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

サイバーセキュリティセミナー in ResorTech Okinawa

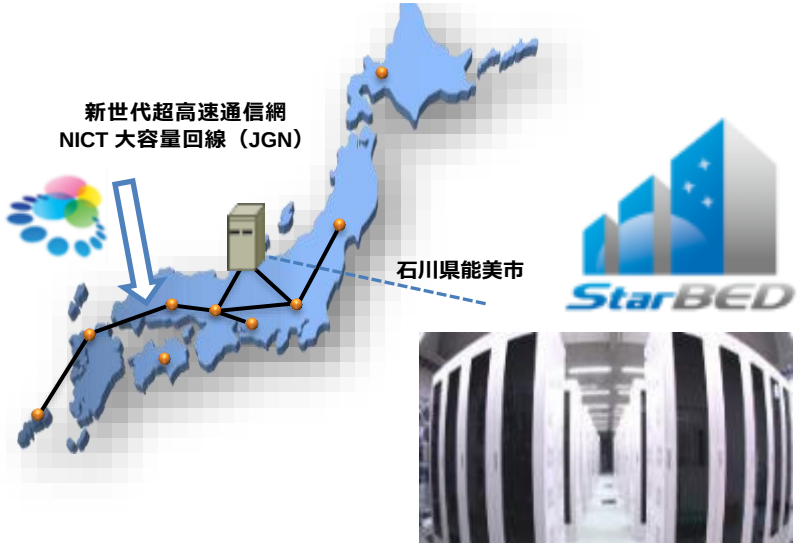
【講演2】40分でわかる実践的防御演習CYDER
(主に自治体の皆様向けバージョン)

花田 智洋 (Tomohiro Hanada)

2021/11/25

国立研究開発法人 情報通信研究機構(NICT)

情報通信分野を専門とする我が国唯一の公的研究機関



自己紹介

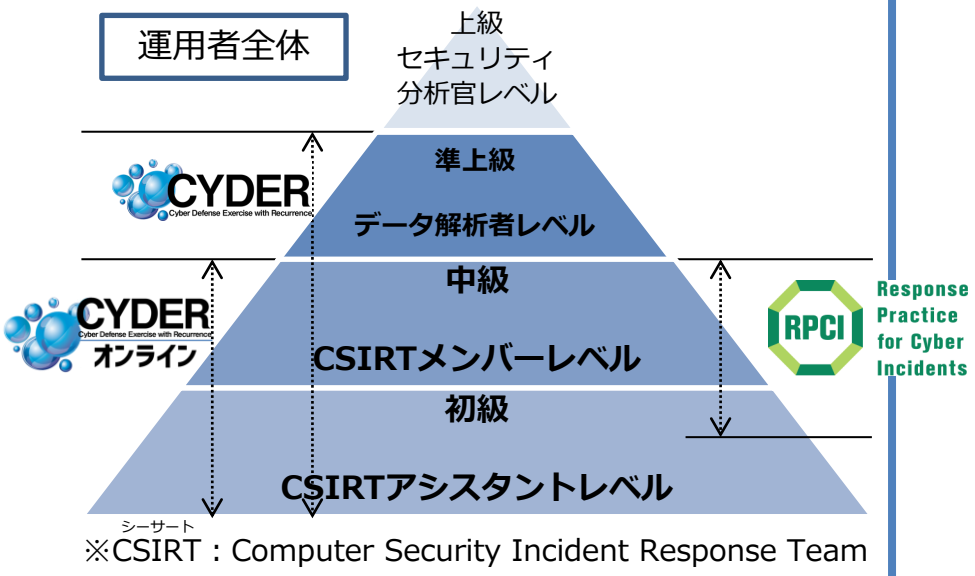
- 氏名: 花田 智洋 (Tomohiro Hanada)
- 勤務先: 2017年1月～
  - NICTサイバーセキュリティ研究所
    ナショナルサイバートレーニングセンター(通称: ナショトレ)
  - CYDER, RPCI, SecHack365,
    CYDERANGE開発等に携わる
- 前職: ～2016年12月末
  - 銀行システムのプロマネ
- 業務外活動:
  - 情報セキュリティコミュニティ運営

「ナショナルサイバートレーニングセンター」の概要

情報通信分野を専門とする我が国唯一の公的研究機関である**NICTの技術的知見、研究成果、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**

セキュリティオペレーター（実践的運用者）の育成

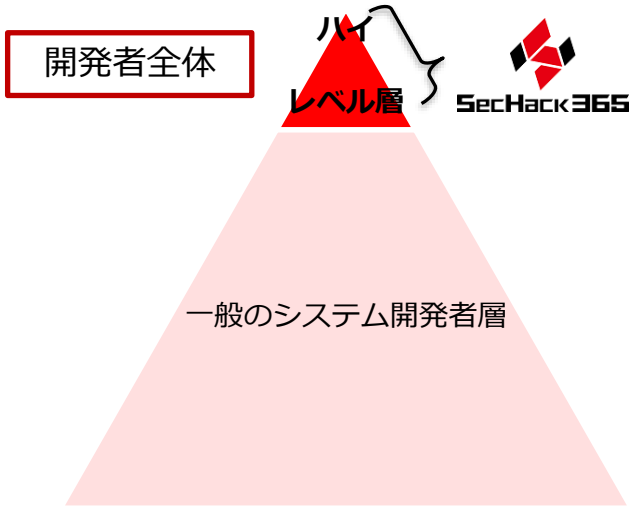
- **行政機関や民間企業等の組織内のセキュリティ運用者（情報システム担当者等）を対象**
- **所属組織が深刻なサイバー攻撃を受けた段階等（＝「有事」）における実践的なインシデント対応能力を育成**



※CSIRT：Computer Security Incident Response Team

セキュリティイノベーター（革新的研究・開発者）の育成

- **セキュリティマインドを持ち、既存ツールを単に「ユーザー」として利用するだけではなく、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**



おしながき

- はじめに
  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のご紹介
- トレンドとキーワードで確認する
  最近のセキュリティニュースやインシデント事例
- インシデントハンドリングとは
- 実践的サイバー防御演習CYDER

NICT National Institute of Information and Communications Technology

トレンドとキーワードで確認する

最近のセキュリティニュースやインシデント事例

CYDER
Cyber Defense Exercise with Recurrence

トレンドで確認!! 最近のセキュリティニュースやインシデント事例

	サイバー情報共有イニシアティブ（J-CSIP） 運用状況	情報セキュリティ安心相談窓口の相談状況	情報セキュリティ10大脅威 2021		情報セキュリティ監査人が選ぶ2021年の情報セキュリティ十大トレンド	2020年セキュリティ十大ニュース
	2021年7月～9月	2021年第3四半期（7月～9月）	個人	組織		
1	ビジネスメール詐欺（BEC）の事例	「ウイルス検出の偽警告」に関する相談	スマホ決済の不正利用	ランサムウェアによる被害	テレワークニーズに追いつかないセキュリティ対策	新型コロナウイルス感染症　七都府県に緊急事態宣言
2	外部から入手したURLリンク付きの画像ファイルがセキュリティ製品で検知された事例	「仮想通貨で金銭を要求する迷惑メール」に関する相談	フィッシングによる個人情報等の詐取	標的型攻撃による機密情報の窃取	史上最悪の天災やパンデミックなどに対応できるIT-BCPへ	ドコモ口座サービスで不正利用発覚
3	自衛隊大規模接種センターを騙るフィッシング	「宅配便業者をかたる偽SMS」に関する相談	ネット上の誹謗・中傷・デマ	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、安全なクラウドサービスへ広がる要求	「デジタル庁」21年に設置へ
4	Excelアドインファイルを悪用した攻撃	「iPhoneに突然表示される不審なカレンダー通知」に関する相談	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃	標的型攻撃の侵入パターンが多様化	東証システム障害で終日売買停止
5	-	「ワンクリック請求」に関する相談	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害	頻発する大規模システム障害への対応	進化を続けるマルウェア「Emotet」の感染急増
6	-	「不正ログイン」に関する相談	インターネットバンキングの不正利用	内部不正による情報漏えい	在宅勤務のセキュリティ対策に求められる説明責任	防衛関連企業、不正アクセス事案の調査結果 を公開
7	-	「Facebookのメッセンジャーに届く動画」に関する相談	インターネット上のサービスからの個人情報の窃取	予期せぬIT基盤の障害に伴う業務停止	手法の高度化が進む金銭目的のサイバー攻撃	GoTo利用し無断キャンセル 千葉のホテル、被害63万円分
8	-	-	偽警告によるインターネット詐欺	インターネット上のサービスへの不正ログイン	在宅勤務者を踏み台にして組織を狙うフィッシング詐欺の横行	期待のISMAP運用開始
9	-	-	不正アプリによるスマートフォン利用者への被害	不注意による情報漏えい等の被害	EasyなネットサービスのEasyな拡大がなりすましの温床に	カプコン、標的型ランサムウェアで最大35万人の個人情報流出か
10	-	-	インターネット上のサービスへの不正ログイン	脆弱性対策情報の公開に伴う悪用増加	ニューノーマルに対応した新たな情報セキュリティ監査	経産省、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定
	https://www.ipa.go.jp/security/J-CSIP/index.html	https://www.ipa.go.jp/security/txt/2021/q2outline.html		https://www.ipa.go.jp/security/vuln/10threats2021.html	https://www.jasa.jp/seminar/sec_trend2021/	https://www.jnsa.org/active/news10/index.html
	2021/10/27	2021/10/19		2021/1/27	2021/1/6	2020/12/25

キーワードで確認!! 最近のセキュリティニュースやインシデント事例

トレンドで確認!! 最近のセキュリティニュースやインシデント事例

	サイバー情報共有イニシアティブ（J-CSIP） 運用状況	情報セキュリティ安心相談窓口の相談状況	情報セキュリティ10大脅威 2021		情報セキュリティ監査人が選ぶ2021年の情報セキュリティ十大トレンド	2020年セキュリティ十大ニュース
	2021年7月～9月	2021年第3四半期（7月～9月）	個人	組織		
1	ビジネスメール詐欺（BEC）の事例	「ウイルス検出の偽警告」に関する相談	スマホ決済の不正利用	ランサムウェアによる被害	テレワークニーズに追いつかないセキュリティ対策	新型コロナウイルス感染症　七都府県に緊急事態宣言
2	外部から入手したURLリンク付きの画像ファイルがセキュリティ製品で検知された事例	「仮想通貨で金銭を要求する迷惑メール」に関する相談	フィッシングによる個人情報等の詐取	標的型攻撃による機密情報の窃取	史上最悪の天災やパンデミックなどに対応できるIT-BCPへ	ドコモ口座サービスで不正利用発覚
3	自衛隊大規模接種センターを騙るフィッシング	「宅配便業者をかたる偽SMS」に関する相談	ネット上の誹謗・中傷・デマ	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、安全なクラウドサービスへ広がる要求	「デジタル庁」21年に設置へ
4	Excelアドインファイルを悪用した攻撃	「iPhoneに突然表示される不審なカレンダー通知」に関する相談	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃	標的型攻撃の侵入パターンが多様化	東証システム障害で終日売買停止
5	-	「ワンクリック請求」に関する相談	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害	頻発する大規模システム障害への対応	進化を続けるマルウェア「Emotet」の感染急増
6	-	「不正ログイン」に関する相談	インターネットバンキングの不正利用	内部不正による情報漏えい	在宅勤務のセキュリティ対策に求められる説明責任	防衛関連企業、不正アクセス事案の調査結果 を公開
7	-	「Facebookのメッセンジャーに届く動画」に関する相談	インターネット上のサービスからの個人情報の窃取	予期せぬIT基盤の障害に伴う業務停止	手法の高度化が進む金銭目的のサイバー攻撃	GoTo利用し無断キャンセル　千葉のホテル、被害63万円分
8	-	-	偽警告によるインターネット詐欺	インターネット上のサービスへの不正ログイン	在宅勤務者を踏み台にして組織を狙うフィッシング詐欺の横行	期待のISMAP運用開始
9	-	-	不正アプリによるスマートフォン利用者への被害	不注意による情報漏えい等の被害	EasyなネットサービスのEasyな拡大がなりすましの温床に	カプコン、標的型ランサムウェアで最大35万人の個人情報流出か
10	-	-	インターネット上のサービスへの不正ログイン	脆弱性対策情報の公開に伴う悪用増加	ニューノーマルに対応した新たな情報セキュリティ監査	経産省、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定
	https://www.ipa.go.jp/security/J-CSIP/index.html	https://www.ipa.go.jp/security/txt/2021/q2outline.html		https://www.ipa.go.jp/security/vuln/10threats2021.html	https://www.jasa.jp/seminar/sec_trend2021/	https://www.jnsa.org/active/news10/index.html
	2021/10/27	2021/10/19		2021/1/27	2021/1/6	2020/12/25

ピックアップ#1: Emotet Returns

Emotetの攻撃活動再開について（2021年11月16日 追記）

2021年11月14日頃から、Emotetの攻撃活動再開の兆候が確認されたという情報があります(*8)。また、Emotetへの感染を狙う攻撃メール（Emotetの攻撃メール）が着信しているという情報も複数観測している状況です。

IPAでは、攻撃メールに添付されていたと思われるWord文書ファイルとExcelファイルを入手し、確認しています。これらは悪意のあるマクロ（プログラム）が仕込まれたもので、今年1月までの攻撃と同様の手口です。引き続き、特にメールを経由して入手したOffice文書ファイルについて、信用できると判断できる場合でなければ、「編集を有効にする」「コンテンツの有効化」というボタンはクリックしないよう注意してください。

今後、攻撃メールの大規模なばらまきに発展する可能性もあります。2019年から2020年にかけ、多くの企業・組織が被害に遭いました。念のため、警戒をお願いします。

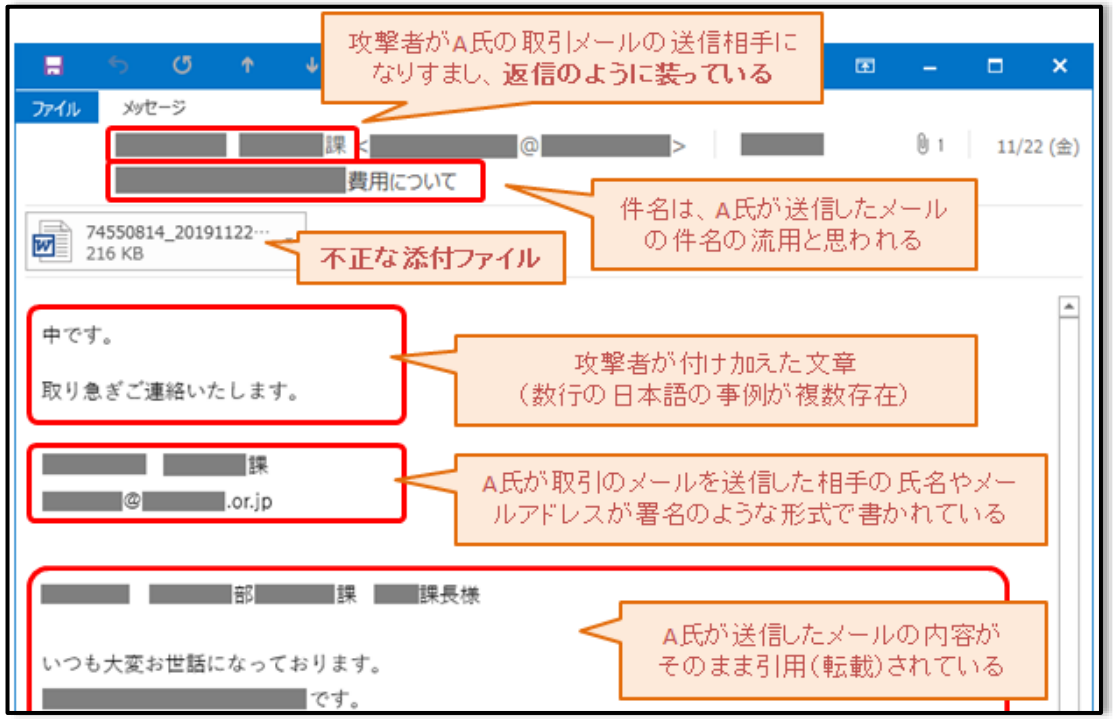
「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/announce/20191202.html#L16

【注意喚起】マルウェアEmotetが10カ月ぶりに活動再開、日本も攻撃対象に | セキュリティ対策のラック
https://www.lac.co.jp/lacwatch/alert/20211119_002801.html

Emotetとは

Emotet(エモテット)はマルウェアの一種。

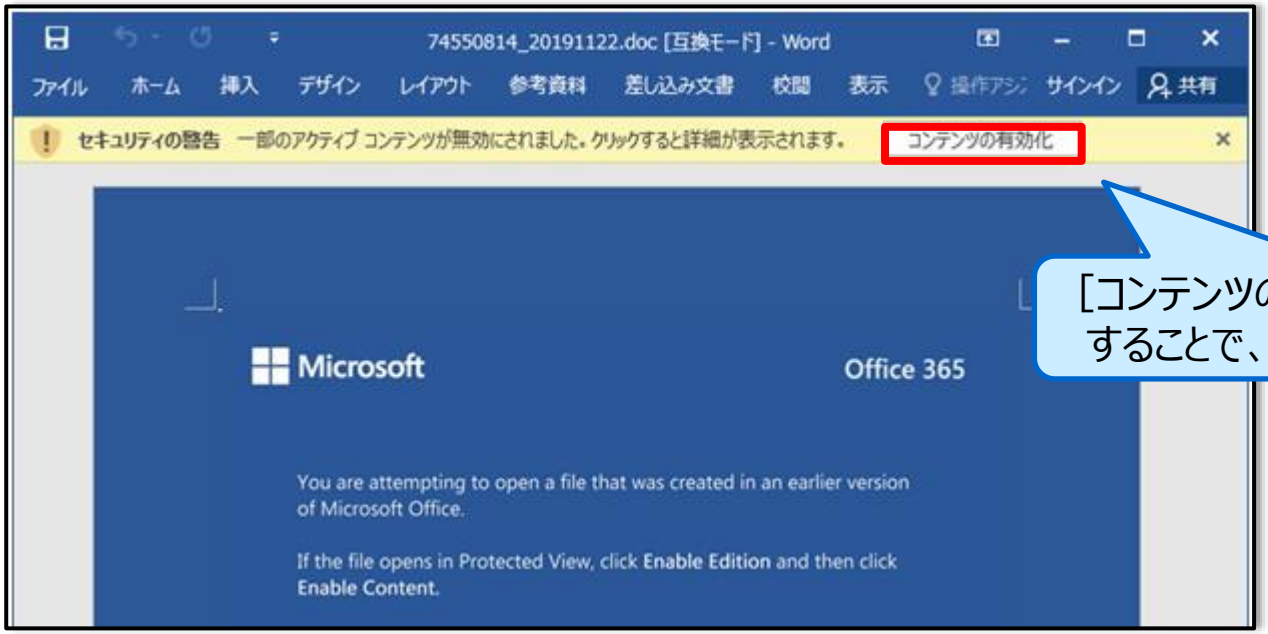
- 主にメールが感染経路。
  - メールの添付ファイルを実行して感染。
  - メールに記載されたURLをクリックしてダウンロードしたファイルを実行して感染。
- Emotetの主な活動は情報搾取と感染拡大。
- Emotetに感染した端末から他者に偽装メールが送信され、さらに感染が拡大。



図はIPAのWebサイト(https://www.ipa.go.jp/security/announce/20191202.html)より引用

Emotet攻撃の手口と対策

Emotetはマクロ機能を悪用して感染する。



図はIPAのWebサイト(https://www.ipa.go.jp/security/announce/20191202.html)より引用

Emotetや同種のマルウェアに感染しないために

- 「コンテンツの有効化」ボタンはクリックしない。
- マクロ機能を無効化する。
- メールに記載されている不審なリンクはクリックしない。
- 端末の脆弱性管理を適切に実施する。
- 不審なメールに対応するための教育を実施する。

トレンドで確認!! 最近のセキュリティニュースやインシデント事例

	サイバー情報共有イニシアティブ（J-CSIP） 運用状況	情報セキュリティ安心相談窓口の相談状況	情報セキュリティ10大脅威 2021		情報セキュリティ監査人が選ぶ2021年の情報セキュリティ十大トレンド	2020年セキュリティ十大ニュース
	2021年7月～9月	2021年第3四半期（7月～9月）	個人	組織		
1	ビジネスメール詐欺（BEC）の事例	「ウイルス検出の偽警告」に関する相談	スマホ決済の不正利用	ランサムウェアによる被害	テレワークニーズに追いつかないセキュリティ対策	新型コロナウイルス感染症　七都府県に緊急事態宣言
2	外部から入手したURLリンク付きの画像ファイルがセキュリティ製品で検知された事例	「仮想通貨で金銭を要求する迷惑メール」に関する相談	フィッシングによる個人情報等の詐取	標的型攻撃による機密情報の窃取	史上最悪の天災やパンデミックなどに対応できるIT-BCPへ	ドコモ口座サービスで不正利用発覚
3	自衛隊大規模接種センターを騙るフィッシング	「宅配便業者をかたる偽SMS」に関する相談	ネット上の誹謗・中傷・デマ	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、安全なクラウドサービスへ広がる要求	「デジタル庁」21年に設置へ
4	Excelアドインファイルを悪用した攻撃	「iPhoneに突然表示される不審なカレンダー通知」に関する相談	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃	標的型攻撃の侵入パターンが多様化	東証システム障害で終日売買停止
5	-	「ワンクリック請求」に関する相談	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害	頻発する大規模システム障害への対応	進化を続けるマルウェア「Emotet」の感染急増
6	-	「不正ログイン」に関する相談	インターネットバンキングの不正利用	内部不正による情報漏えい	在宅勤務のセキュリティ対策に求められる説明責任	防衛関連企業、不正アクセス事案の調査結果 を公開
7	-	「Facebookのメッセンジャーに届く動画」に関する相談	インターネット上のサービスからの個人情報の窃取	予期せぬIT基盤の障害に伴う業務停止	手法の高度化が進む金銭目的のサイバー攻撃	GoTo利用し無断キャンセル　千葉のホテル、被害63万円分
8	-	-	偽警告によるインターネット詐欺	インターネット上のサービスへの不正ログイン	在宅勤務者を踏み台にして組織を狙うフィッシング詐欺の横行	期待のISMAP運用開始
9	-	-	不正アプリによるスマートフォン利用者への被害	不注意による情報漏えい等の被害	EasyなネットサービスのEasyな拡大がなりすましの温床に	カプコン、標的型ランサムウェアで最大35万人の個人情報流出か
10	-	-	インターネット上のサービスへの不正ログイン	脆弱性対策情報の公開に伴う悪用増加	ニューノーマルに対応した新たな情報セキュリティ監査	経産省、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定
	https://www.ipa.go.jp/security/J-CSIP/index.html	https://www.ipa.go.jp/security/txt/2021/q2outline.html		https://www.ipa.go.jp/security/vuln/10threats2021.html	https://www.jasa.jp/seminar/sec_trend2021/	https://www.jnsa.org/active/news10/index.html
	2021/10/27	2021/10/19		2021/1/27	2021/1/6	2020/12/25

ピックアップ#2: テレワーク環境を狙った攻撃

VPN狙うサイバー攻撃で露見　既知の穴塞がぬ日本企業

コラム　＋フォローする

2021年5月23日 2:00 [有料会員限定]

保存

日経XTECH 日経クロステック

セキュリティー対策機器大手の米フォーティネットの製品を巡り、脆弱性を突くサイバー攻撃が相次ぎ問題となってい
の脆弱性で、修正プログラムも提
極的な日本企業が、被害拡大の一

VPN狙うサイバー攻撃で露見　既知の穴塞がぬ日本企業: 日本経済新聞
https://www.nikkei.com/article/DGXZQOUC138DE0T10C21A5000000/

今月(2021年11月)公開されたレポートでの報告内容

- RDP(Remote Desktop Protocol)を経由した侵入を目的とした攻撃が増加。
- 力技での突破を試みる総当り攻撃が多い。

脅威レポート T2 2021 | ESET https://www.eset.com/jp/blog/threat-report/2021-t2/

トレンドで確認!! 最近のセキュリティニュースやインシデント事例

	サイバー情報共有イニシアティブ（J-CSIP） 運用状況	情報セキュリティ安心相談窓口の相談状況	情報セキュリティ10大脅威 2021		情報セキュリティ監査人が選ぶ2021年の情報セキュリティ十大トレンド	2020年セキュリティ十大ニュース
	2021年7月～9月	2021年第3四半期（7月～9月）	個人	組織		
1	ビジネスメール詐欺（BEC）の事例	「ウイルス検出の偽警告」に関する相談	スマホ決済の不正利用	ランサムウェアによる被害	テレワークニーズに追いつかないセキュリティ対策	新型コロナウイルス感染症　七都府県に緊急事態宣言
2	外部から入手したURLリンク付きの画像ファイルがセキュリティ製品で検知された事例	「仮想通貨で金銭を要求する迷惑メール」に関する相談	フィッシングによる個人情報等の詐取	標的型攻撃による機密情報の窃取	史上最悪の天災やパンデミックなどに対応できるIT-BCPへ	ドコモ口座サービスで不正利用発覚
3	自衛隊大規模接種センターを騙るフィッシング	「宅配便業者をかたる偽SMS」に関する相談	ネット上の誹謗・中傷・デマ	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、安全なクラウドサービスへ広がる要求	「デジタル庁」21年に設置へ
4	Excelアドインファイルを悪用した攻撃	「iPhoneに突然表示される不審なカレンダー通知」に関する相談	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃	標的型攻撃の侵入パターンが多様化	東証システム障害で終日売買停止
5	-	「ワンクリック請求」に関する相談	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害	頻発する大規模システム障害への対応	進化を続けるマルウェア「Emotet」の感染急増
6	-	「不正ログイン」に関する相談	インターネットバンキングの不正利用	内部不正による情報漏えい	在宅勤務のセキュリティ対策に求められる説明責任	防衛関連企業、不正アクセス事案の調査結果 を公開
7	-	「Facebookのメッセンジャーに届く動画」に関する相談	インターネット上のサービスからの個人情報の窃取	予期せぬIT基盤の障害に伴う業務停止	手法の高度化が進む金銭目的のサイバー攻撃	GoTo利用し無断キャンセル　千葉のホテル、被害63万円分
8	-	-	偽警告によるインターネット詐欺	インターネット上のサービスへの不正ログイン	在宅勤務者を踏み台にして組織を狙うフィッシング詐欺の横行	期待のISMAP運用開始
9	-	-	不正アプリによるスマートフォン利用者への被害	不注意による情報漏えい等の被害	EasyなネットサービスのEasyな拡大がなりすましの温床に	カプコン、標的型ランサムウェアで最大35万人の個人情報流出か
10	-	-	インターネット上のサービスへの不正ログイン	脆弱性対策情報の公開に伴う悪用増加	ニューノーマルに対応した新たな情報セキュリティ監査	経産省、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）を策定
	https://www.ipa.go.jp/security/J-CSIP/index.html	https://www.ipa.go.jp/security/txt/2021/q2outline.html		https://www.ipa.go.jp/security/vuln/10threats2021.html	https://www.jasa.jp/seminar/sec_trend2021/	https://www.jnsa.org/active/news10/index.html
	2021/10/27	2021/10/19		2021/1/27	2021/1/6	2020/12/25

ピックアップ#3: ランサムウェア

徳島県の町立病院でランサムウエア感染、侵入経路は遠隔保守用の通信回線か

横田 宏幸　日経クロステック／日経コンピュータ

2021.11.01

徳島県北部にある、つるぎ町立半田病院は2021年10月31日、ランサムウエアに感染したと発表した。同病院によると、同日の午前0時半、院内の電子カルテシステムにおいて、英語による文書が大量に印刷されているのを病棟看護師が発見した。

文書には「ハッキングしてデータを暗号化した。

徳島県の町立病院でランサムウエア感染、侵入経路は遠隔保守用の通信回線か｜日経クロステック（xTECH）
https://xtech.nikkei.com/atcl/nxt/news/18/11561/

香川県では、近隣で発生したインシデントをきっかけとして、各医療機関向けに以下を実施。

- 注意喚起
- 点検用チェックリスト配布

ランサムウェアによるサイバー攻撃にご注意ください

令和3年10月31日、徳島県の医療機関において、ランサムウェアに感染し、電子カルテシステムが利用停止になる事案が発生しました。

国内外において、ランサムウェアの感染により、データが暗号化されたり、業務情報や個人情報が窃取されたりする事例が相次いで確認されていることから、各医療機関におかれましては、別添資料を御一読のうえ、改めてサイバー攻撃への対策強化の措置を講じていただきますようお願いいたします。

- ランサムウェアに注意（PDF：391KB）
- ランサムウェアを用いる攻撃者グループによる悪用が報告されているソフトウェアや機器等の脆弱性について（令和3年6月28日付厚生労働省事務連絡より抜粋）（PDF：566KB）
- 「医療情報システムの安全管理に関するガイドライン第5.1版（令和3年1月）」に関する情報（外部サイトへリンク）
- チェックリストとフローチャート（エクセル：139KB）

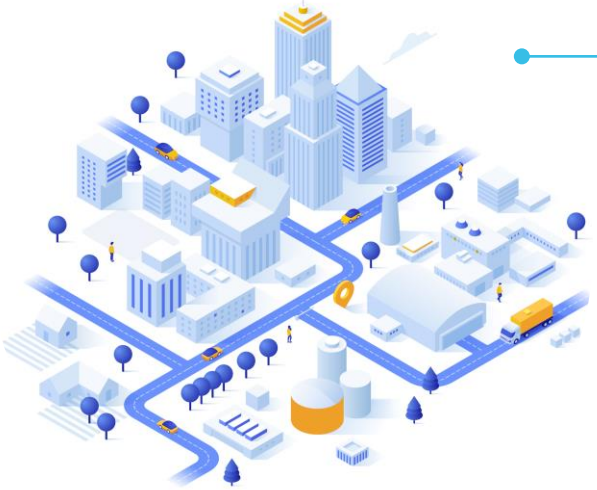
ランサムウェアによるサイバー攻撃にご注意ください｜香川県
https://www.pref.kagawa.lg.jp/imu/iryoushisaku/topics/20211118ransomware.html

National Institute of Information and Communications Technology

インシデントハンドリングとは

CYDER
Cyber Defense Exercise with Recurrence

ケーススタディ



みなさんは「沖縄県さいだ市」の職員です。

みなさんは「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。

さいだ市データ

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、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分割および適切な強靭化の施策は完了している。
- 昨年度、調達を実施。県内有数のSI業者であるバブル企画（株）によってネットワークの3分割は実現された。また更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、現時点は全台物理端末を利用している。
- 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。

- **西田（さいだ）さんはCSIRTとしてセキュリティインシデントに対応するミッションがある。**
- **西田（さいだ）さんは年末へ向けた資料作成の締め切りに追われている。**

色の薄い文字は読まなくても大丈夫です。

西田（さいだ）さんの業務状況

状況1

- CSIRTとしてセキュリティインシデントに対応するミッションがある。
- 年末へ向けた資料作成の締め切りに追われている。

状況2が発生

状況説明

現在2021/11/25 13:15です。

リモートワーク中の職員阿部からCSIRTのPoCに、リモートワークに関連したトラブルが発生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)
午前中のリモートワークには問題ありませんでした。
しかしながら、お昼休みを終えて午後になったら急にリモート接続できなくなってしまいました。
年末へ向けた資料作成をしたいのに困っています。

対応

この通報に対して西田(さいだ)さんはどのような対応をしたら良いでしょうか。

西田（さいだ）さんの業務状況

2021/11/25 13:15現在

状況1

- CSIRTとしてセキュリティインシデントに対応するミッションがある。
- 年末へ向けた資料作成の締め切りに追われている。

状況2

- リモートワーク中の職員阿部からリモートワークに関連したトラブルが発生したという一通の連絡メールが届いた。
- 職員阿部も年末へ向けた資料作成の締め切りに追われている。

状況3が発生

状況説明

現在2021/11/25 13:16です。

久しぶりに庁舎へ出勤した職員金濱からCSIRTのPoCに、マルウェアに関連した
セキュリティインシデントが発生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)
自分宛に届いたメールの添付ファイルを保存したところ、「マルウェアを検知しました」
というポップアップが出ました。
添付ファイルは保存しただけで開いていませんが、何が起きているか分からず不安です！

対応

この通報に対して西田(さいだ)さんはどのような対応をしたら良いでしょうか。

西田（さいだ）さんの業務状況

2021/11/25 13:16現在

状況1

- CSIRTとしてセキュリティインシデントに対応するミッションがある。
- 年末へ向けた資料作成の締め切りに追われている。

状況2

- リモートワーク中の職員阿部からリモートワークに関連したトラブルが発生したという一通の連絡メールが届いた。
- 職員阿部も年末へ向けた資料作成の締め切りに追われている。

状況3

- 久しぶりに庁舎へ出勤した職員金濱からマルウェアに関連したセキュリティインシデントが発生したという一通の連絡メールが届いた。
- 職員金濱は何が起きているか分からず不安のようである。

状況4が発生

状況説明

現在2021/11/25 13:17です。

職員加藤から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。

対応

この通報に対して西田(さいだ)さんはどのような対応をしたら良いでしょうか。

西田（さいだ）さんの業務状況

2021/11/25 13:17現在

状況1

- CSIRTとしてセキュリティインシデントに対応するミッションがある。
- 年末へ向けた資料作成の締め切りに追われている。

状況2

- リモートワーク中の職員阿部からリモートワークに関連したトラブルが発生したという一通の連絡メールが届いた。
- 職員阿部も年末へ向けた資料作成の締め切りに追われている。

状況3

- 久しぶりに庁舎へ出勤した職員金濱からマルウェアに関連したセキュリティインシデントが発生したという一通の連絡メールが届いた。
- 職員金濱は何が起きているか分からず不安のようである。

状況4

- 職員加藤から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いた。
- 職員加藤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。

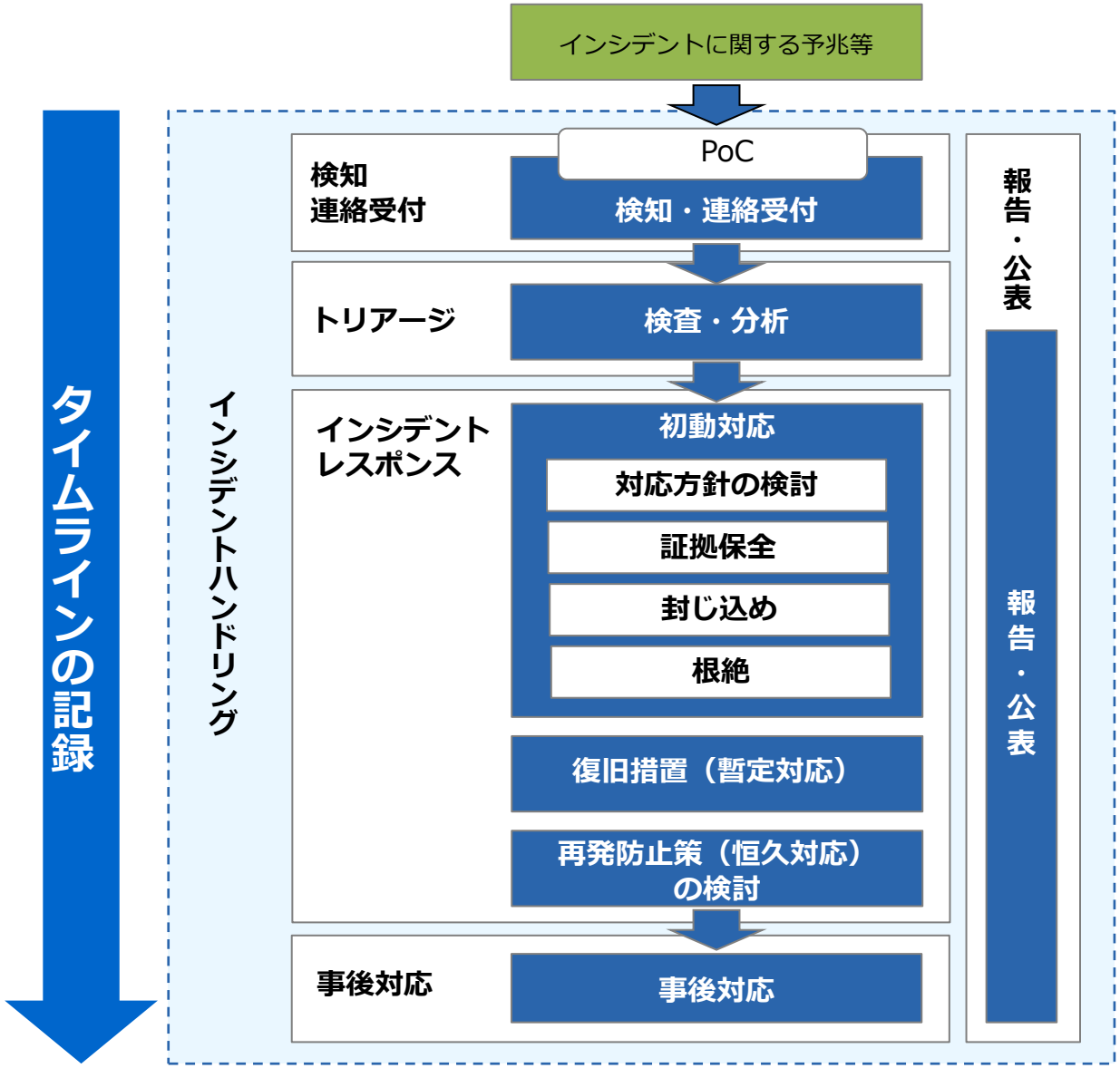
インシデントハンドリング

インシデントマネジメント

「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

■インシデント発生から解決までの一連の業務

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。

教育訓練

インシデントマネジメント

教育訓練の例

- ●ワークショップ
- ●机上演習
- ●実機演習

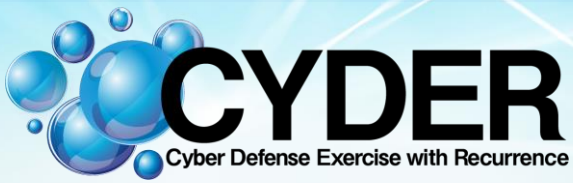
- 正常時の状態把握
- 堅牢な運用管理体制
- 経営と現場の認識合わせ
- ギャップの洗い出し
- ヒヤリハット体験の共有

National
Cyber
Training
Center

人材育成

NICT National Institute of Information and Communications Technology

実践的サイバー防御演習
「CYDER」



たった1ページで分かる CYDER

Cyber Defense Exercise with Recurrence

初級、 中級、準上級、オンライン

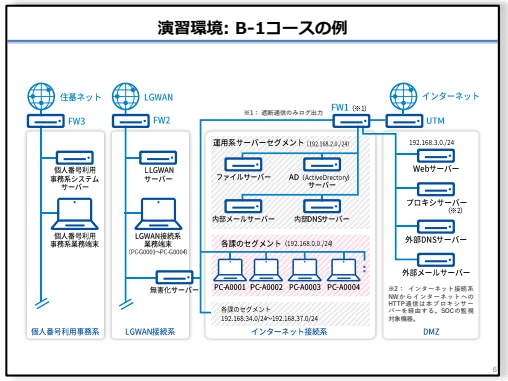
- 最大4名のグループワーク、ハンズオン　等
- 国の機関、地方公共団体等の職員の方は **受講料が無料**
- **新作シナリオ**続々、**繰り返し受講**が効果的
- 受講後に発生した**インシデント対応に役立った**例

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

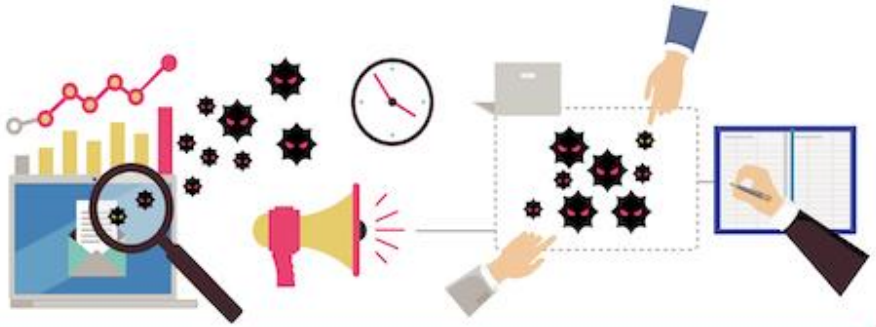


CYDER Aコース、Bコースの演習内容

Aコース(初級)：初心者向け
Bコース(中級)：コンピュータやネットワーク、サイバーセキュリティに関する基礎知識を既にお持ちの方

「事前オンライン学習」と「集合演習(ハンズオン&グループワーク)」により、座学のみで終わらない本格的なトレーニングを受けることができます。

事前オンライン学習により攻撃手法や対策技術に対する理解を深め、集合演習(ハンズオン&グループワーク)を通じて、グループによる一連のインシデントハンドリング(セキュリティ事故への対応)を体験することにより、インシデントレスポンスの手法はもとより、組織で役立つセキュリティポリシー(セキュリティ対応方針)、コミュニケーションの重要性を学びます。



事前オンライン学習
標準学習時間 1時間程度

最近のサイバー攻撃の傾向や対策を理解し、集合演習に必要なインシデントハンドリングの心得について学びます。

集合演習
1日間/回 (例) 9:30～17:30

ハンズオン
端末を用いて、インシデントの検知・報告・影響範囲の特定・隔離、分析・解析、被害状況の確認等を行い、技術的な知識を身につけます。

グループワーク
役割を決め、演習を行うことによって、セキュリティポリシーやインシデントレスポンスの手順などさまざまな気づきの共有を行い、学びを深めます。

参考

事前オンライン学習 サンプル1

第４章　実機演習に必要な知識（使用するツールの紹介）

（標準学習時間：25分）

第４章では、実機演習で必要な知識、使用するツール、使用方法等について紹介します。集合演習当日に利用するツールのためしっかり学んでおきましょう。これからご紹介するソフトウェアは全てフリーです。可能であればソフトウェアをインストールし、触れてみると理解が深まります。

4.1　リモート接続
Windows端末からリモートのLinux端末やWindows端末へアクセスするツールや、ファイルの送受信するツールを学習します。

4.2　メールヘッダ解析
メールヘッダの見方やメールヘッダの詐称の可能性を解説し、不正なメールの見分け方を学習します。

4.3　SPFレコード調査
メールの送信ドメイン認証であるSPFレコードを確認することでメールが詐称されていないことの確認方法を学習します。

4.4　DNS通信ログと出力設定
DNSプロトコルで通信するマルウェアの調査を前提にログ出力の設定方法とログの見方を学習します。

4.5　IOC Finderを使った感染調査
IOCを利用してサイバー攻撃の調査方法の紹介とツールの使い方を学習します。

次ページへ進んで、学習を開始してください。

46

参考

事前オンライン学習 サンプル2

参考1.1 最近のセキュリティ事件・事故

日本語のランサムウェアの登場で国内での被害が増加しています。また、ワナクライのように、ワームとして感染拡大できるランサムウェアが出現し、組織への被害が深刻な事例も増えています。

多様化する脅威　～攻撃の傾向（その２）～

ランサムウェアの被害が増加中

- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、その復元に身代金を要求
- 検出件数が増加、日本語表記のものも確認されており被害が拡大
- Webサイトの脆弱性等を悪用してランサムウェアに感染させるケースが増加中
- 「WannaCrypt(WannaCry、WannaCryptor、Wcry)」（通称：ワナクライ）のように、ワームとして感染拡大する事例が確認された
- 感染したPCだけではなく、共有サーバ等のファイルが暗号化されることも

参考：ランサムウェア「WannaCry(WannaCryptor)」画面

定期的なバックアップと脆弱性対策が重要

CYDER Aコース、Bコースの演習内容

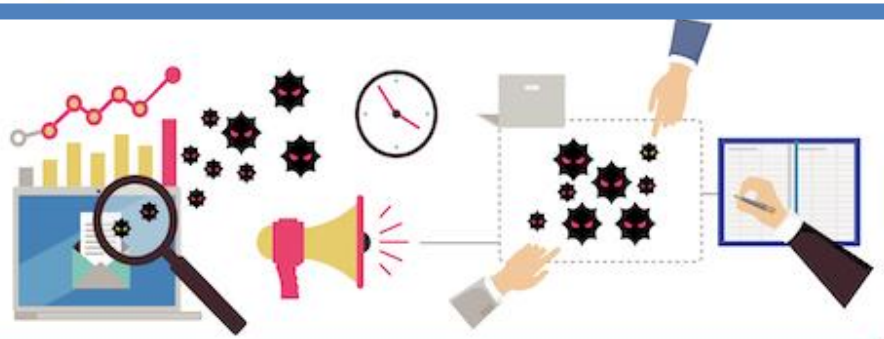
Aコース(初級)：初心者向け
Bコース(中級)：コンピュータやネットワーク、サイバーセキュリティに関する基礎知識を既にお持ちの方

「事前オンライン学習」と「集合演習(ハンズオン&グループワーク)」により、座学のみで終わらない本格的なトレーニングを受けることができます。

事前オンライン学習により攻撃手法や対策技術に対する理解を深め、集合演習(ハンズオン&グループワーク)を通じて、グループによる一連のインシデントハンドリング(セキュリティ事故への対応)を体験することにより、インシデントレスポンスの手法はもとより、組織で役立つセキュリティポリシー(セキュリティ対応方針)、コミュニケーションの重要性を学びます。

事前オンライン学習
標準学習時間 1時間程度

最近のサイバー攻撃の傾向や対策を理解し、集合演習に必要なインシデントハンドリングの心得について学びます。



集合演習
1日間/回 (例) 9:30～17:30

ハンズオン
端末を用いて、インシデントの検知・報告・影響範囲の特定・隔離、分析・解析、被害状況の確認等を行い、技術的な知識を身につけます。

グループワーク
役割を決め、演習を行うことによって、セキュリティポリシーやインシデントレスポンスの手順などさまざまな気づきの共有を行い、学びを深めます。

集合演習の流れ

インシデント発生から解決、事後対応までを体験

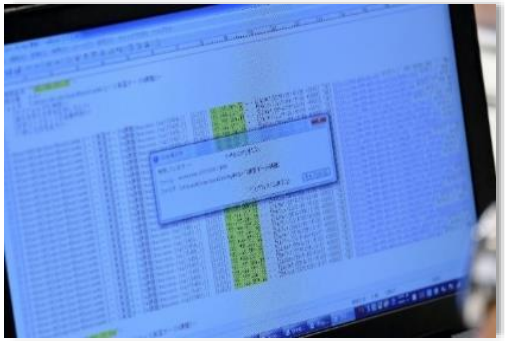
		Aコース	Bコース
Flow 1	― 検知・連絡受付 パソコンやサーバーなどの不審な動作を検知。組織内外からの通報を受け付けます。	説明 実習 解説	実習
Flow 2	― トリアージ（優先順位付け） セキュリティインシデントが疑われる事象に対して、情報収集やログ調査などを行い、事実関係を確認します。インシデントと判断した場合には、被害状況を把握した上で重要度によって対応に優先順位を付けていきます。	説明 実習 解説	実習
Flow 3	― インシデントレスポンス（対応） 組織として、どのように対応すべきか、外部に協力を求める必要があるかなどを検討します。「証拠保全」「封じ込め」「根絶」「復旧措置（暫定対応）」を行います。	説明 実習 解説	実習
Flow 4	― 報告・公表 被害の度合いや影響を及ぼしている範囲に応じて、報告・公表します。組織内部への報告に加えて、被害者、監督官庁や警察機関などの外部関係者にも併せて報告します。	説明 実習 解説	実習
Flow 5	― 事後対応 インシデントに関わったすべての関係者が参加して「振り返り」を実施します。同様のインシデントを防ぐための今後の対応などを含め、最終報告書に取りまとめます。	説明 実習 解説	実習
			全体解説

CYDER演習風景: Aコース（2019年度）

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



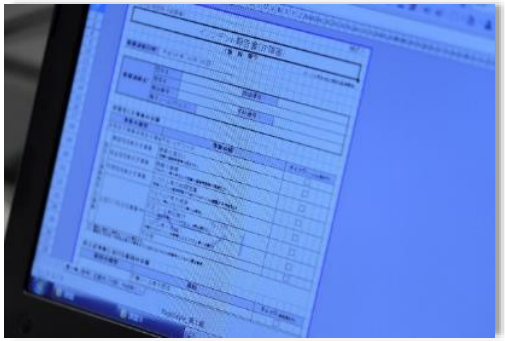
チューターによるサポート

マルウェア挙動調査

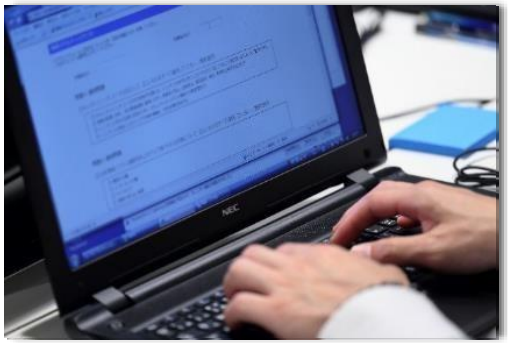
グループワーク

発表

報告書作成



確認テスト



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

課題出題イメージ

状況説明

現在2021/11/25 14:35です。

職員中川から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。

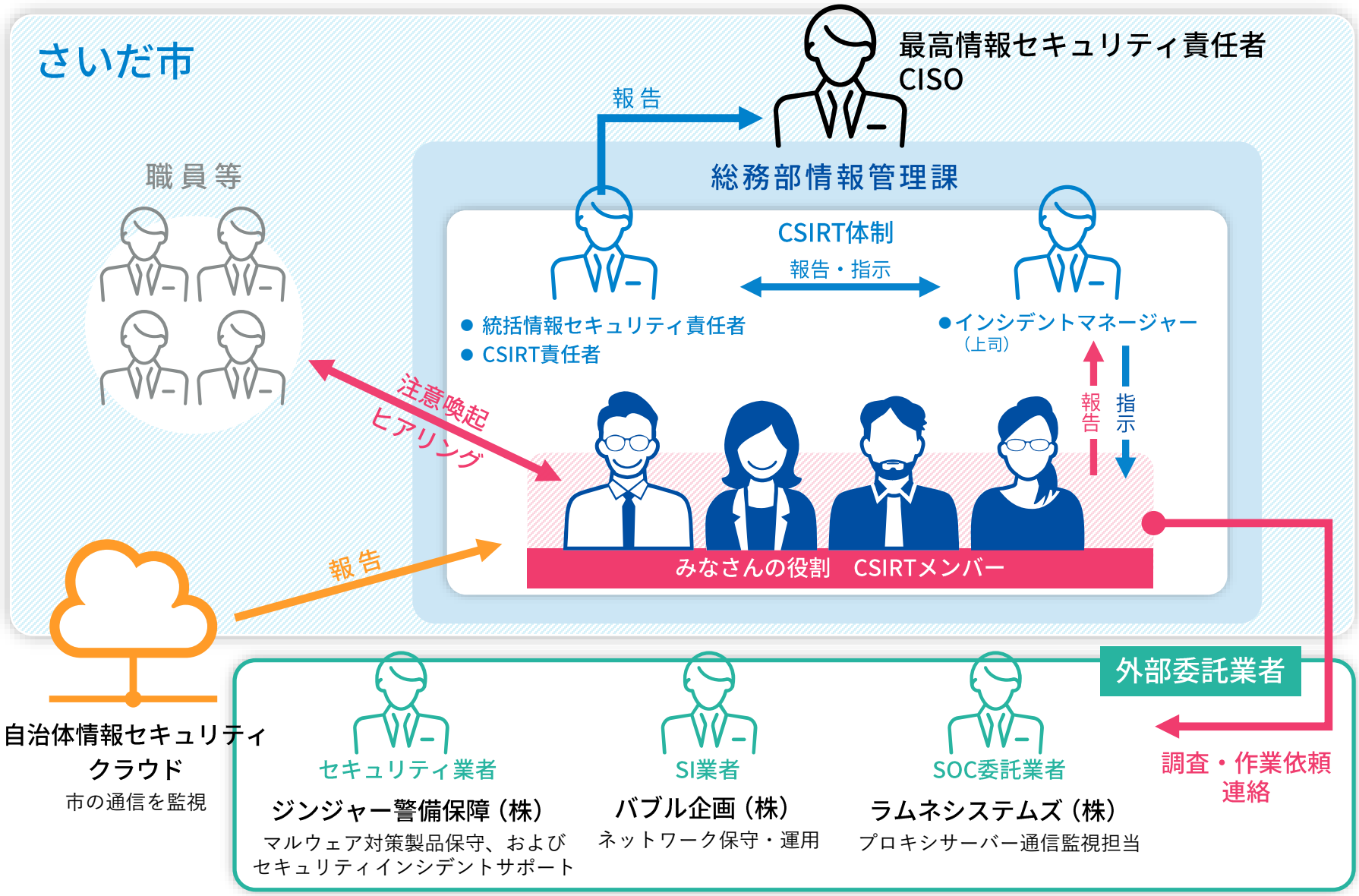
■連絡メール（抜粋）
今朝、私のメールボックスに情報通信研究機構の中村さんという方からのメールが届きました。しかし、私はこの方とは面識がない上に、本文の文面に不自然な日本語が多いなど、不審な点が見られるため、念のためお知らせしました。

課題

この通報に対して、どのような対応を取るべきかグループでディスカッションし、まとめてください。

参考

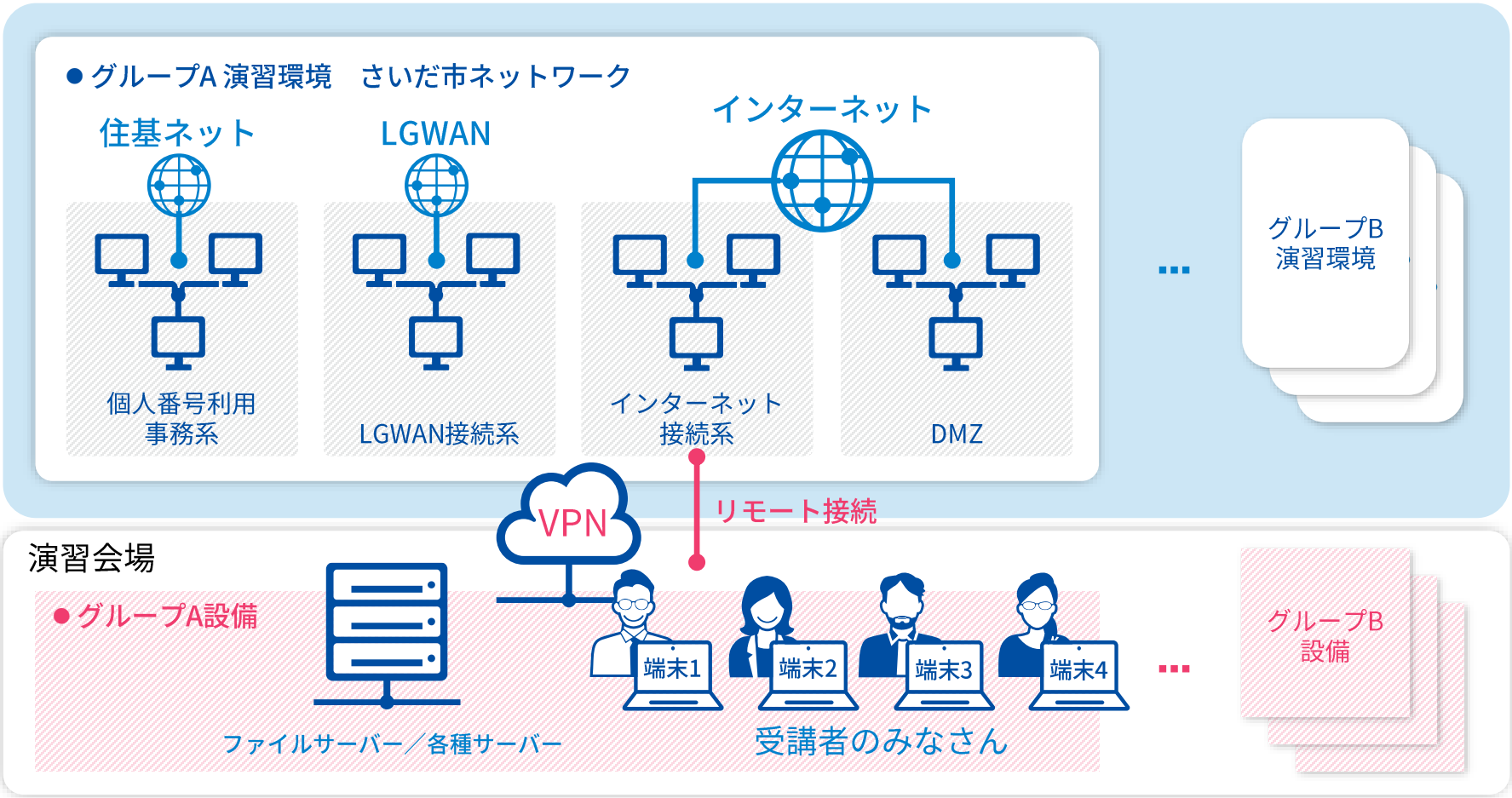
登場人物相関: B-1コースの例



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。




※左上のみ2019年度までの風景
集合演習のメリット

11/9プレスリリース: CYDER「オンラインAコース」

実践的サイバー防御演習CYDER「オンラインAコース」の提供を開始

2021年11月9日

国立研究開発法人情報通信研究機構

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田 英幸）は、実践的サイバー防御演習CYDER[*1]の「オンラインAコース」について、本日から提供を開始しました。本コースの提供により、時間的・地理的要因等で既存の演習への参加が困難であった方も、Webブラウザを搭載したパソコンとインターネット接続環境を用いることで、サイバーインシデント対応をご自宅や職場から体験することが可能となります。CYDER「オンラインAコース」についての詳細等は、CYDER公式Webサイトにてご確認ください。

*1 CYDER（サイダー）: CYber Defense Exercise with Recurrence

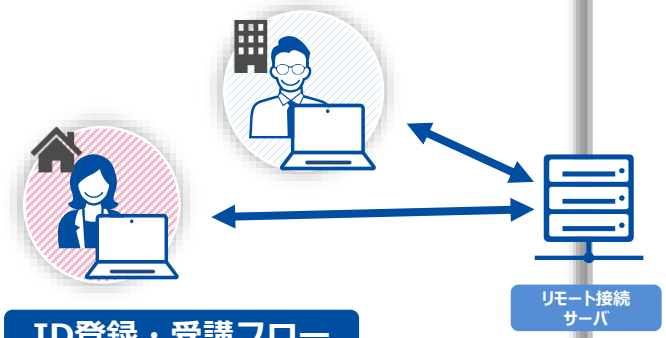
1 CYDER オンラインAコース提供の目的

実践的サイバー防御演習CYDER「オンラインAコース」の提供を開始｜2021年｜NICT-情報通信研究機構 https://www.nict.go.jp/press/2021/11/09-1.html

CYDERオンライン演習

- 職場や自宅のパソコンのWebブラウザから演習環境に接続し、オンライン演習を受講
- 地理的・時間的要因等によりCYDER集合演習が受講できない方への対応として、CYDERオンラインコースを新設（正式サービスを11月から開始予定）
- クローズドβテストを受けて改修を行い、オープンβは個人課題のみで構成

受講イメージ



スライド資料を用いた学習

クイズフォーマットの課題

録画解説ビデオで演習をサポート

仮想演習端末にアクセスして
集合演習同様に実機演習も実施

ID登録・受講フロー

ステップ1	新規アカウント作成（ID登録）
ステップ2	コース申込
ステップ3	演習日の予約
ステップ4	事前学習受講
ステップ5	オンライン演習受講

CYDERオンライン令和2～3年度の実施計画

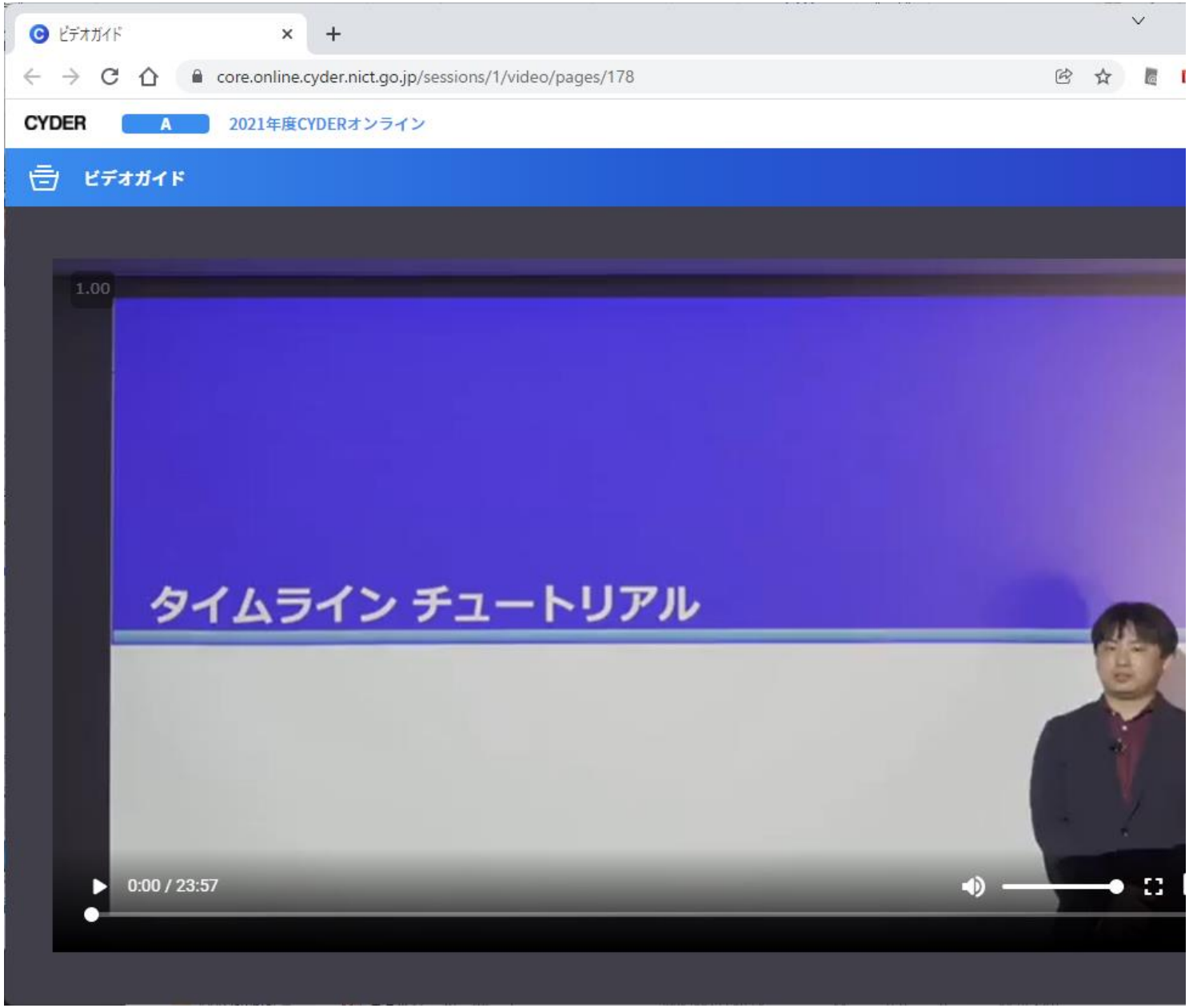
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	…
クローズドβテスト			改修		オープンβテスト			改修・準備		正式版		

主に地方公共団体の既受講者
300人を対象

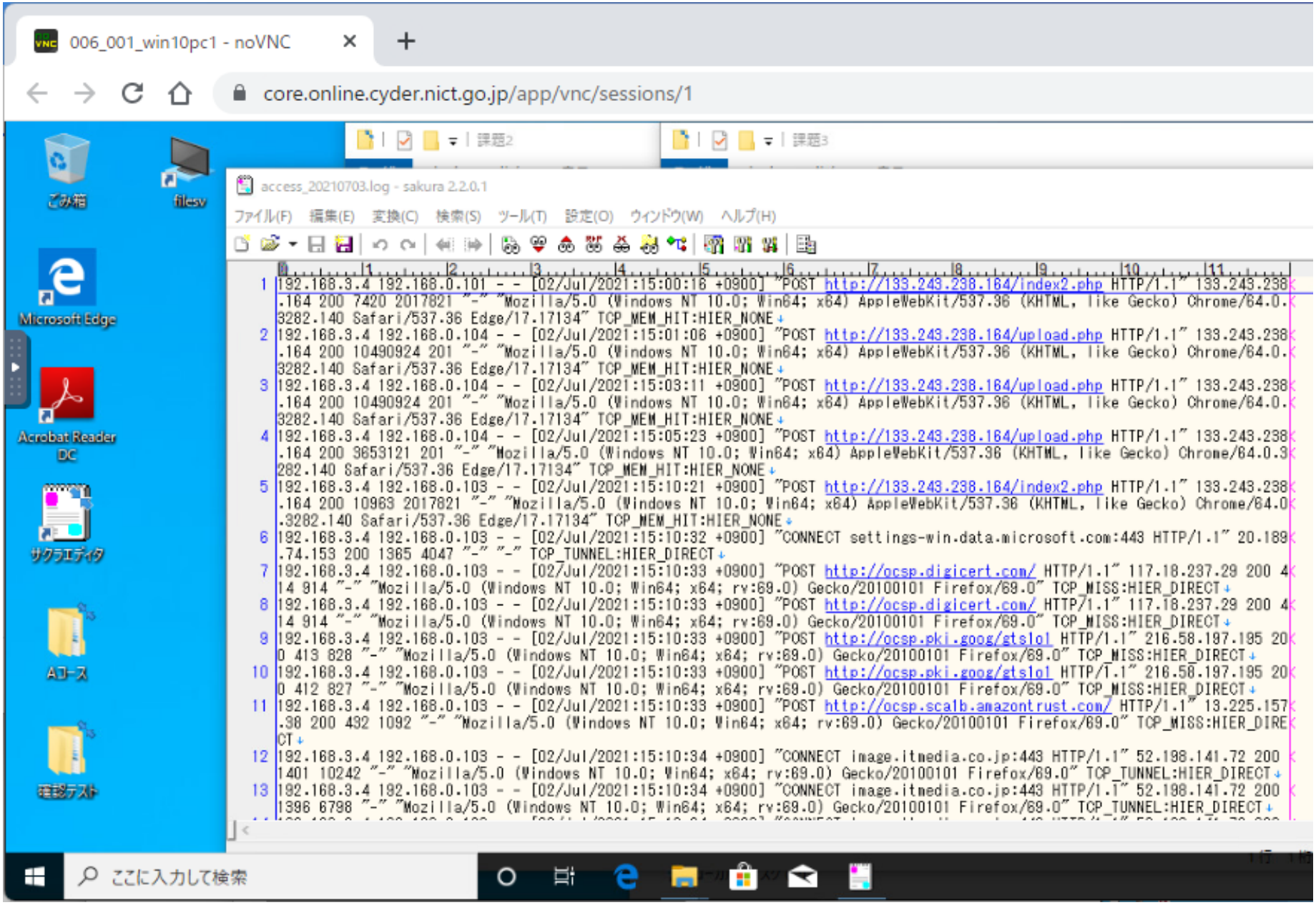
β版受講者を公開募集
300人を対象

スライド資料(講義資料)の閲覧はブラウザで

録画解説ビデオの視聴もブラウザで



実機演習もブラウザで


006_001_win10pc1 - noVNC
core.online.cyder.nict.go.jp/app/vnc/sessions/1
ごみ箱
filesv
Microsoft Edge
Acrobat Reader DC
サクラエディタ
Aコース
確認テスト
access_20210703.log - sakura 2.2.0.1
ファイル(F) 編集(E) 変換(C) 検索(S) ツール(T) 設定(O) ウィンドウ(W) ヘルプ(H)
1 192.168.3.4 192.168.0.101 - - [02/Jul/2021:15:00:16 +0900] "POST http://133.243.238.164/index2.php HTTP/1.1" 133.243.238.164 200 7420 2017821 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134" TCP_MEM_HIT:HIER_NONE
2 192.168.3.4 192.168.0.104 - - [02/Jul/2021:15:01:06 +0900] "POST http://133.243.238.164/upload.php HTTP/1.1" 133.243.238.164 200 10490924 201 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134" TCP_MEM_HIT:HIER_NONE
3 192.168.3.4 192.168.0.104 - - [02/Jul/2021:15:03:11 +0900] "POST http://133.243.238.164/upload.php HTTP/1.1" 133.243.238.164 200 10490924 201 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134" TCP_MEM_HIT:HIER_NONE
4 192.168.3.4 192.168.0.104 - - [02/Jul/2021:15:05:23 +0900] "POST http://133.243.238.164/upload.php HTTP/1.1" 133.243.238.164 200 3853121 201 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134" TCP_MEM_HIT:HIER_NONE
5 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:21 +0900] "POST http://133.243.238.164/index2.php HTTP/1.1" 133.243.238.164 200 10963 2017821 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134" TCP_MEM_HIT:HIER_NONE
6 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:32 +0900] "CONNECT settings-win.data.microsoft.com:443 HTTP/1.1" 20.189.74.153 200 1365 4047 "-" "-" TCP_TUNNEL:HIER_DIRECT
7 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:33 +0900] "POST http://ocsp.digicert.com/ HTTP/1.1" 117.18.237.29 200 414 914 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_MISS:HIER_DIRECT
8 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:33 +0900] "POST http://ocsp.digicert.com/ HTTP/1.1" 117.18.237.29 200 414 914 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_MISS:HIER_DIRECT
9 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:33 +0900] "POST http://ocsp.pki.goog/gts1o1 HTTP/1.1" 216.58.197.195 200 413 828 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_MISS:HIER_DIRECT
10 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:33 +0900] "POST http://ocsp.pki.goog/gts1o1 HTTP/1.1" 216.58.197.195 200 412 827 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_MISS:HIER_DIRECT
11 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:33 +0900] "POST http://ocsp.scalb.amazontrust.com/ HTTP/1.1" 13.225.157.38 200 432 1092 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_MISS:HIER_DIRECT
12 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:34 +0900] "CONNECT image.itmedia.co.jp:443 HTTP/1.1" 52.198.141.72 200 1401 10242 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_TUNNEL:HIER_DIRECT
13 192.168.3.4 192.168.0.103 - - [02/Jul/2021:15:10:34 +0900] "CONNECT image.itmedia.co.jp:443 HTTP/1.1" 52.198.141.72 200 1396 6798 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" TCP_TUNNEL:HIER_DIRECT
ここに入力して検索

オンライン演習の良さ

どこでも参加

- 旅費無し移動時間無しで参加できる
- 時差はあるけど海外であっても同じように

油断した状態でも出席可能(笑)

主催側としては開催会場を借りなくても良い

- ただし、配信インフラやシステムに関わる費用はかかる

集合演習 や オンラインAコース 等の 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

参考

よくあるご相談#1

Q.

- 時間的・地理的要因により、都合がつかず受講できません。

A.

- オンラインAコースを今秋新設しました。
  - グループワークを行う集合演習の補助的な役割を担い、受講者のペースで取り組める個人学習用のオンラインAコースを提供開始しました。これまで「会場が遠い」「開催日に都合がつかない」等の地理的・時間的要因により受講が困難であった方のためのコースです。

参考

よくあるご相談#2

Q.

- 過去にCYDERの受講は済ませており、今後の受講は不要と考えています。

A.

- “繰り返し受講”をおすすめしています。
  - サイバー攻撃は年々複雑化・巧妙化しており、CYDERは現実に起きたサイバー攻撃の最新事例を踏まえ、コース別に異なるシナリオを準備しています。いざという時に、最新の手法で攻撃を受けた場合もすぐに動けることを目的として、消防訓練のように繰り返し受講していただくことを推奨しています。

参考

よくあるご相談#3

Q.

●サイバーセキュリティに関する知識に自信がなく、演習が不安です。

A.

●初級レベルのコースをご用意しています。

- Aコースは初学者を対象としており、サイバー攻撃等のセキュリティインシデント発生～解決までの一通りの対応を、１手順ずつステップ・バイ・ステップで学びます（下図参照）。サイバーセキュリティに関する基礎知識がご不安な方にも気軽に参加いただけるような、初歩的な対応力を高める内容となっております。

<一日の流れ>

参考

よくあるご相談#4

Q.

●中小規模の団体であり、セキュリティ対策ソフトを導入済なので心配していません。

A.

●中小規模の団体を狙った攻撃も増えています。

•近年では、中小規模の団体を踏み台にして国の行政機関や大手企業などに侵入し攻撃するケースも増えており、中小規模の団体もサイバー攻撃の標的となっています。

●セキュリティ対策ソフトだけでは不十分です。

•過去にセキュリティインシデントが発生したことがある組織が43.6%*1と、全体の約半数にのぼるほどサイバー攻撃が多発している昨今、攻撃手法の複雑化・巧妙化もあり、事前に完璧な備えをすることはもはや不可能です。未知のインシデントが発生しても、臨機応変に対応できるよう日頃から訓練を行うことが肝要です。

*1「2019年セキュリティ人材育成事業の方針検討のための基礎調査/ナショナルサイバートレーニングセンター調べ（512組織）」

ここまでを踏まえて 西田（さいだ）さんの業務状況 へのコメント例

2021/11/25 13:17現在

状況1

- CSIRTとしてセキュリティインシデントに対応するミッションがある。
- 年末へ向けた資料作成の締め切りに追われている。

状況2

- リモートワーク中の職員阿部からリモートワークに関連したトラブルが発生したという一通の連絡メールが届いた。
- 職員阿部も年末へ向けた資料作成の締め切りに追われている。

状況3

- 久しぶりに庁舎へ出勤した職員金濱からマルウェアに関連したセキュリティインシデントが発生したという一通の連絡メールが届いた。
- 職員金濱は何が起きているか分からず不安のようである。

状況4

- 職員加藤から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いた。
- 職員加藤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。

セッションのまとめ

はじめに
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のご紹介

トレンドとキーワードで確認する
最近のセキュリティニュースやインシデント事例

インシデントハンドリングとは

このセッション終了後すぐの
お申込みをオススメしています

- **集合演習**
  - **B-1コース@沖縄2/4**
- **オンラインAコース**
  - **受講申込受付中!!**

実践的サイバー防御演習CYDER

Webサイト https://cyder.nict.go.jp/

National Institute of Information and Communications Technology

[ご参考]

2021年度

実践的サイバー防御演習

「CYDER」ご紹介

CYDER

Cyber Defense Exercise with Recurrence

参考

実践的サイバー防御演習「CYDER」の概要

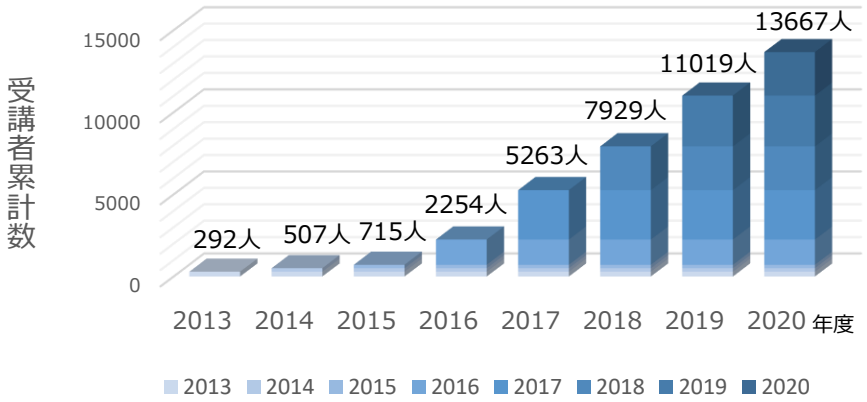
国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等が、組織のネットワーク環境を模擬した環境で、実践的な防御演習を行うことができるプログラムを提供することにより、数千人規模でセキュリティオペレーターを育成

2021年度コース概要

- 毎年 **約 3,000人が受講**
- 演習は1日間(Cコースのみ2日間)
- 集合 (実地) 演習のほか、**オンライン演習コースを新設**
- 組織当たり1名でも**複数名でも参加可能**
- 国の機関、独立行政法人、サイバーセキュリティ戦略本部が指定する指定法人、地方公共団体の職員の方（協力ベンダーを除く）の**受講料は無料**です

詳細は https://cyder.nict.go.jp/ をご覧ください

CYDER受講者数の推移 (累積数)



2021年度実施内容および対象組織

	コース	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
	A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	47都道府県	65回
	B-1		中級	システム管理者運用者 (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	21回
	B-2				地方公共団体以外	全国4都市	13回
New	C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	2回
New	オンラインA	オンライン演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	受講者職場等	-

※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

CYDERのトレーニング内容

- 演習舞台設定
  CYDERの演習舞台 (仮想組織のネットワーク) は、コース別に最適化された仮想環境を構築
- 攻撃・対処シナリオ
  CYDERは、現実に起きたサイバー攻撃の最新事例を踏まえ、コース別に異なるシナリオを準備。
  繰り返し受講することにより、様々な攻撃に対する対処法を学ぶことが可能

演習シナリオ例

Aコース (2020年度)
① 株式会社サイダーの従業員が、取引業者から納品されたUSBメモリを自分の端末に挿入して、マルウェアに感染
② その従業員の端末から社内の他の端末へ感染が拡大

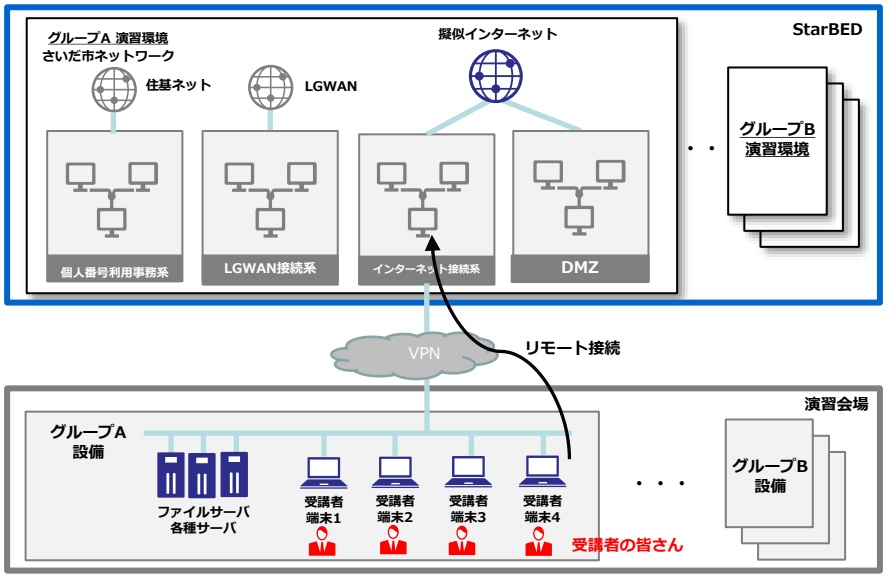
B-1コース (2020年度)
① さいだ市の職員が、改ざんされたアプリケーションを自分の端末にダウンロードして、マルウェアに感染
② その職員の端末から、庁内システム内にマルウェアが感染拡大、感染した管理者端末がメールサーバから外部にフィッシングメールを送信

B-2コース (2020年度)
① 標的型攻撃メールを受信したさいだ省職員が、添付されていたWordファイルを開封して、端末がマルウェアに感染
② その職員の端末を起点とし、省内システム内にマルウェアが感染拡大

Cコース (2021年度新設・予定)
① 外部公開サーバ経由での侵害を発端とする1つの大規模インシデントを、２日間を通して解き明かす

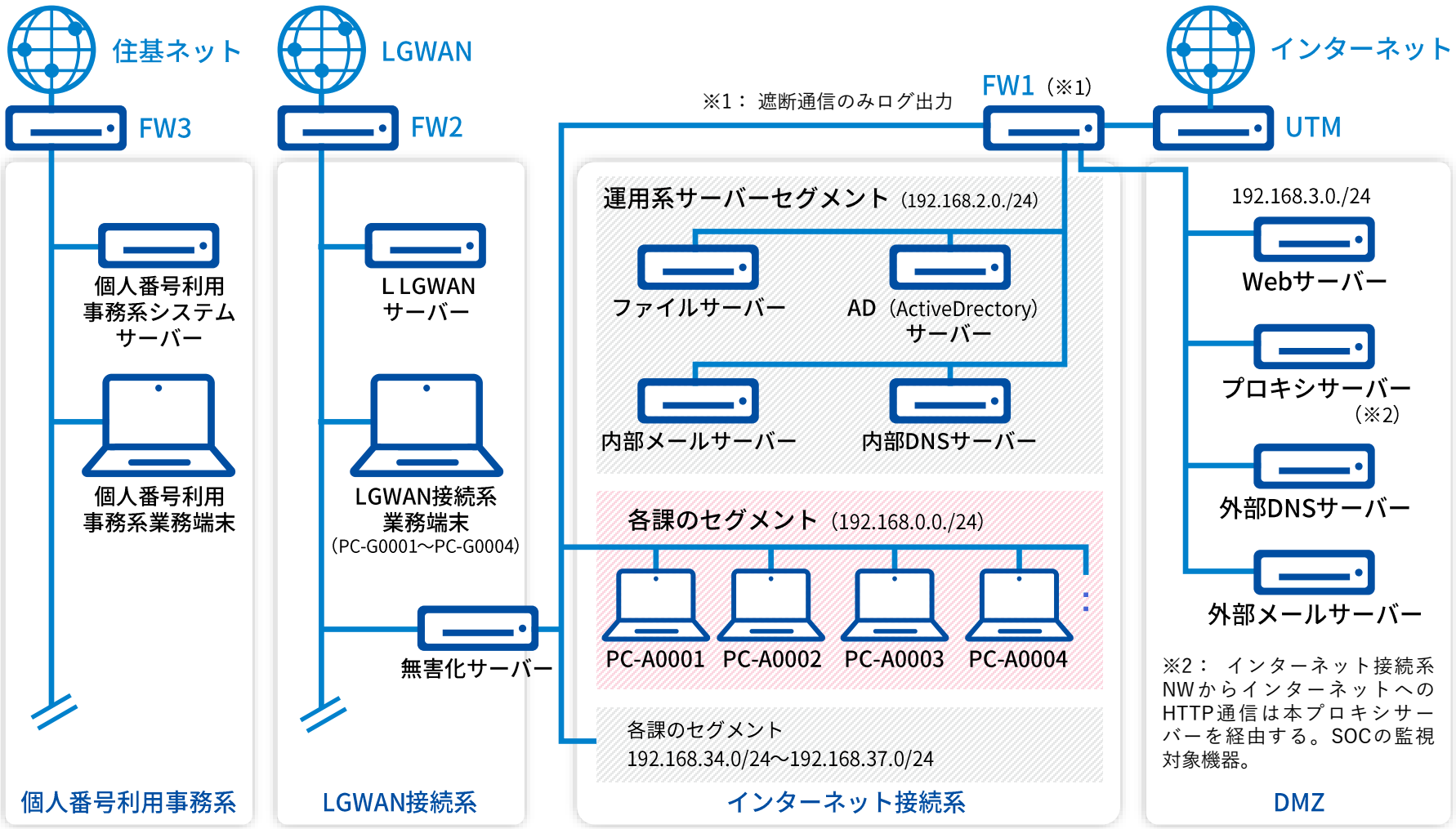
演習舞台設定例 (B-1コース)

各グループそれぞれに提供するネットワーク構成



参考

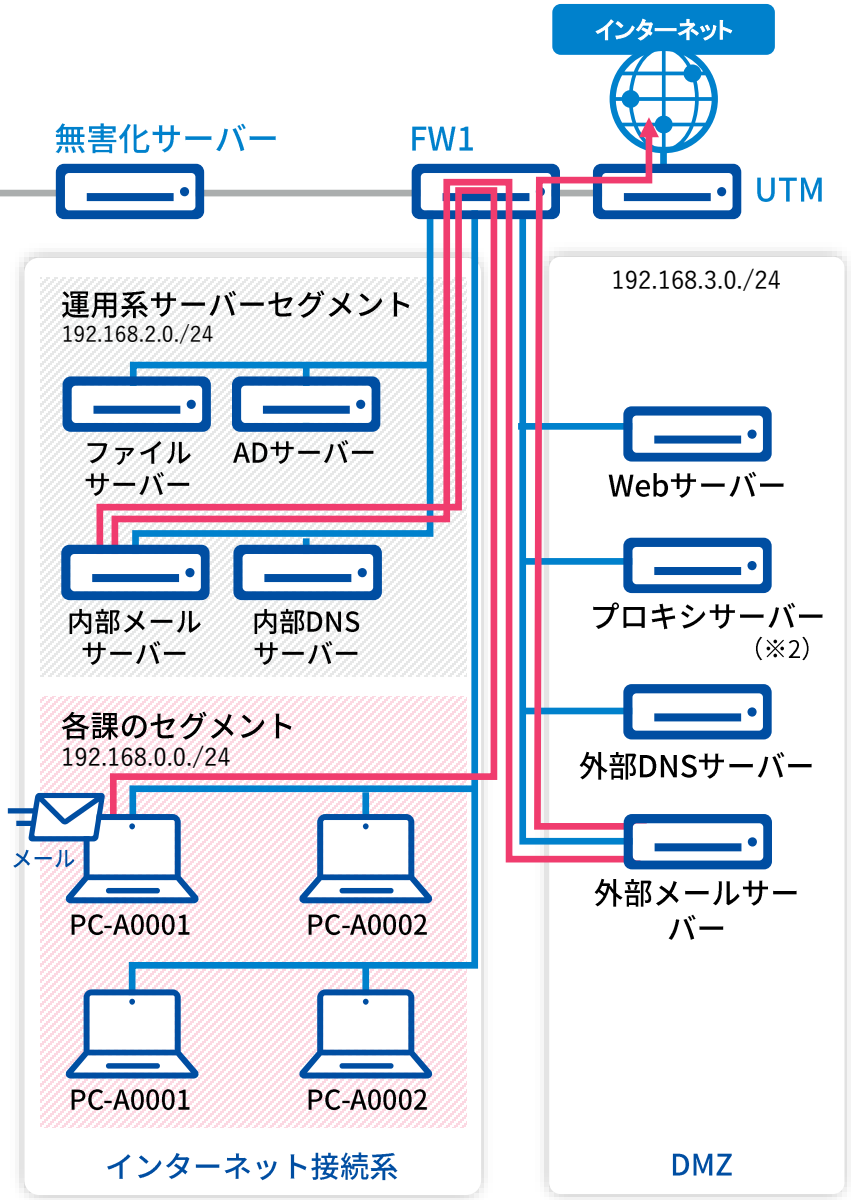
演習環境: B-1コースの例



参考

リアリティのある演習環境をご提供

外部 / 内部 メールサーバー	ネットワークを通じた電子メールの送受信を管理するサーバー。 ※さいだ市では、外部メールサーバーを経由して送受信します。組織内のメールは内部サーバーで送受信します。
外部 / 内部DNS サーバー	ネットワーク上におけるドメイン名とIPアドレスの対応関係を管理するためのサーバー。 ※さいだ市では、端末から名前解決する際、内部DNSサーバーに問い合わせます。
プロキシサーバー	クライアント端末の代わりにWebサーバーなどに代理でアクセスするサーバー。取得したWebコンテンツをキャッシュすることによってアクセスを高速化する。 ※さいだ市では、インターネット接続系NWからインターネットへのHTTP通信は本プロキシサーバーを経由します。
ADサーバー	「ActiveDirectory」の略。同一のドメイン内にある端末や機器を一括管理するWindowsサーバー。さいだ市内のユーザーやリソース、セキュリティポリシーなどを一括管理している。
無害化 サーバー	メールの本文やメールに添付されているファイルに含まれるマルウェアなどの不正なアプリケーションを無害化するサーバー。



参考

セキュリティ人材に必要とされる能力とNICTが行う実践的サイバー演習の対応関係

行政機関や民間企業の現場で働く情報システム担当者等は、日常業務が忙しく、訓練に長時間を割くことが難しい
NICTの実践的サイバー防御演習では、「ベンダーお任せ」では済まない、インシデント発生時の即応的な対処のために最低限必要なスキルを厳選して凝縮し、１日程度のコンパクトで効率的な実機演習を実施している

セキュリティ人材に必要とされる、スキルおよび知識の一覧 (※1)

総合的なセキュリティ人材は、インシデントマネジメント技術のみならず、セキュリティの基礎知識から、計算機やネットワーク等の専門性の高い分野や、事業運営、情報倫理、法制度までを含む、幅広いスキルと知識が必要となる

※1 「セキュリティ知識分野(SecBoK)人材スキルマップ2017年版 (JNSA)」を基に作成

：演習で集中的に得られる技術分野

：演習で部分的に触れる技術分野 (インシデント発生時の即応的な対処能力の習得に焦点を絞れば、必ずしも、演習で集中的に取り組む必要まではない技術分野)

技術領域	具体的な技術分野の例
ICT 基礎	ハードウェア、OS、ネットワーク、システム開発
工学基礎	プロセス工学、フォールトトレランス、数学
セキュリティガバナンス	情報セキュリティアーキテクチャシステム
セキュアシステム設計・構築	システムライフサイクルマネジメント、構成管理
暗号・認証・電子署名	暗号化アルゴリズム、認証手法、一方向性ハッシュ
セキュリティ運用	**セキュリティ運用と事業の衝突回避**
	インシデント対応
	セキュリティ技術に関する知識
セキュリティ基礎	CIA、セキュリティ問題・リスクおよび脆弱性
サイバー攻撃手法	脅威、攻撃手法、脆弱性、マルウェア、ハッキング
デジタルフォレンジックス	データの保全・解析・保管、ライブデータの解析
セキュリティマネジメント	教育、啓発、ポリシー、セキュリティ対策
システムセキュリティ	システムの脅威と脆弱性、バイナリ解析
ネットワークセキュリティ	トラフィック解析、侵入検知、アクセス制御
	フィルタリング、ペネトレーション、脆弱性診断
ビジネス基礎	コミュニケーション能力、組織評価、アセスメント
法・制度・標準	国内外関連法・標準、コンプライアンス、ポリシー

- セキュリティ運用と事業の衝突回避
  - 運用上のセキュリティに関する知識
  - 新興の情報技術と情報セキュリティ技術に関する知識
  - システム診断ツールと障害識別技法に関する知識
  - 自組織内部の構造とプロセスについて報告するコンピュータネットワーク防御 (CND) サービスの提供者に関する知識
  - 主要ベンダの製品と用語及びエクスプロイト／脆弱性にどのように作用するかの相違点に関する知識
  - セキュリティ運用と事業の衝突回避に関するスキル
  - リスク脅威の評価に関する知識
- インシデント対応
  - インシデントのカテゴリ、インシデントレスポンス及び応答のタイムラインに関する知識
  - インシデントレスポンスとハンドリングの方法論に関する知識
  - インシデントハンドリング手法の利用に関するスキル
  - インシデントの根本原因分析に関する知識
  - インシデントに関連したネットワークセキュリティの報告のためのプロセスに関する知識
  - 企業のインシデントレスポンスプログラム、役割及び責任に関する知識
  - インシデントの根本原因分析の実施に関するスキル
  - 報告されたインシデントの文書化と問い合わせに用いられるデータベース手続きに関する知識
- セキュリティ技術に関する知識
  - 内部不正の検出、報告、検出ツール及び法規制に関する知識と経験
  - セキュアな取得に関する知識
  - セキュリティイベント (事象) の相関ツールに関する知識

参考

NICTによるセキュリティオペレーターの育成

NICTの「強み」

長年のサイバーセキュリティ研究による技術的知見

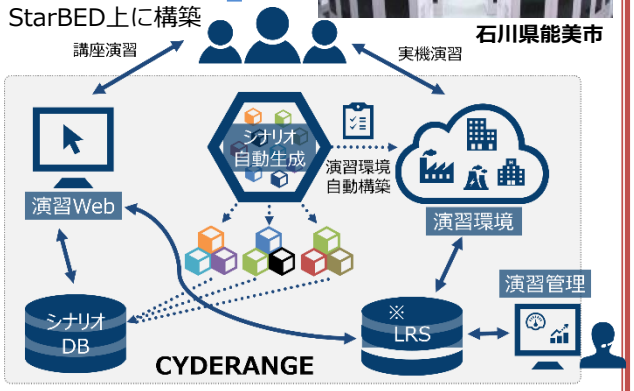
- NICTの長年にわたるサイバーセキュリティ研究で得られた技術的知見を活用し、 我が国固有のサイバー攻撃事例を徹底分析した最新の実機演習シナリオを作成
- インシデントハンドリングに最低限必要なスキルを厳選して凝縮し、コンパクトで効率的なカリキュラムを構成

大規模高性能サーバー群 NICT北陸StarBED技術センター

- **大規模性**
  大規模な組織のネットワーク環境を再現した仮想環境を構築するための大規模なサーバー群
- **運営ノウハウの蓄積**
  大規模仮想環境の効率的かつ安定的な運営に関する高度な知見・ノウハウが蓄積
- **セキュアな環境**
  インターネット等から隔離された強固な閉鎖環境

サイバー演習自動化システム CYDERANGE (サイダーレンジ)

- CYDERANGEはサイバー演習の運営に係るコストの削減と受講者のプロファイルに合わせた効果的な演習プログラムの提供を目指すサイバー演習自動化システムを2018年度から導入



※ Learning Record Store (履歴データベース)

活用

CYDER
Cyber Defense Exercise with Recurrence

サイバー攻撃への対処方法を体得

仮想空間で再現された大規模ネットワーク環境

RPCI
Response Practice for Cyber Incidents

公的機関初の情報処理安全確保支援士向け特定講習

実機演習のノウハウを活かした技術に寄った講習

参考

CYDERANGE（サイダーレンジ）：サイバー演習自動化システム

NICTナショナルサイバートレーニングセンターは、より効率的なサイバー演習を実現するサイバー演習自動化システム “CYDERANGE” を独自に開発。これまでのサイバー演習では、演習プログラムの作成ごとにシナリオや演習環境を手作業で作成することが一般的であったが、この CYDERANGE の開発により、演習シナリオの自動生成等が可能となった (2018年度から実運用を開始)

ポイント

- **世界初の機能**
  - 演習「シナリオ」の自動生成は、既存技術にはない、世界で初めての機能
- **運用性の向上とコストの削減**
  - 演習環境を自動構築することで、演習環境の運用性の向上や演習実施に係る費用の低減を実現
- **次世代の業界標準技術にいち早く対応**
  - フライトシミュレーター等でも用いられる次世代の演習データ記録方式の世界規格である Experience APIを用いたLRS (Learning Record Store) を構築
    → より詳細な受講者データの取得・分析を可能に
- **演習の効果を精密に測定**
  - 膨大な受講者データを機械学習等の技術によって分析することで、演習による学習効果を精密に測定することが可能

参考

サイバー空間における犯罪事例

ランサムウェア

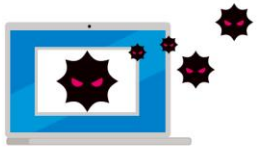
2018年、交通事業者の業務用ファイルサーバーがマルウェアに感染し、業務の一部に支障が生じていると発表された。当該サーバーに保存された全ファイルへのアクセスが不能になった。

【攻撃の手口】

ランサムウェアの攻撃方法は、マルウェアで感染させた後ファイルを暗号化することでデータアクセスを不能にさせる。このデータを身代金やビットコインと引き換えに復旧させるという金銭獲得が主な目的となっている。

Web改ざん

2013年、市立総合病院のWebサイトが不正アクセスを受け、改ざんされていたことが確認された。改ざんされたWebサイトを閲覧した場合、マルウェアに感染する可能性があった。



【攻撃の手口】

Webページを改ざんしたり、不正プログラムを組み込むことでユーザー情報の搾取または悪質なウイルスのばら撒きなどを目的としたもの。

標的型メール攻撃

2018年、国家政策の指針となる基本計画の策定メンバーである、複数の大学の教授数人に対し、政府職員になりすました偽装メールが送信された（本事例での情報流出は起きていない）。

【攻撃の手口】

偽装メールの添付ファイルを開くとマルウェアに感染し、情報を盗み取られる仕組みとなっていた。中国のハッカー集団が関与したとみられている。

DDoS攻撃

2016年、地方公共団体のWebサーバーが閲覧できない障害が発生した。また、同機関のWebサーバー以外にも複数のサイトで障害が発生した。Webサーバーが閲覧できなくなったことに伴い、利用者からの問い合わせの受け付けも一時不可となった。

【攻撃の手口】

複数のコンピューターから標的のサーバーに、ネットワークを介し大量の処理要求を送ることでサービスを停止させたもの。攻撃のあった同日に、ハッカー集団がTwitter上で、同機関のWebサーバーをサービス不能にしたとする投稿があった。

参考

インシデント対応時のマニュアル・チェックリスト(入門)

- **情報漏えい発生時の対応ポイント集　第3版（IPA）**
  - インシデント対応の内容が記載されています。絵が多く見やすく構成されています。
  - https://www.ipa.go.jp/security/awareness/johorouei/

- **中小企業向けサイバーセキュリティ対策の極意ガイドブック（東京都）**
  - サイバー攻撃に関する情報や、攻撃に対する対応方法などがマンガ形式として描かれています。サイバー攻撃への対処方法などを楽しく学ぶことができる内容です。
  - https://cybersecurity-tokyo.jp/security/guidebook/index.html

参考

インシデント対応時のマニュアル・チェックリスト(中級)

- **インシデントハンドリングマニュアル（JPCERT/CC）**
  - インシデントハンドリングの対応フローや各フェーズでの対応方法についての記載があり、インシデントハンドリングのマニュアルづくりに参考となる資料です。
  - https://www.jpcert.or.jp/csirt_material/operation_phase.html
- **サイバー攻撃（標的型攻撃）対策防御モデルの解説（総務省）**
  - インシデントハンドリングの対応情報が記載されています。さらに、チェックすべきログ情報や対処内容などがリスト化されている資料が、別冊として用意されています。
  - https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000125.html
- **情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）**
  - 中・小規模の組織向けのインシデント対応ガイドブックです。インシデントに対する準備やインシデントの対応フローなどが記載されています。
  - http://lab.iisec.ac.jp/~hiromatsu_lab/sub07.html
- **組織対応力ベンチマークシート（一般社団法人オープンガバメント・コンソーシアム）**
  - 事前準備やインシデント対応に関する内容がチェックシート形式で記載されています。
  - https://ogc.or.jp/article/1525
- **セキュリティ対応組織の教科書　v2.1（日本セキュリティオペレーション事業者協議会）**
  - インシデントに対する準備やインシデントの対応フローなどが記載されています。人材育成を観点とした内容も含まれています。
  - https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
- **証拠保全ガイドライン　第8版（デジタル・フォレンジック研究会）**
  - インシデントに関わる証拠保全の内容が記載されています。証拠保全で使用されるツールの一覧なども記載されています。
  - https://digitalforensic.jp/home/act/products/home-act-products-df-guideline-8th/
- **Incident Handler's Handbook（SANS）**
  - インシデントハンドラーのハンドブックです。フェーズごとの対応内容についてのチェックリストが記載されています。WindowsとUNIXのコマンドに関する内容も資料に含まれています。
  - 英語の資料です。
  - https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

参考

インシデント対応時のマニュアル・チェックリスト(上級)

- **コンピュータセキュリティインシデント対応ガイド**
  米国立標準技術研究所による勧告（IPA）
  - インシデントハンドリングに関するガイドラインです。
    技術的な部分も含めて、非常に詳細な情報が記載されています。
    NIST（800-61）の資料の翻訳版です。
  - https://www.ipa.go.jp/security/publications/nist/

- **インシデント対応へのフォレンジック技法の統合に関するガイド**
  米国国立標準技術研究所による勧告（IPA）
  - インシデントに関わるデジタルフォレンジックの内容が記載されています。技術的な内容が多く含まれています。
    NIST（800-86）の資料の翻訳版です。
  - https://www.ipa.go.jp/security/publications/nist/

参考

テレワーク環境のリスクと対策

テレワーク固有のリスクを理解した適切な対応

新型コロナ対応で、十分な準備もできないままリモートワークを実施する組織も多いようです。テレワーク固有のリスクを理解して適切な対応を行う必要があります。

テレワークに関連する事故例

- 大学のリモート授業時に配信したメッセージに、学生の個人情報を誤って添付
- 高校教諭がテレワークのために生徒の個人情報を保存したUSBメモリを紛失
- IT企業が、トラフィック増大等によって障害が多発したため リモートアクセスサービスを終了
- 通信事業者が、リモートアクセスを利用したBYOD端末を経由して VDIサーバーへ不正アクセスを受け、内部情報が流出

テレワークのリスク

- 宅内端末からの情報流出
- 宅内端末を踏み台にした社内への不正侵入
- 宅内端末へのポリシー適用不全による脆弱性の残留
- 宅内端末の通信監視不全による脅威検知の遅延
- 宅内端末への障害対応やインシデント対応の遅延（遠隔対応、端末の回収、代替機送付等）

テレワークのセキュリティ対策例

- 多要素認証によるVPNアクセス認証の厳格化
- VPNアクセスの監視の強化
- 端末へのエンドポイントセキュリティ(EDR等)の実装による、ネットワークアクセス制限の厳格化、インストール制限、セキュリティパッチ管理の強化、操作監視、インシデント発生時の遠隔分析と隔離
- テレワーク環境の管理と利用の規定の整備

*1：BYOD（Bring Your Own Device）
私有デバイスの業務利用

*2：VDI（Virtual Desktop Infrastructure）
仮想的なデスクトップ環境