諮問第　４７　号

平成２５年９月１３日

川西市個人情報保護審議会

会　長　井　上　典　之　様

川西市長　大　塩　民　生

電子計算機の結合による個人情報の提供に関する意見について（諮問）

川西市個人情報保護条例第１３条第２項の規定に基づき審議会の意見を聴くことについて、別紙のとおり諮問します。

《諮問内容》

電子計算機の結合による個人情報の提供について

次期農業共済ネットワーク化情報システム導入に伴う個人情報の提供

日　時　：　平成２５年９月２０日(金)
　　午後６時００分～
場　所　：　川西市役所４階 庁議室

川西市個人情報保護審議会（第５３回）

１　会長あいさつ

２　審議事項

諮問第４７号

電子計算機の結合による個人情報の提供に関する意見について

次期農業共済ネットワーク化情報システム導入に伴う個人情報の提供

３　その他

［別紙］

電子計算機の結合による個人情報の提供について

番号	事務の内容	電子計算機の結合による提供の必要性	提供する個人情報の内容	提供先の保護措置	提供先	所管課
11	次期農業共済ネットワーク化情報システム	農業共済ネットワーク化情報システムは、国が定める「農業災害補償制度に関する事務機械化を推進するための指針」（平成７年２月）に基づき、共済・保険・再保険を運営する各々が内部処理方式により情報処理することを基本とする一方、各々が処理した結果が三段階（農業共済組合・市町村・政府）で連動するものとして、国が全国標準システムを開発・保守管理しており、本市でも３つの事業等システムを運用している。 しかし、近年、制度改正への柔軟な対応、コンプライアンス体制の強化等が求められている。 このような中、現在導入されているＯＳ（Windows ＸＰ）のサポートが平成２６年４月で終了すること、コンプライアンスやセキュリティ上現行体制では問題があることなどから、国が検討を重ね「次期システムの開発等に関する基本設計書」において、平成２５年度末までに現行のシステムからサーバー・ベースド・コンピューティングによる集中運用形態へ移行することを決定した。 当該決定を受け、本市においても、当該運用に参加する必要性が生じている一方で、今後発生を危惧されている大災害時におけるデータ消失等のリスクを回避する等のために、従来、産業振興課内におけるパソコン上での管理に委ねられていた個人情報を、セキュリティの保障されたインターネットデータセンターのサーバー上で管理することで、諸問題を解決するとともに、業務効率の向上に資するものである。	①　水稲共済 ・氏名・性別 ・住所 ・電話番号 ・世帯主氏名 ・農地情報 ②　建物共済 ・氏名・性別 ・住所 ・電話番号 ・世帯主氏名 ・家族人数 ・共済種類 ・建物用途（住宅・寺等） ・建物種類（木造・コンクリート造） ・建物面積 ・建物配置図 ・本人の銀行口座番号 ③　農機具共済 ・氏名・性別 ・住所 ・電話番号 ・世帯主氏名 ・本人の銀行口座番号	提供する情報については、次のセキュリティ措置を講じるものとする。 (1)　市相互間におけるアクセスはできない。 (2)　個人情報へのアクセスは、情報を登録した産業振興課員のみに許可され、原則として外部アクセスはできない。 (3)　データの消失を防止するため、バックアップ用サーバを設置し、定期的に自動バックアップ処理が行われるよう処理する。 (4)　不正アクセスによる情報流出を防止するために、常時不正アクセスを監視するなどの措置を講じる。 (5)　システムへの接続、ログイン動作及び情報セキュリティ確保に関する情報は全て記録の上、一定期間保存する。 (6)　個人情報が格納される機器は高度なセキュリティ機能を有する専門施設内（地上２階以上の場所又は無窓の外壁）にて施錠管理され、不許可者が施設に立ち入ることはできない。 (7)　情報セキュリティに関する人員を配置（情報ネットワーク管理者等）し、セキュリティに関する統括及び管理を行う。 (8)　本件管理業務を他の情報管理専門事業者に委託する場合は、情報セキュリティポリシーを厳格に遵守させることを徹底する。	兵庫県農業共済組合連合会	市民生活部生活活性室産業振興課

平成２５年９月２０日　川西市個人情報保護審議会　資料１

川西市農業共済システムの問題と次期農業共済システムの特徴について

現行システム	次期農業共済ネットワークシステム
・市がサーバーを保守・管理 ・使用 OS：WindowsXP ・データ提出方法：MO、FD ・ネット接続なし	・委託業者がサーバーを保守・管理 ・使用 OS：Windows７ ・データ提出方法：随時 ・光ケーブルを通じ、サーバーのみ接続

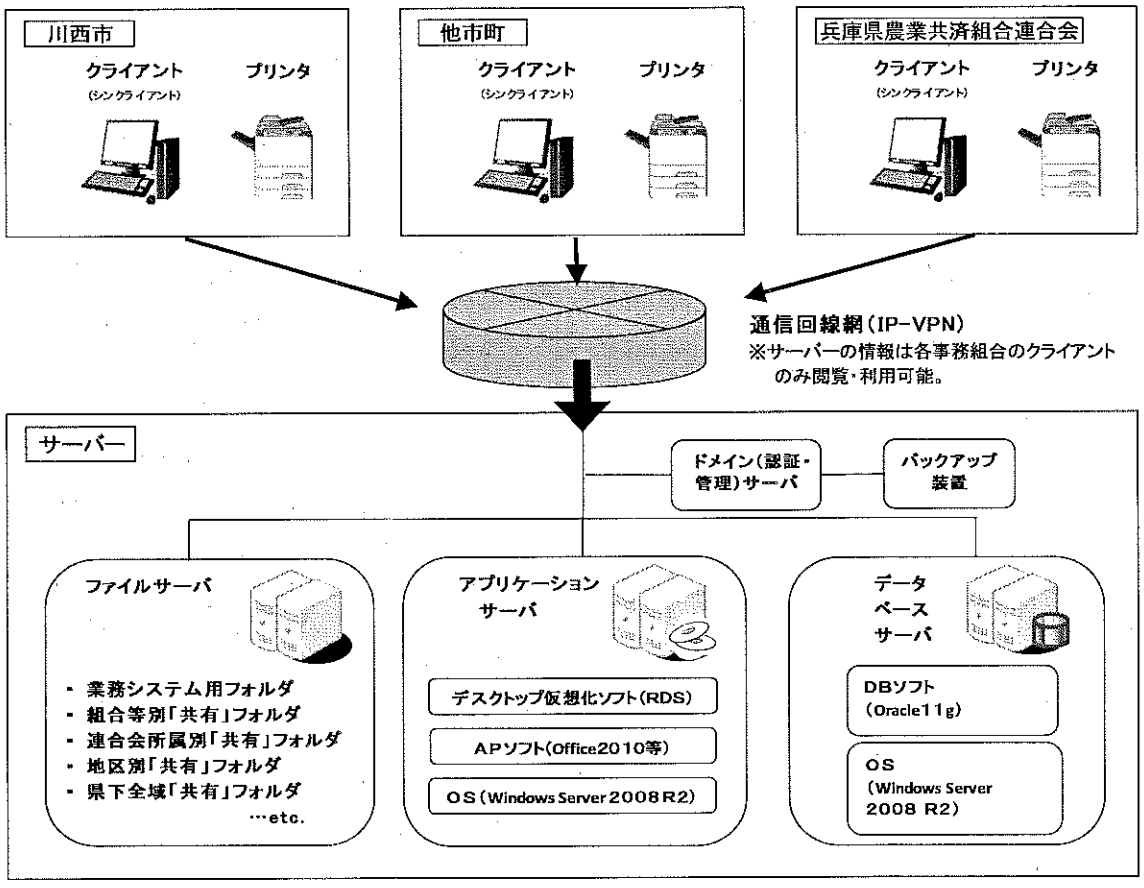
【現行システムの問題点】

①市でサーバーを保管しているため、天災や事変等が起こった際に、情報を失う危険性がある。 → ①兵庫県内の安全な場所にサーバーは保管されているため、市で天災や事変等が起きても情報は保護される。

②現在利用している OS、WindowsXP は、平成２６年４月に Microsoft 社のサポートが終了することから、ウイルス対策が不十分になる。 → ②使用する OS が Windows７になることから、Microsoft 社のサポートを受けることが可能なため、適切なウイルス対策を行うことができる。

③データを報告する際、MO や FD の記録媒体により報告を行っていたが、郵送等の輸送トラブルで紛失する危険性がある。 → ③クライアントでの作業情報がサーバーに保存・管理されるため、これまでのような MO や FD による記録媒体による報告の必要がなくなる。

集中化運用システムのイメージ



集中化運用システムのイメージ

次期農業共済ネットワーク化情報システム

(1) 農林水産省等の定めた基本要件に準拠したＳＢＣ方式による構築

農林水産省及びＮＯＳＡＩ全国が「次期農業共済ネットワーク化情報システムの開発等に関する基本設計書」で定めた要件に準拠したＳＢＣ方式による集中化運用システムを平成２５年度末までに構築し、平成２６年４月に完全移行する。

(2) ＳＢＣ方式を基本としたサーバ統合及びシステム移行

集中化運用システムの構築においては、ＮＯＳＡＩ全国から提供される次期ネットワークシステムの全国標準システムにあわせて、本会が指定するローカルオプションシステム等（以下、総括して「業務システム」という。）もＳＢＣ方式へ移行する。
また、組合等及び本会が有するＥＵＣシステム等もＳＢＣ方式で円滑に運用できるよう、集中化運用システムを構築する必要がある。

(3) ＩＤＣの利用

集中化運用システムにおけるサーバ設置場所は、堅牢なファシリティ及び強固なセキュリティ設備を備える必要があるため、兵庫県内又は兵庫県に隣接する府県内に所在し、本会のサービスを提供する場所としてふさわしいＩＤＣ(※1)のハウジングサービス(※2)を利用する。

※1：ＩＤＣ（Internet Data Center）
顧客のサーバを預かり、インターネットの接続回線や保守・運用サービスなどを提供する施設。耐震性に優れたビルに高速な通信回線を引き込み、自家発電設備や高度な空調設備を備え、ＩＤカードによる入退室管理やカメラによる２４時間監視などでセキュリティを確保する専用施設。

※2：ハウジングサービス
データセンターの利用形態の一つ。顧客がサーバなどの機材を用意してサービス事業者に預け、サービス事業者は機器設置場所と電力等を提供する形式。顧客が独自の機材を持ち込むので、機材の選定や組み合わせの自由度が高い。対して、サービス事業者が機材等も用意し、丸ごと貸し出す方式をホスティングサービスという。

(4) ネットワーク

集中化運用システムに使用する通信回線は、㈱ケイ・オプティコムの「Business 光」回線（常時接続・ベストエフォート 100Mbps 又は 200Mbps）を使用し、インターネットを介さないＩＰ－ＶＰＮ(※3)方式により、県下全組合等、本会及びＩＤＣを１グループとした総合的なリスク管理ができる完全閉鎖環境とする。

※3：ＶＰＮ（Virtual Private Network）
公衆回線をあたかも専用回線であるかのように利用できるサービスで、専用回線を導入するよりコストを抑えられる。ＩＰ－ＶＰＮは、通信事業者の保有する広域ＩＰ通信網を経由して構築される仮想私設通信網で、遠隔地のネットワーク同士をＬＡＮ接続しているのと同じように運用することができる。

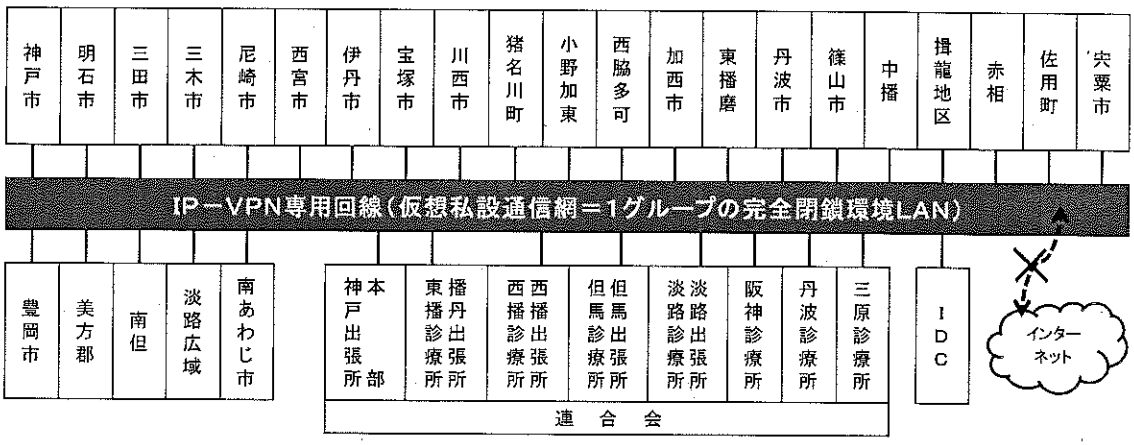


図1　IP－VPN方式によるネットワークイメージ図

(5) セキュリティの確保

集中化運用システムは、加入者等の個人情報を取り扱うため、不正アクセスやウイルス攻撃などによるデータの漏えい・破壊・改ざんなどを防止する措置が必要である。また、データの無断持ち出し、無許可ソフトウェアの使用、設計・開発の不備、操作・設定ミスなど非意図的要因によるデータの漏えい・消失等にも留意しなければならない。

このため、本会及び組合等の情報セキュリティポリシー並びに個人情報保護法などの関係法令に従いシステムを構築するとともに、サーバを本会及び各組合等で共同利用することとなるため、これまで以上にシステムの利用制限等を明確化する。

(6) 信頼性の確保

集中化運用方式は、あらかじめ設定した停止時間等を除き、原則として２４時間３６５日、いつでもシステム利用が確保されなければならないため、高い信頼性を確保したシステムを構築する。

(7) 利便性の確保

集中化運用方式は、各組合等及び本会が利用するシステムであることから、様々な職員や利用環境の違いが想定される。このため、簡易な操作性を有し、効率的な業務運営が確保されるシステムを構築する。

(8) 拡張性の確保

今後のシステム修正やシステム拡張等に備え、集中化運用システムとして十分な領域を確保し、ハードウェア・ソフトウェア両面から各種拡張が柔軟に対応可能なシステムとする。

このため、システムの基幹となるサーバやバックアップ装置などは、システム拡張時に追加システムから利用可能なオープンなインターフェースを有し、複数のシステムで共有可能なものとする。また、ソフトウェアを含め集中化運用システムを構成する資産は、有効活用可能なものを選定し、システム拡張時に必要最低限のシステムの追加で実現可能な構成とする。

(9) サポート体制の確保

集中化運用システムは、すべての組合等及び本会各事務所を専用回線でＬＡＮ構築し、仮想化(※4)等の高度な技術を用いたシステム体系であるため、システム運用にあたっては、専門的な知識や技術を有する要員がこれまで以上に必要になる。

このため、システム運用に係るサポート業務を専門事業者に委託する必要があるが、委託先事業者（以下「サポートセンター」という。）は、障害対応等に迅速・的確に対応するだけでなく、システム運営主体である本会と緊密な連携が図れ、本会が組合等に対して行う操作指導等についても、必要に応じて迅速・適切な支援が行えるなど、総合的なサポートサービスが提供できる事業者を指定する。

※4：仮想化

サーバやストレージ、ネットワークなどのＩＴリソースを物理的な構成にとらわれず、論理的に構成する技術。

(10) 費用負担の考え方

集中化運用システムは、県下全組合等及び本会がサーバを共用することとなるため、共用部分に係る費用(※5)負担は、クライアント数×システム数に応じた額とする。

ただし、システム運用主体は本会であることから、組合等の費用負担分は、現状から大きく増加しないよう調整を行うこととする。

また、原則として組合等には２５年度経費が発生しないよう調整を行うこととし、共用部分に係る各組合等負担費用は、２６年度から３０年度までの５年間、初期費用の５分の１と１年分ランニングコストの合計額を毎年度本会から請求する。

なお、本会が建物・農機具共済システムを運用する組合等に対して助成する「農業共済ネットワーク化情報システム助成金」の２６年度以降の取り扱いについては、別途定める。

※5：共用部分に係る費用

・サーバ及び周辺機器に係る初期費用、それらの機器のハード保守料
・ネットワーク回線及びルータに係る初期費用とランニングコスト、ルータのハード保守料
・ＩＤＣ利用、システム保守及びシステムサポートに係る初期費用とランニングコスト

一方、各組合等に設置するクライアント機及びプリンタに係る初期費用、それらの機器のハード保守料は、個別費用として、現状と同じく組合等から該当業者への直接支払いとする。

(11)　機器更新・システム移行に係る調達

集中化運営システムの構築・運営は「表１　構築・運営形態」に示す通り、ハウジングを含めた総合アウトソーシングとし、「表２　調達範囲」に示す通り、組合等のクライアント機の更新等を含め、本会が一括して指名競争入札を実施する。

表1　構築・運営形態

項　目	基本方針
運営主体	兵庫県農業共済組合連合会
事業者のサービス提供形態	総合アウトソース

表2　調達範囲（案：詳細は変更する場合があります）

調達の範囲	内　容
DBサーバ基盤	ハードウェア（4台） DB基盤の構築（全28インスタンス） 既存データの移行
ドメインサーバ基盤	ハードウェア（2台・冗長化） 認証基盤の構築 ユーザID・初期パスワード及びアクセス権等のセットアップ
ファイルサーバ基盤	ハードウェア（2台・NASストレージ可、1台はバックアップ用） フォルダ構成及びユーザごとのアクセス権等のセットアップ
アプリケーションサーバ基盤	ハードウェア（3台・負荷分散） SBC基盤の構築 アプリケーションのセットアップ
運用管理サーバ基盤	ハードウェア（1台） ウイルス対策管理基盤及びバックアップ基盤（LTOテープライブラリ）の構築
クライアント	シンクライアント（デスクトップ型●台、A4ノート型●台） システムログオン（RDP接続）のセットアップ 機器設置、現地調整及びシステムログオンの操作指導
プリンタ	モノクロページプリンタ（高速機●台、普通機●台） 機器設置、現地調整及び印刷基盤の構築
シンクライアントサービス	デスクトップ公開基盤の構築 印刷基盤の構築
ネットワーク機器	スイッチングハブ1000BASE-T（8ポート●台、16ポート●台） LANケーブルCAT5e（5m●本、10m●本）
業務運用サポート	本会が行なう下記メンテナンス作業等のサポート（設定指導等） ・ユーザメンテナンス・システムメンテナンス ・業務システムのバージョンアップ作業 ・本会が組合等に対して行うヘルプデスク業務 コンサルティング
各基盤の保守	サーバ等各基盤の保守 ・稼働監視 ・セキュリティ監視
業務システム	業務システムのセットアップ 全国標準システムのカスタマイズ
運用管理（監視・障害対応等）	システム監視 データ管理
IDC設備	ファシリティ設備 セキュリティ設備 ネットワーク設備 その他システム稼働に必要な設備
ハード保守（障害対応等）	別途締結する保守契約に基づく障害対応等

(12)　集中運用システムのイメージ図

ア　全体のイメージ図

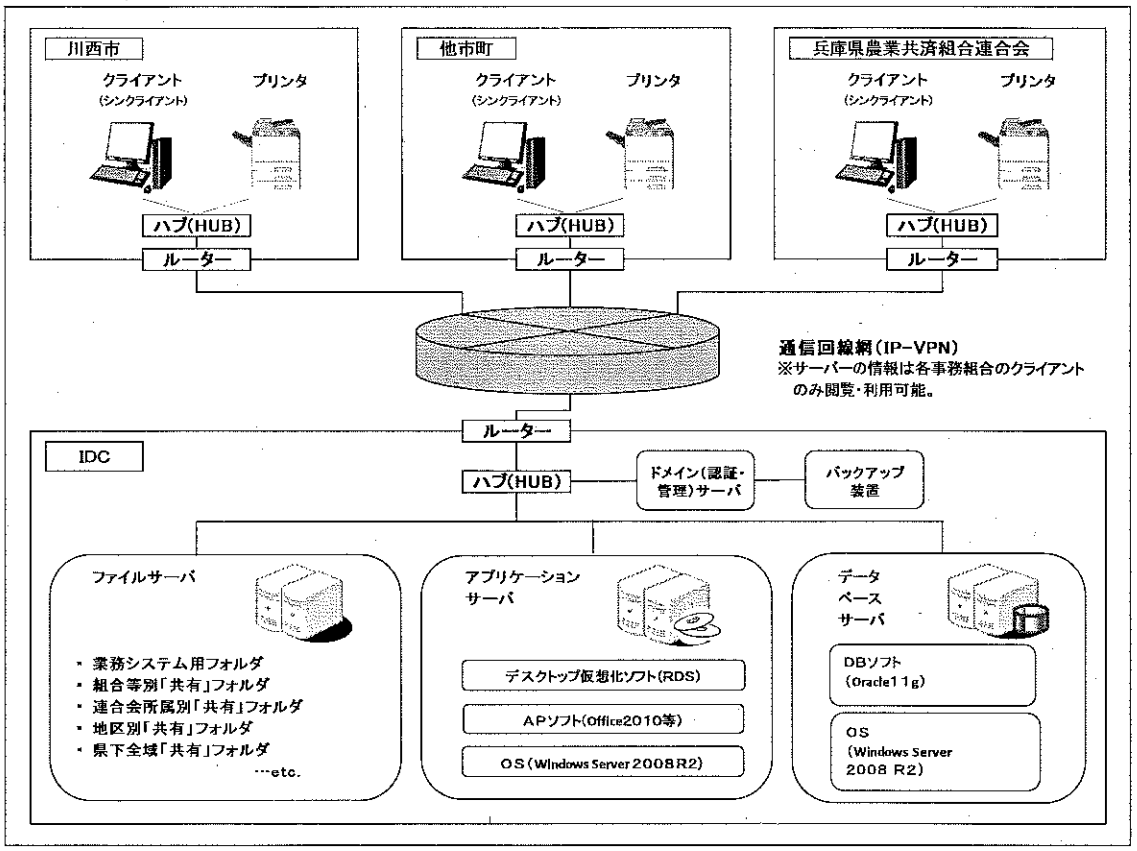


図2 集中化運用システムのイメージ

イ　クライアントの接続イメージ図

ファイルサーバーの共同利用等の必要があれば、業務システムを使用しない一般業務用PC（以下「一般PC」という。）をシステム用LANに接続することを可とする。

ただし、ウイルス対策等の関係から、OSはWindows 7以降、インターネットに接続しない、セキュリティ対策ソフトは指定品を導入するなど、一定条件を定めることとする。

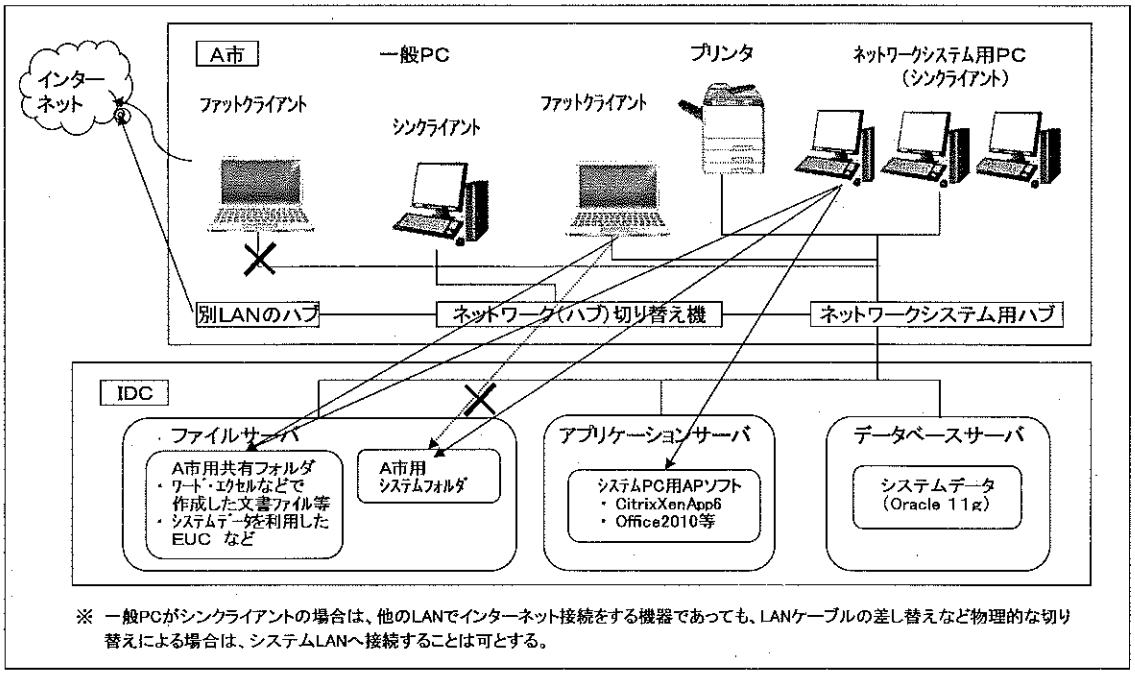


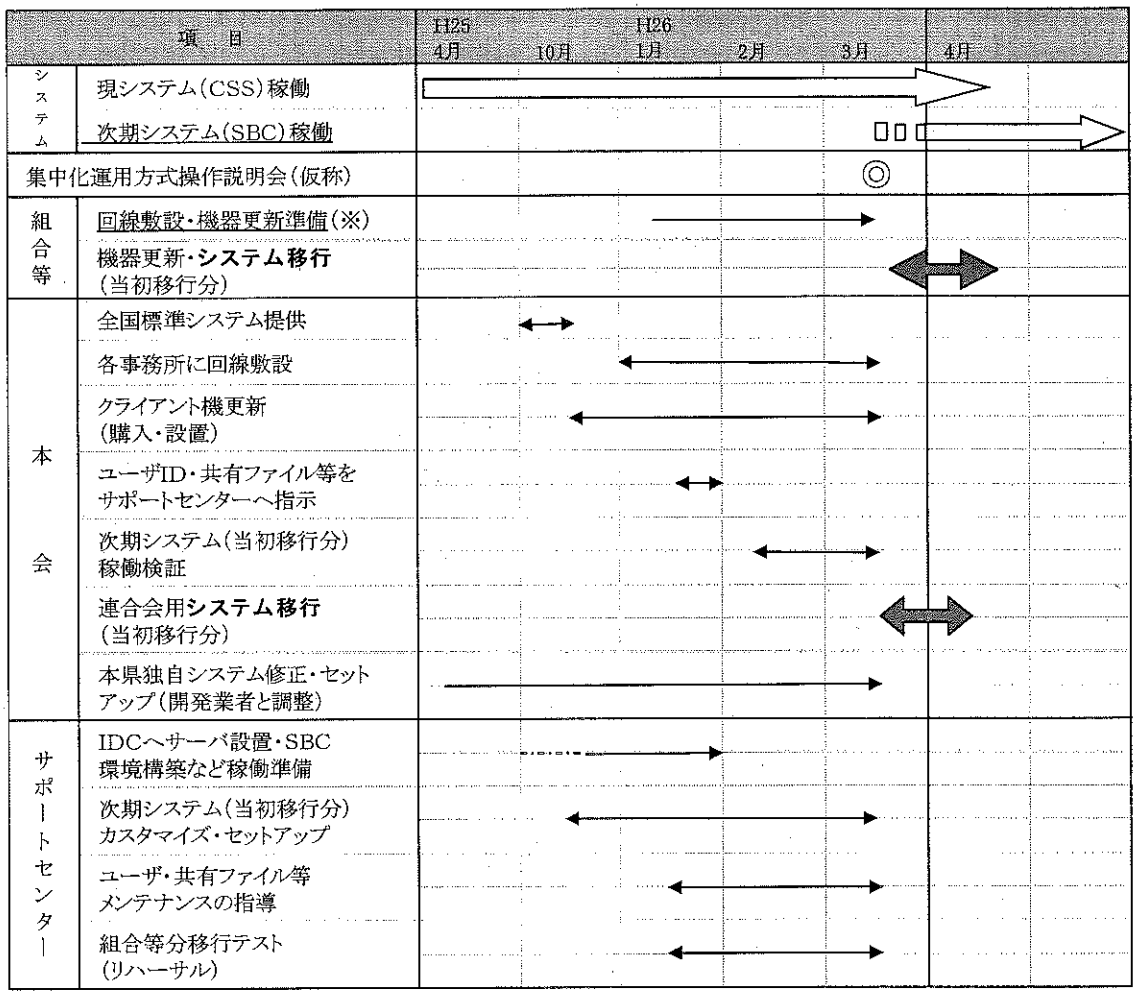
図3 クライアントの接続イメージ

(13) 移行計画

集中化運用システムへの完全移行は、次期ネットワークシステムの本格稼働期日である平成２６年４月とし、移行作業を以下のとおり計画する。

移行スケジュール

原則として、以下のスケジュールで移行作業を行うこととするが、移行作業本番はシステム稼働を停止する必要があり、また、移行作業中のデータ保全を確保するため、テストや事前検証を十分行い、移行作業本番は迅速かつ確実に実施する。



※：機器更新準備について

- 現サーバ及びクライアント機のハードディスク内にあるシステムファイル以外のファイルの移行（次期ファイルサーバの共有フォルダへの移行）については、それぞれの組合等（本会は所属別）が自ら移行作業を行う。組合等は、必要なファイルを整理・バックアップし、移行作業に備える。
- 回線施設に係る標準工事以外の特別工事については、組合等の別途対応及び経費負担となる。（回線施設とは、㈱ケイ・オプティコムの「Business 光」回線引き込み工事及びLAN配線設置工事など）

情報セキュリティポリシー

平成２５年４月１日

安心のネットワーク
NOSAI兵庫
兵庫県農業共済組合連合会

目　　次

情報セキュリティ基本方針

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害や事故などによるシステム障害やシステム運用の機能不全にも備える必要がある。

兵庫県農業共済組合連合会（以下「本会」という。）は、農業災害補償制度の実施主体として農業共済事業の加入者等の個人情報や業務運営上必要となる重要な情報を多数取り扱っているが、それらの多くは農業共済ネットワーク化情報システムをはじめとする情報システムやネットワークに依存している。

したがって、本会は、情報資産に対する安全対策を推進し、様々な脅威から防御することで加入者等からの信頼を確保するとともに、本会業務の安定的・継続的な運営のため、次の事項に積極的に取り組みます。

1　すべての役職員が情報セキュリティ対策に組織的に取り組むための体制を確立します。
2　すべての役職員が情報セキュリティ対策を組織的に実践するための共通の基準として、情報セキュリティ対策基準を策定します。
3　本会の保有する情報資産を適切に管理します。
4　情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するために、職員等に対して必要な教育を実施します。
5　情報セキュリティに関する事故が発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定めます。
6　情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施します。
7　すべての職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守します。
8　本会の会員たる共済事業を行う市町等を含めた本県農業共済組織全体の情報セキュリティの基盤を強化するため、当該市町等に対する注意喚起、連携・協力等に積極的に取り組みます。

平成２５年３月２２日

神戸市中央区下山手通４丁目15-3
兵庫県農業共済組合連合会
会長理事　鷲　尾　弘　志

情報セキュリティ対策基準

第１章　総　　則

１　目　　的

本対策基準は、本会のシステムリスク管理規則第 14 条及び情報セキュリティ基本方針に基づき、兵庫県農業共済組合連合会（以下「本会」という。）が情報セキュリティ対策等を組織的に実践するための共通の基準として、具体的な遵守事項及び判断基準を定める。

２　用語の定義

（１）システムリスク

第２章の要因により、コンピュータシステムのダウンや情報資産が漏えい等することに伴い、本会の会員たる共済事業を行う市町等及びその組合員等並びに本会が損失を被るリスクをいう。

（２）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（３）情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（４）業務システム

情報システムのうち、本会及び委託業者等が開発し、又は購入し、本会の業務遂行上必要な情報処理を行うため導入したソフトウェアをいう。

（５）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（６）情報セキュリティポリシー

情報セキュリティ基本方針及び本対策基準をいう。

（７）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（８）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（９）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

第２章　対象とする脅威

１　災害又は事故等

地震、落雷、火災等の災害、事故、故障等による業務の停止及びシステム運用の機能不全等

２　外部からの攻撃等

サイバー攻撃や不正アクセス等の部外者の侵入及びウィルス攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取

３　内部不正等

情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去

第３章　対象範囲

１　機構の範囲

本対策基準は、本会の職制規則第３条に定める全機構に適用する。

２　職員等の範囲

本対策基準は、本会の職員及び臨時雇員（以下「職員等」という。）並びに本会管理下で委託業務等を行う場合の従事者に適用する。

３　情報資産の範囲

本対策基準が対象とする情報資産は次のとおりとする。

情報資産の種類		情報資産の例
物理的資産	情報システム	サーバ、パソコン、OS・アプリケーションソフト等の市販ソフトウェア（ライセンス含む）、本会及び委託業者等が開発したソフトウェア等
	ネットワーク	通信回線、ルータ、ハブ等
	これらに関する施設・設備	サーバ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
	電磁的記録媒体	CD-R、DVD-R、フロッピーディスク、MO、DLT（Digital Linear Tape）、USB フラッシュメモリ等
データ資産	ネットワーク及び情報システムで取り扱う情報	ネットワーク及び情報システムで取り扱うデータ等（これらを印刷した書類を含む。）
システム資産	システム関連文書	システム設計書、プログラム仕様書、操作マニュアル、ネットワーク構成図等

第４章　組織体制

１　情報セキュリティ統括部署

システムリスク管理に関する取組の企画、立案、調整及び推進をするために、本会に情報セキュリティ統括部署（以下「セキュリティ統括部署」という。）を設置する。

ア　セキュリティ統括部署は、事務機械化等情報処理担当部署である企画普及部企画課とし、企画普及部長が情報ネットワーク管理者（以下「ネットワーク管理者」という。）として指揮、監督する。

イ　セキュリティ統括部署は、情報システムの運用及びコンピュータなどの物理的情報資産の導入、設定、保守等を管理する。

ウ　セキュリティ統括部署は、役職員に対しシステムリスク及び情報セキュリティに関する研修等を実施する。

２　情報セキュリティ最高責任者

情報セキュリティ最高責任者（以下「セキュリティ最高責任者」という。）は、会長とする。

セキュリティ最高責任者は、本会のシステムリスク管理に関する事項を統括し、本会におけるすべての情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

３　情報セキュリティ統括責任者

情報セキュリティ統括責任者（以下「セキュリティ統括責任者」という。）は、参事とする。

セキュリティ統括責任者は、本会のシステムリスク管理及び情報セキュリティ対策に関する事項について、セキュリティ最高責任者を補佐する。

4　情報セキュリティ責任者

情報セキュリティ責任者（以下「セキュリティ責任者」という。）を、職制規則に定める部、出張所、基幹家畜診療所ごとに置くものとし、所属長がこれにあたる。

セキュリティ責任者は、各所属のシステムリスク管理のため、情報セキュリティ対策に関する次の事項を統括する。

ア　情報セキュリティ統括部署との報告・連絡・協議

イ　所属の職員等に対する情報セキュリティに関する教育、助言及び指導

ウ　所管する業務システムの開発、設定の変更、運用、見直し等

エ　その他所属内のシステムリスク管理及び情報セキュリティ対策に関する事項

5　情報取扱管理者

情報取扱管理者を課、出張所、基幹家畜診療所及び出先診療所の各所属に１名置くものとし、課長、出張所次長、基幹家畜診療所次長及び出先診療所次長（以下「課長等」という。）がこれにあたる。

情報取扱管理者は、所属の情報セキュリティ責任者を補佐するとともに、所属の課又は所が保有する情報資産を管理する。

6　業務システム管理者

業務システム管理者は、各業務システムを所管する課長等とする。

業務システム管理者は、所管する業務システムの開発、設定の変更、運用、見直し等を行うとともに、所管する業務システムに関し、必要に応じて情報セキュリティ実施手順の制定、維持、管理を行うことができる。

7　情報セキュリティ監査責任者

情報セキュリティ監査責任者（以下「セキュリティ監査責任者」という。）は、監査指導部長とする。

セキュリティ監査責任者は、監査指導部の職員を指揮し、各部所における情報セキュリティポリシーの遵守について、毎年度１回以上、内部監査を行う。

なお、セキュリティ最高責任者は、情報セキュリティ等に関する専門知識を有する者を監査補助者として指名することができる。

8　情報セキュリティ委員会

システムリスク管理態勢の整備及び情報セキュリティ対策を確実なものとするための研究及び審議する機関として、本会に情報セキュリティ委員会（以下「セキュリティ委員会」という。）を設置する。

（１）セキュリティ委員会の構成

委員は、セキュリティ最高責任者、セキュリティ統括責任者、セキュリティ責任者及びネットワーク管理者とする。

なお、セキュリティ最高責任者が必要と認めた場合は、情報セキュリティに関する専門的な知識及び経験を有した者をアドバイザーとしてセキュリティ委員会に招聘することができる。

（２）召集及び議事

セキュリティ委員会は、次のような場合にセキュリティ最高責任者が召集する。

ア　情報セキュリティポリシーの変更等、情報セキュリティに関する重要な事項を決定するため審議等の必要が生じたとき。

イ　情報セキュリティ対策の改善計画の策定及びその実施状況を確認する必要が生じたとき。

9　業務システム定例会議

業務システムに係る障害対応等の情報共有及び運用改善のための協議などを目的に、毎月１回、業務システム定例会議を開催する。

ア　定例会議の参集範囲は、セキュリティ統括部署、業務システム管理者（ただし、本部職員に限る）及び業務システムに係る委託事業者とする。

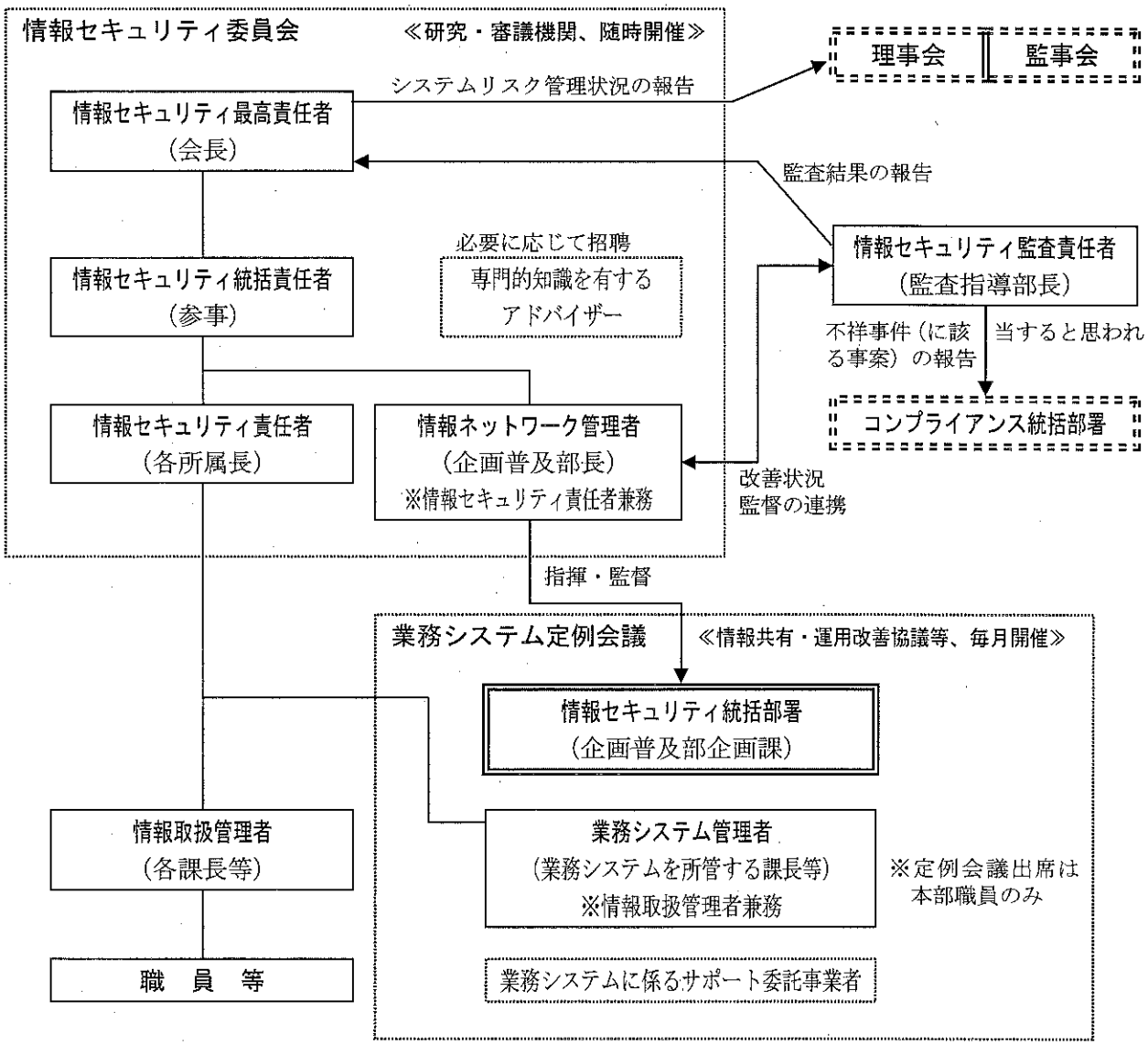
イ　セキュリティ統括部署は、定例会議においてシステムリスク管理及び情報セキュリティ上の重要な課題が協議された場合、速やかにセキュリティ統括責任者に状況報告しなければならない。

10　兼務の禁止

情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

また、監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

11　情報セキュリティ体制



第５章　情報資産の分類と管理方法

１　情報資産の分類

本会における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を定めることができる。

なお、それぞれの分類表の「該当する情報資産」に該当するデータだけでなく、それらが含まれる記録媒体、パソコン、システム等も同様に取り扱わなければならない。

（１）機密性による情報資産の分類

分　類	該　当　す　る　情　報　資　産
機密性３	業務で取り扱う情報資産のうち、特に機密性を要する次のようなもの ・　個人情報に関する情報資産 ・　法令・契約等により守秘義務を課されている情報資産 ・　漏えいした場合に本会の信頼を著しく損なうなど業務運営に支障を来たす恐れがある情報資産 ・　公開することでセキュリティ侵害の恐れがある情報資産
機密性２	業務で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないもの（機密性３には該当しないが、広報等は行っていない情報資産）
機密性１	機密性２又は機密性３以外の情報資産

（２）完全性による情報資産の分類

分　類	該　当　す　る　情　報　資　産
完全性３	業務で取り扱う情報資産のうち、特に完全性を要する次のようなもの ・　改ざん、誤びゅう又は破損により、加入者等の権利が侵害される情報資産 ・　改ざん、誤びゅう又は破損により、業務の適確な遂行に著しい支障を及ぼす恐れがある情報資産
完全性２	改ざん、誤びゅう又は破損により、業務の適確な遂行に支障を及ぼす恐れがある情報資産（完全性３には該当しないが、一部の内部業務に限定的に必要な情報資産）
完全性１	完全性２又は完全性３以外の情報資産

（３）可用性による情報資産の分類

分　類	該　当　す　る　情　報　資　産
可用性３	業務で取り扱う情報資産のうち、特に可用性を要する次のようなもの ・　滅失、紛失又は当該情報資産が利用不可能であることにより、加入者等の権利が侵害される情報資産 ・　滅失、紛失又は当該情報資産が利用不可能であることにより、業務の安定的な遂行に著しい支障を及ぼす恐れがある情報資産
可用性２	滅失、紛失又は当該情報資産が利用不可能であることにより、業務の安定的な遂行に支障を及ぼす恐れがある情報資産（可用性３には該当しないが、一部の内部業務に限定的に必要な情報資産）
可用性１	可用性２又は可用性３以外の情報資産

２　情報資産の管理

（１）複製又は伝送

情報資産が複製又は伝送された場合は、当該複製等も原本同様に管理しなければならない。

（２）情報資産の分類の表示

機密性２以上、完全性３又は可用性３の情報資産（以下「機密制限情報」という。）を外部記録媒体や文書等で保存する場合において、情報資産の分類を表示する必要があるときは、記録媒体のラベルや当該文書の隅等に情報資産の分類を表示しなければならない。

ただし、第三者が重要性の識別を容易に認識できないよう、適切な管理を行わなければならな

い。

（3）情報の作成及び入手

ア　業務上必要のない情報を作成してはならない。

イ　情報の作成時に１の分類に基づき当該情報の分類を定め、必要に応じて取扱制限を定めることができる。

ウ　作成途上の情報についても、紛失や流出等を防止するとともに、作成途上で不要になった情報は、適切に消去しなければならない。

エ　職員等以外の者が作成した情報資産を入手した場合は、１の分類に基づき当該情報の分類を定め、必要に応じて取扱制限を定めることができる。

オ　作成又は入手した情報資産の分類が不明な場合は、情報取扱管理者に判断を仰がなければならない。

（4）情報資産の保管

情報取扱管理者は、次のような点に留意した上で、１の分類に従い情報資産を適切に保管しなければならない。

ア　外部記録媒体に情報資産を長期保管する場合は、書込禁止の措置を講じなければならない。

イ　利用頻度が低い外部記録媒体を長期保管する場合は、温度・湿度・埃などの影響を十分考慮の上、適切な場所及び方法により保管しなければならない。

ウ　機密制限情報を記録した外部記録媒体を保管する場合、施錠可能な場所など適切な場所及び方法により保管しなければならない。

（5）情報の送信

電子メール等により機密性２以上の情報を送信する場合は、情報取扱管理者に許可を得なければならない。また、送信にあたっては、必要に応じ暗号化又はパスワード設定を行うなど、機密性を維持するための措置を講じなければならない。

（6）情報資産の運搬

車両等により機密性２以上の情報資産を運搬する場合は、情報取扱管理者に許可を得なければならない。また、運搬にあたっては、暗号化又はパスワードの設定を行うとともに、必要に応じ鍵付きのケース等に格納するなど機密性を維持するための措置を講じなければならない。

（7）情報資産の提供

機密性２以上の情報資産を外部に提供する場合は、情報取扱管理者に許可を得なければならない。提供にあたっては、必要に応じ暗号化又はパスワードの設定などにより機密性を維持するとともに、完全性及び可用性を確保しなければならない。

（8）情報資産の廃棄

機密性２以上の情報資産を廃棄する場合は、情報取扱管理者に許可を得なければならない。廃棄にあたっては、記録媒体の初期化等、情報を復元できないように処置しなければならない。

第６章　物理的セキュリティ

１　サーバ等の管理

（1）機器の取付け

ネットワーク管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を十分考慮の上、適切な場所及び方法により設置しなければならない。

（2）サーバの冗長化

ネットワーク管理者は、基幹サーバについて、次のような方法により、情報資産の完全性及び可用性の確保に努めなければならない。

ア　ディスクをRAID構成することにより障害発生時でもシステムを停止することなく容易にディスク交換が行えるよう措置する。

イ　本会出先事務所にバックアップ用サーバを設置し、定期的に自動バックアップ処理が行われ

るよう措置する。

（3）機器の電源

ア　ネットワーク管理者は、施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　ネットワーク管理者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（4）通信ケーブル等の配線

ア　ネットワーク管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するための必要な措置を講じなければならない。

イ　ネットワーク管理者は、施設管理部門等から通信ケーブル及び電源ケーブルの損傷等の報告があった場合、セキュリティ統括責任者に速やかに報告し、指示に従い必要な措置を行わなければならない。

（5）機器の定期保守及び修理

ア　ネットワーク管理者は、基幹サーバ及び関連機器の定期保守を実施しなければならない。

イ　ネットワーク管理者は、記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するなど、秘密保持に関して必要な措置を行わなければならない。

（6）敷地外への機器の設置

ネットワーク管理者は、本会施設の敷地外にサーバ等の機器を設置する場合、セキュリティ最高責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（7）機器の廃棄等

ネットワーク管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置からすべての情報を消去の上、復元不可能な状態で廃棄等しなければならない。

2　管理区域の管理

（1）管理区域の構造等

ア　管理区域とは、基幹サーバの設置場所及びその周辺で当該サーバの保守業務等を行うための場所をいう。

イ　セキュリティ統括責任者は、地上２階以上の場所又は無窓の外壁など、外部からの侵入が容易にできないような場所に管理区域を設置しなければならない。

ウ　セキュリティ統括責任者は、管理区域に通ずるドアは必要最小限とし常時施錠するとともに、施設内が無人となる場合には警報装置を稼動させるなど、許可されていない立ち入りを防止しなければならない。

エ　セキュリティ統括責任者は、管理区域内に設置した機器等に、転倒及び落下防止等のための必要な対策を講じなければならない。

オ　セキュリティ統括責任者は、管理区域内に消火薬剤や消防用設備等を設置する場合、消火薬剤等が機器等に影響を与えないよう配慮しなければならない。

（2）管理区域の入退室管理等

ア　ネットワーク管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿による管理を行わなければならない。

イ　ネットワーク管理者は、管理区域に入室しようとする者の身分等を確認しなければならない。

ウ　職員等は、管理区域に入室する際にコンピュータ、通信回線装置、外部記録媒体等を持ち込む必要がある場合は、ネットワーク管理者に許可を得なければならない。

（3）機器等の搬入出

ア　ネットワーク管理者は、搬入する機器等が既存の情報システムに与える影響について、あら

かじめ確認を行ったうえで搬入しなければならない。

イ　ネットワーク管理者は、機器の搬入出に立ち会わなければならない。

3　通信回線及び通信回線装置の管理

セキュリティ統括責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、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を講じなければならない。また、通信回線及び通信回線装置並びにそれらに関連する文書を適切に管理しなければならない。

第７章　人的セキュリティ

1　職員等の責務

（1）情報セキュリティポリシーの遵守等

ア　職員等は、情報セキュリティポリシーを遵守しなければならない。また、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がある場合は、速やかに所属のセキュリティ責任者に相談し、指示を仰がなければならない。

イ　セキュリティ責任者は、職員等が常に情報セキュリティポリシーを閲覧できるようにしておかなければならない。

ウ　職員等は、業務以外の目的に情報資産を利用してはならない。

エ　職員等は、情報資産の分類に応じ適切な取り扱いをしなければならない。

オ　職員等は、業務以外の目的で情報資産の外部への持ち出しや情報システムへのアクセスを行ってはならない。

（2）パソコン等の端末の持ち出し及び外部における情報処理作業の制限

ア　職員等は、本会のパソコン等の端末、ソフトウェア、記録媒体及びデータ資産を外部に持ち出す場合又は外部で情報処理業務を行う場合には、情報取扱管理者の許可を得なければならない。

イ　情報取扱管理者は、許可した情報処理作業の内容が、機密制限情報に関するものである場合、持ち出した情報資産の区分、持出期間や作業期間など管理上必要な事項について記録しなければならない。

ウ　職員等は、外部で情報処理作業を行う際に私物パソコンを利用する必要がある場合には、情報取扱管理者の許可を得た上で、安全管理措置を遵守しなければならない。なお、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

（3）パソコン等の持込

職員等は、私物のパソコン及び記録媒体を本会施設内に持ち込む必要がある場合は、情報取扱管理者の許可を得なければならない。

（4）机上の端末等の管理

職員等は、パソコン等の端末や記録媒体、情報が印刷された文書等について、第三者に情報を閲覧等されることがないように、長時間離席する場合には、端末をロックするとともに記憶媒体・文書等は適切な場所へ保管するなど、必要な措置を講じなければならない。

（5）退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を後任者に引き継ぎするとともに、その後も業務上知り得た情報を漏らしてはならない。

（6）外部委託事業者に対する説明

ネットワーク管理者（業務システムに関する場合は所管する業務システム管理者。以下「所管システム管理者」という。）は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容を説明し、遵守させなければならない。

2・研修

（1）研修の計画及び実施

ア　セキュリティ統括部署は、必要に応じて、職員等に対するシステムリスク及び情報セキュリティに関する研修を計画し、セキュリティ最高責任者の承認を得て実施する。

イ　職員等を新規採用した場合、情報セキュリティに関する研修を実施するなどして、情報セキュリティポリシーの内容を理解させ、遵守させなければならない。

ウ　新規採用以外の職員等に対する研修を実施する場合は、役職や情報セキュリティに関する理解度等に応じてクラス分けするなど、効果的に実施しなければならない。

（2）研修への参加

幹部を含めたすべての職員等は、定められた研修に参加しなければならない。

3　事故、欠陥等

（1）事故等の報告

ア　職員等は、システム上の重大な欠陥及び誤動作などによる情報セキュリティに関する事故について、発見した場合又は外部から報告を受けた場合、速やかに所属のセキュリティ責任者に報告しなければならない。

イ　報告を受けたセキュリティ責任者は、セキュリティ統括責任者及び事故等を引き起こしたシステムに係る所管システム管理者に速やかに報告しなければならない。

ウ　事故等を引き起こしたシステムに係る所管システム管理者は、緊急時対応計画に基づき必要な措置を講じなければならない。

（2）事故等の分析・記録等

セキュリティ統括責任者は、ネットワーク管理者及び事故等を引き起こした部所のセキュリティ責任者を指揮し、これらの事故等を分析し、記録を保存しなければならない。

4　ＩＤ及びパスワード等の管理

（1）ＩＤ等の供与

ネットワーク管理者は、職員等にパソコン等の端末を供与又は操作させる場合は、ＩＤ、パスワード、ユーザー権限及びアクセス権限など情報セキュリティに関し必要な設定をしたうえで供与等しなければならない。また、ＩＤ、パスワード等に関する情報を厳重に管理しなければならない。

（2）ＩＤの取扱い

職員等は、供与されたＩＤを他者に利用させてはならない。また、共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（3）パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理する。

イ　パスワードが流出したおそれがある場合には、所属のセキュリティ責任者に速やかに報告し、指示を仰ぐ。

（4）人事異動等に伴う管理

ア　ネットワーク管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴うＩＤ及びパスワードを適正に管理するため、必要に応じてその取り扱い等を当該職員等に周知しなければならない。

イ　業務システム管理者は、所管する業務システムの利用を停止又は廃止する場合は、当該システムに係るアクセス権限等を抹消するよう、ネットワーク管理者に通知しなければならない。

ウ　ネットワーク管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

第８章　技術的セキュリティ

１　コンピュータ及びネットワークの管理

（１）ファイルサーバの設定等

ア　ネットワーク管理者は、ファイルサーバを部所単位で構成し、職員等が他の部所のフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。

イ　ネットワーク管理者は、個人情報や人事記録等、取扱権限を制限すべきデータについて、別フォルダを作成する等の措置を講じ、同一部所内であっても、取扱権限を持たない職員等が閲覧及び使用できないようにしなければならない。

（２）バックアップの実施

ア　ネットワーク管理者は、ファイルサーバに記録された情報について、サーバの冗長化（RAID構成によるディスク冗長化含む）及び定期的なバックアップにより、業務継続性を確保するための必要な措置を講じなければならない。

イ　業務システム管理者は、データベースサーバなどファイルサーバ以外に記録された業務システム固有の重要データについて、別媒体への定期的なバックアップにより、業務継続性を確保するための必要な措置を講じなければならない。

（３）他団体との情報システムに関する情報等の交換

所管システム管理者は、情報システムに関する情報及びソフトウェアを他の団体と交換する場合、その取扱いに関する事項をあらかじめ定め、セキュリティ統括責任者の許可を得なければならない。

（４）ネットワーク構成図等の管理

ネットワーク管理者は、ネットワーク及びサーバに関する構成図及び仕様書等を適切に管理しなければならない。

（５）アクセス記録の取得等

ネットワーク管理者は、情報セキュリティ上重要なアクセスログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

（６）外部ネットワークとの接続制限等

ア　ネットワーク管理者は、本会のネットワークを外部ネットワークと接続しようとする場合には、セキュリティ最高責任者の許可を得なければならない。

イ　ネットワーク管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を調査し、本会内のすべての情報資産に影響が生じないことを確認しなければならない。

ウ　ネットワーク管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

エ　セキュリティ統括責任者は、外部ネットワークと接続する場合、不正アクセスを防止するため、ファイアウォール、ルータ及び通信ソフトウェア等の設定など、ネットワークに適切なアクセス制御を施さなければならない。

（７）無線ＬＡＮのセキュリティ対策

ア　ネットワーク管理者は、本会のネットワークに無線ＬＡＮを利用しようとする場合には、セキュリティ統括責任者の許可を得なければならない。

イ　セキュリティ統括責任者は、無線ＬＡＮの利用を認める場合、暗号化及び認証技術の使用を義務付けなければならない。

（８）外部ネットワークとのファイル送受信

セキュリティ統括責任者は、電子メール等を使用し外部ネットワークとファイルを送受信する場合、ファイアウォールによる制御など、コンピュータウィルスに対する適切な管理を行い、不正プログラムの本会内部ネットワークへの侵入及び外部への拡散を防止しなければならない。

（9）無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコン等の端末に対し、ネットワーク管理者が定める以外のソフトウェアを導入する必要がある場合は、ネットワーク管理者の許可を得なければならない。

イ　業務システム管理者は、所管する業務システムの運用のためにソフトウェアを導入する必要がある場合は、ネットワーク管理者の許可を得なければならない。

ウ　ネットワーク管理者は、新たに導入するソフトウェアが既存の情報システムに与える影響についてあらかじめ確認を行わなければならない。

エ　ネットワーク管理者は、導入するソフトウェアのライセンスを管理しなければならない。

オ　職員等は、不正コピーなどにより入手したソフトウェアを利用してはならない。

（１０）機器構成の変更の制限

ア　職員等は、パソコン等の端末に対し機器の改造及び増設・交換を行う必要がある場合には、ネットワーク管理者の許可を得なければならない。

イ　ネットワーク管理者は、機器の改造等に関する作業記録を作成し、適切に保存しなければならない。

ウ　職員等は、ネットワーク管理者の許可なくパソコン等の端末をネットワークに接続してはならない。

2　職員等による外部からのアクセス等の制限

ア　業務システム管理者は、所管する業務システムに関し、職員等に外部から内部ネットワークにアクセスさせる必要が生じた場合は、ネットワーク管理者と協議のうえ、セキュリティ統括責任者の許可を得なければならない。

イ　セキュリティ統括責任者は、外部からのアクセスが必要な合理的理由を有する必要最小限の者に限定して許可しなければならない。

ウ　セキュリティ統括責任者は、外部からのアクセスを許可する場合、アクセス方法及び利用方法等について、通信途上の機密性の確保や利用者の本人確認を確保するなど必要な措置を講じなければならない。

3　システムの開発、導入、保守等

（1）システムの調達

ア　所管システム管理者は、システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とするセキュリティ機能を明記し、セキュリティ最高責任者の許可を得なければならない。

イ　所管システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、セキュリティ統括責任者に報告しなければならい。

（2）開発担当者等の指名

ア　所管システム管理者は、システム開発をする際には、開発担当者及び作業者等を指名しなければならない。

イ　所管システム管理者は、システムの開発担当者及び作業者等が使用するハードウェア及びソフトウェアを特定しなければならない。

（3）システムの導入手順

ア　所管システム管理者は、必要に応じて、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

イ　所管システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

ウ　所管システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行の際、既に情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

エ　所管システム管理者は、新たに導入するシステムが、既存の情報システムに与える影響について、テスト環境などによりあらかじめ十分確認を行ったうえで接続しなければならない。

オ　所管システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わ

なければならない。

カ　所管システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（4）システム開発・保守に関連する資料等の保管

ア　所管システム管理者は、システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

イ　所管システム管理者は、テスト結果を一定期間保管しなければならない。

（5）情報セキュリティの確保

所管システム管理者は、システムに各種チェック機能を組み込み、当該システムにおける機密性・完全性・可用性が確保されるようシステムを設計しなければならない。

（6）システムの変更管理

所管システム管理者は、システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（7）障害記録

所管システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

4　不正プログラム対策

（1）不正プログラム対策ソフトウェアの常駐

ネットワーク管理者は、サーバ及びパソコン等の端末にコンピュータウィルス等の不正プログラム対策ソフトウェアを常駐させ、当該ソフトウェア及びパターンファイルを常に最新の状態に保たなければならない。

（2）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア　パソコン等の端末のソフトウェアに関するセキュリティ機能の設定をネットワーク管理者の許可なく変更してはならない。

イ　パソコン等の端末の不正プログラム対策ソフトウェアの設定をネットワーク管理者の許可なく変更してはならない。

ウ　パソコン等の端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

エ　外部から持ち込んだパソコン及び外部記憶媒体等を内部ネットワークに接続する場合は、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

オ　外部からデータ又はソフトウェアを取り入れる場合は、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

カ　添付ファイルが付いた電子メールを送受信する場合は、必ず不正プログラム対策ソフトウェアでチェックを行わなければならない。

キ　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

ク　ネットワーク管理者が提供するウィルス情報を、常に確認しなければならない。

ケ　コンピュータウィルス等の不正プログラムに感染した場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

5　不正アクセス対策

（1）セキュリティ設定

セキュリティ統括責任者は、不正アクセスによる情報資産の改ざん等を防止するために、使用されていないポートを閉鎖するなどの措置を講じなければならない。また、不正アクセスが検出された場合には、速やかに通報するようファイアウォール等を設定しなければならない。

（2）攻撃の予告

セキュリティ最高責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停

止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（3）記録の保存

セキュリティ最高責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の状況を記録するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃

セキュリティ統括責任者は、職員等が使用しているパソコン等の端末から本会内サーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）職員等による不正アクセス

セキュリティ統括責任者は、職員等による不正アクセスを発見した場合、当該職員等が所属する部所のセキュリティ責任者に通知し、適切な処置を求めなければならない。

6　セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集等

ネットワーク管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（2）不正プログラム情報の収集等

ネットワーク管理者は、コンピュータウィルス等の不正プログラム情報を収集し、必要に応じ、職員等に周知しなければならない。

（3）情報セキュリティに関する情報の収集等

セキュリティ統括責任者は、情報セキュリティに関する情報を収集し、必要に応じ関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

第9章　運　　用

1　情報システムの監視

ネットワーク管理者は、重要なアクセスログを取得するサーバの時刻設定は正確にするなど、セキュリティに関する事案を適切に検知するための必要な措置を講じ、情報システムを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

（1）遵守状況の確認及び対処

ア　セキュリティ責任者は、所管する部所における情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにセキュリティ統括責任者に報告しなければならない。

報告を受けたセキュリティ統括責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

イ　セキュリティ統括責任者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題を認めた場合には適切かつ速やかに対処しなければならない。

（2）端末及び記録媒体等の利用状況調査

セキュリティ最高責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

（3）職員等の報告義務

職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに所属のセキュリティ責任者に報告しなければならない。

報告を受けたセキュリティ責任者は、違反行為が直ちに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判断した場合、緊急時対応計画に従って適切に対処しなければならない。

3　侵害時の対応

（1）緊急時対応計画の策定

ア　セキュリティ最高責任者は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、あらかじめ緊急時対応計画を定め、侵害時には当該計画に従って適切に対処しなければならない。

イ　セキュリティ最高責任者は、緊急時対応計画の策定にあたって、必要に応じてセキュリティ委員会での意見集約等を行うことができる。

（2）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

（3）非常災害対応要領との整合性確保

セキュリティ最高責任者は、本会が異常かつ激甚な非常災害に備えて策定する「非常災害対応要領」と情報セキュリティポリシーの整合性を確保しなければならない。

（4）緊急時対応計画の見直し

ア　セキュリティ最高責任者は、情報セキュリティを取り巻く状況の変化や組織体制の改変等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

イ　セキュリティ最高責任者は、緊急時対応計画の見直しにあたって、必要に応じてセキュリティ委員会での意見集約等を行うことができる。

4　外部委託

（1）外部委託先の選定基準

所管システム管理者は、外部委託先の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（2）契約項目

情報システムの運用、保守等を外部委託する場合には、委託事業者との間で次の事項を明記した契約を締結しなければならない。

なお、アからケは必須項目とし、コからシは必要に応じて明記するものとする。

ア　情報セキュリティポリシーの遵守に関する事項

イ　委託先の責任者、委託内容、作業者、作業場所の特定に関する事項

ウ　提供された情報の目的外利用及び受託者以外の者への提供の禁止に関する事項

エ　業務上知り得た情報の守秘義務に関する事項

オ　再委託に関する制限に関する事項

カ　委託業務終了時の情報資産の返還、廃棄等に関する事項

キ　本会による監査、検査に関する事項

ク　事故時等の公表に関する事項

ケ　契約に違反した場合における契約の解除及び損害賠償に関する事項

コ　提供されるサービスレベルの保証に関する事項

サ　従業員に対する教育の実施に関する事項

シ　委託業務の定期報告及び緊急時報告義務に関する事項

（3）確認・措置等

ア　所管システム管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、問題を認めた場合には、セキュリティ統括責任者に報告したうえで指示を仰がなければならない。

イ　報告を受けたセキュリティ統括責任者は、その重要度に応じてセキュリティ最高責任者に問題の内容及び対応状況等を報告しなければならない。

5　例外措置

（1）例外措置の許可

所管システム管理者は、適正な業務の遂行を継続するため、情報セキュリティ関係規定とは異なる方法を採用し、又は関係規定を遵守しないことについて合理的な理由がある場合には、セキュリティ最高責任者の許可を得て、例外措置を取ることができる。

（2）緊急時の例外措置

所管システム管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、自らの判断で例外措置を実施し、事後速やかにセキュリティ最高責任者に報告しなければならない。

（3）例外措置の申請書の管理

セキュリティ最高責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

6　法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

ア　個人情報の保護に関する法律（平成15年5月30日法律第57号）

イ　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）

ウ　著作権法（昭和45年法律第48号）

エ　本会の「個人情報の保護に関する規則」（平成17年4月1日施行）

7　違反時の対応

情報セキュリティポリシー及びこれに基づく文書に違反した職員等及びその監督責任者は、その重大性、発生した事象の状況等に応じて、本会の「職員就業規則」に基づく懲戒処分の対象となる。

また、本会の「不祥事件対応要領」に規定する不祥事件に該当する場合は、同要領に基づく対応を行う。

第10章　評価・見直し

1　監　　査

（1）監査実施計画の立案

セキュリティ監査責任者は、監査を行うに当たって、監査実施計画を立案し、セキュリティ最高責任者の承認を得るものとする。

（2）外部委託事業者に対する監査

外部委託事業者（再委託事業者含む。以下同じ。）との委託契約書に本会による監査の実施を明記している場合は、セキュリティ監査責任者は外部委託事業者の情報セキュリティポリシーの遵守状況等について、委託契約書に基づき監査を行わなければならない。

（3）報告及び監督

セキュリティ監査責任者は、監査結果を取りまとめ、セキュリティ最高責任者に報告するとともに、被監査部所に指摘事項を通知し、セキュリティ統括部署と連携のうえ、その取組状況を監督しなければならない。

（4）監査結果の周知等

セキュリティ最高責任者は、監査結果を踏まえ、全部所のセキュリティ責任者に対する周知等

が必要な指摘事項を認めた場合は、セキュリティ委員会を開催するなどし、同種の課題及び問題点の有無を確認させなければならない。

（5）理事会への報告

セキュリティ最高責任者は、監査結果等システムリスク管理の状況について、半期ごと又は問題がある場合は随時、理事会に報告する。

2　自己点検

（1）実施方法

ア　所管システム管理者は、所管するネットワーク及び情報システムにおける情報セキュリティ対策状況について、毎月１回自己点検を実施しなければならない。

イ　セキュリティ責任者は、所管する部所における情報セキュリティポリシーの遵守について、毎月１回自己点検を行わなければならない。

（2）報告

所管システム管理者及びセキュリティ責任者は、自己点検結果を翌月10日までにセキュリティ統括部署へ報告するとともに、問題点等を発見した場合には、改善策を取りまとめ、あわせて報告しなければならない。

（3）自己点検結果の活用

ア　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　セキュリティ最高責任者及び情報セキュリティ統括部署は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3　情報セキュリティポリシーの見直し

ア　セキュリティ最高責任者は、情報セキュリティポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、必要があると認めた場合、情報セキュリティポリシーの見直し及び情報セキュリティ対策の改善指示等を行わなければならない。

イ　セキュリティ統括部署は、情報セキュリティ監査の結果等により、又は、セキュリティ最高責任者の指示に基づき、この対策基準の見直しを行わなければならない。

ウ　セキュリティ最高責任者は、情報セキュリティポリシーの見直し等にあたって、必要に応じてセキュリティ委員会での意見集約等を行うことができる。

エ　セキュリティ最高責任者は、情報セキュリティポリシーの見直し等にあたって、セキュリティ責任者に所管する部所における意見集約等を行わせることができる。

オ　情報セキュリティポリシーのうち、情報セキュリティ基本方針を見直す場合は、理事会の承認を得るものとする。

補　則

1　施　行

この対策基準は、平成２５年４月１日から施行する。

2　改正手続

この対策基準の改正は、セキュリティ統括部署が行い、セキュリティ最高責任者の承認を得て施行する。

3　旧要領等の廃止

この対策基準の施行に伴い、「記憶媒体の取扱いについて」及び「内部ネットワーク化運用管理要領」は廃止する。