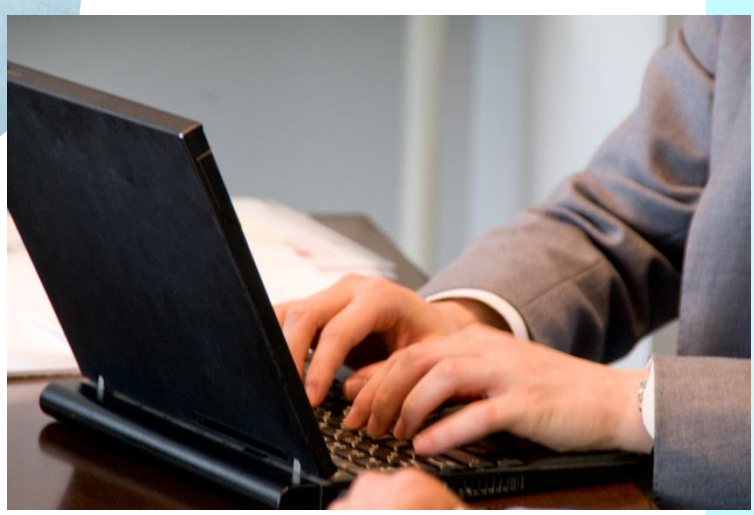
情報セキュリティ
～基礎の基礎～



永江信彦

◯. 目次

はじめに 2

1. 情報セキュリティとは 3

3つの要素を実現します 3

運用のこころがまえ 4

情報資産ってなに？ 5

2. リスク分析 7

リスクの大きさはこう考えます 7

こんな脅威があります 8

3. 情報セキュリティ対策 10

リスクをコントロールしよう 10

お金で解決できることもある 10

受け入れられるレベルまでリスクを下げる 10

デジタルだけではありません 11

事業所で使える一般的な対策 11

おわりに 13

はじめに

　情報セキュリティと言われるとどんな印象を持たれるでしょうか。なにか金庫に入れてがっちりと保護しておくようなイメージで考える人も多いと思います。もちろん、きちんと情報を保護することはとても大切なのですが、業務の中で情報を扱うときには守ることと合わせて使うことも考えておかなければいけません。

　このテキストでは、情報をきちんと保護しつつも適切に使うことで組織活動の助けとなることを目指し、そのための基本的な知識をお伝えしていきます。ここで記すことは情報セキュリティにおいての基礎になりますから、しっかり身につけて実務場面で応用してもらえることが私の希望です。

永江　信彦

1．情報セキュリティとは

3つの要素を実現します

「情報セキュリティをちゃんとしましょう」というと、どうしてもそのうちの一面に意識がいってしまいます。それは「情報をきちんと保護する」ということです。しかし、情報セキュリティというものを考えるときには組織（個人事業を含む）内で行われる活動に役立つものでなければいけません。

情報セキュリティとは次の3つの要素の実現を目指すものです。

機密性 Confidentiality
可用性 Availability
完全性 Integrity

＜機密性 Confidentiality＞

必要な人だけが情報に触れられるようにする

セキュリティという言葉から一番に意識が向くところであり、情報の漏えいや拡散を防ぐことを指します。書類を金庫に入れてカギをかけておいたり、パソコンで使用するアカウントにパスワードを設定しておいたりすることなどで実現できます。

また、もしも情報データが漏えいしても第三者に内容を読み取られないように暗号化しておくことも機密性の実現といえます。

＜可用性 Availability＞

必要な人が必要なときに利用できるようにする

情報を取り扱うことを許された人にとって、業務に必要な範囲内で情報が扱えるようになっていることはとても重要です。

例えばお客様との取引情報を保存したパソコンのパスワードを部長だけが知っていて、問い合せに対応する部下の担当者が部長が不在だと情報を利用できないとしたら業務が遂行できません。

組織が情報を保有するのは目的があってのことであり、その目的を実現するために担当者が情報を取り扱えるようにしておかなければいけません。

＜完全性 Integrity＞

保管されている情報が常に正確であるようにする

組織が利用する情報は正確でなければいけません。欠損したり改ざんされたりしないようにする必要があります。正しくない情報を使用した場合には組織の活動に支障をきたしますし、場合によってはお客様に損害を与えることにもなりかねません。

また、情報の完全性を意識すべき場面は保管されている状況だけではなく、情報を入手すると

きや通信・移送する場面も含まれることにも注意しましょう。

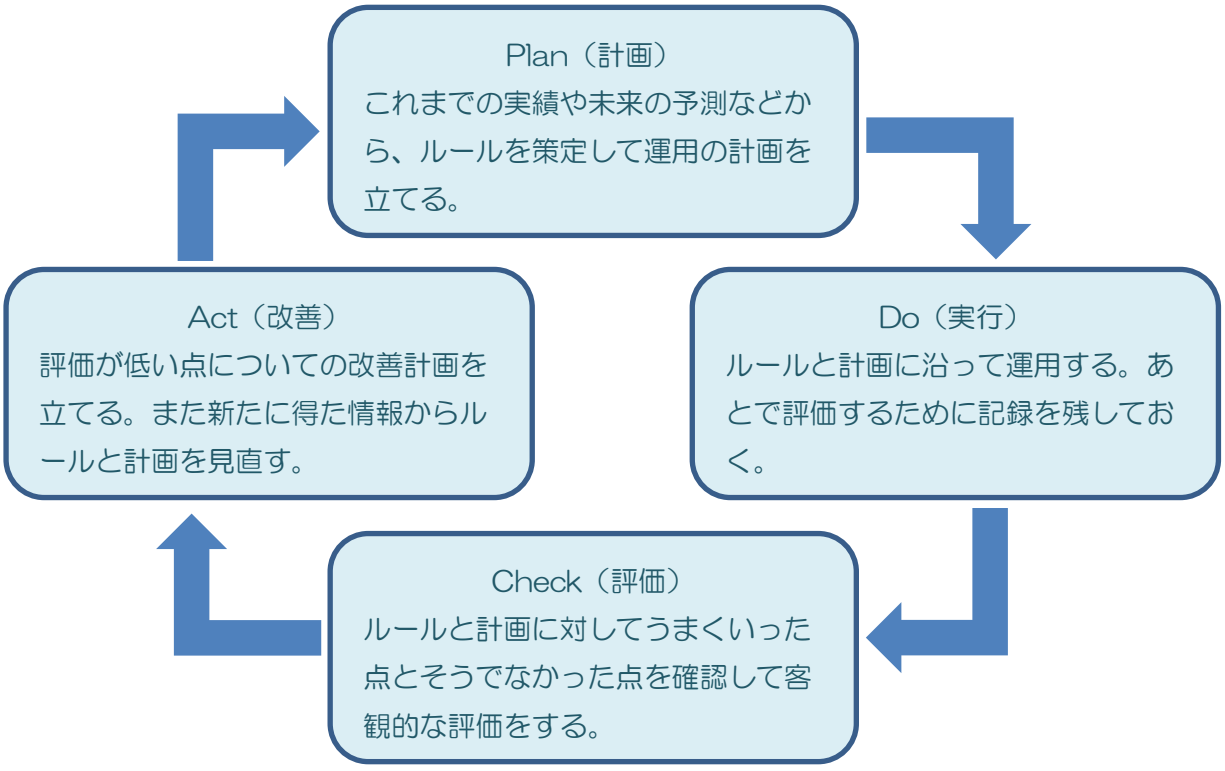
情報が正しくその状態を維持できるように施策を実行した保存媒体や通信機器を使わなくてはいけません。

運用のこころがまえ

＜PDCAサイクル＞

情報セキュリティの対策は、いちど用意すればその後は放置してよいというものではありません。継続的に見直しや修正を行うべきです。特にIT分野における社会的な状況は変化の速度が速いので、新しい情報を常に取り入れるようにして時代に合った対策の実行を目指します。

PDCAサイクルとは、生産や品質管理などに使われるマネジメントシステムの手法です。Plan（プラン＝計画）、Do（ドゥ＝実行）、Check（チェック＝評価）、Act（アクト＝改善）、の4つの段階を繰り返していくことで持続的・継続的な改善に役立ちます。



＜情報セキュリティのルールづくり＞

組織における情報セキュリティのルールづくりは一般的に3つの階層で考えられます。なぜなら、基本となる理念や考え方、それらに基づく判断基準、業務の現場における具体的な手順、と分けて設定しておく方がPDCAの各段階の実行がしやすいからです。

また、次に示す3つのうちで1と2をまとめたものを「情報セキュリティポリシー」としてWebサイト

などで公表する企業も多いです。

1. 情報セキュリティ基本方針（ポリシー）
   組織における情報セキュリティ対策についての基本的な方針や理念。内外に対しての宣言にもなる。

2. 情報セキュリティ対策基準（スタンダード）
   基本方針を実現するために何をしなければいけないのかを示す。
   例） パソコンを使うためには推測されにくいパスワードを設定する

3. 情報セキュリティ実施手順（プロシージャ）
   業務の各場面においてどのようにセキュリティ対策を実施するのかを定めた具体的な手順でありマニュアル。通常は組織外部に公開されることはなく、組織メンバーはこの手順にしたがって業務を遂行することで情報セキュリティ対策を実現する。
   例） パソコンを使うためのパスワードは8文字以上で設定する

情報セキュリティの運用ルールや計画は前述の3つの要素（機密性、可用性、完全性）を実現するための内容にします。1と2については企業がWebサイトで公表しているものが参考になります。3についてはそれぞれの組織固有の事情によって大きく異なる場合がありますが、一般的なものは本テキストの最後で紹介します。

情報資産ってなに？

情報セキュリティ対策は組織が保有したり使ったりする**情報資産**に対して行います。情報資産とは情報そのものと情報を利用するための道具や環境の総称です。

情報セキュリティ対策を実施すためには、情報資産の洗い出しが最初に必要です。見落としが無いように注意しましょう。また、後述する「リスクの大きさ」が小さいものは対象から外しがちですが、対策が必要かどうかの検討は必ずしましょう。

＜情報そのもの＞

紙に書かれていたりパソコンの中に保存されていたりと形は様々ですが、なんらかの媒体になんらかの事柄が記録されていればそれは情報であり情報資産だと考えましょう。

パソコンに保存されたエクセルデータ
CD に保存された画像データ
紙に書かれた電話メモ

ICレコーダに録音された音声データ
ホワイトボードに書かれた会議の議事録

組織が保護すべき情報には個人情報が含まれます。個人情報には顧客情報の他にも役員・従業員の情報も含まれるので、それぞれに適切なルール設定が必要です。

個人情報の定義

個人を識別できる情報、または他の情報と簡単に照合できて個人の特定ができるようになる情報。住所、氏名、年齢、などの基本情報のほかに、クレジットカード番号や病歴などのようなセンシティブ情報がある。

基本情報	住所、氏名、年齢、性別、生年月日、電話番号、メールアドレス、社員番号など
センシティブ情報	学歴、職歴、結婚歴、人種、民族、信教、思想、病歴、前科の有無、勤務先、クレジットカード番号、個人債務の状況、など

＜情報を利用するための道具や環境＞

情報を保存してある媒体（メディア）

紙、黒板、パソコン、サーバコンピュータ、CD－ROM、USBメモリ、カセットテープ、など

通信や運搬のための道具

パソコン、携帯電話、LANケーブル、ルータ、書類ケース、かばん、自動車、など

情報を利用するときの空間環境

建物、事務所のレイアウト、部屋や金庫などのカギ、パソコンのソフトウェア、など

情報セキュリティ対策を考えるときにはIT分野に重点を置きがちですが、物理的な環境整備についても漏れがないようにします。例えば、従業員情報を取り扱う総務部スタッフが使うパソコンのモニタは他の従業員から見えない確度で配置します。一方で総務部門は他部署との連携・連絡が必要ですから、閉鎖された個室空間のようにはならないようなレイアウトの工夫も大切です。

2. リスク分析

リスクの大きさはこう考えます

すべての情報資産に対して同じように情報セキュリティ対策をするのではなく、それぞれの情報資産によって異なる「リスクの大きさ」や実現すべき3つの要素（機密性、可用性、完全性）を考慮して対策の内容を考えます。

リスクの大きさは下記のような式で考えます。

情報資産のリスク　＝　情報資産の価値　×　脅威　×　脆弱性

情報資産の価値

扱っている情報の経済的価値。直接的に収益につながる価値とともに、問題が起きた時に発生する損害によっても算定する。

顧客の個人情報　＞　商品の仕入価格

脅威

問題が発生する可能性、発生しうる脅威の影響範囲などで考える。

ネット利用可能なパソコンへの外部からの攻撃　＞　大きな金庫で保管する書類の盗難

脆弱性

対策されていない状態での弱点。

施錠できない部屋　＞　セキュリティソフトが導入されたパソコン

この式で考えられる情報資産のリスクが大きいものは優先して対策を講じる必要があります。逆に、リスクが小さいと考えられるものについては許容することも含めて検討します。

考える練習

下記のそれぞれのケースについて情報資産としてのリスクの大きさを考えてみましょう。

1. 従業員の名簿（氏名、社員番号、所属部署、役職、メールアドレス）。パソコンで作成して紙に印刷されたもの。総務スタッフが使用するデスクの引き出し（鍵なし）に保管。総務スタッフの座席は全社員が一緒に使用するフロアの端にある。フロアには入退出管理システムによって従業員だけが入れる。

2. 仕入先情報（社名、代表者氏名、担当者氏名、取引の概要、支払いサイト（締日と支払日）、商品名、仕入価格、買掛金の履歴と残高）。仕入担当者のパソコンで作成されたエクセルデータ（パスワード設定済み）。保存場所は専用サーバ（アクセス権は仕入担当者とその上司）。サーバは従業員共有フロアのキャビネット（施錠なし）に設置。フロアには入退出管理システムによって従業員だけが入れる。

こんな脅威があります

情報資産の種類によって様々な脅威が想定されます。脅威や脆弱性の算定をするためには、どのような脅威が考えられるのかを知っておくことが必要です。また脅威に対する対策の不備や見落としは脆弱性となります。

ここでは情報資産に対する脅威を大きく3つに分けて紹介します。

＜物理的な脅威＞

情報資産が物理的に破壊や棄損されてしまう可能性であり、主に災害を想定します。建物の損壊や保管設備の破損などが想定され、最悪の場合は情報そのものを失うこともあります。

例） 地震、落雷、火事、水害、など

＜人的な脅威＞

故意か過失かを問わず、人間の行為によって発生する可能性です。悪意のある行為はもちろん、うっかりミスなども想定しておく必要があります。

例） 誤操作、記入ミス、持ち出し、置き忘れ、故意による漏えい

また、故意に情報を盗み取る手法として**ソーシャル・エンジニアリング**と呼ばれるものがあります。これは、会話の中で巧みに聴き出すことや、ゴミ箱をあさる行為、後方などからこっそり覗き見るなど、人の隙やミスに乗じて情報を盗み出す行為のことです。

＜技術的な脅威＞

IT機器を使う場面において通信技術を応用したり技術的な隙をついたりする脅威が考えられます。大規模な損害を発生させるケースもあるので適切な知識と対策が必要です。

傍受・盗聴

通信経路上で情報を盗み出したり、不正なWebページを用意して重要な情報を送信させたりする。通信パケットを傍受する「パケット盗聴」や偽サイトで情報を入力させる「フィッシング詐欺」などがある。

不正アクセス

本来は許可されていないコンピュータに対してインターネットなどの通信を利用してアクセスする行為。コンピュータ内の情報を盗み出すことやデータの破壊・改ざんを目的とすることが多い。

不正プログラム

コンピュータ・ウィルスなどのようにユーザが望まない挙動をするプログラム。マルウェアと総称され、その性質からウィルスの他にワームやトロイの木馬と呼ばれるものがある。

※主な分類は次ページに記載

・不正プログラム（マルウェア）の分類・

ウィルス	コンピュータ内のデータを破壊したりユーザが意図しないメッセージを表示したりする。感染と増殖が特徴であり、他のプログラムファイルに寄生して、自身を複製しながら別のコンピュータへと拡散していく。
ワーム	ウィルスと同様の問題を起こすが、ファイルに寄生せずに単体でコンピュータ内に存在する。
トロイの木馬	一見すると問題が無いソフトウェアの中に潜り込ませて対象のコンピュータに送り込まれる。コンピュータ内の情報を盗んでインターネットで外部に送信したり、外部からコンピュータを操作するために使われたりする。
ボット	なんらかの手段でコンピュータ内に侵入し、外部からの司令によって一斉に不正行為を始める。別のコンピュータへの攻撃の「踏み台」にするために使われたりする。
スパイウェア	コンピュータを使うユーザの行動や入力情報などを監視して外部に送信する。キーボード入力を盗み出す**キーロガー**はユーザ名やパスワードの漏えいに繋がる。

Dos 攻撃

サーバコンピュータに対して大量のリクエストを送信することで負荷を上げてサービスを停止させるなどする行為。Webサーバに対してはブラウザ表示時のF5キーで実行出来ることから「F5攻撃」とも呼ばれる。ボットを利用して複数のコンピュータから攻撃をしかけるものをDDos攻撃と呼ぶ。

3. 情報セキュリティ対策

リスクをコントロールしよう

情報資産が持っているリスクに対策を講じるときには、その大きさや置かれている状況に応じて個別に内容を考えることになります。対策手法を分類して考えてみましょう。

＜回避・予防＞

脅威と脆弱性を低減する手法です。脅威となる事柄を取り除いたり、脆弱性の原因となる箇所を改善したりして問題が起きにくい状況を作っておきます。情報を取り扱うスペース（事務所等）の施錠をして侵入者を防いだり、パソコンにセキュリティソフトを導入してウィルスの被害から防御したりすること等が該当します。

＜軽減＞

問題が起きてしまったときの損害や影響の大きさをあらかじめ低減しておきます。消火器や防火扉を設置することで火災が起きても最小限の被害ですむようにしておくことなどが該当します。

＜分散＞

重要な情報が一箇所に集約されていると業務には都合がよいですが、問題が起きたときに全ての情報が脅威にさらされます。情報を分散させておくことで万が一のときの被害を軽減することが有効な場合もあります。組織で使用するサーバコンピュータの物理的な所在地を複数に分けるケースなどがあります。

お金で解決できることもある

＜リスクの移転＝保険など＞

問題が発生したときの経済的な損失を第三者に移転しておく手法があり、それが損害保険などです。継続的な費用が必要ですが、脅威が現実になったときの補償額は費用に比べてはるかに大きいものになります。

また、情報の取り扱いを専門業者に委託することが有効な場合もあります。一般的に中小企業では高度なセキュリティを確保したサーバスペースを自前では確保できないので、ホスティングサービス（レンタルサーバスペース）を提供している事業者と契約します。

受け入れられるレベルまでリスクを下げる

情報資産のリスクを全く無くしてしまうことはほとんど不可能です。しかし、出来るだけリスクの大きさを小さくする必要があります。このときにリスクを小さくしようとするあまりにセキュリティを強

固にしすぎて「可用性」に問題があってはいけません。必要な業務を必要な人が行えるようにしつつ**許容できる範囲**にまでリスクを低減していくようにしましょう

情報資産のリスク ＝ 情報資産の価値 × 脅威 × 脆弱性

この式において、右にある項のいずれかの値が下がると情報資産のリスクが下がります。リスク分析を行うときに、例えば各項の評価を5段階としておけば、リスクの値は1から125の範囲となります。計算結果が20以下になったら許容するというルールにしておけばリスク分析とともに対策の評価についても考えやすくなります。

デジタルだけではありません

情報セキュリティというとパソコンに関することや通信における問題が考えられますが、物理的な課題についても考えておく必要があります。

例えば、ある大学で学生の試験に関する情報が紛失したケースでは、書類が入ったカバンを持った職員が電車を利用した際にカバンを車内に置き忘れるということが原因となっています。情報が電子データの形態をとっていたとしてもそれを扱う機材や場所は物理的な存在なので、物理的な面からのリスク分析や対策は忘れないようにしましょう。

また、情報セキュリティを成立、維持させるには情報を取り扱う人間に知識が必要になってきます。組織においては所属するメンバーに対しての継続的な教育や情報供給も欠かせないものになります。

事業所で使える一般的な対策

最後に、一般的な企業において考えられる情報セキュリティ対策を記します。これらの対策について、可用性も意識しつつ、有効で現実的な対応を計画して実行しましょう。

＜パソコンおよび通信ネットワークにおける対策＞

・パソコンにインストールするOSはメーカーのサポート対象となっている正規品を使う
・パソコンのOSは個別ログインとしてパスワードを設定する
・離席するときはパソコンをロックしておく
・パソコンにはセキュリティソフトを導入する
・パソコンの設定で拡張子を表示するようにしておく
・OSやセキュリティソフトの設定で自動更新を有効にする

・重要なデータはバックアップをとるようにする
・電子メールの添付ファイルはウィルスチェックをしてから開く
・電子メールはHTML形式ではなくテキスト形式を使う
・パスワード付きデータファイルを送信するとき、パスワードは別のメールで送る
・Office系ソフトのマクロ機能は信頼できるファイル以外では実行しない
・重要情報を扱うパソコンは有線LANを使う
・無線LANルータを使う場合は暗号化機能やステルス機能があるものを使う
・情報を保存できるメディアは持出しも持込みも禁止とする
・ホームページ等で顧客情報を送信してもらうページではSSL通信を使う
・パスワードは一定の頻度で変更する
・パソコンを廃棄するときは専用ソフトでデータを消去するか専門業者に依頼する
・記録メディアを廃棄するときは物理的に粉砕する

＜物理的または社会的な対策＞

・事業所は施錠できるようにしてカギを持つ人間は最低限にとどめる
・入退室管理システムを導入する
・「ひとり作業」はしない
・重要情報を扱う部署のエリアへの侵入を制限する
・重要情報を扱うパソコンのモニタを入口や窓に向けない
・会議後のホワイトボードは必ずきれいにする
・事務所外で業務に関する会話をしない（ビル共用部、飲食店、公共交通などは特に注意する）
・来客に対応する場所からは重要情報に関するものが見えないようにする
・来客の記録を残す
・書類を破棄するときは必ずシュレッダーで粉砕する
・私物を持ち込まない、社用品を許可無く持ち出さない
・情報セキュリティポリシーや実施手順を定めて従業員に周知徹底する
・情報の入手、保管、通信・移動、廃棄についてのルールを明確にしておく
・定期的に従業員に対する教育を実施する
・定期的にリスク分析と対策の見直しを行う
・それぞれの情報について利用できる従業員を明確にして徹底する

以上はあくまでも一般的な対策です。すべての組織で徹底すべき基本的なものもありますが、事情によっては困難なものも含まれると想います。それぞれの組織に合った適切な対策を考えるようにしましょう。

おわりに

先にも記述したように、情報セキュリティが目指すものは情報を閉じ込めておくようなことではなく、組織に必要な活用を適切にしていくことにあります。使う目的があるからこそ情報を保有しているのですから。

しかし、一方では、手元にある情報はやはりきちんと保護する必要があります。第三者に盗まれないように、望まない棄損や漏えいが起きないよう守るための手段を講じておくべきです。

組織活動の中で適切な情報の取り扱いが出来ているということは、保護と活用がバランスよく運用されているということです。そもそもの組織理念や組織の活動目的に沿った形で情報セキュリティのルールづくりや運用計画が成されなければ意味がありません。

まず組織の目的を明確にする、その中でどんな情報がどんな形で必要なのか、誰がどのようにその情報を活用するのか、ということを常に考えるようにしましょう。

永江信彦