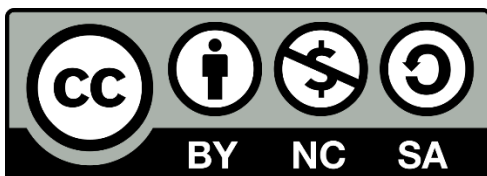


CISO-PRACTSIE

ご利用いただくにあたって

JNSA 社会活動部会 CISO支援ワーキンググループ

Copyright and License



著作権 © 2023-2024 JNSA CISO支援ワーキンググループ. 本著作物は、Creative Commons Attribution Share-Alike 4.0 ライセンスの下で公開されています。再利用や配布を行う場合は、この作品のライセンス条項を明らかにする必要があります。営利目的の利用をご検討される場合は、JNSA(sec@jnsa.org)までご相談ください。

Copyright © 2023-2024 The JNSA CISO support working group. This document is released under the Creative Commons Attribution Share-Alike 4.0 license. For any reuse or distribution, you must make it clear to others the license terms of this work.

Please contact the JNSA(sec@jnsa.org) when considering commercial use.

本マテリアルの位置づけ

CISO-PRACTSIE*は、CISOやセキュリティ責任者に利用いただく事を想定したもので、机上演習を通じて組織内でセキュリティ施策の評価を行い、必要な施策を明らかにすること、部門間、担当間のコミュニケーション基盤を構築することを狙ったものです。

しかし、机上演習を開催には、主催者側に一定のスキルが必要とされます。初めから多くの参加者を募っても成果を上げることは難しく、また、自社の状況に応じた机上演習を行うためには、主催者が事前に机上演習を経験することが必要です。

本マテリアルは、主催者が自社を題材とした机上演習を行うための準備として、仮想企業「JNSA アーキテクト」を題材に、簡単な攻撃シナリオを使って、CISO-PRACTSIEワークショップ（以下、本ワークショップ）を経験し、組織内で机上演習を展開するための第一歩となる事を目的としています。

まずは、本ワークショップを通じて、机上演習の進め方や手順、必要な材料や関係者などを理解いただき、自社を題材とした机上演習に展開してください。

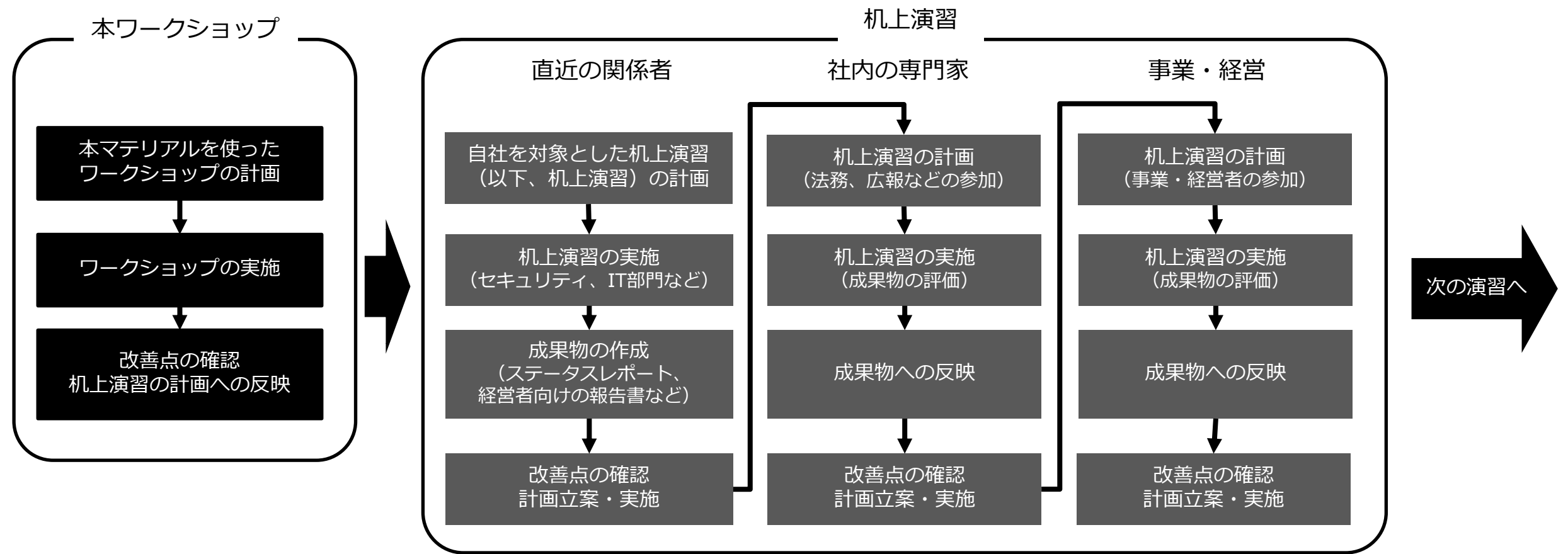
利用いただいた皆様からのフィードバックもお待ちしております。
sec@jnsa.orgまで、CISO支援WG宛と明記してご連絡ください。

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

机上演習への展開（図）

本マテリアルの主要な対象

各組織における、自組織を対象とした机上演習



ワークショップ用マテリアル

本マテリアルは、以下のドキュメントで構成しています。

- 主催者向け資料
 - 00 本資料について.pdf
 - 本マテリアルの概要とライセンスについて記載しています。
 - 10 ご利用いただくにあたって.pdf
 - CISO-PRACTSIE全体の構成と、本ワークショップの位置づけ、ワークショップの開催や、社内へ展開する際の留意点などを記載しています。
 - 12 CISOハンドブック概要
 - CISOハンドブックの概要を記載しています。
- ワークショップ用資料（配布資料）
 - 20 ワークショップ進行用資料.pdf
 - ワークショップの主要な資料で、この資料を中心にワークショップを進行します。
 - 30 サンプルアウトプット.docx
 - 報告のフォーマットで、ステータスレポートは記入例としています。
 - 31 サンプルアウトプット-更新例.docx（「E2-b: レポートの更新」の後に配布）
 - ステータスレポートの更新例です。
 - 状況に応じて、どのようにステータスレポートを更新するかを例示しています。

机上演習への展開のポイント

本ワークショップを、社内の机上演習に展開する上での留意点を以下に記載します。

- 段階的に実施する（当ワークショップから始める）
 - 最初から、事業責任者や経営陣が参加するのは、良いアイデアではありません。
 - セキュリティ関係者、IT関係者、法務や広報などの専門家、事業関係者、経営陣等に対して、有効な議論が出来るように、段階的に参加者を増やし、論点を技術から事業に移すようにしてください。
 - 段階的な取り組みの最初の一步として、本マテリアルを使ったワークショップを活用してください。
- 目的やゴールを明確にする（全体および、各段階）
 - 具体的な目的を持たずに机上演習を行うと、単なるブレインストーミングに終始し、成果につながりません。
 - 主催者は、目的とゴールを明確にし、参加者にも伝えてください。
 - なお、机上演習それぞれの目的とゴールだけではなく、最終的な目的とゴールも意識してください。
 - 組織内で実施する場合は、些末な議論が長引きやすく、目標やゴールに到達することが難しい面があります。この点を配慮して、机上演習の計画を立ててください。
- 成果物に落とす
 - 多くの場合、机上演習の成果は打ち上げと共に消えてなくなります。
 - 机上演習で明らかになった課題に対して、規程類の策定や見直し、実施計画の策定など、具体的なアクションにつなげてください。

机上演習への展開の例

本ワークショップから、社内の机上演習へ展開する手順を、以下に例示します。

1. セキュリティ関係者で本ワークショップを実施する
2. 自社のシナリオを策定し、机上演習を計画し、実施する
 - a. セキュリティ関係者、IT関係者で机上演習を行い、ステータスレポートを策定し、経営者向けの報告書を作成する。
 - b. 報告書に対して、法務、広報、事業部門の意見を確認し、必要な修正を加える。
 - c. 経営者から、報告書やポジションペーパーのレビューを受ける。
 - d. 組織としての意思決定に必要な方々が参加する机上演習を実施する。
 - e. 机上演習で明らかになった課題に対して、実施計画を策定し対策を進める。
3. 次の机上演習を計画し、実施する
 - a. 明らかになった課題に応じた机上演習を計画し、これを実施する。

本ワークショップの
実施にあたって

ワークショップ実施のポイント

本ワークショップを実施する上での留意点を以下に記載します。

- ワークショップは結構大変です
 - 特に組織内の場合は、ポジションや職制から、混乱が生じやすいと言えます。
 - ワークショップを実施するためには、それなりの準備が必要となります。
- 事務局（推進グループ）を作ってください
 - あらかじめ、ある程度内容を理解した事務局（推進グループ）を構成してください。
 - ファシリテーターの他に、サポートメンバーがいると、ワークショップを進めやすくなります。
- 目的・ゴールを明らかにし、事前に参加者と共有してください
 - ワークショップを開催する目的やゴールを明確にし、事前に参加者と共有してください。
 - 参加者が期待している内容にずれがあると、ワークショップの進行が難しくなります。
- 半日～1日かかります
 - CISO支援WGで、当ワークショップを2.5時間で実施しましたが、時間が足りないとのご意見を頂きました。
 - はじめて取り組む場合は、最低でも半日（4時間程度）は見込む必要があります。
 - 参加者の構成、参加可能な時間、議論すべき内容などに応じて、参加者と参加時間を設計してください。
- グループの構成
 - 目的・ゴールにたどり着きやすいグループ構成を設計してください。
 - 特に組織内の場合は、活発な意見交換が出来るように、お立場や参加者の関係性への配慮が必要です。

ワークショップアジェンダの例

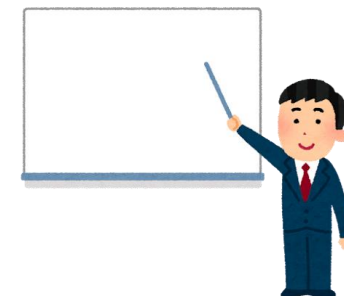
2024年3月に、Security Daysで実施した際のタイムテーブルです。
2時間半で実施しましたが、多くの参加者から時間が足りなかったとのご意見を頂きました。
余裕を持ったタイムテーブルとすることを推奨します。

時間（分）			項目	アウトプット
10:00	10:20	20	オリエンテーション 自己紹介、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	ワークショップの説明と、準備を行います
10:20	10:45	25	セッション1：ランサムウェア-1 (単純感染)	ディスカッション-1：ランサムの対応（端末） ステータスレポートの説明
10:45	11:25	40	セッション2：ランサムウェア-2 (事業の停止)	ディスカッション-2：ランサムの対応（全社） ステータスレポートの更新 経営陣向け報告書の作成
11:25	11:35	10	休憩	
11:35	11:50	15	セッション4：模擬記者会見準備	ポジションペーパーの作成
11:50	12:20	30	セッション5：模擬記者会見	経営者役としての参加者が記者会見を実施 経営者役以外の方は記者役として質問を行う
12:20	12:30	10	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

ワークショップ TIPS

ワークショップを開催する際の、運営上のTIPSを以下に記載します。

- マテリアルは印刷する
 - 机上演習では、マテリアルを印刷し、印刷した紙に書き込んでもらう段取りがスムーズでした。
 - 電子データでも良いのですが、一人のトラブルで、全体の進行が遅れてしまいます。
- 用意しておく便利なもの
 - プロジェクタ・大型TVなど
 - 進行資料の表示などに利用します。
 - ホワイトボード
 - 進行する上で、なにかと便利です。
 - マイクとスピーカー
 - 小さな会場では必要ありませんが、あった方が進行が楽になります。
 - 筆記用具
 - 筆記用具：書き込むためのボールペンなど
 - 付箋紙：大・小
- 作業終了時間の明示
 - 各セッションで作業を行いますが、終了時間をホワイトボードに書くなど、参加者がわかりやすいように明示してください。
 - 例：10:45まで！



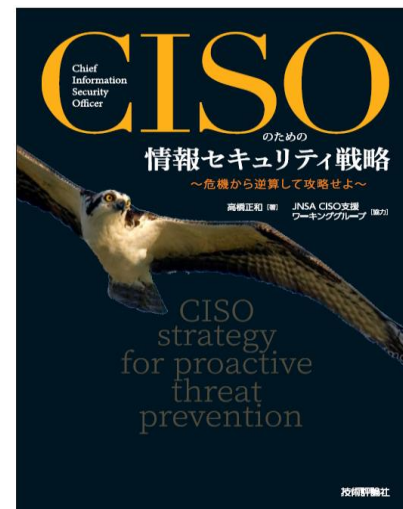
CISO-PRACTSIE関連書籍

ワークショップを始める前に、ぜひCISO支援WGから出版した以下の書籍をご参照ください。
CISO業務についての全体像、机上演習を戦略として社内展開する上での論点をまとめています。



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

An aerial photograph 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