中小企業の情報セキュリティ対策ガイドライン 第3版

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- 独立行政法人 情報処理推進機構（IPA）
- 中小企業*1の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載
  - 情報セキュリティ対策の具体的な 進め方を分かりやすく説明
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録

*1： 中小企業の定義は、従業員数100人以下（サービス業、小売業、卸売業）、同300人以下（製造業などその他）

ガイドラインの構成

投影のみ

- 中小企業の情報セキュリティ対策の考え方や実践方法について、本編２部と付録より構成

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　5分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	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	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

第１部 経営者編

投影のみ

１ 情報セキュリティ対策を怠ることで企業が被る不利益

1. 金銭の損失
2. 顧客の喪失
3. 業務の停滞
4. 従業員への影響

２ 経営者が負う責任

1. 経営者などに問われる法的責任
2. 関係者や社会に対する責任

３ 経営者は何をやらなければならないのか

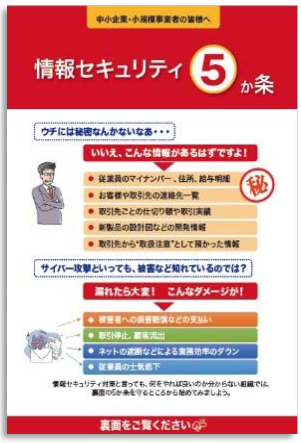
1. 認識すべき「３原則」
2. 実行すべき「重要７項目の取組」

第２部 実践編

投影のみ

- できるところから始めて段階的にステップアップ

Step1
できるところから始める



情報セキュリティ５か条

Step2
組織的な取り組みを開始する

５分でできる！
情報セキュリティ自社診断

Step3
本格的に取り組む

情報セキュリティ関連規程

Step4
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
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- **詳細リスク分析の実施方法**

より強固にするため方策

より強固にするための方策

(6) 詳細リスク分析の実施方法

- 付録6「リスク分析シート」を使い、以下の手順で行う。

手順1　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。

↓

手順2　リスク値の算定

リスクの大きさを算定し対策が必要な情報資産を把握する。

↓

手順３　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。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

(6) 詳細リスク分析の実施方法

手順１：情報資産の洗い出し

- 業種、事業内容、IT環境によって保有する情報資産は異なるため、台帳記入例を参考に、自組織の情報資産を一通り洗い出し、以下の要領で作業を進める。
  - 情報資産を情報資産管理台帳へ記入
  - 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・可用性の評価値から重要度を算定（「重要度」とは事故が起きた場合の影響）

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
						個人情報	要配慮個人情報	マイナンバー	機密性	完全性	可用性	重要度		
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			2	0	0	2		2016/7/1
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		2	2	1	2	5年	2016/7/1
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	2	2	1	2	7年	2016/7/1
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				1	1	1	1		2016/7/1
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			2	2	2	2		2016/7/1
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			2	2	2	2		2016/7/1
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			2	1	1	2		2016/7/1
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			2	1	1	2		2016/7/1

情報資産管理台帳 記入例

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

台帳記入例

投影のみ

業務分類	情報資産名称	情報資産（詳細）	備考（棚卸に関する課題等）	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
							個人情報	要配慮個人情報	マイナンバー	機密性	完全性	可用性	重要度	
入学試験	入試問題			入試委員会	入試委員会	学内サーバー				2	2	1	2	10
学籍関係	卒業証書台帳			教職員	教務部	書類	有			1	1	1	2	10
学籍関係	学籍記録	・退学届記録 ・異動記録 ・休学・退学・除籍届記録		教職員	学部事務局	学内サーバー	有	有		1	1	1	2	3
成績関係	成績資料	・評定一覧 ・卒業判定資料 ・成績素点表		教職員	学部事務局	学内サーバー	有			2	2	1	2	1
成績関係	成績資料	・評定一覧 ・卒業判定資料 ・成績素点表	・成績素点表は、教員の採点作業を考慮して、可搬媒体による持ち出しが可能となっているが、届け出等の制度が無い。	教職員	学部事務局	可搬電子媒体	有			2	2	1	2	1
成績関係	成績通知表			教職員及び当該学生	学部事務局	学内サーバー	有			1	2	1	2	1
成績関係	成績通知表			教職員及び当該学生	学部事務局	書類	有			1	2	1	2	1
学修系	学修記録	・学生の学修記録（レポート、作品） ・学修活動記録（動画・写真等）	・現時点では、学部別に学修記録が保存・活用されており、棚卸し自体が困難。	教職員及び当該学生	学部事務局	学内サーバー	有			1	1	1	2	1
学修系	カリキュラム表			学内	教務部	学内サーバー				0	1	1	1	5
大学広報	公式HP掲載情報			外部公開	広報部	学外サーバー				0	1	2	2	5
大学広報	行事計画			外部公開	広報部	学外サーバー				0	1	1	1	5

「リスク分析シート」の記入要領 ①

「利用方法」シートに記載されています。

投影のみ

台帳記入欄	記入内容解説
①業務分類	情報資産に関連する業務や部署名を記入します。情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。
②情報資産名称	情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは１行にまとめます。
③備考	必要に応じて説明等を記入します。
④利用者範囲	情報資産を利用してよい部署等を記入します。
⑤管理部署	情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。
⑥媒体・保存先	情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので2行に分けて記入します。 例）見積書「電子データを事務所PC に保存」「印刷物書類をキャビネットに保管」
⑦個人情報の種類	各項目が個人情報保護法、マイナンバー法で定義されています。
	〈個人情報〉 個人情報が含まれる場合は「有」を記入します。 ―個人情報の定義― 「 生存する個人に関する情報であって当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの、又は個人識別符号が含まれるもの」 氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、個人の身体、財産、職種、役職等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない。
	〈要配慮個人情報〉 要配慮個人情報が含まれる場合は「有」を記入します。 ―要配慮個人情報の定義― 「 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取り扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」
	〈マイナンバー〉 マイナンバー（個人番号）が含まれる場合（マイナンバー法で「特定個人情報」と定義されています。）は「有」を記入します。
⑧重要度	情報資産の機密性、完全性、可用性それぞれの評価値を記入します。 ３種類の評価値から表１１に基づき重要度が表示されます。なお、⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「２」となります。
⑨保存期限	法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。
⑩登録日	登録した日付を記入します。内容を更新した場合は更新日に修正します。

情報の洗い出しの手順

- 情報資産を情報資産管理台帳へ記入
  - パソコンのハードディスクや机の引き出しを見るのではなく、日常の業務とその流れの中で、どのような電子データや書類を利用しているかを考えて洗い出すと、作成しやすくなります。
- 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業務への影響や、法律で安全管理義務があるなど、表10の評価基準を参考に評価値２～０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、前項の作業で「情報資産管理台帳」の所定欄に記入した機密性・完全性・可用性のそれぞれの評価値の最大値として算定します。

なお、事故が起きると法的責任を問われたり、学生、保護者家庭などの個人に大きな影響があったり、業務に深刻な影響を及ぼすなど、法人の存続を左右しかねない場合や、個人情報を含む場合は、前項の算定結果に関わらず、重要度は２とします。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

【表10】情報資産の機密性・完全性・可用性に基づく重要度の定義（参考）

機密性			完全性			可用性		
アクセスを許可された者だけが情報にアクセスできる			情報や情報の処理方法が正確で完全である			許可された者が必要な時に情報資産にアクセスできる		
評価値	評価基準	該当する情報の例	評価値	評価基準	該当する情報の例	評価値	評価基準	該当する情報の例
2	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	• 個人情報（個人情報保護法で定義） • 特定個人情報（マイナンバーを含む個人情報）	2	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	• 個人情報（個人情報保護法で定義） • 特定個人情報（マイナンバーを含む個人情報）	2	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	• 顧客に提供しているEC サイト • 顧客に提供しているクラウドサービス
	守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある	• 取引先から秘密として提供された情報 • 取引先の製品・サービスに関わる非公開情報		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	• 取引先から処理を委託された会計情報 • 取引先の口座情報 • 顧客から製造を委託された設計図			
	自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため）漏えいすると自社に深刻な影響がある	• 自社の独自技術・ノウハウ • 取引先リスト • 特許出願前の発明情報						
1	漏えいすると業務に大きな影響がある	• 見積書、仕入価格など顧客（取引先）との商取引に関する情報	1	改ざんされると業務に大きな影響がある	• 自社の会計情報 • 受発注・決済・契約情報 • ホームページ掲載情報	1	利用できなくなると事業に大きな影響がある	• 製品の設計図 • 商品・サービスに関するコンテンツ（インターネット向け事業の場合）
0	漏えいしても業務にほとんど影響はない	• 自社製品カタログ • ホームページ掲載情報	0	改ざんされても事業にほとんど影響はない	• 廃版製品カタログデータ	0	利用できなくなっても事業にほとんど影響はない	• 廃版製品カタログ

表中の記述は一般企業の場合の例です。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

記入上のポイント

- 情報資産管理台帳は洗い出した情報資産を「見える化」するための方法の一つです。特にパソコンやネットワークで利用する電子化された情報は人間の五感で感知することができないため、社外のサーバーや個人のスマートフォンに保存されていると気付かないことがあります。電子化された情報を洗い出すときには「普段パソコンで見ているこのデータは、どこに保存されているのだろう。」というように、社内のIT 機器や利用しているクラウドサービスを思い浮かべて記入します。
- 重要度の判断は立場や見識によっても異なることがあるので、記入する前に「重要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。
- 電子データや書類を保存する際のまとめ方は様々ですが、管理方法や重要度が同じ情報は１件にまとめて記入することで作業負荷を減らすことができます。

【管理方法や重要度が同じ情報の例】

事務所内のパソコンで会計ソフトや表計算ソフトを使って帳簿を作成している場合

- 仕訳帳
- 総勘定元帳
- 現金出納帳
- 当座預金出納帳
- 小口現金出納帳
- 売上帳

情報資産名称：「会計データ」
「 会計データバックアップ」（バックアップを取っている場合）など

媒体・保存先：「事務所PC」（会計ソフトが保存先）
「 可搬電子媒体」（USB メモリがバックアップ保存先）

- 情報資産の「重要度」は時間経過とともに変化することがありますが、現時点の評価値を記入してください。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。
- 中規模企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

投影のみ

より強固にするための方策

(6) 詳細リスク分析の実施方法

- 付録6「リスク分析シート」を使い、以下の手順で行う。

手順1 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。

手順2 リスク値の算定

リスクの大きさを算定し対策が必要な情報資産を把握する。

手順３ 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。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

【参考】業務保証としての情報セキュリティ

業務は資源（資産）を使う

資産：人
性質：健康、知識、技能、意欲

資産：金
性質：貨幣価値、流動性、安定性

資産は固有の性質（価値）を持つ

業務
（例：製造、サービス、創造）

資産：物
性質：機能、堅牢性、代替性

資産：情報
性質：機密性、完全性、可用性

守るべきは業務

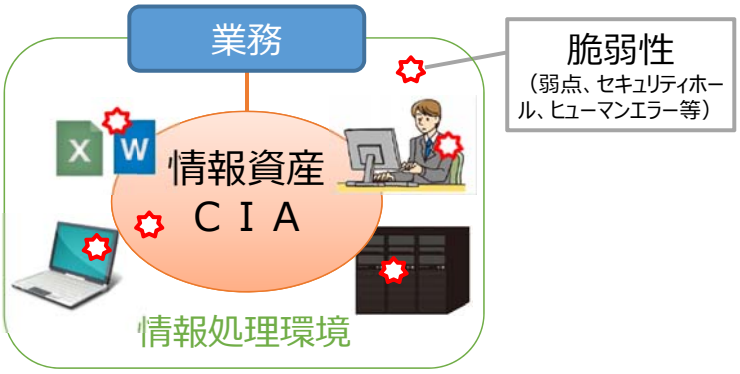
機密性（C）
完全性（I）
可用性（A）

情報資産のＣＩＡが損なわれると業務は回らなくなる。

情報セキュリティの定義

情報資産のＣＩＡを保つことにより、業務の遂行を保証（任務保証）すること。

【参考】情報セキュリティとリスク



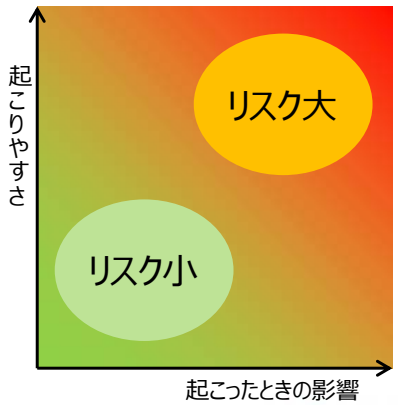
平常時

情報セキュリティ事故（インシデント）発生時

情報資産の脆弱性に脅威が作用すると、情報資産の価値（ＣＩＡ）が損なわれ、業務の遂行に支障をきたす。⇒ インシデント

インシデントは起きるかもしれないし、起きないかもしれない。⇒ リスク

リスクの大きさ　＝　起こったときの影響 × 起こりやすさ
＝（情報資産、脅威シナリオ）×（脅威、脆弱性）



(6) 詳細リスク分析の実施方法

手順２：リスク値の算定

- 手順１で洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定
  - 本ガイドラインでは「重要度」と「被害発生可能性（起こりやすさ）」の２つの数値の掛け算で行う。（**「重要度」とは事故が起きた場合の影響**）

リスク値 ＝ 重要度（影響） × 被害発生可能性
重要度 ＝ 手順1にて算定　　被害発生可能性 ＝ 脅威・脆弱性から算定

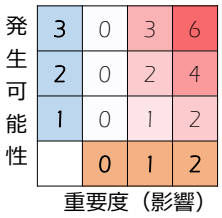
脅威の寄与	
3	通常の状況で脅威が発生する（いつ発生してもおかしくない）
2	特定の状況で脅威が発生する（年に数回程度）
1	通常の状況で脅威が発生することはない

脆弱性の寄与	
3	対策を実施していない（ほぼ無防備）
2	部分的に対策を実施している
1	必要な対策をすべて実施している

可能性 ＝ 脅威 ÷（4－脆弱性）
小数点以下を切り上げ

脅威＼脆弱性	3	2	1
3	3	2	1
2	2	1	1
1	1	1	1

被害発生可能性	
3	通常の状況で被害が発生する（いつ発生してもおかしくない）
2	特定の状況で被害が発生する（年に数回程度）
1	通常の状況で被害が発生することはない



リスク値		
リスク値	4～6 大	深刻な事故が起きる可能性大
	1～3 中	重大な事故が起きる可能性有
	0 小	事故が起きても被害は許容範囲

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

「リスク分析シート」の記入要領 ②

「利用方法」シートに記載されています。

投影のみ

1.　「脅威」の指定

「脅威の状況」シートに列挙されている代表的な脅威のそれぞれについて、自社において発生する可能性があるかどうか、以下の３種類の選択肢から最も近いものを１つ選択します。

選択肢	意味
1:通常では発生しない（数年に１回未満）	通常の業務を行っている範囲内では発生することが考えにくいものに相当します。これには、モバイル機器を使っていない場合のモバイル機器の脅威に関する項目のように、そもそも発生するはずがないものも含みます。
2:特定の状況で発生する（年に数回程度）	1と3のいずれにもあてはまらないと考える場合は2を選んでください。また、過去に起きたことがない事故でも、今後起きる可能性があると感じている場合は1でなく2を選択してください。
3:通常の状態で発生する（いつ発生してもおかしくない）	自社でこれまでに何度か発生したことがあり、今後も発生することが懸念されるものに相当します。

2.　「脆弱性」の指定

「対策状況チェック」シートに示されている11種類55項目の「情報セキュリティ診断項目」ごとに、自社における実施状況を「回答値」欄に表示される下記の選択肢１～４のいずれかを選択します。

選択肢	意味
1:実施している	情報セキュリティ診断項目に記載の通り、あるいはそれ以上の対策を実施している場合に相当します。
2:一部実施している	情報セキュリティ診断項目に記載されている項目の一部であったり、近い内容だがやや効果が不十分と考えられる対策を実施している場合に相当します。
3:実施していない/わからない	情報セキュリティ診断項目に記載されている対策を全く実施していない場合、あるいは対策として書かれている内容を実施しているかどうかわからない場合に相当します。
4:自社に該当しない	情報セキュリティ診断項目に記載されている状況が自社にあてはまらない場合に相当します。例えば、自社でサーバーを運用していない場合の、サーバーに関する項目などがこれにあたります。

3.　リスク値の算定

手順１と手順２の(1)(2)の記入が完了すると、「情報資産管理台帳」シートの右手の「現状から想定されるリスク」欄（オレンジ色の部分）に、情報資産ごとのリスク値に関する分析結果が表示されます。

「現状から想定されるリスク」欄の項目	各項目に表示される内容が意味するもの
脅威の発生頻度	「脅威の状況」シートにおける「対策を講じない場合の脅威の発生頻度」欄に記入した3段階の値のうち、「媒体・保存先」の種類に応じてもっとも大きい値を示しています。
脆弱性	「対策状況チェック」シートで設定した情報セキュリティ診断項目ごとの対策の実施状況をもとに、情報資産管理台帳における「媒体・保存先」の列で指定した内容を考慮した結果が表示されます。
被害発生可能性	脅威の発生頻度と脆弱性に表示されている内容をもとに、当該情報資産を対象とした被害が発生する可能性を高・中・低の３段階で表示します。
リスク値	情報資産の「重要度」と「被害発生可能性」の積をもとにリスクの大きさを大・中・小の３段階で表示します。

「リスク分析シート」でのグループワーク

投影のみ

オリジナルの資産管理台帳シート

カラム		ロジック	入力シート
M	重要度	機密性、完全性、可用性の最大値。但し、個人情報などを含んでいれば2。	（自動表示）
P	脅威	媒体や保存先毎に特定の脅威シナリオ（「脅威の状況」シートの「個別の脅威」列。紛失、攻撃など）を想定し、そのシナリオの発生頻度を見積もる。	脅威の状況
Q	脆弱性	媒体や保存先毎に特定の脅威シナリオ（「脅威の状況」シートの「個別の脅威」列。紛失、攻撃など）を想定し、その脅威に対して有効と考えられる対策の実施状況で評価。	対策状況チェック
R、S	被害発生可能性	可能性 ＝ 脅威 ÷（4－脆弱性） 小数点以下を切り上げ	（自動表示）
T、U	リスク値	リスク値 ＝ 重要度（影響） × 被害発生可能性 0→小、1～3→中、4～6→大	（自動表示）

講習会用の資産管理台帳シート

カラム		記入要領
Q	脅威シナリオ	想定する脅威シナリオを選択する。（選択肢は媒体・保存先によって異なります。）
R	脅威の可能性	想定した脅威シナリオが発生する頻度を3段階で見積もる。
S	脆弱性	想定した脅威シナリオの発生を抑止するための対策の実施状況によって3段階で見積もる。

TREND MICRO

投影のみ

より強固にするための方策

(6) 詳細リスク分析の実施方法

- 付録6「リスク分析シート」を使い、以下の手順で行う。

手順1 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。

手順2 リスク値の算定

リスクの大きさを算定し対策が必要な情報資産を把握する。

手順３ 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。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

TREND MICRO

(6) 詳細リスク分析の実施方法

手順３：情報セキュリティ対策を決定

- 手順２で算定したリスク値の大きいものから対策を検討し、自組織に適した対策を決定する。
- 対策は以下のように区分して検討する。
  1. 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無くす。
  2. リスクを低減する
     自組織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、または、事故が起きた場合の影響を下げる。
  3. リスクを移転する
     自組織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組織の負担を下げる。
  4. 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。
- 個々の対策（管理策）は、公開されているガイドラインやチェックリストなども参照して選択する。

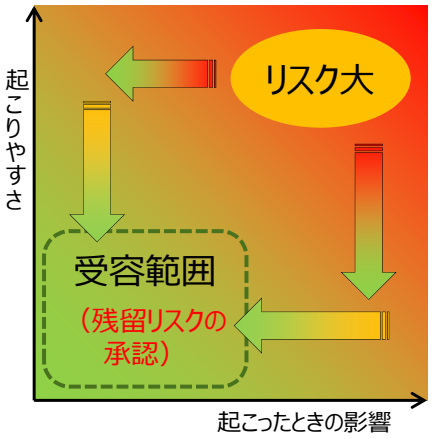
IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

【参考】情報セキュリティ対策の考え方

情報セキュリティ対策とは、リスクの大きさを減らすこと。

どこまで減らすのか ⇒ 組織の受容基準以下にする。

リスクの大きさ ＝ 起こったときの影響 × 起こりやすさ
＝ （情報資産、脅威シナリオ）×（脅威、脆弱性）



対策	考え方	対策例
回避	業務を見直すこと	その業務を止める。情報を持たない。
低減	起こりやすさを減らす	脆弱性を塞ぐ。セキュリティパッチ、アクセス制御、ネットワーク分離など。
	起こったときの影響を減らす	早期検知、暗号化、バックアップ、冗長化など。SOC/CSIRTの整備。情報資産のＣＩＡを強靭にする。
移転	インシデント発生時の損失を転嫁する	サイバーセキュリティ保険、アウトソース。
受容	リスクの大きさが小さいので容認できる。	敢えてそれ以上の対策はしない。（残留リスクは承認する。）

物理的、 論理（技術）的、 管理的

抑止的、予防的、検知的、是正的、回復/復旧的

【参考】その他のリスク分析手法

- ベースラインアプローチ
  - 既存の標準や基準を参照して対策を検討する方法。情報資産ごとに「資産価値」「脅威」「脆弱性」を識別しないので、簡単にできる方法であるが、参照する標準や基準によって、対策のレベルが高すぎたり、低すぎたりする場合がある。

    例）経済産業省、総務省、文部科学省などが公開している情報セキュリティ管理基準、ポリシーガイドラインの対策や、ISO/IEC 27002の管理策を実施する。

    例）IPAの「情報セキュリティ対策ベンチマーク」や、中小企業の情報セキュリティ対策ガイドライン 付録3：「5分でできる！情報セキュリティ自社診断」などを参考にする。
- 非形式的アプローチ
  - 組織や担当者の経験や判断によってリスク分析を行い、対策を検討する方法。短時間に実施することが可能であるが、属人的な判断に偏るおそれがある。

    例）システム管理担当者が情報セキュリティに詳しいITベンダーにアドバイスしてもらい対策を実施する。
- 詳細リスク分析
  - 情報資産ベース：情報資産ごとに「資産価値」「脅威」「脆弱性」を識別し、それらに対してリスク分析を行い、対策を検討する方法。個々の情報資産に適した対策が可能だが手間がかかる。

    例） P.43（6）詳細リスク分析の実施方法に従って対策を実施する。
  - 事業被害ベース：業務の流れと情報の取扱いを識別し、それらに対して事業被害を起こす脅威（攻撃やインシデント）に対してリスク分析を行い、対策を検討する方法。

    例）ランサムウェアの感染による被害を想定して、その予防や復旧のための対策を検討する。DDoS攻撃を緩和する対策を検討する。
- 組合せアプローチ
  - 複数の方法を併用し、それぞれの長所短所を補完する方法。相応の知見、経験を要するが、安全性、利便性、コストなどのバランスを取りやすい。

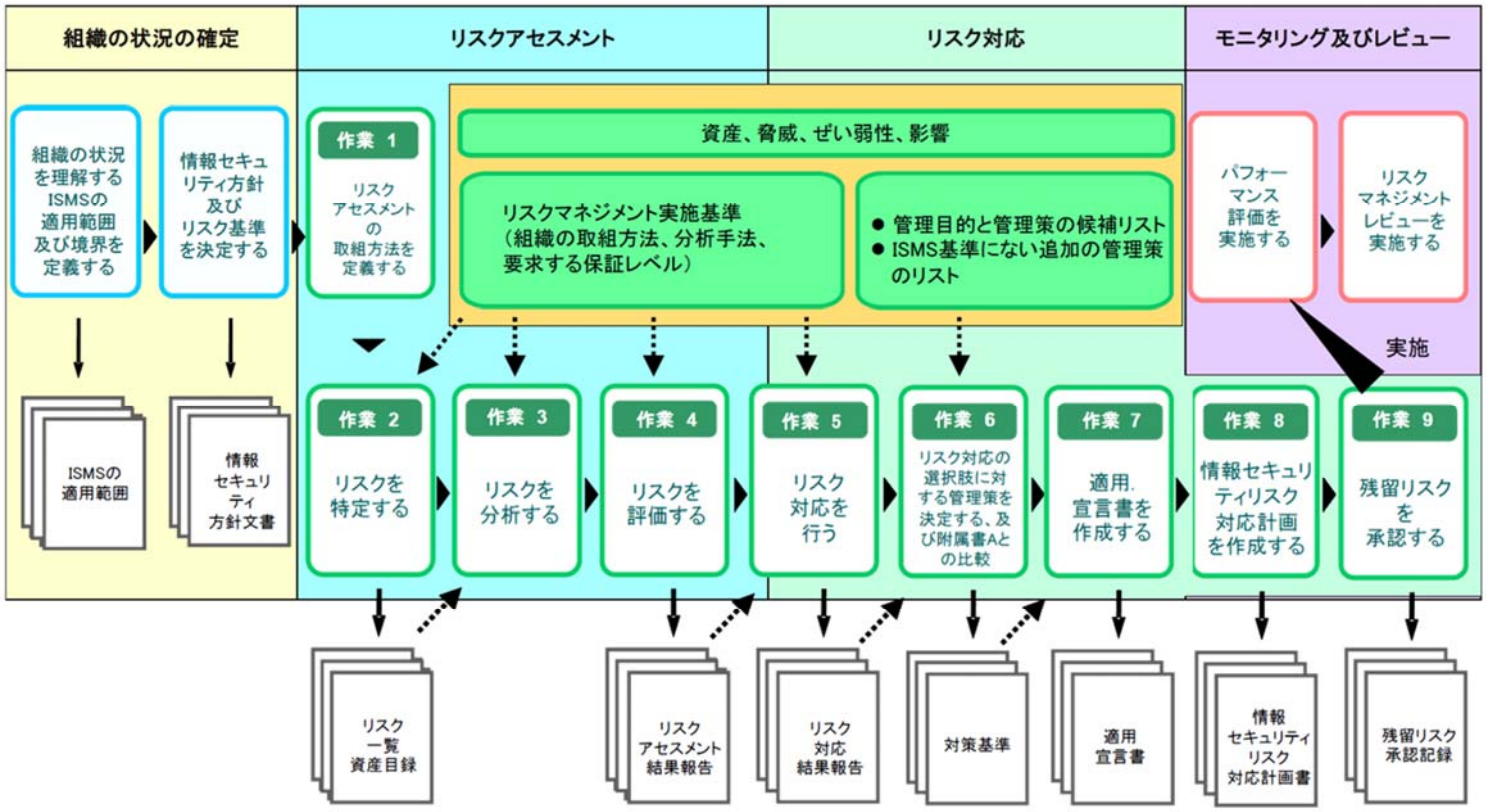
    例）基幹システムに関連する情報資産と個人情報を詳細リスク分析の対象として、その他は汎用的なチェックリストを参照してベースラインアプローチの対策を実施する。

    例）個人情報などの機密性に関するリスク分析は情報資産ベースで行い、業務の継続性、情報の可用性に関するリスク分析は事業被害ベースで行う。

IPA「中小企業の情報セキュリティ対策ガイドライン」を基に作成

【参考】リスクアセスメント及びリスク対応に関する作業

投影のみ



JIPDEC ISMSユーザーズガイド -JIS Q 27001:2014(ISO/IEC 27001:2013)対応- -リスクマネジメント編- より