# リスクとガバナンスから見た情報システム

伊藤重隆†
Shigetaka　Ito†
†みずほ情報総研株式会社

† Mizuho Information & Research Institute Inc.

**要旨**
情報システムは、現代社会では公共、企業等の各重要分野で大きな役割を果たしている。情報システムが提供する情報とサービスは、人間活動に欠かせないものになっている。見方を変えるならば、情報システムが提供する情報とサービスが中断された場合には大きな影響が生じる。社会、企業に取り信頼のある情報システムとするには、ガバナンスとリスク管理が重要な決め手になる。本論では、リスクとガバナンスの視点から現在の情報システムの状況を概観しリスクマネジメントとガバナンスの問題点を提示したい。

## 1. はじめに

情報システムについては、セキュア・ジャパンの施策として重要インフラ１０分野において「安全基準等」の見直しを毎年行っている。安全基準等から抽出した重点項目の中にも「ＩＴ障害の観点から見た事業継続性確保のための対策」が挙げられている。また、２００９年3月２４日に「情報システムの信頼性向上に関するガイドライン」第２版が経済産業省より公表されている。いずれも情報システムの社会における重要性を意識した取組である。又、ＯＥＣＤのコーポレートガバンスの定義を参考に、ＩＳＡＣＡ（Information Systems Audit and Control Association）ではＩＴガバンナスについて、下記の様に定義している。「ＩＴとそれらプロセスのリスクとリターン（利益）のバランスをとりながら、価値を増大させることにより、企業目的達成のために企業の方向付けをしコントロールする一連の関係構造とプロセスである」。コーポレートガバナンスを実現する時の、ＣＯＳＯ内部統制―統合フレームワークが米国トレッドウェイ委員会組織委員会から１９９２年に発表されている。２００４年には、内部統制の枠組みを拡張するものとしてＣＯＳＯエンタープライズ・リスク・マネジメント（ＥＲＭと呼称）がＣＯＳＯから公表されている。ＥＲＭにおいては、内部統制概念を事業体の全体的なリスクの観点から拡張している。この中のリスクの定義として、「企業に影響を及ぼす事象のうち、マイナスの影響を持つもの」とされている。このリスクについて、「事象の識別」、「リスク評価」、「リスク対応」に細分化されている。日本においては、米国における企業改革法を受け、２００６年6月に金融商品取引法が成立し２００７年2月１５日に金融庁から「財務報告に係る内部統制評価及び監査の基準並びに財務報告に係る内部の評価及び監査に関する実施基準の設定」が発表され実施されている。この基準並びに実施基準においても内部統制の基本要素として「ＩＴへの対応」、「リスクの評価と対応」も定められ、企業においては多大な体力とコストをかけ実施している。しかしながら、情報システムの現状を概観すると必ずしも内部統制が十分で無く情報システムに係るリスクが顕在化する事象が散見されリスク管理が有効でないと考えられる。本論では、この問題点について論じる。

## 2. 情報システムのリスク顕在化事例

情報システムについてのリスク顕在事例は、新聞、雑誌に大きく掲載され、公表されている、又は、個別企業から公表されたものをベースに一般化しているが、以下はいずれもリスク大の事象と言える。

### ２.１　基本ＯＳ更改により基幹系システムが全面停止

情報システムが利用しているＯＳ（オペレーティング・システム）がメーカーの保守サービス停止となるので最新ＯＳへ更改した。同時に最新ＯＳとなるのでミドルウェアも最新とした。しかし周辺ユーティリティ・システムは最新ＯＳと関連ないと判断し、最新ＯＳを使用してサービス開始初日にオンラインシステムが待機系システムへ切り替えると言う長時間全面停止が発生した。原因は、関連が無いと考えられたユーティリティ・システムが実は最新ＯＳで稼動した場合、あるケースでミドルウェアに影響しシステムが無応答状態となった。

### ２.２ 一部ハードウェアの不具合により基幹系システムが全面停止

#### ２.２.１ ネットワーク機器の不具合のケース

基幹系システムのネットワークの一部が不安定となり、異常メッセージを多発した。このため、基幹系ホストシステムへの通信経路に異常メッセージが大量に滞留し基幹系システムが通常取引を受信できなくなり全面的に停止し結果、売上減収となった。原因は、ネットワーク上に大量にメッセージが滞留したことが迅速に検知できなかった。

#### ２.２.２ 磁気ディスク装置の故障のケース

基幹系オンラインシステムで利用している磁気ディスク装置の一部が故障したが、予備機が稼動せず基幹系オンラインシステムが全面停止となった。又、この影響で磁気ディスク装置に格納していたデータが消失し、データの再作成に大きな時間を要した。原因は、予備機は迅速に稼動する予定であったが、ハードウェア保守が不適切であった。

### ２.３　システムの制約条件により長時間停止

#### ２.３.１　入力締め切り時刻制限のケース

基幹系システムの運用スケジュールを大幅に変更する必要が生じた。変更するために大量の変更データを基幹系システムへ入力したが、入力データがシステムへ反映されず基幹系システムを長時間運用停止とした。原因は、入力締め切り時刻が考慮されていなかったことによる。

#### ２.３.２　サーバー認証期限切れのケース

基幹系システムでは情報セキュリティ強化のためメッセージ暗号機能を利用していた。この機能がある日、ある時刻以降から利用不可の状況が発生し長時間停止となった。原因は、暗号化機能利用には、有効期限があるがこの期限の延長がされずに原因究明に長時間を要したために長時間停止となった。

### ２.４　異例情報入力の結果、一部投資家損失発生

マーケット・レートと大幅に乖離した異例取引が約定システムで成立し、結果として一部投資家が清算時に大幅に損失を被る状況が発生した。原因は、マーケット・メーカーが異例な価格を提示したが、異例な価格が保留・確認されずに取引表示された。約定システムはリアルタイムであるので即時に取引が成立したもの。　原因は、約定システムではなく情報システムとして適正では無い取引が成立したことによるものであった。

### ２.５　大規模情報システムの機能不全

情報技術を駆使した大規模情報システムは、新規情報システム構築時、以後に過去　紙ベースの情報を移行データとして取り込みデータベースを構築した。しかしながら、移行時のデータ確認が不十分であったので、データベースを使用して作成する資料が不正確で事実を反映しておらず、情報システム再構築となった。原因は、上記の移行データ確認がユーザーとして未済な件数が多かったことによる。

## ３．事例から判明したリスクとガバナンスの課題

### ３.１　情報システムの信頼性評価

情報システムの信頼性評価を行う場合に、情報システムが全面サービス停止となるリスクの所在が明らかにされていない。大きなリスクが顕在化した後に対応がされていて、内部統制で言うリスク評価とリスク対応が不足していてガバナンス上、問題がある。金融商品取引法実施以降、IT 全般統制等の重要性が認識されて来ているが、形式的なリスク評価方法ではリスク抽出が期待できず潜在リスク大の事象抽出を情報システムの安定稼動に影響するクリティカル・ポイントを判別する等の新しいアプローチを必要としている。

### ３.２　情報システムの状況変化への対応

情報システムは、人間活動と同時に成長している。情報システムの構成要素が増加する、利用方法の多様性が発生する、機能変更等が生じる、サービス範囲が拡大している等の運用上に大きな変化が生じる。この情報システムの変化を的確に捉えリスク評価することが必要である。

### ３.３　情報システムの合目的性

情報システムは、情報システム構築時に人間活動を適切にサポートするために構築される。当初の目的が達成されているかを評価することがリスク評価として有効である。更に、従来の情報システムには大量処理、効率性の視点が重視されてきたが、情報システムの社会で果たす役割が大きなものとなっているので保有する情報、伝達する情報の適確性へのガバナンスが課題である。

## ４.リスク評価の新しいアプローチ（試論）

**リスク評価については、リスクマトリックスの様にリスク影響度、発生頻度の組み合わせでリスク事象をとらえる場合が多い。このアプローチは、システムが動的であることが表現されない。リスクマトリックスに時間軸を導入することで、リスク小からリスク大となる事象が抽出されると考える。**
**重要度大の状態に時間経過により重要度小、中の事象が遷移する事象抽出によりリスクマネジメントが強化され未然にシステム停止を防止するケースを図４に例示する。又、この分析は主系統から待機系統への切り替えを想定する場合も適用可能である。**

| | 重要度　大 | 重要度　中 | 重要度　小 |
|---|---|---|---|
| 頻度大 | | | |
| 頻度中 | | | 通信エラー |
| 頻度小 | メモリ容量超 | | |

図４　例示　重要度小から重要度大へ時間経過により遷移するケースの分析表

## ５.まとめ

企業、公共団体は、ユーザーより大きな信頼を受けている。情報システムの信頼性を向上させるのは、社会的な要請と考えられる。一方、事例からわかる様に内部統制が強化される中でＩＴリスク評価もされているが、情報システムとして全面サービス停止となるリスクの未然解消が十分にされていない。

情報システムはＩＴを大きな構成要素としているが、技術の進展、更に情報システムが複雑化により、ガバナンスを発揮すべきユーザー企業、公共団体が追いつけない状態が生じている懸念がある。

今後、情報システムのユーザーのみならず業界レベルにおいてリスク解消に向けた取組が必要である。又、情報システムは人間活動と共に成長すると情報システム構築直後の制約条件が変化するのでこの面からもリスク評価し未然の対応が重要な課題となる。情報システムについては、情報システム構築後にサービス提供主体として情報システムの果たす役割が社会において合目的であるか否かについても評価

し、その評価により情報システムを改善すべきである。

## 参考文献

[1] ハリー・ブーネン＋コーエン・ブランド,峰本展夫監訳、ＣＯＢＩＴ入門,生産性出版,2007.
[2] 経済産業省, 情報システムの信頼性向上に関するガイドライン第２版,2009.
[3] 金融庁, 財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る
内部統制評価及び監査に関する実施基準の設定, 2007.