サイバーセキュリティリーダー養成講座

サイバーリテラシー

2017年11月20日　会津大学

2017年12月4日　ビッグパレットふくしま

中村章人

会津大学

nakamura@u-aizu.ac.jp

Rev. 2

講義の目的

- スマホでの危険行為と対策、インターネットを安全に使うための注意点
- （世の中の実際の事件や身の回りに存在する危険を理解し、考えることを通して、インターネットを安全に利用する素養を身につける）

講義の内容

1. インターネットの世界
2. 不正アクセス等の状況
   統計、事例等
3. 具体的な事件と自衛策
4. なぜ被害がなくならないのか？
   環境の変化、人の特性
5. まとめ

インターネットの世界

- インターネットの特徴
- 知識、モラル、マナー、法律、自衛

インターネットが発展・普及した要因

- 情報処理と通信の両方が統合されたシステムを実現できた
  - 情報を収集し、処理し、記憶できる
  - 地理的に離れていても情報交換できる

- 情報処理 = コンピュータ（今ではスマホも）
- 通信 = ネットワーク

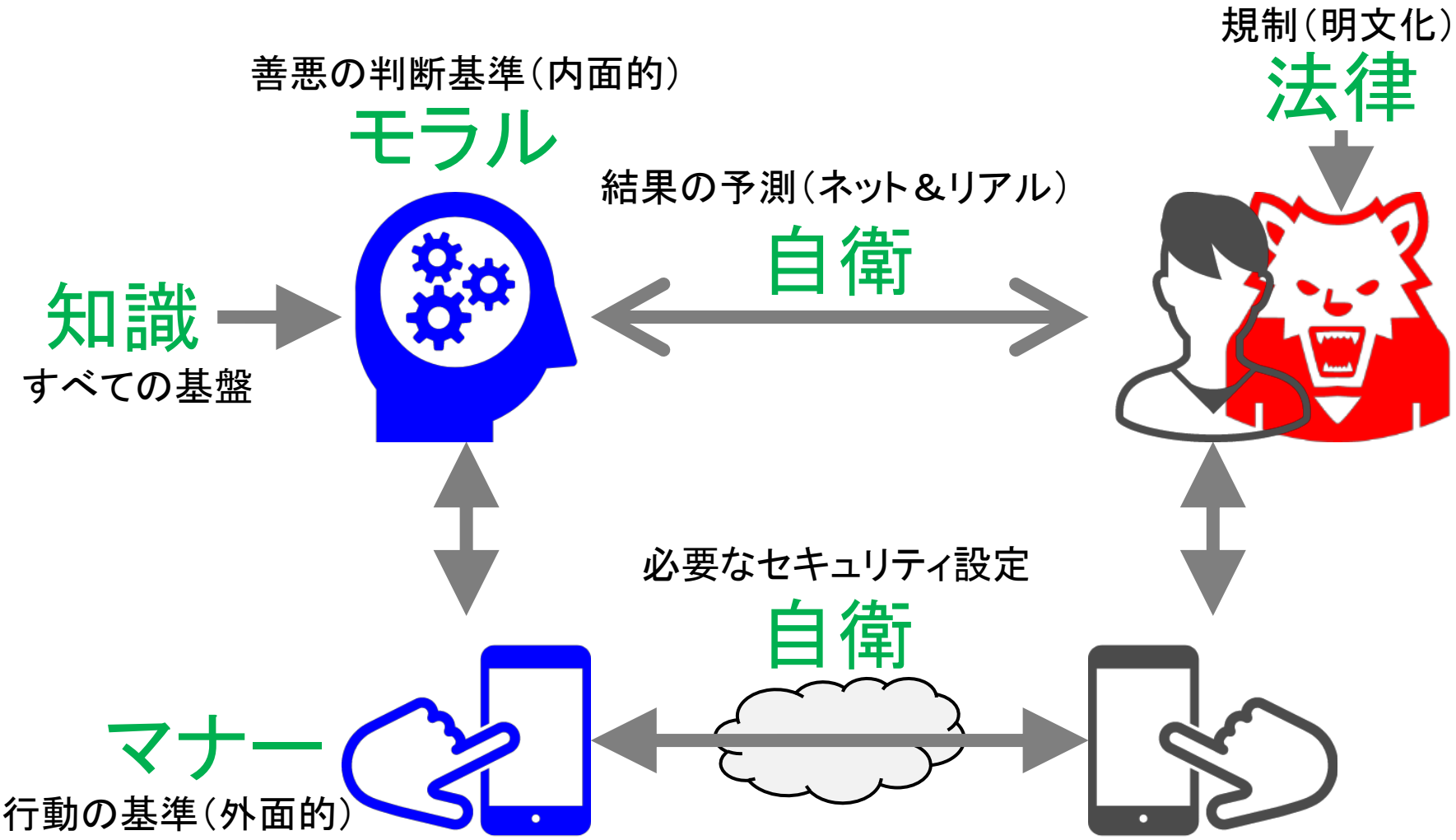
インターネット（the Internet）の特徴

- 世界規模の、相互接続されたネットワークの集合体
- 約束（規約）にしたがい、自律と協調で運用
- さまざまな利用者、自由な情報発信、匿名性

インターネットを楽しく安全に使うには

知識、モラル、マナー、法律、自衛が重要

知識、モラル、マナー、法律、自衛



マインドセット（考え方、心構え）

安易な過信

- これまで問題はなかった、今後もない
- 問題が起きても、自分は対処できる
- 知人から得た情報は正しい

よく考えて

慎重に

知識、モラル、マナー、法律、自衛

法律

情報セキュリティに関連する主な法律

- 刑法
- 不正アクセス禁止法
- 特定電子メール法
- 不正競争防止法
- 電子署名法
- 民法

主な不正アクセス行為

- 他人のID・パスワードを盗用・流布する
- 認証機構を騙す
- マルウェアを利用して不当な利益を得る、業務を妨害する
- データを破壊・改変する、システムを誤動作させる
- コンピュータウイルスの作成・提供・取得・保管
- 機密情報を漏らす

不正アクセス等の状況（統計、事例等）

- 情報漏えい
- 不正アクセス
  - システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を（ネットワークを介して）意図的に行うこと
- マルウェア、ランサムウェア
  - 悪意を持って作成された、望まない結果をもたらすプログラム
  - ファイルを暗号化し、身代金を要求するマルウェア
- DoS/DDoS攻撃
  - サービス妨害（Denial-of-Service: DoS）攻撃。正当なサービスの利用を妨げる
- 現実世界への影響
- 特殊詐欺、ビジネスメール詐欺
  - 業務上のメールを利用する詐欺

情報漏えい事故（日本）

JTB（2016年6月）

- 標的型メールによる遠隔操作ウイルスで顧客情報が漏えい（最大793万件※1）
- 行政からの調査指示、海外からの渡航者が一時的に減少？

※1 後日、679万人に修正

日本年金機構（2015年5月）

- 標的型メールによる遠隔操作ウイルスで年金加入者情報が漏えい（約125万件）
- 基礎年金番号・手帳・証書の再発行、マイナンバーの利用開始を延期

ベネッセ（2014年7月）

- 委託企業の社員が顧客情報を漏えい（約3,500万件）
- おわびの手紙と金券（500円）

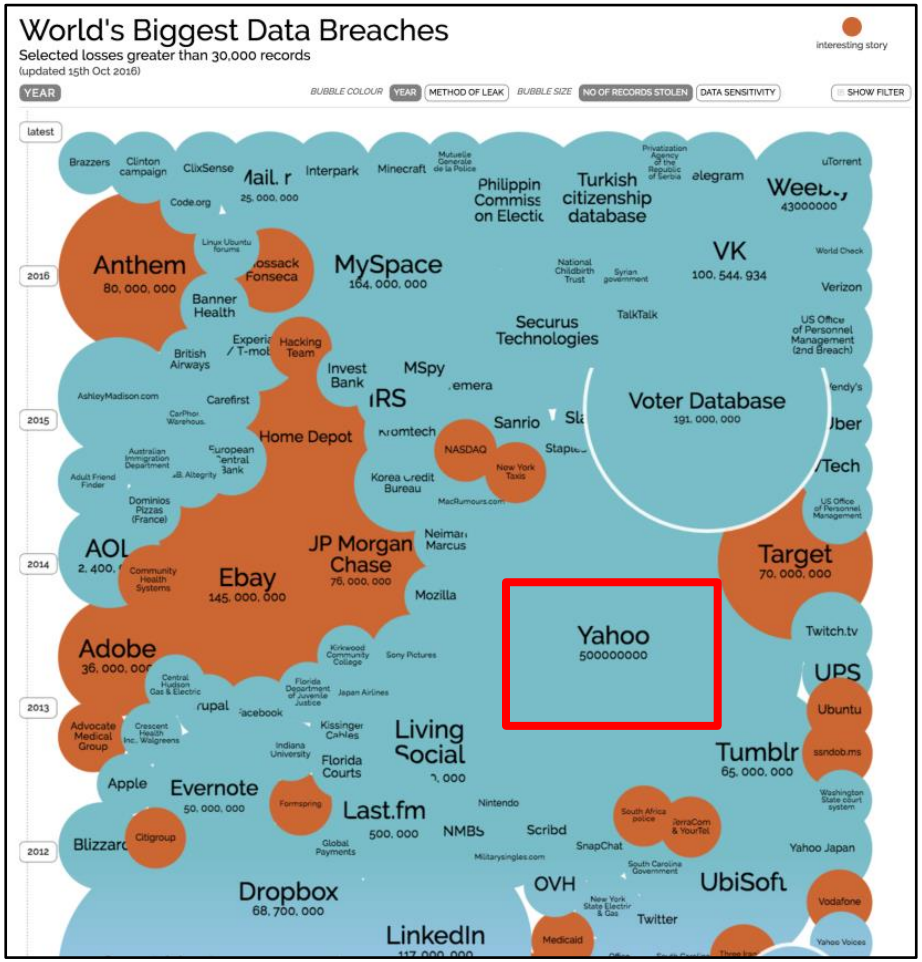
※2 現ソニー・インタラクティブエンタテインメント

ソニー・コンピュータエンタテインメント※2（2011年4月）

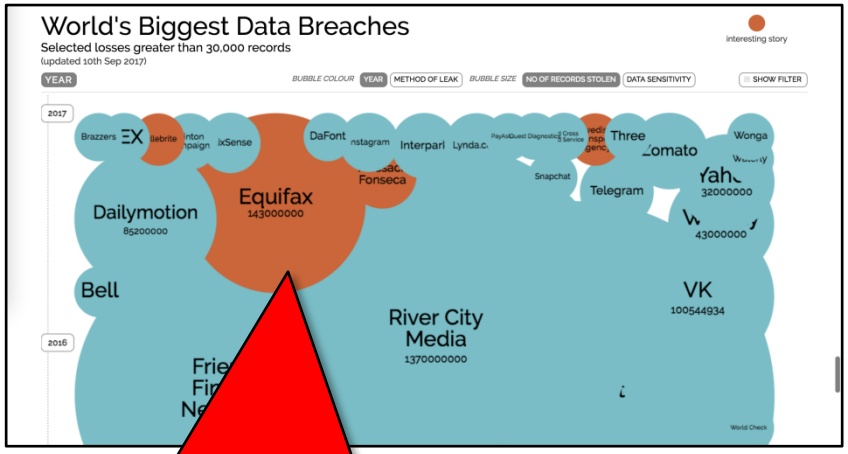
- PlayStation NetworkとQriocityの不正アクセスでユーザ情報が漏えい（最大約7,700万件）
- 行政指導（日本）、議会公聴会で幹部の証言（米国）
- 全ユーザーに対して、コンテンツやサービスの無料提供

情報漏えい事故（世界）

2016年12月時点



2017年9月時点



【Equifax】2017年9月7日発表
- 米国の個人信用情報機関
- 約1億4300万人の個人情報
  （氏名、社会保障番号、生年月日、住所、免許証番号）
- 20万9000人のクレジットカード番号

出典: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

不正アクセスの状況

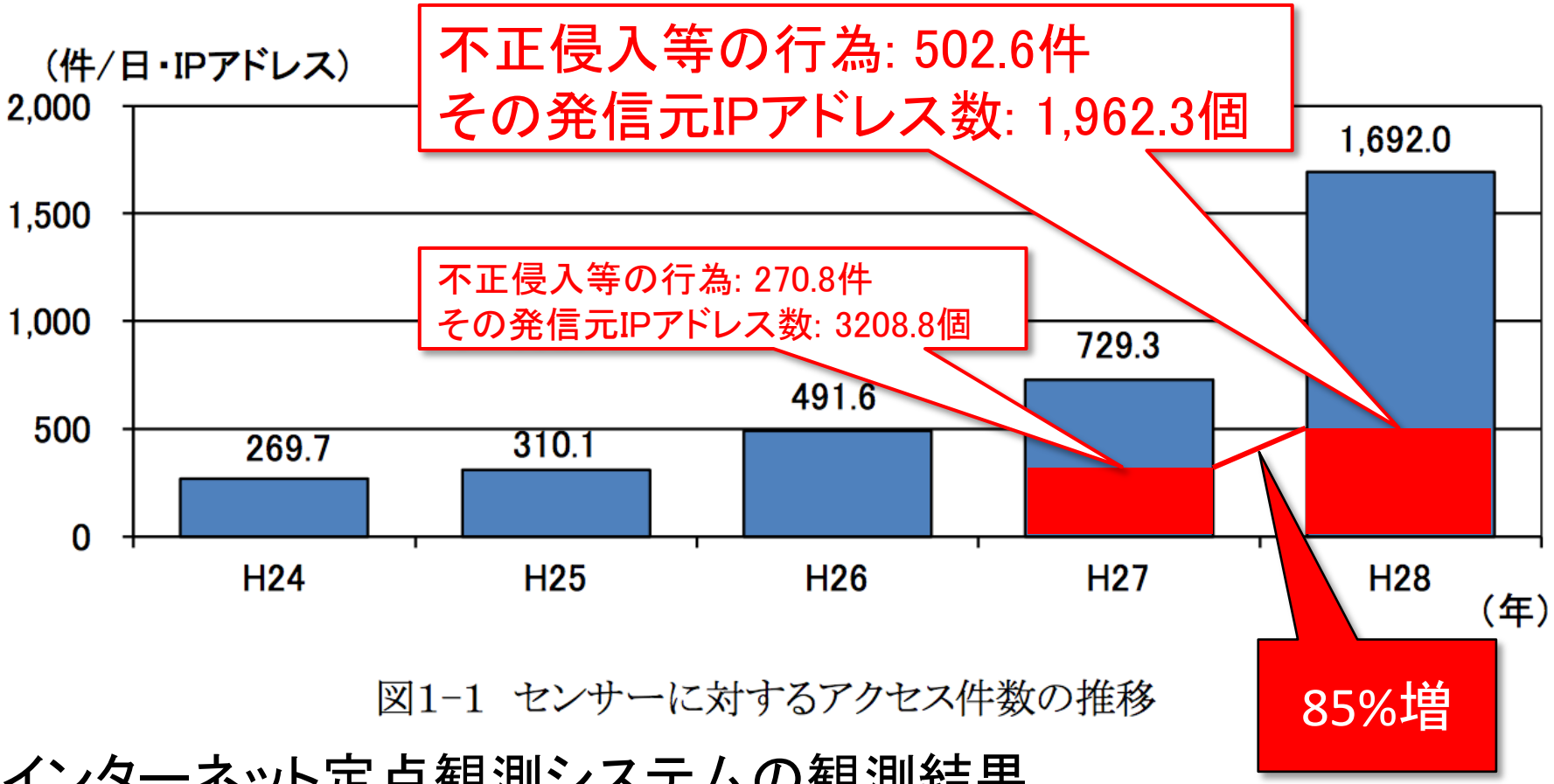
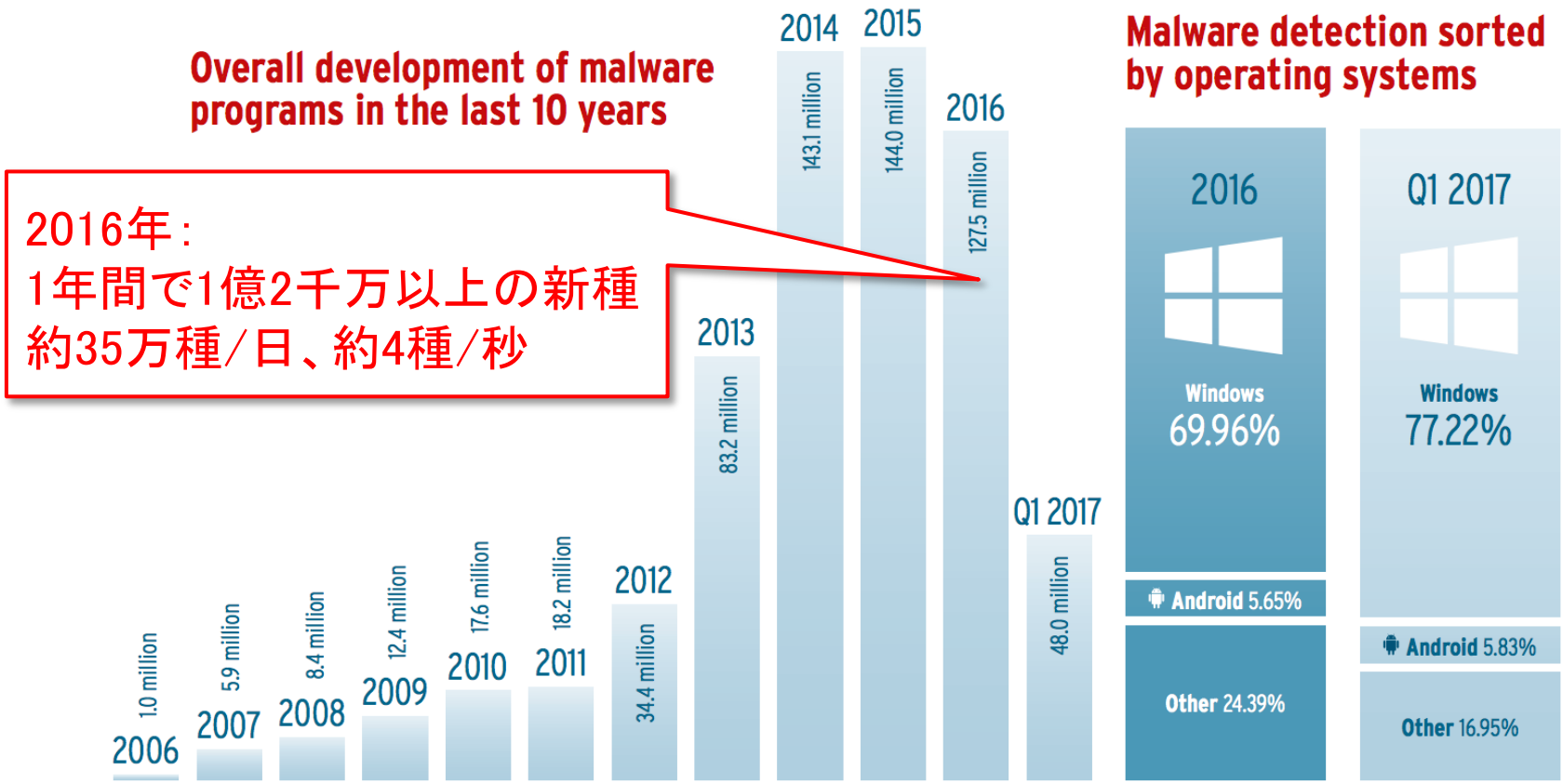


図1-1　センサーに対するアクセス件数の推移

インターネット定点観測システムの観測結果

出典: 警察庁 平成28年観測資料
https://www.npa.go.jp/cyberpolice/detect/pdf/20170323_toukei.pdf

マルウェアの状況



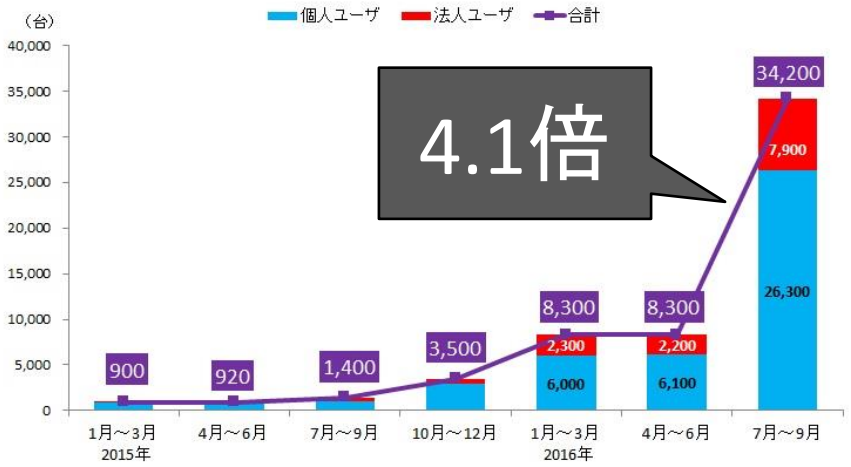
マルウェアの新種検知数

出典: Security Report 2016/17, AV-TEST GmbH

https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf

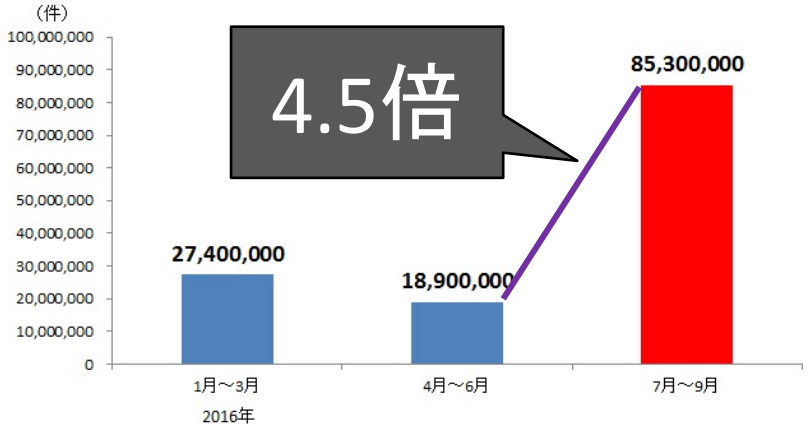
ランサムウェアの状況

ランサムウェア国内検出台数推移（日本）



2015年1月～2016年9月トレンドマイクロによる調査

ランサムウェア感染を狙った不正メールの検出数（全世界）



2016年1月～9月トレンドマイクロによる調査

※出典: http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20161115050616.html

事例: 2017年5月、WannaCryと呼ばれるランサムウェアを使った過去最大規模の一斉攻撃が発生。
--- 画像:ドイツの鉄道駅の案内板（ドイツ・ケムニッツ、5月12日）=AP

ランサムウェア: 成立要件

☆

1. マルウェア
   - ファイルの暗号化: WannaCry
   - スマホの写真、メール、通話履歴などを暴露: LeakerLocker/Android
2. 匿名通貨 ⇐ ビットコイン
   - 匿名かつオンラインで金銭をやりとりするしくみ
     - 一般ユーザにはハードルが高いので、プリカが代用される
3. 匿名通信 ⇐ Tor (The Onion Router)
   - 通信経路/IPアドレスを匿名化するしくみ

これらの組み合わせにより、
匿名で金銭の請求が可能になった！

Dyn DDoS攻撃

日時
- ◆2016年10月21日
- ◆7:10 – 9:20 a.m. EDT
- ◆11:50 a.m. – 1:11 p.m. EDT
- ◆4:00 – 6:11 p.m. EDT

場所
- ◆北アメリカ
- ◆欧州

容疑者
- ◆Anonymous
- ◆New World Hackers

出典: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

標的
- ◆Dyn社（DNSプロバイダ）

方法
- ◆DNS amp DDoS
  最大1.2 Tbps

ボットネット
- ◆マルウェアMiraiに感染した
  IoTデバイス（監視カメラや
  ビデオレコーダー）

影響を受けたサービス

DDoS攻撃の不都合な真実

発信元の特定が困難

- UDP通信、リフレクターの利用

攻撃を停止させるのが困難

- 発信元（ボット）の数が膨大

サービスとしてのDDoS

- DDoS攻撃を闇市場で購入できる

脅迫の道具としてのDDoS

- DDoSの脅威を使って脅迫する

現実世界への影響

自動車

◆安全装備の無効化、自動運転ののっとり
⇒ 大規模なリコール

社会インフラ

◆発電・送電システムへの攻撃
⇒ 停電、設備の破壊による2次被害

政治

◆情報漏えいや偽情報の流布による選挙結果への影響

経済

◆フィッシングメールや偽情報を使った株価操作

事例: ロシアが米大統領選に干渉か

☆

ワシントンポスト 2016-12-11

- 米国中央情報局（CIA）は11日までに、ロシアがサイバー攻撃を通して米大統領選に干渉したと断定
- 大統領選前に民主党全国委員会やクリントン陣営の電子メール数千通を盗み出し、告発サイト「ウィキリークス」に流した複数の人物は、ロシア政府とつながりを持っていた

ホワイトハウス 2016-12-29

- Obama大統領は、ロシアがハッキングを行い、2016年の米大統領選に干渉したと連邦捜査官が判断したことを受け、ロシアへの制裁を発表
  - https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

※ 日本経済新聞 2017-11-17: 英国のEU離脱、スペインのカタルーニャ問題などにも関与か

事例: ウクライナの停電 2年連続

2015年12月23日

- 変電所への攻撃
- 数時間の停電
- 約22万人に影響
- マルウェア BlackEnergy Trojan
- ロシア政府による攻撃か？
  - http://wired.jp/2016/01/07/cyberattack-power-electricity/

2016年12月17日

- 変電所への攻撃
- 30分程度の停電
  - http://wired.jp/2017/01/14/hacking-ukraine-power/

ソーシャルエンジニアリング

- ソーシャルエンジニアリングとは？
- 不正アクセス vs. 詐欺
- なぜソーシャルエンジニアリングか？
- 事例: ID/パスワード、アフィリエイト、ストーカー、プリカ
- 事例: フィッシング
- 事例: ビジネスメール詐欺

ソーシャルエンジニアリングとは？

情報セキュリティに対す攻撃の一種

– 人間の心理的な隙を突き、攻撃者の意図した行為を取るように標的（人）を誘導する行為

狭義では

– 不正アクセスのために、人を騙してIDやパスワードを獲得する行為

⇒ なりすまし

– または、人の行動から目的の情報を探り出す行為

不正アクセス vs. 特殊詐欺

約16.9億円（前年30.7）

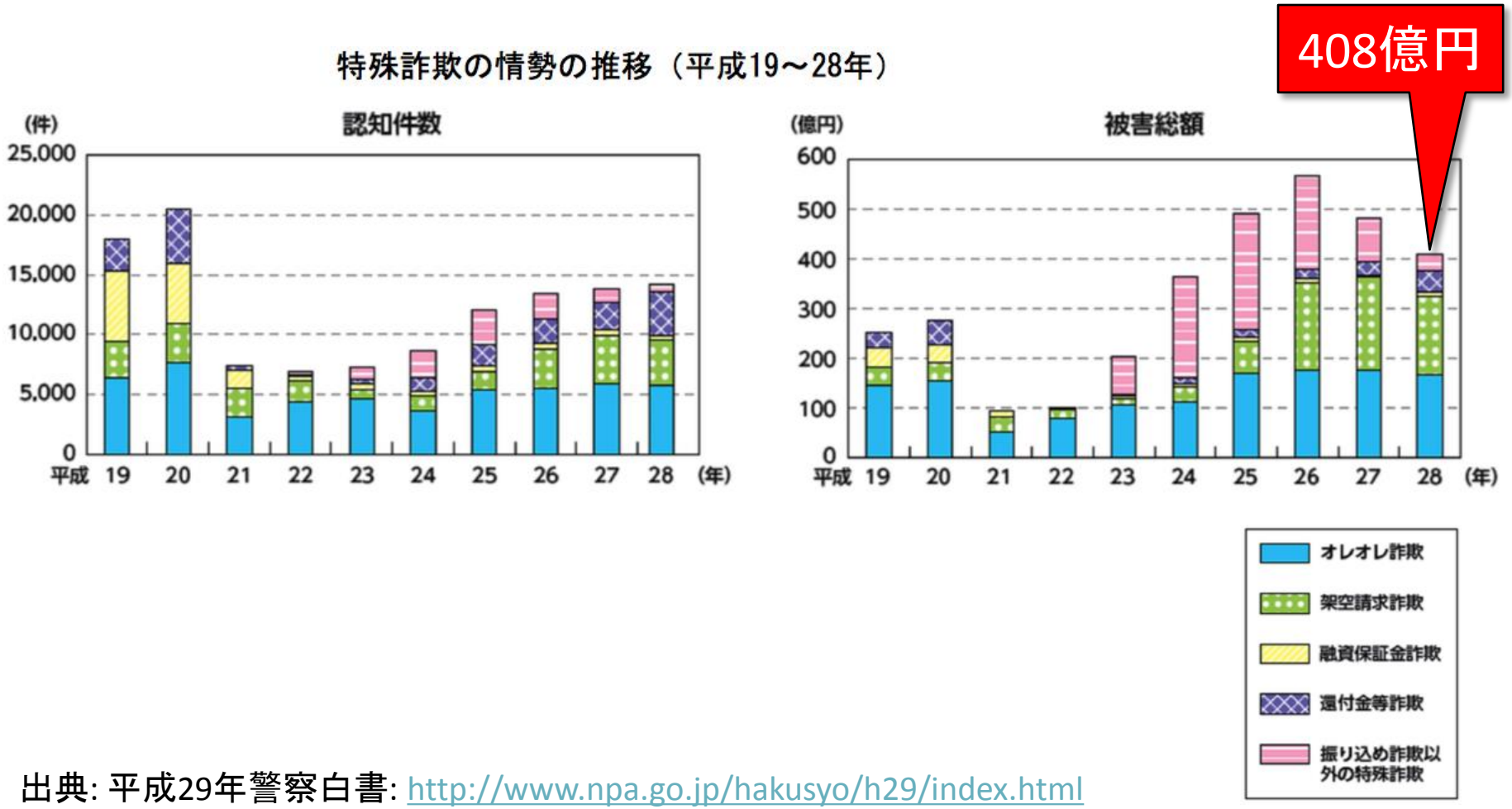
- インターネットバンキングの不正送金被害額
- 2016年/H28
- 警察庁「平成28年中におけるサイバー空間をめぐる脅威の情勢について」
  - https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf
    （参照: 2017-08-25）
- 件数、被害額ともに減少※

約408億円（前年482）

- 特殊詐欺の被害額
- 2016年/H28
- 警察庁「平成28年の特殊詐欺認知・検挙状況等について」
  - https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2016.pdf
    （参照: 2017-08-25）
- 件数微増、被害額減少

※ 被害者の多くはセキュリティ対策（ワンタイムパスワード、電子証明書など）を未実施

特殊詐欺の情勢



出典: 平成29年警察白書: http://www.npa.go.jp/hakusyo/h29/index.html

なぜソーシャルエンジニアリングか？

ITの脆弱性を突くよりも人を騙す方が容易

- 騙されることに対する免疫の不足

攻撃者の候補数が多い

- 攻撃の手段・経路が多様
  - 例: 電話（高度なハッキングスキル/ツールは不要）
  - 例: キーボード入力や付箋の盗み見、ゴミ漁り
- 動機が多様
  - 例: ストーカー、復讐、金銭

成功事例

- 振り込め詐欺、ビジネスメール詐欺
- LINEのなりすましによる電子通貨の購入詐欺

ソーシャルエンジニアリングの分類

【人間指向】

- ◆なりすまし
  - システム管理者
  - 作業員、宅配業者
- ◆物理的（建物）侵入
- ◆盗聴、盗撮
- ◆張り込み、尾行
- ◆聞き込み
- ◆ゴミ漁り（トラッシング）
- ◆盗み見
  （ショルダーサーフィン）

【IT指向】

- ◆Webの情報収集
  - 検索エンジン
  - SNS
  - マップ、ストリートビュー
- ◆フィッシング
- ◆標的型攻撃
- ◆ファーミング／pharming※
  - DNSリバインディング
  - hosts書き換え

※ pharming: コンピュータのアドレス情報を不正に変更し、偽サイトに接続させる攻撃

例: ID・パスワードの入手

システム管理者になりすまし、システムサポートの連絡先変更を偽装メールで通知

【パターン1】標的がトラブル時に連絡してきたら、サポート作業で必要と称してID・パスワードを聞き出す

【パターン2】攻撃者が標的の利用するPCにトラブルを起こし、1を誘発

【パターン3】アカウントが乗っ取られた旨を通知し、指定したパスワードに一時的に変更するよう指示

例: SNSの偽プロフィールで誘導

1. 攻撃者は魅力的な写真などを用意して、偽のSNSプロフィールを作成
   - Instagram, Facebook, LinkedIn, etc.
2. 他人に「いいね」やフォロー
3. 「いいね」やフォローされた側がプロフィールに誘導され、アフィリエイトリンクを手繰る
4. 攻撃者にアフィリエイト※の報酬が入る

※ 成功報酬型広告

例: ストーカー

1. SNSの書き込みから、行動範囲や移動時刻、衣服や持ち物の情報を収集
   - ◆ ○○で△を食べた/買った
   - ◆ ○○駅で電車遅れ
   - ◆ 写真のExif情報（日時、GPSデータ）
2. Googleマップで住所や職場、利用駅を推定、ストリートビューで周辺環境を下見
3. 標的を見つけて尾行

例: プリペイドカード詐欺

プリペイドカードを購入させ、その番号を知らせるように誘導

- 公共料金等の支払いを電話で要求
- 友達から困っているとSNSでメッセージ
- オンラインゲームのアカウント売買

iTunes Card 詐欺

iTunes Card を悪用した詐欺にご注意ください。

税金、医療費、保釈金、借金、光熱費などを払うよう電話で要求する詐欺が横行しています。手口はさまざまで、ギフトカードを悪用するものもあります。iTunes Card も悪用されることがあり、Apple ではこうした詐欺についてお客様に注意を呼びかけております。

支払いの内容や理由にかかわらず、こうした詐欺の手口には一定のパターンがあります。まず、今すぐ支払わなければならないものがあるという差し迫った内容の電話がかかってきます。それを聞いて気持ちが動揺したところで、近くのお店 (コンビニエンスストアや家電量販店など) で iTunes Card を購入し、それで支払うよう言われます。iTunes Card カードを購入したら、カードの裏面の 16 桁のコードを電話越しに教えるように指示されます。

iTunes Card は、iTunes Store、App Store、iBooks Store での商品／サービスの購入や、Apple Music メンバーシップ料金の支払いにしか使えないということを知っておいてください。iTunes Store、App Store、iBooks Store、Apple Music 以外の支払いに iTunes Card を使うように要求された場合は詐欺の可能性が高いため、すぐに警察に通報してください。

https://support.apple.com/ja-jp/itunes-gift-card-scams

http://www.s-kessai.jp/info/data/150514prepaid_sagi_postar.pdf

フィッシング

フィッシングとは？

- ソーシャルエンジニアリングの技法の一つで、詐欺行為
- 本物そっくりのWebサイトに誘導し、重要情報を入力させてそれらを奪取する

例

- 偽のメール等で設定変更を促す
  ⇒ 偽のURLリンクで偽サイトに誘導
  - セキュリティ質問を再設定してください（Apple）
  - あなたのアカウントのパスワードは簡単すぎます（LINE）

フィッシング：例

Google Play をかたるフィッシング 2017-03-15

クレジットカード情報、
個人情報の入力

出典: フィッシング対策協議会 https://www.antiphishing.jp/news/alert/googleplay_20170315.html

フィッシング：コントロール（防御策）

ドメイン名を確認する

- 例: あなたのネット「常識力」はどのくらい？ 質問5

重要情報はHTTPSで入力する

- 証明書に基づくサーバの認証
- （通信路の暗号化）

検索結果からアクセスしたページに重要情報を入力しない

- 正しいURLを使う（手入力やブックマーク）

個人に関する
具体的な事件と自衛策

- ◆ SNS ⇐ 炎上、リベンジポルノ、誹謗中傷
- ◆ 有料サイト ⇐ 不当（架空）請求
- ◆ オンラインゲーム ⇐ クレジットカード盗用、アカウントのっとり
- ◆ プログラミング ⇐ ウイルス作成・供用・取得

ふざけた写真をネットに流した（1/2）

コンビニのバイトで
アイスクリーム用冷蔵庫に
自分が入った写真を撮り
うけると思ってSNSに投稿した。

ふざけた写真をネットに流した(2/2)

【原因と結果】

- (炎上)コンビニのバイトで、アイスクリーム用冷蔵庫に入った写真をうけると思ってSNSに投稿した。
  - ⇒ バイトはクビ、損害賠償を請求され、学校は停学
  - ⇒ 自宅や学校を特定
  - ⇒ 将来の進学・就職にも影響

【注意点と自衛策】

- 一度ネットに流れた情報は、完全に消し去るのが困難
  - ⇐ 検索エンジンなどの事業者には法的な削除依頼をできるが、労力と費用がかかる
  - ⇐ 海外サーバではさらに難しい

見られたくない写真がネットに流れた

【原因と結果】

- （リベンジポルノ）彼氏/彼女と別れた後、嫌がらせで以前に撮った裸の写真を公開された。
  ⇒ 写真があちこちにコピーされ、恥ずかしくて不登校や退職
- （不正アクセス）クラウドに保存していたプライベートな写真がいつのまにか流出していた。パスワードは簡単で忘れにくいものにしていた。
  ⇒ 炎上、機密の暴露

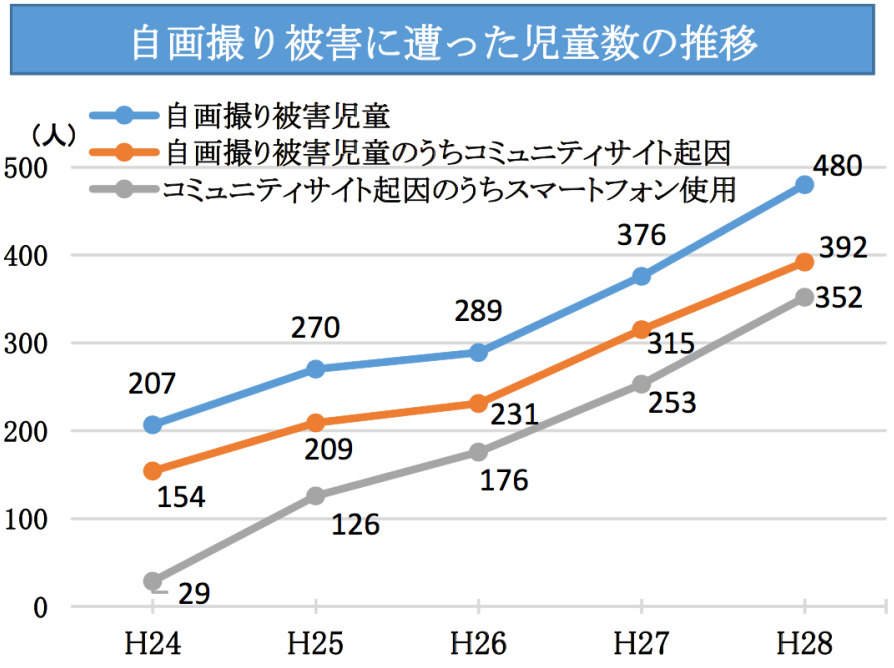
【注意点と自衛策】

- 一度ネットに流れた情報は、完全に消し去るのが困難
  ⇐ 検索エンジンなどの事業者には法的な削除依頼をできるが、労力と費用がかかる
  ⇐ 海外サーバではさらに難しい
- 流出したら困る写真を撮らない、撮らせない、送らない
  ⇐ 信頼できる相手であっても
- 個人情報の発信は必要最小限にする

自画撮りの被害、4年で倍増

警察庁まとめ, 日本経済新聞 2017.05.19夕刊

中高生、9割占める



出典: 警察庁
https://www.npa.go.jp/safetylife/syonen/no_cp/newsrelease/selfy.pdf

※ 自画撮り被害とは、だまされたり脅されたりして自分の裸を撮影させられ、メール等でその画像を送らされる被害

- 2016年摘発数の児童ポルノ事件の被害者数は 1,313人
- 自画撮りの被害者は480人（全体の36.6%）
  - 盗撮などよりも多い

※ 福島県内7人

- 被害者の441人（91.9%）が中高生
- 8割がSNSなどで相手と知り合った
- 面識のない相手への送信が8割、それ以外は友人・知人

※ 2017年上半期: 1,142件を摘発、18歳未満被害者594人（「自画撮り」の被害は約4割の263人、中高生が約9割）

自画撮り被害への対策（立法・行政）

- 性的な対象として子供（18歳未満）を撮影した画像・動画を送信させた行為
  - 児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律（略称: 児童買春・児童ポルノ処罰法）

- わいせつな画像の送信を要求する行為
  - 自治体の条例等で罰則（検討中）

SNSなどで誹謗中傷を受けている

【原因と結果】

- （いじめ）気に入らない同級生や同僚がいるので、悪口やあることないこと、匿名の掲示板でみんなに言いふらした。
  - ⇒ 逮捕
  - ⇒ 退学や停学、懲戒免職
  - ⇒ 相手は不登校や退職

【注意点と自衛策】

- 内容によっては犯罪
  - ⇐ 名誉棄損罪（刑法）
  - ⇐ 侮辱罪（刑法）
- トラブル相談・届
  - ⇐ サービス運営者（削除依頼）
  - ⇐ 法的機関（人権擁護）
  - ⇐ 警察（被害届）

画面に執拗に
料金請求のメッセージが出る（1/2）

興味ある広告を何の気なしにクリックしたら、

「ご入会ありがとうございます！
料金を振り込んでください。」

というメッセージが表示された。

「あなたの身元はわかっている」、
「警察に通報する」や「法的に訴える」
などの文面も。

画面に執拗に
料金請求のメッセージが出る(2/2)

【原因と結果】

- (架空請求、ワンクリック詐欺)興味ある広告を何の気なしにクリックしたら、「ご入会ありがとうございます。料金を振り込んでください。」というメッセージが表示された。「あなたの身元はわかっている」、「警察に通報する」や「法的に訴える」などの文面も。
  - ⇒ ウィンドウを閉じても、再起動しても、すぐに請求メッセージが出る
  - ⇒ だれかにばれるのがいやで、現金振込、プリカを購入して番号通知
  - ⇒ 電話で問い合わせて、確認のため名前や住所などを知らせたら、近所に迷惑電話、自分に脅迫電話

【注意点と自衛策】

- とにかく無視
  - ⇐ 電話やメールで問い合わせない
  - ⇐ お金を払わない
  - ⇐ 指示されたソフトをインストールしない
- 相談
  - ⇐ 警察の生活安全課
  - ⇐ 消費者生活センター
- アプリ・機器の初期化
  - ⇐ ブラウザの履歴・キャッシュの削除
  - ⇐ OSの再インストール/リカバリ

オンラインゲームのアイテム購入に親のクレジットカードを使ってしまった（こっそり）

【原因と結果】

- （覚えのないカード請求）どうしてもほしいアイテムがあったので、親の財布からこっそりクレジットカードを抜き取り、その番号を使って購入した。年齢チェックは20歳以上とうそをついた。
  - ⇒ 翌月のカード請求書でばれる
  - ⇒ ゲーム（端末）の没収
  - ⇒ 親はカードの管理責任を問われ、返金されない可能性

【注意点と自衛策】

- トラブル相談
  - ⇐ ゲーム運営会社
  - ⇐ カード会社
  - ⇐ 消費者生活センター
- ゲーム（端末）の使い方の取り決め
  - ⇐ 家族でルールを決める
- ペアレンタルコントロール
  - ⇐ 未成年者の機能・閲覧制限

オンラインゲームに関する他の事例

- 高価なアイテムの盗難や詐欺
  - アカウントのっとり
  - 先渡し後、音信不通
- リアル・マネー・トレーディング※
  - 規約違反、アカウント抹消
- ログイン不能
  - アカウントのっとり
    + パスワード変更

- パスワードは推測されにくいものを設定し、使いまわさない
- アカウント情報は秘密
- 運営者への通報

※ オンラインゲーム上の通貨やアイテムを、現実の金銭や電子マネーで売買すること

腕試しにコンピュータウイルスを作ってみた

【原因と結果】

- （ウイルス作成）プログラミングの能力を自慢したい。みんなの注目をあびたいので、コンピュータウイルスを作って、ネットで公開した。

  ⇒ 逮捕

【注意点と自衛策】

- ウイルス作成は犯罪

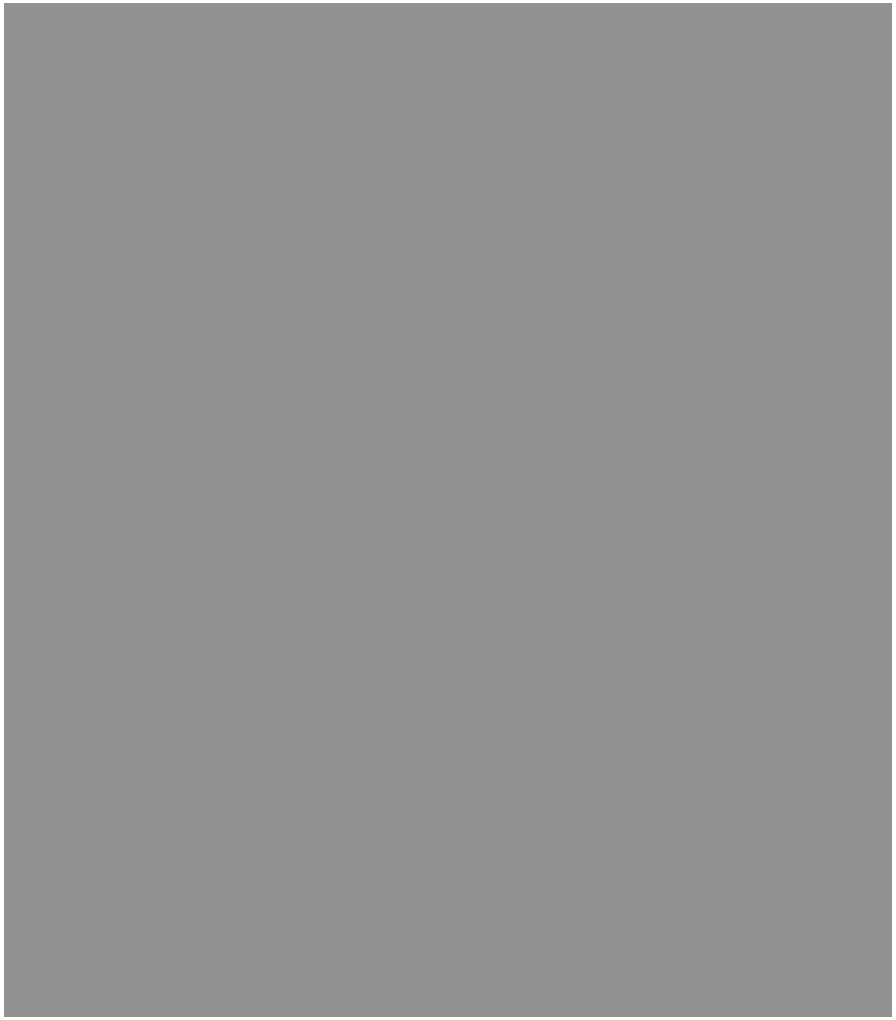
  ⇐ 不正指令電磁的記録に関する罪（コンピュータウイルスの作成、提供、取得、保管、いわゆる「ウイルス作成罪」）

  - 作成・提供: 3年以下の懲役または50万円以下の罰金
  - 取得・保管: 2年以下の懲役または30万円以下の罰金

ウイルス供用 容疑の高1逮捕
パソコン遠隔操作,日本経済新聞 2016-11-02 夕刊

- 高校1年生（16歳）逮捕
  - 不正指令電磁的記録供用（提供）
- 他人にウイルスをダウンロードさせた

「3日でウイルス作成」逮捕の中3
無料ソフト使用,日本経済新聞 2017-06-06



- 中学3年生（14歳）逮捕
  - 不正指令電磁的記録作成
- 独学でランサムウェアを作成
- 海外サイトで公開、SNSに投稿
- ダウンロードした人は不正指令電磁的記録取得の疑い

組織における情報資産と被害のダメージ

★

個人に関する具体的な事件と自衛策を、組織に置き換えて考えてみる

情報資産の例

- マイナンバー、住所録、給与明細
- 顧客や取引先の連絡先
- 製品の設計図などの開発情報
- 取引先から「取扱注意」として預かった情報

ダメージの例

- 被害者への損害賠償
- 取引停止、顧客離れ
- 業務の遅延・停止
- 従業員の士気低下

IPA「中小企業の情報セキュリティ対策ガイドライン（情報セキュリティ5か条）」資料を引用・再構成

なぜ被害がなくならないのか？（セキュリティ管理の難しさ）

- 防御側の不利、攻撃側の有利
- 環境の変化
- 人の特性

防御側の不利、攻撃側の有利

	防御側	攻撃側
経路	可能性のすべて	どこか1点
知識	既知の攻撃	ゼロデイ
タイミング	常に（24h/7d）	好きな時に
性質	ルールに従う	ずるい、汚い

参考: *Writing Secure Code, 2nd ed.,* by Michael Howard and David LeBlanc, Microsoft Press, ISBN-13: 978-0735617223, 2002.

対策をむずかしくする環境の変化

【ITシステム】

◆オンプレミス ⟶ Web ⟶ クラウド ⟶ IoT

【サイバー攻撃】

◆目的: 自己顕示 ⟶ 思想・信条 ⟶ 金銭

◆マルウェア: 単体 ⟶ Web・MITB ⟶ ボットネット

◆属性: 機密性・完全性 ⟶ 可用性

- 【例】DDoS、ランサムウェア

◆ターゲット: IT（サイバー空間） ⟶ 人・もの（実世界）

- 【例】不正送金、ビジネスメール詐欺、自動車の制御

根本的な対策が難しい攻撃

正規サイトの改ざん

- ◆例: Gumblar

表面上に変化を見せないマルウェア

- ◆例: 不正送金マルウェア（MITB）

標的型攻撃、フィッシング

- ◆例: 巧妙なメールと添付ファイル

可用性を侵害するDoS攻撃

- ◆例: Dyn DDoS攻撃

人の特性による被害の拡大

即応性

⇐ 若者

- すぐに応答・返事をしてしまう
  - スマフォを常に使用することが日常化している
- すぐに応答・返事をしないと、嫌われる
  - ネットでのつながりと、リアルのつながりが同等の価値をもつ

まじめ、すなお

⇐ 若者・高齢者

- 相手が間違っていると思って、連絡してしまう
- 自分が間違っていると思って、相手に従ってしまう

面倒くさがり

⇐ だれでも

- 楽な方に流れる

推測しやすいパスワード

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

約17%

6文字以下

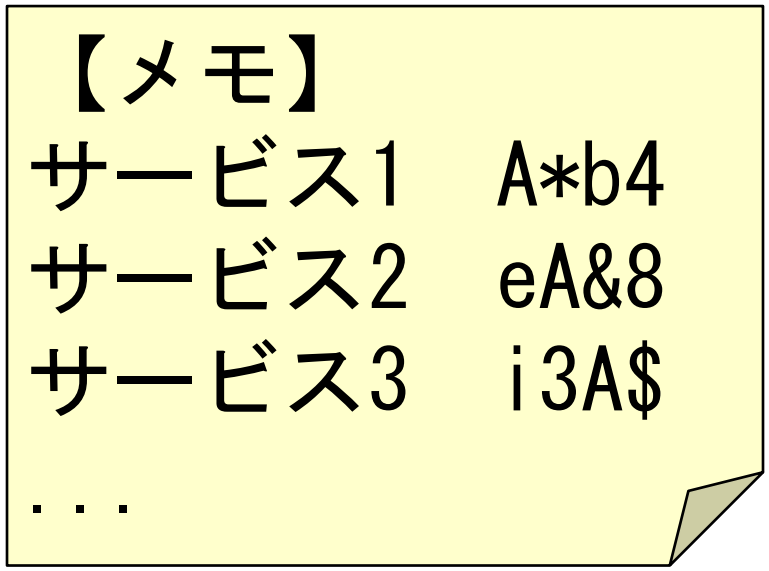
11.	qwertyuiop
12.	mynoob
13.	123321
14.	666666
15.	18atcskd2w
16.	7777777
17.	1q2w3e4r
18.	654321
19.	555555
20.	3rjs1la7qe
21.	google
22.	1q2w3e4r5t
23.	123qwe
24.	zxcvbnm
25.	1q2w3e

- Keeper Security社調査
- 2016年度に漏えいした約1000万件のデータを調査
  - https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

面倒くさい！
覚えられない！

パスワードをメモしない！

でも、どうしてもメモしないと覚えられないときは



＋

【少し記憶】
Xy9?

【さらに置換】A ⇒ 1

他にパスワード管理ツールを使う方法もある。

何から始めればいいのか？

★

- 情報セキュリティ5か条, IPA
- 情報セキュリティ対策9カ条, 内閣サイバーセキュリティセンター（NISC）
- セキュリティ（リスク）マネジメント（午後の講義）

情報セキュリティ5か条, IPA

★

情報セキュリティ 5 か条

1 OSやソフトウェアは常に最新の状態にしよう!

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

対策例
- Windows Update(Windows OSの場合)/ソフトウェア・アップデート(Mac OSの場合)
  OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/Java実行環境(JRE)など利用中のソフトウェアを最新版にする

2 ウイルス対策ソフトを導入しよう!

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

対策例
- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する

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窃取したID・パスワードが流用されることで、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!

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため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。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

対策例
- クラウド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: IPA「中小企業の情報セキュリティ対策ガイドライン(情報セキュリティ5か条)」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

インターネットを安全に利用するための
情報セキュリティ対策9カ条, NISC

出典: 内閣サイバーセキュリティセンター(NISC)
http://www.nisc.go.jp/security-site/trouble/material.html#security9

まとめ

- 後を絶たないサイバー犯罪・事件
  - 中高生や高齢者が狙われている、被害にあっている
  - 奪取できる金額が大きな法人も狙われている
  - 個人情報漏えいのインパクトは大きい
- ICTも万全ではない上に、人間が大きな弱点
  - だまされることに対する免疫不足
  - まじめ・すなおな対応、怠慢
- 被害者にならない！
  - 知識、自衛
- 加害者にならない！
  - 知識、モラル、マナー、法律

困ったときの相談先

警察（福島県警察）

- 警察安全相談室
  #9110
  024-525-3311
  - 月曜～金曜 9:00-17:00
- 最寄りの警察署

福島県消費生活センター

- 相談専用電話
  024-521-0999
  - 月曜～金曜 9:00-18:30
    第４日曜 9:00-16:30
- 消費者ホットライン
  188

参考資料

★

- 福島県警察 サイバー犯罪対策コーナー
  - http://www.police.pref.fukushima.jp/onegai/jyouhou/hightech2/cyber_top.html
- 内閣サイバーセキュリティセンター
  教材「みんなでしっかりサイバーセキュリティ」
  - http://www.nisc.go.jp/security-site/trouble/material.html
- 中小企業の情報セキュリティ対策ガイドライン, IPA
  - https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
- 中小企業向けサイバーセキュリティの極意, 東京都産業労働局
  - http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/jigyou/guidebook/
- ビデオ教材（大人にも役立ちます）
  - 写真や動画が流出する怖さを知ろう, ネット被害（中2～高3）全編, IPA
    - https://www.youtube.com/watch?v=kAxjbkXovvs
  - 大切な情報を守るために, 情報セキュリティ（中2～高3）全編, IPA
    - https://www.youtube.com/watch?v=Zy3OzML8U4o