Japanese Cybersecurity Frameworks and Guidelines

日本のサイバーセキュリティフレームワークとガイドライン

April 16, 2026 / 2026 年 4 月 16 日

English Version

See page 3 →

日本語版

15 ページへ →

eSolia

Japanese Cybersecurity Frameworks and Guidelines

April 16, 2026

Contents

Quick Reference: Which Frameworks Apply?

Use this matrix to identify relevant Japan cybersecurity frameworks based on client industry and size. The ★ (star) ratings refer to **maturity tiers** in Japan's supply chain security system: ★1-★2 are self-declarations any organization can make via IPA's SECURITY ACTION scheme, while ★3-★5 require progressively more rigorous evaluation. See the Supply Chain Security section for full details.

Client Profile	Primary Frameworks	Secondary/Optional
Bank, securities, insurance	FISC + FSA Supervision Guidelines	METI Cybersecurity Management
Large enterprise (non-financial)	METI Cybersecurity Management Guidelines	SCS Evaluation Framework
SME (under ~300 employees)	IPA SME Security Guidelines, SECURITY ACTION	SCS ★3 (if in a supply chain)
Government agency	NISC/NCO Common Standards	Sector-specific guidelines
Government contractor/supplier	METI Cybersecurity Management + SCS ★3/★4	NISC Common Standards (reference)
Healthcare provider	MHLW Medical Information Guidelines	METI Cybersecurity Management
IoT product manufacturer	JC-STAR labeling	METI OT/ICS guidelines
Critical infrastructure operator	Sector-specific CI guidelines	METI Cybersecurity Management
Any enterprise in a supply chain	SCS Evaluation Framework (★3 minimum)	METI Cybersecurity Management

Decision flow:

1. Is the client in a regulated sector (finance, healthcare, government, critical infrastructure)? Start with the sector-specific framework.
2. Is the client part of a supply chain for a larger enterprise or government? Add SCS Evaluation Framework.
3. For all other enterprises, use METI Cybersecurity Management Guidelines as the baseline.
4. For small businesses just starting out, use IPA SME Guidelines and the SECURITY ACTION self-declaration.

Financial Sector

FISC Security Guidelines

Issuing body: Center for Financial Industry Information Systems (FISC)
First published: 1985
Current version: 13th Edition (November 2025)
Scope: Banking and financial institutions

Status: Voluntary, but effectively required — referenced in FSA supervision guidelines
Update cadence: Major revisions every 2-3 years; supplements published as needed

The most comprehensive security framework for Japanese financial institutions, encompassing over 300 controls across four domains:

- Control measures
- Operational measures
- Facility measures
- Audit measures

System configuration implications:

- Enable comprehensive audit logging on all systems (M365 Unified Audit Log, database audit, network device logs)
- Enforce encryption at rest and in transit (TLS 1.2+ minimum, disk encryption)
- Implement network segmentation between internet-facing, internal, and management zones
- Configure access controls with role-based permissions and least privilege
- Retain logs for the period specified in the client's FISC compliance policy (typically 1-7 years depending on log type)
- Set up automated alerting for unauthorized access attempts
- Document all system changes with approval trails

Resources:

- FISC English portal: https://www.fisc.or.jp/english/
- AWS FISC compliance: https://aws.amazon.com/compliance/fisc/
- Google Cloud FISC mapping: https://cloud.google.com/security/compliance/fisc-japan
- Microsoft FISC compliance: https://learn.microsoft.com/en-us/compliance/regulatory/offering-fisc-japan

FSA Comprehensive Supervision Guidelines

Issuing body: Financial Services Agency (FSA)
Scope: Banks, securities firms, insurance companies
Update cadence: Revised periodically; check FSA portal for current version

Sector-specific supervision guidelines that reference FISC and establish cybersecurity obligations including CSIRT establishment, CISO designation, and periodic security assessments. The Guidelines for Comprehensive Supervision of Major Banks include specific cybersecurity requirements.

System configuration implications:

- Designate a CISO and document the reporting chain
- Establish a CSIRT or equivalent incident response function
- Conduct periodic security assessments (penetration testing, vulnerability scanning)
- Maintain incident response plans with defined escalation procedures
- Report significant incidents to FSA within prescribed timeframes

Resources:

- FSA English portal: https://www.fsa.go.jp/en/

General Enterprise

Cybersecurity Management Guidelines

Issuing body: Ministry of Economy, Trade and Industry (METI) and Information-technology Promotion Agency (IPA)
First published: 2015
Current version: Version 3.0 (March 2023)
Scope: Enterprises with dedicated IT divisions
Status: Voluntary
Update cadence: Major revisions every 2-4 years

The baseline cybersecurity guidelines for Japanese enterprises, structured around:

- **3 principles** for management recognition
- **10 material items** for CISO-level direction

Covers risk assessment, security policy development, supply chain security, incident response, and business continuity.

System configuration implications:

- Document and maintain a cybersecurity policy
- Conduct annual risk assessments covering IT assets and data flows
- Implement multi-factor authentication for administrative access
- Configure backup and recovery procedures with tested restore processes
- Run security training programs for all employees (annual minimum)
- Monitor and manage third-party/vendor access to systems
- Maintain an asset inventory covering hardware, software, and cloud services
- Define and test an incident response plan

Resources:

- English PDF (v3.0): https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v3.0_en.pdf
- METI Cybersecurity portal: https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html

Information Security Guidelines for SMEs

Issuing body: IPA
Scope: Small and medium enterprises
Status: Voluntary
Update cadence: Updated periodically; SECURITY ACTION self-declaration scheme is ongoing

A practical starting point for organizations building baseline security. Includes self-assessment questionnaires and the “Information Security 5 To-dos” covering essential baseline measures.

The SECURITY ACTION self-declaration scheme provides two entry levels:

Level	Requirement
★1	Endorse the “Information Security 5 To-dos”
★2	Complete the IPA self-assessment questionnaire and publish a security policy

These two levels form the foundation for the higher SCS evaluation tiers (★3-★5).

System configuration implications (the 5 To-dos):

- Install and maintain antivirus/endpoint protection on all devices
- Keep all OS and application software updated
- Use strong, unique passwords (enforce via policy and technical controls)
- Restrict access to sensitive data to authorized personnel only
- Guard against social engineering and phishing (training + email filtering)

Resources:

- IPA English portal: https://www.ipa.go.jp/en/index.html

Supply Chain Security

SCS Evaluation Framework (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)

Issuing body: METI and National Cybersecurity Office (NCO)
Establishment policy finalized: March 2026
Target launch: Late FY2026 (★3 and ★4 application acceptance)
Scope: Enterprises in supplier/subcontractor roles within supply chains
Status: Voluntary, but expected to become a de facto procurement requirement — particularly for government contracts and large enterprise supply chains

A tiered evaluation framework that makes an organization’s cybersecurity posture visible to trading partners. Builds on top of IPA’s existing SECURITY ACTION self-declaration scheme (★1, ★2) by adding three higher tiers with progressively stricter evaluation requirements.

Level	Evaluation method	Items	Target
★1	Self-declaration (SECURITY ACTION)	5	All organizations
★2	Self-assessment + policy publication (SECURITY ACTION)	25	All organizations
★3	Self-assessment with security expert confirmation	25	General enterprises
★4	Third-party evaluation by accredited assessor	44	Enterprises handling sensitive data, critical supply chain roles, or high-connectivity environments
★5	To be defined (FY2026 onward)	TBD	Highest assurance level

Evaluation criteria align with NIST CSF 2.0 and cover six domains: governance, supplier management, risk identification, system defense, attack detection, and incident response/recovery.

Key characteristics:

- Evaluation scope covers IT infrastructure (including cloud); OT systems and embedded products are explicitly excluded and covered by separate frameworks
- ★3 emphasizes “explainability” — organizations must maintain evidence that controls operate, not just that they exist on paper
- ★4 adds requirements around breach containment, lateral movement prevention, and business continuity
- Evaluation results are expected to be publicly listed, creating market incentive
- A new “Cyber Security Otasuke-tai Service” (new type) will support SME ★3/★4 certification at accessible cost

System configuration implications (★3):

- Maintain an up-to-date IT asset inventory
- Configure centralized log collection and retention
- Enforce access control with role-based permissions
- Implement endpoint protection across all managed devices
- Document and test backup/recovery procedures
- Maintain evidence of control operation (logs, screenshots, audit reports)

Additional for ★4:

- Implement network segmentation to limit lateral movement
- Deploy intrusion detection/prevention systems (IDS/IPS)
- Conduct regular vulnerability assessments
- Establish business continuity and disaster recovery plans

- Engage accredited third-party assessor for formal evaluation

Comparable international frameworks: UK Cyber Essentials / Cyber Essentials Plus (closest structural analog), US CMMC (similar tiered assessment concept for supply chains)

Resources:

- METI establishment policy (finalized, March 2026): https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html
- METI interim summary (April 2025): https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html
- ★3/★4 requirements and evaluation criteria (Excel): attached to the establishment policy press release above

Government Sector

Common Standards on Cybersecurity Measures for Government Agencies

Issuing body: Cybersecurity Strategic Headquarters (CSHQ) and National Cybersecurity Office (NCO, formerly NISC)
Scope: Government agencies and related entities
Status: Mandatory for government; reference for private sector
Update cadence: Revised when the national cybersecurity strategy is updated

A unified framework defining baseline cybersecurity measures for government entities. Private organizations that contract with government agencies often reference these standards voluntarily.

System configuration implications (for government contractors):

- Meet or exceed the security baselines defined in the Common Standards
- Implement information classification and handling procedures
- Configure systems to support government audit and inspection requirements
- Confirm data residency requirements are met (government data may have Japan-residency obligations)

Resources:

- NISC/NCO English overview: https://www.nisc.go.jp/eng/
- Google Cloud NISC mapping: https://cloud.google.com/security/compliance/nisc

IoT and Product Security

Japan Cyber STAR (JC-STAR)

Issuing body: METI
Launched: March 2025 (STAR-1)
Scope: Consumer and industrial IoT products
Status: Voluntary labeling scheme

A four-tier IoT security labeling scheme harmonized with international standards (ETSI EN 303 645, NISTIR 8425):

Level	Description
STAR-1	Unified baseline for all IoT products
STAR-2	Product category-specific (in development)
STAR-3	Product category-specific (in development)
STAR-4	Product category-specific (in development)

Procurement implications:

- When evaluating IoT devices for client environments, prefer JC-STAR labeled products
- STAR-1 compliance indicates baseline security hygiene (default password changes, firmware update capability, secure communication)
- Include JC-STAR certification status in procurement checklists

Resources:

- METI announcement: https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html

Sector-Specific Guidelines

Healthcare

- **Guidelines on Safety Management of Medical Information Systems** — Ministry of Health, Labour and Welfare (MHLW)
- **Guidelines for Information Processing Service Providers Handling Medical Information** — METI
- **Guidelines on Management of Medical Information by Cloud Service Providers** — Ministry of Internal Affairs and Communications (MIC)

Healthcare clients must comply with all three sets of guidelines when handling medical information in cloud or outsourced environments. Key requirements include patient data encryption, access audit trails, and strict data residency controls.

Critical Infrastructure

The Cybersecurity Policy for Critical Infrastructure Protection defines 15 sectors requiring enhanced security measures:

- Energy
- Telecommunications
- Transportation
- Water services
- Finance (covered separately above)
- Healthcare (covered separately above)
- Government services

- And others

Each sector has its own supplementary guidelines. Critical infrastructure operators should identify their sector designation and review the applicable supplementary requirements.

Space Systems

- **Cybersecurity Guidelines for Commercial Space Systems** (v1.1) — METI

OT/Industrial Control Systems

- **OT Security Guidelines for Semiconductor Device Factories** (draft, 2025) — METI
- **ICSCoE training programs** — IPA Industrial Cyber Security Center

OT environments are explicitly excluded from the SCS Evaluation Framework. Organizations with both IT and OT systems need separate compliance tracks.

Key Organizations

Organization	Role	Website
NCO (National Cybersecurity Office)	National coordination, government standards	https://www.nisc.go.jp/eng/
METI	Industrial sector cybersecurity policy	https://www.meti.go.jp/english/
IPA	Guidelines, tools, training, certifications	https://www.ipa.go.jp/en/
FSA	Financial sector supervision	https://www.fsa.go.jp/en/
FISC	Financial sector security guidelines	https://www.fisc.or.jp/english/
MIC	Telecommunications, cloud security	https://www.soumu.go.jp/english/

Professional Certification

Registered Information Security Specialist (RISS)

Administering body: IPA
Established: October 2016
Status: National qualification

Japan's national qualification for cybersecurity professionals, established under the Act on Facilitation of Information Processing. Relevant when clients require certified security personnel on engagement teams or when advising clients on staff qualifications.

Comparison with International Frameworks

Japanese Framework	Comparable International Standard	Key Difference
FISC Security Guidelines	PCI-DSS + FFIEC (financial sector)	FISC is broader — covers facility security, not just data
METI/IPA Cybersecurity Management Guidelines	NIST CSF, ISO 27001 (governance focus)	Less prescriptive than NIST; focuses on management principles
NISC Common Standards	FedRAMP, government-specific controls	Mandatory for government only; private sector use is voluntary
JC-STAR	ETSI EN 303 645, NISTIR 8425 (IoT)	Harmonized with EU/US standards; mutual recognition possible
SCS Evaluation Framework	UK Cyber Essentials, US CMMC	Newer; builds on existing SECURITY ACTION base; ★3/★4 launching FY2026
IPA SME Guidelines	CIS Controls (basic)	Simpler entry point; SECURITY ACTION scheme adds self-declaration

eSolia Service Alignment

How eSolia service offerings address framework requirements:

Framework Requirement	eSolia Service	Typical Activities
Ongoing monitoring and incident response	TotalSupport	Alert triage, incident escalation, monthly reporting
Security gap assessment	Security Assessment	Framework-specific gap analysis, remediation roadmap
Audit logging and SIEM	M365/Cloud Management	Unified Audit Log configuration, retention policies, alert rules
Access control and identity	M365/Entra ID Management	Conditional access policies, MFA enforcement, role-based access
Employee security training	Training Services	Annual security awareness, phishing simulation
Vulnerability management	TotalSupport + Assessment	Patch management, vulnerability scanning, remediation tracking
SCS ★3/★4 evaluation prep	Security Assessment	Self-assessment support, evidence gathering, expert confirmation
Incident response planning	Consulting	CSIRT establishment, playbook development, tabletop exercises
Business continuity	Consulting + TotalSupport	BCP development, backup verification, DR testing
Network segmentation	Network Management	VLAN configuration, firewall rules, micro-segmentation

Framework Revision Tracking

Framework	Current Version	Last Checked	Next Expected Update
FISC Security Guidelines	13th Edition (Nov 2025)	2026-04-15	~2027-2028
FSA Supervision Guidelines	Current	2026-04-15	Revised periodically
METI Cybersecurity Management	v3.0 (Mar 2023)	2026-04-15	v4.0 expected ~2026-2027
IPA SME Guidelines	Current	2026-04-15	Updated periodically
SCS Evaluation Framework	Establishment policy (Mar 2026)	2026-04-15	★3/★4 launch late FY2026
NISC/NCO Common Standards	Current	2026-04-15	Follows national strategy cycle
JC-STAR	STAR-1 (Mar 2025)	2026-04-15	STAR-2-4 in development

Organizational change note: In July 2025, NISC (National center of Incident readiness and Strategy for Cybersecurity) was reorganized as the NCO (National Cybersecurity Office) following the Active Cyber Defense Act. References to “NISC” in older documents now point to NCO.

Notes

- Most Japanese frameworks are **voluntary** but carry significant weight — deviation requires justification during audits or regulatory review
- English translations exist for major frameworks but may lag behind the Japanese versions by months
- The SCS Evaluation Framework (★3/★4) targets late FY2026 for application acceptance; evaluation guides and implementation examples are expected around autumn 2026; ★5 criteria will be developed separately in FY2026 and beyond
- When multiple frameworks apply (e.g., a financial institution that is also part of a supply chain), the most restrictive requirements from each framework take precedence

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

日本のサイバーセキュリティフレームワークとガイドライン

2026 年 4 月 16 日

目次

クイックリファレンス: 適用フレームワーク一覧

クライアントの業種と規模に基づき、該当する日本のサイバーセキュリティフレームワークを特定するためのマトリクスです。★（星）マークはサプライチェーンセキュリティの**成熟度ティア**を示します。★1 と★2 は IPA の「SECURITY ACTION」制度に基づく自己宣言で、★3 以上は段階的に厳格な評価が求められます。詳細は「サプライチェーンセキュリティ」セクションを参照してください。

クライアント区分	主要フレームワーク	補助的/任意
銀行、証券、保険	FISC 安全対策基準 + 金融庁監督指針	サイバーセキュリティ経営ガイドライン（経産省）
大企業（金融以外）	サイバーセキュリティ経営ガイドライン（経産省/IPA）	SCS 評価制度
中小企業（約 300 名以下）	中小企業の情報セキュリティ対策ガイドライン（IPA）、SECURITY ACTION	SCS ★3（サプライチェーンに属する場合）
官公庁	政府統一基準（NISC/NCO）	分野別ガイドライン
政府調達先/下請け	サイバーセキュリティ経営ガイドライン + SCS ★3/★4	政府統一基準（参考）
医療機関	厚労省 医療情報安全管理ガイドライン	サイバーセキュリティ経営ガイドライン
IoT 製品メーカー	JC-STAR ラベリング	経産省 OT/ICS ガイドライン
重要インフラ事業者	分野別重要インフラガイドライン	サイバーセキュリティ経営ガイドライン
サプライチェーンに属する企業全般	SCS 評価制度（★3 以上）	サイバーセキュリティ経営ガイドライン

判断フロー:

1. 規制業種（金融、医療、官公庁、重要インフラ）に該当するか。該当する場合は業種別フレームワークから着手する。
2. 大企業や官公庁のサプライチェーンの一部か。該当する場合は SCS 評価制度を追加する。
3. その他の企業は、サイバーセキュリティ経営ガイドラインをベースラインとする。
4. セキュリティ対策をこれから始める中小企業は、IPA 中小企業向けガイドラインと SECURITY ACTION 自己宣言から着手する。

金融セクター

FISC 安全対策基準

発行機関: 金融情報システムセンター（FISC）
初版発行: 1985 年
現行版: 第 13 版（2025 年 11 月）
対象: 銀行、金融機関

位置付け: 任意だが、金融庁監督指針で参照されており事実上の必須基準
改訂頻度: 2〜3 年ごとに大規模改訂。必要に応じて補足版を発行

日本の金融機関向けとして最も包括的なセキュリティフレームワーク。4 つの領域にわたる 300 以上の管理策で構成されている。

- 技術的対策
- 運用的対策
- 設備的対策
- 監査的対策

システム設定への影響:

- 全システムで包括的な監査ログを有効化する（M365 統合監査ログ、データベース監査、ネットワーク機器ログ）
- 保存時および通信時の暗号化を強制する（TLS 1.2 以上、ディスク暗号化）
- インターネット接続ゾーン、内部ゾーン、管理ゾーン間のネットワークセグメンテーションを実装する
- ロールベースの権限と最小権限の原則に基づくアクセス制御を設定する
- クライアントの FISC 準拠ポリシーで定められた期間、ログを保持する（ログ種類により 1〜7 年）
- 不正アクセス試行に対する自動アラートを設定する
- すべてのシステム変更を承認証跡付きで記録する

リソース:

- FISC 英語ポータル: https://www.fisc.or.jp/english/
- AWS FISC 準拠: https://aws.amazon.com/compliance/fisc/
- Google Cloud FISC マッピング: https://cloud.google.com/security/compliance/fisc-japan
- Microsoft FISC 準拠: https://learn.microsoft.com/en-us/compliance/regulatory/offering-fisc-japan

金融庁 総合的な監督指針

発行機関: 金融庁（FSA）
対象: 銀行、証券会社、保険会社
改訂頻度: 随時改訂。最新版は FSA ポータルで確認

FISC を参照しつつ、CSIRT 設置、CISO 任命、定期的なセキュリティ評価などのサイバーセキュリティ義務を定める業種別監督指針。主要行等向け総合的な監督指針には具体的なサイバーセキュリティ要件が含まれている。

システム設定への影響:

- CISO を任命し、報告体制を文書化する
- CSIRT または同等のインシデント対応機能を設置する
- 定期的なセキュリティ評価を実施する（ペネトレーションテスト、脆弱性スキャン）
- エスカレーション手順を含むインシデント対応計画を維持する
- 重大インシデントは所定の期限内に金融庁へ報告する

リソース:

- FSA 英語ポータル: https://www.fsa.go.jp/en/

一般企業

サイバーセキュリティ経営ガイドライン

発行機関: 経済産業省（METI）、独立行政法人情報処理推進機構（IPA）
初版発行: 2015 年
現行版: Ver 3.0（2023 年 3 月）
対象: 専任 IT 部門を持つ企業
位置付け: 任意
改訂頻度: 2〜4 年ごとに大規模改訂

日本企業向けのサイバーセキュリティ基準で、以下の構成で整理されている。

- 経営者が認識すべき **3 原則**
- CISO 等が指示すべき**重要 10 項目**

リスク評価、セキュリティポリシー策定、サプライチェーンセキュリティ、インシデント対応、事業継続を網羅している。

システム設定への影響:

- サイバーセキュリティポリシーを策定し、維持する
- IT 資産とデータフローを対象とした年次リスク評価を実施する
- 管理者アクセスに多要素認証を導入する
- 復旧テスト済みのバックアップ/リカバリ手順を設定する
- 全従業員向けセキュリティ研修プログラムを実施する（年 1 回以上）
- サードパーティ/ベンダーのシステムアクセスを監視・管理する
- ハードウェア、ソフトウェア、クラウドサービスを網羅した資産台帳を維持する
- インシデント対応計画を策定し、テストする

リソース:

- 英語版 PDF（v3.0）: https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v3.0_en.pdf
- 経産省サイバーセキュリティポータル: https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html

中小企業の情報セキュリティ対策ガイドライン

発行機関: IPA
対象: 中小企業
位置付け: 任意
改訂頻度: 随時更新。SECURITY ACTION 自己宣言制度は継続運用中

セキュリティ対策の基盤構築を始める組織向けの実用的な出発点。自己診断シートと「情報セキュリティ 5 か条」で基本的なベースライン対策をカバーしている。

SECURITY ACTION 自己宣言制度には 2 つのエントリーレベルがある。

レベル	要件
★1	「情報セキュリティ 5 か条」に取り組むことを宣言
★2	IPA 自己診断シートを完了し、セキュリティポリシーを公開

この 2 段階が、上位の SCS 評価ティア（★3〜★5）の基盤となる。

システム設定への影響（5 か条）：

- 全端末にウイルス対策/エンドポイント保護を導入・維持する
- すべての OS とアプリケーションソフトウェアを最新の状態に保つ
- 強固でユニークなパスワードを使用する（ポリシーと技術的制御で強制）
- 機密データへのアクセスを認可された担当者のみに制限する
- ソーシャルエンジニアリングやフィッシングに対する防御を行う（研修 + メールフィルタリング）

リソース:

- IPA 英語ポータル: https://www.ipa.go.jp/en/index.html

サプライチェーンセキュリティ

SCS 評価制度（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）

発行機関: 経済産業省（METI）、国家サイバーセキュリティ局（NCO）
制度構築方針策定: 2026 年 3 月
運用開始予定: 2026 年度後半（★3 および★4 の申請受付開始）
対象: サプライチェーンにおけるサプライヤー/下請け企業
位置付け: 任意だが、調達における事実上の要件化が見込まれる。特に政府調達および大企業のサプライチェーンにおいて顕著

取引先に対してサイバーセキュリティ対策状況を可視化する段階的評価制度。IPA の既存の SECURITY ACTION 自己宣言制度（★1、★2）の上位に、より厳格な評価要件を持つ 3 つの上位ティアを追加する。

レベル	評価方法	項目数	対象
★1	自己宣言（SECURITY ACTION）	5	全組織
★2	自己評価 + ポリシー公開（SECURITY ACTION）	25	全組織
★3	セキュリティ専門家の確認付き自己評価	25	一般企業
★4	認定評価者による第三者評価	44	機密データ取扱、重要サプライチェーン、高接続性環境の企業
★5	未定（2026 年度以降）	未定	最高保証レベル

評価基準は NIST CSF 2.0 に整合し、6 つの領域をカバーする。ガバナンス、サプライヤー管理、リスク特定、システム防御、攻撃検知、インシデント対応/復旧。

主な特徴:

- 評価範囲は IT インフラ（クラウド含む）を対象とする。OT システムと組み込み製品は明示的に除外され、別のフレームワークでカバーされる

- ★3 は「説明可能性」を重視する。管理策が書面上存在するだけでなく、実際に運用されている証拠の保持が求められる
- ★4 は侵害封じ込め、横展開防止、事業継続に関する要件が追加される
- 評価結果は公開リスト化される見込みで、市場インセンティブが生まれる
- 新たな「サイバーセキュリティお助け隊サービス」（新類型）が、中小企業の★3/★4 認証を手頃なコストで支援する予定

システム設定への影響（★3）：

- 最新の IT 資産台帳を維持する
- 集約的なログ収集と保持を設定する
- ロールベースの権限によるアクセス制御を強制する
- 管理対象の全端末にエンドポイント保護を導入する
- バックアップ/リカバリ手順を文書化し、テストする
- 管理策の運用証拠を保持する（ログ、スクリーンショット、監査報告書）

★4 の追加要件:

- 横展開を制限するネットワークセグメンテーションを実装する
- 侵入検知/防止システム（IDS/IPS）を導入する
- 定期的な脆弱性評価を実施する
- 事業継続計画および災害復旧計画を策定する
- 認定された第三者評価者による正式な評価を受ける

比較可能な国際フレームワーク: UK Cyber Essentials / Cyber Essentials Plus（構造的に最も近い）、US CMMC（サプライチェーン向けの段階的評価として類似の概念）

リソース:

- 経産省 制度構築方針（2026 年 3 月策定）: https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html
- 経産省 中間整理（2025 年 4 月）: https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html
- ★3/★4 の評価基準と要件（Excel）: 上記制度構築方針のプレスリリースに添付

政府セクター

政府機関等のサイバーセキュリティ対策のための統一基準

発行機関: サイバーセキュリティ戦略本部（CSHQ）、国家サイバーセキュリティ局（NCO、旧 NISC）
対象: 政府機関および関連団体
位置付け: 政府機関には義務。民間は参考
改訂頻度: 国家サイバーセキュリティ戦略の改定に合わせて改訂

政府機関向けの統一的なサイバーセキュリティ対策基準。政府と取引のある民間企業が、自社のセキュリティ対策の参考として任意に採用するケースもある。

システム設定への影響（政府受託業者向け）：

- 統一基準で定められたセキュリティベースラインを満たすか、それ以上を確保する

- 情報分類と取扱手順を整備する
- 政府の監査・検査要件に対応できるようシステムを設定する
- データ所在地要件を確認する（政府データには日本国内保管義務がある場合がある）

リソース:

- NISC/NCO 英語概要: https://www.nisc.go.jp/eng/
- Google Cloud NISC マッピング: https://cloud.google.com/security/compliance/nisc

---

IoT・製品セキュリティ

JC-STAR（Japan Cyber Security Testing and Rating）

発行機関: 経済産業省（METI）
運用開始: 2025 年 3 月（STAR-1）
対象: 民生用および産業用 IoT 製品
位置付け: 任意のラベリング制度

国際規格（ETSI EN 303 645、NISTIR 8425）と整合した 4 段階の IoT セキュリティラベリング制度。

レベル	概要
STAR-1	全 IoT 製品共通のベースライン
STAR-2	製品カテゴリ別（策定中）
STAR-3	製品カテゴリ別（策定中）
STAR-4	製品カテゴリ別（策定中）

調達への影響:

- クライアント環境向け IoT 機器を評価する際、JC-STAR ラベル取得製品を優先する
- STAR-1 準拠は、基本的なセキュリティ対策（デフォルトパスワードの変更、ファームウェア更新機能、安全な通信）を示す
- 調達チェックリストに JC-STAR 認証状況を含める

リソース:

- 経産省発表: https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html

---

分野別ガイドライン

医療

- **医療情報システムの安全管理に関するガイドライン**（厚生労働省）
- **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**（経済産業省）
- **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**（総務省）

医療クライアントがクラウドまたは外部委託環境で医療情報を取り扱う場合、3 つのガイドラインすべてへの準拠が必要となる。主な要件として、患者データの暗号化、アクセス監査証跡、厳格なデータ所在地管理がある。

重要インフラ

重要インフラの情報セキュリティ対策に係る行動計画では、強化されたセキュリティ対策を必要とする 15 分野を定めている。

- エネルギー
- 情報通信
- 交通
- 水道
- 金融（上記で別途記載）
- 医療（上記で別途記載）
- 行政サービス
- その他

各分野に固有の補足ガイドラインがある。重要インフラ事業者は自社の分野指定を確認し、該当する補足要件を精査する必要がある。

宇宙システム

- **民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン**（v1.1）（経済産業省）

OT/産業制御システム

- **半導体製造装置工場における OT セキュリティガイドライン**（案、2025 年）（経済産業省）
- **ICSCoE 研修プログラム**（IPA 産業サイバーセキュリティセンター）

OT 環境は SCS 評価制度の対象から明示的に除外されている。IT と OT の両システムを持つ組織は、別々のコンプライアンストラックが必要となる。

主要組織

組織	役割	ウェブサイト
NCO（国家サイバーセキュリティ局）	全体調整、政府基準	https://www.nisc.go.jp/eng/
経済産業省（METI）	産業分野のサイバーセキュリティ政策	https://www.meti.go.jp/english/
IPA（情報処理推進機構）	ガイドライン、ツール、研修、資格	https://www.ipa.go.jp/en/
金融庁（FSA）	金融分野の監督	https://www.fsa.go.jp/en/
FISC（金融情報システムセンター）	金融分野のセキュリティ基準	https://www.fisc.or.jp/english/
総務省（MIC）	情報通信、クラウドセキュリティ	https://www.soumu.go.jp/english/

専門資格

情報処理安全確保支援士（RISS）

管轄機関: IPA
創設: 2016 年 10 月
位置付け: 国家資格

情報処理の促進に関する法律に基づき創設された、サイバーセキュリティ専門人材の国家資格制度。クライアントが認定セキュリティ人材をチームに求める場合や、スタッフの資格要件について助言する際に関連する。

国際フレームワークとの比較

日本のフレームワーク	比較対象となる国際基準	主な違い
FISC 安全対策基準	PCI-DSS + FFIEC（金融分野）	FISC はより包括的で、データだけでなく設備セキュリティもカバー
サイバーセキュリティ経営ガイドライン（経産省/IPA）	NIST CSF、ISO 27001（ガバナンス中心）	NIST ほど規範的ではなく、経営原則に重点を置く
政府統一基準（NISC/NCO）	FedRAMP、政府固有の管理策	政府機関のみ義務。民間の利用は任意
JC-STAR	ETSI EN 303 645、NISTIR 8425（IoT）	EU/US 規格と整合。相互承認の可能性あり
SCS 評価制度	UK Cyber Essentials、US CMMC	新しい制度。既存の SECURITY ACTION を基盤とし、★3/★4 は 2026 年度開始予定
IPA 中小企業向けガイドライン	CIS Controls（基本）	よりシンプルな入口。SECURITY ACTION 制度で自己宣言を追加

イソリアサービスとの対応

フレームワーク要件に対するイソリアのサービス提供。

フレームワーク要件	イソリアサービス	主な活動内容
継続的な監視とインシデント対応	TotalSupport	アラートトリアージ、インシデントエスカレーション、月次報告
セキュリティギャップ評価	セキュリティアセスメント	フレームワーク別ギャップ分析、改善ロードマップ
監査ログと SIEM	M365/クラウド管理	統合監査ログ設定、保持ポリシー、アラートルール
アクセス制御と ID 管理	M365/Entra ID 管理	条件付きアクセスポリシー、MFA 適用、ロールベースのアクセス
従業員セキュリティ研修	研修サービス	年次セキュリティ意識向上、フィッシングシミュレーション
脆弱性管理	TotalSupport + アセスメント	パッチ管理、脆弱性スキャン、対応状況追跡
SCS ★3/★4 評価準備	セキュリティアセスメント	自己評価支援、証拠収集、専門家確認
インシデント対応計画策定	コンサルティング	CSIRT 設置、プレイブック作成、机上演習
事業継続	コンサルティング + TotalSupport	BCP 策定、バックアップ検証、DR テスト
ネットワークセグメンテーション	ネットワーク管理	VLAN 設定、ファイアウォールルール、マイクロセグメンテーション

フレームワーク改訂状況

フレームワーク	現行版	最終確認日	次回改訂見込み
FISC 安全対策基準	第 13 版（2025 年 11 月）	2026-04-15	2027～2028 年頃
金融庁監督指針	現行版	2026-04-15	随時改訂
サイバーセキュリティ経営ガイドライン	v3.0（2023 年 3 月）	2026-04-15	v4.0 は 2026～2027 年頃
IPA 中小企業向けガイドライン	現行版	2026-04-15	随時更新
SCS 評価制度	制度構築方針（2026 年 3 月）	2026-04-15	★3/★4 は 2026 年度後半開始予定
政府統一基準（NISC/NCO）	現行版	2026-04-15	国家戦略改定サイクルに準ずる
JC-STAR	STAR-1（2025 年 3 月）	2026-04-15	STAR-2～4 策定中

組織変更に関する注記: 2025 年 7 月、能動的サイバー防御法の施行に伴い、NISC（内閣サイバーセキュリティセンター）は NCO（国家サイバーセキュリティ局）に改組された。旧文書における「NISC」への言及は NCO を指す。

備考

- 日本のフレームワークの大半は**任意**だが、実質的な拘束力を持つ。監査や規制審査の際、不採用には相応の説明が必要となる
- 主要フレームワークの英語翻訳は存在するが、日本語版に対して数か月の遅延がある場合がある
- SCS 評価制度（★3/★4）は 2026 年度後半に申請受付開始を目標としている。評価ガイドと実施例は 2026 年秋頃の公開を見込む。★5 の基準は 2026 年度以降に別途策定予定
- 複数のフレームワークが適用される場合（例: サプライチェーンに属する金融機関）、各フレームワークの最も厳格な要件が優先される

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