SCIS 2019 2019 Symposium on Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics, Information and Communication Engineers

脆弱性データベースを使用した脅威分析方法 ～トピックモデルの活用と過去の分析結果の再利用について～

Threat analyses using vulnerability databases − Practical use of topic models and reuse of past analysis results −

梅澤 克之 *† Katsuyuki Umezawa
三科 雄介 * Yusuke Mishina
Sven Wohlgemuth ‡§
寶木 和夫 * Kazuo Takaragi

あらまし 我々は脆弱性事例データベースとシステム設計情報を活用した脅威分析方法を提案してきた．提案手法はアタックツリー（*AT* と呼ぶ）分析を基にしており，評価対象システムの *AT* と既知の脆弱性に関する *AT* を作成し，両種の *AT* を突合することでより具体的な *AT* を作成可能とする．これにより起きては困る事象の発生確率の計算や今後の分析における活用が可能になる．具体的には脅威分析のアルゴリズムを示し，数式による定式化を行った．またトピックモデル解析ツールを用いて我々のアルゴリズムの中の自然言語処理を用いた突合の実現可能性を検証した．本論文では，ある事例に関する脅威分析で作成した *AT* が，次の脅威分析のための情報として利用可能であることを事例をもとに示す．

キーワード 脅威分析，脆弱性情報，アタックツリー

1 はじめに

セキュリティの脅威によるセーフティへの干渉/中断は、電力，情報通信，自動車，航空，鉄道，医療などの安全重視システムにおいて大きな課題として認識されている．EVITA プロジェクト [1] では，車両内通信のセキュリティに関して，リスク分析，セキュリティ要件設定，アーキテクチャ設計，FPGA による Hardware Security Module (HSM) の試作、デモの実施が行われた．この際のリスク分析にはアタックツリーが用いられた．また，セーフティ（ハザード）とセキュリティ（脅威）の因果関係を分析する方法の 1 つは，フォールトツリー (*FT*) とアタックツリー (*AT*) の組み合わせでその関係を表現することである [2]。

米国 MITRE 社はいくつかの形式の脆弱性データベースを提供している．CVE（Common Vulnerability and Exposure：共通脆弱性識別子）[3] では，個別のソフトウェアの脆弱性がデータベース化されている．また，CWE（Common Weakness Enumeration：共通脆弱性タイプ）[4] では，脆弱性が発生する原因部分に焦点を当て，共通の脆弱性がカタログ化されている．さらに，CAPEC（Common Attack Pattern Enumeration and Classification：共通攻撃パターンタイプと分類）[5] は，攻撃パターン別に分類されたデータベース (DB) となっている．

FT 分析に関連する科学文献は，今日，成熟している．信頼性と安全性の分野では，多数の例と事例が存在する [2]．一方，セキュリティ分析では，問題の複雑度が格段に大きくなる．CVE に報告される脆弱性は年に 1 万件を超えること，さらに，巧妙な攻撃はそれら脆弱性の複数個の組み合わせで起きること，さらに，それらの可能性を網羅的に押さえた *AT* を作成することは容易でない等の問題があった．

我々は，このような問題に着目し，現実的なアプローチとして，脆弱性データベースを使用した脅威分析方法の提案してきた [6][7]．具体的には，まず，攻撃者はアタックする際に、既知攻撃の模倣，あるいは既知攻撃のマイナーな変更である確率が高いと考えた．そこで過去に起きた事例を *AT* で表現することによって，設計者に関連攻撃を気づかせる（危険性を認識させる）ことができると考えた．このアプローチを漸次，継続適用するこ

* 国立研究開発法人産業技術総合研究所, 東京都江東区青海 2-3-26, Advanced Industrial Science and Technology (AIST), 2-3-26 Aomi, Koto-ku, Tokyo 135-0064, Japan
† 湘南工科大学, 神奈川県藤沢市辻堂西海岸 1-1-25, Shonan Institute of Technology, 1-1-25 Tsujido-Nishikaigan, Fujisawa, Kanagawa 251-8511, Japan
‡ 株式会社日立製作所, 神奈川県横浜市戸塚区吉田町 292 番地, Hitachi Ltd., 292 Yoshida-cho, Totsuka-ku, Yokohama, Kanagawa, 244-0817, Japan
§ Sven Wohlgemuth ' s contribution to this work is based on his research at Albert-Ludwig University, Freiburg, Germany, and other organizations before he joined Hitachi, Ltd. in February 2017.

とで，リスク軽減に役立足せることができる。

ただし，今まで提案してきたアルゴリズムの中に，自然言語で記述された *AT* の各ノードを自然言語処理とAI 処理を用いて突合評価を行う処理が記述されているが，文献 [6][7] では，この処理が未解決であった．文献 [9][10] では，トピックモデル解析手法を用いてこの未解決の突合処理の実現性を評価した．本論文では,「このアプローチを漸次，継続適用することで，リスク軽減に役立足せることができる」ことを示すために過去の脅威分析で作成したアタックツリーを次回以降の脅威分析に活用できることを事例をもとに示す.

2　脆弱性データベースを用いた脅威分析方法

我々は脆弱性データベースを使用した脅威分析方法の基本を提案した [6][7]．その全体構成を図 1 に示す．図 1 に示す通り，提案した脅威分析方法は，下記の 3 つの手順に従う.

- 脆弱性モデル情報を作成する (図 1 右側 3 つの角丸四角).
- ソフトウェアに組み込まれている下位のコンポーネント情報を作成する (図 1 左下の角丸四角).
- 分析対象システムの設計情報をもとに脅威分析を行う (図 1 中央の四角).

2.1　脆弱性モデル情報の作成

米国 MITRE 社は，いくつかの形式の脆弱性 DB を公開している [3][4][5]．しかし，これらの DB を参照しただけでは具体的な対象に対する（例えばコネクテッドカーに対する）*AT* を作成することは困難である．既存の攻撃事例の文献，あるいは報告書などを参考に *AT* を作成することになる．このように既存の脆弱性 DB と既存のアタック報告より得られる *AT* を第 1 の *AT* と呼ぶことにする．この第 1 の *AT* は，頂上事象と複数の中間事象，それに，最下位事象に階層化されて描かれる．第 1 の *AT* は，各脆弱性毎に 1 個作成する.

2.2　コンポーネント DB の提案

自動車や IoT 機器などの組み込み系では既存ソフトウェアをそのまま搭載するのではなく必要な下位コンポーネントを必要に応じで組み込むということが行われる．これに対して，CVE のような脆弱性 DB は，あるソフトウェアに対する脆弱性情報は記載しているものの，そのソフトウェアに組み込まれている下位コンポーネントの情報まで記載されていない．そこで，ソフトウェアのバージョンとそのソフトウェアが内部で使用している下位コンポーネントのバージョンの対応表を充実させることによって，IoT などの組み込み機器の製造段階で，脆弱性情報を容易に確認できるようにした.

2.3　脅威分析アルゴリズム

2.1 節で示した脆弱性モデル，2.2 節で示したコンポーネント DB，および分析対象システムの設計情報をもとにした脅威分析アルゴリズムを示す.

(1). 評価対象システムに関する頂上事象（起きては困る事故，安全に関する事故でもよい）をトップノードとする第 2 の *AT* を作成する．*AT* 作成に当たっては、基本的に従来の *FT* 作成と同様に演繹的かつ発見的手法を用いる [8]．この際に，コンポーネント DB に含まれているのと同じコンポーネントが評価対象システムにあれば，そのコンポーネントも第 2 の *AT* に含める．また，コンポーネント DB には含まれていない評価対象システムのコンポーネントついても考察し，コンポーネント DB に記載されている脆弱性と同様の脆弱性があると判断された場合には，そのコンポーネントも第 2 の *AT* に含める.（図 2(2) の黒丸のノード）. 第 2 の *AT* は，頂上事象と複数の中間事象，それに最下位事象に階層化されて描かれる．第 2 の *AT* は 1 個作成される（図 2(2)）.

(2). その後，各脆弱性毎に第 1 の *AT* と第 2 の *AT* を突合評価する（図 2(3)）．この突合評価には，自然言語処理と AI 処理[1]を用い，第 1 の *AT* に現れる頂上事象あるいは中間事象のうち，第 2 の *AT* に現れる中間事象にに同等か近いものがあるかどうかを判定する．もし，に同等か近いものがあれば，中間事象同士で論理和をとる（図 2(4)）.

(3). この論理和が取られたサブツリーに対して，第 1 の *AT* 側の最下位事象に，評価対象のコンポーネントがない中間事象に着目して再度分析を行い，追加すべきと判定されれば追加し，そうでなければその中間ノードを削除する．具体的には，第 2 の *AT* の構成コンポーネントに無関係（異なるコンポーネントやバージョンの違い）のノードを FALSE ノードとしたうえで，FALSE ノードの関係および FALSE ノードの直上の AND 関係の上位のノードの関係を削除する（図 2(5)）.

(4). このような処理を追加したすべての第 1 の *AT* について繰り返し，最終的に修正が終わったら，修正後の第 2 の *AT* を用いて，評価対象システムの頂上事象（起きては困る事故）の真の発生確率を

[1] この突合処理のトピックモデル分析による実現可能性を文献 [9][10] で示している.

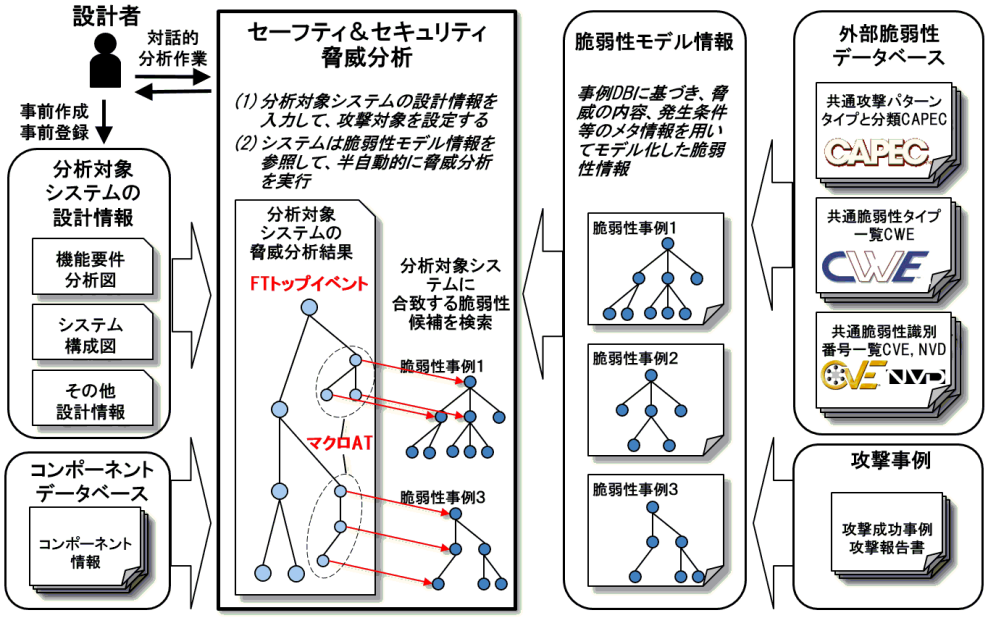

図 1: 提案手法の全体概要 ([6] より引用)

評価する．第 2 の *AT* は，今後の脅威分析における第 1 の *AT* として利用可能である．

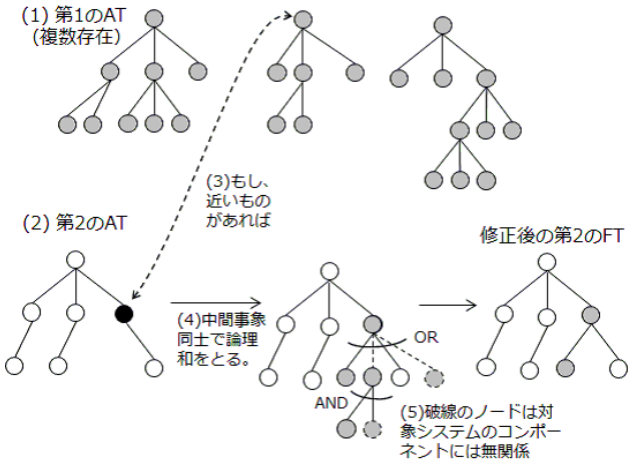

図 2: 脅威分析アルゴリズム ([6] より引用)

なお，文献 [7] では，この提案アルゴリズムの数式による定式化，攻撃確率の計算は，およびテスラの事例 [13] への適用について述べている．

3 トピックモデル解析による突合処理

3.1 潜在的ディリクレ配分法 (Latent Dirichlet Allocation)

文書には顕在的，あるいは，潜在的なトピックがあり，各キーワードはそのトピックから生成されているという考え方をトピックモデルという．トピックモデル解析では，キーワードから潜在的なトピックを推定する潜在的ディリクレ配分法（Latent Dirichlet Allocation（LDA））[14] がある．これは，トピックの確率分布（多項分布のパラメータ θ）がディレクレ分布に従うことを仮定した言語モデルである．トピックをディレクレ分布に従って選択し，そのトピックに対する単語の確率分布に従って単語を選択するというものである．国立研究開発法人産業技術総合研究所では，LDA を含むトピックモデル解析技術を用いたセキュリティ要件分析支援ツール (TACT) を開発している [15].

3.2 突合実験の概要

2.3 節で述べたように，「第 1 の *AT* と第 2 の *AT* の各ノードを突合する際に，自然言語処理と AI 処理を用いる」としている．この突合処理の有効性を検証する．

あるシステムの脆弱性に関する論文等で報告された攻撃手法と似た脆弱性を，別システムで突合することができれば，その後の対策に役立てることができる．また，論文中で具体的な CVE の番号を明記されていればどんな脆弱性が使われたかがわかるが，論文によっては手順が示されているだけで具体的な CVE の番号が明記されていない場合も多い．そのような場合でも単語の背景に隠されたトピックに着目するトピックモデル分析を行えば，CVE 番号が明記されていない自然言語で記述された攻撃手法から該当する CVE 番号を特定できると考えた．

本来の目的は，自然言語で記述されたアタックツリー *AT* のノードを突合することが目的であるが，*AT* 作成時のノードの文章の記述具合によって結果が左右されることが考えられるため，今回は，既存の論文の文章その

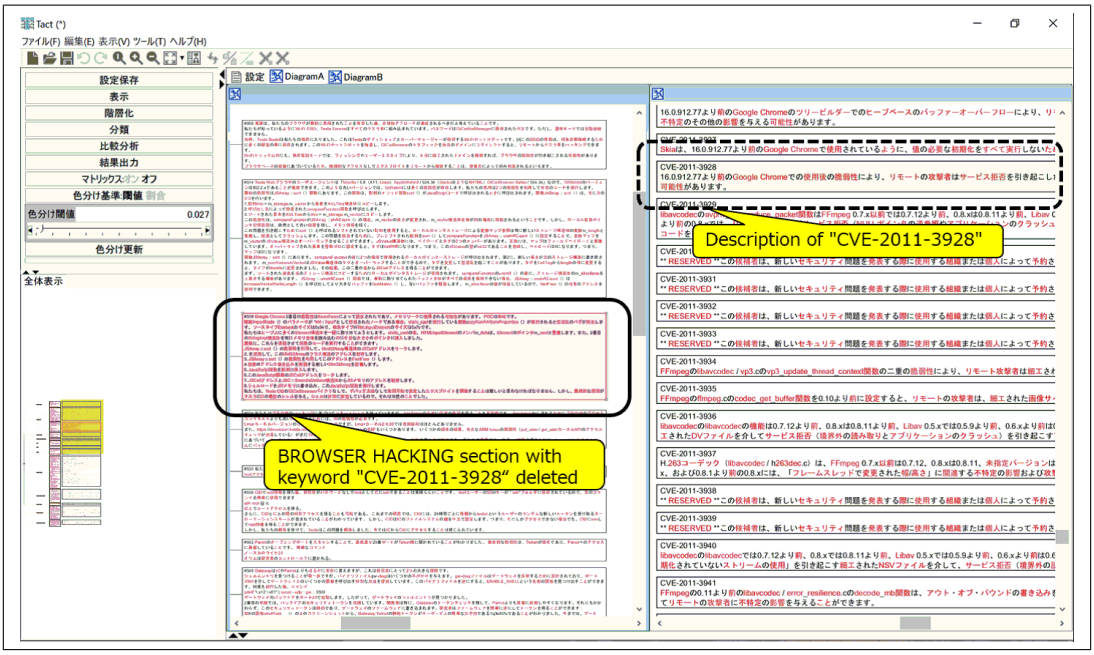

図 3: 攻撃事例と脆弱性データベースの突合 ([10] より引用)

ものを対象とした．具体的には，既知の攻撃手法としてテスラ社の自動車への攻撃の論文 [13] を対象とした．具体的な手順は以下のとおりである．

まず，論文 [13] を各節ごとに Google 翻訳 [16] にかけて日本語訳する[2]．ただし，BROWSER HACKING に関する節は長くかつ内容が 2 つの脆弱性に関する内容のため分割した．注目する脆弱性は，CVE-2011-3928 と CVE-2013-6282 である．CVE-2011-3928 は，BROWSER HACKING の節に，CVE-2013-6282 は LOCAL PRIVILEGE ESCALATION の節にそれぞれ記述されている．キーワードとして CVE-2011-3928 や CVE-2013-6282 が含まれていると，キーワードマッチングで検出される場合があると考えられるため，BROWSER HACKING の節と LOCAL PRIVILEGE ESCALATION の節から，CVE-2011-3928 と CVE-2013-6282 のキーワードは削除した．ただし，BROWSER HACKING の節に関しては，2.2 節で示したコンポーネントの包含関係の問題があり，WebKit の記述がされている文章に “Google Chrome” のキーワードを追加した．これは提案方式のコンポーネント DB を参照することに相当すると考えられる．今回利用したトピック分析ツールは扱う件数に上限があるため，全 CVE を対象とすることができなかったため，対象の脆弱性を含む前後の 500 件を対象とした．具体的には，CVE-2011-3928 を含む CVE2011-3501～4000 と，CVE-2013-6282 を含む CVE2013-6001～6500 を対象とした．論文のそれぞれの節と CVE の各脆弱性を対象として，トピックモデル分析で類似の文章を評価した．その際に，キーワードの抽出方法は「名詞とカナ」，特徴量の抽出方法は「LDA」，文章類似度「Cosine」というオプションを用いた．

3.3 突合実験の結果

論文のそれぞれの節と CVE の各脆弱性とをマッチングした結果を結果を図 3 に示す．このツールは左ペインの文章をクリックすると，それに類似した右ペインの文章が色付けされて表示されるものである．図 3 では見にくいが，左ペインの実線の箇所が “CVE-2011-3928” のキーワードを削除した BROWSER HACKING の節であり、この箇所をクリックすると，右ペインの CVE-2011-3928 の記述である破線の箇所が色付けされ，類似と判定される．今回の場合の画面上では，破線の箇所のみが色付けされ，その他の箇所は色付けされていない．上下にスクロールして確認すると，500 文章中，22 文章が色付けされた．つまり 500 件の中から適切な CVE を含む 22 件に絞り込めたということである．また，CVE-2013-6282 に関しても LOCAL PRIVILEGE ESCALATION の節と CVE をマッチングさせほぼ同様の結果が得られた．こちらも類似と判定された文章の割合は 23/500 であった．

4 事例適用

4.1 第 1 の *AT* の作成

まず，脆弱性 DB をもとに第 1 の *AT* を作成する．第 1 の *AT* は全ての脆弱性について作成することになる．

[2] Google 翻訳を活用する利点として，用語の表記ゆれを防ぐ効果もあると考えられる．

今回は，CVE-2011-3928 および CVE-2014-1635 についての第 1 の *AT* を作成する．それぞれ図 4 および図 5 に示す．

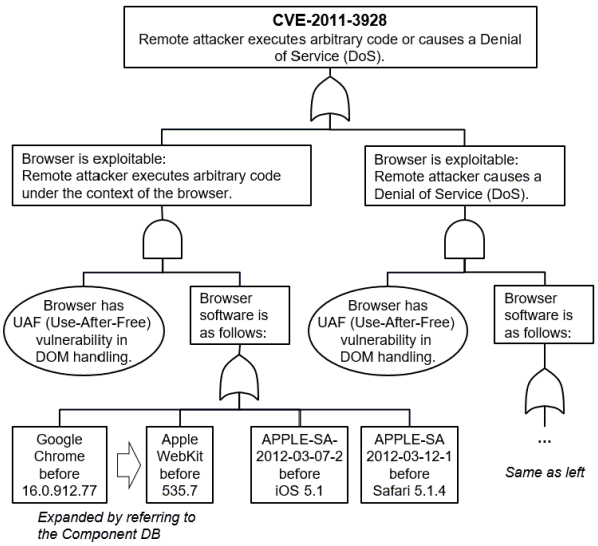

図 4: CVE-2011-3928 から生成した第 1 の *AT*([7] より引用)

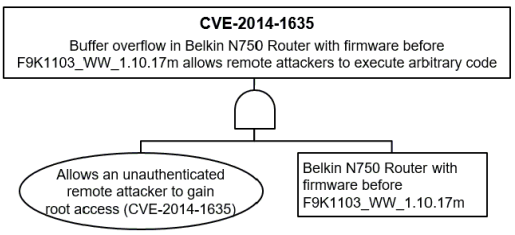

図 5: CVE-2014-1635 から生成した第 1 の *AT*

4.2 Jeep Cherokee の事例への適用

Jeep Cherokee の事例 [11] に関して，第 2 の *AT* を作成してみる．作成した第 2 の *AT* を図 6 に示す．図 6 の破線の部分は，図 5 に示した第 1 の AT との突合の結果，結合されたサブツリーである．また，一点鎖線の部分は，この第 2 の *AT* を次の分析（Tesla の事例）のための第 1 の *AT* として利用したときに突合され再利用される部分である．

4.3 IRB140 industrial robot の事例への適用

次に，IRB140 industrial robot の事例 [12] に関して，第 2 の *AT* を作成してみる．作成した第 2 の *AT* を図 7 に示す．この事例では，CVE は参照しておらず別の脆弱性 DB（ABB 社が提供するロボット向けの脆弱性 DB）を参照している．今回は省略するが，CVE に限らず様々な脆弱性 DB から第 1 の *AT* を生成しておくことが有効と考えられる．図の点線の部分は，この第 2 の *AT* を次の分析（Tesla の事例）のための第 1 の *AT* として利用したときに突合され再利用される部分である．なお今回は，手作業で突合チェックを行い，作業量の関係で網羅的なチェックはできなかった．今後，TACT による計算機処理により，IRB140 industrial robot と Tesla model S 間の網羅的な突合を行うことが課題として残っている．

4.4 Tesla model S の事例への適用

次に，Tesla model S の事例 [13] に関して，第 2 の *AT* を作成してみる．作成した第 2 の *AT* を図 8 に示す．図 8 の破線の部分は，図 4 に示した第 1 の AT との突合の結果，結合されたサブツリーである．また，一点鎖線の部分は，Jeep Cherokee の事例で生成された第 2 の *AT* を今回の脅威分析の第 1 の *AT* として用いた結果，結合されたサブツリーである．さらに，点線の部分は，IRB140 industrial robot の事例で生成された第 2 の *AT* を突合した結果，結合されたサブツリーである．Tesla の事例の実際に攻撃された脆弱性は，Wi-Fi に関しては，CID に SSID とパスワードがハードコーディングされていたためであり，また，GW へのユーザ認証のバイパスもファームウェアにパスワードがハードコーディングされていたためである．攻撃手法としては初歩的なものであるが，ここで重要なのは Jeep や Robot の事例から結合されたサブツリー内に実際の Tesla の攻撃手法が含まれていたということである．このように提案アルゴリズムで示した最終ステップの「第 2 の *AT* は，今後の脅威分析における第 1 の *AT* として利用可能である」の実現性が示された．

5 考察

3 つのケースにおいてすべて，アクセス手段の確保，アクセス権限の取得，システムのルート権限の取得の繰り返しで任意のコマンドを不正に送信できるようにしている点で共通している．ロボットと車の関係としては，IRB140 robot で攻撃の要因として発見された “Wi-Fi access point and Wi-Fi encryption is hacked” と “Bypass the User Authentication System” が，ある条件下で Tesla に適用し得ることが示されている．また，車同士の関係としては，ロボットに比べシステム構成が複雑であるが，Tesla の場合も Cherokee の場合も，上述の手順を繰り返し，Gateway まで到達し，Gateway のファームウェアを書換えて CAN にメッセージを転送処理できるようにした．

Cherokee の場合は，A850 チップが CAN へのメッセージを一元的につかさどる Gateway としての役割を果たすが，ネットワークで分離されているわけではない．しかし，Uconnect System へのアクセス手段の確保，アク

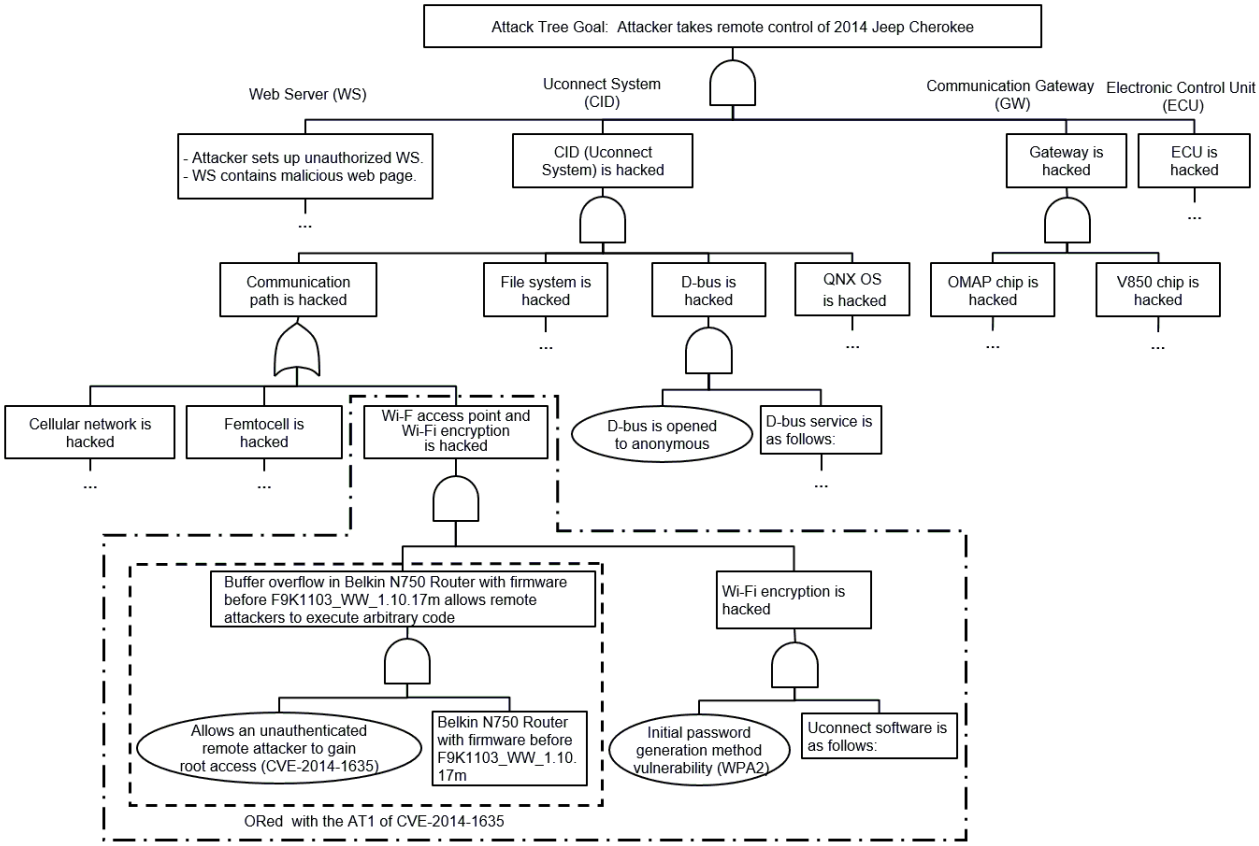

図 6: Jeep Cherokee の事例から生成した第 2 の *AT*

セス権限の取得，システムのルート権限の取得（実際には匿名実行が可能だった）を繰り返し，A850(Gateway) まで到達し，A850 のファームウェアを書換えて CAN にメッセージを転送処理できるようにした．

上記のように侵入の流れは同じで，最終的に Gateway の Firmware を書き換えて CAN にメッセージを届かせることも同じである．CAN へのメッセージをつかさどるチップの Firmware を書き換えられないようにすることで Tesla も Cherokee も攻撃を防げたことになると考えられる．

今回，トピックモデルという，文章を単語の集合として見て，異なる文章間の距離を，異なる「単語の集合」間の距離に置き換えて近さを計るという手法を用いた．トピックモデル分析はいわゆる AI 手法のひとつであり，ビッグデータを計算機で高速処理することが可能でありながら，人には何故そういう結果になったかという理解がし易い点が優れている．今回，新たに検討に加えた IRB140 industrial robot の攻撃論文は論文 48 ページ，プレゼン資料 82 ページという比較的分量の多い技術資料である．このような資料を人が手作業で分析を行うのはたいへんな作業量となる．さらに，今後検討すべき攻撃論文の数が増えることを考慮すると，攻撃論文をトピックモデルで計算機処理する本方法のような手法は意義が大きい．

6 まとめ

トピックモデル解析ツールを用いて，既知の攻撃事例と脆弱性データベースの突合の実現可能性を確認できた．また，過去の脅威分析で作成した第 2 のアタックツリーを次回以降の脅威分析における第 1 のアタックツリーとして活用し我々の提案方式を漸次継続適用することでリスク軽減に役立足せることができることを示した．

謝辞

本研究の一部は，総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました．

参考文献

[1] A. Ruddle et al., “Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios,” Seventh Research Framework Programme of the European Community, July 2008.

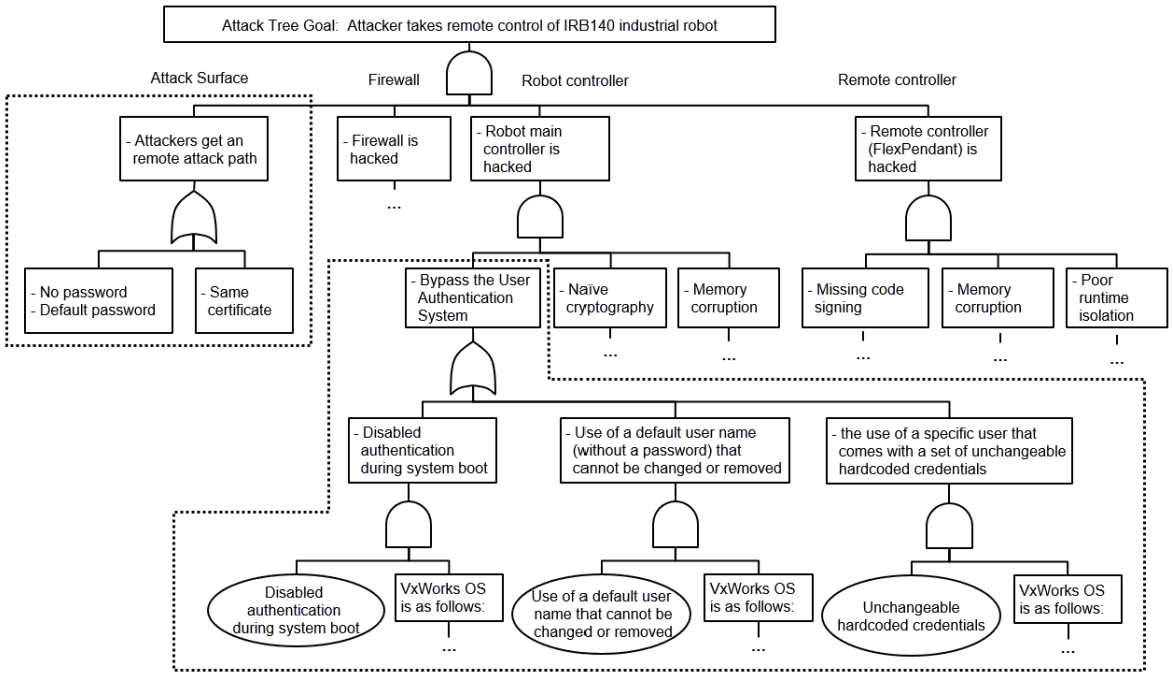

図 7: IRB140 industrial robot の事例から生成した第 2 の *AT*

[2] I. N. Fovino et al., “Integrating cyber attacks within fault trees,” Reliability Engineering and System Safety 94 (2009) p.p.1394–1402.

[3] MITRE Corporation, ”CVE - Common Vulnerability and Exposure,” https://cve.mitre.org/

[4] MITRE Corporation, “CWE List - Common Weakness Enumeration,” https://cwe.mitre.org/data/

[5] MITRE Corporation, ”CAPEC - Common Attack Pattern Enumeration and Classification,” https://capec.mitre.org/

[6] 梅澤克之，三科雄介，田口研治，寶木和夫，“脆弱性データベースを使用した脅威分析方法の提案,” 暗号と情報セキュリティシンポジウム (SCIS2018) 予稿集，1C2-6, Jan. 2018.

[7] Y. Mishina, K. Takaragi and K. Umezawa “A Proposal of Threat Analyses for Cyber-Physical System using Vulnerability Databases,” 2018 IEEE International Symposium on Technologies for Homeland Security (IEEE HST), 2018.

[8] 宝木和夫，“セキュリティ脅威分析,” 情報セキュリティ, 近代科学社, 2012, p.p.39-48.

[9] 梅澤克之，三科雄介，寶木和夫，S. Wohlgemuth，“脆弱性 DB を用いた脅威分析手法へのトピックモデル解析ツールの活用,” 2018 年電子情報通信学会基礎・境界ソサイエティ/NOLTA ソサイエティ大会予稿集，p.32, Sept. 2018.

[10] K. Umezawa, Y. Mishina, S. Wohlgemuth, and K. Takaragi, “Threat Analysis using Vulnerability Databases – Matching Attack Cases and Vulnerability Database by Topic Model Analysis –,” Proceeding of the Third International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2018), p.p. 74-77, Nov. 2018.

[11] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” Briefing, Black Hat USA 2015.

[12] D. Quarta, M. Pogliani, M. Polino, A.M. Zanchettin, and S. Zaner, “Rogue Robots: Testing the Limits of an Industrial Robot’s Security,” Briefing, Black Hat USA 2017, July 2017.

[13] S. Nie et al., “FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS,” Briefing, Black Hat USA 2017, July 2017.

[14] D. Blei, A. Ng, and M. Jordan, “Latent Dirichlet Allocation”, in Journal of Machine Learning Research, 2003, pp. 1107-1135.

[15] 半田剣一，大崎人士，竹内泉，“セキュリティ要件分析支援ツール TACT，” 情報処理学会ソフトウェア工学研究会　ウィンターワークショップ 2017・イン・飛騨高山予稿集，2017.

[16] Google 翻訳 https://translate.google.com/

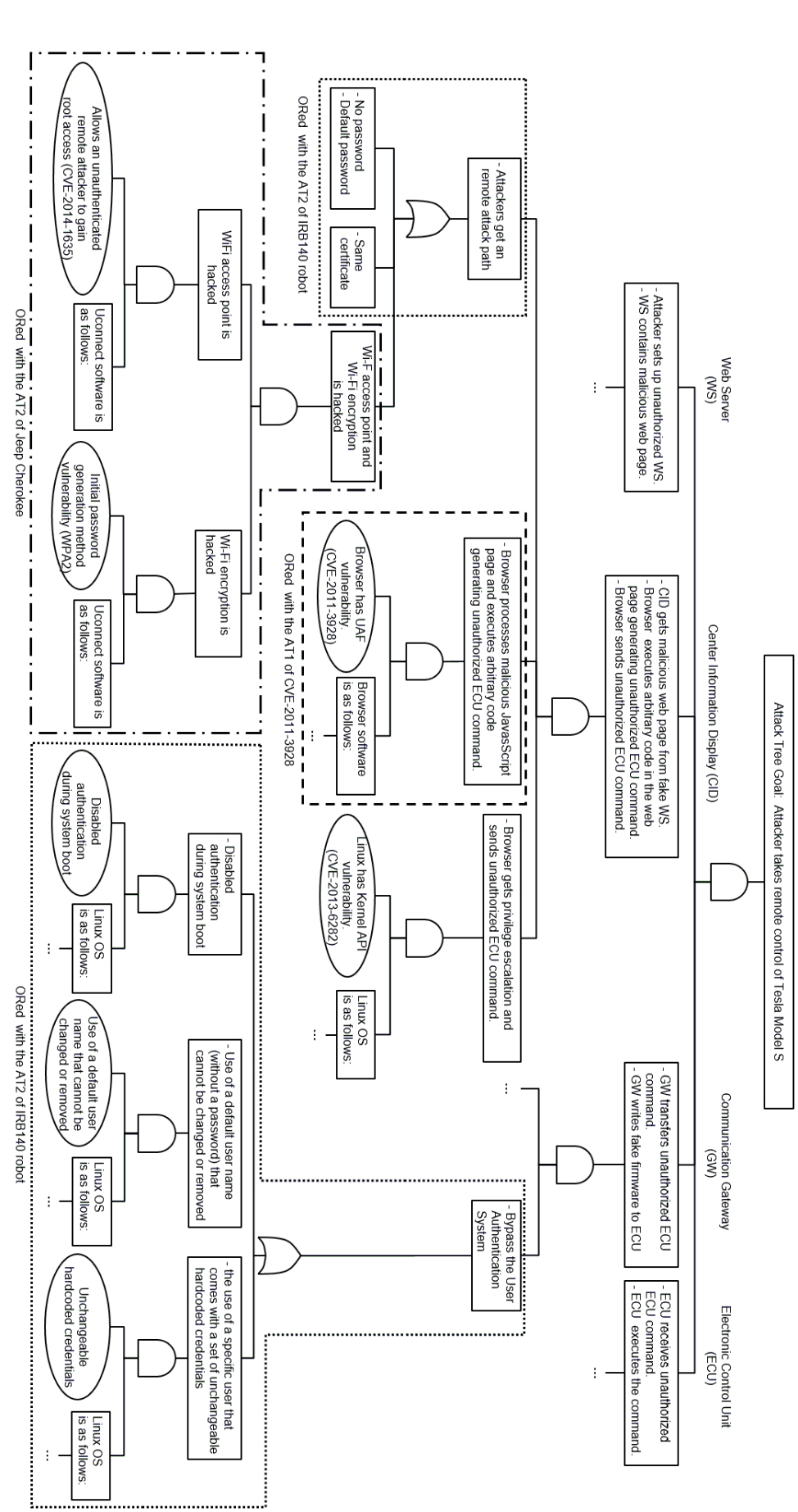

図 8: Tesla model S の事例から生成した第 2 の *AT*