情報セキュリティポリシー
富山市管工事協同組合

平成２９年１月２５日 制定

序　情報セキュリティポリシーの構成

情報セキュリティポリシーは、富山市管工事協同組合（以下「本組合」という。）が所有する情報資産に関する業務に携わる全ての組合員及び組合員等及び外部委託事業者に浸透、普及、定着させるものであり、普遍的な規範であることが要請される。しかしながら一方では、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。

このようなことから、情報セキュリティポリシーを、一定の普遍性を備えた部分(情報セキュリティ基本方針)と情報資産を取り巻く状況の変化に適切に対応する部分(情報セキュリティ対策基準)に分けて策定することとする。

また、情報セキュリティポリシーに基づき、ネットワーク及び情報システムの情報セキュリティ対策の手順である実施手順を策定することとする。

文 書 名		内 容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づき、ネットワーク及び情報システムの情報セキュリティ対策を実施するための具体的な手順

第１章 情報セキュリティ基本方針

１　目的

本組合の各種情報システムが取り扱う情報には、個別業務で扱う個人情報のみならず組合業務運営上重要な情報など、漏洩や改ざん等が発生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、情報資産、情報資産を取り扱うネットワーク及び情報システムを漏洩や改ざん等の様々な脅威から防御することは、業務関係者の財産、プライバシー等を守るためにも、また、本組合の安定的な運営のためにも必要不可欠であり、ひいては、このことが本組合に対する外部からの信頼の維持向上に寄与するものである。

このため、本組合の情報セキュリティ対策を整備した、情報セキュリティポリシー（情報セキュリティ基本方針、情報セキュリティ対策基準）を定める。

このうち、情報セキュリティ基本方針は、本組合の情報セキュリティ対策の基本的な方針を定めるものである。

2　定義

(1) 組合員等

本組合の役員、職員（一時雇用者を含む）、組合員、検針員、作業員を含めた、当組合及び当組合の情報資産の一部を利用するすべての者とする。

(2) 外部委託事業者

当組合と、守秘義務を明記した契約を締結した、当組合の情報資産の一部を利用する者とする。

(3) ネットワーク

コンピュータを相互に接続するための通信網、通信機器及び記録媒体で構成された、情報伝達を行う仕組みをいう。

(4) 情報システム

コンピュータ及び記録媒体で構成された、業務処理を行う仕組みをいう。

(5) 情報資産

ネットワーク及び情報システム上で管理される電磁的に記録された情報をいう。

(6) 情報セキュリティ

情報資産の機密性、完全性、可用性(注)を維持することをいう。

(7) 情報セキュリティ対策

情報セキュリティの阻害要因から情報資産を守る為の手段をいう。

(注) 国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

機密性(confidentiality)

情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(integrity)

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(availability)

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

3　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本組合が取り扱う情報資産に関する情報セキュリティ対策について、総合的かつ体系的に取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。

4　組合員等及び外部委託事業者の義務

本組合が取り扱う情報資産に関する業務に携わる組合員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに情報セキュリティポリシーを遵守する義務を負うものとする。

5　情報セキュリティ管理体制

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ものとする。

6　情報資産の分類

情報資産はその重要度に応じて分類し、その分類に応じた情報セキュリティ対策を行うものとする。

7　情報資産への脅威

情報資産に対する脅威の発生度合や発生した場合の影響を考慮し、情報セキュリティポリシーを策定するうえで、特に認識すべき脅威は次のとおりとする。

(1) 外的要因

○ 部外者の侵入による、機器（通信機器、コンピュータ。以下同じ。）又は情報資産の破壊・盗難

○ 不正アクセス又は不正操作による、情報資産の破壊・盗聴・改ざん・消去

(2) 内的要因

○ 組合員等又は外部委託事業者の不正による、機器又は情報資産の持出

○ 認証情報又はパスワードの不適切管理による、情報資産の破壊・盗聴・改ざん・消去

○ 不正アクセス又は不正行為による、情報資産の破壊・盗聴・改ざん・消去

○ 搬送中の事故又は不適切管理による、機器又は情報資産の盗難

○ 規定外の端末接続による、データ漏洩

(3) その他

○ コンピュータウィルスによる、サービス及び業務の停止

○ 地震、落雷、火災等の災害による、サービス及び業務の停止

○ 事故、故障による、サービス及び業務の停止

8　情報セキュリティ対策

上記７で示した脅威から情報資産を保護するために、物理的、人的、技術的及び運用の観点からセキュリティ対策を講じるものとする。

9　情報セキュリティ対策基準の策定

上記８の情報セキュリティ対策を講じるに当たっては、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、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を明記した情報セキュリティ対策基準を策定するものとする。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するためには、その手順を具体的に定めていく必要がある。そのため、全てのネットワーク及び情報システムに共通のセキュリティ対策を明記した情報セキュリティ実施手順を策定するものとする。

11　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。

12　評価及び見直し

情報セキュリティ監査の結果や情報セキュリティポリシーを取り巻く状況の変化等に対応するため、情報セキュリティポリシーの評価及び見直しを行う。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための本組合業務全般の情報資産に関する情報セキュリティ対策の基準である。

１　管理体制

(1) 組織・体制

情報セキュリティの管理は、以下の組織・体制で行う。

・本組合理事会
・最高情報統括責任者(CIO)(注)
・統括情報管理者
・統括情報管理者補佐
・情報管理者

(2) 役割・責任

ア 本組合理事会

本組合理事会は、情報セキュリティの維持管理を統一的な視点で行うため、次の役割を負う。

・情報セキュリティポリシーの審議、更新
・教育・訓練等の計画の策定

イ 最高情報統括責任者(CIO)

理事長を、最高情報統括責任者とする。

最高情報統括責任者は、最高情報セキュリティ責任者（CISO）を兼務し、本組合における全てのネットワーク、情報システム、情報資産及び情報セキュリティに関する最終決定権限及び責任を有する。

ウ 統括情報管理者

理事長が指名した者を、統括情報管理者とする。

統括情報管理者は、最高情報統括責任者を補佐する。

統括情報管理者は、情報セキュリティ及び各業務の情報システムの責任者とする。

統括情報管理者は、本組合で所管している情報システムの開発、設定の変更、運用、更新等、情報システムに係る情報セキュリティ実施手順の作成、維持、管理等の承認を行う。ただし、軽易なものについては、統括情報管理者補佐が承認を行う。

エ 統括情報管理者補佐

理事長が指名した者を、統括情報管理者補佐とする。
統括情報管理者補佐は、統括情報管理者を補佐する。
(注)CIO：Chief Information Officerの略で、組織における情報戦略を考え、実現する責任者を言う。

オ 情報管理者
事務局長を、情報管理者とする。
情報管理者は、情報システムに係る情報セキュリティに関する権限を有する。
情報管理者は、情報システムの開発、設定の変更、運用、更新等を行う権限を有する。
情報管理者は、情報システムに係る情報セキュリティ実施手順の作成・維持・管理を行うとともに、定められている事項について組合員等に実施及び遵守させなければならない。
情報管理者は、使用する情報システムの機器や記録媒体について、第三者に使用させること、又は許可なく情報を閲覧させることがないように、適切な措置を講じなければならない。

(3) 情報セキュリティに関する統一的な窓口の設置（組合CSIRT(注)）
ア 事務局を、情報セキュリティインシデントの統一的な窓口の機能を有する組織（組合CSIRT）とし、情報セキュリティインシデントについて組合員等より報告を受けた場合には、その状況を確認しCISOへの報告が行われるようにする。
イ CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係組合員等に提供する。
ウ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、関係機関への通知・公表対応を行わなければならない。
エ 情報セキュリティに関して、関係機関との情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。
(注)CSIRT（シーサート）：Computer Security Incident Response Teamの略で、コンピュータやネットワークに係るインシデントについて調査、対応を行う組織。

2 情報資産の分類と管理
(1) 情報資産の分類
対象となる情報資産は、次の重要性分類に従って分類・管理する。
情報資産が複製された場合、その複製も原本と同じ分類として管理する。

重 要 性 分 類
Ⅰ 情報セキュリティの侵害により、市民の生命、財産、プライバシー等へ重大な影響を及ぼす情報。（個人情報及び秘密を要する情報）
Ⅱ 公開することを予定していない情報及びセキュリティ侵害が業務事務の執行等に重大な影響を及ぼす情報。
Ⅲ 上記以外の情報

※以下、重要性分類Ⅰ、Ⅱの情報資産を「重要な情報資産」という

(2) 情報資産の管理方法

ア 情報資産の管理

・情報資産へのアクセスについては、該当する分類に応じたアクセス権限を定めなければならない。

・情報資産は、その重要度に応じたサイクルで定期的に複製を取らなければならない。

・重要な情報資産及びその複製は、外部へ持出し又は送付してはならない。ただし、業務上、外部への持出し又は送付が必要な場合は、統括情報管理者の許可を得なければならない。

・情報資産をコンピュータから可搬記録媒体に記録する場合は、原則解読が困難な暗号化を施さなければならない。

イ 記録媒体の管理

・情報システムからの取出しが可能な記録媒体は、収納庫に保管する等、適切な管理を行わなければならない。

・重要な情報資産を記録した記録媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に保管しなければならない。

・重要な情報資産の複製は、自然災害を被る可能性が低い場所に保管しなければならない。

・記録媒体を搬送する場合は、組合員等又は守秘義務を明記した契約を締結した外部事業者に行わせるとともに、記録媒体の物理的な保護措置を講じなければならない。

ウ 記録媒体の廃棄

・不要となった記録媒体を廃棄する場合は、情報管理者の許可を得なければならない。

また、処理を行った日時、担当者及び処理内容を記録しなければならない。

・不要となった記録媒体を廃棄する場合は、当該媒体に含まれる情報資産を復元できないよう処置を行なわなければならない。

3 物理的セキュリティ

(1) ネットワーク及び情報システムの機器等

ア 機器の取付け

ネットワーク及び情報システムの機器を取付ける場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置しなければならない。

イ 電源

ネットワーク及び情報システムの機器に供給する電源は、その需要に対して十分な量を確保しなければならない。

ウ 配線

ネットワーク及び情報システムの配線は、傍受又は損傷等を受けることが

ないように可能な限り必要な措置を講じなければならない。

(2) 重要な情報資産を扱うサーバ等の設置

・重要な情報資産を扱うネットワークの通信制御機及び情報システムにおけるサーバは、十分なセキュリティ対策を講じた部屋（以下「サーバ保管室」という）又は不正操作や環境上の脅威等から保護された場所に設置するものとする。

(3) 事務室に設置されている端末

・情報管理者は、事務室に設置されている端末の盗難防止について留意しなければならない。

4　人的セキュリティ

(1) 情報セキュリティ対策の遵守義務

・組合員等は、情報セキュリティポリシー及び実施手順に定められている事項を遵守しなければならない。

・組合員等は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報管理者に相談し、指示等を仰がなければならない。

・組合員等は、使用する情報システムの機器や記録媒体について、第三者に使用されること、又は許可なく情報資産を閲覧されることがないように、十分な注意をはらわなければならない。

(2) 情報資産の守秘義務

・組合員等は、異動、退職等により業務を離れる場合には、知り得た情報を他に漏らしてはならない。

(3) 非常勤及び臨時職員の雇用に際しての管理

・非常勤及び臨時職員には、雇用及び契約時に必ず情報セキュリティポリシーのうち守るべき内容を理解させ、遵守させなければならない。

・非常勤及び臨時職員に端末による作業を行わせる場合においては、インターネットへの接続及び事務所内LANのメールの使用が不要の場合には、これを利用できないように設定しなければならない。

(4) 外部委託に際しての管理

・ネットワーク及び情報システムの開発、導入、保守等を外部委託事業者に発注する場合は、情報セキュリティに関し遵守すべき事項及び守秘義務を明記した契約を締結しなければならない。

(5) 教育・訓練

ア 教育

組合員等は、定められた研修に参加し情報セキュリティポリシー及び実施手順を理解しなければならない。

イ 訓練

統括情報管理者は、本組合理事会が定めた計画に基づき、組合員等に緊急時対応を想定した訓練を行わせなければならない。

訓練の計画に当たっては、各ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めることとする。

(6) パスワード等の管理

・組合員等は、自己のＩＤカードの管理及びパスワードの秘匿に関し、十分な注意をはらわなければならない。

・統括情報管理者は、組合員等の認証情報及びパスワードに関する情報を厳重に管理しなければならない。

(7) ネットワーク及び情報システムを使用する際の制限等

・統括情報管理者は、組合員等がネットワーク及び情報システムを使用するにあたって、業務目的に沿って正しく使用するよう、情報資産の取扱いや機器等に制限を加えることができる。

5　技術的セキュリティ

(1) ネットワーク

・外部へのネットワーク接続は業務上必要な場合のみ行うものとし、できる限り接続ポイントを減らさなければならない。

・ネットワークに使用する回線は、伝送途上において破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

(2) 情報システム

・情報システムは、情報管理者から操作を認められた者以外の者が操作できないように、利用者ID、パスワードの設定等の措置を講じなければならない。

・Webサイトにより情報を公開・提供する場合には、当該サイトに係るシステムにおいて、盗難、改ざん、消去、踏み台(注)、DoS(注)等に対する十分な防御措置を講じなければならない。

・メールサーバにおいては、他のシステムに対する攻撃の踏み台とならないように適切な管理を実施しなければならない。

(3) ネットワーク及び情報システムの情報資産

・アクセス記録等、ネットワーク及び情報システムの情報セキュリティの確保に必要な記録は、一定期間保存しなければならない。

・ネットワーク構成図等、ネットワーク及び情報システムの仕組みを表す記録は、その仕組みが廃止されるまで適切に保管しなければならない。

(4) アクセス制御

・統括情報管理者は、各ネットワーク及び情報システムの利用や他のネットワークとの接続などにあたって、アクセス制御を加えることができる。

(5) コンピュータウィルス対策

・統括情報管理者は、コンピュータウィルスの脅威に対し十分な対策を講じなければならない。

・組合員等は、コンピュータウィルスの感染に対し、十分な注意をはらわなけれ

ばならない。

(6) 不正アクセス対策

・統括情報管理者は、不正アクセスの脅威に対し十分な対策を講じなければならない。

(7) セキュリティ情報の収集

・統括情報管理者は、情報セキュリティに関する情報を収集し、必要なネットワーク及び情報システムのソフトウェアにパッチ(注)を当てる等、セキュリティ対策上必要な措置を講じなければならない。

・統括情報管理者は、これらの情報を定期的に取りまとめ、関係組合員等に通知するとともに、情報セキュリティポリシーの改定につながる情報については、本組合理事会に報告しなければならない。

・統括情報管理者は、緊急時対応計画に定める緊急に連絡すべき情報を入手した場合は当該計画に定める情報連絡先に連絡しなければならない。

（注）踏み台：管理者が気づかないうちに第3者に乗っ取られ、不正アクセスや迷惑メール配信の中継地点に利用されているコンピュータ

（注）Ｄｏｓ：ネットワークを通じた攻撃の１つ。相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃。

（注）パッチ：ソフトウェアに保安上の弱点（セキュリティホール）が発覚したときに配布される修正プログラム。

(8) 情報システム開発、導入、保守等

・情報管理者は、情報システムの開発、導入、保守等にあたって、対応の基準を明確にしなければならない。

6　運用

(1) ネットワーク及び情報システムの監視

・統括情報管理者は、セキュリティに関する事案を検知するため、常にネットワーク及び情報システムの監視を行わなければならない。

・統括情報管理者は、アクセス記録及び情報セキュリティの確保に必要な記録を必要に応じて分析、監視しなければならない。

(2) 情報セキュリティポリシーの遵守状況の確認

・情報管理者は、情報セキュリティポリシーが遵守されているかどうかについて、また、問題が発生していないかについて常に確認を行い、問題が発生していた場合には速やかに最高情報統括責任者及び統括情報管理者に報告しなければならない。

・組合員等は、情報セキュリティポリシーの違反が発生した場合は、直ちに情報管理者に報告を行わなければならない。情報管理者は、違反が発生し、それが情報セキュリティ上重大な影響を及ぼす可能性があると考えられる場合は、情報管理者、統括情報管理者及び最高情報統括責任者に報告しなければならない。

・情報管理者は、所管する業務でサーバ等のシステム設定が情報セキュリティポリシーを遵守しているかどうかについて、また問題が発生していないかについて定期的に確認を行い、問題が発生していた場合には速やかに適切に対処しなければならない。

(3) 運用管理における留意点

・統括情報管理者は、アクセス記録、メール受発信記録の情報を閲覧できる権限を有する職員を定めなければならない。

・情報管理者は、組合員等が常に情報セキュリティポリシー及び実施手順を参照できるよう配慮しなければならない。

(4) 事故、欠陥に対する報告

ア 組合員等は以下の場合、その状況を速やかに情報管理者に報告し、その指示に従い必要な措置を講じなければならない。

・情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合

・ネットワーク及び情報システムに関する事故、欠陥について住民から報告・連絡を受けた場合

イ 事故等の内容は、下記のルートにより速やかに統括情報管理者に報告しなければならない。

なお、重大な事故の場合は、最高情報統括責任者に報告しなければならない。

（ア）事務局内で発生した場合

職員→情報管理者→統括情報管理者補佐→統括情報管理者

（イ）組合員の社内で発生した場合

社員→組合員→情報管理者→統括情報管理者補佐→統括情報管理者

ウ 統括情報管理者は、これらの事故等を分析し、再発防止のための記録を保存しなければならない。

(5) 侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じる緊急時対応計画については、当組合情報セキュリティ実施手順に定める。

7 法令遵守

組合員等は、職務の遂行において使用する情報資産について、次の法令等を遵守しこれに従わなければならない。

・不正アクセス行為の禁止等に関する法律(平成11年法律第128号)
・著作権法(昭和45年法律第48号)
・個人情報の保護に関する法律（平成15年法律第57号)
・業務手続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（平成25年法律第27号)
・本組合定款(平成28年５月11日改正)

・本組合就業規則（平成28年11月22日改正）

8　情報セキュリティに関する違反に対する対応

(1) 違反時の対応

組合員等に情報セキュリティポリシーに違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

・情報管理者が、組合員等による情報セキュリティポリシー違反を確認した場合、当該組合員等に対し、違反行為を是正するよう指導しなければならない。

・情報管理者の指導によっても改善されない場合、情報管理者は、統括情報管理者又は統括情報管理者補佐の同意を得て、当該組合員等のネットワーク又は情報システムの使用を停止することができる。

・当該組合員のネットワーク又は情報システムの使用を停止した場合、統括情報管理者又は統括情報管理者補佐は、その旨を最高情報統括責任者に報告しなければならない。

(2) 懲戒処分

情報セキュリティポリシーに違反した組合員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、本組合定款、就業規則または契約書条項による懲戒処分の対象とする。

9　評価・見直し

(1) 監査

・最高情報統括責任者は、ネットワーク及び情報システムの情報セキュリティについて定期的に監査を行わなければならない。

・ネットワーク及び情報システムの開発及び保守を外部委託事業者に委託している場合、必要に応じて情報セキュリティポリシーの遵守について監査しなければならない。

(2) 点検

・統括情報管理者は、組合員等へのアンケート等によって、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうかについて、定期的に点検し、その結果を取りまとめ、最高情報統括管理者に報告しなければならない。

・統括情報管理者は、ネットワーク及び情報システムについて、定期的に点検を実施し、その結果について最高情報統括管理者及び理事会に報告しなければならない。

(3) 情報セキュリティポリシーの更新

・理事会は、監査及び点検の結果を踏まえ、定期的に情報セキュリティポリシーの実効性を評価し、必要な部分の見直しを行わなければならない。

・情報セキュリティポリシーの更新内容、時期については、理事会が決定する。