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

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。

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**

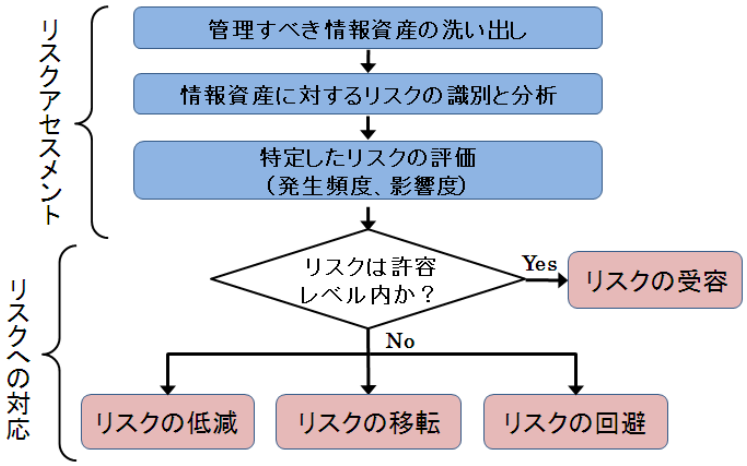
このようなインシデントの発生を未然防止するために、情報セキュリティ対策を導入し、万全を期さなくてはなりません。

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。