Japan Security Framework Readiness Worksheet

日本のセキュリティ・フレームワーク準備ワークシート

April 19, 2026 / 2026 年 4 月 19 日

English Version

See page 3 →

日本語版

10 ページへ →

Japan Security Framework Readiness Worksheet

April 19, 2026

Contents

How to use this worksheet . . . 3
Part 1 — Scorecard . . . 3
Part 2 — Identify your path . . . 4
Part 3 — Roadmaps . . . 4
  Path A — Starting from zero . . . 4
  Path B — ISO 27001 holder . . . 5
  Path C — Supply-chain supplier . . . 5
  Path D — Regulated sector . . . 6
Part 4 — The stacking timeline at a glance . . . 6
Part 5 — Where are the sharp edges? . . . 7
Where eSolia can help . . . 8
Contact Us . . . 9

A practitioner's companion to our article Japan's Security Compliance Stack: How SECURITY ACTION, ISO 27001 and SCS Fit Together. Five scorecard questions map your current state to one of four paths, each with a concrete 90-day and 12-month roadmap — so you can see what to do next and in what order.

How to use this worksheet

Japan's security compliance picture for SMEs in 2026 is a layered stack, not a single badge:

- **ISO/IEC 27001** is the substance layer
- **SECURITY ACTION ★★** (IPA) is the locally-legible signal layer
- **SCS ★3 and above** (METI, launching late FY2026) is the supply-chain procurement-rating layer

Done in the right order and with a control crosswalk, each layer reuses substance from the one below. Done in parallel, as three independent projects, it's slow and expensive.

This worksheet helps you figure out **where you are on that stack today and what to do next**. Work through the scorecard, identify which path matches your answers, then follow the 90-day and 12-month roadmap for that path.

Part 1 — Scorecard

Tick the box next to each statement that is currently true for your company. "Partially" counts as "no".

- □ **Q1. Our company holds ISO/IEC 27001 certification today, or is in an active certification process with a certification body.** Why it matters: ISO 27001 is the substance layer. If you have it, satisfying SECURITY ACTION ★★ and most of SCS ★3 is mostly reformatting, not new control work.
- □ **Q2. We have declared SECURITY ACTION ★1 or ★★ via the IPA management system (kanri shisutemu 管理システム).** Why it matters: ★★ is the cheapest locally-legible signal in the Japan market, and a prerequisite for the IT Introduction Subsidy (IT dōnyū hojokin, IT 導入補助金) in most categories.
- □ **Q3. Our representative director (daihyo 代表者) holds a valid gBizID Prime account.** Why it matters: As of April 1 2026, SECURITY ACTION signup is gated behind gBizID Prime. Prime is becoming the identity layer for many government-facing services, so it's worth having regardless.
- □ **Q4. We sell into Japanese enterprise supply chains** — i.e. our direct customers include Toyota, NTT, Mitsubishi-class primes, their subsidiaries, or other large Japanese enterprises that manage supplier security requirements. Why it matters: Those primes are expected to start writing SCS star ratings into procurement contracts from FY2027 onward. The earlier you watch this, the cheaper it is to get ready.
- □ **Q5. Our business is in a regulated sector** — financial services (banks, securities, insurance), healthcare provider, government-facing work, or critical infrastructure. Why it matters: Sector-specific frameworks (FISC, MHLW, NISC/NCO) apply in addition to the general stack, and they can carry heavier substance requirements than SCS.

Part 2 — Identify your path

Use the combination of your answers above to pick the path that best matches your situation. If you fit two paths, start with whichever is furthest along and layer the other in.

Your answers	Your path
Q1 no, Q2 no, Q5 no	**Path A — Starting from zero**
Q1 yes (or in progress), Q2 no	**Path B — ISO 27001 holder**
Q4 yes (regardless of others)	**Path C — Supply-chain supplier**
Q5 yes (regardless of others)	**Path D — Regulated sector**

The four paths are not mutually exclusive — an ISO 27001 holder selling into Toyota's supply chain is Path B and Path C. Read both.

Part 3 — Roadmaps

Path A — Starting from zero

You have no formal posture today, and are not in a regulated sector or a large-enterprise supply chain yet. The goal is to establish a visible baseline at minimum cost.

Next 90 days

- □ Apply for **gBizID Prime** for your representative director (same-day online with a My Number card, ~2 weeks by post)
- □ Download and read the IPA **25-item self-check** (gofun de dekiru jisha shindan, 5 分でできる自社診断) — see what the bar looks like in practice
- □ Write a short information security policy (one to three pages is enough for ★★; a template from IPA is fine)
- □ Declare **SECURITY ACTION** ★★ via the IPA management system
- □ Add the ★★ logo to your website footer per IPA usage guidelines

Next 12 months

- □ If you apply for the IT Introduction Subsidy, ★★ is now in place as the prerequisite
- □ Review the IPA SME Information Security Guideline and close obvious gaps (MFA, backup, patch discipline, training)
- □ Decide whether the business case for ISO 27001 certification exists — typically driven by overseas-HQ expectations or a large-enterprise customer request

Typical effort: Low. An afternoon for ★★ once Prime is in place; policy writing is a few days of work if starting from scratch.

Path B — ISO 27001 holder

You already have (or are certifying to) ISO 27001. The substance is in place; the job is to put the right wrappers around it.

Next 90 days

- □ Confirm your representative director holds **gBizID Prime**
- □ Confirm the IPA 25-item self-check is satisfied by existing ISMS evidence — this is a formatting review, not new control work
- □ Declare **SECURITY ACTION ★★** and add the logo to your website footer
- □ Start watching METI's SCS publication page for the operational guidance (gaidansu shiryoガイダンス資料), expected H2 2026

Next 12 months

- □ Build (or borrow) a **control crosswalk** mapping ISO 27001 Annex A controls against NIST CSF 2.0 functions and SCS ★3 requirement items — this is what lets ISMS evidence regenerate into SCS format without maintaining two stores
- □ Identify a qualified **Registered Information Security Specialist** (RISS, toroku sekisupe 登録セキスペ) who can perform the SCS ★3 expert confirmation
- □ Run a dry SCS ★3 gap check as soon as the operational guidance is published

Typical effort: Low for ★★ (afternoon). Moderate for SCS ★3 prep (one quarter of format work spread over the year).

Path C — Supply-chain supplier

You sell into Japanese enterprise supply chains. Your primes are expected to start asking about SCS star ratings from FY2027 onward.

Next 90 days

- □ Everything in Path A or Path B as applicable — the ISO 27001 + SECURITY ACTION ★★ foundation is a prerequisite
- □ Check your current customer contracts and RFP responses for any language referencing **SCS**, **Pマーク**, **ISMS**, or **sector-specific security requirements** — these are leading indicators
- □ Identify which of your customers are large enough to write procurement security requirements (the **primes** rather than peer SMEs)

Next 12 months

- □ Build a **control crosswalk** (ISO 27001 Annex A × NIST CSF 2.0 × SCS ★3)
- □ Shortlist a **RISS** for SCS ★3 expert confirmation
- □ Target **SCS ★3 submission** for Q2 2027 (after METI publishes final operational guidance)
- □ Monitor customer RFPs for the first SCS ★ references — these are your earliest warning that ★3 is becoming a procurement expectation
- □ Decide on a **trigger policy for SCS ★4**: SCS ★4 adds third-party evaluation (document + onsite + technical verification) and is not cheap. A common policy is "pursue ★4 only when a named client contract requires it" — that prevents speculative over-investment while keeping you ready to act on real demand

Typical effort: Moderate. SCS ★3 is mostly a format exercise against an ISO-grounded ISMS, plus the RISS fee.

Path D — Regulated sector

You are in financial services, healthcare, government-facing work, or critical infrastructure. Sector frameworks apply on top of (not instead of) the general stack.

Next 90 days

- □ Identify which sector framework applies to you and confirm your current state:
  - **Financial services**: FISC Security Guidelines (13th Edition, Nov 2025) + FSA Supervision Guidelines
  - **Healthcare**: MHLW Safety Management of Medical Information Systems + METI + MIC cloud handling guidelines (all three apply for cloud/outsourced medical info)
  - **Government-facing work**: NCO (formerly NISC) Common Standards on Cybersecurity Measures for Government Agencies
  - **Critical infrastructure**: your designated sector's supplementary guidelines under the national CI policy
- □ Confirm your representative director holds **gBizID Prime**
- □ Declare **SECURITY ACTION ★★** — the local signal still applies, and the substance is a subset of sector requirements

Next 12 months

- □ Treat sector framework compliance as the primary posture, with ISO 27001 as the internationally-legible wrapper
- □ Monitor SCS developments — if you also sell into a supply chain (Path C overlap), SCS ★3 layers on top of sector requirements
- □ Review cloud provider selection against sector data-residency and ISMAP status

Typical effort: Significant — sector frameworks dominate the workload, and the general-stack layers are secondary.

Part 4 — The stacking timeline at a glance

The order in which layers compound, and approximate effort at each step:

Layer	Typical effort	Who does it
gBizID Prime (infrastructure)	Same day (online) or ~2 weeks (postal) · Free	Representative director
SECURITY ACTION ★1	~1 hour · Free	Anyone with gBizID access
SECURITY ACTION ★★	~1 afternoon once policy + self-check are in hand · Free	Anyone with gBizID access
ISO/IEC 27001 certification	9–18 months typical · Certification-body fees + internal time	ISMS lead + external auditor
SCS ★3 (from existing ISMS)	~1–3 months of format work + RISS confirmation	ISMS lead + registered specialist
SCS ★4 (from existing ★3)	~3–4 months focused work + third-party evaluation	ISMS lead + accredited assessor

The specific numbers depend on your size, sector, and how much of the substance is already in place. A single-developer firm with a clean slate will spend more of its time on ISO 27001 and much less on SCS ★3 — the reverse of a larger company with an ISMS already in place.

Part 5 — Where are the sharp edges?

A few specific places where SMEs might get stuck. If any of these describe you, it's worth flagging them early — they're upstream of the certification work itself.

gBizID Prime for foreign representative directors. The online path requires the representative director's **My Number card** with an active signing certificate. The postal path requires a registered personal seal (inkan 印鑑) plus a seal certificate (inkan shoōmeisho 印鑑証明書). Both require **Japanese resident registration** (jūminhyo 住民票). A representative director who doesn't have resident registration hits the wall before SECURITY ACTION is even in view.

Supplier register scope for SCS ★3. SCS treats supplier management as its own domain. Your existing vendor list probably needs a small schema extension (risk tier, security evidence held, date of last confirmation) to satisfy the ★3 evaluation sheet.

Evidence vs. explainability. SCS ★3 explicitly emphasizes evidence that controls operate, not just that they exist on paper. That means retaining logs, access review records, patch cadence screenshots — the kind of artifacts an ISMS internal audit already produces, but not always in a format a procurement team can consume.

Expert confirmation (RISS) capacity. SCS ★3 requires a RISS sign-off. The pool of qualified specialists is finite, and demand is expected to concentrate around the FY2027 launch window. Shortlisting one earlier rather than later is a good idea.

Where eSolia can help

We run this same stack internally — ISO 27001 certification in flight, SECURITY ACTION ★★ declared, SCS ★3 on our FY2027 roadmap, ★4 deferred to client trigger — so we work with clients on it from a practitioner's perspective.

Get in touch, if you want help translating this worksheet into a sequenced plan specific to your business, including:

- Gap assessment against ISO 27001, SECURITY ACTION ★★, or SCS ★3
- Control crosswalk development (ISO 27001 × NIST CSF 2.0 × SCS)
- Policy and evidence-artifact development
- Sector framework review (FISC, MHLW, NCO)
- RISS identification and engagement coordination

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST

日本のセキュリティ・フレームワーク準備ワークシート

2026 年 4 月 19 日

目次

- ワークシートの使い方 11
- Part 1 — スコアカード 11
- Part 2 — 該当パスの特定 12
- Part 3 — ロードマップ 12
  - パス A — ゼロから始める 12
  - パス B — ISO 27001 保有企業 12
  - パス C — サプライチェーン・サプライヤー 13
  - パス D — 規制業種 13
- Part 4 — スタックの全体タイムライン 14
- Part 5 — つまずきやすいポイント 14
- 当社（eSolia）がお手伝いできること 15
- お問い合わせ 16

当社記事「日本のセキュリティコンプライアンス・スタック: SECURITY ACTION、ISO 27001、SCS の組み合わせ方」の実務用補助資料です。5 問のスコアカードで自社の現状を整理し、該当する「パス（道筋）」を特定したうえで、90 日／12 ヶ月のアクションプランに落とし込みます。**海外本社に対して、なぜ日本特有のフレームワークにも取り組む必要があるのかを説明するためのツール** としても活用できます。

ワークシートの使い方

2026 年時点の日本における中小企業のセキュリティコンプライアンスは、**単一の認証ではなく「層構造（スタック）」** として捉える必要があります:

- **ISO/IEC 27001** — 管理策の基盤層
- **SECURITY ACTION ★★**（IPA） — 国内で認知されやすい信頼シグナル層
- **SCS ★3 以上**（経済産業省、FY2026 末に制度開始予定） — サプライチェーン向けの調達評価層

適切な順序で取り組み、コントロール・クロスウォーク（対応表）を整備すれば、各層の実質は下位層から再利用できます。3 つを並行して別々に構築すると、時間とコストが倍増します。本ワークシートは、**スタック上の現在地と、次に取るべき行動を特定する** ためのツールです。スコアカードに回答し、該当パスを確認し、そのパスに沿った 90 日／12 ヶ月のロードマップを実行してください。

Part 1 — スコアカード

自社の現状に当てはまる項目にチェックを入れてください。「部分的に該当」は「該当しない」として扱います。

- □ **Q1. 当社は ISO/IEC 27001 認証を取得済みである、または認証機関との認証手続きを進行中である。** 意義: ISO 27001 は管理策の基盤層である。取得済みであれば、SECURITY ACTION ★★および SCS ★3 の大部分は新規の管理策構築ではなく、フォーマット変換の作業となる。
- □ **Q2. 当社は IPA の管理システムを通じて SECURITY ACTION ★1 または★★を自己宣言済みである。** 意義: ★★は日本国内で最も低コストに取得できる信頼シグナルである。IT 導入補助金の多くのカテゴリで申請要件となっている。
- □ **Q3. 当社の代表者は有効な gBizID プライム・アカウントを保有している。** 意義: 2026 年 4 月 1 日以降、SECURITY ACTION の自己宣言には gBizID プライムが必須となった。プライムは政府関連サービス全般の共通 ID になりつつあり、本制度以外の用途でも取得する価値がある。
- □ **Q4. 当社は日本の大企業のサプライチェーンに組み込まれている** — 直接の取引先にトヨタ、NTT、三菱系列などのプライム企業、その子会社、または取引先のセキュリティ要件を管理する大企業が含まれる。意義: こうしたプライム企業は FY2027 以降、調達契約に SCS の星評価を組み込み始めると予想される。早めに対応するほど準備コストは低い。
- □ **Q5. 当社は規制業種に属する** — 金融（銀行、証券、保険）、医療機関、政府関連業務、重要インフラのいずれか。 意義: 業種別フレームワーク（FISC、厚生労働省、NISC／NCO）が一般スタックに加えて適用され、SCS より厳格な要件を含むことが多い。

Part 2 — 該当パスの特定

上記の回答の組み合わせから、自社に最も該当するパスを選択します。複数のパスに該当する場合は、より進んでいる方から着手し、他のパスを後から重ねます。

回答	該当パス
Q1 = いいえ、Q2 = いいえ、Q5 = いいえ	**パス A — ゼロから始める**
Q1 = はい（または進行中）、Q2 = いいえ	**パス B — ISO 27001 保有企業**
Q4 = はい（他の回答に関係なく）	**パス C — サプライチェーン・サプライヤー**
Q5 = はい（他の回答に関係なく）	**パス D — 規制業種**

パスは相互排他ではありません。例えばトヨタのサプライチェーンに属する ISO 27001 保有企業はパス B かつパス C です。両方のロードマップを参照してください。

Part 3 — ロードマップ

パス A — ゼロから始める

現時点で正式なコンプライアンス姿勢を持たず、規制業種にも大企業のサプライチェーンにも属していない状態。目標は、**最小コストで可視的なベースラインを確立すること**。

次の 90 日

- □ 代表者の **gBizID プライム**申請（マイナンバーカード利用でオンライン即日、郵送で約 2 週間）
- □ IPA **「5 分でできる自社診断」** をダウンロードして一読 — 基準の実態を把握する
- □ 情報セキュリティ方針の策定（★★には 1〜3 ページ程度で十分。IPA のテンプレート利用可）
- □ IPA 管理システムから **SECURITY ACTION ★★** を自己宣言
- □ ★★ロゴをコーポレートサイトのフッターに追加（IPA の使用ガイドラインに準拠）

次の 12 ヶ月

- □ IT 導入補助金に申請する場合、★★は前提要件としてクリア済み
- □ IPA の中小企業の情報セキュリティ対策ガイドラインを確認し、明らかな不足（MFA、バックアップ、パッチ管理、従業員教育）を埋める
- □ ISO 27001 認証取得の必要性を検討 — 一般的に海外本社の要求、または大企業顧客からの要請が動機となる

想定負荷: 低。gBizID プライム取得後、★★は半日程度の作業。方針策定をゼロから行う場合でも数日程度。

パス B — ISO 27001 保有企業

ISO 27001 を既に保有（または認証手続き中）。**実質は整っており、適切な「外殻」を整備するだけ** の段階。

次の 90 日

- □ 代表者の **gBizID プライム**保有を確認

- □ IPA の 25 項目自己診断が既存の ISMS エビデンスで満たされるか確認 ― フォーマット確認であり、新規の管理策構築ではない
- □ **SECURITY ACTION ★★** を自己宣言し、ロゴをサイトフッターに追加
- □ 経済産業省の SCS 公表ページをウォッチし、ガイダンス資料（2026 年後半公開予定）の発表を待つ

次の 12 ヶ月

- □ ISO 27001 附属書 A × NIST CSF 2.0 × SCS ★3 要求事項を対応付ける**コントロール・クロスウォーク** の作成（または借用）― ISMS エビデンスから SCS フォーマットを再生成できるようにし、二重管理を避ける
- □ SCS ★3 の専門家確認を担える**登録セキスペ**（登録情報セキュリティスペシャリスト）の候補を特定
- □ ガイダンス資料公開後、ドライランで SCS ★3 のギャップ分析を実施

想定負荷: ★★は低(半日)。SCS ★3 の準備は中程度(1 年のうち 1 四半期分のフォーマット作業)。

パス C ― サプライチェーン・サプライヤー

日本の大企業のサプライチェーンに納入している企業。プライム企業は **FY2027 以降、SCS 星評価を調達契約に組み込み始める見込み**。

次の 90 日

- □ パス A またはパス B を該当に応じて実施 ― ISO 27001 ＋ SECURITY ACTION ★★の土台は前提条件
- □ 現行の顧客契約および RFP 回答において、**SCS**、**P マーク**、**ISMS**、**業種別セキュリティ要件** への言及を確認 ― 先行指標となる
- □ 調達におけるセキュリティ要件を設定できる規模の顧客（同格の SME ではなく**プライム企業**）を特定

次の 12 ヶ月

- □ **コントロール・クロスウォーク**（ISO 27001 附属書 A × NIST CSF 2.0 × SCS ★3）を整備
- □ SCS ★3 の専門家確認を担う**登録セキスペ** をショートリスト化
- □ **SCS ★3 申請** を Q2 2027 目標で進める（経済産業省のガイダンス資料最終版公開後）
- □ 顧客の RFP における SCS ★への最初の言及をモニター ― ★3 が調達要件化する最も早い兆候
- □ **SCS ★4 のトリガー方針** を策定: SCS ★4 は第三者評価（文書審査＋現地監査＋技術検証）を追加するもので、低コストではない。「特定の顧客契約で要求された場合のみ取り組む」とする方針が一般的 ― 投機的な過剰投資を避けつつ、実需には即応できる体制を保つ

想定負荷: 中程度。SCS ★3 は主に ISO 基盤の ISMS に対するフォーマット作業と、登録セキスペ費用で構成される。

パス D ― 規制業種

金融、医療、政府関連業務、重要インフラのいずれかに属する企業。業種別フレームワークは**一般スタックの代替ではなく、その上に積まれる**。

次の 90 日

- □ 該当する業種別フレームワークを特定し、現状を確認:
  - **金融**: FISC 安全対策基準（第 13 版、2025 年 11 月）＋ 金融庁監督指針
  - **医療**: 厚生労働省「医療情報システムの安全管理に関するガイドライン」＋ 経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」＋ 総務省「クラウド

サービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（クラウド／外部委託で医療情報を扱う場合は 3 つすべてに準拠）
  - **政府関連業務**: 内閣官房国家サイバーセキュリティオフィス（NCO、旧 NISC）「政府機関等の情報セキュリティ対策のための統一基準」
  - **重要インフラ**: 国の重要インフラ指針における該当セクターの補完ガイドライン
- □ 代表者の **gBizID プライム** 保有を確認
- □ **SECURITY ACTION ★★** を自己宣言 ― 国内シグナルとしての価値は業種要件とは別軸であり、実質は業種要件の部分集合

次の 12 ヶ月

- □ 業種別フレームワークへの準拠を主軸とし、ISO 27001 は国際的に通用する認証層として位置付ける
- □ SCS の動向をモニター ― サプライチェーン向け販売も行う場合（パス C 該当）、SCS ★3 は業種要件の上に重ねて取得する
- □ クラウドプロバイダの選定を、業種のデータレジデンシ要件および ISMAP 登録状況に照らして見直す

想定負荷: 高。業種別フレームワークが作業の中心を占め、一般スタックの各層は副次的。

Part 4 ― スタックの全体タイムライン

各層が積み重なる順序と、おおよその作業負荷:

層	想定負荷	実施者
gBizID プライム（インフラ）	即日（オンライン）または約 2 週間（郵送）・無料	代表者
SECURITY ACTION ★1	1 時間程度・無料	gBizID アクセス権を持つ担当者
SECURITY ACTION ★★	方針と自己診断が準備済みなら半日程度・無料	gBizID アクセス権を持つ担当者
ISO/IEC 27001 認証	9〜18 ヶ月が一般的・認証機関費用＋社内工数	ISMS 責任者 ＋ 外部審査員
SCS ★3（既存の ISMS から）	1〜3 ヶ月のフォーマット作業 ＋ 登録セキスペによる確認	ISMS 責任者 ＋ 登録セキスペ
SCS ★4（既存の★3 から）	3〜4 ヶ月の集中作業 ＋ 第三者評価	ISMS 責任者 ＋ 認定評価機関

具体的な数値は、企業規模、業種、既存の実装度合いによって変動します。一人開発体制でゼロから始める企業は ISO 27001 により多くの時間を割き、既に ISMS が整備されている大企業では SCS ★3 により短期間で到達する傾向があります。

Part 5 ― つまずきやすいポイント

中小企業が最もつまずきやすい上流のポイントです。該当するものがあれば、認証作業そのものに着手する前に早期対応することを推奨します。

代表者が外国籍である場合の gBizID プライム取得: オンライン申請には代表者本人の**マイナンバーカード**（署名用電子証明書が有効であること）が必要です。郵送申請には代表者本人の登録済み印鑑と印鑑証明書が必要です。いずれも**住民登録（住民票）**が前提となるため、住民票のない代表者は gBizID の手前で手詰まりとなります。

SCS ★3 におけるサプライヤ登録のスコープ: SCS はサプライヤ管理を独立した領域として扱います。現行のベンダーリストには、★3 評価シートを満たすために軽微なスキーマ拡張（リスク階層、保有セキュリティエビデンス、最終確認日）が必要となる可能性が高いです。

「紙のうえでの存在」ではなく「運用されているエビデンス」: SCS ★3 は、管理策が**運用されている**ことのエビデンスを重視します（単に文書上存在するだけでは不十分）。ログの保管、アクセスレビュー記録、パッチ適用頻度のスクリーンショットなど、ISMS 内部監査が日常的に生み出す成果物を、**調達担当者が消費できる形式**に整える必要があります。

登録セキスペのキャパシティ: SCS ★3 には登録情報セキュリティスペシャリストの承認が必要です。有資格者の人数は限られており、FY2027 の制度開始前後に需要が集中することが予想されます。早めにショートリスト化しておくことを推奨します。

当社（eSolia）がお手伝いできること

当社は同じスタックを内部で運用しています ― ISO 27001 認証は進行中、SECURITY ACTION ★★は自己宣言済み、SCS ★3 は FY2027 のロードマップ、★4 は顧客契約をトリガーとして保留 ― このため、**実践者の視点から**クライアントをサポートできます。

本ワークシートを自社の事業に合わせた具体的な計画に落とし込むためのご支援として、以下のサービスを提供しています:

- ISO 27001、SECURITY ACTION ★★、SCS ★3 に対するギャップアセスメント
- コントロール・クロスウォーク（ISO 27001 × NIST CSF 2.0 × SCS）の作成
- 方針策定およびエビデンス成果物の整備支援
- 業種別フレームワーク（FISC、厚生労働省、NCO）のレビュー
- 登録セキスペの特定および連携コーディネート

お問い合わせ

株式会社イソリア 〒105-7105 東京都港区東新橋 1-5-2 汐留シティセンター 5 階 (Workstyling)

電話	03-4577-3380
メール	hello@esolia.co.jp
Web	https://esolia.co.jp
営業時間	月～金、9:00～18:00