

特別認証：日経ニューオフィス賞に応募された組織の
オフィスセキュリティマーク認証取得について

手続きと、申請時提出必要書類



1.特別認証：「オフィスセキュリティマーク」認証取得 今後の手続きについて



この度は、「オフィスセキュリティマーク」認証取得を希望いただきまして、誠にありがとうございます。
以下に、進め方についてご説明させていただきます。

(1) 申請期間：毎年9月1日～3月31日（必着）まで

(2)認証申請書類の提出

- ・ 認証申請書類(以下、申請書類)を作成の上、当協会に送付してください(送付先は下記)。
- ・ 提出必要書類につきましては、2ページ以降をご覧ください。
- ・ 当協会にて、送付いただいた書類が完備していることを確認の上、受理いたします。

(3)認証審査の実施

- ・ 当協会にて申請書類受領後、認証審査（認証委員会にて）を実施し認証可否を決定いたします。
- ・ 認証審査は、申請書類受領後1～3か月程度かかります。（申請企業数による）
- ・ 特別認証は書類審査のみとなります。
ただし、申請書類で条件を満たしていない箇所があったときは、再提出（または現地確認）をお願いする場合があります。

(4)認証審査結果の通知

- ・ 認証可否決定後、当協会より認証結果を連絡いたします。

(5)認証取得費用に関して

- ・ 今回、認証申請費用及び審査費用はかかりませんが、使用許諾関連費用※（約1万円）が発生いたします。
※認証取得関連費用：オフィスセキュリティマーク使用許諾証・認証盾の制作費用及び発送費用
- ・ 認証後、内訳・請求書を送付。入金確認後、発送の手続きをさせていただきます。

※尚、認証審査結果後の申請の取り消しはできませんのでご注意ください。

(6)申請書類の提出先及び資料作成のご相談・お問合せは下記

提出・お問合せ先

〒104-0043 東京都中央区湊2-4-1 TOMACビル3階

一般社団法人 ニューオフィス推進協会 オフィスセキュリティマーク事務局 藤原・北村

電話：03-3553-3471

HP：<https://www.nopa.or.jp/>

申請時提出必要書類は、下記5点となります。

(1)オフィスセキュリティマーク認証申請書

- ・HPより「オフィスセキュリティマーク認証申請書(特別認証用)」をダウンロードしていただき、必要事項を記入の上、押印下さい。

(2)登記簿の謄本又は抄本（履歴事項証明書）

(3)会社概要

- ・書式は問いません。会社案内でも可です。

※以下の(4)・(5)は、4ページ以降で詳細説明致します。

(4)オフィスセキュリティ基本方針（添付③ひな形）

- ・書式は問いません。
- ・押印をお願い致します。

(5)申請組織が実施している『オフィスにおける経営資産の適切な保護策』について

※日経ニューオフィス賞応募時に作成した書式2－5を参考に具体的に記載して下さい。

- ・**オフィスセキュリティマーク認証基準と同程度又はそれ以上の効果的、かつ実現可能なセキュリティ対策が具体的に示されている『オフィスにおける経営資産の適切な保護策』の提出をお願い致します。**
- ・書式は問いませんが、A4またはA3サイズにて、5枚程度でお願いします。

3. 認証申請書類： ③「オフィスセキュリティ基本方針」の例示



- 貴組織の「オフィスセキュリティ基本方針」または、同様のものを提出してください。
- 貴組織の様式で結構ですが、ご参考までにひな形を例示いたします。
- 必ず記名押印をお願いいたします。

様式 OSM-151

オフィスセキュリティ基本方針

株式会社〇〇〇〇は、事業の継続・発展と社会的責任を重視し、オフィスにおける重要な経営資産を保護することを目的として、効果的なオフィスセキュリティ対策を実施して安全な状態を創出し、維持することを目標とします。

- 1. 重要な経営資産の保護**
経営資産は、その重要度に応じて適切に取り扱い、事件、事故、違反または災害等による損失または漏えい等のリスクから保護します。
- 2. 対策の設定と管理**
オフィスセキュリティの対策となる範囲を設定し、必要なセキュリティのレベルが確保されたエリアごとに適切な管理を行います。
- 3. 管理体制と管理規程の構築**
オフィスセキュリティの適切な管理を行うために、管理組織を編成して体制を構築し、管理規程を制定して履行します。
- 4. 全従業員の参加**
オフィスセキュリティについて、管理者は従業員の教育と指導を行い、従業員は十分に理解して適正な行動に努めます。
- 5. 点検および改善**
オフィスセキュリティの運用状況を定期的に点検・監査し、継続的な改善を行って安全な状態を維持します。

なお、当社はこのオフィスセキュリティ基本方針を外邦に対して開示いたします。(注)

20__年__月__日

株式会社 〇〇〇〇〇〇〇〇〇〇〇〇
代表取締役社長 〇〇〇〇

(注) 外邦への開示は推奨事項である。

オフィスセキュリティ基本方針ひな型

※日経ニューオフィス賞応募時に作成した書式2 - 5を参考に具体的に記載して下さい。

(1)提出形式：A4またはA3用紙 5枚程度

(2)作成ポイント

申請組織が実施しておられる、オフィスセキュリティマーク認証基準（※1）と同程度又はそれ以上の効果的、かつ実現可能なセキュリティ対策を下記例示に沿って具体的に明記をお願い致します。

参) ※1 → http://www.nopa.or.jp/security/pdf/osm_v4.pdf

記

例示(a)： P5 «オフィスセキュリティレベルの概要がわかる資料»

- ・セキュリティエリアごとのレベル分けがされたゾーニング図
- ・それぞれのセキュリティレベル（ゾーン）ごとに取り組んでいるセキュリティ対策
- ・従業員、部外者の識別管理手法について（社員証・社員バッチ・名札・制服等）
- ・入退室管理対策状況がわかるもの（認証器具：入退室管理・カード認証・ストラップ等）

例示(b)： P6 «具体的なセキュリティ対策»

- ・書類管理：重要度分類、保管体制について
- ・情報システム管理：重要度分類、管理対策（PC・サーバー・ウィルス・サイバー対応等）
- ・セキュリティに関する従業員の教育、研修計画や実施状況が分かるもの
- ・セキュリティ管理体制図
- ・BCPへの取り組み等

例示(c)： P7 «その他»

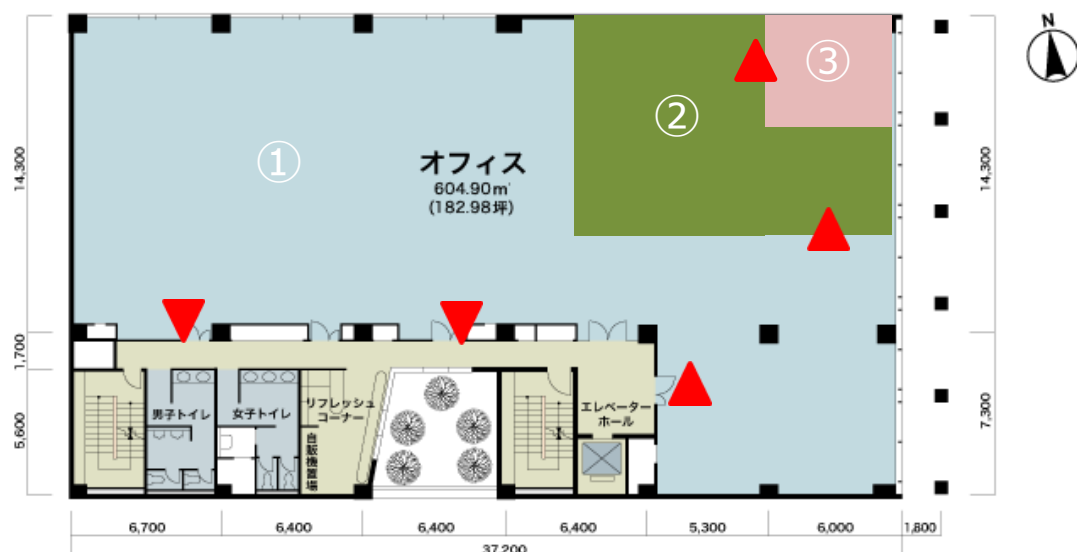
- ・プライバシーマーク、ISMS適合性評価制度の運用等、既に取り組まれておられる対策があれば記載をお願い致します。

2. 別図 (A) : オフィスセキュリティの範囲の設定等、セキュリティ対策の概要を示すもの

- ・セキュリティエリアごとのレベル分けがされたバッチカルゾーニング図、フロアゾーニング図
- ・それぞれのセキュリティレベル（ゾーン）ごとに取り組んでいるセキュリティ対策
- ・従業員、部外者の識別管理手法について（社員証・社員バッジ・名札・制服等）
- ・入退室管理について（入退室管理表・生体認証・カード認証・ストラップ等）

■ セキュリティエリアレベルのゾーニング図（例）

- ・セキュリティエリアごとのレベル分けがされた各フロアゾーニング図
- ・社員出入口の明示 ▲



- ③ ……セキュリティエリアレベル③
- ② ……セキュリティエリアレベル②
- ① ……セキュリティエリアレベル①
- ……オープンエリア

■ セキュリティゾーニング概要（例）

- ・それぞれのセキュリティエリアレベル（ゾーン）ごとに取り組んでいるセキュリティ対策を記載ください

- ③ ……各セキュリティエリアレベル3の説明
- ② ……各セキュリティエリアレベル2の説明
- ① ……各セキュリティエリアレベル1の説明
- ……オープンエリア

■ 入室管理対策状況がわかるもの

- ・入退室管理対策状況がわかるものを記載ください（生体認証・カード認証・ストラップ等）



2. 別図 (B) : 具体的な経営資産の保護策を示すもの

- ・書類等の重要度分類やアクセス権限などの分類・仕組み及び保管方法について
- ・情報システムに関するアクセス権限などの運用ルール・仕組みについて
- ・セキュリティに関する従業員の意識向上を図る教育やマニュアル・規程等の有無について
- ・セキュリティ対策を運営・維持するための管理体制図など
- ・BCPへの取組み等

■ 書類管理

- ・重要度分類の考え方、保管方法について記載ください



■ 情報システム管理

- ・重要度分類、アクセス権限の考え方
- ・情報セキュリティ管理規程・運用マニュアル等の有無



■ 社員教育

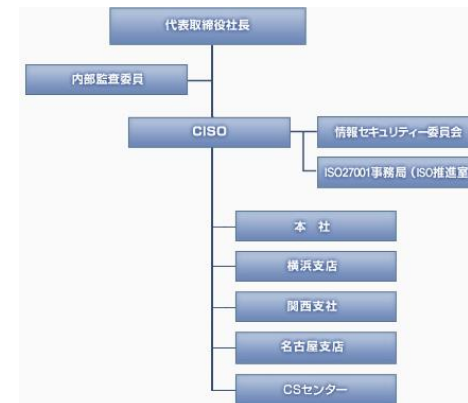
- ・セキュリティに関する従業員の教育・研修計画や実施状況を記載ください



〈セキュリティ社内研修会〉

■ 運営・維持するための管理体制図 BCPへの取組み等

- ・管理体制及び災害時の対策を記載ください



〈防災用品〉

2. 別図 (C) : その他

- ・ プライバシーマークの取得、ISMS適合性評価制度の運用等、①②以外で取り組んでいるものを示してください。



プライバシーマーク



I S M S 適合性評価制度

[目的]

一般社団法人ニューオフィス推進協会は、1987年以来、知的生産活動を担う場としてのオフィスを取り巻く諸問題に関する調査研究、情報の収集・提供、及びオフィス関連の人材の育成等を行い、日本経済新聞社と共催して日経ニューオフィス賞を実施し、我が国のオフィス環境の向上を図り、創造的なオフィスづくりの普及・啓発に努めて参りました。こうした中、我が国では情報通信社会の進展に伴って、情報漏えい事件が多発し社会問題となっています。また、個人情報保護法の施行、最近ではマイナンバー制度の施行などオフィスにおける経営資産である情報の保護に対する企業の社会的責任が求められ、その意識が高まっています。

本会ではオフィスセキュリティの重要性に着目し、経済産業省の指導のもと重点的に研究を進めることにより、オフィスにおけるセキュリティのあり方を示す認証基準を開発しました。オフィスセキュリティマーク認証制度は、企業や組織のオフィスにおけるセキュリティ対策の要請に応える制度として存在しています。

こうした背景の下、オフィスづくりにおいては効果的なオフィスセキュリティ対策を実施して安全な状態を創出することが求められています。そのため日経ニューオフィス賞では審査の視点の一つに知識資産や情報の適切な運用と管理を取り込み、オフィスづくりに欠かせないものとしています。

特別認証は、日経ニューオフィス賞に応募された方々に対し、応募組織のオフィスセキュリティが当協会が定めるオフィスセキュリティ認証基準と同程度又はそれ以上の効果的かつ実現可能なセキュリティ対策が具体的に示されている内容を認証委員会が行う評価に基づき、その申請によりオフィスセキュリティマークを付与するもので、我が国のオフィスづくりにおけるセキュリティの推進を図るものです。



3. (参考) オフィスセキュリティマーク認証制度概要

オフィスセキュリティマーク認証制度は、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、維持し、継続的に改善をはかる経営活動として、オフィスセキュリティマネジメントシステム（OSMS）を実施している組織に対して、一般社団法人ニューオフィス推進協会が定めるオフィスセキュリティマーク認証基準に基づいて、企業の経営資産が適切に保護されているかどうかの適合性を審査し、その基準を満たした組織に対しオフィスセキュリティマーク（OSM）の認証を付与する制度です。

1 計画・構築：

- ・ オフィスセキュリティ基本方針・管理規程・管理体制
- ・ 保護対象資産の重要度分類及び保管・エリアレベルの設定

2 導入・運用：

- ・ 従業員等の管理
- ・ 書類及び情報通信機器・システムの管理
- ・ 鍵の管理
- ・ 配送物の管理
- ・ 外部委託先等の管理

3 点検・監査：

- ・ 入退室記録
- ・ 点検・監査

4 維持・改善：

- ・ 経営者による見直し
- ・ 維持管理
- ・ 事業継続管理

