HP Technology at Work

特集 - 情報セキュリティ最前線

～情報を“活かす”プランと対策とは？～

» もとのページに戻る

IT活用が拡大し、機密情報の漏洩を防ぐための「情報セキュリティ」が、企業の重要な課題となっている昨今。来年4月には「個人情報保護法」も施行され、その対応が急務となっています。本来情報は“活かしてこそ”意味を持つもの。その利点を保ちつつ、守るべき情報を守るには、何に留意し、何を行なっていけばよいのでしょうか。レクチャーするのは、情報セキュリティのコンサルティングに取り組む日本HPのエキスパート、佐藤慶浩と栗田晴彦。セキュリティの“最前線”をお伝えします。

日本HP
個人情報保護対策室
室長
佐藤慶浩

日本HP
コンサルティング・インテグレーション統括本部
ネットワークシステム本部
セキュリティソリューション部
栗田晴彦

強固な守り」と「柔軟な活用」のメリハリが最適な情報セキュリティを支える

Q：まずITにおける「セキュリティ」とは何を指すのか、お教えください。

佐藤：ITで「セキュリティ」と言う場合、それは「情報のセキュリティ」を意味します。情報には、自社の機密情報、「個人情報保護法」の対象となる顧客情報をはじめ、さまざまなものがあります。それらの漏洩を防ぐには、どの情報をどのように守り、取り扱うかといった基準を定め、実現のためにどんな技術を活用し、現場でどんな手順で対処するかを確立していく必要があるのです。

Q：セキュリティを考える時の大事な視点は何ですか。

佐藤：HPの場合、ITは「アダプティブ（＝適応力に富む）」であるべきという視点に立ち、それを実現するには3つの要素が必要だと考えています。一つは「性能」、もう一つは「可用性（ダウンタイムがなく、使いたい時に使える）」。そしてもう一つが「セキュリティ」です。これらは“三つどもえ”で、どれが欠けてもスムーズなITインフラは成り立ちません。ただ「セキュリティ」は少し異色で、他の二つは投資を増やせば生産性が上がるのですが、「セキュリティ」は違います。セキュリティをアップしてがちがちに固めてしまうと自由度がなくなり、「お金を使って性能を落とす」という矛盾に陥ることもあるのです。ですから、いかに多くを投資するかより、「どう投資するか」が重要なんですね。

よく「セキュリティに万全はない」と言われますが、テクノロジー的にセキュリティを万全にすることは実際には可能です。たとえばHPでは米軍に情報システムを提供していますが、こうしたケースでは当然、万全なセキュリティが求められます。一方で企業の場合は、あえてそのレベルを6割くらいに留めないと「情報の活用」ができなくなるという現実があるのです。軍の場合「機密情報が漏れるようならその情報は抹消された方がいい」ということで、そうした技術が使われますが、企業の場合、情報がどんどん消えてしまえば活動に

支障をきたしますから、「消えない程度に守る」方が重要です。ですから大事なのは、情報の「活用する部分」と「保護する部分」のメリハリをはっきりさせることなのです。

栗田：セキュリティはゼロでもいけないし、やりすぎてもいけないということですね。「中庸」を見つけることが大切で、完全に守るのは困難ですし、多くの場合は無駄でもあるのです。まずは「セキュリティの目的」をしっかり設定し、全社レベルのセキュリティのプランを策定すること。守るべきものが何かを見極め、具体的にどう守ればいいのかがわかって、対策を打つ‥‥それを計画的に行うことがとても肝要だということですね。

Q：適切な情報の保護と活用のためには、どんな情報を、どう扱うべきなのですか？

佐藤：絶対に行なった方がいいのは「活用しなければならないものは柔軟に保護する」ということですね。「強固か柔軟か」という選択をするのではなく、それぞれの情報の種類に対して異なる対処を組み合わせることが必要だということです。たとえば「個人情報」は自分のものではなくお客様のものですから、強固に保護すべきですが、新製品情報などは、重要な機密情報であっても、出荷の3ヶ月くらい前にはお得意様に機密保持契約を交わしてお見せできるようにするなど、現場で人が判断できる柔軟性が必要になります。「強固な守り」と「柔軟な活用」。状況に応じてメリハリのある対応をすることがポイントなのです。あと、新しくセキュリティのルールを施行する時は、持っている既存の情報にはこだわらず、新しい情報に対して徹底して行うことも大切。通常、企業の現場の情報は、3〜5年、営業部署では1年で入れ替わると言われますから、既存のもの（情報やシステム）は既存のルールで、新しいものに対しては新しい技術で対処した方が、ルールを徹底させるには確実ですね。既存のものに新しいルールを適用すると、組織全体のルール達成率は低いところから始まることになります。達成率の低いルールに対して、人はおろそかになりがちです。新しいルールを新しいものから適用することにすれば、最初からルール達成率100%を実現することは不可能ではありませんし、新しいルールに少し慣れてから、既存のものにも徐々に適用拡大していくということもできます。ルールを守るのは人ですから、人がルールに無関心にならないようにするための工夫が重要なのです。

情報“格付け”のルールを明確にし、テクノロジーで実行するのが理想的

Q：セキュリティのプランニングのポイントは何ですか？

栗田：セキュリティは、「人」と「システム」に対するプランニングで成り立っています。そもそも何でセキュリティが必要かと言えば、ITを「人間が運用」し、その人間は「不完全な存在だから」ですね。人がいなくて機械だけの世界ならセキュリティは必要ない。ですからまずは、いかに人が使いやすく、運用しやすいもので、一方で間違いが起こらない、悪い気が起こらないようなものにするかを考えるべきで、その仕組みを組織全体に行き渡らせることも必要です。一方システムについて言えば、構築のプラットフォームがさまざまだったり、クライアントやサーバーがあったりと、複雑な環境があるわけです。現実的には決定的な解決法があるわけではなく、それぞれ環境にあったソフトを組み合わせざるを得ません。昔のようにファイアウォールだけというような単一の境界でなく、すべてのシステム構成要素にセキュリティ対策が必要なわけですから、それら全体を「マネージメントする」ことも不可欠になります。つまり数多くのセキュリティを集大成させる必要があり、それらすべてを包括したプランニングが行われないと、セキュリティは成り立たないというのが現実なのです。

佐藤：私はプランニングで重要なのは「人と情報の整理」だと考えています。つまり、人にどういう役割を持たせ、どういう体制を取るかを考えることと、「情報の格付け（クラシフィケーション）」をするということですね。情報にマル秘を付けたりするのもその一つ。情報に対して「誰が何をしてもいいのか」を決め、どうしてもやってはいけない部分については技術を充てていく。とくに日本の企業では、「日々膨大な情報処理を行う中でいちいち判断をしてはいられない」という理由で、情報の格付けには抵抗があるようですが、これは情報セキュリティの出発点として、実はとても重要な部分。基本的にはその情報を作った人が情報が機密かどうかを判断するというのが一番いいでしょうし、格付けができれば、技術の導入も容易になります。たとえば企業の外に漏れると重大な被害を及ぼすと思われる情報に「マル秘」と書くようにすれば、その情報は外に出ないようにすることは技術的には簡単にできるわけで、「どういう場合にマル秘に設定するか」という定義と、情報の取り扱いのルールを定めておき、あとは技術で実装する‥‥それが一番単純でいい形だと言えますね。これがしっかりしていないと、部署ごとにマル秘の技術対策が異なったりして、結局は後工程の手間や費用が増すということになってしまいます。

セキュリティを成功に導くのは、
コストを最小限に押さえるプランニング

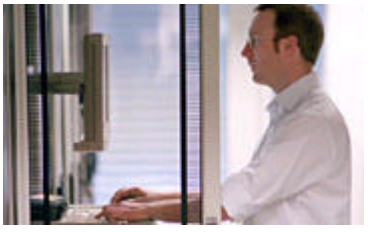
Q :その企業に最適のセキュリティは、どうやって見極めたらいいのですか？

栗田 :一つの考え方としては、「コスト」という観点が判断の基準になるのではないでしょうか。たとえばセキュリティ確保のためにパスワードを難しくすれば、忘れやすくなり、場合によってはアクセスできなくなる。それでは柔軟な運用ができなくなり、生産性が落ちるなど業務に影響が出ます。生産性が落ちるということは、人手が余計かかるということで、それはまさに「コスト増」ということです。一方で、セキュリティのためにテクノロジーを採り入れればそこでもコストがかかります。そうしたコストがどこまで許されるか、ある部分はあえて人間が担当したりしながら、どこまでセキュリティを実現すべきかという妥協点を探ることですね。将来的には「認証のテクノロジー」が発達し、人の意識を介することなくセキュリティを高めることもできるようになると思いますが、現時点でそれを行うと非常にコストがかかってしまい現実的ではありません。

Q :企業はセキュリティのコストをどう捉える傾向にありますか？

佐藤 :日本では「セキュリティのための予算をどうするか」がガイドライン化されていない企業が多く、その原資をどうするかも含めて、プランニングが不十分なことが多いかもしれません。というのも、日本の現場ではセキュリティプランをITの技術者に任せるケースが一般的で、そうすると技術レベルでどうするかという話にはなっても、その予算をどこから捻出するかという視点は抜け落ちがちです。それでは「セキュリティは大事だけど、予算が少ないから難しい」ということになってしまいます。現実的には、ITのシステムを開発するお金と、セキュリティのためのお金がまったく分離してしまうのは難しいので、あえて全社レベルのプランニングの段階で、セキュリティ対策予算を最小化する努力をした方が、結果的にうまく予算取りできるケースが多いですね。つまり、もともと一つの企業のITに対するお財布は一つなので、セキュリティを最優先させてシステム構築の予算を減らし「性能」や「可用性」を落とすより、複数の部署で共通化するセキュリティ対策だけに限定してセキュリティ予算を確保する方が、セキュリティ以外の原資がより多く残り、結果的にセキュリティへのお金が使えるということです。

そうした予算の割り振りを含めて、どう全体をプランニングしていくかが重要ですね。たとえば事業部共通で必要なものは「セキュリティ予算」を充て、社員全員のICカードを作るとすれば、従来アプリで作り上げていたユーザ認証の機能をICカードが果たすことができ、結果的にはシステム開発予算が削減でき、全体のバランスをとることができます。IT部門が用意するものを事業側が使う時代と異なり、最近は「生産性を上げるためにSAPが欲しい」とか、「顧客とのリレーションシップのためにCRMが必要」という風に、事業側の要請に従ってシステム構築が行われますから、その予算獲得の際に、セキュリティ要件を満たすことを必須のものとして組み込まれるようになれば一番望ましいですが。いずれにしても、コスト削減が重要な経営課題である中で、情報セキュリティ予算も例外ではありません。情報セキュリティのプランニングは、コスト削減につながることを示すものでないと頓挫することが多いので、そこはセキュリティを成功に導く非常に重要なカギとなります。



栗田 :今、一つの傾向として、大企業ではさまざまなレベルでセキュリティのインフラ化が進みつつあります。インターネットやメールはもちろん、場合によってはファイルサーバーやOA系、さらに、ディレクトリーサービスや、PKIやICカードなどの認証の仕組みについても、共通のインフラとして提供されるという方向性になってきています。つまり、今まではファイアウォールなどのネットワークレベルでセキュリティやアンチウィルスなどをインフラとして提供していたのが、ディレクトリ整備などでアイデンティティマネージメント（ユーザ管理・本人認証・アクセス制御など）を全社共通のインフラとして整えようとするところが増えているのです。仮にある会社が10個のアプリケーションごとにセキュリティ対策や運用を行っているとすれば、人事異動がある度に登録・削除などの設定変更を全部修正しなければなりません。セキュリティがインフラとして統合されれば、そこでかかるコストはたちまち削減されます。確かに初期投資のコストはかかりますが、その後のV字回復が早く、長い目で見ればITコストを押さえるのにとても有効な方法だと言えるのです。

Q :セキュリティの場合、広い視座を持つことがコストダウンに有効なのですね？

栗田：HPでは提唱している4つのセキュリティのうち2つに「マネージメント」という言葉をつけています（アイデンティティ& アクセス・マネージメントと、セキュリティ・システム・マネージメント）。これは、セキュリティの対策は、設定や運営といったマネージメントがしっかりしていないと、逆にコストがかかってしまったり、セキュリティの目的を果たせないことにつながってしまうというのが背景にあるため。きちんとマネージメントされた運用を行い、全社規模で、中長期的なビジョンを持って、セキュリティも想定したシステムを作りあげることが大事なのです。仮に今あるシステムにあわせてセキュリティ対策を講じるとしても、将来的な方向とあわなければ無駄になるし、運用や管理も二度・三度の手間になってしまいます。システムはだいたい4〜5年単位で変わってしまうので、新しいシステムを構築するときは、インフラにセキュリティ対策を盛り込み、徐々に強固化していくようなプランニングをする‥‥そうした視点が、今後ますます重要視されていくのではないでしょうか。

個人情報保護法は
セキュリティ整備のきっかけに

Q：来年4月に施行される「個人情報保護法」にはどう対処していけばいいのですか？

佐藤：「個人情報」も情報の格付けで「機密」として、セキュリティ対策が万全であれば、技術的に漏洩は防止できます。もしその部分の技術が弱ければ、強化すればいいわけですし、漏洩防止はセキュリティ対策に委ねればいいのです。ただ、日本では「漏洩の防止」に話が集中していますが、実際そこには「プライバシー保護」という視点もあって、現在オプトイン（あらかじめ情報配信の許諾を得る）されていない情報をそのままにしておくと、4月以降、それらを有効に利用できなくなります。活用しないのであれば捨ててしまっても変わりなく捨てるならば漏洩対策は不要ですが、「活用する」という視点に立つなら、「個人情報保護」ではなく「個人情報取り扱い」という取り組みとして、個人情報を4月以降も活用できるようなルールづくりをすることが必要です。そこで急務となっているのは、現在オプトインしていないお客様に対してオプトインの可否の意向をたずね「オプトインされていない情報をオプトイン化」していくこと。ここでは、返事がこない方に対し再確認をするかどうかなどルールを決めていくことも重要で、オプトアウト（情報配信を断る）を希望する人についてもその情報を削除せずに、「オプトアウトリスト」を作るようにすれば、その後も不用意にその人にメールが送られることを防ぐことができます。本来ユーザーは、情報が保護されることだけでなく、「オプトアウトの保証」を求めているのでしょうが、「個人情報保護」と「プライバシー」という2つの違う概念を1つの取り組みの中で行なおうとしているのが日本の現状です。とはいえ、法は法として企業は遵守しなければなりませんから、法律に則る形で、アメリカのようにプライバシー保護に関する自主規制を徹底することが必要でしょうし、そうしなければ今後お客様の期待に応えられないということになってしまいます。

栗田：個人情報というのは、企業の預かり資産で、企業ではなくお客様の資産ですから、大事に取り扱うことは大前提。そのためのセキュリティ対策を整えることは、会社全体のセキュリティを高める非常にいいきっかけになるのではないかと私は考えています。

Q：HPのセキュリティに対する取り組みの、優れた点を教えてください。

佐藤：昔はシステムとセキュリティ対策がきれいに切り分けられたのですが、今はセキュリティを考えながらシステムを実装しなければならなくなっており、お客様のニーズもまさにそこに変わってきています。そんな新しい流れの中で、HPはセキュリティ専門ではなく、総合ITベンダーとしての視点でセキュリティを目的ではなく手段と位置付け、セキュリティ予算を単に増やすのではなく、効果的な使い方を考えます。HP自身が社内で経験した成功と失敗の改善に基づいて、お客様のご要望にお応えできるのが大きな強みだと言えます。

アダプティブ・エンタープライズのための
HPアーキテクチャ

≫新規Windowに拡大画像を表示します

栗田：本来セキュリティは「目的」ではなく、システムをより安全に効率よく使うための「手段」です。そうした観点からHPは、セキュリティ対策における3つの利点を持っています。一つは、総合ITベンダーゆえに、ネットワーク、基本システム、サーバー、クライアント、ストレージ‥‥とさまざまなシステムコンポーネントがある中に、セキュリティを組み込み、スムーズな運用に結びつけていけるということ。もう一つは、近い将来、セキュリティがマネージメント抜きに語れない時代になると予測される中、弊社の運用管理ソフト、HP OpenViewが、重要な役割を担うと考えられること。そしてもう一つは、HPが優秀でマネージメントにも長けたITネットワークエンジニアを数多く擁し、システム構築を含めた的確なプランニングやコンサルティングができるということ。HPは、セキュリティのためのセキュリティではなく「ITを安全に動かすためのセキュリティ」を考える会社であ

り、それがお客様への最大のメッセージでもあると考えています。

関連リンク]
≫**HP セキュリティー・ソリューション**

ご感想をお聞かせください »

»? もとのページに戻る
?