

情報セキュリティ特論

第4回

第4回：不正プログラム対策

今回の目標

- ・不正プログラム対策の理解



1. 不正プログラム対策

「不正プログラム」

通常の動作・期待される機能でなく、**悪意を持った動作**をするプログラム

「悪意のある」という意味の“malicious”という単語から、
一般には「**マルウェア(malware)**」と呼ばれる



昔は「コンピュータウィルス」または単に「ウィルス」と呼ばれていたが、現在ではスパイウェアやランサムウェア等、いろいろなものが出てきたので「マルウェア」と読んでいる。

不正プログラムの種類

- ・ ウィルス：通常のソフトウェアに「感染」する形で侵入するもの
- ・ ワーム：「感染」を必要とせず、単体で動作するもの
- ・ トロイの木馬：有益なソフトに見せかけて侵入するもの
- ・ スパイウェア：侵入したコンピュータの情報を盗むもの
- ・ アドウェア：広告を勝手に表示するもの
- ・ ルートキット：コンピュータの管理者権限を利用して改竄等を行うもの
- ・ ランサムウェア：コンピュータ内の情報を「人質」にして金銭を要求するもの
- ・ ボット：外部から標的を攻撃するもの



不正プログラムの目的

昔はどちらかと言えばコンピュータ内の情報を破壊するものが主流



ウィルス

ハードディスクの初期化
ソフトウェアの改竄



「情報」はお金になる



コンピュータ内の情報を盗む、情報をお金にする



スパイウェア
トロイの木馬

ランサムウェア



代表的なランサムウェア

“WannaCry”（ワナクライ） “泣きたい”

2017年ごろに世界中で猛威を振るったランサムウェア

コンピュータ上のファイルを勝手に暗号化し、
身代金としてビットコインを要求した

（現金だと「足がつく」ので）

世界中の企業・個人が被害にあった



身代金要求の画面

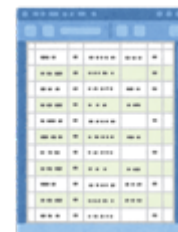
脆弱性と感染源

OSやソフトウェアの不備について、感染を行う

脆弱性

感染ルートは多岐にわたる

- ・メールの添付ファイル
- ・Excelのマクロ
- ・USBメモリ
- ・ブラウザのリンク、ダウンロード
- ・ネットワークを通じて外部から



脆弱性を排除するには

※原理的には、コンピュータ内の全てのプログラム・ライブラリ等が完璧であれば脆弱性は発生しない。

→ もちろん、そんなのは無理な話である

「どのくらい脆弱性があるか」は検疫ソフトウェア等の脆弱性診断を用いることでわかる

が、一般的にはお高い



アンチウィルスソフト

通常、マルウェア対策にはアンチウィルスソフトを使う

「アンチウィルス」だとウィルスにしか対応していないみたいなので、最近では「エンドポイントプロテクション（末端保護）」や「**エンドポイントセキュリティ**」と呼ぶ

- ・ パターンマッチング
- ・ 振る舞い検知
- ・ 動作制御

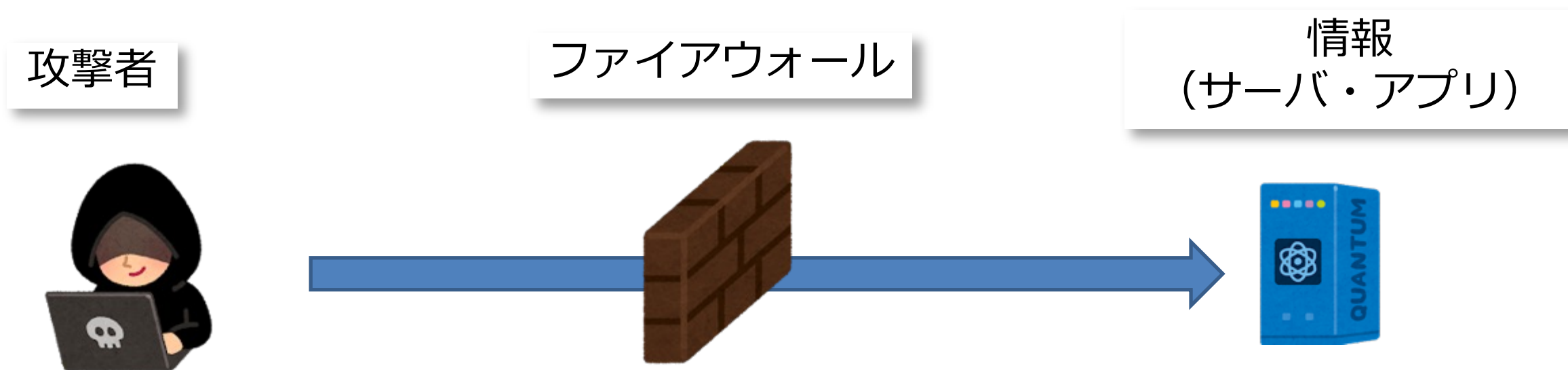


膨大なデータをAI処理することで、より検知精度を上げている

ファイアウォール

特定の通信内容、特定のIPアドレス以外を遮断する

(前回のネットワークのところでも述べた)



通常はコンピュータ (PC) 自体にもファイアウォールが入っている

さまざまな防止策

- ・ 不正侵入検知システム (IDS: Intrusion Detection System)
- ・ 侵入阻止システム (IPS: Intrusion Prevention System)
- ・ 検疫システム
 - ネットワークに接続された端末が安全かを見張るシステム
- ・ アプリケーションファイアウォール (WAF: Web Application Firewall)

Webサーバの脆弱性をカバーするように動作するファイアウォール

防御の限界

永遠のイタチごっこ

攻撃者



攻撃



情報
(サーバ・アプリ)



防御の限界

永遠のイタチごっこ

攻撃者



情報
(サーバ・アプリ)



対策

防御の限界

永遠のイタチごっこ

攻撃者



攻撃



情報
(サーバ・アプリ)



防御の限界

永遠のイタチごっこ

攻撃者



情報
(サーバ・アプリ)



対策

防御の限界

永遠のイタチごっこ

攻撃者



攻撃



情報
(サーバ・アプリ)



防御の限界

永遠のイタチごっこ

攻撃者



情報
(サーバ・アプリ)



対策

別の方法

1. システムの固定化

コンピュータのシステムファイルが変更できないようにする

- ・再起動時に初期化
- ・固定イメージから起動し、イメージを書き換えさせない

情報端末室のPCはこの方法

2. システムのバックアップ

改竄された場合に備えてバックアップしておく