2023 年 7 月 5 日

情報セキュリティの基礎

～ はじめてシステム担当者になった時に知っておきたい基本とポイント　元地方公務員の情報セキュリティ担当者が語る　～

技術士（情報工学部門）
きよし事務所　代表　清　孝雄（Takao Kiyoshi）　著

情報セキュリティの基礎

　このテキストは、初めて市町村で情報セキュリティ担当者になった方向けに、情報セキュリティの基本的な知識と対策を紹介するものです。
　情報セキュリティは、市町村の業務に欠かせない要素であり、担当者として責任を持って取り組む必要があります。
　地方公共団体情報システム機構の研修受講をお勧めします。
　このテキストでは、以下の内容を学びます。

内容

1　情報セキュリティとは何か 2
(1) 情報セキュリティの定義と目的 4
(2) 情報セキュリティの三要素（機密性、完全性、可用性） 4
(3) 情報セキュリティに関する法令や規範 5
2　情報セキュリティの脅威と対策 8
(1) 情報セキュリティの脅威の種類と例 8
(2) 情報セキュリティの対策の分類と例 8
(3) 情報セキュリティの対策の実践方法 9
3　情報セキュリティの管理と監査 10
(1) 情報セキュリティの管理体制と役割 10
(2) 情報セキュリティの方針と計画 10
(3) 情報セキュリティの監査と改善 11

©きよし事務所清孝雄

1　情報セキュリティとは何か

セキュリティとは、安全、防犯、保安、防衛、防護、治安、安心、安全保障などの意味を持つ英単語です。

家のセキュリティを考えてみましょう。

セキュリティとは、家にあるお金や貴金属などの財産を盗難や災害から守るための対策のことです。鍵を複数つけ、金庫を用意したり、監視カメラや、ホームセキュリティの遠隔監視サービスに入ったりしますよね。火災保険などもありますね。

ホームセキュリティとは、自宅内、敷地内に設置したセンサーが異常を感知したときに、警備音で知らせたり、自動的にセンターや警備会社に通知し、必要に応じて安否確認の連絡や警備員が駆けつけたりし、事故を未然もしくは最小限に食い止める、家庭向けの防犯・防災・安全保持システムのことです。

一戸建てにおすすめの防犯対策としては、以下が挙げられます。　　出典「警視庁 HP」、自宅カメラなど

防犯カメラを設置する
玄関ドアを強化する
センサーライトを設置する
防犯ステッカーを貼る

ホームネットワークセキュリティの場合、家庭内にルーターで構成されるネットワークを守るための対策となります。

庁舎には、守衛さんがいたり、ガードマンを外部委託したりしていますよね。

防犯カメラを設置・監視、玄関ドアを強化していますよね。家庭と同じように庁舎管理をしています。

次に、銀行のセキュリティを考えてみましょう。

お客様の大切な資産（お金）を守るために、銀行が行っているセキュリティ対策のことです。銀行は、お客様の口座情報や取引履歴などの情報を適切に管理し、不正アクセスや情報漏洩などを防ぐために、以下のような対策を行っています。

パスワードや暗証番号の設定
セキュリティトークンの利用
SSL 暗号化通信の導入
不正ログイン防止機能の導入
外部記憶媒体の取り扱いルールの徹底

©きよし事務所清孝雄

また、銀行は、お客様が不正な取引に巻き込まれないよう、以下のような注意喚起を行っています。

不審なメールや電話には注意する
パスワードや暗証番号は定期的に変更する
セキュリティソフトを導入する

☕コーヒーブレイク　ちょっと一休み☕

「SECURITY」の語源は、ラテン語の *securus*（安全な）という単語から来ています。

***Se* ＋ *cura*　*se* ⇒ without（なし）、*cura* ⇒ care（心配）**

「心配なし」

「備えあれば憂いなし」と言いかえれますね！

情報セキュリティとは、住民の個人情報を守るための対策のことです。先ほどの「家（ホーム）のセキュリティ」と「銀行のセキュリティ」を合わせたようなものになります。

住民の個人情報を守るためには、以下のようなことが必要です。

- パスワードを設定する
- ウイルス対策ソフトをインストールする
- 不審なメールやサイトにアクセスしない
- 自分の情報を知らない人に教えない
- データを許可なく持ち出さない
- データを持ち出す場合、暗号化、パスワード付き、鍵付きケースで、複数人で運搬
- データを持ち出す場合、暗号化、パスワード付き、鍵付きケースで外部専門サービスへ

これらのことを守ることで、情報を守ることができます。

情報セキュリティとは、大切な住民の情報をさまざまな脅威から守ることです。住民情報は、市町村の業務に必要な資産であり、市民からの信頼にも関わります。だから、住民の情報を守ることは、市町村の重要な責務です。

©きよし事務所清孝雄

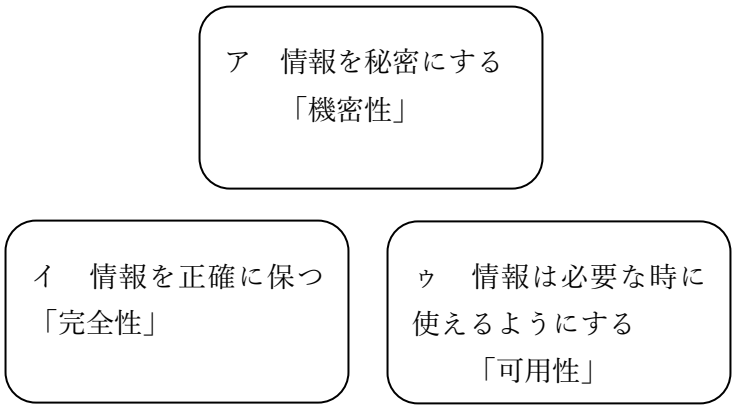
(1) 情報セキュリティの定義と目的

情報セキュリティとは、市町村が扱う様々な情報（個人情報、機密情報、マイナンバーを含む住民情報など）や情報システムに対する、改ざん・盗難・漏えい・暗号化などの様々な脅威から守ること、正しく安全に利用することです。

情報セキュリティの目的は、市町村の信頼性や業務効率を高めるとともに、市民の権利や利益を保護することです。

(2) 情報セキュリティの三要素（機密性、完全性、可用性）

情報セキュリティには、三つの要素があります。それぞれの意味を覚えておきましょう。



上記のア、イ、ゥは、それぞれ次のように定義されます。

ア　情報を秘密にする

「機密性」と言います。情報を知るべき人だけが知ることができるようにすることです。例えば、住民の秘密や、パスワードは他の人に教えないようにすることが機密性を守ることになります。

イ　情報を正確に保つ

「**完全性**」と言います。情報が正確で変更されていないことです。例えば、情報が改ざんされたり、消去されたりすることがないようにすることです。

ゥ　情報は必要な時に使えるようにする

「**可用性**」と言います。情報が必要なときに必要な人が利用できる状態を指します。例えば、情報システムがダウンしてしまった場合、情報を利用することができなくなってしまいます。そのため、情報システムの稼働率を高く保つことが必要です。

これらの要素をバランスよく確保することが重要です。

©きよし事務所清孝雄

☕コーヒーブレイク　ちょっと一休み☕

「CIA」とも言われます。

機密性、完全性、可用性はそれぞれ Confidentiality, Integrity, Availability と表記され、頭文字を繋げて CIA と呼ばれます。

横文字、3文字がお好きですよね！

(3) 情報セキュリティに関する法令や規範

情報セキュリティには、国や自治体が定めた法令や規範があります。これらは、情報セキュリティの基準やルールを示しています。例えば、

ア　個人情報保護法
　個人を識別できる情報（氏名、住所、電話番号など）を適切に取り扱う法律です。

イ　マイナンバー法
　社会保障や税金などに関する個人番号（マイナンバー）を管理する法律です。

ゥ　安全管理措置
　国や自治体が定めた情報セキュリティの対策や手順です。

エ　情報セキュリティポリシー
　情報セキュリティに関するルールです。

●情報の保護および個人情報の保護に関する法令は、
　個人情報保護法、マイナンバー法、電気通信事業法

●サイバー犯罪の取り締まりに関する法令は、
　サイバーセキュリティ基本法
　刑法（コンピュータ犯罪防止法）
　・電磁的記録不正作出及び共用（刑法 161 条の 2 ）
　・電子計算機損壊等業務妨害（刑法 234 条の 2 ）
　・電子計算機使用詐欺（刑法 246 条の 2 ）
　・公正証書原本不実記載等（刑法 157 条）
　・公用文書等廃毀棄（刑法 258 条）
　・私用文書等廃毀棄（刑法 259 条）

©きよし事務所清孝雄

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）
民法（不法行為の損害賠償、財産以外の損害賠償、名誉棄損の現状回復）
迷惑メール対策法（特定電子メールの送信の適正化等に関する法律）
児童ポルノ禁止法（児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律）

●円滑な電子取引サービスの支援に関する法令は、
電子署名法（電子署名及び認証業務に関する法律）
e―文書法（民間事業者等が行う書面の保存等における情報通信技術の利用に関する法律）（民間事業者等が行う書面の保存等における情報通信技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律）
IT 書面一括法（書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律）
電子帳簿保存法
プロバイダ責任制限法（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）

●知的財産権などに係る法令は、
知的財産基本法、著作権法
工業所有権と対象となる法律
・特許法、実用新案法、意匠法、商標法
不正競争防止法

●設備に係る法令は、
建築基準法、建築基準法施行令、消防法、電気通信事業法、電気事業法

●社員及び従業員に係る法令は、
労働基準法、労働者派遣法、地方公務員法など

●基準、ガイドラインなど
「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン（H20/8）」
「地方公共団体における ICT 部門の業務継続計画（ICT-BCP）初動版導入ガイド」
「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書」
「地方公共団体における情報セキュリティポリシーに関するガイドライン」
「地方公共団体における情報セキュリティ監査に関するガイドライン」
「地方公共団体等における特定個人情報等に関する監査実施マニュアル」
「コンピュータウイルス対策基準」
「コンピュータ不正アクセス対策基準」

©きよし事務所清孝雄

「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査票」
「情報システム安全対策基準（経済産業省）」
「情報システム安全対策指針（警察庁）」
「情報通信ネットワーク安全・信頼性基準（総務省）」
「通信販売等を中心とした顧客情報に関する個人情報保護指針」
「労働者の個人情報保護に関する行動指針」
「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」
「個人情報の保護に関する法律」
「システム監査基準」
「システム管理基準」
「システム管理基準　追補版（財務報告に係る IT 統制ガイダンス）」
「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）」
「情報セキュリティ管理基準」

これらの法令や規範を守ることは、情報セキュリティ担当者の義務です。違反すると、罰則や損害賠償などの責任を負うことになります。

☕コーヒーブレイク　ちょっと一休み☕

「情報セキュリティには絶対はなく、事故（インシデント）は起こりうるもの」です。

この前提に立って、対策をその場しのぎの対処療法で済ませるのでなく、自主的に継続的に改善・向上する仕組みが必要です。

対策は、IT 事故の影響を心配するあまり、利便性を犠牲にするのではなく、利便性と安全・安心の両立を目指すことが重要です。

©きよし事務所清孝雄

2　情報セキュリティの脅威と対策

(1) 情報セキュリティの脅威の種類と例

情報セキュリティの「脅威」とは、市町村の大切な住民情報を盗んだり、暗号化・壊したり、使えなくしたりすることです。情報セキュリティの脅威には、たとえば、以下のようなものがあります。

ア　マルウエア、ランサムウエアなど

コンピュータに感染して、情報を暗号化や破損したり、他のコンピュータに広がったりする悪いプログラムです。

イ　ハッキング

インターネットを通して、不正にコンピュータに侵入して、情報を盗んだり、操作したりすることです。

ゥ　内部犯行

市町村の職員や関係者が、故意に、うっかりして、情報を漏らしたり、改ざんしたりすることです。

(2) 情報セキュリティの対策の分類と例

情報セキュリティの対策には、大きく分けて物理的対策、技術的対策、人的対策の三つがあります。

ア　物理的対策とは､情報を扱う機器や媒体を盗難や紛失といった脅威から守ることです。例えば、鍵やロックをかけ施錠したり、防犯カメラを設置し監視をしたり、防火や防水で火事や水漏れを防いだりすることです。

イ　技術的対策とは、情報を扱うコンピュータやネットワークをマルウエア、ランサムウエアやハッキングといった脅威から守ることです。例えば、パスワードや暗号化を設定したり、ウイルス対策ソフトやファイアウォール、ふるまい検知、ログ管理・分析ツールなどを導入したり暗号化や電子署名で情報を保護したりすることです。

ゥ　人的対策とは、情報を扱う職員や関係者の意識や行動を改善し、うっかりミスや悪意のある行動による情報漏えいや破壊、盗難といった脅威から守ることです。例えば、パスワード管理やバックアップで情報を安全に扱うための教育や啓発で情報セキュリティ意識を高めるためのセキュリティ研修を実施したり、情報の取扱いに関する規則やマニュアルを作成し周知したりすることです。

©きよし事務所清孝雄

これらの脅威に対抗するためには、情報セキュリティの対策が必要です。情報セキュリティの対策には、以下のような分類があります。

(3) 情報セキュリティの対策の実践方法

情報セキュリティの対策を実践するには、以下のような方法があります。

ア　パスワード管理とは、コンピュータやネットワークにアクセスする際に必要なパスワードを適切に設定し、定期的に変更し、他人に教えないことです（利用していない、ゲストや退職者などのデータは速やかに削除する。）。

イ　バックアップとは、情報をコピーして別の場所に保存することです。万が一情報が消失したり破損したりした場合に備えるために重要です（ランサムウエア対策には、とても重要。）。

ゥ　教育とは、情報セキュリティに関する知識やスキルを職員や関係者に伝えることです。情報セキュリティの意義や脅威、対策などを理解し、正しい取扱い方を身につけるために必要です（これが、一番重要です。慣れも大敵です。）。

これらの対策を実践することで、市町村の情報セキュリティを向上させることができます。

☕コーヒーブレイク　ちょっと一休み☕

「ウイルスの感染したかも？」

まず、「抜線」
電源は切らないで、すぐに上司へ報告し、ネットワーク管理者へれんらくを。

無線LANを利用している場合は、「Wifiを切る」ことが重要です。
※　ちゃんと切れますか？

©きよし事務所清孝雄

3　情報セキュリティの管理と監査

⑴ 情報セキュリティの管理体制と役割

情報セキュリティの管理体制とは、市町村が情報セキュリティに関する方針や計画を策定し、実施し、評価し、改善するために必要な組織や役割を整備することです。例えば、情報セキュリティ委員会や情報セキュリティ責任者などがあります。

ア　情報セキュリティ委員会とは、市町村の最高責任者が主宰し、各部署の責任者が参加する組織であり、情報セキュリティに関する基本方針や計画を決定し、その運用状況や効果を監視する役割があります。市長が参加する庁議などに開催される場合もあります。

イ　情報セキュリティ責任者は、情報セキュリティ委員会の指示に従って、部署内の情報資産の管理やリスク分析、教育・訓練、事故対応などを行います。また、情報セキュリティ責任者は、部署間の連携や協力を図り、市町村全体の情報セキュリティレベルの向上に貢献します。情報セキュリティ責任者は、市町村の情報セキュリティにおける重要な役割を担っていると言えます。

⑵ 情報セキュリティの方針と計画

情報セキュリティの方針と計画とは、市町村が情報セキュリティを確保するために定める目標や手段のことです。

ア　情報セキュリティ基本方針とは、市町村が情報セキュリティにどんな考え方で取り組むか、情報セキュリティに対してどのような姿勢や基準を持つかを示す文書です。

例えば、「市町村の情報資産は重要であり、その機密性、完全性、可用性を確保することが市民サービスの向上につながる」というようなことを書きます。これを情報セキュリティ基本方針といいます。

イ　情報セキュリティ計画とは、市町村が具体的にどのような対策を行うかを示す文書です。例えば、「パスワードは定期的に変更する」、「ウイルス対策ソフトは常に最新にする」、「教育研修は年に一回実施する」というようなことを書きます。これを情報セキュリティ計画といいます。

©きよし事務所清孝雄

⑶ 情報セキュリティの監査と改善

市町村では、様々な種類の住民情報を扱っています。その中には、個人情報や機密情報など、重要度が高く、漏えいや改ざんされると大きな問題になるものもあります。例えば、マイナンバーは個人を特定できる番号であり、税金や社会保障などに関係する重要な情報です。

マイナンバーを含む個人情報を適切に保護するために、「個人番号法」や「個人情報保護法」などの法令に従って安全管理措置を講じる必要があります。

安全管理措置とは、情報を保護するために行うさまざまな活動です。例えば、

- パソコンや書類などの物理的な保護（施錠や鍵付き引き出しに入れるなど）
- パスワードや暗号化などの技術的な保護（不正アクセスやデータ漏えいを防ぐなど）
- セキュリティ研修やルールの周知などの人的な保護（意識や行動の改善を促すなど）
- セキュリティルールの自己点検など人的な保護（意識や行動の改善を促すなど）

などがあります。これらの安全管理措置は、情報セキュリティの方針や計画に基づいて実施されます。もちろん、外部委託業者に対しても契約前に実施します。

しかし、安全管理措置を実施したからといって、情報セキュリティが完璧になるわけではありません。常に新しい脅威が出現したり、人間のミスや不注意が起こったりする可能性があります。そこで、情報セキュリティの監査と改善が必要になります。

情報セキュリティの監査とは、情報セキュリティの監査とは、市町村が決めた方針や計画に沿って、実際に情報セキュリティの対策が行われているかを確認すること、また、安全管理措置が適切に実施されているかどうかをチェックすることです。例えば、

- パスワードの強度や有効期限を確認する
- パスワードは定期的に変更されているか
- ウイルス対策ソフトは常に最新になっているか
- セキュリティ研修の受講率や理解度を確認する
- 業務に関係のないサイト閲覧がされていないかを確認する
- 教育研修は会計年度職員を含め必要な職員が適時に全員受講しているか
- バックアップの取得や保存状況を確認する

などがあります。情報セキュリティの監査は、定期的に行うほか、不定期に行うこともあります。監査の結果は、報告書にまとめられ、情報セキュリティ委員会や情報セキュリティ責任者に提出されます。

©きよし事務所清孝雄

☕コーヒーブレイク　ちょっと一休み☕

「情報セキュリティ監査には「保証型」と「助言型」があります。
・「保証型」は、情報セキュリティマネジメントについてのいわば「お墨付き」を与える形式。
ただし、「インシデントが発生しない」ことを保証するものではない。
「基準」に準拠しているか否かを保証するもの。
・「助言型」は不備な点、基準とのギャップを指摘するもの。
※　監査実施結果は、実施したこと、概ね良好であったことまで公表し、脆弱性については、公表しないこと。

情報セキュリティの改善とは、監査で見つかった問題や不足点などの監査の結果をもとに、安全管理措置を見直したり、改善策を立案したり、実行したりすることです。例えば、

- パスワードの変更や更新を促したり、通知方法を見直す
- ウイルス対策ソフトの更新方法を簡単にする
- バックアップの取得や保存方法を改善する
- 教育研修の内容や方法を改善する

などがあります。情報セキュリティの改善は、監査と連動して行われます。改善の効果は、次回の監査で確認されます。

情報セキュリティの監査と改善は、情報セキュリティのレベルを高めるために重要なプロセスです。しかし、万が一、情報セキュリティ事故（情報漏えいや改ざんなど）が発生した場合は、迅速かつ適切に対応する必要があります。

情報セキュリティ事故対応とは、事故発生時に行う一連の活動です。例えば、

- 事故発生の確認と原因究明
- 事故発生の報告と連絡（上司や関係者へ）
- 事故拡大防止と復旧作業（パソコンやネットワークの切断や修復など）
- 事故影響評価と対外対応（被害者への謝罪や補償など）
- 事故再発防止策の立案と実施

などがあります。情報セキュリティ事故対応は、市町村内であらかじめ決められた手順やルールに従って行われます。事故対応は、情報セキュリティ担当者だけでなく、他部署や外部機関とも協力して行う必要があります。

©きよし事務所清孝雄