個人・企業情報保護対策への取組み

日本電信電話㈱
第三部門　プロデュース担当
主幹研究員　舘 剛司

企業・組織を取り巻く環境

2005年4月に施行された個人情報保護法、2006年5月に施行された会社法、2006年6月に成立した金融商品取引法（日本版SOX法）など、法制度面から、企業・組織における情報の取扱いに対して、より厳格なルールや運用が求められている。特に会社法や日本版SOX法では、企業自身や取引先に対して、財務報告の信頼性、関連法規の順守、業務の有効性・効率性など、いわゆる内部統制の強化を求めている。

このような状況を受け、情報セキュリティの分野でも特に、部内者の不正行為や過失により発生する個人情報・機密情報の漏洩・改ざん・破壊、などに対する対策の必要性が改めて認識されている。

また、人的リスク要因に加え、システム障害や災害・事故など不慮の事態にどう対処するか、いわゆるBCM（Business Continuity Management：事業継続管理）という観点も、併せて注目されている。特に近年、経済活動が益々グローバルな規模になっていることと、ICTへの依存度が高まっていることとが相まって、一つのシステム障害や自然災害が、想像以上に企業活動に影響を及ぼす事故が多発している。

そこで今回は、図1の右半分の領域（部内者による不正行為・過失、システム障害など）、および左下の領域（災害・事故など）に着目し、情報セキュリティ管理の課題とその対策技術の動向について紹介する。

部内者の不正行為・過失に対する情報セキュリティ対策技術

(1)　ファイル管理・デスクトップ管理・コンテンツフィルタ技術

そもそも情報へのアクセス権限を持つ部内者による不正操作や過失に対して、システムだけで完全に防御することは難しい。システム部門が設計・運用する基幹系業務システムのような環境では、情報セキュリティ対策も比較的徹底しやすいが、近年のPC端末やオープン系システムの普及に伴って拡大してきたEUC（End User Computing）環境では、個々の従業員が扱う情報量や操作の自由度が飛躍的に増大し、内部統制を行き渡らせることが難しくなっている。そのようなEUC環境でも、対処療法として「一部の操作を禁止制御する方法」を採用する企業が増えている。

例えば、ファイル管理システムにより、サーバ上の特定ディレクトリや特定ファイルの閲覧・出力などを制限できる。また、デスクトップ管理システムにより、端末へのアプリケーションインストールやセキュリティ設定変更などを禁止できる。

さらに、誤って機密情報をメール添付して社外へ送ってしまったり、社員が就業時間中に業務上必要のないWebにアクセスしたり、といった行為も日常的に起こりがちである。これらを禁止・制御するために、メールフィルタ製品やURLフィルタ製品などのコンテンツフィルタ技術が有効だ。

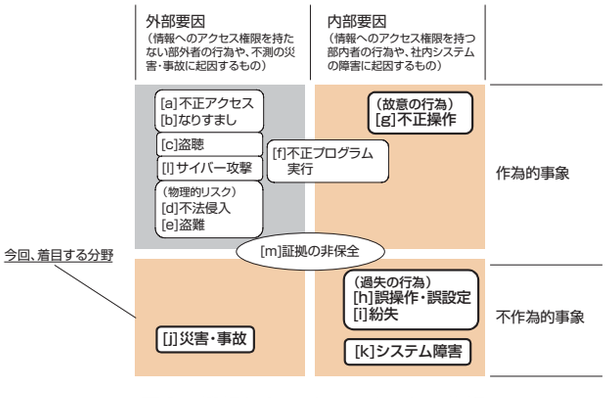

図1　情報セキュリティリスクの分類

これらの対策は、ルールに則って操作を一律禁止してしまうため、営業窓口業務やコールセンターなど、業務範囲をもともと明確に規定・制限している環境には導入しやすい。しかし、企画部門や営業部門など、比較的業務の自由度が高い職場に導入しようとすると、かえって生産性を著しく下げるばかりか、場合によってはシステムの抜け道探し（アカウントの貸し借りなど）を助長することにもなりかねない。導入に際して、まずは現場の実態把握・影響度の評価が重要である。

(2) 操作監視・ログ監視技術

前述のような業務の自由度が高い職場では、「行為を監視して警告を発する方法」を併せて導入するケースも多い。従業員によるファイルアクセスやWeb閲覧の証跡を残して、定期的に上長にレポートしたり、セキュリティポリシーに違反する行為があると、即座に本人や上長にアラームをあげたりすることが、従業員のコンプライアンス意識を高め、不正操作や過失を未然に防止するために有効だ。

また最近では、システム上に記録が残りにくいため、紙媒体や持出し記録媒体などによる情報漏洩も問題になっている。これもやはり行為そのものを一律禁止できないケースも多いので、プリンタ出力や記録媒体への出力ログ、部屋への入退室ログなどを改ざんできない形で保存することが、万が一事故が発生した場合の漏洩内容や漏洩ルートの特定にも役に立つ。

図2に、職場環境のモデルと操作監視・ログ監視技術の必要度を示す。特に「システム管理エリア」のように、ルート権限でシステムへアクセスできるような環境では、監視技術を駆使した厳格な運用が求められる。

ただし、設定ポリシーによっては、アラームがあまりにも頻繁にあがったり、膨大なログレポートを上長がチェックしきれない、といった運用上の課題も指摘されている。より精度よく、少ない手間で監視するための運用面・技術面での工夫が求められている。一方で、ソリューションの導入に際しては、まずは各業務フロー上で、不正操作・誤操作が発生するリスクを徹底的に洗い出し、必要に応じて業務フローの見直しを行った上で、的確な監視ポリシーをシステム上に設定する必要がある。つまり、効率的な社内チェックの仕組みを再構築することが、結果的にIT投資を無駄にしないことにつながる。

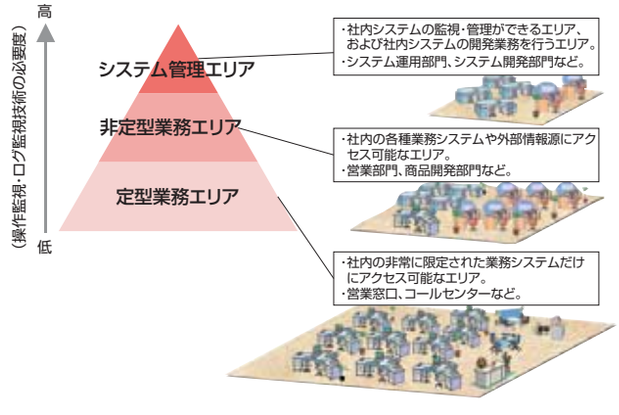

図2　職場環境モデル

(3) アカウント管理技術

従業員によるアカウントの貸し借りや、部外者によるなりすましを防止するために、ユーザー認証として生体認証を採用する企業が増えている。指紋認証や静脈認証など各種方式が提供されており、比較的高価ながら、導入効果が見た目にわかりやすいこともあり、市場は急拡大しつつある。

一方で、ばらばらに導入・運用された各種業務システムをまたがって、いかにアカウント管理を一元化・効率化（ユーザーおよびシステム管理者の観点で）するか、が大きな課題だ。人事異動や組織整備のたびにシステム上でのアカウント登録・変更が必要になるため、誤設定や削除漏れのリスクも増えている。そこで、シングルサインオンシステムを導入することで、ユーザー側でのアカウント管理を容易にするとともに、システム管理者側でもシステム毎のアカウント管理ポリシーを統一できるため、人為的ミスを減らすことができる。

さらに最近では、企業・組織が内部統制を見直す中で、もっと根の深い問題も指摘されている。例えば、同じような業務プロセスに対して、支店毎に業務フローや決裁ルートが違っていたり、取引先や連結決算対象子会社との間で勘定科

目が違っていたり、といったケースは散見される。つまり、必要以上に複雑な業務システム・業務フロー、それに伴う煩雑な決裁ルートやアカウント管理を余儀なくされているのである。このような環境にアカウント管理ソリューションを導入しても、結局、複雑な運用や継続的なカスタマイズが必要である。内部統制を強化する過程で、このような業務プロセスやシステム投資の非効率を見直す活動、いわゆるBPR（Business Process Reengineering）の必要性が叫ばれているが、その中でアカウント管理ソリューションを適用した業務フロー再構築のニーズが高まっている。

(4) 業務アウトプット管理技術

先に述べたEUC（End User Computing）環境で、特に日本版SOX法対応上の課題となるのが、市販の表計算ソフト（パッケージ製品）などを業務に利用して、財務管理業務の一部を実施したりするケースだ。例えば、財務部門で子会社毎の財務管理システムのアウトプットをもとに連結決算を行ったり、営業部門で個々のシステムで収集した販売情報をもとに売上げ計上を行ったり、といったシーンは多くの会社で日常的に見られる。しかし、既存の業務システムがいくら完璧に運用管理されていても、従業員の人手による作業が介在するため、数字の改ざんやパラメータ誤設定による計算ミス、情報漏洩などが発生するリスクが残る。

そこで、帳票管理システムやEAI（Enterprise Application Integration）ツールにより、個別の業務システムからのアウトプットを規定された様式の電子帳票へ自動変換したり、同帳票へのアクセスを管理することが、すでにIT導入率が高い大手企業でも必要とされている。

また表計算ソフトに関しては、従業員が各自で計算ロジックを操作できてしまうため、システムの正当性を証明することも難しくなる。内容の変更管理や計算ロジックの検査などの統制を実現するためには、パッケージ製品を採用しても、その初期設定や管理者権限を一部のメンバーだけに限定するなど、運用上の対処も必要である。

BCM（事業継続管理）のための情報セキュリティ対策技術

(1) システム統合運用管理技術

例えば、デスクトップ管理システムによる端末操作ログ監視や、URLフィルタによるWebアクセスログ監視などのセキュリティ対策を個別に導入・運用した企業でも、日々膨大なログ出力があがるだけで、従業員による一連の操作ログとして、効率的に不正操作や過失を監視・制御できていないケースは多い。それどころか、場合によっては、個々の対策システムの運用管理やログ分析に追われ、不測の事態やインシデント発生時に的確な判断・対処を行えず、止むを得ずシステム停止や業務停止などの非常手段を取らざるをえないことさえある。

そこで、セキュリティ対策を個々に独立して運用するのではなく、企業・組織としての統一したセキュリティポリシーのもと、複数のシステム・対策にまたがった一連の運用プロセスとして再定義することが有効だ。それによって、セキュリティ管理や手間のかかる防御対策を、ある程度自動化し、セキュリティ対策全体の安定運用を実現することができる。

このようなシステム統合運用管理の実現は、企業・組織におけるICTガバナンスを実現するためのキーである。つまり、サーバやネットワーク、ストレージなど、業務システムを構成する個々の装置レベルでの「システム監視」を一元化・集約化するだけでなく、OSメンテナンスやバックアップ、プロビジョニングなどの「システム運用」を一元化・省力化することが重要なのである。

システム統合運用管理ツールは、もともとは肥大化するシステム運用稼働の削減を目的に提供されてきたが、最近では、企業・組織の情報セキュリティ管理や内部統制を支援しつつ、安定したシステム運用を通して事業継続性を高めるための手段としても注目されている。

(2) データ・ストレージ管理技術

日本版SOX法やe-文書法への対応に伴い、取引記録やシステムへのアクセスログ、電子メールなどを一定期間、電子的に保管する用途が急増している。これに伴い、企業が蓄積・管理すべきデータ量は増大の一途をたどっている。特に、電子メー

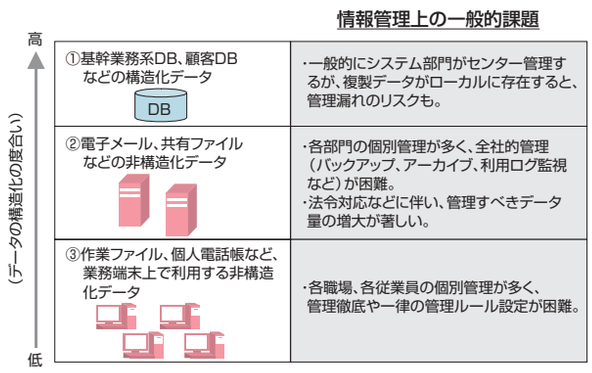

図３　企業・組織において管理すべき情報資産と課題

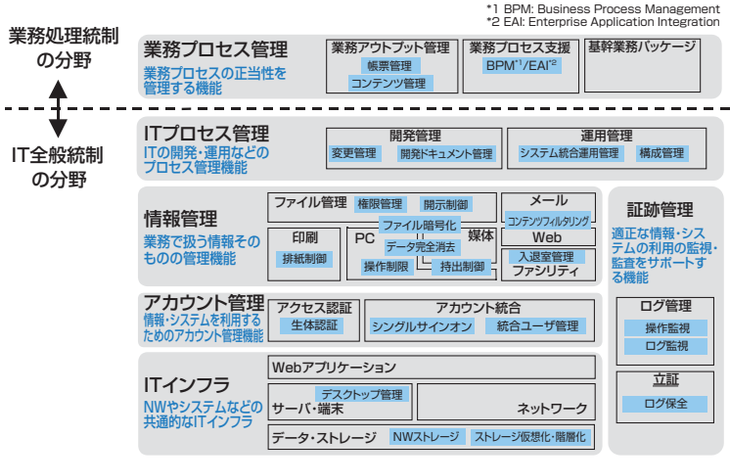

図４　内部統制の観点で注目される情報セキュリティ対策技術

ルや各職場で設置・管理されている共有ファイルサーバ上のデータなど、いわゆる非構造化データの容量増大が近年著しい。ところが、顧客データベースや経理データベースなど、基幹業務系システムで扱う、いわゆる構造化データに比べ、非構造化データでは管理のためのシステムや体制が不十分なことが多く、ICTガバナンスの観点で大きな課題である（図３参照）。

このような背景を受け、データ・ストレージ管理技術には大きく２つの動向がある。第一は、サーバや端末の周辺機器としてのストレージ（DAS: Direct Attached Storage）から、より信頼性・拡張性に優れたSAN（Storage Area Network）やNAS（Network Attached Storage）などのネットワークストレージへの移行である。ネットワークストレージとして集中管理することにより、スケジューラによる定期的なバックアップや、一度書き込まれた内容の変更禁止制御（WORM: Write Once, Read Many）、ディスクアクセスログ管理など、内部統制に必要な機能・運用が実現しやすくなる。

第二は、いわゆるILM（Information Lifecycle Management）を実現するストレージの仮想化技術や階層化技術である。ストレージの仮想化により、システム稼働中でもディスク容量を増やしたり、物理的に分かれたストレージ領域を結合して、必要な容量を確保したり、といった運用が可能となる。ストレージの階層化とは、頻繁にアクセスやデータ更新を行うデータには高速・高性能のディスクを、利用頻度が低くなったデータにはアーカイブ用の低速・低コストのデバイス（磁気テープなど）を、それぞれ割り当てることで、ストレージ管理を効率化することである。

これらの技術はいずれも、ストレージシステムの可用性・耐障害性を高めることで、システム障害や自然災害など不測の事態に備え、事業継続性に貢献するものとして、益々ニーズが高まっている。

まとめ

図４に、今回紹介した主に内部統制の観点での情報セキュリティ管理技術を、大きく５つの分野に分けて示す。

これらの技術・ソリューションは、最近の企業・組織における法令順守を重視する風潮を受けて、特に注目が集まっている分野である。しかし、文中でも述べたとおり、いずれも業務プロセスに深く関わる対策技術であるがゆえに、社内業務への影響をしっかり見極めたうえで導入することが重要である。

さらに、前号で紹介した「外部からの脅威に対するセキュリティ技術」と補完しあう対策であることを念頭におき、社内システムの見直しに際しては、基本的なセキュリティ対策が漏れなく導入・運用されているか、そのための体制ができているか、のチェックも併せて必要であることはいうまでもない。