

サイバーセキュリティ関連サービス

概要・サービス

お問い合わせ・お申し込み

概要・サービス



近年、インターネットやスマートフォンをはじめとしたモバイル端末の普及や、AI・クラウドサービス・IoT機器の浸透などにより、社会、ビジネス、消費者間において、世界的なデジタル化が加速しています。一方で、こうしたデジタル化に伴う攻撃の起点の増加、サイバー攻撃の多様化、高度化、巧妙化により、サイバーセキュリティ対策の重要性が高まっています。

サイバー攻撃を受けた場合、金銭的被害だけでなく、人命やビジネス、社会的信用への莫大な損害が考えられるため、あらゆる産業・企業が攻撃の対象となるなか、すべての企業にとってサイバーセキュリティ対策の推進は急務だといえます。

また、EU（欧州）における、サイバーセキュリティ法に基づく「サイバーセキュリティ認証制度」創設の動きや、サイバーレジリエンス法（CRA）、RE指令（無線指令）、NIS2指令、機械指令（機械規則）、AI法案など、米国や中国をはじめとした世界各国でのサイバーセキュリティに関する法規制、規格開発

ル市場展開をサポートすることはもちろん、お客さまの社会的信頼、価値の向上を支援してまいります。

概要

● サイバーセキュリティ関連の主な法規・規格の例

当機構は、国際規格、各国規格に基づく適合性評価、IECEE CB証明書取得および提携機関プライベート認証等の海外認証取得の申請代行業務を行うほか、ギャップ分析、研修サービスなどの技術相談を承ります。以下は、サイバーセキュリティ関連の主な法規・規格と対象となる製品・サービスの一例です。その他の規格および製品、サービスの対象・非対象については、法または規格の原文をご参照ください。また、表以外の規格に関する評価についても対応可能な場合がございますので、お気軽にお問い合わせください。

● 主な法律や制度

サイバーセキュリティ関連の主な法律や制度	対象となる製品・サービスの一例
欧州	
サイバーレジリエンス法（EU Cyber Resilience Act: CRA）	欧州市場に上市するデジタル要素を含む製品
RE指令－サイバーセキュリティ条項（Radio equipment directive（RED）、欧州無線機器指令、無線指令）	インターネットにつながるすべての無線通信機器、無線装置、無線設備※ ¹ ※ ¹ 無線モジュールを含む
機械規則	機械およびその関連製品、半完成機械類（例：加工機械、安全を確保する論理ユニットなど）
英国 PSTI法	インターネットもしくはネットワークにつながる製品※ ² （例：スマートフォン、スマートTV、スマート家電など） ※ ² 自動車、医療機器、産業用制御機器などは対象外

米国	
The U.S. Cyber Trust Mark	消費者向けのインターネット接続デバイス（IoT製品）
インド	
インド電気通信セキュリティ保証要件 （Indian Telecom Security Assurance Requirements：ITSARs）	IPルーターやWi-Fi CPEなど
中国	
中国サイバーセキュリティ法第23条	ネットワーク重要設備およびネットワークセキュリティ専用製品
シンガポール	
サイバーセキュリティ・ラベリング制度 （Cybersecurity Labelling Scheme; CLS）	IoT機器や医療機器
日本	
セキュリティ要件適合評価及びラベリング制度 （JC-STAR）	インターネットプロトコル（IP）を使用したデータの送受信機能を持ち、直接・間接を問わず、インターネットにつながる（可能性がある／否定できない）機器
医薬品医療機器等法	医療機器

● **主な規格**

サイバーセキュリティ関連の主な規格（規格の発行年は省略）	対象となる製品・サービスの一例
国際	

IEC 62443シリーズ： IEC 62443-2-4 IEC 62443-3-3 IEC 62443-4-1 IEC 62443-4-2	プラント・工場などに使用される、産業オートメーションおよび制御システム（IACS）の、サービスプロバイダ（統合または保守サービスを行う組織） コンポーネントを組み合わせたシステム システムに使用される、PLC・HMI・センサー類などのコンポーネントやサブシステム
欧州	
ETSI EN 303 645	消費者向けIoT※3機器（例：ネットワークカメラ・スマートTVなどのスマート家電をはじめとしたインターネットに接続される機器） ※3 Internet of Things：モノのインターネット
EN 18031-1	EN 18031-1: インターネットに接続される無線機器
EN 18031-2	EN 18031-2: ユーザーデータを処理する無線機器 （例：子ども向けデバイス、玩具、ウェアラブルデバイス）
EN 18031-3	EN 18031-3: 仮想通貨や金銭的価値を扱う無線機器
米国	
NIST SP800-53	情報システム （例：汎用コンピューティングシステム、サイバーフィジカルシステム、クラウドシステム、モバイルシステム、産業用制御システム、IoT機器など）
NIST IR 8425	消費者向けIoT製品 （例：Wi-Fiやイーサネット機能をネットワークインターフェースに持つような製品）
中国	

GB 40050	重要なネットワーク機器 (例：ルーター交換機、サーバー〈ラック式〉、PLC)
日本	
JIS T 81001-5-1 / IEC 81001-5-1	医療機器に組み込むソフトウェアを含むヘルスソフトウェア (例：医療機器の一部としてのソフトウェアなど)

サービス一覧

サービス一覧

制度に基づく評価サービス

技術相談サービス

国際認証サービス

制度に基づく評価サービス

● IECCE CB証明

IECCE CB証明（サイバーセキュリティ分野）

● 当機構のサービスの特色

日本国内で完結する『日本語による適合性評価サービス』。

日本国内で評価が完了するため、評価および認証のプロセスに必要な機密事項を海外に提出する必要はありません。

証明書取得後も、改版や維持に関するサポートを国内で受けられるため、長期的なパートナーシップが期待できます。

● CB証明書を発行できる規格

IEC 62443-2-4:2023

産業用オートメーション及び制御システムのセキュリティ 第2-4部
IACSサービスプロバイダに対するセキュリティプログラム要求事項

IEC 62443-3-3:2013

産業用通信ネットワーク ネットワーク及びシステムセキュリティ 第3-3部
システムセキュリティ 要求事項及びセキュリティレベル

IEC 62443-4-1:2018

産業用オートメーション及び制御システムのセキュリティ 第4-1部
安全な製品開発ライフサイクル要求事項

IEC 62443-4-2:2019

産業用オートメーション及び制御システムのセキュリティ 第4-2部
IACSコンポーネントの技術的セキュリティ 要求事項

ETSI EN 303 645:2020

欧州電気通信標準化協会（ETSI）民生用 IoT 機器のサイバーセキュリティ
ベースライン要件

IECEE CB証明の詳細

● 技術文書（欧州規則・指令対応）における適合性評価レポート

技術文書（欧州規則・指令対応）における適合性評価レポート

● 当機構のサービスの特色

CEマークに必要な技術文書（technical document）に活用できる適合性評価レポートを提供します。

お客さまのご要望に応じて、最小単位での要件に対する評価を行うことができます。

日本国内で評価が完了するため、評価および認証のプロセスに必要な機密事項を海外に提出する必要はありません。※4

日本国内の拠点で評価するため、問い合わせや審査のスケジュール調整が迅速に行えます。※1

日本のビジネス文化や慣習を理解しているため、お客さまの社内プロセスに柔軟に対応できます。

技術文書作成後も、改版や維持に関するサポートを国内で受けられるため、長期的なパートナーシップが期待できます。

● 対応規格

IEC 62443-2-4:2023

産業用オートメーション及び制御システムのセキュリティー第2-4部
IACSサービスプロバイダに対するセキュリティプログラム要求事項

IEC 62443-3-3:2013

産業用通信ネットワークー ネットワーク及びシステムセキュリティー第3-3部
システムセキュリティ要求事項及びセキュリティレベル

IEC 62443-4-1:2018

産業用オートメーション及び制御システムのセキュリティー第4-1部
安全な製品開発ライフサイクル要求事項

IEC 62443-4-2:2019

産業用オートメーション及び制御システムのセキュリティー第4-2部
IACSコンポーネントの技術的セキュリティ要求事項

ETSI EN 303 645:2020

欧州電気通信標準化協会（ETSI）民生用 IoT 機器のサイバーセキュリティ
ベースライン要件

※4 当機構が発行する適合性評価レポートの場合

詳細は、お問い合わせください。

お問い合わせ先

● JC-STAR制度 対応サービス

● 提供するサービス

「自己適合評価」の宣言に向けた技術相談サービス

検証事業者 [☞](#)としての適合性評価

● 当機構のサービスの特色

JC-STARの検証事業者として、日本国内で完結する『日本語による適合性評価サービス』を提供します。

日本国内で評価が完了するため、評価のプロセスに必要な機密事項を海外に提出する必要はありません。

国内に拠点があるため、問い合わせや審査のスケジュール調整が迅速に行えます。

適合ラベル取得後も、維持に関するサポートを国内で受けられるため、長期的なパートナーシップが期待できます。

これまでに当機構が提供してきた電気安全やEMCなどの適合性評価で培ってきたIoT製品の知識を活用します。

● 対象となる適合基準のレベル

★1（レベル1）

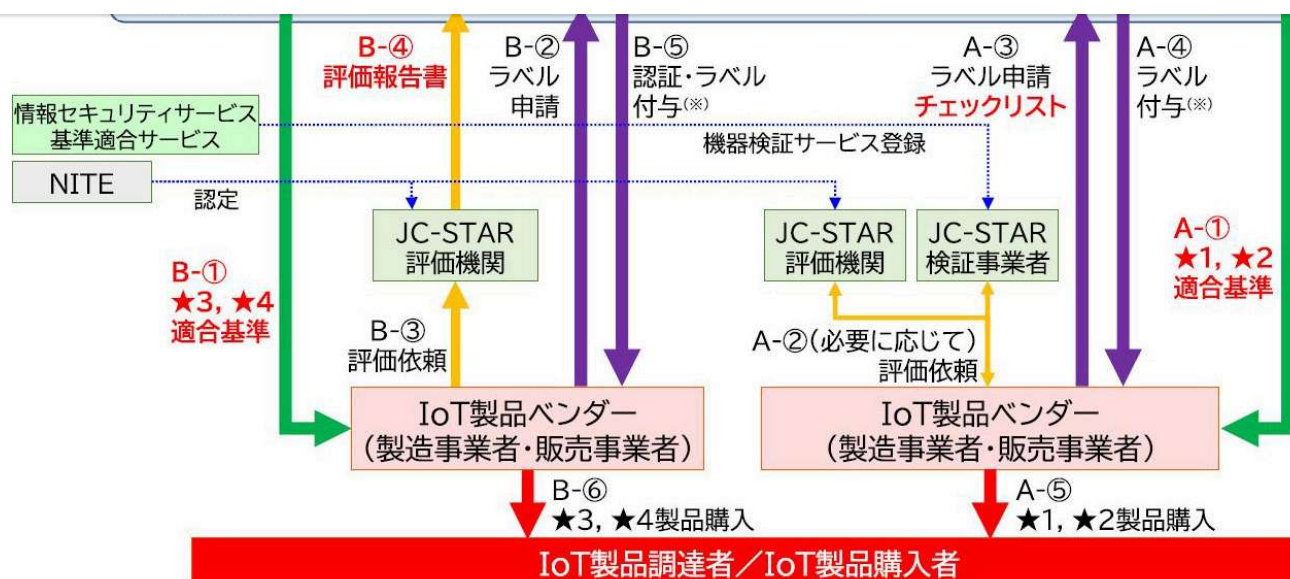
製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことをIoT製品ベンダーが自ら宣言するもの

なお、★2（レベル2）以上については独立行政法人情報処理推進機構（IPA）の申請受け付けが開始次第のサービス提供を計画しています。

● JC-STARとは？

JC-STARは、経済産業省が公表した「IoT製品に対するセキュリティ適合性評価制度構築方針」に基づいて構築されたIoT製品のセキュリティ要件適合評価およびラベリング制度で、2025年3月25日より「★1（レベル1）」の申請受付が開始されました。

この制度は、ETSI EN 303 645、IEC 62443-4-1やIEC 62443-4-2などと調和しつつ、独自に定めた適合基準に基づいて、IoT製品のセキュリティ機能を評価・可視化することを目的とし、IPAによって運営されている制度です。



(※4) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

(出典： [IPA WEBサイト](#) [🔗](#))

● 対象製品

対象製品は、インターネットプロトコル (IP) を使用したデータの送受信機能を持ち、直接・間接を問わず、インターネットにつながる (可能性がある／否定できない) 機器となります。

● 適合基準

製品類型、想定されるセキュリティ脅威や保護すべき情報資産等の違いにより、求められるセキュリティ要件が異なり、4段階のレベルが設けられています。レベルが高くなるほど、求められるセキュリティ要件の項目が多くなります。適合基準のレベルは以下のとおりです。

★1 (レベル1)

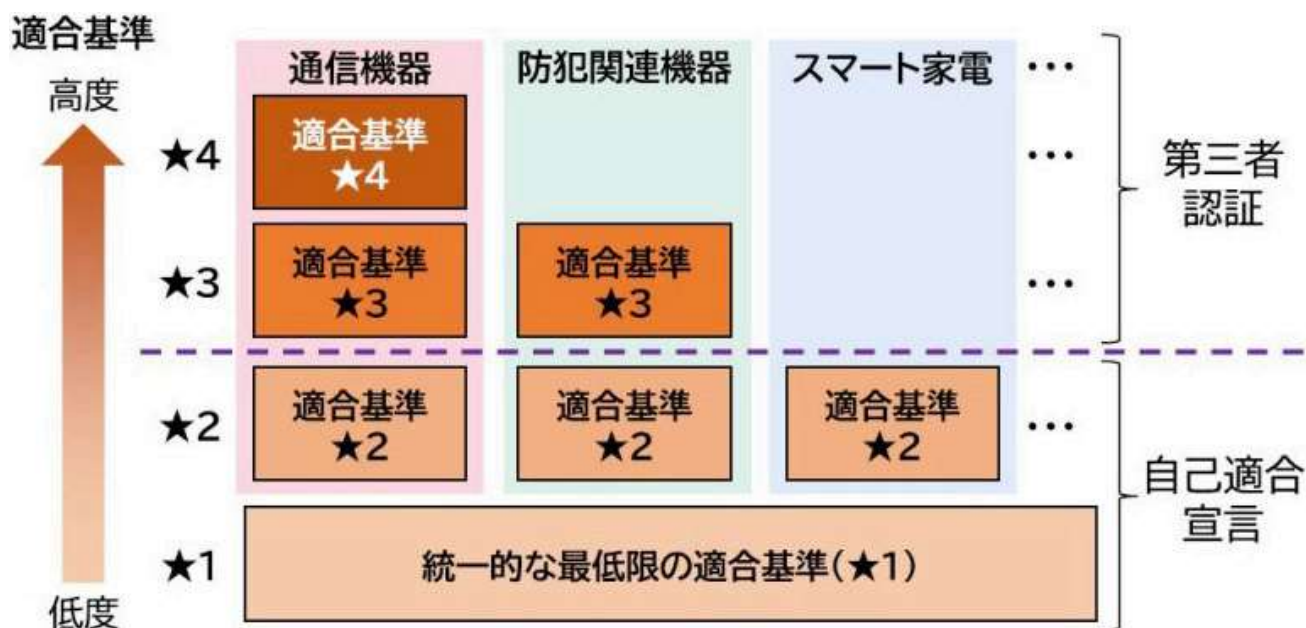
製品として共通して求められる最低限のセキュリティ要件を満たすことを製品ベンダーが自ら宣言したもの。

★2 (レベル2)

製品類型ごとの特徴を考慮し、★1に追加すべき基本的なセキュリティ要件を満たしたことを製品ベンダーが自ら宣言したもの。

★3 (レベル3) および★4 (レベル4)

品類ごとに定められた適合基準を、機器が満たすことを独立した第三者が評価した
もの。



(出典： [IPA WEBサイト](#))

適合基準・評価手順の詳細につきましては、以下の「参考リンク」よりご確認ください。

(上記内容と参考リンクの原文が違っている場合は、原文が優先されますことをご了承ください。また、本文中の日時は現地時間になります。)

詳細は、お問い合わせください。

お問い合わせ先

● 機器検証サービス

経済産業省「情報セキュリティサービス基準」で定められている、IoT 機器をはじめとするネットワーク通信機能を持つ機器およびその機器に対してネットワークを通じて操作・管理・データ処理等を行うアプリケーションから構成されるシステム (IoT システム) を対象として行う、機器検証のサービスです。

情報セキュリティサービス基準の詳細については、経済産業省のWEBサイト：

<https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html> をご覧ください。

機器検証サービス

セキュリティ確保のためのセキュリティ検証の手引き」等、お客さまが適用を希望する規格・基準に基づき、ご依頼の機器の基準適合性の確認と検証を行います。

また、お客さまのご要望に応じてギャップ分析や研修・セミナーなども承ります。

● 対象機器（一例）

プラント・工場などで、産業オートメーションおよび制御システム（IACS）に使用される、PLC・HMI・センサー類などのコンポーネントやサブシステムならびにコンポーネントを組み合わせたシステム

消費者向けIoT機器（ネットワークカメラ・スマートTVなどのスマート家電をはじめとしたインターネットに接続される機器）

組み込みソフトウェアを含むヘルスソフトウェアを組み込んだ医療機器

技術相談サービス

● ギャップ分析

ギャップ分析

お客さまの現状の組織とプロセスを、インタビューや書面により確認し、規格の要求事項との間のギャップを洗い出します。現在のセキュリティ状況を明確に把握でき、どの部分が不足しているかを特定できます。発見されたギャップを優先順位付けし、解消するためのリソースを効率的に配分することで、スムーズに適合性評価へ進むことができます。

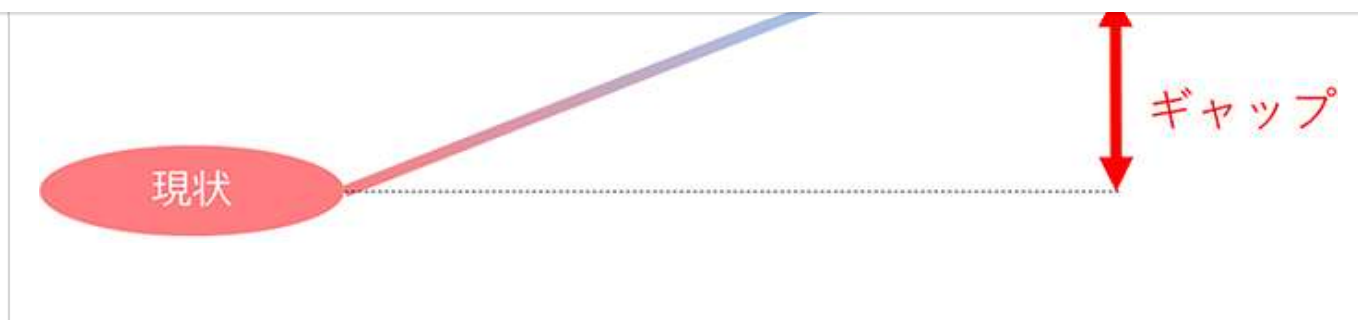
● 当機構のサービスの特色

日本語で作成された、社内規定、帳票類のままで対応できます。

お客さまのご要望に応じて、最小単位での要件に対する分析を行うことができます。

日本国内で分析が完了するため、機密事項を海外に提出する必要はありません。

日本のビジネス文化や慣習を理解しているため、お客さまの現状に対し柔軟に対応し、ご相談いただく事ができます。



詳細は、お問い合わせください。

お問い合わせ先

● 研修・セミナー・ワークショップ

研修・セミナー・ワークショップ

お客さまの目的、受講対象者のレベルに合わせた研修などのトレーニングメニューをオーダーメイドで作成し、サイバーセキュリティ要件を熟知した当機構エンジニアが講師を担当します。

例：サイバーセキュリティ入門研修、IEC 62443-x規格の詳細解説、プロセス理解と構築のためのワークショップなど

詳細は、お問い合わせください。

お問い合わせ先

国際認証サービス

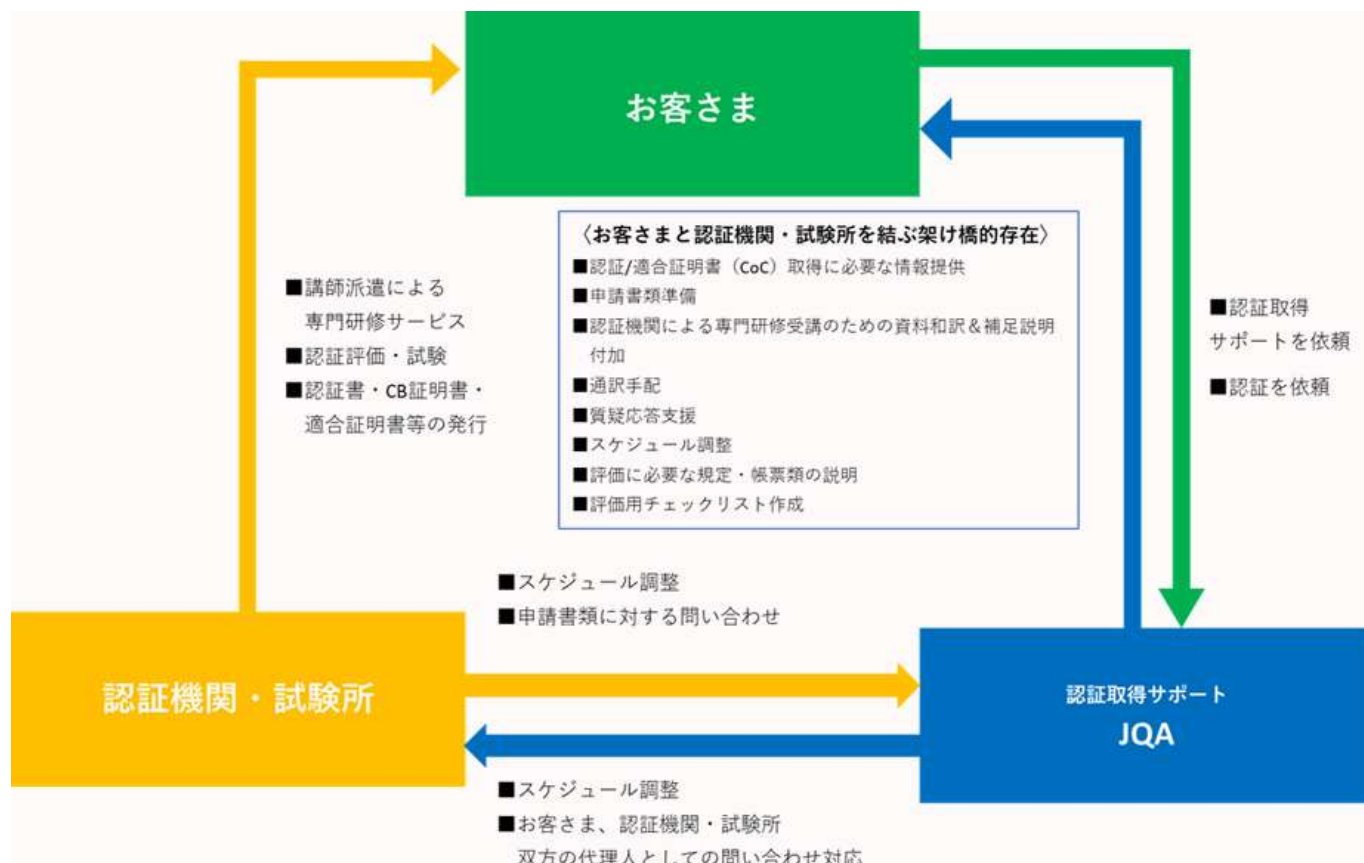
● 申請代行サービス

提携する認証機関・試験所による海外認証・適合証明書（CoC）取得をサポート

● 当機構のサービスの特色

認証機関・試験所による専門研修サービス、WEBミーティングのセッティング

個社のご事情に合わせて柔軟にカスタマイズできます。日本を代表する認証・試験機関として、お客さまの認証、証明書（CoC）等の取得まで責任をもってサポートします。



その他、お客さまのご要望に応じたさまざまな技術相談サービスを提供しております。お気軽にお問い合わせください。

関連リンク（JQA WEBサイト）

[医療機器試験サービス](#)

[国際認証サービス](#)

関連トピックス

2025/03/25 新規サービス

「JC-STAR制度 対応サービス開始」のお知らせ



2025/02/03 ニュース

EU - 「欧州委員会がサイバーセキュリティ規格を発表」のお知らせ



2025/02/03 ニュース

米国（FCC） - 「ホワイトハウスがU.S. Cyber Trust Mark発表」のお知らせ



2024/10/28 ニュース

インド（NCCS） - 「サイバーセキュリティ認証におけるメインモデルと派生モデル」のお知らせ



JQAについて

お問い合わせ

サービス

業種別サービス

セミナー・教育支援

拠点案内

採用情報

プライバシーポリシー

Copyright (C) 2025

JAPAN QUALITY ASSURANCE ORGANIZATION All rights reserved.