サイバーセキュリティの動向とリスクマネジメントの考え方

サイバー犯罪被害から県民を守るためのリーダー養成講座

2016年12月6日、7日

中村章人

会津大学

nakamura@u-aizu.ac.jp

社会的な課題

サイバーセキュリティ

▼

サイバー攻撃

機密情報の漏えい、金銭的被害、信用失墜 etc.

個人/組織、企業/行政、社会インフラ

▼

効果的なセキュリティ対策を実施できるしくみ

（タイムリー、効果的、効率的）

ポイント

継続的なセキュリティ管理が重要

▼

事前にできることを、計画的に

事故前提で、事後処理と復旧策

技術だけでなく、手続き的・物理的対策も

▼

最新情報を基に、継続性をもって取り組む

「人間」も重要な要素

内容

1. 時事評論
2. 情報セキュリティの基本概念
3. 不正アクセス
4. パスワード
5. ソーシャルエンジニアリング
6. セキュリティ管理
7. サイバーレジリエンス

時事評論

- IoTボットネットによる大規模なDDoS攻撃
- ビジネスメール詐欺
- コンビニATMからの現金不正引き出し
- 通信教育企業や公的機関から情報漏えい
- ランサムウェアで身代金要求

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）
- 行政からの調査指示、海外からの渡航者が減少？

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）

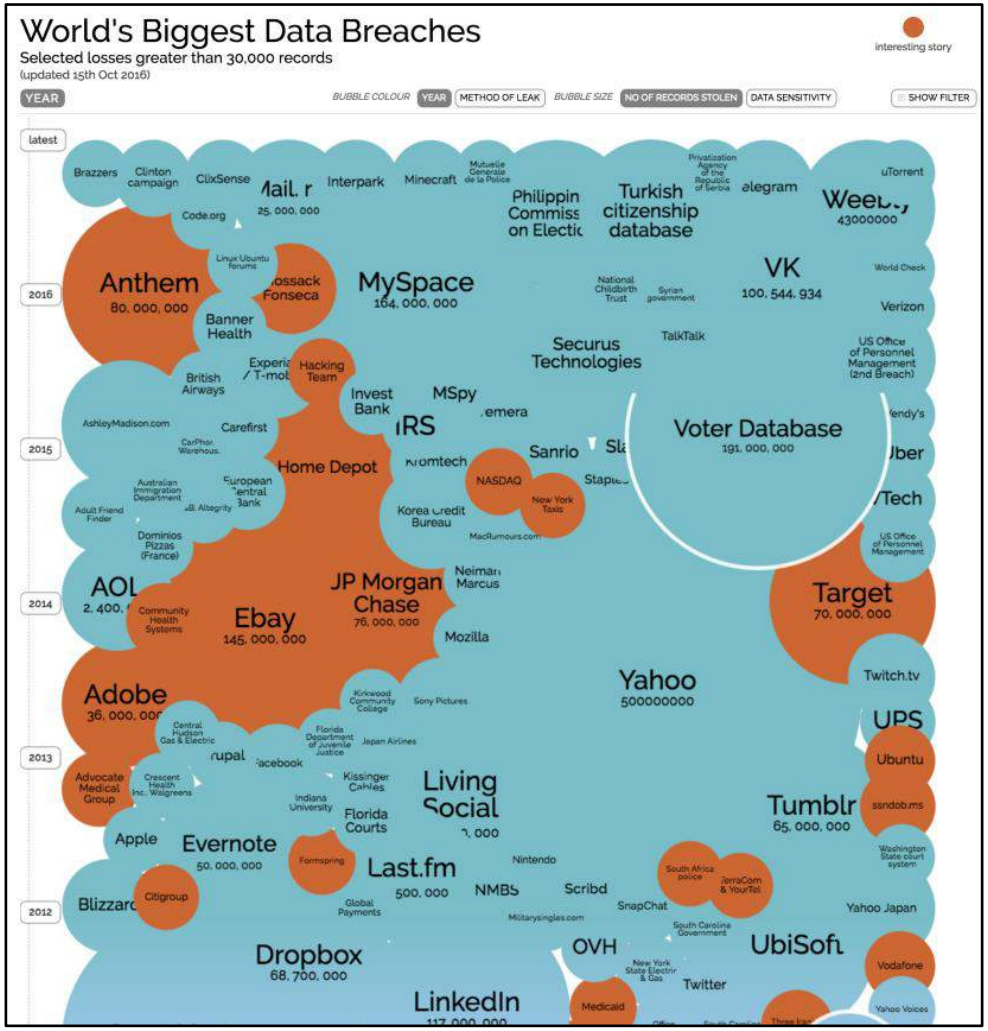
- 委託企業の社員が顧客情報を漏えい（約3,500万件）
- おわびの手紙と金券（500円）

ソニー・コンピュータエンタテインメント※（2011年4月）

※ 現ソニー・インタラクティブエンタテインメント

- 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）



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

マイナンバー制度

- 社会保障・税番号制度
  - マイナンバー = 12桁の個人番号
    - 平成27年10月から通知開始
  - 社会保障、税、災害対策に利用
- 取扱注意 ⇒ 罰則規定あり
  - 個人
    - 必要な相手（勤務先、行政機関等）以外に提供しない
  - 民間事業者（規模によらず）
    - 定められた目的でのみ収集し、適切に管理する
    - 業務委託先を監督する

※ 個人番号関係事務実施者

脆弱なIoT機器

- 市販の製品
  - デジタルビデオレコーダ、監視カメラ
- 医療機器
  - 病院内、個人携帯
- ビル管理システム

- デフォルト/簡単なパスワード
- 脆弱な通信プロトコル
- 単純なネットワーク構成
- 古いOSの利用

攻撃対象ではなく、攻撃の踏み台 ⇒ 加害者になるリスク

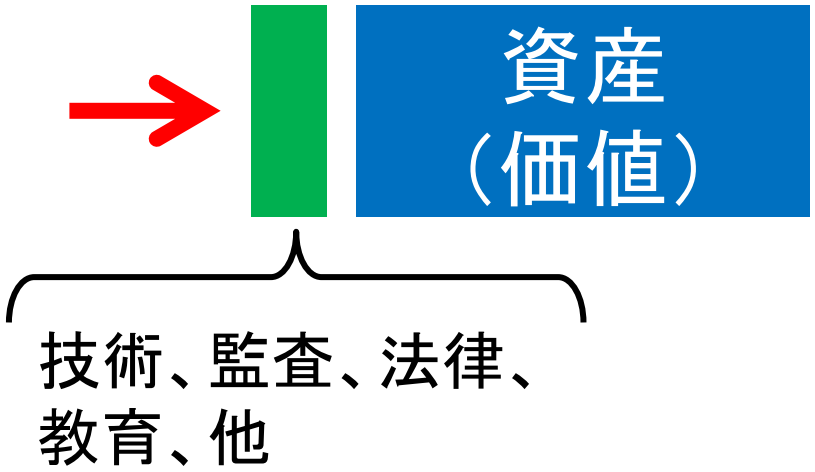
情報セキュリティの基本概念

- 価値ある情報資産のC-I-Aを保障する
- 技術的対策に加えて、物理的・手続き的な対策がある

リスクとセキュリティ

リスク

- 資産が損害を被る可能性がある状況



セキュリティ

- リスクがなく、事故や攻撃による被害を受けない*状態*、または
- 上記の状態を達成する*プロセス*

情報資産

- 種類
  - ハードウェア
  - ソフトウェア
  - ネットワーク
  - データ
  - サービス

- 価値の高い資産
  - 代替のないもの、再現しにくいもの
  - 機密性の高いもの
- 資産の価値は状況次第
  - 時間とともに変化
  - 所持する人に依存

脅威

［定義］資産に損害を与える原因となるもの.

- 例

人間由来		環境由来
悪意あり	悪意なし	
盗聴 情報改ざん システム侵入 マルウェア 盗難	誤り、手抜かり ファイル削除 物理的事故	地震 落雷 洪水 火災

攻撃

情報セキュリティの目的

- 価値ある情報資産を守る
  - 許可のない利用・改変から守る
  - 許可された利用を認めつつ

||

- 情報資産の C-I-A (Confidentiality, Integrity, and Availability) を保障する

情報セキュリティの基本3属性: C-I-A

機密性
Confidentiality
許可された人だけが
情報を閲覧できる

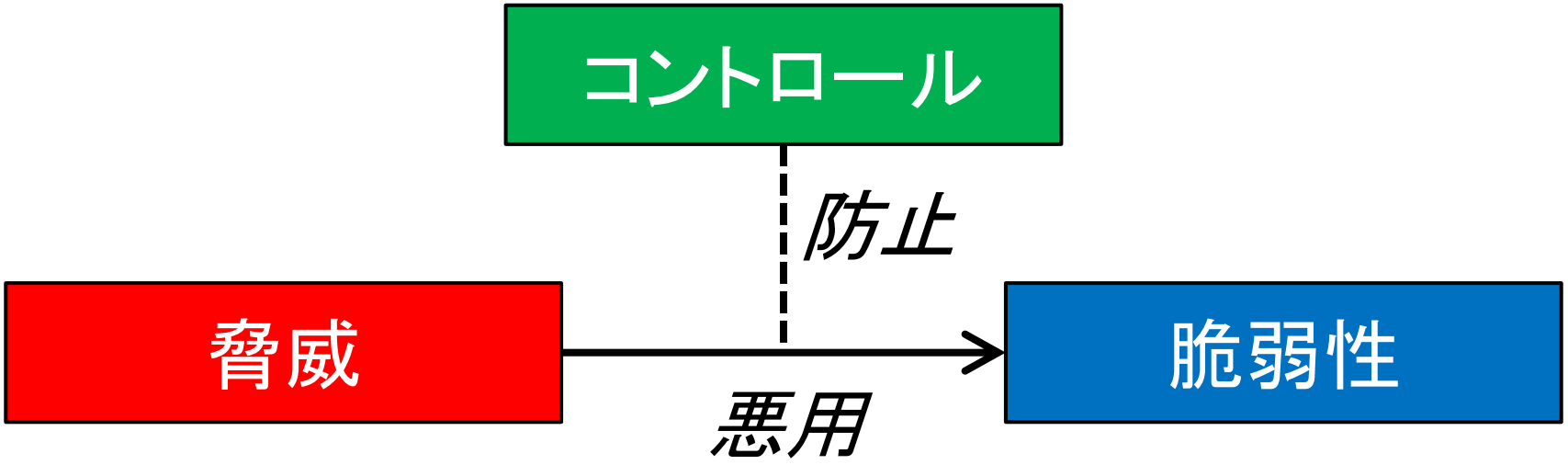
完全性
Integrity
情報が本来あるべき
正確な状態である

可用性
Availability
必要なときに
情報を使える

コントロール

リスクを変更する対策.

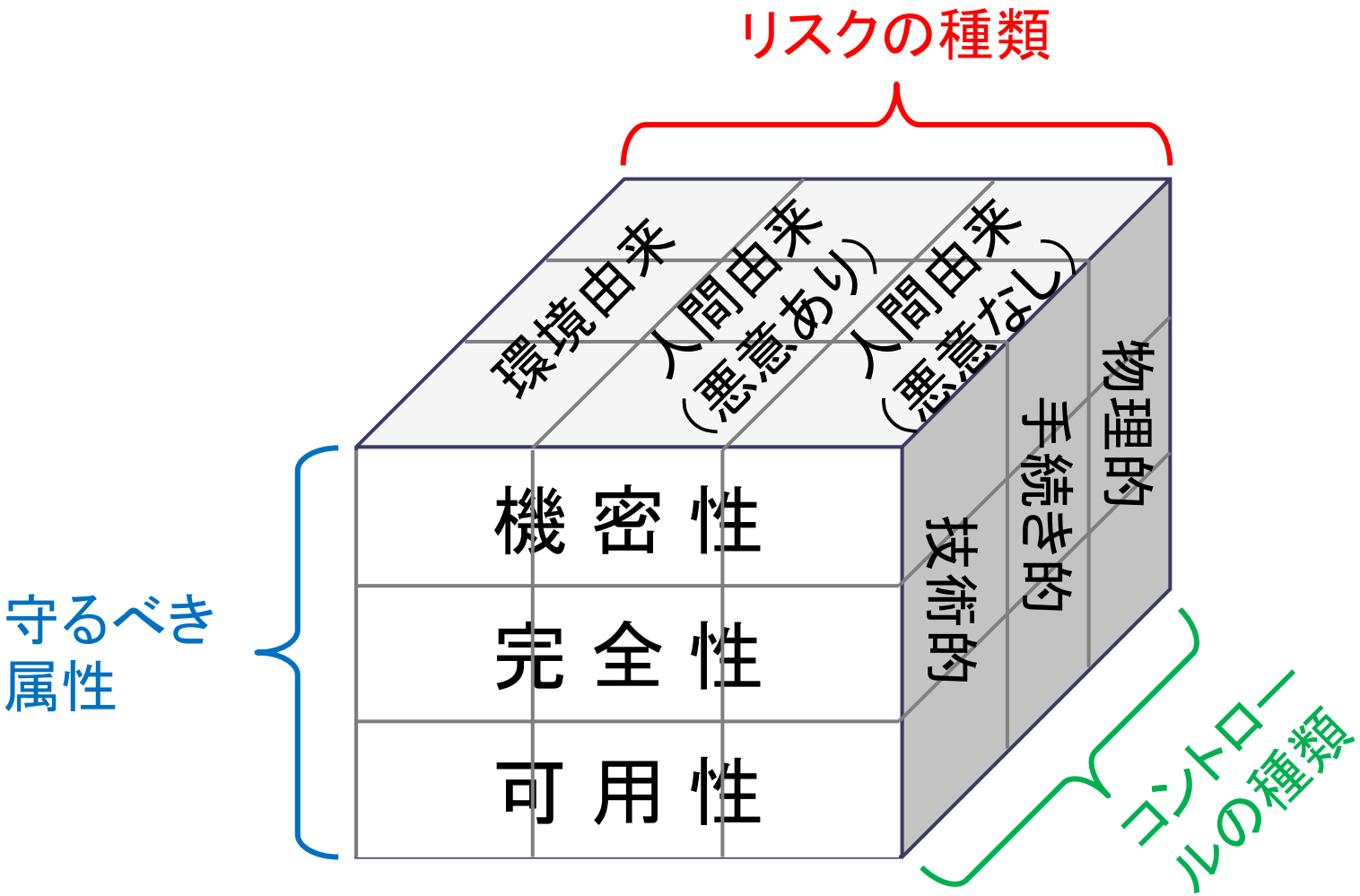
- 例: プロセス、ポリシー、仕掛け、訓練
- 対抗手段 (countermeasure) とも言う



コントロールの種類(1/2)

物理的	手続き的	技術的
有形のものを使った攻撃の阻止	命令や合意	技術で脅威に対抗
例: - 施錠 - ガードマン - 消火器	例: - 法律、規則 - 契約	例: - パスワード - アクセス制御 - 暗号 - ファイアウォール - IDS

コントロールの種類（2/2）

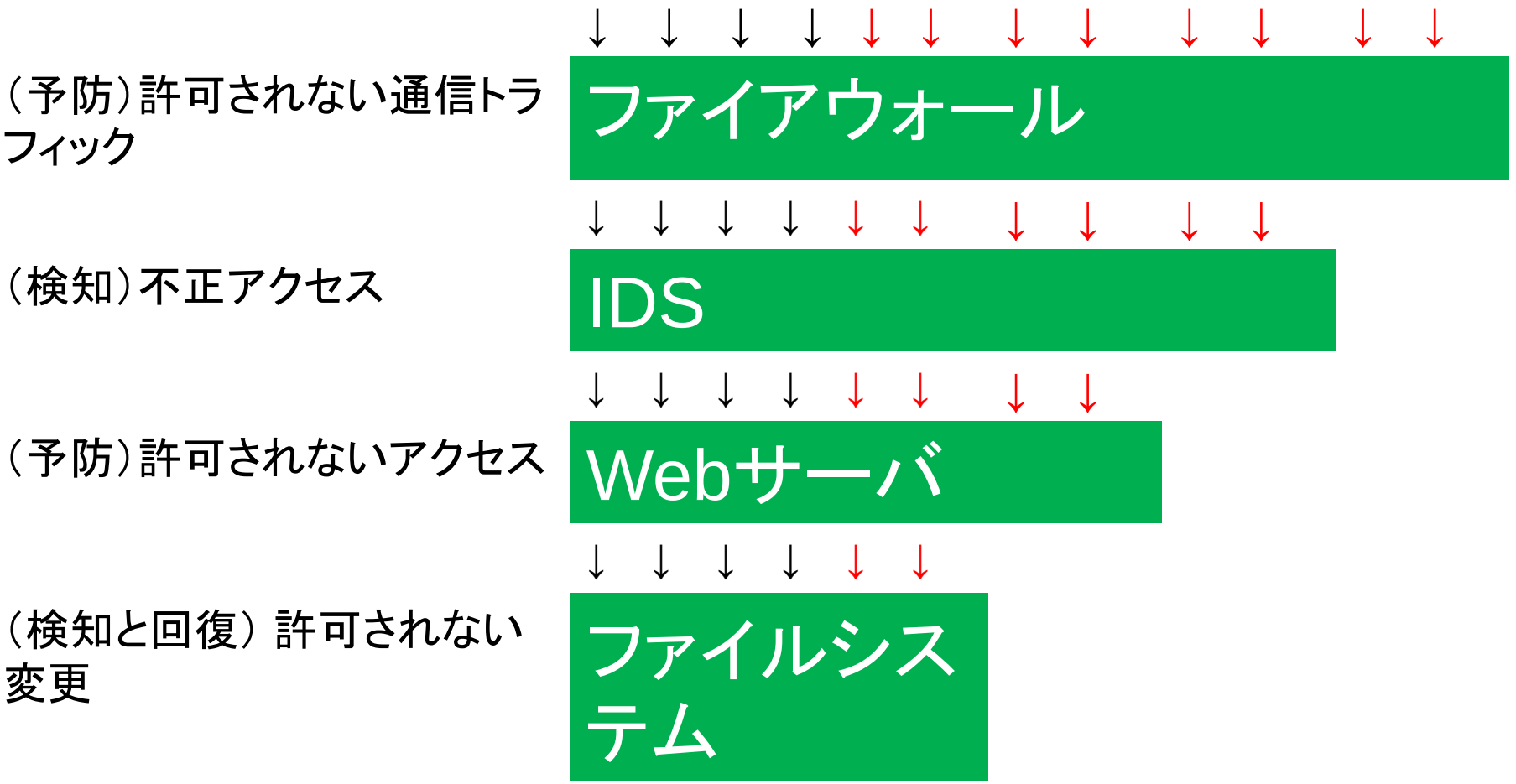


コントロールの機能

抑止	攻撃者を牽制する
予防	攻撃をくい止めるか、脆弱性を解消する
検知	脅威の予兆・顕在化を速やかに発見・通知する
回復	正常な状態に復旧する

- 複数のコントロールを同時に実施する.
  - cf. 多層防御 (defense in depth)

多層防御の例


（予防）許可されない通信トラフィック
ファイアウォール
（検知）不正アクセス
IDS
（予防）許可されないアクセス
Webサーバ
（検知と回復）許可されない変更
ファイルシステム

情報セキュリティ技術とは

- コンピュータ及び通信システム内の情報資産（とシステム自身）のCIAを確保する方法
- 基礎技術
  - 暗号と鍵管理
  - 認証と権限管理（アクセス制御）
  - ネットワーク監視と侵入検知
  - バックアップと復旧、等
- 運用管理
  - ポリシー策定、教育、監査、緊急対応、等

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
- 増加の一途
- 現実社会に影響を与える

不正アクセスの状況（1/2）

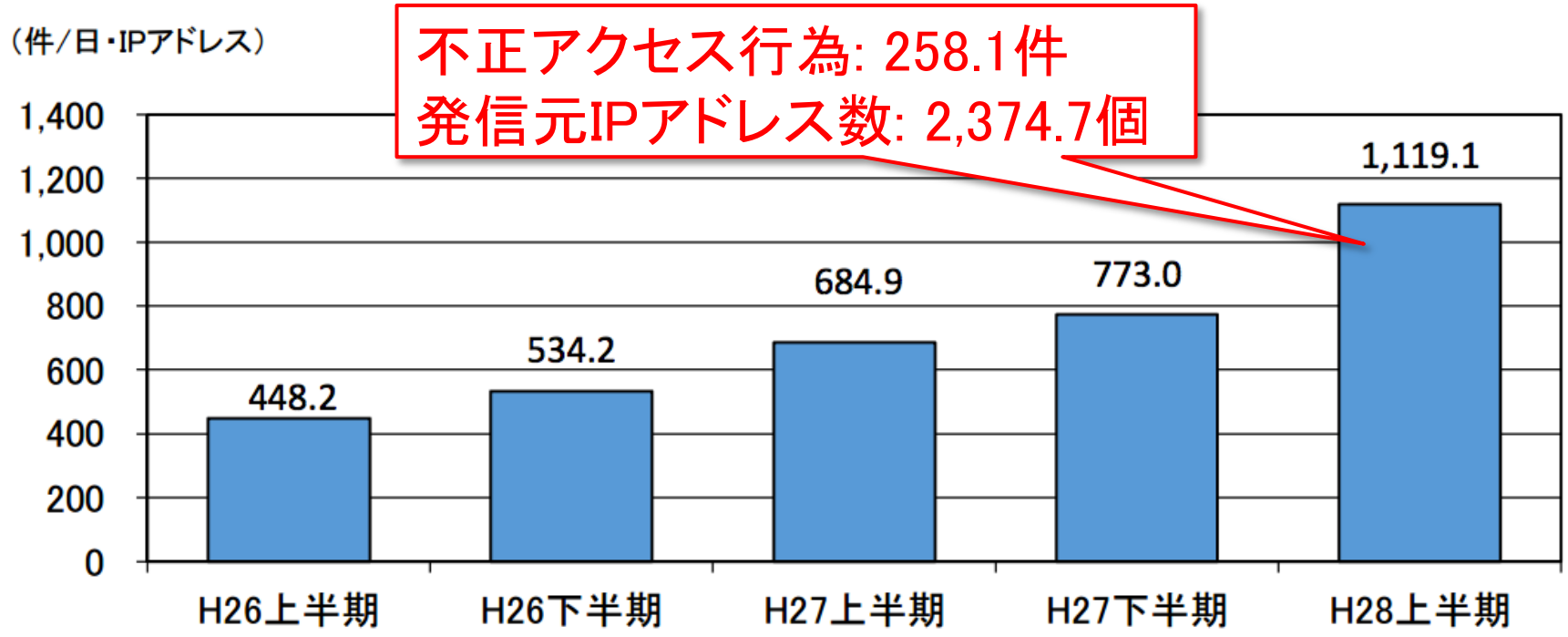


図5-1　センサーに対するアクセス件数の推移

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 インターネット観測結果等（平成28年上半期（1月～6月））

- https://www.npa.go.jp/cyberpolice/detect/pdf/20160915.pdf

不正アクセスの状況(2/2)

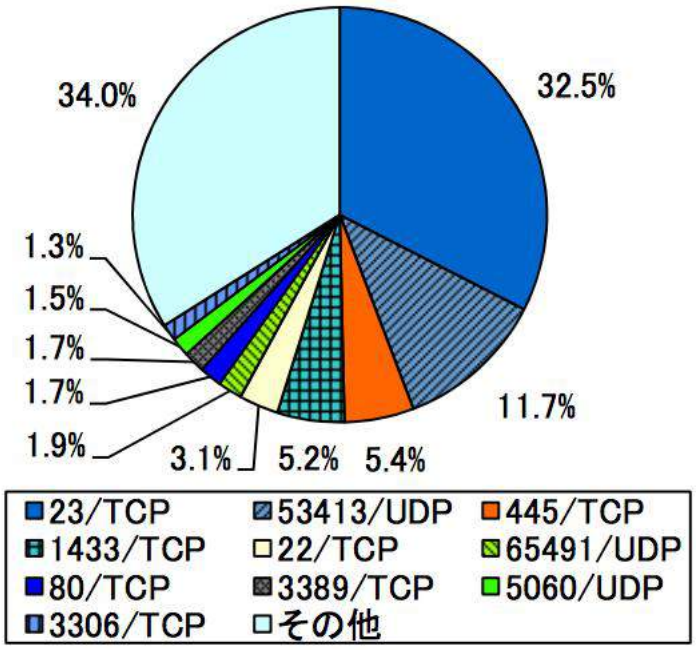


図5-2 宛先ポート別比率(全て)

- 23/TCP: Telnet
  - 発信元は、ルータ、ウェブカメラ、ネットワークストレージ、デジタルビデオレコーダなど(OSはLinuxと推測) ← 攻撃の踏み台
- 53413/UDP: 海外製ルータ
  - 既知の脆弱性を利用した不正プログラムの感染
- 445/TCP: Windows SMB
  - 2008年Conficker以降、高水準
- 1433/TCP: Microsoft SQL Server
- 22/TCP: SSH

現実社会への影響（例）

- 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
- 経済
  - フィッシングメールを使った株価操作

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（営業秘密）を漏らす

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

1 OSやソフトウェアは常に最新の状態にしておこう

新たにひろまるコンピュータウイルスに対抗するため製造元から無料で配布される最新の改良プログラムにアップデートしましょう。

4 身に覚えのない添付ファイルは開かない

身に覚えのない電子メールにはコンピュータウイルスが潜んでいる可能性があります。添付されたファイルを開いたり、URL(リンク先)をクリックしないようにしましょう。

7 大切な情報は失う前に複製しよう

家族や友人との思い出の写真など、大切な情報がパソコンの故障によって失われることのないよう、別のハードディスクなどに複製して保管しておきましょう。

2 パスワードは貴重品のように管理しよう

パスワードは自宅の鍵と同じく大切です。パスワードは他人に知られないように、メモをするなら人目に触れない場所に保管しましょう。

5 ウイルス対策ソフトを導入しよう

ウイルスに感染しないように、コンピュータにウイルス対策ソフトを導入しましょう。(家電量販店などで購入できます)

8 外出先では紛失・盗難に注意しよう

大切な情報を保存したパソコン、スマートフォンなどを自宅から持ち出すときは機器やファイルにパスワードを設定し、なくしたり盗まれないように注意して持ち歩きましょう。

3 ログインID・パスワード絶対教えない用心深さ

金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すような身に覚えのないメールが届いた場合、入力せず無視しましょう。

6 ネットショッピングでは信頼できるお店を選ぼう

品物や映画や音楽も購入できるネットショッピング。詐欺などの被害に遭わないように信頼できるお店を選びましょう。身近な人からお勧めのお店を教わるのも安心です。

9 困ったときはひとりで悩まず まず相談

詐欺や架空請求の電子メールが届く、ウイルスにより開いているウェブページが閉じないなどの被害に遭遇したら、一人で悩まず各種相談窓口に相談しましょう。(下記参照)

http://www.nisc.go.jp/security-site/trouble/material.html#security9

パスワード

- パスワード管理のルール
- 不正ログイン
- パスワード以外の認証方法

パスワードとは？

- 本人しか知らない、秘密の情報
  - 数字、文字、記号の組合せ
- 認証に用いる
  - 本人であることの証拠

【認証/Authentication】本人であることを確かめること

パスワード管理のルール

【よくあるルール】

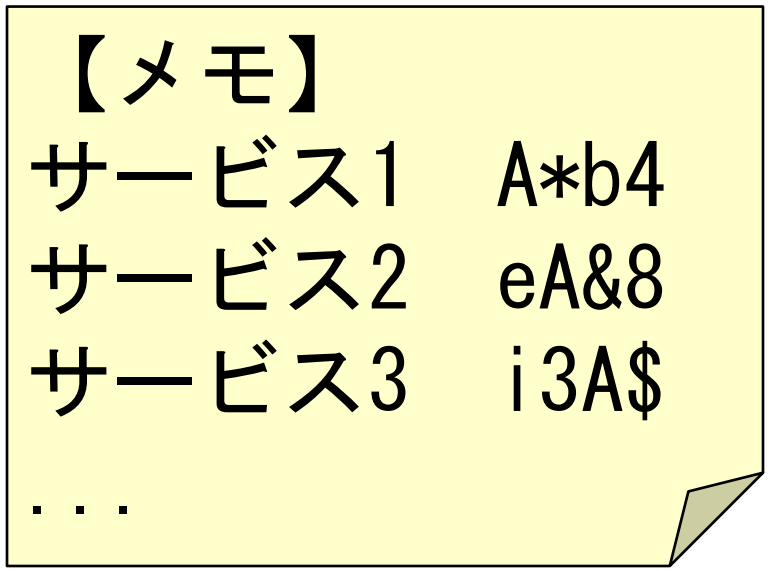
(R1) 推測しにくい(強度の高い)ものを使用する

(R2) 同じものを使いまわさない

(R3) 定期的に変更する

PW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

※ パスワード管理ツールを使う方法も有効

推測しやすいパスワード

- "Worst Passwords of 2015", SplashData, 2016-01-19
  - https://www.teamsid.com/worst-passwords-2015/
  - 漏えいした200万件以上のパスワードを分析

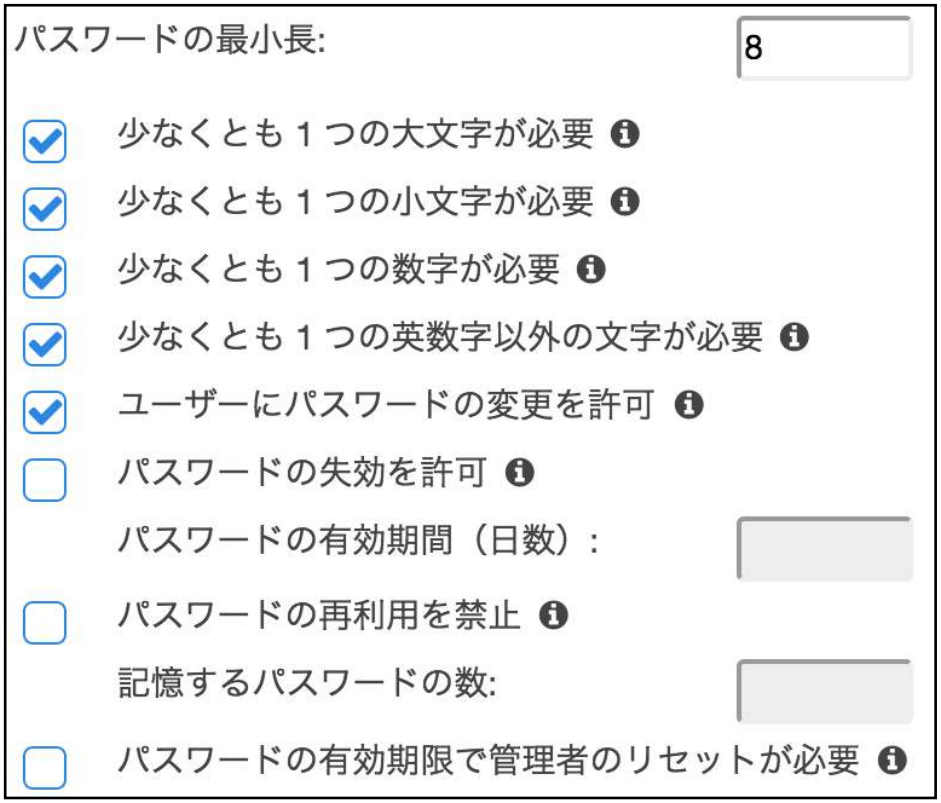
RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘

11	welcome	NEW
12	1234567890	NEW
13	abc123	1 ↗
14	111111	1 ↗
15	1qaz2wsx	NEW
16	dragon	7 ↘
17	master	2 ↗
18	monkey	6 ↘
19	letmein	6 ↘
20	login	NEW
21	princess	NEW
22	qwertyuiop	NEW
23	solo	NEW
24	password	NEW
25	starwars	NEW

推測されにくいパスワード

- 長い
- 英数字以外に記号も使う
- 辞書にある単語は使わない

- AWSの例
  (Amazon Web Services)



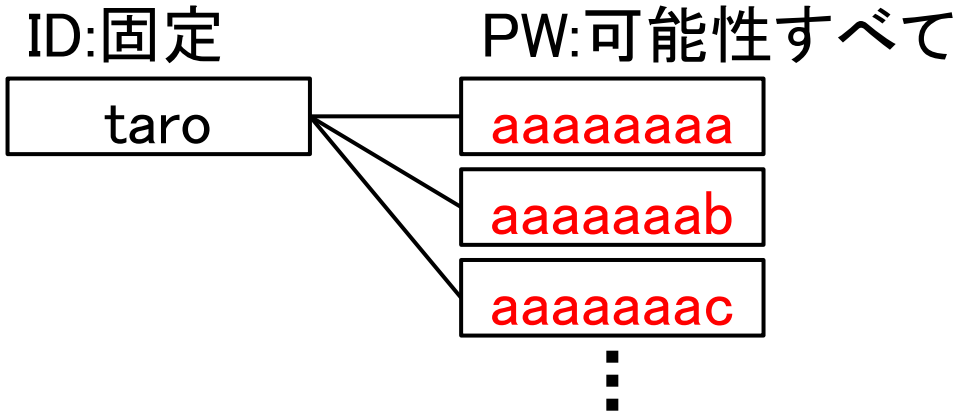
その他の管理ルール

残念な認証システム

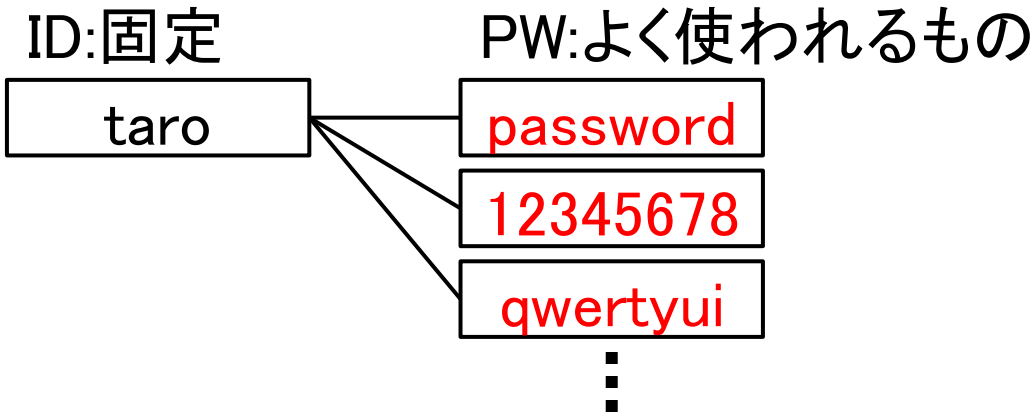
- 「弱い」パスワードしか設定できない
  - 短い（例: 4文字）
  - 少ない文字種（例: 数字のみ）
- 「弱い」パスワードを設定できてしまう
  - 設定できないようにすべき
  - AWSの例を参照

パスワードクラッキングの手法
（オンライン）

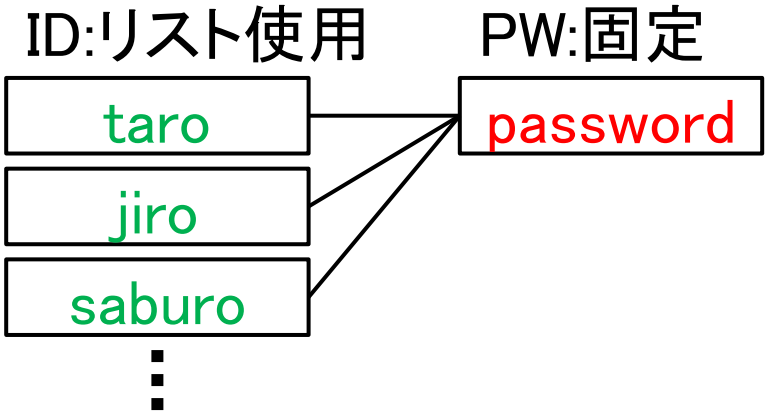
(A1) ブルートフォース攻撃



(A2) 辞書攻撃



(A3) リバースブルートフォース攻撃



パスワード管理ルールR3は不要か？

(R3) 定期的に変更する

【有効なケース】

- PWが漏えいした場合
- PWが推測されてしまった場合

⇒ 不正利用さえる期間を抑えられる

【懸念】

- PWの不正利用期間は短い(変更前に不正利用の目的を達成)
  - LINEのなりすましによる電子通貨の購入依頼
  - 不正送金

別のアプローチ(1):２要素認証

パスワード

（本人だけが知っている）

＋

（仮想）デバイス

（本人だけが持っている）

- ワンタイムトークンをSMSに送信
- デバイスやアプリで時刻同期トークンを生成

【例】AWSのログインにGoogle Authenticatorを使用

【多要素認証/Multi-Factor Authentication】知識、所有物、生体の複数を組み合わせる。

別のアプローチ(2): ログイン履歴

- ログインの履歴表示または通知サービス
  - 不正なログインにいち早く気付く
  - 通知はプッシュ型なので、ユーザは管理不要
  - 実現コストは高くない
  - ログインの失敗を通知することも有効

不正ログインのコントロール（1/2）

- SQLインジェクション脆弱性の解消
  - 漏えいしたPWリストが他のサービスへの攻撃に利用される
- 多要素認証
- ログイン履歴の表示・通知
- 生体認証
- CAPTCHA
- パスワードの暗号化
- 認証情報を自分で管理しない
  - OpenID ConnectとIdP（ID Provider）、OAuthの利用

不正ログインのコントロール(2/2)

- アカウントロック
  - 同一IDに対する連続したログイン失敗を検知
    - リバースブルートフォース攻撃には効果なし
    - 【例】数字4文字の場合のパターンは10,000、アカウント数1,000,000ならば同じPWは平均100人
  - 接続元のIPアドレスごとにログイン失敗を検知
    - ゆっくりした分散攻撃には効果なし
      - 試行間隔が長く、試行回数が少ない
    - 【例】2013年のGitHubに対する不正ログイン攻撃

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？
- 比較: 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？
- 分類
- 例

ソーシャルエンジニアリングとは？

- 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

比較

約30.7億円（前年29.1）

- インターネットバンキングの不正送金被害額
- 2015年
- 警察庁「平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について」
  - http://www.npa.go.jp/cyber/pdf/H280303_banking.pdf（参照: 2016-11-11）

約482億円（前年565）

- 振り込め詐欺の被害額
- 2015年
- 警察庁「平成27年の特殊詐欺認知・検挙状況等について（確定値版）」
  - https://www.npa.go.jp/sousa/souni/hurikomesagi_toukei2015.pdf（参照: 2016-11-11）

※ ターゲット: メガバンク/個人口座 → 地方銀行 → 信金 ⇒ 法人口座

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簡単
  - 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: 金銭、名誉棄損、ストーカー、復讐
- 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: フィッシング（1/2）

1

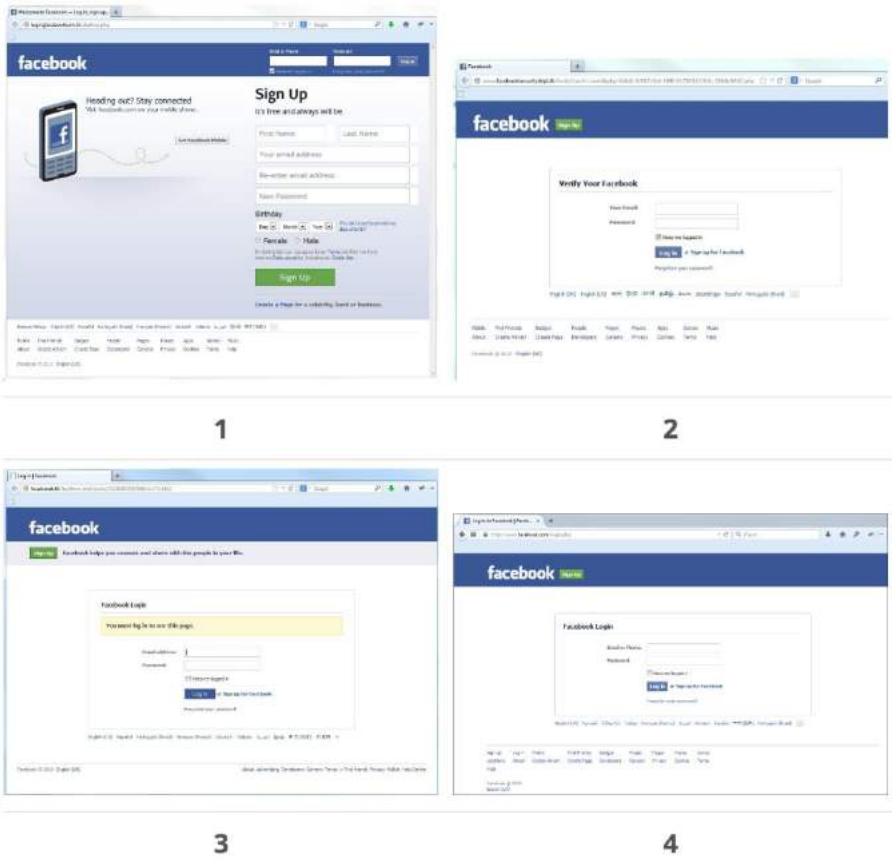
2

3

4

本物のFacebookはどれ？

例: フィッシング（2/2）



URLをよく見ると

1. loginfacebook.tk
2. www.facebooksecuritydept.tk
3. facebaook.tk
4. https://www.facebook.com

.tk: country code for Tokelau,
a territory of New Zealand
located in the South Pacific.

出典: あなたのネット「常識力」はどのくらい？ - カスペルスキー
https://blog.kaspersky.co.jp/cyber-savvy-quiz/

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, LinkedIn, Facebook, 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

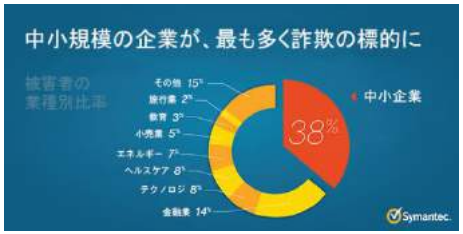
例: ストーカー

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

【警察庁ポータルサイト】https://www.npa.go.jp/cafe-mizen/index.html

新手の詐欺: ビジネスメール詐欺（1/2）

- Business Email Compromise (BEC) Scam
  - 業務上のメールを利用する詐欺（高度なオレオレ詐欺）
  - FBIによる注意喚起（2016年6月）
    - 累積（過去3年）被害者数: 約2.2万、被害額: 約30億ドル
- 手口（例）
  - 【事前調査】役職、業務内容、スケジュール
  - 【メール:社長→経理】今度、業務提携の打合せに出張する。その場で契約するかもしれない。たぶん300万円くらい。
    .....
  - 【メール:社長→経理】今出先だが、この前話した業務提携の件で、至急この口座に200万円送金してくれ。
  - 【メール:経理→社長】承知しました、すぐに処理します。
    .....
  - 【経理→社長】先日の契約の領収書が届かないのですが...
  - 【社長→経理】何の契約？



参考: https://www.ic3.gov/media/2016/160614.aspx
画像: https://www.symantec.com/connect/ja/blogs/bec-0

新手の詐欺: ビジネスメール詐欺(2/2)

- 手口
  - 不正アクセスによる、事前の綿密な調査
  - 社長等の管理職、弁護士、取引先、顧客などを装う
    - 送金の指示、振込先の変更
  - 出張や緊急などの状況設定で、直接確認を避ける

- 対策
  - メールでの指示に対し、電話などで直接確認
  - 不特定多数からの問合せメールを担当する機器の厳格なセキュリティ設定

※ 他に、宅配業者を装う配送連絡メール、顧客を装う商品問合せメールなど

セキュリティ管理

- サイバーセキュリティは経営問題
- さまざまな視点で、継続性をもって取り組むことが重要

サイバーセキュリティは経営問題

- 「サイバーセキュリティ経営ガイドライン」
  - 経済産業省, Ver 1.0, 2015年12月
    - http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html
  - 3原則
    ① 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
    ② 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
    ③ 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

セキュリティ管理のテーマ

テーマ	内容
経営	経営トップがセキュリティを最優先する姿勢を明らかにする
人材	セキュリティ対策の担当者を置く
教育	セキュリティについて関係者に教育する
管理	インシデント発生時の被害の広がりを予想する セキュリティ対策に有効なツールを導入する
監査	セキュリティ対策について外部の目で監査をする

セキュリティ管理の規格

- 国際標準規格
  - ISO/IEC 27000シリーズ
    - ISMS適合性評価制度
  - ISO/IEC 38500（ITガバナンス）
    - 経営者対象の原理原則
- フレームワーク
  - ISMS、COBIT、他
- 補完ドキュメント
  - IPA「組織における不正行為防止ガイドライン」第3版, 2015年3月.
    - https://www.ipa.go.jp/security/fy24/reports/insider/
  - 経産省「情報セキュリティガバナンス確率促進事業」コンテンツ
    - http://www.meti.go.jp/policy/netsecurity/secgov.html

組織として最低限の要素を備えていることを評価・認証

オペレーションレベルにどう落とし込むか？

攻撃側のパラダイム

機会	-	手段	-	動機
when		how		why
時間 アクセス		知識 スキル ツール		理由
【例】 • 公開サーバ • バックドア • 脆弱性		• ドキュメント • ソースコード • 攻撃ツール		• 金銭 • 名声 • 政治活動 • テロ

防御側のコントロール

機会	-	手段	-	動機
時間 アクセス		知識 スキル ツール		理由
【例】 • 脆弱性の解消 • アクセス制御 • 建物/部屋の入退管理 • セキュリティ診断		• 不要な情報の非開示 • ウイルス対策		• 法律 • 教育 • 不満の解消

侵入検知、インシデント対応

セキュリティ対策

- 攻撃者は、脆弱性を悪用して、資産に損害を与えようとする
- 攻撃者の機会・手段・動機を削減するために、物理的・手続き的・技術的コントロールを工夫しなければならない
- 脅威の発生頻度と影響を考慮して、費用対効果のバランスをとる

セキュリティ管理の難しさ

- コントロールは、必ずしも期待した効果を発揮するとは限らない
- 「人間」という要素がもっとも脆弱
- 技術以外の対応策にも目を向ける

防御側の不利、攻撃側の優位

	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.

製品の欠陥: 一般論

製造物 → リコール

製造物責任法(PL法)、
消費生活用製品安全法、
道路運送車両法、など

製造者・販売者による
無償修理、交換、返金など
損害賠償責任

▼

材料、設計方法、製造プロセス、
検査方法などの改善

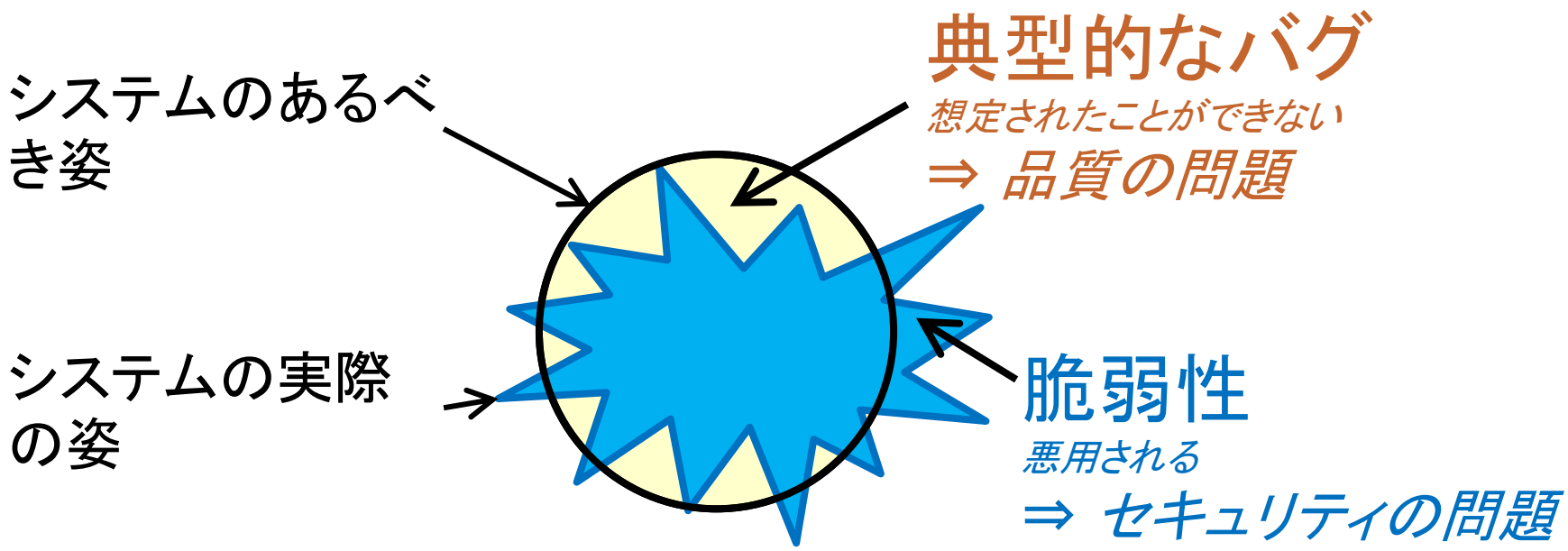
ソフトウェア → ???

無保証(No Warranty)、
ユーザの自己責任

だれがどう対処するか?
どんな技術が必要か?

バグと脆弱性

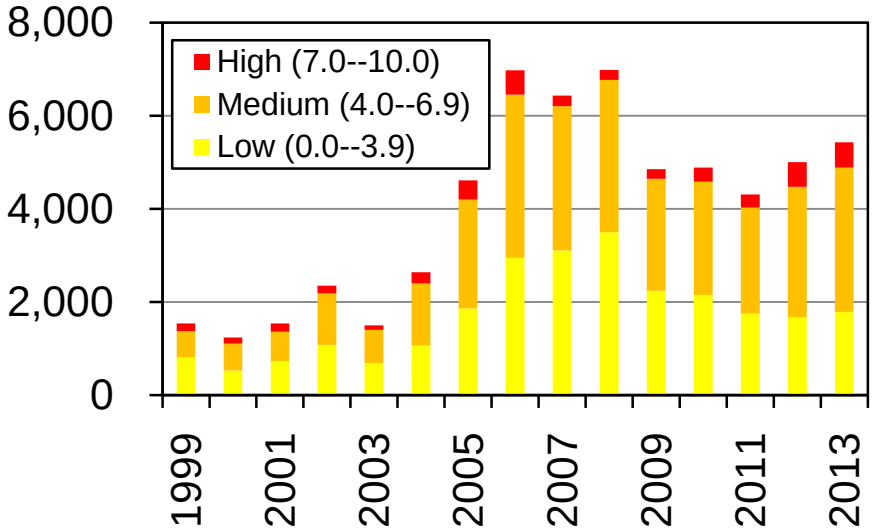
- どちらも欠陥
  - 期待される機能が不足している
  - 指定されたこと以上のことができてしまう



脆弱性管理に必要な情報量

脆弱性の数

約5,000件/年, 15～17件/日



ソフトウェアの種類

1,000 ~ /システム

Debian 7 wheezy	48,559
Ubuntu 14.04LTS	52,720
CentOS 7 (OS)	2,481

✓ 経験上、実際にインストールするのは500～1,000程度

ノード(コンピュータ)の数

脆弱性の数 × ソフトウェアの種類 × コンピュータの台数

最近の話題になった脆弱性

OpenSSL Heartbleed Bug

⇒ 簡単にはみつからない
⇒ Webサーバだけでなく多種のソフトウェアに影響

- 脆弱性識別子: CVE-2014-0160
  - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
  - 問題: Heartbeat Buffer Overread - サーバ内のメモリをリモートから読み出せる。
  - 問題コードの追加: OpenSSL 1.0.1(2012年3月)

ShellShock

- 脆弱性識別子: CVE-2014-6271, CVE-2014-7169
  - https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
  - 問題: 環境変数による関数定義の過実行 - リモートから任意のコードを実行できる。
  - 問題コードの追加: bash 3.0(約20年前)

脆弱性の発見に対する懸賞金

- Google: リモートコード実行 最高$20,000、SQLインジェクション 最高$10,000など
- サイボウズ: CVSS v2の基本値×1～3万円（つまり最高30万円）
- Microsoft: Win8.1上のIE11プレビューに対し最高$11,000
- Microsoft: CoreCLRやASP.NET 5、あるいはVisual Studio 2015でデフォルト提供される「Web Tools Extension」の「最新ベータ版もしくはRC（Release Candidate：出荷候補）版」に含まれる脆弱性で、未発見のものに$500～$15,000

どんなベンダーの製品にも欠陥の可能性

自動更新 ≠ 安全

自動更新ツール

- OS機能： Microsoft Update、各種Linux、Mac...
- アプリ/ベンダ固有： Adobe、Google Chrome、...

利用者の都合で（すぐに）更新できないこともある

- サービスや業務の継続、動作確認、etc.

最新バージョン ≠ 脆弱性なし

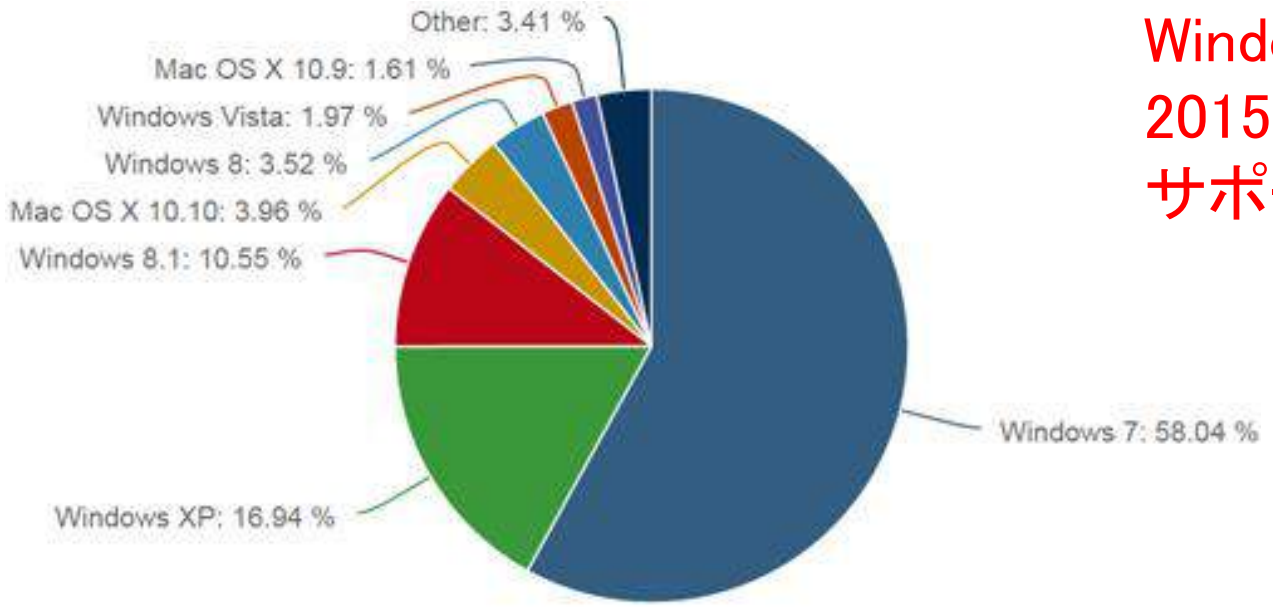
- 「最新なら安全」という誤解

◎現状の正しい理解　〇できるだけ最新（自動）

サポート切れ

Windows XP（2014年4月8日サポート終了）

- デスクトップOSで約17%のシェア
  - 2015年3月のNet Applicationsの調査



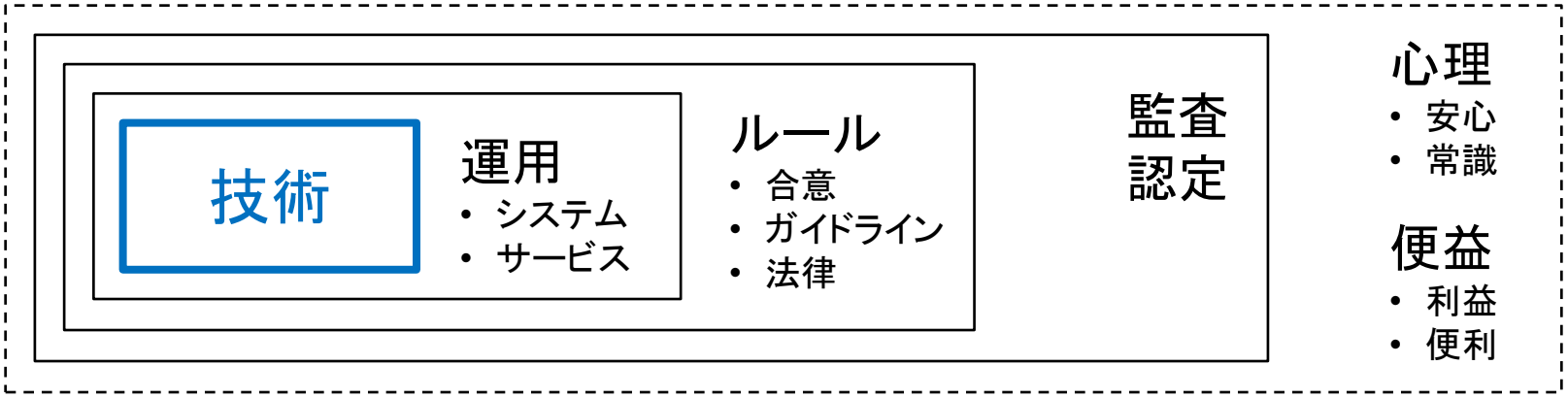
Windows Server 2003
2015年7月15日
サポート終了

http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

技術の役割

セキュリティの課題

▼ 解決手段



リスク対応（1/2）

資産の価値 x 損害の程度 x 脅威の深刻さ

限られた資源
（時間、資金、能力）

↓

防御の優先付けと
コントロール（対策方法）の選択

リスク対応（2/2）

技術的な対策だけで100%を目指さない

セキュリティ対策の考え方

- どのような悪いことが起こり得るか、想像する

- コントロールは、必ずしも期待した効果を発揮するとは限らない
- 完璧なコントロールは存在しない. 事後対応や回復手段を必要とする

サイバーレジリエンス

事故前提の考え方で、いざという時に備える。

サイバーレジリエンス

サイバーセキュリティから
サイバーレジリエンスへ

- レジリエンス/Resilience: 復元力、回復力の意
- 100%の防御は不可能、事故前提の考え方
- バックアップやリカバリまでを含めた対策が必要

  【例】ランサムウェアによるファイル暗号化

  ⇒ バックアップからの復元

バックアップ（1/2）

バックアップの目的

- 古くは
  - 故障リスクの対策
  - システムの信頼性が低かった
- 今は
  - セキュリティリスクの対策
  - いつか起こるインシデントからの復旧手段
    - 【例】ランサムウェア

バックアップ（2/2）

３－２－１ルール

- ３個（以上）のコピーを保存する
- ２種類（以上）のメディアに保存する

  【例】USBメモリとクラウド

- １個は他と離れた場所に置く

  【例】自宅とオフィス

まとめ

- 後を絶たないインシデント
  - インシデント＝リスクの現実化（セキュリティ事故）
  - 情報漏えい等のインパクトは大きい
- セキュリティ対策は継続的に、最新の方法で
  - 身の丈に合わせて、できることを確実に
  - 経営問題と認識する
- 人間も重要な要素
  - 免疫のないソーシャルエンジニアリング
  - ITだけが攻撃の経路ではない
- 「レジリエンス」という考え方

参考文献

- 情報セキュリティ標準テキスト編集委員会/編: 情報セキュリティ標準テキスト, オーム社, 2006年, ISBN: 978-4274202179.
- 株式会社ラックデータベースセキュリティ研究所/著, 情シス担当者のための絵で見てわかる情報セキュリティ, 翔泳社, 2011年, ISBN: 978-4798123769.
- 独立行政法人情報処理推進機構/著, 情報セキュリティ読本 第四訂 ―IT時代の危機管理入門―, 2013年, ISBN: 978-4407330762.
- 徳丸 浩/著, "徳丸浩のWebセキュリティ教室", 日経BP社, 2015年, ISBN: 978-4822279981.