オフィスセキュリティマーク認証基準チェックシート

記入要領（Ver.3.0）

第1節　チェックシートの構成と記入方法

チェックシートは、申請組織が認証を取得しようとする際に、認証基準の要件を満たしているかをチェックし、すべて充足していることを証明するためのリストであり、認証取得のために必須かつ最重要な提出物である。

この記入要領では、チェックシートがどのような構成でできているかを示したうえで、記入の方法を説明する。そして、認証基準の適合を証明するプロセスを充分に理解できるように、チェックの際に必要な確認方法の一覧表とチェックシートの記入例を掲載している。さらに、チェックシートは認証取得時に申請書類として用いるばかりでなく、申請業務支援の始まる時点から運用中の点検･監査にいたるまで、さまざまに活用できることを記している。

このチェックシート及び記入要領は、認証基準への適合を見際める際の極めて役に立つツールであり、コーディネータはこの要点を習熟し、申請業務支援はもとより、オフィスセキュリティ対策の課題を明確にして、その改善を図るさまざまなコンサルティングの業務にも活用できる。

なお、チェックシートそのものは本マニュアルに掲載せず、付属のCD-Rに収録している。

1-1 チェックシートの構成

チェックシートは次の７つの項目に大別されている。

1. 申請組織の適合性
2. 申請組織の単位
3. 申請組織の状態
4. 計画・構築
5. 導入・運用
6. 点検・監査
7. 維持・改善

この中で、4.～7.は、認証基準の番号に合致している。すなわち、認証基準の「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」という規定を、チェックシートでは、「4.1.1　オフィスセキュリティ基本方針が文書化されている」ことをチェックする文言になっている。

チェックシートは62項目のチェック項目からなり、認証基準をすべて網羅している。

チェック項目ごとの構成は次の通りである（図表4-1）。

① それぞれのチェック項目は、太枠で囲って記載されている。その冒頭には□のマークがある。

② 枠の下には、そのチェック項目を充足するための条件が列記されている。それらの冒頭には□または○のマークが付いている。この条件の項目は、認証基準の細則に従っている。

③ さらにその下に、確認内容のコメントを記入する欄として、確認方法･対象、特記事項の項目が破線の枠で囲まれて記載されている。

④ チェック項目によっては、注）として、チェックにあたっての留意事項や参考事例を示している。

図表4-1　チェックシートの項目例

□ 4.1.4 オフィスセキュリティ基本方針が従業員に対して周知されている。

□　従業員に対するオフィスセキュリティ基本方針の周知の方法が、下記のいずれかであることを確認した。

○　文書配布

○　グループウェアやイントラネットによる配信

○　掲示

○　その他（周知の方法を特記事項に記載）

□　オフィスセキュリティ基本方針が、従業員に対して周知されていることを、ヒアリングで確認した。

注）ヒアリングにあたっては、小･中規模の申請組織は３人程度、大規模の申請組織は６人程度のサンプル調査にて確認を行うこと。

□　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していることを確認した。

確認方法･対象：□文書確認（　　）

□ヒアリング（　　）

特記事項：

1-2 チェックシートの記入方法

チェックシートの記入は、次のような手順で行う。

① まず、太枠の下のチェック項目を充足するための条件の項に着目する。

② 条件の項の□のマークの付いた項の記入は必須であり、すべての項にチェックの✓印を入れる必要がある。文書確認、ヒアリング、現場確認のいずれかの方法によって確認し、適合している場合は✓印を入れる。

③ 条件の項の○のマークの付いた項の記入は選択であり、いずれかの適合する項にチェックの✓印を入れる必要がある。２つ以上の項が適合していれば、複数の項に✓印を入れる。

④ このようにして、条件の項に必要とする✓印がすべて入れば、チェック項目の条件が充足していることになり、太枠で囲んだチェック項目の□にチェックの✓印を入れることができる。

⑤ なお、チェック項目や条件の項に、該当するものがない場合や適合することがない場合は、そのチェック項目や条件の項の□に、✓印の代わりに✕印を記入する。

例えば、セキュリティレベル１、２エリアが存在しない場合、セキュリティレベル３エリアの居室または保管庫・キャビネット等が存在しない場合、共用の鍵がない場合、外部委託先がない場合、保護対象資産を外部倉庫に保管･保存していない場合などのケースである。

⑥ 破線の枠で囲まれた確認内容を記載するコメント欄には、次のように記入する。

「確認方法･対象」：

□文書確認　□ヒアリング　□現場確認のいずれか、又は複数が記載されているので、その方法によって確認し、✓印を入れる。

文書確認は、管理規程を始め、基本方針、台帳、記録などによって、記載の有無や記載の内容を確認する。その文書名を（　　）の中に記入する。

ヒアリングは、オフィスセキュリティ管理責任者あるいは従業員の何人かに聞き取り確認を行う。その対象者を（　　）の中に記入する。従業員の場合は、確認相手の職位・氏名を、多人数の場合は代表者の職位・氏名及び人数を記入する。

現場確認は、申請エリア内のさまざまな状況を目視や接触することによって確認する。（　　）の中に、その室名と出入口や通路周辺、デスク周りなどの確認した場所、保管庫・キャビネット等の名称と数、設置場所などを記入する。保管庫・キャビネット等の名称は、保管庫、ファイリングキャビネット、耐火キャビネット、金庫などと記入する。

チェック項目ごとの確認方法は、図表4-3で一覧できるようになっている。

「特記事項」:

条件の項で、（　　）に指摘している事項を記入する。あるいは付記する事項、例えば、確認した詳細や写真を別添した場合などについて、必要に応じて記入する。

⑦ チェックシートの□のすべての項目、○のいずれかの項目について、確認した✓印(または、×印)を入れ、確認内容のコメント欄にすべて記入すれば、次に進む。

⑧ 次項に示すように、「オフィスセキュリティ認証基準チェックシート」の表書きを行って、完了する。

1-3 チェックシートへの署名･捺印

チェックシートの記入がすべて終わると、チェックシートの表紙である様式OSM-131-2.0「オフィスセキュリティ認証基準チェックシート」に記入し捺印を行う（図表4-2）。

申請組織の代表者は、原則としてオフィスセキュリティ最高責任者とする。代表者氏名は、必ずしも自署でなくてもよい。

コーディネータは、登録番号を記入のうえ、自筆で署名する。

確認年月日は、チェックシートに基づく確認作業の実施日を記載する。複数回にわたって実施した場合は、すべての実施日を記載する

図表 4-2　オフィスセキュリティマーク認証基準チェックシートの表紙

様式 OSM-131

オフィスセキュリティマーク認証基準チェックシート

一般社団法人ニューオフィス推進協会　御中

２０＿＿年＿＿月＿＿日

申 請 組 織

フ リ ガ ナ
名　　称 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

代表者役職 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

フ リ ガ ナ
代表者氏名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ ㊞

オフィスセキュリティコーディネータ

フ リ ガ ナ
氏　　名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ ㊞

登 録 番 号 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

確認年月日：20　　年　　月　　日

20　　年　　月　　日

オフィスセキュリティマーク認証申請にあたり、オフィスセキュリティマーク認証基準チェックシートに記載の条件をすべて満たしていることを確認し、申請します。

1-4 チェックシートの活用方法

チェックシート及びこの記入要領は、認証申請に必要な書類の作成に用いる以外に、次に記すようなさまざまな段階で活用することができる。

① 認証取得の申請をしようとする組織への提案や説明段階に活用する。
認証基準によって認証取得に必要な対策の概要を説明するとともに、その対策を講じた後には確認作業を行うことを説明するために、チェックシートや確認方法の一覧表を用いる。

② オフィスセキュリティ対策の計画の与条件や進捗管理に用いる。
認証基準に規定する対策の具体化の判断や計画・構築の進捗把握のために、✓印を記入して管理する。

③ 確認方法のリストは、効率よく確認作業を行うために用いる。
例えば、ヒアリング対象者に何回もヒアリングを繰り返すわけにはいかないので、同じ相手に聞くべき項目をリストから洗い出す。

④ 運用中の点検や内部監査の際に、認証基準に沿った運用が継続されているか、不適合な項目はないかをチェクするリストとして用いる。

第2節　チェックシートの確認方法と記入例

2-1 チェックシートの確認方法

チェックシートに基づいて確認する方法は、文書確認、ヒアリング、現場確認がある。図表4-3は各項目をいずれの方法で確認するかを一覧表にしたものである。

図表4-3　チェックシートの確認方法

大項目	中項目	項目	文書確認		ヒアリング		現場確認	その他の確認文書
			OS管理規程	その他	OS管理責任者	従業員		
1　申請組織の適合性		1		○	○			登記簿謄本、公的書類
2　申請組織の単位		1		○				組織図等
3　申請組織の状態		1		○				従業員名簿等
		2		○				登記簿謄本、賃貸借契約書等
4　計画・構築	1　オフィスセキュリティ基本方針	1		○				オフィスセキュリティ基本方針
		2		○				オフィスセキュリティ基本方針
		3		○				オフィスセキュリティ基本方針
		4	○	○		○		文書、配信データ、掲示物
		5	○	○	○			オフィスセキュリティ基本方針
	2　オフィスセキュリティ管理体制	1	○	○				管理体制図等
		2	○		○			
		3	○	○	○			管理体制図等
	3　オフィスセキュリティ管理規程	1	○					
		2	○					
		3	○					
		4	○	○		○		文書、配信データ、掲示物
		5	○		○			
	4　保護対象資産の分類及び保管・保存	1	○	○				重要度別資産管理台帳
		2	○					
		3	○	○	○			重要度別資産管理台帳
		4	○				○	
	5　エリアのレベル設定	1	○	○	○		○	OSM現状図面、OSM申請図面、アクセス権限管理台帳
		2					○	
		3	○		○		○	
		4	○	○	○		○	アクセス記録台帳
		5		○				OSM現状図面
		6	○					
	6　エリアにおけるセキュリティ対策	1	○					
		2	○					
		3					○	
		4					○	
5　導入・運用	1　従業員等の管理	1	○	○				秘密保持契約書、就業規則等
		2	○	○		○		従業員教育実施計画、記録
		3	○			○		
		4	○					
	2　重要度2以上の保護対象資産の管理	1	○					
		2	○				○	
		3	○			○		
	3　書類及び電子媒体等の管理	1	○	○			○	重要度別資産管理台帳
		2	○		○			
		3	○		○			
	4　情報通信機器及び装置等の管理	1	○		○		○	
		2	○		○	○	○	
		3					○	
	5　情報通信システム等の管理	1	○		○			
		2	○		○			
		3	○		○			
		4	○		○			
		5	○		○			
	6　鍵の管理	1	○	○	○	○	○	鍵管理台帳
		2	○		○			
	7　配送物の管理	1	○		○		○	
	8　外部委託先等の管理	1	○	○	○			外部委託先等管理台帳
	9　外部保管・保存の管理	1	○	○	○			業務委託契約書等
6　点検・監査	1　入退室記録	1	○	○				入退室記録
		2	○		○			
	2　点検	1	○	○	○			点検記録
	3　監査	1	○	○	○			内部監査記録
7　維持・改善	1　経営者による見直し	2	○	○	○			見直し記録
	2　維持及び継続的改善	1	○		○			
		2	○		○			
	3　事業継続管理	1	○		○			
計			50	27	30	7	14	
			77		37		14	

注）OS管理責任者：オフィスセキュリティ管理責任者
　　OS管理規程：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
　　OSM現状図面：オフィスセキュリティマーク現状図面
　　OSM申請図面：オフィスセキュリティマーク申請図面

2-2 チェックシートの記入例

チェックシート記入の際の参考として、いくつかの項目について記入例を示す（図表4-4）。

図表4-4　チェックシートの記入例

1. 申請組織の適合性

☑ 1.1 申請組織の実在及び適合性を確認する。

☑ 申請組織の実在を登記簿謄本、又は定款などの公的書類で確認した。

☑ 申請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を、文書で確認した。

☑ 申請組織は次の欠格事項に該当していない組織であることを、ヒアリングで確認した。

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、協会が不適当と判断した組織。

確認方法･対象：☑文書確認（（株）○○　登記簿謄本）
☑ヒアリング（オフィスセキュリティ管理責任者）
特記事項：

2. 申請組織の単位

☑ 2.1 申請単位は、全社、事業所又は部門等であることを確認する。

☑ 申請単位は、下記のいずれかであることを、組織図等で確認した。

○ 全社

☑ 事業所

○ 部門

○ その他（申請単位を特記事項に記載）

確認方法･対象：☑文書確認（（株）○○　組織図）
特記事項：

3. 申請組織の状態

☑ 3.1 申請組織の従業員数を確認する。

☑ 申請組織の申請エリア内で働く現状の従業員数を、従業員名簿等で確認した。

注）従業員数に、業務委託先の者は含めず、業務繁忙期等の臨時雇用者も含めない。
その他特殊事情がある場合は、現状ではなく通常期の人数とする。

確認方法･対象：☑文書確認（（株）○○　△△支社□□営業所　平成××年度従業員名簿）
特記事項：

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が文書化されている。

☑ 文書化されたオフィスセキュリティ基本方針を、下記のいずれかの文書で確認した。

○ 単独の基本方針

○ オフィスセキュリティ管理規程に含まれる基本方針

☑ その他（文書名を特記事項に記載）

確認方法：☑文書確認

特記事項：（株）○○　企業セキュリティ基本方針の中に記載されていることを確認した。

☑4.1.4 オフィスセキュリティ基本方針が従業員に対して周知されている。

☑ 従業員に対するオフィスセキュリティ基本方針の周知の方法が、下記のいずれかであることを確認した。

○ 文書配布

☑ グループウェアやイントラネットによる配信

☑ 掲示

○ その他（周知方法を特記事項に記載）

☑ オフィスセキュリティ基本方針が、従業員に対して周知されていることを、ヒアリングで確認した。

注）ヒアリングにあたっては、小･中規模の申請組織は３人程度、大規模の申請組織は６人程度のサンプル調査にて確認を行うこと。

☑ 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していることを確認した。

確認方法･対象：☑文書確認（オフィスセキュリティ管理規程）

☑ヒアリング（営業課○○課長　他3名）

特記事項：

☑4.1.5 オフィスセキュリティ基本方針が必要に応じて見直しされている。

☑ 下記のいずれかであることを確認した。

○ オフィスセキュリティ基本方針が必要に応じて見直しされており、その改訂内容が経営者によって承認され､署名又は承認印によって明らかになっている｡(承認手段を特記事項に記載)

☑ オフィスセキュリティ基本方針を作成して短期間であるので、見直しされていない。

☑ 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していることを確認した。

確認方法･対象：☑文書確認（オフィスセキュリティ管理規程）

☑ヒアリング（オフィスセキュリティ管理責任者）

特記事項：

4.4 保護対象資産の分類及び保管・保存

☑4.4.4 保護対象資産が、その重要度に応じたセキュリティエリアに保管・保存されている。

☑ 保護対象資産の保管・保存の状態が、次の通りであることを確認した。

a) 重要度１の保護対象資産が、セキュリティレベル１以上のエリアに保管・保存されている。

b) 重要度２の保護対象資産が、セキュリティレベル２以上のエリアに保管・保存されている。

c) 重要度３の保護対象資産が、セキュリティレベル３エリアに保管・保存されている。

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の保護対象資産が、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・保存されている。

注）現場確認にあたっては、小･中規模の申請組織は 10 件程度、大規模の申請組織は 20 件程度のサンプル調査にて確認を行うこと。

☑ 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が明記されていることを確認した。

確認方法･対象：☑現場確認（セキュリティレベル１エリアの執務室には重要度１の報告書など、セキュリティレベル２エリアの５つの保管庫には重要度２の経理伝票、提案書など、セキュリティレベル３エリアの２つの保管庫には重要度３の顧客情報、社印などの保護対象資産が保管されている。）

☑文書確認（オフィスセキュリティ管理規程）

特記事項：12件のサンプル調査の詳細は別紙「保護対象資産の保管･保存調査」に記載している。

4.5 エリアのレベル設定

☑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ある。

☑ 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を確認した。

☑ セキュリティレベル１エリアの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、下記のいずれかの抑止機能があることを確認した。

☑ 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。かつ出入口は、アクセス権限者の監視下にある。(動線の制限方法を特記事項に記載)

注 1）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。かつ、目につきやすい場所に表示されていること。(表示の表現を特記事項に記載)

注 2）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。(監視カメラ等を設置している場合は特記事項に記載)

○ 出入口の戸が常時開錠で、無断入室禁止表示等がある。

注） 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。かつ、目につきやすい場

所に表示されていること。(表示の表現を特記事項に記載)

○　受付担当者又は警備員等を配置している。受付担当者又は警備員等の不在時には、上記 2 通りのいずれかの状態である。

確認方法･対象：☑現場確認（執務室）

特記事項：出入口はパーティションにより動線を制限していることを確認した。無断入室禁止表示は「許可のない方の入室はお断りします」と適正に表示されていることを確認した。

☑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・キャビネット等である。

(セキュリティレベル２エリアの居室等の条件)

☒　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次の通り堅牢であることを確認した。

a) 境界の壁は天井まで密閉され、容易に移動、倒壊しない、又は破壊されないようになっている。

b) 境界の戸やシャッター等は密閉できる。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である。(密閉されてない場合は、外部から容易に侵入できない状態を特記事項に記載)

☒　セキュリティレベル２エリアの居室等の出入口は、下記のいずれかであることを、アクセスの権限者についてはヒアリングで、施錠状態は現場で確認した。

○　常時施錠しており、アクセス権限者のみが開錠している。

○　施錠しており、アクセス権限者のみが開錠しているが、アクセス権限者の監視下にある場合に限り、施錠していない。

☒　セキュリティレベル２エリアの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していることをヒアリングで確認した。

確認方法･対象：☒ヒアリング（　　）
☒現場確認（　　）

特記事項：

☒　セキュリティレベル２エリアに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ていることを、ヒアリングで確認した。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が明記されていることを確認した。

確認方法･対象：☒文書確認（　　）
☒ヒアリング（　　）

特記事項：

(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)

☑　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を確認した。

☑　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、壁又は床に固定されている、前後左右に連結する等の対策がとられている、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を確認した。(持ち出しできない対策を特記

事項に記載）

☑ 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、下記のいずれかであることを、アクセスの権限者についてはヒアリングで、施錠状態は現場で確認した。

○ 常時施錠しており、アクセス権限者のみが解錠している。

☑ 施錠しており、アクセス権限者のみが解錠しているが、アクセス権限者の監視下にある場合に限り、施錠していない。

確認方法･対象：☑ヒアリング（オフィスセキュリティ管理責任者）
☑現場確認（５つの保管庫がセキュリティレベル１エリアの中にある）
特記事項：壁及び床に固定していることを確認した。

5. 導入・運用

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が適切に行われている。

☑ 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、情報管理対策が講じられていることを確認した。(出力等を行う装置の情報管理対策を特記事項に記載)

☑ 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、運用上の対策が講じられていることを、ヒアリングで確認した。

☑ 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が明記されていることを確認した。

確認方法･対象：☑文書確認（オフィスセキュリティ管理規程）
☑ヒアリング（オフィスセキュリティ管理責任者）
☑現場確認（オープンエリア、セキュリティレベル1エリアの執務室内とその出入口近辺）
特記事項：出力等を行う装置は、オープンエリア、セキュリティレベル1エリアの執務室の出入口近辺には設置していないこと､その設置場所に出力物を放置していないことを確認した。

5.5 情報通信システム等の管理

☑ 5.5.1 アクセス管理等が適切に行われている。

☑ ユーザーＩＤ及びパスワードの管理方法が明確にされ、その遵守の状態が適切に管理されていることを確認した。(アクセス管理方法の要点を特記事項に記載)

☑ 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が明記されていることを確認した。

確認方法･対象：☑文書確認（オフィスセキュリティ管理規程）
☑ヒアリング（オフィスセキュリティ管理責任者）

特記事項：情報システムを利用する従業員に対して、アクセス権限を設定し、固有のユーザーＩＤを割り振っていること､および人事異動等に際しては､速やかにユーザーＩＤを変更していることを確認した。また、推測されにくいパスワード設定していることを確認した。