株式会社グラフィック

□ 原　　本
■ 管 理 版（管理 No.　　002）
□ 非管理版

| 承　認 | 作　成 |
|---|---|
| 個人情報保護管理者 | 事務局 |
| 伊東 | 角田 |
| 2019 年 7 月 1 日 | 2019 年 7 月 1 日 |

# 個人情報保護安全対策基準

## 第 1.0 版

2019 年　7 月　1 日制定

改訂履歴

| 版 | 作成／改訂年月日 | 内容 |
|---|---|---|
| 1.0 | 2019年 4月 1日 | ・新規作成 |

# 個人情報保護安全対策基準　目次

## 第1章　基本事項

### 第1条　目的

1．本基準は、「個人情報保護基本規程」A.3.4.3.2 の要求に従い、JIS 規格附属書 C（参考）に則り、個人情報の安全管理のために必要、かつ、適切な措置を定めることを目的とする。

### 第2条　用語の定義

1．本基準における用語の定義は、本基準の項目内において定めるもののほか、「個人情報保護基本規程」による。

## 第2章　物理的安全対策

### 第3条　物理的領域の設定（C.11.1）

1．目的

当社の施設を保護するために、物理的セキュリティ領域を定める。

2．管理策

（1）領域

敷地内の屋外ゾーンや来訪者が入場するゲストゾーン以外は機密領域とする。

敷地、建物を含む使用する領域について、セキュリティレベルを設定し、各事業所の建物図面に表示する。

セキュリティレベルは、以下の通りとする。

① レベル 1（屋外ゾーン）

屋外敷地（従業者、警備員等の監視下にある不特定の第三者が入場する領域）

② レベル 2（ゲストゾーン）

応接室、ロビー、ショウルーム（従業者、及び一定の手続きを経た第三者が入場する領域）

③ レベル 3（従業者共用ゾーン）

従業者の執務室（全ての従業者の入場を許可する領域）

④ レベル 4（ワークゾーン）

個人情報の印刷・プリンタ出力・加工、人事情報・取引先の個人情報取扱い等を行う領域（特定の従業者が入場する領域）

⑤ レベル 5（ハイセキュリティゾーン）

個人情報の電算処理領域、経理室（特定の従業者が入場する領域）

※レベル 3 ～ 5 を機密領域とする。

（2）領域境界

① 屋外との境界となる壁や窓は、物理的に頑丈なものとし、権限の無い者が容易に侵入できないようにするとともに、ドアには、セキュリティカード制御等による入退制御装置を備え、入退管理をする。

② 敷地外との境界には、物理的な境界壁（塀）を設置し、不審者が侵入できないようにする。また、防犯用の監視カメラを設置し、監視する。

### 第4条　入退管理（C.11.1）

1．目的

領域は、認可された者だけにアクセスを許すことを確実にするために、入退管理策によって保護する。

2．管理策

機密領域では、セキュリティカード等による入退制御装置を備え、入退管理をする。

（1）従業者の入退管理

① 全ての従業者に、目に見える証明書（社員証）の常時携行･明示を義務付ける。

② 機密領域内のセキュリティレベルの高い領域（室）に入退室する場合は記録をとるものとし、当該領域の入退室の記録は、定期的に確認する。

③ 入室できる従業者の権限設定は、人事異動、新規採用、退職、役割変更等の発生の都度、部門長が速やかに変更する。また退職時には、IC カードを速やかに、総務部に返却する。

④ 入室できる従業者の権限設定は、各室毎に定期的に見直す。

（2）来訪者

① 屋外とゲストゾーンとの境界には、有人受付、インターホン受付等の受付機能を設置する。

② 機密領域に入る来訪者の受付を行い、会社名、氏名、日付、時刻を「御来社受付カード」に記録する。

③「御来社受付カード」は、単票（1 件 1 葉）方式とする。

④「御来社受付カード」は、1 年間保存する。

⑤ 来訪者には、「ゲストカード」若しくは「ゲスト腕章」の携行･明示を依頼する。

⑥ 総務部門部門長は、来訪者の受付記録を定期的に確認する。

**【関連様式】**「御来社受付カード（pms-09-04)」

## 第 5 条　施設管理（C.8.1、C.11.1、C.11.2、C.17.2）

1．目的

執務室、工場等の施設に対する認可されていないアクセスや、環境上の脅威及び災害からのリスクを低減化した物理的セキュリティを設定し、管理、運用する。

2．管理策

（1）執務室

① クライアント端末等の機器は、情報システム責任者の許可を得て設置する。

② 無人となるエリアに設置したノート PC その他可搬機器は、盗難を防止するため、ワイヤーロック又は不使用時は施錠保管する。

③ 机上には書類等を放置せず、整理･整頓･クリアデスクを励行する。

（2）サーバ室

① サーバ室は常時施錠し、鍵は総務部部門長及びジタルメディア部部門長が管理する。

② サーバや通信機器等の機器は、情報システム責任者の確認の上、各部門長の許可を得て設置する。

③ サーバ、NAS、通信機器等はラック内に設置し、ケーブル類は、損傷、妨害等から保護する。

④ ラック内の設置が難しい場合は、盗難防止措置を講じた上、他の一般機器と混在、混同しない場所に設置し、機器の管理者を表示する。

⑤ サーバ室に入退室する場合は記録をとり、情報システム責任者が管理する。入退室の記録はデジタルメディア部部門長が定期的に確認する。

⑥ 機器類に関しては、可用性･完全性の維持を確実にするために、定期的に保守を実施する。

（3）工場･作業場所

① 室内は、出来るだけゆとりのある空間で、死角がないようにする。

② 材料、仕掛品、製品が一目で判別できるようにする。

③ 室内は、整理･整頓する。

（4）荷受･搬出搬入場所

① 荷物の受渡し場所は、屋内の決められた場所とし、屋外での受渡しは不可とする。

② 荷受・搬出搬入場所が無人となる場合は施錠する。

③ 荷物の受渡し場所から、別の場所に荷受物を移動する際は、盗難・紛失等の防止対策をとる。

（5）災害に対する保護対策

① 火災対策としては、消火器を各所に設置する。

② 水害対策としては、情報機器類の近くには水回り設備を避け、水漏れ等の被害を受けないようにする。エアコン等の空気吹き出し口からの水滴等にも配慮する。

③ 停電対策としては、サーバ等に無停電電源装置（UPS）を設置する。

④ 地震対策としては、情報機器を設置した机や、情報機器を格納したラックには可能な限り転倒防止策をとる。

（6）盗難等に対する保護対策

① 入退監視カメラ

・各執務室の出入口には入退監視カメラを設置し、常時録画し適宜監視する。

・画像は、個人を識別できるレベルの鮮明さとし、総務部部門長が管理する。

・不正入室の抑止効果が期待でき、盗撮とならないように撮影場所に監視カメラ作動中の表示をする。

② 社内の撮影等

・社内においては、部門長の事前承認なく、撮影、録画、録音等を行ってはならない。また、これらの映像、音声等を無断で使用してはならない。

## 第6条　授受管理（C.8.1、C.8.3、C.13.2）

1．目的

個人情報を記録した媒体への認可されていないアクセスや不正使用、若しくは紛失等を防止する。

2．管理策

（1）委託元又は提供元との授受

① 個人情報を記録した媒体（紙媒体、電子媒体）を顧客等から受け取る場合は、「個人情報お預り証」に、媒体・数量・件数、取得に関する合意等の記録を残す。

② 受領する電子媒体に記録したファイルの暗号化やパスワードロック等の秘匿化措置を、委託元又は提供元に依頼する。

③ 個人情報の重要度に応じて、適切な運搬手段（社用車、宅配便、宅配セキュリティ便等）を用いる。

④ 社外で受領した媒体の移送時は、封筒・ファイル等に入れ、施錠可能なカバン等で肌身離さず持ち運ぶ。

⑤ 業務終了後までに、預かった媒体は、受取り時と同様の運搬手段・方法で顧客に返却し、「個人情報お預り証」で返却の授受記録を残す。

（2）委託先との授受

① 個人情報を記録した媒体（紙媒体、電子媒体）を委託先に受け渡す場合は、「個人情報お預り証」に準じた授受記録、並びに返却、消去及び廃棄等の指示記録を残す。

② 受け渡す電子媒体に記録したファイルの暗号化等の秘匿化やパスワードロックの措置を実施する。

③ 個人情報の重要度に応じて、適切な運搬手段（社用車、宅配便、宅配セキュリティ便等）を用いる。

**【関連様式】**「個人情報お預り証（委託・提供される場合）（pms-08-07）」
「個人情報授受記録（委託・提供する場合）（pms-09-06）」

## 第7条　保管管理（C.14.3）

1．目的

媒体等への認可されていないアクセスや盗難・紛失のリスクを低減化し、保護する。

2．管理策

（1）入稿媒体

① 紙媒体や記録媒体（USB メモリ、CD-R 等）等の顧客から預かった個人情報を記録した入稿媒体は、施錠保管し、鍵の管理は、部門長が行う。

（2）納品物

① 個人情報を印刷した製品等の顧客への納品物は、納品まで、施錠保管し、鍵の管理は、部門長が行う。

② 施錠保管が難しい場合は、記載された個人情報が見えない措置をとる。

（3）廃棄物

① 個人情報を含むヤレ紙は、個人情報を含まないものと識別し、廃棄業者にて処分するまでヤレ籠に保管する。鍵の管理は、部門長が行う。

### 第8条　廃棄管理（C.8.3、C.11.2、C.14.3）

1．目的

機器・媒体等は廃棄・返却される前に、全ての個人情報を消去していることを確実にする。また個人データを保管する必要がなくなったときは、当該個人データを遅滞なく消去する。

2．管理策

（1）HDD 等の記憶機器

① 完全消去ソフトによるデータ消去を行い、復元できない状態にしてから廃棄する。又は、業者に消去・廃棄を依頼し消去・廃棄証明書を受領する。若しくは物理的破壊を実施する。

（2）媒体

① 個人情報を記録した紙媒体を廃棄する場合は、シュレッダー等で粉砕処理して廃棄する。

② 個人情報を含むヤレ紙は、委託先の評価を行い、委託契約を行った専門業者に処分を委託する。若しくは、ヤレ紙は断裁し、個人情報が確認できない状態で一般廃棄物として廃棄する。個人情報を含むヤレ紙を処理又は廃棄までの間、構外に置く場合は、設置場所・籠の施錠管理を行う。

③ 記録媒体（USB メモリ、CD-R 等）は、メディアシュレッダー等で物理的に破壊し、再利用不可能にした状態で廃棄する。

④ 廃棄する際は、廃棄・消去の記録を取り、3年間保管する。

（3）リース・レンタル機器

① リース・レンタル期間終了等により、システム機器を業者に引き渡す場合は、完全消去ソフトによってデータ消去し、復元できない状態にしてから引き渡す。

② 故障等で情報の消去が行えない場合、機密データが流出・漏えいしないよう、機密保持契約等の覚書を締結した後に引き渡す。

（4）保管期間を過ぎた個人データ

① 保管期間を過ぎ、保管する必要がなくなった個人データは、消去した証跡が残る方法で、速やかに消去する。

## 第3章　技術的安全対策

### 第9条　情報システムの構築（C.12.1）

1．目的

個人情報を含むデータを処理する情報システムは、認可されていないアクセスや不正使用を排除し、適切

に利用できるように構築し、資産として管理する。

また、機器及び環境を、正確かつセキュリティを保った手順で運用する。

2．管理策

（1）管理体制

① 情報システム責任者は、社長及び個人情報保護管理者の承認を受け、情報システムの設計、設定、管理、運用を行い、情報システムの運用管理に関する指示、通達等を行う。

② 情報システム責任者は、情報システムのネットワークを含む構成図を作成し、維持する。

（2）システム運用

① 情報システム責任者は、サーバ、端末及び電子媒体等の設置場所、台数、仕様、業務責任者、システム利用者を記録及び管理し、必要に応じて、利用状況、電子機器の所在を確認し、「情報システム機器管理台帳」に記載して管理する。

② 情報システム責任者は、長期間利用しない、又は当面業務に必要でないサーバ、端末、ネットワーク等は社内ネットワークから隔離する。

③ 情報システム責任者は、従業者が情報システムやパソコン等の機器を適切に取り扱えるようにするため、各部門長と協力して必要に応じて OJT 等を実施する。

④ 第三者が提供するサービス（外部サーバやクラウドサービス）を利用する場合は、当該部門が情報システム責任者に申請を行い、情報システム責任者がサービス内容の安全性を審査した上で、個人情報保護管理者が承認を行う（委託先評価は「個人情報保護取扱基準」による）。また、受託業務でこれらのサービスを利用する場合は、必要に応じ事前に委託元の了解を得る。

⑤ 操作手順は文書化し、必要とする全ての利用者に対して利用可能にする。

⑥ 機器や環境、システム等の変更に関して、変更管理を実施する。

⑦ 容量･能力管理を実施し、運用を確実にするために、機器やシステム等の利用状況を監視･調整する。また、将来必要とする容量･能力を予測する。

⑧ 業務システム等の開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために環境分離する。

## 第１０条　ネットワーク管理（C.10.1、C.12.6、C.13.1、C.13.2、C.14.1）

1．目的

コンピュータネットワーク環境が安全かつ安定して稼動し、利用を許可したネットワーク及びネットワークサービスへのアクセスの利用者への提供を確実にする。

2．管理策

（1）ネットワーク接続

① 通信回線を経由して社内ネットワークをインターネットと接続する場合、情報システム責任者は、利用するファイアウォール、ルータ及びサーバ等の機器の設定に際し、機密性、完全性及び可用性を確保する。

② 個人情報を取り扱う情報システムへの外部からのアクセスを記録･保管し、定期的に監視する。

（2）インターネット･電子メール利用

① 従業者は、業務上の理由により、インターネット･電子メールの利用環境を必要とする場合は、業務責任者を通じて、情報システム責任者の許可を得て利用する。

② 従業者は、インターネット･電子メールを業務の用途以外に使用しない。

③ 業務責任者は、従業者の退職･異動等により当該従業者の利用アドレスが不要になったと判断した場合、速やかに総務部へ利用停止を申し出る。総務部より連絡を受けたデジタルメディア部は、利用停止の処

置を行う。

④ 情報システム責任者は、定期的な利用アドレスの棚卸によって、第三者による不正利用を防止する。

⑤ 従業者は、不正アクセスやウイルスの伝搬等によって、情報システムの安全を脅かす、危険な Web サイト、ダウンロードファイル、電子メール、添付ファイルが存在することを認識し、不審と感じた場合には、それらを不用意に開いたり閲覧したりしない。

⑥ 従業者は、電子メール等インターネットの使用時に、情報システムに対する侵入又はそのおそれを発見した場合、クライアント端末をネットワークから切り離した上で、速やかに所属部門長並びに情報システム責任者に報告し、指示を仰ぐ。

⑦ 従業者は、電子メールを送信する際には、誤送信を防ぐために、以下を実施する。

・会社指定のメールソフトを使用する。
・送信先アドレスや To、Cc、Bcc の選定が正しいことを確認する。
・添付ファイルが正しいことを確認する。
・添付ファイルは暗号化やパスワードロックをし、パスワードは添付ファイルを送信するメールとは別の手段で通知する。

（3）その他利用

① 無線 LAN

・無線 LAN 接続は許可制であり、以下のクライアント端末が許可される。
- 支給時に情報システム責任者が必要と判断したクライアント端末。
- 情報システム責任者の許可を受けた既設クライアント端末。

・情報システム管理担当者が接続設定を行い（ユーザにはアクセスキーには教えない）、ユーザ自身でアクセスポイントへの接続は行わせない。
・アクセスポイントでは、WPA2 以上での暗号化を設定し、アクセスキーは情報システム責任者の判断で変更を行う。

② ファイル転送サービス

・委託元や委託先との間で、データの授受を行う場合、ファイルの暗号化措置を行うなど、情報システム責任者が安全性を確認した上で、委託元や委託先と合意をとり、必要な対策をとる。

③ リモートアクセス

・社外からのリモートアクセスの利用には、申請と情報システム責任者の許可が必要である。申請の項目は以下の通りとする。
- 申請日
- 利用開始日（及び期限）
- 利用者所属部門
- 接続先ホスト
- 利用者名
- 利用目的
- 利用場所
- 部門長の承認

※利用者が社員以外（業者など）の場合は、秘密保持契約の締結を行い、上記申請はその部門責任者が行う

・リモートホスト（接続先）は、接続記録（ログ）が保存されなければならない。接続記録には、以下の項目が必要である。
- 接続成功
- 接続時のアカウント名
- 接続失敗
- 発信者識別
- 接続の開始時間と終了時間
- 障害情報（エラー情報）

・リモートホスト（接続先）は、上記記録（ログ）及びホストのデータが定期的に複製保存（バックアップ）されていなければならない。
- 接続記録：1 分ごとに複製を更新
- データ：原則として 1 日 1 回以上

④ 個人情報の取得

・ホームページを用いて個人情報を取得する場合、クロスサイトスクリプティング（XSS）対策、SQLインジェクション対策等の脆弱性への対策を実施する。また、SSL 等の通信経路の暗号化等についても、情報システム責任者が安全性を確認した上で使用する。

⑤ SNS の利用

・従業者は、ツイッターやフェイスブックなどのソーシャルメディアの利用に当たっては、発言や投稿の内容によって、本人への非難にとどまらず当社の社会的信頼を損なう場合があることを認識し、以下の点に注意して適切に利用する。

- 業務上知り得た情報を書き込まない。
- モラルを逸した内容の情報を書き込まない。
- 発言や投稿に対して非難が集中した場合、速やかに業務責任者を通じて情報システム責任者へ報告する。

（4）ぜい弱性管理

① サービス開始前に本番環境での脆弱性スキャンを実施し、脆弱性が残存していないことを管理者に報告し、承認を得た後、サービス担当へリリースする。

② システムに追加修正を行った際、アップロード前に脆弱性スキャンを実施し、脆弱性が残存していないことを管理者へ報告し、承認を得た後、アップロードを行う。

③ IPS にて不要なポートを閉じ、アクセスの制限を行う。

④ EC サイトのユーザパスワードはハッシュ化を行い、万が一の流出に備えるとともに、複雑化させて総当たり攻撃を防ぐ。

## 第１１条　機器・端末の利用（C.6.2、C.8.3、C.9.3、C.9.4、C.11.2）

1．目的

情報機器・端末の利用に当たっては、利用者管理を確実に行い、認可された者だけのアクセスを許すように保護する。

2．管理策

（1）ユーザ ID 管理

① 総務部は、従業者の新規ユーザ ID 発行要請があった場合には、その従業者が所属する部門長の承認を得ていることを確認した上で、申請を受け付ける。

② 総務部は、申請の内容を確認し承認した後に、当該ユーザ ID とパスワードを発行する。

③ 部門責任者は、従業者が、異動・休職・退職等によりその職務権限が失われた場合、総務部に利用資格を喪失したユーザ ID を、削除又は無効とするよう連絡し、総務部は速やかに削除又は無効処理し、その内容を記録する。

④ 総務部は、ユーザ ID を付与した従業員管理台帳を管理し、定期的に業務責任者へユーザ ID 付与者の適正を確認し、維持する。

（2）パスワード管理

① 発行を受けたユーザ ID は、そのパスワードを守秘し、第三者に利用されないようにする。

② 総務部が発行したパスワードは、以下の手順で管理を行う。

・パスワードは、容易に推測されない 8 文字以上の英数で設定する。

・パスワードには、英文字、数字を混在させる。

・パスワード入力時に、第三者に見られないように注意する。

・パスワードをメモしたものを机上、クライアント端末及び該当機器等に表示しない。

・パスワードの漏えい等がないように各自で管理する。

（3）クライアント端末の利用

① デジタルメディア部にて、クライアント端末の初期設定をした後、従業者にクライアント端末を貸与する。

② 初期設定に当たっては､パスワードを設定したスクリーンセーバー（起動時間 15 分以内）設定及び OS 等の基本ソフトウェアの自動更新を実施する設定を有効にする。

③ 利用者は、長時間離席する場合は、シャットダウンやログオフする等の方法で、クライアント端末の機密性を確保する。

④ また、終業時や休日、祝日、長期休暇時には必ずクライアント端末の電源を切る。クライアント端末を長期間利用しない場合は、ネットワークから切り離しておく等の措置を実施する。

⑤ 利用者は、クライアント端末の紛失･破損･障害等が発生した場合、速やかに各部門長若しくはデジタルメディア部に連絡し、指示を仰ぐ。

⑥ 利用者は、共有ファイルが見られない、メールが使用できない、ホームページの閲覧ができない等、ファイルサーバ、Web・メールサーバ等が原因と思われる障害、コンピュータウイルスを発見したときは、速やかにデジタルメディア部に連絡し指示を仰ぐ。

⑦ セキュリティレベル2のエリアに設置されたノートPCやクライアント端末に接続する外付けハードディスクには、ワイヤーロックや退社時にキャビネットに施錠保管をする等の盗難防止対策を実施する。

（4）FAX の利用

① 個人情報の送信には FAX を利用しない。

② 利用者は、FAX にて資料等を送信する場合、誤送信を防ぐために、以下の措置を実施する。

・送信頻度の高い宛先は短縮登録を行う。（登録時には宛先番号を確認する）

・送信時に宛先を 2 度確認する。

③ 受信された FAX は、担当がわかる状態であれば担当に渡し、担当がいない若しくは宛先がわからない FAX は保管 BOX に収容する。保管 BOX 内の書類は、2 日間保管の後、廃棄する。

（5）携帯電話、スマートフォン、タブレットの利用

① 会社貸与の携帯電話、スマートフォン、タブレットは、業務上必要な範囲に限り使用し、以下の措置を実施する。

・安全対策として、パスコードロックの実施を行う。

・充電等であっても、会社のクライアント端末の USB ポートに接続することを厳禁する。

・盗難、紛失の場合は速やかに総務部（携帯電話、スマートフォン）若しくはデジタルメディア部（タブレット）に連絡し、回線の停止と遠隔ロックの措置をとる。

・スマートフォン、タブレットを使用する場合は MDM を導入し、OS は原則最新のバージョンを適用する。

（6）記録媒体の利用

① USB メモリ、CD-R、メモリーカード等の記録媒体は、会社支給のものを使用する。

② 社外とのやり取りがある USB メモリ等の記録媒体は、使用後は速やかにデータを消去する。管理担当者は定期的に棚卸をし、利用状況を確認する。

（7）社外へのノート PC 持出し利用

① ノート PC の社外持出しは、原則禁止とする。

② 業務上やむを得ない事情がある場合は、以下の措置を実施する。

・持ち出す際は、事前に使用するノート PC や周辺機器、使用者名、使用期間、使用目的につき、所属

部門長の承認を得て、情報システム責任者へ申請し許可を受ける。

・使用者は、持ち出したノートPCが盗難されないよう、気を配り、電車等の網棚にのせたり、社用車に放置したりすることなく、自分の身から離さないようにする。また、酒席へ持ち込むことのないようにする。

・使用者は、持ち出すノートPCに保管する情報を必要最小限とし、原則として機密データは保管しない。リスクを分散するため、機密データは周辺機器に保管することを原則とし、持ち出すノートPCに機密データを保管する必要がある場合は、機密データの漏えいを防ぐため、暗号化やアクセス制御等の対策を講じる。

・使用者は、持ち出したノートPCにおける機密データの使用を、必要最小限にとどめる。

・使用者は、社外のネットワークへの接続を行わない。

## 第１２条　情報のアクセス管理（C.9.1、C.9.2、C.9.3、C.9.4）

１．目的

システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止する。

２．管理策

（1）情報システム管理

① 情報システム責任者は、個人情報にアクセスする者の登録を行う作業担当者（アクセス登録作業者）を任命し、登録作業を行う権限を付与する。アクセス登録作業者台帳を管理し、作業担当者の適正を確認し、維持する。

② 業務責任者は個人情報を取り扱う情報システムへのアクセスを必要最小限にする。

③ 情報システム責任者は、業務責任者より情報システムへのアクセス者登録の申請を受け、アクセスの必要最小限を審査・承認し、アクセス者登録台帳を作成し、アクセス登録作業者に登録を指示する。アクセス登録作業者は指示に従い登録作業を実施する。

④ 情報システム責任者は、アクセス登録作業者からの登録完了の報告を受け、承認したアクセス者のみ登録されていることを確認する。

⑤ 情報システム責任者は、システムへのアクセス者登録台帳を管理し、定期的に登録者の適正を確認し、維持する。

（2）利用者

① クライアント端末には原則として機密データは保管せず、アクセス制限が設定された共有ファイルサーバに保管する。

② アプリケーション、サービス、IT資産、情報システムへのアクセスに際しては、業務上必要な利用の範囲で行う。

## 第１３条　ソフトウェア管理（C.9.4、C.12.5、C.12.6）

１．目的

情報システムで使用するソフトウェアは、システムの完全性を確実にするために、ソフトウェア導入を管理する手順を実施する。

２．管理策

（1）ソフトウェア導入

① デジタルメディア部は、所有するアプリケーション・ソフトウェア及びライセンス証書を管理し、そのソフトウェアをインストールする。

② 情報システム責任者は、クライアント端末管理台帳を作成し維持する。また所有するライセンスのソフトウェアをインストールしたインストール台帳を作成し、維持する。クライアント端末毎に所有するライセンス以上にインストールされていないことを点検し、不適切なインストールがあった場合は速やかに是正する。

（2）ソフトウェア利用

① 利用者は、情報システム責任者の指定するソフトウェアを使用する。

② ファイル交換ソフトウェア等の情報システム責任者が許可していないソフトウェア（Winny、Share等）の使用は禁止する。

③ 指定外のソフトウェアを使用する場合は、情報システム責任者に申請し、許可を得てから使用する。

④ 利用者は、使用しないソフトウェアをシステム担当者に返却する。

⑤ ライセンスのないソフトウェアの使用、会社ソフトウェアの私的利用、私有ソフトウェアの利用は禁止する。

## 第１４条　ウイルス対策管理（C.12.2）

１．目的

データや情報システムが、ウイルスから保護されることを確実にする。

２．管理策

（1）ウイルス対策ソフトウェアの導入と利用

① 情報システム責任者は、クライアント端末、制御端末等の情報機器にウイルス対策ソフトウェアを導入し、自動更新により常に最新のパターンファイルを適用する。

② 情報システム責任者は、オフライン等で自動更新に設定できないクライアント端末については、当該機器に適したウイルス対策を講じ、最新のパターンファイルを随時、手動で更新を指示し実施させる。

③ 情報システム責任者は、ウイルスの自動検索を、業務の支障のない時間帯に設定する。

④ 情報システム責任者は、外部から持ち込んだ媒体のウイルスチェックを行う環境を整備する。

⑤ 情報システム責任者は、平素よりセキュリティ情報の収集に努め、不具合が発生した場合、速やかな対応ができるようする。

⑥ 情報システム責任者は、メーカーがサポートを終了したOSやソフトウェアを使用する場合は、リスク分析を実施し、影響範囲を特定し、影響が最小限になるよう対策を施し、残留リスクを認識した上で使用を許可する。

⑦ 利用者は、ウイルス感染が生じた場合、あるいはその可能性があると判断された場合、当該機器を速やかにネットワークから遮断し、所属部門長及び情報システム責任者に連絡する。その際、利用者は情報システム責任者の対応を待ち、自らの判断で作業してはならない。情報システム責任者は、当該事例に対応する有効な情報を収集し、適切な対応に努める。

⑧ 利用者は、ウイルス定義ファイルが最新になっているか確認する。

⑨ 利用者は、ウイルス対策ソフトのリアルタイム検索をONにする。

⑩ 入稿担当者は、受取りデータをウイルスチェックしてから、データを取り込む。委託元や委託先から入稿担当者以外がデータを受け取る場合も、ウイルスチェックを実施してからデータを取り込む。

⑪ 出稿担当者や納品担当者は、納品データをウイルスチェックしてから出荷する。直接現場や委託先からデータを納品する場合は、ウイルスチェックを実施してから出荷させる。

⑫ 最新のパターンファイルの適用の確認を、運用の点検で、対象となる全てのクライアント端末で行う。

（2）セキュリティパッチの適用

① 情報システム責任者は、情報システム（コンピュータ、サーバ等）のOSやソフトウェア等に対する最

新のセキュリティ対策用修正ソフトウェア（セキュリティパッチ）を適用する。

② 情報システム責任者は、パターンファイルや修正ソフトウェアによる更新後の有効性や動作の安定性を必要に応じ確認する。

③ OS のセキュリティパッチを、自動更新で適用する。
（サーバについては、更新後の有効性や動作の安定性を調査後、適用する。）

④ 情報システム責任者は、メーカーがサポートを終了した OS やソフトウェアを使用する場合は、影響範囲を特定し、影響が最小限になるよう対策を施し、残留リスクを認識した上で使用を許可する。

⑤ 最新のセキュリティパッチが適用されていることの確認を、運用の点検で、対象となる全てのクライアント端末に対して行う。

### 第１５条　バックアップ管理（C.12.3）

１．目的

個人情報のバックアップ方針を定め、それに基づき定期的にバックアップを取得する。

２．管理策

（1）バックアップ方針

① 情報システム責任者は、バックアップの必要な個人情報を特定し、必要な方法でバックアップを取得する。

② 情報システム責任者は、共有ファイルサーバやクライアント端末内のデータのバックアップを実施し、バックアップの記録を残す。バックアップは、毎日差分を取り、定期的（週 1 回程度）にファイルサーバ全体のバックアップを行う。

③ 情報システム責任者は、盗難、不正持出しを防止するため、バックアップした媒体の施錠保管を行う。

### 第１６条　ログ管理（C.12.4、C.13.2、C.16.1）

１．目的

情報へのアクセスログや利用者の活動等のイベントログを取得し、保持し、定期的に点検する。

２．管理策

（1）ログの取得･保持

① 情報システム責任者は、ログの取得が必要なアクセスやイベントを定め、必要な方法でログを取得し、保持する。

② 取得するログは、異常なアクセス･イベント（例えば、休業日、業務時間外のアクセス、ログインエラー等）を含むものとし、以下のものを取得する。

･個人情報へのアクセスや操作の記録。個人情報へのアクセスや操作を記録できない場合は、情報システムへのアクセスの成功と失敗の記録

･外部からの不正アクセスの記録

･外部への大量のアップロードの記録

③ 取得したログの保管期間は 13 ヶ月とする。

④ 情報システム責任者は、取得したログが改ざんされないよう、保護しなければならない。

⑤ 情報システム責任者は、ログを正確に取得するために、情報システムの時刻を、日本標準時が設定されたサーバと同期させなければならない。

⑥ 情報システム責任者の情報システムへの作業記録（ログ）は保管し、定期的に個人情報保護管理者がレビューする。

（2）ログの点検

① 情報システム責任者は、定期的にログを点検する。

② 点検は、取得したログに、異常なアクセス・イベントがないかを確認する。異常を発見した場合、速やかに個人情報保護管理者に報告し、指示に従う。

③ 点検結果は、アクセスログ点検表に記録し、定期的に個人情報保護管理者の承認を受ける。

## 第4章　改訂

### 第１７条　改訂

1．本基準の改訂は、個人情報保護管理者の承認を得て行う。