NS Next Security

セキュリティ診断サービス ご提案

セキュリティ対策評価制度（SCS）対応版

もう「対岸の火事」ではない、
サプライチェーンという経営リスク

IPAが公表する「情報セキュリティ10大脅威 2025」で、**サプライチェーン攻撃は第2位**にランクイン。
2019年の初登場以来、7年連続で選出される **主要な経営リスク** になっています。

IPA 情報セキュリティ10大脅威 2025
「組織」向け脅威

2 位
(全10項目中)

**サプライチェーンや
委託先を狙った攻撃**

7年連続 7回目のランクイン

上位5脅威（2025年版・組織）

1	ランサム攻撃による被害	10年連続10回目
2	**サプライチェーンや委託先を狙った攻撃**	**7年連続 7回目**
3	システムの脆弱性を突いた攻撃	5年連続 8回目
4	内部不正による情報漏えい等	10年連続10回目
5	機密情報等を狙った標的型攻撃	10年連続10回目

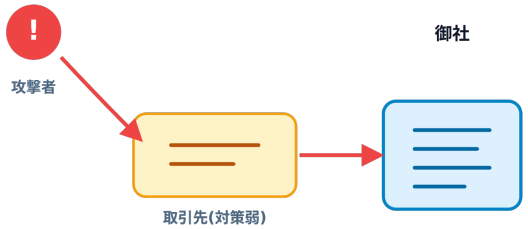
出典:IPA 情報セキュリティ10大脅威 2025(組織)

自社への攻撃がビジネス全体を停止させる

サプライチェーン攻撃＝攻撃者が本命を狙わず、**対策の甘い「取引先・関連会社・利用サービス」を踏み台**にする手口
入口はどこであれ、事業全体を止められる恐れがあります。

取引先経由の侵入

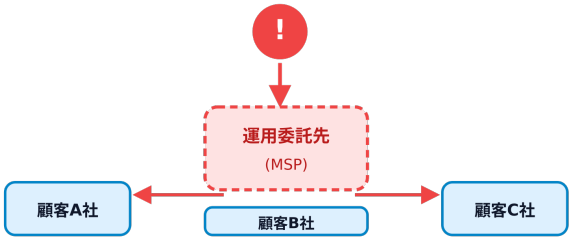
ビジネスサプライチェーン攻撃



対策が手薄な子会社や海外拠点をまず攻撃。
そこから**ネットワーク経由で本社へ侵入**する手口。

委託サービスの乗っ取り

サービスサプライチェーン攻撃



運用を任せている委託先を乗っ取り、**管理者権限で複数顧客に一斉侵入**。
短時間で被害が広範囲に拡大します。

ソフトウェア汚染

ソフトウェアサプライチェーン攻撃

正規のアップデートに**ウイルスを混入**させ、全ユーザーに配布。信頼された製品として入るため**検知が極めて困難**です。

被害は**現実**に起きています

いずれも取引先や委託先を経由し、**被害企業側は"自社を狙われた覚えがなかった"**事例です。

情報漏えい

通信サービス企業

2023年11月 / 2024年2月

約44万件

利用者情報が漏えい

委託先企業の従業員PCがマルウェア感染。第三者による不正アクセスで、後日さらに**従業員等の個人情報 約8万件**も追加で判明。

医療停止

公立病院

2022年10月

2ヶ月+

通常診療ができない状況

外部業者を介した不正侵入でランサムウェア攻撃を受け、電子カルテシステムに障害が発生。**緊急以外の手術・外来診療が一時停止**。

生産停止

自動車部品メーカー

2022年3月

全工場

1日稼働停止(連係企業も)

部品メーカーがランサムウェア攻撃を受けサーバがダウン。**連係する自動車メーカーの国内全工場も稼働を停止**する事態に。

サービス停止

クラウド事業者

2023年6月

データ暗号化

一時サービス提供不能

データセンターのサーバが不正アクセスされ**ランサムウェア感染**。データが暗号化され、利用企業がサービスを使えない状態に。

2026年度末
新しい「ものさし」
がスタート。

経済産業省が主導する**「セキュリティ対策評価制度（SCS）」**により、企業のセキュリティ対策は**共通の基準で見える化**される時代へ。

今後は「弊社は**★3を取得している**」と一言で説明できる状態が、取引の"信頼の証"になります。

SCS評価制度とは

経済産業省による「サプライチェーン強化に向けたセキュリティ対策評価制度」。**サプライチェーン全体のセキュリティを、共通の"ものさし"で見える化する**仕組みです。

WHAT

**共通の基準で
対策レベルを可視化**

★3〜★5の段階で、自社の対策状況を客観的な"数字"のように示せる仕組みです。

WHY

コスト → 信頼の証へ

セキュリティ対策を"経費"ではなく、取引先から選ばれる**競争力の源泉**に変えます。

WHO

**取引に関わる
すべての企業**

大企業だけでなく、その取引先の**中堅・中小企業も対象**。今後、幅広い業界に広がる見込みです。

【POINT】

**任意制度ですが、「弊社は★3を取得している」という一言が、
取引先での信頼獲得や商談の後押しになる可能性があります**

出典: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

5分でわかる！SCS評価制度（セキュリティ対策評価制度）導入ガイド

2026年度末開始！サプライチェーン全体のセキュリティレベルを共通の「ものさし」で可視化し、信頼できる取引環境を構築。

制度の目的：共通の「ものさし」による可視化

業界共通の基準で自社の対策を証明し、
取引先ごとの異なる調査への対応負担を軽減します。

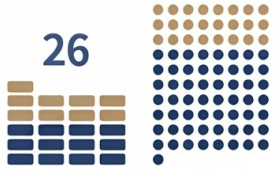
評価レベル（★3・★4）の決定的な違い

★3（Basic）：すべての企業が目指すべき「基礎水準」

目指す水準:
一般的な脅威を防ぐ
最低限実装すべき基礎対策

評価方法:
専門家確認付きの
自己評価 (有効期間1年)

主な項目数:
26要求事項 / 83評価基準

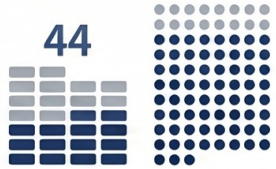


★4（Standard）：機密情報を扱う企業向けの「標準・高度水準」

目指す水準:
被害拡大防止を含む
包括的対策

評価方法:
第三者評価機関による実地
審査・技術検証 (有効期間3年)

主な項目数:
44要求事項 / 157評価基準



対象範囲と7つの評価領域

評価対象は「企業のIT基盤」

対象。

※製造ライン（OT）や
製品自体は原則対象外。

NIST CSFベースの7つの評価分類

重要：運用実績（証跡）の提示が不可欠

「ツールの導入」だけでなく、
ログや教育記録、復元テストなどの
「運用の証拠」が評価されます。

まず目指すのは、★3の取得です

すべての企業が最初に目指すべき**基礎水準**が★3。
機密情報を扱う企業向けの**高度水準**が★4です。

★★★

すべての企業が目指すべき基礎水準

一般的なサイバー脅威を防ぐために、最低限実装すべきセキュリティ対策

要求事項	評価基準
26 項目	83 基準

評価方法
専門家確認付きの自己評価（有効期間 1年）

★★★★

機密情報を扱う企業向けの高度水準

★3に加え、**被害拡大の防止**まで含む、より包括的な対策

要求事項	評価基準
44 項目	157 基準

評価方法
第三者評価機関による実地審査（有効期間 3年）

評価は7つの領域から、
あなたの会社を360°チェック

国際基準（NIST CSF）に、日本ならではの**「取引先管理」**を加えた7つの分類で、対策の穴を残さず確認します。

01
ガバナンス
GOVERNANCE

セキュリティ担当者・責任・方針・経営層への報告体制

02
取引先管理
SUPPLY CHAIN

機密情報の共有先、重要取引先の対策状況・役割分担

03
リスクの特定
IDENTIFY

情報資産の棚卸、ネットワークや外部サービスの管理

04
防御
PROTECT

ID・アクセス権限、パスワード、境界防御、マルウェア対策

05
検知
DETECT

ログ取得、監視、異常検知、分析の仕組み

06
インシデント対応
RESPOND

緊急時の対応手順、連絡体制、報告・情報共有

07
復旧
RECOVER

復旧手順、時間、バックアップ・事業継続計画

重要:「製品を導入しただけ」では不十分。運用の証跡（ログ・教育記録・訓練実績）まで含めて客観的に示せることが評価の対象になります。

あなたの会社の現在地を知る
サイバーセキュリティの「健康診断」
NSセキュリティ診断

経済産業省が主導する**「セキュリティ対策評価制度（SCS）」**
★3を取得に対して、なにが出来ていてなにが足りないのかを
企業のセキュリティ状態を**見える化します**

セキュリティ対策の状態が一目でわかります

「セキュリティの健康診断」という考え方

機械やツールで **スキャン** するのではなく、お医者さんが患者さんに問診するように、**担当者へのヒアリング**を通じて現状の対策を丁寧に確認していく診断です。

お医者さんの「問診」と同じ

治療の前に **いろいろな質問(問診)** をして、
病気の有無や病状を判断する。それと同じ流れです。

御社にとっての「診断」とは

1. **担当者へのヒアリングが中心**
   実機を触る調査ではなく、質問で状況を丁寧に洗い出します。
2. **「どこに課題があるか」を見つける**
   対策の抜け漏れや優先すべきポイントを可視化します。
3. **具体的な処方箋（対策提案）まで**
   課題ごとに、次に何をすべきかをレポートに落とし込みます。

診断の進め方 – 4つのステップ

実機の調査は**不要**。ヒアリング中心のシンプルな流れで、**Web会議で完結する**ことも可能です。

Step 01
事前準備

診断内容や事前にご準備いただきたい資料をご説明し、ヒアリング日程を決定します。

所要時間
60分 / Web会議可

Step 02
ヒアリング

診断票に基づき、担当者へのヒアリングを実施します。**実機調査はありません。**

所要時間
90分 / Web会議可

Step 03
レポート作成

ヒアリング結果を、診断結果報告書としてまとめます。現状・課題・優先すべき対策を明記。

作成期間
2〜3週間

Step 04
結果報告会

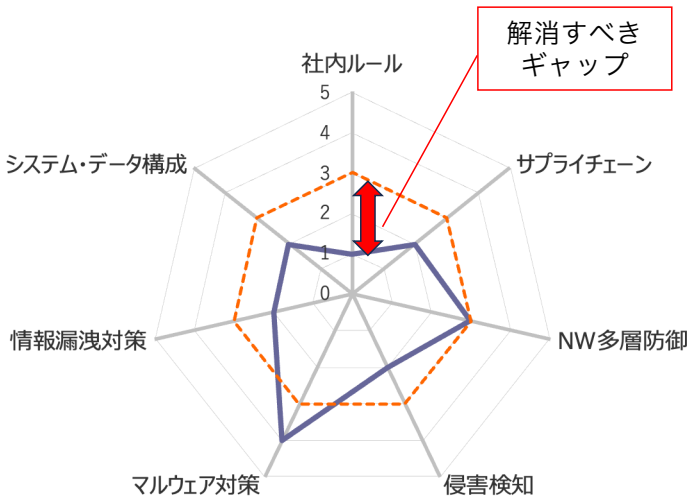
報告書を元に結果をご報告し、今後の進め方を協議します。

所要時間
90分 / Web会議可

成果物 1 – 診断結果報告書で、現在地が一目でわかる

7つのカテゴリ・42項目を評価し、**レーダーチャート**で可視化。**現状 → ★3達成**のギャップと、
優先すべき対策までを明示します。

7カテゴリのレーダーチャート



レポートに含まれる内容

総評 / カテゴリ別スコア

7カテゴリを1〜5の点数で評価し、体制全体の傾向を明示。

現状のリスク

「ポリシーがない」「侵入検知ができない」「復旧ができない」など、
具体的な穴を明記。

個別診断項目の詳細

項目ごとに**4色アイコン**で優先度を可視化
(即時対応 / 中長期 / 推奨 / アドバイス)。

優先すべき対策 (処方箋)

何から着手すべきか、次のアクションを明確化。単なるダメ出しではなく★3
達成に向けた具体策を提示します。

成果物２ – 個々の診断項目に対する詳細な説明

個々の診断項目について、現状の課題と対策・推奨項目を説明します。対策は4色のアイコンで示されており対策の優先度が一目でわかります

🔴即時の対応が必要　🟠中長期的な対策が必要　🟢推奨　🔵アドバイス

	現状→目標	現状の課題	対策・推奨項目
社内ルール	1→3	□**取引先とのビジネスおよびシステム上の関係**　現状は、業務委託先やシステム連携を行っている取引先の情報が各担当者に属人化しており、…	🔴**取引先の棚卸しと台帳作成:** 現在取引のある全ての委託先・ベンダーを洗い出し、 🔴**システム接続形態の明確化:** 各取引先とどのような経路で接続しているか
サプライチェーン	2→3	□**機密情報の取り扱い** 取引開始時に秘密保持契約（NDA）は締結しており、法的な枠組みはできています。しかし、実際の業務において、メールで	🟠**情報の重要度分類（格付け）の定義**: 自社の情報を「極秘・社外秘・公開」などに 🟢**取引先との授受ルールの明確化:** 上記のルールに基づき、取引先と機密情報をやり
ネットワーク多層防御	3→4	□**サプライチェーンとのネットワーク接続** 保守ベンダーやシステム開発会社などが利用する「リモートメンテナンス用VPN」や「遠隔操作ツール」の利用状況が、	🔴**外部接続の棚卸しとリスト化:** 各部門へのヒアリングを行い、保守用VPN、専用線 🟢**「必要な時だけ接続」への運用変更:** 原則として24時間365日の常時接続を禁止
侵害の検知とインシデント対応	2→3	□**インシデント対応** 社内の連絡網はあるものの、委託先やシステム連携先との間での「緊急時の報告ルール」が取り決められていません。	🔴**相互緊急連絡網（ホットライン）の構築:** 営業担当者経由の連絡では遅延するた 🔴**責任分界点の確認:**「ウイルス感染時はどちらが回線を切断するか」

診断後、達成に向けたロードマップをご提案します

診断結果をもとに、★3達成に向けた優先対策を 整理してご提案いたします

こちらは1例です

1 組織的対策

GOVERNANCE

- ✓ セキュリティポリシーの策定
- ✓ 情報資産の特定と管理台帳の作成
- ✓ インシデント対応体制と連絡網の整備

2 技術的対策

TECHNICAL

- ✓ 統合脅威管理(UTM)による多層防御の実現
- ✓ ログ監視・分析ソリューションでの検知能力強化
- ✓ バックアップ運用の見直し(3-2-1ルールの徹底)

3 人的・物理的対策

PEOPLE & PHYSICAL

- ✓ 従業員へのセキュリティ教育・訓練
- ✓ クリアデスク・クリアスクリーンの徹底
- ✓ サーバ室への監視カメラ設置

4 サプライチェーン

SUPPLY CHAIN

- ✓ 機密情報の取り扱いルールの確認
- ✓ 外部接続方式の見直し
- ✓ 取引先との連絡網整備

セキュリティを、
「コスト」から「信頼の証」へ。

01 現状の可視化

「お医者さんの問診」のようなヒアリングで、負担なく**現状のリスクとギャップ**を洗い出します

02 具体的な処方箋

単なるダメ出しではなく、**★3達成に向けたロードマップ**と優先順位を提示します

03 対策の指南役

診断後の**有料にて伴走支援も行えます**
自社だけでは進めにくい対策を外部の指南役としてサポートします

まずは無料ヒアリングから。 ★3獲得への準備を、今日から。

お問い合わせ
株式会社MOIN
電話：0238-49-7610
Mail：info@moin.co.jp