システム監査マニュアル
（実施要綱および実施手順）

株式会社〇〇〇〇

情報システム部門

2013 年 7 月版

改定履歴

版数	改定内容	ページ	作成	承認	作成日
1.0.0	制定	ALL	情報システム 管理担当者	情報システム 管理責任者	20XX.XX.XX

～ 目次 ～

■　定義

１．本書の目的

本書は、当社の情報システムが安全に稼動し、一定水準のセキュリティレベルが保たれていることを、社内において自発的に確認するための実施要綱および実施手順である。

本書で扱うシステム監査は、組織における「IT 統制」の整備状況の確認にも同様に活用することができる。

IT 統制は、2008 年 4 月に施行された金融商品取引法（J-SOX 法）によって企業に義務付けられた「財務報告に係わる内部統制」の基本要件の一つであり、その整備状況および運用状況は、定期的に企業の経営層に報告する必要がある。

このような背景から、本書では『システム管理基準　追補版（財務報告に係る IT 統制ガイダンス)』に基づき、「IT への対応」で要求される以下の IT 統制項目について、整備状況の実態把握を行うための評価項目を定める。

１．アカウント管理
２．アクセス権管理
３．証跡管理（ログ管理）
４．システム運用・保守管理
５．情報セキュリティ管理

なお、本書は上記の管理状況について監査するための事項を示したものであり、本書に記載のない IT 統制項目については、必要に応じて適宜定めることが望まれる。

２．監査対象

本書において監査の対象となる情報システムは以下のとおりとする。

- ドメインコントローラ（Active Directory ／ Windows Server）
- ファイルサーバ
- データベースサーバ
- プリントサーバ
- クライアント PC（Windows OS を搭載した端末）

３．利用する監査ツール

本書では以下のソフトウェア製品を利用して、監査に必要となる証跡を作成する。

- ALog ConVerter
  …ドメインコントローラ、ファイルサーバ、プリントサーバの
  アクセスログを収集する。
- ALog ConVerter DB
  …データベースサーバのアクセスログ、操作ログを収集する。
- Resource Athlete
  …クエリ（情報の収集命令を発行する機能）を用いて、監査対象システムの
  アクセス権、アカウント情報等、さまざまな情報を収集する。

４．証跡となる監査レポート

監査における証跡とする監査レポートは、次頁に示す表のとおりとし、「３．利用する監査ツール」に定める監査ツールを用いてこれらを作成する。

併せて、監査レポートの作成対象となる情報システムおよび、監査レポートの作成に利用するログまたはクエリを、同表に記載する。

No	監査レポート	対象システム	監査レポートの作成に利用するログ／クエリ
A	**ALog ConVerter による監査レポート**		
A01	ユーザアカウントの作成／削除	ドメインコントローラ	管理者操作ログ
A02	ユーザアカウントの有効化／無効化	ドメインコントローラ	管理者操作ログ
A03	ユーザアカウントの変更	ドメインコントローラ	管理者操作ログ
A04	グループアカウントの作成／削除	ドメインコントローラ	管理者操作ログ
A05	グループアカウントの変更	ドメインコントローラ	管理者操作ログ
A06	グループメンバの追加／削除	ドメインコントローラ	管理者操作ログ
A07	ユーザアカウントの作成／パスワード設定	ドメインコントローラ	管理者操作ログ
A08	ファイル／フォルダのアクセス権変更	ファイルサーバ	アクセス権変更ログ
A09	ログオン／ログオフ	ドメインコントローラ	ログオン／ログオフログ
A10	重要フォルダへのアクセス	ファイルサーバ	ファイルアクセスログ
A11	重要フォルダのファイル編集／削除	ファイルサーバ	ファイルアクセスログ
A12	土日のファイルアクセス	ファイルサーバ	ファイルアクセスログ
A13	夜間のファイルアクセス	ファイルサーバ	ファイルアクセスログ
A14	ログオン失敗	ファイルサーバ	ログオン／ログオフログ
A15	書き込み・削除の失敗	ファイルサーバ	ファイルアクセスログ
A16	重要フォルダ内のファイル印刷(サーバ)	プリントサーバ	プリントログ
A17	特権管理者アカウントによるファイル操作	ファイルサーバ	ファイルアクセスログ
A18	重要フォルダへのアクセス	ファイルサーバ	ファイルアクセスログ
A19	退職予定者のアクセス状況	ファイルサーバ	ファイルアクセスログ
D	**ALog ConVerter DB による監査レポート**		
D01	データベースユーザの追加／削除	データベースサーバ	管理操作ログ
D02	データベースユーザへの特権付与	データベースサーバ	RAWSQL ログ
D03	重要な情報システムのデータベース操作	データベースサーバ	アクセスログ
D04	特権ユーザによるデータベース操作	データベースサーバ	RAWSQL ログ
D05	特定アプリケーション以外のテーブル操作	データベースサーバ	アクセスログ

No	監査レポート	対象システム	監査レポートの作成に利用するログ／クエリ
R	**Resource Athlete による監査レポート**		
RA01	全ユーザアカウント一覧	ドメインコントローラ	アカウントクエリ
RA02	無効なユーザアカウント一覧	ドメインコントローラ	アカウントクエリ
RA03	一定期間利用されていないアカウント一覧	ドメインコントローラ	アカウントクエリ
RA04	一定期間パスワード未変更のアカウント一覧	ドメインコントローラ	アカウントクエリ
RA05	グループアカウントとグループ構成の一覧	ドメインコントローラ	アカウントクエリ
RA06	特権管理者アカウント一覧	すべての対象サーバ	アカウントクエリ
RA07	既定の管理者アカウント(Administrator)	ドメインコントローラ	アカウントクエリ
RS01	全フォルダのアクセス権一覧	ファイルサーバ	サーバクエリ
RS02	全フォルダのアクセス権一覧［前回との差分］	ファイルサーバ	サーバクエリ
RS03	共有フォルダのアクセス権一覧	ファイルサーバ	サーバクエリ
RS04	重要フォルダのアクセス権一覧（※1）	ファイルサーバ	サーバクエリ
RP01	ハードウェアインベントリ	すべての対象サーバ	PC クエリ
RP02	コンピュータリソースの利用状況	すべての対象サーバ	PC クエリ
RP03	ディスク容量／残量一覧	すべての対象サーバ	PC クエリ
RP04	プロセス稼働状況	すべての対象サーバ	PC クエリ
RP05	サービス稼働状況	すべての対象サーバ	PC クエリ
RP06	ソフトウェアインベントリ	クライアント PC	PC クエリ
RP07	ライセンス管理対象 SW インストール状況（※1）	すべての対象システム	PC クエリ
RP08	保守対象 SW インストール状況（※1）	すべての対象システム	PC クエリ
RP09	ウィルス対策ソフトインストール状況（※2）	クライアント PC	PC クエリ
RP10	ウィルス対策ソフト稼働状況（※1）	クライアント PC	PC クエリ
RP11	Windows Update 実施状況（※3）	クライアント PC	PC クエリ

※1: お客様ご自身による若干の設定作業が必要になります。
※2: 次バージョンより搭載されるクエリテンプレートです。詳細はお問い合わせください。
※3: カスタマイズによる対応となりますので、別途お問い合わせください。

５．監査レポートの運用サイクル

監査レポートの作成頻度および保管期間は、下表のとおりとし、保管期間を経過した監査レポートは無条件で破棄を認める。

No	監査レポート	作成頻度	保管期間
A	**ALog ConVerter による監査レポート**		
A01	ユーザアカウントの作成／削除	月１回	３年間
A02	ユーザアカウントの有効化／無効化	月１回	３年間
A03	ユーザアカウントの変更	月１回	３年間
A04	グループアカウントの作成／削除	月１回	３年間
A05	グループアカウントの変更	月１回	３年間
A06	グループメンバの追加／削除	月１回	３年間
A07	ユーザアカウントの作成／パスワード設定	月１回	３年間
A08	ファイル／フォルダのアクセス権変更	月１回	３年間
A09	ログオン／ログオフ	月１回	３年間
A10	重要フォルダへのアクセス	月１回	５年間
A11	重要フォルダのファイル編集／削除	月１回	５年間
A12	土日のファイルアクセス	月１回	３年間
A13	夜間のファイルアクセス	月１回	３年間
A14	ログオン失敗	月１回	３年間
A15	書き込み・削除の失敗	月１回	３年間
A16	重要フォルダ内のファイル印刷(プリントサーバ)	月１回	３年間
A17	特権管理者アカウントによるファイル操作	月１回	３年間
A18	重要フォルダへのアクセス	月１回	３年間
A19	退職予定者のアクセス状況	月１回	３年間
D	**ALog ConVerter DB による監査レポート**		
D01	データベースユーザの追加／削除	月１回	３年間
D02	データベースユーザへの特権付与	月１回	３年間
D03	重要な情報システムのデータベース操作	月１回	５年間
D04	特権ユーザによるデータベース操作	月１回	３年間
D05	特定アプリケーション以外のテーブル操作	月１回	３年間

No	監査レポート	作成頻度	保管期間
R	Resource Athlete による監査レポート		
RA01	全ユーザアカウント一覧	半期に 1 回	3 年間
RA02	無効なユーザアカウント一覧	半期に 1 回	3 年間
RA03	一定期間利用されていないアカウント一覧	月 1 回	3 年間
RA04	一定期間パスワード未変更のアカウント一覧	月 1 回	3 年間
RA05	グループアカウントとグループ構成の一覧	半期に 1 回	3 年間
RA06	特権管理者アカウント一覧	半期に 1 回	3 年間
RA07	既定の管理者アカウント(Administrator)	半期に 1 回	3 年間
RS01	全フォルダのアクセス権一覧	半期に 1 回	3 年間
RS02	全フォルダのアクセス権一覧［前回との差分］	半期に 1 回	3 年間
RS03	共有フォルダのアクセス権一覧	半期に 1 回	3 年間
RS04	重要フォルダのアクセス権一覧	半期に 1 回	3 年間
RP01	ハードウェアインベントリ	週 1 回	1 年間
RP02	コンピュータリソースの利用状況	週 1 回	1 年間
RP03	ディスク容量／残量一覧	週 1 回	1 年間
RP04	プロセス稼働状況	週 1 回	1 年間
RP05	サービス稼働状況	週 1 回	1 年間
RP06	ソフトウェアインベントリ	半期に 1 回	3 年間
RP07	ライセンス管理対象 SW インストール状況	半期に 1 回	3 年間
RP08	保守対象 SW インストール状況	半期に 1 回	3 年間
RP09	ウィルス対策ソフトインストール状況	月 1 回	3 年間
RP10	ウィルス対策ソフト稼働状況	月 1 回	3 年間
RP11	Windows Update 実施状況	月 1 回	3 年間

■　監査基準

本章では前述のとおり、以下の IT 統制項目において組織が定めるべき管理策を列挙し、これらを監査における監査基準とする。

１．アカウント管理
２．アクセス権管理
３．証跡管理（ログ管理）
４．システム運用・保守管理
５．情報セキュリティ管理

１．アカウント管理

本章ではアカウント管理を以下のように区分し、それぞれの監査基準を記載する。

１－１　ユーザアカウント管理
１－２　グループアカウント管理
１－３　パスワード管理
１－４　特権管理

１－１　ユーザアカウント管理

ユーザアカウント管理は、ユーザアカウントの作成、変更、削除が定められた手続きに従って行われること、ユーザアカウントが常に適切な状態に保たれることを目的とする。

ユーザアカウント管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① ユーザアカウントの新規作成は、定められた手続きに従って実施すること。
② ユーザが退職により情報システムへアクセスする必要がなくなった場合は、速やかにユーザアカウントを削除すること。
③ ユーザが休暇や休職により長期（原則として一ヶ月以上）にわたって情報システムへアクセスしない場合は、速やかにユーザアカウントの利用を停止すること。
④ ユーザアカウントの作成、削除、停止に係る手続きは、適切な権限を持つ者（原則として情報システム管理者）が行うこと。
⑤ ユーザアカウントの権限の変更は、定められた手続きに従って適切な権限を持つ者（原則として情報システム管理者）が行うこと。
⑥ 長期間利用されていないユーザアカウントや、退職者のユーザアカウントなどが放置されないよう、ユーザアカウントを定期的に棚卸し、常に適切な状態に保つこと。
⑦ 停止されているユーザアカウントの必要性の有無を定期的に点検し、必要に応じ

て削除すること。

１－２　グループアカウント管理

グループアカウント管理は、グループアカウントの作成、変更、削除が定められた手続きに従って行われること、グループアカウントおよびそれを構成するユーザアカウントが常に適切な状態に保たれることを目的とする。

グループアカウント管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① グループアカウントの作成および削除は、適切な権限を持つ者（原則として情報システム管理者）が、定められた手続きに従って実施すること。

② ユーザの異動や退職によりグループアカウントの構成に変更が生じる場合は、速やかに変更を行うこと。

③ グループアカウントの作成、削除に係る手続きは、適切な権限を持つ者（原則として情報システム管理者）が行うこと。

④ グループアカウントを定期的に棚卸し、その構成および状況を適切な状態に保つこと。

１－３　パスワード管理

パスワード管理は、情報システムにアクセスするアカウントのパスワードが組織のパスワード要件（パスワードポリシー）を満たし、正しく運用されることを目的とする。

パスワード管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 新規に発行されたユーザアカウントには初期パスワードを付与すること。

② ユーザはパスワードを 90 日ごとに更新すること。

③ ユーザのパスワードが定期的に更新されているか点検し、未更新のユーザに更新の実施をアナウンスすること。

１－４　特権アカウント管理

特権管理は、特権が業務上必要最小限の範囲に限定して利用されること、特権を行使したユーザおよびその操作内容が把握できること、特権ユーザアカウントが一般のユーザアカウントと区別され厳重に管理されることを目的とする。

特権管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 特権ユーザアカウントは個人を識別できるものとし、システムの既定の特権ユーザアカウントを利用しないこと。
② 特権ユーザアカウントは、一般のユーザアカウントと重複しないアカウントとすること。
③ 特権ユーザアカウントを、特権を必要としない操作に利用しないこと。
④ 特権ユーザアカウントは、その発行数および利用者数をいつでも把握できる状態で管理すること。
⑤ 特権ユーザアカウントが不要になった場合は速やかに削除すること。
⑥ 重要な情報を保管するデータベース、特に財務報告に係るデータベースに特権ユーザアカウントを追加する場合は、適切な権限を持つ者（原則として情報システム管理者）が、情報システム責任者の承認を得たうえで行うこと。

２．アクセス権管理

本章ではアクセス権管理を以下のように区分し、それぞれの監査基準を記載する。

２－１　ファイル／フォルダアクセス権管理

２－１　ファイル／フォルダアクセス権管理

ファイル／フォルダアクセス権管理は、ファイル／フォルダアクセス権の付与および削除が定められた手続きに従って行われること、ファイル／フォルダアクセス権がユーザの業務内容や必要性に応じた適切な状態に保たれることを目的とする。

ファイル／フォルダアクセス権管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① ファイル／フォルダのアクセス権は、ユーザの業務の種類ごとに、必要な範囲に限定して付与すること。
② 重要なフォルダ、特に財務報告に係るファイルが保管されているフォルダのアクセス権は必要最低限のユーザにのみ付与すること。
③ ユーザが新たにファイル／フォルダのアクセス権を必要とする場合、定められた手続きに従って申請およびアクセス権の付与を行うこと。
④ ユーザに付与されているファイル／フォルダのアクセス権が、異動等によって不要不要になった場合、速やかにアクセス権を抹消すること。
⑤ ファイル／フォルダのアクセス権の付与および削除に係る手続きは、適切な権限を持つ者（原則として情報システム管理者）が行うこと。
⑥ ファイル／フォルダアクセス権は定期的に棚卸し、前回の棚卸結果との差異を考慮し、不要なアクセス権や、不適切なアクセス権等のチェックを行うこと。

３．証跡管理（ログ管理）

本章では証跡管理（ログ管理）を以下のように区分し、それぞれの監査基準を記載する。

３－１　アクセス履歴の管理

３－２　管理者操作履歴の管理

３－３　不正アクセスの監視

３－１　アクセス履歴の管理

アクセス履歴の管理は、アカウント管理およびアクセス権管理を含むアクセス制御の有効性評価に必要な記録の取得を目的とする。

アクセス履歴の管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 重要な情報資産に対するすべてのアクセスを継続的に記録すること。

② 重要な情報、特に財務報告に係るファイルの更新および削除を行う際は、その記録を残すこと。

③ ユーザアカウント認証の成功と失敗を記録すること。

④ 重要な情報を保管するデータベース、特に財務報告に係るデータベースに対する操作を継続的に記録すること。

３－２　管理者操作履歴の管理

管理者操作履歴の管理は、特権またはを行使したユーザおよびその操作内容を把握し、特権の取り扱いが適正であることを評価するために必要な記録の取得を目的とする。

管理者操作履歴の管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① ユーザアカウント、グループアカウントの権限を変更する場合は、その記録を残すこと。

② グループアカウントの構成を変更する場合は、その記録を残すこと。

③ ファイル／フォルダのアクセス権の付与および削除に関する操作を記録すること。

④ 重要な情報を保管するデータベース、特に財務報告に係るデータベースに対し特権を用いて実施した操作を記録すること。

３－３　不正アクセスの監視

不正アクセスの監視は、情報資産への不正アクセスを検出することを目的とする。

不正アクセスの監視において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 定期的にアクセス記録の点検を行い、不正アクセスの有無、異常アクセスの有無を確認すること。

② 認証に関するエラー、アクセスに関するエラーを点検し、不正なアクセスの有無を確認すること。

４．システム運用・保守管理

本章では、システム運用・保守管理を以下のように区分し、それぞれの監査基準を記載する。なお、本章には、システムの移行管理および構成管理に関する監査基準を含める。

４－１　ハードウェア管理

４－２　ソフトウェア管理

４－３　情報システムのモニタリング

４－１　ハードウェア管理

ハードウェア管理は、情報システムを構成するハードウェアが適切に維持管理されること、障害に備えた対策がなされていることを目的とする。

ハードウェア管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 情報システムを構成するハードウェアを識別し、その構成を管理すること。

② ハードウェアの構成に変更が生じた場合は、その変更内容を記録すること。

４－２　ソフトウェア管理

ソフトウェア管理は、業務に必要なソフトウェアが適切に維持管理されること、ソフトウェアの知的財産権が侵害されないことを目的とする。

ソフトウェア管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① ソフトウェアライセンスは適切に管理し、ソフトウェアの知的財産権を侵害しないこと。

② 保守の対象となるソフトウェアは、そのソフトウェアがインストールされている機器を明確に識別すること。

４－３　情報システムのモニタリング

情報システムのモニタリングは、情報システムの信頼性、安全性、効率性、有効性を確認するための記録の取得を目的とする。

情報システムのモニタリングにおいて監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 情報システムの稼働状況を定期的に点検し、異常なプロセス等の情報セキュリティインシデントの予兆または発生がないか確認すること。

② 情報システムを構成するコンピュータのリソースの状態を定期的に点検し、現状の容量や能力が十分であるか確認すること。

５．情報セキュリティ管理

本章では情報セキュリティ管理を以下のように区分し、それぞれの監査基準を記載する。

５－１　クライアントPCの利用管理

５－２　悪意ある攻撃への対策

５－３　情報の持ち出し管理

５－１　クライアントPCの利用管理

クライアントPCの利用管理は、ユーザが組織のネットワークに接続する端末においてセキュリティを保った運用を行うことを目的とする。

クライアントPCの利用管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① クライアントPCは、1日の業務終了後、ログオフすること。

② クライアントPCにあらかじめインストールされているソフトウェアを許可なく削除しないこと。

５－２　悪意ある攻撃への対策

悪意ある攻撃への対策は、コンピュータウィルスやクラッキング行為などの悪意ある攻撃からソフトウェアおよび情報の完全性を保護することを目的とする。

悪意ある攻撃への対策において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① ウィルスへの感染、拡大による被害を防ぐため、クライアントPCにウィルス対策ソフトをインストールすること。

② クライアントPCにインストールされたウィルス対策ソフトは常に動作を有効にすること。

③ クライアントPCのOSには常に最新のセキュリティパッチを導入すること。

５－３　情報の持ち出し管理

情報の持ち出し管理は、業務に係る情報資産がその価値に応じて適切に保護管理されることを目的とする。

情報の持ち出し管理において監査基準となる管理策は以下のとおりとし、監査においてこれらの遵守状況を評価する。

【管理策】

① 重要な情報の印刷は必要最低限に留め、印刷する場合はその記録を残すこと。

② 従業員の異動や退職、契約の変更または終了等の際、営業秘密および個人情報等の不正使用が起こらないよう適切な安全管理措置を取ること。

■　監査手順

本章では、前述した監査基準に基づいて、監査人が IT 統制の整備状況を監査する際の監査手順を詳述する。

はじめに、本章に記載する監査手順における項目について、下表のとおり解説する。

監査手順		
監査基準	章見出し	監査すべき事項が記載されている章、節、項等の番号および見出しを記載する。監査すべき事項とは、本書の「監査基準」において定義した管理策を指す。
	管理要求	監査すべき事項（管理策）を記載する。
監査手続き	監査レポート	監査の実施に用いる監査レポートの名称を記載する。 本書の「■定義　４．証跡となる監査レポート」に定めるレポート名およびレポート No に対応するものとする。
	前提条件	監査を実施するために、あらかじめ必要な情報、条件、定義等を記載する。
	確認項目	監査の具体的な実施手順や確認事項を記載する。
	評価基準	監査基準を満たしているか否かの評価基準を記載する。本章においては「適合」または「不適合」のいずれかとする。

以上の項目に従い、次頁より監査手順を詳述する。

１．アカウント管理

１－１　ユーザアカウント管理

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　①
	管理要求	ユーザアカウントの新規作成は、定められた手続きに従って実施すること。
監査手続き	監査レポート	A01 ユーザアカウントの作成／削除
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	新規ユーザアカウントの作成を実施したユーザアカウントが、すべて情報システム管理者のものであり、情報システム管理者でない者がユーザアカウントを作成していないことを確認する。
	評価基準	ユーザアカウントの作成を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　②
	管理要求	ユーザが退職等により情報システムへアクセスする必要がなくなった場合は、速やかにユーザアカウントを削除すること。
監査手続き	監査レポート	A01 ユーザアカウントの作成／削除
	前提条件	退職したユーザのユーザアカウントが識別でき、退職時期がわかること。
	確認項目	ユーザアカウントを削除した時期と、ユーザの退職時期が合致していることを確認する。 （サンプリング調査とする）
	評価基準	ユーザアカウントを削除した時期と、ユーザの退職時期が 合致する・・・・不適合 合致しない・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　③
	管理要求	ユーザが休暇や休職により長期（原則として一ヶ月以上）にわたって情報システムへアクセスしない場合は、速やかにユーザアカウントの利用を停止すること。
監査手続き	監査レポート	RA03 一定期間利用されていないアカウント一覧
	前提条件	（なし）
	確認項目	一ヶ月以上ログインしていないユーザアカウントが、正当な理由のあるものを除き、すべて無効にされていることを確認する。
	評価基準	一ヶ月以上ログインしていないユーザアカウントが 存在する・・・・不適合 存在しない・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　④
	管理要求	ユーザアカウントの作成、削除、停止に係る手続きは、適切な権限を持つ者（原則として情報システム管理者）が行うこと。
監査手続き	監査レポート	A01 ユーザアカウントの作成／削除 A02 ユーザアカウントの無効化／有効化
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	ユーザアカウントの作成、削除、停止を実施したユーザアカウントが、情報システム管理者のものであり、情報システム管理者でない者が操作をしていないことを確認する。
	評価基準	ユーザアカウントの作成、削除、停止を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　⑤
	管理要求	ユーザアカウントの権限の変更は、定められた手続きに従って適切な権限を持つ者（原則として情報システム管理者）が行うこと。
監査手続き	監査レポート	A03 ユーザアカウントの変更
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	ユーザアカウントの権限の変更を実施したユーザアカウントが、情報システム管理者のものであることを確認する。
	評価基準	ユーザアカウントの変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　⑥
	管理要求	長期間利用されていないユーザアカウントや、退職者のユーザアカウントなどが放置されないよう、ユーザアカウントを定期的に棚卸し、常に適切な状態に保つこと。
監査手続き	監査レポート	RA01 全ユーザアカウント一覧 RA03 一定期間利用されていないアカウント一覧
	前提条件	（なし）
	確認項目	ユーザアカウントの定期的な棚卸の実績があることを確認する。
	評価基準	ユーザアカウントの定期的な棚卸を 実施している・・・・適合 実施していない・・・不適合 ※以下をもって棚卸実施の実績とする ・監査レポートが定期的に出力されていること ・過去分の監査レポートが適切に保管されていること

監査手順		
監査基準	章見出し	１．アカウント管理 １－１　ユーザアカウント管理　⑦
	管理要求	停止されているユーザアカウントの必要性の有無を定期的に点検し、必要に応じて削除すること。
監査手続き	監査レポート	RA02 無効なユーザアカウント一覧
	前提条件	（なし）
	確認項目	停止されているユーザアカウントの定期的な点検の実績があることを確認する。
	評価基準	停止されているユーザアカウントの定期的な点検を 実施している・・・・適合 実施していない・・・不適合 ※以下をもって点検の実績とする ・監査レポートが定期的に出力されていること ・過去分の監査レポートが適切に保管されていること

１－２　グループアカウントの管理

監査手順		
監査基準	章見出し	１．アカウント管理 １－２　グループアカウントの管理　①
	管理要求	グループアカウントの作成および削除は、適切な権限を持つ者（原則として情報システム管理者）が、定められた手続きに従って実施すること。
監査手続き	監査レポート	A04 グループアカウントの作成／削除
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	グループアカウントの作成または削除を実施したユーザアカウントが、情報システム管理者のものであり、情報システム管理者でない者が操作を実施していないことを確認する。
	評価基準	グループアカウントの作成、削除を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－２　グループアカウントの管理　②
	管理要求	ユーザの異動や退職によりグループアカウントの構成に変更が生じる場合は、速やかに変更を行うこと。
監査手続き	監査レポート	A06 グループメンバの追加／削除
	前提条件	異動または退職したユーザのユーザアカウントが識別でき、異動時期または退職時期がわかること。
	確認項目	グループアカウントを変更した時期と、ユーザの異動または退職時期が合致していることを確認する。 （サンプリング調査可）
	評価基準	グループアカウントの変更時期とユーザの異動または退職時期が 合致する・・・・適合 合致しない・・・不適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－２　グループアカウントの管理　③
	管理要求	グループアカウントの構成または権限を変更する場合、適切な権限を持つ者（原則として情報システム管理者）が、変更の妥当性を確認した上で変更を行い、その記録を残すこと。
監査手続き	監査レポート	A05 グループアカウントの変更 A06 グループメンバの追加／削除
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	グループアカウントの構成の変更に関する記録の有無を確認し、その記録においてグループアカウントの構成の変更を実施したユーザアカウントが、情報システム管理者のものであることを確認する。
	評価基準	グループアカウントの構成の変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－２　グループアカウントの管理　④
	管理要求	グループアカウントを定期的に棚卸し、その構成および状況を適切な状態に保つこと。
監査手続き	監査レポート	RA05 グループアカウントとグループ構成の一覧
	前提条件	（なし）
	確認項目	グループアカウントの定期的な棚卸の実績があることを確認する。
	評価基準	グループアカウントの定期的な棚卸を 実施している・・・・適合 実施していない・・・不適合 ※以下をもって棚卸実施の実績とする ・監査レポートが定期的に出力されていること ・過去分の監査レポートが適切に保管されていること

１－３　パスワード管理

監査手順		
監査基準	章見出し	１．アカウント管理 １－３　パスワード管理　①
	管理要求	新規に発行されたユーザアカウントには初期パスワードを付与すること。
監査手続き	監査レポート	A07 ユーザアカウントの作成／パスワード設定
	前提条件	（なし）
	確認項目	ユーザアカウントの作成時にパスワードが設定されていることを確認する。
	評価基準	ユーザアカウントの作成と同時刻にパスワードの設定が 行われている・・・・適合 行われていない・・・不適合 ※ALog ConVerter は、新規に作成されたユーザにパスワードを付与した場合、ユーザアカウントの作成、パスワードの設定（Windows Server 2008 以降の場合は「パスワードリセット」となる）の２つのログが出力されるため、両方のログが同時に出力されていれば初期パスワードの付与とみなす。

監査手順		
監査基準	章見出し	１．アカウント管理 １－３　パスワード管理　②
	管理要求	ユーザはパスワードを 90 日ごとに更新すること。
監査手続き	監査レポート	RA04 一定期間パスワード未変更のアカウント
	前提条件	（なし）
	確認項目	現在有効なドメインユーザアカウントに、90 日以上パスワードを変更していないユーザアカウントが存在しないことを確認する。
	評価基準	パスワードを 90 日以上変更していないユーザアカウントが 存在する・・・・不適合 存在しない・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－３　パスワード管理　③
	管理要求	ユーザのパスワードが定期的に更新されているか点検し、未更新のユーザに更新の実施をアナウンスすること。
監査手続き	監査レポート	RA04 一定期間パスワード未変更のアカウント
	前提条件	（なし）
	確認項目	定期的にユーザアカウントのパスワード更新状況を点検している実績があることを確認する。
	評価基準	ユーザアカウントのパスワード更新状況の定期的な棚卸を 実施している・・・・適合 実施していない・・・不適合 ※以下をもって定期的な点検の実績とする ・監査レポートが定期的に出力されていること ・過去分の監査レポートが適切に保管されていること

１－４　特権管理

監査手順		
監査基準	章見出し	１．アカウント管理 １－４　特権管理　①
	管理要求	特権ユーザアカウントは個人を識別できるものとし、システムの既定の特権ユーザアカウントを利用しないこと。
監査手続き	監査レポート	RA07 既定の管理者アカウント（Administrator）
	前提条件	（なし）
	確認項目	すべての情報システムにおいて、既定の特権ユーザアカウントが利用できないよう、リネームまたは停止されていることを確認する。
	評価基準	システムの既定の特権ユーザアカウント名が 利用できる状態である・・・・不適合 利用できない状態である・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－４　特権管理　②
	管理要求	特権ユーザアカウントは、一般のユーザアカウントと重複しないアカウントとすること。
監査手続き	監査レポート	RA06 特権管理者アカウント一覧
	前提条件	一般業務に利用するユーザアカウント名が識別できること。
	確認項目	すべての情報システムにおいて、特権ユーザアカウントが与えられているユーザが、一般業務に利用するドメインユーザアカウントでないことを確認する。
	評価基準	特権ユーザアカウントにの中に、一般業務に利用するユーザアカウント名が 存在する・・・・不適合 存在しない・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－４　特権管理　③
	管理要求	特権ユーザアカウントを、特権を必要としない操作に利用しないこと。
監査手続き	監査レポート	A17 特権管理者アカウントによるファイル操作
	前提条件	（なし）
	確認項目	特権ユーザアカウントの操作履歴に通常業務の操作が含まれないことを確認する。
	評価基準	特権ユーザアカウントが通常業務に類する操作を 行っている・・・・不適合 行っていない・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－４　特権管理　④
	管理要求	特権ユーザアカウントは、その発行数および利用者数をいつでも把握できる状態で管理すること。
監査手続き	監査レポート	RA06 特権管理者アカウント一覧
	前提条件	（なし）
	確認項目	すべての情報システムにおいて、特権ユーザアカウントの台帳を作成していることを確認する。
	評価基準	特権ユーザアカウントの台帳を 作成している・・・適合 作成していない・・・不適合 ※監査レポートの出力をもって台帳の作成とみなす。

監査手順		
監査基準	章見出し	１．アカウント管理 １－４　特権管理　⑤
	管理要求	特権ユーザアカウントが不要になった場合は速やかに削除すること。
監査手続き	監査レポート	RA06 特権管理者アカウント一覧
	前提条件	不要な特権ユーザアカウントが識別できること。
	確認項目	すべての情報システムにおいて、不要な特権ユーザアカウントが含まれていないことを確認する。
	評価基準	不必要な特権ユーザアカウントが 存在する・・・・不適合 存在しない・・・適合

監査手順		
監査基準	章見出し	１．アカウント管理 １－４　特権管理　⑥
	管理要求	重要な情報を保管するデータベース、特に財務報告に係るデータベースに特権ユーザアカウントを追加する場合は、適切な権限を持つ者（原則として情報システム管理者）が、情報システム責任者の承認を得たうえで行うこと。
監査手続き	監査レポート	D01 データベースユーザの追加／削除 D02 データベースユーザへの特権付与
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	特権ユーザアカウントの作成または権限変更の作業が情報システム管理者によって実施されていることを確認する。併せてその際の手続き（承認、指示等）を確認する。
	評価基準	データベースの特権ユーザアカウントの作成または権限変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

２．アクセス権管理

２－１　ファイル／フォルダアクセス権管理

監査手順		
監査基準	章見出し	２．アクセス権管理 ２－１　ファイル／フォルダアクセス権管理　①
	管理要求	ファイル／フォルダのアクセス権は、ユーザの業務の種類ごとに、必要な範囲に限定して付与すること。
監査手続き	監査レポート	RS01 全フォルダのアクセス権一覧 RS03 共有フォルダのアクセス権一覧
	前提条件	ユーザの業務内容からアクセスするフォルダが識別できること。
	確認項目	各フォルダに業務に関係のないユーザへアクセス権が付与されていないことを確認する。 （サンプリング調査可）
	評価基準	各フォルダにアクセスする必要のないユーザが アクセス権を与えられている・・・・不適合 アクセス権を与えられていない・・・適合

監査手順		
監査基準	章見出し	２．アクセス権管理 ２－１　ファイル／フォルダアクセス権管理　②
	管理要求	重要なフォルダ、特に財務報告に係るファイルが保管されているフォルダのアクセス権は必要最低限のユーザにのみ付与し、その権限レベルを最小限に留めること。
監査手続き	監査レポート	RS04 重要フォルダのアクセス権一覧
	前提条件	重要なフォルダへのアクセスを許可されているユーザのユーザアカウントが識別できること。
	確認項目	重要なフォルダにアクセス権を持つユーザアカウントの権限レベルが、その業務内容に応じた適切な権限レベルであることを確認する。
	評価基準	重要なフォルダにアクセスできるユーザアカウントが 適切な権限レベルである・・・・・・・適合 必要以上の権限が与えられている・・・不適合

監査手順		
監査基準	章見出し	２．アクセス権管理 ２－１　ファイル／フォルダアクセス権管理　③
	管理要求	ユーザが新たにファイル／フォルダのアクセス権を必要とする場合、定められた手続きに従って申請およびアクセス権の付与を行うこと。
監査手続き	監査レポート	A08 ファイル／フォルダのアクセス権変更
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	ファイル／フォルダに対するアクセス権の変更が情報システム管理者によって実施されていることを確認する。
	評価基準	アクセス権の変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	２．アクセス権管理 ２－１　ファイル／フォルダアクセス権管理　④
	管理要求	ユーザに付与されているファイル／フォルダのアクセス権が、異動等によって不要不要になった場合、速やかにアクセス権を抹消すること。
監査手続き	監査レポート	RS01 全フォルダのアクセス権一覧 RS03 共有フォルダのアクセス権一覧
	前提条件	異動したユーザのユーザアカウントが識別できること。
	確認項目	人事異動があった部門の業務で利用するフォルダに、異動したユーザのアクセス権が残っていないことを確認する。 （サンプリング調査可）
	評価基準	調査対象となったフォルダにアクセスする必要のないユーザが アクセス権を与えられている・・・・不適合 アクセス権を与えられていない・・・適合

監査手順		
監査基準	章見出し	２．アクセス権管理 ２－１　ファイル／フォルダアクセス権管理　⑤
	管理要求	ファイル／フォルダのアクセス権の付与および削除に係る手続きは、適切な権限を持つ者（原則として情報システム管理者）が行うこと。
監査手続き	監査レポート	A08 ファイル／フォルダのアクセス権変更
	前提条件	情報システム管理者のユーザアカウントが識別できること。
	確認項目	アクセス権の付与および削除の作業が情報システム管理者によって実施されていることを確認する。
	評価基準	アクセス権の変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査手順		
監査基準	章見出し	２．アクセス権管理 ２－１　ファイル／フォルダアクセス権管理　⑥
	管理要求	ファイル／フォルダアクセス権は定期的に棚卸し、前回の棚卸結果との差異を考慮し、不要なアクセス権や、不適切なアクセス権等のチェックを行うこと。
監査手続き	監査レポート	RS01 全フォルダのアクセス権一覧 RS02 全フォルダのアクセス権一覧［前回との差分］ RS03 共有フォルダのアクセス権一覧
	前提条件	（なし）
	確認項目	ファイルサーバのフォルダ体系およびアクセス権を定期的に点検しているかを確認する。
	評価基準	アクセス権の定期的な棚卸を 実施している・・・・適合 実施していない・・・不適合 ※以下をもって棚卸実施の実績とする ・監査レポートが定期的に出力されていること ・過去分の監査レポートが適切に保管されていること

３．証跡管理（ログ管理）

３－１　アクセス履歴の管理

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－１　アクセス履歴の管理　①
	管理要求	重要な情報資産に対するすべてのアクセスを継続的に記録すること。
監査手続き	監査レポート	A10 重要フォルダへのアクセス
	前提条件	重要な情報が格納されているフォルダが識別できること。
	確認項目	重要な情報資産に対するアクセス履歴が保管されていることを確認する。
	評価基準	情報資産に対するアクセス履歴が 保管されている・・・・適合 保管されていない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－１　アクセス履歴の管理　②
	管理要求	重要な情報、特に財務報告に係るファイルの更新および削除を行う際は、その記録を残すこと。
監査手続き	監査レポート	A11 重要フォルダのファイル編集／削除
	前提条件	重要な情報が格納されているフォルダが識別できること。
	確認項目	重要な情報の更新および削除に関する記録が保管されていることを確認する。
	評価基準	重要な情報の更新および削除に関する記録が 保管されている・・・・適合 保管されていない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－１　アクセス履歴の管理　③
	管理要求	ユーザアカウント認証の成功と失敗を記録すること。
監査手続き	監査レポート	A09 ログオン／ログオフ
	前提条件	（なし）
	確認項目	ユーザアカウント認証の成功と失敗の記録が保管されていることを確認する。
	評価基準	ユーザアカウント認証の成功と失敗の記録を 保管している・・・・適合 保管していない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－１　アクセス履歴の管理　④
	管理要求	重要な情報を保管するデータベース、特に財務報告に係るデータベースに対する操作を継続的に記録すること。
監査手続き	監査レポート	D03 重要な情報システムのデータベース操作
	前提条件	（なし）
	確認項目	重要な情報を保管するデータベースに対する操作履歴が保管されていることを確認する。
	評価基準	重要な情報を保管するデータベースに対する操作履歴が 保管されている・・・・適合 保管されていない・・・不適合

３－２　管理者操作履歴の管理

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－２　管理者操作履歴の管理　①
	管理要求	ユーザアカウント、グループアカウントの権限を変更する場合は、その記録を残すこと。
監査手続き	監査レポート	A03 ユーザアカウントの変更 A05 グループアカウントの変更
	前提条件	（なし）
	確認項目	ユーザアカウント、グループアカウントの権限の変更に関する記録が保管されていることを確認する。
	評価基準	ユーザアカウント、グループアカウントの権限の変更の記録が 保管されている・・・・適合 保管されていない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－２　管理者操作履歴の管理　②
	管理要求	グループアカウントの構成を変更する場合は、その記録を残すこと。
監査手続き	監査レポート	A06 グループメンバの追加／削除
	前提条件	（なし）
	確認項目	グループアカウントの構成の変更に関する記録が保管されていることを確認する。
	評価基準	グループアカウントの構成の変更の記録が 保管されている・・・・適合 保管されていない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－２　管理者操作履歴の管理　③
	管理要求	ファイル／フォルダのアクセス権の付与および削除に関する操作を記録すること。
監査手続き	監査レポート	A08 ファイル／フォルダのアクセス権変更 RS02 全フォルダのアクセス権一覧［前回との差分］
	前提条件	（なし）
	確認項目	情報資産へのアクセス権の付与および削除に関する記録が保管されていることを確認する。
	評価基準	情報資産へのアクセス権の付与および削除の記録が 保管されている・・・・適合 保管されていない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－２　管理者操作履歴の管理　④
	管理要求	重要な情報を保管するデータベース、特に財務報告に係るデータベースに対し特権を用いて実施した操作を記録すること。
監査手続き	監査レポート	D04 特権ユーザによるデータベース操作
	前提条件	特権が付与されているデータベースユーザ名が識別できること
	確認項目	重要な情報を保管するデータベースに対する特権ユーザの操作履歴が保管されていることを確認する。
	評価基準	重要なデータベースへの特権を用いた操作の記録が 保管されている・・・・適合 保管されていない・・・不適合

３－３　不正アクセスの監視

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－３　不正アクセスの監視　①
	管理要求	定期的にアクセス記録の点検を行い、不正アクセスの有無、異常アクセスの有無を確認すること。
監査手続き	監査レポート	A12 土日のアクセス A13 夜間のアクセス A18 重要フォルダへのアクセス D05 特定アプリケーション以外のテーブル操作
	前提条件	（なし）
	確認項目	情報資産に対するアクセス記録を定期的に取得し、点検していることを確認する。
	評価基準	不正アクセス、異常アクセスの有無を 確認している・・・・適合 確認していない・・・不適合

監査手順		
監査基準	章見出し	３．証跡管理（ログ管理） ３－３　不正アクセスの監視　②
	管理要求	認証に関するエラー、アクセスに関するエラーを点検し、不正なアクセスの有無を確認すること。
監査手続き	監査レポート	A14 ログオン失敗 A15 書き込み・削除の失敗
	前提条件	（なし）
	確認項目	ユーザ認証のエラーに関する記録を定期的に点検していることを確認する。
	評価基準	ユーザ認証のエラーの記録を 確認している・・・・適合 確認していない・・・不適合

４．システム運用管理

４－１　ハードウェア管理

監査手順		
監査基準	章見出し	４．システム運用管理 ４－１　ハードウェア管理　①
	管理要求	情報システムを構成するハードウェアを識別し、その構成を管理すること。
監査手続き	監査レポート	RP01 ハードウェアインベントリ
	前提条件	（なし）
	確認項目	情報システムを構成するハードウェアが識別されており、そのインベントリが保管されていることを確認する。
	評価基準	情報システムを構成するハードウェアのインベントリが 保管されている・・・・適合 保管されていない・・・不適合

監査手順		
監査基準	章見出し	４．システム運用管理 ４－１　ハードウェア管理　②
	管理要求	ハードウェアの構成に変更が生じた場合は、その変更内容を記録すること。
監査手続き	監査レポート	RP01 ハードウェアインベントリ
	前提条件	システムのリプレース、増設等があった時期が識別できること。
	確認項目	情報システムを構成するハードウェアの構成情報が保管され、システムのリプレース、増設等があった時期に更新され、版管理されていることを確認する。
	評価基準	情報システムを構成するハードウェアのインベントリの履歴が 管理されている・・・・適合 管理されていない・・・不適合

４－２　ソフトウェア管理

監査手順		
監査基準	章見出し	４．システム運用管理 ４－２　ソフトウェア管理　①
	管理要求	ソフトウェアライセンスは適切に管理し、ソフトウェアの知的財産権を侵害しないこと。
監査手続き	監査レポート	RP07 ライセンス管理対象 SW インストール状況
	前提条件	ライセンス管理の対象となるソフトウェアが識別できること。
	確認項目	ライセンス管理の対象となるすべてのソフトウェアにおいて、そのソフトウェアがインストールされている機器の数が、ソフトウェアライセンスの購入数を上回っていないことを確認する。
	評価基準	ライセンス管理対象となるソフトウェアがインストールされている機器の数が 購入数以下である・・・・・適合 購入数を上回っている・・・不適合

監査手順		
監査基準	章見出し	４．システム運用管理 ４－２　ソフトウェア管理　②
	管理要求	保守の対象となるソフトウェアは、そのソフトウェアがインストールされている機器を明確に識別すること。
監査手続き	監査レポート	RP08 保守対象 SW インストール状況
	前提条件	保守対象となるソフトウェアが識別できること。
	確認項目	保守対象となるソフトウェアがインストールされている機器が識別できる状態であることを確認する。
	評価基準	保守対象となるソフトウェアがインストールされている機器が 識別できる・・・・適合 識別できない・・・不適合

４－３　情報システムのモニタリング

監査手順		
監査基準	章見出し	４．システム運用管理 ４－３　情報システムのモニタリング　①
	管理要求	情報システムの稼働状況を定期的に点検し、異常なプロセス等の情報セキュリティインシデントの予兆または発生がないか確認すること。
監査手続き	監査レポート	RP04 プロセス稼働状況 RP05 サービス稼働状況
	前提条件	（なし）
	確認項目	情報システムのサービスおよびプロセスの稼働状況が定期的に点検されていることを確認する。
	評価基準	情報システムのプロセスおよびサービスの稼働状況が 定期的に点検されている・・・・適合 定期的に点検されていない・・・不適合

監査手順		
監査基準	章見出し	４．システム運用管理 ４－３　情報システムのモニタリング　②
	管理要求	情報システムを構成するコンピュータのリソースの状態を定期的に点検し、現状の容量や能力が十分であるか確認すること。
監査手続き	監査レポート	RP02 コンピュータリソースの利用状況 RP03 ディスク容量／残量一覧
	前提条件	情報システムを構成するコンピュータが識別できること。
	確認項目	情報システムを構成するコンピュータのリソースが定期的に点検されていることを確認する。
	評価基準	情報システムを構成するコンピュータのリソースが 定期的に点検されている・・・・適合 定期的に点検されていない・・・不適合

５．情報セキュリティ管理

５－１　クライアントPCの利用管理

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－１　クライアントPCの利用管理　①
	管理要求	クライアントPCは、1日の業務終了後、ログオフすること。
監査手続き	監査レポート	A09 ログオン／ログオフ
	前提条件	（なし）
	確認項目	業務終了後にクライアント PC からログオフしていることを確認する。 （サンプリング調査可）
	評価基準	業務終了後にクライアントPCからログオフを 恒常的に実施している・・・・・・適合 実施していないことがある・・・・不適合

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－１　クライアント PC の利用管理　②
	管理要求	クライアント PC にあらかじめインストールされているソフトウェアを許可なく削除しないこと。
監査手続き	監査レポート	RP06 ソフトウェアインベントリ
	前提条件	クライアント PC にあらかじめインストールされているソフトウェアが識別できること。
	確認項目	クライアント PC にあらかじめインストールされているソフトウェアが許可なく削除されていないことを確認する。 （サンプリング調査可）
	評価基準	クライアント PC にあらかじめインストールされているソフトウェアを削除している PC が 存在する・・・・不適合 存在しない・・・適合 ※正当な理由があり許可を得て削除したものについては適合とする。

５－２　悪意ある攻撃への対策

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－２　悪意ある攻撃への対策　①
	管理要求	ウィルスへの感染、拡大による被害を防ぐため、クライアント PC にウィルス対策ソフトをインストールすること。
監査手続き	監査レポート	RP09 ウィルス対策ソフトインストール状況
	前提条件	組織内で利用されているウィルス対策ソフトが識別できること。
	確認項目	ウィルス対策ソフトがインストールされていないクライアント PC が無いことを確認する。
	評価基準	ウィルス対策ソフトが インストールされている・・・・適合 インストールされていない・・・不適合

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－２　悪意ある攻撃への対策　②
	管理要求	クライアント PC にインストールされたウィルス対策ソフトは常に動作を有効にすること。
監査手続き	監査レポート	RP10 ウィルス対策ソフト稼働状況
	前提条件	ウィルス対策ソフトのプロセスが識別できること。
	確認項目	ウィルス対策ソフトが稼働していないクライアント PC が無いことを確認する。 （サンプリング調査可）
	評価基準	すべてのクライアント PC においてウィルス対策ソフトが 稼働している・・・・適合 稼働していない・・・不適合 ※正当な理由があり動作を停止しているクライアント PC は評価対象外とする。

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－２　悪意ある攻撃への対策　③
	管理要求	クライアントPCのOSには常に最新のセキュリティパッチを導入すること。
監査手続き	監査レポート	RP11 Windows Update 実施状況
	前提条件	セキュリティパッチの導入を Windows Update によって実施していること。
	確認項目	すべてのクライアントPCの Windows Update の最終実行日が、一定期間（原則として１か月）以内であることを確認する。
	評価基準	すべてのクライアントPCにおいて Windows Update が １か月以内に実施されている・・・・適合 １か月以上実行していない・・・・・不適合 ※正当な理由があり Windows Update を実施していないクライアントPCは評価対象外とする。

５－３　情報の持ち出し管理

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－３　情報の持ち出し管理　①
	管理要求	重要な情報の印刷は必要最低限に留め、印刷する場合はその記録を残すこと。
監査手続き	監査レポート	A16 重要ファイルの印刷
	前提条件	重要な情報に関するファイルが特定できること。
	確認項目	重要な情報の印刷に関する記録が保管されており、記録上において必要以上に印刷行為が行われていないことを確認する。
	評価基準	重要な情報の印刷が 必要最低限である・・・・・・適合 必要以上に行われている・・・不適合

監査手順		
監査基準	章見出し	５．情報セキュリティ管理 ５－３　情報の持ち出し管理　②
	管理要求	従業員の異動や退職、契約の変更または終了等の際、営業秘密および個人情報等の不正使用が起こらないよう適切な安全管理措置を取ること。
監査手続き	監査レポート	A19 退職予定者のアクセス状況
	前提条件	（なし）
	確認項目	従業員の異動や退職、契約の変更または終了にあたって組織が実施している対策を確認し、その妥当性を評価する。
	評価基準	監査レポートが退職予定者等の不正行為を 監視できるものである・・・・適合 監視できない・・・・・・・・不適合

■　監査証跡

----- 本章には、「■定義」に定めるレポートを、監査証跡として添付する -----