ش χ ʊ Ă خ Б › Щ

03

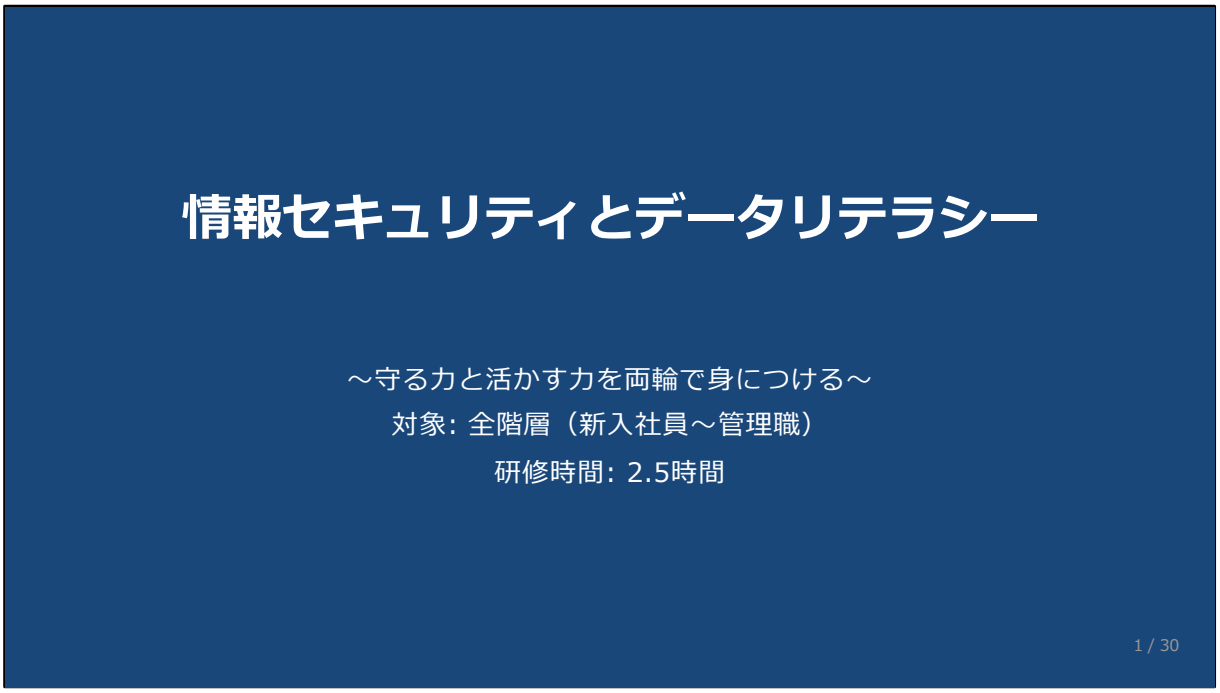
Л І þ а е Б ŧ о
В › Њ е Б д Ђ ›

غم ◗ Щ Ж а б ж

REFERENCE

M26_03

INSTRUCTOR GUIDE SERIES



【開始前の準備 / 所要5分】
- 受講者を4～5名のグループに分けておく（可能であれば部署・階層をミックス）
- 配布資料：ワークシート（3種類）、インシデント対応フローカード
- Wi-Fi接続情報を掲示（演習でデータ分析のデモを行う場面あり）
- 「今日はセキュリティとデータの"両方"を学びます。どちらも皆さんの日常業務に直結するテーマです。IT部門だけの話ではなく、全員が当事者です」と声かけ
- 全階層共通のため、受講者の役職・経験年数にばらつきがある。セキュリティ担当者がいれば、ワーク時にグループ内でアドバイザー的な役割を依頼すると効果的
- 本プログラムは共通01「DXリテラシー基礎」や共通02「AI活用入門」と一部テーマが接するが、本研修は「セキュリティ」と「データの読み解き・活用」に特化している。受講者に重複受講の方がいれば「今回はより実践的な"守り"と"活用"に踏み込みます」とポジショニングを明示する

本日の目標

この研修を通じて、以下のことができるようになります

1. 情報セキュリティの3要素（CIA）を説明し、日常業務でのリスクを特定できる
2. 最新のサイバー脅威を理解し、自分が取るべき対策を実行できる
3. データを正しく読み解き、グラフや統計の落とし穴を見抜ける
4. データに基づく意思決定のプロセスを業務に適用できる

【時間: 3分】
- 「皆さんの中で、"パスワードを使い回している"方はいらっしゃいますか？」と問いかける。正直に手を挙げにくいテーマなので「心の中で挙手してください」と軽いトーンで
- 続けて「"データを根拠に提案や報告をしたことがある"方は？」と聞き、セキュリティとデータ活用の両面に意識を向けさせる
- 「今日は"守る力"と"活かす力"の両方を身につけます。この2つは対立するものではなく、セットで初めて機能します」

アジェンダ

第1部：情報セキュリティ編

1. 情報セキュリティの基本 ― CIA3要素（15分）
2. 最新サイバー脅威と対策（20分）
3. 日常業務のセキュリティ実践（20分）
4. インシデント対応と報告（10分）

第2部：データリテラシー編

5. データリテラシーとは何か（15分）
6. データの読み方・グラフの落とし穴（20分）
7. データに基づく意思決定（15分）

まとめ

8. 総合演習と振り返り（15分）　　※ 第1部と第2部の間に休憩10分を入れます

【時間: 2分】
- 全体の流れを簡潔に説明
- 「前半がセキュリティ、後半がデータリテラシーです。一見別のテーマに見えますが、最後の総合演習で2つが結びつきます」
- リモート参加者がいる場合は、チャット機能やブレイクアウトルームの使い方を案内
- 「専門知識は不要です。日常業務の視点で考えていきましょう」と安心感を与える

アイスブレイク「あなたのセキュリティ＆データ体験」

【グループワーク】（所要時間: 5分 / 4〜5名1組）

テーマ

「最近、"ヒヤッとした"セキュリティの経験、または"データを見て驚いた"経験」

- メールやSMSで怪しいメッセージが届いた経験
- パスワードを忘れて困った経験
- ニュースやSNSで見た数字・データに「本当？」と思った経験
- グループ内で1人1分程度シェアしてください

【時間: 8分（説明1分＋ワーク5分＋共有2分）】
- セキュリティもデータも「身近なもの」であることを実感させるのが狙い
- 例を出すとハードルが下がる：「例えば"宅配便の不在通知SMS"が実はフィッシング詐欺だったとか、"コロナ禍で感染者グラフの縦軸が途中から変わっていて印象操作に見えた"とか」
- 2〜3グループに代表的なエピソードを共有してもらう
- 「今日の研修で、こうした場面でどう判断すべきかが明確になります」とセクション1への橋渡しをする

セクション1 ー 情報セキュリティの基本：CIA3要素

情報セキュリティとは、情報の**CIA**（3要素）を守ることです

要素	英語	意味	具体例
機密性	Confidentiality	許可された人だけがアクセスできる	顧客情報の閲覧権限管理
完全性	Integrity	情報が正確で改ざんされていない	契約書データの変更履歴管理
可用性	Availability	必要なときに情報を使える	システム障害時のバックアップ

この3つはトレードオフの関係にあります

- 機密性を高めすぎると → 可用性が下がる（アクセスが煩雑になる）
- 可用性を重視しすぎると → 機密性が下がる（誰でもアクセスできてしまう）

5 / 30

【時間: 7分】
- CIAは情報セキュリティの国際規格ISO 27001でも基盤となる概念であることを補足
- 「セキュリティ」と聞くと「パスワード」や「ウイルス対策」だけを思い浮かべがちだが、本質は「情報の価値を守ること」であると伝える
- トレードオフの例：社内の全ファイルに10段階の承認フローを設けたら安全だが、仕事にならない。適切なバランスが重要
- 想定質問：「CIAのうちどれが一番大切ですか？」→「業種・業務によって優先度は異なります。例えば医療現場では可用性が最優先、金融機関では機密性が重視される傾向があります」

情報セキュリティとデータリテラシー

【個人ワーク】自分の業務の CIA リスクを洗い出す　ワークシート①

自分の日常業務における情報セキュリティリスクを 1 つずつ書き出してください

CIA 要素	あなたの業務で考えられるリスク	現在の対策
機密性		
完全性		
可用性		

【グループワーク】このグラフ、おかしくない？　ワークシート②

各グラフについて、何がおかしいか・どう読むべきかをグループで話し合ってください

グラフ 1：自社製品の満足度推移（棒グラフ）

ヒント：縦軸をよく見てください