

リスク分析シート

2024年7月

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

中小企業の情報セキュリティ対策ガイドライン第3.1版

- 中小企業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（第1部）
 - 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（第2部）
 - 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



ガイドラインの構成

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。
	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。
	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	情報漏えいやシステム停止などのインシデント対応のための手引きです。

第2部
5-(8)

詳細リスク分析の実施方法

- 本編第2部「実践編」にて詳細リスク分析の実施方法を3つのステップで説明
- 実施にあたっては付録7「**リスク分析シート**」を活用

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

リスク値の 算定

優先的・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

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（入力不要・自動表示）			
						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	脆弱性 ※「対策状況チェッ ク」シートに入力すると表示	被害発生 可能性	リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3		2023/4/1	3:通常の状態では脅威が発生する (いつ発生してもおかしくない)	2:部分的に対策を実施して いる	2 可能性： 中	6 リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3		2023/4/1	2:特定の状況で脅威が発生する (年に数回程度)	2:部分的に対策を実施して いる	1 可能性： 低	3 リスク小
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		3	3	2	3	5年	2023/4/1	2:特定の状況で脅威が発生する (年に数回程度)	2:部分的に対策を実施して いる	1 可能性： 低	3 リスク小
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	3	3	2	3	7年	2023/4/1	3:通常の状態では脅威が発生する (いつ発生してもおかしくない)	2:部分的に対策を実施して いる	2 可能性： 中	6 リスク大

付録7「リスク分析シート」

【参考】リスク分析の手法

① 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。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。

② 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。

③ 詳細リスク分析

情報資産ごとに「資産価値」「脅威」「脆弱性」を識別し、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。

④ 組み合わせアプローチ

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。よく用いられるのは、ベースラインアプローチと詳細リスク分析の組合せ。重要な情報資産に対する対策とその他の情報資産に対する対策とのバランスがとりやすい。

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1-1 情報資産管理台帳の作成

● 情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

● 情報資産管理台帳

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

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			保存期限	登録日
						個人情報	要配慮個人情報	特定個人情報		
			人事部 人事部	人事部 人事部	情報資産の媒体や保存場所を記入	有 有	個人情報の有無を記入			情報資産の登録日を記入
人事	健康診断の結果	雇入時・定	人事部	人事部			有			23/4/1
経理	給与システムデータ	税務 源泉徴収票	経理部	経理部	PC			有	情報資産の保存期間を記入	23/4/1

情報資産に関連する業務や部署名を記入

情報資産の内容を簡潔に記入

必要に応じて説明等を記入

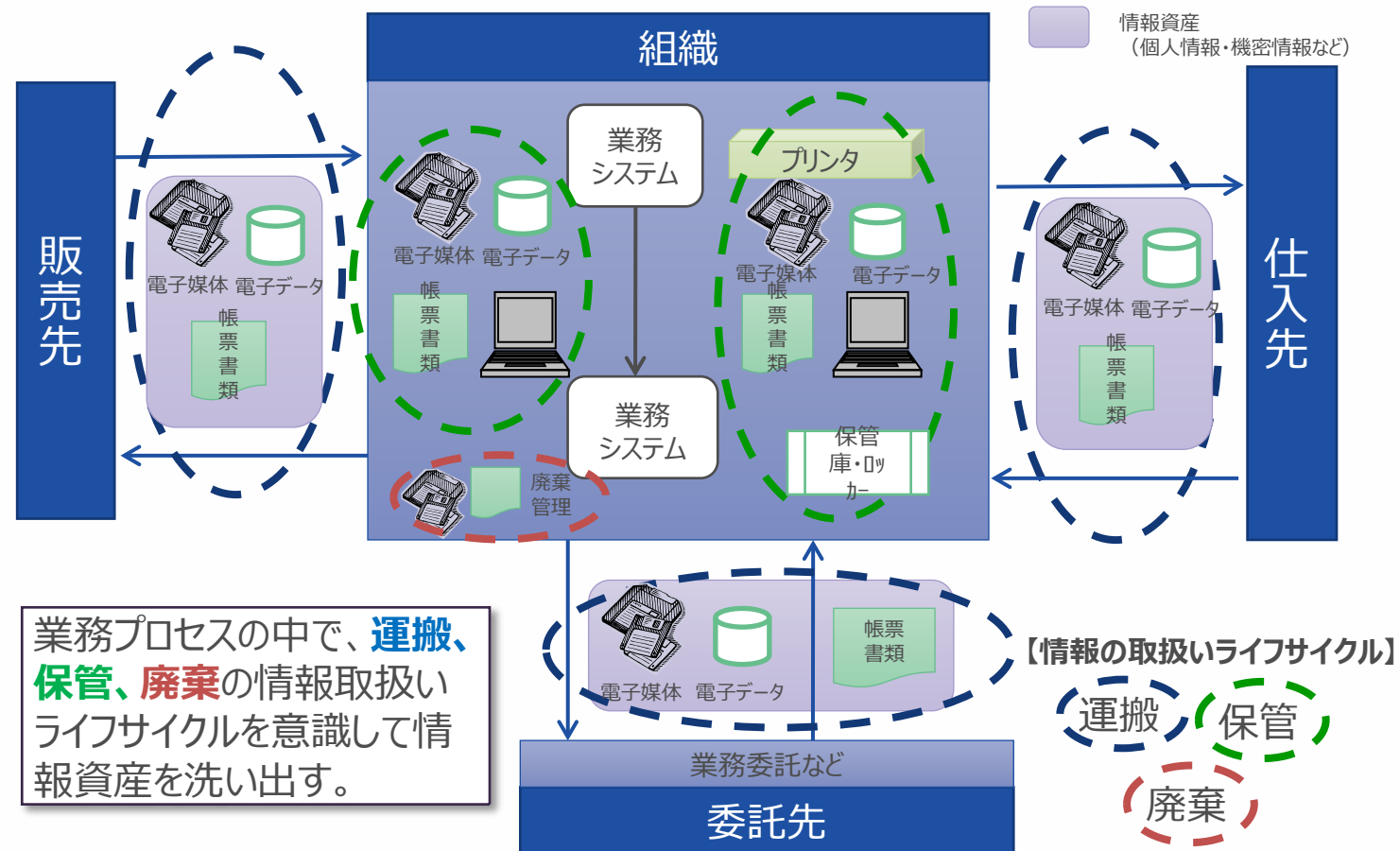
情報資産を利用してよい部署等を記入

情報資産の管理責任がある部署等を記入

- 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する
- 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する
- 電子データや書類を保存する際のまとめ方は様々だが、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担を減らすことができる
- 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るが、現時点の評価値を記入する。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、最大値で評価する
- 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

情報資産洗い出しのポイント

- 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すと、作成しやすくなる



手順1-2 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、次頁の評価基準を参考に評価値 3 ～ 1 を記入する

- ✓ **機密性 (Confidentiality)**

アクセスを許可された者だけが情報にアクセスできる

- ✓ **完全性 (Integrity)**

情報や情報の処理方法が正確で完全である

- ✓ **可用性 (Availability)**

許可された者が必要な時に情報資産にアクセスできる

手順1-2 機密性・完全性・可用性の評価

評価基準（機密性）

評価値	評価基準	該当する情報の例
3	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）
	守秘義務の対象や限定提供データ※1 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
	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
2	漏えいすると事業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	漏えいしても事業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

※1 限定提供データ

不正競争防止法で次のように定義されています。「第二条 7 この法律において「限定 提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理 されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

手順1-2 機密性・完全性・可用性の評価

評価基準（完全性）

評価値	評価基準	該当する情報の例
3	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）
	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
2	改ざんされると事業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	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

手順1-2 機密性・完全性・可用性の評価

評価基準（可用性）

評価値	評価基準	該当する情報の例
3	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
2	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）
1	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

手順1-3 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する

判断基準	重要度
機密性・完全性・可用性評価値のいずれかまたはすべてが「3」の情報資産	3
機密性・完全性・可用性評価値のうち最大値が「2」の情報資産	2
機密性・完全性・可用性評価値すべてが「1」の情報資産	1

● 重要度の判断例

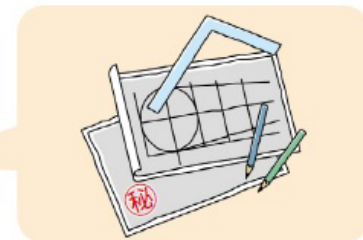
●『独自技術に基づいた設計図』(書類)

機密性: 主力製品の設計図であり、流出すると他社との差別化ができなくなり、売上が減少する 評価 = 3
完全性: 改ざんや無断の変更があると、製造に支障がある 評価 = 2
可用性: 原本のCADデータはサーバーに保存しており、必要なときに閲覧や再印刷が可能なので、利用できなくなっても困ることはない 評価 = 1

情報資産管理台帳 重要度欄

評価値			重要度
機密性	完全性	可用性	
3	2	1	3

機密性の3が最大値なので重要度は3



●『自社のホームページ』(電子データ)

機密性: 公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない 評価 = 1
完全性: 不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う 評価 = 3
可用性: サーバーの障害などでアクセスできなくなると、来店客が減少し、売上も減少する 評価 = 3

情報資産管理台帳 重要度欄

評価値			重要度
機密性	完全性	可用性	
1	3	3	3

完全性と可用性の3が最大値なので重要度は3



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

リスク値の算定について

- 対策の優先度を定めるため、情報資産ごとにリスク値(リスクの大きさ)を算定する
- リスク値は「重要度」「脅威」「脆弱性」の数値から算定する。重要度は【手順1】で算定しているので、ここでは脅威と脆弱性から被害発生可能性を算定する

$$\text{リスク値} = \text{重要度} \times \text{被害発生可能性}$$

手順1にて算定

脅威・脆弱性から算定

手順2-1「脅威」の識別

- 「脅威の状況」シートで、媒体・保存先ごとの脅威がどのくらいの頻度で発生する可能性があるかを「対策を講じない場合の脅威の発生頻度」欄に表示されるリストから1～3のいずれかを選択する

社内 サーバー	情報窃取目的の社内サーバーへのサイバー攻撃	3：通常の場合で脅威が発生する（いつ発生してもおかしくない）
	情報窃取目的の社内サーバーでの内部不正	2：特定の状況で脅威が発生する（年に数回程度）
	社内サーバーの故障による業務に必要な情報の喪失	1：通常の場合で脅威が発生することはない

媒体・保存先

個別の脅威

脅威の発生頻度（1～3から選択）

- 媒体・保存先
書類、可搬電子媒体、事務所PC、モバイル機器、社内サーバー、社外サーバー

手順2-2「脆弱性」の認識

- 「対策状況チェック」シートで、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「実施状況」欄に表示されるリストから1～4のいずれかを選択する

物理的セキュリティ対策	業務を行う場所に、第三者が許可なく立ち通りができないようにするための対策（物理的に区切る、見知らぬ人には声をかける、等）が講じられていますか？	2：一部実施している
	最終退出者は事務所を施錠し退出の記録（日時・退出者）を残すなどのように、事務所の施錠をしていますか？	1：実施している
	高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？	3：実施していない ／わからない
	秘密情報を保管および扱う場所への 個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？	4： 自社に該当しない

情報セキュリティ診断項目(チェック項目)

実施状況(1～3+4:自社に該当しない)

手順2-3 リスク値の算定

- 「脅威」の識別 と 「脆弱性」の認識 が完了すると、「現状から想定されるリスク」欄に、情報資産ごとに「脅威の発生頻度」「脆弱性」「被害発生可能性」「リスク値」が表示される

現状の状況から想定されるリスク（入力不要・自動表示）					
脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値	
3：通常で状況で脅威が発生する（いつ発生してもおかしくない）	2：部分的に対策を実施している	2	可能性：中	4	リスク大
2：特定の状況で脅威が発生する（年に数回程度）	2：部分的に対策を実施している	1	可能性：低	2	リスク中

情報資産ごとの脅威の発生頻度

情報資産ごとの脆弱性(対策状況)

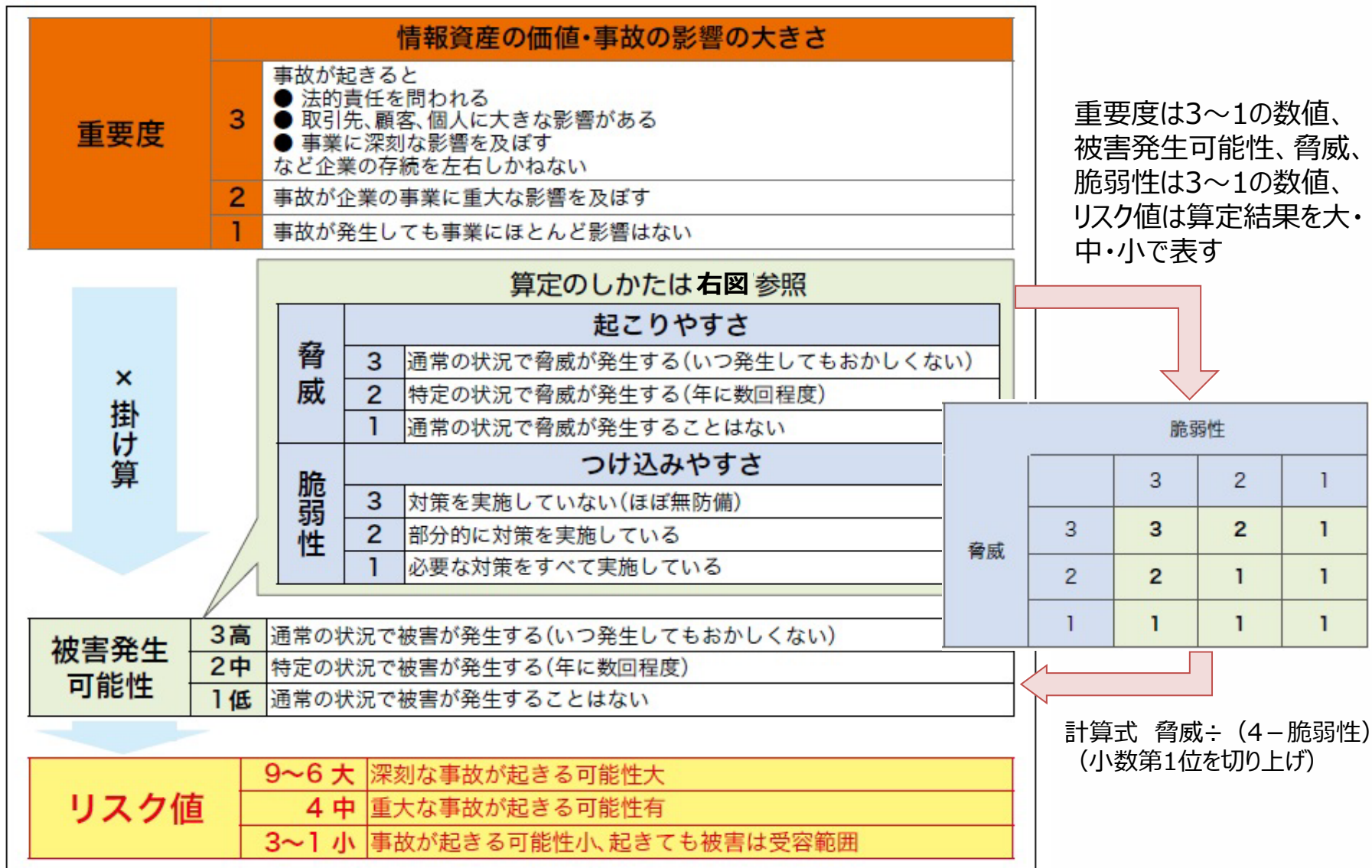
情報資産ごとの被害発生可能性(高・中・低の3段階)

情報資産ごとのリスク値(大・中・小の3段階)

【参考】「診断結果」シート

情報セキュリティ対策の種類 (付録5 情報セキュリティ関連規程名称)		情報セキュリティ関連 規程策定の必要性	対策状況チェック の診断結果 (対策の実施率)	対策検討・実施の可否
1	組織的対策	◎	50.0%	不足する対策を検討・実施してください
2	人的対策	◎	50.0%	不足する対策を検討・実施してください
3	情報資産管理	○	50.0%	不足する対策を検討・実施してください
4	アクセス制御及び認証	—	50.0%	(該当する情報資産なし)
5	物理的対策	◎	50.0%	不足する対策を検討・実施してください
6	IT機器利用	—	50.0%	(該当する情報資産なし)
7	IT基盤運用管理	—	50.0%	(該当する情報資産なし)
8	システム開発及び保守	△	50.0%	不足する対策を検討・実施してください
9	委託管理	△	50.0%	不足する対策を検討・実施してください
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	◎	50.0%	不足する対策を検討・実施してください

リスク値算定の全体イメージ



脅威例に応じたリスクのレベル（例）

脅威の例	重要度(a)	脅威	脆弱性	被害発生可能性(b)	重要度(a) × 被害発生可能性(b)	リスク値
1,000人を超える顧客の個人データを保存しているノートパソコンの盗難 (脆弱性) データを暗号化していない	3	2	3	2	6	リスク大
(対策改善) ハードディスクやデータを暗号化する	3	2	1	1	3	リスク小
クレジットカード番号を含む顧客の個人データを保持したECサイトへ不正アクセス されることによる情報漏えい (脆弱性) ウェブサイトの技術的脆弱性を認識せず対策が不十分	3	3	3	3	9	リスク大
(対策改善) ECサイトの設計・開発段階から脆弱性を作り込まないように技術 的セキュリティを実装する	3	3	1	1	3	リスク小
メールの添付ファイルを開いてしまいランサムウェアに感染し、サーバーのデータとオン ラインバックアップが暗号化される (脆弱性) オンラインバックアップしか取得していない	3	3	2	2	6	リスク大
(対策改善) 定期的にオフラインバックアップを取得する	3	3	1	1	3	リスク小

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

リスク対応方法の検討

- リスク値の算定により、優先的・重点的に対策が必要な情報資産に対して、リスクが事業に与える影響を考慮した上で、**リスクの対応方法**を検討し、**情報セキュリティ対策**を決定する

リスク 対応方法	内容	対応例
①低減する	脆弱性に対して情報セキュリティ対策を講じることにより、 脅威の発生可能性を下げる	マルウェア対策ソフトを導入する、外部記憶媒体の接続を制限する等
②保有する	リスクが事業に与える影響小さい、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、 対策を講じず許容範囲内として現状を維持 する。	（対策を講じた後に残ったリスク、および対策されずに残ったリスクは、 残留リスク とも言われる）
③回避する	脅威発生の要因を停止あるいは全く別の方法に変更することで、 リスクが発生する可能性を取り去る 。	外部からの不正アクセスという脅威に対し、機密情報が保存されているサーバは外部接続を行わないこと等
④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 。	社内サーバをセキュリティ対策の充実した外部クラウドサービスに移行する、情報セキュリティに関連した保険商品に加入する等

【参考】情報セキュリティ関連規程（サンプル）

対策検討にあたっては中小企業の情報セキュリティ対策ガイドライン付録「情報セキュリティ関連規程(サンプル)」をベースラインとして組み合わせて活用することができる

	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御方針や認証のルールを定めます。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域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。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 及び事業継続管理	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定めます。
11	テレワークにおける対策	テレワークのセキュリティ対策についてルールを定めます。

IPA