ndis
NDIソリューションズ株式会社

星取得をめざすサプライチェーン関連企業向け

セキュリティ対策評価制度の概要と実践ポイント徹底ガイド

～ 制度を活用して取引先から 選ばれる企業 に ～

2026年6月版

※ 2026年3月27日 経産省公開の最新情報を反映しています

ndis
NDIソリューションズ株式会社

はじめに

経済産業省の主導により、2026年下期「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」が施行されます。
この制度の施行は、サプライチェーンに関わる企業にとって、自社のセキュリティ対応が取引先からの信頼やビジネス機会を大きく左右することを意味します。

サプライチェーンに関与する企業の皆さまには、本制度への対応を単なる「義務」と捉えるのではなく、公的機関および取引先の双方から信頼を獲得し、ビジネスを広げるためのチャンスとして、ぜひ最大限にご活用いただければ幸いです。

本資料の構成

以下の5つのセクションで構成しています。

※ 本資料は、2026年3月27日に経済産業省から公開された**「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」**の内容を反映しています。
https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

ndis
NDIソリューションズ株式会社

Section 1

セキュリティ対策評価制度がもたらすサプライチェーン関連企業への影響

Section 1

セキュリティ対策評価制度がもたらすサプライチェーン関連企業への影響

「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」がはじまります

2026年下期、経済産業省の主導で『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』の施行が予定されています。企業を星マークで評価レベルを1～5段階に分け、可視化することで、サプライチェーン全体のセキュリティ水準向上を目指しています。

経済産業省
Ministry of Economy, Trade and Industry

「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」を公表しました（2026/3/27）
経産省は、本方針に基づき、2026年度末頃の制度開始を目指した取組を進める予定です。

https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

「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」 が施行されるに至った背景

― 2つの課題と、制度が目指すもの

＜課　題 1＞サイバー攻撃・ランサムウエア被害の深刻化

近年のサプライチェーンを狙ったサイバー攻撃・ランサムウエア被害の深刻化です。ここ数年でサプライチェーン経由での情報漏えいや事業継続の障害が急増しています。
IPAの『情報セキュリティ10大脅威 2026』では、『サプライチェーンや委託先を狙った攻撃』が2位に4年連続でランクインしており、依然として高い脅威であることが示されています。ランサムウェアの被害件数は年間200件以上、その63%が中小企業です。さらに大手企業でも影響は避けられず、2025年10月に発生した大手食品企業のランサムウエア被害は記憶に新しく、被害の規模は甚大でした。こういったことから、サプライチェーン全体でのセキュリティ対策は急務です。

課題1　近年におけるサプライチェーン経由のサイバー攻撃による被害の深刻化
～ サプライチェーン全体が、“狙われる経路”になっている 現実 ～

IPA 独立行政法人 情報処理推進機構
情報セキュリティ10大脅威2026
サプライチェーンや委託先を狙った攻撃が
4年連続で2位にランクイン
※1

日本国内企業の
ランサムウエア被害件数
発生件数 年間 200件 以上
内 63% は中小企業
※2

多発する
大手企業のランサムウエア被害
2025年に発生した 大手食品会社 の被害
物流をはじめとする影響は甚大に･･･

※1 出展：情報セキュリティ10大脅威2026
※2 出典：令和6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

Section 1

セキュリティ対策評価制度がもたらすサプライチェーン関連企業への影響

＜課　題 2＞取引先ごとに異なるセキュリティ要求が企業の負担に･･･

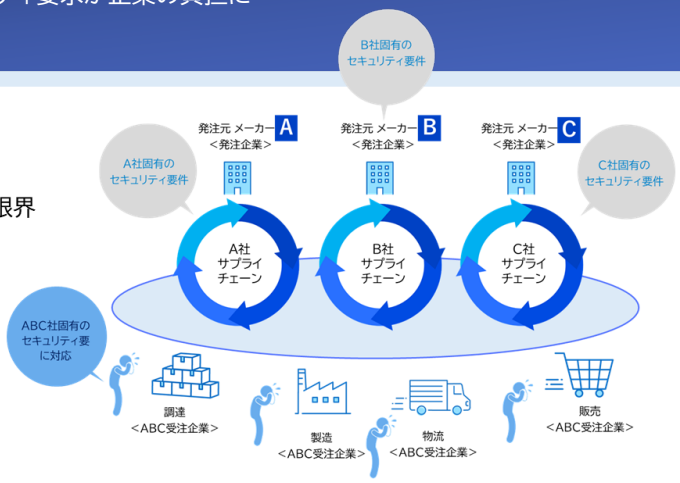
発注企業からは『取引先のセキュリティをきちんと担保せよ』という指示があり、一方、受注企業から見れば『取引先ごとにバラバラな要求で対応が限界』という状況です。
結果として、対策の重複や非効率が生まれ、サプライチェーン全体でのセキュリティ対策の底上げが進みにくいという課題が浮き彫りになっています。

課題2　取引先ごとに異なるセキュリティ要求が企業の負担に･･･

発注企業の立場　取引先のセキュリティを担保せよ

受注企業の立場　取引先ごとにバラバラな要件対応で限界

セキュリティ対策の**重複・非効率化**が進み
サプライチェーン全体の底上げが進まない･･･
「守りたいのに、守り方が統一されていない」



制度施行の背景には
「サプライチェーンを狙った攻撃の深刻化」と**「取引先ごとに異なる要求による負担の増大」**が深く関連しています。

「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」の目的

セキュリティ対策評価制度の目的＝
「サプライチェーンにおけるセキュリティ対策の重要性を踏まえ
満たすべきセキュリティ対策を明確化し、対策状況を可視化することで
サプライチェーン全体でのセキュリティ水準の向上を目指す」

つまり、関連各社のセキュリティ対策状況を可視化することで、サプライチェーン全体でセキュリティ水準が底上げされて、取引先との信頼性向上を実現します。この制度を活用することで『守りの対策』が整理されるだけでなく、サプライチェーン全体での信頼構築に直結します。

課題 1
課題 2
＞ 制度の目的

セキュリティ対策を明確化し、対策状況を可視化することで、サプライチェーン全体での、セキュリティ水準の向上を目指す。

01 取引先に求めるセキュリティ要件の統一／明確化

02 取引各社のセキュリティ対策状況を可視化

03 取引先との信頼関係を強化
＜発注元 ⇔ 取引先＞

Section 1

セキュリティ対策評価制度がもたらすサプライチェーン関連企業への影響

セキュリティ対策評価制度施行による、発注者側のメリット／受注者側のメリット

統一基準で、セキュリティ対策状況を可視化することで、発注・受注者双方の信頼強化とサプライチェーン産業全体の発展に寄与します。

発注者側のメリット

- 受注者側のセキュリティ対策状況が可視化され **評価判断が容易** になる。
- 統一基準によって、リスクの低減と安心感が向上し **取引先選定がスムーズ** になる。

受注者側のメリット

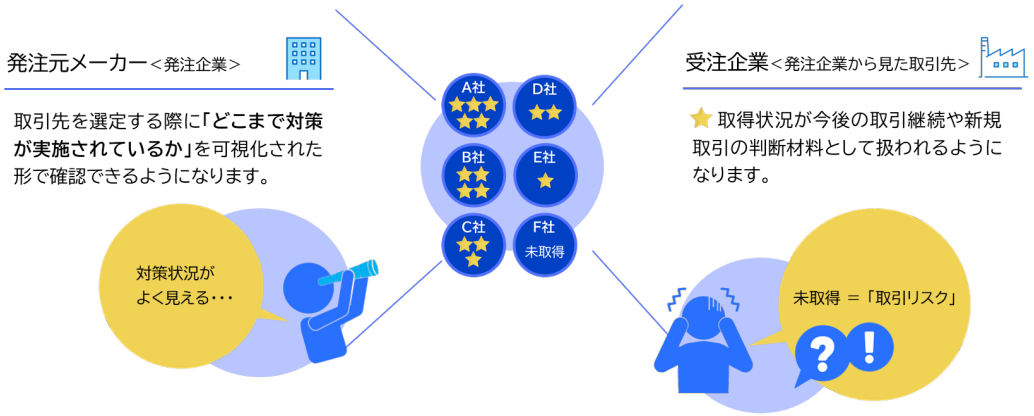
- 国が定めた基準に基づく対策の実施により
  取引先に対して **セキュリティ対策を正面から説明できる。**
- 取引先ごとに異なる対策要求への対策負担が軽減され
  標準的な対策レベルの維持が可能。

企業への影響　― 制度施行により、これから起こると予想されること ―

これから先は、セキュリティ対策の強度が取引や調達の “新しいスタンダード” として定着していくと考えられます。

- ✓ 発注企業は、取引先を選定する際に「どこまで対策が実施されているか」を可視化された形で確認できるようになります。
- ✓ 一方、受注企業の立場から見ると、星の取得状況が今後の取引継続や新規取引の判断材料として扱われるようになります。

つまり、“対策していない企業”が、自然と選ばれにくくなる時代に入る、ということです。
制度対応は、もはや先送りできるテーマではなく、**「ビジネスを守るための必須条件」**へと変わりつつあると言えるかもしれません。



制度施行後は **“セキュリティ対策の強度”** が新しい取引条件のスタンダードに

Section 1

セキュリティ対策評価制度がもたらすサプライチェーン関連企業への影響

セキュリティ対策評価制度を活用して“選ばれる企業”へ

ネガティブにとらえないで！
制度対応は **ビジネスチャンス！“選ばれる企業”**への近道

事実として、対応が遅れると、発注企業からの星取得要請に応えられず、ビジネス機会を逃してしまう可能性も否めません。ただし、一方で先行対応しておくと、取引先からの信頼を獲得でき、調達条件や取引機会で優位に立てます。
つまり、この制度対応のメリットは “選ばれる企業”になるためのチャンス　とも言えます。

さらなる副産物として、制度に対応した企業は、「サイバー攻撃に強い」ということです。
つまり星取得の段階で、セキュリティ対策を可視化するので、おのずと体制が強化され、サイバー攻撃や情報漏えいのリスクが自然に低減します。ビジネス拡大も大事ですが、「自社をサイバー攻撃から守る」ということが、まず前提になります。

★取得による企業のメリット

取引先信用度の向上／ビジネスチャンスの拡大

- 取引先からの信頼獲得
- “選ばれる企業”として他社との差別化
- 調達・取引条件での優位性
- サプライチェーン全体での評価向上に貢献

サイバー攻撃に強い会社になる

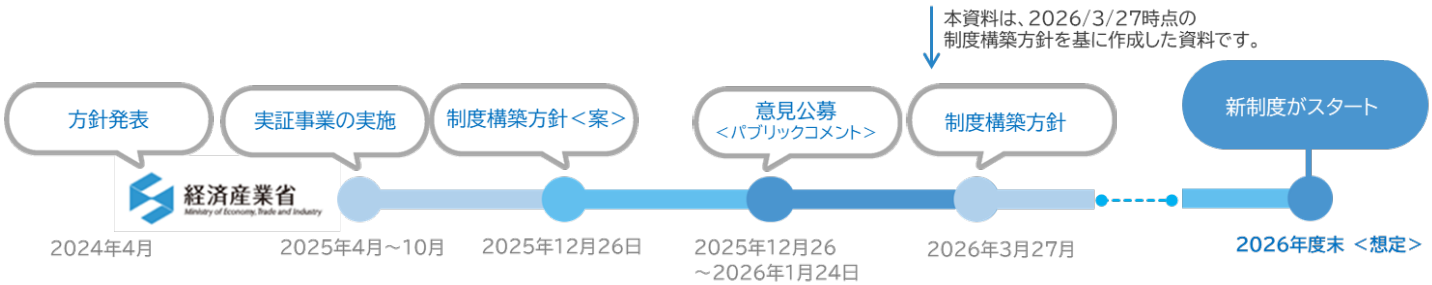
自社のセキュリティ体制が強化されるため
サイバー攻撃や情報漏えいのリスクが自然に低減する。

政府機関の承認
★取得＝「サイバー攻撃に強い会社」

セキュリティ対策評価制度の全体像

セキュリティ対策評価制度とは？

経済産業省の主導により企業の「サイバーセキュリティ対策状況」を星<★>5段階で格付けする新制度。
2026年末頃の施行予定（運用開始）。



セキュリティ対策評価制度の目的 → ✓ サプライチェーン全体でのセキュリティ水準の向上
✓ 企業のセキュリティ対策レベルの可視化

Section 2

セキュリティ対策評価制度の全体像

※ 本セクションは、2026年3月27日に経済産業省から公開された**「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」** の内容を反映しています。
https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

新規追加	上記発表により、追加された内容
更 新	上記発表により、更新された内容
	更新された内容の主な変更点

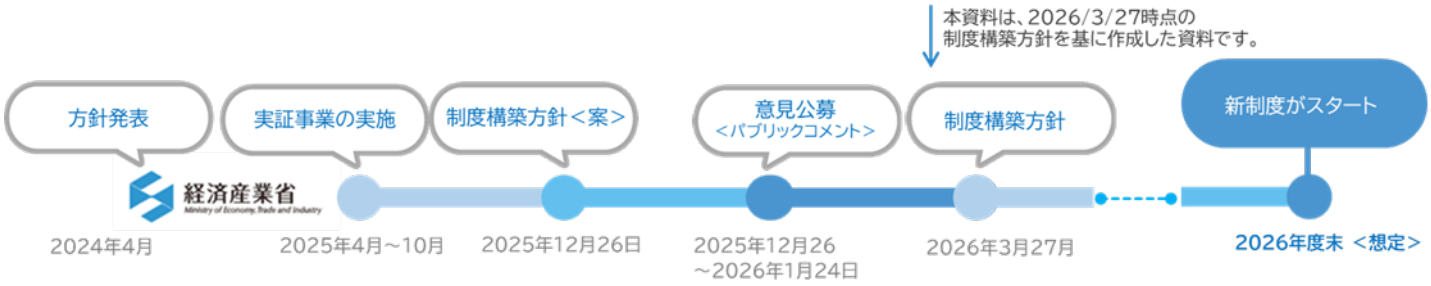
Section2

セキュリティ対策評価制度の全体像

セキュリティ対策評価制度の全体像

セキュリティ対策評価制度とは？

経済産業省の主導により企業の「サイバーセキュリティ対策状況」を星<⭐>5段階で格付けする新制度。
2026年末頃の施行予定（運用開始）。



セキュリティ対策評価制度の目的 →
- ✓ サプライチェーン全体でのセキュリティ水準の向上
- ✓ 企業のセキュリティ対策レベルの可視化

星 ＜★＞ 5段階による評価制度

星の取得が企業の「セキュリティ対策状況を示す」一つの指標に・・・

本制度は、企業のセキュリティ対策レベルを1から5までの星5段階で可視化し、取引先との間でセキュリティ対策状況を確認しやすくすることを目指しています。下表は各星の評価レベルと、求められる対策、評価方法を整理したものです。

＜星1・2について＞ ⭐⭐

IPA（独立行政法人情報処理推進機構）が運用している「SECURITY ACTION宣言」の枠組みを流用した、基本的な自己宣言のレベルです。

更新

	Security Action セキュリティ対策に取り組むことを自ら宣言		サプライチェーン対策評価制度 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		
	⭐	⭐⭐	⭐⭐⭐	⭐⭐⭐⭐	⭐⭐⭐⭐⭐
概要	情報セキュリティ5か条 取り組むことの宣言	自社診断＋基本方針 取り組むことの宣言 ※	**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	**発注者からみた 重要な企業**	未定 2026年以降に具体化予定
評価	自己責任	自己責任	専門家確認つき 自己評価	**第三者評価**	未定 2026年以降に具体化予定
項目	ー	ー	81項目	153項目	未定 2026年以降に具体化予定

※「5分でできる！情報セキュリティ自社診断（IPA）」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。

Section2

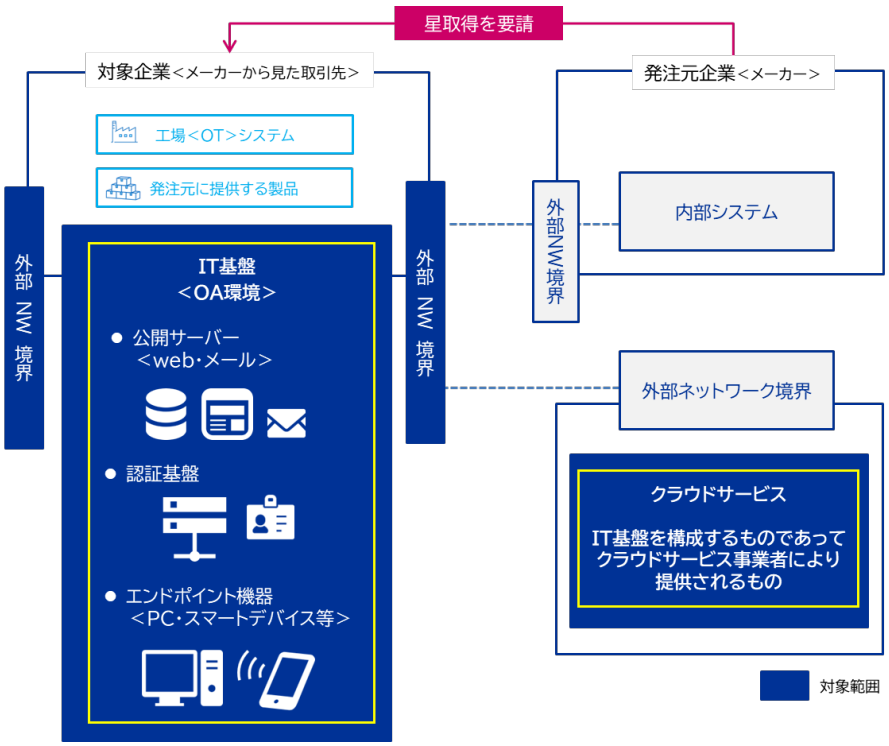
セキュリティ対策評価制度の全体像

対象となるセキュリティ対策範囲について

本制度の対象となるセキュリティ対策範囲は、**オンプレミス環境、クラウド環境にかかわらず、企業のIT基盤**が対象になります。

※ 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しています。

更新

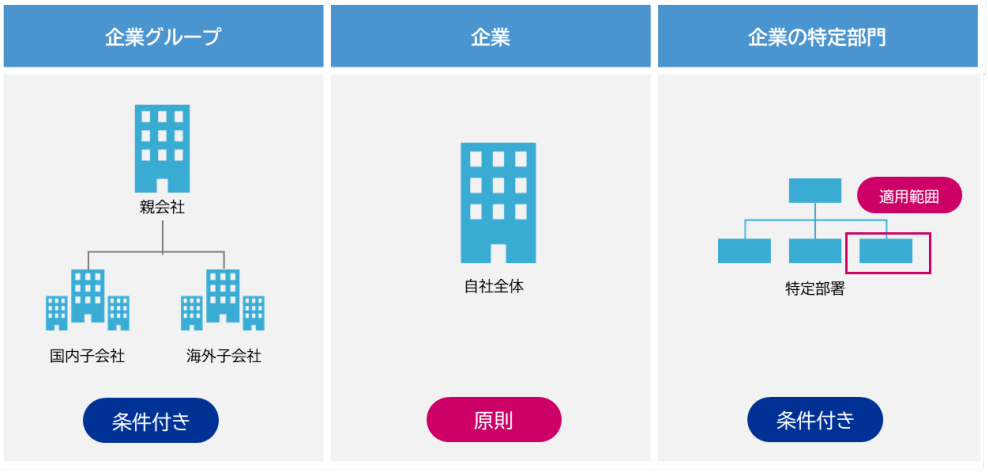


※取得範囲外のシステム等とは、ネットワーク機器等により、適用範囲との通信を必要最小限に制御する必要があります。

星を獲得する適用範囲

更新

取得範囲は「**原則：法人単位**」で設定します。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になります。



取得範囲外のシステム等とは、ネットワーク機器等により、適用範囲との通信を必要最小限に制御する必要があります。

Section2

セキュリティ対策評価制度の全体像

サプライチェーン関連企業が目指すべき目標　ー 制度の焦点は、星3・4 ー

制度の焦点は、星3と4のレベルです。

＜星3について＞★★★

「全てのサプライチェーン企業が最低限実装すべきセキュリティ対策」と位置づけられています。
ここでは、基礎的な組織的対策とシステム防御策を中心に実施し、一般的なサイバー攻撃への対処を念頭に置いています。

＜星4について＞★★★★

「サプライチェーン企業等が標準的に目指すべきセキュリティ対策」であり、**「供給停止等によりサプライチェーンに大きな影響をもたらす企業」**が対象になっています。
星4で求められるのは、単なる防御策ではなく、組織ガバナンス、取引先管理、システム防御・検知、インシデント対応など包括的な対策の実施であり、セキュリティ対策が組織的な仕組みに基づき、継続的に改善していることが要求されます。

＜星5について＞★★★★★

「到達点として目指すべきセキュリティ対策」と位置づけられていますが、まだ未定の項目も多く、今後明らかになっていくものと思われます。（2026年3月時点）

サプライチェーン対策評価制度
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

	★★★	★★★★	★★★★★
概要	**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	**発注者からみた** **重要な企業**	未定 2026年以降に具体化予定
評価	専門家確認つき 自己評価	**第三者評価**	未定 2026年以降に具体化予定
項目	81項目	153項目	未定 2026年以降に具体化予定

サプライチェーン関連企業が
取引拡大の優位性を得るために目指すべきレベル

更新

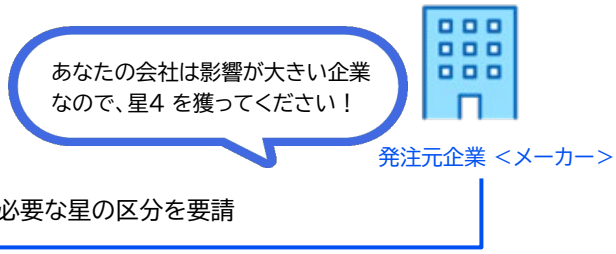
経済産業省の「セキュリティ対策評価制度」は、サプライチェーン全体での対応を前提としており、今後多くの企業でまずは「星3★★★」将来的には「星4★★★★」水準を見据えた対策が求められる可能性があります。

Section2

セキュリティ対策評価制度の全体像

獲得すべきはどっち？！　― 発注者目線から見た星3と4の違い ―

前述の通り「**全てのサプライチェーン企業が最低限実装すべきセキュリティ対策**」として、取得が求められるのは「**星3**」であり、さらなる競争優位性を目指すのであれば「**星4**」の取得が望ましいでしょう。
しかし実際のビジネスの現場においては **発注者側の企業が取引先に対して必要な星の区分を設定、要請** し、取引先企業が、それに応じる形になります。



取得すべき星の数は？ 発注者元企業 目線からの判断の観点

星3 ★★★	サプライチェーンに与する企業＜取引先＞が、最低限取得すべきレベル
星4 ★★★★	↓↓ 以下の観点から判断して、該当する企業＜取引先＞が求められるレベル↓↓

判断の観点

事業継続リスク	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 ＜考慮すべき観点の例＞ ● 製品・サービス供給の中断による自社への影響範囲が大きい ● 同業他社からの調達できない・困難である ● 在庫確保が難しい
情報管理リスク	取引先へのサイバー攻撃により、自社の機密情報に影響が出る恐れがある ＜考慮すべき観点の例＞ ● 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

ほぼ全ての取引先において、星3は最低限取得すべきレベルです。
「 止まる・漏れると発注者へ与える影響が大きい」取引先は、星4の取得が必要です。

Section2

セキュリティ対策評価制度の全体像

星取得に対する、経済産業省・構成取引委員会が整備すべき対応について

取引企業<受注側企業> の立場からすると、セキュリティ対策に必要なコストなど、相応の負担がかかることは否めません。
しかしながら今後、独占禁止法・取適法(旧下請法)の観点から**「問題にならない考え方」**を経済産業省・構成取引委員会が整理していく方針であり、対策にかかる費用は、正当な価格交渉が可能になる予定です。

取引企業<受注側企業> が感じがちな不安

- 対策を求められたが費用負担が重い
- 断ると取引が不利になりそう
- 価格交渉を切り出しにくい

具体的なアクション

発注元企業に「必要性などを確認」 → 様々な支援策を活用し、対策コストを抑える → 対策コストを整理し、価格交渉を実施 → 合意内容を双方で書面に残す

	発注元企業 <メーカー>	取引先企業
基本的な考え方	サイバーセキュリティは経営者の責務	取引継続・信頼確保のために対応
目的	サプライチェーン全体のセキュリティ強化 (一方的でなく**パートナーシップ重視**)	要請にこたえ、取引上の信頼を維持
実施すべきこと	評価制度に基づく**星取得を要請**	要請内容を理解し対応
具体的な行動	**方針策定、説明会の実施、支援策の共有**	様々な支援策を活用し、対策を実施
費用負担・価格交渉	対策費用は**価格交渉の対象**と周知	**対策コストについて価格交渉**
合意の扱い	合意内容を書面で保存	合意内容を書面で保存
備考	ー	価格交渉などで困ったときは、**取引かけこみ寺等へ相談**が可能

Section2

セキュリティ対策評価制度の全体像

星＜★＞3･4 で求められる評価基準

星＜★＞3･4で求められる **「要求事項」「評価基準」「参考文献」** を含む**正式版**が公表されました。

更新

大分類No.	大分類	中分類No.	中分類	要求事項No.	★3	★4	要求事項名	要求事項	★3/★4	評価基準No.	評価基準	NIST CSFにおける
1	ガバナンスの整備	1-1	組織の状況	1-1-1		○	社内ルール	セキュリティに関する法令等に規定された事項を考慮し、社内ルールを策定及び周知すること。	★4	1-1-1-1	・セキュリティに関連する以下の事項を把握した上で、社内ルールを定めること。 - 自社に関連する法令(事業法、個人情報保護法等) - 所管省庁及び関係団体における基準 - 取引先が提示する制限事項及び要求事項	統治(GV)
										1-1-1-2	・No.1-1-1-1で定める事項の改定及び変更の状況について、年１回以上の頻度で確認を行い、社内ルールの内容を点検すること。	
										1-1-1-3	・策定・見直した社内ルールを役員、従業員、派遣社員及び受入出向者へと周知すること。	
		1-2	役割、責任、権限	1-2-1	○	○	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	★3	1-2-1-1	・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。	
										1-2-1-2	・平時のセキュリティ推進活動に必要な役員(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連絡先リストを定めること。	
										1-2-1-3	・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。	
									★4	1-2-1-4	・セキュリティリスクは、経営に重大な影響を及ぼすことを前提として、その対応について、経営層が参加する情報セキュリティ委員会等の経営判断ができる体制を設置すること。	
				1-2-2		○	サイバー攻撃の監視・分析体制	サイバー攻撃及び予兆を監視・分析をする体制を整備すること。	★4	1-2-2-1	・サイバー攻撃及び脆弱性に関する公開情報又は非公開情報を活用する体制を整備すること。	
										1-2-2-2	・入手した情報又はログの相関分析等により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。	
				1-2-3	○	○	守秘義務のルール	守秘義務のルールを策定し、遵守させること。	★3	1-2-3-1	・役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。	
										1-2-3-2	・入社時又は社外要員の受入時に守秘義務のルールを説明すること。	
									★4	1-2-3-3	・自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。(社外要員を除く。)	
										1-2-3-4	・派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結すること。	
		1-3	ポリシー	1-3-1	○	○	セキュリティ対応方針の策定	自社のセキュリティ対応方針を策定し、周知すること。	★3	1-3-1-1	・自社のセキュリティ対応方針を定めること。	
										1-3-1-2	・定期的に役員、従業員、派遣社員及び受入出向者が最新のセキュリティ対応方針を参照できるようにすること。	
										1-3-1-3	・セキュリティ対応方針の改正時に、当該改正内容を役員、従業員、派遣社員及び受入出向者に周知すること。	
									★4	1-3-1-4	・年１回以上の頻度でセキュリティ対応方針の内容を点検すること。	
		1-4	監督	1-4-1		○	セキュリティ対策推進計画	セキュリティ対策推進計画を策定し、定期的に経営層へ対策実施状況に関する報告を行うとともに、報告結果を対策の推進に反映すること。	★4	1-4-1-1	・セキュリティ担当部署は、年１回以上、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)に対して、以下にて求める対策の点検の結果を踏まえたセキュリティ対策の実態及び当該実態を踏まえて策定した今後の対策推進計画を報告し承認を得た上で、当該報告結果を社内部署と共有すること。 [点検を求める対策(評価基準)] No.1-1-1-2、1-2-1-3、1-3-1-4、2-1-1-2、3-1-1-4、3-1-1-7、3-1-2-4、3-1-4-2、3-1-4-4、3-1-4-6、3-1-5-3、3-2-1-5、4-1-7-2、4-1-9-3、4-2-1-5、4-2-2-3、5-1-2-2、6-1-1-4	

経済産業省 HPより抜粋：https://www.meti.go.jp/press/2025/03/20260327001/20260327001-dr.xlsx

評価基準は、現場運用や実際のサイバー攻撃を踏まえた**実践的な内容**に見直されました

更新

1. 評価基準の整理･構造見直し

評価基準の内容が整理され、項目構成を見直し

★★★ 3：　83項目　→　**81項目**

★★★★ 4：157項目　→　**153項目**

※ 対策が減ったわけではなく、重複や表現の整理による見直しが行われました。

3. ガバナンス（経営関与）の強化

セキュリティをIT部門単独ではなく経営課題として位置づける

＜例＞

- セキュリティ体制へ経営層参加を明記
- 対策計画に統括役員の承認を要求
- サプライチェーン管理対象に子会社を追加

2. 現場で運用できる内容へ見直し

「書類対応」ではなく実際に運用できているかを重視

＜例＞

- パスワード運用など一部基準を整理･削除
- ルールの「周知」を明確に評価対象へ追加
- 廃棄時の表現を「消去」→「抹消」に変更

4. 技術要件の具体化 ＋ 柔軟な対応方法を明確化

実際のサイバー攻撃を踏まえ要件を具体化しつつ、達成方法は柔軟に選択可能と整理

＜例＞

- 境界機器の重大脆弱性対策を要求
- 多要素認証の対象範囲拡大
- 代替手段によるログ取得を許容

Section2

セキュリティ対策評価制度の全体像

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。

更新

星★★★

評価基準 81 項目

星★★★★

評価基準 153 項目

要求事項が多岐にわたる

統治
- ガバナンス整備
- 取引先管理

識別
- リスクの特定

防御
- 攻撃等の防御

検知
- 攻撃の検知

対応
- インシデントへの対応

復旧
- インシデントからの復旧

星<★>3・4 の評価方法

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。
評価機関による審査・技術検証があるため、「評価基準を正しく理解した対策」が必要です。

星★★★ 評価の主体は **専門家** です。獲得には、専門家による厳格な審査が必要です。

1. 適用範囲の決定
2. 自社で自己評価結果の記入
3. 専門家による審査
4. 不適合事項の対応
5. 専門家による内容確認
6. 経営層による自己適性宣誓
7. 事務局に提出／台帳登録

星★★★★ 評価の主体は **第三者評価機関** です。
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になります。

1. 適用範囲の決定
2. 自社で回答の準備
3. 第三者評価機関の審査の実施
4. 技術検証事業者の検証の実施
5. 不適合事項の対応
6. 第三者評価機関の内容確認
7. 事務局に提出／台帳登録・証書発行

Section2

セキュリティ対策評価制度の全体像

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るため、評価基準を正しく理解した対策が必要です

	★★★	★★★★		
	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・規定や操作画面等の確認による評価	攻撃パターンを試行

※ 書類準備や報告書作成は除く

＜補足＞ 実地審査・技術検証 ★★★★

更新

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**を実施する。

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。

※ 直近の脆弱性検査結果を提出することで、技術検証の代替と認められる場合があります。

Section2

セキュリティ対策評価制度の全体像

セキュリティ専門家の役割

セキュリティ専門家は公的資格保持と研修受講が求められます。
作業は作業従事者に委任可能ですが、最終確認は必ず専門家が実施する必要があります。

	役割	公的資格	研修の受講
セキュリティ専門家	● 作業全般を統括 ● 自分の責任において署名を行う	以下のいづれかの資格を保持／維持 ● 情報処理安全確保支援士 ● 公認情報セキュリティ監査人 ● CISSP ● CISM ● CISA ● ISO27001 主任審査員	必須
作業従事者	● 作業確認者 ※ セキュリティ専門家の監督下で実施	不要	必須

セキュリティ対策評価制度は更新制です

セキュリティ対策評価制度は更新制です。 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

	★★★	★★★★
有効期間	1年	3年
手続き方法	自己評価（セキュリティ専門の確認・助言）	毎年、自己評価／3年に1回は評価機関による審査
合格基準	原則として、すべての評価基準への適合が必要	
注意点	虚偽の報告や情報隠蔽などが確認された場合、**獲得した星が一時停止又は取り消される場合があります。**	

＜ ★★★★ の特記事項＞

- 星4の有効期間は3年間ですが、その期間中であっても、前回取得時から対象範囲の変更や評価結果に大きく影響する変更があった場合は、改めて評価機関の審査が必要です。

  ＜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やサーバ等の大規模リプレイス、クラウドシフトなど

- 規定・手順書等における誤字脱字・体裁の修正や。要求事項・評価基準の達成に大きな影響のない軽微な設定・運用上の変更は除きます。

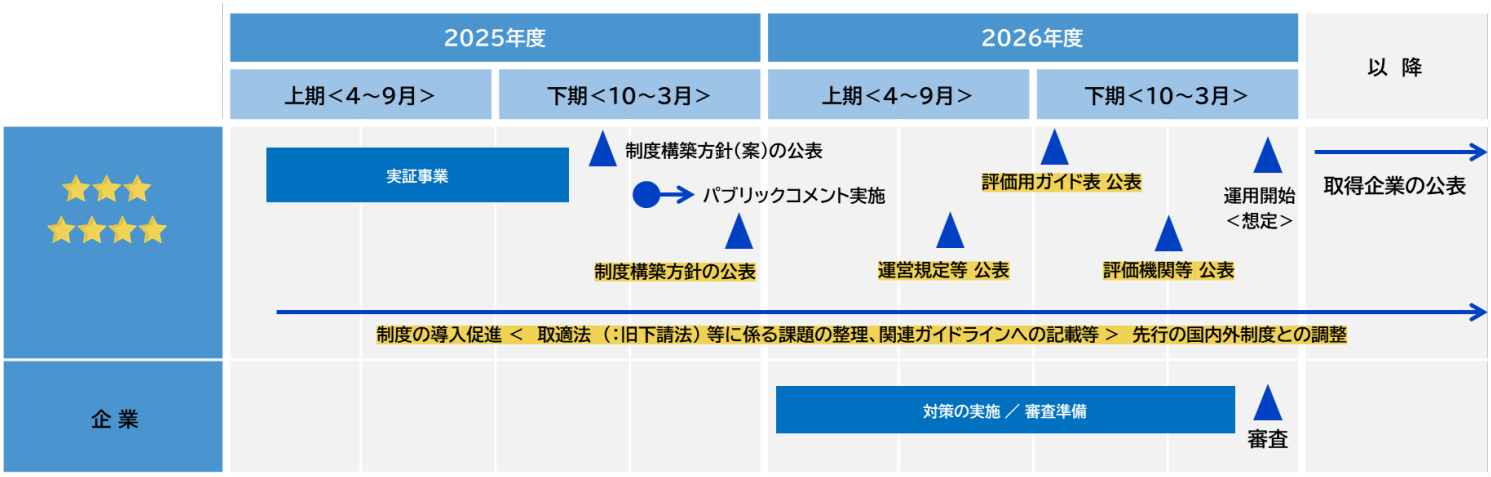
Section2

セキュリティ対策評価制度の全体像

運用開始までのスケジュール

更新

星3・4を目指す企業のための スケジュールは下表の通りです。
制度開始は、当初の予定通り2026年度末の予定です。 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。
先行して進めることが、競争優位性を確保し、ビジネスチャンスを広げる鍵となります。この準備期間にぜひ対策をご検討ください。



セキュリティ対策評価制度 最新情報のまとめ

新規追加

- サプライチェーンに**関与する企業が対象**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。
- 独占禁止法・取適法の観点から「問題にならない進め方」が公表され、**取引先へのセキュリティ対策要請は今後広がる可能性があります**。
  また、受注者は対策コストを踏まえ、**提供価格の見直しを交渉できる枠組み**が示されています。
- 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。
- 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。
- 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。

Section2

セキュリティ対策評価制度の全体像

＜補足＞

過去の事例に学ぶ ：Pマーク ＜プライバシーマーク＞

Pマークのような、過去の事例が示すように、制度が始まってから対策を始めても、**「取得が当たり前ゾーン」**に入ってしまい、競争優位性が失われてしまう可能性が否めません。

星の取得を目指す企業の方は、このスケジュールをチャンスと捉えて早めの準備をおすすめします。先行して進めることが、競争優位性を確保し、ビジネスチャンスを広げる鍵となります。

過去の事例：Pマーク ＜プライバシーマーク＞

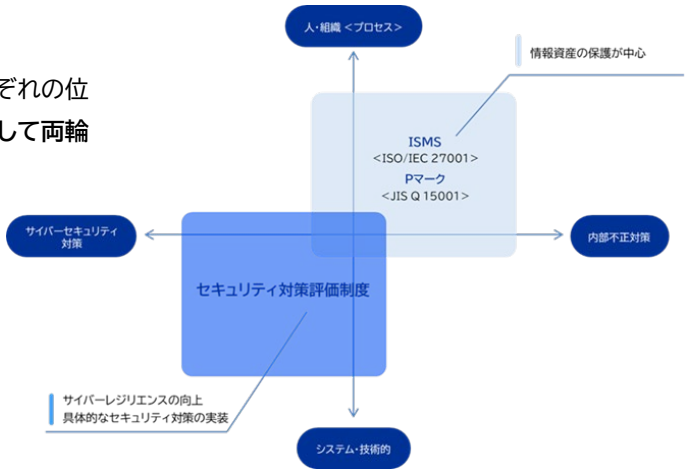
過去のPマークの事例が示すように、競合他社が追随する前に、先行対応をすることによって、貴社を「取引先から選ばれる存在」へと導きます。

- 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。**

星の獲得はビジネスチャンスの拡大につながります
「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！

各制度の関係性について

「① ISMS」「② Pマーク」と「③ セキュリティ対策評価制度」 それぞれの位置付けとして、①②③ 全ての取得が求められ、**相互補完的な制度として両輪で発展**する予定です。



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。

ndis
NDIソリューションズ株式会社

Section 3

星＜★＞の獲得を実現するための実践的な手段のご提案

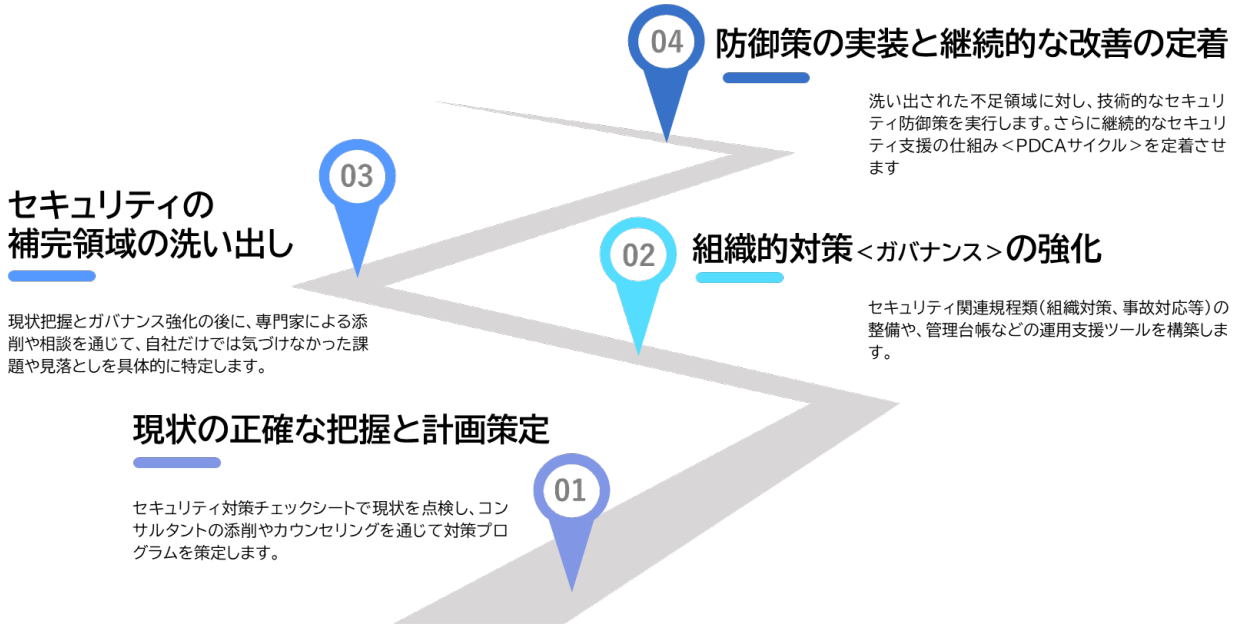
Section3

星＜★＞の獲得を実現するための実践的な手段のご提案

本セクションでは、星獲得に向けて最短でつなげるための実践的な進め方に焦点を当てます。
必要なステップをどのように効率的かつ効果的に進めていくか、具体的な手段をご紹介します。

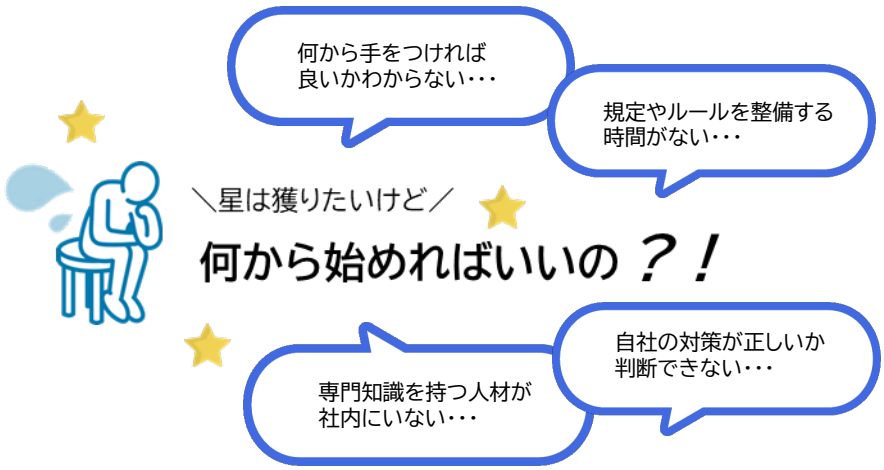
星 ＜★＞取得までに必要な4つの準備プロセス

3－4の獲得を照準にした場合、必要な準備のプロセスは以下の4つです。
これらのステップをどのように効率的かつ効果的に進めていくのかが、勝敗を握るカギになります。



多くの企業が直面する“最初の一歩の壁”

セキュリティ対策評価制度の重要性や、星を獲得することによって得られる「競争優位性」も理解できたけど、何から準備をはじめて良いのかわからない、、という方も多いのではないでしょうか。
星獲得へ向けた具体的な準備のプロセスは、ひとつではなく、様々な方法があります。 この資料ではNDIソリューションズからの提案として 、次頁より**「ガイドライン対応サポートアカデミー」**をご紹介しています。進め方のひとつのご参考として、読み進めてください。



これらの課題を解決するのが
体系化された**「伴走型アプローチ」**です。

Section3

星＜★＞の獲得を実現するための実践的な手段のご提案

プロの目線で星の獲得を伴走支援「ガイドライン対応サポートアカデミー」とは

経済産業省「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」への対策支援

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

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。
本サービスにより、自社の現状を“ 正しく把握 ”していただき、プロの目線で星の獲得を伴走支援いたします。

サポートアカデミー の 3つのポイント

コンサルタントが プロ目線 で 対策の改善点を抽出

セキュリティ対策状況の振り返りができるチェックシート ※1 を コンサルタントが添削するサービスをご提供。対策漏れや改善のポイントをプロの目線でチェックすることで、自社だけでは気づかなかった課題まで可視化できます。

解説動画 と 個別相談 で、具体的な対策実行をサポート

対策の基礎から実践まで、分かりやすい解説動画をいつでも何度でも視聴可能。メール・Web会議での個別相談 ※2 や、対策の優先順位のアドバイスに加えて、セキュリティ関連規程のひな形などお役立ちコンテンツもご提供。具体的な対策実行までサポートします。

最初のご購入の後も 年間更新で 継続的 にサポート

最初のご購入（利用期間：9カ月）の期間満了後は、1年単位での更新が可能。継続しやすい価格設定で、セキュリティ対策の定期的な見直し・改善も伴走支援。新たな脅威や要求されるセキュリティ対策の変化への対応までサポートします。

※1 ご購入のパッケージにより、対象となるチェックシートが異なります。
※2 Web会議での個別相談は回数制限があります。

Section3

星＜★＞の獲得を実現するための実践的な手段のご提案

サポートアカデミーと、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 サイバーセキュリティ対策
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お問い合わせください。
※3 総合的なセキュリティ対策をNDIソリューションズ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チェックシートのご提供。更にコンサルタントによる第三者目線でアドバイスもご提供。
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。

Section3

星＜★＞の獲得を実現するための実践的な手段のご提案

星＜★＞獲得までのステップをサポートアカデミーで伴走支援いたします。

Step1	Step2	Step3	Step4	Step5	Step6
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

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

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＜★＞3･4 の取得を目指す方向けの サポートアカデミー ＼ 2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2つの支援コースをご用意しています。

実践コース ＜ライト＞ ★★★	セキュリティ対策評価制度 星3 を取得するための支援コース
実践コース ＜ベーシック＞ ★★★ ★★★★	セキュリティ対策評価制度 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

実践コース ＜ライト＞

狙いを「星3」に絞って、取得するためのご支援

★★★

新規購入
利用期間： 9ヶ月
定価：￥300,000＜税抜＞

上記終了後 継続更新
利用期間：12ヶ月
定価：￥120,000＜税抜＞

実践コース ＜ベーシック＞

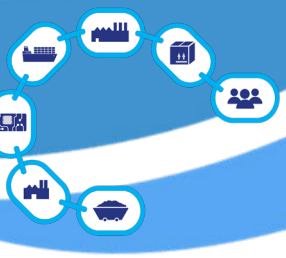
「星3」はもちろん、「星4」水準を含む
総合的なサイバーセキュリティ対策をご支援

★★★
★★★★

新規購入
利用期間： 9ヶ月
定価：￥450,000＜税抜＞

上記終了後 継続更新
利用期間：12ヶ月
定価：￥120,000＜税抜＞

※ 上記2コース以外に、現状把握だけを実施したい方向けの「学習コース」もございます。



Section3

星＜★＞の獲得を実現するための実践的な手段のご提案

各ご支援内容の概要

●● ライトコース ●● ベーシックコース

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

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

チェックシート添削
記入したチェックシートにセキュリティコンサルタントがアドバイス

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

個別相談＜メール＞
メールによる個別相談をご提供

個別相談＜web会議＞
オンラインによる個別相談をご提供

よろづ相談会
テーマに沿った相談会を開催

対策講座
対策実施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

教育コンテンツ
従業員教育で活用できる説明資料と理解度確認テストをご提供

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

お役立ち情報配信
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

「サポートアカデミー」のご提供コンテンツ

サポートアカデミーでは　各種規程のひな型・教育コンテンツや管理台帳・申請書のフォーマット　など、組織的対策に役立つコンテンツを多数ご提供します。

各種規程ひな型	教育コンテンツ	各種運用支援ツール
1.情報セキュリティ方針案 2.組織対策 3.人的対策 4.情報資産保護 5.物理環境保護 6.IT機器管理 7.システム管理 8.システム管理（アクセス制御及び認証） 9.外部委託先管理 10.セキュリティ事故対応 11.インシデント対応手順	**＜1. 従業員向け＞** ● 【基礎1】 情報セキュリティ対策方針 ● 【基礎2】 業務で利用する情報機器の利用ルール ● 【基礎3】 情報セキュリティ事件・事故の予防と発生時の対応 ● 【基礎4】 重要情報の漏えいを防止するためのルール ● 【基礎5】 その他の情報セキュリティ関連ルール ● 理解度チェックテスト **＜2.管理者向け＞** ● 【管理者向け教育資料】 部門管理者の役割と責任 **＜3.経営層向け＞** ● 【経営者向け教育資料】 経営者の役割と責任	1.誓約書（守秘事項）の文章案） 2.機密保持契約書の文章案 3.退職/期間満了時の回収物一覧チェックシート 4.インシデント管理台帳 5.ID/アクセス権管理台帳 6.共有ID利用台帳 7.アクセス権管理ルール遵守状況チェックリスト 8.情報資産管理台帳 9.機密区分運用ルール遵守状況チェックリスト 10.取り交わし情報一覧表 11.外部情報システム管理台帳 12.ヒヤリハットテンプレート 13.入退室管理台帳 14.持込物管理台帳 15.FWフィルタリング設定台帳 16.管理者権限管理台帳 17.サーバ・NW機器設定変更作業申請書

Section3

星＜★＞の獲得を実現するための実践的な手段のご提案

「ガイドライン対応サポートアカデミー」導入後の壁

サポートアカデミーを導入して、「星＜★＞取得に向けてやるべきこと」や「規定集・チェックシート」等の必要資料は入手できたけど、自社だけでは突破できない「実務の壁」を感じてしまう、、。 そんな企業様に向けた伴走支援サービスのご紹介です。

サポートアカデミー導入後に直面する “3つの壁”

チェックシート記入や規程（ポリシー）策定の実務を自社だけで進めるのはリソースや知識の面で厳しい・・・

- **時間の壁**：通常業務が忙しく、81/153項目のチェック項目を確認する時間が取れない。
- **判断の壁**：「達成基準」を自社が満たしているか、プロの目がないと判断しきれない。
- **策定の壁**：ひな形（テンプレート）はあるが、自社の実態に合わせた「規程」に落とし込む作業が難しい

「星取得へのステップはわかった。でも、実務を動かすリソースが足りない」

—— そんな企業の皆様をndisが直接サポートします。

ndis 伴走支援サービス①　GAP診断支援サービス

最短でGAPを可視化する**「GAP診断支援サービス」**※

チェックシート記入のフェーズでつまずいている企業様向けの、短期集中支援です。

サービス概要　ndisの専門家がチェックシート記入に伴走し、最短2か月で現状を整理。

支援内容　全4回（1回2時間）のヒアリング形式で実施。「できていること」「できていないこと」をプロの視点で最短で切り分け。

得られる効果
- 専門家の確認を経た、精度の高い「対策プログラム」の早期確定。
- チェックシートの完成。

サービス詳細情報

価　格	実施期間	実施頻度	対象企業
￥150,000 ＜税抜＞	約2ヶ月	1回2時間×全4回	企業規模問わず

※ NDIソリューションズ経由でサポートアカデミーを導入済のユーザー様に提供させていただくサービスです。

ndis 伴走支援サービス②　規定策定支援サービス

規定整備を伴走支援**「規定策定支援サービス」**※

こんなお悩みをお持ちの方に、ご検討いただきたいサービスです。

ひな型から自社への落とし込みで苦労している→	ひな形資料があっても、具体的な着手点が不明確
時間・人材が不足している→	自社でセキュリティ規程を策定するリソースが不足
サポートアカデミー＋αをご希望→	メール等のサポート支援をもっと充実させたい
セキュリティ対策評価制度の星＜★＞取得を目指している→	要求事項がまだ把握できていない

サービス概要

サポートアカデミーの各種規定ひな形資料を活用し、NDIソリューションズの専門家が情報セキュリティポリシーの策定から継続的な更新まで一貫して伴走支援します。

支援内容

基本方針の策定	資産保護	システム管理	組織・人的対策	差分整理
情報セキュリティ 基本方針の策定・更新	資産保護に関する 社内規定	システム管理に関する 社内規定	組織・人的対策に関する 社内規定	既存規定との 差分管理

作成資料

セキュリティ対策評価制度に対する事項を対象とします。

- 情報セキュリティ基本方針
- 社内規程(組織・人的対策
- 社内規程(資産保護/システム)
- 差分整理レポート

導入のメリット

業務不可の軽減： 自社リソースでの対応と比較して、セキュリティ対策評価制度の星＜★＞取得に向けたガイドライン対応・資産管理の負荷を大幅に軽減します。

専門家による安心感： 専門家が担当することで品質・網羅性・法令準拠に対する高い安心感を提供します 。

サービス詳細情報

	価　格	作業時間	作業頻度
初回策定支援	￥2,080,000＜税抜＞	合計150時間まで	年50時間まで
次年度以降 ＜更新支援＞	￥660,000＜税抜＞/年	初回のみ	年1回 ＜法改正・システム変更時に随時見直し＞

※ NDIソリューションズ経由でサポートアカデミーを導入済のユーザー様に提供させていただくサービスです。

ndis
NDIソリューションズ株式会社

Section 4

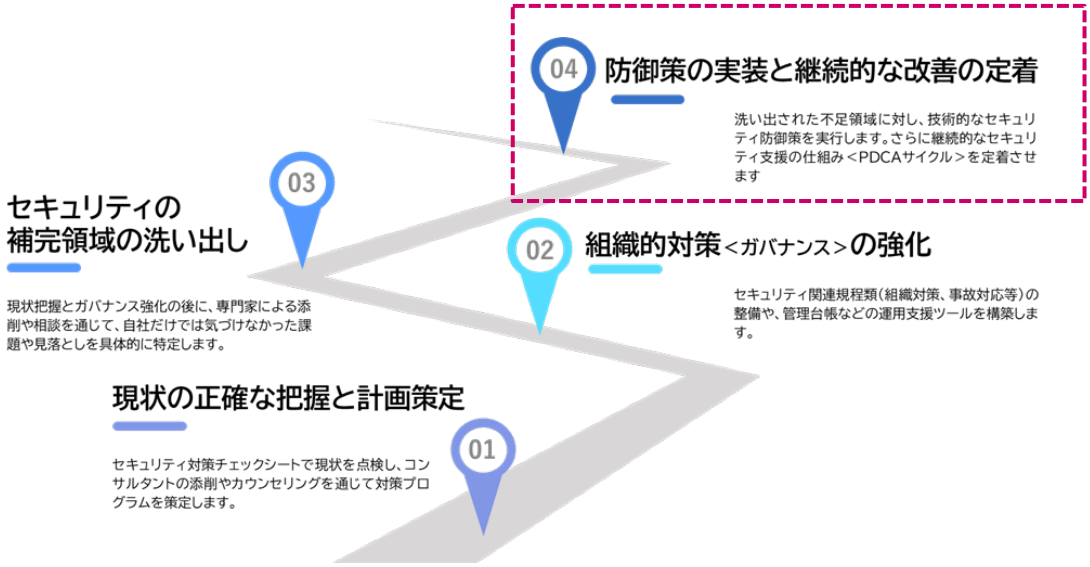
星＜★＞獲得のために必要なセキュリティ不足領域の適合製品選定とご支援策

Section4

星＜★＞獲得のために必要なセキュリティ不足領域の適合製品選定とご支援策

可視化されたセキュリティ補完領域のご支援について

例えば、＜Section2＞でご紹介のサポートアカデミー等のサービスを活用して、貴社が星獲得のために必要な「セキュリティの不足領域」が明らかになった後、セキュリティを担保するための適合製品の導入（不足項目の充足）が必要です。本Sectionでは、NDIソリューションズの考えるご支援策をご紹介いたします。



セキュリティ環境整備において、多くの企業に共通する課題

リスクの特定
- 資産/脆弱性の棚卸が不十分
- 社内システム構成の把握が曖昧
- 古いソフトウェアの使用継続

攻撃等の検知
- EDRやログ活用、24/365監視が不足
- 監視の盲点や対応体制の不備
- インシデント検知の遅れ

攻撃等の防御
- 対策が部分最適、設定/運用にばらつき
- バックアップ対策の不備
- アクセス制御の管理不足

当社が補完すべき
セキュリティ領域は理解したけど・・・

- 何から着手すべき？！
- 製品・サービスの選定は？！
- 限られた予算で最大の効果を得るには？！

これらの疑問をNDIソリューションズが
お客様の環境にあわせた伴走型で支援いたします。

Section4

星＜★＞獲得のために必要なセキュリティ不足領域の適合製品選定とご支援策

NDIソリューションズのご支援策

お客様毎の環境に合わせた 計画的な星取得を
伴走型 でサポートします。

サポアカチェックシート

チェック結果から優先順位付けを行いロードマップ策定

- チェックシートの結果確認
- お客様毎のロードマップ策定

課題の顕在化

複数ソリューションの比較

優先度の高い項目について複数製品の比較検討

- 製品比較資料
- 費用比較
- 製品説明、見積

ソリューション検討

ndis 導入サポート

情報インフラ全体を、人的・技術的・物理的な側面から包括的にご支援します。設計から構築、運用まで、一貫した体制で対応いたします。また、一部作業をお客様にて実施される場合など、ご要望に応じて柔軟な構築プランをご提案し、セキュリティ環境の整備をサポートいたします。

構築・運用

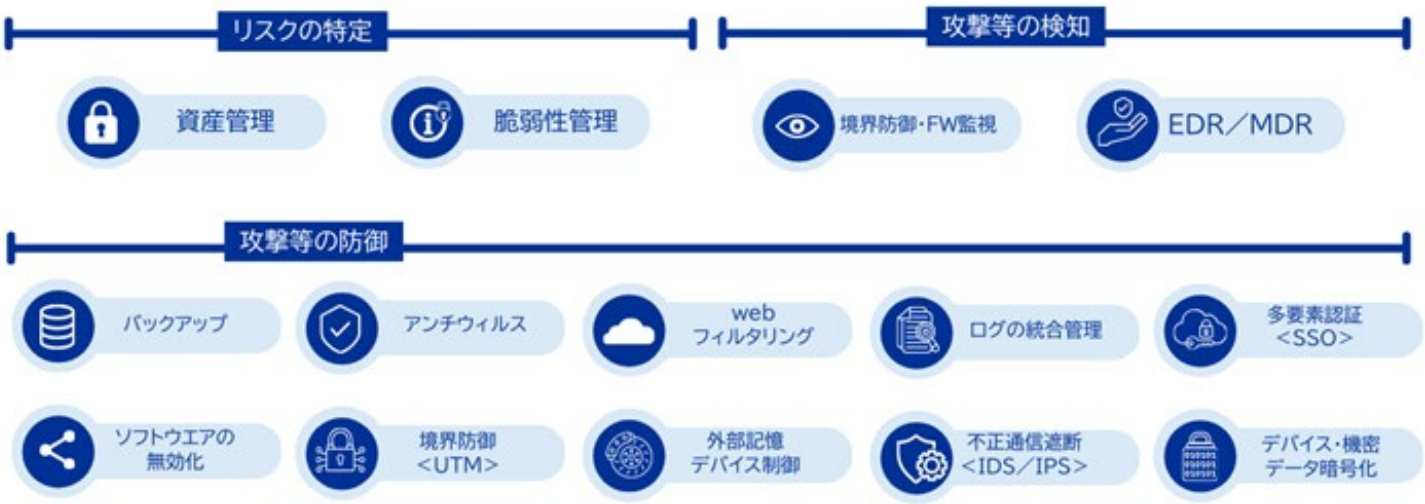
継続的なご支援

セキュリティは一過性の対応では不十分。脅威は日々変化するため、継続的な監視と改善が企業防衛の要となります。NDISが定期的なフォローアップを行い、最新の対策を継続的に提案します。

継 続

星＜★＞4認定に求められる技術的対策

以下のセキュリティ技術カテゴリの中から、貴社の補完すべき技術的対策、および具体的なソリューションを選択の上、NDIソリューションズがご支援をさせていただきます。



ndis
NDIソリューションズ株式会社

おわりに

セキュリティ対策評価制度は、**義務** ではなく
未来のビジネスを強くするチャンス です。

この制度は、貴社のセキュリティ体制を見直し、より強固なものへと高める絶好の機会でもあります。
本制度を通じて、取引先からの信頼向上はもちろん、新たなビジネスチャンスの創出や、事業の拡大・発展につながることを心より願っております。
NDIソリューションズの取り組みが、その一助となれば幸いです。

ndis 変化の一歩先を。 NDI SOLUTIONS LTD.

2026年6月吉日

お問い合わせ

本資料に関するご質問やお問い合わせは、下記までご連絡をお願いいたします。

NDIソリューションズ 株式会社
ndis マーケティング事務局
ndi.marketing@ndisol.com
Web: https://www.ndisolutions.co.jp

付録

経済産業省 更新・追加情報一覧

公開日：2026/3/27

経済産業省 「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」

https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

付 録

経済産業省 更新・追加情報一覧

2026年3月27日公開情報

経済産業省 「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」

更 新

https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

Point 1 制度の範囲・位置づけ

- 取得は「原則：法人単位」と整理 （条件付きで事業部・グループも可）
- 評価対象範囲の考え方が実務に合わせて現実的に整理

Point 2 スケジュール

- 2026年度末の制度開始予定は変更なし
- 制度ルール・評価ガイド等の公開時期が具体化

Point 3 要求事項・評価基準

- 評価基準が整理され、実務に合わせた内容へ見直し
- 「書類対応」ではなく「実際に運用できているか」を重視する内容へ変更

Point 4 FAQ公開

- セキュリティ対策評価制度の制度構築方針に対して、よく寄せられる質問への公式回答を公開

詳 細

制度構築方針（案）で明確になった4つのポイント

Point 1 制度の範囲・位置づけ

- **取得単位は「原則：法人単位」に整理**

  これまで「グループ・企業・部門など柔軟」とされていたが、最新では 企業（法人）単位が基本 と明確化された。
  例外として、専門家または評価機関が妥当と判断した場合のみ事業部単位・グループ単位での取得が可能。

- **評価対象範囲の考え方が実務に合わせて現実的に整理**

  適用範囲に含めないシステムがある場合は、**範囲内外の通信を必要最小限に制御する**ことが求められることが明確化。
  （＝**完全分離ではなく、通信を必要最小限に制御する**へ整理）

Point 2 スケジュール

- **制度開始時期は変更なし**

  2026年度末（1月～3月頃）運用開始予定。

- **今後の公開スケジュールが具体化**

  運営規程等：2026年度上期（7～9月頃）/ 評価ガイド等：2026年度下期初（10月頃） / 評価機関公表：2026年度末直前

Point 3　要求事項・評価基準

- **評価基準の整理（項目数の見直し）**
  評価基準の内容が整理され、項目数が一部変更
  星＜★＞3：　83項目 → 81項目
  星＜★＞4：157項目 → 153項目
  ※対策が減ったわけではなく、重複や表現の整理による見直し

- **実務に合わせた評価内容へ修正**
  現場で運用できることを重視した内容に変更
  ＜例＞
  - ✓ パスワード運用など一部基準を整理・削除
  - ✓ ルールの「周知」を明確に評価対象へ追加
  - ✓ 廃棄時の表現を「消去」→「抹消」に変更（実務寄りに整理）

- **ガバナンス（経営関与）の強化**
  セキュリティをIT部門だけでなく経営課題として位置づけ
  ＜主な例＞
  - ✓ 情報セキュリティ体制に経営層の参加を明記
  - ✓ 対策計画は統括役員の承認が必要に変更
  - ✓ サプライチェーン管理対象に「子会社」が追加

- **技術対策の具体化・強化**
  実際のサイバー攻撃を踏まえた要件が追加・明確化
  ＜例＞
  - ✓ インターネット境界機器に重大な脆弱性がないことを要求
  - ✓ インターネット経由接続時の多要素認証の対象範囲を拡大
  - ✓ 管理者IDも含めた認証管理を明確化

- **「方法は固定しない」考え方を明確化**
  同じ目的を達成できれば、対応方法は柔軟に選択可能
  ＜例＞
  - ✓ デフォルトID停止　→ または強固な認証でも可
  - ✓ 未許可ソフト削除　→ または禁止設定でも可
  - ✓ 必要ログが取得できない場合　→ 代替手段での取得を許容

Point 4　FAQ公開

- **セキュリティ対策制度の制度構築方針に対してよく寄せられる質問への公式回答（FAQ）が公開**

＜例＞

Q 星の取得は公共事業の入札要件になりますか？
A 今後、政府機関や重要インフラ事業者等の調達での活用を検討

Q セキュリティ対策評価制度は、どのような業種や企業規模に適用されるのですか？
A 業種・企業規模を問わず、幅広い事業者が対象

Q 星は必ず取得しなければならないのですか？
A 制度上の取得義務はなく、取引上の判断材料として活用される想定

※ その他FAQは公式資料参照

2026年6月版

※ 2026年3月27日 経産省公開の更新情報を反映しています

本資料に関するご質問・ご相談は下記よりお問い合わせください

NDIソリューションズ 株式会社

ndis マーケティング事務局

ndi.marketing@ndisol.com

Web: https://www.ndisolutions.co.jp