

# インシデント対応を軸にしたセキュリティマネジメント指導 ～ 副業で広げるキャリア ～

2025年11月7日(金)

令和6年度事業 セキュリティマネジメント指導担当  
久保田 秀男

## 自己紹介



# 久保田 秀男

### 経歴

名古屋銀行及び同行リース子会社  
製造業(中小企業)  
公益財団法人  
名古屋エージェンシー株式会社【在職】

### 主な取得資格

情報処理安全確保支援士(登録番号000022)  
システム監査技術者

### 所属団体など

特定非営利活動法人日本システム監査人協会  
独立行政法人情報処理推進機構 登録セキュリティプレゼンター  
独立行政法人中小企業基盤整備機構 中小企業アドバイザー(経営支援)

# 目次

2. 副業として取り組むセキュリティマネジメント指導
3. 指導先を知る：事業内容・課題の把握
4. 指導シラバス（ツール）の活用（インシデント対応編）
5. 実際の指導実績と効果
6. セキュリティ専門家としての心構え
7. セキュリティマネジメント指導：課題と改善
8. まとめ — 指導を通じて得られた学びと今後

## 2. 副業として取り組むセキュリティマネジメント指導 1/3

**副業するにあたっては必ず勤務先に確認しよう**  
**有給日数を管理しよう（半日休暇、時間単位での休暇制度など利用できる制度の確認）**  
**過重労働にならないように労働時間管理に気をつけよう。無理のない範囲で取り組む**

### 副業に対する社会全体の対応動向

#### 【1】制度・政策の動向

政府は「働き方改革」の一環として副業・兼業を促進  
モデル就業規則でも「原則認める」方向に転換  
地方創生策として、副業・兼業人材を地方へ呼び込む補助制度を推進中

#### 【2】企業の対応状況

副業解禁の広がり  
大企業中心に解禁が進み、制度導入企業は過半数を超える

#### 実態とのギャップ

制度はあっても実際に副業する社員は少なく、利用率は2割前後

#### 条件付きでの運用

勤務時間・競合関係・研修期間中などの制限を設ける企業が多い

## 2. 副業として取り組むセキュリティマネジメント指導 2/3

### 【3】働く人の意識・実態

副業意向の高まり

「収入補填」「将来不安」「スキル活用」などが主な理由

実施率の低さ

副業経験者は全体の約8%前後にとどまる

禁止企業での葛藤

解禁を望む声が強く、非公認で行う人も一定数存在

### 【4】課題・リスク

労働時間の管理・健康リスク

競合・情報漏洩の懸念

中小企業・地方での制度整備の遅れ

公私の線引きが曖昧になりやすい点

### 【5】 今後の方向性

副業を「人材確保・スキル転換・地域活性」の戦略的手段とする流れ

マッチングサービスなど新たな副業支援市場の拡大

労働時間制度や副業ルールの更なる明確化・標準化が見込まれる

### 【6】 まとめ

副業は「容認から活用へ」とフェーズが変化中

個人にとってはスキル拡張・収入補完のチャンス

企業にとっては人材獲得とイノベーションの機会

今後は制度整備と実運用のバランスが鍵となる

### 3. 指導先を知る：事業内容・課題の把握

#### 初回面談までにやっておくこと

- ホームページなどで指導先の事業内容など可能な限り掴んでおく
- その業界の概況、課題など一般的なところを掴んでおく
- 同業他社でセキュリティインシデントがあれば内容を把握しておく

## 4. 指導シラバス（ツール）の活用（インシデント対応編） ～ 本資料の位置づけ ～

本資料は、IPAが実施する「令和6年度セキュリティ人材活用促進実証」において実施する、サイバーセキュリティ専門家が中小企業に対して行う個別訪問指導「**セキュリティマネジメント指導（テーマ別）**」の概要説明資料です。

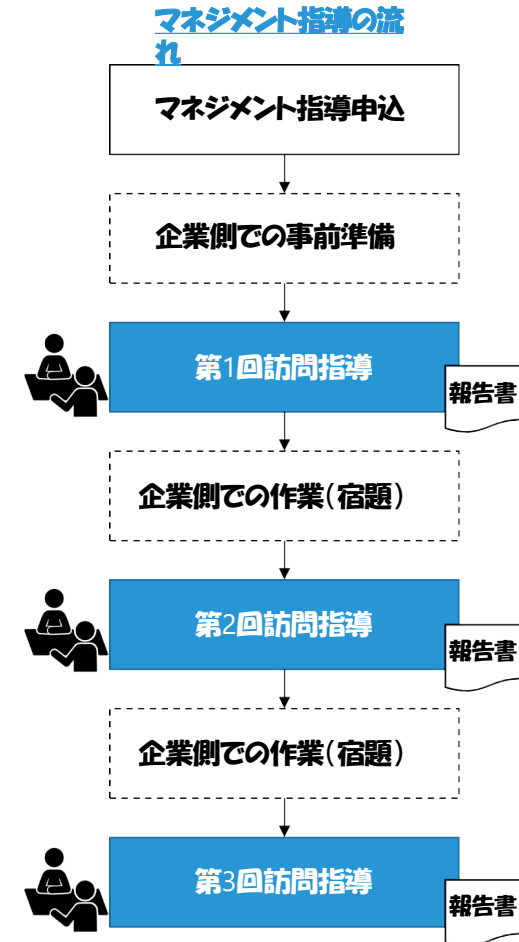
訪問指導では、専門家が中小企業の特성에応じたセキュリティ対策を指導する際の基本的なフレームワークを提供することを目的としています。特に中小企業は、限られたリソースの中で情報セキュリティ対策を行う必要がありますが、どの部分に重点を置くべきかが明確でないケースが多々あります。

マネジメント指導（テーマ別）では、そのような中小企業に対して、**①情報セキュリティ規程の整備、②情報資産の洗い出しとリスク分析、③クラウドサービスの安全利用、④セキュリティインシデント対応、そして⑤従業員向けのセキュリティ教育**の5つの主要なテーマを指導するための具体的な方法と手順を提供しています。

各テーマにおいては、どのような企業がその指導を必要としているのか、指導によって達成されるべき目標、さらには具体的な作業内容や使用ツール、指導後の効果の考え方等を想定しています。これにより、専門家は訪問先の企業ごとに適切な指導計画を立て、効率的に支援を行うことができると考えています。

本資料では、専門家が現場で利用できる具体的なシラバスやチェックシート、ガイドラインも挙げております。実際には企業に訪問した際は、企業の実情に応じた柔軟な対応をお願いすることとなりますが、ツール活用によってある程度訪問指導の際の一貫性が確保され、企業においても自律的なセキュリティ対策の強化が期待できると考えます。

専門家のみなさまにおかれましては、本資料に記載された趣旨をご理解の上、中小企業へのセキュリティ個別指導にご対応ください。





## 4. 指導シラバス（ツール）の活用（インシデント対応編） ～ マネジメント指導のテーマと狙い ～

今回用意したマネジメント指導のテーマは以下の5テーマです。

企業の実情に即し、原則として以下のテーマから選定の上、企業への訪問指導を行っていただきます。

指導 テーマ	1 情報セキュリティ 規程の整備	2 情報資産の 洗い出しと リスク分析	3 クラウドサービスの 安全利用	4 セキュリティ インシデント対応	5 従業員向け 情報セキュリティ 教育
どういった企業に 受けてもらいたいのか	<u>サイバー攻撃の増加や法令遵守の必要性に直面しつつも、情報セキュリティ規程が未整備な中小企業。</u> 特に、従業員が多様なITツールを使って業務を行っているが、具体的な指針がなく、責任範囲が曖昧な企業に必要である。	<u>デジタル化が進み、膨大な情報を管理しているが、どの情報が重要か、リスクがどこにあるかが把握できていない企業。</u> 特に、製造業やサービス業など、顧客情報や技術情報を大量に扱う企業に必要である。	<u>業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な企業。</u> 特に、情報管理の外部委託が進んでいるが、適切な安全対策ができていない中小企業に必要である。	<u>セキュリティインシデントが発生した際の対応が曖昧で、事後対応に時間がかかり、被害が拡大するリスクがある企業。</u> 特に、 <u>サプライチェーンの一部として他社との連携が多い企業</u> に必要である。	<u>従業員のセキュリティ意識が低く、パスワード管理やフィッシング攻撃に対する対応が不十分な企業。</u> 特に、ITリテラシーの差が大きい企業や、非専門職の従業員が多く、日常的なセキュリティ対策が徹底できていない企業に必要である。
マネジメント指導を 受けたことによる効果	不足していた情報セキュリティ規程が整備され、社内での運用・周知方法まで確立されることで、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。	企業が保有する情報資産が洗い出され、リスク分析シートとして整備することで、自律的な運用が図れるとともに、リスク低減策等の検討の題材にもなる。	当該支援先企業における「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用に伴うリスクを理解できるようになる。	インシデント対応プロセスを整備し、必要に応じ、従業員の訓練も実施することで、セキュリティインシデント発生時に迅速かつ効果的に対応できる体制が構築できる。	セキュリティ教育プログラムを策定するとともに、定期的に見直しと更新を行う体制を構築。実際に従業員に対するセキュリティ教育を実施することで、社内の意識向上にもつなげられる。

## 4. 指導シラバス（ツール）の活用（インシデント対応編） ～ 指導テーマ④ | セキュリティインシデント対応 ～



### 背景

- デジタル化が進む現代のビジネス環境において、サイバー攻撃やデータ漏洩などのセキュリティインシデントは企業にとって重大な脅威である。適切なインシデント対応体制を整備することは、被害の最小化と迅速な復旧に不可欠である。

### 施策の対象となる企業像

- セキュリティインシデントが発生した際の対応が曖昧で、事後対応に時間がかかり、被害が拡大するリスクがある企業。特に、サプライチェーンの一部として他社との連携が多い企業に必要である。

### マネジメント指導の目標（ゴール）

- セキュリティインシデント発生時に迅速かつ効果的に対応できる体制を構築する。
- インシデント対応プロセスを整備する。   **主要なアウトプット**
- 具体的な模擬インシデントを題材に、従業員の訓練を実施する。これにより、支援先企業におけるインシデント対応力を向上させる。

### 指導の際に活用できる既存資料等

- 中小企業の情報セキュリティ対策ガイドライン | 付録8  
「中小企業のためのセキュリティインシデント対応手引き」

# 4. 指導シラバス（ツール）の活用（インシデント対応編） ～ 指導テーマ④ | セキュリティインシデント対応 ～

## シラバス案

### ■第1ステップ(指導申込み～第1回面談まで)

#### 現状のセキュリティインシデント対応体制の評価と重要項目の説明

##### <指導先企業側事前作業>

期間(目安)	概ね1～2週間
作業内容	<ul style="list-style-type: none"><li>- 「5分でできる！情報セキュリティ自社診断」チェックシートの記入</li><li>- 現在のインシデント対応プロセスやポリシーの確認と事前評価を実施する。チェックシートに基づき、対応体制の現状を整理する。</li></ul>
使用するツール	<ul style="list-style-type: none"><li>- 記入様式   「5分でできる！情報セキュリティ自社診断」チェックシート</li><li>- 記入様式   インシデント対応体制チェックリスト(★)</li><li>- 参照資料   中小企業の情報セキュリティ対策ガイドライン   付録8「中小企業のためのセキュリティインシデント対応手引き」</li></ul>

##### <第1回面談時>

確認・指導事項等	<ul style="list-style-type: none"><li>- 支援先企業のセキュリティインシデント対応体制を評価し、現状を把握する。既存のインシデント対応プロセスやポリシーの見直し、改④点等を洗い出す。</li><li>- IT-BCPの考え方を説明し、インシデント発生時に事業や自分たちの顧客に何が起きるか(ビジネスインパクト)を考えさせる。そのため、「USBメモリ紛失」や「ランサムウェア感染」等典型的なセキュリティインシデントを題材に、演習形式でディスカッションワークを実施。その上で重要項目等を説明する。</li><li>- 次回(第2回)面談時までの企業側宿題として、インシデント対応手順書案の検討を指示。</li></ul>
使用するツール	<ul style="list-style-type: none"><li>- 記入様式   インシデント対応体制チェックリスト(★)</li><li>- 記入様式   セキュリティインシデント対応ワークシート</li><li>- 参照資料   中小企業の情報セキュリティ対策ガイドライン   付録8「中小企業のためのセキュリティインシデント対応手引き」</li></ul>

## 4. 指導シラバス（ツール）の活用（インシデント対応編）

インシデント対応に限らないが「5分でできる！情報セキュリティ自社診断」チェックシートを利用し指導先企業のセキュリティ状況を把握する。現場の担当者、システムを担当している人、経営層（社長、役員）など違う立場の人に自己診断をしてもらい、項目ごとに突合せを行い意識合わせをしていくと当該企業の状況がより解るのと同時に、指導先企業内での自社のセキュリティ状況に対する共通認識を持たせる効果がある。・・・ 補足1 資料

インシデント対応に限らず、システム概要図の提出をお願いする。中小企業においては自社のネットワーク、サーバーの設置場所などを全体像として把握していないケースが多い。ない場合は、支援先企業のシステムベンダーに協力を仰ぐなどを依頼し、作成していただく。精緻なものでなくとも概要図があれば、リスクの特定を行いやすい。・・・ 補足2 資料

規程類の確認を行う。規程間で齟齬がないか、実際にインシデントが発生した場合を想定し、例えば権限が不明確などの実行性があるか否かなどを確認する。今回指導した企業においては「自工会／部工会サイバーセキュリティガイドライン」も考慮 ・・・ 補足3 資料

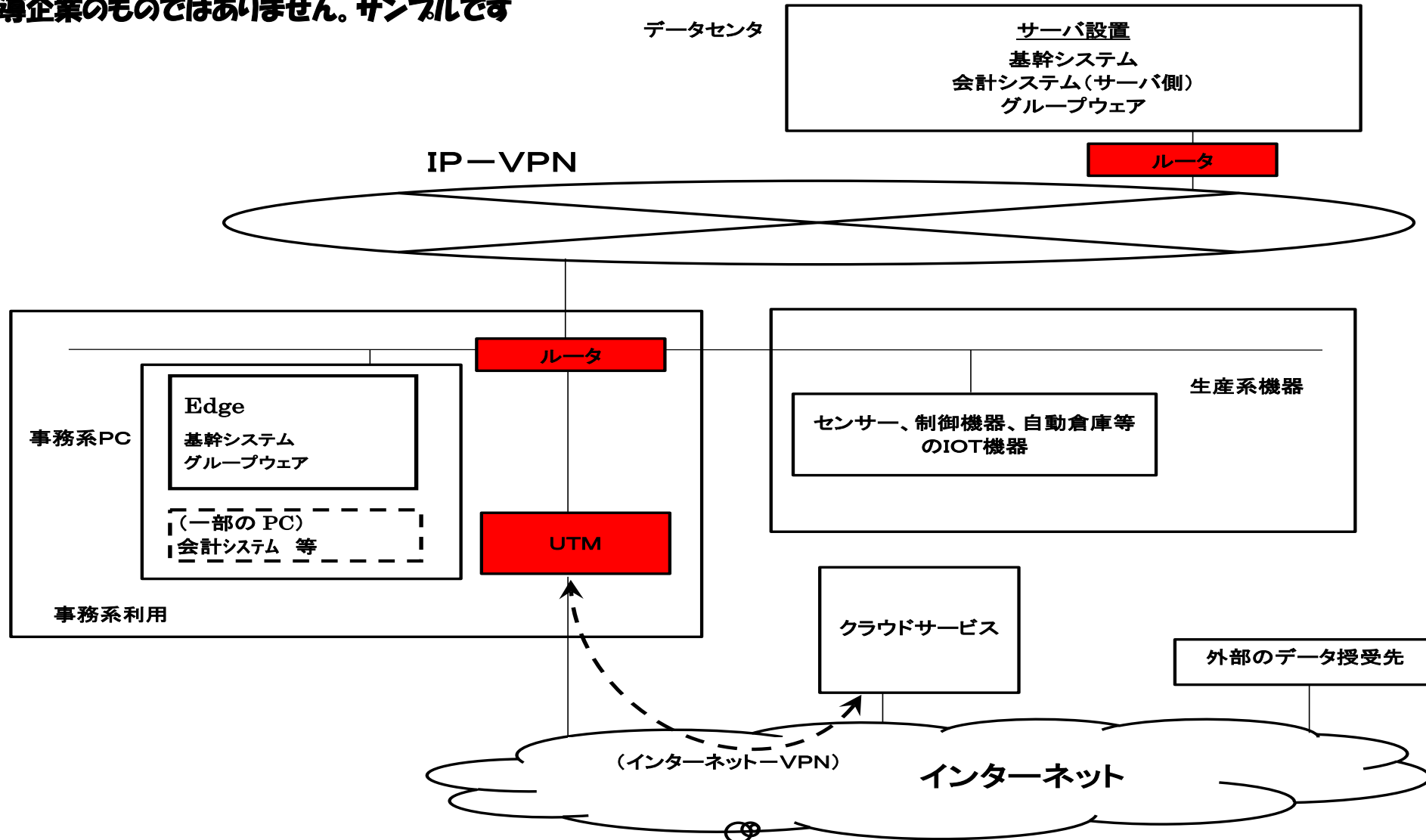
## 4. 【補足1】指導シラバス（ツール）の活用（インシデント対応編）

※今回指導企業のものではありません。サンプルです

診断項目	No	診断内容	該当するものにプルダウンで「✓」を入力（択一選択）			
			実施している（4点）	一部実施している（2点）	実施していない（0点）	わからない（-1点）
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？		✓		
	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？		✓		
	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？ 一部パスワードの設定なしのPCあり		✓		
	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？ 契約書は棚に格納（鍵のかからないところに保管）		✓		
	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？ システム担当よりメールでの注意喚起は実施		✓		
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？ システム担当よりメールでの注意喚起は実施		✓		
	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？			✓	
	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？		✓		
	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？		✓		
	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？			✓	
	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？		✓		
	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。 契約書は棚に格納（鍵のかからないところに保管）			✓	

## 4. 【補足2】指導シラバス（ツール）の活用（インシデント対応編）

※今回指導企業のものではありません。サンプルです





## 4. 【補足3】指導シラバス（ツール）の活用（インシデント対応編）

### JAMA・JAPIA

#### 自工会/部工会・サイバーセキュリティガイドライン

自動車産業における  
サイバーセキュリティ対策の一層の進展のために

### 2.3 版

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
			38	Lv1	情報セキュリティ事件・事故発生時の対応について教育・訓練を実施している	<b>【規則】</b> ・情報セキュリティ事件・事故発生時の対応について、教育資料配布・掲示、e ラーニング、集合教育等による教育や訓練を実施すること <b>【対象】</b> ・役員、従業員、社外要員（派遣社員等） <b>【頻度】</b> ・新規受け入れ時、かつ、1 回／年以上
		情報セキュリティ事件・事故に迅速かつ適切に対応できるように事前に備え、事故発生時の被害拡大の防止・迅速な復旧を図る	39	Lv3	組織を跨いだ情報セキュリティ事件・事故発生時の対応について教育・訓練を実施している	<b>【規則】</b> ・組織を跨いだ情報セキュリティ事件・事故発生時の対応について、教育資料配布・掲示、e ラーニング、集合教育等による教育や訓練を実施すること <b>【対象】</b> ・セキュリティ関連部門 <b>【頻度】</b> ・1 回／年以上
		自組織内あるいは組織を跨いで影響する情報セキュリティ事件・事故の発生と影響を抑制する教育・訓練を行っていること	40	Lv1	教育・訓練の内容を必要に応じて見直ししている	<b>【頻度】</b> ・教育・訓練実施前後、もしくは1 回／年以上

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
			152	Lv2	サーバー等の設置エリアには、設備に災害対策、環境対策を実施している	<b>【規則】</b> ・火災、水害、停電に対する対策を行うこと ・温湿度管理を行うこと
		セキュリティインシデントを想定し事業継続の要件に沿った復旧に必要なデータを準備できていること。	153	Lv2	事業継続上重要なシステムについては、重要度に応じて決められた各システムの復旧ポイント、復旧時間を満足するデータと手順が整備されている	<b>【規則】</b> ・求められる復旧ポイントへ復帰可能なバックアップ及びトランザクションデータログを保管すること。 ・求められる復旧時間でリストアできる手順書を整備すること  <b>【対象】</b> ・事業継続上重要なシステム

# 4. 指導シラバス（ツール）の活用（インシデント対応編） ～ 指導テーマ④ | セキュリティインシデント対応 ～

## シラバス案

### ■第2ステップ(第1回面談～第2回面談) セキュリティインシデント対応体制の検討と評価

#### <指導先企業側事前作業>

期間(目安)	概ね2週間
作業内容	<ul style="list-style-type: none"><li>- セキュリティインシデント対応手順書案の検討・策定。</li><li>- インシデント対応チーム(CSIRT)立ち上げに向けた検討会を推進する。</li><li>- 専門家からの指導に基づき、インシデント対応手順書のドラフト内容をレビューする。</li></ul>
使用するツール	<ul style="list-style-type: none"><li>- 記入様式   インシデント対応体制チェックリスト(★)</li><li>- 参照資料   中小企業の情報セキュリティ対策ガイドライン   付録8「中小企業のためのセキュリティインシデント対応手引き」</li></ul>

#### <第2回面談時>

確認・指導事項等	<ul style="list-style-type: none"><li>- インシデント対応チームの編成と役割分担について明確化するよう指南。</li><li>- インシデントシナリオを用いた模擬訓練計画案の策定に向けた指南。</li><li>- 次回(第3回)面談時までの企業側宿題として、具体的な訓練計画(シナリオ含む)の確認と修正指示。</li><li>- 可能であれば第3回面談時に社内での机上演習を実施すべく、プランを練る。</li></ul>
使用するツール	<ul style="list-style-type: none"><li>- 記入様式   インシデント対応体制チェックリスト(★)</li><li>- 参照資料   中小企業の情報セキュリティ対策ガイドライン   付録8「中小企業のためのセキュリティインシデント対応手引き」</li></ul>



## 4. 指導シラバス（ツール）の活用（インシデント対応編）

他社の事例などから得られている注意点を踏まえ、インシデント対応手順書の確認を行う。  
また、権限者が不在の場合の代行者が定められているか（規程されているか）を改めて確認する。  
電話回線数などを確認し取引先からの連絡にどの程度対応できるか確認し、電話でこなしきれないと思われる場合はメール、ホームページでの連絡などを考える。  
営業担当者等が取引先に連絡する場合、どの程度の先にかけることが可能かを考える（社内電話回線が不足すると思われる場合はBYODの利用について検討する 等 の実際に発生した場合のシナリオの実現可能性について検討する

### 【実際に2回目訪問終了後の指導内容報告】

指導先企業が作成したインシデントシナリオの説明を受け、過不足についてディスカッション。シナリオをブラッシュアップした。取引先への連絡、警察などへの相談等、いくつかの不十分と思われるところについて事例等をまじえ説明し追加修正を加えた。復旧するサーバの優先順位づけなどについても踏み込んだ議論を行った。対応に必要な人的な資源の確保についても議論した。

## 4. 指導シラバス（ツール）の活用（インシデント対応編）

スケジュール	予定時間	項目
13:10-13:20	10分	前回実施内容の確認 本日の進め方の確認
13:20-14:20	60分	作成いただいたシナリオ案の確認 貴社規程類との整合性確認
14:20-14:30	10分	休憩
14:30-15:10	40分	インシデント対応手順書の例の記載項目との 比較突合せ
15:10-16:00	10分	全体を通してのQ&A 次回以降の日程と準備事項の確認 追加依頼資料等

## 4. 指導シラバス（ツール）の活用（インシデント対応編）

※インシデント対応手順書例 今回指導企業においてはタイムスケジュールから担当者ごとの対応手順書レベルまで作成していた

ステップ	フェーズ	手順項目	詳細手順	担当者	予め準備しておかなければならないもの
検知・初動対応	検知と連絡受付	感染兆候の検知	IT管理担当者が社内PCやサーバーの感染兆候（暗号化やメッセージ表示）を確認し、クラウドサービスの異常も検知する。	IT管理担当者	連絡先リスト、感染兆候チェックリスト
	初動対応	感染端末の隔離	IT管理担当者が感染端末をネットワークから切断し、クラウドサービスのアクセスも一時停止。	IT管理担当者	感染端末隔離手順、連絡先リスト
	対応体制の立ち上げ	インシデント対応会議の開催	IT管理担当者が経営管理部長に状況を報告し、インシデント対応会議を招集。経営管理部長がインシデント対応会議にて、IT管理担当者、製造管理部門主任、経営層などの役割分担を確認。	経営管理部長	役割分担リスト、連絡先リスト
	対応体制の立ち上げ	関係者への周知	IT管理担当者が経営管理部長にインシデント発生を報告し、経営管理部長が全従業員に使用停止を通知。必要に応じて取引先にも速報。	IT管理担当者、経営管理部長	連絡先リスト
報告・公表	第一報	初期報告	IT管理担当者が感染範囲を報告し、経営管理部長および社長に対し詳細を報告。社長が主要取引先に発生を説明。	IT管理担当者、経営管理部長、社長	連絡先リスト、詳細報告書テンプレート
	第二報以降・最終報	詳細報告書の作成	IT管理担当者が感染経路や対応進捗を含む報告書を作成し、経営管理部長が取引先や従業員に適切に説明できるよう調整。	IT管理担当者、経営管理部長	詳細報告書テンプレート

## 4. 指導シラバス（ツール）の活用（インシデント対応編） ～ 指導テーマ④ | セキュリティインシデント対応 ～

### シラバス案

#### ■第3ステップ(第2回面談～第3回面談)

#### インシデント対応模擬訓練(机上演習)の実施とレビュー

##### <指導先企業側事前作業>

期間(目安)	概ね2週間
作業内容	<ul style="list-style-type: none"><li>- インシデント対応訓練計画を策定する(シナリオ含む)。</li><li>- インシデント対応訓練実施に向けて、社内調整を行う(演習参加メンバーの選定、スケジュール調整等)。</li></ul>
使用するツール	<ul style="list-style-type: none"><li>- 記入様式   インシデント対応体制チェックリスト(★)</li><li>- 記入様式   インシデント対応机上訓練計画案(★)</li><li>- 参照資料   中小企業の情報セキュリティ対策ガイドライン   付録8「中小企業のためのセキュリティインシデント対応手引き」</li></ul>

##### <第3回面談時>

確認・指導事項等	<ul style="list-style-type: none"><li>- 策定したインシデント対応手順書に従い、模擬机上訓練を実施。社員全体ではなく、セキュリティ担当者を対象とした訓練としてもよい。専門家が訓練のコーディネイトを支援する。</li><li>- 訓練結果レビューの考え方について指導するとともに、今後の継続的な訓練体制の構築とガイドライン策定に向けたアドバイスを行う。</li></ul>
使用するツール	<ul style="list-style-type: none"><li>- 記入様式   クラウドサービスチェックリスト(★)</li><li>- 参照資料   インシデント対応机上演習資料</li><li>- 参照資料   中小企業の情報セキュリティ対策ガイドライン   付録8「中小企業のためのセキュリティインシデント対応手引き」</li></ul>

## 4. 指導シラバス（ツール）の活用（インシデント対応編）

訓練を実施する。実施後に必ず振り返りを行い。よかったところ、改善すべきところを洗い出してインシデント対応手順書のブラッシュアップを図る。

## 5. 実際の指導実績と効果

### 【マネジメント指導後に提出した私のレポート】

営業、設計等別に具体的な手順書まで作成し実施。演習シナリオもよく考えたものになっていた。実際にシナリオに基づき進めるなかで、若干の不具合が発生するものの、都度、協議しながら修正し演習を進めた。そのため、営業、設計等への説明（教育の側面も含むが）を含め予定より時間がかかった。演習シナリオがランサムウェア対応のみでなく、なりすましメールの他社への送信、情報漏洩を含んでおり、少し盛りすぎな内容であったことも問題の焦点がはっきりせず時間がかかる要因となった。その点に配慮しながら、問題整理をしながらのアドバイスができた。

中部地方		事例No.5
業種	製造業	自動車業界ガイドラインに沿った具体的なインシデント対応指南
従業員数	50人以下	
資本金	5千万円以下	A株式会社
推進担当者	(非公開)	
指導専門家	久保田 秀男	

## ■ 企業・団体紹介

生産設備の設計から製造・保守までを手掛ける、様々な規模の機器やオートメーションシステムを提供している。製造現場の要求に応じた最適な解決策を提案し、生産性向上と効率化を支援することで、ものづくり現場を支えている。

## ■ 参加の動機

約2年前から自動車産業サイバーセキュリティガイドライン及びチェックシートへの対応を進めてきた。同ガイドラインに沿って、社内体制の整備、規程の整備、情報資産の洗い出し(台帳整備)等を実施しているものの、対応が適切であるか判断ができなかった。

今回、地元の商工会議所からの案内で相談会及びマネジメント指導が受けられることを知り、専門家の意見を聞くことができるとの機会と考え参加した。

## ■ 情報セキュリティ上で感じていた課題

- 規程整備や情報資産の洗い出しなど、ガイドラインでは多岐にわたるチェック項目が設定されている。これに基づき一通り対策を講じたものの、それが適切な水準に達しているか判断ができなかった。
- 規程や体制の整備を踏まえて、インシデント演習等の実効的な取り組みを進めたいが、取引先や公的機関などへの対応が必要となるため、適切に実施できるかという懸念点があった。

## 専門家指導のポイント

- 自己診断チェックシートと整備済みセキュリティ規程を突き合わせ、適切に状況確認・アドバイス

同社は自動車産業サイバーセキュリティガイドラインに沿った形で規程や手順、体制整備をかなり高いレベルで実施済みであった。改めて自己診断チェックシートで対策に抜け漏れがないかを詳細に確認し、一部取り組みが過剰であると思われる項目については適切な水準にするよう指南した。

- より実効的なセキュリティ対策の意識付けのために、手順に沿ったインシデント対応演習を実施

作成済みのインシデント対応手順書に沿った形で、「ランサムウェア対応」のシナリオによる演習を実施することを同社は希望した。同社が作成したシナリオ案をチェックし、特に取引先への連絡や警察への相談などのタイミング、実際のインシデント発生時に想定される細かい事象等も盛り込むよう指導した。また複数あるサーバの復旧手順(順序)や、対策に必要な人的資源など、業務内容に応じてかなり踏み込んだ内容まで確認した。作成したシナリオをもとに、実際に社長や営業担当者も交えて会社全体で本格的な演習を実施した。組織内での情報伝達や対応等一通り演習を行うことで、シナリオ自体の不備や要改善点(やや盛り込みすぎている等)も浮き彫りになった。

## 指導先企業からのコメント

### ■ 専門家指導の成果

- 取り組み状況について具体的なアドバイスをいただくことで、今後の情報セキュリティ推進の方向性が一層明確になった。
- 短期間で効率的に指導をいただき、シナリオ作成から演習まで無事に実施できた。演習を通じて、社内外での情報伝達や実践的な対応能力の向上、また会社全体のサイバーセキュリティ対策の意識の向上にもつながった。

### ■ ご意見・ご感想

社内では気づけなかった改善点を指摘していただき、大変参考になった。今後も、継続的に効果的な対策を実施できるよう取り組む所存である。



## 6. セキュリティ専門家としての心構え 1/4

### 信頼を守る使命と責任

- セキュリティ専門家は「社会の信頼を守る守護者」
- 情報の背後には必ず“人”と“社会”がある
- 小さなミスが大きな損害に直結する
- 倫理観・誠実さがプロとしての基本
- 「一度の事故が企業や社会の信頼を失わせる。技術力よりもまず責任意識と倫理観が何より大切」



## 6. セキュリティ専門家としての心構え 2/4

### 技術よりも倫理を優先する姿勢

- 「できるからやる」ではなく「できてもやらない」判断が重要
- 情報へのアクセス権 = 信頼の証
- 法令遵守 + 社会的倫理の両立
- 誠実な対応が最大のセキュリティ対策
- 「情報を扱う立場では、技術力以上に倫理観が問われる。」

## 6. セキュリティ専門家としての心構え 3/4

### 変化に学び、仲間と守る

- 脅威や技術は常に進化し続ける
- 継続的な学習と情報共有が不可欠
- 経営・現場・利用者との連携が鍵
- 専門用語をかみ砕いて伝える力＝信頼を築く力
- 「セキュリティは一人では守れない。学びと協働が鍵。」

## 6. セキュリティ専門家としての心構え 4/4

### 社会の安全を支えるプロフェッショナルへ

- セキュリティ専門家は公共性の高い職業
- インシデント時は「隠さず・正確に・迅速に」
- 技術 × 倫理 × 継続的努力 がプロの三本柱
- 信頼される行動が最も強い防御
- 「技術を操る前に、信頼を守る覚悟を持つ。」

## 7. セキュリティマネジメント指導：課題と改善

経営層の関与が薄い場合などは、その後の支援先の改善の進捗がうまくいかないことも考えられるが、支援前よりよい状態となるように努めることが必要

これまで支援に入ったところは、概ねセキュリティアクション2つ星を宣言している。

## 8. まとめ ― 指導を通じて得られた学びと今後

本業で情報セキュリティに関わっていない場合でも、自社で不足していること、あるいはできているところを客観的にとらえることができたことは大きな学び