

(仮訳)

協力覚書 (MoC)

日本国経済産業省およびシンガポール共和国サイバーセキュリティ庁

IoT セキュリティ制度の相互承認

(JC-STAR★ 1 および シンガポール・CLS レベル 1)

日本国経済産業省およびシンガポール共和国サイバーセキュリティ庁 (以下、単独では「参加者」、
総称して「両参加者」という。)

国際的にサイバー空間の安全性を高め、全体的なサイバー衛生水準を向上させることを目的とし
て、

日本およびシンガポール共和国におけるそれぞれのモノのインターネット (以下「IoT」という)
機器のサイバーセキュリティ制度の相互承認に関する効果的な仕組みの構築に向けて取り組む
ため、

両参加者は、シンガポール・サイバーセキュリティ・ラベリング制度および JC-STAR に関する
相互承認に向けた協力を強化する意向を有し、

以下のとおり合意する。

第 1 条

(目的)

両参加者は、それぞれの権限および責任の範囲内で、かつ自国の法令を遵守し、適切な範囲にお

(仮訳)

いて、本協力覚書（以下「本 MoC」という。）に定める事項に基づき、IoT サイバーセキュリティ分野における協力を強化し、両参加者の IoT サイバーセキュリティ制度の相互承認を促進することを旨とする。

第 2 条

(定義)

本 MoC において使用される用語の定義は、以下のとおりとする。

- **「適合性評価手続」**

シンガポールにおいては、IoT 製品が CLS の要件に適合しているかを判断する手続をいい、日本においては、IoT 製品が JC-STAR（セキュリティ要件適合評価）の要件に適合しているかを判断する手続をいう。

- **「サイバーセキュリティ制度」**

日本の場合は JC-STAR 制度を、シンガポールの場合はシンガポール CLS をいう。

- **「IoT 製品」**

日本の場合は日本のサイバーセキュリティ制度の対象となる製品をいい、シンガポールの場合は CLS の対象となる製品をいう。

- **「ラベル」**

日本の場合は JC-STAR 制度に基づき発行される日本のサイバーセキュリティ・ラベルをいい、シンガポールの場合は CLS に基づき発行されるラベルをいう。

(仮訳)

- 「要件」

日本の場合は JC-STAR★1 に定められた該当製品カテゴリに適用されるセキュリティ要件をいい、シンガポールの場合は CLS レベル 1 に定められたセキュリティ要件をいう。

第 3 条

(ラベルの相互承認)

1. 各参加者は、相手方の IoT サイバーセキュリティ制度を信頼性のある制度として認識する。
2. 各参加者は、以下のとおり、相手方のラベルの承認に努める。
 - a. 日本の適合性評価手続に基づき有効な JC-STAR ラベルを取得した IoT 製品は、当該ラベルを提示することにより、シンガポール共和国サイバーセキュリティ庁が定めるシンガポールのサイバーセキュリティ制度における CLS レベル 1 ラベル取得のための簡素化された申請手続を受けることができる (附属書 A 及び附属書 B 参照)。
 - b. シンガポールの適合性評価手続に基づき有効な CLS ラベルを取得した IoT 製品は、当該ラベルを提示することにより、日本の独立行政法人情報処理推進機構 (IPA) が定める日本のサイバーセキュリティ制度における JC-STAR★1 ラベル取得のための簡素化された申請手続を受けることができる (附属書 A 参照)。
3. 本条に基づく相互承認の目的において、
 - a. シンガポールのサイバーセキュリティ制度 (CLS) のすべてのレベルは、CLS レベル 1 と同等とみなされ、承認される。

(仮訳)

- b. 日本のサイバーセキュリティ制度 (JC-STAR) のすべてのレベルは、JC-STAR★1 と同等とみなされ、承認される。
4. 明確化のため、本条は、第三国との他の相互承認取決めに基づき発行された消費者向け IoT 製品のラベルには適用されない。
5. 一方の参加者が、他方の参加者による IoT 製品のラベリングの判断に不服がある場合、両参加者は相互協議を通じて解決に努め、必要に応じて関連情報を共有する。協議により解決できない場合、当該 IoT 製品のラベルは本条第 2 項に基づく承認の対象とはならない。
6. 各参加者は、本条第 2 項に基づき相手方の IoT 製品に発行されたラベルを取り消した場合、当該措置を講じてから 30 営業日以内に相手方に通知する。
7. 本 MoC の範囲内で、日本またはシンガポールの適合性評価手続に基づき発行されたラベルを有する IoT 製品は、完全に承認されるものとする。この承認は、新たに発行されたラベルおよび有効性を維持している既存のラベルの双方に適用され、当該 IoT 製品が定められた基準および要件を満たしていることを条件とする。

第 4 条

(協力の形態)

1. 両参加者は、適用される標準の策定、IoT 製品に対するサイバー脅威および攻撃手法、要件、その他 IoT サイバーセキュリティ制度に関する慣行について、適切な範囲で情報交換およびベストプラクティスの共有を行うことができる。

(仮訳)

2. 両参加者は、消費者向け IoT サイバーセキュリティ制度、関連法令および要件に関する最新情報を共有するため、少なくとも年 1 回の協議を行うよう努める。
3. 本 MoC の文脈において、両参加者は、適切な場合には、IoT サイバーセキュリティ制度のさらなる発展に向けた協力を行うよう努める。
4. 本 MoC に基づく情報交換、検証、証拠提供その他の活動のために発行される関連文書が英語以外で作成されている場合には、必要に応じて英語翻訳を添付するものとする。

第 5 条

(資金および資源)

本 MoC に基づいて実施される協力活動は、各参加者の当該時点における資金および資源の利用可能性に従うものとする。両参加者が書面で別途合意しない限り、各参加者は、本 MoC の枠組み内で実施されるすべての活動およびプログラムに関する費用および経費を、それぞれ自ら負担するものとし、各自の予算措置に従う。

第 6 条

(秘密保持)

1. 両参加者は、本 MoC の運用において相手方から受領した文書、情報およびその他のデータについて、自国の法令または国際的義務により認められる範囲内で、秘密および機密を保持する。

(仮訳)

2. 両参加者は、本 MoC に基づき提供または生成された情報が、その提供目的にのみ使用され、相手方の事前の書面による同意なく第三者に開示されないよう、合理的かつ合法的な措置を講じる。
3. 本 MoC に基づき提供または生成されたすべての情報は、両参加者の国内法令または国際的義務に従って保護、使用、送信、保管および取り扱われるものとする。
4. 本条の規定は、本 MoC が終了した後も引き続き尊重される。

第 7 条

(紛争解決)

本 MoC の解釈または実施に関して生じるいかなる紛争または相違についても、両参加者は、国内外の裁判所または第三者に付託することなく、相互協議により、友好的かつ誠意をもって解決するものとする。

本条の規定は、本 MoC が終了した後も引き続き尊重される。

第 8 条

(国内法および国際法との関係)

1. 本 MoC はいずれの参加者に対しても、国内法または国際法上の法的拘束力のある権利または義務を創設するものではなく、その意図も有しない。
2. 本 MoC は、国際連合憲章第 102 条に基づく登録の対象とはならない。

(仮訳)

3. 本 MoC またはこれに基づくいかなる行為も、両参加者が締約国である既存の国際協定または条約に基づく権利および義務に影響を及ぼすものではない。

第 9 条

(修正)

本 MoC は、両参加者の書面による相互の同意により、いつでも修正することができる。当該修正は、両参加者が定める日から効力を生じ、本 MoC の不可欠な一部を構成するものとする。

第 10 条

(参加者の権限の留保)

1. 本 MoC のいかなる規定も、消費者の安全を確保するために適切と考える保護水準を、立法、規制または行政措置により決定する各参加者の権限を制限するものと解釈されない。
2. また、本 MoC のいかなる規定も、IoT 製品が以下のいずれかに該当すると判断した場合に、各参加者が適切かつ即時の措置を講じる権限を制限するものと解釈されない。
 - a. 人の健康または安全を害する場合
 - b. 自国の法令に適合しない場合
 - c. 国家安全保障を損なう場合
 - d. その他、要件を満たさない場合

(仮訳)

第 11 条

(最終規定)

1. 両参加者は、本 MoC に基づく責任を履行するために、適切な措置を講じる。
2. 本 MoC は **2026 年 6 月 1 日**に効力を生じ、当初 **3 年間有効**とする。当初期間満了後は、いずれかの参加者が第 3 項に従って終了させない限り、**3 年ごとに自動更新**される。
3. いずれの参加者も、いつでも本 MoC を終了させることができる。終了を希望する参加者は、終了予定日の **6 か月前までに**書面で相手方に通知するものとする。本 MoC の終了に際しては、未処理事項の取扱いについて両参加者が協議する。
4. 第三者との契約上の義務は、本 MoC の終了によって影響を受けない。
5. 本 MoC に記載された事項は、両参加者間で到達した合意の全体を構成する。

本 MoC は、**2026 年 3 月 18 日**に日本において、英語により、同一内容の原本 2 通が署名された。

日本国経済産業省の名において：

シンガポールサイバーセキュリティ庁

の名において：

井野 俊郎

ラハユ・マザム

経済産業副大臣

デジタル開発・情報省 国务大臣兼保健省

経済産業省

国务大臣

日本

シンガポール

(仮訳)

附属書 A

一般 IoT に関する日本およびシンガポールの制度要件の同等性

表 A-1

日本の JC-STAR★ 1 要件とシンガポール CLS レベル 1 要件の適合状況

日本の JC-STAR★ 1 要件	シンガポール CLS レベル 1 要件の適合状況
適合要件番号 1	該当なし
適合要件番号 2	完全適合
適合要件番号 3	完全適合
適合要件番号 4	完全適合
適合要件番号 5	完全適合
適合要件番号 6	一部適合 ※JC-STAR への適合性評価が必要
適合要件番号 7	完全適合
適合要件番号 8	完全適合
適合要件番号 9	一部適合 ※JC-STAR への適合性評価が必要
適合要件番号 10	完全適合
適合要件番号 11	該当なし
適合要件番号 12	該当なし

(仮訳)

適合要件番号 13	該当なし
適合要件番号 14	該当なし
適合要件番号 15	該当なし
適合要件番号 16	一部適合 ※JC-STAR への適合性評価が必要

表 A-2

シンガポール CLS レベル 1 要件と日本の JC-STAR★ 1 要件の適合状況

シンガポール CLS レベル 1 要件	日本の JC-STAR★ 1 要件の適合状況
規定 5.1-1	完全適合
規定 5.1-2	完全適合
規定 5.1-3	完全適合
規定 5.1-4	完全適合
規定 5.1-5	完全適合
規定 5.2-1	完全適合
規定 5.3-2	完全適合
規定 5.3-3	完全適合
規定 5.3-7	一部適合

(仮訳)

	※CLS への適合性評価が必要
規定 5.3-8	完全適合
規定 5.3-10	完全適合
規定 5.3-13	完全適合
規定 5.3-16	完全適合

附属書 B

ホームゲートウェイの追加的な要件に関する日本およびシンガポールの制度要件の同等性

シンガポール CLS レベル 1 要件	日本の JC-STAR★ 1 要件の適合状況
規定 5.3-1	完全適合
規定 7.3-1	一部適合 ※CLS への適合性評価が必要
規定 7.3-4	該当なし
規定 5.3-6	該当なし
規定 7.3-6	該当なし
規定 7.3-7	一部適合 ※CLS への適合性評価が必要
規定 5.3-9	完全適合