Hitachi Solutions Create

HITACHI

サイバーセキュリティトレーニング サービスの紹介

株式会社 日立ソリューションズ・クリエイト
セキュリティビジネス本部
セキュリティサービス部

HITACHI

目次

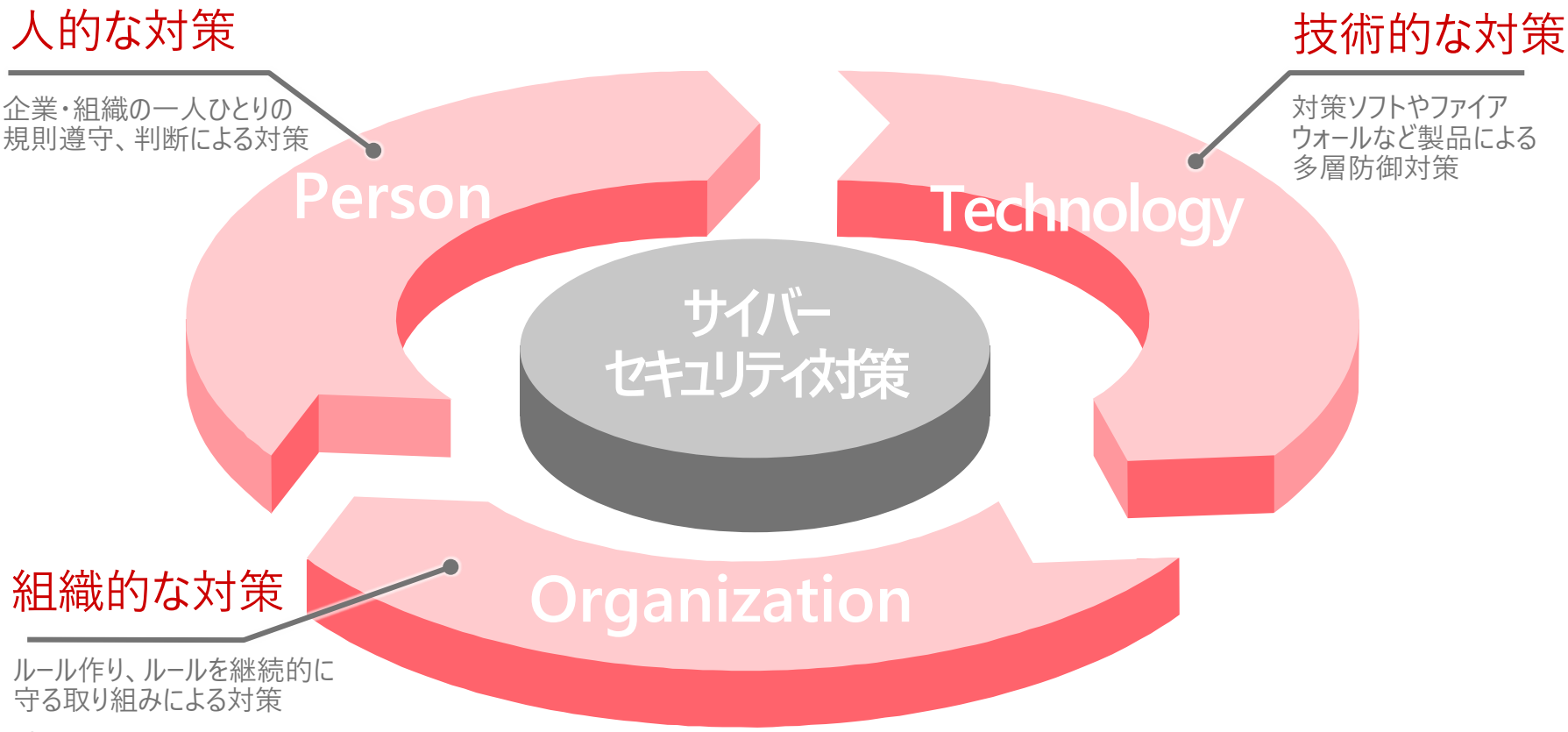
１．サイバーセキュリティ対策

HITACHI

サイバー攻撃から守るには

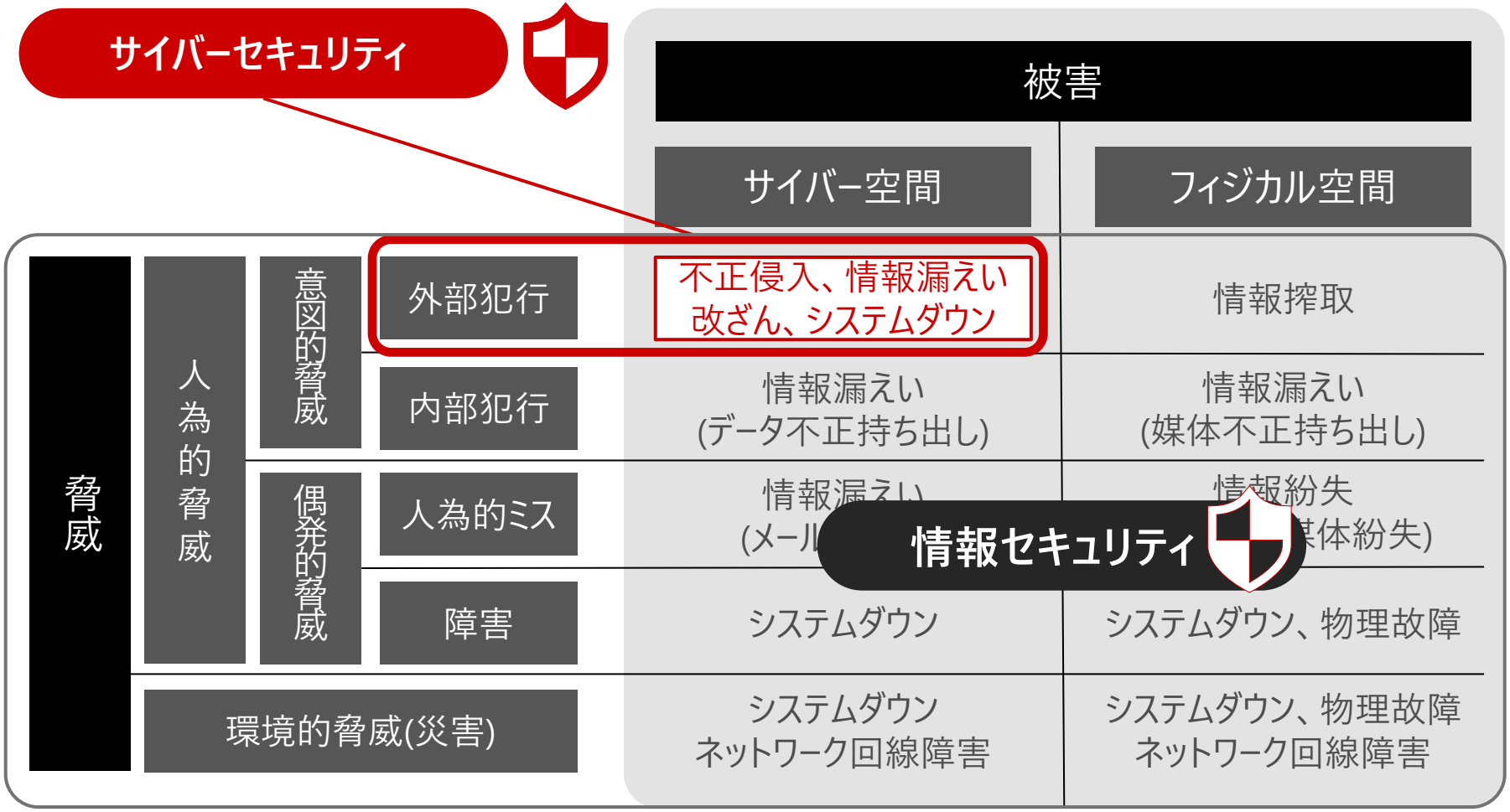
標的型攻撃をはじめとしてサイバー攻撃の高度化・巧妙化が進展し、既存の情報セキュリティ対策ではネットワークへの侵入、マルウェアの感染などの脅威を完全に防ぐことが困難となってきています。

サイバーセキュリティ対策は、**技術・組織・人**の全ての対策が重要です。

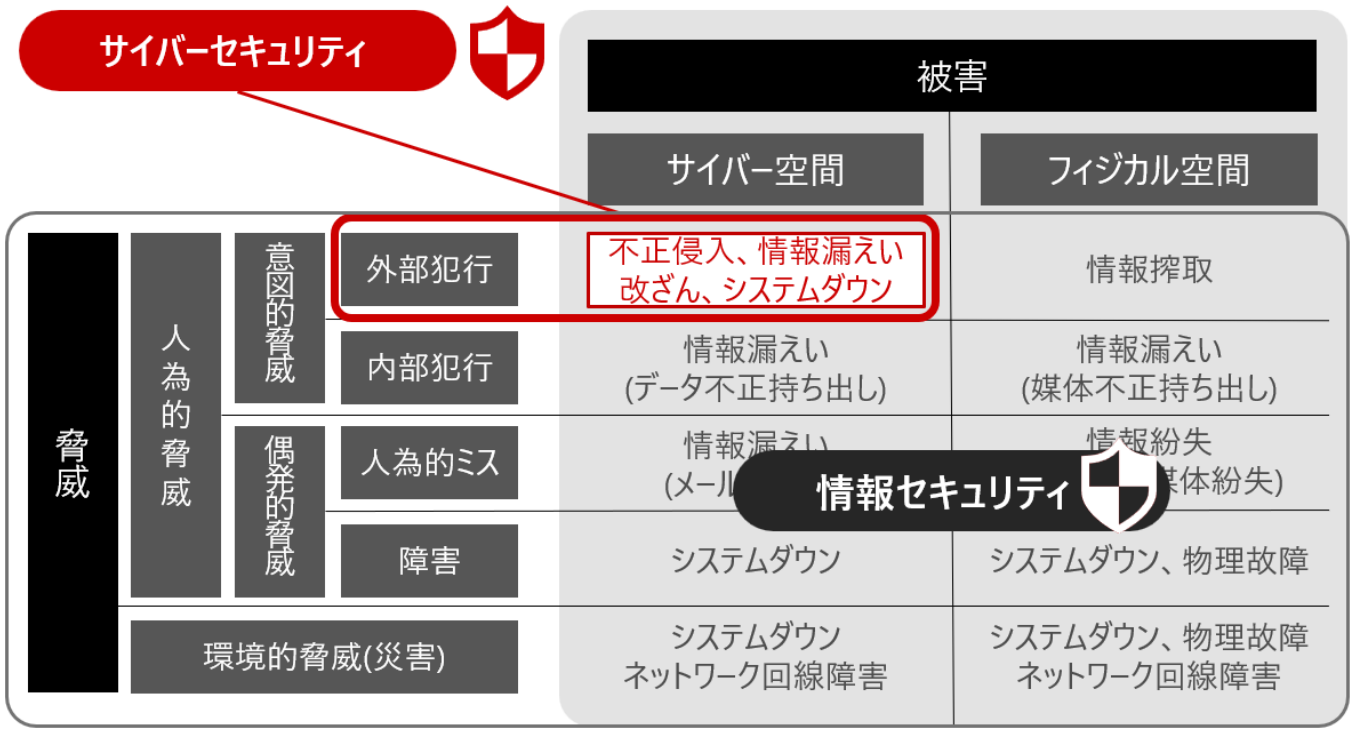


HITACHI

サイバーセキュリティとは**サイバー空間における外部脅威から**
企業・組織の**重要な情報とシステムを守ること**



HITACHI



想定できない脅威

想定できる脅威
パターン化した
対応方法が有効
(マニュアルに従った
対応)

サイバー攻撃は高度化・巧妙化し、想定したパターン化の対応では
防ぎきれません。
このため、最先端のサイバーセキュリティ技術に加え、**攻撃の変化に瞬時に対応できる人材(能動的な人材)**と、**組織としての対応**が求められます。

1-4　サイバーセキュリティ体制と人材

HITACHI

経済産業省では、企業内の経営層から人事担当者、実務者に至るさまざまな立場の人が、
体制構築・人材確保において考慮すべき要点をまとめた手引き(第2版)を2022年6月に公開しました。
この中で、**組織としてのセキュリティ体制の構築とセキュリティ人材の育成が重要である**
ということが書かれています。

「サイバーセキュリティ体制構築・人材確保の手引き」における検討のポイント

指示２ **サイバーセキュリティリスク管理体制の構築**	**2.1** **サイバーセキュリティに関して「やるべきこと」の明確化**	①自社で対処すべきサイバーセキュリティリスクを認識し、そのリスクを低減するために具体的に「やるべきこと（タスク）」を明確化していく。 ②ITSS+（セキュリティ領域、次ページ参照）なども参考にしながら、負荷が大きい部分はスモールスタートから始め、継続的に改善する。
	2.2 **セキュリティ統括機能の検討**	① 組織内でサイバーセキュリティ機能をうまく働かせるには、CISO等の経営層を補佐する「セキュリティ統括機能」（次ページ参照）を設置すべき。 ② セキュリティ統括機能には大きく4つの類型があり、自社の状況に合わせて検討する。
	2.3 **セキュリティ関連タスクを担う部門・関係会社の特定・責任明確化**	① サイバーセキュリティ体制の具体的な構築にあたっては、ITSS＋（セキュリティ領域）を参考にすることで、関係部署や委託先の役割が明確になる。 ② 実際のところほとんどの企業においてサイバーセキュリティに関する機能の一部を外部委託することが適切であるが、丸投げではない適切な役割分担と、品質の担保されたサービスの選定が重要である。
指示３ **サイバーセキュリティ対策のための資源確保**	**3.1** **セキュリティを主たる業務とする人材の確保**	① 外部委託を積極活用していても、サイバーセキュリティリスクの把握と対策を推進する自社要員を割り当てる必要があり、当該人材には役割に応じた知識・スキルが求められる。 ② サイバーセキュリティに関する専門性を有する人材は不足状態にあり、確保には工夫が求められる。
	3.2 **「プラス・セキュリティ」の取組推進**	① 事業部門、管理部門等においてそれぞれの業務に従事する人材が、DX等のデジタル活用を進めるなかでセキュリティを意識し、業務遂行に伴う適切なセキュリティ対策の実施やセキュリティ人材との円滑なコミュニケーションに必要な能力を育成する「プラス・セキュリティ」の取組が欠かせない。 ②「プラス・セキュリティ」を担う人材に自らの役割と責任の自覚を促すための意識付けを行う。
	3.3 **教育プログラム・試験・資格等の活用と人材育成計画の検討**	① 各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格の活用を検討する。 ② 自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を検討する。

出典：経済産業省「付録F(概要版) サイバーセキュリティ体制構築・人材確保の手引き 第2.0版」
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

1-5　サイバー攻撃の脅威（1/2）

HITACHI

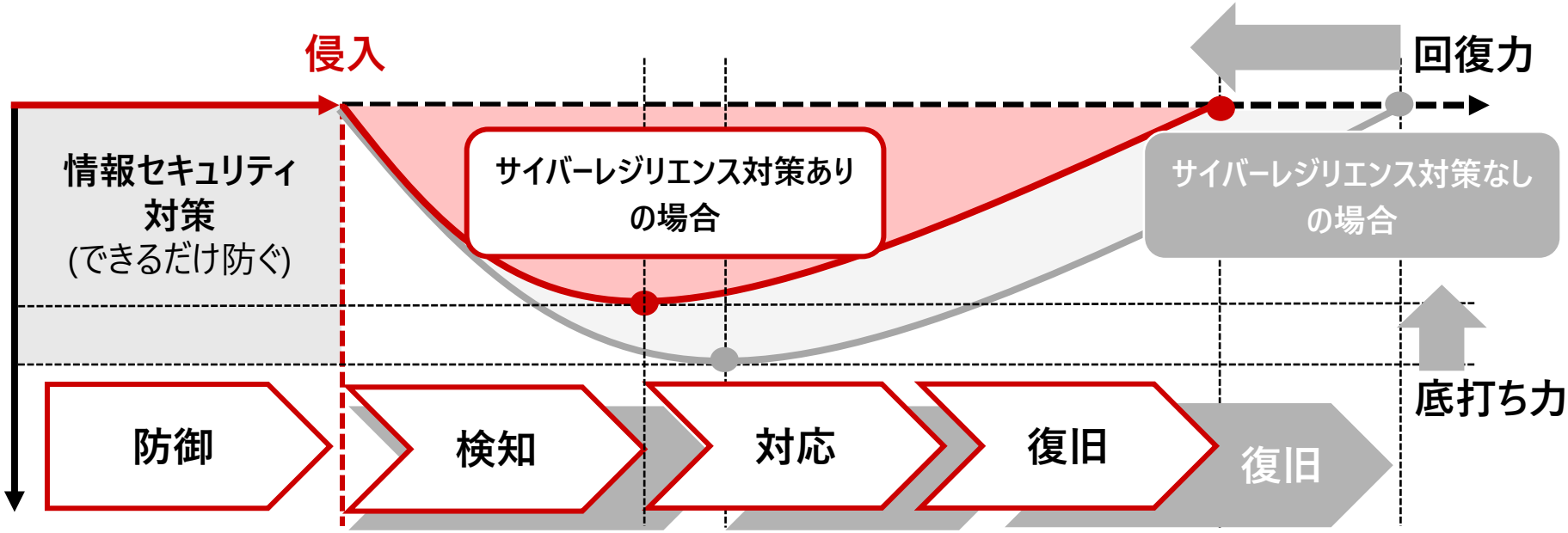
HITACHI

システム脅威とその対応

目的 / 脅威	組織的対応	人的対応	その他
IT障害	• IT障害発生時の社内外の情報連絡	• サイト内のコールド/ホットスタート	• IT障害発生時のBCP発動
自然災害	• 自然災害時のシステム担当者を含む社内の情報連絡	• サイト間のコールド/ホットスタート • 通信障害発生時の原因究明	• 大規模震災発生時のBCP発動
サイバー攻撃	• **サイバー攻撃発生時の社内外の情報連絡**	• **インシデント解析** • **ログ解析** • **サイト内、サイト間の手動切替**	• **サイバー攻撃発生時のマスコミ発表内容**

1-6　サイバーレジリエンス対策(侵入前提で備える)

HITACHI



NISC 2019　重要インフラの情報セキュリティ対策に係る第4次行動計画によると、
「サイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、**IT障害の発生を可能な限り減らす**とともに、
IT障害発生時の迅速な復旧を図ることで重要インフラを防護する」とあります。

IT障害の発生を可能な限り減らす
→情報セキュリティ対策

IT障害時の迅速な復旧を図る
→侵入前提で備えるサイバーレジリエンス対策

参考：NISC 2019　重要インフラの情報セキュリティ対策に係る第 4 次行動計画
https://www.cyber.go.jp/pdf/policy/infra/infra_rt4_r2.pdf

HITACHI

近年は、侵入前提で備える**サイバーレジリエンス対策の強化**が
求められており、攻撃を受けた際のレジリエンスが重要

まずやるべきことは、組織のサイバーレジリエンスの
現状を客観的に評価し、課題を特定すること

サイバー演習が効果的

1-8　サイバー演習

HITACHI

「サイバー演習」とは、サイバー攻撃に対する『**組織全体の防災訓練**』です。

サイバー演習の目的は、**組織の対応力を検証すること**です。
想定される事案シナリオを作成し、判断・行動の対応を演練し、
組織として欠落している事項を確認することです。

HITACHI

サイバー攻撃は「人」を狙う

- 近年、標的型攻撃といった**企業・組織の社員・職員を狙うサイバー攻撃が増加**
- サイバー攻撃による情報漏えいの大半が**人的要因**

従来の「技術対策」だけでの**100％防御は難しい。**
人的対策として、
「規則遵守(教育)」と「判断による対策(訓練)」が必要

HITACHI

サイバー攻撃に対応するセキュリティ人材に必要な能力

- 最新の攻撃実態の知識、攻撃者の行動を読み取る**「発想力」**
- インシデントが組織に与える影響を想像できる**「想像力」**
- 習得した知識やスキルを使いこなす**「応用力」**
- 社内外のさまざまな人と連携しながら行動を促す**「コミュニケーション力」**
- 自社のビジネスの視点から俯瞰的にインシデント対応の判断ができる**「判断力」**

このような能力を初めから持っている人材は少ないです。
また、最新のサイバー攻撃に対応するためには、継続的な研鑽が必要です。

個人での学習や演習が必要不可欠

HITACHI

- 高度化・巧妙化するサイバー攻撃に対応するためには、**技術・組織・人全て**の対策が重要

①技術的な対策：**製品の導入**

②組織的な対策：**サイバー演習**

③人的な対策：**教育と訓練**

２．サイバーセキュリティトレーニングの紹介

HITACHI

日々高度化するサイバー攻撃に
能動的に対応できる人材が
不足している

サイバーセキュリティ
人材育成が進まない

組織内にCSIRT・PSIRT(※)はあるが、
技術者の育成が進んでいない

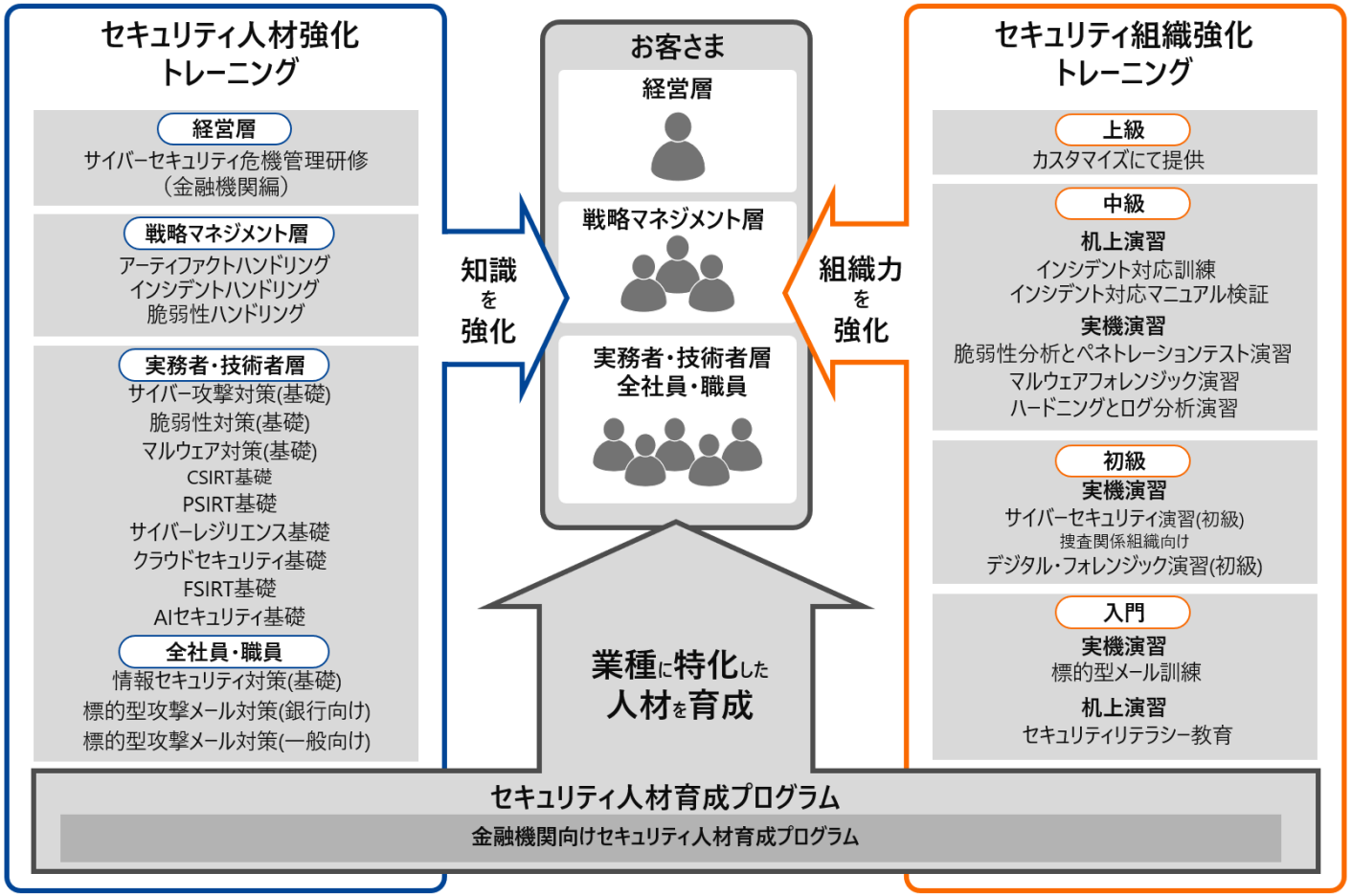
インシデントが発生した際の
対応能力を
組織として習得・強化したい

(※)CSIRT: Computer Security Incident Response Teamの略で、主に組織内のセキュリティを守る
PSIRT: Product Security Incident Response Teamの略で、主に自社製品・サービスのセキュリティを守る

このような課題
「**サイバーセキュリティトレーニング**」が解決します

2-1　サイバーセキュリティトレーニング（2/2）

HITACHI



サイバーセキュリティトレーニングを受講することで、
インシデント対応能力を**個人と組織の両面から強化可能！**

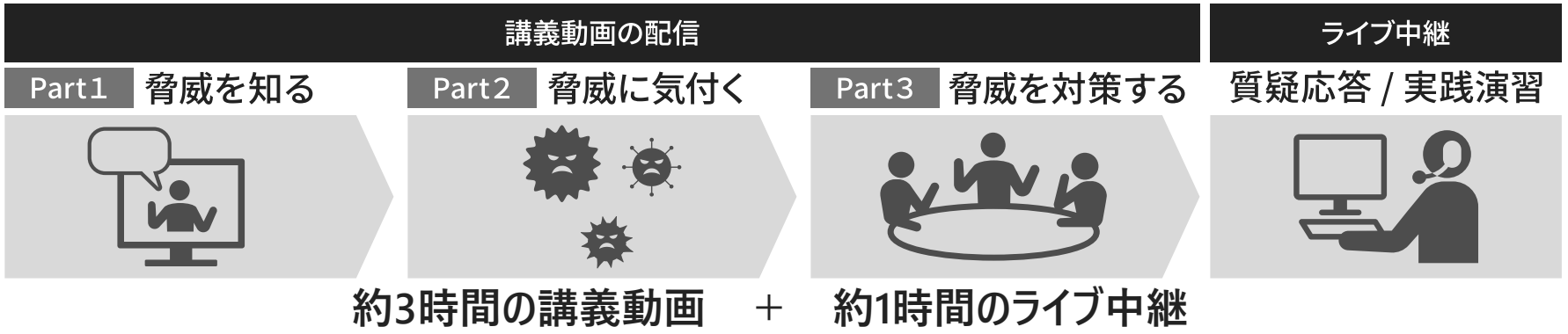
3. セキュリティ人材強化トレーニングの紹介

3-1　セキュリティ人材強化トレーニング

HITACHI

サイバー攻撃の挙動やマルウェア感染などの疑似体験、ライブ中継での質疑応答や実践演習を通じて、

サイバー攻撃に能動的に対応できる人材の育成が可能



➢ **特長**

① 動画配信とライブ中継を組み合わせたスタイルにより、
学習定着率が高く**効率的な知識習得**を実現

② セキュリティに関する知識・知見豊富な当社の**ホワイトハットハッカーが講師を担当**

3-2　コース一覧

HITACHI

セキュリティ人材強化トレーニング

経営層	サイバーセキュリティ危機管理研修(金融機関編)		
戦略マネジメント層	アーティファクトハンドリング	インシデントハンドリング	脆弱性ハンドリング
実務者・技術者層	サイバー攻撃対策(基礎)	脆弱性対策(基礎)	マルウェア対策(基礎)
	CSIRT基礎	PSIRT基礎	サイバーレジリエンス基礎
	クラウドセキュリティ基礎	FSIRT基礎	AIセキュリティ基礎
全社員・職員	情報セキュリティ対策(基礎)	標的型攻撃メール対策(銀行向け)	標的型攻撃メール対策(一般向け)

3-3　コース内容(経営層)

HITACHI

経営層 **サイバーセキュリティ危機管理研修(金融機関編)**

- ✓ 金融庁ガイドラインが要求する経営層の役割と責任を実務レベルで理解(経営層は積極的にサイバーセキュリティに関わる研修・訓練に関与するなど)
- ✓ 経営層がとるべき初動行動と説明責任(いつ・誰が・どこまでを・どのように)を具体的に習得

【受講料】
個別見積 (受講人数、実施場所などにより変動)

3-4　コース内容(戦略マネジメント層)

HITACHI

戦略マネジメント層 **脆弱性ハンドリング**

- ✓ 効果的な脆弱性管理/対策を学ぶ
- ✓ 実際にセキュリティ診断を映像で疑似体験しながら、サイバーセキュリティ診断の手法を学ぶ
- ✓ ライブ中継で実際に脆弱性を分析し、リスク評価を実践

戦略マネジメント層 **インシデントハンドリング**

- ✓ インシデントハンドリングの流れを学ぶ
- ✓ 不正アクセスの痕跡調査を疑似体験し、早期検知、対応を学ぶ
- ✓ ライブ中継でログ分析を実践し、ログ管理の重要性を理解

戦略マネジメント層 **アーティファクトハンドリング**

- ✓ サイバー攻撃が残す代表的な痕跡(アーティファクト) と対応までの一連の流れを習得
- ✓ サイバー攻撃やマルウェアの静的解析・動的解析を映像で疑似体験
- ✓ ライブ中継でアーティファクト解析を実施し、影響範囲の特定などハンドリングを理解

【受講料】

講義動画の受講のみ　　：40,000円/1コース/人

講義動画＋ライブ中継(実践演習)：50,000円/1コース/人

3-5　コース内容(実務者・技術者層)（1/3）

HITACHI

実務者・技術者層　サイバー攻撃対策(基礎)

- ✓ 攻撃者がマルウェア感染したパソコンを遠隔操作し、ネットワーク内の機密情報を搾取する様子などを疑似体験
- ✓ サイバーキルチェーンの攻撃行動を学習

実務者・技術者層　脆弱性対策(基礎)

- ✓ 脆弱性のあるオンラインバンキングから非公開情報が漏えいしてしまう例などを疑似体験
- ✓ 攻撃者の手順、脆弱性の対策方法を学習

実務者・技術者層　マルウェア対策(基礎)

- ✓ マルウェアが感染拡大する様子など、代表的なマルウェアの挙動を疑似体験
- ✓ 攻撃者の手順を学び、脅威からの防御という考え方を学習

実務者・技術者層　CSIRT基礎

- ✓ CSIRTの役割や分類など、CSIRTに関する基礎的な知識を習得
- ✓ 脅威を映像で疑似体験することで、CSIRT運用の重要性を理解

【受講料】

講義動画の受講のみ　　：20,000円/1コース/人(税別)

講義動画＋ライブ中継(質疑応答)　：25,000円/1コース/人(税別)

3-5　コース内容(実務者・技術者層)（2/3）

HITACHI

実務者・技術者層 **PSIRT基礎**

- ✓ PSIRTの役割や分類など、PSIRTに関する基礎的な知識を習得
- ✓ 製品・サービスに対する脅威を映像で疑似体験することで、PSIRT運用の重要性を理解

実務者・技術者層 **サイバーレジリエンス基礎**

- ✓ サイバーレジリエンスを実現するために企業が備えるべき「予測力」、「抵抗力」、「回復力」、「適応力」について、具体的な対策技術とあわせて学習

実務者・技術者層 **クラウドセキュリティ基礎**

- ✓ クラウドやクラウドサービスの基礎、セキュリティの脅威について学習
- ✓ 安全にクラウドサービスを利用・提供するための、さまざまな技術的・人的・組織的対策を習得

実務者・技術者層 **FSIRT基礎**

- ✓ 制御システムを取り巻く脅威、FSIRTの基礎について学習
- ✓ FSIRT技術者として対応するための、インシデント発生前・発生中・発生後の役割を習得

【受講料】

講義動画の受講のみ	：20,000円/1コース/人(税別)
講義動画＋ライブ中継(質疑応答)	：25,000円/1コース/人(税別)

3-5　コース内容(実務者・技術者層)（3/3）

HITACHI

実務者・技術者層

AIセキュリティ基礎

- ✓ AIの基礎や、AIセキュリティの脅威について学習
- ✓ AIに携わる社員・職員として、AI開発者、AI提供者、AI利用者の立場からのセキュリティ対策を習得

【受講料】

講義動画の受講のみ	：20,000円/1コース/人(税別)
講義動画＋ライブ中継(質疑応答)	：25,000円/1コース/人(税別)

3-6　コース内容(全社員・職員)（1/2）

HITACHI

全社員・職員　情報セキュリティ対策(基礎)

- ✓ ビジネスメール詐欺など身近な脅威を疑似体験、脅威を理解し、防御を学習
- ✓ 脅威を見分ける着眼点や、脅威が発生した場合の初動対応を紹介

【受講料】
講義動画の受講のみ：20,000円/1コース/人(税別)
講義動画＋ライブ中継(質疑応答)：25,000円/1コース/人(税別)

全社員・職員　標的型攻撃メール対策(銀行向け)

- ✓ 近年のサイバー攻撃のトレンドを紹介、流行するサイバー攻撃の手口を理解
- ✓ 不審メールの添付ファイル開封やURLリンククリックで発生する被害の疑似体験、影響の学習
- ✓ 行員に必要となる不審メールを見分けるポイントの解説、銀行における添付ファイルの開封、URLリンククリックをしてしまった場合の対処を紹介

【受講料】
初年度：600,000円※(税別)
次年度標準価格：300,000円(税別)
※本コースは受講人数に関わらず、上記の料金です。他コースと異なり作成した動画データを提供するコースです。

全社員・職員　標的型攻撃メール対策(一般向け)

- ✓ 近年のサイバー攻撃のトレンドを紹介、流行するサイバー攻撃の手口を理解
- ✓ 不審メールの添付ファイル開封やURLリンククリックで発生する被害の疑似体験、影響の学習
- ✓ 不審メールを見分けるポイントの解説、添付ファイルの開封、URLリンククリックしてしまった場合の対処として社員・職員一人ひとりが実施する内容を紹介

【受講料】
初年度：600,000円※(税別)
次年度標準価格：300,000円(税別)
※本コースは受講人数に関わらず、上記の料金です。他コースと異なり作成した動画データを提供するコースです。

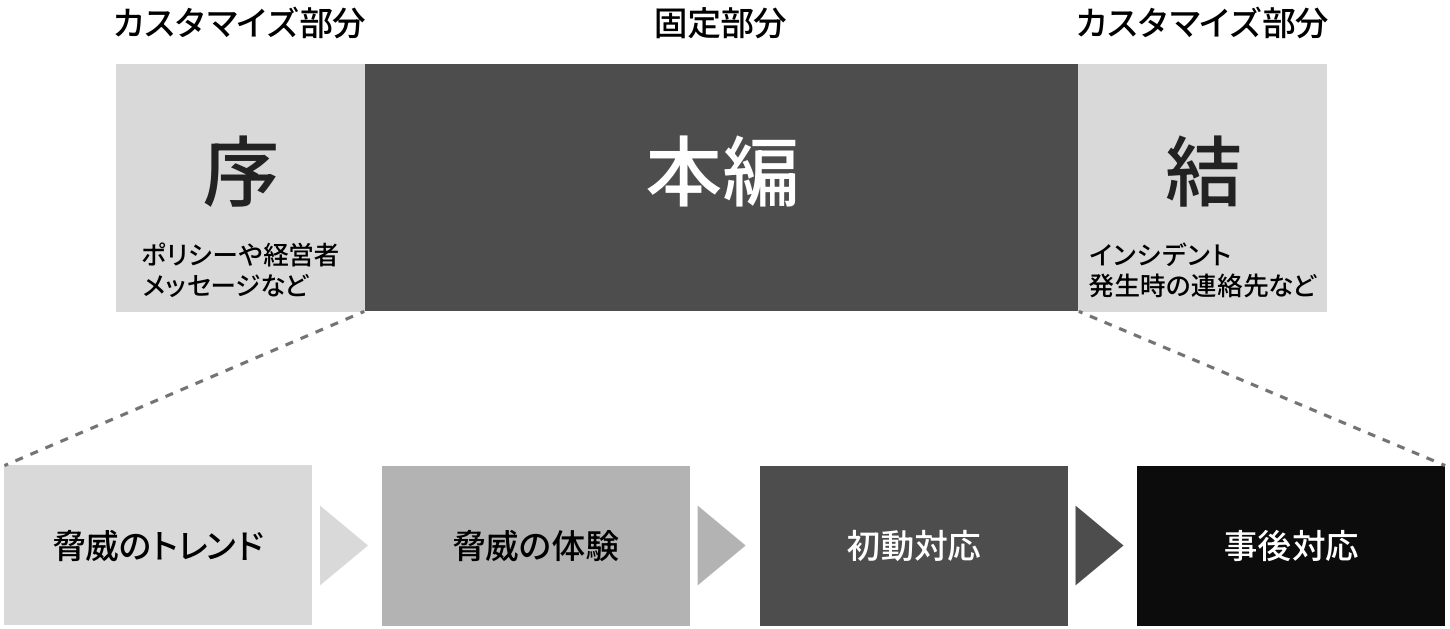
3-6　コース内容(全社員・職員)（2/2）

HITACHI

全社員・職員

標的型攻撃メール対策(銀行向け)
標的型攻撃メール対策(一般向け)

- 「序」、「本編」、「結」の３つで構成
  「序」と「結」の部分はお客さま独自のカスタマイズが可能
- 動画時間：約20分(カスタマイズ内容により変動)



3-7　CSIRT向けトレーニングパック

HITACHI

実務者・技術者層1コース、戦略マネジメント層3コースをまとめた**CSIRT向けトレーニングパック**
CSIRT技術者として行うインシデント対応のライフサイクル(準備・検知と分析・封じ込めと根絶・復旧・事後対応)に加え、日立製作所 Hitachi Incident Response Team(HIRT)のセキュリティアナリストや日立ソリューションズのセキュリティ専門家と当社の講師がインシデントレスポンスをテーマに討議する動画など、「マニュアルの知識」にとどまらない充実した内容で、**CSIRT技術者の育成**に貢献します。

トレーニングパックの内容

受講者層	コース名	パック料金
実務者・技術者層	CSIRT基礎	150,000円/人(税別)
戦略マネジメント層	アーティファクトハンドリング インシデントハンドリング 脆弱性ハンドリング	

講義動画(各コース約3時間、視聴期間1カ月) ＋ライブ中継(2時間×2回) です。

3-8　PSIRT向けトレーニングパック

HITACHI

実務者・技術者層2コース、戦略マネジメント層1コースをまとめた**PSIRT向けトレーニングパック**
PSIRT技術者として製品・サービスを取り巻く脅威についての理解を深め、利用者の安心・安全を脅かす脆弱性やサイバー攻撃への対応を学べます。
また、PSIRT人材の育成などを行っている日立製作所のセキュリティアナリストや、脆弱性診断などを行っている日立ソリューションズのセキュリティ専門家と当社の講師が製品・サービスの脅威や脆弱性対応をテーマに討議する動画など、現場で役立つ実践的な内容で、**PSIRT技術者の育成**に貢献します。

トレーニングパックの内容

受講者層	コース名	パック料金
実務者・技術者層	脆弱性対策(基礎) PSIRT基礎	75,000円/人(税別)
戦略マネジメント層	脆弱性ハンドリング	

講義動画(各コース約3時間、視聴期間1カ月) ＋ライブ中継(2時間×1回) です。

3-9　サイバーレジリエンス基礎パック

HITACHI

実務者・技術者層2コースをまとめた**サイバーレジリエンス基礎パック**
サイバー攻撃の流れや脅威についての理解を深め、侵入を前提とした新しい視点でのセキュリティ対策「サイバーレジリエンス」について学べます。また、この学習を通じて、企業のサイバーレジリエンスを実現する担当者の職務に役立つ実践的なスキルを習得できるため、**現場で活躍できる人材の育成、企業のサイバーレジリエンスを強化できます。**

トレーニングパックの内容

受講者層	コース名	パック料金
実務者・技術者層	サイバー攻撃対策(基礎) サイバーレジリエンス基礎	40,000円/人(税別)

講義動画(各コース約3時間、視聴期間1カ月) ＋ライブ中継(2時間×1回) です。

3-10　標的型攻撃メール対策パック(銀行向け)

HITACHI

標的型攻撃メール対策(銀行向け)と標的型メール訓練を合わせたパック

「教育」により行員一人ひとりが脅威について理解を深めた上で、疑似の標的型攻撃メールを用いた「訓練」を実施し、訓練結果の検証・分析を行うことで、組織として**継続的な標的型攻撃メールへの対応力強化**や、銀行の現状の**リスクレベルの把握・評価、行員への教育定着度の確認**を行えます。

トレーニングパックの内容

受講者層	コース名	パック料金
全社員・職員	標的型攻撃メール対策(銀行向け) 標的型メール訓練	個別見積

3-11　標的型攻撃メール対策パック(一般向け)

HITACHI

標的型攻撃メール対策(一般向け)と標的型メール訓練を合わせたパック

「教育」により社員・職員一人ひとりが脅威について理解を深めた上で、疑似の標的型攻撃メールを用いた「訓練」を実施し、訓練結果の検証・分析を行うことで、組織として**継続的な標的型攻撃メールへの対応力強化**や、企業の現状の**リスクレベルの把握・評価、社員・職員への教育定着度の確認**を行えます。

トレーニングパックの内容

受講者層	コース名	パック料金
全社員・職員	標的型攻撃メール対策(一般向け) 標的型メール訓練	個別見積

4. セキュリティ組織強化トレーニングの紹介

HITACHI

セキュリティ組織強化トレーニング

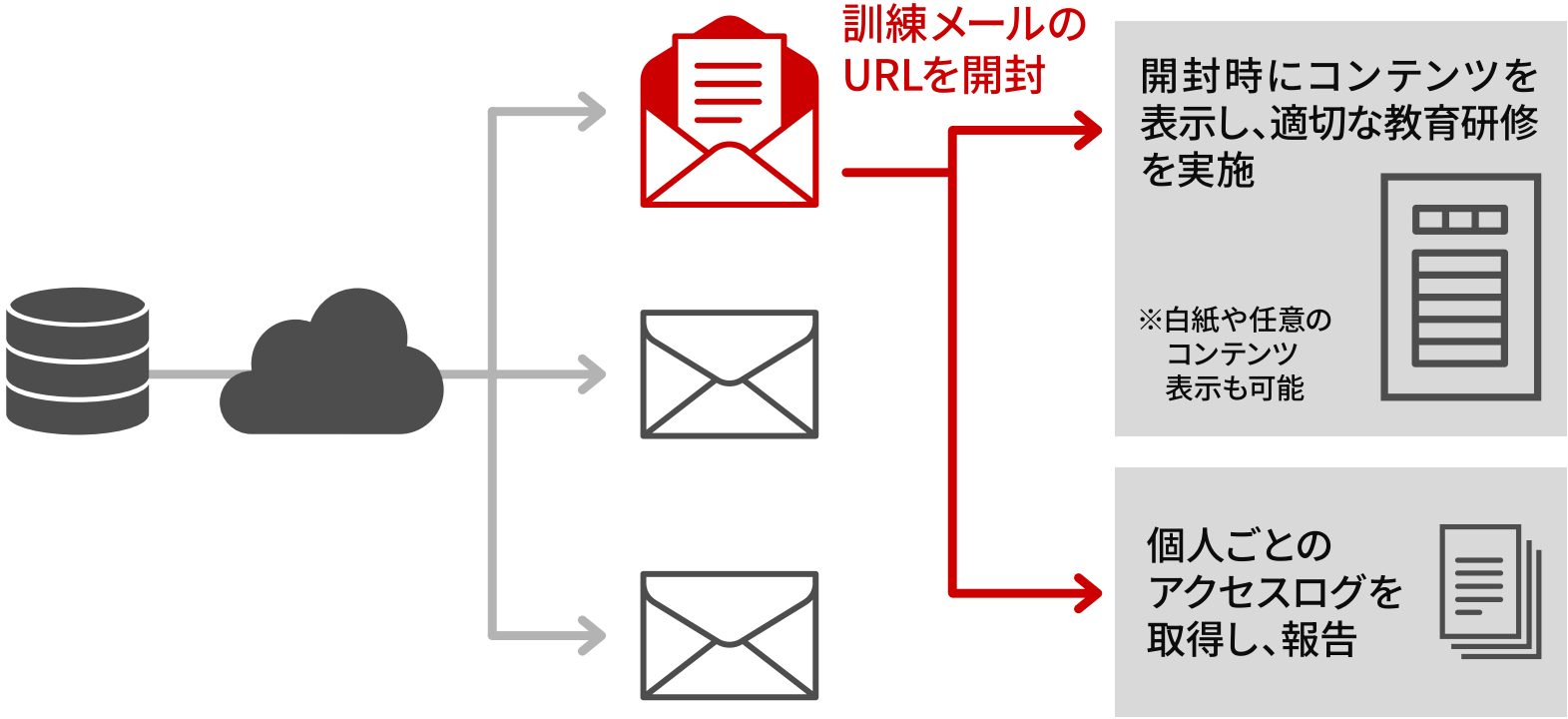
入門	初級	中級
標的型メール訓練	サイバーセキュリティ演習(初級)	インシデント対応訓練
セキュリティリテラシー教育	捜査関係組織向けデジタル・フォレンジック演習(初級)	インシデント対応マニュアル検証
		脆弱性分析とペネトレーションテスト演習
		マルウェアフォレンジック演習
		ハードニングとログ分析演習

HITACHI

入門

標的型メール訓練

標的型攻撃メールを模擬した訓練メールを対象者に送信
標的型攻撃メールへの意識向上や受信時の初動対応について事前教育をすることで、
標的型メール受信時の対策が個人単位で可能



HITACHI

入門

セキュリティリテラシー教育

セキュリティリテラシーの向上を目的とし、受講者が個人や組織で、正しい知識を持って
ポリシーやルールを守り、パソコンやスマートフォンを安全かつ適切に活用できるようになる

【受講料】
個別見積 (受講人数、実施場所などにより変動)

4-4　コース (入門)の特長

HITACHI

1

GSX(※)独自開発システムによる、柔軟なカスタマイズ対応

システムは全てGSX内で独自に開発しています。訓練メールの本文、送信元、開封時コンテンツ、さらには訓練メールの送信間隔などについても、柔軟にカスタマイズすることが可能です。

2

訓練サービス自体への効果的なセキュリティ対策

お客さまのメールアドレス情報の取り扱いや、訓練メールの第三者への転送対策、訓練用サーバーへの不正アクセス対策など、万全のセキュリティ対策を実施した上で当該サービスを提供しています。

3

初めての訓練でも、手間を掛けずに、効果の高い訓練を実現するサポートコンテンツ

初めてのお客さまでも、他社での豊富な実施実績をご紹介できます。
また、訓練メールテンプレート・社内通知メールテンプレート・ヘルプデスクの対応マニュアルなどについても準備しています。

4

継続的な訓練では、開封時の初動対応訓練が可能(オプション)

継続的に訓練を実施されるお客さまには、開封時の初動対応までを訓練できる、分散型送信や開封時通知メールなどのオプションを準備しています。

※標的型メール訓練サービスは、グローバルセキュリティエキスパート株式会社(本資料ではGSXと略します)のサービスです。

HITACHI

初級

サイバーセキュリティ演習(初級)

インシデント発生時の一通りのハンドリングを、グループで実際に手を動かして体験することにより、**組織としてのインシデント対応能力を強化**

時間割例／コース内容

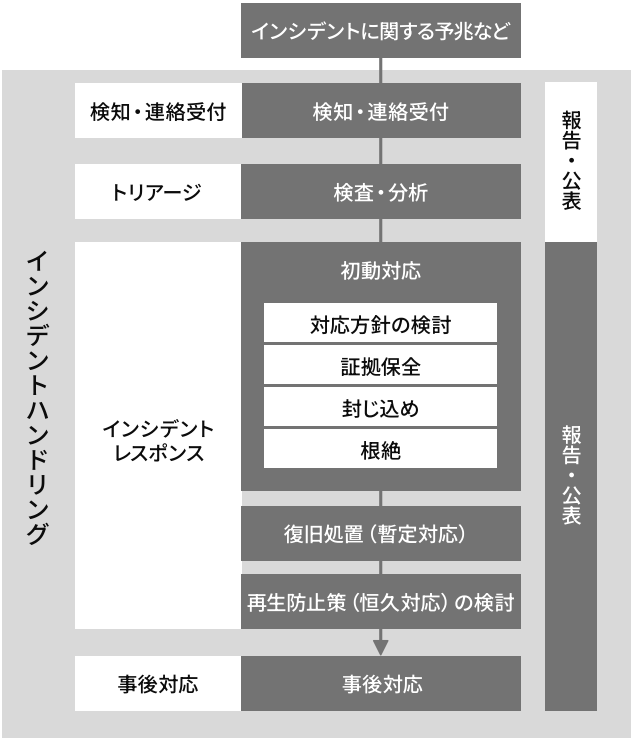
10:00　1 オリエンテーション
- ・連絡事項　・講義（座学）
- ・実機演習の進め方の説明

10:55　2 実機演習　※昼休みなどの休憩を取りながら進めます。
- 2-1 検知・連絡受付
- 2-2 トリアージ
- 2-3 インシデントレスポンス
  - (1) 初動対応・対応方針の検討、証拠保全・封じ込め、根絶
  - (2) 復旧措置（暫定対応）
  - (3) 再発防止（恒久対応）
  - (4) 報告・公表
- 2-4 事後対応

16:30　3 確認テスト

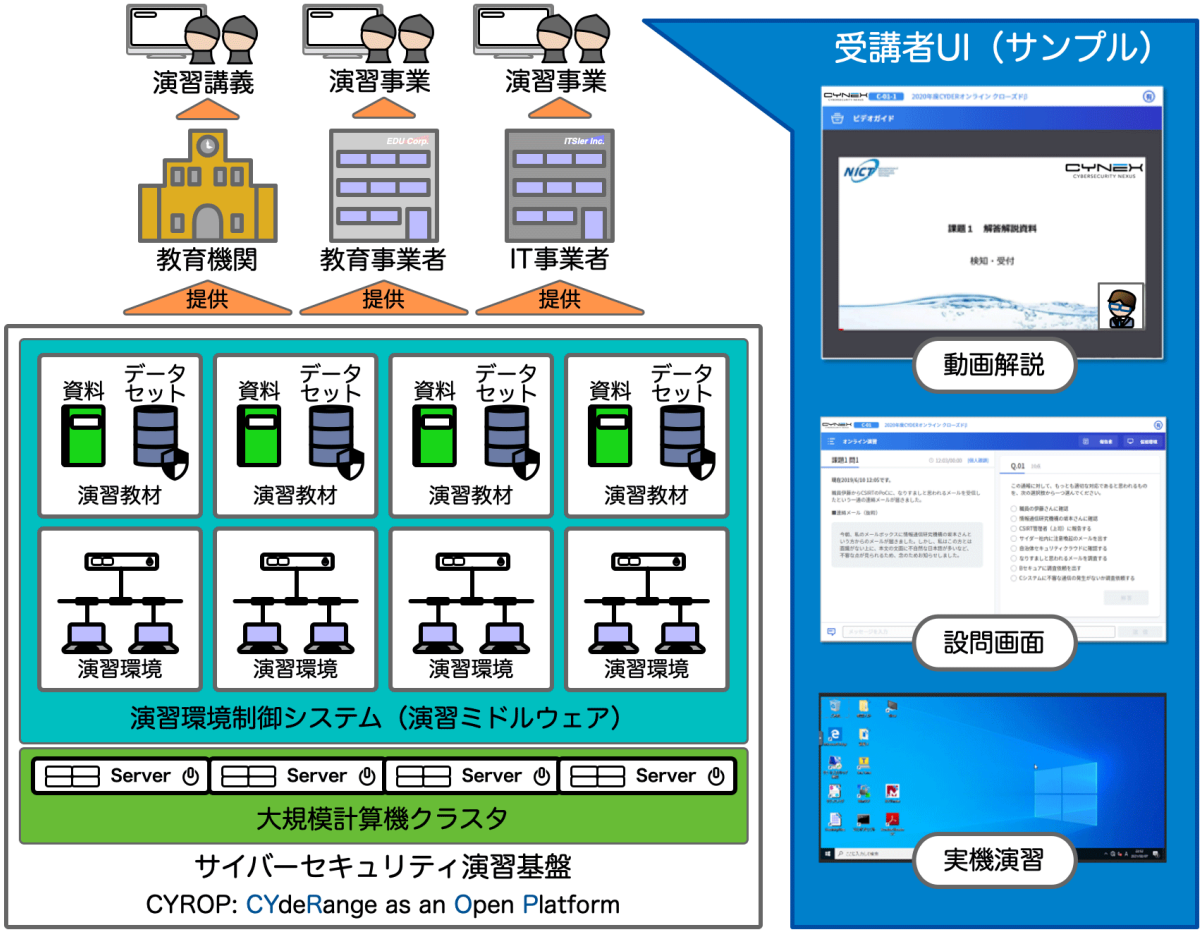
17:00　4 アンケート

17:30　終了



HITACHI

総務省国立研究開発法人情報通信研究機構(NICT)がオープン化のトライアルを開始した演習基盤(CYROP)を活用した演習



これまで主に国の機関や地方公共団体向けに実施していたサイバーセキュリティ演習の演習教材と演習環境を、セキュリティ人材育成事業の実施を希望する民間事業者や大学などの教育機関向けにオープン化

出典：サイバーセキュリティ演習基盤CYROPのオープン化トライアルを開始(https://www.nict.go.jp/press/2022/02/03-1.html)

HITACHI

NICT
総務省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**国内唯一の公的研究機関**として、
情報通信技術の研究開発を基礎から応用まで統合的な視点で推進

NICTでは長年のサイバーセキュリティ研究で得られた技術的知見で
サイバー攻撃に係る**日本固有の傾向などを徹底的に分析**

サイバーセキュリティ演習(初級)では、**民間企業で初めて**NICTの演習基盤を
活用して演習を実施

現実のサイバー攻撃事例を再現した訓練シナリオでの演習により
組織としてのインシデント対応能力を強化可能

HITACHI

中級　インシデント対応訓練/インシデント対応マニュアル検証

インシデント対応訓練では、割り当てられた役割で机上演習を実施いただき、**インシデント対応における組織間の連携を検証・評価**します。

インシデント対応マニュアル検証では、お客さまのインシデント対応マニュアルの内容を事前に把握し、机上演習を通じて**マニュアルどおりに対応できるか、マニュアルどおりに対応して問題(課題)はあったかなどを検証・評価**します。

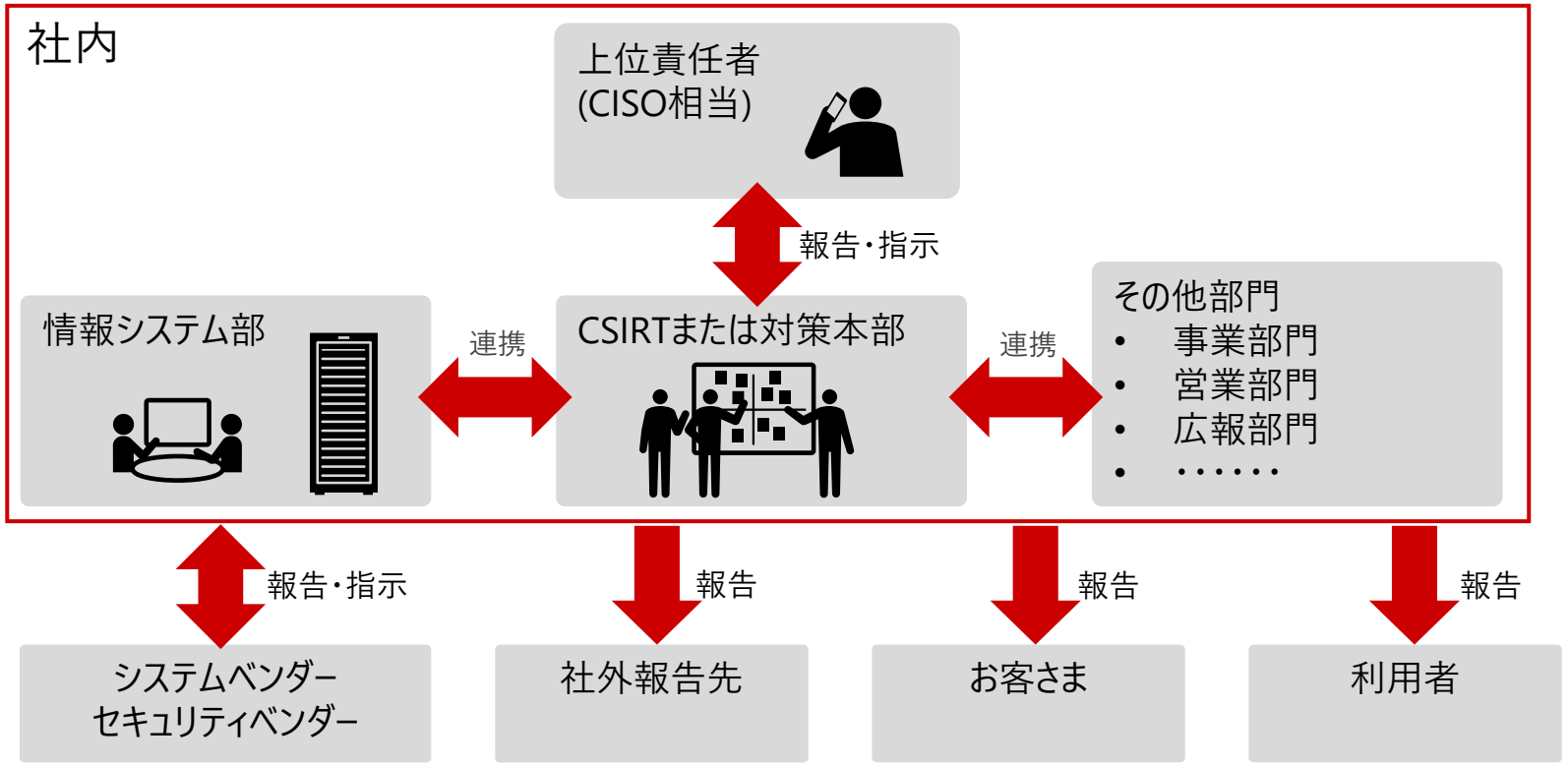
実施項目			インシデント対応訓練	インシデント対応マニュアル検証
標準提供	実施	机上演習(1シナリオで半日程度)	●	●
	評価・報告	プロセス評価	●	●
		インシデント対応マニュアルへの準拠性評価	-	●
		報告書提出	●	●
オプション提供	-	• 報告会の実施 • 出張演習 • 演習シナリオのカスタマイズ ・お客さま組織ベースに変更 (組織体制評価含む) ・インシデント内容の変更 その他、ご要望があればお問い合わせください。	オプション提供	

HITACHI

インシデントレスポンスの部門間連携を確認

■机上演習

- 状況付与型の机上演習によりインシデントレスポンスにおける部門間の連携を検証
- 実際に使用する連絡経路・方法(メール、TEL、報告形式など)での演習が可能(オプション)



(注) 演習に参加されない部門と社外組織は当社が対応します

HITACHI

中級　脆弱性分析とペネトレーションテスト演習

脆弱性分析	脆弱性の内容を分析し、対応の優先度を付ける際に必要な観点について理解を深める
ペネトレーションテスト	ADサーバーに対するペネトレーションテストを実施し、ペネトレーションテストの流れや手法に関する理解を深める

中級　マルウェアフォレンジック演習

メモリ保全・メモリ解析	メモリの保全やメモリの解析を通して、ファイルレスマルウェアの特長や解析方法について理解を深める
マルウェア解析	マルウェア感染機器の調査を通して、永続化などマルウェアの挙動について理解を深める

4-7　コース内容(中級) （4/4）

HITACHI

中級

ハードニングとログ分析演習

スレットハンティング	高度な脅威を事前に検出、防御する取り組みや手法に関する理解を深める
ログ分析	ログ分析ツールを利用したサイバー攻撃の調査方法について理解を深める
ハードニング	組織のサイバー攻撃対策に必要な防御手法について理解を深める

4-8　コース(中級)の特長（1/2）

HITACHI

組織ごとに異なるセキュリティポリシーに柔軟に対応

インシデントレスポンスに絶対的な正解はなく、また対応部門の構成、役割も組織により異なるため、
当社では演習対象組織のセキュリティポリシーに対応した教育となる演習を提供します。

ホワイトハットハッカーが教材の作成・講義を自ら実施

インシデントレスポンスにおいて、「攻撃を知らなければ防御ができない」という考えから、
当社では高度セキュリティ人材が講師を担当し、実践的な演習を提供します。

当社人材が保有する主なセキュリティ国際資格

CEH(認定ホワイトハットハッカー)

CEH(Certified Ethical Hacker)は、EC-Council認定の国際的な情報セキュリティ資格(ホワイトハットハッカー資格)

CISSP(Certified Information Systems Security Professional)

セキュリティ プロフェッショナル認定資格制度(CISSP)は、国際的に認定されている資格であり、セキュリティ専門家としてのスキルの保有を示します

GMON (GIAC Continuous Monitoring Certification)

GMON認定資格保有者は、防御可能なセキュリティ アーキテクチャ、ネットワーク セキュリティ監視、継続的な診断と緩和、および継続的なセキュリティ監視に関する知識の保有を示します

CompTIA Network Security Professional (CNSP)
CompTIA Network Vulnerability Assessment Professional (CNVP)

CompTIAが検証するネットワークセキュリティ、および脆弱性アセスメントに関する国際資格

4-8　コース(中級)の特長（2/2）

HITACHI

実機演習を通じて、有事の際の迅速な対応力強化を支援

「脆弱性分析とペネトレーションテスト演習」、「マルウェアフォレンジック演習」、「ハードニングとログ分析演習」は、実機演習を交えた1日の集合演習です。座学に加え、実機演習を実施することで、個人で学習した知識の活用や、実践を意識したリアルな環境で対応力を養えます。

NICTの演習基盤を活用した、実践的な演習

NICTでは長年のサイバーセキュリティ研究で得られた技術的知見でサイバー攻撃に係る日本固有の傾向などを徹底的に分析しており、この演習基盤による実機演習により、現場ですぐに役立つノウハウや実践的なスキルの習得が可能です。

経験豊富な講師陣がノウハウやスキルの習得を支援

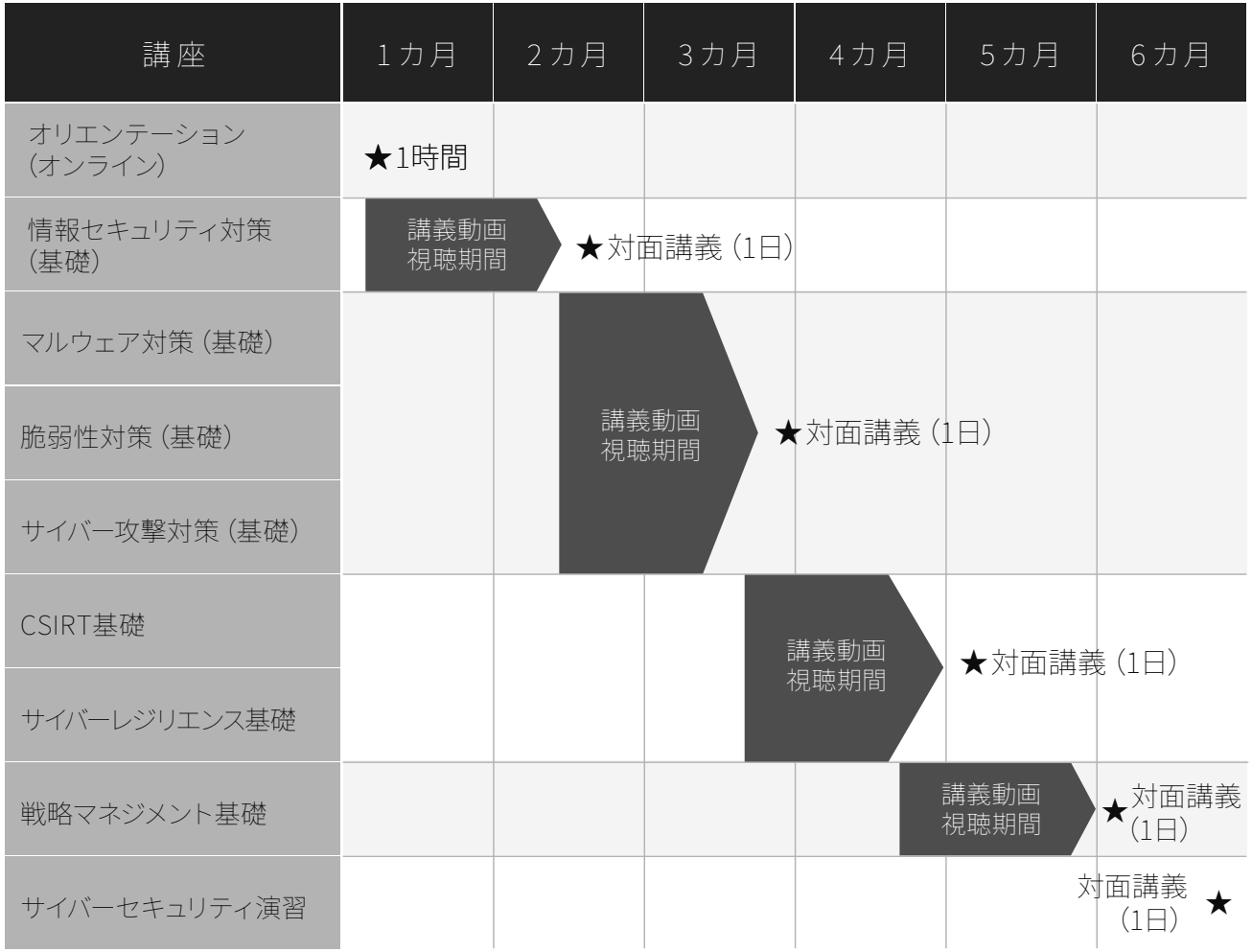
当社の講師陣には、NICTが主催する実践的サイバー防御演習「CYDER」や、実践サイバー演習「RPCI」などの講師経験を有するメンバーが在籍しており、高度な専門知識と実践を加味した的確な指導により質の高い教育を提供します。

５．金融機関向けセキュリティ人材育成プログラムの紹介

5-1　プログラムの内容

HITACHI

約6カ月の育成プログラムとなり、期間内に講義動画(約3時間×7コース)視聴＋
対面講義(約6時間×4回)＋サイバーセキュリティ演習(7時間)を受講します。



HITACHI

- セキュリティリスクの管理やセキュリティ対策の企画・立案などができる人材の育成や、組織演習を通じてインシデント対応力の向上が可能
- 金融機関で特に重要となる、有事の際の迅速な復旧につながるサイバーレジリエンスの考え方まで習得
- 日立グループで実践している対策方法や、現場での経験・体験談を提供することで「マニュアルの知識」にとどまらないノウハウやスキルを習得でき、金融機関のサイバーセキュリティ対策を担う人材を育成

金融庁と日本銀行が求める
「地域金融機関におけるサイバーセキュリティセルフアセスメント」に
対応した体制の整備につながります

HITACHI

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

https://www.hitachi-solutions-create.co.jp/contact/solution.html

※該当のソリューションをお選びください

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

お問い合わせ情報についてご相談・ご依頼いただいた内容は回答などのため、当社の関連会社(日立ソリューションズグループ会社)および
株式会社日立製作所に提供(共同利用も含む)することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。

表示に関する注意事項

HITACHI

■他社商品名、商標などの引用に関する表示

- 標的型メール訓練サービスは、グローバルセキュリティエキスパート株式会社のサービスです。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様・価格は、2025年12月現在のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。