Copyright© 2018 The Institute of Electronics,
Information and Communication Engineers

SCIS 2018 2018 Symposium on
Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics,
Information and Communication Engineers

システムに対する脅威分析におけるコスト及び属人性低減に向けた手法の提案

Threat Analysis Method: Reducing costs and variability in results

中野 学[1] 堀部 千壽[1] 小林 鉄平[2] 松木 隆宏[2]
Manabu Nakano Yukihisa Horibe Teppei Kobayashi Takahiro Matsuki

あらまし 脅威分析とは，システムやデバイスにおいてセキュリティ事故や故障の原因となる脅威の有無を分析し，必要な対策を明確にする作業である．要件定義や設計の段階で脅威分析を行う事で，その後のプロセスでは修正が困難な設計上の脆弱性や問題のある仕様を発見，除去する事ができる．しかしながら，一般に脅威分析には多くの時間を要する．加えて，分析対象とするシステムの詳細知識，及び専門的なセキュリティ知識が要求されるため，開発プロセスの一部として普及していないのが現状である．昨今，様々な技術を用いたシステムやサービスが開発されているが，それらはサイバー攻撃や障害などの脅威への対応が求められている．安全なシステムを開発する上で脅威分析の実施は必須であるが，規模や複雑さが増すにつれ，過不足なくシステム全体を分析する事は困難となる．そこで本論文では，過去の分析結果の傾向から，システム中の分析対象とする箇所に優先度を設定する事で，効率的に脅威分析を実施する手法を提案する．さらに，システムのユースケースや機能から体系的に DFD を作成する手法を紹介した後，その成果に対して分析優先度を設定する方法を考察する．

キーワード 脅威分析，システム設計開発，コスト低減，フォルトツリー解析

1. はじめに

1.1 研究背景

サイバー攻撃を受けるリスクは, ネットワークの高度化, サイバー攻撃のビジネス化などに伴い, 飛躍的に増大した. また IoT の隆盛やシステムの複雑化に伴い, システムに存在する脅威は以前にも増してきている.

そのためネットワークに接続するあらゆるシステムにおいて，設計段階からセキュリティ対策を考慮する事で, システムに存在する脅威を事前に見つけ出す必要がある.

システムに存在する脅威を見つけ出す手段を, 脅威分析と言う. 現在存在する脅威分析の手法は比較的古くから存在するものが多く, システムが扱う資産や構成要素が多様化，複雑化した現代の事情にあわせた改良の余地がある. また，システムの複雑化に伴い，システムを調査するコストも飛躍的に増している．これらのことより，システム開発において脅威分析は必須であるにも関わらず, 導入が困難であるという問題を抱えている.

今後ますますシステムの複雑化, 及び攻撃手段の高度化は進むと想定され, あらゆるシステム開発に対して容易に導入できる脅威分析手法が求められている.

1.2 研究目的

本研究の目的は, 従来手法と比較してコストの少ない脅威分析手法を開発，提案する事である.

まず，既存の手法を参考に，2 つの視点から考案した脅威分析手法を報告する．これらの利点と課題点をまとめ, 効率的に脅威分析を行う際に必要な視点を明らかにする. これより明らかになった視点から 2 つの脅威分析手法を統合した脅威分析手法を提案する.

1.3 本論文の構成

本論文は，本章を含めて 5 章から構成される.

第 2 章では，まず従来手法の課題点を指摘する．次に従来手法の課題点を解決するため考案した, システムの評価を行う際の視点が異なる脅威分析手法を 2 つ報告する.

第 3 章では，第 2 章において考案した 2 つの脅威分析手法を統合した脅威分析手法を提案する.

第 4 章では，第 3 章で提案した脅威分析手法をモデルシステムに適用した結果を報告する．この結果より，提案手法の利点，及び解決が必要な課題点について述べる.

第 5 章では，本論文で述べた研究内容を総括し，今後の脅威分析研究の展望を述べる.

[1] パナソニック株式会社 製品セキュリティセンター,
〒571-8506 大阪府門真市大字門真 1006 番地 AIS 社西門真地区 11B 棟, "nakano.manabu@jp.panasonic.com", "horibe.yukihisa@jp.panasonic.com"
[2] 株式会社 FFRI 基礎技術研究室,
〒150-0013 東京都渋谷区恵比寿 1 丁目 18 番 18 号 東急不動産恵比寿ビル 4 階, "tkobayashi@ffri.jp", "matsuki@ffri.jp"

2　従来手法

一般に脅威分析は，システムからの脅威の抽出，及び抽出した脅威の評価の 2 段階に分けられる．そのため，脅威分析は複数の手法を組み合わせて実施される．

本節では，脅威の抽出方法と評価方法のそれぞれについて，既存の手法で用いられることの多い DFD, STRIDE, Attack Tree を挙げ，それらの解説を行うとともに課題点を指摘する．

2.1.1. DFD を用いたシステム構成要素の洗い出し

一般的な用途で用いる DFD(Data Flow Diagram)は，システムを構成するプロセスやデータ，入出力やデータフローなどの要素をエンティティとして記述する．脅威分析で用いる場合は，加えて信頼境界を記述する事で，アクセス権限を含めたシステム全体の構成を明らかにする．ここで信頼境界とは，エンティティがセキュリティ上信頼できるか否かを基準として，図中に記入する境界線である．信頼境界はネットワーク境界部に位置する場合や，物理的境界部に位置する場合が多い．

分析者は設計書や仕様書などの開発資料からシステムを構成するエンティティを抽出し，高度なセキュリティ知識を以って信頼境界を設定し，システムのアーキテクチャを示す図を DFD として作成する．作成した DFD を後述の STRIDE などと組み合わせる事で，システム中に存在する脅威を発見，抽出する．

本手法の課題点は，分析者がシステムとセキュリティの両方に精通している必要がある点である．また，システムの複雑化とともにエンティティ数も増大し，作業量の増大やエンティティの記入漏れなどが生じうる．

2.1.2. STRIDE による脅威の抽出と分類

STRIDE とは，Microsoft 社の Adam Shostack 氏が開発した，脅威の分類を行う手法である [1]．システムを構成する要素に着目し，それぞれの要素に存在する脅威を発見，分類する．

STRIDE とは情報セキュリティにおける脅威のアクロニムであり，”Spoofing”（なりすまし），”Tempering”（改竄），”Repudiation”（否認），”Information Disclosure”（情報漏洩），”Denial of Service”（サービス妨害），”Elevation of Privilege”（権限昇格）の 6 種類を指す．

抽出する際のシステム構成要素に対して着目すべき点について，参考文献 [1]から表 1 に引用する．表中「システム外要素」については，改竄と情報漏洩，サービス妨害及び権限昇格は本質的に生じない．対してユーザーやクライアントへのなりすまし，通信の否認などは生じうるという事を意味する．

本手法の課題点は DFD と同様に，分析者がシステムとセキュリティの両方に精通していなくてはならない点である．脅威の発見漏れや分類の誤りが生じ，脅威分析として満足な結果を得られない可能性があるためである．

2.1.3. Attack Tree による脅威の分析

Attack Tree は，脅威が生じうる原因を分析する手法である [2]．先述の STRIDE などで抽出した脅威について，それぞれが生じる原因を調査し，詳細に解析を行う．

Attack Tree は木構造で表現される図である．木構造の頂点に分析対象の脅威を配置し，生じる原因の粒度ごとに枝を作成し，脅威の発端となる原因を葉で表現する．

本手法の課題点は，脅威の数だけ Attack Tree を作成する必要がある点である．似通った原因により生じる脅威であっても，全く同じでない場合は原因の発見漏れなどを防ぐため，それぞれを個別のものとして扱う必要があるためである．

2.1.1.項から 2.1.3 項において，脅威分析を行う際に組み合わせて利用される，既存の手法について述べた．

これらに存在する課題点に共通するのは，脅威分析の精度が分析者のスキルに依存する点と，分析作業に多くの時間的コストが要求される点である．これらの課題点を解決する事で，開発プロセスに脅威分析を組み込むことができ，セキュリティ対策のコストを低減する事が可能である．

従来は，これらの複数の手法を分析者が組み合わせ，システムに対して脅威分析を実施していた．分析者は情報セキュリティ技術と分析対象のシステムの両方に精通している必要があり，手法によってはシステムに含まれるあらゆる要素を網羅的に分析する必要があった．

次節からは，既存の手法における課題点の解決を目的として考案した，2 種類の脅威分析手法について述べる．

構成要素	S（なりすまし）	T（改竄）	R（否認）	I（情報漏洩）	D（サービス妨害）	E（権限昇格）
システム外要素	○		○			
プロセス	○	○	○	○	○	○
データフロー		○		○	○	
データストア		○	△	○	○	

表 1　STRIDE による，システム構成要素に対する着目箇所

2.2　想定される被害に基づく脅威分析手法

まず我々は，システム中で想定される被害について開発者とセキュリティ担当者が共同で想定し，対象のシステムにおいて生じうる重大な被害についてのみ，脅威分析を実施する手法を考案した．

2.2.1. 考案手法の実施工程

本手法の特徴は，システムの開発者とともに脅威分析を実施する点である．システムの要素を把握している開発者にヒアリングを行う事で，資料からのみでは読み取れない可能性のある脅威を発見する事ができる．

本手法の実施手順は，次の通りである．

1. システム中で生じうる致命的な被害を開発者とともに想定し，被害を受けうる資産を特定する．
2. システムの持つ機能ごとに DFD を作成し，作成した全ての DFD を単一の DFD に転記し，エンティティを統合する．前工程，及び本工程の概念図を，図 1 に示す．ここで，図 1 における DFD を作成する際，システムの例として参考文献 [3]を利用した．
3. 作成した DFD 上のエンティティに，1.で特定した被害を関連付ける．
4. 3.で作成した DFD より Attack Tree を作成し，攻撃手段や経路を想定する．

結果として，システムで生じうる重大な被害のリスト，システムの DFD，重大な被害ごとに作成した Attack Tree が得られる．同じシステムに対して脅威分析を実施する場合，これらは再利用が可能である．

2.2.2. 課題点

本手法では致命的な被害のみを想定するため，それ以外の被害に対する網羅性は担保されない．そのため，システムに生じうる全ての脅威を洗い出す用途には不向きである．

また，Attack Tree の作成時，高度なセキュリティ知識が必要であるため，脅威分析結果が分析者の知識，経験などのスキルに依存する点も課題である．

2.3　資産の重要度に基づく脅威分析手法

次に我々は，システム中に存在する資産の重要度に着目した手法を考案した．資産の重要度，及びその出現頻度に応じて脅威分析を実施する範囲を絞り込む．すなわち，システム内に存在する資産価値を一通り評価する事で，重要な箇所のみを詳細に分析する事を目的としている．

また本手法では，開発者に対してヒアリングを行わず，システムの設計開発資料のみを利用して実施する．

2.3.1. 考案手法の実施工程

本手法の実施手順は，次の通りである．

1. システムの設計開発資料をもとに，Microsoft 社による脅威分析ツールである TMT [4]を用いて，システム全体の DFD を作成する．
2. 1.で作成した DFD より，システムに存在する全ての資産のリストを作成する．システム中で考えられる脅威は，参考文献 [5]を利用した．
3. 2.で作成した資産のリストに対して，全ての資産の重要度を評価する．重要度の評価においては，基準として表 2 を利用する．
4. システム中に存在する全ての資産について，重要度評価結果の平均を求める．この結果から，システム全体の重要度を評価する．
5. システム全体の重要度から脅威分析対象とする資産の基準を決定し，該当する資産を洗い出す．表 2 に，分析対象とする基準を示す．3.で作成した資産の重要度評価結果において，基準を超えている資産のみを脅威分析の対象とする．
6. TMT に脅威分析対象とする資産のリストを入力し，自動分析を行う．その後，分析結果から誤検出を取り除く．

結果として，システムの DFD，システム中に存在する全資産の重要度評価結果，TMT により検出された脅威リストが得られる．ただし，TMT による検出には誤検出が生じる場合があり，分析者による精査が必要である．同じシステムに対して脅威分析を実施する場合，得られた DFD や脅威リストなどは，再利用が可能である．

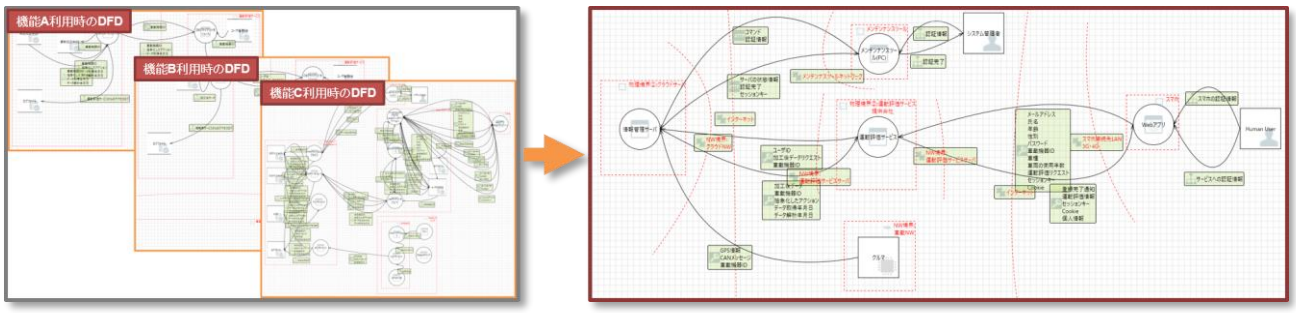

図 1　システムの持つ機能ごとに作成した DFD を単一の DFD に統合，簡略化した結果

2.4　課題点

本手法の課題点は，システムに存在する全ての資産について，重要度を評価する必要がある点が挙げられる．また資産のリストを作成する際，分析者により資産の粒度に差が生じる．同様に資産の評価時においても，分析者により判断の差が生じる．

前節で述べた被害に着目する手法とは異なり，全てのシステム構成要素や扱う資産が明確になっていないと，正確な分析が実施できない点も課題点として挙げられる．

2.5　考案手法の比較

それぞれの手法について，主な利点と課題点を述べる．

2.2.節で述べた手法は，致命的な被害のみに着目して脅威分析を行うため，作業量を低減できる点が利点である．対して，分析者に高度なセキュリティ知識が要求される点が，依然として課題点である．

2.3.節で述べた手法は，システムの重要度に応じて脅威分析の範囲を調節するため，システムの規模に応じて適切な脅威分析を実施できる点が利点である．対して，システムに存在する全ての資産を一通り評価する必要があり，作業量が増大する点が課題点である．

以上より，脅威分析を実施するシステムの範囲を明確にする事で作業量を低減し，分析者のセキュリティ知識への依存を低減することで、脅威分析のコストを低減できる．

システム中に脅威が潜在する箇所を予測する事で，これらの課題の解決を試みる．脅威が潜在する箇所を予測できれば，高度なセキュリティ知識を持たない分析者が脅威分析を実施した場合であっても，原因の発見漏れや分類ミスを低減する事ができる．さらに，予測するために必要な資料を再利用できる形式にする事で，脅威分析全体の作業量を低減する．これらは，2.2.節と 2.3.節で述べた手法を統合する事で，可能であると考えられる．

次章において，本論文の提案手法を詳細に述べる．

3　提案手法
「脅威頻出箇所表を用いた脅威分析手法」

前章では，従来の脅威分析手法で組み合わせて用いられていたいくつかの手法の解説と課題点の指摘を行った後，指摘した課題点を解決するために考案した 2 つの新しい手法について述べた．

本章では 2.4.節で指摘した，分析結果が分析者の能力に依存する点，及び作業量を低減する必要がある点の 2 点を解決するため，前章で報告した 2 つの手法を組み合わせた，新しい脅威分析手法を提案する．

提案手法では，脅威分析作業を 2 つのフェーズに分解し，それぞれのフェーズの担当者を「脅威分析の専門家」，「分析者」に分離する事で，これらの課題を解決する．

1 つめのフェーズでは，「脅威頻出箇所表」を作成する．分析対象とするシステムのアーキテクチャに着目し，脅威が頻出する箇所を予測した表である．

脅威頻出箇所表の特徴は，類似のアーキテクチャを持つシステムであれば，作成した表を再利用できる点である．これはシステムに特有であるエンティティを除き，脅威が頻出する箇所は類似すると考えられるためである．

脅威頻出箇所表の作成には，専門的なセキュリティ知識を要する．そのため，本フェーズは「脅威分析の専門家」が実施する必要がある．

2 つめのフェーズでは，実際の分析対象システムに対して，作成した脅威頻出箇所表を用いて脅威分析を実施する．

TMT 上で分析対象のシステムの DFD を作成し，1 つめのフェーズで作成した脅威頻出箇所表と照らし合わせる事で分析対象とする要素を決定し，分析を行う．

本フェーズでは，分析対象のシステムについての知識が必要となる．そのため「分析者」は，システム設計開発資料を用意する必要がある．

次節より，提案手法の実施工程を 2 節に分けて詳説する．

資産評価	機密性（Confidentiality）の評価基準
5	・利用者の機微な個人情報，あるいは顧客から提示された機密情報 ・大量の個人情報等，機密性が失われた場合に利用者の資産や社会的インフラに重大な影響が発生するもの
4.5	・資産評価4の基準に該当する資産の内，単体機器に含まれているか，サーバーが保持するセキュリティ・金銭に関わるか，サーバーや機器を横断する顧客や著名に関わるもの
4	・利用者の機微な個人情報，あるいは顧客から提示された機密情報 ・機密性が失われた場合，利用者の資産もしくは社会的インフラの一部に影響が発生するもの ・機密性を担保する機能で使用されているもの
3.5	・資産評価3の基準に該当する資産の内，単体機器に含まれているか，サーバーが保持するセキュリティ・金銭に関わるか，サーバーや機器を横断する顧客や著名に関わるもの
3	・利用者の個人情報，あるいは顧客から提示された機密情報
2.5	・資産評価2の基準に該当する資産の内，単体機器に含まれているか，サーバーが保持するセキュリティ・金銭に関わるか，サーバーや機器を横断する顧客や著名に関わるもの
2	・システム提供者（メーカ・販売・保守）と利用者のみが知りうる情報等
1	・公開情報

資産評価	完全性（Integrity）の評価基準
5	・常に完全な状態であることが必要 ・完全性が失われた場合，利用者の生命，資産，もしくは社会的インフラに重大な影響が発生する
4.5	・5の資産評価基準のいずれかを満たす
4	・常に完全な状態であることが必要 ・完全性が失われた場合，利用者の資産もしくは社会的インフラの一部に影響が発生するかサービスやシステムの継続的稼動に重大な影響が発生する
3.5	・4の資産評価基準のいずれかを満たす
3	・常に完全な状態であることが必要 ・完全性が失われた場合，サービスやシステムの一部に影響が発生するか，機器の主要機能に影響が発生する
2.5	・3の資産評価基準のいずれかを満たす
2	・完全な状態に復元できることが必要ではない
1	・復元できない場合でも支障がない

資産評価	可用性（Availability）の評価基準
5	・常にアクセスできることが必要（1分以内） ・アクセスできない場合，利用者の生命や資産，もしくは社会的インフラに重大な影響が発生する
4.5	・5の資産評価基準のいずれかを満たす
4	・常にアクセスできることが必要（1分以内） ・アクセスできない場合，利用者の資産もしくは社会的インフラの一部に影響が発生するか，サービスやシステムの継続的稼動に重大な影響が発生する
3.5	・4の資産評価基準のいずれかを満たす
3	・常にアクセスできることが必要（1分以内） ・アクセスできない場合，サービスやシステムの一部に影響が発生するか，機器の主要機能に影響が発生する
2.5	・3の資産評価基準のいずれかを満たす
2	・24時間以内にアクセスできることが必要 ・アクセスできない場合，サービスやシステム，製品が提供する機能に影響が発生する
1	・24時間以内にアクセスできなくても良い

システムレベル	システム中の資産を分析対象とする条件
低	・経済的損失が大きい資産 ・漏洩した場合，当事者が精神的に大きな苦痛を受ける情報 ・CIA別資産価値基準の内，下記のいずれかが基準値を超えている資産 - 機密性 … 4.0 以上 - 可用性… 4.0 以上 - 完全性… 4.0 以上
中	・CIA別資産価値基準の内，下記のいずれかが基準値を超えている資産 - 可用性… 3.0 以上 - 完全性… 3.0 以上
高	・CIA別資産価値基準のいずれかが2.0を超えている資産

表 2　資産の評価基準，及びシステム中の資産を分析対象とする条件

3.1　専門家による脅威頻出箇所表の作成

本節ではまず，脅威分析について専門的な知識を持つ人物を「脅威分析の専門家」とし，脅威頻出箇所表の作成工程を述べる．

脅威頻出箇所表とは，特定のアーキテクチャを持つシステムにおいて，脅威が潜在しやすい箇所を予測した表である．

次に，専門家による脅威頻出箇所表の作成工程を示す．

1.　システムで生じうる被害の想定

分析対象のシステム，あるいは類似のアーキテクチャを持つシステムに対して，システム中で生じうる重大な被害を想定する．分析対象のシステムに対して想定を行う場合，システム開発者と共同で行ってもよい．
想定した被害のリストを作成し，次工程で利用する．

2.　想定した被害の分析・分類

前工程で想定した被害を分析する．この際，被害を受ける資産の分類と，資産に生じうる被害の分類を行う．被害を受ける資産は「機能」と「情報」に分類し，「機能」の受ける被害を「悪用」と「妨害」の 2 通りに分類する．「機能」の設置場所は信頼境界を基準とした内外，及び境界上の 3 通りである．「情報」は「悪用」と「損失」の 2 通りに分類し，最終的に被害を 8 通りに分類する．分類後，被害の分類ごとに，想定した被害のリストを作成する．

3.　DFD の作成

分析対象のシステム，あるいは類似アーキテクチャを持つシステムの開発資料から，システム全体の DFD を作成する．DFD の作成方法は，2.3 節で述べた工程と同様である．

4.　被害事例と脅威を関連付けた DFD の作成

2.で作成した被害事例リストを，3.で作成したシステム全体の DFD に関連付ける．この際，被害事例リストごとに DFD を作成する．また，システムに特有の脅威が考えられる場合は，本工程において記述する．

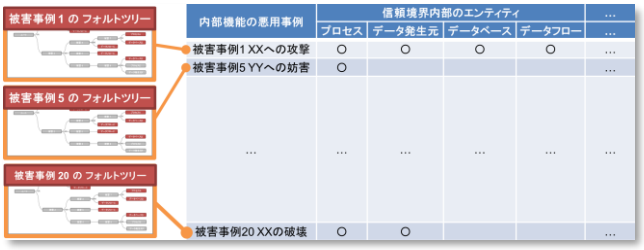

表 3　脅威頻出箇所集計表の作成

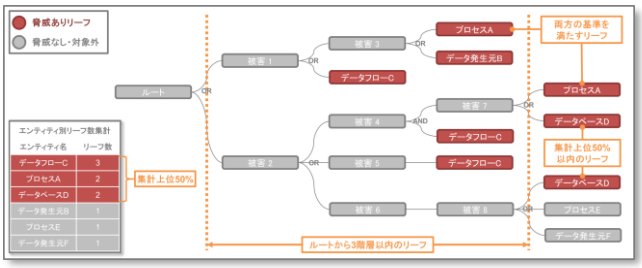

図 2　解析を実施する対象の抽出

5.　被害分類別の脅威頻出箇所集計表の作成

工程 5 で作成した被害事例リストごとの DFD それぞれに対して，フォルトツリー解析を行う．作成したフォルトツリーにおいて，リーフの総数や存在箇所に基づき，脅威が潜在する可能性が高い箇所を脅威頻出箇所として，チェック対象とする．脅威頻出箇所集計表の作成方法を，表 3 に示す．また，フォルトツリー中のリーフをもとに脅威頻出箇所とする基準を，図 2 に示す．図 2 に示した基準に基づいて，脅威が潜在すると判断したエンティティを集計し，脅威の潜在箇所を決定する．

6.　脅威頻出箇所表の作成

前工程で作成した脅威頻出箇所集計表を 1 つに統合する事で，脅威頻出箇所表を作成する．作成した脅威頻出箇所表を，表 4 に示す．

上記の工程により作成した脅威頻出箇所表を用いて，任意のシステムに対して脅威分析を実施する．

脅威頻出箇所表を用いた脅威分析を実施する際は，脅威分析について高度な知識は必要なく，システムに精通している技術者であれば分析が可能である．

次節より，提案手法において分析者が行う作業を述べる．

脅威分類 ＼ 頻出箇所			DFD							
			信頼境界内				信頼境界外			
資産分類	脅威分類	場所	プロセス	データ発生源	データベース	データフロー	プロセス	データ発生源	データベース	データフロー
機能	悪用	外部	○				○	○		○
		内部	○	○			○	○		
		境界	○	○			○	○		
	妨害	外部	○	○			○			○
		内部	○	○			○	○		○
		境界	○	○		○	○	○		○
情報	悪用		○				○	○		
	損失		○	○	○		○	○		

表 4　提案手法により作成した脅威頻出箇所表

3.2　分析者による脅威分析の実施

本節では，脅威分析について専門的な知識を持たない分析者が実施する工程を述べる．専門家が作成した脅威頻出箇所表を利用する事で，システム設計開発資料のみを用いた脅威分析が可能である．

次に，分析者による脅威頻出箇所表を用いた脅威分析手法の実施工程を示す．

1.　DFD の作成

分析対象とするシステムの設計書，仕様書などの開発資料から，システム全体の DFD を作成する．DFD の作成方法は，2.3 節で述べた工程，及び脅威頻出箇所表を作成する際の工程と同様であるため，専門家が先にシステム全体の DFD を作成している場合は再利用してもよい．

2.　脅威分析の対象を決定

前工程で作成，あるいは用意した DFD と，脅威頻出箇所表を関連付ける．脅威頻出箇所表では，あるアーキテクチャにおいて脅威が頻出する箇所を定義している．

ここで「関連付け」とは，DFD 中の要素ごとに，脅威頻出箇所表において脅威が潜在するとされているか確認する作業を指す．これより，分析対象とする要素を決定する．分析対象とする判断基準を，図 3 に示す．

この際，同時に分析対象外とする要素も決定する事で，TMT による自動分析で不要な検出結果の出力を抑える事ができるため，誤検出を低減できる．

3.　自動分析

TMT に脅威分析対象とする資産のリストを入力し，自動分析を行う．前工程で誤検出の対策は行っているが，分析結果に誤検出が存在する場合は手動で取り除く．

前節で述べた専門家が行う脅威分析箇所表の作成フェーズと，本節で述べた分析者が行う脅威分析のフェーズを，まとめて図 4 に示す．

次節において，提案手法において「脅威が頻出する」と判断する基準について，考察を述べる．

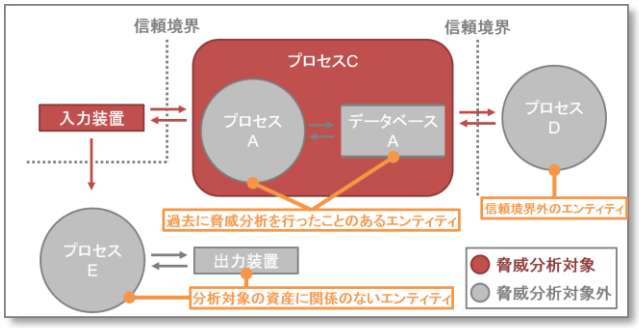

図 3　脅威分析対象とする基準

3.3　提案手法における脅威頻出箇所の基準

本節では 3.1 節で述べた，脅威頻出箇所表を作成する際の脅威が頻出すると判断する閾値について考察を述べる．

今回我々は，例として「ベイズ推定」を用いた評価基準に対し，「脅威分析レベル」を複数定義する事で，脅威分析の対象とするエンティティを決定した．

新たな脅威が生じた場合や，脅威分析対象のアーキテクチャに変更が加えられた場合，脅威頻出箇所表のアップデートが必要となる．その際，ベイズ推定を用いた脅威の潜在確率を定義する事により，従来の脅威頻出箇所表による脅威が潜在するとした事前確率と，アップデートによる脅威が潜在する事後確率を求める事で，新たな脅威への対応が容易になる．

ここで「脅威分析レベル」として，脅威が潜在する確率の閾値 20%，40%，60%，80%をそれぞれ脅威分析レベル 1，2，3，4 と定義した．脅威分析レベルが上がるにつれて，分析対象とするエンティティの数は増加し，閾値を超えたエンティティに対して脅威分析を実施する．100%はシステムの全エンティティに対して脅威分析を実施する事を意味し，0%は脅威分析を行わない事を意味する．

システムに対して適切な脅威分析レベルは，システムのアーキテクチャや重要度，あるいは要求される機密性，完全性，可用性等，あらゆるパラメータに依存する事は明らかである．そのため，手法の提案時において一意に定義する事は難しく，エンティティに対する脅威の潜在確率は，専門家，あるいは分析者が任意で決める必要がある．

次章において，実際にモデルシステムより作成した脅威頻出箇所表を用いて行った脅威分析の結果を述べる．

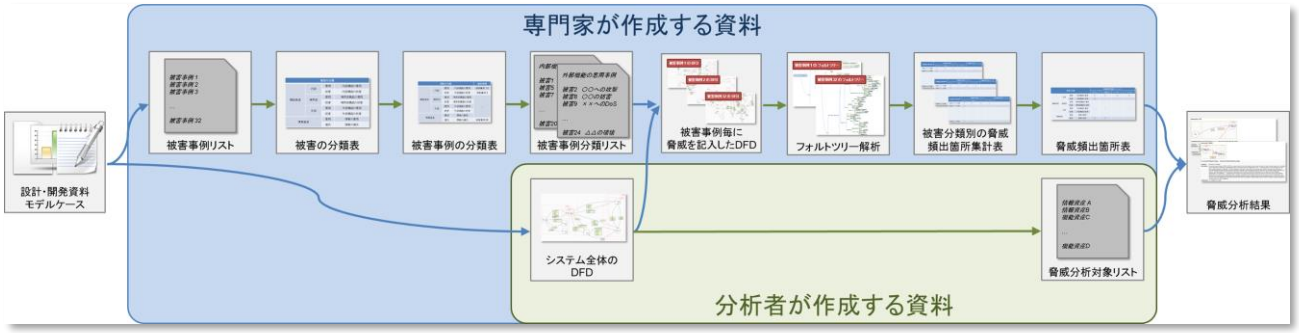

図 4　提案手法の工程図

4　モデルシステムに対する提案手法の適用

我々は今回，参考文献 [3]で示されている自動車内ネットワークに対するテレメトリーシステムに対して提案手法を適用し，実際に脅威分析の所要時間を計測した．

参考文献 [3]で検討されているシステムは，自動車の制御状態情報，各種センサー情報などの自動車内ネットワークで取得したメタ情報をクラウド上にアップロードし，車両利用者，自動車メーカー，損保会社などがデータを応用する事を想定している．以下，参考システムと記述する．

参考システムは主に，自動車，情報管理サーバー，第三者によるサービス群，及びそれらをセキュアに相互接続するインターネット回線から構成されている．さらなる詳細については，本論文では説明を省略する．

これらの情報をシステム設計資料と見なし，提案手法による脅威分析を実施した．

次節より，専門家が行う脅威頻出箇所表の作成及び，分析者が行う脅威分析の結果をそれぞれ示す．

4.1　脅威分析専門家による脅威頻出箇所表の作成

まず，参考システムを構成する全要素を参考文献から抽出し，さらに必要と考えられる要素を加えたシステムを想定した．以下，想定システムと記述する．

表 4 より，本手法においてはシステムの資産と脅威の種類，及び脅威の存在する場所により，8 種類の被害事例を想定した．表 5 に，想定した被害の分類結果を示す．

なお被害想定については，各分類結果において 1 つずつの具体的被害を想定しているため，分類ごとの被害想定リストは作成していない．

次に，想定システム全体の DFD を作成し，前工程で作成した表 5 を関連付ける．結果を，図 5 に示す．想定システムを構成するサーバー，サービス，ツールなどの構成要素を円形のエンティティとし，ネットワーク境界を信頼境界としている．システム管理者やシステム利用者，自動車を正方形のエンティティとしている．さらに，データフローで取り扱うデータを，箇条書きで記入している．

これらの結果からフォルトツリーを作成し，最終的な脅威頻出箇所表を表 6 に示す．なお，脅威頻出箇所表そのものには脅威の潜在確率が記載されており，表 6 は脅威分析レベル 3（60%）において閾値を超えたもののみを「○」として記載している．

被害想定の分類			想定した被害の具体例
資産分類	脅威分類	場所	
機能	悪用	外部	各種情報を閲覧するWebアプリケーションの乗っ取り
		内部	第三者の提供するサービスの乗っ取り
		境界	第三者の提供するサービスのサーバーに踏み台化
	妨害	外部	テレメトリングを行う車載器へのDDoS攻撃
		内部	収集した情報を管理するサーバーのなりすまし
		境界	テレメトリングに対する通信妨害
情報	悪用		収集した情報に含まれる個人情報の漏洩
	損失		収集した情報を保存したデータベースの破壊

表 5　想定した被害の具体例と分類結果

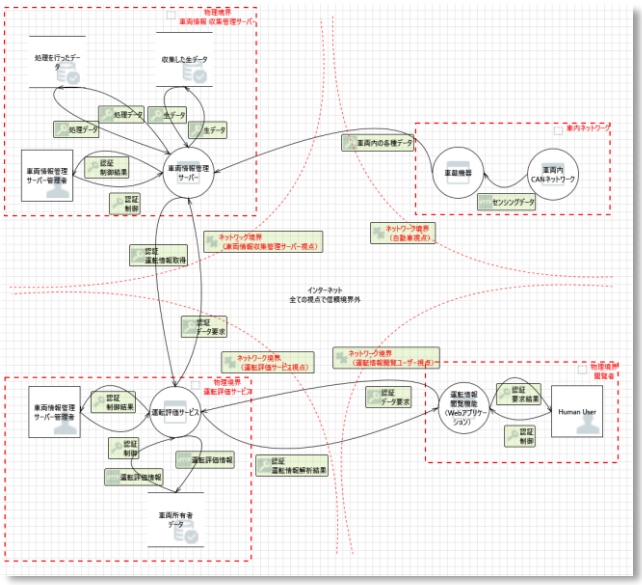

図 5　想定システムの DFD

脅威分類＼頻出箇所			DFD							
			信頼境界内				信頼境界外			
資産分類	脅威分類	場所	プロセス	データ発生源	データベース	データフロー	プロセス	データ発生源	データベース	データフロー
機能	悪用	外部				○	○	○		○
		内部	○	○	○					
		境界	○	○						
	妨害	外部					○	○		○
		内部	○	○			○			
		境界	○	○			○	○		
情報	悪用		○				○			
	損失		○	○	○					

表 6　想定システムより作成した脅威頻出箇所表

本想定システムではデータをサーバーに集約するため，信頼境界外にデータベースは存在しない．脅威頻出箇所表を作成した事で，データベースに関する脅威が信頼境界外に存在しない点が明示的になった．

次節では，分析者による脅威分析の実施結果，即ち提案手法の適用により抽出した脅威を概説する．

4.2　分析者による脅威分析の実施

前工程で作成した脅威頻出箇所表を用いて，分析者が脅威分析を行った結果について述べる．今回，想定システムについて専門家が予め作成した DFD と被害想定リストを再利用する事で，分析者の負担を軽減している．分析者が行ったのは，脅威頻出箇所表と DFD の関連付け，TMT による自動分析と誤検知の除去である．

一般に Attack Surface とされる，信頼境界と交わるデータフローを含めて，TMT に自動分析対象のエンティティを入力した．本実験では，全 29 箇所のエンティティに対して，12 箇所のエンティティが脅威分析対象となった．即ち，17 箇所は脅威が潜在する確率が 60%以下であったため，脅威分析の対象外となった．

TMT で自動分析を行った結果，12 箇所のエンティティに対して 38 個の脅威が検出された．さらにこの結果から，TMT 上での条件設定が不十分であったために生じた誤検出を取り除いた結果，　26 個の脅威が顕在化した．

次節では，本手法を想定システムに適用した脅威分析に要した時間を述べる．

4.3　提案手法による脅威分析に要した時間

本節では，専門家が脅威分析箇所表を作成する際に要した時間について述べる．

本手法において，最も時間を要するのはフォルトツリーの作成である．これはフォルトツリー解析そのものの課題であり，提案手法の改善で解決する事は難しい．表 7 に，想定システムにおけるフォルトツリー解析で要した時間と，フォルトツリー中に作成したリーフ数を示す．

システムに対して，各被害分類において 1 つずつ被害を想定した場合，フォルトツリー作成には 20 時間弱を要した．想定される被害が多くなるにつれて，脅威頻出箇所表の作成に必要な時間は増大する．

本手法の特徴として，実際の製品開発プロセス内での，分析者による脅威分析の実施コストを下げられる点が挙げられる．

対して，専門家による脅威頻出箇所表の作成は複数の脅威を想定し，DFD，及びフォルトツリーを想定した脅威と同じ数だけ作成する必要がある．また，継続的なアップデートも必要であり，分析者への負荷が大きい点が明らかになった．

4.4　今後の課題

本節では，提案手法の課題点と，解決策を検討する．

- より明確な被害事例分類方法の検討

現在，被害事例は 8 種類に分類しており，各被害事例の重複を許可していない．そのため，想定した被害事例が少ない場合などに，作成した脅威頻出箇所表の結果に，偏りが生じる可能性が考えられる．脅威頻出箇所表に偏りが生じた結果，最終的な脅威分析結果にまで影響を及ぼす可能性がある．

解決策として，被害事例を分類する際，複数の原因により生じると想定される被害について，分類の重複を許可する事が考えられる．これにより想定すべき被害事例数を抑えられるとともに，作成するフォルトツリー，DFD 数を抑える事が可能である．

- 脅威頻出箇所表のアップデート

第 3 章において，本論文における提案手法を述べた．脅威頻出箇所表の作成工程については詳細に述べたが，アップデートに関して，一意な基準を設けていない．これは脅威分析の対象により，システムの重要度や製品サイクルが異なるためである．

解決策として，ベイズ推定の事前確率として過去全ての脅威分析結果を利用するのではなく，一定数の結果を利用する事が挙げられる．各エンティティにおける脅威存在確率を 50～100%としたシミュレーションの結果，過去 5 回分の結果をもとに事前確率を求めた場合に，精度が保たれる結果となった．ただし，条件がシステムにより異なるため，さらなる検討が必要である．

想定した被害の具体例	作成時間	作成したリーフ数
各種情報を閲覧するWebアプリケーションの乗っ取り	2時間40分	26
第三者の提供するサービスの乗っ取り	2時間30分	66
第三者の提供するサービスのサーバーに踏み台化	2時間00分	29
テレメトリングを行う車載器へのDDoS攻撃	2時間30分	29
収集した情報を管理するサーバーのなりすまし	2時間30分	49
テレメトリングに対する通信妨害	3時間00分	64
収集した情報に含まれる個人情報の漏洩	1時間40分	54
収集した情報を保存したデータベースの破壊	2時間10分	134

表 7　フォルトツリー解析に要した時間と作成したリーフ数

5　まとめ

本論では，システム開発及び脅威分析に対し専門的な知識や経験を持たない技術者であっても，過去の分析結果を活用する事によって，要点を押さえた脅威分析が実施できる手法を提案した．

この提案手法によって脅威分析に対する専門的な知識を持たない技術者であっても，システムにおいて脅威が比較的多く潜在する箇所を推測し脅威分析を実施する事が可能となる．提案手法では，導入時にフォルトツリーによって脅威頻出箇所表を作成する必要があるが，脅威頻出箇所表は多くの脅威分析において共有が可能なので，長期的には脅威分析業務全体のコストを削減する事ができる．

ただし，提案手法は重視すべき箇所に限定し分析するため，脅威分析において網羅性の高さが要求されるケースではこの手法は適さない．

今後，実際の開発プロセスに導入し実用性を評価するとともに，他の脅威分析手法との比較方法についても検討していく必要がある．

参考文献

[1]　A. Shostack, Threat Modeling: Designing for Security, Wiley, February 2014.

[2]　B. Schneier, “Attack Tree,” Dr. Dobb's Journal, Vol. 24, p. No. 12, December 1999.

[3]　金. 鶴. 手. 井. 江﨑貴也,“全車載 LAN データをクラウドサービスで安全に利用するためのシステムの試作,” 第 9 回地域間インタークラウドワークショップ, 2016.

[4]　Microsoft Corporation, “Microsoft Threat Modeling Tool 2016,” Microsoft Corporation, 6 October 2015. [オンライン]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=49168.

[5]　独立行政法人 情報処理推進機構, “守るべき情報資産・情報リスクの考え方,” December 2004. [オンライン]. Available: https://www.ipa.go.jp/files/000013297.pdf.