NOPA-OSM101-3.0

OFFICE SECURITY

オフィスセキュリティマーク認証基準（Ver.3.0）

細則及び推奨

社団法人ニューオフィス推進協議会

まえがき

「オフィスセキュリティマーク認証基準（Ver.3.0）細則及び推奨」は、同認証基準(Ver.3.0）を具体的に実践するための事項を示したものであり、認証基準の条文とそれに対応した細則及び推奨からなる。

細則は、認証基準の解説及びオフィスセキュリティマーク認証のための判断基準として細部を規定したものである。

推奨は、オフィスセキュリティマーク認証審査の判断基準とは別に、より望ましいレベルのオフィスセキュリティ対策について記載している。また、参考となる事項を注記している。

目次

0. 序文

本認証基準は、社団法人ニューオフィス推進協議会が 2006 年 10 月 1 日より施行した「オフィスセキュリティマーク認証基準（Ver.2.0)」を基に、オフィスにおけるセキュリティ対策の実効性、有効性等に配慮して見直しを行い、「認証基準（Ver.3.0)」として改訂したものである。

1. 適用範囲

1.1 本認証基準は、事業の種類、形態、規模を問わず、あらゆる組織に適用する。

＜細則＞

(1) 組織は、日本国内に活動拠点があり、企業、官公庁、公益法人、個人事業主等であること。

(2) 次の欠格事項に該当する組織は申請を行うことができない。

a) オフィスセキュリティマーク申請日の前３ヶ月以内に、認証の申請又は再審査の請求について否認決定を受けた組織。

b) オフィスセキュリティマーク申請日の前２年以内に、認証の取消しを受けた組織。

c) 違法行為等によって、オフィスセキュリティマーク認証制度に弊害を及ぼす恐れのある組織。

d) その他、協議会が不適当と判断した組織。

1.2 申請単位は、全社、事業所又は部門等である。

2. 用語及び定義

本認証基準で用いる主な用語及び定義は、次の通りである。

2.1 オフィスセキュリティ

オフィスにおける経営資産を適切に保護し、想定される脅威に対して安全な状態を創出し、維持する経営活動。

2.2 オフィス

組織が業務のために利用する建物又は居室等。

2.3 経営資産

組織を経営していく上で必要となる価値ある資産。有形の経営資産を主とするが、必要最小限の無形の情報通信システム等についても対象とする。

2.4 保護対象資産

申請組織により特定された保護すべき経営資産。

2.5 エリア

外壁、内壁、間仕切り又は什器備品等によって囲まれた居室等、及び保管庫・キャビネット等。

2.6 申請エリア

オフィスセキュリティマーク認証を取得するために、申請組織が申請するエリア。

2.7 セキュリティエリア

申請エリア内にあって、必要なセキュリティのレベルが確保されたエリアで、セキュリティレベル1～３エリアがある。

2.8 オープンエリア

申請エリア内にあって、セキュリティエリアに該当しないエリア。

2.9 経営者

申請組織における経営上の責任者であり、オフィスセキュリティ対策全般に関する最終的な意思決定及び経営資源の投入の権限を有する代表取締役、取締役、執行役等の者。

2.10 従業員

申請組織に勤務する者。正社(職)員のみならず、契約社員、派遣社員、嘱託、パートタイマー、臨時雇用者等で外部委託先等の者を除く。

2.11 オフィスセキュリティ管理責任者

オフィスセキュリティの計画、構築、導入、運用、点検、維持及び改善に関して、経営者により委嘱された申請組織に属する最高の責任を有する者。

3. 一般要求事項

3.1 組織は、自らの事業の活動全般にわたって想定される脅威に対するリスクを考慮して、オフィスセキュリティマネジメントシステムを構築し、実行しなければならない。

＜細則＞

(1) オフィスセキュリティマネジメントシステムとは、計画・構築、導入・運用、点検・監査、維持・改善のＰＤＣＡサイクルによって、オフィスセキュリティを適切にマネジメントすることである。

(2) 想定される脅威とは、事件、事故、違反又は災害等により、経営資産が損失又は漏えいすることである。

4. 計画・構築

4.1 オフィスセキュリティ基本方針

4.1.1 オフィスセキュリティ基本方針を文書化しなければならない。

＜細則＞

(1) オフィスセキュリティ基本方針は、単独の方針として作成する、もしくはオフィスセキュリティ管理規程又はそれに準じる規程類の中に記載すること。

（注）社団法人ニューオフィス推進協議会が作成するオフィスセキュリティ基本方針モデルを参考にすることができる。

4.1.2 オフィスセキュリティ基本方針には、オフィスセキュリティの基本的な考え方を示さなければならない。

＜細則＞

(1) オフィスセキュリティに関する基本的な考え方は、オフィスセキュリティ対策を実施する

際の目的、目標、管理のあり方等とすること。

4.1.3 オフィスセキュリティ基本方針を経営者が承認しなければならない。

＜細則＞

(1) 経営者の承認は、署名又は承認印によって明らかであること。

(2) 事業所単位や部門単位での申請で、基本方針が全社組織の適用でない場合は、申請組織の最高責任者が承認すること。

4.1.4 オフィスセキュリティ基本方針を従業員に対して周知しなければならない。

＜細則＞

(1) 従業員に対する周知は、文書配布、グループウェアやイントラネットによる配信、又は掲示等の方法によること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 基本方針は、外部に対して開示することが望ましい。

(2) 基本方針は、取引先、契約先、外部委託先等に理解してもらうことが望ましい。

4.1.5 オフィスセキュリティ基本方針を必要に応じて見直さなければならない。

＜細則＞

(1) オフィスセキュリティ基本方針を必要に応じて見直しを行い、改訂すること。

(2) その改訂内容を経営者が承認すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.2 オフィスセキュリティ管理体制

4.2.1 オフィスセキュリティ管理体制を整備しなければならない。

＜細則＞

(1) オフィスセキュリティマネジメントシステムを構築し実行するための管理体制を整備すること。

(2) オフィスセキュリティ管理体制を図示すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.2.2 オフィスセキュリティ管理体制には、主要な管理者の責任及び権限を定義しなければならない。

＜細則＞

(1) 経営者は、申請組織におけるオフィスセキュリティ管理責任者を指名すること。

(2) オフィスセキュリティ管理責任者は、部門の責任者を指名すること。なお、オフィスセキュリティ管理責任者のみでその役割を十分に果たすことができる小規模な組織では、部門の責任者を置く必要はない。

(3) オフィスセキュリティ管理責任者と部門の責任者の管理対象及び責任、権限を定義すること。
(4) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.2.3 オフィスセキュリティ管理体制を必要に応じて見直さなければならない。

＜細則＞
(1) オフィスセキュリティ管理体制を必要に応じて見直しを行い、改訂すること。
(2) その改訂内容を経営者が承認すること。
(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.3 オフィスセキュリティ管理規程

4.3.1 オフィスセキュリティ管理規程を文書化しなければならない。

＜細則＞
(1) オフィスセキュリティ管理規程は、単独の規程として作成する、又は他のセキュリティに関わる規程類の中に記載すること。
(注) 社団法人ニューオフィス推進協議会が作成するオフィスセキュリティ管理規程モデルを参考にすることができる。

4.3.2 オフィスセキュリティ管理規程には、オフィスセキュリティの具体的な管理策を示さなければならない。

＜細則＞
(1) オフィスセキュリティの具体的な管理策は、オフィスセキュリティの計画、構築、導入、運用、点検、監査、維持及び改善に関する規則等とすること。

4.3.3 オフィスセキュリティ管理規程を経営者が承認しなければならない。

＜細則＞
(1) 経営者の承認は、署名又は承認印によって明らかであること。
(2) 事業所単位や部門単位での申請で、管理規程が全社組織の適用でない場合は、申請組織の最高責任者が承認すること。

4.3.4 オフィスセキュリティ管理規程を従業員に対して周知しなければならない。

＜細則＞
(1) 従業員に対する周知は、文書配布、グループウェアやイントラネットによる配信、又は掲示等の方法によること。
(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.3.5 オフィスセキュリティ管理規程を必要に応じて見直さなければならない。

＜細則＞

(1) オフィスセキュリティ管理規程又はそれに準じる規程類を必要に応じて見直しを行い、改訂すること。

(2) その改訂内容を経営者が承認すること。

(3) 改訂を行った場合は、改訂履歴を記録すること。

(4) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.4 保護対象資産の分類及び保管・保存

4.4.1 保護対象資産を特定し、その重要度に応じて３段階に分類しなければならない。

＜細則＞

(1) 重要度１～３の３段階の分類基準は次の通りである。

a) 重要度１の保護対象資産は、事件、事故、違反又は災害等により、漏えい又は損失等が生じた場合において、業務への影響が少ないと想定される経営資産であること。

b) 重要度２の保護対象資産は、事件、事故、違反又は災害等により、漏えい又は損失等が生じた場合において、業務に大きな影響を与える可能性のある経営資産であること。

c) 重要度３の保護対象資産は、事件、事故、違反又は災害等により、漏えい又は損失等が生じた場合において、事業の継続に大きな影響を与える可能性のある経営資産であること。

(2) 保護対象資産は、重要度に応じた分類を行い、重要度別資産管理台帳等に記載し、管理すること。

(3) 保護対象資産の特定及び分類の結果を経営者が承認すること。

(4) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 下記に示す一般的に重要度の高い経営資産については、重要度２又は３に分類することが望ましい。

a) 高額な現金、有価証券等。

b) 社印、代表者印、銀行印等。

c) 下記のような重要な情報を記録している書類、電子媒体又は情報通信機器。

①法令で保存が定められている書類等。

②個人情報に係わる顧客情報、人事情報等。

③経営にかかわる計画書、財務上のデータ等。

④事業活動における重要な契約書等。

⑤知的財産としての価値の高い新規開発製品、事業情報等。

⑥その他秘密として管理されている事業活動に有用な経営上の情報等。

4.4.2 保護対象資産の特定及び分類の基準について文書化しなければならない。

＜細則＞

(1) 保護対象資産の特定及び分類の基準を、オフィスセキュリティ管理規程又はそれに準じる規程類に明記すること。

4.4.3 保護対象資産の特定及び分類の基準を必要に応じて見直さなければならない。

＜細則＞

(1) 保護対象資産の特定及び分類の基準を必要に応じて見直しを行い、改訂すること。

(2) その改訂内容を経営者が承認すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.4.4 保護対象資産は、その重要度に応じたセキュリティエリアに保管・保存しなければならない。

＜細則＞

(1) 保護対象資産の重要度に応じたセキュリティエリアは、次の通りである。

a) 重要度１の保護対象資産は、セキュリティレベル１以上のエリアに保管・保存すること。

b) 重要度２の保護対象資産は、セキュリティレベル２以上のエリアに保管・保存すること。

c) 重要度３の保護対象資産は、セキュリティレベル３エリアに保管・保存すること。

d) 申請エリアが全てセキュリティレベル３エリアの場合、重要度３の保護対象資産は、申請エリア内に別途設けるアクセス権限を特定したセキュリティレベル３エリアの居室等又は保管庫・キャビネット等に保管・保存すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

4.5 エリアのレベル設定

4.5.1 申請エリアは、その境界が外部からの不正侵入等に対して堅牢であり、かつ業務時間外等の不在時は、申請エリアにアクセス権限が付与されている者以外が立入れないよう施錠しなければならない。

＜細則＞

(申請エリアの条件)

(1) 申請エリアは、申請者が専有し、かつ日常的に使用していること。賃貸ビルに入居している場合は、賃借スペース以外のスペース（エレベータホール、廊下、機械室等）を申請エリアに含めることはできない。

(2) 申請エリアは、次のいずれかであること。

a) 建物全体。

b) 同一建物の複数フロア。フロアは連続している必要はない。

c) 建物の１フロア、又はフロアの一部。

(3) 申請エリアの実態と、オフィスセキュリティマーク現状図面及びオフィスセキュリティマーク申請図面に相違がないこと。

(申請エリアの境界の条件)

(1) 申請エリアの境界は、外部からの不正侵入等に対して堅牢であること。具体的には次の通りである。

a) 境界の壁は、天井まで密閉されているか、戸やシャッター等により密閉できるものであること。法令や建物の構造、設備上の制約等により密閉が困難な場合は、外部から容易に侵入できない状態になっていること。

b) 境界の壁は、容易に移動、倒壊しない、又は破壊されない壁であること。

c) 業務時間外等の不在時は、アクセス権限者以外が立ち入れないよう申請エリアの境界の出入口や窓等の開口部を施錠すること。

なお、次の事項に留意すること。

① 賃貸ビルに入居している場合、建物や共用部への出入口を施錠している場合でも、独自に申請エリアの出入口を施錠すること。

② 自社ビルにあって、申請エリアがその一部である場合、建物や共用部への出入口を施錠している場合でも、独自に申請エリアの出入口を施錠すること。

③ エレベータが申請エリアの出入口である場合、当該階が不停止となる状態は施錠とみなすこと。

(アクセス権限管理)

(1) 申請エリア内の各セキュリティレベルのエリアごとに、アクセスできる権限の範囲、条件及びアクセス権限者等を定め、管理台帳等に記載し適切に管理すること。

アクセス権限とは、セキュリティレベルの設定された居室等に入室することのできる権限、及びセキュリティレベルが設定された保管庫・キャビネット等を解錠できる権限をいう。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

(申請エリア内の機密保護)

(1) 重要度３の保護対象資産、セキュリティレベル３エリアに指定された居室等、及び保管庫・キャビネット等の所在を、申請エリアの外部やオープンエリアにおいて容易に認識できないこと。

＜推奨＞

(1) 堅牢性のレベルを、床、壁、天井(屋根)や開口部(出入口、窓等)などの個別部位の強度から、定量的、総合的に評価することが望ましい。

(2) 堅牢性を高めるために、建物の各部位にＣＰ認定のものを利用することが望ましい。

(3) 強度の低い部位が存在する場合は、センサーによる非常警報装置や監視カメラ等を設置することが望ましい。

(4) 地震、火災等の非常時におけるアクセス権限の特別措置等を定めることが望ましい。

(注) ＣＰ（Crime Prevention）は防犯の意味であり、ＣＰ認定とは、侵入盗（許可されていない空間に侵入し窃盗を企図する者)の７割が侵入を諦めるとされる５分間の破壊行為や侵入行為に耐えることを基準に、防犯性能試験をクリアした戸、ガラス、錠、

サッシなどの防犯性能の高い建物部品を認定したものである。
ＣＰ認定は（財）全国防犯協会連合会のホームページを参考にすることができる。
（ http://www.bohan.or.jp/index2.htm）
また、官民合同会議（警察庁、国土交通省、経済産業省および建物部品関連の民間団体）が公表した「防犯性能の高い建物部品目録」を参考にすることができる。
（ http://www.cp-bohan.jp/index.asp）

4.5.2 セキュリティレベル１エリアは、入室抑止機能があり、アクセス制限を行うことができる居室等でなければならない。

＜細則＞

(1) セキュリティレベル１エリアの居室等の境界は、外部から容易に侵入できないこと。

(2) 居室等の出入口には、アクセス権限者以外の者が入室できないように、次のいずれかに該当する抑止機能があること。

a) 出入口の戸が常時開放で、無断入室禁止表示等があり、外部又はオープンエリアからセキュリティレベル１エリアへの入室の出入口は、パーティション又は什器備品等により動線を制限していること。
かつ出入口は、アクセス権限者の監視下にあること。
アクセス権限者の監視下とは、アクセス権限者が目視で確認できる距離に常時存在し、監視性が保たれていることをいう。監視カメラ等を設置して出入口を常時モニタリングすることでもよい。

b) 出入口の戸が常時開錠で、無断入室禁止表示があること。
開錠とは、戸が閉じており施錠していない状態をいう。

c) 受付担当者又は警備員等を配置していること。受付担当者又は警備員等の不在時には、上記 a)又は b)の状態であること。

(3) 無断入室禁止表示等は、例えば「許可のない方の入室はご遠慮ください」等の表示であり、単に「入室禁止」のようなあいまいな表示でないこと。

(4) 無断入室禁止表示等は、目につきやすい場所に表示すること。

＜推奨＞

(1) 出入口には、セキュリティエリア内の従業員等に連絡できるインターホン、内線電話等の設備があることが望ましい。

4.5.3 セキュリティレベル２エリアは、出入口の戸が常時施錠で、アクセス制限を行うことができる居室等であること、もしくはセキュリティエリアの中にある常時施錠で、アクセス制限を行うことができる保管庫・キャビネット等でなければならない。

＜細則＞

(セキュリティレベル２エリアの居室等の条件)

(1) セキュリティレベル２エリアの居室等の境界は、外部からの不正侵入等に対して堅牢であること。具体的には次の通りである。

a) 境界の壁は、天井まで密閉されているか、戸やシャッター等により密閉できるものであること。法令や建物の構造、設備上の制約等により密閉が困難な場合は、外部から容易に侵入できない状態になっていること。

b) 境界の壁は、容易に移動、倒壊しない、又は破壊されない壁であること。

c) 居室等の出入口以外の開口部（窓等）は、業務時間外等の不在時は施錠すること。

(2) 居室等の出入口は、常時施錠とし、アクセス権限者のみが解錠できること。ただし、アクセス権限者の監視下にある場合に限り、常時施錠の必要はない。

(3) アクセス権限者以外の者が入室する必要のある場合は、アクセス権限者が同行すること。かつ、オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

(セキュリティレベル２エリアの保管庫・キャビネット等の条件)

(1) セキュリティレベル２エリアの保管庫・キャビネット等は、セキュリティエリアの中にあること。

(2) セキュリティレベル２エリアの保管庫・キャビネット等は、それ自体を容易に持ち出しできないよう、壁又は床に固定する、前後左右に連結する等の対策がとられていること。又はそれ自体を容易に持ち出しできない重量があること。

(3) セキュリティレベル２エリアの保管庫・キャビネット等は、常時施錠とし、アクセス権限者のみが解錠できること。ただし、アクセス権限者の監視下にある場合に限り、常時施錠の必要はない。

＜推奨＞

(1) 出入口の戸は、解錠して入室後、自動的に閉じ、かつ自動的に施錠されることが望ましい。

(2) 車輪のついた保管庫・キャビネット等は、車輪を取り外す、又は容易に移動しないものにワイヤー等で固定することが望ましい。

(注)堅牢な境界の望ましい施策については、4.5.1 の＜推奨＞を参照のこと。

4.5.4 セキュリティレベル３エリアは、出入口等の開口部が常時施錠でアクセス制限を行うことができ、かつアクセス記録をとることができる居室等であること、又はセキュリティエリアの中にあり、常時施錠で、アクセス制限を行うことができ、かつアクセス記録をとることができる保管庫・キャビネット等でなければならない。

＜細則＞

(セキュリティレベル３エリアの居室等の条件)

(1) セキュリティレベル３エリアの居室等の境界は、外部からの不正侵入等に対して堅牢であること。具体的には次の通りである。

a) 境界の壁は、天井まで密閉されているか、戸やシャッター等により密閉できるものであること。法令や建物の構造、設備上の制約等により密閉が困難な場合は、外部から容易に侵入できない状態になっていること。

b) 境界の壁は、容易に移動、倒壊しない、又は破壊されない壁であること。

c) 居室等の出入口以外の開口部（窓等）は、常時施錠し、外部から容易に侵入できないようになっていること。ただし、アクセス権限者の監視下にある場合に限り、常時施

錠の必要はない。

(2) 居室等の出入口は、常時施錠とし、アクセス権限者のみが解錠を行い、かつアクセス記録をとること。ただし、アクセス権限者が１人であり、鍵を本人のみが所有し、本人のみが解錠する場合に限り、アクセス記録をとらなくてよい。

解錠がその都度、貸与される共用の鍵等による場合は、その貸与記録をアクセス記録としてよい。

(3) アクセス権限者以外の者が入室する必要のある場合は、アクセス権限者が同行し、その者の入室及び退室記録をとること。

かつ、オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

(セキュリティレベル３エリアの保管庫・キャビネット等の条件)

(1) セキュリティレベル３エリアの保管庫・キャビネット等は、セキュリティエリアの中にあること。

(2) セキュリティレベル３エリアの保管庫・キャビネット等は、それ自体を容易に持ち出しできないよう、壁又は床に固定する、前後左右に連結する等の対策がとられていること。又はそれ自体を容易に持ち出しできない重量があること。

(3) セキュリティレベル３エリアの保管庫・キャビネット等は、常時施錠とし、アクセス権限者のみが解錠を行い、かつアクセス記録をとること。ただし、アクセス権限者が１人であり、解錠の鍵も本人のみが所有し、本人のみが解錠する場合に限り、必ずしもアクセス記録をとらなくてよい。

解錠がその都度、貸与される共用の鍵等による場合は、その貸与記録をアクセス記録としてよい。

(アクセス記録の条件)

(1) アクセス記録を保存する期間を定めること。

アクセス記録とは、居室等に入室する場合、及び保管庫・キャビネット等を解錠する場合、その当事者の氏名、及びその日時の記録のことをいう。記録には自動的に行われるもの、及び筆記によるものがある。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 出入口の戸は、解錠して入室後、自動的に閉じ、かつ自動的に施錠、及び記録されることが望ましい。

(2) 出入口の鍵は、容易に不正な解錠が行われないＣＰ認定のものを使用することが望ましい。

(3) 出入口の戸の付近は、監視カメラにより監視し、画像を記録することが望ましい。

(4) 業務時間外の出入口、窓等の開口部の施錠なされていない、又は不正な侵入がある状態に対して警備会社等に自動的に通報できる装置があることが望ましい。

(5) 居室等の場合は、入室時のみならず、退室時の記録をとることが望ましい。

(6) 保管庫・キャビネット等の場合は、解錠のみならず、出し入れした格納物の内訳についてもアクセス記録をとることが望ましい。

(7) 車輪のついた保管庫・キャビネット等は、車輪を取り外す、又は容易に移動しないものに

ワイヤー等で固定することが望ましい。

(8) アクセス記録は、カード認証、生体認証などにより自動的に記録をとることが望ましい。

(注)堅牢な境界の望ましい施策については、4.5.1 の＜推奨＞を参照のこと。

4.5.5 申請エリアには、必ずセキュリティレベル３エリアを含まなければならない。

＜細則＞

(1) 申請エリアが全てセキュリティレベル３エリアとなる場合は、別途にアクセス権限を特定したセキュリティレベル３エリアの居室等又は保管庫・キャビネット等を設けること。

4.5.6 セキュリティエリアのレベル設定についての決定及び変更の方法を定めなければならない。

＜細則＞

(1) セキュリティエリアのレベル設定についての決定及び変更の方法を、オフィスセキュリティ管理規程又はそれに準じる規程類に明記すること。

4.6 エリアにおけるセキュリティ対策

4.6.1 各セキュリティレベルのエリアの利用目的を明確にしなければならない。

＜細則＞

(1) 各セキュリティレベルのエリアの利用目的を、オフィスセキュリティ管理規程又はそれに準じる規程類に明記すること。

4.6.2 各セキュリティレベルのエリアの作業指針を定めなければならない。

＜細則＞

(1) 各セキュリティレベルのエリアごとの作業の禁止事項、規制事項、注意事項等、オフィスセキュリティに関する作業指針を定めること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 作業指針には、次のような事項を記載することが望ましい。

a) 各セキュリティエリアに許可されていない者が入室する場合は、アクセス権限者が同行すること。

b) 各セキュリティエリアをセキュリティ管理責任者又は部門責任者の許可なくカメラや携帯電話等で撮影しないこと。

c) セキュリティレベル２以上のエリアで、可燃性の高いものを保管・保存しない、及び喫煙、ストーブ等の火気を禁止すること。

d) セキュリティレベル２以上のエリアに解錠して入室する場合、鍵を錠前に差し込んだままにしないこと。

e) セキュリティレベル３エリアに入室する場合、アクセス権限を持たない者が同行する場合は、同行者の氏名を明確にすること。

f) 特に厳重なセキュリティレベル３エリアに入室する場合、アクセス権限をもつ複数の者が同行すること。

4.6.3 居室等におけるオフィス設計においては、セキュリティ上の対策を適切に行わなければならない。

＜細則＞

(1) オフィス設計においては、次の事項に留意して行うこと。

a) 高次のセキュリティレベルのエリアは、出入口に近い場所に配置しないこと。やむを得ず配置する場合は、その居室又は保管庫・キャビネット等の存在が容易に認識できないゾーニングやレイアウトとする等の対策を行うこと。

b) 通行が頻繁な通路沿いに、重要度の高い情報を作成又は出力する機器を配置しない等の対策を行うこと。

＜推奨＞

(1) セキュリティエリアは、低次のレベルから高次のレベルになるに従って、入れ子状のゾーニングを行うことが望ましい。

(2) 申請エリアが複数階の場合、高次のセキュリティレベルのエリアは、外部から侵入しやすい階に配置しないことが望ましい。

(3) 重要度の高い情報を扱う従業員の席は、通路を背に配置しない、パネル（ローパーテション）で囲むなどの情報管理対策を講じることが望ましい。

4.6.4 保管庫・キャビネット等については、防災上の対策を適切に行わなければならない。

＜細則＞

(1) 地震、火事、水害等により、重要な保護対象資産が散逸する、損失する等がないよう対策を講じること。

(2) 保管庫･キャビネット等の扉や引き出しは、ラッチ機構やインターロック機構があること。かつ、扉や引出しは、使用後、確実に閉じること。

(3) 保管庫・キャビネット等が複数並ぶ場合は、転倒しないよう相互に連結すること。

(4) 特に重要な保護対象資産は、耐火性能をもつ保管庫・キャビネット等（金庫、耐火庫）に格納すること。

＜推奨＞

(1) 防災対策については、次の事項を行うことが望ましい。

a) 保管庫の扉のガラスは、飛散防止フィルムを貼る等の対策を講じること。

b) 居室の中央に設置する場合、単独の保管庫・キャビネット等の高さは、1.2m程度を限度とすること。

c) 壁面に設置する背の高い保管庫・キャビネット等は、壁及び床に固定すること。

d) 書類倉庫等の背の高い保管庫・キャビネット、書架や軽量棚は、上部を連結棒で連結すること。

e) 火気のある場所に近接して、重要な保護対象資産を保管･保存することを避けること。

f) 水害に備え、地下階に重要な保護対象資産を保管・保存することを避けること。

g) 水を扱う場所の近辺に、重要な保護対象資産を保管・保存することを避けること。

5. 導入・運用

5.1 従業員等の管理

5.1.1 従業員の秘密保持の管理を適切に行わなければならない。

＜細則＞

(1) 従業員から秘密保持の誓約書を取る、又は秘密保持の義務を課した就業規則等によって雇用契約を締結する等、重要情報の流出を防止するための管理を行うこと。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 誓約書又は就業規則等に秘密保持に違反した際の罰則規定を記載することが望ましい。

5.1.2 オフィスセキュリティに関する従業員教育を適切に実施しなければならない。

＜細則＞

(1) 従業員教育の対象、方法、時期等について明確にすること。

(2) 従業員教育の実施記録を作成すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 朝礼や講習等において、オフィスセキュリティに関する啓発活動を継続的に行うことが望ましい。

5.1.3 従業員等の識別管理を適切に行わなければならない。

＜細則＞

(1) 組織の規模等の実情にあわせて、識別証等による管理を行うこと。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 識別証による管理を行う場合は、次の事項を行うことが望ましい。

a) 識別証は、胸等の見やすい位置に着用すること。

b) 識別証を紛失した者は、直ちに部門の責任者もしくはオフィスセキュリティ管理責任者に届けること。

c) 人事異動、退職、契約解除等に際しては、速やかに識別証を返還させる措置を講じること。

d) 識別証管理台帳を作成して管理し、識別証の配布状況について定期的に棚卸を行うこと。

5.1.4 オフィスセキュリティに係る禁止事項､及びそれに違反した場合の処分を定めなければならない。

＜細則＞

(1) オフィスセキュリティに係る禁止事項、及びそれに違反した場合の処分を、オフィスセキュリティ管理規程又はそれに準じる規程類に明記すること。

5.2 重要度２以上の保護対象資産の管理

5.2.1 重要度２以上の保護対象資産の取り扱いの作業指針を定めなければならない。

＜細則＞

(1) 重要度２以上の保護対象資産を取り扱う場合の禁止事項、規制事項、注意事項等、オフィスセキュリティの作業指針を定めること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 作業指針には、次のような事項を記載することが望ましい。

a) 重要度２以上の書類や保護対象資産を、それを管理する担当部門の責任者の許可なくカメラや携帯電話等で撮影しないこと。

b) 作業中の重要度２以上の書類等が、机上に散乱して置かれる等により、部外者から容易に見られることのないようにすること。

5.2.2 机上等に重要度２以上の保護対象資産を長時間放置してはならない。

＜細則＞

(1) 長時間の離席時や退社時には、その都度、重要度２以上の保護対象資産を保管庫・キャビネット等に格納し施錠すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 長時間の離席については、組織の実情に合わせて具体的な時間を設定することが望ましい。

5.2.3 重要度２以上の保護対象資産は、オフィスセキュリティ管理責任者等の許可なしに、申請エリアの外部に持ち出してはならない。

＜細則＞

(1) 重要度２以上の保護対象資産は､オフィスセキュリティ管理責任者及び規程類で定める管理責任者の許可なしに申請エリアの外部への持ち出しを禁止すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

5.3 書類及び電子媒体等の管理

5.3.1 書類及び電子媒体等の保管・保存の方法を適切に行わなければならない。

＜細則＞

(1) 保管・保存する書類は、重要度に応じた分類を行い、管理台帳に記載し、管理すること。

(2) 分類の単位及び個別の表題は、その内容が容易に認識できること。
(3) 書類及び電子媒体の保存期間を定めること。法定保存年限のあるものはそれに準拠すること。
(4) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞
(1) 重要度３の書類のうち、特に厳重に原本保存が求められる書類については、準原本を作成し、原本とは異なる場所に保存することが望ましい。
(2) 保管、保存、廃棄のルールを定め、書類の生涯を管理するファイリングシステムを導入することが望ましい。
(3) ファイルリスト（ファイル基準表）を作成する場合は、重要度分類欄を設けるとともに、その保管・保存場所を明確にすることが望ましい。

5.3.2 書類及び電子媒体等の廃棄を適切に行わなければならない。

＜細則＞
(1) 保存期間が満了している、又は活用が終了した書類及び電子媒体等の廃棄は、次の事項に留意して行うこと。
  a) 書類等は、シュレッダーでの破砕処分又は焼却炉での焼却処分等を行うこと。
  b) 電子媒体は、シュレッダー、工具、はさみ等により破砕処分等を行うこと。
  c) 書類及び電子媒体等の廃棄を外部に委託する場合は、廃棄証明を発行できる会社を選定し、その内容が他に漏れることのないよう処理すること。
(2) 廃棄処分が予定されている書類及び電子媒体等を処分予定日より前から保管する場合は、同じセキュリティレベル以上のエリアで保管すること。
(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

5.3.3 重要度２以上の保護対象資産である書類及び電子媒体等を再利用してはならない。

＜細則＞
(1) 重要度２以上の保存書類や電子媒体は、再利用して訂正・加筆・削除等の改ざんを行わないこと。
(2) 重要度２以上の書類の裏面をコピー用紙、メモ用紙等に使用しないこと。
(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

5.4 情報通信機器及び装置等の管理

5.4.1 コピー機、ＦＡＸ又はプリンタ等の書類の出力等を行う装置及び出力物は、セキュリティ上の対策を適切に行わなければならない。

＜細則＞
(1) オープンエリア、出入口近辺に、コピー機、ＦＡＸ又はプリンタ等書類の出力等を行う装置の設置及び出力物を放置しない、それらの周囲をパネル（ローパーテーション）で囲む

など、情報管理対策を講じること。

(2) コピー機、ＦＡＸ又はプリンタ等の書類の出力等を行う装置及び出力物が、許可なくアクセス権限者以外の者によって操作及び持ち出しされないように、運用上の対策を講じること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

5.4.2 コンピュータ等の情報通信機器は、セキュリティ上の対策を適切に行わなければならない。

＜細則＞

(1) 長時間の離席時や退社時は、机上等のコンピュータの電源を切る、スクリーンセーバを利用するなどのクリアスクリーンの対策を講じること。

(2) ノートブック型パソコンは、業務終了後には保管庫・キャビネット等に保管し、扉や引き出しを施錠する、ワイヤーロック等で机に固定するなどの対策を講じること。

(3) ノートブック型パソコンは、オフィスセキュリティ管理責任者又は規程類で定める管理責任者の許可なしに、申請エリアの外部への持ち出しを禁止すること。

(4) ユーザーＩＤ及びパスワードに関する情報を、コンピュータ本体及びその周辺に掲示しないこと。

(5) 会議室等で使用する電子黒板（ホワイトボード等を含む）に重要な情報が記載されている場合は、使用後は記載内容を消去すること。情報共有のために記載内容を一定期間消去しない場合は、記載内容が容易にアクセス権限者以外の目につかない処置をとること。

(6) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 長時間の離席については、組織の実情に合わせて具体的な時間を設定することが望ましい。

(2) サーバ等の重要な情報通信機器は、重要度３に分類することが望ましい。

5.4.3 ケーブル配線及び装置等は、セキュリティ上の対策を適切に行わなければならない。

＜細則＞

(1) 情報通信機器のケーブル配線等は、断線及び損傷等が生じない対策を講じること。

＜推奨＞

(1) 情報通信機器の電源プラグや通信用ジャックは、容易に抜けないものを使用することが望ましい。

5.5 情報通信システム等の管理

5.5.1 アクセス管理等を適切に行わなければならない。

＜細則＞

(1) ユーザーＩＤ及びパスワードの管理方法を明確にし、その遵守の状態を適切に管理すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 情報システム利用者に対してアクセス権限を設定し、固有のユーザーＩＤを割り振ること、又は本人認証ができる装置があることが望ましい。

(2) 人事異動、退職、契約解除等に際しては、速やかに情報システム利用者のユーザーＩＤを変更することが望ましい。

(3) ユーザーＩＤを管理する者は、管理者権限を限定し、管理者ＩＤを独自に割り振ることが望ましい。

管理者権限とは、情報システムへの全てのアクセスの権限が与えられている権限である。

(4) 情報システム利用者は、パスワードを設定することが望ましい。

(5) パスワードは、推測されにくいものを設定することが望ましい。

(6) パスワードは、定期的に変更することが望ましい。

(7) アクセス管理は、カード認証や生体認証を活用して行うことが望ましい。

5.5.2 電子メール等に関する管理を適切に行わなければならない。

＜細則＞

(1) 電子メール等の利用方法を明確にし、その遵守の状態を適切に管理すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) メールサーバに電子メール管理ソフトを導入し､添付ファイルの管理を行うことが望ましい。

5.5.3 インターネットに関する管理を適切に行わなければならない。

＜細則＞

(1) インターネットの利用方法を明確にし、その遵守の状態を適切に管理すること。

インターネットの利用方法とは、ホームページの閲覧制限、受送信相手の制限、インターネット受送信可能な情報機器の制限、ファイル等のダウンロードの制限等がある。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 不要なサービスポートを停止することが望ましい。

(2) ファイアウォールを導入し、不正な情報の流入、無用な情報の取得等を防止することが望ましい。

(3) ウェブサーバ上に重要度の高いデータを保存しないことが望ましい。

(4) 重要度の高い情報を扱う情報システムは、インターネットに接続された情報ネットワークから物理的に切り離すことが望ましい。

5.5.4 不正ソフトウェア等に関する管理を適切に行わなければならない。

＜細則＞

(1) インストールしてもよいソフトウェアを明確にし、その遵守の状態を適切に管理すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) コンピュータウイルス対策ソフトウェアを導入することが望ましい。

5.5.5 情報システム等に関する管理を適切に行わなければならない。

＜細則＞

(1) システム及びデータのバックアップの方法を明確にし、その遵守の状態を適切に管理すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) バックアップは、サーバ等で自動的に行うことが望ましい。

(2) 重要度の高いデータ及びファイルは、暗号化することが望ましい。

(3) 情報システム利用者のアクセス記録をとり、定期的に内容を分析し、適切にセキュリティ対策を講じることが望ましい。

(4) アクセス記録は、一定期間保存することが望ましい。

(5) システム開発、保守作業におけるデータの管理（テストデータの使用等）を行うことが望ましい。

(6) システム開発、保守作業における作業員のアクセス権限管理、及びアクセス記録の管理を行うことが望ましい。

(7) 保守管理及び保存期間等については、組織の実情に合わせて具体的な期限・期間を設定することが望ましい。

5.6 鍵の管理

5.6.1 居室等及び保管庫・キャビネット等の鍵を適切に管理しなければならない。

＜細則＞

(1) 個人が管理する鍵は、他人に使用されないように本人が常時所持すること、又は他人が使用できないように定めた場所に保管すること。

(2) 共用の鍵（機械式の鍵及びカード等）は、管理責任者を設定し、鍵の保管場所を定めて、許可されていない者が使用できないように管理すること。

(3) 共用の鍵を貸与する場合は、鍵の貸与及び返却の記録をとること。

(4) 人事異動、退職、契約解除等に際しては、速やかに鍵を返還させる措置を講じること。

(5) 鍵管理台帳を作成して管理し、鍵の貸与状況について定期的に棚卸を行うこと。

(6) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 共用の鍵の保管は、施錠できるキーボックス又は保管庫・キャビネット等に格納し、確実に管理することが望ましい。

(2) キーボックスは、鍵の借り出し、返却が自動的に記録されるものを使用することが望ましい。

5.6.2 鍵の紛失時には適切に対応しなければならない。

＜細則＞

(1) 鍵を紛失した場合は、直ちに鍵の管理責任者に報告し、紛失した鍵を無効にする処置をとること。

(2) 暗証番号がアクセス権限者以外の者に漏えいした場合は、直ちに鍵の管理責任者に報告し、暗証番号を変更すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

5.7 配送物の管理

5.7.1 配送物の管理を適切に行わなければならない。

＜細則＞

(1) 配送物を放置しないチェック体制を整備すること。

(2) 受領した物や配送する物は、受け渡し場所を定め、無人の状態で放置しないこと。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 施錠できる郵便受けを設置することが望ましい。

5.8 外部委託先等の管理

5.8.1 申請エリアに出入りする外部委託先等の秘密保持の管理を適切に行わなければならない。

＜細則＞

(1) 申請エリアに出入りする主たる外部委託先等と秘密保持の契約を締結すること。

(2) 外部委託先等管理台帳等を作成し、管理すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 申請エリアに出入りする外部委託先の者は、外部委託者であることを容易に識別できることが望ましい。

5.9 外部保管・保存の管理

5.9.1 外部倉庫等に保管・保存する保護対象資産の管理を適切に行わなければならない。

＜細則＞

(1) 保護対象資産の保管・保存を外部の倉庫会社等に委託する場合は、オフィスセキュリティ管理責任者又は規程類で定める管理責任者の許可を得ること。

(2) 重要な保護対象資産の保管・保存を委託する倉庫会社等に対して、セキュリティに留意した条項を含んだ業務委託契約等を締結すること。

(3) 外部倉庫等に保管・保存する保護対象資産は閲覧、持ち出し、返却の都度、台帳に記入すること。

(4) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 保護対象資産の定期的な棚卸をすることが望ましい。

6. 点検・監査

6.1 入退室記録

6.1.1 初回入室時及び最終退室時の記録をとらなければならない。

＜細則＞

(1) 出退勤時に、定められた出入口からの初回入室及び最終退室の時間と入退室者の記録をとること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 出退勤時の入退室の時間と入退室者は、カードシステム等により、自動的に記録されることが望ましい。

6.1.2 初回入室時及び最終退室時の記録をオフィスセキュリティ管理責任者等が確認しなければならない。

＜細則＞

(1) オフィスセキュリティ管理責任者もしくは規程類で定める管理責任者が、定期的に入退室の記録を確認すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 月１回以上確認することが望ましい。

(2) テナントビルで、初回入室及び最終入室の記録がビル側でとられている場合、その記録を確認することが望ましい。

6.2 点検

6.2.1 オフィスセキュリティに関する点検を行わなければならない。

＜細則＞

(1) 部門の責任者等が、定期的にオフィスセキュリティの対策及び運用状況に関する部門内の点検を行うこと。

(2) オフィスセキュリティ管理責任者又は規程類で定める管理責任者が、定期的にオフィスセキュリティに関する全般的な点検を行うこと。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 部門内の点検は、月１回以上行うことが望ましい。

(2) 全般的な点検は、年１回以上行うことが望ましい。

（注）点検は、オフィスセキュリティコーディネータに依頼することができる。

6.3 監査

6.3.1 オフィスセキュリティに関する内部監査を行わなければならない。

＜細則＞

(1) 経営者が委嘱するオフィスセキュリティ管理責任者以外の者が、定期的に全般的なオフィスセキュリティに関する内部監査を実施すること。

(2) 内部監査については、基本方針、管理規程等が遵守され、オフィスセキュリティマーク認証基準に適合していることを確認すること。

(3) 監査の結果は、経営者に報告すること。

(4) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 内部監査は、年１回以上、行うことが望ましい。

（注）内部監査は、オフィスセキュリティコーディネータに依頼することができる。

7. 維持・改善

7.1 経営者による見直し

7.1.1 経営者は、オフィスセキュリティ全般について、必要に応じて見直さなければならない。

＜細則＞

(1) 経営者は、オフィスセキュリティ全般について必要に応じて見直しを行い、改善すること。

(2) 経営者は、監査報告を受け、課題があればその見直しを行い、改善すること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

7.2 維持及び継続的改善

7.2.1 オフィスセキュリティマネジメントシステムを維持し、かつ継続的に改善しなければならない。

＜細則＞

(1) オフィスセキュリティマネジメントシステムを維持し、かつ継続的に改善すること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

（注）オフィスセキュリティマネジメントシステムの維持及び継続的な改善の支援を、オフィスセキュリティコーディネータに依頼することができる。

7.2.2 オフィスセキュリティに係る重大な事象が発生した場合の報告体制を整備し、必要に応じて改善策をとらなければならない。

＜細則＞

(1) 申請組織において、事件、事故又は違反等が発生した場合、従業員は速やかにオフィスセキュリティ管理責任者へ書面にて報告すること。オフィスセキュリティ管理責任者は、報告に基づいて必要な対策を講じること。

(2) 申請組織の外部において、事件、事故又は違反等が発生した場合、及びオフィスセキュリティに関連する法律、公的なガイドラインの施行又は改正があった場合等は、オフィスセ

キュリティ管理責任者は必要な対策を講じること。

(3) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

7.3 事業継続管理

7.3.1 事件、事故、違反及び災害等により重要度の高い保護対象資産が漏えい又は損失した場合、事業の継続を可能とする方策をとらなければならない。

＜細則＞

(1) 事件、事故、違反及び災害等により、重要度の高い保護対象資産が漏えい又は損失した場合の対応策を定めること。

(2) オフィスセキュリティ管理規程又はそれに準じる規程類にその旨を明記すること。

＜推奨＞

(1) 重要度の高い書類等の保護対象資産は、バックアップをとることが望ましい。

(2) バックアップをとった保護対象資産は、高次のセキュリティレベルのエリア又はセキュリティを確保した外部で、保管・保存することが望ましい。

(3) 重要度の高い保護対象資産は、損害保険をかけることが望ましい。

(4) ＢＣＰ（事業継続計画）を立案することが望ましい。

（注）ＢＣＰについては内閣府の「事業継続ガイドライン」(http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf) や、中小企業庁の「中小企業ＢＣＰ策定運用指針」(http://www.chusho.meti.go.jp/bcp/index.html)を参考にすることができる。

附則

この認証基準は、2009 年 2 月 1 日に公示し、2009 年 10 月 1 日から施行する。