総論

情報セキュリティ
～守りから攻めへの変革の時～

日本電信電話株式会社
研究企画部門
チーフプロデューサ
影井　良貴

はじめに

情報セキュリティ対策というと、なにか非常に後ろ向きで、できればやりたくないものという感じで捉えられていることが多いのではないだろうか。情報セキュリティ対策には、できるだけお金をかけたくないのに、問題があるたびに計画外の出費があり、どこまでやればよいかもわからず、先が見えないといったような意見も良く聞く。この状態を打破すべく、再度情報セキュリティの何であるかを考え、視点を転換することにより、「もっと主題的に考えていくことにより効率的にできるもの」、「守りの情報セキュリティから攻めの情報セキュリティへの認識の転換」を推進したい。ここ数年実施してきた個別の対策が一巡した今こそ、この変化を進める良い機会なのではないか。

情報セキュリティに対する考え方の相違

現在の情報化の成り立ちについては、２つの大きな流れからきていると考えている。１つはインターネットを起源とするものであり、もう１つは情報処理システム系を起源とするものである。この２つには、もともとシステムに対する根本的な考え方の相違があり、その違いが情報セキュリティ対策への考え方の違いのもとになっている。

1. インターネットを起源とする情報化の流れから見て

まず、インターネットを起源とする情報化という観点である。この場合には、通信を想定したものである。従来の通信というのは、電話機相互間を交換網で接続するという形態を頭に描きながら利用しているわけである。従来の電話網の機能のうち、利用者宅に設置している電話機の機能は、専ら接続のために必要な番号情報の送出と、音声から電気信号へ、およびその逆の変換に特化している。電話が使えなくなると、電話局に（別の電話で）連絡することになる。

また通信の漏洩を防ぐには、小声で話すくらいであり、その他は利用者宅の外の通信業者の役目である。このため、通信手段がPC等に置き換わったとしても、そこでは利用者はあくまで利用者であり、自分で情報を守るという意識は非常に希薄である。セキュリティに投資をするなんて到底考えられないことであり、もし対策をしなくてはらないならば、できるだけ投資は抑制したいと考えることになるのは、この経緯を考慮すると仕方が無いことかもしれない。

現在のコミュニケーションの中核技術であるIP（Internet Protocol）技術自体は、もともと軍事用に開発されたものであり、利用に当たってはセキュリティも十分確保されていた。実際その時の利用方法は、専用線（地上回線、衛星回線等）を中心にして関係者だけを結んだネットワークの中での使用であった。それを軍事だけでなく商用に展開して利用し始めた時に現在の問題は始まったといってよい。

2. 情報処理システムを起源とする情報化の流れから見て

一方、情報処理システム系における考え方は全く異なっており、その異なった設計思想に基づいて構築されてきている。それは、情報システムは故障するものであり、元来不具合が内在するものであるということ

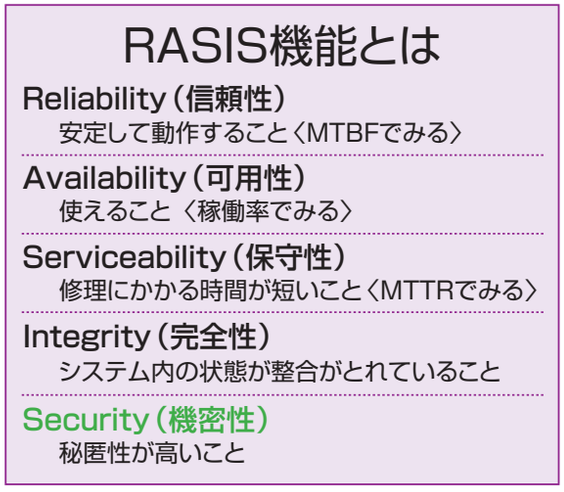

図１　RASIS機能

を前提に設計されていることである。ここまで情報化が進んでくると、当たり前のようにコンピュータを企業活動や個人生活に利用しているが、その要求条件にアプリーケーションソフトウェアへの機能要件に加えて、システム全体の信頼度等の要求を個別に行うことは、徐々に少なくなってきているように見える。事業としてサーバを利用している企業でさえ、信頼性はベンダーに依存して、ほとんどアプリケーションの機能の具備だけに特化しているのではないだろうか。いわんや、電話の延長でしか考えていない個人ユーザに至っては、もともとセキュリティは考慮しなくても良いものであるべきと考えていると思ってよい。

このような不具合を前提とした情報処理システム系の設計思想に従ってシステムに作りこまれる機能に、RASIS機能（図１）というものがある。

3. RASISとは

RASISとは、

- Reliability（信頼性）
- Availability（可用性）
- Serviceability（保守性）
- Integrity（完全性）
- Security（機密性）

の５つの機能の頭文字をとった言葉であり、それぞれの言葉の意味は、図１に書いてあるとおりである。情報処理の分野でシステム作る際には、例えば銀行の勘定系システムであれば、預金等の機能をシステムとして作りこむのは当然として、そのほかにRASISの機能をも作りこむのが常識である。RASIS自体は、もともと信頼性工学の言葉であるが、この５つの機能のうちの１つがSecurityであり、もともとシステムの構築に当たって、最初から作りこむべき機能として定義されているわけである。

どのくらいの稼働率を目標にするのか、故障した場合の復旧方法はどのようにして、復旧時間はどのくらいか、またどのようにして情報の正確性を保証し外部から秘匿を行うのか、などを決めてRASIS機能として作りこむわけである。

情報セキュリティを取り巻く環境

実際の情報セキュリティ対策については、技術論では語れない部分が大きいものである。もともと、どのようなセキュリティが必要なのかという要求条件は、当然周囲の状況や常識に従うものでる。

1. 法制度に基づく情報セキュリティ対策

昨今では、法制度上の規定で情報セキュリティの要求条件が決まるようになってきた。

その代表的な例としては、個人情報保護法（正式には「個人情報の保護に関する法律（平成15年５月30日法律57号）」）や、JSOX法（正式には「金融商品取引法　平成18年６月７日」といい、証券取引法を改題したものである）等がある。この中では、個人情報の扱いや情報システムの内部統制について規定されている。

個人情報保護法は、住民基本台帳ネットワークが作られることになった段階で、個人情報の管理を厳しく行うことを求める世論に応じて作られたという経緯があり、その時の議論の結果として、かなり厳しい規定が採用されている。

JSOX法については、その名前が示すように、米国のSOX法の日本版である。SOX法自体は、米国エネル

ギー企業のエンロンの粉飾決算等を発端に企業の内部統制の正常性の担保を経営者に義務付け、投資家保護を推進するためのものであり、本法案の提出者であるPaul Sarbans氏をMichel G.Oxley氏のにちなんでサーベンス・オクスリー法といわれている。

日本版のJSOXの特徴は、各企業の情報システムについてもその処理が問題ないこと、間違いないことを担保することを求めている点にある。その意味では、情報システム内部の種々の処理結果が改竄されていないことをどのように証明するのかなど、少し従来とは異なった観点での情報セキュリティ対策も考慮しなくてはならなくなってきている。

2. 技術的未成熟に対応した情報セキュリティ対策

電話というのは、長い技術開発の蓄積と運用実績の上に成り立っているものであり、かなり完成度の高いものであった。それに比べ、現状のPCやサーバベースのシステムというのは、もともとスタンドアロンのPCやUNIXマシンが急速にネットワークに接続されてできてきており、その技術は未成熟であり、その運用実績の蓄積も少ない。さらには新しい利用方法が次々に創出されており、未知の部分はどんどん拡大しているといってもよい。

このような技術に基づく現代の情報システムは、その技術の未熟さゆえに、その技術を採用することにより必要となるセキュリティ対策もある。代表的なものは、コンピュータウイルスの類である。コンピュータウイルスは、ソフトウェアの脆弱性を狙ったものであるが、相手先から不正プログラムを仕込まれる可能性があり、それを内部に置かれた後には、不正なプログラムが動作して、システムを停止させたり、誤動作させたり、外に情報をばら撒いたりということになる可能性がある。このようなことを防ぐには、現在のPCのアーキテクチャを現在のネットワークをベースとした状況に最適な、アーキテクチャに変更することにより技術的には対処可能であるが、実際には従来の基本的な方式を急に変更することは不可能である。したがって、現状ではPCにはウイルス対策ソフトを常駐させる必要がある。しかも、それは次々に出てくる新しいウイルスに対応できるようにするため、毎日のようにアップデートが必要である。企業においては、不正な情報が侵入してこないようにファイアウォール装置などを設置している。

さらに、最近の動向としてスパイウェアという新手の不正プログラムが流行りつつある。これは、正規のプログラムのインストール手順に則ってPC内部に知らない間に取り込まれるソフトウェアのことであり、人間がインストールをする限り技術的には防ぎようの無いものである。

このように技術的にまだ未成熟なものを利用しているために、採用しなくてはならない情報セキュリティ対策もある。

3. 社会のマナーの変化に対応した情報セキュリティ

PCの電子メールを利用している人のほとんどが困っているのはスパムメールであろう。スパムメール自体が直接悪さをするということは無いが、その量が半端ではなく、業務に支障が出ている人は多いのではないか。電話の時代にも間違い電話やいたずら電話というものがあったが、現状の発生頻度に比べると、はるかに少なかった。間違い電話については、一月に1回くらいあれば多いなと感じたのではないかと思うが、スパムメールは日に数十通から百通くらい到着する。スパムメールの問題は、それにフィッシングサイト等への誘導情報が含まれている点であり、その罠にはまった場合には時間的な損失だけでなく、情報漏洩のような実害が発生しうるということも重要なことである。

また、DDoS攻撃のように、非常に多くのアクセスを一箇所に集中させて、そのサイトがサービスできないようにしてしまうことも発生している。電話のときも人気ミュージシャンのチケット発売直後は、電話交換機がパンクして繋がらなくなるということはあったが、それを意図的に行うようなことはなかった。

さらには、URLの売買等が可能であるため、JPドメインが必ずしもJPにあるとは限らない、COMは米国企業には限らない等、当初のルールと実態がずれて

いることもある。

これらは、利用者の社会的な規範が現在の情報化の仕組みによって変わってきていることを示している。そのような行動に対応するための情報セキュリティ対策も施さなくてはならない。

4. 現在のICT社会の本質的課題に対応する情報セキュリティ

前述のようないろいろな現象についていろいろな情報セキュリティ対策が必要になってきているが、現在のICTを駆使した社会の本質的な課題は、人間の能力で把握できない状況になっていることである。メールにしても、Webシステムにしても、人間の相手は機械である。人間は、音声を主体とする電話による通信では、たかだか3.4kHzの狭い帯域を通した品質の悪い通話であっても、その話し方や内容から相手が知り合いかどうかをほとんど判別が可能である。しかし、機械は一定の反応しかできないため、正しい機械かどうかを人間が直接確認する術は無い。

また、現在の印刷はいわゆるプリンタによるものが主流であり、その印刷自体の真贋判定は難しい。その他、カラーコピーを利用した場合には、人間の目では判別できないような複製ができる。

さらには、コンピュータの中で何か行われているのか認識することもできない。今スクリーンに映っているジョブだけが実行されているわけではなく、バックグラウンドではどのような処理が実行されているのかは認識できない。例えばどこかのサイトを閲覧した時には、裏ではクッキーが作られ、自分の行動が記録され、読み出されているということ認識する術はない。ということは、コンピュータがある役目を果たした時、その結果の正常性判定や真贋判定もコンピュータに頼らなくてはならないということで、従来の人間の能力を中心に頼りにしていた対応は、既に困難な社会構造になってきたということである。

継ぎはぎだらけの情報セキュリティ

このように見てくると、現在の情報セキュリティ対策というのは、各課題が表面化した段階での個別対処の固まりになっていると考えられる。実際に次から次に新しい問題が出てきて、それに対する対策が次から次へと出されているのが現状である。

このような状況を見る限り、情報セキュリティ対策というのは必要なものではあるが、問題が無いのならば、本当は対策なんかしたくないものであるという気持ちになることは理解できる。また情報セキュリティ対策というのは、どこまでやったらよいのかがわからず、際限なく対応をしなくてはならないものなのではないかという気持ちになることもわかる。このような状況を繰り返していく限り、我々は情報化に翻弄されている被害者にしか思えない。

本当の情報セキュリティとはなにか

最初に述べたように、RASISの機能の一つである情報セキュリティというのは、元来情報化を進める際に最初から作りこむべき機能なのであって、単なる個別の問題解決の手段の集合体ではないはずである。

であるので、情報化の最初の段階で作りこむ機能としての情報セキュリティの定義を、ここで以下のように見直しすることにする。

「情報セキュリティは、情報の流れを制御する機能である」

具体的にいうと、どの情報をどの範囲で流通させるのか制御する機能ということである。これは反対の言い方では、意図した範囲以外には情報を出さないように秘匿する機能となるわけであり、従来の情報セキュリティと同じではないかと考える人もいると思うが、反対に言うことによって、もっと積極的に情報セキュリティ機能を導入すべきであるということがわかると思う。

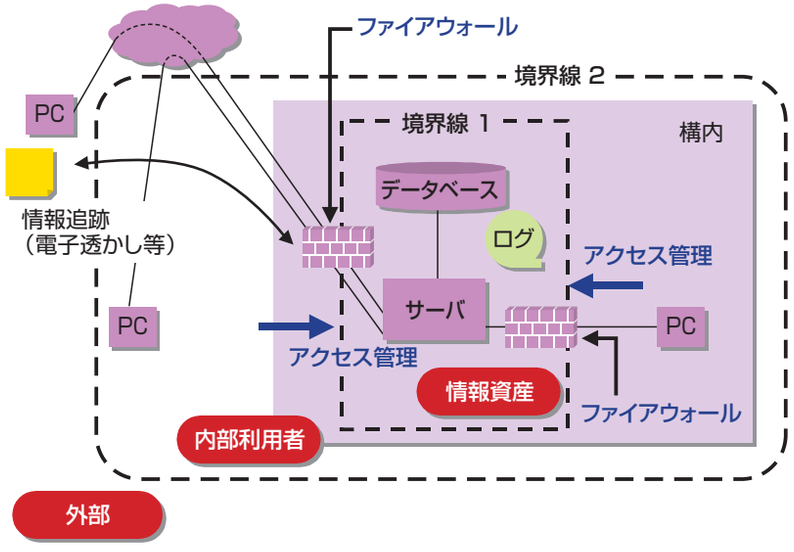

図２　セキュリティ基本的構造

もともと完全なオープンな情報以外は、各企業や個人が所有している情報を知らせる範囲は自分でコントロールすべきであり、それは被害者的な意識の中での対策ではなく、もっと肯定的に自分で自分の情報の流通をコントロールするという元来必要な機能として考えることができる。このような発想の転換を行い、情報セキュリティの攻め方を考えていくことが重要である。

情報セキュリティの基本的構造

前述の情報セキュリティの再定義に沿って、情報化における情報セキュリティの基本的な構造について述べる。

図２に示すような2重の境界線に囲まれている構造を考える。境界線1に囲まれた領域は、情報のデータベースや中核の処理機能であり、境界線２に囲まれた領域は、境界線１に囲まれた情報資産にアクセス可能な利用者やその利用者が使用している機器類である。その外側はそれ以外であり、情報のやり取りがある場合も、完全に無関係な場合もある。

この構造の中で必要な機能は大きく５つである。

（１）アクセス管理機能

（２）境界におけるファイアウォール機能

（３）操作ログの取得と管理機能

（４）情報の追跡機能

（５）各装置の維持管理機能

以下に、これらの各機能についての概略を説明する。

（１）アクセス管理機能

アクセス管理機能には大きく二つある。

一つは、境界線１に囲まれている情報資産の領域へのアクセスの管理機能である。従来は、外部のネットワークからのアクセスだけを管理していた。社内の端末は、基本的に信頼に足るものと考え簡単にアクセスできる形で運用していたが、現在では社内LANへ不明なPCが接続される危険性等を排除するために、社内のPCも一台一台管理しアクセス権の確認をすることが求められてきている。特に、無線LANでの収容形態を採用している場合には絶対に必要な機能である。その他、正規のPCであってもウイルスに感染している可能性を排除するために、ウイルス対策ソフトが最新にアップデートされているか等をチェックする検疫機能を具備することも重要になっている。

もう一つは、個別の情報や機能へのアクセスの管理である。組織単位や個人別等により、必要な情報や処理

以外にはアクセスできないように管理する機能である。

これらのアクセス管理機能は、攻めの情報セキュリティ機能の一番基礎的な機能である。

（2）境界におけるファイアウォール機能

基本的には、境界線1のところでの外部との接続点で、各種の攻撃に対する対策を講ずる。侵入防止、ウイルス対策、スパム対策、コンテンツフィルタリング等の機能をこの部分に置く。それによって不正な情報が侵入しないようにする。

（3）操作ログの取得と管理機能

情報資産に対する各利用者の行動記録を取得し、それを保存する。いつ誰がどこからアクセスしたか。どの情報に誰がいつアクセスしたか。印刷状況や記録メディアへの保存の状況。メールの記録等を取得して保存する機能である。これは、情報資産に対する異常が発生した場合に、その原因を特定するために必要な機能である。さらには、その記録が法廷闘争等に使用されることも想定される。その場合には、非改竄性の証明として、タイムスタンプ等による証明が必要になってくる。

（4）情報の追跡機能

境界線2から外へ出した情報や、境界線1から何らかの理由により漏洩した情報が、自分の所有していた情報かどうかが確認でき、また、いつ誰に開示した情報であるのかを確認できる機能である。これには、情報の加工による初歩的な方法から電子透かしのような高度技術による方式等がある。

（5）各装置の維持管理機能

これは、PC等のソフトウェアのアップデート機能やウイルス対策ソフト等のように、もともと各構成装置類の状態を正常に保つための機能である。

以上を情報セキュリティの基本機能として作りこむことにより、必要な情報資産を正規の権限を持った利用者だけがアクセスでき、万が一問題が発生した場合には後日状況の把握ができ、原因の特定ができるようになる。また、この基本構造をセキュリティポリシーとしてそれぞれの機能の定義を明確化することにより、本来必要な基本的な情報セキュリティ対策を決めることができる。この考え方の良いところは、必要なセキュリティ機能を明確に定義できるところである。この定義を作ることは、どの情報を誰に伝えるべきかを明確にすることになるわけであり、何らかの関係で採用すべき技術等に関して迷った場合には、原点に立ち戻って何をしたかったのかという基準に照らして、なすべきかどうかを判断できることになる。それは、脅威に対する対策ではなく、あくまで自分の思いのままに情報資産をコントロールできるかどうかという観点での検討になるわけで、それは決して被害者的対策ではなく、もともと必要な機能としての検討として肯定的に捕らえることができる。

最後に

以上のように情報セキュリティは、もともと情報化を行う上で必須な機能であり、防戦のための消極的な対策ではなく自分で情報の流通をコントロールするための機能であって、積極的な機能として捉えるべきものであるということを述べてきた。自分の情報の価値を維持するための機能であって、外部から強要される機能ではなく、独自に能動的に具備すべき機能である。

現状のような次々に起こる課題への対処をするために、年度当初の計画にはない想定外の支出を余儀なくされるような情報セキュリティ対策に振り回されるのではなく、自分の手の中に情報のコントロール権を取り戻すために、他の機能への投資と同様に年度計画のうちの一定割合を情報セキュリティ機能のための投資として確保することが重要である。

これまでの経験を活かし、自分の情報化戦略に適した情報セキュリティ機能を、自ら構造的に設計構築していく方向に転換する時期に来ているのではないだろうか。