FUJITSU

IoTクラウド向けのセキュリティ品質向上のための品質要件の体系化の取り組み

株式会社富士通ゼネラル
空調機商品開発本部
空調機商品技術部
AI技術開発部　奥村聡司

目次

- 背景
- 従来のセキュリティ対策について
- 課題と方針
- 今回作成したセキュリティ要件リストについて
- セキュリティ要件リストの利用方法
- まとめ

背景

- 近年、ICT（情報通信技術）の急激な進歩によって、今まで独立していた機器はセンサーを通じてインターネット上に接続することで、サービスの享受やデータの収集、分析によるサービスの向上が図られるようになってきた。

インターネットに接続されるようになった製品例
・ウェアラブル機器
・テレビなどの家電
・監視カメラ
・自動車
など

クラウド、センサデータの利用、AI学習、遠隔操作など様々なサービス、製品が増えてきている

背景

- 様々な機器がインターネットにつながることにより想定されるセキュリティリスク

・インターネットからの不正アクセス、乗っ取り等による機器の不正操作

⇒異常な設定や他の機器へのアクセスの経路としての利用

・DoS/DDoS攻撃のアクセス増加によるクラウドサーバー負荷

⇒サービス停止による事故の発生

・個人情報やデータの漏洩

従来のセキュリティ対策について①

FUJITSU

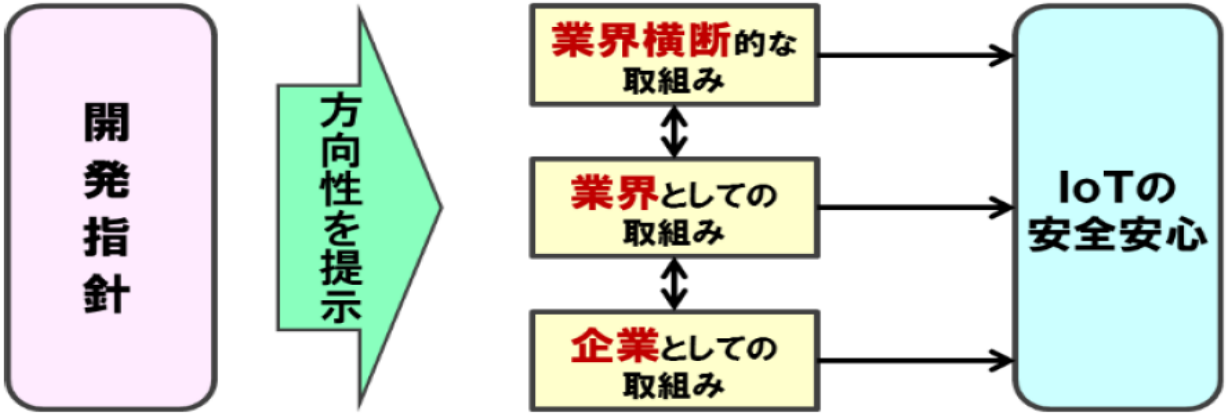
- IPAからIoT製品開発の指針が提示されており、対策の実施は当事者の判断で行うよう記されている
- 指針の使い方
  - チェックリスト

・IoT 製品やシステムの開発時のチェックリストとして利用する

  - カスタマイズ

・指針で記述している事項は、検討時に企業や団体、業界の実情に合わせてカスタマイズして利用する

・内部での開発のみならず受発注の要件確認にも活用する



引用：IPA/つながる世界の開発指針～安全なIoTの実現に向けて開発者に認識してほしい重要ポイント～

従来のセキュリティ対策について②

FUJITSU

- 現在、セキュリティについての資料や文献は少なく、対策が具体的でないものが多い
  - 必要な機能がおおまかにまとめられ書かれているもの
  - ガイドラインとしてセキュリティ対策の指針と要点がまとめられているもの
  - 事例や攻撃方法が書かれているもの

IoT 高信頼化機能			
1	初期設定機能	13	状態可視化機能
2	設定情報確認機能	14	構成情報管理機能
3	認証機能	15	隔離機能
4	アクセス制御機能	16	縮退機能
5	ログ収集機能	17	冗長構成機能
6	時刻同期機能	18	停止機能
7	予兆機能	19	復旧機能
8	診断機能	20	障害情報管理機能
9	ウイルス対策機能	21	操作保護機能
10	暗号化機能	22	寿命管理機能
11	リモートアップデート機能	23	消去機能
12	監視機能		

引用：IPA/つながる世界の開発指針の実践に向けた手引き

大項目	指針	要点
方針	指針1 IoT の性質を考慮した基本方針を定める	要点 1. 経営者が IoT セキュリティにコミットする
		要点 2. 内部不正やミスに備える
分析	指針2 IoT のリスクを認識する	要点 3. 守るべきものを特定する
		要点 4. つながることによるリスクを想定する
		要点 5. つながりで波及するリスクを想定する
		要点 6. 物理的なリスクを認識する
		要点 7. 過去の事例に学ぶ
設計	指針3 守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする
		要点 9. つながる相手に迷惑をかけない設計をする
		要点 10. 安全安心を実現する設計の整合性をとる
		要点 11. 不特定の相手とつなげられても安全安心を確保できる設計をする
		要点 12. 安全安心を実現する設計の検証・評価を行う
構築・接続	指針4 ネットワーク上での対策を考える	要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける
		要点 14. 機能及び用途に応じて適切にネットワーク接続する
		要点 15. 初期設定に留意する
		要点 16. 認証機能を導入する
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点 17. 出荷・リリース後も安全安心な状態を維持する
		要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える
		要点 19. つながることによるリスクを一般利用者に知ってもらう
		要点 20. IoT システム・サービスにおける関係者の役割を認識する
		要点 21. 脆弱な機器を把握し、適切に注意喚起を行う

引用：経済産業省/IoTセキュリティガイドラインver1.0

セキュリティ対策の課題と方針

FUJITSU

- インターネットに繋がる製品やクラウドサービスの増加によりIoTデバイスの開発者が新たにセキュリティの対策をする必要がでてきた

  ⇒セキュリティ面の仕様やテスト方法がまとまっておらず、

  セキュリティ対策が十分であるか確認ができない

セキュリティ対策をまとめた「セキュリティ要件リスト」を作成

IoT、クラウド関連の製品開発に利用し、セキュリティ対策を確認、保証する

セキュリティ要件リストの項目の方針①

FUJITSU

- 既存のセキュリティ対策の知見から当社製品、サービスに必要なものを抽出
  - 当社で以前使用したセキュリティのST項目
  - 安全なWebアプリケーションの作り方/徳丸浩
  - つながる世界の開発指針/IPA
    - ・開発製品にかかわるもの、クラウドや通信路など

- 今回、対象外としたものの例

・ルータやスマートフォン本体のセキュリティに関するもの

→ルータやスマートフォンの開発は行っていないため

・PCI DSS（クレジットカード）

→クレジットカードの情報を扱わないため

セキュリティ要件リストの項目の方針②

FUJITSU

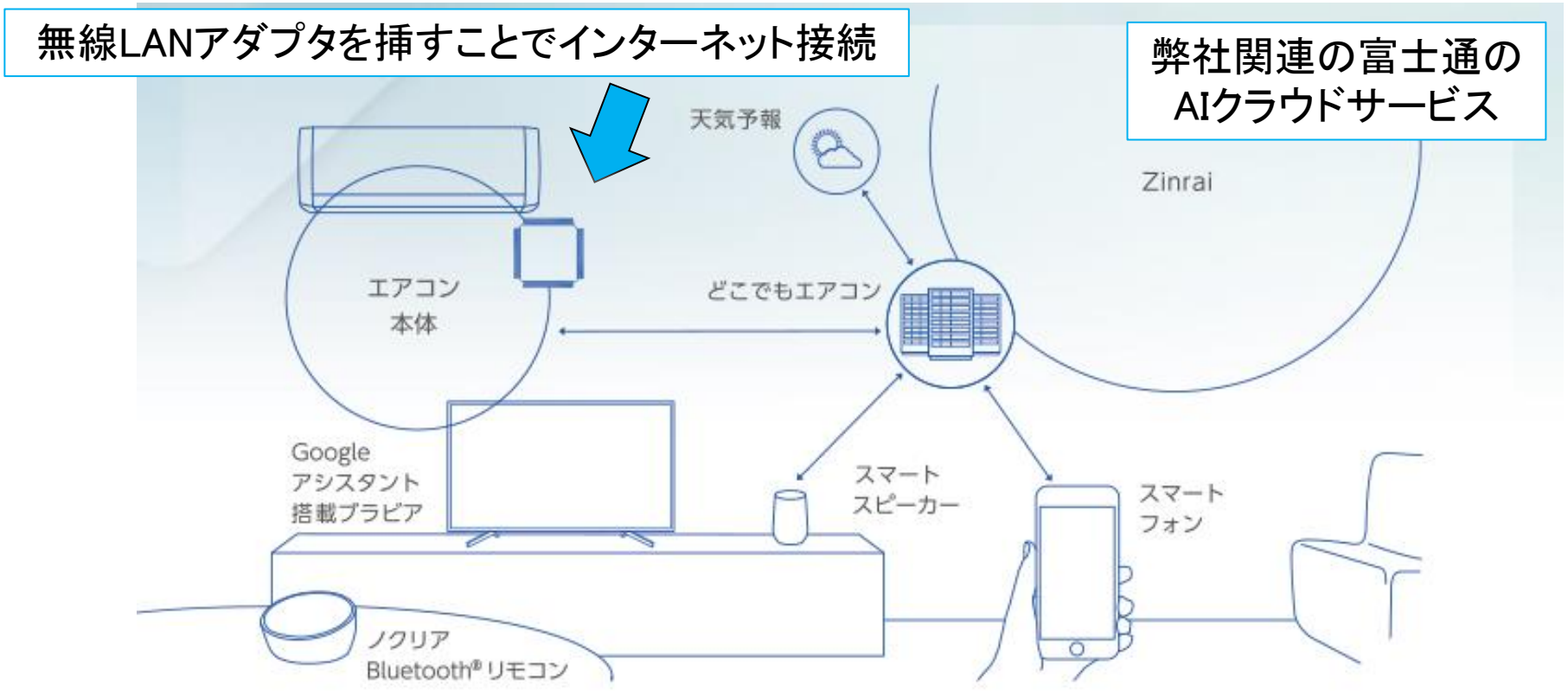
■ セキュリティ要件リストを作成するにあたり必要なポイント

1. 対策方法や検証方法を具体的に記載
2. 網羅性の確保
3. セキュリティ対策の対象を分類

・リストは発注の要件確認に使用できるように、また必要項目を当社向けにカスタマイズ
・主に空調機システムについてのセキュリティ対策をまとめ要件リストを作成
・要件リストでは対象やパターンを分類し、システムの安心安全を目指す

システム構成

■ 当社ルームエアコン（2019年）モデルの構成図



対策例
・通信路の暗号化
・エアコン等への不正アクセス対策
・クラウドのDos,DDos対策

セキュリティ要件リストの対象と分類について

FUJITSU

- セキュリティの対象をクラウド、エッジ、デバイスの大きく3種類に分類
  - 当社のシステムに合わせると

クラウド・・・クラウド（スマホ、AI、保守）

エッジ・・・無線LANアダプタ

デバイス・・・エアコン、リモコン

- IPAによってセキュリティ対策を大きく分けて6種類に分類されている

	デバイス	エッジ	クラウド
認証	○	○	○
アクセス制御			○
ログ収集		○	○
ウィルス対策	○	○	○
暗号化			○
アプリ脆弱性			○

表2 対象とそれぞれの必要セキュリティ

ユーティリティツリーについて

- セキュリティの項目を関心事から定量評価可能なシナリオでまとめたユーティリティツリーを作成
- 定量的な評価にすることで曖昧なものをなくす
- セキュリティのシナリオより要件リストを作成

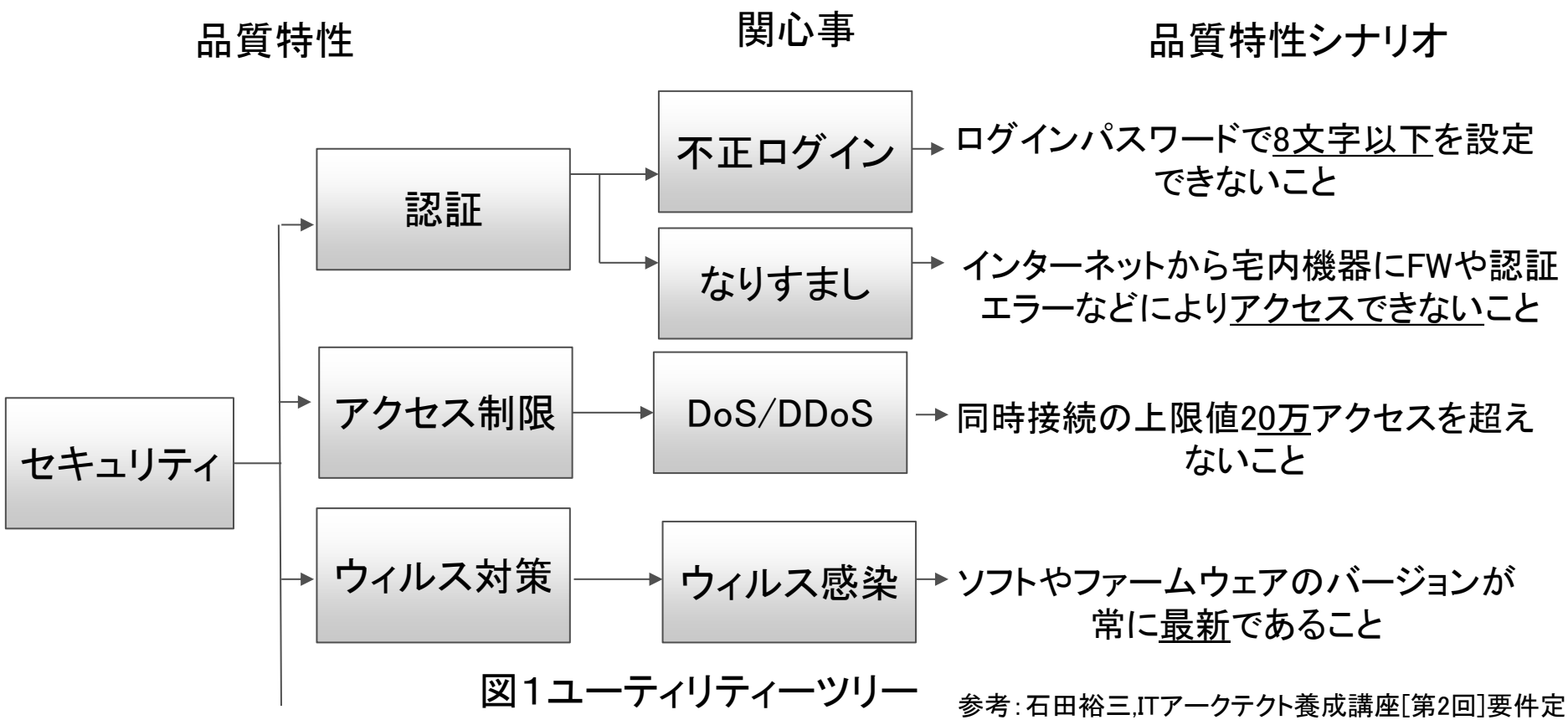


図1ユーティリティーツリー

参考：石田裕三,ITアーキテクト養成講座[第2回]要件定義

セキュリティ要件リスト

FUJITSU

■ コンテンツ

・対象、あるべき仕様、重要度、検証方法、事例

・品質特性シナリオと検証方法の記載により、仕様と設計での確認とテストでの確認に用いることができる

No	対象			大項目	中項目	関心事（事例、未実装のリスク）	品質特性シナリオ	重要性 ※特に重要なものは★	検証方法	補足説明	備考
	デバイス	エッジ	クラウド								
1	○		○	認証		不正ログイン	パスワードのチェック（桁数、文字種類、IDと同じパスワードの禁止、ありがちな単語の禁止）をする。	重要★	安易なパスワードを入力して拒否されることを確認	【例】8文字以上の文字列であること パスワードに数字や記号が含まれていること	安易なパスワード例シート参照
2	○		○	認証		不正ログイン	アカウントロック（ID毎に間違いの回数を数える、上限値を超えるとロック）をする。正常にログインした場合はパスワード		複数回認証失敗させ、機能制限されることを確認		上限値は10回程度が良い 実際に総当たり攻撃があると、ロックさ

要件リストについて

FUJITSU

■ 要件リストの内容について

全項目数：156項目

認証：22項目、認可（アクセス制御）：24項目、Webアプリ脆弱性：68項目、

ログ収集機能：7項目、ウィルス対策：33項目、暗号化機能：2項目

→全156の内、重要★（特に重要なもの）：67項目、重要:75項目

（システム開発の経験者の暗黙知を重要度として明文化）

<u>最低限、重要な項目を確認することで効率の良い開発を行うことができる</u>

テストについて

FUJITSU

- 自社開発製品のセキュリティ対策は仕様・設計し、テストする

- 他社のクラウドサービスなどは設計や詳細なテストができない場合があるため、契約時にセキュリティ対策についての要求を出し、サービスとして保証してもらう必要がある

	仕様・設計	テスト
自社開発	○	○
調達（他社）	×	△

表3 検証パターン

例：セキュリティ診断ツールの適用

FUJITSU

テストに関しての注意事項

- Webアプリケーション脆弱性については確認する内容が多く、確認に時間がかかる。そこでセキュリティ診断ツールを活用することで工数が削減でき、確認漏れなども防止できる

  - 診断ツールの例：

・ポートスキャナ　Nmap

→ポートをスキャンして外部からアクセス可能か調査

・脆弱性スキャナ　OWASP ZAP

・脆弱性スキャナ　nikto

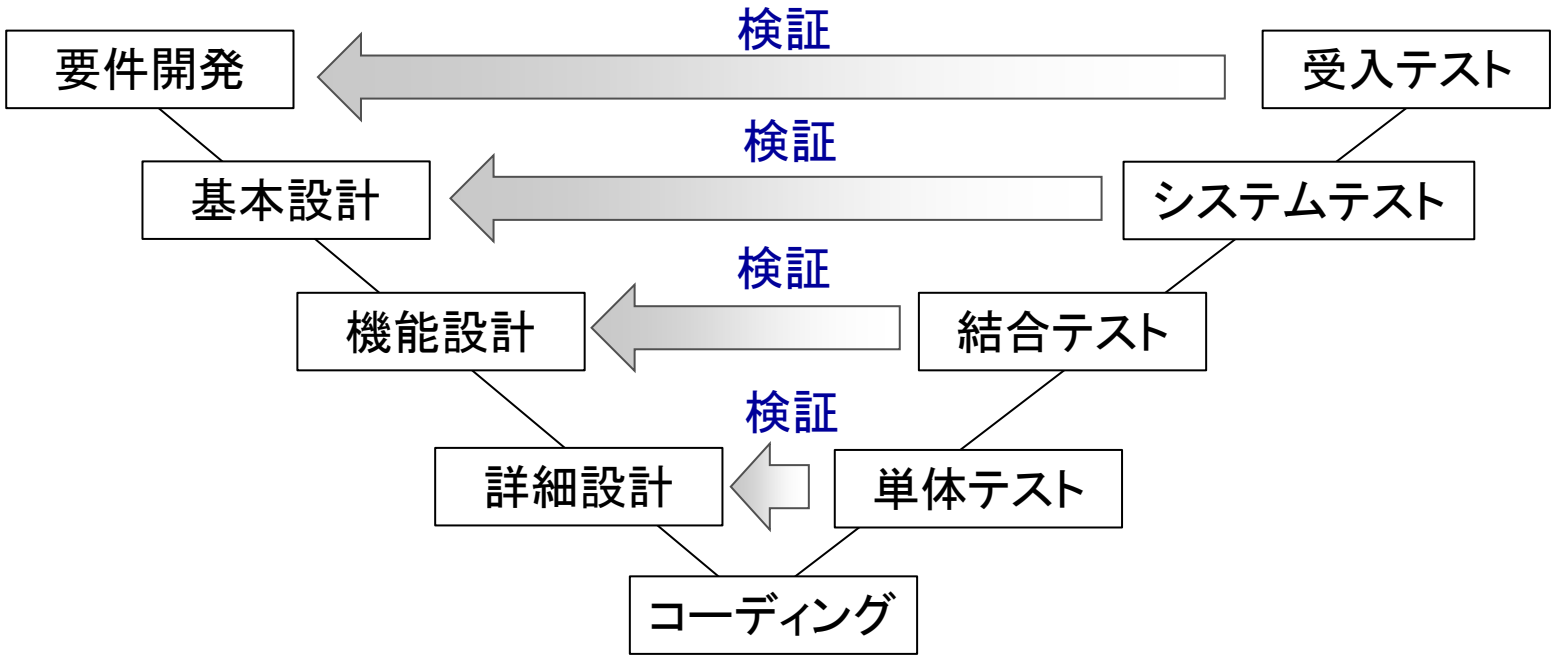
→調査対象となるWebアプリケーションへ攻撃を仕掛けて弱点を診断する

これらの診断ツールは自動で診断してくれるため便利であるが、ハッカーとして誤認識されることや不正アクセス禁止法に接触する可能性があるため使用する際は注意しなければならない

セキュリティ要件リストの利用について

利用方法

システム開発工程において要件、設計、テストに使用する



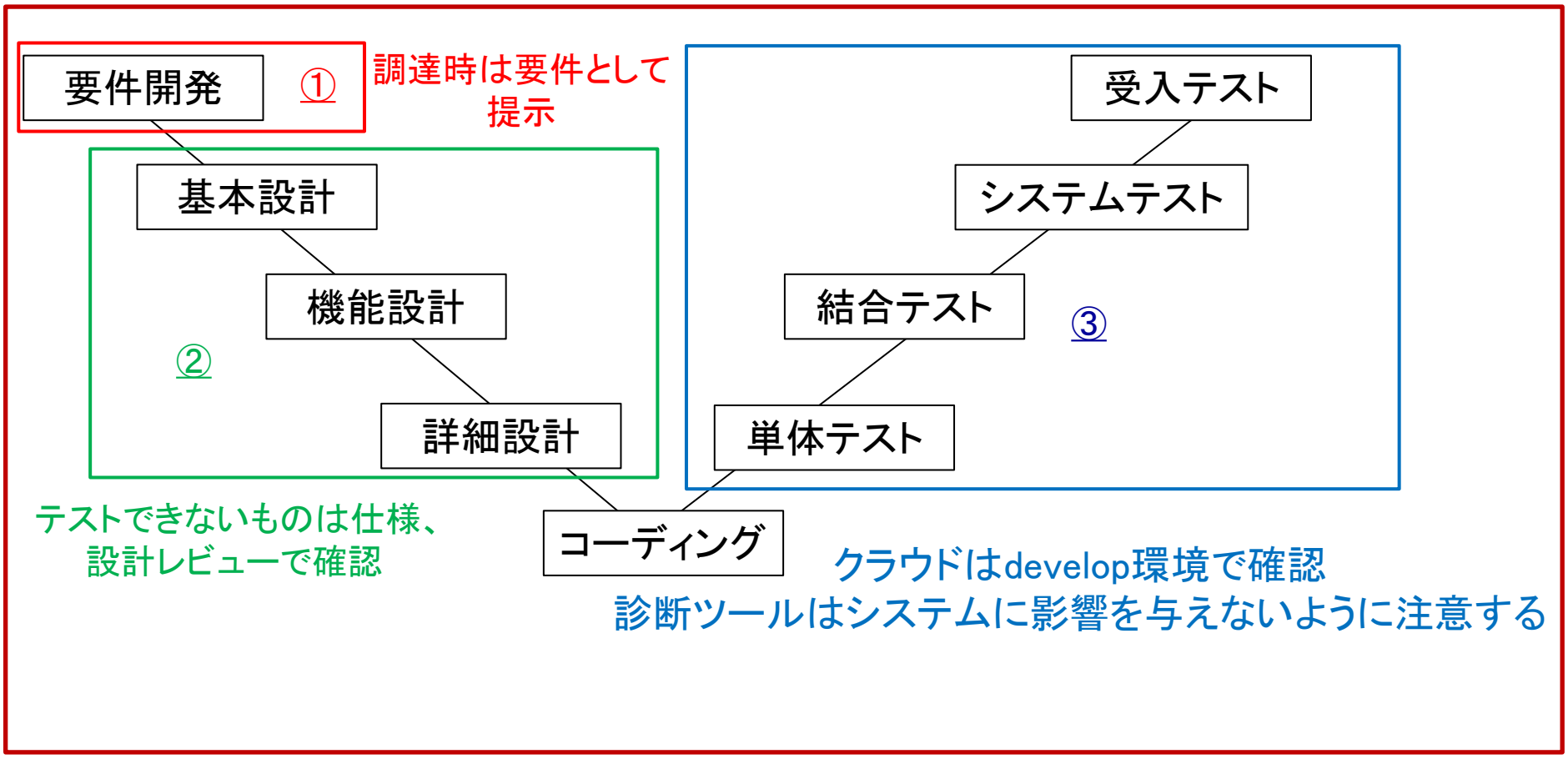
V字モデル

セキュリティ要件リストの利用について

①調達時に要件としてリストを提示

②設計時に仕様を確認

③テスト時に検証する



まとめ

FUJITSU

・IoT、クラウドのシステム、製品開発についてのセキュリティ対策として要件リストを作成した

・ユーティリティーツリーによる対策の網羅性、経験者による重要度付け、対象の判別により必要なセキュリティ対策を効率よく行い、ソフトウェアやシステムの品質を保つことができる

今後について

・リストはIoTやそれに関わるクラウドに特化したものであり、対象外として外した項目（クレジットカードに関するものなど）があり、これらの用途向けには更なる拡張が必要である

・サイバー攻撃は常に新しいものが出てくるため最新情報を収集し、対策を更新していかなければならない

参考文献

- 徳丸浩,安全なWebアプリケーションの作り方 第2版,2018,SBクリエイティブ株式会社
- IPA,SEC,「つながる世界の開発指針」の実践に向けた手引き[IoT高信頼化機能編] ,2017
- IPA,SEC,つながる世界のセーフティ＆セキュリティ設計入門～IoT時代のシステム開発『見える化』～,2015
- IPA,SEC,つながる世界の開発指針 ～安全安心なIoTの実現に向けて開発者に認識してほしい重要ポイント～　第2版,2017
- 経済産業省,IoT セキュリティガイドラインver 1.0,2016
- IPA,企業における情報システムのログ管理に関する実態調査,2016
- 石田裕三,ITアーキテクト養成講座[第2回]要件定義,2012

株式会社 富士通ゼネラル