効果的なセキュリティ対策を目指すための第一歩

～ステークホルダー間のギャップとその背景～

JNSA 社会活動部会 CISO支援ワーキンググループ
株式会社Preferred Networks, Security Architect

高橋　正和

CISO支援WGの活動と本セッションについて

WGの活動概要と本セッション内容

- CISOを中心としたセキュリティ対策を具体化するための活動
  - ドキュメントの公開や書籍の執筆
  - 公表資料を実践するワークショップの開催
- WG活動を通じた気付き
  - CISO、エンジニア、経営陣、ベンダー間にギャップ
  - このギャップが、効果的なセキュリティ対策の壁となっている

- 本セッションの内容
  - CISO支援WGの活動
  - セキュリティ施策の有効性評価（机上演習）の概要
  - CISOに求められる業務執行の視座
  - 組織やプロジェクトの共通のゴールについて考察

料理で考える本講演の論点

料理人としてのシェフ
担当責任者としてのシェフ
経営者としてのシェフ

ソリューションのスキーム

Research
素材と鮮度の探求

Best of breed（最高の材料）
セキュリティ製品・サービス

ここにフォーカスしすぎてないか？

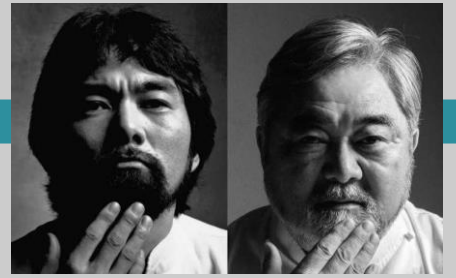
Research
器具と調理法の探求

Best Practice（最高の方法論）
セキュリティ規範・規準

専門家のスキーム

Skilled Operation
熟練の料理人

良い素材x良いレシピ＝良い料理



三流シェフ（幻冬舎） 三國清三

素材とレシピがあれば出来る？

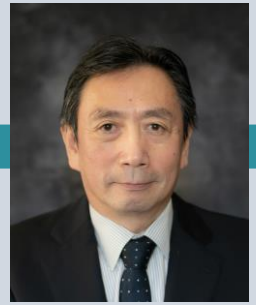
最高！

オーダーは、この料理なのか？

事業（ユーザー企業）のスキーム

Unskilled Operation
非熟練者

良い素材x良いレシピ≠良い料理



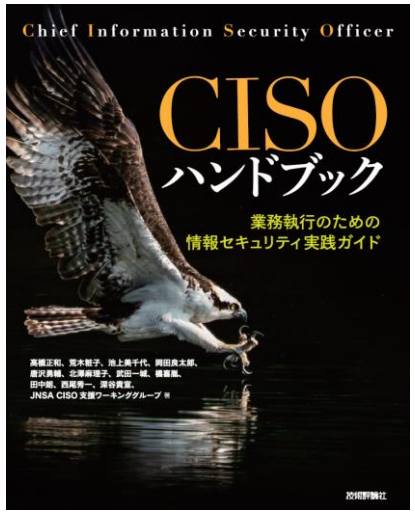
CISO

こいつをどうにかしないと
ダメなんじゃないか？

ひどい・・・

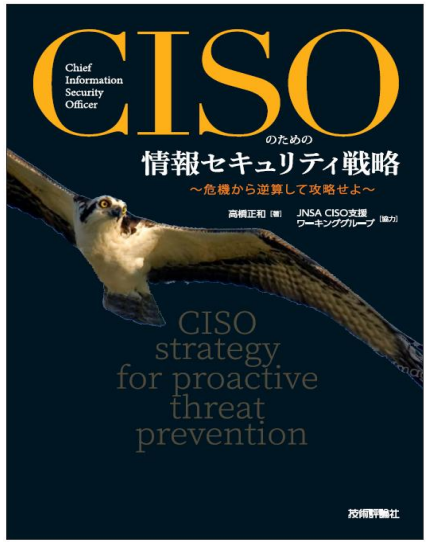
結果から考えないとダメ？

書籍の執筆



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

CISO-PRACTSIE 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
  - 具体的な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…

- 2023/09/XX 企業向けワークショップ（非公開）
  - 参加　12名＋α　（全員 セキュリティ資格保有者）
  - 社内のセキュリティスペシャリスト
  - 高い専門性を感じると共に、専門領域の外への関心の薄さを感じた

CISO-PRACTSIEマテリアルの公表

CISO-PRACTSIEワークショップ用マテリアル
（CISO支援ワーキンググループ）

2023.7.14掲載

「CISO-PRACTSIEワークショップ用マテリアル」について

本資料は、2023年１月に出版した「CISOのための情報セキュリティ戦略」*1で掲載した、机上演習を行うためのマテリアル（フォーマットなどのドキュメント群）の見直しを行い、ワークショップ進行用の資料を追加したもので、以下に記載するクリエイティブ・コモンズ（表示-非営利-継承）*2の元で公開いたします。

「営利目的の利用」「転載・引用」「資料内容に関するお問い合わせ」については「報告書の転載・引用連絡（JNSA）」（リンクはこちら>>）からご連絡下さい。「営利目的の利用」でのお問合せの場合は、「８．引用部分 」の自由記入欄にご要望をご記入ください。

CISO-PRACTSIEワークショップ用マテリアル

ドキュメントの内容は、「01 ワークショップ進行用資料」に記載されています。2ページ目の「資料　ドキュメント名」と照らして参照下さい。
ご自身の企業にあった内容に修正して活用いただけるよう、Word形式で提供しています。

- 01 ワークショップ進行用資料　（PDF）>>
- 02-1 ワークショップ用-仮想企業設定（抜粋）（印刷用抜粋資料）　（Word）>>
- 02-2 ワークショップ用-仮想企業設定（全体）　（Word）>>
- 03 セッション２関係者の見解　（Word）>>
- 20 アウトプット　（Word）>>
- 21 アウトプット（サンプル）　（Word）>>
- 00 license-ライセンスの説明　（PDF）>>

https://www.jnsa.org/result/act_ciso/2023/index.html

誰が読むかはともかく、
英語版も公開予定！

CISO BRIDGES

- CISO、経営者へのインタビューというのを少しやりました。
  - Business and Risk-management Integration for Developing Growing Enterprise Security
- この活動は、今後も継続していく予定です。

CISO支援WGの主な成果物

CISO支援WG

X ポスト

▶2023/7/14

報告書 2023年１月に出版した「CISOのための情報セキュリティ戦略」で掲載した、机上演習を行うためのマテリアルを見直し、ワークショップ進行用の資料を追加した**「CISO-PRACTSIEワークショップ用マテリアル」**を公開しました。

▶2023/1/12

書籍発売 **「CISOのための情報セキュリティ戦略」**技術評論社より出版されました。

会員限定ワークショップ開催

「CISOのための情報セキュリティ戦略」で紹介した、机上演習を通じて自社のセキュリティ施策を評価する**「CISO-PRACTISEワークショップを開催」**しました。

▶2021/1/20

書籍発売 **「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」**技術評論社より出版されました。

▶2019/9/10

成果物公開 中小企業の CISO やセキュリティ担当者が、セキュリティに関わる業務を執行し、経営陣と適切なコミュニケーションを進めるうえで明確にすべき項目と内容を例示した**「MY CISO ハンドブック」**を公開しました。

▶2018/9/1

JNSA Press寄稿 JNSAが発行する会報誌「JNSA Press46号」で**「CISO 支援ワーキンググループの紹介」**を掲載しました。

▶2018/5/11

成果物公開 CISOが経営陣の一員としてセキュリティ業務を執行する上で前提となる、経営の基本的な枠組みを整理し、明確にすべき目標と指標、そして施策を評価する判断基準を提供する **「CISO ハンドブック」**を公開しました。

こちらに年度をまたいで、まとめていただいています。

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

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

CISOのための情報セキュリティ戦略

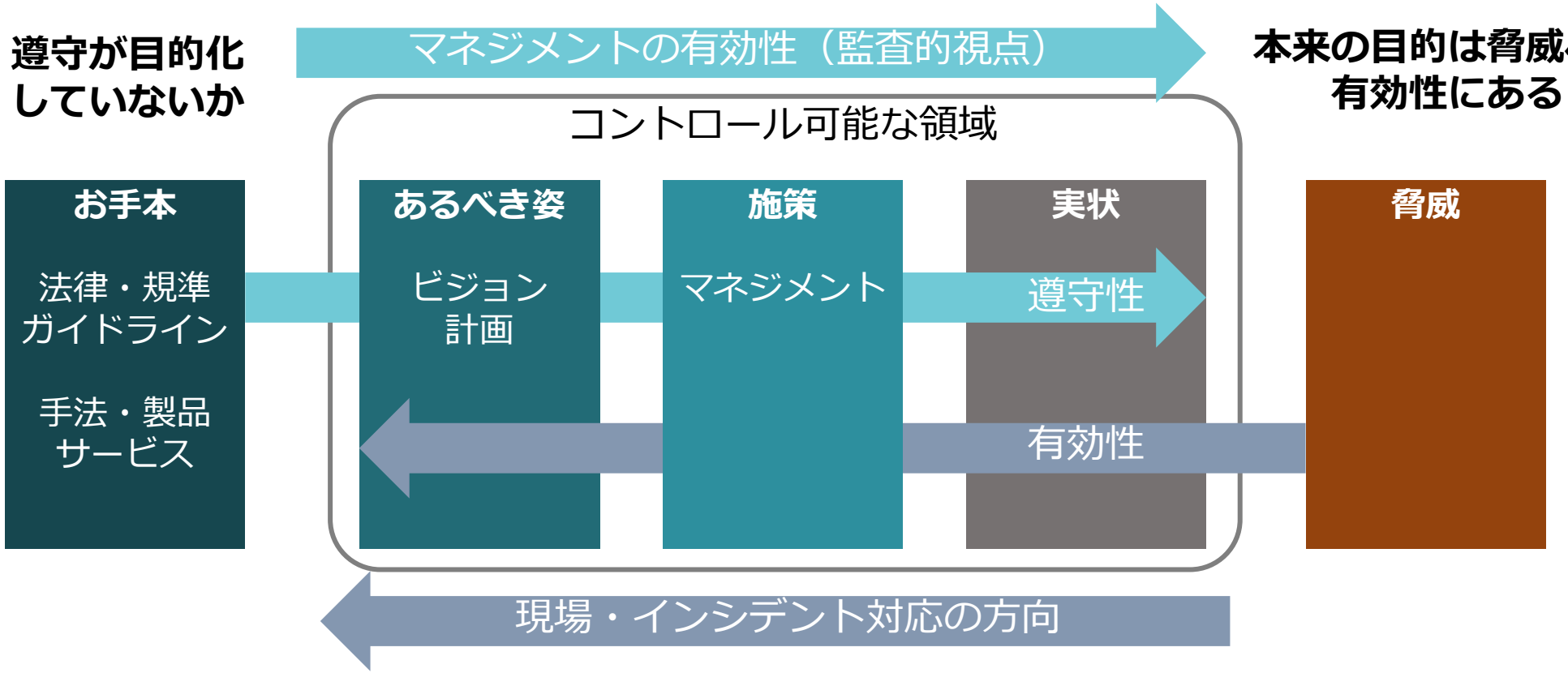
CISO-PRACTISEの目的とゴール

- 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

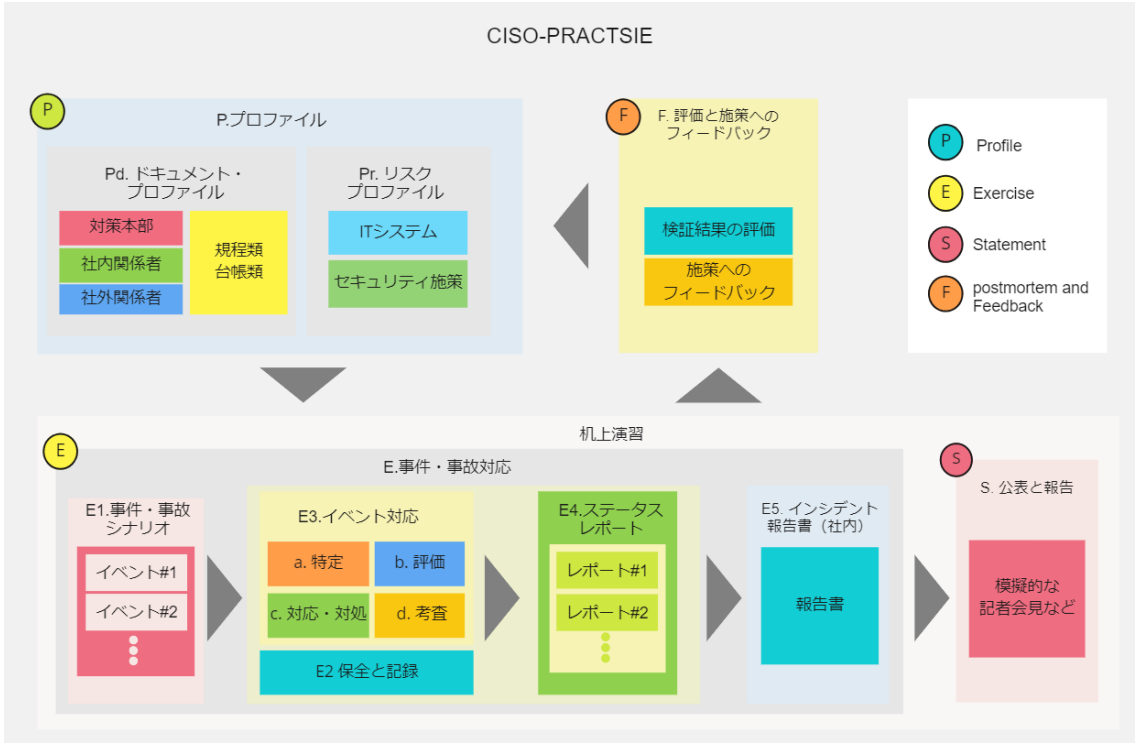
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

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



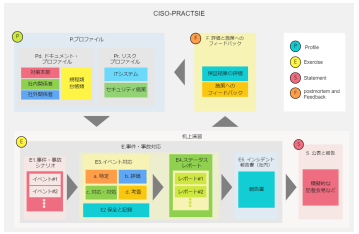
OUTPUT

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



P **プロファイル**
規程類、施策、計画
プロファイル

イベント
シナリオの把握

ディスカッション

CSIRT
E
状況の整理
ステータスレポート

社内ステークホルダ
事業部門
スタッフ部門
法務、広報、人事
社外の専門家など
CISO
経営陣への報告
報告書

経営陣/経営者
公表内容の作成と経営陣の承認
ポジションペーパー

S
顧客・世間
メディア
監督官庁など
公表内容
（模擬記者会見）
模擬記者会見の実施
ステートメント, QA

ポストモーテム
（振り返り）
F
ポストモーテム・計画の承認
改善計画書

- 会社の状況、セキュリティ施策、経営計画など、対応を行うため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、意見を交換します

- 関係者に確認する項目を確認し、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に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

- 模擬会見から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

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

- 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

E1-a:ディスカッション

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	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）		

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

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

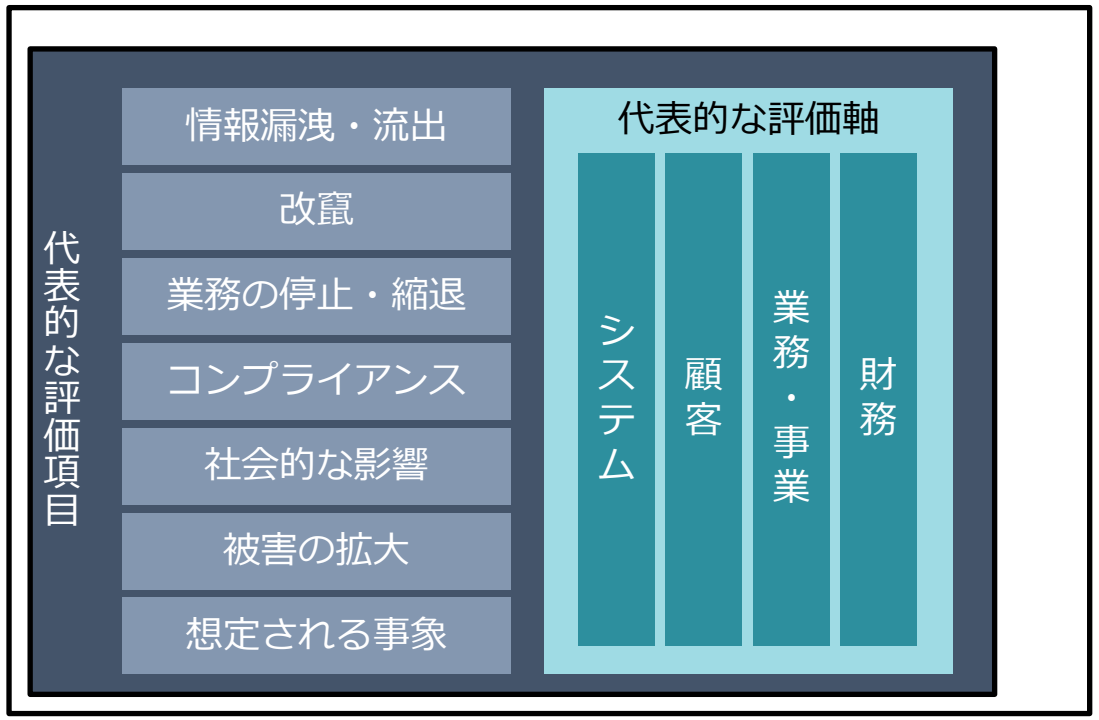
E2-a:ディスカッション-2

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** ● **警察には届けますか**
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

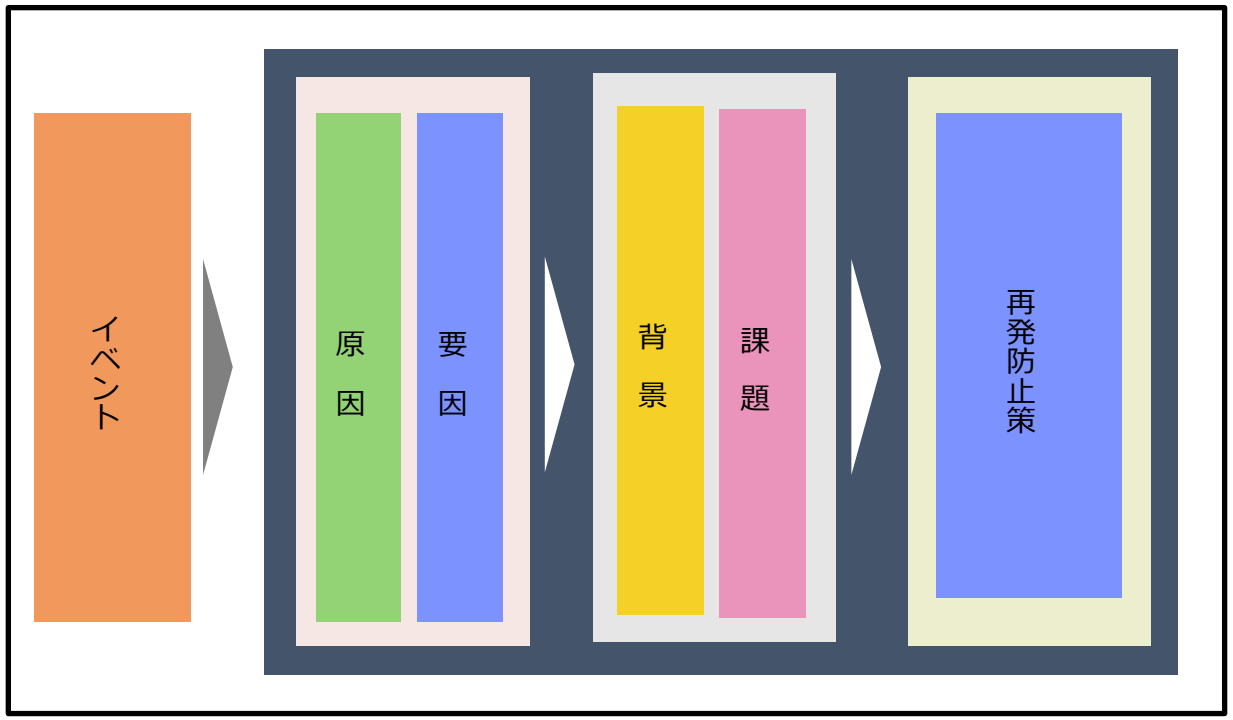
E-b:状況と必要な対応の把握

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



E-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

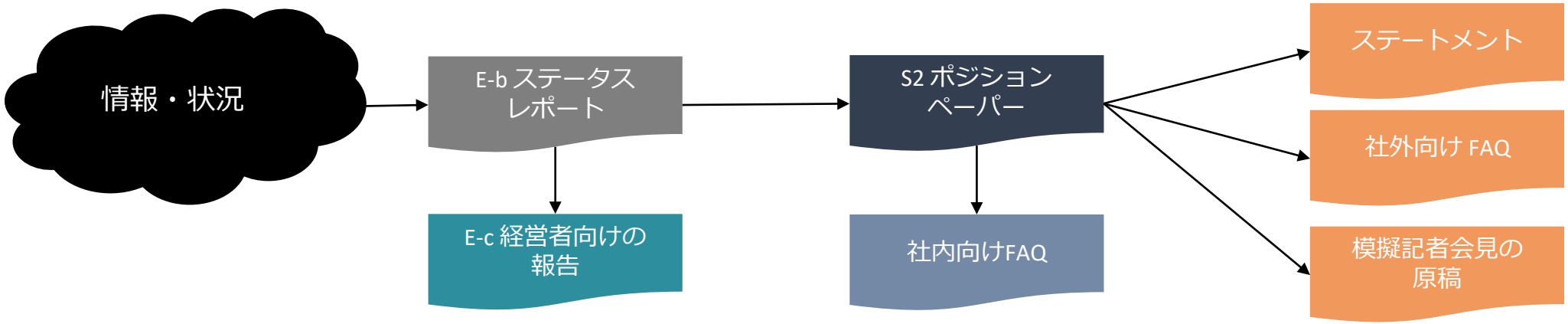
可能性

occur	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
low	起きる可能性は低い
-	起きる可能性はない

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の担当者の資料
- 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：公式な公表を前提とした、社内で情報を共有するための資料
  - 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



E-b:状況の把握（ステータスレポート1/2）

対象事業	(b)-1 事業の概要	事業の名称（　　）担当責任者（　　）　売上（　　）顧客数（　　） 事業概要：		
	(b)-2影響を受ける情報の種類	□個人情報　□クレジットカード情報　□顧客の機密情報　□自社の機密情報 □ 公表済みの情報　□ 特定が困難（端末・メール等）□ その他　□ 不明		
	(b)-3 システム停止の影響		(b)-4コンプライアンス	
	(b)-5社会的影響		(b)-6その他	
事業への影響	(s)-1対応レベル(RACI)	- 経営陣 - 事業担当執行役員等 - 広報　- 情シス　– CSIRT　– CISO　- 法務・知財　- 人事　- 社員全般		
	(s)-2 状況・概要	*イベント・インシデントが事業に与える状況の概要を記載*		
	(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	*対応の状況や背景について記載*
	(s)-4 顧客・取引先の被害	□ 金銭的な被害　□ 詐欺行為など　□ 機密情報の漏洩　□ 業務停止　□ 脅迫行為　□ その他　□ なし　□ 不明		
	(s)-5 自社の被害	□ 金銭的な被害　□ 詐欺行為など□ 機密情報の漏洩　□ 業務停止　□ 脅迫行為（身代金） □ 信用の失墜　□ 社会的責任　□ その他　□なし（軽微）□ 不明		
	(s)-6 深刻度	□ S:既に深刻な状況　□ A:深刻な影響の可能性　□ B:一定の影響がある可能性) □ C:軽微な影響の可能性　□ D:実質的な影響はない　□ その他		
	(s)-7 緊急度	□ S:即時対応　□ A:24時間以内の対応　□ B:3日(72時間)以内の対応　□ C:1週以内の対応 □ D:特段の対応は必要ない□ その他		
顧客への影響	(i)-1 影響の概要	*影響を受ける情報・データがある場合、その概要を記載*		
	(i)-2 影響の状況	データ量：*データ量について記載* 被害者数：*影響を受ける被害者数*	(i)-3 影響を受ける被害者の特徴	*被害者を特定するための特徴などを記載*
	(i)-4 想定される二次被害	*懸念される二次被害について記載*	(c)-1 被害の確認方法	*影響を確認する方法を記載*
	(c)-2 被害者のワークアラウンド	*すぐに実施できる回避策、軽減策*	(c)-3 被害者が実施できる対策	*被害者が実施できる対策*
	(r)-5 外部の専門家	□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　□ 保険会社　□ 特に必要はない		

E-b:状況の把握（ステータスレポート2/2）

財務への影響	(f)-1直接的な損害	■金銭損害 身代金　詐欺被害　搾取	■利益損害 直接的的な機会損失	間接的な機会損失
	(f)-2費用・賠償・制裁金等	■費用損害 事故原因調査・対応、広告・宣伝、 コールセンター、見舞金等	■損害賠償 賠償費用、弁護士費用等	■行政損害 個人情報保護法、GDPR/CCPAなど
	(f)-3 無形損害・その他	■無形損害 ブランド棄損、株価	■その他	
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、報告先、時間的な制約	□ 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	取引先名、先方担当者、自社担当者	□ 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	自社担当者：	□ 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	影響を受けない利用者等	*影響を受けない利用者への対応を記載*
当該システム	(t)-1 システムの名称・概要	■名称、■責任者（事業、技術）	■システム概要	
	(t)-3 情報流出の懸念	*情報流出の懸念について記載*	(t)-4 システム停止の懸念	*システム停止の懸念、必要性について記載*
	(t)-5 システム侵害の懸念	*攻撃が継続、拡大する懸念*	(t)-7事故の原因・要因	*事件・事故の原因・要因を記載*
	(t)-8 再発防止策	*再発防止策について記載*		

E-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				

CISO-PRACTSIEワークショップ用マテリアル
https://www.jnsa.org/result/act_ciso/2023/index.html

S2:模擬記者会見・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	

CISO-PRACTISEでみえてきた

CISOに求められる業務執行の視座

CISOの育成に向けて.

ワークショップ参加者からのフィードバック

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。
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）	• 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。 • 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
ワークショップで改善すべき点を挙げてください	• 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 • 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
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」があり、
CISO以外の方々から、CISOを育成する視点が欲しい、との要望があった。

ワークショップにみる傾向

これまでに実施したワークショップにみられた傾向
（あくまでも、個人の感想で、若干誇張しています）

現役CISO

- ワークショップの狙いに沿った内容になった
- 会社としての立場で、考える習慣が見られた
- 対応は違っていても、意外なほど論点が共通していた（プロトコルがありそう）

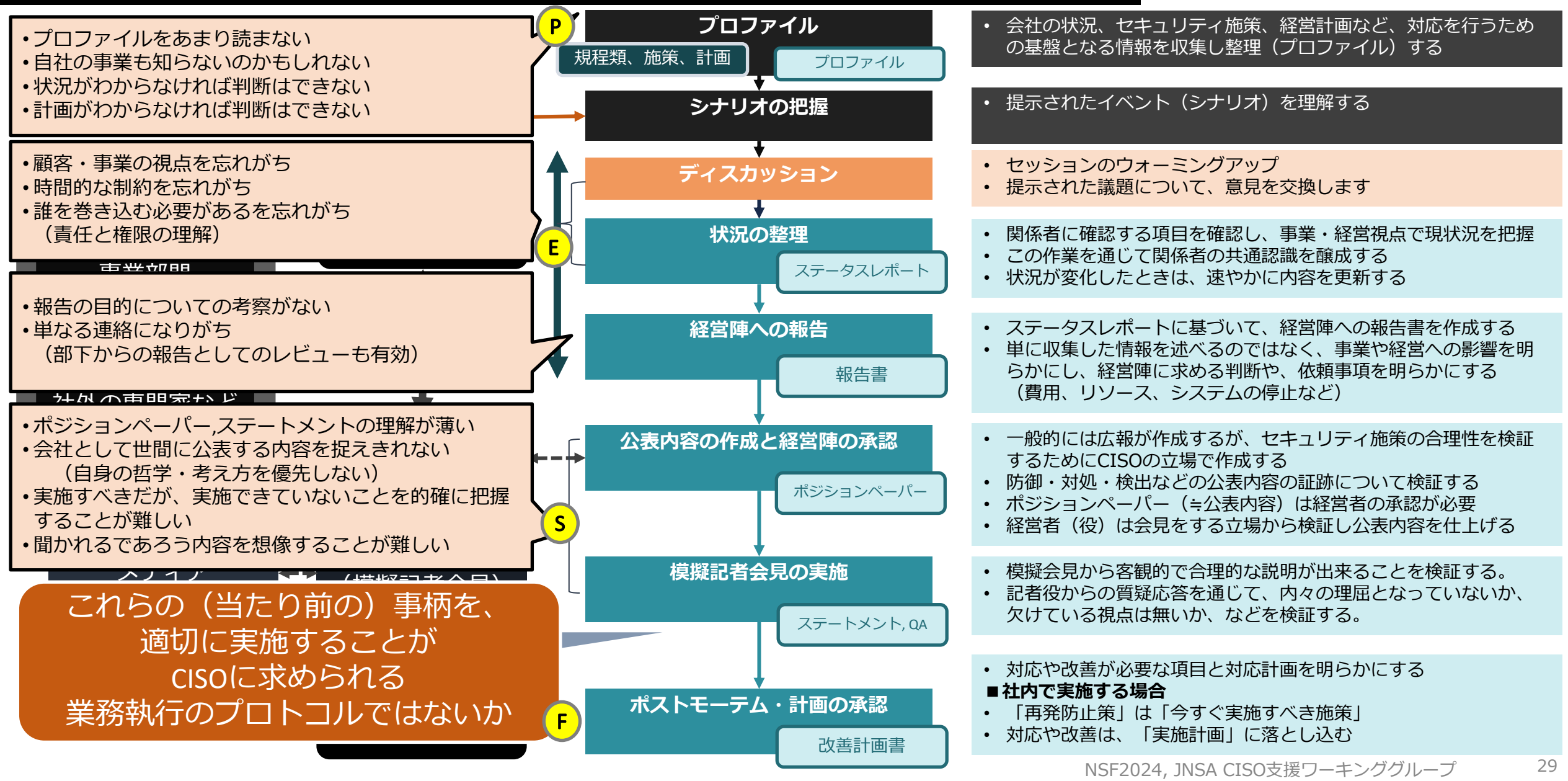
セキュリティベンダー

- 会社状況への興味が薄い（当事者感が薄い）
- 正解を探す傾向にある
- 報連相に終始する傾向にある
- 企業を代表する立場への認識が薄い
- ある意味、当然の傾向だが、ユーザ企業とベンダーの溝は、この辺りに要因がありそう

社内のセキュリティ担当者

- 自身のロールに求められる範囲で判断をする傾向にある
- 必ずしも、事業への興味を感じない
- 報連相に終始する傾向がある
- 企業を代表する立場への認識が薄い
- ある意味、当然の傾向だが、「経営者がセキュリティを理解していない」と感じる要因は、この辺りにありそう

CISOと担当者のありがち違い



- プロファイルをあまり読まない
- 自社の事業も知らないのかもしれない
- 状況がわからなければ判断はできない
- 計画がわからなければ判断はできない

- 顧客・事業の視点を忘れがち
- 時間的な制約を忘れがち
- 誰を巻き込む必要があるを忘れがち
  （責任と権限の理解）

- 報告の目的についての考察がない
- 単なる連絡になりがち
  （部下からの報告としてのレビューも有効）

- ポジションペーパー,ステートメントの理解が薄い
- 会社として世間に公表する内容を捉えきれない
  （自身の哲学・考え方を優先しない）
- 実施すべきだが、実施できていないことを的確に把握することが難しい
- 聞かれるであろう内容を想像することが難しい

これらの（当たり前の）事柄を、
適切に実施することが
CISOに求められる
業務執行のプロトコルではないか

- 会社の状況、セキュリティ施策、経営計画など、対応を行うため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、意見を交換します

- 関係者に確認する項目を確認し、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に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

- 模擬会見から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

CISOの育成はできるのか？

- テンプレートを用意すれば、自動的に解決すると思っていたが…
  - どうも、そうでもないようだ

- 本を読んでも自転車に乗れるようにならない*
  - もしかして、CISOに就くまではCISOになれないのではないか
  - しかし、何の準備もなしにCISOを担えるものでもない

- CISOになればよいという物でもないけれど…
  筋がわかるようになれば、少し幸せに近づくんじゃないか？

- ワークショップでの気づきから、提言としてまとめると…

*「経営」の目線ができないのは「お金」と紐づきすぎているから　デザイナーが起業してわかった、本当にお金をかけるべきこと - ログミーBiz (logmi.jp)
https://logmi.jp/business/articles/329245

CISOに対する提言

- コミュニケーション：巻き込み方が重要
  - 全役員と一斉に情報共有する仕組みが必要
  - 上司が先に知っていると厄介なので、報告が早くなり、対応も早くなる
- 具体的な情報を確認しておこう
  - 演習で言うところのプロファイリングは重要
  - CSF*などでいうインベントリの一部に相当する作業
- オープンな場を心がけよう
  - むやみに怒ると、状況が上がってこなくなる
- 会社の代表としての視点を持とう
  - 経営者の視点を持って考えることが必要
  - セキュリティを成功要因（Business Enabler）として位置づける

- ワークショップの狙いに沿った内容になった
- 会社としての立場で、考える習慣が見られた

- 対応は違っていても、意外なほど論点が共通していた（プロトコルがありそう）

CSF*: NIST Cyber Security Framework

社内のセキュリティ担当者に対する提言

- 自社の事業に興味を持とう
  - 自分の会社の売上も知らないのはどうだろう
  - どんな事業を行っているか、
    どんな人が事業をしているかに興味を持とう
- 上司の上司の視点を持とう
  - 上司の上司に報告できるような報告を心がけよう
    - 「報連相」から「報連相＋提案」に
    - 提案が入らない報告を受けるとつらいよ
  - 「正しい」ことより望ましい結果を目指すことが重要

- ステークホルダーとのコミュニケーションに注意しよう
  - だれがステークホルダーかを知ろう
  - 相手に何をして欲しいか（要望や判断）を明確にしよう
  - 専門用語を使わないで説明を心がけよう
    - 相手にとってのインパクトが伝わるか
    - 相手の立場を考慮した説明が出来るか

- 自身のロールに求められる範囲で判断をする傾向にある
- 必ずしも、事業への興味を感じない
- 報連相に終始する傾向がある
- 企業を代表する立場への認識が薄い

- ある意味、当然の傾向だが、「経営者がセキュリティを理解していない」と感じる要因は、この辺りにありそう

セキュリティベンダーに対する提言

- 顧客の状況に対して興味を持とう
  - 契約形態にもよるけど、事業概要くらいは調べよう
- ソリューションに期待される事、期待に応えていない事を知ろう
  - 単にソリューションの説明に終始していない？
    - 本社のプレゼンそのまま使ってない？
  - ソリューションの位置づけをきちんと伝えよう
    - 出来ること、出来ないこと、必要なオペレーション
- 正解を求めるのではなく…
  - 適切さを求めるのが良さそう
- 担当者目線だけでなく、CISO目線で対応しよう
  - 担当者がCISOや上司に説明できる資料を心がける

- 会社状況への興味が薄い（当事者感が薄い）
- 正解を探す傾向にある
- 報連相に終始する傾向にある
- 企業を代表する立場への認識が薄い

- ある意味、当然の傾向だが、ユーザ企業とベンダーの溝は、この辺りに要因がありそう

CISO支援WG
次のステップ

次のステップ

- CISO-PRACTSIEマテリアルの英語版を出す！
  - 誰が読むか分からないけど　　まもなく公開、協力者絶賛募集中！
- シナリオを増やす
  - ランサムだけでは物足りない
- 海外を含めた類似の資料との比較を試みる
- CISO BRIDGESの継続
  - 対応いただける経営者、CISO、CTOなど募集してます!!

- ゆる～～～いWGですが、メンバー募集中です
  - sec@jnsa.org までご連絡ください。

Security Days W4-01 緊急告知！

Security DaysでCISO-PRATSIEワークショップ開催します！

- CISO-PRACTSIE
  セキュリティ施策の有効性評価のためのワークショップ
  - 高橋 正和、池上 美千代、唐沢 勇輔 、桐本 直樹、
    田中 朗、戸田 勝之、中村匡秀、深谷 貴宣

  - W4-01：3.15(金) 10:40-11:20
    - https://f2ff.jp/introduction/8757?event_id=secd-2024-01-Tokyo


Thank you