AMIYA

Ver 1.2

一般社員向け
情報セキュリティ教育

(C) AMIYA Corporation

AMIYA

”従業員の意識“が組織を守る

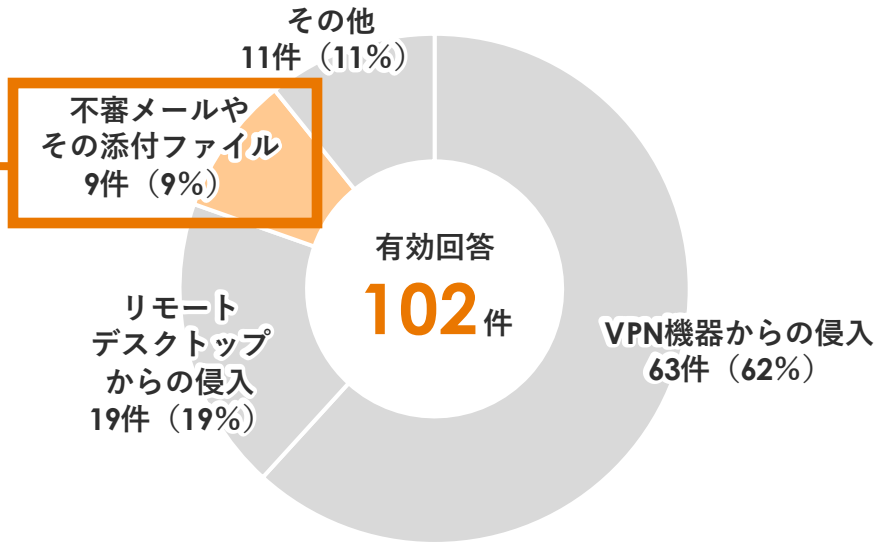
IPA「情報セキュリティ10大脅威 2024 [組織]」

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

従業員の意識でリスクを下げられる攻撃

出典：独立行政法人情報処理推進機構 （IPA）情報セキュリティ10大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

ランサムウェアの感染経路（日本の場合）



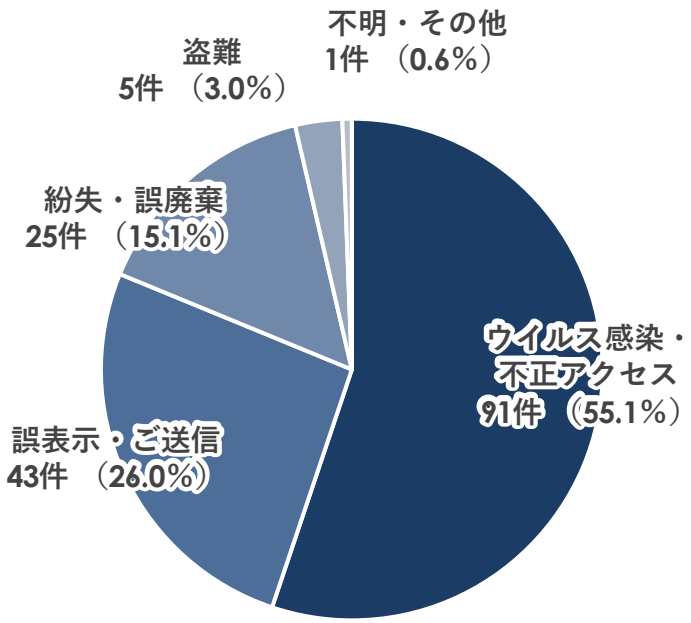
出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

“従業員”がサイバー攻撃対策の「最後の砦」となるか、「経路」となるかは、セキュリティ意識次第。

(C) AMIYA Corporation

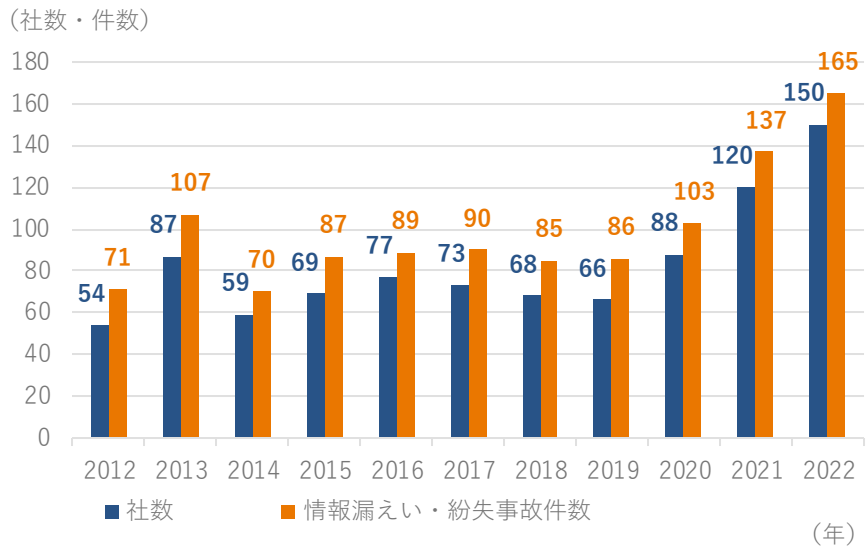
情報漏洩・紛失事故

情報漏洩・紛失事故件数（原因別）



出典：東京商工リサーチ
https://www.tsr-net.co.jp/data/detail/1197322_1527.html

漏洩・紛失事故　年次推移



※社数は年毎にカウント

東京商工リサーチ調べ

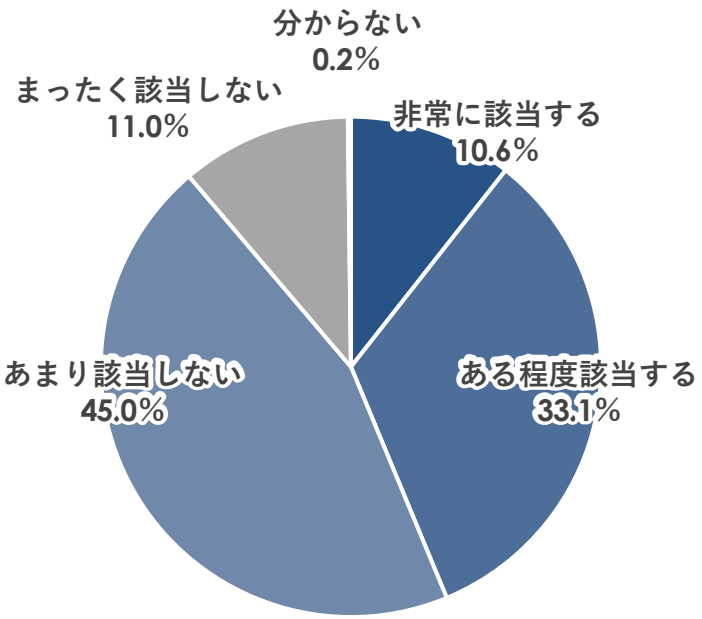
出典：東京商工リサーチ
https://www.tsr-net.co.jp/data/detail/1197322_1527.html

サイバー攻撃対策だけでなく、内部不正や事故への対策も必要

(C) AMIYA Corporation

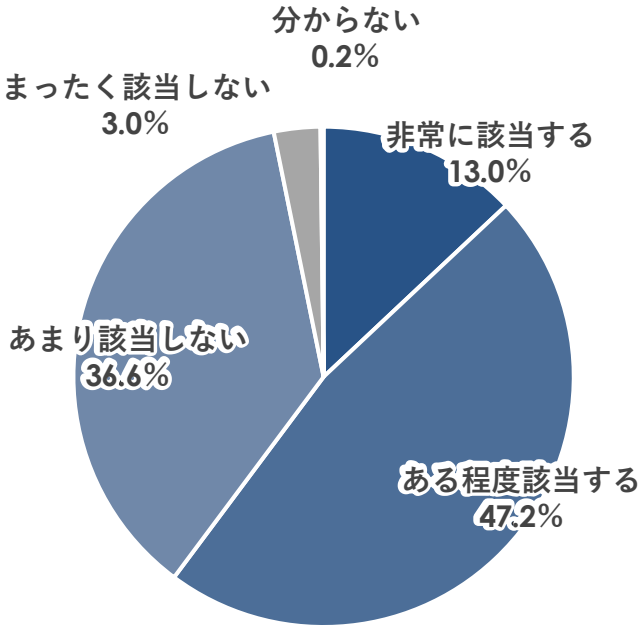
セキュリティ意識の現状（国内企業の従業員に対する調査）

「従業員のセキュリティに対する意識が低い」と回答



出典：Gartner「従業員のセキュリティ意識の現状に関する調査結果」

「自社のセキュリティ・ルールがわかりにくい」と回答



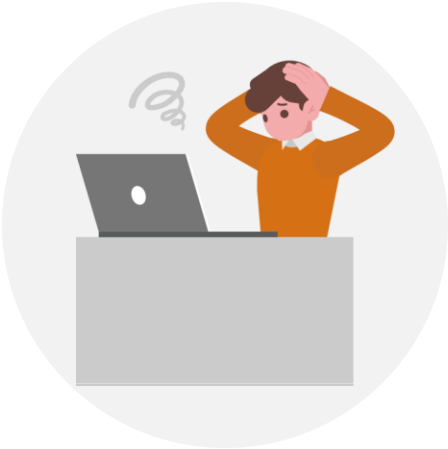
出典：Gartner「従業員のセキュリティ意識の現状に関する調査結果」

従業員自身もセキュリティ意識・ルールに対する問題を認識

(C) AMIYA Corporation

情報セキュリティ教育よくある悩み

こんなお悩みありませんか？



効果測定がしづらい

情報セキュリティ教育を
実施することが目的化している。
そのため、リテラシー向上などの
効果測定ができていない。

目的が不明確

形式的で効果が薄い

PマークやISMS対応として
形式的に年一回の情報セキュリティ
教育を実施しているが、
やらされ感があり、効果が薄い。

頻度不足

最新情報に追いつけない

サイバー攻撃の新手口や生成AIや
SNSなどセキュリティ脅威は
日々新しいものが登場。
その情報に追従できない。

判断の軸がない

(C) AMIYA Corporation

効果的なセキュリティ教育のアプローチ

セキュリティ意識定着のフェーズを理解し、教育の目的を明確化する

フェーズ1　セキュリティの基礎を知る（インプット）

IT全般やセキュリティ全般、サイバー攻撃手法、被害事例、社内規程など、
セキュリティの基礎を知ることからスタートする。

フェーズ2　セキュリティの基礎を実践（アウトプット）

パスワード管理やメールの誤送信、個人情報の取り扱い、標的型攻撃メールを見抜く、
インシデント対応など、知識として理解したセキュリティの基礎を実践し、定着させる。

フェーズ3　セキュリティリスクを自ら考え行動（原理原則の理解）

新しいサイバー脅威の登場などにおいて判断が必要となる場面において、
自らがセキュリティの原理原則（セキュリティリスクマネジメント）をベースに考え、
行動/相談できるようにする。

(C) AMIYA Corporation

セキュリティ教育の年間計画を作成

3カ年計画や年間計画を作成し、必要十分なセキュリティ教育を実施する

例：セキュリティの基礎を知る&実践

メールセキュリティ オンライン講習（情シス向け）

セキュリティ基礎研修（オンライン開催）＋ **試験**

目的：情報セキュリティを理解するために必要な前提知識（用語や脅威事例等）を理解

セキュリティ基礎研修（初回保存動画の視聴）＋ **試験**

目的：情報セキュリティを理解するために必要な前提知識（用語や脅威事例等）を理解（定着のための復習）

4月　5月　6月　11月　12月

標的型攻撃メール訓練（1回目）

目的：標的型攻撃メールを見抜けるスキルを獲得
数値目標：開封率（初回は測定のみ）

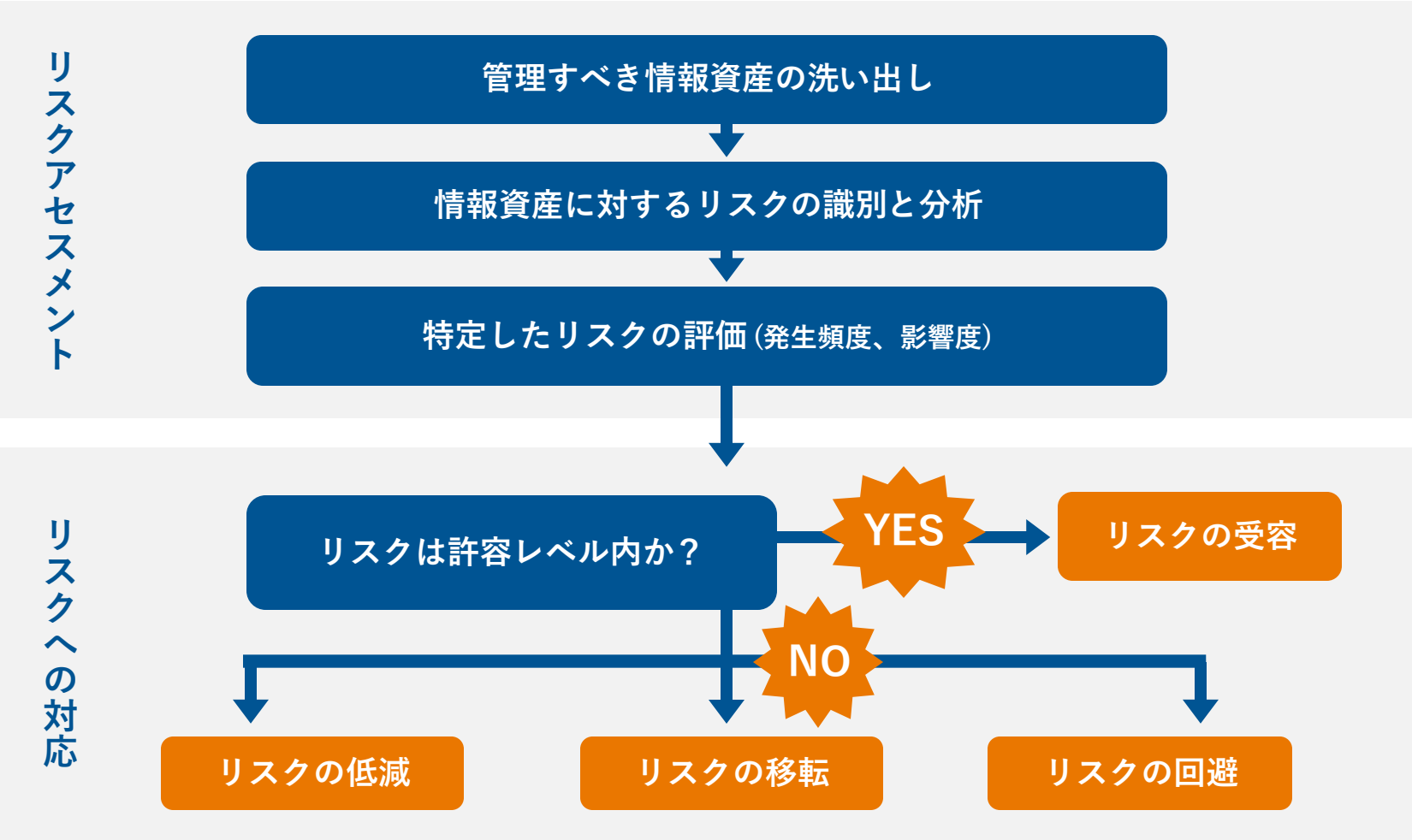
標的型攻撃メール訓練（2回目）

目的：標的型攻撃メールを見抜けるスキルを獲得
数値目標：開封率の5%低下（前回比較）

(C) AMIYA Corporation

セキュリティの原理原則を浸透

セキュリティリスクマネジメントを浸透させる



(C) AMIYA Corporation

AMIYAの情報セキュリティ教育

フルラインナップのセキュリティ教育プログラム

フェーズ1　知る

- 情報セキュリティ講習
- eラーニング
- セキュリティニュース配信

※未リリース

フェーズ2　実践する

- 標的型攻撃メール訓練
- インシデント対応訓練

フェーズ3　自ら考える

- コンサルティング

(C) AMIYA Corporation

セキュリティ講習サービス

フェーズ1 知る

セキュリティコンサルタントがお客様の状況をヒアリングし、
最適な講習プログラム及び説明資料の作成、そして講習まで実施します。

状況・ニーズ
ヒアリング

▶

プログラムと資料の
作成

▶

講習
（オンライン・オフライン）

お客様の状況・ニーズに合わせたプログラムを作成

プログラム例「情報セキュリティの基礎」

1. 情報セキュリティとは？
2. なぜ情報セキュリティが重要か？
3. 情報を安全に扱うためのポイント
   情報セキュリティルール、PCの安全管理、
   パスワード管理、インターネットアクセス、
   電子メール、可搬型記憶装置及び媒体の保護、
   クリアデスク・クリアスクリーン、
   セキュリティインシデント対応

プログラム例「標的型攻撃メール講習」

1. サイバー攻撃の現状
   標的型攻撃メール、マルウェア、ランサムウェア、サプライチェーン攻撃について
2. サイバー攻撃被害
3. 標的型攻撃メールとは
4. 標的型攻撃メールの見抜き方
5. 標的型攻撃メールへの対策（対応フロー）
6. 犯罪の手口（APT攻撃）

(C) AMIYA Corporation

eラーニング

フェーズ1 知る

空いている時間に受講が可能なeラーニングで、確認テストやアンケートが可能。
一般ユーザへの分かりやすさと意識づけを徹底したコンテンツで情報セキュリティの基礎を習得します。

アカウントの発行 ▶ 視聴 ▶ 確認テスト・アンケート

アニメ調のコンテンツなので、リテラシーを気にしない

引用：https://www.kel-gsx.com/informationsecurity/minasecure.html

1. はじめに『あなたと組織を守るために』
2. オフィスで持つべきセキュリティ意識 ①
   ＜メールを扱う上での注意点＞
3. オフィスで持つべきセキュリティ意識 ②
   ＜インターネットやシステムを使う上での注意点＞
4. オフィスの外でも、きちんと持つべきセキュリティ意識
5. 万が一のときに、すぐ報告するのもセキュリティ意識

・アンケート機能

(C) AMIYA Corporation

セキュリティニュース配信 ※未リリース

フェーズ1 知る

情報セキュリティ事件や気を付けるべきポイントなどをまとめたペーパーを月に1回配信。
定期的なセキュリティ情報のインプットにより、セキュリティ意識を向上。

ペーパー
月1回配信

▶

配布
閲覧

定期的な情報発信がセキュリティ意識を醸成

ー サンプルイメージ ー

(C) AMIYA Corporation

比較

フェーズ1 知る

各組織の状況に合わせ、目的にあった教育サービスを選択

	セキュリティ講習	eラーニング	セキュリティニュース配信 ※未リリース
コンテンツのカスタマイズ性	○ コンサルタントが教育コンテンツを作成	×	×
導入のしやすさ	△ リアルタイム開催となるため、従業員のアサインが大変 録画データ視聴でカバー	○ 視聴URLとアカウントの配布のみ	○ ペーパーの配布のみ
時間	△ 1時間程度	△ 1時間程度	○ 5分
頻度	△ 年1回程度	△ 年1回程度	○ 1ヶ月に1回
用途	社内規程の浸透 特定範囲のセキュリティリテラシーの向上	網羅的な情報セキュリティ教育 入社時の研修、 初めての情報セキュリティ教育	情報セキュリティ意識の定着

(C) AMIYA Corporation

標的型攻撃メール訓練

フェーズ2 実践する

標的型攻撃メールへの脅威の高まりから、今日では従業者を対象にした標的型攻撃メール訓練の実施がスタンダードになってきています。
標的型攻撃メール訓練とは、実際の攻撃に似た内容のメールを従業者に送り、そのリアクションを確認する訓練サービスです。

標的型攻撃メールを疑似体験

安全な標的型攻撃メールを送信 ▶ 対象者のリアクション ▶ 結果を確認（報告書）

効果

標的型攻撃のセキュリティリスクを軽減

従業員はサイバー攻撃対策の「最後の砦」。
セキュリティ意識向上が必要不可欠。

(C) AMIYA Corporation

標的型攻撃メールを見抜く力をつける

フェーズ2 実践する

標的型攻撃メールは、より開封されるよう巧妙かつ自然なメールに変わってきています。
ちょっとした違和感に気づくためにも、”見抜く力”を身につける必要があります。

見抜くポイント

① 差出人（送信者）
- 送信者の名前やアドレスが見慣れない
- フリーメールアドレスから送信
- 関係者のメールアドレスに偽装

② 件名
- 興味を持たせて開封したくなる内容
- 【緊急】と急がせて吟味させまいとしている

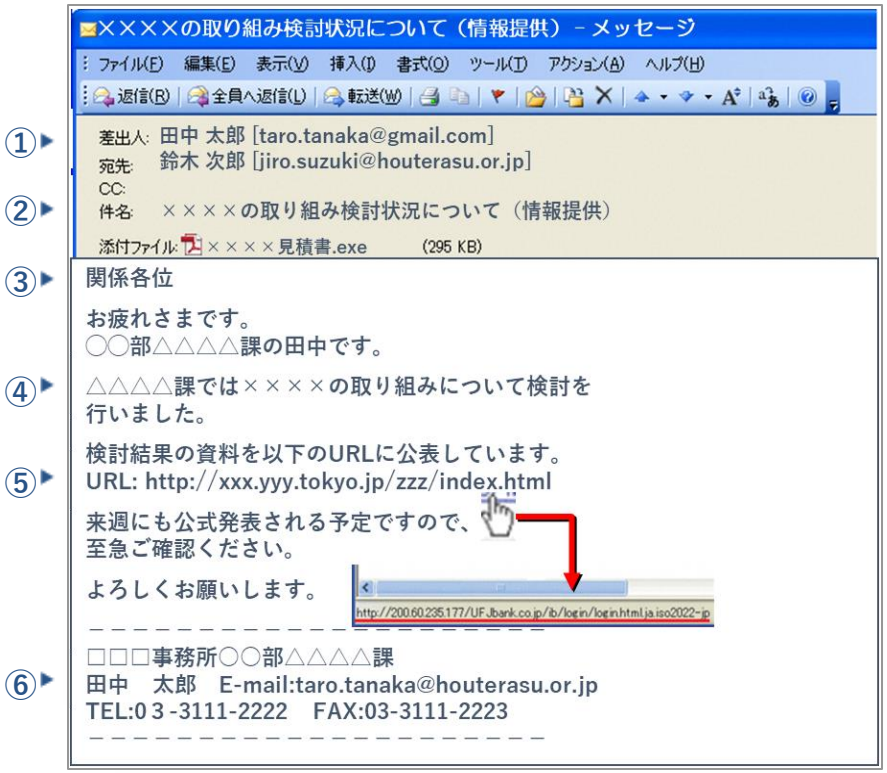
③ 添付ファイル
- 本文と関係のないファイル名である
- 実行形式ファイル（exe / scr / cplなど）、ショートカットファイル（lnk など）が添付されている
- 上記ファイルとわからないようアイコン偽装

④ 本文
- 記載URLをクリックさせるよう不自然に誘導
- 信頼しそうな組織になりすましている

⑤ URL
- 本文表示とカーソル時のURLが異なる（HTMLメールの場合）

⑥ 署名
- 送信者の署名が存在しないか、曖昧である
- 架空の組織名、氏名を使っている
- 差出人のメールアドレスと署名が異なる
- 本人は実在するが電話番号が実在しない

標的型攻撃メールの文面（例）

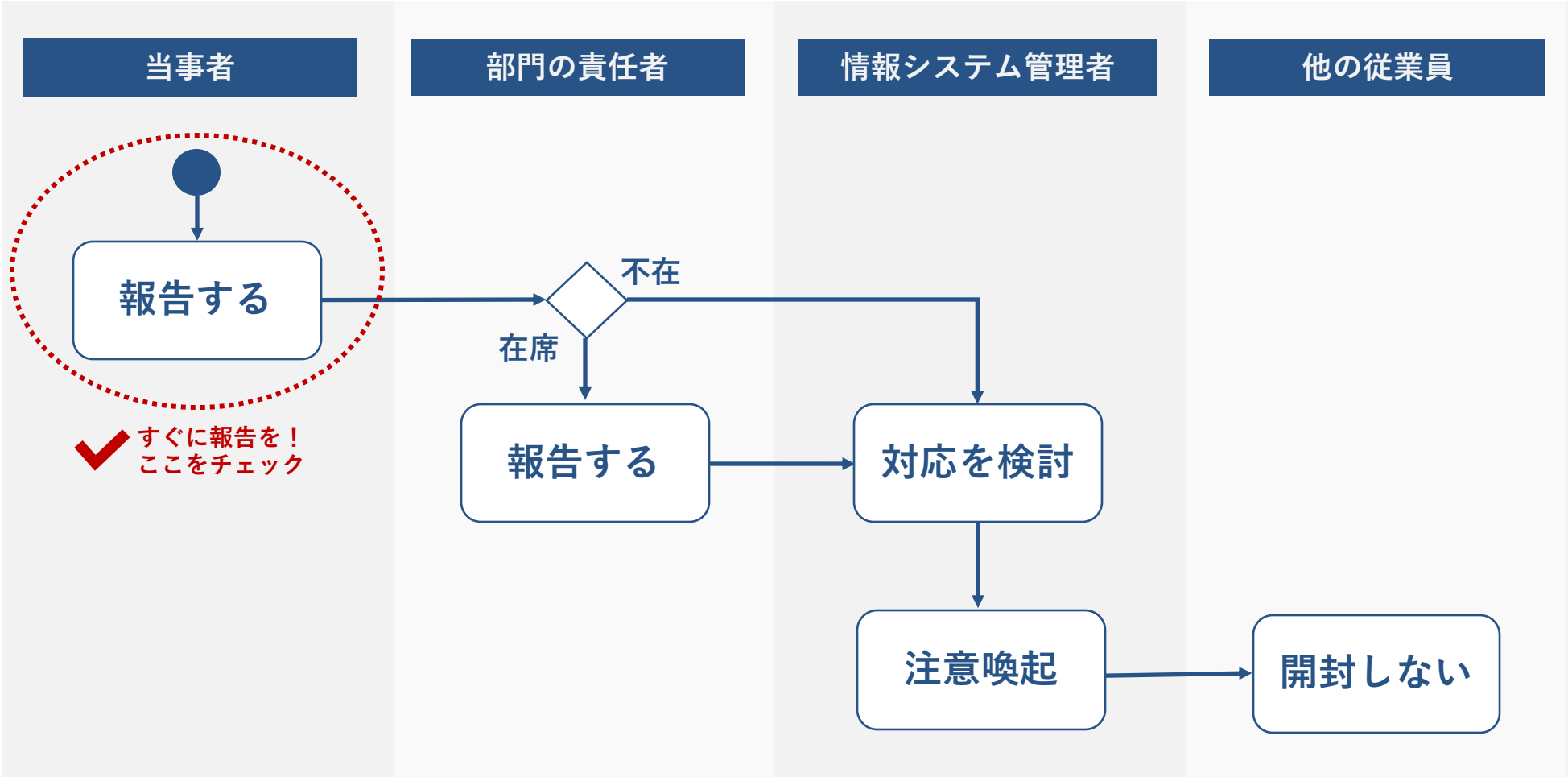


(C) AMIYA Corporation

適切な初動対応ができる組織へ

フェーズ2 実践する

標的型攻撃メールを開かないことも重要ですが、何より本訓練で大切なことは、
ちょっとした違和感を感じた時にフローに沿って報告ができるようになること。



(C) AMIYA Corporation

セキュリティ講習のセットがオススメ

フェーズ2 実践する

標的型攻撃メール訓練後の意識が高い状況で、サイバー攻撃の最新動向や被害事例、標的型攻撃メールの見分け方、報告の重要性をセキュリティ講習で学ぶことで、より効果の高いトレーニングとなります。

セキュリティ講習とセットで効果を最大化

標的型攻撃メール訓練 ＋ **セキュリティ講習（オプション）** **理解度テスト（オプション）**

実施例

実施方法　：ZOOMウェビナー（リアルタイム）
　　参加できない方は、録画データを視聴

実施時間　：1時間（50分講習10分質疑応答）

受講者数　：メール訓練配信の全従業員or開封者など

オプション：・プログラムのカスタマイズ
　　・理解度テスト

プログラム例

1. サイバー攻撃の現状
   標的型攻撃メール、マルウェア、ランサムウェア、サプライチェーン攻撃について
2. サイバー攻撃被害
3. 標的型攻撃メールとは
4. 標的型攻撃メールの見抜き方
5. 標的型攻撃メールへの対策（対応フロー）
6. 犯罪の手口（APT攻撃）

※プログラムの個別作成やセキュリティ全般の教育も可能

(C) AMIYA Corporation

インシデント対応訓練サービス

フェーズ2 実践する

事前に作成したインシデントシナリオに沿って、CSIRT組織のインシデント対応を訓練します。
第三者のトレーナーが進行/アドバイスをすることで、効果的な訓練が可能です。

インシデントシナリオの作成 ▶ シナリオに沿った対応訓練 ▶ 課題の整理（ディスカッション）

インシデントは発生することを前提に、被害を最小化することを考える

インシデント対応の流れ

① 検知/連絡受付	セキュリティツールによる検知や従業員からの報告を受付
② トリアージ	情報収集と整理、判断基準に沿って対応の必要性及び優先順位を判断
③ インシデントレスポンス	事象の詳細分析から対応計画、封じ込め、証拠保全、根絶、復旧、再発防止策検討の流れで対応
④ 報告/情報公開	外部への報告、情報公開を検討し実施。 また、組織内部への情報展開も検討。

タイムスケジュール例（120分）

【20分】①検知・連絡受付

【30分】②トリアージ（検査・分析）

【20分】③対応方針の検討

【20分】④復旧措置と再発防止

【20分】⑤情報公開の検討

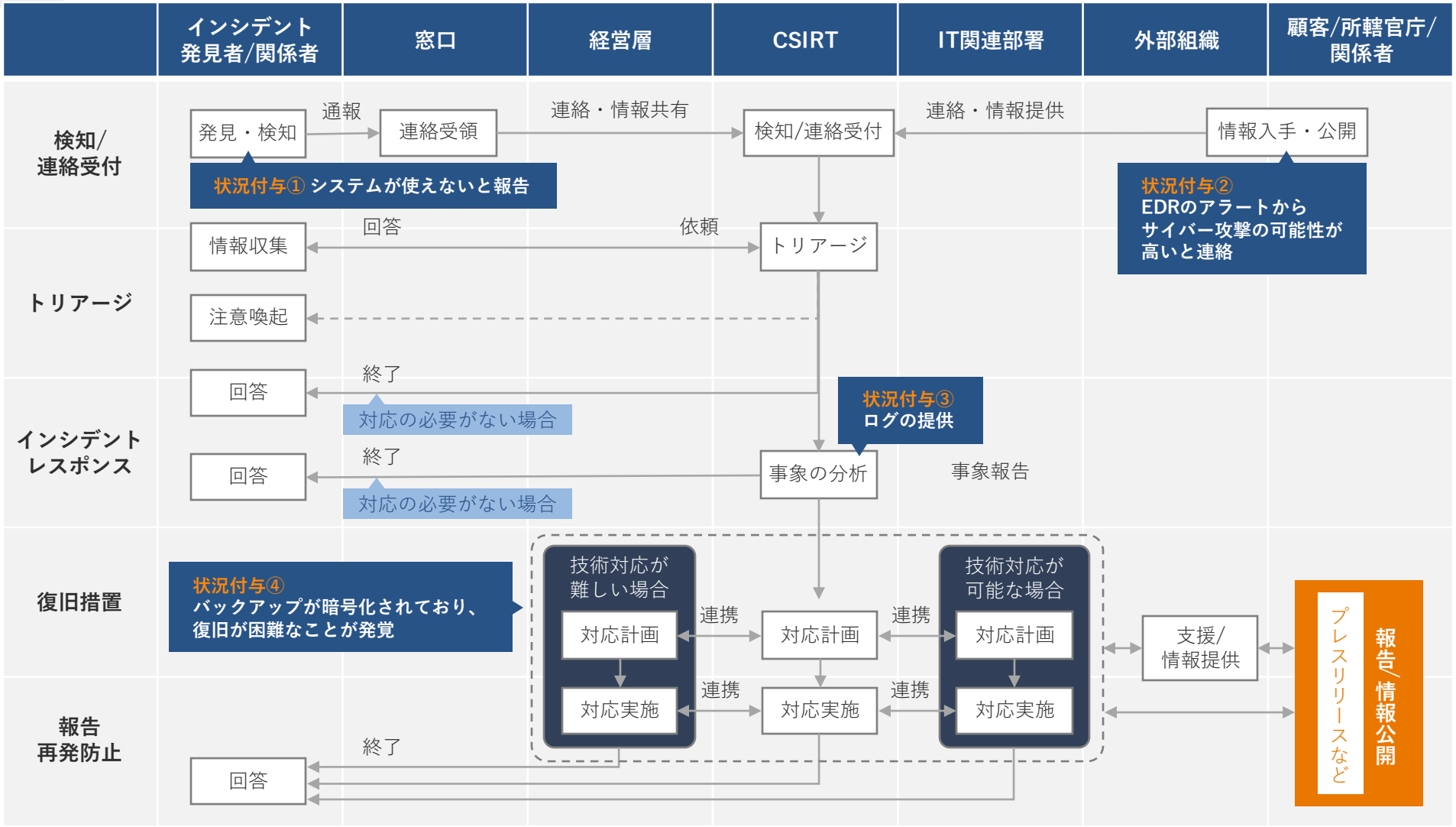
【10分】⑥まとめ及び質問

(C) AMIYA Corporation

シナリオイメージ

フェーズ2 実践する

貴社のCSIRT体制やCSIRTマニュアル、システム環境、セキュリティリスク、最新のサイバー攻撃トレンドからシナリオを作成します。



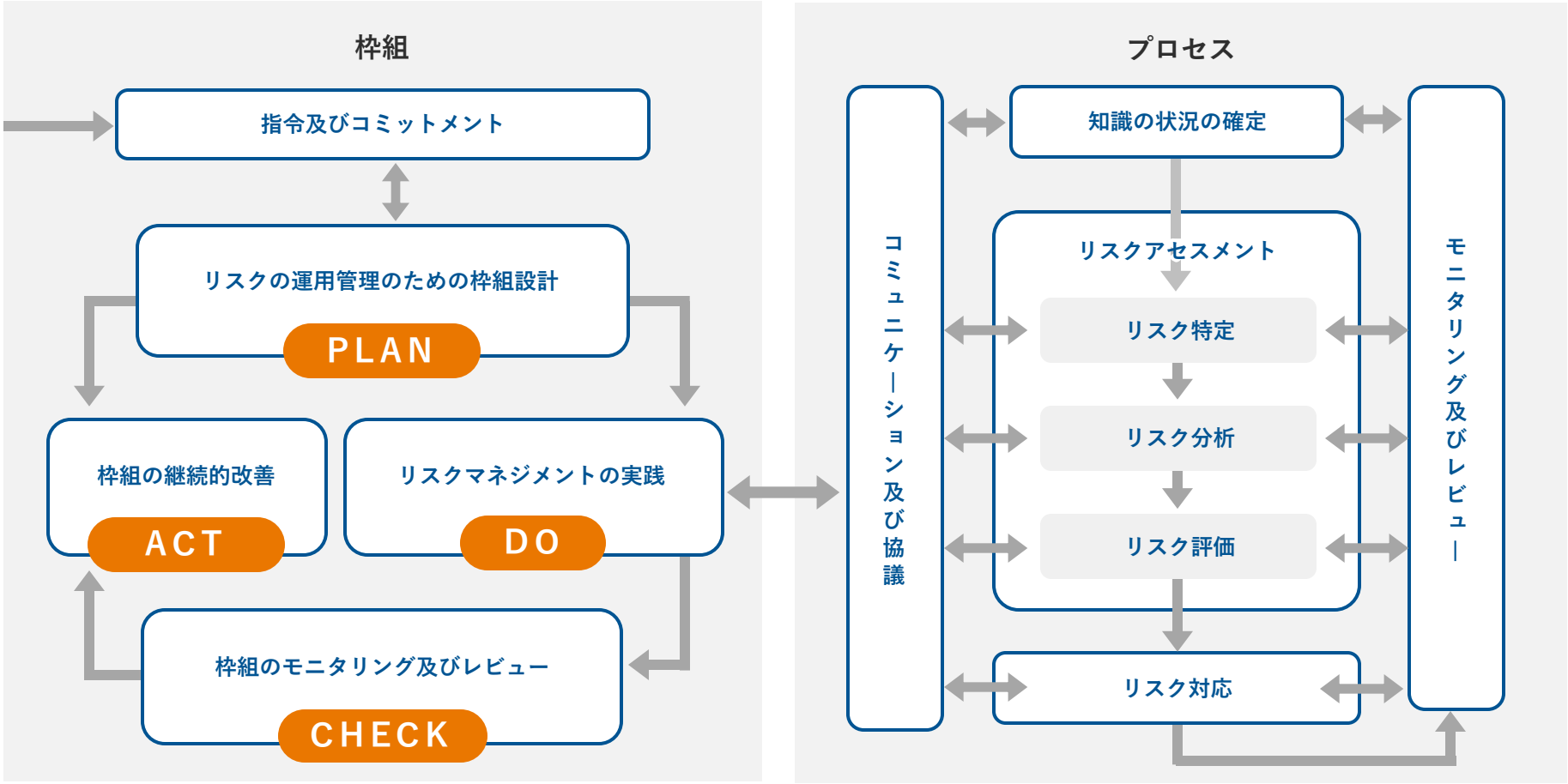
(C) AMIYA Corporation

セキュリティリスクアセスメント

フェーズ3 自ら考える

公的資格を有するセキュリティスペシャリストがセキュリティリスクアセスメントを支援します。
セキュリティリスクを洗い出し、今後の対策へ繋げるだけでなく、アセスメントの手法についても浸透させます。

自ら考え行動するためには、リスクの認識がスタートポイント



※ISO31000から引用

(C) AMIYA Corporation

セキュリティリスクアセスメント

フェーズ3 自ら考える

セキュリティリスクアセスメントには、資産リスクベースと事業被害ベースの２つが存在。
組織の特徴や要望、対象者に合わせて、適切なアセスメントを実施します。

資産ベースのリスク分析シート

凡例: ○ 対策実施　空欄 対策未実施　グレーアウト行: 該当資産で考慮しない脅威　対策の脚字: 対策の補足情報

項番	資産種別	対象装置	評価指標 脅威レベル	脆弱性レベル	資産の重要度	リスク値	脅威(攻撃手法)	説明	対策 防御 侵入/拡散段階		目的遂行段階		検知/被害把握		事業継続		対策レベル 脅威値
1	制御系資産	制御サーバ	2	2		B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	ファイアウォール 通信相手の認証 IPS/IDS パッチ適用 脆弱性回避	 ○			IPS/IDS ログ収集・分析 統合ログ管理システム				2
2			2	1		C	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理 施錠管理	○ ○			監視カメラ 侵入センサー				3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証	○							2
4			2	3		A	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング/Webレピュテーション メールフィルタリング								1
5			2	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		デバイス接続・利用制限		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1
6			3	1		B	プロセス不正実行										
7			3	2		A	マルウェア感染										
8			3	2		A	情報収取										
9			3	2		A	情報改ざん										
10			2	2		B	情報破壊										
11			3	3		A	不正送信										
12			3	3	3	A	機能停止										
							制御不能・異常動作										

事業被害ベースのリスク分析シート

1. 広域での○○供給停止

項番	攻撃シナリオ 1-1	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階		目的遂行段階		検知／被害把握		事業継続		対策レベル 攻撃ステップ	攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	構成ステップ（項番）
	1-1	広域供給停止操作の実行により、広域で供給が停止する。																
1		[N]侵入口=監視端末 悪意ある第三者が、監視端末に不正アクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	○ ○ ○			ログ収集・分析 統合ログ管理システム				2			
2		悪意ある第三者が、監視端末からデータヒストリアン（中継）に不正アクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	● ● ●			IPS/IDS ログ収集・分析 統合ログ管理システム 機器死活監視				1			
3		悪意ある第三者が、データヒストリアン（中継）からデータヒストリアンへ不正にアクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	● ●			IPS/IDS ログ収集・分析 統合ログ管理システム 機器死活監視				1			
4		悪意ある第三者が、データヒストリアンからHMIに不正にアクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	○ 			IPS/IDS ログ収集・分析 統合ログ管理システム 機器死活監視				2			
5		悪意ある第三者が、HMIからコントローラに広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認				ログ収集・分析 統合ログ管理システム				1	2	#1	1,2,3,4,5
6		[P]侵入口=HMI 内部関係者が、計器室に入室する。					入退管理（ICカード） 施錠管理	● ●			監視カメラ 侵入センサ ログ収集分析 統合ログ管理システム	○ ○			1			
7		内部関係者が、HMIにログインする。					操作者認証				ログ収集・分析 統合ログ管理システム				1			
8		内部者関係者が、過失によりマルウェアに感染したUSB媒体をHMIに接続し、HMIがマルウェアに感染する。					アンチウイルス（媒体） アンチウイルス（HMI） ポートの物理的閉塞 ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1			
9		マルウェアが、HMIからコントローラに広域供給停止操作をして、広域に及ぶ供給が停止する。	2	3	3	A	セグメント分割／ゾーニング データ署名 重要操作の承認				ログ収集・分析 統合ログ管理システム				1	1	#2	6,7,8,9

(C) AMIYA Corporation

AMIYAの情報セキュリティ教育

フルラインナップのセキュリティ教育プログラム

フェーズ1　知る

- 情報セキュリティ講習
- eラーニング
- セキュリティニュース配信

※未リリース

フェーズ2　実践する

- 標的型攻撃メール訓練
- インシデント対応訓練

フェーズ3　自ら考える

- コンサルティング

(C) AMIYA Corporation

実践的エンジニア向けセキュリティトレーニング

リアルタイムのサイバー攻撃を体験できる
イスラエル発の最先端セキュリティトレーニングを展開

(C) AMIYA Corporation

AMIYA

一般社員向け
情報セキュリティ教育

(C) AMIYA Corporation