「サイバーセキュリティ人財育成研修」実施カリキュラム

1)「経営者が知っておきたい“会社を守る”サイバーセキュリティ入門」

・実施日時：令和 7 年 11 月 18 日（火）13：30～16：30（3 時間）

・実施形態：オンライン（Zoom 利用）

・対象：県内企業・団体の経営者やこれからサイバーセキュリティ対策を検討中のご担当者等
（その他、サイバーセキュリティ対策にご関心ある方はお気軽にご参加ください）

・内容：国内外で進む DX 化や生成 AI などの利活用促進とともに現れてきている最新のサイバーセキュリティの脅威の動向と対策への必要性を感じていただき、企業にとっての経営者の役割の重要性や、最初に取り組むべきことを紹介します。

【実施カリキュラム】

■IPA「情報セキュリティ 10 大脅威 2025」から

（参考：https://www.ipa.go.jp/security/10threats/10threats2025.html）

最新のサイバーセキュリティの脅威の動向、必要な対策などについて、これから学ぶ方のためのわかりやすい解説をします。

■IPA「中小企業の情報セキュリティ対策ガイドライン（第 1 部経営者編）」から

（参考：https://www.ipa.go.jp/security/guide/sme/about.html）

・情報セキュリティ対策を怠ることで企業が被る不利益

・経営者が負う責任

・経営者は何をやらなければならないのか

■IPA「中小企業の情報セキュリティ対策ガイドライン（第 2 部実践編）」から

・できるところから始める（「情報セキュリティ 5 か条」等）

・組織的な取り組みを開始する

（「情報セキュリティ基本方針」の作成と周知

「実施状況の把握、対策の決定と周知）

・「5 分でできる！情報セキュリティ自社診断」で現状の対策

・「情報セキュリティハンドブック（ひな形）」を参考にした具体的な手順書の作成・活用

■生成 AI の活用について

・生成 AI の利活用にあたっての留意点（ファクトチェック、社内ルール、著作権や倫理等）

・経営リスク軽減に向けて（コンプライアンス違反、プライバシー侵害、デマ情報等への対策）

2)「セキュリティの課題をその場で解決！サイバーセキュリティ実践演習」

・実施日時：令和 7 年 12 月 12 日（金）10：00～16：00（定員 15 名）
（※12:00～13：00 お昼休み、5 時間）

・実施形態：集合形式。パソコンによる実習も行います。

・実施会場：株式会社ソフトアカデミーあおもり（青森市第二問屋町 4-11-18）

・定員：15 名

・対象：県内企業・団体の情報担当者等。サイバーセキュリティ対策の組織、ルール作りにこれから取り組む方など。

・内容：サイバーセキュリティ対策をする上での体制構築、規程の整備などの基盤作りやリスク分析の講義と演習を行います。

【実施カリキュラム】

■IPA「情報セキュリティ 10 大脅威 2025」から
（参考：https://www.ipa.go.jp/security/10threats/10threats2025.html）
組織としての対応上の留意点、新規で対応が迫られている最新の動向等を解説。

■IPA 「中小企業の情報セキュリティ対策ガイドライン（第 2 部実践編）」から
（参考：https://www.ipa.go.jp/security/guide/sme/about.html）
以下の演習用付録教材を利用。
「情報セキュリティ関連規程（サンプル）」
「中小企業のためのクラウドサービス安全利用の手引き」
「リスク分析シート」

【講義内容】

a)本格的に取り組む

・管理体制の構築、DX の推進と情報セキュリティの予算化

・情報セキュリティ規程の作成（解説と演習：規程の作成）

・委託時の対策、点検と改善

b)より強固にするための方策

・情報収集と共有、ウェブサイトの情報セキュリティ

・クラウドサービスの情報セキュリティ、テレワークの情報セキュリティ

・セキュリティインシデント対応、情報セキュリティサービスの活用（IPA 各種サービス等）

・技術的対策例と活用

・詳細リスク分析の実施方法（解説と演習：情報資産洗い出しとリスク分析）

c)生成 AI の脅威と対策

・技術的脅威の実際
（ディープフェーク偽造画像、フィッシングメール、サプライチェーン攻撃等）

・生成 AI ガイドライン策定や企業や団体での教育について
（国や業界団体での実例、企業や団体での啓発についての紹介等）

＊パソコン等は運営側で準備します。持参ご希望の方はおお伝えください。
＊当日は演習で、社内ルールや体制、情報資産の洗い出しをする演習を予定しています。
演習に必要な情報をご持参いただきたくお願いします。
（パソコンや USB メモリをご持参いただく場合は、申請資料が必要となります。
必要な資料をお渡ししますので、ご面倒をおかけしますが、ご連絡ください。）
＊作成いただいた電子ファイル（Word、Excel、PowerPoint、PDF 形式）は、
データを DVD でお持ち帰りいただきます。情報管理の面から、弊社では保管は致しません。

演習付属教材サンプル

※出典：中小企業の情報セキュリティ対策ガイドライン ｜ 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/guide/sme/about.html

診断編

診断項目	No	診断内容	チェック 実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記１～24 など）をルール化し、従業員に明示していますか？	4	2	0	−1

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。
※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。

	A 実施しているの合計点	B 一部実施しているの合計点	C わからないの合計点
	点	点	マイナス(−)　点
A+B+C 合計			点

診断の後は次ページ以降を読んで対策を検討してください。

3

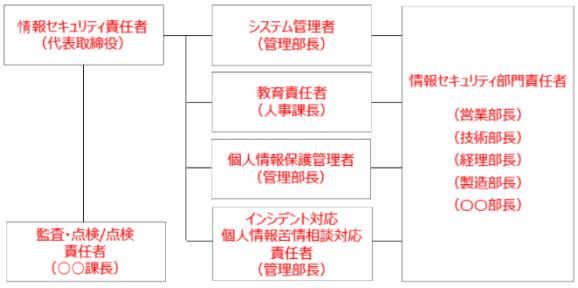
1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1.情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者 個人情報苦情相談対応	事故の影響を判断し、対応について意思決定する。 個人情報の取扱いに関して本人からの苦情・相談に対応する。
個人情報保護管理者	個人情報の取扱いについて関連法令を遵守する責任を負う。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。

＜情報セキュリティ委員会体制図＞



1

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類 個人情報	要配慮個人情報	特定個人情報	評価値 機密性	完全性	可用性	重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示） 脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェックリスト」シートに入力すると表示	被害発生可能性		リスク値	
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	3	5年	2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2	3	7年	2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	社内サーバー	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			3	2	2	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	モバイル機器	有			3	2	2	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	社内サーバー				2	2	2	2		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク中
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク小