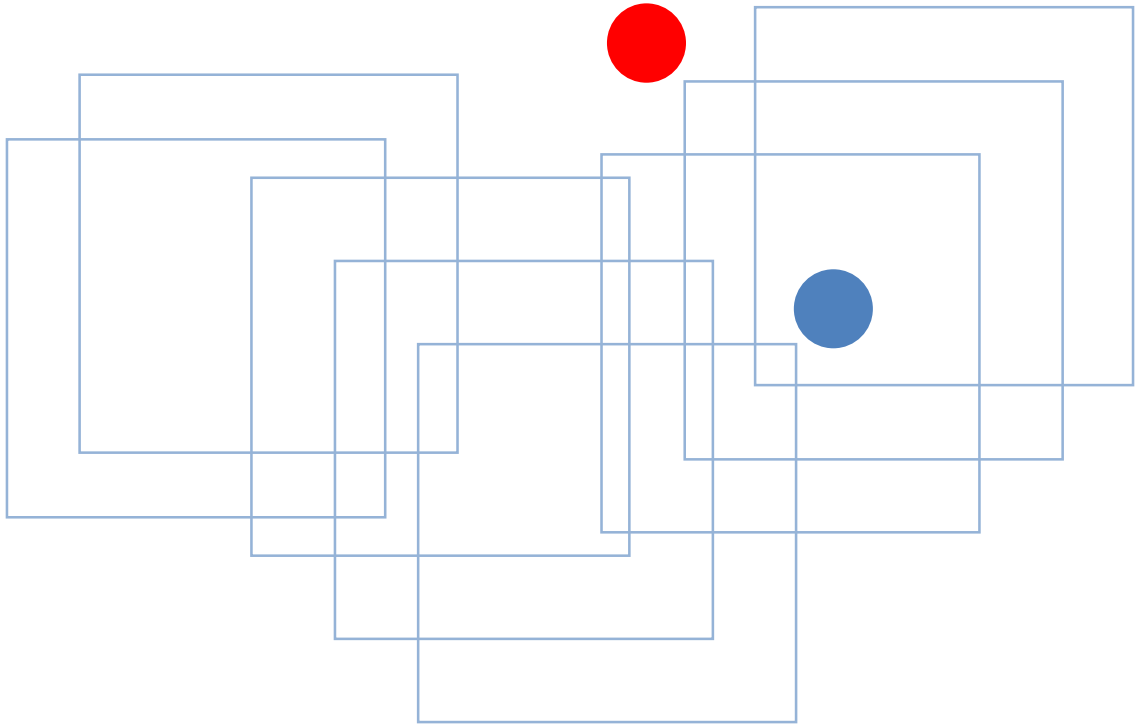
Security 安全･安心



秋田県立大学
令和元年 情報セキュリティセミナー
～スマートフォン、SNSの安全な使い方～

令和元年 11月21, 22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
セキュリティコンサルティング本部
ゼネラルマネージャー

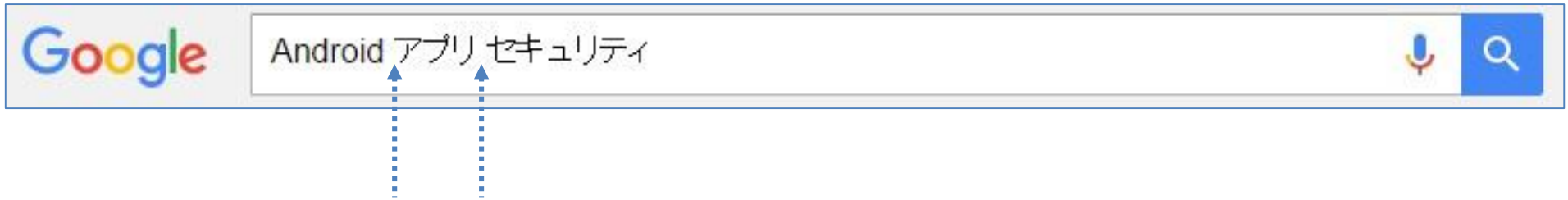
＜資格＞
CISSP
情報セキュリティ監査人補
情報セキュリティプランナー

＜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＞
- 総務省/経済産業省 クラウドサービスの信頼性確保に関する検討会　監査検討WG 委員
- 経済産業省 産業サイバーセキュリティ研究会 WG1分野横断SWG委員
- 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
- 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
- JASA-クラウドセキュリティ推進協議会 コアメンバー

- 分からないところは後でネット検索して調べてみましょう。
- 今日覚えたことは身近な人に伝えてください。

ネット検索の方法



単語の間に空白（スペース）を入れると、並べた単語を含むページが検索できる。

【例】　「Android」と「アプリ」と「セキュリティ」を含むページが表示される。

つながる！　スマホとインターネット

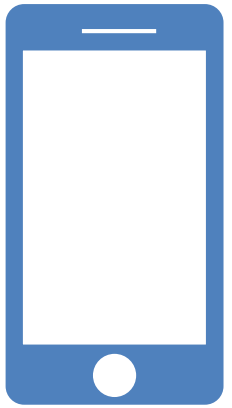
インターネット

mobage

DoCoMo

au

SoftBank



スマホ

YouTube

LINE

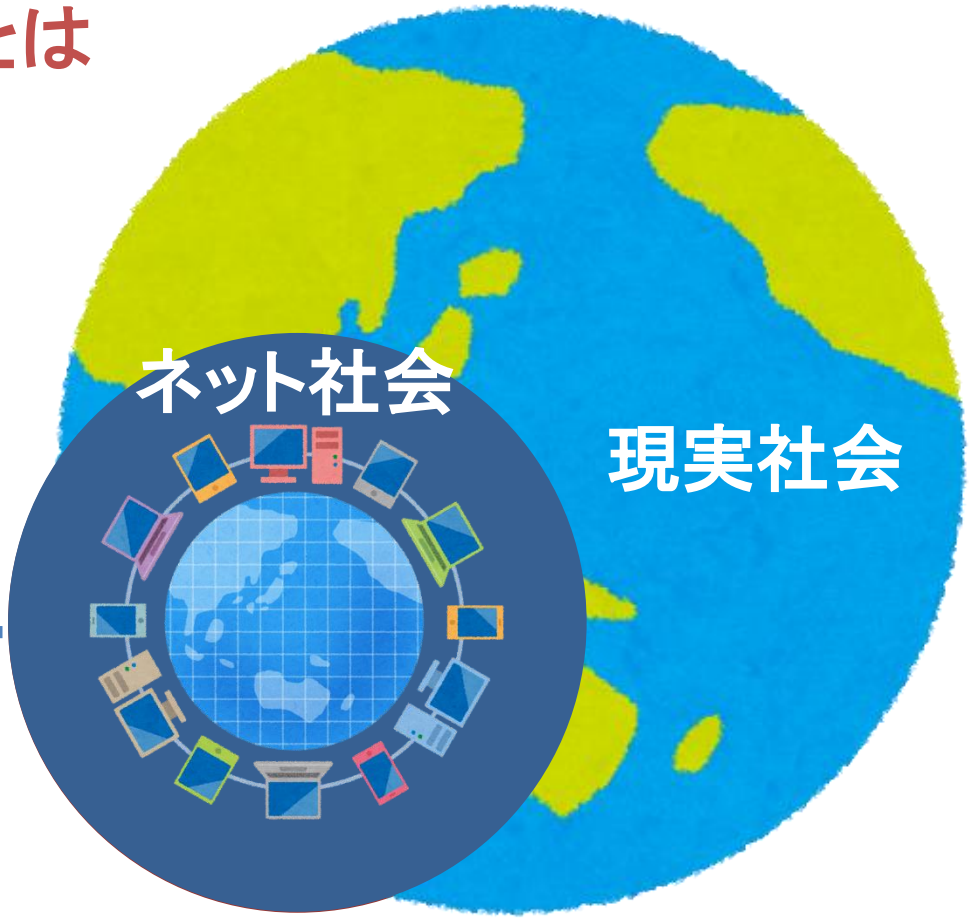
WiFi

ゲーム機

ほとんど現実の世界と同じ

■現実社会で起こることはネットでも起こる

■現実社会で解決できないことは
ネットでも解決できない



インターネット特有の
性質を理解する

大学の情報セキュリティ事故事例

県立広島大学は、推薦入試の出願者に送信した連絡メールにおいて誤送信が発生し、メールアドレスが流出。

室蘭工業大学は、サーバの設定ミスが原因で、学生1187人の氏名、所属、成績が含まれる個人情報がインターネット経由で閲覧できる状態になった。

東京女子大学の研究室用ウェブサーバにおいて、研究者5人のアカウントが不正アクセスを受け、あわせて52件のファイルが不正にアップロードされた。対象の研究者が学外のシステムで使用していたパスワードを不正に使用された可能性。

金沢大学において、複数の教職員が偽装メールを受信し、内25人がフィッシングサイトへアクセスしてメールのパスワードを入力してメールアカウントを乗っ取られた。乗っ取られたメールアカウントが踏み台として悪用され4万1697件のフィッシングメールが送信された。

大阪市立大学医学部付属病院の医師が、患者15人分の氏名や電話番号、年齢、性別、担当医師名、予約日や予約時間などが記載された書類を自転車のかごに入れたまま駅の駐輪場に駐輪して放置し紛失。

今日のお話し

1. 日常の情報セキュリティ
   - 1-1. スマートフォンを守る
   - 1-2. SNSを安全に使う
   - 1-3. ネット詐欺に注意
   - 1-4. パスワードを守る
   - 1-5. 困ったときは

2. 情報セキュリティ トピックス
   - 2-1. QR決済サービスへの不正アクセス
   - 2-2. 就職支援サイトの個人情報利用方法不備
   - 3-3. ビジネスメール詐欺
   - 2-4. 高度化するサイバー攻撃
   - 2-5. AIとセキュリティ

1. 日常の情報セキュリティ

1-1. スマートフォンを守る

スマートフォンを落としたら

- 悪意のある人にスマートフォンを拾われたら何をされると思いますか？

- 中の情報を見られる。
- 中の情報を取られる。
  （拡散、流出に発展）
    - 写真、アドレス帳等
- 中の情報を消される。
- いつも使っているサイトにアクセスされる。
- 課金サービスで買い物をされる。
- 本人になりすまして電話やメールを使われる。

スマートフォンを守る (1)

✓画面ロックする

- SIMロック、画面ロックパスワード (または指ジェスチャー入力ロック、指紋認証)

✓データをこまめにバックアップする

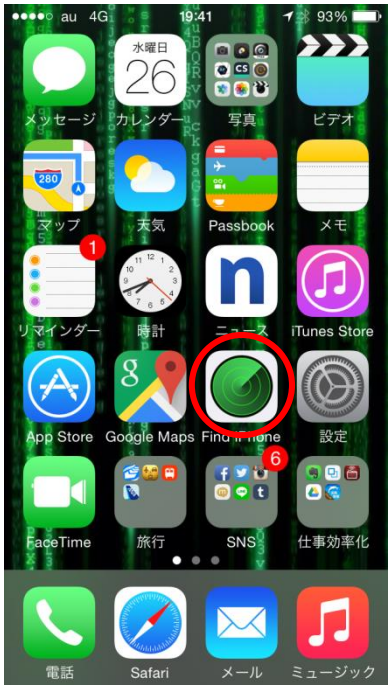
- Android： Googleドライブ等
- iPhone： iTunes、iCloud等

✓紛失したら遠隔削除する

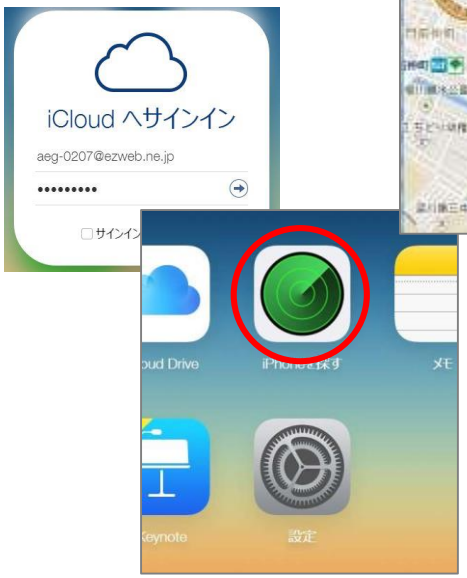
- PCからGPSで位置を確認、遠隔操作しスマートフォンをロックするか中のデータを削除する
  - Android： Android デバイス マネージャー
  - iPhone： iPhone を探す

GPSで位置確認、遠隔操作で削除

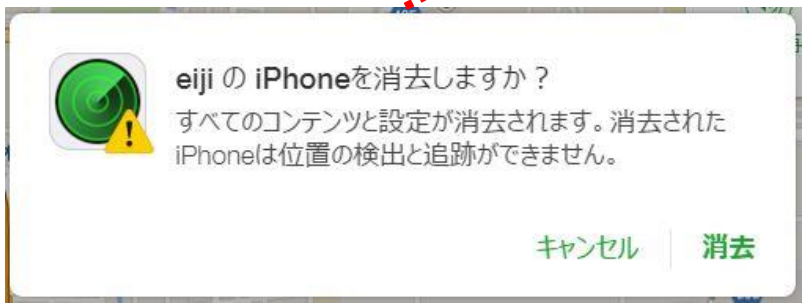
- iPhone を探す



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

スマートフォンを守る (2)

✓アプリケーションのインストールは慎重にする

- 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

✓ 使わなくなったスマホは初期化する

- 解約したスマホでもWiFiを利用してSNSやショッピングサイトにアクセスしたり、Webメールを利用したりできます。

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。

現在地

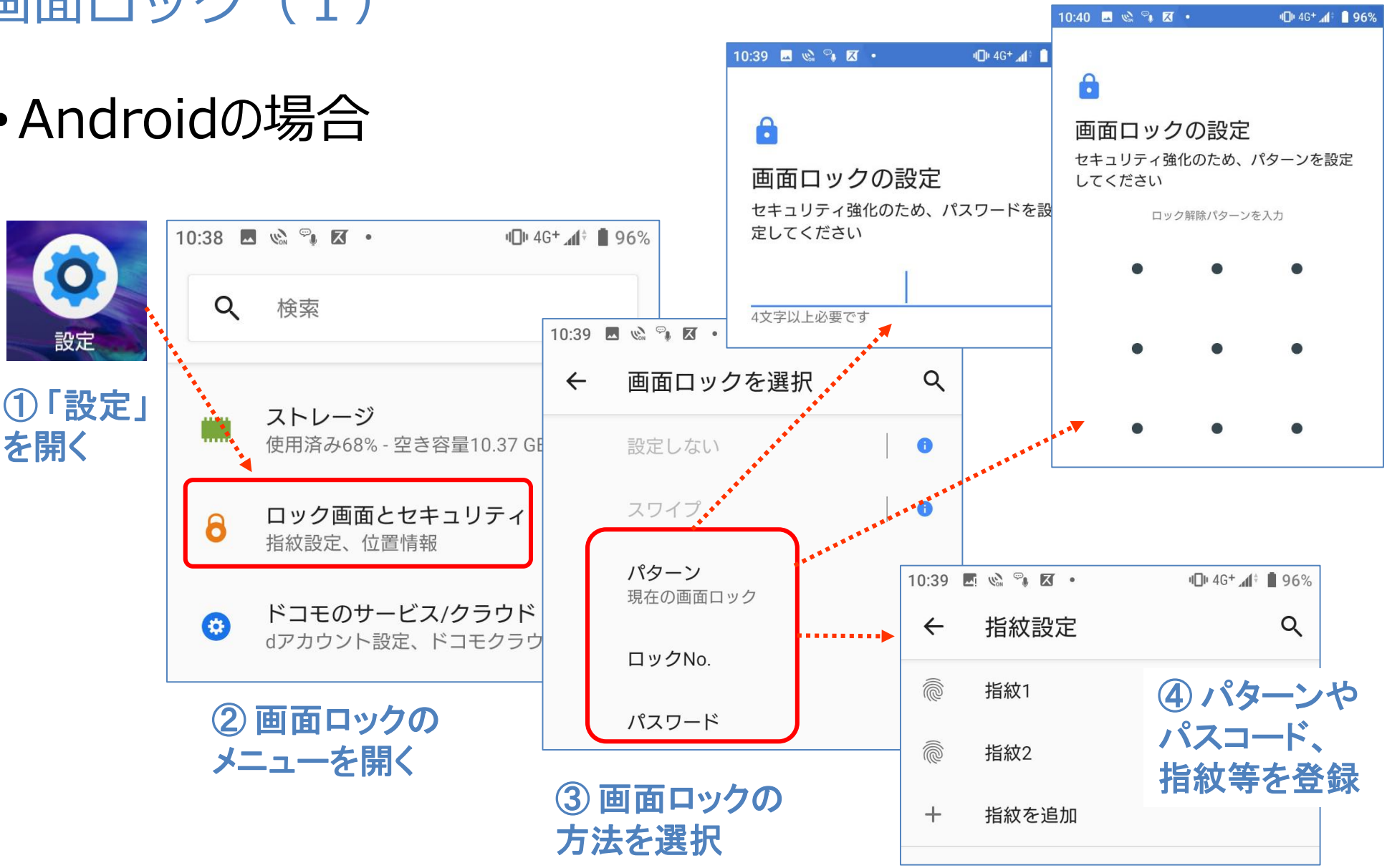
ユーザーのおおよその位置情報を取得することをアプリに許可します。この位置情報はネットワーク位置情報源(基地局やWi-Fiなど)を利用した位置情報サービスから取得されます。これらの位置情報サービスはONの状態にして、機器でアプリがサービスを利用できるようにする必要があります。アプリはこの位置情報を利用してユーザーのおおよその現在地を特定できます。

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。

画面ロック（１）

- Androidの場合



【注意】スマートフォンの機種やソフトのバージョンにより表示や設定方法が変わります。
詳しい設定方法は製品のマニュアルを参考にしてください。

画面ロック（２）

- iPhoneの場合

①「設定」を開く

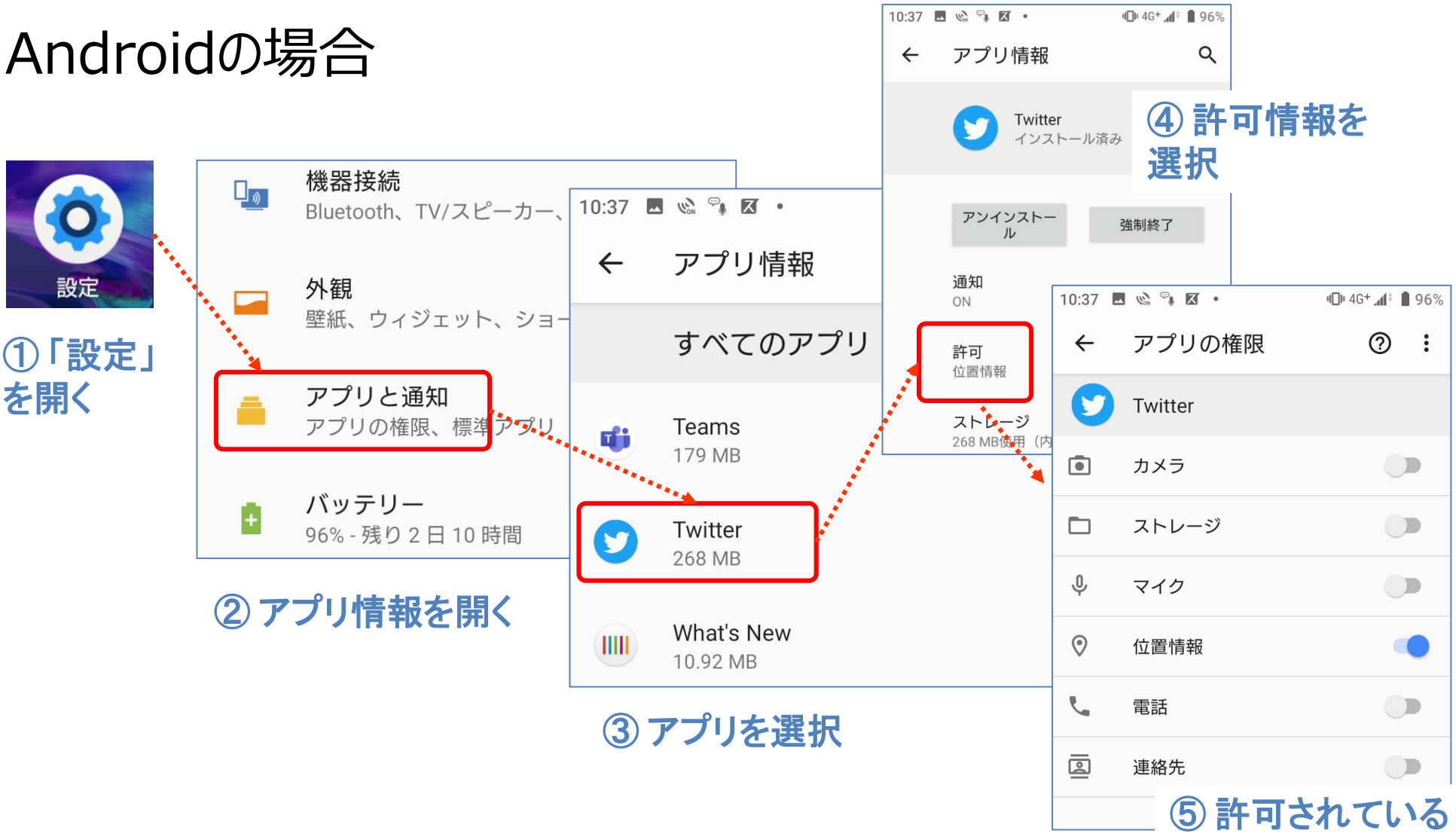
② IDとパスコードを開く

③ パスコードや指紋を登録する（機種によっては顔認証もある）

【注意】スマートフォンの機種やソフトのバージョンにより表示や設定方法が変わります。
詳しい設定方法は製品のマニュアルを参考にしてください。

アプリケーション許可情報（２）

- Androidの場合

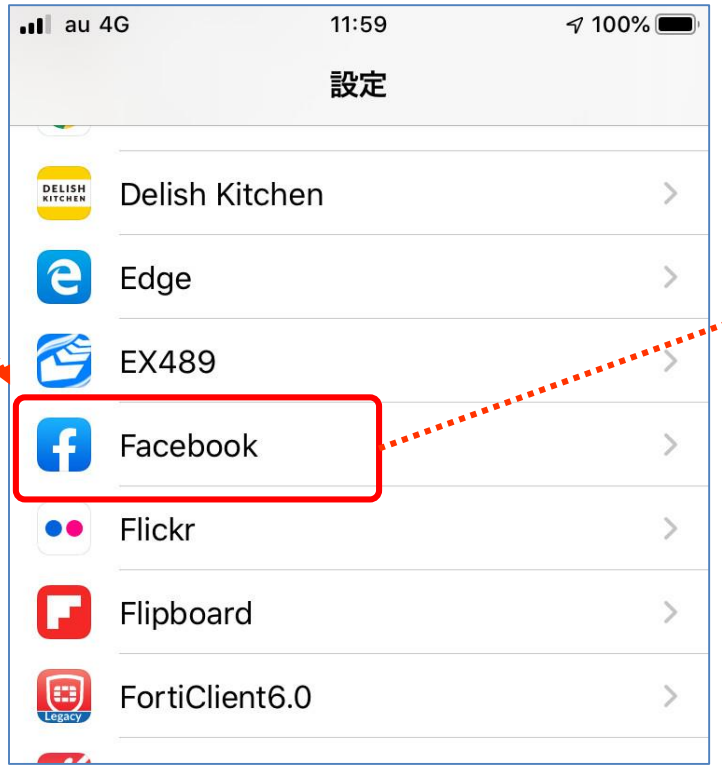


【注意】スマートフォンの機種やソフトのバージョンにより表示や設定方法が変わります。
詳しい設定方法は製品のマニュアルを参考にしてください。

アプリケーション許可情報（１）

- iPhoneの場合

①「設定」を開く



② アプリー覧からアプリを選択

③ 許可されている機能を確認

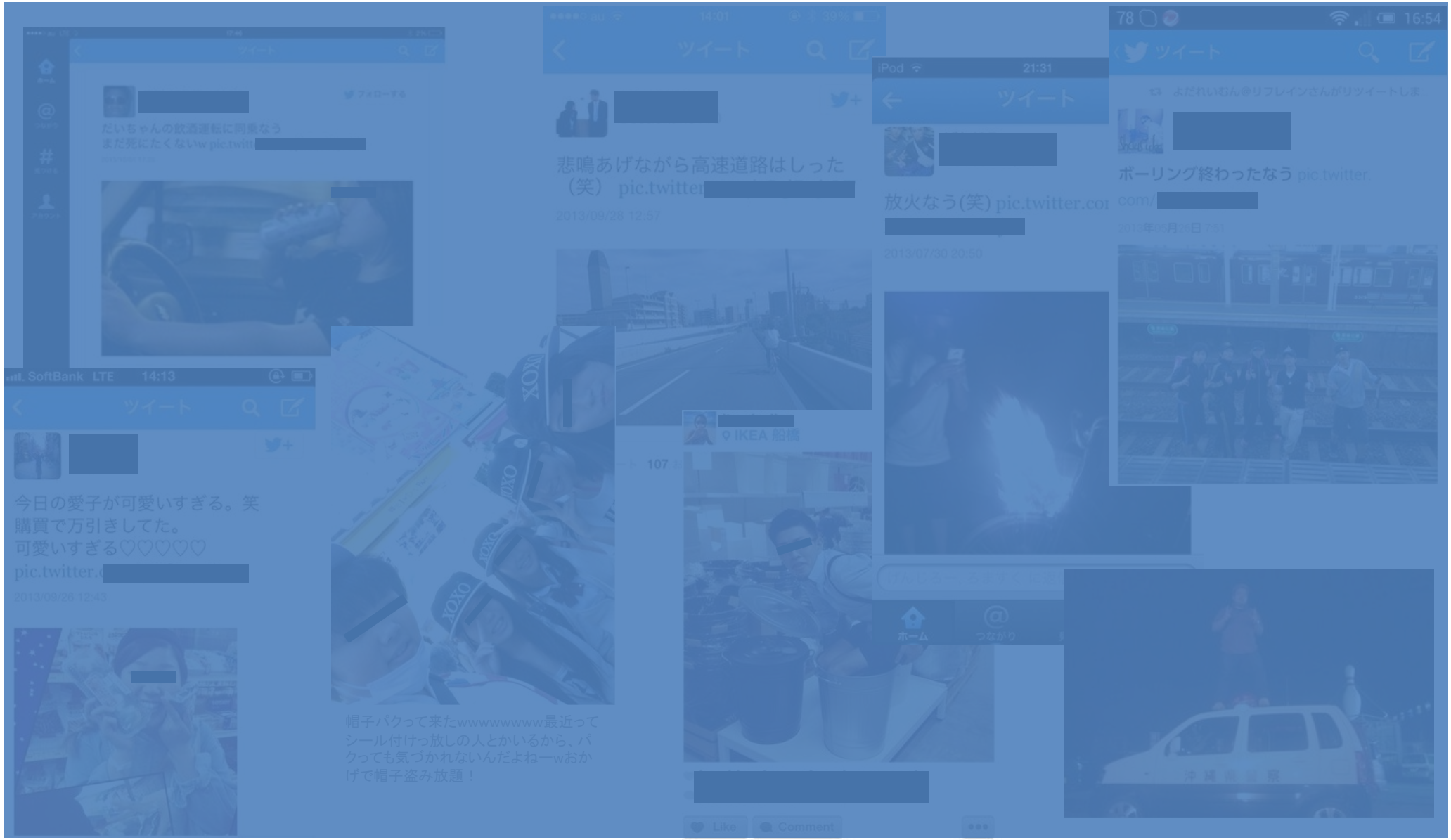
【注意】スマートフォンの機種やソフトのバージョンにより表示や設定方法が変わります。
詳しい設定方法は製品のマニュアルを参考にしてください。

1-2. SNSを安全に使う

ソーシャルメディア

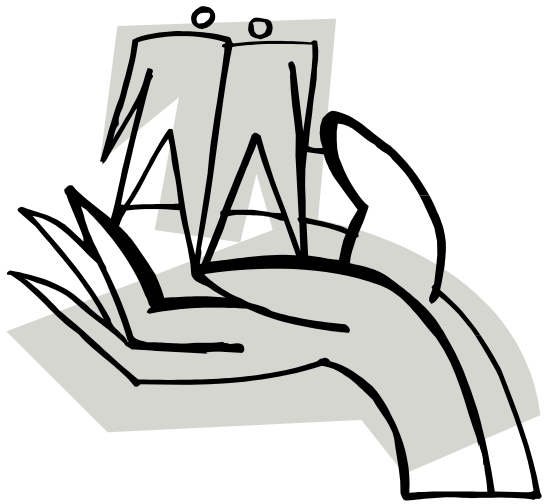
- Facebook、Instagram、mixi、Google+、Linkdein等のSNS（ソーシャル・ネットワーク・サービス）
- Twitter等のミニブログ
- Youtube、USTREAM、ニコニコ動画等の動画共有サイト
- その他ブログ、LINE、ゲームサイト内のコミュニティ等

バカッター


だいちゃんの飲酒運転に同乗なう
まだ死にたくないw pic.twitt
悲鳴あげながら高速道路はしった（笑） pic.twitter
2013/09/28 12:57
放火なう(笑) pic.twitter.cor
2013/07/30 20:50
ボーリング終わったなう pic.twitter.com/
今日の愛子が可愛いすぎる。笑
購買で万引きしてた。
可愛いすぎる♡♡♡♡♡
pic.twitter.c
2013/09/26 12:43
帽子パクって来たwwwwwwww最近ってシール付けっ放しの人とかいるから、パクっても気づかれないんだよねーwおかげで帽子盗み放題！
IKEA 船橋
ホーム
つながり
Like
Comment

ソーシャルメディアを使う時の心得

- ✓ 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
- ✓ ネットは匿名ではないことを知る
- ✓ 個人情報の書き込みは最小限に
- ✓ 公開範囲を最小限に



特に写真のアップには注意！

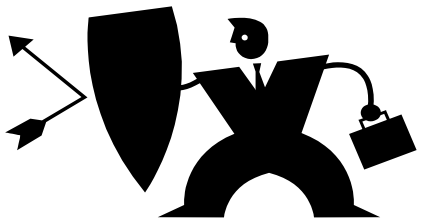
- 窓の外の風景から家の場所が分かる
- いつもの散歩道で待ち伏せされる
- 家族旅行中にドロボウに入られる

写真には大量の情報が
含まれている

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。



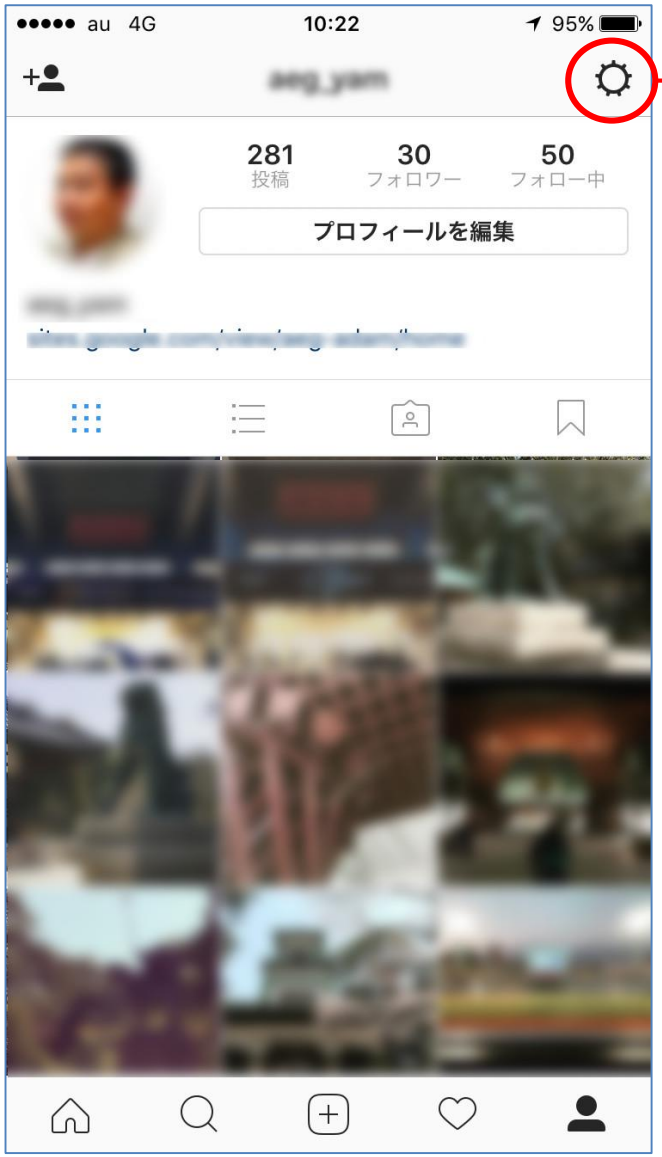
利用者が投稿した情報は、設定により自分の責任で守る必要がある。

Facebookの公開範囲設定

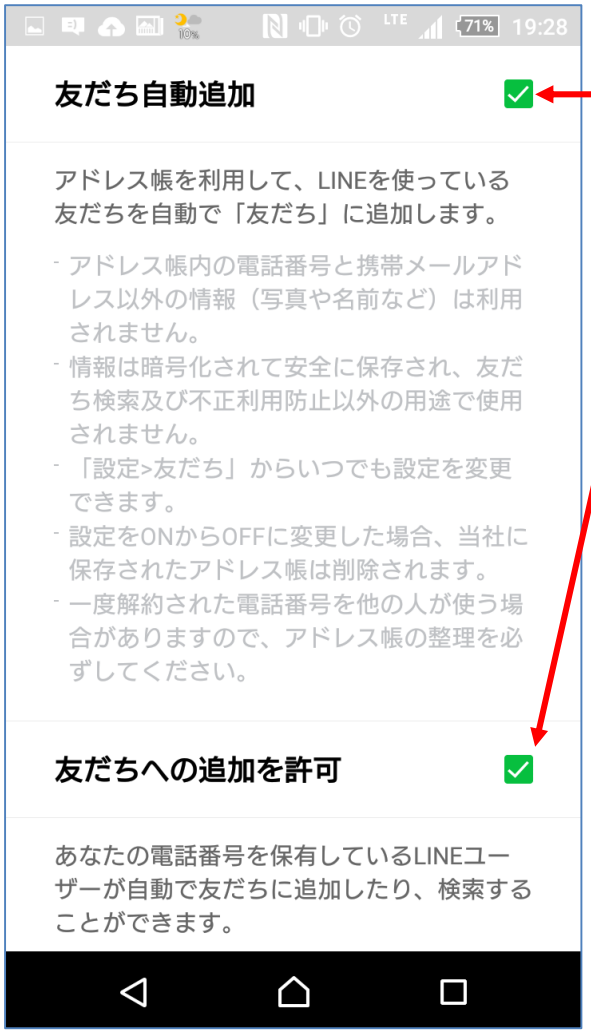
初期設定は「公開」になっているので、希望する範囲を指定する

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/

フェイクニュース（偽ニュース）に騙されるな

会社経営者の女性が、常磐自動車道で起きた「あおり運転暴行」事件の容疑者と同乗していた女性だとのデマを流され、批判する電話が会社に殺到し、業務に必要な電話を取ることができない等の被害を受けた。

デマを信じた愛知県豊田市の市議がインターネットで拡散し、女性から提訴され、責任を取って辞職。

芸能人らがインターネットにアップした「血液クレンジング療法（オゾン療法）」が、裏付けの不確かな医療行為として炎上。

芸能人などのインフルエンサーが、お金をもらってSNSで広めるステルスマーケティングも多いが、芸能人の写真が勝手に使われている広告もみられる。

フェイクニュース（偽ニュース）に騙されるな

- 一般個人の発信情報は疑う
- 発信しているサイトの特性を確認する
- 根拠が示されているか確認する
- いくつかの異なった情報をあたって見る

- 炎上を誘うような話だけでなく、涙を誘う感動話等も嘘であることが多い。

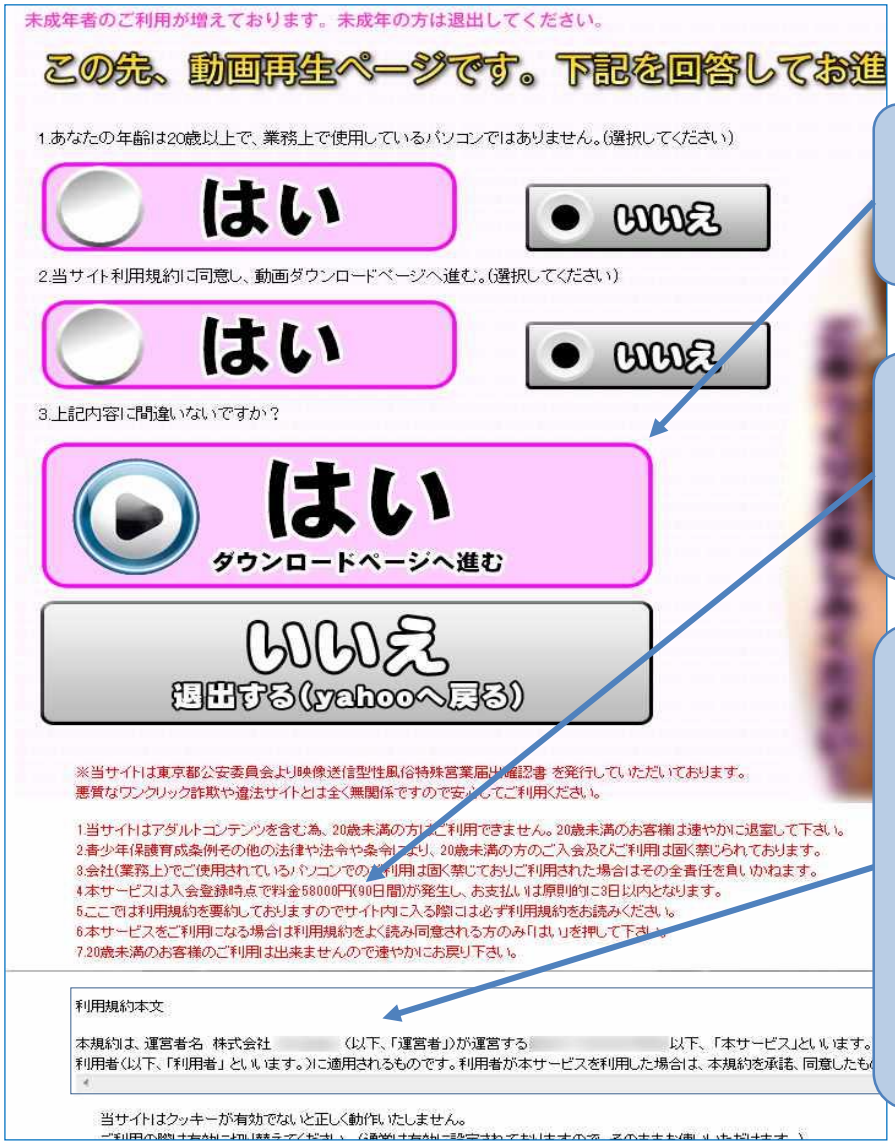
TikToKにISのプロパガンダ動画投稿

- IS（イスラム国）が、中国のIT企業「字節跳動（バイトダンス、ByteDance）」が運営するTikTok（ティックトック）にプロバガンダ動画を投稿
  - ISの力を誇示する、あるいは人材勧誘手段として利用する狙い
  - アジア圏の若者との接点を持つ意図もある

＜参考＞2019年10月22日 ウォールストリートジャーナル「イスラム国がTikTokに動画投稿、若者勧誘など狙いか」

1-3. ネット詐欺に注意

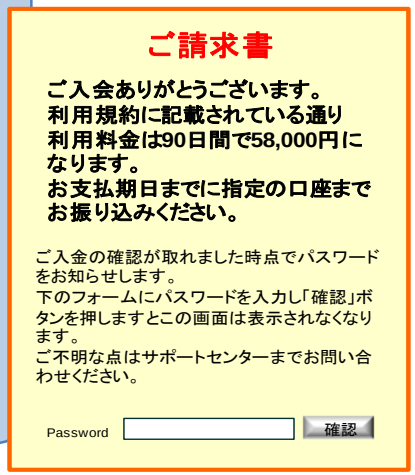
不正請求サイト



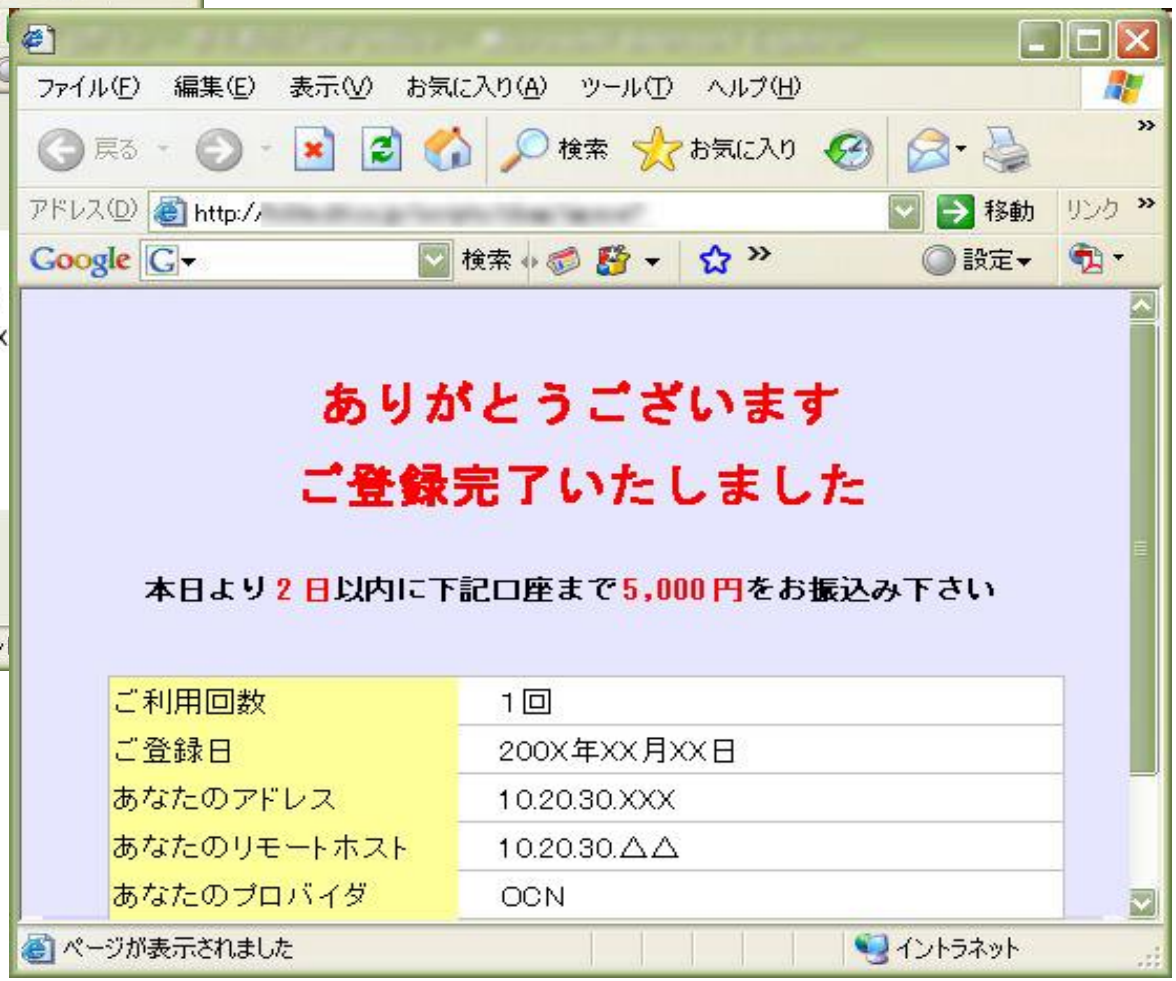
何度も「はい」を押させることで「ワンクリックではない」と主張

小さな字で“入会時点で**料金58000円**”が発生すると書かれている

小さな枠で**「利用規約本文」**が置かれている
“「動画を見る」ボタンを押した時点で入会とする”
“料金支払い完了まで、**請求案内が画面に表示**されることを承知したこととする”



不正請求サイト



確認画面でOKボタンを
押すと登録完了

不正請求（スマホ・携帯電話の場合）

■■■〇〇〇〇に入会ありがとうございます■■■
あなたの個体識別番号Docomo/2.0/D703i xxxxxxxxxxを登録させていただき入会手続きを完了しました。
■ご利用期間
90日間
■ご利用料金
¥58,000
■振込先
〇〇銀行〇〇支店（普）〇〇〇〇〇　口座名××
■お振込み期日
本日より4日以内
期日までに上記の口座までお振込み下さい。
期日を過ぎても入金が確認出来ない場合、規約に基づき個体識別番号をもとに当サイトよりご利用料金とは別に延滞1日に付き1,000円の延滞金を加算して直接請求いたします。

あわてないで不正請求

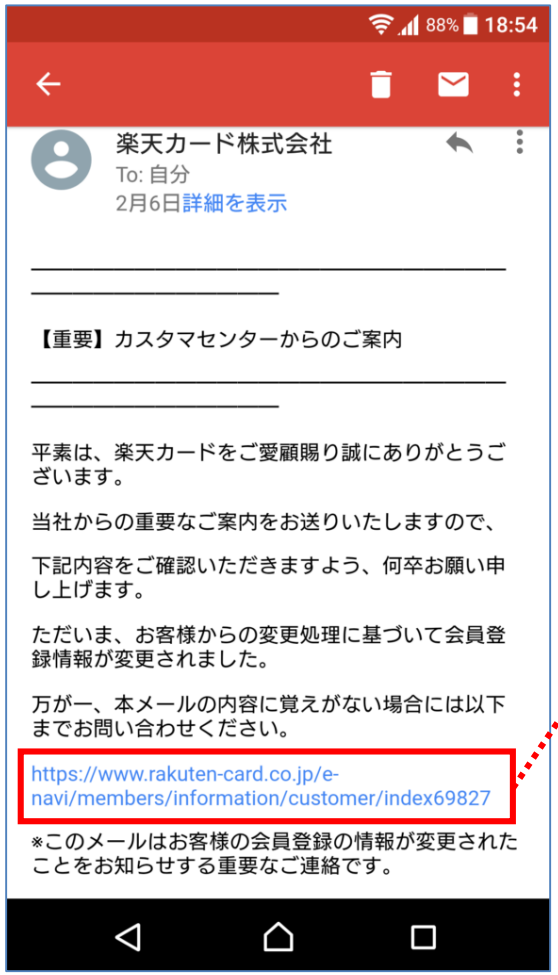
- 個人を特定されたわけではない
  - あなたのＩＰアドレス、プロバイダー名、個体識別番号などが表示されても個人を特定されたわけではない

✓返事を送ってはいけない
  - 「特定商取引法」で決められた手続きがなければ、契約したことにならない
  - 返事をしたり連絡を取ると被害が大きくなる

✓あやしいサイトには行かない
  - アダルトサイトの閲覧、アイドル名の検索で詐欺サイトへ誘導されることが多い

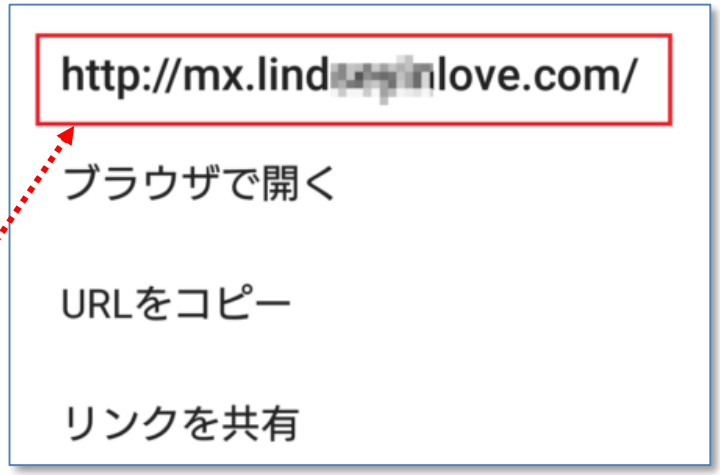
偽装メール による偽サイトへの誘導

- ばらまき型偽装メール



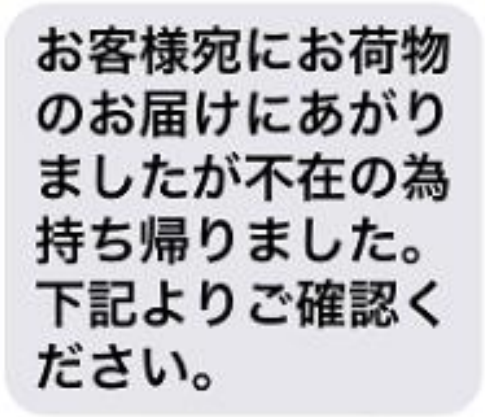
- 無差別に送信
- アマゾン、楽天、アップル、佐川急便、クロネコヤマトなどをかたることが多い
- ID/パスワードや個人情報を求める

実際のサイトは楽天ではない



偽装メール による偽サイトへの誘導

- ショートメッセージ（SMS）で届くこともある



Facebookメッセンジャーで届いた例

- **偽サイト（フィッシングサイト）に誘導されたり、ウイルスに感染したりする**
- **相手に登録していないはずのアドレスや電話番号に通知が来た場合は注意**

偽サイト（フィッシングサイト）

- 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

偽のサイトの見分け方

✓ URLが「https」からはじまっているか

- 個人情報やパスワードを入力するページは「http」ではなく「https」で始まる。

✓ SSL証明書の警告が出たらアクセスをやめる

- 「このWebサイトのセキュリティ証明書には問題があります。」と警告が出たら「ここをクリックしてこのWebページを閉じる。」を選択し画面を閉じる。

✓ ウイルス対策をしっかり行う

- フィッシングサイトへアクセス時に警告表示

1-4. パスワードを守る

LINEで友人になりすまし、電子マネーを窃取

Facebookで友人になりすまし、模造品販売サイトへ誘導

「ソニーポイント」に不正アクセス　75万ポイント不正交換

芸能人のプライベート写真を覗き見

あなたのパスワードは大丈夫？
～インターネットサービスの不正ログイン対策～

予測されやすいパスワードも見直す

AKB48HKT48

password1

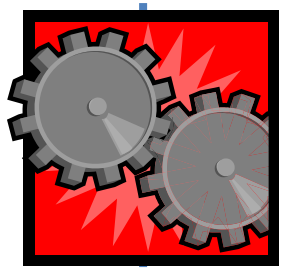
suzukisuzuki

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

原因は「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

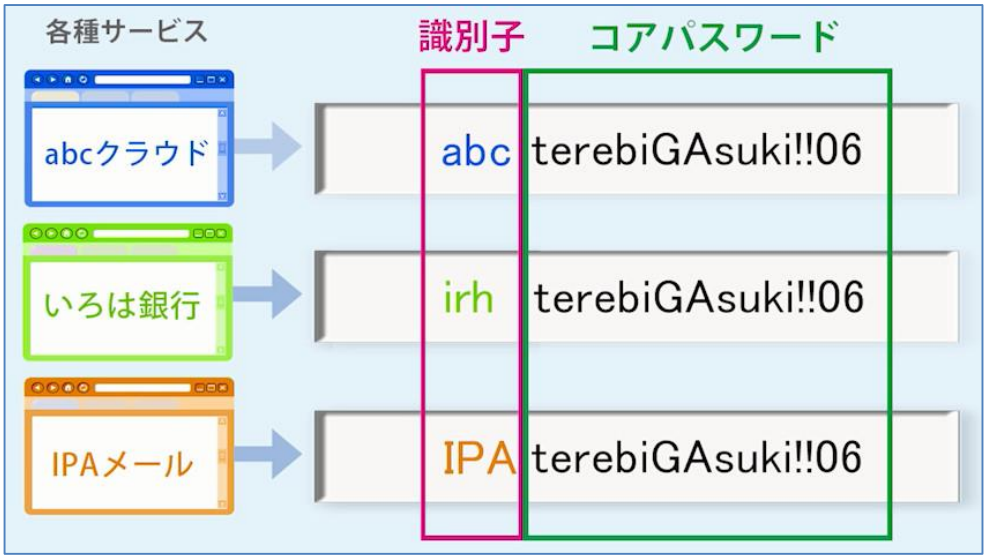
複雑に

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

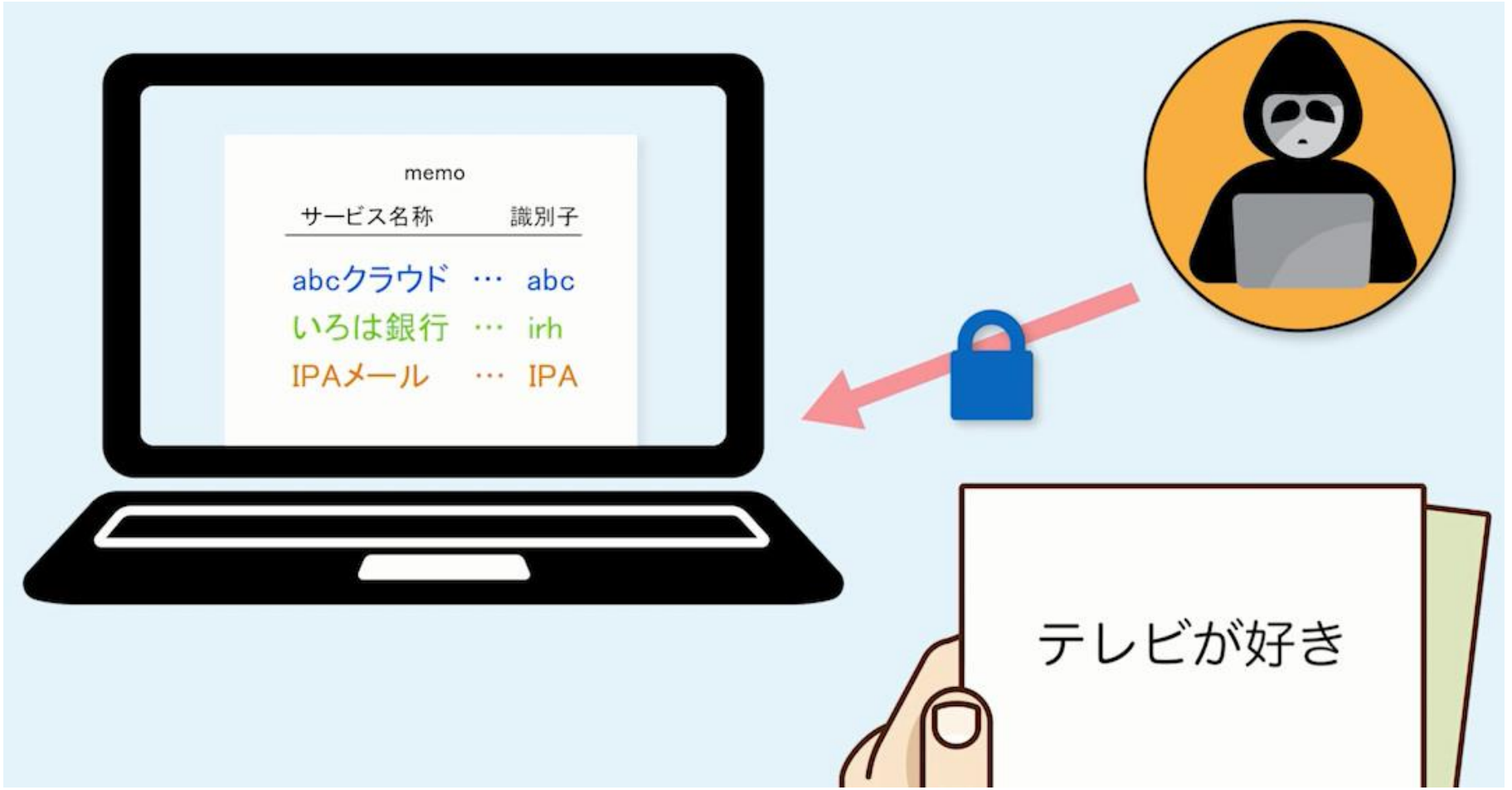
② サービスごとに異なるパスワードの作成



＜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」

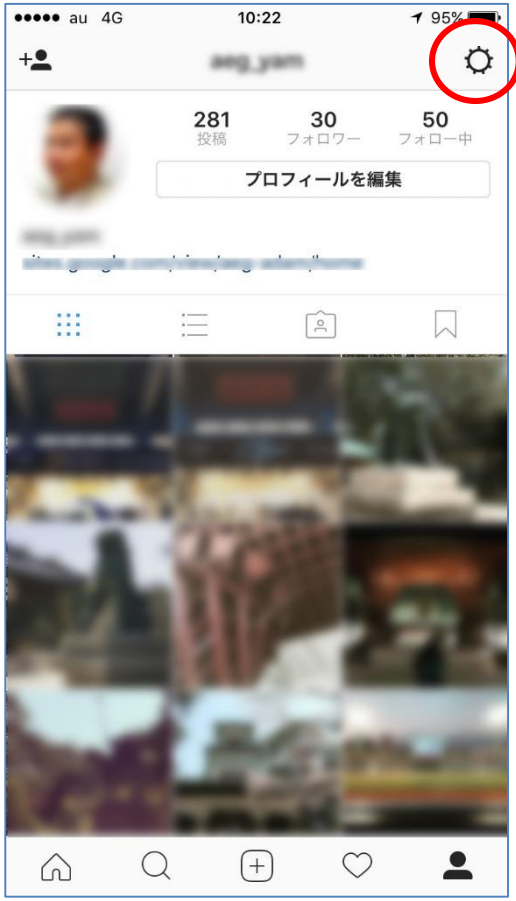
質問「あなたの母親の旧姓は？」
応え「前田かもしれない」

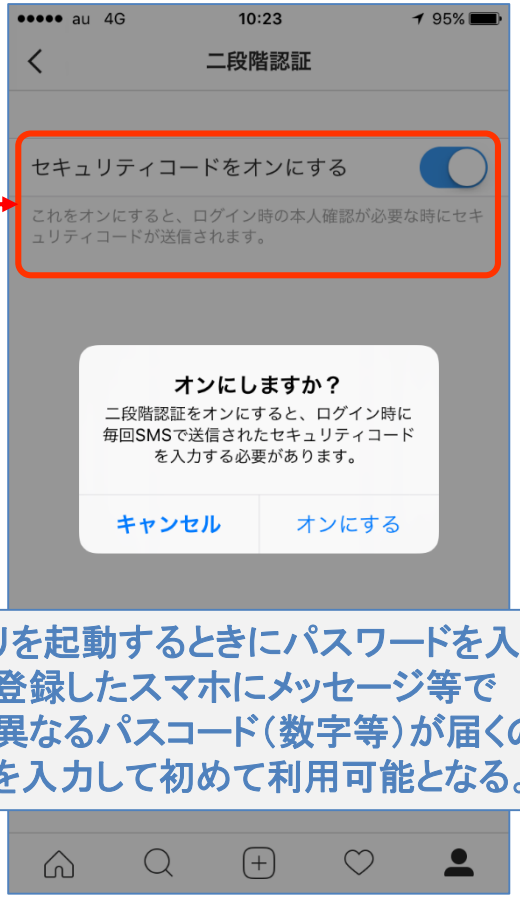
＜出典＞ 独立行政法人 情報処理推進機構（IPA） 啓発ビデオ
https://www.youtube.com/user/ipajp

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。
  - 記憶しているもの（暗証番号の入力）
  - 持っているもの（スマホに届く数字の入力）

これは二要素認証の例





アプリを起動するときにパスワードを入れると、
予め登録したスマホにメッセージ等で
毎回異なるパスコード（数字等）が届くので、
それを入力して初めて利用可能となる。

パスワードが漏えいしたと思ったら

✓ パスワードを使い回しているサイトやサービスのパスワードを変更する

- 利用しているサイトやサービスの最終アクセス時間を確認する
  - 心当たりのない日時にアクセスしている場合は、不正アクセスされた可能性がある
- 決裁に利用しているサイトやサービスの購入履歴を確認する
  - 心当たりのない購買履歴がある場合は、クレジットカード会社に通知する
- 心当たりのない書き込みや投稿がないか確認する
  - 自分になりすました書き込みがある場合は、友達に注意を促す

1-5. 困ったときは

書き込みを消したい (1)

- 書き込み先サイトの管理運営者へ削除申請する
  - 事前に、利用規約や削除ガイドラインを参照する
    - 削除依頼の方法を確認
    - 削除条件を確認：　虚偽の内容である／人権を侵害する内容である・・・
  - 削除依頼があったことを投稿者に事前確認する場合があることに注意
  - 一部の掲示板等では、法人や第三者からの削除依頼について公開される可能性があることに注意

➢ 削除依頼する際に、こちらのメールアドレスを知られたくない場合は、グーグル Gmailやマイクロソフト Hotmail、ヤフー Yahoo!メール等で一時的なメールアドレスを作成し、それを連絡用に用いる

書き込みを消したい (2)

【削除手順】

- 書き込みのあるページのURL（http://・・・）を記録して画面をコピーする
  - 画面コピー（画面キャプチャ）の方法が分からない場合は、画面を印刷するかスマホ等のカメラで画面を撮る。
  - URL、投稿者のアカウント名、投稿内容・日付、印刷（取得）日付が含まれるようにコピーする。
- 書き込みのある掲示板等の利用規約や削除ガイドラインが指定する、問い合せフォームや削除依頼様式等を用いて削除依頼する。
  - 削除依頼に際しては基本的に個人情報（氏名、連絡先）を知らせる必要はない。ハンドルネームや一時的なメールアドレスを用いてやり取りをする。

- 相手が削除依頼に応じない場合
  - 各地域の法務局へ相談

相談窓口

- ワンクリック詐欺、オークション詐欺、身に覚えのない請求
  - 国民生活センター 消費者ホットライン　188（局番なし）
  - 通販110番／社団法人日本通信販売協会　http://www.jadma.org/
  - 一般社団法人ECネットワーク　http://www.ecnetwork.jp/
  - 経済産業省／消費者相談室　http://www.meti.go.jp/intro/consult/a_main_01.html
- IPA「情報セキュリティ安心相談窓口」

  https://www.ipa.go.jp/security/anshin/

  ① 「よくあるご相談」で類似の質問を参考にする

  ② 「役立つコンテンツ」や「公開情報」を見て解決

  ③ 「安心相談窓口」に相談する

  TEL: 03-5978-7509（相談料無料）

  10:00-12:00 / 13:30-17:00 土日祝日・年末年始除く

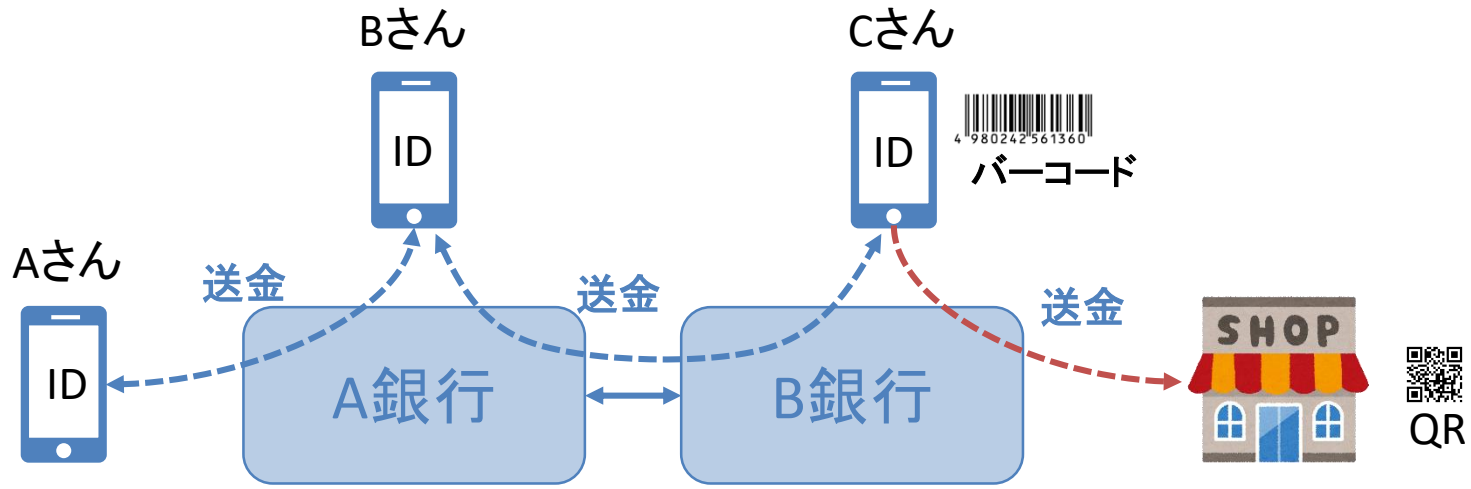
  E-mail: anshin@ipa.go.jp
- 詐欺で被害を受けた、ストーカー被害にあっている、出会い系でトラブルになっている、脅迫を受けた、ネットで誹謗中傷された
  - 警視庁ハイテク犯罪対策総合センター

    http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku1.htm　　TEL: 03-3431-8109

2. 情報セキュリティトピックス

2-1. QR決済サービスへの不正アクセス

QR決済とは



- 個人間送信がベース
  - IDを知っている者同士の送金
  - IDを知らせる方法としてQRコードやバーコードを提示
- 銀行法の改正と資金決済法の制定・改正で銀行以外が電子決済代行業が可能に
- 国内の代表的なサービス
  - Origami Pay、LINE Pay、楽天ペイ、PayPay 、d払い、au PAY、merpay

7payの不正アクセス

- 専門会社「セブン・ペイ」を設立して決済サービスを開始
- 事件の概要
  - 7payへの不正アクセスにより、不正チャージ、不正購入が発生
    - 不正アクセス被害 約900人／被害額 約5580万円
- 問題点
  - 技術的問題： グループ各社のサービスの決済に利用する共通アプリとして構想したが技術的に困難
  - スケジュールの問題： 10月1日のポイント還元施策に間に合わせるための7月1日にリリース

↓

「セブン-イレブンアプリ」にアドオン的に追加された「決済機能」として提供

  - パスワードリセットの仕組みの問題も指摘されている
- Security by Design
  - 情報セキュリティを企画・設計段階から確保するための方策
- 社長は「二段階認証」を知っていないとダメなのか？
  - 参考
    - https://www.huffingtonpost.jp/entry/7pay-service-end_jp_5d479ee4e4b0ca604e34313a
    - https://piyolog.hatenadiary.jp/entry/2019/07/04/065925
    - https://news.yahoo.co.jp/byline/mikamiyoh/20190704-00132766/

2-2. 就職支援サイトの個人情報利用方法不備

リクナビにおける学生情報の利用方法の不備

- インシデント概要
  - リクルートキャリアは8月1日、「リクナビDMPフォロー」のサービスの中で、サイトの行動履歴などを基に計算した内定者個人の内定辞退率を、学生の同意が不十分なまま採用企業38社に提供していたと発表。
  - 2019年7月初旬に行政機関の個人情報保護委員会から「個人情報の第三者提供に関する規約が就活生にとって分かりにくい」との指摘を受け、8月5日には当該サービスを廃止。
  - サイト上にあるプライバシーポリシーの同意取得画面の一部で「リクナビDMPフォロー」に関する表記もれと、同意取得フローの考慮不足があり、7983人の学生から適切な同意を得られていなかったことが判明したのが廃止の理由。
- 「リクナビDMPフォロー」とは
  - 今年度リクナビに登録している特定の学生のサイトの行動履歴を分析し内定辞退率を算定して契約企業に提供するサービス。

リクナビは何が悪かったのか

- 問題点1： 個人情報利用目的の通知の方法の不備
  - 当サービスに登録時に個人情報の利用目的をサイト上で表示していたが、その内容が「個々の辞退率を予測し、それを企業に提供される」ことまで想定できる表現でないことが問題とされた。
- 問題点2： 個人情報の第三者提供の手続き不備
  - 内定辞退率は統計的データであるが、特定の学生が特定の企業の内定を辞退する確率という個人に紐づいた情報として提供されるものであり、個人情報の第三者提供にあたる。しかし、問題点1にあるように学生が自分の個人情報がどのような目的で利用されるか「理解」していたと言いづらい中で、もし同意ボタンを押させていたとしても同意を取ったとみなすのは難しい。
- 問題点3： 企業との契約内容の曖昧さ
  - 本サービスは、企業が内定辞退の予想を元に採用人数を調整することを目的としており、リクルートナビは、本サービスを利用する企業に対し採用の可否の判定には使わない同意書を得た上で内定辞退率を提供していたが、その通り利用されていたかは学生からは見えず不信感が生じた。

参考 https://www.sbbit.jp/article/cont1/36852
https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/02708/?n_cid=nbpnxt_twcm_it
https://business.bengo4.com/articles/613

2-3. ビジネスメール詐欺

ビジネスメール詐欺の被害例

- ビジネスメール詐欺（BEC： business email compromise）
  - 実在する取引先に成りすまして偽装メールを送って嘘の指示をして金銭を窃取するなどを行う攻撃手法
- 被害例
  - トヨタ紡織 ベルギーの子会社
    - 2019/8/4　外部からの虚偽の指示により、経理担当者が送金関連の情報を操作したことで、40億円の資金が流出。
  - 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。

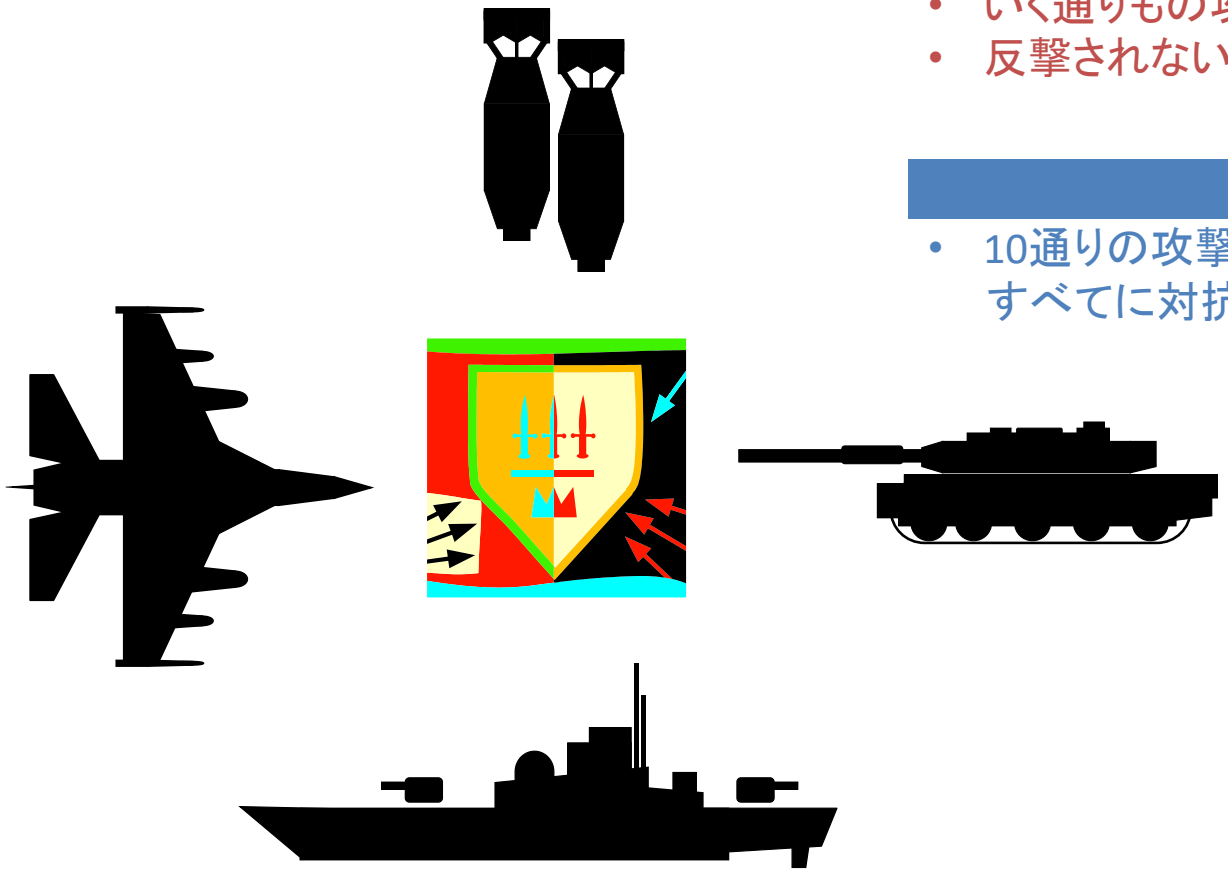
ビジネスメール詐欺の対策

- 普段と異なるメールに注意
  - 送金指示の通知
  - 急な変更依頼（振込先の変更等）
  - 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
  - 他人に予測されにくいパスワードの設定。多要素認証の導入。

＜参考＞ IPA： 2018年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

2-4. 高度化するサイバー攻撃

サイバー攻撃は攻める方が断然有利



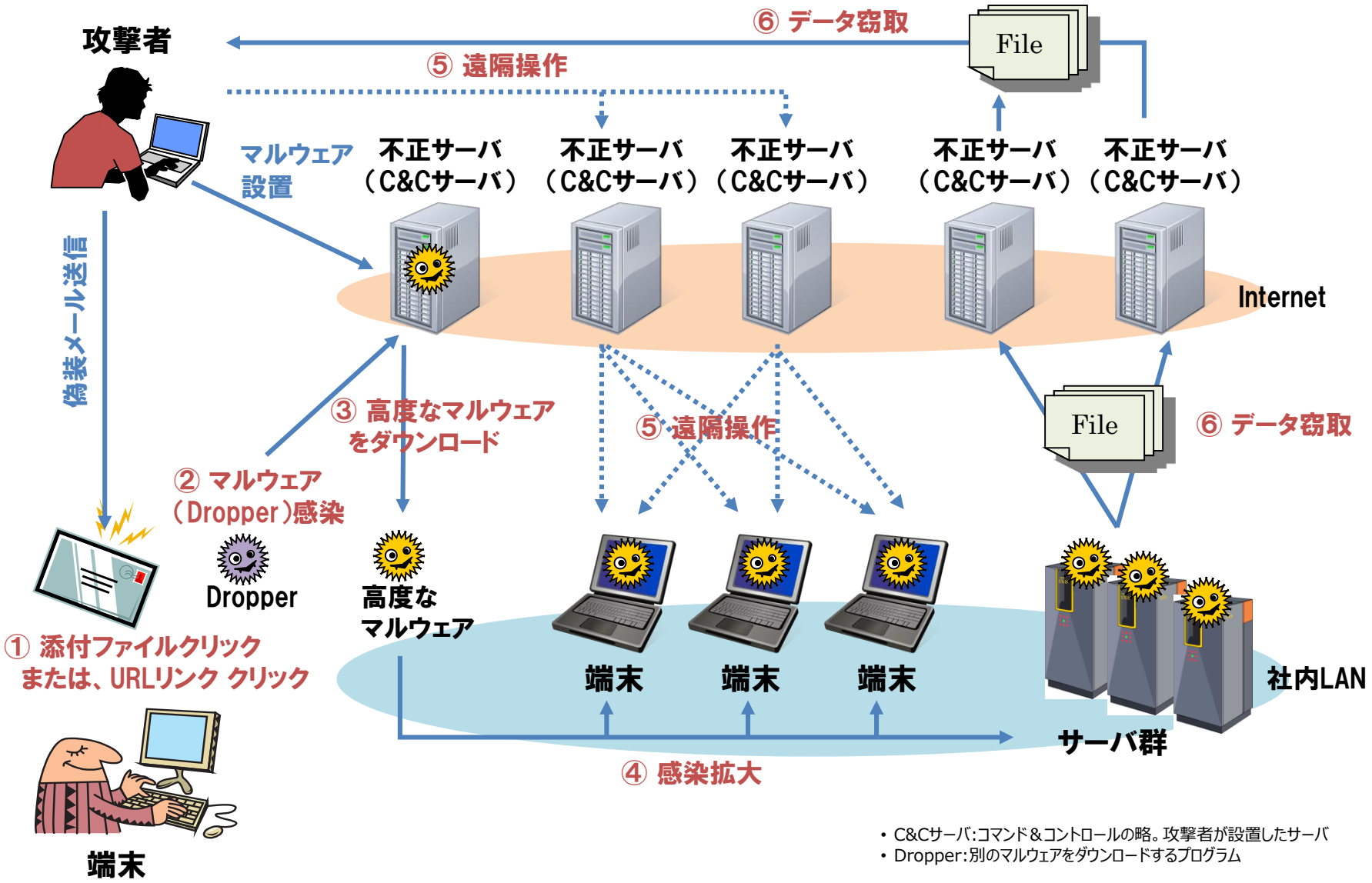
攻撃する側

- 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

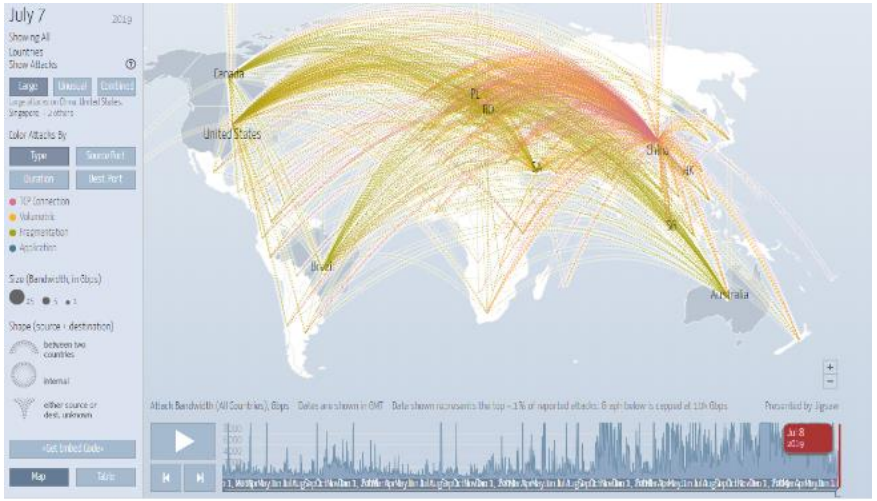
サイバー攻撃の流れ



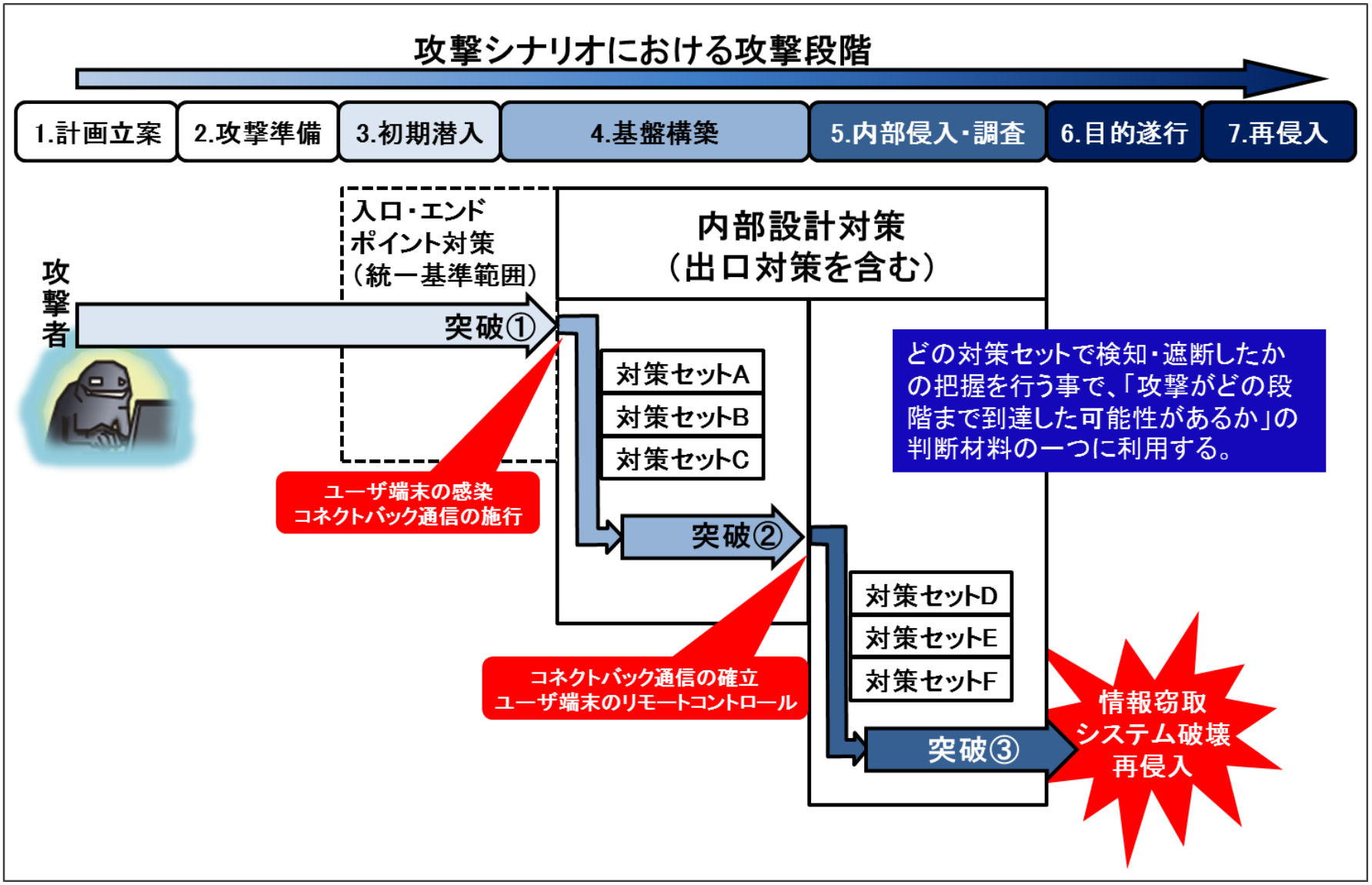
- C&Cサーバ:コマンド＆コントロールの略。攻撃者が設置したサーバ
- Dropper:別のマルウェアをダウンロードするプログラム

他国からの高度な攻撃

- 他国の国営の攻撃組織が関与
- 相手国の経済動向や政策を窃取
  - 経団連、シンクタンク等
- 数年間かけて継続的に侵入
- 高度な技術
  - 検出できないウイルス
    - ウイルス対策ソフトで検出できないことを試してから送り込み
  - ウイルスが端末毎に変化
    - 1台の端末から検出しても他の端末で検出できない
  - 指令を出す不正サーバ（C&Cサーバ）の所在が頻繁に変化
    - 不正サーバのアドレスが頻繁に変化するため不正サーバへの通信を遮断できない
  - システム管理者が常時監視されている
    - メールの内容も監視されているので対策計画も筒抜け
  - 対策の裏をかく
    - 端末を入れ替えてもすぐにウイルス感染を繰り返す
- きっかけはオーソドックス
  - 偽装メールでウイルスを送り込む



対策のための参考資料（多層防御）



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)

対策例

- 対策セットA
  - ブラウザのプロキシ設定を有効にする
  - ファイアウォールにおいて、内部から外部へのフィルタリングルールを設計・設定する
- 対策セットB
  - プロキシの認証機能を有効にする
  - ブラウザのオートコンプリート機能を禁止する
  - プロキシ認証ログを監視・分析する
- 対策セットC
  - プロキシにACLを追加する
  - 外部通信を計画的に遮断し、長期間維持されたセッションを発見する
- 対策セットD
  - 運用管理専用の端末を準備する
  - 運用管理セグメントを構築する
  - 業務ごとのネットワーク分離とアクセス制御を設計する
- 対策セットE
  - ユーザ端末間のファイル共有を禁止する
  - 認証失敗ログの出力を設定する
  - トラップアカウントを作成し認証試行を監視する
  - タスクスケジューラやPsExecの実行を監視する
- 対策セットF
  - ユーザ端末で使用するアカウントの権限を最小化する
  - ドメインの管理者アカウントを使用する業務を最小化する
  - Domain Adminsグループのログイン履歴を確認する

2-5. AIとセキュリティ

AIのセキュリティ留意点 (1)

- AI（Artificial Intelligence） ＝人工知能
  - コンピューターが物事やルールを理解するための仕組み
- AIの分類
  - 特化型と汎用型
    - 特化型AI（AGI） ：個別の領域に特化して能力を発揮するAI（現在主流）
    - 汎用型AI（GAI） ：異なる領域で多様な問題を解決するAI
  - 強いAIと弱いAI
    - 強いAI：人間と同様の精神能力を有し、人間と同じような動作をするAI
    - 弱いAI：人間の持つ力を模倣し、人間よりも正確・迅速に処理するAI （現在主流）
- AIの活用
  - 言語： 翻訳、構文理解、文章創作等の自然言語の処理
  - 音声： 音声認識、音声→文章変換、翻訳、スマートスピーカーへの応用
  - 画像： 物体認識、顔識別、画像や映像の加工、スマホ美肌処理などに応用
  - 制御／推論：未知の状態を予測、家電や自動車の制御、通販サイトでのおすすめ商品の表示等に応用

AIのセキュリティ留意点 (2)

- AIに関する留意点（主にディープラーニングの場合）
  - 処理結果の正しさの検証が困難
  - 教師データの質や量により処理結果が偏ることがある
  - AIの意思決定に対する法的責任があいまい
  - 人間の能力を超えたAIが制御できなくなる可能性
- 翻訳サービスなどにおける留意点
  - インターネット上のAIを使用した翻訳サービス等は、サービスの精度を上げるために入力された文章をや出力した文章を教師データとして活用されることに留意。
- 情報セキュリティ分野におけるAI
  - AI技術を活用したサイバー攻撃の可能性
    - 機械学習アルゴリズムを使ってネットワーク内でのユーザーの動作を模倣して検出を回避
  - AI技術を活用したセキュリティツール
    - 正常なファイルの特徴、正常な通信の特徴等を学習させ未知の攻撃へ対抗

教師データ： 機械学習においてあらかじめ与えられる例題と答えについてのデータ

ご清聴ありがとうございました