FIT大阪フォーラム セキュリティセミナー

ミッションクリティカルな金融系業界に伝えたい
サイバーセキュリティ対策と人材育成

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)

2024/02/22

NICT: 国立研究開発法人情報通信研究機構

情報通信分野を専門とする我が国唯一の公的研究機関

重点5分野

- ✓ 電磁波先進技術
- ✓ 革新的ネットワーク
- ✓ **サイバーセキュリティ**
- ✓ ユニバーサルコミュニケーション
- ✓ フロンティアサイエンス

＋オープンイノベーション

エヌアイシーティー

NICT
サイバーセキュリティ研究所

サイバーセキュリティ
研究室

サイバーセキュリティ技術

セキュリティ
基盤研究室

暗号技術

サイバーセキュリティ
ネクサス

産学官の『結節点』

ナショナルサイバー
トレーニングセンター

セキュリティ人材育成

ナショナルサイバー
オブザベーションセンター

IoT機器の調査

総合企画室

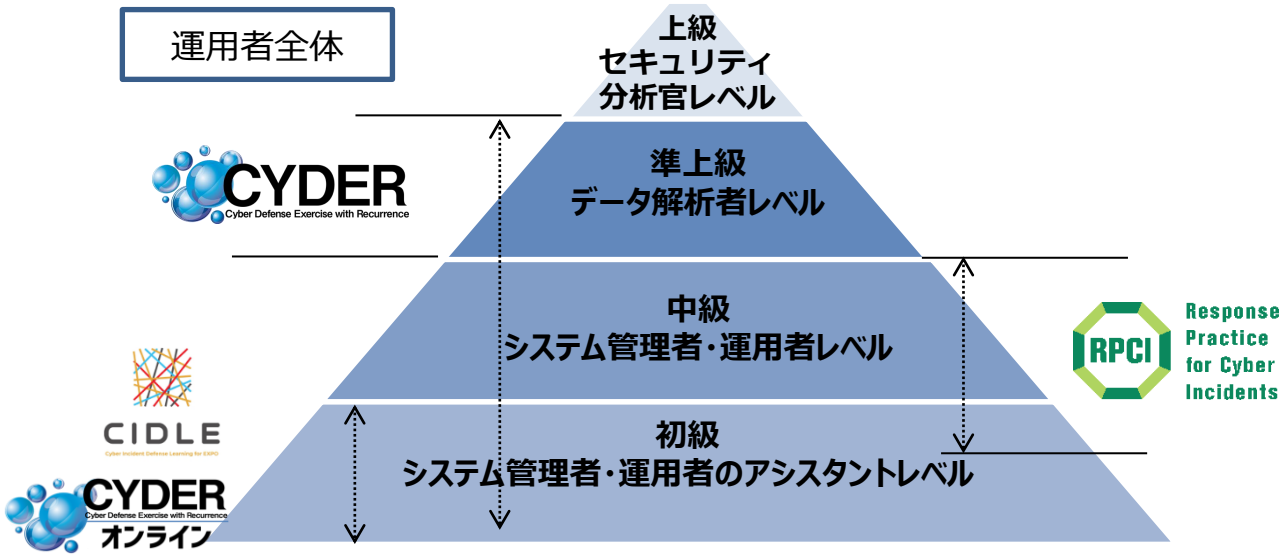
研究活動の支援

ナショナルサイバートレーニングセンター

- **NICTの技術的知見、研究施設等を最大限に活用し、実践的なサイバートレーニングを企画・推進**する組織として設置（2017年4月1日）
- 日本全体のサイバーセキュリティエコシステムの能動的な発展のため、**インシデント対応の実務に携わる運用者**及び**革新的なセキュリティサービス等を開発するハイレベルな人材**の育成を実施

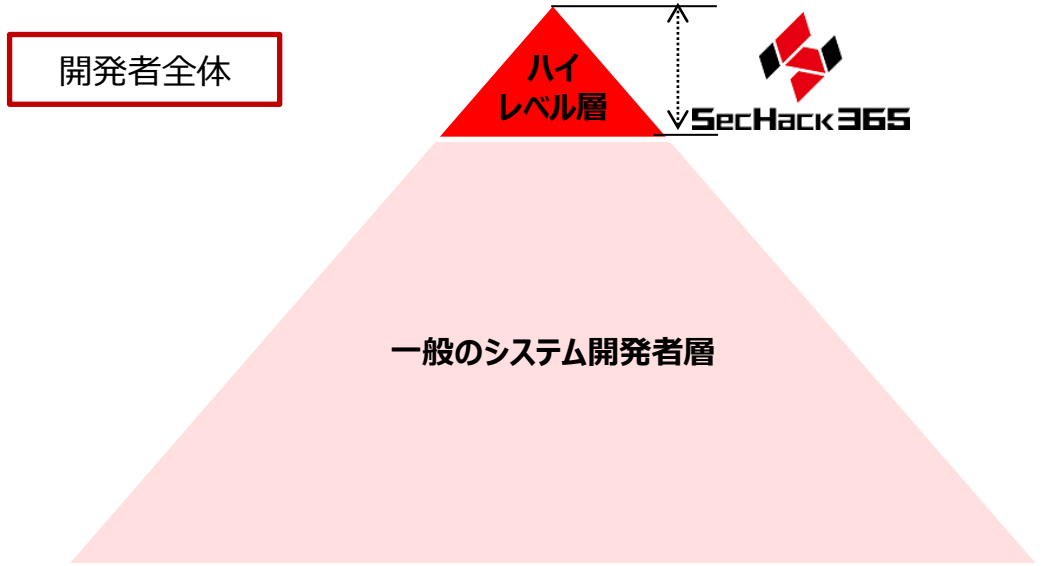
セキュリティオペレーター（実践的運用者）の育成

- **行政機関や民間企業等の組織内のセキュリティ運用者(情報システム担当者等)を対象**
- **年間約3000名の規模で、所属組織がサイバー攻撃を受けた段階等(＝「有事」)における実践的なインシデント対応能力を育成**



セキュリティイノベーター（革新的研究・開発者）の育成

- **単なる「ユーザー」として既存ツールを利用するだけではなく、セキュリティマインドを持ち、革新的なセキュリティソフトウェア等を自ら「研究・開発」していくことができるハイレベルな人材を育成(年間約40名)**



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, CIDLE,
    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

前職で担当した業務の例

ホスト、基幹システム系

- 勘定系システム、情報系システム、システム統合、営業店システム…

預金、チャネル系

- ATM, コンビニATM, CAFIS, 統合ATM, インターネットバンキング…

分散系

- 営業推進支援、印鑑、電子還元資料…

トラブル対応のレスキュー　等

…の経験を活かして
サイバーセキュリティの人材育成に携わっています。

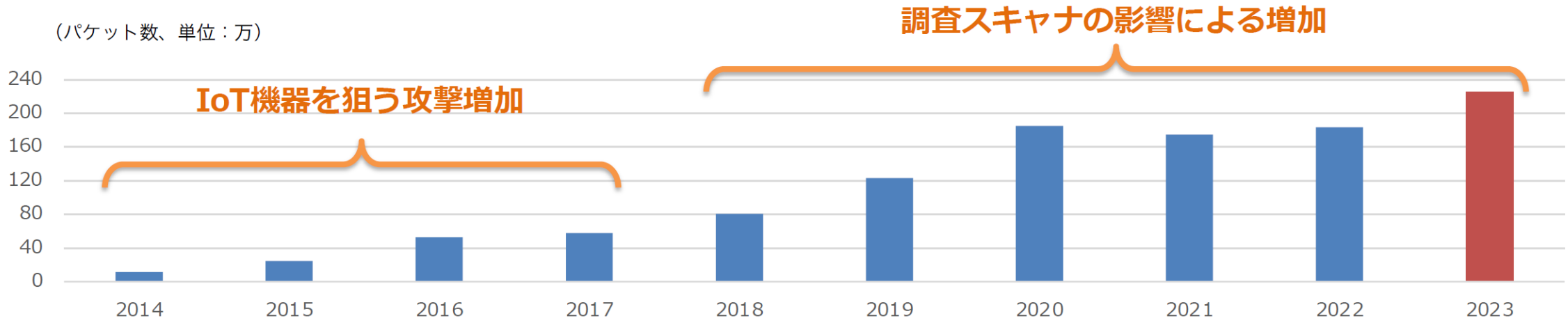
Agenda

- トレンドとキーワードでがっちり！ 最近のセキュリティ動向
- セキュリティインシデント ＆ インシデントハンドリング
- もしアナタの組織にインシデントが発生したら?

トレンドとキーワードでがっちり！
最近のセキュリティ動向

New 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
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
2023	**約6,197億**	**289,686**	**2,260,132**



1 IPアドレス当たりの年間総観測パケット数

令和6年2月最新版!! 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(五十音順)	情報セキュリティ10大脅威 2023 組織	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（2024年予測）	JNSA 2023セキュリティ十大ニュース	情報セキュリティ安心相談窓口の相談状況 2023年第4四半期（10月～12月）
1	インターネット上のサービスからの個人情報の窃取	ランサムウェアによる被害	生成ＡＩの悪用と誤用により増加するセキュリティ事故	マイナンバー相次ぐ紐付けトラブル、デジタル庁に行政指導も	2-1.「ウイルス検出の偽警告」に関する相談
2	インターネット上のサービスへの不正ログイン	サプライチェーンの弱点を悪用した攻撃	他人事ではありません。日常化するランサムウェア被害	元派遣社員の顧客情報持ち出し10年間ずさんな内部不正対策	2-2.「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
3	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等の被害	国家支援型組織によるサイバー攻撃の深刻化	全銀ネットでシステム障害　三菱UFJやりそなど10の銀行で振込できず	2-3.「不正ログイン」に関する相談
4	スマホ決済の不正利用	標的型攻撃による機密情報の窃取	重要インフラを支える供給網（中小企業）がサイバー攻撃ターゲットに	報道番組を装った総理大臣の偽動画拡散、AIのセキュリティリスク	2-4.「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
5	偽警告によるインターネット詐欺	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	重要性が高まる事前評価，　生成ＡＩのリスク	内閣サイバーセキュリティセンターが不正侵入被害	2-5.「ワンクリック請求」に関する相談
6	ネット上の誹謗・中傷・デマ	不注意による情報漏えい等の被害	クラウド設定不備によるセキュリティ事故の多発	ランサムウェア感染により名古屋港の全ターミナルが機能停止	相談事例1　自社ウェブサイトを改ざんされ偽ECサイトへリダイレクトする踏み台にされた被害
7	フィッシングによる個人情報等の詐取	脆弱性対策情報の公開に伴う悪用増加	人材の流動化に伴う営業機密の流出増加	富士通への行政指導、サイバー攻撃対策とシステム品質に	相談事例2　自社をかたる不審なメールの発信
8	不正アプリによるスマートフォン利用者への被害	ビジネスメール詐欺による金銭被害	脆弱性管理体制の再検討の加速	ハマス・イスラエル戦争のサイバー攻撃余波、日本に	相談事例3　偽のセキュリティ警告（サポート詐欺）からネットバンキングの不正送金をされた被害
9	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	テレワーク等のニューノーマルな働き方を狙った攻撃	止まらないランサムウェアの進化	偽セキュリティ警告(サポート詐欺)の月間相談件数が過去最高	相談事例4　偽SMSのフィッシングから不正送金されたと思われる被害
10	ワンクリック請求等の不当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）	経営課題として浮上，サイバー人材育成	ニンテンドーアカウントがパスキー対応　パスワード不要でログイン可能に	-
	情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/10threats/10threats2024.html	情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/10threats/10threats2024.html	監査人の警鐘- 2024年 情報セキュリティ十大トレンド | JASA (Japan Information Security Audit Association) https://www.jasa.jp/seminar/sec_trend2024/	JNSAセキュリティ十大ニュース https://www.jnsa.org/active/news10/index.html	情報セキュリティ安心相談窓口公開レポート | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/anshin/reports/index.html
	2024/1/24	2024/1/24	2024/1/9	2023/12/26	2024/1/23

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)	URL	メモ(時々並べ替えします)
31	2月-24	民間企業	個人情報漏えいに関するお詫びとお知らせ(クミショクファーム)	https://www.kg-shoku.jp/publics/index/75/detail=1/b_id=1/r_id=89/sp_ssid=3	ペイメントアプリケーション改ざん、クレジットカード情報漏洩
32	2月-24	民間企業	【セキュリティ ニュース】鹿児島農産品の通販サイトで個人情報流出の可能性 - クレカや認証情報も（1ページ目 / 全2ページ） ：Security NEXT	https://www.security-next.com/153918	ペイメントアプリケーション改ざん、クレジットカード情報漏洩
33	2月-24	民間企業	【セキュリティ ニュース】トヨタの社用車管理サービスに不正アクセス - 原因は古いアクセスキー（1ページ目 / 全1ページ） ：Security NEXT	https://www.security-next.com/153922	
34	2月-24	地方公共団体	「市民税・県民税課税 契約および法令違反に		
35	2月-24	地方公共団体	【セキュリティ ニュー 再委託 - 熊谷市（1ペ		
36	2月-24	民間企業	セキュリティ強化費用 ア攻撃 | ScanNetSecu https://scan.netsecurit		
37	2月-24	民間企業	住友重機械工業のサー 喚起も発表 | ScanNet https://scan.netsecurit		
			臨床検査事業を行うア		

#	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)	URL	メモ(時々並べ替えします)
120	2月-24	民間企業	【セキュリティ ニュース】健康食品通販サイトに不正アクセス - 個人情報流出の可能性（1ページ目 / 全2ページ） ：Security NEXT	https://www.security-next.com/153260	クレジットカード情報流出
185	1月-24	民間企業	【セキュリティ ニュース】ケーズデンキ通販サイトに不正ログイン - 約300万円の不正注文（1ページ目 / 全2ページ） ：Security NEXT	https://www.security-next.com/152800	クレジットカード不正
195	1月-24	民間企業	【セキュリティ ニュース】年末に通販サイトでクレカの不正取引を多数検知 - ラシェール化粧品（1ページ目 / 全1ページ） ：Security NEXT	https://www.security-next.com/152893	クレジットカード不正
203	1月-24	民間企業	【セキュリティ ニュース】通販サイトで不正利用が多発、クレカ決済停止 - 医学書院（1ページ目 / 全1ページ） ：Security NEXT	https://www.security-next.com/153002	クレジットカード不正
242	1月-24	民間企業	ケーズデンキで“なりすまし注文”17件　不正ログイン受け - ITmedia NEWS https://www.itmedia.co.jp/news/articles/2401/18/news147.html	ケーズデンキで“なりすまし注文”17件　不正ログイン受け - ITmedia NEWS https://www.itmedia.co.jp/news/articles/2401/18/news147.html	クレジットカード不正
251	1月-24	民間企業	【セキュリティ ニュース】年末に通販サイトでクレカの不正取引を多数検知 - ラシェール化粧品（1ページ目 / 全1ページ） ：Security NEXT	https://www.security-next.com/152893	クレジットカード不正
259	1月-24	民間企業	【セキュリティ ニュース】通販サイトで不正利用が多発、クレカ決済停止 - 医学書院（1ページ目 / 全1ページ） ：Security NEXT	https://www.security-next.com/153002	クレジットカード不正
270	1月-24	民間企業	【重要】不正注文への対応について – WEEK END	https://weekend.jp/blogs/news/20240119	クレジットカード不正
271	1月-24	民間企業	「WEEK ENDオンラインストア」でクレジットカード不正利用が疑われる決済、警察に収集データ提出も | ScanNetSecurity https://scan.netsecurity.ne.jp/article/2024/01/29/50513.html	「WEEK ENDオンラインストア」でクレジットカード不正利用が疑われる決済、警察に収集データ提出も | ScanNetSecurity https://scan.netsecurity.ne.jp/article/2024/01/29/50513.html	クレジットカード不正
			「医学書院ウェブサイト」でクレジットカード決済の取扱を停止、不正利用が多発 | ScanNetSecurity	「医学書院ウェブサイト」でクレジットカード決済の取扱を停止、不正利用が多発	クレジットカード不正

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2024年1, 2月報道分

インシデント事例ピックアップ#1: サイバーセキュリティと金銭被害

#	情報セキュリティ10大脅威 2023 個人(五十音順)	情報セキュリティ10大脅威 2023 組織	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（2024年予測）	JNSA 2023セキュリティ十大ニュース	情報セキュリティ安心相談窓口の相談状況 2023年第4四半期（10月～12月）
1	インターネット上のサービスからの個人情報の窃取	ランサムウェアによる被害	生成ＡＩの悪用と誤用により増加するセキュリティ事故	マイナンバー相次ぐ紐付けトラブル、デジタル庁に行政指導も	2-1.「ウイルス検出の偽警告」に関する相談
2	インターネット上のサービスへの不正ログイン	サプライチェーンの弱点を悪用した攻撃	他人事ではありません。日常化するランサムウェア被害	元派遣社員の顧客情報持ち出し10年間ずさんな内部不正対策	2-2.「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
3	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等の被害	国家支援型組織によるサイバー攻撃の深刻化	全銀ネットでシステム障害　三菱UFJやりそなど10の銀行で振込できず	2-3.「不正ログイン」に関する相談
4	スマホ決済の不正利用	標的型攻撃による機密情報の窃取	重要インフラを支える供給網（中小企業）がサイバー攻撃ターゲットに	報道番組を装った総理大臣の偽動画拡散、AIのセキュリティリスク	2-4.「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
5	偽警告によるインターネット詐欺	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	重要性が高まる事前評価，　生成ＡＩのリスク	内閣サイバーセキュリティセンターが不正侵入被害	2-5.「ワンクリック請求」に関する相談
6	ネット上の誹謗・中傷・デマ	不注意による情報漏えい等の被害	クラウド設定不備によるセキュリティ事故の多発	ランサムウェア感染により名古屋港の全ターミナルが機能停止	相談事例1　自社ウェブサイトを改ざんされ偽ECサイトへリダイレクトする踏み台にされた被害
7	フィッシングによる個人情報等の詐取	脆弱性対策情報の公開に伴う悪用増加	人材の流動化に伴う営業機密の流出増加	富士通への行政指導、サイバー攻撃対策とシステム品質に	相談事例2　自社をかたる不審なメールの発信
8	不正アプリによるスマートフォン利用者への被害	ビジネスメール詐欺による金銭被害	脆弱性管理体制の再検討の加速	ハマス・イスラエル戦争のサイバー攻撃余波、日本に	相談事例3　偽のセキュリティ警告（サポート詐欺）からネットバンキングの不正送金をされた被害
9	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	テレワーク等のニューノーマルな働き方を狙った攻撃	止まらないランサムウェアの進化	偽セキュリティ警告(サポート詐欺)の月間相談件数が過去最高	相談事例4　偽SMSのフィッシングから不正送金されたと思われる被害
10	ワンクリック請求等の不当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）	経営課題として浮上，サイバー人材育成	ニンテンドーアカウントがパスキー対応　パスワード不要でログイン可能に	-
	情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/10threats/10threats2024.html 2024/1/24	情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/10threats/10threats2024.html 2024/1/24	監査人の警鐘- 2024年 情報セキュリティ十大トレンド | JASA (Japan Information Security Audit Association) https://www.jasa.jp/seminar/sec_trend2024/ 2024/1/9	JNSAセキュリティ十大ニュース https://www.jnsa.org/active/news10/index.html 2023/12/26	情報セキュリティ安心相談窓口公開レポート | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/anshin/reports/index.html 2024/1/23

インシデント事例ピックアップ#1: サイバーセキュリティと金銭被害

- 盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について | 2023年 | 一般社団法人 全国銀行協会
https://www.zenginkyo.or.jp/news/2023/n122801/
- 元派遣社員「金に困ってやった」 NTT西・子会社の情報流出 |47NEWS（よんなニュース）
https://www.47news.jp/10470972.html

インシデント事例ピックアップ#1: サイバーセキュリティと金銭被害

- マルウェア、ランサムウェア被害
- 決済サービスの悪用
- 秘密情報の売却、転用

			を登録する場合有り)	URL	メモ(時々並べ替えします)
17	2月-24	民間企業	品通販サイトに不正アクセス - 個人情報ージ）：Security NEXT	https://www.security-next.com/153260	クレジットカード情報流出
73	1月-24	民間企業	デンキ通販サイトに不正ログイン - 約全2ページ）：Security NEXT	https://www.security-next.com/152800	クレジットカード不正
83	1月-24	民間企業	通販サイトでクレカの不正取引を多数検 / 全1ページ）：Security NEXT	https://www.security-next.com/152893	クレジットカード不正
94	1月-24	民間企業	イトで不正利用が多発、クレカ決済停止ジ）：Security NEXT	https://www.security-next.com/153002	クレジットカード不正
130	1月-24	民間企業	7件　不正ログイン受け - ITmedia ews/articles/2401/18/news147.html	ケーズデンキで“なりすまし注文”17件　不正ログイン受け - ITmedia NEWS https://www.itmedia.co.jp/news/articles/2401/18/news147.html	クレジットカード不正
139	1月-24	民間企業	通販サイトでクレカの不正取引を多数検 / 全1ページ）：Security NEXT	https://www.security-next.com/152893	クレジットカード不正
147	1月-24	民間企業	【セキュリティ ニュース】通販サイトで不正利用が多発、クレカ決済停止 - 医学書院（1ページ目 / 全1ページ）：Security NEXT	https://www.security-next.com/153002	クレジットカード不正
158	1月-24	民間企業	【重要】不正注文への対応について – WEEK END	https://weekend.jp/blogs/news/20240119	クレジットカード不正
159	1月-24	民間企業	「WEEK ENDオンラインストア」でクレジットカード不正利用が疑われる決済、警察に収集データ提出も | ScanNetSecurity https://scan.netsecurity.ne.jp/article/2024/01/29/50513.html	「WEEK ENDオンラインストア」でクレジットカード不正利用が疑われる決済、警察に収集データ提出も | ScanNetSecurity https://scan.netsecurity.ne.jp/article/2024/01/29/50513.html	クレジットカード不正
165	1月-24	民間企業	「医学書院ウェブサイト」でクレジットカード決済の取扱を停止、不正利用が多発 | ScanNetSecurity https://scan.netsecurity.ne.jp/article/2024/01/24/50490.html	「医学書院ウェブサイト」でクレジットカード決済の取扱を停止、不正利用が多発 | ScanNetSecurity	クレジットカード不正

Quiz: サイバー攻撃者の侵入方法

攻撃者はどのような方法で組織内に侵入するのか？
正しいと思われるものをすべて選んでみてください。

- 忙しい組織内関係者を装って組織内ユーザーに接触し、組織内にアクセスするユーザー名やパスワードを聞き出す。
- 送信元を偽装し、ユーザーの業務環境に応じた件名や内容のメールを送り付け、添付したマルウェアやリンク先のマルウェアを実行させる。
- 組織内ネットワークの入り口であるVPN装置※1の脆弱性※2を悪用する。
- セキュリティ対策が不十分な取引先や拠点等を足掛かりにする。

※1 VPN装置・・・VPNはVirtual Private Networkの略。組織内のネットワークと組織外のネットワークを安全に繋ぐ装置。
※2 脆弱性　・・・ システムの不具合や欠陥。セキュリティホールと呼ばれる場合もある。

インシデント事例ピックアップ#2: 新しい働き方への脅威

#	情報セキュリティ10大脅威 2023 個人(五十音順)	情報セキュリティ10大脅威 2023 組織	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（2024年予測）	JNSA 2023セキュリティ十大ニュース	情報セキュリティ安心相談窓口の相談状況 2023年第4四半期（10月～12月）
1	インターネット上のサービスからの個人情報の窃取	ランサムウェアによる被害	生成ＡＩの悪用と誤用により増加するセキュリティ事故	マイナンバー相次ぐ紐付けトラブル、デジタル庁に行政指導も	2-1.「ウイルス検出の偽警告」に関する相談
2	インターネット上のサービスへの不正ログイン	サプライチェーンの弱点を悪用した攻撃	他人事ではありません。日常化するランサムウェア被害	元派遣社員の顧客情報持ち出し10年間ずさんな内部不正対策	2-2.「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
3	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等の被害	国家支援型組織によるサイバー攻撃の深刻化	全銀ネットでシステム障害　三菱UFJやりそなど10の銀行で振込できず	2-3.「不正ログイン」に関する相談
4	スマホ決済の不正利用	標的型攻撃による機密情報の窃取	重要インフラを支える供給網（中小企業）がサイバー攻撃ターゲットに	報道番組を装った総理大臣の偽動画拡散、AIのセキュリティリスク	2-4.「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
5	偽警告によるインターネット詐欺	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	重要性が高まる事前評価，　生成ＡＩのリスク	内閣サイバーセキュリティセンターが不正侵入被害	2-5.「ワンクリック請求」に関する相談
6	ネット上の誹謗・中傷・デマ	不注意による情報漏えい等の被害	クラウド設定不備によるセキュリティ事故の多発	ランサムウェア感染により名古屋港の全ターミナルが機能停止	相談事例1　自社ウェブサイトを改ざんされ偽ECサイトへリダイレクトする踏み台にされた被害
7	フィッシングによる個人情報等の詐取	脆弱性対策情報の公開に伴う悪用増加	人材の流動化に伴う営業機密の流出増加	富士通への行政指導、サイバー攻撃対策とシステム品質に	相談事例2　自社をかたる不審なメールの発信
8	不正アプリによるスマートフォン利用者への被害	ビジネスメール詐欺による金銭被害	脆弱性管理体制の再検討の加速	ハマス・イスラエル戦争のサイバー攻撃余波、日本に	相談事例3　偽のセキュリティ警告（サポート詐欺）からネットバンキングの不正送金をされた被害
9	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	テレワーク等のニューノーマルな働き方を狙った攻撃	止まらないランサムウェアの進化	偽セキュリティ警告(サポート詐欺)の月間相談件数が過去最高	相談事例4　偽SMSのフィッシングから不正送金されたと思われる被害
10	ワンクリック請求等の不当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）	経営課題として浮上，サイバー人材育成	ニンテンドーアカウントがパスキー対応　パスワード不要でログイン可能に	-
	情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/10threats/10threats2024.html 2024/1/24	情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/10threats/10threats2024.html 2024/1/24	監査人の警鐘- 2024年 情報セキュリティ十大トレンド | JASA (Japan Information Security Audit Association) https://www.jasa.jp/seminar/sec_trend2024/ 2024/1/9	JNSAセキュリティ十大ニュース https://www.jnsa.org/active/news10/index.html 2023/12/26	情報セキュリティ安心相談窓口公開レポート | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/anshin/reports/index.html 2024/1/23

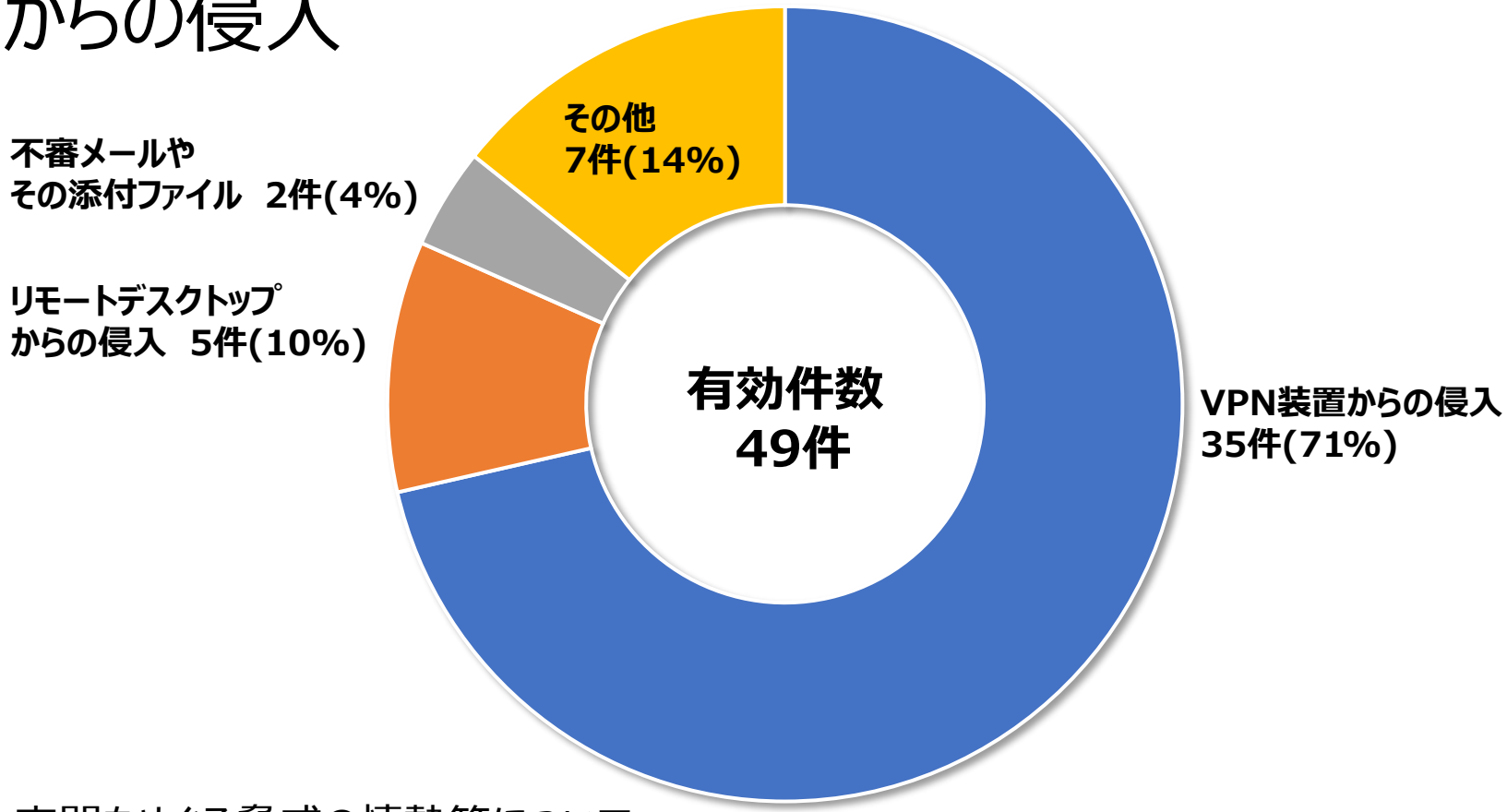
インシデント事例ピックアップ#2: 新しい働き方への脅威

- 共同捜査で国際ハッカー集団摘発　ランサムウエア、名古屋港も攻撃|47NEWS（よんななニュース）
https://www.47news.jp/10552263.html
- 名古屋港システム停止、脆弱なＶＰＮ狙われたか…最新「修正プログラム」適用せず無防備状態：読売新聞
https://www.yomiuri.co.jp/national/20230727-OYT1T50215/

今、VPN装置が狙われている

ランサムウェアの侵入経路

- 約71%がVPN装置からの侵入



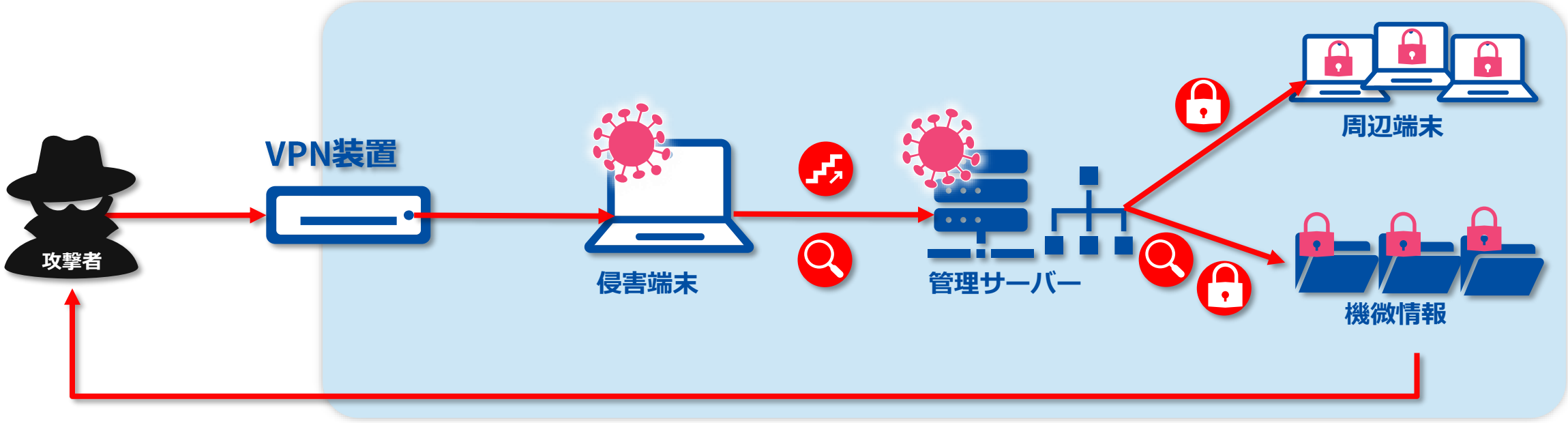
警察庁 令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

なぜVPN装置が狙われる？

- VPNの利用が増えた
- VPN装置等のセキュリティ対策の不備
- 組織内部に入りやすい

もしアナタの組織のVPN装置がやられたら?

- 企業や組織の内部ネットワークに攻撃者が「侵入」した後、情報窃取やランサムウェアを用いたファイルの暗号化などを行う。
- 情報窃取により、二重脅迫※される可能性もある。

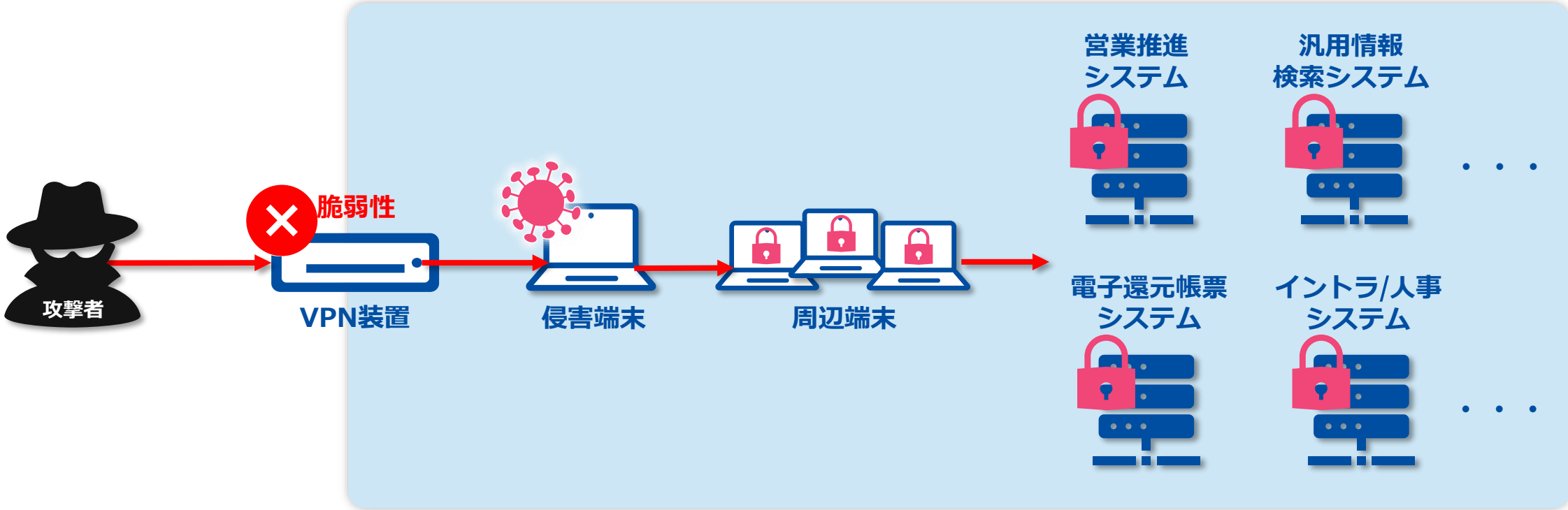


※ 二重脅迫: 攻撃者は、ターゲット組織の情報を暗号化して、身代金を要求するだけでなく、さらに、窃取した情報を公開すると脅しをかけて身代金を払わせる攻撃。

出典：JPCERT/CC 「侵入型ランサムウェア攻撃を受けたら読むFAQ」を参考に作成
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

[Case Study]もし銀行システムが攻撃されたら?

- 機器のメンテナンス等を行う際に接続するVPN装置の脆弱性を悪用し侵入
- 業務用端末や様々なサーバーに不正ログイン、暗号化



VPN装置への対策

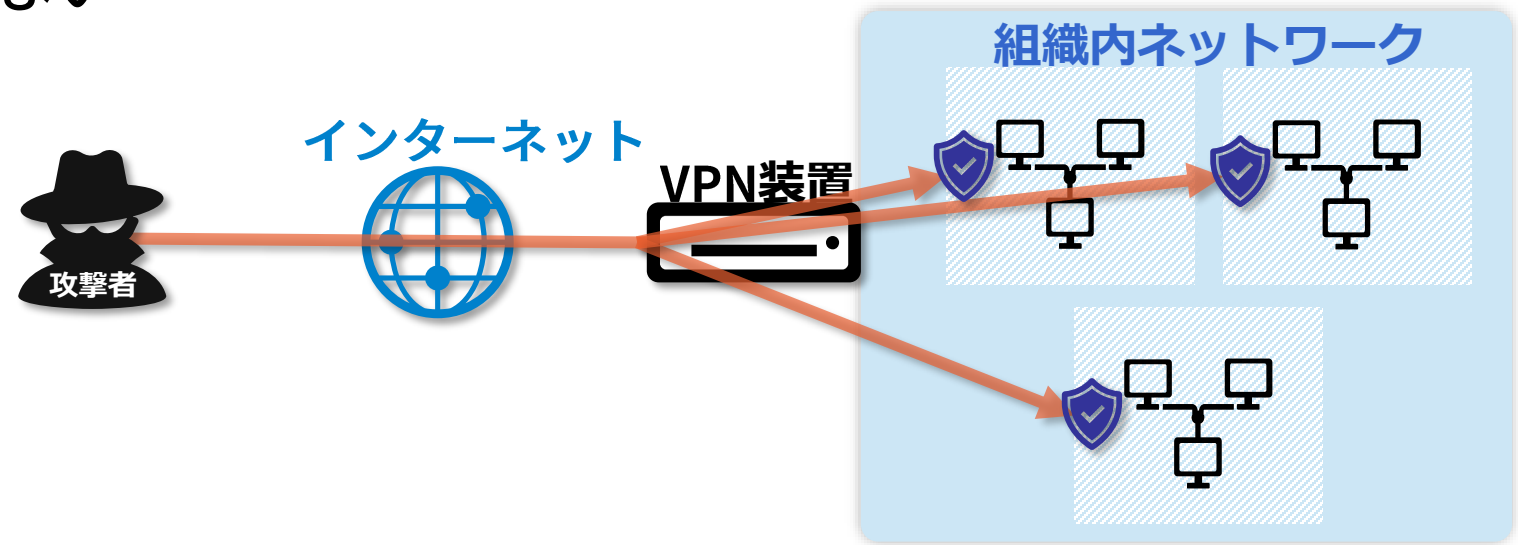
- パッチ適用
- 認証強化
- 監視強化
- ベンダーとの要件確認(再確認)

その他の対策

VPN装置を突破されても、**内部のセキュリティを強化**していれば、被害拡大を防ぐことができる

- OSやアプリケーションを最新バージョンにアップデートする
- マルウェア対策ソフトを更新する
- 脆弱なパスワードを使用しない
- 定期的にバックアップを行う

等々



セキュリティインシデント
&
インシデントハンドリング


しかったんです
個人情
攻撃受けなす術もなく

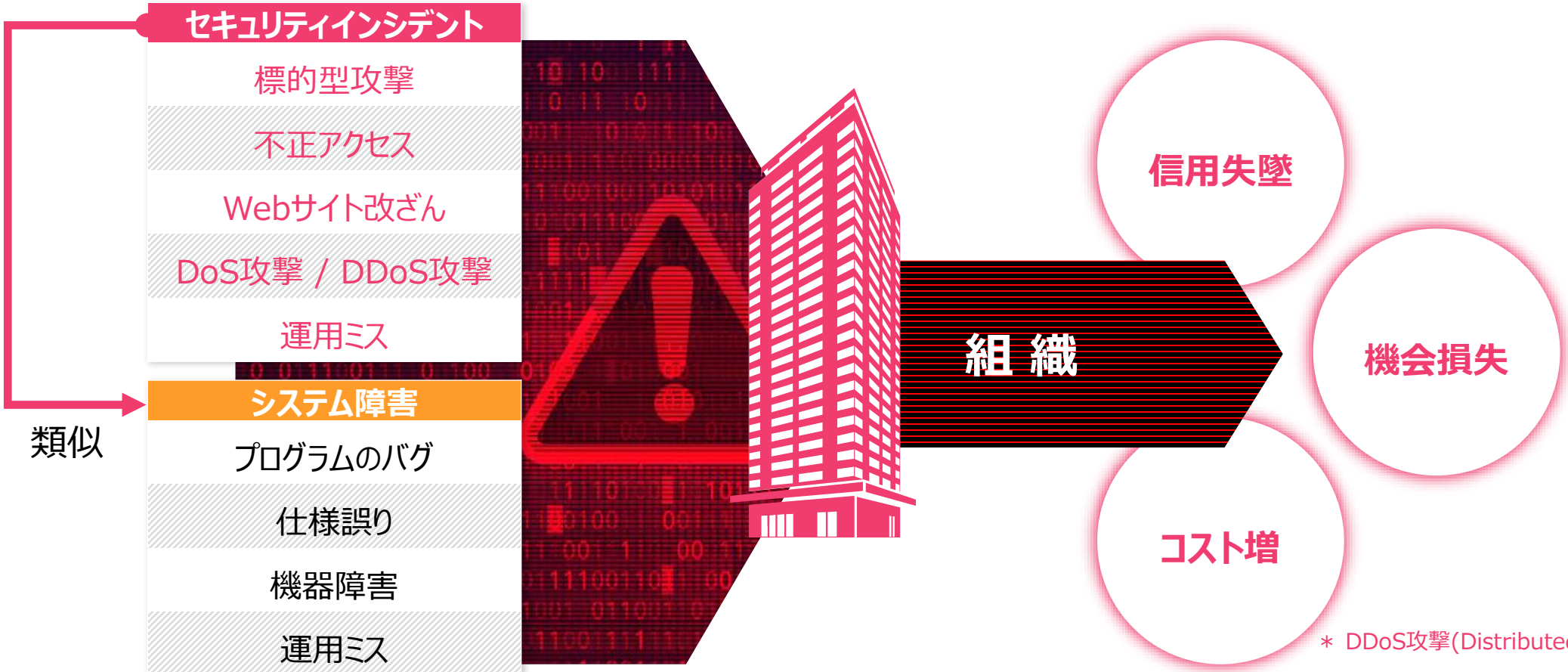
サイバー攻撃、セキュリティインシデントは

システム障害と同様に**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
- …

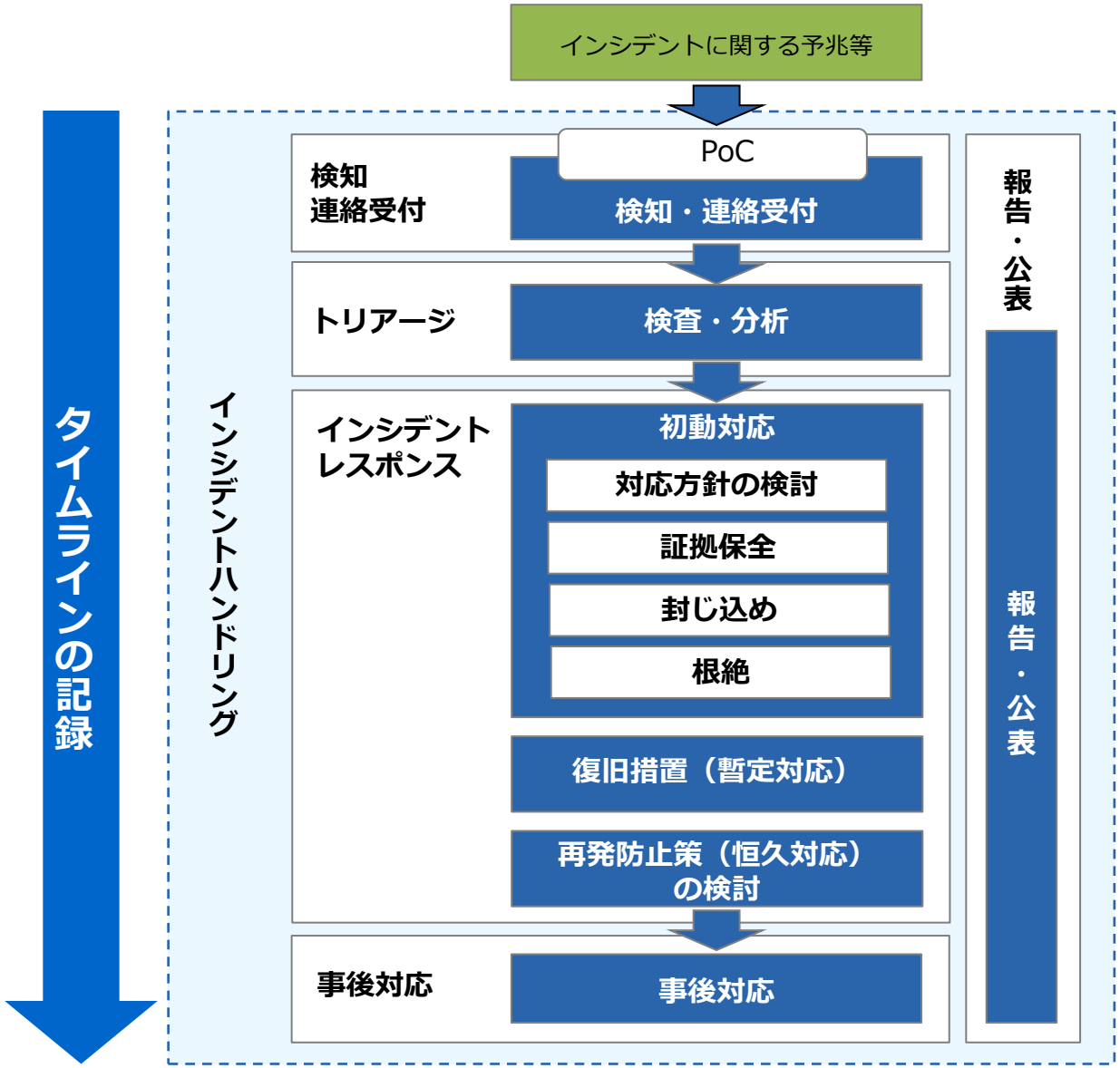
セキュリティインシデントとは

- 人為的なトラブルのほか、自然災害も含まれます。
- 悪意を持って引き起こされた不正アクセスやWebサイト改ざん等のサイバー攻撃のほか、運用ミス、端末やUSBメモリの紛失、災害等によって生じる問題もセキュリティインシデントです。



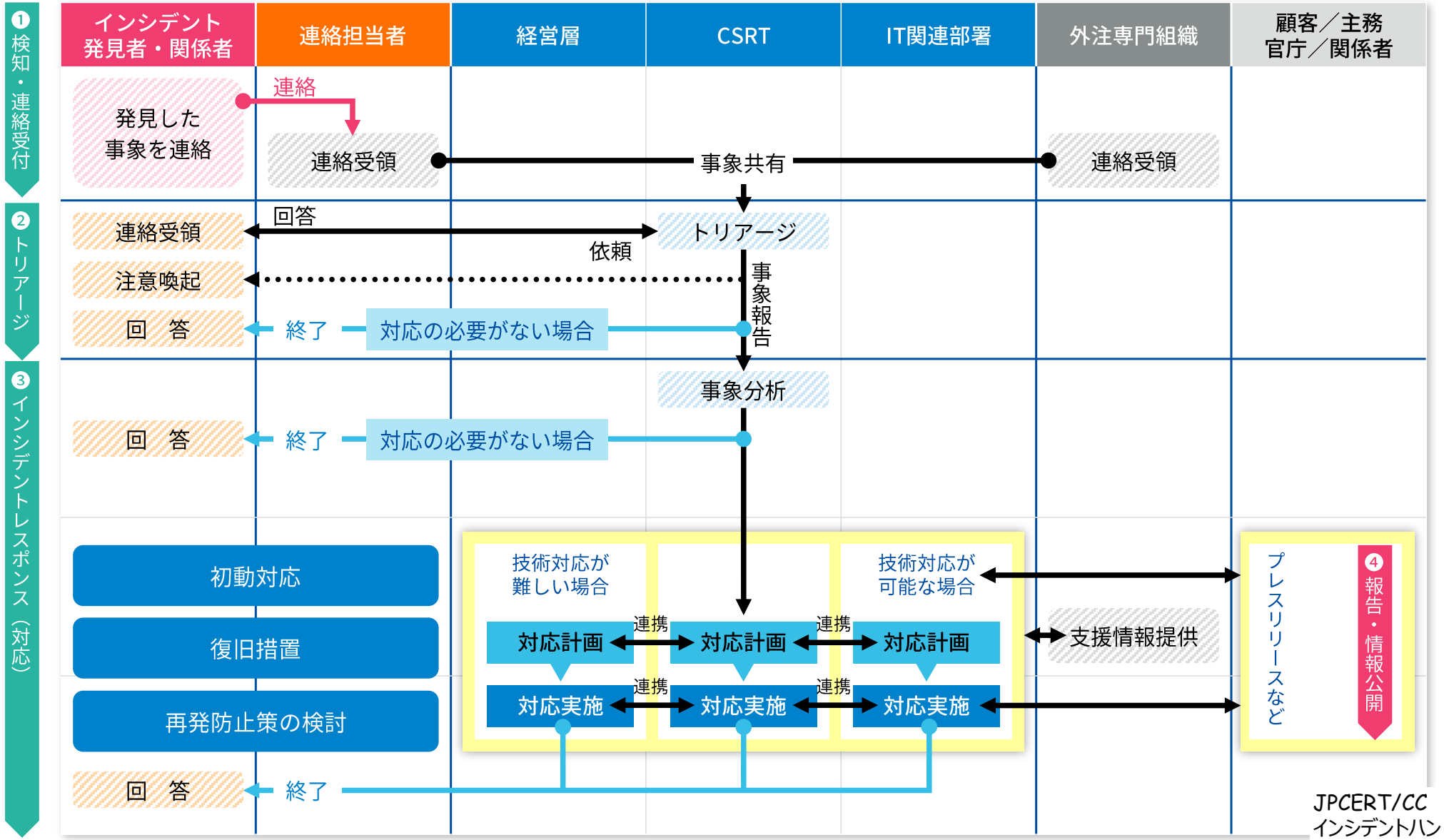
＊ DDoS攻撃(Distributed Denial of Service attack)
： 分散型サービス拒否攻撃

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。

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

インシデントハンドリングステップとシステム障害対応の対比

ステップ	内 容	インシデント対応の例	システム障害対応の例
検知・連絡受付	●インシデントが発生した旨の連絡を受領 ●関係各所に報告	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。	市場への入金処理が大量に実施されていないクレームが、運用オペレーションセンターに届いた。
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。	調査の結果、新機能リリースに伴うバッチ処理変更に漏れがあり、センターカット(集中記帳)用のデータ作成に失敗。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。	センターカット用訂正データ作成、臨時ジョブ実行により、入金を処理実施した。 新機能に伴うバッチ処理の手順を追加した。
報告・公表	●被害状況や影響範囲に応じて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。	システム障害により顧客に影響のある障害を発生させた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。	発生した障害について報告書に取りまとめた。

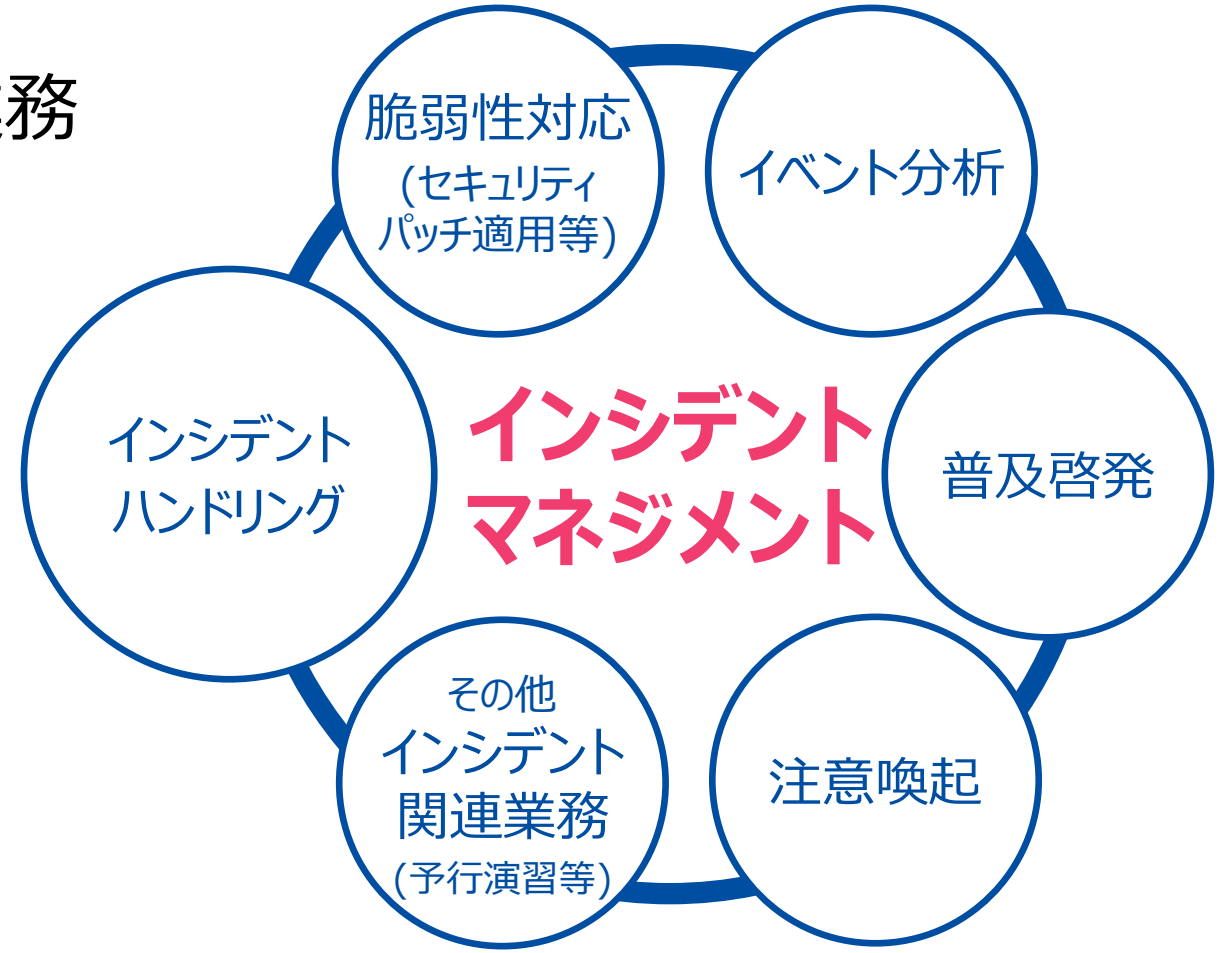
※ SOC事業者: 外部からネットワーク機器やサーバー類を常時監視し、サイバー攻撃の検出と分析、対応策のアドバイスを提供する組織、企業のこと

もしアナタの組織にインシデントが発生したら?

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

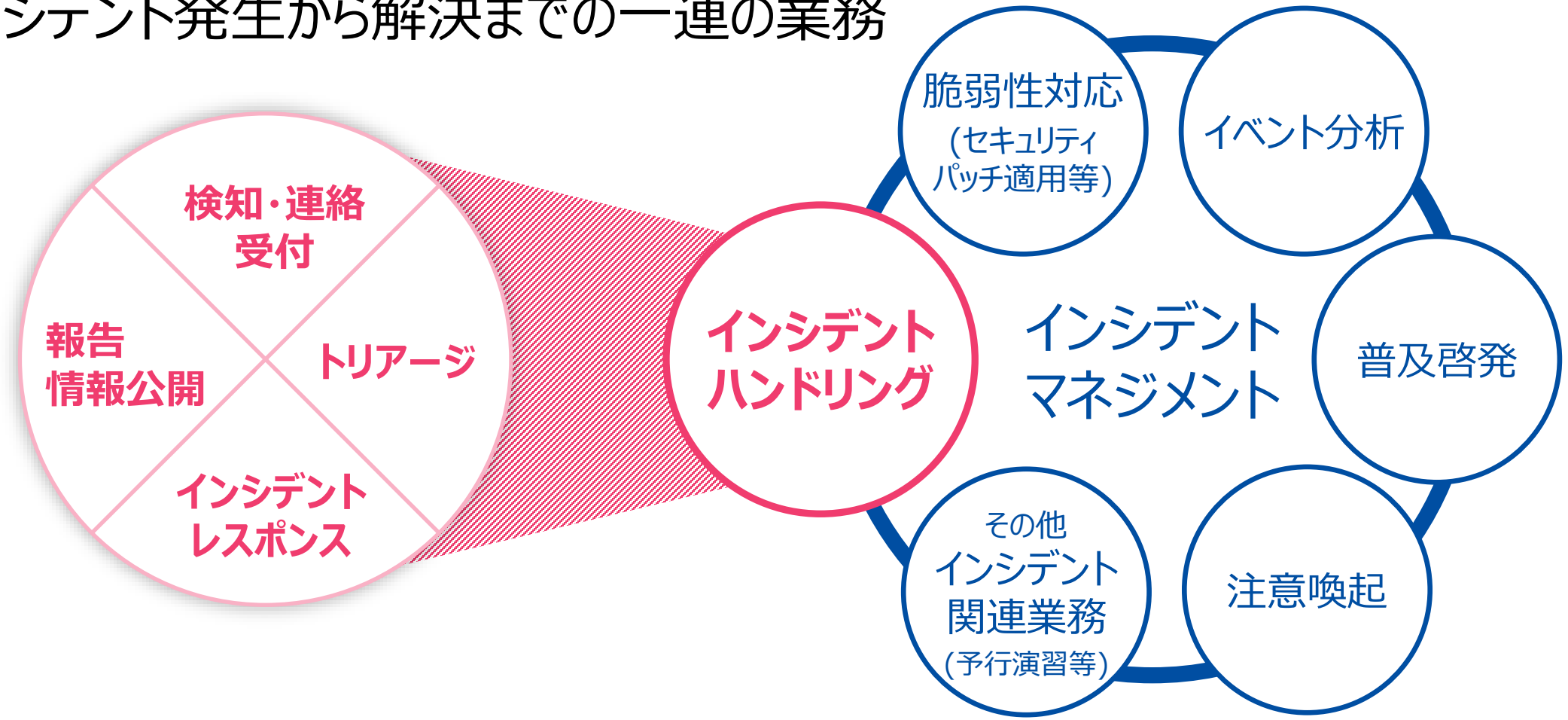
- CSIRTが「事前」の準備を含めた
  インシデントに対して行う一連の業務



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

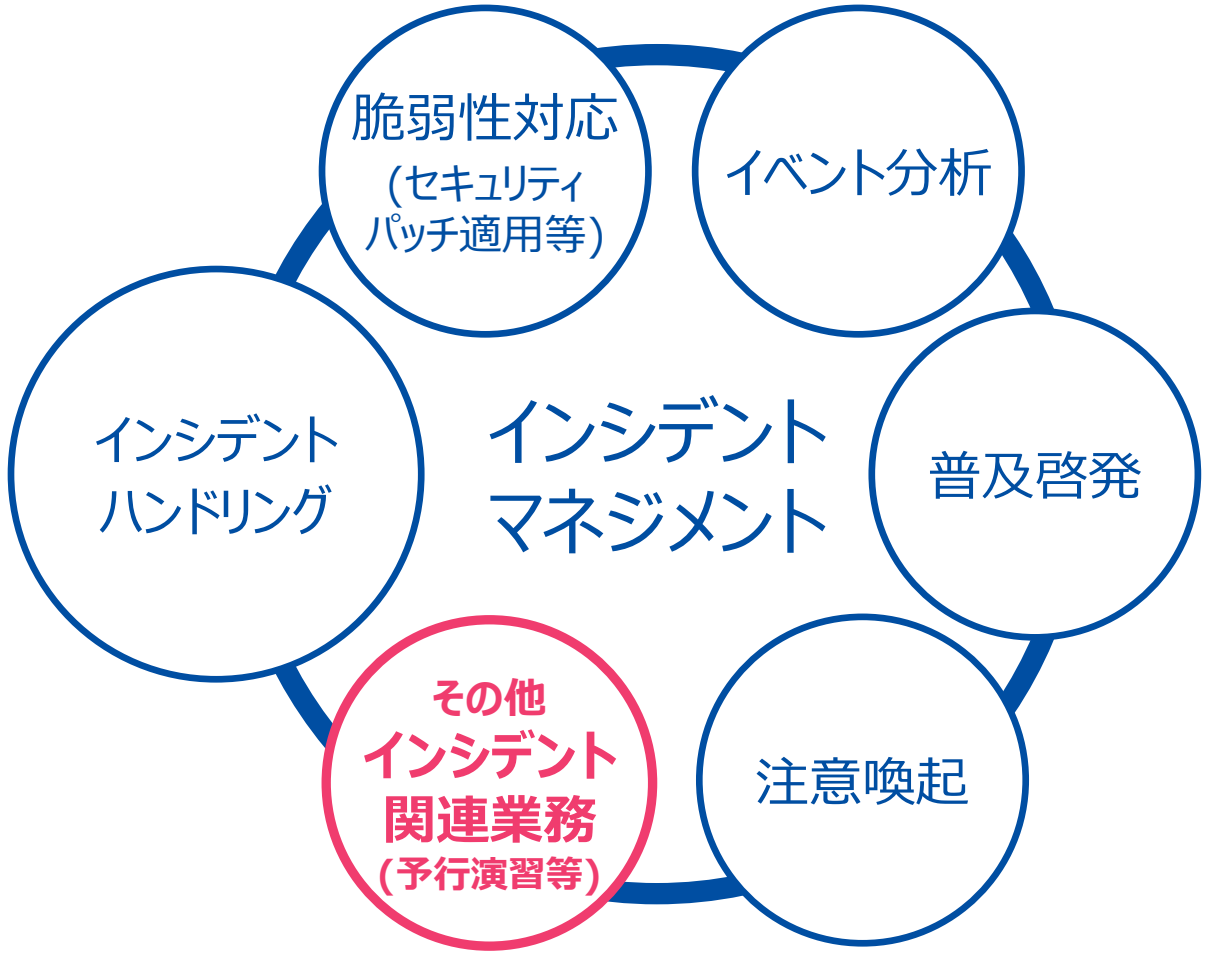
- インシデント発生から解決までの一連の業務



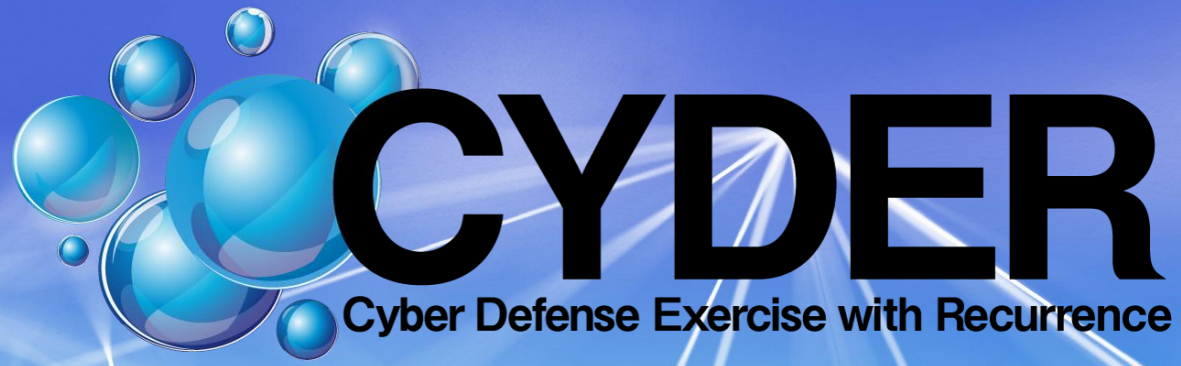
教育・訓練

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



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

New

初級、 中級、準上級、オンライン(入門・プレCYDER)

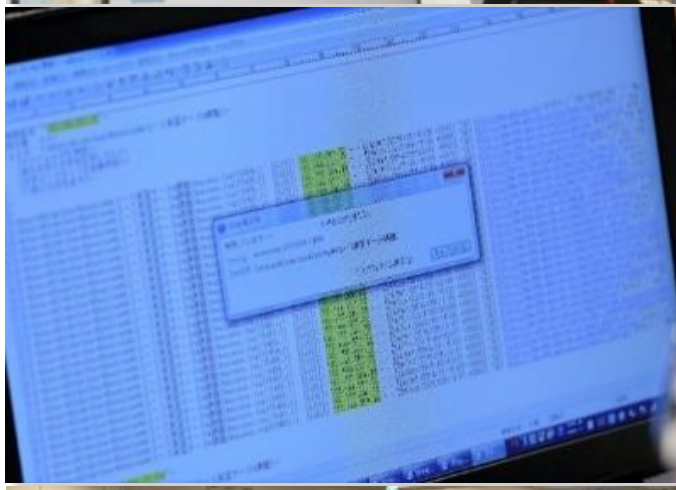
- 最大4名のグループワーク、ハンズオン　等
- 国の機関、地方公共団体等の職員の方は受講料が無料
- **新作シナリオ**続々、**繰り返し受講**が効果的
- 受講後に発生した**インシデント対応に役立った**例

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**

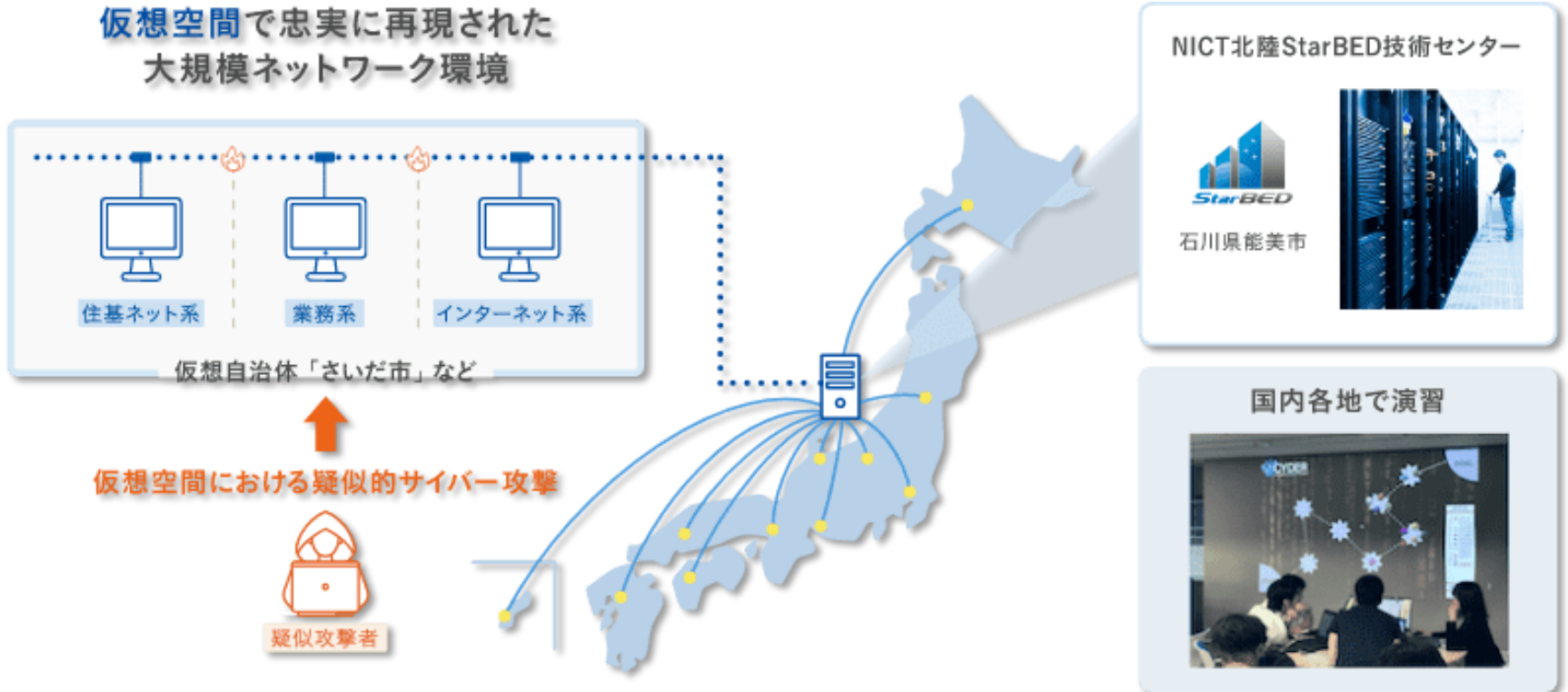


サイダー CYDERとは
Cyber Defense Exercise with Recurrence

CYDER(Cyber Defense Exercise with Recurrence)

✓実践的サイバー防御演習のことであり、サイバー攻撃を受けた際の一連の対応(インシデント対応)をPCを操作しながらロールプレイ形式で体験できる演習。

✓実際のネットワーク環境を再現したリアルな環境で一連の流れを体験。



CYDERの提供コース

CYDERは、学習レベル、対象組織、演習形式によってコースが分かれており、受講目的やスキル等に合わせてコース選択可能。

		Aコース	B-1コース	B-2コース	Cコース	プレCYDER
レベル		初級	中級	中級	準上級	–
対象組織		全ての組織	地方公共団体	国の機関	全ての組織	国の機関
				重要社会基盤事業者等		地方公共団体等
開催場所		全国47都道府県	全国11地域	東京・大阪名古屋	東京	オンライン
演習項目		事前学習 ハンズオン グループワーク	事前学習 ハンズオン グループワーク	事前学習 ハンズオン グループワーク	事前学習 ハンズオン グループワーク	–
期間	事前学習	2～5時間程度				なし
	演習	1日間	1日間	1日間	2日間	2～3時間程度

CYDER Aコース 内容紹介

- ある仮想組織の一員となって、そこで発生するインシデントに対応する。
- インシデントハンドリングのフェーズごとに課題があり、
1つ1つのフェーズの内容を体験することにより、理解を深める。
- 課題には、ディスカッション課題とハンズオン課題がある。
  - ディスカッション課題はグループで課題に取り組み、対策を検討する。
  - ハンズオン課題は、個人で課題課題に取り組み、実機を使用した技術的な調査解析を行う。
- インシデント対応とはどのようなことをするのか、
何を考えればよいのかを知り、普段からどのような準備をすれば
よいかを考えるきっかけとなる。

コンテンツ例 – 配布テキストから抜粋

演習の説明、シナリオの舞台設定、課題の解説、詳細な
ハンズオン手順(ツール等の詳しい操作方法を含む)のテキストを提供。

実習舞台設定（概要）

ビデオガイド

- 皆さんは「さいだ市」の職員で、組織内の情報システムネットワークを管理する総務部情報管理課に所属しています。
- 情報システムを扱う部署としてネットワーク運用、保守はもとより、CSIRTとして組織内で発生したセキュリティインシデントに対応するミッションを持っています。

さいだ市

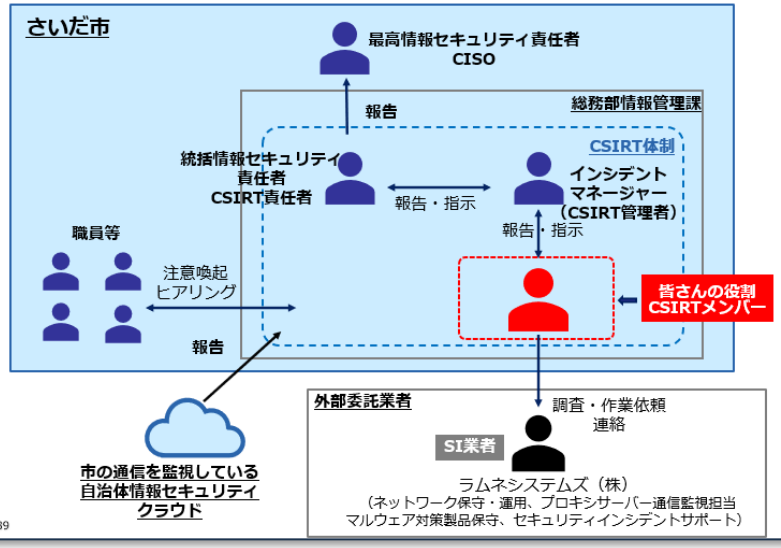
面積：84.87 km²　人口：168,245 人

県北部に位置し、県庁所在地から北東約40kmに位置し、中心地域は県北部の中心都市としての性格を有している。
総務省のインターネット分離に関するガイドラインを受け、内部ネットワークをより強固にするために、2019年度に調達を実施し、県内有数のSI業者であるラムネシステムズ（株）によって、自治体情報システム強靭性向上モデルに基づく組織内ネットワークの3分割（*1）および適切な強靭化の施策は完了している。
また、さらなる強靭化を図るため、端末からの情報持ち出し対策、二要素認証などを検討中で来年度には実現する予定である。なお、職員が利用する端末はインターネット接続系およびLGWAN接続系ともに現時点では全台物理端末を利用している。
また、自治体情報セキュリティクラウドについては、県側と連携しながら利用中である。

（*1）2020年12月に改訂されたガイドラインにおける「αモデル」に相当

Page 37

実習舞台設定（登場人物相関）



Page 39

ハンズオン【課題2】メモリ保全手順（5/6）

メモリ保全実行

メモリ保全完了までの時間は端末環境に依存します。
本演習では5分以上時間を要する場合があります。

- メモリを保全が正常終了すると次のような表示になります。

```
c:¥Users¥cyderuser¥Desktop¥Aコース¥課題2>winpmem -d -t -o memdump.aff4
2020-06-15 16:55:30 W Output file memdump.aff4 will be truncated.

c:¥Users¥cyderuser¥Desktop¥Aコース¥課題2>_
```

-dオプションをつけることで、実行直後にメッセージが表示されます。

- 「dir」コマンドを実行し、ファイルが作成されたことを確認します。

```
c:¥Users¥cyderuser¥Desktop¥Aコース¥課題2>dir
 ドライブ C のボリューム ラベルがありません。
 ボリューム シリアル番号は A2AF-59DF です

 c:¥Users¥cyderuser¥Desktop¥Aコース¥課題

2020/06/15  17:10    <DIR>          .
2020/06/15  17:10    <DIR>          ..
2020/06/15  17:13     8,641,518,767 memdump.aff4
2020/06/15  14:22         2,549,056 winpmem.exe
               2 個のファイル        8,644,067,823 バイト
               2 個のディレクトリ  41,828,872,192 バイトの空き領域

c:¥Users¥cyderuser¥Desktop¥Aコース¥課題2>_
```

①dirコマンドを実行します。

②メモリデータを保全したファイルが作成されていることを確認します。

Page 101

実習課題例

課題	テーマ	ディスカッション課題	ハンズオン課題	課題概要
1	検知・連絡受付、 トリアージ、 対応方針の検討	○		発生している事象に対する 対応の優先度付け
2	証拠保全		○	インシデントに関する 証拠の保全 **(ハンズオン)**
3	封じ込め・根絶	○	○	影響範囲の特定と 対応方針の検討 **(ハンズオン)**
4	復旧措置・再発防止策の検討	○		インシデント収束に向けた 対応の検討
5	報告・公表	報告書作成		

ディスカッション課題例

状況説明

現在2024/2/9 15:45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。

ハンズオン課題例

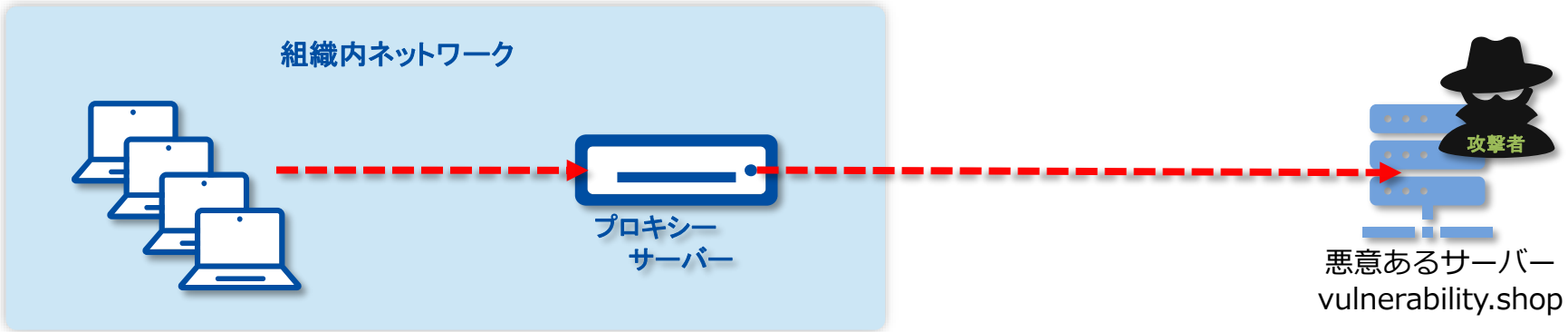
状況説明

※ vulnerability.shop は演習上の架空のホストです。

セキュリティ監視センターから以下の連絡がありました。
「あなたの組織から、悪意あるサーバーに向けて不審な通信が発信しています。
通信情報は以下の通り。

通信先ホスト名： vulnerability.shop※
通信先URL　　： http://vulnerability.shop/index/?87329...

上記の通信先ホストと通信している機器があるか、調査をしなさい。
もし、その機器が存在する場合、何台あるか、また、それぞれの機器の
IPアドレス、通信回数についても調査しなさい。



ハンズオンの実施イメージ

access.log - メモ帳

(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:
"http://5pb.jp/games/topics/3134.html"
Gecko) Chrome/51.0.2704.79 Safari/537.3
192.168.110.141 - - [10/Jun/2019:11:15:
HTTP/1.1" 200 1366 963 "http://live.nic
AppleWebKit/537.36 (KHTML, like Gecko)
192.168.110.141 - - [10/Jun/2019:11:15:
HTTP/1.1" 200 1176 960 "http://live.nic
AppleWebKit/537.36 (KHTML, like Gecko)
192.168.110.141 - - [10/Jun/2019:11:15:1
"http://live.nicovideo.jp/watch/lv45847829" "Mozilla/
like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14
192.168.110.123 - - [10/Jun/2019:11:15:11 +0900] "POST http://
NT 10.0; Win64; x64; ServiceUI 8) AppleWebKit/537.36 (KHTML, like
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"

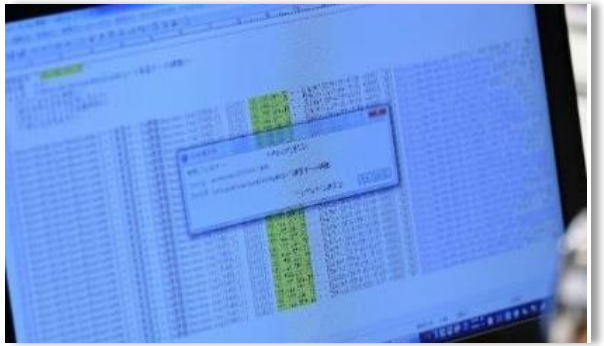
膨大なログの中から
不正な通信を見つけ出す

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

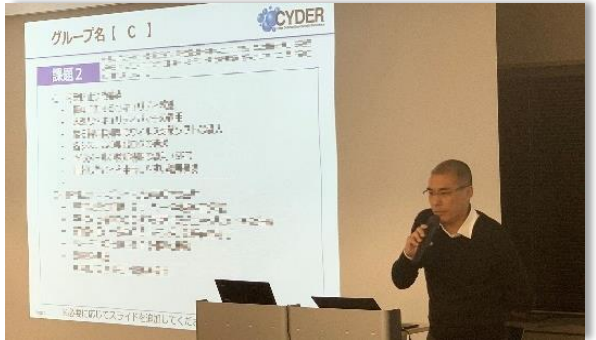


チューターによるサポート

マルウェア挙動調査

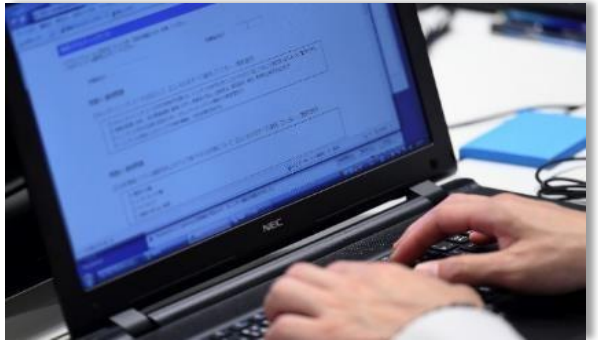
グループワーク

発表



報告書作成

確認テスト



CYDER Aコース 受講者の声 -アンケート結果より

- 発生したインシデントに対して、初動時にとるべき対応、その後根絶に至るまで、今までは外部委託業者任せとなっていたが、その内容について少しでも理解することができたので自分と組織にとって非常に大きな成果だと思いました。
- インシデント発生から収束までの流れを体験することはなかなかできないため、とてもよかった。また、同じグループの人と情報交換(立場が近い人と話をすること)ができたことは本当に良かった。
- 組織ぐるみで、脅威対策の必要を感じた。元の知識不足もあり、理解が追い付かないところがあったが、専門的とは言わなくとも、知識を身に着けておくことは必要だと感じた。

⇨**CYDER Aコースの受講により、自組織における準備の必要性や必要な対策について、気付きを得ていただけます。**

なお、自組織のセキュリティリスクを可視化し、将来的にサイバー侵害を受ける可能性を調査するために、セキュリティアセスメントを使用することも有用です。

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

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がっちり！最近のセキュリティ動向

セキュリティインシデント & インシデントハンドリング

もしアナタの組織にインシデントが発生したら?

- 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)

National Cyber Training Center

ナショナルサイバートレーニングセンター

中途採用強化中。出向受け入れもやっています。ご相談ください。

【中途採用強化中】研究員が語る、国立研究開発法人情報通信研究機構（NICT）ならではのやりがいとは？

2024.02.09 | Sponsored

【中途採用強化中】国立研究開発法人情報通信研究機構（NICT）の「女性初の研究所長」に働きがいを聞いた

2023.11.29 | Sponsored

【中途採用強化中】研究員が語る、国立研究開発法人情報通信研究機構（NICT）で身につくスキルとは？

2024.01.15 | Sponsored

【中途採用強化中】“日本社会のリテラシー向上を担っている”国立研究開発法人情報通信研究機構（NICT）で働く魅力

2023.08.30 | Sponsored

【中途採用強化中】“転職組”の研究員たちが、国立研究開発法人情報通信研究機構（NICT）を選んだワケ

2023.12.26 | Sponsored

【中途採用強化中】“国のセキュリティ人材を育てる”国立研究開発法人情報通信研究機構（NICT）の仕事とは？

2023.07.28 | Sponsored

日本を守る“サイバーセキュリティ”｜新R25 - シゴトも人生も、もっと楽しもう。https://r25.jp/series/cybersecurity

ご参考資料

CYDER

Cyber Defense Exercise with Recurrence

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)

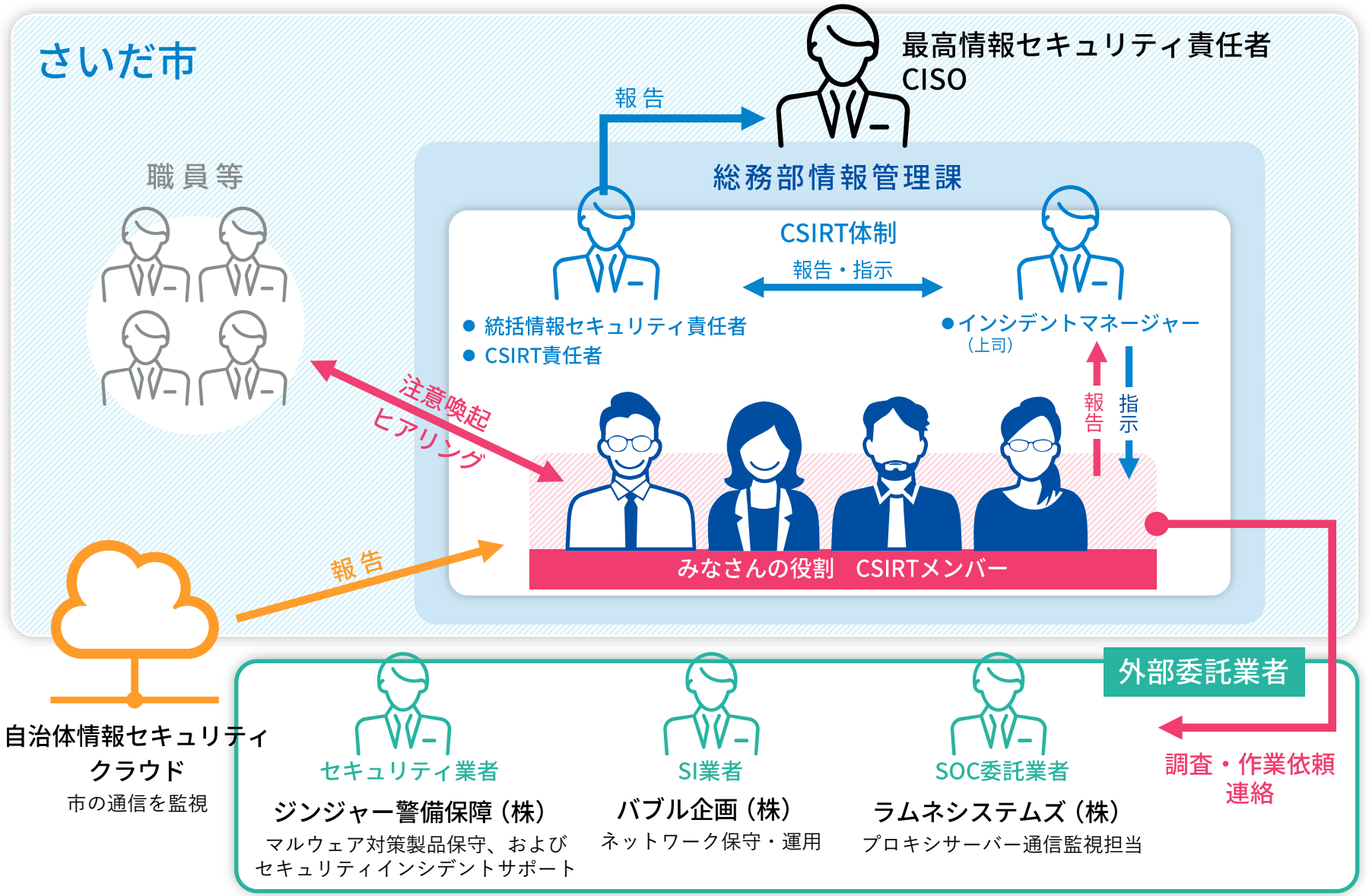
2023年度実施内容および対象組織

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

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
職員等
総務部情報管理課
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）
報告
指示
注意喚起
ヒアリング
報告
みなさんの役割　CSIRTメンバー
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

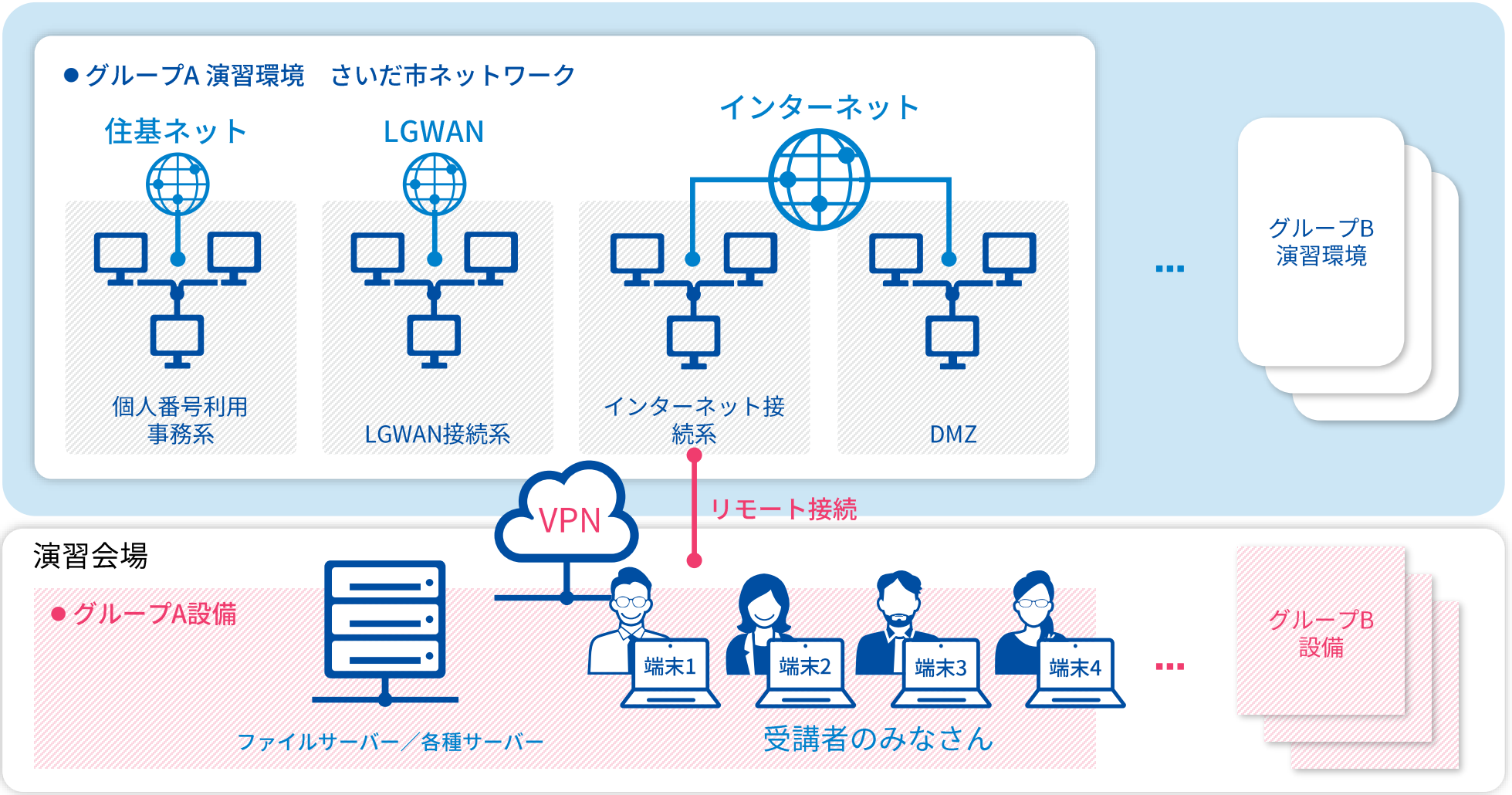
■ Hands-on はハンズオン課題、それ以外はディスカッション課題です。
※ディスカッションで検討した内容について、数チームに発表していただきます。その他チームからの質問、助言等の意見交換を行います。

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。



National Cyber Training Center

CYBERSECURITY

Research Institute


NICT
国立研究開発法人
情報通信研究機構