

CISO-PRACTSIE

机上演習によるセキュリティ施策の評価

JNSA CISO支援ワーキンググループ

CISO-PRACTSIE ワークショップ！

時間	項目	アウトプット
13:30-14:00	オリエンテーション ワークショップの進め方 仮想企業 JNSA アーキテクトの説明	オリエンテーション(20) JNSAアーキテクトの理解 (10)
14:00-14:45	セッション1：ランサムウェア-1 (単純感染)	説明 (5) ディスカッション-1 (10) ステータスレポートの作成 (15) 経営陣向けの報告書 (作成 10, 発表 10)
14:45-15:00	休憩	
15:00-15:40	セッション2：ランサムウェア-2 (事業の停止)	説明 (10) ディスカッション-2(15) ステータスレポートの更新(15)
15:40-16:00	セッション3：公表内容の作成	ポジションペーパー(20)
16:00-16:15	休憩	
16:15-16:45	セッション4：経営者の承諾	経営者に発表内容を説明し承諾を得てください
	セッション5：指摘事項の反映	経営者からの指摘事項を反映し、発表内容を修正してください
17:15-17:30	セッション6：ラップアップ	良かった点、伸ばすべきこと 不足していたこと、今後考慮すべきこと(15)

資料

ドキュメント名	概要
01 ワークショップ進行用資料	当ワークショップ進行用の資料
02 ワークショップ用-仮想企業設定 (抜粋)	仮想企業、JNSAアーキテクトに関する情報の抜粋
03 セッション2 関係者の見解	シナリオに対する関係者の見解
20 アウトプット	ワークショップのアウトプット

CISO-PRACTSIE

机上演習による セキュリティ施策の評価

CISO-PRACTSIE ワークショップの目的とゴール

- CISO-PRACTSIEは、インシデントの机上演習を通じて、技術的な視点だけではなく、事業視点、経営視点から、セキュリティ対策の有効性を評価する手法を身に着けることを目的としています。
- CISOは、経営陣の一員としての業務執行が必要ですが、事業上の課題と、セキュリティ上の課題を共通の課題とすることは、なかなか難しい問題です。しかし、セキュリティは単独で成り立つものではなく、事業や他の業務に対するリスク対応の取り組みです。
- このワークショップを自社で展開することで、経営視点・事業視点から、セキュリティ施策全般を評価するだけではなく、経営陣や事業部門とコミュニケーションを促進し、共通のゴールを目指すことにつながります。
- ワークショップの各セッションに正解はありません。
- インシデントをハンドリングするうえで、経営陣や事業部門に求められること、これに応えるために検討すべき事柄などの気づきが重要であり、これを自社で検討し展開するための手法を身に着けてください。

経営者はリスクに鈍いのか？

経営者はセキュリティがわからないことを前提として考えられることが多い
しかし、経営者がセキュリティに鈍いとは限らない

考えてみれば、企業経営は財務的な目標をアウトプット、
各種の状況をインプットとして設定し、
未来を予測しながらリスクと向き合う作業といえる。

セキュリティについても、インプットとアウトプットを設定し
これに対応するプロセスを評価することが出来れば、
経営者とセキュリティ専門家の「ギャップ」は、「共通の課題」と出来ないか。

端的には、実際に事件・事故が起きるまで、リアリティを持って深く考えることは難しい
だから、事前に共通の経験をすることが、共通の課題とするうえで重要になる

公表内容から有効性を評価する

財務的な目標ではなく、合理的な公表内容を目標とする

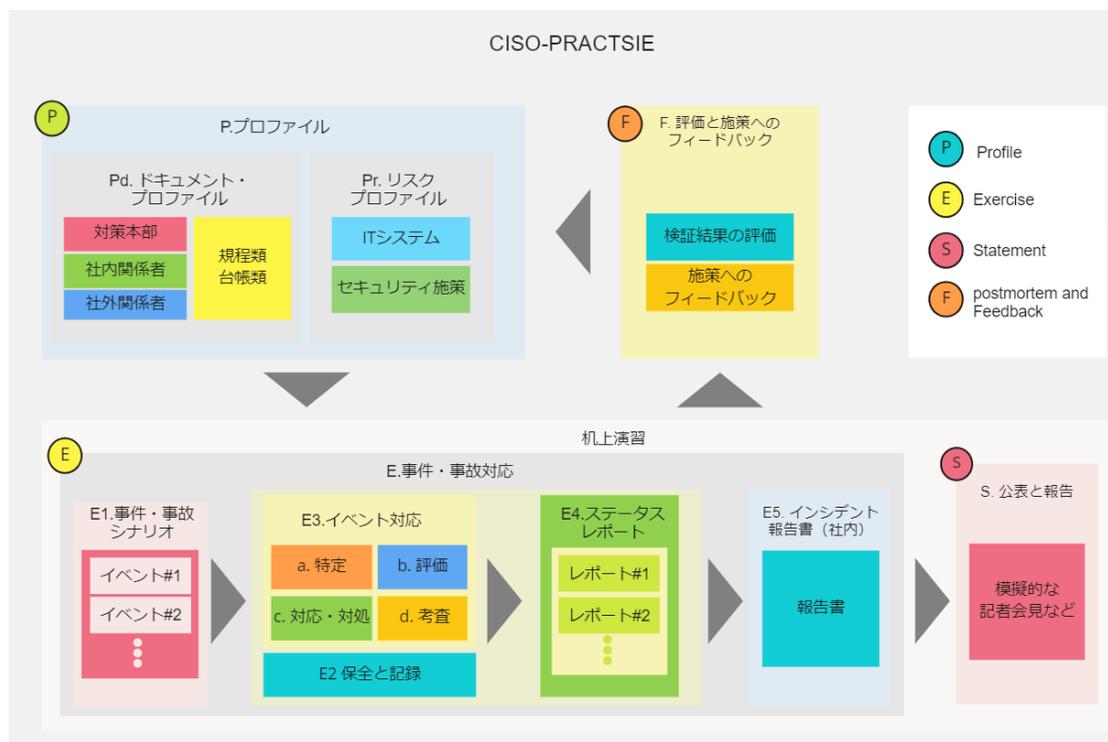
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

INPUT

セキュリティ事件・事故のケース

- 標的型攻撃で機密情報が漏れた可能性
- ハッカーの侵入を受けて、すべてのメールがインターネットに公開された
- WEBページから顧客情報が閲覧可能な状態
- 弊社にしか登録をしていない「メールアドレスに広告が入った」とのクレーム
- 顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」
- インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている
- 弊社が所有するIPアドレスから攻撃を受けているとのクレームが入った
- 弊社のメールアカウントを使った、標的メールが取引先に送信された

PROCESS



OUTPUT

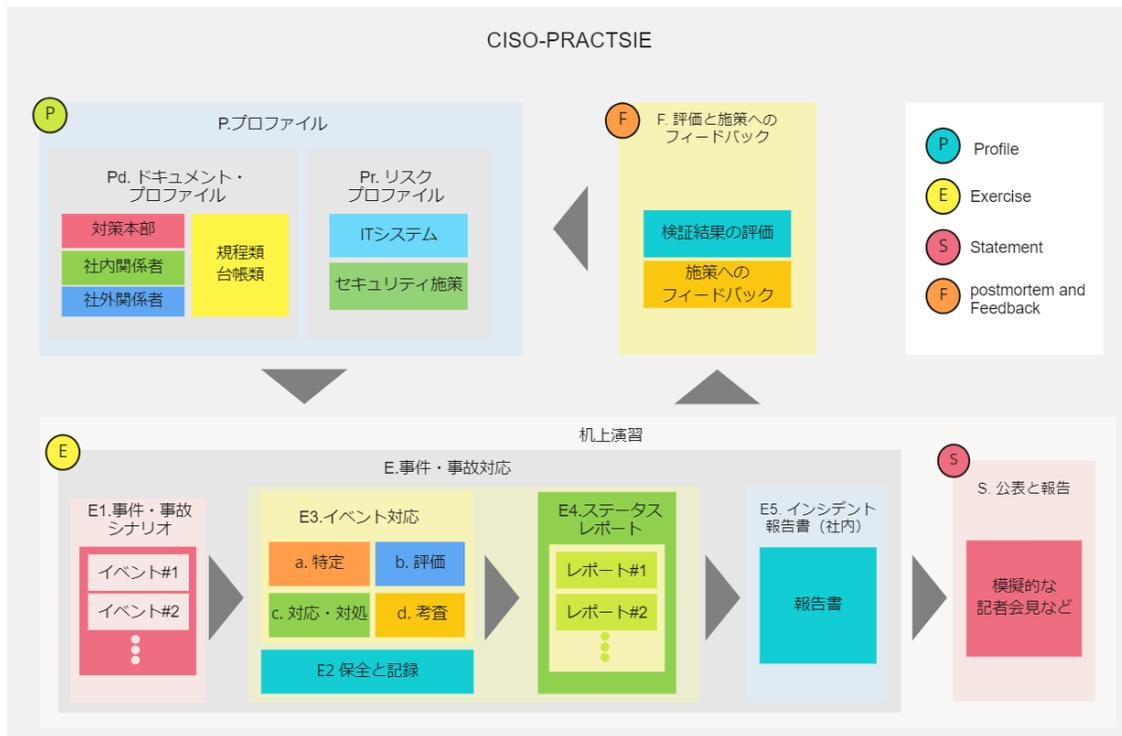
公表内容：ポジションペーパー

影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される2次被害
事業への影響	ワークアラウンド (被害の軽減策)
	被害者への補償
	事業の停止・再開の予定と根拠
事件・事故の経緯	事業レベルの対応 (営業停止、継続、縮退など)
	事件・事故の原因・要因 (なぜ防げなかったのか)
再発防止策	対応のタイムライン (経営者が認識したタイミング)
	再発防止策の内容と実施時期
責任関係	関係者の処分など

CISO-PRACTSIE: PRactical Assessment for Company-wide security measures Through Security Incident Exercise for CISO

CISO-PRACTSIE, JNSA CISO支援ワーキンググループ

CISO-PRACTSIEの構成

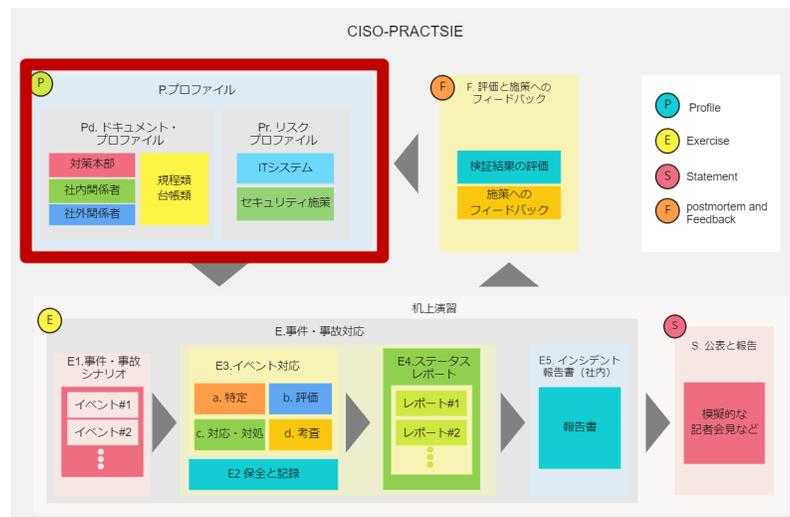


- P：プロフィール：現状の対策状況を整理する
 - 規定類、台帳類、技術資料
 - システム一覧、リスク評価結果
 - セキュリティ施策
- E：演習：机上演習を通じて対策状況を評価する
 - シナリオを設定し、演習に投入するイベントを作成する
 - イベントに対して、特定、評価、対応・対処、考査を行う
 - ひな型（ステータスレポート）を使って、状況を整理する
 - 社内報告書を作成し、経営・事業目線でイベントを評価する
- S：公表と報告
 - 模擬的な記者会見を通じて、外部の目線から検証する
 - 公表を行う上で、不足する情報や対策を検証する
 - 報告や届け出が必要な組織と内容を検証する
 - 再発防止策をまとめることで、現状で対応が必要な施策を明らかにする
- F：評価とフィードバック
 - 演習の結果、評価すべき対策などを明らかにする
 - 再発防止策として明らかになった課題の改善策を策定する
 - 演習を通じて構築したコミュニケーション基盤を維持する

プロフィール

CISO-PRACTSIEでは、最初に本来あるべき資料関係を確認し整理する作業から始めます。

- ISMSをはじめとしたセキュリティ規準では、規定類や台帳類の適切な管理が求められます。
- インシデント対応では、技術的な能力が重視される傾向があり、これらの資料は重視されない傾向がありますが、インシデントに対して、技術レベル・事業レベルで状況を判断し、適切かつ迅速に対応していくためには、生命線となる資料でもあります。
- CISO-PRACTSIEは、本来は自社のセキュリティ対策が対象となりますが、本ワークショップでは、仮想企業を設定し、その仮想企業のセキュリティ対策を対象としています。
- 各資料の有用性、必要性について考察し、自社・自組織で必要な資料などに不足がないか検討する、手掛かりとしてください。



規程類・手順のプロファイル

▼表3-1 JNSA：情報セキュリティポリシーサンプル改版(1.0版)注1

01_情報セキュリティ基本方針	08_セキュリティ・インシデント対応規程
01_情報セキュリティ方針	09_システム変更管理規程
02_人的管理規程	10_システム開発規程
03_外部委託先管理規程	11_システム管理規程
04_文書管理規程	12_ネットワーク管理規程
05_監査規程	13_システム利用規程
06_物理的管理規程	14_スマートデバイス利用規程
07_リスク管理規程	15_SNS利用規程

規定類

▼表3-2 関係者とコンタクト方法

コンタクト先	氏名	連絡方法	備考
緊急対応手順などに記載された役職・役割など	該当する人物の氏名	メール、ビジネスチャット、電話などの具体的な連絡方法 メーリングリスト名、チャンネル名など	秘書を通じて連絡する場合は読み取り許可がないなど、コミュニケーションの作法

関係者と
コンタクト方法

▼表3-3 外部コンタクト先の例

ITシステムなど	ITシステムの構築を行ったベンダー システム開発を委託したベンダー 使用している機器のメーカー
セキュリティ企業	緊急対応サービス マルウェアなどの解析 フォレンジックサービス セキュリティ検査 セキュリティ監視サービス セキュリティコンサルティング全般
法務全般	弁護士、法律事務所
会計財務	公認会計士、税理士、税務署など
保険金	保険会社
輸出入管理	安全保障貿易情報センター

▼表3-4 通報・連絡窓口の例

外部からの連絡・通報窓口		内部の連絡・通報窓口
一般的な窓口 ・代表・大代表 ・顧客窓口 ・サポート窓口 ・広報窓口 ・採用窓口 ・各種通報窓口	セキュリティ関係の窓口 ・CSIRT ・セキュリティ通報窓口 ・個人情報関係の窓口 ・プライバシー窓口 ・データ保護責任者 ・EU代理人	・顧客担当 ・ヘルプデスク ・情シス ・CSIRT

▼表3-5 収集する技術資料の例

一般的な名称	目的
情報資産管理台帳	イベントの深刻度、緊急度、影響範囲を分析・評価する
ネットワーク構成図	ネットワークレベルで、イベントの深刻度、緊急度、影響範囲などを分析・評価する際に必要
IPアドレス一覧	IPアドレスが起点となるイベントで、セグメントや端末を、ネットワーク構成図や、情報資産管理台帳と紐づけるために必要

技術資料

▼表3-6 主要システム一覧の例

カテゴリ	システム名	システムごとの情報
基本的なITインフラ	認証システム	<ul style="list-style-type: none"> システム名 実装(システム名、サービス名など) オーナー(責任者)・担当者 関連ベンダー(開発、構築、運用など) 実施しているセキュリティ対策 ログの種類、内容、保存期間など アカウント、特権アカウント システムが保有する情報(特に個人情報、機密情報)
	メールシステム	
	ファイルサーバー	
	カレンダー	
	ビジネスチャット	
公開システム	ホームページ	
	コンシューマ向けシステム	
	ビジネス向けシステム	
	SNS公式アカウント	
社内システム	求人関係	
	ERP、決済システム	
	給与明細・源泉徴収	
	電子契約システム	
システム開発環境	その他	
	GitHub	

システム一覧

▼表3-7 アカウントと特権

システム名称	システムなどの名称
アカウント管理者	責任者および担当者
管理方式	IDMによる管理、ローカルアカウントで管理など
アカウントの種類	システムにおける権限(ロール)の種別と付与条件
特権アカウントのライフサイクル	作成・変更・無効化・削除などのライフサイクル
アカウントのライフサイクル	一般アカウントの作成・変更・無効化・削除などのライフサイクル
特権アカウント所有者	特権アカウントを付与したアカウントと権限
アカウント一覧	台帳または確認方法

アカウントと
特権

リスク・プロファイル

システムごとの
プロファイル

▼表3-9 事業視点でのリスク評価項目

項目	例・視点	顧客	業務	財務 ^{注8}
情報漏えい・流出	情報の機密度・情報量 情報の種類（個人情報、知財等） 認証情報など	影響 影響範囲 顧客数	影響 回復時間 影響範囲	費用損害（事故対応損 事故原因調査 対外対応 広告・宣伝、コールセンター 見舞金、被害範囲等調査 復旧および再発防止 システム復旧、再発防止 賠償損害 賠償費用、弁護士費用等 利益損害 直接的・間接的な機会損失 金銭損害 身代金（ランサムウェア） 詐欺被害、オンラインバンク 行政損害 個人情報保護法、GDPR、CCPA 無形損害 ブランド毀損、株価
改ざん	情報の機密度・情報量 情報の種類（個人情報、知財等） 認証情報など	顧客業務		
業務の停止・縮退	停止 縮退（一部停止）			
コンプライアンス	制裁金、行政命令 PL法・リコール 拘束、逮捕、拘留、起訴			
社会的な影響	人命・身体 環境汚染			
被害の拡大	ランサムウェア APT/バックドア 他サービスへの影響			
想定される事象	報道、炎上 不買運動、取引停止 脅迫・詐欺行為、暴露			

事業レベルの
リスク評価

システムレベルの
リスク評価

▼表3-11 技術的なプロファイル（社内のサービスのプロファイル）（続く）

ENISA	具体的な確認項目
O01: Geographic spread	O0100 複数のデータセンターを利用している
O02: Elasticity	O0200 柔軟なキャパシティを持つインフラを利用している
O04: Physical security	O0400 信頼できるデータセンターを利用している
O05: Incident response around-the-clock	O0500 事業がCSIRTを持っている
	O0510 事業のインシデント対応窓口が用意されている
O06: Software development	O0600 SDLが実装されている
	O0610 標準に基づいたセキュリティ検査を実施している
O07: Patching and updating	O0700 合理的なパッチマネジメントが行われている
O08: Backups	O0810 特定の日にリカバーできる
O09: Server-side storage	O0900 ボリュームレベルの暗号化をしている／できる
O10: Security-as-a-service and security add-ons	O1000 具体的なセキュリティ対策を実装している
O11: Certification and compliance	O1100 セキュリティ認証を取得している
R01: Software security vulnerabilities	R0100 ホストレベルの要塞化を実施している
	R0120 ホストレベルのセキュリティ検査を実施している

▼表3-10 評価対象事業・システムのプロファイル例（暗号資産取扱事業者）

項目	確認する内容	暗号資産取扱事業者の例
事業概要	事業概要	事業概要、ユーザー特性、 利用形態などを記載する
	事業責任者	役職と氏名を記載する
	運用責任者・担当者	特に責任者は、役職と氏 名を記載する
	開発責任者・担当者	特に責任者は役職と氏名 を記載する
	ユーザー数（有償、無償）	システムを利用するユー ザー数を記載する
	売上高・見込み	対象事業の売上高または、 見込みを記載する
	ユーザーの居住地域 サービス提供地域	海外対応が必要かを判断 するため、ユーザーの主 な居住地域を記載する
連絡窓口	ユーザーサポート 顧客担当 会社代表 インシデント・脆弱性	Webに問い合わせページ 担当営業制度はない
取り扱う情報	情報の種類	取り扱う情報の種類を記 載する。特に、機微性の 高い情報に着目する
	改ざんされた場合の影響 （自社・顧客など）	たとえば、マルウェア拡散、 金銭的な損害、社会イン フラの停止、人命への影響、 会計処理の問題、炎上
業務停止の影響	SLA	システム停止、金銭的な 処理、責任の所在など
	自社への影響	業務の停止・遅延、決済 の停止などの影響

サンプル会社：JNSAアーキテクト

ネットワーク構成図

▼表D-1 JNSAアーキテクト 会社概要

社名	株式会社JNSAアーキテクト
設立	2000年4月13日
本社所在地	〒105-0003 東京都港区西新橋
資本金	3億円
従業員数	270名
平均年齢	42歳
事業内容	PCオンラインゲームの開発及びサービスの提供 モバイルゲームの開発及びサービスの提供
役員 (2022年4月1日時点)	
代表取締役会長 (CEO)	田中 英彦
代表取締役 CFO	下村 正洋
取締役	中尾 康二 高橋 正和
社外取締役	本川 祐治 林 佳子
(監査等委員)	土井 充

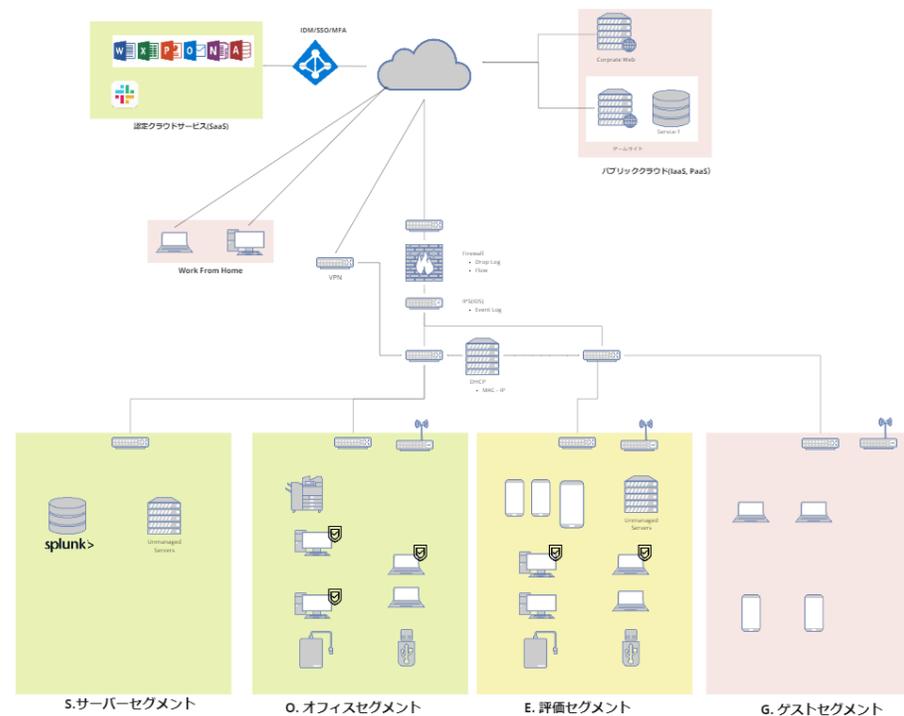
会社概要

組織構成

▼表D-2 組織構成

組織	責任者	主要なメンバー
財務・経理	下村 CFO	黒川 D
法務 (知財、輸出入管理を含む)	下村 CFO	稲葉 D
人事	下村 CFO	三宅 M、桜井 M
総務	中尾 取締役	川内 M、元持 M
広報	小屋 執行役員	唐澤 M
ゲーム事業部	佐々木 執行役員	中村 D、福沢 M
システム開発部	藤井 開発本部長	GanGan 開発 G (後藤 M) SokoSoko 開発 G (金子 M)
システム運用部	青島 D	GanGan 運用 G (山口) SokoSoko 運用 G (前田)
情シス	矢野 CIO	佐藤 M、鈴木 M
セキュリティ	石田 CISO	辻井 D、駒瀬 M
CSIRT	石田 CISO	平山、大和、吉田
GanGan 事業部	田中 CEO	井上 D、野間 D、平山 M
SokoSoko 事業部	高橋 事業部長 (取締役)	森山 D、前川 M
データ保護管理責任者	堀口 DPO	

ネットワーク構成図



▼表D-8 セグメント間の通信

Source Segment		Destination Segment				I. Internet	V. VPN
		S. サーバー	O. オフィス	E. 評価	G. ゲスト		
Source Segment	S. サーバー	○	○	×	×	○	×
	O. オフィス	○	○	×	×	○	×
	E. 評価	×	×	○	×	○	×
	G. ゲスト	×	×	×	×	○	×
	I. Internet	×	×	×	×	○	×
	V. VPN	○	○	○	×	○	×

ネットワークアクセス制御

JNSAアーキテクト社の理解

「仮想企業、JNSAアーキテクト」をよく読み、
インシデント対応の対象となる
企業の情報・状況を理解に努めてください

演習の実施

事件・事故のシナリオを作成し、これをイベントに分解し、イベントに対する対応・対処の机上演習を行います。イベントへの対応は、技術的な判断に偏りがちですが、事業視点、経営視点からの評価・対応を行うようにします。

- 投入される複数のイベントに対して、特定、評価、対応・対処、考査を行い、これをひな型（ステータスレポート）にまとめます。
- 新しいイベントにより、状況が変化した場合は、ステータスレポートを更新します。
- 経営陣などへの報告が必要となったタイミングで、経営者向けの報告書を作成します。



セッション1 端末の ランサムウェア感染

シナリオ

WFH(ワークfromホーム)で業務を行っているPCが、ランサムウェアに感染したシナリオで演習を行います。

このシナリオでは、PC単体の問題であり、事業レベルでの影響よりは、技術的な視点が中心となるかもしれません。

演習にあたっては、判断の根拠を示す視点から取り組むことが重要になります。

このインシデントを起点に、被害が拡大する可能性についても考慮したうえで、経営陣への報告を行ってください。

JNSAアーキテクトのCSIRTに、WFHで業務を行っている社員からおかしな画面が出たとのメールで連絡がありました。画面のハードコピーを送ってもらったところ、ランサムウェアに感染していることがわかりました。



当該社員Aにヒアリングを行った内容は以下の通り

- 2022/07/23 12:17に業務利用のPCにランサムウェアと考えられる脅迫画面が表示された。
- 同日、12:30にCSIRTに連絡を行った
- 在宅で勤務しており、会社とのVPN接続は行ってない
- オンラインストレージと同期をしているフォルダがある
- 電話による連絡は可能と確認できている

1-1 ディスカッション

CSIRTからの報告を受けて、どのような対応を指示または実施しますか？

以下に対応の例を記載しますので、それぞれの項目に対する判断と、その前提条件や考慮すべき点を記載してください。

	対応・対処	判断	前提条件、備考など
1	1 アンチウイルスでフルスキャンを指示する		
	2 PCの電源を落とす、ネットワークケーブルを抜染する		
	3 当該PCの初期化を指示する		
	4 代替えのPCを送付し、感染したPCを回収する		
2	5 主要なシステムで、当該社員のアカウントを無効化する		
3	6 サーバーなどへのアクセスを調査する		
4	7 社員が身代金を支払うことをサポートする		
5	8 情報セキュリティ委員会・経営陣に報告する		
6	9 セキュリティ企業に調査を依頼する		
	10 ランサムウェアの種別を特定する		
	11 侵入経路を特定する		
	12 徹底的に原因を調査する（フォレンジックなど）		

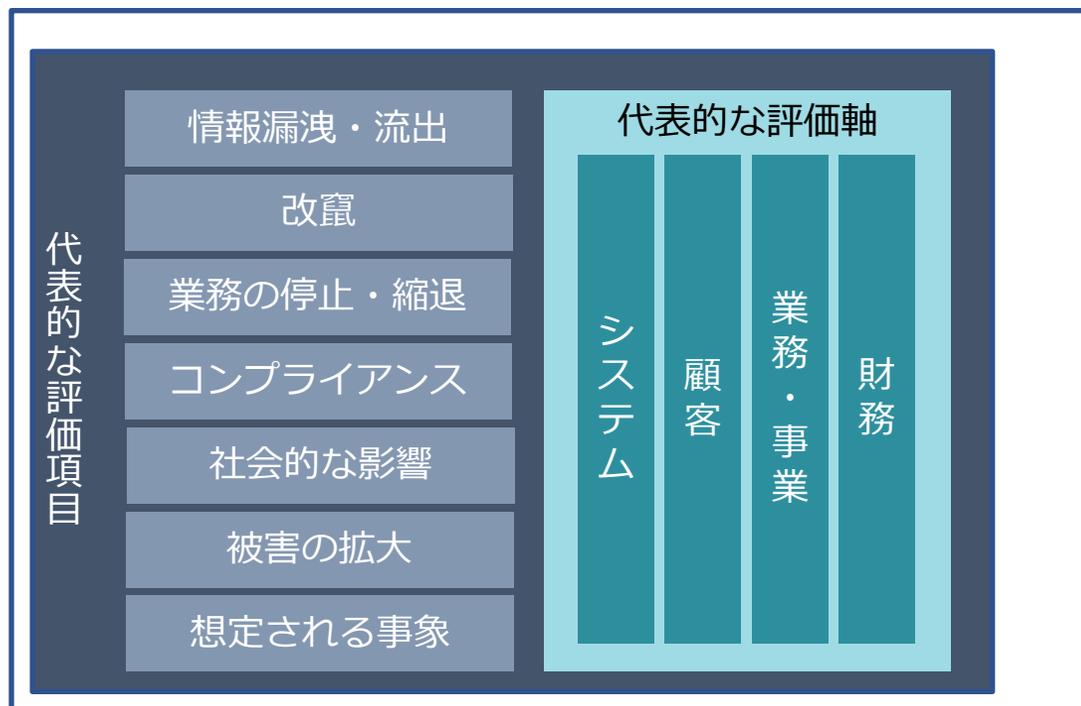
判断：A:すぐやる、B:やるかもしれない、C:この段階ではやらない、D:絶対やらない、E:可能ならやりたい

1-2 ステータスレポートの作成

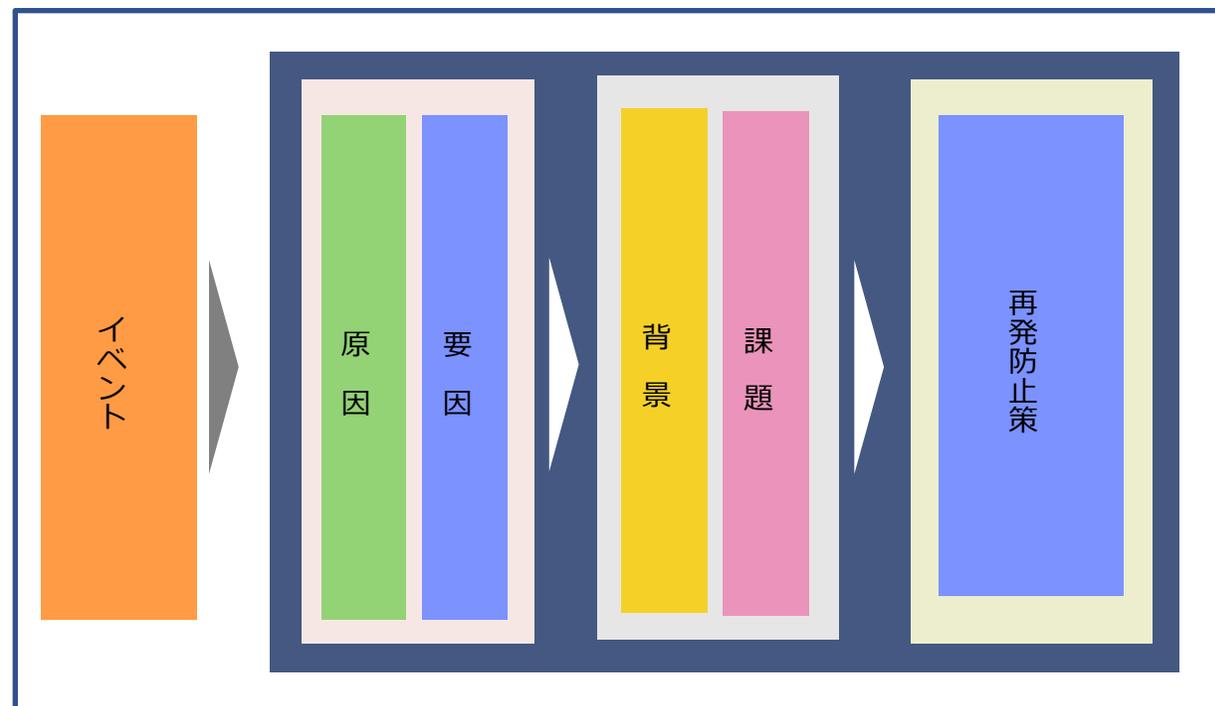
ディスカッションの結果を、「ステータスレポート」にまとめてください。
影響度、深刻度については、「事業視点でのリスク評価項目」に基づいて、顧客、業務、財務の視点から評価し、「原因・要因・背景・課題」を参考に、技術的な原因だけではなく、組織としての背景や課題についても検討してください。

なお、ステータスレポートに正解はありません。各項目を記載するうえで必要な事柄を考慮して作成してください。

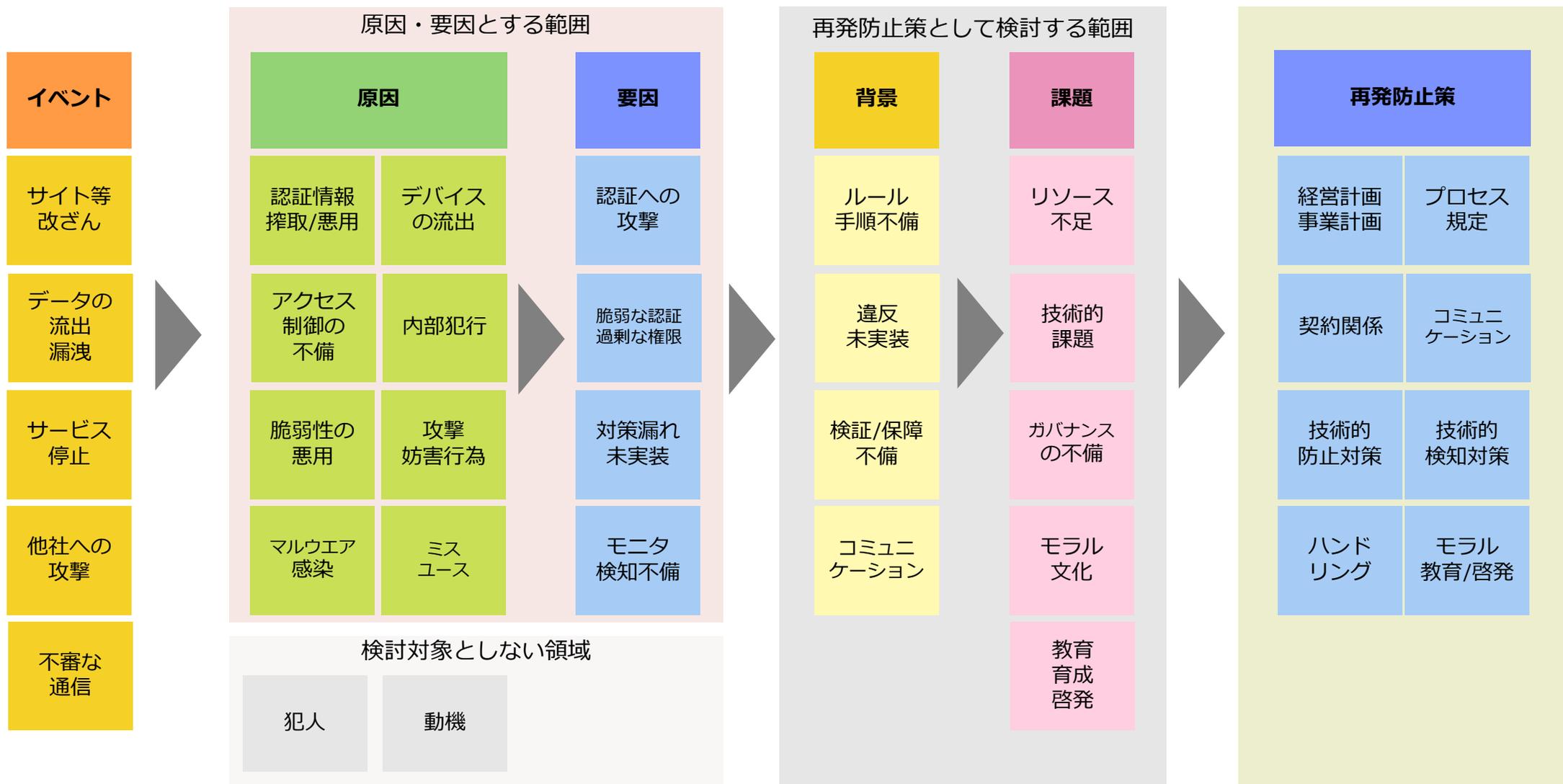
事業視点でのリスク評価項目



原因・要因・背景・課題

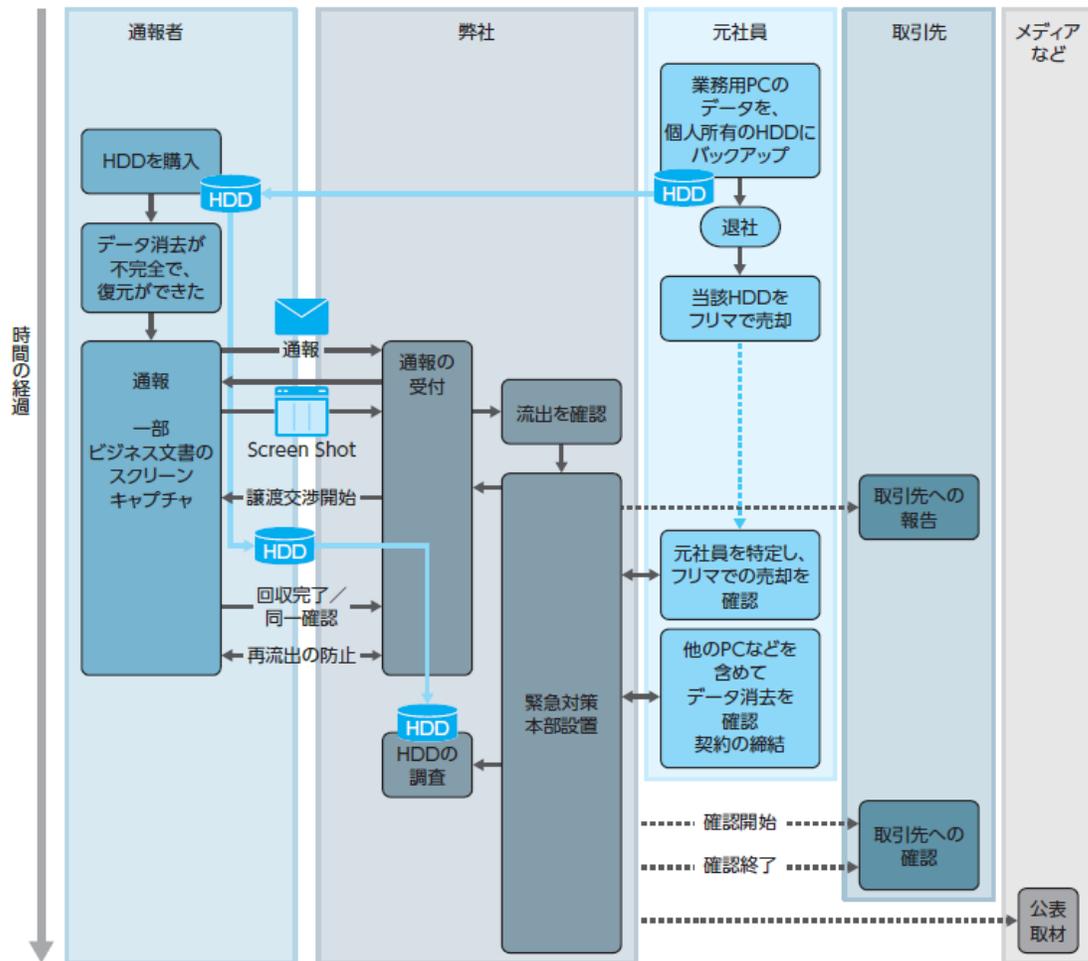


原因・要因・背景・課題・再発防止策



1-3 タイムラインの例 (HDD売却)

▼図C-3 シナリオ2：HDD転売のタイムライン



セッション1-4 CISOから 経営者への報告

インシデントが起きた場合、現状で把握している内容、実施した対処、今後の予定と見込みなどについて、適切なタイミングで経営陣などへの報告が必要です。

ここでは、ステータスレポートとしてまとめた内容に基づいて、経営者への報告を行います。

報告書のひな型を用意してありますが、不足している項目があれば、自由に追加してください。

ひな型の項目

- 対応責任者
- 事件・事故の概要
- 影響を受ける事業
- 顧客や取引先への影響
- 事業への影響
- 財務への影響
- 事件・事故の経緯（タイムライン）
- 責任関係
- 対応の評価

1-4 CISOから経営者への報告例-1

対応責任者			
事件・事故の概要			
影響を受ける事業	事業・インフラなど		
顧客や取引先への影響	影響の概要		
	影響を受ける被害者数と特徴	ワークアラウンド	
	想定される2次被害	被害者への補償	
事業への影響	事業の停止・再開の予定と根拠	事業レベルの対応 (営業停止、継続、縮退など)	
財務への影響	金銭損害、利益損害		
	費用・賠償・制裁金など		
	無形損害・その他		
事件・事故の経緯	事件・事故の原因・要因 (なぜ防げなかったのか)		
	実施した対処		
	対応のタイムライン		
	再発防止策		
責任関係	関係者の処分など		
対応の評価			

ヒント

- ご自身が部下からの報告を受ける視点でレビューしてください
- 経営者が他の経営陣、株主、世間に説明できる内容でしょうか
- 経営者に求めるアクションは明確でしょうか (なにもない、アクション)

セッション2

主要システムの停止 身代金支払いの是非

セッション1が起点となり、経営に対して大きな影響を与えるインシデントに発展しました。

収益を上げているシステムを人質に取られることは、企業にとって大きな問題となり、難しい判断に迫られることとなります。対応や考え方は、企業の状況や当事者の立場によって異なるはずです。

当セッションにおいても、自社のランサムウェア対応を検討する起点となるように、多様な視点を意識しながら議論を進めてください。

- ランサムウェアの攻撃の対応に有効な対策
- 身代金支払いの是非の判断（人にも注目する）
- 支払う際に必要な社内手続
- 顧客、取引先、メディアなどへの対応
- 法執行機関やセキュリティ組織への対応

社員Aの対応を進めているうちに、GanGanゲームサイトの運用担当者から、システムの継続が難しい状況になったとCSIRTの窓口につながりました。クラウド上のサーバーのストレージが暗号化をされ、GanGanのサーバーに以下の内容が表示されたとのことでした。

社員AはGanGanの運用者のひとりであり、GanGanサーバーのアクセス情報を持ってことから、セッション1に関連した攻撃かもしれません。

- ・システムは、ハッカーグループ「Condor」の制御下に置かれている
- ・システムのストレージ上のデータは、「Condor」により暗号化が行われた
- ・暗号を解除するためには、3日以内に2BTC(約600万円)ビットコインで支払う必要がある
- ・テレグラムの連絡先も表記されている

- ・ GanGanシステムが保有する情報
 - アカウント情報 (ID (メールアドレス)、ハッシュ化されたパスワード)
 - GanGan上でユーザーが入力した情報 (チャット、プライベートチャット)
 - クレジットカード情報など
- ・ データベースのストレージも暗号化されたため、データベースもアクセスできません
- ・ サイバー保険には加入していません

- CSIRT
 - 侵入経路
 - ✧ 最初に感染したPCからPC所有者のGanGanシステム管理者としてのSSHの認証鍵を含めた、認証情報を使って侵入が行われた。
 - ✧ このアカウントから横展開をして、GanGanシステムの管理者権限を取得した模様
 - ✧ 現在は、侵入を受けたPCは、初期化しており、このPCから更なる侵害の懸念はないと判断している
 - 脆弱性などの悪用：脆弱性の悪用
 - データ漏洩：データ漏洩の懸念は
 - 運用チーム
 - 状況
 - ✧ 基本的に、GanGanシステムは暗号化されている
 - ✧ GanGanシステムは、完全に暗号化されていない状況
 - ✧ バックアップは、一週間前のバックアップを実施したことはない
 - ✧ GanGanは、他のシステムとは独立したシステム・アカウントで構成をしているため、GanGanを起点に侵害が広がる懸念は少ない
 - ✧ 全てのサーバーは、国内のリージョンを使用している。
 - ✧ 顧客には海外の方も含まれるが、国内向けのサービスであり、特に国外向けの事業は行っていない。
 - システム（プログラム）の1か月前のスナップショット（バックアップ）がある
 - ✧ 決済代行を使っており、この情報からアカウントの復旧が可能（決済のステータスレポートなど、ただし、パスワードは戻らない）
 - ✧ 支払いの記録などは、決済代行業者に記録されている
 - アカウント情報はバックアップがある
 - 開発部の回答
 - ソースコードは復旧が可能
 - ゲームのデータセットは、バックアップがない（キャラクター、画像、ゲームの設定、その他）
 - スクラッチ（=新しいクラウドアカウント）からシステムを構築すると1か月（20人月）かかる
 - ✧ 加えて、動作検証にも1か月程度、セキュリティ検証に2週間（は必要）
- 同じ内容を以下のドキュメントにまとめてあります
03 セッション2 関係者の見解.docx
- 事業責任者
 - 一刻も早く復旧をしてほしい
 - サポート窓口
 - 苦情がたくさん上がっていて、電話回線がパンクしている
 - メールでの対応も追いつかない、何とかしてほしい。
 - 個人情報が大規模に漏洩したとの問い合わせが多数
 - クレジットカード情報が漏えいしたとの問い合わせも多数。
 - 犯人
 - 身代金を払えば、復旧するための情報を確実に提供する犯行グループとの評判
 - 被害者が独自に復旧を試みた場合、復号鍵を使っても復号できない場合があると主張

想定する状況	対応
バックアップが無い場合	<ul style="list-style-type: none"> ● 身代金の支払いを選択しますか ● 選択肢を検討するために、何をしますか、何が必要ですか。
バックアップから復旧が出来る可能性がある 復旧の目途は、5日間と見積もられていますが、これまで、このような復旧を行ったことが無いため、確実に復旧できるわけではありません。	<ul style="list-style-type: none"> ● 指示・報告・届出等がありますか ● 経営陣にはどのように伝えますか ● 顧客にはどのように伝えますか ● 警察には届けます —
復旧が出来ない場合に、身代金を支払いますか 他の事例から、暗号鍵を入手しても復号化に1週間はかかると想定されています	<ul style="list-style-type: none"> ● 支払いますか、支払いませんか、判断と理由を述べてください ● コントクトは行いますか、どのようなコンタクトを行いますか？ ● 指示・報告・届出等がありますか ● 身代金を支払ったことを公表しますか ● メディアから暴露された場合はどのような対応をとりますか
身代金を支払ったが、復旧が出来なかった場合はどのように対応しますか（身代金支払いから1週間経過）	<ul style="list-style-type: none"> ● 指示・報告・届出等がありますか ● どのような対応を行いますか ● 選択肢を検討するために、何をしますか

ヒント

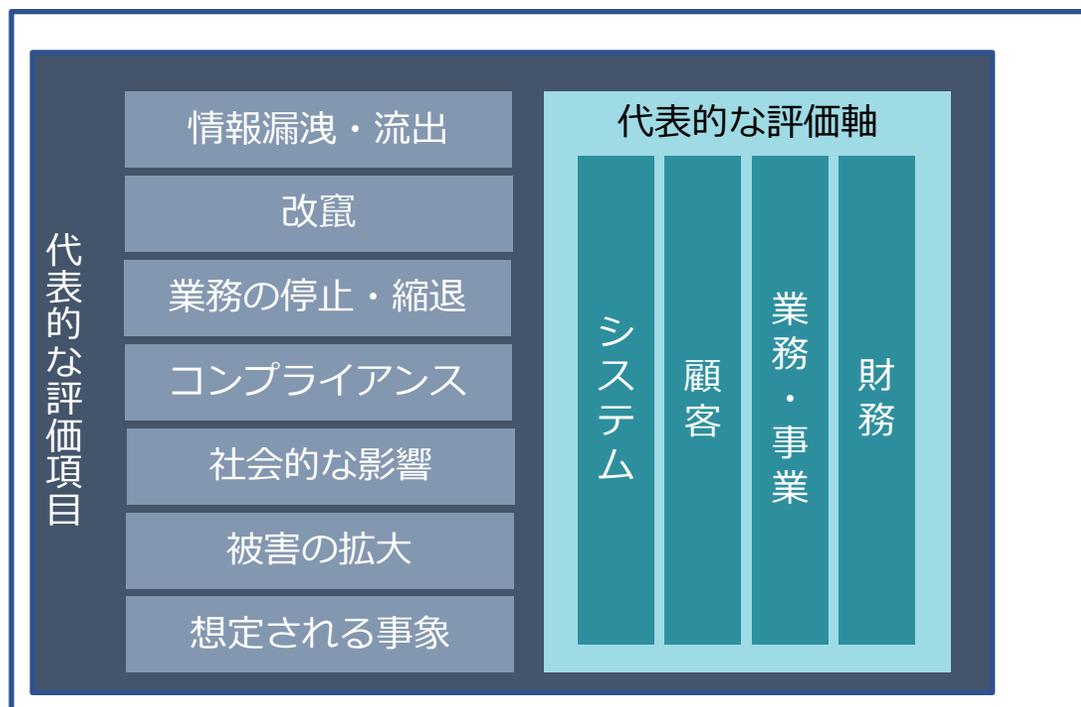
- 判断が顧客や事業にどのような影響があるかを検討しましょう
- RACIを使って、誰にどんなレスポンスビリティがあるかを検討しましょう
- タイムラインを意識して検討しましょう
- 法的な側面、対処が明らかになった（公表した）場合の対応も検討しましょう
- 類似事案ではどうなのか、どのように評価されているかを参考にしましょう

2-2 ステータスレポートの更新

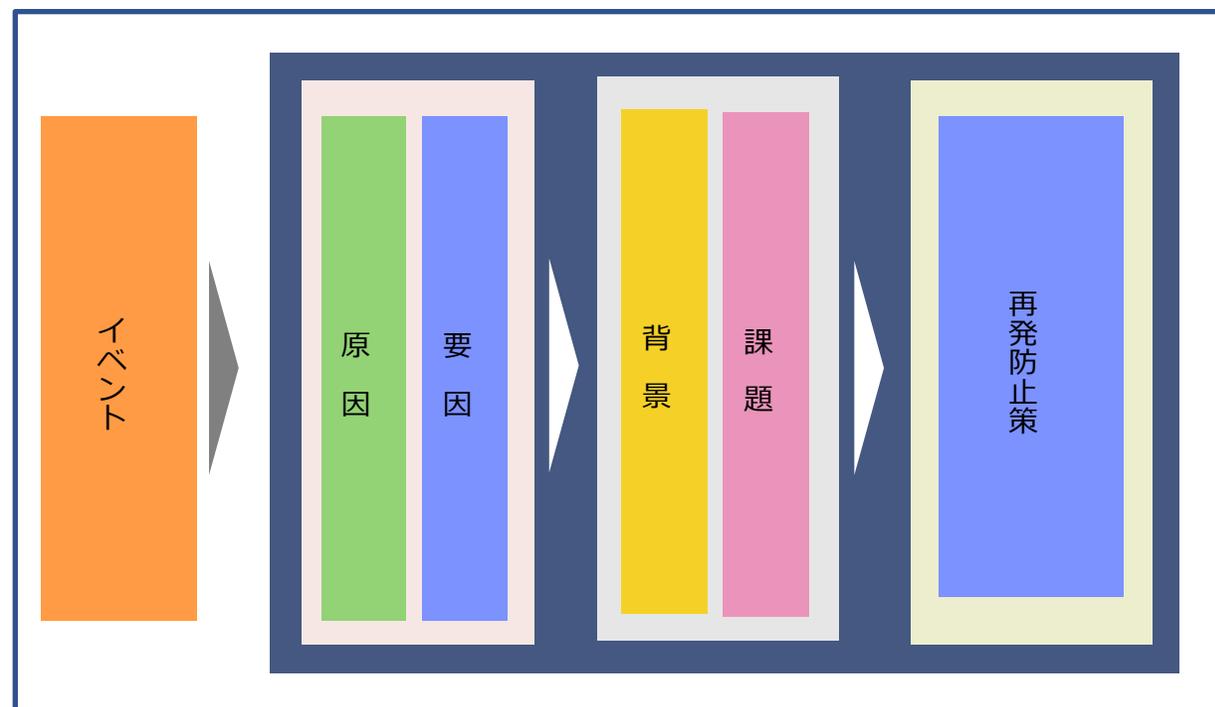
ディスカッションの結果に基づいて、「ステータスレポート」を更新してください。
影響度、深刻度については、「事業視点でのリスク評価項目」に基づいて、顧客、業務、財務の視点から評価してください。

「原因・要因・背景・課題」を参考に、技術的な原因だけではなく、組織としての背景や課題についても検討してください。

事業視点でのリスク評価項目



原因・要因・背景・課題



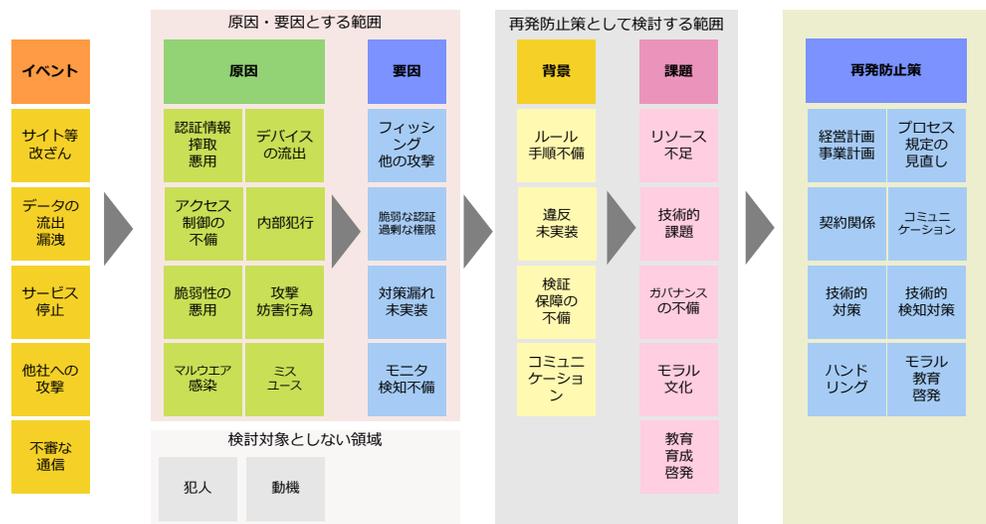
2-3

原因・要因・背景・課題 再発防止策

再発防止策を検討するために、原因・要因・背景・課題について検討してください。

CISO-PRACTSIEでは、原因・要因・背景・課題を以下のように定義しています。

- イベント：
 - 例：サイトの改ざん
- 原因：事件・事故につながった直接的な原因
 - 例：認証情報の悪用
- 要因：原因につながった要因
 - 例：脆弱な認証システム
- 背景：要因の背景となった習慣・文化・手続き
 - ルール違反・未実装
- 課題
 - リソース不足
- 再発防止策
 - 原因・要因・背景・課題を視野に入れて、これらを解決し、再発を防止するための施策をまとめます。



2-3 ディスカッション-3

調査の結果、やはり、運用担当者のPCがあランサムウェアに感染した際に、アクセストークンとアクセスに必要な情報を搾取されたことで、GanGanシステムのアクセス権が奪われたことがわかりました。

(MFAの有無を確認する)

原因・要因・背景・課題の視点から分析を行い、再発防止策を提案してください。

原因		
要因		
背景		
課題		
再発防止策		

セッション3 模擬的な公表

ここまでの内容に基づいて、模擬的な記者会見を行います。報告書をまとめるだけでは、自社の理屈に留まり、社会的に許容できない内容になりがちです。

本セッションでは、模擬的な記者会見を行うことで、事件・事故を自身の問題として捉え、透明性を持った説明責任が果たすことを目指します。

経営者の参加を得ることが望まれますが、本ワークショップでは、参加者が経営者の立場から、模擬記者会見を行うようにしてください。

この作業を通じて、経営者がセキュリティ対策の必要性や合理性について知見を深めること、経営者の視点からセキュリティ施策を評価・考察する機会を得ることが期待できます。

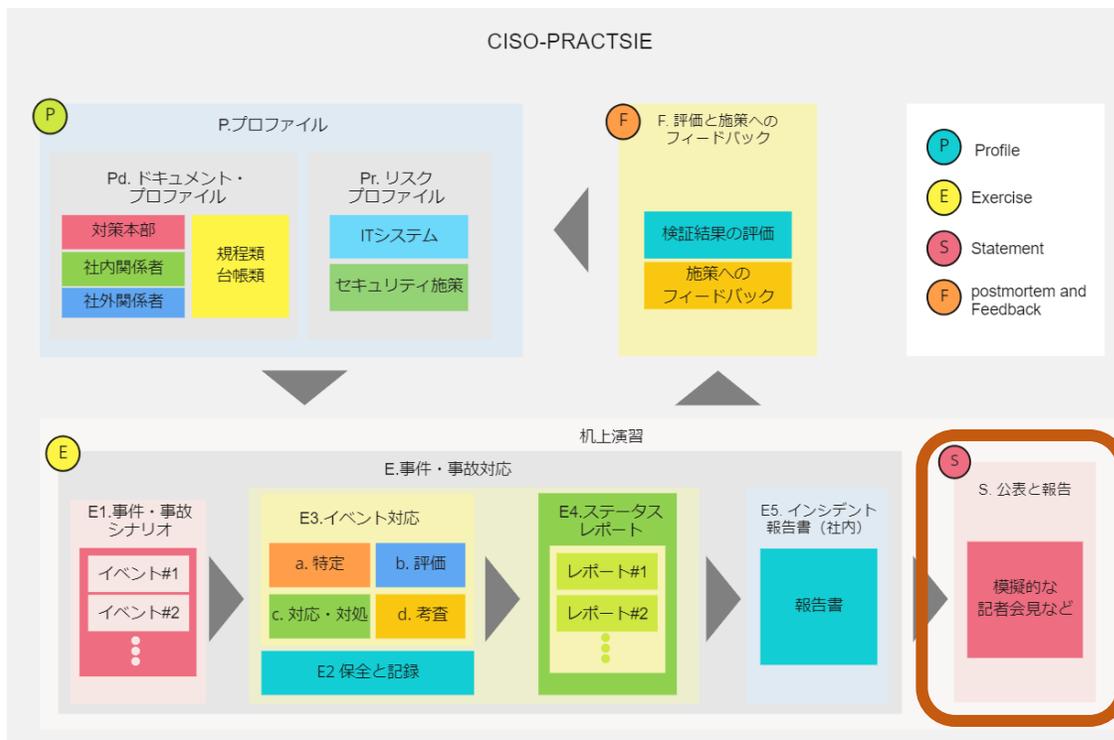
- 公表必要性の判断
- ポジションペーパー
- ステートメント・Q&A集
- 模擬記者会見の実施

模擬的な公表の位置づけ

- 当事者として事案を評価する
- 当事者と世間のギャップを認識する
- 公表・報告・届出が必要な相手を確認する
- 公表が必要な内容を確認し、公表が可能かを確認する
- 再発防止策として現状の課題を明らかにする

セキュリティ事件・事故のケース

- 標的型攻撃で機密情報が漏れた可能性
- ハッカーの侵入を受けて、すべてのメールがインターネットに公開された
- WEBページから顧客情報が閲覧可能な状態
- 弊社にしか登録をしていない「メールアドレスに広告が入った」とのクレーム
- 顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」
- インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている
- 弊社が所有するIPアドレスから攻撃を受けているとのクレームが入った
- 弊社のメールアカウントを使った、標的メールが取引先に送信された



公表内容：ポジションペーパー

影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される2次被害
事業への影響	ワークアラウンド (被害の軽減策)
	被害者への補償
	事業の停止・再開の予定と根拠
事件・事故の経緯	事業レベルの対応 (営業停止、継続、縮退など)
	事件・事故の原因・要因 (なぜ防げなかったのか)
再発防止策	対応のタイムライン (経営者が認識したタイミング)
	再発防止策の内容と実施時期
責任関係	関係者の処分など

3-1 模擬記者会見の準備

セキュリティ事件・事故が起きた場合、必ずしも公表が望ましい結果を招くとは限りません。一方で、公表を行わなかった場合、企業責任が厳しく問われる可能性もあります。ここでは、模擬記者会見の準備として、公表の必要性を判断し、公表する内容をポジションペーパーとしてまとめ、公表資料としてステートメント・Q&A集などを作成してください。また、記者役の質問項目についても、まとめるようにしてください。

- 公表必要性の判断
- ポジションペーパー
- ステートメント・Q&A集

- 記者役の質問項目

今回のワークショップは、短時間で行うため、ポジションペーパーとステートメントは、並行して作成するのが良いかもしれません。

3-1 公表の判断（今回は公表が前提）

システムが止まっていることについて、メディアからの問い合わせが増えています。
まだ、解決には至っていない状況での、記者会見や事案の公表について議論してください。
議論の結論に関わらず、記者会見を実施するものとして、記者会見の準備を行い、模擬記者会見を実施してください。

公表の必要性

- 被害者の財産、身体などに影響がある
- 被害者が特定できないか、多数に及ぶため個別の連絡が難しい
- 事業や顧客への深刻な影響がある
- 危機の継続や二次被害の可能性がある
- 顧客や行政への報告義務や道義的な責任がある
- 誤った風評が流れている
- すでに報道されているか、複数のメディアから取材申し込みがある
- 経営幹部や組織ぐるみの違法行為がある

公表を配慮するケース

- 被害者に直接連絡が可能な状況
全ての被害者に連絡が取れていれば必ずしも公表の必要はない
- 利害関係者への通知が済んでいない状況
取引先に二次的な被害が想定される場合
- 公表により被害が拡大・深刻化する可能性がある状況
攻撃手法の公開や、漏洩情報の拡散につながる場合
- 取引先や被害者（企業）の株価などへの影響が懸念される状況

公表の判断

- 実施する / 実施しない
- 判断の理由・根拠

公表のタイミング

- タイミング
- 判断の理由・根拠

3-2 ポジションペーパー

	項目	内容
影響を受ける事業	事業の概要	
顧客や取引先への影響	影響や被害の概要	
	影響を受ける被害者数と特徴	
	想定される2次被害 (これから起きるかもしれない事)	
	ワークアラウンド (被害の軽減策)	
	被害者への対応と補償	
	問合せ窓口など	
事業への影響	事業の停止・再開の予定と根拠	
	事業レベルの対応 (営業停止、継続、縮退など)	
事件・事故の経緯	事件・事故の原因・要因 (なぜ防げなかったのか)	
	対応のタイムライン (経営者が認識したタイミングを含む)	
再発防止策	再発防止策の内容と実施時期	
責任関係	関係者の処分など	

3-3 ステートメント

項目	留意点	内容
事実・内容 (事故、事件)	誰が、いつ、どこで、なにをしたのかを 5 W1Hの形で簡潔に記載	
経過	発生から現在に至るまでの経過を日時、時間単位で箇 条書きにする 経過の結果、現在の状況説明を加える	
原因	憶測事項は書かない	
対策	対策が策定できていない場合は、「いつまでに対策を 発表する」かを記載した方がよい	
見解 (結論)	事件・事故について会社としてどう思うか どのように結論付けるのか どう責任を取るのか	

3-4 模擬記者会見のルール

ルール	適切な役職、立場	担当者
スポークスパーソン	経営者、事業責任者	
司会役	広報担当者等	
記者役	記者、ITを担当しない方 複数のグループがある場合は、他のグループ 1グループの場合は、上記以外のメンバー	

3-5 記者役の質問の例

質問の論点	質問内容
タイムラインに関する質問	
顧客の被害、影響に関する質問	
被害への補償、対応、窓口など	
事業への影響に関する質問	
対策の内容に関する質問	
再発防止策に関する質問	
責任の所在と処分に関する質問	
その他	

3-2-a 経営者から 公表内容の了承を得る (セキュリティ担当者向け)

アジェンダ

予定される公表内容を、経営者に説明し、了承を得てください。

公表先は必ずしも記者会見に限りません。

ホームページやSNSで公表する場合も、内容について経営者の了承を得る必要があります。

発表のスク립ト（文面）は、了承を得たのちに広報と作成することとします。

全般的な留意点

- ・ 報告ではなく、了承・承認を得ることが目的であることを踏まえて、説明を組み立ててください。
- ・ 公表が必要な理由、不必要な理由を述べてください
- ・ 経営者に何をしたいか、何を判断して欲しいかをはっきりとさせてください
- ・ 費用の発生が見込まれる場合は、予算の承諾・承認を得てください
- ・ 事実（エビデンスがあること）と、推測を区別して伝えてください
- ・ 必須なこと（義務）と望ましいことを、区別して伝えてください。

3-2-b 模擬記者会見の実施

(CISO向け)

アジェンダ

- 1 司会者による呼び込み
- 2 登壇者の記者会見場への入場
- 3 冒頭のステートメント発表
- 4 質疑応答
- 5 登壇者の退場

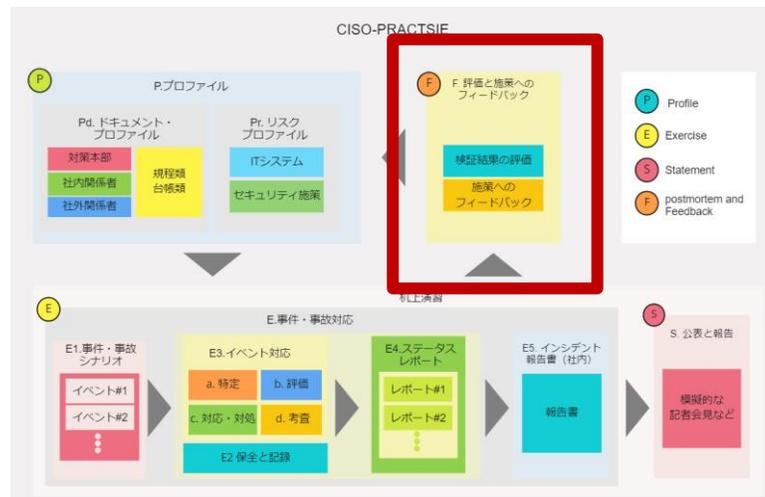
全般的な留意点

- ・ 誰が被害者で、何を守るかを明確にする
- ・ Q&A 集は必ず目を通す
- ・ 棒読みをせず自身の言葉で表明する
- ・ 専門用語は極力避ける
- ・ 挑発的な質問に対しても冷静に誠意を持って対応する
- ・ 質問は最後まで聞く
- ・ 正確かつ簡潔に説明し、含みを持たせる言い方をしない
- ・ 憶測や仮定の話はしない
- ・ 自己弁護に終始しない
- ・ 質問が途切れるまで記者会見を続ける
(身だしなみにも気を付ける)

セッション4 ポストモーテム

ここまでの作業を振り返り、伸ばすべき点、改善すべき点などをまとめてください。

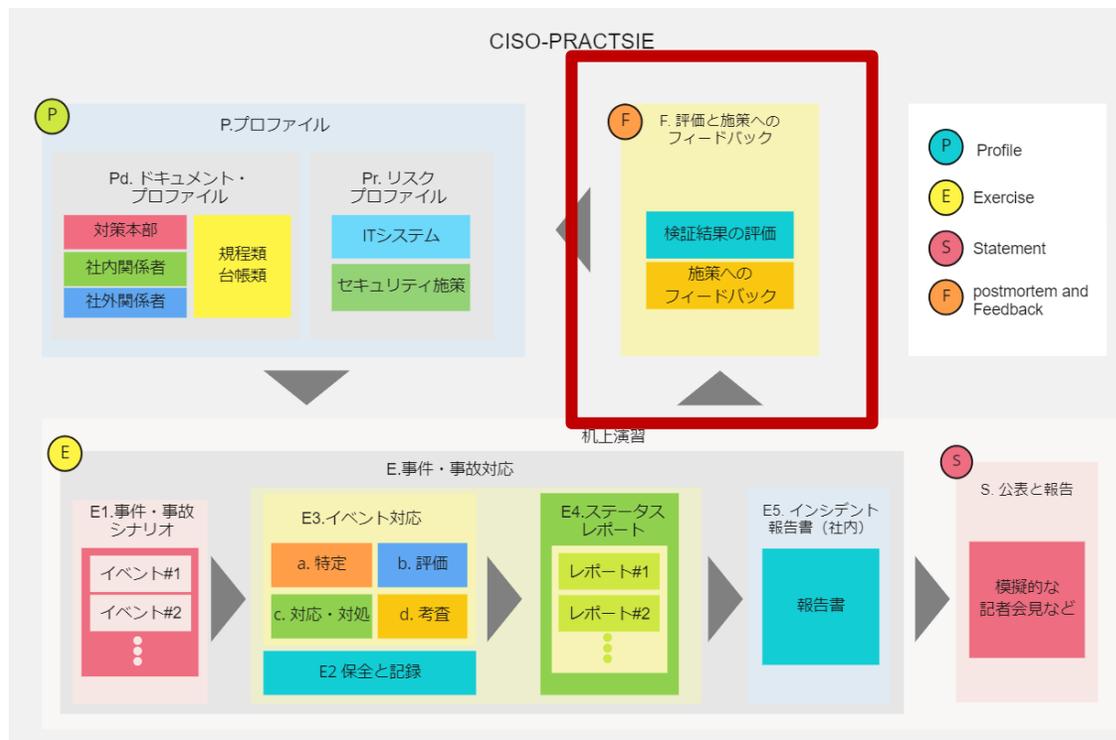
また、ワークショップでは難しいかもしれませんが、社内外のコミュニケーション基盤を維持するための施策についての考察してください。



- 演習の成果を確認する
- 再発防止策から改善計画を策定する
- 計画の実施状況を追跡する
- コミュニケーションチャネルを維持する

セキュリティ事件・事故のケース

- 標的型攻撃で機密情報が漏れた可能性
- ハッカーの侵入を受けて、すべてのメールがインターネットに公開された
- WEBページから顧客情報が閲覧可能な状態
- 弊社にしか登録をしていない「メールアドレスに広告が入った」とのクレーム
- 顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」
- インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている
- 弊社が所有するIPアドレスから攻撃を受けているとのクレームが入った
- 弊社のメールアカウントを使った、標的メールが取引先に送信された



公表内容：ポジションペーパー

影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される2次被害
事業への影響	ワークアラウンド (被害の軽減策)
	被害者への補償
	事業の停止・再開の予定と根拠
事件・事故の経緯	事業レベルの対応 (営業停止、継続、縮退など)
	事件・事故の原因・要因 (なぜ防げなかったのか)
再発防止策	対応のタイムライン (経営者が認識したタイミング)
責任関係	再発防止策の内容と実施時期
	関係者の処分など

設問4：ラップアップ

検討項目	参加者からのコメントなど
学んだ点、参考になった点がありますか	
JNSA アーキテクトが事前に準備すべきだった点がありますか (やっておけばよかったこと)	
ワークショップで改善すべき点を挙げてください	
自社にフィードバックしたい点を挙げてください	
その他	

むすび

セキュリティ施策をデバッグしよう！

まずはひとりで

STEP1：手元にある資料をプロファイルする

STEP2：不足している情報や資料の収集を試みる

STEP3：シナリオに基づいて対策を評価する

少しずつ参加者を増やして

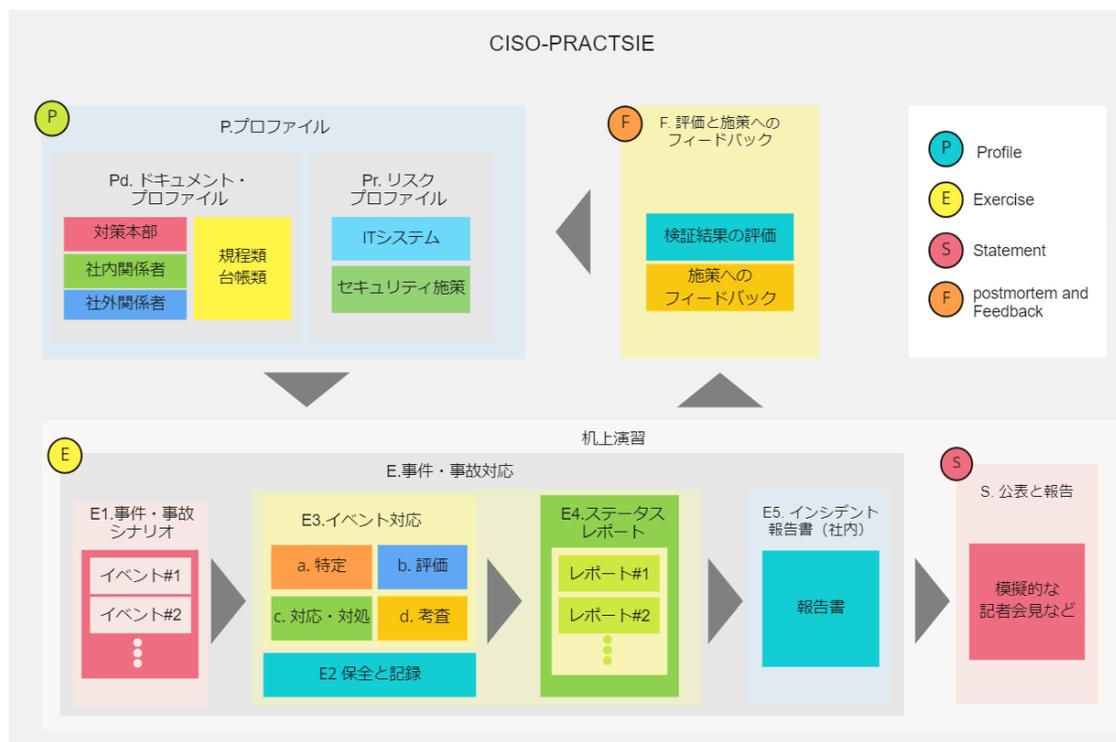
STEP4：少人数で演習を実施する

STEP5：関係者を増やして演習を実施する

STEP6：定期的に演習を実施する

セキュリティ事件・事故のケース

- 標的型攻撃で機密情報が漏れた可能性
- ハッカーの侵入を受けて、すべてのメールがインターネットに公開された
- WEBページから顧客情報が閲覧可能な状態
- 弊社にしか登録をしていない「メールアドレスに広告が入った」とのクレーム
- 顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」
- インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている
- 弊社が所有するIPアドレスから攻撃を受けているとのクレームが入った
- 弊社のメールアカウントを使った、標的メールが取引先に送信された



公表内容：ポジションペーパー

影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される2次被害
事業への影響	ワークアラウンド (被害の軽減策)
	被害者への補償
事件・事故の経緯	事業の停止・再開の予定と根拠
	事業レベルの対応 (営業停止、継続、縮退など)
再発防止策	事件・事故の原因・要因 (なぜ防げなかったのか)
	対応のタイムライン (経営者が認識したタイミング)
責任関係	再発防止策の内容と実施時期
	関係者の処分など

An aerial, high-angle view of a dense city skyline, likely New York City, with the Empire State Building prominently visible in the center. The image is overlaid with a semi-transparent blue filter. The text "Thank you" is centered in a large, white, sans-serif font.

Thank you