セキュリティ品質評価技術
～ゾーン分析による品質予測～

森 拓海[1,*]　小寺 健太[1]

概要：サイバー攻撃のリスクに対応するために法令等でセキュリティ分析が義務化されるが，セキュリティ品質を対外的に説明することは難しい．著者らは，製品開発におけるセキュリティプロセスとセキュリティ対策機能に対し，網羅度の観点で評価する仕組みを開発した．この評価方法は，評価時点での評価にとどまるため，開発の手戻りが大きくなる可能性がある．そこで，ソフトウェア開発における品質予測を行うゾーン分析に着目し，セキュリティ評価に拡張した方法を提案する．
まず，MITRE ATT&CK 等の攻撃ナレッジベースを参考に，x 軸に「セキュリティ対策密度」，y 軸に「緩和されたセキュリティ脅威の密度」を定義する．それぞれの軸の上限・下限の範囲から下限同士と上限同士の交点を結ぶ直線を引くことで複数の区画を生成し，それぞれの区画に品質の見解を割り当ててゾーンモデルを生成する．次に，セキュリティ品質評価対象のセキュリティ脅威および対策情報からゾーンモデルに評価点をプロットし，プロットされた点が属する区画に割り当てられた品質見解をセキュリティ品質の評価とする．この評価を開発途中の段階で複数回行うことで，脅威に対するセキュリティ対策の品質の予測を行うことができる．

キーワード：セキュリティ品質，ソフトウェア，IEC62443，ゾーン分析

The Security Quality Evaluation Method
~ Quality Estimation by Zone Analysis ~

Takumi Mori[1,*]　Kenta Kodera[1]

Abstract: Although security analysis is required by some security laws and regulations for mitigation to the risk of cyberattacks, it is difficult to explain security quality. We developed a mechanism to evaluate security processes and security functions coverage in product development. This evaluation method is limited to evaluate the condition of the target system at the time of evaluation, which may cause some reworks in development. Therefore, we focus on zone analysis to estimate software quality and propose a method that is extended to security evaluation.
At first, define "Density of Security mitigations" on the *x*-axis and "Density of mitigated security threats" on the *y*-axis by referring to attack knowledge bases such as MITRE ATT&CK. Next, generate multiple sections by drawing a straight line connecting the intersection of the lower and upper points of each axis, and generate a zone model by setting a quality view to each section. Finally, plot the evaluation points on the zone model by the security threat and mitigations of the target product, and decide the quality view from the section belonging to plotted point. The target product's quality of mitigations against security threats can be estimated by using the proposal method multiple times in the middle of development.

Keywords: Security Quality, Software, IEC62443, Zone Analysis

1. はじめに

様々な製品の IoT 化が進み，サイバー攻撃に対するセキュリティ対策を製品に具備することは必須となっている．欧州サイバーレジリエンス法などのセキュリティ関連の法令や，IEC62443[1]等のセキュリティ関連規格では，セキュリティ分析[2]を実施したうえで，必要なセキュリティ機能を製品に搭載することが求められる．

セキュリティ分析は，想定される脅威の特定と対策手法の検討を実施し，製品設計に反映させる活動である．しかしながら，検討したセキュリティ対策の評価は，専門家による属人的で定性的なものとなりやすい．そのため，法令や規格対応の第三者評価を受ける際のセキュリティ品質の説明には，多くの専門的なスキルと時間を要する．

また，特にソフトウェアを含む製品は，アジャイル手法で開発することが多くなっており，開発対象製品の具備する機能が次々に変化していく．そのため，セキュリティ品質の評価を都度行う必要があるが，セキュリティ分析を繰り返し実施するのは非常にコストが大きい．

そこで本研究では，ソフトウェア開発における「ゾーン分析」をセキュリティの概念に適用することで，セキュリティ品質を予測する手法を開発する．

まず，分析対象システムのシステム構成要素に対し，x 軸をシステム構成要素数で正規化した対策数，y 軸をシステム構成要素数で正規化した緩和された脅威数，とした 2 次元のゾーンモデルを定義する．次に，作成したゾーンモデ

1 三菱電機株式会社情報技術総合研究所
Mitsubishi Electric Corporation, Information Technology R & D Center.

* Mori.Takumi@db.MitsubishiElectric.co.jp

ルに対して，分析対象のシステム構成要素に対する想定脅威とその対策が紐づいたセキュリティ分析結果の情報から，ゾーンモデル上での座標を算出する．最後に，その座標が位置するゾーンに割り当てられた品質見解を，現時点でのセキュリティ品質とする．

評価時点でのゾーンから，より好ましい品質見解を持つゾーンにするために，追加のセキュリティ対策をどのように実施すれば効果的かを知ることができ，コストの大きいセキュリティ分析の実施頻度を減らすことができる．

また，評価対象に適用された緩和策全体の効果を予測するミクロ評価と，追加で適用した緩和策によって分析対象に残存する脅威を予測するマクロ評価について，いくつかの緩和策パターンで評価し，ゾーン分析のパラメータ調整によって，適切な品質予測が可能であることを確認した．

2. 関連研究

ソフトウェアの品質予測のモデルとしてゾーンモデルがある[3]．ゾーンモデルは，複数の測定量に対するそれぞれの組からなる空間をゾーンに分類するモデルである．与えられたテーマをある特徴に着目した視点によってゾーンに分割し，ゾーンに基づいた評価を行うことをゾーン分析と呼ぶ．ソフトウェアテストにおける欠陥の残存を予測するために，x 軸にテスト密度，y 軸に欠陥密度を取ったゾーン分析が一般的である．

一方で，セキュリティの観点で製品の品質を評価する手法として，ISO/IEC 15408 に定められた Common Criteria（CC）がある[4]．Mellado らは，CC をソフトウェア開発に活用するプロセスを提案し[5]，また Houmb らは要件エディターである HeRA[6]とセキュリティ関連情報のトレースを行う UML 拡張である UMLSec[7]を組み合わせた SeqReq と呼ばれる手法を提案している[8]．しかしながら，CC は，認証スキームが複雑で高度な専門知識を必要とする評価成果物が求められ，後述するセキュリティ保証のレベルが高いほど時間がかかる．そのため，基本的には単一のコンポーネントで構成される製品を対象としており，複数のコンポーネントを持つシステム製品に適用するには課題がある[9]．

さらに，システムのセキュリティ要件を活用した品質評価手法として，セキュリティ保証に関する研究がある．セキュリティ保証とは，NIST SP 800-39 においてセキュリティの機能が効果的であると確信できる根拠であると定義される[10]．Shukla らは，セキュリティ保証を対象として系統的文献レビューを行っており[9]，評価のフレームワーク開発や，定量的評価のための手法，IoT デバイスやクラウドなどの環境ごとの評価手法など様々な研究が行われている[11][12][13][14][15]．

近年主流となっているアジャイル型のソフトウェア開発プロセスは，短期間で設計から実装とデプロイを繰り返し行い，ユーザーからのフィードバックを得て適応的に価値を提供する開発手法である[16]．アジャイル開発におけるセキュリティの側面は重要であり，これまで多くの研究がなされてきた[17][18][19]．しかし近年の体系的文献レビューにおいてもいくつかの課題が挙げられている[20]．例えばセキュリティ要件を考慮することでアジャイル開発の敏捷性が損なわれるという課題があり[21][22][23][24]，セキュリティ保証のようにセキュリティ品質を評価するプロセスとアジャイル開発の間には依然としてギャップがある．

そこで我々は，セキュリティ品質の評価予測を行うゾーンモデルを作成し，評価対象の製品に対する「適用したセキュリティ対策(緩和策)数」と「緩和された脅威数」の情報を用いて素早く品質予測を行う方式を提案する．

3. 提案方式

サイバー攻撃を受ける可能性のある製品が具備すべきセキュリティ機能が，想定されるセキュリティリスクに対して十分であるかを評価することを目的に，セキュリティ品質を予測するゾーンモデルを作成し，ゾーン分析を行う．

3.1 定義

提案方式の説明を行うための定義を示す．

En	：分析対象のシステム構成要素数
Tn	：想定脅威数
Mn	：適用した緩和策(セキュリティ対策)数
Gn	：緩和された脅威数($Gn \leqq Tn$)
$Mmin$	：セキュリティ対策(緩和策)数の下限
$Mmax$	：セキュリティ対策(緩和策)数の上限
$Gmin$	：緩和された脅威数の下限
$Gmax$	：緩和された脅威数の上限

3.2 提案方式

提案方式の詳細な動作を説明する．本方式は，ゾーンモデルの作成と，モデルを使ったゾーン評価の 2 つからなる．

3.2.1 ゾーンモデルの作成

ゾーンモデルで分析を行う対象は図 1 のように，分析対象に対し，システム構成要素ごとに想定される脅威と緩和策が紐づいた情報とする．

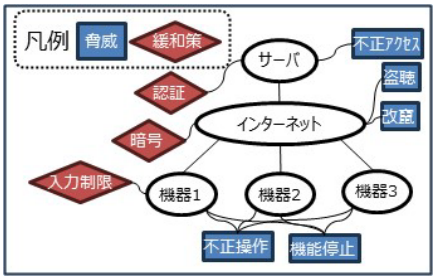

図 1 分析対象の例

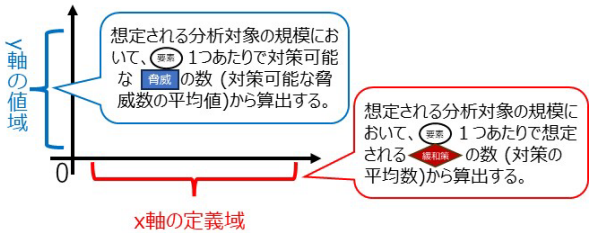

図 2 ゾーンモデルの 2 軸の定義イメージ

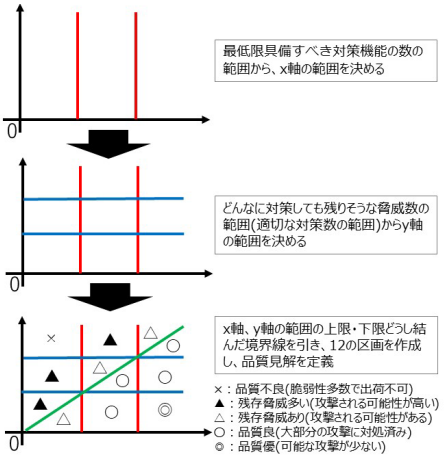

図 3 ゾーンモデルの生成手順

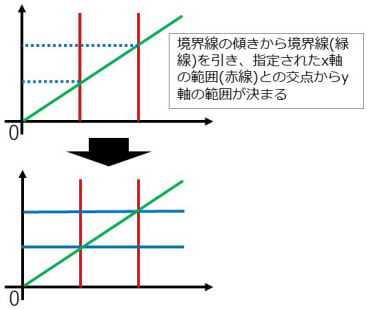

図 4 その他のゾーン生成手順

ゾーンモデルは *x* 軸と *y* 軸の 2 軸からな図 2 のような 2 次元上に作成する．ゾーンモデルの大まかな生成手順は図 3 に示した．まず，*x* 軸はシステム構成要素 *En* に対して適用可能な緩和策数とする．*y* 軸は，緩和策により対策可能な脅威数とする．脅威や緩和策は，MITRE ATT&CK 等の攻撃ナレッジベースを参照し，定義するものとする．

次に，*x* 軸と *y* 軸の下限・上限を決める．*x* 軸の範囲(*Mmin*～*Mmax*)は，例えば，システム構成要素に対して適用可能な緩和策(の種類)の総数から，分析対象が最低限具備すべき緩和策から，その範囲を算出する．*y* 軸の範囲(*Gmin*～*Gmax*)は，例えば，対策が非常に困難で，どんなに対策しても残りそうな脅威の数の範囲から定める．

さらに，*x* 軸，*y* 軸の範囲の下限同士と上限同士を結んだ直線を引く．この直線は (*Mmin*, *Gmin*)，(*Mmax*, *Gmax*) および原点を通る．傾きが(*Gmax* - *Gmin*)/(*Mmax* - *Mmin*)となるため，次の式(1)のように表現できる．

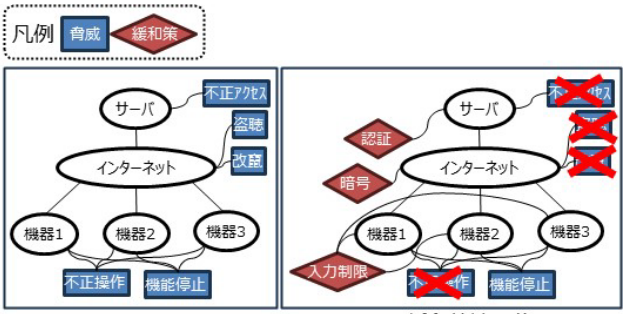

図 5 緩和策適用後の分析対象

$$y = \frac{(Gmax - Gmin)}{(Mmax - Mmin)}x \quad (1)$$

この直線は原点および(*Mmin*, *Gmin*), (*Mmax*,*Gmax*)を通るため，*Mmin*，*Mmax* を固定した場合は *Gmin*，*Gmax* の範囲は限られる．そのため，*Mmin*, *Mmax* または，*Gmin*, *Gmax* のいずれかと，直線の傾きを与えるのが適切である(図 4)．直線の傾きは，例えば「1 つの緩和策で期待される脅威の減少数は 2 である」とすれば，傾きは 2 である．

最後に，*x* 軸，*y* 軸の下限・上限および直線からなる全 12 の区画について，品質見解を割り当てる．この 12 区画と品質見解を持つ 2 軸のモデルをゾーンモデルとする．

3.2.2 ゾーン評価

分析対象のシステムに対して，緩和策を適用後(図 5)に，適用された緩和策の品質をゾーンモデルによって評価する．

分析対象のシステム構成要素に対して，緩和策 *Mn* と緩和された脅威 *Gn* から，ゾーンモデルに評価点をプロットする．*Tn* は図 5 における脅威の総数，*Mn* は緩和策の総数，*Gn* は，緩和策によって成立しなくなった脅威の数(図中"×"のついた脅威)である．作成したゾーンモデルに対してプロットする座標 *P*(*x*,*y*)は，次の式(2)によって求める．

$$P(x, y) = \left(\frac{Mn}{En}, \frac{Gn}{En}\right) \quad (2)$$

ゾーンモデル上の *P*(*x*,*y*)が属する区画に割り当てられた品質見解を，セキュリティ品質の評価とする．

4. 実装・評価

提案方式は，CI/CD パイプラインに組み込み，自動で行われることが望ましい．そこで，Web API によって提案方式を動作させる実装を行った．ゾーンモデルの可視化には，matplotlib ライブラリを利用した．実装したゾーン評価システムの画面を図 6 に示した．*Mmin*, *Mmax*, *Gmin*, *Gmax* および各ゾーンの品質見解は設定ファイルに記述しておく．評価対象の *En*,*Mn*,*Gn* をそれぞれ入力すると，ゾーン分析結果が表示される．この実装環境により提案方式の評価を実施した．

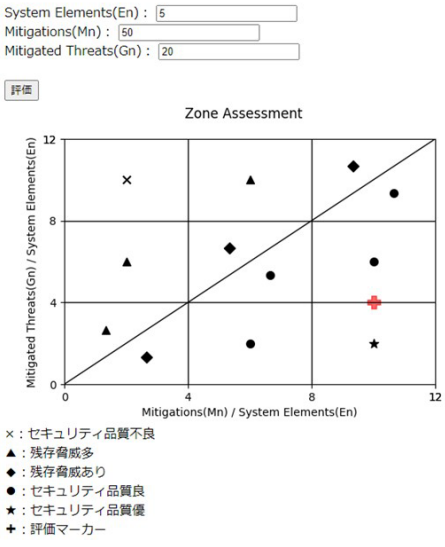

図 6 実装したゾーン評価システム

4.1 評価

提案方式が予測する品質評価値に対し，MITRE ATT&CK Navigator(https://mitre-attack.github.io/attack-navigator/) を用いて，単純な条件(*En*=1)で妥当性を確認する．

4.1.1 評価パラメータ

想定するシステム構成要素の脅威パラメータは表 1 に示した．ICS(Industrial Control System)における機器とし，ICS を標的とした最初のマルウェアである Stuxnet を想定する．このパラメータでは，ATT&CK における攻撃 technique は 26 種類(*Tn*=26)が選択される(図 7).

表 2 に適用する緩和策を示した．今回は 3 つのパターンを用意し，適用する緩和策を 1 つずつ増加させている．

ゾーン評価は，次の 2 つの目的により評価方法が異なる．

① 適用した緩和策の組み合わせを評価(ミクロ評価)

② 追加した緩和策から残存脅威を評価(マクロ評価)

①の場合，適用した緩和策に対してヒットした脅威が多いほど品質が良いと判断する．緩和策は見直すことができるため，特定の脅威に対する重複した緩和策を見直し，より幅広い脅威に対処する緩和策設計を促すものとする．この場合，*Gn* は適用されたすべての緩和策によって対処された脅威をカウントする．①の評価に用いるゾーン評価のパラメータは表 3 に示した．最低 1 つの緩和策を適用する前提で，1 つの緩和策で平均 3.5 の脅威が緩和されるものとしてすべての適用済み緩和策の品質を予測する．このパラメータによるゾーンの品質見解は図 8 の通りである．

②の場合，あらかじめ脅威への緩和策は実施されているという前提条件を置き，追加した緩和策によって新たに対処された脅威を *Gn* としてカウントする．この評価では，評価対象全体における残存脅威を予測する．②の評価に用いるゾーン評価のパラメータは表 3 に示している．

表 1 想定脅威パラメータ

項目	設定値
ATT&CK Navigator のバージョン	v.5.0.1
ATT&CK のバージョン	v15
ドメイン	ICS (Industrial Control System)
想定プラットフォーム	None※
攻撃者の能力	Software：Stuxnet

※ATT&CK v15 の ICS ドメインにはプラットフォーム情報はない

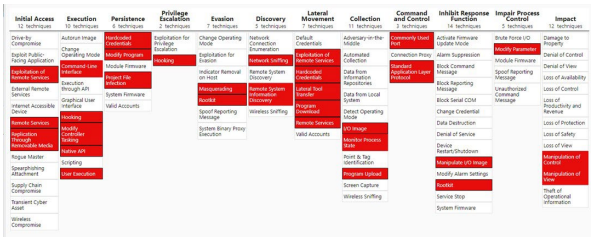

図 7 評価対象で実施可能な technique(26 種類)

表 2 緩和策パターン

緩和策パターン	適用する緩和策
1	Access Management
2	Access Management, AntiVirus/Antimalware
3	Access Management, AntiVirus/Antimalware, Audit
4	Access Management, AntiVirus/Antimalware, Audit, Data Backup
5	Access Management, AntiVirus/Antimalware, Audit, Data Backup, Network Segmentation

表 3 ゾーン評価のパラメータ

パラメータ	ミクロ評価	マクロ評価
Mmin	1	2
Mmax	4	4
Gmin	3.5	4
Gmax	14	8
直線の傾き	3.5	2

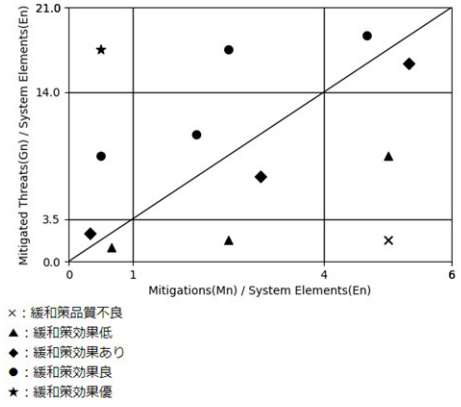

図 8 各ゾーンの品質見解①(ミクロ評価)

今回は Stuxnet の *Tn*=26 の脅威に対する残存脅威を予測するものとする．最低でもシステム構成要素あたり 2 つの緩和策が適用されていることとし，1 つの緩和策に対して発見される脅威が 2 つ以下であることを求めるようにしている．このゾーンの品質見解は図 9 の通りである．

4.1.2 評価結果

各緩和策パターンについて *Gn* を求めるには，ATT&CK Navigator のレイヤー演算機能を用いた．図 7 の Stuxnet の脅威レイヤーに対し，緩和策パターン 1 であれば図 10 のような緩和策レイヤーを作成する．今回の評価では脅威や緩和策に重さは設けず，脅威スコア=100，緩和策スコア=100 として，脅威スコアから緩和策スコアを減算する．図 11 のように，スコアが 100 の場合は赤色，スコアが 0 の場合は緑色で示した．同様に，緩和策パターン 2～5 についても図 12～図 15 に示した．

● ミクロ評価

まず，適用したすべての緩和策の品質を評価するミクロ評価の結果を示す．ATT&CK Navigator により緩和された脅威を数え上げ a, *Gn* の値とする．緩和策パターンごとの *Mn*, *Gn* を表 4 に示した．また，緩和策パターンごとのゾーン分析結果を図 16～図 20 に示した．

まず，緩和策パターン 1 では「緩和策効果良」という判定となった(図 16)．実際に，図 11 の緑部分のように 1 つの対策で 4 つの脅威(重複無し)に対策可能で効果が高い．

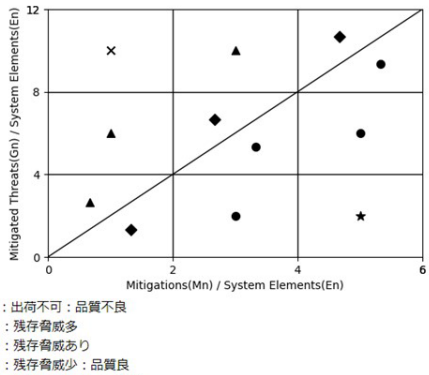

図 9 各ゾーンの品質見解②(マクロ評価)

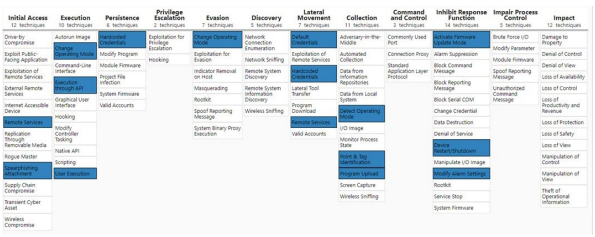

図 10 緩和策パターン 1

次に緩和策パターン 2 のゾーン分析結果(図 17)では，「緩和策効果あり」という判定になった．緩和策パターン 1 よりも脅威の低減効果は低く図 12 に示したように緩和策パターン 1(図 11)とほとんど変わらない．つまり，緩和策パターン 2 で適用した緩和策の集合は，緩和策パターン 1 の集合よりも品質が低いといえる．

緩和策パターン 3 のゾーン分析結果(図 18)では，「緩和策効果良」の評価に戻る．このパターンの組み合わせは，緩和策パターン 1 と同様に脅威低減の効果が高いといえる．

同様に図 19 の緩和策パターン 4 では，品質見解は「緩和策効果あり～緩和策効果低」，図 20 の緩和策パターン 5 では，「緩和策効果良」となる．

図 11 緩和策パターン 1 で緩和された脅威

図 12 緩和策パターン 2 の残存脅威

図 13 緩和策パターン 3 の残存脅威

図 14 緩和策パターン 4 の残存脅威

図 15 緩和策パターン 5 の残存脅威

表 4 評価結果(ミクロ評価)

緩和策パターン	*Mn*	*Gn*
1	1	4
2	2	5
3	3	11
4	4	13
5	5	18

a 脅威は tactics にまたがって重複するものもあることに注意

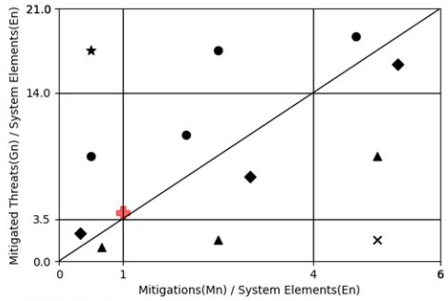

図 16 評価パターン 1 のゾーン分析結果(ミクロ評価)

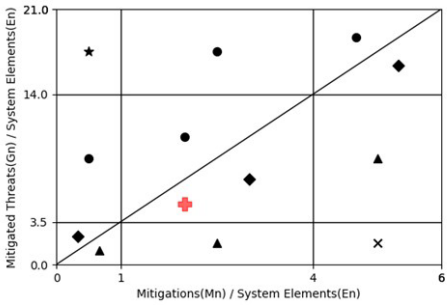

図 17 評価パターン 2 のゾーン分析結果(ミクロ評価)

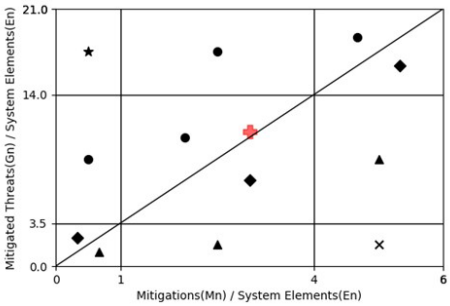

図 18 評価パターン 3 のゾーン分析結果(ミクロ評価)

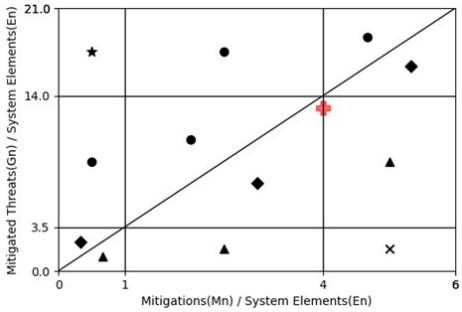

図 19 評価パターン 4 のゾーン分析結果(ミクロ評価)

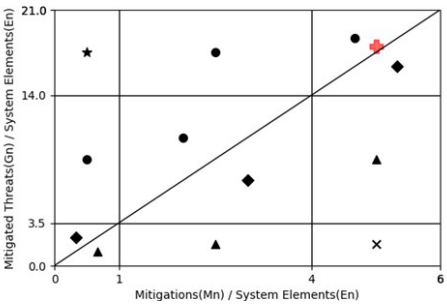

図 20 評価パターン 5 のゾーン分析結果(ミクロ評価)

表 5 評価結果(マクロ評価)

緩和策パターン	*Mn*	*Gn*	追加された緩和策
1	1	4	Access Management
2	2	1	AntiVirus/Antimalware
3	3	6	Audit
4	4	2	Data Backup
5	5	5	Network Segmentation

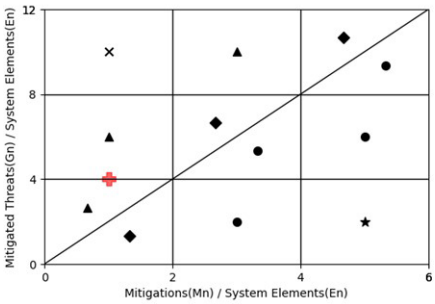

図 21 評価パターン 1 のゾーン分析結果(マクロ評価)

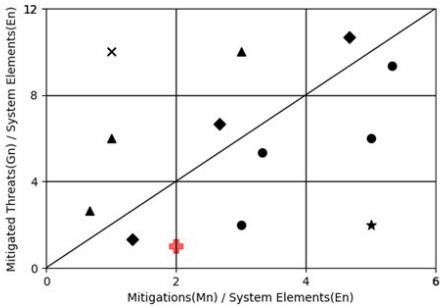

図 22 評価パターン 2 のゾーン分析結果(マクロ評価)

● マクロ評価

追加した緩和策の品質を評価するマクロ評価の結果を示す．*Gn* の値は，緩和策パターンごとの差分であり，適用された緩和策によって対処された脅威を数え上げたものとする．緩和策パターンごとの *Mn*，*Gn* および追加された緩和策を表 5 に，緩和策パターンごとのゾーン分析結果を図 21～図 25 に示した．

まず，緩和策パターン 1 では，「残存脅威多」という判定となった(図 21)．実際に，図 11 の赤色部分のように残存脅威が多いことがわかる．

次に緩和策パターン 2 のゾーン分析結果(図 22)では，「残存脅威あり～残存脅威少：品質良」という判定になったが，図 12 のように残存脅威はまだ多いことがわかる．

緩和策パターン 3 のゾーン分析結果(図 23)を見ると，緩和策パターン 2 と同じく「残存脅威あり～残存脅威少：品質良」の評価である．しかし，図 13 のように残存脅威が 15/26 のため，半分以上の脅威が残っている．

緩和策パターン 4 になると，残存脅威は図 14 に示したように 13/26 となり，半分の脅威に対応する．評価は，「残

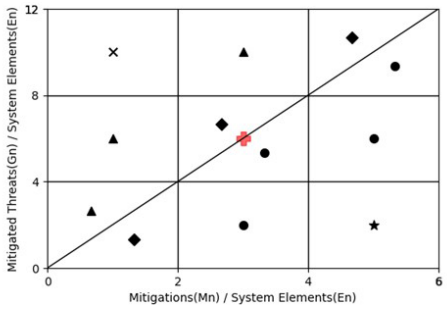

図 23 評価パターン 3 のゾーン分析結果(マクロ評価)

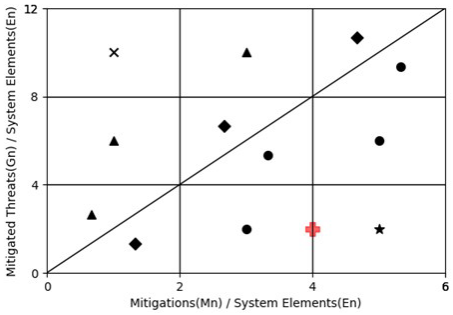

図 24 評価パターン 4 のゾーン分析結果(マクロ評価)

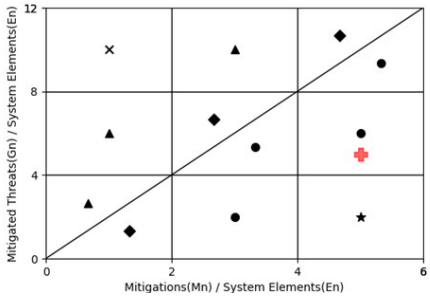

図 25 評価パターン 5 のゾーン分析結果(マクロ評価)

存脅威少:品質良～残存脅威僅少:品質優」となる(図 24).

最後に，緩和策パターン 5 では，図 15 のように 8/26 脅威となり全体の約 30%が残存脅威の状態で，図 25 に示した評価では「残存脅威少：品質良」となる．

5. 考察

評価結果をもとにゾーン評価のためのパラメータの決め方について考察する．ソフトウェアの品質評価としてのゾーン分析では，*x* 軸，*y* 軸の範囲は経験・実績に基づいて設定される．しかしながら，本方式はそのように決めることができないため，著者らがこれまでに実施してきたセキュリティ分析の経験・ノウハウから主観的に決定した．本評価を通じた *x* 軸, *y* 軸の上限・下限に対する見解を述べる．

まず，ミクロ評価については，緩和策パターンが 1~5 の変化で妥当な評価が得られているように見える．評価した Stuxnet の脅威に対して選択した緩和策の組み合わせでは，うまく評価できていると言える．

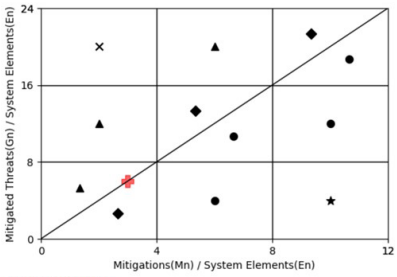

図 26 緩和策パターン 3 の再評価(マクロ評価)

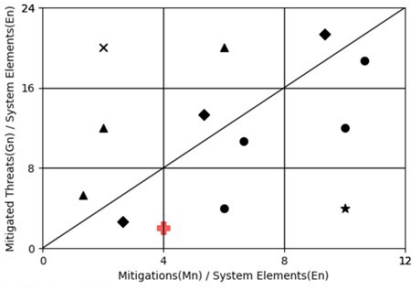

図 27 緩和策パターン 4 の再評価(マクロ評価)

一方，マクロ評価は，緩和策パターン 3,4 において，実際の残存脅威数が多いにも関わらず，評価予測値では品質が良いと予測され，乖離があるように見える．

通常のソフトウェアの品質評価では，ある程度不具合対策がされたうえでの残存不具合の評価を行う．今回のマクロ評価では，*Mmin*=2 としたことが乖離の原因と考えられる．よほど効果的な緩和策を選択しない限り，*Mmin*=2 では適用する緩和策が少なすぎると考えられる．適用する緩和策が少なすぎる場合，ランダムに緩和策を適用させると残存脅威へのヒット率に大きく影響する．そのため，少なくとも半分程度の脅威に緩和策が適用された状態を想定した *Mmin*=4 の設定が必要と考えられる．*Mmin*=4，*Mmax*=8 とした場合の緩和策パターン 3,4 の評価結果は，図 26, 図 27 のようになる．緩和策パターン 3 が「残存脅威多い～残存脅威あり」，緩和策パターン 4 が「残存脅威あり～残存脅威少：品質良」となり，乖離が解消する(その他の緩和策パターンの品質見解は同じ).

このように，想定する脅威の集合によって，取り得る緩和策の集合と，どの程度まで残存脅威を下げる必要があるかを考慮し，ゾーン分析のパラメータを調整することで，正確な評価が可能になる．例えば，IEC62443 のセキュリティ要件(SR,CR)およびセキュリティレベル(SL)によって目標を定め，分析対象の特性に応じてパラメータを決定する方法がある．

今回は，単一のシステム構成要素(*En*=1)に対して評価を実施したが，システム全体の緩和策や残存脅威を評価する際に，各システム構成要素が評価として分割可能である(緩和策が独立している)ならば，脅威と緩和策の評価をシステム構成要素で正規化するアプローチは妥当である．

しかしながら，現実的には脅威ごとにリスク大きさに差があり，また，緩和策の効果範囲がシステム構成要素をまたがることも多い．このような場合，例えば，脅威のカウントは，分析対象における脅威に対するリスクの大きさや，攻撃シナリオにおける攻撃の進行度によって重さを決める方法がある．また，緩和策に関しても UTM(Unified Threat Management)，EDR(Endpoint Detection and Response)といった高機能で多くの脅威に対して統合的に対応するものに関しては，重さを大きく設定すると正確なゾーン評価が実施できると考えられる．

6. おわりに

ソフトウェアを含む製品開発における，セキュリティ品質を評価するために，x 軸をシステム構成要素数で正規化した対策数，y 軸をシステム構成要素数で正規化した緩和された脅威数，とした 2 次元のゾーンモデルを用いた品質予測の方法を開発した．

このゾーン分析により，製品に適用する緩和策の品質と，製品に残存する脅威を予測できることを実装・評価により確認した．

より正確なセキュリティ品質予測のためには，セキュリティ分析の実績値や，セキュリティガイドライン等による脅威と緩和策の関係性をゾーン分析パラメータに適用させることが有効である．

参考文献

[1] ISA. The 62443 series of standards: Industrial automation and control systems security, 1–4, 2018.

[2] IPA. 制御システムのセキュリティリスク分析ガイド第 2 版. https://www.ipa.go.jp/security/controlsystem/riskanalysis.html (参照:2023-08-04).

[3] IPA:定量的品質予測のススメ，オーム社, 2008.

[4] ISO/IEC 15408 Standard: “Information Technology -- Security Techniques -- Evaluation Criteria for IT Security --”, 1999.

[5] Mellado, D., Fernandez-Medina, E., Piattini, M.:A common criteria based security requirements engineering process for the development of secure information systems, Computer standards & interfaces, 29.2: 244-253, 2007.

[6] Knauss, E., Lubke, D., Meyer, S.: Feedback-Driven Requirements Engineering: The Heuristic Requirements Assistant, Proceedings of the 31st International Conference on Software Engineering (ICSE 2009), Vancouver, Canada, pp. 587-590, 2009.

[7] Jürjens, J.: Secure systems development with UML, Springer Science & Business Media, 2005.

[8] Houmb, S.H., Islam, S., Knauss, E., Jurjens, J., Schneider, K.: Eliciting security requirements and tracing them to design: An integration of Common Criteria, heuristics, and UMLsec. Requirements Engineering 15(1), pp. 63-93, 2010.

[9] Sshukura, A., et al.: System security assurance: A systematic literature review, Computer Science Review, 45, 100496, 2022.

[10] NIST: NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View”, 2011.

[11] Kim H.: A framework for security assurance in component based development, International Conference on Computational Science and Its Applications, Springer, pp. 587-596, 2004.

[12] Vivas, J. L., Agudo, I., and Lopez, J. :A methodology for security assurance-driven system development, Requirements Engineering, vol. 16, no. 1, Springer, pp. 55-73, 2011..

[13] Katt, B., Prasher, N.: Quantitative security assurance metrics: REST API case studies, Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings, , pp. 1-7, 2018.

[14] Ardagna C.A., Damiani E., Schutte J., Stephanow P. :A case for IoT security assurance, Internet of Everything, Springer, pp. 175-192, 2018.

[15] Shukla, A., Katt, B. & Yamin, M.M. : A quantitative framework for security assurance evaluation and selection of cloud services: a case study, Int. J. Inf. Secur. 22, 1621-1650, 2023.

[16] Larman, C., Basili, V.R. :Iterative and Incremental Development. A Brief History, IEEE, Computer, 2003.

[17] Beznosov, K. and Kruchten, P. :Towards agile security assurance, Proceedings of the 2004 workshop on New security paradigms, 2004.

[18] Keramati, H., Seyed-Hassan Mirian-Hosseinabadi.: Integrating software development security activities with agile methodologies, 2008 IEEE/ACS International Conference on Computer Systems and Applications. IEEE, 2008.

[19] Bartsch, S.:Practitioners' perspectives on security in agile development, 2011 Sixth International Conference on Availability, Reliability and Security. IEEE, 2011.

[20] Munir, A., Assiri, M., Alam, S. N., Khan, M., Butt, W. H., and Humayun, M.: A Systematic Review of Approaches for Reviewing Security-Related Aspects in Agile Requirements Specification of Web Applications, 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), pp. 701-707. IEEE, 2023.

[21] Alsaqaf, W., Daneva, M. and Wieringa, R.: Quality requirements in large-scale distributed agile projects-a systematic literature review, Requirements Engineering: Foundation for Software Quality: 23rd International Working Conference, REFSQ 2017, Essen, Germany, February 27-March 2, 2017, Proceedings 23. Springer International Publishing, 2017.

[22] Daneva, M., Wang, C.: Security requirements engineering in the agile era: How does it work in practice? , 2018 IEEE 1st International Workshop on Quality Requirements in Agile Projects (QuaRAP), pp. 10-13, August 2018.

[23] Terpstra, E., Daneva, M., and Wang, C. :Agile practitioners’ understanding of security requirements: insights from a grounded theory analysis, 2017 IEEE 25th international requirements engineering conference workshops (REW). IEEE, 2017.

[24] Cruzes, D. S., et al. :How is security testing done in agile teams? A cross-case analysis of four software teams, Agile Processes in Software Engineering and Extreme Programming: 18th International Conference, XP 2017, Cologne, Germany, May 22-26, 2017, Proceedings 18. Springer International Publishing, 2017.