# 国際規格・ＩＳＯ２７００１

## (情報セキュリティマネジメントシステム=ＩＳＭＳ)

株式会社環境セキュリティ・システム研究所
TEL092-483-1595

## １.「ＩＳＭＳ（情報セキュリティマネジメントシステム)」とは

### １－１.「情報資産」(information　asset)

① 人そのもの＝知識・ノウハウ・社内で知り得た情報
② 顧客・取引・営業・財務・社員・人事などの情報で紙または電子データ
③ 情報を処理する為のマニュアル・規定・手順書・指示書
④ コンピュータ及び周辺機器のハード・ソフトとネットワーク機器
⑤ 情報を保管する媒体・ＰＣ／サーバ・保管庫
⑥ 電源設備・施設・建物、運搬機器など

### １－２.「情報セキュリティ」

情報の「Ｃ」と「Ｉ」と「Ａ」を維持すること

**機密性**（confidentiality）：アクセスを認可された者だけが情報にアクセスできることを確実にすること

**完全性**（integrity）：情報及び処理方法が、正確であること及び完全であることを保護すること

**可用性**（availability）：認可された者が、必要なときに情報及び関連する資産にアクセスできることを確実にすること

### １－３.「情報セキュリティマネジメントシステム（ＩＳＭＳ)」

プロセスアプローチに基づく、**Ｐ**ｌａｎ（計画）―**Ｄ**ｏ（実施）―**Ｃ**ｈｅｃｋ（点検）― **Ａ**ｃｔ（見直し・改善）の仕組みをもった経営管理の手法を採用している。

《 詳細は、別紙参照 》

### １－４．ＩＳＯ２７００１

２００５年１０月に、従来の、ＢＳ７７９９（英国)、ISMS 認証基準（日本）をベースとして、国際規格化されました。

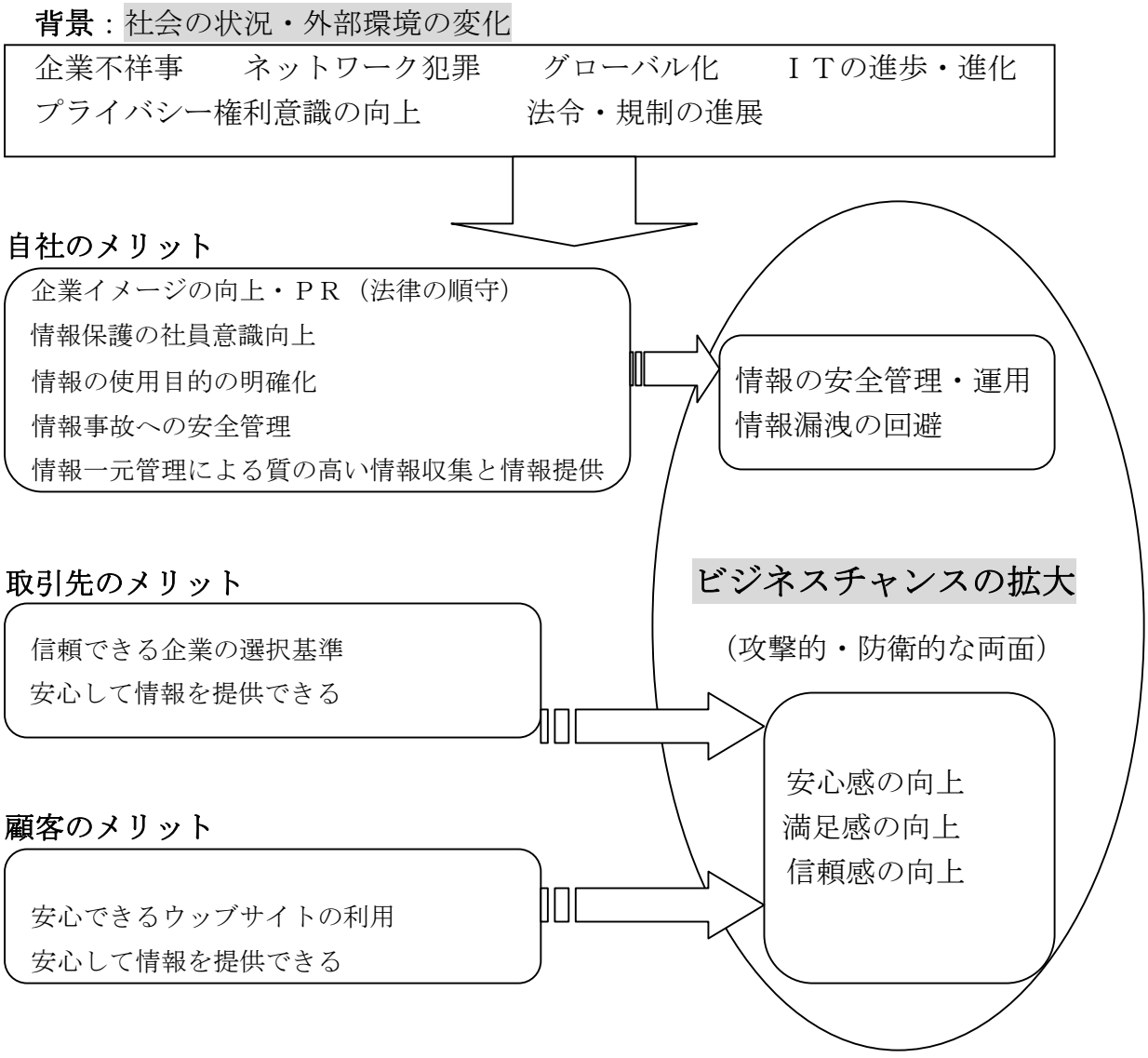
# ２．ＩＳＭＳの背景と必要性

## ２－１．ＩＳＭＳの背景

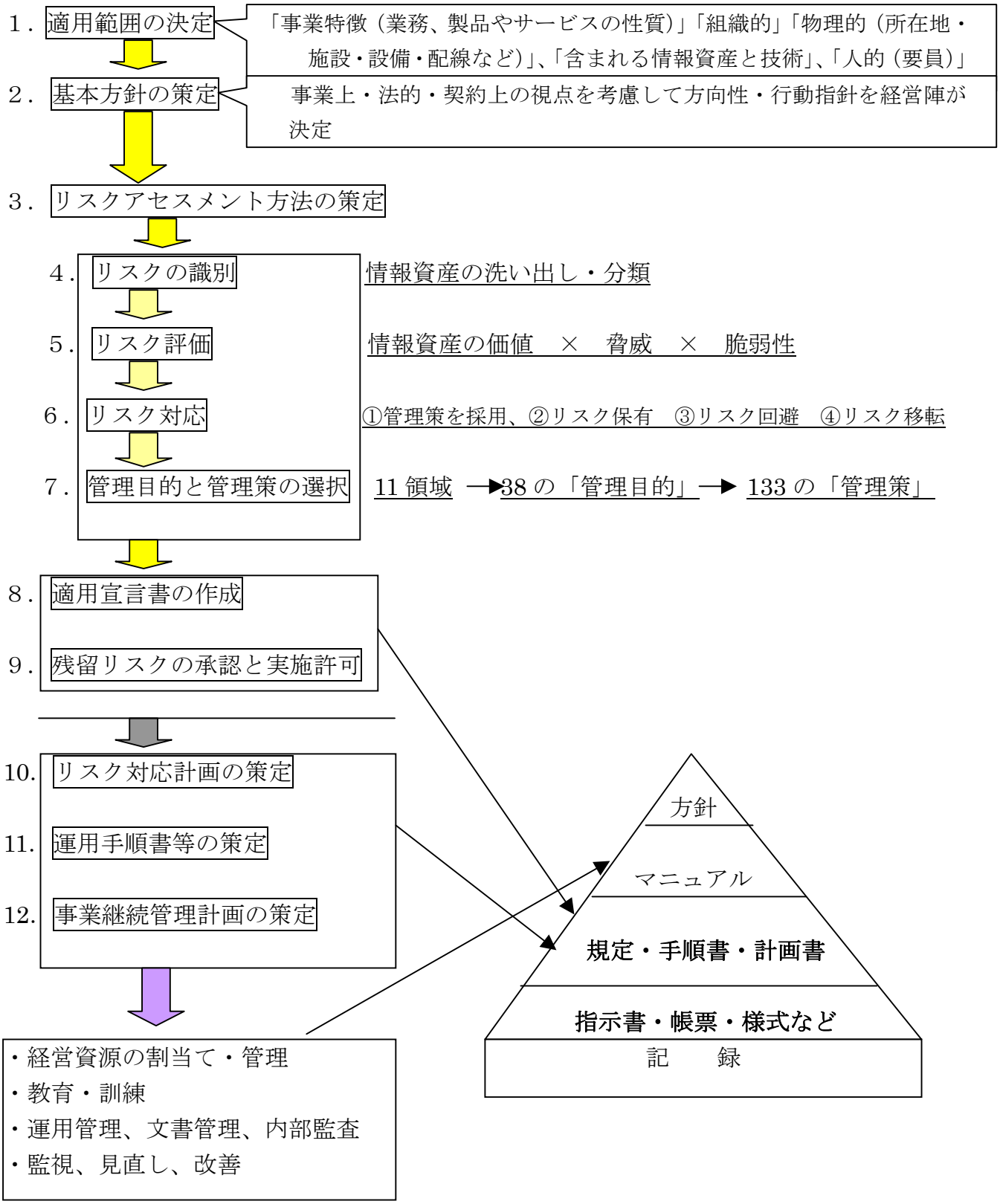
ＩＴの進歩・進化に相まって、企業活動において「情報資産（特に、情報処理施設やデータ）」は、非常に便利で、効率的な業務を行ううえで、現在では必要不可欠なものとなっている。逆に言えば、グローバル化やネットワーク化のなかでは、企業は情報について大きな経営リスクを背負い込んだ。
このことを解決する手段として、情報セキュリティ技術とマネジメントシステムを組み合せたＩＳＭＳが広がりつつある。

## ２－２．情報セキュリティ事件・事故

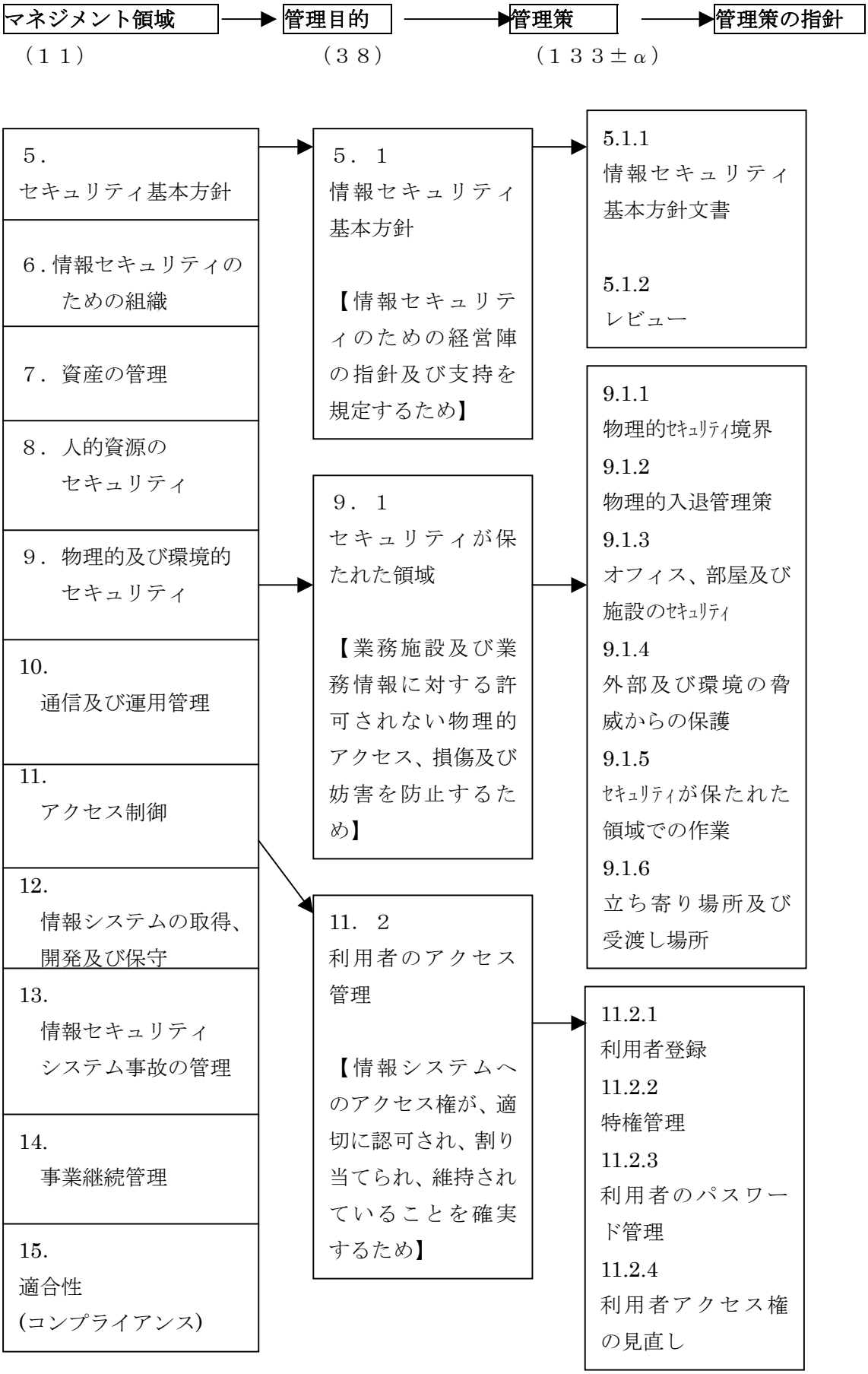
個人情報漏えい：“ヤフー２４０万人漏洩（５００円、１万円、10 万円）”　“ｼﾞｬﾊﾟﾈｯﾄたかたの漏洩”
金融機関のシステムダウンやトラブル：“ＡＴＭの１日利用不能”　“顧客の口座からの二重引き落し”
証券会社のシステムダウンやトラブル：“取引不能”“誤取り引き”
社外での情報資料の盗難　電子メールの誤送信
情報資産の被害状況：コンピュータウイルス発見・感染、不正アクセス被害、スパムメールの中継・踏み台、ウエブでの誹謗中傷、ホームページ改ざん、故意・過失の情報漏えい



## ３．ＩＳＭＳの構築手順と内容



# ４．ＩＳＭＳ「詳細管理策」の構成



## ５．「プライバシーマーク」と「ISMS(ISO27001)」の違い

| | プライバシーマーク | ISMS(ISO27001) |
|---|---|---|
| 対象情報 | 個人情報 | 情報資産全般 |
| 対象範囲 | 全社（全事業所） | 範囲を組織で設定 |
| 基準 | 日本工業規格 JISQ15001<br>個人情報保護法 | 国際規格 ISO27001（2005.10） |
| 審査機関 | （財）情報処理開発協会<br>など６団体 | ISO 審査機関（現状、２０社程度） |