○上球磨消防組合情報セキュリティポリシー

平成26年11月1日
消防長訓令第3号

第1章　情報セキュリティ基本方針

1　目的

組合の各情報システムが取り扱う情報(以下「情報資産」という。)の中には、住民の個人情報のみならず組合運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。したがって、これらの情報資産及び情報システムをさまざまな脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、ひいては、このことが組合に対する住民からの信頼の維持向上に寄与するものである。

これらのことから、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠なことから、情報資産の機密性、完全性及び可用性を維持するための対策(以下「情報セキュリティ対策」という。)を整備するために、この上球磨消防組合情報セキュリティポリシー(以下「セキュリティポリシー」という。)を定めるものである。

2　定義

(1)　ネットワーク　コンピュータ等の機器が接続され、データの伝送等の処理を行うための通信網をいう。

(2)　インターネット　異なるネットワーク同士を相互に接続することにより、世界中に広がったネットワーク環境をいう。

(3)　情報システム　業務系の電子計算機(業務系におけるネットワーク、ハードウエア及びソフトウエア)及び記録媒体で構成され、処理を行う仕組みをいう。

(4)　情報セキュリティ　情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(5)　不正アクセス　利用する権限のない第三者が、ネットワークを通じて別の場所にあるコンピュータに不正に接続、侵入する行為のこと。

(6)　機密性、完全性及び可用性　国際標準化機構(ISO)がこれらについて定めており、機密性とは、情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること、完全性とは、情報及び処理の方法の正確さ及び完全である状態を安全防護すること、可用性とは、許可された利用者が必要な時に情報にアクセスできることを確実にすること、とそれぞれ定められている。

3　位置付けと職員の責務

セキュリティポリシーは、情報資産に関する情報セキュリティについて、総合的、体系的かつ具体的にとりまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、管理者をはじめとして情報資産に関する業務に携わるすべての職員及び部外委託者は、情報セキュリティの重要性について共通の認識をもつとともに、業務の遂行にあたってセキュリティポリシーを遵守する責務を負うこと。

4　情報資産の管理

情報資産は、重要度に応じた情報セキュリティ対策を施したうえ、管理すること。

5　情報資産の管理体制

情報資産について、幹部が率先して情報セキュリティ対策を推進、管理するための体制を確立すること。

6　情報資産への脅威

情報資産に対する脅威として特に認識すべきものは、以下のとおりである。

(1)　部外者による故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し、盗聴、改ざん、消去、機器及び媒体の盗難等

(2)　職員による意図しない操作、故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し、盗難、改ざん、消去、機器及び媒体の盗難並びに規定外の端末接続によるデータ漏洩等

(3)　地震、落雷及び火災等の災害並びに事故及び故障等による業務の停止

7　情報セキュリティ対策

上記で示す脅威から情報資産を保護するため、次の情報セキュリティ対策を講ずること。

(1)　物理的セキュリティ対策　情報システムを設置する施設への不正な立ち入り、情報資産への損傷及び妨害等から保護するために物理的な対策を講ずること。

(2)　人的セキュリティ対策　情報セキュリティに関する権限や責任を定め、全ての職員及び外部委託事業者にセキュリティポリシーの内容を周知徹底する等、充分な教育及び啓発が講じられるように必要な対策を講ずること。

(3)　技術におけるセキュリティ対策　情報資産を外部からの不正なアクセス等から適切に保護するため、次に掲げる対策を講ずること。

①　情報資産へのアクセス制御

②　ネットワーク管理等の技術面の対策

(4)　運用面におけるセキュリティ対策　緊急事態が発生した際に迅速な対応を可能とするため、セキュリティ対策に関する危機管理対策を講ずること。また、通常時においても、庁内システムの運用にあたり、次に掲げる対策を講ずること。

①　システム開発等の外部委託

②　ネットワークの監視

③　セキュリティポリシーの遵守状況の確認

8　構成

セキュリティポリシーを定めるにあたり、職員に対し浸透、普及及び定着させるものでなければならず、そのためには安定的な規範であることが求められる。しかしながら一方では、情報技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。したがって、一定の普遍性を持たせた部分については、この基本方針がその役割を果たし、情報資産を取り巻く状況の変化に依存する部分については、対策基準により規定することとする。

9　対策基準の策定

情報資産に対し情報セキュリティ対策を講ずるにあたり、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、対策基準の策定にあたっては、情報セキュリティ対策を行う上で必要となる基本的な要件、実施手順の策定、監視方法や評価、運用の見直し等の事項について明記することとする。

第2章　情報セキュリティ対策基準

1　基準の目的、対象範囲

(1)　この対策基準は、基本方針の規定に基づき、情報資産の機密性、完全性及び可用性を維持するための具体的な対策(以下「情報セキュリティ対策」という。)を示すことで、部外漏洩など情報に対するさまざまな脅威から情報資産を守り、事務の安定的運営及び組合に対する住民からの信頼の維持向上を図ることを目的とする。

(2)　対策基準の適用対象範囲を次のとおり定める。

①　消防本部、消防署及び分署に設置してあるすべての端末及びOA機器類(以下「端末等」という。)

②　消防本部、消防署及び分署における業務の円滑な遂行を図るため導入されたシステム全般(以下「庁内システム」という。)

(3)　職員及びすべての部外委託者は、情報資産を取り扱う場合、対策基準の規定で定める事項を遵守すること。

2　組織

(1)　情報管理室長は、情報セキュリティ対策業務を総合的に監視、統括する。

(2)　情報管理室員は、情報管理室長を補佐し、情報セキュリティ対策業務を適正に運営するため、情報セキュリティ対策業務に関する事務を所掌する。

3　電子情報の管理

(1)　庁内システムで扱う組合保有の電子情報(以下「電子情報」という。)については、ファイル、記録媒体等に入っている情報の種類が分かるよう適切な管理を行うこと。

(2)　情報管理室員は、業務外の者が容易に電子情報を閲覧できないよう措置を講ずること。

(3)　職員は、電子情報の複製、バックアップ等を通常の保管場所から外部へ持ち出し又は送付を行うときは、業務上必要最小限の場合に限るとともに、情報管理室員の許可を得たうえで行うこと。
(4)　取り出し可能な記録媒体の取扱い等運用方法については、別に定める。

4　電子情報の取扱い
(1)　電子情報を、電子メールを含むインターネット上で不特定多数の者に公開する際の基準については、上球磨消防組合情報公開条例(平成18年条例第7号)の規定を準用する。
(2)　電子情報のうち、個人に関する情報については特に細心の注意を払い取り扱うとともに、その基準については、上球磨消防組合個人情報保護条例(平成18年条例第8号)の規定を準用する。
(3)　すべての電子情報について、その情報を管理するための責任者を明確にすること。
(4)　システム管理者は、電子情報の管理状況について把握するとともに、重要性の高いものを中心に重要度を検討・分類し、分類後の電子情報についてリスクの評価を行うこと。

5　ユーザーID、パスワードの管理
(1)　ユーザーID、パスワード(以下「ユーザーID等」という。)については、正当な利用者であることを証明する情報であり、第三者に知られた場合、電子情報の漏洩、データの破壊、システムの不正利用などの事態を招く危険があるため、ユーザーID等を所有する職員が、各自の責任において管理すること。
(2)　職員は、ユーザーID等を業務以外の目的で使用してはならない。
(3)　職員は、第三者に対しユーザーID等を教えてはならない。

6　コンピュータウィルス対策
(1)　コンピュータの動作不能や、データの破壊のおそれがあるコンピュータウィルスに対し、職員は充分な注意を払う責務を負う。
(2)　職員は不審な電子メールが届いた場合、添付ファイルも含め十分注意すること。また、必要のない電子メールは削除するものとし、開く操作を行ってはならない。
(3)　外部と接続している端末等には、ウィルスチェックプログラムを必ず導入すること。
(4)　外部から入手したファイルについては、いかなる手段で入手した場合であっても、ウィルスチェックを行わなければならない。
(5)　万一のコンピュータウィルス被害に備え、定期的にデータのバックアップを行うこと。
(6)　ウィルス感染を発見した場合は、直ちに情報管理室員に報告すること。

7　ハードウエア利用時の心構え
(1)　サーバ室及び設置機器
①　ネットワークの基幹をなすサーバ等の機器(以下「サーバ等」という。)については、耐震・防火措置がされている管理区域が明確な場所(以下「サーバ室」という。)に設置すること。
②　サーバ室の入退室は、業務に必要な場合に限るものとし、業務に関係のない職員の入退室については、システム管理者が認める場合を除きこれを禁止する。
③　削除
④　サーバ等については、その装置を固定し、耐震・落雷等災害への対策を充分に行ったうえ、その対策の一環として予備電源を備えること。
⑤　外部へのネットワーク接続は必要最低限のものに限定すること。
(2)　設置端末
①　各部署に設置してある端末等についてはその所在を明確にするものとし、無断で部署外へ移動してはならない。
②　情報管理室員は、端末等の設置箇所について把握すること。
③　職員は使用している端末について異常がある場合は情報管理室員に報告すること。
(3)　機器の廃棄等　システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去のうえ、復元不可能な状態にする措置を講じなければならない。

8　ソフトウエア利用時の心構え
(1)　インターネット

① インターネットを利用して電子情報の受信及び発信を行う場合、職員はそれによって生じるリスクや社会的責任、法的責任を負うことを常に留意するとともに、不用意な行為、行動は特に慎むこと。
② インターネットを利用する場合、常に他者の立場や状況に配慮し、適切なコミュニケーションを行うよう心掛けること。
③ 職員は、インターネット上で以下の情報を発信・公開してはならない。
ア 公序良俗に反するもの
イ 性的な画像や文章
ウ 差別的なもの
エ 虚偽のもの
オ 他者の名誉・信用を傷つけるおそれのあるもの
カ 他者のプライバシーを侵害するおそれのあるもの
キ 組合の信用・品位を傷つけるおそれのあるもの
④ 職員は、以下の行為をしてはならない。
ア 庁内システムを他のシステムへの不正アクセスのための足場として使うこと。
イ 他のシステムへの侵入及び侵入後のデータの閲覧、改ざん行為など、他のシステムの運用を妨害し損害を与える行為
ウ 他人のユーザーID等、メールアドレスの盗用、偽造
エ 許可されていない大量メールの作成、コピー、送信、再送信
⑤ 情報管理室員は、庁内システムの適正利用の維持・管理を目的として、以下の項目について常に監視し、管理すること。その際、職員はこれに協力すること。
ア 職員が送受信した電子メールの履歴、内容
イ 職員がインターネットへアクセスした履歴、内容
⑥ 上記の規定を遵守のうえ、インターネットの個人的利用については、業務及び庁内システムの管理、運用に支障をきたさない限りこれを認める。

(2) 電子メール
① あらゆる電子メールシステムを業務目的及びこれに派生する個人的目的のために使用することを認める。ただし、以下のような使用についてはこの限りでない。
ア 法令及び組合の定める条例、規則等に反する使用
イ 業務に支障をきたす長時間の使用
ウ 個人的な営利活動のための使用
エ 庁内コンピュータ資源を不当に独占する使用
② 電子メールの作成、発信にあたっては、受信者に不快な意識や疑義を生じさせないよう、マナーを遵守して行うこと。
③ 電子メールを利用し、ユーザーID等、秘密情報などを発信することは避ける。必要な場合、暗号化するなどの措置を講じて発信すること。
④ 電子情報を転送する際は、関連法規を遵守したうえ慎重に行うこと。
⑤ 庁内の電子メールシステムを利用して外部のメーリングリストに参加することは、業務上必要な場合のみこれを認める。

(3) その他庁内システム
① 職員は、業務の遂行のため、庁内のネットワークを介し庁内システムを利用することができる。
② 情報管理室員は、前項の規定にかかわらず、特定の情報を扱うシステムについて業務上必要と認められる場合は、そのシステムを利用できる職員を制限することができる。

9 職員の心構え
(1) 電子媒体による問い合わせ等への対応
① 電子メールやインターネット等を利用した住民等からの問い合わせ、苦情又は要望等(以下「電子媒体による問い合わせ等」という。)の処理については、その事項、内容に応じて決裁を受けること。ただし、広く組合の構成町村内外に周知されている事項を回答する場合等、簡易なものについてはこの限りでない。

② 電子媒体による問い合わせ等に対する回答は、正確かつ迅速に行い、簡潔、明りょうな内容となるよう努めること。

③ 次の項目に一つでもあてはまる電子媒体による問い合わせ等については、上記規定にかかわらず、回答する必要がないものとする。

ア 氏名のないもの

イ 住所、電子メールアドレス、電話番号のうち、いずれの情報についても明確にわからないもの

ウ 誹謗・中傷・いたずら等、悪意をもった内容であると明確に判別できるもの

エ その他、回答の必要がないと認められるもの

(2) 端末等の利用にあたっての心構え

① 業務時間内の端末等の利用については、職員が遂行しなければならない業務又はそれに付随する業務に関する目的で利用することとし、それ以外の目的で利用してはならない。

② 業務時間外の端末等の利用については、業務及び庁内システムの管理・運用に支障をきたさない限り、利用することができる。

③ 上記規定にかかわらず、職員は端末等の利用にあたり、以下の行為をしてはならない。

ア 法令及び組合の定める条例、規則等に反する行為

イ 情報管理室員に無断で行う端末等の改造や構成変更、庁内システムの改修行為

ウ その他庁内システムに重大な支障をきたすおそれのある行為

(3) 関連法規の遵守

① 著作権侵害のおそれのある以下の行為を行うことを禁止する。

ア 他者のホームページや電子掲示板に載っている文章や写真などを、無断で他のホームページや電子掲示板に転載すること。

イ 他者の電子メールを無断で転載すること。

ウ 書籍、雑誌、新聞などの記事、写真を無断で転載すること。

エ テレビやビデオから取り込んだ画像やデータを無断で掲載すること。

オ 芸能人や著名人の写真、キャラクターを真似て描いた絵、音楽及び歌詞等のデータを無断で掲載すること。

カ 他人が作成したソフトウエアやそれを改変したプログラムを無断で掲載すること。

② 商品やサービスを識別するために設定してある商標について、誤解を招くような使用をしてはならない。

③ 本人の許可なく、その顔や容姿などを撮影し、その写真をインターネット上で公開、発信することは、肖像権の侵害となるためこれを禁止する。

④ 上記規定に定めるもののほか、職員は端末等及び庁内システムを利用する場合は、関連する法令等を遵守しなければならない。

10 運用・見直し

(1) 監視・監査

① 情報システムの安全性を高めるため、情報管理室員は常時使用状況を監視しなければならない。その際、使用状況について記録、保存のうえ、結果の情報は情報セキュリティ対策に活用すること。

② 情報管理室員は、必要に応じて情報セキュリティ対策の実施状況、適切な運用等について監査を実施することができる。

(2) 点検、更新

① 情報管理室員は、常時適切な情報セキュリティ対策を遂行することができるよう、セキュリティポリシーの点検を怠らないこと。

② 情報管理室員は、適切な情報セキュリティ対策を遂行するため、対策基準の一部又は全部を更新することができる。

11 周知

(1) 職員への周知

① 情報管理室員は、情報セキュリティポリシーについて職員に文書、電子媒体等により配布するとともに、変更が生じた場合はその都度周知を行わなければならない。

② 職員は、セキュリティポリシーの内容を理解したうえ、情報セキュリティ対策に充分配慮して業務を行わなければならない。
③ 職員は、セキュリティポリシーをみだりに第三者に公開してはならない。

(2) セキュリティ教育の実施

① 情報管理室員は、人事教養担当課と協議のうえ、随時情報セキュリティ対策等に関する教育活動を実施する。
② 前項の規定については、説明資料の配布及び周知により代えることができる。

附 則

この訓令は、令達の日から施行する。

附 則(令和2年消防長訓令第1号)

この訓令は、令達の日から施行する。