サイバー攻撃の最新動向から見る大学の新たなリスク

2018年8月23日

JPCERT/CC
早期警戒グループ 洞田慎一

目次

- はじめに
- インシデントとは
- 大学等で発生したインシデントを振り返る
- 大学等に求められる対策とインシデントへの備え
- まとめ

自己紹介

- 洞田 慎一
  - 2006-2015年 総合研究大学院大学 学術情報基盤センター
  - 2015年~ JPCERT コーディネーションセンター
- 外部委員等
  - 2016年 金融情報センター コンティジェンシープラン改訂に関する検討部会
  - 2017年 金融情報センター IT人材育成検討部会
  - 2017年 私立大学情報教育協会 情報セキュリティ対策問題小委員会
  - 2018年 日本学術振興会 契約等監視委員会
  - 2018年 国立大学法人 総合研究大学院大学 情報セキュリティアドバイザー
- 講演
  - 金融ISAC 名古屋ワークショップ 基調講演 “Open Source Intelligence のススメ”, 2018.
  - 民間放送連盟・放送セプター情報セキュリティ対策に関する説明会, “2017年度の放送におけるインシデントの振り返り”, 2018.
- 論文
  - S. Abe, Y. Tanaka, Y. Uchida, S. Horata, "Developing Deception Network System with Traceback Honeypot in ICS Network", SICE Journal of Control, Measurement, and System Integration, 2018.
  - 高等教育機関に対するサイバー攻撃の動向と情報セキュリティ対策の考え方, 大学と教育, 2018年3月号.

JPCERT/CC とは

- **一般社団法人 JPCERT コーディネーションセンター**
  Japan Computer Emergency Response Team / Coordination Center
  - https://www.jpcert.or.jp/
  - コンピュータセキュリティインシデントへの対応、
    国内外にセンサをおいたインターネット定点観測、
    ソフトウエアや情報システム・制御システム機器等の脆弱性への対応など
    我が国における「セキュリティ向上を推進する活動」を実施
  - **サービス対象:**
    日本国内のインターネット利用者やセキュリティ管理担当者ソフトウエア製品開発者等（主に、情報セキュリティ担当者）
  - インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**我が国の窓口となる「CSIRT」**
    ※各国に同様の窓口となる　CSIRTが存在する
    (例、米国のUS-CERT, CERT/CC, 中国のCNCERT, 韓国のKrCERT/CC)
- 経済産業省からの委託事業として、**サイバー攻撃等国際連携対応調整事業を実施**

「JPCERT/CCをご存知ですか？」

JPCERT/CCの活動

インシデント予防　インシデントの予測と捕捉　発生したインシデントへの対応

脆弱性情報ハンドリング

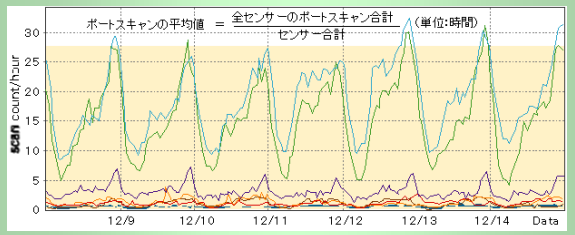
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

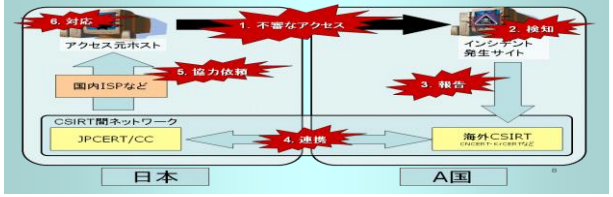
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応 *調整*支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

JPCERT/CCの活動全体像

世界各国144組織との連携
27か国の組織とMoU締結

世界的なCSIRTの集まりであるFISRTの理事を長年務める

高度なマルウェアの解析能力

重要インフラ／制御システムのセキュリティに関して2007年から取り組み

年間約4千件の脆弱性案件を調整し公表へ

年間1万件以上のインシデント情報に対応

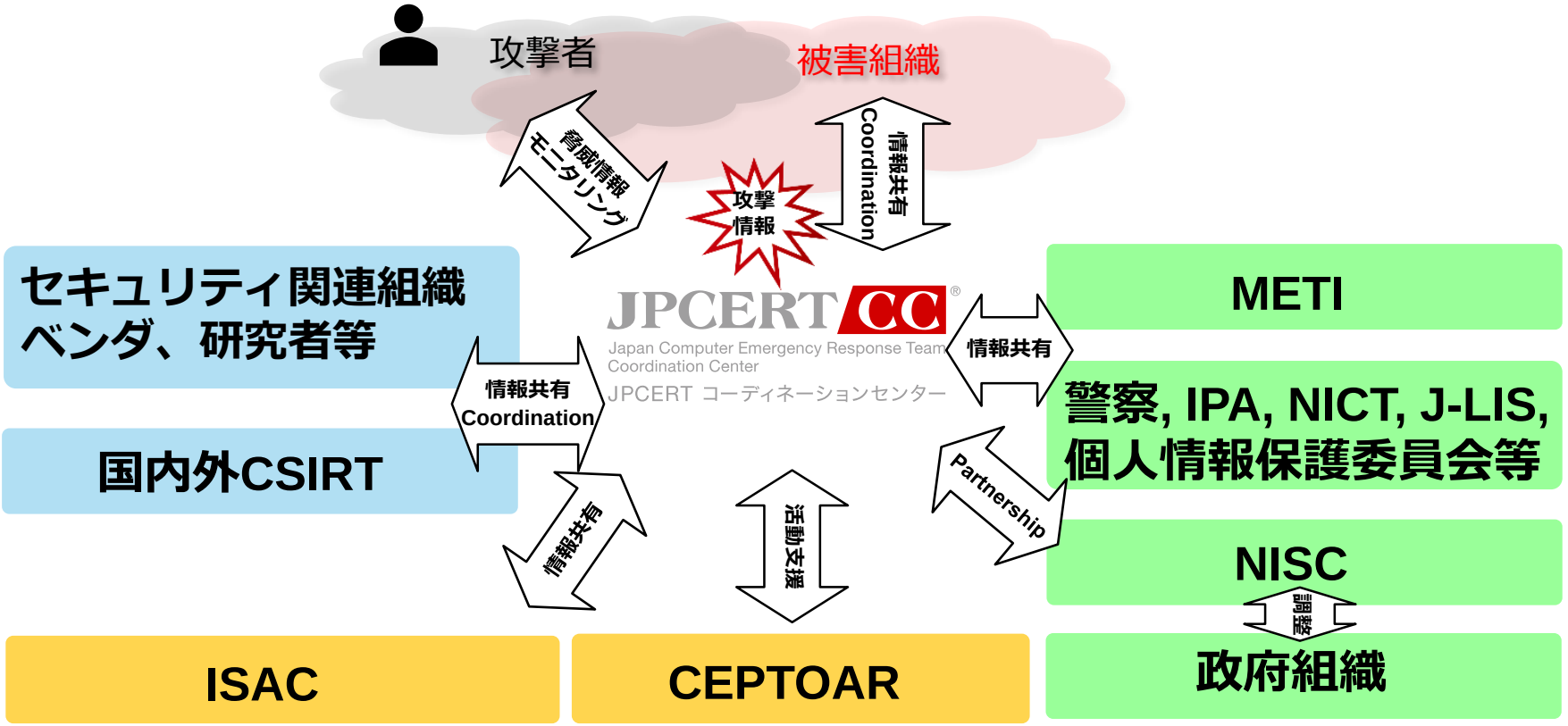
アジア各国間連携によるインターネット観測網

重要インフラによる情報共有体制（ISAC）等への活動支援
・セプターカウンシル（13インフラ分野）
・金融ISAC
・電力ISAC
・民放連　　等

政府機関、専門機関、重要インフラ、各種メーカー等との連絡・連携ネットワーク

コーディネーションセンターとしての役割

さまざまなパートナーとの調整



インシデントに関する調整 (coordination) 機関として、問題解決に向けて、必要な人に必要な情報を届ける業務を行っています

JPCERT/CCの活用

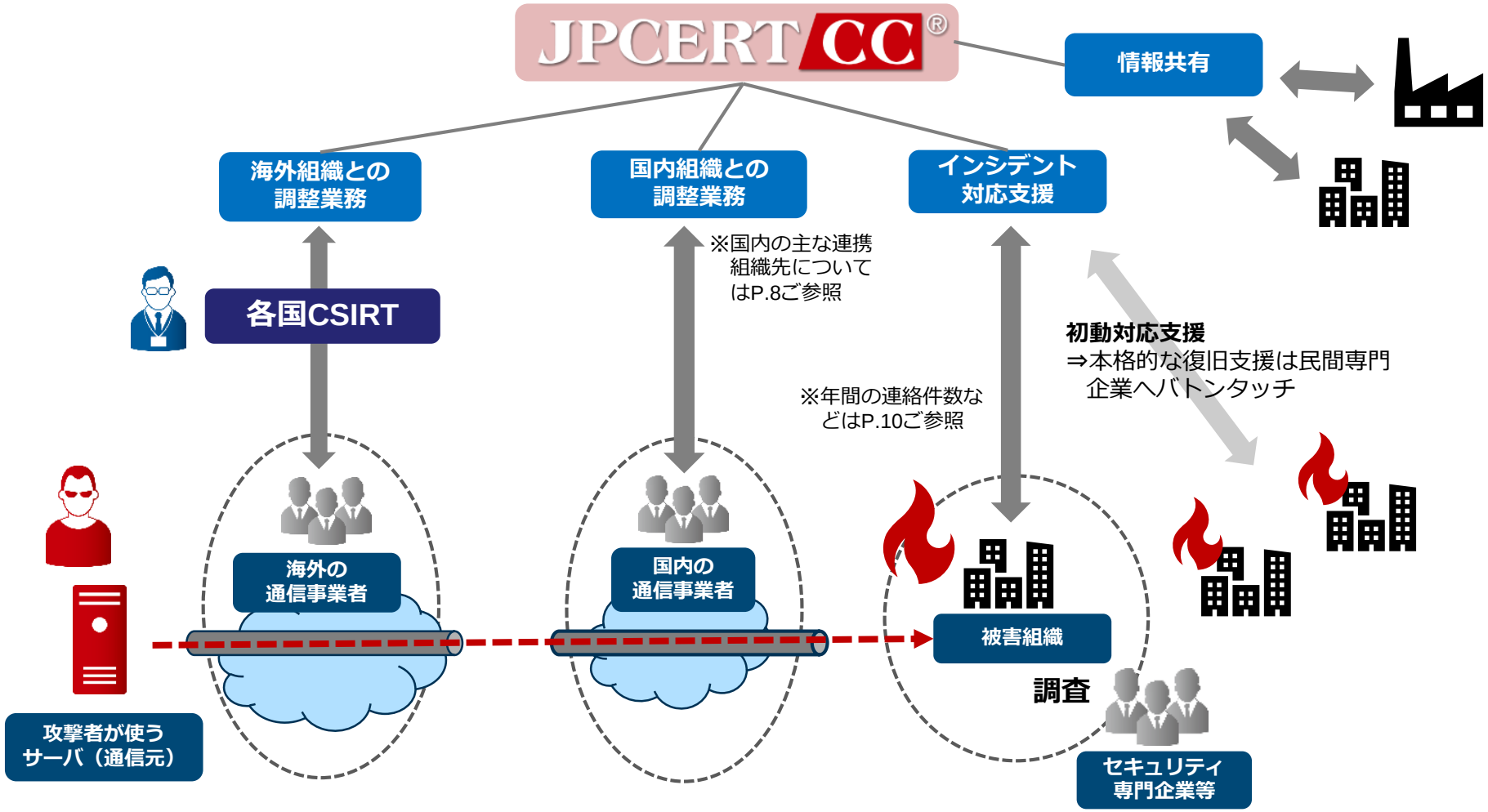
- **コーディネーションセンターの役割と活用**
  - インシデントレスポンス
  - 脆弱性・脅威情報に関する情報流通
    - 脆弱性情報 【JVN】
    - 脅威情報、注意喚起、早期警戒情報他
  - アーティファクト分析【検体解析など】
  - 国内外 のCSIRT 連携促進、コミュニティ推進

“インシデント”に沿った活動を展開しています

- **例えば、こんなときにお役立てください**
  - インシデントが発生し、初動対応での技術的な支援や情報が必要となるケース
  - 日々の対策を進める上で、脆弱性や脅威に関する情報が必要となるケース
  - その他、よろずお気軽にご相談ください

サイバー攻撃の停止に向けた国内・海外組織との調整

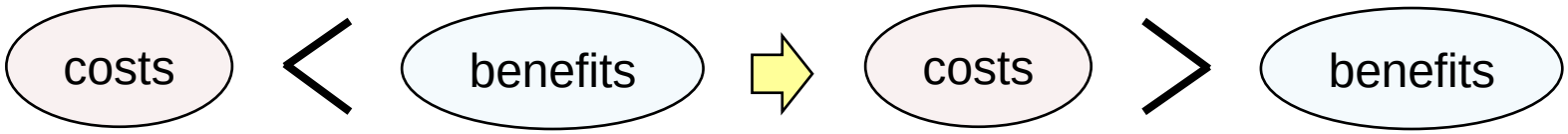
- 攻撃の停止に向けて国内外の複数組織間の情報共有・調整業務を実施
- 国内複数組織への広範囲な攻撃について情報を収集し各方面へ共有



サイバー攻撃のリスクを下げる活動

■ 攻撃：コストとベネフィット

- 攻撃にもコストが必要 (攻撃インフラ、ツール等)
- **環境を改善しない限り攻撃は終わりません**



利益の方が大きい
→攻撃動機を助長

コストの方が大きい
→攻撃動機が減退

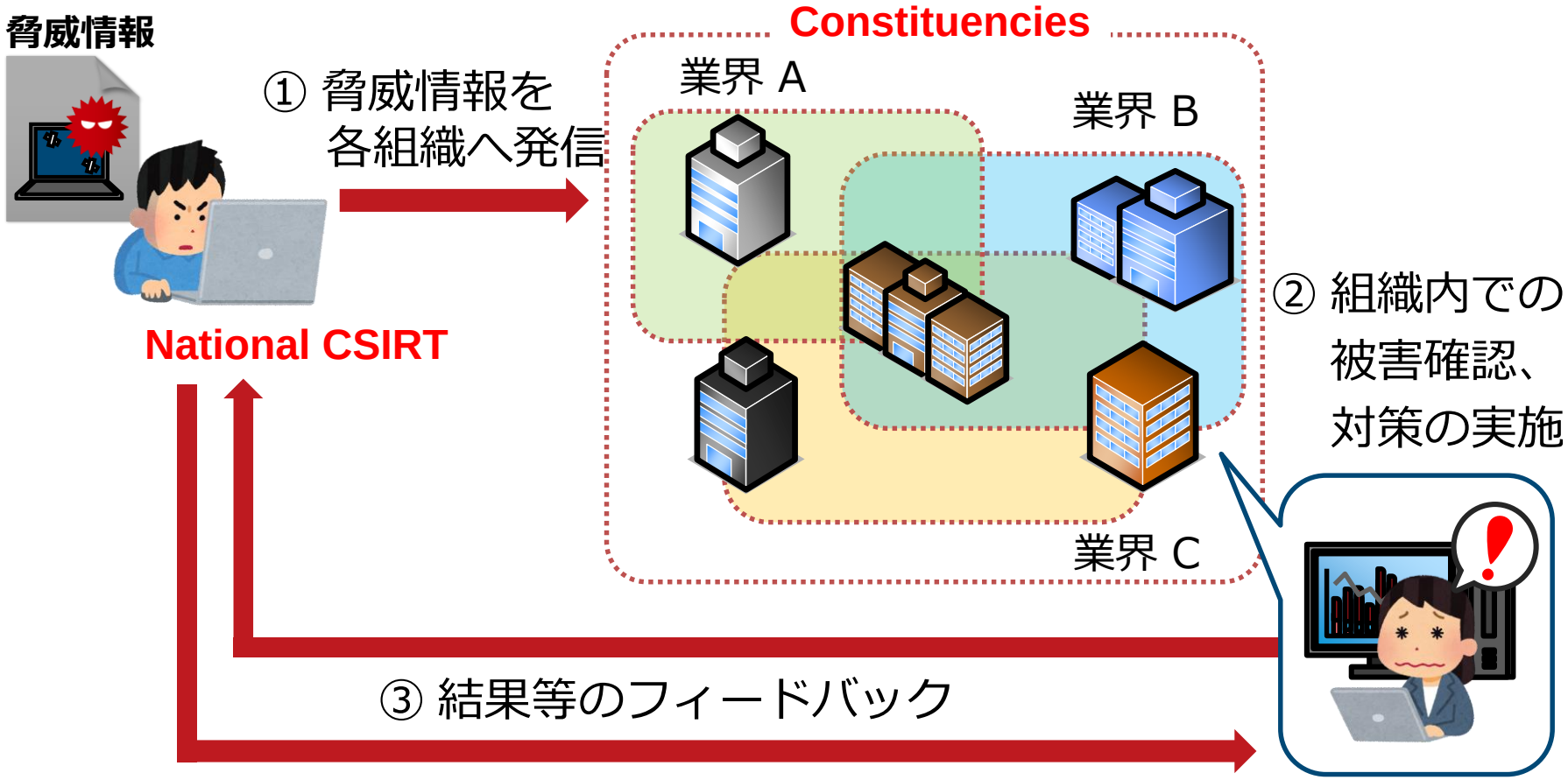
■ インシデントを防ぎ、サイバー攻撃のリスクを下げるには、攻撃のコストを上げていけるかが鍵

- 適切かつ迅速な初動活動・対応
- 正確な技術情報
- 普段からの脆弱性への対応 (作る側・使う側)

JPCERT/CCは、サイバー攻撃のリスクを下げるための活動を展開しています

脅威情報の共有による防御

- サイバー攻撃などの脅威情報を共有することで、組織におけるサイバー脅威に対するリスクを軽減



JPCERT/CC における情報提供の流れ (概念)

公開情報

注意喚起

脆弱性関連情報

レポート等

他

コミュニティへの情報

情報セキュリティに関する話題

早期警戒情報 (CISTA)

制御システムセキュリティに関する話題

制御システムセキュリティ情報共有ポータルサイト (ConPaS)

他

脅威度や内容に基づき判断

公開・周知することが適切なもの
(公開情報、レポート、
ソフトウエアの脆弱性・注意喚起)

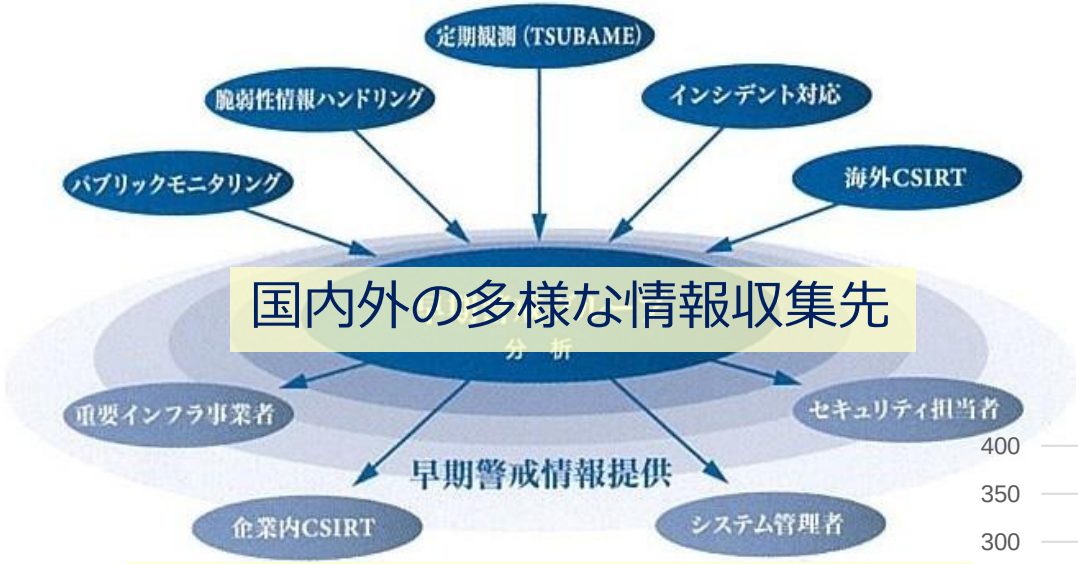
特定の組織やCSIRTに対策を促すことで
より有効に機能するもの
(未修正の脆弱性や攻撃情報等に関する早期
警戒情報、 インディケータ情報、特定のグ
ループ・コミュニティーに特化したセキュリ
ティ情報)

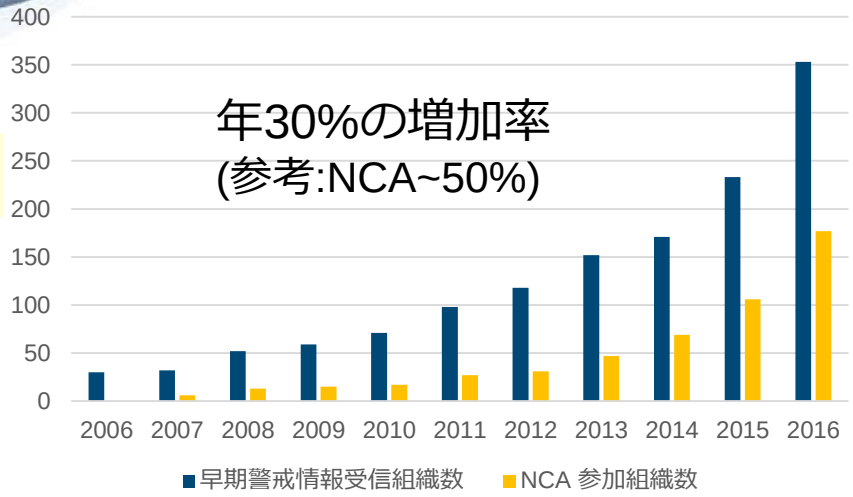
分析

情報収集

早期警戒情報の提供

- 情報セキュリティに関する情報の収集件数：約16,000件/年
- 早期警戒情報の発信数：約60,000件/年 (発行総数×ユーザ数)
- 早期警戒情報の受信組織数：500以上





情報の受け取りにご興味のある方は、お気軽にご相談ください

インシデントとは

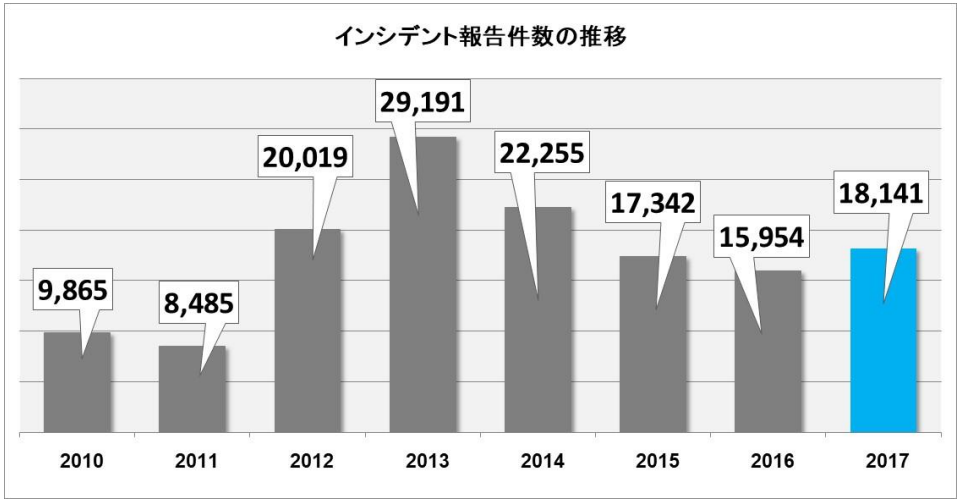
インシデントとは

- （コンピュータセキュリティ）インシデントとは
  - コンピュータセキュリティに関わる事象（事件・事故）
    - 顧客情報の入ったUSBメモリを紛失した
    - 機密情報をSNSにアップしてしまった
    - システムの不具合で生産・製造ラインが停止してしまった
    - **サイバー攻撃によって**ウェブサイトが改ざんされた
      マルウエアに感染し情報を盗まれた

ウェブサイト改ざんによる被害の流れ（一例）

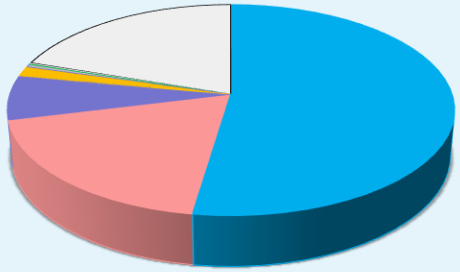
インシデント対応状況（2017年4月～2018年3月）

- JPCERT/CCへの報告
  - 全報告件数
    18,141件
  - 全インシデント件数
    18,768件
- JPCERT/CCからの連絡
  - 全調整件数
    8,891件



JPCERT/CC インシデント報告対応四半期レポートより
https://www.jpcert.or.jp/ir/report.html

インシデント件数のカテゴリ別割合



カテゴリ	割合
スキャン	52.3%
Web サイト改ざん	6.7%
フィッシングサイト	18.8%
マルウエアサイト	1.6%
DoS / DDoS	0.1%
標的型攻撃	0.2%
制御システム関連	0.4%
その他	19.8%

海外におけるインシデントの傾向

- 組織数：**65**（JPCERT/CCは公表データを提供）
- インシデント件数：**42,068**
- データ漏洩/侵害件数：**1,935**

引用：verizon　2017 Data Breach Investigations Report（DBIR）
http://www.verizonenterprise.com/verizon-insights-lab/dbir/
（日本語版: https://www.verizonenterprise.com/jp/DBIR/2017/）

誰もがデータ漏えい/侵害の被害を受ける可能性がある	61% が従業員数千人未満の企業・組織
フィッシング攻撃におけるマルウエアへの感染と情報漏えい	情報漏えい/侵害に発展したフィッシング攻撃の95 %で、何らかのソフトウエアがインストールされ使われた
平易なパスワードの使用	攻撃により漏えいしたパスワードの 80% は平易なものが使用されていた
インシデントのパターン	9つのパターンに分類可能 (88%) (1) クライムウェア (2) サイバースパイ活動 (3) DDoS (4) 内部者による特権の不正利用 (5) 人的ミス (6) ペイメントカードスキミング (7) POSへの侵入 (8) 物理的窃盗 (9) Webアプリケーション攻撃

個人情報漏えいが発生してしまったとき

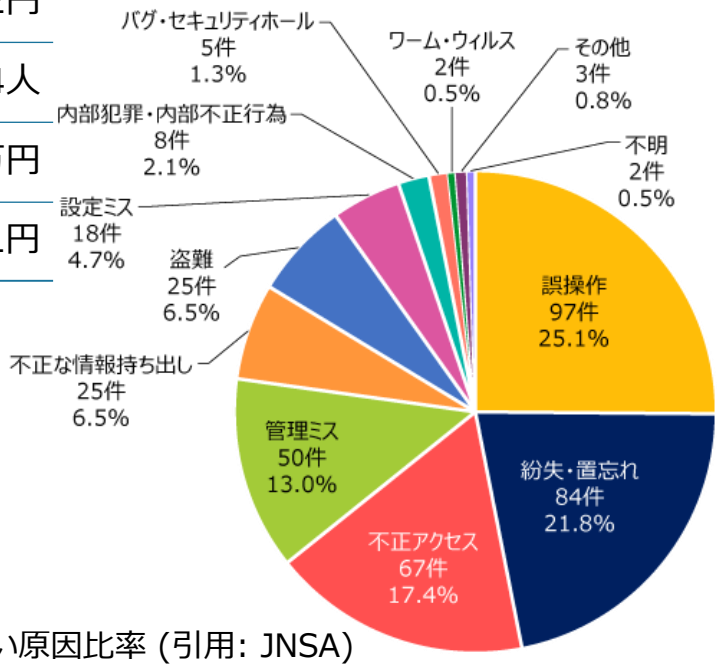
リスク・コストへの対応

— 紛失、誤操作、管理ミス、不正アクセス等の様々なインシデント

2017年個人情報漏えいインシデント概要データ【速報】（JNSA)

漏えい人数	519万8,142人
インシデント件数	386件
想定損害賠償総額	1,914億2,742円
一件あたりの漏えい人数	1万4,894人
一件あたり平均想定損害賠償額	5億4,850万円
一人あたり平均想定損害賠償額	2万3,601円

引用: 日本ネットワークセキュリティ協会
2017年情報セキュリティインシデントに関する調査報告書【速報】
http://www.jnsa.org/result/incident/



漏えい原因比率 (引用: JNSA)

— 金額には換算できないコスト負担も

【参考】攻撃被害の例

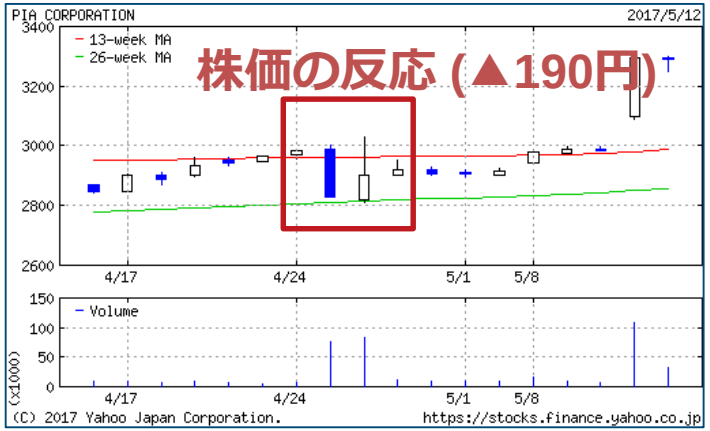
ぴあ株式会社の例

(B.LEAGUEチケットサイト及びファンクラブ受付サイトにおける個人情報流出事案に関する、その後のお詫びとご報告 (4月25日/5月18日発表)　及び業績予想の修正に関するお知らせ (4月25日発表) より抜粋)

- 漏えい件数　：　**38,695 件**
  (カード会員名・カード会員番号・有効期限・セキュリティコード)
- 不正使用の件数と金額　：　**379 件 / 約 880 万円** (5月8日現在)
- 親会社株主に帰属する当期利益修正（増減額）　：
  ※特別損失（お客様対応費用等の引当）の計上等
  ▲ 250 百万円

業績や株価への影響

- 経営責任や株主への説明責任を考える上で参考となる材料



大学等で発生した
インシデントを振り返る

富山大学にて発生した標的型メール攻撃 (2015年11月)

■ 標的型メール攻撃による被害

① ウイルスが仕込まれた添付ファイルをメールで受信

② 添付ファイルを展開したPCにウイルスが感染

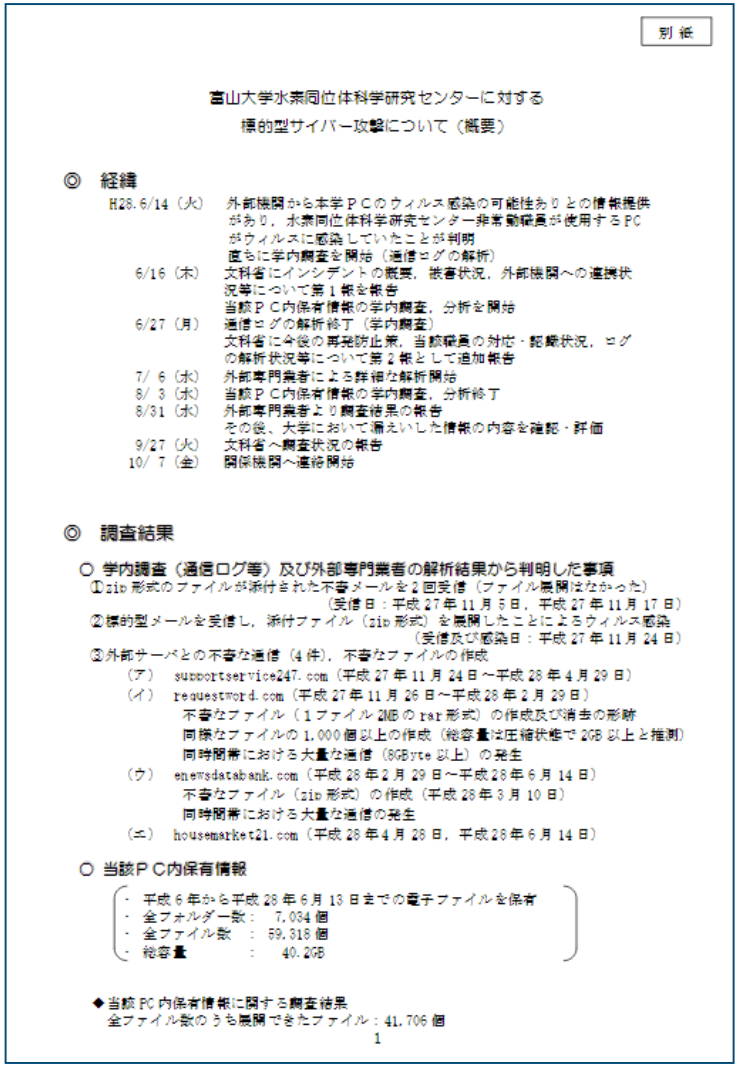
③ 感染したPC内のファイルが窃取された可能性

■ メールを開く関係者や環境に注意

— メールは、教員と非常勤職員に届いていた

— メールに添付されたファイルを開いた非常勤職員のPCが感染

教職員、学生などそれぞれ置かれている立場を理解して、全学的に対策をすることが望ましい（部ごとの縦割り管理）



別紙

富山大学水素同位体科学研究センターに対する
標的型サイバー攻撃について（概要）

◎ 経緯

H28.6/14（火） 外部機関から本学ＰＣのウィルス感染の可能性ありとの情報提供があり，水素同位体科学研究センター非常勤職員が使用するＰＣがウィルスに感染していたことが判明
直ちに学内調査を開始（通信ログの解析）
6/16（木） 文科省にインシデントの概要，被害状況，外部機関への連絡状況等について第１報を報告
当該ＰＣ内保有情報の学内調査，分析を開始
6/27（月） 通信ログの解析終了（学内調査）
文科省に今後の再発防止策，当該職員の対応・認識状況，ログの解析状況等について第２報として追加報告
7/ 6（水） 外部専門業者による詳細な解析開始
8/ 3（水） 当該ＰＣ内保有情報の学内調査，分析終了
8/31（水） 外部専門業者より調査結果の報告
その後、大学において精査した情報の内容を確認・評価
9/27（火） 文科省へ調査状況の報告
10/ 7（金） 関係機関へ連絡開始

◎ 調査結果

○ 学内調査（通信ログ等）及び外部専門業者の解析結果から判明した事項
①zip 形式のファイルが添付された不審メールを２回受信（ファイル展開はなかった）
（受信日：平成 27 年 11 月 5 日，平成 27 年 11 月 17 日）
②標的型メールを受信し，添付ファイル（zip 形式）を展開したことによるウィルス感染
（受信及び感染日：平成 27 年 11 月 24 日）
③外部サーバとの不審な通信（4 件），不審なファイルの作成
（ア） supportservice247.com（平成 27 年 11 月 24 日～平成 28 年 4 月 29 日）
（イ） requestword.com（平成 27 年 11 月 26 日～平成 28 年 2 月 29 日）
不審なファイル（１ファイル 2MB の rar 形式）の作成及び消去の形跡
同様なファイルの 1,000 個以上の作成（総容量は圧縮状態で 2GB 以上と推測）
同時間帯における大量な通信（8GByte 以上）の発生
（ウ） enewsdatabank.com（平成 28 年 2 月 29 日～平成 28 年 6 月 14 日）
不審なファイル（zip 形式）の作成（平成 28 年 3 月 10 日）
同時間帯における大量な通信の発生
（エ） housemarket21.com（平成 28 年 4 月 28 日，平成 28 年 6 月 14 日）

○ 当該ＰＣ内保有情報

- 平成 6 年から平成 28 年 6 月 13 日までの電子ファイルを保有
- 全フォルダー数： 7,034 個
- 全ファイル数 ： 59,318 個
- 総容量 ： 40.2GB

◆当該 PC 内保有情報に関する調査結果
全ファイル数のうち展開できたファイル：41,706 個

1

引用：富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について(事案の概要)
https://www.u-toyama.ac.jp/news/2016/1011.html

各大学で観測される標的型メール攻撃

- **「科研費」にまつわる標的型メール攻撃を毎年確認**
  - 2016年5月 「【文科省（ご連絡）】新学術領域研究の中間・事後評価について」
  - 2017年1月 「【H29科研費】繰越申請について」
  - 2018年1月 「平成30年度文部科学省の研究計画書」

- **学会活動や研究内容などに関連した標的型メール攻撃も継続して観測**
  - 攻撃者は、さまざまな情報を狙います

- **いつ誰が被害を受けるかは予測困難**
  - 学内の誰が被害を受けても、インシデント対応可能なよう風通しの良い環境や体制の整備が不可欠

大学サービスに関連したフィッシングメール攻撃

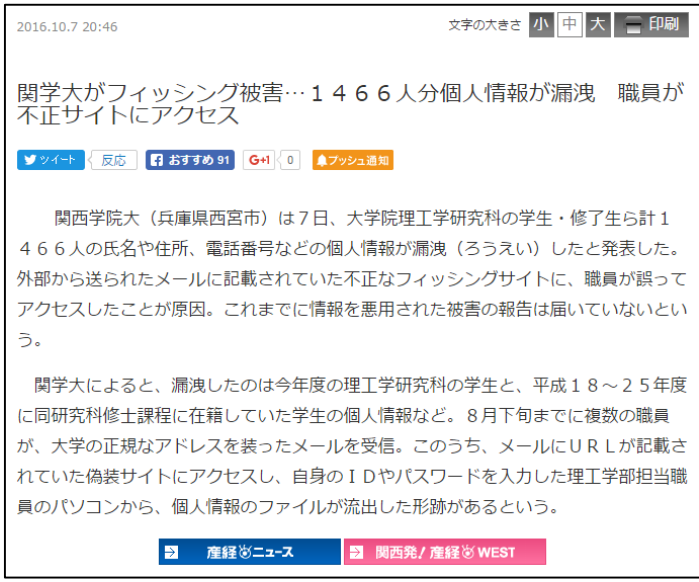
- **大学のメール、クラウド (Office365 等) へのフィッシングメール攻撃は常に存在**

From: [redacted] University Admin
件名: こんにちは

あなたは、電子メールのストレージスペースの[redacted]アクティブが少なくなっています。ここをクリック
あなたの[redacted]アクティブ電子メールストレージにスペースを追加します。

どうもありがとうございました。
C著作権2016年[redacted]大学。 全著作権所有。

- **「たかが、大学の ID、パスワードなんて」と思っていませんか？**
  - 関西学院大学の事例 (2016年)
    - ID,パスワードの窃取から学生、卒業生ら1,466名の個人情報が漏えい
    - Office365を介してファイルへのアクセスに関する報道



2016.10.7 20:46

文字の大きさ 小 中 大 印刷

関学大がフィッシング被害…１４６６人分個人情報が漏洩　職員が不正サイトにアクセス

ツイート 反応 おすすめ 91 G+1 0 プッシュ通知

関西学院大（兵庫県西宮市）は７日、大学院理工学研究科の学生・修了生ら計１４６６人の氏名や住所、電話番号などの個人情報が漏洩（ろうえい）したと発表した。外部から送られたメールに記載されていた不正なフィッシングサイトに、職員が誤ってアクセスしたことが原因。これまでに情報を悪用された被害の報告は届いていないという。

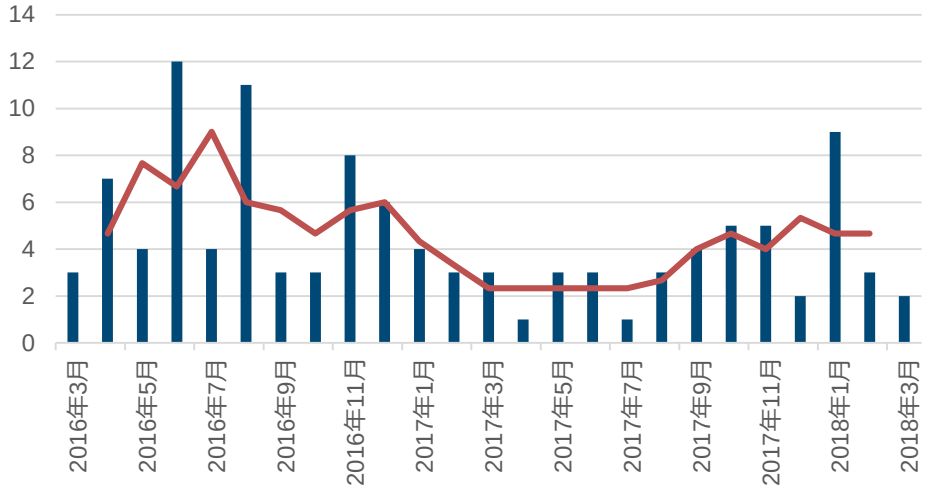
関学大によると、漏洩したのは今年度の理工学研究科の学生と、平成１８～２５年度に同研究科修士課程に在籍していた学生の個人情報など。８月下旬までに複数の職員が、大学の正規なアドレスを装ったメールを受信。このうち、メールにＵＲＬが記載されていた偽装サイトにアクセスし、自身のＩＤやパスワードを入力した理工学部担当職員のパソコンから、個人情報のファイルが流出した形跡があるという。

産経ニュース 関西発/ 産経WEST

各大学で観測されるフィッシングメール

- **いずれの大学でも観測されており、波もある**
  - どの大学でも同じようなインシデントが発生しうる可能性

各大学の情報系センターなどのWebサイトにて、ID パスワードを狙うフィッシングメールに対する注意の呼びかけがなされた件数



- **他大学、他研究所でIDやパスワードを使いまわしていませんか？**
- **日本人学生以外にも留学生にも注意**

Brute Force Attacks Conducted by Cyber Actor

- Brute Force Attacks Conducted by Cyber Actors
  - イラン人 (Mabna Instituteの関与) によるサイバー攻撃
  - Password-Spray 攻撃やフィッシングメールなどによる情報収集・不正ログイン


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA18-086A)
Brute Force Attacks Conducted by Cyber Actors

More Alerts

Original release date: March 27, 2018 | Last revised: March 28, 2018

Print | Tweet | Send | Share

Systems Affected

Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals, who were associated with the Mabna Institute, for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

引用: US-CERT, https://www.us-cert.gov/ncas/alerts/TA18-086A


Mabna Institute

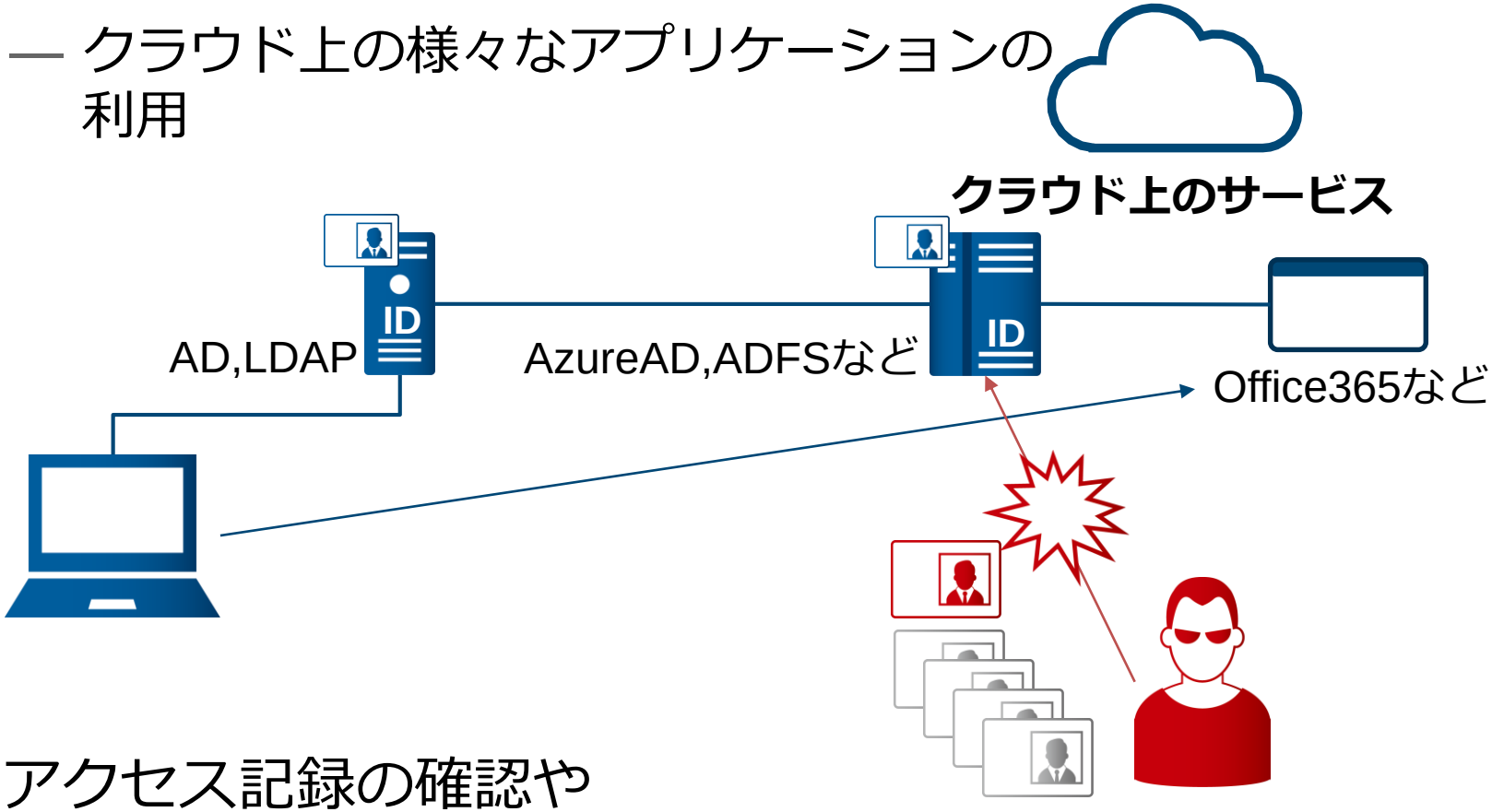
As previously detailed, the Mabna Institute was publicly identified in an FBI indictment as a front company engaged in hostile state-sponsored cyberespionage on behalf of the Iranian state. Our OSINT research identified a single domain, mabna-ins[.]ir, which could correspond to the group. The domain was previously hosted on an Iranian IP 5.144.130[.]23 and since April 22, 2017, points at German VPS IP 144.76.87[.]86. This VPS also hosts over 2,000 other domains, most of which are .ir domains.

Source: mabna-ins[.]ir

引用: Recorded Future, https://www.recordedfuture.com/iran-hacker-hierarchy/

グループ、社内でこのような状況ありませんか？

- **クラウドサービスを含めた Single Sign On (SSO)**
  - 社内の様々なシステムやデータへのアクセス
  - クラウド上の様々なアプリケーションの利用



- アクセス記録の確認や
  各個人のIDの管理について気にかけていますか？

大阪大学にて発生した不正アクセス (2017年5月)

- **一人のIDを起点として大学全体の問題へ拡大**
  - ① 何らかの方法で一人のID、パスワードが窃取され、悪用
  - ② 不正なプログラムが設置され管理者のID,パスワードが窃取
  - ③ 利用者情報のさらなる取得
  - ④ 学内グループウェアなどへの不正アクセス

不正アクセスに対して守るべきものは認識していますか？

大阪大学総長コメント

個人情報の取扱いにつきましては、各種研修、会議、学内通知等を通じて、教職員への啓発を行うことにより、適切な管理を図ってきたところですが、今回、このような事態が発生し、関係者の皆さまに多大なご迷惑おかけしたことを深くお詫び申し上げる次第です。

本学といたしまして、今回の個人情報漏えいを極めて重大な問題であると受け止め、全構成員に対して個人情報の取扱い及びＩＤとパスワードの適切な管理について、より一層の周知徹底を図るとともに、個人情報を含む学内の重要情報を守るため、セキュリティの強化に努めてまいります。

なお、現在のところ、二次被害は確認されておりませんが、関係者の皆様からの相談につきましては、適切に対処していく所存です。

平成 29 年 12 月 13 日

大阪大学総長　西　尾　章治郎

引用:
http://www.osaka-u.ac.jp/ja/news/topics/2017/12/13_01

産総研にて発生した不正アクセス (2018年2月)

- 不正アクセスにともない、長期間にわたりインターネットアクセスを制限
- 所内関係者からと思われる書き込みも散見される
  - 掲示板、Twitterなど
- 政府も調査に乗り出す状況へ

果たして大学等は無関係と言えますか？

産総研
国立研究開発法人 産業技術総合研究所
NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY (AIST)

エネルギー・環境 | 生命工学 | 情報・人間工学 | 材料・化学 | エレクトロニクス・製造 | 地質調査 | 計量標準

ホーム > ニュース > お知らせ

お知らせ

2018/02/13

弊所に対する不正なアクセスに関する事案について

平成30年2月13日
国立研究開発法人産業技術総合研究所

平成30年2月6日（火）、弊所に対する外部からの不正なアクセスがあったことを確認しました。業務の遅延等により、関係者の方々にご迷惑、ご心配をおかけしており、深くお詫び申し上げます。

不正なアクセスの確認後速やかに情報セキュリティ対策本部を設置し、現在外部の専門事業者にも協力を依頼して原因究明を進めているところです。現時点で判明している情報につきお知らせします。

1. 内容
平成30年2月6日（火）、弊所に対して外部からの不正なアクセスがあったことを確認しました。当該事案は重大なセキュリティインシデントであると判断し、弊所の情報セキュリティ規程第20条に基づき情報セキュリティ対策本部を設置、外部の専門事業者にも依頼して原因究明を進めているところです。

なお、本事案についてはすでに関係省庁へ報告し、警視庁にも相談を行っているところです。

2. 対応状況

2月6日	不正なアクセスがあったシステム（以下「本件システム」という。）に対する外部からのアクセスを緊急に遮断。本件システムを提供する事業者に連絡し、対応を協議。原因及び影響範囲の調査を開始。
2月7日	重大なセキュリティインシデントであると判断し、副理事長の下に情報セキュリティ対策本部を設置。
2月8日	全職員の本件システムに関するパスワードを強制変更。原因及び影響範囲の調査継続。
2月9日	全職員に通知した上で、本件システムはメール及びスケジュール機能のみを残し、他の機能を停止。全業務システムに関する点検を開始。
2月10日～12日	原因及び影響範囲等の調査を継続。
2月13日早朝	弊所内部からのインターネット接続を遮断。

2月13日以降、安全を確認できた部分から業務システムを順次再開予定（インターネットの遮断は継続）。

3. 今後の対応
第三者及び弊所の知的財産に関する情報や保有個人情報の漏えいの可能性なども懸念されることから、引き続き、早急に、原因及び影響範囲等の調査を進めます。

引用:
http://www.aist.go.jp/aist_j/news/announce/au20180213.html

大学等に求められる対策とインシデントへの備え

【参考】大学等に求められる対策

（サイバーセキュリティ戦略本部第14回会合資料より）

⑤大学等における情報セキュリティ対策の向上

多岐に渡る情報資産、多様なシステムの利用実態といった大学等における多様性を踏まえ、当該特性に応じて、大学等の情報セキュリティ対策の強化を促進するとともに、大学等の相互の協力による自律的活動の向上に向けた取組を促す。

具体的には、**各大学等は、教育・研究等の多様性に配慮しつつ、中長期的な情報セキュリティ対策基本計画を策定し、マネジメント面及び技術面の取組を推進**する。また、**大学等の連携によるサイバー攻撃検知体制の整備や人材育成の取組を推進**する。なお、国は、これらの取組に対し、必要な支援に努める。

○ 大学等における自主的な取組

ア マネジメント面

・企画・法務・広報など関係部門と連携したインシデント対応体制の構築と対処能力の向上
・情報セキュリティポリシーや情報の取扱規程等の見直しや組織への浸透
・多様な構成員に対応した教育・訓練や啓発活動の実施
・構成員の役割に応じた自己点検や中立性を有する者による監査の実施

イ 技術面

・組織内の情報機器の把握と適切なアクセス制御の実施
・重要情報を扱う機器へのアクセス等を監視する機能等の実装
・組織内で利用しているソフトウェアの適切な更新が可能な仕組みの整備

○ 文部科学省等による支援

・大学等における自主的な取組の促進の観点から、**インシデント対応力の向上やセキュリティ監査手法に関する研修の実施及び機会の充実、情報システムの侵入耐性診断の実施に関する支援、諸会議における周知、啓発及びグッドプラクティスの共有並びに情報セキュリティ対策基本計画の進捗状況のフォローアップその他自主的な取組加速のための支援**を実施

○ 大学等の相互協力による取組

国立情報学研究所において、大学等と連携し、SINET におけるサイバー攻撃検知システムの運用や、同システムの実環境を用いた技術職員の実地研修の実施、脅威情報等の共有促進により、大学等のインシデント対処能力向上を図る。また、連携機関の拡大については、今後、運営上の課題を含めて検討する。

大学等共通の課題の検討や知見の共有等について、各大学等の枠を超えてCSIRT 担当者同士のコミュニティを形成し、脅威情報の共有や共通課題の検討等を実施予定。

大学等における自主的な取組（前掲資料抜粋）

■ マネジメント面

- 企画・法務・広報など**関係部門と連携したインシデント対応体制の構築と対処能力の向上**
- 情報セキュリティポリシーや情報の**取扱規程等の見直し**や**組織への浸透**
- 多様な構成員に対応した**教育・訓練や啓発活動の実施**
- 構成員の役割に応じた自己点検や中立性を有する者による**監査の実施**

■ 技術面

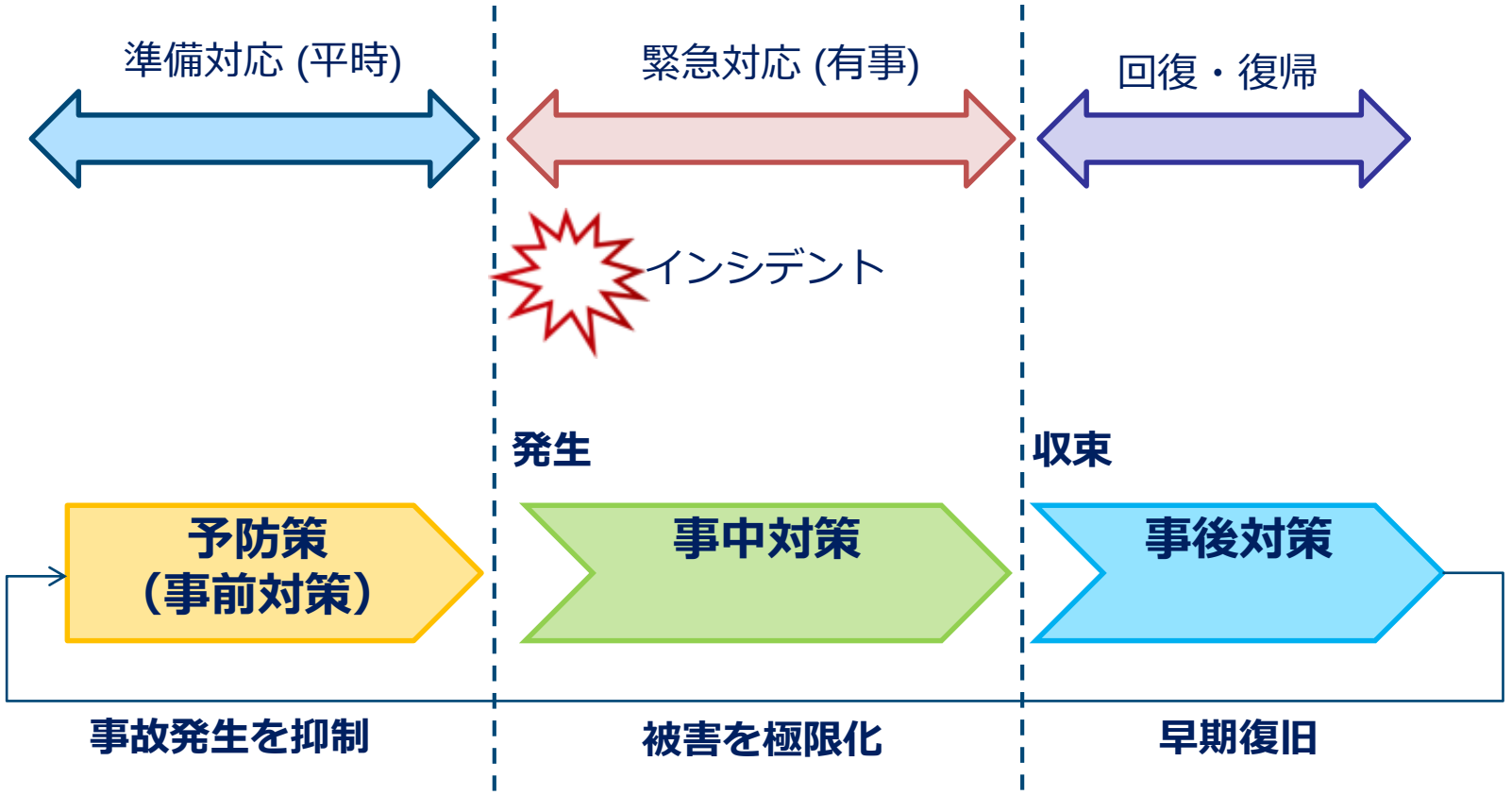
- 組織内の**情報機器の把握**と適切な**アクセス制御の実施**
- 重要情報を扱う機器への**アクセス等を監視する機能**等の実装
- 組織内で利用している**ソフトウェアの適切な更新**が可能な仕組みの整備

何を求められているのか？～前掲資料の考察～

- **CSIRTの構築とインシデント対応**
  - そのCSIRT機能しますか？
- **規程の見直し、組織への浸透、教育訓練**
  - 下書きがあったとしても内容を理解して策定していますか？
  - やりたいことはISMS準拠ですか？それとも？
  - そもそも全員やるべきことを理解して、実践できますか？
- **情報資産・機器の把握、アクセス制限やモニタリング**
  - 例外を作らなければならない状況は一つでも避ける
- **ソフトウエアの更新のしくみ**
- **監査の実施**

➢ **本日インシデントを取り上げた組織は、これらの仕組みがなかった組織だったでしょうか？**
➢ **ただやればいい、では片づけられなくなっています。**

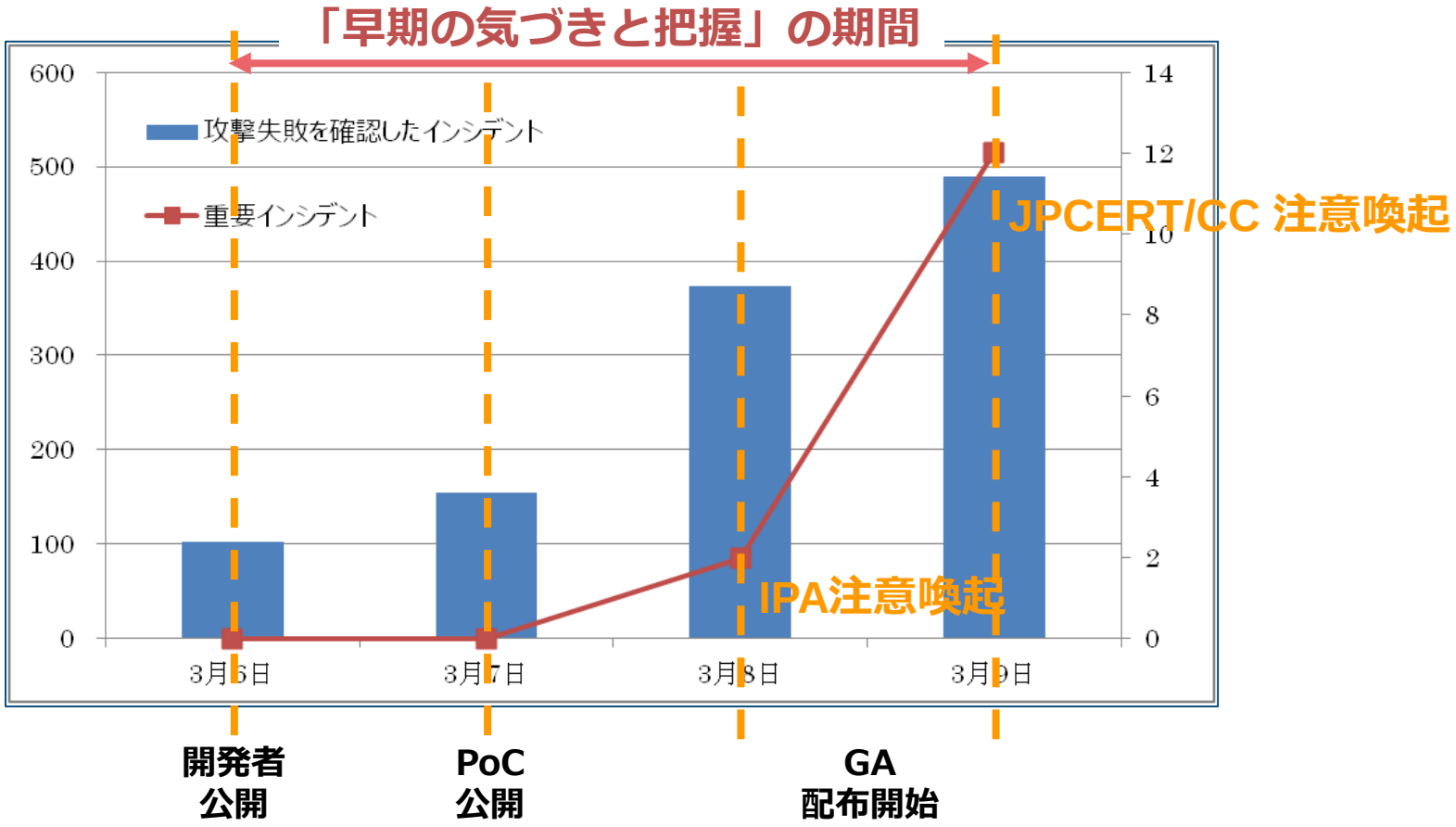
事故発生を前提とした危機管理・緊急体制の確立



予防策だけでなく、**「発生時、発生後」**の対応を考慮

脆弱性情報が流れ始めた初期から攻撃が始まる

- 攻撃の観測の時系列を振り返る



引用・編集：株式会社ラック「Apache Struts 2における脆弱性 (S2-045、CVE-2017-5638)の被害拡大について」にJPCERET/CCが加筆編集
https://www.lac.co.jp/lacwatch/alert/20170310_001246.html

割れ窓理論とサイバーセキュリティ

- **「建物の窓が壊れているのを放置すると、誰も注意を払っていないという象徴になり、やがて他の窓もまもなく全て壊される」**
  - ① 建物の窓が壊れているのを放置すると、それが「誰も当該地域に対し関心を払っていない」というサインとなり、犯罪を起こしやすい環境を作り出す
  - ② ゴミのポイ捨てなどの軽犯罪が起きるようになる
  - ③ 住民のモラルが低下して、地域の振興、安全確保に協力しなくなるそれがさらに環境を悪化させる
  - ④ 凶悪犯罪を含めた犯罪が多発するようになる

- **サイバーセキュリティに果てはめてみるとどうか？**
  - ① マルウエア対策や、アップデートなどを放置
  - ② 軽度なインシデントが起き始める（マルウエア感染や、Web サイトの改ざん)
  - ③ 全体のモラル低下（業界全体でのインシデント増加）
  - ④ 高度サイバー攻撃の発生
  - ⑤ 結果として…

放置しない、人任せにしない

- **使用しているPCや、サーバを放置しない**
  - アップデートや、マルウエア対策を施し、定期的に確認する
  - 軽微なインシデントでも放置しない

- **情報担当者が守ってくれる、と人任せにしない**
  - 自分が重大インシデントの起点になるかもしれないという意識を持つ
  - 悲劇のヒロインにならない
    - 「マルウエア感染に至ったかわいそうな被害者」ではいられません
  - 自分たちの行動を狭めることにつながるかもしれない

- **物理的な災害やインシデントと同様に、平時から備える**
  - 誰に報告し、何をしなければいけないか理解していますか？
  - 責任者は、何に責任を持たねばならないか理解していますか？

放置したら何が起こるのか？

- **「便利だからやってしまえばよい」、「トラブルを起こしたのは使い方が分かっていない人だから、自分は大丈夫」、「隣の人がトラブルにあったけれど、自分は関係ない」 – 独りよがりの考え方が続くと考えられること**
  - ルールがより厳格に・厳しくなる
  - 教育・研究・事務の活動などにも影響が生じる可能性

- **放置しても、よいことなど何もないです**
  - **異常なことがあったら隠さない。相談しあう**
  - **異常なことが起きても叱らない。解決を目指す**
  - **責任は逃れられません。覚悟を持ってください**
  - **人に責任を押し付けなでください。一人ひとりが注意深く行動することで防げることも少なくありません**

まとめ

高等教育機関で発生しているインシデント

- **複雑なインシデントが複数の大学で発生**
  - 標的型メール攻撃などの高度サイバー攻撃
    - 科研費にまつわる標的型攻撃メール
    - 学会などの活動を囮文章にもつものも存在
  - 不正アクセス事案
    - 一つの ID から組織全体の問題につながるようなインシデントが発生

- **いつ、大学がインシデントに巻き込まれるかは予測がつかない**
  - その引き金が、誰なのかも予測がつかない

リスクの認識と、対策の浸透を

- **標的型攻撃に関する社会の認識が変化してきています**

「**攻撃が来るはずがない。**
被害を受けても**被害者**であり、攻撃者が悪い。」

という意見が以前は一部でありましたが、現在は

「攻撃は来て当たり前。
組織、顧客、取引先の情報を守るためには
適切な対策が必要。」

という流れに・・・

リスク評価をせず、さらにセキュリティ対策を行っておらず、重大なインシデントにより情報が漏えいした場合、組織の対策や経営への責任を問われることになります。

個人情報漏えい時の対応から考えてみる

個人情報漏えい時の「望ましい対応」

引用：個人情報保護委員会, 漏えい等の事案が発生した場合の対応等の概要について, https://www.ppc.go.jp/files/pdf/170530_rouei_gaiyou.pdf

- 事業者内部における報告及び被害拡大防止
- 事実関係の調査及び原因の究明
- 影響範囲の特定
- 再発防止策の検討及び実施
- 影響を受ける可能性のある本人への連絡（事案に応じて）
- 事実関係及び再発防止策の公表（事案に応じて）

一度にすべてをやり切ろうとせず、順序だてて考える

まとめ

■ 確実に発生しているインシデント

- ✓ JPCERT/CC では、多様なサイバー攻撃を確認しています
- ✓ 毎週のように**新しい脆弱性**や**事例**が報告されています

■ 脆弱性を悪用された攻撃の被害を防ぐために

- ✓ **悪用されやすい脆弱性は、数日のうちに悪用され、しばらく悪用が続く**こともあります
- ✓ 早期のうちにアップデートすることが望まれます

■ サイバー攻撃は、対岸の火事ではありません

- ✓ **「ウチは狙われない」**という意識を捨てることが重要です
- ✓ 攻撃を防止するだけでなく、**早期検知**、**復旧**、**追跡調査**ができる準備をしておくことも大切です

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

ご静聴ありがとうございました