情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

セキュリティ要求分析・保証の統合手法CC-CaseとIoTセキュリティ

2017.5.24

金子　朋子

自己紹介

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

金子朋子
博士（情報学）
公認情報セキュリティ監査人（CAIS)
独立行政法人情報処理推進機構（ＩＰＡ）SEC研究員

情報セキュリティ大学院大学　田中研究室客員研究員
　博士課程前期　2009年修了
　博士課程後期　2013年修了

日本ネットワークセキュリティ協会(JNSA)
優秀論文賞受賞（2015年）

研究テーマ：
セキュア開発方法論、セーフティ&セキュリティ開発、品質保証

目次

- 研究の背景と目的
  - セキュリティ・バイ・デザイン
- CC-Caseの目的・定義
- 関連知識
  - アシュアランケース・セーフティとセキュリティ
  - コモンクライテリア(CC)
- CC-Caseの特徴
  - 可視化・保証
- CC-Caseの有効性実験
- まとめと今後の方向性

➢研究の背景と目的

セキュリティ・バイ・デザイン

研究の背景と目的

より巧妙化する脅威に対して，より安全なソフトウェアを開発するにはどうしたらよいか？

解決方法

- 開発者に対する教育と訓練
- 経験の伝達
- プロジェクト管理の徹底
- 運用管理の向上
- セキュリティ方針の厳密化

開発方法論・プロセス

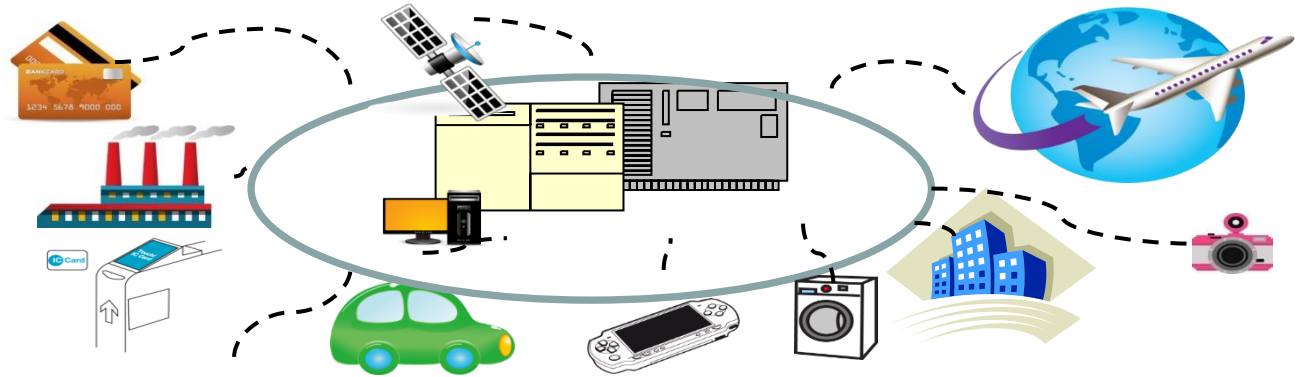
CC-Caseで提案

システム・ソフトウェアの仕組みの中に脅威への対抗手段を含めることがより根本的な対策になりうるから
：セキュリティ・バイ・デザインの発想

IoTの特徴と開発の課題

IoT：モノのインターネット（Internet of Things）
IoTの特徴：多様な機器・システムがつながること
IoT開発→より複雑なセキュリティ要件をもつことになる。
　　セキュリティが不安。

設計がまとまってから、セキュリティの対処を検討していいの？



IoTセキュリティの現状

IoTシステムへの脅威事例は日増しに増加

- HDDレコーダーの踏み台化は情報家電に対する初期の攻撃事例（2004年）
- 心臓ペースメーカの不正操作（2013年）
- Jeepを車載のインフォメーションシステムを経由してインターネットから操作できる研究（2013年）
- スマホでATMから現金を引き出すウイルス（2014年）
- Black Hat
  - HW／組込み，IoT，スマートグリッド／インダストリ・IoT関連テーマがカテゴリに登場

  →IoTハッキング技術を身につけ，実践をはじめるハッカーが増加

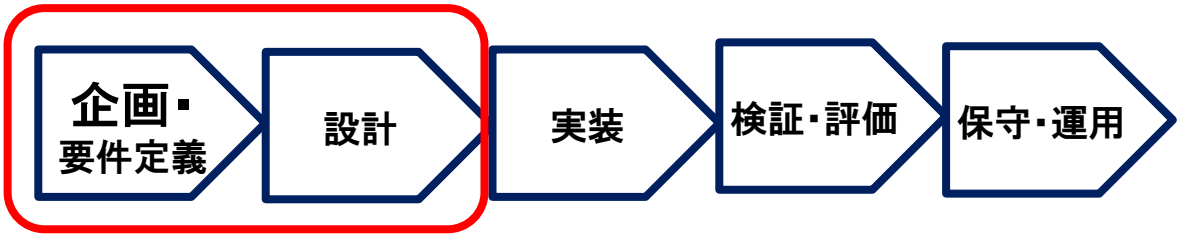
IoTセキュリティの課題

- 対象が情報だけでなく，実体を伴うモノになるため．与える被害も致命的であり，攻撃の被害は甚大にならざるを得ない→IoTセキュリティの確保は重大事
- IoTセキュリティの対象となる機器やシステムに対する脅威には盗聴や不正アクセスによる情報漏えいやプライバシー侵害，データやソフトウェア改ざんによる誤動作や予期せぬ停止など，様々なものが想定される
- 事故の発生や顧客の信頼失墜，機器交換・システム改修コストなど多大な損害も懸念
- 業界，製品・システムごとに要件が異なるため，セキュリティの対応レベルが異なり，標準化の動向も異なっている
- IoTのセキュリティを確保するための技術や手法，標準，基準はまだ確立されていない

脅威となる対象の洗い出し・目標を設定するセキュリティ要求分析手法・リスク評価の手法，要件を可視化する技術が必要）

セキュリティ・バイ・デザインの定義(NISC)

「情報セキュリティを企画・設計段階から確保するための方策」



”情報セキュリティ”でなく、”セキュリティ”とすればIoT製品やサービスにも適用できると考えられる。

安全なIoT システムのためのセキュリティに関する一般的枠組

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

平成28年8月26日

内閣サイバーセキュリティセンター

1.目的

IoT(Internet of Things)システムについては、モノが接続されることから、IT と物理的システムが融合したシステムとして捉える必要があり、同システムが提供するサービスには、従来の情報セキュリティの確保に加え、新たに安全確保が重要となる。また、将来、個々のシステムが相互に接続されることを見据え、システム相互間の接続が新たな脆弱性となる懸念があることを踏まえ、セキュリティ・バイ・デザイン(Security by Design)の思想で設計、構築、運用されることが不可欠

3. 基本原則

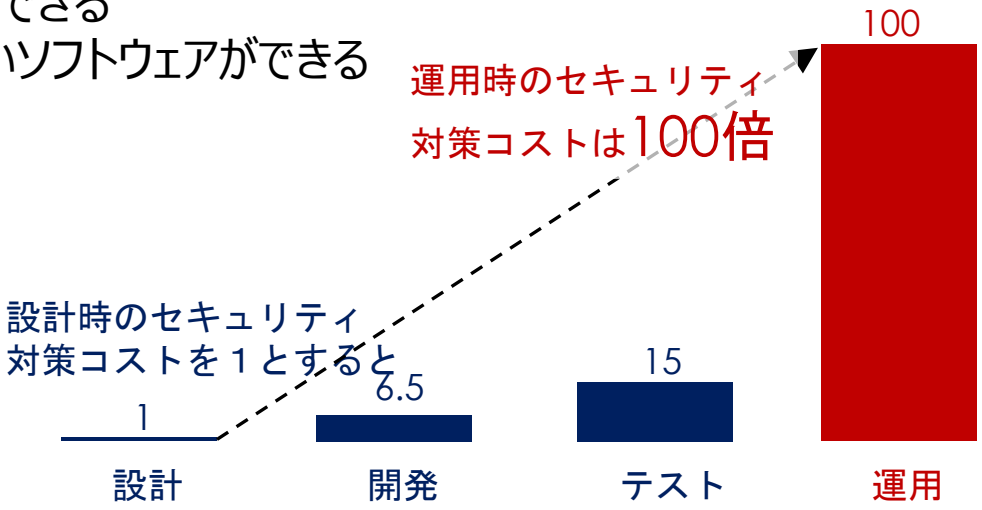
IoT システムの設計・構築・運用に際しては、セキュリティを事前に考慮するセキュリティ・バイ・デザインを基本原則とし、これが確保されていることが当該システムの稼働前に確認・検証できる仕組みが求められる。

セキュリティ・バイ・デザインのメリット①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

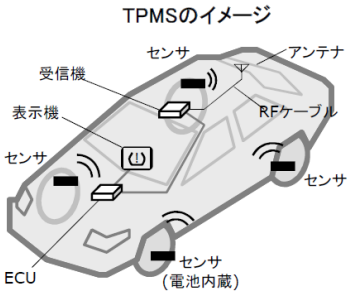
開発の早い段階から入れ込むので、

①手戻りが少なく納期を守れる
②コストも少なくできる
③保守性の良いソフトウェアができる



IPA資料「セキュリティ・バイ・デザイン入門」より

セキュリティ・バイ・デザインのメリット②



米国ではTREAD法によりタイヤ空気圧監視システム
TPMS （Tire Pressure Monitoring Systems）の）装着が2007年から完全義務化。
・南カリフォルニア大とラトガーズ大は、TPMSのプロトコル解析に成功、近傍の車両の無線通信と区別するため、車輪毎に32bitの固有IDが割当てられていることを発見。
・車輪IDを読み出すことで、車両を追跡したり、誤った情報の送信により誤った警告灯の表示が可能。
攻撃ツールの開発に要した原価は$1,500程度。

セーフティの観点から設計すると車輪毎の固有ID付与は妥当だが、
セキュリティの観点からは車両の追跡や誤った警告灯の表示という脅威を生む。

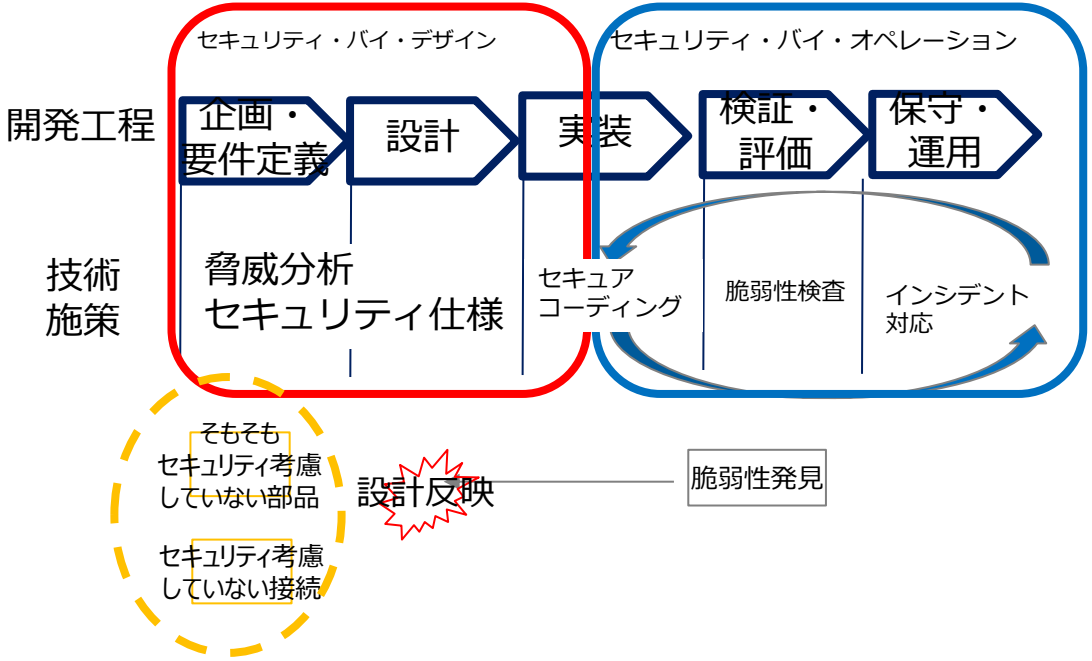
CCDS資料より引用

問題の解決には、統合的観点でのセキュリティ・バイ・デザインが必要

設計思想の転換

セキュリティ・バイ・デザイン

- 企画・要件定義段階からのセキュリティ考慮（→セキュリティ・バイ・デザイン）がなければ、セキュリティの根本的な解決にはつながらない。

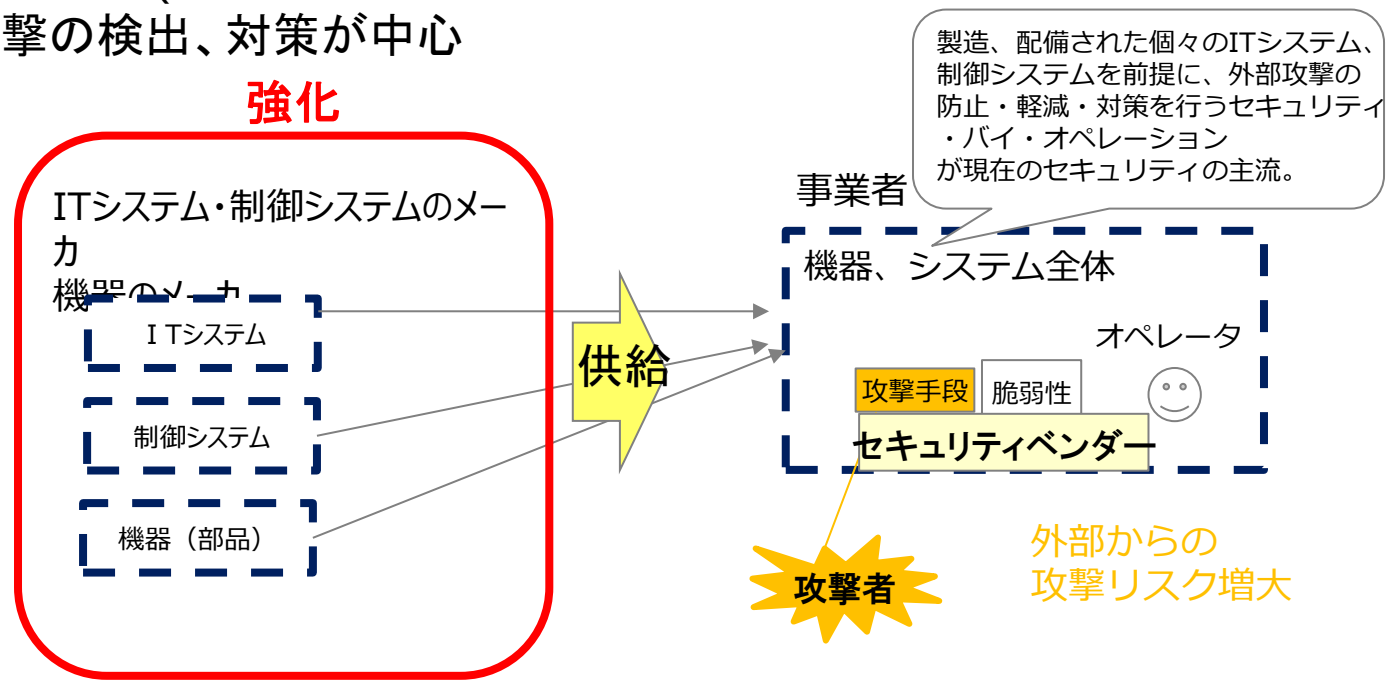


セキュリティの現状

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

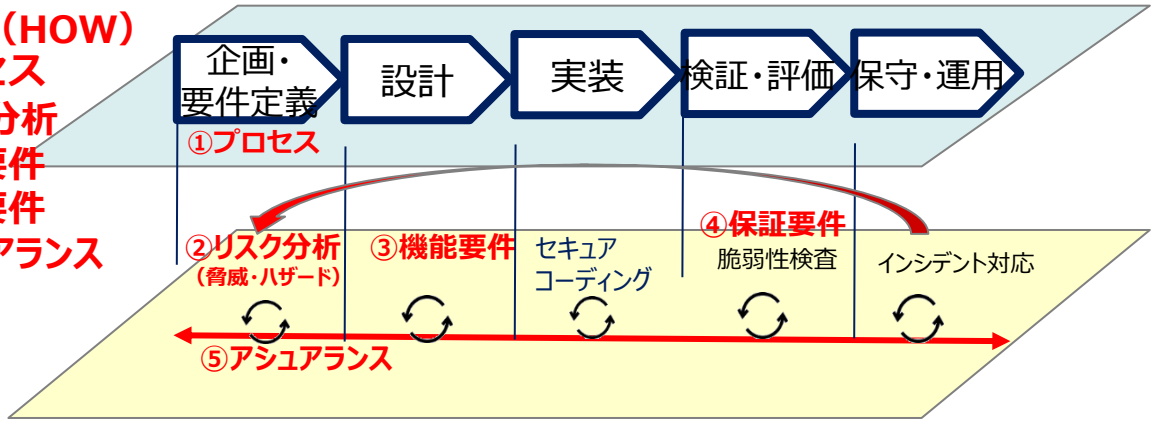
IoTでは（これまで隔離されてきたプラント含め）ネットワーク接続が前提、外部からの攻撃リスク増大

ユーザ (事業者）サイドでのセキュリティ対策は、運用段階での攻撃の検出、対策が中心



- **セキュリティ・バイ・デザインのために必要なもの（WHAT）**
  - ①セキュリティ要件の可視化
  - ②セキュリティ機能の確実な設計・実装
  - ③セキュリティの保証

- **必要な技術（HOW）**
  - **①プロセス**
  - **②リスク分析**
  - **③機能要件**
  - **④保証要件**
  - **⑤アシュアランス**



➢CC-Caseについて

CC-Caseの目的・定義

CC-Caseの定義

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

CC-Caseの定義

セキュリティ要求分析と保証の統合開発方法論

＊「統合」はCCとアシュアランスケースの長所を統合してセキュリティ要求分析を実施するとともに保証を実施することを意味している

CC-Caseの目的

開発のセキュリティ上の課題を解決し、セキュアなシステム開発を実現

→IoT時代にセキュリティ・バイ・デザインを実現できる開発フレームワークを目指す

要求O.K

CCのセキュリティ目標を満たす

＋

保証O.K

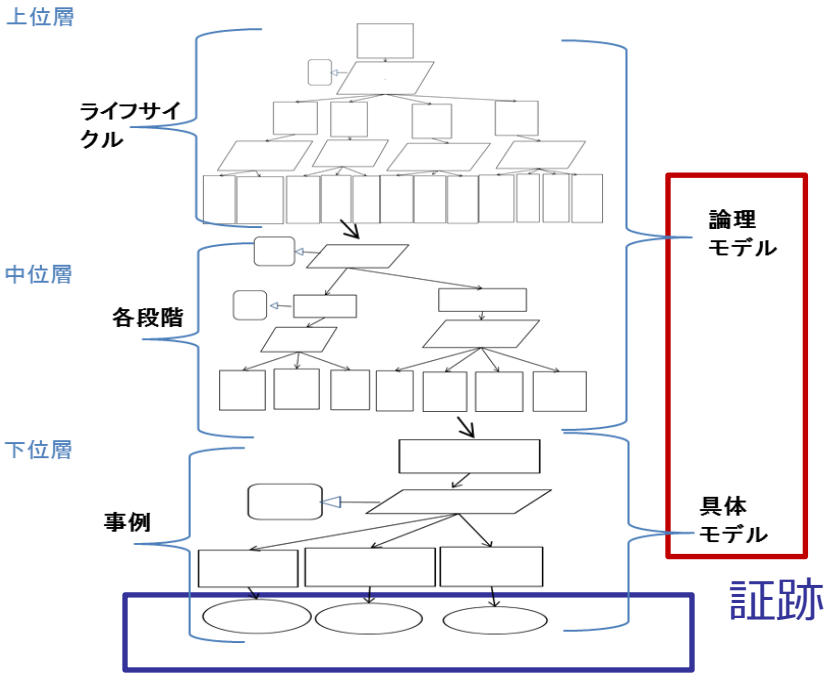
アシュアランスケースの要求事項を満たす

＝

CC-Case

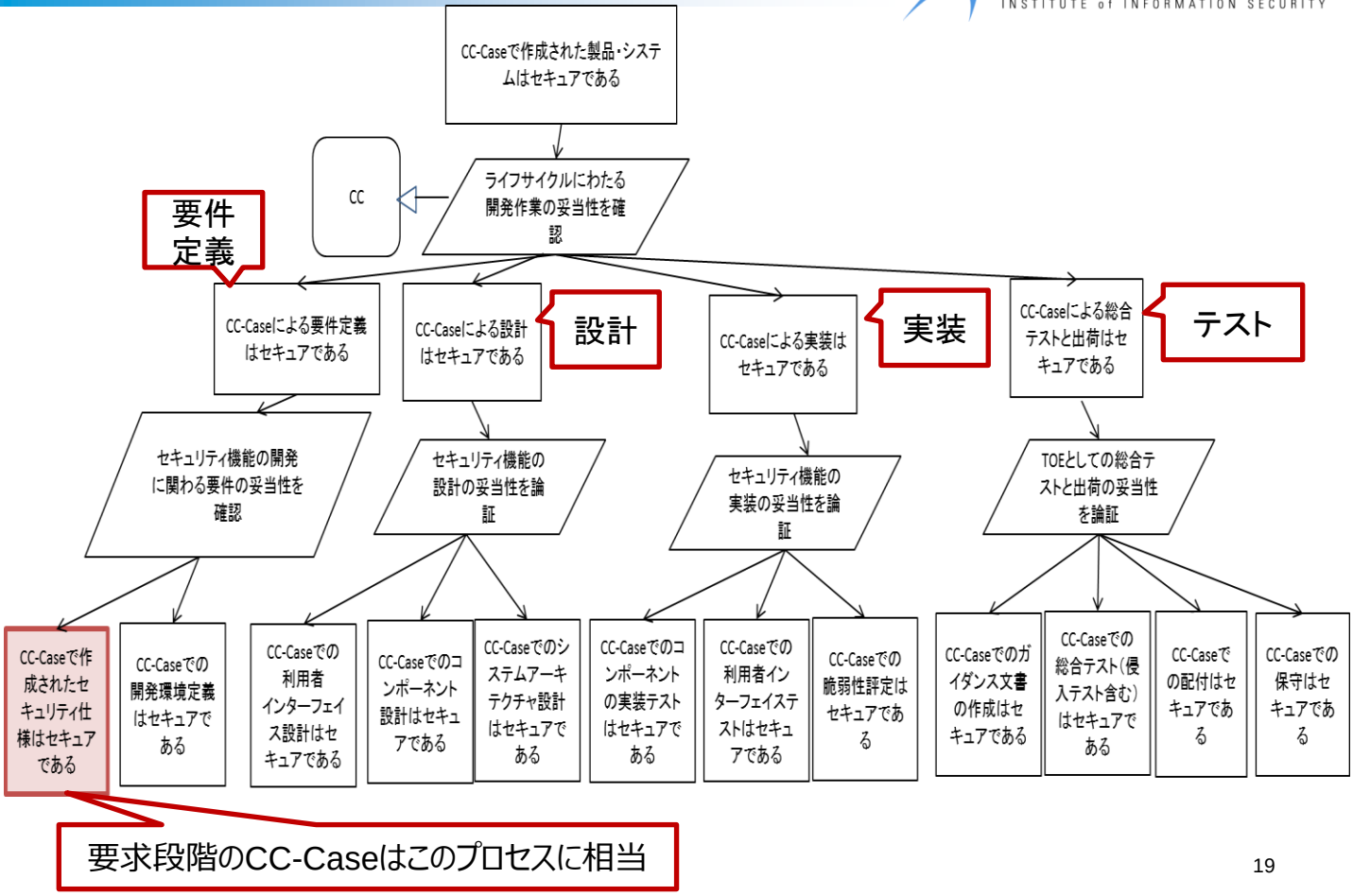
CC-Caseの構造・適用対象

- 論理モデルと具体モデルに分類される
- ライフサイクルプロセスはシステム・製品の要件定義・設計・実装・テスト・保守にわたるプロセスを規定（詳細は次スライド）



＊CC-Caseの適用対象はシステムまたは製品。仕様を決める際に承認を取る特定の顧客がいない場合は要件を決めるうえでの関係者と読み替える.

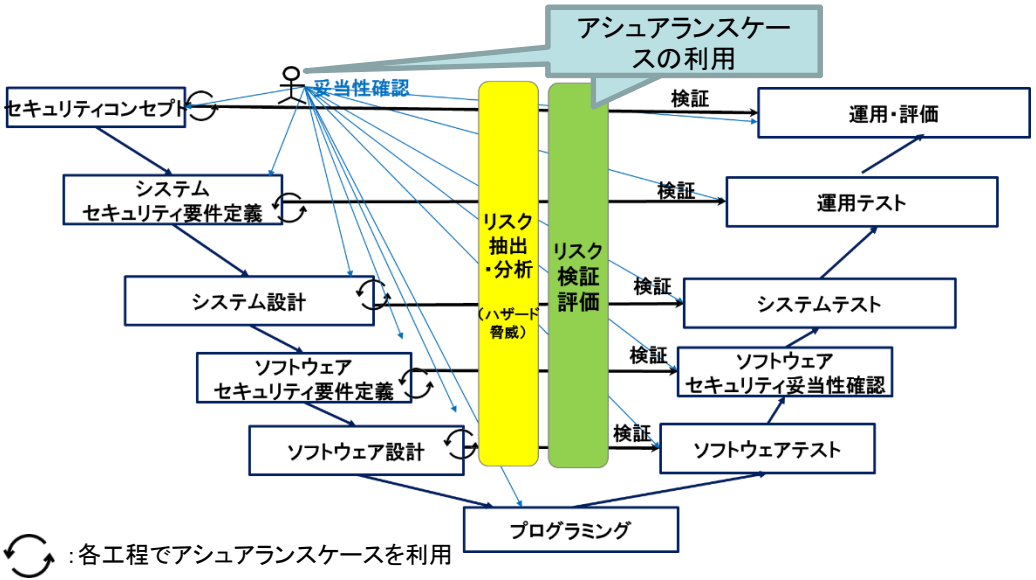
CC-Caseのライフサイクルプロセスの概要



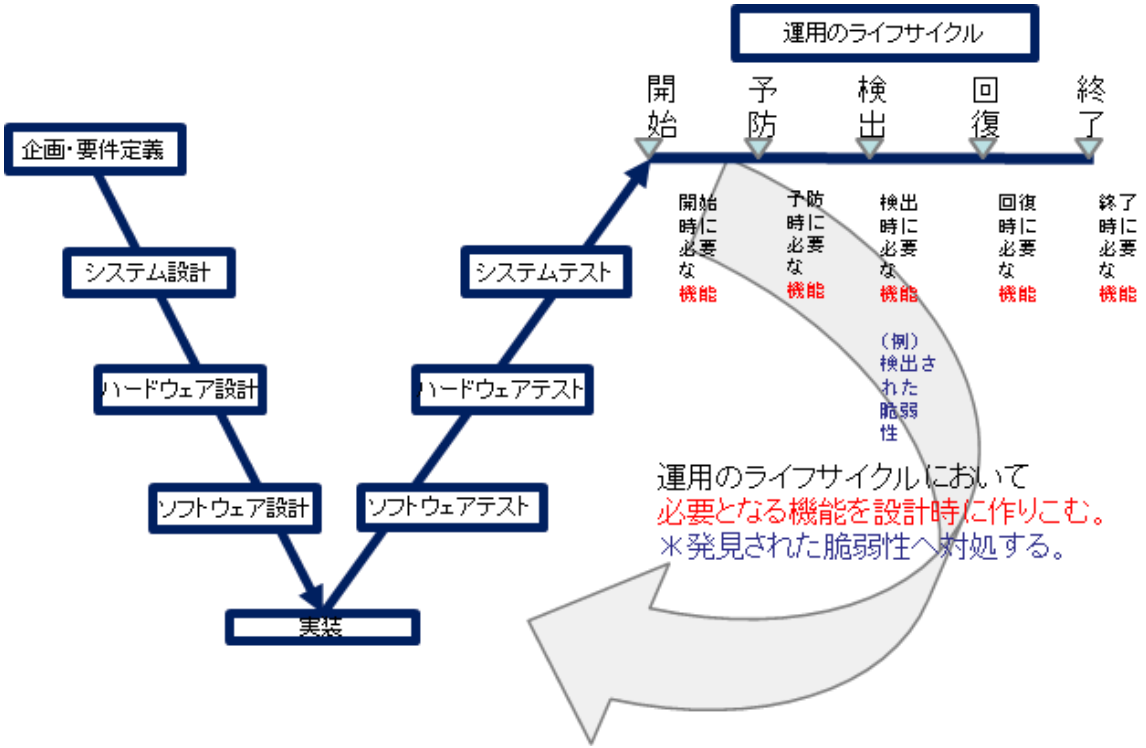
要求段階のCC-Caseはこのプロセスに相当

CC-Caseによる検証・妥当性確認

- アシュアランスケースによるライフサイクルのトレーサビリティ確保

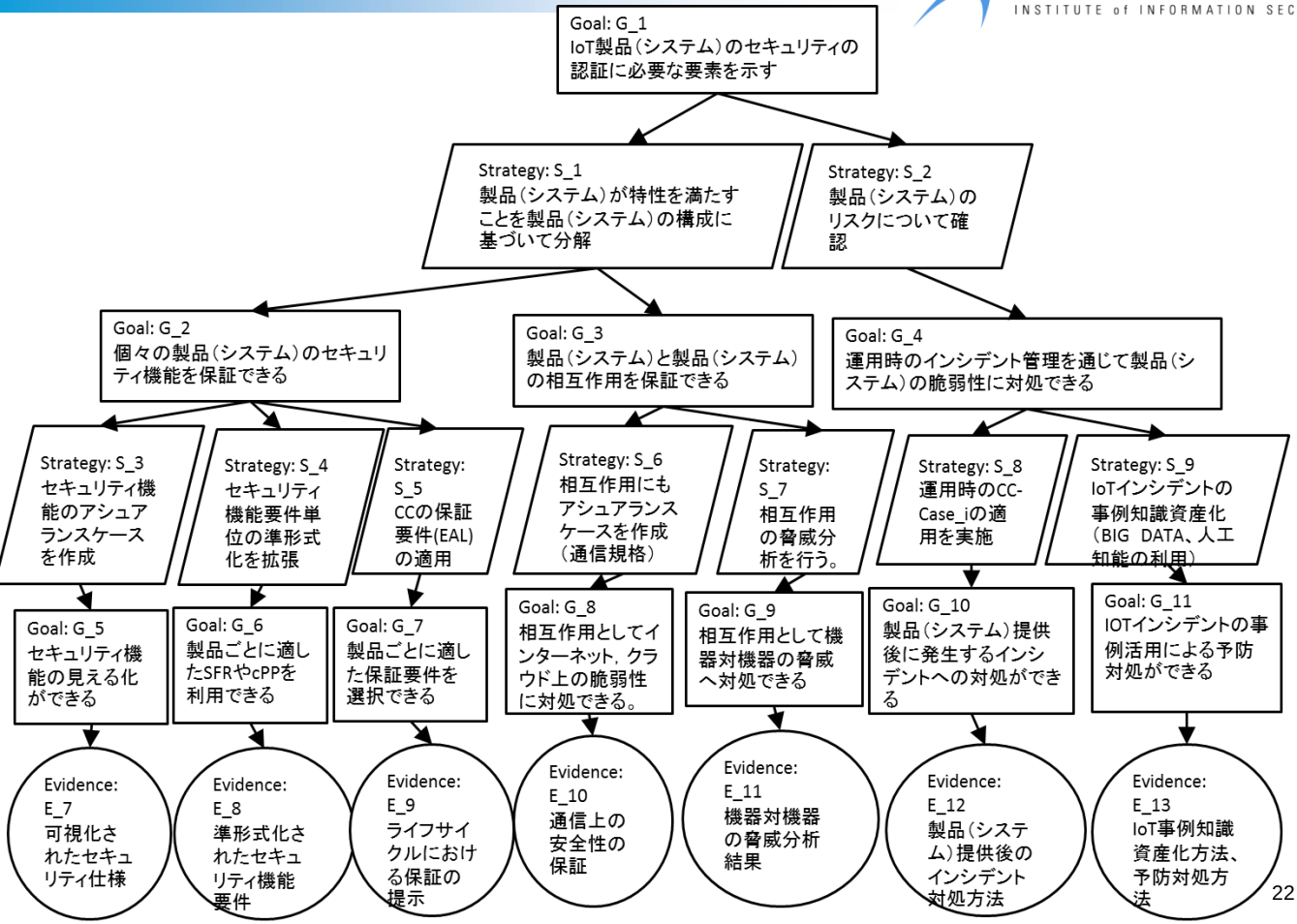


運用で必要となる機能の作りこみ



IoTセキュリティ認証に必要な要素

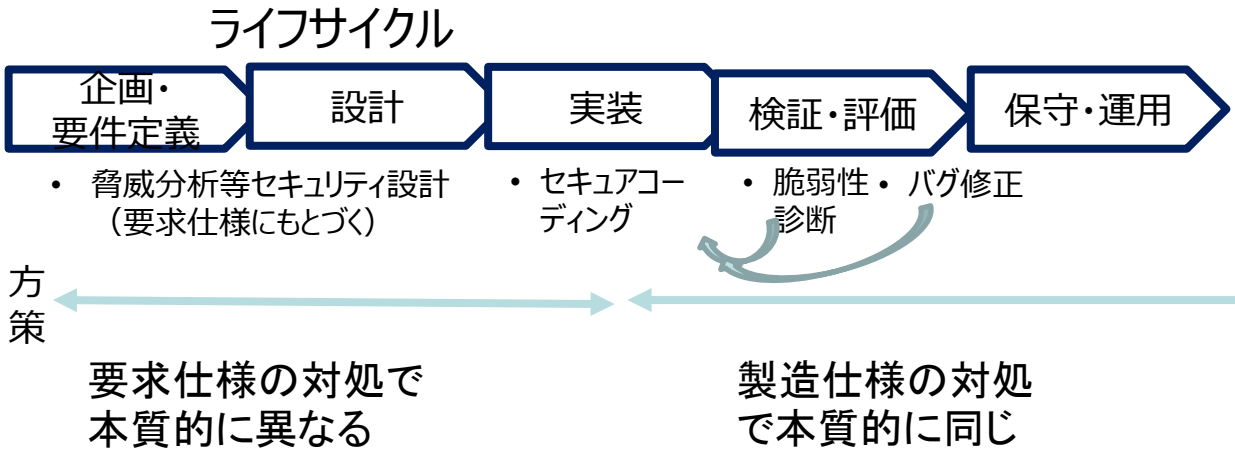
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



イテレーションの必要性

- 日本で主流のウオーターフォールモデルはイテレーションがないため、セキュリティ・バイ・デザインを実現しにくい。

- セキュアコーディングも含めたセキュリティ・バイ・デザイン実現のためには、イテレーションしながらセキュリティを回す仕組みにする必要がある。イテレーションの仕方は各工程ごともあるし、上流から下流までの工程を繰り返す方法もある（プロトタイプ）



CC-Caseのフレームワークを構成する技術要素

- CC-Caseは以下の技術要素を含む

分類	具体的技法	技術のポイント	IoT対応今後の方向性
①プロセス	CCのセキュリティライフサイクルプロセス	CCに規定されたセキュリティプロセスとセーフティプロセスをすり合わせ	各機能安全規格等の設計プロセスを適用
②リスク分析	SARM、STAMP/STPA-Sec	一般の機能要求とセキュリティ要求を統合的に分析	機器間の網羅的セキュリティ要求分析が可能
③機能要件	ＰＰ（プロテクションプロファイル）の活用	準形式化したセキュリティ機能要件で共通言語化	幅広い機器への要件化で認証方式としての効率的な保証を可能に
④保証要件	CCの保証要件の活用	ＥＡＬの評価基準を利用	セーフティと合わせた評価基準化が必要
⑤アシュアランス	ＧＳＮ	セキュリティケースとして脅威分析、セキュリティセーフティのすり合わせ、インシデント評価に利用。論理の見える化を図る	ライフサイクルにわたるイテレーショナルなトレーサビリティ技法化

- 関連知識

アシュアランケース

IoTの特徴にあった可視化手法は？

複雑なセキュリティ要件をもつIoTにはアシュアランスケースが向いている

アシュアランスケース（ISO/IEC15026）とは？

テスト結果や検証結果をエビデンスとしそれらを根拠にシステムの安全性，信頼性を議論し，システム認証者や利用者などに保証する，あるいは確信させるためのドキュメント

GSNの構成要素

名称	図式要素	説明
ゴール（主張）		システムが達成すべき性質を示す。下位の主張や説明に分かれる
戦略（説明）		主張の達成を導くために必要となる説明を示す。下位の主張や説明に分解される
コンテキスト（前提）		主張や説明が必要となる理由としての外部情報を示す
未定義要素		まだ具体化できていない主張や説明であることを示す
証跡		主張や説明が達成できることを示す証拠

アシュアランスケース（ISO/IEC15026）とは？

テスト結果や検証結果をエビデンスとしそれらを根拠にシステムの安全性，信頼性を議論し，システム認証者や利用者などに保証する，あるいは確信させるためのドキュメント

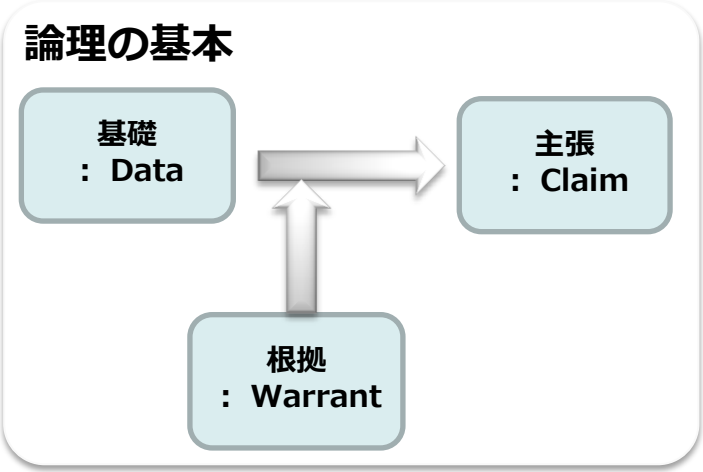
- IoTの対象となる航空，鉄道，軍事，自動車，医療機器の分野の複数の安全性規格やガイドラインで要求され，欧州を中心に広く利用されている

設計品質のロジカルな説明ができる

- アシュアランスケースは対象となる機器やシステムについて，なぜその設計で目標が達成されるかを事実に基づき，論理的かつ第三者でも容易に理解できる表記で説明する手法

アシュアランス（Assurance:保証）＋ ケース（Case:論拠）

トゥールミン・ロジックの基礎

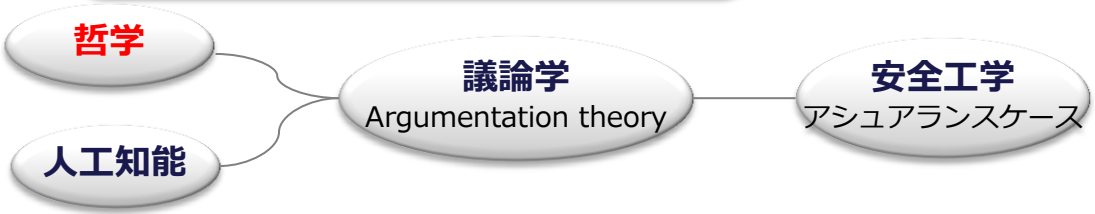


主張（C論理）
論理として構築されるひとつの主張

基礎（D論理）
論理の根拠となる、状態、事実など
最初に呈示される説明情報

根拠（W論理）
クレームの根拠としてデータが利用
可能であることを正当化する情報

ディベートで超論理思考を手に入れる
ISBN 978-4-904209-13-4
著者： 苫米地英人　脳機能学者/カーネギーメロン大学博士



アシュアランスケースの表記法一覧

	CAE	GSN	D-Case
正式名称	Claim、Argument、Evidence	Goal Structuiring Notation	Dependability Case
登場時期	1998年	2011年	2012年
構成要素	3種類	6種類	GSNを拡張
開発組織	英Adelard社、ロンドン大学	英ヨーク大学	日本DEOSプロジェクト

アシュアランスケースと認証規格

■アシュアランスケースの作成、提出を義務付けている規格

- Yellow Book(*1): 鉄道システムの改変時の安全管理
- EUROCONTROL: 安全で機能的な航空管制管理
- ISO26262: 自動車の電気、電子システムの機能安全規格
- Def-Stan 00-56: 英国防衛省策定の防衛システムの安全管理
- US. Food and Drug Administration (FDA)
  Infusion Pump Improvement Initiative:
  点滴ポンプなどの医療器具の病院導入時

■ セーフティだけでなく、セキュリティ等にも広がりつつある。

＊1 The principles of the safe management of engineering change

- 関連知識

セーフティとセキュリティ

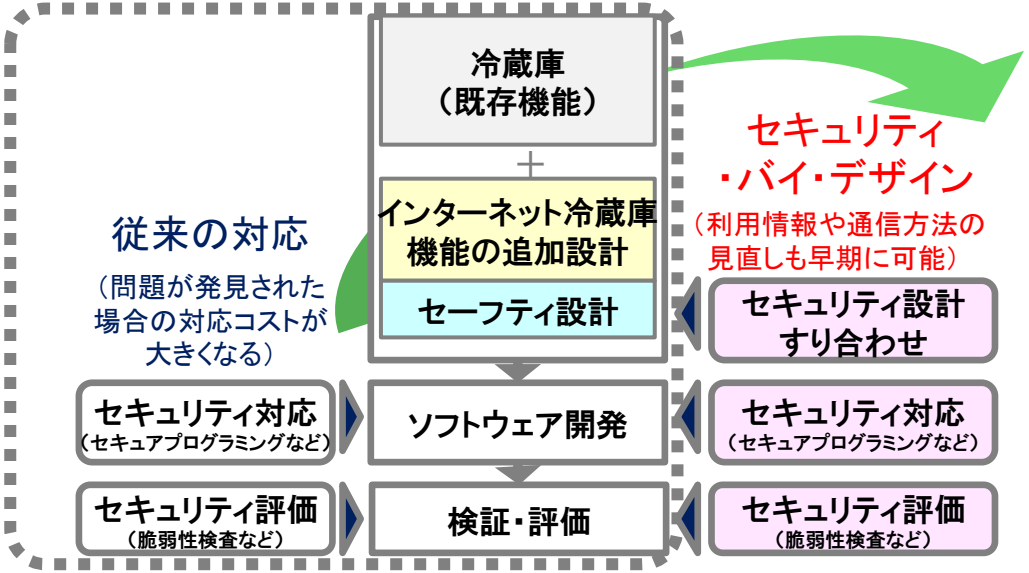
Safety セーフティ：
偶発的なミス、故障などの悪意のない危険に対する安全

Security セキュリティ：
悪意をもって行われる脅威に対しての安全

SE（離れる）＋**CURE**（気がかり）→安心

セーフティをまもれるセキュリティ

- セキュリティ・バイ・デザインの考え方はセキュリティだけのものではない。
- セキュリティで脅かされるセーフティも守ることができる。



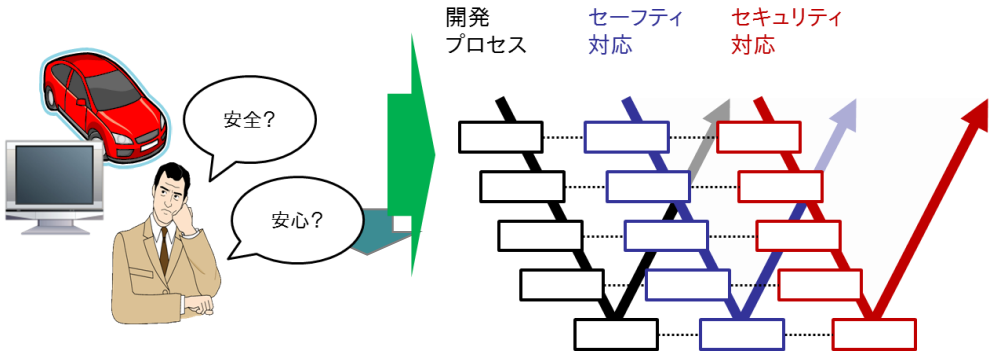
IoT機器等のセキュリティ・バイ・デザインのイメージ（インターネット冷蔵庫の例）

セーフティ設計とセキュリティ設計のすり合わせ

- 早期の段階でセーフティ設計とセキュリティ設計のすり合わせすれば、余計なことが省かれる

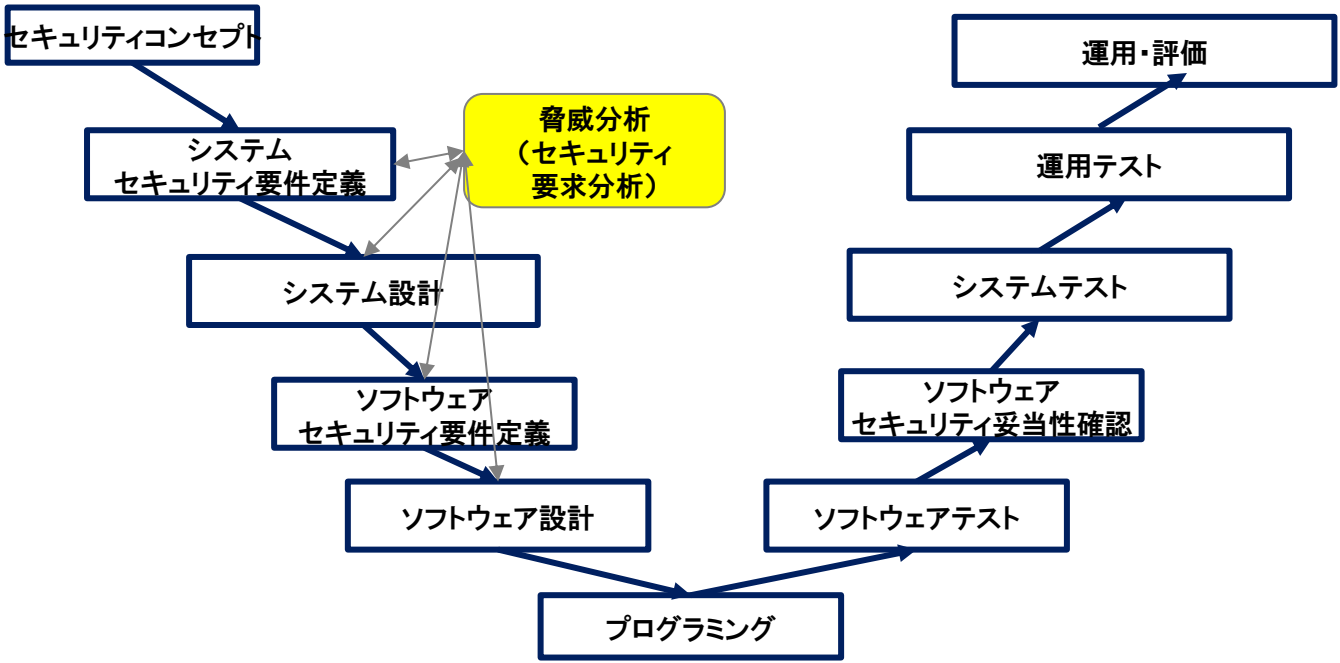
設計がまとまってからセーフティ／
セキュリティ対応するのではなく・・・

開発プロセスの上流から組み入れる

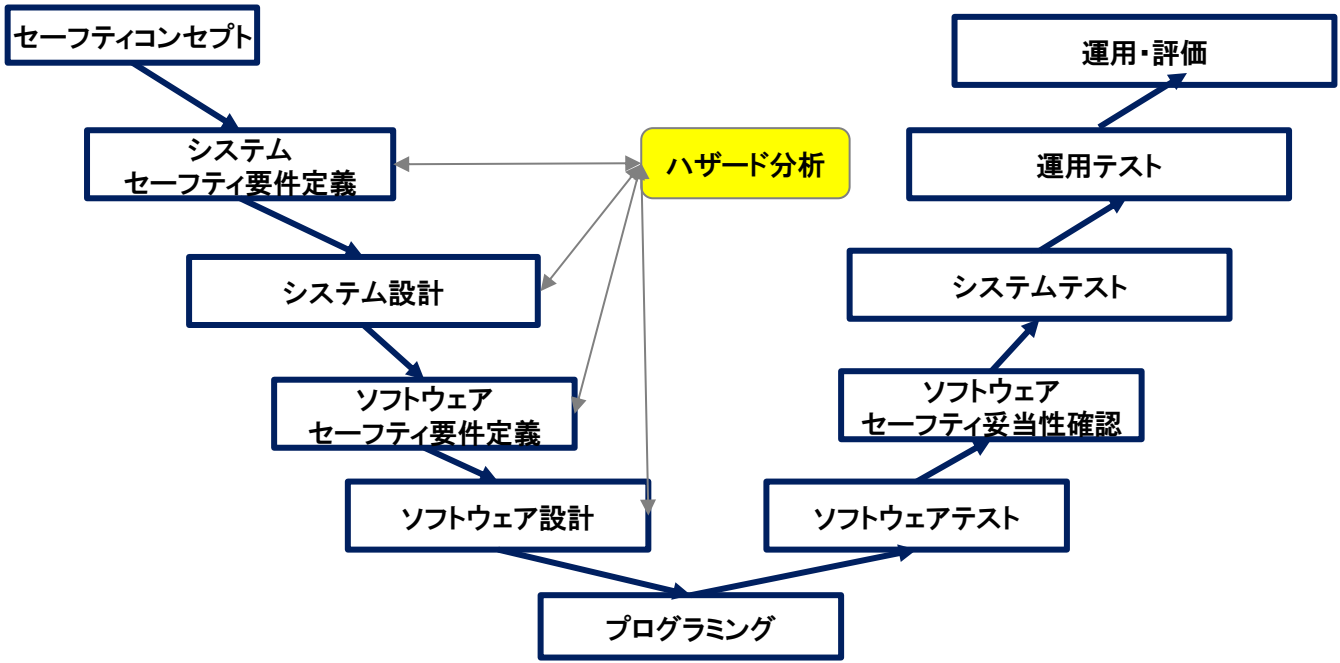


IPA資料「セキュリティ・バイ・デザイン入門」より

セキュリティ設計プロセス



セーフティ設計プロセス



セーフティとセキュリティの特徴の比較

相違点	セーフティ	情報セキュリティ
保護対象の違い	人命、財産（家屋等）など	情報の機密性、完全性、可用性など
原因の違い	合理的に予見可能な誤使用、機器の機能不全	意図した攻撃
被害検知の違い	事故として表れるため、検知しやすい	盗聴や侵入など、検知しにくい被害も多い
発生頻度	発生確率として扱うことができる	人の意図した攻撃のため確率的には扱えない
対策タイミング	設計時のリスク分析・対策で対応	時間経過により新たな攻撃手法が開発されるので、継続的な分析・対策が必要

セーフティとセキュリティは

両輪の輪!!

＊特に生命、健康にかかわるセーフティの要件は重要

- CC-Caseの特徴

可視化

CC-Case　見える化の特長

CC-Caseはアシュランスケースを用いて要求と保証に対する見える化を図る

1. 主張の見える化：
ゴールとしての主張とその主張の正しさを裏付ける証跡が存在すること
- アシュアランスケースはトップゴールの主張を満たすことを図の最下層に証跡として示すことで可視化する手法だから

2.論理の見える化：
- 前提条件・戦略・ゴールの関係性の明示により，トップの主張から証跡までの論理を明確化

3.リスクの変化への対応性：
- 前提条件を変更することにより、リスクの変化を柔軟に記述できる

4.セーフティ・セキュリティのすり合わせ：
- セーフティとセキュリティ両方の観点で記述されたアシュアランスケースを統合し、要件をすり合わせる

CC-Caseによるセキュリティケースの分類

1.脅威分析のアシュアランスケース

脅威分析のリスク結果抽出、双方の突き合わせ、対策立案を実施
結果の検証において、関係者で検討し、合意するための利用（→妥当性確認となる）

2.セーフティセキュリティ設計要件すり合わせのアシュアランスケース

機能安全の各規格に対して、要件を満たしているかを検証したうえで、セキュリティ要件のすり合わせを実施するアシュアランスケースを作成

3.ライフサイクルのトレーサビリティ確保のアシュアランスケース

セキュリティ設計の妥当性に対する説明責任を果たすため、ライフサイクルの各工程でアシュアランスケースを作成

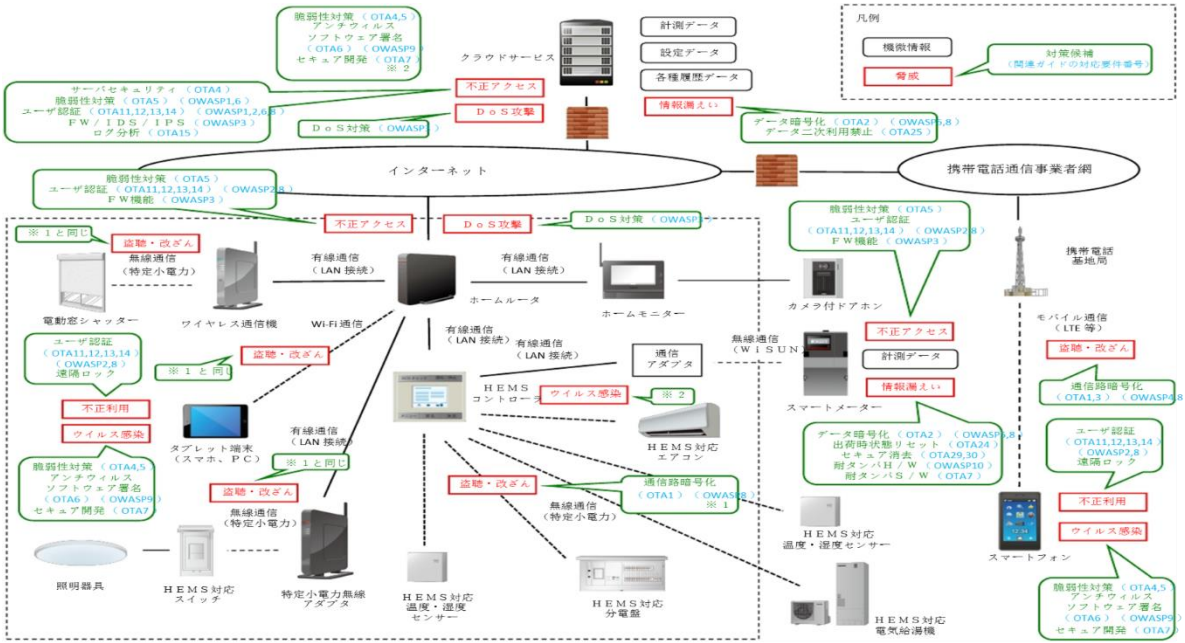
4.セキュリティ機能ごとのアシュアランスケース

CCのセキュリティ機能要件のアシュアランスケースを作成し、セキュリティ機能設計と検証を実施

5.運用段階のアシュアランスケース

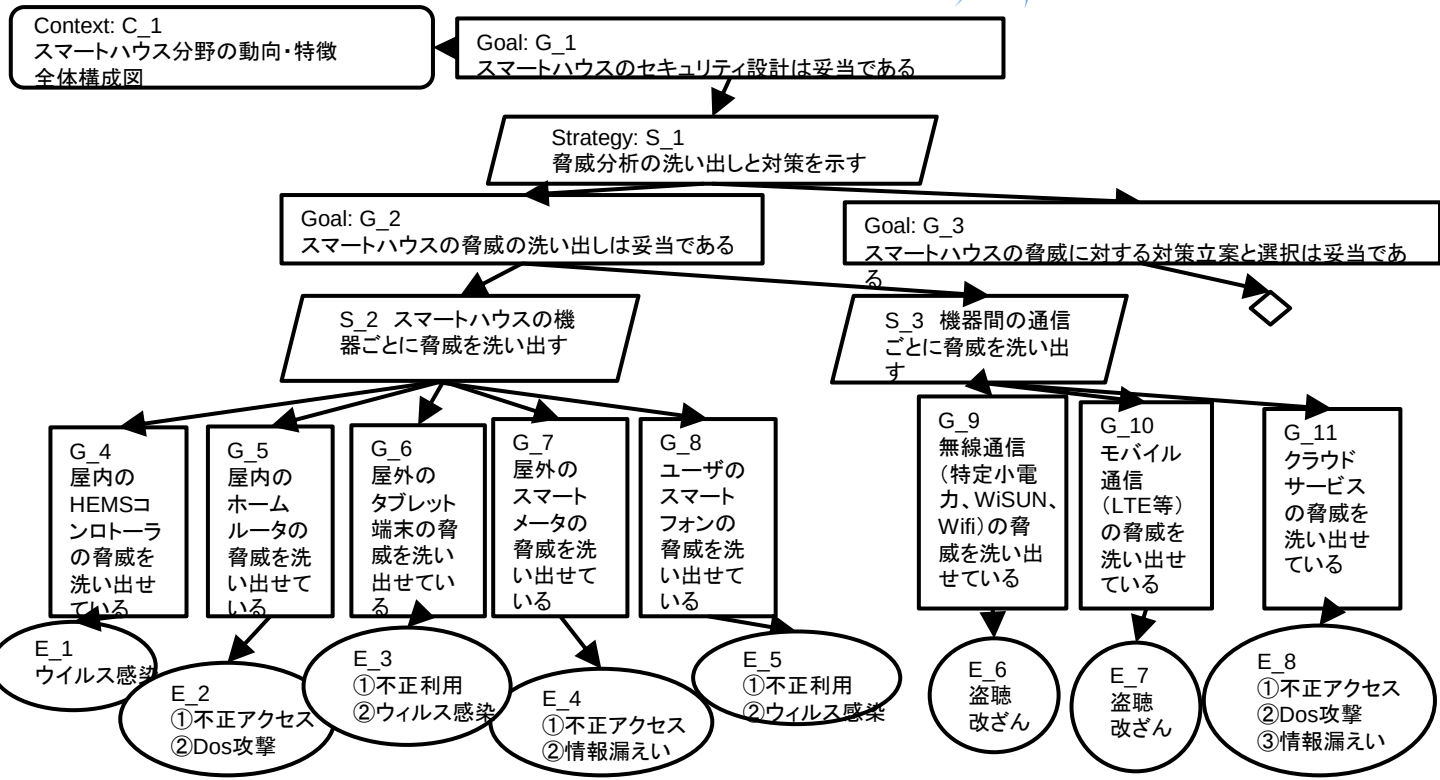
発生したインシデントに対して対応の正しさを確認し、説明するアシュアランスケースを作成

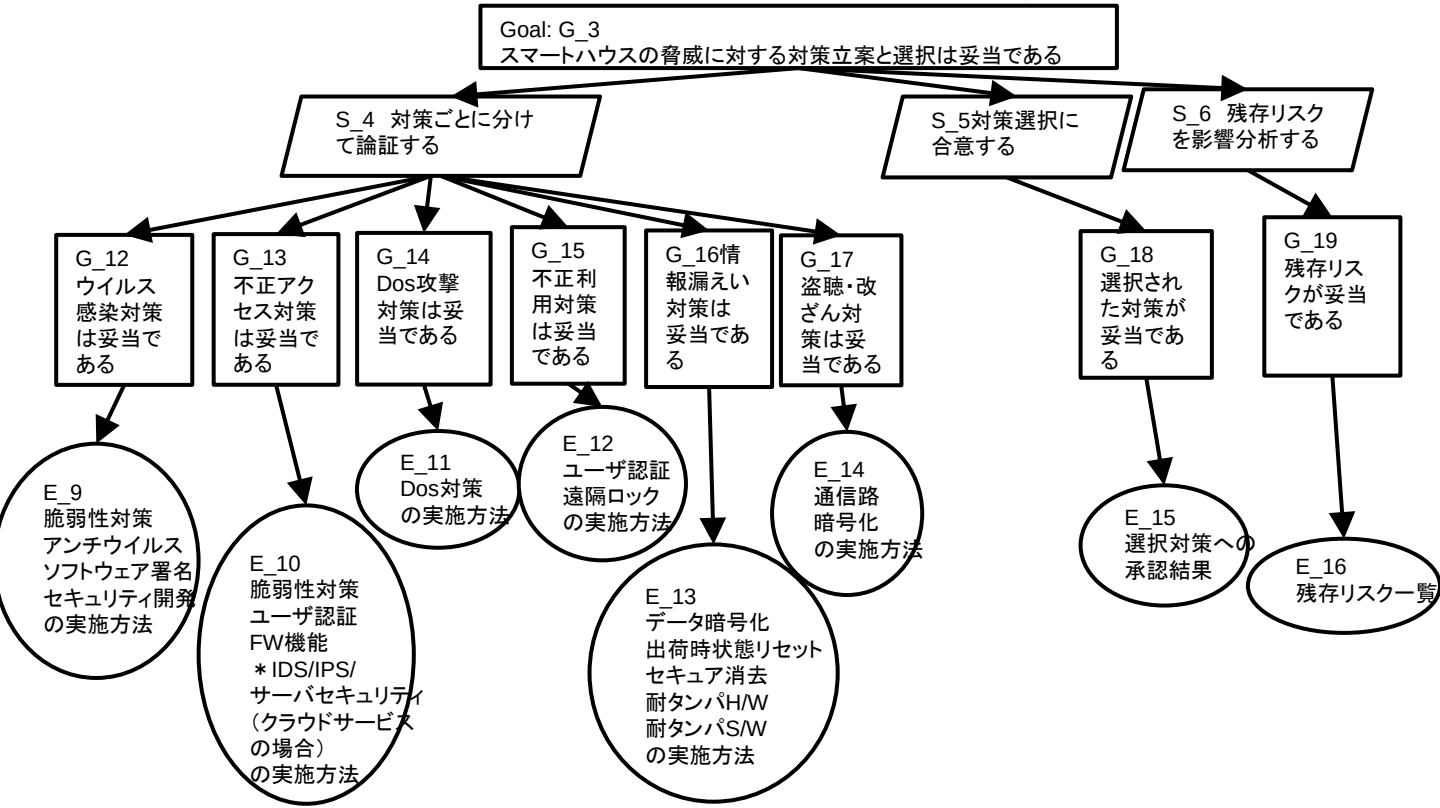
スマートハウスの脅威分析と対策の検討例

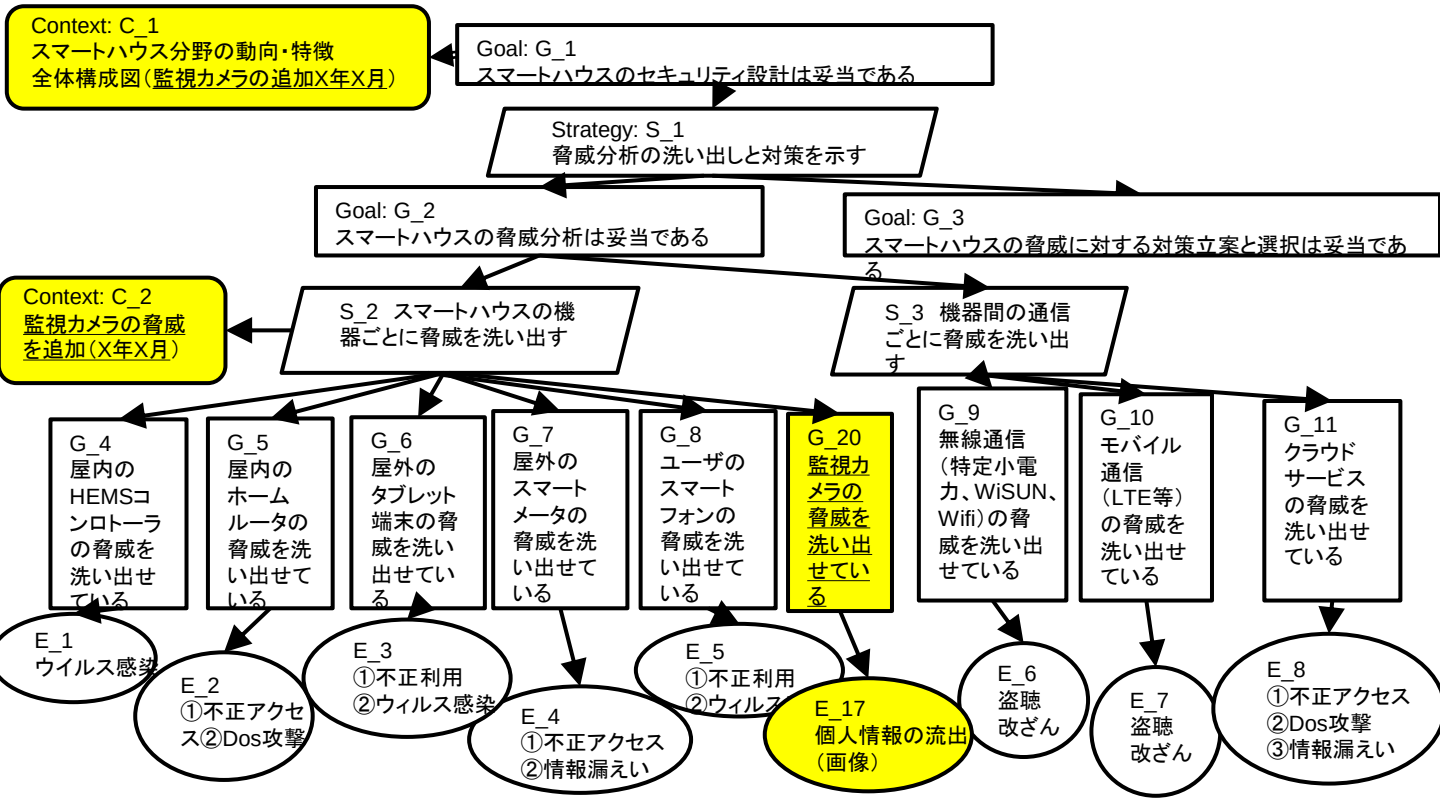


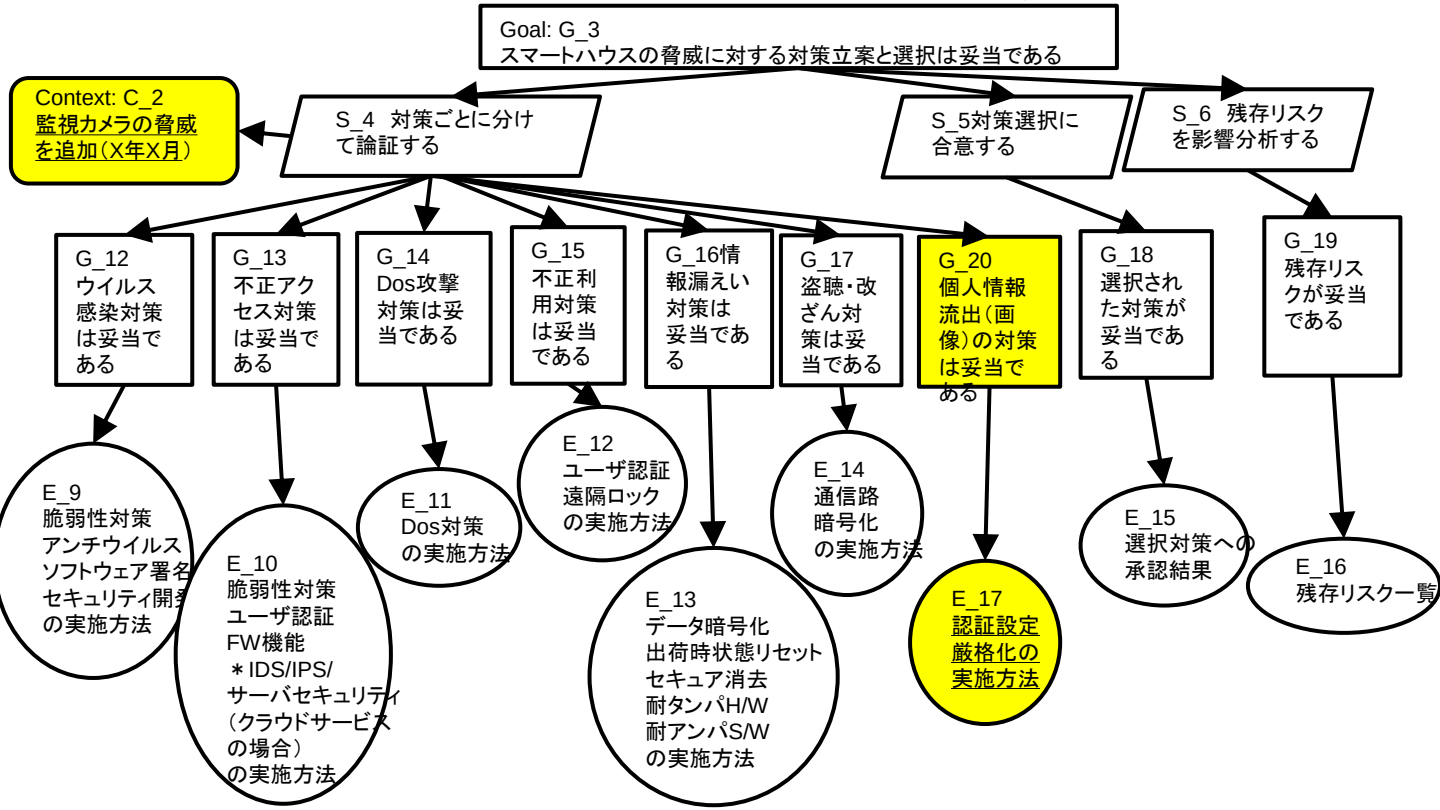
出典：
IPA セキュリティセンター
「IoT開発におけるセキュリティ設計の手引き」

スマートハウス：家庭内機器を一元管理することによって、省エネルギーを実現するIoT システム


Context: C_1
スマートハウス分野の動向・特徴
全体構成図
Goal: G_1
スマートハウスのセキュリティ設計は妥当である
Strategy: S_1
脅威分析の洗い出しと対策を示す
Goal: G_2
スマートハウスの脅威の洗い出しは妥当である
Goal: G_3
スマートハウスの脅威に対する対策立案と選択は妥当である
S_2 スマートハウスの機器ごとに脅威を洗い出す
S_3 機器間の通信ごとに脅威を洗い出す
G_4 屋内のHEMSコントローラの脅威を洗い出せている
G_5 屋内のホームルータの脅威を洗い出せている
G_6 屋外のタブレット端末の脅威を洗い出せている
G_7 屋外のスマートメータの脅威を洗い出せている
G_8 ユーザのスマートフォンの脅威を洗い出せている
G_9 無線通信（特定小電力、WiSUN、Wifi）の脅威を洗い出せている
G_10 モバイル通信（LTE等）の脅威を洗い出せている
G_11 クラウドサービスの脅威を洗い出せている
E_1 ウイルス感染
E_2 ①不正アクセス ②Dos攻撃
E_3 ①不正利用 ②ウィルス感染
E_4 ①不正アクセス ②情報漏えい
E_5 ①不正利用 ②ウィルス感染
E_6 盗聴 改ざん
E_7 盗聴 改ざん
E_8 ①不正アクセス ②Dos攻撃 ③情報漏えい


Goal: G_3
スマートハウスの脅威に対する対策立案と選択は妥当である
S_4 対策ごとに分けて論証する
S_5対策選択に合意する
S_6 残存リスクを影響分析する
G_12 ウイルス感染対策は妥当である
G_13 不正アクセス対策は妥当である
G_14 Dos攻撃対策は妥当である
G_15 不正利用対策は妥当である
G_16情報漏えい対策は妥当である
G_17 盗聴・改ざん対策は妥当である
G_18 選択された対策が妥当である
G_19 残存リスクが妥当である
E_9 脆弱性対策 アンチウイルスソフトウェア署名 セキュリティ開発の実施方法
E_10 脆弱性対策 ユーザ認証 FW機能 ＊IDS/IPS/ サーバセキュリティ（クラウドサービスの場合）の実施方法
E_11 Dos対策の実施方法
E_12 ユーザ認証 遠隔ロックの実施方法
E_13 データ暗号化 出荷時状態リセット セキュア消去 耐タンパH/W 耐タンパS/Wの実施方法
E_14 通信路暗号化の実施方法
E_15 選択対策への承認結果
E_16 残存リスク一覧


Context: C_1
スマートハウス分野の動向・特徴
全体構成図（監視カメラの追加X年X月）
Goal: G_1
スマートハウスのセキュリティ設計は妥当である
Strategy: S_1
脅威分析の洗い出しと対策を示す
Goal: G_2
スマートハウスの脅威分析は妥当である
Goal: G_3
スマートハウスの脅威に対する対策立案と選択は妥当である
Context: C_2
監視カメラの脅威を追加（X年X月）
S_2 スマートハウスの機器ごとに脅威を洗い出す
S_3 機器間の通信ごとに脅威を洗い出す
G_4 屋内のHEMSコントローラの脅威を洗い出せている
G_5 屋内のホームルータの脅威を洗い出せている
G_6 屋外のタブレット端末の脅威を洗い出せている
G_7 屋外のスマートメータの脅威を洗い出せている
G_8 ユーザのスマートフォンの脅威を洗い出せている
G_20 監視カメラの脅威を洗い出せている
G_9 無線通信（特定小電力、WiSUN、Wifi）の脅威を洗い出せている
G_10 モバイル通信（LTE等）の脅威を洗い出せている
G_11 クラウドサービスの脅威を洗い出せている
E_1 ウイルス感染
E_2 ①不正アクセス②Dos攻撃
E_3 ①不正利用 ②ウィルス感染
E_4 ①不正アクセス ②情報漏えい
E_5 ①不正利用 ②ウィルス
E_17 個人情報の流出（画像）
E_6 盗聴 改ざん
E_7 盗聴 改ざん
E_8 ①不正アクセス ②Dos攻撃 ③情報漏えい


Goal: G_3
スマートハウスの脅威に対する対策立案と選択は妥当である
Context: C_2
監視カメラの脅威を追加（X年X月）
S_4 対策ごとに分けて論証する
S_5対策選択に合意する
S_6 残存リスクを影響分析する
G_12 ウイルス感染対策は妥当である
G_13 不正アクセス対策は妥当である
G_14 Dos攻撃対策は妥当である
G_15 不正利用対策は妥当である
G_16情報漏えい対策は妥当である
G_17 盗聴・改ざん対策は妥当である
G_20 個人情報流出（画像）の対策は妥当である
G_18 選択された対策が妥当である
G_19 残存リスクが妥当である
E_9 脆弱性対策 アンチウイルス ソフトウェア署名 セキュリティ開発 の実施方法
E_10 脆弱性対策 ユーザ認証 FW機能 ＊IDS/IPS/ サーバセキュリティ （クラウドサービスの場合） の実施方法
E_11 Dos対策 の実施方法
E_12 ユーザ認証 遠隔ロック の実施方法
E_13 データ暗号化 出荷時状態リセット セキュア消去 耐タンパH/W 耐アンパS/W の実施方法
E_14 通信路 暗号化 の実施方法
E_17 認証設定 厳格化の 実施方法
E_15 選択対策への 承認結果
E_16 残存リスク一覧

- 関連知識

コモンクライテリア（CC）

IoTの特徴にあったセキュリティ基準は？

IoTの特徴：多様な機器・システムがつながること

個別の機器，個別の業界の基準のみではサポートできない部分が発生

↓

汎用的で広く認知されたセキュリティ基準として２つの国際規格

CC（ISO/IEC15408） ＝ITセキュリティ評価標準 →セキュリティ機能を評価する規格である 製品・システムのセキュリティ機能の安全性を第3者に示し，保証することができる基準	ISMS（ISO/IEC 27001） ＝セキュリティ・マネジメント規格 →セキュリティ機能を評価する規格ではない 機器・システムのセキュリティ機能の実現方法ではなく、組織が何を行うべきかを主に記述

↓

相互に依存するIoT機器・システムはその1つ1つが安全であり，相互依存関係においても安全でなければ，セキュリティ上の保証ができないから

◆ＣＣパート１　概説と一般モデル

セキュリティ目標（ＳＴ）

ST概説
適合性主張
セキュリティ課題定義
　脅威　　組織のセキュリティ方針　　前提条件

セキュリティ対策方針
　TOEのセキュリティ対策方針
　運用環境のセキュリティ対策方針　　セキュリティ対策

拡張コンポーネント定義

セキュリティ要件
　セキュリティ機能要件　　セキュリティ要件根拠
　セキュリティ保証要件

TOE要約仕様

プロテクションプロフェイル（ＰＰ）

◆　ＣＣパート２　機能コンポーネント

◆　ＣＣパート３　保証コンポーネント

◆　ＣＥＭ　情報セキュリティ評価方法

CCはITセキュリティ評価の国際標準

- 開発者が主張するセキュリティ保証の信頼性に関する評価の枠組みを規定

STはセキュリティ保証の目標を規定した文書

- 評価対象のシステムが装備するセキュリティ機能を定義
- 必須のセキュリティ評価対象

IoTセキュリティ認証に対するCCの有効性

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

表2 公開されているPPの例

分野	PP名称	発行日
ネットワーク基盤	PP_ND_V1.1	2012/6/8
ファイアウォール	PP_ND_TFFW_EP_V1.0	2011/12/19
VPNゲートウェイ	PP_ND_VPN_GW_EP_V1.1	2013/4/15
IPsec VPNクライアント	PP_VPN_IPSEC_CLIENT_V1.4	2013/10/23
SIPサーバー	PP_ND_SIP_EP_V1.0	2013/2/6
無線LANアクセスポイント	PP_WLAN_AS_V1.0	2011/12/1
無線LANクライアント	PP_WLAN_CLI_V1.0	2011/12/19
汎用OS	PP_GPOS_V3.9	2013/1/15
モバイルデバイス基盤	PP_MD_V1.1	2014/2/18
モバイルデバイス管理	PP_MDM_V1.1	2014/3/7
USBフラッシュドライブ	PP_USB_FD_V1.0	2011/12/1
ソフトウェアフルディスク暗号化	PP_SWFDE_V1.1	2014/3/31
認証局	PP_CA_V1.0	2014/5/16
VOIPアプリ	PP_VOIP_V1.2	2013/10/23
Emailクライアント	PP_EMAILCLIENT_V1.0	2014/4/1
Webブラウザ	PP_WEBBROWSER_V1.0	2014/3/31
BIOSアップデート	PP_BIOS_V1.0	2013/2/13
企業セキュリティ管理ポリシー管理	PP_ESM_PM_V2.1	2013/11/21
企業セキュリティ管理アクセス制御	PP_ESM_AC_V2.1	2013/11/12
企業セキュリティ管理ID・クレデンシャル管理	PP_ESM_ICM_V2.1	2013/11/21
データベース管理システム	PP_DBMS_V1.3	2010/12/24
デジタル複合機	PP_HCD_EAL2_V1.0	2010/2/26
デジタル複合機	PP_HCD_BR_V1.0	2009/6/12
IDS(侵入検知システム)	pp_ids_sys_br_v1.7	2007/7/25

IPA2014年度版　ＳＴ作成講座資料より

従来のPPとcPPの違い

STによる文書審査中心の評価
→cPP又はPPに適合するための技術分野ごとのテストや脆弱性分析中心の評価に移行

	PP	cPP
対象範囲	製品分野	技術分野
作成者	調達者(政府機関・認証機関)	国際的テクニカルコミュニティ(製品ベンダ，調達者，評価者，認証者)
評価保証レベル	EAL3～4	原則EAL1～EAL2
評価期間	18か月～	6か月以下(米国は90日以下を目標に推進中)
評価品質	評価者の能力に強く依存(評価機関・国によるバラツキ)	具体的なテスト，評価手法をサポート文書として規定することで，必要な品質を確保
暗号評価	CC/CEMに詳細な規定なし	サポート文書に詳細なテスト方法を記載．将来的にCC/CEMに盛り込む計画

PPとは

- 特定の製品分野のために用意されるセキュリティ要件
- 想定されるセキュリティ課題、機能要件を規定
  （セキュリティターゲットのテンプレート）
- 調達者、業界団体等が開発し、調達要件として活用

各技術分野毎に
世界共通となるPPの開発

調達要件、ST開発の中で
PPの積極的な活用が期待

これまでは…

開発者：
独自に要件を定義し、STを作成
STに基づき製品を開発、認証取得

製品調達者：
公開されたST、認証報告書を見て
自分のニーズに合う製品かを判断
（調達要件とのミスマッチ発生のリスク）

Protection Profileを活用した製品調達

製品調達者：
自分のニーズに合うPPをベースに
調達要件を提示

開発者：
提示されたPPに適合したSTの作成
STに基づく製品開発、認証取得

⇨ 要件にマッチした製品の提供

IPA2014年度版　ST作成講座資料より

PP適合STの作成イメージ

STが適合を主張するPP

- 第1章　PP概説
- 第2章　適合主張
- 第3章　セキュリティ課題定義
- 第4章　セキュリティ対策方針
- 第5章　拡張コンポーネント定義
- 第6章　セキュリティ要件

第1章　ST概説
- PPに規定されたTOE概要をベースに、TOE記述（評価範囲、評価対象となる機能の内容等）を具体化

第2章　適合主張
- PP識別名をコピー
- PPの規定内容をベースに適合種別を記述
- 論証適合の場合はPPと同等または、より制限的であると見なせる根拠を記述

第3章　セキュリティ課題定義
第4章　セキュリティ対策方針
- 基本的にPPからそのままコピー（追加の要件がある場合は脅威・対策方針を定義）

第5章　拡張コンポーネント定義
第6章　セキュリティ要件
- 基本的にPPからそのままコピー（追加の要件がある場合は要件を新たに定義）
- 操作が未完了の機能要件について操作を完了する

第7章　TOE要約仕様
- この製品では定義された機能要件をどのように実現しているのか具体的に記載する

IPA2014年度版　ST作成講座資料より

- CC-Caseの特徴

保証

「セキュリティ保証書」：論理的根拠を明示

CCベースでセキュリティ要件の論理関係をステークホルダで共通認識ができる

第3者機関

製品・システムの利用者

一般のシステム開発者

ステークホルダ間の認識の食い違いを防ぎ，納得感のもてる検証・妥当性確認を可能とする！！

CCの課題と利点

- CCはFAXのためだけの使えないセキュリティ基準？
（CCに基づく認証はコスト高との批判）

- 認証制度の運用方法と認証の方式や参照とする基準は分けるべき
- CCにはセキュリティ機能要件（PP)というツールボックスと保証要件の規定という優れた点がある

セキュリティ機能要件の操作

選択したコンポーネントに対して、次の操作を行うことによってコンポーネントを修整しなければならない。

- 割付
- 選択
- 繰返し
- 詳細化

＜例＞
識別と認証
認証失敗時に行われる処理を規定する
CCパート2の規定(一部抜粋)

FIA_AFL.1.1

TSFは、[割付:認証事象のリスト]に関して、[選択:[割付:正の整数値],「[割付:許容可能な値の範囲]内における管理者設定可能な正の整数値」]回の不成功認証試行が生じたときを検出しなければならない。

最後に成功した認証以降の各クライアント捜査員の認証

5

IoTセキュリティ認証へのＰＰの適用

- 従来、インターネットにつながっておらず、セキュリティ機能ももたなかった機器が多い。
- これらのセキュリティ設計とセキュリティ評価にＰＰは利用可能ではないか。

- 個々のIoT機器・システムがどのようなセキュリティ機能をもっているかを、CC　PART2に規定されるカタログ化されたセキュリティ機能要件を利用して提示する

- セキュリティ機能要件の見える化と評価が簡単にできる

- セキュリティ機能要件の利用は政府調達のみならず、一部、民間認証の動きもある

- CC-Caseの有効性実験

CC-Caseの有効性実験の概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

(1) 事前講義およびグループ分け

総計42名の専門学校生、大学生、社会人大学院生を対象として実施
事前講義を実施（30分程度）講義終了後、理解度調査
→事前設問1のGSNの理解度が分散するように担当資料を決定

(2) 担当資料の読み込み

被験者は，担当資料のみを確認（10分程度）

(3) スマートハウスの図の再現

- 配布資料を作成するために使用したスマートハウスの図を加工し，【1】リスクや対応策を削除したり，【2】記述内容を誤ったものに書き換えたりしたものを解答用紙として配布図を正す作業を実施【3】追加の機器の設定

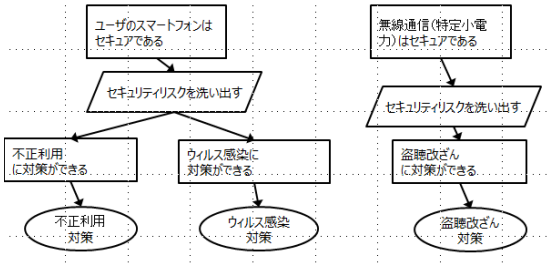
- 与えられた資料の分析しやすさ【4】、理解しやすさ【5】、可視化の観点【6】、妥当性確認の観点【7】での優位性評価

平文とGSNの事例

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

【平文２】
スマートハウスの屋外には スマートメーター、ＨＥＭＳ対応 電気給湯機、ＨＥＭＳ対応 温度・湿度 センサー、カメラ付ドアホンがある。屋外には監視カメラが追加され、ホームモニターから有線通信（LAN 接続）で設置された。
スマートメーターには不正アクセスや情報漏えいの脅威が想定される。
スマートメーターの不正アクセスの脅威に対して、脆弱性対策、ユーザ認証、ＦＷ機能が対策として挙げられる。
スマートメーターの情報漏えいの脅威に対して、データ暗号化、出荷時状態リセット、セキュア消去、耐タンパＨ/W、耐タンパS/W が対策として挙げられる。
スマートフォンにはウイルス感染、不正利用の脅威が想定される。
スマートフォンの不正利用にはユーザ認証、遠隔ロックが対策として考えられる。
スマートフォンのウイルス感染には脆弱性対策、アンチウィルス、ソフトウェア署名、セキュア開発が対策として挙げられる。
スマートハウスの屋外ではスマートフォン・ 基地局間の無線通信が可能である。
スマートフォン・ 基地局間のモバイル通信 （LTE 等）において、盗聴・改ざんなどの脅威が想定される。
基地局間のモバイル通信 （LTE 等）の盗聴・改ざんに関しては通信路暗号化が対策として挙げられる。
スマートハウスの屋内には ホームルータ、ＨＥＭＳ コントローラ、ＨＥＭＳ対応 温度・湿度 センサー、タブレット端末 （スマホ、ＰＣ）がある。
ＨＥＭＳ コントローラは通信 アダプタと有線通信 （LAN 接続） されている。
ＨＥＭＳ コントローラはウイルス感染の脅威が想定される。
ＨＥＭＳ コントローラはウイルス感染の脅威に対して、脆弱性対策、アンチウィルス ソフトウェア署名、セキュア開発が対策として挙げられる。
ホームルータには、不正アクセス、ＤｏＳ攻撃の脅威が想定される。
ホームルータの不正アクセスには脆弱性対策、ユーザ認証、ＦＷ機能の対策がある。
ホームルータのＤｏＳ攻撃にはＤｏＳ対策が対策として挙げられる。
スマートハウスの屋内には無線通信 （特定小電力）でホームルータと特定小電力無線アダプタが接続されている。
ホームルータと特定小電力無線アダプタ間の無線通信 （特定小電力）には盗聴・改ざんの脅威が想定される。
ホームルータと特定小電力無線アダプタ間の無線通信 （特定小電力）における盗聴・改ざんの脅威に対して、通信路暗号化が対策として挙げられる。
スマートハウスの屋内には無線通信 （Wi-Fi 通信）でホームルータとタブレット端末 （スマホ、ＰＣ）が接続されている。
ホームルータとタブレット端末 （スマホ、ＰＣ）間の無線通信 （Wi-Fi 通信）には盗聴・改ざんの脅威が想定される。
ホームルータとタブレット端末 （スマホ、ＰＣ）間の無線通信 （Wi-Fi 通信）における盗聴・改ざんの脅威に対して、通信路暗号化が対策として挙げられる。
無線通信（ＷｉＳＵＮ）でスマートハウスの屋内の通信アダプタとスマートハウスの屋外のスマートメーターが接続されている。
スマートハウスの屋内の通信アダプタとスマートハウスの屋外のスマートメーターの間の無線通信 （ＷｉＳＵＮ）には盗聴・改ざんの脅威が想定される。
スマートハウスの屋内の通信アダプタとスマートハウスの屋外のスマートメーターの間の無線通信 （ＷｉＳＵＮ）における盗聴・改ざんの脅威に対して、通信路暗号化が対策として挙げられる。
スマートハウスの屋内のタブレット端末 （スマホ、ＰＣ）には不正利用、ウイルス感染の脅威が想定される。
スマートハウスの屋内のタブレット端末 （スマホ、ＰＣ）に対する不正利用の脅威に対して、ユーザ認証、遠隔ロックが対策として挙げられる。
スマートハウスの屋内のタブレット端末 （スマホ、ＰＣ）に対するウイルス感染の脅威に対して、脆弱性対策、アンチウィルス、ソフトウェア署名、セキュア開発が対策として挙げられる。
クラウドサービスには、不正アクセス、DoS 攻撃、情報漏えいの脅威が想定される。
クラウドサービスの不正アクセスの脅威に対して、脆弱性対策、ユーザ認証、FW／IDS／IP、ログ分析、サーバセキュリティが対策として挙げられる。
クラウドサービスの DoS 攻撃の脅威に対して、ＤｏＳ対策が対策として挙げられる。
クラウドサービスの情報漏えいの脅威に対して、データ暗号化、データ二次利用禁止が対策として挙げられる。
監視カメラには個人情報の流出（画像）の脅威が想定される。
監視カメラの個人情報の流出（画像）の脅威に対して、認証設定厳格化が対策として挙げられる。

図２平文の事例



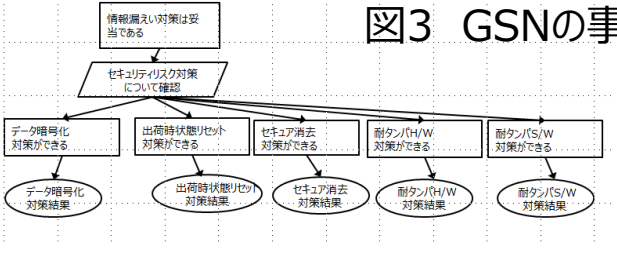


図3　GSNの事例

CC-Caseの有効性評価実験

【設問1】 ①CC-Case＞②GSN＞③平文
【設問2】 正解率は平文．正答率はCC-Caseが優位
【設問3】 リスク対応率　有効な値を得られていない
【設問4】 分析の容易さ:①CC-Case＞②GSN＞③平文
【設問5】 理解しやすさ:①CC-Case＞②GSN＞③平文
【設問6】 可視化の観点:①CC-Case＞②GSN＞③平文
【設問7】 妥当性の観点:①CC-Case＞②GSN＞③平文

CC-Caseは全般的に高い評価
GSNと違いがでるのが不明であったが，プロセスベースで形式化を図ったCC-Caseの方が有用であるとの評価になった

アンケート結果より（CC-Caseが良いと記述した理由）

- 「平文と比較して多量の文章を読まなくてよい．GSNと比較して多量のツリー図をみなくてよく全体を見通しやすい．」，「脅威や対策が見やすい」，「問題と解決がまとめて横並びにされていて見やすい．」「エビデンスとの対応がわかりやすく見やすいと思いました．」，「コンパクトにまとまっているCC-Caseが見やすいし，図の形さえわかれば，理解できるため有効そうだと思った．」

- まとめと今後の方向性

まとめ：CC-Caseのフレームワークを構成する技術要素

- 本日説明対象外とした①②④も含め、具体的事例適用を進める

分類	具体的技法	技術のポイント	IoT対応今後の方向性
①プロセス	CCのセキュリティライフサイクルプロセス	CCに規定されたセキュリティプロセスとセーフティプロセスをすり合わせ	各機能安全規格等の設計プロセスも適用
②リスク分析	SARM、STAMP/STPA-Sec	一般の機能要求とセキュリティ要求を統合的に分析	制御システムのリスク分析も可能に 機器間の網羅的セキュリティ要求分析が可能
③機能要件	ＰＰ（プロテクションプロファイル）の活用	準形式化したセキュリティ機能要件で共通言語化	幅広い機器への要件化で認証方式としての効率的な保証を可能に
④保証要件	CCの保証要件の活用	ＥＡＬの評価基準を利用	セーフティと合わせた評価基準化が必要
⑤アシュアランス	ＧＳＮ	セキュリティケースとして脅威分析、セキュリティセーフティのすり合わせ、インシデント評価に利用。論理の見える化を図る	ライフサイクルにわたるイテレーショナルなトレーサビリティ技法化

IoT時代に向けたCC-Caseのポイント

IoTセキュリティ認証に最適対応を図る開発方法論

＜要求＞

- 多様・複雑化するリスクを洗い出せるセーフティ・セキュリティのリスク手法を確立（SARM、STAMP/STPA−SEC）→変化するリスクへの対応

- アシュアランスケースの論理モデルにISO15408にのみならず各種共通基準を適用→機能安全規格からプロジェクトの開発基準まで各種プロセス準拠の説明責任を果たす

＜保証＞

- ツールボックスとしてのPP機能要件を拡張・活用→効率的なセキュリティ機能開発

- アシュアランスケースによるライフサイクルのトレーサビリティ確保

- セキュリティ保証要件の拡張・活用

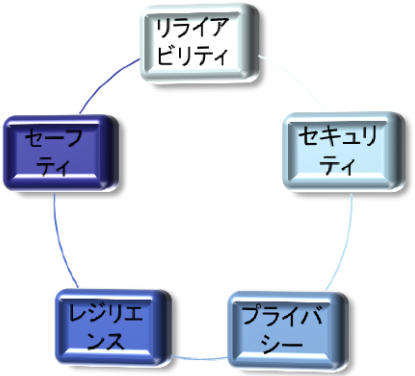
CC-Caseの目指す方向性

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- IoTの5つの特性をサポートする高信頼な開発方法論へ展開

- 企画・分析段階から始まるが、ライフサイクルをサポートできる開発方法論
  各工程ごとのリファレンス技術を吟味し、全体をつなげる方法論にする

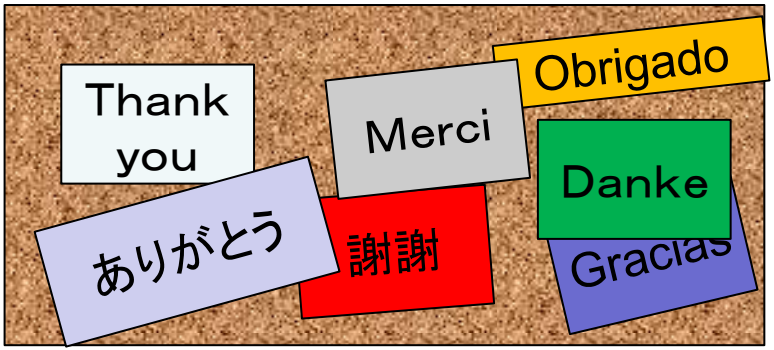
- アシュアランスケースを、工程を超えたイタレーティブに利用する方法論の確立



多様で複雑だからこそ、全体観にたったフレームワークが必要

IoT時代の安全安心の開発方法論CC-Case

ご清聴ありがとうございました!!



参考文献

1) IPA, つながる世界の開発指針，http://www.ipa.go.jp/files/000054906.pdf（2016）
2) IPA, つながる世界のセーフティ＆セキュリティ設計入門ーIoT時代のシステム開発『見える化』, http://www.ipa.go.jp/sec/reports/20151007.html (2015)
3) IPA, IoT開発におけるセキュリティ設計の手引き, https://www.ipa.go.jp/files/000052459.pdf(2016)
4) 金子朋子,山本修一郎,田中英彦,アクタ関係表に基づくセキュリティ要求分析手法（SARM）を用いたスパイラルレビューの提案，情報処理学会論文誌（ジャーナル）Vol.52 No.9（2011）
5) 田渕治樹：国際規格による情報セキュリティの保証手法,日科技連（2007）
6) セキュリティ評価基準（CC/CEM）：http://www.ipa.go.jp/security/jisec/cc/index.html
7) 金子朋子，山本修一郎，田中英彦：CC-Case―コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法, 情報処理学会論文誌(ジャーナル)Vol.55No.9（2014）
8) Kaneko,T.,Yamamoto, S. and Tanaka, H.: CC-Case as an Integrated Method of Security Analysis and Assurance over Life-cycle Process, IJCSDF 3(1): 49-62 Society of Digital Information and Wireless Communications, 2014 (ISSN:2305-0012)
9) 金子朋子，村田松寿：セキュリティ基準コモンクライテリアが変わる-ユーザもベンダも乗り遅れるな！, 情報処理学会デジタルプラクティス．Vol6 No.1（2015）
10)金子朋子,より安全なシステム構築のために～CC-Case_iによるセキュリティ要件の見える化,日本セキュリティ・マネジメント学会（2016）：JNSA15周年記念論文 学術部門優秀賞受賞論文
11)金子朋子,髙橋雄志,勅使河原可海, 田中英彦,CC-Caseを用いたIoTセキュリティ認証方法の提案,CSEC研究会論文（2016）
12)金子朋子,髙橋雄志,勅使河原可海,吉岡信和,山本修一郎,大久保隆夫，田中英彦, セキュリティ要求分析・保証の統合手法CC-Caseの有効性評価実験,CDS研究会論文（2017）

アシュアランスケースを詳しく学習するために

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

【書籍教材】

- **D-Case入門 ～ディペンダビリティ・ケースを書いてみよう！～**
  松野裕、高井利憲、山本修一郎
  発行所　株式会社ダイテックホールディング
  http://www.dcase.jp/pdf/JissenDCase.pdf

- **実践D-Case ディペンダビリティケースを活用しよう！**
  松野裕、山本修一郎
  2013年3月25日発行
  ISBN 978-4-86293-091-0
  http://www.dcase.jp/pdf/JissenDCase.pdf

基礎編
5．アシュアランスケース概論
6．D-Case作法
応用編
7．D-Case演習
8．議論分解パターン
9．D-Case Editorの使い方

3．D-Case/GSNの基礎
4．D-Case作成法
5．議論分解パターン

- **D-Case Stencil - PowerPoint Add-in for D-Case**
  http://www.jst.go.jp/crest/crest-os/tech/D-CaseStencil/index.html

【ビデオ教材】

- **GSN解説(1) - GSN (Goal Structuring Notation)とは何か？** 名古屋大学 山本修一郎教授 (2:58)
  https://www.youtube.com/watch?v=cV8oJ4mcMwM

- **GSN解説(2) - GSNの基礎とその構成要素** 名古屋大学 山本修一郎教授 (2:32)
  https://www.youtube.com/watch?v=0OOxmxrnZS0

- **アシュアランス・セイフティーケース概論 ～歴史的背景と制度～ 産総研　田口研治 招聘研究員**(4:54)
  https://www.youtube.com/watch?v=VedmkvMcBEg