

最新情報を解説！

経産省「セキュリティ対策評価制度（SCS評価制度）」とは？
発注企業はどの星を要請する？「SCS評価制度」対応の進め方

※「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」の略称です。
（2026年3月に経済産業省が公表した「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に関する制度構築方針」より

エムオーテックス株式会社

© MOTEX Inc.

会社概要

MOTEX

会社名	エムオーテックス株式会社
代表取締役社長	徳毛 博幸
設立	1990年7月
拠点	大阪本社・東京本部・名古屋支店 九州営業所・長崎 Innovation Lab
事業内容	サイバーセキュリティに関する プロダクト開発・サービス事業

© MOTEX Inc.

エムオーテックスが提供する5つのセキュリティソリューション



エンドポイントセキュリティ

IT資産管理・MDM・EPP・EDR・MDR

- PC・スマホ一元管理
- 内部不正・情報漏洩対策
- AIによるサイバー攻撃対策

クラウドセキュリティ

SaaS・IaaSの設定診断
Microsoft 365 監査ログ管理

- 国家資格取得者による設定診断
- 業界トップクラスの診断項目数
- 監査ログの取得・アラート管理

ネットワークセキュリティ

脆弱性診断・AI ネットワーク脅威検知
サプライチェーンリスク評価

- Web・ネットワークの脆弱性診断
- AIによるネットワーク監視・遮断
- 外部公開資産の洗い出し・リスク評価

IDセキュリティ

IDaaS

- パスキー(FIDO2)・多要素認証による確実な本人認証
- アカウントと権限の統合管理によるID統制の強化
- シングルサインオンによるアクセス効率化

コンサルティング

経産省SCS評価制度（セキュリティ対策評価制度）※支援
各業界セキュリティガイドライン支援

- ガイドラインの理解・対策ノウハウの学習
- ガイドライン要件に照らした課題の洗い出し
- 各種ひな形の提供・策定・改定支援

※「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」の略称です。
（2026年3月に経済産業省が公表した「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に関する制度構築方針」より）

© MOTEX Inc.

アジェンダ

1. 本日お伝えしたいこと
2. SCS評価制度（セキュリティ対策評価制度）の最新情報
3. 発注企業は取引先に何を求め始めているのか（実態調査から読み解く）
4. SCS評価制度への具体的な進め方
5. サポアカ・SCS評価制度対応の支援実績とキャンペーン
6. 本日のまとめ

© MOTEX Inc.

本日お伝えしたいこと

© MOTEX Inc.

本日お伝えしたいこと

✓ 経済産業省の「SCS評価制度」は、サプライチェーン全体での対応を前提としており、今後多くの企業でまず星3、将来的には星4水準を見据えた対策が求められる可能性があります。

✓ 星獲得を目指すうえでは、評価基準を正しく理解し、自社の現状を把握することが最初の重要なステップになります。

✓ 制度開始を待つのではなく、今から準備を始めることが、取引先からの信頼確保や新たなビジネスチャンスにつながります。

© MOTEX Inc.

SCS評価制度（セキュリティ対策評価制度）の最新情報

出典：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（SCS評価制度）：https://www.ipa.go.jp/security/scs/index.html

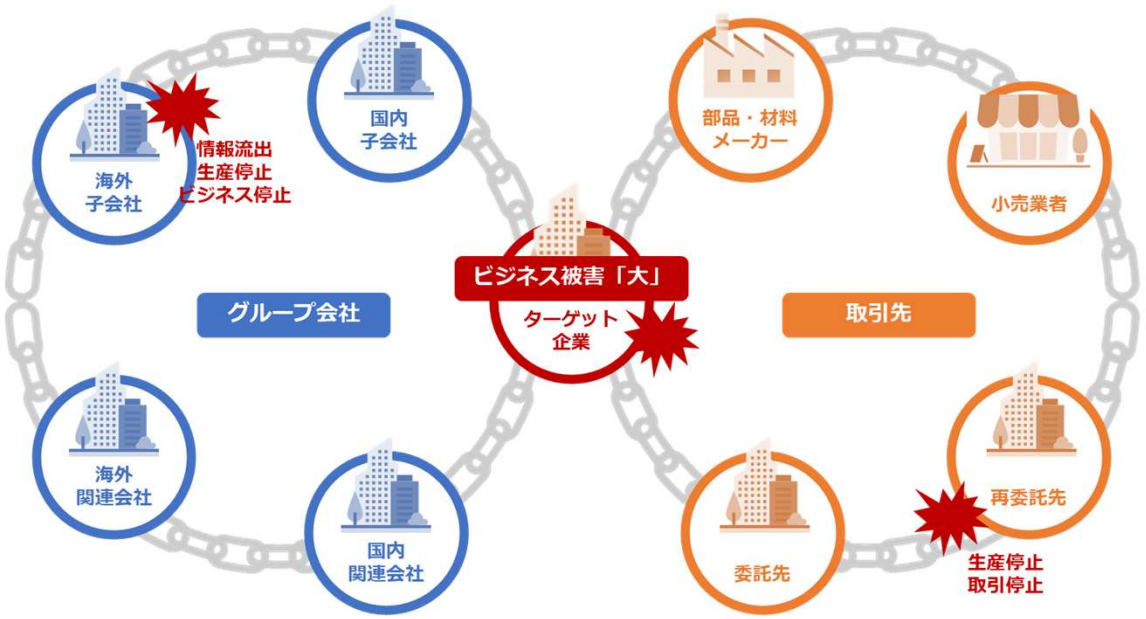
© MOTEX Inc.

新制度スタートの背景

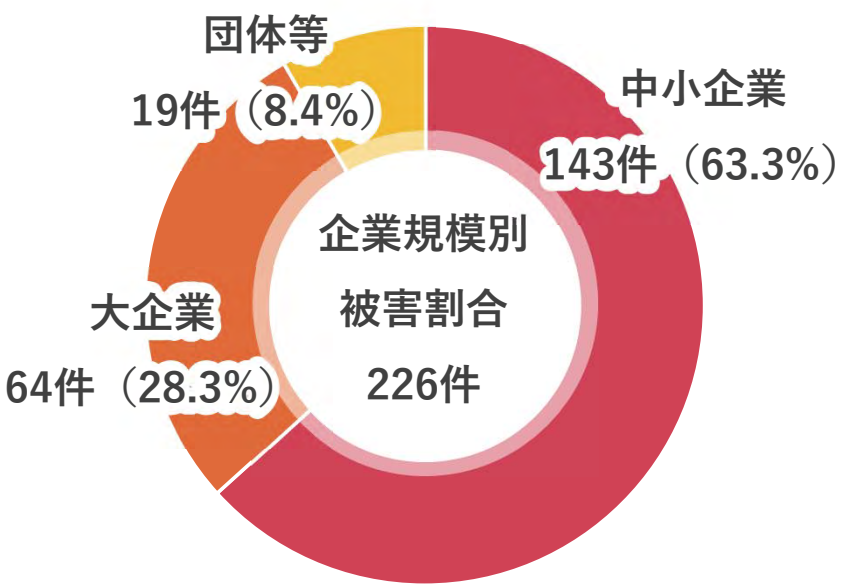
サプライチェーンに関与するすべての企業が対策に取り組むことが必須
企業規模を問わず、対策を怠ると被害者ではなく加害者にもなりうる

1つの企業でセキュリティインシデントが発生すると、取引先企業や顧客の企業などの他の企業（＝サプライチェーン）にも被害が拡大します。一部の大企業だけでなく中小企業を含めてすべての企業がサイバーセキュリティ対策に取り組み、対策の底上げをすることが必要です。

サプライチェーンの概念図



ランサムウェア被害の規模別報告件数



出典：令和７年における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

© MOTEX Inc.

SCS評価制度の具体化が進み、制度開始に向けた段階へ

2026年8月～10月に**基本規程・評価用ガイド等**が公開されました

- 経産省が方針発表 — 2024年 4月
- 実証事業の実施 — 2025年 4月～10月
- 制度構築方針 — **2026年 3月27日**
- 基本規程等が公開 — **2026年 8月28日**
- 評価用ガイド等が公開 — **2026年 10月28日**
- SCS評価制度スタート — **2027年 3月頃**

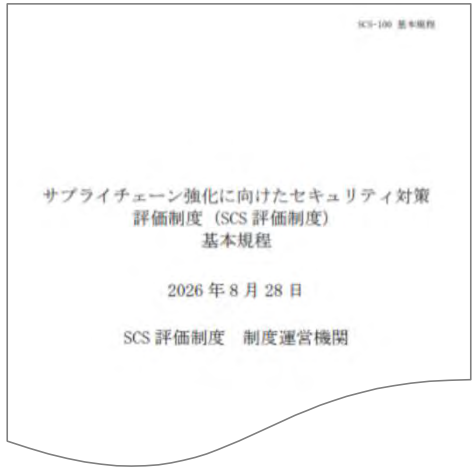

経済産業省　国家サイバー統括室

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に関する制度構築方針

令和８年３月

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に関するサプワーキンググループ

事務局


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（SCS 評価制度）基本規程

2026 年 8 月 28 日

SCS 評価制度　制度運営機関


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（SCS 評価制度）★3・★4 自己評価等ガイド

2026 年 10 月 28 日

SCS 評価制度　制度運営機関

・・・

© MOTEX Inc.

SCS評価制度（セキュリティ対策評価制度）とは？　～概要～

サプライチェーンに関与するすべての企業を対象に、セキュリティ対策レベルを可視化・底上げ
～信頼できる企業とそうでない企業を区別できるようにする～

	【SECURITY ACTION】 セキュリティ対策に取り組むことを自ら宣言		【SCS評価制度（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		
	★1	★2	★3	★4	★5
概要	情報セキュリティ5か条 取組むことの宣言	自社診断＋基本方針 ※ 取組むことの宣言	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 セキュリティ対策
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	未定 2026年度以降に具体化予定
評価	自己宣言	自己宣言	専門家確認付き自己評価	第三者評価	
項目	–	–	81項目	153項目	

※「5分でできる！情報セキュリティ自社診断」と「情報セキュリティ基本方針」を策定し外部公開した上で、情報セキュリティ対策に取り組むことを宣言するものです。

© MOTEX Inc.

内容更新

取得範囲は「原則：法人単位」で設定

事業部・グループ単位での取得も、合理的理由がある場合に可能

法人・個人事業主単位

大原則



事業部単位等

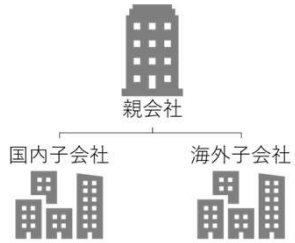
例外①



- ✓ **責任者の明示**：セキュリティ責任者（所属・役職）が明確であること
- ✓ **常設の組織**：継続的な組織であること（一斉プロジェクト等は不可）

企業グループ単位

例外②



- ✓ **IT基盤の一体化**：全社で共通のIT基盤（システム）を使っていること ※構成図で要明示
- ✓ **ルールの一体化**：グループ共通のセキュリティ方針（ルール）があること

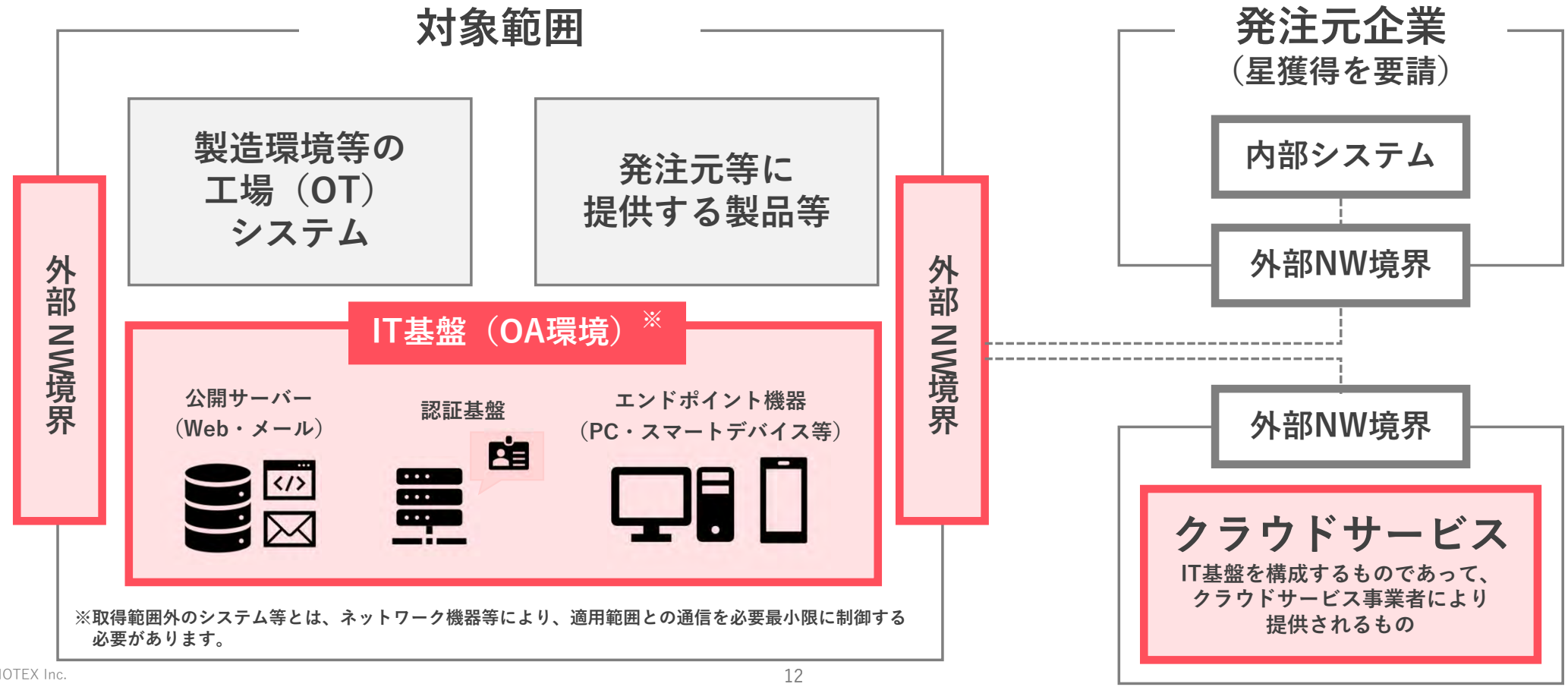
※取得範囲外のシステム等とは、ネットワーク機器等による**通信分離が原則**です。
ただし、同一拠点等で分離が困難な場合、**相手側も同等以上のセキュリティ対策が講じられていることが確認できれば、境界保護を免除**できます）

© MOTEX Inc.

SCS評価制度とは？　～範囲・位置づけ～

IT基盤（オンプレミス環境、クラウド環境すべて）が対象

制御（OT）システムなどは他の制度・ガイドライン等に基づき対応することを想定



© MOTEX Inc.

新規追加

個人所有端末（BYOD）の業務利用は原則対象

ただし「通話・SMS・多要素認証アプリ専用」は除外可能

■端末の所有形態及び利用場所に応じた適用範囲の考え方

	端末（PC・スマホ等）	ルータ
会社支給 （登録希望組織所有）	適用範囲に **含める**	適用範囲に **含める**
個人所有 （BYOD）	**条件付き** ※ （**業務利用する場合は含める**）	適用範囲に **含めない**
委託先所有	適用範囲に **含めない**	適用範囲に **含めない**



在宅でVPNを使う場合

自宅ルータ：**含めない**

会社側の境界機器：**含める**

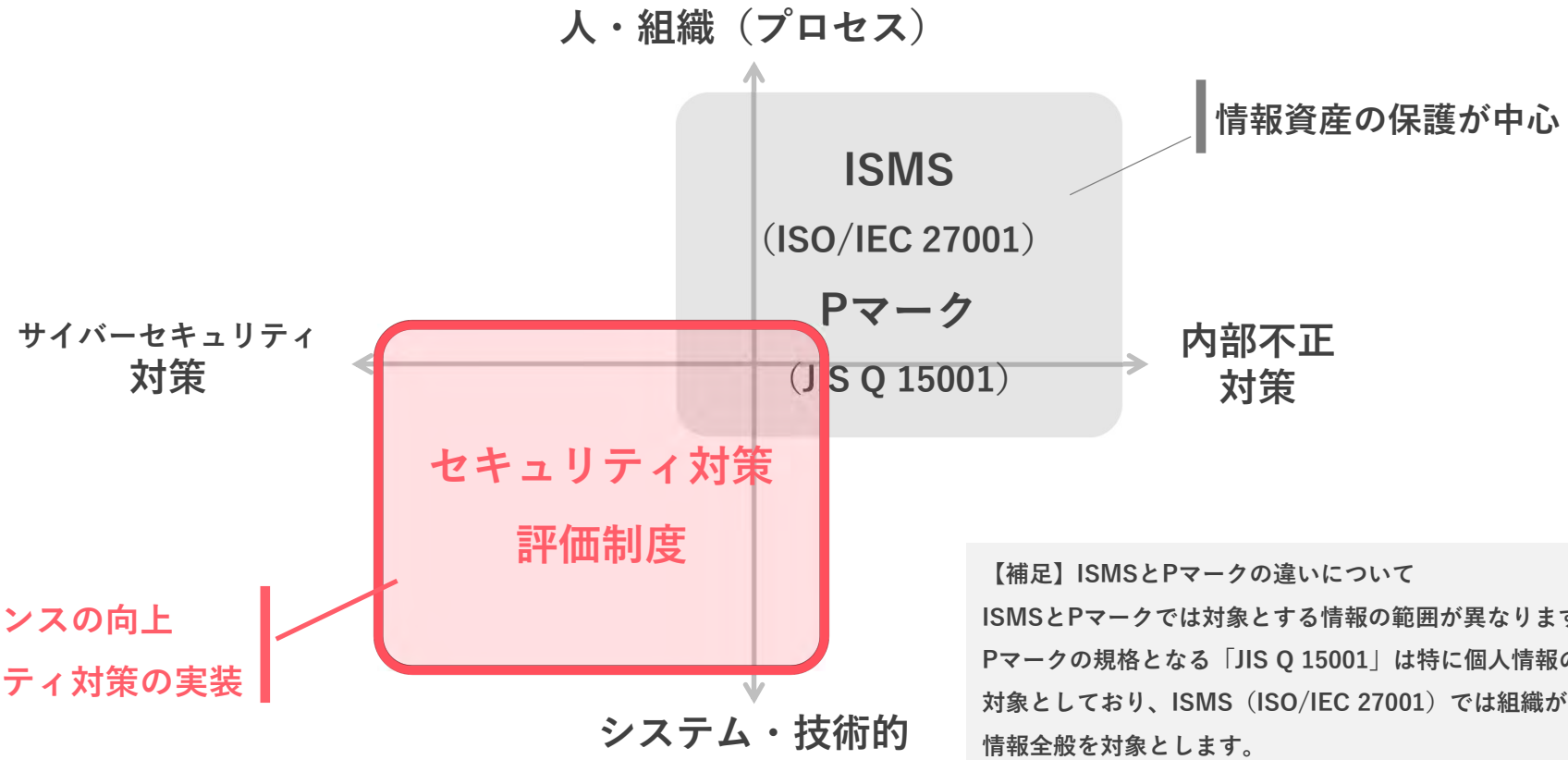
※通話・SMS・多要素認証アプリのみの利用は除外可能

© MOTEX Inc.

SCS評価制度とは？　～範囲・位置づけ（ISMS・Pマークとの関係性）～

相互補完的な制度として両輪で発展予定

「ISMS」「Pマーク」と「SCS評価制度（セキュリティ対策評価制度）」の両方の取得が求められる



【補足】ISMSとPマークの違いについて
ISMSとPマークでは対象とする情報の範囲が異なります。
Pマークの規格となる「JIS Q 15001」は特に個人情報のみを対象としており、ISMS（ISO/IEC 27001）では組織が持つ情報全般を対象とします。

© MOTEX Inc.

SCS評価制度とは？　～対象企業の星の決定～

発注者側の企業が取引先に対して必要な星を設定し要請する

発注側の企業 → 星X 獲得要請 → 受注側の企業（取引先）



うちの会社、星獲得してないから
検討の土俵にすら上がらない？



© MOTEX Inc.

SCS評価制度とは？　～対象企業の星の要請の考え方～

事業継続や情報管理のリスクを考慮し、特に影響が大きい場合は星4を求めることも

ほぼ全ての取引先

★3 基本要求

事業活動上重要な業務がIT基盤に依存

メール　ファイル　業務システム

影響大なら

特に影響が大きい取引先

★4 追加要求

発注者からみて「事業継続」「情報管理」に大きな影響

事業継続リスク

- 製品供給の中断による発注者の事業への影響が大きい
- 同業他社からの調達が困難
- 在庫確保が困難

情報管理リスク

- 発注者の重要な機密情報へのアクセス可否
- 発注者のシステム、ネットワークへのアクセス可否

© MOTEX Inc.

SCS評価制度とは？　～評価基準～

求められるセキュリティ対策は幅広く、網羅的に定義
統治からインシデント復旧まで全方位の対策が求められます



要求事項が多岐にわたる

統治	識別	防御	検知	対応	復旧
・ガバナンス整備 ・取引先管理	リスクの特定	攻撃等の防御	攻撃の検知	インシデントへの対応	インシデントからの復旧

© MOTEX Inc.

SCS評価制度とは？　～星3の要件と基準～

NIST CSF 機能	SCS評価制度			
	大分類	中分類	項目数	**要件のポイント整理**
統治(GV)	ガバナンス整備	役割、責任、権限	8項目	• セキュリティ統括役員と担当部署の**役割・連絡体制を定め、年1回点検する。**
		ポリシー		• 自社のセキュリティ対応方針を**定め、常時参照可能**とし、**改正時に周知**する。
	取引先管理	サイバーセキュリティサプライチェーン リスクマネジメント	4項目	• 自社資産が接続する取引先と、機密情報共有の契約内容を**把握する。**
識別(ID)	リスクの特定	資産管理	11項目	• IT資産、ネットワーク、情報の**管理範囲とルールを把握・点検する。**
防御(PR)	攻撃等の防御	アイデンティティ管理、認証、アクセス制御	48項目	• IDと権限を申請承認で管理し、**多要素認証を用いる。**
		意識向上とトレーニング		• 全従業員等に**インシデント対応教育を定期実施し、記録・点検する。**
		データセキュリティ		• データのバックアップと**遠隔地保管を行い、復旧手順を整備する。**
		プラットフォームセキュリティ		• 端末・サーバーを**安全に保ち、攻撃を防ぐ**（マルウェア対策、安全な設定、更新 など）
		技術インフラのレジリエンス		• 内外のネットワークを適切に分離し、**境界部分を防護する**
検知(DE)	攻撃等の検知	継続的監視	3項目	• **社内外ネットワーク通信を監視**し、**不正な通信を検知・把握**できるようにする
対応(RS)	インシデントへの対応	インシデント管理	6項目	• インシデント対応の**手順・体制・報告方法を整備する。**
復旧(RC)	インシデントからの復旧	インシデント復旧計画の実行	1項目	• 重要なシステムについて、サイバー攻撃を想定した**復旧方法をあらかじめ定めておく**

81項目

© MOTEX Inc.

SCS評価制度とは？　～星4の要件と基準～

NIST CSF 機能	SCS評価制度			
	大分類	中分類	項目数	**要件のポイント整理**
統治(GV)	ガバナンス整備	組織の状況	19項目	• 法令や契約を踏まえ、組織としてセキュリティルールを定め、**毎年見直す。**
		役割、責任、権限		• セキュリティの責任者・担当部署を定め、**組織的な体制を毎年点検する。**
		ポリシー		• 自社のセキュリティ方針を定め、**周知と定期点検**を行う。
		監督		• 年度計画を策定し、**経営報告と改善反映を継続する。**
	取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	7項目	• 重要な機密情報を扱う取引先の**対策状況を把握する。** • 契約終了時に、**情報とアクセス権の回収を確認する。**
識別(ID)	リスクの特定	資産管理	24項目	• IT資産・ネットワーク・情報の**管理範囲を把握する。** • 加えて、**リモートワーク端末と情報のルールを管理する。**
		リスクアセスメント	5項目	• 脆弱性・脅威情報を**収集・判断・対応し、継続的に管理する。**
防御(PR)	攻撃等の防御	アイデンティティ管理、認証、アクセス制御	82項目	• ID・認証・アクセス権を適切に管理し、**利用状況を継続的に見直す。**
		意識向上とトレーニング		• **経営層を含む全員に、毎年教育・訓練を継続実施する。**
		データセキュリティ		• 重要データの暗号化、情報共有ルールの周知、**バックアップ管理を徹底する。**
		プラットフォームセキュリティ		• パソコン・サーバー・端末を**安全に保ち攻撃を防ぐ**(マルウェア対策ソフトウェア、ログ取得など) • Webゲートウェイ対策に加え、**メールによるマルウェアチェックを実施。**
		技術インフラのレジリエンス		• 社内外ネットワークを分離し、**不正通信を継続的に制御する。**
検知(DE)	攻撃等の検知	継続的監視	8項目	• ネットワークと端末の挙動を**常時監視し異常を検知する。**
		有害事象の分析		• インシデントの**対象範囲と判断基準を明確にする。**
対応(RS)	インシデントへの対応	インシデント管理	6項目	• インシデント対応の**手順・体制・報告方法を整備する。**
復旧(RC)	インシデントからの復旧	インシデント復旧計画の実行	2項目	• サイバー攻撃を想定した**重要システムの復旧準備する。**
			153項目	

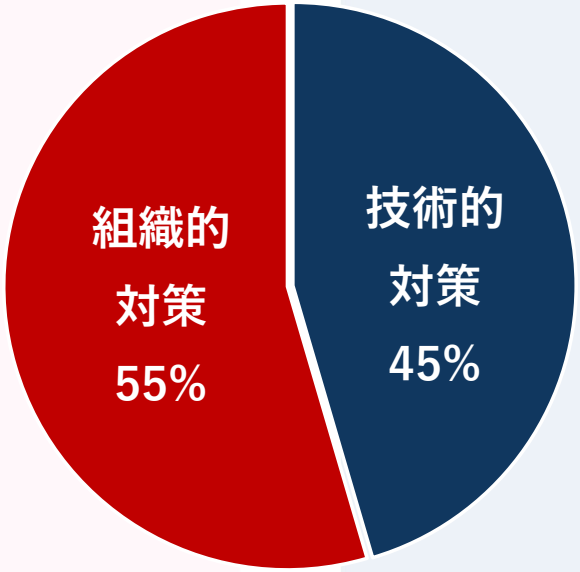
© MOTEX Inc.

制度対応のポイントとは？　求められる対策

セキュリティ対策評価制度の星4で求められる組織的対策と技術的対策

組織的対策

- 社内・管理ルールの作成・教育
- セキュリティ体制の整備
- セキュリティ対策状況の棚卸し
- サプライチェーンの管理
- 情報資産の管理
- ネットワークの一覧化
- サーバーエリアの入退室管理
- セキュリティ教育
- セキュリティインシデントの対応手順書の作成
- 復旧手順書の作成　など



技術的対策

- IT資産管理
- 脆弱性管理
- バックアップ
- アンチウイルス
- 境界防御（UTM）※監視含む
- デバイス制御
- Webフィルタリング
- ログの統合管理
- 不正な通信遮断（IDS/IPS）
- 多要素認証（SSO）
- デバイス・機密データの暗号化
- EDR/MDR　など

© MOTEX Inc.

SCS評価制度とは？　～審査方法～

すべての評価基準への適合が必須。

1項目でも抜けがあれば星は獲得できません

★★★ 審査フロー

評価の主体は**専門家**

1. 適用範囲の決定
2. 自社で評価結果を記入
3. **専門家による審査**
4. 結果チェック＆改善
5. **専門家による改善内容の確認**
6. 経営層による自己適正宣誓
7. 提出・登録

★★★★ 審査フロー

評価の主体は**第三者評価機関**

1. 適用範囲の決定
2. 自社で評価結果を記入
3. **第三者評価機関が審査**
4. **技術検証事業者が検証**
5. 結果チェック＆改善
6. **第三者評価機関による改善内容の確認**
7. **経営層による自己適正宣誓**
8. 提出・登録

© MOTEX Inc.

SCS評価制度とは？　～★3・★4の評価・確認を行う専門家の要件～

★★★

社内外の SCSセキュリティ専門家が確認・助言

自社の有資格者をSCSセキュリティ専門家として登録し、
自己評価結果を確認・助言します。

社内でも
社外でも
OK

社内の有資格者

自己評価結果を確認・助言

署名

主な要件

- ✓ 情報処理安全確保支援士などの対象資格を保有
- ✓ 制度所定の研修を受講
- ✓ SCSセキュリティ専門家として登録

★★★★

社外の独立した第三者のみ

指定された評価機関が、客観的な立場で評価・確認を行います。

評価機関の専門家

指定評価機関

評価報告書

主な要件

- ✓ 指定評価機関による第三者評価
- ✓ SCSセキュリティ専門家の配置（評価責任者）
- ✓ 過去3年以内に構築・運用等に関与した人の評価はNG
- ✓ 自己評価に関与した人の評価はNG

評価機関を選定する際は、公平性・独立性を確認しましょう。

© MOTEX Inc.

SCS評価制度とは？　～「SCSセキュリティ専門家」に求められる要件～

1 資格・専門性

IT・セキュリティに関する高度な知見を持つ専門家であることが求められます。

対象となる主な資格（例）

- ✓ 情報処理安全確保支援士
- ✓ 公認情報セキュリティ監査人
  （公認情報セキュリティ主査監査人を含む）
- ✓ CISSP
- ✓ CISM
- ✓ CISA
- ✓ ISO27001 主任監査員

**ITSSレベル4以上 または
相当の力量が求められます。**

2 制度研修

SCS評価制度を理解し、確認・評価を適切に行うための研修を受講・終了する必要があります。

研修の全体時間

約315分（約5時間15分）

主なカリキュラム

① **知識編　180分**
制度の理解、基準の読み解き、対象の整理など

② **技能編　120分**
ケーススタディによる実践演習など

③ **まとめ　15分**
注意事項の再確認など

特に求められる力量
**グレーゾーンでも根拠を示して
客観的に判断する力**

3 修了・更新

**研修終了後、登録することで
SCSセキュリティ専門家として活動できます。**

修了試験
正答率70%以上で合格
（テキスト参照可・生成AI等の利用不可）

↓

受講証書の有効期間
3年間

↓

資格更新（フォローアップ研修）
有効期間満了の半年前から満了日までに
受講・終了でさらに3年間更新

- 不合格後、1ヵ月間は再試験不可
- 原則、同じ研修事業者で受験
- 再試験は通算5回まで（6回目は再受講が必要）

**自社の有資格者を
SCSセキュリティ専門家として活用する場合**

資格 ＋ **研修受講・終了** ＋ **登録**

© MOTEX Inc.

内容更新

星4の審査では、実地審査・技術検証により**対策の実効性が確認されます**
評価基準を正しく理解した対策が必要です

	★3	★4		
	文書確認	文書確認	実地審査	技術検証
審査員	専門家	評価機関	評価機関	技術検証事業者
所要時間（想定）	1日～2日程度	1日～2日程度	1日～2日程度 ※	1日～2日程度 ※
内容	提出書類の確認	提出書類の確認	ヒアリング、規程や操作画面等の確認による評価	攻撃パターンを試行

※事前準備や報告書作成は除く

実地審査

重要な項目について、「実際にできているか」を資料や
画面などの証拠を見ながら確認・評価

【例】
- 法令や契約等に規定された事項を考慮した社内ルールの策定
- 脆弱性の管理体制、管理プロセス
- セキュリティインシデント対応手順
- 事業継続要件に沿った復旧準備

技術検証

リスクの高いインターネット公開機器
（VPN・ルータ等）について、**脆弱性検査の実施** ※

No.	評価基準
4-4-4-3	・インターネットとの境界に設置されているネットワーク機器のOS及びファームウェアについては、CVSS 基本値 7.0以上の脆弱性を有していないこと。

※過去1か月以内に実施した脆弱性検査結果（指定事業者等）の証跡を提出・審査することで、技術検証の「実施免除（代替）」が可能です。（ガイドSCS-430で正式規定）

© MOTEX Inc.

SCS評価制度とは？　～申請・登録にかかる費用構造～

申請・登録に伴う制度上の費用に加え、
★3・★4では**外部の確認・評価にかかる費用**が発生

税込み価格

★★★ の場合

- 制度運営機関（IPA）
- 登録料 ※1 1万円（1年分）

＋

- 外部委託する場合 セキュリティ専門家（★3確認責任者）
- 委託費用 ※2

★★★★ の場合

- 制度運営機関（IPA）
- 登録料 6万円（3年分）

＋

- 評価機関 ＋ 技術検証事業者
- 委託費用 ※2

※1 2028年4月1日以降は登録料が「2万円」になります。
※2 外部の★3確認責任者・評価機関・技術検証事業者への費用は、それぞれの契約により定められます。
※3 SCSセキュリティ専門家の登録料は「無料」です。

© MOTEX Inc.

SCS評価制度とは？　～有効期間～

SCS評価制度は更新制
評価基準を正しく理解した対策を継続して維持する必要があります

	★3	★4
有効期間	1年	3年
有効期間中	–	毎年、自己評価
更新時	セキュリティ専門家（★3確認責任者）の確認・助言	3年ごとに第三者評価
変更があった場合	–	変更内容によっては再評価
合格基準	原則、すべての要求事項・評価基準への適合が必要	原則、すべての要求事項・評価基準への適合が必要

【★4｜有効期間中の大きな変更に注意】

- 有効期間中であっても、**適用範囲の変更や、要求事項・評価基準の達成に顕著な影響を及ぼす変更**がある場合は、再度評価機関の評価が必要です。
  例）社内規程・手順書等の大幅な変更 、運用方法の大幅な変更、PC・サーバ等の大規模リプレイス、クラウドシフト

© MOTEX Inc.

SCS評価制度とは？　～登録後の対応～

SCS評価制度では、登録後の状況変化や不正行為等に対しても、
登録組織として適切に対応することが求められます。

ケース	制度上の対応
① 大きな変更があった場合	★4は、変更内容によって **改めて評価機関の評価を受ける必要があります**
② 不正行為が確認された場合	虚偽申請や情報隠蔽等の不正行為が確認された場合、 **登録が取り消される場合があります。**
③セキュリティインシデントが発生した場合	セキュリティインシデントが発生した場合、 **事実確認や原因究明等の調査への協力を求められる場合があります。**

例）
・社内規程・手順書等の大幅な変更
・IT基盤を構成する端末やサーバ等の大規模なリプレイス
・クラウド基盤への大規模な移行
・ネットワーク構成の顕著な変更　など

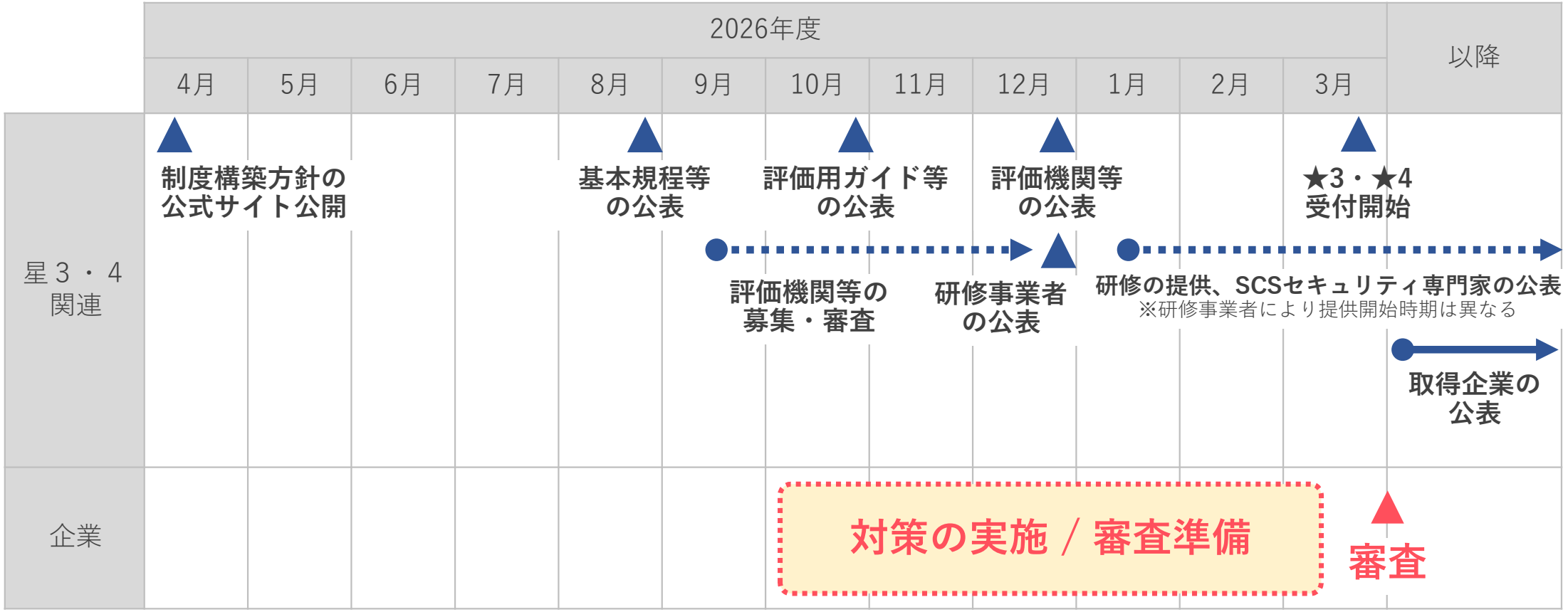
SCS評価制度の登録は「取得した時点」で完結するものではなく、
登録後の状況変化にも適切に対応することが重要です。

© MOTEX Inc.

SCS評価制度とは？　～スケジュール～

制度開始は**2027年3月**頃の予定

早期に星の取得を目指す場合は、**今のうちから準備を進めておくことが重要**です。



© MOTEX Inc.

新規追加

SCS評価制度への**一本化に向けて検討開始**。運用開始は**2028年度（仮）**

1-6-2. SCS評価制度への対応方針（自工会・部工会）

「SCS評価制度」について、自工会・部工会として対応方針を整理しましたので、ご報告いたします

●自動車業界として目指す姿

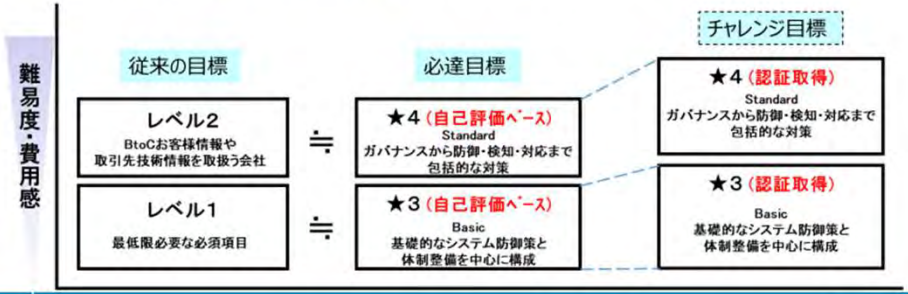
最終的には、国の新制度に一元化すべきと考える（ダブルスタンダードにならないようにする）

●自動車業界としての新制度の活用方法

1）準拠すべきガイドラインは、新制度ガイド１本とする（自動車産業ガイドから、新制度ガイドに乗り換える）

2）新制度ガイドに基づいた「自己評価の実施」と「その結果の提出」を従来同様に各社様にお願いしたい
自工会としての「自己評価結果の集計・分析」と「その結果の公表」も従来同様に継続実施する

3）★３★４の認証取得を必須とはしない（各社の任意とする）



11

Copyright© Japan Automobile Manufacturers Association, Inc.

出典：2026年10月2日公開　日本自動車工業会「2026年度 自己評価の実施・展開及び経営層向け説明会」
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_supply_chain.html#FY2026_self_assessment

© MOTEX Inc.

SCS評価制度の最新情報のまとめ

① サプライチェーンに関与するすべての企業が対象となり、星を獲得する範囲は原則として個社単位で評価されます。

② 要求事項は幅広く、すべての評価基準への適合が必須であり、評価機関による審査・技術検証を踏まえた正しい対応が求められます。

③ 制度は更新制で、一度取得して終わりではなく、継続的な対策の見直しと改善が重要です。

④ 制度開始は2026年度末の予定のため、いち早く星を獲得するためには、今から準備を進めることが重要です。

© MOTEX Inc.

発注企業は取引先に何を求め始めているのか（実態調査から読み解く）

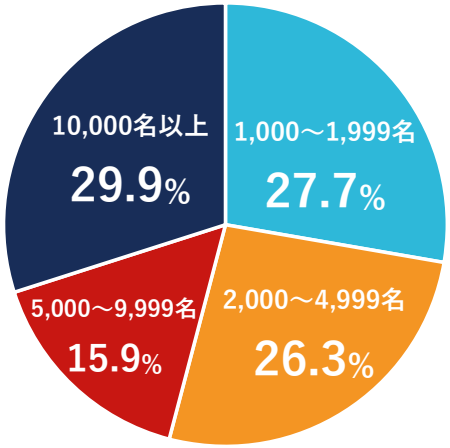
© MOTEX Inc.

SCS評価制度に関する実態調査

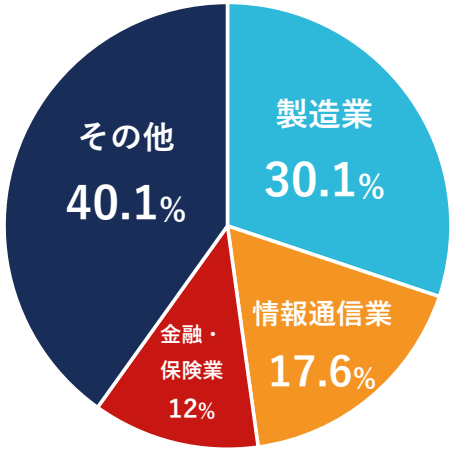
調査概要　「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」についての実態調査

- 調査期間：2026年3月3日～ 2026年3月10日
- 調査方法：インターネット調査
- 調査人数：1,002名
- 調査対象：従業員数1,000名以上の企業に所属している情シス・セキュリティ担当者（発注者側のお立場）
- モニター提供元：株式会社PRIZMAリサーチ
- 調査機関：株式会社PRIZMA

Q. あなたの企業の従業員数を教えてください
【有効回答数：1,002】



Q. あなたの企業が属する業界を教えてください
【有効回答数：1,002】



＜その他の企業の内訳＞

サービス業（6.5%）、運輸業・郵便業（5.5%）、建設業（4.9%）、電気・ガス・熱供給・水道業（4.1%）、卸売業・小売業（4.9%）、医療・福祉（3.3%）、不動産業・物品賃貸業（2.5%）、学術研究・専門・技術サービス業（2.2%）、教育・学習支援業（1.3%）、複合サービス事業（1.3%）、鉱業・採石業・砂利採取業（1.1%）、宿泊業・飲食サービス業（0.9%）、生活関連サービス業・娯楽業（0.7%）、漁業（0.4%）

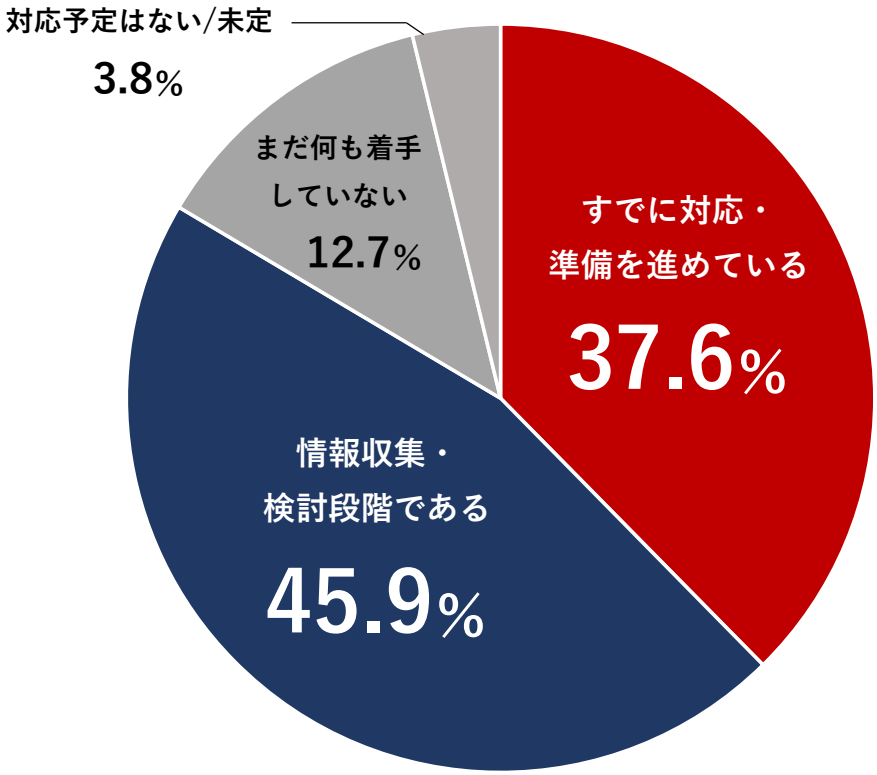
※図中の数値は小数点第二位以下を切り捨てのため、必ずしも 100% になりません

© MOTEX Inc.

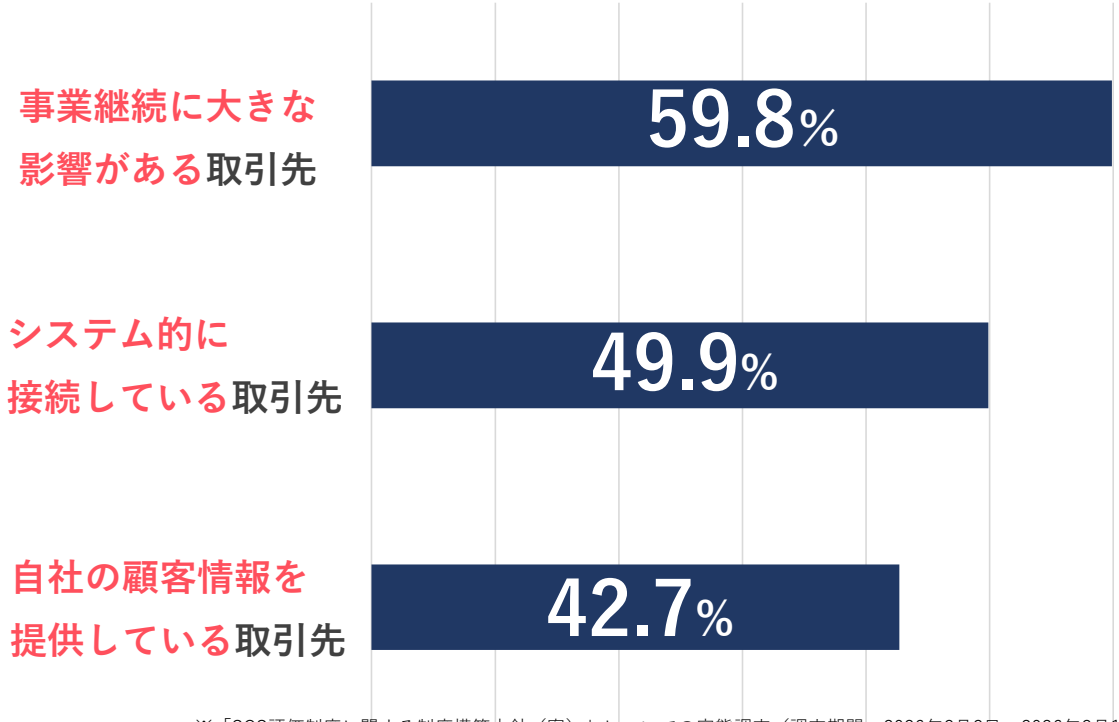
SCS評価制度に関する実態調査

サプライチェーンの発注側の企業の８割以上が、制度開始に向けて動き出している
星取得の要請対象とする取引先の範囲ついても検討を始めている状況です

SCS評価制度の対応状況（有効回答数：1,002）



星取得の要請対象とする取引先（有効回答数：1,002・複数回答可）



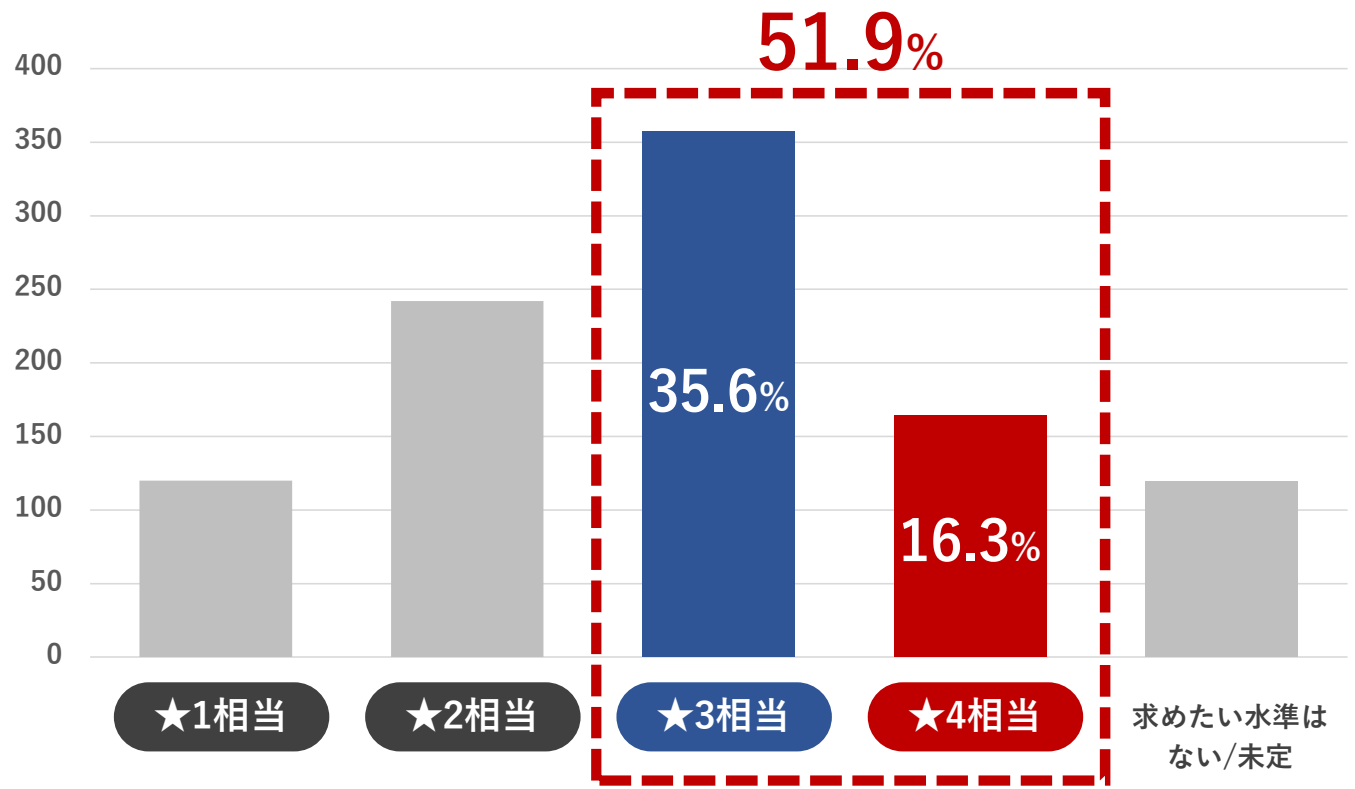
※「SCS評価制度に関する制度構築方針（案）」についての実態調査（調査期間：2026年3月3日～2026年3月10日）
株式会社PRIZMAが従業員数1,000名以上の企業に所属している情シス・セキュリティ担当者に調査

© MOTEX Inc.

SCS評価制度に関する実態調査

2026年度末予定のSCS評価制度開始時点で、取引先に対して、星3・星4取得を求める組織が過半数以上

制度開始の初年度に最低限求めたい水準（有効回答数：1,002）



※「SCS評価制度に関する制度構築方針（案）」についての実態調査（調査期間：2026年3月3日～2026年3月10日）
株式会社PRIZMAが従業員数1,000名以上の企業に所属している情シス・セキュリティ担当者に調査「事業継続に大きな影響がある取引先」の結果を掲載

© MOTEX Inc.

SCS評価制度に関する実態調査

2026年度末予定のSCS評価制度開始時点で、
取引先に対して、星3・星4取得を求める組織が過半数以上

SCS評価制度を活用したセキュリティ要請は、
今後、取引の前提として定着していくことが想定されます。
制度が開始されて早々に、星が求められる可能性があります。



※「SCS評価制度に関する制度構築方針（案）」についての実態調査（調査期間：2026年3月3日～2026年3月10日）
株式会社PRIZMAが従業員数1,000名以上の企業に所属している情シス・セキュリティ担当者に調査「事業継続に大きな影響がある取引先」の結果を掲載

© MOTEX Inc.

SCS評価制度への具体的な進め方

© MOTEX Inc.

星獲得までのステップ

着実な準備と対応が星獲得へのカギです



※本ステップは最短で星獲得を目指す場合の一例であり、実際のスケジュールは各社のセキュリティ対策状況や体制により異なります。

© MOTEX Inc.

星獲得までのステップ

STEP 2 「現状把握」がなぜ重要なのか？

要求事項が幅広い

- ✓ 星3「81項目」にわたる評価基準
- ✓ 星4「153項目」にわたる評価基準



“やっている”と“評価される”のズレ

- ✓ 対策は存在するが
  → 実効性・証跡・説明が不足
- ✓ 自己判断では見落としやすい



審査は“全体適合”での判断

- ✓ 1項目の抜けが星取得に影響
- ✓ 部分最適では通らない



自己評価だけでは足りない第三者視点で“評価される整理”が必要です

© MOTEX Inc.

星獲得支援が可能な「ガイドライン対応サポートアカデミー」とは

SCS評価制度の評価基準への対応状況を、
コンサルタントの「プロの視点」でチェック・アドバイス。星の取得に向けた対応を支援します



標準化された提供コンテンツ
（企業に共通する支援をパッケージ）

多くの企業に共通して必要とされるノウハウを
コンテンツ化してポータルサイトからご提供することで
コストを抑え、利用しやすい価格を実現

ガイドライン対応サポートアカデミー

標準化 × 個別支援

企業ごとの状況に合わせた
実効性の高い支援 を
30万円※～の低コストで提供

専門家による個別支援
（企業ごとの課題に合わせた支援）

企業ごとに異なる環境・既存対策に対して
情報処理安全確保支援士の国家資格を保有する
コンサルタントが個別にサポート



© MOTEX Inc.

なぜガイドライン対応サポートアカデミーが必要なのか？

チェックシート添削やカウンセリングの結果をもとにセキュリティを見える化
お客様が抱えている課題に対して適切なソリューション紹介が可能になる

お客様

ガイドライン対応
サポートアカデミー

セキュリティの見える化

販売店様



ソリューション紹介

© MOTEX Inc.

目的にあわせて選べるプラン

サイバーセキュリティ対策パッケージ

すべての企業が共通で実施するべき基本的なサイバーセキュリティ対策の実施を支援

「経済産業省 セキュリティ対策評価制度」「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」 や「IPA 中小企業の情報セキュリティ対策ガイドライン」、「IPA 情報セキュリティ対策ベンチマーク」などをもとにした、企業が実施するべきセキュリティ対策の実施状況の点検ができるオリジナルのチェックシートを提供。自社の現状把握から対策強化までサポートします。

自工会／部工会・サイバーセキュリティガイドライン対策パッケージ

自動車産業に特化したセキュリティレベルの維持・向上を支援

自動車産業にかかわるすべての企業・団体を対象としたセキュリティガイドライン「自工会／部工会・サイバーセキュリティガイドライン」に特化した支援をご提供します。年に1回自工会が求めている自己評価チェックシートの提出もサポートします。

教育情報セキュリティポリシーに関するガイドライン対策パッケージ

教育委員会が策定する教育情報セキュリティポリシーの策定・更新を支援

文部科学省の「教育情報セキュリティポリシーに関するガイドライン」に特化したプランです。文部科学省は全国の教育委員会 に対して教育情報セキュリティポリシー策定を強く求めています。ガイドラインに沿ったポリシーの策定・更新から、ポリシーに基づく実施手順の策定までご支援します。

© MOTEX Inc.

目的にあわせて選べるプラン

サイバーセキュリティ対策パッケージ

すべての企業が共通で実施するべき基本的なサイバーセキュリティ対策の実施を支援

「経済産業省 セキュリティ対策評価制度」「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」 や「IPA 中小企業の情報セキュリティ対策ガイドライン」、「IPA 情報セキュリティ対策ベンチマーク」などをもとにした、企業が実施するべきセキュリティ対策の実施状況の点検ができるオリジナルのチェックシートを提供。自社の現状把握から対策強化までサポートします。

自工会／部工会・サイバーセキュリティガイドライン対策パッケージ

自動車産業に特化したセキュリティレベルの維持・向上を支援

自動車産業にかかわるすべての企業・団体を対象としたセキュリティガイドライン「自工会／部工会・サイバーセキュリティガイドライン」に特化した支援をご提供します。年に1回自工会が求めている自己評価チェックシートの提出もサポートします。

教育情報セキュリティポリシーに関するガイドライン対策パッケージ

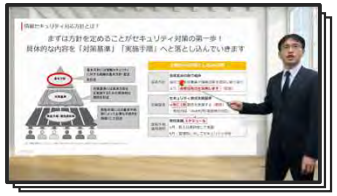
教育委員会が策定する教育情報セキュリティポリシーの策定・更新を支援

文部科学省の「教育情報セキュリティポリシーに関するガイドライン」に特化したプランです。文部科学省は全国の教育委員会 に対して教育情報セキュリティポリシー策定を強く求めています。ガイドラインに沿ったポリシーの策定・更新から、ポリシーに基づく実施手順の策定までご支援します。

© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

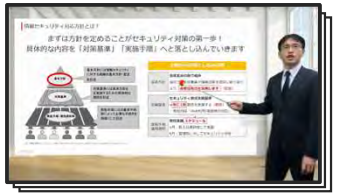
星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

【理解・適用範囲の整理】解説講座

STEP 1

サイバーセキュリティ対策の理解と実施方法を、コンサルタントが動画で分かりやすく解説します

利用期間中は何度でも視聴可能です

前提として知っておきたい知識の解説

サイバーセキュリティに関する難しい内容も、
身近な具体例を交えてわかりやすく解説します。



対策項目を一つひとつを達成基準まで解説

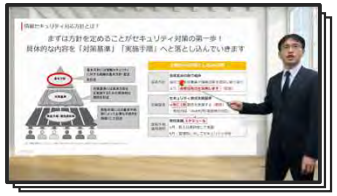
各対策項目の内容と達成基準について、わかりやすく解説します。
文章だけでは理解しにくい部分も、丁寧に説明します。



© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

「できている」と自己評価した項目にも、専門家から指摘

STEP 2

「できているつもり」と「SCS評価基準を満たしている状態」は、**必ずしも一致しません。**



100%

「できている」と自己評価した項目について、

専門家による添削で指摘で発生



© MOTEX Inc.

「できている」と自己評価した項目にも、専門家から指摘

STEP 2

要求事項名	要求事項	評価基準No.	評価基準
インシデント対応手順	セキュリティインシデントへの対応手順、対応体制等を定めること。	6-1-1-5	・セキュリティインシデントの報告フォーマットを整備すること。

© MOTEX Inc.

自己評価の例

STEP 2

6-1-1-5
インシデント対応手順
セキュリティインシデントの報告フォーマットを整備すること。

自己評価の結果

- セキュリティインシデントの報告フォーマットを整備している

© MOTEX Inc.

専門家による確認の例

STEP 2

6-1-1-5
インシデント対応手順
セキュリティインシデントの報告フォーマットを整備すること。

自己評価の結果

- セキュリティインシデントの報告フォーマットを整備している

専門家からの指摘・アドバイス



- **発見報告から最終報告まで、必要な報告フォーマットが整備されていますか？**
- **それぞれのフォーマットに、必要な項目は含まれていますか？**

© MOTEX Inc.

ガイドライン対応サポートアカデミーなら

STEP 2

6-1-1 インシデント対応手順

サポアカ サイバーセキュリティ対策パッケージ
【SCS評価制度対応 解説講座詳細】6.インシデントへの対応

要求事項

セキュリティインシデントへの対応手順、対応体制等を定めること。

評価基準

6-1-1-1	以下の手順を含んだセキュリティインシデントへの対応手順を定めること。 ①発見報告、②初動、③調査・対応、④復旧、⑤最終報告
6-1-1-2	セキュリティインシデント発生時における社内外組織(関係当局及び所管省庁を含む。)の連絡先及び報告・情報共有ルートを定めること。
6-1-1-3	セキュリティインシデント発生時におけるセキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定めること。
6-1-1-4	年1回以上の頻度でNo.6-1-1-2及びNo.6-1-1-3にて定めたセキュリティインシデント発生時の体制について点検すること。
6-1-1-5	**セキュリティインシデントの報告フォーマットを整備すること。**
6-1-1-6	年１回以上及び社内外で重大なセキュリティインシデントが発生した際に、インシデント事例及びその対応策を社内部署へ共有していること。

審査員のチェック観点

01 社員がCSIRTへ提出するセキュリティインシデント初報用の報告書様式を整備しているか。

セキュリティインシデント報告フォーマットの項目例：

- 受付番号（インシデントID）
- 報告日時、発見日時、報告者（所属、氏名、連絡先）
- 検知契機（ログ検知、利用者申告、取引先連絡など）
- 事象概要、影響範囲
- 現在の状況

02 CSIRTから経営層へのセキュリティインシデント対応中の報告様式を整備しているか。

セキュリティインシデント報告フォーマットの項目例：

- 受付番号（インシデントID）
- 重要度・レベル（自社のレベル定義に基づく）
- 報告者（所属、氏名、連絡先）
- 事象概要（何が起きたか、どこで起きたか）
- 影響範囲（対象端末、アカウント、システム、影響人数など）
- 検知契機（ログ検知、利用者申告、取引先連絡など）
- 現在の状況（継続中、収束、再発有無）
- 対応状況
- 暫定原因
- 今後の対応予定
- エスカレーション／連絡状況（社内外への報告状況）

03 CSIRTから経営層へのセキュリティインシデント最終報告用のフォーマットを整備しているか。

セキュリティインシデント報告フォーマットの項目例：

- 報告日
- 受付番号（インシデントID）
- 事象概要（何が起きたか、どこで起きたか）
- 影響範囲（対象端末、アカウント、システム、影響人数など）
- 原因
- 対応内容
- 復旧状況
- 再発防止策実施結果

審査時に必要となるドキュメント・ツール例

※記載内容は一例です。名称や形式は問いません。複数記載している場合でも、すべての作成・運用が必須となるものではありません。評価基準に対応したルールや運用が確認できれば問題ありません。

- 報告書テンプレート
- チケット起票様式
- インシデント管理台帳

10

© MOTEX Inc.

※10月公開予定の評価ガイドの内容を踏まえ、見直す可能性があります。

ガイドライン対応サポートアカデミーなら

STEP 2



© MOTEX Inc.

※10月公開予定の評価ガイドの内容を踏まえ、見直す可能性があります。

【現状把握】添削で対策漏れをプロ目線でチェック

STEP 2

入力済みのチェックシートを提出すると、コンサルタントが添削

対策漏れ・改善ポイントをプロの目線でチェック



コンサルタントの添削

達成状況チェック項目と達成状況 ―― お客様入力欄

No	チェック項目	達成基準	SCS対策評価制度	達成状況をご入力ください	具体的な実施内容・実施状況
1-1	会社としてセキュリティに対する基本的な方針を作成していますか	情報セキュリティに対する企業姿勢を宣言する文書を策定している	3つ星	できている	○○規程を策定している
		文書内に「経営者の責任」「法令順守」の内容が含まれている	推奨	できている	含まれている
1-2	作成した方針を社内に周知し、セキュリティ意識を高めていますか	ポリシーは定常的に、かつ改正時に社内へ周知され、従業員が誰でも容易に確認できる	3つ星	できている	策定直後に全社の朝礼にて展開した
1-3	社内外の環境変化を踏まえて、基本方針の内容を定期的に見直ししていますか	年に1回以上の頻度で見直ししている	4つ星	できている	年度の初めに見直し改善している

○

△

法令順守として
自社が守るべき法令を
網羅できていますか？
抜け漏れはありませんか？

×

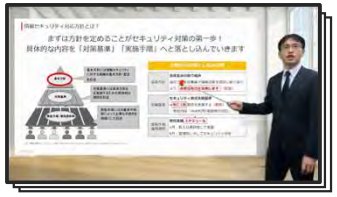
このやり方では、その日の朝礼に不参加の方に周知ができていません。
「誰でも容易に確認できる状態」とも言えません

○

© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

【対策計画の策定】カウンセリング

STEP 3

お客様ごとに「対策プログラム」を作成し、
対応優先度や導入が必要なセキュリティ対策ツールなどをアドバイスします。

■未対応項目の優先順位

【ガバナンス強化】　主に社内ルールの策定や組織体制の整備により達成できる項目です。

優先順位	ラベル	項目ナンバー	優先順位の理由	サポートアカデミーコンテンツ対応一覧		
				解説講座	対策講座	MOTEXひな型・フォーマット
1	2 機密情報を扱うルール	No.8	適切なルールまめ、それを守ることにより、セキュリティ水準が維持されます。	Lv1 講義①	・利用規程3	・「03_情報資産保護」規程 ・【基礎2】業務で利用する情報機器の利用ルール
2	5 体制(事故時)	No.18、20	情報セキュリティ事件・事故は完全に防ぐことができません。発生時に被害を最小限に抑えるためには体制を整備し、役割と責任を明確にする必要があります。	Lv1 講義②	・利用規程2	・「01_組織対策」規程 ・「09_セキュリティ事故対応」規程
3	6 事故時の手順	No.24	早急な対応が被害を最小化します。そのためには事故時の手順を事前にまめておく必要があります。	Lv1 講義②	・利用規程2	・「09_セキュリティ事故対応」規程
4	10 情報資産の管理(情報)	No.54、56、58	情報漏えいを防止するためには、守るべき情報を把握し、適切に取り扱うことが重要です。	Lv1 講義③	・利用規程3	・「03_情報資産保護」規程 ・情報資産管理台帳 ・機密区分運用ルール順守状況チェックリスト

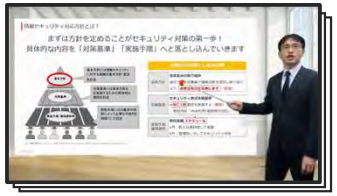
【ツール導入】　主にセキュリティ対策製品などの導入と活用により達成できる項目です。

優先順位	ラベル	項目ナンバー	優先順位の理由	導入が必要なツール	サポートアカデミーコンテンツ対応一覧		
					解説講座	対策講座	MOTEXひな型・フォーマット
1	10 情報資産の管理(情報)	No.58	情報資産の適切な管理を行うことで、情報漏洩のリスクを低減することが重要です。	資産管理ツール	Lv1 講義③	・利用規程3	・「03_情報資産保護」規程 ・情報資産管理台帳 ・機密区分運用ルール順守状況チェックリスト
2	2 機密情報を扱うルール	No.8	適切にルールを守ることにより、情報漏洩による被害を防ぐことが重要です。	資産管理ツール	Lv1 講義①	・利用規程3	・「03_情報資産保護」規程 ・【基礎2】業務で利用する情報機器の利用ルール

© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

【対策実行・運用開始】各種規程ひな型 / 教育コンテンツ / 各種運用支援ツール

STEP 4

規程ひな型・教育コンテンツ・申請書のフォーマットなど**コンテンツを多数ご提供**



情報セキュリティ方針案／組織対策／人的対策／情報資産保護／物理環境保護／IT機器管理／システム管理／システム管理（アクセス制御及び認証）／外部委託先管理／セキュリティ事故対応／インシデント対応手順／誓約書（守秘事項）の文章案）／機密保持契約書の文章案／退職/期間満了時の回収物一覧チェックシート／インシデント管理台帳／ID/アクセス権管理台帳／共有ID利用台帳／アクセス権管理ルール遵守状況チェックリスト／情報資産管理台帳／機密区分運用ルール遵守状況チェックリスト／取り交わし情報一覧表／外部情報システム管理台帳／ヒヤリハットテンプレート／入退室管理台帳／持込物管理台帳／FWフィルタリング設定台帳／管理者権限管理台帳／サーバ・NW機器設定変更作業申請書　等

※現在、IPAなどの公表情報を踏まえて準備中のため、内容が変更になる場合があります。

© MOTEX Inc.

参考：SCS評価制度を支援するMOTEXプロダクト・サービス一覧（星３）

STEP 4

セキュリティ対策評価制度 星３獲得に求められるソリューション例

ガバナンスの整備

- セキュリティ規定の策定（インシデント対応手順含む）
- ガイドライン対応サポートアカデミー

リスクの特定

- IT資産管理 — LANSCOPE Endpoint Manager Cloud

攻撃等の検知

- 境界防御（F/W）監視
- LANSCOPE対応外

攻撃等の防御

- バックアップ
- 境界防御（UTM）
- ソフトウェア無効化
- アンチウイルス

→ LANSCOPE対応外

- LANSCOPE Endpoint Manager Cloud
- LANSCOPE Cyber Protection

- 多要素認証（MFA）
- ID管理製品
- パスワード管理

→ LANSCOPE ID Access Manager

※一部、プロダクト・サービスでは対応できない要求事項・評価基準があります。詳細については、別途ご用意しております対応表をご確認ください。

© MOTEX Inc.

参考：SCS評価制度を支援するMOTEXプロダクト・サービス一覧（星４）

STEP 4

セキュリティ対策評価制度 星４獲得に求められるソリューション例

ガバナンスの整備

- セキュリティ規定の策定（インシデント対応手順含む）

ガイドライン対応サポートアカデミー

リスクの特定

- IT資産管理
- 脆弱性管理

LANSCOPE Endpoint Manager Cloud

攻撃等の検知

- 境界防御（F/W）監視
- EDR/MDR

LANSCOPE対応外

LANSCOPE Cyber Protection

攻撃等の防御

- バックアップ
- 境界防御（UTM）
- デバイス・機密データの暗号化

LANSCOPE対応外

- ソフトウェア無効化
- Webフィルタリング
- 外部記憶デバイス制御

LANSCOPE Endpoint Manager Cloud

- アンチウイルス

LANSCOPE Cyber Protection

- ログの統合管理

データアナライザー splunk>

- 多要素認証（MFA）
- ID管理製品
- パスワード管理

LANSCOPE ID Access Manager

- メールセキュリティ対策
- 不正通信遮断（IDS/IPS）

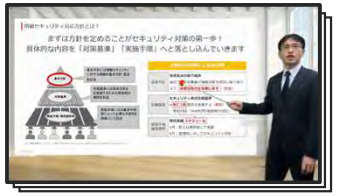
LANSCOPE対応外

※一部、プロダクト・サービスでは対応できない要求事項・評価基準があります。詳細については、別途ご用意しております対応表をご確認ください。

© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

【再評価・提出準備】添削で対策漏れをプロ目線でチェック

STEP 5

評価基準の考え方で、自己評価を見直す
星獲得前の「模試」として活用ください！



コンサルタントの添削

達成状況チェック項目と達成状況　　お客様入力欄

No	チェック項目	達成基準	SCS対策評価制度	達成状況をご入力ください	具体的な実施内容・実施状況
1-1	会社としてセキュリティに対する基本的な方針を作成していますか	情報セキュリティに対する企業姿勢を宣言する文書を策定している	3つ星	できている	○○規程を策定している
		文書内に「経営者の責任」「法令順守」の内容が含まれている	推奨	できている	含まれている
1-2	作成した方針を社内に周知し、セキュリティ意識を高めていますか	ポリシーは定常的に、かつ改正時に社内へ周知され、従業員が誰でも容易に確認できる	3つ星	できている	策定直後に全社の朝礼にて展開した
1-3	社内外の環境変化を踏まえて、基本方針の内容を定期的に見直ししていますか	年に1回以上の頻度で見直ししている	4つ星	できている	年度の初めに見直し改善している

○ 法令順守として自社が守るべき法令を網羅できていますか？抜け漏れはありませんか？

△ 含まれている

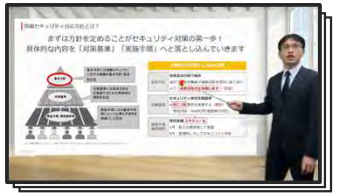
× このやり方では、その日の朝礼に不参加の方に周知ができていません。「誰でも容易に確認できる状態」とも言えません

○

© MOTEX Inc.

星獲得までのステップをサポアカで伴走支援

ガイドライン対応サポートアカデミーでは「SCS評価制度（セキュリティ対策評価制度）」対応の
実務ステップを包括的にサポートします

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6
理解・適用範囲の整理	現状把握	対策計画の策定	対策実行 運用開始	再評価 提出準備	申請・審査
					
解説講座	チェックシート添削	カウンセリング	各種規程ひな型など	チェックシート添削	

星獲得

個別相談（メール / Web会議）

© MOTEX Inc.

ガイドライン対応サポートアカデミー サイバーセキュリティ対策パッケージ 提供内容（詳細）

			総合セキュリティ※1		SCS評価制度（★3専用）
			学習コース（ベーシック）	実践コース（ベーシック）	実践コース※2（ライト）
学習・現状把握	チェックシート	お客様の現状把握が可能なサイバーセキュリティに特化したチェックシートをご提供します。	●	●	●
	解説講座	サイバーセキュリティ対策に必要な知識の習得を目的とした講座動画をご提供します。専用ポータルからいつでも何度でも視聴できます。	●	●	●
	チェックシート添削	お客様にてチェックシートに記入した内容を、セキュリティコンサルタントが確認し、記載内容の妥当性をアドバイスします。	●※3	●※3	●※3
計画	カウンセリング	お客様にてチェックシートに記入した内容を、セキュリティコンサルタントが確認し、視聴すべき対策講座と対策プログラムをご提供します。	-	●※3	●※3
改善	各種規程ひな型	各種セキュリティ関連規程のひな型をご提供します。	●	●	●
	対策講座	サイバーセキュリティ対策に必要な実際に対策を行うためのポイントを解説した講座動画をご提供します。専用ポータルからいつでも何度でも視聴できます。	-	●	●
	教育コンテンツ	サイバーセキュリティ対策に必要となる従業員教育について、集合研修等で活用できる説明資料と理解度確認テストをご提供します。	-	●	●
	各種運用支援ツール	管理台帳や申請書などの各種フォーマットをご提供します。	-	●	●
サポート	個別相談（メール）	メールによる個別相談をご提供します。	●	●	●
	個別相談（Web会議）	オンラインによる個別相談をご提供します。	●※3	●※3	●※3
	よろづ相談会	テーマに沿った相談会を開催します。	-	●	●
	お役立ち情報配信	ガイドラインの改定や、セキュリティ対策に関連する法令の変更、最新のサイバー攻撃情報など、サイバーセキュリティ対策の見直しに役立つ情報を配信します。	-	●	●

※1 SCS評価制度の星4までの取得の支援に加え、IPA等が公表する各種セキュリティガイドラインへの対応まで、企業のセキュリティ対策を総合的に支援します。
※2 星3取得支援に特化したコースのため、実践コース（ベーシック）の内容と一部異なります。
※3 実施回数の制限があります。

© MOTEX Inc.

SCS評価制度対応を支援する3つのコース

星3取得から将来の星4水準まで、段階的に取り組める支援コース

＼ セキュリティ人材の育成からSCS評価制度の星3・星4取得支援など、総合的にサポート ／

SCS評価制度「星4」水準を含む、
総合的なサイバーセキュリティ対策を支援

- SCS評価制度 星３
- SCS評価制度 星4
- 各種ガイドラインで推奨とする対策

＼ SCS評価制度の星3取得に絞って支援 ／

SCS評価制度「星３」を
取得するための支援

- SCS評価制度 星３

学習コース（ベーシック）

定価：¥225,000
利用期間：3ヵ月

実践コース（ベーシック）

【新規購入時】
定価：¥450,000
利用期間：9ヵ月

【継続更新】
定価：¥120,000
利用期間：12ヵ月

実践コース（ライト）

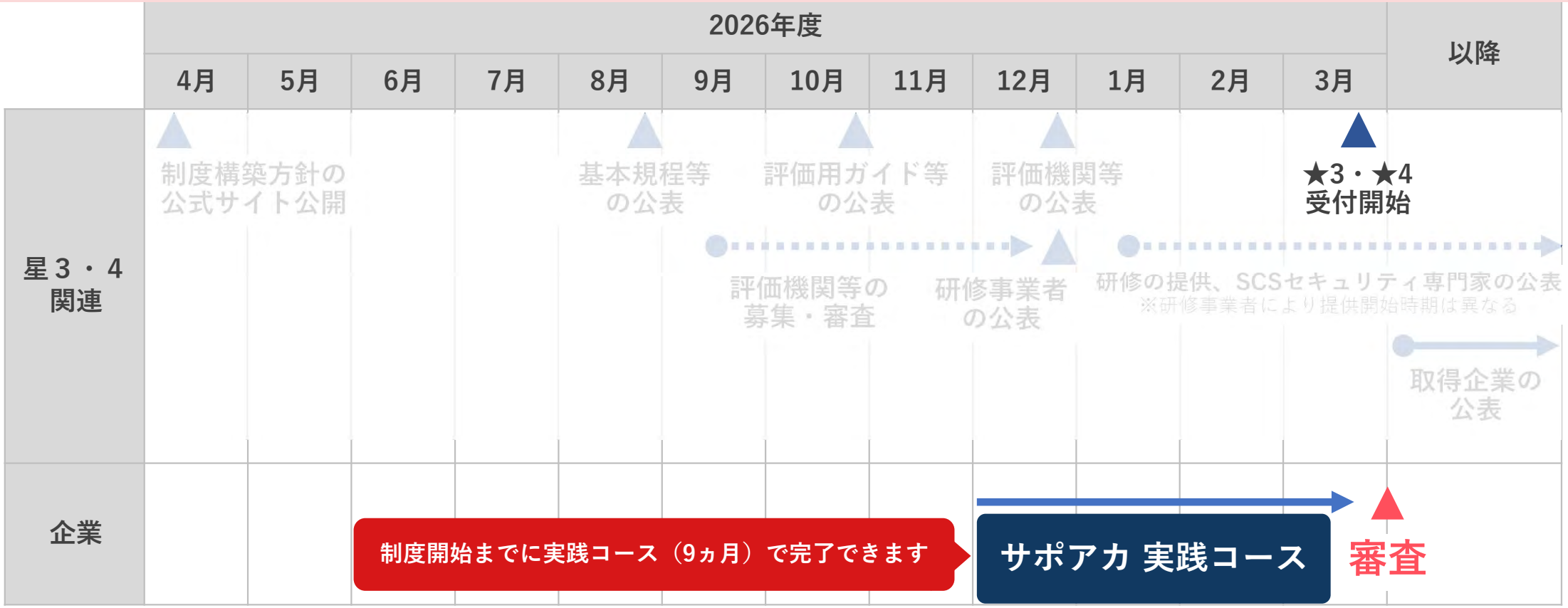
【新規購入時】
定価：¥300,000
利用期間：9ヵ月

【継続更新】
定価：¥120,000
利用期間：12ヵ月

© MOTEX Inc.

SCS評価制度とは？　～スケジュール～

ガイドライン対応サポートアカデミー を使えば、間に合います！



© MOTEX Inc.

セキュリティ投資が生む信頼とビジネスチャンス　～過去の事例：Pマーク～

星の獲得は新たなビジネスチャンスにつながります
「制度が始まってから」ではなく”先行して”準備を進めましょう！

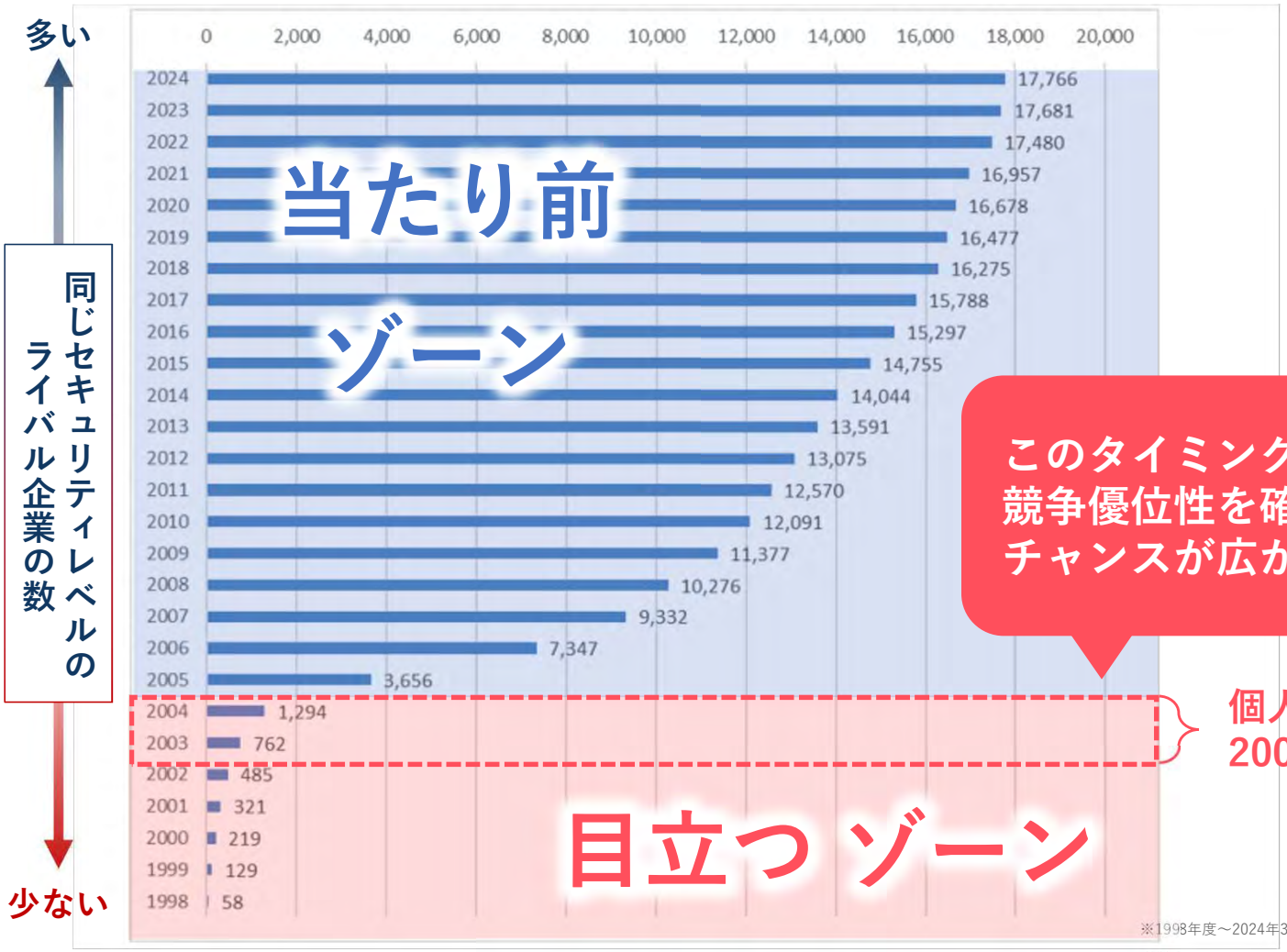
過去の事例：Pマーク（プライバシーマーク）

- 1998年に制度が開始し、2003年の**個人情報保護法の制定**～
  2005年の全面施行をきっかけに大きく取得企業数を伸ばした。
- Pマークは広く企業のHPや社員の名刺などに掲載されており、
  顧客の信頼獲得に活用されている。
- 官公庁等の入札では**Pマークの取得が参加条件**となっており、
  未取得の場合はその時点で**商談機会を失う。**

© MOTEX Inc.

セキュリティ投資が生む信頼とビジネスチャンス　～過去の事例：Pマーク～

▼Pマーク取得企業数の推移



このタイミングで獲得していることで競争優位性を確保し、信頼性とビジネスチャンスが広がります。

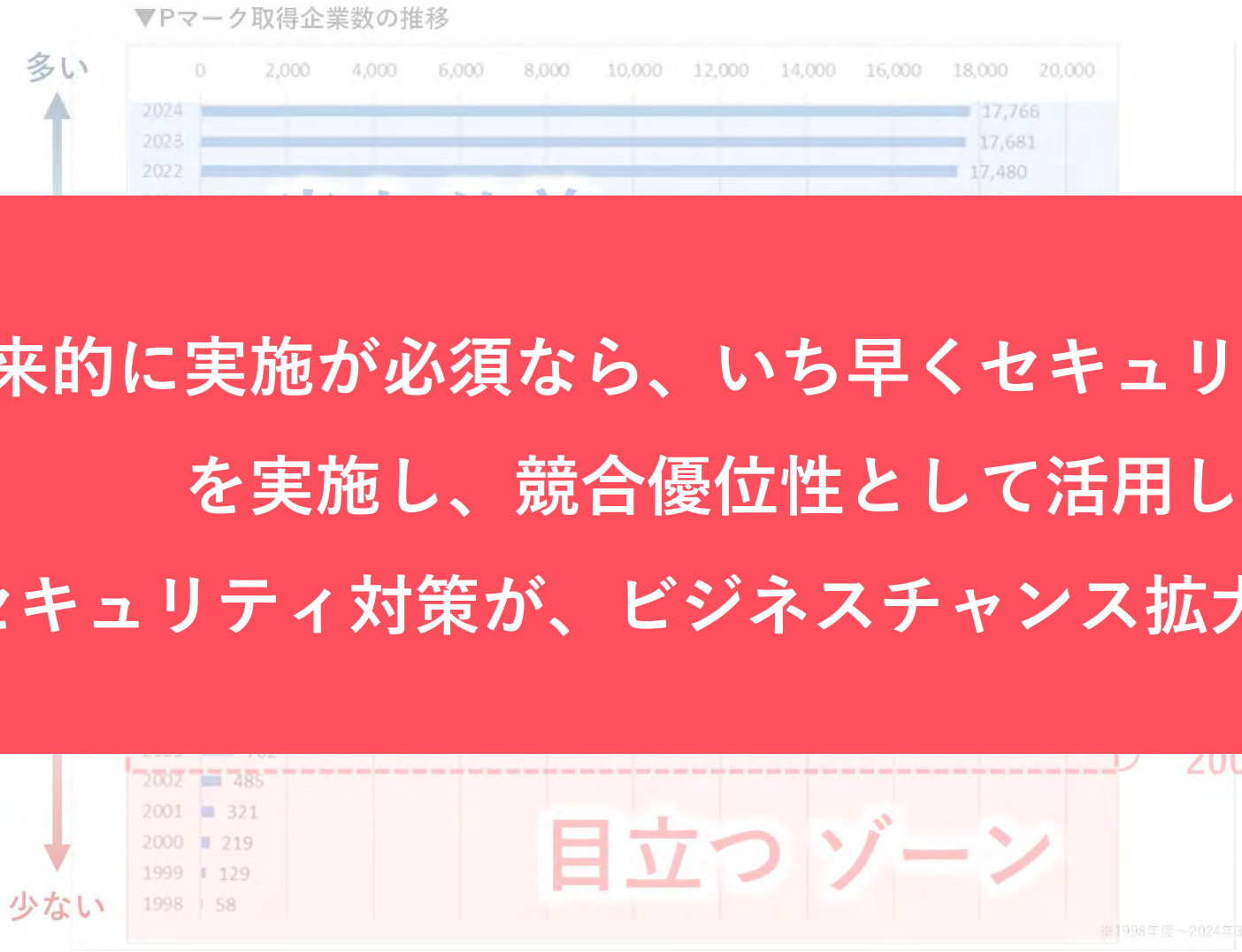
個人情報保護法が2003年5月に制定、2005年4月全面施行される

※1998年度～2024年3月31日時点の事業者数

出典：日本情報経済社会推進協会（JIPDEC） プライバシーマーク付与事業者情報（2024年9月30日版）
https://privacymark.jp/certification_info/data/g7ccig0000000gll-att/pmark_data_20240930.pdf.pdf

© MOTEX Inc.

セキュリティ投資が生む信頼とビジネスチャンス　～過去の事例：Pマーク～



将来的に実施が必須なら、いち早くセキュリティ対策（星獲得）
を実施し、競合優位性として活用しましょう！
セキュリティ対策が、ビジネスチャンス拡大の鍵となります。

※1998年度～2024年3月31日時点の事業者数
出典：日本情報経済社会推進協会（JIPDEC）プライバシーマーク付与事業者情報（2024年9月30日版）
https://privacymark.jp/certification_info/data/g7ccig0000000gll-att/pmark_data_20240930.pdf.pdf

© MOTEX Inc.

サポアカ・SCS評価制度対応の支援実績とキャンペーン

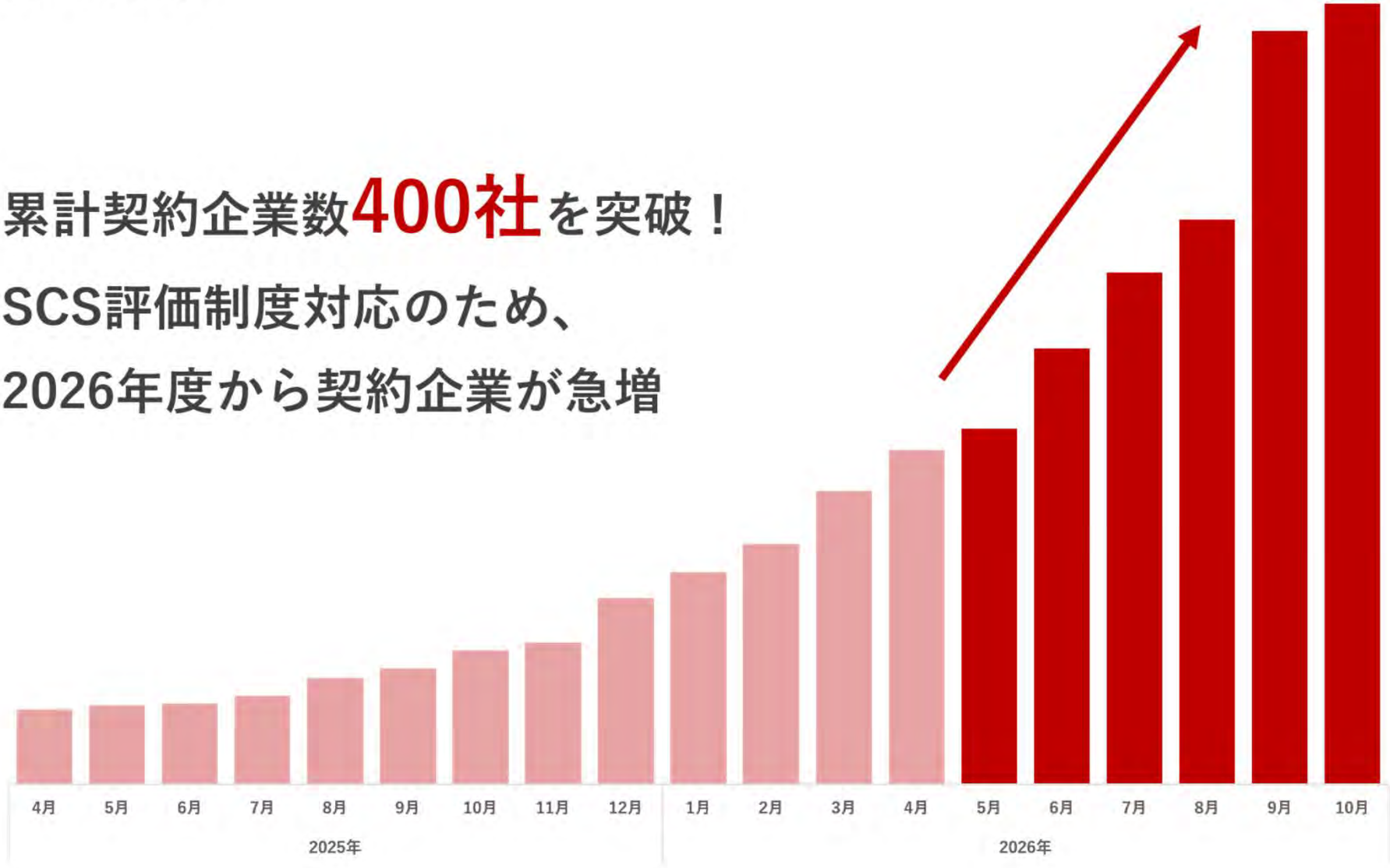
© MOTEX Inc.

サポアカ支援実績

累計契約企業数**400社**を突破！

SCS評価制度対応のため、

2026年度から契約企業が急増



© MOTEX Inc.

サポアカ支援実績

ご契約者様専用サイトの充実したコンテンツによる支援が好評



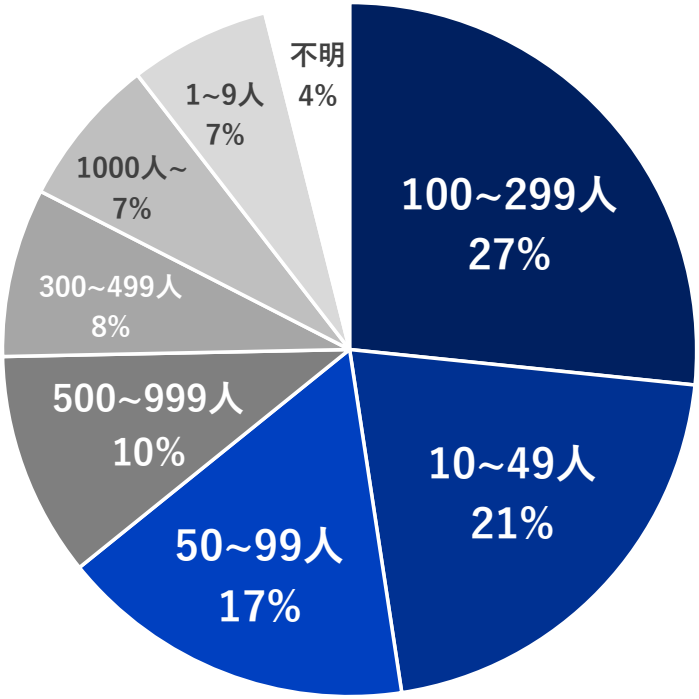
※ポータルサイトのコンテンツ満足度
2026年4月～9月における、ポータルサイトおよびポータルサイトより提供する各コンテンツへの満足度アンケートの結果（n=220）

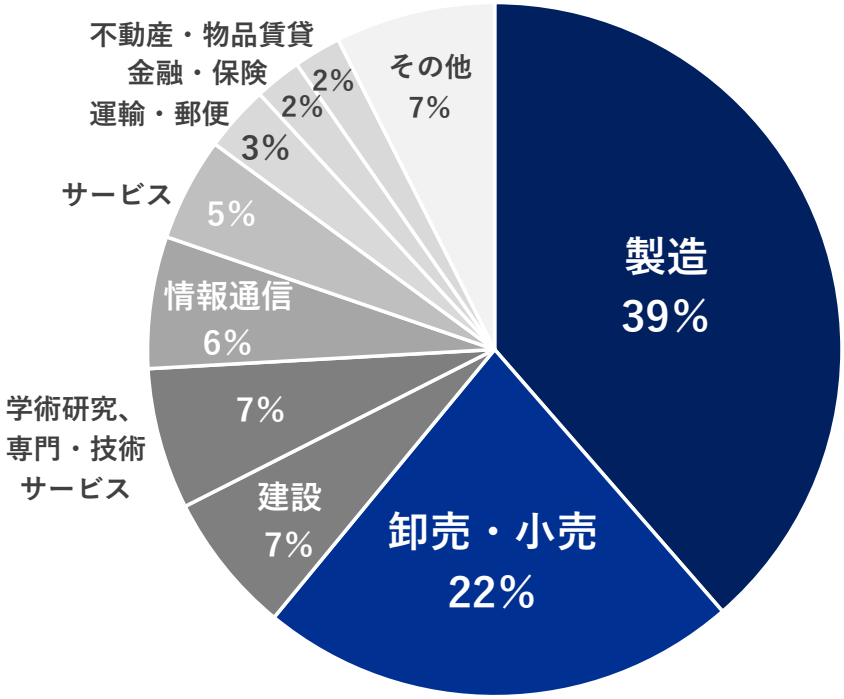
© MOTEX Inc.

サポアカをご利用いただいている企業の特徴

SCS評価制度への対応は、すでに大手企業だけでなく**中小・中堅企業にも広がっている**

サポアカご契約企業の属性分析結果





（数値はすべて弊社調べです）

© MOTEX Inc.

SCS評価制度対応を支援する3つのコース

星3取得から将来の星4水準まで、段階的に取り組める支援コース

＼ セキュリティ人材の育成からSCS評価制度の星3・星4取得支援など、総合的にサポート ／

SCS評価制度「星4」水準を含む、
総合的なサイバーセキュリティ対策を支援

- SCS評価制度 星３
- SCS評価制度 星4
- 各種ガイドラインで推奨とする対策

＼ SCS評価制度の星3取得に絞って支援 ／

SCS評価制度「星３」を
取得するための支援

- SCS評価制度 星３

学習コース（ベーシック）

定価：¥225,000
利用期間：3ヵ月

実践コース（ベーシック）

【新規購入時】
定価：¥450,000
利用期間：9ヵ月

【継続更新】
定価：¥120,000
利用期間：12ヵ月

実践コース（ライト）

【新規購入時】
定価：¥300,000
利用期間：9ヵ月

【継続更新】
定価：¥120,000
利用期間：12ヵ月

© MOTEX Inc.

SCS評価制度 星3取得応援キャンペーン！

ガイドライン対応
サポートアカデミー

実践コース（ライト） の初回購入¥300,000が、今なら¥225,000で始められます！

●キャンペーン概要
SCS評価制度への取り組みを開始しやすくするため、星3取得に特化した新コースの提供を開始します。
より多くの企業の制度対応を後押しするための応援キャンペーンです。

●キャンペーン対象/お申込条件
・「サイバーセキュリティ対策パッケージ 実践コース（ライト）」を新規にご購入いただく方
・本キャンペーンは、SCS評価制度の普及状況等を踏まえ、予告なく終了する場合があります。

●注意事項
・本キャンペーンは、キャンペーン適用あり／なしを選択してお申込みいただくことが可能です。
・キャンペーン適用後に実践コース（ベーシック）へアップグレードされる場合、アップグレード費用は通常価格￥150,000ではなく、
「サイバーセキュリティ対策パッケージ アップグレード（実践ライトキャンペーン-実践ベーシック）￥225,000」のご購入となります。
なお、実践コース（ベーシック）までの合計費用は￥450,000となります。

＼ 今なら選べる購入方法 ／
キャンペーン有り・無しを
選択可

●購入例



※アップグレードの場合は「実践コース（ベーシック）」との差額のみで「実践コース（ベーシック）」を利用できます。

© MOTEX Inc.

本日のまとめ

© MOTEX Inc.

ま　と　め



- ✓ SCS評価制度は、サプライチェーン全体で求められる**新しいセキュリティの共通基準**です。
- ✓ 実態調査からも、発注者側では取引先への星要請を見据えた準備が進み始めており、多くの企業では、初年度から**星の取得**が求められる可能性があります。
- ✓ 評価基準は幅広く、すべての基準への適合が求められるため、**正しい理解と客観的な現状把握が重要**になります。
- ✓ 2026年度末の制度開始に向けて、**今から準備を始めることが、取引先からの信頼確保や新たなビジネス機会の創出につながります**。
- ✓ ガイドライン対応サポートアカデミー（サポアカ）では、**星獲得に向けた準備から対応までを支援します**。



© MOTEX Inc.