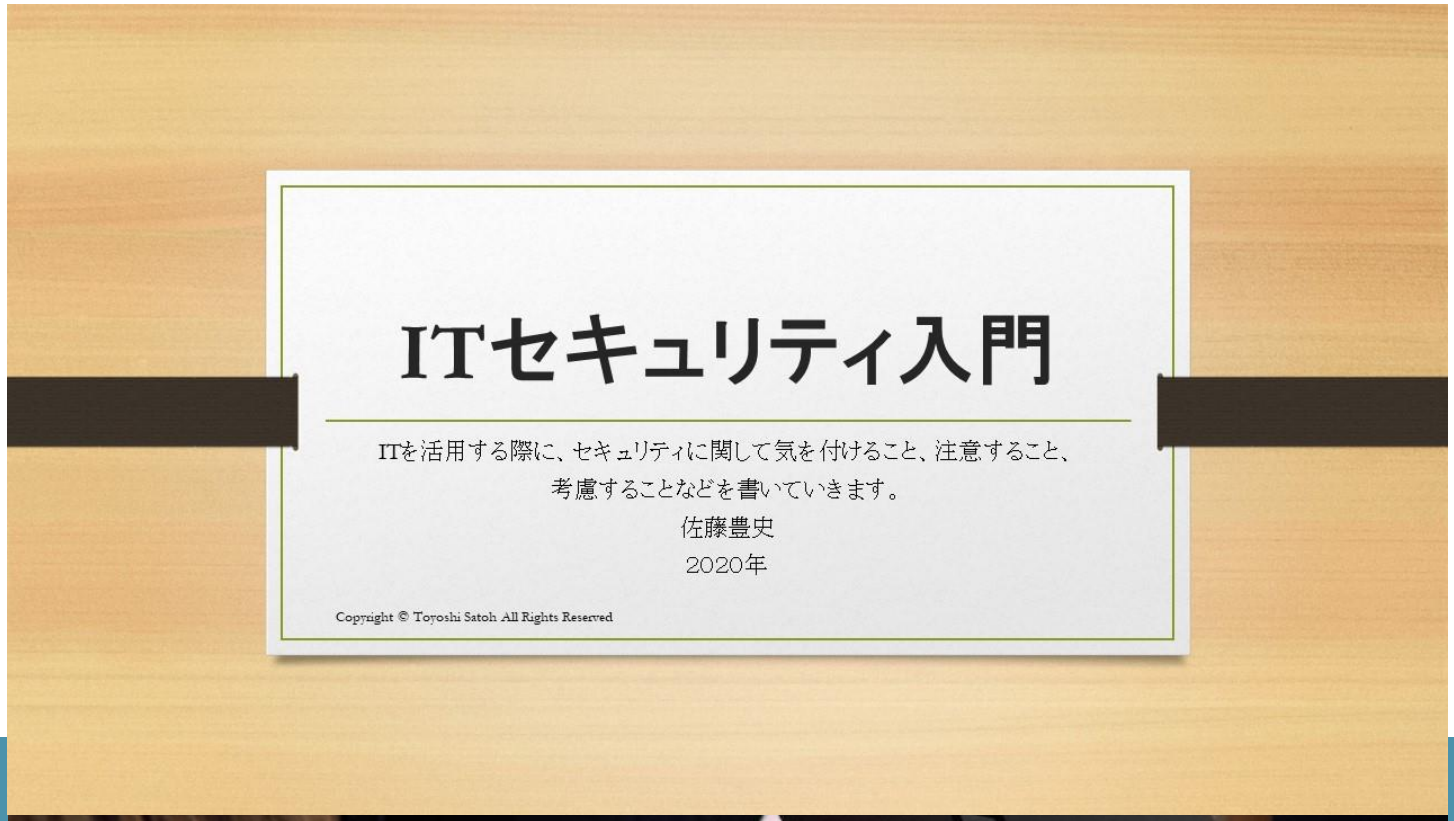
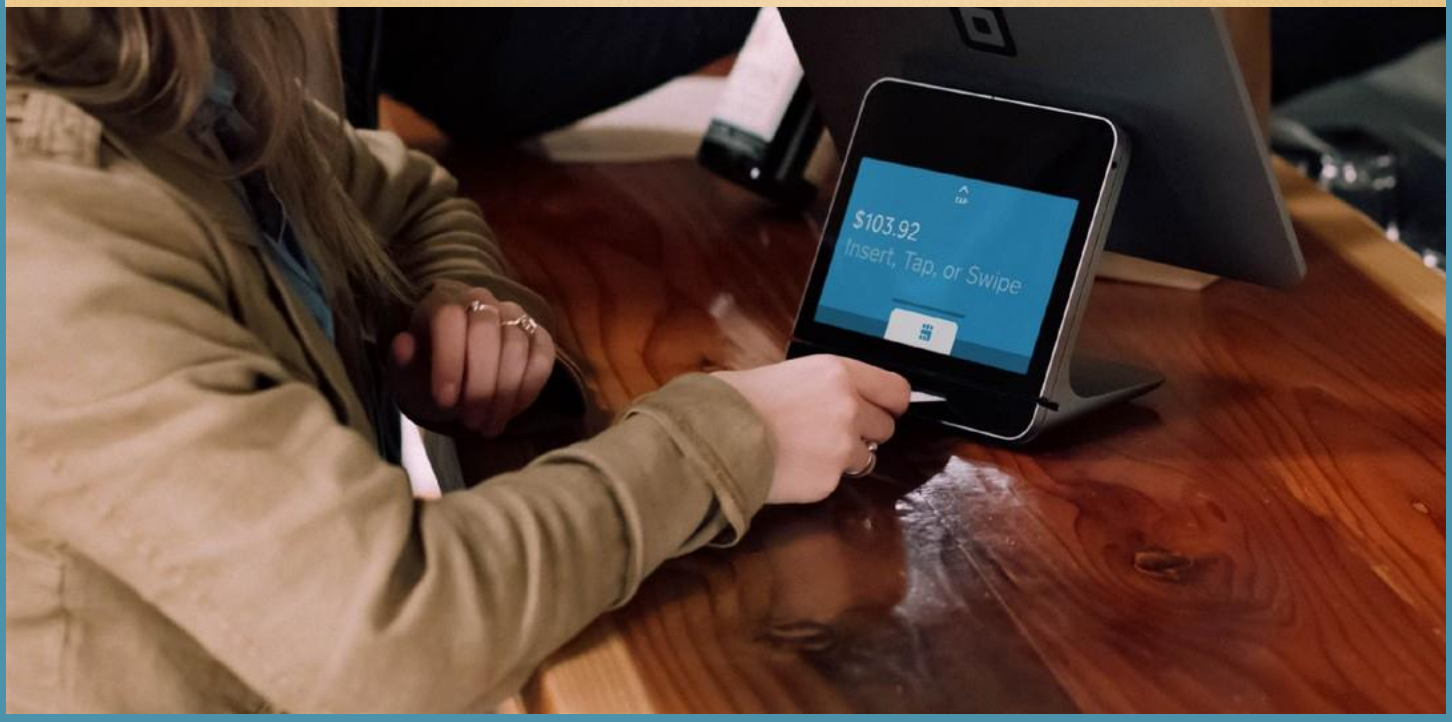
ITコンサルタント：佐藤豊史（さとうとよし）のブログ

ITセキュリティ入門

IT初心者向け、セキュリティ担当者として知っておくべきこと





ITコンサルタント：佐藤豊史（さとうとよし）のブログ

ITセキュリティ入門

はじめに

外資系食品会社のIT部門で、これまでシステム開発から運用までいろいろな仕事を担当してきました。
これまで経験してきたことをもとに、ITを活用する際に、セキュリティに関して気を付けること、注意すること、考慮することなどを書き連ねてみました。
ビジネスの現場でITを活用する際のセキュリティとはというのはどのようなものか、またITセキュリティに関連する一般的にはあまり認識されていないと思われていることなども書いていますので、何らかの新たな気づきなどを得てもらえればと思います。

目次

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１：ITセキュリティとは？

ITセキュリティとは？

ITセキュリティとは何か？そして何のために必要なのか？

私達がインターネットやコンピュータを使う上で、自分たちが使う情報を守ったり、必要な情報やサービスがいつでも使えるようにしておくことは大切です。しかし、守っておきたい情報が外部に漏れたり、コンピュータウィルス等に感染してデータが壊されたり、はたまた使いたいサービスが使えなくなったりすることが、残念ながらありえます。これらは、第三者の悪意のある行為によってだったり、悪意はなくても不注意やシステムの不備による事故で発生したりします。このような状況を防ぐために必要な対策をすることが、ITセキュリティといえます。

まず基本として、次の3点が、よくITセキュリティの教科書などで紹介されている情報セキュリティの3要素で、これらを維持していくことが、ITセキュリティと定義されます。

- 機密性（Confidentiality）：許可された者だけが、情報資産にアクセスできること。つまり、本人だけがその情報を利用できることです。
- 完全性（Integrity）：情報及び処理方法が、正確及び完全であること。つまり、間違いなくデータが処理されることです。
- 可用性（Availability）：許可された者が、必要な時に情報資産にアクセスできること。つまり、本人だけはいつでもその情報を利用できることです。

マイノート（これまでの私の体験・見聞から一言）

ITセキュリティが必要なことは、大抵の人が理解はしてくれるのですが、ではITセキュリティの対策をどこまでするのか、あるいはどこまで費用をかけるのかは常に議論になるところです。

ITセキュリティ対策を強化すればするほど、コンピュータシステムの利便性が低下する、つまり使い勝手が悪くなったり、ユーザ側に負担が増えたりします。例えば、パスワード解析をされにくくするために、パスワードの文字数や文字の種類を増やして強度を向上させると、ユーザは複雑なパスワードを覚えたり入力したりしなくてはならなくなるので、使い勝手が悪くなります。

また、ITセキュリティ対策に費用をかけても、それ自体で売上や利益を増加させるわけではなく、あくまでセキュリティリスク（危険性）を抑えるだけです。したがって、それらにかける費用は投資というよりかは、保険と同じように考える必要があります。

実際に私自身が以前ITセキュリティ担当だった頃は、社内関係者にとっては耳の痛いことばかりを言わなければならないので、社内で疎まれながらも仕事をしなければならなかった部分はありましたね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－２：リスクにはどのように対応する？

リスクにはどのように対応する？

ITセキュリティの対策を考えるにあたっては、セキュリティリスク（危険性）とはどのようなことで、それらに対してはどのように対応していくべきかを考える必要があります。

リスクとは下記のように定義されますが、具体例としては、個人情報を漏洩させないように、不正アクセス対策をしていたが、それが不十分だったために個人情報漏洩の発生するような危険性のことです。まずは、次のリスクアセスメントという手法によって、そのようなリスクを洗い出して、評価をすることになります。

- リスク：脅威（ある要因）が情報資産の脆弱性を利用して、情報資産への損失または損害を与える可能性のこと
- リスクアセスメント：リスクがどこに、どのように潜在しているかを特定して、その影響の大きさを分析し評価して、優先順位を付ける。

そして、評価をしたそれぞれのリスクについて、次のいずれかの対応をとることになります。

- リスク保有（受容）　影響度が小さい場合はリスク発生を受け入れる　対応なし
- リスク軽減（低減）　リスクの損失額や発生確率を低く抑える　例：情報を暗号化する、入退室管理をする
- リスク回避　リスクの原因・要因を除去（停止）する　例：サービスの停止、個人情報を取得しない
- リスク移転（転嫁）　契約などでリスクを第三者へ移転・転嫁（第三者と共有）する
  例：保険に加入、システムの外部委託

マイノート（これまでの私の体験・見聞から一言）

リスクへの対応については、一番初めに頭に浮かぶのがリスク軽減で、どのようなセキュリティ対策を実施するべきかを検討することかと思います。しかし、対応の仕方には、そもそもそのリスクが発生しても仕方がない、発生したらそのときに発生したことによる影響を受け入れるというリスク受容の考え方もあります。これはリスクが発生したときの費用を負担するつもりであるとも言えます。このように、受容するリスクもなく、すべてのリスクに対策をしていたら、膨大な費用が発生しますので、どこまで受容するかを決めるのは重要です。これはある意味経営的な判断にもなりますので、私自身がセキュリティ担当者だったときは、大変悩みどころでした。

また、リスク回避や移転も重要で、そもそもリスクのあることは実施しないということも大切です。私の経験では、Eコマースシステムでクレジットカード決済をするために、自社のシステムではクレジットカード情報は取り扱わずに、クレジットカード決済代行業者にシステム委託をして、リスク回避・移転をしていました。

したがって、まずはそれぞれのリスクに対して、自分たちにとってどのように影響があるかを考えるということは大切ですね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－３：個人情報はどのように取り扱う？

個人情報はどのように取り扱う？
システムで個人情報を取り扱う場合は、様々な注意や考慮が必要です。

個人情報はその個人のプライバシーに関わる権利・利益を保護するために、適切に取り扱い、管理する必要があります。そして、個人情報保護法により、個人情報を取り扱う事業者が遵守すべき義務などが定められています。

まず、個人情報とは何かですが、生存する特定の個人を識別できる情報と定義されます。例えば、名字だけでは特定の個人を識別できませんが、氏名と住所や生年月日などの複数の情報が組み合わさることで、識別できるようになります。また、メールアドレスにはユーザ名や所属（ドメイン名）が記載されているので、これも個人情報に当たります。
また、改正された個人情報保護法では個人識別符号として、次のような情報も対象になりました。
身体的特徴をコンピュータで使うために変換した符号（例：バイオメトリクス認証で用いる静脈や指紋などの生体情報）
個人に割り当てられた文字・数字・記号などの符号（例：マイナンバー、パスポート番号）
これらの個人情報は、基本的に次のような点を注意して取り扱う必要があります。

個人情報を取得するときには、その使用目的を明確にする
取得した個人情報は、目的外の使用は行わない
個人情報を第三者に提供する場合は、本人の同意を得る

マイノート（これまでの私の体験・見聞から一言）
まずは、システムで取り扱うデータの中でどれが個人情報に相当するのかについて、関係者間で合意を取ることが大切です。通販システムなどで取得した個人のお客様の情報が、個人情報に当たることは明らかに誰でも認識をしていますが、法人顧客の担当者の情報なども個人情報として取り扱う必要があります。ところが、その顧客の営業担当者は得てしてその意識が薄かったりします。今は担当者レベルでも容易に顧客リストを作成して持ち歩くことが可能ですので、まずは取り扱いには注意が必要だという意識付けが必要でしょう。

また、昨年欧州連合（EU）が施行した「一般データ保護規則（General Data Protection Regulation：GDPR）」によって、対象は欧州のユーザですが、生体情報やマイナンバーといった情報だけでなく、IPアドレスやブラウザのクッキー情報のようなインターネットにおける情報まで個人情報として考慮すべき場合も出てきました。これらの規則は、まずはグーグルやフェイスブックのようなITジャイアント企業を意識していると思われますが、今後は一般企業にも影響が出てくるでしょう。ますます個人情報の保護については、一層の注意が必要になってきましたね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－４：個人情報はどのように取り扱う？（パート２）

個人情報はどのように取り扱う？（パート2）
個人情報を保護するためには、個人情報を適切に管理するための個人情報保護方針を策定して、その方針を実行するための体制を構築します。そして、個人情報保護管理者を任命して、その体制のもとで管理システムを構築・運用していくことになります。管理システムを維持していくためには、継続的な改善の仕組み、すなわちPDCAサイクルの導入も必要になります。

そのようにして、個人情報の取り扱いについて適切な体制を整備している事業者を認定する制度、プライバシーマーク制度というものがあります。この取得には厳しい基準をクリアする必要がありますので、取得事業者は個人情報を取り扱う組織として信頼を得ることになります。

個人情報保護のためには、特に次のような点に注意します。

- 安全管理措置：安全管理のための必要な措置を講じる義務がある
- 委託先の監督：個人情報の取り扱いを委託する場合には、適切な委託先を選定して監督する義務がある
- 要配慮個人情報：本人の人種、信条、病歴などの配慮が必要な個人情報は、原則として本人の同意を得る義務がある

マイノート（これまでの私の体験・見聞から一言）
個人情報を保護する必要性は分かっていても、専門の事業者でない限り、一般の企業では上記に述べられたような体制を構築するのは、なかなかむずかしいかもしれません。

しかし、昨今はほとんどビジネスでそうだと思いますが、自分たちのビジネスで個人情報を取り扱う可能性があるのであれば、少なくとも方針と責任者を決めておく必要があると思います。そうしておけば、いざというときに誰が何をするべきかで社内で揉めることなく、何をどのようにするべきかという議論にすぐに入れると思います。

また、個人情報の取り扱いを専門業者に委託することは、よくあるケースだと思います。別の見方では、専門の業者に取り扱いを任せたほうが安心とも言えるかもしれません。しかし、そのしましたが、定期的に委託先を訪問したりしてチェックをすることが大切ですね。場合でも委託元に個人情報保護の責任はありますので、適切な委託先を選定したり、委託先の運用を監督する義務は発生します。委託先の体制や運用が適切かどうかを確認するためには、私自身も経験しましたが、定期的に委託先を訪問したりしてチェックをすることが大切ですね。

ITセキュリティ入門（IT初心者向け）－５：事業継続のために必要なこと

事業継続のために必要なこと
事業継続計画（BCP：Business Continuity Plan）とは、災害やシステム障害など予期せぬ事態が発生した場合でも、重要な業務の継続を可能にするためやシステムの復旧、再開をするために、事前に策定される行動計画のことです。

BCPとして対応すべきこととしては、まずは最低限の事業を継続するための暫定対応と、システムを早期に復旧して事業を再開するための恒久対応があります。

BCPを策定する場合は、業務が停止した場合の影響などを分析し、許容される最大停止時間などを決定するビジネスインパクト分析を行います。

また、停止したシステムを復旧するために、次のような目標値を設定します。

- 目標復旧時点：どの状態まで復旧させるのかを示す目標値
- 目標復旧時間：いつまでに復旧させるかを示す目標値

マイノート（これまでの私の体験・見聞から一言）
BCPを策定する場合は、まずは重要な業務の洗い出しを行います。すべての業務がいつ何時も停止することができないというわけではないはずですから、どうしても中断できない業務は何かを選択する必要があります。このときには、ある程度の割り切りをしないとあれもこれも必要だということになり、重要な業務をなかなか絞りきれないことになります。内部の関係者だけではなく、顧客や外部の関係者にも影響を与える業務は、BCPの対象から外すことはむずかしいと思いますが、より重要な業務がそのほかにあるのであれば、対象外にする勇気も必要だと思います。

また、今どきシステムを使用しない業務などないでしょうから、システムが停止した場合にその重要な業務にどのような影響を与えるかを分析します。そして、その業務をどのように継続するかを考えるわけですが、システムを使用しなくても手作業、マニュアル作業で業務を継続できるのであれば問題ありませんが、作業量や作業の複雑さを考慮すれば、とてもマニュアル作業ではできないという結論になることが多いと思います。そうなると、代わりにその業務の処理をするためのシステムが別途必要になるということになります。本当に止められない業務に使用しているシステムであれば、結局代替のシステムを用意しておくということになりますね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－６：ユーザやデータは本物か？

ユーザやデータは本物か？

システムを使うユーザや、やり取りするデータが正しいかどうかを確認することは、セキュリティの観点からは必須です。

認証（AuthenticationまたはCertification）とは、ユーザやデータなどを検証して、それらが確実に本物であることを確認することです。ユーザの場合であれば、第三者に対して自分がなりすましではなく、本人であることを証明、確認します。また、データの場合は、改ざんや破壊などによって、不正な変更や異常がないことを確認します。

本人であることを確かめるための認証方式については、次のように分類できます。

- 知識認証（ID・パスワードなど）：本人のみが知り得る情報を確認
- 所有物認証（鍵・トークンなど）：本人のみが所有しているものを確認
- バイオメトリクス認証（指紋、声紋など）：本人の身体的・行動的特徴を確認

認証の強度を上げるために、次のような方式を用いることもあります。

- 2要素認証：異なる認証方式を2つ用いる、例：キャッシュカード（所有物）と暗証番号（知識）
- 2段階認証：同じ認証方式を2つ用いる、例：ID・パスワード（知識）と認証コード（知識）

また、やり取りするデータに改ざんや異常がないことを確認するために、そのデータをもとに生成したハッシュ値という特定の長さのコードを用いて、改ざんや異常がないことを検知するメッセージ認証があります。

マイノート（これまでの私の体験・見聞から一言）

システムを使う上でまず必要なのが、このユーザ認証です。大抵のシステムでIDとパスワードを使用してログインをすることになると思いますが、このID・パスワードの管理がよく問題になります。基本的には、ユーザ個人ごとにID・パスワードを付与するべきですが、場合によっては共有のID・パスワードを使う場合もあります。この場合は、この認証ではユーザ個人を特定することはできないし、誰でもログインして使用できるという前提で、システムを運用しなければなりません。

また、ユーザ個人ごとにID・パスワードを付与する場合は、パスワードの管理が大変重要です。ユーザ各個人でパスワードを管理して、他人に知られないようにしなければなりませんが、つい紙などに書いて人目につくようなことになったり、誕生日や電話番号などの容易に推測可能なパスワードを設定したりしてしまいます。

安易なパスワードを設定できないように、複雑なパスワード（桁数を長くする、英数字記号を含むなど）を設定するように、また定期的にパスワードを変更するように、システムで制限することが多いと思います。しかし、こうなるとパスワードを忘れたりして、使いたいときにシステムが使えないことがよく起こります。そのために、最近はパスワードを管理するためのツールを使用することも増えてきたかと思います。また、パスワードを定期的に変更することが安易なパスワードを設定することにつながるとして、複雑なパスワードを変更せずにずっと使用するべきという考え方もあるようです。

いずれにしろ、パスワード管理は永遠の課題ですね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－７：暗号技術のセキュリティ効果

暗号技術のセキュリティ効果
データを第三者に知られることなく秘匿するための暗号化は、セキュリティ対策上大変重要です。

暗号化とは、暗号化されていない平文と呼ばれるデータに対して、暗号化アルゴリズム（手順）と鍵（パスワードなど）を用いて暗号化処理を加えて暗号文にすることです。逆に、暗号文に復号処理をして平文に戻すことを復号といいます。

主な暗号方式は、次のとおりです。

- 共通鍵暗号方式：暗号化と復号に用いる鍵が同じ。共通鍵を用いる。
- 公開鍵暗号方式：暗号化と復号に用いる鍵は異なる。公開鍵と秘密鍵を用いる。

そして、暗号化技術には、次のような効果があります。

- 盗聴防止：第三者にデータを解読されないように防ぐ（機密性）
- 改ざん検出：第三者にデータを改ざんされていないことを保証する（完全性）
- なりすまし防止：第三者が情報発信の相手になりすますことを防ぐ（正当性）
- 否認防止：情報発信の相手が本人であることを否認できないようにする（正当性）

マイノート（これまでの私の体験・見聞から一言）
インターネットでは、データが不特定多数のサーバーを経由して通信されますので、機密性が必要なデータには暗号化技術を使用します。

一般的に第三者に秘匿すべきデータを、インターネットを経由してやり取りする場合は、暗号化したデータとパスワードを相手に送ることが多いと思いますが、この場合は共通鍵暗号方式を使ってデータをやり取りしていることになります。このときに、パスワードをどうやって相手と共有するか、またそのパスワードをどのように管理するかが問題になります。当然、暗号化したデータとパスワードを一緒に送っては意味がありませんし、同じパスワードを使い続けることもリスクがあります。

しかしながら、実務の現場ではよくありがちなことで、私自身も暗号化したデータのパスワードをデータとは別に送ったつもりだったのに、実はデータも一緒に添付されていたことがあり、恥ずかしい思いをしたこともあります。また、同じパスワードを使うこともよくあるかと思いますが、これも第三者が知り得た場合は暗号化の効果がなくなりますので、基本的にはやめるべきですが、現場ではなかなかむずかしいですね。

公開鍵暗号方式を使えば、このような問題は解消されると思うのですが、個人間で暗号化したデータのやりとりをするのに使うには、まだまだハードルが高いように思います。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－８：暗号技術のセキュリティ効果（パート２）

暗号技術のセキュリティ効果（パート2）
インターネットなどでデータ通信をする際に、データを暗号化するために暗号化通信の技術が使われます。主な暗号化通信には、次のような技術があります。

- IPSec：Internet Protocolのセキュリティ技術で、IPパケットと呼ばれる小さく分割したデータを暗号化する。
- VPN：仮想的な専用線のことで、通信事業者の通信網を使う場合とインターネット網を使う場合がある。
- SSL：ウェブブラウザとWebサーバ間でデータを暗号化する。HTTPSは、HTTP通信を暗号化したプロトコルで、認証局と呼ばれる信頼された第三者機関から発行されたサーバ証明書で証明された公開鍵を用いて暗号化通信をする。

昨今は当たり前のように使用される無線LANについても、セキュリティの脅威から防御するために、暗号化技術が使われています。WiFiと呼ばれる無線LAN装置の業界団体が規定した規格で、一般的に無線LAN装置の通信が行われています。無線LANの暗号方式には、WEPやWAP，WAP2などがあり、セキュリティ強度が異なりより安全なWAP2を使います。また、接続先のアクセスポイントを識別するためにSSIDという識別名が使われ、無線LANの設定画面に表示されて、パスワードで認証できれば通信ができるようになります。なお、セキュリティ対策のために、SSIDを表示させないステルス（隠蔽）機能もあります。

マイノート（これまでの私の体験・見聞から一言）
インターネットの初期の頃は、とても便利なネットワークなので、可能な限りインターネットを使って通信をしたいと考えましたが、セキュリティの観点から盗聴などの脅威からどのように防御するかが常に懸念点でした。それらを解決するために、いろいろな暗号化通信の技術が発達してきましたが、いまでは暗号化通信が標準で使われる時代で、暗号化されていない通信は、ビジネスでもプライベートでもほとんど無くなる方向にあると思います。

ただし、現在使用しているシステムを一旦暗号化通信にしたからと言っても、それを脅かそうとする技術が生まれてくるために、暗号化通信の技術も常にアップデートしていく必要があります。そのアップデートをしていくために、ときには既存のシステムを変更することが必要になったり、それに対応できない端末が出てきたりして、結構影響があることがあります。しかし、セキュリティ強度が弱くなった暗号化通信を使い続けるわけにはいかないので、何か影響があったとしても対応していくしかないですね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－９：アクセス制御とログ管理

アクセス制御とログ管理
情報システムやネットワークへのアクセス権限を制限したりすることが、アクセス制御です。
アクセス権限をユーザに付与する際には、必要以上の権限、過剰権限が付与されないように、次のような観点で適切な権限を付与する必要があります。

- 職責分離：担当者と承認者の権限や職務上の責任を明確に分離すること
- 最小権限：付与する権限は必要最低限の権限のみにすること

そして、アクセス制御が正しく行われているかを監視するために、様々な情報システムやネットワーク機器、アプリケーションのログを収集、保存、分析するログ管理も重要です。
ログ管理の目的としては、次のような点が挙げられます。

- 異常や不正の検出
- セキュリティ事件・事故の原因究明、原因分析
- システムの点検、評価

ログを収集して一元管理するログ管理サーバを使用して、各システムや機器に保存されているログと、ログ管理サーバで収集したログを比較することで、ログの改ざんを検出できるようにする場合もあります。
また、このようなログを使用して、不正アクセスなどの原因究明調査や法的証拠性確保をすることを、ディジタルフォレンジックスといいます。

マイノート（これまでの私の体験・見聞から一言）
アクセス制御はセキュリティの観点から、大変重要な対策です。考え方としては当然のことですし、実施するのも一見そんなに難しいことではないように思えますが、実際に運用するとなると、結構大変なことが分かります。

例えば、アクセス権限を付与する場合に当初は適切に設定されていても、担当者の職務が変わったり、新しい担当者が加わったときに、適切にアクセス権限をメンテナンスすることは重要です。特に、あるユーザに権限が不要になったにもかかわらず、そのまま権限が削除されずに残ったままということが、往々にして発生します。

アクセス権限の変更依頼をユーザ部門からしてもらうような場合は、担当者が異動しても、その権限の削除申請がされずに、そのまま残るということがよくあります。したがって、定期的にアクセス権限の見直しをすることが肝心です。

また、様々なログも通常の運用ではほとんど使用することはありませんが、何か問題などが起こったときには、大変重要な情報になりますので、ログ管理もおろそかにするわけには行きません。私の経験でも、ある問題でディジタルフォレンジックスをしてもらったことがありますが、このときには改めてログの重要性を認識しました。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１０：ネットワークの防火壁、ファイアウォール

ネットワークの防火壁、ファイアウォール
ファイアウォールとは防火壁という意味で、LANなどの内部ネットワークとインターネットなどの外部ネットワークの境界に設置して、外部からの不正アクセスを防ぐ役割があります。一般的にはパケットフィルタリングという機能を使って、データの通過（許可）または遮断（拒否）を行います。

- パケットフィルタリング：IPパケットのヘッダ情報（送信元IPアドレスや送信先IPアドレス、送信元ポート番号や送信先ポート番号など）を解析して、アクセスリスト（IPパケットの禁止・許可ルール一覧）をもとに許可されたIPパケットだけを通過させる。

そして、非武装地帯という意味のDMZ（DeMilitarized Zone）という内部ネットワークと外部ネットワークの間に構築するネットワークがあります。DMZには、インターネットに公開するWebサーバやメールサーバなどを設置して、内部ネットワークを隔離して保護します。

また、WAF（Web Application Firewall）というウェブアプリケーションへの攻撃（クロスサイトスクリプティング、SQLインジェクションなど）に特化したファイアウォールもあります。

マイノート（これまでの私の体験・見聞から一言）
外部ネットワークからの攻撃を防ぐのに、まずはファイアウォールが必要です。仕組み自体はシンプルで、必要な通信データだけを通過させるという技術です。そのためには、アクセスリストという禁止・許可ルール一覧が重要で、このアクセスリストにどのIPパケットは通過させるか、遮断するかを設定しておきます。

ただし、このアクセスリストのメンテンナンスは容易ではありません。ネットワーク内のサーバや機器が増えてくると、それらに対するアクセスリストへのルールの追加設定が必要になってきます。このようにしてアクセスリストが、往々にして複雑で長いリストになっていきます。そうなると、不必要になったルール設定などが削除されなかったりして、不要なデータが通過できる状態になったりします。とにかくアクセスリストの定期的な見直しは重要です。

また、WAFはウェブアプリケーションへの攻撃を防ぐのにとても効果的ですが、この設定も気をつけないと、本来許可すべきデータが遮断されてウェブアプリケーション自体が正しく動作しないという事が起こったりします。

ファイアウォールは重要なセキュリティ対策ですが、その適切な設定を維持していくのは、容易ではありませんね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１１：サイバー攻撃（その１）コンピュータウィルス

サイバー攻撃（その1）コンピュータウィルス
不正アクセスやコンピュータウィルスなどにより、情報の盗聴・窃取、データ改ざんや破壊・消去を行うことを、サイバー攻撃（クラッキング）と呼びます。そして、その攻撃で使用される有害なプログラムを、コンピュータウィルスまたはマルウェアといいます。どちらも、不正に動作させる意図で作成された悪意のあるソフトウェアやプログラムのことで、ユーザにとって有害で様々な被害をもたらします。特に、コンピュータウィルスは次のような機能を有するものと定義されています。

- 自己伝染：他のシステムに伝染する
- 潜伏：発病するまで症状を出さない
- 発病：設計者の意図しない動作をする

コンピュータウィルスには次のような種類があります。

- ファイル感染型：アプリケーションなどの実行型ファイルに感染する
- マクロ感染型：アプリケーションのマクロ機能を悪用する
- トロイの木馬：特定の条件を満たすと不正プログラムを実行する
- ワーム：自己複製しながら他のコンピュータに感染する

また、次のような目的に使用されます。

- スパイウェア：端末情報やアクセス情報を収集して流出させる
- ボット（BOT）：コンピュータを外部から不正に操る
- ランサムウェア：データを勝手にロックして、ロック解除に身代金要求する
- バックドア：通常のアクセス経路以外で侵入するための裏口を組み込む

マイノート（これまでの私の体験・見聞から一言）
コンピュータウィルスは、特殊なシステム環境を使用している人達だけの問題ではなく、間違いなく一般のユーザもこの脅威にさらされています。私自身もこれまでの仕事の中で何度も実際のコンピュータウィルス感染を経験しています。

例えば、十数年前に当時猛威を振るったNimdaと呼ばれるワーム型のコンピュータウィルスに社内端末の一部が感染したために、急遽ネットワークを遮断して、すべてのサーバや端末のウィルスチェック作業を実施したことがあります。このときは海外の端末が感染しただけだったので、国内のサーバや端末には被害はありませんでしたが、週末も使って作業を行いました。

また、数年前にはウェブサイトにあるコンピュータウィルスを仕掛けられて、その対応に奔走しました。本当にこのときは大変な思いをしたので、個人的にはこのような経験は二度としたくないと決意しました。
このようにコンピュータウィルスは決して他人事ではなく、身近にある脅威のひとつであることを改めて認識をする必要がありますね。

ITセキュリティ入門（IT初心者向け）－１２：サイバー攻撃（その２）ウィルス感染対策

サイバー攻撃（その2）ウィルス感染対策

コンピュータウィルス感染を未然に防ぐためには、次のような対策があります。

- ウィルス対策（アンチウィルス）ソフトの導入
- OSやアプリケーションソフトウェアなどの修正プログラム（セキュリティパッチ）の適用

ウィルス対策ソフトには、ウィルスを検知するために次のような検出技術があります。

- パターンマッチング方式：既知ウィルスのシグネチャ（ウィルスを識別できる特徴的なコード）を記録したウィルス定義ファイル（パターンファイル）を使用して検出する。新種のウィルスが出現するたびに、最新版のパターンファイルが提供される。
- ビヘイビア方式：プログラムのシステム内での挙動を監視し、異常現象や不審な動きを検知する。（振る舞い検知）

ウィルス定義ファイル（パターンファイル）は、ファイル上に登録されたウィルスしか検出できないために、最新のウィルスには感染する危険性があります。そのために、パターンファイルは常に最新の状態に更新する必要があります。

また、OSやアプリケーションソフトウェアなどの脆弱性を突いて攻撃するウィルスを防ぐために、その脆弱性を修正するための修正プログラム（セキュリティパッチ）を適用しますが、こちらも常に最新のセキュリティパッチを適用する必要があります。

マイノート（これまでの私の体験・見聞から一言）

パターンファイル、セキュリティパッチともに常に最新の状態にしておくことが肝心です。ただし、これは言うは易く行うは難しで、常にそのような状態にしておくことはなかなか容易ではありません。

例えば、パターンファイルは、管理しているネットワーク内にある全てのコンピュータに対して最新の状態に更新しておかないと、一台でも最新の状態になっていないとそのコンピュータが感染して被害が発生する可能性があります。また、コンピュータ内をスキャンしないとウィルスが潜んでいる可能性もあるので、定期的に最新のパターンファイルでスキャンをする必要もあります。私の経験でも、強力なウィルスが出現するたびに、管理するすべてのコンピュータのパターンファイルを最新の状態に更新して、そのパターンファイルでスキャンをするということを手間ひまかけて繰り返していました。

また、セキュリティパッチは適用すると、場合によってはその他のソフトウェアやプログラムに影響を与える可能性があるので、常に慎重に適用をしなければなりません。事前に重要なソフトウェアやプログラムに影響がないことをテストして適用するべきですが、なかなかそのテストが進まずに、適用のタイミングが遅れていくことがよく発生します。私の経験でも、セキュリティパッチは迅速に適用することが難しく、時間をかけてテストをしてから、ある程度の数のセキュリティパッチをまとめて適用をしていました。

ウィルス対策は日々の地道な運用が大切ですね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１３：サイバー攻撃（その３）パスワード管理

サイバー攻撃（その3）パスワード管理

ID・パスワードの認証情報は第三者に知られるだけで、なりすましによる不正利用が容易に可能になってしまいます。そのために、ID・パスワードを解析して不正に取得をしようとする、次のようなパスワード解析の攻撃方法があります。

- 辞書攻撃：辞書にあるようなよく用いられる単語などの文字列を生成して、手当り次第に試みる攻撃。
- 総当たり攻撃（ブルートフォースアタック）：すべての文字列の組み合わせを一つずつ試行していく攻撃
- パスワードリスト攻撃：あるシステムで使用されているID・パスワードのリストを何らかの方法で入手して、そのリストで他のシステムへ不正にログインを試みる攻撃

上記の攻撃からの対策としては、次のような適切なパスワード管理が必要になります。

- 辞書に掲載されるような推測されやすい用語は使用しない
- 文字数や文字種類を増やす
- 所定回数の入力間違いが発生すると、アカウントロックでIDの使用停止、または一定時間使用停止にするように、パスワード入力回数を制限する
- 有効期限を設定し、定期的にパスワードを変更するようにして、パスワード漏洩のリスクを減らす
- 複数のシステムで同じID・パスワードの使い回しをしない
- ２要素認証（パスワード認証以外の認証）を導入する

マイノート（これまでの私の体験・見聞から一言）

現在でもなお、ほとんどのシステムでID・パスワード認証が主流だと思いますが、そのための適切なパスワード管理は昔からある重要な課題の一つだと思います。

パスワードが漏洩しないように、各ユーザに次のような管理が求められますが、現場で徹底することはなかなか容易ではありません。

- パスワードを他人に教えない、または共有しない
- パスワードを紙などに記載しない
- パスワードをPCやサーバのファイルなどにデータ保存しない

有効期限を設定して定期的にパスワードを変更させることも、変更する立場からすると、以前に使用したパスワードとよく似た安易なパスワードを使いがちですので、逆に推測されやすいというリスクがあります。そこで、定期的にパスワードを変更することはやめて、複雑な推測されにくいパスワードを使い続けるほうが安全だという考え方もあるようです。

昨今はID・パスワードを使用するシステムが増えたために、同じID・パスワードを使い回すことが多いと思いますが、このような状況を防ぐために、複数のパスワードを管理するツールを使うことも必要でしょう。ただし、このツールにログインするときにもパスワードが必要だと思いますが、このパスワードが漏洩してしまったら、逆に被害は大きくなってしまいますね。

また、最近の経験では、あるシステムのパスワードが漏洩した可能性が判明したために、急遽2要素認証に切り替えるためのワンタイム認証コードを導入したシステムもありました。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１４：サイバー攻撃（その４）ネットワーク攻撃

サイバー攻撃（その4）ネットワーク攻撃

外部ネットワークからのサイバー攻撃としては、次のような攻撃方法があります。

- 不正アクセス
  - IPスプーフィング：送信するパケットの送信元IPアドレスを偽って、攻撃対象にパケットを送信する
  - ポートスキャン：TCP/IPプロトコルのポート番号を順番に変えながらサーバにアクセスして、侵入口と成り得る脆弱なポートがないか調べる
- サービス停止
  - DoS（Denial of Service）攻撃：特定のサーバに大量のパケットを送りつけて、負荷を与えサービスを妨害する
- 悪意のある命令実行
  - クロスサイトスクリプティング：ユーザに悪意のスクリプトを送りつけて、脆弱なサイトでユーザにスクリプトを実行させる
  - SQLインジェクション：脆弱なサイトにて、悪意のあるデータベースの操作命令をSQLで実行する

上記攻撃からの対策としては、次のような対策があります。

- ファイアウォールなどで不要なポートを遮断したり、不審なパケットを破棄する
- サーバなどで不要なサービスを停止する
- セキュリティホールと呼ばれるセキュリティ上の脆弱性に対する修正プログラム（セキュリティパッチ）を迅速に適用する
- サイト制作するときに、悪意のあるスクリプトが実行されないように、プログラムのコーディングで対策をする

マイノート（これまでの私の体験・見聞から一言）

外部ネットワークからの対策としては、ファイアウォールが重要な役割を担いますが、このファイアウォールが適切に設定されているかを確認することが重要です。そのために、擬似的なポートスキャンをして、問題のあるポートや設定がないかを確認することができます。

また、サイト制作する際には、悪意のあるスクリプトが実行されないようにコーディングすることが必要ですが、コーディングのガイドラインなどを作成して、そのガイドラインに則ってサイト制作することも有効です。私の経験でも、そのようなガイドラインを業者に提供して、サイト制作をしてもらっていました。

そして、悪意のあるスクリプトが実行されないか、サイトのスキャンをすることも必要です。ポートスキャンも含めて、そのようなスキャンサービスを提供している業者に、重要なネットワークやサーバなどには定期的にスキャンをしてもらうことが望ましいと思います。以前私が担当していたネットワークやサーバは、四半期や一年ごとにスキャンを実施して、問題がないことを確認していました。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け） －１５：サイバー攻撃（その５）標的型攻撃

サイバー攻撃（その5）標的型攻撃
特定の会社や組織を攻撃対象（標的）にして、最終的には機密情報の入手・破壊や、会社や組織に大きな損害を与えることを目的とした攻撃があります。

特定の会社や組織に送信する電子メールを悪用する標的型攻撃メールがあり、次のような特徴があります。

- マルウェア感染：差出人を取引先や知人のように偽装してメールを送信し、マルウェア感染する添付ファイルを実行させたり、偽のリンク先でマルウェア感染するサイトに誘導したりします。
- フィッシング：実在する会社などを装ったメールを送信して、偽のサイトに誘導して個人情報や機密情報などを騙し取る攻撃です。

また、人間の心理的な弱さを利用したソーシャルエンジニアリングという、次のような不正行為もあります。

- 緊急、非常事態などを装い混乱させ誘導して、情報を入手する
- 取引先や知人になりすまし聞き出して、情報を入手する
- 肩越しなどから情報を覗き見（盗み見）して、情報を入手する（ショルダーハック）
- 廃棄された紙ゴミなどを収集して、情報を入手する（スカベジング）

昨今では、機密情報の入手だけではなく、会社や組織の経理担当者に近づき、取引先を装って偽の口座へ送金させるような巧妙な手口も横行しているようです。

マイノート（これまでの私の体験・見聞から一言）
標的型の攻撃に対しては、技術的な対策だけでは十分ではありません。

攻撃された会社や組織に属している個人が、偽装されたメールやサイトを信用してしまえば、防ぎようがありません。そのために、これらの攻撃に対してはユーザへの啓蒙活動が重要です。怪しいメールやサイトに対してはすぐにアクセスをせずに、真偽を確認してから対応するようにすることが必要です。しかし、何をもって本物か偽物かを確認するかは容易ではないので、例えばメールのリンクのURLやサイトのドメイン名を確認したりするなどの具体例を挙げて説明しないと、なかなか判断ができるものではありません。

私の会社でも、これらの攻撃への対策として社員全員にEラーニングの受講を必須にしており、定期的に受講することが求められています。しかしながら、これくらい徹底的に啓蒙活動をしても、すべての攻撃を防ぐことができずに、ときどき被害の報告がされています。

今後は技術的な攻撃だけではなく、このようなソーシャルエンジニアリング的な攻撃で大きな被害を生む可能性があると思われます。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１６：サイバー攻撃（その６）情報漏えい

サイバー攻撃（その6）情報漏えい

機密情報や個人情報などの重要な情報が不正に外部に流出しないように、情報漏えい対策が必要です。昨今はノートPCやスマートフォンといった情報端末のHDDなどに様々な情報が保管されているために、情報端末の物理的盗難や紛失または重要な情報ののぞき見が発生した場合は、情報漏えいのリスクが高まります。

そのような盗難・紛失やのぞき見（ショルダーハック）への物理的情報漏えい対策として、次のような対策があります。

- のぞき見防止フィルム：正面以外からは画面を見えにくくする保護フィルム
- クリアスクリーン：スクリーン画面上にフォルダやショートカットなどの設定をしなかったり、認証機能付きスクリーンセーバーを使う
- セキュリティワイヤ：物理的なカギで情報端末を机などに固定する
- クリアデスク：離席時は書類や情報端末を施錠した場所に保管する
- シンクライアント：情報端末側でデータを保存しない
- モバイル端末管理：端末の設定やアプリケーションを一元管理して、リモートによるデータ消去などができるようにする

情報の廃棄時には、記録媒体（HDDなど）の情報をデータ消去用ソフトなどですべて上書きしたり、書類などの紙媒体などもシュレッダーで断裁して再読不可能にしたりする必要があります。そのうえで、適切な産業廃棄物処理業者に廃棄処理を委託して、マニフェスト（廃棄物管理票）を発行してもらいます。

また、アクセス権限を持った人間が機密情報や個人情報を不正に持ち出したり、盗み出したりする内部不正について、次のような対策も必要です。

- 牽制：不正行為を思いとどまらせる。別担当による相互牽制など。
- 監視：状態を監視する。アクセスログの履歴管理や入退管理、監視カメラによるモニタリングなど。

マイノート（これまでの私の体験・見聞から一言）

情報漏えいを防ぐには、技術的なセキュリティ対策だけでは十分ではありません。特に物理的なセキュリティ対策が必要となってきます。
ノートPCやスマートフォンなどは持ち運びすることが多く、それらが紛失するリスクは結構な確率で発生しますし、特にデータを保存した外付けHDDやUSBメモリなどの記憶媒体は紛失をする可能性は高いです。したがって、そのような情報端末には機密情報や個人情報などのデータを保存しないことが基本です。しかしながら、それらのリスクに対する認識が低かったりすると、外付けHDDやUSBメモリはデータの持ち運びに大変便利なので、つい重要なデータを保存してしまいます。

私自身も情報端末や記憶媒体の紛失の報告を受け、都度対応をした経験がありますが、様々なリスクを検討して判断しなければならないので、大変難しいですね。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１７：ITセキュリティ関連法規

ITセキュリティ関連法規
ITセキュリティに関連する法律を下記に挙げてみます。

- 個人情報保護法：個人情報の有用性に配慮しつつ、個人の権利利益を保護する。
- 電子計算機に関する刑法：電子計算機や電磁的記録に関する破壊などでの業務妨害行為や虚偽の情報などでの詐欺行為を取り締まる。
- 不正アクセス禁止法：不正アクセス目的の他人のID・パスワードの取り扱いを規制する。
- 特定電子メール法：迷惑メールやチェーンメールを規制する。広告宣伝メールを配信する場合には、事前に相手に承諾と同意を得なければならない。（オプトイン方式）
- サイバーセキュリティ基本法：サイバーセキュリティ戦略を定め、戦略本部を内閣に置く。

また、IT関連の創作物を保護するために、次のような知的財産権が定義されています。

- 著作権：文化的な創造物に対する権利で、創造者の表現や利益保護を目的とする。プログラム言語やアルゴリズム・プロトコルは保護対象外だが、プログラム（ソースコード）やウェブサイトなどは保護対象となる。また、著作権者の許可がない情報公開やアップロード、コピーなどは違反行為であるが、次の条件では自由に利用することができる。
    - 私的目的：自分など限られた範囲内での複製
    - 引用：正当な範囲内で引用として利用
    - 商品紹介：商品出典の際の紹介として利用
    - 非営利目的：営利を目的としない著作物の上演など
- 産業財産権：新しい技術、新しいデザインなどの扱いについて独占権を与え保護するための権利で、次のようなものを対象としている。
    - 特許権：発明、自然法則や仕組みを用いた高度な創作物。
    - 実用新案権：考案、発明ほど高度でない創作物。
    - 意匠権：デザイン、形状、模様、色彩などの工業物。
    - 商標権：識別標識、会社名や商品名など。

マイノート（これまでの私の体験・見聞から一言）
ITセキュリティに関連する法律は、コンピュータシステムやデータ、それを利用するユーザを保護することを目的としています。そして、それらが適切に保護されていないと、私達の生活に支障をきたすことになるぐらい、ITセキュリティが身近なものになっていると思います。これらを遵守するためには悪意のある攻撃から守ることももちろん重要ですが、自分たちがしっかりと意識していないと違反行為をしてしまう可能性があることも認識しておく必要があると思います。

私の経験から特に注意が必要だと思われるのは、個人情報の取り扱いやオプトインの取得です。広告宣伝メールはできるだけ多くの人達に配信をしたいものですが、事前に同意を取得しておくことが必要ですので、これらのチェックは重要です。また、個人的にも注意をしなければならないのが、著作権の保護です。うっかり著作権者の許可なく情報公開などをしないように気をつける必要があります。

ITセキュリティ入門

ITセキュリティ入門（IT初心者向け）－１８：ITセキュリティ管理活動

ITセキュリティ管理活動
ITセキュリティに関連する管理については、次のような活動があります。

- システム監査

組織の情報システムに対して、監査対象とは関わりを持たない第三者であるシステム監査人が客観的に、安全性・信頼性・効率性の観点から、点検、評価して保証または助言をする。必要に応じて、指摘事項に対する改善勧告（フォローアップ）を行う。

- 情報セキュリティ監査

情報セキュリティに関する監査で、ISMSと整合性が取られている情報セキュリティ監査基準に基づいて実施する。情報資産が監査対象になり、リスクアセスメントに基づいた適切なコントロールの整備や運用状況を、点検、評価して保証または助言を与える。

- 内部統制

健全な経営を実現するために、必要な組織内部のルールや業務プロセスを整備、運用すること。目的としては、業務の有効性と効率化、財務報告の信頼性、法令遵守（コンプライアンス）、資産の保全である。対応（コントロール）としては、次の3つがある。

  - 牽制機能：故意への対処のために、相互監視、職務分掌（業務分掌）などの対策をする。
  - 誤謬機能：過失への対処のために、フールプルーフ（うっかりミス防止）、クロスチェック、教育などの対策をする。
  - 監視機能：内部統制が有効に機能しているか継続的に監視（モニタリング）・評価する。

- コーポレートガバナンス

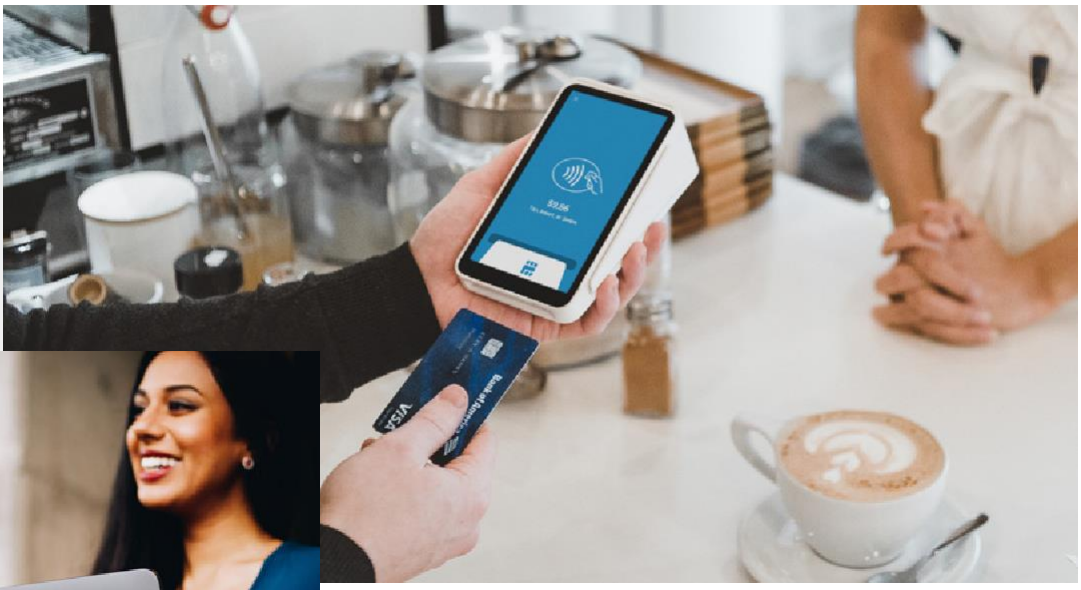
経営管理が適切に行われているか監視して、組織との利害関係者である顧客、従業員、株主、取引先などのステークホルダに対して組織活動の正当性を維持する仕組み。社外取締役を置くなどが、その例に当たる。

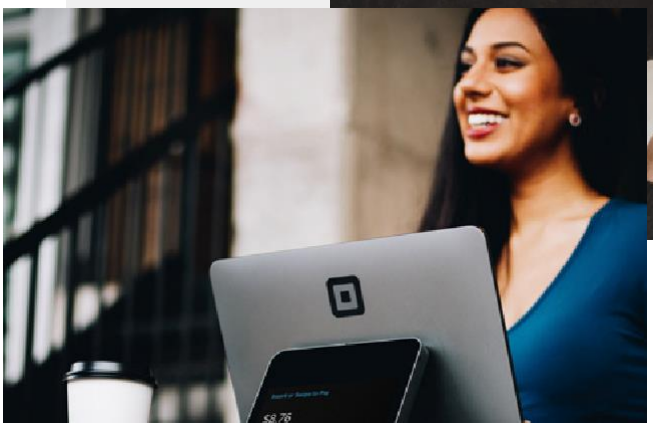
- ITガバナンス

企業の競争優位性を確保するために、IT戦略の策定・実行をコントロールして、あるべき方向に導く仕組み。ITを適切に活用する能力。

マイノート（これまでの私の体験・見聞から一言）
ITセキュリティが適切に管理・運用されているかを、適宜チェックすることは重要です。そして、その管理・運用状況を監視する体制を確保することも大切です。しかし、これらを維持していくことは容易ではありません。現場で日々の仕事に追われていると、業務優先でついITセキュリティを疎かにしがちですので、しっかりとした内部統制が求められると思います。

また、監査というと問題を指摘されてそのことで管理体制を評価されたり、非難されるように思いがちですが、本来はその指摘を管理・運用を改善できる機会と捉えることが大切だと思います。そのためには、なかなか難しいとは思いますが、監査する側も監査される側もオープンな態度で監査に望むことが必要だと思います。





おわりに

私自身がIT部門、すなわち社内情報システム部門で実際に働いてきて、ときには奮闘したり、また苦労してきたなかで、私なりにこれは重要だと思うことや、これは一般の人達には案外認識されていないだろうと感じたことを書いてみましたが、いかがだったでしょうか。

今回紹介した記事では、特定のシステムやツールなどについて具体的に記述したものはありませんが、セキュリティ担当者としてITを活用する際のセキュリティについて知っておくべき一般的な知識や考え方を挙げられたと私は考えています。そのようなことも踏まえて、これから一般企業内で新たにセキュリティ担当者に任命された方や、セキュリティ担当者として活躍したいと考えている方の参考になればと思っています。

なお、セキュリティ担当者といっても会社によってそれぞれ異なるかと思いますし、会社や人によってそれぞれ状況や立場が違うと思いますので、また違った問題や課題を抱えておられるかもしれませんね。

もし、何かご意見があれば、少しでもコメントいただければ幸いです。

お問い合わせ

ITコンサルタント：佐藤豊史（さとうとよし）のブログ