2　情報セキュリティ対策の基礎

2-1　情報セキュリティの３要素

情報セキュリティとは、企業の情報システムを取り巻くさまざまな脅威から、情報資産を機密性・完全性・可用性（3 要素）の確保を行いつつ、正常に維持することです。

機密性の確保

- **情報資産を正当な権利を持った人だけが使用できる状態にしておくこと**

  情報漏えい防止、アクセス権の設定、暗号の利用などの対策

完全性の確保

- **情報資産が正当な権利を持たない人により変更されていないことを確実にしておくこと**

  改ざん防止、検出などの対策

可用性の確保

- **情報資産を必要なときに使用できること**

  電源対策、システムの二重化、バックアップ、災害復旧計画などの対策

指導者向け参考情報

用語解説

CIA
情報セキュリティの３要素は、「機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）」の英語の頭文字より、CIA とも呼ばれています。

指導ポイント

２-１の説明にある通り、情報にはさまざまな特性があります。CIA 全てを同等の観点で見て情報の管理を強化するのではなく、情報の特性に応じて機密性を強くしたり、機密性は弱くても、完全性や可用性を強化して管理する必要があります。また、CIA の特徴として、完全性が必要な場合、可用性も必要になることが多いといえます。

2-2　情報のライフサイクル管理

情報のライフサイクル

企業にとって第４の経営資源である情報には、人の一生と同じようにライフサイクルがあります。

生成：新規作成　複写による作成　他からの取得
利用：編集　加工　参照　複製　伝達　移送
保存：格納　バックアップ　アーカイブ
廃棄：廃棄　消去

情報のライフサイクル管理

これらの過程を通じて、情報セキュリティの３要素が確保されるよう、管理しなければなりません。

例えば、

- **生成時：情報がその目的のために必要かつ十分で正しい内容を持つものとして作成すること**
- **利用時：必要な人のみがアクセスでき、許される範囲だけの処理（閲覧、編集、複製、移送等）がされること**
- **保存時：改変や改ざん、消失・紛失、不正な持ち出しが起こらないように安全な場所、方法で保存すること**
- **廃棄時：第三者に拾われたり盗み見られたりすることがないよう、確実に消し去ること**

などが大切です。

指導者向け参考情報

指導ポイント

文書の格付けとライフサイクル管理ルールの制定・運用
生成時に、その文書のセキュリティ／重要度格付けを作成者が行い、上司が承認する習慣を身につけましょう。

- 利用時には、格付けに基づいて処理・格納をする。
- 保存のレベルや暗号化も格付けに基づいて実施する。
- 廃棄も格付けごと、媒体の種類ごとに指定された方法で実施する。

2-3 情報セキュリティリスク

情報セキュリティリスクとは、情報セキュリティを損ねる要因です。

情報セキュリティにとっての脅威

- **システムが想定した通りに機能しない可能性**
- **悪意ある外部者または偶発的な要素による妨害・加害行為**
- **内部者の故意、ミス、不作為による事故**

リスクを顕在化させるぜい弱性

- **システム内部にある隠れた欠陥、いわゆるバグ、不具合**
- **ネットワーク境界の適切な防御の欠如、不備、不足**
- **組織運営上のルール、従業員のリテラシーやモラルに関わる不備、不足、欠陥、管理不足、実践不足**

ここに示した脅威がぜい弱性と結びついたとき、情報セキュリティのインシデント（でき事、事故）となって顕在化します。インシデントは、脅威とぜい弱性の組み合わせにより、いくつかの類型に分けられます。

また個々のインシデントは、その発生確率と発生したときの影響の度合いにより、その深刻度（インパクト）が違ってきます。

典型的なインシデント

- **マルウェア感染やネットワークからの不正侵入によるシステムの停止、データの破損、情報の窃取**
- **人的な不注意やミス、もしくは故意による情報の紛失、漏えい、持ち出し、悪用**
- **銀行口座の情報、技術情報などの重要情報が第三者に悪用されることによる、金銭的被害や技術競争力の喪失**
- **これら事故の二次被害として、風評被害、損害賠償負担、信用の失墜、機会損失等**

このようなインシデントの発生を未然防止するために、情報セキュリティ対策を導入し、万全を期さなくてはなりません。

指導者向け参考情報

重要！

＜リスクとその管理に関する用語と意味＞

1 リスクマネジメント（JIS Q 0073:2010 および JIS Q31000:2010 より）
リスクマネジメント：「リスクについて、組織を指揮統制するための調整された活動」
リスクマネジメントプロセスは「コミュニケーション及び協議」「組織の状況の確定」「リスクアセスメント」「リスク対応」「モニタリング及びレビュー」で構成

2 リスク：「目的に対する不確実さの影響」（JIS Q 0073:2010）
・事象や結果の目標達成への影響
・事象の結果または周辺環境変化の結果と、その起こりやすさの組み合わせ
・不確実性とは、イベントやその結果や結果の見込みに関する情報・知識の欠如

3 情報セキュリティリスク： 「脅威が資産または資産グループのぜい弱性を利用し、その結果、組織に害を及ぼす可能性」（ISO/IEC 27000:2009）
［解釈］ リスクは、情報資産の機密性・完全性・可用性・適法性を損なうことで情報の露呈、漏えい、改ざん、損壊、滅失、利用停止等を招き結果的に自社および利害関係者に損失をもたらす脅威とぜい弱性として認識されます。

4 リスクアセスメント（JIS Q 0073:2010 および JIS Q31000:2010 より）
リスクアセスメント＝リスクの評価は、リスクを洗い出す（特定する）、リスクを分析する、リスクを評価する、プロセスが含まれます。（詳細は 2-4 参照）

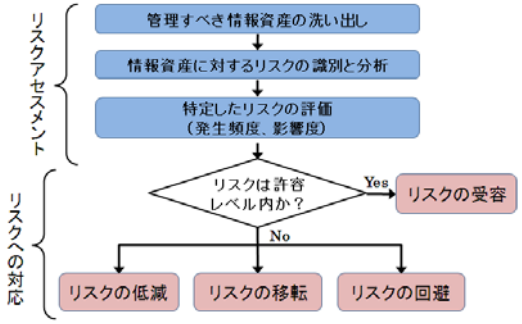
5 リスク対応の検討
リスクアセスメントに基づき、リスクに対してどのように対応するかを検討します。
（詳細は 2-4 参照）

2-4　リスクアセスメントとリスク対応

現実に自社が持つ情報資産（経営情報や預かり情報と、それを扱うITシステムや、紙を含む記録媒体）について、どのようなリスクが存在するのか、調査して洗い出し、そのインパクトを評価して、対応を決める必要があります。この一連の作業をリスクアセスメントといいます。

リスクアセスメント

リスクアセスメントと、それに基づく対応の流れは以下のようになります。

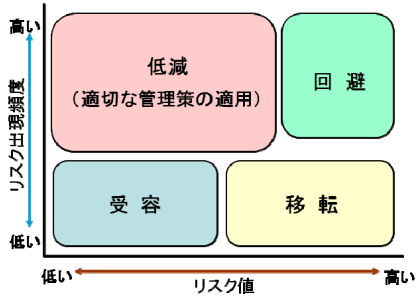


リスクアセスメントの代表的方法として以下のものがあります。

- ギャップ分析によるリスクアセスメント（ベースラインアプローチ）
- 討議によるリスクアセスメント（非形式アプローチ）

リスクへの対応

リスク評価に基づき、リスクへの対応を行います。以下の図の考え方に基づき、経営リスク管理の一環として判断・選択します。リスクごとに自社にとって最適の対応を選びます。



指導者向け参考情報

重要！

＜リスクとその管理に関する用語と意味＞（2-3から続く）

4 リスクアセスメント（JIS Q 0073:2010 および JIS Q31000:2010 より）
リスクアセスメントには「リスク特定」「リスク分析」「リスク評価」を含みます。

4．1 リスクの洗い出し＝リスクの特定・分析
リスクを洗い出す際には、業務プロセス上の情報の取り扱い、IT管理、物理的管理、人／組織管理に着目します。以下に代表的な検討事項を挙げます。

a. 業務プロセス上の情報の取り扱いに関連するリスク
　・情報のライフサイクルに関連するリスク
b. IT管理に関連するリスク
　・社内外からのITシステムへのアクセスに関するリスク
　・ウイルスなど技術的ぜい弱性に関するリスク
　・開発・変更・受け入れのプロセスや管理手続きに関するリスク
c. 物理的管理に関連するリスク
　・区画の境界の安全仕様・実装に関するリスク
　・区画への人の出入りとその管理に関するリスク
　・区画内の行動に関するリスク
d. 人/組織管理に関連するリスク
　・規則に関するリスク
　・人の意識・知識に関するリスク
　・人/組織の役割に関するリスク

4．2 リスクがもたらす影響＝リスクの分析・評価
洗い出したリスクがもたらすであろう結果とその影響を予測します。
　・誰に対し影響があるか
　・どのような影響を及ぼすか（経済的損失、精神的苦痛、信用失墜等）
　・リスクの大きさ（強度）：顕在化したときの影響の大きさ×発生確率

5 リスク対応の検討
リスク対応を考える際には、以下の観点に着目します。また、『中小企業が知っておくべき情報セキュリティ対策』（本書）を参考にすることもできます。
・リスクの原因究明
　・技術的観点、マネジメント的観点で分析する
・リスク対応の選択肢
　・低減、移転、回避、受容
・リスク低減のための手段＝情報セキュリティ対策
　・予防、防御、抑止、検知

用語解説

ギャップ分析によるリスクアセスメント（ベースラインアプローチ）
あらかじめ用意された情報セキュリティ基準に照らし、現時点での自社における情報セキュリティ対策の実施レベルをはかり、基準を満たさない箇所の情報セキュリティ対策を強化し、組織全体の情報セキュリティレベルを一定水準にします。

討議によるリスクアセスメント（非形式アプローチ）
社員が集まり、その討議によって日常業務におけるリスクを洗い出し、洗い出したリスクについての対応案を検討します。