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1月版

※ 2025年12月26日 経産省公開の更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、2025年12月26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（案）」** の内容を反映しています。
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.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構築に向けた中間取りまとめ」を公表しました（2025/4/14）
制度の最新情報は経済産業省のサイトにて順次公開されます。

https://www.meti.go.jp/press/2025/04/20250414002/20250414002.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 2025』では、『サプライチェーンや委託先を狙った攻撃』が2位に3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2025
サプライチェーンや委託先を狙った攻撃が
3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2025
※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･･･

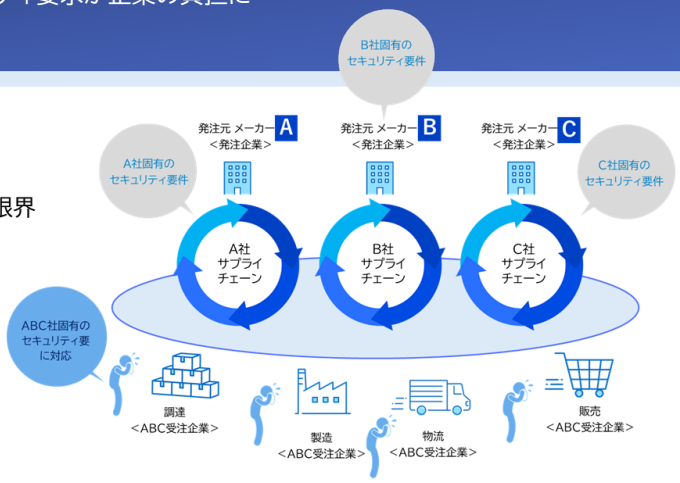
発注企業からは『取引先のセキュリティをきちんと担保せよ』という指示があり、一方、受注企業から見れば『取引先ごとにバラバラな要求で対応が限界』という状況です。
結果として、対策の重複や非効率が生まれ、サプライチェーン全体でのセキュリティ対策の底上げが進みにくいという課題が浮き彫りになっています。

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

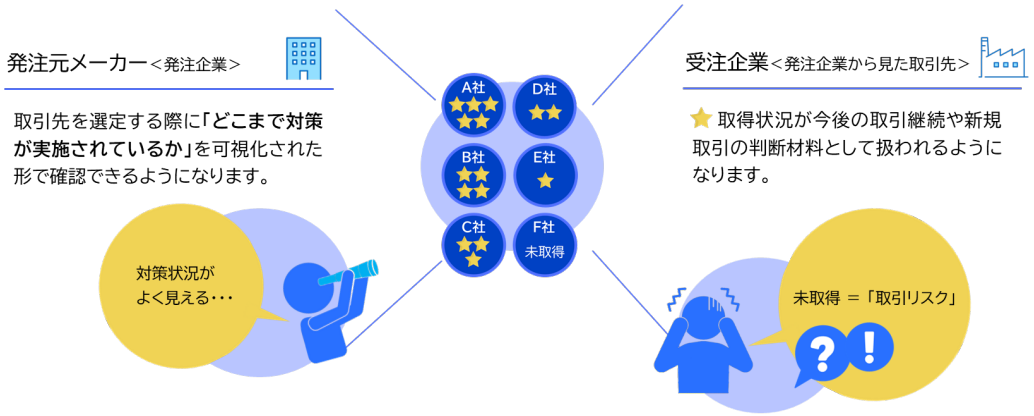
- 国が定めた基準に基づく対策の実施により
  取引先に対して **セキュリティ対策を正面から説明できる。**
- 取引先ごとに異なる対策要求への対策負担が軽減され
  標準的な対策レベルの維持が可能。

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

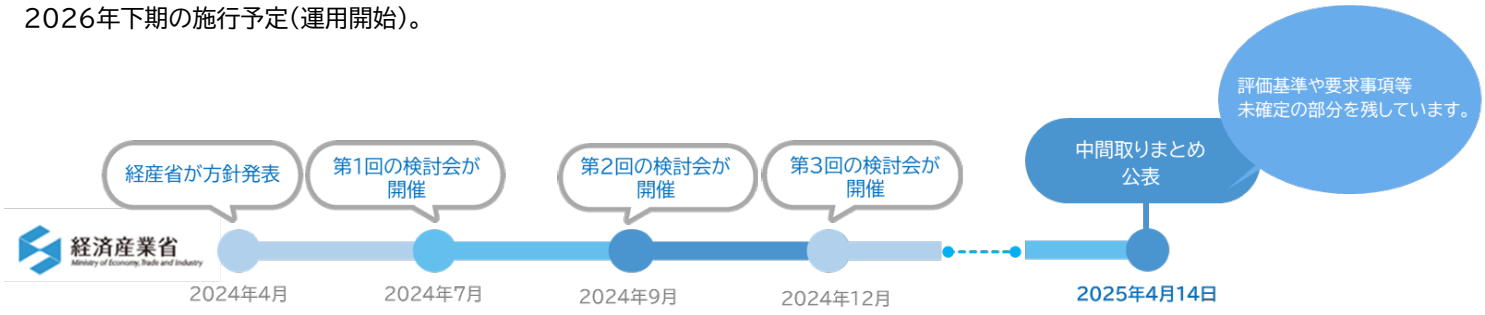
自社のセキュリティ体制が強化されるため
サイバー攻撃や情報漏えいのリスクが自然に低減する。

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年下期の施行予定（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、2025年12月26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（案）」**　の内容を反映しています。
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.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

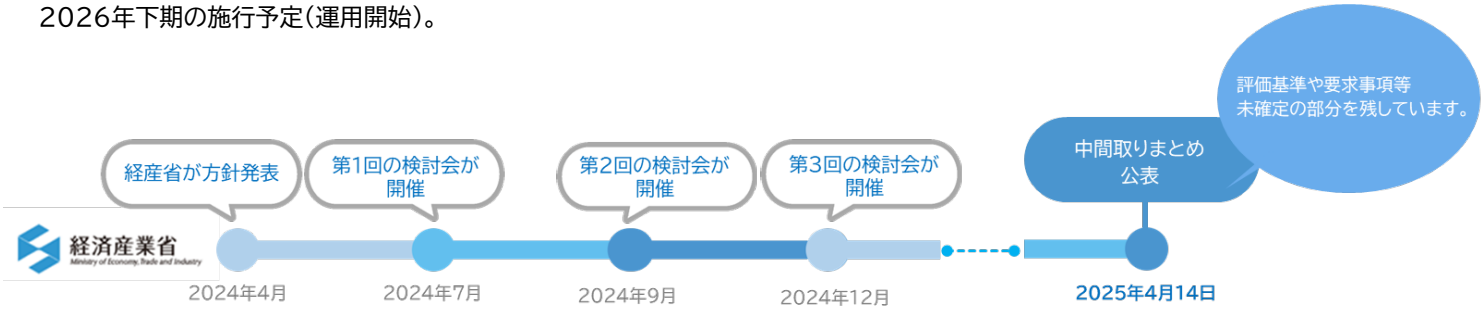
Section2

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年下期の施行予定（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段階評価による格付け

星の取得状況によって「信頼できる企業か否か」の選定基準に・・・

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、企業の信頼度を星の数で区別できるようにな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。

	⭐	⭐⭐	⭐⭐⭐	⭐⭐⭐⭐	⭐⭐⭐⭐⭐
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	―	―	**83項目**	**157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。

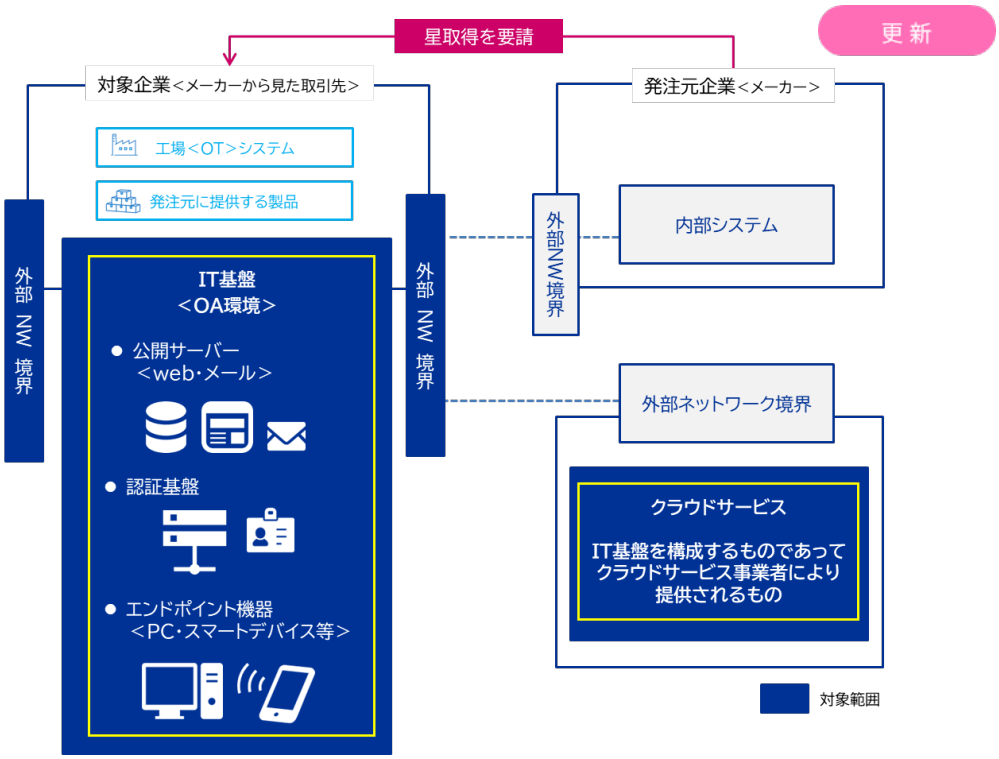
Section2

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、本制度の対象外となります。



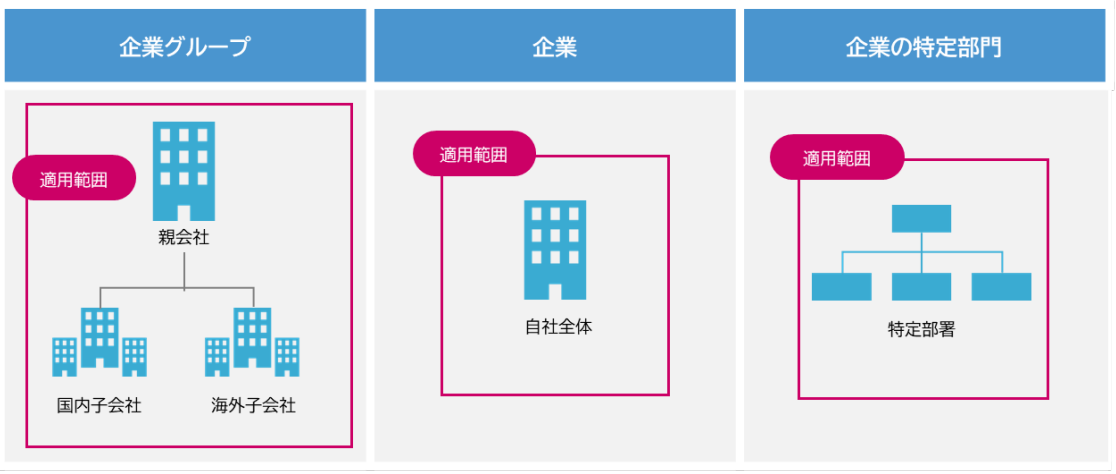
※要求事項を満たすことが困難なIT機器やソフトウェアは例外的に適用範囲に含めないことが許容されます。
その場合は、セキュリティ専門家又は評価機関による妥当性評価が必要です。

星を獲得する適用範囲

新規追加

星を獲得する範囲は柔軟に定めることが可能です。

範囲外については、取得範囲外の会社・拠点との間の通信をネットワーク機器等により必要最小限にする等、ネットワークの分離が必要です。



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＞

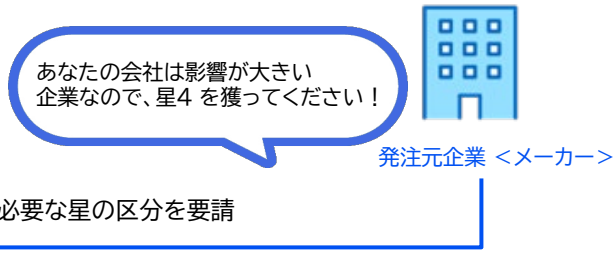
「到達点として目指すべきセキュリティ対策」と位置づけられていますが、まだ未定の項目も多く、今後明らかになっていくものと思われます。（2025年11月時点）

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

更新

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・サービス供給の中段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＞ ● 自社の重要な機密情報の取扱っている・アクセスできる ● 取引先から自社のシステム、ネットワークへのアクセスできる ※アクセス可能な自社システム・ネットワークの範囲を考慮

サプライチェーンを構成する多くの企業において、星4の検討が重要です。
「 止まる・漏れると取引先に影響する」可能性のある企業は、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

新規追加

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

星＜★＞3・4 で求められる評価基準

評価基準は、現実の脅威と運用実態を踏まえ、実効性を重視する考え方に見直されています

新規追加

1. 全体構造の整理

2025年4月公開の要件案をもとに、
NIST CSFを軸に再整理
大分類：変更なし中分類：表現の微調整
のみ（考え方は継続）

3. 評価基準項目数の増加

44項目 → **157**項目

※ 評価基準ごとに項目が細分化。
実質的に求められる対策内容が増えたわけではない

2. 評価基準の見直し（追加・削除）

＜追加項目（約9項目）＞
- リモートワークにおけるルール（★4）
- メールによるマルウェア感染防止対策（★4）など

＜削除項目（約9項目）＞
- 退職者による機密情報の持ち出し対策
- 管理者権限を持つ共有アカウントのアクセスログ取得など

4. 評価の考え方の変化

「文書化する」「一覧を作成する」などの記載が
「仕組みを整備すること」に変更

→目 的が達成されていれば、手段は柔軟に評価！？

評価基準表 一覧

更 新

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	23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。

次頁に続く

Section2

セキュリティ対策評価制度の全体像

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
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	85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・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	9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	7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。
			157項目	

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。

更新

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　新規追加

	★★★	★★★★		
	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 ★★★★

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**　※。

例

- 対象IPアドレスに対してポートスキャン
- CVSS 7.0以上の脆弱性の有無
- 認証強度

※直近における対象機器への脆弱性検査の実施結果でも問題ありません。
※実地審査及び技術検証の詳細な内容は2026年度に公開予定新規追加。

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。

新規追加

	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
  ＜例＞ PCやサーバ等の大規模リプレイス、クラウドシフト）など

- 変更が軽微な場合は、評価結果に影響がないことを示す自己適合宣誓書の提出で対応可能です。

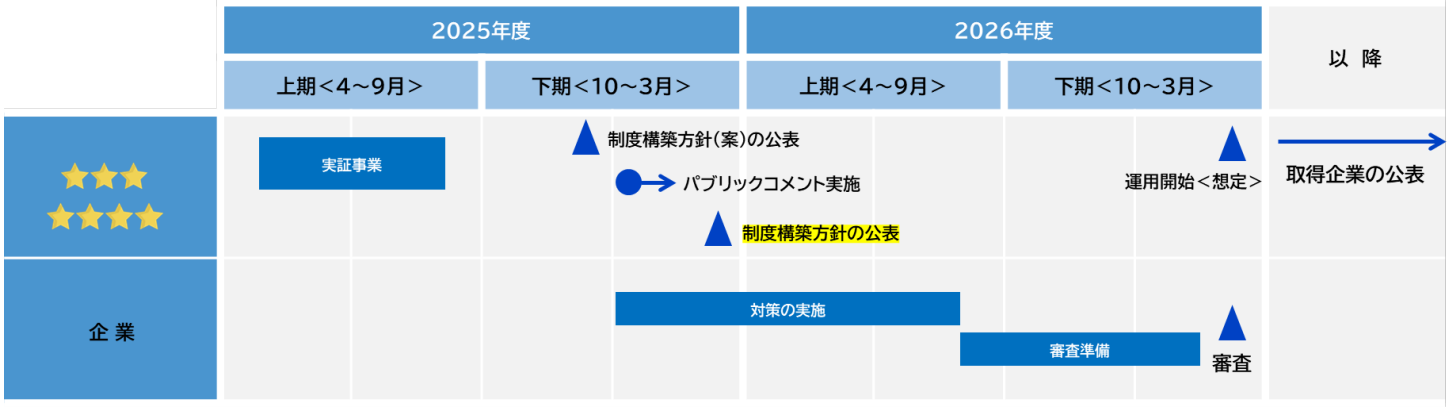
Section2

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

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。
2026年度上期には、評価基準や要求事項が確定する予定であり、現時点では大まかなスケジュールしか把握できません。
しかしながら、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。この準備期間を無駄にせず、対策をご検討ください。

更 新



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。

運用開始までのスケジュール

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。**

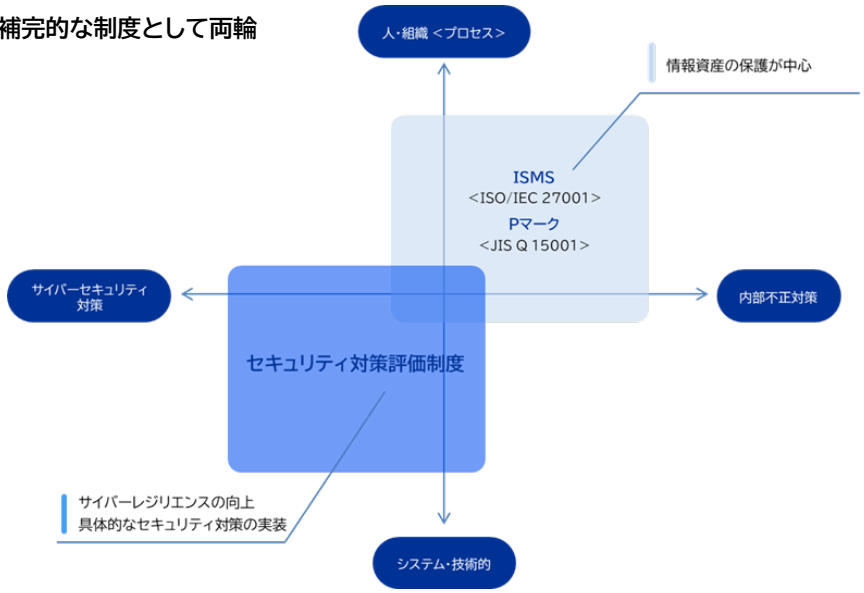
星の獲得はビジネスチャンスの拡大につながります
「制度が始まってから」ではなく ”先行して” 準備を進めましょう！

Section2

セキュリティ対策評価制度の全体像

＜補足＞　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

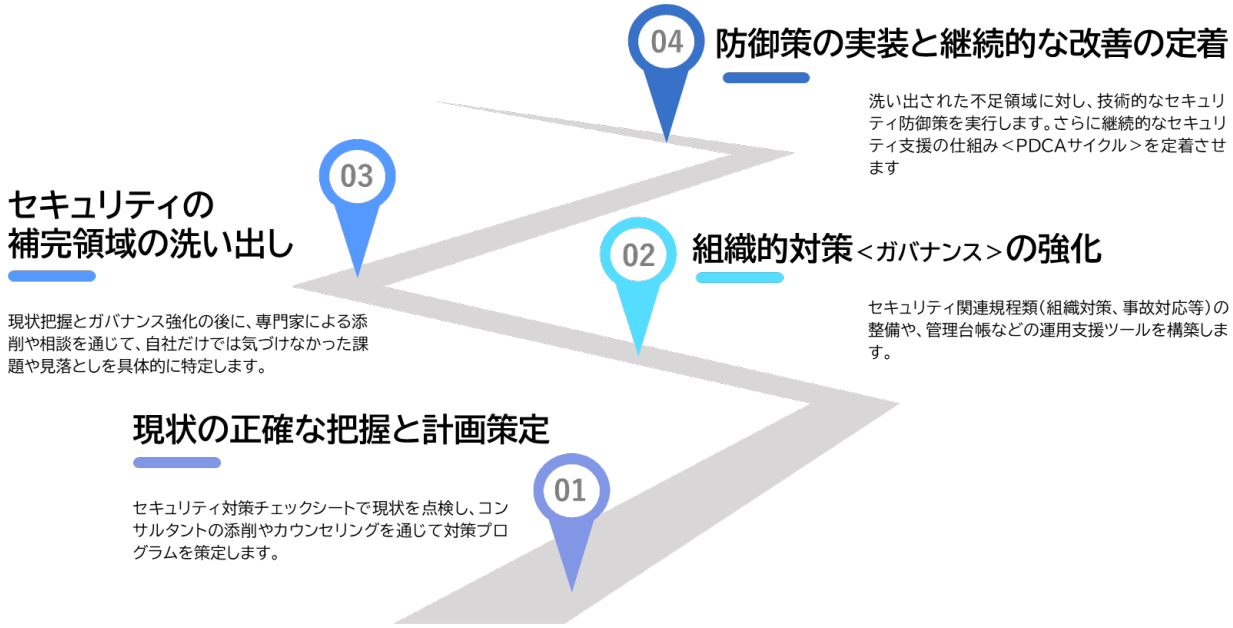
Section3

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。

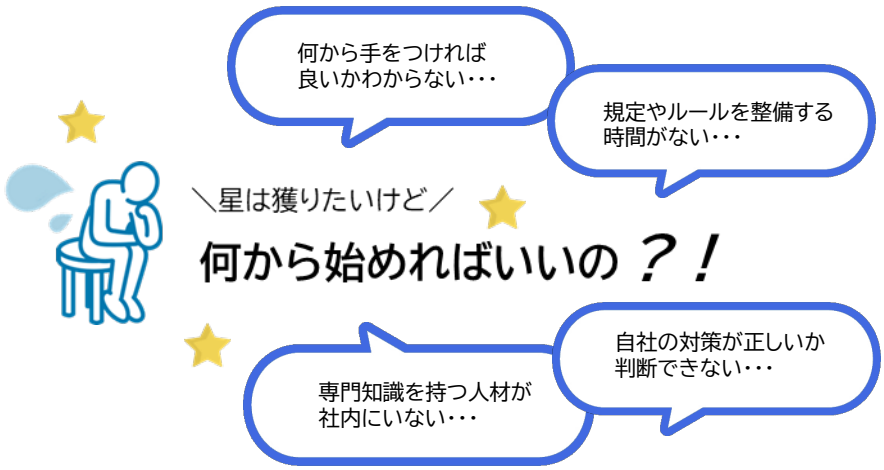
星 ＜★＞取得までに必要な4つの準備プロセス

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

「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

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

教育コンテンツ

＜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

各種運用支援ツール

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

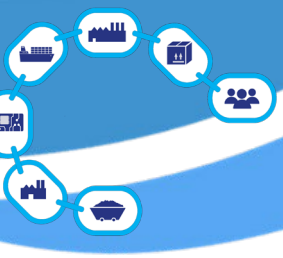
13.入退室管理台帳

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

2つのコースとご提供価格

＼まずは自社の現状や課題を把握したい企業向け／

学習コース

定価：¥225,000 ※1
利用期間：3カ月

含まれるご支援内容

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

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。

＼改善を進めたい・セキュリティレベルを維持したい企業向け／

実践コース

＜ 新規購入時 ＞
定価：¥450,000 ※1
利用期間：9カ月

＜ 継続更新 ＞
定価：¥120,000 ※1
利用期間：12カ月

含まれるご支援内容

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

※1 価格は税別表示です
※2 実施回数の制限があります。

各ご支援内容の概要

●●学習コース ●実践コース

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

カウンセリング（●）

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

ndis
NDIソリューションズ株式会社

Section 4

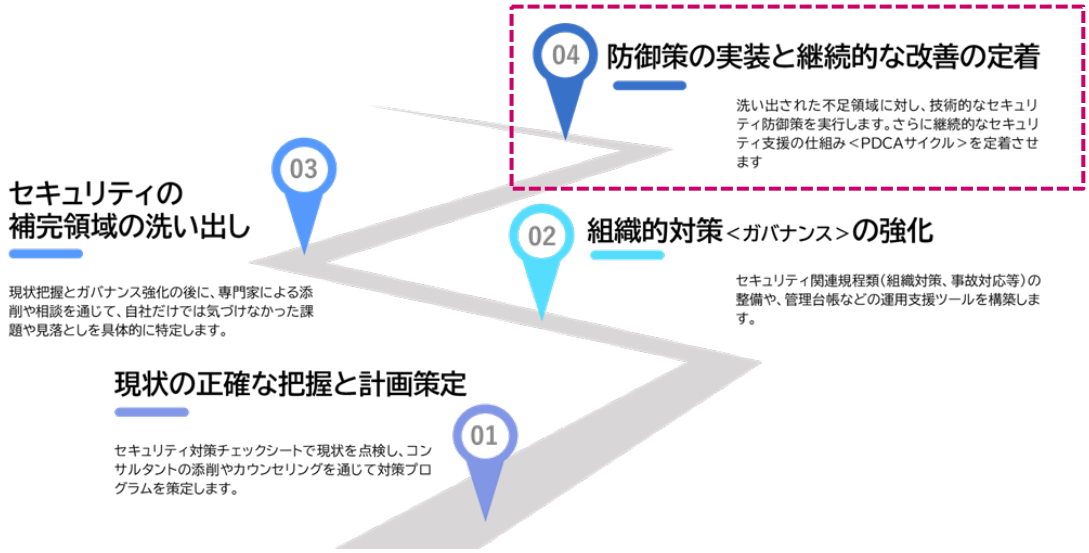
星＜★＞獲得のために必要なセキュリティ不足領域の補完とご支援策

Section4

星＜★＞獲得のために必要なセキュリティ不足領域の補完とご支援策

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補完が必要です。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補完とご支援策

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

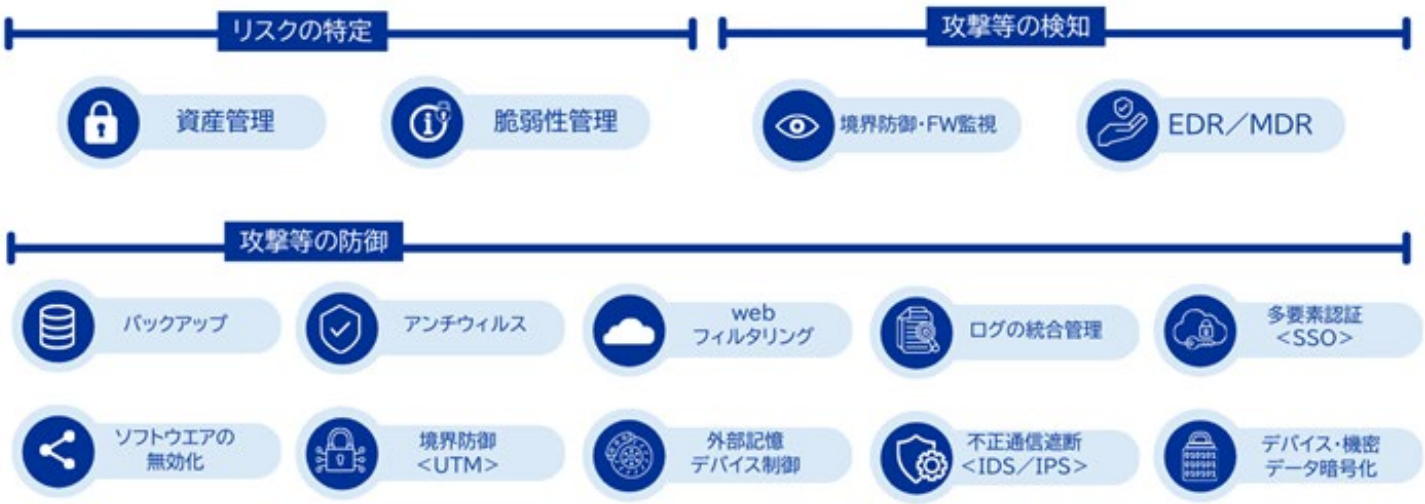
継続的なご支援

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1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：2025/12/26

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（案）」
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

付 録

経済産業省 更新・追加情報一覧

2025年12月26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(案)」

https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

制度構築方針(案)で明確になった5つのポイント

Point 1 制度の範囲・位置づけ

- 評価対象のIT基盤の範囲が明確化(公開サーバ、クラウド等)
- 取得範囲はグループ／企業／部門など柔軟に設定可能

Point 2 星の取得要請<発注者の役割>

- 星4取得要否は事業継続・情報管理リスクを踏まえ発注者が判断
- 星取得要請の際に独占禁止法・取適法に抵触しない進め方を国が整理する予定

Point 3 審査方法

- 全評価基準への適合が原則必須(例外は審査者確認)
- 技術検証は外部からの脆弱性検査(VPN・ルータ等)を実施

Point 4 スケジュール

- 2026年3月 方針公表／2026年度末 運用開始予定

Point 5 要求事項・評価基準

- NIST CSFをもとに再整理
- 評価軸は『書類』から『実効性(仕組み)』へ

詳 細 制度構築方針(案)で明確になった5つのポイント

Point 1 制度の範囲・位置づけ

- 取得する範囲が柔軟に設定することが可能に
  例)企業グループ、企業、企業の特定部門
- 取得する範囲の対象は「IT基盤」
  IT基盤であることは変更ないが、公開サーバや認証基盤、クラウドサービスも範囲であることが明確化

※ 補足として、要求事項を満たすことが困難なIT機器やソフトウェアを例外的に適用範囲に含めないことが許容された(妥当性の評価は必要)

Point 2　星の取得要請 <発注者の役割>

- 星4に該当する企業の決定が発注企業側にて考える必要がある
  変更前）星4に該当するケースが明確であった
  変更後）事業継続リスクと情報管理リスクの観点から発注企業にて観点を整理して対象となる取引先を検討する必要がある

- 取得する範囲の対象は「IT基盤」
  発注者から要請する際に独占禁止法・取適法に抵触しない「問題にならない進め方」のベストプラクティスを経済産業省・公正取引委員会が公表

Point 3　審査方法

- すべての評価基準に適合しないと星は獲得できないことが公開された。
  そのため、不適合事項があった場合は審査者にて内容確認を受けて問題なければ、星獲得となる

- 星3の申請スキームに「経営層による自己適正宣誓」が追加
- 星4は認定取得後に証書の発行がある（星3については証書の発行は無い）
- 具体的な審査内容と、おおよその所要時間が公開

審査項目	内容	星 ★★★	星 ★★★★
文書確認	提出書類の確認	●	●
実地審査	ヒアリングや規程・操作画面の確認による評価	―	●
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）への脆弱性検査の実施	―	●

取得した認定の有効期間は、星3が1年、星4が3年。星4は1年ごとに自己評価で対策状況を申告します。

Point 4　スケジュール

- 2026年3月までに「制度構築方針の公表」
- 具体的な審査内容と、おおよその所要時間が公開

Point 5　要求事項・評価基準

- 全体構造の整理

  2025年4月公開の要件案をもとに、NIST CSFの枠組みに当てはめて再整理
  大分類：変更なし
  中分類：表現の微調整のみ（考え方は継続）

- 評価基準の見直し ＜追加・削除＞

  追加項目

  - リモートワークにおけるルールの整備（リスクの特定／資産管理）
  - メールによるマルウェア感染防止対策（星4）
  - サイバー攻撃を想定した事業継続・復旧対応（星3）など、約9項目が追加

  削除項目

  - 退職者による機密情報の持ち出し対策
  - 重要システムのデータベース暗号化
  - 管理者権限を持つ共有アカウントのアクセスログ取得など、約9項目が削除

- 評価基準の項目数が **44項目 → 157項目** に大幅増加

  評価基準ごとに細分化・番号付けされただけで、実質的に**求められる対策が大きく増えたわけではない**

- 評価の考え方の変化

  「文書化する」「一覧を作成する」などの記載が『仕組みを整備すること』などの表現に変更

2026年1月版

※ 2025年12月26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