

セキュリティ品質を考慮したSDLにおける QAの役割(上流工程編)

2017年 第8期ソフトウェア品質保証部長の会 第7グループ

キヤノン（株）
キヤノンOB/日科技連ソフトウェア品質保証部長の会企画委員
（株）モバイルインターネットテクノロジー

日下 宏（リーダー・発表者）
永田 哲
二川 勇樹

※50音順

お伝えしたいこと

あらゆるシステムがネットワークに繋がることでセキュリティ上の脅威が格段に増大したためにシステムのセキュリティ品質の確保が必須になってきました。

私たちソフトウェア品質保証や品質評価部門（QA）は
「セキュリティ品質が高い＝脆弱性が無いソフトウェア開発」
と考えます。

QAとして、ビジネスドメインに応じてセキュリティリスクを軽減した「安全・安心なシステム」をセキュリティデベロップメントライフサイクル（SDL）として保証できる仕組みを考えます。

前期ふりかえり：2016年のセキュリティグループの活動

■ 「セキュリティ開発ライフサイクル（SDL）におけるQAの役割」

2016年の品質シンポジウムでは、このセキュリティグループメンバーの永田氏の講演により、公開されているセキュリティインシデントの事例を題材にセキュリティ問題の深刻度を解説し、「21世紀の品質はセキュリティが必須」であり、その中でQAの役割を定義づけしました。

セキュリティ対策としてセキュリティ品質を確保するためのマイクロソフト社のSDLをベストプラクティスと位置付けて紹介し、ソフトウェア開発プロセスに組み込む方法とQAの役割について考察しました。

しかし、実際に適用する
粒度までは至ってませんでした。

セキュリティ開発ライフサイクル（SDL） におけるQAの役割

セキュリティ対策をソフトウェア開発プロセスに組み込む方法とQAの役割について考察しました。実際の適用は未だですが...

OWASP ASVS／Testing Guide／
MS Threat Modeling Tool 2016
を使用。

SWセキュリティ対策グループ
元キャノン(株) 永田哲（リーダー）
(株)リンクレア 早崎伸二
キャノン(株) 日下宏
(株)モバイルインターネット
テクノロジー 二川勇樹

SDLの例：マイクロソフト

- Microsoft SDLはソフトウェア開発ライフサイクルに必須のセキュリティアクティビティをまとめたものです。

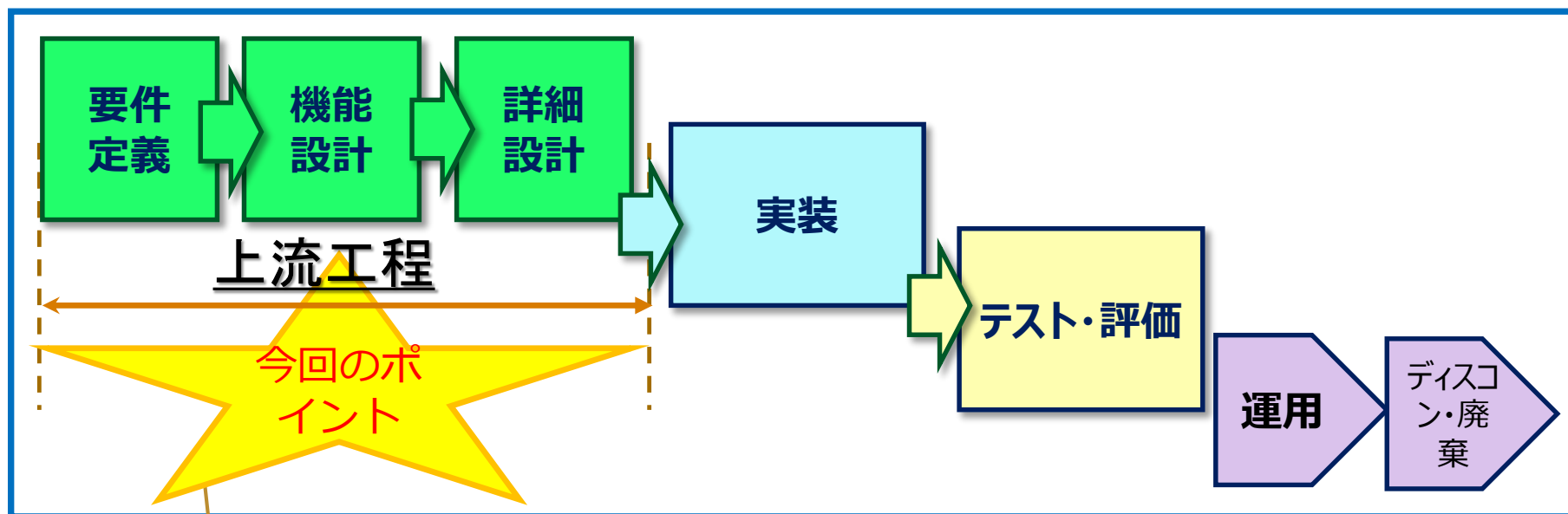


簡略化したマイクロソフトのセキュリティ開発ライフサイクル

出典:マイクロソフト社Microsoft SDL の簡単な実装 Japanese Simplified Implementation of the SDL.docx (2010/12/13)

2017年8期セキュリティグループの活動

- 一般的なソフトウェア開発ライフサイクルを以下のように定義し、要件定義～詳細設計の工程を設計開発上流工程と呼びます。



8期のセキュリティグループは“要件～設計”におけるセキュリティ品質確保方法の具体策を検討し、ソフトウェア開発サイクルがSDL(Security Development Lifecycle)として具体的に機能するよう議論を重ねました。

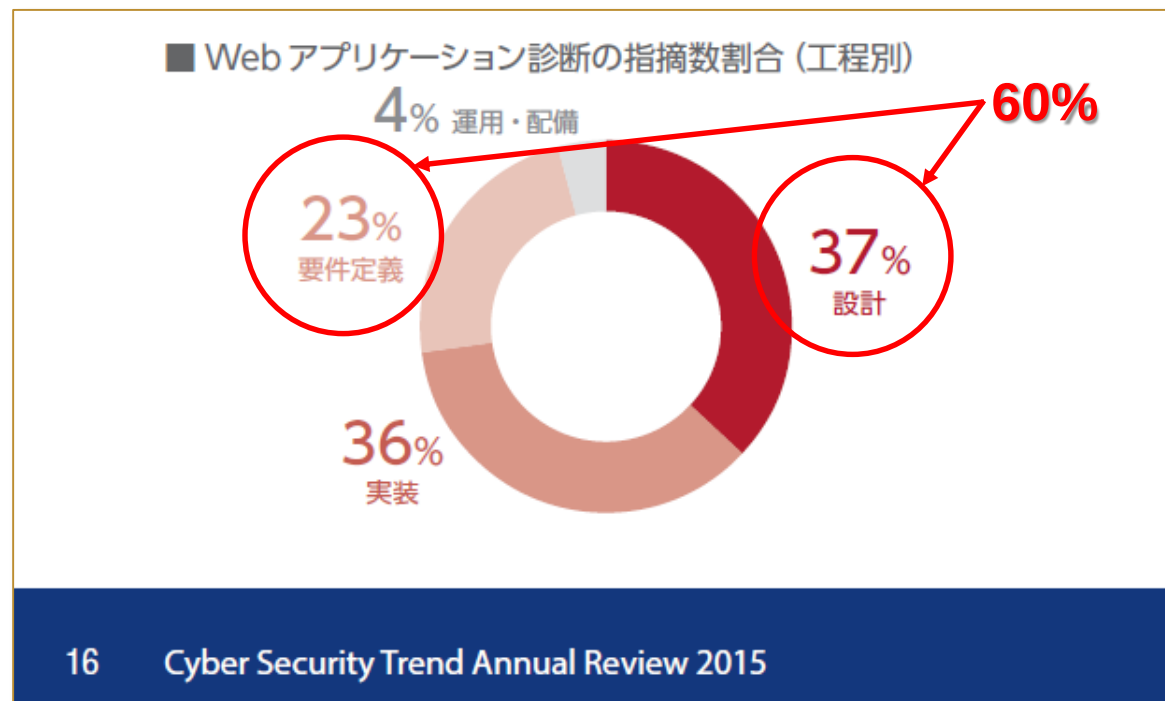
上流工程のセキュリティ対策が必要な理由

設計開発上流工程で60%の脆弱性が埋め込まれています。

(Webアプリケーションの例 N R I セキュアテクノロジーズ サイバーセキュリティ：傾向分析レポート2015より)

工程の初期段階でセキュリティ対策を実施することで以下の効果が期待できます。

- ① 市場へのセキュリティ不備流出の低減や防止
- ② 開発コストやスケジュール超過の防止



16 Cyber Security Trend Annual Review 2015

出典：N R I セキュアテクノロジーズ サイバーセキュリティ：傾向分析レポート2015

セキュリティ品質上流活動の確立に向けて

■ QAとしてセキュリティ品質上流活動を確立したい

- ソフトウェア品質は上流工程で作り込むのと同様に、セキュリティ品質も上流工程で作り込みが必要です。
- プロセスQA視点で、セキュリティ品質を高める活動を実施します。

セキュリティ品質が高い状態 = セキュリティ上の欠点である脆弱性が無い

セキュリティ設計の実施状況をレビューにより検証し、セキュリティ品質を高めるプロセスが正しく実施されている確認を行います。

セキュリティ品質上流活動の確立に向けて

■ QAとしてセキュリティ設計の実施状況を確認したいポイント

- ① 各プロセスの設計書からセキュリティを脅かす存在（脅威）から守るべき情報や機能が特定されている
- ② 各プロセスの設計書からセキュリティを脅かす存在（脅威）が想定され、脅威が利用する脆弱性が抽出されている
- ③ 脅威が利用する脆弱性に対してリスク分析と脆弱性評価が行われている
- ④ リスクを軽減する脆弱性対策の要否や度合いが明確化されている
- ⑤ 脅威にさらされる脆弱性の残存リスクが受容できる

「脆弱性／脅威／リスク」用語の整理

脆弱性はセキュリティ上の**欠点**です。

脆弱性は**脅威**によって**利用される**恐れのある**弱点**です。

脅威とは何らかの**損害の可能性を引き起こす事象**です。

脆弱性は表面化することがなければ問題ありません。

脆弱性を持ったソフトウェアには**リスク**が付きまといます。

リスクとは**脅威に脆弱性が利用されて起きる****危害の発生確率**と、その**危害の程度**の組み合わせです。

リスクを徹底的に低減する（発生確率を0に近づける＋危害の程度を0に近づける）→脆弱性を無くす
→セキュリティ品質が良い状態です。

セキュリティ品質活動の取り組み策

① 守るべき情報・機能資産を明確化する

1. 工程の粒度に合わせてDFD（データフロー図）を作成
2. DFD図から情報資産・機能を明確化

② 脅威が利用する脆弱性を明確化する

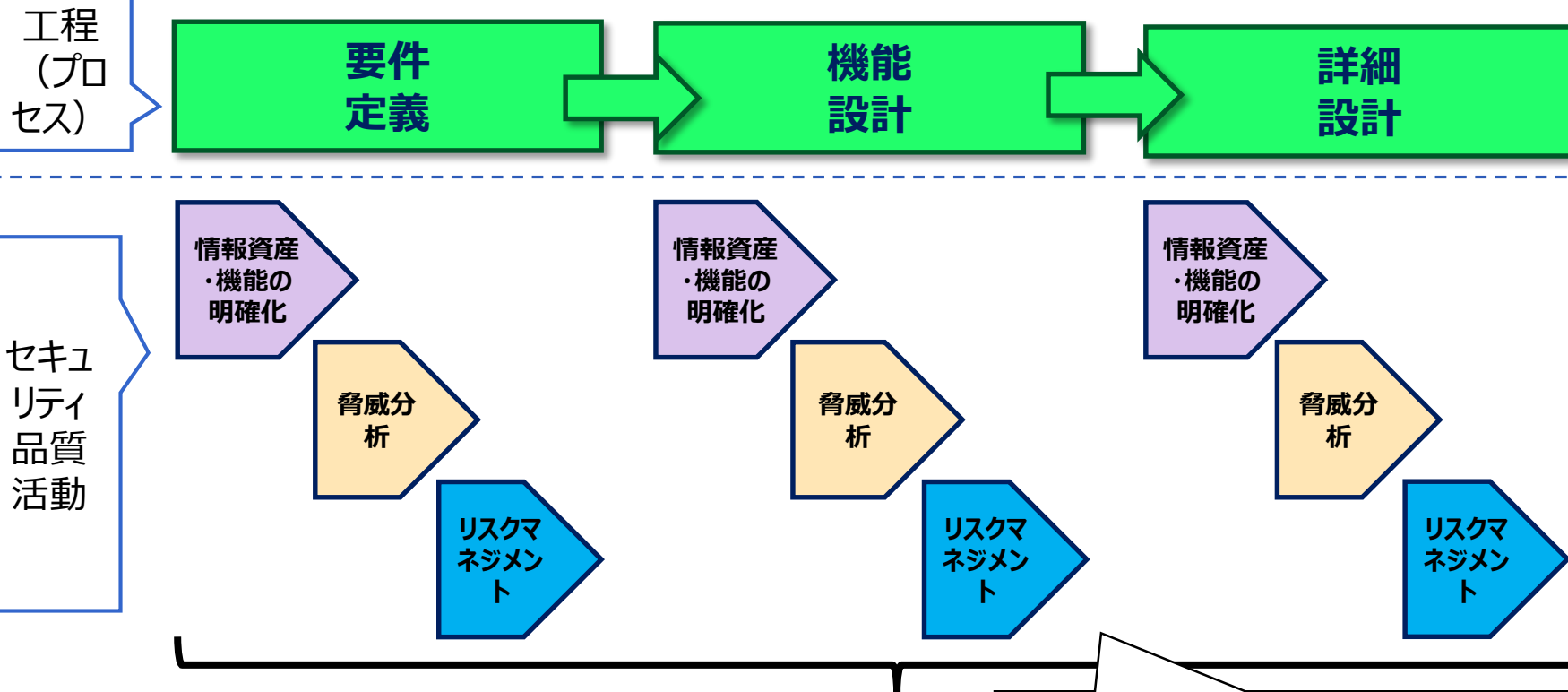
1. DFD図を用いた仕様書から脅威分析
2. 脅威のモデリング → ツールを活用した脅威分析（脆弱性の明確化）

③ 脅威が利用する脆弱性を無くす（軽減化）

1. リスクマネジメントの実施
2. リスクの無効化、軽減

工程におけるセキュリティ品質活動の取り組み

- 反復的にセキュリティ品質上流活動を実施



セキュリティ品質活動の取り組み策(まとめ)

1. 脅威分析が可能な粒度にシステム全体構成を明確化する

◎開発は設計書として**データフロー（DFD）図の作成**

2. 守るべき情報・機能の特定する

- ① 情報資産・機能の名称
- ② 脅威による脆弱性から予見される危害／危険状態
- ③ リスクの推定・評価
 - 1. 発生頻度
 - 2. 価値評価
 - 3. 発生時の損害評価

→**リスクマネジメントの開始：リスクマネジメントチェックシートへ記載**

3. 守るべき情報・機能に対する脅威の想定と利用する脆弱性の明確化する

◎DFD図から脅威分析ツールを活用（**Microsoft Threat Modeling Tool**）

4. 脅威が利用する脆弱性のリスクマネジメントを実施する （次ページへ続く）

脅威分析を工程ごとに実施
（**反復的**に実施）し網羅性
や内容の精度を高めます

セキュリティ品質活動の取り組み策(まとめ)

1. 脅威分析が可能な粒度のシステム全体構成を明確化
2. 守るべき情報・機能の特定する
3. 守るべき情報・機能に対する脅威の想定と利用する脆弱性の明確化
4. 脅威が利用する脆弱性のリスクマネジメントを実施する
セキュリティ上、守るべき情報・機能の価値・損害評価、対策方法から、
リスクアセスメントを実施し対策を決定する(リスクの低減、受容)
ビジネス面を考慮する：経済性（コスト）、期間、被害
→リスクマネジメントチェックシートへ記載（完成）
脅威：システムに損害を与えたり、安定をおびやかす可能性がある存在
脅威とは何らかの損害の可能性を引き起こす事象

脅威分析を工程ごとに実施（**反復的に実施**）し
網羅性や内容の精度を
高めます

セキュリティ品質上流活動の実現方法

データフロー図（DFD）の作成

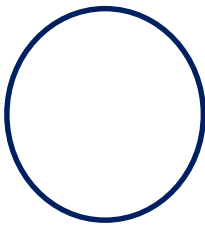
DFD（Data Flow Diagram）

構造化分析において外部エンティティ（実体）からシステムやプロセス間のデータの流を
図で表現し、それらがどのような過程を経て処理されていくかを記述します。

DFDの記載は 4 つの構成要素があります。



①外部エンティティ
データの発生源やデータの行先



②プロセス
データの処理



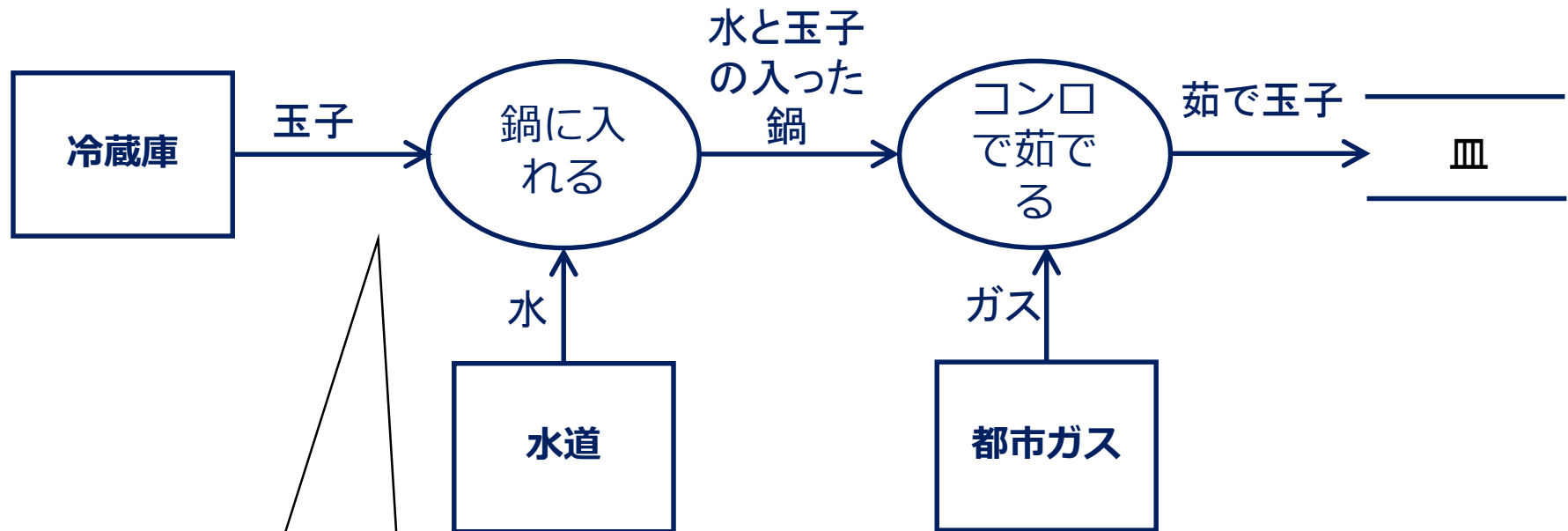
③データストア
一時的なデータの格納先



④データフロー
①、②、③の要素間のデータの
流れ

セキュリティ品質上流活動の実現方法

データフロー図（DFD）の作成例



DFDではプロセスやデータ保管先、データ発生源がアロディヤグラムで表現される。

リスクマネジメントチェックシート

リスクマネジメントを適切に実行した後、全体的な残留リスクが受容可能であることを明確に記録するために、リスクマネジメントチェックシートを作成します。

まず最初はDFD図から情報資産・機能を記載し、リスクの推定・評価を行います。

情報資産・機能	脅威による脆弱性から予見される危害／危険状態	リスクの推定・評価			リスクコントロール			リスク低減策の実施により新たな危害／危険状態等が発生していないか
		① 発生 頻度	② 損害 ／ 重大度	③ 評価	リスク低減方法	リスク低減方法実行後の評価		
						① 発生 頻度	② 損害 ／ 重大度	③ 評価

この範囲を実施します。

情報資産・機能の特定

DFD図から守るべき情報資産や機能を特定します。

先に記載したDFD図作成例から守るべき情報資産・機能の特定してみました。

情報資産・機能	脅威による脆弱性から予見される危害／危険状態	リスクの推定・評価		
		① 発生頻度	② 損害／重大度	③ 評価
玉子	冷蔵庫のドアを勝手に開けて、食材が無くなってお腹が空いて機嫌が悪くなり暴れたす	時々	軽微な	受容可能
水	水栓が開かれたままで水浸しになる	しばしば	重大な	受容できない
ガス	ガス栓が開かれたままでガスが充満して中毒や爆発火災になる	起こりそうにない	破局的	受容できない

脅威分析

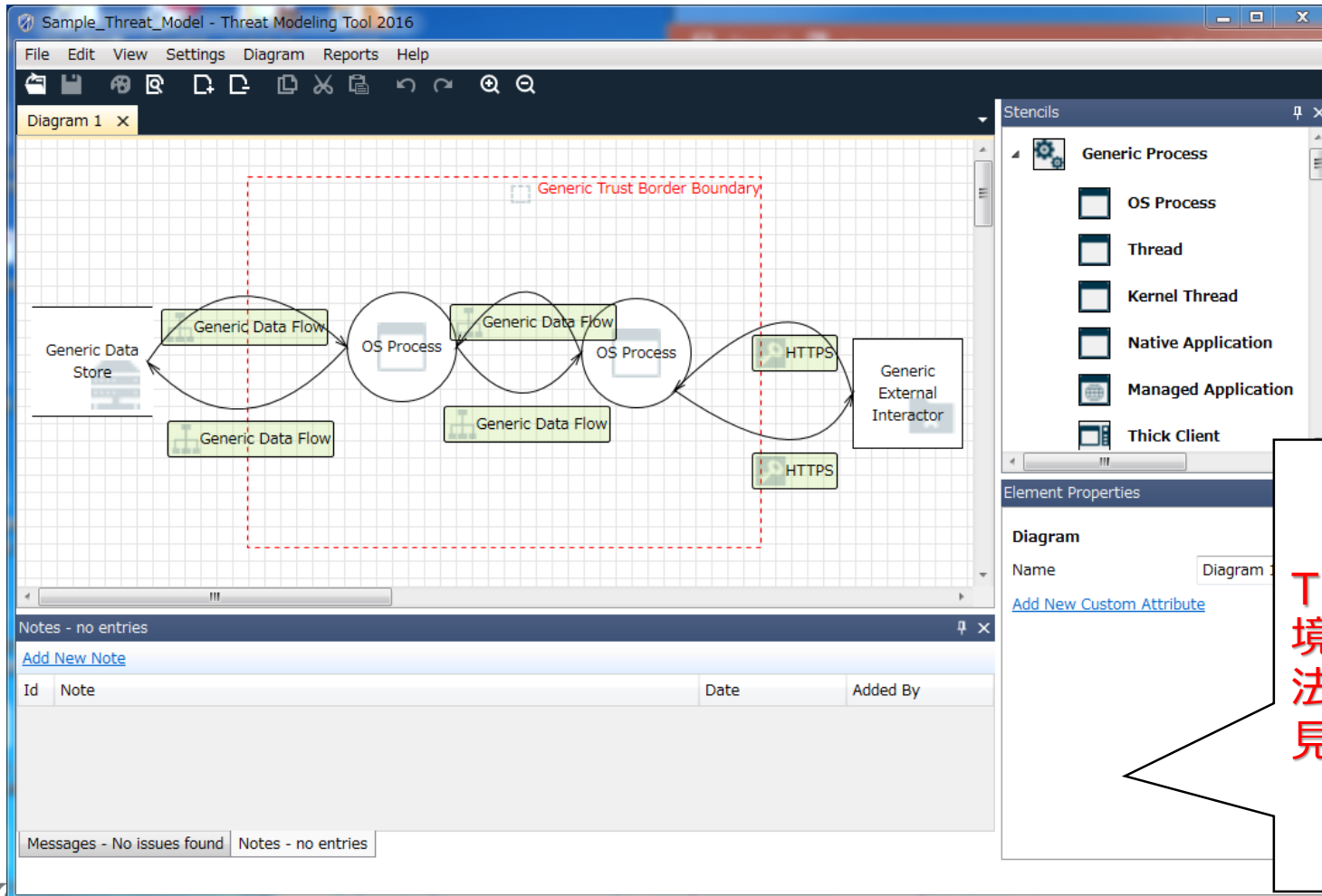
情報資産や機能に損害を与える脅威を洗い出し、分析し、明確化する（脅威分析）にはマイクロソフト Threat Modeling Tool(以降 TMTと呼ぶ）が効率的で有用性があると評価しました。

特徴：

- ① 2017年7月現在、Microsoft Threat Modeling Tool 2016 が無償公開されています
- ② 英語版のみです
- ③ 先に作成したDFD図を効率的に作成する機能が備わっています

ツールを活用した脅威分析

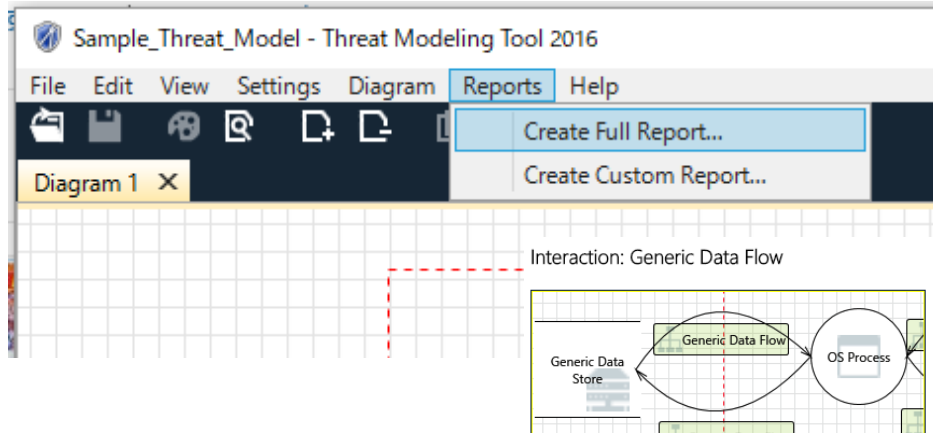
MS Threat Modeling Tool 2016 による脅威分析



TMTはデータフローの境界で、STRIDE手法により脅威を発見する

ツールを活用した脅威分析

MS Threat Modeling Tool 2016 による脅威分析 レポート出力



1. Spoofing the OS Process Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: OS Process may be spoofed by an attacker and this may lead to information disclosure by Generic Data Store. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

2. Spoofing of Source Data Store Generic Data Store [State: Not Started] [Priority: High]

Category: Spoofing

Description: Generic Data Store may be spoofed by an attacker and this may lead to incorrect data delivered to OS Process. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

3. Potential Data Repudiation by OS Process [State: Not Started] [Priority: High]

Category: Repudiation

Description: OS Process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: <no mitigation provided>

4. Weak Access Control for a Resource [State: Not Started] [Priority: High]

リスクマネジメントチェックシート

TMTから脅威による脆弱性から予見される危害／危険状態を記載します。

情報資産・機能	脅威による脆弱性から予見される危害／危険状態	リスクの推定・評価			リスクコントロール			リスク低減策の実施により新たな危害／危険状態が発生していないか
					リスク低減方法	リスク低減方法実行後の評価		
		①発生頻度	②損害／重大度	③評価		①発生頻度	②損害／重大度	
この範囲を実施します。								

この範囲を実施します。

リスクマネジメント

徹底的に脅威を除去する活動は医療機器の開発・品質管理や機械安全の安全性確保を行うためのリスクマネジメント手法と共通しており、すでに確立されているこの考え方が有用であると考えました。

ISO14971/JIS T 14971:2012 医療機器 - リスクマネジメントの医療機器への適用

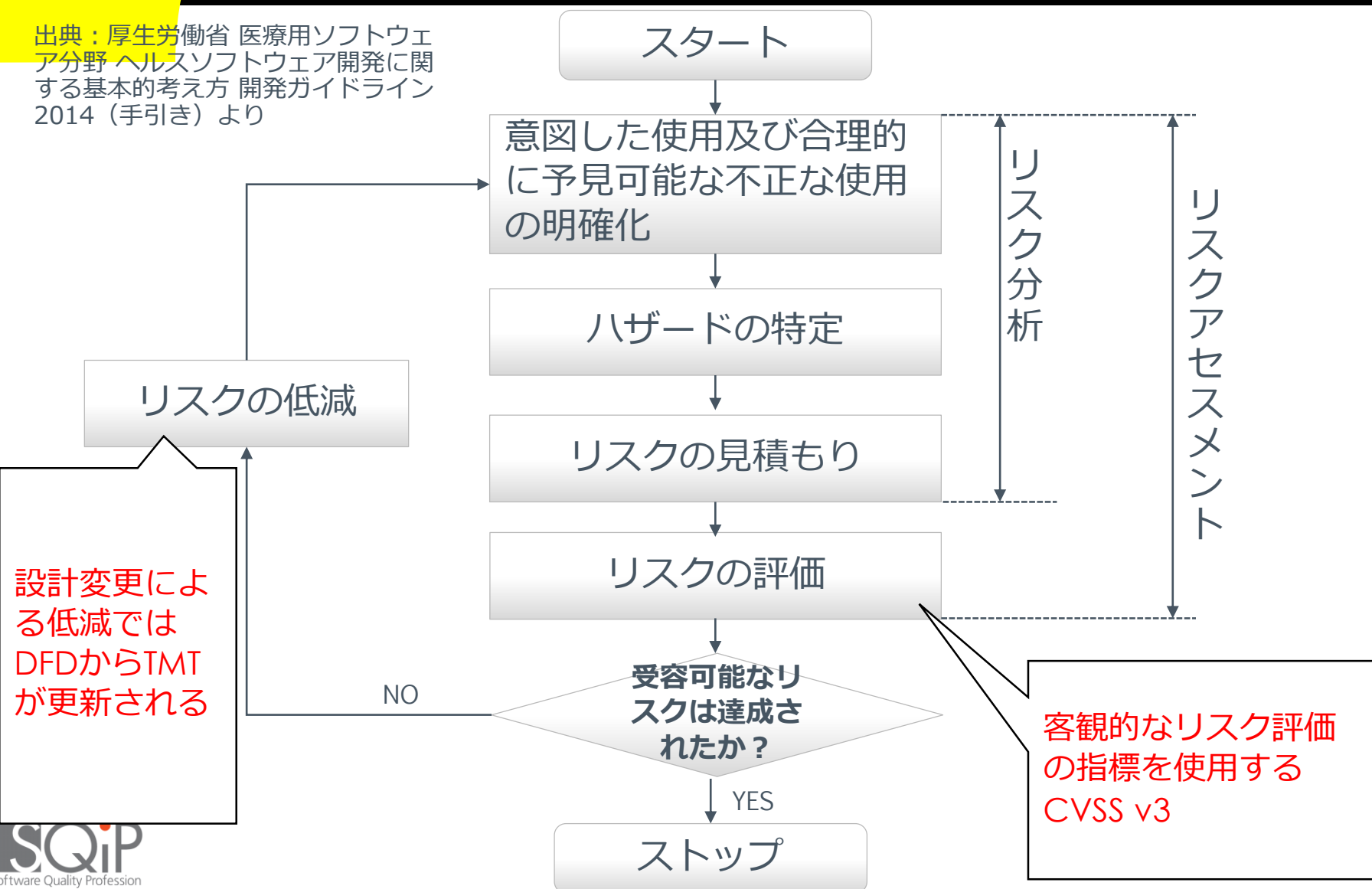
医療機器は法令でリスクマネジメントが要求されています。

ISO/IEC Guide51:2014 / JIS 8051:2015 安全側面－規格への導入指針 製品安全の安全規格体系

安全の国際標準の定義「許容できないリスクがないことと、「危険をゼロにする（絶対安全）」

リスクマネジメント

出典：厚生労働省 医療用ソフトウェア分野 ヘルスソフトウェア開発に関する基本的考え方 開発ガイドライン 2014（手引き）より



リスクマネジメント

ISO/IEC Guide 51では、設計者が想定した使用法(intended use) のみならず、**“合理的に予見可能な誤使用”**(reasonably foreseeable misuse)も含んだ範囲でリスクを評価し、受け入れ可能なレベルに達するまでリスク低減を行う反復プロセスを図示しています。

→「合理的に予見可能な誤使用」をリスクアセスメントの範囲とすることを明記したことが極めて重要です。

セキュリティのリスクアセスメントでは**“非常識な予見困難な攻撃”**を想定してリスクアセスメントを実施します。

リスク評価

リスク評価に、CVSS v3を採用を検討し、客観的なリスク評価ができる点を重視しました。

Threat Modeling Toolから出力された脆弱性を CVSSで評価します。

->リスク評価は

基本評価基準(Base Metrics)で評価

->個々の条件確認やリスク低減後は

環境評価基準(Environmental Metrics)で評価

注) 現状評価基準は脆弱性の現在の深刻度を評価する基準のため使用せず

CVSS v3とは

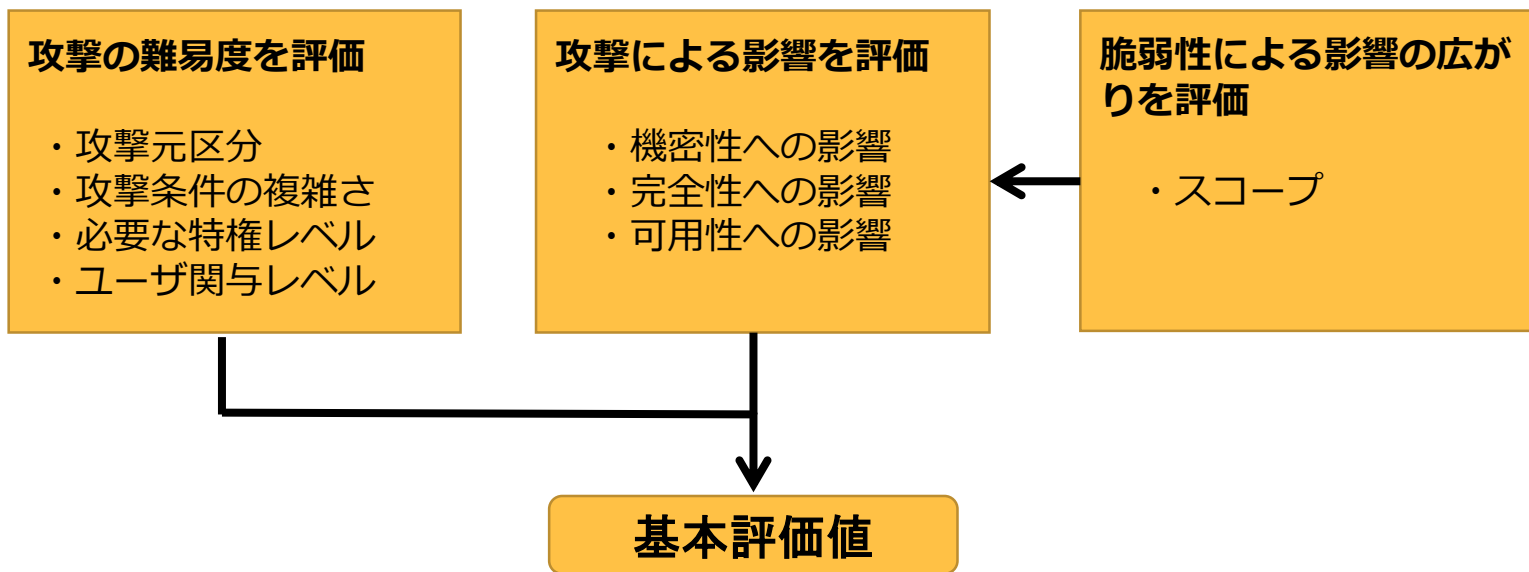
CVSS(Common Vulnerability Scoring System)は、ベンダーに依存しない脆弱性の共通の評価手法。脆弱性の深刻度を同一基準で比較できます。

※CVSS v3の計算は、WEBで公開されているCVSS計算ソフトウェアで可能。

<http://jvndb.jvn.jp/cvss/v3/>

リスク評価

CVSS の基本評価基準の概要



脆弱性そのものの特性を評価する基準。
ベンダーや脆弱性を公表する組織などが、
脆弱性の固有の深刻度を表すために利用。

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

リスク評価

CVSS の環境評価基準の概要

対象セキュリティの要求度を評価

- ・ 対象システムのセキュリティ要求度/機密性
- ・ 対象システムのセキュリティ要求度/完全性
- ・ 対象システムのセキュリティ要求度/可用性

リスク低減後の評価

- ・ 後の攻撃元区分
- ・ 低減後の攻撃条件の複雑さ
- ・ 低減後の必要な特権レベル
- ・ 低減後のユーザ関与レベル
- ・ 低減後のスコープ
- ・ 低減後の機密性への影響
- ・ 低減後の完全性への影響
- ・ 低減後の可用性への影響

環境評価値

ユーザの利用環境も含め、最終的な脆弱性の深刻度を評価する基準。
脆弱性の対処状況を評価し、算出。

リスクの低減

リスク評価した結果、数値が高いものはリスク低減を実施します

低減方法 → **スリーステップメソッド**

- ① 本質安全設計 – 設計変更
- ② 保護手段（安全防護） – 利用環境制限
- ③ 使用上の情報 – マニュアルへの制限事項記載

低減方法を決定や実施後、再度リスクアセスメントを実施

- ① 評価点が受容可能→完了
- ② 評価点が受容不可→低減策を再度検討

リスクマネジメントチェックシート

リスクマネジメントを適切に実行した後、全体的な残留リスクが受容可能であることを明確に記録するために、リスクマネジメントチェックシートを作成します。

リスクマネジメントを適切に実行した後、全体的な残留リスクが受容可能であることを明確に記録作成します。

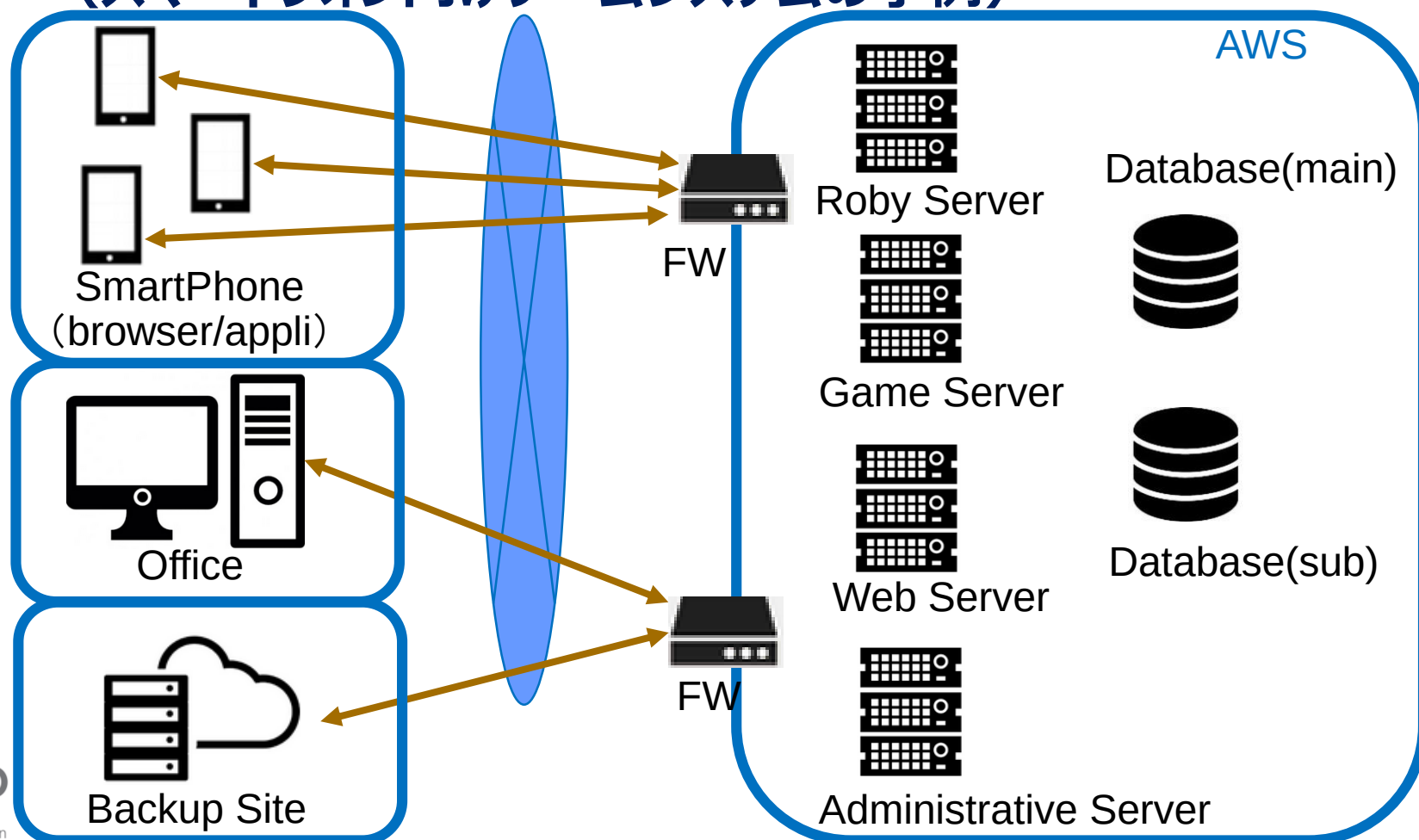
情報資産・機能	脅威による脆弱性から予見される危害／危険状態	リスクの推定・評価			リスクコントロール				リスク低減策の実施により新たな危害／危険状態等が発生していないか
		① 発生 頻度	② 損害／ 重大度	③ 評価	リスク低減方法	リスク低減方法実行後の評価			
						① 発生 頻度	② 損害／ 重大度	③ 評価	

この範囲を実施します。

この範囲を実施します。

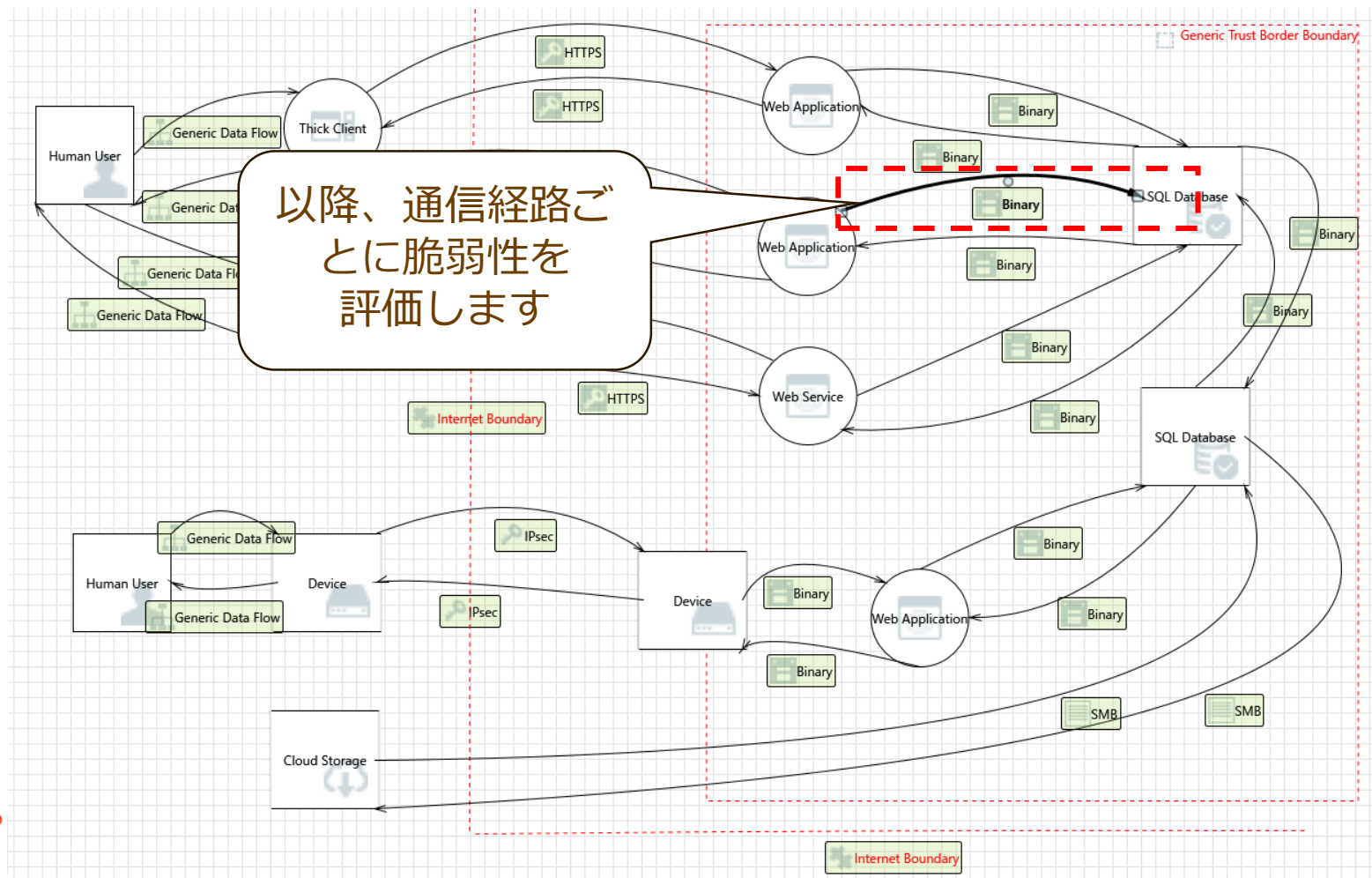
セキュリティ上流品質活動による効果

- 試行した実施事例に基づいて効果や検証結果
(スマートフォン向けゲームシステムの事例)



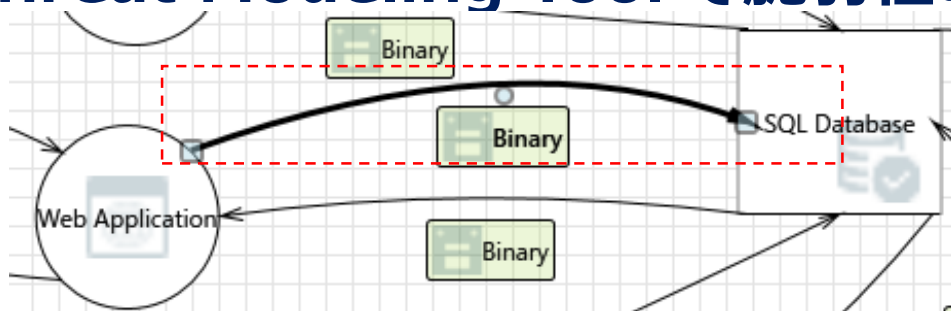
セキュリティ上流品質活動による効果

■ 1) Threat Modeling Tool でDFDの作成



セキュリティ上流品質活動による効果

2) Threat Modeling Tool で脆弱性の分析



CATEGORY: Spoofing

THREAT: Spoofing of Destination Data Store
SQL Database

CATEGORY: Tampering

THREAT: Potential SQL Injection Vulnerability
for SQL Database

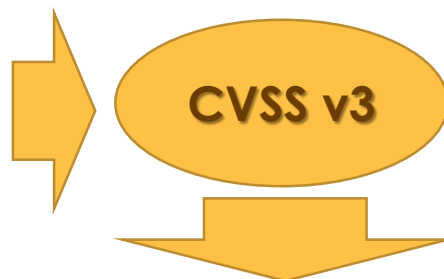
CATEGORY: Denial Of Service

THREAT: Potential Excessive Resource Consumption
for Web Service or SQL Database

セキュリティ上流品質活動による効果

3)脆弱性情報をCVSS v3へ入力し、基本評価値を確認

攻撃区分	影響の想定範囲
攻撃の複雑さ	完全性への影響
攻撃に必要な特権区分	機密性への影響
利用者の関与	可用性への影響



	脆弱性の特性	
	基本評価	深刻度
CATEGORY: Spoofing THREAT: Spoofing of Destination Data Store SQL Database	7.5	重要
CATEGORY: Tampering THREAT: Potential for SQL	9.9	緊急
CATEGORY: Denial of Service THREAT: Potential Excessive Resource Consumption for Web Service or SQL Database	9.1	緊急
通信経路に対する評価値	3件	緊急

通信経路の
脆弱性の深刻度が
「注意」以上の件数

通信経路の
脆弱性の深刻度が
一番高いもの

セキュリティ上流品質活動による効果

4) リスク低減等をCVSS v3へ入力し環境値で効果を確認

機密性の要求度	低減後の攻撃条件の複雑さ	低減後の完全性への影響
完全性の要求度	低減後の攻撃に必要な特権レベル	低減後の機密性への影響
可用性の要求度	低減後の利用者の関与	低減後の可用性への影響
低減後の攻撃元区分	低減後の影響の想定範囲	

CVSS v3

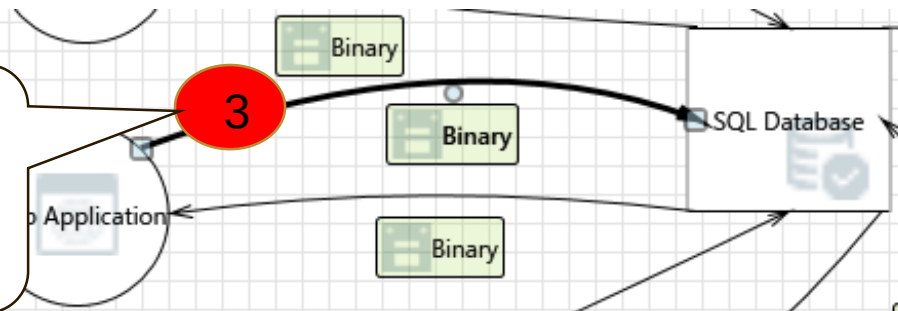
	脆弱性の特性		リスク低減策後	
	基本評価	深刻度	環境評価	深刻度
CATEGORY: Spoofing THREAT: Spoofing of Destination Data Store SQL Database	7.5	重要	3.4	注意
CATEGORY: Tampering THREAT: Potential SQL Injection Vulnerability for SQL Database	9.9	緊急	2.7	注意
CATEGORY: Denial Of Service THREAT: Potential Excessive Resource Consumption for Web Service or SQL Database	9.1	緊急	2.8	注意
通信経路に対する評価値	3件	緊急	3件	注意

セキュリティ上流品質活動による効果

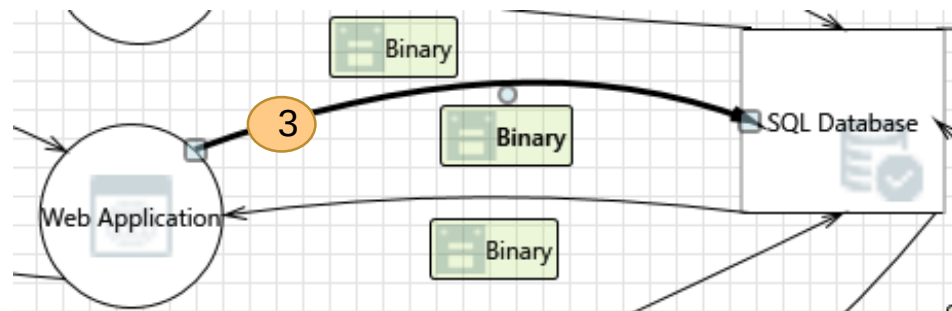
5)脆弱性や対策後対する対策や環境を可視化 DFD上でセキュリティの視認性を高める

[脆弱性評価]

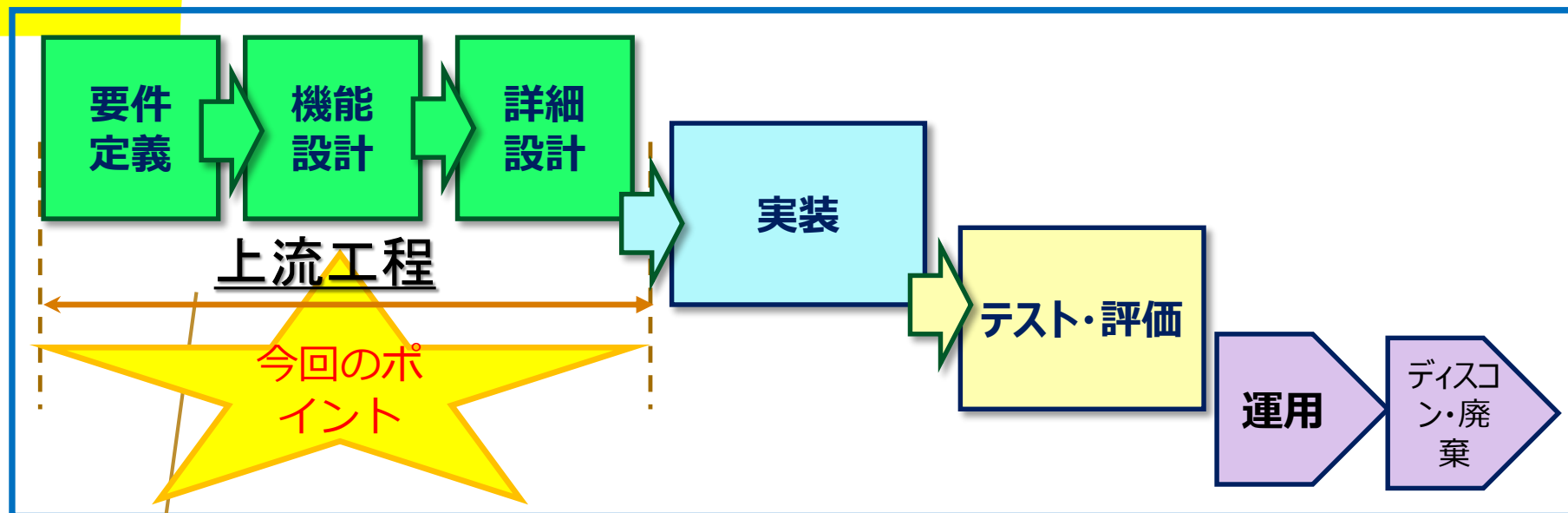
通信経路の脆弱性の
「深刻度」を色と大きさで
「件数」を数値で表現



[対策後]



2017年8期セキュリティグループまとめ



脅威分析を実施しましょう

活用するツール

- ① DFD図
- ② Microsoft Threat Modeling Tool 2016
- ③ リスクマネジメント、リスクマネジメントチェックシート
- ④ CVSS V3

QAはしっかり上流工程のセキュリティ品質の作り込みを設計開発と確認しましょう

参考情報・参照

- MICROSOFT SECURITY DEVELOPMENT LIFECYCLE TOOLS

<https://www.microsoft.com/en-us/SDL/adopt/tools.aspx>

- Microsoft SDL の簡単な実装

<https://www.microsoft.com/ja-jp/download/details.aspx?id=12379>

- NRIセキュアテクノロジーズ サイバーセキュリティ：傾向分析レポート2015

<https://www.nri-secure.co.jp/security/report/2015/cstar.html>

- 経済産業省：リスクアセスメントのハンドブック

http://www.meti.go.jp/product_safety/recall/risk_assessment.html

- 情報処理推進機構（IPA）：共通脆弱性評価システムCVSS v3概説

<https://www.ipa.go.jp/security/vuln/CVSSv3.html>

- ソフトウェア品質保証部長の会 第7期 成果発表会

<http://www.juse.or.jp/sqip/community/bucyo/7/index.html>

- 経済産業省 医療機器等の開発・実用化促進のためのガイドライン策定事業

http://www.meti.go.jp/policy/mono_info_service/healthcare/report_iryoku_fukushi.html

- 一般社団法人 重要生活機器連携セキュリティ協議会

CCDS製品分野別セキュリティガイドライン_車載器編_Ver2.0

CCDS製品分野別セキュリティガイドライン_IoT-GW編_Ver2.0

https://www.ccds.or.jp/public_document/index.html

End of Slide

ご清聴ありがとうございました