

サイバー攻撃によるリスクと 大学等で発生した インシデントの振り返り

2019年8月29日

JPCERT/CC

早期警戒グループ 洞田慎一

説明の流れ

- はじめに
- 大学で発生するインシデントへの課題
- インシデント対応体制に向けて
- まとめ

はじめに

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

- 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、ソフトウェアや情報システム・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、ソフトウェア製品開発者等（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/CC, 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

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



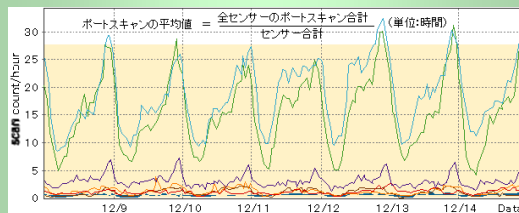
JVN Japan Vulnerability Notes

インシデントの予測と捕捉

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

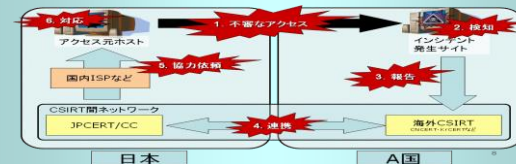


発生したインシデントへの対応

インシデントハンドリング

(インシデント対応調整支援)

- マルウェ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機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

マルウェア（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

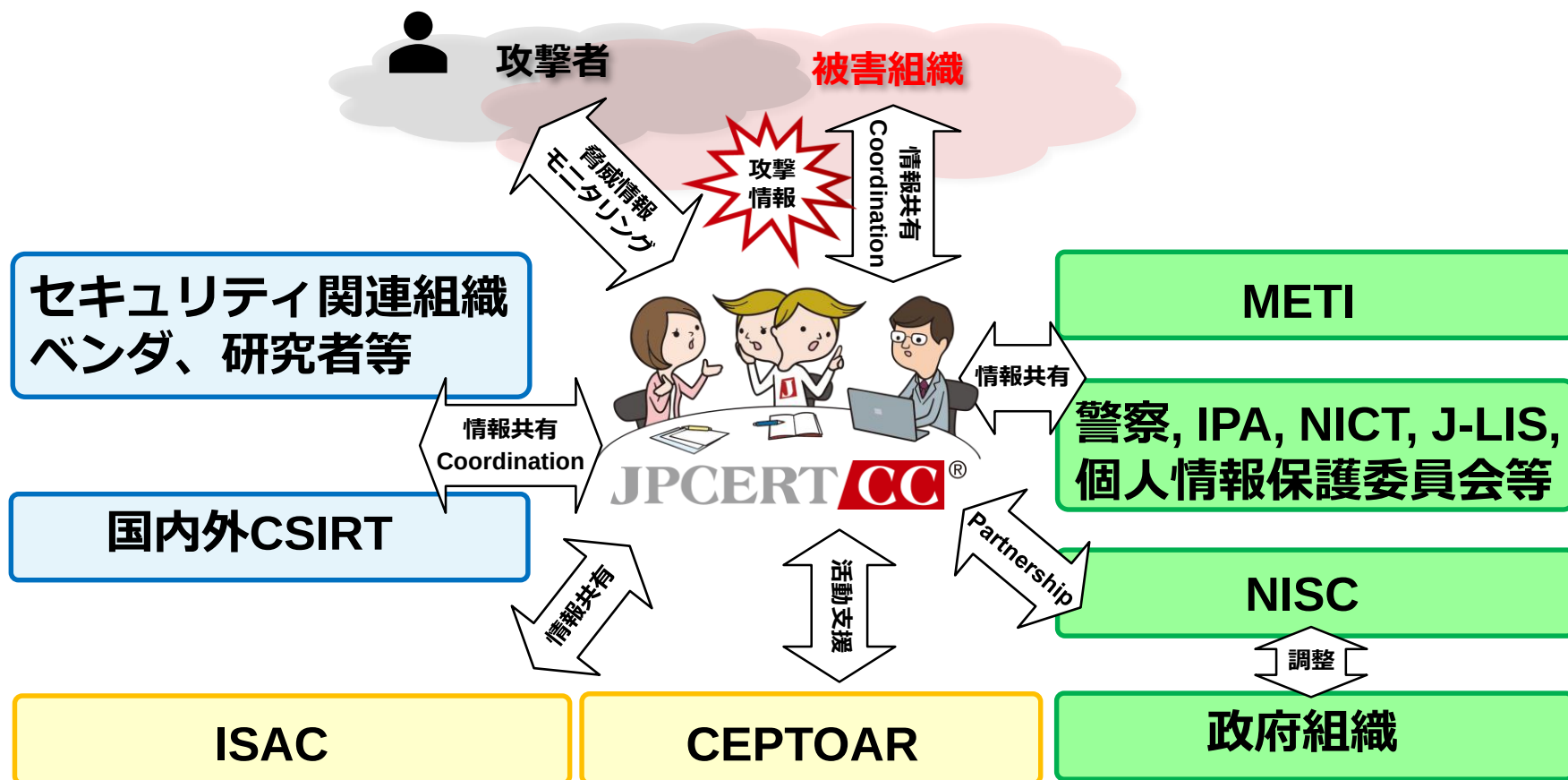
日本シーサート協議会、フィッシング対策協議会の事務局運営等

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

コーディネーションセンターとしての役割

■ 様々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

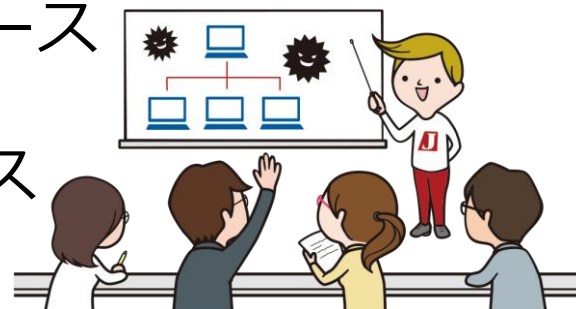
■ コーディネーションセンターの役割と活用

- 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”に向き
合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

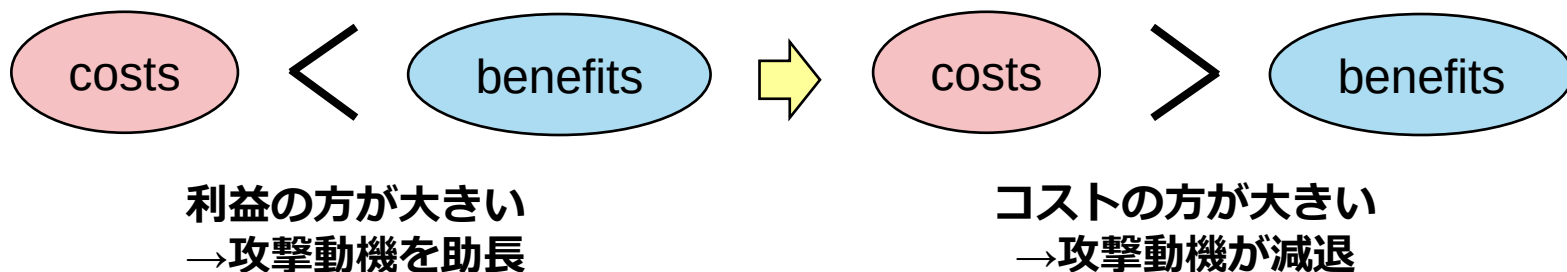
- インシデントが発生し、初動対応での技術的な支援や情報が必要となるケース
- 日々の対策を進める上で、脆弱性や脅威に関する情報が必要となるケース
- その他、お気軽にご相談ください



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



■ 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

攻撃のリスクを下げる取り組みの例

■ 脆弱性情報への適切な対応 (主に事前)

- 報告者、開発者と脆弱性情報を適切に取り扱い、アップデート情報とともに情報を公開 (IPA、JPCERT/CC)
- 公開された情報を基に早期にアップデートを実施 (利用者)
- セキュアコーディング等の脆弱性を作りこまない方法の啓発 (開発者)

■ 正しい技術情報に基づいた適切かつ迅速なインシデント対応 (主に事中・事後)

- アーティファクト分析に基づいた迅速な対応

■ その後の脅威へのモニタリングと集団防護 (主に事後)

- 継続的なモニタリングによる脅威の発見
- 同じタイプの攻撃を防ぐため、グループでの情報共有

サイバー攻撃の種類と事例（１）

標的型サイバー攻撃

マルウェアが添付されたメールによりネットワーク内部に侵入し、長期間にわたって潜伏し、機密情報や営業秘密、個人情報等を窃取する攻撃

例：日本年金機構（2015年6月）、JTB（2016年6月）、三菱重工（2011年9月）

年金機構の125万件情報流出 職員、ウイルスメール開封

2015/6/1付

保存 共有 印刷 共有 ツイート その他

日本年金機構は1日、年金情報を管理するシステムに職員の端末を通じて外部から不正アクセスがあり、個人情報約125万件が外部に流出したとみられると発表した。情報には基礎年金番号や氏名が含まれ、うち約5万2千件には生年月日や住所も含まれていた。職員がウイルスの組み込まれた電子メールの添付ファイルを誤って開封し、不正アクセスされたと想定されるという。

同日記者会見した水島藤一郎理事長は「深くおわびする。誠に申し訳ない」と陳謝した。同機構を巡り、これだけ大規模な情報流出が発覚したのは初めて。

流出したのは年金記録を管理するのに一人一人に割



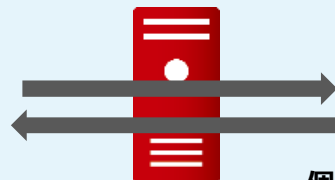
【引用】2015年6月1日 日本経済新聞
https://www.nikkei.com/article/DGXLASDG01HCD_R00C15A600000/

Webサイト（サーバ）への不正アクセス

インターネット上に公開されているWebサイトへのシステムの管理不備や脆弱性を突いて不正アクセス

個人情報やクレジットカード窃取するほか、Webサイト閲覧者にマルウェアを感染させたり、スパムメールの配信に悪用するなど、他の攻撃の踏台に利用

例：森永乳業（2018年5月）、プレミアムアウトレット（2018年4月）、幻冬舎（2018年1月）



個人情報やクレジットカード情報が保管

サイバー攻撃の種類と事例（2）

Webサイト改ざん

Webサイトを改ざんして、政治的なメッセージを掲載したり、改ざん箇所を隠した上で、閲覧者にマルウェアを感染させる踏台に悪用する攻撃。

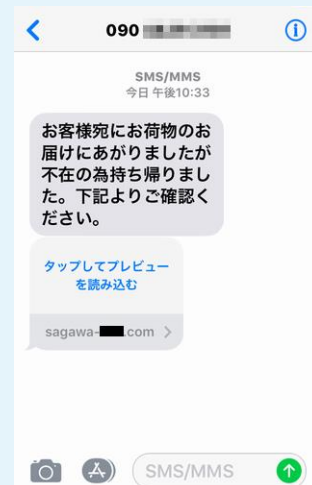
例：長野県河川水位情報のWebサイトが改ざんされ、閲覧者がマルウェア感染する恐れ（2017年7月）



フィッシング

正規のオンラインサービスからの連絡になりすまし、個人情報やクレジットカード情報、インターネットバンキングのID/PWを窃取しようとする攻撃

例：
2018年8月10日に
確認されたAmazonをかたる
フィッシングメール



DDoS攻撃

Webサイトなどのインターネット上に公開されたシステムに対して、大量の通信等を送り付けることにより、回線をパンクさせたりサービスを停止させる攻撃

例：厚生労働省（2015年11月）、NEXI、IPAのWebサイトへの攻撃（2016年9月）



インシデント対応状況（2018年4月～2019年3月）

■ JPCERT/CCへの報告

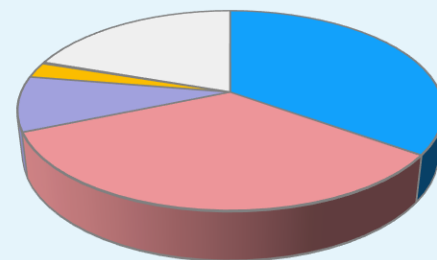
- 全報告件数
16,398件
- 全インシデント件数
16,464件

■ JPCERT/CCからの連絡

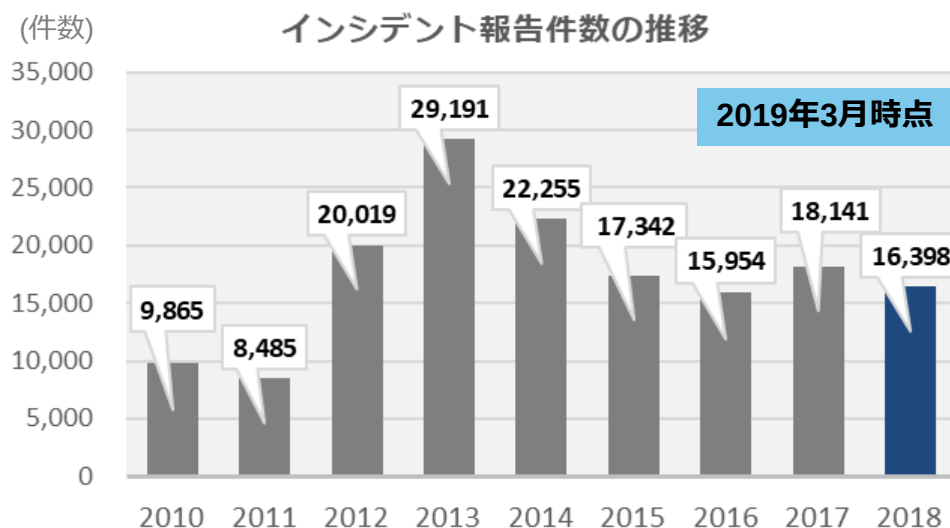
- 全調整件数
9,835件

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	38%
Web サイト改ざん	6.2%
フィッシングサイト	35.4%
マルウェアサイト	2.4%
DoS / DDoS	0.2%
標的型攻撃	0.2%
その他	17.6%



大学で発生する インシデントへの課題

大学という環境でのインシデントとリスク

■ 大学でのサイバーセキュリティを考える上で考慮しておきたいこと

- 多様な構成員

 - 職員、教員、研究員、学生、その他

 - 彼らが接続するフラットなネットワーク

- 国際的なつながり

- 多数のオンラインシステム

- 大学を特徴づけるガバナンス

■ 「大学だから起きうること」が、極めて広範囲に及ぶ可能性がある

標的型攻撃は「組織」を狙った攻撃とは限らない

■ 大学の特徴（教育・研究）を支える多様な人材

- 様々な分野
- 同窓生を含む国内外に広がる人間関係
- **組織が保有する情報と、構成員が保有する情報のいずれにも注目される可能性がある**

■ 標的型攻撃は、「組織」を狙った攻撃であると言い切れる根拠はない

- 潜伏後横断的に侵害し、組織内ネットワークに保持されていた情報にアクセスするケース
- 感染端末に保持されていた情報にアクセスするケース
※ 例: 2017年 富山大学での事例

「一人だけ」に届いたメッセージに対応できますか？

■ 広範囲にばらまかれたスパム・フィッシングメールへの対応と、特定の関係者だけに送られたメッセージとの違いに注意

— 例①

広範囲にみられるマルウェア添付の日本語スパムメール

— 例②

大学のID、パスワードを取得しようとするフィッシングメール

— 例③

特定の関係者に送られた標的型攻撃メール

■ 加えて、メッセージはメールだけとも限らない

■ CSIRT (情報系センター等) での、それぞれの報告の違いは想像がつきますか？

標的に近づく手段はメールとは限らない

■ 学術関係者を装って標的に近づこうとしたケース

- Hard Pass: Declining APT34's Invite to Join Their Professional Network (FireEye, 2019)
<https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html>
- LinkedIn にて Cambridge University の関係者を装って標的に近づき、マルウェア感染へ誘導
- 【参考】中東地域では、過去にも LinkedIn を用いて標的に近づく行為が確認されている (Secureworks, 2015)
Hacker Group Creates Network of Fake LinkedIn Profiles
<https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles>

■ 国際的な動向:メール以外への注意

2019 Data Breach Investigation Report (Verizon, 2019)

<https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

- でも Cyber-Espionage において、Social Attack のうち 84% がメールに由来するものと説明される
- 一方で、Mobile や Social Media への注意も言及される

国内で観測されている事例だけとは限らない

■ 大学関係者がもつ多様な接点

- 海外とのコンタクト
- 外国人スタッフ (教員, 研究者)
- 留学生

■ 必ずしも明確に国内組織等をターゲットとした攻撃ではないものにもあたる可能性

- 海外の大学・研究機関を狙った攻撃の中に含まれるケースにも注目しておく必要性
 - 日本語以外のフィッシングメッセージに遭遇するケース
 - 不自然な日本語であってもアクセスしてしまうケース
- 海外の類似分野で発生した攻撃に巻き込まれているケース
 - 技術・テクノロジー、国際情勢など分野は幅広い

国際的に幅広く攻撃がなされていたケース

■ 広くフィッシングが行われた事例 ～ COBALT DICKENS

Back to School: COBALT DICKENS Targets Universities

<https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities>

- 14カ国 76 大学に影響が及ぶ (オーストラリア、カナダ、中国、イスラエル、**日本**、スイス、トルコ、英国、米国等)
- COBALT DICKENS の活動に関与したとされる関係者・組織 (Mabana Institute) は、米司法省により告発されている (2018年3月)
- メールにより、偽ログインページに誘導
- 認証情報を盗み、知的情報へのアクセスを行っていたとされる

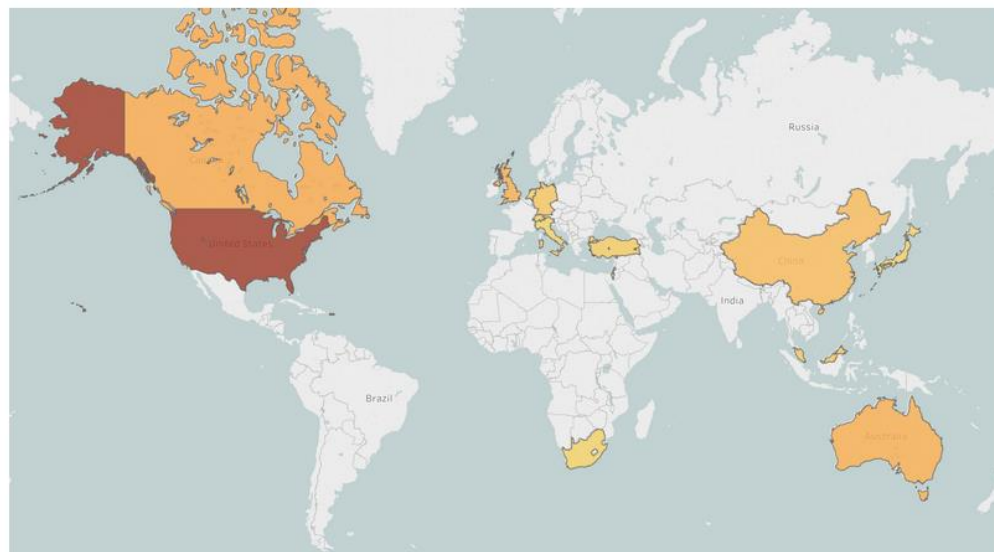


Figure 1. Countries with targeted universities. The darker the color, the higher the number of affected universities. (Source: Secureworks)

出典: <https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities>

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

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

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

Print Tweet Send Share

Systems Affected
Networked systems

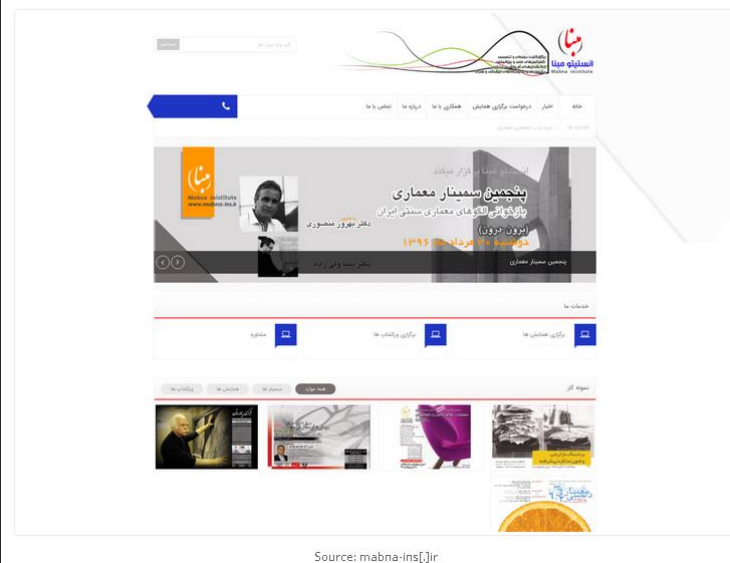
Overview
According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

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](http://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.



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

特殊な環境下での対応の困難さ

■ たった一人だけに送られたメッセージは正しくエスカレーションされ、トリアージできるか？

- 大学以外にも広く確認されているものと、特定の範囲にのみ展開されたもの
- 周辺情報が限られる場合に、どう対応できるか？
 - 「一旦様子を見よう」→具体的には何をする？
 - 国内の情報源にのみ頼っていないか？
 - 特殊なケースでは専門組織でも情報を持っていないものもあります

■ 個人デバイスや研究室内の独自ネットワーク、CSIRTはどの範囲まで対応ができるか？

- 個人持ち込みの端末や特殊な環境などへの対応
- CSIRTは何をどこまで確認することができるか

大学 CSIRT はどこまでが活動の範囲となるか？

■ 意図せず持ち込まれてしまうマルウェアへの対応

— 既に感染済みの端末が持ち込まれるケース

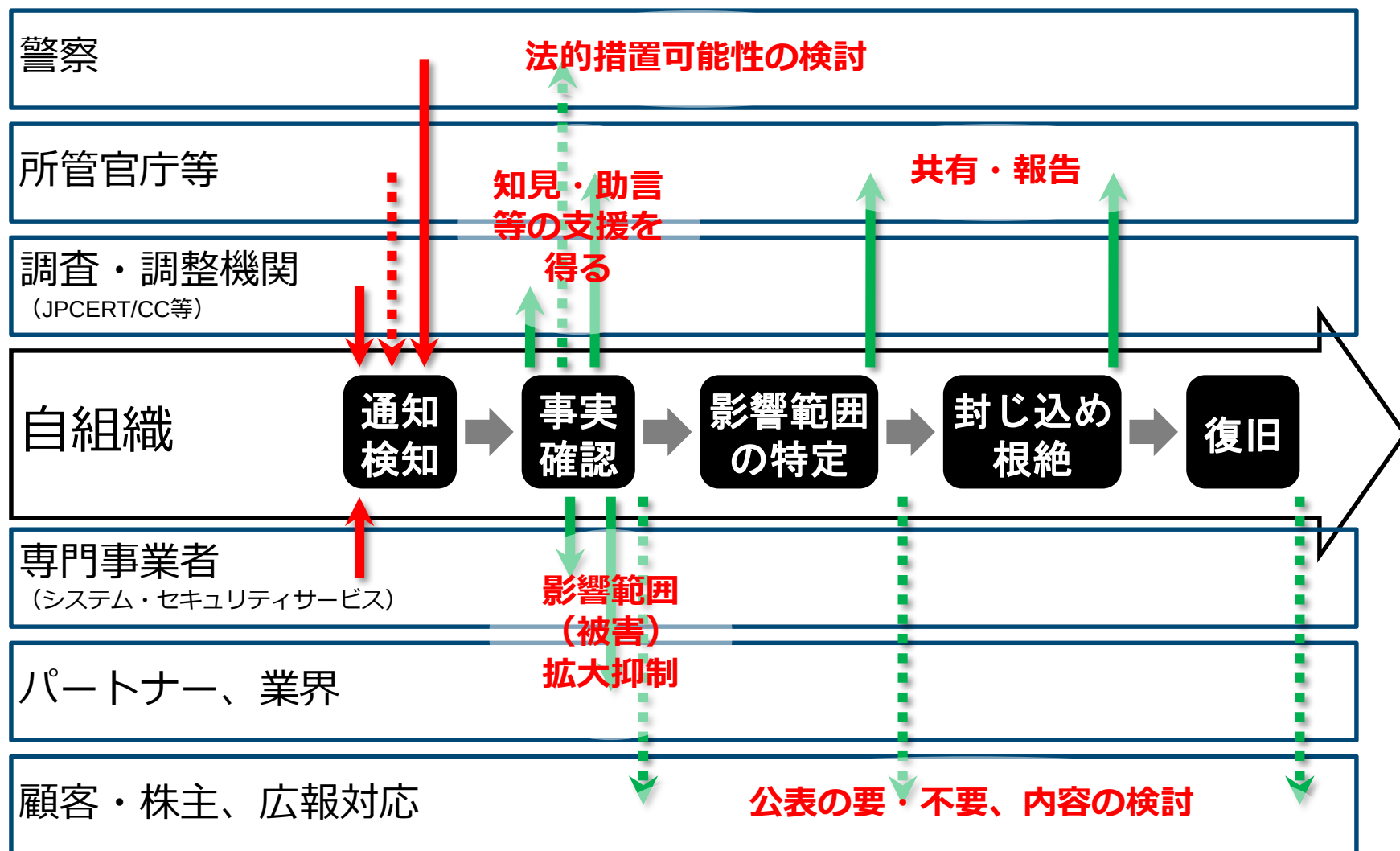
- マルウェアによってはネットワーク内への拡散機能をもっている場合もある
- 特に SIM 搭載型 PC など、直接グローバル IP が割り当てられるケースでは、組織外で感染後、組織内に持ち込まれるケースも考えられる

■ ゲストユーザへの対応

- ゲストのネットワーク利用 (学内ゲスト用ネットワークや国際ローミングなど) におけるインシデント対応やネットワーク設計
- 利用時の当日では問題に気が付かないこともある
 - 後日調べてみたら・・・

インシデント対応体制に向けて

発覚から復旧まで



理想的な対応と現実

■ 現実での対応は難しい

— 理想



— 現実

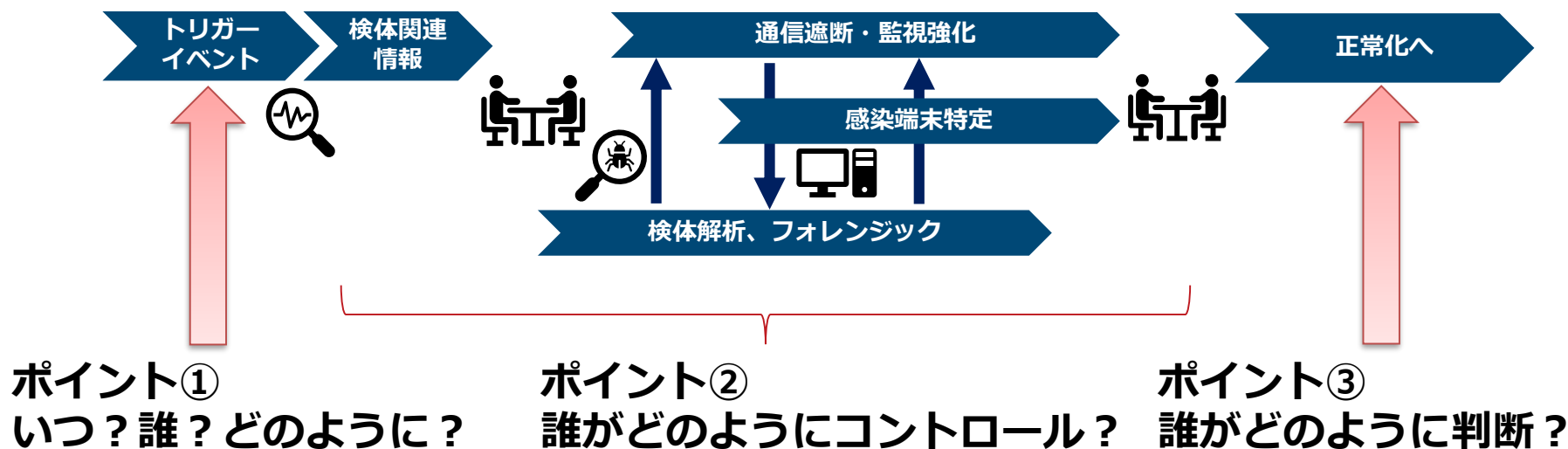


実際の対応において | トリガーと判断

■ インシデントに気が付くトリガーは様々

- マルウェアの拡散・感染を検知できるトリガー
- 不審なメッセージに気が付くトリガー
- 不審な通信先に気が付くトリガー
- その他、学内外からの報告・問い合わせに基づくトリガー
- など

一般的に言われるインシデント対応



実際の対応において | エスカレーションルート

■ エスカレーションのプロセスにおいて、話題が変化していく可能性

- 複数の人を介するなどで、伝言ゲームとなる可能性
- 複数のエスカレーションルートが存在すると、それぞれのパスで温度感の変化も発生

■ 判断の場所における問題

- 現場での対応判断と、エスカレーション先での判断
- 温度感や問題意識がすれ違った場合には異なった判断につながる可能性もある
 - インシデントの初動対応において、正確な技術情報やリスクに基づいた適切なリソースの投入・意思決定が不可欠

インシデント対応の「残念」なケース

■ 外部からの「通知」後すぐに動けない

ーJPCERT/CCや警察、セキュリティ専門企業など外部機関が把握した攻撃情報を受け取っても理解ができず、**初動対応が遅れてしまった**

■ 被害状況が一向に把握できない

ー知見や技術が不足していたり、部署間の連携がうまくできず、**被害把握がすすまず、お客様への対応等が遅れてしまった**

■ 対応を始めたのに二次、三次の攻撃を許してしまう

ー原因究明や応急措置に不備があり、**再度の攻撃**を許してしまった

被害は何件なんだ！

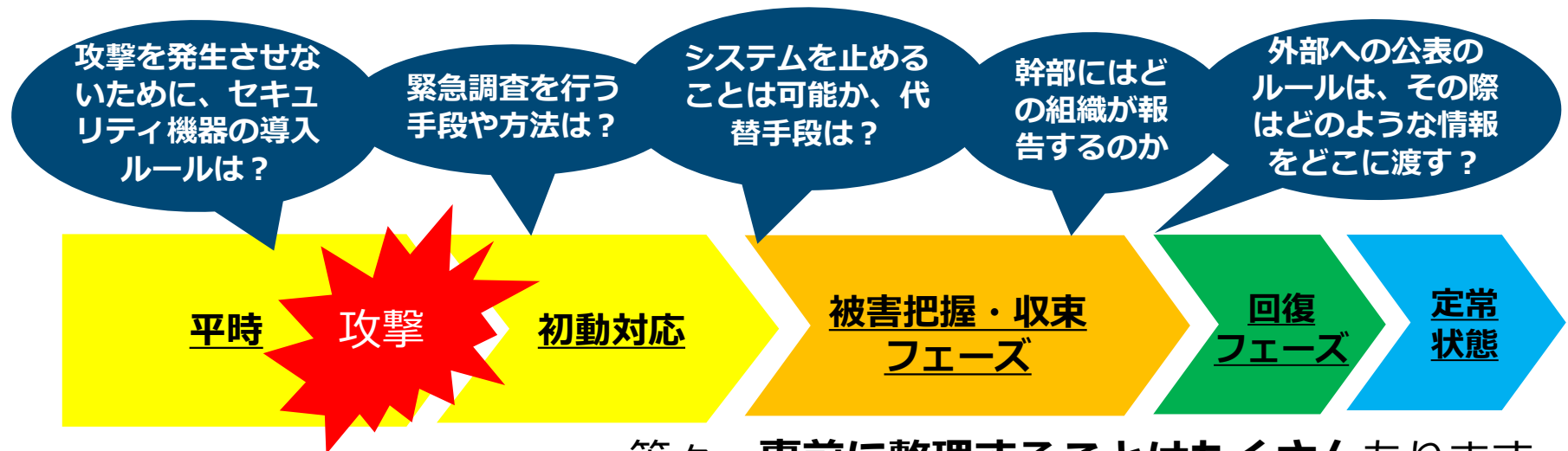


いつ復旧するんだ！？

事前の対策事項

■ 事中だけに注目しない～事前の対策で被害を軽減

- インシデントを発生させないための防御策
- 発生した際の、対応スキームの整理と**社内への落とし込み**
- インシデント演習による、インシデントへの対応速度と質の向上



等々、事前に整理することはたくさんあります

インシデント発生に対して事前に備えておくべき事項

- インシデントが発生した場合、事案への対処、顧客の保護等、進めていかねばならないことは、企業の大きさや、事前の準備の如何によらず、やらなければならないことは基本的に同じ
 - これだけやっておけば大丈夫
 - これを導入しておけば大丈夫
- ↓
- ✓ 攻撃者は日々新たな攻撃手法を探している。
 - ✓ 「（セキュリティ対策）ここまでやればよい」という解はない。

■ この観点で CSIRT の構築と運用を考えてみる

- インシデント発生をみこして、機能する組織を作る
- 実業務として、「サイバーセキュリティ経営ガイドライン 付録 C インシデント発生時に組織内で整理しておくべき事項」を参考にしてみる

インシデント対応の事前準備



攻撃発生

攻撃・被害の認知

初動対応

被害範囲の確認

サービス停止有無の
判断

顧客・取引先対応

外部専門企業等への
調査依頼

原因調査

侵害原因調査

システムの
脆弱性等の確認

被害の詳細確認

事後対策

再発防止策の
検討・実施

第一報

※表1の項番1-11を記載

インシデントが発生したことを速やかに周知。
必要に応じてサービス停止や二次被害防止の
ための注意喚起を行う目的で報告

第二報以降

※インシデントの分類に応じた表を選択
調査の結果、判明した内容を記載

インシデントによる被害範囲がおおよそ確定し、
原因が判明した後に、被害を受けた人に対する周知と他組織が同様の攻撃による被害を受けないための情報共有を行う目的で報告

最終報

※再発防止策を含む全てを記載

被害に対する対応と、その後の再発防止策を含めた事後対策の実施等について、周知を行うことで関係者の安心と、他組織が参考とする目的で報告

■ 攻撃・被害の認知

— 受け取り窓口

■ 初動対応

— 調査する術、意思決定

■ 原因調査

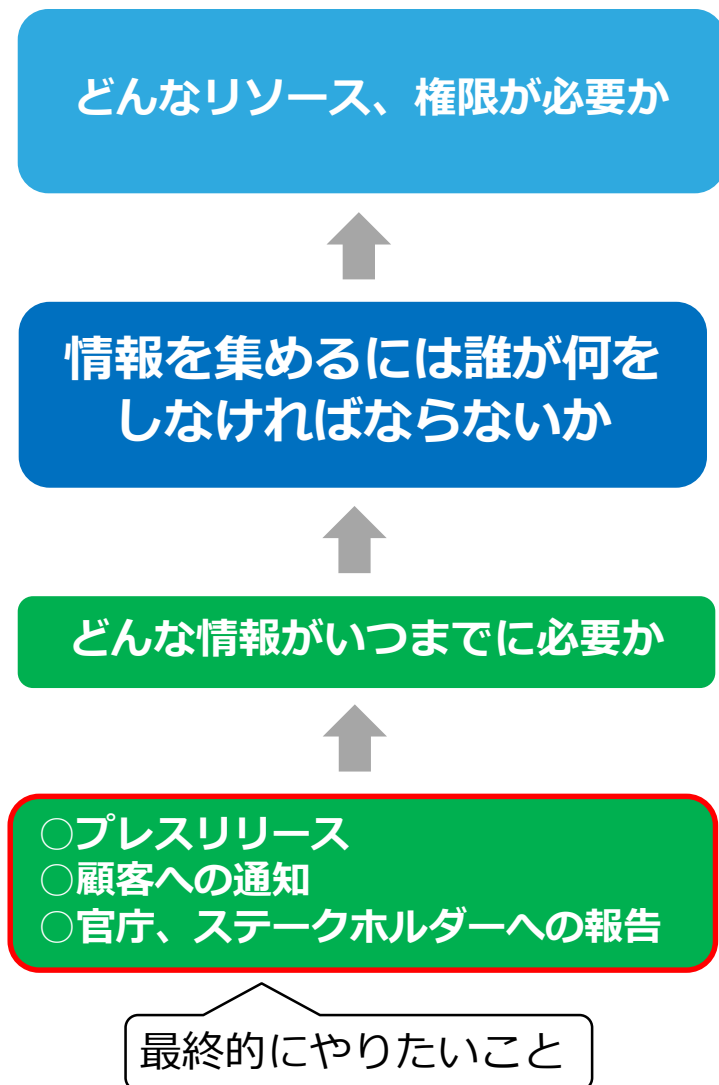
— 被害の全容調査に向けた関係者間の認識

■ 事後対応

— 効果的な対策を提案する上での事前の認識

事前にやっておきたいこと：

「アクション」と「ルート」の交通整理をしよう



【アクションの整理】

事故対応時の情報発信に必要な情報を集めるためのアクションを整理する

(例) 漏えい情報数の推定に必要なこと

- ・ 侵害を受けたサーバに格納されていた情報の最大数の把握
- ・ 攻撃者が持ち出そうとしたデータの確認
- ・ 攻撃者の行動をログ分析から確認

【ルートの整理】

アクションを行うために必要なリソース、連絡ルート、決済ルートを整理する

(例) 最短時間で初動対応に取り掛かるために必要なこと

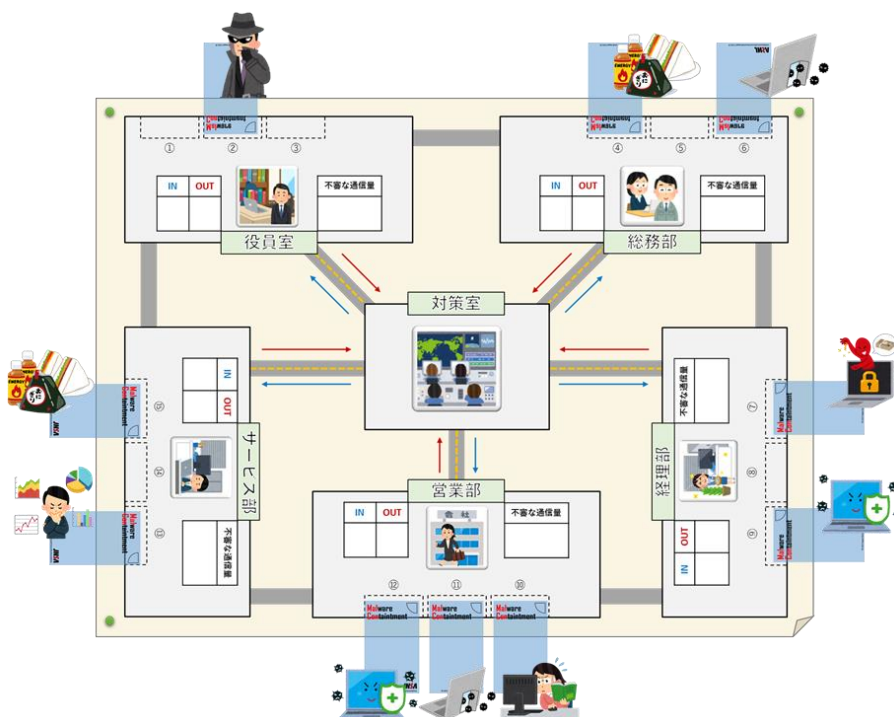
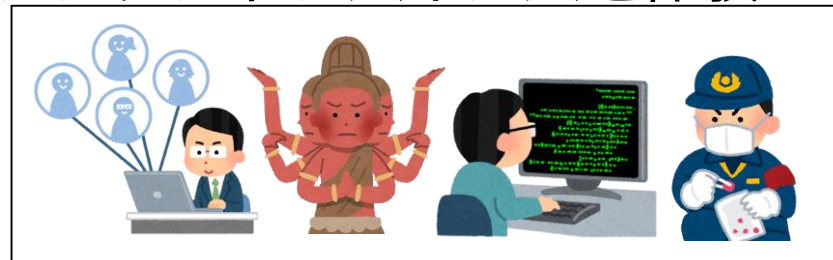
- ・ 誰の判断でシステム／サービスを止めることができるか
- ・ どの役員、部門が対応を指揮するのか

参考：ゲームによる意識の誘導

■ MALware CONtainment (MALCON)

— ゲームを通じてCSIRTでのインシデントレスポンスを体験

- 規程ターン（期日）内にCSIRTのメンバーが協力して、遠隔操作されている端末を調査し封じ込める作業を体験



方針決定会議（3分）

勤務時間（午前）

会話不可

勤務時間（午後）

会話不可

勤務時間（残業）

会話不可

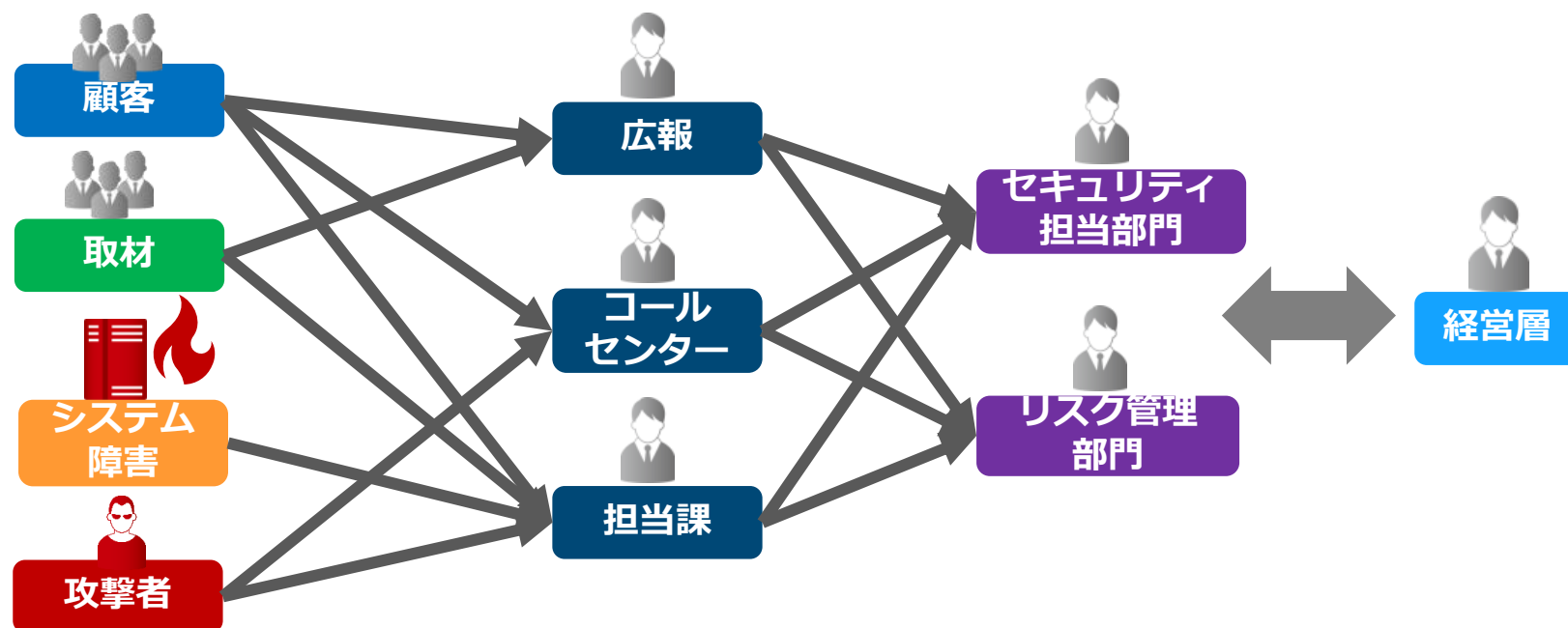
1日の終わり

- ・ 自身の役割を理解すること
- ・ 何のために何をするのかを考えること
- ・ 正確な情報を伝え、メモを取ること

高専などでの授業でも活用

外部通知を視野に入れた対応体制の必要性

- CSIRT が扱うインシデントも実際には組織内では気が付きにくく、外部からの通知より発覚することも多い
 - どのように情報が届いたとしても必要な担当部門にすみやかに共有される仕組み作りが不可欠



まとめ

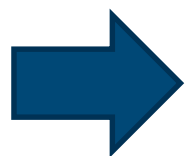
「目的をもった攻撃」への意識と対応

■ 「目的をもった攻撃」を意識する

- 様々な手段を用いて達成しようとする
- 複数の攻撃先、繰り返される攻撃
- 内部ネットワークまで到達する

■ 「見えていないもの」に気付くための手段を確保する

- 各組織内においてデータを保全・共有する
ログ / インシデント対応履歴 / 対処方法
- 他組織との間でデータを突合させる
これって、ウチだけ???



「知見の集約」がキーワード
経営課題としてのセキュリティを意識

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、不正アクセス事例などの高度サイバー攻撃
 - 国際的な教育機関として国内外両方のケースが考えられる
 - 安易にクローズせずに、“原因”や“展開の可能性”など、複数の組織とよく相談することが望ましい
 - 攻撃の初期段階においてたとえ専門機関であっても一般的な情報しか持ち合わせていないこともある

■ 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
- 大学という特殊な環境下でのインシデント対応

大学におけるCIO/CISOの重要性

■ 大学という特殊な環境下でのCSIRTの業務を正しく遂行する上で、経営層の関与は不可欠

- 情報系センタ (管理部門) の立ち位置や「兼務」スタッフ
- 部局よりも弱い立場になりがち
 - 言うことを聞いてくれない、対応が見えない

■ CIO/CISO と情報系センタ (CSIRT) の間で適切にコミュニケーションできていますか？

- 経営層の思いは、現場に伝わっていますか？
- 現場の思いは、経営層に伝わっていますか？
- お互いに伝わらないのが普通。普段からの工夫が不可欠
 - 工夫は大学や、組織形態、担当者により異なる
- お互いに相互信頼・相互信用を心がける

おわりに

■ インシデントは確実に発生している

- ✓ 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には

- ✓ 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めます

■ サイバー攻撃は、対岸の火事ではない

- ✓ 「**ウチは狙われない**」という意識を捨ててください。
- ✓ 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
- <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>