総　論

情報セキュリティのCIA＋α

前・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（セキュリティ）
影井 良貴

情報セキュリティとは？という質問に対して、一般的な共通認識として秘匿性、完全性、可用性の３つ概念が定義されている。最近では更に真正性、責任追跡性、否認防止、信頼性という言葉も出てきている。今回は、それぞれの意味と、それを解決するためのキーワードを説明し、これからの情報セキュリティについて、何をしていけばよいかについての基本的な方向感を示す。

CIAとは

CIAというと、一般の方は米国中央情報局（CIA：Central Intelligence Agency）を考えると思う。やっぱり、情報セキュリティというのはスパイの世界の話なのか、と思うのは間違いで、情報セキュリティの分野でのCIAとはConfidentiality（秘匿性）、Integrity（完全性）、Availability（可用性）の３つの機能の頭文字である。CIAは現在、情報セキュリティの三大理念と言われ、ISO 7498-2:1989（JIS X 5004:1991）の中で定義されているものである。

これは、OECD（Organization for Economic Cooperation and Development：経済協力開発機構）においても情報セキュリティの基本概念として「可用性」、「機密性」、「完全性」を説明し、この３概念を使って「情報システムセキュリティの目的は、情報システムに依存する者を、可用性、機密性、完全性の欠如に起因する危害から保護することである。」と解説している。

Confidentiality（秘匿性）

情報セキュリティという言葉から考える機能としては、秘匿性が一番目であろう。現在の社会的な関心事である個人情報の保護の観点からも、漏えいから守るための情報セキュリティというものが注目されていると同時に、セキュリティの主要な基本技術である暗号という言葉からも、秘匿性というのは誰でも情報セキュリティの重要な機能であると考えるだろう。しかし、ここでいう秘匿性というのは、隠すことだけを言っているのではなく、権限を持った者がアクセスできる状況の中で、権限のない者からは確実に秘匿できることを求めている。

その意味では、いわゆるアクセスコントロールが十分に機能していることが、秘匿性のポイントである。現状のアクセスコントロールでの課題には大きく分けて２つある。一つは、認証方式の仕組みの課題であり、もう一つはきめ細かい権限の設定の困難さである。

一般にアクセス権限を認めるには、その者が誰かを認証（Authentication）し、その者に付与されている権限を認定（Authorization）するという２つの手順を踏むことになる。最初の認証の部分の方法論として、一般的なID/Passwordによる方式やICカード等の持ち物による認証方式が採用されてきたが、最近は指紋のような生体認証がだんだん取り入れられて来ている。従来の方法の課題は、盗用による成り済ましが容易であったということである。それに比べ生体認証系は、もともと個人の生体としての固有情報に基づくものであり、なかなか生身では他人に成り済ますことは難しい。しかし、これでさえ、偽の指を作るなど技術的な仕掛けにより破られる可能性はあるし、現在の生体認証の精度では100％大丈夫というわけではないという意味では、一長一短というところである。

認証方式において、確実性と操作性は、トレードオフ的な関係にある。銀行のキャッシュカードの中には、生体認証を用いて個人を確実に認証しようとしているものもあるが、家族が代理でATMを操作しようとするとできないため、不便だという意見は多い。では、どっちでもできるようにしようすると全体のセキュリティ強度は落ちてしまう。

また、システム毎にID/Passwordが異なって非常に煩雑なため、最近話題なっているのがSSO（Single Sign On）である。これは非常に便利であるが、逆に1つ漏れればすべてにアクセスできてしまうという危険が増大することになる。

このようにみると、実際には要求されるセキュリティの高さに応じた方式を採用するが、必要に応じて他方式と組合せたり、2人で一緒に認証することを条件にしたりするような対策をとることになる。

もう一つの課題である権限の設定の複雑さであるが、この課題の根源はいろいろある。各個別の情報の重要度の設定が複雑であること。情報と処理が必ずしも1対1対応していないこと。組織とポストと権限が非常に流動的であることなどに依ってその複雑さが発生する。

情報の重要度の設定については、一般的には情報の作成者がその任に当たることが多いが、その設定が正しさのチェック機構が抜けている場合が多い。またアクセス者と権限との対応をつけるためには一般的にACL（Access Control List）のようなものでそのコントロールを行うが、通常はドメイン、サーバ、フォルダ等の情報の置き場所単位での指定までが普通である。また、現在の社会の変化は早く、人の異動も激しくなり、組織の再編も頻繁に行われるようになっていることも、より困難にしている要因になっている。現在の技術レベルでも、代理決裁くらいはできるようになっているが、細かい制御は難しく、各組織の中で実践を積み重ね、一番良い方法を作り上げていく必要がある。

Integrity（完全性）

Integrityについては、保全性という訳も使われているが、私はより広い意味での完全性という訳が良いと考えている。

完全性とは、情報が正しく保持されていることである。意図せず変化したり、改ざんされたりしていないことであり、これはいわゆるデータだけでなく、処理ロジックが改ざんされていないことも含まれる。また、元々の処理ロジックそのものの正しさも含まれると考えるべきである。意図しない結果を生むことがないよう、必要な情報や処理について、それが正しいことが要求されるわけである。

情報やプログラム等が正規のもの（改ざんされていないもの）であることを技術的に識別するための技術には、良く知られている電子署名というものがある、ある情報のビット列に対しハッシュ関数と公開鍵暗号を使って電子的に署名を行うものであり、元の情報のどこかを変更したらそれを検知できる。最近では、ネットワーク経由で配布するプログラム等も正規のものであることを保証するために署名が付けられていることが多い。

昨今のように、各企業間でいろいろな情報が飛び交っている状況を考えると、完全性は自己の内部の情報等だけを見ていても不十分であり、情報が流通する範囲内での完全性を求められていることに注意すべきである。

Availability（可用性）

可用性とは、必要な時に所期の情報にアクセスできること、利用できることである。この場合の前提として、権限を持つ者がアクセスしたときに限りということは、前述の秘匿性が要求していることから自明である。この可用性だけは、他の二つと多少異なっている。他の二つは、どちらかというと制限を作る機能であるが、可用性は制限をはずすような機能である。どれだけ秘匿性が高く、また完全性に優れたシステムでも、使いたい時に使えないのでは全く意味がない。その意味では、利用者側の立場に立った場合の理念であり、要求である。

可用性というのは、使いたいときに使えるというものであり、常時使えるようにしておくということではないことは注意すべき点である。24時間365日（ちょっと、脱線。米国ではこれを24hours7daysと表現します。これは日曜日でもやっているということで休みなくということを表現しているわけですが、日本では年中無休という年単位の表現が一般的です。日本人の方が気が長いとい

うことでしょうか）ではなく、使いたいときには使えるということを、サービスの提供条件としてどのよう扱うかは、良く考えるべきである。

■ 他の機能について ■

ISO 27000シリーズの中では、前述の三大理念に加えて、

- Authenticity真正性
- Accountability責任追跡性
- Non-repudiation否認防止
- reliability信頼性

の4つを加えてもよいとされている。

（1）真正性

真正性とは、利用者、プロセス、システム、情報などが本物であることを確実にするということである。

現在のようなネットワークを介したやり取りの中で、これを確実に行うためには、特定のグループ内の場合は、合言葉でも決めておけばよい。しかし、任意の2者間モデルになったとたんに、事前の取り決めができなくなるため、絶対的に必要になる存在がTTP（Trusted Third Party ： 信頼できる第三者機関）である。TTPとして現在の代表的な存在は、電子証明書の発行局である。国内でも、民間の企業もあれば公的個人認証のように行政が行っているものもある。信頼できない相手とのやり取りを行うわけであり、そこには必ず信用できる第三者の主体が必要となる。

話は少し飛ぶが、日本国内の実社会でいろいろな取引や契約が行われているが、その場合でも法人の登記簿や戸籍謄本の提出を要求されることがある。国内では、これらの書類は結構しっかり整備されており、その書類に疑義を挟む余地はほとんどない。しかし、問題は、物理的な個人の身分証明がないため、その書類とその人間の関係の保証は甚だ心許無いということである。これが振込め詐欺の温床である架空口座に結びついていることは、明らかである。実社会でもこんな状況であり、さらにネットワークを利用した社会になれば、この真正性の確保というのは非常に重要なことになるのは当然である。

現在、法人の実存を確認して証明するサーバ証明書等については、金融機関を中心に利用されてきているが、近い将来、個人やデバイスも同様の真正性の確保が重要になってくると考えている。

言っておくが、このような真正性の確保は、ある種の匿名性の排除ということになるが、これは、必要な場合にこれができればよいのであって、すべてのネットワーク内の活動に真正性を導入すべきと言っているのではない。要は選択できればよいのである。互いに必要だと思った時、確認ができれば良いのである。

（2）責任追跡性と否認防止

責任追跡性とは、何らかの処理ややり取りがどのようにされていたかを後で順を追っていけるようにすることで、否認防止というは、その処理ややり取りについて後になって知らないといわれないようにすることである。

これは、別々の機能として定義してもよいが、組織内では責任追跡と言い、組織間では否認防止と言うことになるわけで、私自身は同一視してもよいのではないかと考えており、合わせで証跡管理性とでもいうべきではないかと考えている。

証跡管理性とは、どの主体が、何時、何処で、何をしたかを証跡として残し、それを管理することにより、後日の確認を可能とするということである。

具体的には、何時、何処で、何をしたかであるので、重要なのは、時刻と主体の認証と情報の非改竄性の3つである。誰（何所）と誰（何所）の間で、何年何月何日何時何分何秒に、どのような情報のやり取りがされたかを、残すことが必要である。

主体の認証については、もともと三大理念のひとつの秘匿性に含まれており、その必要性については、前述の通りである。また、情報の非改竄性についても完全性に含まれており、これも既述である。従って、残る証跡管理性に必要な機能が時刻で、これらが揃うことで情報を管理して、後から確認のために使えるようにできるわけである。

時刻というと、PCの内部の時計は、最近では標準時に合わせるようになってきたが、昔はPC内部の自走の時計を使っていた。従って、時刻はずれて、精度もバラ

バラであった。年月日も好きなように設定できる。やろうと思えば1年前に遡ることもできるのである。このような状況の中では、何時発生した事象かということは証明できない。これでは事象の前後関係が明確にできず、証跡管理性などは到底実現できないのは明白である。

最近、時刻認証という技術が発達して、一部的であるが、その法的な根拠も整備されつつある。これこそが今後の重要な証跡管理性の技術となることは間違いない。

（3）信頼性

信頼性については、よくその言葉は聞くと思うが、いわゆるシステム等の信頼性だけでなく、いろいろなプロセスが意図した動作や結果となっていることを指している。

三大理念の中に可用性があった。それは利用したいときに利用できるということであり、信頼性は意図した通りに動作しているということである。この2つは同じようなことを言っているわけであるが、可用性は利用者側からの発想であり、信頼性は提供者側からの発想である。

提供条件としての可用性は、同様のサービスが複数存在し選択できる環境を前提とするならば、利用者の意思決定事項と考えられるが、選択した後の利用している状況では、信頼性を実現するのは供給者側になるわけで、サービス提供者側での信頼性への取組みは大変重要なことであり、この概念を除いて考えるべきではない。

とかく、現在のサーバベースのシステム開発においては、ありもののハードとソフトを組み合わせて開発するという形態が多く、もともと必要な信頼性設計を行っていることは少ないのではないか。パッケージソフトを前提にするならば、それが動作する環境は、自ずと決してくる。そのハードやOS、ミドルウェアなどを組み合わせてできる範囲の信頼性、ということではないか。

さらには、信頼性を考える上で、二重化等とかMTTR（Mean Time To Repair）を短くする仕掛け等、いわゆる保守性（Serviceability）も信頼性と同様に考慮すべきである。

■ 情報セキュリティへの基本的考え方 ■

以上のように、情報セキュリティとは、という問いに対する共通認識の整備は進められてきている。

秘匿性、完全性、可用性については一番基本的なものとして、その他として真正性、証跡管理性、信頼性等々も加えてもよいとされている。

ここで、良く考えるべきことは、これは情報セキュリティの概念であるということだ。決して情報システムのセキュリティの概念ではないということだ。秘匿性にしても、完全性にしても、可用性にしても、これは、紙ベースの情報についても同様のことが言えるということである。ということは、企業や組織の情報セキュリティのあるべき姿はここにあるということである。これらのプロセスを社内のシステムとして実現したら、それには技術的な対応が必要だろうし、外部とのやり取りをシステム化したらば、それに応じた対応が必要になるということである。

また、可用性まで含めた概念であるということは、利用できることが重要であるということである。行き過ぎた保護により、必要な時でも情報を使えないような状態では意味がない。最近の個人情報保護の行き過ぎのようなものは、今回の情報セキュリティの概念から見れば良くない状態にあるということができる。

このようにいうと何かおかしいように思えるかもしれないが、もともと情報というものは、それを保持することが目的ではなく、その情報を利用して何かを行うためのものであって、必要な時に利用できない状況は、そのほうがおかしいというべきである。

しかし、情報の利用については、その情報の提供者と利用者がいるわけであり、それぞれの思惑が交差している状況での利用になるわけである。従って、一律の情報セキュリティの決まりですべてが動くということではなく、関係者の考え方の調整の上に成り立つべきであるともいえる。

このように考えてみると、私が従来から言っているように、「情報セキュリティというのは、情報を自分でコントロールすること」であり、どのようにコントロールすべきかという概念を定義しているのが、前述の情報セキュリティの概念であり、その概念の実現に必要で、情報を自分の管理下に置いてコントロールできるようにするためのものが、情報セキュリティ技術であるといえる。