情報セキュリティ

第4回： コンピュータウイルスについて

授業計画

① ガイダンス
② インターネット上の脅威について
③ 攻撃について
④コンピュータウイルス（マルウェア）について
⑤ 小テスト，ネットワーク上の各種攻撃の紹介
⑥ 攻撃の技術
⑦ 情報・ネットワーク技術の基礎
⑧ ネットワークセキュリティに関する技術と方法
⑨ 暗号の基礎
⑩ 小テスト，セキュリティ技術と方法に対する確認
⑪ 対処法１（システムリスク）
⑫ 対処法２（ソーシャルリスク：SNS）
⑬ 対処法３（ソーシャルリスク：インターネット・スマホゲーム）
⑭ 対処法に関する小テスト
⑮ 全体のまとめ

本日の講義内容

1. マルウェアの感染経路と感染原因
2. マルウェアに感染するとどうなるのか？
3. マルウェアの分類
4. マルウェアの検知方法
5. 個人レベルでのマルウェア対策

1. マルウェアの感染原因と感染方法

1.1 マルウェアの感染経路

(1) ファイルのオープンによる感染

- メールの添付ファイルやWebサイトからダウンロードしたファイルにウイルスが潜んでいる場合，ユーザがファイルを開く（クリックする）と，ウイルスプログラムが起動され，ウイルスが活動を開始して感染します．
- USBメモリやSDカードなど外部記憶媒体の中にウイルスが潜んでいることもあります．例えば，Windows OSのオートラン機能を悪用し，任意のプログラム（マルウェア）を実行します．
- ファイルに関して巧妙な手口が使われていることもあります．
  例：二重拡張子やアイコンの偽装，ユーザが自分に関係あると錯覚するようなメールへの添付ファイル，公的機関を装ったメールの添付ファイル．

- スマートフォンのアプリケーションとしてマルウェアをアプリケーションマーケットや他のWebサイト等で配布します．正規のアプリケーションに悪意のあるプロフラムを挿入し再パッケージしたもの，もしくは一般のアプリケーションのように装ったものを，マーケット等で配布する方法が用いられます．
- P2Pファイルのコンテンツとして密かにマルウェアをアップロードしP2Pネットワークに流通させ，ユーザの興味を引くようなファイル名を付けることで，ユーザに誤って実行させマルウェアに感染させます．また，感染したホスト上の情報を窃取して自身とともにP2Pネットワーク上に再度アップロードする自己拡散機能を保有しています．

（2）Webページの閲覧による感染（メールによる誘導を含む）

- 攻撃者が仕掛けた特定のWebページを見るだけでマルウェアに感染します．
- 正規のWebサイトが改ざんされてマルウェアが仕込まれ，そのWebサイトを見ると，マルウェアに感染します．

（3）ネットワークへの接続による感染

- ウイルスは，ネットワークにつながっているコンピュータに対して，特殊なメッセージを発信し（ポートスキャン等），OSや他ソフトの脆弱性のあるコンピュータを探します．脆弱性のあるコンピュータを発見すると，ウイルスファイルを送り込みます．
- ウイルスは，パスワードの設定が甘いネットワーク上の共有フォルダに対し，パスワードを破って共有フォルダにアクセスし，ウイルスファイルを自動的に書き込みます．

1.2 マルウェアの感染原因

(1) ユーザの誤操作による感染

以下のファイルを誤って自ら実行，もしくはインストールすることで感染します．

- メールの添付ファイル
- Web上のコンテンツ
- P2Pアプリケーションのファイル
- スマートフォンアプリ　等

これはユーザを騙す手法を用いて行われるため，セキュリティに関して十分な知識を保有しない個人が感染することが多いです．

（2）プログラム脆弱性による感染

OSやアプリケーションなどのプログラムに含まれる脆弱性を標的とした攻撃を受け，制御を奪われた後に強制的にマルウェアのインストールが実行されることで感染します．

プログラムに脆弱性が存在した場合は，開発ベンダがセキュリティパッチを配布しますが，そのセキュリティパッチが適用される前や，セキュリティパッチが適用されないままプログラムが利用された場合，このようなマルウェア感染が容易に発生します．

プログラムの開発段階で脆弱性の混入を防ぐプログラムの検査・テスト手法などが講じられていても，脆弱性の完全な排除は困難です．

- 脆弱性のあるプログラム例１： バッファオーバフロー

buf.c

```
main() {
        char a[10]="", b[10]=""
            gets(a);  /* キーボードから文字をaへ読み込む */
            printf("a=%s¥n", a);
            printf("b=%s¥n", b);
}
```

正しい入力

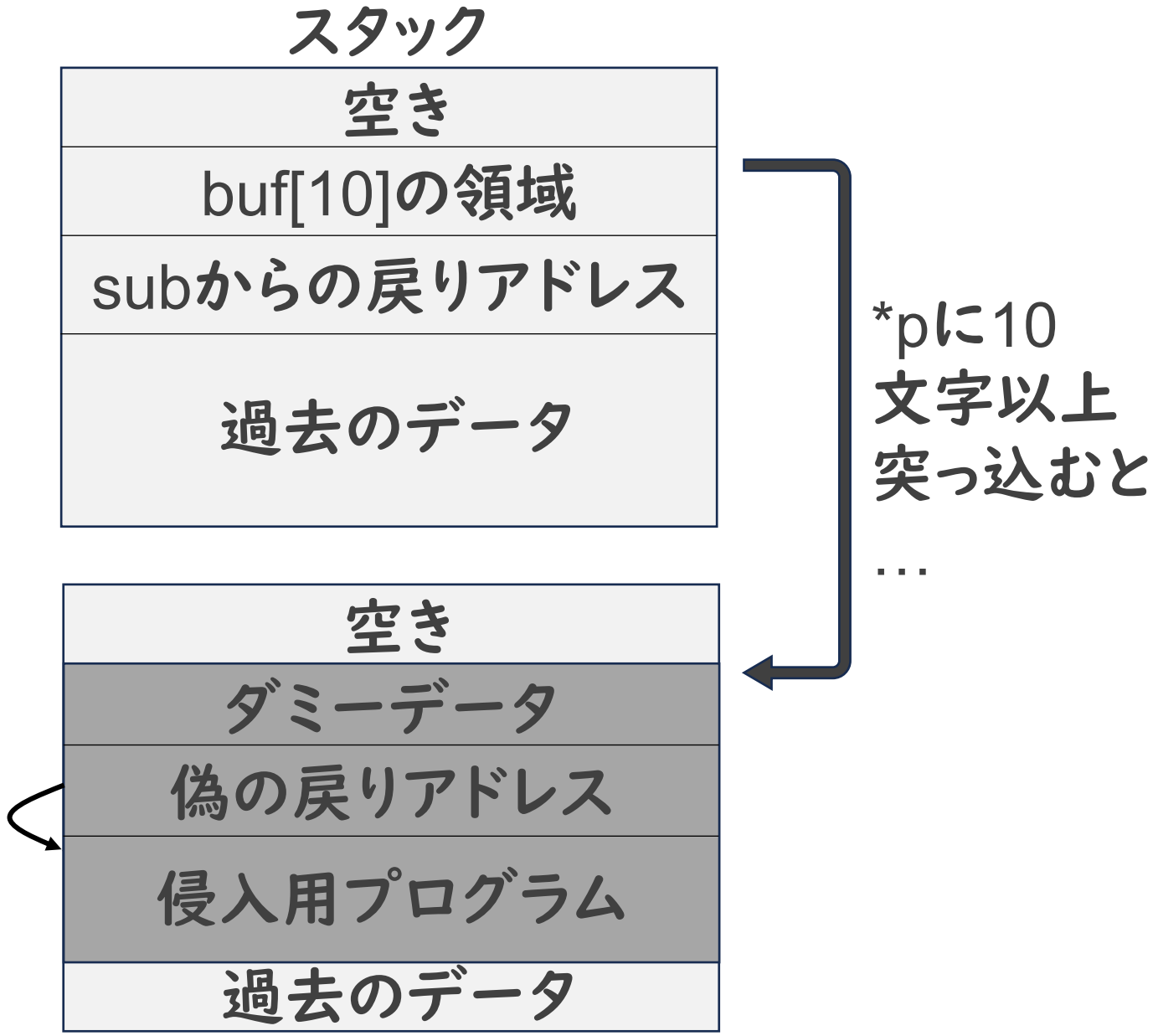
```
./buf
HELLO
a = HELLO
b =
```

不正な入力

```
./buf
HELLO123456789
a = HELLO123456789
b = 89    ← 入力されていないのに!!
```

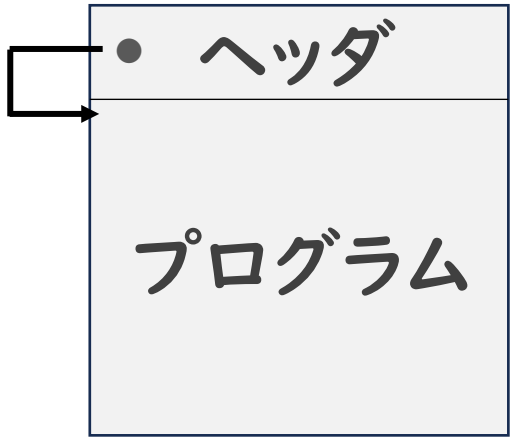
- 脆弱性のあるプログラム例2：スタックオーバフロー

```
void sub()
{
    char buf[10];
    …
    strcpy(buf, p);
    …
    return;
}
```

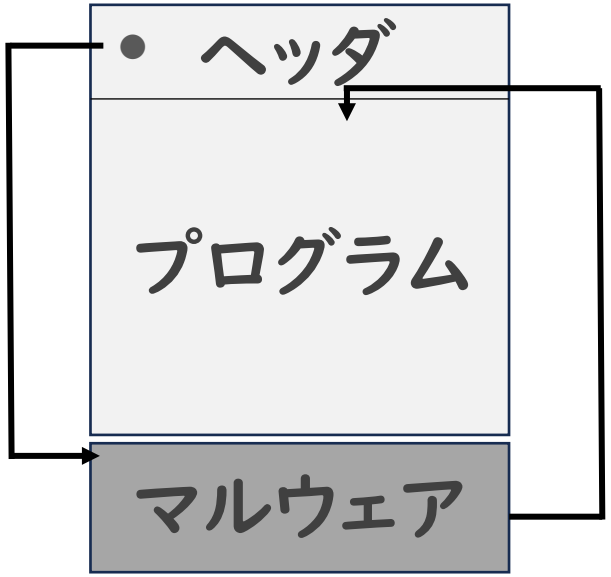


- 実行型プログラムにおける感染の仕組み

  実行型プログラムの先頭にデータ領域と命令領域の先頭アドレスなどを指定したヘッダがあります．マルウェアはそこをマルウェアの開始アドレスに置き換えます．マルウェアの実行後で，本来のプログラムへ制御を戻して感染したことに気付かれないようにします．



COM,EXE
等実行型
プログラム



感染後

2. マルウェアに感染するとどうなるのか？

マルウェアに感染するとさまざまな被害を受けてしまいます．

（1）情報漏えい

組織や個人の情報を窃取されます．

（2）悪意のあるサイトへの誘導やマルウェアのダウンロード

一旦あるマルウェアに感染すると，このマルウェアは，感染したコンピュータからインターネットにアクセスして，別のマルウェアを次々にダウンロードします．

また，ブラウザを乗っ取って悪意のあるサイトに誘導したり，意図しない検索結果を表示させたりします（スパイウェア）．

（3）金銭要求

コンピュータ内にある文書や画像などのファイルを暗号化し，使用できない状態します．そして，暗号化を解除するためには，身代金の支払いが必要です．また，コンピュータが起動しなくなったり遠隔操作されたりすることもあります．（ランサムウェア）．

（4）他ホストへの攻撃の踏み台になる

感染したコンピュータを踏み台にして，DDoS攻撃を行います．（ボット）同一のボットに感染したコンピュータ群は，攻撃者の指定サーバを中心としてネットワークを組み，いっせいに動作し，数千～数十万に達することで，ターゲットに集中攻撃します．

3. マルウェアの分類

（1）ウイルス

他のファイルやプログラムに自身を寄生させるもの. 寄生するファイルやプログラムを必要とし, 単体では動作しません. コンピュータに侵入してユーザが望まないあらゆる悪事を行います.

（2）ワーム

寄生せずに単独のファイルとして存在します. 自身に感染活動の機能が備わっているもので, 単体で動作し増殖します. ネットワークを這い回り, 脆弱性のあるマシンに侵入することからワーム（worm）と名付けられました.

（3）トロイの木馬

トロイの木馬は，便利なソフトウェアにみせかけて，正規のプログラムを装い標的のホストにインストールおよび実行され，ユーザに気付かれないように悪意のある動作を行います．例えば，グリーティングカードを装い，クリックすると花火の画像を表示します．花火の画像が見えたところで，すでにマルウェアに感染しています．

（4）スパイウェア

標的ホスト上でユーザに気付かれないように動作し，ホスト上の個人情報や行動履歴（キーボードのログ等）を外部（攻撃者）に送信します．

（5）ランサムウェア

ユーザのデータを暗号化して“人質”とすることでユーザから身代金を搾取することを目的として使用されます．

（6）ボット

外部の指令者（攻撃者）からの遠隔操作によって，さまざまな活動（スパムメール送信や情報漏えい，他ホストへの攻撃活動等）を行います．
ボットに感染すると，知らないうちにボットネットワークに参加させられて，DDoS攻撃などに加担することになります．
悪者に操られる「ロボット」のイメージがあるので「ボット」と呼ばれています．

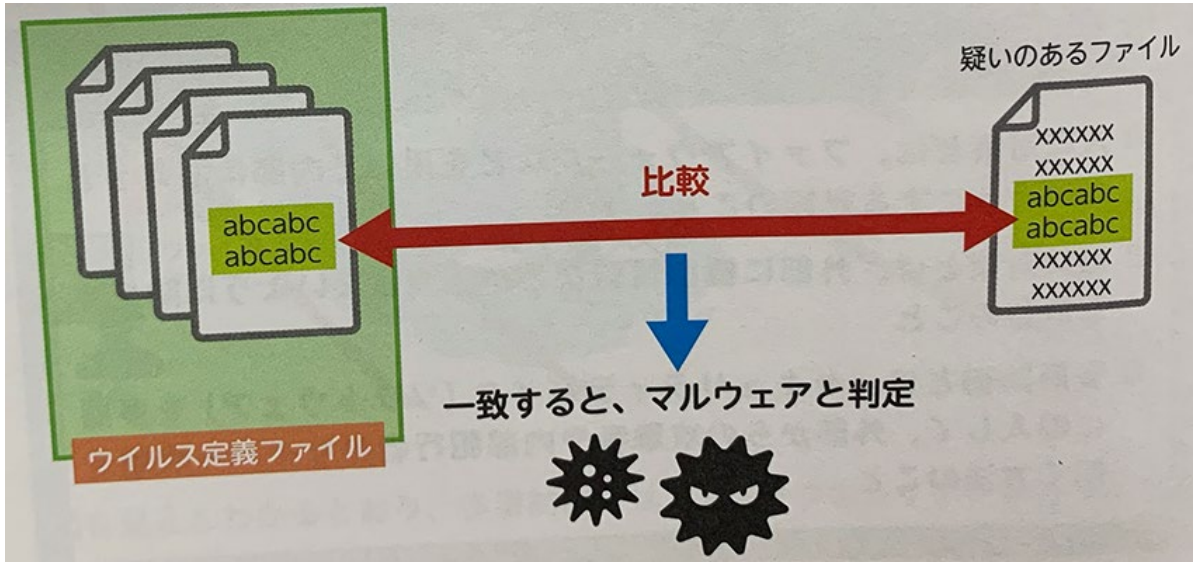
4. マルウェアの検知方法

これらの方法で前述すべてのマルウェアを検知できるわけではない

検知方法は複数ありますが，実際，1つの方法だけでなく，いくつか併用することで検知能力を上げていくことができます．

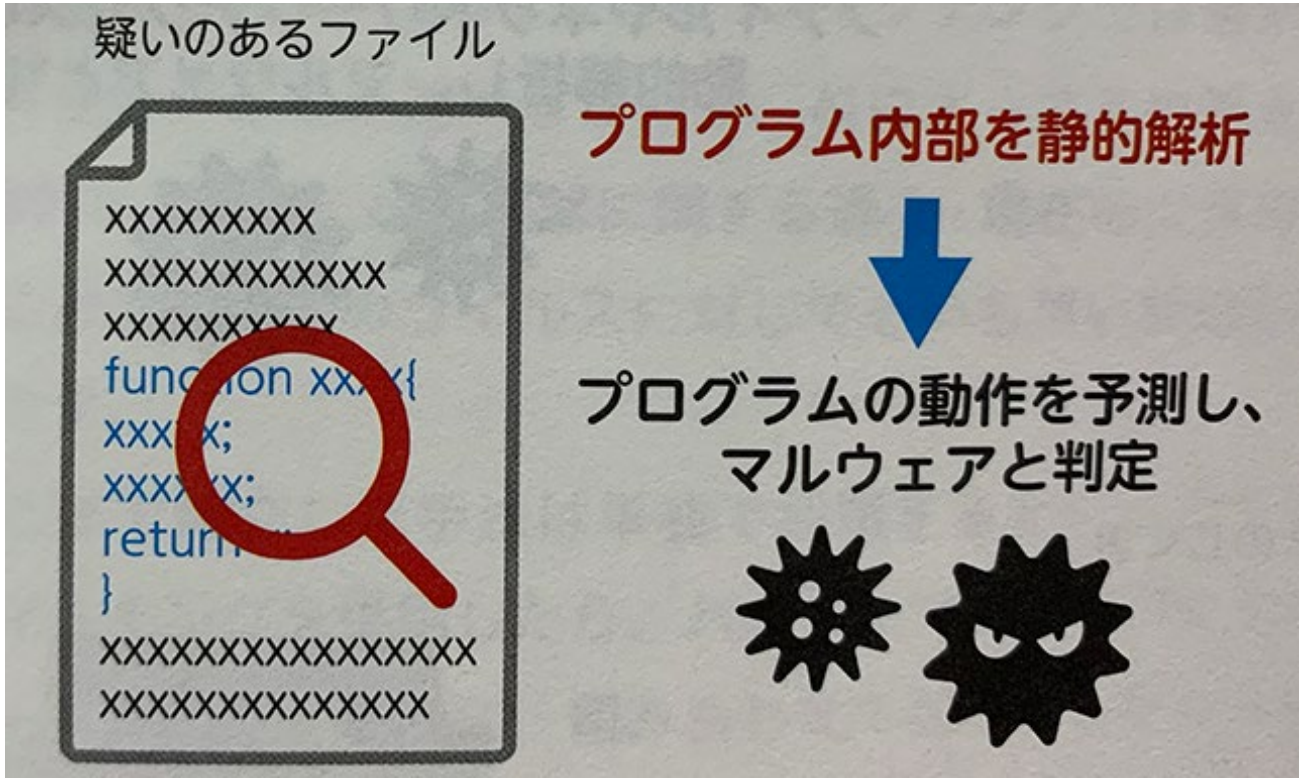
（1）パターンマッチング

マルウェア対策ソフトのベンダーが作成するマルウェア定義ファイル（「パターンファイル」とも呼ばれる）には，マルウェアの特徴が保存されています．パターンマッチングではそのマルウェア定義ファイルと疑義のあるファイルを比較し，特徴が一致すればそのファイルはマルウェアであると判断します．



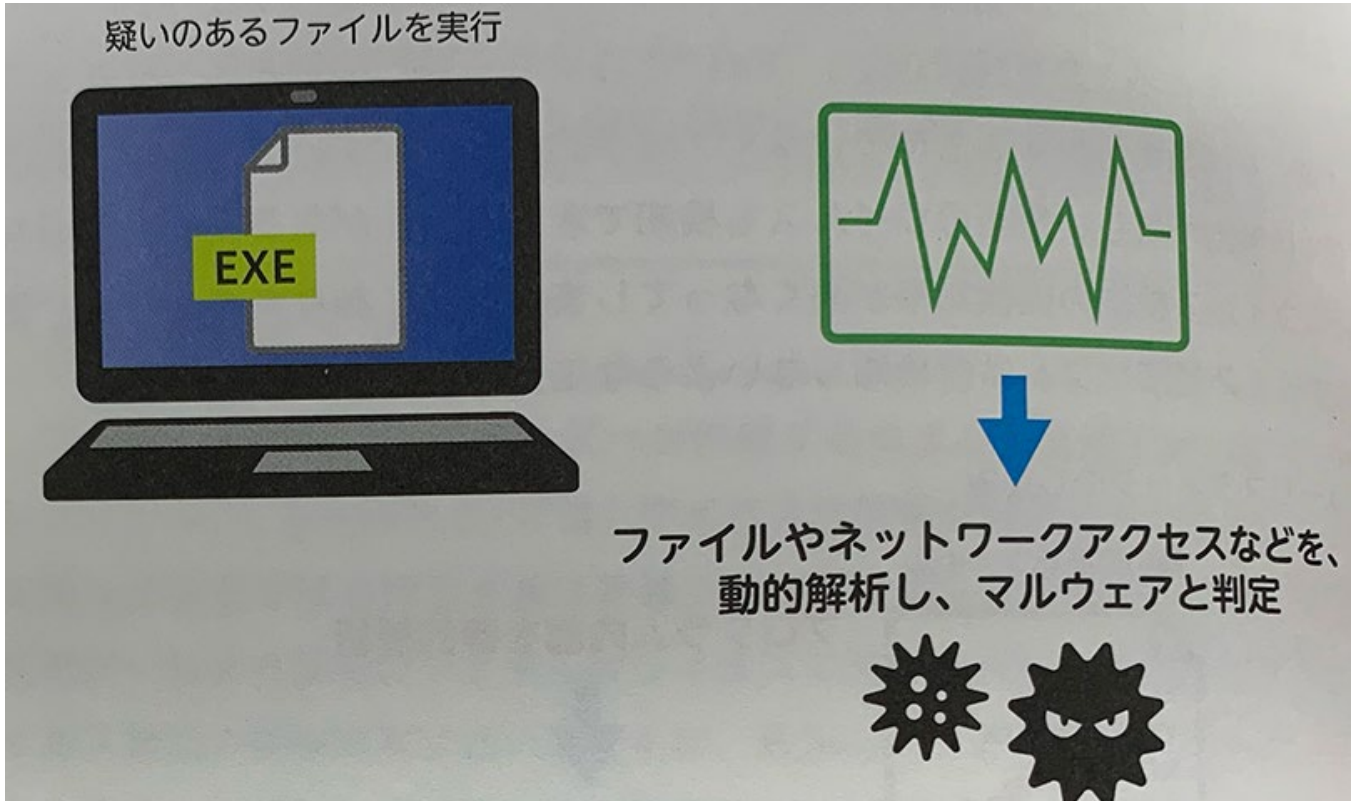
（2）ヒューリスティック

ヒューリスティックでは疑いのあるファイルのプログラムを静的解析して，マルウェアなのかどうかを判断します．簡易的な解析を行い，パターンマッチングでは検出が難しい最新のマルウェアも検知できる可能性があります．ただ，誤検出率が高くなってしまう傾向もありますが，最近，誤検出しないような工夫がされています．

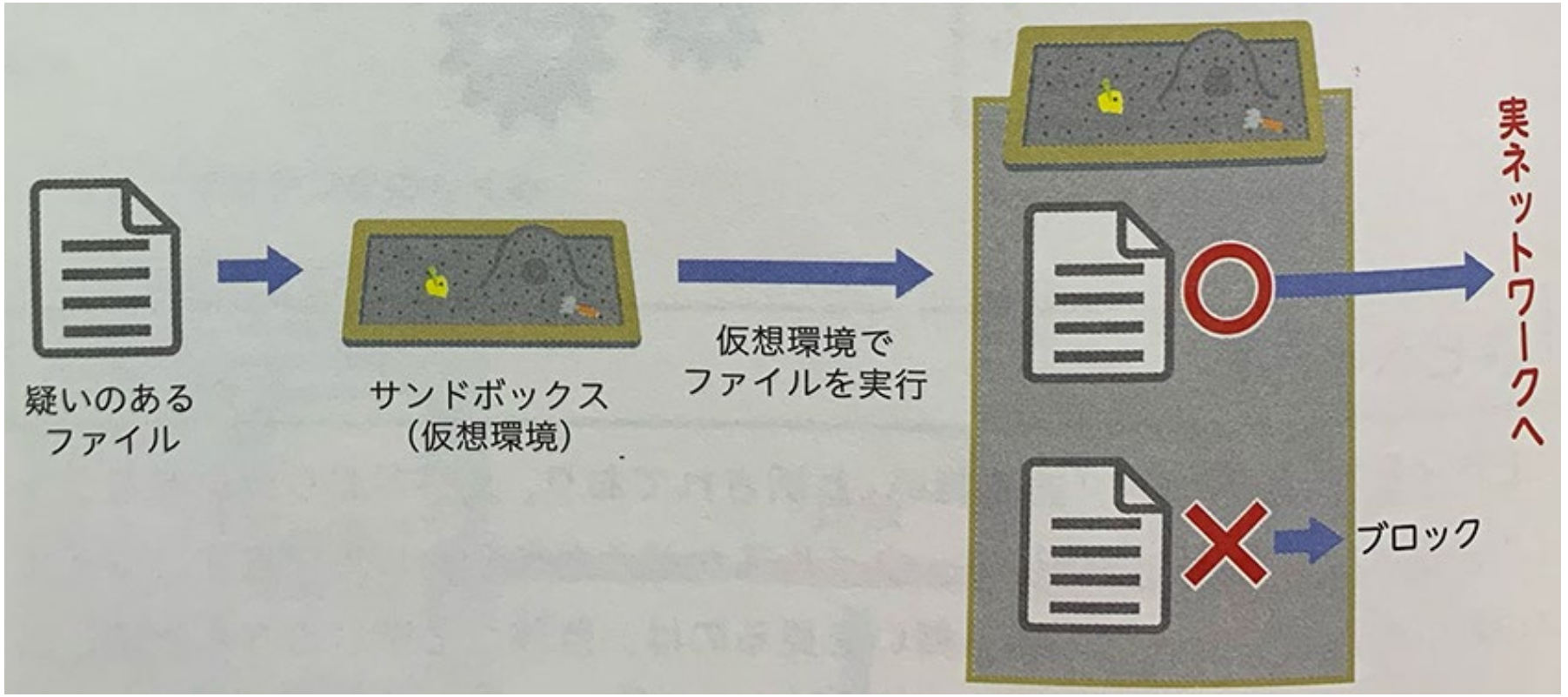


（3）ビヘイビア／サンドボックス

「振る舞い」と訳されており，文字どおり疑いあるファイルの振る舞いを動的に解析して，マルウェアかどうかを判断します．マルウェア対策ソフトがマルウェアと判断した直後にその振る舞いを止め，プロセスを終了します．この方法ではマルウェア感染を完全に防ぐことが難しいので，サンドボックスと協同します．

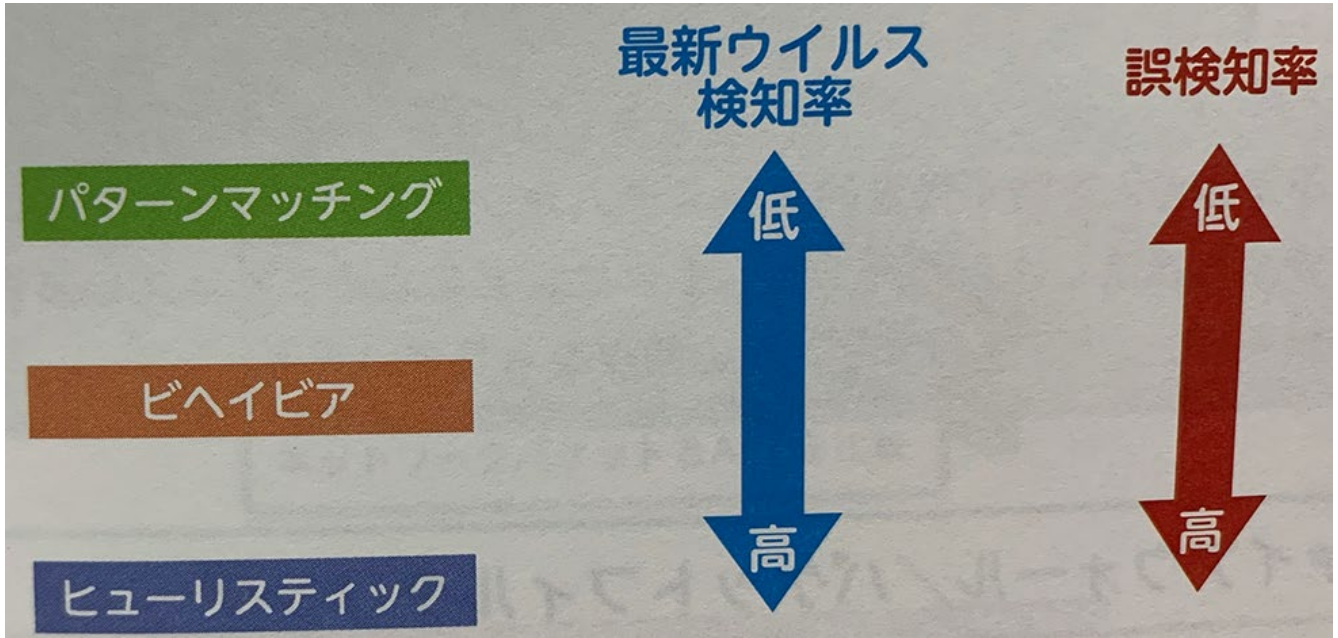


サンドボックスでは，実環境とは異なる仮想環境上という「閉じた空間」で疑いあるファイルの振る舞いを解析します．そのため，たとえマルウェアが感染を試みても仮想環境上でしか影響がないので，実環境がマルウェアに感染する可能性は非常に低いです．



（4）3種類の検知手法の比較

パターンマッチングでは最新のマルウェアを検知できない可能性がありますが，AIを活用してその弱点を補うことが可能です．具体的には，サイバー攻撃に関する過去・現在の大量の情報をAIによって分析することで，未知のマルウェアに対してもいち早い検知と対処ができるようになるのです．また，AIとパターンマッチングを併用したり，パターンマッチングとヒューリスティックを併用したりといった具合に，組み合わせて利用するかたちが一般的です．



5. 個人レベルでのマルウェア対策

（1）脆弱性の解消

OSやソフトウェアに脆弱性があると，そこを突破口とされ，マルウェアに感染したり，その他の攻撃を受けたりします．解消方法は以下です．

- Windows Updateなどの機能を利用した自動的な方法
- メーカーから提供される修正プログラムを適用する手動的な方法ソフトウェアの脆弱性を修正するプログラムはパッチと呼ばれ，メーカーから通常無償で提供されています．オンラインでダウンロードしてバージョンアップが可能：スマホや組み込み機器など

(2)マルウェア対策ソフトウェアのインストールと更新

マルウェア対策ソフトウェアは，パターンファイルと呼ばれるマルウェア検出用のデータファイルを使用して，ファイルやディスクに潜んでいるマルウェアを発見していきます．

最近のマルウェア対策ソフトウェアのほとんどは，最新のパターンファイルを自動的にダウンロードして更新するようになっています．

（3）パーソナルファイアウォールの活用

パーソナルファイアウォールは，正しく設定・運用すれば，外部からのマルウェア感染や不正アクセスを防いでくれます．

WindowsやMacOSなどには標準機能として搭載されています．また，マルウェア対策ソフトウェアの中には，パーソナルファイアウォール機能を持つものもあります．

(4)Webブラウザのセキュリティ対策

Webブラウザのセキュリティをできるだけ高く設定し，また最新版にアップデートすることで，ファイルのダウンロードやリンクのクリックによってマルウェアに感染するなど被害に遭う可能性を低減することができます．

(5)ネットサーフィン時の対策

Webサイトには，各種マルウェアが，普通の無害なプログラムを装って置かれていることがあります．安易なダウンロードは避けるべきです．

（6）不審な添付ファイル，迷惑メールの取り扱い

- 開かないことが基本．そのまま削除します．必要な場合，関係部門（管理者，専門家やプロバイダに相談）
- 添付ファイルは，開く前や実行する前にマルウェア検査を行います（マルウェア対策ソフトウェア等を使って）．
- 見た目に惑わされず，添付ファイルの拡張子とアイコンを確認します．ファイルを右クリックして「プロパティ」を選択し「全般」タブの「ファイルの種類」の表示を確認しましょう．文書ファイルのように見えるにも関わらず，ここに「アプリケーション」や「ショートカット」と表示された場合は，偽装された危険なファイルの可能性があります．
  危険ファイルの拡張子の例：.exe　.scr　.bat　.js　.wsf

(7) 外部記憶媒体の利用

- 自身が管理していない外部記憶媒体は，自身のパソコンには接続しません．
- 自身が管理していないパソコンには，自身の外部記憶媒体を接続しません．
- 外部記憶媒体の自動実行機能を無効化します．

(8) マルウェアに感染してしまった場合の対処方法

- ネットワーク接続を遮断し，システム管理者や専門家の指示に仰ぎます．
- 最新のマルウェア対策ソフトウェアで検査を行い，マルウェア名を特定します．
- マルウェアに合った適切な駆除を行います．
- データが破壊されたときは，バックアップから復旧します．
- 最新のマルウェア対策ソフトウェアでもう一度検査を行います．

- 再発防止の予防策を講じます.（感染経路の特定と原因の排除, パッチ当てなど）

練習問題

1. プログラムの脆弱性を利用したマルウェアの感染の仕組みについて述べなさい．

2. マルウェアの種類とそれに対応可能な検知方法を整理しなさい．