http://www.tokiorisk.co.jp/

TRC EYE Vol. 214

東京海上日動リスクコンサルティング(株)
情報グループ
セイフティコンサルタント　植草宏和

情報システムを外部委託から見直す

１．はじめに

情報システムは、企業にとって欠くことのできない経営基盤に成長し、企業に与える利益とは裏腹にその停止や蓄積している機密情報の漏洩などにより、企業経営に重大な損失を与えるようになってきた。システム障害による取引業務の停止が市場混乱を招いた事故や不正アクセスにより約450万人分の個人情報漏洩を起こした事件など、情報システムに係る事故・事件はまだ記憶にあたらしい。このように情報システムは、企業にとってe-ビジネス上の有益な手段である一方その安全かつ安定的な運用・管理が重要な課題となってきている。その上高機能化、多様化が進む情報システムの運用・管理には、構成要素であるハードウェア、ソフトウェア、ネットワークに関する幅広い知識とノウハウが不可欠であり、自社内で関連する業務をすべて行うことは大企業でも難しいのが現状である。

ここでは、情報システムの安全かつ安定的な運用・管理の手段として、多くの企業がすでに実施している運用・管理業務の外部委託（アウトソーシング）に着目し、情報システムの運用・管理業務と外部委託との関係について整理し、今後の課題と対策について検討する。

以下、はじめに情報システムの現状を整理し、外部委託の観点から課題の抽出を行う。次に外部委託の範囲と情報システムの運用・管理業務との関係を整理し、今後の外部委託の方向を明確にする。なお、外部委託の範囲には、近年、情報漏洩に対して高いセキュリティがあるとして話題となっているシンクライアントシステム導入事例も検討に加えている。最後に情報システムの外部委託における課題整理から、今後企業において外部委託を進める上での対策の提案を行う。

２．情報システムの現状

情報システムの現状は、ホームページに公表されている調査結果を参考に以下の３点について整理した。

- 情報システムへの不正アクセスの発生状況と個人情報漏洩事故の傾向
- 情報システムのライフサイクルと運用・管理の現状
- 情報システムに関連する法、規格、ガイドライン等の推移

（１）情報システムへの不正アクセスの発生状況と個人情報漏洩事故の傾向

情報システムに対する不正アクセスの発生状況については、経済産業省が平成20年(2008年)2月に公表した「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況について」（参考資料１）の調査結果を基に、平成16年(2004年)から平成19年(2007年)の過去４年間の不正アクセス状況及び被害を受けたアクセス管理者の推移について整理した。結果を図１に示す。

なお、図では被害を受けたアクセス管理者としてプロバイダーと一般企業を対象とした。

図１より、被害を受けたアクセス管理者の件数は、平成19年ではプロバイダーが1,372件(75%)あり、一般企業の437件(24%)の３倍の件数となっている。

また、４年間の被害件数の推移では、プロバイダーの被害件数が平成17年に一般企業を逆転し、平成18年以降では年々倍増しているのに対し、一般企業の被害件数の増加率は平成18年が59%、平成19年が35%と年々減少している。このことから、不正アクセスの対象が年々プロバイダーへ移行する傾向にあると考えられる。このことから不正アクセスへの対応における課題としては、外部委託先における不正アクセス対策及びアクセス発生時の対処手順等の確認・評価が考えられる。

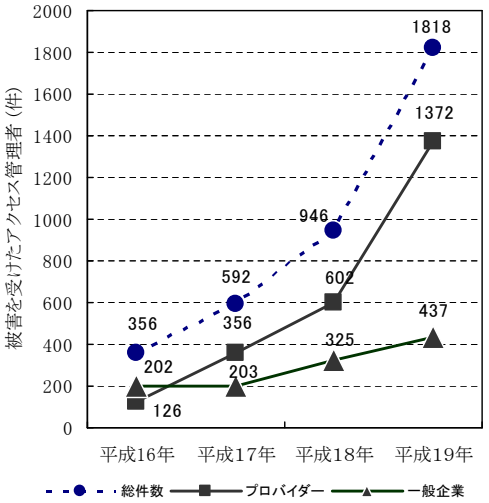


図１　被害を受けたアクセス管理者の推移

(出典：経済産業省「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況について」)

情報漏洩事故については、ニュースガイア㈱が情報セキュリティニュースサイト「Security NEXT」にて公表している個人情報漏洩事故一覧(参考資料2)の事故報告を基に、平成 20 年(2008 年)上半期に発生した原因が明確な事故 328 件を対象に、原因の所在が組織内か組織外(外部委託先など)かで集計・整理した。さらに、組織内に原因の所在がある事故276 件の内、従業員及び職員に起因する事故 156 件についてその原因を整理した。結果を図２、３に示す。なお、上記の個人情報漏洩事故件数は、漏洩形態がCD, USB など電子データによるもの以外に紙資料によるものも含んでいる。

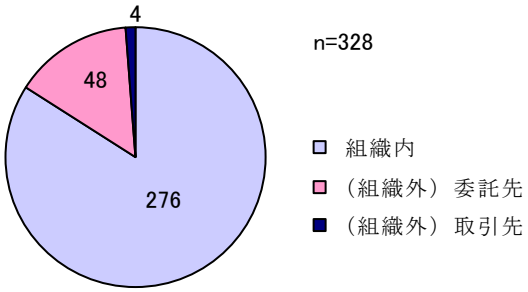


図２　個人情報漏洩事故件数
(組織内外別)
(出典：ニュースガイア㈱ 個人情報漏洩事故一覧を基に作成)

図２より漏洩原因の所在が組織内か組織外(外部委託先など)かによる整理では、外部委託先を含む組織外での情報漏洩が 48 件(約 15%)あり、外部委託先における情報管理の不備も情報漏洩事故を防止する上での課題であることがわかる。

図３より従業員、職員に起因する事故の整理では、漏洩事故156 件の原因として、情報の組織外への持出が 84 件(約 54%)で約半数を占め最も多く、次に誤配信、誤送付の情報取扱い担当者のミスが 50 件(約32%)の順となり、この２つの原因による個人情報漏洩事故は、全体の８割以上を占めている。

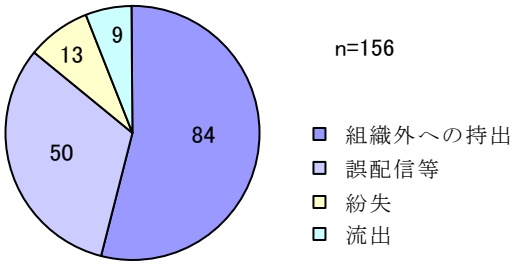


図３　個人情報漏洩事故件数
(従業員、職員に起因する事故)
(出典：ニュースガイア㈱ 個人情報漏洩事故一覧を基に作成)

このことから情報漏洩の防止における課題としては、従業員、職員による情報の組織外への持出しの防止と情報取扱い担当者の意識向上が考えられる。

以上より、情報システムへの不正アクセスの発生状況と個人情報漏洩事故の傾向からの課題としては、以下の点が挙げられる。

・外部委託先における不正アクセス対策及びアクセス発生時の対処手順等の確認・評価。
・外部委託先における情報管理の評価・監視。
・情報の組織外への持出しにおける管理策の見直し。
・情報取扱い担当者のコンプライアンス向上。

（２）情報システムのライフサイクルと運用･管理の現状

情報システムのライフサイクルについては、（社）日本情報システム・ユーザー協会が公表している第14回「企業IT動向調査2008」（参考資料３）に代表的な基幹業務システムのライフサイクル（図４）として報告されている。

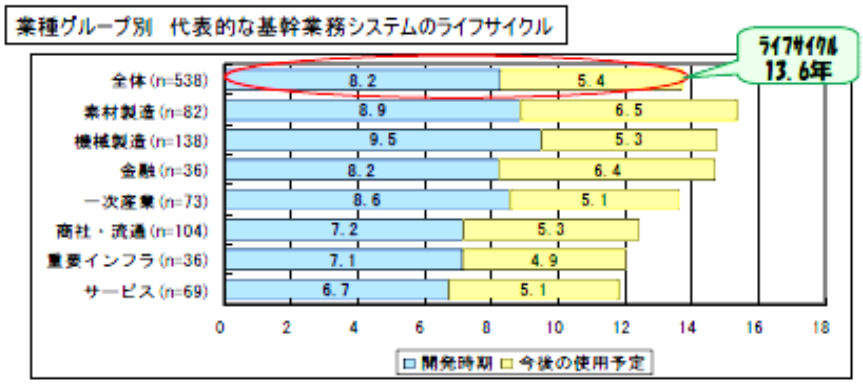


図４　業種グループ別 代表的な基幹業務システムのライフサイクル
（出典：（社）日本情報システム・ユーザー協会 第14回「企業IT動向調査2008」）

図４より、基幹業務システムに対し期待しているライフサイクル（導入から更改までの期間）の平均は13.6年と報告されており、企業が情報システムのライフサイクルに対してかなり長い期間を見込んでいることがわかる。

ここで、上記ライフサイクルの平均値（13.8年）を情報システムの各構成要素の減価償却期間（耐用年数）と対比してみた。 表１に国税庁が示している耐用年数の取扱通達（2-7-6の2）及び平成13年（2001年）度の耐用年数の改正における電子計算機の耐用年数の短縮を考慮して整理したLAN設備の耐用年数を示す。

表１から情報システムの主要な構成機器の耐用年数は、サーバを５年、端末機を６年、ソフトを５年としている。 耐用年数はあくまでも資産価値に関する指標であるが、装置の陳腐化（資産性の低下）による更改の目安と仮定すると、構成要素の耐用年数から情報システムのライフサイクルは５～６年で、企業が期待している情報システムのライフサイクルの平均値（13.8年）の約半分となり、過剰な期待感が伺えるとともにライフサイクルの見直しが必要と考える。 また、企業が期待するライフサイクルと耐用年数との隔たりについては、ハードは交換するが自社で開発した業務システムなどのアプリケーションソフトは永く利用したいとする企業姿勢の表れと考えられる。

表１ LAN設備の耐用年数

（耐用年数の取扱通達（2-7-6の2）及び平成13年（2001年）度の耐用年数の改正における電子計算機の耐用年数の短縮を考慮して作成）

個別の減価償却資産	耐用年数	主な「種類」「構造又は用途」「細目」
サーバ	５年	「器具備品」「事務機器及び通信機器」「その他のもの」
端末機	４年	「器具備品」「事務機器及び通信機器」「パーソナルコンピューター（サーバ用のものを除く）」
プリンター	５年	「器具備品」「事務機器及び通信機器」「その他の事務機器」
ネットワークオペレーションシステム、アプリケーションソフト	５年	「無形減価償却資産」「ソフトウェア」「その他のもの」
ハブ、ルーター、リピーター、ＬＡＮボード	１０年	「器具備品」「事務機器及び通信機器」「電話設備その他の通信機器」「その他のもの」
ツイストペアケーブル、同軸ケーブル	１８年	「建物附属設備」「主として金属製のもの」など
光ケーブル	１０年	「建物附属設備」「その他のもの」など

さらに、同報告では、ハードの保守停止やソフトのサポート打ち切りにより困った経験のある企業について報告（図５）されている。

図５より、「ソフト」のサポート打ち切りと「サーバ」の保守停止に困った経験があるとしている企業は、従業員の規模によらず50%以上となっており、特に従業員が1000人以上の大企業では70%を超えている。このことからも企業が望む情報システムのライフサイクルはその構成要素（ハード、ソフトなど）のライフサイクルとの間にギャップがあり、このギャップをいかにして埋めるかが情報システムの安定運用上の大きな課題と考えられる。

以上より情報システムのライフサイクルと運用・管理の現状からの課題としては、以下の点が挙げられる。

・ 情報システムの構成要素（ハード、ソフトのライフサイクル）は、企業が期待するシステムのライフサイクルの約半分程度であり、その隔たりの解消。

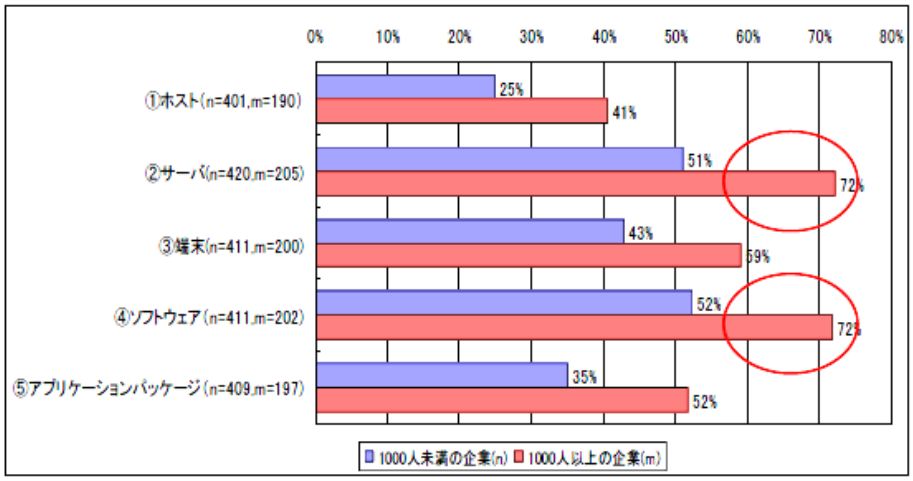


図５ ハードの保守停止やソフトのサポート打ち切りにより困った経験のある企業（企業規模別）

（出典：（社）日本情報システム・ユーザー協会が公表している第14回「企業IT動向調査2008」）

（３）情報システムに関連する法、規格、ガイドライン等の推移

情報システムに関する事故が、発生企業のみならずそのステークホルダ及び社会にも大きな影響を及ぼすことから、情報システムに対する法的要請も近年強まってきている。そこで情報システムに要求される要件がどのように推移してきているかについて、昭和 59 年(1984 年)から平成 20 年(2008 年)４月までの関連する主な法律、規格、ガイドライン等を時系列的に整理した。結果を表２に示す。

なお、表２では、各法律、規格、ガイドライン等の要求事項が、情報セキュリティ、個人情報保護、内部統制、SLA(サービスレベルアグリーメント)、事業継続の５つの分野のいずれ要件に該当するかを併せて示した。

表２ 情報システムに係る主な法律･規格･ガイドライン

情報システムに係る主な法律、規格、ガイドライン等			
昭和59年 (1984年)	12月	情報セキュリティ	【郵政省】 電気通信事業法
平成5年 (1993年)	5月	情報セキュリティ	【経済産業省】 不正競争防止法
平成11年 (1999年)	8月	情報セキュリティ	【総務省】 「不正アクセス行為の禁止等に関する法律」（不正アクセス禁止法）
平成14年 (2002年)	5月	情報セキュリティ	【総務省】 「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」 (プロバイダ責任制限法)
平成15年 (2003年)	3月	ＳＬＡ	【総務省】 「公共ITにおけるアウトソーシングに関するガイドライン」
	5月	個人情報保護	【内閣府】 「個人情報の保護に関する法律」
平成16年 (2004年)	3月	ＳＬＡ	【独立行政法人情報処理推進機構】 「情報システムに係る政府調達へのＳＬＡ導入ガイドライン」
	8月	個人情報保護	【総務省】 「電気通信事業における個人情報保護に関するガイドライン」
	10月	情報セキュリティ	【経済産業省】 新「システム監査基準」、「システム管理基準」
平成17年 (2005年)	3月	事業継続	【経済産業省】 「事業継続計画（BCP）策定ガイドライン」
	8月	事業継続	【内閣府】 「事業継続ガイドライン 第一版」
	12月	情報セキュリティ	【情報セキュリティ政策会議】 「政府機関の情報セキュリティ対策のための統一基準(全体版初版)」
平成18年 (2006年)	2月	事業継続	【中小企業庁】 中小企業ＢＣＰ（事業継続計画）策定運用指針
	3月	情報セキュリティ	【NISC】 「外部委託における情報セキュリティ対策実施規程策定手引書」
	4月	内部統制	【金融庁】 「金融機関等から業務の委託を受けた者に対する検査について」

平成18年 (2006年)	5月	情報セキュリティ	【(財)日本規格化協会】 JIS Q 27001:2006 「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」
		ＳＬＡ	【(財)日本情報処理開発協会(JIPDEC)】 「JIS Q 15001：2006 個人情報保護マネジメントシステム―要求事項」
		情報セキュリティ	【内閣官房情報セキュリティセンター(NISC)】 「外部委託における情報セキュリティ対策に関する評価手法の利用の手引」
		内部統制	【法務省】 「会社法」
	6月	内部統制	【金融庁】 「金融商品取引法」(制定)
	10月	ＳＬＡ	【(社)電子情報技術産業協会JEITA】 「民間向けＩＴシステムのSLAガイドライン第三版」
平成19年 (2007年)	2月	内部統制	【金融庁】 「財務報告に係る内部統制の評価及び監査に関する実施基準」
平成20年 (2008年)	4月	内部統制	【金融庁】 「金融商品取引法」(施行)

表２より、情報システムに対する法的要請の推移は、昭和59年（1984年）から平成16年（2004年）では情報セキュリティ分野、個人情報保護分野及びSLA分野における要件を規定する法律・ガイドライン類の制定が多く、平成17年（2005年）以降では、SLA分野、事業継続分野、内部統制分野における要件を規定する法律・ガイドライン類の制定へと推移している。外部委託の要件に直結するSLA分野においては、平成15年（2003年）３月の総務省による「公共ITにおけるアウトソーシングに関するガイドライン」の公表後、順次行政から民間企業へと対象が移行し、ガイドライン等の整備が行なわれてきている。

この情報システムに対する要件分野の推移は、企業のe-ビジネスへの事業拡大や地方自治体の電子政府の構築推進により情報システムの構築・導入が盛んに行なわれた情報システム成長期でのセキュリティ対策の強化から、情報システムが行政サービス及び企業経営の基盤となり、情報システム事故が個人情報の大量漏洩、業務停止など企業経営を左右し、社会問題を引き起こすような情報システム定着期での運用・管理の強化へと、情報システムに対する社会的要請が変化してきた表れと考えられる。

以上より、情報システムに関連する法、規格、ガイドライン等の推移からの課題としては、以下の点が挙げられる。

・ 情報システムの運用・管理におけるSLA分野、事業継続分野、内部統制分野の要請に対する対応強化。

３．　情報システムの外部委託の状況

（１）企業におけるインターネット利用状況と利用上の問題点

企業におけるインターネット利用状況に関しては、総務省が公表している「平成 18 年通信利用動向調査」（参考資料５）の調査結果において、個人、企業及び事業所のインターネット利用率(図６)及び企業におけるホームページ開設率(図７)が報告されている。

図６では、平成 18 年(2006 年)末時点において、企業におけるインターネット利用率は98.8%、また図７からホームページ開設率は87.2%となっており、ほとんどすべての企業がインターネットサービスプロバイダーを利用したインターネット接続を行ない、WWW サーバによ

http://www.tokiorisk.co.jp/

るホームページを開設していることがわかる。さらに、同調査では、企業における情報通信ネットワーク利用上の問題点（図８）が報告されている。

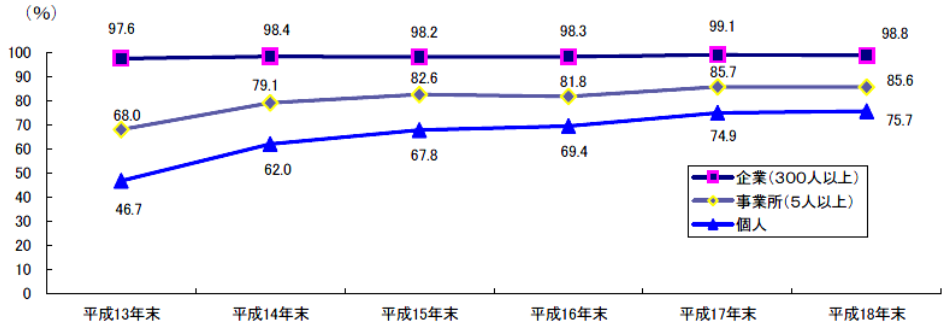


図６　インターネット利用率（個人、企業及び事業所）

（出典：総務省；「平成 18 年通信利用動向調査」）

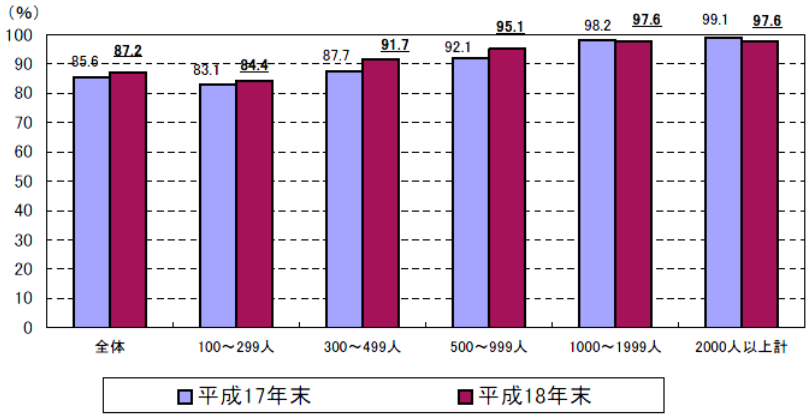


図７　ホームページの開設率（企業）

（出典：総務省；「平成 18 年通信利用動向調査」）

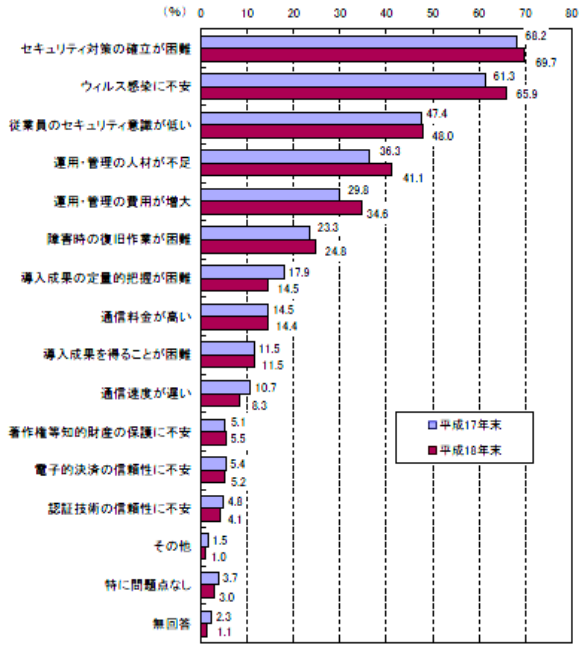


図８　ネットワーク利用上の問題点（企業）（複数回答）

（出典：総務省；「平成 18 年通信利用動向調査」）

図８では、企業通信網、インターネットなどの情報通信ネットワークの利用上の問題点として、「セキュリティ対策の確立が困難」が 69.7%と最も多く、次いで「ウィルス感染に不安」の 65.9%と続き、「セキュリティ関連」が上位を占め、前年度調査と同じ結果となっている。 また、「従業員のセキュリティ意識が低い」、「運用・管理の人材が不足」など、人材面の問題を挙げる企業も多数にのぼっている。特に、昨年と比べ、「ウィルス感染に不安」、「運用・管理の人材が不足」、「運用管理の費用が増大」が、いずれも４ポイント以上の増加を示している。

このことから、企業は、インターネットを利用する上でそのセキュリティ上の脅威への対策に不安を抱くとともに「運用・管理の人材が不足」と回答している企業の増加から、社内における情報システムの運用・管理に必要な知識、スキルが不足または不十分と判断している企業が増えていることがわかる。

以上より、企業におけるインターネット利用状況と利用上の問題点からの課題は、以下が挙げられる。

・情報システムの運用・管理における人材を含む知識・スキル不足の解消

（２）情報システムと外部委託範囲との関係

情報システムの運用・管理に必要とされる知識・技術は、今後もその高度化、複雑化が進むことは確実であり、企業における情報システムの運用・管理を行う人材の確保及び育成はさらに難しくなり、その結果として外部委託への依存が今以上に進むことが予想される。そこで以下では、情報システムの運用・管理における外部委託への依存度の高まりについて、委託範囲の拡がりと委託対象となる情報システムの主要な構成要素（ファイヤーウオール(FW)、サーバ、ソフトなど）とを対応させ、委託範囲と情報システムの運用・管理業務との関係について整理した。なお、整理では委託範囲と委託対象となる情報システムの構成要素との対応を５段階(STEP1からSTEP5)に区分し説明している。

図９にSTEP1からSTEP5の５段階の委託範囲と情報システムの構成要素との対応関係を示した。

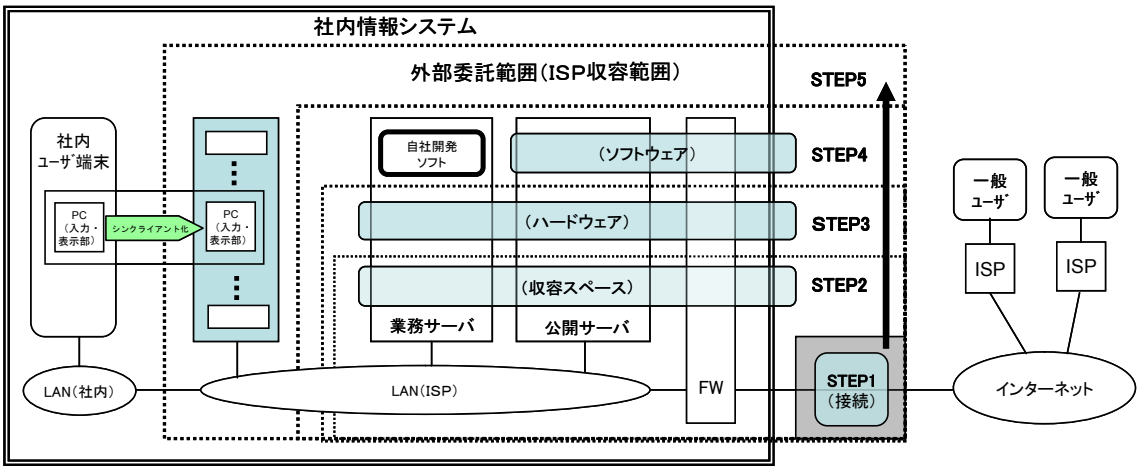
図では、各STEPの委託範囲を矩形領域として示し、STEP1からSTEP5へ移行による委託範囲の矩形領域の広がり（図中↑矢印方向）を情報システムの外部委託への依存度が高まりに対応させている。

また、表３にSTEP1からSTEP4の各委託範囲における概要とメリット・デメリットを示した。

なお、STEP5に関しては、シンクライアントシステム導入時の外部委託を事例として取り上げたことから、STEP1からSTEP4の検討（表３）の後に、シンクライアントシステム方式の説明及び概要とメリット・デメリットを表４、表５で整理している。

図９よりSTEP1からSTEP4へと外部委託が進み、委託範囲の矩形領域が拡がると、矩形領域内の委託対象である情報システムの構成要素は、社内から電源二重化対策、入退出管理対策の優れた外部委託先へと設置環境が移り、構成要素の物理セキュリティ対策が向上するとともに構成要素に対する保守業務の外部委託も併せて進むこととなる。 ただし、情報システムの構成要素の設置場所が自社から遠隔地の外部委託先へと移ることから、自社と外部委託先との間における通信回線切断のリスクが新たに課題として発生するが、情報システムの外部委託において同リスクは避けては通れない課題である。

さらに、STEP5のシンクライアント導入時では、社内ユーザ端末の本体部分(入力、表示部を除く)を外部委託することとなり、情報システムにおけるセキュリティ対策は社内利用者に対する対策へ集約され、運用・管理業務は主に外部委託先との調整及び管理へと移行することになる。



LAN:ローカルエリアネットワーク、FW:ファイアーウオール、ISP:インターネットサービスプロバイダー

公開サーバ ： WWWサーバ、メールサーバ、FTPサーバ等

業務サーバ ： ファイルサーバ、データベースサーバ等

図９ 情報システム構成要素と外部委託範囲

表３ STEP1 から STEP4 の各委託範囲における概要と主なメリット･デメリット

委託範囲	概　要	主なメリット・デメリット
STEP1	■インターネット接続機能の借用 通信回線によりプロバイダーがインターネット接続しているＧＷ(ゲートウェイ)装置と社内ＬＡＮと接続し、ＧＷを介してインターネットと接続する。 (個人ユーザが、ＡＤＳＬなどの通信回線でプロバイダと接続し、インターネット利用する場合と同じ。但し、企業の場合は、通信速度の早い専用線等で接続するのが一般的。)	【メリット】 ・インターネット上で様々なサービスの利用が可能。 【デメリット】 ・インターネット接続に伴う不正アクセス、侵入ウィルス等へのセキュリティ上の脅威への対策が必要。
STEP2	■サーバなどの設置環境の借用 耐震性のあるビル内の制震性ラック、二重化電源等のプロバイダーの機器設置環境を借用し、自社サーバ等を設置し、その物理セキュリティを確保する。 (大企業においても、災害時の事業継続の観点からこのサービスを利用する傾向。)	【メリット】 ・地震・火災等の災害から情報システムの主要装置を守ることが可能となる。 ・入退出管理の厳格なサーバルームに主要な装置が設置されることからその物理的なセキュリティが確保される。 【デメリット】 ・設置場所が遠隔地となり、保守作業に時間を要する。
STEP3	■サーバ(ハードウェア)のレンタル・リース プロバイダーからサーバ機器(ハードウェア)をレンタル/リースし、自社サーバとして運用する。 (サーバOS上で動作するアプリケーションソフトウェア(自社で開発した業務管理ソフトなど)のインストール、設定等は自社で実施する。)	【メリット】 ・ハードウェアの設備投資、更改経費の削減。 ・代替機、在庫部品交換などによる障害時の早期復旧。 【デメリット】 ・障害発生時におけるハード側(プロバイダ)、ソフト側(利用企業)切り分け作業の分担、責任範囲の明確化が難しい。
STEP4	■サーバ機能のレンタル・維持管理 プロバイダが構築、動作検証を済ませ、プロバイダ環境に設置されているサーバ(WWW、メール、FTPなど)をレンタルし、自社サーバとして運用する。 (業務支援ソフトウェアなど自社開発ソフトウェアは含まれないのが一般的。)	【メリット】 ・情報システムの運用・管理・保守稼動(障害監視、障害対応、OSへのパッチ作業等)の削減。 ・セキュリティ対策も社内ユーザ対応部分(パスワード管理、ウィルス対策など)となる。 【デメリット】 ・情報システムの運用・管理・保守スキルの低下。

表３より STEP1 から STEP4 へ委託範囲が拡がることにより、情報システムの運用・管理業務は外部依託先の専門家へと移行し、社内の業務軽減が図られ、情報システムの運用経費は削減される。

その反面、情報システムの運用・管理に関する社内の知識･スキルは低下し、自社情報システムの評価、改善等に関する適切性判断が自社でできない状況が企業内に生じる恐れがある。このこと

から、外部委託範囲を広げることは、情報システムの物理的なセキュリティの確保、外部脅威からの保護、運用・管理業務の軽減及び経費削減、保守の迅速化等様々なメリットを企業にもたらす手段となるが、運用・管理に係る人材不足、知識・スキルの低下による委託先管理能力の低下という課題を内包していることに注意が必要となる。 以上、STEP1 から STEP4 の４段階の外部委託と情報システムにおける運用・管理業務の軽減及び物理セキュリティの確保との関係について述べた。

以下ではシンクライアントシステム導入時の委託範囲区分としたSTEP5について外部委託との関係を整理する。まず、ここで取り上げるブレードＰＣ方式について簡単に説明する。シンクライアントシステムの方式は、画面転送方式とネットワークブート方式に大別され、画面転送方式は実装方法によりさらに３つに区別され整理される。表４に結果を示す。

表４ シンクライアントシステムの方式

方式分類		使用形態
画面転送方式	サーバベースド・コンピューティング方式	サーバのアプリケーションソフトを複数のクライアントで共有して使用する。
	仮想化ＰＣ方式	サーバに仮想化ソフトウェアをインストールし、サーバ上に複数の仮想ＰＣを構成し、各クライアントは仮想ＰＣの一つを使用する。
	ブレードＰＣ方式	ＰＣを演算処理部、記憶部（ブレードＰＣ）と入出力部（シンクライアント）に物理的に分離し、複数のブレードＰＣを機器集約し、各クライアントはシンクライアントから遠隔でブレードＰＣを使用する。
ネットワークブート方式		ＰＣ起動時毎に、ディスクレスのクライアントＰＣにネットワーク経由でＯＳとアプリケーションをダウンロードして使用する。

表４よりシンクライアントシステムの４つの方式は、方式ごとに使用形態が異なり、どの方式を導入するかにより外部委託の内容や形態が異なってくる。STEP5では、シンクライアント導入時の社内ユーザ端末の物理構成と機密情報漏洩との関係が理解し易いようにシンクライアントシステムの導入例としてブレードPC方式を取り上げている。

図10にブレードPC方式によるシンクライアントシステム導入時における外部委託範囲（STEP5）を示す。図ではブレードPC方式での社内ユーザ端末における物理構成の変化、情報の漏洩部分の社内から外部委託先へ移行及び取扱い情報（画像情報）の流れについて示した。

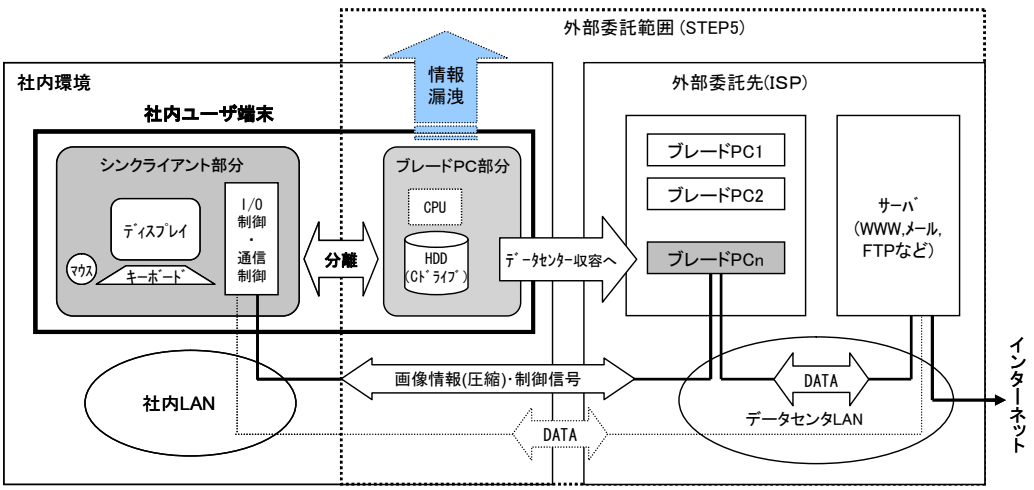


図 10 シンクライアントシステム導入時における外部委託範囲(STEP5)

図10よりブレードPC方式では、ユーザ端末の本体部分である演算処理部(CPU等)、記憶部(HDD)、外部媒体（CD、USB等）用のドライブ及びポート部と表示部(ディスプレイ)及び入力部(マウス、キーボード)が分離され、本体部分は遠隔地の外部委託先環境(データセンタなど)に物理的に集約・収容されることとなる。そのため社内ユーザは、ネットワークとの接続機能、ネットワークを介して送受信される画像情報の処理機能及び入出力機能(マウス、キーボード、ディスプレイ)だけのクライアント部分を使用することなり、情報の取扱いはディスプレイの画面表示だけとなり、外部媒体への出力はできない状態となる。

表５に STEP5 の各委託範囲における概要と主なメリット･デメリットを示した。

表５ STEP5 の各委託範囲における概要と主なメリット･デメリット

委託範囲	委託概要	主なメリット・デメリット
STEP5	■ブレードＰＣレンタル・維持管理 プロバイダが、構築、動作検証を済ませ、プロバイダ環境に設置されているブレードＰＣ（演算部、記憶部）をレンタルし、社内クライアントＰＣ（入出力部）から遠隔でブレードＰＣを使用する。	【メリット】 ・重要情報の物理的セキュリティの確保。 ・社内ユーザ端末(クライアント端末）に情報の保存・出力機能はなく、従業員による社外への情報持出しがない。 【デメリット】 ・現状使用端末のシンクライアントシステムへの移行に伴う更改コストが発生する。

表５よりシンクライアントシステム(ブレードPC方式)導入時の外部委託では、現在の社内ユーザ端末をシンクライアントへ変更するための導入コストが必要となるが、情報システムの運用･管理の観点からは、セキュリティ対策を社内ユーザ対策に絞ることができ、運用･管理業務はパスワード管理、表示管理などへ大幅に軽減される。 さらに、情報漏洩の観点からは、取扱い情報はすべて入退出管理の確保された遠隔地の外部委託先に存在し、社内ユーザはその情報をディスプレイで表示する使用形態となることから、社内ユーザの情報出力による外部情報漏洩を防止することが可能となる。

このようにシンクライアントシステム(ブレードPC方式)導入による外部委託は、情報システムの運用・管理及びセキュリティ上で大きなメリットを期待できるが、その一方で運用・管理業務の外部委託先への大幅な依存が、業務実施に必要な情報システムに関する社内担当者の知識・スキルのレベル低下を招き、ひいては外部委託先の専門家からの説明内容も社内担当者が正確に理解できないような人材の空洞化が企業で顕在化するものと考えられる。

このためシステム更改のコストを除くと、STEP5 における情報システムの運用･管理上での課題は、STEP1～STEP4 と同様に社内における知識･スキルの低下にともなう委託先管理能力の低下への対策と考えられる。

以上より、情報システムと外部委託範囲との関係からの課題としては、以下の点が挙げられる。

・企業と外部委託先を接続する通信回線切断リスクへの対策。
・情報システムの運用･管理に関する知識･スキルの低下にともなう委託先管理能力の低下への対策

（３）まとめ

以上、各章での情報システムの運用・管理の外部委託における課題を表６に整理した。

表６より、企業において外部委託を進める上での課題としては、外部委託先の情報管理（委託先従業員のコンプライアンス向上を含む）の点検・監視体制の確立ならびに外部委託先管理を実施するのに十分な社内における知識・スキルの確保に集約されると考えられる。

表６ 情報システムの運用・管理の外部委託における課題

■情報セキュリティ上での課題
・外部委託先における不正アクセス対策及びアクセス発生時の対処手順等の確認・評価。 ・外部委託先における情報管理の評価・監視。 ・情報の組織外への持出しにおける管理策の見直し。 ・情報取扱い担当者のコンプライアンス向上。
■情報システムのライフサイクル上での課題
・情報システムの構成要素であるハード、ソフトのライフサイクルは、企業が期待するシステムのライフサイクルの約半分であり、その隔たりの解消。
■情報システムに要求される要件上での課題
・情報システムの運用・管理におけるSLA分野、事業継続分野、内部統制分野の要請に対する対応強化。
■インターネット利用上での課題
・情報システムの運用･管理における人材、知識･スキル不足の解消。
■外部委託範囲の拡大による課題
・企業と外部委託先を接続する通信回線切断リスクへの対策。 ・情報システムの運用･管理に関するに知識･スキルの低下にともなう委託先管理能力の低下への対策。

この課題への対策として、ここでは外部委託先への第三者による監査の定期的実施を提案する。

具体的には、情報システムに関する専門的知識を有する第三者に外部委託先への監査を依頼し、外部委託先の監査結果にある改善提案に添って自社の外部委託先管理における委託先選定基準、管理方法等について見直しを行うことである。なお、第三者による現状分析においては、2.3にて取上げた情報システムに対する５つの分野(情報セキュリティ、個人情報保護、SLA、事業継続、内部統制)における要求条件について、社内経営戦略に照らし適宜選択・重点化して、分析の観点に盛込み、法的準拠性に対する確認を併せて行うこととする。

さらに、提案における監査を定期的に実施することで自社の外部依託先管理の適切性が確認されるとともに情報システムの専門家との監査対応を通して、社内における委託先管理のスキル向上、人材育成にもつながることが期待される。

４．終わりに

情報システムの運用・管理は、システムの高度化、複雑化、多様化が進んでいる状況下において、その業務のすべてを自社の情報システム要員で処理することは技術的にもコスト的にも難しく、企業にとって情報システムの外部委託は避けられないのが現状である。さらに今後、シンクライアント方式への拡張などにより外部委託範囲が拡大し、外部委託先への依存度が高まると想定すれば、情報システムの外部委託先選定・管理が情報システムの安定運用の要であり、その見直しが最大の課題であることを多くの企業が再認識する必要があると考える。ここでの外部委託先への第三者監査の提案により、多くの企業において定期的な監査が実践され、外部委託先企業の業務品質及び信頼性が向上し、ひいては企業の情報システムの安定的かつ経済的な運用･管理が達成されることを期待している。

（第214号　2008年12月発行）

http://www.tokiorisk.co.jp/

参考資料

１．経済産業省：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況について（平成20年(2008年)2月29日公表）
http://www.meti.go.jp/press/20080229010/02_husei_a.pdf

２．ニュースガイア(株)：個人情報漏洩事故一覧(情報セキュリティニュースサイト「Security NEXT」にて公表)
http://www.security-next.com/cat_cat25.html

３．（社）日本情報システム・ユーザー協会：第 14 回「企業 IT 動向調査 2008」
http://www.juas.or.jp/project/survey/it08/

４．国税庁：LAN 設備の耐用年数の取扱いに関する質疑応答
http://www.nta.go.jp/shiraberu/zeiho-kaishaku/joho-zeikaishaku/hojin/020215/01.htm

５．総務省：「平成 18 年通信利用動向調査」
http://www.soumu.go.jp/s-news/2007/pdf/070525_1_bt.pdf