IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2009年2月20日

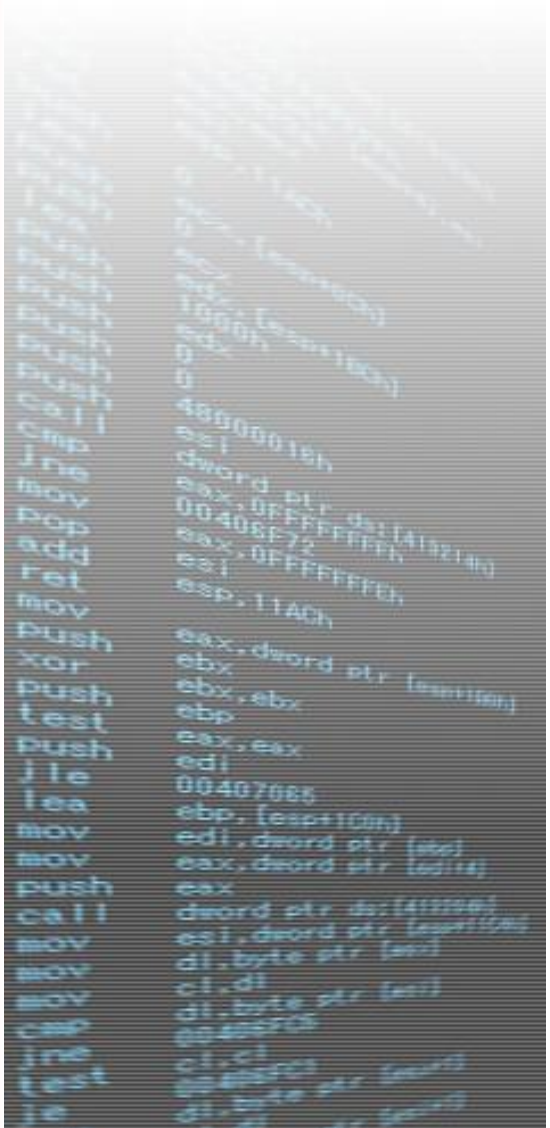
重要インフラがかかえる潜在型攻撃によるリスク

騙しのテクニック「ソーシャル・エンジニアリング」と
セキュリティ脆弱性を巧みに利用した標的型攻撃

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

アジェンダ



- 発表概要
- IPAを語った標的型攻撃の事例
- 本攻撃の手口
- 本攻撃で想定される被害
- 本攻撃の対策
- 攻撃のトレンドと今後
- 脅威対策のためのアプローチ

はじめに

・騙しのテクニック「ソーシャル・エンジニアリング」
・セキュリティ脆弱性

これらを巧みに利用した標的型攻撃が日本国内で次々と発生。

2008年4月、「IPAセキュリティセンター」を騙った標的型攻撃が発生。

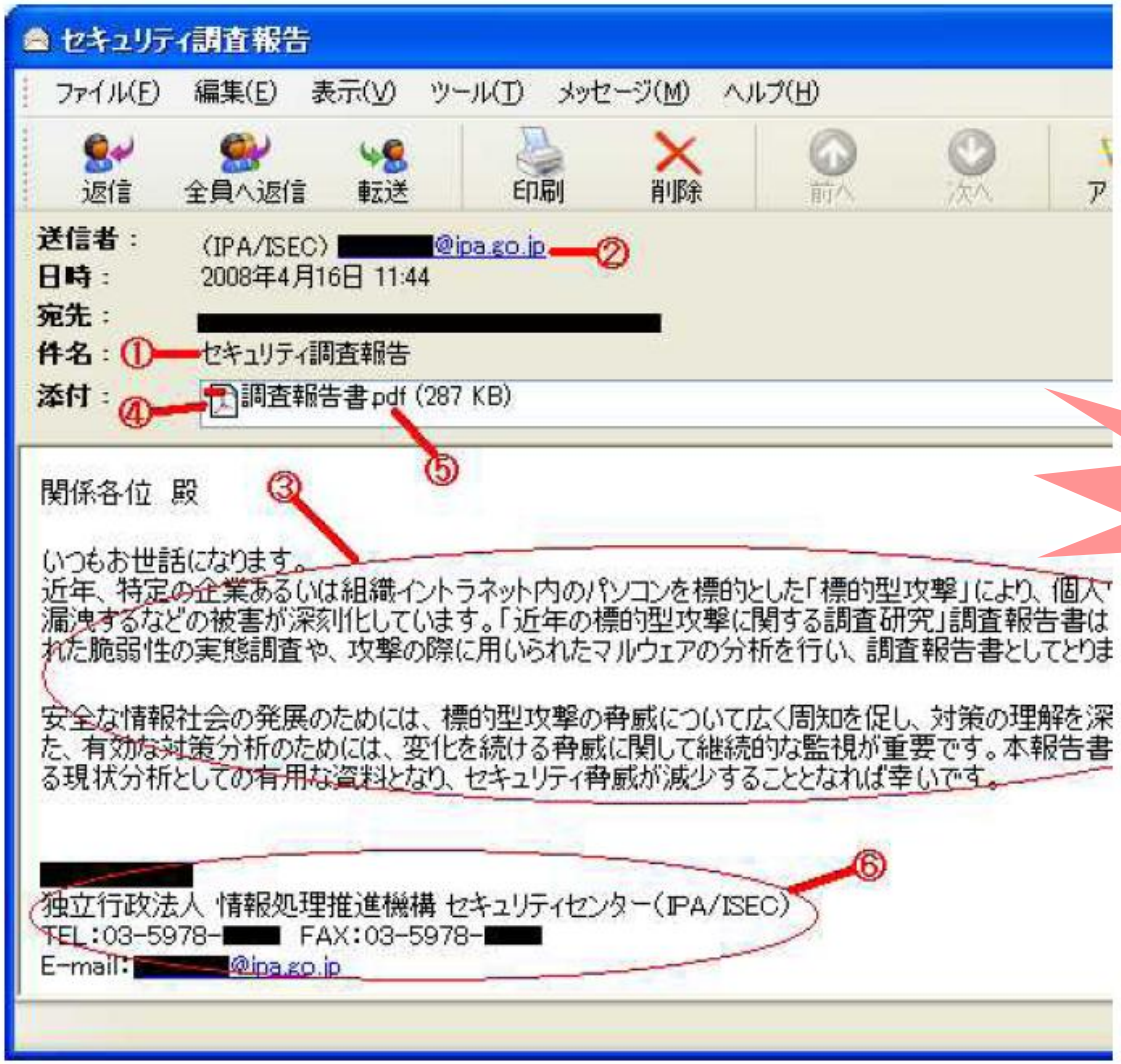
- メール差出人をIPA職員に偽装 → 現実の職員
- メール本文が信憑性のある文章 → ソーシャルエンジニアリング
- 通常危険性が無いPDFファイルが添付

セキュリティ専門家でも攻略されかねない。

近年、攻撃が相次いだ
「ソーシャルエンジニアリング」＋「脆弱性攻略」
による巧妙な標的型攻撃の事例と手口を解説。

「今時」の標的型攻撃への対抗策と、分析技術の現状を解説。

なりすましメール



① メール受信者が興味を持つ件名
② 信頼できそうな組織
③ 件名に関わる本文
④ 本文に合った添付ファイル
⑤ 安全とされる文書ファイル
⑥ ②に対応した署名

IPAを偽装した攻撃

IPAが2008年3月18日に公開した「近年の標的型攻撃に関する調査研究」に関する内容。
添付ファイルは、そのプレスリリース全文にマルウェアを仕掛けたもの。

本攻撃の特徴と傾向

- 当該プレスリリースを公表後、およそ1ヵ月後
- メールの受信者は攻撃の存在を推測することが非常に困難
- 攻撃は、OSの脆弱性を狙ったものからアプリケーションの脆弱性を狙ったものに
- ソーシャル・エンジニアリングを巧みに利用。
  攻撃成功の確度を上げる試み。

類似例

- コンピュータセキュリティシンポジウム（CSS）2008においても確認

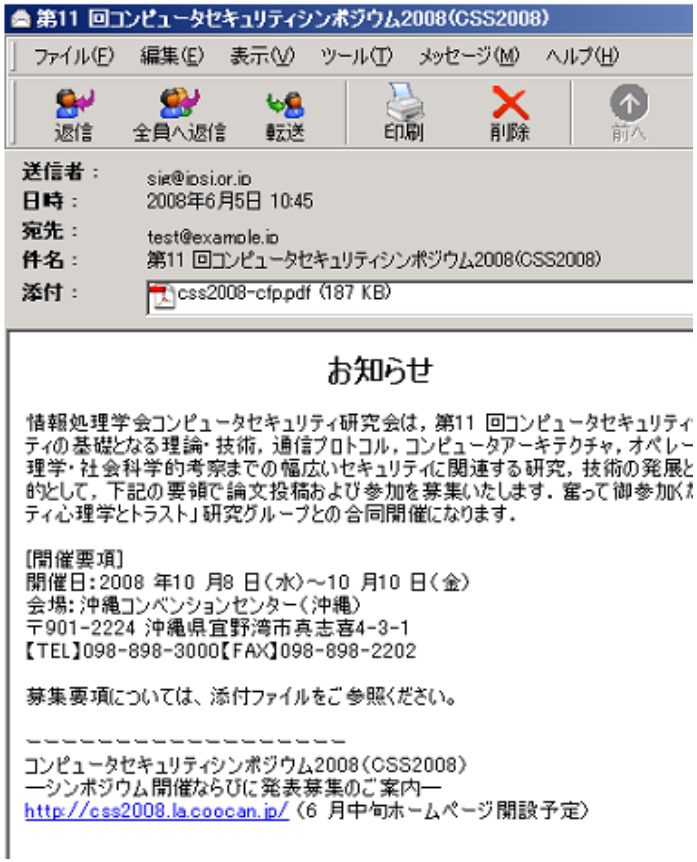
  CSS　：(社)情報処理学会コンピュータセキュリティ研究会主催
  　　コンピュータセキュリティに関する研究会

- CSSからのCFP（論文募集）を装ったメール
  マルウェアが仕掛けられたPDFファイルが添付

- 一貫してCSSからのCFP配布を偽装。
  メールから攻撃を推測することは困難。

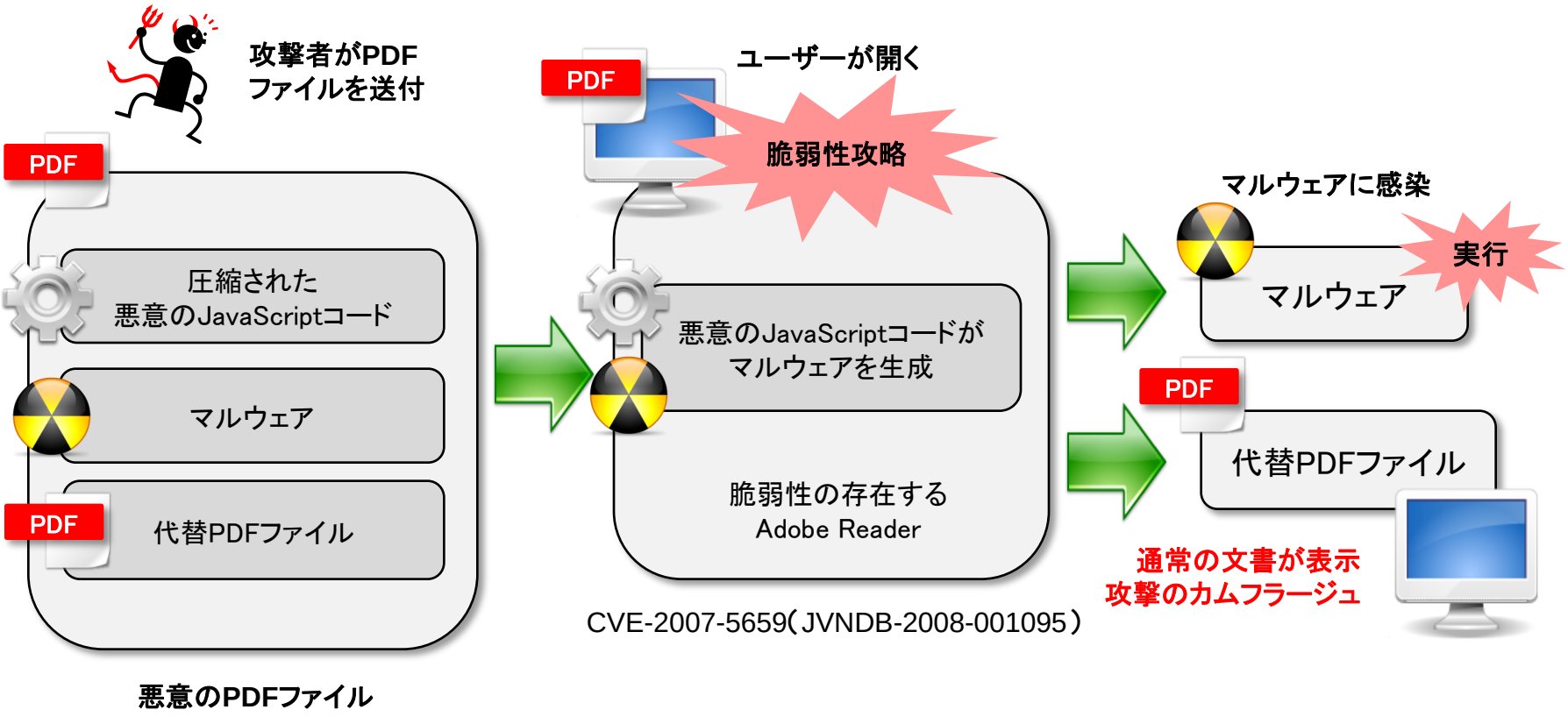
- 攻撃偽装のための一次情報が、
  現実に即している点で共通。

- CSSのWebにてCFPを公開した約16日後に発生



Hitachi Incident Response Team
「CSS2008のCFPを騙ったウイルスメールに関する情報」
http://www.sdl.hitachi.co.jp/csec/css2008-cfp-secinfo.html

攻撃の流れ


攻撃者がPDF
ファイルを送付
PDF
圧縮された
悪意のJavaScriptコード
マルウェア
PDF
代替PDFファイル
悪意のPDFファイル
ユーザーが開く
PDF
脆弱性攻略
悪意のJavaScriptコードが
マルウェアを生成
脆弱性の存在する
Adobe Reader
CVE-2007-5659（JVNDB-2008-001095）
マルウェアに感染
実行
マルウェア
PDF
代替PDFファイル
通常の文書が表示
攻撃のカムフラージュ

マルウエアの動作

・OSのバージョン
・言語ID
・コンピュータ名
・IPアドレス
・gethostbyname(コンピューター名）

・Proxyの設定

HKEY_CURRENT_USER¥¥SOFTWARE¥¥Microsoft¥¥Windows¥¥CurrentVersion¥¥Internet Settings¥

ProxyEnable => 0（無効）/1（有効）
ProxyServer => 1.1.1.1:80

攻撃者用制御サーバーと通信し、コマンドを受信

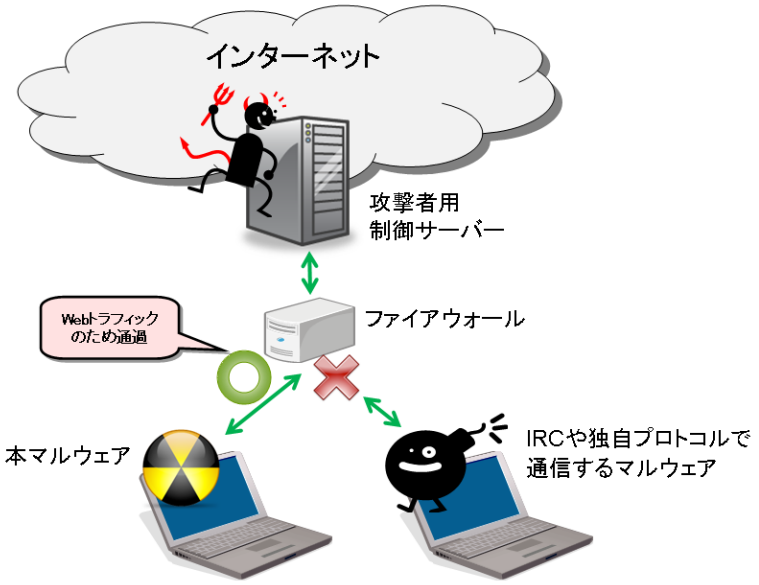
攻撃の特徴 (1)
～ HTTP経由で攻撃者用制御サーバーとの通信

ボットなど従来マルウェアの多くは、IRC（6667/tcp）や、独自プロトコルで通信。

本マルウェアはHTTP（80/tcp）を利用。

内部ネットワークから外部ネットワークに対するHTTPの通信は多くの場合許可。

外向き通信が適切にフィルタリングされていても、本マルウェアの通信はブロック困難。



攻撃の特徴 (2)
～ HTTP Proxyサーバーへの対応

IPAにて2008年3月公開した
「近年の標的型攻撃に関する調査研究」

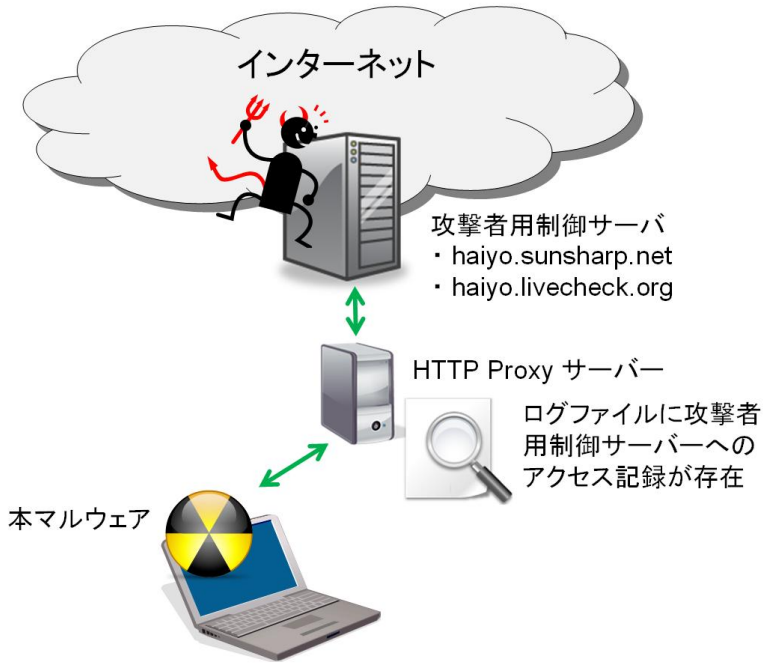
制御サーバーと通信するマルウェアへの対策

→ HTTP Proxyサーバーの導入が有効と報告

しかし本マルウェアは・・・

HTTP Proxyサーバーが利用されていた場合、
それを利用して攻撃者用制御サーバーと通信。

HTTP Proxyサーバーで脅威低減は困難。



想定される被害

攻撃者用制御サーバーから受信したコマンドに応じて以下の処理を実行。

- **任意のプログラムの実行**
  攻撃者用制御サーバーから指定された任意のプログラムを実行。
  結果を攻撃者用制御サーバーに送信。
- **ファイルの一覧取得**
  ファイルの一覧を取得。結果を攻撃者用制御サーバーに送信。
- **ファイルの送受信**
  指定されたファイルを攻撃者用制御サーバーに送信。
  攻撃者用制御サーバーから送信されたファイルを受信。
- **任意のファイルの削除**
  指定された任意のファイルを削除。

プログラム実行が可能であるため、二次マルウエア感染などあらゆる攻撃が可能。

エンドユーザー向けの対策

- **最新版ソフトウェアの利用**

  攻撃に利用されているAdobe Readerの脆弱性は、2008年2月に報告されたもの。
  ベンダーは既に修正バージョンを公開。
  ソフトウェアを最新版にアップデート。

  http://get.adobe.com/jp/reader/

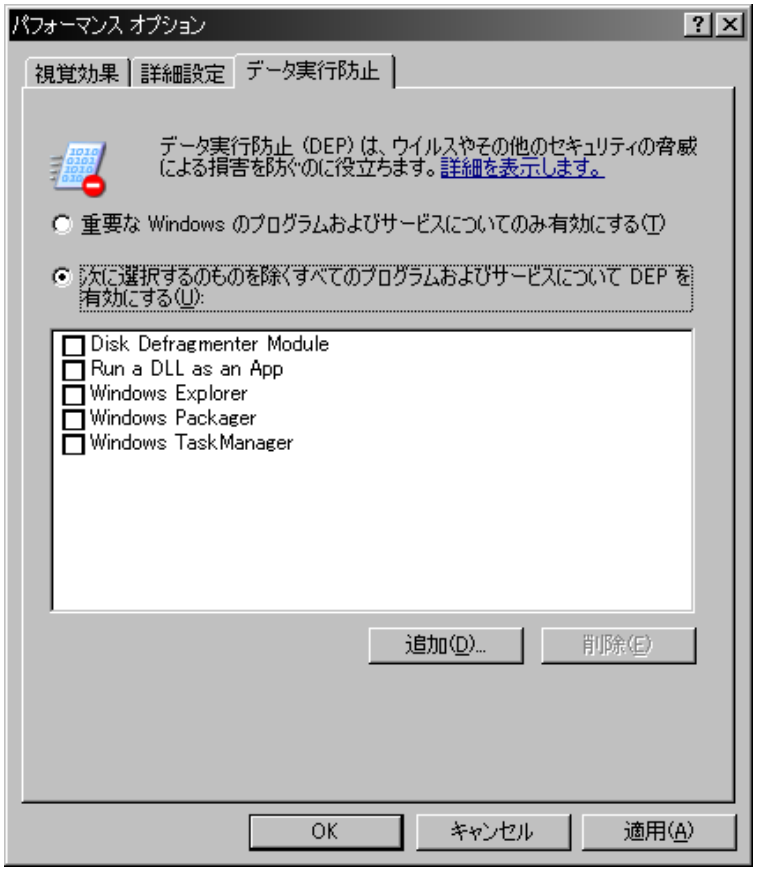
- **ハードウェアDEPの利用**

  Microsoft Windows XP SP2以降では、
  ハードウェアDEP (Data Execution Prevention)
  と呼ばれるセキュリティ機構がOSに搭載。

  OS、およびプロセッサの両方がこれに対応
  している必要がある。

  ハードウェアDEPを利用することで、本攻撃など
  メモリ破壊起因の脆弱性攻撃の多くを防止可能。

  http://support.microsoft.com/kb/884515/ja

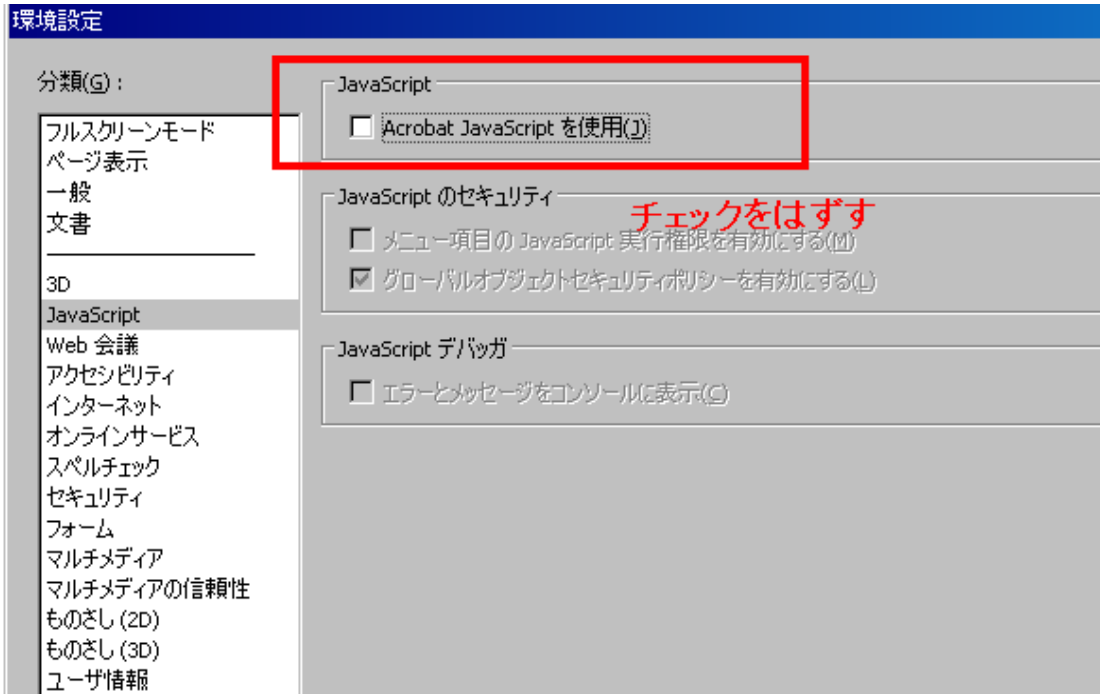


エンドユーザー向けの対策 – つづき

- **不要な機能の無効化**

本攻撃は、Adobe ReaderのJavaScriptエンジンに実装されている特定関数の脆弱性を利用。

Adobe ReaderにおいてJavaScriptサポートが不要の場合は機能を無効化。



システム管理者向けの対策

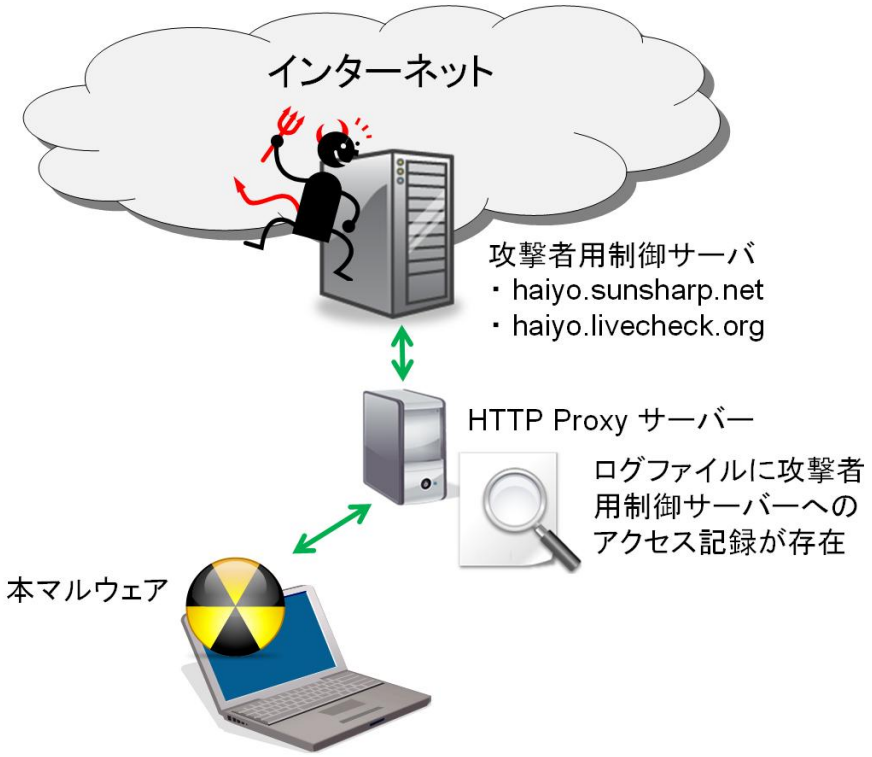
・HTTP Proxyサーバーのログの確認。

下記のドメイン名を持つ攻撃者用制御サーバーと通信。

haiyo.sunsharp.net
haiyo.livecheck.org

HTTP Proxyサーバーのログを確認。

自組織内のマルウェア感染端末を確認。



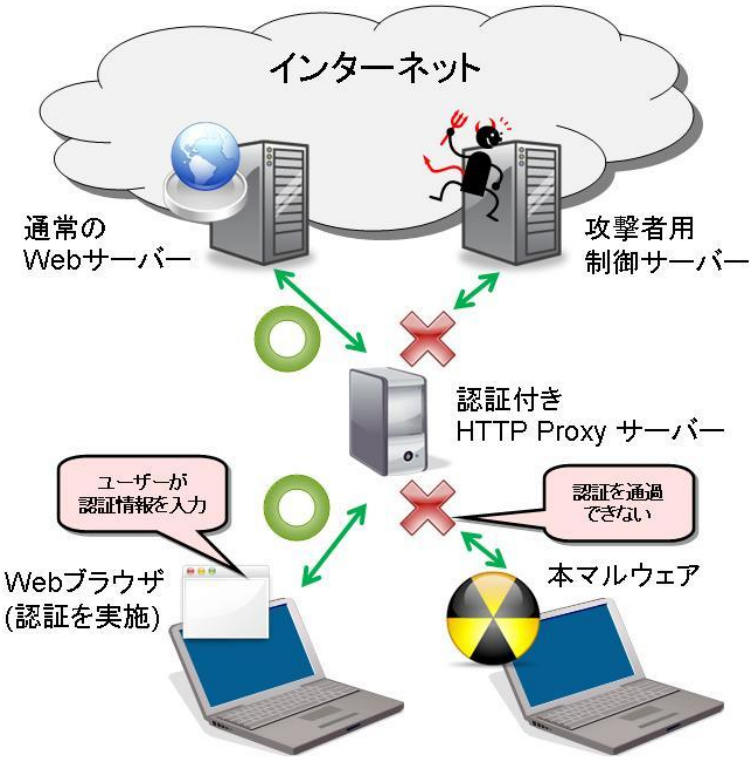
システム管理者向けの対策 – つづき

・**認証付きHTTP Proxyサーバーの導入**

本マルウェアと攻撃者用制御サーバーの通信をブロック可能。

一般的には、認証付きHTTP Proxyによる
対策を回避することも技術的には可能。

過信は禁物 !!



攻撃のトレンドと今後

今回のIPAを騙った攻撃：

「ソーシャルエンジニアリング」＋「脆弱性攻略」

既知の脆弱性攻略であったため、意識の高いパッチ適用者は攻撃を免れた。
しかし、未知脆弱性を利用したケースも既に存在。

→ 2006年8月、一太郎の0-day脆弱性を利用した攻撃発生が報道されている。
（Symantec社の発表。ただし、出所や攻撃手法の詳細は不明）

「ソーシャルエンジニアリング」＋「未知脆弱性攻略」

もはやセキュリティ専門家でも防御困難
深刻な脅威トレンド

対策手法の研究が望まれる

脅威対策のためのアプローチ

近年の攻撃の解析を継続。
手口を詳細に把握し、ノウハウを蓄積。

本質的な対策手法の研究

しかし・・・

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

－ 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

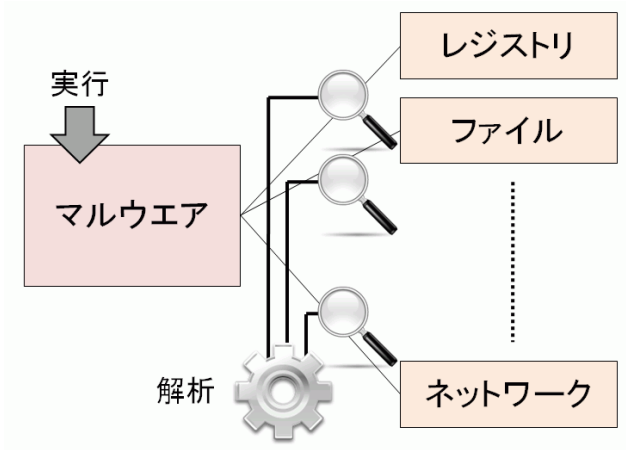
近年の標的型攻撃、マルウエアは、解析が非常に困難

マルウエア解析手法

動的解析

プログラムの挙動に着目。実際に実行し、ファイルアクセスや通信等を監視。

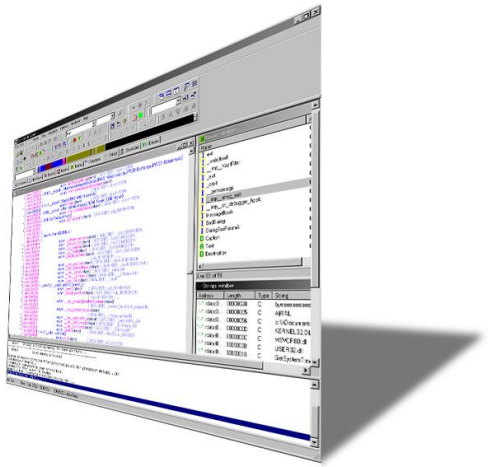
挙動を容易に把握できるが、仕様や実行されていない処理の解析が困難。



静的解析

プログラムの構造、および仕様に着目。逆アセンブルし1命令ずつ解析。プログラムの仕様を完全に把握。

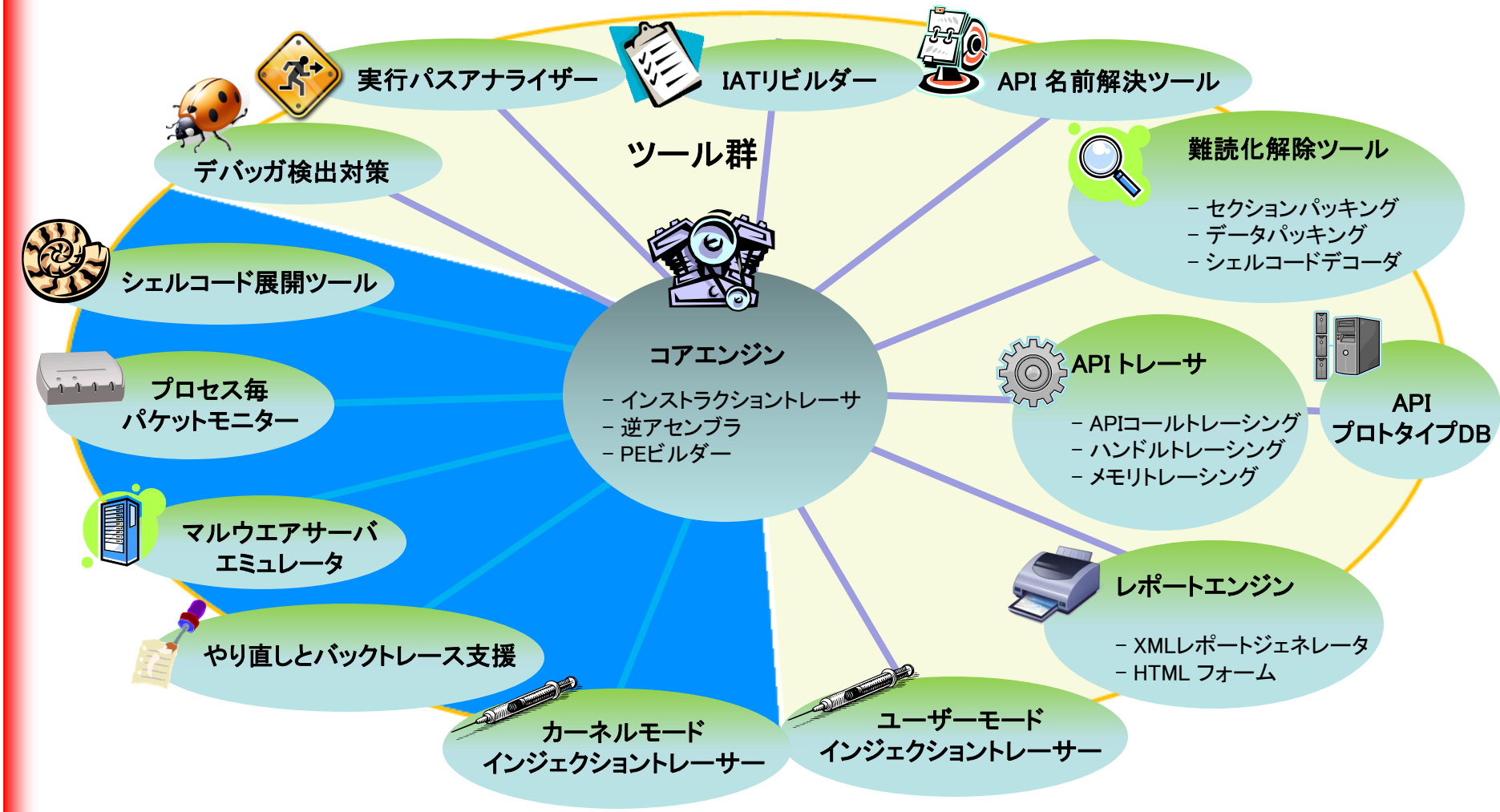
全容を正確に分析することができるが、熟練技術と時間が必要。



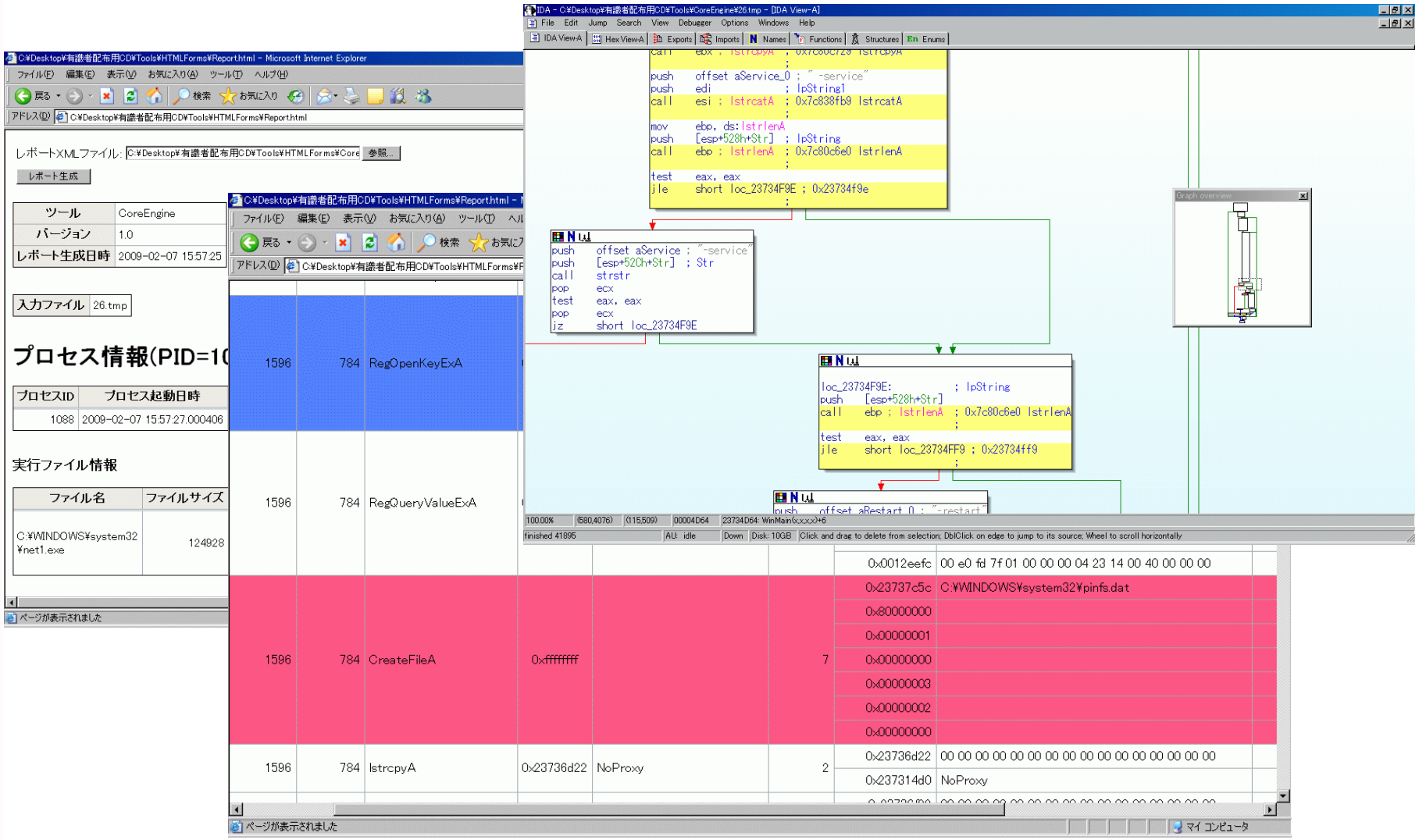
近年の攻撃では・・・

動的解析と静的解析に対して解析を困難にするための様々な耐解析機能を有す

IPAでは、脆弱性を利用した標的型攻撃のための解析ツールを開発



セキュリティ研究者、IT管理者に有用な情報を出力



さまざまな対解析技術を回避。多くのケースで分析が正確・簡単・迅速に。

さいごに

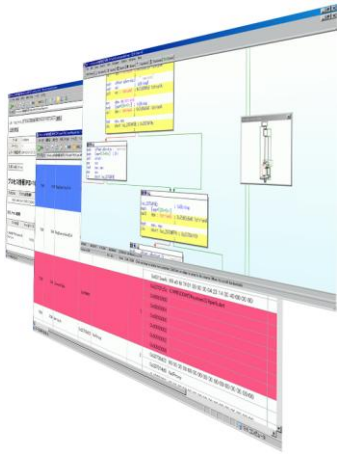
・監視・調査・分析の継続

今後の新たな脅威についても調査・分析を継続して実施。対策を発表。

IPAでは、「不審メール110番」相談窓口を設置している。
http://www.ipa.go.jp/security/virus/fushin110.html

・「脆弱性を利用した標的型攻撃のための解析ツール」をリリース

・近年の脅威に対する解析基盤の整備
・セキュリティ研究者にとって有用な情報の発信
・対策手法に関する研究成果の発表



新たな脅威に対して、多方面から対策を推進する。