制御システムセキュリティセンター　ISASecure SSA/SDLA/EDSA認証 説明会

ISASecure EDSA説明
「制御機器認証と拡張について」

EDSA 2.0.0（FSA-E/SDLPA/SDA-E）

2015年5月14日（東京）、5月22日（大阪）
技術研究組合制御システムセキュリティセンター

研究員　清水 良昭

アジェンダ

1. 制御機器認証（EDSA認証）について

- EDSA認証とは
- EDSA認証の評価項目
- EDSA 2.0.0 の体系
- 認証レベル、評価項目数
- EDSA規格のドキュメント体系（EDSA 2010.1）
- EDSA規格のドキュメント体系（EDSA 2.0.0）
- 要求事項の比較

2. 組込み機器の機能セキュリティ評価とは

- FSA-Eの概要
- 割り当て可能 (Allocatable)
- FSA-Eの主な要求事項
- 7つの機能カテゴリにおける要求事項

3. 組込み機器の開発プロセスに関する評価とは

- SDLPA/SDA-E の概要
- SDLA-312の見方

4. 最後に

- EDSA認証を受けられる方へ

アジェンダ

1. 制御機器認証（EDSA認証）について

- EDSA認証とは
- EDSA認証の評価項目
- EDSA 2.0.0 の体系
- 認証レベル、評価項目数
- EDSA規格のドキュメント体系（EDSA 2010.1）
- EDSA規格のドキュメント体系（EDSA 2.0.0）
- 要求事項の比較

2. 組込み機器の機能セキュリティ評価とは

- FSA-Eの概要
- 割り当て可能 (Allocatable)
- FSA-Eの主な要求事項
- 7つの機能カテゴリにおける要求事項

3. 組込み機器の開発プロセスに関する評価とは

- SDLPA/SDA-E の概要
- SDLA-312の見方

4. 最後に

- EDSA認証を受けられる方へ

1．制御機器認証（EDSA認証）について

1．制御機器認証（EDSA認証）について ・・・ EDSA認証とは

- ISASecure® **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

- EDSA**認証の対象**は，組込み機器（**embedded device**）
  例）PLC，SISコントローラ，DCSコントローラ等

※ ISCI： ISA Security Compliance Institute

EDSA：Embedded Device Security Assurance
PLC：programmable logic controller，　SIS：Safety Instrument System，　DCS：distributed control system

1．制御機器認証（EDSA認証）について ・・・ 組込み機器とは

EDSA-300 ISA Security Compliance Institute – Embedded Device Security Assurance – ISASecure certification requirements :

3.1.3 組込み機器

組込みソフトウェアを実行する**特殊目的のデバイス**であり，産業プロセスを直接監視し，制御し，又は作動させるように設計されたもの

注記 組込み機器には，次のような属性がある。回転メディアがない，公開サービスの数が制限されている，外部インタフェース，組込み OS 又はファームウェアに相当する機能，リアルタイムスケジューラを通じてプログラムされる，制御パネルが取り付けられている場合がある，通信インタフェースを備えていることがある。たとえば，PLC，フィールドセンサデバイス，SIS コントローラ，DCS コントローラなどがある。

3.1.3 embedded device

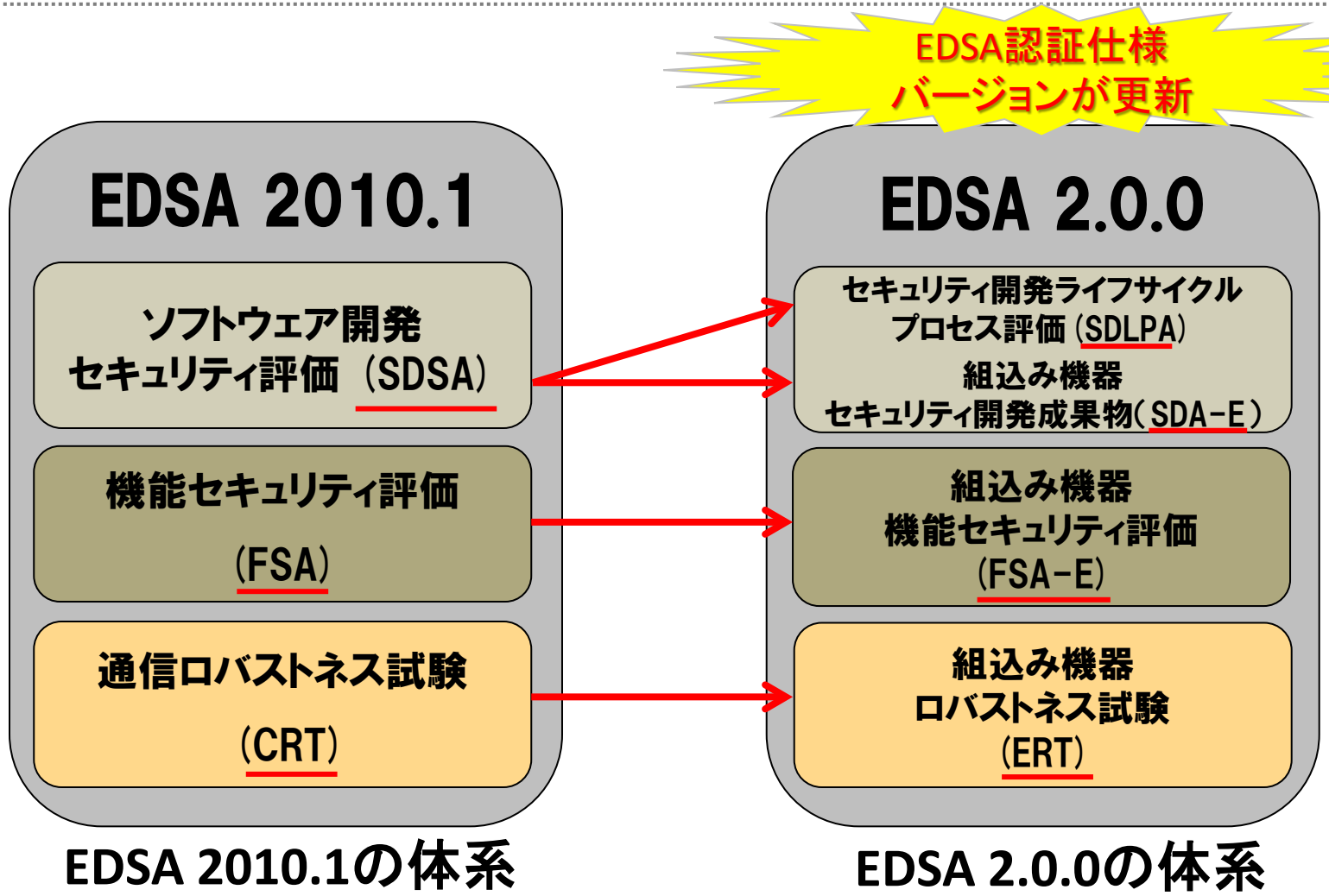
special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

出典：http://www.isasecure.org/Documents/EDSA-JP/EDSA-300-ISASecure-cert-req(v2_0)_JP.aspx

EDSA：Embedded Device Security Assurance
PLC：programmable logic controller，　SIS：Safety Instrument System，　DCS：distributed control system

1. 制御機器認証(EDSA認証)について ・・・ EDSA認証の評価項目



SDSA : Software Development Security Assessment , FSA : Functional Security Assessment , CRT : Communication Robustness Testing ,
SDLPA : Security Development Lifecycle Process Assessment , SDA-E : Security Development Artifacts for Embedded Devices ,
FSA-E : Functional Security Assessment for Embedded Devices , ERT : Embedded Device Robustness Testing

1. 制御機器認証(EDSA認証)について ・・・ EDSA 2.0.0の体系

◆3つの項目を評価・試験することで、想定脅威に対する対策のカバー範囲が十分であることを認証

EDSA 2.0.0

セキュリティ開発ライフサイクル プロセス評価(SDLPA) 組込み機器 セキュリティ開発成果物(SDA-E)

組込み機器 機能セキュリティ評価 (FSA-E)

組込み機器 ロバストネス試験 (ERT)

体系的な設計不良の検出・回避のための評価

- 組込み機器(コンポーネント)をセキュアに開発するための開発プロセスが規定されているかどうかを評価
- 当該開発プロセスにもとづき開発が行われているかどうかを評価(アーティファクトを確認)

※3段階のセキュリティレベルにより評価項目数が決まる

実装エラー / 実装漏れを検出するための評価

- セキュリティ機能要件について、目標とするセキュリティレベルに対応する全要件が実装済みであるかどうかを評価

※3段階のセキュリティレベルにより評価項目数が決まる

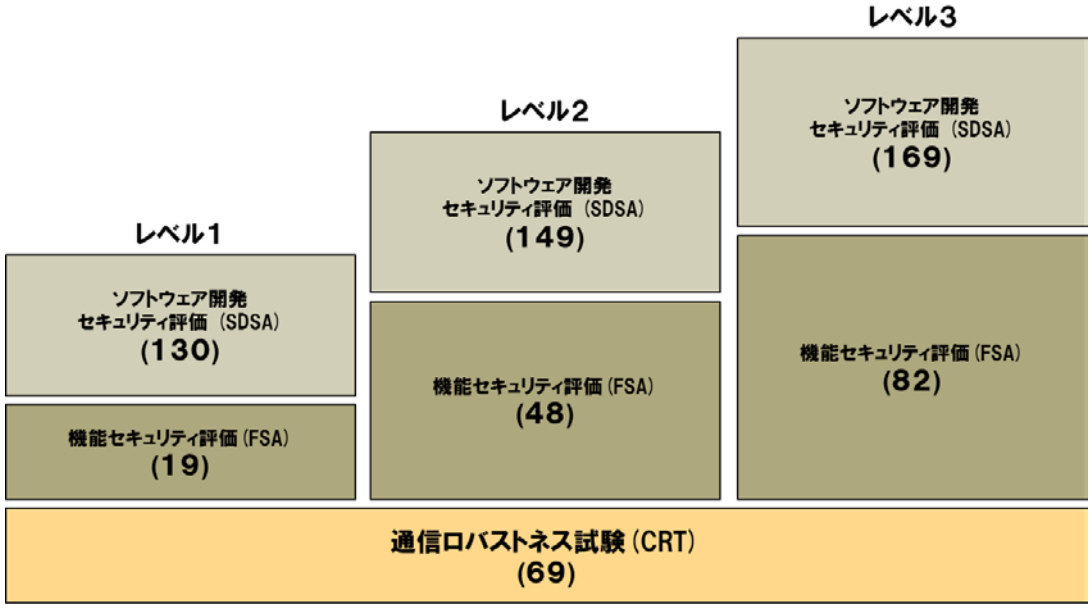
デバイスの堅牢性を評価する試験

- 潜在的な脆弱性を発見するためネットワーク実装のロバストネス(堅牢性)について試験
- 既知の脆弱性を発見するための試験

※セキュリティレベルによらず、評価項目数は同一

SDLPA : Security Development Lifecycle Process Assessment , SDA-E : Security Development Artifacts for Embedded Devices , FSA-E : Functional Security Assessment for Embedded Devices , ERT : Embedded Device Robustness Testing

1. 制御機器認証(EDSA認証)について ・・・ 認証レベル、評価項目数

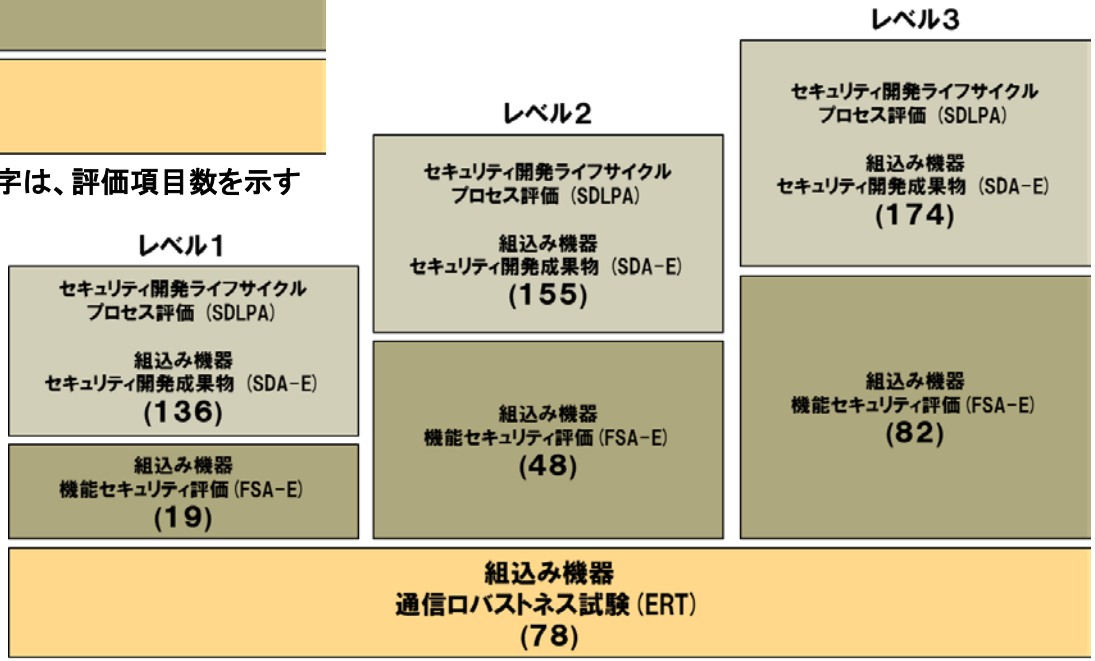


EDSA 2010.1

※括弧内の数字は、評価項目数を示す

EDSA 2010.1、EDSA 2.0.0 共に、
認証レベルは3段階

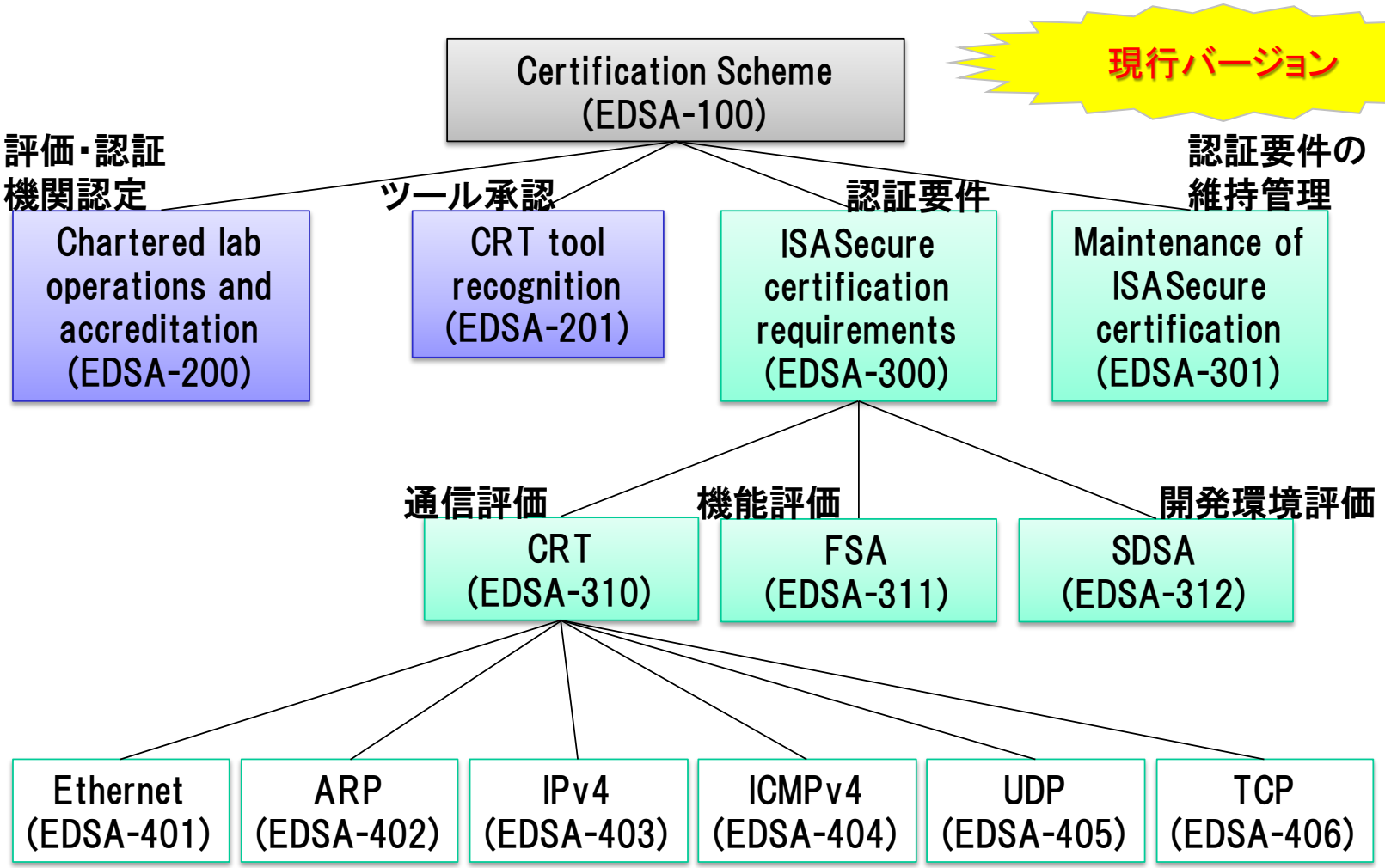
(レベル1⇒2 ⇒ 3の順にレベルが高くなる)



EDSA 2.0.0

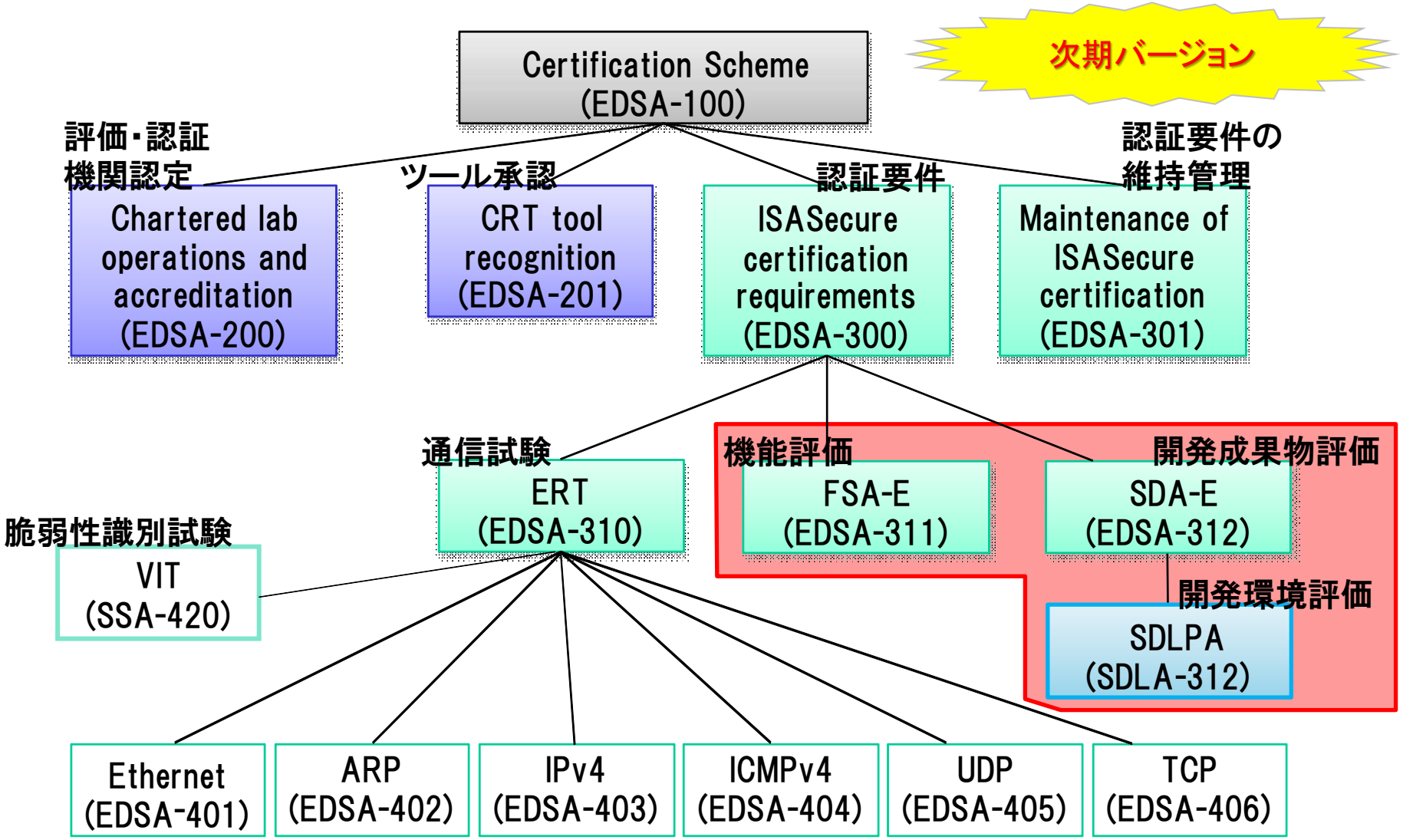
※括弧内の数字は、評価項目数を示す

1．制御機器認証（EDSA認証）について ・・・ EDSA規格のドキュメント体系（EDSA 2010.1）



◇ IPAにより翻訳されたEDSA標準の対訳版はISCIウェブサイトにて公開。
http://www.isasecure.org/Certification/EDSA-Certification-(In-Japanese)

1．制御機器認証（EDSA認証）について ・・・ EDSA規格のドキュメント体系（EDSA 2.0.0）



http://www.isasecure.org/Certification/IEC-62443-4-2-EDSA-Certification の Version2

1. 制御機器認証(EDSA認証)について ・・・ 要求事項の比較

要求事項に関して、大きな変更は無い(追加削除:数項目有り)

EDSA 2010.1 ※現行バージョン	EDSA 2.0.0 ※次期バージョン
• **SDSA** (Software Development Security Assessment) ⇒ **EDSA-312**	• **SDLPA** (Security Development Lifecycle Process Assessment) ⇒ **SDLA-312の"Component"にチェックされた項目("Development Organization and SDL Validation Activity")** • **SDA-E** (Security Development Artifacts for embedded devices) ⇒ **SDLA-312の"Component"にチェックされた項目の("Component or System Validation Activity")**
• **FSA** (Functional Security Assessment) ⇒ **EDSA-311**	• **FSA-E** (Functional Security Assessment for embedded devices) ⇒ **EDSA-311**

- 基本的にはSDSAと同じ構成
- 追加削除が数項目あり

- FSAは変更なし

アジェンダ

1. 制御機器認証（EDSA認証）について

- EDSA認証とは
- EDSA認証の評価項目
- EDSA 2.0.0 の体系
- 認証レベル、評価項目数
- EDSA規格のドキュメント体系（EDSA 2010.1）
- EDSA規格のドキュメント体系（EDSA 2.0.0）
- 要求事項の比較

2. 組込み機器の機能セキュリティ評価とは

- FSA-Eの概要
- 割り当て可能 (Allocatable)
- FSA-Eの主な要求事項
- 7つの機能カテゴリにおける要求事項

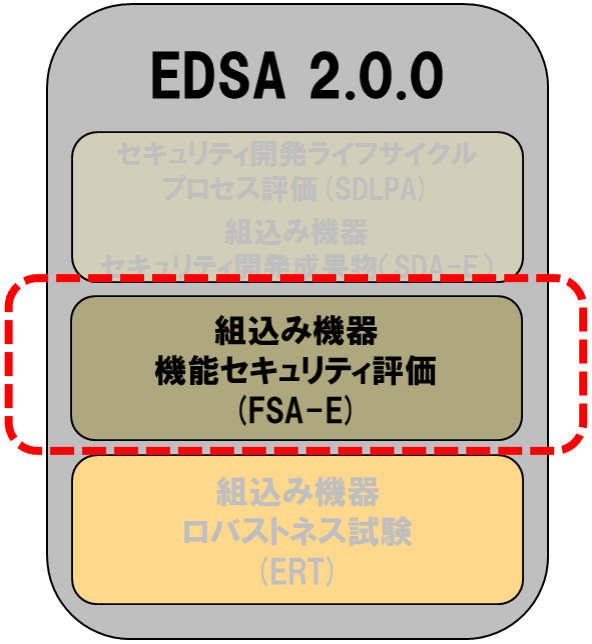
3. 組込み機器の開発プロセスに関する評価とは

- SDLPA/SDA-E の概要
- SDLA-312の見方

4. 最後に

- EDSA認証を受けられる方へ

2. 組込み機器の機能セキュリティ評価とは



2. 組込み機器の機能セキュリティ評価とは ・・・ FSA-Eの概要

■ セキュリティ機能の実装評価

FSA-E： *Functional Security Assessment for Embedded Devices*

【目的】

対象製品が一定のセキュリティ機能要件を満たすことを監査する。

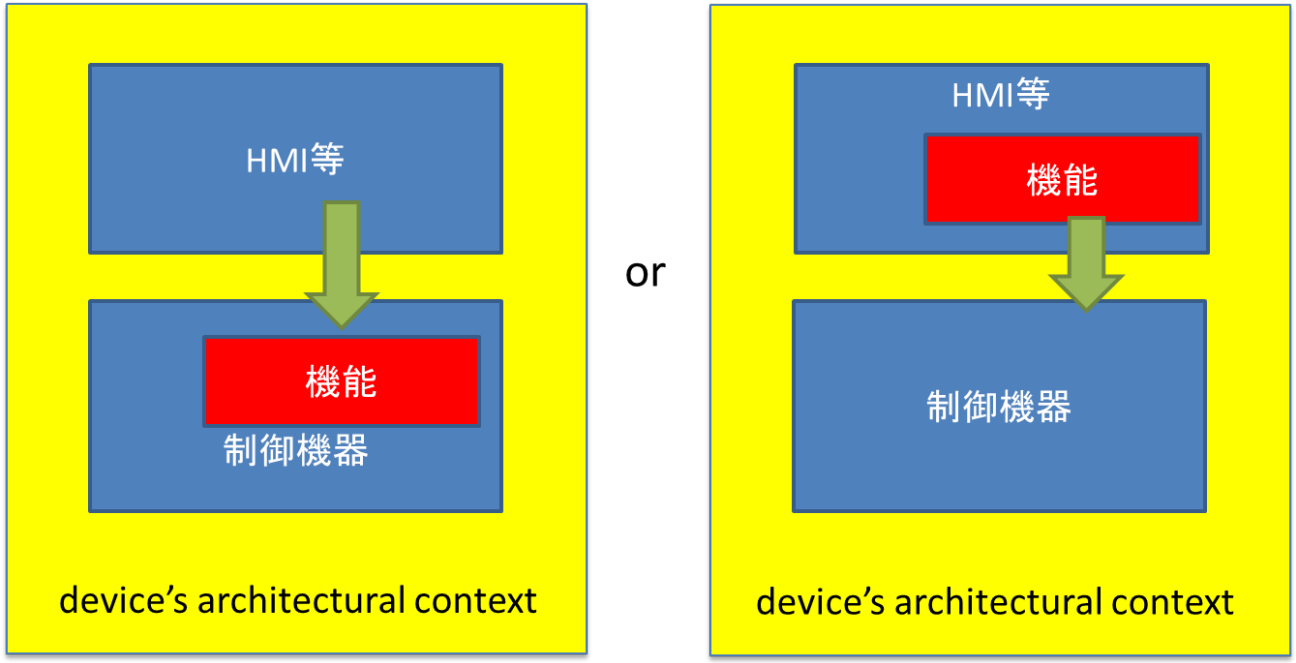
【実施内容】

1. 対象とする制御機器のセキュリティ機能を評価する。
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/不適合を評価する。
3. 一部の要求事項については、実際に実機を用いて動作を確認する。

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。

2. 組込み機器の機能セキュリティ評価とは ・・・ 割り当て可能(Allocatable)

- 割り当て可能(Allocatable)
  - 要求事項の一部は、EDSA認証対象(制御機器)の周辺機器(other components in a device's architectural context)で実現してもよい。[EDSA-200 3.1.4]
  - 割り当て可能とできる機能については、現時点ではEDSA仕様として非公開 ⇒ NDA対象として開示可能



※制御機器(コントローラ等の組込み機器)と周辺機器(同一コンテキスト内)との組み合わせで要求されている機能を実現してもよい。

2. 組込み機器の機能セキュリティ評価とは ・・・ FSA-Eの主な要求事項

7つの機能カテゴリ、そして、各カテゴリに複数の要求事項がある

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 Authentication, 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 : Data 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
ネットワークリソースの可用性 (NRA : Network Resource Availability)	**サービス不能攻撃防御、バックアップと回復** Denial of Service Protection, Backup & Recovery

（EDSA-311参照）

7つの機能カテゴリ

カテゴリ内の複数の要求事項

FSA-E

7つの機能カテゴリにおける要求事項

FSA-E要求事項数と実機テスト数

要求項目数

大項目	合計	All	>1	>2	Not required
AC(Access Control)：アクセスコントロール	22	9	6	7	1
UC(Use Control)：使用コントロール	13	2	4	7	0
DI(Data Integrity)：データの完全性	29	1	14	14	0
DC(Data Confidentiality)：データの機密性	6	1	3	2	0
RDF(Restrict Data Flow)：データフロー制限	4	1	1	2	0
TRE(Timely Response to Event)：イベントへのタイムリーなレスポンス	1	0	0	1	0
NRA(Network Resource Availability)：ネットワークリソースの可用性	7	5	1	1	0
	82	19	29	34	1

注: FSA-AC-2.2は、”Not required”とされており、要求事項とはなっていない

実機テスト数

大項目	合計	All	>1	>2
AC(Access Control)：アクセスコントロール	17	6	5	6
UC(Use Control)：使用コントロール	10	1	3	6
DI(Data Integrity)：データの完全性	17	1	8	8
DC(Data Confidentiality)：データの機密性	4	1	2	1
RDF(Restrict Data Flow)：データフロー制限	0	0	0	0
TRE(Timely Response to Event)：イベントへのタイムリーなレスポンス	0	0	0	0
NRA(Network Resource Availability)：ネットワークリソースの可用性	6	5	1	0
	54	14	19	21

AC (Access Control) : アクセスコントロール

AC	UC	DI	DC	RDF	TRE	NRA

- 概要
  - 全てのユーザ（人間、プロセス、および装置）を識別し、認証する機能。システムや資産へのアクセスを許可する。
- 要求事項数

合計	All	>1	>2
22	9	6	7

- 主な確認対象
  - ユーザ文書(マニュアル、他)
  - 実機テスト

注: FSA-AC-2.2は、”Not required”とされており、要求事項とはなっていない

UC (Use Control) : 使用コントロール

AC	UC	DI	DC	RDF	TRE	NRA

●概要

– 無許可の装置運用と情報利用から保護するため、選択された装置、または装置と情報の両方の利用を制御する機能。また、IACS(Industrial Automation Control System)に及ぼす要請された働きを実行するため、認可されたユーザ（人間、ソフトウェアプロセス、または装置）の割り当てられた権限を実施し、権限の利用を監視する。

●要求事項数

合計	All	>1	>2
13	2	4	7

●主な確認対象

– ユーザ文書(マニュアル、他)
– ソフトウエア設計書
– 実機テスト

DI (Data Integrity) : データの完全性

AC	UC	DI	DC	RDF	TRE	NRA

●概要

– データに対する無許可の変更から保護するため、選択された通信チャネル上のデータの完全性を保証する機能
（データパケットの挿入や削除などの防止）

●要求事項数

合計	All	>1	>2
29	1	14	14

●主な確認対象

– ユーザ文書(マニュアル、他)
– ソフトウエア設計書
– 実機テスト

DC (Data Confidentiality) : データの機密性

AC	UC	DI	DC	RDF	TRE	NRA

- 概要
  - 情報漏洩や拡散を防ぐため、通信チャネル上の情報と、リポジトリ(データベース)上のデータの機密性を保証する機能
- 要求事項数

合計	All	>1	>2
6	1	3	2

- 主な確認対象
  - ユーザ文書(マニュアル、他)
  - ソフトウエア設計書
  - 実機テスト

RDF (Restrict Data Flow) : データフロー制限

AC	UC	DI	DC	RDF	TRE	NRA

●概要

– 不必要なデータフローを制限するため、ゾーン(領域)とコンジット(伝送路)によって制御システムを分割する機能。また、無許可の情報源の公開を防止するため、通信チャネルのデータフローを制限する機能。

●要求事項数

合計	All	>1	>2
4	1	1	2

●主な確認対象

– ユーザ文書(マニュアル、他)
– ソフトウエア設計書
– 実機テスト

TRE (Timely Response to Event) : イベントへのタイムリーなレスポンス

AC	UC	DI	DC	RDF	TRE	NRA

- ●概要
  - –インシデント自動報告機能
    - ◆ セーフティ／ミッションクリティカルな状況において、タイムリーな補正措置を自動的にとり、関係当局への通知並びに、必要なフォレンジック証拠を報告することで、セキュリティ違反に対応する
- ●要求事項数

合計	All	>1	>2
1	0	0	1

- ●主な確認対象
  - –ユーザ文書（マニュアル、他）

NRA (Network Resource Availability) : ネットワークリソースの可用性

AC	UC	DI	DC	RDF	TRE	NRA

●概要

– 重要なネットワークサービスへの DoS(サービス不能)攻撃から、全てのネットワーク資源の可用性を保証する機能

●要求事項数

合計	All	>1	>2
7	5	1	1

●主な確認対象

– ソフトウエア設計書
– ベンダーによるテストの実施記録
– 実機テスト(CRTのテスト結果)

アジェンダ

1. 制御機器認証（EDSA認証）について

- EDSA認証とは
- EDSA認証の評価項目
- EDSA 2.0.0 の体系
- 認証レベル、評価項目数
- EDSA規格のドキュメント体系（EDSA 2010.1）
- EDSA規格のドキュメント体系（EDSA 2.0.0）
- 要求事項の比較

2. 組込み機器の機能セキュリティ評価とは

- FSA-Eの概要
- 割り当て可能 (Allocatable)
- FSA-Eの主な要求事項
- 7つの機能カテゴリにおける要求事項

3. 組込み機器の開発プロセスに関する評価とは

- SDLPA/SDA-E の概要
- SDLA-312の見方

4. 最後に

- EDSA認証を受けられる方へ

3. 組込み機器の開発プロセスに関する評価とは

3. 組込み機器の開発プロセスに関する評価とは ・・・ SDLPA/SDA-Eの概要

■ 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

SDLPA： ***Security Development Lifecycle Process Assessment***

SDA-E： ***Security Development Artifacts for Embedded Devices***

【目的】

SDLPA ：組込み機器(コンポーネント)をセキュアに開発するための開発プロセスが規定されていることを監査する。

SDA-E ：SDLPAで監査した開発プロセスにもとづき開発が行われていることを監査する。

【実施内容】

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する。
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)を評価する。

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。

3. 組込み機器の開発プロセスに関する評価とは ・・・ SDLA-312の見方

- SDLPA、SDA-Eの要求事項は、SDLA-312の規格文書に書かれている。
- EDSA認証の評価対象は、“Component”欄（下図①）に「X」印の付いた項目であり、
- SDA-Eの要求内容は、“Component or System Validation Activity”欄（下図②）に記載。
- SDLPAの要求内容は、“Development Organization and SDL Validation Activity”欄（下図③）に記載。

①

②

③

SDLA-312

System	Component	Requirement ID	Requirement Name	Requirement Description	Component or System Validation Activity (Applies for Component or System Certification)	Development Organization and SDL Validation Activity (Applies for SDLA Certification. Also applies if for Component/System if organization has not been previously SDLA Certified)	Va Inde Requ
Project Management							
X	X	SDLA-SMP-1	Security Management Plan	A security management plan, which documents the plan for ensuring that security is addressed throughout the development lifecycle, shall be created as a stand alone document or as part of another plan, unless security management is already included as part of the standard software development lifecycle.	Verify a security management plan exists for the component or system	Verify that a security management plan is included as part of the standard development lifecycle and verify by reviewing examples from past or ongoing projects.	
X	X	SDLA-SMP-1.1	Identification of responsibilities	The persons, departments and organizations which are responsible for carrying out and reviewing the applicable security related activities shall be documented.	Verify that all security related activities and that those responsible for carrying out the activities are listed in the project documentation.	Verify the standard development lifecycle requires that all security related activities and those responsible for carrying out the activities are documented in a security management plan.	
X	X	SDLA-SMP-1.2	Review of security ma	If a security management plan is created it shall be reviewed ibility in the plan.	Verify the existence of review minutes with a list of action items all of which have been closed.	Verify that the security development lifecycle procedure requires a review of the security management plan.	
X	X	SDLA-SMP-1.3	Life	stablish a life-cycle model intenance of the all be documented.	Verify that the component or system was developed using the lifecycle model that is documented. This can be shown by the existence of all of the deliverables defined in the lifecycle.	Verify that the lifecycle model is documented and includes all of the required phases of the security development lifecycle.	
X	X	SDLA-SMP-1.3.1	Lifecycle Model Details	e transition between software lifecycle processes by specifying: (1) The inputs to the process, including feedback from other processes, (2) Any integral process activities that may be required to act on these inputs, (3) Availability of tools , methods, plans, and procedures.	Verify that development organization has been shown to meet this requirement (See Development Organization and SDL Validation Activity Column).	Verify that lifecycle documentation documents the inputs to each phase, the process activities within the phase, and any tools, methods, plans or procedures that should be used in the phase	
X	X	SDLA-SMP-1.3.2	Agile Lifecycle Model	The lifecyle model used may be an agile lifecyle in which multiple sprints (iterations) are done for each release.	None. This requirement does not have to be validated, but ensures that an agile lifecycle is acceptable.	None. This requirement does not have to be validated, but ensures that an agile lifecycle is acceptable.	
X	X	SDLA-SMP-1.3.2.1	Sprint Requirements	If an agile lifecycle is used, security phases may be skipped during some sprints, but each security phase must be done in at least one sprint. In this case, the security phases to be practiced for each sprint shall be documented.	If an agile method is used, confirm that the security phases to be practiced for each sprint are documented, and each phase is practiced in at least one sprint.	If an agile method is used, confirm that the required security phases to be practiced for each sprint must be documented, and that is required that each phase is practiced in at least one sprint.	
				All people involved in software development of a component or system, that has security concerns shall be given basic training			

出典）http://www.isasecure.org/Documents/SDLA-312-Sec-Dev-Lifecycle-Assess(v3_0)-(1)

SDLPA、SDA-Eの要求事項（SDLA-312）に関しては、
この後の、
『**制御システム・機器のセキュリティ開発ライフサイクル**』
のセッションでご紹介致します。

アジェンダ

1. 制御機器認証（EDSA認証）について

- EDSA認証とは
- EDSA認証の評価項目
- EDSA 2.0.0 の体系
- 認証レベル、評価項目数
- EDSA規格のドキュメント体系（EDSA 2010.1）
- EDSA規格のドキュメント体系（EDSA 2.0.0）
- 要求事項の比較

2. 組込み機器の機能セキュリティ評価とは

- FSA-Eの概要
- 割り当て可能 (Allocatable)
- FSA-Eの主な要求事項
- 7つの機能カテゴリにおける要求事項

3. 組込み機器の開発プロセスに関する評価とは

- SDLPA/SDA-E の概要
- SDLA-312の見方

4. 最後に

- EDSA認証を受けられる方へ

4. 最後に

4. 最後に ・・・ EDSA認証を受けられる方へ

- SDLA認証※を既に取得されている方

評価項目		評価
組込み機器の開発プロセスに関する評価 • セキュリティ開発ライフサイクルプロセス評価 • 組込み機器セキュリティ開発成果物	SDLPA	取得された開発プロセスに変更がなければ、実施しません
	SDA-E	実施します
組込み機器の機能セキュリティ評価	FSA-E	
組込み機器ロバストネス試験	ERT	

- SDLA認証をお持ちでない方

評価項目		評価
組込み機器の開発プロセスに関する評価 • セキュリティ開発ライフサイクルプロセス評価 • 組込み機器セキュリティ開発成果物	SDLPA	実施します
	SDA-E	
組込み機器の機能セキュリティ評価	FSA-E	
組込み機器ロバストネス試験	ERT	

- EDSA 2010.1 で認証取得済みの製品を、EDSA 2.0.0 に更新したい方

⇒ CSSC認証ラボラトリーに別途御相談ください。

※ SDLA認証については、この後の、『制御システム・機器のセキュリティ開発ライフサイクル』のセッションでご紹介致します。

【参考1】EDSA 2010.1 規格文書

FSA 規格文書（EDSA-311）

原文（英語）：EDSA-311 Functional Security Assessment

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dEDSA-311-Functional-Security-Assessment(v1_4)

対訳版（日本語）：EDSA-311 機能セキュリティアセスメント

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dJP_EDSA-311-Functional-Security-Assessment(v1_4)

SDSA 規格文書（EDSA-312）

原文（英語）：EDSA-312 Software Development Security Assessment

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dEDSA-312-Software-Development-Security-Assessment(

対訳版（日本語）：EDSA-312 ソフトウェア開発セキュリティアセスメント

http://www.isasecure.org/Documents/EDSA-312-Software-Development-Security-Assessment(

【参考2】EDSA 2.0.0 規格文書

FSA-E 規格文書（EDSA-311）

原文（英語）：EDSA-311 Functional Security Assessment

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dEDSA-311-Functional-Security-Assessment(v1_4)

対訳版（日本語）：EDSA-311 機能セキュリティアセスメント

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dJP_EDSA-311-Functional-Security-Assessment(v1_4)

SDLPA, SDA-E 規格文書（SDLA-312）

原文（英語）：SDLA-312 Security Development Lifecycle Assessment

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dSDLA-312-Sec-Dev-Lifecycle-Assess(v3_0)-(1)

ご清聴ありがとうございました。

セキュアな制御システムを世界へ未来へ

CSSCホームページ
http://www.css-center.or.jp/

CSSC説明ビデオ（日本語版）
http://www.youtube.com/watch?v=wbEiDQZU5sI&feature=youtu.be