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 SDLA説明
「制御システム・機器のセキュリティ開発ライフサイクル」

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

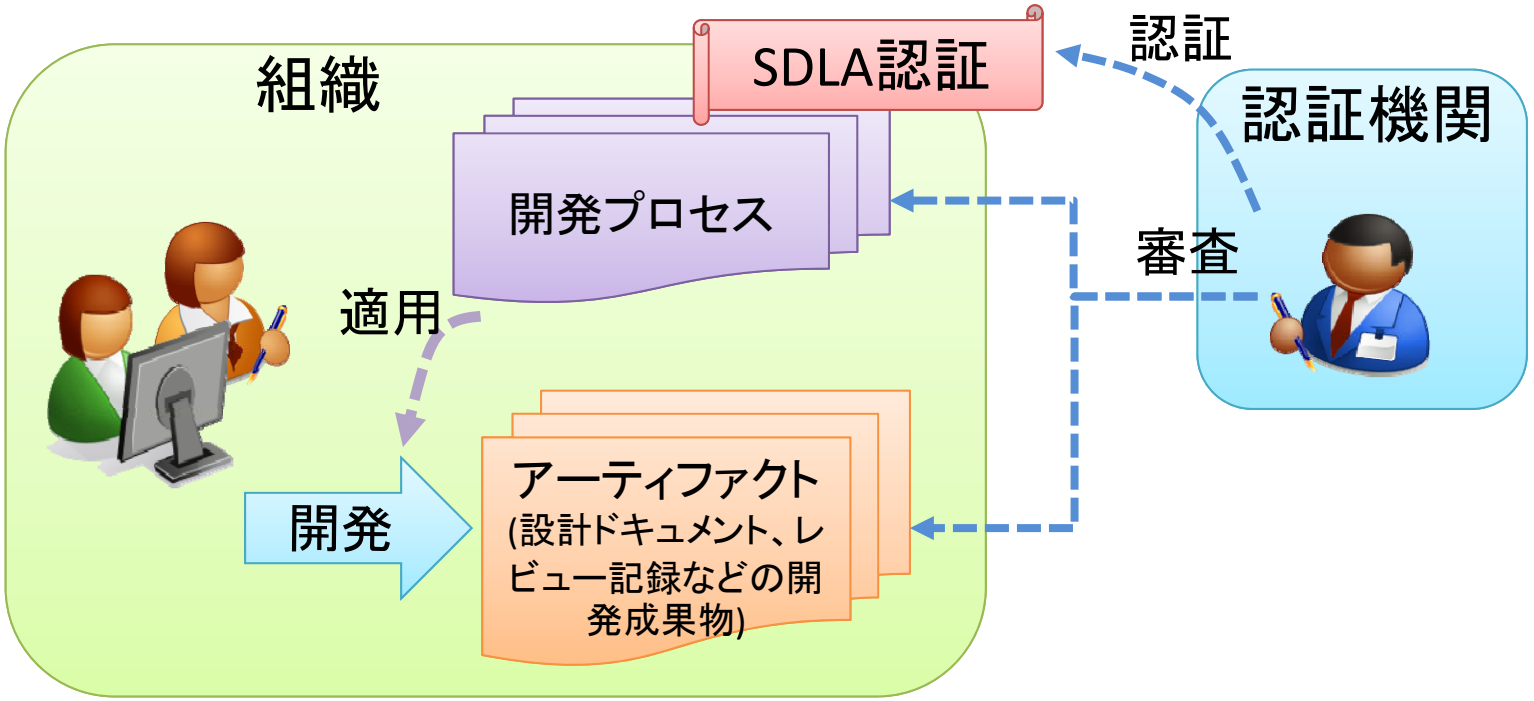
研究員　穂積 徹也 (CISSP)

目次

- SDLA認証とは　(Security Development Lifecycle Assurance)
- 開発プロセスの適用先
- SDLA認証とEDSA認証(V2.0.0)
- SDLA認証とSSA認証
- SDLA認証の有効期間
- SDLA認証を複数製品に適用する例
- SDLA認証のドキュメント体系
- SDLA審査のフロー
- SDLA要求事項

SDLA認証とは （Security Development Lifecycle Assurance）

- 組織のセキュリティ開発プロセスを評価する
  - セキュアなコンポーネントまたはシステムを開発するための開発プロセスが規定(文書化)されていること
  - 当該開発プロセスにもとづき開発が行われていること （アーティファクトを確認)
  - レベルは１～４の４段階



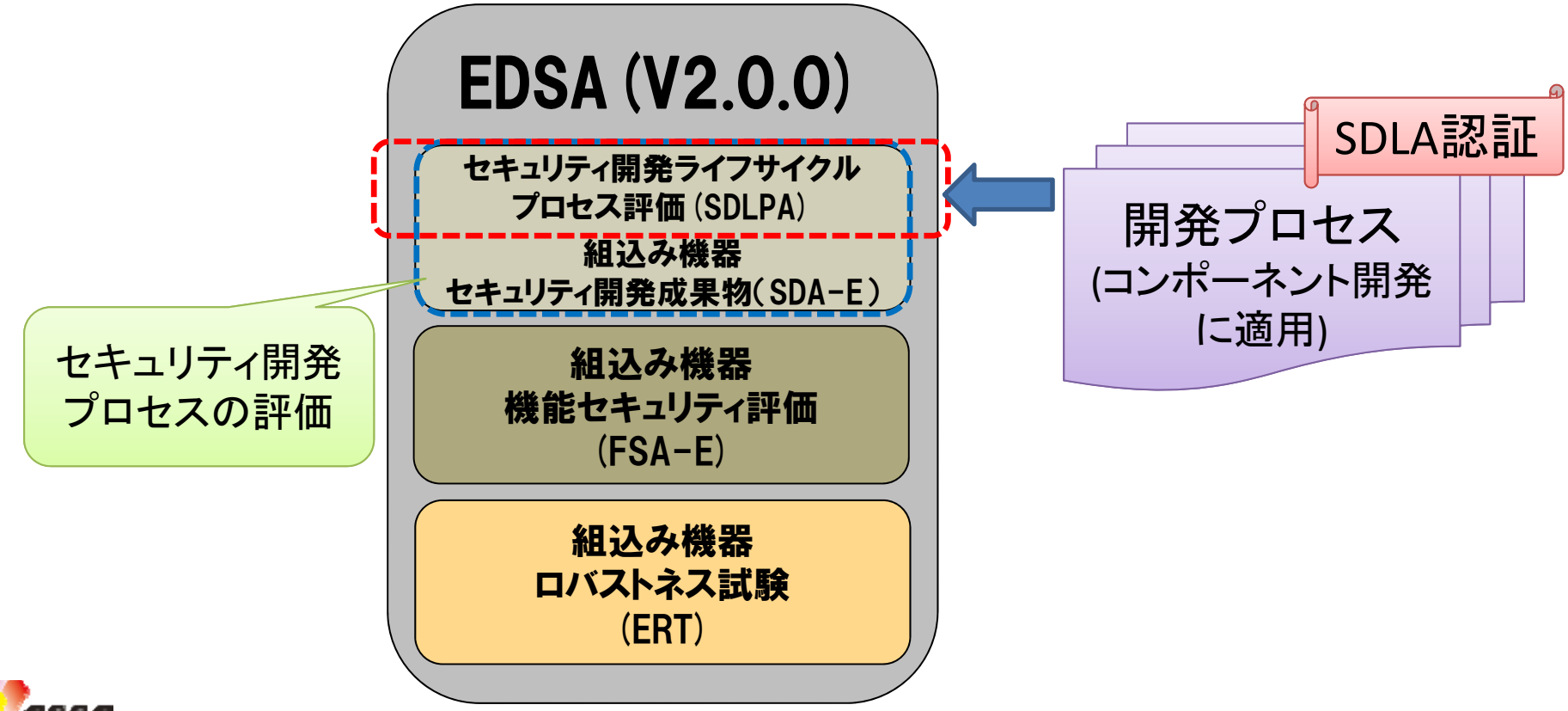
開発プロセスの適用先

- 組織は開発プロセスの適用先を規定する必要がある
  - コンポーネントの開発に適用する (EDSA認証)
  - システムの開発に適用する (SSA認証)
  - コンポーネントの開発とシステムの開発の両方に適用する

- 開発プロセスを適用する製品の範囲を規定する必要がある
  - 特定製品に適用する
  - 全てに適用する

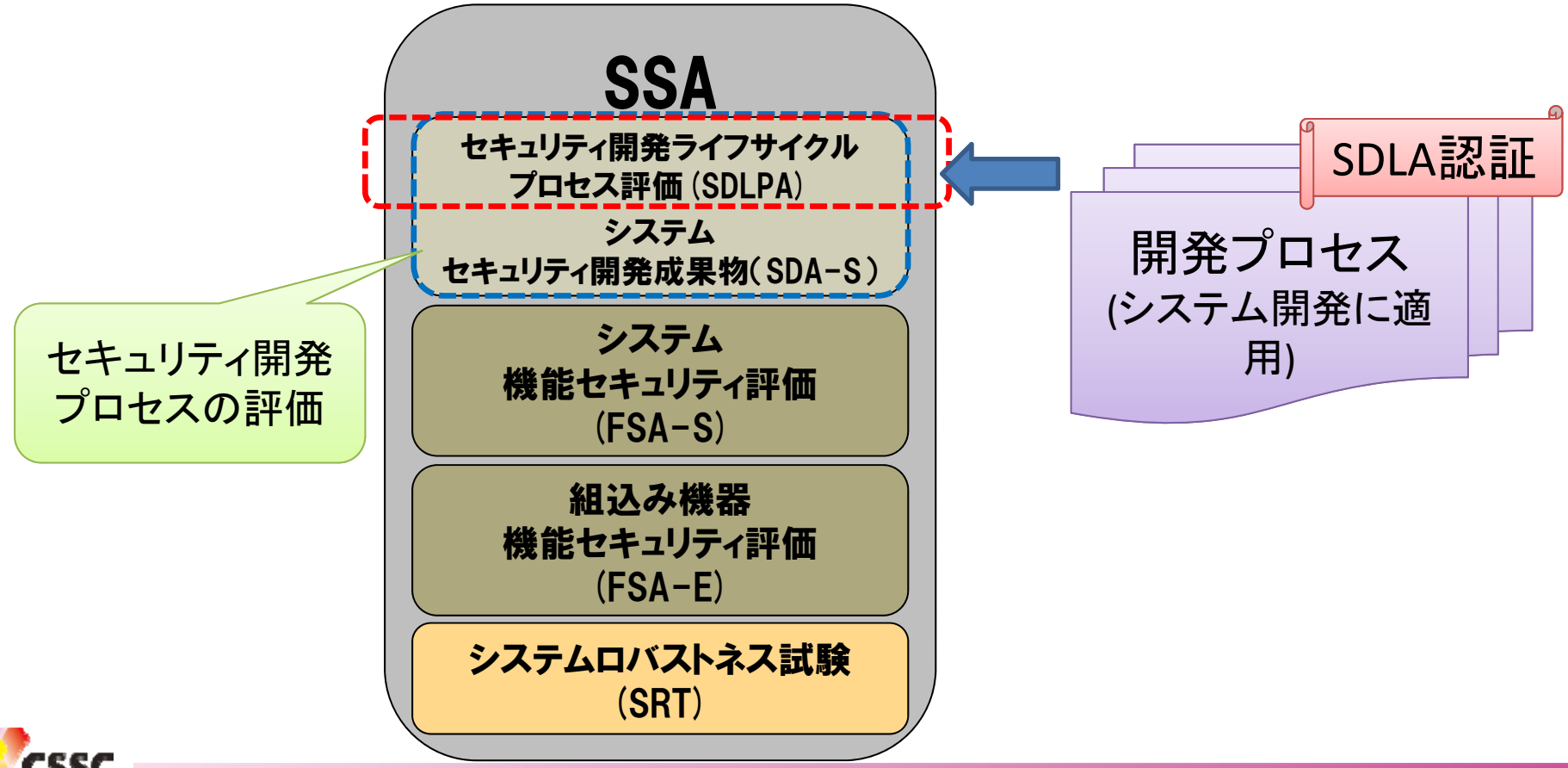
SDLA認証とEDSA認証 (V2.0.0)

- 対応するレベルのSDLA認証を取得していれば、EDSA認証(V2.0.0)におけるセキュリティ開発ライフサイクルプロセス評価(SDLPA)は、SDLA認証によって適合と評価される
  - EDSA認証の審査時にSDLA認証を取得することも可能



SDLA認証とSSA認証

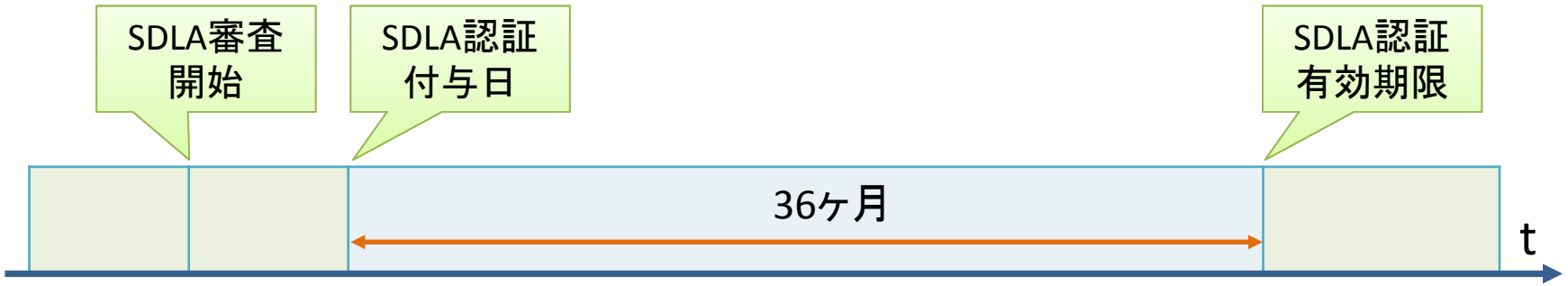
- 対応するレベルのSDLA認証を取得していれば、SSA認証におけるセキュリティ開発ライフサイクルプロセス評価(SDLPA)は、SDLA認証によって適合と評価される
  - SSA認証の審査時にSDLA認証を取得することも可能



SDLA認証の有効期間

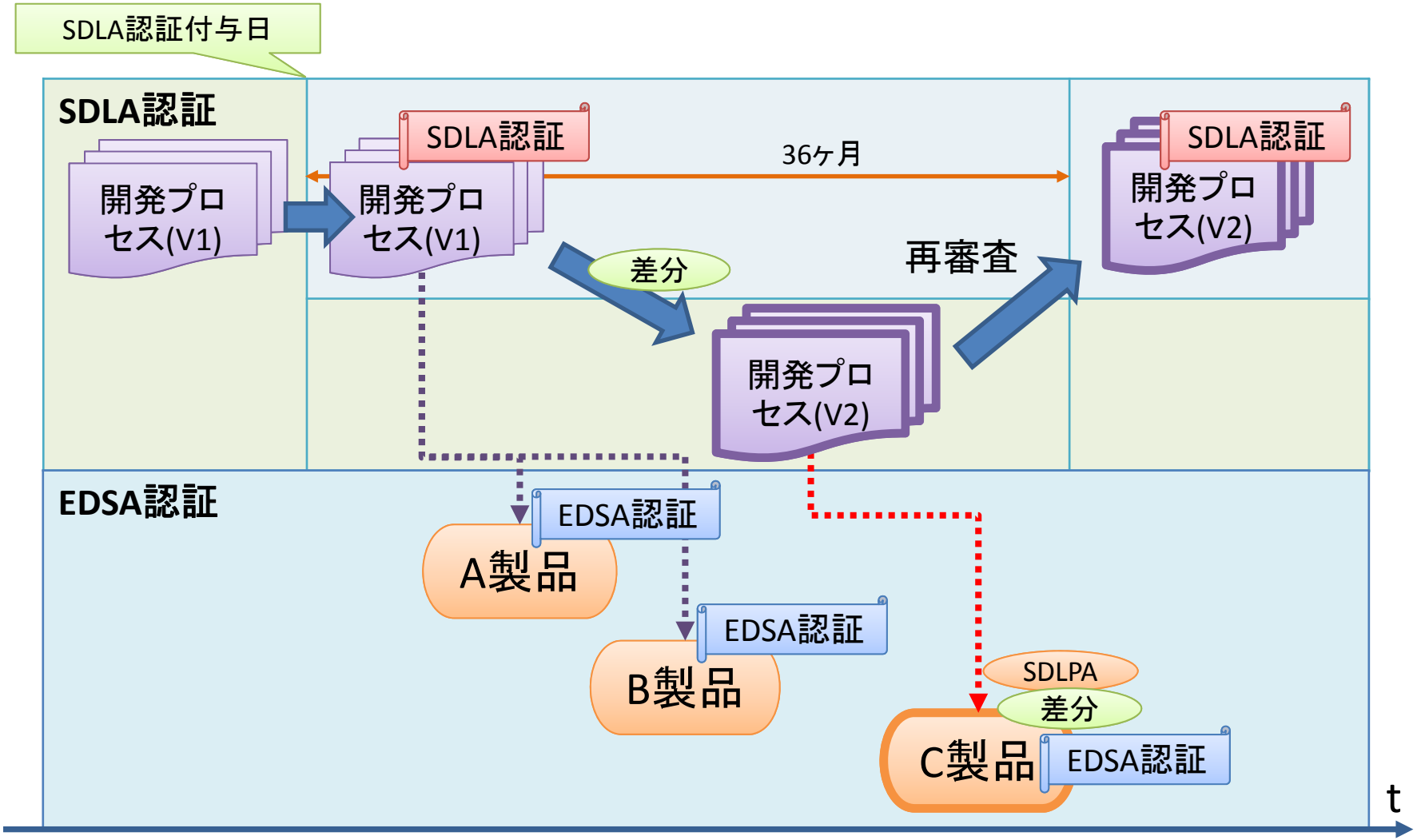
●SDLA認証には有効期間(認証付与日から36ヶ月)が存在する

– 有効期間の延長は、有効期間内に再認証審査を受ける必要がある



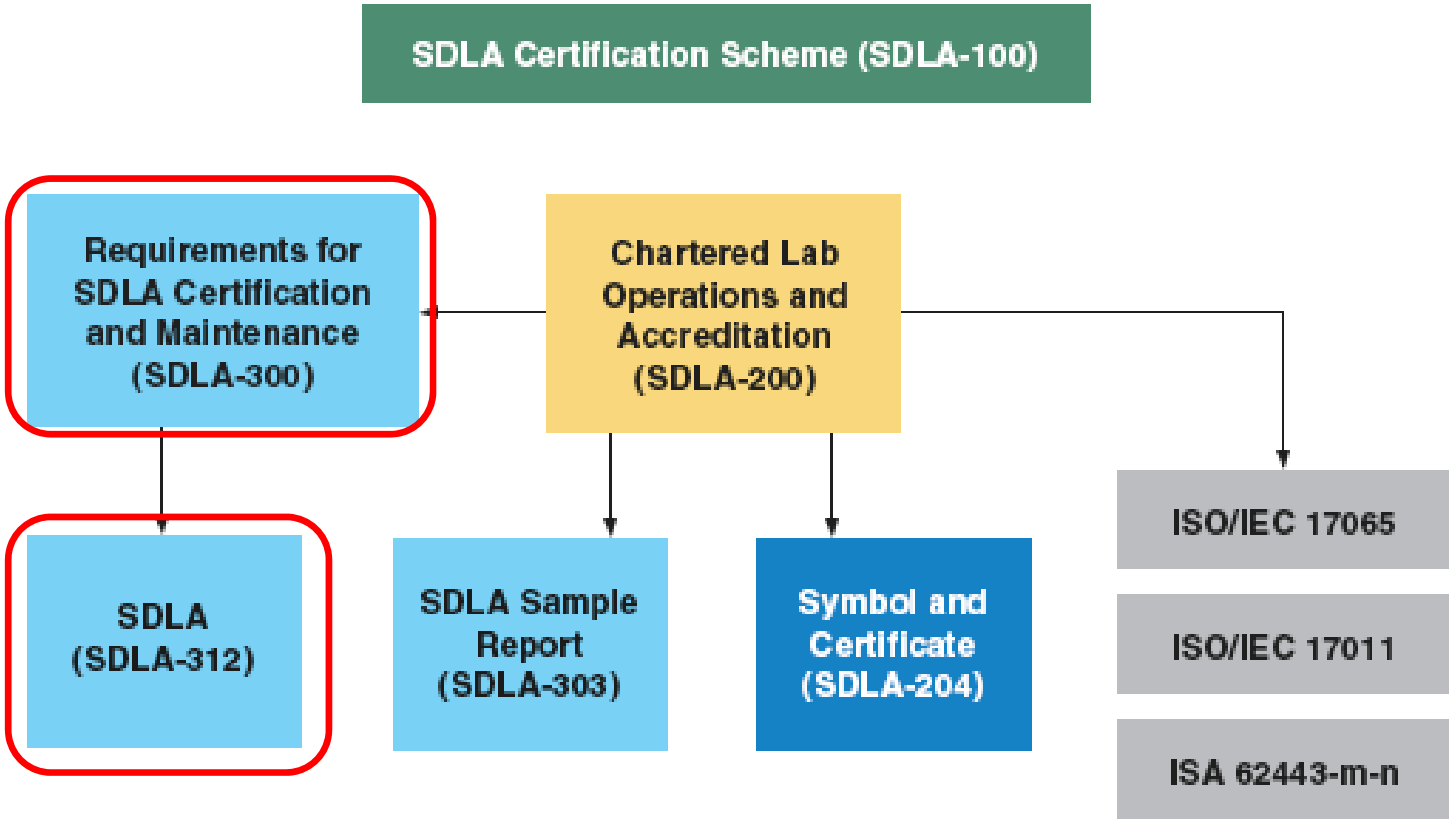
※EDSA認証、SSA認証には有効期間は存在しない

SDLA認証を複数製品に適用する例



コンポーネント開発の場合(EDSA認証)

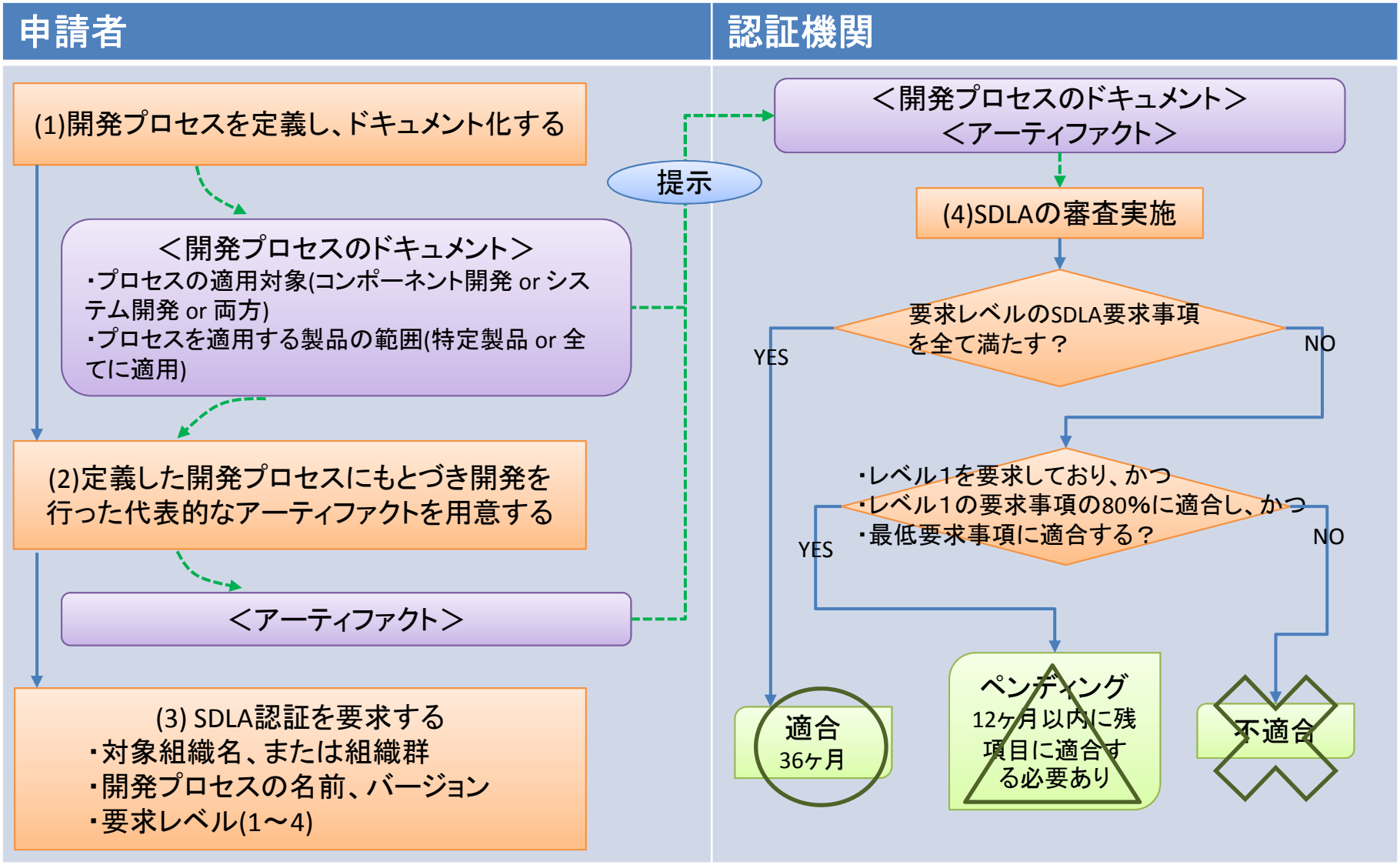
SDLA認証のドキュメント体系



出典：http://www.isasecure.org/Certification/SDLA-Certification

Figure 1 - ISASecure SDLA Documents

SDLA審査のフロー


申請者
認証機関
(1)開発プロセスを定義し、ドキュメント化する
＜開発プロセスのドキュメント＞
・プロセスの適用対象(コンポーネント開発 or システム開発 or 両方)
・プロセスを適用する製品の範囲(特定製品 or 全てに適用)
(2)定義した開発プロセスにもとづき開発を行った代表的なアーティファクトを用意する
＜アーティファクト＞
(3) SDLA認証を要求する
・対象組織名、または組織群
・開発プロセスの名前、バージョン
・要求レベル(1～4)
提示
＜開発プロセスのドキュメント＞
＜アーティファクト＞
(4)SDLAの審査実施
要求レベルのSDLA要求事項を全て満たす？
YES
NO
・レベル1を要求しており、かつ
・レベル1の要求事項の80%に適合し、かつ
・最低要求事項に適合する？
YES
NO
適合
36ヶ月
ペンディング
12ヶ月以内に残項目に適合する必要あり
不適合

SDLA認証の要求事項　…概要

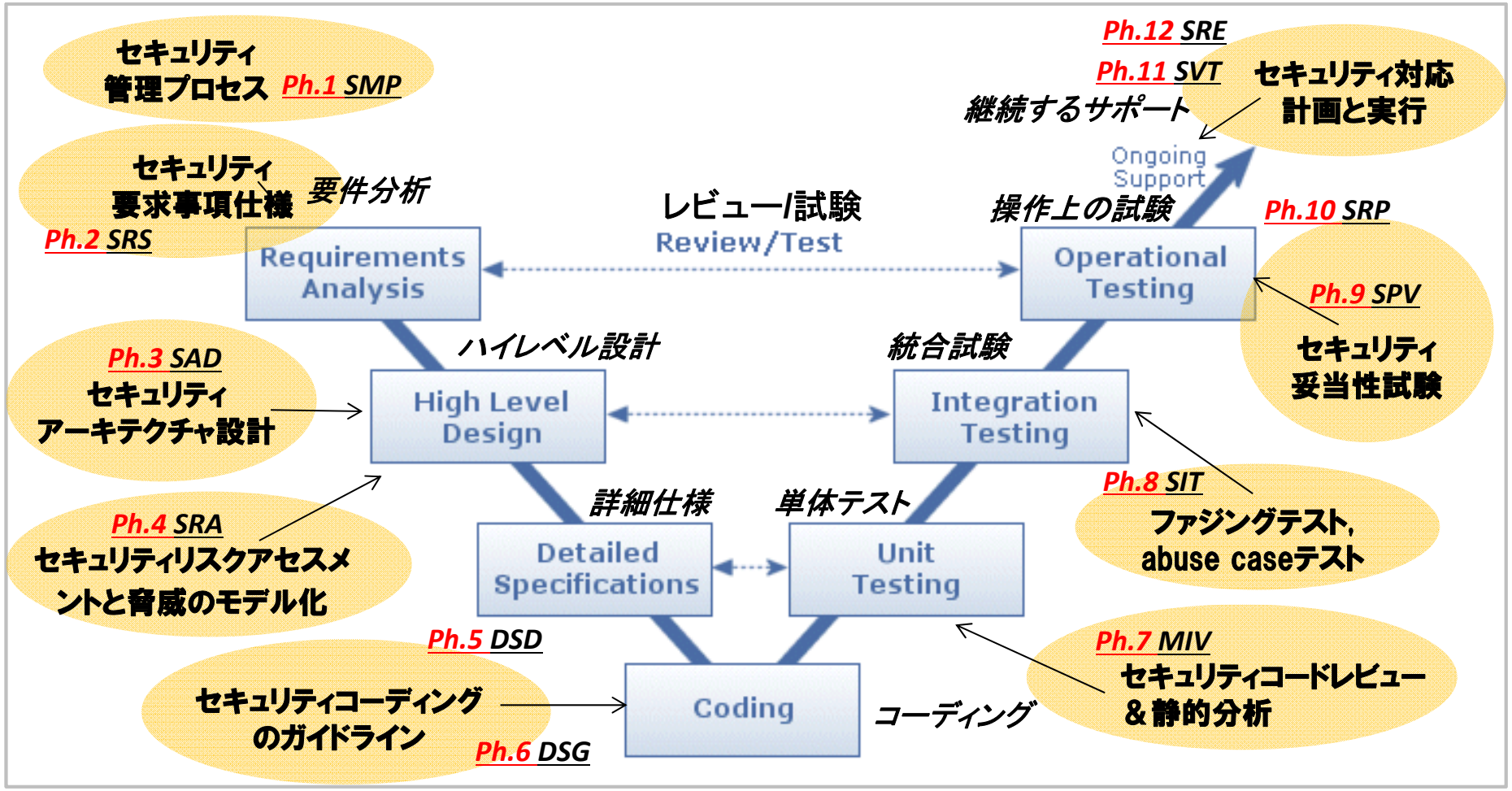
- 要求事項
  - 現行EDSA(2010.1)のSDSA(Software Development Security Assessment)の要求事項と類似
  - 12の活動フェーズと各フェーズに対する要求事項で評価される
    - 要求事項はSDLA-312で定義される
  - 4段階のISASecure レベルと、コンポーネントとシステムのどちらに適用するかに応じて、満たすべき要求事項の数は異なる(最大174項目)

SDLA認証の要求事項　…活動フェーズ

番号	活動フェーズ
PH1	セキュリティ管理プロセス (SMP)
PH2	セキュリティ要求仕様 (SRS)
PH3	セキュリティ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	セキュリティ妥当性確認 (SVT)
PH12	セキュリティ対応実行 (SRE)

SDLA認証の要求事項　…開発プロセスと活動フェーズ

SDLAでは、例えば、下図に示す開発プロセスのV字モデルに従った活動フェーズが開発プロセスに組み込まれていることを監査する。



SDLA認証の要求事項　…レベルごとの要求事項数

活動フェーズ	合計	ALL	>1	>2	>3
セキュリティ管理プロセス (SMP)	37(39)	25(26)	6(6)	6(7)	0
セキュリティ要求仕様 (SRS)	13(13)	13(13)	0	0	0
セキュリティアーキテクチャ設計 (SAD)	9(11)	9(10)	0(1)	0	0
セキュリティリスクアセスメントと脅威のモデル化(SRA)	14(14)	14(14)	0	0	0
詳細ソフトウェア設計 (DSD)	10(10)	3(3)	2(2)	5(5)	0
セキュリティ指針文書 (DSG)	19(19)	19(19)	0	0	0
モジュールの実装と検証 (MIV)	19(19)	3(2)	9(10)	7(7)	0
セキュリティ統合テスト (SIT)	11(11)	11(11)	0	0	0
セキュリティプロセス検証 (SPV)	10(10)	10(10)	0	0	0
セキュリティ対応計画 (SRP)	15(15)	15(15)	0	0	0
セキュリティ妥当性確認 (SVT)	8(8)	8(8)	0	0	0
セキュリティ対応実行 (SRE)	5(5)	5(5)	0	0	0
	170(174)	135(136)	17(19)	18(19)	0

システム(コンポーネント)

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

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●概要

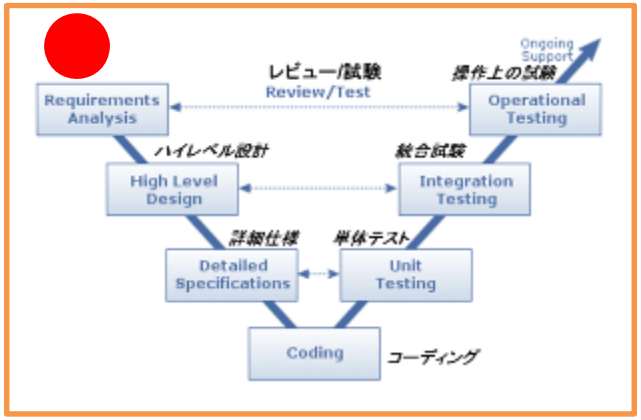
– コンポーネントまたはシステムに対して確実にセキュリティが設計されるように、セキュリティ開発を管理するアクティビティを計画する。

●要求事項数

合計	All	>1	>2	>3
37(39)	25(26)	6(6)	6(7)	0

●主な確認対象

– ソフトウェ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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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。

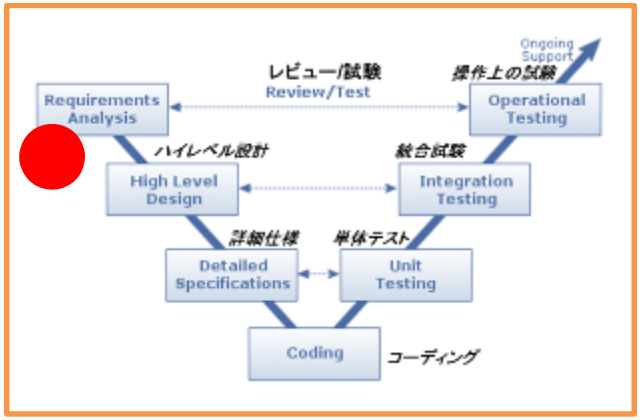
●要求事項数

合計	All	>1	>2	>3
13(13)	13(13)	0	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



セキュリティアーキテクチャ設計（SAD: Software Architecture Design）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●概要

– 最上位のソフトウェアまたはシステムの設計。セキュリティが設計に組み込まれるように保証する。

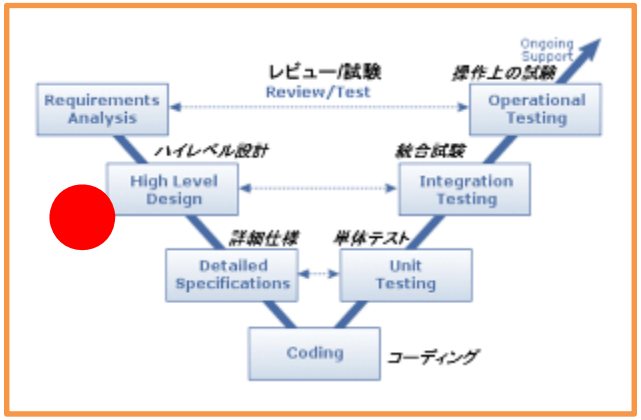
●要求事項数

合計	All	>1	>2	>3
9(11)	9(10)	0(1)	0	0

●主な確認対象

– ソフトウェ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と脅威のモデル化 (SRA: Security Risk Assessment Threat Modeling)

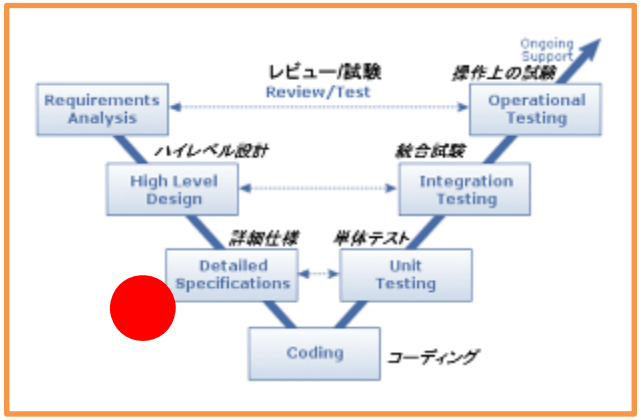
SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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を判断する。
- 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	>3
14(14)	14(14)	0	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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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またはシステムの設計をモジュールまたはゾーンレベルに詳細化する。

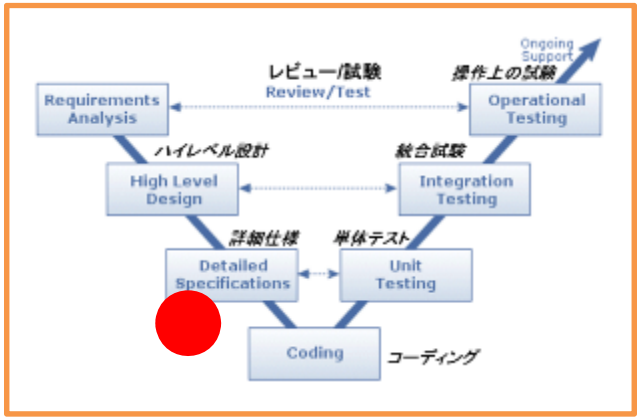
●要求事項数

合計	All	>1	>2	>3
10(10)	3(3)	2(2)	5(5)	0

●主な確認対象

– ソフトウェア詳細設計書

– 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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●概要

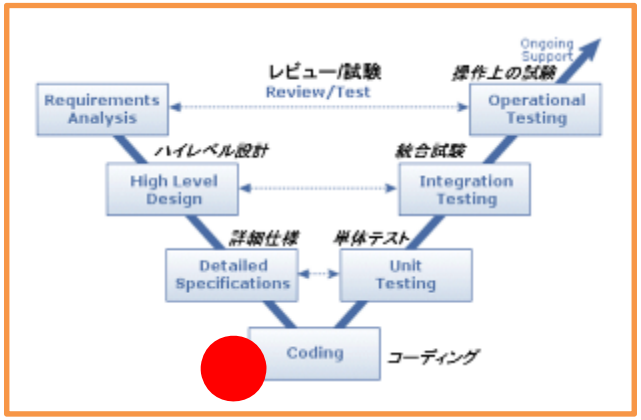
– セキュリティ要求事項を確実に満たすためにコンポーネント又はシステムのユーザ及びアドミニストレータが従う必要がある指針を作成する。

●要求事項数

合計	All	>1	>2	>3
19(19)	19(19)	0	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）

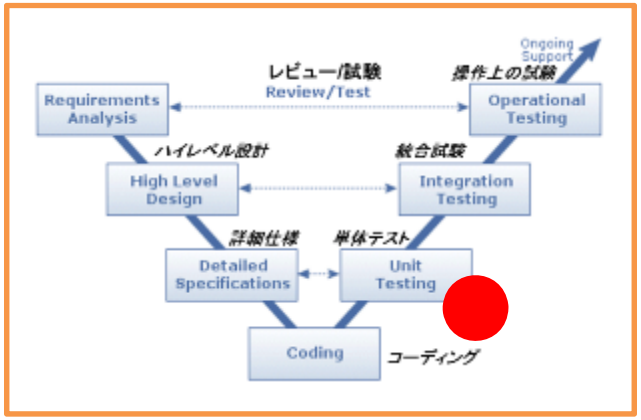
SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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又はゾーンが確実に正しく実装されるようにする。
- セキュリティコードのレビュー、静的解析、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	>3
20(20)	3(2)	9(10)	7(7)	0

●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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●概要

– ファズテスト、悪用テスト、及び脆弱性識別テストなどのセキュリティ固有のテストを実行する。

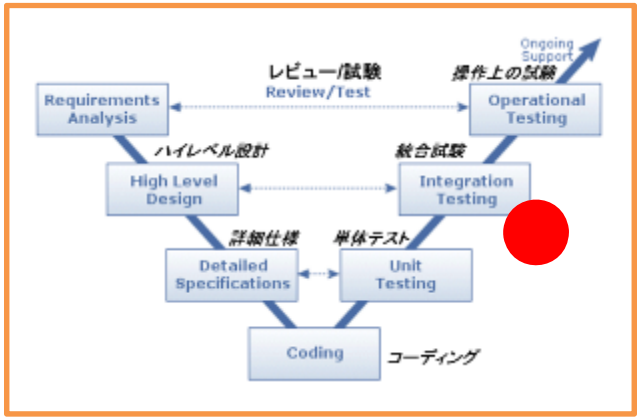
●要求事項数

合計	All	>1	>2	>3
11(11)	11(11)	0	0	0

●主な確認対象

– 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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●概要

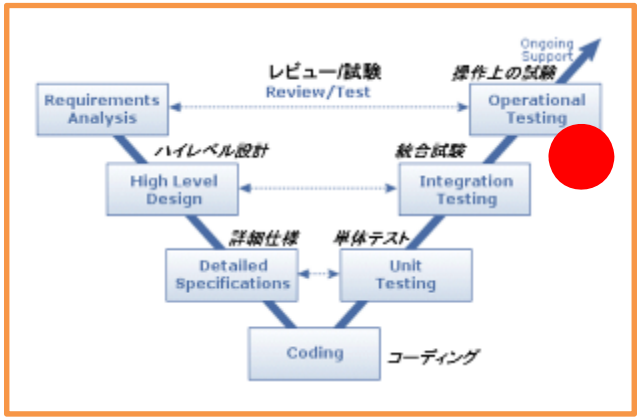
– ソフトウェアまたはシステムの開発プロセスを検証する（振り返る）。

●要求事項数

合計	All	>1	>2	>3
10(10)	10(10)	0	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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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

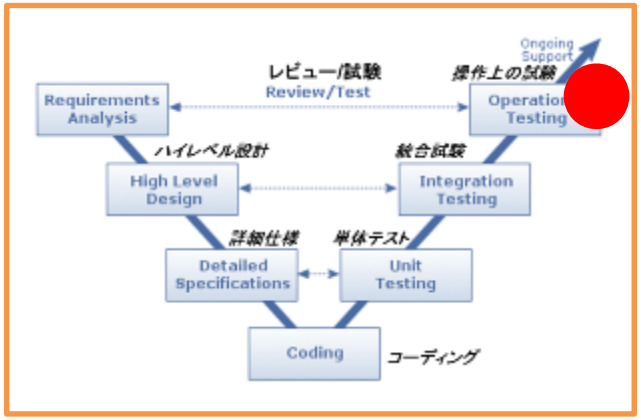
合計	All	>1	>2	>3
15(15)	15(15)	0	0	0

●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)



セキュリティ妥当性確認 (SVT: Security Validation Testing)

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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テストまたは解析によって確認する。

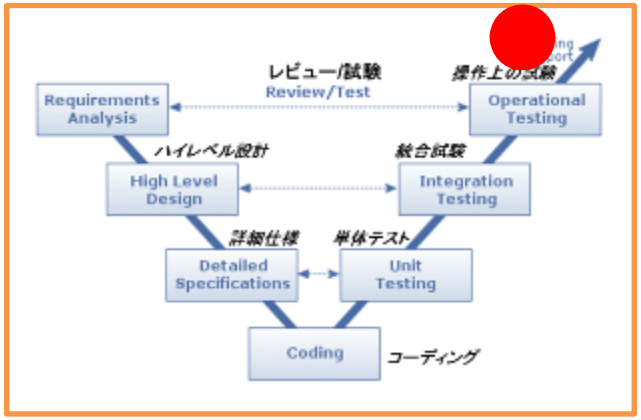
●要求事項数

合計	All	>1	>2	>3
8(8)	8(8)	0	0	0

●主な確認対象

– 妥当性確認テスト計画書

– 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）

SMP	SRS	SAD	SRA	DSD	DSG	MIV	SIT	SPV	SRP	SVT	SRE

●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。

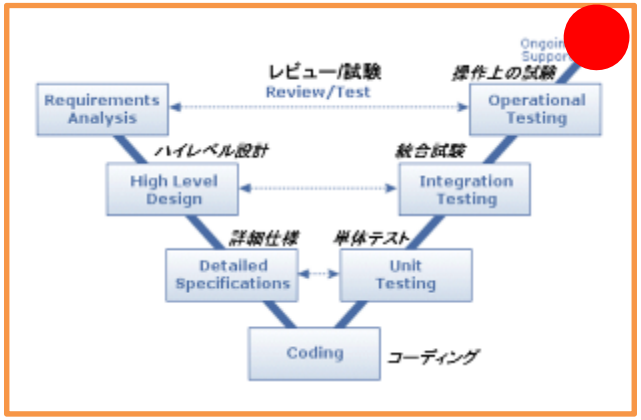
●要求事項数

合計	All	>1	>2	>3
5(5)	5(5)	0	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)



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

技術研究組合
制御システムセキュリティセンター
Control System Security Center

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