「彼を知り己を知れば百戦殆うからず」～サイバーセキュリティの現状と防止策について

埼玉工業大学　工学部
情報システム学科　講師
森川　智博

背景（1）

東映子会社のECサイトに不正アクセス　カード情報1万件に流出の可能性

2020年10月01日 13時44分

印刷

PR 最新ビジネス情報を比

東映の子会社であ
ョップ」が不正アク
た可能性があると発

マルウェア「Emotet」9月に入って急拡大　手口はさらに巧妙に

2020年09月04日 17時04分 公開

[ITmedia]

印刷

PR 最新ビジネス情報

メールの添付ご
入って国内で急拡
る手口もさらにエ

ヨドバシカメラのAndroidアプリに脆弱性　フィッシングサイトなど任意のURLへのアクセスに使われる恐れ

2020年09月07日 13

印刷

PR 最新ビジネス情

ヨドバシカメ
って任意のURL

ドコモ口座と連携中止する銀行相次ぐ　35行中18行が受付停止

2020年09月09日 17時05分 公開

[谷井将人，ITmedia]

印刷

PR 最新ビジネス情

NTTドコモの
害が相次いでい
行が9月9日まで

LINE Payでも不正引き出し被害　知人の犯行か　被害総額約50万円

2020年09月16日 07時00分 公開

[谷井将人，ITmedia]

印刷　136　Share　B!　4

PR 最新ビジネス情報を比較入手！KEL 無料セミナーモールオープン！

LINE Payは9月16日、電子決済サービス「LINE Pay」を悪用してゆうちょ銀行から不正に現金を引き出す被害が発生したと発表した。被害件数は2件で、被害総額は合計49万8000円に上る。LINE Payはゆうちょ銀行の口座登録や口座からの残

背景（2）

ハッカー？　脆弱性？　ウィルス？

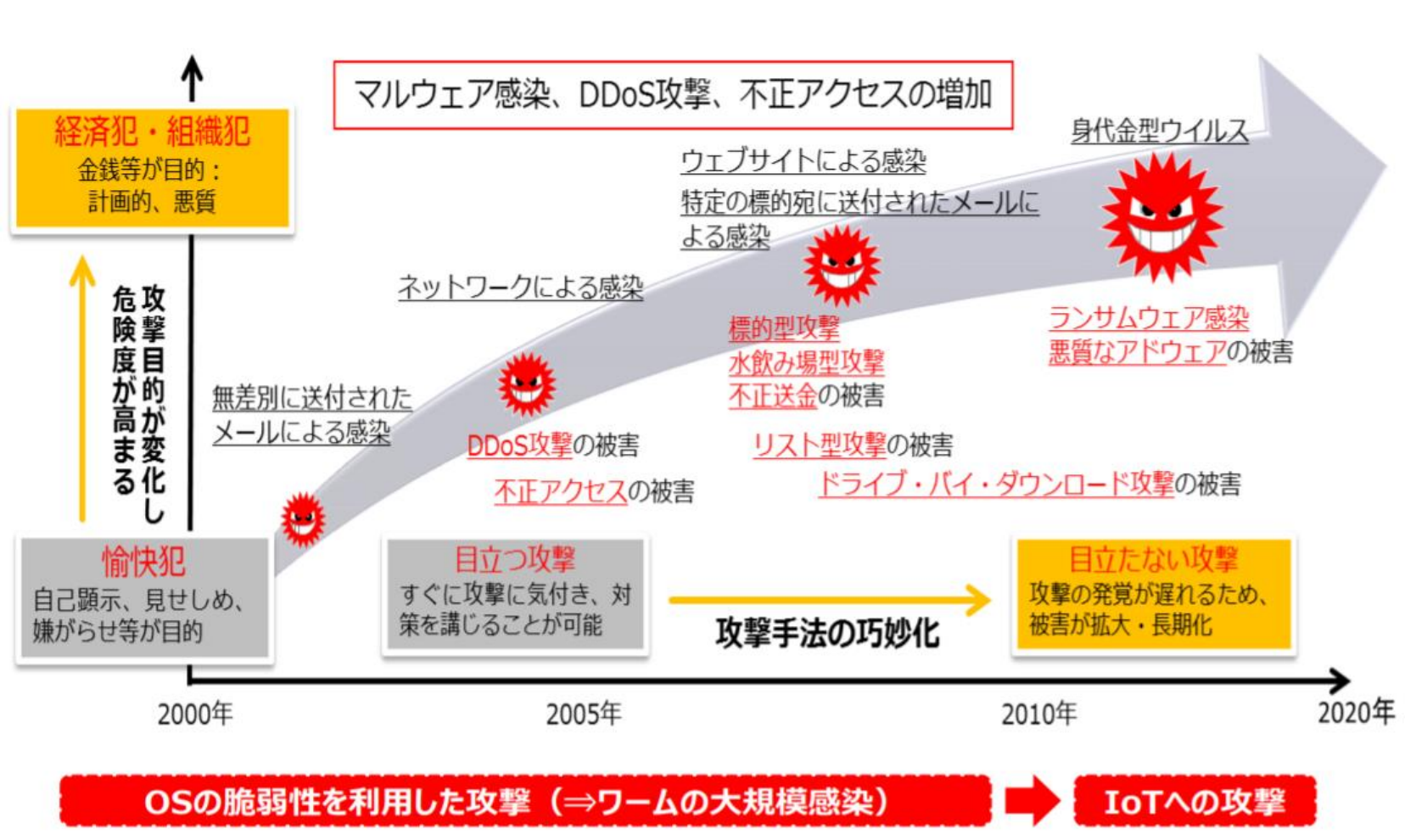
サイバーセキュリティ

ランサムウェア、スパイウェア、
フィッシングサイト、
DDoS攻撃、標的型攻撃メール

それだけではない

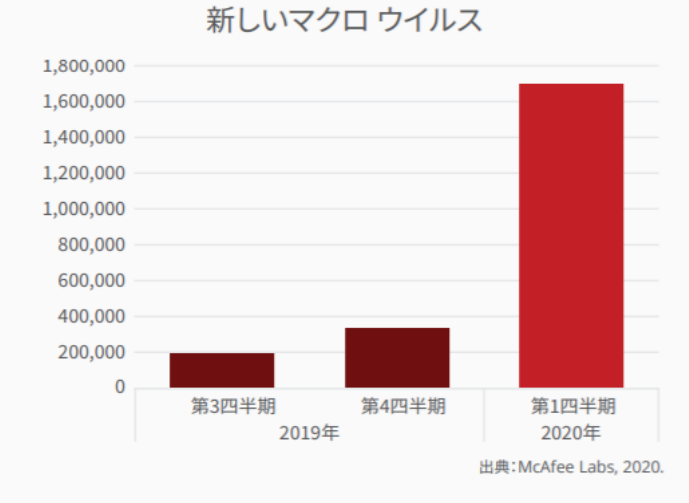
攻撃の種類は多岐にわたっている

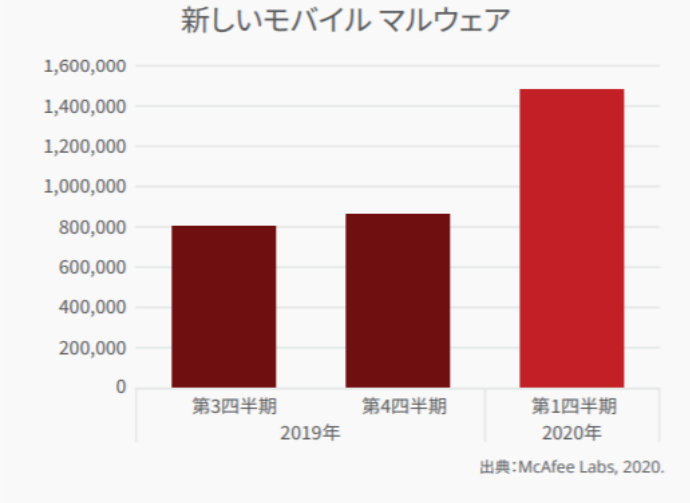
背景（3）

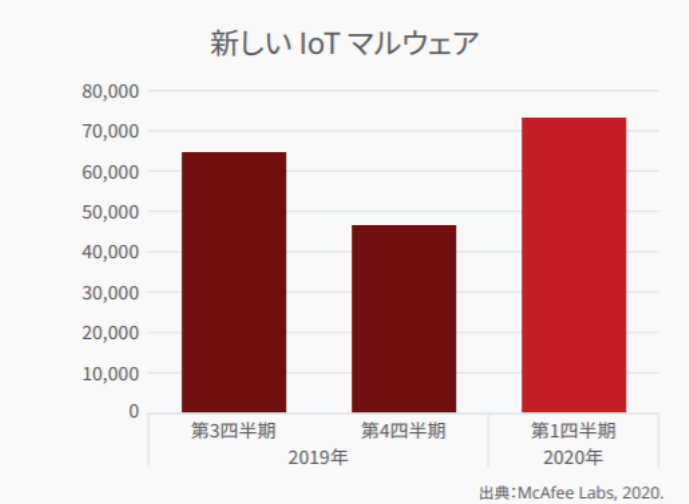


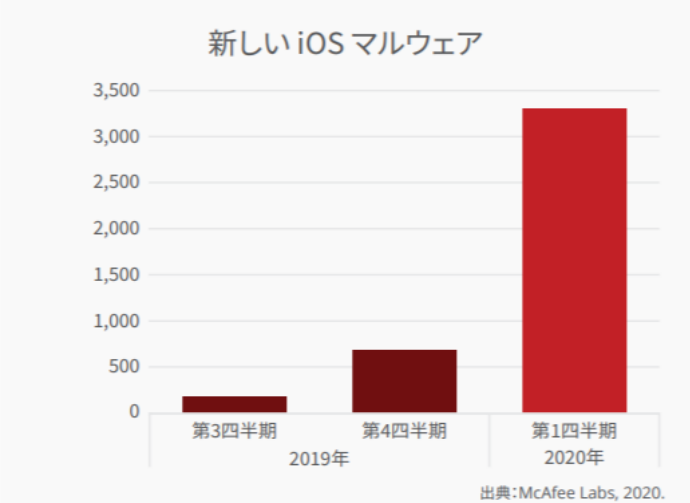
出典：「サイバー攻撃の最近の動向等について」（総務省）（https://www.soumu.go.jp/main_content/000722477.pdf）

背景（4）


新しいマクロ ウイルス
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
第3四半期
第4四半期
第1四半期
2019年
2020年
出典:McAfee Labs, 2020.


新しいモバイル マルウェア
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
第3四半期
第4四半期
第1四半期
2019年
2020年
出典:McAfee Labs, 2020.


新しい IoT マルウェア
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
第3四半期
第4四半期
第1四半期
2019年
2020年
出典:McAfee Labs, 2020.


新しい iOS マルウェア
3,500
3,000
2,500
2,000
1,500
1,000
500
0
第3四半期
第4四半期
第1四半期
2019年
2020年
出典:McAfee Labs, 2020.

背景（5）

出典：各種公開資料等より総務省作成

国内事例

2015年６月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者の情報約125万件が流出（標的型攻撃）
2015年11月	東京五輪組織委員会のホームページにサイバー攻撃、約12時間閲覧不能（DDoS攻撃）
2016年６月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
2017年５月	国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）
2018年１月	コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）
2020年	**三菱電機やNEC等において防衛関連情報を含む情報が外部へ流出した可能性が判明（不正アクセス） ドコモ口座経由で、不正に入手された口座番号・暗証番号等を使用した不正出金が判明（不正アクセス） カプコンがランサムウェアによる標的型攻撃を受け、個人情報等が外部へ流出した可能性が判明（ランサムウェア）**

海外事例

2015年６月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年５月	世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCryの感染被害が発生。行政、民間企業、医療等の多くの組織に影響（ランサムウェア）
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年９月	エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）

その他、最近では、新型コロナウィルスに乗じたサイバー攻撃の事例を多数確認

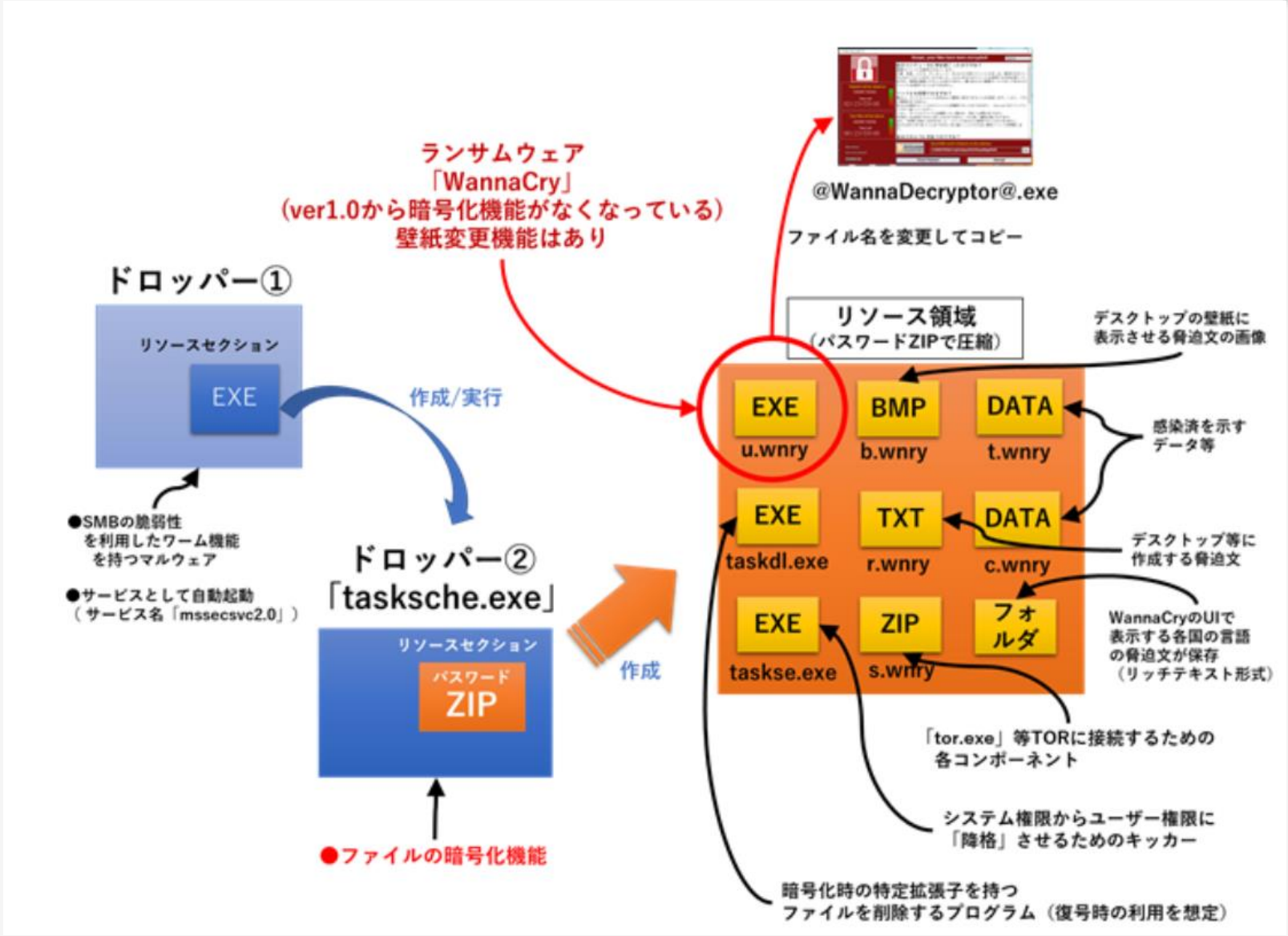
出典：「サイバー攻撃の最近の動向等について」（総務省）（https://www.soumu.go.jp/main_content/000722477.pdf）

背景（6）

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの 不正ログイン
不正アプリによる スマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの 不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

引用：https://www.ipa.go.jp/security/vuln/10threats2021.html

WannaCry（１）


ランサムウェア
「WannaCry」
(ver1.0から暗号化機能がなくなっている)
壁紙変更機能はあり
@WannaDecryptor@.exe
ファイル名を変更してコピー
ドロッパー①
リソースセクション
EXE
作成/実行
●SMBの脆弱性
を利用したワーム機能
を持つマルウェア
●サービスとして自動起動
（サービス名「mssecsvc2.0」）
ドロッパー②
「tasksche.exe」
リソースセクション
パスワード
ZIP
作成
●ファイルの暗号化機能
リソース領域
（パスワードZIPで圧縮）
EXE
u.wnry
BMP
b.wnry
DATA
t.wnry
デスクトップの壁紙に
表示させる脅迫文の画像
感染済を示す
データ等
EXE
taskdl.exe
TXT
r.wnry
DATA
c.wnry
デスクトップ等に
作成する脅迫文
EXE
taskse.exe
ZIP
s.wnry
フォルダ
WannaCryのUIで
表示する各国の言語
の脅迫文が保存
（リッチテキスト形式）
「tor.exe」等TORに接続するための
各コンポーネント
システム権限からユーザー権限に
「降格」させるためのキッカー
暗号化時の特定拡張子を持つ
ファイルを削除するプログラム（復号時の利用を想定）

WannaCry（2）

多言語対応化

WannaCry ver 1.0

- ●壁紙変更あり
- ●ボリュームシャドーコピーの削除あり
- ●ファイルの暗号化あり

一つのバイナリで完結していた

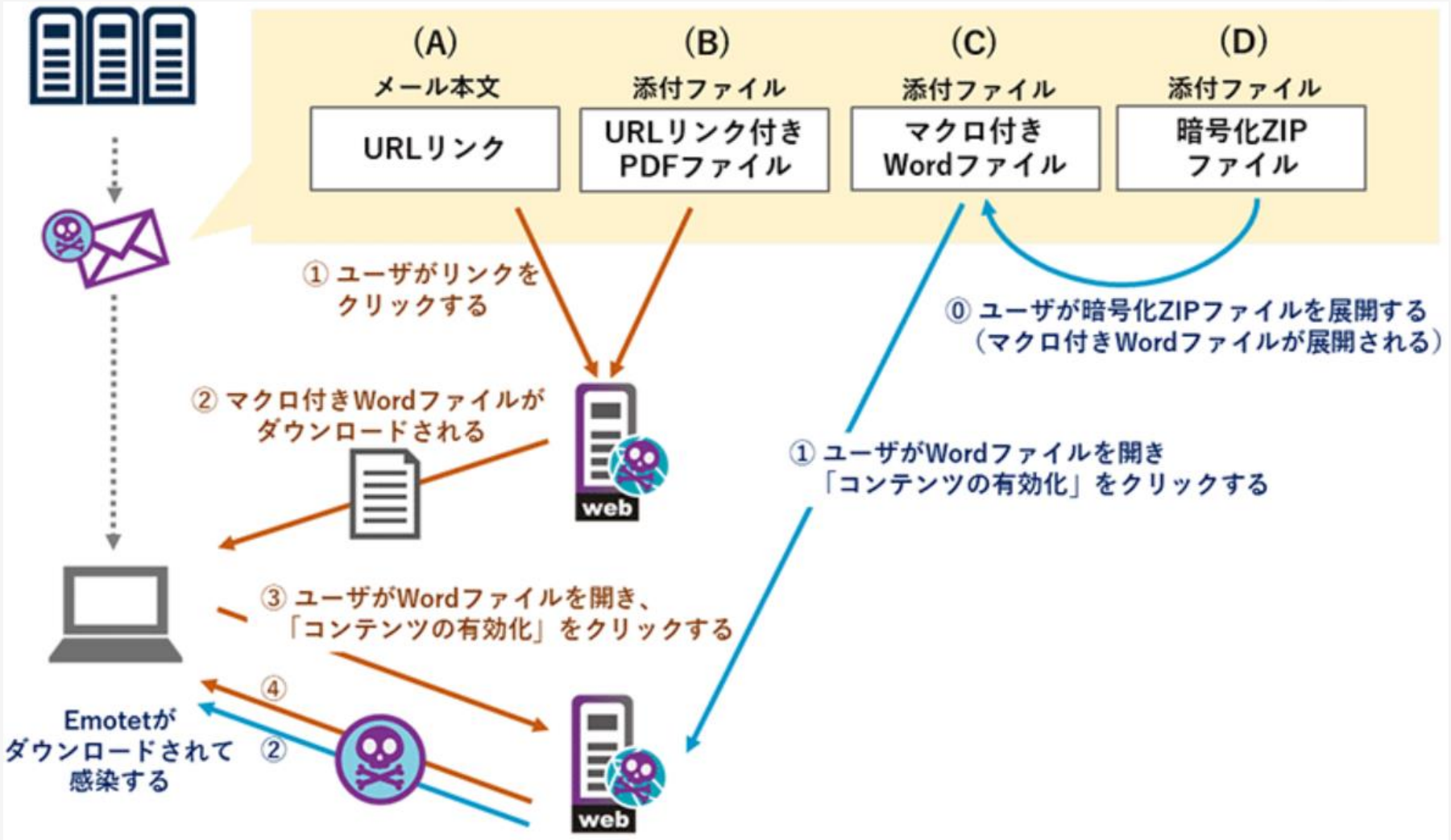
WannaCry ver 2.0 (GUI)

- ●壁紙変更あり
- ●ボリュームシャドーコピーの削除なし
- ●ファイルの暗号化なし　※注※

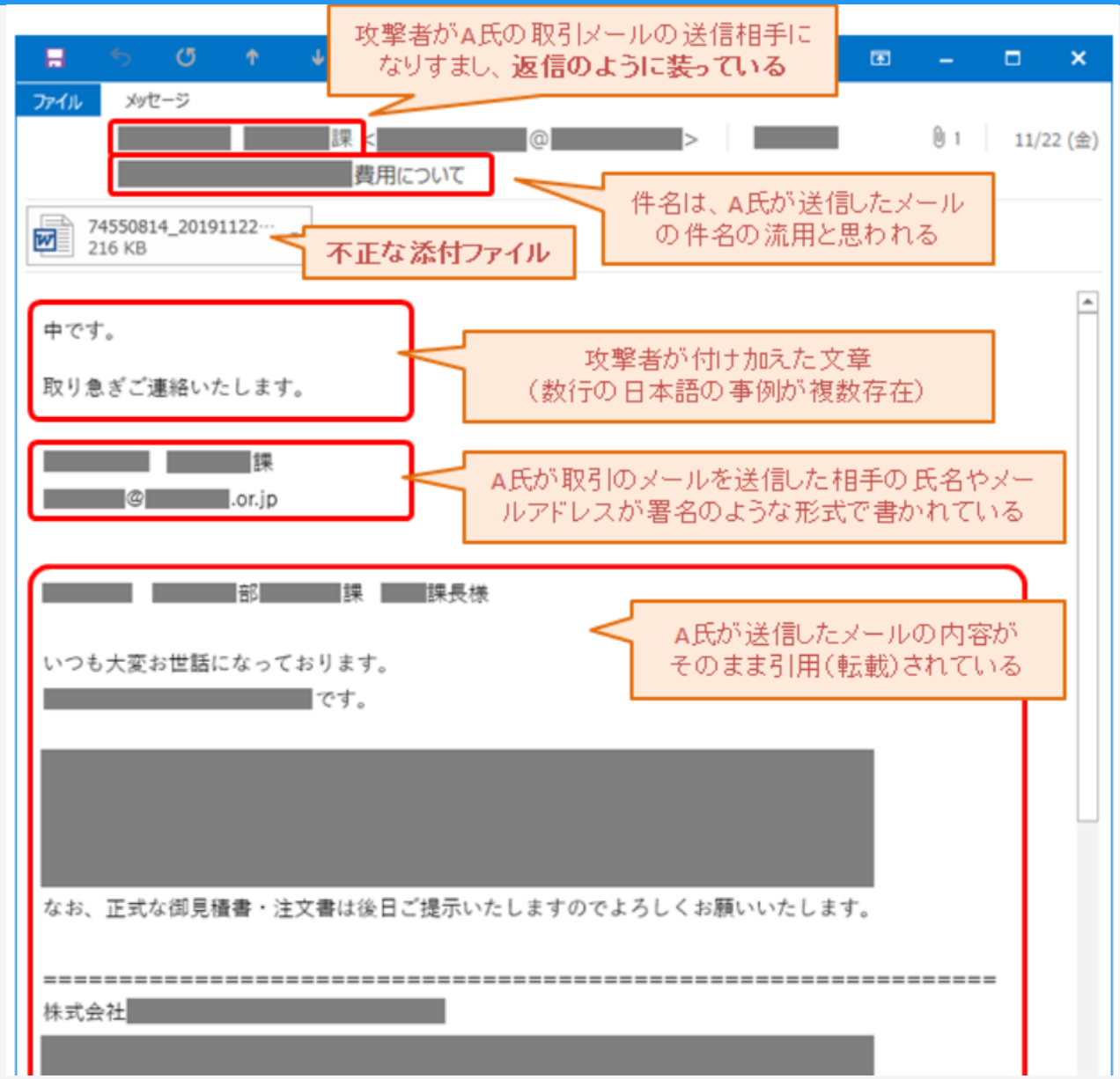
一つのバイナリで完結せず、機能分離した

※注※ WannaCry 2.0では、
暗号化機能等が別の実行ファイルに分離している

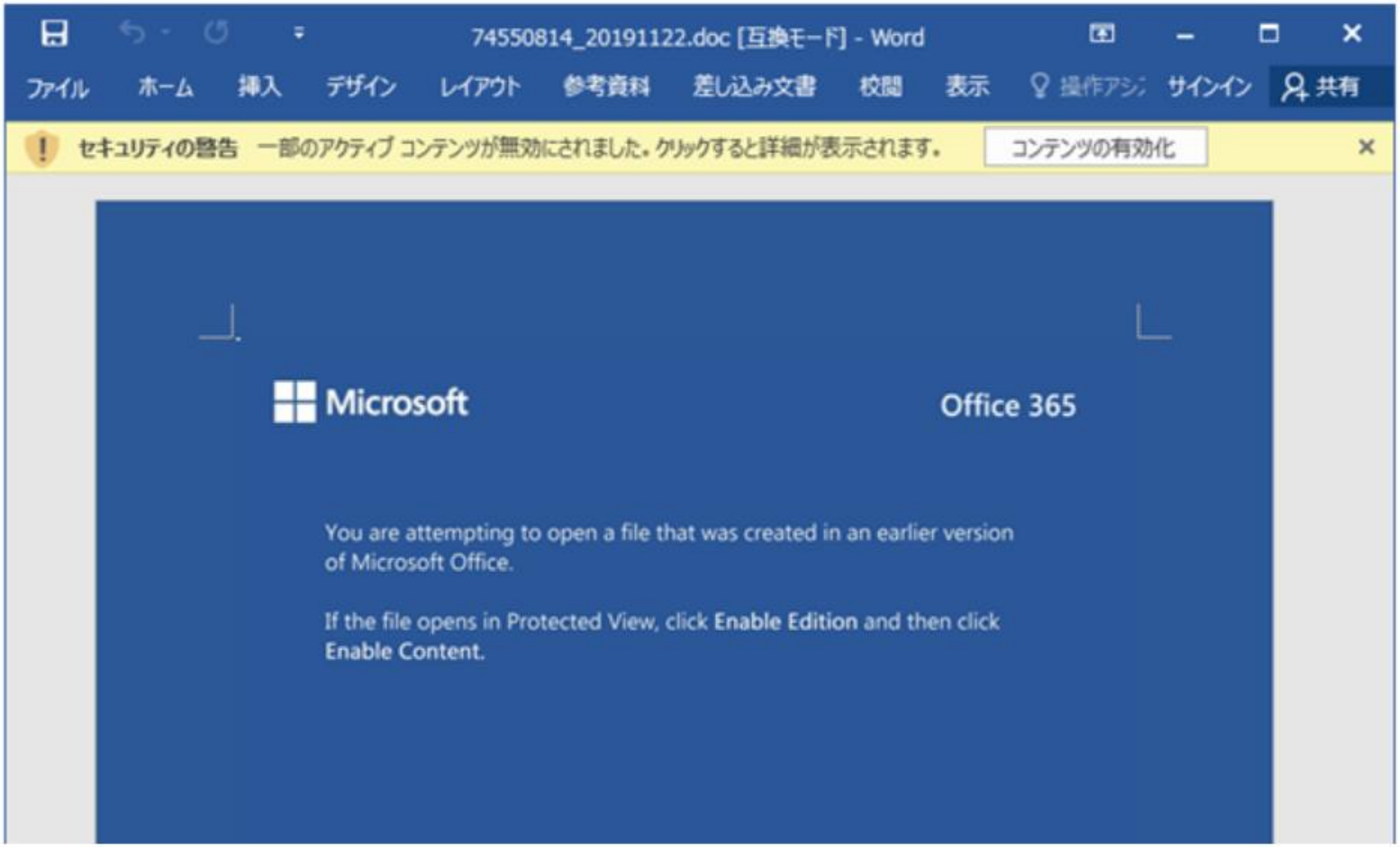
Emotet（１）


(A)
メール本文
URLリンク
(B)
添付ファイル
URLリンク付き
PDFファイル
(C)
添付ファイル
マクロ付き
Wordファイル
(D)
添付ファイル
暗号化ZIP
ファイル
① ユーザがリンクを
クリックする
⓪ ユーザが暗号化ZIPファイルを展開する
（マクロ付きWordファイルが展開される）
② マクロ付きWordファイルが
ダウンロードされる
web
① ユーザがWordファイルを開き
「コンテンツの有効化」をクリックする
③ ユーザがWordファイルを開き、
「コンテンツの有効化」をクリックする
④
Emotetが
ダウンロードされて
感染する
②
web

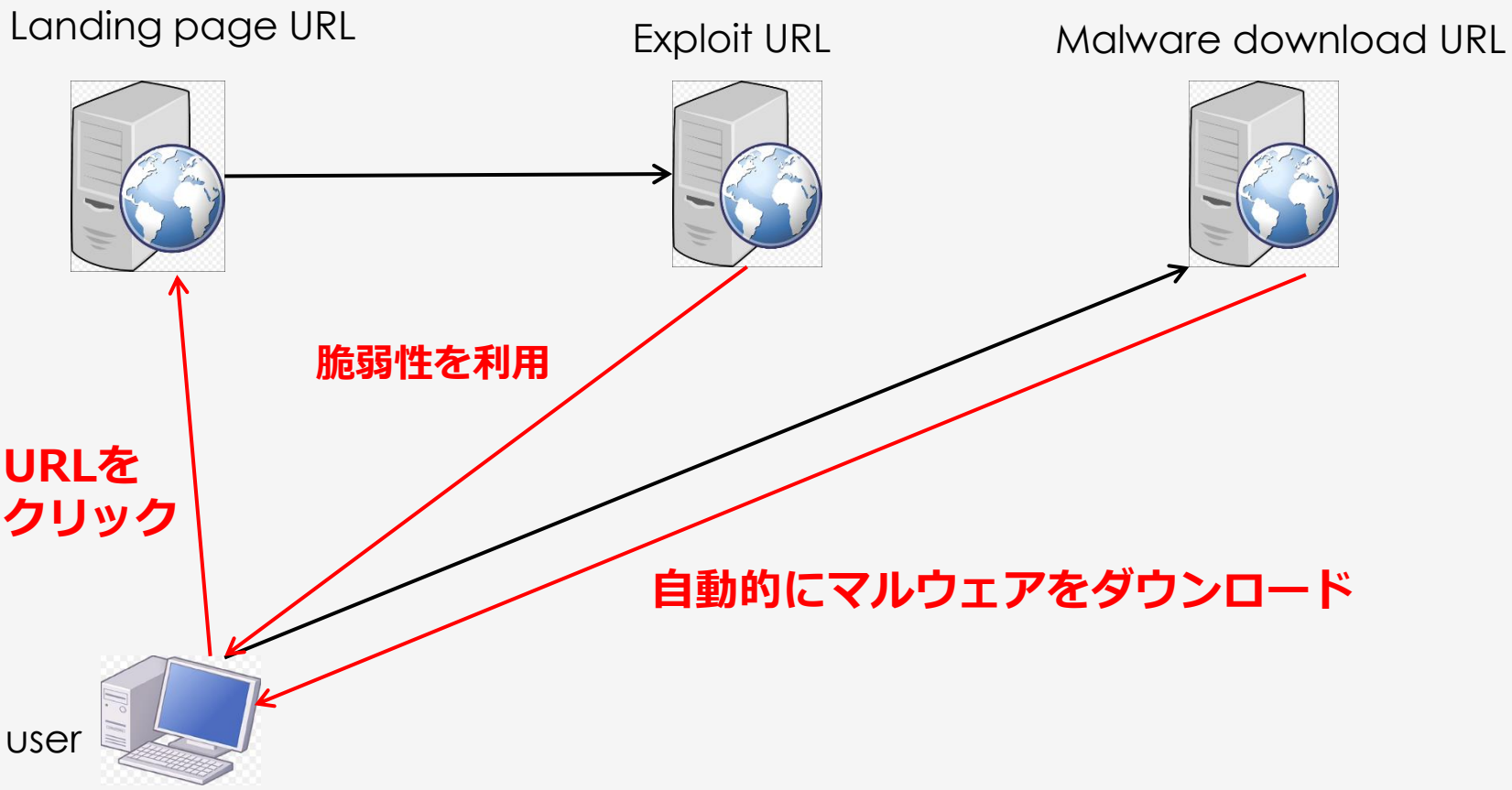
Emotet（2）


攻撃者がA氏の取引メールの送信相手になりすまし、返信のように装っている
ファイル
メッセージ
[redacted]課 <[redacted]@[redacted]>
11/22 (金)
[redacted]費用について
件名は、A氏が送信したメールの件名の流用と思われる
74550814_20191122…
216 KB
不正な添付ファイル
中です。
取り急ぎご連絡いたします。
攻撃者が付け加えた文章
（数行の日本語の事例が複数存在）
[redacted]課
[redacted]@[redacted].or.jp
A氏が取引のメールを送信した相手の氏名やメールアドレスが署名のような形式で書かれている
[redacted]部[redacted]課 [redacted]課長様
いつも大変お世話になっております。
[redacted]です。
A氏が送信したメールの内容がそのまま引用（転載）されている
なお、正式な御見積書・注文書は後日ご提示いたしますのでよろしくお願いいたします。
==========
株式会社[redacted]

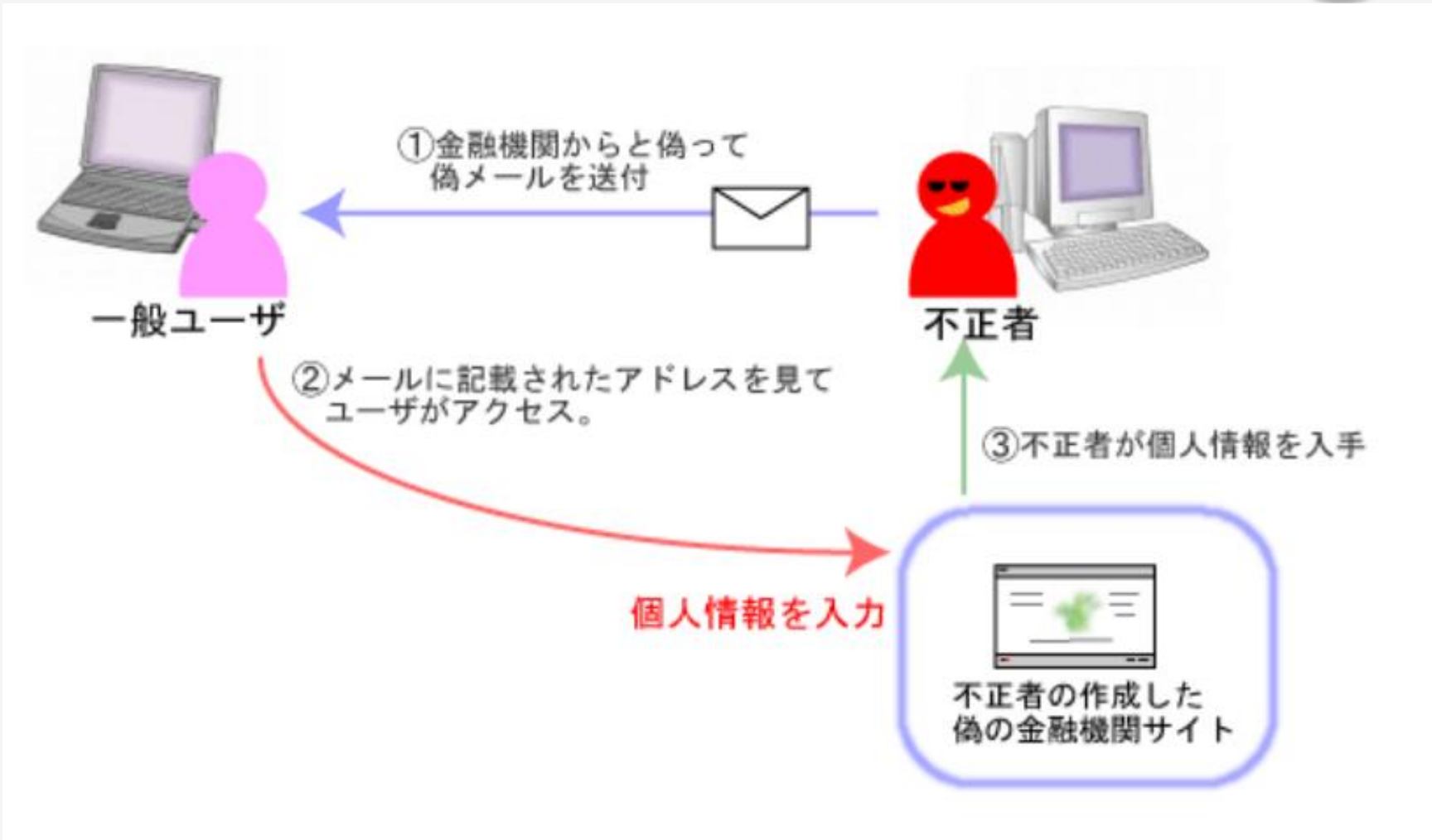
Emotet（３）


74550814_20191122.doc [互換モード] - Word
ファイル
ホーム
挿入
デザイン
レイアウト
参考資料
差し込み文書
校閲
表示
操作アシ
サインイン
共有
セキュリティの警告 一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。
コンテンツの有効化
Microsoft
Office 365
You are attempting to open a file that was created in an earlier version of Microsoft Office.
If the file opens in Protected View, click Enable Edition and then click Enable Content.

ドライブバイダウンロード攻撃



フィッシング攻撃


①金融機関からと偽って
偽メールを送付
一般ユーザ
不正者
②メールに記載されたアドレスを見て
ユーザがアクセス。
③不正者が個人情報を入手
個人情報を入力
不正者の作成した
偽の金融機関サイト

標的型攻撃

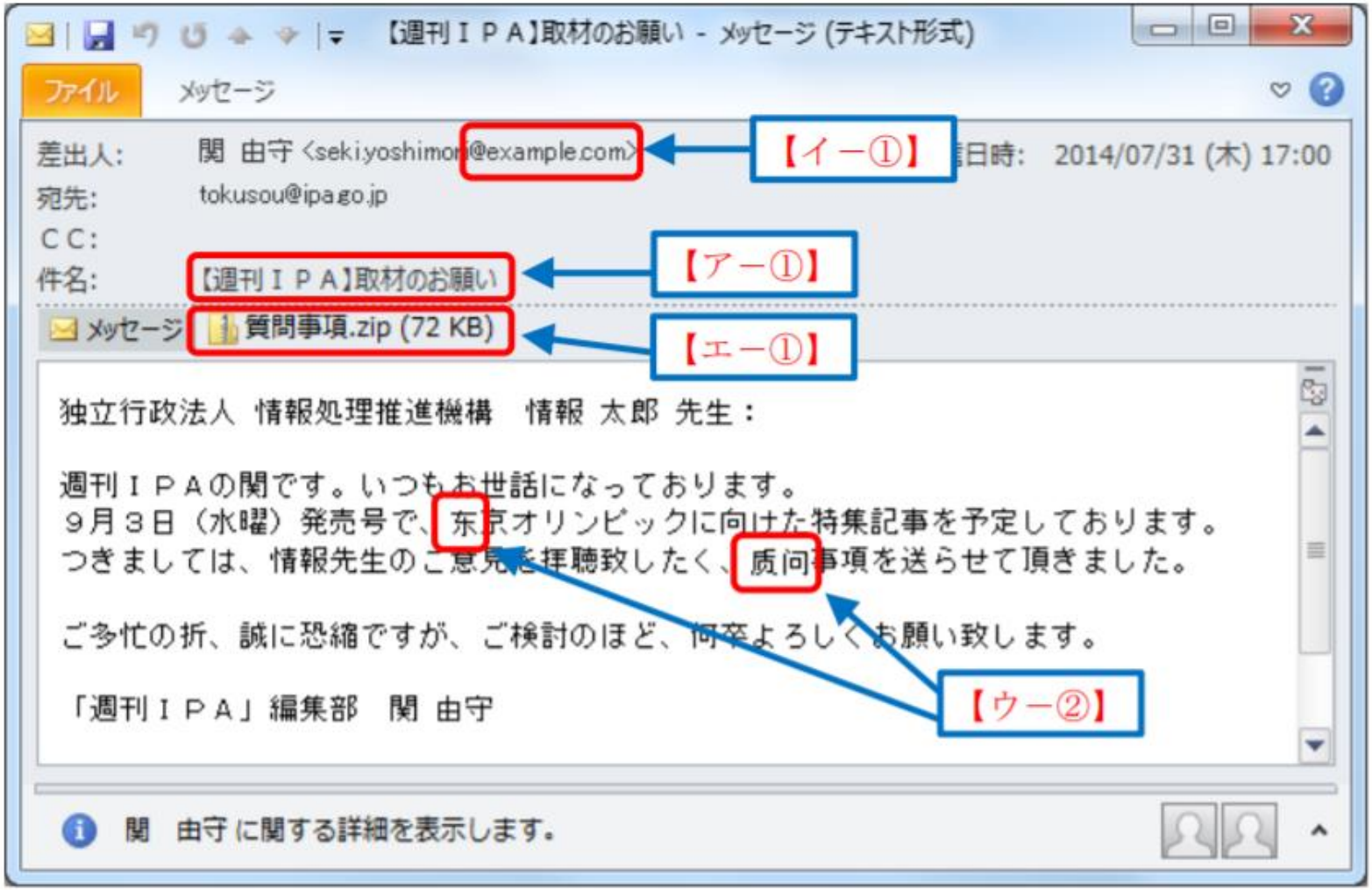
- 特定の相手に対するサイバー攻撃「標的型攻撃」

	手口	狙い
DoS・DDoS攻撃	メール爆弾・F5連打など	標的システム・サーバーのダウン
標的型メール攻撃	なりすましメールの送付	メールを開いたデバイス内の情報の盗難・破壊
Webサイト改ざん	管理者アカウントの乗っ取り、webサイトの脆弱性を利用	イタズラ、個人情報の抜き取りによる金銭的利益の受領
水飲み場型攻撃	標的がよく訪れるwebサイトを改ざんしウイルス設置	ウイルスに感染したデバイス・システムの乗っ取り、内部の情報を破壊

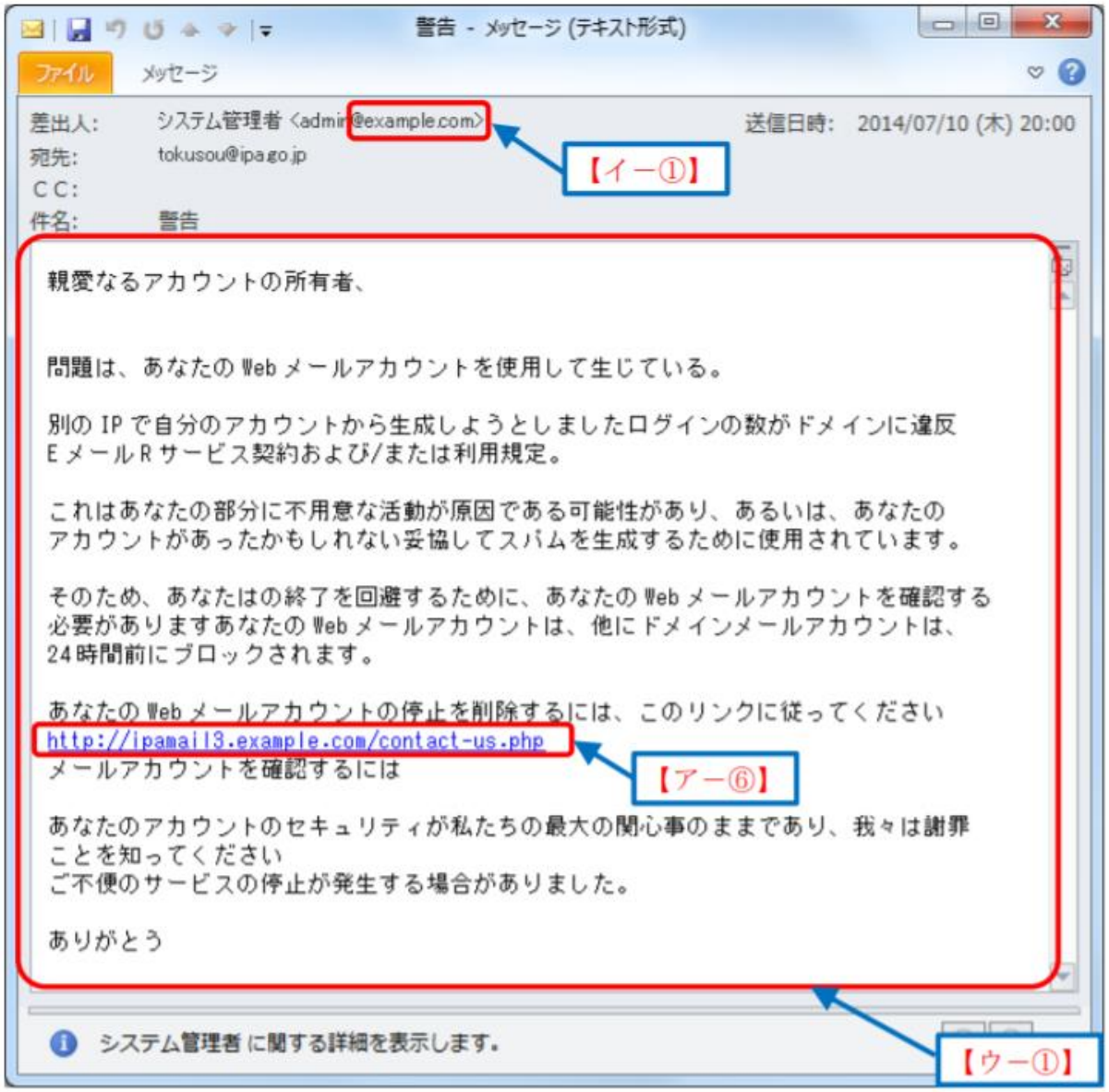
標的型メール攻撃（１）

- 標的型攻撃とは、ターゲットを特定の組織やユーザー層に絞って行うサイバー攻撃。そのターゲットに関して知り合いや取引先のふりをして悪意のあるファイルを添付したり、悪意のあるサイトに誘導するためのURLリンクを貼り付けたメールを送信し、パソコンやスマートフォンなどの端末をマルウェアに感染させようとする攻撃

標的型攻撃メールの例と見分け方（１）



標的型攻撃メールの例と見分け方（２）



標的型メール攻撃の対策

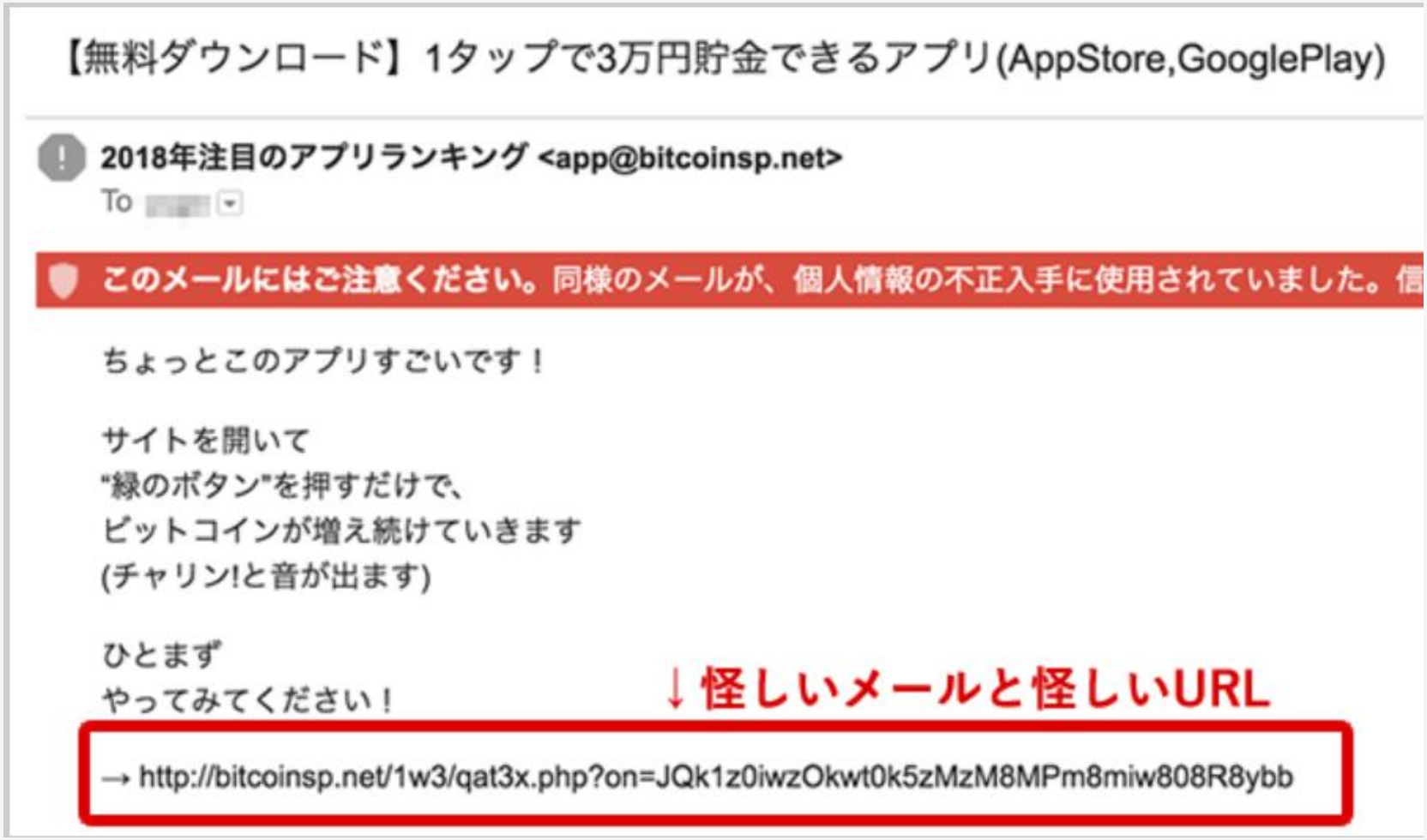
- OS・ソフトウェアを最新の状態にして脆弱性のリスクを最小限にする
- セキュリティ対策ソフトを導入する
- 怪しいメールを見分ける方法を知る・社内で共有する
- 標的型攻撃を疑似体験する
- 重要な情報は隔離しておく

ウイルスに感染しないための対策（１）

- OS・ソフトウェアを最新の状態にする

ウイルスに感染しないための対策（２）

- 不審なメールを閲覧しない

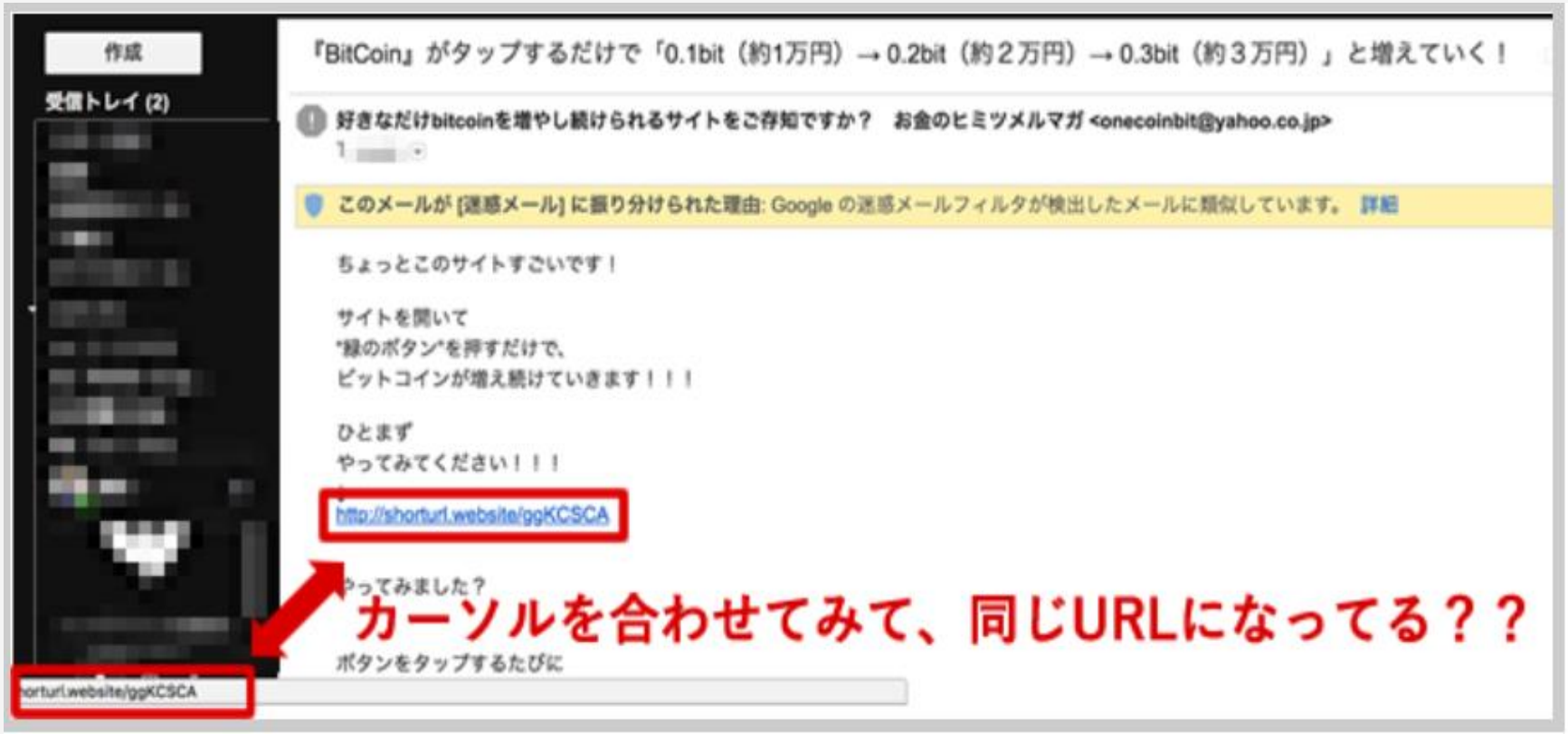


ウイルスに感染しないための対策（３）

- 怪しいサイトを閲覧しない

ウイルスに感染しないための対策（４）

- リンク先をチェックする



ウイルスに感染しないための対策（５）

■ セキュリティソフトを導入する

ノートン

Symantec（シマンテック）社からリリースされているノートンシリーズはセキュリティ対策ソフトの定番の１つ。
主に個人向け製品で、Windows、Macのウイルス対策だけでなく、パソコンの最適化、ディスククリーンアップ、データのオンラインバックアップなども可能です。
30日無料体験版あり

イメージ

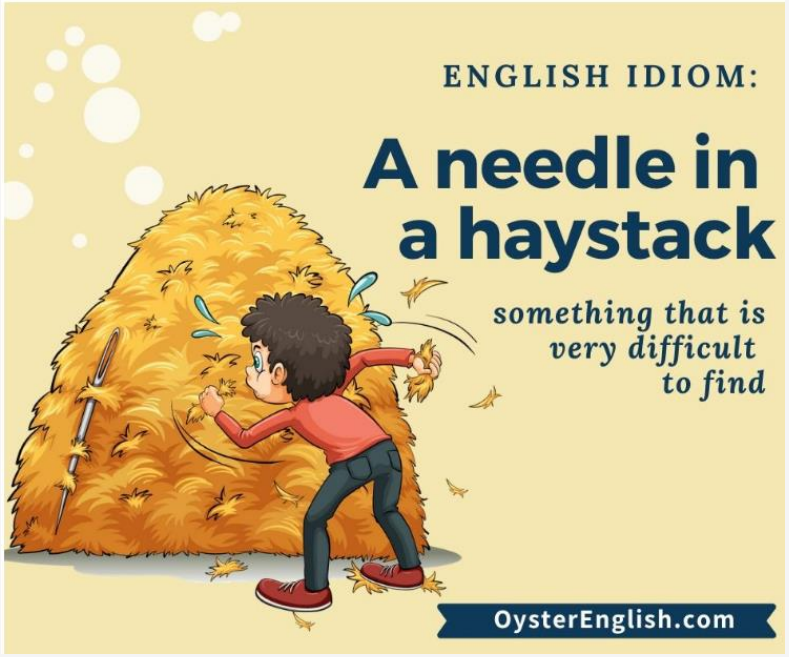
▸詳細はこちら

カスペルスキー

ロシアのカスペルスキー社のセキュリティソフト。上記のノートンに比較すると日本での知名度は下がるが、性能は非常に優れている。
Windows、Mac、Android対応の総合セキュリティソフトで、ウイルス対策、危険なWebサイトへのアクセス防止、ネット決済時の保護など、パソコンやモバイル端末を安全に使うためのセキュリティを提供。
30日無料体験版あり

研究の背景

- セキュリティ技術者たちは手動でサイバー攻撃を分析
- しかし、サイバー空間には、大量のデータが存在する。例えば、URLー＞30兆
- 大規模なデータからサイバー攻撃を検出するのは困難

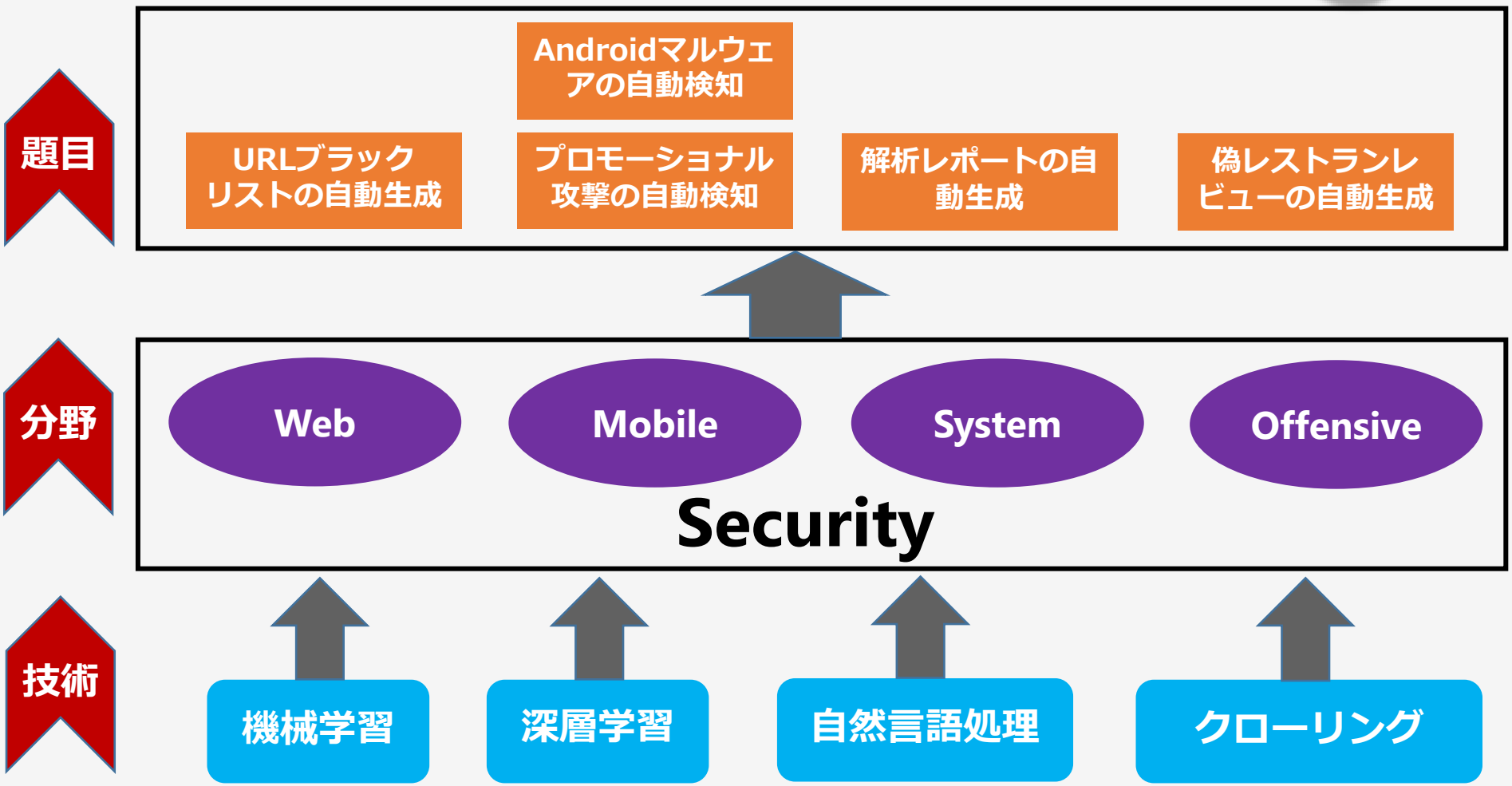


干し草の山の中にある一本の針を見つけ出す

機械学習や自然言語処理などの技術を用いて、サイバー攻撃の対策を自動化する必要がある

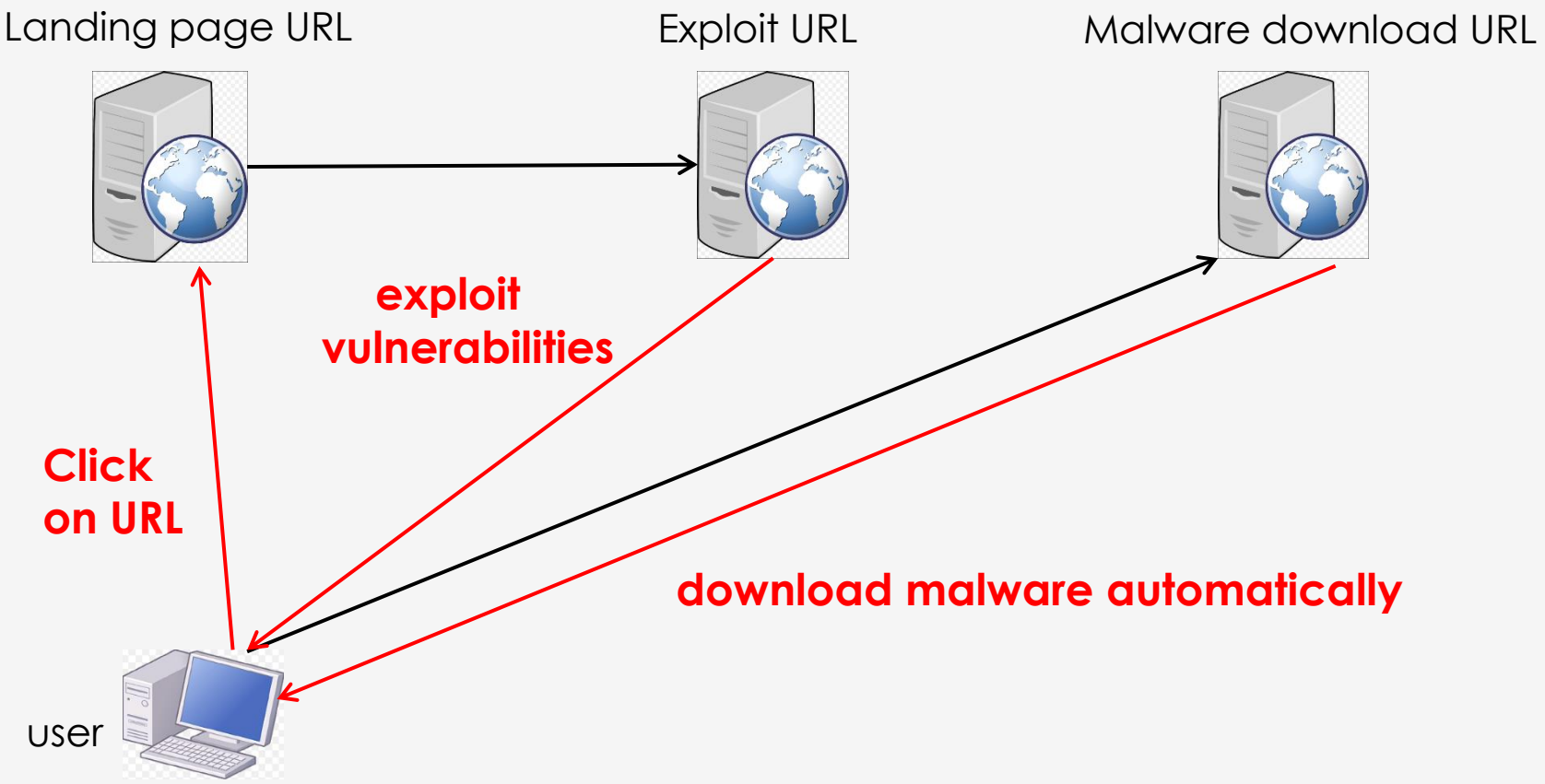
画像引用：https://www.oysterenglish.com/idiom-a-needle-in-a-haystack.html

研究経歴（全体像）


題目
Androidマルウェアの自動検知
URLブラックリストの自動生成
プロモーショナル攻撃の自動検知
解析レポートの自動生成
偽レストランレビューの自動生成
分野
Web
Mobile
System
Offensive
Security
技術
機械学習
深層学習
自然言語処理
クローリング

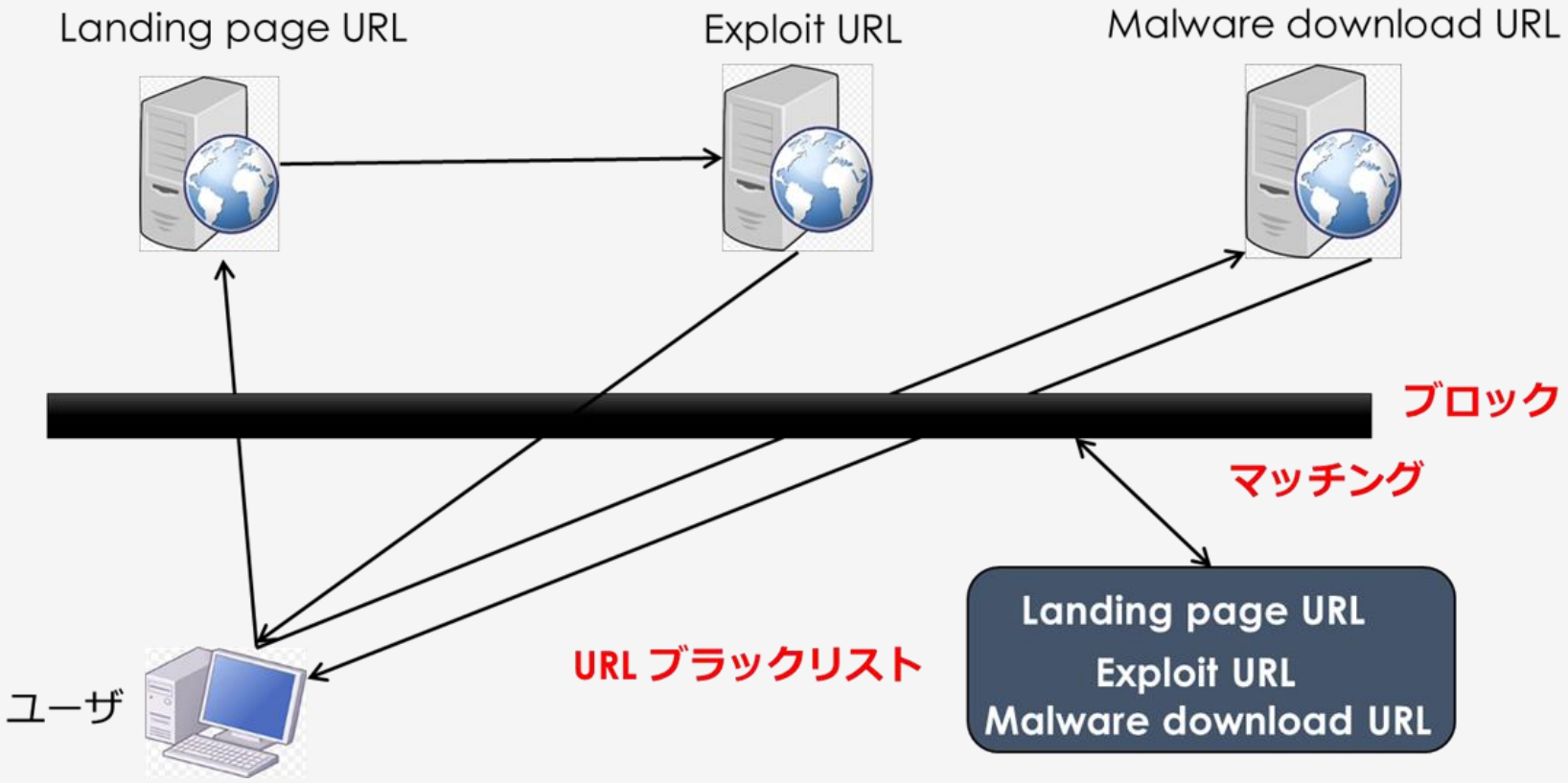
URLブラックリストの自動生成（１）

- Drive-by-download攻撃とは？



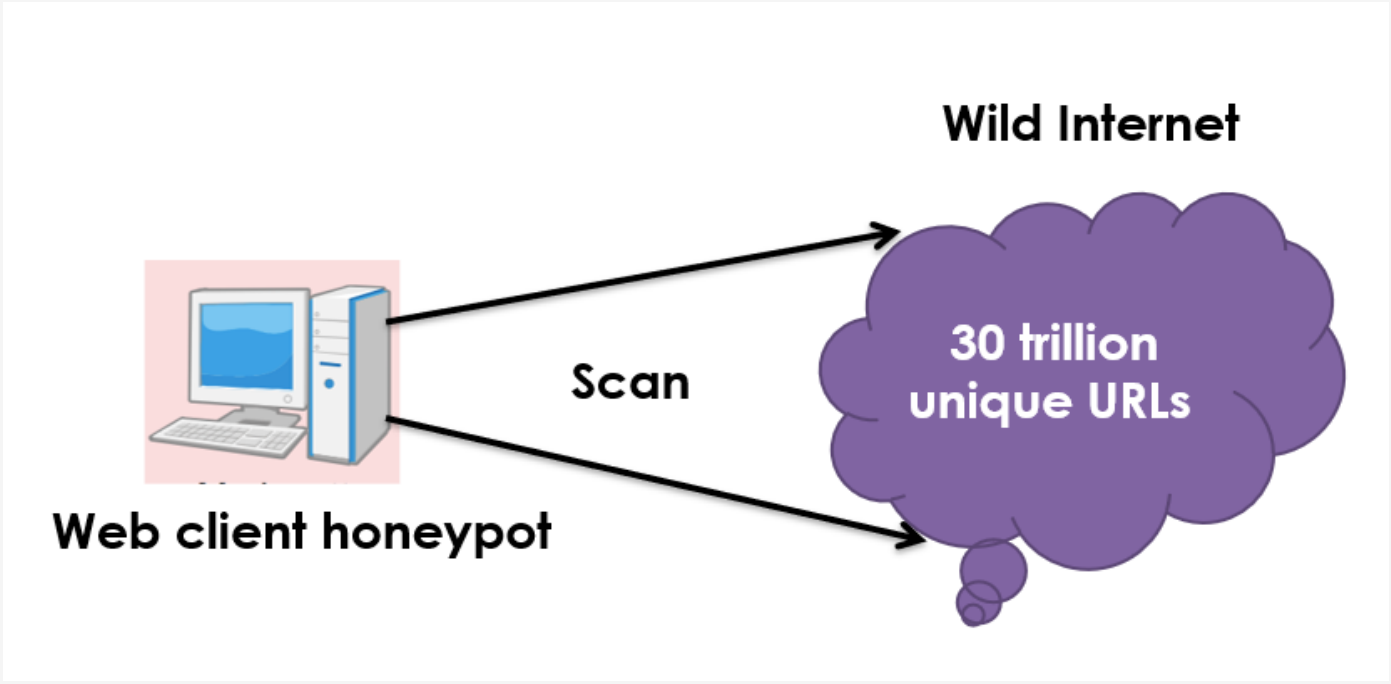
URLブラックリストの自動生成（２）

- URL ブラックリストとは？



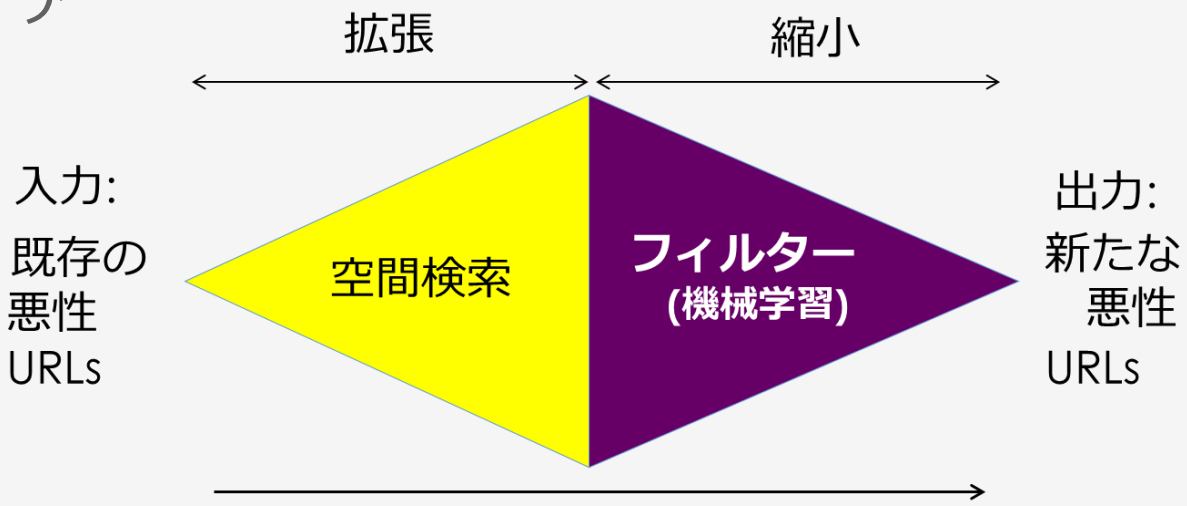
URLブラックリストの自動生成（３）

- 問題点
  - ✓しかし, URL ブラックリストは未知の悪性URLに対応できない
  - ✓URLブラックリストを有効に保つため，悪性URLを更新するのは重要

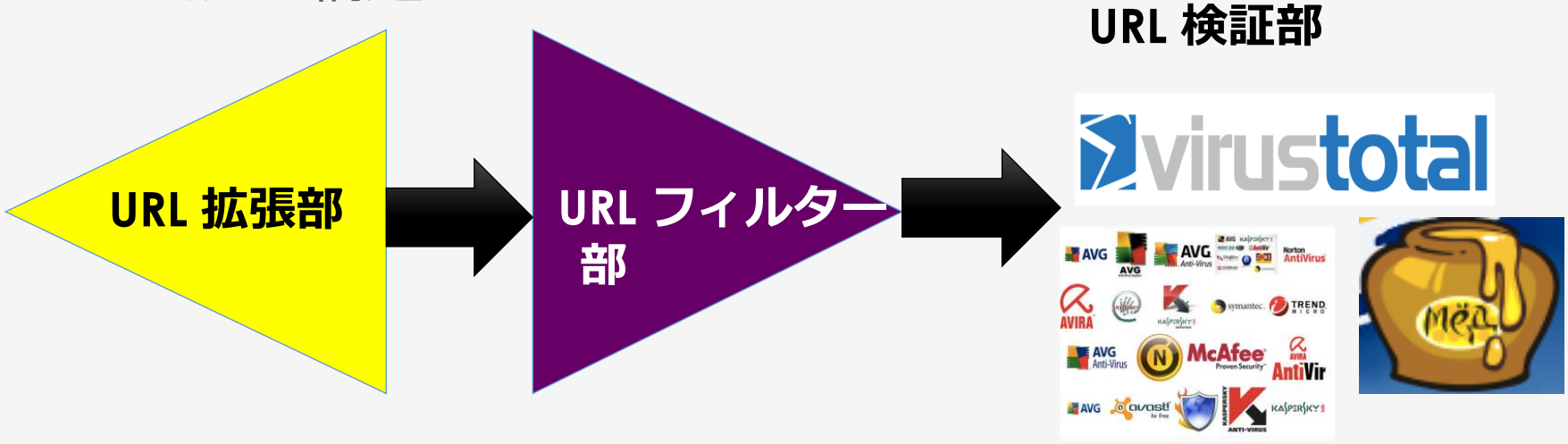


URLブラックリストの自動生成（４）

- アイディア

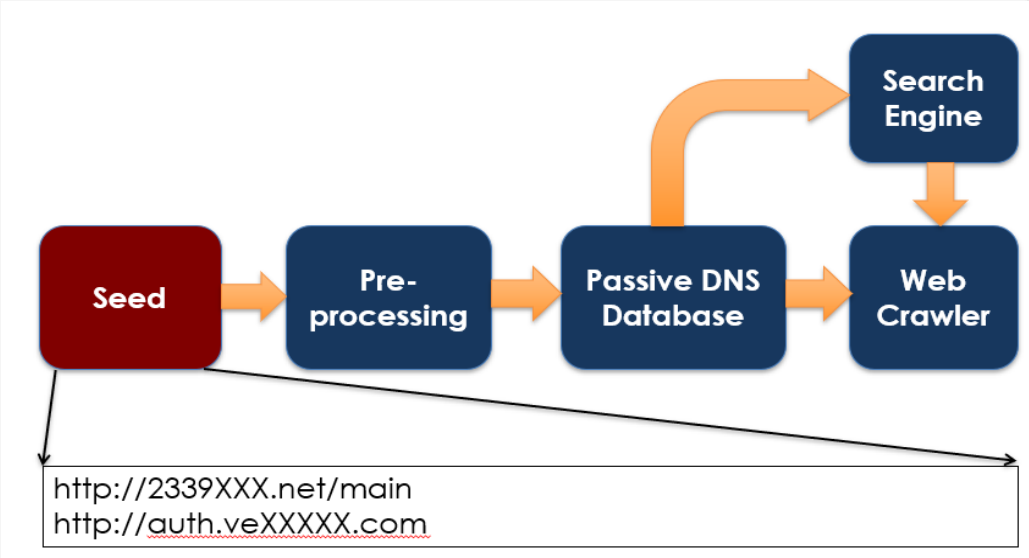


- システム構造

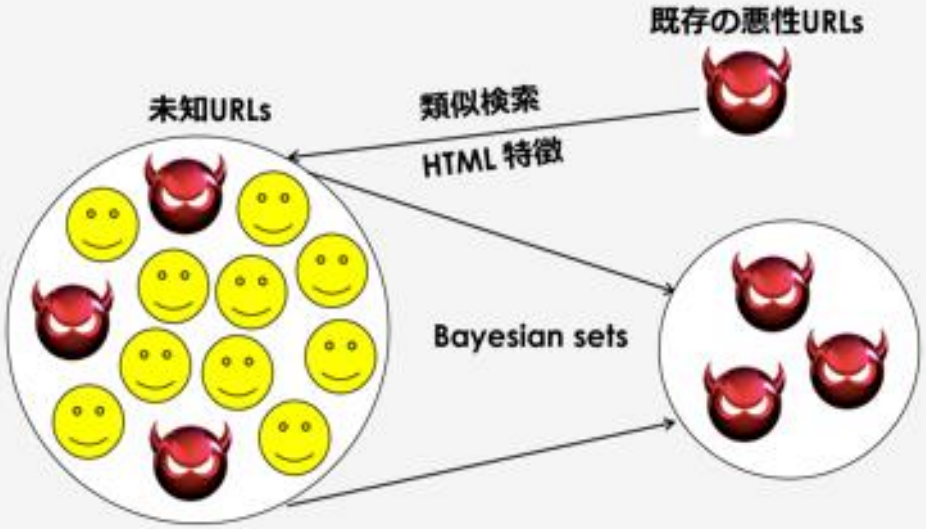


URLブラックリストの自動生成（５）

- URL拡張部



- URLフィルター部

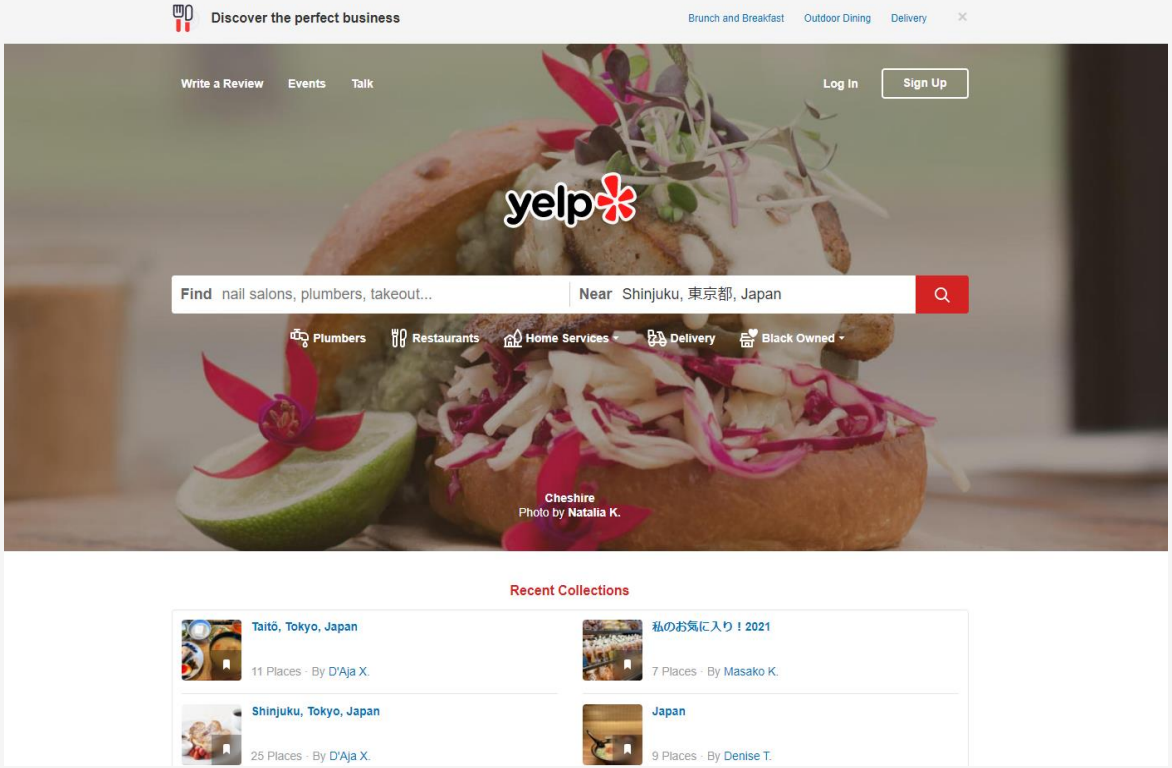


URLブラックリストの自動生成（６）

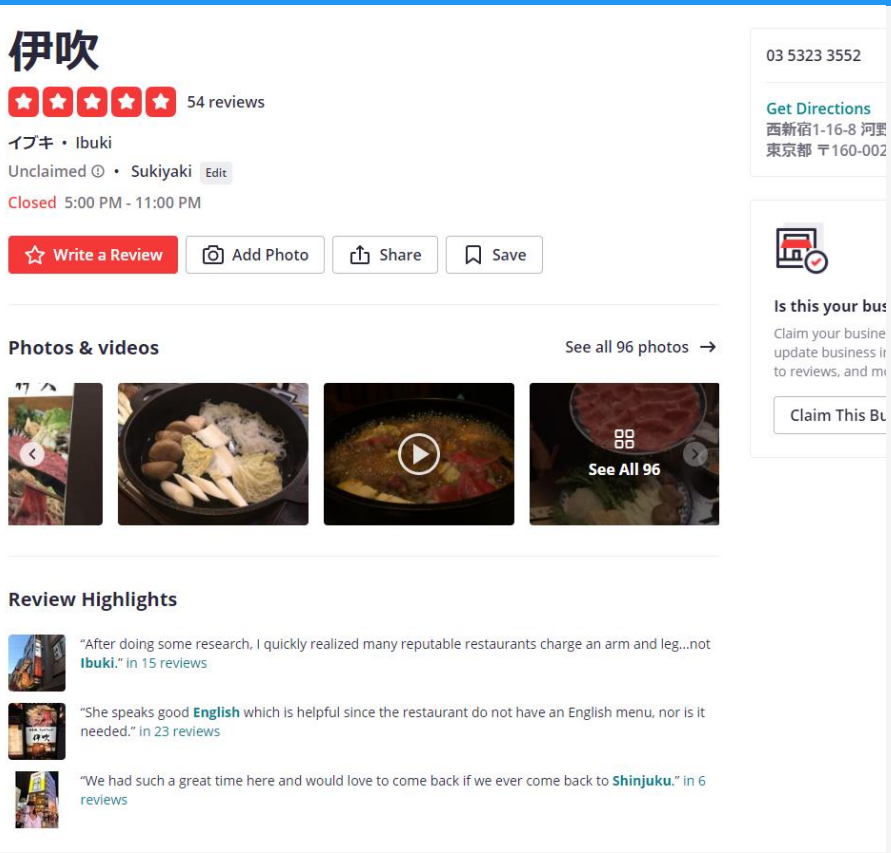
- 抽出結果
  - ✓クライアント型ハニーポット:
    - ➢1.16%, **確実に悪性**
    - ➢エクスプロイトのウェブページへリダイレクトが存在
  - ✓アンチウイルスソフト:
    - ➢3.8%, **高度に疑わしい**
    - ➢悪性のJavaScript等の静的な特徴
  - ✓ウィルストータル:
    - ➢16.5%, **疑わしい**
    - ➢ 手作業の検査が必要
- 処理時間
  - ✓URLフィルター部が利用しない場合: 合計100 hours以上
  - ✓URLフィルター部の利用: 合計約６時間

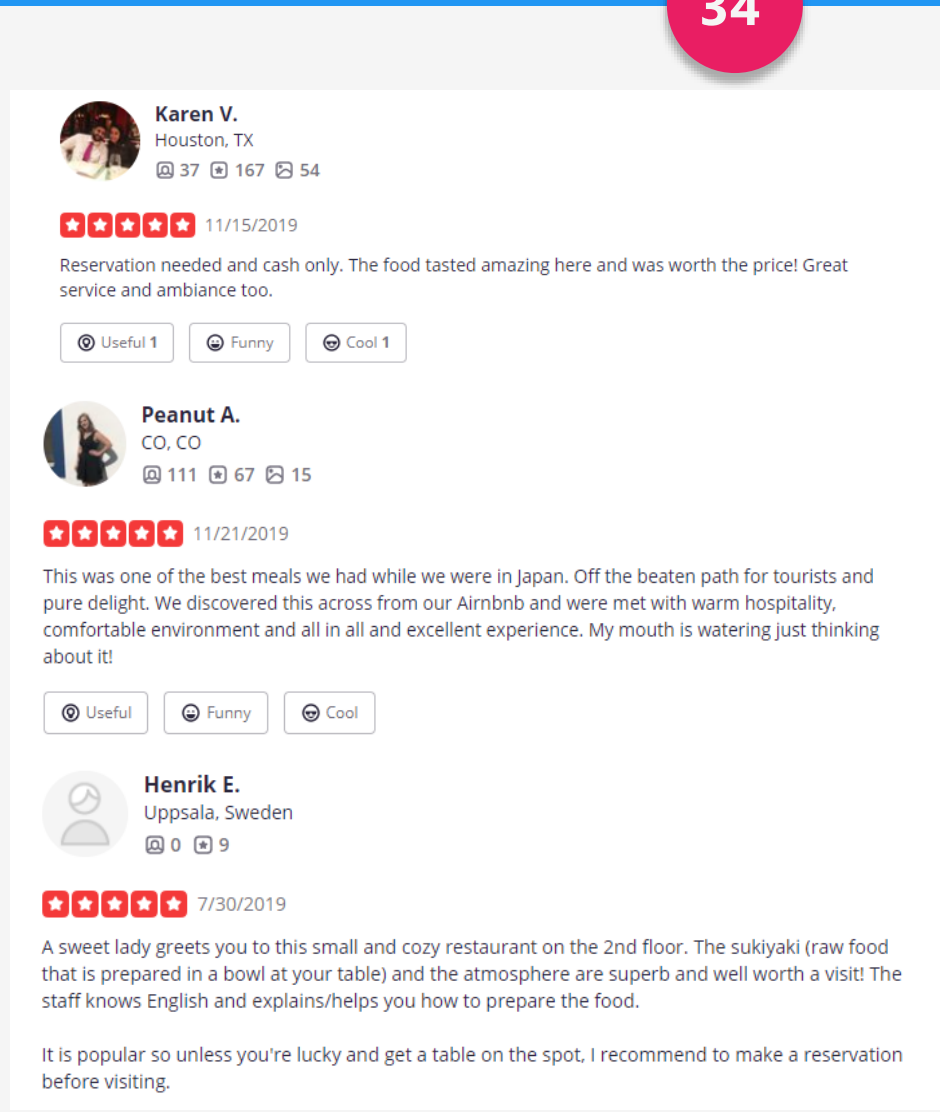
偽レストランレビューの自動生成（１）

- 背景
  - ✓各レストランを評価するためのレビューシステムがつくられている
  - ✓人を雇ってポジティブなレビューを投稿することは、レストランの評判を人為的にコントロールする手段である。



偽レストランレビューの自動生成（2）

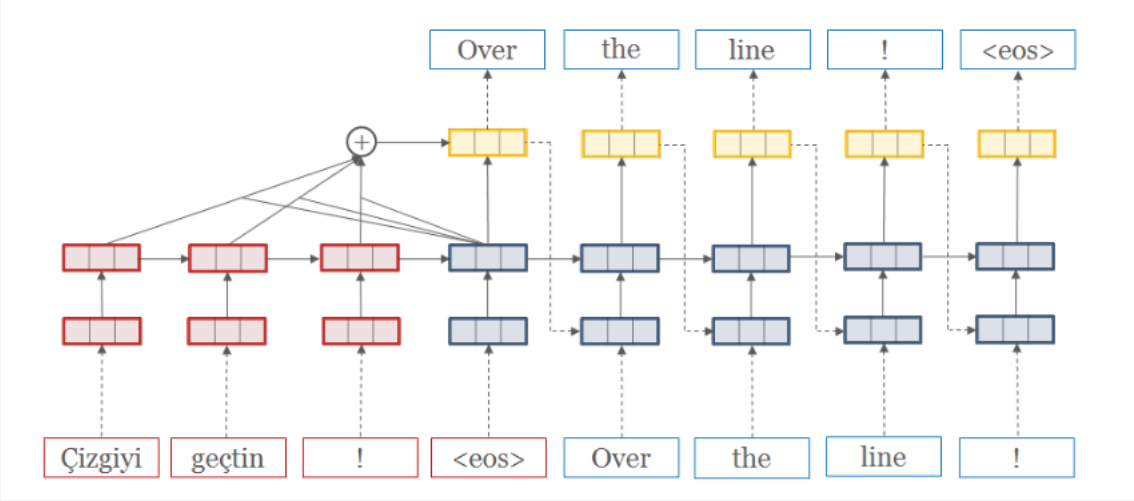




- 問題点
  - ✓コストが高い
  - ✓大規模な投稿ができない
- 目的
  - ✓トピックに沿った自然なレビューを大量に自動生成

偽レストランレビューの自動生成（３）

- 手法：ニューラル機械翻訳



- 例

5 Gina ‘ s Place
Cleveland OH
Diners Breakfast

“The best breakfast place in Cleveland. Great prices and great service. I highly recommend the homemade eggs Benedict, it’s a must try!”

偽レストランレビューの自動生成（４）

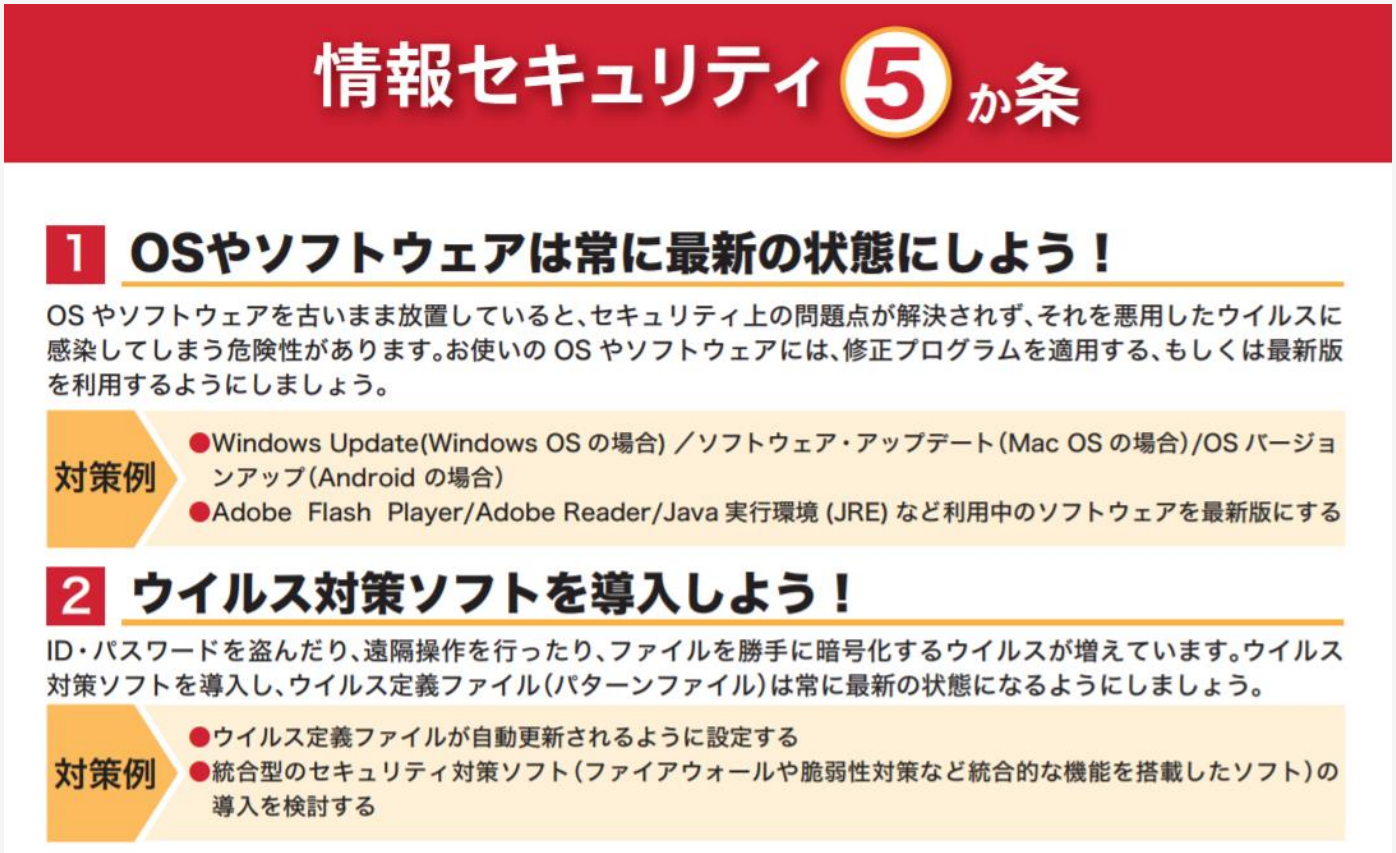
- ユーザスタディ（ Amazon mTurkersを利用 ）

Native English mTurkers detection rate					
I	II	III	IV	V	VI
45%	**40%**	55%	50%	57%	50%

- 対策
  - ✓特徴：n-gram, part of speech, readability score
  - ✓AdaBoostを用いた検知モデル
  - ✓F1-score : **97%**

中小企業のセキュリティ対策（１）

- 最低限の対策としては、下記の５項目を実施すること



出典：情報処理推進機構、情報セキュリティ5か条　https://www.ipa.go.jp/files/000055516.pdf

中小企業のセキュリティ対策（２）

3 パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。

対策例

- パスワードは英数字記号含めて10文字以上にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない

4 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

対策例

- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク（NAS）などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更（削除）漏れがないように注意する

5 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例

- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

出典：情報処理推進機構、情報セキュリティ5か条　https://www.ipa.go.jp/files/000055516.pdf

中小企業のセキュリティ対策（３）

- 最低限の対策を講じても、まだ色々な脅威が存在する。
- 例えば、
- 従業員の情報持ち出し
- 退職者の情報持ち出し、競合他社への就職
- ホームページへの不正アクセス
- 委託した先からの情報漏えい
- 電子メール経由でのウイルス感染
- 中小企業における組織的な情報セキュリティ対策ガイドライン（https://www.ipa.go.jp/files/000014950.pdf）を活用する。

出典：情報処理推進機構、中小企業向け情報セキュリティ対策、 https://www.ipa.go.jp/security/manager/know/sme-guide/sme-security_guidline.html

中小企業のセキュリティ対策（４）

- セキュリティ専門の会社が提供している対策サービスを利用する
- NTT com、Cisco Systems、NRI、Lac、FFRI
- メリット：
- 導入、利用、運用の全てが容易で、手離れも良い
- フルタイムで働くセキュリティ研究者やエンジニアが在籍
- デメリット：
- 費用が発生する

ご清聴ありがとうございました

画像引用：https://www.theastuteadvisor.com/davids-personal-finance-qa-february-2017/

参照元

- https://cybersecurity-jp.com/security-measures/17886#i
- https://www.mbsd.jp/blog/20170518.html
- https://thinkit.co.jp/article/13332
- https://www.atmarkit.co.jp/ait/articles/1504/27/news032.html
- https://www.lac.co.jp/lacwatch/alert/20200907_002276.html
- https://www.tku.ac.jp/iss/environment/security/security/phishing.html
- https://www.fujitsu.com/jp/innovation/security/column/06/
- https://bp-affairs.com/news/2018/10/20181005-8119.html
- https://cybersecurity-jp.com/security-measures/18646
- https://it-trend.jp/cyber_attack/article/problem
- https://www.ipa.go.jp/files/000043331.pdf
- https://www.soumu.go.jp/main_content/000722477.pdf
- https://www.ipa.go.jp/security/manager/know/sme-guide/sme-security_guidline.html