令和8年度 中小企業庁
情報モラル啓発セミナー　in 仙台
ビジネスパーソンの情報モラル
悪意のない「つい」が会社と人を傷つける　～社会人のネット基本作法～

【講演2】

社会人のネット基本作法

～AIが、そこにいる時代のアップデート～

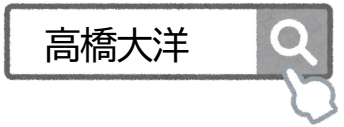
2026年11月10日

高橋大洋（株式会社ミヤノモリ・ラボラトリー）
taiyo@miyanomorilab.co.jp

主催：中小企業庁／東北経済産業局

投票や質問の書き込みに
menti.comを利用します
（アクセスコードは当日ご案内）

講師自己紹介



フィルタリングやコンピュータウイルス対策など情報セキュリティ企業勤務をきっかけに、利用者の知識習得・行動変容の重要性に気づく。それから20年間、子ども・大人からシニア層までのネット利用についての調査・研究、学習カリキュラム開発、指導者支援を行う。

現在は「デジタル利活用推進」「ネットと人権」等をテーマにした研修講師の他、情報活用・人材育成についての企業向けアドバイザーも務める。

株式会社ミヤノモリ・ラボラトリー 代表取締役社長。一般社団法人セーファーインターネット協会 客員研究員。小樽商科大学・帯広畜産大学・北見工業大学 非常勤講師（インターネットのメディアリテラシー）。JFCファクトチェックトレーナー。著書（共著）『はじめてのSNS社会の歩き方』（講談社）。北海道札幌市在住。

本講演のゴール

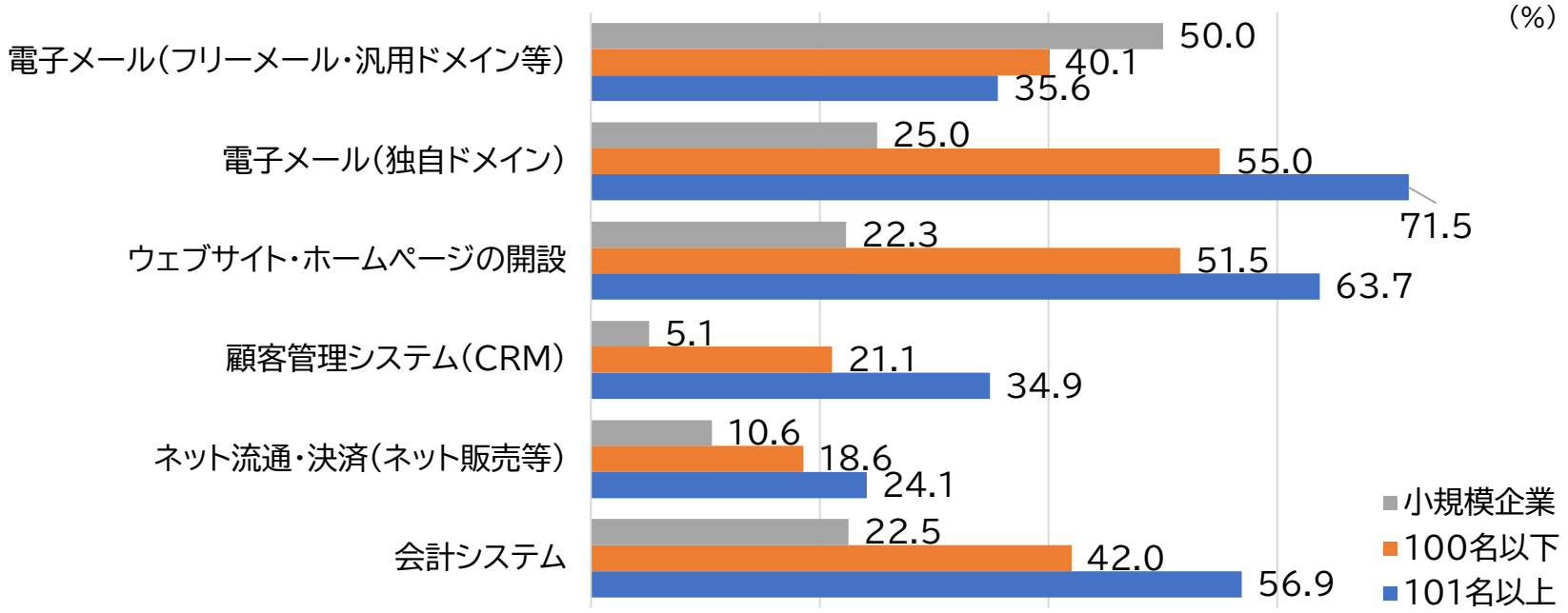
- 作法とは…行動(所作)の「型」
  - ルール(他律)やマナー(他者志向)とは異なる
  - 誰が見ていなくてもいつでも自分を整えるイメージ
  - 合理性が宿っている、自律・修練で身につけていく

職場で情報を扱う人が身につけておきたい「型」とは？

本講演の流れ

1. 情報発信による人権侵害リスクは
   職場の「あたりまえ」に潜んでいる
2. AI普及で、意図せず発信してしまう場面がさらに増加
3. 事故は注意喚起だけでは防げない
4. 組織外との分担にも目を向ける必要が明らかに
5. 求められている対応のアップデート

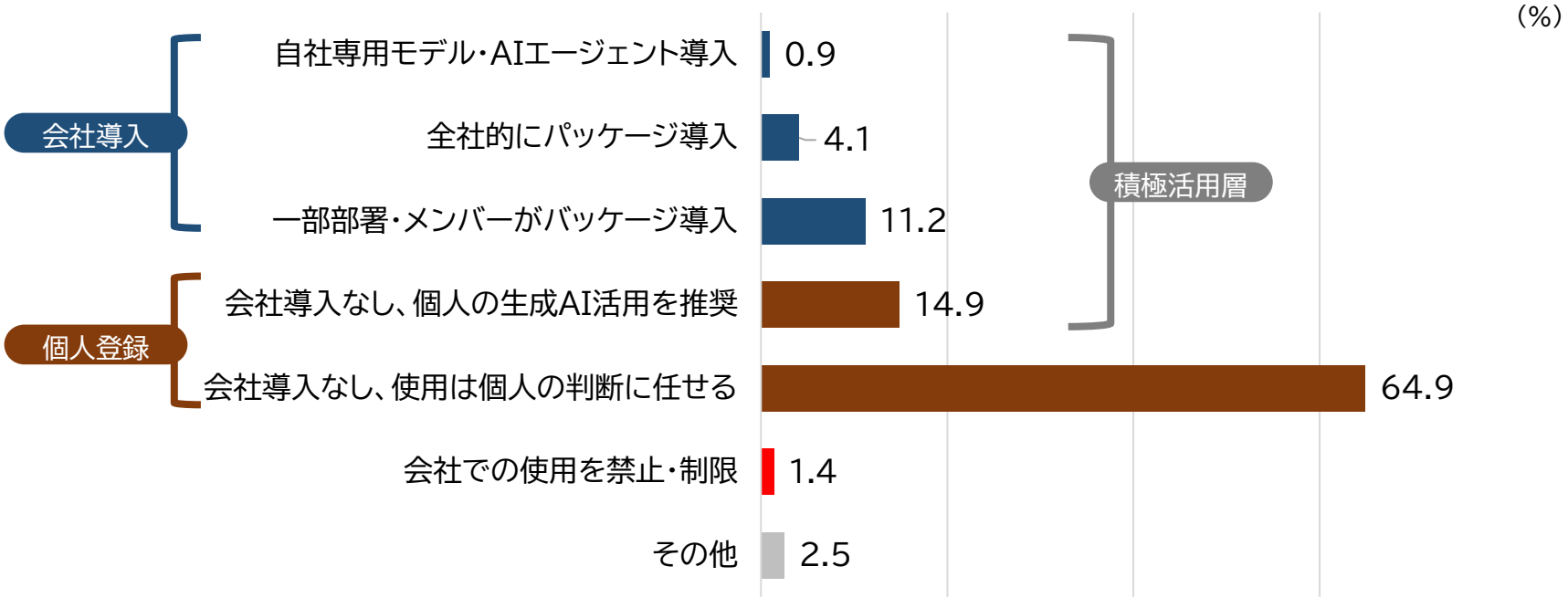
利用・導入しているサービス



中小組織が利用しているどのサービスも自社内だけでは閉じていないはず

＊IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」p.109-110　利用・導入しているサービスやシステム　一部抜粋
(小規模企業:1～5名の商業・サービス業、1～20名の製造業その他)
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

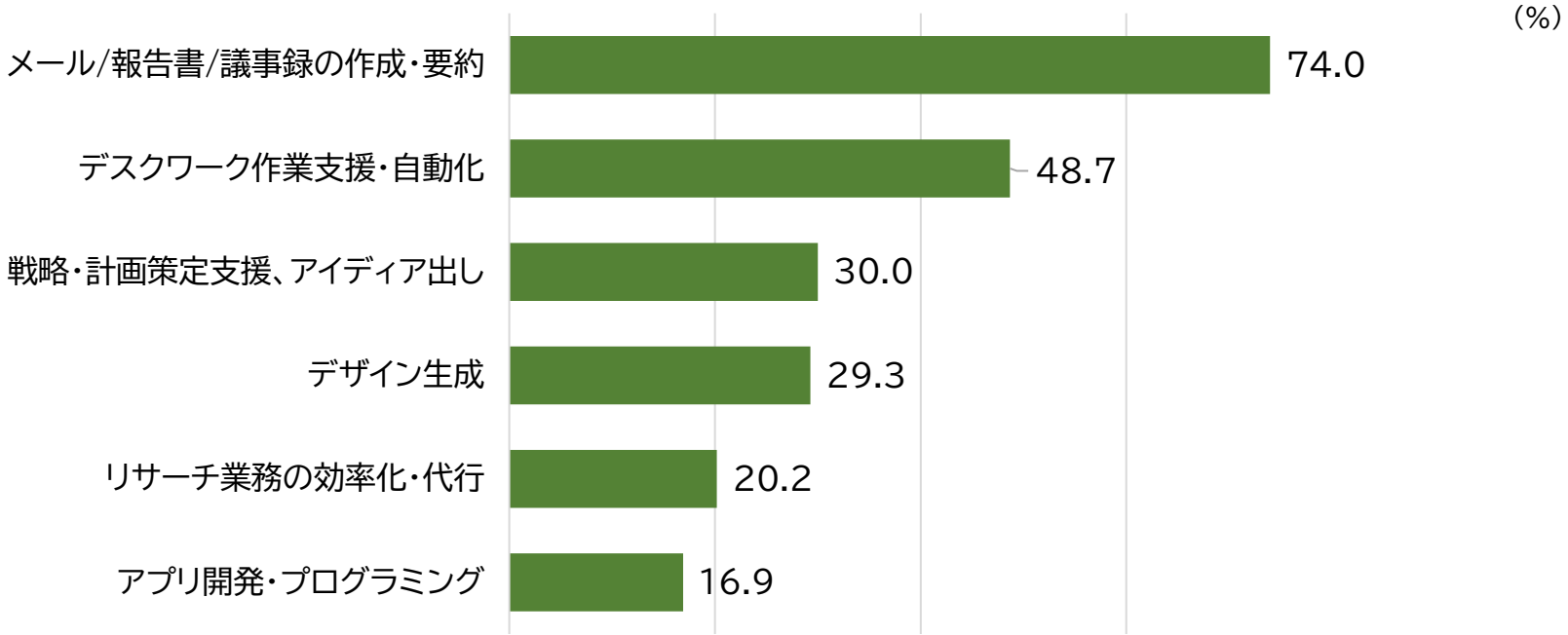
生成AI導入状況



いわゆるシャドーAIが中小組織では「あたりまえ」化

＊商工中金「中小企業の生成AIの利用にかかる調査（2026年1月調査）」p.3　生成AIの導入状況（対象：商工中金の取引先中小企業　有効回答数3,892社）
https://www.shokochukin.co.jp/report/data/assets/pdf/futai202603.pdf

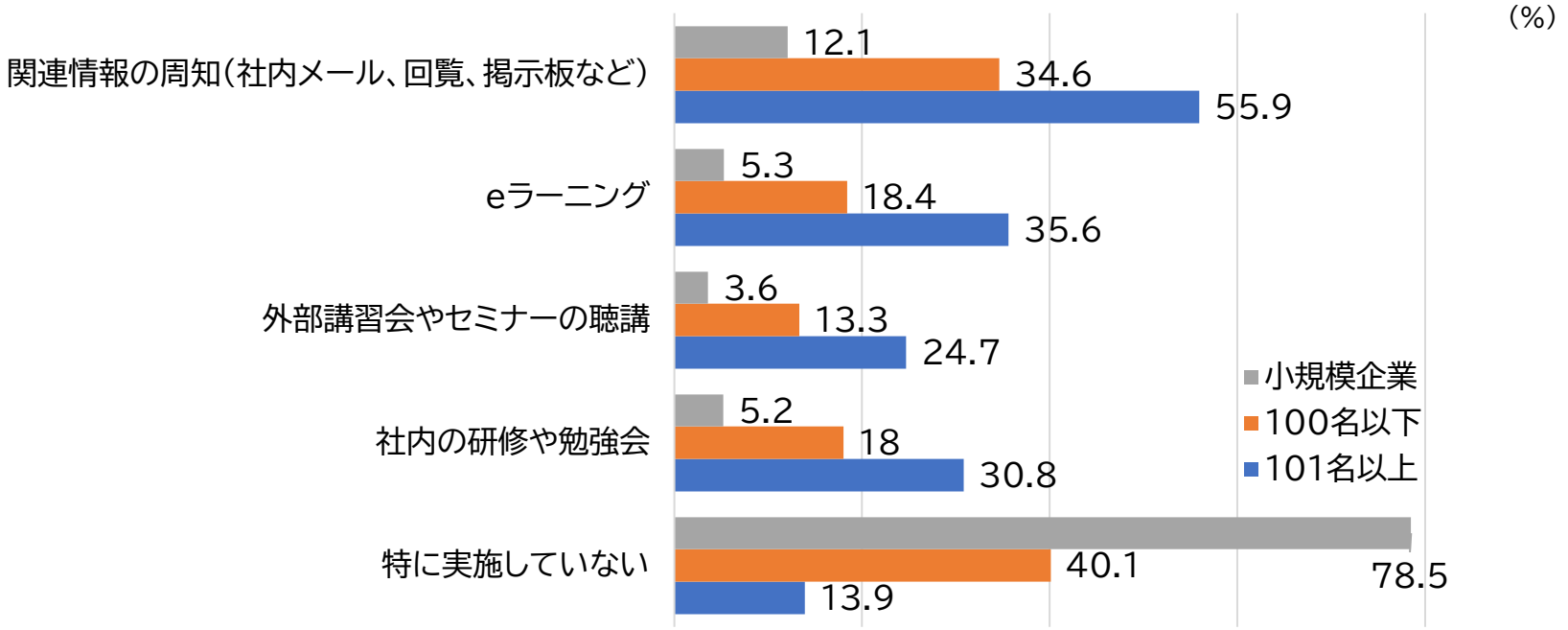
生成AI活用事例



社内外の機微な情報を生成AIに取り扱わせている可能性が高い

＊商工中金「中小企業の生成AIの利用にかかる調査（2026年1月調査）」p.6　生成AIの活用事例 一部抜粋 （対象：生成AI積極活用層）
https://www.shokochukin.co.jp/report/data/assets/pdf/futai202603.pdf

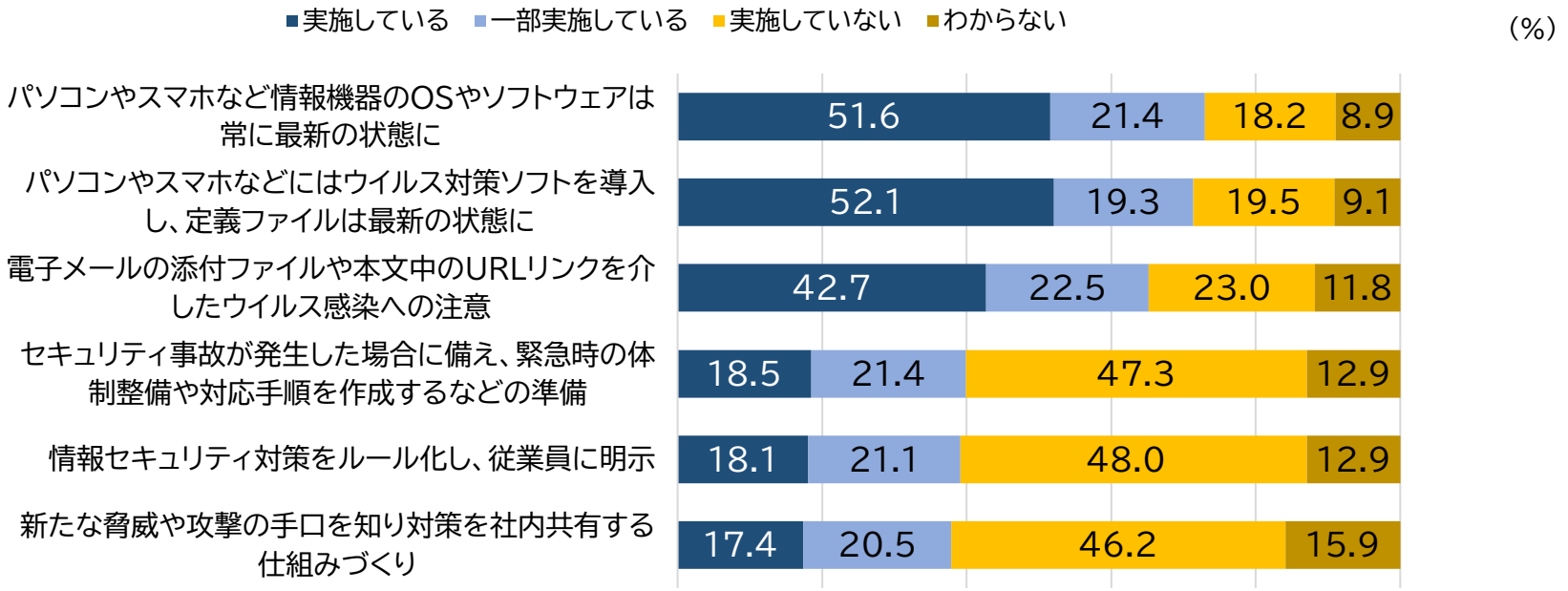
従業員向けセキュリティ教育



組織の規模が小さいほど従業員向けの働きかけは弱いのが現実

＊IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」p.120 従業員に対するセキュリティ教育の実施状況から一部抜粋
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

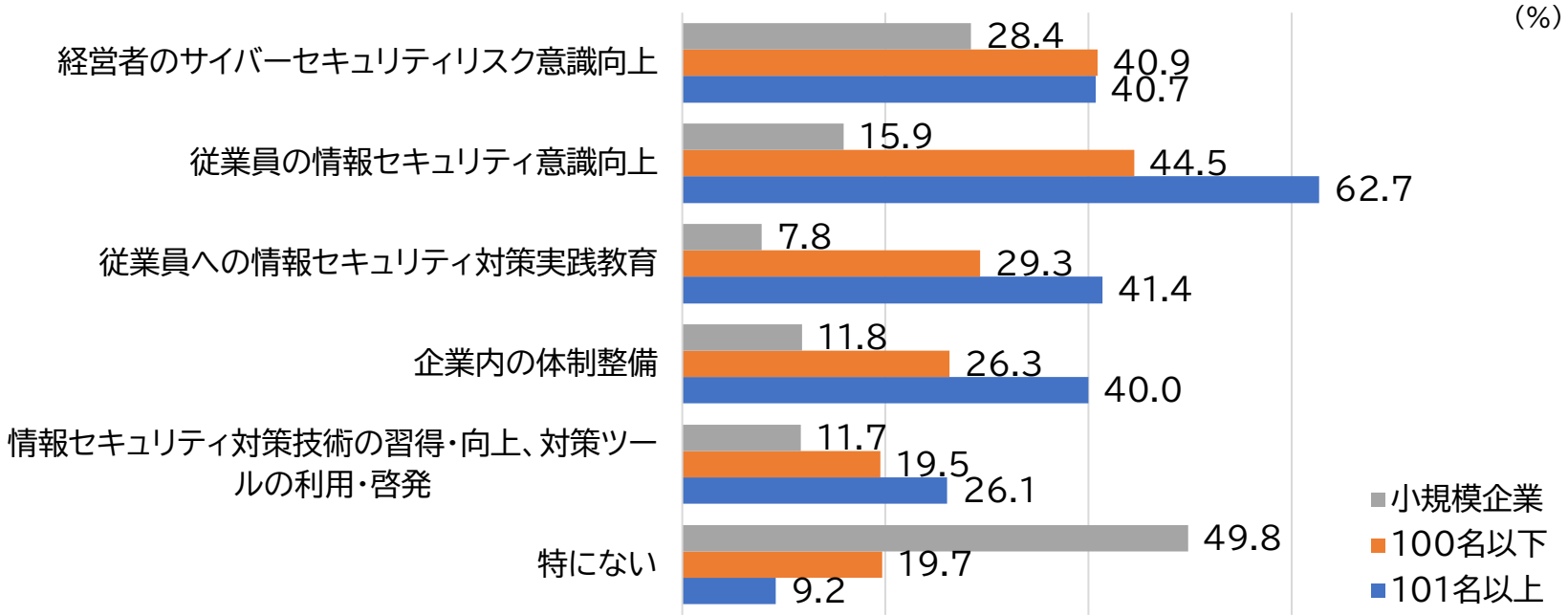
セキュリティ対策実施状況



個人単位でできる対策は浸透しつつあるが、組織での対策は後手に回っている

＊IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」p.250 自社診断25項目の実施状況から上位3項目、下位3項目を抜粋
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

今後の対策向上に必要なこと



「終わりがない」はずの対策向上に目が向かないのが小規模組織の現実

＊IPA「2024年度中小企業における情報セキュリティ対策に関する実態調査」p.125　情報セキュリティ対策をさらに向上させるために必要と思われること　一部抜粋
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

事故を起こす行動と対策

- 意図的に（違反・手抜き）　＊本講演では取り扱わない
- 意図せず（ヒューマンエラー）
  - 知識や経験の不足、誤解（思い込み）
  - 疲れていた・急いでいた
  - 作業や環境の特性・不備

エラーはゼロにならない（フェイルセーフ）前提に立つ必要

＊厚生労働省「職場のあんぜんサイト」 https://anzeninfo.mhlw.go.jp/yougo/yougo90_1.html、
東京都産業労働局「令和8年度　中小企業サイバーセキュリティ社内体制整備事業フォローアップ」https://cybersecurity-taisaku.metro.tokyo.lg.jp/ などを参考に作成

情報モラルのフェイルセーフ

1. 作業や環境を整える

- 事故誘発ポイントを見つける、減らす、置き換える
  ＊私物AIではなく法人として契約する、メール添付ではなく期限付きリンクでファイル共有する　など

2. エラーが起きる前提で備える

- 利用システム・サービスの分担を明確に把握＊更新作業が抜け落ちがち
- バックアップや代替手段を準備しておく

3. 知識・経験を高める取り組み

- リスク認知と従業員教育

＊厚生労働省「職場のあんぜんサイト」 https://anzeninfo.mhlw.go.jp/yougo/yougo90_1.html、
東京都産業労働局「令和8年度　中小企業サイバーセキュリティ社内体制整備事業フォローアップ」https://cybersecurity-taisaku.metro.tokyo.lg.jp/ などを参考に作成

リスク認知のプロセス

進度	段階	状況	進め方
1	リスクの同定	そういうリスクがある（名前）	「周知」が可能
2	リスクイメージの形成	そのリスクはイヤだ、起きてほしくない	
3	リスクの推定	遭遇する可能性がある （イヤな予感がする）	「自分ごと」として 考えさせる必要
4	リスクの評価	リスクを避けるか便益をとるか	
5	リスクの統制	遭遇しても被害が最小限になるよう工夫する	持続させる必要 役割分担が必要

＊楠見、匹田による提案をもとに一部表現を改変

従業員教育のポイント

1. 「知識」「行動」にはバラつきが残る前提で
   - 正規分布の中央値を動かす
2. 「大人の学び方」や行動を知る
   - 動機づけ、経験との結び付け、認知の省エネ
   - 業務利用と私的利用の連続性、インターネットの「学びにくさ」
3. 組織内・外での「協同」を目標に置く
   - 知識習得度合い＋具体的な助け合い行動で事後評価する

まとめ

職場で情報を扱う人が身につけておきたい「型」とは

- 情報モラルは一人では完結しないことに気づき、同僚や外注先と、いつも息を合わせて動く
  - 誰もが質問・相談しやすい社内環境をつくる
    （自分が苦手な領域で詳しい人にしてほしいことを思い出す）
  - 自社の分担を知り、外注先が動きやすいように発注・契約する

いざという時に頼りになるのは？

	確かめておきたいこと	社内 （最初の連絡先・責任者は誰？）	社外 （社名・連絡先・どこまで頼める契約？）
パソコン・ ネットワーク・サーバ	どこから購入・設置した？ 設定内容（記録）は誰が把握している？ データのバックアップは？		
メール	契約しているサービスの内容は？ 退職者アカウントの対処は？ 権限や設定を閲覧・変更できるのは誰？		
ウェブサイト	ドメイン・レンタルサーバ・CMSの更新や コンテンツのバックアップ体制は？ 権限や設定を変更できるのは誰？		
顧客管理 システム（CRM）	設定内容（記録）は誰が把握している？ バックアップや更新は？		
会計システム	設定内容（記録）は誰が把握している？ バックアップや更新は？		
AIサービスやSNS	何を、誰が使っている？		

セキュリティ情報源・相談先

- IPA（独立行政法人情報処理推進機構）
  - 中小企業の情報セキュリティ対策ガイドライン
    https://www.ipa.go.jp/security/guide/sme/about.html
  - 5分でできる！情報セキュリティ自社診断
    https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_3.pdf
  - サイバーセキュリティ相談窓口（企業組織向け）
    https://www.ipa.go.jp/security/support/soudan.html

＊上記に加え、不正アクセス特別相談窓口（03-6759-5760） が開設されています。（10/16～）
https://www.ipa.go.jp/security/support/incident-support.html

＊ 情報セキュリティ安心相談窓口（個人向け）もご利用いただけます。
https://www.ipa.go.jp/security/anshin/about.html

ネット上の書き込み・人権相談先

- 違法・有害情報相談センター
  https://ihaho.jp/

- インターネット人権相談（法務省 法務局）
  https://www.moj.go.jp/JINKEN/jinken113.html

- 誹謗中傷ホットライン（SIA）
  https://www.saferinternet.or.jp/bullying/