

情報セキュリティ対策、再考 ～「安心＝安全×？」～

伊藤 慎

要 旨

情報セキュリティ対策は、いったいどこまでやればよいのか?—営業支援部門に身を置くものとして、多くの企業・団体のお客様からお聞きするテーマです。情報セキュリティに関わる脅威(リスク)の種類は多く、また、日々新たな脅威が出現してきます。本稿では、安心できる情報セキュリティ対策とは何か、また、そこに至るためには何が必要かについて、お客様に対応するなかで得た考えを述べます。

キーワード

●安心 ●安全 ●CIA ●数えるマネジメント

1. はじめに

多くの企業・団体では、個人情報保護法への対応がひと段落したのも束の間、現在は、内部統制の対応に追われています。一方、情報漏えい事故も後を絶たず、引き続きセキュリティ対策を計画・実行しなければならないという声も、よくお聞きします。このように企業や団体では、情報セキュリティに関する取り組みが、まだ道半ばの状況ですが、人も資金も潤沢にあるわけではありません。効果的な情報セキュリティ対策と実践とは、どのように考えればよいのでしょうか。本稿では、筆者がふだん多くのお客様と接するなかで感じる情報セキュリティ対策における「マネジメント」の重要性とその実現方法について説明します。

2. 情報セキュリティ対策の原点

そもそも情報セキュリティ対策とは、いったい何をすることなのでしょう。このような疑問に対し、よく引き合いに出されるのが、「CIA (Confidentiality, Integrity, Availability)」の考え方です。これは、機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)の3つの観点で対策を講じ、かつバランスをとるべきだというもの。機密性とは、秘密文書、データなどを誰かに見られないよう、盗まれないようにすることです。完全性とは、守るべき情報が正しい状態か、改ざんされないような対策がされているかということを指しま

す。可用性は、使える人が使いたいときに使える状態にあるようにすること、です。たとえばウイルス対策が弱く、感染しやすいネットワーク環境では、これらのどれ1つとして成立しません。情報セキュリティ対策を考える上では、これら3つの視点が守られているかどうかを調べるのが大事な観点です(図1)。

お客様の具体的な状況を例にとりて考えてみます。あるお客様の組織では、ファイアウォールを導入しました。次に、ファイルを暗号化し、ID/パスワードを共用利用から一人ひとりにIDを割り振り、パソコンの操作ログも採取するようにしました。USBメモリも暗号化し、メールもフィルタリングソフトを導入

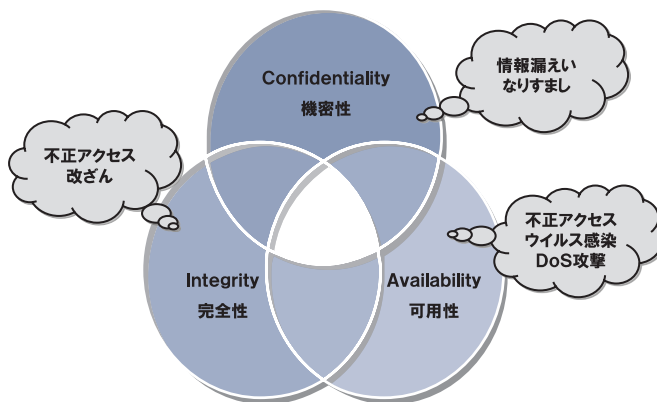


図1 情報セキュリティ対策の原点

し、秘密情報があれば誤って外へ送信されることのないようにしました、という対策を行いました。これで一見完璧にみえます。しかし、いくつかの対策を場当たりに重ねてきた結果、現状が情報セキュリティ対策として満足できる状態なのか否かが、お客様自身が明確に判断できなくなり、その結果、次の段階へ進む計画を策定するときに、何をどのように、どれだけの投資をして実施していくべきなのかの計画で立ち止まってしまった、という事例がありました。市場では、様々な対策ツールが乱立といえるほど揃っています。もう一度、守るべき情報資産ごとにCIAの観点で足りないことは何か、バランスはどうか再整理し、今後の対策を考えることが重要です。そのためには、自社のセキュリティ対策の現状を正確に把握し、全体最適なセキュリティ対策を計画・実行することが必要であり、常に全体を把握し制御し続けるマネジメントシステムの構築が重要になります。情報セキュリティマネジメントシステムの国際標準ISO/IEC 27001は、それらの計画策定のための指針となるべく制定されたものです。

3. 効果的な情報セキュリティマネジメントシステム(ISMS)のポイント

本章では、情報セキュリティの効果的な対策として、情報セキュリティマネジメントシステムの果たす役割を考えてみます。

情報セキュリティにおけるPDCAサイクル(Plan, Do, Check, Action)とは、情報セキュリティポリシーを具体化した制度(ルール)とIT対策の実施状況を把握し、常に改善を施すサイクルを実行することです。この改善のサイクルを繰り返し回していくためには、脅威、脆弱性の可視化(見える化)が重要です。それを着実に行うためには、可視化(見える化)の尺度、すなわち脅威、脆弱性の度合いを測る適当な管理指標を設定し、定量的に把握することが重要です。「測る化」とも言われますが、NECでは、これを「数えるマネジメント」と呼び、マネジメントシステムの要諦として重要視しています(図2)。

現在の情報システムの状況を定量的に把握することで、あるべき姿を示す目標と実際の実態との差が分かりやすくなり、その差を解決する対策が考えやすくなると同時に、対策を実施し運用した結果を再度確認することで、その対策の効果、目標への達成に向けた計画が関係者のなかで共有しやすくなります。

たとえば「ウイルス感染」という脅威に対し、ネットワーク上に接続されているパソコンやサーバの台数、セキュリティパッチの適用状況、アンチウイルスソフトの導入台数、パター

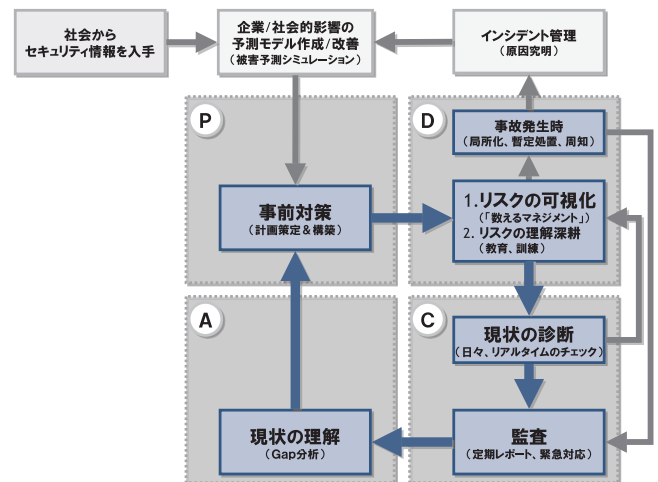


図2 PDCAサイクル

ンファイルの適用状況を常に数えていると、新種のウイルスが発生した際に、セキュリティパッチ未適用による感染の可能性のあるパソコンの台数が分かります。仮に、100台のパソコン環境において90台がセキュリティパッチ未適用であれば、ウイルス感染による被害は大きいものと予想されますから、その場合は、直ちに一斉通知(メール、館内放送等)により適用を促進すべきです。それでも対処されないパソコンは残るかもしれませんので、次の対策として当該パソコンの利用者に直接電話連絡して処置を促します。90台が60台に、60台が30台にと、その量により対策も変えながら「ウイルス感染」という脅威を低減していきます。

情報セキュリティマネジメントシステムのめざす姿は、脅威・脆弱性の可視化(見える化)を図り改善を繰り返す組織とするために、効果的な定量把握(数えるマネジメント)を実践する環境を実現することと言えます。ここで運用において重要なのは、最初から完璧を狙うのではなく、PDCAサイクルを回しながら、少しずつ目に見える形で改善していけば、いつかは目標状態に達成できるという信念に基づいて継続的に活動をしていくことと言えます。

4. めざすべきゴール

守るべき情報資産を明確にし、脅威を見極め、その脆弱性ポイントに対策を講じ、その実施状況を可視化し改善を繰り返すサイクルが回り始めると、では「我々はどこまでやれば

情報セキュリティ対策、再考 ～「安心=安全×?」～

よいのか?」という課題に直面します。

たとえば、すべてのパソコンに暗号化ソフトを導入すれば情報漏えい対策は十分と仮定した場合でも、安心できる状況を構築するのは至難の業です。もしかしたら、設置してあるパソコンのなかには、指示を徹底したにもかかわらず暗号化ソフトを入れていないパソコンがあるかもしれませんし、暗号化ソフトを入れたはずなのに削除されたパソコン(OSの再インストールなど)があるかもしれません。

本章では、「安心」と「安全」について議論します。一見似たような意味に使われがちな2つの言葉ですが、それらの違いを論じ明確にした上で、自社の組織の現状と目標を設定することが、「我々はどこまでやればよいのか?」に対する答えになります。

まず、「安心」とは、普通に使われる場合、情緒的な言葉であり、その意味は人によって異なります。ある人は、暗号化ソフトを配布したのだから大丈夫だろうと思うかもしれませんが、しかし、それで大丈夫だろうかと不安に思う人もいるでしょう。「安心」を対策のめざす拠り所とするとゴールが曖昧になり、誰も自信をもって「うちは大丈夫だ」と言えなくなります。

一方、「安全」という言葉はどうでしょう。「安全対策基準」などと呼ばれるように、「安全」は、ある関係者のなかで客観的な基準を設けて測定し、共通認識を持つことが可能な言葉です。情報セキュリティ対策は、最終的には、ある組織に関わるすべての当事者が「安心」を得ることを目標とすべきです。ただし、そのためには、まず「安全」の確保を前提と考えるべきです。情報セキュリティマネジメントシステムによるPDCAサイクルのなかで必要なセキュリティ対策を実施し「安全」の確保を図っていくことが重要です。

NECでは、2001年に出現したウイルス(CodeRed、Nimda)により社内のネットワークが過負荷により使用不能状態が発生し、大きな被害を経験しました。すぐさまIT部門を中心として対策が検討され、CAPSと呼ばれるウイルス対策システムが開発されました。このシステムは、社内のすべてのパソコンのセキュリティパッチの適用状況、ウイルス対策ソフトの導入状況、パターンファイルの更新状況などを集中管理するものでした。CAPSシステムが稼働し始めると、新たなウイルスが出現しても、社内のどのパソコンが感染の可能性があるのかを的確に把握することが可能となり、事前にセキュリティパッチの適用が可能となりました。このシステムは、「安全」な環境を実現したと言えます。それと同時に、IT部門に「安心」をもたらしました。「ウイルス感染」の可能性を定量的に把握でき、ウイルス感染が広まる前に安全域(社内ネットワーク、業務システ

ムに影響の出ない状態)へ抑え込むことが可能になったからです。「数えるマネジメント」で述べた定量把握の効果です。

ところがこのシステムは、さらに大きな効果をもたらしました。従業員は、日々、新しいセキュリティパッチが配布されると自分のパソコンにその適用を促す指示が表示され、指示に従ってセキュリティパッチを適用します。すると、一人ひとは、自分がセキュリティパッチを適用すると同時に、社内の誰もが同じようにセキュリティパッチを適用していると無意識に思い始めました。社内のほぼすべてのパソコンは、常に最新のセキュリティパッチが適用されていると思えるようになりました。すなわち、社内のネットワークにウイルスが感染する脅威は非常に低いと感じるようになり、IT部門のみならずすべての従業員が、社内のネットワーク環境に対し安心感を抱くようになりました。今では、社内のネットワークがウイルスに感染し大きな被害が起きるかもしれないという不安は、誰も持っていないと思われま(実際には、ゼロデイアタック等脅威はますます大きくなり、IT部門の緊張は続いてはいますが)。

このNECの例は、「安全」を確保するために構築したシステムが、いつの間にかそこに関わるすべての関係者に「安心」をもたらした一例を示しています。この例で、「安全」から「安心」へ変えた原動力は何でしょうか。それは、システムに対する信頼感の醸成です。このシステムで集中管理していれば、新しいウイルスが出現しても大事には至らないという想いを、全従業員が実感することができたから、社内に「安心」が生まれたのだと思います。めざすべき「安心」とは、このように「安全」を確保した上で、その組織に関わるすべての関係者が「信頼」を実感できたときに得られるものです(図3)。安全な環境は必須ですが、同時に信頼も欠かせません。どちらが欠け

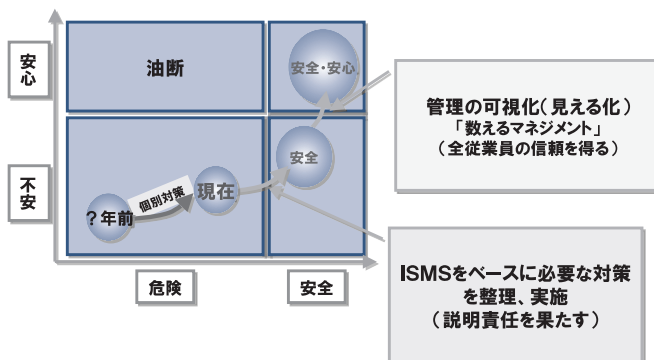


図3 安心 = 安全 × 信頼

ても「安心」というゴールにはたどり着かないと思われます。

5. 信頼できる環境の実現のため、ITに何をさせるべきか

本章では、「ウイルス対策」から「情報漏えい対策」という、より広い概念について、同様に「見える化」のアプローチを適用する方法について論じていきます。第4章で述べたように、NECのウイルス対策システムでは、すべてのパソコンのセキュリティパッチの適用状況を把握し、感染の脅威があるパソコンがどこに何台あるかを集中管理しました。これにより、危険なパソコンの所有者に直接指示することが可能になり、効果的にセキュリティパッチの適用率を向上することができました。これは「数えるマネジメント」と呼ぶ脅威、脆弱性の可視化(見える化)を図る例です。

現在、情報漏えい対策が情報セキュリティにおける重要課題であることは言うまでもありませんが、「情報漏えい」対策の可視化(見える化)を図るための定量把握は、ウイルス対策に比して容易ではありません。いったい何を数えると「情報漏えい」という脅威を未然に防ぐ効果的な指標になるかという課題があります。内部犯行、うっかりミスなどにより引き起こされる情報漏えい事故に対し、入退場管理の強化、ネットワーク接続時の認証強化、秘密情報のアクセス制限、暗号化、事故発生時の原因究明のための操作ログ採取等々、その対策は枚挙にいとまなしです。

誰が、いつ、何をアクセスしたかの記録のみならず、秘密情報を含むファイルの数、アクセス数、メールへの添付数、印刷枚数、外部媒体へ出力したファイル数などを日ごろから数えることにより、通常と異なる動きが可視化されるかもしれません。最近では、この領域への適用をめざしてデータマイニング技術も進展しています。

ただし、これらも現状を把握(アセスメント)し、CIAの観点で実施すべき対策とその実施計画を策定し、そのなかで単に対策の積み重ねでなく、定量把握をベースに「数えるマネジメント」によるすべての関係者に対しマネジメントの可視化(見える化)を図る仕組みを埋め込んでいくことが重要です。ITの活用は、まさに定量把握の自動化、稼働状況の可視化(見える化)において活躍の場があります。

ますます大きくなるばかりです。重要なのは、情報セキュリティマネジメントシステムを構築し現状把握の上に実施計画を策定し、その上で様々なセキュリティ対策を実行・運用することですが、本稿では、同時にすべての関係者が「信頼」できる管理体制をめざすことが、「安全」から「安心」へステップアップさせるということを説明しました。

執筆者プロフィール

伊藤 慎
システム・サービス事業本部
ニューソリューション開発本部
部長

6. むすび

情報セキュリティ事故による組織の影響、社会的影響は、