道 営 住 宅 管 理 シ ス テ ム

情報セキュリティ対策実施手順

平成２４年３月

建設部住宅局住宅課

目　　次

Ⅰ　総　則

1　目的

この手順は、北海道情報セキュリティ対策基本方針第７に基づき、北海道情報セキュリティ対策基準第26の定めるところにより、道営住宅管理システム（以下「住宅管理システム」という。）の運用等に必要な情報セキュリティ対策について定めるものとする。

2　適用範囲

（１）対象者

本手順の対象者は、住宅管理システムを開発（改修）、保守、運用及び利用する職員のほか、次に掲げる者を対象とする。

・　道営住宅等の指定管理者（ただし地方自治体を除く。以下「公募の指定管理者」と言う。）において指定管理業務（以下「管理業務」と言う。）に携わる者

（２）対象とする情報資産

本手順の対象とする情報資産は、住宅管理システム及び住宅管理システムで取り扱うすべての情報（ソフトウェア及びシステム内部又は外部記録媒体に記録された電磁的記録を含む。）を含めた総称を言う。

3　用語の定義

（１）情報セキュリティ対策

「情報資産」の機密を守り、誤った使用や持ち出し、持ち込み、改ざんを防ぎ、許可された者が必要なときに安全確実に利用できるよう、必要な対策を実施することを言う。

（２）情報システム管理者

情報システム管理者とは、建設部住宅局住宅課住宅管理担当課長を言う。

（３）情報システム担当者

情報システム担当者とは、情報システム管理者の指示を受け、住宅管理システムの開発（改修）、保守及び運用を担当する職員を言う。

（４）情報システム利用課長等

情報システム利用課長等とは、次に掲げる者を言う。

・　各総合振興局及び振興局建設指導課長（ただし、「北海道情報セキュリティ対策基準」の情報セキュリティ管理者と定められた者。）

・　公募の指定管理者の管理業務責任者

（５）情報システム利用者（職員等）

情報システム利用者とは、住宅管理システムを利用する次の者を言う。

・　建設部住宅局住宅課の職員

・　各総合振興局及び振興局建設指導課の職員

・　公募の指定管理者で管理業務に携わる者

Ⅱ　実施体制及び知識・技術の向上

1　情報セキュリティ対策の実施体制

住宅管理システムの運用に当たり、情報システム管理者及び情報セキュリティ管理者である情報システム利用課長等は、それぞれの役割分担を明確にした上で、相互に連携し、情報セキュリティ対策を実施しなければならない。

（1）情報システム管理者

情報システム管理者は、住宅管理システムの開発（改修）、保守及び運用に関するセキュリティ対策について次の責務を負う。

ア　住宅管理システムの運用等に係るセキュリティ対策の実施

イ　住宅管理システムの運用障害発生時における原因の究明、障害の復旧及び再発防止措置等の実施

ウ　情報システム利用者に対する情報セキュリティ対策に係る知識・技術習得に関する研修の実施、指導及び支援

（2）情報システム利用課長等

情報システム利用課長等は、利用する住宅管理システムのセキュリティ対策に関して次の責務を負う。

ア　情報セキュリティ対策ガイドライン（以下「ガイドライン」という。）及び本手順で定められている事項の遵守並びにこれに関する情報システム利用者の指導

イ　運用障害発生時における情報システム管理者への報告並びに情報システム管理者からの指示に基づく復旧及び再発防止措置等の実施

ウ　情報セキュリティ対策に係る職場研修の実施及び情報システム利用者による自己点検の指導

（3）情報システム利用者（職員等）

情報システム利用者は、住宅管理システムの利用に当たって、次により適切に取り扱わなければならない。

ア　本手順を遵守し、情報セキュリティ対策を行うこと。

イ　情報システム管理者及び情報システム利用課長等の指示に従うこと。

2　知識・技術の向上

情報システム利用課長等は、情報システム利用者が日ごろから取り組むべき情報セキュリティ対策について、ガイドライン、情報セキュリティハンドブック（以下「ハンドブック」という。）及び職場研修用資料等を活用して研修を行うものとする。

情報システム利用者は、ハンドブックにより日常的に自己点検を行う。

Ⅲ　情報資産

1　情報資産の管理

情報システム管理者は（1）に掲げる情報資産について、情報システム利用課長等は

（２）に掲げる情報資産について、また、情報システム利用者は（３）に掲げる情報資産について、それぞれ適切に管理するものとする。

なお、情報資産の詳細については、セキュリティ上、非公開とする。

（１）情報システム管理者

ア　住宅管理システムにおけるネットワーク関係機器

イ　住宅管理システムの業務内容に係る情報を記録したサーバなどＣＰＵ

ウ　上記ア、イに係る住宅管理システム、これらの機器に記録されたシステム仕様及び各種設定など、システムの開発及び運用管理に関する情報。また、イの機器に記録された情報システムの業務内容に係る情報

エ　外部記録媒体に記録された上記ウのバックアップファイル

（２）情報システム利用課長等

ア　住宅管理システムで利用するパソコン、プリンタ及びこれに附属する機器

イ　上記アに係る住宅管理システム及びこれらのパソコン等に記録された情報

ウ　外部記録媒体に記録された上記イのバックアップファイル

エ　上記アのパソコンで直接、外部記録媒体に作成したファイル

（３）情報システム利用者

ア　利用するパソコンやプリンタ等の端末機器

イ　利用するパソコンの記録媒体に記録される情報

ウ　利用する外部記録媒体及び外部記録媒体に記録される情報

２　情報資産の管理に当たっての留意事項

（１）情報資産保護のためのアクセス権限の設定

情報システム管理者は、情報システム利用者に対し、その利用目的に沿ったアクセス権限を設定しなければならない。

（２）情報資産の保護のための臨時的措置

情報システム管理者は、次のような事態が生じた場合、又は生じるおそれがある場合、住宅管理システムの全部又は一部の切断措置等を行うことができる。

ア　地震、落雷、火災等の災害及び事故、故障等によるネットワークシステムの障害

イ　部外者等による不正アクセス又は不正操作による情報資産の持出し、改ざん、消去などの不測の事態

ウ　情報システム利用者及び委託業者による意図しない操作、未許可の端末接続による情報流出等の不測の事態

エ　その他情報システム管理者が切断措置等が必要と認める事態

（３）ガイドラインの遵守

情報システム利用課長等は、管理責任を有する情報資産について、適切な管理が図られるよう情報システム利用者を指導する。

情報システム利用者は、次の事項について、ガイドラインで定める情報資産の管理方法を遵守しなければならない。

・情報資産の処分

・パソコンの持ち出し

・外部記録媒体の持ち出し、持ち込み

・情報資産に記録された情報の複写

・利用者以外の者のパソコン等の接続
・利用者の個人所有のパソコン等の接続

3　外部委託を行う場合の情報資産の管理

情報システム管理者は、外部に委託して住宅管理システムの開発（改修）、保守及び運用を行う場合、契約のなかでガイドライン及び本手順の遵守について規定するなど、自らの情報資産のセキュリティ対策について適切な措置をとらなければならない。

Ⅳ　機器等の安全確保

1　管理が必要な区域及び機器

情報システム管理者は、住宅管理システムの運用に当たって、特にＬＡＮ関連機器及びサーバ等が集中的に配備されている区域を管理区域とし、必要な安全対策を講じるほか、個別の機器等についても、それぞれ必要な安全対策を講じるものとする。

また、外部委託によって、ＬＡＮ関連機器及びサーバ等のシステムを設置して、業務処理を行う場合にあっては、確実な安全対策を講じることができる委託業者を選定するものとする。

なお、管理区域及び個別に設置する機器の配置場所については、セキュリティ上、非公開とする。

2　管理区域において講ずべき安全対策

情報システム管理者は、管理区域の安全対策として、次の措置を講ずるものとする。

（1）自然災害、火災等に備えるため、必要な措置を講じる。

ア　管理区域には、火災等に備えるため、火災検知装置及び消火装置を配備する。

イ　機器及びサーバ等を固定するなどの転倒防止策を施す。

（2）管理区域における入退室の管理について、必要な措置を講じる。

ア　管理区域の管理責任者（以下「管理責任者」という。）は情報システム管理者とし、外部委託によって、ＬＡＮ関連機器及びサーバ等のシステムを設置し、業務処理を行う場合は、当該委託契約書で定める業務処理責任者とする。

イ　管理責任者は、次のいずれかに該当し、事前に登録された者の入室を許可することができる。

（ア）住宅管理システムの開発及び機器や情報の管理を行う情報システム担当者

（イ）住宅管理システムの開発及び機器や情報の管理を行う委託業者

（ウ）住宅管理システム機器の保守点検作業に従事する委託業者

（エ）管理区域の電気設備及び空調設備等の保守点検作業に従事する委託業者

（オ）その他管理責任者が必要と認める者

ウ　鍵及び入室カードの管理は管理責任者が行う。

エ　管理責任者は、入退室の許可を得た者に限り、鍵または入室カードを貸与する。

オ　管理区域に入退室する者は、管理責任者の指示に従うとともに、次に掲げる事項を遵守しなければならない。

（ア）業務処理に必要ない機器や外部記録媒体は持ち込まないこと。
（イ）許可なく撮影機材を室内に持ち込み、又は撮影をしないこと。
（ウ）室内において喫煙又は飲食をしないこと。

カ　管理責任者は、委託業者が管理区域に入室する場合、情報システム担当者を立ち会わせなければならない。ただし、外部委託によって、ＬＡＮ関連機器及びサーバ等のシステムを設置して業務処理を行う場合は、この限りでない。

3　管理区域以外において講ずべき安全対策

情報システム管理者は、住宅管理システムの運用に当たって、配備されているサーバ等の機器等について、次のとおり安全対策を講じる。

（1）サーバ等は、機器及び設置場所等の態様に応じて、ラック等に入れて保管・施錠、若しくはＩＣカードやパスワード等によるアクセス制限を行うなどの措置を講じる。

（2）機器及びサーバ等は、固定するなどの転倒防止策を施す。

（3）委託業者が、住宅管理システムの開発及び運用管理、又は機器等の保守点検を行う際には、情報システム管理者が必要な指示を行えるように、情報システム担当者を立会いさせるものとする。

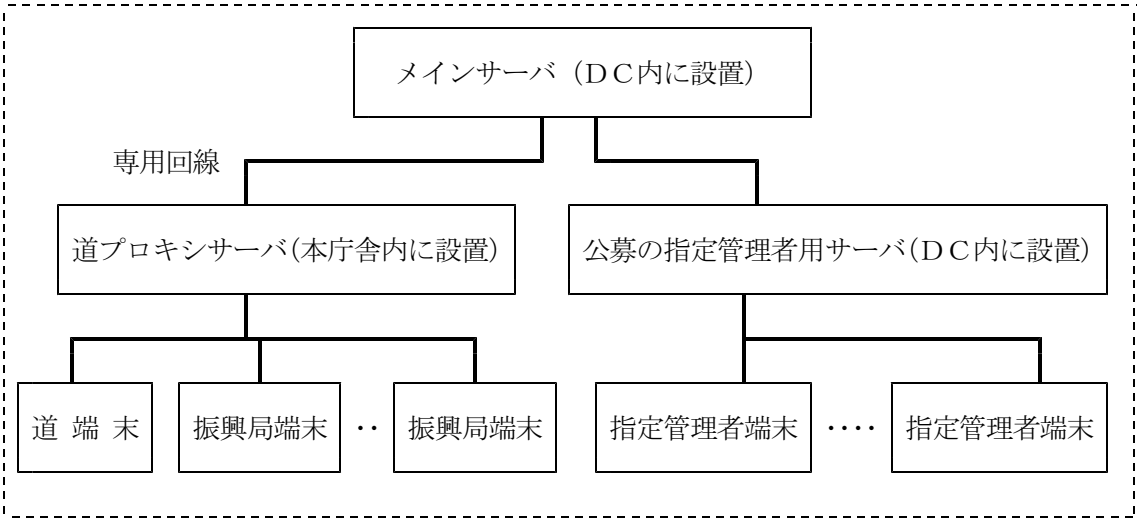
4　回線の安全対策

情報システム管理者は、室内、廊下等、触れることが可能な場所にある構内回線については、誰もが容易に触れないようプロテクタなどで配線を保護する。

Ⅴ　住宅管理システムの運用

1　住宅管理システムの概要

集合住宅などの建築物及び駐車場の整備状況並びにその利用者（入居者・駐車場利用者）の家賃及び駐車場使用料の収納管理など道営住宅の管理運営に必要な情報を電子計算処理組織をもって記録保存及び活用するため、外部データセンターのサーバに独自アプリケーションを登載し、専用回線で接続したパソコン端末でのオンライン処理を行っている。



2　住宅管理システムの運用

（１）運用の日程及び時間

住宅管理システムは、次のとおり運用を行うことを基本とする。

・日　程　　１月１日から１２月３１日まで（３６５日運用）

・時　間　　０時から２４時まで（２４時間運用）

※）ただし、毎週日曜日の６時から７時までの間は、サーバ再起動処理のため、運用ができない。

（２）運用の制限

住宅管理システムの適切な運用を確保し、年間処理計画に沿って、例月及び年次の処理を確実に実行するため、システム管理者は、あらかじめ利用者に運用制限の日程及び対象端末等を周知した上で、運用制限を行うものとする。

ア　全端末の運用制限

次の場合においては、全ての端末の運用を制限し、住宅管理システムへのログインができないものとする。

・　修正プログラム適用などによりやむを得ずメインサーバを停止する場合

・　口座振替情報による収納消込など（例月処理）を実行する場合

・　収入一括認定など（年次処理）を実行する場合

・　その他システム管理者が必要と認める場合

イ　関係する端末の運用制限

次の場合においては、関係する端末の運用を制限し、住宅管理システムへのログインができないものとする。

①道端末及び振興局端末の運用制限

・計画停電などでやむを得ず道プロキシサーバを停止する場合

・その他システム管理者が必要と認める場合

②指定管理者端末の運用制限

・システム管理者が必要と認める場合

（３）利用の制限

次の場合においては、全ての端末の利用を制限し、住宅管理システムの一部機能の実行処理ができないものとする。

ア　収納消込処理による利用制限

・収納消込処理主体　収納事務を受託する公募の指定管理者

・利用制限時間　　平日１３時から１３時３０分まで

イ　その他利用制限

情報システム利用課長等から申し出があり、システム管理者が特に必要と認める場合、あらかじめ利用者に利用制限の日程及び対象端末等を周知し、上記アに準じた利用制限を行うものとする。

3　住宅管理システムへの接続

（１）利用者情報の管理

情報システム管理者は、情報システム利用課長等からの申請に基づき、情報システム利用者のログインＩＤ等の利用者情報の登録、変更及び抹消を行う。

なお、利用者情報の登録内容については、情報システム管理者が別に定める。

（２）パスワードの管理

情報システム利用者は、システムに接続する場合、ログイン時に必要となるパスワードを次により厳重に管理しなければならない。

ア　パスワードのメモを作成しないなど、他人に漏れないようにすること。

イ　パスワードの共有は行わないこと。

ウ　パスワードの照会等には一切応じないこと。

（３）他の情報システムとの接続

情報システム管理者は、他の情報システムと接続する場合にあってはその方法を確認・検証し、管理運用する情報資産に、影響が生じないことを確認するものとする。

情報システム管理者は、他の情報システムがウイルスに感染するなどのセキュリティ上の問題が発生したことにより、管理運用する情報資産に被害が生じた、又は生じる恐れがある場合は、速やかに他の情報システムとの接続を物理的に遮断し、被害や影響の有無を確認するものとする。

4　住宅管理システムに接続したパソコンの利用

住宅管理システムに接続したパソコンを利用する情報システム利用者は、次の事項を遵守しなければならないものとする。

（１）情報システム利用者は、各種システム、文書処理や表計算等のソフトウェアなどを業務以外の目的で利用しないこと。

（２）情報システム利用者は、業務に必要のないソフトウェアをパソコンにインストールしないこと。承認等を得ていないネットワークに接続しないこと。

（３）情報システム利用者が業務処理中に離席する場合は、使用中のパソコンをロックし、又は住宅管理システムからログオフするなどして、不正な使用を防止すること。

○　スクリーンセーバーのパスワード機能活用によるロック

○　オペレーティングシステムのロック機能の活用によるロック

○　住宅管理システムからのログオフ

（４）情報システム利用者は、システム管理者の承認等を得た場合を除いて、システムに接続しているパソコンに対し、ＬＡＮカードやモデム等の通信機能を有する機器の増設や接続を新たに行い、他のネットワークやインターネットに接続してはならない。

5　住宅管理システムの保守

住宅管理システムの円滑な運用及び安定した稼働を確保するため、システム管理者は、本システムのプログラム開発及び電子計算処理組織の運用等に関する高度の専門的知識を有し、障害発生時等に速やかな復旧措置を講ずる体制の整備ができる者に保守業務を委託する。

（１）委託業務の設定

障害発生時の復旧措置対応全般は言うまでもなく、システム管理者は、住宅管理システムの円滑な運用及び安定した稼働を確保するため、連関したつながりを保持して実行すべき保守、点検及び監視並びにそれらの記録及び報告等に関する作業全般を委託業務として設定する。

（２）受託者の責務

委託業務の遂行に当たり、受託者は次の責務を有するものとする。

ア　定期的保守

住宅管理システムが日常業務に支障が生じないように円滑かつ安定的に機能するように点検、調整、監視すること。

イ　障害発生時の対応

住宅管理システムに障害が発生した場合、速やかに正常状態に復旧させ、再発の恐れがある場合は再発防止措置を講ずること。

ウ　セキュリティ対策

「Ⅳ　機器等の安全確保」による管理区域において講ずべき安全対策を確実に実施するとともに、別に定める「住宅管理システム運用上のセキュリティ対策」をシステム管理者が適切に実施するために必要となる点検、調整及び監視並びに技術的

助言、提案及び情報提供を行うこと。

Ⅵ　住宅管理システム運用上のセキュリティ対策

1　コンピュータウィルス対策

（1）情報システム管理者が行う対策

ア　情報収集と情報システム利用者への情報提供

情報システム管理者は、情報セキュリティ総括管理者、関係機関等から提供される情報及びインターネットから収集した情報に基づき、ウイルスに関して注意を喚起する必要がある場合、情報システム利用課長等及び情報システム利用者へ周知しなければならない。

イ　ウイルス対策ソフトの活用

情報システム管理者は、ウイルス対策ソフトにより、次の対策を講じなければならない。

（ア）サーバにインストールしたウイルス対策ソフトのパターンファイル（ウイルス定義ファイル）を常に最新のものにすること。

（イ）情報システム利用者に対し、パソコンにインストールするウイルス対策ソフトを指定し、また、最新のパターンファイルの情報を提供すること。

（ウ）ウイルス対策ソフトのインストール状況を定期的に把握し、インストールされていないパソコンやサーバは情報システムから切り離し、その旨を情報システム利用課長等に通知すること。

ウ　ウイルスに感染の恐れがある場合の対処

（ア）情報システム管理者は、ウイルス感染の恐れがある場合には、次により情報システム利用課長等及び情報システム利用者に指示しなければならない。

○ＬＡＮケーブルを抜き、外部と接触できないようにすること。

○ウイルス対策ソフトでウイルスチェックを行い、万一ウイルスが発見された場合、駆除を行うこと。

○再度ウイルスチェックを行い、ウイルスが完全に駆除されていることを確認した上で、ＬＡＮケーブルを接続すること。

（イ）情報システム管理者は、感染したウイルス名、感染経路等の情報について調査する。

（2）情報システム利用者が行う対策

ア　ウイルス対策ソフトの使用

情報システム利用者は、次によりウイルス対策ソフトを使用しなければならない。

（ア）住宅管理システムにパソコンを接続する場合は、情報システム管理者から指定されたウイルス対策ソフトを必ずインストールすること。

（イ）定期的に、全ローカルドライブのウイルスチェックを行うこと。

（ウ）ウイルス対策ソフトが動作していない場合、速やかに情報システム管理者へ連絡すること。

イ　ウイルス対策ソフトのパターンファイル等の確認

情報システム利用者は、次によりウイルス対策ソフトのパターンファイルの更新状況などを確認し、ウイルス対策が適切に行われるようにしなければならない。

（ア）情報システム管理者から提供された情報に基づき、ウイルス対策ソフトのパターンファイルが最新であることを確認すること。

（イ）パターンファイルが最新でない場合、情報システム管理者へ連絡すること。

（ウ）情報システム管理者が提供するウイルス対策情報を必ず閲覧し、適切にウイルス対策を行うこと。

ウ　ウイルス感染の防止

情報システム利用者は、次によりウイルス感染を未然に防止しなければならない。

（ア）外部記録媒体による外部とのデータ授受は行わないこと。

（イ）ソフトウェア等をインストールする場合は、当該ソフトウェア等の利用規約等に従って処理するとともに、ネットワーク経由でのファイルのダウンロード等の手段により、外部との間でデータを授受する場合は、ウイルスチェックを行うこと。

（ウ）他の業務で使用していたパソコンを、住宅管理システムに接続する場合は、接続前に必ずウイルスチェックを行い、ウイルスに感染していないことを確認の上接続すること。

（エ）ソフトウェアのぜい弱性によりパソコンがウイルスに感染し、情報が流出することを防止するため、情報システム管理者の指示に基づきソフトウェアの修正プログラムのインストールを行うこと。

エ　ウイルスに感染した恐れがある場合の対処

情報システム利用者は、ウイルスに感染した恐れがある場合は、次の手順により適切に対処しなければならない。

（ア）ウイルスに感染した恐れがある場合は、ＬＡＮケーブルを抜くなどにより、ネットワークと切断すること。

（イ）速やかに情報システム管理者へ連絡し指示を受けること。

（ウ）連絡手段は電話等を用い、電子メールを使用しないこと。

（エ）ウイルスに感染した場合は、情報システム管理者からの指示に従い、ウイルスの駆除を行うこと。

《ウイルス感染時の症状》

○システム立ち上げに異常に時間がかかる。

○パソコンの動きが遅い。

○再起動を繰り返す。

○情報システム利用者の意図しないディスクアクセスがおこる。

2　不正アクセス対策

（１）外部との接続制限

情報システム管理者は、住宅管理システムにおいて、インターネットや他のネットワークと接続する場合、使用しないポート（情報の受送信口）については、ファイアーウォール、中継機器等の設定によって確実に閉鎖するものとする。

（２）住宅管理システムの停止

情報システム管理者は、情報政策課長からのセキュリティ情報により不正アクセス

を受ける恐れがあると認められる場合は、住宅管理システムの設定変更や停止等の措置をとらなけらばならない。

（３）情報政策課との連携

情報システム管理者は、不正アクセス行為を受けた場合、情報政策課長と連携を図り、適切な対策を講じなければならない。

（４）セキュリティに関する情報収集

情報システム管理者は、住宅管理システムの脆弱性や攻撃ツール等のセキュリテイに関する情報を収集し、住宅管理システムに影響を及ぼす恐れがある場合は、セキュリティパッチ（修正プログラム）の適用等について、情報システム利用者に周知しなければならない。

３　住宅管理システムの監視

情報システム管理者は、住宅管理システムを安全に稼動させるため、次よりネットワークや住宅管理システムの常時監視を行い、異常が確認され、住宅管理システムに影響を及ぼす恐れがある場合は、ネットワークの切断や住宅管理システムの停止などの措置を講じるとともに、原因を究明し、再発の恐れがある場合は再発防止策を講じるものとする。

（１）情報システムの常時監視

ア　トラフィック監視

情報システム管理者は、設置されているネットワーク機器のトラフィック情報を定期的に監視する。

イ　ファイアウォール監視

情報システム管理者は、外部（インターネット）及びパソコンからの不正なアクセスについて監視する。

ウ　ウイルス監視

情報システム管理者は、ウイルス対策ソフトにより、ウイルスの検知及び感染の情報を取得する。

エ　ネットワークの侵入監視

情報システム管理者は、ネットワーク侵入監視装置の動作を監視し、必要があれば、住宅管理システムの脆弱性について調査する。

Ⅶ　住宅管理システムの安全対策

１　住宅管理システムの調達

（１）調達仕様書の作成

情報システム管理者は、住宅管理システムの調達を委託する場合、次の事項に留意して調達仕様書の作成を行わなければならない。

ア　住宅管理システムに必要な機器等について、ＩＰアドレス等の設定情報を記載し

ないこと。

イ　機器の設置場所、設置環境などの外的要件やセキュリティ要件などを勘案し、必要となる機器、部材等を調達する旨、記載すること。

ウ　重要なサーバ等については、可能な限り二重化する旨、記載すること。

エ　住宅管理システムで調達するソフトウェアについては、最新のバージョンとすることとし､最新のサービスパック及び修正プログラムを適用するよう記載すること。

オ　住宅管理システムで調達するハードウェア、ソフトウェアに関する設定内容ついては、別に指示する旨、記載すること。

カ　住宅管理システムで調達するハードウェア、ソフトウェアに関するセキュリティ上の問題については､瑕疵担保適用期間中は､委託業者の責任において対処する旨、記載すること。

（2）委託する場合の留意事項

情報システム管理者は、システムの開発、運用保守等を外部に委託する場合、次の事項に留意して契約を締結するものとする。

ア　ガイドライン及び本手順の遵守、また、遵守されなかった場合の損害賠償規定を明記すること。

イ　外部へ搬送した外部記録媒体の盗難防止や不正な複製等の防止について明記すること。

ウ　委託業務の終了時には、委託業務期間中に使用した情報や記録媒体の消去、廃棄等を行うことを明記すること。

エ　委託業者が再委託をする場合、上記の事項に準ずる条項を含む契約を締結することを明記すること。

2　使用ソフトウエアの安全性の確保

情報システム管理者は、住宅管理システムを安全な状態で運用するため、使用しているオペレーティングシステム等のソフトウェアを常に最新の状態にするとともに、セキュリティ対策上、必要なプログラムの修正を行うよう、情報システム利用課長及び情報システム利用者に周知するものとし、情報システム利用者は、速やかにソフトウェアの更新及びプログラムの修正を行うものとする。

また、ソフトウェアや修正プログラムの適用に関する具体的要件については、情報システム管理者が別に定める。

（1）情報システム管理者は、新しいオペレーティングシステムやサービスパックなどの修正プログラムが提供された場合、住宅管理システムへの導入の可否を検討の上、適用を行う。

（2）情報システム管理者は、住宅管理システムに接続されているパソコンのオペレーティングシステムやソフトウェア等のサポートが終了し、セキュリティ対策上、問題を生じる恐れがある場合は、住宅管理システムとの接続ができなくなる旨、十分な猶予期間を設けた上で、事前に情報システム利用管理者に周知し、情報システム利用管理者は、パソコンやオペレーティングシステムの更新を円滑に行う。

（3）情報システム管理者は、住宅管理システムに接続するパソコンについて、情報システム管理者が別に定める要件を満たしていない場合は、当該パソコンの接続を停止する。

3　障害及び事故への対処

道営住宅管理システムの障害、不正アクセス、ウイルス感染、情報流出等（以下、「システム障害」という。）の事案が生じ、または生じる恐れがある場合、情報システム管理者、情報システム利用管理者及び情報システム利用者は、システム障害を未然に防止し、システム障害が起きた場合の被害を最小限にとどめるなど、次の手順により対処する。

（1）情報システム利用者の対処

ア　情報システム利用者は、システム障害の事案が生じ、または生じる恐れがあると認められる場合は、情報システム管理者に速やかに連絡しなければならない。

イ　情報システム利用者は、ネットワーク上の他のパソコンや情報システムに影響を及ぼす恐れがある場合は、情報システム管理者の指示により、適切に対処する。

（対処方法の例）

○ＬＡＮケーブルを抜くなどにより、ネットワークと切断すること。

○パソコンやネットワーク機器の電源を切断すること。

（2）情報システム利用課長等の対処

ア　システム障害事案の発生により、他の情報システムに影響を及ぼす恐れがあるときは、情報システム利用課長等は、情報システム管理者の指示により、速やかに調査を行い、報告しなければならない。

イ　情報システム利用課長等は、調査の結果、他情報システムに影響を及ぼす恐れがある場合は、関係者に連絡するなど適切に対処する。

ウ　情報システム利用課長等は、再発の恐れがある場合は防止策を講じ、情報システム管理者に報告する。

（3）情報システム管理者の対処

ア　情報システム管理者は、情報システム利用者やヘルプデスクから事案の報告を受けた場合は、情報システム利用者に対し必要な措置を講じるよう指示する。

イ　情報システム管理者は、事案が全庁的あるいは他機関等に影響を及ぼす恐れがある場合は、ネットワークの切断や情報システムの停止などの措置を講じる。

ウ　情報システム管理者は、システム障害の事案の原因を究明し、復旧にあたる。

原因の究明に当たっては次の事項について調査・分析する。

・各種イベント
・システム負荷状況・ログ
・ネットワーク負荷状況・ログ
・ファイルの改ざん
・存在すべきファイルの抹消や不明なファイルの存在
・ファイル利用量の急激な増減
・本来稼動しているはずのサービスの停止
・不明なプロセス
・本来利用できないはずのシステム利用者のシステムアクセス

エ　情報システム管理者は、再発の恐れがある場合は、再発防止策を講じること。

4　住宅管理システムの安全確保に関する記録管理

情報システム管理者は、システム障害の原因調査等に資するため、システム変更記録等のほか、次の記録管理を行う。

（1）システム監視情報

情報システム管理者は、次の監視によって得られる情報を定期的に保存する。

ア　トラフィック監視

イ　ファイアウォール監視

ウ　ウイルス監視

（2）不正アクセス情報

情報システム管理者は、ネットワーク侵入監視装置により得られる次の情報を、定期的に保存する。

ア　イベント詳細メッセージ

イ　アクセス元ＩＰアドレス

ウ　影響を受けるシステム名（ＯＳ・ソフトウェア・プロトコル）

（3）障害情報

情報システム管理者は、システムの障害に対する処理、問題点等を障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

ア　故障処理及び故障履歴に関する記録

イ　障害履歴に関する記録

Ⅷ　本手順の取扱い

この手順は、情報セキュリティ対策を効果的に実施するため、原則として非公開の取扱いとする。

道営住宅管理システム情報セキュリティ対策実施手順の概要

□策定趣旨

道営住宅管理システムのセキュリティ対策の具体的な手順を文書で定め、同システムの情報セキュリティを一定の水準で確保する。

根　拠　　道情報セキュリティ対策基本方針第７、道情報セキュリティ対策基準　第２６
※）いずれも道総合政策部が所管

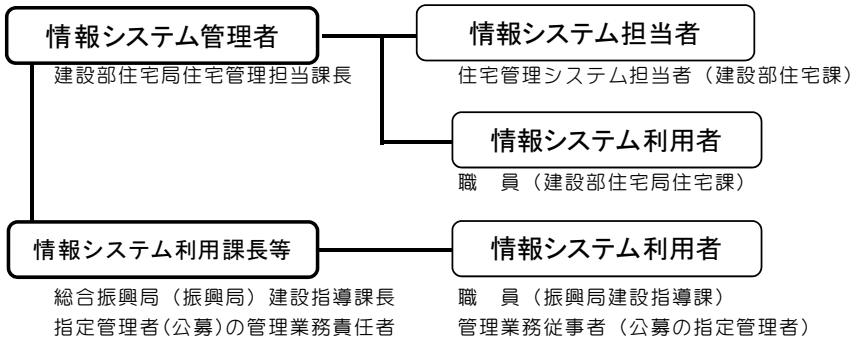
□情報セキュリティ対策とは

情報資産の機密を守り、誤った使用や持ち出し、持ち込み、改ざんを防ぎ、許可された者が、必要なときに安全確実に利用できるように必要な措置を講ずること。

□手順の適用範囲

１　対 象 者　住宅管理システムを開発、保守、運用及び利用者（道職員・指定管理者）
２　対象情報　住宅管理システムのハード・ソフト、記録データ（外部の電磁的記録を含む）

□情報セキュリティ対策の実施体制



□情報セキュリティ対策の役割分担

	システム管理者	利用課長等	利　用　者
情報資産の管理	・ネットワーク機器 ・サーバ（ＣＰＵ） ・開発運用情報 ・外部委託時の措置	・所属のパソコン、プリンタ ・所属の記録情報	・利用する端末機器 ・利用する記録情報
セキュリティ対策	・利用者等への情報提供 ・ウィルス対策ソフト活用 ・ウィルス感染等の対処 ・不正アクセス対策	○「ガイドライン」の遵守 ・情報資産の処分 ・パソコンの持出し ・記録情報の複写	・ウィルス対策ソフト利用 ・パターンファイル等確認 ・ウィルス感染の防止 ・ウィルス感染等の対処

□道営住宅管理システムの運用

○運用日程　365日･24時間運用（ただしサーバ再起動時を除く）
○運用制限　サーバ停止時、口振収納消込時のほか管理者が必要とするとき
○利用制限　平日13時から13時30分まで
（収納事務実施の指定管理者の収納消込処理を優先）
○運用保守　障害発生時の速やかな復旧可能な者に委託
～ 受託者が点検、調整、監視、技術的助言、提案･情報提供

□障害・事故への対処

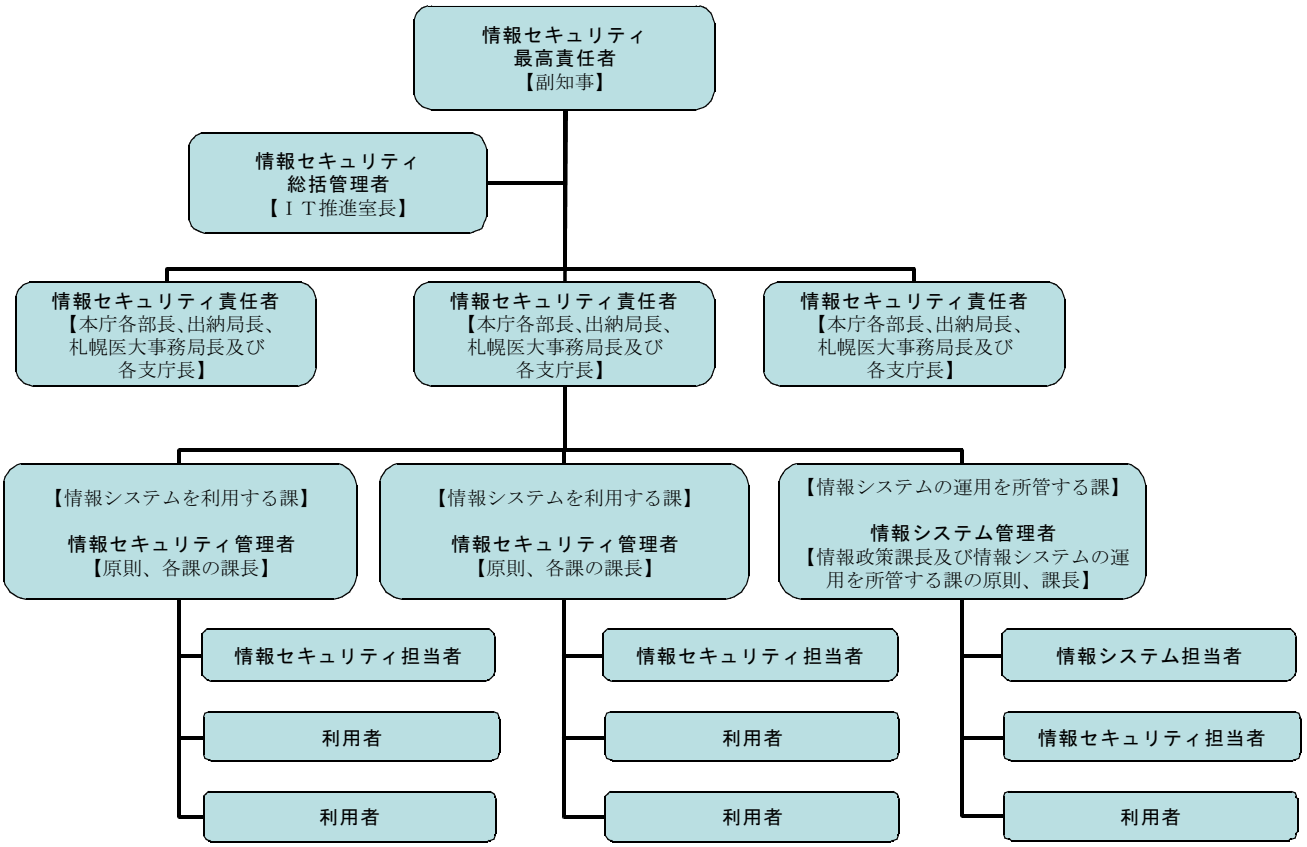
それぞれの的確な対処によって、システム障害を未然に防止し、障害発生時の被害を最小限にとどめる。

システム管理者	利用課長等	利　用　者
・利用者に対する指示 ・システム停止等の実行 ・原因究明と復旧措置 ・再発防止策の実行	・調査と管理者への報告 ・関係者への連絡 ・再発防止策の実行と管理者への報告	・管理者への連絡 ・ネットワークとの切断 ・電源の切断

※情報セキュリティ対策を効果的に実施するため、本手順は、原則非公開の取扱いとする。

情報セキュリティ対策ガイドラインの概要

□情報資産の管理体制図



※管理体制図の説明

区　分	定　義	役　割
情報セキュリティ最高責任者	情報化を担当する副知事	道の全庁的かつ総合的な情報セキュリティ対策を行う。
情報セキュリティ責任者	本庁の部長、出納局長、札幌医科大学事務局長及び各支庁長	所管における情報セキュリティ対策を行う。
情報セキュリティ総括管理者	企画振興部ＩＴ推進室長	道の情報セキュリティ対策の総括的な管理を行う。
情報セキュリティ管理者	【本庁】 課長（課に相当する組織の長を含む。以下同じ。） 【出先機関】 課（課に相当する組織を含む。以下同じ。）を置くものにあっては当該出先機関の課長、課を置かないものにあっては当該出先機関の長	所管する課において、次の事項を行う。 ・情報セキュリティ対策を実施すること。 ・利用者に対し情報セキュリティに関する研修を実施すること。 ・利用者に対し、本ガイドライン及び情報システム管理者の指示を遵守させること。
情報セキュリティ担当者	情報セキュリティ管理者の指名する者	情報セキュリティ管理者の指示を受け、課内全体の情報セキュリティ対策を行う。
情報システム管理者	情報システムの運用を所管する課の情報セキュリティ管理者	所管する情報システム及び取り扱うすべて情報に関して、次の事項を行う。 ・情報セキュリティ対策を実施すること。 ・利用者に対して情報セキュリティ対策に関する遵守事項を指示すること。
	情報政策課長は、上記のほか全庁的なセキュリティ対策を行う。	
情報システム担当者	情報システムの運用を所管する課において情報システムの運用管理を担当する者	情報システム管理者の指示を受け、所管する情報システム及び取り扱うすべての情報に関して、情報セキュリティ対策を行う。
利用者	道が管理運用している情報資産を利用する者	本ガイドラインを遵守し、情報セキュリティ管理者及び情報システム管理者の指示に従い、情報セキュリティ対策を行う。

（出所：情報セキュリティ対策ガイドライン）