

人と社会を支える サイバーセキュリティ



CERT 統括責任者 / 副CISO

松浦 知史 (matsuura@cii.isct.ac.jp) 1

本日の話題

- サイバーセキュリティとは何なのか
- 世の中では、科学大ではどんな事件が起きているのか
- どんな技術が必要か、技術以外に何が必要か

サイバーセキュリティとは

「情報セキュリティ」と「サイバーセキュリティ」はどう違うか

ちょっとその前に・・・

運送業者(荷物)の安全とは？



出典: by Álvaro Ibáñez <https://www.flickr.com/photos/alvy/11309312793/>

交通網(交通社会)の安全とは？



出典: Mail Online <http://www.dailymail.co.uk/sciencetech/article-1043123/Extraordinary-satellite-images-ordinary-day-Britain--seen-space.html>

- ・ どんな危険が存在するか
- ・ どんな対策が存在するか
- ・ 従業員はどう振る舞うべきか
- ・ 個々人はどう振る舞うべきか

情報資産の安全とは？



出典: Hack A Mod <http://hacknmod.com/hack/worlds-most-stunning-data-centers/>

・情報セキュリティ

規模：組織

対象：情報資産(データ)



どう守るか？

CIA

Confidentiality(機密性), Integrity(完全性), Availability(可用性)

サイバー空間の安全とは？



出典: the-internet <https://visit4it.wordpress.com/internet/the-internet/>

・サイバーセキュリティ

規模：社会

対象：サイバー空間(インフラ+人)



どう守るか？

?

大学を取り巻く環境

情報セキュリティの確保 = 重要な経営課題

I. 全体方針 1. 情報セキュリティ対策基本計画の目的

公共性の高い国立大学法人等において、情報セキュリティ対策は社会的に求められるものであり、経営上の重要課題との認識の下、法人全体として組織的及び計画的に取り組み、情報セキュリティ水準を維持し、さらに向上を図っていくことが不可欠なものである。

国立大学法人 東京科学大学 情報セキュリティ対策基本計画

全ての業務はデジタル基盤上で行われる時代 = セキュリティは必須

サイバー攻撃の深刻化や巧妙化の進展

- 国家を背景とした攻撃の拡大、未知の脆弱性を悪用したゼロデイ攻撃の増大等、サイバー攻撃の洗練化・巧妙化が一層進展。生成AI等の新技術の普及に伴う新たなリスクも増大。
- ⇒ 政府機関・重要インフラ事業者、ユーザにサービスを提供するテクノロジー企業などの能力ある主体がより多くの役割を果たすことが重要。サイバー安全保障の観点も含め、平素からの対策強化や対処能力の向上、セキュアバイデザイン・セキュアバイデフォルト原則に基づく措置の具体化、欧米主要国をはじめとする関係国との協調・連携が必要に。

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせるデジタル社会の実現	国際社会の平和・安定及び我が国の安全保障への寄与
経済社会における情勢 - 企業活動におけるITの利用促進に伴う脅威の高まり。 - 大企業への直接のサイバー攻撃だけでなく、その取引先の協力会社を攻撃の踏み台にした例も見られる。 - 直接の攻撃を受けた組織のみならずサプライチェーン全体にも被害が及び得る - ランサムウェア被害の約半数が中小企業。 中小企業・サプライチェーン対策 - 組織向けのサプライチェーン・リスクへの対策は必須であり、特に中小企業を対象とした民間部門に対する対策の支援サービスや機能充実が必要。 IoT製品のセキュリティ確保に向けた取組の推進 - 悪用が懸念されるIoT機器のセキュリティ評価等の対策が必要。	経済社会基盤を支える各主体における情勢 ①政府機関等 - インシデント件数は高止まりしている。 (2021年度207件、2022年度266件、2023年度233件) - GSOCによる政府機関等への脆弱性情報等の提供も増加。 (2021年度598件、2022年度630件、2023年度861件) - 第一、第二GSOCの緊密連携等が必要。 - 脆弱性等の是正を促す仕組み(ASM)や、悪性サイト等のIPアドレスを検知・蓄積するプロテクトDNSを導入。 ②重要インフラ - 国内外の重要インフラ分野等において、システム障害や情報流出の事例が多数発生。 (例: 港湾施設が、ランサムウェアによるサイバー攻撃を受けて停止) - 侵入を前提とした多層防御の考え方に基づくシステム設計・運用、サイバー被害を想定した事業継続計画の立案・点検等が必要。 ③大学・教育研究機関等 - 大学等の特性を踏まえた上で、主体的なセキュリティ水準の維持・向上を図る必要。 ④東京オリンピック・パラリンピック競技大会に向けた取組から得られた知見等の活用 - 大阪・関西万博等への知見の活用が重要。	国外の動き(諸外国の国際動向)  米国 - 国防総省「サイバー戦略2023」の概要を公表(2023年9月) 「セキュアバイデザイン・セキュアバイデフォルト原則」に関する国際ガイダンスの改訂 (我が国を含む13の国・組織が共同署名)(2023年10月)  英国 「セキュアAIシステム開発ガイドライン」を作成 (我が国を含む18の国・組織が共同署名)(2023年11月)  豪州 「2023-2030年豪州サイバーセキュリティ戦略」及び「アクションプラン」を公表(2023年11月) 「AIシステム使用に関するガイダンス」を作成 (我が国を含む11の国・組織が共同署名)(2024年1月)  EU 「サイバー強靱化法」を欧州議会が承認、「サイバー連帯法」の政治合意(2024年3月)  ASEAN - 日本ASEAN友好協力50周年特別首脳会議の開催、「共同ビジョン・ステートメント」及び「実施計画」の公表(2023年12月) 国際協力が不可欠。各国の動向を踏まえ、強化に取り組む。
横断的施策		
サイバーセキュリティ分野の研究開発 - 生成AIの普及、量子等の先端的な技術の進展、昨今の国際情勢の複雑化等により安全保障の裾野がサイバー分野に拡大する中、サイバー空間の安全・安心の礎となる研究開発の重要性はますます向上。 - 研究の裾野を広げる観点からの産学官エコシステム構築に向けた体制整備、実践的な研究開発構想の検討を実施。	IT・サイバーセキュリティ人材 - サイバーセキュリティ人材確保の需要の高まりに加え、DXを進めるに当たり、現時点で知識・業務経験を有しない人材のリスク等に対する需要が引き続き増大。 「デジタル田園都市国家構想総合戦略」において、サイバーセキュリティ人材を含むデジタル推進人材を2026年度末までに230万人の育成を目指す。 - スキルを習得できる環境整備、「プラス・セキュリティ」等の経営層の意識改革、大学・高専等での取組強化が必要。	国民の意識・行動 - デジタル化が着実に進展する一方、フィッシングによる不正送金の被害件数、被害額が過去最多。 - サイバーセキュリティ対策の必要性につき、訴求すべき対象に応じたよりきめ細かな普及啓発活動とともに、各主体が密接に連携・協働することが必要。 「サイバーセキュリティ意識・行動強化プログラム」に基づき、引き続き普及啓発活動に取り組む必要。

* NISC: サイバーセキュリティ2024の概要

- <https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024_gaiyou.pdf>

国を挙げて、大学(先端研究/政府機関)の情報・知財に非常に強い関心！！

情報セキュリティインシデント = 多大な経営資源の損失

バックドアの存在に7年間気づかず、政策研究大学院大学がネット接続を8カ月間遮断

安藤 正芳 日経クロステック／日経コンピュータ

2023.09.22

有料会員限定



全2810文字

急務であるバックオフィスのDX化、導入の事例やその効果についてご紹介 **PR**
生成AIで循環型社会/データ活用：東京大学 越塚氏とメルカリ石川氏 **PR**
CPU/GPUの排熱が最新サーバーの差別化ポイントとなる、その理由は？ **PR**

政策研究大学院大学がインターネット接続を遮断する事態に追い込まれた。攻撃者が公開Webサーバーにバックドアを設置。これを利用した不正アクセスを受けたことが原因だ。情報システム担当者がメンテナンス作業中に不正な通信を検知して発覚した。バックドアは7年前に仕掛けられたもので、システム更改時にも気づかなかった。

2023年8月22日、政策研究大学院大学の田弘子学長が「本学で発生した情報セキュリティインシデントについてのお詫び」という文書を公表した。同大学は2022年8月29日に、不正アクセスによるセキュリティインシデントが発覚。2023年5月までの約8カ月の間、大学内からインターネットが使えない事態に陥った。

同じ2023年8月22日には、インシデント対応から復旧までに従事した学外の専門家がまとめた「政策研究大学院大学の情報システムに対する不正アクセスの調査報告書」と題した文書を公表している。

産総研のネット接続再開に目処 - 他国立研究開発法人では被害確認されず

産業技術総合研究所が2月に不正アクセスを受け、インターネット接続を遮断している問題で接続再開に目処が立ったことが明らかになった。

問題となった不正アクセスは、産総研において2月6日に確認したもの。重大なセキュリティインシデントであると判断し、知的財産や個人情報の漏洩の可能性も含めて影響の範囲や原因などの調査を進めている。

産総研では、インターネット接続を遮断し、安全を確認できた業務システムより順次再開する方針を示していたが、管内閣官房長官は3月15日の記者会見で、インターネット接続についても目処が立っているとの報告を受けていることを明らかにした。

また内閣サイバーセキュリティセンターにより調査を実施し、ほかの主要国立研究開発法人において同様の被害が発生していないことを確認したという。今回の問題を受けて管氏は、サイバーセキュリティの脅威が飛躍的に高まっているとの認識を改めて示し、政府としてもしっかり対応していくことを強調した。

(Security NEXT - 2018/03/16)

人的資源が極端に毀損される

50万/月 x 2ヶ月 x 3000人 = 30億円

* バックドアの存在に7年間気づかず、政策研究大学院大学がネット接続を8カ月間遮断
- <https://xtech.nikkei.com/atcl/nxt/column/18/01157/091900094/>

* 産総研のネット接続に再開の目処 - 他国立研究開発法人では被害確認されず
- <http://www.security-next.com/091178>

**(産総研)2ヶ月程度インターネットが遮断状態→研究活動に甚大な支障
日々の業務を継続的に行うという当たり前の事が崩壊してしまう**

政研大に対する標的型攻撃（2022年）

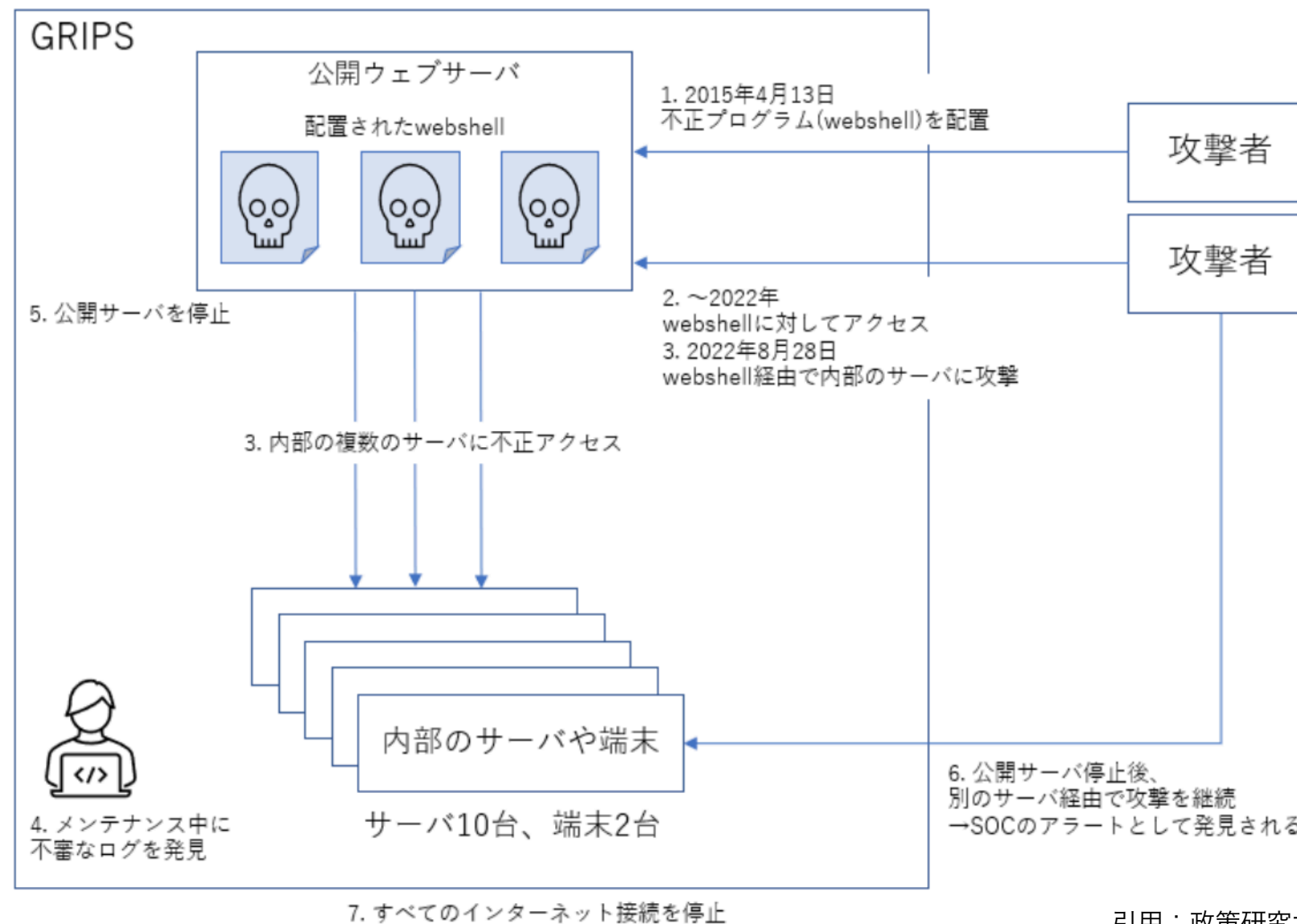
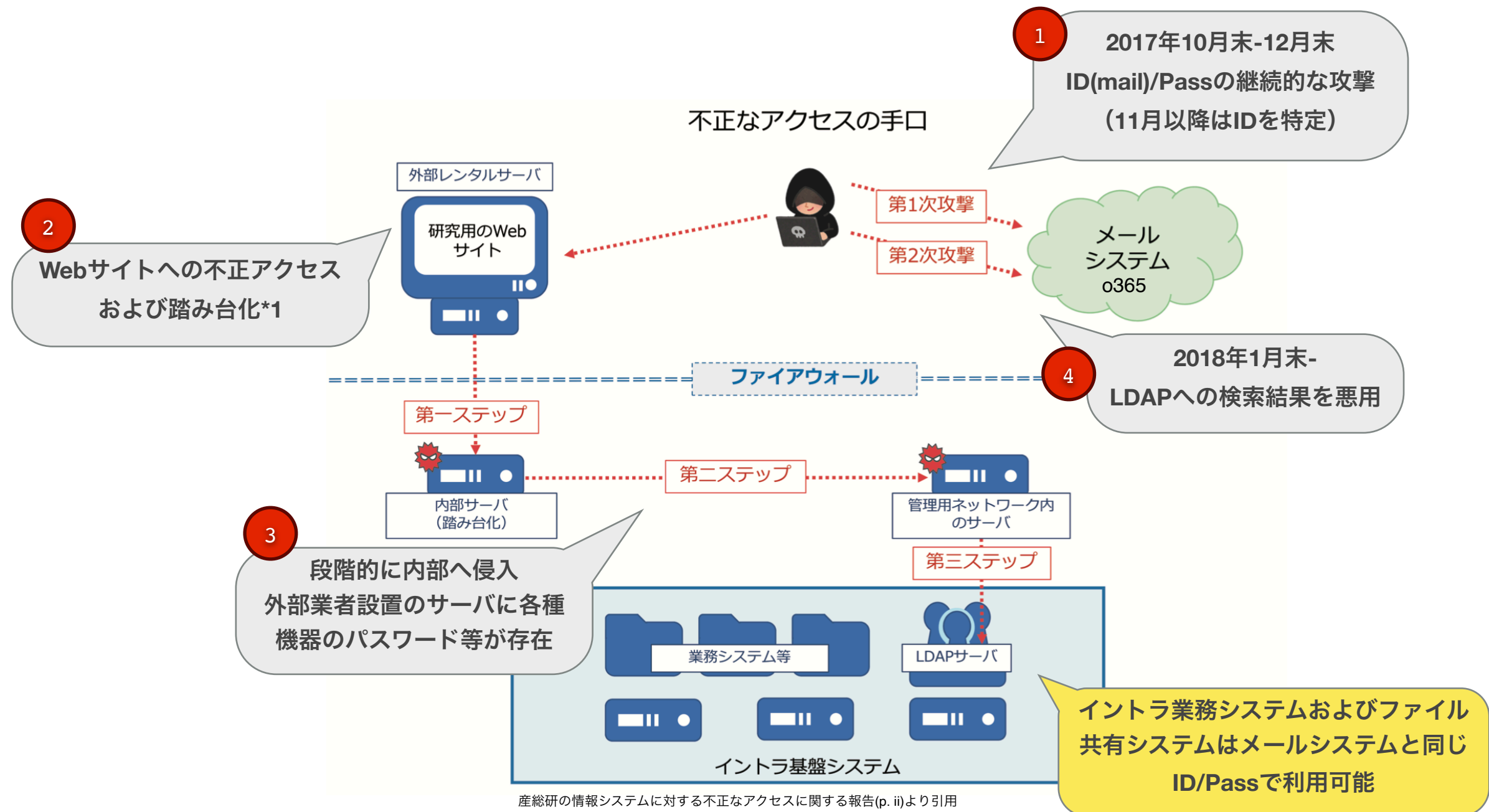


図 1 不正アクセスの概要

引用：政策研究大学院大学の情報システム
に対する不正アクセスの調査報告書

8ヶ月におよぶインターネット遮断、各種業務システムの停止など
日常的な業務が出来ない状態が長期間継続した。心身両面における
健康被害、文科省やNISC含め社会的評価の低下など被害は多岐に渡る

産総研に対する不正アクセス（2018年）



*1 SSHによる緩やかで継続的な攻撃によりログインが成立。またJenkinsを利用し内外を跨いで利用していた事が内部侵入を許したと推測される（スクリプトコンソール機能を悪用されて、内部サーバ側にSOCKサーバ等が仕込まれたか？）。

情報セキュリティを考慮した組織体制

• 連絡体制の確立

- 報告者を褒める文化を！(被害の最小化を最優先する)
- 誰にどこに連絡するか事前に共有する(上司 / 学内CSIRT等)

• データ管理体制の確立

- データ中心に考える！(守るべき対象を中心に考える)
- 適切なアクセス制限を設ける（人・空間・時間の観点が重要）
 - * 人：アカウント管理が適切か。権利の無い人に必要以上のアクセス権が無いのか。
 - * 空間：IPアドレス空間の制限が適切か。世界中からのアクセスを許す必要があるか。共同研究拠点で十分でないか。
 - * 時間：保存期間、破棄プロセスが適切か。プロジェクト終了後にデータを保管する必要があるか。
- 管理者を決定する (継続的にアップデート等を行う)
- 研究データ、個人情報等を分離する

• 留学生を中心にした情報セキュリティ・倫理教育

- 事件を起こした学生は罪の意識が希薄かつ悪意が無い事が多い(文化の違い)
- 日常の中での声かけが特に重要

組織マネジメントと情報セキュリティの関係

情報セキュリティが何処に存在するか → 組織に関係するシステムのあらゆる場所

セキュリティの取り組みを通して、組織全体を改善できる可能性！！

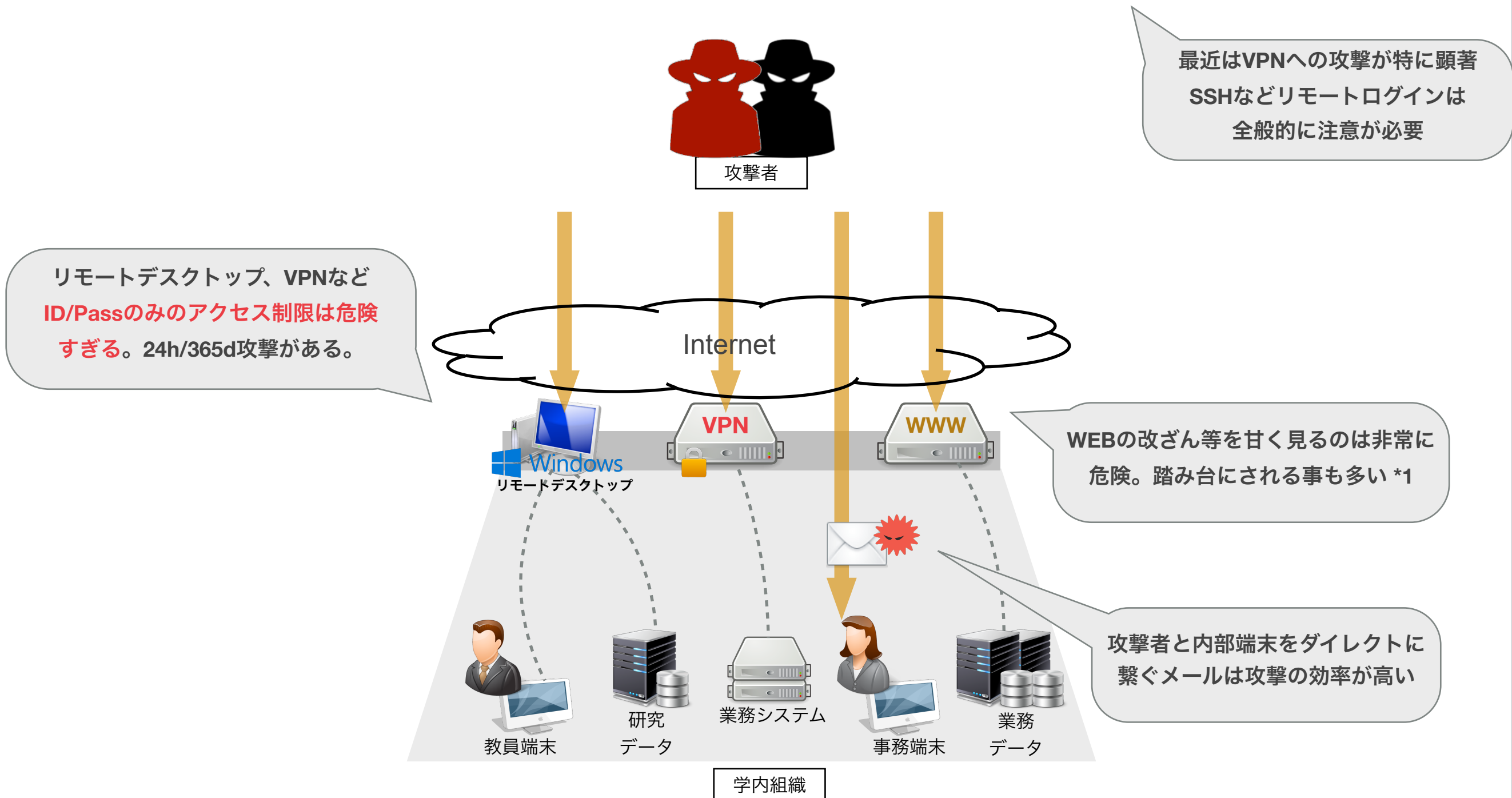
- セキュリティをきっかけに、組織の隅々まで良い影響を！

組織内外の連絡体制、日頃からのコミュニケーション、
風通しの良いグループ、個別組織の文化の守り方、
チームワークの大切さ、リスクマネジメント自体への意識等々

サイバーリスクは、ITの(情報部門の)問題では無くリスク管理の(全学の)問題として扱う必要がある！

イメージ：火災リスクは消防署の問題では無い
→ 当事者意識を持ち火の元管理を行おう！

一般的な内部侵入方法 (RDP / VPN / Mail / WWW)



*1 Blog等にWEB Shellを設置される事が一般的。下記の様なPHPファイル置くだけでも任意のコマンド実行が可能。

```
<?php echo '<pre>'; system($_GET['cmd']); echo '</pre>';?>
```


サイバーレジリエンスの観点

悪条件、高ストレス下においても 組織本来の活動を継続出来る能力

Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

予測力 抵抗力 回復力 適応力



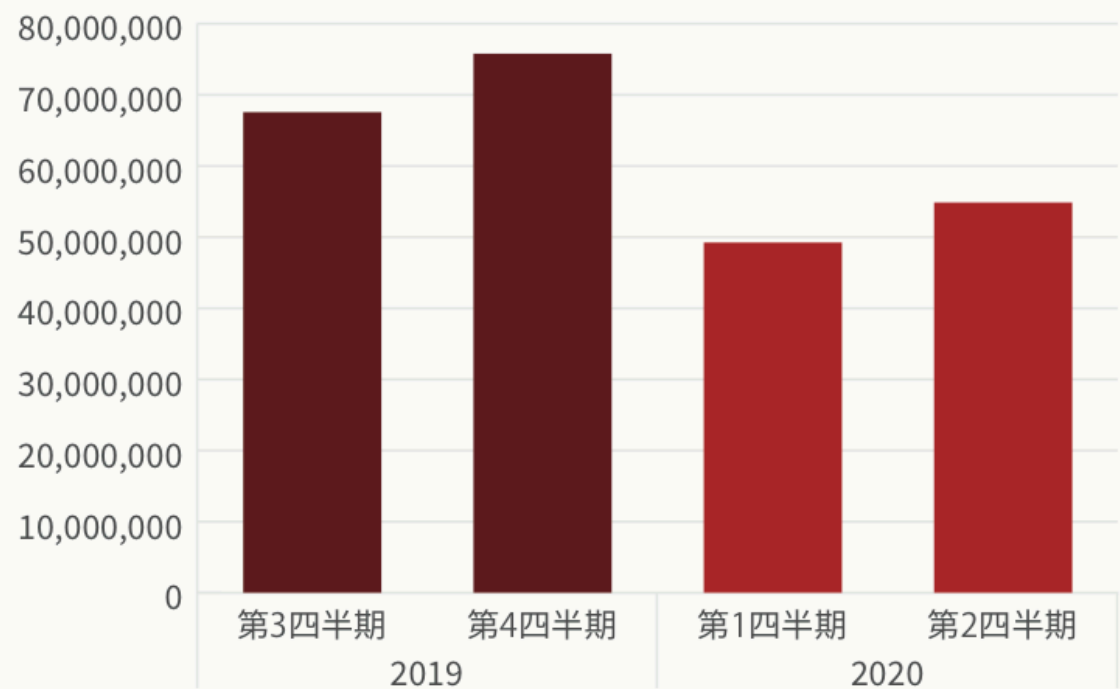
- ミッション / ビジネス機能に焦点を当てる
- 環境の変化を想定する
- APT(標的型攻撃)の影響に焦点を当てる
- 敵対者がシステムや組織を侵害することを想定する
- 敵対者がシステムまたは組織内に存在し続けることを想定する

サイバーレジリエンスにおける5つの特徴 NIST SP 800-160 Vol.2 P.77

最新のニュース

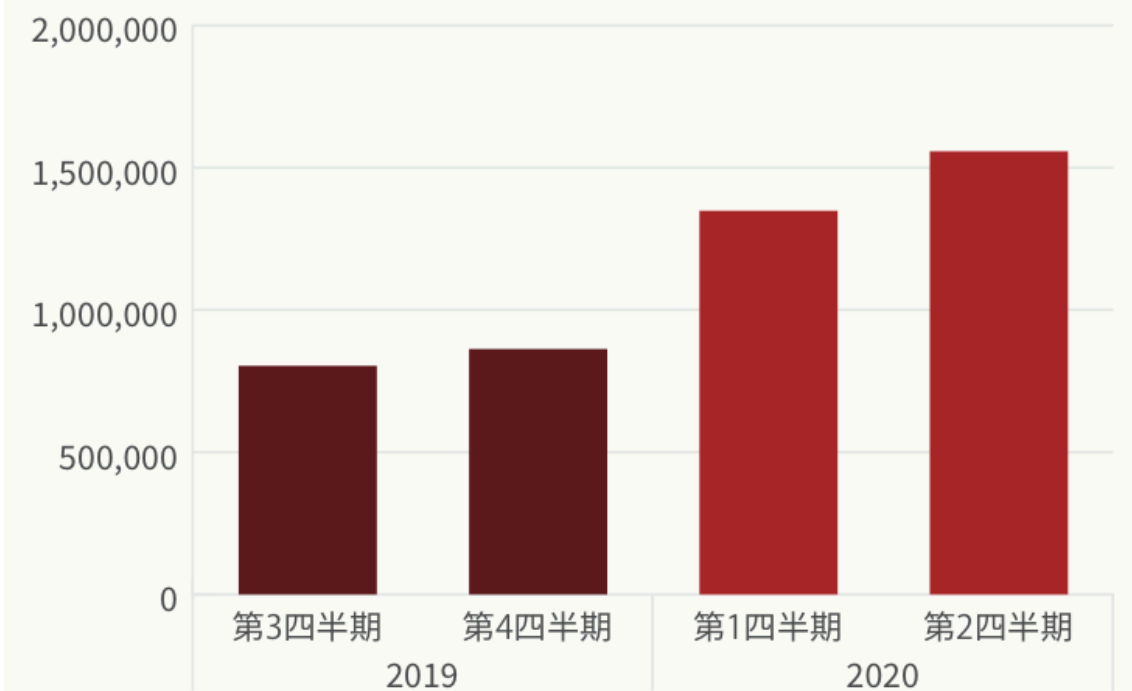
マルウェアに関する統計 1

新しいマルウェア



出典: McAfee Labs, 2020.

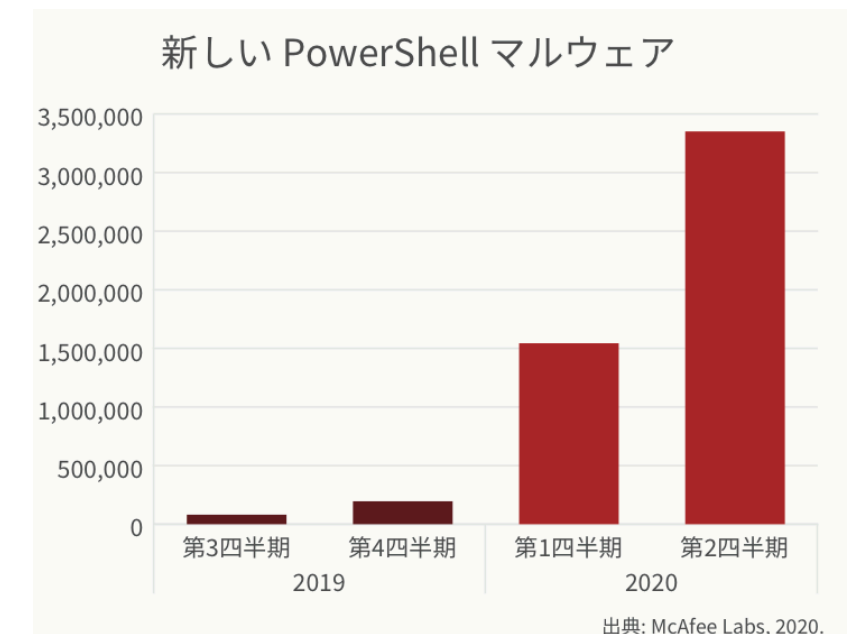
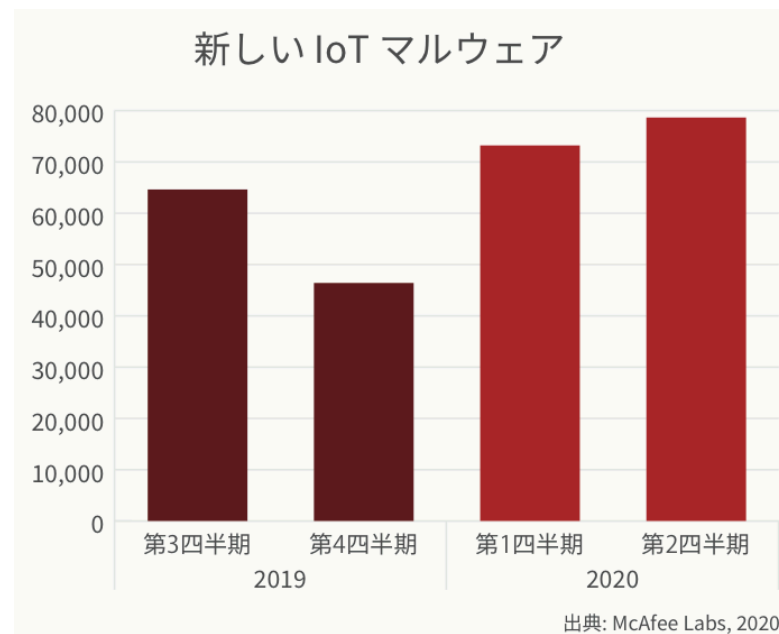
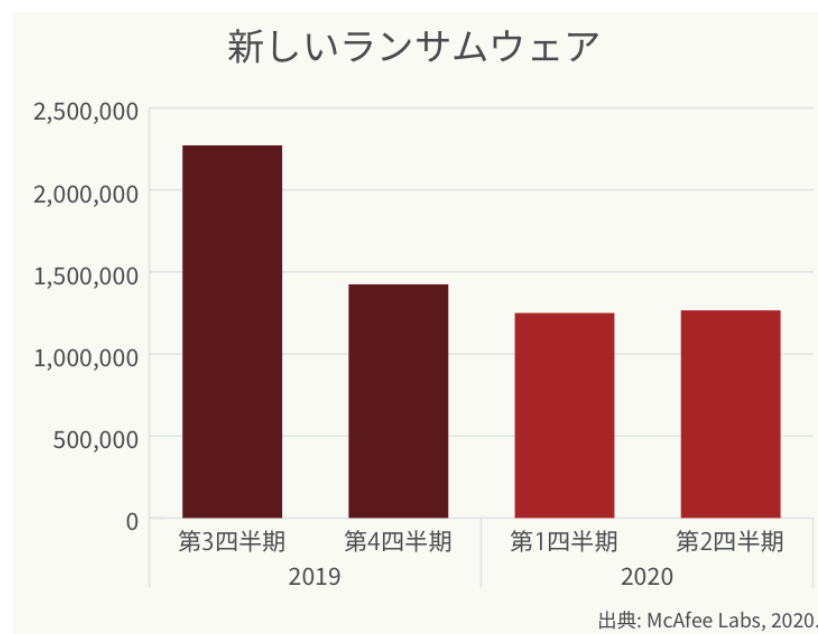
新しいモバイル マルウェア



出典: McAfee Labs, 2020.

1分間に430件の新しい脅威が生まれています
11%程度のモバイル端末が感染しています

マルウェアに関する統計 2



Windows/Android以外にも多くの脅威が存在します

なりすましメールで感染拡大、Emotetウイルスの脅威

安藤 正芳＝日経 xTECH／日経SYSTEMS

日経 XTECH



2014年に世界的に大流行したウイルス「Emotet（エモテット）」が再び猛威を振っている。2019年11月1日には首都大学東京が「教員のPCがEmotetに感染し、1万8843件のメールが不正に流出した」と発表。11月25日には京都市観光協会が「職員のPCがウイルスに感染し、迷惑メールが送信された」と公表した。同協会によれば「調査中だが、感染したウイルスはEmotetだと認識している」という。

Emotetの流行を受け、JPCERTコーディネーションセンター（JPCERT/CC）は11月27日にWebサイト「CyberNewsFlash」で注意喚起を出した。JPCERT/CCの佐條研インシデントレスポンスグループセキュリティアナリスト／マルウェアアナリストは「2019年10月からEmotetの感染報告や相談が相次ぎ、11月末の時点で数十件寄せられている」と話す。同氏によれば「ここまで相談が寄せられたウイルスは珍しい」といい、さらなる感染拡大に警鐘を鳴らす。

知人から（正規ルートから）
攻撃メールが届く

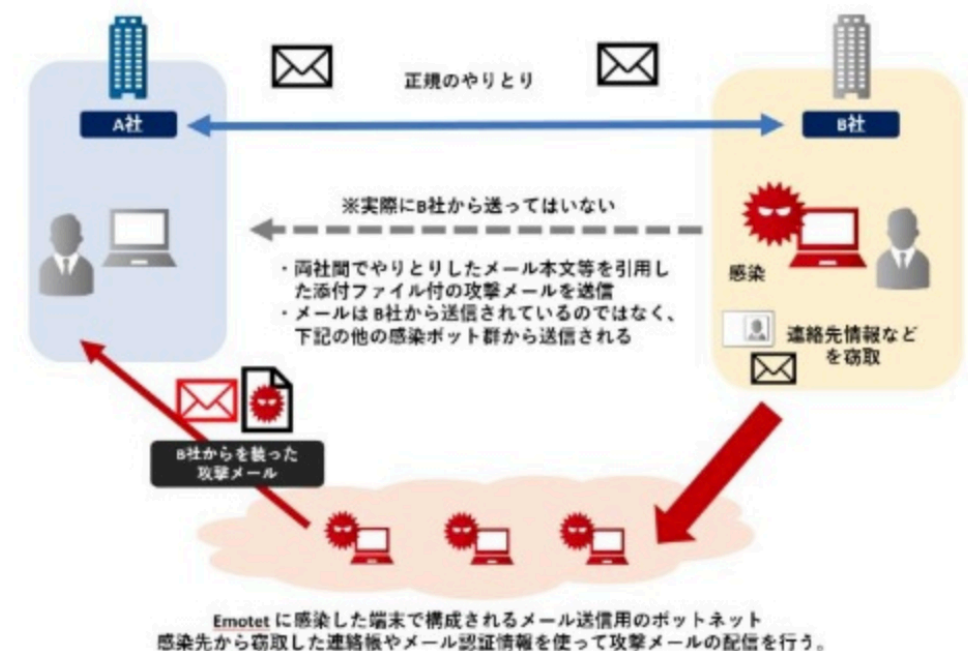
日本の被害が非常に多く、他大学や
関係する企業から返信メールの形で
大学に対する多くの攻撃が発生

2014年当時から進化

Emotetが最初に流行したのは2014年。当時のEmotetは感染者のPCにキーロガーなどを仕込み、ネットバンキングの情報を抜き取るバンキングマルウェアとして恐れられた。現在流行中のEmotetは海外でバンキングマルウェアやランサムウェアなどと一緒に配布され、攻撃対象を拡大している。Emotet自体はモジュール型のウイルスであり、モジュールの追加で様々な不正操作が可能だ。

現在日本で流行するEmotetは主にメールを介して感染範囲を広げている。Active Directoryやファイル共有サービス通じて社内PCが感染することもあるという。

Emotetに感染するとPCに保存されたパスワード、メール内容やメールアドレスが盗まれ、ネット上の指令サーバー（C&Cサーバー）に送られる。Emotetはこの情報を基に別の感染者から不正メールを送信させる。



* なりすましメールで感染拡大、Emotetウイルスの脅威

- <https://tech.nikkeibp.co.jp/atcl/nxt/cpbook/18/00038/00001/>

標的型攻撃に変化、狙いは経営幹部から役員秘書に

Symantecが取りまとめた2013年の脅威動向によると、標的型攻撃では従来と異なる特徴がみられるようになった。

印刷/PDF

ツイート 71

いいね! 97

m チェック

g+1 0

Pocket 11

大学教授を騙り、一部の
大学関係者にメール攻撃も

PR [セコム元会長が語る、東京五輪に向けた世界最高水準のIT社会](#)

標的型攻撃で狙われるのは大企業や幹部——従来にみられたこうした特徴に変化が生じているという。シマンテックが4月16日に公開した最新版のインターネットセキュリティ脅威レポートで明らかになった。

同レポートは2013年のセキュリティ脅威動向を取りまとめたもの。企業に関する注目点では大規模なデータ侵害事件が多発していることや、標的型攻撃の傾向に変化がみられていることなどを挙げている。

標的型攻撃ではメールを使った攻撃の発生件数が2012年比で91%増の779件に達した。一方、1つの攻撃キャンペーンに使われるメールの数や受信者の数は減少した。キャンペーンあたりの攻撃期間は2011年平均4日から2013年は同8.3日と、2倍以上に長期化している。このことから標的を絞り込んで執ように攻撃を展開する傾向が強まっている。

標的にされた企業規模別の割合は、従業員2501人以上の大企業で50%台から39%になった一方、2500人以下の中・小規模企業が半数以上を占めるようになった。

また、標的型攻撃メールを受け取るリスクが最も高いのは、役員秘書や広報関係者であることも分かった。従来は役員などの経営層や上級管理職を狙う傾向にあったものの、その周囲の関係者を標的にする傾向が強まっているという。

* 標的型攻撃に変化、狙いは経営幹部から役員秘書に

- <http://www.itmedia.co.jp/enterprise/articles/1404/17/news025.html>

あなたのメールも見られている？：

JALもだまされた こんなに怖い「ビジネスメール詐欺」

🕒 2018年01月10日 14時58分 公開

【濱口翔太郎, ITmedia】



「2017年は、セキュリティ上の欠陥が企業に深刻な影響を与えた1年だった」——トレンドマイクロ セキュリティエバンジェリストの岡本勝之氏はこう話す。中でも猛威を振るったのが、不審な業者が企業の取引先になりすまし、偽の送金指示や振込先の変更依頼などをメールで行う「ビジネスメール詐欺」（BEC、Business Email Compromise）だ。

日本でBECが広く知られる事になったJALの事例（2017年）

BECは海外で被害が広がっており、米連邦捜査局（FBI）によると13年10月～16年12月の被害総額は約53億米ドル（約5950億円）に上るという。17年は日本企業でも被害が本格化。12月には、取引先を装ったメールで旅客機のリース料などの振込先を変更するよう依頼された日本航空（JAL）が、偽の銀行口座に約3億8000万円を振り込み、だまし取られたニュースが世間を騒がせた。



JALの公式Webサイト

振り込み先の口座が凍結されていたため被害を免れたものの、航空事業者のスカイマークにも同様の詐欺メールが送られていたことが明らかになっている。

* JALもだまされた こんなに怖い「ビジネスメール詐欺」

- <<https://www.itmedia.co.jp/business/articles/1801/10/news097.html>>

ニュース

トヨタ紡織が欧州で最大40億円の詐欺被害、「虚偽の指示で資金流出」

玄 忠雄 = 日経 xTECH / 日経コンピュータ



2019年の事例
日系企業の海外子会社が
標的にされるケースが散見される



トヨタ紡織は2019年9月6日、ベルギーにある欧州子会社で最大40億円の詐欺被害が発生したと発表した。具体的な手口は捜査情報に関わるため非公表としているが、ビジネスメール詐欺（BEC）の可能性がある。

トヨタ紡織の発表によると事件は2019年8月14日に発生した。「悪意ある第三者による虚偽の指示に基づき資金を流出させた」といい、犯行グループはメールなどを使って取引先などを装った可能性がある。資金の流出後まもなく指示が虚偽であることに気付いたという。

同社は弁護士らによるチーム体制を組織し、現地の捜査機関に被害を申し入れた。現地での捜査に全面協力しており、流出した資金の保全・回収手続きに全力を尽くすとしている。

* トヨタ紡織が欧州で最大40億円の詐欺被害、「虚偽の指示で資金流出」
- <https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05922/>

bashの脆弱性を抱えるNASへの攻撃、日本や韓国が標的に

日本や韓国の大学や研究機関で使われているNASを狙った標的型攻撃が確認された。

[ITmedia]

印刷/PDF

ツイート 203

いいね! 128

チェック

g+1 2

Pocket

PR [歴史的な転換点 IoTとスマートデバイスが想像する未来の世界](#)
PR [【3,000円あたり】初心者でもわかる バックアップメルマガ](#)

身の回りの機器のアップデートが
出来ていますか？ PC/スマホ以外を
ちゃんとチェックしてますか？

LinuxなどUNIX系OSで使われているシェルの「bash」に極めて深刻な脆弱性が発覚した
問題で、セキュリティ企業の米FireEyeは現地時間の10月1日、日本や韓国、米国の
NAS（Network Attached Storage）システムを標的する攻撃を確認したと発表した。

この問題は「Shellshock」と呼ばれ、bashで特定の細工を施した環境変数进行处理する方法
に起因する脆弱性が複数存在する。脆弱性を悪用されると、アプリケーションの権限で任意
のOSコマンドが実行されてしまう恐れがある。一般的な設定でネットワークを介して容易に
悪用できるとされ、2014年4月に発覚したOpenSSLの脆弱性（Heartbleed）を超える危険
だとの指摘も聞かれる。

FireEyeが確認した攻撃では日本や韓国、米国の大学や研究機関で利用されているQNAP
Systems製のNASなどが標的になっているという。攻撃者はバックドア型のマルウェアを使
って標的のシステムからSSH鍵のファイルを盗み出すために、「/cgi-bin/authLogin.cgi」
の管理ログインページに攻撃を仕掛けて、脆弱性の悪用を試みているという。調査から少な
くとも2種類のマルウェアが韓国と米国のサーバにホストされていることも分かった。

* bashの脆弱性を抱えるNASへの攻撃、日本や韓国が標的に

- <http://www.itmedia.co.jp/enterprise/articles/1410/03/news109.html>

東海大にサイバー攻撃、臨時サイトに対応 学長「復旧1カ月以上も」

🔒 有料記事

上野創 2025年4月21日 17時30分



[list](#)

1



学校法人 東海大学（東京都 渋谷区）は、ネットワーク内のサーバーなどが不正アクセスを受け、ランサムウェアに感染したため、法人関連の全ての学校や病院などで、ネット接続を遮断したと発表した。外部からのメールが届かず、一部の授業が休講になるなどの影響が出ており、神奈川県 警が捜査している。大学は臨時サイトを設けて、学長名で「復旧には1カ月以上かかる可能性もある」と説明している。

法人広報によると、今月17日朝、大学関連の一部のサイトが表示されないことが分かり、前日夜にコンテンツファイルの 拡張子 が書き換えられていたことが判明したため、同日午後に法人全体のインターネット接続を遮断した。その後、大学内の複数のパソコンが、ランサムウェアに感染していることが分かったという。

同時期に複数キャンパスでの攻撃を観測しており、同時多発的に攻撃された可能性が考えられる。大学だけでなく病院にも影響が出ている。



[PR]

影響を受けているのは、湘南（神奈川県 平塚市）、伊勢原（神奈川県 伊勢原市）、品川（東京都）、静岡（静岡市 清水区）、熊本、阿蘇くまもと臨空（熊本県）、札幌の7キャンパス。講義全体の1割にあたるオンラインの講義は、一部を学外の会議システムや対面に切り替えて対応する。また、19日正午に臨時サイトを開設し、木村英樹学長による説明文などで学生、教職員らへ情報を提供している。

* 東海大にサイバー攻撃、臨時祭とで対応 学長「復旧1ヶ月以上も」

- <https://www.asahi.com/articles/AST4P2FKZT4PULOB00MM.html>

ネットワーク越しのフォルダも
全て暗号化されてしまう



過去には全学事務機能の
長期停止の事例も(海外)。

最近は標的型攻撃+ランサム

アサヒのシステム障害、混乱拡大「週明けにもスーパードライが消える」...共同配送の同業他社にも波及

2025/10/04 07:52

📌 保存して後で読む



水野友晴 石川泰平

アサヒグループホールディングス（GHD）のシステム障害で、社内外の混乱がさらに拡大している。受注・出荷業務の停止に伴い、取引先の飲食店や小売店ではビールなどの欠品が出始め、アサヒの業績に響きかねない状況だ。業務効率化に向けて社内システムの統合を急いできたことが裏目に出た格好といえる。（水野友晴、石川泰平）

他社銘柄で代替



「ブルヴァールトーキョー」で提供しているアサヒスーパードライ。来週には品切れになる可能性もあるという（3日、東京都中央区で）＝石川泰平撮影

障害発生から5日目となる今月3日、東京・日本橋のビアバー「ブルヴァールトーキョー」は、サッポロビールの黒ラベルなど他社銘柄での代替を検討し始めた。2019年の開業時から取り扱うビールはほぼ「アサヒー筋」だったが、店舗売上高の15%を占める主力の「アサヒスーパードライ」の在庫が来週にも尽きる見通しとなった。運営会社の代表取締役、佐藤裕介さん（46）は「この状況が続けば商売にならず、売り上げにも影響しかねない」と肩を落とす。

影響は同業他社にも波及し、麒麟ビール、サッポロも一部商品に配送の遅れが出ているという。都内の業務用酒卸売店「佐々木酒店」によると、アサヒを含めたこの3社は都内などで工場や倉庫から問屋に運ぶ際、同じトラックに載せる共同配送を行っており、アサヒの出荷遅延が影響している模様だ。佐々木実社長

ランサムウェア攻撃により、ERPが攻撃され、被害が拡大した可能性がある。

長期化するとシェア減少などの影響が考えられる。

2022.03トヨタの国内全14工場の停止（取引先の小島プレスへのランサムウェア攻撃）など、どの会社が攻撃を受けても大きな被害に繋がる可能性がある。

* アサヒのシステム障害、混乱拡大「週明けにもスーパードライが消える」

- <https://www.yomiuri.co.jp/economy/20251003-0YT1T50181/>

サイバー攻撃から3週間 大阪の病院 外来など多くの診療停止

11月21日 18時05分



大阪市にある大阪急性期・総合医療センターが「ランサムウェア」と呼ばれるウイルスによるサイバー攻撃を受けてから3週間がたちました。

病院では救急患者の受け入れを一部再開しましたが、外来など多くの診療は停止したままでシステムの復旧を急いでいます。

ランサムウェアにより病院業務の大半が数週間停止。復旧までには2ヶ月以上を要した案件。

通常の業務継続が行えず病院としての機能が失われてしまった事案

大阪・住吉区の大阪急性期・総合医療センターは、先月（10月）31日に「ランサムウェア」とよばれる身代金要求型のウイルスによるサイバー攻撃を受けて電子カルテなどのシステムに障害が発生しました。

今月（11月）17日からはバックアップとして保管されているデータを使って院内におよそ2300台ある電子カルテの端末のうち21台が利用できるようになったため、救急患者の受け入れを一部再開しました。

さらに、一部の外来診療や手術については紙のカルテを作成して対応を行っていて、21日も病院の職員が訪れた患者に整理券を手渡し、外来の窓口へ案内していました。

一方、新規の患者の受け入れなど診療の多くは停止したままで、病院では警察や情報セキュリティの専門家などの協力を得て、来年（令和5年）1月上旬に全面復旧できるよう作業を進めています。

つるぎ町半田病院に対するランサムウェア攻撃(2021.10)においても2ヶ月程度病院の通常業務が行えない状況が発生した。

BCP対策の手順に沿ってトップがインシデントを主導した事が被害の拡大を抑えた

* サイバー攻撃から3週間 大阪の病院 外来など多くの診療停止

- <https://www3.nhk.or.jp/kansai-news/20221121/2000068429.html>

電子チケット販売「Peatix」に不正アクセス 最大677万件の個人情報流出

🕒 2020年11月18日 10時22分 公開

[岡田有花, ITmedia]



印刷



309



Share



20



PR [ニューノーマルに必須 コミュニケーション活性化のカギとは](#)

日系ベンチャーの米Peatixは11月17日、電子チケット販売プラットフォーム「Peatix」（ピーティックス）が10月に不正アクセスを受け、ユーザーの氏名やメールアドレス、暗号化されたパスワード最大677万件が引き出されていたと発表した。被害拡大を防ぐため11月15日から、全ユーザーに対して、パスワード再設定を依頼している。

同サービスは、一部の自治体でプレミアム商品券の販売にも使われており、波紋が広がりそうだ。



Peatixのイメージ（公式サイトより）

Peatixは、個人や企業、自治体のイベントなどで広く利用されているプラットフォーム。流出したとみられるデータが、ハッキングフォーラム上に出回っているという情報もある。

不正アクセスは10月16日から17日にかけて発生。ユーザーの氏名やメールアドレス、暗号化されたパスワードが引き出されたことを確認した。

* 電子チケット販売「Peatix」に不正アクセス 最大677万件の個人情報流出

- <https://www.itmedia.co.jp/news/articles/2011/18/news066.html>

Adobe, Yahoo!等々大手だけでなく、
学会用のWEBサイト等からも
アカウント情報は大量に流出している。
→パスワード使い回しはあり得ない

典型的な不正アクセス

1. google検索、OSINTツールでIDとなるメールアドレスを自動的に収集
2. パスワード辞書、流出しているアカウント情報を基に1. と組み合わせて順番にログインを試行する

マイクロソフトのサポートを装った詐欺にご注意ください

2021年1月29日 | Japan News Center

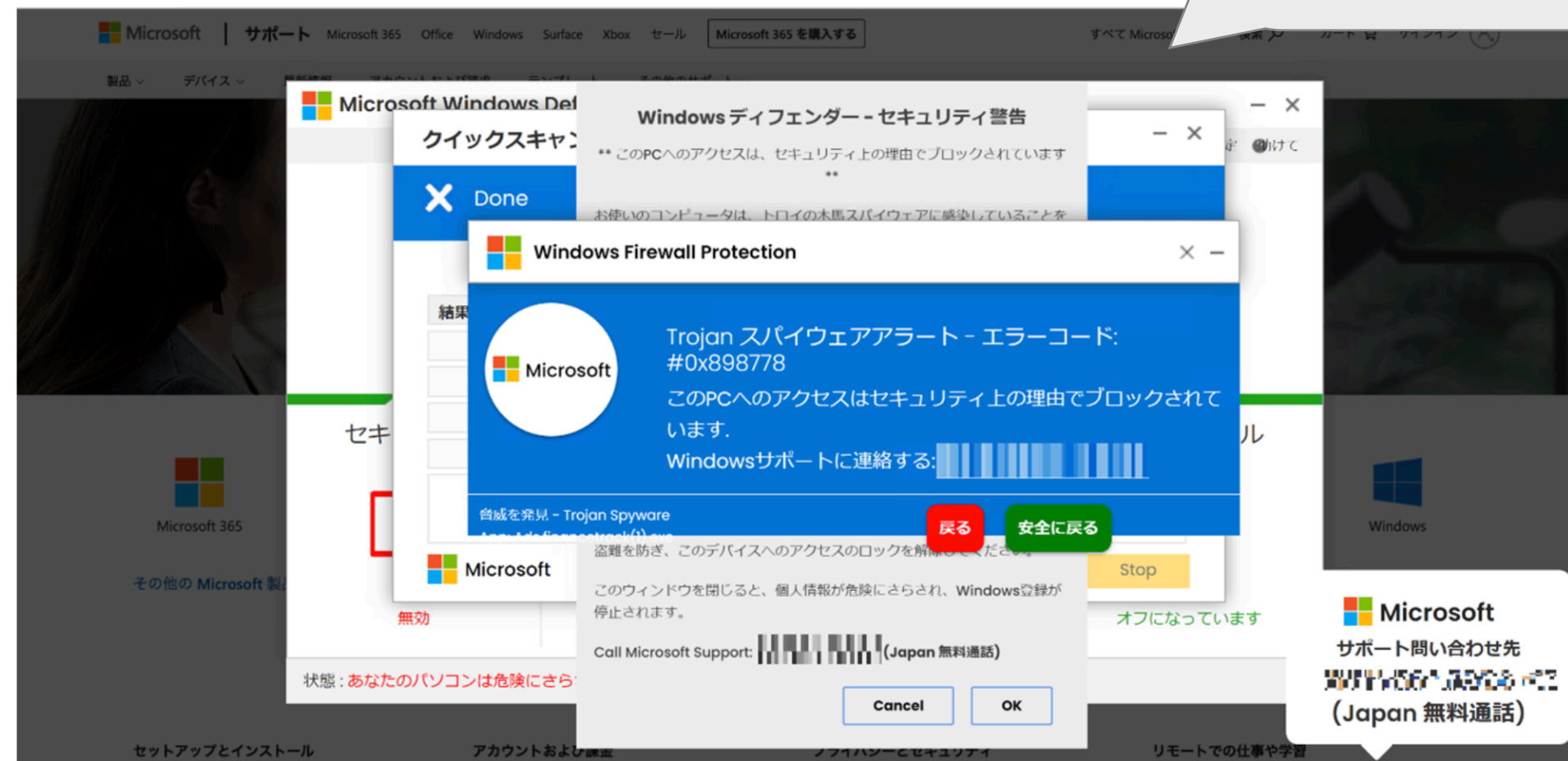
<偽警告画面の内容の例>

『この PC へのアクセスはブロックされました』
『このウィンドウを閉じると、個人情報に危険にさらされ Windows 登録が停止されます』
『この重要な警告を無視しないでください』
『Trojan スパイウェアアラート - エラーコード: #0x898778』
※こちらはあくまで一例です。類似した内容で表示される場合があります。

<偽警告画面の例>

画面を覆い尽くす様にして操作を奪い、
過剰なメッセージや音などで不安を煽って
偽のサポートに繋ぎ金銭を要求する詐欺。

サポートのためにリモートアクセス可能な
ツールをインストールする様に促す事も



※こちらはあくまで一例です。類似した内容や別の電話番号が表示される場合があります。

* マイクロソフトのサポートを装った詐欺にご注意ください

- <<https://news.microsoft.com/ja-jp/2021/01/29/210129-information/>>

DMMビットコイン流出は「北朝鮮の攻撃」 SNSで接触、日米特定

🔒 有料記事

編集委員・吉田伸八 2024年12月24日 7時00分



✉️ f X B! ...
[list](#) 30



警察庁が入る庁舎=2024年9月2日午後1時17分、東京都千代田区、板倉大地撮影



NVIDIA H100 NVL

好評発売中!



大規模言語モデルや生成 AI を加速

JCS
Japan Computing Systems

 **NVIDIA**

詳細はこちら

[PR]

暗号資産交換業DMM ビットコイン（東京）から今年5月、約482億円相当のビットコインが流出した事件について、警察庁と米連邦捜査局（FBI）は日本時間24日、北朝鮮の軍傘下の組織による窃取と特定したと発表した。日米が連携した捜査の結果から判明したという。

ヘッドハンティングを装った SNS でのやりとりをきっかけにシステムに侵入されたといい、警察庁と内閣サイバーセキュリティセンター（NISC）などはこうした手口への注意を呼びかけた。今回の公表は、サイバー攻撃の攻撃者や背景の国家を特定し非難する「パブリック・アトリビューション」にあたる。

DMMビットコインはネット関連会社DMM.comのグループ企業。警察庁によると、同社から窃取したのは、北朝鮮軍の対外工作機関「偵察総局」と関連する「トレーダー・トレイター」と呼ばれるグループという。日本などへのサイバー攻撃に関わってきたとされる「ラザルス」と呼ばれるグループの一部とみられる。

LinkedIn経由のヘッドハンティングを装い接触
→URLを踏ませて感染

* DMMビットコイン流出は「北朝鮮の攻撃」 SNSで接触、日米特定

- <https://www.asahi.com/articles/ASSDR44R6SDRUEFT00RM.html>

レコード件数別の損失推定額範囲

レコード件数	予測 (下限)	平均 (下限)	推定	平均 (上限)	予測 (上限)
100	\$1,170	\$18,120	\$25,450	\$35,730	\$555,660
1,000	\$3,110	\$52,260	\$67,480	\$87,140	\$1,461,730
10,000	\$8,280	\$143,360	\$178,960	\$223,400	\$3,866,400
100,000	\$21,900	\$366,500	\$474,600	\$614,600	\$10,283,200
1,000,000	\$57,600	\$892,400	\$1,258,670	\$1,775,350	\$27,500,090
10,000,000	\$150,700	\$2,125,900	\$3,338,020	\$5,241,300	\$73,943,950
100,000,000	\$392,000	\$5,016,200	\$8,852,540	\$15,622,700	\$199,895,100

情報漏洩 1,000件 : 1012万円 (= \$67,480 * 150円/\$)
 情報漏洩 10,000件 : 2684万円 (= \$178,960 * 150円/\$)
 情報漏洩 100,000件 : 7119万円 (= \$474,600 * 150円/\$)
 情報漏洩 1,000,000件 : 1.88億円 (= \$1,258,670 * 150円/\$)

* Verizon 2015年度 データ漏洩/侵害調査報告書 (p.30 図23. レコード件数別の推定損失額範囲)

- <https://www.verizonenterprise.com/jp/DBIR/2015/>

stuxnetとは？

どうやってイランの核施設に大きな被害を与えたでしょうか

stuxnet targeted Iran's nuclear facilities

- Features

- only target specific system (PLC of Siemens SIMATIC WinCC)
- ability to tamper with monitor screens and warning signs
- uses zero day vulnerabilities
- update via C2 or P2P communication
- worm virus (replicates itself and conceal its existence)

- Damage (Nov. 2010)

- 8,400 centrifuges stopped
- 1,000 centrifuges were broken
- suspension of uranium enrichment

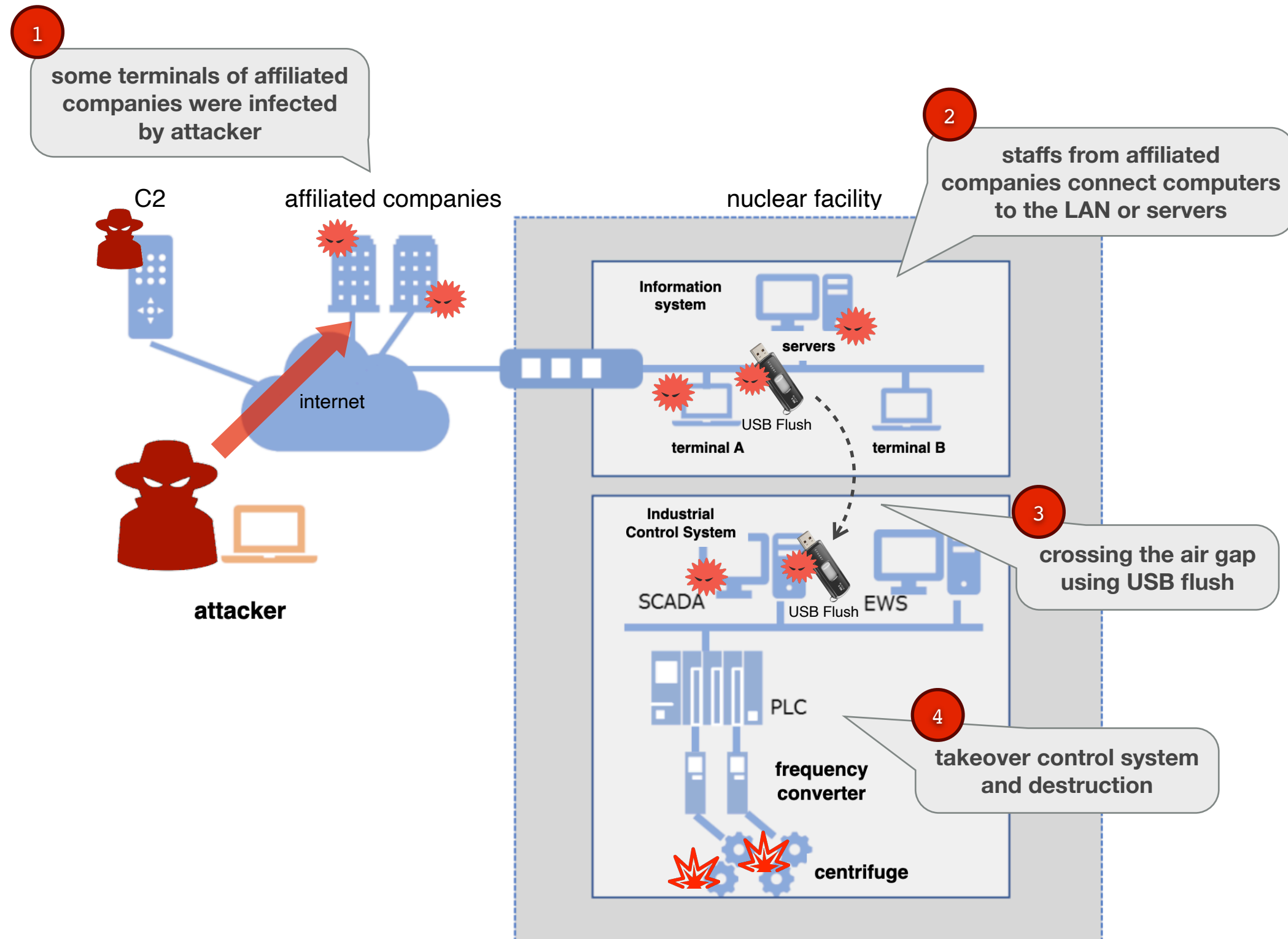
The centrifuge is an essential machine for uranium enrichment activities



Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008.

OFFICE OF THE PRESIDENCY OF THE ISLAMIC REPUBLIC OF IRAN

stuxnet: infection process



source: IPA <https://www.ipa.go.jp/files/000080701.pdf>

PLC : Programmable Logic Controller
EWS : Engineering Work Station
SCADA: Supervisory Control and Data Acquisition

イラン、原子力施設に被害 「サイバーテロ」と批判

改良型遠心分離機の稼働直後

中東・アフリカ

+ フォローする

2021年4月11日 17:19 (2021年4月12日 0:40更新)

📌 保存

🖨️ ✉️ 📄 🐦 📘 📶



イランが19年に公開したナタンズの原子力施設にある遠心分離機「IR6」=AP

【ドバイ=岐部秀光】イラン原子力庁のサレヒ長官は11日、中部ナタンズの原子力施設へのサイバー攻撃があり配電網への被害があったと発表した。サレヒ氏は「テロ行為」と批判し、国際原子力機関（IAEA）など国際社会に対応を求めた。ナタンズの施設でイランは10日に改良型遠心分離機「IR6」を稼働させたばかりだった。

ナタンズでは2020年夏にも不可解な爆発があり、イラン当局者は「破壊活動」によるものとの見方を示唆していた。ナタンズの施設は過去にイスラエル、米国によるとされるサイバー攻撃の標的ともなった。

* イラン、原子力施設に被害「サイバーテロ」と批判 -改良型遠心分離機の稼働直後-

- <<https://www.nikkei.com/article/DGXZQ0GR111R20R10C21A4000000/>>

ドイツの製鉄所がハッキング攻撃で操業停止、ドイツ連邦電子情報保安局が報告書を公開

Posted 1 years 3 months ago, by Daniel Rose

ハッカーグループがドイツの製鉄所に対して、電子メールに添付したマルウェアを使って、ネットワークにアクセスするためのユーザーIDとパスワードを入力させた上で、そのアカウントを使って内部システムにアクセスし、操業を停止させていたことがBundesamt für Sicherheit in der Informationstechnik（ドイツ連邦電子情報保安局）が公開した2014年版サイバー犯罪白書によって明らかとなった。

BSIでは、この製鉄所は、操業をシャットダウンさせられたことから、生産設備が損傷する大きな被害を受けたとしている。

これまで大規模な工場や発電所といった施設がハッキング攻撃を受けるということが可能性としては指摘されてきたが、欧米にある施設が実際にハッキング攻撃を受けて、施設が損傷する被害が生じていたことが明らかとなったのは今回のBSIによる報告書による記述が初のものとなる。

BSIでは、具体的にどこの製鉄所がこのハッキング攻撃を受けて、操業停止の状態に追い込まれたかなど、ハッキング攻撃の詳細については明らかにしていない。

過去においては、Stuxnetと呼ばれるウィルスを使ったハッキング攻撃により、イランにあるウラン濃縮工場の生産が操業停止に追い込まれるという事件も起きていた。その後のNew York Timesの報道によりこのハッキング攻撃は米国とイスラエルの情報機関による「Operation Olympic Games」という作戦名で行われたものである可能性が指摘されていた。

* ドイツの製鉄所がハッキング攻撃で操業停止、ドイツ連邦電子情報保安局が報告書を公開

- <<http://www.businessnewsline.com/news/201412230814210000.html>>

ウクライナの「ハッキングによる大規模停電」で強まる、サイバー戦争への懸念

ウクライナで、変電所に対するハッキング攻撃が行われ、多くの住民が電気のない生活を強いられた。ドイツでも2014年、製鋼所へのハッキング攻撃で溶鉱炉のひとつが甚大な被害を受ける事件が発生している。

PHOTOGRAPH BY WIKIMEDIA COMMONS

TEXT BY MATT BURGESS

TRANSLATION BY MAYUMI HIRAI/GALILEO

WIRED NEWS (UK)

「サイバー戦争」への懸念を象徴するかのような事件だ。ウクライナでハッカーが変電所を攻撃し、140万人ともされる多くの住民が電気のない生活を強いられた。

ウクライナの停電は、地元の情報筋が2015年12月23日（現地時間）に初めて伝えたもので、地域のコントロールセンターがオフラインになった。マルウェアが原因とされ、ウクライナ保安庁はただちにロシアからの攻撃だと非難した。

停電を起こすために使われたのは、2007年にサーヴィス拒否（DDoS）攻撃を生み出すツールとして登場し、その後高度なマルウェアに進化した「BlackEnergy Trojan」だと報道されている。

* ウクライナに「ハッキングによる大規模停電」で強まる、サイバー戦争への懸念

- <<http://wired.jp/2016/01/07/cyberattack-power-electricity/>>

DXとセキュリティの関係@科学大

DX = 料理



食材



料理



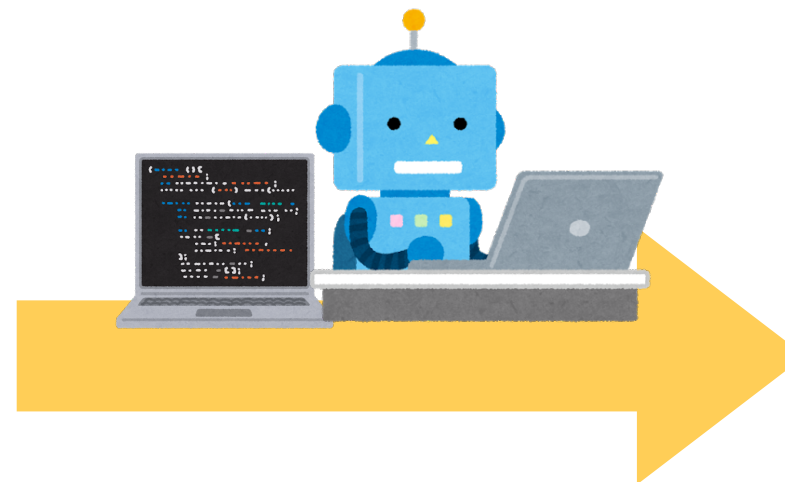
食事

シェフの視点を
構成員全員が持てる様に！



D

Data



X

Transformation

DXの成果

夕食はカレーにしよう！
→レシピをWEB検索→食材をスーパーで調達
同じ事を大学DXで出来る様にしたい！

必須の3要素！ どれが欠けてもDXは成り立たない！ 文化形成がキモ！！

シェフの観点：プログラマーの三大美德を再考する

1. 怠慢(Laziness)、2. 短気(Impatience)、3. 傲慢(Hubris)

【1. 怠慢】

全体の労力を減らすために手間を惜しまない気質。この気質の持ち主は、役立つプログラムを書いてみんなの苦労を減らしたり、同じ質問に何度も答えなくてもいいように文書を書いたりする。よって、プログラマーの第一の美德である。

小飼弾 訳

1. LAZINESS

The quality that makes you go to great effort to reduce overall energy expenditure. It makes you write labor-saving programs that other people will find useful, and document what you wrote so you don't have to answer so many questions about it. Hence, the first great virtue of a programmer. (Larry Wall)



これまで、プログラマーだけがやりたい仕事をコンピュータに行わせる事が出来た。ノーコード、ローコード、RPA、ワークフローツール等々の充実によって、誰でも自分の力でコンピュータに仕事を行わせる事が出来る時代に！！

プログラマーの美德が → 職業人の美德に

DX推進のポイント

- 透明性あるデータ共有、オープンなコミュニケーション
- コミュニケーションとデータの分離（業務に基づくデータ管理）
- 認証メンバー同士での安全性の高いデータ共有・コミュニケーション
- 個別システム中心の考え方からデータ中心へ

認証基盤が支える情報セキュリティ

- ・メールを中心にWEBなどインターネット全域と繋がるツールは危険が多過ぎる（事件が絶えない）
ーそもそもグローバルに繋がる必要があるか？（特定の研究教育機関、企業等と繋がりたい）
 - ・HTTPSに代表される様に暗号化通信の割合が増加（幹線ネットワークの単純な監視はその内限界に）
 - ・大学の先生は自由（EDR+集中管理の様なセキュリティやネットワークのポリシーをかけにくい）
 - ・そもそもセキュリティ確保は組織のパフォーマンス向上のため（足かせでは無い）
- **みなが喜んで使いたくなるサービスが結果としてセキュリティ担保に繋がる様にしたい**

DX推進に欠かせないツール群は
認証基盤が基本必須



その他講義支援、教員評価などなど
様々な学内サービスが連携

東工大メンバー

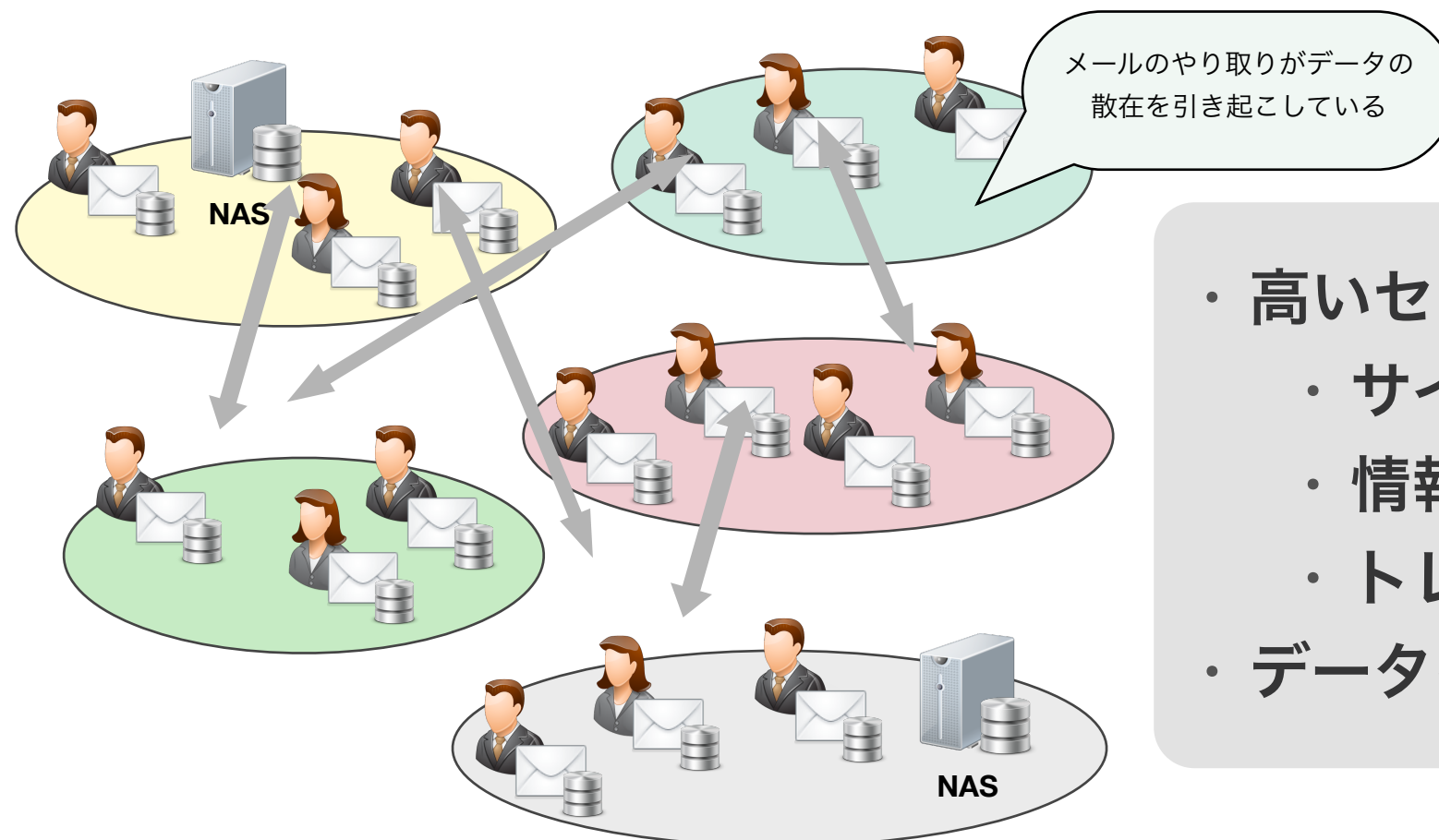
ポータルサイト経由（2要素認証）

東工大メンバー限定の環境

問題点：メール中心が引き起こすデータの散在

根本的な原因

- ・メール中心でメーラーがデータ保管庫と化し、データ散在に拍車がかかる
- ・業務フローに沿ってではなく、メールのやり取りに沿ってデータが付随
- ・コミュニケーションとデータが強く結合し、メールに引っ張られている



問題点

- ・ 高いセキュリティリスク
 - ・ サイバー攻撃に対して脆弱
 - ・ 情報漏洩が容易に発生
 - ・ トレーサビリティが無い
- ・ データを統合的に扱う事が不可能

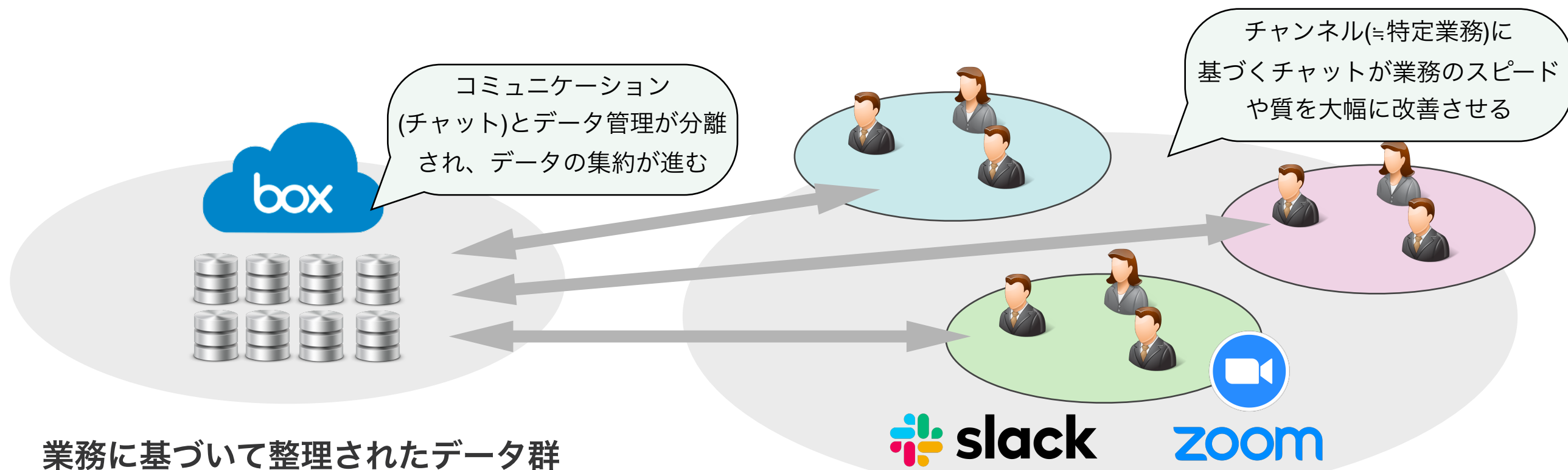
学長→全学、指導教員→学生など人間関係を悪用したメール攻撃なども多い（認証重要）
データ管理に関してはスーパーにほど遠い

メール(コミュニケーション)によるデータの散在

コミュニケーションとデータの分離

1. 散在しているデータを集約し、業務に応じた整理(保管)を行い、適切なアクセス制限を施す
2. 相手を確認できる(認証機能のある)コミュニケーションツールを導入する
 - 1.を利用して、コミュニケーションとデータを分ける（業務に応じてデータを保管する）

・データのコンテキストに応じて、フォルダ分けしデータを整理する



Box: 使い勝手を損なわないアクセス制限

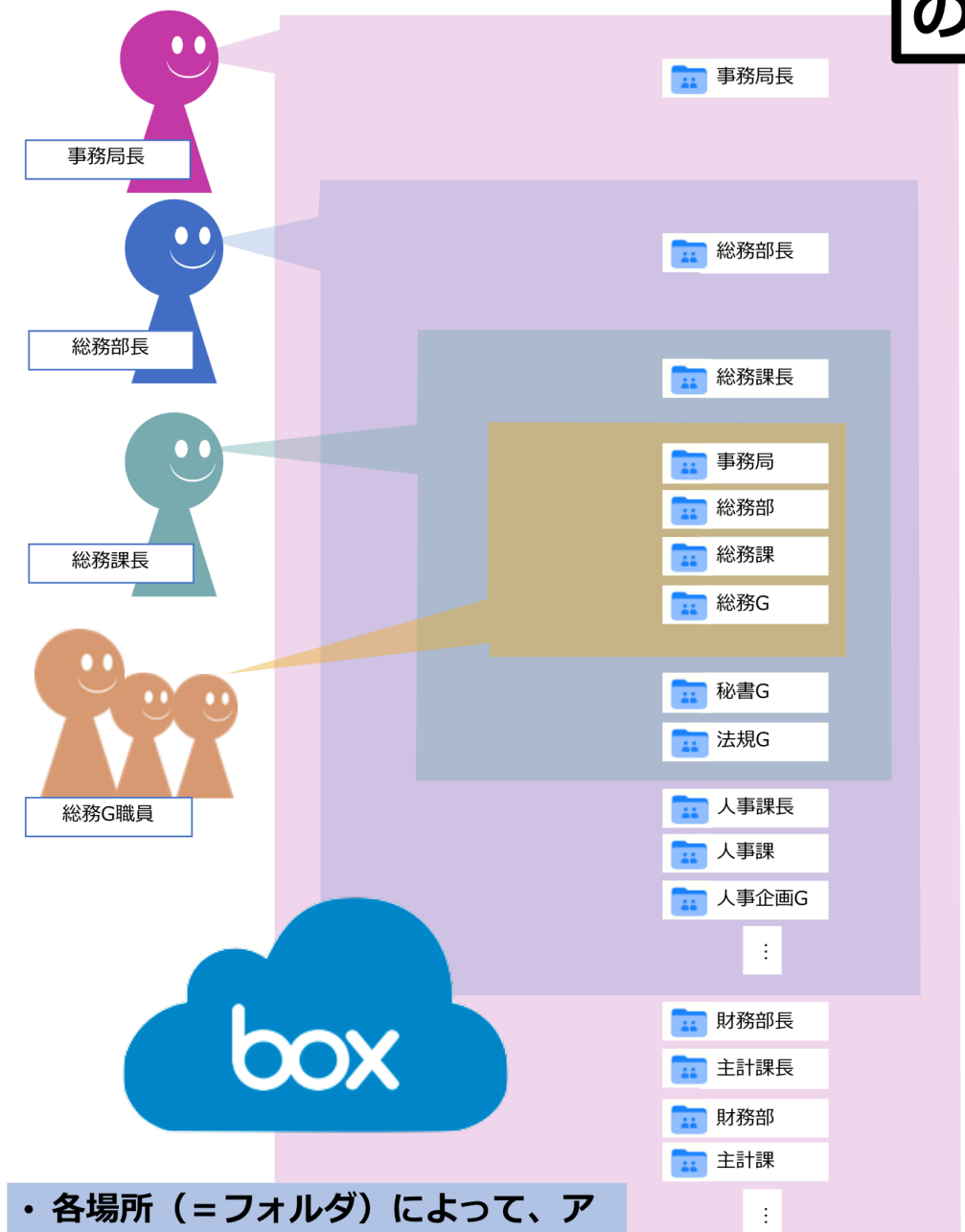
- 人事情報から組織に合わせて自動的に権限を付与
- ファイル作成時にアクセス制限が（意識せずに）自然に設定される

機密性3のレベルからスタート
- 厳しいが使い勝手は損なわれないアクセス制限から出発して、必要に応じて他部署にもフォルダやファイル毎にアクセス権限を加える
- 例：法規グループが "2022年度 / 学内規則"などのフォルダを作成するとグループ内メンバおよび上長のみがデータにアクセス可能。情報セキュリティ規則に関わる配下のフォルダのみをセキュリティ担当部署のメンバーを追加して共同編集可能し業務を進める

組織フォルダとコラボレーションの設定を事前に施し、自由に使いながらもリスクを低減させる

Boxのアクセス権限の考え方（表現その1）

事務局の場合



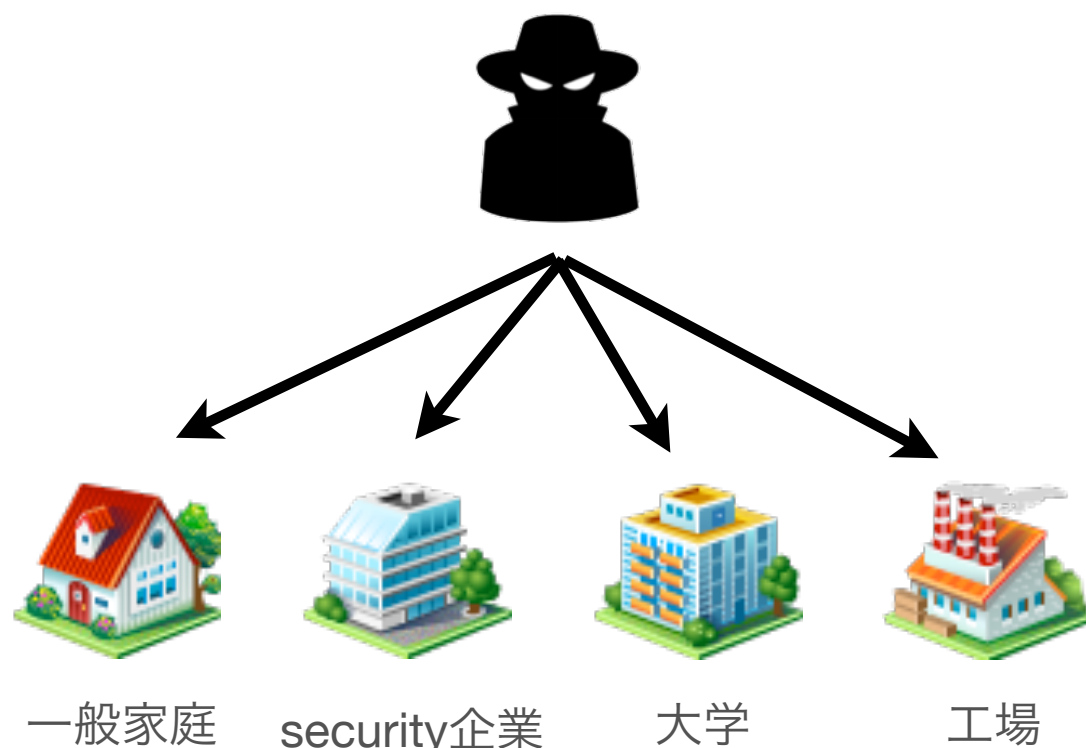
- 各場所（＝フォルダ）によって、アクセスできる人は異なる。
- 所属や役職によって、アクセスできる場所（フォルダ）は異なる

総務部職員からの見え方の例

セキュリティを取り巻く複雑さ困難さ

標的型攻撃攻撃

ワーム、ボット感染



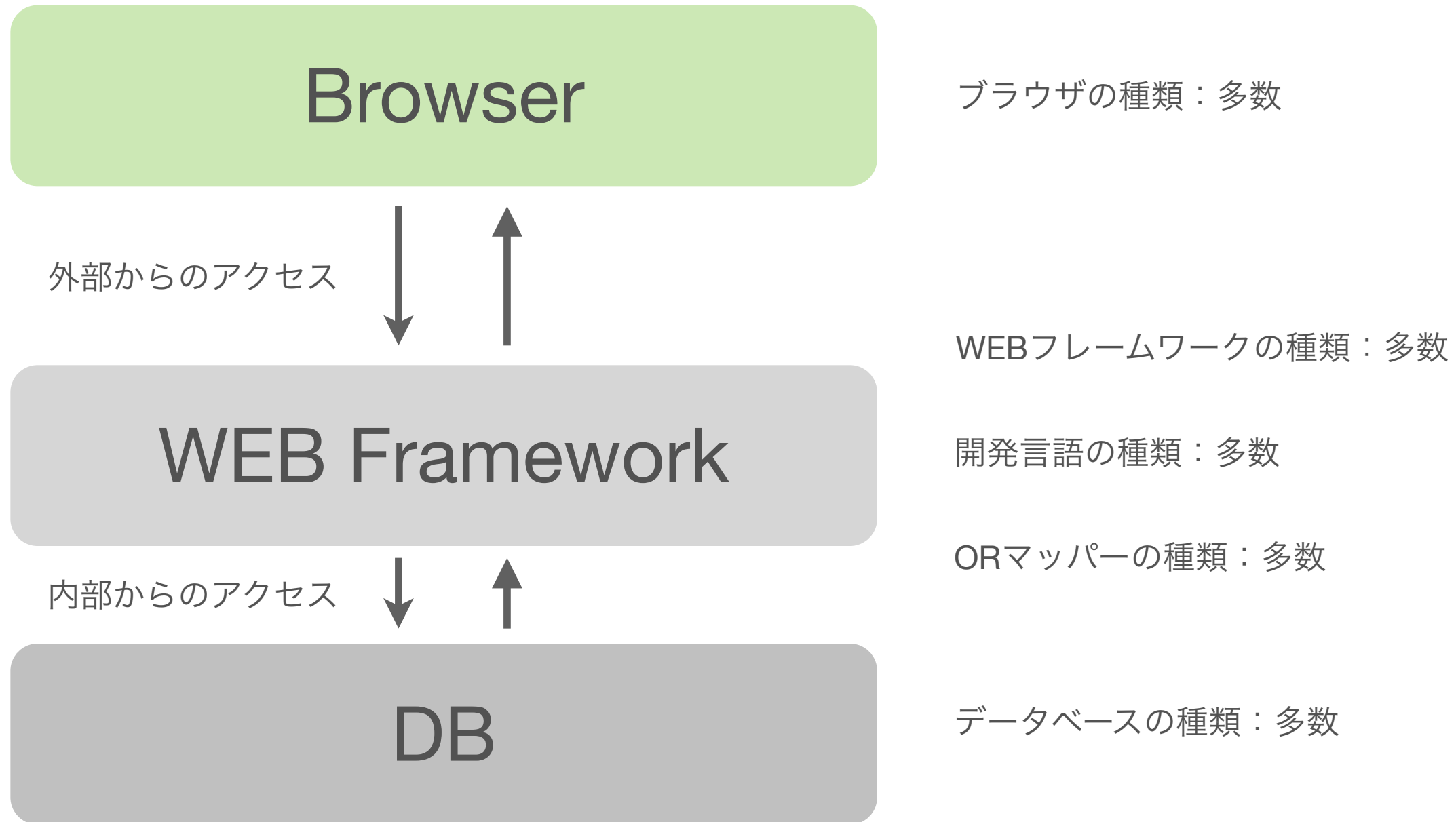
- ・ 広範囲に及ぶ攻撃
- みんなが同じ攻撃を受ける
- 特定機関による攻撃の分析
- 全体での対処法の共有

標的型攻撃



- ・ 個別の機関を狙った攻撃
- みんなが別の攻撃を受ける
- **自分自身で気付く**
- **自分自身で対処する**

複雑さの例：WEBセキュリティ

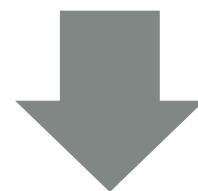
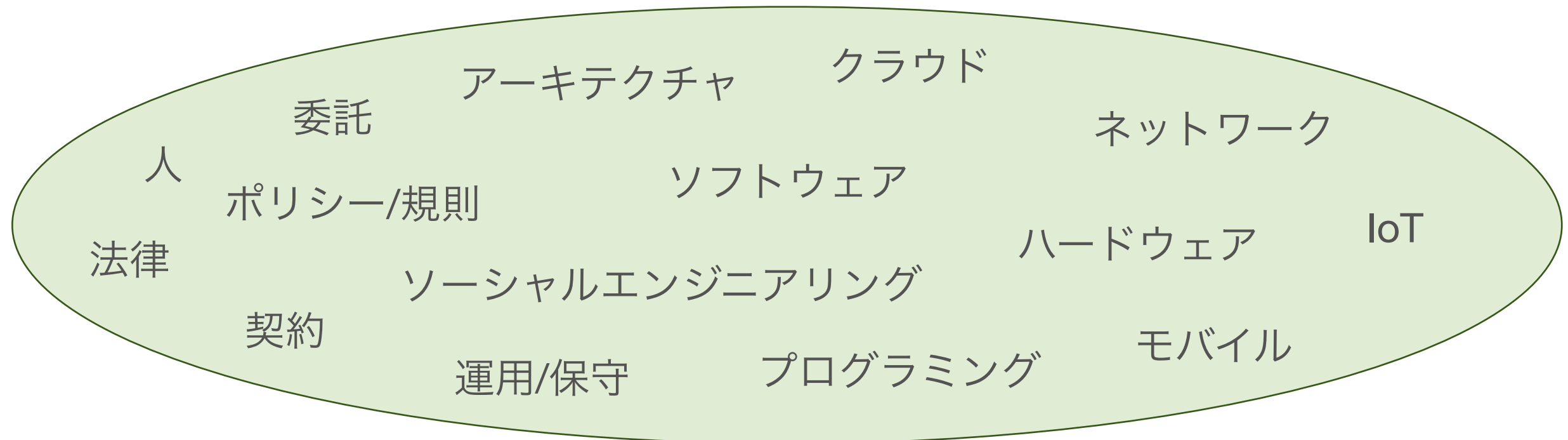


- ・ 内部 x 外部を繋ぐそもそもの困難さ
- ・ 多くのコンポーネント x 非常に種類の多いツール群



個別のケースを解決出来ても
他に応用が利かない

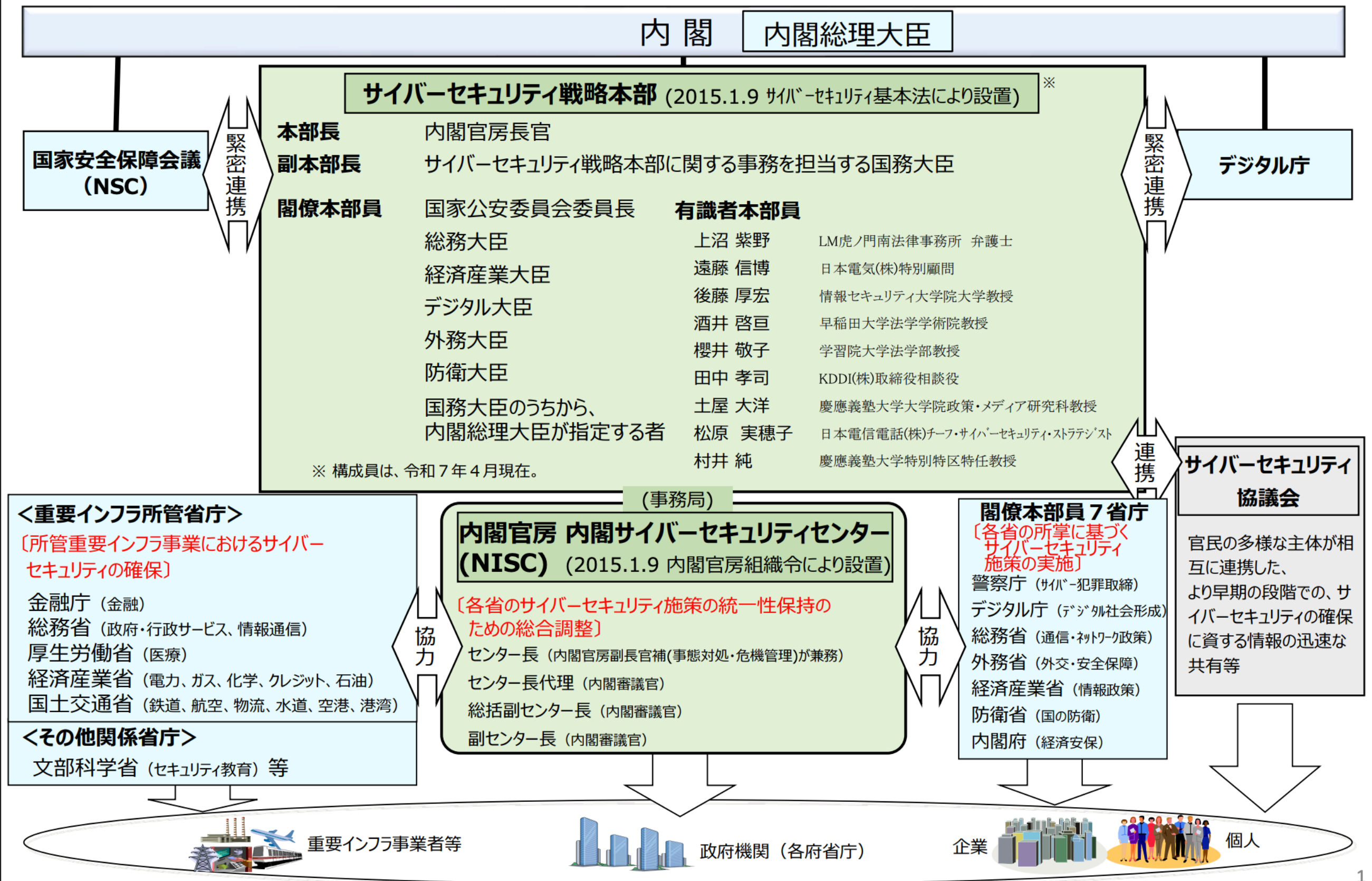
広範囲かつ複雑すぎるセキュリティの現状



どんな取り組みが必要だろうか？

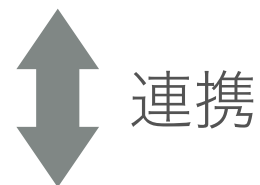
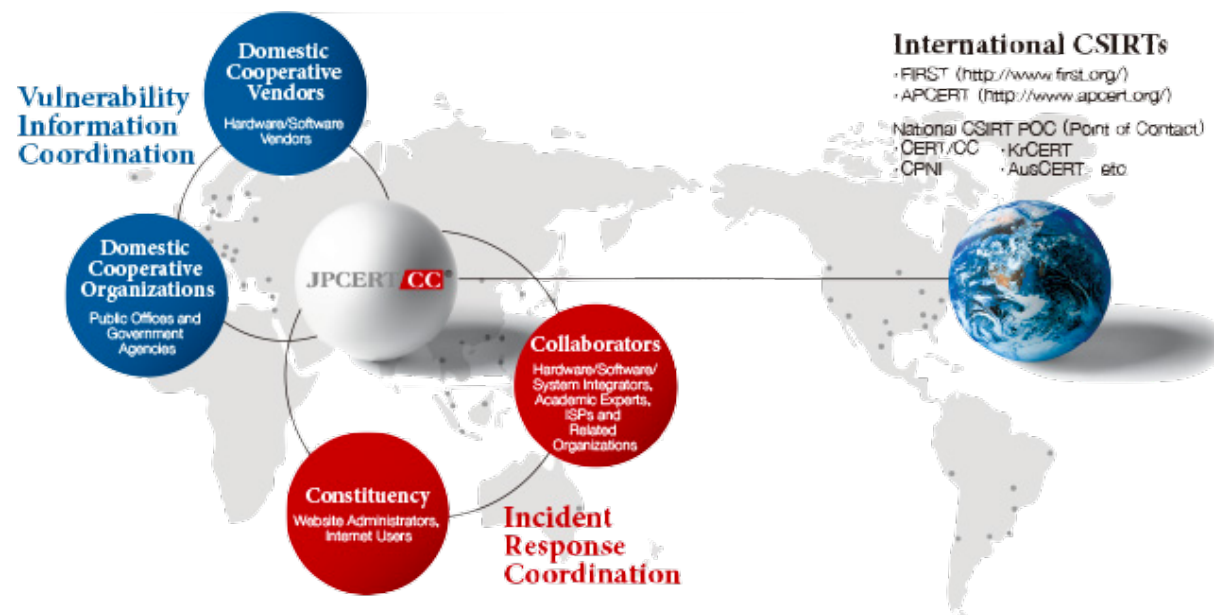
組織的・社会的な取り組み

サイバーセキュリティ政策の推進体制



出典: NISC 我が国のサイバーセキュリティ政策の概要
https://www.nisc.go.jp/pdf/about/nisc_gaiyou.pdf

JPCERTコーディネーションセンター



IPA 情報処理推進機構



- ・ インシデント対応の調整/取りまとめ
- ・ 脆弱性情報の調整/取りまとめ
- ・ 国際的なCSIRTとの協調

- ・ 種々の情報発信、啓蒙
- ・ 届け出、相談
- ・ JVN (脆弱性情報ポータル)

- ・ サイバー情報共有イニシアティブ(J-CSIP)
- ・ 情報処理技術者試験
- ・ セキュリティキャンプ / 未踏

啓発活動 (NISC/IPA)



CSF: Cyber Security Framework

- ・サイバーセキュリティ対策を改善するためのフレームワーク
- ・アメリカのNIST(National Institute of Standards and Technology)が発行
- ・重要インフラ向けに作成されたが、広範囲な業種で積極的に利用されている

表 1: 機能とカテゴリーの識別子

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション

2024.02.26にV2.0にバージョンアップされた。全工程にガバナンスの機能が追加され、サプライチェーンに対して重点が置かれるなど時代に即した更新が行われている

1. コア：機能(5) → カテゴリー(23) → サブカテゴリー(108)
2. ティア：4段階の成熟度 (Partial / Risk Informed / Repeatable / Adaptable)
3. プロファイル：セキュリティ対策のAs Is / To Be

CSFをどのように利用するかは組織に委ねられている。
CSFは指針や体制作りに向く → 具体的な手法や手順はNIST SP-800シリーズを参照するという補完関係にある。

人材育成の事例



出典: @IT <http://www.atmarkit.co.jp/ait/articles/1403/18/news005.html>

- ・ CTF (セキュリティコンテスト) - 人材発掘
例：SECCON (2020年大会 1000チーム)
産業界を中心とした産官学の取り組み



- ・ 大学におけるセキュリティ教育 - 新規の人材育成
例：IT-Keys, SecCap (4大学 20名/年→14大学 110名/年)
大学を中心とした産官学の取り組み

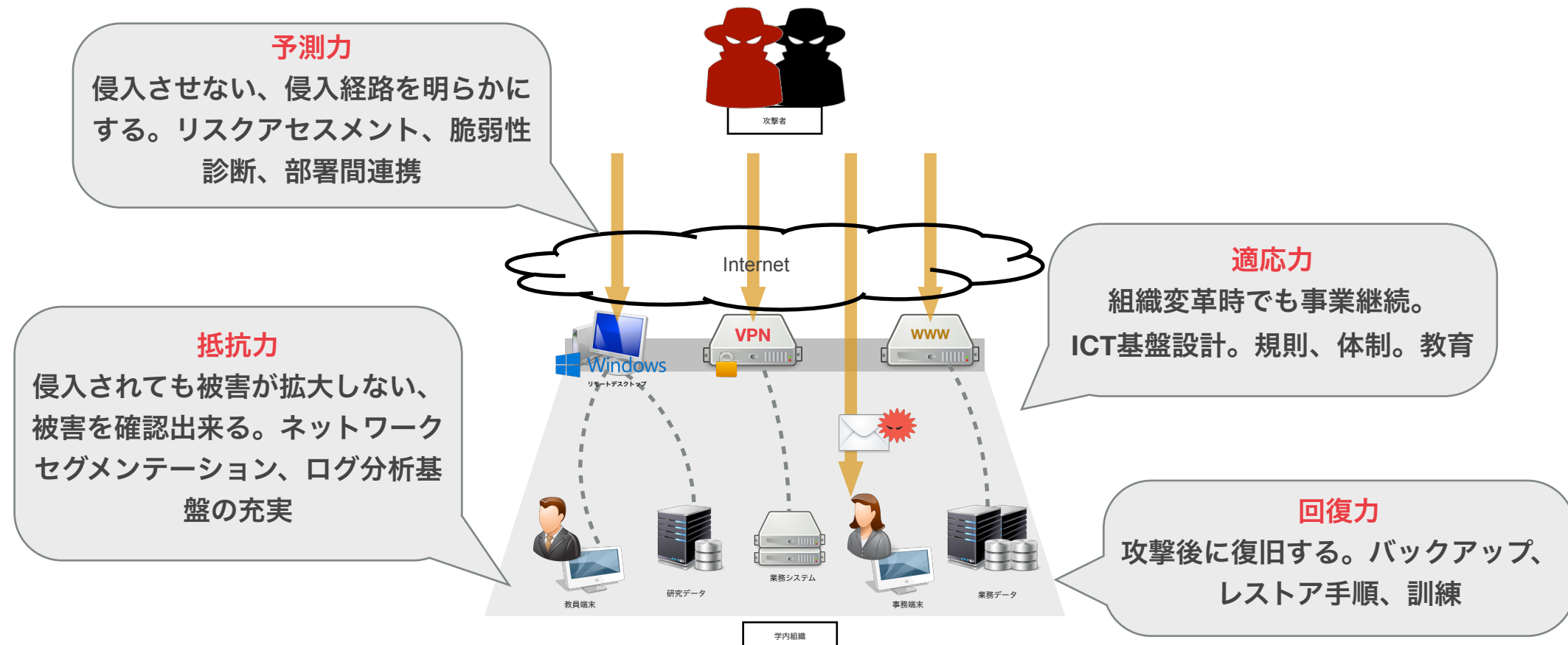


出典: IT pro <http://itpro.nikkeibp.co.jp/atcl/news/15/031801000/>

- ・ 官公庁/企業向けセキュリティ演習 - 現場の人材育成
例：CYDER (6回 200名/年)
省庁(総務省)を中心とした産官の取り組み

まとめ

サイバーレジリエンスを考慮した対策



悪条件、高ストレス下においても 組織本来の活動を継続出来る能力

Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

予測力 抵抗力 回復力 適応力



サイバーセキュリティ確保にむけて



出典: the-internet <https://visit4it.wordpress.com/internet/the-internet/>

・サイバーセキュリティ

規模：社会

対象：サイバー空間(インフラ+人)



どう守るか？

社会活動に関わるあらゆる分野に関連した対策

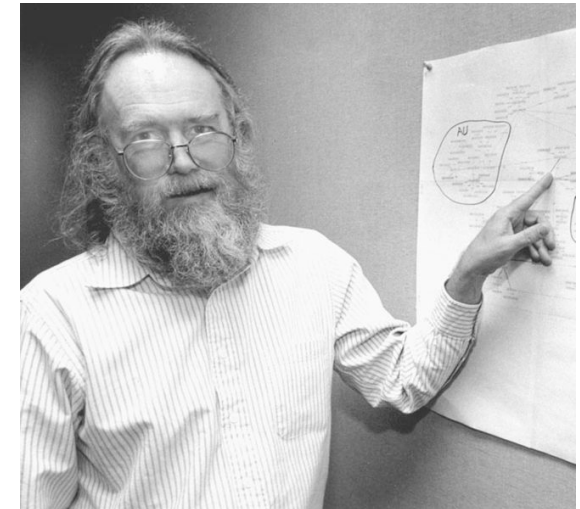
サイバーレジリエンスの考えを社会に広げて考える (技術、政策等々から社会活動を健全に継続させる)

- ・ 社会機能に焦点を当てる
- ・ 社会環境の変化を想定する
- ・ APT(標的型攻撃)の影響に焦点を当てる
- ・ 敵対者が社会インフラを侵害することを想定する
- ・ 敵対者が社会インフラ内部に存在し続けることを想定する

予備スライド

Internet culture

be conservative in what you do,
be liberal in what you accept from others



Jon Postel

We reject: kings, presidents and voting.
We believe in: rough consensus and running code.



David D. Clark

WWW → Google Search → AI(LLM)

- Internet: (自律分散)ネットワーク上での情報通信が可能に
- WWW: Internet上に散在するコンテンツを相互参照可能に
- Google Search: キーワードからコンテンツの所在地を参照可能に
 - Googleがインデックス情報を独占
- AI(LLM): 会話(質問)の続きを生成可能に
 - AI起業(OpenAIなど)が言葉のコンテキスト情報(AIモデル)を独占

