CSSC認証ラボラトリー　ISASecure EDSA認証 説明会

ISASecure EDSA FSA/SDSA説明

2014年1月15日

CSSC認証ラボラトリー 評価員
奥村 剛, CISSP

アジェンダ

- 概要
- EDSA標準のドキュメント体系とFSA/SDSA要求事項
- FSA
  - FSA: Functional Security Assessment
  - 割り当て可能(allocatable)
  - FSAの主な要求事項
  - 要求事項数と実機テスト数
  - 各機能カテゴリ説明
- SDSA
  - SDSA: Software Development Security Assessment
  - SDSAの主な要求事項
  - 要求事項数
  - フェーズ一覧
  - 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
  - 各フェーズ説明
- 最後に

概要

- FSA: Functional Security Assessment (EDSA-311)
  - 対象機器のセキュリティ機能のアセスメント
  - EDSA-311の要求事項に沿って、対象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
  - 実機テスト
    - 一部要求事項については、実機を用いて実際に動作を確認する
- SDSA: Software Development Security Assessment (EDSA-312)
  - 対象機器のソフトウェア開発プロセスのアセスメント
  - 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)
- EDSA情報
  - ISASecure Webサイト

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

EDSAの体系

◆SDSA、FSA、CRTの3つを評価することで、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

ISASecure

EDSA

ソフトウェア開発セキュリティ評価（SDSA）

機能セキュリティ評価（FSA）

通信ロバストネス試験（CRT）

体系的な設計不良の検出と回避

- ベンダのソフトウェア開発とメンテナンスのプロセス監査
- 堅牢（robust）で,セキュアなソフトウェア開発プロセスを当該組織が守っていることを評価する。

※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 / 実装漏れの検出

- 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

- コンポーネントのロバストネス（堅牢性）について試験
- 奇形や無効な形式のメッセージを送り、脆弱性等を分析

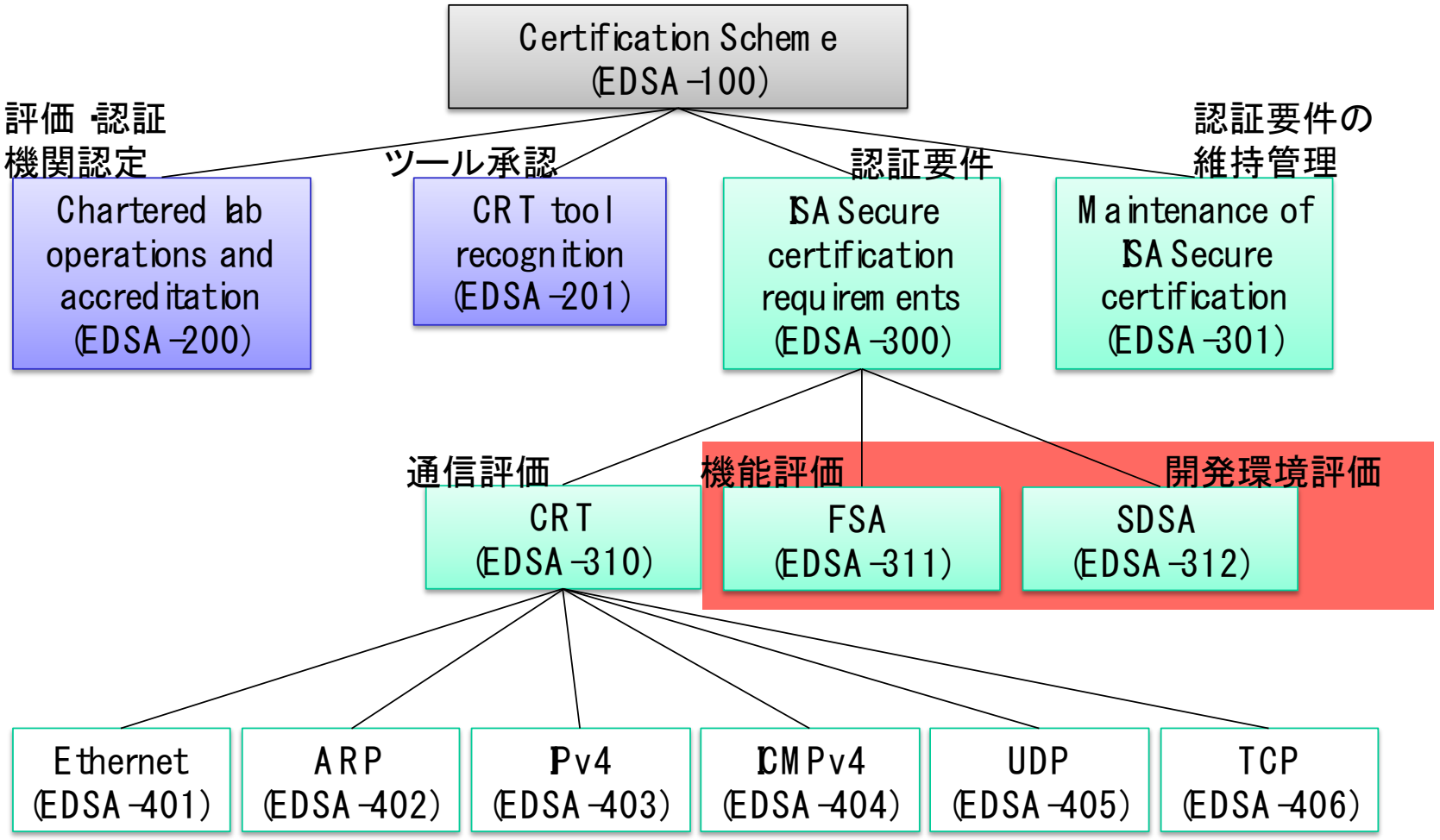
※セキュリティレベルによらず、評価項目数は同一

EDSA：Embedded Device Security Assurance

Communication Robustness Testing(CRT), Functional Security Assessment (FSA), Software Development Security Assessment(SDSA)

出典:「ISA Security Compliance Institute （ISCI） and ISASecure™及びhttp://www.css-center.or.jp/sympo/2013/documents/sympo20130528-article.pdf

EDSA標準のドキュメント体系とFSA/SDSA要求事項



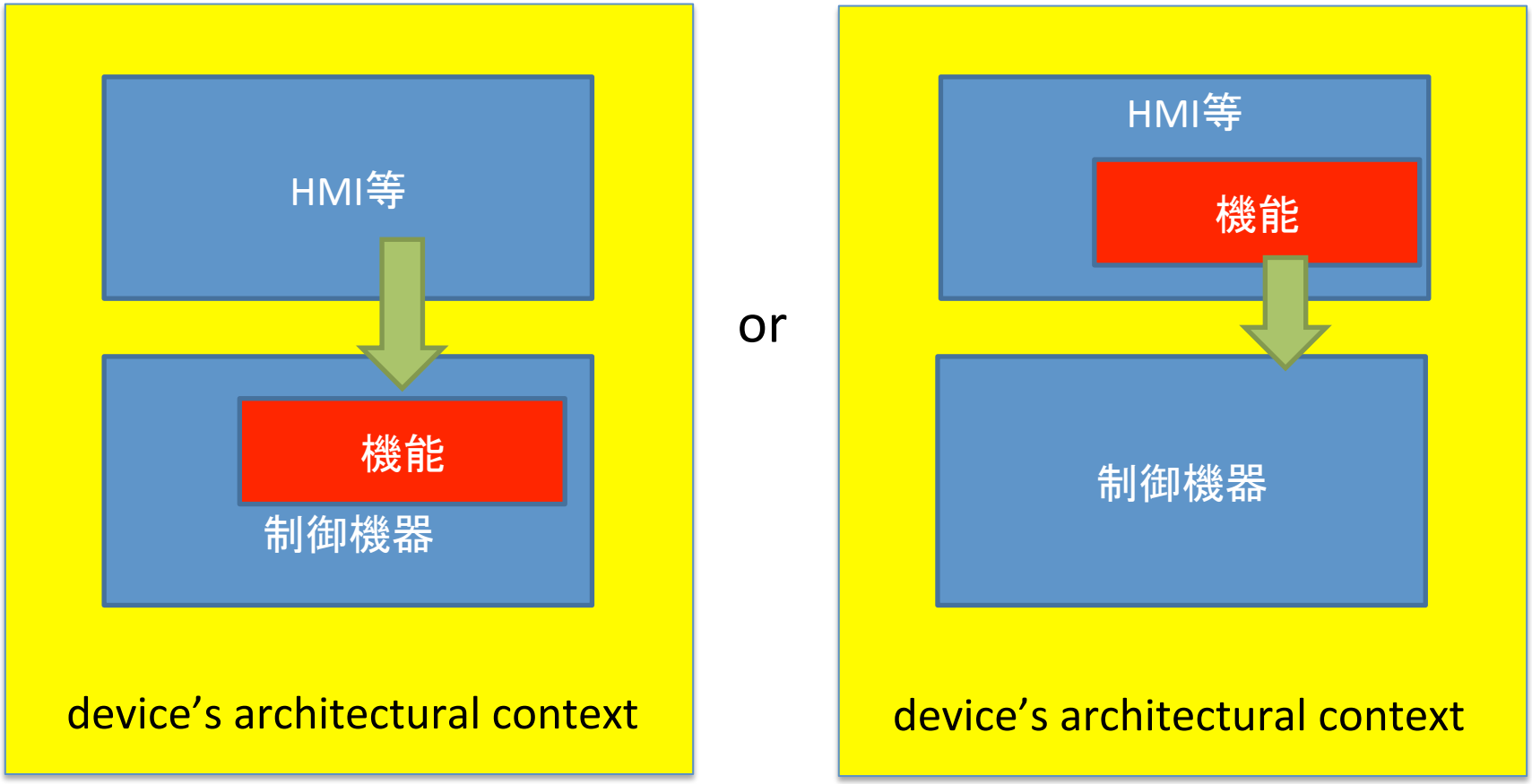
◇ IPAにより翻訳されたEDSA標準の対訳版はISCIウェブサイトにて公開。
http://isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspx

FSA

FSA: Functional Security Assessment

- 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
- 要求事項
  - 7つの機能カテゴリと83個の要求事項(機能、設定等)
  - ISASecure レベルに応じて、満たすべき要求事項の数は異なる
- 割り当て可能(Allocatable)
  - 要求事項の一部は、対象デバイスの周辺機器(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

割り当て可能（allocatable）



制御機器(コントローラ)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

FSAの主な要求事項

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 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

FSA要求事項数と実機テスト数

大項目	合計	All	>1	>2	Not required
AC(Access Control): アクセスコントロール	23	10	6	6	1
UC(Use Contorol):使用コントロール	13	2	4	7	0
Data Integrity (データの完全性)	29	1	14	14	0
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
	83	20	29	33	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 Contorol):使用コントロール	10	1	3	6
Data Integrity (データの完全性)	17	1	8	8
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

●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	(Not required)
23	10	6	6	1

●主な確認対象

–ユーザ文書(マニュアル、他)

–実機テスト

UC (Use Control) : 使用コントロール

●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

- 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

- 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

●概要

– 不必要なデータフローを制限するため、ドメイン(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

●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

- 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)

SDSA

SDSA: Software Development Security Assessment

- 目的
  - 対象製品の開発プロセスがセキュアに行われていることを監査する
- 要求事項
  - 12の活動フェーズと各フェーズに対する合計 169個の要求事項
  - ISASecure レベルに応じて、満たすべき要求事項の数は異なる
- V字モデル(V-Model)適用
  - ソフトウェア開発プロセスが V字モデルになっていることを前提として構成
  - 既存製品のモデルチェンジ開発への適用には注意が必要

SDSAの主な要求事項

セキュリティ管理プロセス(SMP: Security Management Process)	This phase specifies a process for planning and managing security development activities to ensure that security is designed into a product. For example, this phase incorporates requirements that the development team have a security management plan and that the developers assigned to the project are competent and have been provided basic training in good security engineering practices and processes. Also includes requirements that the project team creates and follows a configuration management plan.
セキュリティ要求事項仕様(SRS: Security Requirements Specification)	Most vulnerabilities and weaknesses in software intensive information systems can be traced to inadequate or incomplete requirements. This phase requires that the project team document customer driven security requirements, security features and the potential threats that drive the need for these features.
ソフトウェアアーキテクチャ設計(SAD: Software Architecture Design)	Software architecture facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects. This phase requires the project team develop a top-level software design and ensures that security is included in the design.
セキュリティリスクアセスメントと脅威のモデル化(SRA: Software Risk Assessment and Threat Modeling)	This phase requires the project team determine which components can affect security and plan which components will require security code reviews and security testing. Also requires that a threat model be created and documented for the product.
詳細ソフトウェア設計(DSD: Detailed Software Design)	This phase requires the project team design the software down to the module level following security design best practices.
セキュリティ指針文書(DSG: Document Security Guidelines)	This phase requires the project team create guidelines that users of the product must follow to ensure security requirements are met.
モジュールの実装と検証(MIV: Module Implementation & Validation)	This phase requires the project team implement design by writing code following security coding guidelines. It ensures that software modules are implemented correctly by conducting security code reviews, static analysis and module testing.
セキュリティ統合テスト(SIT: Security Integration Testing)	This phase requires that the project team perform security specific tests such as fuzz testing and penetration testing.
セキュリティプロセス検証(SPV: Security Process Verification)	This phase requires an independent assessment that all required software development processes have been followed
セキュリティ対応計画(SRP: Security Response Planning)	This phase requires the project team establish a process to be able to quickly respond to security issues found in the field if and when they happen.
セキュリティ検証テスト(SVT: Security Validation Testing)	This phase requires that the project team confirm that all security requirements have been met preferably by test or by analysis.
セキュリティ対応実行(SRE: Security Response Execution)	This phase requires the project team respond to security problems in the field by taking action to both preventative and corrective action.

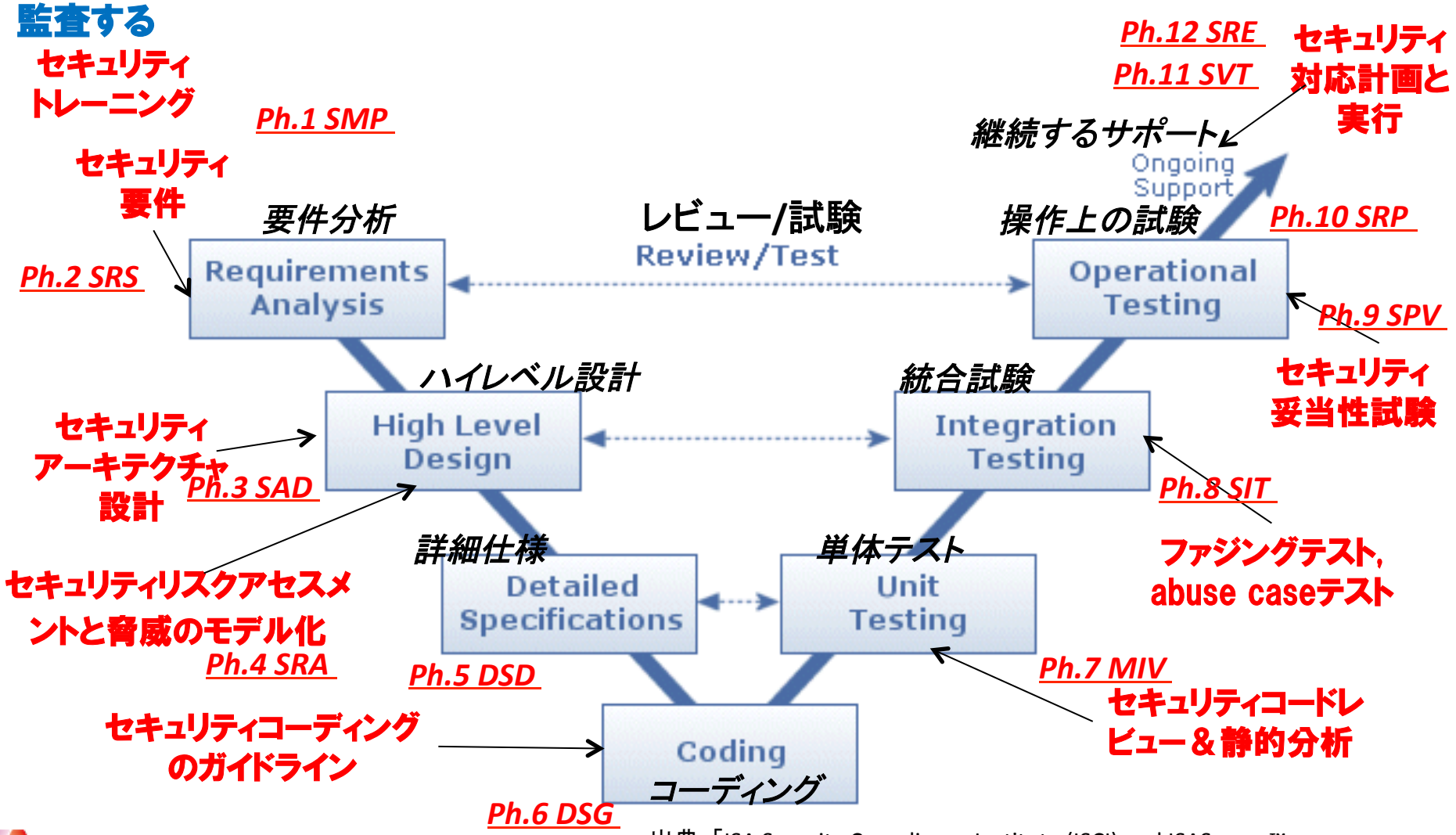
出典：ICSJWG Spring 2011, (ASCI) 「Validating the Security Assurance of Industrial Automation Products

活動フェーズ一覧

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）

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

SDSAでは、開発プロセスのV字モデルに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する



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

SDSA要求事項数

大項目	合計	All	>1	>2
SMP:Security Management Process	37	24	6	7
SRS:Security Requirements Specification	13	13	0	0
SAD:Software Architecture Design	10	8	1	1
SRA:Software Risk Assessment and Threat Modeling	15	15	0	0
DSD:Detailed Software Design	9	3	2	4
DSG:Document Security Guidelines	19	19	0	0
MIV:Module Implementation&Verification	20	2	10	8
SIT:Security Integration Testing	8	8	0	0
SPV:Security Process Verification	10	10	0	0
SRP:Security Response Planning	15	15	0	0
SVT:Security Validation Testing	8	8	0	0
SRE:Security Response Execution	5	5	0	0
	169	130	19	20

セキュリティ管理プロセス（SMP: Security Management Process）

●概要
- 製品に対して確実にセキュリティが設計されるようにセキュリティ開発を管理するアクティビティを計画する。

●要求事項数

合計	All	>1	>2
37	24	6	7

●主な確認対象
- ソフトウエア開発プロセス標準、レビュー実施要領
- セキュリティ管理計画書
- 構成管理計画書、および構成管理システム
- リリース規程
- 開発体制図、要員計画書
- 能力管理手順書、教育計画書、教育実施履歴、スキルマップ
- 上記に対するレビューの記録

セキュリティ要求仕様（SRS: Security Requirements Specification）

- 概要
  - ユーザ主導のセキュリティ要件、セキュリティ機能、およびこれらの機能の必要性を高める潜在する脅威を文書化する。
- 要求事項数

合計	All	>1	>2
13	13	0	0

- 主な確認対象
  - セキュリティ要求仕様書（または、それと同等のもの）
  - 上記に対するレビューの記録

ソフトウェアアーキテクチャ設計 (SAD: Software Architecture Design)

- 概要
  - 最上位のソフトウェア設計。セキュリティが設計に組み込まれるように保証する。
- 要求事項数

合計	All	>1	>2
10	8	1	1

- 主な確認対象
  - ソフトウエアアーキテクチャ設計書
  - 上記に対するレビューの記録

セキュリティリスクアセスメント/脅威のモデル化 (SRA: Security Risk Assessment Threat Modeling)

- 概要
  - どのコンポーネントがセキュリティに影響する可能性があるか判断する。
  - どのコンポーネントで脅威分析、セキュリティコードのレビュー、およびセキュリティテストが必要になるかを計画する。
- 要求事項数

合計	All	>1	>2
15	15	0	0

- 主な確認対象
  - 脅威モデル、および脅威モデル更新履歴(または更新ポリシー)
  - 脅威リスト
  - データフロー図
  - セキュリティノート
  - セキュリティ設計レビュー計画
  - 不正使用事例テスト計画
  - 上記に対するレビューの記録

詳細ソフトウェア設計（DSD: Detailed Software Design）

●概要

– セキュリティ設計のベストプラクティスに従いソフトウェア設計をモジュールレベルに詳細化する。

●要求事項数

合計	All	>1	>2
9	3	2	4

●主な確認対象

– ソフトウエア詳細設計書

– 上記に対するレビューの記録

セキュリティ指針文書（DSG: Document Security Guidelines）

●概要

– 製品のユーザが確実にセキュリティ要件を満たすために従う必要のあるガイドラインを作成する。

●要求事項数

合計	All	>1	>2
19	19	0	0

●主な確認対象

– 以下の情報がドキュメント化されていること
  ◆ユーザ向けセキュリティガイドライン
  ◆アプリケーション開発者向けセキュリティガイドライン
  ◆運用と保守のためのインストラクション
  ◆セキュリティツール
– 上記に対するレビューの記録

モジュールの実装と検証（MIV: Module Implementation &Verification）

- 概要
  - セキュリティコーディングガイドラインに従ってコードを記述することで設計を実装する。
  - ソフトウェアモジュールが正しく実装されるように確保する。
  - セキュリティコードのレビュー、静的分析、およびモジュールテストが含まれる。
- 要求事項数

合計	All	>1	>2
20	2	10	8

- 主な確認対象
  - コーディング標準
  - コードレビューチェックリスト、およびコードレビューの記録
  - 静的解析実施報告書
  - モジュール試験仕様書、および結果報告書
  - COTS(Commercial Off-The-Shelf:汎用市販)オペレーティングシステム

セキュリティ統合テスト（SIT: Security Integration Testing）

●概要
– ファジングや侵入テストなどのセキュリティ固有のテストを実行する。

●要求事項数

合計	All	>1	>2
8	8	0	0

●主な確認対象
– (ファジング、不正使用等の事例を含む)テスト計画書、および結果報告書
– 上記に対するレビューの記録

セキュリティプロセス検証（SPV: Security Process Verification）

●概要
- –ソフトウェア開発プロセスを検証する（振り返る）。

●要求事項数

合計	All	>1	>2
10	10	0	0

●主な確認対象
- –セキュリティアセスメント計画書
- –製品開発時の体制図(アセッサーの独立性を示すため)
- –脅威モデルのレビュー記録
- –バグ追跡システム、バグ管理票等とその運用
- –未修正のバグの承認記録

セキュリティ対応計画（SRP: Security Response Planning）

- 概要
  - (リリース後に)フィールドでセキュリティ問題が発生した場合、その問題に迅速に対応できるようにプロセスを整備する。
- 要求事項数

合計	All	>1	>2
15	15	0	0

- 主な確認対象
  - 脆弱性報告窓口(Webサイト上などに明記されているか）
  - セキュリティ管理計画書(体制図や連絡体系、対策の判断基準等)
  - 脆弱性修正プロセス標準(インプット-処理-アウトプット)

セキュリティ検証テスト (SVT: Security Validation Testing)

- 概要
  - すべてのセキュリティ要求事項が問題なく満たされていることを分析又はテストによって確認する。
- 要求事項数

合計	All	>1	>2
8	8	0	0

- 主な確認対象
  - ソフトウエア妥当性確認テスト計画書
  - ソフトウエア妥当性確認テスト結果報告書

セキュリティ対応実行（SRE: Security Response Execution）

●概要
- フィールドでのセキュリティ問題への対応を実行する。
- 修正措置と予防的措置の両方を講じる。

●要求事項数

合計	All	>1	>2
5	5	0	0

●主な確認対象
- (パッチ等の)リリース規程
- セキュリティ脆弱性対応規程(修正と予防)

最後に

FSA/SDSA受審のために

- 脅威モデルと管理計画
  - 製品のユースケースに基づいた脅威モデルの設定
  - 脅威モデルの分析により、セキュリティ管理計画を策定
  - 設定したモデルや対策の網羅性、妥当性チェック
- PDCAサイクルの徹底
  - 上記セキュリティ管理モデルに基づく開発プロセスの実行
  - プロセスが確実に実行されていることのレビュー
- 情報開示
  - ユーザがセルフアセスメントできること
- 人材育成
  - セキュリティに関する専門知識を有する人材育成
  - 専門性に関する妥当性を示す基準(資格、職務経験等)
- 経営層のコミットメント
  - セキュリティ対策の重要性の認識
  - 環境変化に対応した開発プロセスの導入

ご清聴ありがとうございました

参考:CERT C/C++セキュアコーディングスタンダード

JPCERT CC® Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

- セキュアコーディングとは、プログラムの実装(コーディング)段階で、脆弱性を作り込まない、あるいは作り込まれた脆弱性を検出し修正する取組みや手法である。CERT C / C++ セキュアコーディングスタンダードは、脆弱性に直接つながる製品の弱点となるコードや、セキュリティ品質に関わるコーディングを特定し、セキュアで品質の高いコードを作成するためのコーディング規約としてまとめられている。
- 全てのルールに準拠する必要はなく、各ルールに設定された優先度に基づき、組織や開発プロジェクトに合わせてカスタマイズして利用することが可能である。このCERT C / C++ セキュアコーディングスタンダードを導入することで、以下の実現が期待できる。
  - より高品質でセキュアな製品開発
  - 発生しうる攻撃リスクの把握
  - コードのセキュリティ品質を評価する指標のひとつとして活用
  - 2014年度より開始が予定されているEDSA認証の要求事項の一部への対応

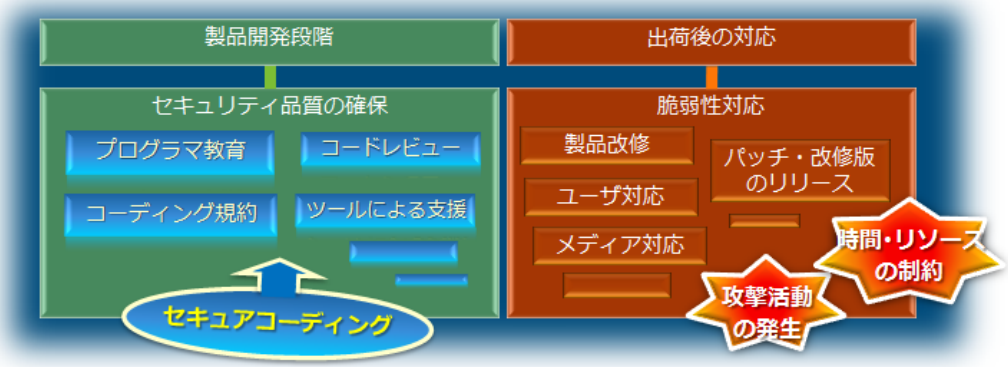


図１：製品へのセキュリティ対策導入タイミングがもたらす効果の違い

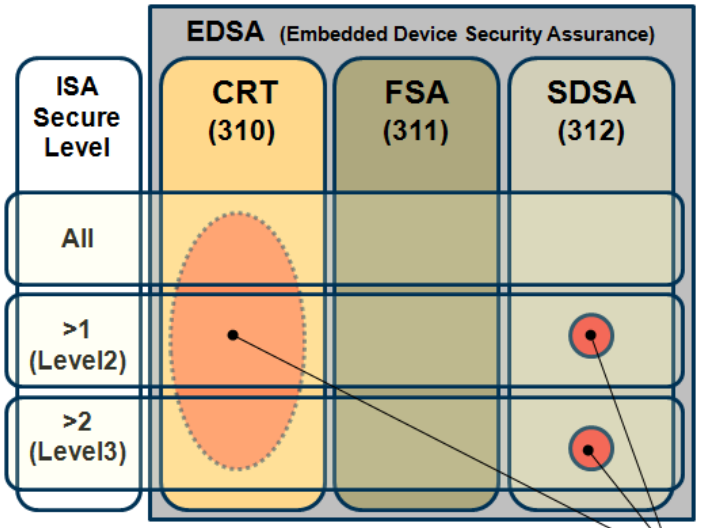


図２：CRTとSDSAの要求事項の一部充足が期待できる

CERT セキュアコーディングスタンダードは、C / C++ / Java の3種類を提供中
詳細情報: https://www.jpcert.or.jp/securecoding.html
本件に関する連絡先:secure-coding@jpcert.or.jp