Canon

令和8年度末頃 制度開始 予定

# サプライチェーン強化に向けた セキュリティ対策評価制度

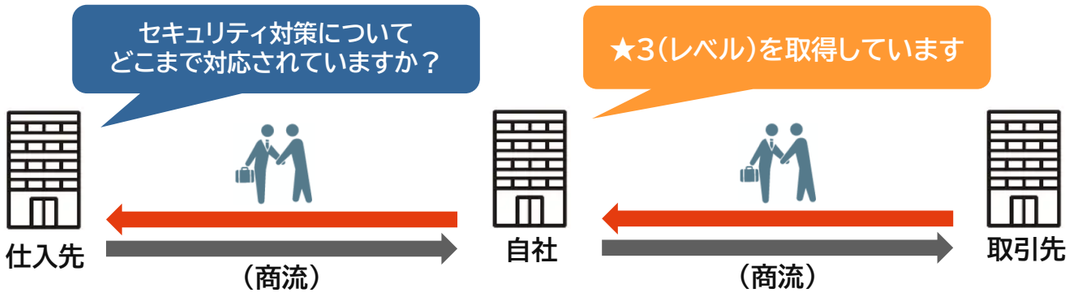
## セキュリティ対策評価制度（概要）

近年、サプライチェーンを狙ったサイバー攻撃が増加し、企業間取引において適切なセキュリティ対策の実施が重要となっています。こうした状況を踏まえ、経済産業省では、サプライチェーン全体のリスク低減とサイバー攻撃に強い体制の構築を目的として、企業のセキュリティ対策状況を可視化する「サプライチェーン強化に向けたセキュリティ対策評価制度」の検討を進めています。
本制度は、令和8年（2026年）度末頃の制度開始を予定しています。

| | 【SECURITY ACTION】（セキュリティ対策に取り組むことを自ら宣言） | | 【セキュリティ対策評価制度】（基準に適合する対策が実施できていることをチェック・認定） | | |
|---|---|---|---|---|---|
| | 一つ星 ★ | 二つ星 ★★ | 三つ星 ★★★ | 四つ星 ★★★★ | 五つ星 ★★★★★ |
| 概要 | 情報セキュリティ5か条への取り組み宣言 | 自社診断＋基本方針策定＆公開 | 最低限実装すべきセキュリティ対策 | 標準的に目指すべきセキュリティ対策 | 到達点として目指すべき対策 |
| 対象 | 全ての企業 | 全ての企業 | 全ての企業 | 発注者から見た重要な企業 | ー（未定） |
| 項目 | ー | ー | 26項目 | 44項目 | ー（今後検討） |
| 評価 | 自己宣言（IPA「SECURITY ACTION」） | | 専門家確認付き自己評価 | 第三者認証型 | |

経済産業省が2025年12月「制度構築方針（案）」を基に作成しております。今後、内容は変更される可能性があります。

## セキュリティ対策評価制度を利用するメリット




**■発注企業が得られる効果**

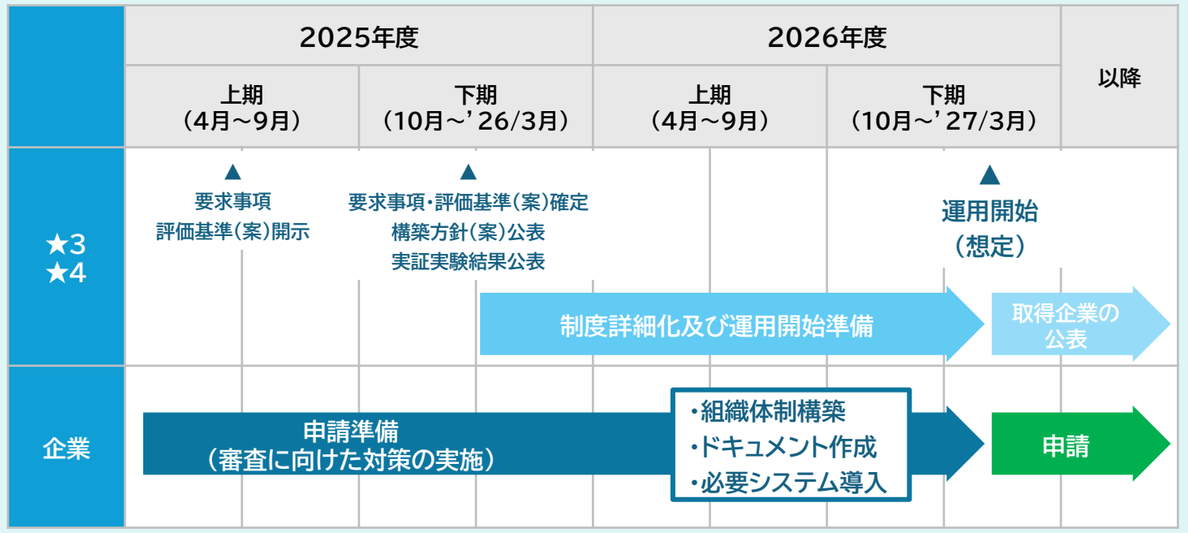
- ✓ セキュリティ対策の状況把握が容易、適切になる
- ✓ 自社のセキュリティリスクが低減される

**■受注企業が得られる効果**

- ✓ 自社がどの程度のセキュリティ対策を実施するべきか明確になる
- ✓ セキュリティ対策に係る説明が明確になる

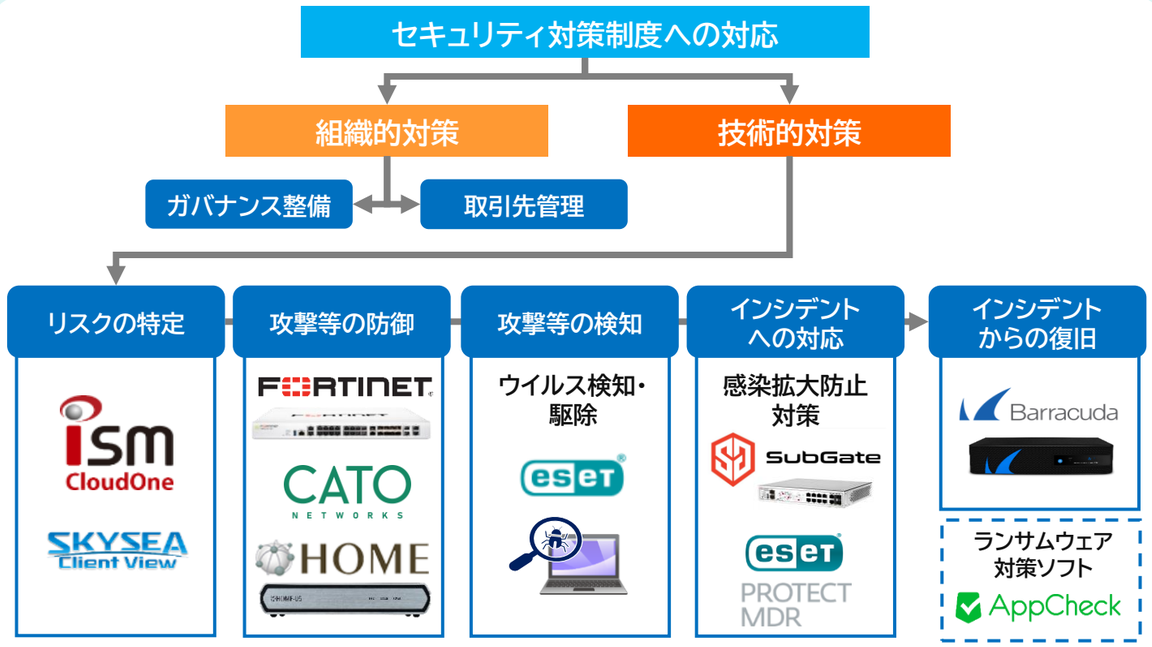
**発注者・受注者双方にとって、適切なセキュリティ対策の決定や対策状況の説明が容易・適切となる**

## セキュリティ対策評価制度のスケジュール




経済産業省が2025年12月「制度構築方針（案）」を基に作成しております。今後、内容は変更される可能性があります。

## セキュリティ対策評価制度に基づいた具体的な対策




□＜★2取得支援サービス＞をご用意しております。

各製品・サービスの詳細は営業までお問い合わせください。

# いま求められる ランサムウェア対策

企業規模、業種問わず被害が相次ぐサイバー攻撃
「システムの停止」＝「企業活動の停止」

## 情報セキュリティ10大脅威　2026年版（IPA公表）

| 順位 | 「組織」向け脅威 | 初選出年 | 10大脅威での取り扱い（2016年以降） |
|---|---|---|---|
| 1 | ランサム攻撃による被害 | 2016年 | 11年連続11回目 |
| 2 | サプライチェーンや委託先を狙った攻撃 | 2019年 | 8年連続8回目 |
| 3 | AIの利用をめぐるサイバーリスク | 2026年 | 初選出 |
| 4 | システムの脆弱性を悪用した攻撃 | 2016年 | 6年連続9回目 |
| 5 | 機密情報を狙った標的型攻撃 | 2016年 | 11年連続11回目 |
| 6 | 地政学的リスクに起因するサイバー攻撃（情報戦を含む） | 2025年 | 2年連続2回目 |
| 7 | 内部不正による情報漏えい等 | 2016年 | 11年連続11回目 |
| 8 | リモートワーク等の環境や仕組みを狙った攻撃 | 2021年 | 6年連続6回目 |
| 9 | DDoS攻撃（分散型サービス妨害攻撃） | 2016年 | 2年連続7回目 |
| 10 | ビジネスメール詐欺 | 2018年 | 9年連続9回目 |

**1位**

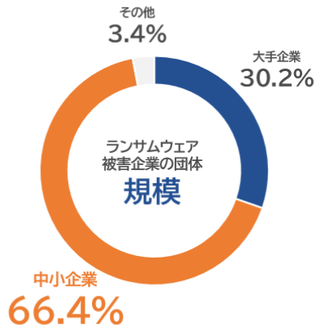
**ランサム攻撃による被害（1位・11年連続選出）**

- ○ 事業停止や情報漏えいなど、経営への影響が極めて大きい
- ○ 攻撃手法の高度化により、業種・規模を問わず被害が拡大
- ○ 被害が連鎖し、取引先や社会全体へ波及するおそれ

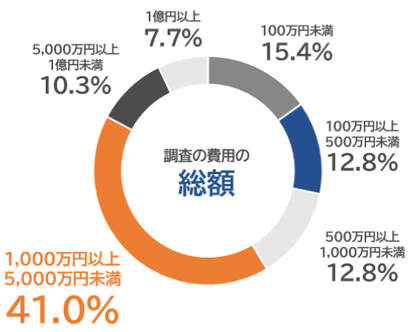
出典：独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威 2026」を基に作成しております。

## 警察庁 ランサムウェア被害の総計 2025年

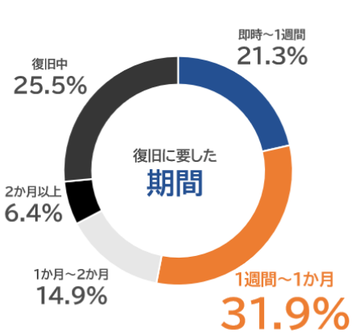
狙われるのは
半数以上が
**中小企業**




被害の総額
**1,000～5,000 万円**

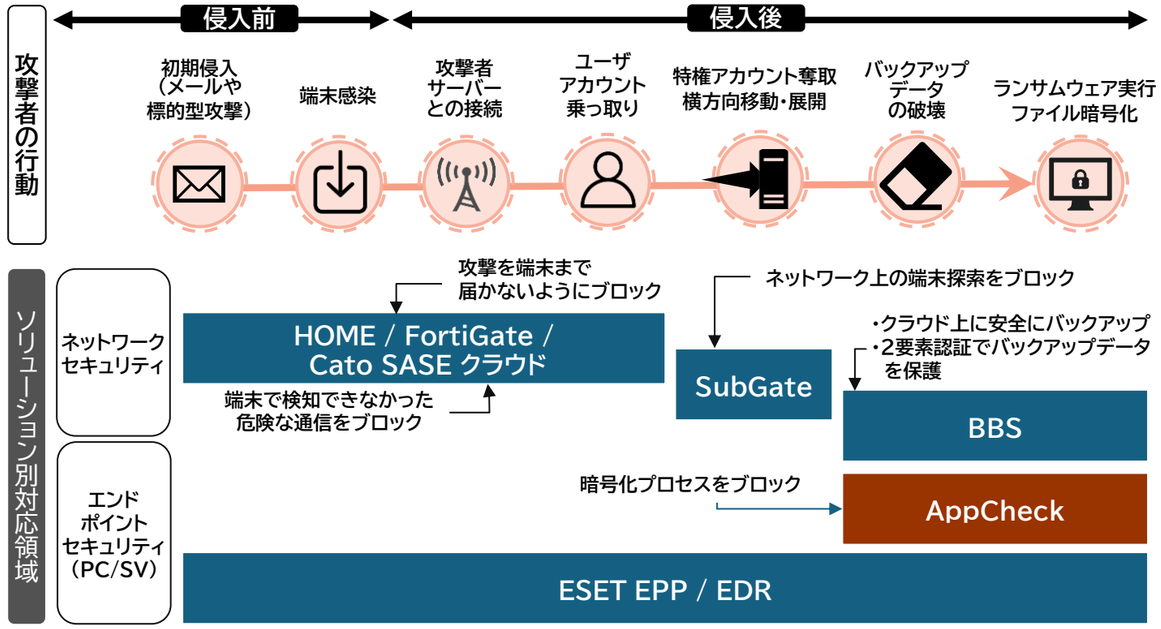



復旧に要した期間
**1週間以上～77%**

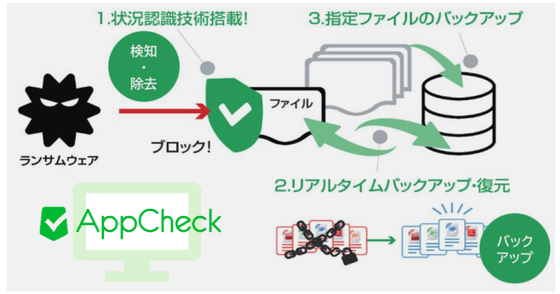



出典：警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」を基に作成作成しております。

## ランサムウェアの行動と対策ソリューション




### ランサムウェアの暗号化特化対策 AppCheck




□特徴①…**状況認識技術を搭載**
状況認識技術によりファイル自体の変化を検出し、ランサムウェアによるファイル毀損をブロック。

□特徴②…**リアルタイムバックアップ・復元**
リアルタイムのバックアップで正常なファイルを保護。万が一ファイルが感染しても、元の状態に復元可能。

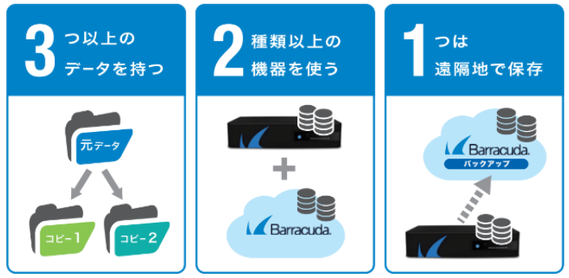
□特徴③…**軽快な動作**
シグネチャを使用しないため、動作が軽快。既存のセキュリティ環境との共存が可能。

←約2分の動画でAppCheckの動作を確認可能！

### 非常時のバックアップ対策 Barracuda Backup

これ1台で、**バックアップの3-2-1ルール**に対応！

Barracudaはクラウドサイトへ自動的にデータを転送しバックアップデータの二重化を行います。




**バックアップデータを安全に保護**