Attack Tree を用いたクリティカルパス検出による効果的対策の提案

柴田 理洋[†1]　大久保 隆夫[†1]

概要：近年サイバーセキュリティのリスクが増大する一方で，既に稼動しているシステムの脆弱性を根本的に修正することは難しく，要求工学の見地から未然にセキュリティを確保することが必要である．一方，既存の主流な脅威分析手法には対策手法選定や網羅性，属人性など複数の既知問題があり，現場レベルでの実用性向上が求められている．そこで本研究では，セキュリティ対策の選択において効率的な対策選定を実現する手法として，アタックツリー分析を用い導出した「クリティカルパス」と呼称する概念による観点から攻撃パスをふさぐ手法を提案する．

キーワード：攻撃木，脅威分析，効率化

Proposal of effective measures by Attack Tree based on detection of critical path

Tadahiro Shibata[†1]　Takao Okubo[†1]

Abstract: It is necessary to ensure security in advance in terms of requirements engineering, because of the increase of cyber-attacks and the difficulty of fixing the vulnerabilities of the running system.　On the other hand, the existing major threat model analysis methods have several known problems. So, a practical approach is needed.

In this study, we propose a method to block the attack path that was derived using the attack tree analysis from the point of view of the critical path. This approach implements the effective selection of security measures.

Keywords: Attack Tree , Threat analysis , efficiency

1. はじめに

近年，重要インフラや多くの産業システムがインターネットを活用し利便性を向上させた一方で，それらのシステムを狙ったサイバー攻撃が増加している．最新の脅威情報は現場で共有され，何らかのインシデントが発生した際も即座に対応する体制が世界的に整えられるようになってきた．しかし，いかにインシデントレスポンスを向上させたとしても，セキュリティを侵害されてしまえばその損害は非常に大きい．またシステムの膨大化・複雑化に伴い，守るべきセキュリティの要件も煩雑かつ広範囲になっており，セキュリティ対策の漏れを完璧に防ぐことは難しくなってきている．さらには一度運用を始めたシステムでは可用性の問題から根本的な対策を行なうことが困難なケースもある．このようなセキュリティ上のリスクを回避するために，未然にセキュリティを確保することが重要となっている．

従来の工業機械などでは安全性を何より最優先として実現させるために，設計段階からリスクを分析し，実現する手法がとられてきた．このような視点をサイバーセキュリティに導入した脅威分析も存在する．

情報システムの設計段階で想定されうるリスクやインシデントを分析し，対策することでインシデントを未然に防ぐことが可能であり，今後のセキュリティ対策で重要な手法であると考える．

2. 既存の脅威分析手法

2.1 Attack Tree

Attack Tree または攻撃木（以下アタックツリー）分析とは，攻撃者の視点による段階的な攻撃手法の分析である．ツリー構造のルートには攻撃者の最終目標を設定し，その目標を達成するために考えられる，より具体的な手法・手段を下層に記述する．これを繰り返すことで攻撃者が取りうる攻撃方法を分析し，それぞれのリスクの度合いを分析するトップダウンの解析手法である[1][3][4].

後述する脅威分析手法と異なり，アタックツリー分析における標準的な取り決めは存在しない[1].

簡易な例として，Attack Tree の考案者である Schneir の web サイト[2]より図 1 を引用する．

†1 情報セキュリティ大学院大学
Institute of Information Security

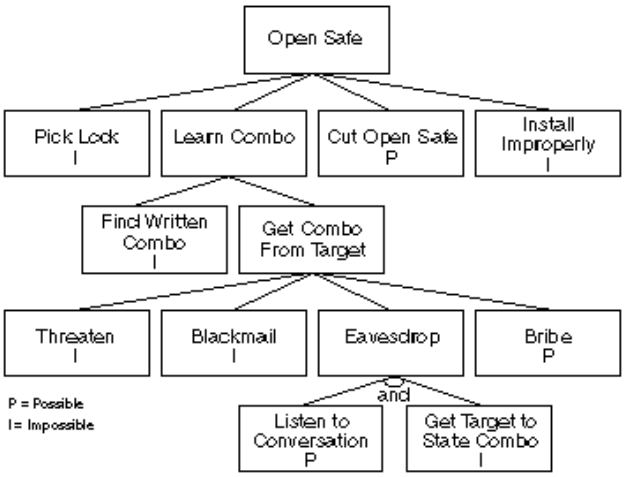

図 1 Attack Tree の一例（引用）

2.2 STRIDE

STRIDE 手法は, マイクロソフト社の Security Engineering and Communications グループによって考案された脅威分析の記法である[4]．STRIDE という名称は以下の，(1)Spoofing(なりすまし)，(2)Tampering(改ざん)，(3)Repudiation(否認), (4)Information Disclosure(情報漏えい), (5)Denial of Service(サービス拒否)，(6)Elevation of Privilege(特権の昇格)という 6 つの脅威の頭文字をとったものである．これら 6 つに脅威を大別し，攻撃者がどのような攻撃を行うのか予想セキュリティ課題を分析する．

それぞれの脅威に対する防御特性を関連付けて考えることで，安全なシステム開発を行うための基本的な指針となる．このような指針を元に，システム開発段階で安全性の検証を行なうことで，より安全なシステムの開発を目的とする[5][6][7].

2.3 i*-Liu

i*-Liu とは，i*と呼ばれる要求分析の手法をセキュリティ要求分析のために拡張した手法である[8].

i*とは複数のステークホルダー間の意図や因果関係を分析する，ゴール指向と呼ばれる要求手法である．アクタ（関係者），ゴール，タスク，ソフトゴール（非機能要求），ソースの概念によりシステム要求を定義する．これらをグラフのノードで表現し，相互の依存関係を記述する．

i*-Liu 分析は i*の図式要素にアクタとして「攻撃者」を加え，攻撃者，悪意，脆弱性，攻撃方法およびその対策を分析する．攻撃者アクタに対応して，通常のタスクと同様にゴール・ソフトゴール・タスク・リソースを記述する．

2.4 KAOS

i*と並ぶゴール指向要求分析の代表であり，主要な記述方法も類似している．KAOS には，システムが満たすべき目標点であるゴールと，攻撃者が満たすべき目標点である反ゴールの，2 種類の区別されるべきゴールが存在する[9].

i*が「誰（アクタ）」から分析を開始するのに対し，KAOS は「何故（反ゴール）」から分析を開始する点で異なる．

2.5 FTA

FTA は Fault Tree Analysis の略で日本語では故障の木解析という．ツリー構造のルートに故障などのシステムの望ましくない結果を置き，その原因となる事象を階層的に展開していく．末端の葉ノードにはルートに設定した「望ましくない事象」の原因事象となる[10].

下層のノードは AND もしくは OR で上位ノードに接続しており，各葉ノードに設定される発生確率を加算ないし乗算していくことでルートである故障の発生確率を定量的に求めることが可能である．

情報システムではなく，主に工業機械の開発に用いられる分析手法である．

2.6 ETA

ETA は Event Tree Analysis の略で日本語では事象木解析という. 膨大でツリー構造が煩雑となってしなう FTA をより分かりやすく表現するための手法として考案された[10].

ETA は起因事象（大本として発生する事象）を始点として，その事象への対策を時期列に沿って順に記述する．各対策は成功/失敗で分岐しており, 失敗の場合に次の対策に遷移する．こちらも成功/失敗の確率を積算することで起因事象の発生確率を求めることができる．

FTA と同様に情報システムではなく工業機械の開発に用いられる．

3. 用語

3.1 クリティカルパス

クリティカルパスとはプロジェクトマネジメント手法において効率性を図る数学的アルゴリズムである．プロジェクト完了までに必要な全ての要素を依存関係に従って記述し, 各要素の完了に必要な時間をコストとして設定する．これらの値を用い，最もプロジェクトが最長となる経路を求めたものがクリティカルパスと呼ばれる．このクリティカルパス上に存在する要素が遅延するとプロジェクト全体の遅延に直結するため，スケジュール管理を行なう上で最も重要な要素とされる．

以上のように，クリティカルパスという用語は最短，あるいは最長経路問題という意味であるが，本論文中においては「ツリー構造，またはグラフ構造を用い，視覚的・直感的に判断可能な手法をクリティカルパスと述べる．

3.2 ボトルネック

クリティカルパス上において，もっとも重要となる箇所のノードをボトルネックと称する．効率化において，最も優先順位が高く，対策による費用対効果が大きいことを意味する．

4. 脅威分析における既知の問題点

4.1 要求の完全性

要求工学とは事前にステークホルダーの要求を完全に導出し，それらの要求を実現するための手法である．しかしセキュリティという領域において要求工学を適用しようとすると，最も重要なステークホルダーである攻撃者の要求を事前に把握することができないという根本的な要求の欠落が存在する．これは上記に示したいずれの脅威分析手法も満たすことができない．

4.2 要求される技術力

4.1 節で示したように要求分析の段階で攻撃者の要求を知ることは難しい．したがって脅威分析を行なうためにはシステムの開発者が攻撃者の視点を想定した分析を行なうこととなる．しかし攻撃手法に精通し，設計段階で漏れなくリスクを洗い出した上で対策まで考案できる高度な技術者は多くない．つまり現場技術者のレベルによっては脅威分析の実用性が得られない場合が発生しうる．

4.3 コストに見合わない対策

セキュリティ要求分析を行なったとき，考慮しうる全てのリスクに対応することが基本となる．確かに理想としてはどのようなシステムであっても完璧なセキュリティを実現することが望ましいが，現実問題としてセキュリティ対策に割くことができるコストは有限である．したがって状況に応じては対策を行なわないリスクを考慮する必要がある．

4.4 確率

3 章で例示した脅威分析手法，特に Attack Tree や構造が類似した FTA では，確率論を元にセキュリティリスクを算出している．確かに攻撃者の視点において，あるシステムに対する攻撃が成功するか否かは確率的に表現することが可能である．しかし防御側の視点としてセキュリティを設計する際には，脅威分析を漏れなく行なうことが可能であると仮定した場合，あるリスクにおいてインシデントが発生するか否かは確率ではなく成功／失敗の二値で表されるべきである．特に近年話題となっている標的型攻撃においては標的とされたシステムに最適化された攻撃が行われるため，一般化された攻撃の確率を用いることが可能であるか疑問である．

5. 提案

5.1 提案手法

本研究では 4 章で述べた問題点のうち，特にコストの問題に着目し，現場レベルの実用的な低コストでの脅威分析を実現するための手法を提案する．コストとトレードオフの関係となる網羅性・完全性については多少失うことを許容するものとする．

具体的な手法としては，まずはアタックツリー分析をベースとして，ある情報システムにおける脅威を分析する．その結果として得られるツリー構造において，ボトルネックとなっているノードを抽出し，当該中間ノードの対策の優先順位を高く設定する．これにより全末端ノードの対策を行なうよりも低コストで最終目標を達成することが可能であるという仮定を立てた．

5.2 利用手法

本提案ではアタックツリー分析を用いる．

その理由として，以下の点が上げられる．

1. ツリー構造であるため，ボトルネックとなるノードを視覚的に導出しやすい．
2. 攻撃者視点による分析であるため，確率論ではなく可能／不可能による二値での判定となる．
3. 異なる攻撃目的のために同一の下層が存在するため，ツリーではなくグラフとして表現することが可能である．
4. 基本的には各末端ノードが対策すべきノードであるが，必ずしもそうではなく，効率性を視覚的に明示可能である．

またオリジナルの Attach Tree による記述法との差異を以下に述べる[2][3].

オリジナルの記法においては，末端ノードでの対策コスト・普遍性の 2 要素に着目して最適な対策手法を求める．Schneier の web サイトより図を引用する[2].

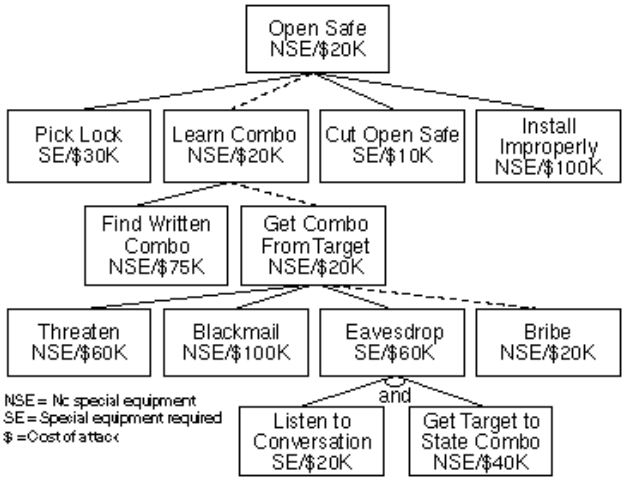

図 2　各要素を含めて記述した Attack Tree（引用）

1. 末端ノードに導出された攻撃手法を行なうためのコストを求める．本図では単位は 1000 ドル．またコストの求め方は Attack Tree の範疇ではない．
2. 末端ノードに導出された攻撃手法が SE（特殊な手法が必要）もしくは NSE（特殊な手法が不要）かを記述する．
3. 下位ノードから上位ノードのコスト値を順に求める．このとき，下位ノードに SE と NSE が混在する場合，無条件に NSE ノードを採用するものとする．
4. 下位ノードが And 回路であればコストの合算コスト，Or 回路であれば下位ノード群の最も安いコスト値を

上位ノードのコストとする.

5. ルートノードまで繰り返す.
6. ルートノードで得られたコストが，ルートノードに設定された攻撃目標を最も安く達成するコストである．そのため，当該コストの元となった末端ノードを最も優先して対策すべきである.

このようにオリジナルの手法においては末端ノードに着目して対策の優先順位を決定している．しかしこの方法では真に攻撃者の攻撃手法を決定しているとはいえない．なぜなら他に攻撃を受け入れる可能性のあるパスが存在している以上，明確な意思を持った攻撃者による攻撃を防ぐことはできないからである．この Attack Tree の仕様は，Attack Tree が考案された 1999 年という時代背景上，スクリプトキディによるイタズラ的犯行が横行していたためと推測する.

したがって本研究では，「攻撃の行いやすさ」ではなく，「攻撃者視点で作成した Attack Tree に対し，防御視点として自明に攻撃パスを塞ぐこと」を評価基準とした.

5.3 記述規則

本研究における Attack Tree の作成手順を以下に示す.

1. 脅威分析を行なう情報システムにおいて想定されるセキュリティリスクから，攻撃者が目標にすると推測されるリスクを抽出する.
   例 : 情報の取得，システムの停止，web ページの改竄，など.
2. 手順 1 で抽出された要素をルートノードとして，それぞれに通常の Attack Tree 分析を行なう.
3. 複数のノードにおいて，そのノードより下位に存在するノードが共通している場合，共通しているノードを統合し，ツリー構造からグラフ構造に変化させる.
4. ルート・末端を含む全ノードにおいて，当該ノードに指向するノード数および当該ノードから指向するノード数を計算する.
5. 上記計算式で得られた数値において，数字が大きいノードがボトルネックであり，優先して対策を行なうべきノードである.

5.4 実証

本研究では比較的システムの詳細がインターネット上で公開されている日本年金機構の，2015 年時点でのものを用いる.

まず標的型攻撃の目標を情報の取得と仮定し，アタックツリーを作成したものを図に示す．アタックツリーの作成にあたり，厚生労働省がホームページに記載している調達情報の一部，年金機構情報漏洩事案の報告書，および標的型攻撃に関して公開されている一般的な対策手法を参考とした[11][12][13][14][15].

作成したアタックツリーを図 2 に示す.

改めてこのアタックツリーを分析した際に，各ノードにおいて依存しているノード数と依存されているノードの合計数が多いノードがボトルネックの箇所ということができる．これを表 1 にまとめる.

表 1　パス数の多いノード

ノード	個数
LAN 内の端末に侵入	5
個人情報が外部からアクセス可能	4
無線 LAN からの侵入	4
物理的アクセス	4
マルウェア感染	4

しかし表に示したノードには，非常に近類似した具体的手法が書かれているために個数が増加しているものがある．記述として恣意的に個数が増減する可能性はあるが，それだけ周知されている脆弱性でクリティカルであると考える．この点において，どのように正規化するかは今後の課題である.

またシステム設計上，自明として「個人情報が外部からアクセス」と「物理的アクセス」はリスクとしえ除外される.「無線 LAN からの侵入」も，運用ポリシー違反が露呈した組織であるため断言はできないものの，システム設計図上では無線 LAN は運用されていないため今回は除外する.

以上より，最も優先的に対処すべき箇所として「LAN 内の端末に侵入」，次点で「マルウェア感染」と判明する.

体が困難であるため本研究の対象外である．

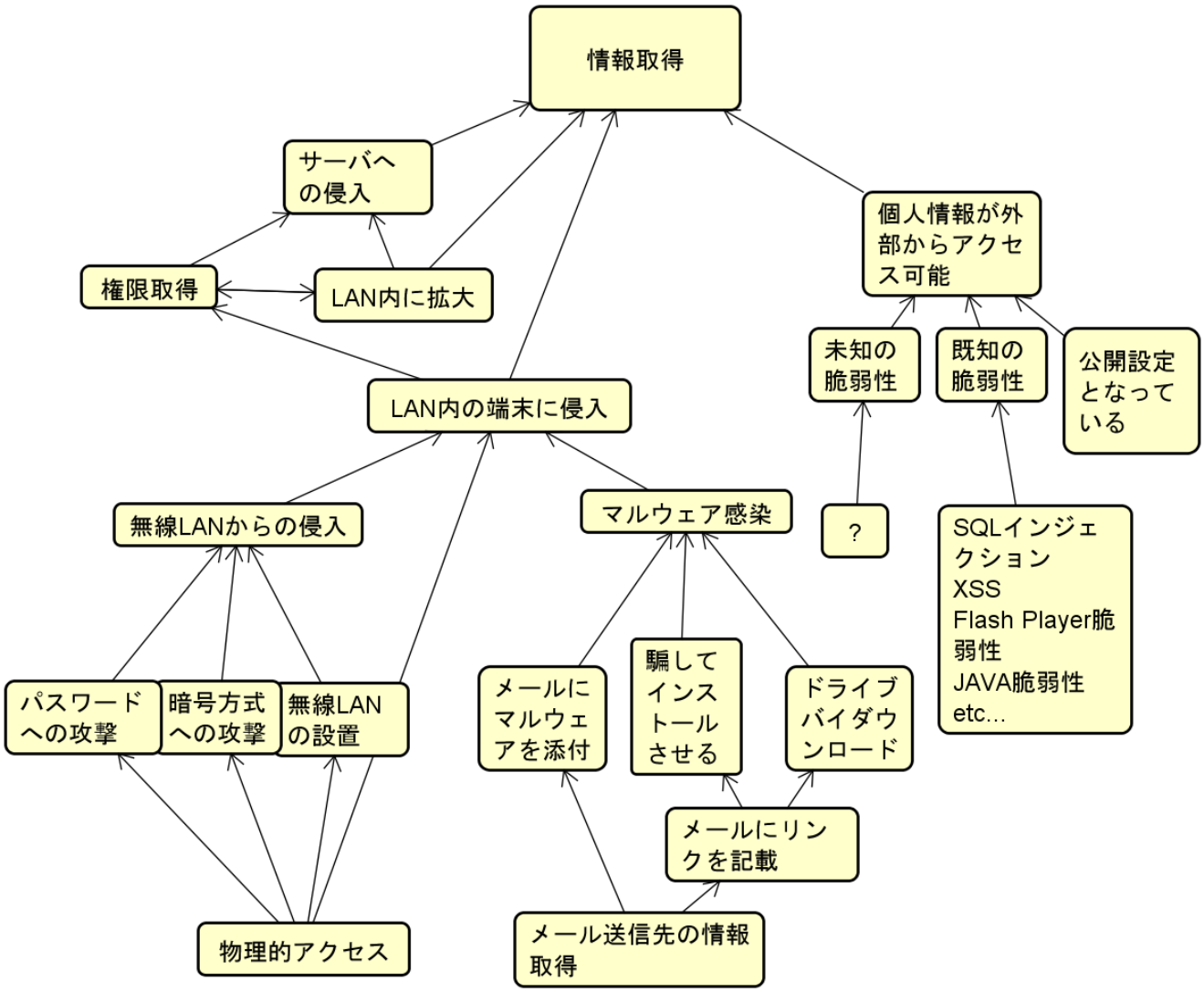

図 3 年金機構における Attack Tree

6. 評価

以上の方法により得られた中間ノードが全て対策可能である必要がある．今回の実証事例において導出された中間ノードについて，それぞれ検証する．

1. 個人情報が外部からアクセス可能
   単純にクローズドなシステム設計とすることで解決可能．
2. 無線 LAN からの侵入
   有線のみとし，無線 LAN を物理的に設置しないことで解決可能．
3. 物理的アクセス
   入退室管理を行なう，警備員を配置するなどにより解決可能．
4. マルウェア感染
   既知マルウェア，もしくは未知であっても挙動が単純なマルウェアであればセキュリティソフトの導入により対処可能．高度な未知マルウェアについては検出自
5. LAN 内の端末に侵入．
   一時感染された端末内に機密情報が存在，もしくは LAN 内の端末に共有状態で機密情報が存在する場合に機密情報が攻撃者に漏洩する．したがって機密情報は暗号化されたサーバーなどで一元管理することで解決可能．しかし Golden Ticket 攻撃などにより，権限を不正に取得された上でサーバー上のデータベースにアクセスされることは防ぐことは出来ない．このような既知の権限昇格攻撃はパッチ等により解決可能．

以上のことから，本実証においては中間ノードの対策自体は可能であることを示すことができた．しかし最も大きなボトルネックとなった「LAN 内の端末に感染」ノードにおいては単一の対策により簡易に解決を示すことが出来なかった．これは上層へ指向するパスが複数存在する場合，パスによって適切な対策が異なることを意味する．単一の中間ノードに対して複数の対策を必要とするならば，本研究の仮定として提起した「中間ノード対策による低コスト化」を自明に示すことができなくなり，別アプローチから

の評価が必要である．

7. 考察

評価の章で示したように，単純な Attack Tree のグラフ化では対策数の減少によるコスト減を示すことが困難である．その理由としては，Attack Tree 上に記述したノードに，複数の性質が混在したことが挙げられる．具体的には技術的な脆弱性と運用上の脆弱性であり，攻撃の視点では区別する必要はないが，防御の視点では明確に取るべき対応が異なる．例えばサーバー上に存在する機密情報へのアクセスに際し，技術的な面としては LAN 内の端末がマルウェアに感染すること想定して，ユーザー権限によりアクセスを制限する，暗号化しパスワードを要する，などが挙げられる．一方，運用上の面としては，ローカルに機密情報を保存しない，不用意に不審な実行ファイルを実行しない，などが挙げられる．前者は攻撃が可能か不可能かを，当該システムの現状によって明確に示すことができる．後者は特定の情報システムであっても運用状況如何によって攻撃の可能／不可能が変化するので，Attack Tree 上で表現するためには図 4 に例示するように，なんらかの方法で条件を記述する必要がある．

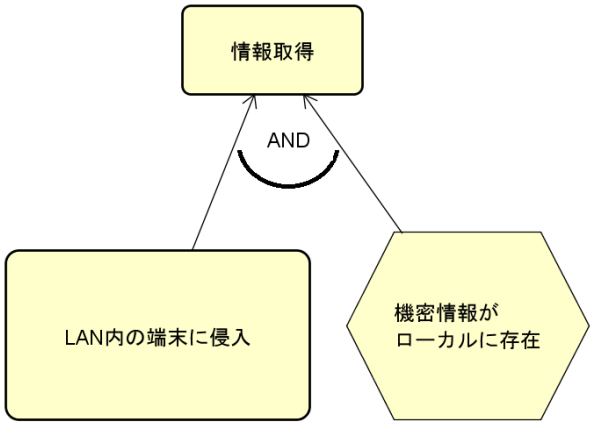

図 4 条件を記述した Attack Tree の記法

6 章で示した LAN 内の端末に感染」ノードにおいては，複数の上方向パスが存在し，なおかつそれぞれが技術的問題と運用的問題であったことも対策が煩雑になる要因と考えられる．

8. まとめ

本研究では Attack Tree を応用することにより，効率的な対策手法の選定基準の可能性を提示できた．しかし確実にそうといえる評価は示すことができておらず，今後の課題である．

また本研究の提案手法では脅威分析における既知の脆弱性において，以下の二点が未解決である．

まず属人性が高いという点を解決できておらず，誰しも同様に利用可能とする必要がある．このために簡易なアルゴリズム化や，マニュアルの作成が必要と考える．

次に完璧にリスクを網羅していることを保証できない点である．本提案手法においても真にシステムに対するリスク全てを考慮したうえで対策を示すことを保証してはいない．

今後はノードの性質を念頭においたノードの集約方法を模索し，更なる別アプローチも含め低コストでの対策手法選定を示したい．

参考文献

[1] “アタックツリーによる脅威分析”，第一回脅威分析研究会，2016/1/12
[2] Schneier, “Attack Trees“. https://www.schneier.com/academic/archives/1999/12/attack_trees.html, (参照 2016-08-09).
[3] 松並 勝，“脅威分析研究会発表資料 Chapter4 Attack Trees”. https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6M2UzZDhjYWE5ZmU2NzJjYQ, (参照 2016-08-09).
[4] 松並 勝，“仕様と設計のセキュリティ分析”. https://www.asteriskresearch.com/wp-content/uploads/, (参照 2016-08-09).
[5] “Microsoft セキュリティ上の脅威の評価 “. https://msdn.microsoft.com/ja-jp/library/ms172104(v=vs.80).aspxa, (参照 2016-08-09).
[6] Micheal Howard, David LeBlanc ,WRITING SECURE CODE 2004,90p
[7] Adam Shostack. threat modeling designing for security, 2014, 59p,87p
[8] 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 Vol.52 No.9 P2775 - 2787，2011/09/15 .
[9] 田原 康之，“セキュリティ要求工学の実効性:4.KAOS によるセキュリティ要件の獲得・分析”，情報処理 Vol.50 No.3 P203-208，2009/3/15.
[10] 後藤 伸寿，重盛正哉，“フォールトツリー解析及びイベントツリー解析によるリスク評価の事例”，みずほ情報総研技報 Vol.7 No.1，2015/3 http://www.mizuho-ir.co.jp/publication/giho/pdf/007_06.pdf (参照 2016-08-09)
[11] “『高度標的型攻撃』対策に向けたシステム設計ガイド”，https://www.ipa.go.jp/security/vuln/newattack.html, (参照 2016-08-09)
[12] “日本年金機構間接業務システム ハードウェア等賃貸借一式 調達仕様書”，http://www.mhlw.go.jp/sinsei/chotatu/chotatu/kankeibunsho/090410/dl/01.pdf，(参照 2016-08-09)
[13] “日本年金機構における個人情報流出事案に関する原因究明調査結果”，http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf , (参照 2016-08-09)
[14] “脅威を増す標的型のサイバー攻撃に関する注意喚起 別紙”，https://www.ipa.go.jp/about/press/20111018.html (参照 2016-08-09)
[15] “高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて”，2016/3/31，https://www.jpcert.or.jp/research/apt-guide.html