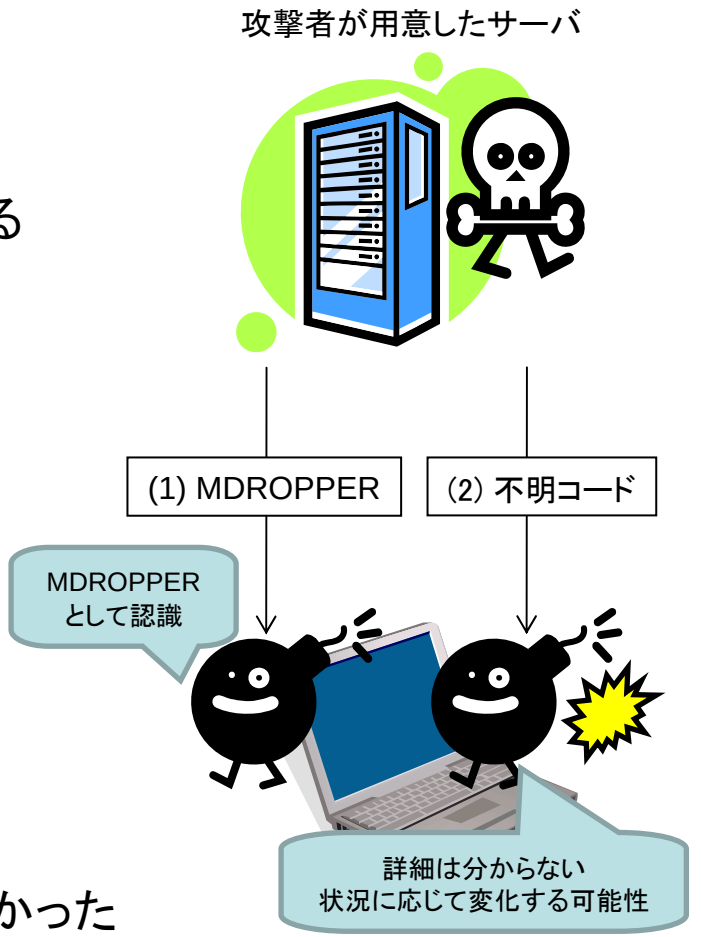
→ パケットは暗号化　**自動解析では検証不可**

そもそも・・・

- ダウンロードした新たなコードが情報を送信している
- これはもはや、MDROPPERによる攻撃ではない
  既に**第2次のマルウエアの攻撃が成立**している

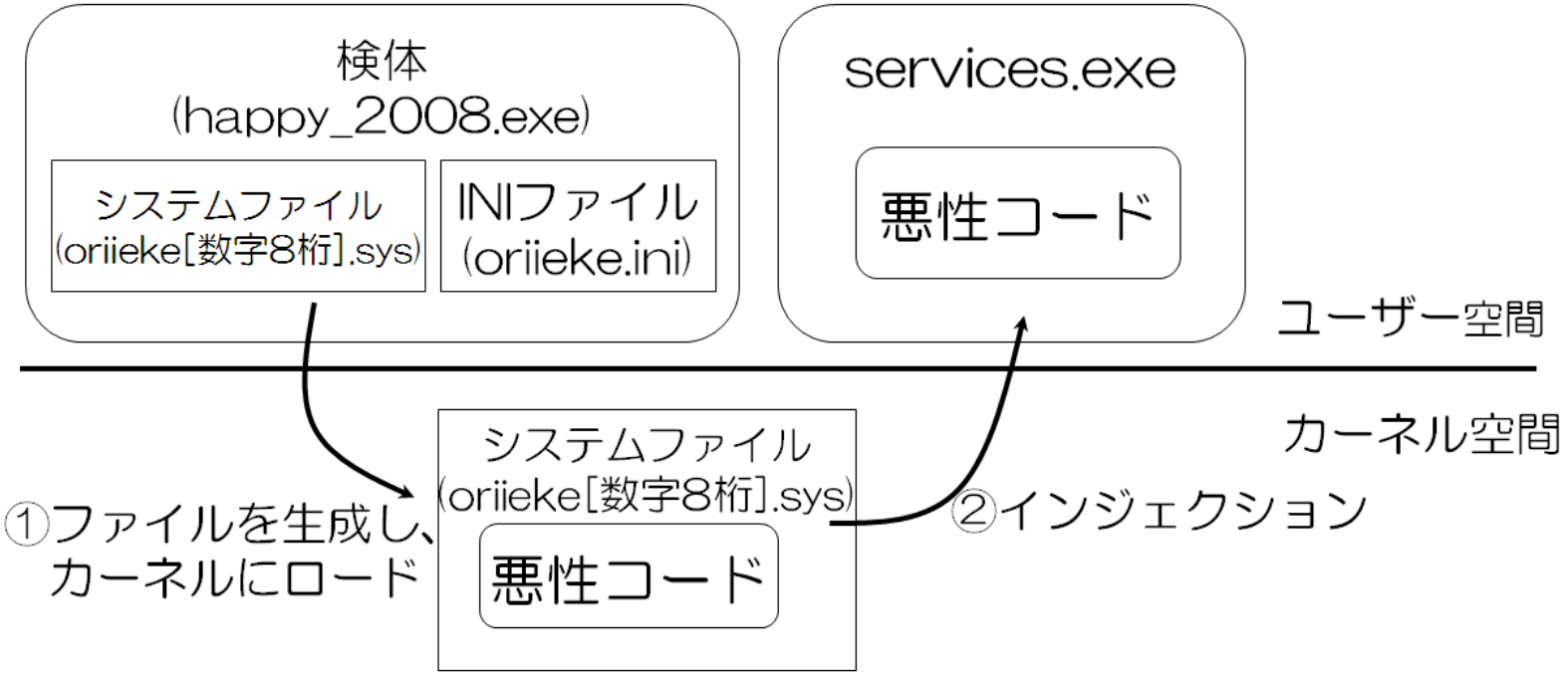
- 何が起こるのかは攻撃者が用意したサーバ上のコード次第
  MDROPPER自体を解析しても分からない
- アンチウイルス情報を元にした脅威分析やインシデント対応は不適切なケースも

キーログ情報だけが盗まれたとは言えないことが分かった



無差別攻撃型マルウエアとの比較

Storm Worm (Peacomm)



コードインジェクションなど基本技術については類似性が多数

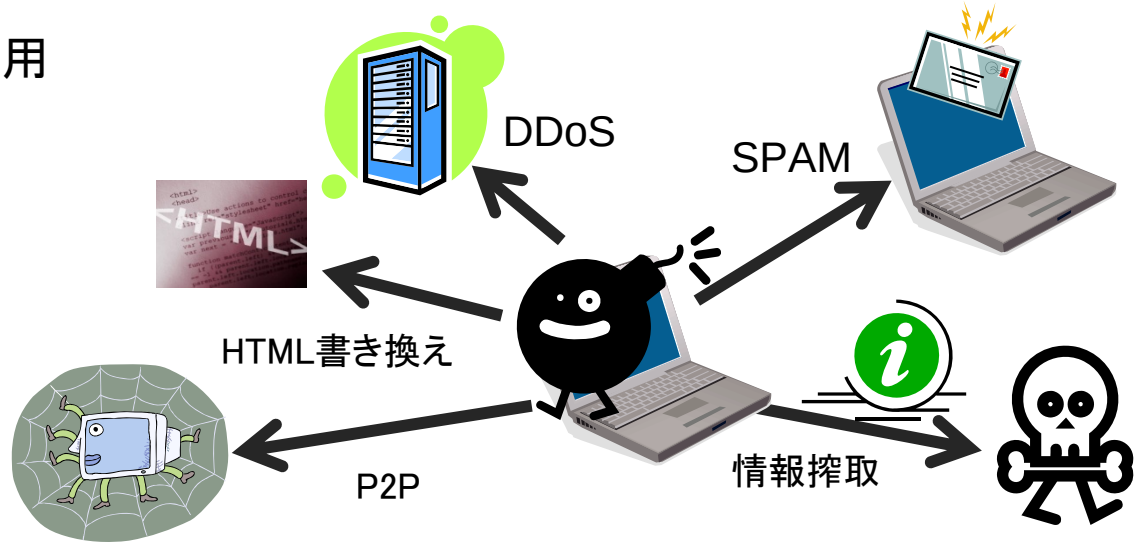
感染事実を極力隠蔽する様々な工夫が施されており、攻撃が非常に見えにくい

アンチフォレンジックやアンチデバッギングなど様々な解析対策が施されている
→ セキュリティベンダーによる対策を遅らせる

無差別型マルウエアと標的型マルウエアの用途

大量無差別型のマルウエア

SPAMなど様々な用途に利用
される事が前提
→「大規模多機能型」



標的型攻撃のマルウエア

目的が情報搾取に特化
→「小規模特定機能型」

効率の良い脅威分析手法

・ファイルシステム内にさまざまなファイルを生成
・ファイルシステムモニタでファイルを捕獲可能
・新たな実行ファイルをダウンロードしてシステムに展開した場合も対応可

ただし、

・インジェクトコードやダウンロードされたオンメモリ動作コードは捕獲できない
・一般的なマルウエア自動解析手法では正確な脅威分析ができない

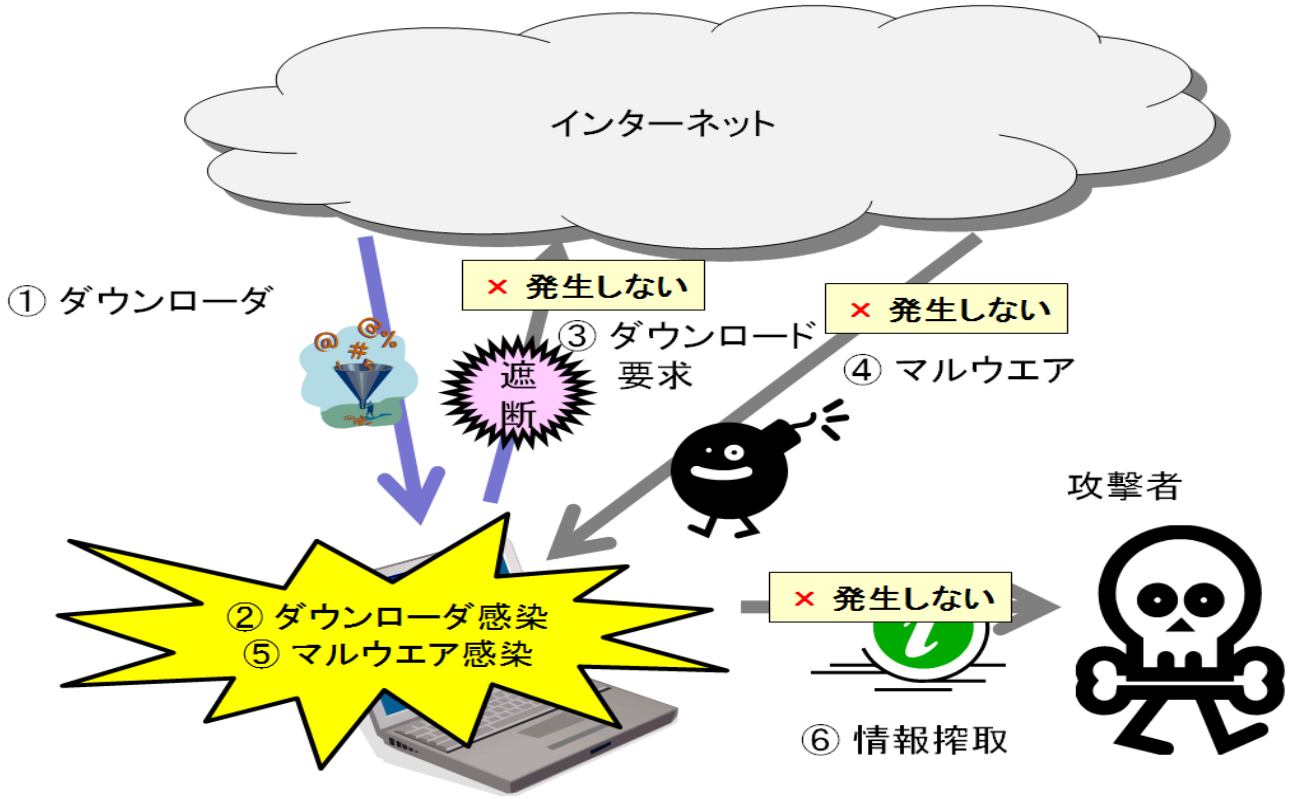
そこで、

APIトレースで攻撃者が用意したサーバからのパケット受信が行われた時点で切り分ける

・それ以前を動的解析、それ以降を静的解析
・効率的かつ正確な脅威分析が可能

標的型攻撃用マルウエアの検知と対策

TROJ_MDROPPER系、PCCLIE系、TROJ_PPDROP系のコードを解析した結果、
それらについては、ダウンロード要求を遮断できれば脅威が発生しない事が分かった



1. **不必要な外向きのTCPポート**を全て閉じる
2. 80/TCP、443/TCPにて**HTTP、HTTPS以外の通信検知**で通信遮断
3. HTTP(80/TCP)、およびHTTPS(443/TCP)は**Proxy経由**のみ

さいごに

さまざまな解析対策や解析を困難にする要素がある

1.多重難読化
2.独自API (Application Program Interface)テーブル
3.多数の無駄コード挿入
4.アンチデバッギング
5.アンチリバースエンジニアリング
6.マルチスレッド
7.圧縮されたコードの展開
8.他プロセスへのインジェクト
9.リモートホストからの部分コード受信と実行

今後の課題

・コードサイズも大きく大半でIDA(HexRay社の高機能ディスアセンブラ)が利用不可
・迅速な解析を行うためには、熟練した解析技術が必要
・解析エンジニアの育成が重要
・解析効率化ツール環境等の基盤整備が必要
・有効な対策分析の為には脅威変化の継続監視が重要