日本版SOX法対策

データベース・セキュリティの強化でITガバナンスを支援

05年は個人情報保護法の施行により金融業界におけるデータベース・セキュリティに対する認知度が大幅に向上し、多くの企業にデータベース・セキュリティ・ソリューションIPLocksが採用された。

企業の重要な情報が保管されているデータベースを大もとから守るIPLocksは大切な情報の漏えいだけでなく、不正な改ざんにも対応することが可能。

このため、IPLocksのデータベース・セキュリティ・ソリューションは08年3月期から施行が計画されている日本版SOX法への対応についても有効なソリューションとして注目を集めている。

個人情報保護法とデータベース・セキュリティ

05年4月に個人情報保護法が施行され、特に金融業界では金融庁の『金融分野における個人情報保護に関するガイドライン』やそれに基づく金融情報システムセンター(FISC)の「安全対策基準」に記載されている具体的な項目に従って、個人情報を扱っている情報システムのセキュリティ対策は大幅に進歩した。

これらのセキュリティ対策には従来からあるファイアウォール、ウイルス対策、データの暗号化などに加えて、メールの添付ファイルの自動チェックツールや、個人のパソコンにデータを保管させないシンクライアントなど、様々なものが採用された。

また、これらは主に社内外とデータをやり取りする経路を監視したり、プロテクトすることで、個人情報の漏えいを防ごうとするものだった。

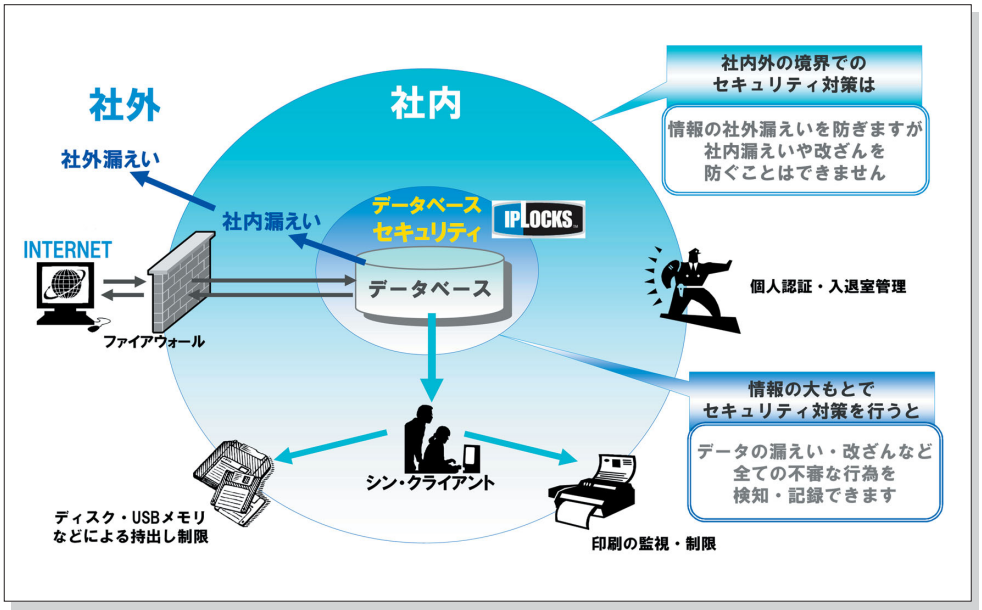
これに対してIPLocksが提供するデータベース・セキュリティは企業の最も重要な情報が保管されているデータベースに対する全てのアクセスを監視できるので、不審アクセスがあればその時点ですぐに管理者に通報される。また、個人情報など大切な情報に対する全てのアクセス記録を保持しているので、事故が発生した場合、いつ(When)、誰が(Who)、どこから(Where)、何を(What)読み出したのかを調査することが可能だ。

この『個人データへのアクセス記録および分析』という要件は『金融分野における個人情報保護に関するガイドライン』の第10条　安全管理措置の中の技術的安全管理措置の項目の中に明確に規定されており、この要件を満たすためにも金融機関にとってIPLocksの導入は欠かせないものとなっている。

また、IPLocksはデータベースからのデータ読出しばかりでなく、書込みも監視しているので、不正なデータ改ざんについても監視し通報することができる。

IPLocksによるデータベース・セキュリティ対策をネットワーク・セキュリティなど他のセキュリティ対策と上手く組合せることで、個人情報保護対策はよりレベルの高いものとなる。(図1)

図1　データベース・セキュリティの有効性



SOX法とデータベース・セキュリティ

01年にアメリカで発生したエンロン社の破綻は企業経営者が社員や多くの一般投資家を欺いたことにより大きな社会問題となった。このような事件の再発防止のために02年に成立したのが米国企業改革法（Sarbanes Oxley Act：以下SOX法）だ。SOX法では企業の財務報告内容を経営者自身がレビューし、その内容が真正であることを宣誓すること、さらにそのための内部統制の仕組みが有効に機能していることについて評価報告を提出することが求められている。

このSOX法は米国国内の企業に適用され既に2年目を迎えており、SOX法対応のための内部統制の仕組を構築する際にCOSO（米国トレッドウェイ委員会組織委員会）のフレームワークが広く一般に採用された。

一方、日本においても08年の3月期決算からの適用開始を目標にして日本版SOX法と呼ばれる内部統制に関する法律の整備が進んでおり、米国と同様に企業の財務報告に係る内部統制の仕組み構築が求められることになる。日本版SOX法では米国のCOSOのフレームワークをベースに『資産の保全』という目的と『ITへの対応』という要素を加えて構成されているのが特徴だ。

さて、それではこの内部統制の仕組構築をどのように進め、構築においてIPLocksがどのような役割を果たすのかを見ていこう。

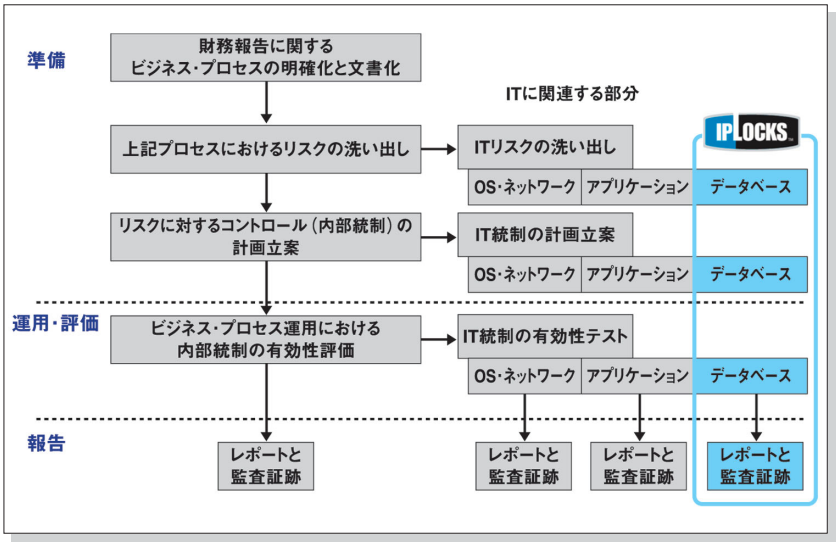
まず、はじめに財務報告に関する現状のビジネス・プロセスの明確化を行う。ここではビジネス・プロセス・フロー図などを使って、誰（組織、役職）が、いつ、どのような情報を基に、何を行い、何をアウトプットとして、次に誰に渡すかといったことを細かく明確化・文書化していく。

次に、このプロセスの中にどのようなリスクが存在するかを洗い出す。リスクには大きく分けて業務プロセス（人、組織、書類、手順など）に関係するものとITに関係するものがある。ITに関するリスクはさらにネットワークやOSに関わるもの、アプリケーションシステムに関わるもの、データベースに関わるものに分けることができる。SOX法のコンプライアンスにおいてデータベースの役割は極めて重要だ。なぜなら、主要な会計及び財務ソフトウェアはデータベースに依存しているため、企業は財務会計データベース内の評価、監査に重点を置かなければならない。このステップではIPLocksの脆弱性評価機能がデータベースに内在する潜在的リスクを洗い出し、必要な対策を検討する上で有効となる。またここで挙げられたリスクはその発生の可能性、発生した場合の被害の大きさなどを想定しておくことが必要だ。

リスクの洗い出しが終わったら、各リスクを最小化するための内部統制の計画を作成し、各リスクの発生を防ぐために必要な内部統制の仕組を設計する。業務プロセスに関してもITプロセスに関しても、ある特定の個人が一人で何でもできてしまうような状況は排除して、作業者の作業結果を第三者が監査・確認できる仕組みが重要となってくる。ここではIPLocksの監査機能がデータベースの構成変更や重要情報へのアクセスや更新について不正や間違いなどがなく行われていることを監査人が監査する上で必要となる証跡を提供する。

SOX法対応のための内部統制の有効性評価は1回限りの作業でなく、毎年繰り返し行うことが求められる。この作業量は膨大なものになることが予想されるが、これを効率的に行うためには、ITツールをうまく使いこなすことが企業にとって重要な課題となる。（**図2**）

図2　SOX法対応ステップとIPLocksのサポート



IPLocksのデータベース・セキュリティ・ソリューションは企業の財務情報が保管されているデータベースに関する現状のリスク評価（脆弱性評価）、内部統制の監査において企業の日本版SOX法への対応を強く支援する。

詳細は、IPLocks（http://www.iplocks.co.jp）まで