CISO-PRACTSIE

机上演習によるセキュリティ施策の評価
仮想企業を題材としたワークショップ

JNSA 社会活動部会 CISO支援ワーキンググループ

Copyright and License

机上演習による
社内横断的な有効性評価
アプローチ
CISO-PRACTSIE

CISOのための情報セキュリティ戦略

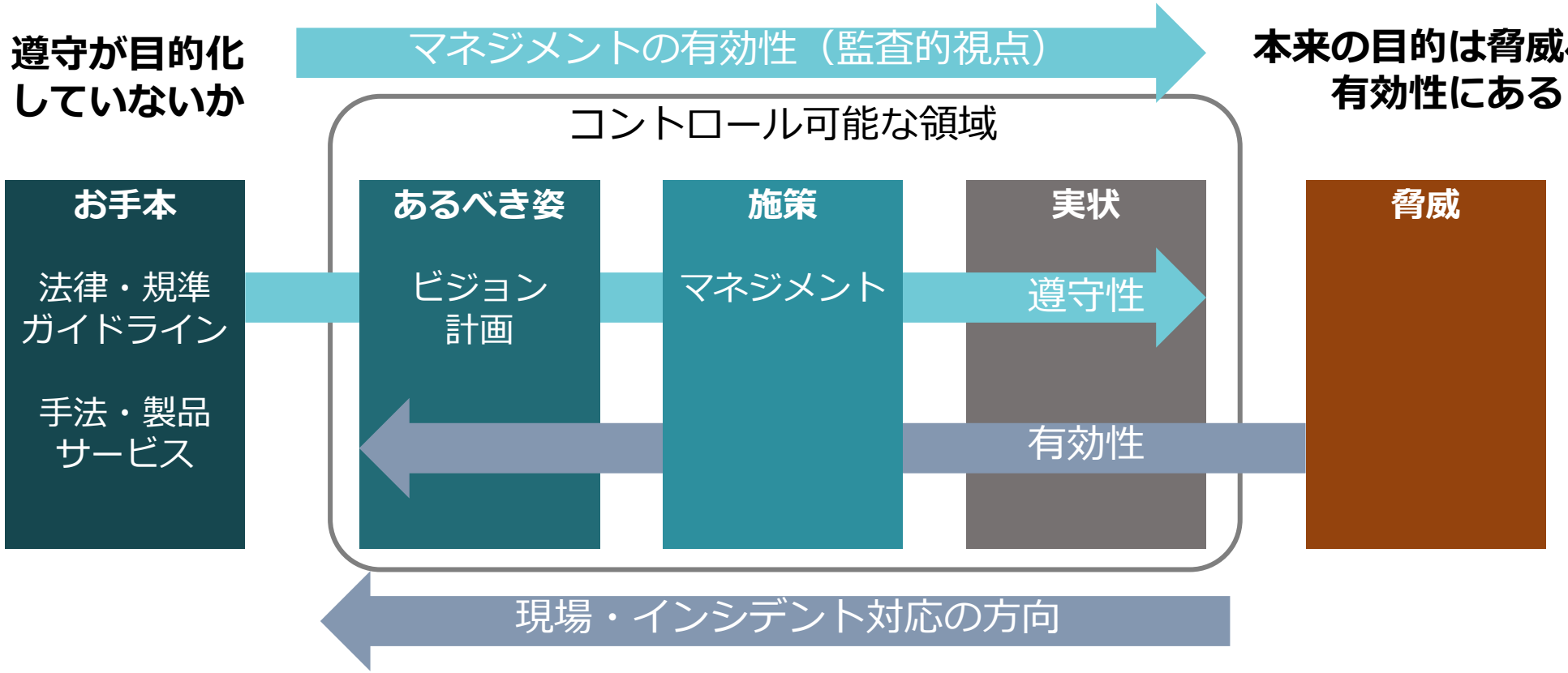
CISO-PRACTISEの目的とゴール

- 遵守性と有効性の視点
- 技術的な視点だけではなく、
  事業視点、経営視点から有効性を評価する
- 外部視点から、有効性を評価する
- セキュリティを全社共通の課題とする
- セキュリティが主導的な役割を図る

二つの論点：遵守性と有効性

本当の目的は、
事業のマネジメントにある。

仮に完璧なセキュリティ対策が実現できても、会社が潰れては意味がない



有効性の評価は、フォルトツリー検証をするということかもしれない

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

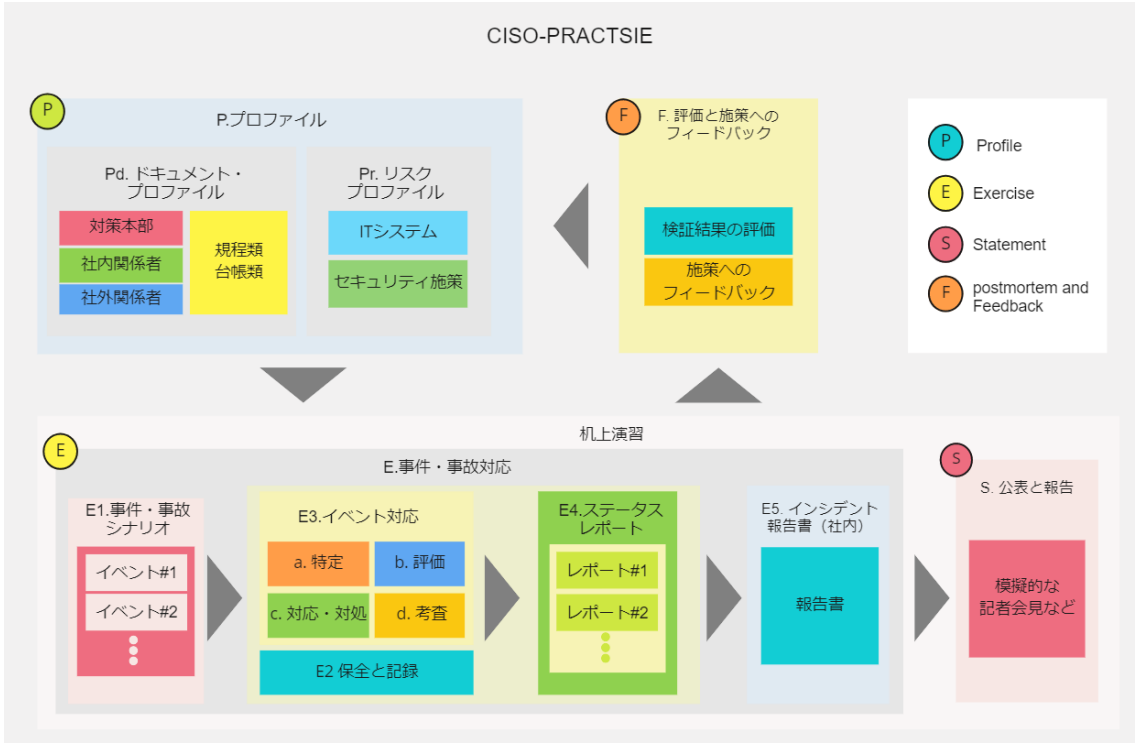
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

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



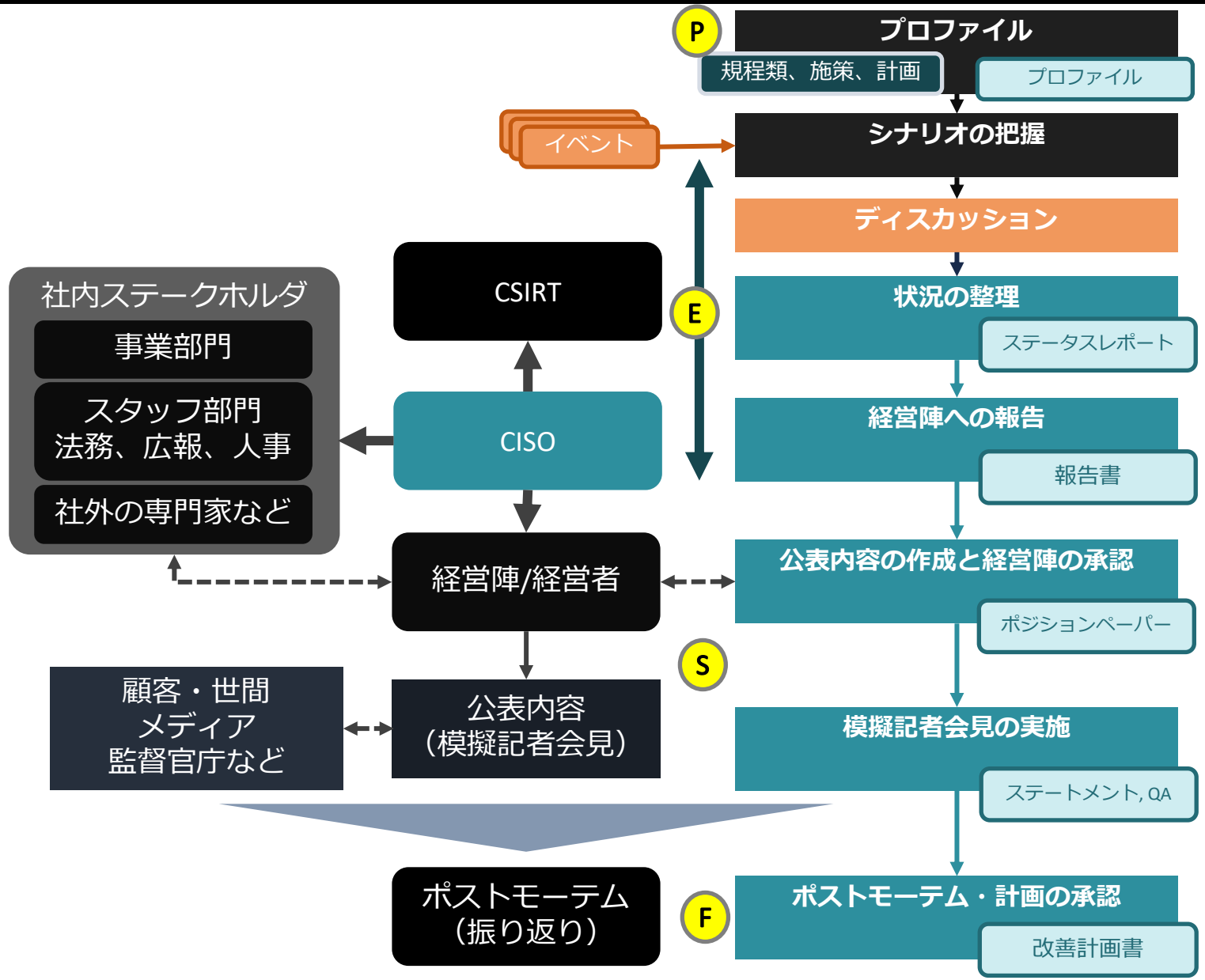
OUTPUT

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の流れ



- 会社の状況、セキュリティ施策、経営計画など、事案対応の基盤となる情報を収集し整理（プロファイル）する

- 提示されたイベント（シナリオ）を理解する

- セッションのウォーミングアップ
- 提示された議題について、意見を交換を行う

- 関係者に確認する項目に基づき、事業・経営視点で現状況を把握
- この作業を通じて関係者の共通認識を醸成する
- 状況が変化したときは、速やかに内容を更新する

- ステータスレポートに基づいて、経営陣への報告書を作成する
- 単に収集した情報を述べるのではなく、事業や経営への影響を明らかにし、経営陣に求める判断や、依頼事項を明らかにする（費用、リソース、システムの停止など）

- 一般的には広報が作成するが、セキュリティ施策の合理性を検証するためCISOの立場で作成する
- 防御・対処・検出などの公表内容の証跡について検証する
- ポジションペーパー（≒公表内容）は経営者の承認が必要
- 経営者（役）は会見をする立場から検証し公表内容を仕上げる

- 模擬会見で客観的で合理的な説明が出来ることを検証する。
- 記者役からの質疑応答を通じて、内々の理屈となっていないか、欠けている視点は無いか、などを検証する。

- 対応や改善が必要な項目と対応計画を明らかにする

■社内で実施する場合

- 「再発防止策」は「今すぐ実施すべき施策」
- 対応や改善は、「実施計画」に落とし込む

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、これらの資料が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。

- 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、そのセキュリティ対策をCISO-PRACTSIEの対象としています。
- 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。

JNSAアーキテクトのプロファイル-1

JNSAアーキテクト　会社概要（未上場）

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	170名
平均年齢	42歳
売上高	34億円（2022年3月期）
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（202x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

JNSAアーキテクト 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）	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(EO)	唐澤M
ゲーム事業部	佐々木 執行役員(EO)	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	佐々木 執行役員(EO)	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	

JNSAアーキテクトのプロファイル-2

事業概要 1/2

項目	GanGanシステム
事業概要	ビジュアルを強化したロールプレイングゲーム ユーザー間での共有や、SNSへの投稿が可能 有償サービスあり（月額200円）
事業責任者	担当執行役員：佐々木執行役員
運用責任者・担当者	青島D、GanGan運用グループ（山口）、業務委託の計画あり
開発責任者・担当者	藤井 開発本部長, GanGan開発グループ（後藤M）
ユーザー数	全体　約200万人の登録ユーザー、有償　約10万名
売上高・見込み	年間で20億円 月額会費：2.4億（10万名*200円*12カ月） 有償アイテム販売など：9.6億円 広告など：8億円
ユーザーの居住地域 サービス提供地域	日本（海外のユーザーはいるが、事業展開は日本のみ） 海外展開も検討中（EU,US）
窓口	ask-gangan@jnsa-architect.com

事業概要 2/e

項目	GanGanシステム
情報の種類	個人情報、決済はサービス代行業者が実施
改竄された場合の影響 （自社・顧客など）	マルウエア拡散、キャラクターの削除、盗難、不正な課金など クレジットカード番号は保持していない
SLA	利用規約の中で稼働率は保証しない旨を記載
自社への影響	ユーザーからのクレーム、金銭的な保証の可能性
顧客などへの影響	直接的に金銭的な損害をあたえる可能性は極めて低い
直接的な機会損失 （平均売上・利益）	有償サービスとしては約550万円/日、約23万円/時に相当 補填などが求められる可能性がある
法的な義務など	個人情報保護法（海外展開後は、各国の規定など）
制裁金・罰金・罰則など	GDPR : €2000万（27億円） CCPA: $2,500(約32万円), $7,500(約100万円)
監督官庁など	経済産業省（窓口 佐々木執行役員） 個人情報保護委員会（窓口 堀口DPO）
取引銀行	あけぼの銀行

JNSAアーキテクトでは、もう一つのシステムSokoSokoを運用していますが、本ワークショップでは対象せず、省略しています。

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。
このような判断を行う場合は、判断の根拠を残すという視点で、演習を行ってください。
また、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、経営陣への報告書を作成してください。

E1: 端末の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

- 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$600(約90万円)の送金が求められている。
- 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。

E1-a: 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）		

グループで、以下を取りまとめてください。

A（すぐにやる）を4項目
D（絶対やらない）を２項目

選択した項目と理由を述べてください。

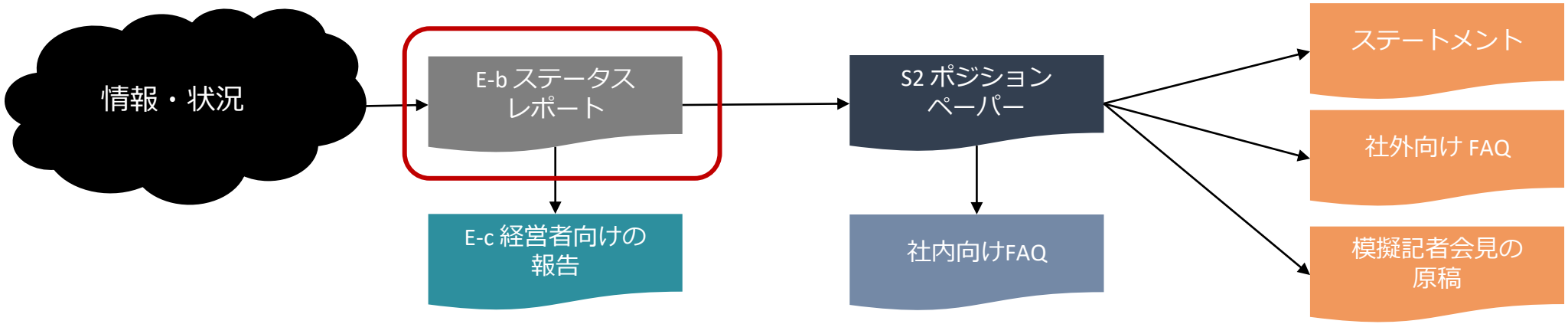
判断：A:すぐやる、B:やるかもしれない、C：この段階ではやらない、D:絶対やらない、E：可能ならやりたい

E1-b
ステータスレポート

E1-b: レポート・作成資料の構成

関係者向けの整理 -> 経営者向けの報告 -> 公表内容の整理 -> 公表資料の作成　の手順で資料を作成します

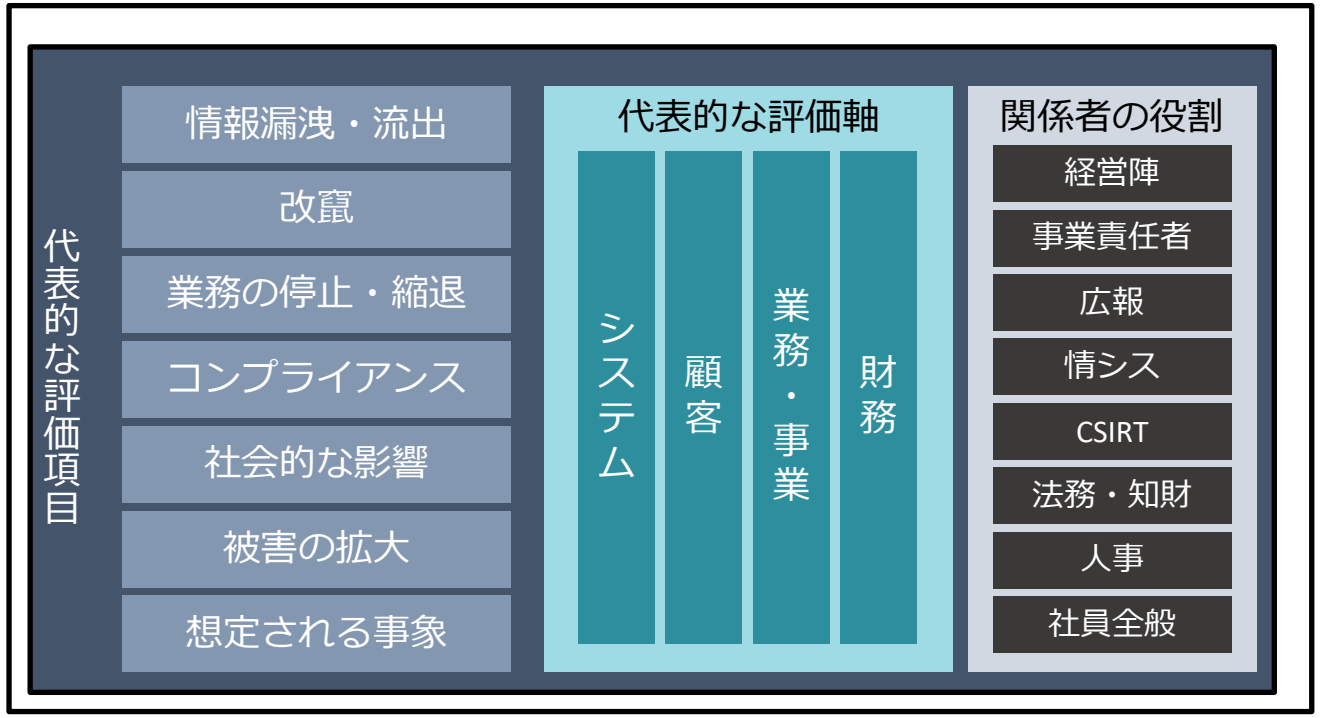
- 関係者向けの整理
  - ステータスレポート：できるだけ客観的に情報や状況をまとめるために担当者間で共有する資料
- 経営者向けの報告
  - 経営者向けの報告：会社・組織としてのインパクトを明らかにし、経営判断を仰ぐための資料
- 公表資料の整理
  - ポジションペーパー：事案の概要や状況などに対する公式見解（公表内容）を社内で統一するための社内資料
  - 社内向けのFAQ：想定される質問に対する共通した見解を述べるための社内向け資料
- 公表資料の作成
  - ステートメント：報道向けへの配布、ホームページでの公表等に使用する資料
    ステートメントは、公表できる内容のみを記載し、憶測や実現できない内容は記載しない
  - 社外向けのFAQ：ステートメントを補完するもので、メディアや顧客などに配布・公表する資料



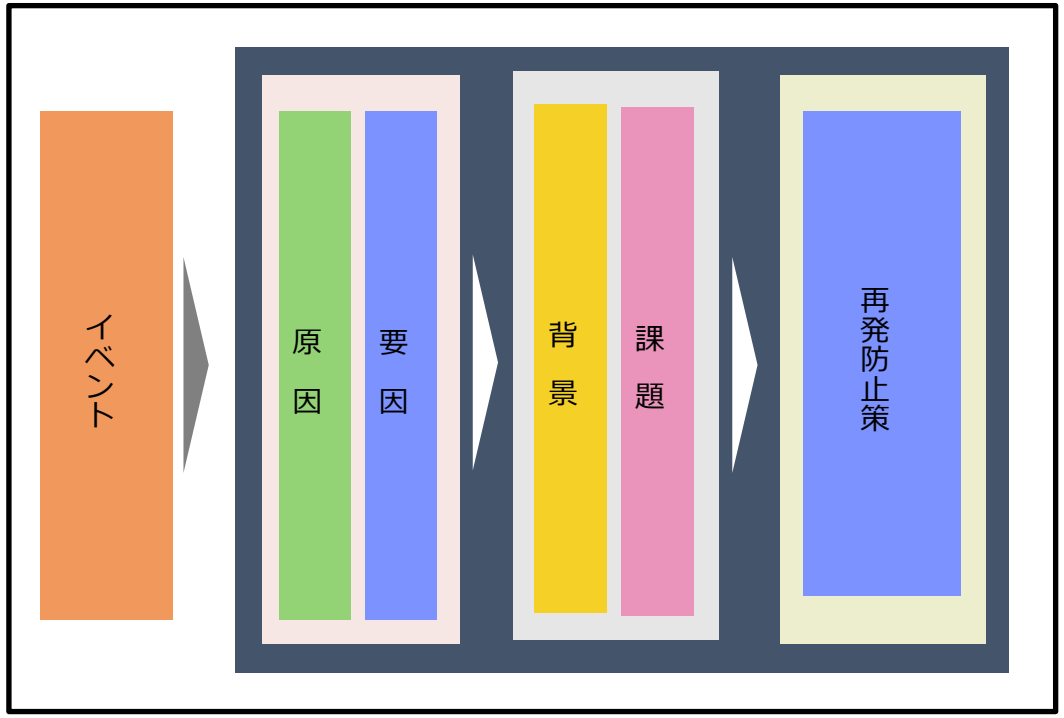
E1-b: 状況と必要な対応の把握

状況と必要な対応・対処についてディスカッションし、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と評価軸（重要度・深刻度）



原因・要因・背景・課題で分析する



E1-b: 関係者の役割と深刻度・可能性

ステータスレポートでは、ステークホルダーの役割をRACIで分類し、深刻度と可能性を５段階で評価します。

RACI: 関係者の役割をRACIで分類する

(s)-1対応レベル RACIで記載(- 対象外) Responsible, Accountable Consult, Inform	I 経営陣 A 事業担当執行役員等 I 広報	R 情シス R CSIRT A CISO C 法務・知財	- 人事 - 社員全般

- **R**esponsible（実行責任者）　- 責任者
- **A**ccountable（説明責任者）　- 外部からの問合せの対応責任者
- **C**onsulted（協業先）　- 意見を求められる者。双方向の対話
- **I**nformed（報告先）　- 進捗を常に把握している者。一方向の通信

深刻度と可能性

(s)-4 顧客・取引先の被害 深刻度：Critical ,Serious , Moderate Light, - 可能性：occure, hlgh,medium,low, -	Mo 金銭的な被害 Sm 詐欺行為など Lm 機密情報の漏洩	C- 業務停止 Mm 脅迫行為	□□ その他（不明）

深刻度

Critical	深刻な影響がある
Serious	重大な影響がある
Moderate	ある程度の影響がある
Light	軽微な影響がある
-	具体的な影響は考えにくい

可能性

occurred	既に起きている
high	起きる可能性が高い
medium	起きる可能性がある
unlikely	起きる可能性は低い
-	起きる可能性はない

E1-b: 対象事業

対象事業	**(b)-1 事業の概要**	**事業：**JNSAアーキテクト事業全般 **担当責任者：**石田CISO・矢野CIO **事業概要：**PCオンラインゲーム開発及びサービス提供 **売上：**年間で約30億円 **顧客数：**約200万人の登録ユーザー、有償　約10万名（GanGanシステムから）	
	(b)-1.5 事件・事故の概要	従業員が業務で利用するPCがランサムウエアに感染し、約1千万円の身代金が要求されている。 在宅で勤務しており、会社とのVPN接続は行っていないが、オンラインストレージと同期。	
	(b)-2影響を受ける情報の種類 深刻度：Critical ,Serious , Moderate Light, - 可能性：occur, high, medium, unlikely, -	Mu 個人情報 Lu クレジットカード情報など Mu 顧客から預かった機密情報 Lu 自社の機密情報	Lu 公表済みの情報 Cu認証情報 Su 特定が困難（端末・メール等） Lu その他
	(b)-3 システム停止の影響	業務用PC1台であるため、大きな影響はない。	
	(b)-4コンプライアンス	コンプライアンス上の問題はないと判断。	
	(b)-5社会的影響	社会的な影響はないと考えるが、身代金を支払らうことになった場合に、これが明らかになると、一定の批判をあびる可能性がある。	
	(b)-6その他	特になし。	

E1-b: 事業への影響

事業への影響	**(s)-1対応レベル** RACIで記載(- 対象外) Responsible, Accountable Consult, Inform	i 経営陣 i 事業担当執行役員等 - 広報	RA 情シス RA CSIRT A CISO - 法務・知財	- 人事 - 社員全般
	(s)-2 状況・概要	業務用PC1台であるため、大きな影響はない。 また、在宅勤務であり、VPNを利用していないことから、イントラネットへの侵入した可能性は低い。		
	(s)-3 事業面の対応	☐ 事業の停止 ☐ 事業の縮退（一部停止） ■ 事業の継続	**・背景・状況：**原因はまだ確認できていない 規定通りに、EDR、自動アップデートが有効であった。	
	(s)-4 顧客・取引先の被害 深刻度：Critical ,Serious , Moderate Light, - 可能性：occur, high, medium, unlikely, -	-- 金銭的な被害 -- 詐欺行為など Lu 機密情報の漏洩	-- 業務停止 -- 脅迫行為 -h なし	-- その他（不明）
	(s)-5 自社の被害 深刻度：Critical ,Serious , Moderate Light, - 可能性：occurred, high, medium, unlikely, -	Lo 金銭的な被害 -- 詐欺行為など Mu 機密情報の漏洩 L- 業務停止	Lo 脅迫行為（身代金） Lu 信用の失墜 Lu 社会的責任 -h なし（軽微）	-- その他（不明）

E1-b: 顧客への影響

顧客への影響	(i)-1 影響の概要	現段階では、顧客に関連する情報への影響はない。	
	(i)-2 影響を受ける データ量・被害者数	**被害者数：**不明 **データ量：**現段階では、当該PCの暗号化が行われているだけだが、漏洩についても懸念あり。 当該社員のメールボックス等に顧客に関する情報が含まれている。	
	(i)-3 影響を受ける 被害者の特徴	不明。	
	(i)-4 想定される二次被害	N/A	
	(c)-1 被害の確認方法	N/A	
	(c)-2 被害者の ワークアラウンド	N/A	
	(c)-3 被害者が 実施できる対策	N/A	
	(r)-5 外部の専門家 RACINで記載(- 対象外) Responsible, Accountable Consult, Inform,Notification	- 公認会計士など - 弁護士 - 安全保障貿易情報センター - 労働局	- SIベンダー - セキュリティ企業 - 損害保険窓口 - その他：

E1-b: 財務への影響

財務への影響	f-(1)直接的な損害	■金銭損害 身代金：90万円（支払う場合） 詐欺被害：N/A 現金の引き出し等：N/A	■利益損害 直接的な機会損失：N/A 間接的な機会損失：N/A
	f-(2)費用・賠償・制裁金等	■費用損害 事故原因調査：CSIRT 1 人日 事故対応：上記に含む 広告・宣伝：なし コールセンター：なし 見舞金等：なし 被害範囲等調査：事故原因調査に含む	■損害賠償 賠償費用、弁護士費用等：なし ■行政損害 個人情報保護法：なし GDPR/CCPAなど：なし
	f-(3) 無形損害・その他	■無形損害 ブランド棄損：なし 株価：なし	■その他

E1-b: 外部への連絡・報告

外部への連絡・報告	(r)-1 必須の連絡先 （監督官庁など）	**担当者：**N/A **報告先：**N/A **時間的な制約：**N/A	☐ 個人情報保護委員会 ☐ GDPR ☐ 監督官庁 ☐ 警察 ■不要 ☐ その他
	(r)-2 取引先	**担当者：**N/A **取引先名：**N/A	☐ 第一報を即時入れる ☐ ある程度事実関係が分かった段階で報告 ☐ 確実な状況が把握できるまで連絡しない ■ 報告の必要はない
	(r)-3 影響を受ける被害者	**担当者：**N/A	☐ 第一報を即時入れる ☐ ある程度事実関係が分かった段階で報告 ☐ 確実な状況が把握できるまで連絡しない ■ 外部の被害者はいない
	(r)-4 メディア等の公知	**担当者：** ☐ メディア ☐ ホームページ ☐ SNS等 ☐ その他 ■ 不要	影響を受けない被害者：N/A

E1-b: 影響を受けるシステム

影響を受けるシステム	(t)-1 システムの名称・概要	■名称：社員ＡのＰＣ ■責任者：本人 ・ビジネス面（責任者,担当者） ・技術面 責任者：石田CISO, 矢野CIO 担当者：	■システム概要
	(t)-3 情報流出の懸念	暗号化されたが、情報漏洩は確認されていない。 しかし、近年のランサムウエアの手口を考えると、情報の流出も想定する必要がある。	
	(t)-4 システム停止の懸念	PCは初期化または調査のため停止するが、代替えのＰＣを提供し、業務への影響は最小限にした。	
	(t)-5 システム侵害の懸念	WFHでVPN接続を行っていないことから、イントラネット等への侵害は考えにくい。 ファイルサーバーを利用しているため、ファイルサーバーに怪しいファイルがおかれていないか、至急確認する必要がある。	
	(t)-7事故の原因・要因	EDRが稼働しており、シグネチャも最新に保たれている。OSの自動アップデートも実施されており、現段階での直接的な原因・要因は掴めていない。	
	(t)-8 再発防止策（具体的）	原因・要因が分かり次第対策を検討する。	

セッション２
主要なシステムの停止

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（役割にも注目する）
- 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

E2: 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に関連した攻撃の可能性があります。

・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1BTC(約1000万円)*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

*2024年5月の相場で概算。相場にかかわらず、約1千万として扱ってください。

・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）
・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

E2: 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。
    - データ量から推測し、リストアには５日程度必要と考えられる。
    - 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。
- 開発部の回答
  - ソースコードは復旧可能。
  - 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30億円相当。
- 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。

E2-a: ディスカッション-2

CSIRTがシステム被害状況の調査を行っています。現段階では、システムが稼働していない事、その原因はランサムウエアによるファイルなどの暗号化であること、だけがわかっている状況です。
身代金の支払いについて、CISOであるあなたは何をすべきでしょうか。
以下の観点から、チームで議論してください。

想定する状況	対応
バックアップから復旧が出来る可能性があり、復旧の目途は、５日間と見積もられていますが、これまで、このような復旧作業を行ったことはありません。	**以下の項目について対応方針を述べてください** ● **経営陣にはどのように伝えますか？** ● **顧客への対応はどうしますか？** ● **経営陣に対して、身代金の支払いの是非をどのように提言しますか？**

後日、参考にして頂きたい資料

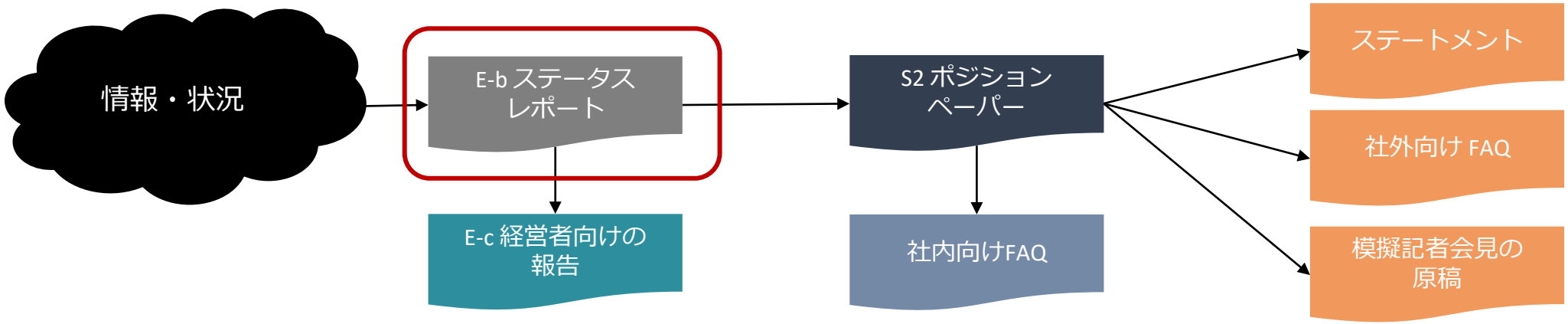
- ランサムウェア被害防止対策｜警察庁Webサイト (npa.go.jp)
  https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html
- ランサムウェア対策特設ページ | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
  https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html
- 侵入型ランサムウェア攻撃を受けたら読むFAQ (jpcert.or.jp)
  https://www.jpcert.or.jp/magazine/security/ransom-faq.html

E2-b
ステータスレポート

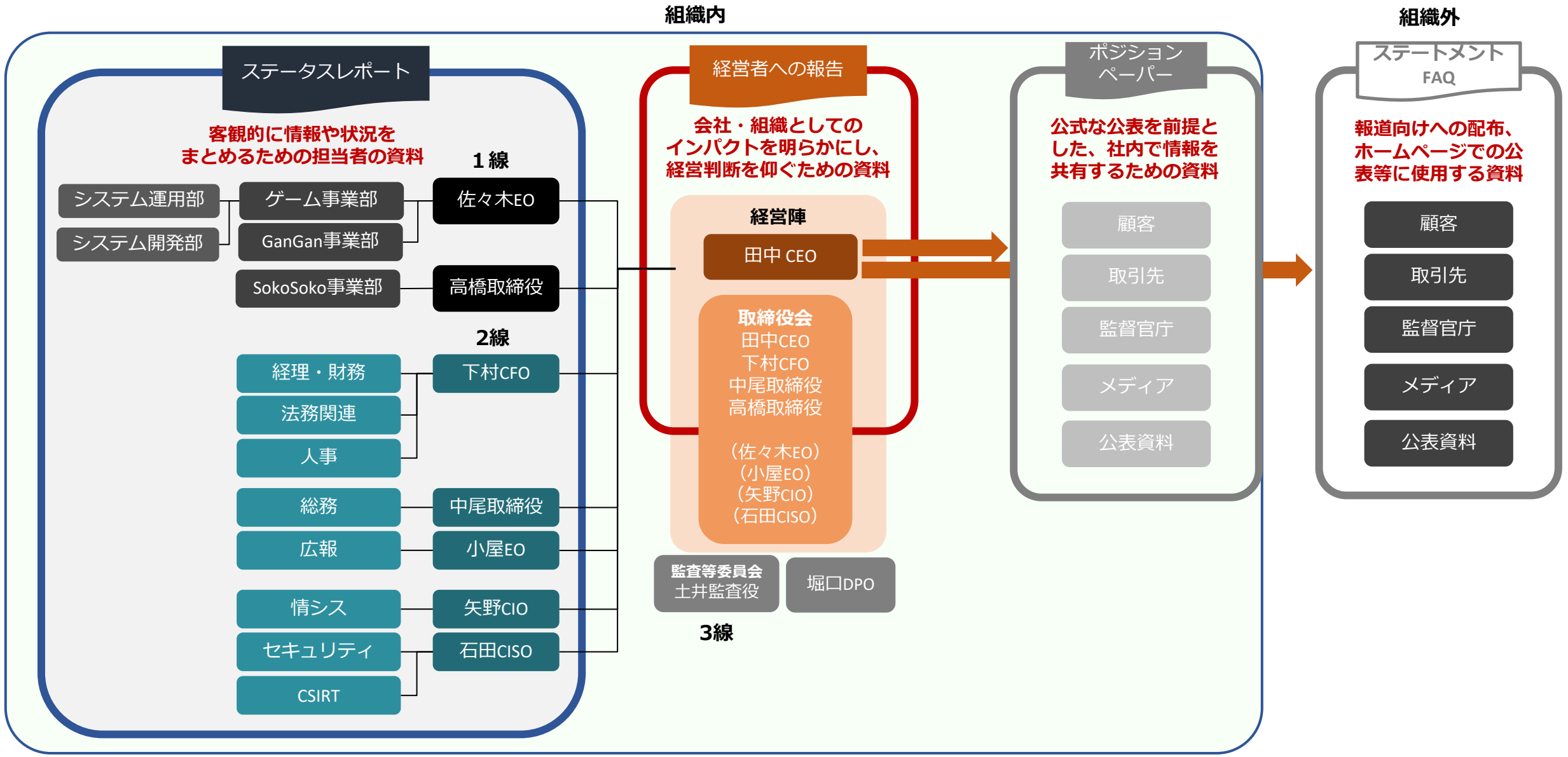
E2-b: レポート・作成資料の構成

関係者向けの整理 -> 経営者向けの報告 -> 公表内容の整理 -> 公表資料の作成　の手順で資料を作成します

- 関係者向けの整理
  - ステータスレポート：できるだけ客観的に情報や状況をまとめるために担当者間で共有する資料
- 経営者向けの報告
  - 経営者向けの報告：会社・組織としてのインパクトを明らかにし、経営判断を仰ぐための資料
- 公表資料の整理
  - ポジションペーパー：事案の概要や状況などに対する公式見解（公表内容）を社内で統一するための社内資料
  - 社内向けのFAQ：想定される質問に対する共通した見解を述べるための社内向け資料
- 公表資料の作成
  - ステートメント：報道向けへの配布、ホームページでの公表等に使用する資料
    ステートメントは、公表できる内容のみを記載し、憶測や実現できない内容は記載しない
  - 社外向けのFAQ：ステートメントを補完するもので、メディアや顧客などに配布・公表する資料



E2-b: 誰のためのレポートか？



E2-b: レポートの更新

- 経営向けの報告書をまとめるにあたって、配布したステータスレポートを、現状に基づいて更新してください。
- 例示した「事業への影響」を参考に「顧客への影響」を更新してください。

- スタッフが適時確認を行うので出来る限り対応をするようにしてください。

E2-b: 対象事業

対象事業	**(b)-1 事業の概要**	**事業：**JNSAアーキテクト事業全般 **担当責任者：**石田CISO・矢野CIO **事業概要：**PCオンラインゲーム開発及びサービス提供 **売上：**年間で約30億円 **顧客数：**約200万人の登録ユーザー、有償　約10万名（GanGanシステムから） JNSAアーキテクト GanGanシステム 佐々木 EO ビジュアルを強化したロールプレイングゲーム ユーザー間での共有や、SNSへの投稿が可能 有償サービスあり(月額200円) 20億円
	(b)-1.5 事件・事故の概要	従業員が業務で利用するPCがランサムウエアに感染し、90万円の身代金が要求されている 在宅で勤務しており、会社とのVPN接続は行っていないが、オンラインストレージと同期 システムが止まっている(売上:約550万円/日)、 3日以内に身代金の支払いが求められている(bitcoinで約1千万円)
	(b)-2影響を受ける情報の種類 深刻度：Critical ,Serious , Moderate Light, - 可能性：occur, high, medium, unlikely, -	Mu 個人情報　Sm Lu クレジットカード情報など　Lu Mu 顧客から預かった機密情報　Cm Lu 自社の機密情報　Sm Lu 公表済みの情報　Lm Cu認証情報　Cm Su 特定が困難（端末・メール等）　Cm Lu その他　Sm
	(b)-3 システム停止の影響	業務用PC1台であるため、大きな影響はない 主要なビジネスであるGanGanが止まっているため、約550万円/日の機会損失となる。 また、システムの停止に伴い、利用者のサービス離れも起きると考えられ、事業の存続に関わる状況。
	(b)-4コンプライアンス	コンプライアンス上の問題はないと判断 ユーザー情報が漏えいしている可能性があるため、個人情報保護法上の対応を検討する必要がある
	(b)-5社会的影響	社会的な影響はないと考えるが、身代金を支払らうことになった場合に、これが明らかになると、一定の批判をあびる可能性がある 利用者のチャット機能上の機徴なデータが漏れた場合、一定の社会的な影響があると考えられる。 また、身代金の支払いの是非は、センシティブな問題である点も、考慮する必要がある。
	(b)-6その他	特になし

E2-b: 事業への影響

事業への影響	**(s)-1対応レベル** RACIで記載(- 対象外) Responsible, Accountable Consult, Inform	i 経営陣 RA i 事業担当執行役員等 RA - 広報 RA	RA 情シス R RA CSIRT R A CISO RA - 法務・知財 法務:C	- 人事 - 社員全般 I
	(s)-2 状況・概要	業務用PC1台であるため、大きな影響はない また、在宅勤務であり、VPNを利用していないことから、イントラネットへの侵入した可能性は低い 1週間前のバックアップはあるが、リストアの実績はない。リストアは5日間程度かかると予想されるが、復旧できるかは未知数。また、ソースコードは復旧できるが画像等のバックアップはない。 他のシステムとは独立したアカウントを使っているため、他のシステムが影響をうける可能性は低い 海外のユーザーは存在するが、日本向けのサービスであることから、GDPRの対応は必要がないと判断		
	(s)-3 事業面の対応	□ 事業の停止 L □ 事業の縮退（一部停止） ■ 事業の継続	**・背景・状況:**原因はまだ確認できていない 規定通りに、EDR、自動アップデートが有効であった システムはすでに止まっている	
	(s)-4 顧客・取引先の被害 深刻度：Critical ,Serious , Moderate Light, - 可能性：occur, high, medium, unlikely, -	-- 金銭的な被害 Mm -- 詐欺行為など Lu Lu 機密情報の漏洩 Sm	-- 業務停止 Co -- 脅迫行為 Co -h なし	-- その他（不明）
	(s)-5 自社の被害 深刻度：Critical ,Serious , Moderate Light, - 可能性：occurred, high, medium, unlikely, -	Lo 金銭的な被害 -- 詐欺行為など MI 機密情報の漏洩 L- 業務停止	Lo 脅迫行為（身代金） Lu 信用の失墜 Lu 社会的責任 -h なし（軽微）	-- その他（不明）

セッション３
CISOから経営陣への報告

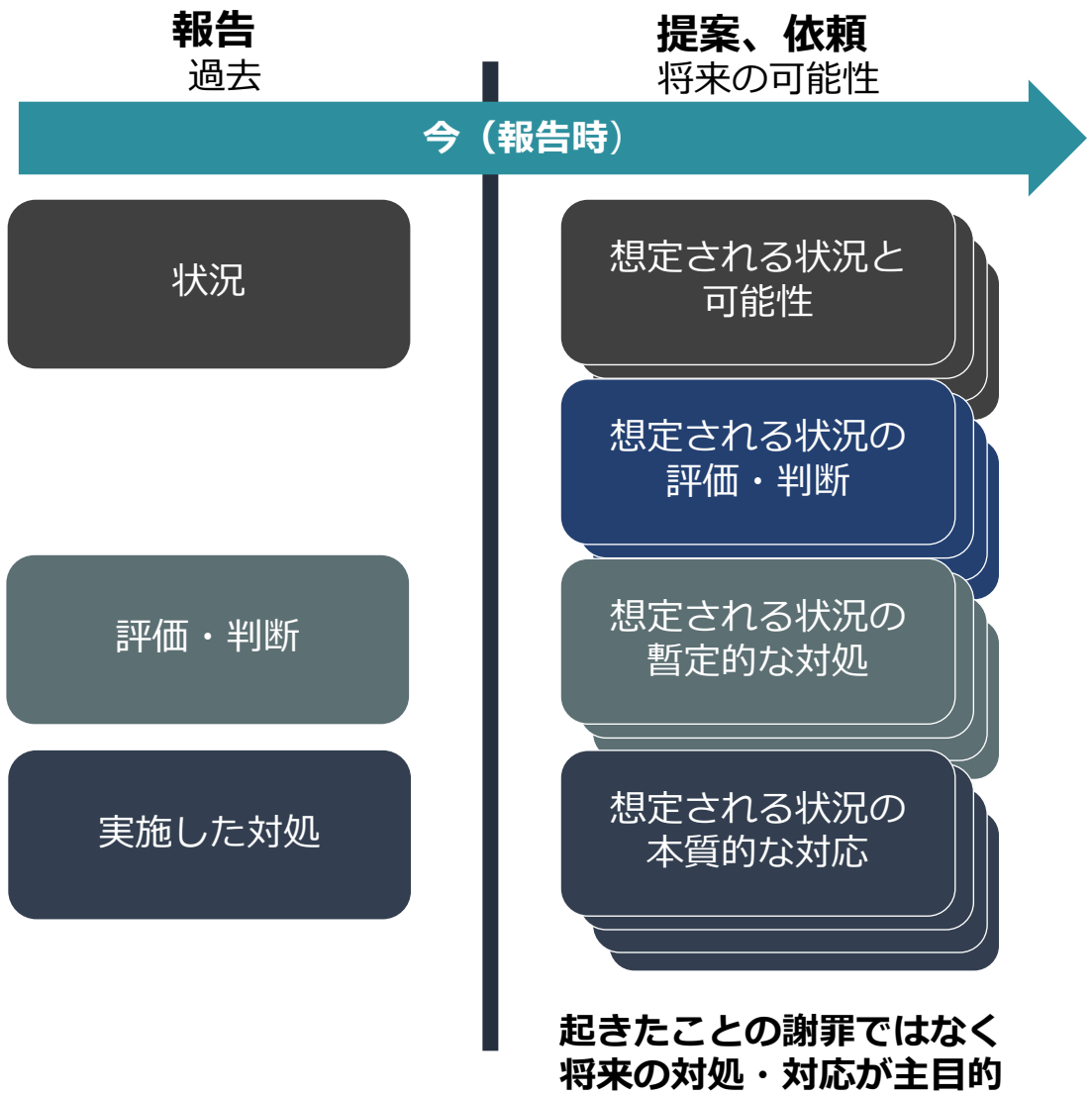
E2-c: 経営者向けの報告

- 更新したステータスレポートにもとづいて「経営者向けの報告」を作成してください。

- なお、ステータスレポートは、状況をまとめることを目的としているため、対応内容については言及していません。
- この点を念頭に置いて、経営者に伝えるべきこと、判断を仰ぐことを明確にしてください。

- スタッフが適時確認を行うので出来る限り対応をするようにしてください。

E2-c: 報告に関する留意点



いわゆる報連相のフォーマットでは、報告にならない点に注意してください。
単に状況や実施済みの対策を報告するだけではなく、経営陣などの報告先が、状況を把握し、必要な対応を判断し、対策を打つことにつながるように報告する必要があります。

報告のフォーマット例

XXXをご判断願います
- 放置すると〇〇〇になります
- これらの選択があり、適切と思われるものを提案します。
- 必要な費用はこのくらいです
- △△△部門の協力が必要なので、△△△部門への協力要請をお願いします

直接報告する上司をターゲットとせずに、報告した上司が、
その上司や取引先などに報告する状況を念頭に置いて報告する。

自身の裁量で手に負えないと判断したときは、指揮権の返上も提案する必要がある。
当事者としての行動は、必ずしも自分が決定を下すことではない。
上司が適切な判断が出来るように情報を整理すること、提言をすることも、当事者としての行動。

考察：報連相で良いのか？

報連相

「報連相」は、部門内、グループ内で解決すること、または、本来出来るはずのことについて述べられているように思われる。つまり、「提案」が含まれず、現状を報告し「指示」を仰ぐという構造になっている。Role & Responsibilityや専門性という概念はなく、報告を受けた上長が報告者のスーパーセットであることを前提としている。

- 報告
  - 報告とは、部下が上司に対して、仕事の進捗や状況、結果を伝えること
- 連絡
  - 連絡とは、部下が上司などに対して、客観的事実を周知すること
- 相談
  - 相談とは、ひとりでは判断に迷ったり困ったりしたことについて、意見を求める

I-SBAR

医療機関などで利用される報告のフレームワークSBAR, I-SBARでは、報告者の提案がRecommendationとして独立した項目となっており、Recommendationに基づいて、議論が行われる。
インシデントに関わる報告は、医療機関と同様に、Role & Responsibilityが重要であり、経営陣等の「判断」を求める専門家、Roleの責任者としての「提案」が含まれる必要がある。
「相談」は「提案」と似ているが、「提案」のない「相談」が許されるのは、いわゆる平社員のときだけ。

- I：Identify
  - 報告者、対象者の同定
- S：状況 Situation（What is happening)
  - 今何が起こっているか（What)
  - どのような経緯か（Why）
- B：背景 Background
  - どのような事情がこの状況をもたらしたのか
- A：評価　Assessment
  - 問題は何であるか
- R：提案　Recommendation
  - 問題の修正のために、どうしたらよいと思うか

「何のためにその報告をしているのか？」を考える｜新人ナースのホウレンソウ［4］｜看護roo![カンゴルー] (kango-roo.com)
https://www.kango-roo.com/learning/3561/

E2-c: CISOから経営者への報告

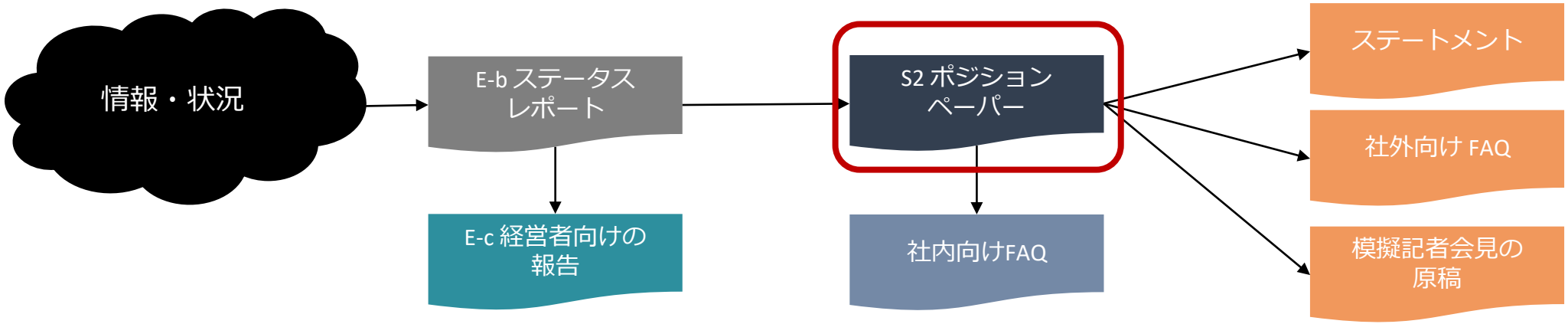
対応責任者				
事件・事故の概要				
影響を受ける事業	事業・インフラなど			
顧客や取引先への影響	影響の概要			
	影響を受ける被害者数と特徴		ワークアラウンド	
	想定される２次被害		被害者への補償	
事業への影響	事業の停止・再開の予定と根拠		事業レベルの対応 （営業停止、継続、縮退など）	
財務への影響	金銭損害、利益損害			
	費用・賠償・制裁金など			
	無形損害・その他			
事件・事故の経緯	事件・事故の原因・要因 （なぜ防げなかったのか）			
	実施した対処			
	対応のタイムライン			
	再発防止策			
責任関係	関係者の処分など			
対応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

セッション４
模擬記者会見の準備
ポジションペーパーの用意

S: ポジションペーパーを作るにあたって

ポジションペーパーの位置づけと目的

- 公表資料の整理
  - **ポジションペーパー：公表を前提とした、社内で情報を共有するための資料**
    - **当事者としてのスタンスで取り組む**
    - **確認できた”事実”が原則（憶測、推測は書かない）**
    - **実施できないこと、公表できないことは書かない（補償、復旧目途、その他）**
    - **自社だけではなく、顧客や関係者の損害を最小限にすることを意識する**
  - 社内向けのFAQ：想定される質問に対する共通した見解を述べるための社内向け資料
- 公表資料の作成
  - ステートメント：報道向けへの配布、ホームページでの公表等に使用する資料
    ステートメントは、公表できる内容のみを記載し、憶測や実現できない内容は記載しない
  - 社外向けのFAQ：ステートメントを補完するもので、メディアや顧客などに配布・公表する資料



S1: ポジションペーパーの作成

- 公表資料の基礎となるポジションペーパーをまとめてください。
- ステータスレポートや、経営者向けの報告書に基づいて、公表にふさわしい内容としてください。
  - 記者会見は、「誠意ある行動・態度、相手にとっての有益性を追求している姿勢を視覚的・聴覚的に伝え、早期の信頼回復につなげる*」ことが目的です。
  - 公表や記者会見の狙いを整理してポジションペーパーを作成していきください。
    - 「企業としての説明責任を果たす」では、不明瞭です。
    - 例
      - 被害者の損害を最小限にする
      - 二次被害の発生を防ぐ
      - 社会的な信用の失墜を防ぐ・最小限にする
      - 責任の所在を明らかにする

      顧客の利益を守る
      ユーザーの流出を防ぐ・最小限にする
      誤った風評を是正する
      法令等に基づいて実施する
- スタッフが、質問やコメントを入れるので、出来る限り対応をするようにしてください。

*出典：PR TIMES MAGAZINE: https://prtimes.jp/magazine/apology-press-conference/

S1: ポジションペーパー

項目		内容 （顧客や世間に向けたもの）
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	

セッション5
模擬記者会見の実施

S2: 模擬記者会見の実施

- CISO役の方に登壇者をお願いします
  - 本来は経営陣や事業責任者が会見を行います。会社を代表する立場を意識してください。
  - 他のグループの方、WGメンバーが記者役を担います。

- 司会が登壇者を呼び出しますので５分を目途にスピーチしてください
  - スピーチにあたっては、以下の点に注意してください。
    - 会社を代表する当事者であることを意識する。
    - 棒読みはせずに、自分の言葉で話す。
    - 専門用語は極力避ける。
- スピーチ終了後に司会が質疑応答を始めます
  - 質問は最後まで聞いてから答える。
  - 挑発的な質問にも冷静に対応する。
  - 失言に注意する。
    - 当事者意識のない発現：取扱説明書で警告、法的な問題はない、不正改造が原因
    - 法律や規制を軽視した発現：当社だけではない、たかが～です
    - 含みを持たせた発言：ノーコメント、ご想像にお任せします、～かもしれません

- 司会が記者会見を終了します
  - 一礼をして退席ください。

セッション６

ポストモーテム
改善計画の承認

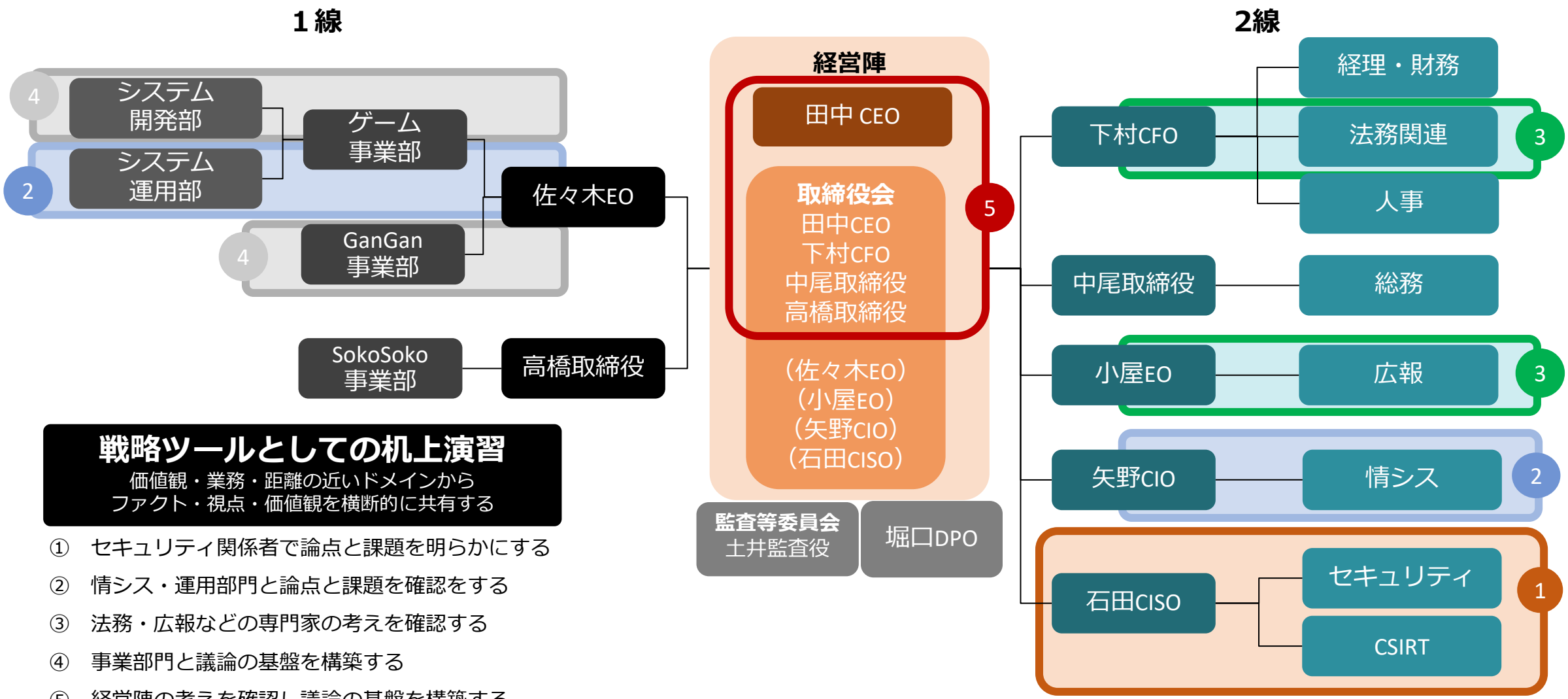
F: ラップアップ

セッション4

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	
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

組織図：なぜ机上演習なのか？

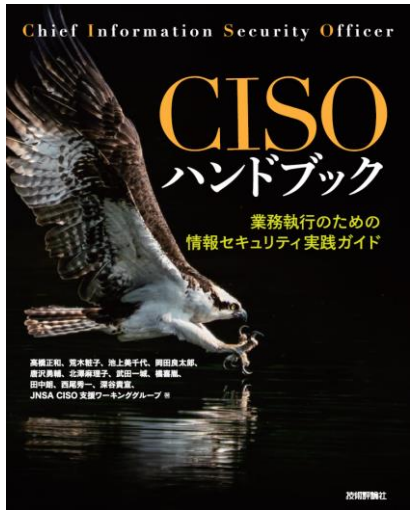


戦略ツールとしての机上演習

価値観・業務・距離の近いドメインから
ファクト・視点・価値観を横断的に共有する

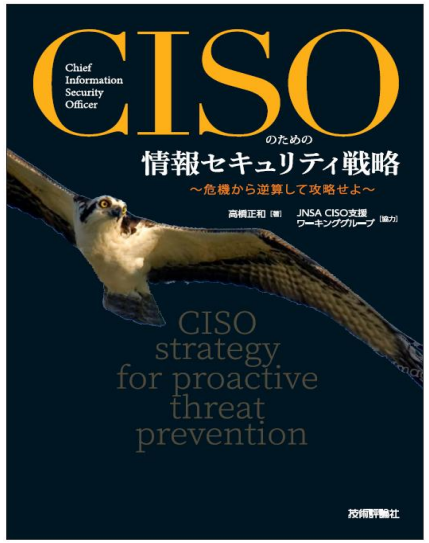
① セキュリティ関係者で論点と課題を明らかにする
② 情シス・運用部門と論点と課題を確認をする
③ 法務・広報などの専門家の考えを確認する
④ 事業部門と議論の基盤を構築する
⑤ 経営陣の考えを確認し議論の基盤を構築する

CISO支援WG関連書籍の紹介



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

JNSAからの公開資料

ワークショップで利用する資料など、CISOハンドブックや、CISO-PRACTSIEに関する資料は、JNSAのこちらのページで公開しています。

https://www.jnsa.org/result/act_ciso/index.html


Thank you