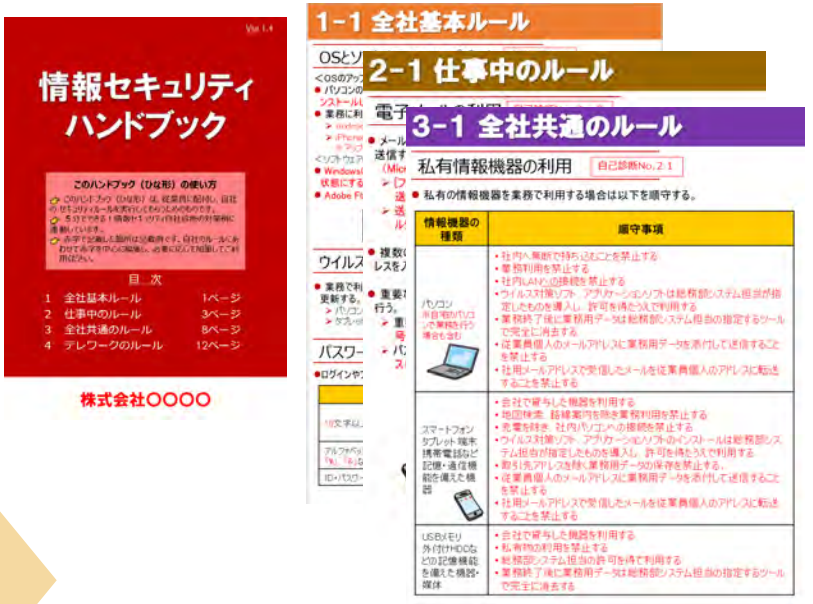
Step2 組織的な取り組みを開始する

(3) 対策の決定と周知

- 自社診断で問題があった項目は、解説編を参考に対策を決定
- 付録4「情報セキュリティハンドブック（ひな形）」を編集して社内周知

解説編を参考に、対策を決定



「情報セキュリティハンドブック」を編集
社内周知

Step3 本格的に取り組む

(1) 管理体制の構築

- 情報セキュリティ対策を推進するための管理体制を決定
- 付録5「情報セキュリティ関連規程」を活用して自社の管理体制を社内に周知

【表８】情報セキュリティ管理のための役割と責任分担(例)

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です。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、全責任を負います。
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です。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と権限を有します。
システム管理者	情報セキュリティ対策のためのシステム管理を行います。
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・実施します。
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点検します。

【表９】緊急時対応体制の役割と責任(例)

役職名	役割と責任
情報セキュリティ責任者 (例：代表取締役)	事故の影響を判断し、対応について意思決定する。
情報セキュリティ部門責任者 (例：管理部長、営業部長)	・事故の原因を調べて情報セキュリティ責任者に報告する。 ・情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行う。 ・事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行う。
システム管理者 (例：管理部長兼務)	事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行う。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告する。

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。

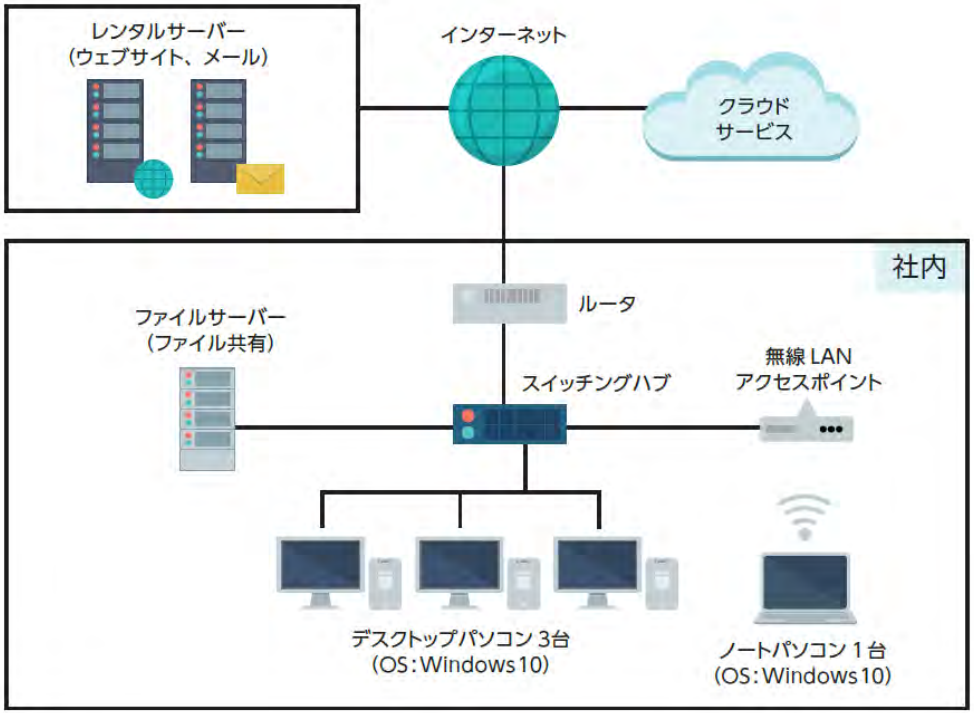
役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
情報システム管理者	情報セキュリティ対策のためのシステム管理を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者	事故の影響を判断し、対応について意思決定する。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。
特定個人情報事務取扱責任者	特定個人情報の情報セキュリティに関する責任者。
特定個人情報事務取扱担当者	特定個人情報を取り扱う事務に従事する従業員。
個人情報苦情対応責任者	個人情報に関する苦情の対応責任者。

<情報セキュリティ委員会体制図>

Step3 本格的に取り組む

(2) DXの推進と情報セキュリティの予算化

- 自社の情報システムについて、インターネットとの接続状況を把握
- 情報セキュリティ対策を検討して予算を確保



テレワークを導入するにあたり・・・

クラウドのセキュリティ確認
リモート接続のセキュリティ確保
利用者認証の強化

DX（Digital Transformation）

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。

Step3 本格的に取り組む

(3) 情報セキュリティ規程の作成

① 対応すべきリスクの特定

- 経営者が避けたい重大事故から、対応すべきリスクを特定
  - 外部状況：法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など
  - 内部状況：経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など

② 対策の決定

- リスクが大きなものを優先して対策を実施
  - いつ事故が起きてもおかしくない
  - 事故が起きると大きな被害になるなど

- リスクな小さなものは許容するなど、合理的に対応
  - 事故が起きる可能性が小さい
  - 発生しても被害が軽微であるなど

③ 規程の作成

- 付録5「情報セキュリティ関連規程（サンプル）」を参考に、自社に適した規程にするために修正を加える
  - サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成
  - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記

付録5

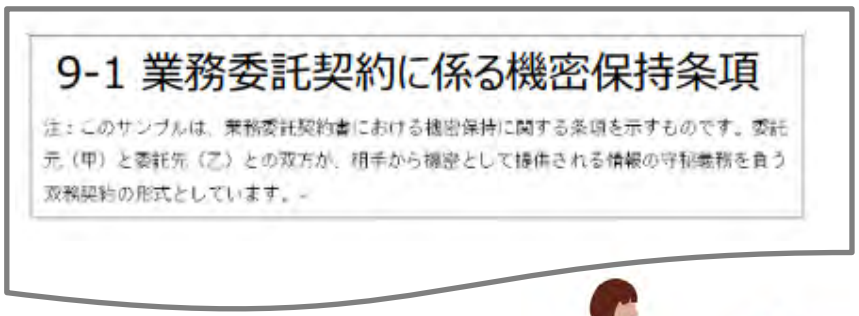
情報セキュリティ関連規程（サンプル）

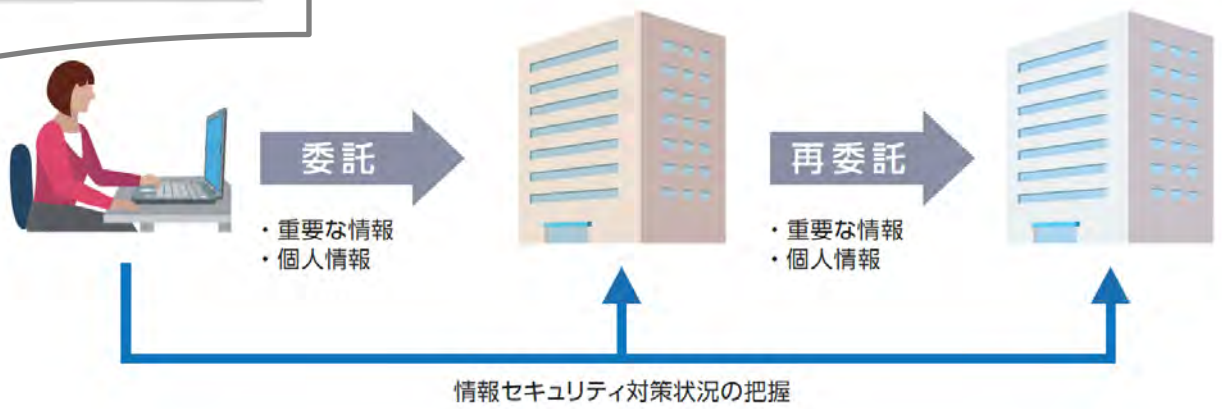
	名称	概要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制限方針や認証のルールを定めます。
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
6	IT機器利用	IT機器やソフトウェアの利用などのルールを定めます。
7	IT基盤運用管理	サーバーやネットワーク等のITインフラに関するルールを定めます。
8	システムの開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを決めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。
12	テレワークにおける対策	テレワークにおけるセキュリティに関するルールを定めます。

Step3 本格的に取り組む

(4) 委託時の対策

- 契約書や覚書に具体的な対策を明記
- 個別に契約や覚書を交わすことができる場合は、委託先のサービス規約や情報セキュリティ方針を確認
- 個人情報保護法では、個人データの取り扱いを委託する場合は、必要かつ適切な監督の実行

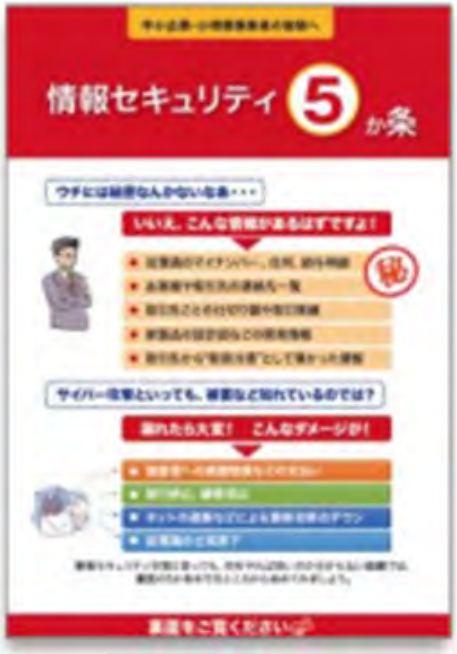




Step3 本格的に取り組む

(5) 点検と改善

- 情報セキュリティ対策が本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役に立っているか、等を確認
- 点検の基準例
  - その1)「情報セキュリティ5か条」「5分でできる！情報セキュリティ自社診断」
  - その2)情報セキュリティ対策に関するルール・規程



Step4 より強固にするための方策

- より強固な情報セキュリティ対策に取り組むために、以下の8つの区分について説明

（1）情報収集と共有
（2）ウェブサイトの情報セキュリティ
（3）クラウドサービスの情報セキュリティ
（4）テレワークの情報セキュリティ
（5）セキュリティインシデント対応
（6）セキュリティサービス例と活用
（7）技術的対策例と活用
（8）詳細リスク分析の実施方法

Step4 より強固にするための方策

(1) 情報収集と共有

- 情報セキュリティに関する情報収集の方法と情報共有の枠組みについて説明

① 情報収集の方法

- 定常的に情報収集ができる方法を検討し、体制を整備
- 情報セキュリティの専門機関、セキュリティベンダーなどのメールマガジンやソーシャルメディアに登録
- セミナーに参加して積極的な情報収集

② 情報共有の枠組み

- 収集した情報は社内の関係者だけではなく、取引先や同業者に対しても共有することで、対策の向上を図る
- 共有する情報に機密情報が含まれる可能性がある場合は、守秘義務契約を交わす
- 情報共有の枠組みとしては、日本シーサート協議会の他、業界別のISAC*が組織されている場合がある

* ISAC(Information Sharing and Analysis Center)同業界の事業者同士でサイバーセキュリティに関する情報の共有・分析などを行う組織

Step4 より強固にするための方策

(2) ウェブサイトの情報セキュリティ

- ウェブサイトを安全に構築し、運営するためのポイントを説明

ウェブサイト運営形態の検討

ウェブサイトでの運営形態によってセキュリティ対策が異なるため、**自社の状態に見合った運営形態**を検討しましょう。

ウェブサイトの構築

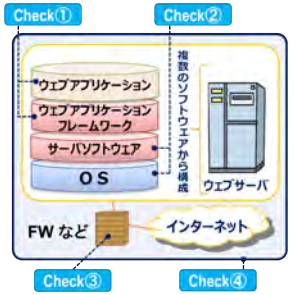
ウェブサイトの**技術的な脆弱性を認識**したうえで、必要なセキュリティ対策を設計・開発の段階から検討しましょう。

ウェブサイトの運営

運用開始後に発覚した情報セキュリティ上の問題にも適切に対応し、**ウェブサイトの安全性を維持向上**しましょう。

ウェブサイト開設等における運営形態の選定方法に関する手引き

安全なウェブサイトの作り方



安全なウェブサイトの運用管理に向けての20ヶ条

技術的な解説については手引き・ガイドラインを紹介

Step4 より強固にするための方策

(3) クラウドサービスの情報セキュリティ

- クラウドサービスを安全に利用するためのポイントを説明

クラウドサービスの選定

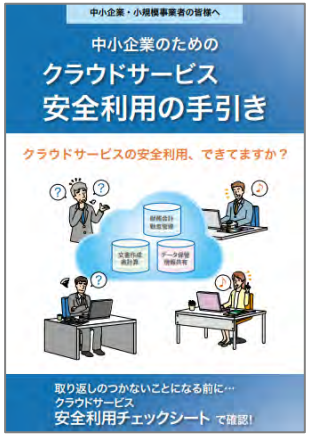
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、業務のセキュリティ要件に見合ったサービスを選定しましょう。

クラウドサービスの運用

クラウドサービスは提供者と利用者が連携して運用するため、その特性を理解して運用しましょう。

クラウドサービスのセキュリティ対策

クラウドサービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。



付録6「中小企業のためのクラウドサービス安全利用の手引き」にて ポイント(チェックリスト)の各項目について解説

付録6

中小企業のためのクラウドサービス安全利用の手引き

1	**どの業務で利用するか明確にする**	どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	**クラウドサービスの種類を選ぶ**	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	**取扱う情報の重要度を確認する**	クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？
4	**セキュリティのルールと矛盾しないようにする**	自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？
5	**クラウド事業者の信頼性を確認する**	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	**クラウドサービスの安全・信頼性を確認する**	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？
7	**管理担当者を決める**	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	**利用者の範囲を決める**	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
9	**利用者の認証を厳格に行う**	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
10	**バックアップに責任を持つ**	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？
11	**付帯するセキュリティ対策を確認する**	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	**利用者サポートの体制を確認する**	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	**利用終了時のデータを確保する**	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
14	**適用法令や契約条件を確認する**	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
15	**データ保存先の地理的所在地を確認する**	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

Step4 より強固にするための方策

(4) テレワークの情報セキュリティ

- テレワークを安全に実施するためのポイントを説明

テレワークの方針検討

テレワークを行う際のシステム構成や機器をどうするか方針を検討しましょう。

テレワークのセキュリティ対策

テレワークで利用するシステム構成や機器によって必要なセキュリティ対策を構築しましょう。

テレワークの運用

テレワークに関するルールを定め、テレワーク勤務者に周知し、事故に気をつけて安全に運用しましょう。

Step4 より強固にするための方策

(5) セキュリティインシデント対応

- セキュリティインシデント発生時の対応に関するポイントを説明

検知・初動対応

インシデントを検知した場合は、速やかに情報セキュリティ責任者へ連絡し、被害を拡大させないための初動対応を行いましょう。

報告・公表

顧客や関係者、行政機関、一般・メディア等に対して、必要な場合は適時の報告や情報公開を行いましょう。

復旧・再発防止

システム管理者や外部専門組織と協力して、迅速な復旧作業や根本的な再発防止策を検討しましょう。

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の手引き**」にて
対応方法の詳細や相談・報告先などを解説

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

- インシデント発生時の対応について、「検知・初動対応」「報告・公表」「復旧・再発防止」の3つの段階に分けて検討事項を説明
- インシデント対応時に整理しておくべき事項や相談窓口・報告先などを紹介

ステップ1
検知・初動対応

- 検知と連絡受付
- 対応体制の構築
- 初動対応

ステップ2
報告・公表

- 第一報
- 最終報・第二報以降

ステップ1
検知・初動対応

- 対応・調査
- 証拠保全
- 復旧
- 再発防止

Step4 より強固にするための方策

(6) セキュリティサービス例と活用

- 外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施することが可能
- セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用

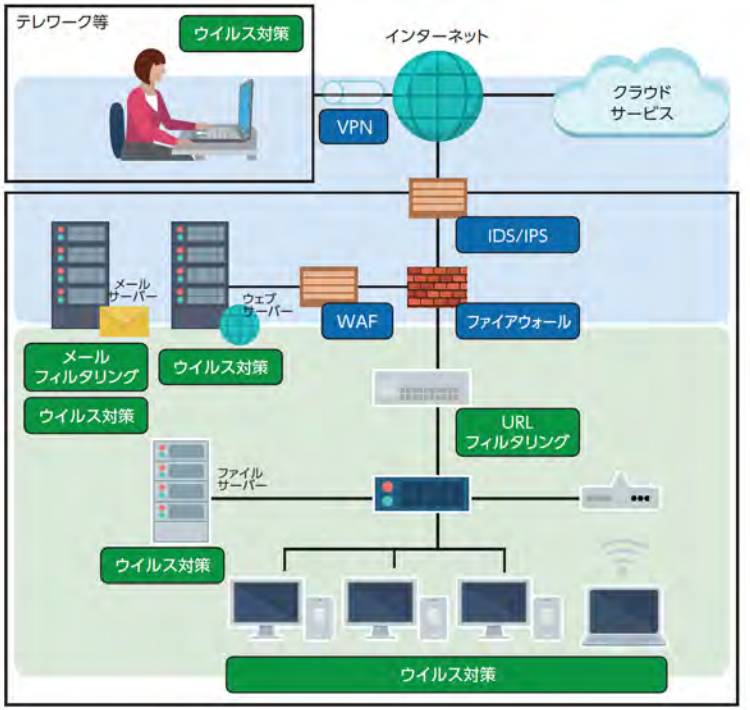
① 情報セキュリティコンサルテーション
② 情報セキュリティ教育サービス
③ 情報セキュリティ監査サービス
④ 脆弱性診断サービス
⑤ デジタルフォレンジックサービス
⑥ セキュリティ監視・運用サービス

Step4 より強固にするための方策

(7) 技術的対策例と活用

- コンピュータやインターネットを利用する際の技術的対策（製品やソフトウェア）を紹介

① ネットワーク脅威対策
② コンテンツセキュリティ対策
③ アクセス管理
④ システムセキュリティ管理
⑤ 暗号化
⑥ データの破棄



Step4 より強固にするための方策

(8) 詳細リスク分析の実施方法

- 付録7「リスク分析シート」を活用した詳細リスク分析の実施方法を説明

情報資産の洗い出し

どのような情報資産があるか洗い出して重要度を判断する

●情報資産管理台帳の作成
日常どのような電子データや書類を利用して業務を行っているかを考えて洗い出します。

●情報資産ごとの機密性・完全性・可用性の評価
機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなどを踏まえて、評価値を記入します。

●機密性・完全性・可用性の評価値から重要度を算定
重要度は、機密性、完全性、可用性いずれかの最大値で判断します。

リスク値の算定

先的・重点的に対策が必要な情報資産を把握する

情報セキュリティ対策の決定

リスクの大きな情報資産に対して必要とされる対策を決める

①リスクを低減する
自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げる
②リスクを保有する
事故が発生しても許容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持する。
③リスクを回避する
仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくす。
④リスクを移転する
自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げる。

サイバーセキュリティお助け隊
サービス制度

サイバーセキュリティお助け隊サービス制度

https://www.ipa.go.jp/security/otasuketai-pr/

中小企業に対するサイバー攻撃への対処として不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすものを「サイバーセキュリティお助け隊サービス」として登録・公表

➢ 「サイバーセキュリティお助け隊サービス基準」の主な内容

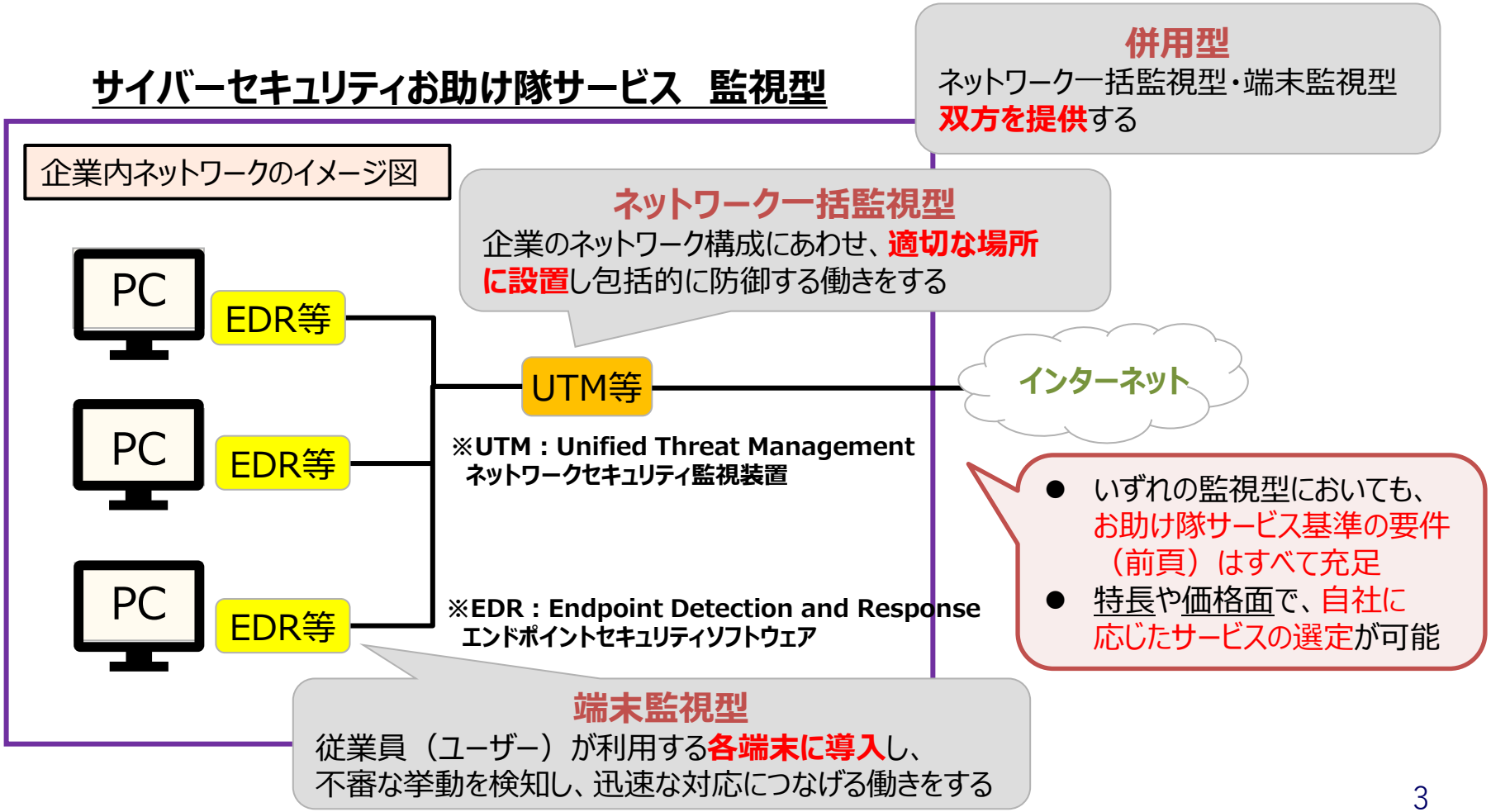
主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク及び／又は端末を**24時間見守る仕組み**を提供
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・運用できる簡単さ	**専門知識がなくても導入・運用できるような工夫**
簡易サイバー保険	突発的に発生する駆付け費用等を補償する**サイバー保険**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）** ・併用型：**これらの和に相当する価格を超えないこと** ※端末1台から契約可能であることが条件

相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

本サービスを採用することを通じて、取引先企業に対する**自社の信頼性のアピール**に

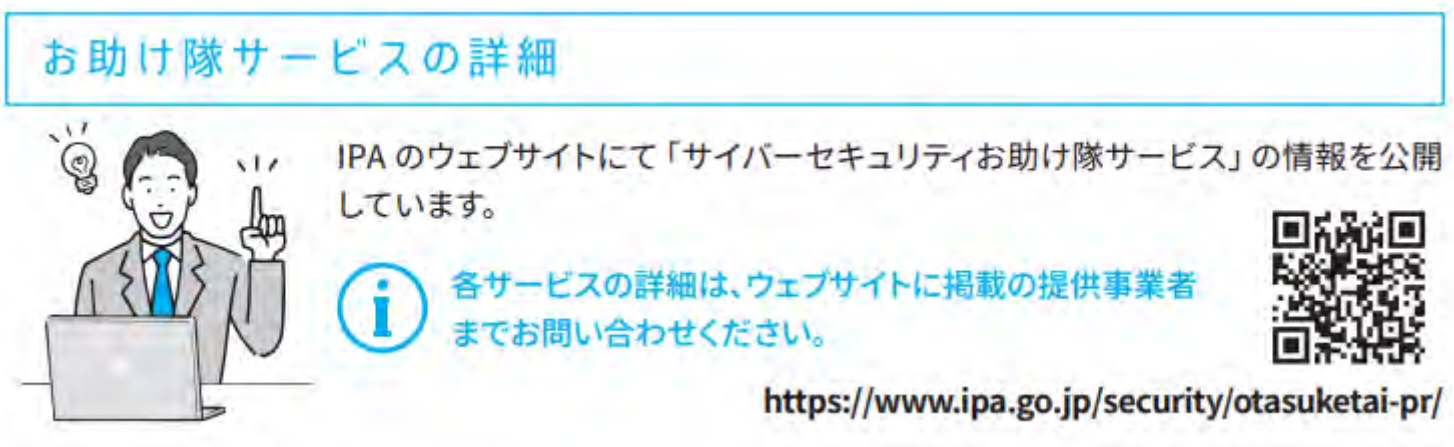
異常監視の仕組み

- サイバーセキュリティお助け隊サービスは、異常の監視の仕組み（監視型）ごとに大別して3類型あり、各サービスの特長を踏まえ選定・導入が可能

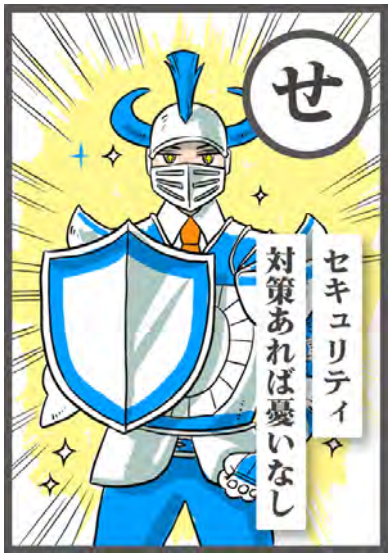


登録サービスリスト

- 2024年6月時点、40事業者 57のサービスが登録。今後も拡充予定。
- https://www.ipa.go.jp/security/otasuketai-pr/



導入のメリット①



ワンパッケージで簡単導入

(1)相談窓口
(2)異常の監視の仕組み
(3)緊急時の対応支援
(4)中小企業でも導入・運用できる簡単さ
(5)簡易サイバー保険

企業のセキュリティ対策に必要な(1)～(5)をまとめて導入できます。

- 専用の窓口で、ユーザーからの質問にお答えします
- ネットワークや端末を24時間見守り・監視しています
- インシデント発生などの緊急時には駆付け支援いたします
- 専門知識がなくても大丈夫！
- サイバー保険付きで安心

（＊サービスによって提供内容が異なります。詳しくは各サービス内容をご確認下さい。）

導入のメリット②

中小企業が導入・維持できる価格

端末1台からでもＯＫ！

ネットワーク一括監視型の場合、
サービスによって監視対象の端末数
が異なります

・ネットワーク一括監視型:月額1万円以下（税抜き）
・端末監視型:月額2,000円以下/台（税抜き）※
・併用型:これらの和に相当する価格を超えないこと

※端末1台から契約可能

価格設定に上限があり、サービス運用コストを抑えられます。

- コストを抑えたセキュリティ対策の導入が可能
- 各企業に適した監視型（ネットワーク一括監視型・端末監視型・併用型）を選択することで、効果的な運用ができます
- サービスの維持・管理が無理なくできます

（＊導入時に、別途初期費用が必要となる場合があります。詳しくは各サービス内容をご確認下さい。）
（＊「サイバーセキュリティお助け隊サービス」以外のオプション設定の場合は価格が異なります。）

導入のメリット③

サプライチェーンの中の
中小企業を狙った攻撃が
確認されています！

安心・信頼性をアピール

自社のセキュリティを高めるとともに、取引先や、グループ企業のセキュリティを守ることにもつながります

サプライチェーンにおけるセキュリティ対策にもなります。

- 取引先企業に対してアピール可能
- セキュリティ対策は、企業としての社会的信用を高めます
- 企業のBCPに貢献
- セキュリティ対策をすることで、企業の機密事項や顧客の個人情報を守ります