



これから始めるテレワーク ～気になるセキュリティの第一歩～

トレンドマイクロ株式会社
ビジネスマーケティング本部
吉田 睦



本日のアジェンダ

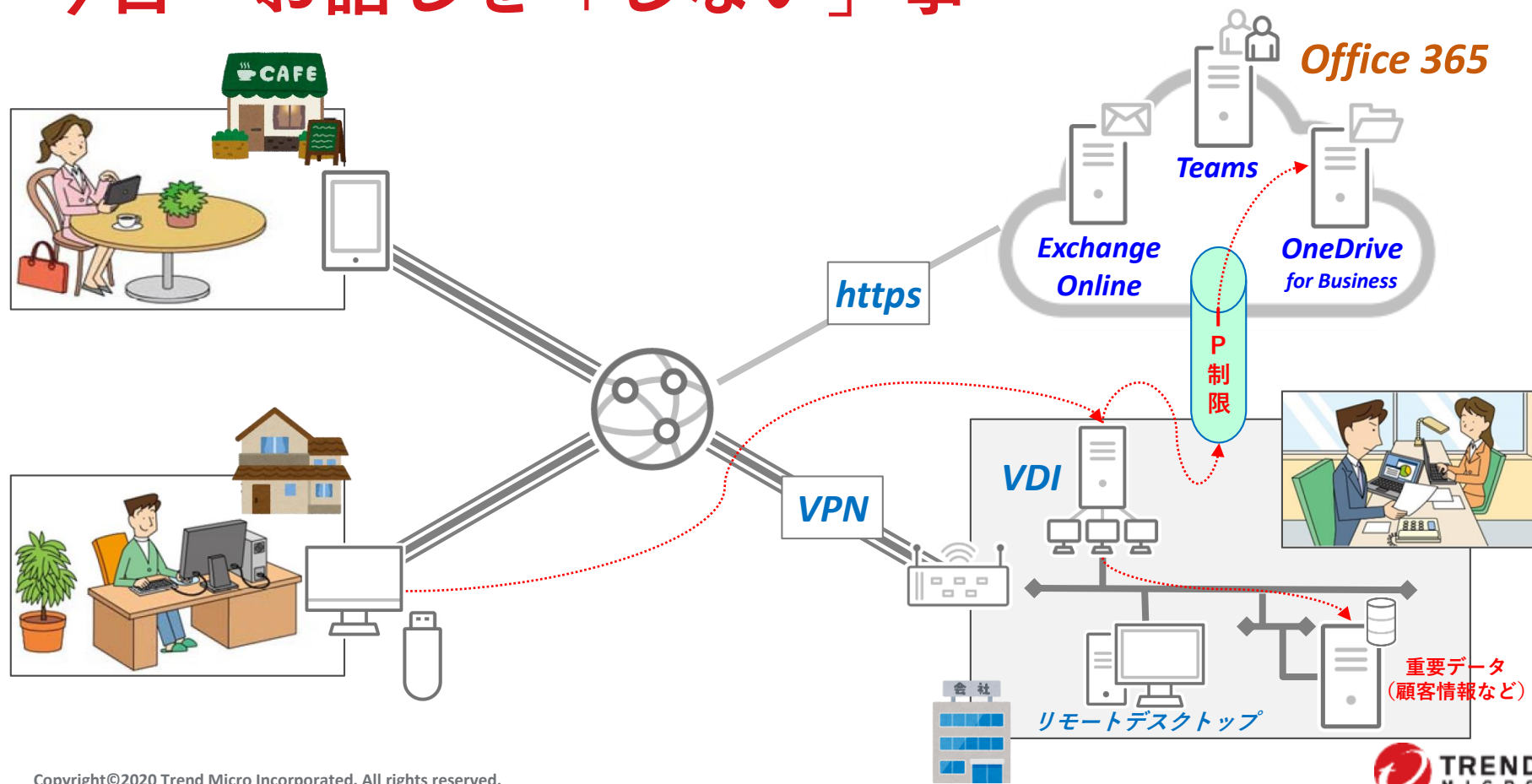
- これから始めるテレワーク
セキュリティの勘所【セキュリティ管理者編】
- これから始めるテレワーク
セキュリティの勘所【テレワーカー編】



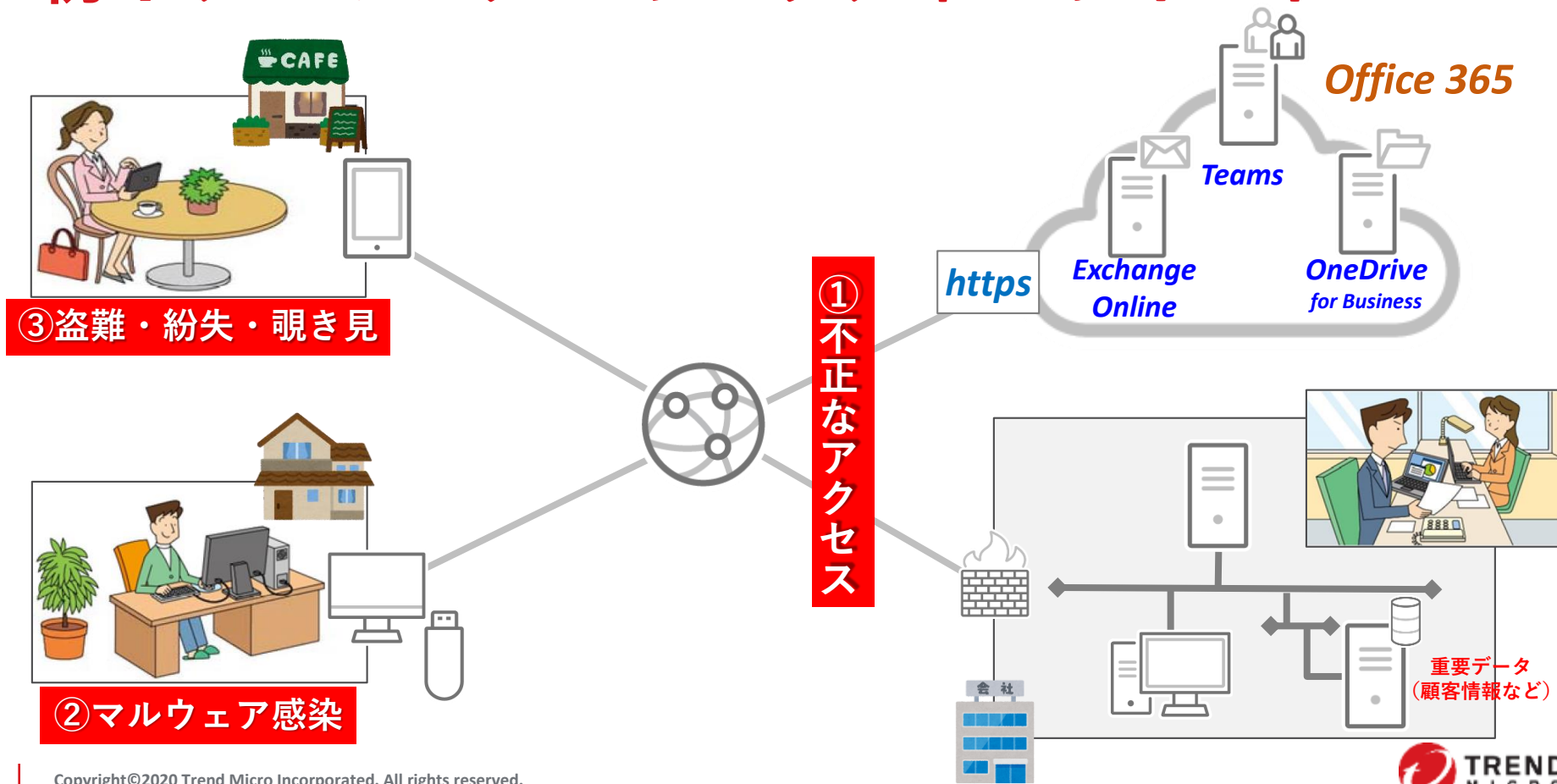
【セキュリティ管理者編】

これから始めるテレワーク
セキュリティの勘所

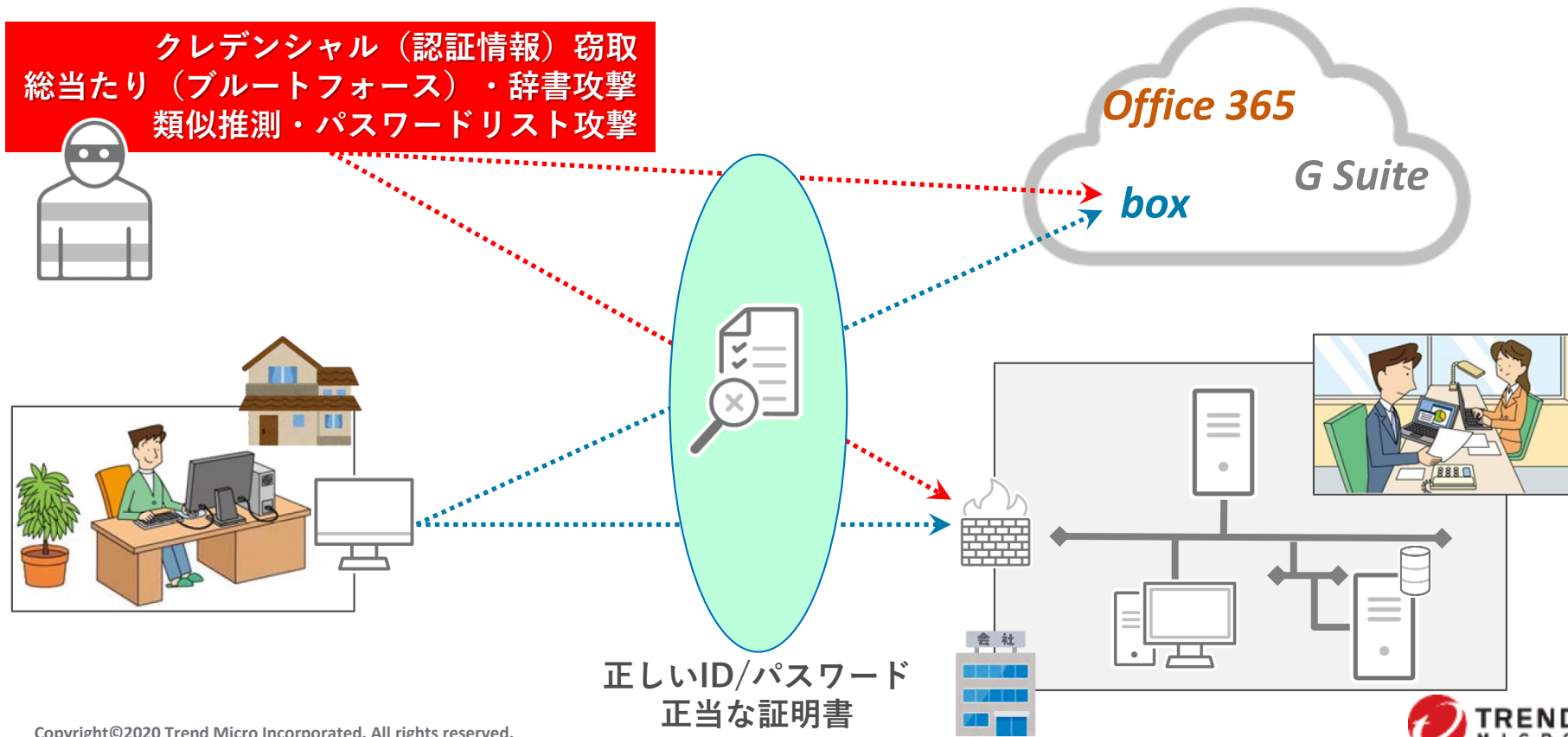
今日 お話を「しない」事



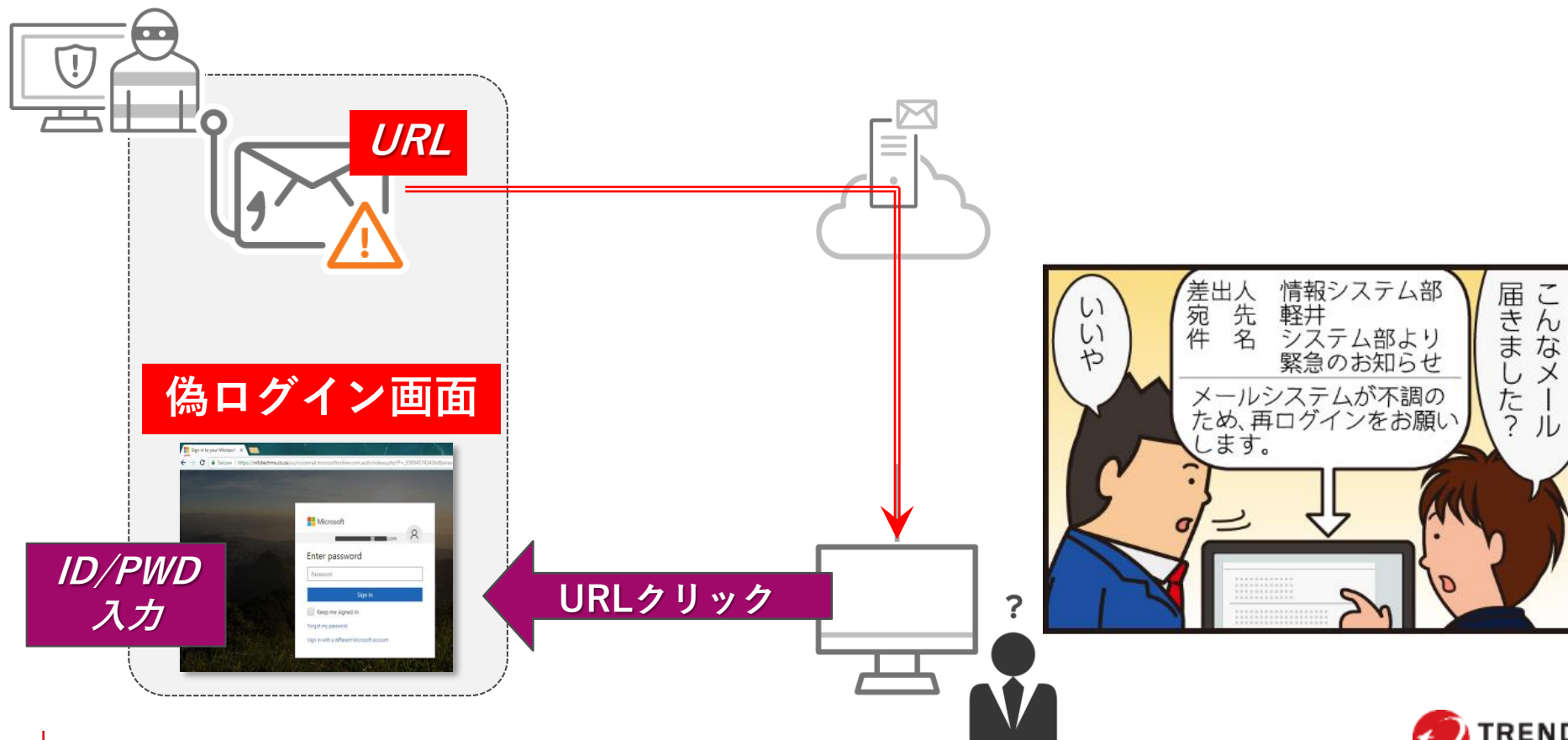
初！テレワークセキュリティのポイント



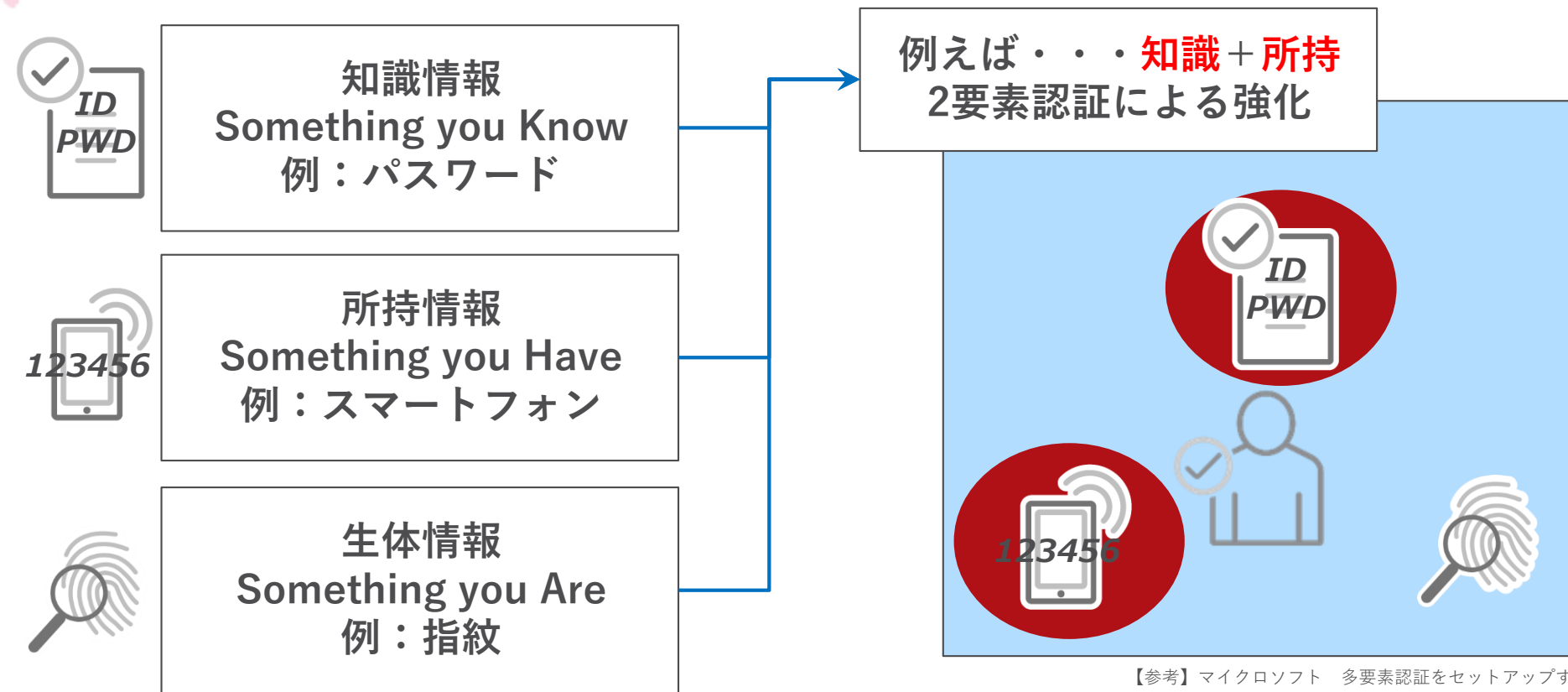
外部からの不正アクセスを防ぐ



クレデンシャルフィッシング(認証情報)の窃取例



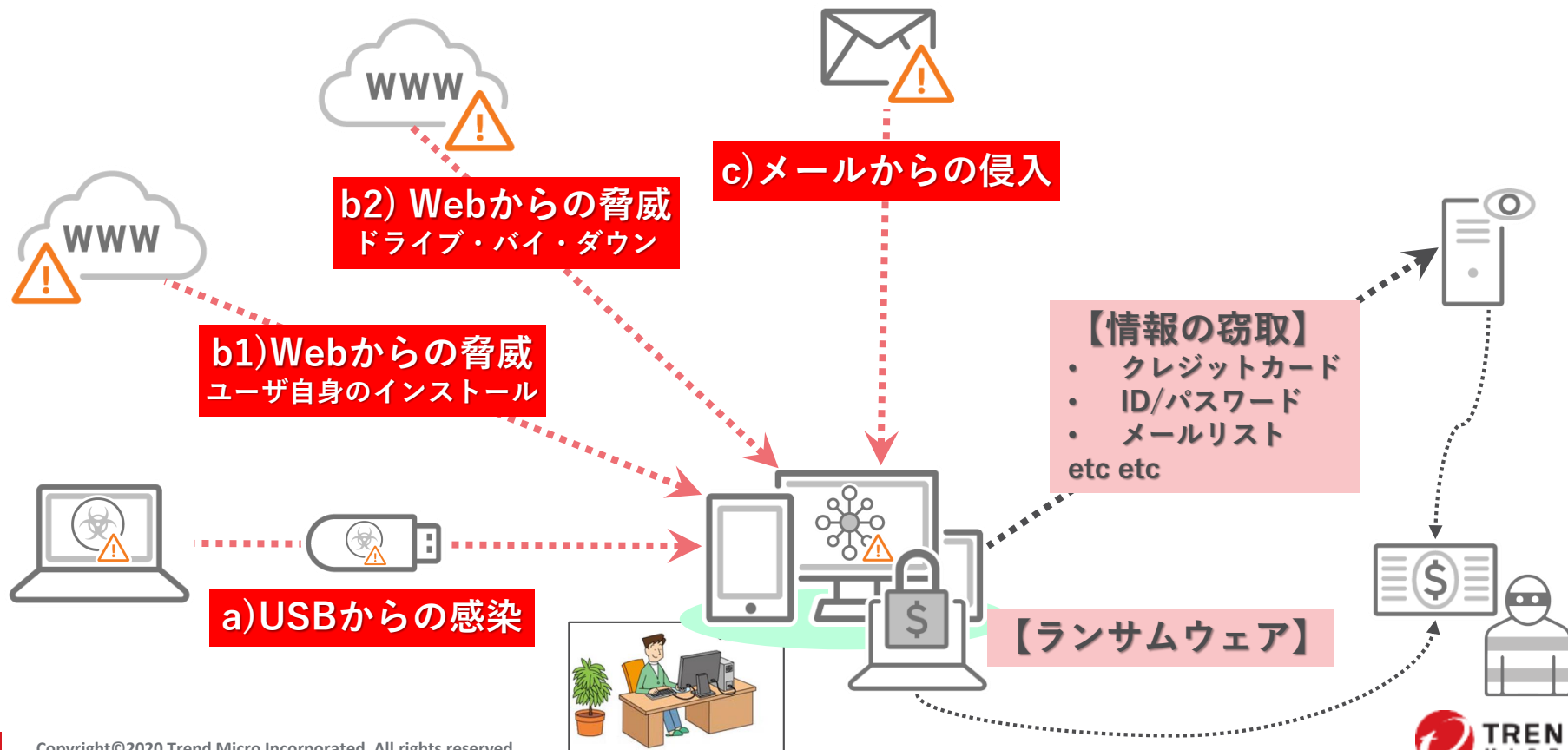
多要素認証による利便性と安全性の両立



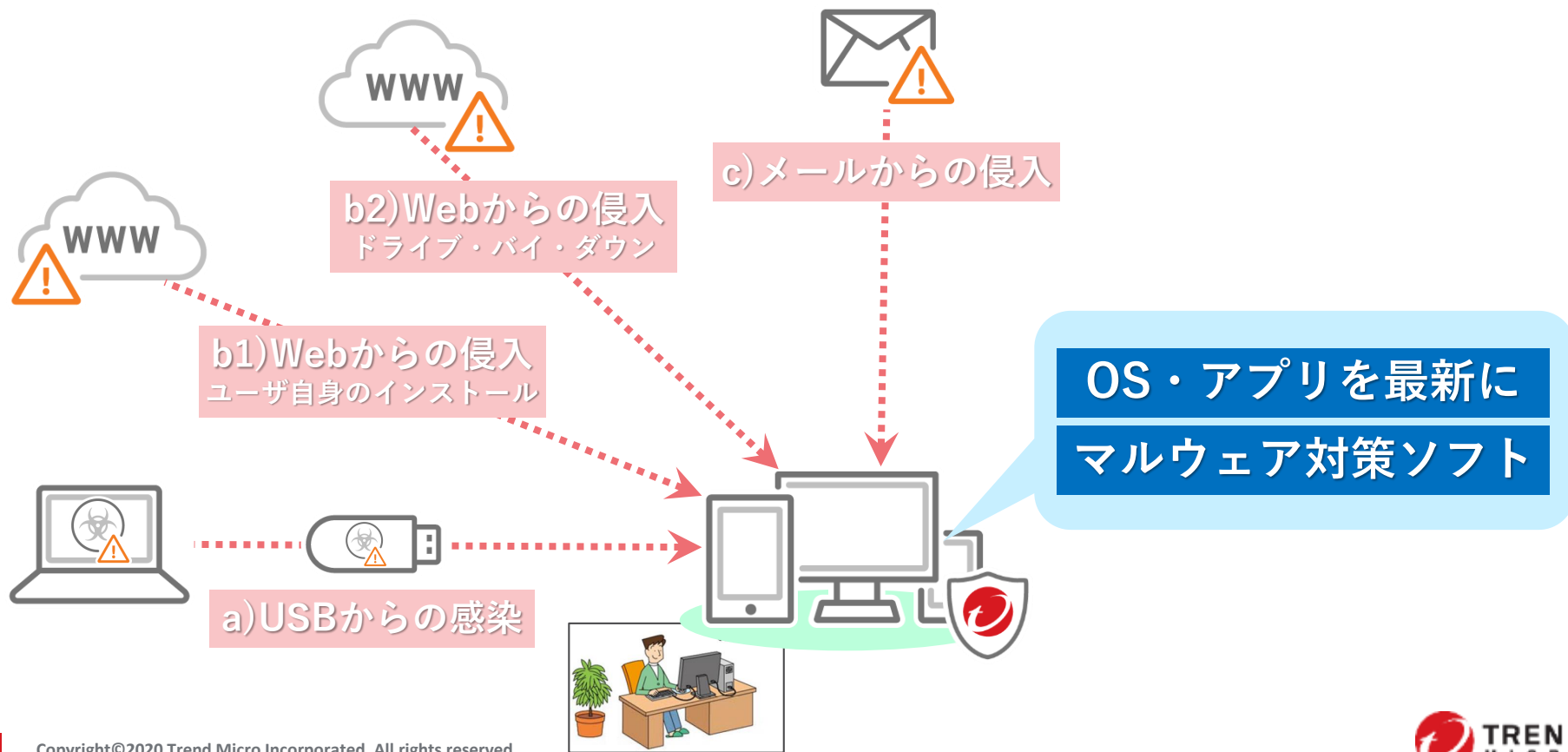
【参考】マイクロソフト 多要素認証をセットアップする

<https://docs.microsoft.com/ja-jp/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication>

マルウェアはどこから来るのか？



感染対策のための管理者初めの一步



最新Verのための自動アップデート

【Trend Micro ApexOne自動アップデートの設定】

<https://success.trendmicro.com/jp/solution/1301642#apex>

エージェント自動アップデート

特定のイベントが発生した時点、または予約された日時にエージェントを自動的にアップデートします。

イベント起動配信

- ☒ Apex Oneサーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントを更新します。
- ☐ スタンドアロンモードおよびオフラインモードのエージェントを含む。
- ☒ 再起動時、またはApex Oneサーバへの接続時にコンポーネントアップデートの開始を許可します。
- ☐ アップデート後、ScanNowを実行する（スタンドアロンモードのエージェントを除く）。

予約アップデート

分
時間
☒ 毎日
毎週 日曜日

開始時刻 00 : 00 (時分)
アップデートの開始: 4 時間以内

保存 キャンセル

【Windows 10自動アップデートの設定】

https://www.is702.jp/manga/3355/partner/12_t/

Windows Update

一部の設定は組織によって管理されています。

再起動が必要です
お使いのデバイスは、アクティブ時間外に再起動されます。

2018-06-x64 ベース システム用 Windows 10 Version 1803 の累積更新プログラム (KB4284848)
状態: 再起動の保留中

今すぐ再起動する 再起動のスケジュール

アクティブ時間の変更
更新の進捗を表示する

アクティブ時間

このデバイスを通常いつ使うかを知らせるアクティブ時間を設定します。アクティブ時間中は自動的に再起動せず、使用中かどうかを確認せずに再起動することはありません。

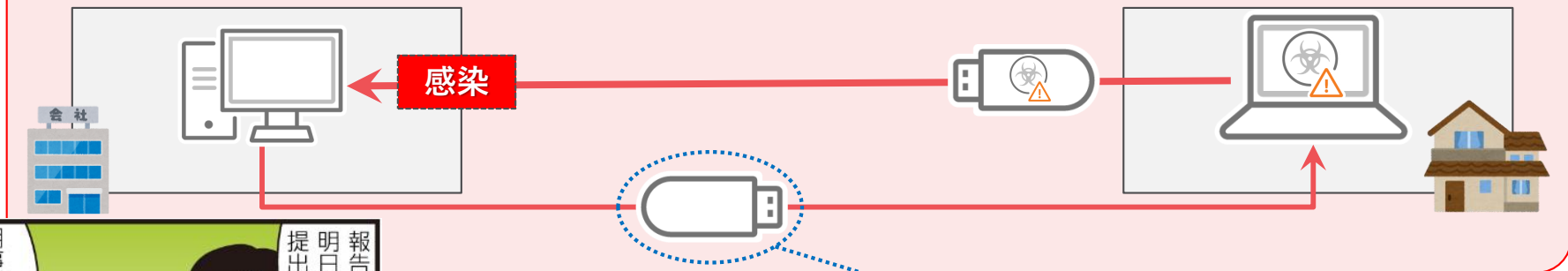
開始時刻 8 00
終了時刻 (最大 18 時間) 22 00

保存 キャンセル

※ OSやアプリのバージョンアップによって、アプリが影響を受ける時があります。
特にメジャーバージョンアップは、確認の上実行されるのが良い時があります。

a)USBからの感染を防ぐ

私物・未認可のUSBは使用禁止



会社で準備する
ウイルス対策USBのみ使用

デジタルライフ、もっと簡単に
BUFFALO

株式会社バッファロー

I-O DATA

株式会社アイ・オー・データ機
器

ed-contrive
MAKE YOUR FUTURE LIFE

イーディーコントライブ株式会
社

GREEN HOUSE

株式会社グリーンハウス

JMC

株式会社JMC

ELECOM

エレコム株式会社

SECURDRIVE

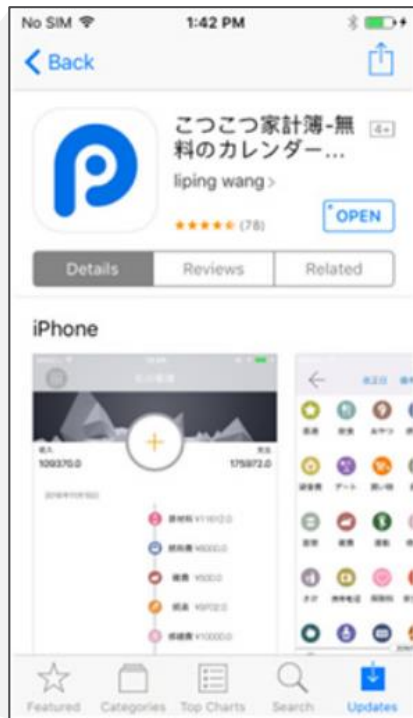
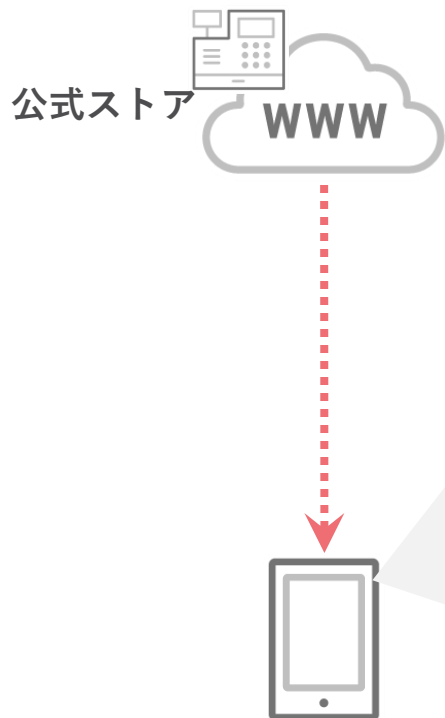
セキュドラライブ株式会社



Webからの脅威例 1

b1) App Storeで配布されていた不正アプリの一例

(注：正規アプリ「こつこつ家計簿-無料で簡単 人気のカレンダー家計簿」とは別のものです。)



業務に不要なアプリは
インストールしない

Webからの脅威例 2

b2) ドライブ・バイ・ダウンの例

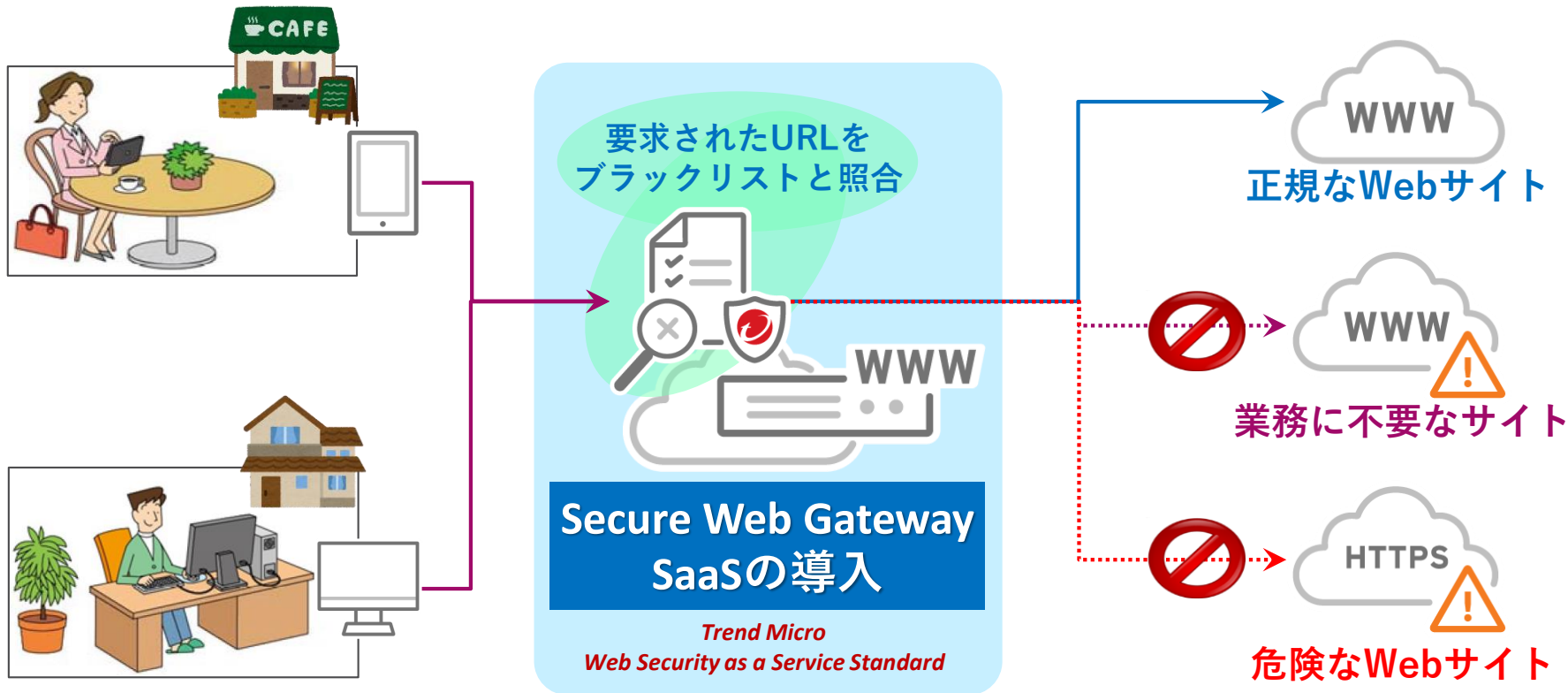
PCのアプリ脆弱性を超えて、閲覧しているだけなのに
ランサムウェアがインストールされている

右側のプロセスエクスプローラを
見ると、不正プログラムが自動的
にインストールされている



OS・アプリを最新に

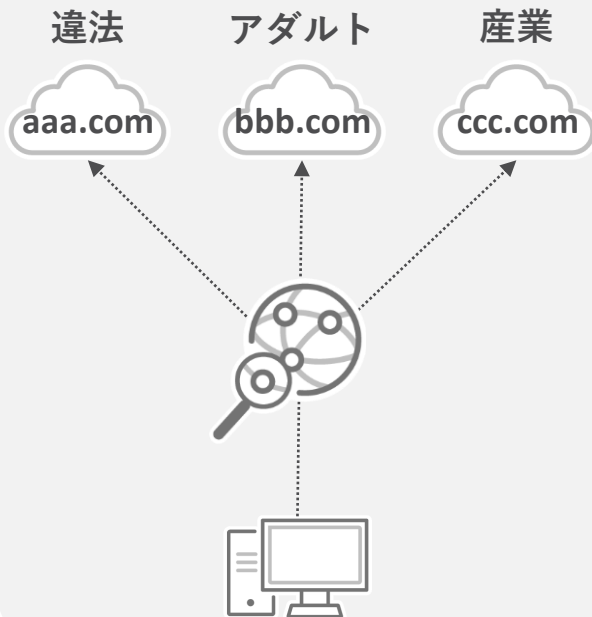
管理者としてWebの脅威に対する



知っておきたい違い、似て異なるモノ

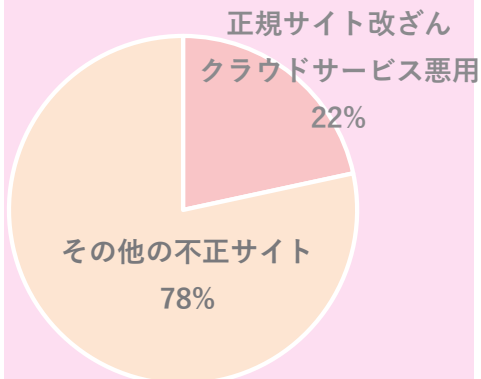
【Webフィルター】

Webサイトを**種類別に分類**



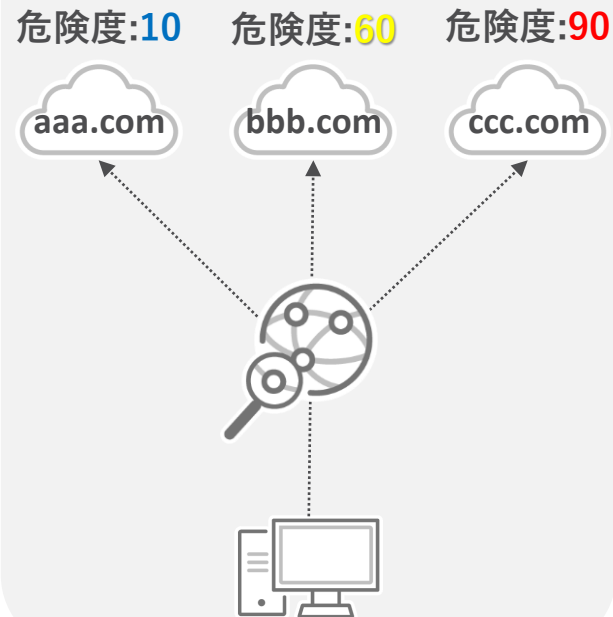
Q 1 : 社内セクハラ防止に
アダルトサイトへの接続を
止めたい

Q 2 : C&Cサーバへの
接続を止めたい

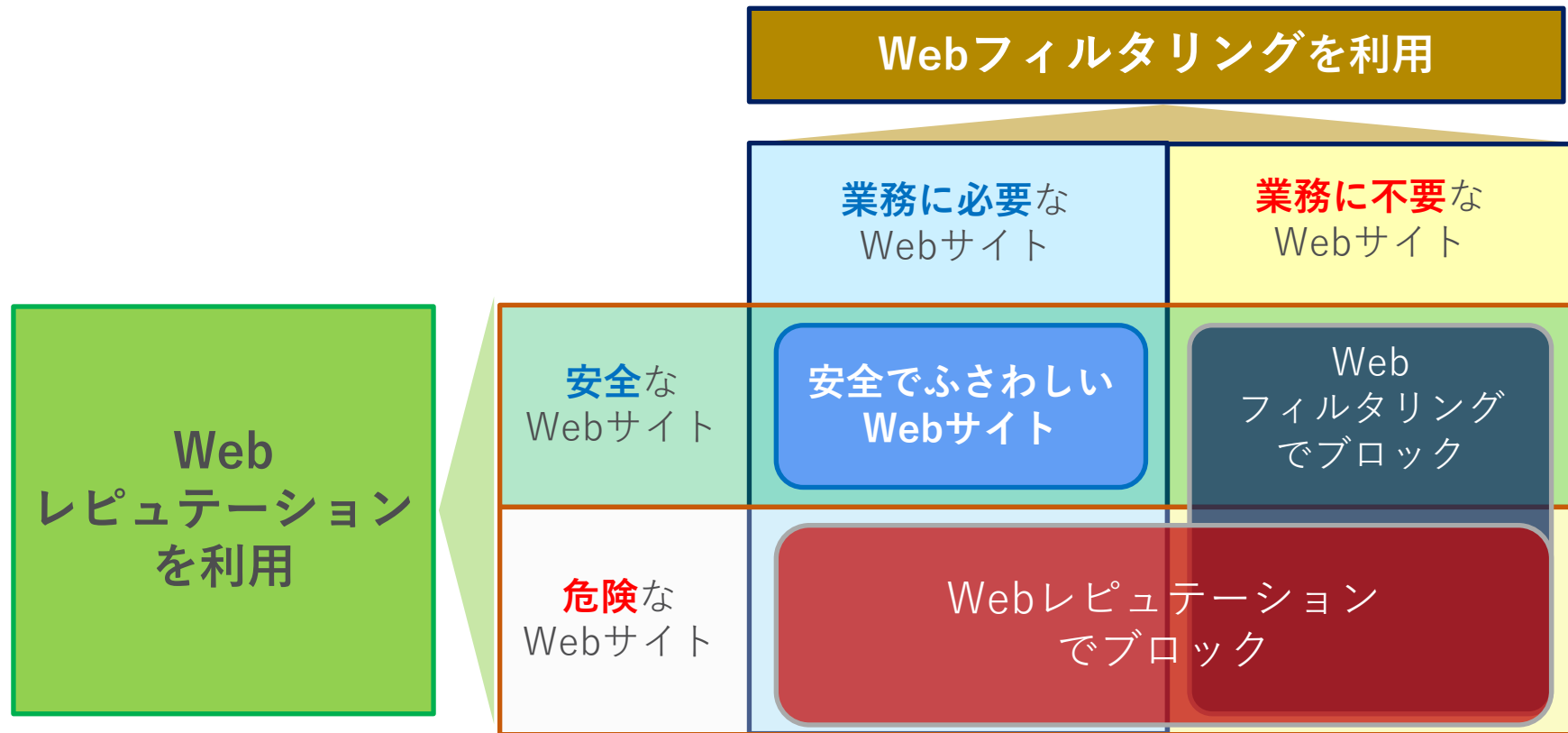


【Webレピュテーション】

Webサイトを**危険度を得点化**



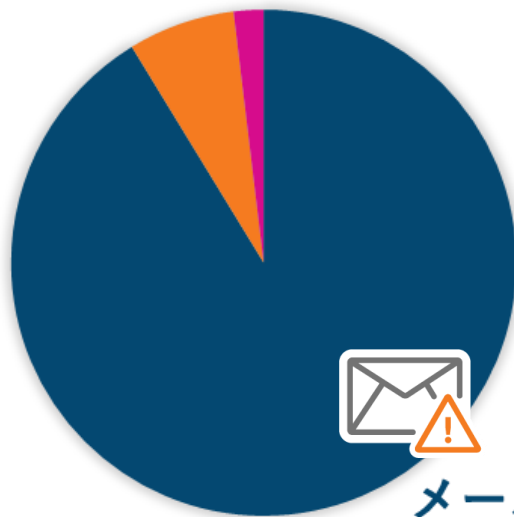
兼用が脅威対策と業務効率化に有効



メール経由の脅威が全体の9割以上

■図：トレンドマイクロ製品で検知した脅威総数のレイヤー別割合（2019年、全世界）

Webの脅威：2%
ファイルの脅威：7%



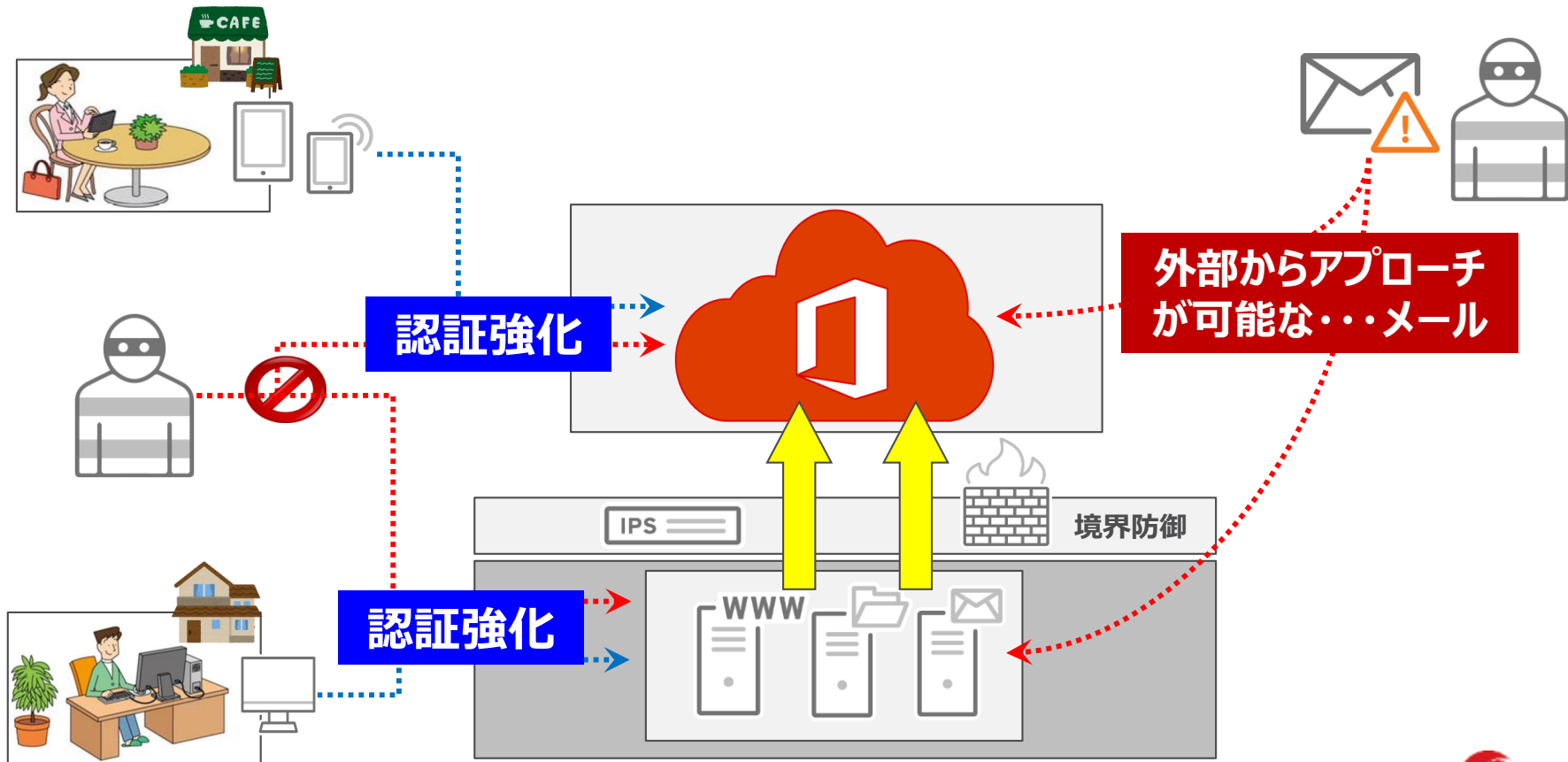
メールの脅威：91%

2019年年間のメール脅威数

477億

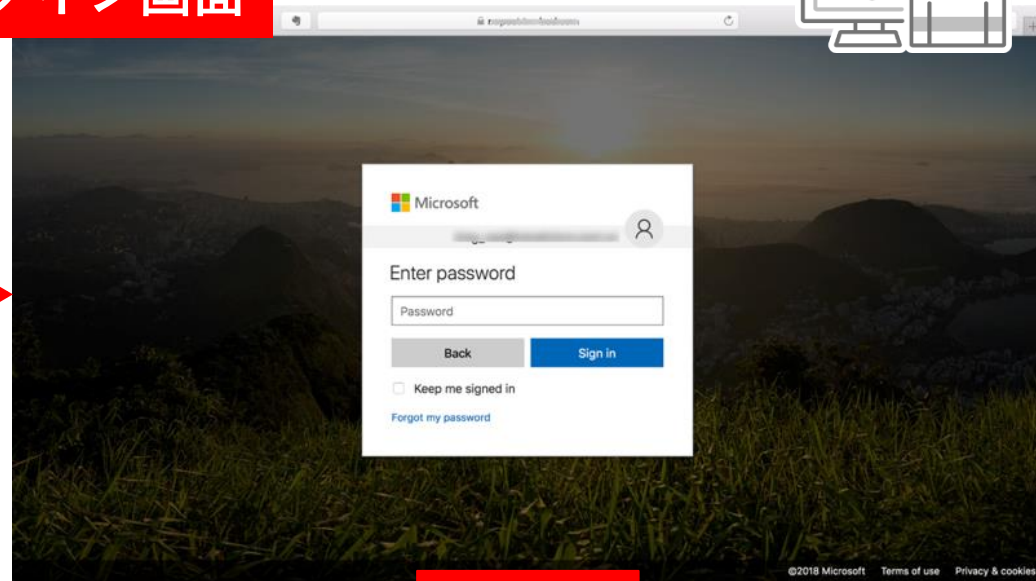
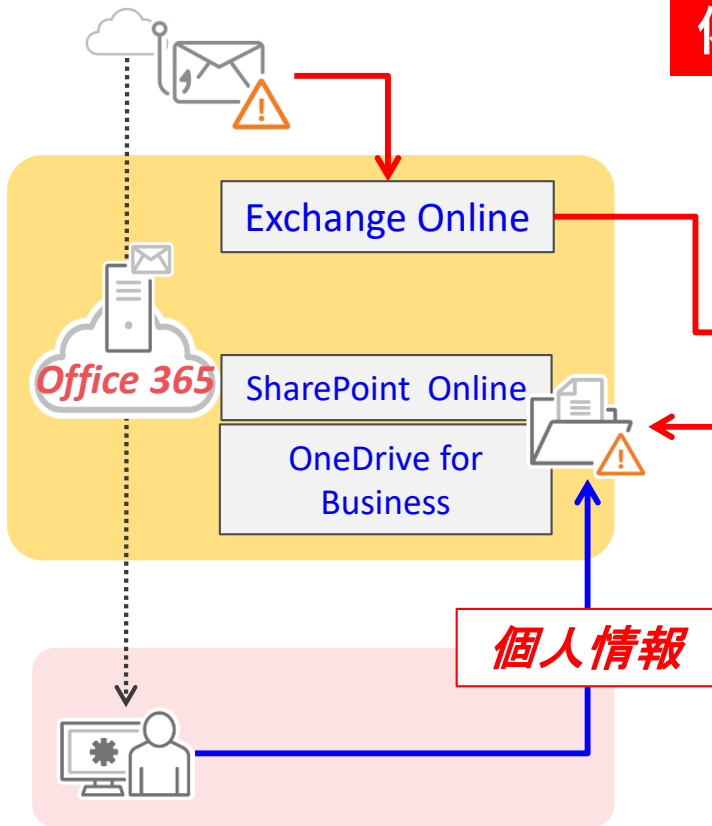
- ① EMOTET
- ② 標的型サイバー攻撃
- ③ ランサムウェア
- ④ クレデンシャル・フィッシング
- ⑤ ビジネスメール詐欺 (BEC)

何故、



認証情報窃取からの情報漏えい事例

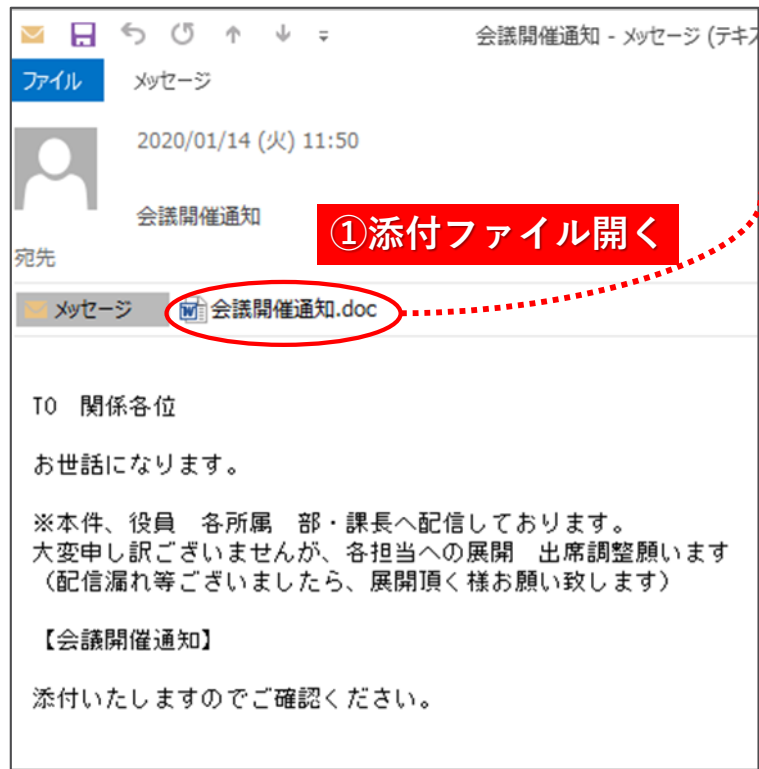
偽ログイン画面



ID/PWD

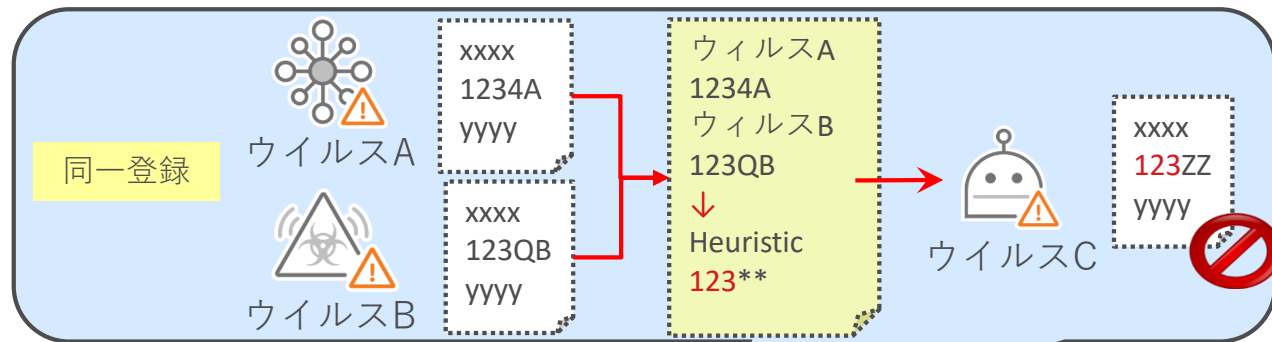
- ・ 利用して良いクラウドサービスの選定
- ・ クラウドサービスで保存して良いデータの種別ルール化

メール添付ファイルからの感染例



**③感染⇒EMOTET
ダウンロード**

対策ソフトウェアをすり抜ける新種ウイルス



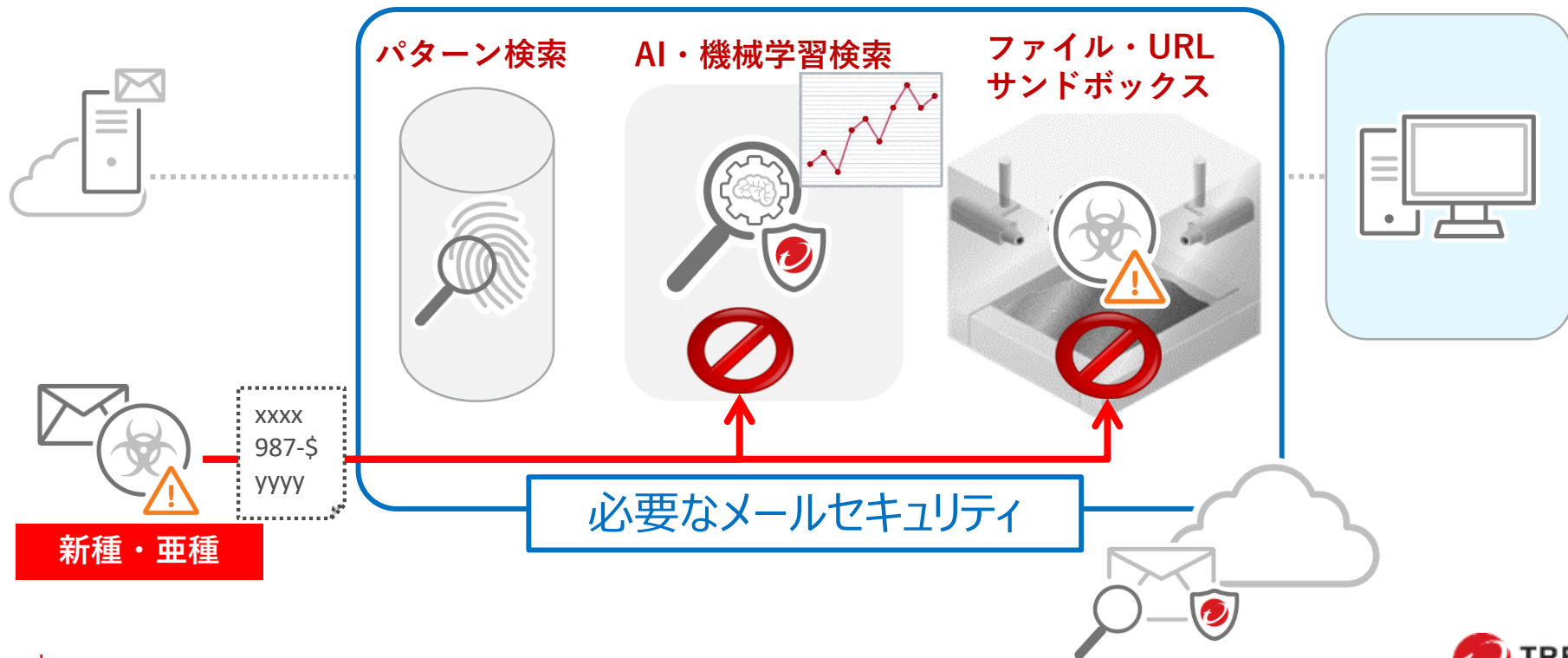
既知

新種・亜種

メールセキュリティウイルス対策
(パターン検索)

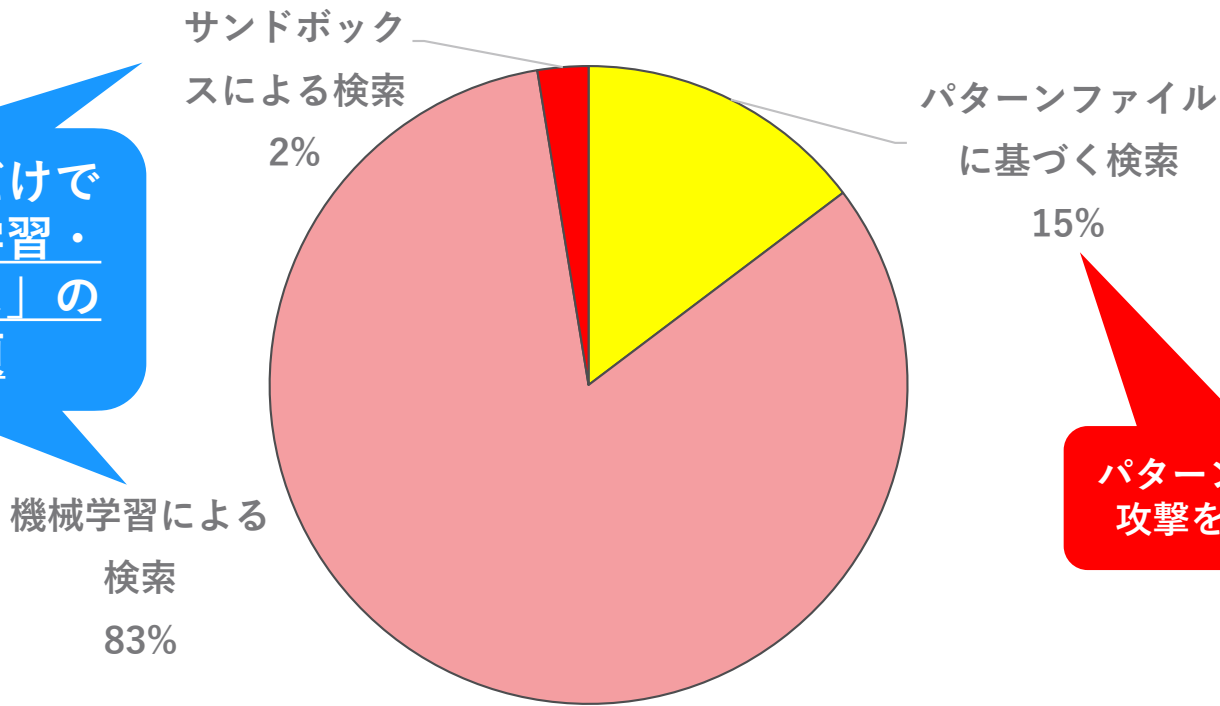
着弾

新技術による新種ウイルスの検知



検証結果例：EMOTET検出テクノロジー

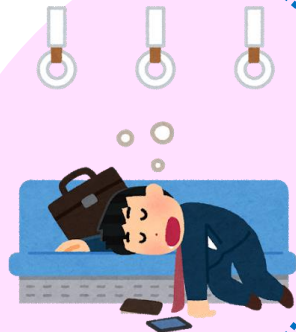
パターン検索だけではなく「機械学習・サンドボックス」の搭載は必須



パターン検索だけでは攻撃を止められない

社外で使うものだから

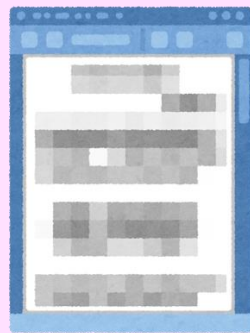
紛失



盗難



パソコンHDD
の暗号化



盗み見



プライバシー
スクリーンの採用



もしもの事故発生時、原因を追跡するために

Office 365 の監査ログ設定画面例

Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Turn on auditing

Search

Clear

Activities

Show results for all activities

Start date

2019-09-23 00:00

End date

2019-10-01 00:00

Users

Show results for all users

File, folder, or site

Add all or part of a file name, folder name, or URL.

Search

Results

Date	IP address	User	Activity	Item
------	------------	------	----------	------

監査ログ(Audit Log)は
必ずオンに

<https://docs.microsoft.com/ja-jp/microsoft-365/compliance/turn-audit-log-search-on-or-off>



【テレワーカー編】

これから始めるテレワーク
セキュリティの勘所

対策を踏まえたテレワーカーの「すべき事」

ルール化

公知・教育

自覚・遵守

	管理者	テレワーカー
ID・パスワードの漏えい対策	外部アクセス時の多要素認証採用	推測されにくいパスワードの設定
OS/ブラウザ/アプリの最新化	自動化の検討	通知時の確実な実行
ウイルスソフトの実装・最新化	自動配布・自動アップデートの検討	通知時の確実な実行
未公認のアプリインストールの禁止	公認アプリの選定と公知	インストールの禁止遵守
未公認のUSBの利用禁止	対策済みUSBの配布と管理	利用禁止の遵守
未公認クラウドサービスの利用禁止	公認クラウドの選定と公知	利用禁止の遵守
公認クラウドサービス漏えい対策	クラウドで保存して良いデータ種別のルール化	ルールの遵守
紛失・盗難・覗き見への対応	HDD暗号化検討とフィルター配布	情報資産を持っている自覚と注意
Webからの脅威対策	Secure Web Gateway の採用検討	業務上不要なWebへの接続をしない 証明書の確認(Page29)
なりすましメールによる侵入対策	最新技術を含むメールセキュリティ多層防御	メール送信者の確認(Page29)
自宅ルータ (Wi-Fi)の安全性	ルールの設定	後述(Page30)
外出時のネットワーク接続の安全性	会社公認のモバイルルータの貸与	後述(Page31)

メールやWebのちょっと確認ポイント

【マウスオンで送信者を確認】



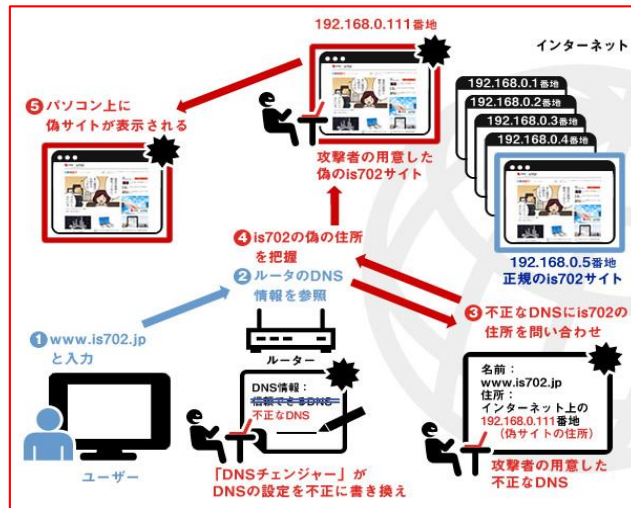
【マウスオンで証明書を確認】



自宅の



乗っ取られたルータのリスク



- ❑ Wi-Fi（ルータ）のIDとパスワードは初期値から必ず変更
- ❑ Wi-Fiの通信暗号化を「WPA2」に、（機器が対応していれば）「WPA3」に
- ❑ 常に最新の状態に
 - ❑ （設定可能な機器なら）ファームウェアは自動アップデートを設定
 - ❑ サポート切れのハードウェアは、残念ながら買い替えを

外出時のネットワーク接続のポイント



- 会社から貸与されるモバイルルータや貸与スマホのデザリング機能を使うことが基本
- (使わざろう得ない時) 「信用できる公衆Wi-Fi」を選択
 - 携帯電話事業者の公衆Wi-Fi
 - 事業者による「公衆Wi-Fiのエリアサイン」があり、ユーザID／パスワードの入力、セキュリティに関するお知らせなどがきちん行われている公衆Wi-Fi
- 一時的に接続したWi-Fiの「自動接続をしない設定」をする
- 公衆Wi-Fiでは出来る限り、**重要な情報 (*) は送信しない**
(*個人・機密情報、ログイン、クレジットなど金融情報 etc)

is702：セキュリティお役立ち情報

<https://www.is702.jp/>



is702はトレンドマイクロが提供するインターネットを安全に楽しむためのセキュリティ情報サイトです。

is702について ニュース 特集 4コマ漫画 パートナープログラム 学習資料ダウンロード



親子の話し合いとルール作りが大切
お子さんをネットの危険から守るために保護者ができる対策とは

お子さんをネットの危険から守ることは保護者の務めです。まずはネットの危険を知り、お子さんへの教育とルール作り、セキュリティ製品を用いた対策を行いましょう。

2020/03/26

続きを読む→

特集



不要になったアプリを削除していますか？
スマホをより便利に使いこなすための4つのアプリ整理術

スマホを長く使い続けたいと、インストールしたアプリでホーム画面が散らかりがちです。使わなくなったアプリは削除し、バッテリーやストレージ容量の無駄遣いを防ぐだけでなく、



SNSのアプリ連携に思わぬ落とし穴
SNSのアカウント乗っ取り対策ともしものときの対処法

SNS上で不要なアプリ連携は禁物です。連携対象となるアプリの中には、SNSアカウントの乗っ取りを目的とする不正アプリも含まれます。不正アプリとの連携を防ぐための2...

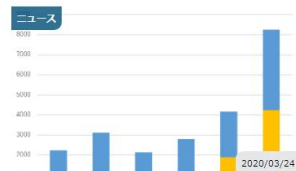


スマホからモニタリングされる！？
ストーカーウェアから身を守るための自衛策とは

ストーカーウェアはスマホにストーカーウェアをインストールされて、自分のスマホにストーカーウェアがインストールされてしまった場合、どのような被害に遭う可能性があるでしょう...

特集一覧→

ニュース



ここ数年でフィッシングサイトの傾向が変化、半数はHTTPSに対応 | JPCERT/CC

JPCERTコーディネーションセンター (JPCERT/CC) は3月19日、JPCERT/CCに報告されたフィッシングサイトの傾向について公表しました。2014年～現在...



製品のサポート終了、いつ？なにが問題？などの情報を整理 | マイクロソフト

マイクロソフトは3月12日、公式ブログで「[サイバーセキュリティ] 製品のサポートが終了したらどうなるの？」と題する記事を公開しました。同社の製品サポート...



【注意喚起】新型コロナウイルスに便乗したネット詐欺などにご注意ください

新型コロナウイルスに便乗したネット詐欺などの事例を紹介しています。同様の手口に騙されないよう、対策にお役立て下さい。

4コマ漫画



ひろしとアカリのセキュリティ事情
お子さんをネットの危険から守ろう
おじいちゃん、ツトムのネット利用状況を確認しています



ひろしとアカリのセキュリティ事情
スマホのアプリを整理しよう
ツトムはスマホのアプリを整理しているようです

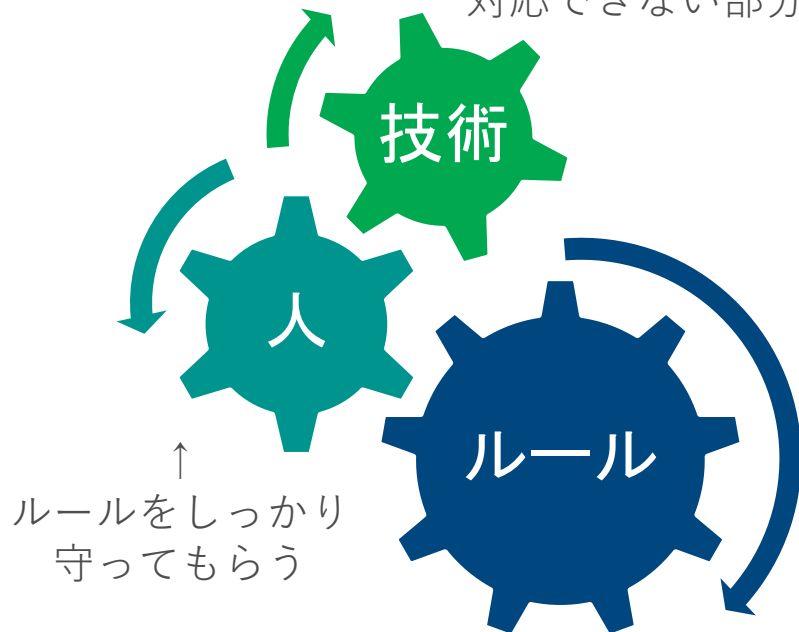


ひろしとアカリのセキュリティ事情
SNSのアプリ連携は慎重に
アカリのSNSに「ONLY FOR YOU」と書かれたダイレクトメッセージが来たようです

4コマ漫画一覧→

セキュリティを実現する要素

↓「ルール」「人」では
対応できない部分を補完



↑
ルールをしっかり
守ってもらう

↑安全を確保できる
仕事の進め方

経営者の参画・理解

テレワーク実施を考慮した
情報セキュリティポリシーの策定

情報の重要度に応じたレベル分け
と、テレワークでの利用可否判断

事故時の連絡体制確立と訓練奨励

テレワークセキュリティに必要な
人材や資源の予算確保





THE ART OF CYBERSECURITY

トレンドマイクロはセキュリティソリューションを
オンプレミスからSaaSへシフトしていきます。実際
のデータを用いて、アーティストの**Stefanie**
Posavecによって作成されました。