「認証／証跡」管理と個人情報保護対策

2005年４月全面施行の個人情報保護法に合わせ、各企業ともセキュリティ対策を推進している。しかし、セキュリティ対策はITの進歩とともに継続的に行われなくてはならないものである。本稿では、システム運用の観点から、情報漏えいリスクを軽減するための重要な手段である「認証管理」と「証跡管理」について考察していく。

高まる情報リスク管理の重要性

2004年春以降、企業の個人情報漏えいにまつわる不祥事が相次いで発覚し、社内の機密情報である個人情報の社外流出に対する危機意識は非常に高まっている。2005年４月１日、個人情報保護法が全面施行されることもあり、各企業ともその対策に全力を注いでいる。

このように、2004年は「情報セキュリティ対策≒個人情報保護法対策」としての側面が強くクローズアップされることとなった。しかし、これは単なるコンプライアンス（法令順守）だけの問題では済まされない。たしかに、法律上の罰則を受けることは企業にとって大きな汚点ではあるが、個人情報漏えいは、それ以上に回復困難な信用失墜につながる危険性がある。こうした点において、情報リスク管理は、企業のリスク管理のなかで非常に重要な地位を占めるようになってきている。

企業がリスク管理を行うことの重要性はあらためて論じるまでもないが、ここ10年で起きたリスク管理の質的変化はしっかり認識しておく必要がある。すなわち、ITの進歩・普及、マーケット（お客様）の変化は「失われた10年」と対極に位置する大きなものであり、リスク管理の質を大きく変えることになった。

(1) 消費者の嗜好の変化

同一同種の製品、サービスに満足していた消費者が、他人とは異なる製品、サービスを求める「個人志向」が強まった結果、そのニーズに対応できるよう、企業はマーケティング力を高めることが必要となった。これにともない、「顧客情報（個人情報）」の充実、蓄積が行われるようになり、購買状況や趣味情報などの個人情報を分析する情報系システムが広く利用されることとなった。マーケティング機能が求められることにより、個人情報は過去とは比べものにならないほど、資産価値が高まったのである。

(2) システム基盤の変化

これと同時進行で、システム開発期間の短縮、コストダウンが求められ、従来の大型汎用コンピュータからクライアントサーバーシステムへと、システム環境が大きく変わりはじめた。この環境変化により、特殊端末で行われた業務が汎用端末（PC）にも解放され、集中管理していたデータ（情報）もさまざま

NRIデータサービス
基盤サービス事業本部
基盤サービス技術室
上級システムエンジニア
孕石幸弘（はらみいしゆきひろ）
専門は運用セキュリティ

なシステムで分散利用されるようになった。かくしてデータ（情報）の拡散が始まった。

(3) PC（Windowsマシン）の普及

クライアントサーバーシステムという分散したシステム環境への移行に合わせ、PC（Windows）の企業導入が進んだ。いまや企業においては、従業員１人にPC１台が当たり前となっている。さらにディスクの大容量化、データ書き込み装置（CD-R、USB対応メモリーなど）の利便性向上により、PCから大量のデータ（情報）を簡単に保存、持ち出しできるようになった。

(4) ユビキタスネットワークの始まり

社会全体にインターネットが普及したことにより、消費者はインターネット経由で企業サービスを利用できるようになり、従業員は社内でのみ利用していた社内システムに社外からアクセスして業務ができるようになった。電子メールやWebは、情報交換を簡便に行える環境を提供しており、「いつでも、誰でも、どこからでもネットワークを利用できる」ユビキタスネットワークの先駆けとなった。

個人情報の特徴

こうした社会の変化により、「個人情報」は企業の「機密情報」の一部であり、高い価値を有するものであるにもかかわらず、日々リスクにさらされていることがわかる。すなわち、業務システムは一般社員、派遣社員、パートナーといった広範な人間に利用されており、容易に持ち出し、交換がなされ得る状況にあるわけである（表１参照）。

表１　個人情報の特性

対象	顧客情報、社員情報の基本属性、取引情報、人事情報など
利用者	一般社員、パートナー、契約社員など
利用形態	利用に合わせて任意の加工ができる
利用範囲	社内一般部署（社外への持ち出しのケースもある）
漏えい時の影響範囲	信用の失墜を招き、対策のコミットを迫られる ⇒対策範囲の拡大、長期化のおそれ

こうした過大なリスクを抱えながら、業務は日々行われているのであり、業務開始のための「PCの立ち上げ」と「社内ネットワークへの接続」が、情報漏えいリスクの始まりとなっていることを認識する必要がある。

このように、人的なインタフェースの部分で情報漏えいリスクが発生している以上、システム的にいかなる対策を講じようとも、100％問題が解決することはあり得ない。しかし、逆の見方をするならば、いかなるシステムであれ、情報の出入口の適正な管理がリスク軽減につながる。すなわち、利用者がPCを通じて情報にアクセスすることを、いかに制御するかがセキュリティ確保のポイントとなるのである。

漏えいリスクの事前／事後対策を徹底する

個人情報漏えいに関して、情報の出入口の適正な管理をシステム側に当てはめると、「ど

んな個人情報が、どこのシステムに、誰が利用できる状態にあるのか」を把握しておくことが、最低限必要であるということになる。そしてこれを基に、利用端末側の適正な管理を考えていく。すなわち「認証管理」と「証跡管理」を見直すことにより、今後何をすべきかの方向性が明確になる。ちなみに、「認証管理」は漏えいリスクの事前対策であり、「証跡管理」は漏えいリスクの事後対策である。

すでに対策すべき課題が明確であるという企業は、その脆弱性の対策を行っていけばよい。しかし、まだ課題が明確ではないというのであれば、「出入口を固める」ことが非常に重要であり、かつ有効となる。

「認証管理」は、システムを利用するためのPC、ネットワークの使用許可と利用レベルを管理するものである。具体的には、ユーザーID・パスワードと利用権限を管理することである。きわめて基本的な対策ではあるが、これまで発生した事件の多くは、ユーザーID・パスワードの適正な管理が行われていれば、回避されたものも少なくない。そして現実の運用においては、適正な管理がなされていないケースがままみられる。

というのは、利用システムが多くなれば、1人の利用者に与えられるユーザーID・パスワードはこれに比例して多くなる。そして、すべて覚えきれないID・パスワードがメモとしてPCに貼付されたりする。また、利用者の数が多くなれば、人事異動にともなう利用権限変更・退職者のユーザーID抹消が迅速に処理されない企業も出てきてしまう。こうした状況では、いかなるセキュリティ対策の仕組みを作っても十分に機能することはない。

適正な認証管理を実現する仕組みはさまざまだが、重要なのは次の2点である。

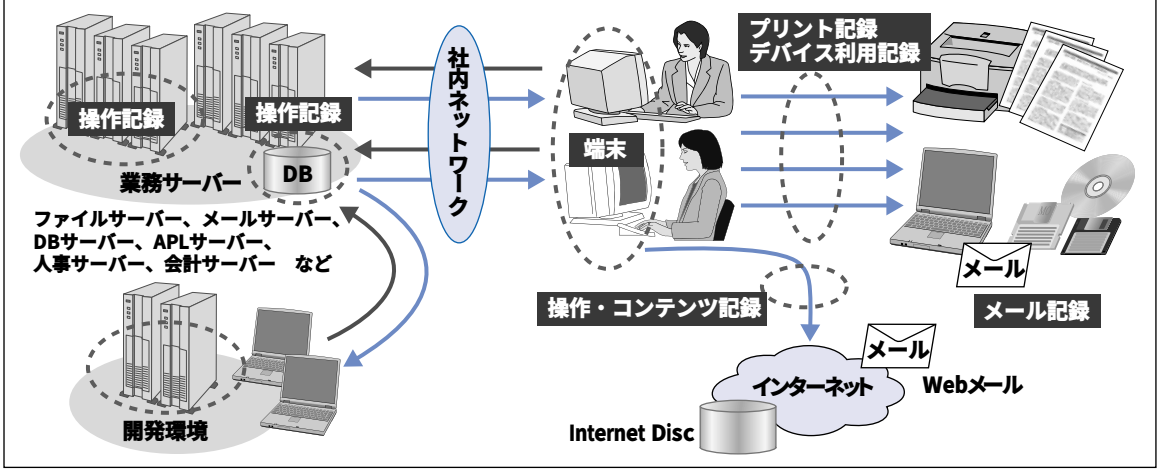
まず、第一は、限定の原則である。これは職務上必要な人、または組織に、必要な役割・権限を与えることである。そして第二は、運用の継続である。これは、速やかに、抜け漏れなく行うことを保ち続けることを指す。必要以上の権限を与えたり、適正な状態を保つことができなかったりすれば、それだけリスクを大きくすることとなる。

証跡管理――実行ログの見極め

認証管理が適正に行われ、利用者が正しく利用しても、適正なルールを逆手にとった「悪意ある事故」や「過失の事故」を防ぐことはきわめて難しい。過去の漏えい事件をみても、「社内の犯行、不注意」は決して少なくはない。このため、認証管理の事後的な補完機能として、証跡管理が重要となってくる。これは、システムに対する操作（オペレーション）やシステムに生じた内容（イベント）を実行ログとして記録、保存管理することである（図1参照）。

証跡管理において、第一に重要なのは「警告」である。すなわち、ルールと異なる操作や許可されていない作業が行われれば、シス

図1　証跡を確保する箇所（例）



テム管理者に通知がなされる。これにより、事故の未然防止が期待できるほか、実行ログの存在自体により、けん制や抑止効果が期待できる。

第二に、「分析」である。実行ログ分析により特異点（不正、異常）をいち早く発見することにより、問題に対処する予防機能が期待できるほか、発生した漏えい事故の事実確認を速やかに行い、正確な状況を把握することができる。正確かつ迅速な公表は、企業に対する消費者の評価を大きく左右するという結果が出ており、「企業の信用失墜」リスクを軽減する効果があると言える。

ただし、あらゆる実行ログを記録、保存するのはコストばかりかかり、いざというとき役に立たないということになってしまうため、取得すべき実行ログはその企業において脆弱性の高いと考えられる箇所を見定める必要がある。

セキュリティ対策は継続的運用が最も重要

セキュリティ対策の第一歩は、自社のシステムの現状を把握し、整理し、問題点を明確化することである。その上で、認証管理と証跡管理を行うことにより、セキュリティはより強固なものとなる。

すでに述べたとおり、いかなるシステムを導入しても100％の解決を得ることはできない。導入したシステムをいかに自らが定めた規定（ルール）どおりに保ち続けるかが重要なのである。導入しただけの高価なシステムに対し、機能的にはその70％のレベルであったとしても、適切に維持管理されている（メンテナンスが行き届いた）システムであれば、その情報リスク管理ははるかに実効性の高いものとなる。決めたルールの実施と問題点の速やかな解決という基本動作を継続、実践することこそ、最大のリスク軽減となる。 ■