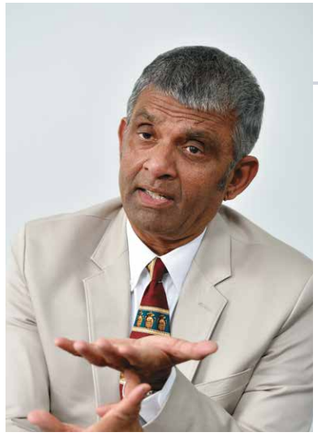
ITジャーナリスト 三上 洋が 訊く

“4つの対策”で情報漏洩は95%まで防御できる！

企業からの情報漏洩事件が後を絶たない。さらに現在の事態が深刻なのは、自社からの情報漏洩にさえ気付かない企業があることだ。システムの安全性を担保するために、日本企業は何に留意し、どのような対策を講じていけばいいのか。セキュリティ分野のリーディングカンパニー2社に話を聞いた。

ITジャーナリスト　三上 洋
専門分野はネットの安全対策やIT活用など。企業のセキュリティ対策に関する講演多数。読売オンラインでは一般向けセキュリティ記事を長期連載中。



米STRONGKEY社
CTO
Arshad Noor氏

セキュリティ対策には経営者の理解が必要

2015年5月に発生した日本年金機構からの個人情報流出事件以降も、企業からの情報漏洩事件は相変わらず多い。国内ではあまりに多すぎて、ニュースにすらならなくなってきた感がある。そんな中、2018年11月に世界最大手のホテルチェーンであるマリオットからの顧客情報流出が報じられた。その数は実に約3億8300万件。しかしそれ以上に愕然とさせられたのは、サイバー攻撃者からのハッキング行為は、その4年も前から始まっていたという事実だ。同ホテルは4年間、自分たちのシステムに侵入されていることにさえ気付いていなかった。この件について、グローバル市場で豊富な実績を持つセキュリティアプライアンス製品『Tellaro（テラーロ）』を開発した米STRONGKEY社 CTOのArshad Noor氏は、次のように話してくれた。

「セキュリティの問題は、経営者が事の深刻さを十分に理解した上で解決策を講じていかなければ、根本的には解決しません。マリオットの事件は、世界中の企業のマネジメント層の情報漏洩に対する危機感が、いかに薄いかを如実に物語るものだといえます。そこに私は大きな危機感を抱いています」

翻って日本企業のセキュリティ事情を眺めてみれば、もっと拙い状況にあると考えられるのではないか。

情報漏洩の95%を防ぐ4つの対策

Noor氏が指摘するように、セキュリティ対策に対するマネジメント層のコミットメントは確かに重要だ。しかしこれだけ情報漏洩事件が続いている状況を見ていると、もう企業からの情報漏洩は避けることができないのではないかとも思えてくる。この点についてはどうだろうか。

「確かに情報漏洩を完全に防ぐことはできません。しかし95%は防ぐことができるでしょう。しかもそのために企業は、4つのことをすればいいだけです。1つめが、より強固なユーザ認証方式であるFIDO2認証を採用して、攻撃者が自社システムに侵入することを困難にすること、2つめが、万一情報が持ち出されても内容を読み取られないように、データを暗号化しておくこと。許可されたアプリケーションによってのみデータが復号化できるように、暗号化をアプリケーション層で行うことが重要です。そして3つめがデータの保全で、データが改ざんされた場合にその変化を検知できるようにしておくことです。最後に、暗号化鍵が暗号化ハードウェアモジュールによって管理および保護されていることが重要です。この4つの機能を提供するのが、我々の開発したテラーロです」（Noor氏）

これまで日本企業は、サイバー攻撃そのものへの対策には力を入れてきた。例えば有事マニュアルの作成やCSIRT（Computer Security Incident Response Team）の設置などだ。しかし万一、重要な情報が漏

株式会社システナ 取締役 兼 上席執行役員
ソリューション営業本部長
田口 誠氏

れてしまった場合に備えての対策までには手が回っていなかった。その意味において、前述の4つの対策が非常に有効な解決策だと言えるだろう。

ワンストップで手間なく導入できる製品は有用

米STRONGKEY社は、米国商務省配下の機関であるNIST（アメリカ国立標準技術研究所）が設立したNCCoE（国立サイバーセキュリティセンターオブエクセレンス）によって彼らのプロジェクトにおけるセキュリティエキスパートに選ばれた企業で、同社の提供するテラーロは、米国の政府機関や通信キャリアをはじめとするフォーチューン500企業、欧州の中央銀行などで採用されている。グローバル市場では既に豊富な導入実績を持っており、日本国内では2019年春から、ITソリューションベンダーの株式会社システナが販売を開始する予定だ。国内での展開について、システナ 取締役の田口誠氏は次のように説明してくれた。

「政府や金融機関、病院や大学、さらには製造業、サービス業など、機密情報を持っている日本の組織や企業すべてに、テラーロを推奨します。特に国内では、2019年、2020年と国際的なスポーツイベントが開催されますが、その際にはサイバーテロの標的となるリスクが非常に高まります。テラーロは、まずは顧客情報を守りたいとか、従業員の情報を守りたいという一部のデータを対象にした導入も可能です。企業規模の大小を問わず、これから日本企業がより強固なセキュリティ対策を実現するためのご支援をしたいと思っています」

私のこれまでの感覚では、既存のシステム環境にFIDO2認証やデータ暗号化のソリューションを追加で導入するのは、かなり面倒で負荷の大きい作業だ。しかしテラーロは、エンドユーザのPCと、各サーバもしくはプライベートクラウドとの間に設置するだけで済む。これによってパスワードレスによる認証が可能となり手間なく安全性が高まり、さらに万一情報が漏洩した場合でもデータの暗号化により中身を読み取られる心配もない。こうした機能をワンストップで提供してくれるテラーロは、日本企業にとっても非常に便利で有用な製品だといえる。

インシデント前提のセキュリティ対策を

Noor氏は、情報漏洩事件を起こして企業が多額の賠償金を支払うことになったとき、そのお金は結局、自社の顧客から支払われていることに他ならないと指摘する。一方の田口氏も、これからセキュリティ対策に必要なお金はコストではなく、企業にとって必須の“投資”であると考えるべきではないか、と語る。

繰り返しになるが、今の時代は、情報漏洩が起きた後のことを真剣に考えなければならないという大前提がある。そこでデータ暗号化の必要性が出てくるが、テラーロは加えてFIDO2認証と改ざん検知の機能までを提供する製品だ。特に改ざん検知の機能があれば、サイバー攻撃だけでなく、企業のセキュリティ被害で一番損害額が大きいと言われる内部不正まで防ぐことができる。日本企業は、自社にもセキュリティインシデントは絶対に存在しているという視点に立ち、セキュリティ対策を考えていただきたいと思う。