システム管理規程

1.0版

システム管理規程

システム管理規程

１　趣旨

本規程は、サーバ、PC 及びスマートデバイス上の機密性・完全性・可用性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

２　対象者

（１）システム管理者

※システム管理者はサーバ管理者、ネットワーク管理者、クライアント端末管理者を指す。

（２）オペレータ

（３）システム設計者

（４）情報システム部

（５）情報セキュリティ委員会

３　対象システム

（１）本社、営業所、ホスティング、ハウジングを含む、全ての物理サーバシステム及び仮想サーバシステム。

（２）当社より支給・貸与した PC。

※本規程内では、「PC」はノートパソコンを含んだ PC 端末のことを指す。

（３）当社より支給・貸与したスマートデバイス。

※本規程内では、「スマートデバイス」はスマートフォン及びタブレット端末を指す。

４　遵守事項

４．１ アカウントの管理

４．１．１　アカウントの作成

(A.9.1.1、A.9.2.1、A.9.2.2、A.9.2.4、A.9.4.1)

（１）正式な社内プロセスにより、利用部門からシステム、アプリケーション、情報へアクセスするための新規アカウントの申請があった場合、システム管理者は、申請を受けたアカウントを利用者ごとに作成し、アカウントには業務に必要最小限のアクセス権限を設定すること。

（２）システム管理者は、作成したアカウントを『アカウント管理台帳』に記録すること。

（３）システム管理者は、アカウントに設定した初期パスワードは、推測しにくいものを設定し、セキュリティを確保し利用者へ確実に伝達すること。

４．１．２　アカウントの変更

(A.9.2.1、A.9.2.2、A.9.2.5)

（１）正式な社内プロセスにより、利用部門からアカウント変更の申請があった場合、システム管理者は、申請に従いアカウントの変更を行うこと。

（２）システム管理者は、定期的(例えば 1 年に１度)に利用部門の管理職にアカウント権限の見直しを依頼し、権限の変更が必要な場合、アカウント権限を変更すること。

（３）システム管理者は、『アカウント管理台帳』にアカウント変更内容を記録すること。

４．１．３　不要となったアカウントの削除

(A.9.2.1、A.9.2.2、A.9.2.6)

（１）正式な社内プロセスにより、利用部門からアカウント削除の申請があった場合、システム管理者は、申請に従いアカウントを停止・無効化すること。

（２）システム管理者は、定期的(例えば 1 年に 1 度)に利用部門の管理職にアカウントの棚卸しを依頼し、不要なアカウントは停止・無効化すること。

（３）システム管理者は、アカウント管理システムのアクセスログを確認し、一定期間(例えば３ヶ月間)使用されていないアカウントを停止・無効化すること。

（４）システム管理者は、『アカウント管理台帳』にアカウントの停止・無効化を記録すること。

４．１．４　特権アカウントの管理

(A.9.2.3、A.9.4.4)

（１）システム及びアプリケーションを制御するためのシステムユーティリティプログラムの使用はシステム管理者に制限する。

４．１．５　アカウント管理システム

(A.9.4.2、A.9.4.3)

（１）システム管理者は、パスワード管理システムのパスワードポリシーを次のように設定すること。

①パスワード長及び質(例：８文字以上、大文字、小文字、特殊文字の組み合わせ)を設定する。

②定期的(例：３カ月ごと)にパスワードを変更するように設定する。

③過去(例：過去１０回以内)に使用したパスワードの再使用を防止する。

④最初のログオン時に、利用者がパスワードを変更するように設定する。

⑤特に、重要なシステム、データへのアクセスが必要なアカウントには、パスワードに加え、二段階、二要素認証を実装する。

⑥認証に複数回(例：１０回)続けて失敗した場合、アカウントを使用停止にする。

４．１．６　パスワードを忘れた場合の処置

(A.9.2.2、A.9.2.4)

（１）パスワード再発行の申請を受けたシステム管理者は、速やかに新規のパスワードを発行して、利用者に通知すること。

（２）システム管理者は、申請してきた利用者が本人自身であることを何らかの方法（例えば電話返信）で確認すること。

４．２ サーバ管理

４．２．１　設計時の規定

(A.14.2.5、A.17.2.1)

（１）システム設計者は、サーバの設置の目的と当該サーバに保存する情報を明確にすること。また保存する情報に「顧客情報、プライバシー情報」などを含む場合は、『人的管理規程』を遵守すること。

（２）システム設計者は、サーバのセキュリティ設計を行う上で、必ずリスク分析を行うこと。リスク分析を行う上で、以下の項目を明確にすること。

①保護・脅威の対象（守るべき情報）

② 脅威

③ 脅威の原因、プロセス

④ 対策（予防、防御、検査、対応：回復）

（３）システム設計者は、OS のアクセス制御とアプリケーションとサービスのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定すること。この設計書は、変更履歴を含めて保管管理すること。

（４）システム設計者は、データのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定すること。これらのデータには、OS のシステムファイルやアプリケーション、アプリケーション設定ファイルなども含むこと。これらの設計書は、変更履歴を含めて保管管理すること。

（５）システム設計者は、CGI、API などのアプリケーション開発を行う際、リスク分析を実施し、仕様書の段階から、データの入力チェックなどの、セキュリティ対策の実施を行うこと。

（６）外部公開サーバに関して、情報セキュリティ委員会は、推奨プラットホームを規定すること。システム設計者は外部公開サーバのプラットホームについては、

情報セキュリティ委員会が規定する推奨プラットホームを採用すること。

（7）『リスクマネジメント規程』に従い、システム設計者がリスクアセスメントを実施した結果、サーバの高可用性が要求される場合、アセスメント結果に応じて、以下を考慮して冗長化を検討すること。

①仮想化技術を使用した冗長化

②アクティブ-アクティブ、アクティブ-スタンバイ構成による冗長化

③RAID(1、5、6)による冗長化

④データバックアップとコールドスタンバイによる冗長化

４．２．２　導入時の規定

(A.11.2.1、A.11.2.2、A.11.2.4、A.12.1.1)

（１）サーバ管理者は、サーバの設置場所をサーバルームまたは、それに準ずるセキュリティを確保でき、かつサポートユーティリティ(電気、通信サービス、空調、換気、給水等)を備えた場所にすること。

（２）サーバ管理者は、サーバを設置する場合、サーバ設置申請書を作成し、情報セキュリティ委員会で認可を受けること。

（３）サーバ管理者は、サーバの設置申請時にそのシステム構成を明確にすること。情報セキュリティ委員会により、システム構成の不備もしくは、改善要求を受けた場合、サーバ管理者は、直ちにシステム構成の再検討を行うこと。

（４）サーバ管理者は、情報及び情報システムの正しく安全な運用を確実にするため、管理体制及びサーバ管理者を明確にすること。人的不注意および故意の誤用のリスクを低減するため、サーバ管理者及びオペレータを２名以上任命すること。

（５）サーバ管理者は、サーバの設置申請時に運用手順書を作成し、情報セキュリティ委員会へ提出すること。また、運用手順書には侵害時対応手順を含むこと。

（６）システムセキュリティ責任者は、本規定が適用される以前の既存のサーバについては、３ヶ月以内に本規定に適合するようにすること。３ヶ月以内に、本規定に適合しない場合、情報セキュリティ委員会は、サーバの運用を強制的に停止させることができる。

４．２．３　環境設定の規定

(A.9.2.3、A.12.5.1、A.12.6.2、A.13.1.2)

（１）サーバ管理者は、サーバに使用するＯＳ及びソフトウェア（マルウェア対策ソフト、脆弱性検査ソフトを含む）には、情報セキュリティ委員会が規定したものを使用すること。

（２）サーバ管理者は、ＯＳのアクセス制御、ファイルのアクセス制御、アプリケーション及びサービスのアクセス制御は、厳密に行うこと。

（３）サーバ管理者、システム設計者は、ＷＥＢアクセスなどに使用する匿名ユーザアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可すること。

（４）システム設計者は、リスク分析を実施し、仕様書の段階から、データの入力チェック、内部でのデータの処理プロセス、出力されるデータの妥当性などの、セキュリティ対策の実施を CGI、API などのアプリケーション開発を行う者に義務づけること。

（５）サーバ管理者は、サーバの趣旨、用途に応じた必要最低限のアプリケーション・サービス及びネットワーク・サービスのみインストールすること。

（６）サーバ管理者は、サーバには、システム管理者あるいはオペレータごとに個別のアカウントを割り当て、推測困難なパスワードを設定すること。特にシステム管理者もしくはシステム管理者に類する権限を持つアカウントのパスワードは、厳重に管理すること。

４．２．４　運用時の規定

(A.12.2.1、A.12.4.1、A.12.4.2、A.12.4.4、A.12.6.1)

（１）サーバ管理者は、サーバで使用するソフトウェアに最新のＯＳバージョン、最新のアプリケーションバージョンを使用し、最新のセキュリティパッチを適用すること。また不要サービスの削除を常に行うこと。

（２）サーバ管理者は、マルウェア対策として常にマルウェア対策ソフトウェアの定義ファイル、エンジンが最新のものとなるよう設定し、更新があった場合は直ちに最新のマルウェア対策ソフトウェアでサーバをチェックすること。

（３）サーバ管理者はサーバの認証ログ、アクセスログ、トランザクションログ、アプリケーションログ等サーバの趣旨、用途に応じたログの取得を行わなければならない。

（４）サーバ管理者は、ログを安全な場所に一定期間(例えば１年間)保存すること。

（５）サーバ管理者は、定期的(例えば毎月)にログの分析を行うこと。

（６）サーバ管理者は、サーバを信頼できる標準時刻と同期させたマスタクロックと同期させること。

（７）サーバ管理者は、定期的(例えば四半期に１度)に、第三者による以下の検査を受けること。

①脆弱性検査ソフトによる最新の脆弱性情報を含む検査

②「サーバ設置申請書」と実際の設置機器との整合性

③不要なアクセス権が存在しないこと

④不要なサービスが起動していないこと

⑤不要なアカウントが存在しないこと

⑥推測可能なパスワードが設定されていないこと

（７）サーバ管理者は、第三者による検査結果は必ず記録し、一定期間保管すること。

（８）第三者による検査によりセキュリティの不備が発見された場合、サーバ管理者は、直ちに不備を是正し、不備の内容と対策状況を情報セキュリティ委員会に報告すること。

（９）サーバ管理者は、セキュリティ侵害が発生した場合、セキュリティ侵害時の対応手順書に則って速やかに対応すること。またサーバ管理者は、セキュリティ侵害時の情報を、できるだけ速やかに、情報セキュリティ委員会に報告すること。情報セキュリティ委員会は、前述の報告を受けた後、各行政機関等への通報を含めて迅速に対応すること。

（１０）万が一、想定外のセキュリティ侵害が発生し、セキュリティ侵害時の対応手順書のみでは状況の改善が見込めない場合、サーバ管理者は即座に情報セキュリティ委員会に報告すること。サーバ管理者は、情報セキュリティ委員会の指示のもと、手順書外の行為を行うことができる。但し、作業実施記録は詳細に記録し保管すること。

（１１）サーバ管理者は、状況の改善後、作業実施記録を元にセキュリティ侵害時の対応手順書を更新すること。

４．３ クライアント端末の管理

４．３．１　クライアント端末の設定

(A.8.1.2、A.9.4.2、A.11.2.8、A.12.2.1、A.12.4.1、A.12.6.1、A.12.6.2)

（１）当社の業務において、従業員が使用できるPC、スマートデバイスは当社が支給・貸与したもののみとする。クライアント端末管理者は、PC、スマートデバイスを管理台帳で管理すること。

（２）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、使用場所、使用する情報の重要度に応じて、ID、パスワードによる認証の他、二段階、二要素の認証機能を有効にすること。

（３）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、規定されたソフトウェアを導入すること。したがって、それ以外のソフトウェアを導入できないように設定すること。

（４）クライアント端末管理者は、導入したソフトウェアを常に最新の状態とするため、修正プログラム等を自動適用する設定にすること。

（５）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、規定されたマルウェア対策ソフトウェアを導入し、常に定義ファイル、エンジンが最新のものとなるように設定すること。

（６）クライアント端末管理者は、当社が支給・貸与するPC、スマートデバイスには、

規定された使用者ログ収集ソフトを導入すること。

（７）クライアント端末管理者は、当社が支給・貸与する PC、スマートデバイスのスクリーンロックを、PC に関しては１５分、スマートデバイスに関しては１分に設定すること。

（８）クライアント端末管理者は、当社が支給・貸与するスマートデバイスとクラウドサービスとのデータ連携機能を停止すること。

４．３．２　持ち出しクライアント端末の設定

(A.10.1.1、A.11.2.6)

（１）クライアント端末管理者は、持ち出し PC には、基本認証以外にも BIOS 上での認証を行うように設定すること。

（２）クライアント端末管理者は、持ち出し PC には、セキュリティチップ、暗号化機能を搭載した機種を選定すること。

（３）クライアント端末管理者は、持ち出しスマートデバイスには、認証機能、セキュリティチップ、暗号化機能を搭載した機種を選定すること。

４．３．３　クライアント端末の再利用

(A.11.2.7)

（１）PC、スマートデバイスの利用者が変わる場合、PC、スマートデバイスを初期化し、再設定すること。

４．４　ＬＡＮ接続

４．４．１　ＬＡＮ接続申請への対処

（１）情報システム部は、LAN に接続するクライアント端末は、当社が支給・貸与したもののみとし、利用者の個人所有の機器の LAN 接続を許可してはならない。

（２）情報システム部は、利用者からの申請に対し、利用目的、利用形態を審査し、審査結果を申請者に連絡すること。

（３）情報システム部は、利用申請に対し許可を与える場合、一定規則に則ってホスト名、IP アドレスを決定すること。また、必要に応じて DNS、およびディレクトリへの情報登録を行うこと。DHCP など、動的に IP アドレスが変化する利用が発生する場合は、その旨を認識すること。

（４）情報システム部は、利用申請に対し許可を与える場合に、接続する HUB・情報コンセント・利用ケーブル番号など、接続箇所を決定すること。

（５）情報システム部は、利用者に提供する以下の情報一覧（必要に応じて図を利用）を保存し、管理すること。

①IP アドレス利用一覧

②ホスト名称、DNS 登録一覧

③接続箇所利用一覧

（６）情報システム部は、利用申請に対し許可を与える場合、以下の情報を保存し、管理すること。

①利用者情報（氏名、所属、連絡先等）

②利用目的

③利用形態（設置箇所、利用時間帯、利用サービス、予定期間）

④利用機器情報（管理者、連絡先、MAC アドレス等ハードウェア情報、機器名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

（７）情報システム部は、利用申請に対し許可を与える場合、申請者に対して以下の情報を連絡すること。

①許可された利用目的

②許可された利用形態（設置箇所、利用時間帯、利用サービス、予定期間）

③利用機器情報（ホスト名称、IP アドレス、アドレス取得形態（固定 IP/DHCP）、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

４．４．２ ＬＡＮ接続時の留意点

（１）情報システム部は、緊急を要する場合など、必要に応じて利用者の LAN 接続を制限（アクセスの制御、切断など）することができる。また緊急時には、情報システム部は利用者に対して指示を与える前に LAN 接続を制限してもよい。

（２）情報システム部は、利用者の接続形態にあわせ、適切な認証機能・暗号化機能等を提供し、情報の保護に努めること。

①無線 LAN を利用する場合、認証および暗号化機能を利用すること。

②Switching HUB 等を利用して、利用者間でのパケットキャプチャができない仕組みを用いること。

③LAN に接続する機器の通信は、『システム利用規程』に照らして適切な通信のみに限定すること。

④リモートアクセスについては、『システム利用規程』に照らして適切な通信のみに限定すること。

⑤各サーバへのアクセス状況については、『本規程』に基づいて対処すること。

４．４．３ ＬＡＮ接続情報の更新、通知

（１）情報システム部は、利用者に許可した LAN 接続形態が守られているか、許可後 2 週間以内に、申請内容に照らして確認すること。また半年に一度、部門ごとの LAN 接続状態を確認すること。

（2）情報システム部は、利用者に許可した LAN 接続について、申請・変更時に予定していた期間が満了する2週間前に､利用者に期間の満了について通知すること。また、期間を満了する機器が周辺業務に影響を及ぼす事が無いか、あわせて調査すること。

４．４．４ 変更手続き

（1）情報システム部は、利用者からの変更申請に対し、利用目的・利用形態を審査し、申請結果を申請者に連絡しなければならない。変更申請は、変更時の申請に必要な情報（箇所、目的、事由）が明確になっていない場合、および変更前と比較して、同等以上のセキュリティが確保できない場合にはこれを許可しないこと。

（2）情報システム部は、変更申請に対し許可を与える場合、管理している情報（利用者情報、利用目的、利用形態、利用機器情報）を更新すること。

（3）情報システム部は、変更申請に対し許可を与える場合、申請者に対して以下の情報を連絡すること。

①許可された利用目的

②許可された利用形態（設置箇所、利用時間帯、利用サービス、予定期間）

③利用機器情報（ホスト名称、IP アドレス、アドレス取得形態（固定 IP/DHCP)、接続箇所情報、DNS 登録の有無、ディレクトリ登録情報）

４．４．５ 機器の撤去

（1）情報システム部は、以下に該当する場合、利用者の LAN 接続の終了を確認すること。

①申請・変更時に予定していた期間を満了した場合

②緊急時など、情報システム部が必要と判断した場合

③その他接続が不要、あるいは不適当と見なされる場合

（2）情報システム部は、利用者の LAN 接続終了にあわせ、利用者管理情報を更新（接続終了と判断できる状態に）すること。

（3）情報システム部は、以下の情報一覧を更新すること。

①IP アドレス利用一覧

②ホスト名称、DNS 登録一覧

③接続箇所利用一覧

４．５ マルウェア対策

４．５．１ マルウェア対策ソフトウェアの選定

（1）当社は、全てのサーバ、PC 及びスマートデバイスにマルウェア対策ソフトウェアを導入する。

（2）マルウェア対策ソフトウェアは、情報システム部が選定し、定期的に見直しを実施する。

（3）情報システム部が選定するマルウェア対策ソフトの要件には、以下の機能が含まれていなければならない。

①定義ファイルの自動更新機能

（ベンダー→社内サーバ→PC、ベンダー→スマートデバイス）

②常時スキャン機能

（サーバ、PC、スマートデバイス）

４．５．２　マルウェア対策ソフトの設定

（1）システム管理者は、マルウェア対策ソフトウェアは、常駐設定にし、ファイルへのアクセスおよび電子メールの受信時に、常時スキャンできるように設定すること。

（2）システム管理者は、常時スキャンだけではなく一週間に一度、ファイル全体に対するスキャンを実施するように設定すること。

（3）システム管理者は、定義ファイルを常時更新するように設定すること。

４．５．３　マルウェア対策窓口の設置

（1）情報システム部は、社内のマルウェア被害状況等を迅速に収集するために、マルウェア対策窓口を設置し周知徹底すること。

（2）マルウェア対策窓口は、社内のマルウェア被害状況を掌握し、問題発生時の一次対応を実施すること。

４．５．４　マルウェアに感染した場合

（1）利用者よりマルウェア感染の連絡を受けたシステム管理者は、ネットワーク機能を停止することを指示し、現場に急行すること。

（2）現場では、マルウェア対策ソフトの定義ファイルがいつ更新されているかを確認すること。最新であれば、PC、スマートデバイスに対してフルスキャンを実行し、マルウェアが検知されるかを確認すること。

（3）マルウェアが検知された場合、システム管理者は、そのマルウェアの特性上どのような挙動を示すか予測し、影響範囲の特定を実施すること。マルウェアが検知されなかった場合、ファイアウォールのログを確認し、怪しいログが残っていないかどうかを確認するなどして、原因を特定すること。

（4）情報システム部は、マルウェア被害の影響範囲が、社外にまで至っている場合、『セキュリティインシデント報告・対応規程』に従って、問題の沈静化を図ること。

４．６ 媒体の管理

４．６．１　サーバ、PC、スマートデバイス（IT 機器）の修理

（１）情報システム部は、故障の状況により、保管されている情報の確認や保護が実施できない場合、ハードディスク等の情報が保管されている装置を取り外して修理を依頼すること。

（２）情報システム部は、外部業者が社内に立ち入って修理を行う場合、『物理的管理規程』に基づいて対応すること。

４．６．２ 媒体の保管・再利用

(A.8.3.1、A.10.1.1、A.10.1.2)

（１）情報システム部は、機密性の高い情報を媒体に保存する場合、権限のない者が保管された情報にアクセスできないように、暗号化を行うか、媒体を鍵のかかる場所に保管し、鍵は容易に持ち出しが出来ない場所に保管すること。

（２）情報システム部は、暗号化鍵を、機密情報を保存した媒体とは別媒体に保管し、それぞれ別々の場所に保管すること。

（３）情報システム部は、機密性の高い情報が保存されている媒体を再利用する場合、保存されていた情報を、再生できない方法で消去すること。）

４．６．３　サーバ、PC、スマートデバイス（IT 機器）と媒体の廃棄

(A.8.3.2)

（１）情報システム部は、機密性の高い情報が保管されたハードディスク等媒体を廃棄する場合、理論的に情報を消去するか物理的に破壊して、情報が再生不能な状態にすること。

（２）情報システム部は、機密性の高い情報が保管されたバードディク等媒体の処分を外部業者に委託する場合、情報セキュリティ委員会の承認を得ること。外部業者に委託する場合、秘密保持及び、処分依頼品の再利用の禁止を契約書に含めること。

４．７ 脆弱性管理

４．７．１　脆弱性情報の収集

(A.12.6.1)

（１）情報システム部は、ソフトウェア及びハードウェアの各管理台帳をもとに、社内システムに導入されている全てのハードウェア及びソフトウェアの脆弱性情報を定期的に収集すること。

（２）脆弱性情報は、IPA、CERT、各ベンダーの Web サイトやサポートページなど、信用できる情報源から収集すること。

（3）収集した情報は、重要性、影響範囲などから以下の様に分類すること。

危険度　高：サーバの管理権限の剥奪などにより、業務が停止してしまう、または取引先などに影響を与える可能性があり、即座に対処が必要な情報

危険度　中：業務が停止あるいは取引先などには影響を与えないため、即座に対処する必要はないが、定期メンテナンス時などに対処する必要がある情報

危険度　低：特殊な環境/設定でのみ発生し、社内のシステムには関係がないため、特に対処しなくともよい情報

４．７．２　脆弱性情報の配布

(A.12.6.1)

（1）情報システム部は、収集した情報を危険度に応じて関係者に周知させること。

危険度　高：発見次第即座に関係者全員に連絡。連絡方法は基本的にはメールを使用。場合によっては社内放送なども利用。

危険度 中：週 1 回程度の定例報告を実施。メールにて関係者全員に連絡。

危険度 低:週 1 回程度の定例報告を実施。メールにてシステム管理者に連絡。

（2）情報システム部は、収集した情報を基に以下のものを作成、公開すること。

①サーバ設置時の OS の適用パッチ一覧

②サーバ設置時に必要となるサービスなどをまとめたセキュリティ設定チェックリスト

③アプリケーションの適用パッチ一覧

④アプリケーションの実装変更

４．７．３　脆弱性対応

(A.12.6.1)

（1）システム管理者は、セキュリティパッチの適用が可能な場合、危険度に応じて、パッチの適用を行うこと。

（2）システム管理者は、社内全てのサーバ、PC、スマートデバイス(IT 機器)に対して、（1）のパッチが適切に適用されているかを確認すること。

（3）セキュリティパッチの適用が、アプリケーションに大きな影響を与える可能性等が有る場合、システム管理者は、リスク分析を行い、情報セキュリティ委員会に報告し、以下の対応策の指示を受けること。

①障害のリスクを受容し、パッチを適用する。

②パッチを適用せず、リスクに運用で対処する。

③パッチを適用せず、リスクを受容する。

４．８　ログの取得及び監視

４．８．１　システムのログによる監視

(A.12.4)

（１）システム管理者は、対象システムの以下のログを取得すること。なお取得されたログはアクセス制御を施したログサーバに転送し、規定の期間(例えば１年間)安全に保管すること。

①取得対象

（ア）ログオン・ログオフの記録

（イ）サーバのアクセスログ

（ウ）システムログ

（エ）アプリケーションログ

（ウ）PC の使用ログ

②取得内容

（ア）アクセス時刻

（イ）アクセスの成功/失敗

（ウ）認証の成功/失敗

（エ）ファイルの作成/読み込み/書き込み/移動/コピー/消去

（オ）USB 等記録媒体の利用

（カ）メール、Web の利用履歴

（２）システム管理者は、許可された処理だけが実行されていることを確認するため、ログを定期的(例えば月１回)に分析すること。分析の結果、以下のような事象が確認された場合、情報セキュリティ委員会に報告すること。

①連続したアクセスの失敗

②連続した認証の失敗

③データベースからの大量データの送受信

④違反行為

⑤権限外の処理の試み

⑥ユーザアカウントに関する変更（追加、削除、グループ変更等）

⑦アクセス権の変更

（３）システム管理者は（２）の事象が、不正アクセスによってもたらされた疑いがある場合、『セキュリティインシデント報告・対応規程』に基づいて、原因究明、再発防止計画の作成等、適切な対応を実施すること。

（４）システム管理者は、（１）で取得するログの時間情報を適切に保ち、ログの証拠としての有効性を高めるため、NTP サーバを用いてシステム間の時刻同期をとる

こと。ただし、その場合、NTP サーバ自身のセキュリティ対策にも十分配慮すること。

４．９　サーバのバックアップ

(A.12.3)

（１）サーバ管理者は、業務上重要なサーバ（基幹システム、データベースサーバ、WWW サーバ、mail サーバ、ログサーバなど）については、そのデータ及び構成情報を定期的にバックアップすること。

（２）パッチの適用など、サーバのシステムに対して何らかの変更を行う場合、変更後、不具合が発生する可能性がある。その為、サーバ管理者は、サーバに対して変更を行う前にサーバのシステムバックアップを取ること。

（３）パッチの適用など、サーバのシステムに対して何らかの変更を行った場合、サーバ管理者は、安定動作確認後、サーバのシステムバックアップを取ること。

（４）サーバ管理者は、バックアップ頻度、バックアップ方法、バックアップメディア、バックアップメディアの保管場所を、以下を考慮して決定すること。

①事業継続性

②どの時点の情報にあるいはシステム構成に戻す必要があるのか

③何時までにシステムを復旧する必要があるのか

４．１０　システムの監視について

(A.12.1.3)

（１）システム管理者は、システム障害等の兆候をいち早く見つけるため、死活監視、リソース(CPU、メモリ、保存容量、IO、ネットワーク帯域等)監視、Error ログの監視を行うこと。

４．１１　運用業務

（１）システム管理者の運用業務はオペレータに委任することができるが、オペレータは運用手順書以外の操作を行ってはならない。

（２）システム管理者は、次の項目を含んだ運用日誌を作成し一定期間（例えば５年間)、保管管理すること。

①システムへのログイン時間とログオフ時間

②システムの設定変更内容

③ログの保存記録

④バックアップ実施記録

⑤システムエラーの記録とその是正処置

（３）情報セキュリティ委員会は、定期的に運用日誌を検査し不適切な記載が発見さ

れた場合、適切な是正処置をシステム管理者に指導すること。

５　運用確認事項

（１）『アカウント管理台帳』、『ハードウェア、ソフトウェア資産管理台帳』、『ログ』等運用において必要な記録が残っているかを定期的に確認すること。

（２）ハードウェア、ソフトウェアライセンスの棚卸しを定期的に実施すること。特に、持ち運びが可能な装置(ノート PC、スマートデバイス、USB 等)は高頻度で棚卸しを実施すること。

（３）本規程に基づき、システムが運用、管理されていることを定期的に確認すること。

（４）サーバ、クライアント端末ログの分析結果は、ネットワーク管理者と情報共有すること。

（５）『リスク管理規程』によるリスク評価結果、脆弱性管理の結果に基づき、定期的に運用方法を見直しすること。

（６）リスクを受容して運用している場合、新技術、運用方法により、リスクを低減する方法が無いかを定期的に評価すること。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならな

ﾚﾝ。