4-1 人的セキュリティ対策

綿密にポリシや規定を作り上げて明文化しても、それを運用する人のセキュリティ意識が低ければ意味が有りません。教育などの活動によって啓発していく必要があります。

4-1-1 人的セキュリティ対策

人的セキュリティ対策では、情報セキュリティの重要性や対策の方針を組織全体に浸透させていく事が大切です。そのためにガイドラインを作成し、啓発活動を行っていきます。

□組織における内部不正対策

→組織における内部不正を防止する為には、内部不正対策の体制を構築することが重要です。「組織における内部不正防止ガイドライン（第5版）」によると、内部不正防止の基本原則は次の5つです。

1.犯罪を難しくする（やりにくくする）
2.捕まるリスクを高める（やると見つかる）
3.犯罪の見返りを減らす（割に合わない）
4.犯行の誘因を減らす（その気にさせない）
5.犯罪の弁明をさせない（言い訳させない）

具体的な内部不正対策としては、次のような事を実行していく必要があります。

①資産管理

→それぞれの情報にアクセス権を指定し、アクセス管理を行います。
また、機密情報には秘密指定を行い、外部に漏洩しない様に管理します。
また、しさん管理を効率的に行うためには、IT資産管理ツールの仕様が有効です。
PCなどの機器にインストールされているアプリケーションのバージョンが最新か一括でチェックできます。

②情報機器や記憶媒体の持ち込み、持ち出し管理

→持ち出し可能なノートPCやスマートフォンなどの情報機器や、USBメモリ、CD-Rなどの記憶媒体について、持ち出しの承認、記録等の管理を行います。
個人の情報機器や記憶媒体の業務利用や持ち込みは制限します。
また、持ち出すときに情報を暗号化するなどの対策を施す必要があります。

③業務委託時の確認

→業務委託をする場合には、セキュリティ対策を事前に確認・合意してから契約し、委託先が契約通りに情報セキュリティ対策を実施しているか定期的に確認する必要があります。

④証拠確保

→アクセス履歴や操作履歴のログ・証跡を残します。システム管理者のログ・証跡もきちんと残し、システム管理者以外の者が定期的に確認する必要があります。

⑤雇用終了時の手続き

→雇用終了時に、必要に応じて秘密保持義務を課す誓約書の提出を求める等、退職後の重要情報の漏洩等の不正行為が発生しない様にする必要があります。
また雇用終了時には情報資産をすべて返却し、情報システムの利用者IDや権限を

削除しなければなりません。

⑥適正な労働環境及びコミュニケーションの推進
→労働環境が悪く、コミュニケーションが十分に図れていないと、ストレスが溜まり、内部不正が発生するおそれが高まりやすくなります。
それを防ぐために、適正な労働環境と、適切にコミュニケーションが図れる環境を用意する必要があります。

⑦相互監視
→単独作業では不正が発生しやすい為、相互監視が出来ない環境での仕事を制限します。
具体的には、休日や深夜などの単独での作業を制限する必要があります。

□情報セキュリティ啓発
→情報セキュリティ啓発とは、情報セキュリティに関する意識や知識を向上させるための取り組みを周知徹底させていく活動の事です。
情報セキュリティ啓発の主な内容は次の様な活動になります。

①教育（情報セキュリティ教育）
→策定した情報セキュリティポリシの周知や、ソーシャルエンジニアリングに対する心構えなどについて、集合教育や各人への指導などによって教育していきます。
教育の対象は、派遣従業員や取締役なども含めた、組織に関係する全関係者となります。また、教育は業務に従事する者に対して業務を最初に行う前に実施し、従事後も定期的に実施します。内容は、対象者の担当業務や役割、責任に応じて変更する必要があります。

②訓練
→攻撃を受けた想定での実践や、手順にしたがって実施に対応するなどの訓練を行います。

標的型攻撃メールを実際に受け取ったときの対応を訓練する標的型攻撃メール訓練があります。また、実際のサイバー攻撃に近い形で疑似的なサイバー攻撃を行うレッドチーム演習があります。攻撃者の視点で様々な側面から攻撃を仕掛ける事でセキュリティ対策の実効性を検証できます。

③資料配布
→情報セキュリティに関する必要な事項を資料にまとめ、配布します。

④メディア活用
→動画やソーシャルメディア、eラーニングなど、様々なコンテンツを活用して啓発を行っていきます。

□パスワード管理
→パスワード管理の方法は、教育などで周知徹底させる必要があります。
そのポイントは次の通りです。

①質の良いパスワードを設定する。
→推測されにくく文字数の多いパスワードを設定する事が大切です。

②同じパスワードを使いまわさない
→システムごとに異なるパスワードを用意し、使い分けることが大切です。

③組み合わせでパスワードを管理する。
→パスワードを覚えられない時に紙に書いたりアプリで保管したりすると、
それが漏洩した場合に被害に会う可能性が有ります。
「アプリ+紙」など、複数の組み合わせでパスワードを管理すると
漏洩の危険性が下がります。

④パスワードをPCに保管しない
→パスワードやIDはPCに保管せず、毎回入力するようにします。
PCに記憶させて自動的に認証出来る様にしないことが大切です。

■利用者アクセスの管理
→利用者のアクセスを適切に制限するため、利用者が使用するアカウントに対して適切に
アカウント管理を行うことが重要です。アカウント管理では、技術的なアクセス制限
だけではなく、アカウントの運用管理を適正に行うことが必要となりとなります。

利用者アクセスを管理するときに意識するポイントには、次のようなものがあります。

①Need-to-know(最小権限)の原則
→利用者にアクセス権を設定する際の最も大切な考え方は、Need-to-know(最小権限)の
原則です。必要最小限のアクセス権を与え、行に必要のない情報は
見せないようにします。

②一人1アカウントの原則
→利用者のアクセス管理では、利用者一人ひとりを識別できるようにすることが重要です
そのため、一人ずつ別々のアカウントを設定し、誰がアクセスしているのかを
わかるようにします。

アカウントの共有や貸与は禁止し、一人一アカウントの原則でアカウントを管理します

③責務の分離
→最小権限、一人一アカウントを満たした後で、それぞれのアカウントに権限が
集中しないよう、責務の分離を行います。各人に業務に必要な最低限の権限を与え、
互いにチェックする体制を整えて相互牽制します、特に、職位の高い人にすべての
アクセス権を与えるなどの運用は不正を行いやすくしてしまうので、
職務に必要な最低限のアクセス権限を設定する必要があります。

具体的には、業務を実行する従業員には捜査権限、それを承認する上司には
承認権限のみを与え、上司に操作権限を与えないなどの運用を行います。

④特権アカウント管理
→通常の利用者権限と異なる、システムを変更することができるアクセス権を
特権的アクセス権といい、そのアクセス権をもつ赤つんとが特権アカウントです。
特権アカウントでも、最小権限の原則に沿って、アカウントを付与する利用者を
最小限にし、必要最小限の権限のみを付与します。

また、不正が生じたときに追跡しやすいように、特権アカウントで一人ひとりを識別
できるようにしておく必要があります。

⑤速やかな削除・変更
→アクセス権は、不要になった場合には速やかに削除することが肝心です。
退職者のアカウントなどをそのままにしておくと、不正アクセスが
起こりやすくなります。また、異動や業務の変更などで必要なアクセス権が
変わった場合にも、速やかに対応する必要があります。

会社の人事制度と連動させたり、ユーザーごとではなく、ロールを用いて
アクセス制御を行うなど、アカウントの変更管理を速やかに行う仕組みを
構築することが大切です。

■ログ管理と監視
→利用者のアクセスについては、ログ管理を行い、アクセスログを保管して、
誰がいつアクセスしたのかを正確に管理する必要があります。
ログを取得するだけではなく、ログを監視し、定期的にチェックすることが
大切です。

ログ管理では、ログを監視していることを周知するだけで、内部不正の抑止効果が
あります。ログを監視していることは周知するが、具体的な監視方法は知らせない
ことが、不正を防止するために最も効果的です。

■ファイルの属性の設定
→ファイルには、属性情報としてアクセス権を設定することが可能です。
通常は、読み取り、書き込み、実行の3種類の権限を設定します。
また、ユーザーごと、グループごとなどにアクセス権を設定することも
可能です。大切なのはNeed-to-knowの原則であり、
必要最小限のアクセス権限を設定することです。

■セキュリティクリアランス
→セキュリティクリアランスとは、政府が保有する安全保障上重要な情報にアクセスする
必要がある者に対し、その者の信頼性を調査・確認した上でアクセスを認める
制度です。政府が指定する重要経済安保情報を対象とします。適合事業者は、
政府の調査・確認を受けたのち、行政機関と契約を締結して情報開示を
受けることになります。

情報漏洩に対しては厳しい罰則が設けられています。

■秘密保持契約・誓約書

→秘密保持契約・誓約書は、従業員や取引先との間で秘密情報の取り扱いについて合意する文書です。雇用契約書や、別途用意した契約書に情報セキュリティに関する事項を盛り込んで契約します。秘密情報の定義、禁止行為、罰則などを明確に規定し、従業員に情報セキュリティ方針の順守を誓約させます。

雇用終了後も一定期間、秘密保持義務が続く様、契約で規定することが良くあります。

第5章法務

5-1 情報セキュリティ関連法規
⇒情報セキュリティ関連法規には、不正アクセス禁止法や個人情報保護法をはじめ
様々なものがあり、さらに新しい法規が追加され続けています。

5-1-1 サイバーセキュリティ基本法
→サイバーセキュリティ基本法では、国のサイバーセキュリティ対策の
司令塔として、内閣にサイバーセキュリティ戦略本部を設置する
事が定められています。

■サイバーセキュリティ基本法
→国のサイバーセキュリティに関する施策を進めるにあたっての基本理念や
国の責務などを定めた法律です。

サイバーセキュリティとは何かを明らかにし、必要な施策を講じるための基本理念や
基本的施策を定義しています。また、その司令塔として、
内閣にサイバーセキュリティ戦略本部を設置することが定められています。
国民には、基本理念にのっとり、サイバーセキュリティの重要性に関する
関心と理解を深め、サイバーセキュリティの確保に必要な注意を払う様努める
事が求められています。

さらに、様々な機関の情報共有の仕組みとして、サイバーセキュリティ協議会を
設置することも定められています。

■サイバーセキュリティとは、
→サイバーセキュリティ基本法の第二条では、サイバーセキュリティとは次のように
定義されています。

「電磁的方式により記録され、または発信され、伝送され、若しくは受信される
情報の漏洩、滅失または毀損の防止そのほかの当該情報の安全管理の為に
必要な措置並びに情報システム及び情報通信ネットワークの
安全性及び信頼性の確保の為に必要な措置が講じられ、
その状態が適切に維持管理されている事」

つまり、サイバー攻撃に対する防御行為全般をサイバーセキュリティ
といいます。

■サイバーセキュリティ関連の組織
→内閣サイバーセキュリティセンター
(NISC:National center of Incident readiness and Strategy for Cybersecurity)は、
サイバーセキュリティ基本法に基づき、
内閣にサイバーセキュリティ戦略本部が設置され、同時に内閣官房にNISC
が設置されました。

これらの組織は、国のサイバーセキュリティ対策の司令塔で、IT総合戦略本部や
国家安全保障会議などと連携して、国全体の安全を保障する為の活動を行います

また、公共の組織と各業界や団体が協力し、専門機関等から得られた対策情報を
戦略的かつ迅速に共有するための仕組みとして、サイバーセキュリティ協議会
が設置されています。

■政府機関等のサイバーセキュリティ対策の為の統一基準群
→政府機関等のサイバーセキュリティ対策の為の統一基準群は、
政府機関等の情報セキュリティ対策を統一するために定められた基準群で、
サイバーセキュリティ戦略本部が発表しています。
国の行政機関等のサイバーセキュリティに関する対策の基準となる
ガイドラインとなる物です。

政府機関等のサイバーセキュリティ対策のための統一規範や
サイバーセキュリティ対策の運用等に関する指針、対策基準策定の為の
ガイドラインなど、様々な基準や適用個別マニュアルが公表されています。
政府機関等のサイバーセキュリティ対策の為の統一基準では、
気密性、完全性及び、可用性それぞれの観点による情報の格付けの区分を
定義しています。

5-1-2 不正アクセス禁止法
→不正アクセス禁止法は、不正アクセスを規制する法律です。
実際の被害を与えなくても、不正なアクセスを行うだけで犯罪となります。

■不正アクセス禁止法
→不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）は、
インターネットなどでの不正アクセスを規制する法律です。
ネットワークへの侵入、アクセス制御のための情報提供を処罰の対象
としています。

不正アクセス禁止法では、被害が無くても不正アクセスをしただけ、
またはそれを助けただけの助長行為も処罰の対象と対象となります。
さらに、不正悪アセスを行わなくても、その目的で利用者IDや
パスワードの情報を集めただけで、不正に保管する行為として
処罰の対象となります。

■アクセス制御機能
→不正アクセス禁止法では、第一条に「アクセス制御機能により実現される電気通信
に関する秩序の維持」となり、アクセス制御機能を用いて利用者のアクセスを制限
することが推奨されています。不正アクセス禁止法の処罰の対象となるのは、
アクセス制御を超えて権限の無いコンピュータ資源にアクセスする事です。

■不正アクセス行為
→不正アクセス行為は、アクセス権限の無いコンピュータ資源にアクセスすることですが
具体的には次の様な事が想定されています。

・他人のIDやパスワードを盗用または不正使用し、その人になりすまして認証を行う事、
・認証サーバの脆弱性（セキュリティホール）などをついた攻撃で、

認証を行わずにコンピュータ資源にアクセスできるようになること
・目標の端末にアクセスするため、その端末のネットワークのゲートウェイの認証を不正に
突破し、目標の端末にアクセスすること

■不正アクセス行為を助長する行為
→実際の不正アクセス行為だけでなく、不正アクセスを助長する行為も処罰の対象と
なります。具体的には、IDやパスワードなどの認証情報を、
端末利用者や管理者以外の人に漏らすなどの行為が助長行為とされています。
ただし、情報セキュリティ教育を行う、注意喚起するなど正当な理由
がある場合には、処罰の対象となりません。

5-1-3個人情報保護法
→個人情報保護法は、個人情報を守るための法律です。個人情報保護マネジメントの
考え方に基づき、目的外利用の禁止や、個人情報保護マネジメントシステムの運用
などについて定められています。

■個人情報保護マネジメント
→個人情報とは、氏名、住所、メールアドレスなど、それ単体もしくは組み合わせる事に
よって生存している個人を特定できる情報の事です。
対象となる個人が死亡していたり、法人の場合には個人情報とはなりません。

個人情報保護の基本的な考え方は、個人情報は本人の財産なので、それが勝手に
別の人の手に渡ったり（第三者提供）、間違った方法（目的外利用）で
使われたり、内容を勝手に変えられたりしないように適切に管理する必要が
有るという事です。

そのためには、個人情報を守るシステムである
PMS(Personal Information protection Management System
:個人情報保護マネジメントシステム)を構築し、
ISMSと同様に維持管理していく必要があります。

個人情報保護に関するガイドラインは、JIS Q 15001として定められています。

■JIS Q 15001
→JIS Q 15001は、PMSを事業者が構築し、適切にマネジメントしていくための
仕組み作りについて定めている基準規格です。
個人情報の保護に関係する法律と整合性を図られた日本独自の規格で、
最新版は2023年に改正されたJIS Q 15001:2023です。

JIS Q 15001:2023(個人情報保護マネジメントシステム-要求事項)では、
主に次の事が要求されています。

・個人情報保護方針の策定と公表
・個人情報の特定（匿名加工情報なども含む）とリスク分析
・個人情報の利用目的の明確化
・内部規定を定め、個人情報を適切に管理する事（PDCAサイクル運用）

・本人の同意を得て、開示・訂正・苦情などに対応する事、

個人情報保護方針とは、個人情報保護に関する取り組みについて
文書化したもので、企業のWEBページなどで公開されています。

■OECDプライバシーガイドライン
→国際的なプライバシーに関する原則としては
OECD(Organization for Economic Co-operation and Development
:経済協力開発機構)が発表した、
OECDプライバシーガイドラインが有ります。
プライバシー保護と個人データの国際流通についてのガイドラインに関する
理事会勧告として出されています。

このガイドラインには、個人情報保護に関する次の
8原則(OECD8原則)が定められています。

1.収集制限の原則
→個人情報の収集は適法かつ不正な手段によらなければならない。
本人の認識や同意が必要。

2.データ内容の原則
→個人情報は、必要な範囲内で、正確で完全で最新のものでなければならない。

3.目的明確化の原則
→収集目的は、収集時に特定されていなければならない。

4.利用制限の原則
→収集目的を超えて開示、提供、利用されてはならない。

5.安全保護の原則
→紛失、改ざんなどのリスクに対して安全対策が必要。

6.公開の原則
→個人情報の取扱いについて基本方針を公開する。

7.個人参加の原則
→本人の求めに応じて、回答を行わなければならない。

8.責任の原則
→管理者は、1~7のルールに準拠する責任をもつ。

■個人情報保護法
→個人情報を守るために制定された法律が、
個人情報の保護に関する法律(個人情報保護法)です。
個人情報をデータベース等として保持し、事業に用いている事業者は
個人情報事業者とされ、
以下の事を守るために安全管理措置を行う義務が有ります。

・利用目的の特定
・利用目的の制限（目的外利用の禁止）
・適正な取得
・本人の権利（開示・訂正・苦情・利用停止・第三者提供記録など）への
対応（窓口での苦情処理）
・漏洩等が発生した場合の個人情報保護委員会やほんにんへの通知

個人情報などの第三者への提供は原則自由で、提供して欲しくに場合には
本人が拒否を通知するという仕組みをオプトアウトといいます。
これに対し、提供する為には本人の同意を得る必要が有る仕組みを
オプトインといいます。改正された個人情報保護法では、
オプトアウトの手続きが厳格化され、本人の同意を得ずに提供
する場合には、あらかじめ本人に通知する等の
措置を取ったうえで、
個人情報保護委員会への届け出が必須となります。

また、「人種」「信条」「病歴」など、
特別な配慮が必要となる要配慮個人情報は、オプトアウトでは提供できません。

個人情報の利活用については、後述する匿名化技法を用いた
匿名加工情報や、個人情報から氏名などの情報を取り除いた
仮名加工情報は、データ分析の為に利用条件が緩和されています。

■プライバシーマーク
→JIS Q 15001の要求を満たし、個人情報保護に関して適切な処理を行っていると
認定される事業者には、プライバシーマークの利用が認められます。

プライバシーマーク制度の認定は、JIPDEC(日本情報経済社会推進協会)
が行っています。

■マイナンバー法
→行政手続きにおける特定の個人を識別するための番号の利用等に
関する法律（マイナンバー法）とは、国民一人一人にマイナンバー（個人番号）を
割り振り、社会保障や納税に関する情報を一元的に管理するマイナンバー制度を
導入するための法律です。マイナンバー法には、内閣府の外局として、
個人情報を適切に取り扱うために設置された機関である個人情報保護委員会
について記載されています。

各種法定書類にマイナンバーが必要となるので、企業の従業員や個人事業主などは
関係する機関にマイナンバーを提示する必要があります。

■特定個人情報の適正な取扱いに関するガイドライン
→特定個人情報とは、マイナンバーやマイナンバーに対応する符号をその内容
に含む個人情報の事です。マイナンバーに対応する符号とは、
マイナンバーに対応し、マイナンバーに変わって用いられる番号や記号などで、
住民票コード以外のものを指します。

特定個人情報の適正な取り扱いに関するガイドラインは、個人情報保護委員会が
策定したもので、（事業者編）と（行政機関等・地方公共団体等編）の
２種類があり、特定個人情報を扱う際の注意点がまとめられています。

ガイドラインでは、マイナンバーの利用目的を特定し、源泉徴収票などの
特定の業務以外でのマイナンバーの利用を制限しています。
また、必要が無い場合にマイナンバーを請求することが制限されており、
委託する場合にも義務が限られ、監督責任が生じます。

さらに、不要になって一定の保管期間を過ぎた場合には速やかに廃棄する
事が定められています。

■プライバシー対策の3つの柱
→個々の組織やプロジェクトが個人情報保護対策を検討する前提となる、
個人情報保護に関する法律やガイドライン、指令等を
プライバシーフレームワークといいます。

このフレームワークを規範として、組織での個人情報保護がどのように
運用されているか、プライバシー要件を満たしているかについて、
組織の判断を支援するシステムが
プライバシー影響評価（PIA:Privacy Impact Assessment）です。

また、技術面からのプライバシー強化策は、
プライバシーアーキテクチャと呼ばれます。

これら3つがプライバシー対策の柱として運用され、個々の組織や
プロジェクトでカスタマイズされます。

■匿名化手法
→匿名化とは、個人情報を活用する際、その個人を徳的出来ないようにするために、
属性に対して削除、加工などを行うことです。
匿名化の手法としては、元のデータから一定の割合・個数でランダムに抽出
するサンプリングや、同じ保護属性の組み合わせを持つレコードが少なくとも
k個存在するように属性の一般化やレコードの削除を行うk-匿名化が有ります

匿名化手法を使用して作成した情報を匿名加工情報といい、データ分析など
で活用されています。また、個人情報を加工し、他の情報と照合しない限り
個人を識別できないようにした情報を、仮名加工情報といいます。
JIS Q 15001:2023では、個人情報だけでなく、匿名加工情報や
仮名加工情報、個人関連情報も、個人情報管理台帳で特定する
対象となりました。

5-1-4　刑法

→刑法の改正で、コンピュータ犯罪に関する条文が追加されました。
電磁的記録に関する犯罪行為、詐欺行為などに加え、ウイルスの作成・提供行為
なども対象とされています。

■コンピュータ犯罪防止法

→刑法では、1987年の改正から、コンピュータ犯罪も処罰の対象となりました。
その時に制定された刑法をコンピュータ犯罪防止法といいます。
コンピュータ犯罪防止法では、電子計算機損壊等業務妨害罪や
電子計算機使用詐欺罪など、様々な犯罪が定義されています。

①電子計算機損壊等業務妨害罪

→人の業務に使用する電子計算機（コンピュータ）を破壊するなどして
業務を妨害することを処罰する法律です。
企業が運営するWebページを改ざんする、またはその改ざんによって
企業の信用を傷つける情報を流すなどで、
業務の遂行を妨害した場合に適用されます。

また、実際に被害が発生せず、未遂に終わった場合にも罰せられます。

②電子計算機使用詐欺罪

→電磁的記録を用いて財産上不法の利益を得る犯罪を処罰する法律です。
虚偽の内容や不正な内容を作成する不実の電磁的記録の作出と、
内容が虚偽の電磁的記録を他人のコンピュータで使用する
電磁的記録の併用の2種類の累計が定められています。

インターネットを経由して銀行のシステムに虚偽の情報を送る事で、
不正な振り込みや送金を実現させることなどが該当します。

③電磁的記録不正作出及び共用罪

→人の事務処理を誤らせる目的で、その事務処理に関連する電磁的記録を
不正に作るという罪です。

④支払い用カード電磁的記録不正作出等罪

→人の財産用の事務処理を誤らせる目的で、その事務処理に関連する電磁的記録を
不正に作るという罪です。代金・料金の支払用のカード(クレジットカードや
プリペイドカードなど)や、預金等のカード（キャッシュカードなど）を
不正に作ると、この法律により罰せられます。

⑤不正指令電磁的記録に関する罪（ウイルス作成罪）

→2011年に改正された刑法で新たに追加された不正指令電磁的記録に関する罪
（ウイルス作成罪）は、マルウェアなど、不正な支持を与える電磁的記録の作成
及び提供を正当な理由が無いのに故意に行うことを処罰する法律です。

ウイルスの作成については、他人の業務を妨害した場合には、
もともと電子計算機損壊等業務妨害罪として処罰の対象となっています。
しかし、ウイルスの作成自体が、コンピュータ・ネットワークの

安全性に対する公衆の信頼を損なうものと考えられるため、
社会一般の信頼を保護するための法律として、
ウイルス作成罪が新設されました。

5-1-5 その他のセキュリティ関連法規・基準
→情報セキュリティ関連では、その他にも様々な法規があります。
また、情報セキュリティに関連する基準は、様々な省庁から公表されています

■その他のセキュリティ関連法規
→これまで取り上げてきた法規の他に、次の様なセキュリティ関連法規が有ります。

①電子署名及び認証業務に関する法律（電子署名法）
→インターネットを活用した商取引などでは、ネットワークを通じて
社会経済活動を行います。そのために、相手を信頼できるかどうか確認する
必要があり、PKI(公開鍵基盤)が構築されました。
そのPKIを支え、電子署名に法的な効力を持たせる法律に電子署名及び
認証業務に関する法律（電子署名法）があります。

電子署名法により、電子署名に押印と同じ効力が認められるようになりました。
電子署名で使う電子証明書を発行できる機関は認定認証事業者と呼ばれ、
国の認定を受ける必要があります。

②プロバイダ責任制限法
→WEBサイトの利用やインターネット上での商取引の普及、拡大に伴い、
サイト上の掲示板などでの誹謗中傷、個人情報の不正な公開などが増えてきました
こういった行為に対し、プロバイダが負う損害賠償責任の範囲や、
情報発信者の情報の開示を請求する権利を定めた法律がプロバイダ責任制限法
です。正式名称は「特定電気通信役務提供者の損害賠償責任の制限
及び発信者情報の開示に関する法律」
といいます。
ここで定義されている特定電気通信役務提供者には、
プロバイダだけでなく、Webサイトの運営者なども含まれます。

プロバイダ責任制限法では、他人の権利を侵害した書き込みがなされたとき、
プロバイダがそれを知らなかった場合には責任は問われないとされています。

③特定電子メール法
（特定電子メールの送信の適正化等に関する法律：特定電子メール送信適正化法）
→広告などの迷惑メールを規制する法律です。俗に迷惑メール防止法
と呼ばれることもあり、スパムメール（迷惑メール）を規制するための
内容となっています。

広告や宣伝の手段として送る広告宣伝メールの事を特定電子メールといいます。
特定電子メールでは、原則的にオプトイン方式が採用され、あらかじめ許可を
得た場合以外はメールを送信することが出来ません。

■情報セキュリティに関する基準
→情報セキュリティに関する基準は、経済産業省などがガイドライン・基準として
公開しています。主に以下のようなものがあります。

①コンピュータウイルス対策基準
→コンピュータウイルスに対する予防、発見、駆除、復旧のために
実効性の高い対策を取りまとめた基準です。

②コンピュータ不正アクセス対策基準
→コンピュータ不正アクセスによる被害の予防、発見、復旧や拡大、
再発防止のために、企業などの組織や個人が実行すべき対策を
取りまとめた基準です。

③ソフトウェア等脆弱性関連情報取扱い基準
ソフトウェアの脆弱性関連情報等