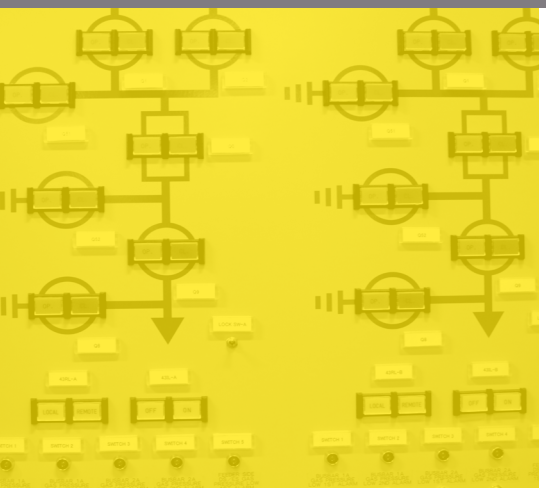
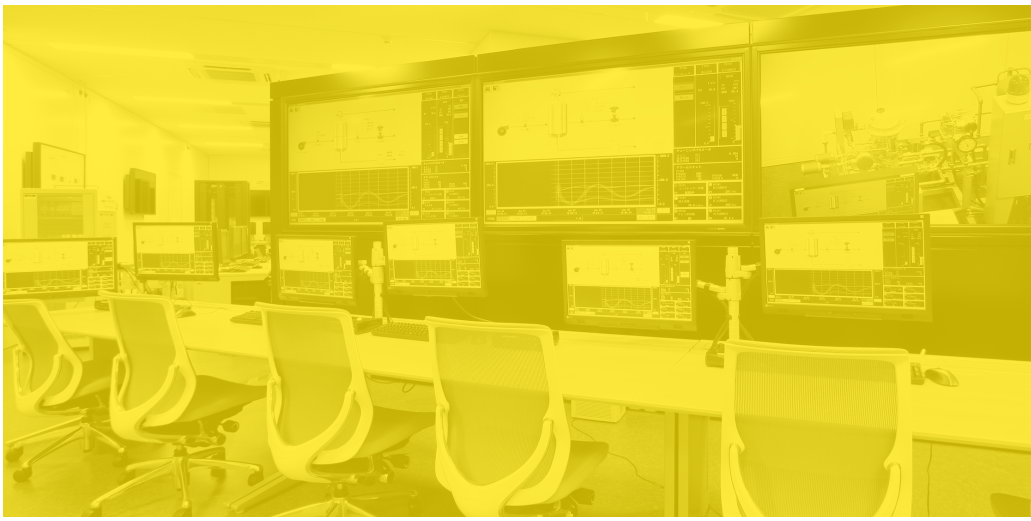
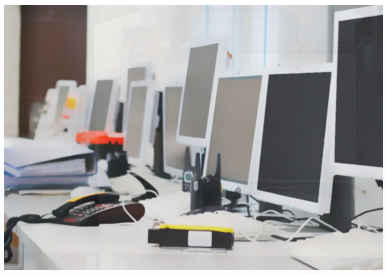
CSSC 認証ラボラトリー

CSSC Certification Laboratory



ISASecure EDSA 認証



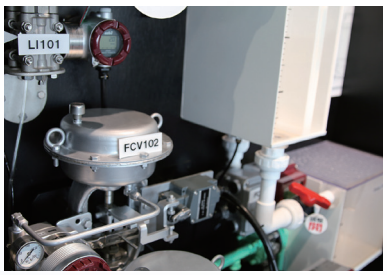

はじめに

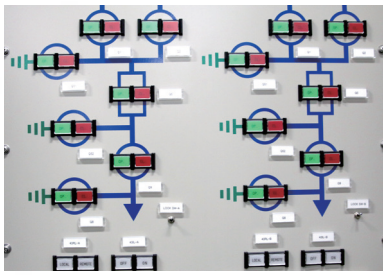
社会インフラに対するサイバー攻撃

近年、社会インフラのコンピュータ化（ソフト化）やネットワーク化が進んでいます。それに伴いサイバー攻撃も著しく増加しており、その脅威が現実のものになってきています。社会インフラは私たちの日常生活や経済活動の基盤であり、もし大規模なサイバー攻撃によりサービスを持続できなくなった場合、その影響は甚大なものです。特に電力、ガス、水道、鉄道、航空、石油、化学などの重要な社会インフラを支える制御システムに対してはセキュリティの強靭さ（レジリエンス）が強く望まれています。

国際的な制御システムのセキュリティ標準

このような背景から、現在の社会インフラを支える制御システムにおいては、多種多様なサイバー攻撃に耐えうるセキュリティ対策の実装が必要不可欠です。国際標準組織の ISA や IEC では、ISA/IEC 62443 という制御システム向けセキュリティ標準を推進しセキュリティ要件を整理するとともに、リスク分析の軸として健康や安全、環境 (HSE : Health, Safety, Environment) への影響の観点で分析することを求めると同時に、セキュリティ対策の強度（攻撃者に対する防護壁・ハードルの高さのようなもの）を評価する軸としてセキュリティレベルの考えを導入しています。





注目を浴びる国際的なセキュリティ認証標準

セキュアな制御システムを実現するためには、制御システムを構成する各制御機器（コンポーネント）がセキュアで安全かつ安定的に利用できることが重要です。そこで制御機器ベンダにより制御機器のセキュリティ対策の強靭化に向け、ISA/IEC62443 の制御システムセキュリティ標準を参照してセキュリティ機能の実装がされています。セキュリティ機能の実装に対して各制御機器が国際標準の要求に適合しているか評価を実施し、評価結果を判定する認証が必要です。

国際的に注目されているのは、ISA セキュリティ適合性協会 ISCI (ISA Security Compliance Institute) の EDSA(Embedded Device Security Assurance) 認証（以下、EDSA 認証）です。この認証は第三者の認証機関で実施されます。

国際的な相互承認に基づいたフレームワーク

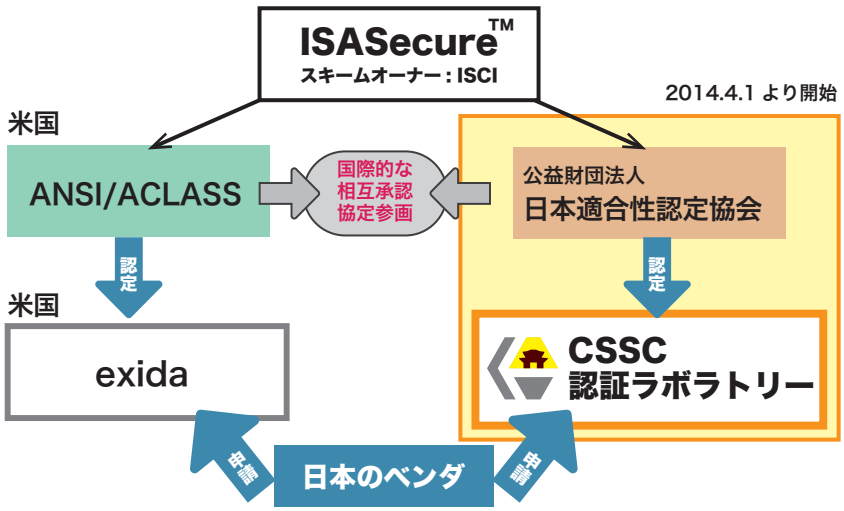
CSSC 認証ラボラトリーの提供する EDSA 認証は、国際的な相互承認のフレームワークです（次ページ図参照）。これまでは国際的な EDSA 認証を取得するためには米国の認証機関において、英語で受審する必要がありました。しかし、これからは CSSC 認証ラボラトリーのある日本で、日本語により EDSA 認証を得ることが可能となります。

日本で取得した EDSA 認証が海外でも通用することは、制御機器ベンダが海外輸出する際、競合力を確保する面からも非常に有効です。

EDSA 認証スキームの日本での展開

国際的な相互承認により、世界に通用する EDSA 認証

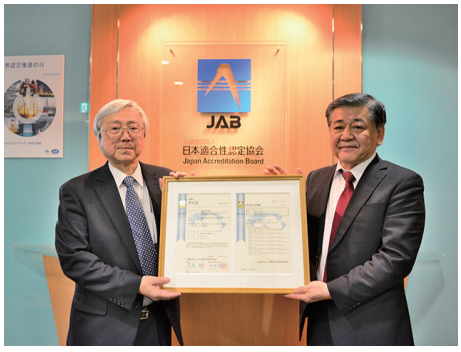
EDSA 認証は、下図に示すような国際的な相互承認により、日本国内だけでなく世界に通用する製品認証の制度です。CSSC 認証ラボラトリーは、試験所認定、製品認証機関認定ともに ISCI の定める EDSA 基準に達したと公益財団法人日本適合性認定協会（JAB）により認められました。
2014 年 4 月から CSSC 認証ラボラトリーは、EDSA 認証の評価実施および合格した制御機器への EDSA 認証書発行が可能になりました。



国際的な相互承認制度の図。CSSC 認証ラボラトリーは ISASecure EDSA 認証機関の要件を満たしていることを日本適合性認定協会（JAB）により認められた。

日本初、世界でも 2 番目の ISASecure EDSA 認証機関

CSSC 認証ラボラトリーはアジアで初めて、世界でも 2 番目の EDSA 認証機関となりました。国内の社会インフラのセキュリティ向上を実現すること、さらに日本で日本語による世界共通の EDSA 認証を取得できることにより、制御機器を開発・輸出する日本のベンダの国際競争力の向上を目標とします。
なお、この CSSC による EDSA 認証は、「サイバーセキュリティ戦略」（平成 25 年 6 月情報セキュリティ政策会議決定）の中で記載されているもので、国の制御システムの評価･認証機関の整備の政策に合致しているものです。



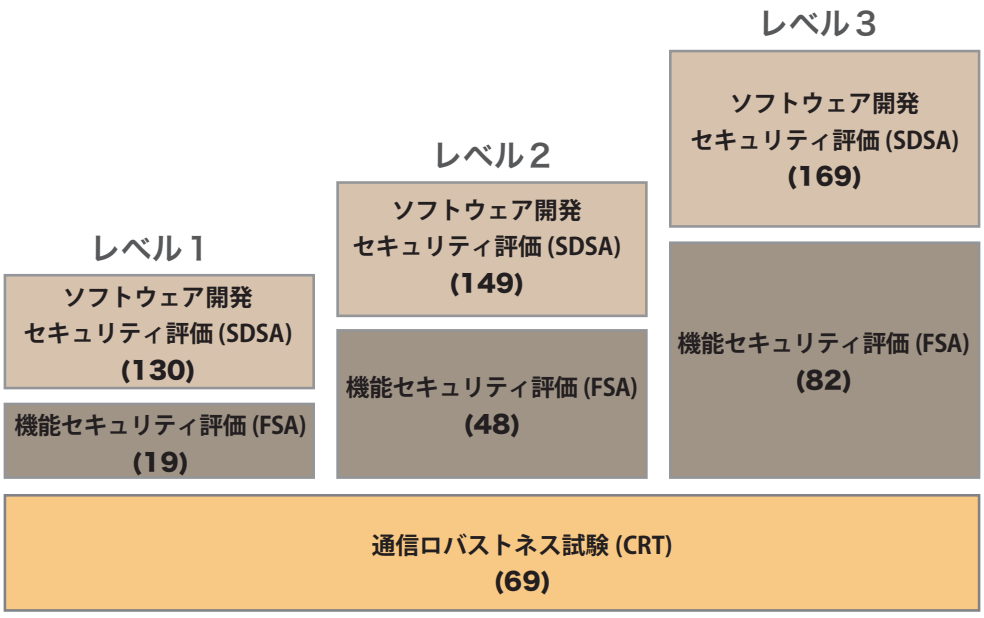
左：CSSC 認証ラボラトリー最高責任者 小林（左）と JAB 久米専務理事（右）
右：CSSC 認証ラボラトリー評価センター長 吉松（左）

ISASecure EDSA 認証　3 つの評価項目

ISCI は、ISA/IEC62443 標準のフレームワークを使って ISASecure EDSA 認証（以下、EDSA 認証）の仕様を開発しました。EDSA 認証は，スキームオーナーである ISCI が運営する制御機器のセキュリティ保証に関する認証制度であり、以下の 3 つの評価項目があります。EDSA 認証を受けるためには、 3つの評価項目に同時に合格する必要があります。

評価項目１：ソフトウェア開発の各フェーズにおけるセキュリティ評価
(SDSA：Software Development Security Assessment)
評価項目２：セキュリティ機能の実装評価
(FSA：Functional Security Assessment)
評価項目３：通信の堅牢性テスト
(CRT：Communication Robustness Testing)

セキュリティのレベルは3段階設けられています。
評価項目3の CRT テストはレベル1～3において共通ですが、SDSA と FSA 評価の要求事項は、レベルとともにその数が増加します。



( ) 内数値は要求事項の数です。

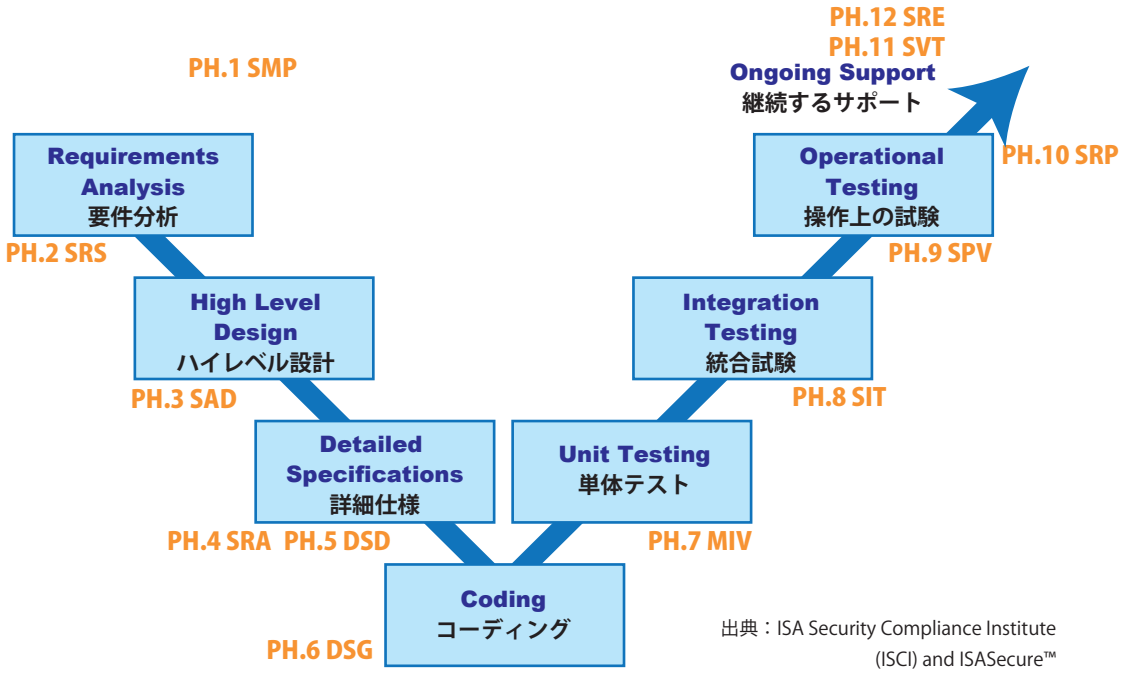
評価項目1：ソフトウェア開発の各フェーズにおけるセキュリティ評価

SDSA: Software Development Security Assessment (EDSA-312)

①　対象とする制御機器のソフトウェア開発プロセスを評価します。

②　開発ドキュメント (計画 / 成果物) とレビュー記録 (PDCA プロセスの妥当性と記録確認) を評価します。

認証機関の監査人は、認証を受けるために提出されたドキュメントと開発者へのインタビューを含む現地訪問を実施します。SDSA では、例えば、下図に示す開発プロセスの V 字モデルに従ったセキュリティ活動フェーズが組み込まれていることを監査します。この評価により、ソフトウェア開発ライフサイクルへのセキュリティ導入を推進することを目的としています。



出典：ISA Security Compliance Institute (ISCI) and ISASecure™

番号	活動フェーズ
PH1	セキュリティ管理プロセス (SMP)
PH2	セキュリティ要求事項仕様 (SRS)
PH3	ソフトウェアアーキテクチャ設計 (SAD)
PH4	セキュリティリスクアセスメントと脅威のモデル化 (SRA)
PH5	詳細ソフトウェア設計 (DSD)
PH6	セキュリティ指針文書 (DSG)
PH7	モジュールの実装と検証 (MIV)
PH8	セキュリティ統合テスト (SIT)
PH9	セキュリティプロセス検証 (SPV)
PH10	セキュリティ対応計画 (SRP)
PH11	セキュリティ検証テスト (SVT)
PH12	セキュリティ対応実行 (SRE)

評価項目2：セキュリティ機能の実装評価

FSA：Functional Security Assessment (EDSA-311)

①対象とする制御機器のセキュリティ機能の評価をします。

② EDSA-311 の要求事項に沿って、対象とする制御機器の機能や初期設定等の確認を行い、適合 / 不適合を評価します。

③実機テスト：一部の要求事項については、実機を用いて実際に動作を確認します。

認証機関の監査人は、ユーザ向けや設計用ドキュメント、監査のために特別に提出されたドキュメント及び制御機器に対してのテスト結果に基づいて監査を実施します。監査の主な要求事項を下の表に示します。

要求事項	
アクセスコントロール (AC: Access Control)	ユーザ承認、ユーザ認証、システム使用通知、セッションロック / 終了 User Authorization, User Authenticaiton, System Use Notification, Session Locking/Termination
使用コントロール (UC: Use Control)	デバイス認証、監査証跡 Device Authentication, Audit Trail
データの完全性 (DI: Date Integrity)	転送中のデータ、保管中のデータ Data in Transit, Data at Rest
データの機密性 (DC: Data Confidentiality)	転送中のデータ、保管中のデータ、暗号化 Data in Transit, Data at Rest, Crypto
データフロー制限 (RDF: Restrict Data Flow)	情報フロー実施、適用パーティッショニング、機能分離 Information Flow Enforcement, Application Partitioning, Function Isolation
イベントへのタイムリーなレスポンス (TRE: Timely Response to Event)	インシデント応答 Incident Response

EDSA 適合スキーム定義関連ドキュメント

日本語に簡易翻訳された EDSA 適合スキーム定義関連ドキュメントは、下記の ISCI ホームページからダウンロードできます。ここには、技術仕様、認定 / 認可、シンボルと認証書、構成及び外部参照ドキュメントなどについて解説されています。

http://isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspx

評価項目3：通信の堅牢性テスト

CRT：Communication Robustness Testing (EDSA-310 他)

① ISCI 認定の試験デバイスにより試験パケットを試験対象 DUT（Device Under Test）に対して送信し、サービスの維持を確認します。

②6つの必須サービスの維持が合否判定の基準となります。この時コントローラだけではなく、事実上 HMI 側の用意も必要となります。

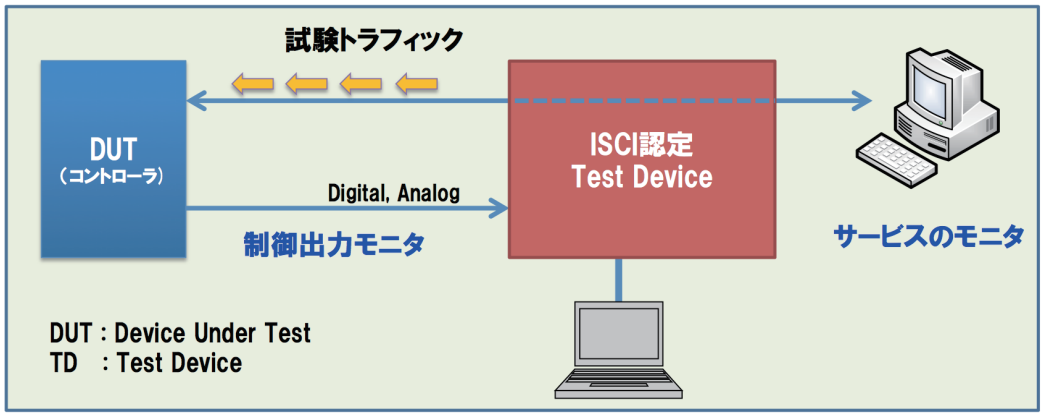
③ CRT 試験には、ISCI の認定した試験デバイスを用います。以下の URL を参照ください。

http://www.isasecure.org/Supplier-Resources/Recognized-Test-Platforms-for-CRT.aspx

認証機関の監査人は、認証機関に持ち込まれた制御機器に対して上記の通信堅牢性テストを実施します。

現在の通信堅牢性テストの対象となる通信プロトコルは次の 6 種類です。

EDSA-401：IEEE 802.3(Ethernet)、ARP、IPv4、ICMPv4、UDP、TCP



■ 6つの必須サービス

次の機能を用いたサービスが適切に維持されていることを確認する

① 制御ループ
・規定の信号を出力する機能

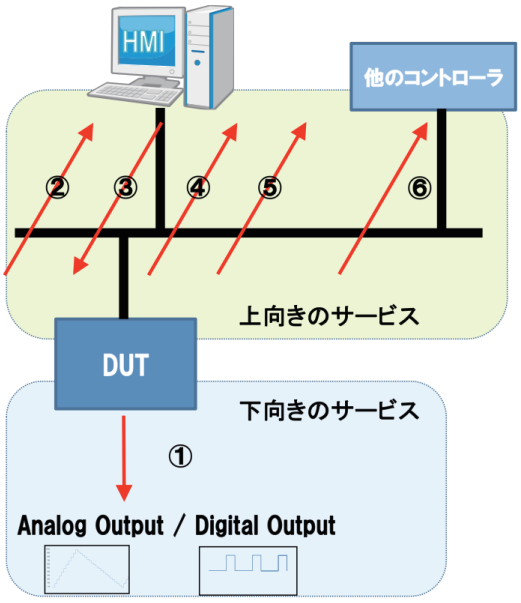
② プロセスのビュー
・プロセスビューを適切なタイミングで提供する機能

③ コマンド
・上位システムからの命令に適切なタイミングで応答する機能

④ プロセスアラーム
・プロセスアラームを適切なタイミングで送信する機能

⑤ 必須履歴データ
・必須履歴データを適切なタイミングで送信する機能
適用除外可能

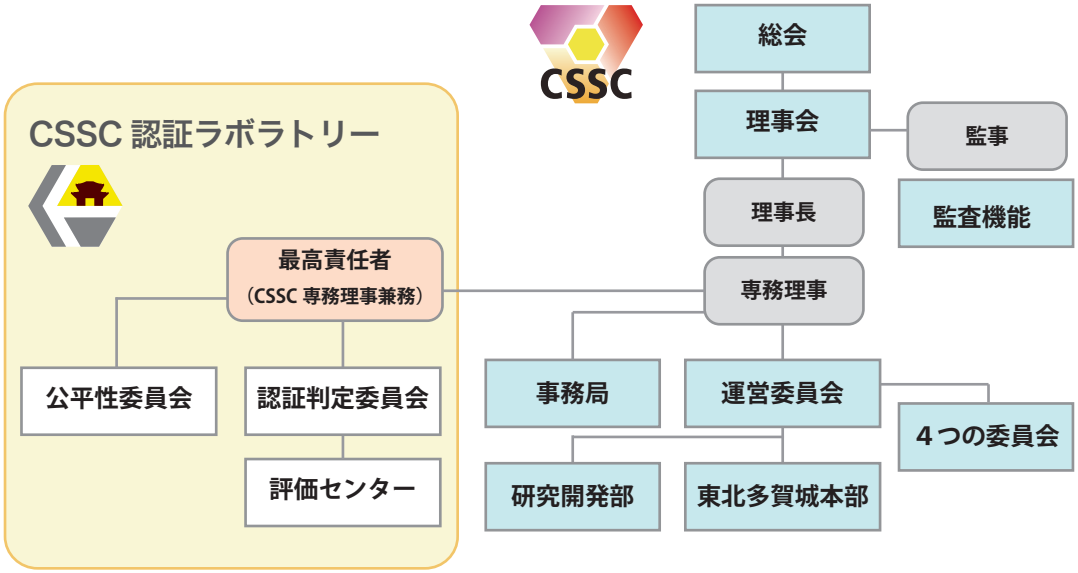
⑥ ピアツーピア制御通信
・ピアツーピア制御通信を送信する機能
・適用除外可能



CSSC 認証ラボラトリーについて

CSSC 他部門とは独立した体制で認証業務を実施

CSSC 認証ラボラトリーは、技術研究組合制御システムセキュリティセンター（CSSC）内の独立組織です。下図に示すように CSSC の中で他の部門とは独立した体制での認証業務を実施しています。このような体制で、公平・公正な認証業務を実施しています。



EDSA 認証の受審費用について

制御機器の複雑さや構成などで受審項目や期間が決まります。EDSA 認証受審の詳細な見積もりについては、別途打合せで決めることになります。詳細はお問い合わせ下さい。

問い合わせ先

技術研究組合制御システムセキュリティセンター
CSSC 認証ラボラトリー

〒 985-0842　宮城県多賀城市桜木 3-4-1
みやぎ復興パーク F-21 棟 6 階

TEL：022-353-6751　メール：info@cssc-cl.org

Web サイト：http://www.cssc-cl.org

※苦情・異議申し立てに関しては、ホームページの「お問い合せ」をご覧下さい。
http://www.cssc-cl.org/contact/index.html

2014 年4月 発行
CSSC 認証ラボラトリー

〒985-0842　宮城県多賀城市桜木3−4−1　みやぎ復興パーク F21 6 階
TEL : 022-353-6751　FAX : 050-3153-0000
http://www.cssc-cl.org