

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

- 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**
- 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**
- 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等へ指示すべき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。

図2-4.2 F社で想定したサイバー攻撃の事例とリスクの例

分類	攻撃手法	システム	被害発生可能性	被害発生影響	リスク
WEBサイト侵害	攻撃者からの不正アクセスによる情報の漏えい	情報管理サイト	低	低	1
	フィッシング攻撃による顧客情報の漏えい	ECサイト	有	中	2
システム障害	ランサムウェアによるデータの暗号化	社内サーバ	有	高	3
	DDoS攻撃によるサービスの停止	ECサイト	有	中	2
機密情報漏えい	不正アクセスによる顧客情報の漏えい	業務用PC	有	高	3
	不正アクセスによる顧客情報の漏えい	モバイル機器	有	中	2
その他	クラウドサービスへの不正アクセス	業務用PC	有	高	3
	脆弱性を利用したシステムの不正アクセス	社内サーバ	有	中	2

図2-4.1 F社で利用した被害発生可能性とリスクを算定する方法の例

被害発生可能性	被害発生影響	リスク	
		発生可能性	被害発生影響
高	高	2	3
中	中	1	2
低	低	1	1

<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）



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＞

どの事業者のサービスを選べば良いかわからない

信頼できるサービス事業者をお願いしたい

ユーザ
(企業、政府機関等)

選定時に活用

我が社のサービスをもっと見つけて欲しい

我が社の技術力、サービス品質をアピールしたい

ベンダー
サービス提供事業者

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

サービス名	事業者名	登録年月日	サービス種別	審査登録機関
脆弱性診断サービス	IPA 登録事業者	2024/12/12	脆弱性診断	IPA
セキュリティ監査サービス	IPA 登録事業者	2024/12/12	セキュリティ監査	IPA
デジタルフォレンジックサービス	IPA 登録事業者	2024/12/12	デジタルフォレンジック	IPA
セキュリティ監視・運用サービス	IPA 登録事業者	2024/12/12	セキュリティ監視・運用	IPA
機器検証サービス	IPA 登録事業者	2024/12/12	機器検証	IPA

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

○情報セキュリティサービス基準 (METI)

技術

品質

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

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

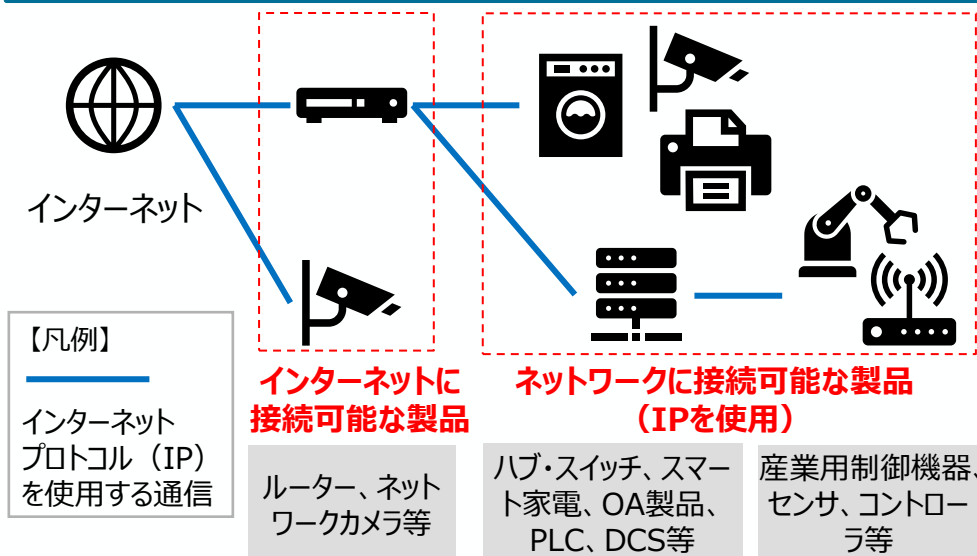
セキュリティ要件適合評価
及びラベリング制度

JC-STAR

(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

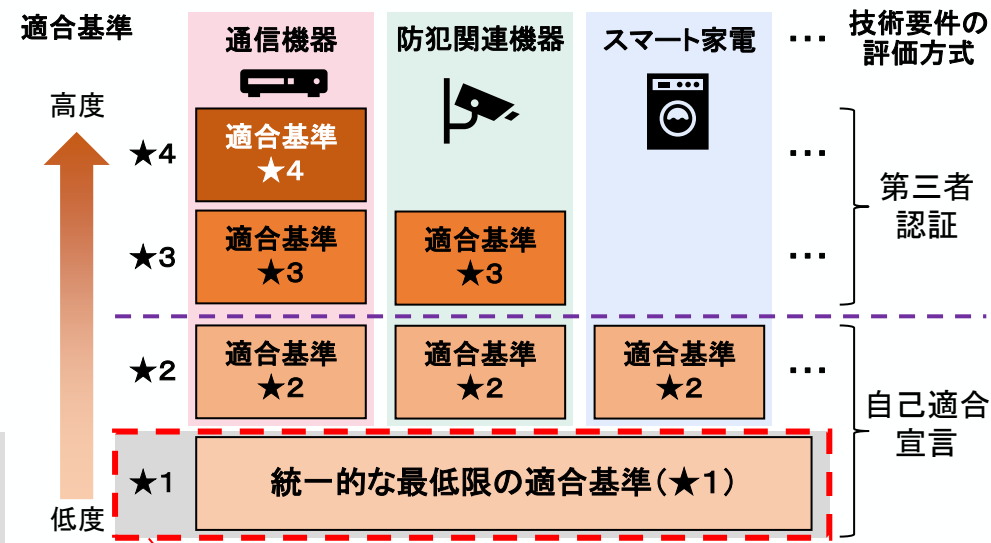


対象製品の概要



※ 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）



2024年度中（2025年3月末を想定）に開始予定

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



<SECURITY ACTION>



情報セキュリティ5か条
に取り組む

【情報セキュリティ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！



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

サイバーセキュリティお助け隊サービス

- 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。



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

EDR・UTM等による
異常監視

緊急時の対応支援
・駆付けサービス

相談窓口

簡単な導入・運用

簡易サイバー保険

中小企業でも導入・維持できる価格で
ワンパッケージで提供

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA

サービス提供

お助け隊サービスB

お助け隊サービスC

自社の信頼性を
アピール

中小企業

取引先
(大企業等)

お助け隊サービス利用の推奨等の
中小企業の取組支援

IT導入補助金に「セキュリティ推進枠」創設
(補助率：中小企業1/2、小規模事業者2/3 補助上限：150万円)