令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

サイバーセキュリティを取り巻く環境および
中小企業に求められるサイバーセキュリティ対策

サイバーセキュリティ
人材育成
社内体制整備支援

講師紹介

氏名	星野 樹昭（ほしの しげあき）
業務経歴	25年（セキュリティ経験：19年）
専門分野	ITインフラ設計 / 構築 / テスト 移行設計 セキュリティ製品導入支援 ISMS導入支援
保有資格	情報処理安全確保支援士（登録番号 第002047号） MCP
コメント	官公庁や金融機関などの大規模環境から、中小零細企業規模まで、オンプレ/クラウド問わず様々な環境のITインフラ環境導入・移行の経験あり。 セキュリティ製品の導入支援では、DB暗号化ソフトウェアやWeb Application Firewall、クライアントPCのセキュリティ対応など、実績豊富。 現在はISMSコンサルも実施しており、活動は多岐にわたる。

目的

- 継続的な社内のセキュリティ対策ができる人材を育成する
- 実践的な課題解決で社内セキュリティ体制を強化する

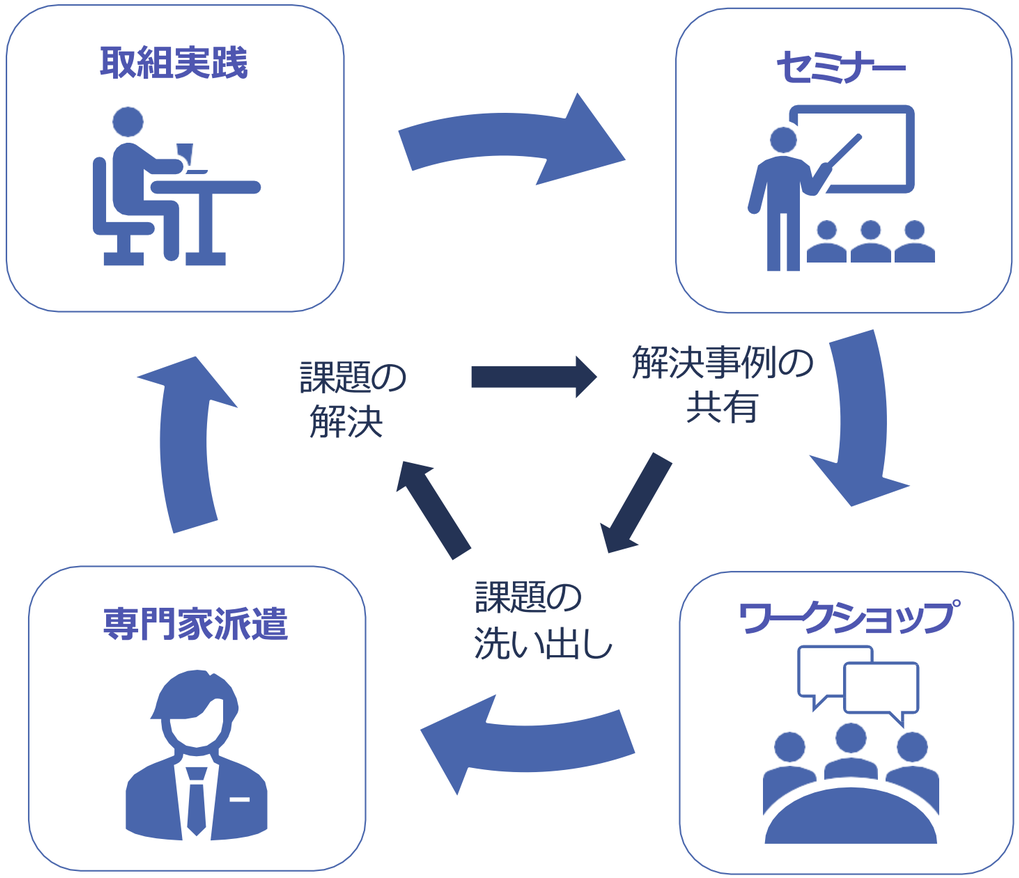
東京都他事業と本事業の位置づけ

【支援領域】 組織的支援 人的支援 技術的支援

成熟度レベル　※COBITを援用し設定		0	1	2	3	4	5
事業と主な支援領域 ＼ ステータス		セキュリティ意識もなく、対策等も考えていない状態	セキュリティ対策を実施しないといけないと思っている状態	セキュリティに関する方針・ルール、対策を決めている状態	セキュリティマネジメント計画や行動を決め、実践している状態	リスクを分析し、方針・ルール・対策の見直しを行っている状態	最適化や習慣化がされている状態
中小企業サイバーセキュリティの極意	組織的支援 人的支援	→	→				
中小企業サイバーセキュリティ向上支援事業	組織的支援 技術的支援		→				
中小企業サイバーセキュリティ対策強化サポート事業	技術的支援		→				
中小企業サイバーセキュリティ対策継続支援事業（本事業）	組織的支援 人的支援			Before →	After →		
Tcyss（東京中小企業サイバーセキュリティ支援ネットワーク）	組織的支援	→	→	→			
サイバーセキュリティ対策促進助成金	技術的支援		→	→	→	→	→

支援内容

セミナーで得た知見やワークショップの事例を参考に、専門家と決めた取組を実践します。不明点や不安点などは、コミュニティを通して質問を行い、専門家だけでなく、参加企業同士でフォローします。

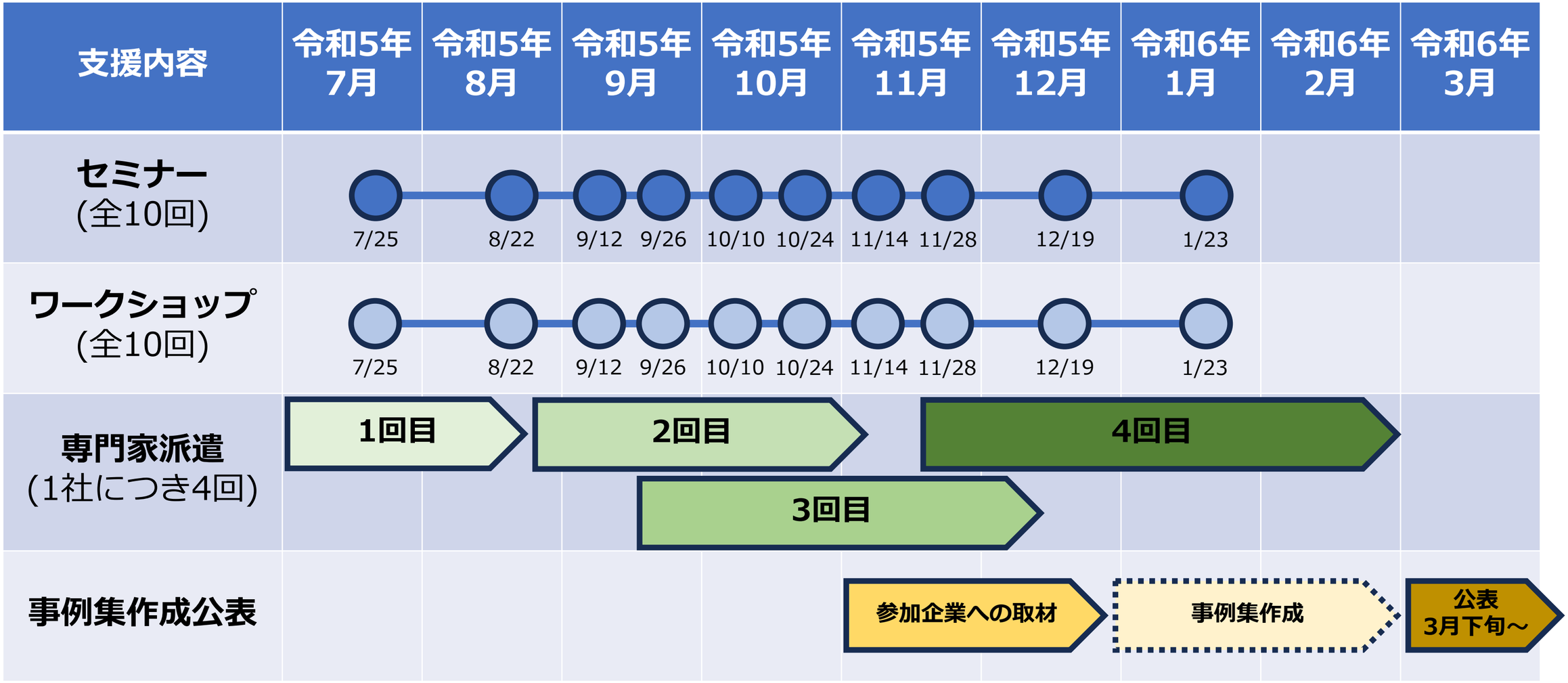


導入済みのセキュリティ機器の日常的な運用方法や、業務内容に沿ったセキュリティルールの策定方法など、中小企業の皆様が自主的にセキュリティ対策業務を運営する上で生じる疑問点の解決に直接役立つ、実践的な知識・ノウハウを講義形式でお伝えします。

ワークショップで洗い出した課題やセミナー・ワークショップの気づきをもとに、企業が直面しているセキュリティ上の問題点解決や、社内体制構築へ向けた支援を行います。

参加企業の皆様同士で、それぞれの課題に一緒に取り組み、解決策を考えます。自社の問題だけでなく、他社の事例に触れることで、様々な課題の解決に向けた引き出しとなる知識を得られます。

スケジュール


支援内容
令和5年 7月
令和5年 8月
令和5年 9月
令和5年 10月
令和5年 11月
令和5年 12月
令和6年 1月
令和6年 2月
令和6年 3月
セミナー (全10回)
7/25
8/22
9/12
9/26
10/10
10/24
11/14
11/28
12/19
1/23
ワークショップ (全10回)
7/25
8/22
9/12
9/26
10/10
10/24
11/14
11/28
12/19
1/23
専門家派遣 (1社につき4回)
1回目
2回目
3回目
4回目
事例集作成公表
参加企業への取材
事例集作成
公表 3月下旬～

セミナー内容

1. デジタル時代の社会とIT情勢
   デジタル時代の社会変革とIT情勢の関係性

2. 事例を知る：重大インシデント発生から課題解決まで
   情報セキュリティの概況
   重大インシデント事例から学ぶ課題解決

3. サイバーセキュリティの基礎知識
   各種資格試験から得るサイバーセキュリティの基礎知識
   Security Action（セキュリティ対策自己宣言）
   サイバーセキュリティ対策基準レベル

1. デジタル時代の社会とIT情勢

デジタル時代の社会変革とIT情勢の関係性

デジタル時代の社会変革とIT情勢の関係性 【参照：セミナーテキスト1-1-1.】

社会の現状と今後の動向（Society5.0）

- Society5.0とは
  「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）」
  内閣府. “Society 5.0” https://www8.cao.go.jp/cstp/society5_0/ , (参照 2023-07-06)

- Society1.0：狩猟社会
  Society2.0：農耕社会
  Society3.0：工業社会
  Society4.0：情報社会
  Society5.0：未来社会
  https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_mirai1.html
  Society5.0 ビックデータ連携がもたらす未来社会像
  https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_bigdata1.html

デジタル時代の社会変革とIT情勢の関係性 【参照：セミナーテキスト1-1-1.】

デジタルトランスフォーメーション(DX)とは

【定義】

「DXとは、企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。」

経済産業省. “デジタルガバナンス・コード2.0” https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf , (2023-07-06)

【概要】

- DXは、データやデジタル技術を使って新たな価値を生み出すこと。
- DXには、ビジネスモデルや企業文化の変革が必要。
- DX戦略では、経営ビジョンを描き、関係者を巻き込んで課題を解決する。
- DXは「知識」、「人材」、「**セキュリティ**」が重要な要素。

デジタル時代の社会変革とIT情勢の関係性 【参照：セミナーテキスト1-1-1.】

IT化とDXの違いって？？

ことば	意味	視点
IT化	情報技術を活用して業務プロセスなどを効率化し、コスト削減すること。	社内
DX	ITを含むデジタル技術を駆使してビジネスを変革し、新しい価値を生み出すこと。	顧客 社会

デジタル社会の三方良し
「売り手良し」⇒「社内」
「買い手良し」⇒「顧客」
「世間良し」　⇒「社会」

デジタル時代の社会変革とIT情勢の関係性

サイバーセキュリティ経営ガイドライン

経営者が認識するべき3原則

1. 「経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要」

2. 「サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要」

3. 「平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要」

経済産業省. “サイバーセキュリティ経営ガイドライン Ver 2.0” https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf , (2023-07-06)

2. 事例を知る：重大インシデント発生から課題解決まで

情報セキュリティの概況

重大インシデント事例から学ぶ課題解決

情報セキュリティの概況 【参照：セミナーテキスト2-1-1.】

情報セキュリティの脅威を学ぶ

【目的】

- 適切な予防策や対策を講じること

【内容】

- 攻撃手口の**傾向**を把握する
- 脅威に対する対策方法を理解する

【活用するべき代表的な刊行物】

- 情報セキュリティ白書

  情報セキュリティに関する現状や課題、脅威、対策について包括的に学ぶことができる。毎年発行されている。

- 情報セキュリティ10大脅威

  1年間の状況を反映して作成され、何を重視して対策を実施するべきかを学ぶことができる。毎年発行されている。

IPA.”情報セキュリティ白書2022”.
https://www.ipa.go.jp/publish/wp-security/sec-2022.html
(参照 2023-07-06).

IPA.”情報セキュリティ10大脅威 2023”.
https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf
(参照 2023-07-06).

情報セキュリティの概況 【参照：セミナーテキスト2-1-2.】

情報セキュリティ白書

【記載内容】

- セキュリティインシデントの事例
- セキュリティ対策強化の取組み
- サイバーセキュリティ経営ガイドライン
- 国内外のセキュリティの動向
- セキュリティ人材の育成
- 中小企業のセキュリティ対策
- 個別テーマ（IoT、インフラシステム等）のセキュリティ動向
- セキュリティツールの紹介

情報セキュリティの概況 【参照：セミナーテキスト2-1-3.】

情報セキュリティ10大脅威 [組織編]

順位	前年順位	組織
1	1	ランサムウェアによる被害
2	3	サプライチェーンの弱点を悪用した攻撃
3	2	標的型攻撃による機密情報の窃取
4	5	内部不正による情報漏洩
5	4	テレワーク等のニューノーマルな働き方を狙った攻撃
6	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	8	ビジネスメール詐欺による金銭被害
8	6	脆弱性対策の公開に伴う悪用増加
9	10	不注意による情報漏えい等の被害
10	圏外	犯罪のビジネス化（アンダーグラウンドサービス）

IPA.”情報セキュリティ10大脅威 2023”. https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf (参照 2023-07-06).

情報セキュリティの概況 【参照：セミナーテキスト2-1-3.】

情報セキュリティ対策の基本

攻撃の糸口	対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・糸口を知る	手口から重要視するべき対策を理解する

備える対象	対策の基本＋α	目的
インシデント全般	責任範囲の明確化	クラウドサービスを契約する際に、インシデント発生時は誰が対応する責任があるのかを明確化する
クラウドの停止	代替案の準備	業務が停止しないように代替案を準備する
クラウドの仕様変更	設定の見直し	更新情報を定期的に確認し、仕様変更により意図せず変更された設定を適切な設定に直す

IPA.”情報セキュリティ10大脅威 2023”. https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf (参照 2023-07-06).

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-1.】

インシデント事例から学ぶ

【目的】

- 予防策の理解と強化
- リスクの認識
- 教育／訓練の材料
- 事後対応の改善

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

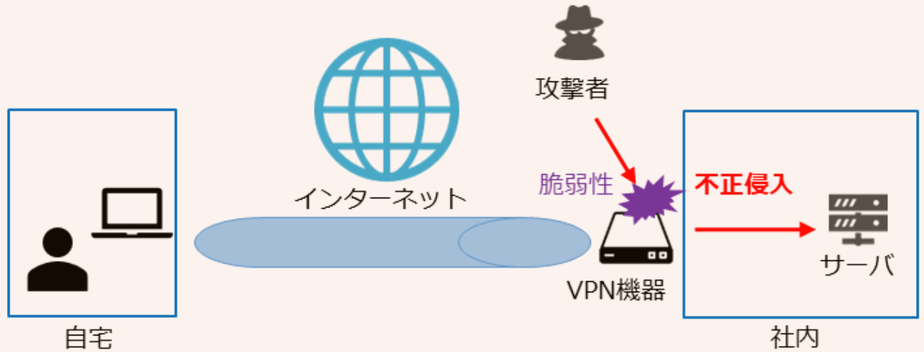
テレワークによるサイバー被害

【事例概略】

- テレワーク導入のために、社外からVPN接続できるようにした。
- VPN機器の脆弱性対応を実施した。
- すでに接続アカウントは抜かれた後で、そのアカウントを悪用された。

【対処ポイント】

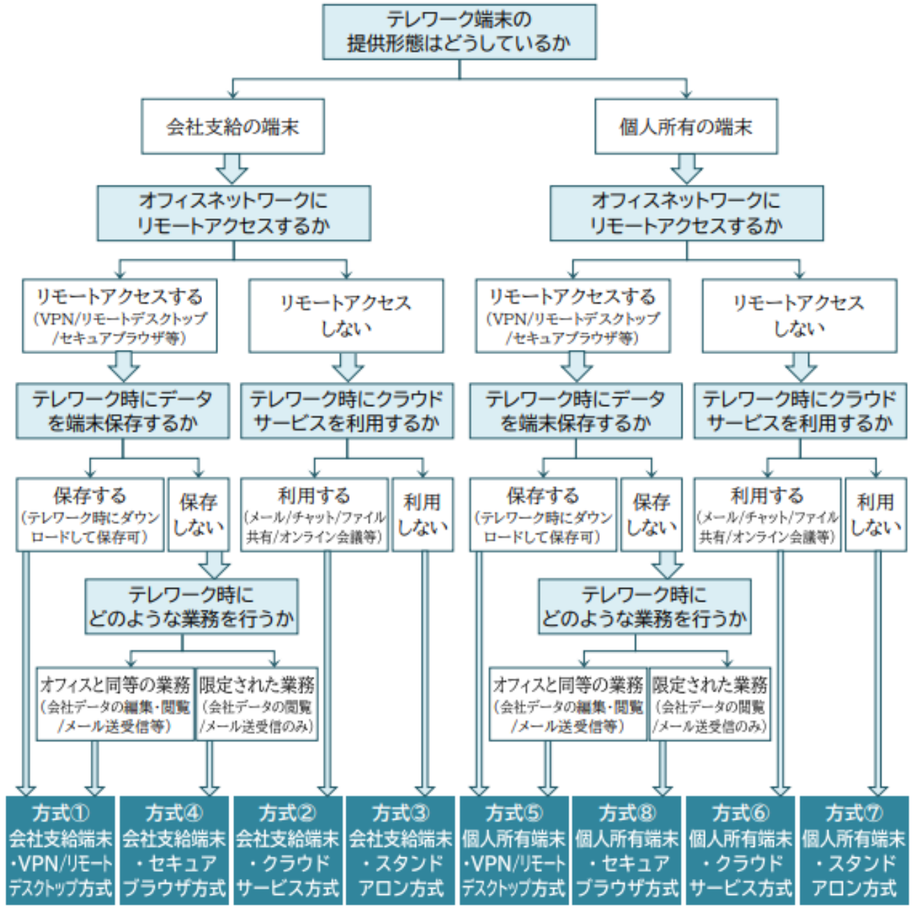
- 脆弱性を悪用されることで、何が起こるのかを理解する。
- すでに攻撃を受けていることを前提とする。



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【テレワーク方式概要】



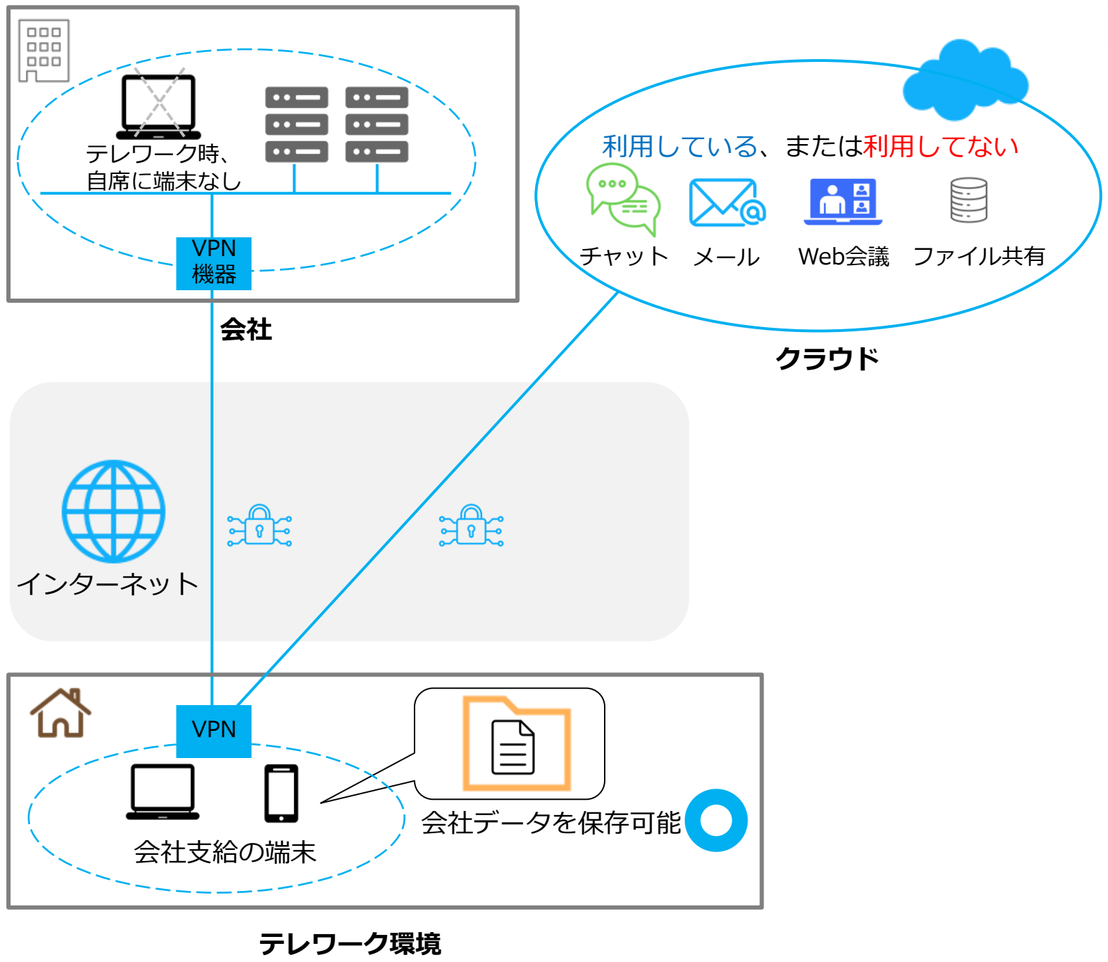
No	方式名
方式1	会社支給端末・VPN/リモートデスクトップ方式
方式2	会社支給端末・クラウドサービス方式
方式3	会社支給端末・スタンドアロン方式
方式4	会社支給端末・セキュアブラウザ方式
方式5	個人所有端末・VPN/リモートデスクトップ方式
方式6	個人所有端末・クラウドサービス方式
方式7	個人所有端末・スタンドアロン方式
方式8	個人所有端末・セキュアブラウザ方式

総務省. ”中小企業等担当者向けテレワークセキュリティの手引き”. https://www.soumu.go.jp/main_content/000753141.pdf (参照 2023-07-06).

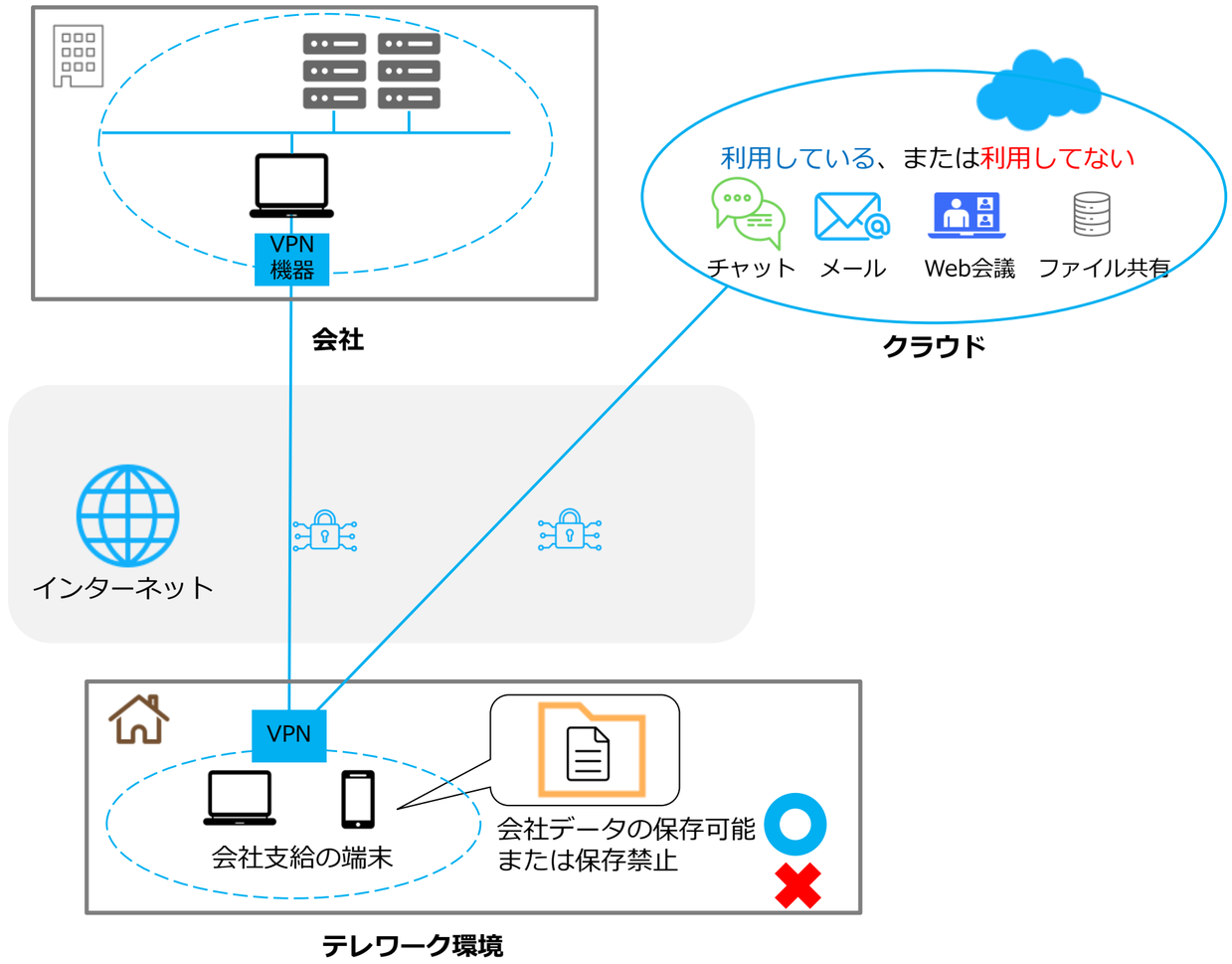
重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【VPN方式】



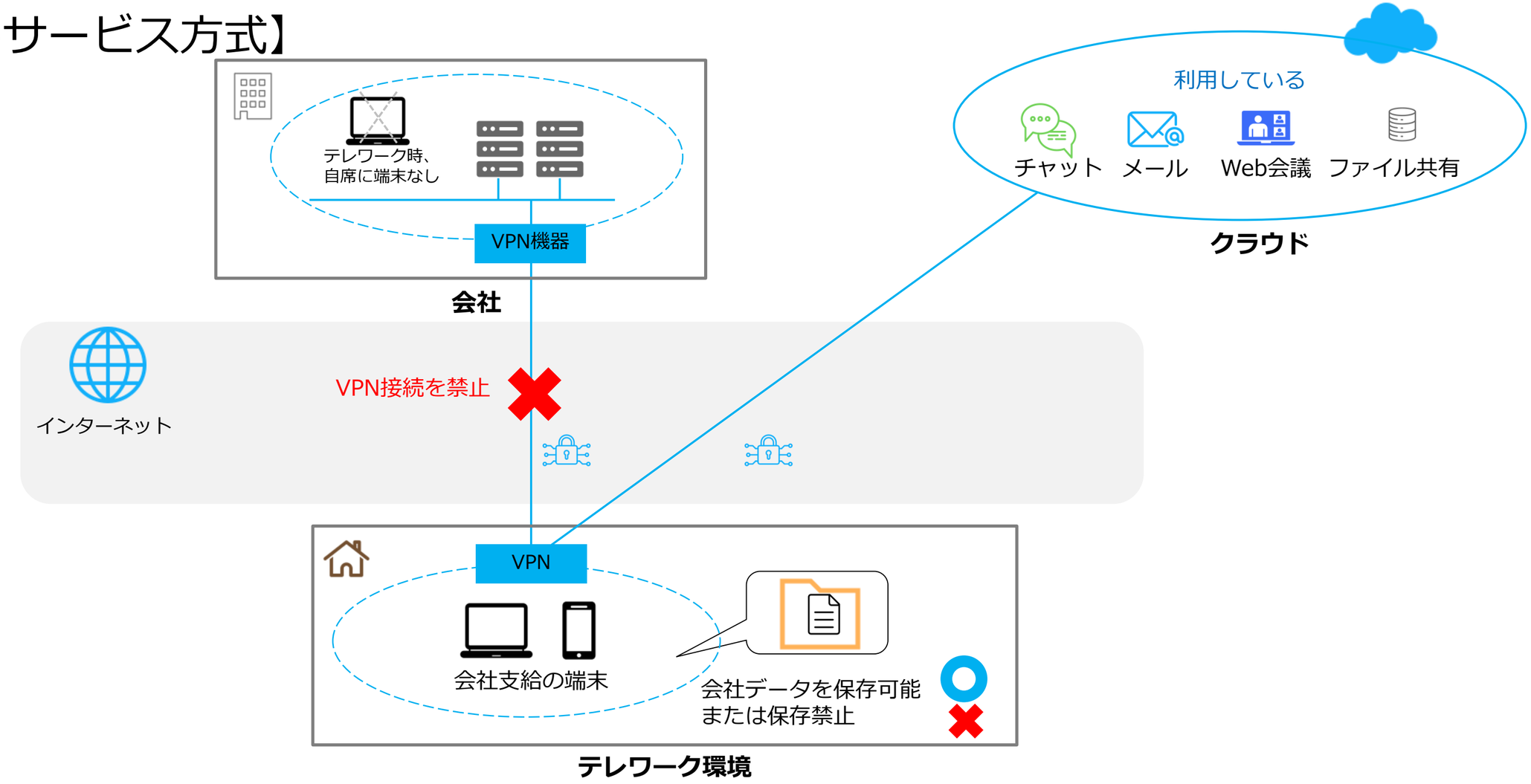
【リモートデスクトップ方式】



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

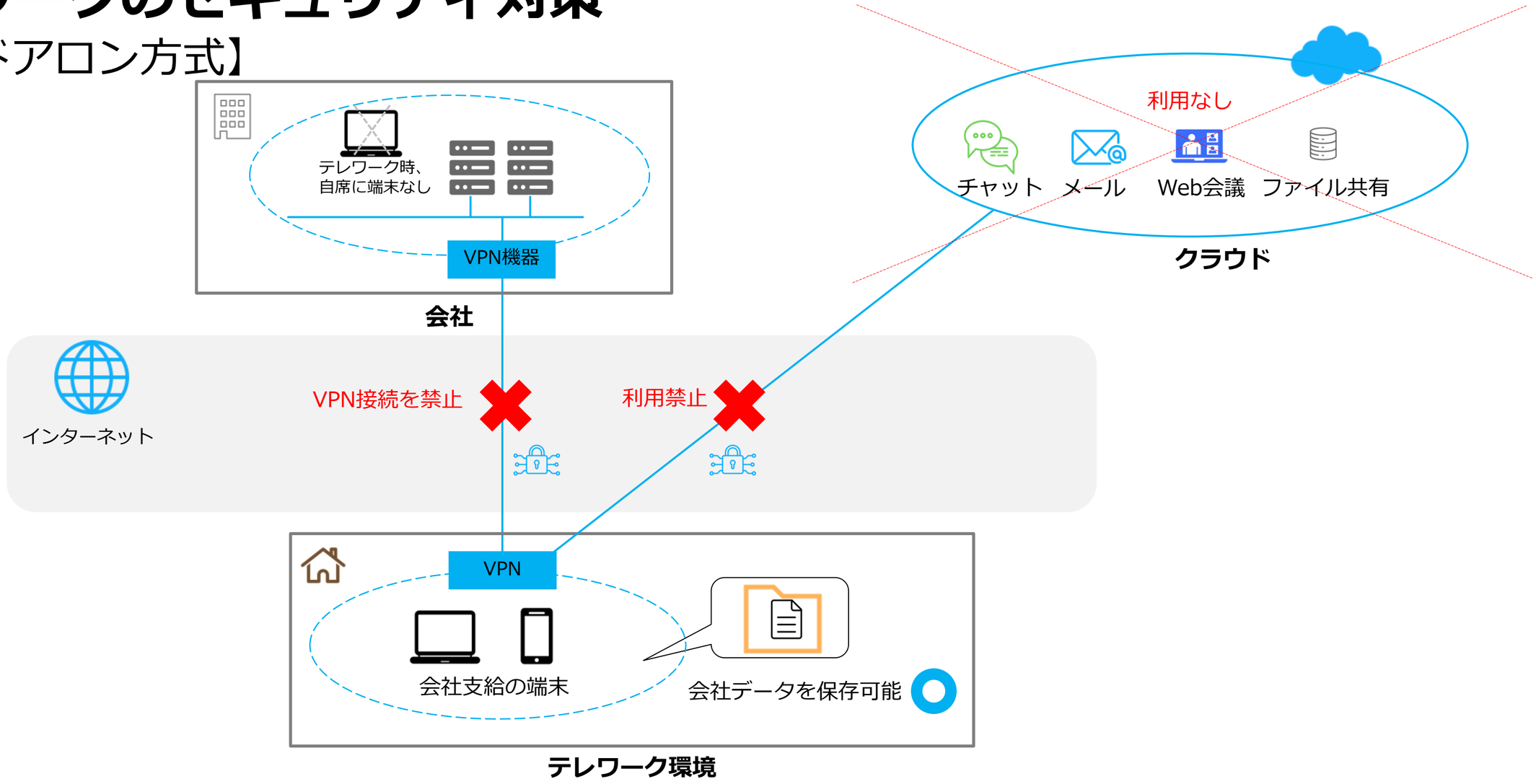
【クラウドサービス方式】



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

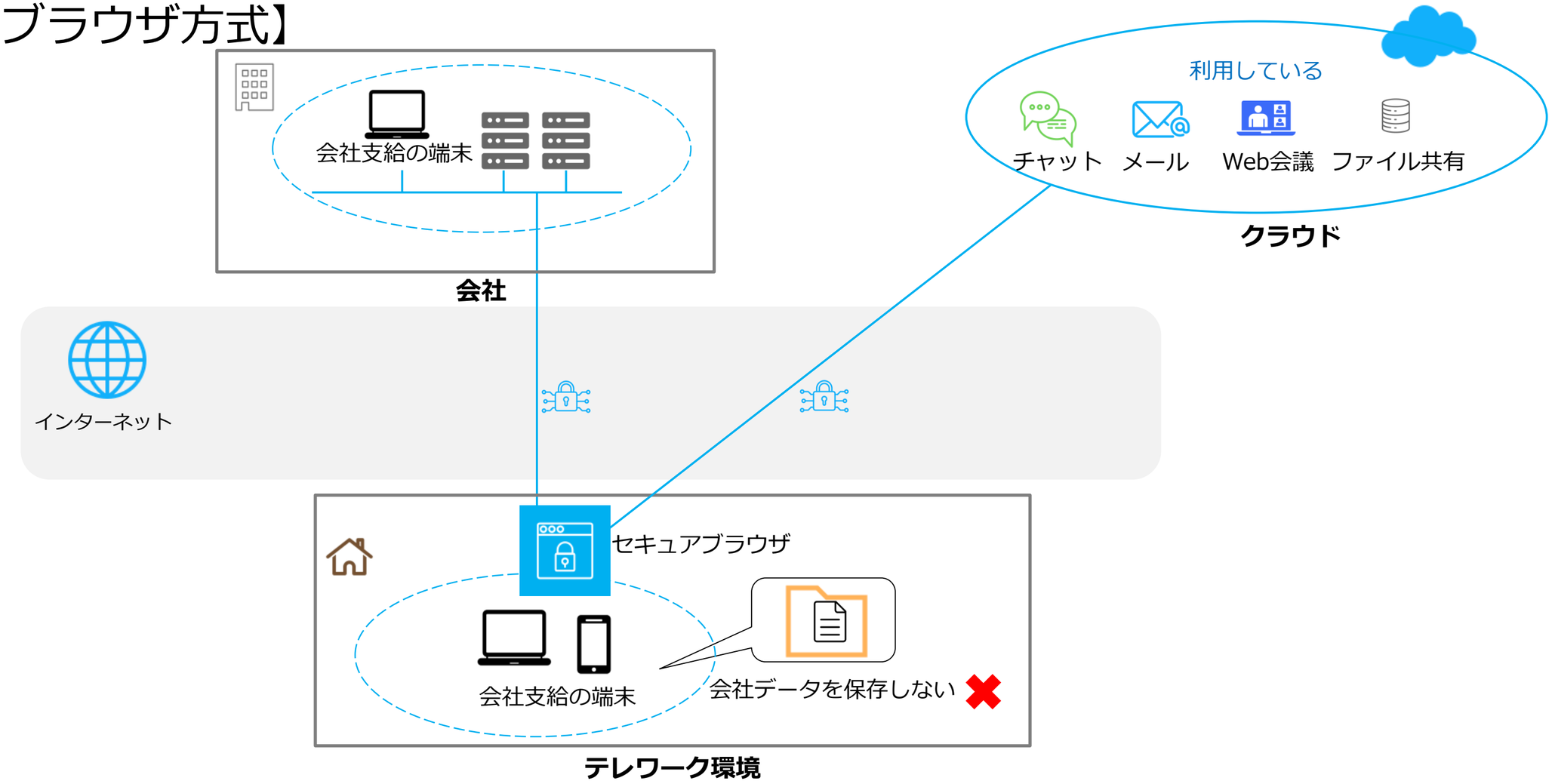
【スタンドアロン方式】



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【セキュアブラウザ方式】



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【想定される脅威】

- マルウェア感染
- 不正アクセス
- 端末の紛失・盗難
- 情報の盗難

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【想定される脅威の起因と対策】

脅威の起因	想定される対策
マルウェア感染 • 添付ファイル付きのメールを受信し開封 • 悪意のあるサイトを閲覧し、ソフトをダウンロード • USBメモリの接続	**マルウェア感染** • 検知製品（EPP）の導入 →不十分 • 挙動監視・対応支援製品（EDR）の導入 • UTM（マルウェア検知機能）の導入 • USBの利用制限 • USB自動実行の禁止
不正アクセス • VPN機器の脆弱性 • パスワードの使いまわし • 強度の弱いパスワード設定	**不正アクセス** • 脆弱性の確認とパッチ適用 • サイトやサービスごとにパスワード変更 • 10文字以上の複雑なパスワード作成 • MFA（多要素認証）の導入 • UTM（IPS/IDS機能）の導入

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【想定される脅威の起因と対策】

脅威の起因	想定される対策
端末の紛失・盗難 • サテライトオフィスに端末を忘れて帰って紛失 • 電車やタクシー置き忘れ、紛失 • カフェ等で離席した際に盗難	**端末の紛失・盗難** • 社内ルールの徹底 →出しっぱなしにしない お酒を飲むときは持ち歩かない タクシーでは荷物を出口側に置く • ケンジントンロックの利用
情報の盗難 • Web会議のURL不正利用 • 覗き見 • フリーWifiの利用	**情報の盗難** • Web会議の入室にパスワードを設ける • 覗き見防止フィルターを付ける • Windows Firewallを有効にする

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-2.】

テレワークのセキュリティ対策

【チェックリストの活用】

- テレワーク方式ごとのチェックシートが用意されている
- チェックシートは、2種類の優先度ごとに記載されている
  優先度：◎
  　セキュリティ対策の重要性が高いもののうち、実施難易度が低い（専門知識、追加コストの観点で懸念が小さい）もの
  優先度：○
  　セキュリティ対策の重要性が高いもののうち、実施難易度が中程度（ITセキュリティに関する知識を必要とするが、実施困難ではない）もの
- 具体的な設定内容については、設定一覧を活用する

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト3-1-1.】

EPPとEDR、UTMについて

EPP（Endpoint Protection Platform）の役割

- マルウェアの**感染を防止**することに特化した製品
  →パターンマッチングや振る舞い解析による検知製品

EDR（Endpoint Detection Response）の役割

- マルウェア**感染後の対応**を支援する製品
  →感染後、攻撃が始まる前に脅威を検知し、原因の削除や対処法を提供する。

UTM（Unified Threat Management）の役割

- 多くのセキュリティ機能を一元化させた製品
  →ファイアウォール、IPS/IDS、アンチウイルスなどの機能が含まれる。

重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-2-4.】

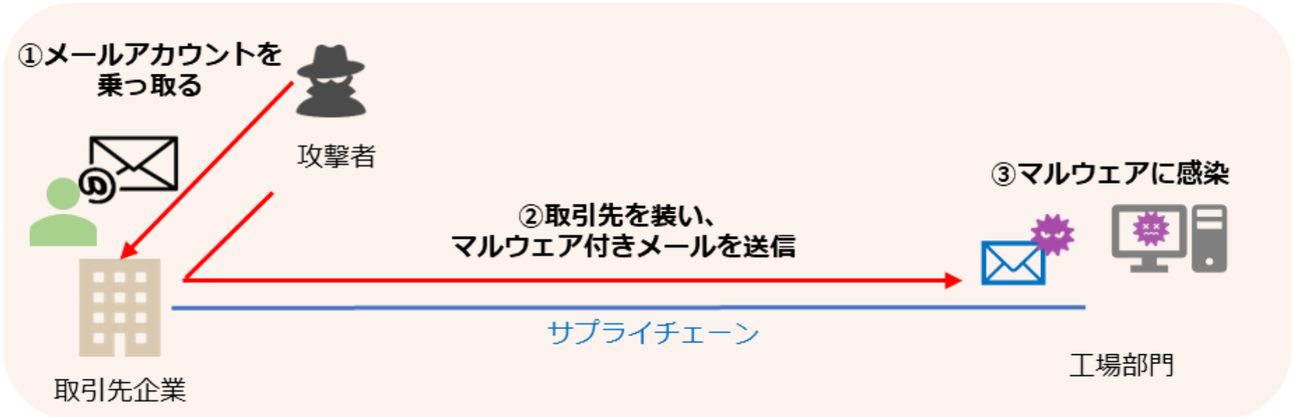
サプライチェーンを介した標的型メール攻撃

【事例概略】

- 取引先企業のメールアカウントが乗っ取られる。
- 攻撃者が取引先企業のふりをして、マルウェアが添付されたメールを送信してきた。
- 受信したPCのうち、2台がマルウェアに感染した。
- EPPでは検知できず、EDRによって早期検知ができ、感染拡大を食い止めた。

【問題点・課題】

- 攻撃者は正規アカウントを乗っ取っているため、不審な点を見つけにくい



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-3-2.】

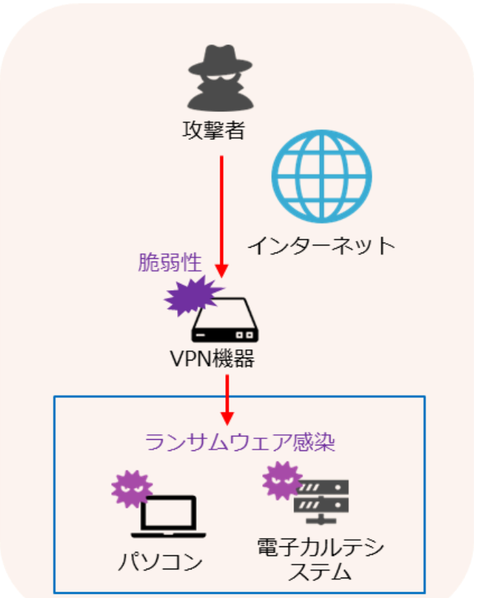
ランサムウェアによる電子カルテシステムの停止

【事例概略】

- リモートメンテナンス用のVPN機器の脆弱性が悪用され、不正アクセスされる。
- LockBit2.0が仕掛けられ、電子カルテ関連サーバが暗号化される。
- 事前に策定していたBCPを発動し、発生当初から災害級の扱いでインシデント対応にあたった。

【問題点・課題】

- VPN機器の脆弱性が放置されていた。
- 脆弱なパスワードが使用されており、簡単に特権アカウントでシステムに接続できた。
- ベンダー側のセキュリティ知識が不足していた。



重大インシデント事例から学ぶ課題解決 【参照：セミナーテキスト2-3-3.】

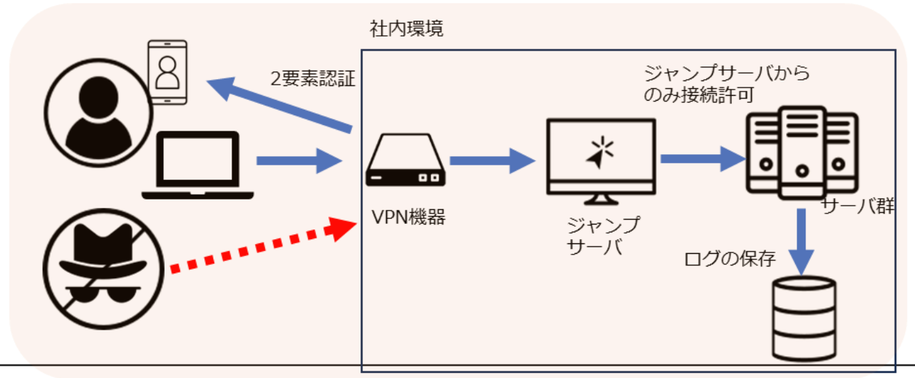
具体的な対策

【考え方】

- アクセス元の信頼性を重視し、すべてのアクセスを監視する。

【実施するべき技術的対策】

- VPN機器への接続に多要素認証を導入し、接続元の信頼性を上げる。
- 外部から中枢のサーバに対し、VPN経由での直接接続をさせない。
- サーバやPCの特権アカウントのパスワードを定期的に変更する。
- OSのファイアウォール機能を有効にし、接続元を限定する。
- サーバやネットワーク機器のログを取得し、定期的に確認する。
- 脆弱性情報を高い頻度で確認する。
- パッチマネジメントを実施する。
- EDRなどの製品を導入する。



重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【複雑さを持つパスワードの作り方】

1.単語ではなく、文章にする
単語の場合、ディクショナリ検索でヒットする確率が上がるため、
文章として考える

Cyber Security Keizoku Shien
↓
CyberSecurityKeizokuShien

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

2. 数字を入れる

CyberSecurityKeizokuShien**0723**

3.単語の母音を削除し、読めなくする（aiueo）

Cyb**e**rS**e**c**u**r**i**tyK**ei**z**o**k**u**Sh**ie**n0723

↓

CybrScrtyKzkShn0723

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

4. 特殊記号を数文字入れる
   #、%、@を単語の区切りに入れる

CybrScrtyKzkShn0723

↓

Cybr**#**Scrty**%**Kzk**@**Shn0723

ベースパスワード完成！

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

5. サービス識別文字を入れる

例

Amazon ： a6

FaceBook ： f8

a6Cybr#Scrty%Kzk@Shn0723

f6Cybr#Scrty%Kzk@Shn0723

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

6．自分にしかわからない固定文字を入れる

例　イニシャル

SH　→　$H

$Ha6Cybr#Scrty%Kzk@Shn0723

$Hf6Cybr#Scrty%Kzk@Shn0723

メモするときはベース部分のみをメモする

$Ha6**Cybr#Scrty%Kzk@Shn0723**

重大インシデント事例から学ぶ課題解決

認証方式と管理

- パスワードマネージャー（ソフトウェア）
  複雑なパスワードを生成し、管理するためのソフトウェア。
  端末間の同期を行うことで、複数のデバイスで共有できる。
- ワンタイムパスワード
  定期的に更新され、1度しか使用できないパスワード。
  パスワードは、専用のデバイスやソフトウェアで確認できる。
- PINコード方式
  パスワードとは異なり、デバイスに対する認証となるため、ネットワーク上を流れることがない。
- 公開鍵方式のパスキー
  公開鍵と秘密鍵の2種類の鍵のペアで認証を行う方式

3. サイバーセキュリティの基礎知識

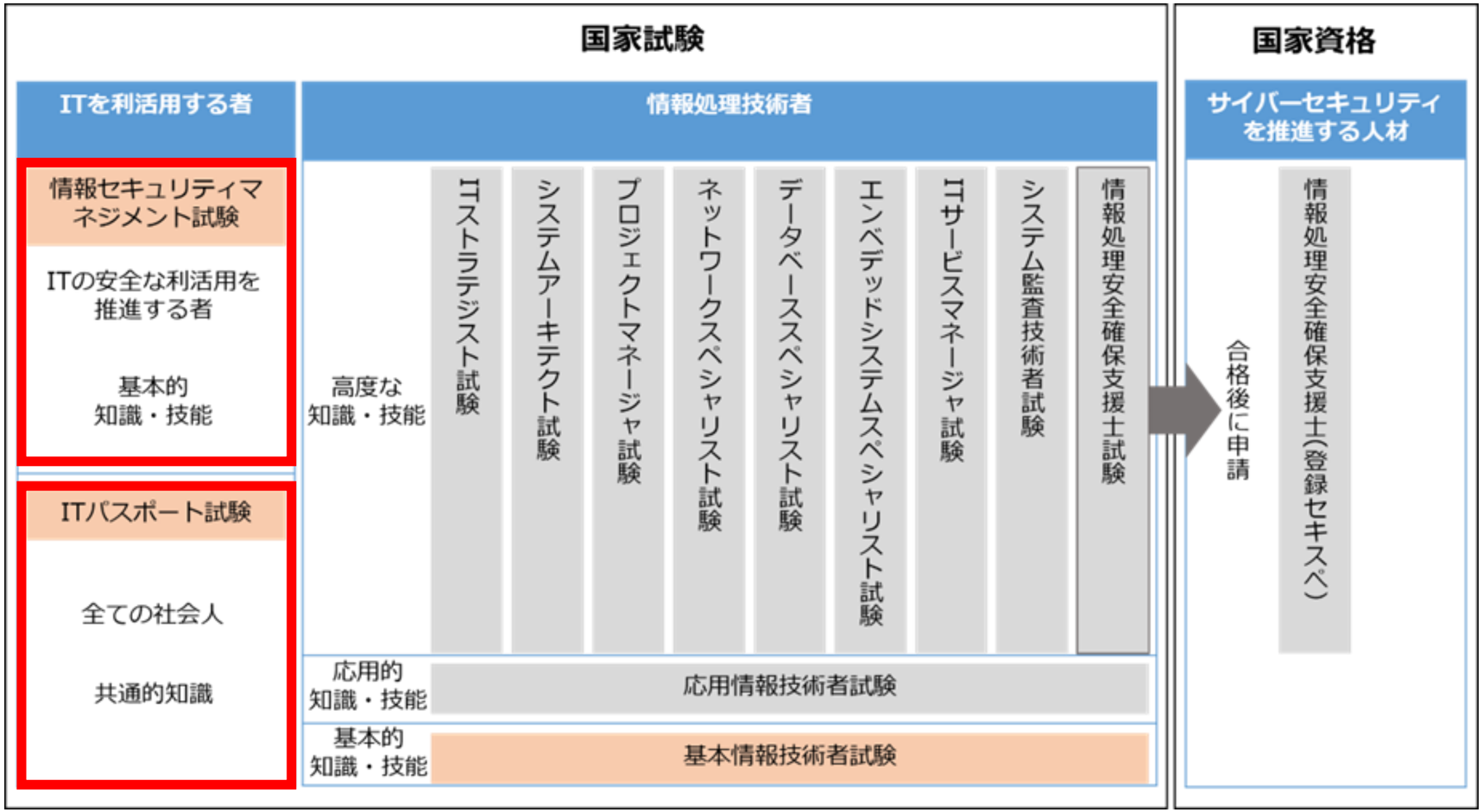
各種資格試験から得るサイバーセキュリティの基礎知識

Security Action（セキュリティ対策自己宣言）

サイバーセキュリティ対策基準レベル

各種資格試験から得るサイバーセキュリティの基礎知識 【参照：セミナーテキスト3-2-1.】

社員に取得させたい資格



IPA.”試験区分一覧”を基に作成. https://www.ipa.go.jp/shiken/kubun/list.html (参照 2023-07-06).

Security Action 宣言　二つ星レベル 【参照：セミナーテキスト3-3-1.】

レベルごとの宣言内容

レベル	宣言内容
★ 1つ星	次の情報セキュリティ5か条に取り組むことを宣言する 1. OSやソフトウェアは常に最新の状態にしよう！ 2. ウイルス対策ソフトウェアを導入しよう！ 3. パスワードを強化しよう！ 4. 共有設定を見直そう！ 5. 脅威や攻撃の手口を知ろう！
★★ 2つ星	• 5分でできる！情報セキュリティ自社診断で自社のセキュリティ対応状況を把握する • 情報セキュリティ方針を策定する （理念、指針、原則、目標等を表した「方針書」「宣言書」等を指す）

セキュリティ対策自己宣言

IPA. ”SECURITY ACTION セキュリティ対策自己宣言”. https://www.ipa.go.jp/security/security-action , (参照 2023-07-06).

サイバーセキュリティ対策基準レベル 【参照：セミナーテキスト3-4-1.】

対策基準レベルの概要

レベル	概要
Lv.1 クイック アプローチ	緊急に、狙われやすい大きな穴（セキュリティホール）を塞ぐ
Lv.2 ベースライン アプローチ	素早く多くの穴を塞ぐ
Lv.3 網羅的 アプローチ	じっくりと、小さな穴を残さないように確実に塞ぐ

サイバーセキュリティ対策基準レベル 【参照：セミナーテキスト3-4-1.】

Lv.1 クイックアプローチ

項目	説明
内容	様々なインシデント事案の対応内容を参考として、「リスクが大きい（発生頻度が高い、被害が大きい）」と思われる事例から、重要な対策を実施していく。 何から実施していいかわからない。という組織は、まずはここから。
参考資料	• 【IPA】情報セキュリティ10大脅威2023 • 【NISC】サイバー攻撃を受けた組織における対応事例集（事実例における学びと気づきに関する調査研究） など

サイバーセキュリティ対策基準レベル 【参照：セミナーテキスト3-4-1.】

Lv.2 ベースラインアプローチ

項目	説明
内容	セキュリティ対策の基準やガイドラインを定義することにより、組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指す。ただし、追加のセキュリティ対策やリスクに対する適切な対応策を検討し、網羅的なアプローチを推進することが必要となる。 • セキュリティの基準となるベースラインを定義し、組織全体で一貫性を確保 • 網羅的なアプローチの出発点
参考資料	• 【IPA】中小企業の情報セキュリティ対策ガイドライン第3版 • 情報セキュリティハンドブック（ひな形） • 中小企業のためのクラウドサービス安全利用の手引書 • 情報セキュリティ関連規程（サンプル）

サイバーセキュリティ対策基準レベル 【参照：セミナーテキスト3-4-1.】

Lv.3 網羅的アプローチ

項目	説明
内容	可能な限り多くの脅威や攻撃手法に対して対策を講じることを目指すアプローチとなる。ただし、全体的な実施には時間がかかるため、即時性を重視するアプローチではない。 • 可能な限り多くの脅威や攻撃手法に対して対策を講じる • 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持する
フレームワーク	ISMS CIS Controls など

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業