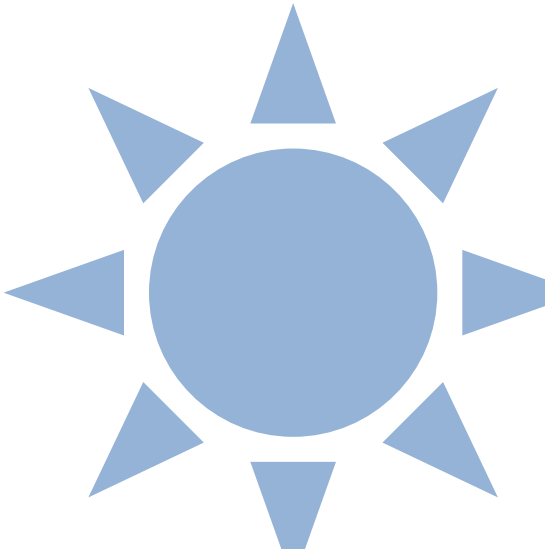
2018年度
情報セキュリティ講習会
個人と組織の情報セキュリティ対策



2018年 11月1日、2日
山田 英史（株式会社ディアイティ）

自己紹介

山田 英史（やまだ えいじ）
株式会社ディアイティ
セキュリティサービス事業部 部長

＜資格＞
CISSP
情報セキュリティ監査人補
情報セキュリティプランナー

＜業務＞
情報セキュリティコンサルティング
ISMS事務局支援
情報セキュリティ監査
情報セキュリティ教育

＜協会活動等＞
- NPO 日本セキュリティ監査協会（JASA）
  監査ツールWGリーダー
- NPO 日本ネットワークセキュリティ協会（JNSA）
  セキュリティ啓発WGリーダー
- 日本スマートフォンセキュリティ協会　幹事
- JASA-クラウドセキュリティ推進協議会
  コアメンバー
- JASA ISO/IEC 27017に基づくISMSクラウドセキュリティ認証制度 審査員研修用資料作成タスクフォースリーダー
- 情報処理安全確保支援士 講師認定委員会委員
- 情報処理安全確保支援士 講師認定講師

今日の内容

- サイバー攻撃対策
  - APT攻撃
  - ランサムウェア
  - ビジネスメール詐欺
  - セキュリティトピックス
- 個人のセキュリティ対策
  - 日常業務のセキュリティ
  - パスワードの強化
  - スマートフォンを守る
  - SNSの安全な使い方

IPA セキュリティ10大脅威

順 位	2015年	2016年（組織）	2017年（組織）
1位	インターネットバンキングやクレジットカード情報の不正利用	標的型攻撃による情報流出	標的型攻撃による被害
2位	標的型攻撃による情報流出	ランサムウェアによる被害	ランサムウェアによる被害
3位	ランサムウェアを使った詐欺・恐喝	ウェブサービスからの個人情報の窃取	ビジネスメール詐欺による被害
4位	ウェブサービスからの個人情報の窃取	サービス妨害攻撃によるサービスの停止	脆弱性対策情報の公開に伴う悪用増加
5位	ウェブサービスへの不正ログイン	内部不正による情報漏えいとそれに伴う業務停止	脅威に対応するためのセキュリティ人材の不足
6位	ウェブサイトの改ざん	ウェブサイトの改ざん	ウェブサービスからの個人情報の窃取
7位	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ	ウェブサービスへの不正ログイン	IoT機器の脆弱性の顕在化
8位	内部不正による情報漏えいとそれに伴う業務停止	IoT機器の脆弱性の顕在化	内部不正による情報漏えい
9位	巧妙・悪質化するワンクリック請求	攻撃のビジネス化（アンダーグラウンドサービス）	サービス妨害攻撃によるサービスの停止
10位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	インターネットバンキングやクレジットカード情報の不正利用	犯罪のビジネス化（アンダーグラウンドサービス）
	10大脅威2016	10大脅威2017	10大脅威2018

新規ランクイン

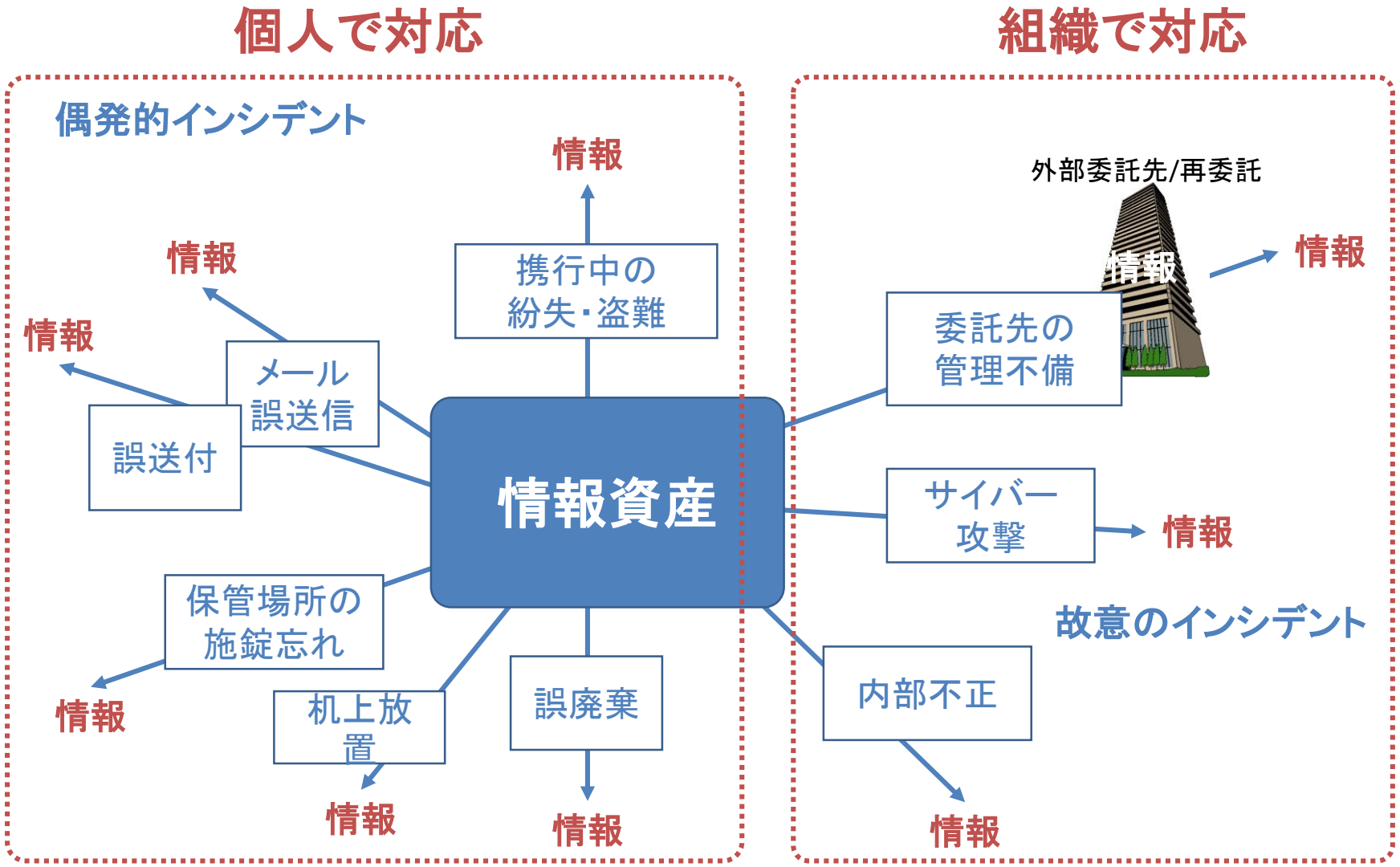
脆弱性関連	ウェブサイト関連 不正ログイン関連 パスワード関連	標的型攻撃関連	インターネット バンキング関連	情報漏えい関連 内部不正、Winny	スマートフォン 関連

IPA：独立行政法人 情報処理推進機構

セキュリティ環境の変化

攻撃目的	情報の窃取	→	金銭の窃取
攻撃対象	特定の組織	→	無差別

情報セキュリティリスクを認識する



サイバー攻撃対策

APT攻撃

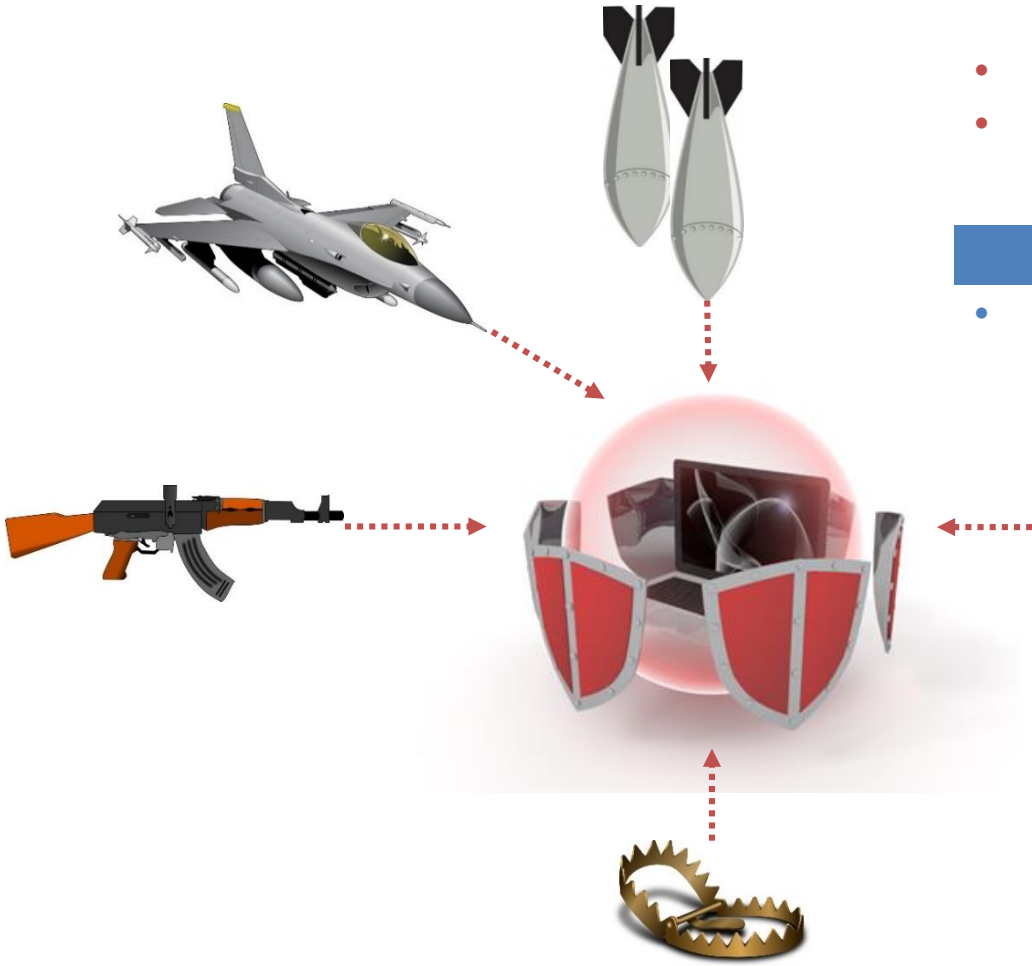
APT攻撃（Advanced Persistent Threat：継続的で執拗な脅威）

大学におけるサイバー攻撃の事例

- 大阪大学は、2017年5月18日から7月4日にかけて、教育用計算機システムが不正アクセスを受け、教員のIDとパスワードを用いて侵入され、システム内部に設置された不正プログラムにより、システム管理者のアカウントが盗まれた。
- 管理者用アカウントが奪われたことで、同システムの利用者に関する氏名やID、メールアドレス、所属、学籍番号など約7万件が流出した可能性があることを公表。
- 職員59人のアカウントが不正に利用され、同大学内のグループウェアに対する不正アクセスが行われていたことも判明。
- 対象となる関係者に対して謝罪。パスワードのルールについて強化し、全利用者のパスワードを変更した。

参考：Security NEXT

サイバー攻撃は攻める方が断然有利



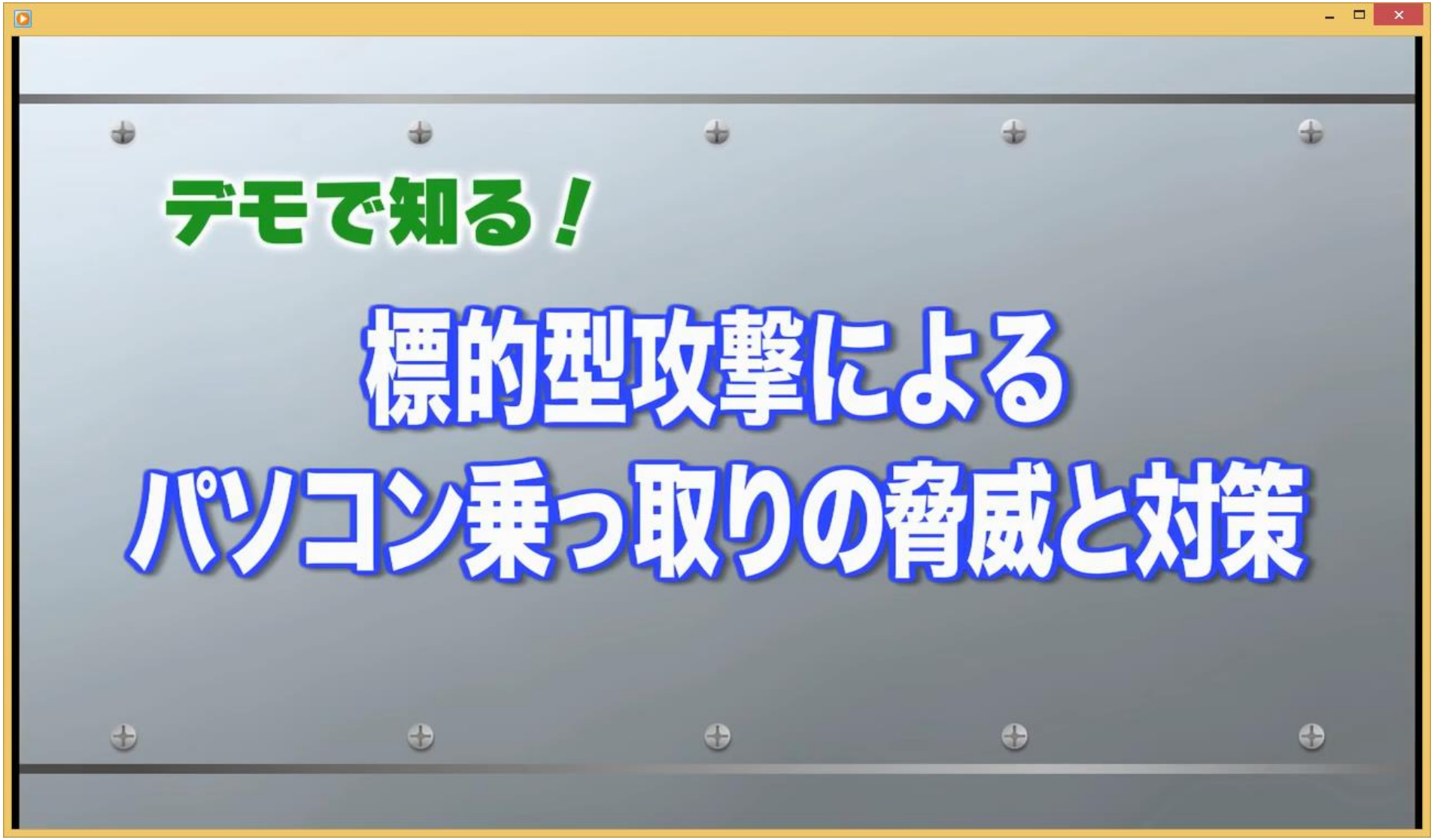
攻撃する側

- 10通りの攻撃手法があれば、
  その内1つでも成功すれば良い
- いく通りもの攻撃が低コストで試せる
- 反撃されないので失敗しても損失が無い

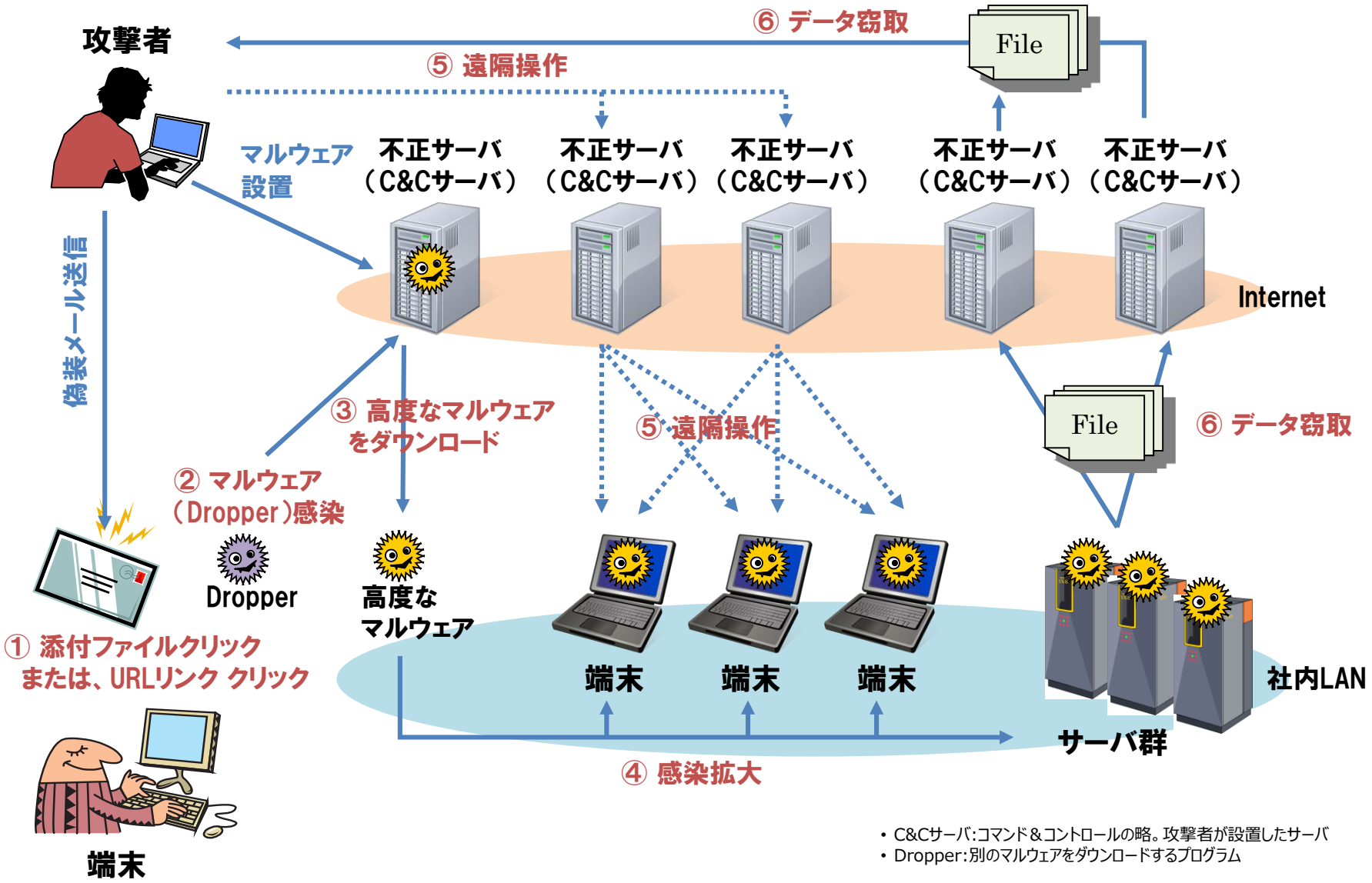
守る側

- 10通りの攻撃手法があれば、
  すべてに対抗策を講じなければいけない

ビデオ上映



標的型メールを契機にしたサイバー攻撃の流れ



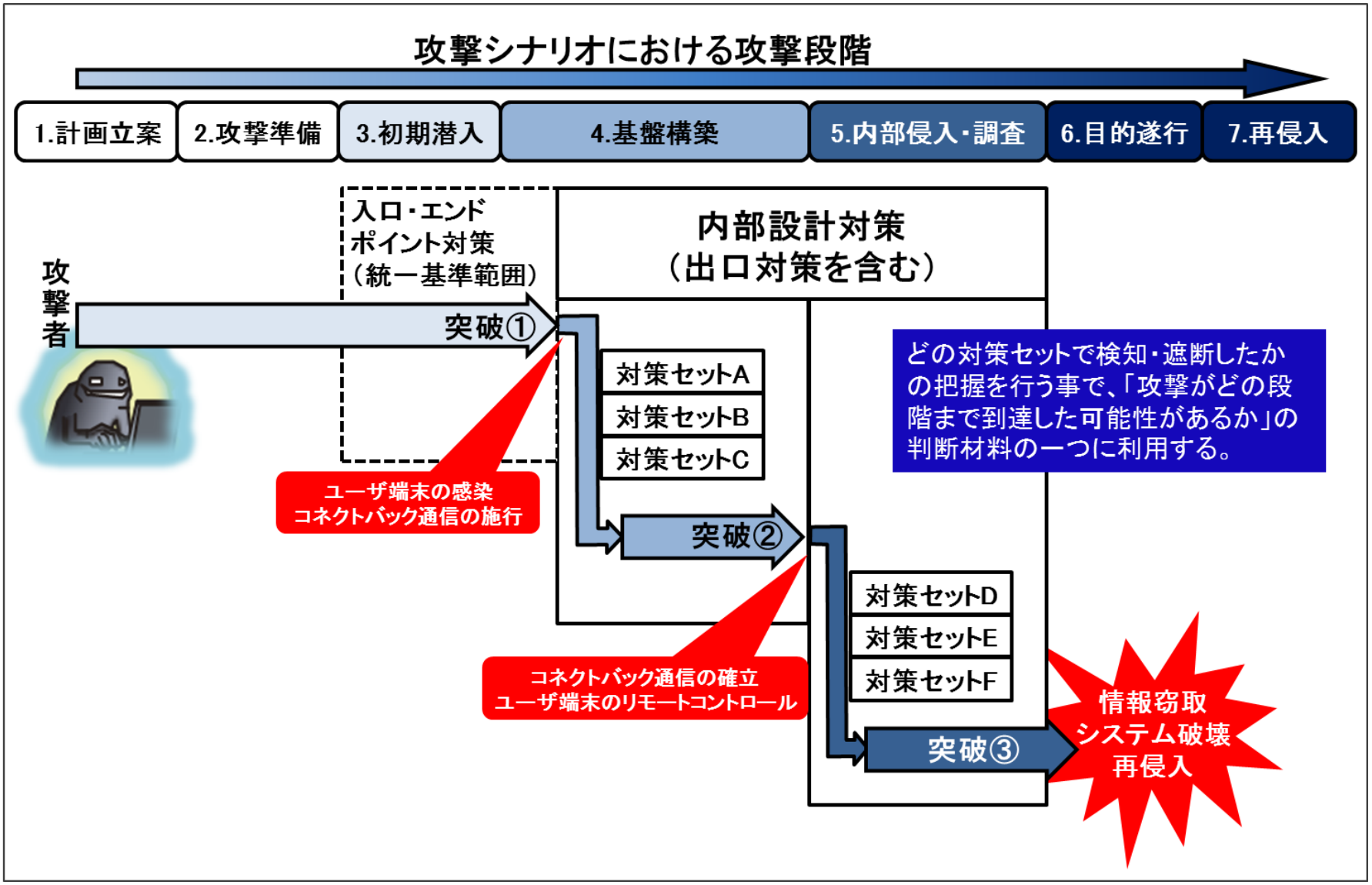
- C&Cサーバ:コマンド＆コントロールの略。攻撃者が設置したサーバ
- Dropper:別のマルウェアをダウンロードするプログラム

サイバー攻撃対策のポイント

a. 侵入されることを前提に考える。
b. いかに早く異常を検知するか。
c. いかに情報流出を最小限にするか。
d. いかに流出情報を不正利用されないようにするか。

多層防御（入口対策、内部対策、出口対策）

対策のための参考資料



参考文献： IPA「「高度標的型攻撃」対策に向けたシステム設計ガイド」(2014年9月)

大学におけるサイバー攻撃の対策

- 大学における問題点の傾向
  - a.管理されていない研究用・実験用のサーバ等の存在
    - 研究・実験終了後に放置されメンテナンスされていないデバイス
  - b.無秩序に割り振られたグルーバルアドレスの存在
    - Firewallに保護されていないグルーバルアドレスが付与されたデバイス

【リスク】
- スパムメールやDDosの踏み台に利用される
- 不正Webサイトに改ざんされる
- マルウェア感染の起点に利用される

【対策】
- 不要なサーバ等デバイスの発見と撤去
- 管理されていないサーバ等デバイスの発見とアップデート
- 不要なグルーバルアドレスの発見と撤去又はプライベートアドレスへの切り替え

ランサムウェア

ランサムウェア

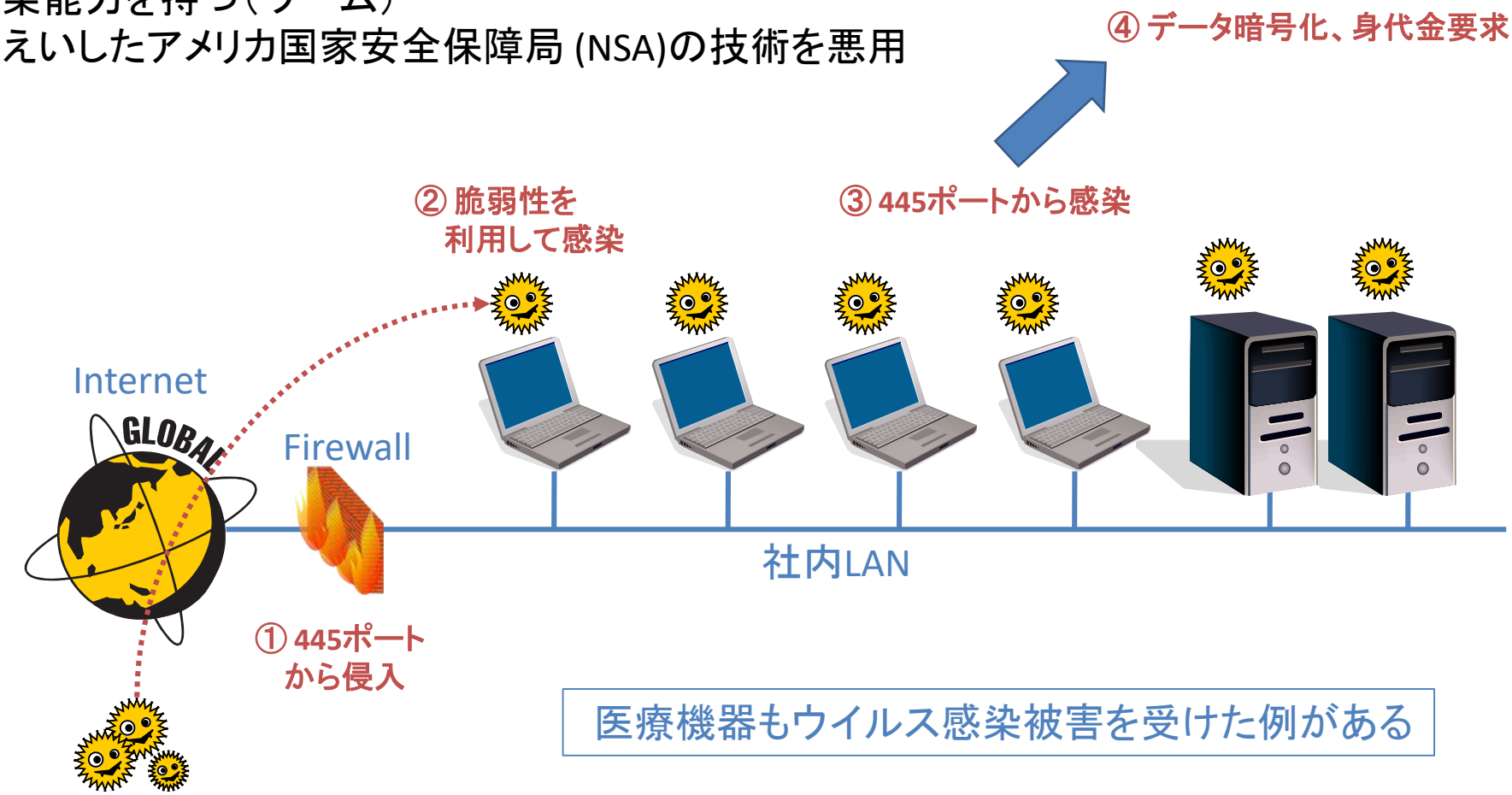
- ランサムウェア（ウイルスの一種）
  - PC内のデータを勝手に暗号化 → 元に戻したければ金を払え
  - ウイルスの一種
  - 金を払っても元に戻る保証はない
    - 反社会的組織に利益を与えたとみなされる可能性
- ランサムウェアの対策
  - OS（Windows等）やアプリケーションを最新にする
  - ウイルス対策ソフトを導入する
  - 脅迫に対する対応の方針を決めておく
  - データをこまめにバックアップする

Ransom（身代金）

IPA今月の呼びかけ （2015年6月分）
https://www.ipa.go.jp/security/txt/2015/06outline.html

補足： ランサムウェア WannaCry

・ファイル共有機能（SMBv1）の脆弱性（MS17-010）を攻撃
・インターネットから直接侵入（メール経由とは限らない）
・感染能力を持つ（ワーム）
・漏えいしたアメリカ国家安全保障局 (NSA)の技術を悪用



医療機器もウイルス感染被害を受けた例がある

ランサムウェアの脅迫画面

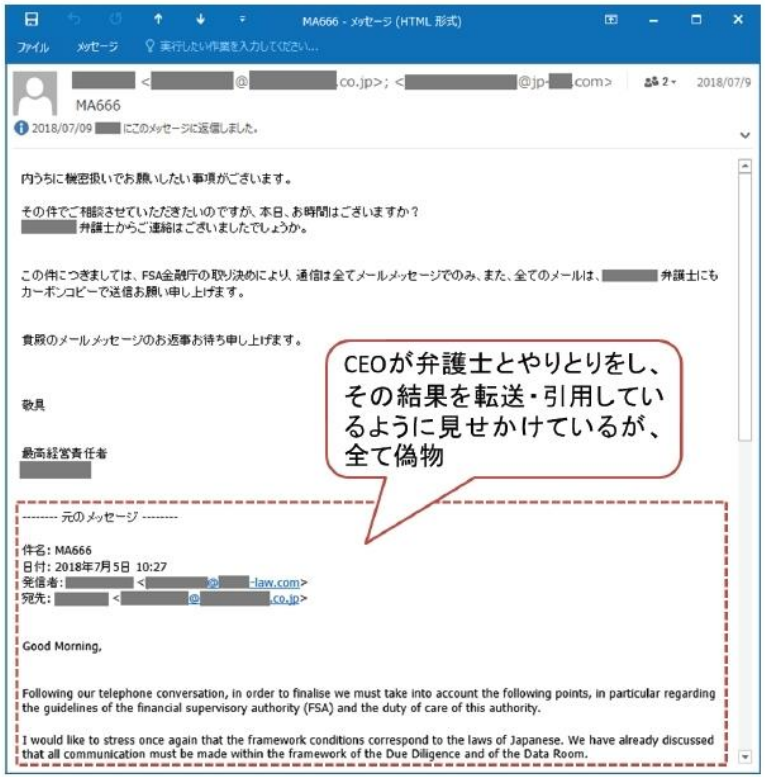
ビジネスメール詐欺

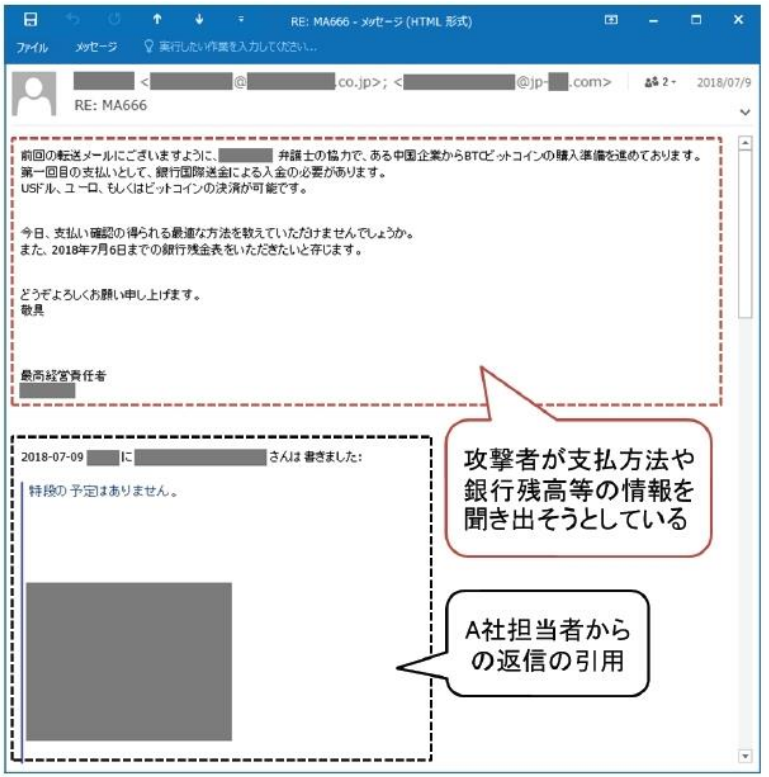
ビジネスメール詐欺の事例（１）

- JALの事例
  - 2017/12/20　米国の金融会社からリース契約で導入している機体の支払いに関し、取引のある金融会社の担当者を装うメールが届き、支払口座を香港の銀行に変更したと伝えてきた。
  - 送信元のアドレスは画面表示上、担当者のものと同じだったため、日航側は信じて約３億６千万円を送金した。後日、本物の金融会社から督促があり、だまされたことがわかった。
- ドルチェ＆ガッバーナの事例
  - 日本法人社長が、ミラノ本社の経理部長から、金融取引のために中国の銀行に送金せよとの指示をメールで受信。内容に従い、社長は部下に指示して送金。
  - 後日、詐欺だったと判明し、社長と部下クビになったうえ、自宅を仮差押えされ、社から提訴された。

ビジネスメール詐欺の事例（２）

- 日本語のビジネスメール詐欺
  - 送信者は最高経営責任者（CEO）を詐称
  - 文中に偽の弁護士の存在にも触れ、受信者に機密扱いを要求
  - 受信者が返信すると、約5分後に「ビットコインの購入準備のため、国際送金の必要がある」と返信





＜出典＞ IPA： 8月27日、偽口座への送金を促す“ビジネスメール詐欺”について注意喚

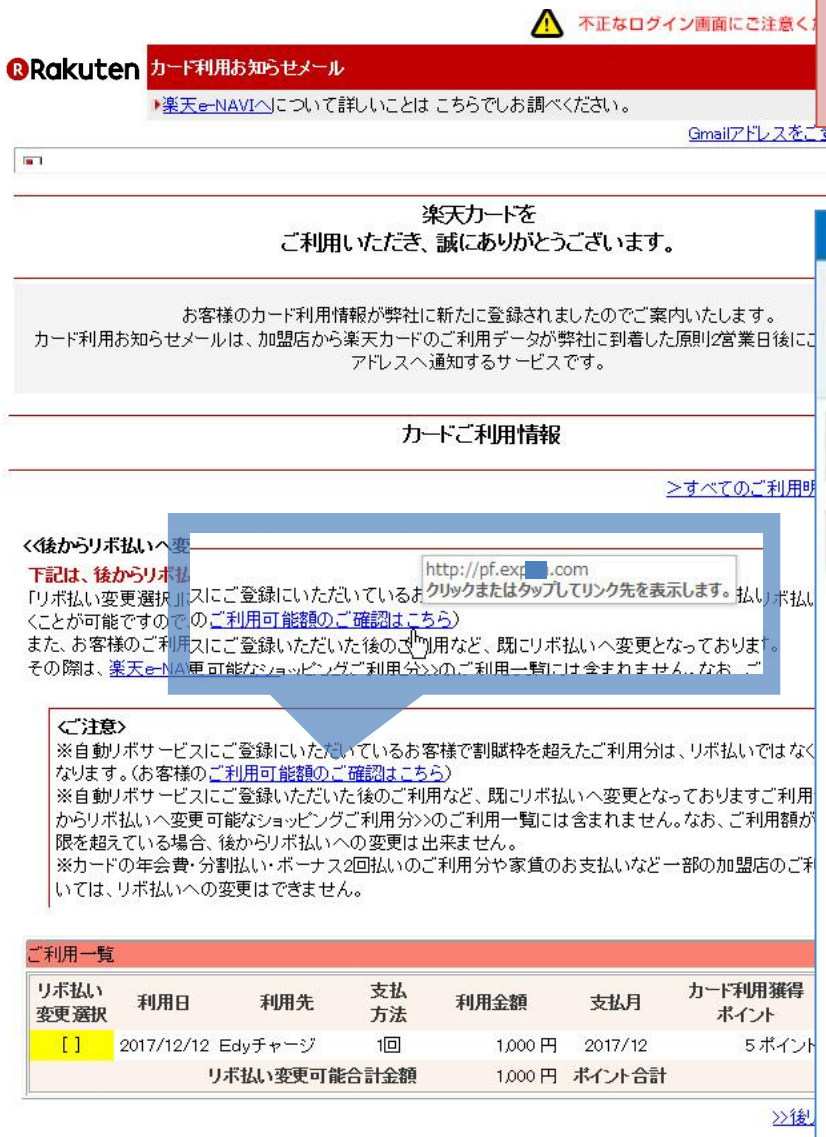
ビジネスメール詐欺への対応

- 普段と異なるメールに注意
  - 送金指示の通知
  - いつもと異なる時期の通知、いつもと違う手順
  - 振込先の変更依頼
  - 不審なメールは社内で相談・連絡し、情報共有する
- 電信送金に関する社内規程の整備（チェック体制の整備）
  - 急な振込先や決済手段の変更等が発生した場合、取引先へメール以外の方法で確認する
- ウイルス・不正アクセス対策
  - セキュリティソフトを導入し、最新の状態にする
  - メールアカウントに推測されにくい複雑なパスワードを設定し、他のサービスとの使い回しをしない
  - メールシステムでの多要素認証、アクセス制限の導入を検討する

＜参考＞ IPA： 8月27日、偽口座への送金を促す“ビジネスメール詐欺”について注意喚

ばらまき型偽装メール（１）

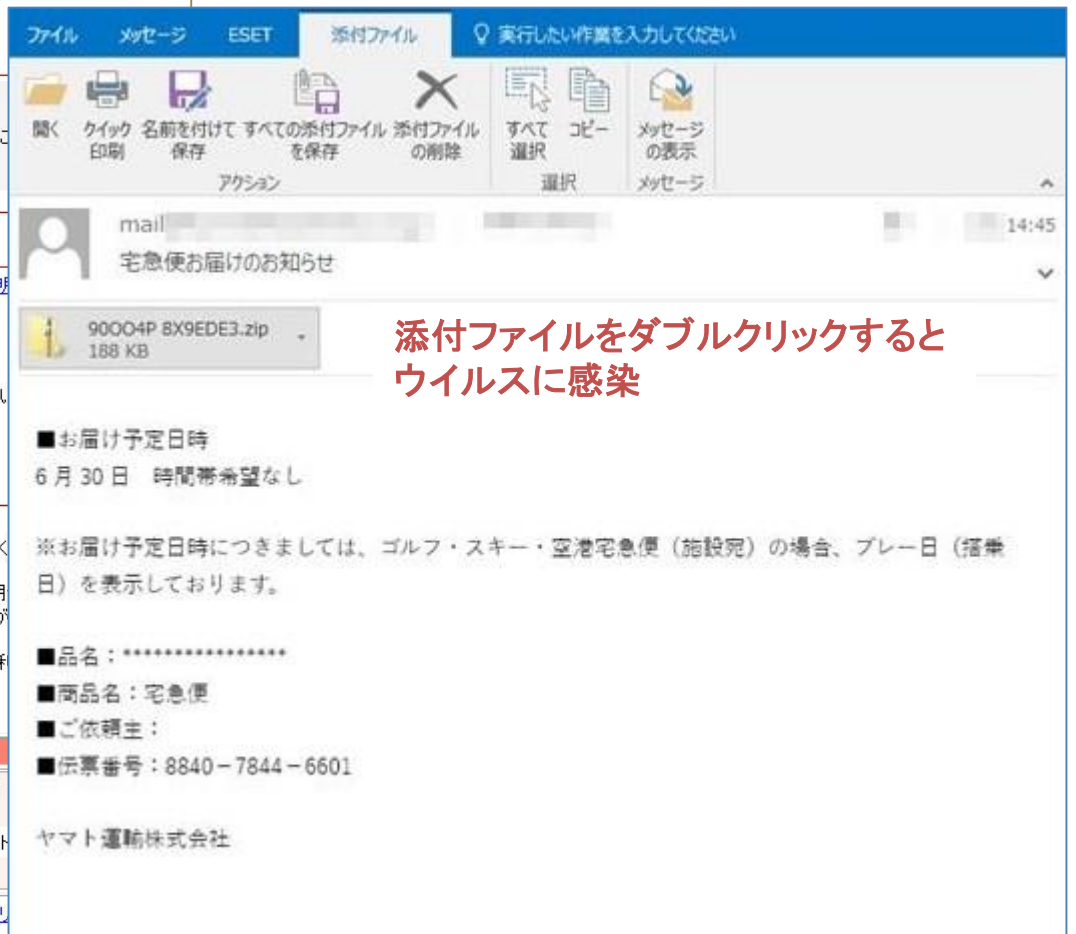
リンク（青字の箇所）をクリックすると
不正サイトにつながりウイルスに感染



注意すべきメール

① メールの添付ファイルは疑う
　拡張子が .exe　.lzh　.zip　.pdf　のファイルは注意
② メールに記述されたURLは不用意にクリックしない

URL：ホームページへのリンク



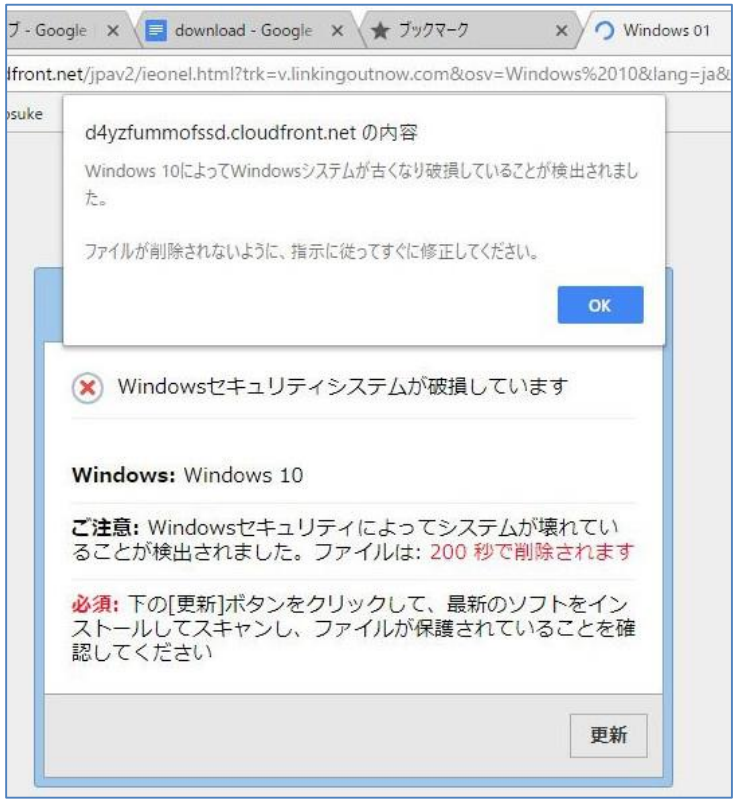
添付ファイルをダブルクリックすると
ウイルスに感染

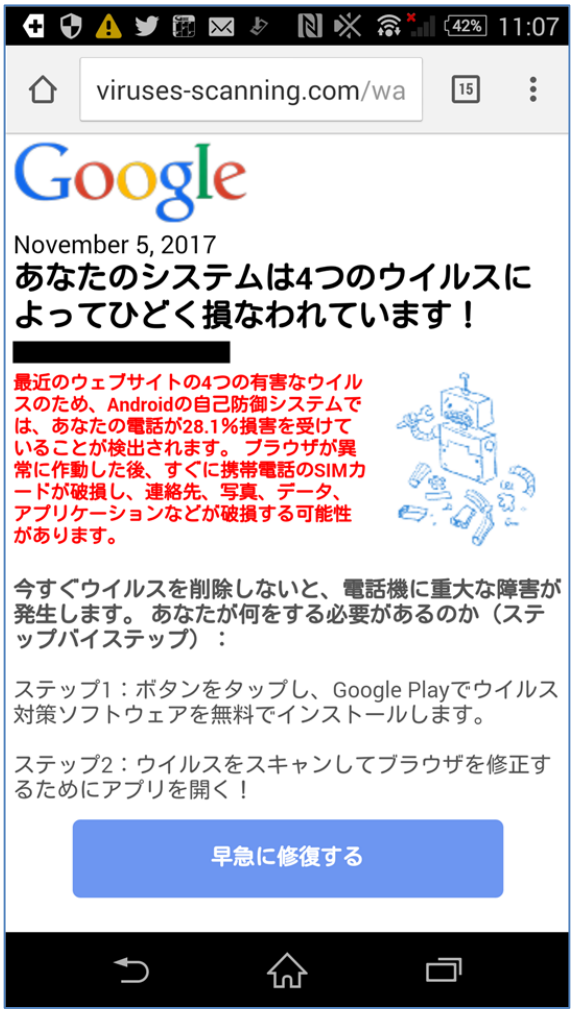
ばらまき型偽装メール（２）

気付いたらすぐ報告！

偽のウイルス対策ソフトに注意

- ウイルス対策ソフトをインストールするように促す警告を表示
  - -それ自体がウイルス





クイズ

【問題】 添付ファイルが付いた不審なメールを受信した時に、
最もやってはいけないことはどれでしょう。

① 何もせず、決められた学内窓口に報告する
② メールを開いて内容を読み偽装メールかどうか判断する
③ 添付ファイルを実行してウイルス検知されるかどうか確認する

【答え】③

- ②の「メールを開いて読んだ」だけでは感染はしません

セキュリティトピックス

自動車のサイバーセキュリティ

- コネクティッドカーのリスク
  - インターネット経由の侵入
    - 交通情報等のリアルタイム更新、遠隔診断、エンジン制御・・・
    - Bluetooth、WiFi、移動体無線等のネットワーク機能の搭載
    - 各センサー、制御ユニット、ネットワークユニットのハード/ソフトの脆弱性の存在
    - 誤った指令による制御、誤った情報を与えられることによる誤作動・・・
  - プライバシー侵害
    - 車両ネットワークで収集したデータ（位置情報、速度、運転特性等）の保険、広告、エネルギー分野での活用、売買
    - 蓄積した情報の窃取、流出、目的利用・・・
- 対策
  - 設計段階でのセキュリティ機能の組み込み
  - サプライチェーンにおけるセキュリティの取り組み
  - 品質としてのセキュリティ試験

参考：PWC　自動車サイバーセキュリティ

仮想通貨マイニングウイルス

- 仮想通貨マイニング
  - 仮想通貨の取引の正当性を裏付けるために、数学的に難度の高い計算を行い、その報酬として仮想通貨を受け取ることをマイニング（採掘）という。
    - 仮想通貨での取引が発生すると世界中の採掘者が競って計算を行い、最も早く計算を終了した者に報酬が与えられる。
    - 高速で計算を行うためには、大量のコンピュータを同時に稼働させる必要があり、それに係る電気代も莫大なものになる。
- 仮想通貨マイニングウイルス
  - マイニングのために自分で大量のコンピュータを用意する代わりに、他人のコンピュータにウイルスを感染させて計算をさせる。
- Webサイトに置かれたコインマイナー
  - Webサイトに仮想通貨を採掘するツールを設置しておき、そのサイトを閲覧するユーザのPC上でマイニング（計算）させる仕組み。
  - ウイルス共用容疑でWebサイト運営者数名が逮捕された。
  - 広告収入に代わる収入方法として行っていたもので、違法か否かが議論となっている。

ネットのアンダーグランド領域「ダークウェブ」

Surface Web

検索可能な一般のサイト

Deep Web

ID/パスワード等で保護され
検索結果に表示されない領域
（メール、公開制限されたSNS、
通販等のMyページ、有料コンテンツ等）

Dark Web

特殊なアプリや方法でしかアクセス
できない違法サイト等

個人のセキュリティ対策

日常業務のセキュリティ

大学関連の事故事例 ①

群馬大学医学部において個人情報を含むUSBメモリが、所在不明に。（2018/7/23）

- USBメモリの暗号化、パスワード保護等　・USBメモリの台帳管理と定期的な棚卸し
- 保管場所の指定と施錠保管　・ストラップ等による携行時の紛失予防

- その他 情報携行時の対策
  - 電車の網棚に鞄を置かない　- 鞄を車中に放置しない
  - 自転車の前の籠に鞄を置かない　- 自宅に会社の情報を保管しない
  - 宴席に重要情報は持っていかない　- 持ち歩く情報は最小限に

東京大学の教員が所有する、学生や非常勤講師の個人情報が保存されたパソコンが、学内で盗難被害に遭った。（2018/7/31）

- パソコンを置く区画の入退室制限と監視カメラなどによる監視
- ノートPCのワイヤロックまたは施錠保管
- PC内ハードディスクの暗号化、BIOSロック等

参考：Security NEXT

大学関連の事故事例 ②

東京女子医科大学東医療センターにおいて、退職した医師が患者の個人情報を不正に持ち出した。（2018/8/10）

- 個人情報へのアクセスログの取得　・PC端末の操作ログの取得
- ログの定期的な評価、退職前の挙動分析　・監視システムによるデータアクセス監視
- 退職時の秘密保持条項を盛り込んだ誓約書への署名

大阪市立大学のシンポジウムの案内メールで誤送信が発生し、メールアドレスが流出したことを公表した。（2018/9/03）

- 送信前の宛先アドレスの再確認（@の右側）
- 送信前の宛先アドレス、メール内容、添付ファイルのダブルチェック
- 添付ファイルの暗号化、パスワード保護

参考：Security NEXT

大学関連の事故事例 ③

新潟大学の複数の教職員のメールアカウントがフィッシングにより乗っ取られ、迷惑メールを送信するための踏み台に悪用されたほか、個人情報が閲覧された。（2018/9/28）

- フィッシング対策
  - URLが「https」からはじまっているか確認する
  - SSL証明書の警告が出たらアクセスをやめる　- ウイルス対策をしっかり行う

参考：Security NEXT

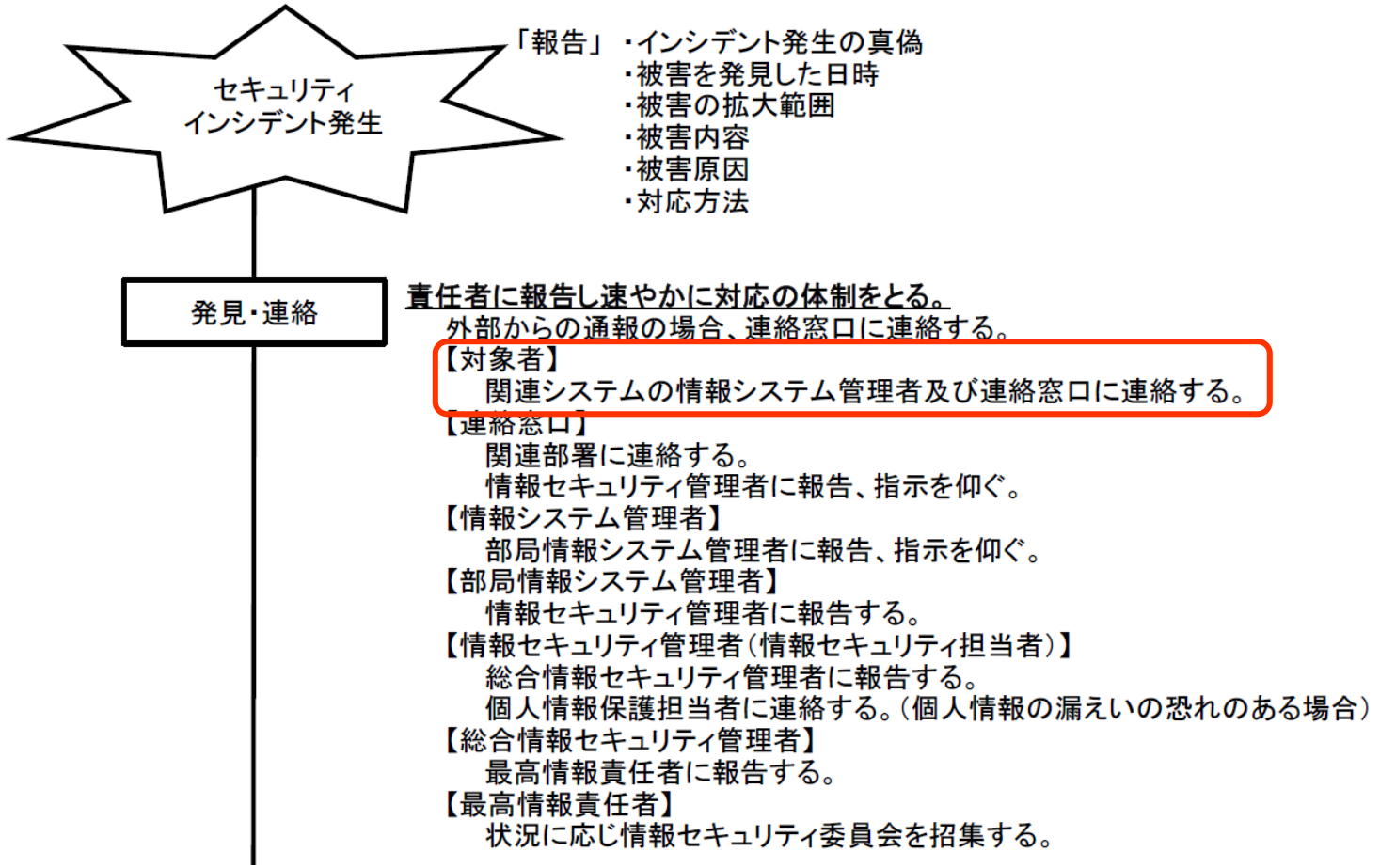
フィッシング (phishing) 詐欺とは

実在の銀行やクレジットカード会社などを装った偽ホームページに迷惑メールで誘導され、個人情報の入力を要求される

<出典> フィッシング対策協議会
www.antiphishing.jp

まず、報告する！！

- 他の人が同じ攻撃を受けている可能性を考え情報共有する。



「緊急時対応計画（情報セキュリティ）別紙1」より抜粋

まずは業務における重要情報の把握から

① 重要情報の定義

- 全校共通の重要な情報とは？
- 学部、学科において重要な情報とは？

② 重要情報の所在の把握

- 各人の管理範囲での所在の把握
- 学部、学科単位での情報の把握
- 全校での情報の把握

③取り扱い状況の把握と点検

- 情報の生成/取得、保管、出力、移送、廃棄の実施方法の確認
- リスク評価と改善

パスワードの強化

予測されやすいパスワードも見直す

AKB48HKT48

password1

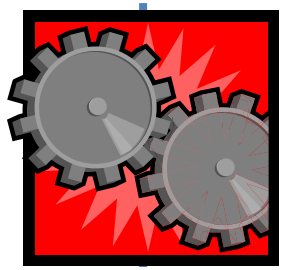
suzukisuzuki

忘れにくい簡単なパスワード

qwerty1234

123456

yamada123



ツールによる解読

他人による予測

	8桁	10桁
英子文字のみ(26文字種)	4秒	47分
英大小文字+数字+記号(96文字種)	1.7日	42年

株式会社ディアイティ 調査　Windowsパスワード(NTLMハッシュ)のケース

パスワードリスト攻撃

＜出典＞ 独立行政法人 情報処理推進機構（IPA） 啓発ビデオ
https://www.youtube.com/user/ipajp

望ましいパスワードとは

出来るだけ長く

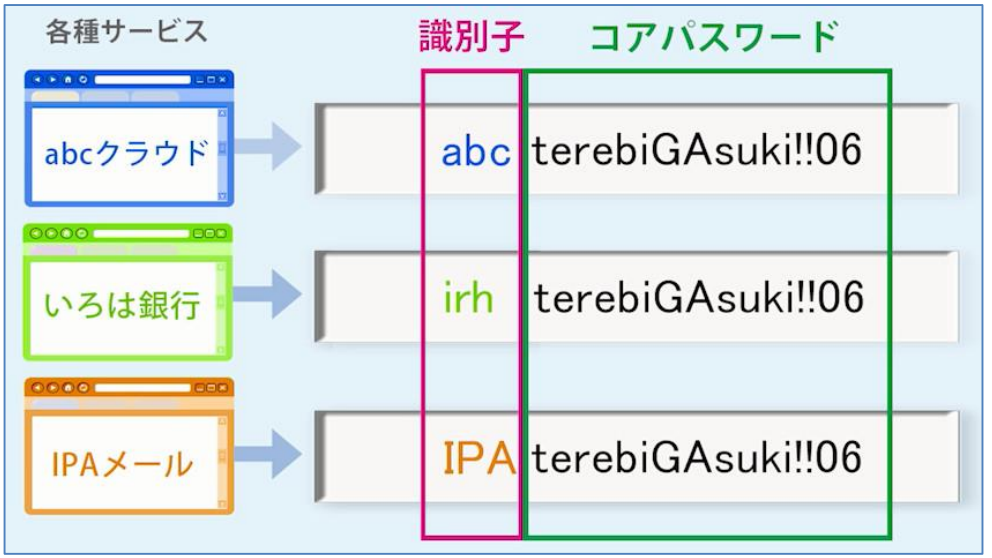
複雑に

使いまわさない

パスワードの設定

① コアパスワードの作成

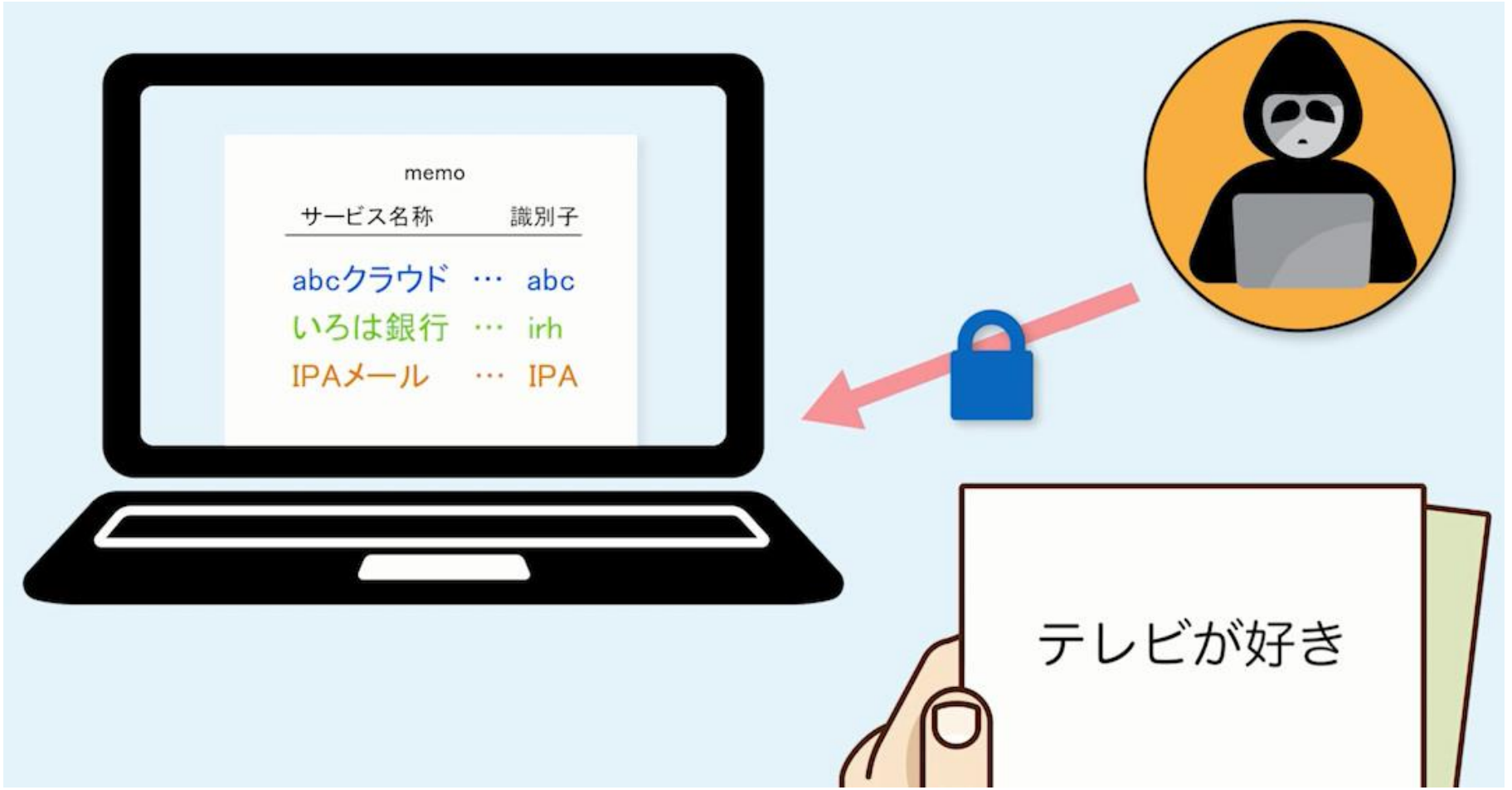
② サービスごとに異なるパスワードの作成



＜出典＞ 独立行政法人 情報処理推進機構（IPA） 啓発ビデオ
https://www.youtube.com/user/ipajp

パスワードの管理

- コアパスワードと識別子を別々に管理すると一方が流出しても悪用できない



＜出典＞ 独立行政法人 情報処理推進機構（IPA） 啓発ビデオ
https://www.youtube.com/user/ipajp

「秘密の質問」の設定

- 本来の答えに独自フレーズを追加

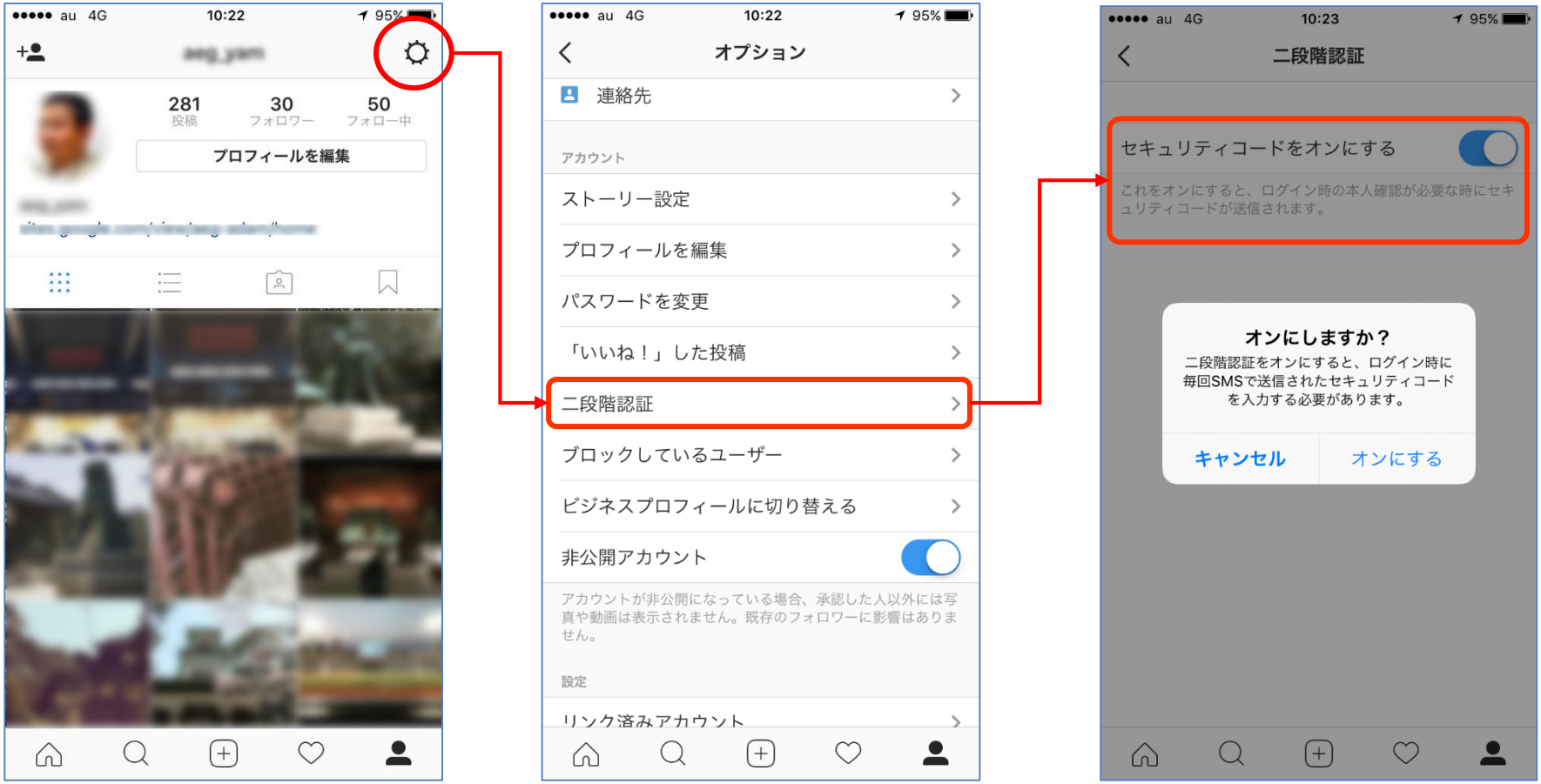
質問「あなたの好きな果物は？」
応え「みかんかもしれない」

質問「あなたの母親の旧姓は？」
応え「前田かもしれない」

＜出典＞ 独立行政法人 情報処理推進機構（IPA） 啓発ビデオ
https://www.youtube.com/user/ipajp

二段階認証

- 二段階認証を利用すると、より安全性が高まる。
  - 何を知っているか（暗証番号）
  - 何を持っているか（スマホ）



クイズ

【問題】 最も安全だと思われるパスワードはどれでしょう。

① E1j1Y@m@d@
② @men1m0M@kezu
③ 1qazxsw23edc

【答え】②

- ①は名前を基にしているので予測される
- ③はキーボードの配列をそのまま使用している

スマートフォンを守る

スマートフォンを守る

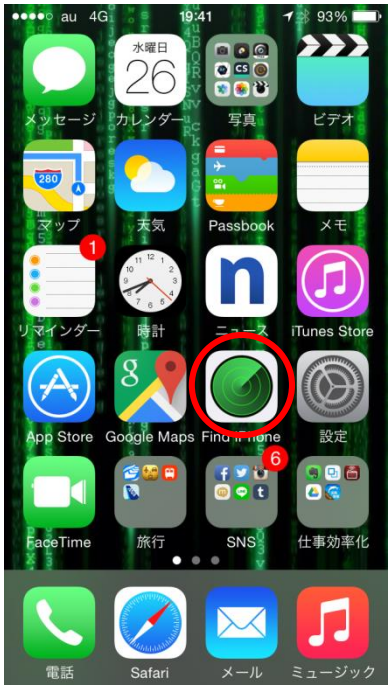
✓ 画面ロックする
- SIMロック、画面ロックパスワード (指紋認証、指パターン入力ロック)

✓ データをこまめにバックアップする
- Android： Googleドライブ等
- iPhone： iTunes、iCloud等

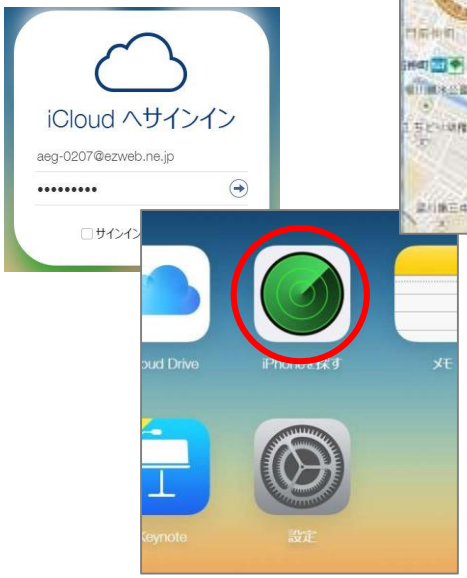
✓ 紛失したら遠隔削除する
- PCからGPSで位置を確認、遠隔操作しスマートフォンをロックするか中のデータを削除する
  - Android： Android デバイス マネージャー
  - iPhone： iPhone を探す

GPSで位置確認、遠隔操作で削除

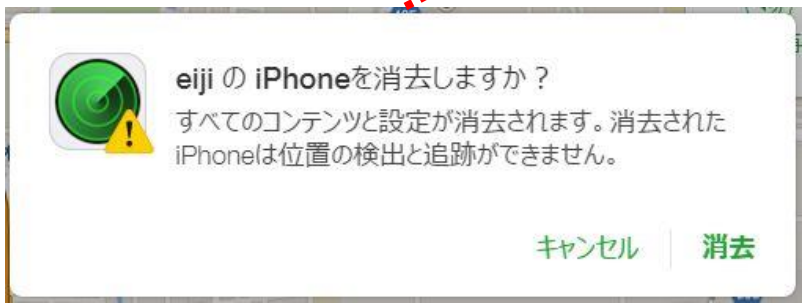
- iPhone を探す



iPhoneに
「Find iPhone」を
インストール



Cloud上で
「iPhoneを探す」
をクリック



「iPhoneの消去」
をクリックして消去

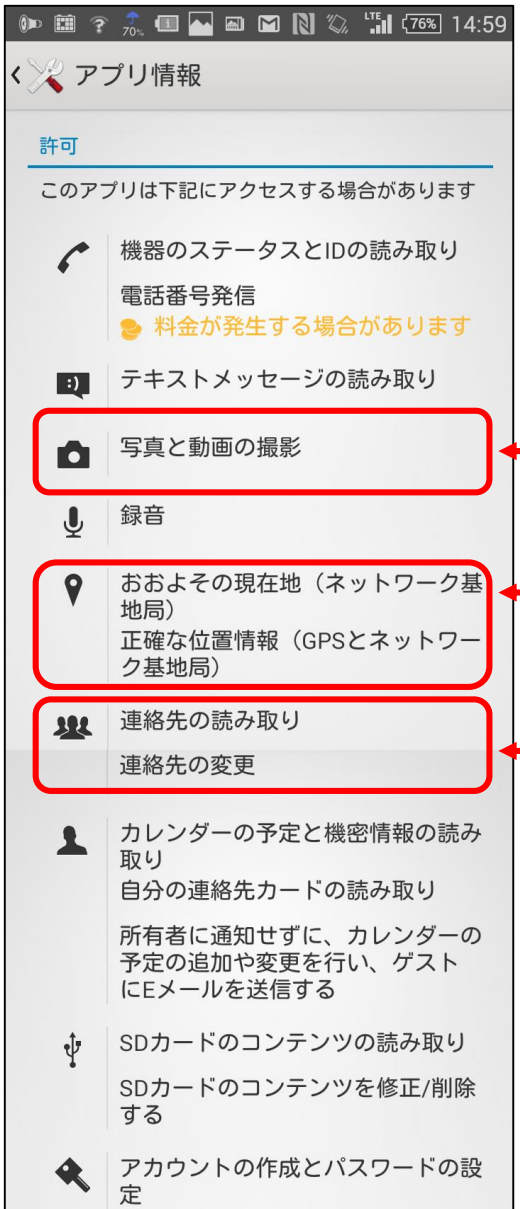
アプリケーションのインストールは慎重に

✓ 正式サイトからダウンロードする
- Android： Playストア（Google Play）
- iPhone： App Store
- その他 通信事業者（au、docomo、Softbank等）の運営サイト
- インストールしようとするアプリの評判をネットで確認する

✓ アプリケーションの許可情報を確認し納得できればインストールする
- 設定 → アプリ でアプリケーションを開き「許可情報」を確認
- アプリの目的と許可情報が合わない場合は注意
  - 電池を長持ちさせるアプリなのに「カメラ」や「連絡先」を利用するのはおかしい

✓ ウイルス対策ソフトをインストールする

アプリケーションの許可情報を確認する



カメラ

カメラでの写真と動画の撮影をアプリに許可します。これにより、アプリが確認なしでいつでもカメラを使用できるようになります。

ソーシャル情報

携帯電話に保存されている連絡先に関するデータの読み取りをアプリに許可します。このデータには、電話、Eメール、または他の手段で特定の相手と連絡をとった頻度も含まれます。これにより、アプリに連絡先データの保存を許可することになり、悪意のあるアプリによって知らないうちに連絡先データが共有される恐れがあります。

現在地

ユーザーのおおよその位置情報を取得することをアプリに許可します。この位置情報はネットワーク位置情報源(基地局やWi-Fiなど)を利用した位置情報サービスから取得されます。これらの位置情報サービスはONの状態にして、機器でアプリがサービスを利用できるようにする必要があります。アプリはこの位置情報を利用してユーザーのおおよその現在地を特定できます。

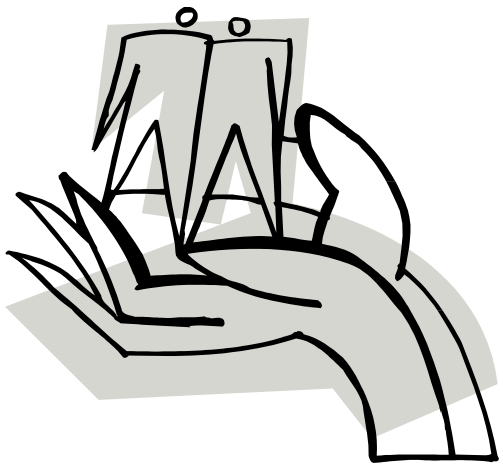
SNSの安全な使い方

ソーシャルメディア

- Facebook、mixi、Google+、Linkdein、SNOW等のSNS（ソーシャル・ネットワーク・サービス）
- Twitter等のミニブログ
- Youtube、USTREAM、ニコニコ動画等の動画共有サイト
- その他ブログ、LINE、ゲームサイト内のコミュニティ等

ソーシャルメディアを使う時の心得

- ✓業務に関することは書き込まない
- ✓友達以外も見ていることを意識する
- ✓一度発信した情報は取り戻せないことを知る
- ✓匿名ではないことを意識する
- ✓個人情報の書き込みは最小限に
- ✓公開範囲を最小限にする



特に写真のアップには注意！

- 窓の外の風景から家の場所が分かる
- いつもの散歩道で待ち伏せされる
- 家族旅行中にドロボウに入られる

写真には大量の情報が
含まれている

クイズ

【問題】 SNSに自宅内で撮った写真をアップする時に、特に気を付けることは何でしょう。

① 散らかしたままの部屋の様子がばれること。
② 写り込んだ本棚から趣味がばれること。
③ 背景から、住んでいる場所が予測されること。

【答え】 ②と③

- ②で趣味がわかると、同じ趣味を装って近づかれる
- ③窓の外の情景や部屋の壁紙の様子から住んでいる場所が特定される

「書き込み」チェックは人事の常識

- 入社前から危険人物を徹底駆除「炎上してからでは遅い」
  危険人物の雇用を未然に防ぐため採用段階で学生らのネットの書き込みをチェックする企業が増えている

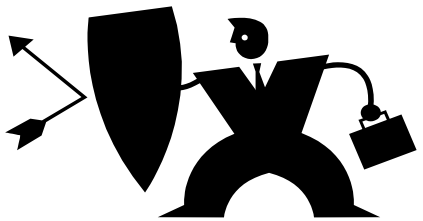
2015/5/22 産経ニュース

ALSOKの監視サービス

自分の情報は自分でコントロールする

- Facebookの利用規約（抜粋）

> 2. コンテンツと情報の共有
>
> 利用者がFacebookで投稿したコンテンツおよび情報は、すべて利用者が所有するものであり、プライバシー設定およびアプリケーション設定を使用して、利用者自身がどのように共有するかを管理することができます。

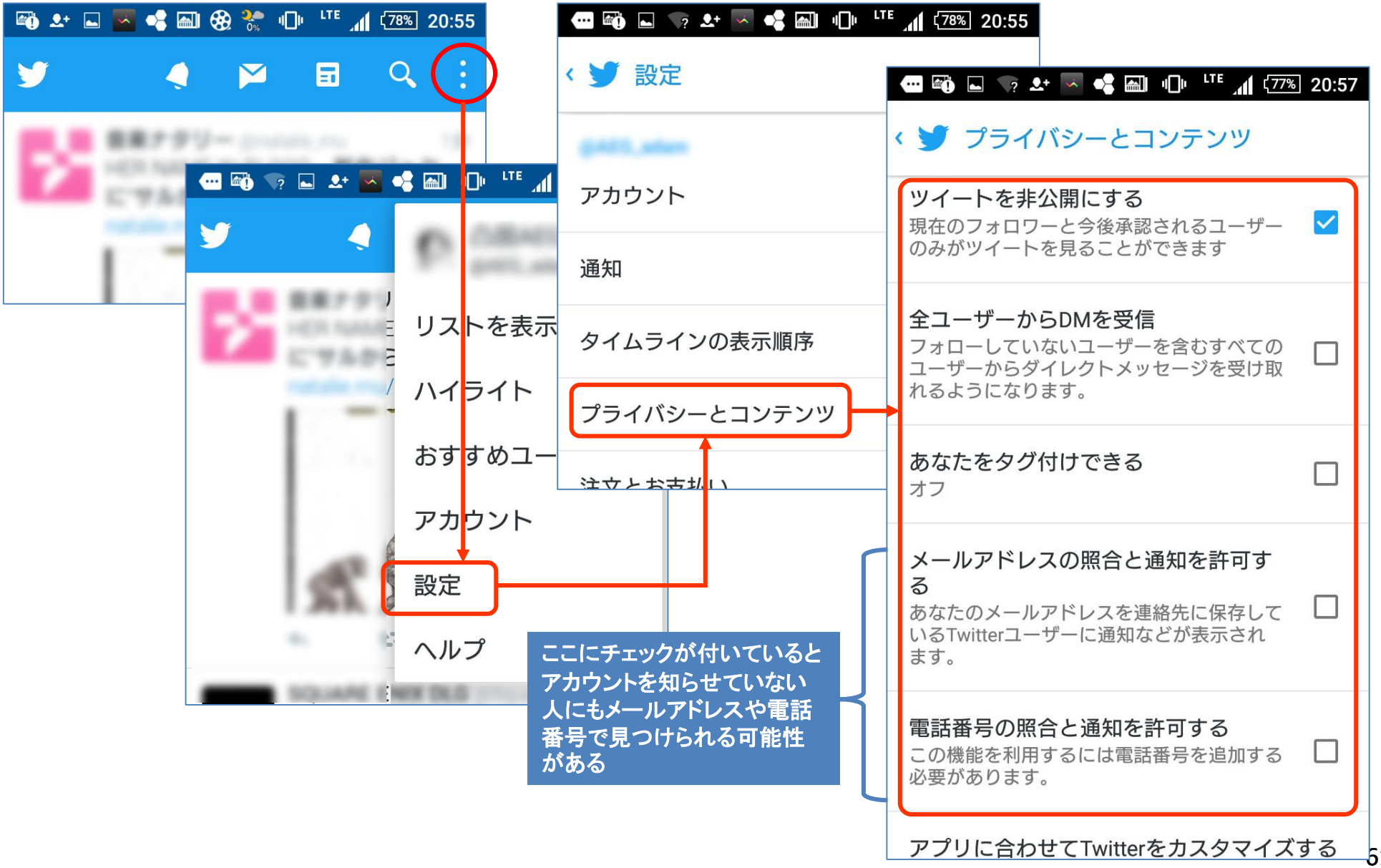


利用者が投稿した情報は、設定により自分の責任で守る必要がある。

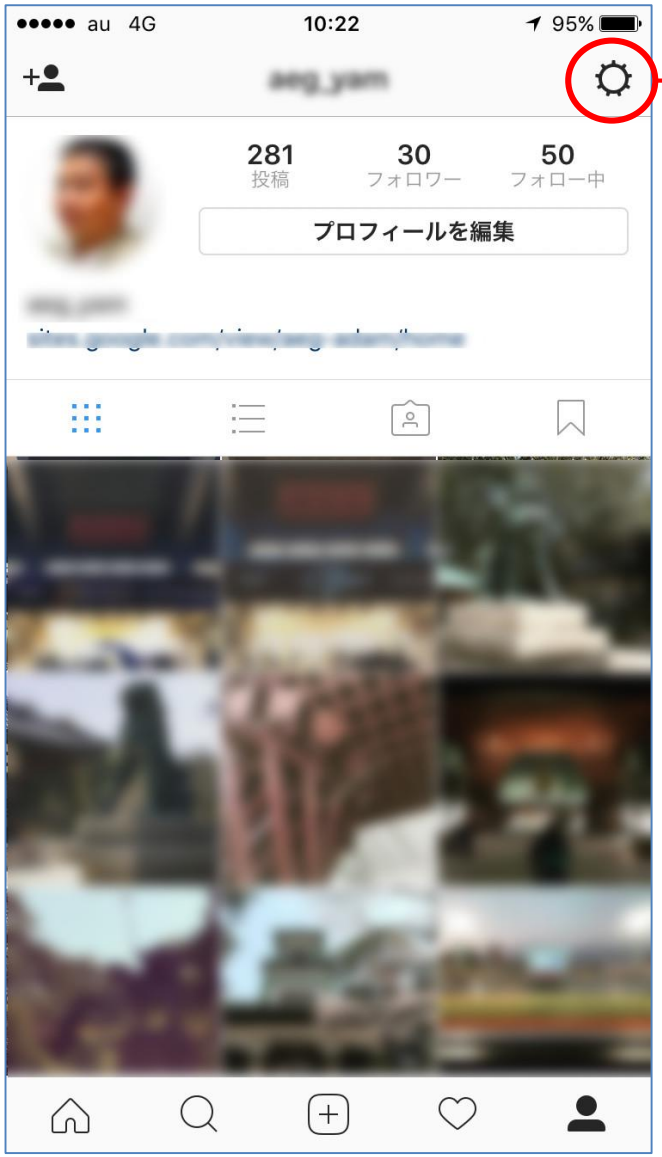
Facebookの公開範囲設定

初期設定は「公開」になっているので、希望する範囲を指定する

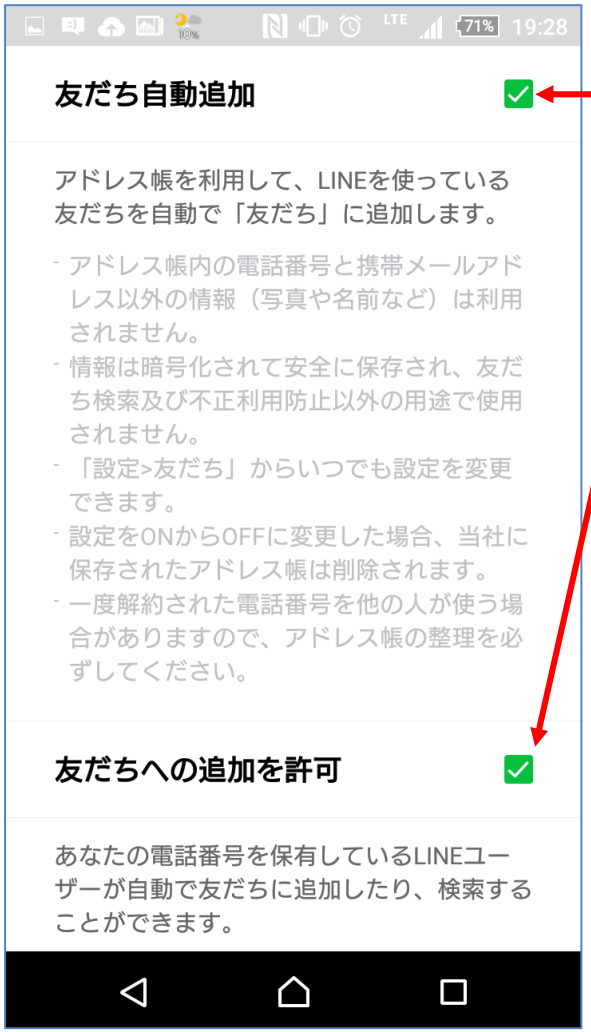
Twitterの公開範囲設定



Instagramの公開範囲設定



LINEのセキュリティ設定



初期状態（デフォルト）でチェックが入っている

- 「友だち自動追加」
  アドレス帳に登録した人を自動的に「友だち」に追加する機能
- 「友だちへの追加を許可」
  相手が自分の電話番号をアドレス帳に登録していると自動的に「友だち」に追加する機能

- 意図せず他者に友達追加されたくない場合はチェックを外す

＜参考＞ http://official-blog.line.me/ja/archives/cat_544056.html

LINEのセキュリティ設定

http://line.me/safety/ja/

ご清聴ありがとうございました