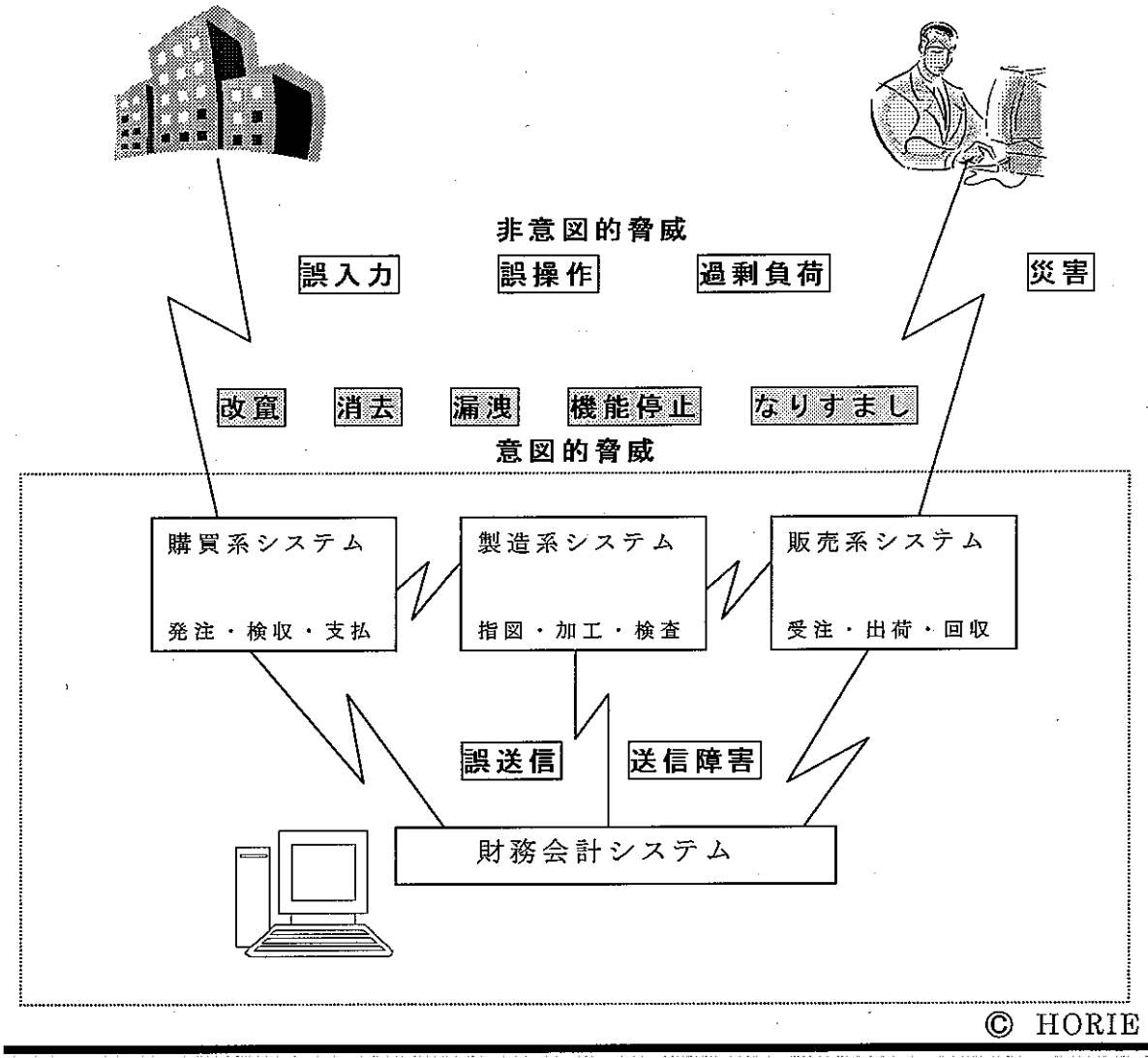
資 料 1

# IT 統制と IT 統制規準

目　　次

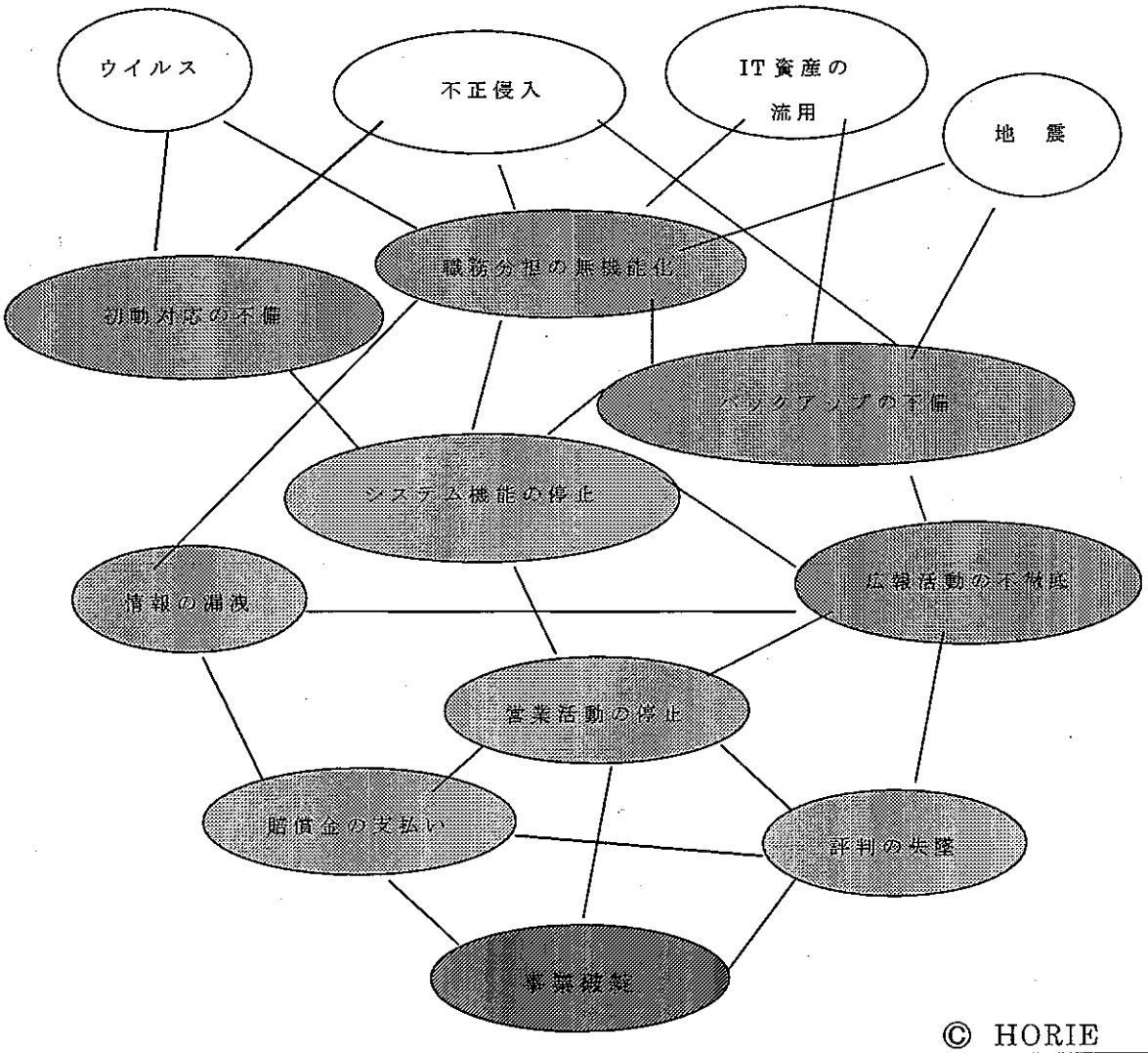
# 1 財務会計システムとITリスク

## （1）財務会計システムをめぐるさまざまな脅威



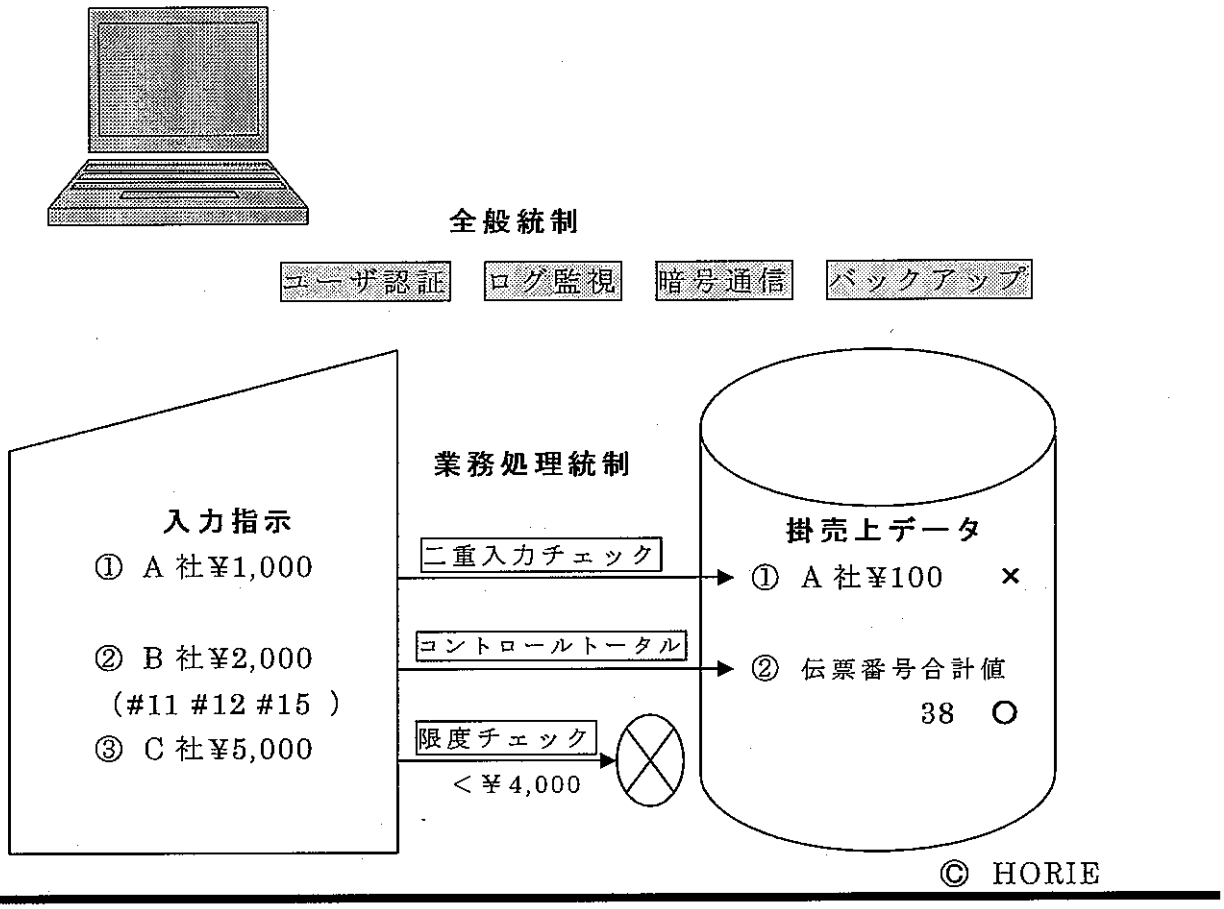

- 脅威には、意図的なもの（なりすましによるデータの不正入力など）と意図的でないもの（キー操作ミスによる二重入力など）があり、また企業外部からの脅威（DoS攻撃によるシステムの機能停止など）もある。
- 財務会計データは各種業務プロセスの結果として受け入れることから、財務会計システムに対する脅威は、企業外部との接点をもつこともある購買系システムや販売系システム（Webやメールシステムを含む）に対する攻撃や機能不全によることが多い。

## （２）ITリスクの連鎖（ビジネスリスクとしてのITリスク）




・ コンピュータウイルスやシステムへの不正侵入が、初動対応やバックアップの不備と結びつくと、システムの機能停止、そして営業活動の長時間にわたる停止を招き、顧客への広報活動の失態でも重なれば、事業体の信用や評判に大きなキズがつく、という「原因―誘因―帰結」のつながりでリスクの連鎖をとらえると、ITリスクは決して技術的なリスクにとどまらないことが分かる。ITリスクはビジネスリスクとして捉えることが重要である。

## 2 IT統制の仕組み（財務会計データの正確性・網羅性・正当性の確保）




- 業務処理システム（購買・製造・販売・在庫・人事・会計システム等々）に共通し、その基盤となる統制を「全般統制」と呼び、個々の業務処理システムごとに、正当なデータが正しくかつ漏れなく入力・処理・出力されることを確保するための統制を「業務処理統制」と呼ぶ。
- 全般統制には、パスワードや生体識別などを使ったユーザ認証、アクセスログやネットワークログの監視、ファイルや通信回線の暗号化、バックアップなどがある。
- 業務処理統制には、入力データの正確性を確保するための二重入力チェック、網羅性を確保するためのコントロール・トータル・チェック（伝票番号や日付などの合計値照合）、正当性を確保するための限度チェック（入力限度などの条件照合）などがある。

## 3 IT統制の規準（IT統制のベストプラクティス / ベンチマーク）

### （1）統制種別型：「ISO/IEC 17799：2000（JIS X 5080:2002）」

**＜統制の体系＞**

- セキュリティ基本方針
- 組織のセキュリティ
- 資産の分類および管理
- 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
- システムの開発及び保守
- 事業継続管理
- 適合性

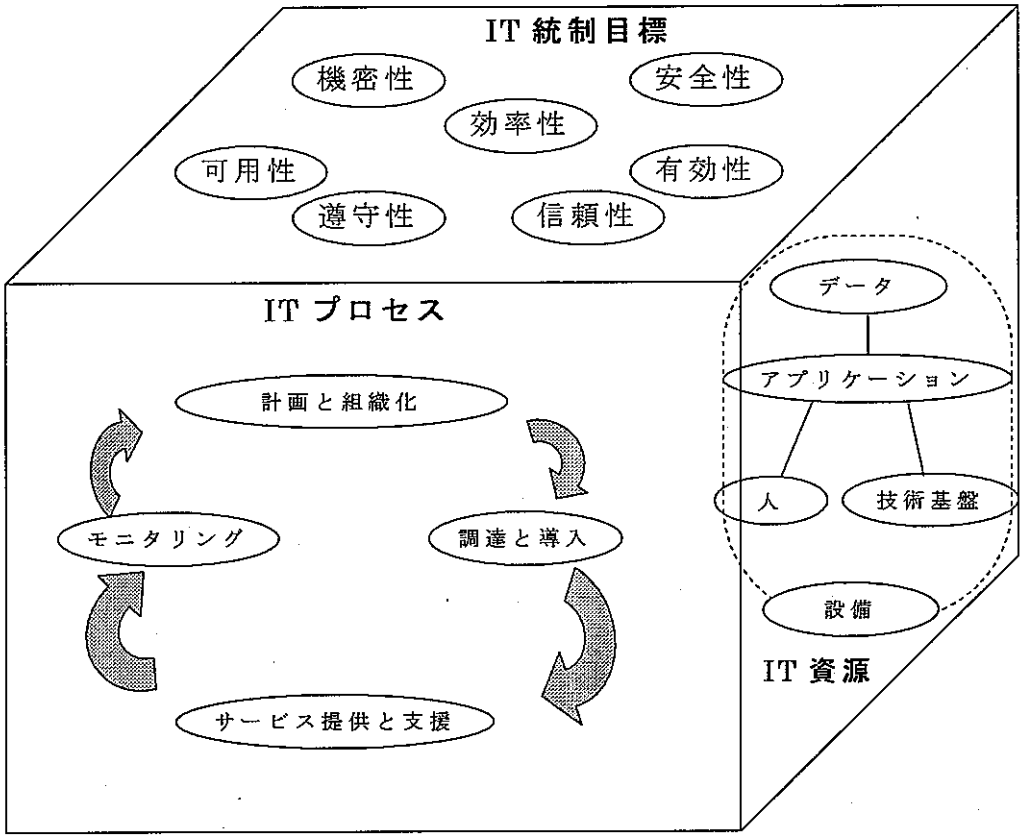
**＜統制目標＞**

- 機密性（confidentiality）
- 完全性（integrity）
- 可用性（availability）

---

- ISO/IEC 17799とは、国際標準化機構（ISO）及び国際電気標準会議（IEC）が共同で組織した委員会から公表されている企画で、国際的にみても、もっともポピュラーなIT統制規準である。我が国では、本規格の内容を修正することなく翻訳し、日本工業規格JIS X 5080:2002として公表されている。
- 情報セキュリティに特化した規準であり、統制の種別ごとに、統制目標と具体的な統制手続を規定する方式をとっている（統制種別型）。
- 我が国では、（財）日本情報処理開発協会が運営するISMS（情報セキュリティマネジメントシステム適合性評価制度）で利用される規準となっている。

## （２）統制要素関連付け型：「COBIT」（情報システムコントロール協会）




[出所：*COBIT —Framework—*, 2000, p.16.を修正の上転載]

---

- COBIT とは、情報システム監査やコントロールに携わる人達がボランティアで運営している情報システムコントロール協会から公表されている IT 統制と監査のガイドラインで、そこに含まれる Control Objectives が IT 統制規準となる。
- 情報セキュリティだけでなく、IT システムの有効性や効率性などのいわゆる前向き統制規準も含んだものであり、IT プロセスごとに、IT 統制目標と IT 資源とを関連づけて、具体的な統制手続を規定する方式をとっている（統制要素関連付け型）。
- Audit Guidelines がセットになっており、Control Objectives に対応した具体的な監査手続が規定されている。

### （３）システムライフサイクル型：「システム管理基準」（経済産業省）

- 情報戦略
- 企画業務
- 開発業務
- 運用業務
- 保守業務
- 共通業務

### （４）その他の規準

① AICPA, *Trust Service Principles and Criteria*
② CICA, *IT Control Guidelines*
③ IIA, *eSAC*
④ その他

---

- 「システム管理基準」は、経済産業省から公表されているもので、戦略策定、ITシステムの企画、開発、運用、保守、そしてそれらに共通する統制という体系になっており、基本的には、ITシステムのライフサイクルに沿って具体的な統制手続を規定する方式をとっている（システムライフサイクル型）。
- 管理基準とセットで公表されている「システム監査基準」に則って監査を実施する場合の判断の尺度として策定されたものであるが、もちろん監査を前提としないでITシステム管理のガイドラインとして利用することもできる。
- 米国公認会計士協会（AICPA）、カナダ勅許会計士協会（CICA）、内部監査人協会（IIA）からも、IT統制規準が公表されている。
- その他、我が国では、情報サービス産業協会の「情報資産活用のための情報セキュリティガイドライン」、ソフトウェア資産管理コンソーシアムの「ソフトウェア資産管理基準」、金融情報システムセンターの「金融機関等コンピュータシステムの安全対策基準」なども、IT統制規準としての性格をもったものである。

## 4 IT統制をめぐるトピックス

### （1）統制の成熟度モデル





| レベル1 | レベル2 | レベル3 | レベル4 | レベル5 |
|---|---|---|---|---|
| 最低限のIT統制を場当たり的に実施 | IT統制は計画され、結果が追跡 | IT統制のプロセスが標準化 | IT統制を定量的に把握 | IT統制が継続的に改善 |

© HORIE

### （2）統制の段階保証モデル（NISTのモデル）

| | 統制の成熟度 | | 保証手続の厳格度 |
|---|---|---|---|
| 認証レベル1 | 低 | …… | 低 |
| 認証レベル2 | 中 | …… | 中 |
| 認証レベル3 | 高 | …… | 高 |

---

- 成熟度モデル（maturity model）とは、要求特質を定義することによって、IT統制を段階的にレベル分けする考え方である。ソフトウェア開発プロセスの能力評価のために開発されたモデルをIT統制に応用したものである。成熟度の区分けは、3段階でも、4段階でもよい。このモデルを使えば、統制目標ごと、対象部門ごと、あるいは対象システムごとに、現在のIT統制水準を明らかにできる。
- この成熟度モデルに応じて、保証手続の厳格度に差を設けて、段階認証を行おうとするモデルもある（National Institute of Standards and Technology：NISTの連邦情報システムセキュリティ認証制度）。

## ＜参 考＞ IT の脅威と IT 統制の現状

### （１）セキュリティ侵害

| CSI/FBI 調査（2004） | |
|---|---|
| ウイルス | 78% |
| 内部者不正アクセス | 59% |
| PC の盗難 | 49% |
| システム侵入 | 39% |
| 情報へ未承認アクセス | 37% |
| DoS 攻撃 | 17% |

| 総務省調査（2004） | |
|---|---|
| ウイルス | 97.8% |
| スパムメールの踏み台 | 11.6% |
| DoS 攻撃 | 7.9% |
| IP・メールアドレス詐称 | 7.1% |
| Web 上での誹謗等 | 4.5% |
| 内部者不正アクセス | 1.1% |

### （２）セキュリティ対策

| CSI/FBI 調査（2004） | |
|---|---|
| ウイルスソフト | 99% |
| ファイアウォール | 98% |
| 送信データの暗号化 | 64% |
| ワンタイムパスワード | 35% |
| 生体認証 | 11% |

| 総務省調査（2004） | |
|---|---|
| ウイルスソフト | 95.9% |
| ファイアウォール | 89% |
| 暗号化 | 40.9% |
| ワンタイムパスワード | 18% |
| 生体認証 | 2.1% |

### （３）セキュリティ被害額/復旧コスト

| CSI/FBI 調査（2004） | |
|---|---|
| ウイルス被害額 | $55,053,900 |
| DoS 攻撃被害額 | $26,064,050 |
| 情報資産の盗難被害額 | $11,460,000 |
| 内部ネット悪用被害額 | $10,601,055 |

| 総務省調査（2004） | |
|---|---|
| ウイルス被害復旧コスト | |
| 10 万円以上 | 20.7% |
| 5～10 万円 | 0.8% |
| 1～5 万円 | 2.7% |
| 0 万円 | 26.4% |

＊ CSI/FBI, *Computer Crime and Security Survey*, 2004（回答者の約65%が従業員 500 名以上の事業体に所属）

＊ 総務省「情報セキュリティに関する実態調査」2004(上場会社を対象としたデータを利用)