サイバーセキュリティ経営ガイドラインVer.3.0

- 経済産業省では、経営者にリーダーシップをとってサイバーセキュリティ対策を推進していただくため、**経営者を対象としたガイドライン**を策定しています。合わせて、ガイドライン**実践のためのプラクティス集**や、**セキュリティ対策の実施状況を可視化するツール**なども整備しています。

<サイバーセキュリティ経営ガイドライン（ポイント）>

1．経営者が認識すべき３原則

（1）経営者が、**リーダーシップを取って対策**を進めることが必要
（2）自社のみならず、**サプライチェーン全体にわたる対策**への目配り
（3）平時及び緊急時のいずれにおいても、**社内外関係者との積極的なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

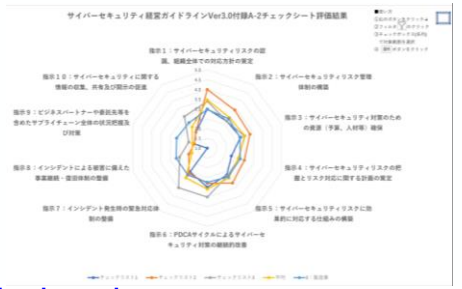
リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	**指示10** 情報収集、共有及び開示の促進

<サイバーセキュリティ経営ガイドラインVer3.0 実践のためのプラクティス集>

- **経営者**に加え、**CISO**、**セキュリティ担当者**を主な読者と想定し、実践事例に加え、セキュリティ担当者の**日常業務における悩みに対する具体的対応策を提示。**

<サイバーセキュリティ経営可視化ツール>

- 「サイバーセキュリティ経営ガイドライン」で定める重要10項目の実施状況を5段階の成熟モデルで可視化（レーダーチャート表示）

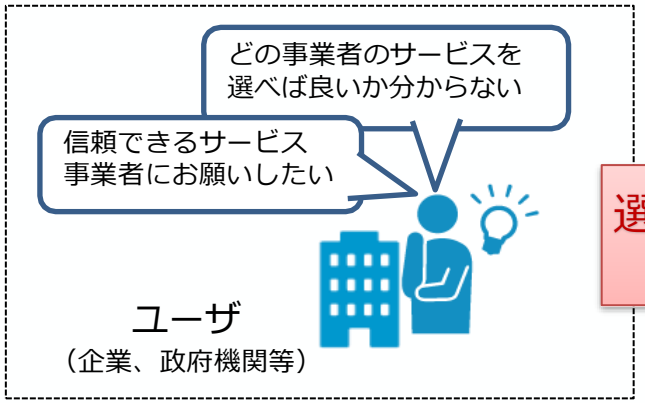


サイバーセキュリティ経営ガイドラインと支援ツール：https://www.meti.go.jp/policy/netsecurity/mng_guide.html

情報セキュリティサービス基準適合サービスリスト

- 経済産業省では、**「情報セキュリティサービス基準」を策定**し、審査登録機関による**審査をクリアしたサービスのリストを公開**※しています。※IPA（独立行政法人情報処理推進機構）が公開。
- 脆弱性診断やセキュリティ監査などのサービス（全5種、オプション1種）が対象になっており、これらのサービスを利用する際のサービス提供事業者の選定に本リストを活用いただけます。

＜情報セキュリティサービスにおける課題＞



選定時に活用

○情報セキュリティサービス基準適合サービスリスト（IPA）

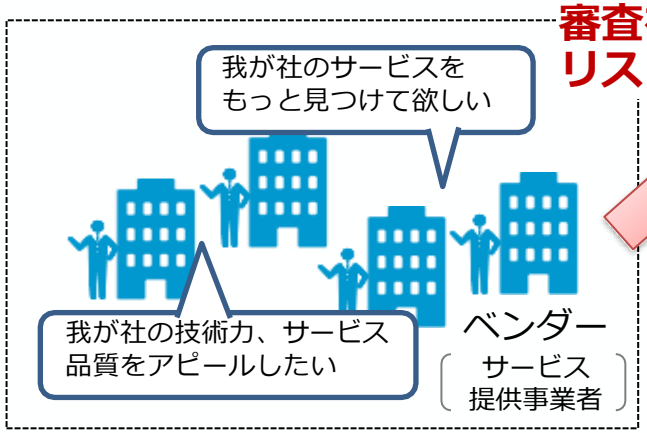
審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

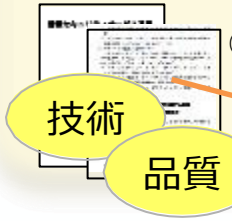
基準を満たした339サービスを掲載

- 情報セキュリティ監査（72サービス）
- 脆弱性診断（159サービス）
  うちペネトレーションテスト(侵入試験)あり(12サービス)
- デジタルフォレンジック（39サービス）
- セキュリティ監視・運用（52サービス）
- 機器検証 （17サービス）

2024年12月現在

審査を受けてリストに掲載





○情報セキュリティサービス基準（METI）

上記5サービス、1オプションに関して技術要件・品質管理要件を 定めた基準

本制度を通じて目指す社会

- **専門的知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる**
- **技術と品質を備えた情報セキュリティサービスの普及・発展**
- **制度の普及・浸透**

情報セキュリティサービス基準適合 サービスリスト：https://www.ipa.go.jp/security/service_list.html

IoT製品に対するセキュリティ適合性評価制度

- 経済産業省及びIPAでは、**IoT製品に対するセキュリティ適合性を評価**し、適合基準を満たすものについて、**ラベルを付与**する制度を、2025年3月※から**「JC-STAR（ジェーシースター）」**という制度名で開始します。　※2025年3月時点では最低限の適合基準（★１）についてのみ運用開始予定。
- 近年、IoT製品を狙ったサイバー攻撃が増加しているため、IoT製品の調達・購入・利用時には、本制度によるラベル取得の有無を確認し、セキュリティ要件を満たした安全なIoT製品を選びましょう。

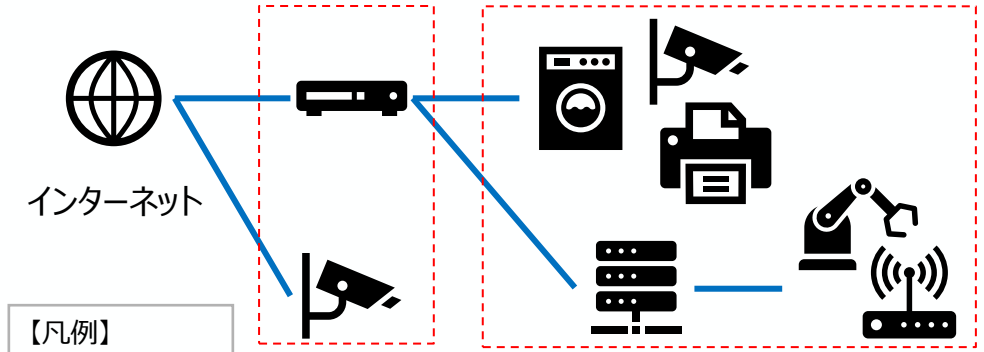
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

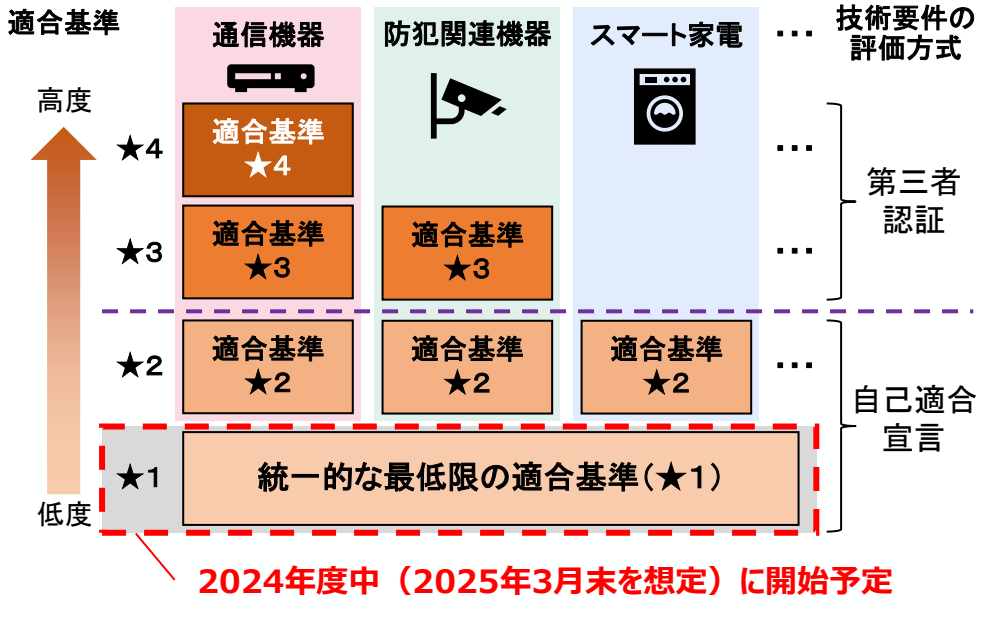
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



セキュリティ要件適合評価及びラベリング制度（JC-STAR）：https://www.ipa.go.jp/security/jc-star/index.html

サイバーセキュリティインシデント発生時の相談窓口

- サイバー攻撃又はその疑いにより、情報漏えい、ウイルス感染、システム停止などの**インシデントが発生した場合**、迅速な対応が必要です。
- 金銭被害、信用低下、事業停止等や関係者（顧客、取引先、従業員等）への**被害拡大を最小限に抑えられるよう**、警察への相談に加え、初動対応を支援する以下の**専門機関の活用**を検討ください。

独立行政法人情報処理推進機構（IPA）

- 不正アクセス等のインシデントに関する相談や届出、情報提供の受付：
  https://www.ipa.go.jp/security/todokede/incidentportal.html

（相談例）
- ランサムウェアに感染したため、対処方法について相談したい
- 普段の情報セキュリティの対策やIPAのセキュリティ施策について知りたい
- サイバー攻撃被害について、サイバー保険の適用を受けるために公的機関への届出を行いたい

一般社団法人JPCERTコーディネーションセンター

- インシデント初動対応（必要な調査、対応方針の検討、被害箇所の特定等）のサポートなどの依頼相談：

  https://www.jpcert.or.jp/form/

- インシデント対応に関する様々な相談、情報提供の受付：

  https://www.jpcert.or.jp/ir/consult.html

中小企業の情報セキュリティ対策ガイドライン第3.1版

- 経済産業省及びIPAでは、中小企業におけるセキュリティ対策を促進するため、**具体的な対策を示すガイドライン**を策定しています。**経営者編**と**実践編**から構成されており、個人事業主や小規模事業者を含む中小企業による活用を想定しています。
- ガイドラインの付録を活用した**「SECURITY ACTION」**は、**全ての企業に必ず実施していただきたいセキュリティ対策をまとめたもの**です。「SECURITY ACTION」を自己宣言することが、各種補助金の要件にもなっています。

＜中小企業の情報セキュリティガイドライン（ポイント）＞

- 中小企業の経営者や実務担当者が、情報セキュリティ**対策の必要性**を理解し、**情報を安全に管理**するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき**「3原則」**、経営者がやらなければならない**「重要7項目の取組」**を記載
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等の**ひな形**を付録
  - **「中小企業のためのセキュリティインシデント対応の手引き」**を追加

中小企業の情報セキュリティ対策ガイドライン：
https://www.ipa.go.jp/security/guide/sme/about.html

＜SECURITY ACTION＞

★一つ星

情報セキュリティ５か条に取り組む

【情報セキュリテイ５か条】

- OSやソフトウェアは常に最新の状態にしよう！
- ウイルス対策ソフトを導入しよう！
- パスワードを強化しよう！
- 共有設定を見直そう！
- 脅威や攻撃の手口を知ろう！

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

【基本方針の記載項目例】

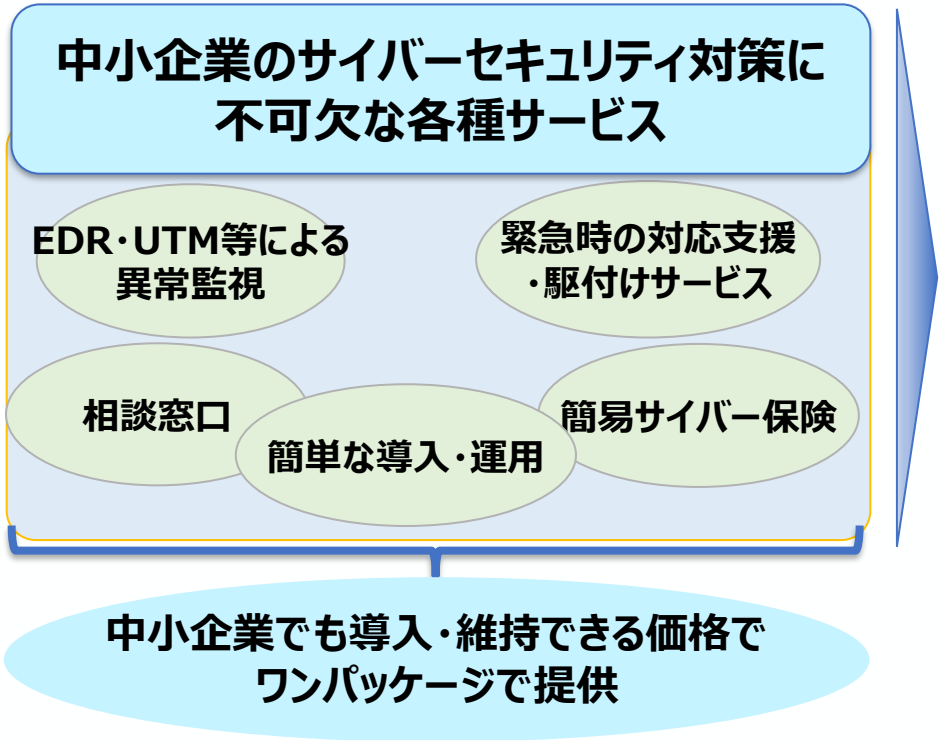
- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

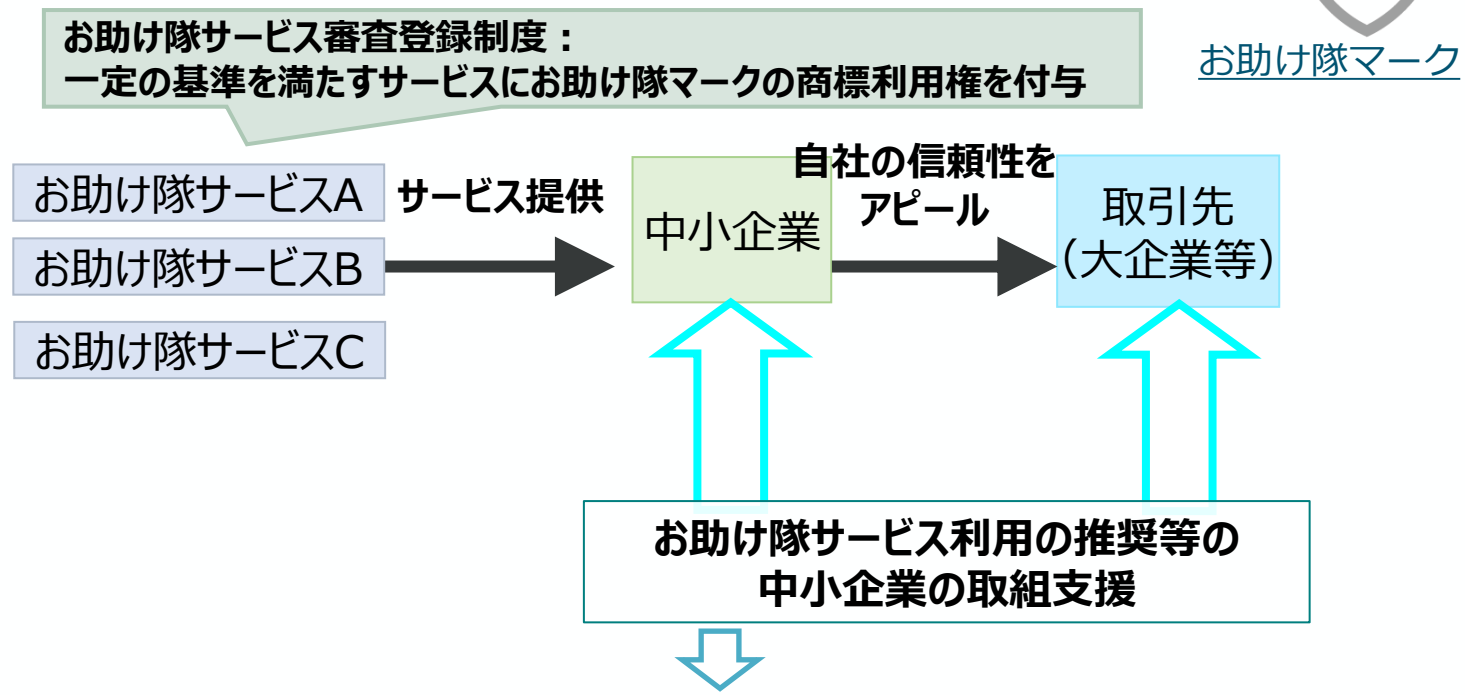
SECURITY ACTIONサイト：https://www.ipa.go.jp/security/security-action/

サイバーセキュリティお助け隊サービス

中小企業向け

- サイバーセキュリティお助け隊サービスは、**中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービスです。**IT導入補助金「セキュリティ対策推進枠」を活用することで、**費用の1/2（小規模事業者は2/3）の補助を受けられます。**





サイバーセキュリティお助け隊マーク

サイバーセキュリティお助け隊サービスの利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/