TRC EYE Vol. 64

東京海上日動リスクコンサルティング（株）
所属　リスクコンサルティング室情報グループ
主席研究員　近森　健三

情報サービス業を取り巻くリスクとリスク管理の重要性について

１．IT 社会の進展と情報リスク

情報通信業界における価格競争の激化と技術の向上、e-Japan 戦略など国をあげての IT 推進により、IT 社会、ネットワーク社会が急速に進展しています。ブロードバンド化によるインターネットサービスの充実、携帯電話の高機能化によって、一般消費者もいつでも気軽にショッピングや証券取引ができるようになりました。このように社会全体が IT の恩恵を得ている一方で、コンピュータウイルスによる被害、顧客情報の流出、システムダウンなどの事故事例が多くなり、企業や消費者に被害が発生しています。その頻度と被害の規模は、IT 化の進展とともにより広範囲にかつ深刻になっていると言えます。特に、社会をささえる重要なシステムの場合は、甚大な被害に繋がる恐れもあります。

（表１）重要インフラを巡る最近の IT 障害の事例　（報道ベース）

サイバー攻撃	非意図的要因（人為的ミス）等
・豪クイーンズランド州で、市の水道施設の制御システムに侵入した犯人が、未処理の汚水100万リットルを河川および沿岸部に流し込んだ（平成12年3月） ・米カリフォルニア州の電力会社の送電網システムに外部者が不正侵入（平成13年6月） ・SQL slammerワームが猛威を振るい、韓国では一時インターネットに障害が発生（平成15年1月） ・米鉄道の信号システムがコンピュータウイルスに感染、ワシントン周辺3路線で列車が停止したりダイヤが乱れるなどした（平成15年8月）	・大手銀行の合併に伴うシステム統合において、口座振替の未処理など大規模なシステム障害が発生、復旧に時間を要した（平成14年4月） ・インターネットバンキングのサービスがデータベースサーバの障害により全面的にダウン（平成15年5月） ・飛行計画情報処理システムがプログラムミスによりダウンし、200便近くが遅れるなど、航空ダイヤが全国的に混乱（平成15年3月） ・注文件数の増加により証券取引所の売買システムや株価情報システムの処理が遅延（平成15年7月） ・通信制御プログラムの不具合が原因で、金融機関同士のATMネットワークで結ぶ「統合ATMスイッチングサービス」に障害発生。全国約20の金融機関のATMで他行カードを利用した取引が不可に（平成16年1月） ・航空路レーダー処理システムのトラブルでメインシステムを停止、国内便約130便に影響（平成16年4月）

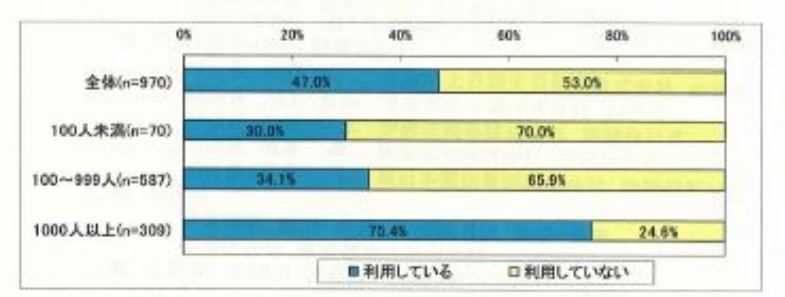
（内閣官房情報セキュリティ対策推進室報道発表資料より抜粋）

２．アウトソーシングの増加とリスク

企業が情報システムの開発や運用を外部にアウトソースする割合は引き続き高く、特に大企業においてその傾向は顕著です。（社）日本情報システム・ユーザ協会（JUAS）が毎年実施して

いる企業 IT 動向調査によると、従業員１０００人以上の大規模企業のうちシステム運用業務をアウトソースしている割合は、２００５年調査では 75.4%（前年度は 68%）
と７割を超える水準となっています。アウトソースを選択する狙いは様々と思われます。コストの明確化や圧縮が主目的である場合が多いのですが、特にここ数年、ウィルスなどの被害拡大や個人情報保護の高まりを受け、システムベンダーが持つ情報セキュリティについての専門的技術やノウハウを活用することにより、運用の安全性や安定性の確保の実現を期待するところが大きいと考えられます。その裏返しとして、システムサービスベンダーは、より高度なセキュリティ体制を維持する責任を負うことになります。

（図１）JUAS 企業 IT 動向調査２００５

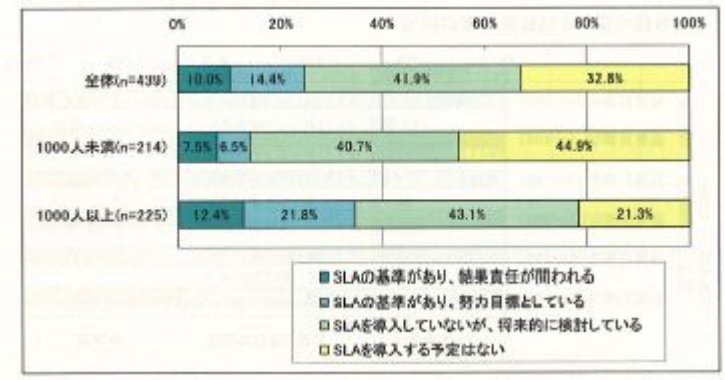


※４７％の企業が運用業務をアウトソーシング。大企業では７５.４％。

３．サービスレベルアグリーメントの浸透とリスク管理

このようなアウトソーシングにおいて、企業とシステムサービスベンダーとの間におけるサービスレベルについて、より詳細な取り決めを契約時の仕様書に記載しておくケースが増えています。一般的にサービスレベルアグリーメント（SLA）とも言われており、SLA によってシステムサービスベンダーは、ユーザー企業に対し一定レベルのサービスを保証する責務を負うことになります。前述の JUAS 企業 IT 動向調査２００５年においては、従業員１０００人以上の大規模企業において、「導入済み」が 34.2%、「将来検討している」が 43.1%となっており、今後 SLA が浸透する傾向にあることを示しています。

（図２）JUAS 企業 IT 動向調査２００５



※４割強が将来的にＳＬＡの採用を検討。

SLA の対象となるサービスレベルには、サービスの利用可能時間や稼動率などシステムの稼動時間に関する事項や、情報処理量や応答時間などパフォーマンスに関する事項などがあり、これに付随してトラブル発生から復旧までの時間や障害発生件数の上限数値を決めるケースもあります。そして、万が一このサービスレベルが守れない場合には、システムベンダーに対して一定のペナルティが課せられるほか、場合によっては損害賠償責任を負うことにもなります。

４．システム開発をめぐるトラブル

SLA は主にシステム運用における品質管理に関わるものですが、システム開発過程における品質管理が原因でトラブルが発生する事例も多くあります。ここ数年でシステム関連の訴訟が増加しているとの報告もあり、納品したシステムの品質に問題があったためにトラブルが発生し、ユーザー企業が損害を被ったというケースが新聞等でも報じられています。システム開発においてシステムベンダーとユーザー（発注者）との間での権利義務関係は、いわゆるシステム開発委託契約書などで定めておくわけですが、その内容は大規模なものであってもテストや検収など品質をチェックするための手順や判定方法まで詳細に定めたものは少なく、一般的な雛形が使われているケースが多いのではないでしょうか。

もちろん請負契約であれば検収責任や瑕疵担保責任などが謳われているわけですが、納品後トラブルが発生した場合において、どちらに責任があるか不明確な場合も往々にしてあります。当初の契約に想定していなかった仕様変更の発生や、当事者間のコミュニケーション不足によるプロジェクトの遅延などがトラブルにつながることもあり、契約時およびその後における両者の責任を契約書に盛り込んでおくことが重要と言えます。

（表２）訴訟事例

概要	詳細／原因
ソフトウェア開発委託において、ライセンス料の支払いと仕様変更による開発期間の遅延と開発委託費の負担について争いとなったケース ・　著作権侵害差止請求 ・　開発委託費請求	【詳細】 委託者Ａ社はソフトウェア開発をＢ社に発注。当初詳細仕様までは決まらなかったことから基本設計までの見積もり書により契約。その後、詳細設計レベルでの契約において、Ｂ社の見積もり額がＡ社の予定価額を大きく超過していたため値引きを要請。結局、Ｂ社は完成品の販売数１本ごとにライセンス料を受け取ることを条件として値引きを承諾。その後、ソフトウェア開発の過程において、Ａ社より仕様変更の要請があったが、Ｂ社は明示的な金額を見積もらないままに対応を実施。結局、仕様変更が重なり商品としては不完全なまま販売を開始したもの。 Ｂ社はソフトウェアの委託費の支払いが完了していないため著作権を留保したうえで、仕様変更に伴う委託金額の支払いと、販売数量に応じたライセンスの支払いをＡ社に請求。一方Ａ社は、不具合の修正と仕様の反映が完了していないとの理由からＢ社の請求を拒否し著作権の侵害を訴えるという争いとなった。 【原因】 契約内容があいまいなままソフトウェア開発に着手したこと、仕様変更についてその都度見積もりのうえ書面で確認するという行為をすることなく開発を進めたことが原因。

システム開発委託において、検収後の不具合の発生と代替システムの開発費用について、委託者に損害賠償を請求したケース ・　損害賠償請求	【詳細】 Ａ社はシステム開発をＢ社に委託。Ｂ社はＡ社に告知したうえでＣ社に再委託。開発が終了しＣ社からＢ社での検収を経て、Ａ社に納品されたが、Ａ社でテストを実施した結果多くの不具合が発見された。Ｂ社の検収に合格していたためＣ社は非協力的であり改修が進まず、結局Ｂ社は代替システムをＤ社に発注したが稼動開始は大幅に遅延。 Ｂ社は障害対応に要した費用と代替システム開発費をＣ社に損害賠償請求する訴訟を提起したが、調停の結果Ｂ社は全額を取り戻すことはできなかった。 【原因】 テスト要件を明確にしていなかったこと、案件を再委託先に丸投げしていることのリスクを把握しておらず管理できていなかったことが原因。
システム保守委託において、保守会社の作業ミスによる損害賠償請求と、追加作業の費用に支払い請求を争ったケース ・　損害賠償請求 ・　開発委託費請求	【詳細】 Ａ社の基幹業務システムの保守を請負っていたＢ社は、Ａ社と合意のうえシステム改修テストを本番データのコピーを利用して実施することを計画。コピーの手順についてＡ社と詰めないまま、コピーを実施したところ作業手順を間違え直前１ヶ月の本番データを誤って消去。Ｂ社も協力のうえ手作業にてデータを復旧したが、改修計画は大幅に遅延。そのため当初契約ではＡ社が行うとしていた改修バージョンの端末へのインストール作業をＢ社が代行。改修した部分に不具合が発生し修正を実施したため更に遅延。 Ａ社はデータ復旧作業や遅延による損失をＢ社に損害賠償請求。請求額は契約書において委託金額を上限と定めていたが、それを超えるものであったためＢ社はこれを拒否。結局Ａ社はＢ社に対して訴訟を提起、Ｂ社もインストール作業等の追加費用の支払いを求める訴えを提起した。調停の結果、Ｂ社の請求額がかなり減額されたが委託金額を超える金額をＡ社に支払うことで決着。 【原因】 本番データを扱う保守作業における手順の確認を怠ったこと、システム改修部分についてのテストが不十分であったこと、トラブルが発生した後の対応や費用負担について取り決めをしなかったことが原因。

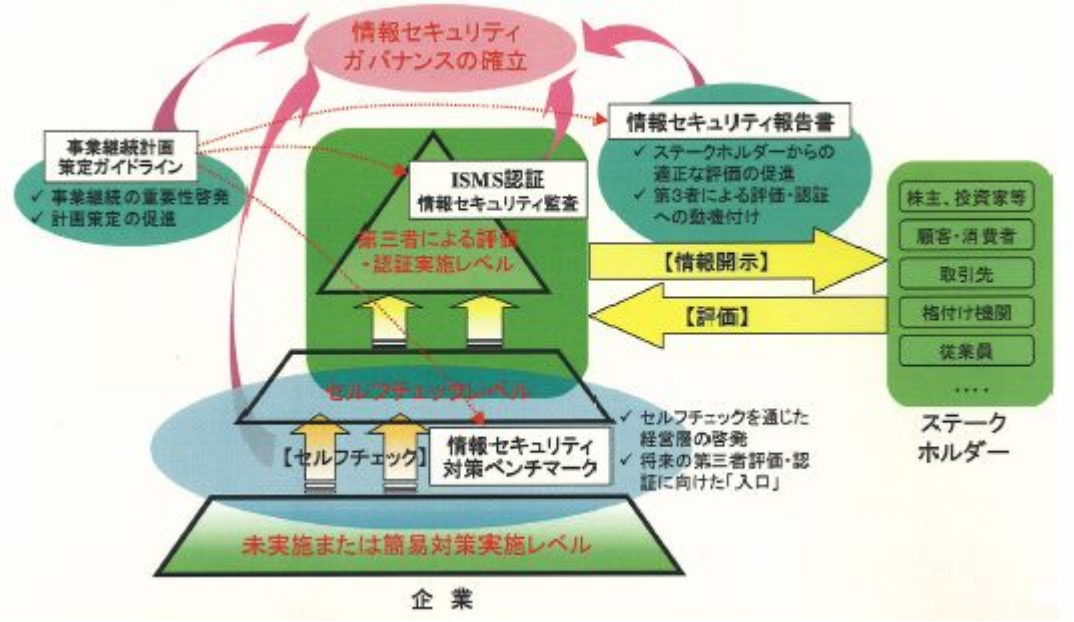
実際は、システム開発にはハードトラブルやソフトバグが付き物であり、トラブルが発生した場合にいかに被害の発生を最小限に食い止めるべく迅速なアクションを取るかがポイントとなります。これがうまく行かない場合において、当事者間での責任問題となり、訴訟にまで発展してしまうことになります。従って、システムベンダーサイドとしては、開発終了後においても、トラブル発生に備えた危機管理を敷いておくことが重要です。

また、2005 年４月から本格施行された個人情報保護法の関係から、システム開発委託や情報処理サービス委託契約において、発注者（委託者）側に委託先管理責任が課せられているため、システムベンダー（受託者）に対しより強い義務を課すような契約書の締結を求めるケースが増えています。受託者側の過失による損害賠償額の設定においていても、これまで委託料を上限としていたものを、場合によっては上限を定めないケースも出てきています。システムベンダーとしては、ますますリスク管理の必要性が高まっていると言えます。

５．事業継続計画（Business　Continuity　Plan）とリスク管理

２００５年４月に経済産業省の「企業における情報セキュリティガバナンスのあり方に関する研究会」から、事業継続計画策定ガイドラインが開示されました。この情報セキュリティガバナンス研究会では、IT が企業、ひいては社会の「神経系」を担う一方、情報セキュリティを脅かす種々のリスクが顕在化しているにもかかわらず、その対応が場当たり的になってしまい同じような事故を繰り返している状況を踏まえて、企業が自ら情報セキュリティへの取り組みを推進する仕組みを普及するためにいくつかの施策ツールについて提言しています。これら施策ツールの中で、自然災害等による情報システムのダウンや重要情報の流出等、企業の情報システムやネットワーク、情報資産に関連する突発的な事故が発生した場合であっても、事業を中断せず維持する仕組みとして提案されているのが、「事業継続計画策定ガイドライン」です。

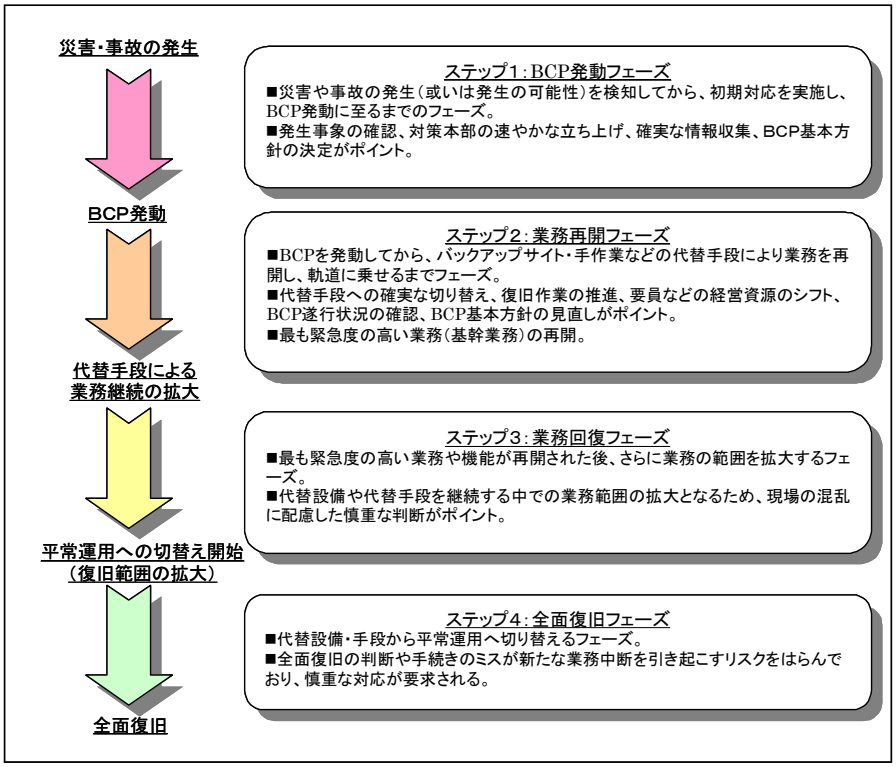
（図３）施策ツールと ISMS 認証等との基本的関係



（経済産業省・企業の情報セキュリティガバナンスのあり方に関する研究会報告書より抜粋）

「事業継続計画」とは、企業が情報システムの事故の発生を想定し、災害や事故の発生から完全復旧までの間、事業・基幹業務を中断することなく継続させるための具体的な計画（BCP）です。

（図４）BCP の流れ



（経済産業省・企業における情報セキュリティガバナンスのあり方に関する研究会報告書・事業継続計画策定ガイドラインより抜粋）

このガイドラインにおいては、BCP について、方針をたて、策定し、対策を実行に移し、教育・訓練し、見直すという、立案・策定から維持・管理のサイクル（PDCA サイクル）をマネジメントする仕組みを提案しています。

情報サービス業は、自らが重要な社会的インフラである情報通信やネットワークサービスを提供する事業体として、BCP のマネジメントに取り組むことが求められているばかりでなく、ユーザー企業の情報システムを支える企業として、ユーザー企業の BCP の策定や運営に重要な役割を果たすことになります。このような観点からも、情報サービス業においてリスク管理の重要性がますます問われることになると考えられます。

６．協力会社との関係

システムベンダーがユーザーとの関係において高度なリスク対応が求められている一方、協力会社に対しては、発注者の立場からよりきめ細かい管理を実施する必要がでてきています。システム開発プロジェクトや運用サービスにおいて、協力会社における品質管理はもちろんのことですが、機密情報を取扱う場合のセキュリティ対策が十分かどうか、不具合等が原因でトラブルが発生した場合の対応力があるかという情報セキュリティの観点からのパフォーマンス、万が一訴訟問題に発展した場合において賠償能力があるかどうか、賠償責任保険に入っているかなど財務面についても評価を行い、委託業務管理を実施していくことが重要となります。

（本稿は、『Corporate Risk（コーポレート・リスク）』2005 年vol.2（きらら保険サービス株式会社）に掲載されたものを、同社の許可をもって転載したものです。）

（第64号　2005年9月発行）