（１） CIA について

CIA というと、どうしてもアメリカの中央情報局を思い出しますが、実は、情報セキュリティの基本的な考え方も CIA といいます。C は Confidentiality の C で機密性、I は Integrity の I で完全性、A は Availability の A で可用性の頭文字をそれぞれ取っています。

機密性とは、社外秘の情報を外部に漏らさないようにするなど、情報の利用権利のない不正な利用者からのアクセスを防ぐことで、盗聴や不正アクセス、不正利用から情報資産を守ることです。

完全性とは、利用すべき情報が正当、正確さ、網羅性、一貫性が保たれているようにする、ということで、情報が改ざんがない、情報の部分的あるいは全体的なデータ破壊、意図しない変更が無いようにすることです。

可用性というのは、ややもすると情報セキュリティという観点からは軽視されがちですが、情報を利用したいときにいつでも正常に利用可能となるように適当な方法で保管したり、提供可能な状態に保つことです。

情報セキュリティというと、機密性、完全性という、盗聴、成りすまし、不正アクセス、改ざんを防止するための取組みに重点が置かれがちですが、情報というのは、有効に利用してはじめて資産としての価値があるわけですから、可用性を損なうような情報セキュリティというのは、本末転倒と言わざるを得ません。情報の可用性が軽視されている情報セキュリティ管理の実例を少し紹介したいと思います。最近、情報紛失の危険性を回避するために、USB メモリー利用の制限をしている企業が少なくありません。もともと USB メモリーは情報を手軽に持ち運べ、非常に便利な情報処理ツールであり、情報の活用のためにも有効な機器です。しかしながら、セキュリティの観点からは、小さいために紛失しやすいとの理由で（実際紛失することが多いのも事実です）、使用不可となることが多いのです。会社によっては、さらに情報漏えい防止のために USB の差込口を物理的に破壊して PC を使用しているケースもあります。なかなか企業の情報セキュリティ管理は、人的なミス、不正などを見越して管理強化をしているため、このようなルールもやむを得ないケースも少なくないのが現状です。しかし、よく考えると情報資産の有効活用の観点からはやりすぎではないでしょうか？このような矛盾を解決するためにも情報セキュリティ技術を正しく利用するなどの情報セキュリティ対策を施して情報資産の有効活用を目指したいと思います。

（２） 情報セキュリティ対策について

情報セキュリティ対策というのは、端的に言えば、情報資産を有効に活用するために、いろいろな脅威から守るための対策ということが言えると思います。ただ、技術だけで脅威から情報資産を守るのは不可能で、管理、運用により実現することも必要です。現に、セキュリティの事故（たとえば、個人情報を紛失したり）というのは、人間のうっかりミスから起こることも多く、これらは運用ルールの順守によって回避することも多いのが実態です。

情報セキュリティ対策を整理するために、情報セキュリティの脅威をリストアップし、それぞれに対しての想定されるリスク、対策（技術、運用）をあげてみたものが下の表です。

まず、環境的な脅威として、このたび発生した大地震のような自然災害というものがあげられます。これにより、情報の紛失、システムの破壊による情報利用機能の喪失などのリスクが想定されます。情報セキュリティ対策というのは、情報資産の CIA を保つための対策ですので、技術的にはバックアップシステムの利用により災害発生後のシステム復旧に備えることができます。また、システムだけあってもそれを利用ルールに基づいて日頃からきちんと活用すること、また、バックアップシステムが近隣にあったのでは、同様の被害を受けるので、遠隔地、特に海外のデータセンターの利用などが有効となります。

セキュリティの事故発生例をみると、やはり人的な原因によるものが圧倒的に多いというのが現実です。人的要因の中でも、故意ではなく人的ミスによるものも少なくありません。外出時に電車の網棚にカバンを置き忘れたことによる情報紛失、最悪の場合はこれが情報流出につながります。携帯電話の紛失、USB メモリーの紛失などなど。ミスは誰にでもあることなので、これを完全になくすことは難しいのですが、電車では網棚を利用しない、携帯電話はストラップを装着する、USB メモリーはストラップをつける、などルールを守ることは徹底できます。それにより人的ミスによる情報セキュリティ事故の発生は画期的に減らすことが可能です。また、データ紛失については、バックアップシステムによりデータ復旧に備えることは必要ですし、情報が万一悪意のある人に渡った場合を想定し、暗号化を常に心がけることも有効です。

人的要因の中で、たちが悪いのが故意による脅威です。悪意を持った人が、ウィルスをばらまいたり、大量の迷惑メールを送りつけたり、企業のサーバなどに入り込んで不正アクセスをし、データを盗聴したり改ざんしたり、などなどです。また故意という中には、内部の人間がそのアクセス権限などを悪用して、データ流出、データ改ざんなどの犯罪を犯すケースも発生しています。これらの脅威から情報資産守るための対策は、市販のセキュリティソフトウェアの利用が有効なことは、すでにご存知と通りと思います。迷惑メールについては、怪しいメールはまずは迷惑メールフォルダーに避け、受信者のチェックで迷惑メールと判断した場合は次回以降受け取らないような設定をするとか、問題ないから以降は受信箱に直接入れるとかメールソフトで対策を施すことができます。ウィルスソフトはメールに添付されてきたファイル、Web アクセス時にアクセスしたページ、すでに PC 内あるファイルなどのウィルス感染をチェックし、削除したり駆除したりということを実行してくれます。これら、迷惑メールやウィルスは新たなものが次々と現れてくるため、これらのソフトウェアもそれらに対応し、日々アップデートされていきますので、ソフトウェアの更新作業も欠かせない作業です。また、サーバに対する不正アクセス、盗聴に対しては、暗号技術の活用による盗聴防止、成りすまし防止、改ざんチェックなどの機能を活用することにより、強力なセキュリティの確保ができます。（暗号技術に関しては別の機会にもう少し詳細にご紹介させていただきます）

技術的な対策に加えて、運用による対策も必要です。データ暗号化の徹底、パスワード利用・定期的な更新、アクセス権限の管理、各種対策ソフト利用・更新実施管理、システムアップデート実施管理、物理的な入退室管理などの対策を併せて実行することによりリスク発生を大幅に減らすことが可能になります。

脅威の種類		脅威	リスク	技術的対策	運用による対策
環境的脅威		自然災害など	情報紛失、情報破壊など	バックアップシステム	遠隔地にバックアップを持つ
人的脅威	偶発	人的ミス	情報紛失、情報漏えいなど	バックアップシステム 暗号	人的ミスを回避するためのルール
	故意	ウィルス、迷惑メール、不正アクセス、データ改ざん、盗聴、盗難など	情報紛失、情報漏えい、データ改ざん、システムダウン	暗号、不正アクセス防止、改ざん検知、盗聴防止、フィルタリング、ウィルス検知・駆除	データ暗号化、パスワード設定、アクセス管理、対策ソフト利用、システムアップデート実施、入室管理

（３） 事例

一般的な話はこのくらいにして、具体的に、現場で実際に発生している情報セキュリティ事故の事例とそれらに対する対策例をご紹介します。

① 携帯電話の紛失事故

企業で働いている方であれば、周りの方の中には一人や二人携帯電話を落として無くしてしまったという方がいらっしゃるのではないでしょうか？携帯電話の中には当然よく電話をかける相手の方の電話番号、あるいはメールアドレスを電話帳に記録していると思います。それが業務上の相手だとすると、取扱い注意の個人情報となり、それが万一でも外部の第三者しかも悪意のある第三者の手に渡り悪用されることになると、大変な問題となります。対策としては、

→　クリップ付ストラップの装着　：　まず携帯電話を落とさないようにクリップ付ストラップにより衣服などに止めておくことが、非常に効果的な対策となります。現に、これにより携帯電話紛失事故が皆無になった例も報告されています。

→　携帯電話の遠隔ロック機能利用　：　万一紛失した後でも、遠隔から携帯電話端末のロックを有効にする機能を利用し、第三者の悪用を防ぎます。

②　Winny による情報漏えい事故
　悪名の高いソフトになってしまいましたが、Winny というファイル交換ソフトを使っていた人が、事故を起こした事例です。Winny そのものは、インタネットを通して、音楽、動画などのファイルを交換するためのソフトですが、これがウィルス（Antinny）に感染したことによって情報流出という問題を起こすソフトになってしまうわけです。仕事を家に持ち帰らないというのは、よく言われたものですが、自宅にも PC を持つようになると、やりかけの仕事をファイルとして持ち帰り自宅で仕事をする人も少なくない思われます。その自宅の PC というのは、普段は音楽を楽しんだり、インターネットを楽しんだりするための個人的な楽しみとして利用するため、ファイル交換ソフトで音楽ファイルを入手したりなどということもあるわけですが、そのソフトがウィルスに感染し、その仕事のデータ（特に個人情報などを含んでいるような）が、たまたまその PC 内にあったために、いっしょに流出してしまうという事故につながったわけです。これに対して取られている対策は、

→　Winny などファイル交換ソフト使用禁止　：　Winny などの問題を起こしかねない危険なソフトについては、個人の PC といえども保持しないように従業員に指導する。ということがルール化されている企業が多いようです。

→　業務データを自宅 PC に持ち込まない　：　自宅の PC 内に業務上のデータがたまたまあったために事故が発生したわけです。やはり仕事は家に持ち帰らないということです。

→　ウィルス対策ソフト導入と更新の徹底　：　ウィルス感染によって、問題を起こすソフトは他にもあります。ウィルス対策を完全に実施することが必須といえます。

以上、事例を二つ紹介しましたが、紛失事故については、携帯電話だけでなく、カバンを置き忘れ、飲み会の帰り道にいろいろなものを紛失などなど、が後を絶ちません。仕事上、重要な情報はなるべく持ち歩かない、というわけにはいかないと思いますので、紙の形では持たず電子化して notePC 内に暗号化して持ち歩く、飲み会があるときはカバンは職場

においておく、鍵のかかるカバンに入れる、など自分の業務形態にあった対策を日頃から心がけることをお勧めし、今回の情報セキュリティ対策概要のお話を終えたいと思います。実際の情報セキュリティ技術、特に脅威からの情報保護に強力な力を発揮する暗号技術については、改めてご紹介することにします。