

マネジメント指導

ツール と 事例

チャレンジした感想

2025年11月20日
セキュリティマネジメント指導ツール活用セミナー

自己紹介



高橋 真悟

愛知県名古屋市在住

2019年10月1日に登録

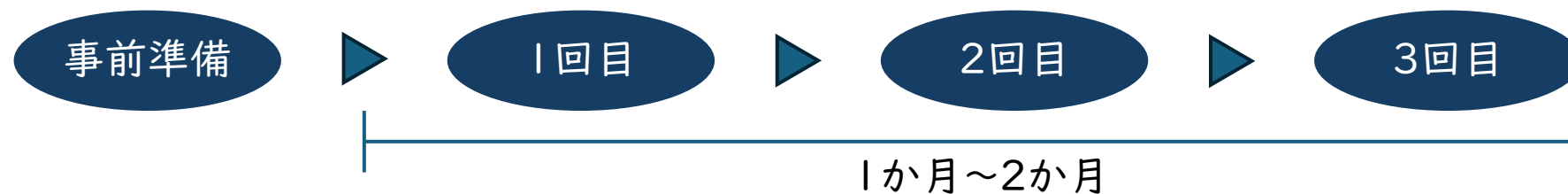
セキュリティプレゼンターへ登録し
2022年度からIPAセキュリティセミナー事務局からの
依頼で年に数回講師として登壇
他にも業界団体等の依頼でセキュリティ講師として活動しています。

ネットワーク設計の経験とサンデープログラマーとして
薄く広く情報セキュリティに携わっています。
最近はログの分析なども行っています。

5つの指導テーマとそれぞれにツールがあります



3回の訪問で完了するように構成されています



セキュリティマネジメント指導ツールの良かった点

課題となっていると思われる5つのテーマ

3回で完了するため、1回ごとのやることがはっきりしている

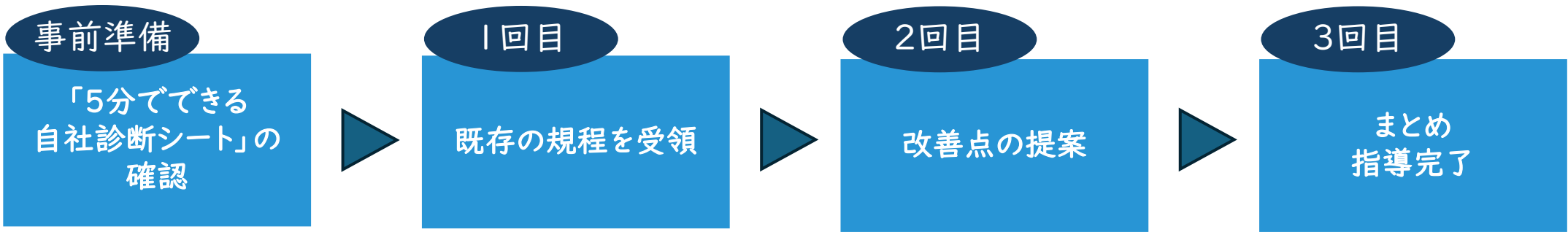
ツールの活用で一定の品質が確保される

2024年度に
取り組んだマネジメント指導について

指導テーマ「情報セキュリティ規程の整備」

(初回訪問時)

DX推進のために生成AIの活用のルールを定めたい。
あわせて既存のセキュリティ規程をチェックしてもらいたい。



活用したツール等

指導ツール

- 情報セキュリティ関連規程（サンプル）
- 情報セキュリティ規程チェックシート

- テキスト生成AI 利活用におけるリスクへの対策ガイドブック（α版）デジタル庁」
- AI事業者ガイドライン（第1.0版）「総務省 経済産業省」
- 自治体、団体等が公表しているガイドライン等

ツールの活用：サンプルと比較して規程の漏れをチェック

○	制定済
▲	一部未制定
✖	記載なし

自社診断結果	高得点
セキュリティ規程	制定済み

制定済のセキュリティ規程

1	組織的対策	▲
2	人的対策	○
3	情報資産管理	○
4	アクセス制御及び認証	○
5	物理的対策	▲
6	IT機器利用	○
7	IT基盤運用管理	○
8	システム開発及び保守	✖
9	委託管理	✖
10	情報セキュリティインシデント対応及び事業継続管理	▲
11	テレワークにおける対策	▲

比較

情報セキュリティ関連規程（サンプル）

1	組織的対策
2	人的対策
3	情報資産管理
4	アクセス制御及び認証
5	物理的対策
6	IT機器利用
7	IT基盤運用管理
8	システム開発及び保守
9	委託管理
10	情報セキュリティインシデント対応及び事業継続管理
11	テレワークにおける対策

サンプルと比較後に気になる点をチェック

既存の規程

紙媒体での重要情報は施錠された書庫等に保管すること

事故が発生した際は速やかに報告すること

具体的に記載しないと理解してもらえないのでは？

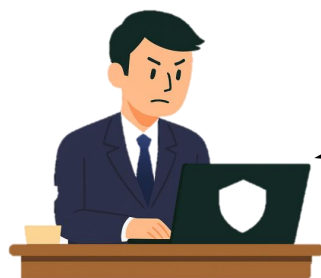
重要情報とは

- 取引先から預かっている情報
 - 個人情報
 - 「社外秘」「部外秘」と記載がある書類
- など

下記に記載されている事故が発生した時および発生の際恐れがある場合は速やかに〇〇に報告すること

- ウイルス対策ソフトからの警告メッセージをうけとったとき
 - 不審なメールのURLをクリックしてしまったとき
 - 会社からの貸与物（パソコン、スマートフォン等）を盗難、紛失したとき
- など

生成AIの活用のためのルール作り



【指導先ご担当者】

DX推進のために生成AIを活用していきたいが、会社内の情報を学習させてしまって、その内容が公になるなどの問題は起きないようにしたい。
しかし、いろいろ制限をすることで活用が進まなくなるのではないかと心配もしている。



使用できる範囲を限定する



利用履歴を記録する

生成AI活用の際の注意事項として定めたルール

生成AIを介した
情報漏えい

- 使用する生成AIを限定する
- オプトアウトの設定

生成AIの出力結果は
正しいとは限らないこと

- 過去の学習内容から偏りがある可能性
- 結果が正しいか必ず確認すること

第三者の権利を
侵害する恐れがあること

- 著作権等を理解してもらうため用語の説明

第3回

新規規程の運用方法の確認

新規規程の運用案について確認し、適切なアドバイスを行います。作成に際し企業側で生じた疑問や質問等に回答・アドバイスします。また、重点対策と合わせた今後の実行計画を検討するとともに、企業側で作成した基本方針や規程の見直し案について、マネジメントシステムの実効性の視点からレビューを行います。

セキュリティマネジメント指導（テーマ別）実施要領
テーマ① | 情報セキュリティ規程の整備より抜粋

あえて規程に定めない項目



【アドバイス】

脅威、脆弱性、リスクが存在することを経営層に理解をしてもらった上で許容してもらうこと

定めた規程を守らせるための取り組み



【アドバイス】

定期的な規程の見直しを規定化
ActiveDirectory等を利用したポリシーの設定
アクセスログ等の取得と管理

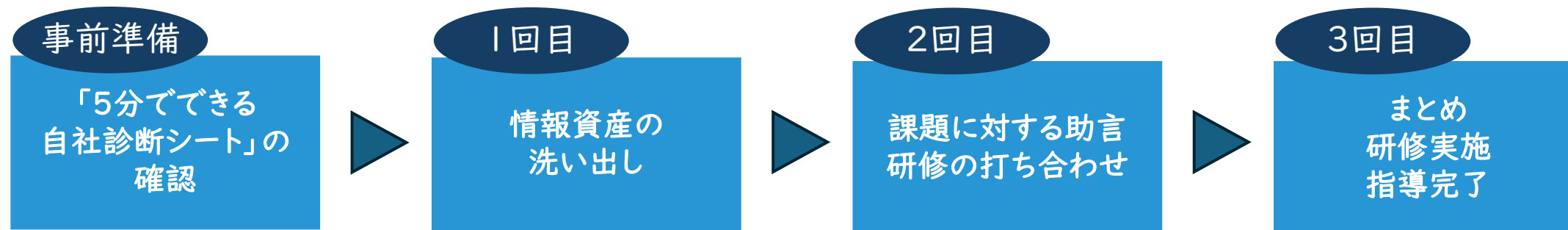
指導テーマ「従業員向けセキュリティ教育」 「情報資産の洗い出しとリスク分析」

(初回訪問時 経営層より)

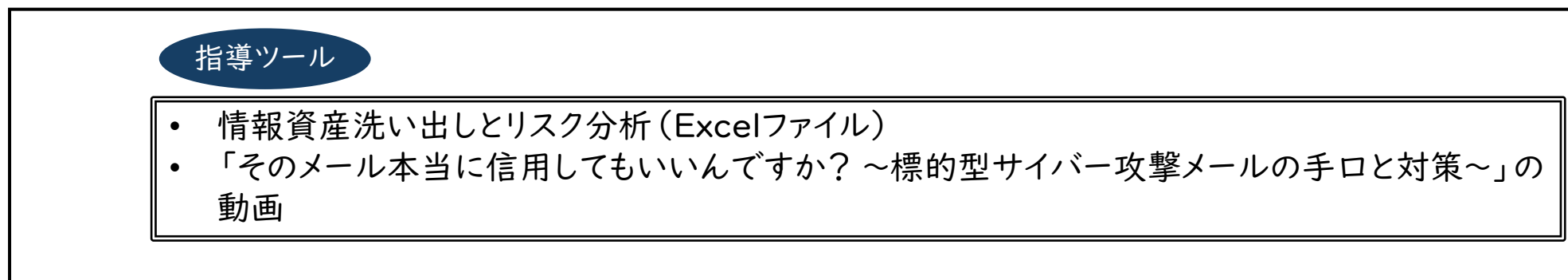
現状の取り組み状況を評価してもらいたい

(2回目訪問時 ご担当者より)

3回目は従業員を集めるので30分程度の研修を行ってほしい



活用したツール等



ツールの活用：情報資産洗い出しとリスク分析（Excelファイル）

自動保存 指導テーマ② 情報資産洗い出しとリスク分析・最終更新日時: 1月16日															
ファイル ホーム 挿入 ページレイアウト 数式 データ 校閲 表示 自動化 開発 ヘルプ Acrobat															
A1 情報資産管理台帳															
1	情報資産管理台帳														
2	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			評価値			保存期限	登録日	現状から想定されるリスク（入力）
3							個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度		脅威の発生頻度 ※「脅威の状況」シートに入力すると表示
4															脆弱性 ※「脆弱性の状況」シートに入力すると表示
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															

【指導先企業】

全てを洗い出すのは非常に大変で難しい



【アドバイス】

全てを網羅することが望ましいが
今回はデータは除いて、サーバーやルーター等機器
の一覧を書き出してもらいたい
2回目以降にデータ、紙情報の一部を追加していき
ましょう

研修用の動画はたくさんあります



サンプルプログラム①_標的型サイバー攻撃メールの手口と対策
映像+パワーポイント資料



サンプルプログラム②_内部不正による情報流出のリスク
映像+パワーポイント資料

他にもIPAのウェブサイトには研修資料の作成に役立つ多くの映像コンテンツがあります。

映像で知る情報セキュリティ

<https://www.ipa.go.jp/security/videos/list.html>

私の マネジメント指導におけるスタンス①

ありのままの現状を把握 (否定しない)

中小企業の多くは限られたリソースの中で取り組んでいます。担当者も他の業務と兼務していることが多くセキュリティ対策は優先度が低いことが多いです。



私の マネジメント指導におけるスタンス②

指導の流れは
ツールを意識しつつも柔軟に

マネジメント指導を希望する企業は中小企業の中ではセキュリティ対策への感度は高く、話を前向きに聞いてはくれますが、ツールで設定されている項目を網羅することは難しいこともあります。

ツールに沿ってマネジメント指導を行うことにこだわりすぎると担当者が「うちでは無理だ」とあきらめてしまうかもしれません。



私の マネジメント指導におけるスタンス③

例えば「ソフトウェアの更新を徹底する」としても

- ゼロデイ攻撃の可能性
- 人的要因による更新作業もれ など

絶対に安全である状態にはならないことを理解してもらいましょう。

残留リスクの共有

対策は事故の発生確率・被害の大きさを低減させるもの

対策を進めた項目であっても、絶対に事故が発生しないとは断言できません。また、「〇〇の部分においては技術的、費用的に現時点では対応しない。」等の結果となることもあります。

残留リスクを説明し、継続的に対策を進めてもらえるようアドバイスをすることも重要です。



5つのテーマから逸脱していないのか

申込時のテーマが変更することは良いのか

正直悩みました。

「わずかでもテーマに該当する」

「セキュリティ対策が進むきっかけになる」

上記の観点から指導先企業の希望を優先して対応しました。

マネジメント指導にチャレンジした感想

指導ツール以外にもIPAのウェブサイトに活用できる資料が豊富

5つのテーマ以外の悩み事もある

内容によっては企業側も大変

結論

良い経験になりました

約1か月間で3回訪問し完了するというスケジュールは双方厳しく感じましたが、短期間に集中できたからこそ無事に完了できたとも感じています。

指導テーマ以外の相談は想定外ではありますが、一緒に考えるのが良いのかなと思います。

マネジメント指導を通して感じた企業側のニーズ①

専門家（誰か）に相談したい

- つながりのあるベンダーに相談しても自社商品以外の情報を提供してくれない。
- ベンダーに言われるがままに、いろいろな機器（UTM等）やソフトウェアを導入したが活用できているのかがわからない。
- そもそも何から手を付けてよいのかわからない。

マネジメント指導と通して感じた企業側のニーズ②

当たり前のことであっても
外部の人が説明することが効果的

- 「ソフトウェアの更新」、「パスワードは使いまわさない」、「怪しいメールには注意する」等のわかってはいるけど徹底できないことを社内のセキュリティ担当者が話をして、会議と同じ空気になってしまう。
- 第三者の専門家が経営層への提案を補助してくれると聞いてもらやすい。

みなさんも
「セキュリティ専門家リスト」へ登録し
マネジメント指導に取り組んでみてはいかがでしょうか

経験を通じて
視野が広がる

