Interview

組織の根幹を揺るがす データベースセキュリティ

金融界がリーダーシップを

個人情報保護法の施行後、日本国内では数多くの情報漏洩事件・事故が起きている。金融界でも、大量の顧客名簿の流出や紛失を引き金に、クレジットカード詐欺やスパイウェアによる情報の詐取などが発生。これまで看過されてきた情報セキュリティシステムの脆弱性が厳しく問われている。

米国・カリフォルニア州サンノゼに本社を置く、アイピーロックスのセキュリティソフト「IPLocks」に関心が集まっている。既存の情報セキュリティシステムが抱える根本的な問題「脆弱性の検証」に着眼して、データベース(DB)そのものの弱点を補うためのセキュリティソフトとして開発された「IPLocks」。米国金融界ではすでに導入が進んでおり、日本でも、すでに導入実績80社を誇り、個人情報保護法施行後のベスト・ソリューションとして注目されている。

「金融界でこそ早急な取り組みが必要」と語る米国本社・坂本明男プレジデント兼CEOに、情報セキュリティシステムの現状と問題点、今後の対策などについて話しをきいた。

米国アイピーロックス
プレジデント兼CEO
坂本　明男 氏

情報漏洩は企業の根幹を揺るがす

Q.情報セキュリティの歴史的経緯は。

A.現在注目されている情報セキュリティへの取り組みは、インターネットが普及しはじめた92年頃に始まった。コンピューターウィルスや外部からの不正アクセスといった問題が顕在化しはじめ、ファイアウォールやVPNといった技術が開発されたのがこの頃だ。次いでIDSやアプリケーションソフトに対するセキュリティが登場。これらの技術は、もともとイントラネット化に係るもので、セキュリティについてもネットワークを守るための対策が先行していった。この後にITバブルの崩壊、多くの企業が消えていったが、セキュリティを扱う企業は生き残っている。当時も今もIT社会においてはセキュリティが重要であり、常に課題だった。

Q.情報セキュリティ対策の現状はどうか。

A.情報セキュリティが不可欠といっても、ITにおけるその歴史は短く、インターネットの普及とともにまだ十数年しか経っていない。他分野でのセキュリティと比較すれば、システムの枠組みと技術の双方において未だ不十分だ。例えば、大型コンピューターを使っても解読は難しいと言われた暗号化技術に「トリプルDES」があるが、マサチューセッツ州に住む技術者がわずか24時間で解いてしまった。厳重なセキュリティシステムを構築したつもりでも、視点を変えれば不備な点がいくつも見えてくる。どんなセキュリティも破られる可能性が残っているということだ。

Q.まだまだ情報セキュリティへの取組みは甘いのか。

A.米国ではサーベンス・オクスレー法など、規制の強化により、厳格な情報管理が求められるようになった。例えば、カリフォルニア州ではデータベース(DB)攻撃を受けた場合に、ユーザーに対しての攻撃の事実を報告することが法律で義務づけられている。いずれ、この流れは全米に広がるだろう。実際に、4000万人の顧客情報が流出したというクレジットカード会社や、シティ・グループ、バンク・オブ・アメリカ等の情報漏洩事件を受け、情報管理が顧客の評価と信頼を左右することが分かった。金融界では対策を急いでいるが、現在のセキュリティシステムが抱える根本的な問題を見落とさず、一刻も早い処置をとる必要がある。情報セキュリティ対策は、いまや企業の根幹を揺るがす重大な経営問題と言える。

企業財産を守る3つのポイント

Q.情報セキュリティの最大の課題は。

A.企業にとって一番重要なものは、顧客データや財務データなどが詰まったDBだ。しかし、我々が耳にする多くのDBは、パスワードとユーザーネームの2つでしか守られていない。つまり、パスワードとユーザーネームさえ合致すれば、誰でもDBにアクセスできてしまう。例えば、IT部門のシステム管理者はスーパーユーザー権限というシステムへの自由なアクセス権限を持つ。これらの権限を持つシステム管理者、運用者やソフトウェア技術者が社内やアウトソース会社に何人もいる。彼らになりすますことができれば、社内全ての扉をあけることができる鍵を得たのと同じだ。この鍵の運用状況を監視できない現状は極めて危険だ。

Q.なぜ、そのような権限を放置するのか。

A.IT社会では、ビジネスの継続性が最も重要だ。不測の事態によるビジネスの中断は、大きな経営リスクとなる。このため、いつでも、どこからでもシステムにアクセスする権限を持つ人材が必要となる。しかし、この権限こそが情報漏洩や内部犯罪の原因にもなっている。

Q.DBを守る手立てはないのか。

A.企業にとって、あらゆるデータが保存されているDBは、最も価値ある財産だ。誰もが、財産を金庫に入れるときには、まず、金庫の格納場所のセキュリティを高くし、かつ金庫そのものの強度を高くする。さらにガードマンで不審者をチェックするのと同時に、監視カメラで24時間365日金庫のアクセス状況を記録するはずだ。情報セキュリティシステムにも同じことが言える。まず、DBを守るパスワード(鍵)の強度やソフトウェアの弱点、そしてセッティングの問題点などを細部にわたってチェックするために脆弱性の評価から始める必要がある。次に、重要なアクセスは端末を特定するなど、ルールに基づくチェックによってシステムへのアクセスや変更等をリアルタイムで監視しながら異常な操作について警鐘を鳴らすこと(ガードマン)。それから誰が、何時、どこから、何を、どのようにしてアクセスしたかのログを保存(監視カメラ)し、定期的に状況を監査できるようにする。以上の3点がポイントになる。DBに対する犯罪行為の多くは3ヶ月以内に発生するとの調査報告もあるが、アクセス・ログをどのくらいの期間保存しておくかはコンプライアンス絡みからも決定する必要がある。また、内部犯行が多い情報漏洩事件では、社員自身も自分の行動が記録・監視されていると知れば、犯罪の抑止力になる。

データベースセキュリティの要(かなめ)

Q.「IPLocks」が支持を集めている理由は。

A.情報セキュリティシステムの問題点がDBにあることを把握し、情報漏洩の多くが内部からの脅威であることに正面から取り組んだからだろう。DBセキュリティ対策で求められるものは、「脆弱性評価」「監視」「監査」の3つだ。それは、前述の「金庫室や金庫の強度」「ガードマン」「監視カメラ」と同じだ。まず、DBそのものの「どこが弱点か」を把握しなければならない(脆弱性の評価)。システムの弱い箇所を評価して全体のセキュリティ強化を図るのがDBセキュリティの基本であり、いずれかが欠けてもロジカルではない。いくら事後監査を強化してもセキュリティが低い金庫室と金庫では事故は防げないということだ。多くのセキュリティソフトがこの点を見落とし事故後の証拠を残す監査ログばかりに力を入れている。これでは顧客情報の流出が起きて顧客に迷惑はかけ、かつ会社の信用を落としても、証拠さえ残しておけば良いといっているのと同じだ。なぜ、ネットワークでは脆弱性の評価が当たり前になっているのに、DBではそれをしないのか。ネットワークセキュリティで求められる対策の全てをDBに対しても行うのが当然だと考えている。実際に、システムの脆弱性評価については、金融界でも手付かずといった状態だったが、それに気づいた米国ではいち早く、銀行で引き合いが殺到している。

Q.セキュリティは「いたちごっこ」と言われるが。

A.セキュリティを取り巻く脅威は常に変化している。当然、それに対応するシステムも必要に応じて強化されねばならない。そのため当社では、3カ月程度でバージョン・アップを行っている。より安全性の高い機能を提供することが重要で、必要性については利用者の判断に委ねている。利用する側で、時期を見極めて導入していただければ良い。

金融界のリーダーシップに期待

Q.DBセキュリティに対する意識改革をどのように進めるか。

A.米国では実害が出てから取り組みが本格化されてきた。DBへの犯罪によって弊社ソフトの優位性が認知されるのは皮肉な話だ。日本でもいつ同様の犯罪が発生するか誰にも予想がつかないし、発生してからではもう遅い。いまや情報セキュリティは社会問題化しており、十分な対策を行わないとCIOなど情報管理の責任者は枕を高くして眠れないだろう。

Q.金融界での今後の動向は。

A.米国では、金融機関が率先して情報セキュリティ対策に取り組んでいる。日本でも重要な顧客情報を持ち、DBの重要性を認知している金融機関こそ、DBセキュリティの強化を行うことが必要で、より安全で効率的な情報利用のためにリーダーシップをとってくれることを期待している。

IPLocksの日本法人はアイピーロックスジャパン株式会社です。
http://www.iplocks.co.jp でご確認下さい。