

## 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



---

今後の手続きと、申請時提出必要書類



# 1. 「オフィスセキュリティマーク」 認証取得 申請時提出必要書類について



(1)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

- ・「①オフィスセキュリティマーク認証申請書(特別認証用)」に必要事項を記入の上、押印ください。

**\*このホームページより、ダウンロードしてください。**

②登記簿の謄本又は抄本その他の申請組織の存在を証する公的書類

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、次ページ以降で詳細説明いたします。**

④オフィスセキュリティ基本方針

- ・書式は問いません。
- ・押印してください。

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。

- ・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。

(2)申請期間：2017年9月1日～2018年3月31日(必着)

(3)資料作成のご相談、お問合せは下記まで

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

TEL：03-3553-3471 FAX：03-3553-3470

E-mail：[akamatsu@nopa.or.jp](mailto:akamatsu@nopa.or.jp)(赤松) [sakuramachi@nopa.or.jp](mailto:sakuramachi@nopa.or.jp)(櫻町)

## 2. 「④オフィスセキュリティ基本方針」説明



- 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、下記のひな形が必要な場合は事務局までご連絡下さい。
- 押印してください。

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. 対象の設定と管理

オフィスセキュリティの対象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部に対して開示いたします。(注)

平成\_\_\_\_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) 外部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

下記項目を記載下さい(例示は5～7ページにあります)。

- ・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
- ・入退室管理対策状況がわかるもの(カード認証・ストラップ等)
  
- ・書類管理について、重要度分類、保管体制について
- ・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
- ・地震や災害対策への取り組み
- ・セキュリティ管理体制図等
  
- ・その他のセキュリティ対策
  - ・従業員の識別管理手法(社員証、社員バッジ、名札、制服等)
  - ・プライバシーマーク、ISMS適合性評価制度の運用等

## 4. 「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」の例示(a)

- ・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
- ・入退室管理対策状況がわかるもの（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

- ・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



- 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

- ・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の説明
- ② ……各セキュリティエリアレベルの説明
- ① ……各セキュリティエリアレベルの説明
- ……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（カード認証・ストラップ等）

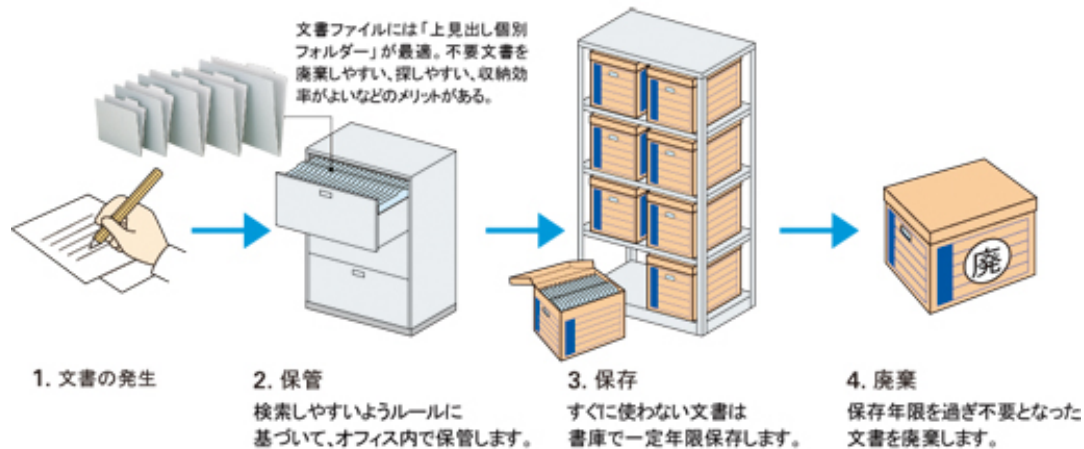


## 5. 「⑤申請組織が実施しているオフィスにおける経営資産の適切な保護策について」の例示(b)

- ・書類管理について、重要度分類、保管体制について
- ・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
- ・地震や災害対策への取り組み
- ・セキュリティ管理体制図等

### ■ 書類管理

- ・書類管理について重要度分類、保管方法について記載ください



### ■ 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



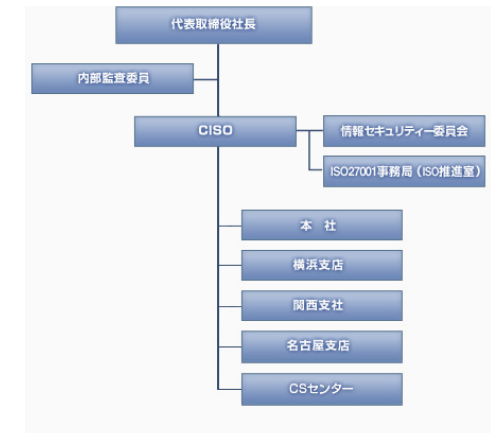
<セキュリティ社内研修会>

### ■ 地震や災害対策への取り組み

- ・災害時の対策や体制について記載ください



<防災用品>





## 6. 「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」の例示(c)

- ・その他の実施されているセキュリティ対策がありましたら、図及び文章でお書き下さい。



プライバシーマーク



I S M S 適合性評価制度

## 7. (参考) オフィスセキュリティマーク認証制度について

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：

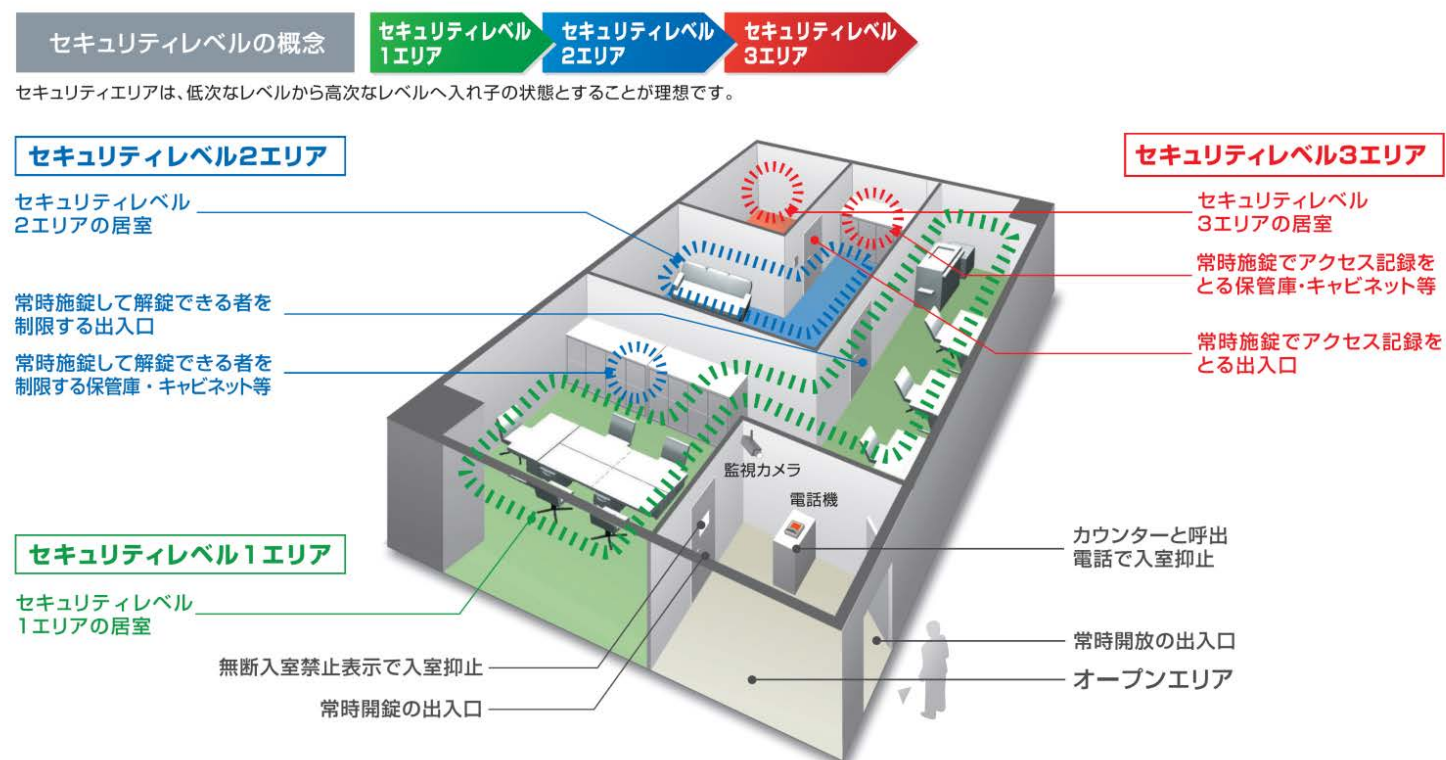
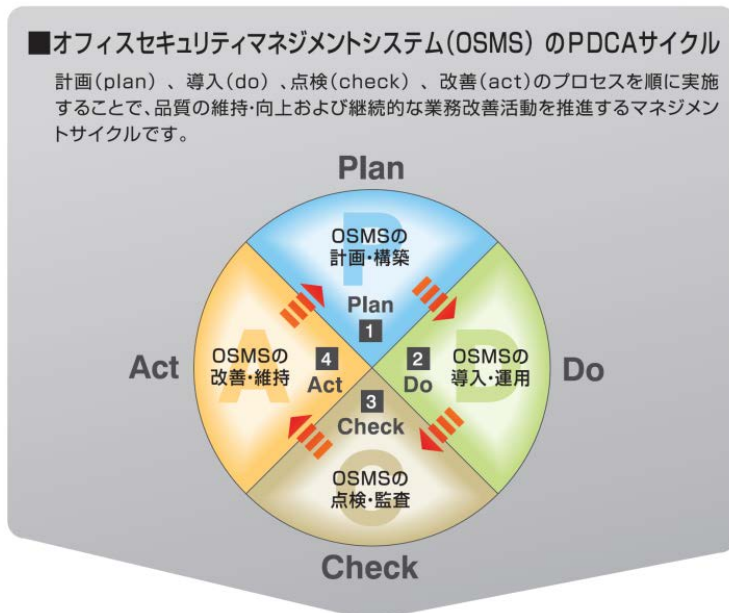
- ・ 従業員等の管理
- ・ 書類及び情報通信機器・システムの管理
- ・ 鍵の管理
- ・ 配送物の管理
- ・ 外部委託先等の管理

### 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





**OFFICE  
SECURITY**

