
情報セキュリティ対策について

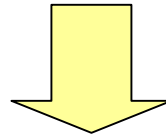
株式会社 アイライト
内藤 響

目次

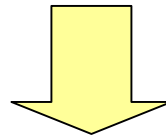
- 情報セキュリティをめぐる現状
- 情報セキュリティの主な流れ
- 情報セキュリティを複雑にしている要因
- 情報セキュリティの概要
- 情報セキュリティ対策で必要な知識
- リスクアセスメント
- 情報セキュリティ対策
- 情報セキュリティ規程の構成
- 必ず必要な情報セキュリティ対策
- 情報セキュリティ対策支援

情報セキュリティをめぐる現状

95年以降、急速に企業でのパソコン利用が進展したが、その利用は社員個人の道徳心や価値観に依存していた。



しかし、最近になり、パソコンやインターネットなどの情報システムに関するいろいろな問題がクローズアップされるようになった。



いろいろな問題を解決するために、情報の管理が必要であるという認識が徐々に生まれつつあるが、管理のもとになる規則をどのようにつくっていけばよいのかという疑問が生じている。

情報セキュリティの主な流れ

海外の動き

1995年 BS 7799
「情報セキュリティマネジメントのための実践的なガイドライン」
英国規格協会 (BSI)

1998年 BS 7799-1 :1999
「情報セキュリティマネジメントの実施のための規範」;ベストプラクティスが記載
BS7799-2:1999
「情報セキュリティマネジメントシステム—仕様及び利用の手引き」;組織の情報セキュリティに関するマネジメントシステムの適合性を評価するための要求事項

2002年 BS 7799-2 :2002
体系的リスクアセスメントの定義と継続的な実施の必要性
経営陣の責務の明確化
QMS、EMSとの整合性に配慮

日本の動き

2001年 ISMS 認証基準 Ver0.8
パイロット事業としてスタート

2002年 ISMS 認証基準 Ver1.0
正式に認証事業がスタート

2003年 ISMS 認証基準 Ver2.0
BS7799-2の2002年の改訂を受けてリリース

英国規格協会(BSI)は、品質マネジメントシステム、情報セキュリティマネジメントシステムをはじめとして、各種の標準規格の中心として世界を牽引している。

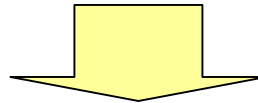
情報セキュリティを複雑にしている要因

情報資産とは何か

情報: データの形で格納されている情報
ドキュメント: 紙媒体に保管されているもの
施設機器: ハード、ネットワーク機器など
ソフトウェア: アプリケーション
要員: 業務を行ううえで必要なスタッフ
サービス: 業務を行ううえで必要なサービス
媒体: 電子媒体
その他: その他の業務に必要な資産

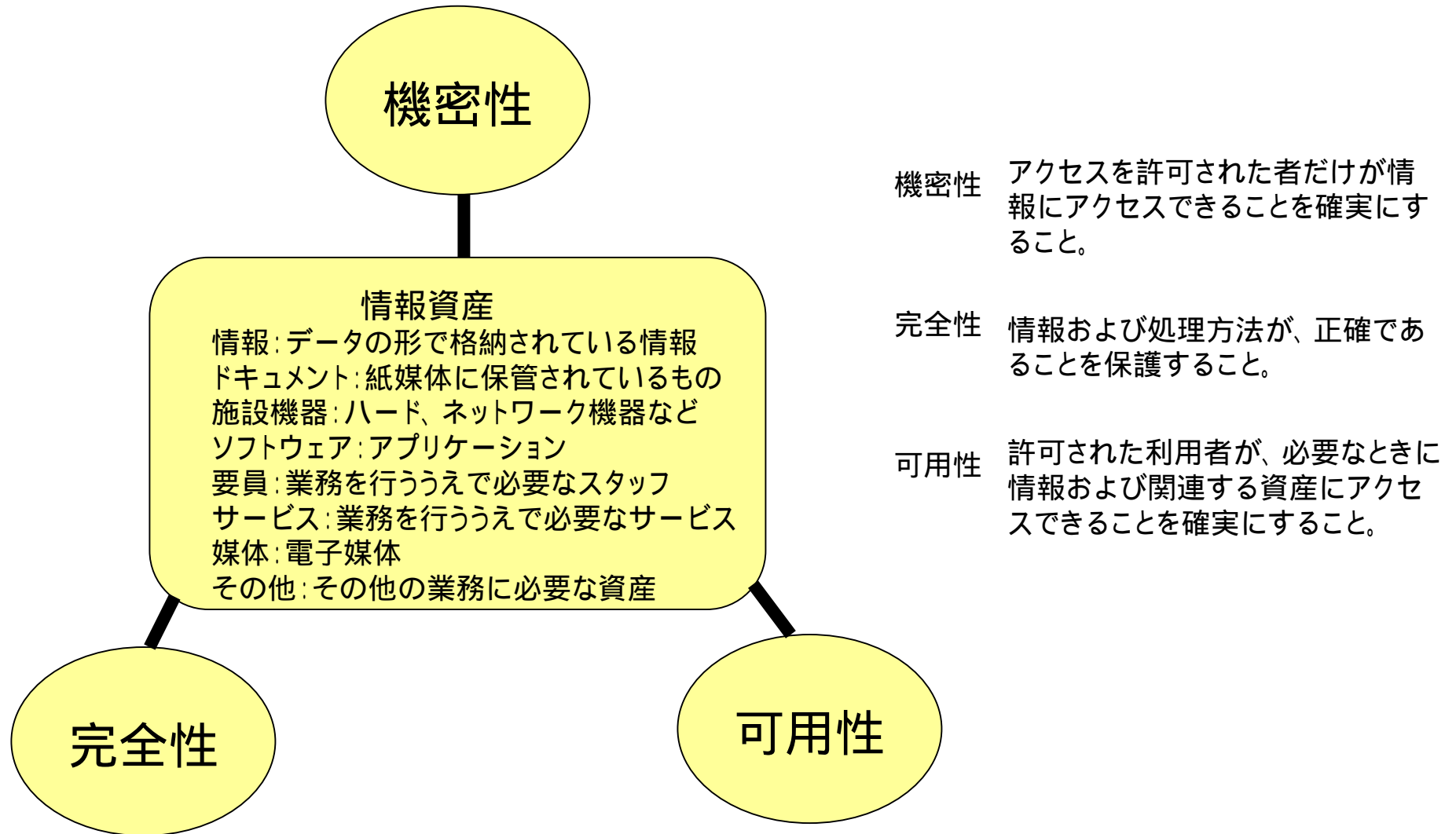
情報はどこにあるか

個人用のコンピュータ
サーバ
電子媒体
机の中
キャビネット、倉庫



情報セキュリティを複雑にしているのは、情報が複数の形態を持ち、存在するところも複数あるということに要因があると思われる。

情報セキュリティの概要



情報セキュリティ対策で必要な知識

管理・人的知識

情報セキュリティ基本方針
組織人事
文書管理
人的セキュリティ(教育など)
事業継続管理

技術的知識

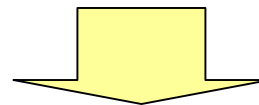
サーバ要塞化
アクセス権
認証
暗号化
デジタル署名
コンピュータウイルス対策
侵入検査

物理的知識

物理的および環境的セキュリティ

法律的知識

不正競争防止法
第3者との契約



情報セキュリティは、情報システムだけの問題ではないので、会社全体で取り組む必要がある。

リスクアセスメント

情報資産の価値

- 1: 事業に大きな影響を及ぼす
- 2: 業務の停止など事業に影響を及ぼす
- 3: 軽微な損害が発生する
- 4: 業務効率が低下する
- 5: 影響なし

脅威

「情報資産に関して、ビジネスリスクを顕在化し、実際の損害を発生させる物や行為や自然現象などのこと」

例

物: 水、ホコリ、火

行為: 不正アクセス、操作ミス

自然現象: 台風、地震

脆弱性

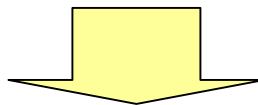
「脅威の攻撃により、情報資産が破壊されたり、盗難されたりすること」

例

施設: 入退出

アプリケーション: 不正アクセス

データ: 情報漏洩



リスク対策の方針

リスク回避

情報資産そのものを保有しないこと

リスク低減

リスクが顕在化する可能性を低くすること

リスク移転

自身が損害を被らないようにすること

リスク受容

そのリスクを受容すること

情報セキュリティ対策

業務プロセスの洗い出し

あらゆるプロセスに潜むリスクを把握しなければならないので、すべてのプロセスを漏れなく洗い出すことが必要である。

具体的なプロセス把握の作業は、プロセスの担当者に業務のプロセスを決まったフォーマットの書類に記入してもらう。

情報セキュリティ対策の選択

ISMS(情報セキュリティマネジメントの規格)の付属書「詳細管理策」を参考にする。

例
情報セキュリティ基本方針
組織のセキュリティ
人的セキュリティ
物理的及び環境的セキュリティ
通信及び運用管理
アクセス制御
システムファイルのセキュリティ
事業継続性管理

情報セキュリティ対策の手法・手段

費用対効果を考えて対応する。

どうしても、コストが捻出できない場合には、ハードウェアやソフトウェアの導入によって得られる効果を人的作業に置き換える。

情報セキュリティ規程の構成

情報セキュリティ基本方針

情報セキュリティに対する会社の取組姿勢や理念を表現した文書であり、すべての情報セキュリティ対策のよりどころとなる。

各種規程・基準

情報セキュリティ基本方針を受けて、分野別に行動規範を示した文書であり、業務の中での情報セキュリティ対策の基本的な対策を規程している。

手順・マニュアル・ガイドライン

各種規程・基準で規定されている情報セキュリティ対策を、より業務に密着した形式でまとめた文書である。

記録・ログ

情報セキュリティ対策の実施に関する記録である。

必ず必要な情報セキュリティ対策

項目	内容
サーバの要塞化	バージョン最新化、パッチ適用、不要なサービスや機能の停止。
アクセス制御	ある情報資産に対してアクセス権限がある者となない者とを明確に区別する。
認証	ユーザアカウントおよびパスワードの発行基準を明確にしておく。
ウイルス対策	パソコン、サーバ、インターネットとの接続口にウイルス対策ツールを導入する。
侵入検査	ネットワーク、サーバでログを取る。
データのバックアップ	保管期間、保管場所、復旧手順を検討する。
稼働情報の監視	システムリソースの使用状況をリアルタイムに監視する。

情報セキュリティ対策支援

1. 主なスケジュール

フェーズ	内容	回数
現状調査・リスク分析	情報セキュリティ保護方針の作成、情報の特定、業務フローの洗い出し、など	6回程度
マニュアル作成	情報セキュリティマニュアルの作成、など	5回程度
仮運用・監査・申請	運用計画作成支援、内部監査、申請、現地審査是正処理、など	4回程度

2. 主なサービス・特典

- 1) 約30分程度の無料相談を実施中です。
- 2) 1回からの訪問も可能です。
- 3) ご契約先には、弊社が作成した電子ファイルを提供します。

3. 料金

1回の訪問(概ね3時間程度)で、10万円(税込み、10万5千円)。