取引先対応は大丈夫？
～経済産業省「セキュリティ対策評価制度」実践的対策～

エムオーテックス株式会社
営業本部　東日本営業部
津田 禎史

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
従業員数	472名（2025年4月現在）
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

LANSCOPEを通して、お客様の “Secure Productivity” (安全と生産性向上の両立)を支援

エンドポイントセキュリティ

統合エンドポイント管理

Endpoint Manager

- IT 資産管理・MDM
- 内部情報漏洩対策
- 外部脅威対策

AI アンチウイルス

Cyber Protection

- EPP
- EDR
- MDR

リモートコントロール

Remote Desktop

- リモートアクセス
- ヘルプデスク効率化

クラウドセキュリティ

Microsoft 365 セキュリティ

Security Auditor

- 監査ログ管理
- アラート管理

脆弱性診断

Professional Service

- Webアプリ 診断
- ネットワーク診断
- クラウド診断

ネットワークセキュリティ

AI型ネットワーク脅威検知

DARKTRACE

- NDR
- ネットワーク遮断
- Email 監視

サプライチェーンリスクマネジメント

Panorays

- セキュリティスコアリング
- ASM

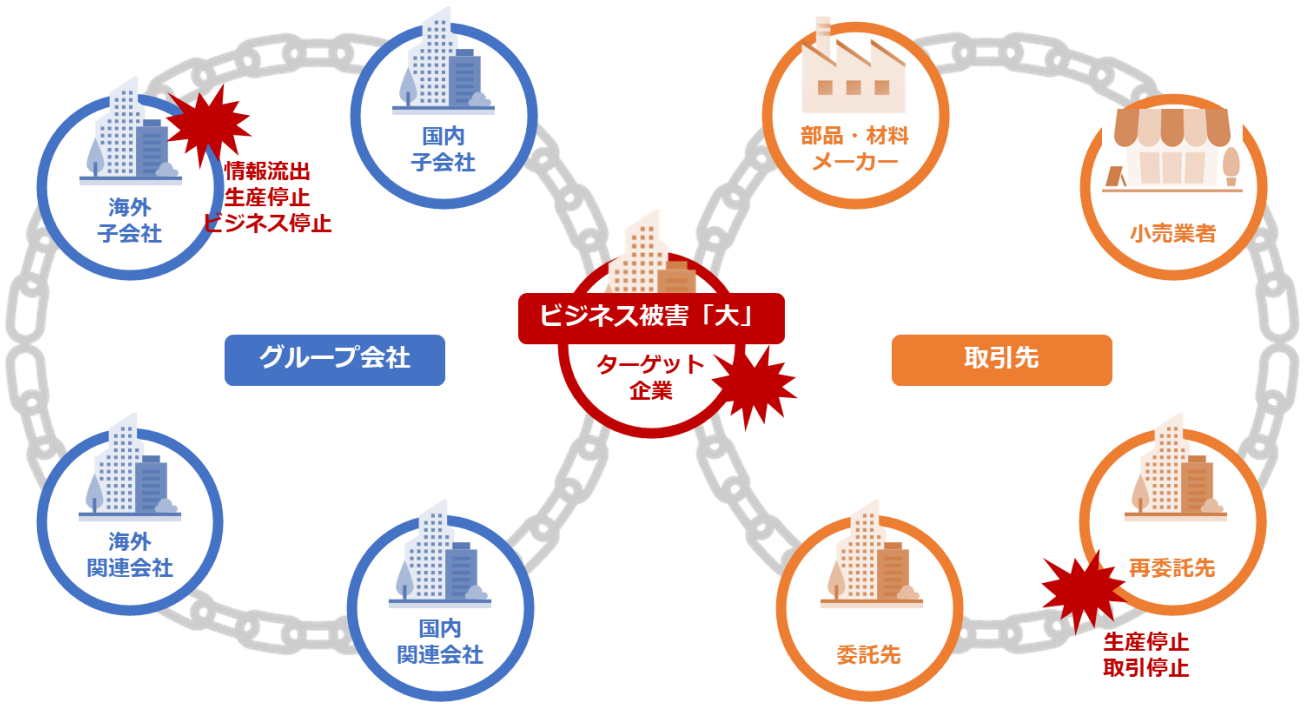
Professional Service コンサルティング／コンサルティングパッケージ

セキュリティ対策評価制度の最新情報

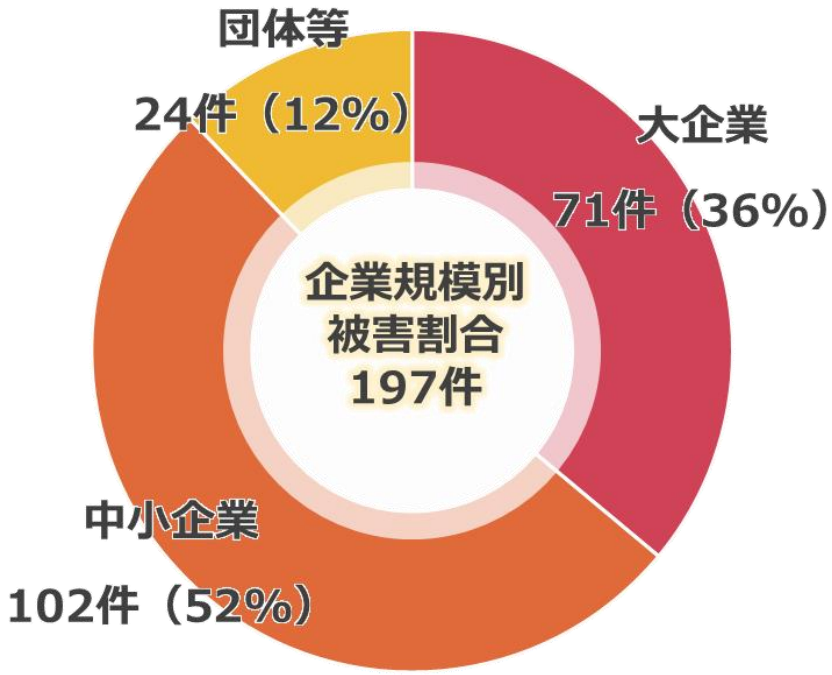
サイバー空間の安全確保には **すべての企業**が対策に取り組むことが**必須**
企業規模を問わず、対策を怠ると被害者ではなく**加害者**にもなりうる

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５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/R5/R05_cyber_jousei.pdf

某情報処理サービス企業がハッカー集団のサイバー攻撃の標的に業務を委託していた全国の自治体や企業などに**被害が拡大**

某情報処理サービス企業

情報処理サービスなどを展開する某企業で、2024年5月に社内の一部のサーバーやPCがランサムウェアに感染。ハッカー集団が犯行声明を出し、盗み取ったとするデータを公開した。

複数の地方自治体

新型コロナ予防接種券や
納税者などの個人情報など

15万件～103万件

大手機器メーカー

顧客の利用・請求明細など

6万件

商工会議所

会員企業の個人情報

4万件

某情報処理サービス企業がハッカー集団のサイバー攻撃の標的に業務を委託していた全国の自治体や企業などに**被害が拡大**

某情報処理サービス企業

情報処理サービスなどを展開する某企業で、2024年5月に社内の一部のサーバーやPCがランサムウェアに感染。ハッカー集団が犯行声明を出し、盗み取ったとするデータを公開した。

ただの不幸な事故では片づけられない、企業側のセキュリティ対策の甘さ

- **本来であれば個人情報はネット環境から分離された別サーバーで保存されているはずだったが、それが徹底されていなかった**
- **委託元との契約終了後にデータ消去することを取り決めており、削除したとの報告も行っていたにも関わらず、実際には削除されていなかった**

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**

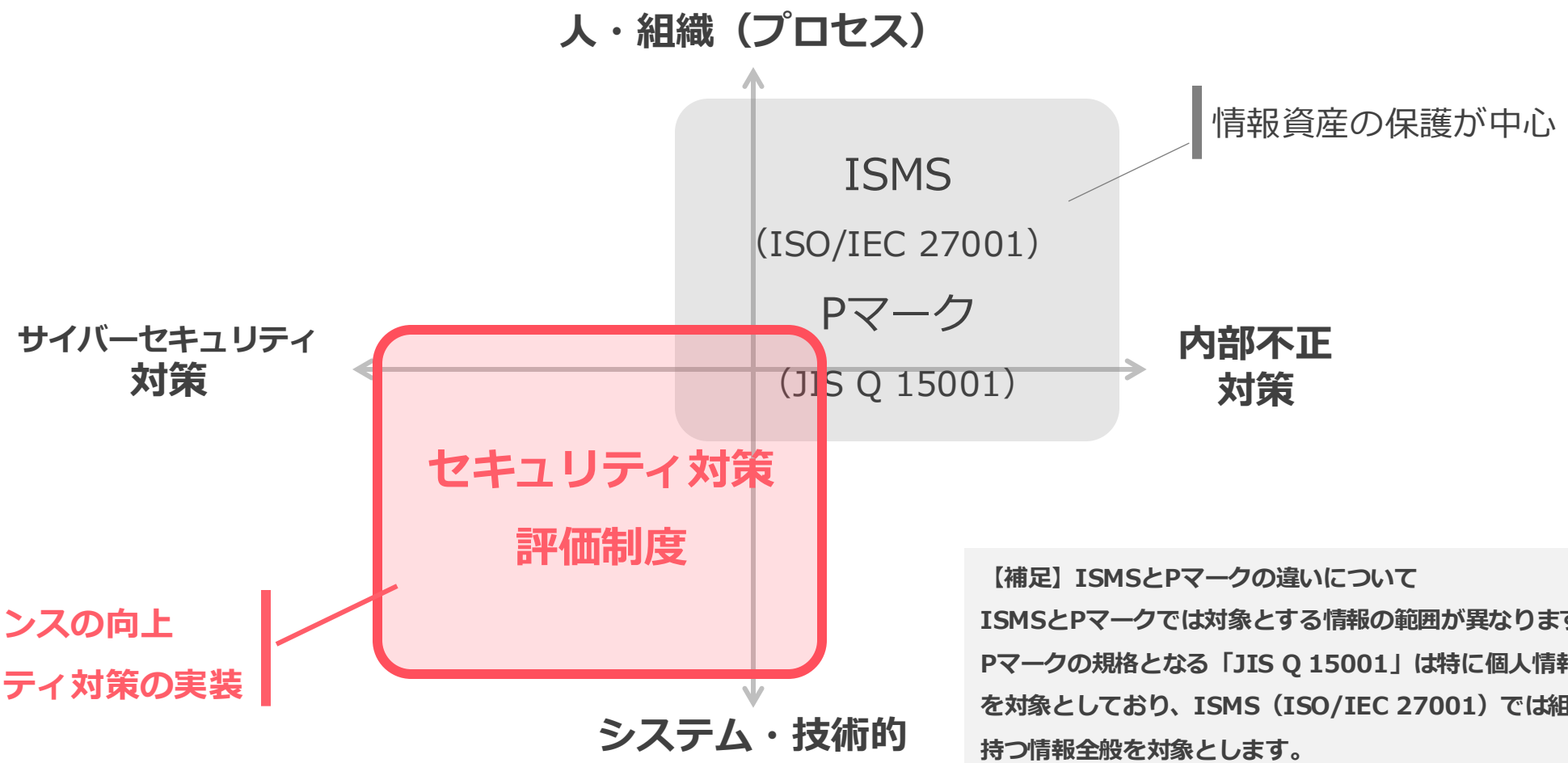
【セキュリティ対策評価制度】
基準に適合する対策が実施できている
ことを**チェック・認定**

	★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
評価	自己宣言	自己宣言	自己評価 （専門家による評価）	第三者評価	未定
項目	－	－	25項目	44項目	未定

※「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。

相互補完的な制度として両輪で発展予定

「ISMS」「Pマーク」と「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

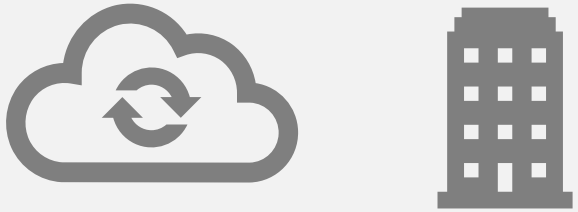
ISMSとPマークでは対象とする情報の範囲が異なります。
Pマークの規格となる「JIS Q 15001」は特に個人情報のみを対象としており、ISMS（ISO/IEC 27001）では組織が持つ情報全般を対象とします。

発注者側の企業が取引先に対して必要な認定の区分を設定し**要請する**

判断の観点		★3	★4
ビジネス観点	データ保護	全ての企業	• 発注者の**重要な機密情報が取引先のIT基盤**で扱われている
	事業継続		• **取引先が停止すると、自社業務に許容できない遅延**が発生する
システム観点	ネットワーク アクセス		• 取引先から**発注者の内部システムにアクセス可能**である

【追加要素 例】
- 直近、取引先や同業他社でインシデントが発生し、**リスクが高まっている**
- **再委託先に自社にとって重要な事業者**が含まれる

▼★４に該当すると考えられるケース

発注者の重要な機密情報が取引先のIT基盤で扱われている	取引先が停止すると、自社業務に許容できない遅延が発生する	取引先から発注者の内部システムにアクセス可能である
業務委託を受けている企業など	**クラウド・子会社など**	**システム保守・監視業者など**
		
例） • 営業代行（テレマコール） • 運送、製造、建築設計 • Webサイト制作	例） • クラウド事業者（メール、ERPなど） • データセンター事業者 • 子会社	例） • IT運用・保守を提供する企業 • セキュリティ監視（SOC）企業

評価機関による評価に加え、実際のシステムへアクセスして検証する技術検証も実施される

正しいセキュリティ対策を実施しなければ星評価の獲得は困難と想定されます。

★3

評価の主体は**有資格者**

有資格者による厳格な審査

❶ 自社で自己評価結果の記入

↓

❷ 有資格者による評価 ※

↓

※有資格者は社内外どちらでもOK

※有資格者の例
　情報処理安全確保支援士

↓

❸ 登録機関に提出／台帳へ登録

★4

評価の主体は**評価機関**

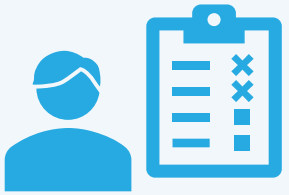
技術検証が課せられるため、適正な対策を講じなければ星獲得は困難

STEP❶

自社で
回答準備

STEP❷

評価機関による評価の実施



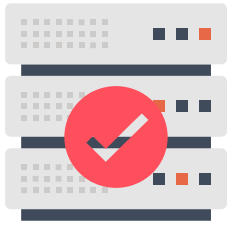
STEP❸

技術検証事業者による検証の実施

STEP❹

登録機関に提出
台帳へ登録

パソコン・システムに対して抜き取りで**実監査の実施**が考えられる
＝正しい対策を漏れなく実施しないと認定を受けられない！



社有PC・社有携帯

- ✓ ウイルス対策ソフトのパターンファイルが最新？
- ✓ サポート切れのOSやソフトウェアは使っていない？
- ✓ 認証(ログイン)は強固な設定になっている？

etc

サーバー

- ✓ ウイルス対策ソフトのパターンファイルが最新？
- ✓ サポート切れのOSやソフトウェアは使っていない？
- ✓ 認証(ログイン)は強固な設定になっている？

etc

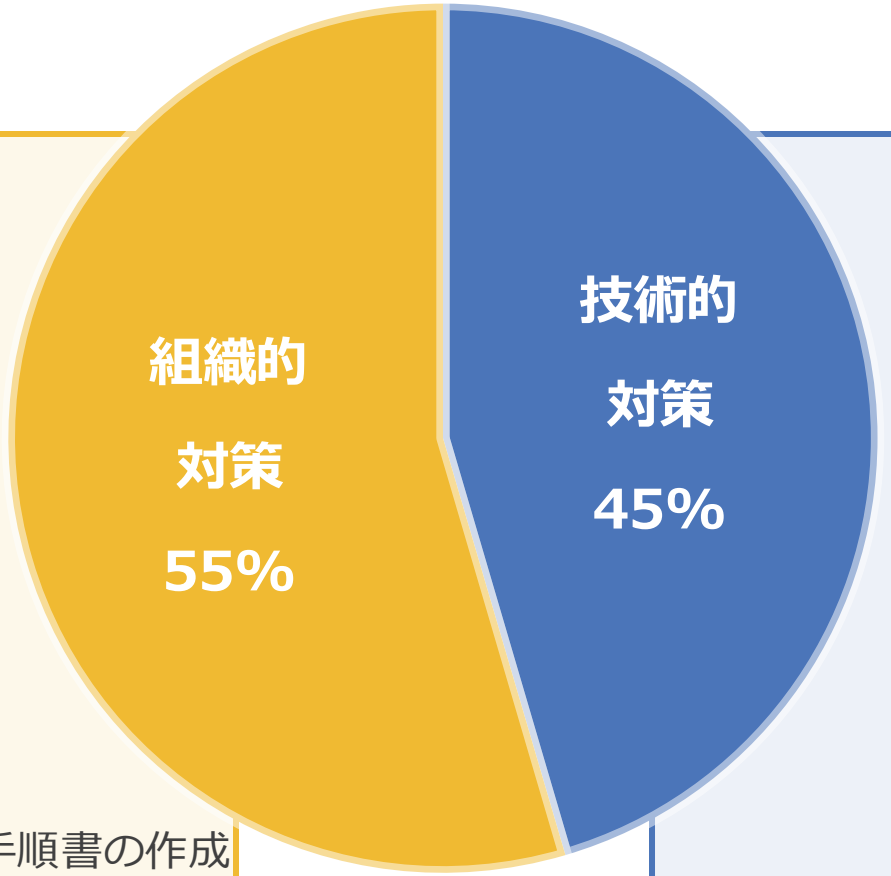
ファイアウォール

- ✓ 最新バージョン？
- ✓ 不要なポートが空いたままになってない？
- ✓ デフォルトの管理パスワードは使ってないよね？

etc

★４で求められる組織的対策と技術的対策

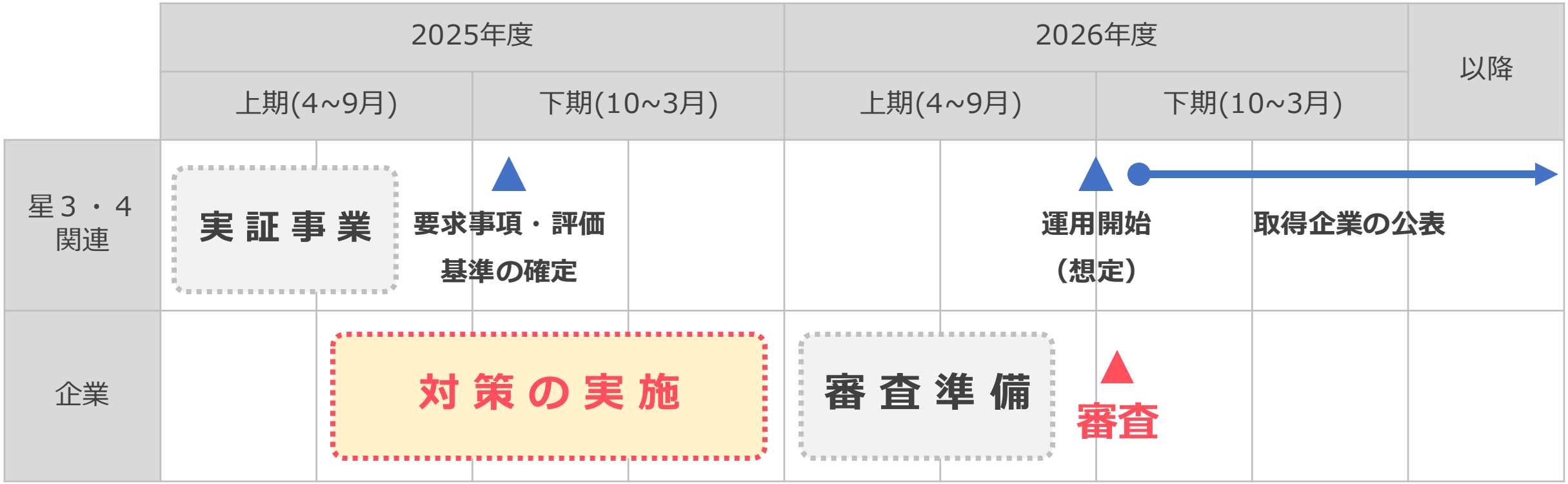
- 社内・管理ルールの作成・教育
- セキュリティ体制の整備
- セキュリティ対策状況の棚卸し
- サプライチェーンの管理
- 情報資産の管理
- ネットワークの一覧化
- サーバエリアの入退室管理
- セキュリティ教育
- セキュリティインシデントの対応手順書の作成
- 復旧手順書の作成　など



- 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

制度開始は**2026年度10月ごろ**の予定

いち早く星を獲得するためには、**2025年度に必要な対策を進めていく必要**があります！



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構築に向けた中間取りまとめ」を公表しました」
「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構築に向けた中間取りまとめ」（経済産業省、2025年4月14日）

ガイドライン対応サポートアカデミー

好きな時に、ずっと使える。学びとコンサルで築く確かなセキュリティ。

お客様のセキュリティレベルの向上を「アカデミー形式」で実現するコンサルティングパッケージです。
個別支援に加え、ポータルを活用した集合学習を通じて、体系的かつ効果的にセキュリティガイドラインの遵守を
支援します。全てのお客様対応のプランと、業界特化したプランをご用意しています。

一般的なコンサルティングサービスとの違い

	一般的なコンサルティング サービス	ガイドライン対応 サポートアカデミー
目的	定めた目的（成果物）の完遂	セキュリティ運用を根付かせる （セキュリティ人材の育成・支援）
主体性	コンサルタント	お客様ご自身
支援内容	定めた目的の完遂のため コンサルタントが主体となり対応	人材育成・対策の実践に必要な 知識取得・必要なツール・サポート提供
価格	高額 数百万～数千万※3	低価格 標準的なプランで45万円※2
支援期間	スポット 数百万～数千万※3	継続支援が可能 年間12万円

※1：9か月間の初回契約を満了後、1年ごとの契約更新が可能です。
※2：サポートアカデミーのすべての支援内容を9か月間利用できるプランの価格です。購入プランにより異なります。プランごとの価格はサービス詳細をご確認ください。
※3：総合的なセキュリティ対策をエムオーテックスへご依頼いただいた場合の参考価格となります。

「セキュリティ対策評価制度」に向けて今すぐに始めるべき3つのアクション

ガイドライン対応サポートアカデミー

正しくセキュリティ対策を理解する

解説講座

知識の習得を目的とした講座動画
専用ポータルから
いつでも何度でも視聴が可能

自社の対策状況の現状把握を行う

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
たチェックシートのご提供

対策方法や実施スケジュールを検討する

カウンセリング

お客様ごとに「対策プログラム」を作成
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

主な支援内容：チェックシート

サイバーセキュリティ対策として実施が必要な事項を定義したチェックシートをご提供します。
現在の対策状況を入力することで、自社の弱点が一目でわかる結果サマリーを作成できます。

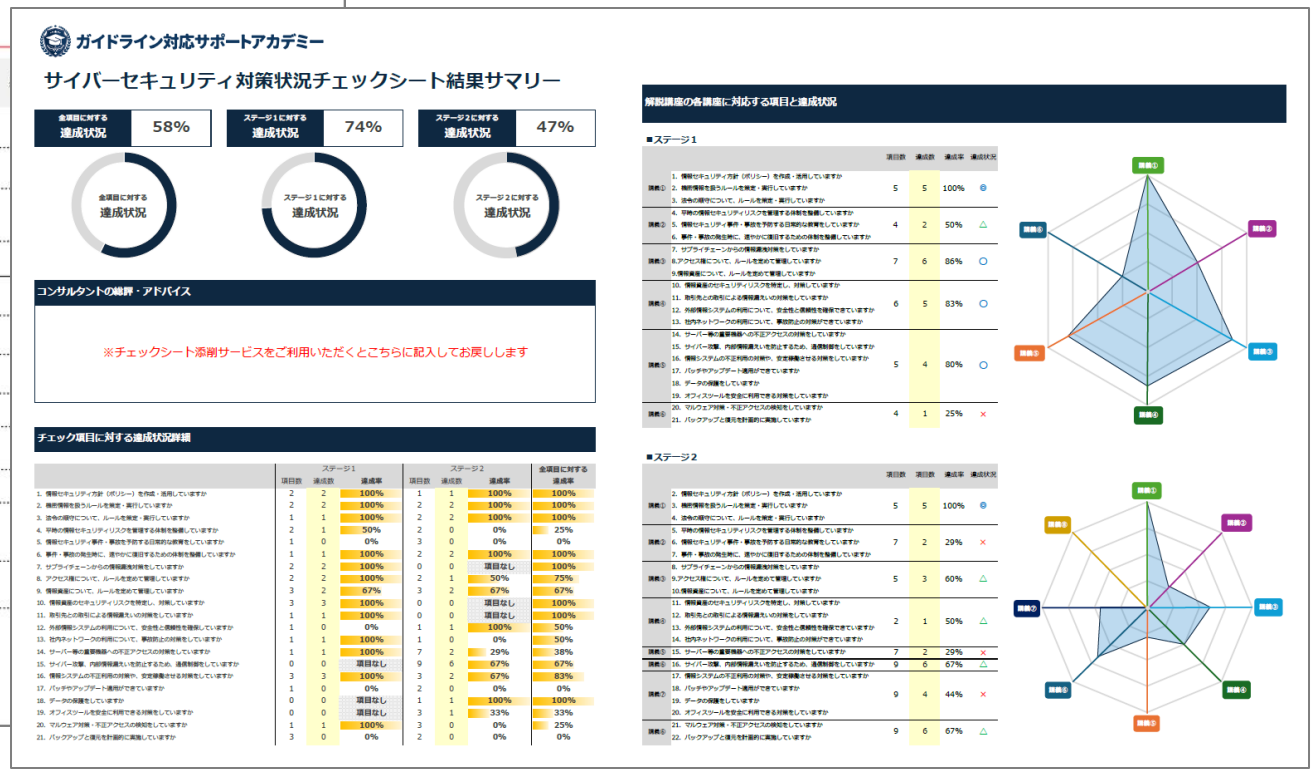
本チェックシートは、主に以下の内容をベンチマークして作成しています。
・経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク
・IPA 中小企業の情報セキュリティ対策ガイドライン
・情報セキュリティ対策ベンチマーク（IPA 独立行政法人情報処理推進機構）


ガイドライン対応サポートアカデミー達成状況チェックシート V1.1

「お客様入力欄」の入力方法については「初めにお読みください」の内容をご参照ください

達成状況チェック項目と達成状況 — お客様入力欄

カテゴリ	No	ステージ	チェック項目	判定	達成基準	達成状況をご入力ください
1. 情報セキュリティ方針（ポリシー）を作成・活用していますか	1	1st	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	▽プルダウンで選択ください
					文書内に「経営者の責任」「法令順守」の内容が含まれている	▽プルダウンで選択ください
	2	1st	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	-	【作成したポリシーがA/Bのいずれかの状態にある】 A：ポリシーが社内に周知されている B：従業員が誰でも容易に確認できる	▽プルダウンで選択ください
	3	2st	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ていますか	-	年に1回以上の頻度で見直ししている	▽プルダウンで選択ください
2.機密情報を扱うルールを策定・実行していますか	4	1st	自社の守秘義務のルールを規定し、守らせていますか	-	自社の守秘義務を文書化している	▽プルダウンで選択ください
					守秘義務には「退職・期間満了時に会社の機密情報を持ち出さない」という内容を含めている	▽プルダウンで選択ください
					社員の入社時、派遣社員等の受け入れ時に、守秘義務について説明している	▽プルダウンで選択ください
	5	1st	BYOD含む情報機器について、取り扱いのルールを決めて情報漏えいを防止していますか	-	情報機器の利用ルールを策定している	▽プルダウンで選択ください
					利用ルールには「利用開始時・終了時の手続き」「利用中の遵守・禁止事項」「紛失時の手続き」を含んでいる	▽プルダウンで選択ください
					利用ルールを容易に確認できる状態にしている	▽プルダウンで選択ください
					【利用中の遵守事項に①～②をすべて含めている】 ①職務時にパソコン画面の覗き見や勝手な操作ができないように設定する ②退社時にノートパソコンや備品の盗難防止対策を実施する	▽プルダウンで選択ください
	6	2st	定めたルールが守られるよう、誓約書・契約書を提出・締結させていますか	-	従業員に対して守秘義務の誓約書を提出させている （派遣社員など社外要員を除く）	▽プルダウンで選択ください
					【派遣社員・受入出向社員について、①～②をすべて実施している】 ①派遣元、出向元企業と守秘義務に関する契約（NDAなど）を締結している ②契約書に「業務で知り得た情報を外部に漏えいさせない」旨の記載がある	▽プルダウンで選択ください


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状況チェックシート結果サマリー

全項目に対する達成状況	ステージ1に対する達成状況	ステージ2に対する達成状況
58%	74%	47%

コンサルタントの総評・アドバイス

※チェックシート添削サービスをご利用いただくとこちらに記入してお戻しします

チェック項目に対する達成状況詳細

	ステージ1			ステージ2			全項目に対する
	項目数	達成数	達成率	項目数	達成数	達成率	達成率
1. 情報セキュリティ方針（ポリシー）を作成・活用していますか	2	2	100%	1	1	100%	100%
2. 機密情報を扱うルールを策定・実行していますか	2	2	100%	2	2	100%	100%
3. 法令の順守について、ルールを策定・実行していますか	1	1	100%	2	2	100%	100%
4. 平時の情報セキュリティリスクを管理する体制を整備していますか	2	1	50%	2	0	0%	25%
5. 情報セキュリティ事件・事故を予防する目的の教育をしていますか	1	0	0%	3	0	0%	0%
6. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか	1	1	100%	2	2	100%	100%
7. サプライチェーンからの情報漏洩対策をしていますか	2	2	100%	0	0	項目なし	100%
8. アクセス権について、ルールを定めて管理していますか	2	2	100%	2	1	50%	75%
9. 情報資産について、ルールを定めて管理していますか	3	2	67%	3	2	67%	67%
10. 情報資産のセキュリティリスクを特定し、対策していますか	3	3	100%	0	0	項目なし	100%
11. 取引先との取引による情報漏えいの対策をしていますか	1	1	100%	0	0	項目なし	100%
12. 外部情報システムの利用について、安全性と信頼性を確保していますか	1	0	0%	1	1	100%	50%
13. 社内ネットワークの利用について、事故防止の対策をしていますか	1	1	100%	1	0	0%	50%
14. サーバー等の重要機器への不正アクセスの対策をしていますか	1	1	100%	7	2	29%	38%
15. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか	0	0	項目なし	9	6	67%	67%
16. 情報システムの不正利用の対策や、安定稼働させる対策をしていますか	3	3	100%	3	2	67%	83%
17. パッチやアップデート適用ができていますか	1	0	0%	2	0	0%	0%
18. データの保護をしていますか	0	0	項目なし	1	1	100%	100%
19. オフィスツールを安全に利用できる対策をしていますか	0	0	項目なし	3	1	33%	33%
20. マルウェア対策・不正アクセスの検知をしていますか	1	1	100%	3	0	0%	25%
21. バックアップと復元を計画的に実施していますか	3	0	0%	2	0	0%	0%

解説講座の各講座に対応する項目と達成状況

■ステージ1

		項目数	達成数	達成率	達成状況
講義①	1. 情報セキュリティ方針（ポリシー）を作成・活用していますか 2. 機密情報を扱うルールを策定・実行していますか 3. 法令の順守について、ルールを策定・実行していますか	5	5	100%	◎
講義②	4. 平時の情報セキュリティリスクを管理する体制を整備していますか 5. 情報セキュリティ事件・事故を予防する目的の教育をしていますか 6. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか	4	2	50%	△
講義③	7. サプライチェーンからの情報漏洩対策をしていますか 8. アクセス権について、ルールを定めて管理していますか 9. 情報資産について、ルールを定めて管理していますか	7	6	86%	○
講義④	10. 情報資産のセキュリティリスクを特定し、対策していますか 11. 取引先との取引による情報漏えいの対策をしていますか 12. 外部情報システムの利用について、安全性と信頼性を確保できていますか 13. 社内ネットワークの利用について、事故防止の対策ができていますか	6	5	83%	○
講義⑤	14. サーバー等の重要機器への不正アクセスの対策をしていますか 15. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか 16. 情報システムの不正利用の対策や、安定稼働させる対策をしていますか 17. パッチやアップデート適用ができていますか 18. データの保護をしていますか 19. オフィスツールを安全に利用できる対策をしていますか	5	4	80%	○
講義⑥	20. マルウェア対策・不正アクセスの検知をしていますか 21. バックアップと復元を計画的に実施していますか	4	1	25%	×

■ステージ2

		項目数	達成数	達成率	達成状況
講義①	2. 情報セキュリティ方針（ポリシー）を作成・活用していますか 3. 機密情報を扱うルールを策定・実行していますか 4. 法令の順守について、ルールを策定・実行していますか	5	5	100%	◎
講義②	5. 平時の情報セキュリティリスクを管理する体制を整備していますか 6. 情報セキュリティ事件・事故を予防する目的の教育をしていますか 7. 事件・事故の発生時に、速やかに復旧するための体制を整備していますか	7	2	29%	×
講義③	8. サプライチェーンからの情報漏洩対策をしていますか 9. アクセス権について、ルールを定めて管理していますか 10. 情報資産について、ルールを定めて管理していますか	5	3	60%	△
講義④	11. 情報資産のセキュリティリスクを特定し、対策していますか 12. 取引先との取引による情報漏えいの対策をしていますか 13. 外部情報システムの利用について、安全性と信頼性を確保できていますか 14. 社内ネットワークの利用について、事故防止の対策ができていますか	2	1	50%	△
講義⑤	15. サーバー等の重要機器への不正アクセスの対策をしていますか	7	2	29%	×
講義⑥	16. サイバー攻撃、内部情報漏えいを防止するため、通信制御をしていますか	9	6	67%	△
講義⑤	17. 情報システムの不正利用の対策や、安定稼働させる対策をしていますか 18. パッチやアップデート適用ができていますか 19. データの保護をしていますか 20. オフィスツールを安全に利用できる対策をしていますか	9	4	44%	×
講義⑥	21. マルウェア対策・不正アクセスの検知をしていますか 22. バックアップと復元を計画的に実施していますか	9	6	67%	△

2 つのコースと提供価格

※1 価格は税別表示です
※2 実施回数の制限があります。

＼ まずは自社の現状や課題を把握したい ／

学習コース

定価：¥225,000 ※1
利用期間：3ヵ月

含まれる支援内容

チェックシート	個別相談（メール）
解説講座	個別相談（Web会議）※2
チェックシート添削 ※2	
各種規程ひな型	

＼ 改善を進めたい・セキュリティレベルを維持したい ／

実践コース

【新規購入時】 ※1
定価：¥450,000
利用期間：9ヵ月

【継続更新】 ※1
定価：¥120,000
利用期間：12ヵ月

含まれる支援内容

チェックシート	個別相談（メール）	対策講座
解説講座	個別相談（Web会議）※2	教育コンテンツ
チェックシート添削 ※2	カウンセリング ※2	各種運用支援ツール
各種規程ひな型	よろづ相談会	お役立ち情報配信

個別相談(Web会議)はそれぞれ毎月1回分を標準価格に含みます。メールでのご相談は回数無制限です！

ま と め

- ✓ セキュリティ対策評価制度は、ISMS取得済み企業を含むすべての企業が対象です。**星の獲得をいち早く目指すことで、ビジネスチャンスの拡大が期待**できます。

- ✓ 多くの企業が目指す星４評価の取得は、評価機関による厳正な審査と技術検証を伴います。そのため、**必要なセキュリティ対策を“正しく”理解し、実践すること大切**です。

- ✓ ガイドライン対応サポートアカデミーでは、**“正しく”理解すること、自社の現状把握など、星獲得に向けた支援が可能**です。
  星獲得に向けた準備でお困りの場合は、ぜひエムオーテックスにご相談ください。