企業における
サイバーセキュリティ対策について

National
Cyber
Training
Center

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター
花田 智洋 (Tomohiro Hanada)

2023/09/29

スピーカー

- 氏名: 花田 智洋 (Tomohiro Hanada)
- 勤務先: 2017年1月～現在
  - NICTサイバーセキュリティ研究所
    ナショナルサイバートレーニングセンター(通称: ナショトレ)
  - CYDER, RPCI, SecHack365,
    CYDERANGE開発等の事業に携わる
- 前職: ～2016年12月末
  - 銀行システム担当のプロジェクトマネージャー
- 業務外活動:
  - 情報セキュリティコミュニティ運営(2006-現在)
  - SECCON実行委員長(2018-2022), 副実行委員長(2023-現在) 他

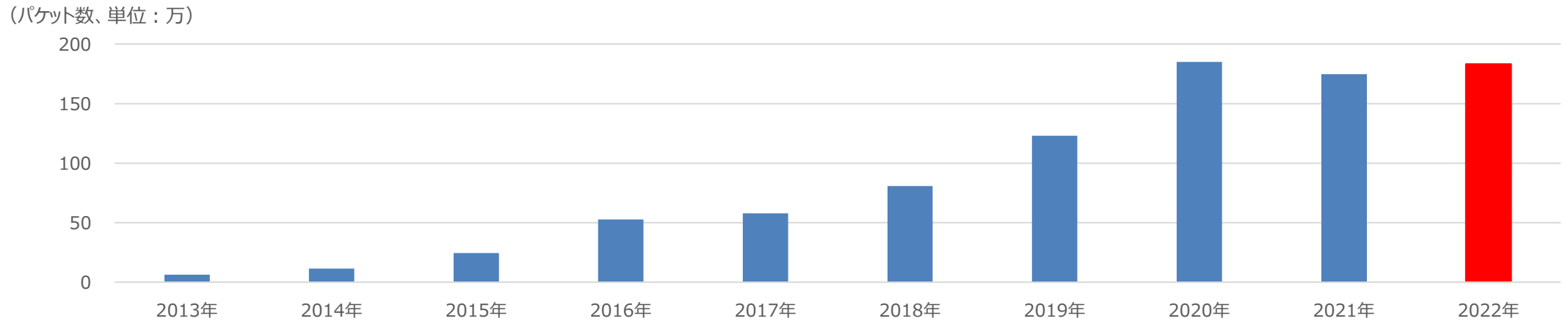
PMP CISSP CompTIA CTT+ CERTIFIED

トレンドとキーワードで確認する最近のセキュリティ動向

NICTERダークネット観測統計(過去10年)

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2013	約128.8億	209,174	63,682
2014	約241.0億	212,878	115,335
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	**約5,226億**	**288,042**	**1,833,012**

1アドレスあたり
17秒に1回
攻撃関連通信受信



1 IPアドレス当たりの年間総観測パケット数

最近のセキュリティトレンド

#	情報セキュリティ10大脅威 2023 個人	情報セキュリティ10大脅威 2023 組織	サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023年4月～6月]	情報セキュリティ安心相談窓口の相談状況 2023年第2四半期(4月～6月)	情報セキュリティ監査人が選ぶ情報セキュリティ十大トレンド（2023年予測）
1	フィッシングによる個人情報等の詐取	ランサムウェアによる被害	3 ビジネスメール詐欺（BEC）の攻撃事例	(ⅰ)「ウイルス検出の偽警告」に関する相談	大規模社会インフラシステム障害により増大するサイバーリスク
2	ネット上の誹謗・中傷・デマ	サプライチェーンの弱点を悪用した攻撃	3.1 海外関連会社を狙った電話を併用する攻撃	(ⅱ)「宅配便業者・通信事業者・公的機関をかたる偽SMS」に関する相談	ITサプライチェーンの統制強化
3	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	標的型攻撃による機密情報の窃取	3.2 偽造文書を使い海外取引先を狙った攻撃	(ⅲ)「不正ログイン」に関する相談	サイバーランサムによってあぶりだされる「怠け者システム管理者」や「ダメ経営者」
4	クレジットカード情報の不正利用	内部不正による情報漏えい	4 2つのCEO詐欺の続報	(ⅳ)「暗号資産（仮想通貨）で金銭を要求する迷惑メール」に関する相談	クラウド障害による社会的影響の拡大
5	スマホ決済の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃	4.1 複数組織へ行われたCEOを詐称する一連の攻撃	(ⅴ)「ワンクリック請求」に関する相談	要注意！大事故につながるクラウドサービスのユーザ設定不備
6	不正アプリによるスマートフォン利用者への被害	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	4.2「日本語化（多言語化）」されたCEO詐欺の攻撃	(ⅵ)「Emotet」ウイルスに関する相談	働き方改革に追いつかない組織管理
7	偽警告によるインターネット詐欺	ビジネスメール詐欺による金銭被害	-	-	待ったなし！中小企業のセキュリティ対策
8	インターネット上のサービスからの個人情報の窃取	脆弱性対策の公開に伴う悪用増加	-	-	ディープフェイク等高度化する虚偽情報を使ったネット詐欺に要注意
9	インターネット上のサービスへの不正ログイン	不注意による情報漏えい等の被害	-	-	経済安全保障上の観点からも重要なサイバー攻撃対策
10	ワンクリック請求等の不正請求による金銭被害	犯罪のビジネス化（アンダーグラウンドサービス）	-	-	オープンソースソフトウェアの脆弱性懸念に対するSBOM普及の期待
	情報セキュリティ10大脅威 2023	情報セキュリティ10大脅威 2023	サイバー情報共有イニシアティブ J-CSIP（ジェイシップ）について	情報セキュリティ安心相談窓口公開レポート	監査人の警鐘- 2023年 情報セキュリティ十大トレンド
	2023/1/25	2023/1/25	2023/8/22	2023/7/20	2023/1/6

最近の報道されたインシデント事例

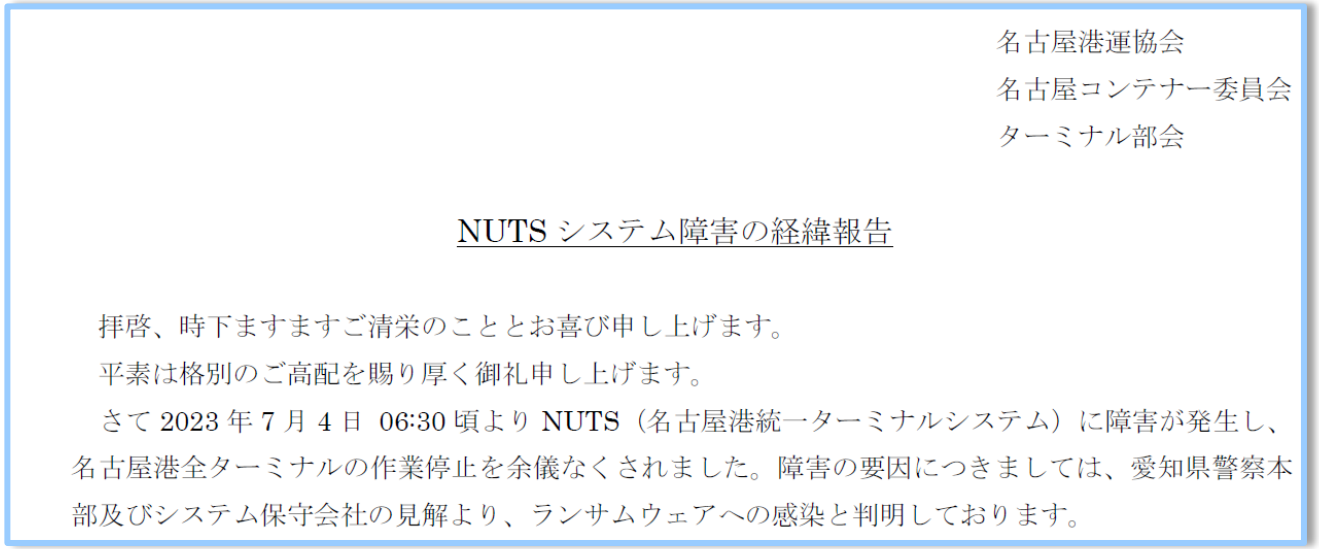
#	報道年月	対象	情報源(同一事案の複数情報ソースを登録する場合有り)	メモ(時々並べ替えします)
7	9月-23	民間企業	当院における個人情報漏えいについて｜お知らせ｜日本大学医学部附属板橋病院：Nihon University Itabashi Hospital https://www.itabashi.med.nihon-u.ac.jp/news/post/735	意図しない情報公開(クラウドと思われる)
8	9月-23	民間企業	【セキュリティ ニュース】患者情報含むファイルがネット上で閲覧可能に - 日大板橋病院（1ページ目 / 全1ページ）：Security NEXT https://www.security-next.com/149617	意図しない情報公開(クラウドと思われる)
9	9月-23	地方公共団体	業務用携帯電話等の一時紛失｜東京都 https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2023/09/19/03.html	携帯電話紛失
10	9月-23	地方公共団体	【セキュリティ ニュース】飲酒後に携帯電話を鞄ごと置き忘れ、翌日回収 - 都教育支援機構 https://www.secu	携帯電話紛失
11	9月-23	地方公共団体	個人情報が閲覧 https://www.town abi.pdf	
12	9月-23	地方公共団体	【山形】大石田 くらんぼテレビ) https://news.yah f16	
13	9月-23	地方公共団体	【セキュリティ に - 大石田町（1 https://www.secu	
14	9月-23	地方公共団体	消防職員の処分 https://www.city.a s/20230904shou	
			【セキュリティ	

#	報道年月	対象	情報源(同一事案の複数情報ソースを登録する場合有り)	メモ(時々並べ替えします)
60	9月-23	民間企業	コクヨグループへのランサムウェア攻撃、商品直送サービス委託のアスクルにも影響	ScanNetSecurity https://scan.netsecurity.ne.jp/article/2023/09/19/49965.html	ランサムウェア
61	9月-23	民間企業	当社グループが管理するサーバへの不正アクセスについて https://www.alpsalpine.com/cms.media/20230914_Cyber_Attack_Update2_476681e12a.pdf	ランサムウェア
62	9月-23	民間企業	当社グループが管理するサーバへの不正アクセスについて（第２報） https://www.alpsalpine.com/cms.media/20230912_Cyber_Attack_J_104fbf84ee.pdf	ランサムウェア
63	9月-23	民間企業	アルプスアルパイングループ管理サーバにランサムウェア攻撃、生産・出荷等に影響	ScanNetSecurity https://scan.netsecurity.ne.jp/article/2023/09/20/49971.html	ランサムウェア
64	9月-23	民間企業	弊社と雇用関係にあった方へ｜ソフマップ(Sofmap) https://www.sofmap.co.jp/news/2023/130	エムケイシステム
65	9月-23	民間企業	エムケイシステムへのランサムウェア攻撃、ソフマップと雇用関係にあった者の個人情報も漏えい可能性を完全に否定できず	ScanNetSecurity https://scan.netsecurity.ne.jp/article/2023/09/14/49950.html	エムケイシステム
66	9月-23	民間企業	Microsoft、パスワードを含む38テラバイトの情報漏えいの可能性	TECH+（テックプラス）	

スピーカーが個人でまとめている
最近のインシデント事例メモ抜粋
※直近の2023年9月報道分

インシデント事例ピックアップ＃1

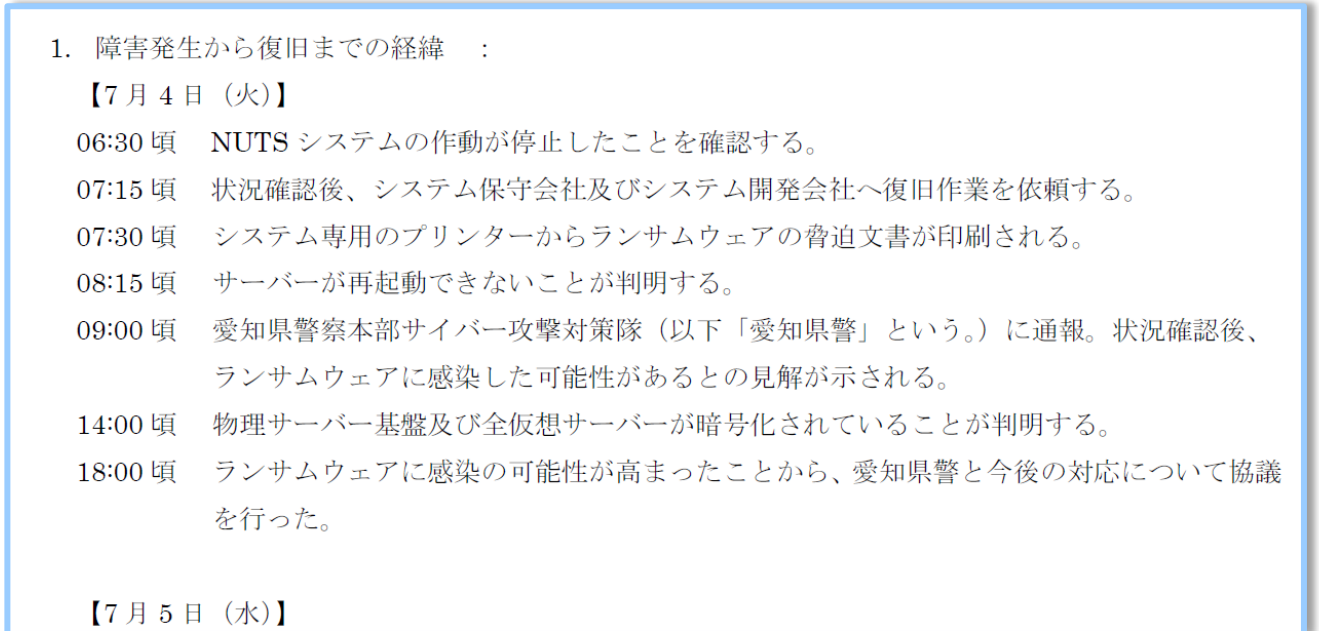
（お知らせ）名古屋港コンテナターミナル利用者様各位 | 名古屋港運協会
https://meikoukyo.com/archives/3336



名古屋港運協会
名古屋コンテナー委員会
ターミナル部会

NUTS システム障害の経緯報告

拝啓、時下ますますご清栄のこととお喜び申し上げます。
平素は格別のご高配を賜り厚く御礼申し上げます。
さて 2023 年 7 月 4 日 06:30 頃より NUTS（名古屋港統一ターミナルシステム）に障害が発生し、名古屋港全ターミナルの作業停止を余儀なくされました。障害の要因につきましては、愛知県警察本部及びシステム保守会社の見解より、ランサムウェアへの感染と判明しております。



1. 障害発生から復旧までの経緯　：

【7 月 4 日（火）】

06:30 頃　NUTS システムの作動が停止したことを確認する。
07:15 頃　状況確認後、システム保守会社及びシステム開発会社へ復旧作業を依頼する。
07:30 頃　システム専用のプリンターからランサムウェアの脅迫文書が印刷される。
08:15 頃　サーバーが再起動できないことが判明する。
09:00 頃　愛知県警察本部サイバー攻撃対策隊（以下「愛知県警」という。）に通報。状況確認後、ランサムウェアに感染した可能性があるとの見解が示される。
14:00 頃　物理サーバー基盤及び全仮想サーバーが暗号化されていることが判明する。
18:00 頃　ランサムウェアに感染の可能性が高まったことから、愛知県警と今後の対応について協議を行った。

【7 月 5 日（水）】

最新動向のピックアップ＃1

警察庁
National Police Agency

› English › 国家公安委員会 › サイトマップ

警察庁について　お知らせ　政策　法令

ホーム › 各部局から › サイバー警察局 › 注意喚起 › 中国を背景とするサイバー攻撃グループBlackTechによ

中国を背景とするサイバー攻撃グループ BlackTechによるサイバー攻撃について

警察庁及び内閣サイバーセキュリティセンター（NISC）は、米国家安全保障局（NSA）、米連邦捜査局（FBI）及び米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）とともに、中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出しました。

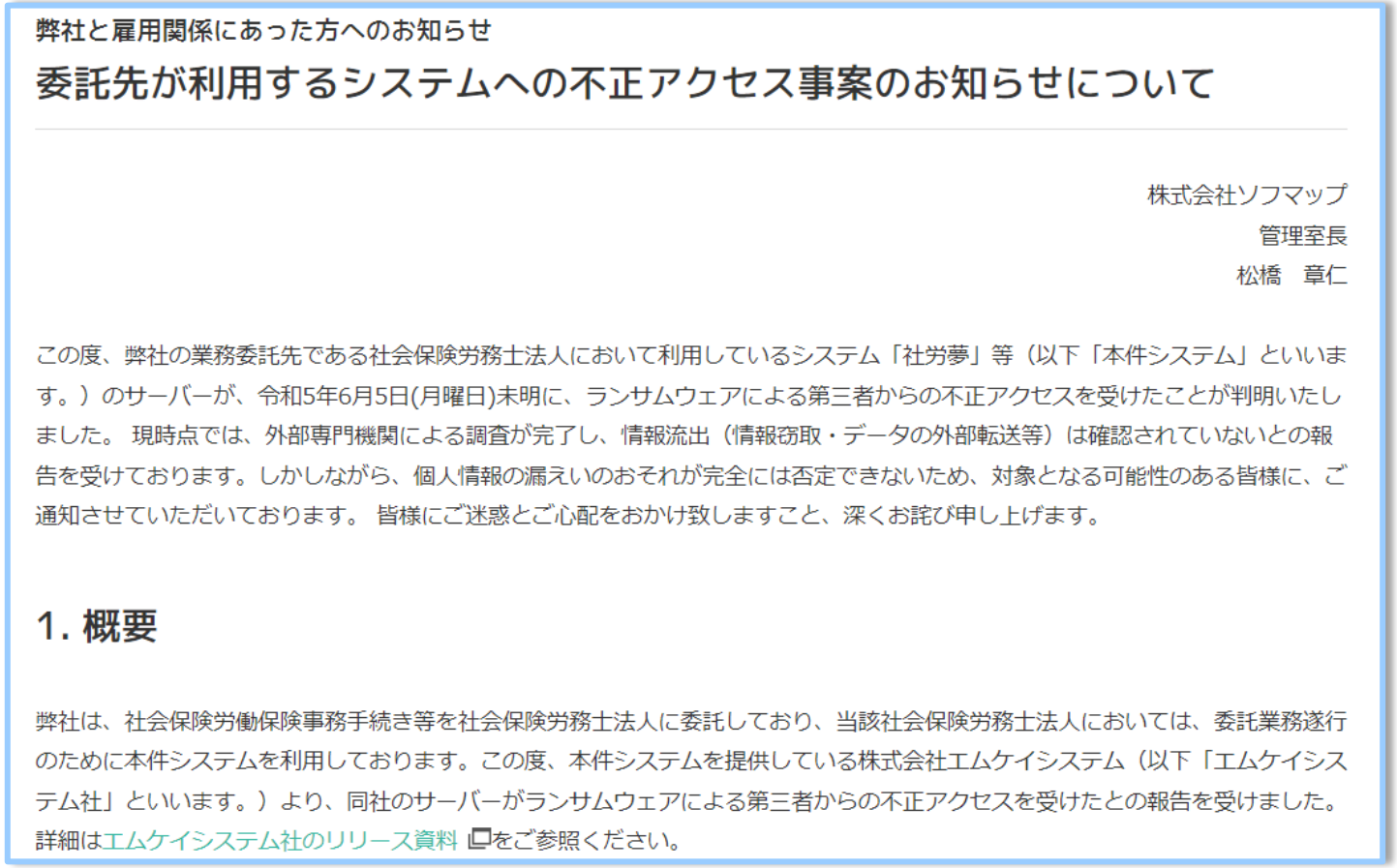
中国を背景とするサイバー攻撃グループBlackTechによるサイバー攻撃について（注意喚起）

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

中国を背景とするサイバー攻撃グループBlackTechによるサイバー攻撃について｜警察庁Webサイト
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20230927.html
中国を背景とするサイバー攻撃グループ 警察庁などが注意喚起｜NHK｜サイバー攻撃
https://www3.nhk.or.jp/news/html/20230928/k10014208601000.html

2023/09/27公開

インシデント事例ピックアップ#2



弊社と雇用関係にあった方へのお知らせ

委託先が利用するシステムへの不正アクセス事案のお知らせについて

株式会社ソフマップ
管理室長
松橋　章仁

この度、弊社の業務委託先である社会保険労務士法人において利用しているシステム「社労夢」等（以下「本件システム」といいます。）のサーバーが、令和5年6月5日(月曜日)未明に、ランサムウェアによる第三者からの不正アクセスを受けたことが判明いたしました。 現時点では、外部専門機関による調査が完了し、情報流出（情報窃取・データの外部転送等）は確認されていないとの報告を受けております。しかしながら、個人情報の漏えいのおそれが完全には否定できないため、対象となる可能性のある皆様に、ご通知させていただいております。 皆様にご迷惑とご心配をおかけ致しますこと、深くお詫び申し上げます。

1. 概要

弊社は、社会保険労働保険事務手続き等を社会保険労務士法人に委託しており、当該社会保険労務士法人においては、委託業務遂行のために本件システムを利用しております。この度、本件システムを提供している株式会社エムケイシステム（以下「エムケイシステム社」といいます。）より、同社のサーバーがランサムウェアによる第三者からの不正アクセスを受けたとの報告を受けました。詳細はエムケイシステム社のリリース資料 をご参照ください。

エムケイシステムへのランサムウェア攻撃、ソフマップと雇用関係にあった者の個人情報も漏えい可能性を完全に否定できず｜ScanNetSecurity https://scan.netsecurity.ne.jp/article/2023/09/14/49950.html
弊社と雇用関係にあった方へ｜ソフマップ(Sofmap) https://www.sofmap.co.jp/news/2023/130

インシデント事例ピックアップ#3

和歌山県 九度山町 KUDOYAMA TOWN
美しい九度山 歴史に生きる町
背景色 白 青 黒 文字サイズ 小 中 大
HOME | くらし・手続き | 健康・医療・福祉 | 子育て・教育・文化 | 産業・町づくり | 防
HOME > 総務課 > 個人情報を含む書類の紛失について

個人情報を含む書類の紛失について

この度、九度山町職員において和歌山県下水道協会（以下「協会」という。）が開催する和歌山県下水道排水設備工事責任技術者の試験等運営委員会（以下「委員会」という。）に出席した際、会議にて配布された資料のうち、191名の個人情報が記載された和歌山県下水道排水設備工事責任技術者更新講習対象者リスト（以下「リスト」という。）を、開催会場である和歌山市勤労者総合センター（以下「会場」という。）内外にて紛失するという事案が発生しました。

関係者の皆様には多大なるご心配とご迷惑をおかけすることとなり、心よりお詫び申し上げます。詳細につきましては、下記のとおりご報告致します。

1．概要

令和５年７月７日（金曜日）、協会が開催する委員会にてリストを含む関係資料一式を受け取り、会議終了後

個人情報を含む書類の紛失について｜九度山町 https://www.town.kudoyama.wakayama.jp/soumu/2023-0801-1506-38.html
【セキュリティ ニュース】個人情報含む技術者講習対象者リストを紛失 - 九度山町（1ページ目 / 全1ページ） ：Security NEXT
https://www.security-next.com/148388

最新動向のピックアップ#2

能動的サイバー防御

- 日本政府が2022年12月
  新たな国家安全保障戦略の1つとして導入を発表
  - 「国家安全保障戦略」「国家防衛戦略」「防衛力整備計画」
- アクティブ・サイバー・ディフェンス(active cyber defence)
  - 被害に遭う前に攻撃を「無害化」

被害に遭う前に攻撃を「無害化」、常識覆す能動的サイバー防御とは何か | 日経クロステック（xTECH）
https://xtech.nikkei.com/atcl/nxt/column/18/02559/082300001/
「能動的サイバー防御」導入へ　背景と課題 NHK解説委員室 https://www.nhk.or.jp/kaisetsu-blog/100/486718.html
「能動的サイバー防御」は効果があるのか？ ～注目が集まるoffensiveなオペレーションの考察～ - JPCERT/CC Eyes | JPCERT コーディネーションセンター公式ブログ https://blogs.jpcert.or.jp/ja/2023/08/effectiveness-of-active-cyber-defense.html

やらかす？やられる？

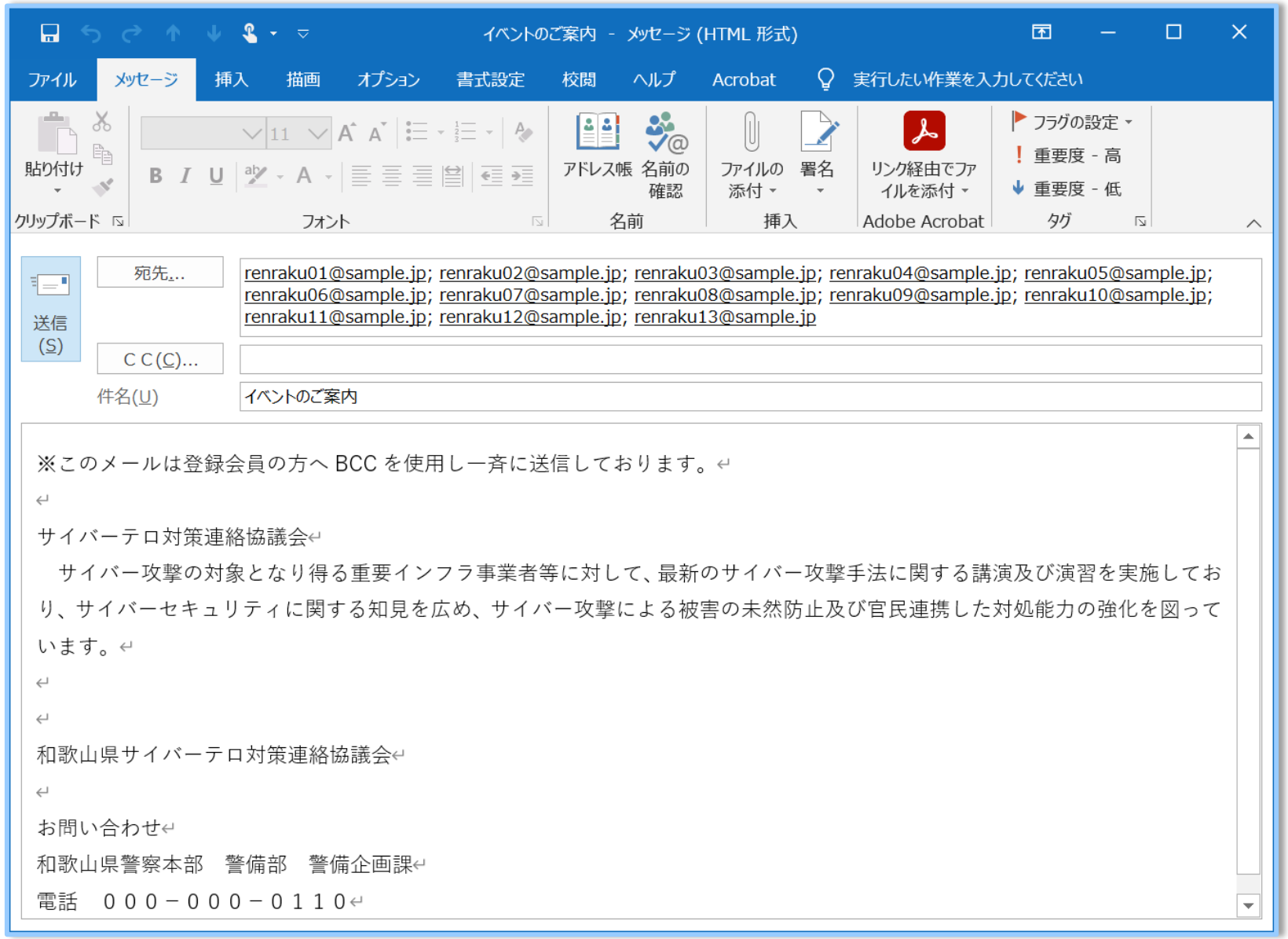
サイバー攻撃、セキュリティインシデントは

突然発生する。

- 忙しい
- 手が回らない
- 人が足りない
- 期限が迫っている
- もっと支援が欲しい
- …


せかいたいせ
個人情報
攻撃受けなす

とあるメール例



イベントのご案内 - メッセージ (HTML 形式)

ファイル　メッセージ　挿入　描画　オプション　書式設定　校閲　ヘルプ　Acrobat　実行したい作業を入力してください

貼り付け　クリップボード　フォント　アドレス帳　名前の確認　名前　ファイルの添付　署名　挿入　リンク経由でファイルを添付　Adobe Acrobat　フラグの設定　重要度 - 高　重要度 - 低　タグ

送信 (S)

宛先...　renraku01@sample.jp; renraku02@sample.jp; renraku03@sample.jp; renraku04@sample.jp; renraku05@sample.jp; renraku06@sample.jp; renraku07@sample.jp; renraku08@sample.jp; renraku09@sample.jp; renraku10@sample.jp; renraku11@sample.jp; renraku12@sample.jp; renraku13@sample.jp

C C(C)...

件名(U)　イベントのご案内

※このメールは登録会員の方へ BCC を使用し一斉に送信しております。

サイバーテロ対策連絡協議会

　サイバー攻撃の対象となり得る重要インフラ事業者等に対して、最新のサイバー攻撃手法に関する講演及び演習を実施しており、サイバーセキュリティに関する知見を広め、サイバー攻撃による被害の未然防止及び官民連携した対処能力の強化を図っています。

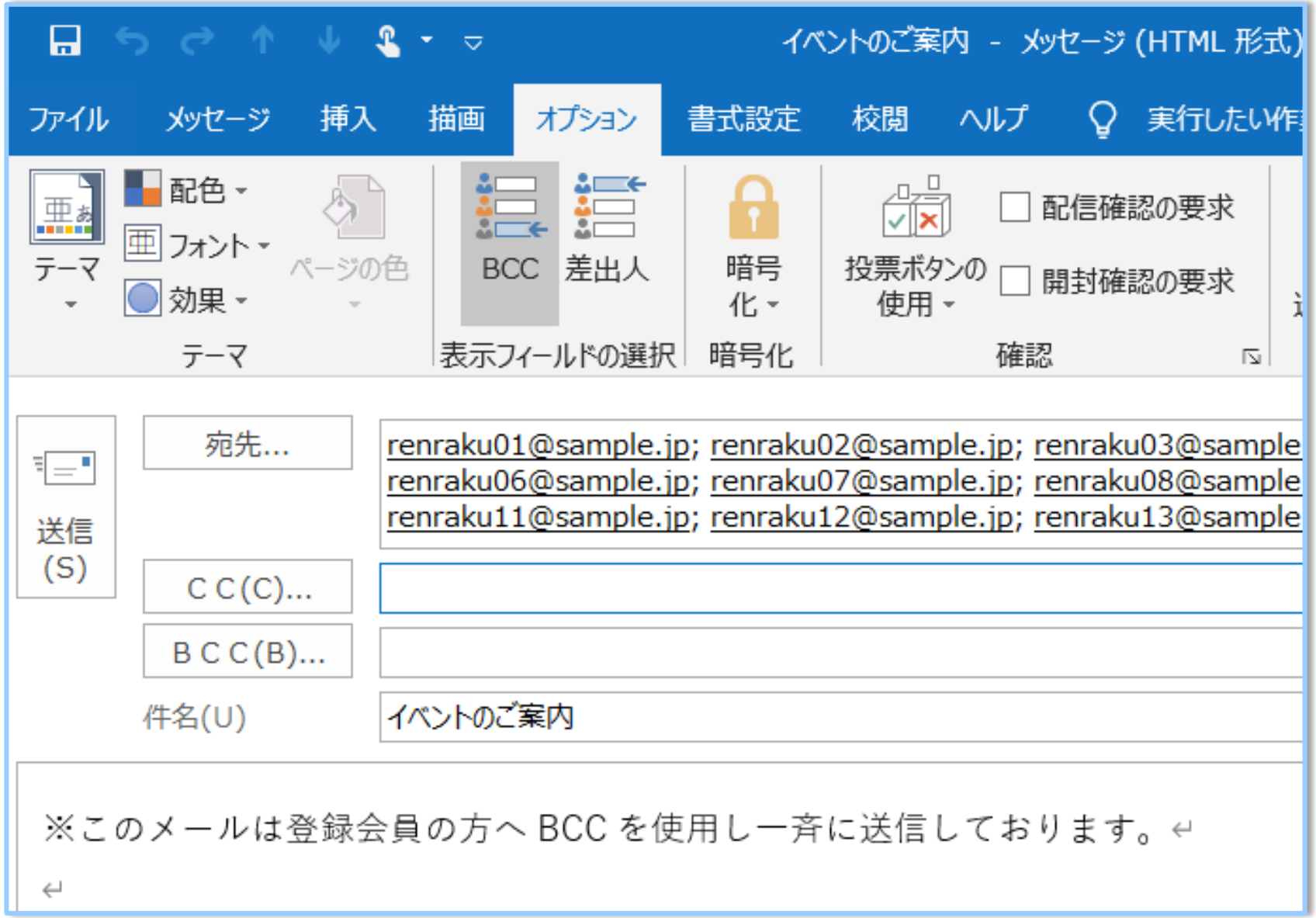
和歌山県サイバーテロ対策連絡協議会

お問い合わせ

和歌山県警察本部　警備部　警備企画課

電話　０００－０００－０１１０

とあるメール例


イベントのご案内 - メッセージ (HTML 形式)
ファイル
メッセージ
挿入
描画
オプション
書式設定
校閲
ヘルプ
実行したい作
テーマ
配色
フォント
効果
ページの色
BCC
差出人
暗号化
投票ボタンの使用
配信確認の要求
開封確認の要求
テーマ
表示フィールドの選択
暗号化
確認
送信(S)
宛先...
renraku01@sample.jp; renraku02@sample.jp; renraku03@sample
renraku06@sample.jp; renraku07@sample.jp; renraku08@sample
renraku11@sample.jp; renraku12@sample.jp; renraku13@sample
C C(C)...
B C C(B)...
件名(U)
イベントのご案内
※このメールは登録会員の方へ BCC を使用し一斉に送信しております。

最近の報道されたインシデント事例 から見た 原因の例

やらかす

- BCCメール失敗
- 紛失
- 設定誤り

やられる

- 不正アクセス
- 引っかかる、騙される

やらかす？

原因分析はしっかり行えているか

- なぜなぜ分析(5 Whys)
- 根本原因の例
  - 理解不足・確認不足、不慣れ・経験不足、慣れ・過信・慢心、プロセス、組織・体制、情報伝達、環境 等
- 根本原因を追求できない組織風土になっていないか

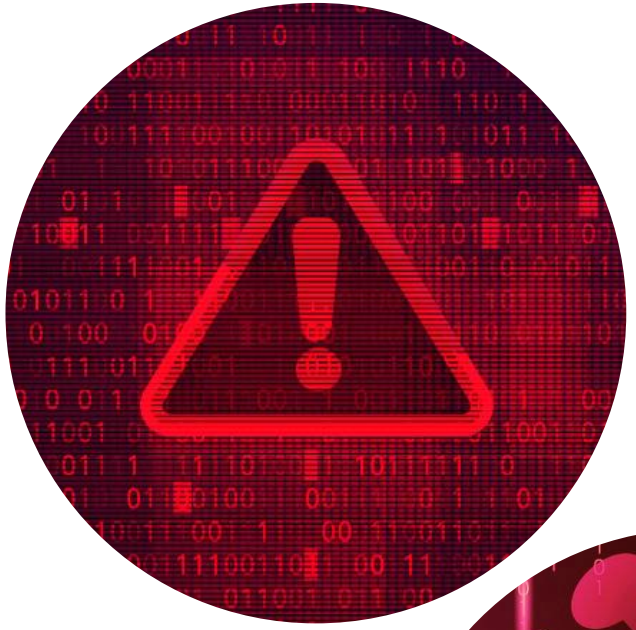
再発防止策

- 「再発」が本当に防止できるか
- NG: 根性論、頑張ります、スローガン

やられる？

サイバー攻撃経路例:

- メール
- USBメモリ、外部記憶媒体
- Web, ドライブバイダウンロード
- リモートアクセス、リモートエクスプロイト
- 汚染ソフトウェア、アプリ
- 持ち込み機器、持ち出しPC
- サポート詐欺　等



サイバー攻撃の分類

おおまかに

- 直接的な攻撃
- 詐欺的な攻撃

直接的な攻撃の例

外部向けWebサービスを例に

- ページ内容を書き換えられてしまう
- 登録ユーザーのデータを抜き取られてしまう
- 登録ユーザーのデータを悪用されてしまう
  - 成りすましで酷い書き込み、個人の住所の特定、他人を罠にはめて金銭的被害など
- 登録ユーザーのデータを破壊されてしまう
- 使用不能にされてしまう

詐欺的な攻撃の例

- 調達品を仕入れようと検索で探し当てたサイトで購入したら、実は詐欺サイトだった

- DMで「セキュリティ侵害があったので急いでURLをクリックして解除を…」と届く

- SMS(ショートメッセージ)で「ヤマト運輸ですがご不在だったので荷物持ち帰りました。再配送ご希望の場合はURL…」と届く

詐欺的な攻撃のねらい

- 悪者が感染させたい添付ファイルを開かせようとする
- 悪者がクリックしてほしいリンクを開かせようとする
- 検索結果から罠に嵌めようとする手口
  - Webサイト丸ごと成りすまし(フィッシング)
  - 専門家でも見分けることが難しいほどの巧妙化

- 関連分野のニュースを毎日チェックしていたとしても、
<u>引っかかる可能性はゼロではない</u>
- もはや「十分気をつけて引っかからないようにしましょう」というのは無理

BCP有無が明暗を分ける

[事例]秋田県建設・工業技術センター(2022)

- BCP(業務継続計画)を策定していなかった
- メール機能が回復するまで数ヶ月を要した

[事例]つるぎ町立半田病院(2021)

- 災害時診療を前提としたBCPを策定済みだった
  →ただし、サイバー系BCPは策定されていなかったため、電子カルテの復旧(再稼働)には2ヶ月以上かかった
- 被害発覚後数日で診療再開

サイバー攻撃を想定したBCPが必要な段階になってきている

BCPと共に必要なもの

サイバーインシデント(事件・事案)への緊急対応力

- 業務継続と同時に原因追及
  - 原因がわからなければ再発する可能性がある
- 被害に遭ったコンピューターは2次攻撃マシンになる可能性
  - 要緊急隔離：どうやって切り離すか
- 警察に捜査依頼するなら証拠保全が必要
- 専門家との連携
- BCPでは想定しえなかった事態への対応

参考

サイバー攻撃によるインシデントの例

- アクセスを集中させて Web ページ閲覧などを不可能にしてしまうDoS攻撃(Denial of Service attack)
- コンピューターウイルス(マルウェア)と感染後ファイル群を暗号化して身代金を要求するランサムウェア攻撃
- 業務上のメール等を装って金銭を騙し取るビジネスメール詐欺(BEC)
- サーバーの脆弱性等を悪用してIDやパスワードの入力を回避し、勝手にデータを盗み出したり破壊したりする攻撃

インシデントへの初動対応

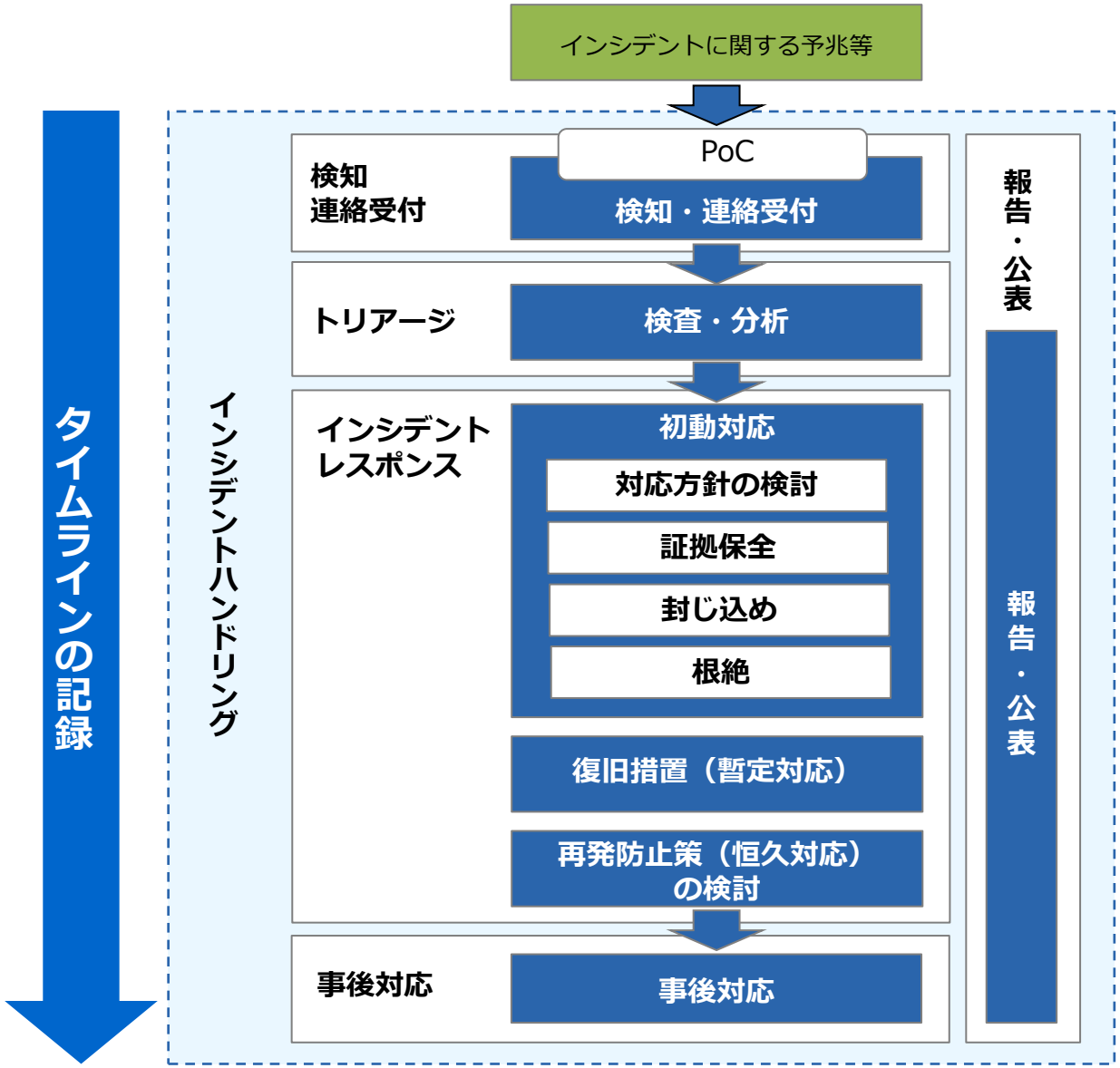
第一報の受領、分析、確認、優先順位付け等

初動対応の影響は大きい

- 適切な対応、優先順位か
- 組織の方針に則っているか

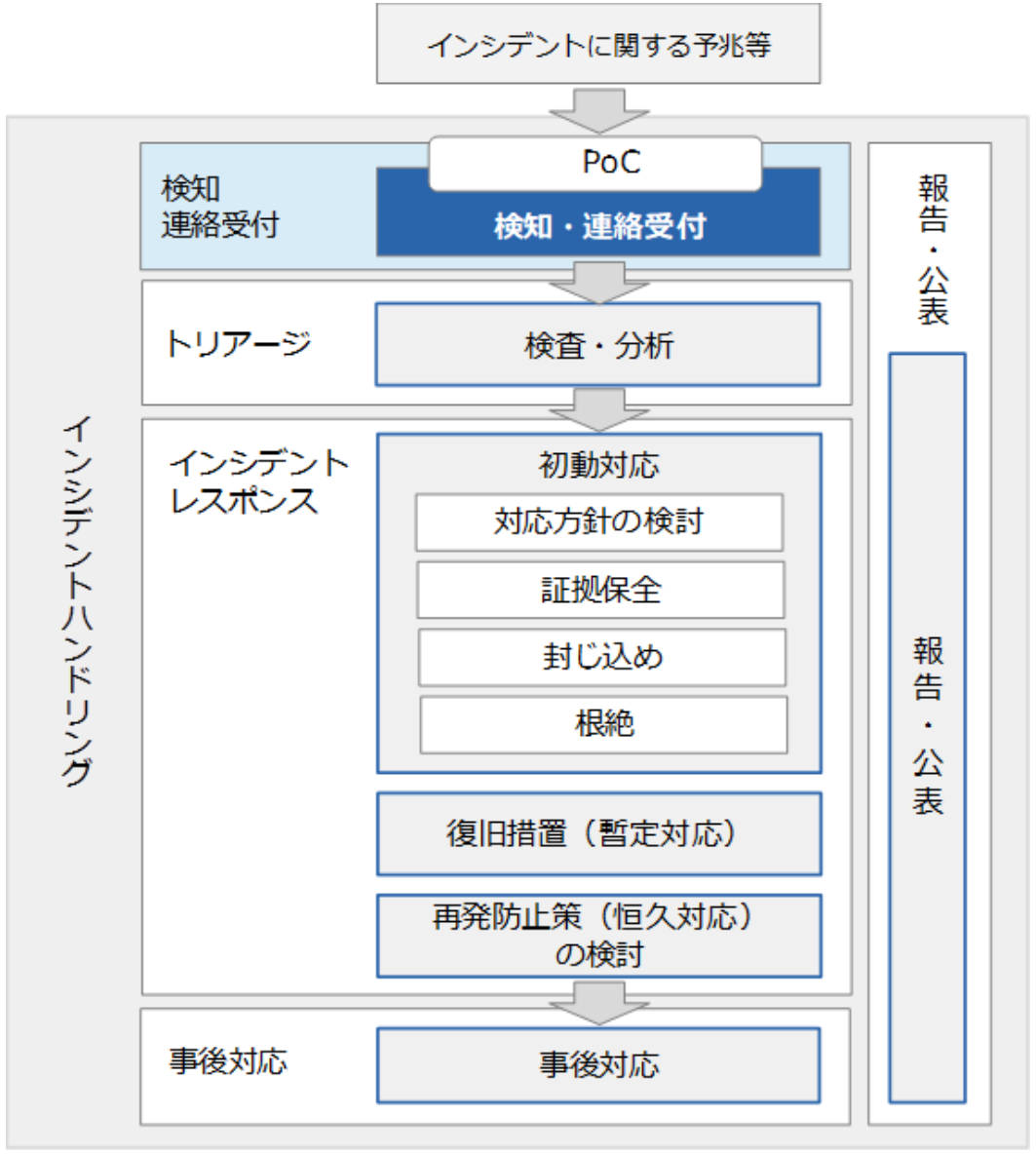
初期の判断の誤りを訂正するコストは
時間経過とともに増大します

インシデントハンドリングの流れ



※実際のインシデントハンドリングにおいては、
各組織のルールに則った対応をしてください。

初動対応: 検知・連絡受付



- **<u>初動対応ミスからのリカバリーは、プロセスが進むほど大変</u>**になります。
- 早い段階で必要な知識を仕入れ、判断に活かすことでミスを防ぐ確率を高めます。
- 実際のハンドリング時には、予想外の突発事が起きることもあるので、**<u>踏んだ場数が重要</u>**になってきます。

初動対応のポイント

事前

- どこから専門家に任せるか決めておく、任せ方を手順化しておく
- 攻撃被害に遭ったらどうするか、シミュレーションしておく

事後

- 情報の確からしさを確認しながら着実に進む
- 優先順位決めの基本方針を合意しておく

ベンダーや他組織との関わり

対応すべてを自組織で実施できる

- ・・・そんな組織はほとんど無い

ベンダーや専門家がやっていること、言っていることを

- 理解できるか
- 評価できるか

参考

初動対応のサンプル事例

状況説明

現在2023/9/29 15:02です。

職員伊藤からCSIRTのPoCに、なりすましと思われるメールを受信したという一通の連絡メールが届きました。

■連絡メール（抜粋）

今朝、私のメールボックスに情報通信研究機構の花田さんという方からのメールが届きました。しかし、私はこの方とは面識がない上に、本文の文面に不自然な日本語が多いなど、不審な点が見られるため、念のためお知らせしました。

課題

この通報に対して どのような対応を取るべきか まとめてください。

注意喚起

職員の伊藤さんはなぜ気付けたのか

伊藤さんと同じメールが来ていたらどうすれば良いか

- (一般論として)メールに添付されたファイルを不用意に開かない
- (一般論として)メールに記述されているリンクを不用意にアクセスしない
- 手元に類似するメールが来た場合はCSIRTへ通報

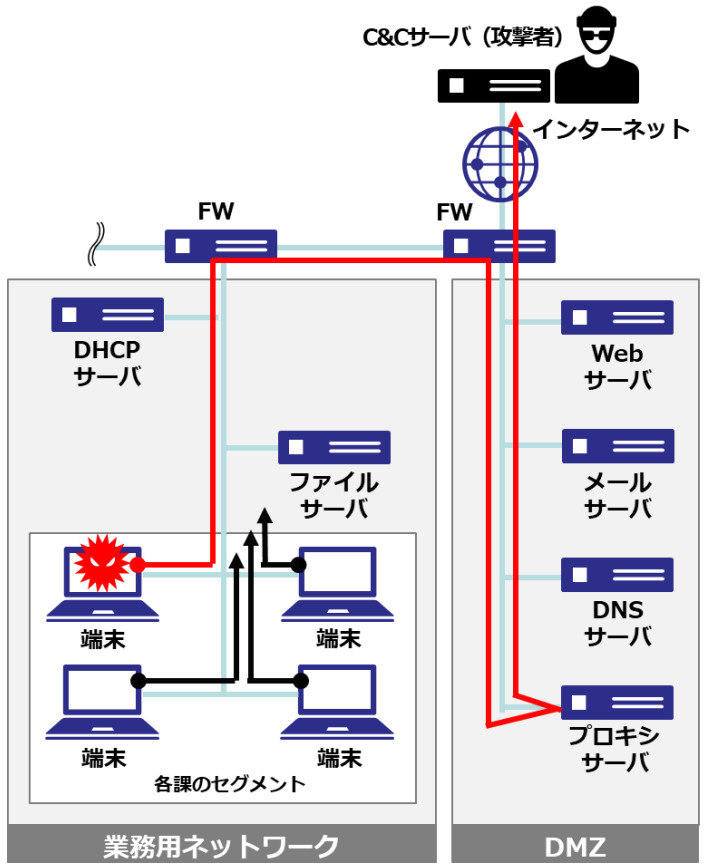
注意喚起の発信で気をつけるべき点は？

- 偽物では無い、正式な注意喚起かどうか
- URL等そのまま伝えない(ヒューマンエラー防止)

参考

ログ調査

C&Cサーバーと通信してしまっている端末を突き止める



192.168.1.102 - - [14/May/2019:15:48:25 +0900] “GET http://cyder.nict.go.jp/ HTTP/1.1“ 200 72428 477 ”http://www.nict.go.jp/” “Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:60.0) Gecko/20100101 Firefox/60.0” TCP_MISS:HIER_DIRECT　（ログサンプル）

- 192.168.1.102＝端末に割り振られたIPアドレス
- +0900＝世界標準時との時差(JST)
- http://cyder.nict.go.jp/
  ＝通信相手(Webページデータを取りに行くWebサーバー)
- 200＝ステータスコード(正常に取得できた)
- 72428＝取得したデータのサイズ(バイト)

access.log - メモ帳

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

```
10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
TCP_TUNNEL:HIER_DIRECT
192.168.110.141 - - [10/Jun/2019:11:15:11 +0900] "CONNECT www.rakuten.ne.jp:443 HTTP/1.1" 200 86063 221 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36
Edge/14.14393" TCP_TUNNEL:HIER_DIRECT
192.168.110.105 - - [10/Jun/2019:11:15:11 +0900] "CONNECT www.youtube.com:443 HTTP/1.1" 200 842437 217 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
TCP_TUNNEL:HIER_DIRECT
192.168.110.115 - - [10/Jun/2019:11:15:1                                                                    1309 679
"http://5pb.jp/games/topics/3134.html"                                                                      /537.36 (KHTML, like
Gecko) Chrome/51.0.2704.79 Safari/537.3
192.168.110.141 - - [10/Jun/2019:11:15:                                                                     tisements.jsonp?
HTTP/1.1" 200 1366 963 "http://live.nic                                                                     64; ServiceUI 8)
AppleWebKit/537.36 (KHTML, like Gecko)                                                                      CT
192.168.110.141 - - [10/Jun/2019:11:15:                                                                     vertisements.jsonp?
HTTP/1.1" 200 1176 960 "http://live.nic                                                                     64; ServiceUI 8)
AppleWebKit/537.36 (KHTML, like Gecko)                                                                      CT
192.168.110.141 - - [10/Jun/2019:11:15:1                                                                    HTTP/1.1" 200 535 904
"http://live.nicovideo.jp/watch/lv45847829" "Mozilla/                                                       T 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14                                                    SS:HIER_DIRECT
192.168.110.123 - - [10/Jun/2019:11:15:11 +0900] "POST http://                                              igicert.com/ HTTP/1.1" 200 910 478 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like                                           cko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
TCP_MISS:HIER_DIRECT
192.168.110.110 - - [10/Jun/2019:11:15:12 +0900] "GET http://vulnerability.shop/index/?873292698692 HTTP/1.1" 200 673 806 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36
Edge/14.14393" TCP_MISS:HIER_DIRECT
192.168.110.115 - - [10/Jun/2019:11:15:12 +0900] "CONNECT bidder.criteo.com:443 HTTP/1.1" 200 11144 221 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36
Edge/14.14393" TCP_TUNNEL:HIER_DIRECT
192.168.110.123 - - [10/Jun/2019:11:15:12 +0900] "CONNECT bs.nakanohito.jp:443 HTTP/1.1" 200 736 219 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
TCP_TUNNEL:HIER_DIRECT
192.168.110.141 - - [10/Jun/2019:11:15:12 +0900] "CONNECT bs.nakanohito.jp:443 HTTP/1.1" 200 736 219 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393"
```

膨大なログの中から
不正な通信を見つけ出す

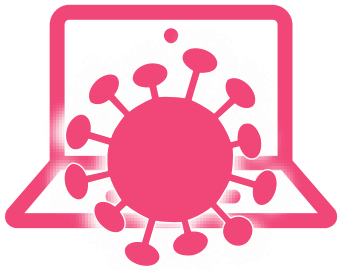
証拠保全とは

- 専門的調査に必要な作業
- 「汚染された」証拠は証拠としての能力が著しく劣化
  - 汚染例:
    - ✓攻撃者による証拠隠滅や改ざん
    - ✓攻撃対象となったサーバーの管理者による新たな行動記録
    - ✓システムの利用者による日常的なシステム利用
    - ✓機器故障による欠損、欠落、消失
- 「汚染された」証拠は証拠データ全体の信用を損なってしまう

サイバー犯罪者向けビジネスモデルの洗練

- プロフェッショナルサービス for サイバー犯罪の台頭
- 質の向上、専門化、分業化
- 仮想通貨によって金銭を(悪人にとって)安全に授受できるようになった

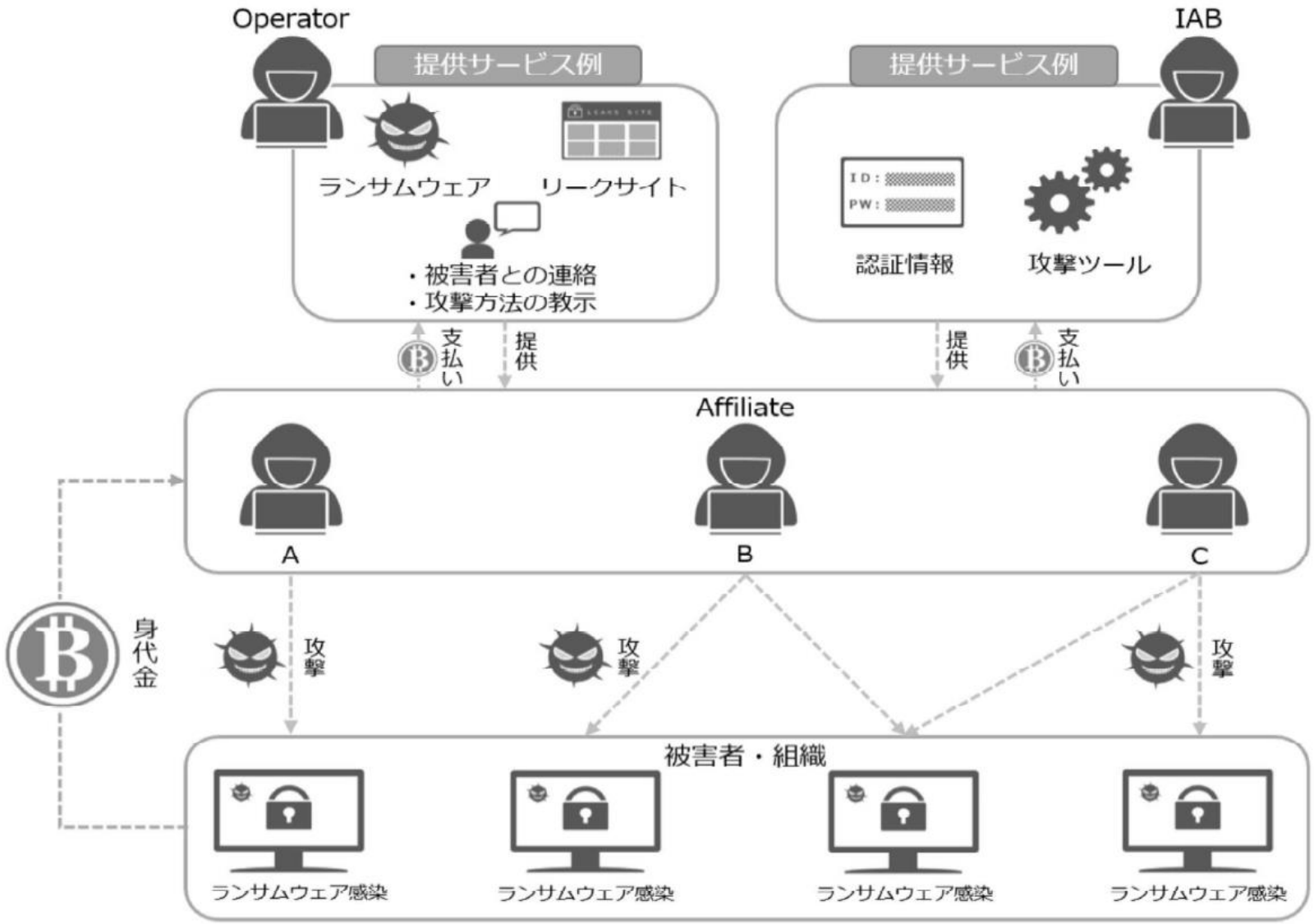
- ランサムウェアの変遷



- 情報を勝手に暗号化し、元に戻して欲しければお金寄越せ
  →情報を勝手に持ち出して例示し、破壊されたくなかったらお金寄越せ

サイバー空間をめぐる脅威の情勢等 | 警察庁Webサイト

【図表38：ランサムウェア等を提供する者と攻撃を実行する者】



2023/09/21公開

IT, ICTシステムを抱えている限り

今や被害に遭うことは不可避

- 「いや、ウチは被害に遭ってないよ？」

今後サービスをICTの力によって拡大していくなら狙われる機会増だろう

どんな業界が狙われているのか

- ビジネスに関する情報のインパクト(＝盗まれたり破壊されたりしたらとても大変なことになる度合い)が大きいのは医療分野
- 自動車系列で工場が止まる、という被害の形も出てきている
- 社会的インパクトが大きい重要インフラが狙われる傾向が強まるのでは
  - 2023年7月：日本の重要インフラが攻撃され、
    コンテナ搬出入作業停止等の港湾物流運営に大きな支障が出た事例
- さらに身代金支払いについての社会的な締め付けもキツくなる

暗号化されてしまったら？

犯人の手を借りずに自前復号できる？

- まず無理。ただ、よほど弱い暗号実装であれば脆弱性を突いて復号することが可能な場合もあるだろう。

バックアップをとってあれば良い？

- バックアップを狙うものもある。バックアップの隔離性というか独立性次第。別媒体、別コンピューター、別ネットワーク、クラウドなど、どこにバックアップデータを置くか
- バックアップサービスを即座に立ち上げor構築できるか

このようなリスクへの対応も含んだBCP(業務継続計画)が重要

通報・相談しやすい環境の整備

【図表28：「サイバー事案の被害の潜在化防止に向けた検討会」報告書概要】

「サイバー事案の被害の潜在化防止に向けた検討会」　報告書概要

背景・課題

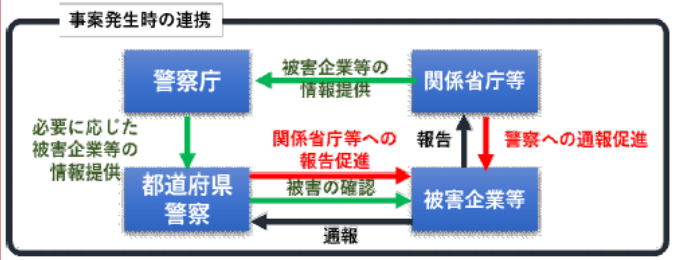
○　サイバー事案に対しては、犯人を検挙して犯行の制圧を迅速に行い、また、被害の拡大防止と未然防止により、その被害が多方面に拡大することを防ぐことが重要。
○　一方で、サイバー事案においては、被害に遭ったことへの引け目や被害者に対する社会的評価の悪化の懸念（レピュテーションリスク）、捜査協力への負担等から被害申告がためらわれるなどの、いわゆる「被害の潜在化」が生じている状況がうかがえる。

今後の方策

関係機関等と連携した通報・相談の促進

○　関係機関等との連携強化

・　被害発生時の被害概要等に関する情報共有
・　関係省庁等からの被害企業等に対する通報・相談の促進



【被害企業等に対する通報・相談の促進のイメージ】

○　サイバー事案の被害に関する報告窓口の一元化

・　被害企業等が届け出る内容や様式の統一化
・　被害者に対する支援等に係る効果的な役割分担の整理、広報

通報・相談しやすい環境の整備

○　被害者に対する積極的な情報発信

・　都道府県警察におけるウェブサイトのコンテンツの改善
・　インターネット上の通報・相談窓口の統一化

【通報・相談窓口の統一化のイメージ】

○　高齢者や青少年等に対する広報啓発活動

・　携帯電話事業者等と協力したスマートフォン契約者への注意喚起
・　老人クラブ、学校、運転免許センター等における広報・啓発　等

○　警察における対応改善に向けた取組

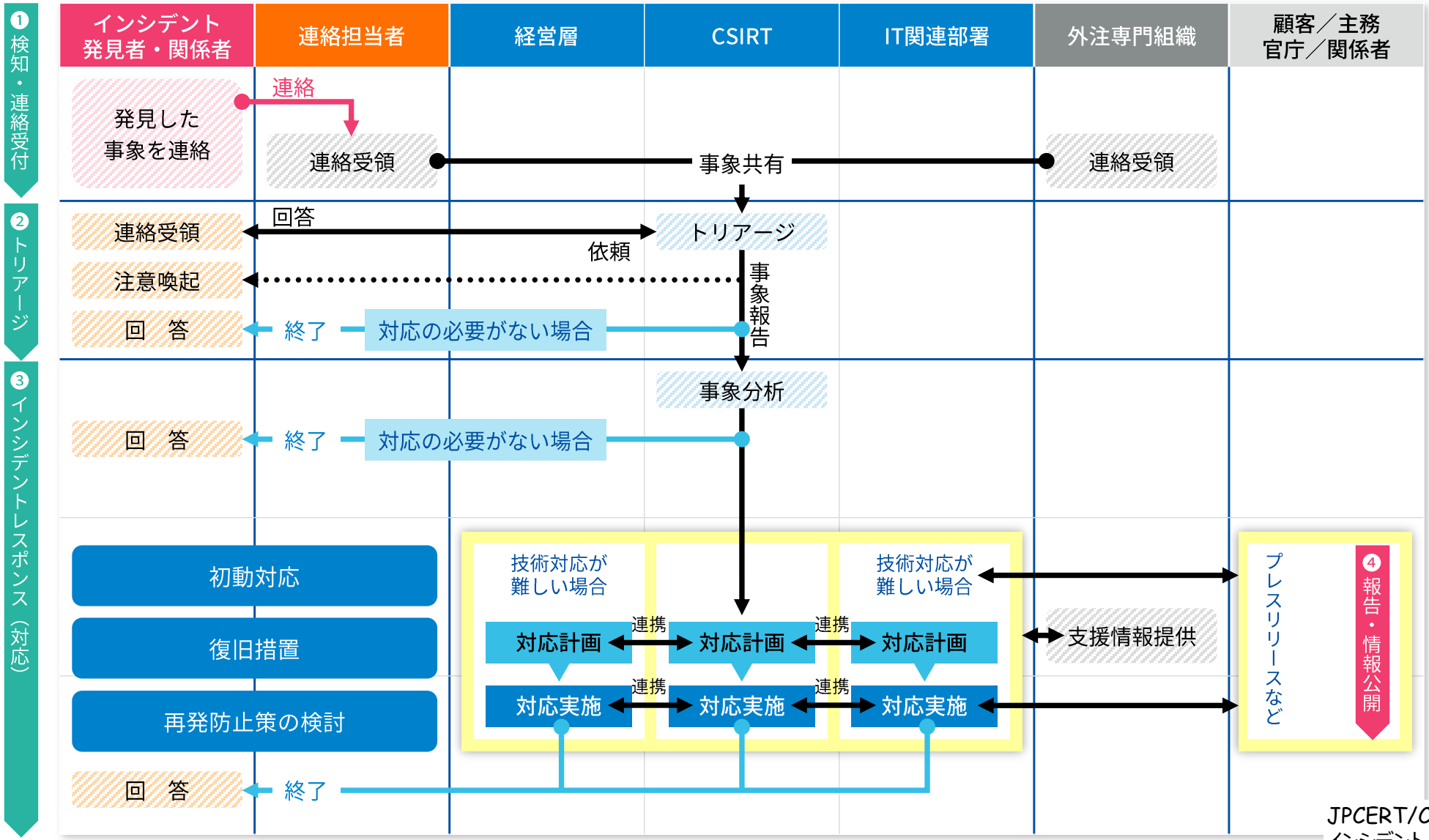
・　被害者の視点に立った通報・相談への対応マニュアルの整備
・　通報・相談に対応する職員のリテラシー向上、サポート体制の強化

被害者の被害拡大防止や被害回復への貢献、犯罪手口や未然防止対策に関する情報の速やかな還元等の活動を充実させることで、**被害の通報・相談が自ずと行われる社会的な気運を醸成**

サイバー空間をめぐる脅威の情勢等
｜警察庁Webサイト

参考

インシデントハンドリングのフロー例



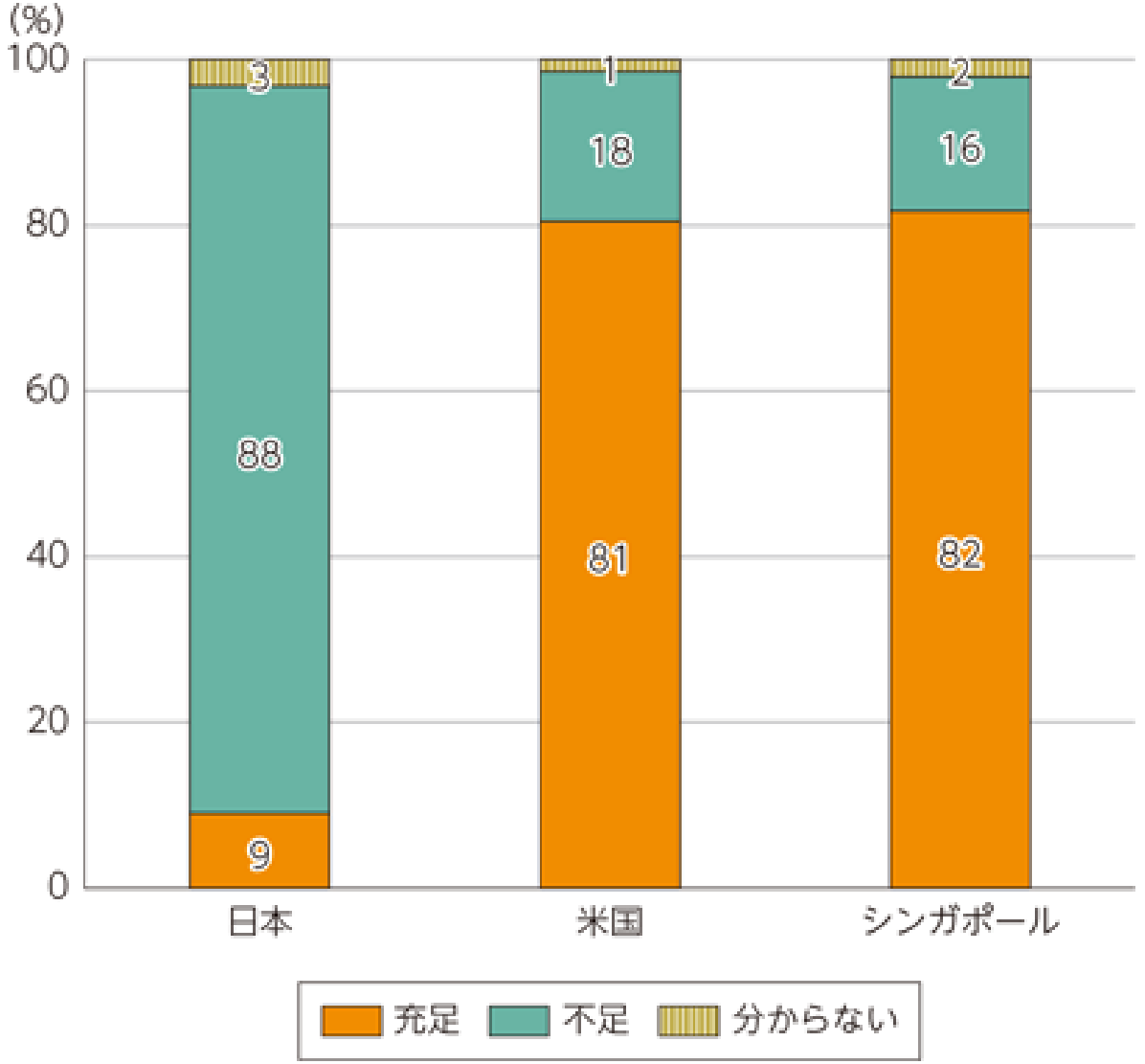
JPCERT/CC
インシデントハンドリングマニュアルより

参考

インシデントハンドリングステップの内容と具体例

ステップ	内　容	具体例
検知・連絡受付	●インシデントが発生した旨の連絡を受領	Webサーバーから外部に不審な通信が発生していると Security Operation Center(SOC事業者※) から報告を受けた。 ※SOC事業者とは外部からネットワーク機器やサーバー類を常時監視し、サイバー攻撃の検出と分析、対応策のアドバイスを提供する組織、企業のこと
トリアージ	●事実関係や状況を確認 ●インシデントか否かの判断 ●対応の優先順位付け	調査の結果、サーバー内に不審なファイルを発見し、サイバー攻撃を受けており、速やかに対応が必要と判断した。
インシデントレスポンス	●対応方針の検討 ●被害の原因を取り除き、元の状態に復旧	Webサーバーを停止した後、バックアップから復旧した。 攻撃に利用された脆弱性にセキュリティパッチを適用した。
報告・公表	●被害状況や影響範囲に応じ組織内外に対して報告・公表	サイバー攻撃により個人情報が漏えいした疑いがあることを経営幹部に報告した。
事後対応	●報告書の取りまとめ ●振り返りの実施	発生したイベントについて報告書に取りまとめた。

セキュリティ人材は不足？



https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd134530.html

不足しているのはどんな人材か

1位	セキュリティ戦略・企画を策定する人	54.3%
2位	セキュリティリスクを評価・監査する人	39.3%
3位	ログを監視・分析して、危険な兆候をいち早く察知できる人	38.4%
4位	セキュリティインシデントへの対応・指揮ができる人	35.7%
5位	関係部署との調整をしながら、セキュリティ対策を推進・統括できる人	26.7%

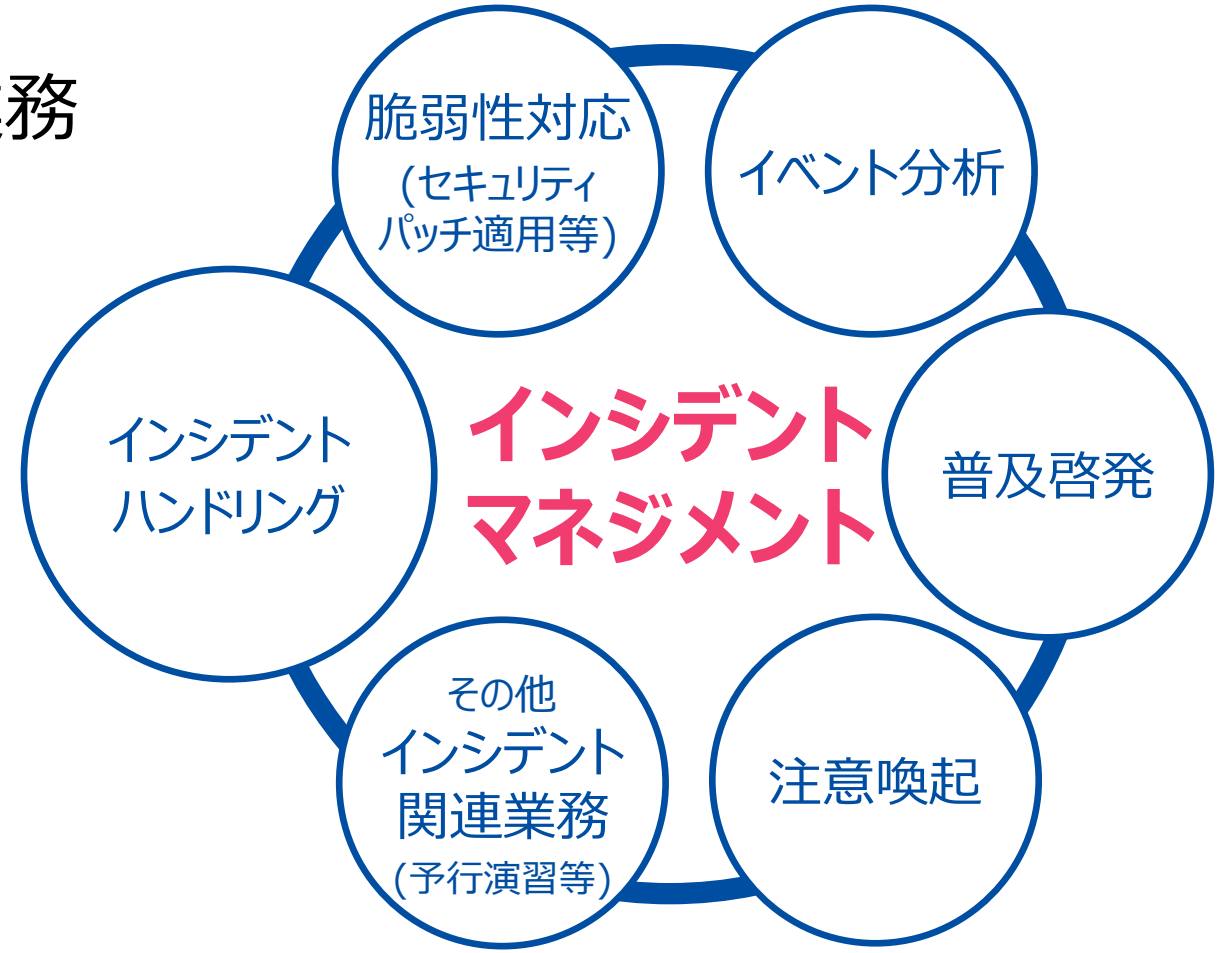
NRI Secure Insight 2021より。
他の選択肢にセキュアなプログラミングができる人、ビジネス・事業部門側のセキュリティ担当者などがある。

では、どうしたら良いか？

インシデントマネジメント と インシデントハンドリング

インシデントマネジメント

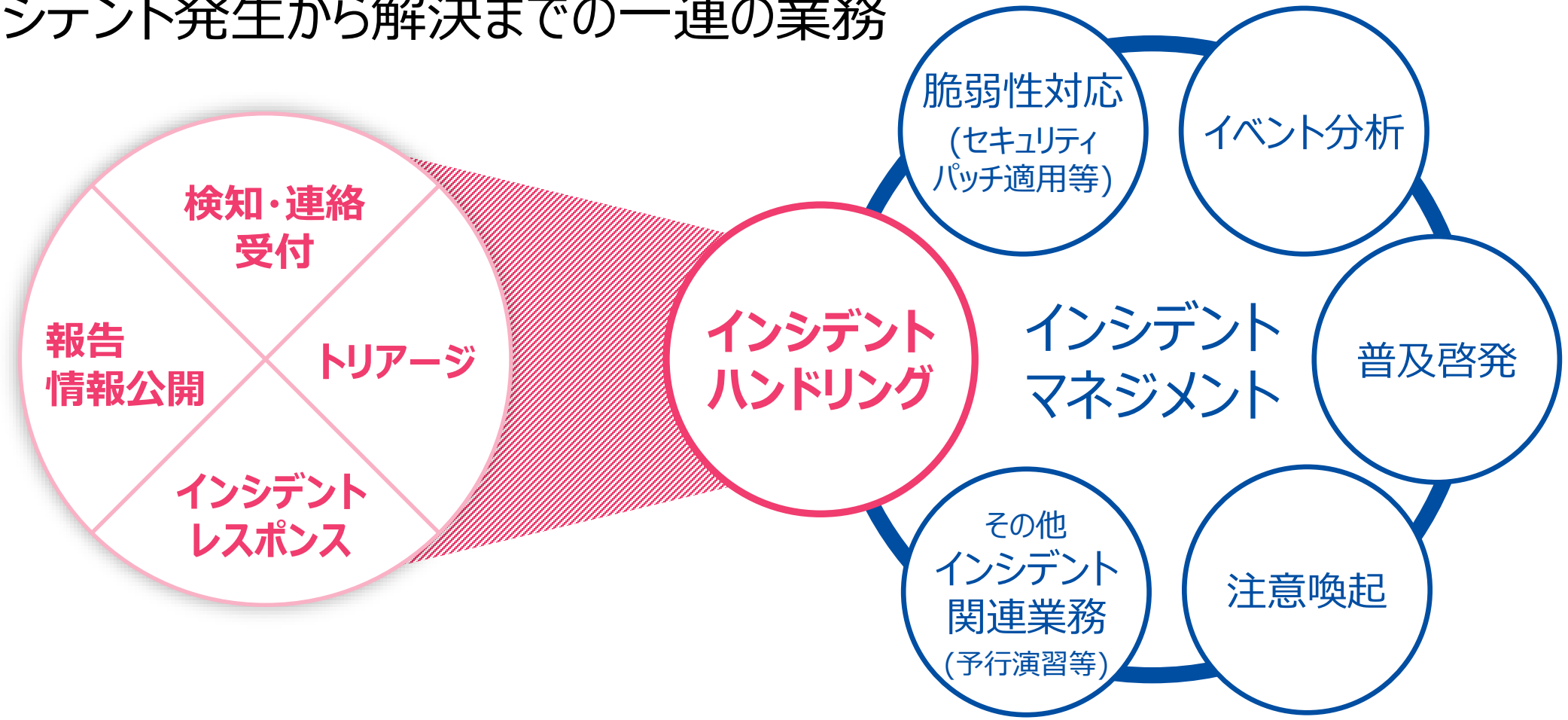
- CSIRTが「事前」の準備を含めた
  インシデントに対して行う一連の業務



インシデントマネジメント と **インシデントハンドリング**

インシデントハンドリング

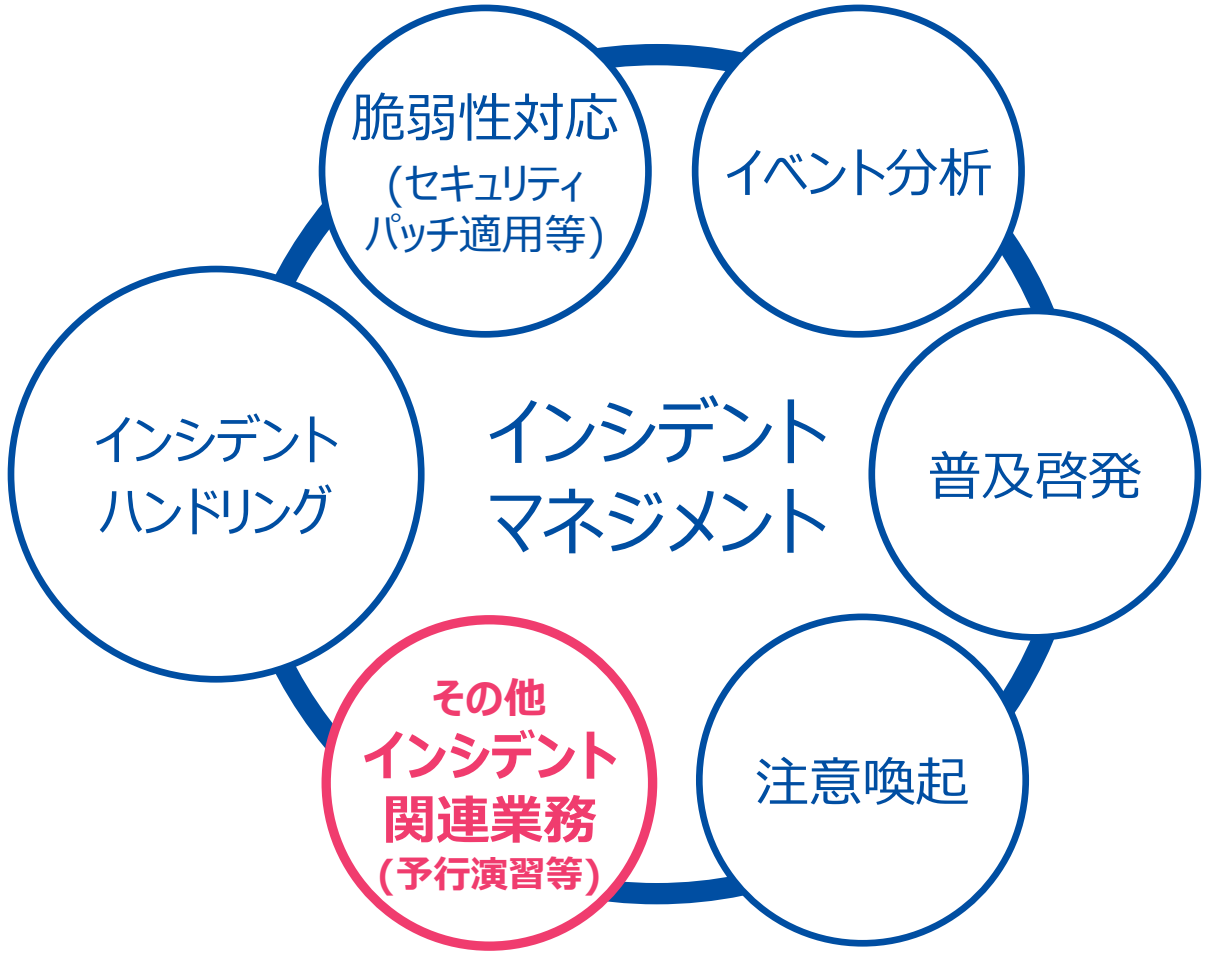
- インシデント発生から解決までの一連の業務



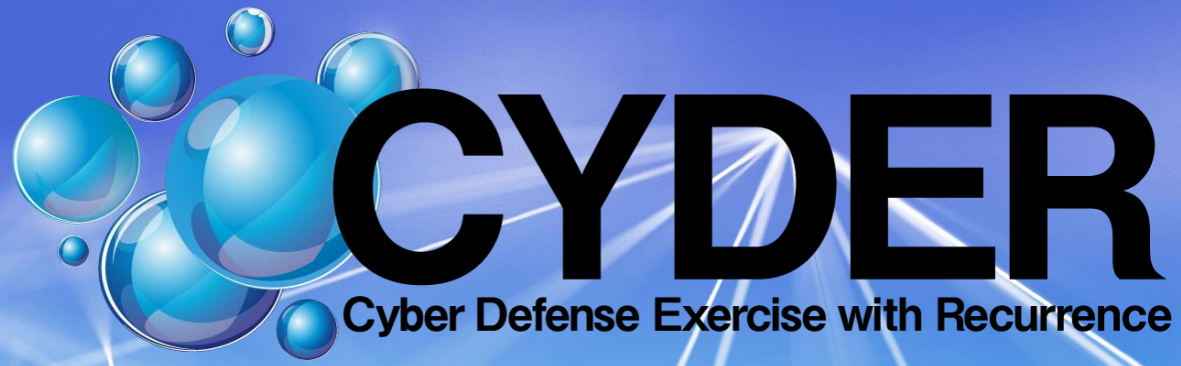
教育・訓練

教育訓練の例

- セミナー
- ワークショップ
- 机上演習
- 実機演習



実践的サイバー防御演習



2023年度実践的サイバー防御演習(CYDER)の概要

国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成

2023年度コース概要

- 毎年 **約 3,000人が受講**
- 演習は1日間 (Cコースは2日間)
- 集合 (実地) 演習のほか、オンライン演習(個人学習)を実施
- 組織当たり1名でも複数名でも参加可能
- 重要社会基盤事業者、民間企業等は、受講料が必要
  - A/B/オンライン入門コース … 77,000円 (税込)
  - Cコース … 121,000円 (税込)

CYDER受講者数の推移 (累積数)

2023年度実施内容および対象組織

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	情報システム担当の経験2年以内相当の知識をお持ちの方 (事案発生時の対応の流れ・ベンダーとの円滑な情報連携)	全組織共通	47都道府県	64回	7月～翌年1月
B-1		中級	情報システム担当の経験2年以上相当の知識をお持ちの方 (主体的な事案対応・セキュリティ管理)	地方公共団体	全国11地域	20回	10月～翌年1月
B-2				地方公共団体以外	東京・大阪・名古屋	13回	翌年1月
C		準上級	情報システム担当の経験3～4年以上相当の知識をお持ちの方 (高度なセキュリティ技術)	全組織共通	東京	3回	11月～翌年1月
入門	オンライン演習	入門	情報システム担当経験1年前後で知識のアップデートをお考えの方 (集合演習Aコースの受講に必要な最低限の知識)	全組織共通	(受講者職場等)	随時	5月～7月
プレCYDER		―	インシデント発生時の対応の学習をこれから始める、または、始めたばかりの方 (CSIRT担当者として知っておきたい基礎的な事項)	国の機関等、地方公共団体			12月～翌年1月

※CYDERは、(ISC)² が提供する資格の認定継続に必要なCPEクレジット (継続教育単位) 付与対象の演習

たった1ページで分かる サイダー CYDER 2023
Cyber Defense Exercise with Recurrence

初級、 中級、準上級、オンライン(入門･プレCYDER) New

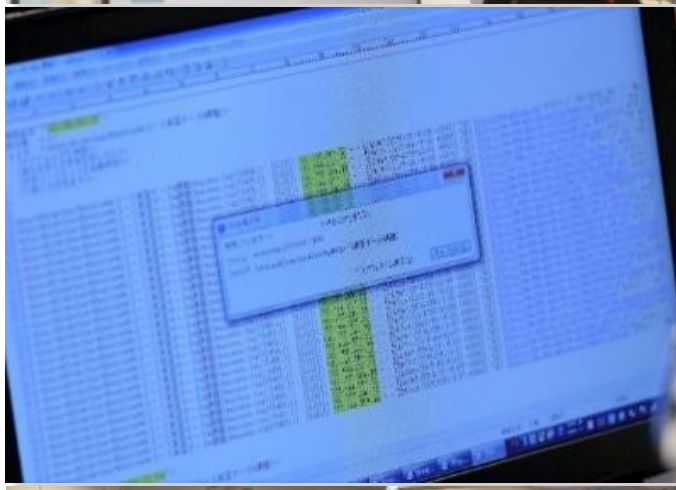
- 最大4名のグループワーク、ハンズオン　等
- 国の機関、地方公共団体等の職員の方は受講料が無料
- 新作シナリオ続々、繰り返し受講が効果的
- 受講後に発生したインシデント対応に役立った例

演習環境CYDERANGE

- 各グループに専用の演習環境を提供
- NICTの強み① 大規模計算機環境＆StarBED

そのときどきの旬なシナリオの提供

- NICTの強み② 研究実績と攻撃観測データの蓄積

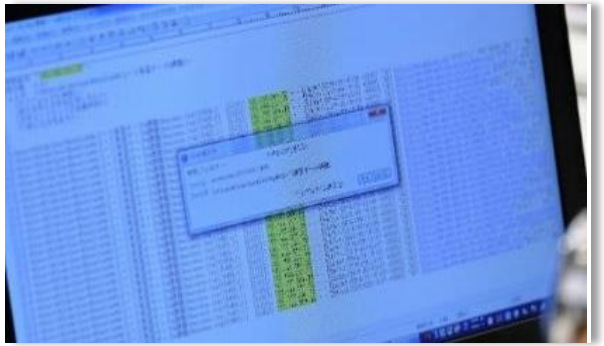


CYDER演習風景: Aコース

オリエンテーション

演習フロー説明

インシデント発生～事実確認

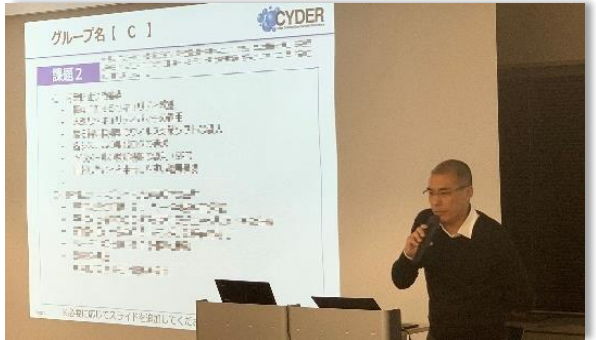


チューターによるサポート

マルウェア挙動調査

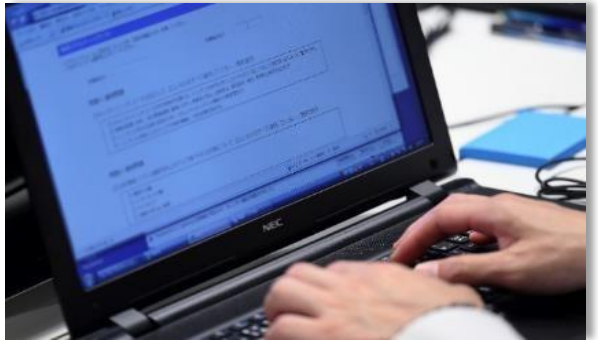
グループワーク

発表



報告書作成

確認テスト



集合演習のメリット

2023年度CYDER演習開催スケジュール

Aコース（初級）（全組織共通）

地域	開催県	開催日	
北海道	北海道	8/22 札幌	10/5 網走
東北	青森県	8/25 青森	
	岩手県	10/11 盛岡	
	宮城県	7/21 仙台	10/13 仙台
	秋田県	9/5 秋田	
	山形県	8/30 山形	
	福島県	9/29 郡山	
関東	茨城県	7/19 水戸	
	栃木県	7/25 宇都宮	
	群馬県	9/26 高崎	
	埼玉県	9/22 さいたま	
	千葉県	9/20 千葉	
	東京都	7/11 東京	8/10 東京
		8/23 東京	9/29 東京
		10/17 東京	10/18 東京
		12/12 東京	1/12 東京
	神奈川県	9/26 横浜	12/21 小田原
	山梨県	8/8 甲府	
信越	新潟県	9/12 新潟	
	長野県	7/28 長野	11/10 茅野
北陸	富山県	9/8 富山	
	石川県	9/15 金沢	
	福井県	8/31 敦賀	
東海	岐阜県	8/29 岐阜	
	静岡県	8/31 静岡	
	愛知県	7/26 名古屋	9/22 名古屋
		11/28 名古屋	
	三重県	9/15 津	

地域	開催県	開催日	
近畿	滋賀県	8/4 大津	
	京都府	10/31 京都	
	大阪府	7/28 大阪	9/12 大阪
		11/28 大阪	12/6 大阪
	兵庫県	11/7 神戸	
	奈良県	8/29 奈良	
	和歌山県	10/27 和歌山	
中国	鳥取県	8/10 倉吉	
	島根県	11/2 出雲	
	岡山県	9/5 岡山	
	広島県	8/25 広島	
	山口県	10/20 山口	
四国	徳島県	10/31 徳島	
	香川県	9/8 高松	
	愛媛県	8/1 松山	
	高知県	10/27 高知	
九州	福岡県	8/22 福岡	12/14 福岡
	佐賀県	11/14 佐賀	
	長崎県	11/10 長崎	
	熊本県	10/17 熊本	
	大分県	10/24 大分	
	宮崎県	10/13 日向	
	鹿児島県	8/4 鹿児島	
沖縄	沖縄県	10/6 那覇	

オンラインコース（全組織共通）

オンラインにより受講可能なコースを時期を分けて開催
　第1期（5月16日から7月14日）　　第2期（12月から1月予定）

B-1コース (中級)(地公体向)

開催地域	開催日	
北海道	11/2 札幌	
東北	11/8 盛岡	11/14 仙台
関東	10/11 東京	12/13 東京
	12/19 東京	1/10 東京
信越	11/17 新潟	
北陸	11/21 金沢	
東海	10/24 名古屋	11/29 名古屋
近畿	10/20 大阪	11/29 大阪
	12/7 大阪	
中国	11/7 広島	11/17 岡山
四国	11/22 高松	
九州	12/8 熊本	12/15 福岡
沖縄	12/1 那覇	

B-2コース (中級)(国・重要ｲﾝﾌﾗ)

開催地域	開催日	
関東	1/11 東京	1/16 東京
	1/17 東京	1/19 未定
	1/23 東京	1/24 東京
	1/25 東京	1/26 東京
	1/30 東京	1/31 東京
近畿	1/23 大阪	1/24 大阪
東海	1/19 名古屋	

Cコース（準上級）（全組織共通）

開催地域	開催日	
関東	11/21~22	東京
	1/25~26	東京
	1/30~31	東京

和歌山近郊で開催予定のCYDER

Aコース

- 10/27@**和歌山** お急ぎください
- 11/28@大阪 満席(キャンセル待ち)
- 12/06@大阪 残席僅か

B-2コース

- 1/23@大阪 11月頃受付開始予定
- 1/24@大阪 11月頃受付開始予定

B-1コース

- 10/20@大阪 満席(キャンセル待ち)
- 11/29@大阪 満席(キャンセル待ち)
- 12/07@大阪 満席(キャンセル待ち)

CYDER 繰り返し受講 をオススメする理由

インシデントハンドリングはさまざま。

絶対的な正解はない

- 共通要素はあるが
  部分的に違うシナリオを体験
- 共通要素の洗練
- 「想定内」の想定範囲が広くなれば、
  多少のことでは慌てなくなる


CYDER
Cyber Defense Exercise with Recurrence

国立研究開発法人
情報通信研究機構

受 講 証 明 書

証書No.H30-20001

実践的サイバー防御演習 CYDER

（演習概要：攻撃者により不正改造されたアプリケーションを
発火点とする事案へのインシデントハンドリング）

斉田　太郎 殿

まとめ

トレンドとキーワードで確認する最近のセキュリティ動向

やらかす？やられる？

では、どうしたら良いか？

- インシデントマネジメント と インシデントハンドリング
- 教育・訓練
- 実践的サイバー防御演習(CYDER)

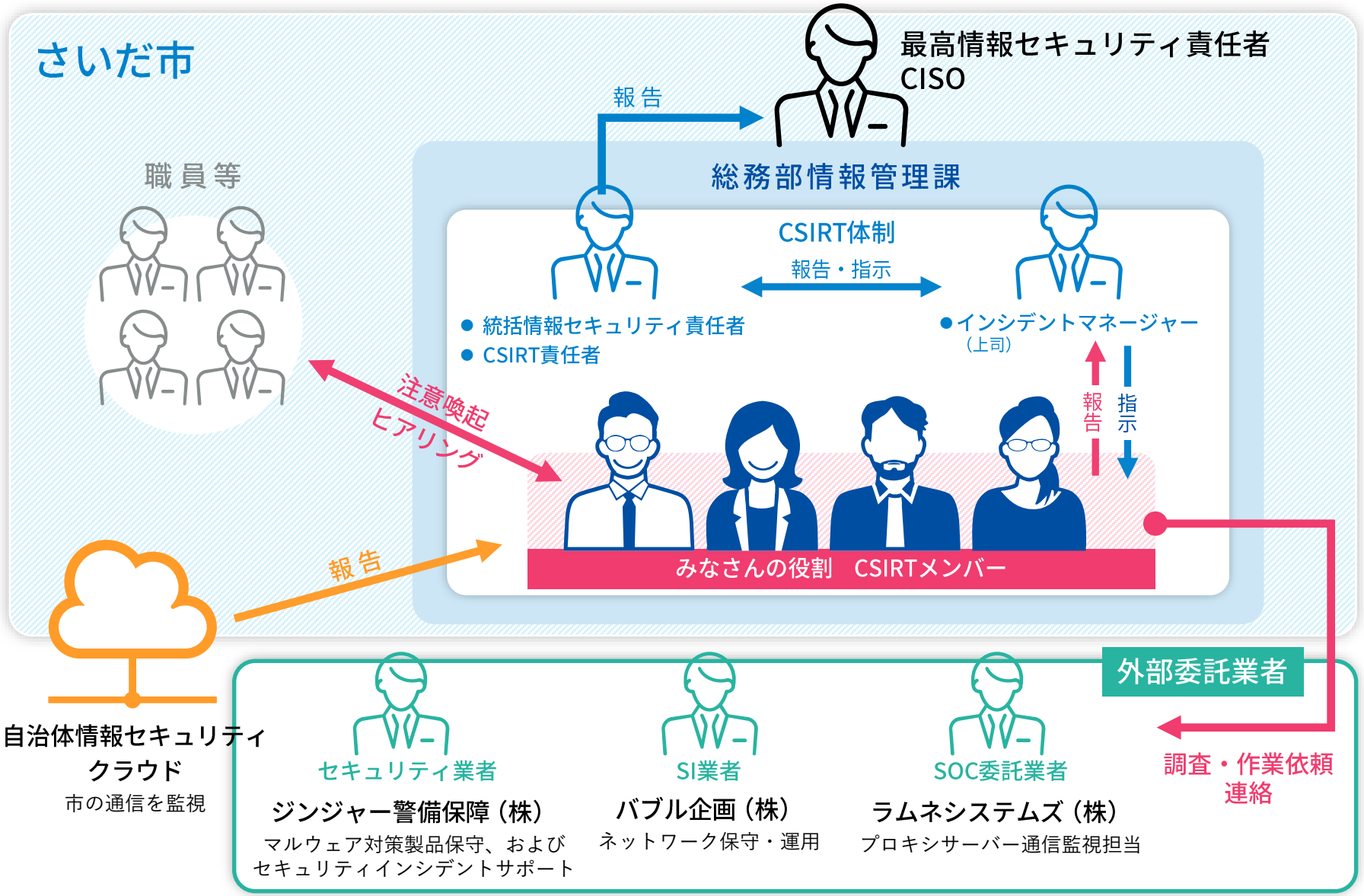
ご参考資料

CYDER

Cyber Defense Exercise with Recurrence

参考

登場人物相関の例


さいだ市
最高情報セキュリティ責任者
CISO
報告
総務部情報管理課
職員等
CSIRT体制
報告・指示
● 統括情報セキュリティ責任者
● CSIRT責任者
●インシデントマネージャー
（上司）
注意喚起
ヒアリング
報告
指示
報告
みなさんの役割　CSIRTメンバー
報告
外部委託業者
自治体情報セキュリティ
クラウド
市の通信を監視
セキュリティ業者
ジンジャー警備保障（株）
マルウェア対策製品保守、および
セキュリティインシデントサポート
SI業者
バブル企画（株）
ネットワーク保守・運用
SOC委託業者
ラムネシステムズ（株）
プロキシサーバー通信監視担当
調査・作業依頼
連絡

参考

集合演習の課題出題例

課題	テーマ	課題概要
1	検知・連絡受付	連絡受付に対する事実確認および対処
2	トリアージ（ログ調査） Hands-on	事実確認のためのログ調査
3	トリアージ（ヒアリング）	現場当事者への指示・依頼
4	対応方針の検討	事実関係の整理、今後の対応方針の検討
5	証拠保全 （ディスクイメージ調査） Hands-on	事象の詳細調査（１）
6	証拠保全 （マルウェア解析） Hands-on	事象の詳細調査（２）
7	封じ込め・根絶／報告・公表	事実関係の整理、封じ込め・根絶策検討
8	復旧措置・報告書作成	報告書作成
9	再発防止策の検討	改善点の洗い出し

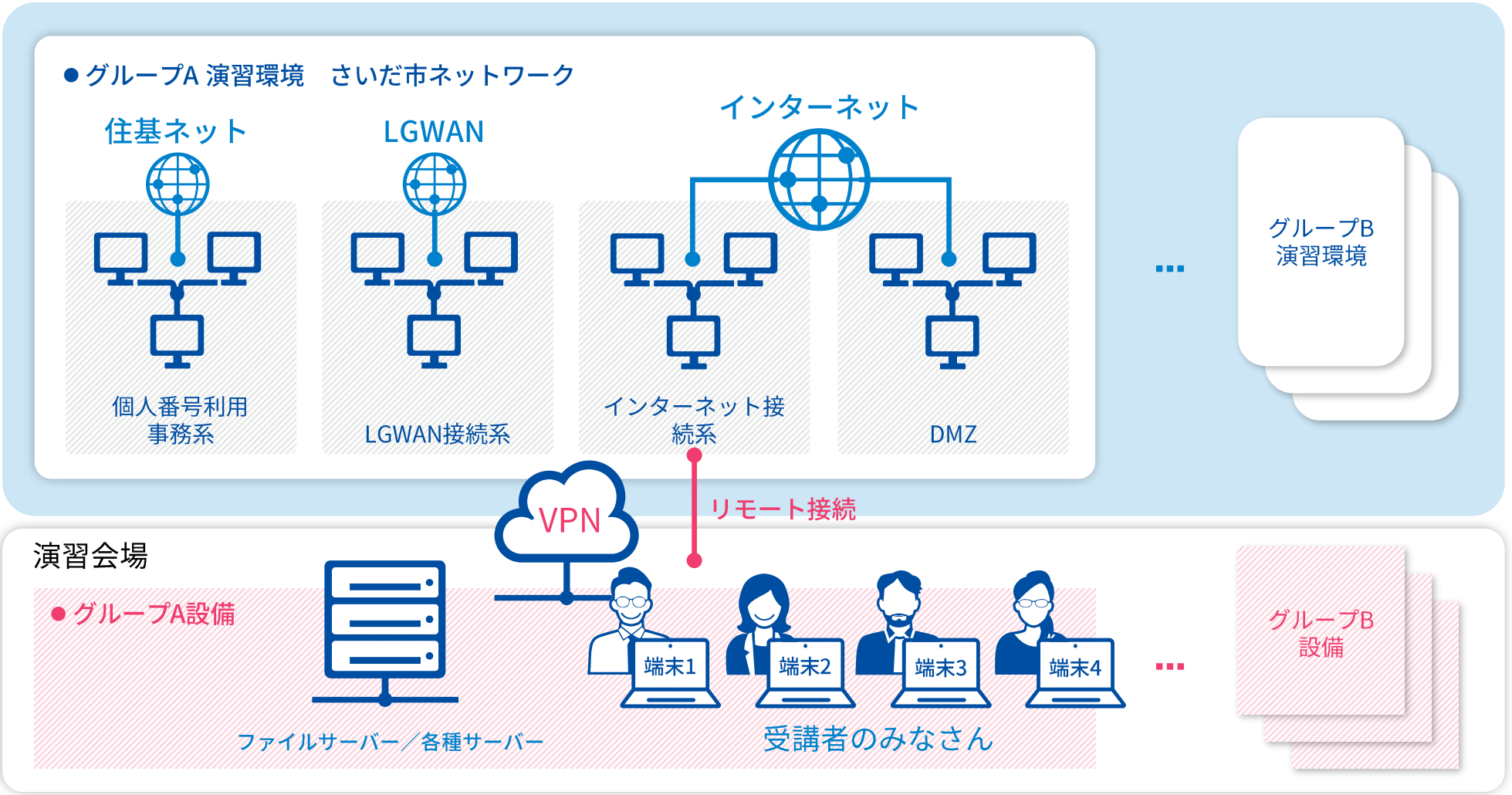
■ Hands-on はハンズオン課題、それ以外はディスカッション課題です。
※ディスカッションで検討した内容について、数チームに発表していただきます。その他チームからの質問、助言等の意見交換を行います。

参考

各グループそれぞれに提供するネットワーク構成例

演習環境［StarBED］

※StarBED：NICTが構築した、大規模なシミュレーションを実施できる計算機群です。
本演習では、さいだ市のネットワークをシミュレーションし、演習環境として利用しています。



参考

資料ダウンロード

CYDERに関する資料をこちらからダウンロードいただけます。

CYDERパンフレット

ダウンロード
（PDF：2.35MB）

CYDERポスター

ダウンロード
（PDF：14.3MB）

ナショナルサイバートレーニングセンター
組織案内資料

本編（PDF：3.9MB）

参考資料（PDF：5.2MB）

CYDER｜資料請求｜https://cyder.nict.go.jp/request/index.html

National Cyber Training Center

CYBERSECURITY

Research Institute


NICT
国立研究開発法人
情報通信研究機構