CISOハンドブック
ワークショップから見えてきた
セキュリティ界隈の傾向と課題

JNSA CISO支援ワーキンググループ　WGリーダー
（株）Preferred Networks VP 最高セキュリティ責任者
高橋　正和

略歴

1980年代-1999年：ソフトウェア開発、開発環境
「事前の言い訳としてのセキュリティ」

ソフトウェア開発、品質管理
米国ブランチ

JNSA

1999年 – 2006年　：Internet Security Systems(ISS)
「合理的で再現可能な工学的セキュリティ」

技術マネージャ、事業立上げ
CIO、CTO

Dynamic Defense WG

2006年 - 2010年：マイクロソフト
「製品品質としてのセキュリティ」

2010年 – 2013年：マイクロソフト
「サイバー攻撃対応としてのセキュリティ」

2014年 – 2017年：マイクロソフト
「クラウドとIDベースのセキュリティ」
「業務執行としてのセキュリティ」の模索

CSA（Chief Security Advisor)

脆弱性や事件・事故のメディア対応
（定例更新の定例記者説明会）
技術や戦略のスポークスパーソン
SDL: Security Development Lifecycle
サイバー犯罪対策の国際連携
　ボットネット Takedown

CISOハンドブック v1.1β（Web版）

副会長
理事・幹事

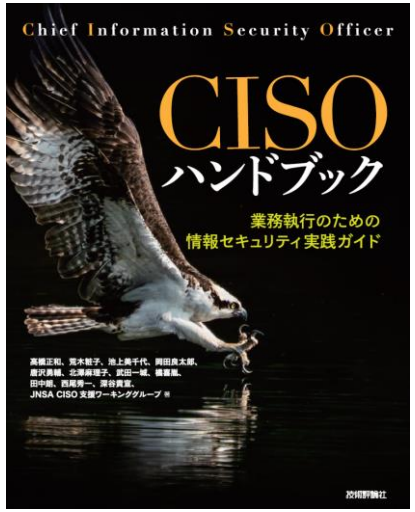
CISO支援WG

2017年 – ：Preferred Networks
「業務執行としてのセキュリティ」の実践

CSO（Chief Security Officer)

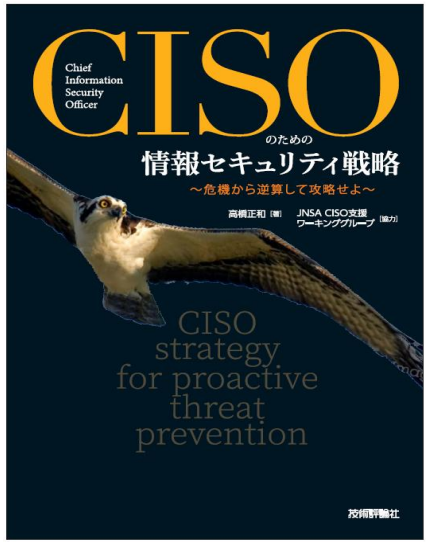
CISOハンドブック
CISOのための情報セキュリティ戦略

業務執行としての情報セキュリティ



CISOハンドブック
―業務執行のための
情報セキュリティ実践ガイド
著作： JNSA CISO支援
ワーキンググループ

出版社：技術評論社
発売日：2021/1/20
単行本（ソフトカバー）：400ページ
ISBN-13：978-4297118358



CISOのための情報セキュリティ戦略
～危機から逆算して攻略せよ～
高橋 正和（著）
JNSA CISO支援ワーキンググループ（協力）

出版社：技術評論社
発売日：2023/1/21
単行本（ソフトカバー）：200ページ
ISBN978-4-297-13294-1 C3055

事業責任者の立場になってみると
業務執行に関する資料が見つからない
- 経営の書籍≒経営者の成功物語かMethod（手法）
- マネジメントの書籍≒庶務管理
- 業務を執行する当事者目線の資料がない

ハンドブックは悪くないが実務への展開が難しい
by WGメンバー
ハンドブックを補完する内容として目指したこと
- 網羅性から、具体的なシナリオへ
- 計画の策定から、計画の検証とコミュニケーションへ
- わかるから、出来るへ

机上演習を使った社内横断的評価と検証のアプローチ

CISOのための情報セキュリティ戦略

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

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で、
経営者とセキュリティ専門家の「ギャップ」を「共通の課題」と出来るのではないか。

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、セキュリティを共通の課題とすることが重要となる

CISO-PRACTSIE(ワークショップ)の概要

財務的な目標ではなく、
合理的な公表内容を目標とする

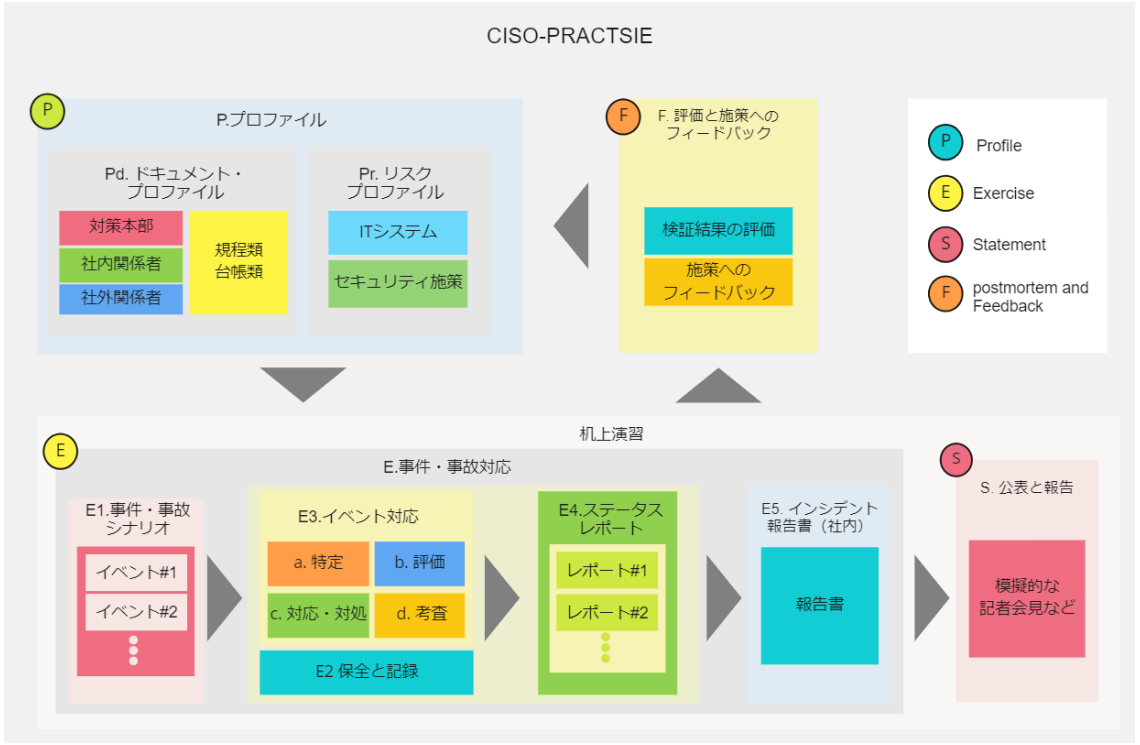
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

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

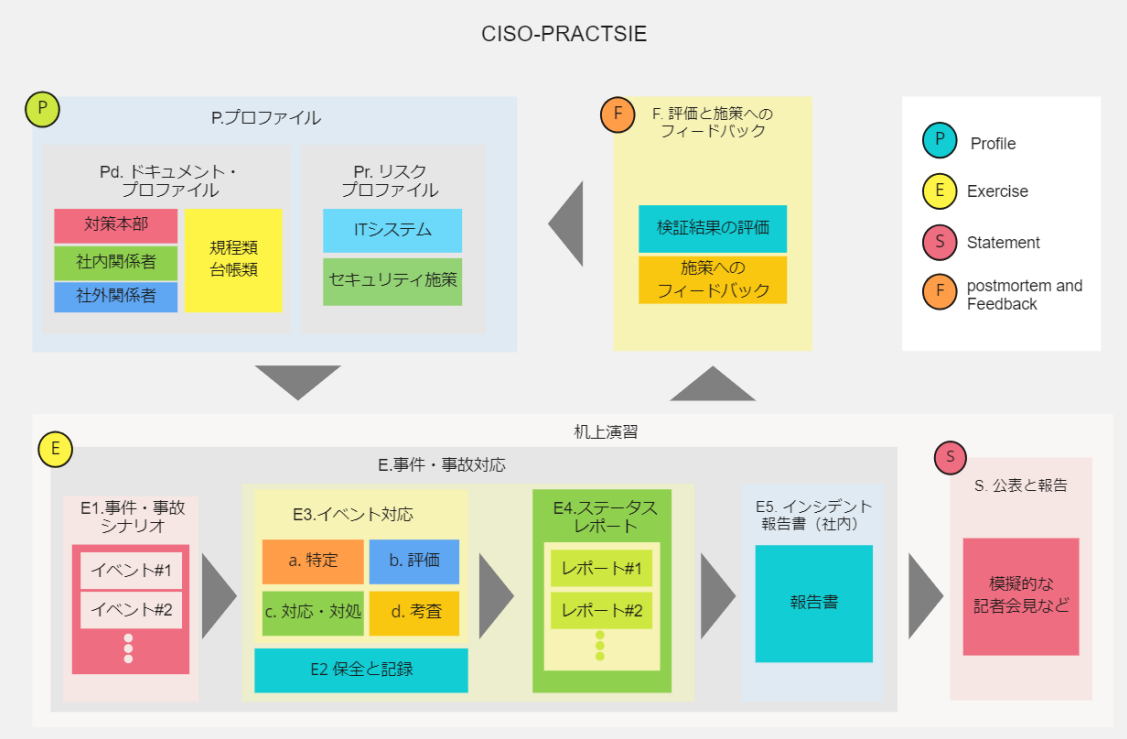


OUTPUT

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
	ワークアラウンド（被害の軽減策）
	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）
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）
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

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

CISO-PRACTSIEの構成



- P：プロファイル：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

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

基本的なアジェンダ

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：ランサムウエア-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：ランサムウエア-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)

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

ワークショップ開催実績

- 2023/04/15 WGメンバー向け　ワークショップ
  - WGメンバー７名（くらい…）
  - ディテールの議論に時間がかかった（10分予定のディスカッションに1.5時間）
  - 経営者への報告は、現役CISOが担当したので、概ね期待した内容
  - 模擬記者会見は時間切れで実施できなかった

- 2023/04/xx CISO向け　ショートワークショップ（非公開）
  - 約30名のCISOおよびCISO的な業務を行っている方
  - 概ね期待した内容で少し驚く
  - 事業を背景としたコメントが多く、様々な視点と企業の文化・哲学を知ることができた

- 2023/04/27 JNSA会員向けワークショップ
  - 申し込み7名＋WGメンバー4名+1
  - 当然ながら、提供者側からセキュリティにかかわっている方が中心
  - 残念ながら期待した内容にはならなかった…

参加者からのフィードバック

セッション 4

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、参考になった点はありますか	• フォーマットが参考になった • 「原因・要因・背景・課題」に対する腹落ち感があった • エビデンスがないと答えにくい。（質問されても）回答の仕方が異なる。 • 今これをやったら将来どういう影響があるかなど、長期的視野が必要と感じた。 • （経営者に）助けてもらう、相談するという視点は無かった。 • 世の中の動向やトレンドを掴んでおかないと、経営者に提案ができない 身代金の支払も、動向を知らないと経営者に説明（説得）できない。 • ワークショップの振り返りとして、ラップアップを丁寧にして欲しい • 広報や法務などのステークホルダーを巻き込む必要がある • CISOを育成する視点が欲しい • CISO検定があったら受けてみたい
JNSA アーキテクトが事前に準備すべきだった点はありますか （やっとけばよかったこと）	
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	

「現役CISO」と「セキュリティ専門家」に大きな「ギャップ」があった。
まず、ワークショップの概要を紹介し、この「ギャップ」について考察する。

CISO-PRACTSIE

机上演習による
セキュリティ施策の評価

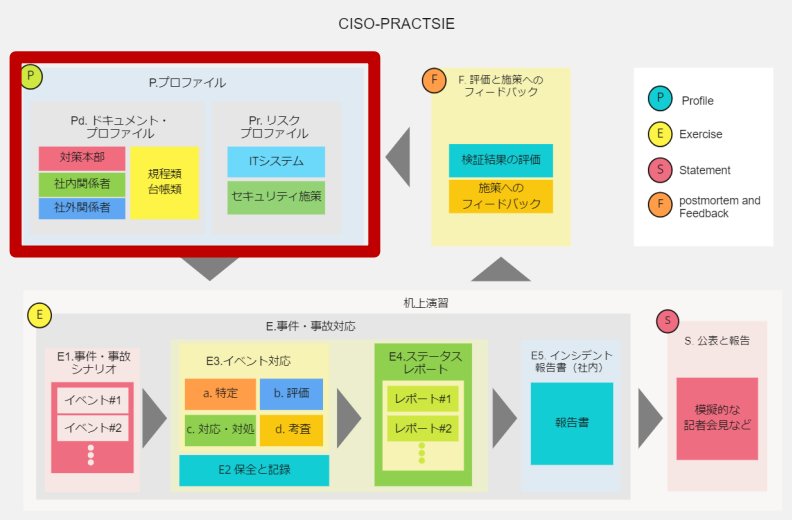
CISO-PRACTISE　ワークショップの目的とゴール

- CISO-PRACTISE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。

プロファイル



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。

サンプル会社：JNSAアーキテクト

会社概要

▼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
	髙橋 正和
社外取締役	本川 祐治
	林 佳子
（監査等委員）	土井 充

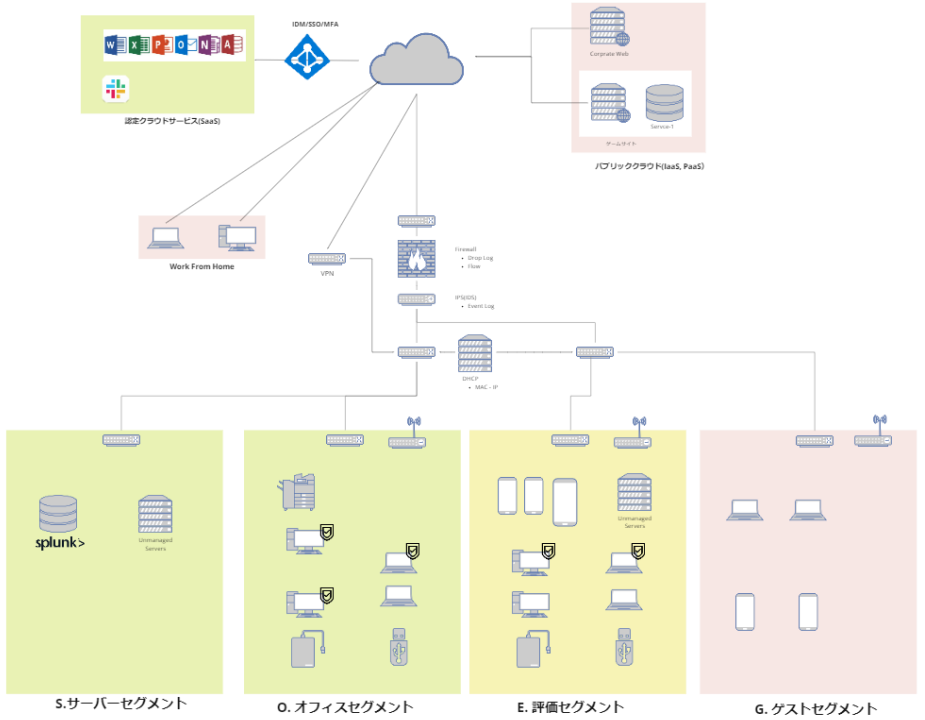
組織構成

▼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

ネットワーク構成図



ネットワーク
アクセス制御

▼表D-8　セグメント間の通信

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

規程類・手順のプロファイル

規定類

▼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
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

関係者とコンタクト方法

▼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	
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、チャネル名など	秘書を通は読まない、休日は反応がない など、コミュニケーションのお作法

▼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

技術資料

▼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

システム一覧

▼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
基本的なITインフラ	認証システム	・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	
	求人関係	
社内システム	ERP、決済システム	
	給与明細・源泉徴収	
	電子契約システム	
	その他	
システム開発環境	GitHub	

アカウントと特権

▼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

出典：CISOのための情報セキュリティ戦略

リスク・プロファイル

事業レベルのリスク評価

システムレベルのリスク評価

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 顧客業務	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			
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			

▼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 特定の日時にリカバーできる
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

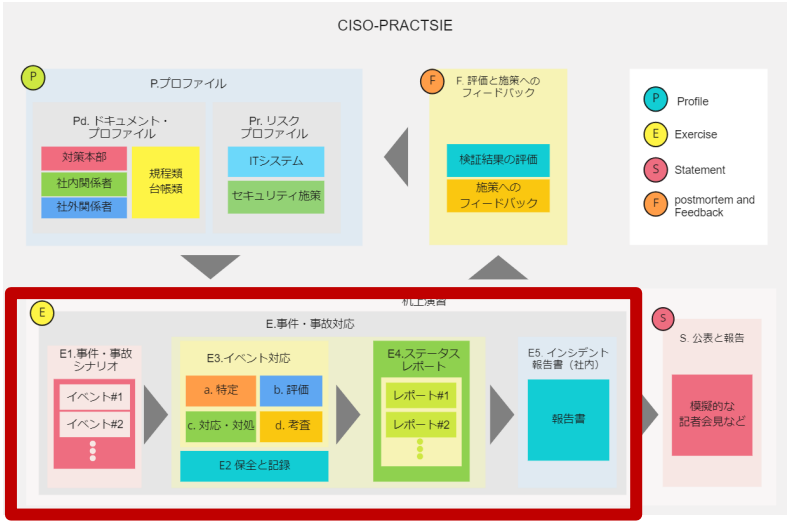
▼表3-10　評価対象事業・システムのプロファイル例（暗号資産取扱事業者）

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	暗号資産の売買代行システム ・主要な収益は手数料 ・評価差額は持たない
	事業責任者	役職と氏名を記載する	担当執行役員：北澤常務
	運用責任者・担当者	特に責任者は、役職と氏名を記載する	システム側：後藤システム部長 システム運用グループ（秋葉M） ビジネス側：本庄企画部長 コンシューマビジネス企画室（伊藤D）
	開発責任者・担当者	特に責任者は役職と氏名を記載する	システム：後藤システム部長 システム開発グループ（垣内M） ビジネス開発は考えなくてよい
	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	150万人
	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	年間　売上取扱高　１千億円 利益　600億円
	ユーザーの居住地域 サービス提供地域 日本、EU、US、CH、KOなど	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	日本国籍および国内居住者（金融庁免許）
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	インシデントが報告される可能性のある連絡窓口を記載する	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	■個人情報　□仮名個人情報　■金融関連情報　□その他の機微情報
	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	自社が保管している暗号資産が盗まれる可能性がある 顧客資産はオフラインになっているので、盗難の可能性は低いが、暗号鍵が盗まれた場合は、この限りではない
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	明確なSLAはない
	自社への影響	業務の停止・遅延、決済の停止などの影響	売上機会の損失 ユーザーが他社に逃げる可能性 システム停止中の価格変動に対する訴訟の可能性 金融監督庁からの業務停止命令など

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
ランサムウエア感染

シナリオ

WFH(ワークフロムホーム）で業務を行っているPCが、ランサムウエ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。

セッション１：ランサムウエアの感染

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、ランサムウエ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にランサムウエ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接続は行っていない
- オンラインストレージと同期をしているフォルダーがある
- 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

セッション 1

原因究明 VS 拡大防止

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	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		
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		
6	サーバーなどへのアクセスを調査する		
7	社員が身代金を支払うことをサポートする		
8	情報セキュリティ委員会・経営陣に報告する		
9	セキュリティ企業に調査を依頼する		
10	ランサムウエ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）		

1 2 3 4 5 6

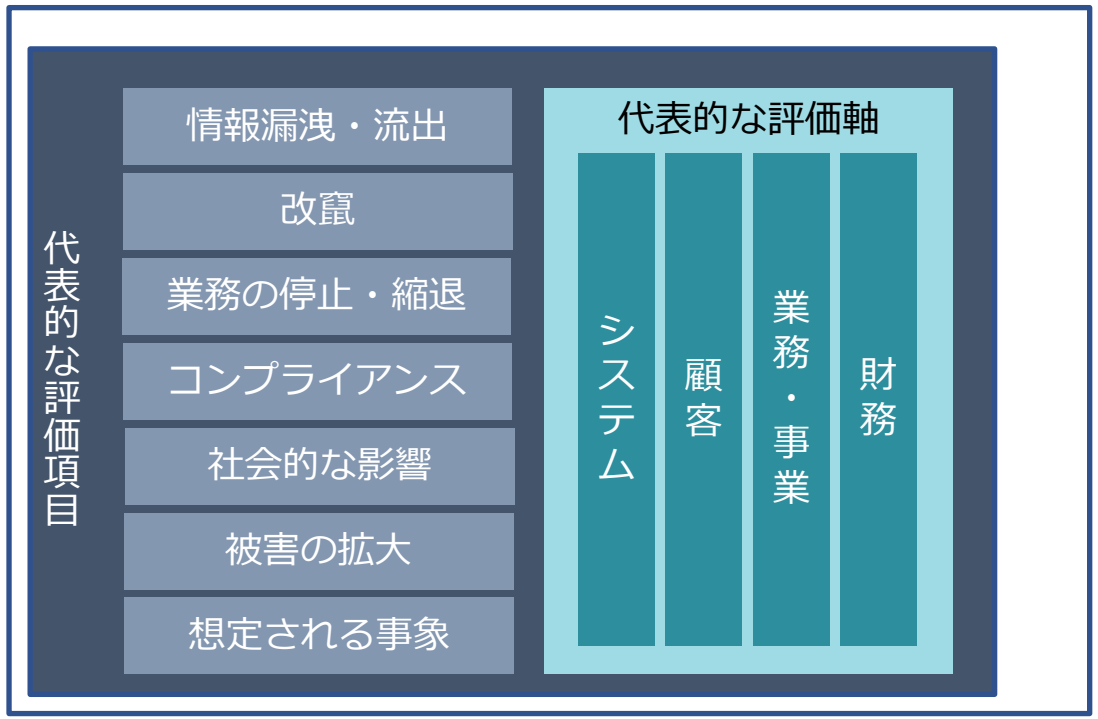
判断：A:すぐやる、B:やるかもしれない、C：この段階ではやらない、D:絶対やらない、E：可能ならやりたい

1-2 ステータスレポートの作成

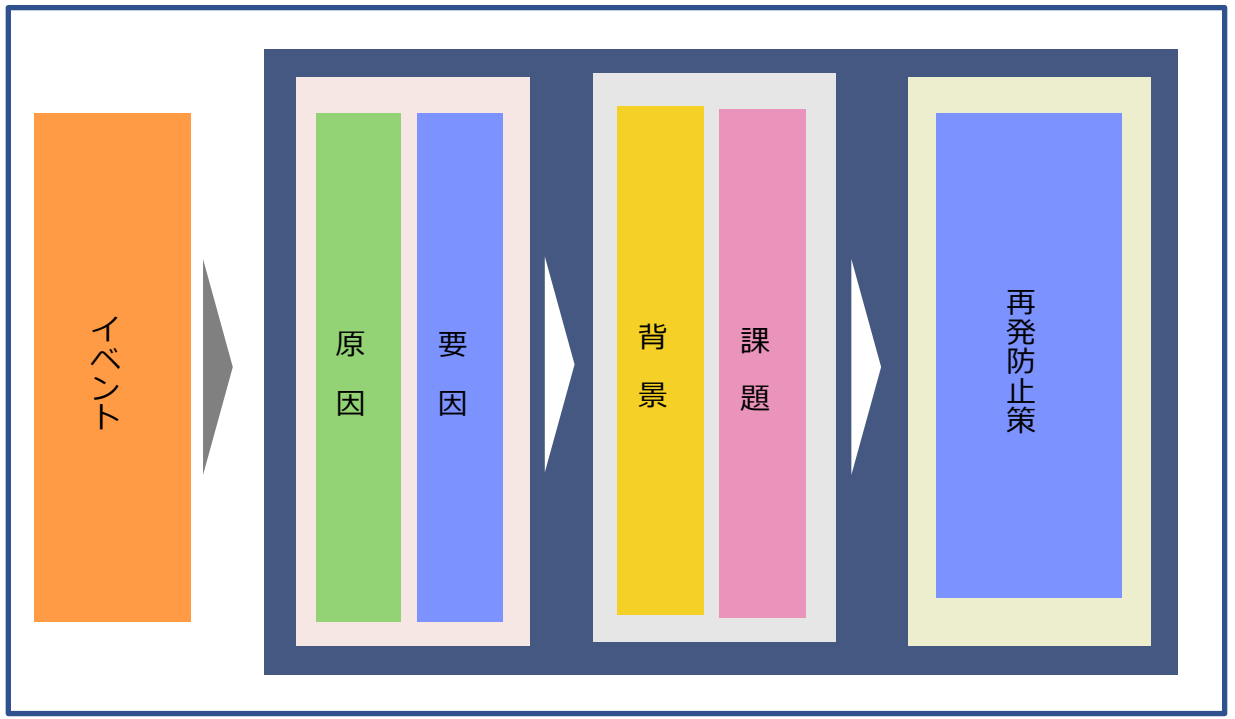
セッション1

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



1-4 CISOから経営者への報告例-1

セッション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				

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になります。
対応や考え方は、企業の状況や当事者の立場にによって異なるはずです。
当セッションにおいても、自社のランサムウエ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。

- ランサムウエ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

セッション２：システム停止と身代金の要求

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の窓口に連絡が入りました。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す。
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

セッション２：関係者の見解

- 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：脆弱性の悪用については、わかっていない
  - データ漏洩：データ漏洩の懸念は拭えない
- 運用チーム
  - 状況
    - 基本的に、GanGanシステム全体が侵害されていて、データもほぼすべて暗号化されている
    - GanGanシステムは、完全にCondorの配下にあり、業務継続は出来ない状況
    - バックアップは、一週間前のバックアップが利用できるが、リストア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、決済代行事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。
    - この対応を行った場合、現在進めている６カ月後にリリース予定の新規開発ゲームのリリースが遅れる（２～３カ月）。
  - ユーザーが保有しているゲーム内ポイントの総額は、前月末で３千万円相当。
- 法務の回答
  - 身代金を支払うことは推奨できない
  - 警察への届出をしておくことが望ましい。直接、事件が漏れることはないはず。
- 広報
  - メディアに公表する必要がありそう
  - 停止直後から、SNS等で話題になっている
- 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

2-1 ディスカッション-2

セッション 2

想定する状況	対応
バックアップが無い場合	● 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。	● **指示・報告・届出等はありますか** ● **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** ー
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	● 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 ● コンタクトは行いますか、どのようなコンタクトを行いますか？ ● 指示・報告・届出等はありますか ● 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）	● 指示・報告・届出等はありますか ● 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

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
- 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

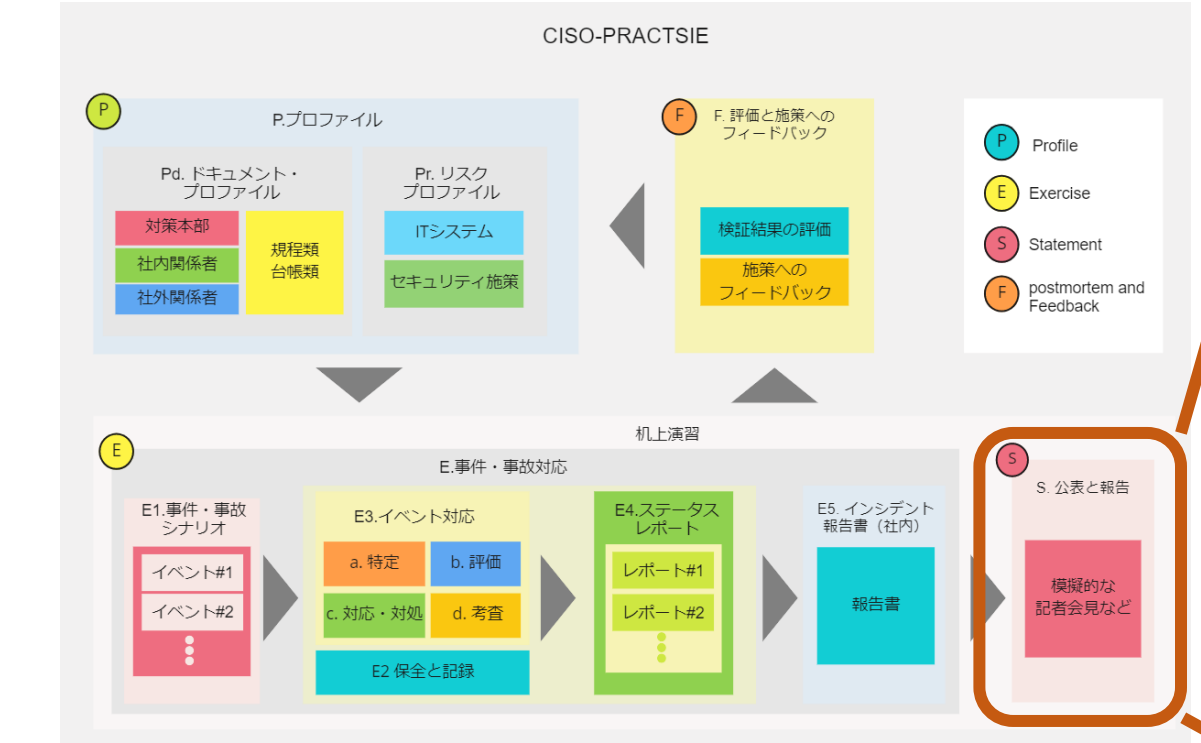
セッション３

- 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
	ワークアラウンド（被害の軽減策）
	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）
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）
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

3-1
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
- 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）

セッション 3

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

セッション 3

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	

感想@JNSA

- 私の経験からは、公表すると炎上を招きかねない内容が目に付いたので、経営者から了承を得るセッションを追加して、内容の修正を狙った
（田中さんに経営者役をお願い）

3-2-a
経営者から
公表内容の了承を得る

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。
発表のスクリプト（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
- 経営者に何をして欲しいか、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

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

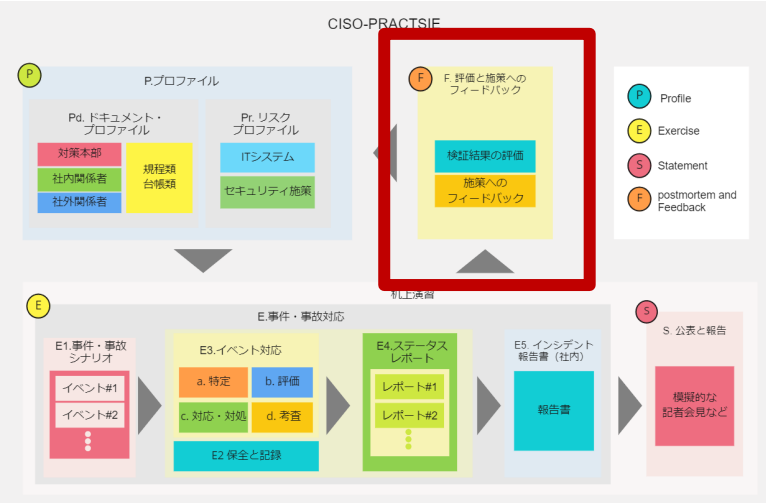
全般的な留意点

・　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

違いはどこにあったか

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。



CISOと専門家のギャップについて

WGメンバーからのコメント
「ギャップ」があるというけれど、そもそも、ワークショップはCISOや経営陣を対象としたもので、セキュリティ専門家を対象にするのは違うのでは？

いやいや、そうじゃない！
ワークショップはCISOが主幹する想定だが、セキュリティ専門家は、ワークショップの重要なメンバー。つまり、ワークショップで見えたギャップは、実際のインシデント対応でも起きるギャップとなる。
だから、「ギャップ」を明らかにすることは、インシデント対応時ばかりではなく、セキュリティ対策全般に対して重要な取り組みとなる。

セッション-1：ランサムウエア単純感染

初動対応（ディスカッション）

感想@CISOs

- 特権とストレージサービスへの注目度が高かった
- 原因究明と拡大防止のバランスに意見が分かれた

感想@JNSA

- 仮想企業への着目が不足していたようだ
- 個別要素の判断に留まり、予算や事業継続を判断の基準とする視点が薄い傾向があった
- 十分な情報がないなかで、何を確認すべきか具体化しなかった（例、特権やストレージへの注目など）
  - ワーストケースの想定した手順が見られなかった
  - 何をもって終了とするかの議論が見られなかった
- 想定される影響範囲に対する注目が少なかった

経営陣への報告

感想@CISOs

- 現状と今後の懸念が、概ね的確に報告されていた

感想@JNSA

- 何のための報告かという視点が薄かった
  - 経営者に報告をする必要のない内容が少なくなかった
  - 経営者に依頼する視点が見られなかった
    - 今後起こるかもしれないこと、もし起きた場合に必要な対応
    - 必要な予算、リソース
- 総じて報告の構成（プロトコル）が感じられなかった

セッション-2：ランサムウエア事業停止

身代金支払いについてのディスカッション

感想@CISOs

- 売上と身代金を比較して速攻で払うと判断し方がいた
- 自身の将来の評価に影響するため絶対に払わないという方がいた
- まず顧客にどう伝えるかが重要であるとの意見があった
- 支払う場合の手続きについて言及があった（決済方法など）
- 犯人と交渉するという意見も少なくなかった

感想@JNSA

- 自身の理念に基づいて是非を判断する傾向がみられた
- 売上高と身代金の比較などPL目線のアプローチが見られなかった
- 顧客に伝える内容が、自身の理念に基づいたもので、事業の視点・顧客の視点が薄いように思われた
- インシデント対処のフレームワークは見られたが、リスク評価の基本的なフレームワークを感じなかった
- 具体的な連絡先が把握されていなかった（警察への届出など）

セッション-3：模擬記者会見

公表内容に対する経営者の承認

感想@JNSA

- 報告に終始し、経営者にどのような判断を求めているかが不明瞭
  - 予算確保や権限移譲など、必要な対処を経営者に提案するアプローチが見られなかった
- 全チームが事業継続を前提としていた
  - 補償を提案するチームがあったが、効果的とは思えなかった
- 確認が取れていることと、推測が混在していることがあった
- コンプライアンス上の義務について触れられていなかった

模擬記者会見

感想@CISOs

- 社長役で登壇をお願いした方から、登壇してはじめて不安を覚えた、とのコメントがあった
- 話すべきこと、話さないことのメリハリがあり会見が成立しいた
- このシナリオでは絶対に記者会見は開かないという意見があった

感想@JNSA

- 記者会見の目的・狙いが不明瞭だった（やらされ会見）
  - 記者会見のタイトルを考える必要がある
  - 世間の視点や興味、警戒すべき発言への配慮が必要
- 一般に、記者会見は難しいことを痛感した
- 模擬記者会見は、経営陣に限定し、そうでない場合は、経営者の承諾を得るセッションに変更するのが良さそう

ワークショップを通じた気付き

- 現役CISOとセキュリティ専門家には深くて暗い河があった…
  - 現役CISOには、共通したプロトコル（フレームワーク）が見られた
  - セキュリティ専門家には、そのプロトコルが見られなかった。
    - 後日、「自身の報告を部下からの報告に置き換える」と、報告の適切さを判断しやすくなる、という気づきがあった

- セキュリティ専門家が経営陣としてのプロトコルを学ぶ必要がある
  - CISO-PRACTSIEは、フォーマットがあれば、事業的な経験がなくても、適切な対応ができるという考えだったが、前提が違っているようだ
  - 経営者・経営陣にセキュリティの知見を期待するのは、球団オーナーや監督に剛速球や大ホームランを期待することかもしれない
    - たぶん選手（専門家）がゲームやシーズンに関する知見を深める方が現実的
  - 経営者は一様ではなく、経営も一様ではないが、共通するプロトコルがある
    - 経営の構成（経営者と経営陣、Role & Responsibility、オペレーション、Representative）などを意識する必要がある。

現役CISOとセキュリティ専門家のギャップを補う
CISO育成を目指したアプローチができないか？

むすび

CISO育成コンテンツは出来るのか?

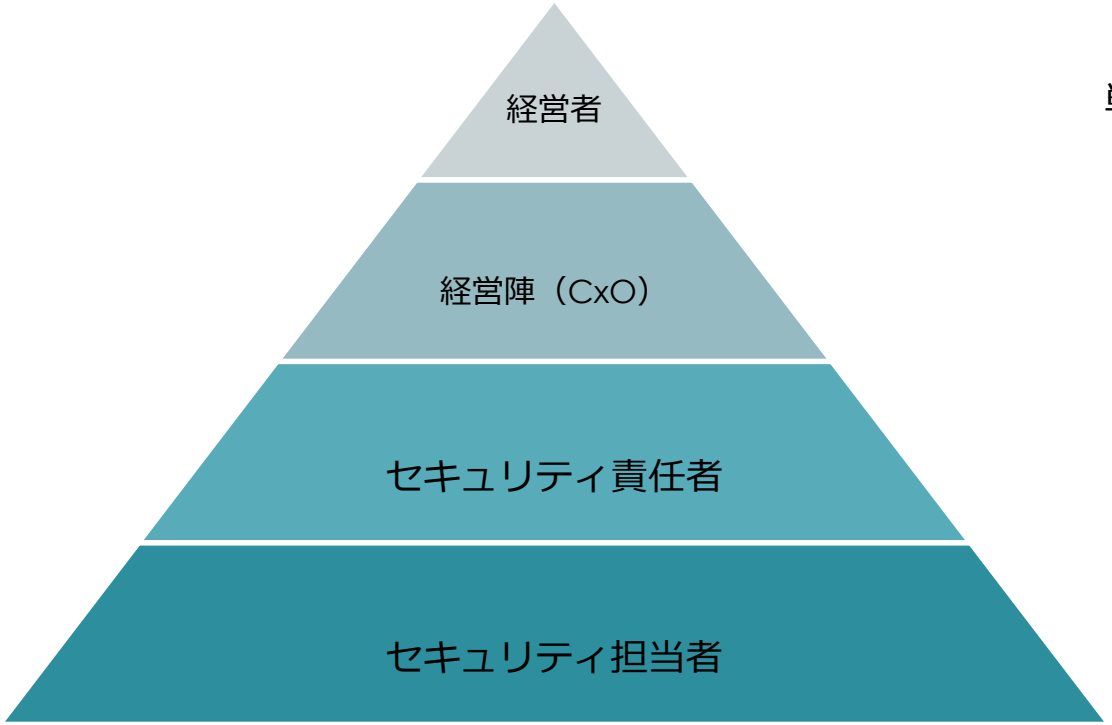
育成というアプローチが必要か？

②CISO-PRACTSIE

CISOがセキュリティ施策の検証と、
組織内の共通基盤を構築するための
フレームワーク（プレーブック）

①CISOハンドブック

業務執行としてセキュリティに
取り組むためのフレームワーク



③育成のためのアプローチ（企画中）

セキュリティ責任者・担当者が
業務執行としてセキュリティを身に着けるための
フレームワーク

単に、攻撃されます！、危ないです！
だけではない伝え方

提供側にとっては、企業の担当者だけ
ではなく、CISOや他の事業責任者に受
け入れられる提案のベースとして

CISO支援ワーキンググループの活動

- 本年度の活動目標
  - これまでの成果物をブラッシュアップする
  - CISO育成マテリアルの作成にチャレンジする
    - 経営者の話を伺い、フィードバックをもらえる機会を企画してみる

- WGの活動
  - Slackを中心にコミュニケーションを取っています
  - 毎週月曜の夕方にオンラインミーティングを開催（時々さぼります）
    - 驚くほど緩い運営です
    - 今回は話しきれなかった内容なども、逐次取り上げています
- 参加方法
  - sec@jnsa.orgにCISO支援WG参加希望とお伝えください
  - ご質問などあれば、会場でお声がけください


Thank you