

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02020/090077

発行日 令和3年2月15日(2021.2.15)

(43) 国際公開日 令和2年5月7日(2020.5.7)

(51) Int.Cl.

G06F 21/57 (2013.01)

F I

G06F 21/57 370

テーマコード(参考)

審査請求 有 予備審査請求 未請求 (全 31 頁)

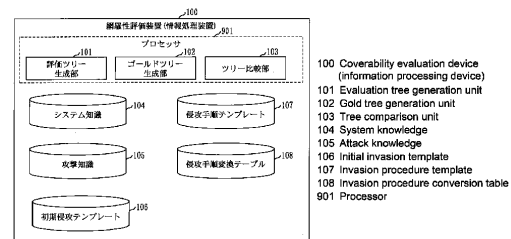
出願番号	特願2020-554703 (P2020-554703)	(71) 出願人	000006013
(21) 国際出願番号	PCT/JP2018/040641		三菱電機株式会社
(22) 国際出願日	平成30年11月1日(2018.11.1)		東京都千代田区丸の内二丁目7番3号
(81) 指定国・地域	AP (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA (AM, AZ, BY, KG, KZ, RU, TJ, TM), EP (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT	(74) 代理人	110002491 溝井国際特許業務法人
		(72) 発明者	山本 匠 日本国東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内
		(72) 発明者	島邊 遼佑 日本国東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内
		(72) 発明者	浅井 健志 日本国東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理方法及び情報処理プログラム

(57) 【要約】

評価ツリー生成部(101)が、述語論理を用いた推論に基づく、情報システムについてのアタックツリーを評価ツリーとして生成する。ゴールドツリー生成部(102)が、情報システムのネットワーク構成が示されるネットワーク構成情報と情報システムへの侵攻において想定される侵攻手順が示される侵攻手順情報とを用いて、情報システムへの侵攻経路が網羅され情報システムへの侵攻手順が反映されるゴールドツリーを生成する。ツリー比較部(103)は、評価ツリーとゴールドツリーとを比較する。



【特許請求の範囲】**【請求項 1】**

述語論理を用いた推論に基づく、情報システムについてのアタックツリーを第 1 のアタックツリーとして取得する第 1 のアタックツリー取得部と、

前記情報システムのネットワーク構成が示されるネットワーク構成情報と前記情報システムへの侵攻において想定される侵攻手順が示される侵攻手順情報とを用いて、前記情報システムへの侵攻経路が網羅され前記情報システムへの侵攻手順が反映されるアタックツリーを第 2 のアタックツリーとして生成する第 2 のアタックツリー生成部と、

前記第 1 のアタックツリーと前記第 2 のアタックツリーとを比較するツリー比較部とを有する情報処理装置。

10

【請求項 2】

前記第 1 のアタックツリー取得部は、

複数の攻撃ステップが含まれる攻撃パスが複数含まれるアタックツリーを前記第 1 のアタックツリーとして取得し、

前記第 2 のアタックツリー生成部は、

複数の攻撃ステップが含まれる攻撃パスが複数含まれるアタックツリーを前記第 2 のアタックツリーとして生成し、

前記ツリー比較部は、

前記第 2 のアタックツリーに含まれる特定の攻撃パスに含まれる複数の攻撃ステップが前記第 2 のアタックツリーと同じ順序で前記第 1 のアタックツリーに含まれていない場合に、前記特定の攻撃パスを出力する請求項 1 に記載の情報処理装置。

20

【請求項 3】

前記情報処理装置は、更に、

前記情報システムについての前記述語論理を用いた推論において推論に失敗した要素が含まれるアタックツリーを失敗ツリーとして取得する失敗ツリー取得部を有し、

前記ツリー比較部は、

前記第 2 のアタックツリーと、前記第 1 のアタックツリー及び前記失敗ツリーとを比較する請求項 1 に記載の情報処理装置。

【請求項 4】

前記第 1 のアタックツリー取得部は、

複数の攻撃ステップが含まれる攻撃パスが複数含まれるアタックツリーを前記第 1 のアタックツリーとして取得し、

前記第 2 のアタックツリー生成部は、

複数の攻撃ステップが含まれる攻撃パスが複数含まれるアタックツリーを前記第 2 のアタックツリーとして生成し、

前記失敗ツリー取得部は、

複数の攻撃ステップが含まれる攻撃パスが複数含まれるアタックツリーを前記失敗ツリーとして取得し、

前記ツリー比較部は、

前記第 2 のアタックツリーに含まれる特定の攻撃パスに含まれる複数の攻撃ステップが前記第 2 のアタックツリーと同じ順序で前記第 1 のアタックツリー及び前記失敗ツリーのいずれにも含まれていない場合に、前記特定の攻撃パスを出力する請求項 3 に記載の情報処理装置。

30

40

【請求項 5】

前記ツリー比較部は、

前記述語論理を用いた推論の前提に欠陥があることが推定される旨を通知するメッセージを出力する請求項 4 に記載の情報処理装置。

【請求項 6】

前記ツリー比較部は、

前記第 2 のアタックツリーに含まれる特定の攻撃パスに含まれる複数の攻撃ステップが

50

前記第2の攻撃ツリーと同じ順序で前記第1の攻撃ツリーには含まれていないが前記失敗ツリーには含まれている場合に、前記特定の攻撃パスを出力する請求項3に記載の情報処理装置。

【請求項7】

前記ツリー比較部は、

前記述語論理を用いた推論の前提に欠陥がないことが推定される旨を通知するメッセージを出力する請求項6に記載の情報処理装置。

【請求項8】

コンピュータが、述語論理を用いた推論に基づく、情報システムについての攻撃ツリーを第1の攻撃ツリーとして取得し、

前記コンピュータが、前記情報システムのネットワーク構成が示されるネットワーク構成情報と前記情報システムへの侵攻において想定される侵攻手順が示される侵攻手順情報とを用いて、前記情報システムへの侵攻経路が網羅され前記情報システムへの侵攻手順が反映される攻撃ツリーを第2の攻撃ツリーとして生成し、

前記コンピュータが、前記第1の攻撃ツリーと前記第2の攻撃ツリーとを比較する情報処理方法。

【請求項9】

述語論理を用いた推論に基づく、情報システムについての攻撃ツリーを第1の攻撃ツリーとして取得する第1の攻撃ツリー取得処理と、

前記情報システムのネットワーク構成が示されるネットワーク構成情報と前記情報システムへの侵攻において想定される侵攻手順が示される侵攻手順情報とを用いて、前記情報システムへの侵攻経路が網羅され前記情報システムへの侵攻手順が反映される攻撃ツリーを第2の攻撃ツリーとして生成する第2の攻撃ツリー生成処理と、

前記第1の攻撃ツリーと前記第2の攻撃ツリーとを比較するツリー比較処理とをコンピュータに実行させる情報処理プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、攻撃ツリーの評価に関する。

【背景技術】

【0002】

近年、機密情報又は個人情報の漏えい事件、ランサムウェアによる被害等により、情報資産を取り扱うエンタープライズにおけるセキュリティの重要性が増している。また、制御システムのネットワーク化に伴い、発電プラント、ガスプラント等の重要インフラストラクチャーへのサイバー攻撃が脅威となりつつある。これらサイバー攻撃は、国家の安全保障を揺るがす重大な懸念事項となっている。重要インフラストラクチャーに対する攻撃の代表事例としてイランの原子力発電施設で起きたStuxnetが挙げられる。本事例では、USBメモリ経由で制御システムを操作する内部ネットワークのマシンがマルウェアに感染し、さらに遠心分離装置を制御するプログラムが改ざんされ、同装置の不正動作により濃縮ウランの製造に影響が出たと言われている。遠心分離装置などはインターネットに接続されていなかった(air-gapped)が、攻撃経路の1つとして、内部のスタッフが利用するUSBメモリがあったことが報告されている。このことから、あらかじめ様々な脅威を想定してセキュリティを向上させる必要があることがわかる。

【0003】

セキュリティを向上させるためには、まず、攻撃目標に対する脅威とそのリスクを明確にするセキュリティ分析が重要である。セキュリティ分析では、攻撃目標に対する脅威をリストアップする。次に、発生頻度が高く重大な影響を持つ脅威に対して高いリスク値を割り当てる。そして、高いリスク値が割り当てられた脅威に優先的に適切な対策を実施していく。

脅威をリストアップする際に、リストアップ漏れがあっては意味が無い。そのため、ア

10

20

30

40

50

タックツリーなどのツールを用いて、攻撃目標への侵攻手順を系統的に抽出することが行われる。

従来、アタックツリーの作成は人の手で行われていた。そのため作成されたアタックツリーの質は、作成者の創造力、経験、スキルに依存していた。作成時にミスが混入する可能性もあり、作成されたアタックツリーの網羅性については常に疑問視されていた。

そこで、Prologなどの述語論理の推論エンジンを利用して、攻撃目標に対する侵攻手順を、与えられた前提知識をもとに推論し、推論過程からアタックツリーを自動生成する技術が考えられている（例えば、非特許文献1及び非特許文献2）。以降、このようなアタックツリーを自動生成する技術をアタックツリー自動生成技術と呼ぶ。アタックツリー自動生成技術によれば、アタックツリーの生成過程において人手を介さないため、アタックツリーの網羅性は人の創造性及び経験に依存しない。本技術では、事前に用意した前提知識と推論ルールをもとに、与えられた攻撃目標が成功するかを推論する。全ての組合せを試し、成功した推論過程のみをもとにアタックツリーを生成する。アタックツリーの作成に人の手を介さないため、作成者の能力やミスによる影響を受けにくい。

しかし、アタックツリー自動生成技術においても、推論エンジンに与える知識や推論ルールは人手で用意する必要がある。このため、アタックツリー自動生成技術を用いて生成されたアタックツリーについても網羅性の根拠を強く主張することができない。

また、非特許文献3の技術では、形式証明を利用してアタックツリーを評価する。アタックツリーはあるモデル（Transition system model）の中で生成される。アタックツリーの網羅性及び健全性は当該モデルの中で保証される。しかし、当該モデルは人が作成するため、経験及び知識の差異によるモデルのばらつきが発生し得る。また、モデルの作成に人為的ミスが入る可能性が高い。そのため、モデルの中で保証された網羅性や健全性には疑問が残る。

【先行技術文献】

【非特許文献】

【0004】

【非特許文献1】Xinming Ou, Sudhakar Govindavajhala, Andrew W. Appel, MulVAL: A Logic-based Network Security Analyzer, Proceeding SSYM '05 Proceedings of the 14th conference on USENIX Security Symposium-Volume 14

【非特許文献2】浅井健志、島邊遼佑、河内清人、サイバー攻撃対策の選定に向けたアタックツリーの自動生成、SCIS2018 暗号と情報セキュリティシンポジウム、1C1-1

【非特許文献3】Maxime Audinot, Sophie Pinchinat, Barbara Kordy, Is my attack tree correct? Extended version, CoRR abs/1706.08507 (2017)

【発明の概要】

【発明が解決しようとする課題】

【0005】

このように、従来の技術では、生成されたアタックツリーの網羅性に疑問が残るという課題がある。

本発明は、このような課題を解決することを主な目的とする。具体的には、本発明は、アタックツリーの網羅性を高めることを主な目的とする。

【課題を解決するための手段】

【0006】

本発明に係る情報処理装置は、

述語論理を用いた推論に基づく、情報システムについてのアタックツリーを第1のアタックツリーとして取得する第1のアタックツリー取得部と、

前記情報システムのネットワーク構成が示されるネットワーク構成情報と前記情報システムへの侵攻において想定される侵攻手順が示される侵攻手順情報とを用いて、前記情報システムへの侵攻経路が網羅され前記情報システムへの侵攻手順が反映されるアタックツリーを第2のアタックツリーとして生成する第2のアタックツリー生成部と、

前記第1のアタックツリーと前記第2のアタックツリーとを比較するツリー比較部とを有する。

【発明の効果】

【0007】

本発明では、第1のアタックツリーを、情報システムへの侵攻経路が網羅され情報システムへの侵攻手順が反映される第2のアタックツリーと比較するため、第1のアタックツリーの網羅性を評価することができる。このため、評価結果を第1のアタックツリーの生成手順にフィードバックすることが可能になり、第1のアタックツリーの網羅性を高めることができる。

10

【図面の簡単な説明】

【0008】

【図1】実施の形態1に係る網羅性評価装置のハードウェア構成例を示す図。

【図2】実施の形態1に係る網羅性評価装置の機能構成例を示す図。

【図3】実施の形態1に係る網羅性評価装置の動作例を示すフローチャート。

【図4】実施の形態1に係る攻撃知識の例を示す図。

【図5】実施の形態1に係るシステム知識の例を示す図。

20

【図6】実施の形態1に係る推論過程を表すツリーの例を示す図。

【図7】実施の形態1に係るアタックツリーの例を示す図。

【図8】実施の形態1に係るゴールドツリー生成部の内部構成例を示す図。

【図9】実施の形態1に係るゴールドツリー生成部の動作例を示すフローチャート。

【図10】実施の形態1に係る制御システムのネットワーク構成例を示す図。

【図11】実施の形態1に係る侵攻経路を網羅したツリーの例を示す図。

【図12】実施の形態1に係る初期侵攻テンプレートの例を示す図。

【図13】実施の形態1に係る初期侵攻テンプレートの例を示す図。

【図14】実施の形態1に係る侵攻手順テンプレートの例を示す図。

【図15】実施の形態1に係る侵攻手順テンプレートの例を示す図。

30

【図16】実施の形態1に係る初期侵攻テンプレート及び侵攻手順テンプレートの適用後のツリーの例を示す図。

【図17】実施の形態1に係る初期侵攻テンプレート及び侵攻手順テンプレートの適用後のツリーの例を示す図。

【図18】実施の形態1に係る初期侵攻テンプレート及び侵攻手順テンプレートの適用後のツリーの例を示す図。

【図19】実施の形態1に係るツリー比較部の内部構成例を示す図。

【図20】実施の形態1に係るツリー比較部の動作例を示すフローチャート。

【図21】実施の形態1に係る評価ツリーの例を示す図。

【図22】実施の形態1に係る評価ツリーの例を示す図。

40

【図23】実施の形態1に係る比較動作を実現する疑似コードを示す図。

【図24】実施の形態2に係るツリー比較部の内部構成例を示す図。

【図25】実施の形態2に係るツリー比較部の動作例を示すフローチャート。

【図26】実施の形態2に係る失敗ツリーの例を示す図。

【図27】実施の形態2に係る比較動作を実現する疑似コードを示す図。

【図28】実施の形態1に係るANDノードとORノードを含む評価ツリーの例を示す図。

。

【発明を実施するための形態】

【0009】

以下、本発明の実施の形態について、図を用いて説明する。以下の実施の形態の説明及

50

び図面において、同一の符号を付したものは、同一の部分又は相当する部分を示す。

【0010】

実施の形態 1.

構成の説明

図 1 は、本実施の形態に係る網羅性評価装置 100 のハードウェア構成例を示す。

網羅性評価装置 100 は、情報処理装置に相当する。また、網羅性評価装置 100 により行われる動作は、情報処理方法及び情報処理プログラムに相当する。

【0011】

本実施の形態に係る網羅性評価装置 100 は、コンピュータである。

網羅性評価装置 100 は、ハードウェアとして、プロセッサ 901、主記憶装置 902、補助記憶装置 903、通信デバイス 904、キーボード 905、マウス 906 及びディスプレイ 907 を備える。

補助記憶装置 903 には、図 2 を用いて後述する評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 の機能を実現するプログラムが記憶されている。当該プログラムは、補助記憶装置 903 から主記憶装置 902 にロードされる。そして、プロセッサ 901 が当該プログラムを実行して、後述する評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 の動作を行う。

主記憶装置 902 又は補助記憶装置 903 には、評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 に用いられるデータが格納される。また、主記憶装置 902 又は補助記憶装置 903 には、評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 の処理結果を示すデータが格納される。

通信デバイス 904 は、例えば LAN (Local Area Network) を介してインターネットに接続されている。

キーボード 905 及びマウス 906 は、網羅性評価装置 100 のユーザが網羅性評価装置 100 に各種指示を入力するのに用いられる。

ディスプレイ 907 は、網羅性評価装置 100 のユーザに各種情報を表示するのに用いられる。

【0012】

図 2 は、本実施の形態に係る網羅性評価装置 100 の機能構成例を示す。

【0013】

網羅性評価装置 100 は、評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 を有する。

前述したように、評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 は、例えばプログラムで実現される。そして、当該プログラムはプロセッサ 901 で実行される。

図 2 では、プロセッサ 901 が評価ツリー生成部 101、ゴールドツリー生成部 102 及びツリー比較部 103 の機能を実現するプログラムを実行している状態を模式的に表している。

【0014】

評価ツリー生成部 101 は、Prolog などの述語論理を用いた推論に基づき、攻撃対象の情報システムについてのアタックツリーを生成する。評価ツリー生成部 101 が生成するアタックツリーを評価ツリーという。評価ツリー生成部 101 は、例えば、非特許文献 1 又は非特許文献 2 の技術を用いて評価ツリーを生成する。評価ツリーには、複数の攻撃ステップが含まれる攻撃パス（以下、単にパスともいう）が複数含まれる。

なお、評価ツリーは第 1 のアタックツリーに相当する。このため、評価ツリー生成部 101 は第 1 のアタックツリー取得部に相当する。また、評価ツリー生成部 101 により行われる処理は、第 1 のアタックツリー取得処理に相当する。

【0015】

ゴールドツリー生成部 102 は、攻撃対象の情報システムへの侵攻経路が網羅され当該情報システムへの侵攻手順が反映されるアタックツリーを生成する。ゴールドツリー生成

10

20

30

40

50

部 1 0 2 が生成するアタックツリーをゴールドツリーという。ゴールドツリーには、評価ツリー同様、複数の攻撃ステップが含まれる攻撃パスが複数含まれる。

ゴールドツリーは第 2 のアタックツリーに相当する。このため、ゴールドツリー生成部 1 0 2 は第 2 のアタックツリー生成部に相当する。また、ゴールドツリー生成部 1 0 2 により行われる処理は、第 2 のアタックツリー生成処理に相当する。

【0016】

ツリー比較部 1 0 3 は、評価ツリーとゴールドツリーとを比較する。ツリー比較部 1 0 3 は、ゴールドツリーに含まれる特定の攻撃パスに含まれる複数の攻撃ステップがゴールドツリーと同じ順序で評価ツリーに含まれていない場合に、当該特定の攻撃パスをディスプレイ 9 0 7 に出力する。

10

ツリー比較部 1 0 3 により行われる処理はツリー比較処理に相当する。

【0017】

また、評価ツリー生成部 1 0 1 及びゴールドツリー生成部 1 0 2 がアタックツリーの生成に用いるデータとして、システム知識 1 0 4、攻撃知識 1 0 5、初期侵攻テンプレート 1 0 6、侵攻手順テンプレート 1 0 7 及び侵攻手順変換テーブル 1 0 8 がある。

システム知識 1 0 4、攻撃知識 1 0 5、初期侵攻テンプレート 1 0 6、侵攻手順テンプレート 1 0 7 及び侵攻手順変換テーブル 1 0 8 は、主記憶装置 9 0 2 又は補助記憶装置 9 0 3 に格納されている。プロセッサ 9 0 1 が評価ツリー生成部 1 0 1 及びゴールドツリー生成部 1 0 2 として動作する際に、プロセッサ 9 0 1 は、システム知識 1 0 4、攻撃知識 1 0 5、初期侵攻テンプレート 1 0 6、侵攻手順テンプレート 1 0 7 及び侵攻手順変換テーブル 1 0 8 を読み出す。

20

システム知識 1 0 4、攻撃知識 1 0 5、初期侵攻テンプレート 1 0 6、侵攻手順テンプレート 1 0 7 及び侵攻手順変換テーブル 1 0 8 の詳細は、後述する。

【0018】

図 3 は、本実施の形態に係る網羅性評価装置 1 0 0 の動作例を示す。

図 3 を参照して、本実施の形態に係る網羅性評価装置 1 0 0 の動作例を説明する。

【0019】

ステップ S 1 0 1 において、評価ツリー生成部 1 0 1 は、評価ツリーを生成する。

評価ツリー生成部 1 0 1 は、P r o l o g などの述語論理を用いた推論ベースで評価ツリーを生成する。前述したように、評価ツリー生成部 1 0 1 は、例えば、非特許文献 1 又は非特許文献 2 の技術を用いて評価ツリーを生成する。

30

推論ベースのアタックツリー生成技術からは、推論過程がログとして出力される。P r o l o g では、与えられた命題（攻撃目標）が成立するか否かを再帰手続きによって探索する後ろ向き推論が行われる。推論過程のログとは、後ろ向き推論の中で、成功したルール、失敗したルールを記述したログである。

網羅性評価装置 1 0 0 には、攻撃対象の情報システムを表現した知識（ネットワーク構成、脆弱性のある箇所、攻撃者の前提条件）、推論ルールが予め用意されている。

具体的には、攻撃対象の情報システムを表現した知識として、図 2 に示すシステム知識 1 0 4 が網羅性評価装置 1 0 0 に用意されている。

システム知識 1 0 4 内の攻撃対象の情報システムのネットワーク構成についての知識には、情報システムのネットワーク構成が示されている。このため、当該知識は、ネットワーク構成情報に相当する。

40

また、推論ルールとして、図 2 に示す攻撃知識 1 0 5、初期侵攻テンプレート 1 0 6 及び侵攻手順テンプレート 1 0 7 が網羅性評価装置 1 0 0 に用意されている。

また、初期侵攻テンプレート 1 0 6 及び侵攻手順テンプレート 1 0 7 には、攻撃における侵攻手順が示されている。このため、初期侵攻テンプレート 1 0 6 及び侵攻手順テンプレート 1 0 7 は、侵攻手順情報に相当する。

評価ツリー生成部 1 0 1 に攻撃目標が入力されると、評価ツリー生成部 1 0 1 は、前述の知識、推論ルールを利用して、後ろ向き推論により攻撃目標が成立する全てのケース（攻撃パス）を導出する。そして、評価ツリー生成部 1 0 1 は、全ての攻撃パスをつなげる

50

ことで評価ツリーを生成する。

【0020】

図4と図5を参照して、アタックツリーの生成に必要な知識とルールを説明する。

図4は、攻撃知識105の例を示す。図5は、システム知識104の例を示す。

図4及び図5は、Prologの表記方法に従って表記されているが、表記方法は図4及び図5に示す方法に限らない。

攻撃知識105とシステム知識104を評価ツリー生成部101に入力し、例えば、「manipulateProg(a, c) (攻撃者aはマシンcのプログラムを書き換えることができる)」という質問をした場合、Prologの推論過程は図6のようなツリーで表現することができる。図6では、推論失敗の過程の記載は、ボディ部に書かれたゴールが初めて失敗する段階で止めている。

10

「manipulateProg(a, c)」が真となる（成立する）場合は、再帰手続きによって探索する後ろ向き推論が行われる。図6のツリーから推論が成功したパスのみを選び出すと図7のツリーが得られる。このような手順を経て評価ツリーが生成される。

図7のツリーの場合、2つの攻撃パスが推論されている。1つ目のパスは、図7の左下のノードから延びるパスである。つまり、1つ目のパスは、「攻撃者aがパスワードp1を盗み」(stealPass(a, p1)=True)、「攻撃者aがマシンm1のパスワードp1を持ち」(hasPass(a, p1)=True pass(m1, p1)=True)、「マシンm1とマシンcのネットワークアドレスが同じで、攻撃者aは物理的にマシンm1をコントロールすることができ」(network(m1, net1)=True network(c, net1)=True physicallyControllable(a, m1)=True)、「マシンm1からマシンcに物理的にアクセスでき、マシンm1に遠隔操作ツールがあり、マシンm1は攻撃者がコントロールすることができ」(accessible(m1, c)=True hasRemoteTool(m1)=True controllable(a, m1)=True)、「攻撃者aが遠隔にあるマシンm1からマシンcをコントロールでき」(remoteControllable(a, M, c)=True (M=m1))、「攻撃者aがマシンcをコントロールでき」(controllable(a, c)=True)、「攻撃者aはマシンcのプログラムを書き換えることができる」(manipulateProg(a, c)=True)である。

20

30

2つ目のパスは、図7の右下のノードから延びるパスである。つまり、2つ目のパスは、「攻撃者aがパスワードp3を盗み」(stealPass(a, p3)=True)、「攻撃者aがマシンcのパスワードp3を持ち」(hasPass(a, p3)=True pass(c, p3)=True)、「攻撃者aは物理的にマシンcをコントロールすることができ」(physicallyControllable(a, c)=True)、「攻撃者aはマシンcをコントロールすることができ」(controllable(a, c)=True)、「攻撃者aはマシンcのプログラムを書き換えることができる」(manipulateProg(a, c)=True)である。

【0021】

40

次に、ステップS102において、ゴールドツリー生成部102がゴールドツリーを生成する。

より具体的には、ゴールドツリー生成部102は、システム知識104から、総当たり的にネットワークの侵入経路をリストアップする。そして、ゴールドツリー生成部102は、初期侵攻テンプレート106と侵攻手順テンプレート107とを利用して、情報システムへの侵攻経路が網羅され、情報システムへの侵攻手順が反映されるゴールドツリーを生成する。

【0022】

最後に、ステップS103において、ツリー比較部103が、評価ツリーとゴールドツリーを比較し、差分を抽出する。

50

【0023】

図8は、ゴールドツリー生成部102の内部構成例を示す。

図8に示すように、ゴールドツリー生成部102は、ネットワーク網羅部1021及びテンプレート適用部1022から構成されている。また、ゴールドツリー生成部102は、システム知識104、初期侵攻テンプレート106及び侵攻手順テンプレート107を用いて、ゴールドツリーを生成する。

【0024】

図9は、ゴールドツリー生成部102の動作例を示す。

【0025】

まず、ステップS1021において、ネットワーク網羅部1021は、システム知識104から、攻撃対象の情報システムの情報（ネットワーク構成、脆弱性のある箇所、攻撃者の前提条件）を抽出する。システム知識104は、評価ツリー生成部101が推論ベースで攻撃パスを導出するために、例えばXML形式などの機械的に読み取り可能な形式で構成されている。ネットワーク網羅部1021は、攻撃対象の情報システムに存在する全てのマシンについての情報を抽出する。

【0026】

次に、ステップS1022において、ネットワーク網羅部1021は、情報システム内のあるマシンを攻撃対象としたときに取り得る、当該マシンまでの重複を含まない全ての侵攻経路を列挙する。システム知識104には情報システムのネットワーク構成の情報が含まれる。ネットワーク網羅部1021は、情報システムのネットワーク構成を用いて、論理的及び物理的に矛盾のない侵攻経路を抽出することができる。

【0027】

図10は、情報システムのネットワーク構成の一例として、簡略化した制御システムのネットワーク構成を示す。

図10の制御システムでは、制御機器を制御するコントローラCが制御ネットワークと保守ネットワークに接続されている。コントローラCを保守する保守計算機Bが保守ネットワークに接続されている。コントローラC及び制御ネットワークを監視する表示用の表示計算機Aが制御ネットワークに接続されている。以下、表示計算機A、保守計算機B及びコントローラCをそれぞれ単に、A、B、Cとも表記する。

図10の例では、「A、B、C」がマシンリストである。攻撃対象のマシンをコントローラCとした場合、ネットワーク構成を考慮しない、コントローラCまでの重複を含まない取り得る全ての侵攻経路は、「C、CB、CBA、CA、CAB」となる。理論的な経路の数は「 $1 + {}_2P_1 + {}_2P_2$ 」である（Pは順列を意味する）。上記「C、CB、CBA、CA、CAB」のうち、単体の「C」は、攻撃者がコントローラCを直接操作して攻撃することを意味する。「CB」は、攻撃者が保守計算機Bを直接操作しコントローラCに侵攻しコントローラCを攻撃することを意味する。「CBA」は、攻撃者が表示計算機Aを直接操作し保守計算機Bに侵攻しさらにコントローラCに侵攻しコントローラCを攻撃することを意味する。「CA」及び「CAB」についても同様である。

ネットワーク構成を考慮し、論理的及び物理的に明らかに矛盾のある経路を除去すると、侵攻経路の組合せは「C、CB、CA」となる。

【0028】

次に、ステップS1023において、ネットワーク網羅部1021が、抽出した侵攻経路をまとめ、侵攻経路を網羅したツリーを生成する。

図10の制御システムの場合、ネットワーク構成を考慮した侵攻経路を網羅したツリーは図11に示すようになる。本実施の形態では、各ノードの階層上の位置づけにかかわらず（各ノードが末端ノードであるか中間ノードであるかにかかわらず）、攻撃者が各ノードを直接操作して親ノードに侵攻すること想定する。なお、図11では、便宜上、表示計算機Aの下には、エンタープライズネットワークのノードを配置している。

【0029】

次に、ステップS1024において、テンプレート適用部1022が、初期侵攻テンプレ

10

20

30

40

50

レート106及び侵攻手順テンプレート107を利用し、侵攻手順を反映させたツリーを生成する。

図12は、初期侵攻テンプレート106の例を示す。初期侵攻では、盗んだパスワードによるログイン、USBメモリ経由のマルウェア感染等の手順が考えられる。具体的な手順が記された初期侵攻テンプレート106の例を図13に示す。

図14は、侵攻手順テンプレート107の例を示す。侵攻手順テンプレート107は、マシンタイプごとに侵攻手順が列挙されたテーブルである。バッファオーバーフローによる任意のプログラムの実行、盗んだパスワードによるリモートデスクトップ接続等の手順が侵攻の手順である。2つのマシンの間に複数のネットワークが存在する場合は、マシンタイプに加え、ネットワークタイプごとに侵攻手順テンプレート107に侵攻手順を列挙してもよい。具体的な手順が記された侵攻手順テンプレート107の例を図15に示す。

侵攻手順テンプレート107及び初期侵攻テンプレート106に記載する手順は、参考文献1、参考文献2等の形式化された公開データベースから抽出して利用することができる。

図11のツリーに図13の初期侵攻テンプレート106及び図15の侵攻手順テンプレート107を適用した後のツリーを図16に示す。

また、図17に具体的な手順が記されたツリーを示す。また、図18は、図17の記載をマシンリーダブルな記載に変更したツリーの例を示す。図18では、「表示計算機A」は「Machine A」と表記し、「保守計算機B」は「Machine B」と表記している。

なお、図18が、ゴールドツリーに該当する。

参考文献1：MITER、ATT&CK、https://attack.mitre.org/wiki/Main_Page

参考文献2：CAPEC、<http://capec.mitre.org/index.html>

【0030】

なお、制御システム内の全てのノードを攻撃対象に指定し、ノードごとにゴールドツリーを生成することもできるが、非効率のため、本実施の形態では、ゴールドツリー生成部102は、評価ツリーのトップにあるノードに記載されているマシンのみを攻撃対象に指定してゴールドツリーを生成する。

侵攻手順テンプレート107及び初期侵攻テンプレート106は、全てのマシンに共通に用いられてもよい。また、侵攻手順テンプレート107及び初期侵攻テンプレート106は、通常のPC(Personal Computer)、サーバ、コントローラなどマシンのタイプごとに用意してもよい。更に、侵攻手順テンプレート107及び初期侵攻テンプレート106を、マシンにインストールされているOS(Operating System)又はアプリケーションプログラムのバージョンごとに用意してもよい。

【0031】

図19は、ツリー比較部103の内部構成例を示す。

図19に示すように、ツリー比較部103は、パス抽出部1031及びパス比較部1032で構成される。また、ツリー比較部103は、侵攻手順変換テーブル108を参照する。

【0032】

図20は、ツリー比較部103の動作例を示す。

まず、ステップS1031において、パス抽出部1031は、ゴールドツリーからパスを抽出する。パス抽出部1031は、ゴールドツリーのリーフノードからルートノードまで親ノードをたどることでパスを抽出する。図18のゴールドツリーからは、以下の10個のパスが抽出される。なお、以下では、図18の一部の表記が省略されている。

1) remoteLogin(__, machineA, passwordA)⇒manipulateProgram(machineA, controllerC, tool)

2) remoteExploit(__, machineA, vul1)⇒manipul

```

ateProgram(machineA, controllerC, tool)
3) remoteExploit(__, machineA, Vul2) ⇒ manipulateProgram(machineA, controllerC, tool)
4) localControl(__, machineA, passwordA) ⇒ manipulateProgram(machineA, controllerC, tool)
5) usbMalwareRun(__, machineA, __) ⇒ manipulateProgram(machineA, controllerC, tool)
6) maliciousEmailClick(__, machineA) ⇒ manipulateProgram(machineA, controllerC, tool)
7) usbMalwareRun(__, machineB) ⇒ manipulateProgram(machineB, controllerC, tool)
8) localControl(__, machineB, passwordB) ⇒ manipulateProgram(machineB, controllerC, tool)
9) changeProgram(__, controllerC, usb)
10) localControl(__, controllerC, passwordC)

```

10

【0033】

次に、ステップS1032において、パス抽出部1031は、評価ツリーからパスを抽出する。パス抽出部1031は、評価ツリーのリーフノードからルートノードまで親ノードをたどることでパスを抽出する。なお、本実施の形態に係る評価ツリーはORノードのみで構成されているが、評価ツリーにANDノードが含まれることがありうる。この場合は、パス抽出部1031はANDノードに繋がる子ノード（ANDの条件）については、全ての組合せの順番のパスを抽出する。例えば、図28の例においては、以下6個のパスが抽出される。パス抽出部1031は、各ノードから末端ノードに向かうパスを再帰的に求め、親ノードとの関係（ORなのかANDなのか）に応じて、親ノードとのパスの連結の仕方を変える要領で、全パスを抽出していく。

20

- 1) $A \rightarrow B \rightarrow D \rightarrow C$
- 2) $A \rightarrow B \rightarrow E \rightarrow F \rightarrow G \rightarrow C$
- 3) $A \rightarrow B \rightarrow E \rightarrow G \rightarrow F \rightarrow C$
- 4) $A \rightarrow C \rightarrow B \rightarrow D$
- 5) $A \rightarrow C \rightarrow B \rightarrow E \rightarrow F \rightarrow G$
- 6) $A \rightarrow C \rightarrow B \rightarrow E \rightarrow G \rightarrow F$

30

図10の制御システムに対して、評価ツリー生成部101により図21に示す評価ツリーが生成されたとする。ゴールドツリーとの比較を容易にするために、図21の記載を図18の記載形式に変更したツリーを図22に示す。図22の評価ツリーからは、以下の7つのパスが抽出される。なお、以下では、図22の一部の表記が省略されている。また、攻撃が成功するための細かな条件やルールについても記載を省略している。

```

A) remoteExploit(__, machineA, vul1) ⇒ remoteControl(__, machineA, __) ⇒ manipulateProgram(machineA, controllerC, Tool) ⇒ manipulateProgram(__, controllerC, __)
B) remoteLogin(__, machineA, passwordA) ⇒ remoteControl(__, machineA, __) ⇒ manipulateProgram(machineA, controllerC, tool) ⇒ manipulateProgram(__, controllerC, __)
C) usbMalwareRun(__, machineA, __) ⇒ malwareInfection(__, machineA, __) ⇒ remoteControl(__, mac

```

40

50

h i n e A, _) ⇒ c o n t r o l (_, m a c h i n e A, _) ⇒ m a n i p u l a t e P r o g r a m (m a c h i n e A, c o n t r o l l e r C, t o o l) ⇒ m a n i p u l a t e P r o g r a m (_, c o n t r o l l e r C, _)

D) m a l i c i o u s E m a i l C l i c k (_, m a c h i n e A, _) ⇒ m a l w a r e I n f e c t i o n (_, m a c h i n e A, _) ⇒ r e m o t e C o n t r o l (_, m a c h i n e A, _) ⇒ c o n t r o l (_, m a c h i n e A, _) ⇒ m a n i p u l a t e P r o g r a m (m a c h i n e A, c o n t r o l l e r C, t o o l) ⇒ m a n i p u l a t e P r o g r a m (_, c o n t r o l l e r C, _)

E) l o c a l C o n t r o l (_, m a c h i n e B, p a s s w o r d B) ⇒ c o n t r o l (_, m a c h i n e B, _) ⇒ m a n i p u l a t e P r o g r a m (m a c h i n e B, c o n t r o l l e r C, t o o l) ⇒ m a n i p u l a t e P r o g r a m (_, c o n t r o l l e r C, _)

F) u s b M a l w a r e R u n (_, m a c h i n e B, _) ⇒ m a l w a r e I n f e c t i o n (_, m a c h i n e B, _) ⇒ c o n t r o l (_, m a c h i n e B, _) ⇒ m a n i p u l a t e P r o g r a m (m a c h i n e B, c o n t r o l l e r C, t o o l) ⇒ m a n i p u l a t e P r o g r a m (_, c o n t r o l l e r C, _)

G) c h a n g e P r o g r a m (_, c o n t r o l l e r C, u s b) ⇒ m a n i p u l a t e P r o g r a m (_, c o n t r o l l e r C, _)

【0034】

ステップS1033において、パス比較部1032が、ゴールドツリーと評価ツリーのそれぞれから抽出したパスを比較する。そして、パス比較部1032は、ゴールドツリーのパス中にある攻撃ステップを必ず含むパスを評価ツリーから抽出する。

説明のために、ゴールドツリーから抽出される攻撃パスの攻撃ステップをgStep（メンバーはa, n f, n t, i, s）と表す。攻撃ステップgStepは、主体gStep.sが、侵攻手順gStep.aを利用し、補足情報gStep.iを使って、攻撃元ノードgStep.nfから攻撃先ノードgStep.ntを攻撃することを意味する。

m a l E m a i l C l i c k (m 1, x, ,) の場合は、gStep.aがm a l E m a i l C l i c kである。gStep.nfはxである。gStep.ntはm 1である。gStep.iは「 」(ドントケア)である。gStep.sは「 」(ドントケア)である。

同様に、評価ツリーから抽出される攻撃パスの攻撃ステップをaStep（メンバーはa, n f, n t, i, 侵攻手順s）と表す。攻撃ステップaStepは、主体aStep.sが、侵攻手順aStep.aを利用し、補足情報aStep.iを使って、攻撃元ノードaStep.nfから攻撃先ノードaStep.ntを攻撃することを意味する。

r e m E x p (a, x, m 1, v u l l) の場合は、aStep.aがr e m E x pである。aStep.sはaである。vStep.nfはxである。aStep.ntはm 1である。aStep.iはv u l lである。

「a c c e s s (x, m 1, , _), c l i c k M a l E m a i l l (a, x, m 1, _), c o n t r o l (a, x, _, _)」のように1つの攻撃ステップの中に複数の侵攻手順（もしくは条件）が含まれている場合がある。このような攻撃ステップは、要素の数に関係なく、侵攻手順の集合として扱う。

ゴールドツリーから抽出した各攻撃パスは攻撃ステップ（侵攻手順）が要素となる順序リストである。評価ツリーから抽出した各攻撃パスは攻撃ステップ（侵攻手順の集合）が要素となる順序リストである。パス比較部1032は、以下のように、ゴールドツリーの攻撃パスと評価ツリーの攻撃パスとを比較する。

【0035】

パス比較部1032は、ゴールドツリーから抽出した攻撃パスを1つずつピックアップし、さらに評価ツリーから抽出した攻撃パスを1つずつピックアップする。

次に、パス比較部1032は、ゴールドツリーの攻撃パスに含まれるすべての要素（侵

10

20

30

40

50

攻手順)を順序通り含む攻撃パスを評価ツリーから探す。評価ツリーの攻撃パスの各要素は侵攻手順の集合で表現されている。このため、パス比較部1032は、ゴールドツリーの攻撃ステップの侵攻手順が評価ツリーの侵攻手順の集合に含まれるか否かを判定する。

【0036】

ゴールドツリーと評価ツリーに利用されている侵攻手順(侵入手口および侵攻手口)の形式が異なる場合(例えば、malEmailClick(x, m1)とclickMalEmail1(a, x, m1))のために、侵攻手順間の対応関係が得られるように侵攻手順変換テーブル108が用意されている。

それぞれの侵攻手口には、あらかじめCAPECやATT&CKなどの攻撃手口の識別子を紐づけておく。

侵攻手順変換テーブル108には、対応する攻撃手口名、主体、補足情報、攻撃元ノード、攻撃先ノードに加え、対応する識別子(CAPECまたはATT&CK)が記載される。

パス比較部1032がゴールドツリーの攻撃パスと評価ツリーの攻撃パスとを比較することで、ゴールドツリーの攻撃パスに対応する評価ツリーの攻撃パスが辞書形式で出力される。このようなパス比較部1032の比較動作をmatchedAttackPathDictという。

【0037】

図23に、パス比較部1032の比較動作を実現する疑似コード(compareAttackPaths)を示す。

matchedAttackPathDictにおいて空集合(ϕ)となっている各エントリー(gPath)が求めたい差分(ゴールドツリーに含まれるが評価ツリーに含まれない攻撃パス)である。

【0038】

最後に、ステップS1034において、パス比較部1032は、評価結果を出力する。

例えば、評価ツリーにおいて網羅できていないパスが存在する場合は、パス比較部1032は、評価ツリーにおいて網羅できていないパスをディスプレイ907に表示する。網羅性評価装置100のユーザは、ディスプレイ907に表示されたパスを解析して、システム知識104、攻撃知識105等を改訂することができ、評価パスの網羅性を向上させることができる。

【0039】

実施の形態の効果の説明

本実施の形態では、評価ツリーを、情報システムへの侵攻経路が網羅され情報システムへの侵攻手順が反映されるゴールドツリーと比較するため、評価ツリーの網羅性を評価することができる。また、本実施の形態では、評価ツリーで網羅できていないパスを抽出し、抽出したパスを網羅性評価装置100のユーザに提示することができる。このため、ユーザは、提示された内容を評価ツリーの生成手順にフィードバックすることができ、この結果、評価ツリーの網羅性を高めることができる。

【0040】

実施の形態2.

実施の形態1では、評価ツリーで網羅できていないパスが抽出された場合に、抽出されたパスをユーザに提示するのみである。本実施の形態では、評価ツリーで網羅できていないパスが抽出された場合に、当該パスが評価ツリーで網羅できていない理由を示す構成を説明する。

【0041】

構成の説明

本実施の形態でも、網羅性評価装置100のハードウェア構成例は図1に示す通りである。また、網羅性評価装置100の機能構成例は図2に示す通りである。

本実施の形態では、ツリー比較部103の内部構成例が実施の形態1と異なる。

図24は、本実施の形態に係るツリー比較部103の内部構成例を示す。

10

20

30

40

50

【0042】

図24では、図19の構成と比較して、失敗ツリー生成部1033が追加されている。

失敗ツリー生成部1033は、情報システムについての述語論理を用いた推論において推論に失敗した要素が含まれるアタックツリーを生成する。つまり、失敗ツリー生成部1033は、評価ツリー生成部101による評価ツリーの生成において推論に失敗したパスで構成されるアタックツリーを生成する。失敗ツリー生成部1033が生成するアタックツリーは失敗ツリーという。失敗ツリーには、評価ツリー同様、複数の攻撃ステップが含まれる攻撃パスが複数含まれる。

失敗ツリー生成部1033は、失敗ツリー取得部に相当する。

【0043】

本実施の形態では、パス抽出部1031は、失敗ツリーからもパスを抽出する。

また、本実施の形態では、パス比較部1032は、評価ツリーとゴールドツリーを比較するとともに、ゴールドツリーと失敗ツリーも比較する。

そして、パス比較部1032は、ゴールドツリーに含まれる特定の攻撃パスに含まれる複数の攻撃ステップがゴールドツリーと同じ順序で評価ツリー及び失敗ツリーのいずれにも含まれていない場合に、当該特定の攻撃パスをディスプレイ907に出力する。更に、パス比較部1032は、述語論理を用いた推論の前提、すなわち、システム知識104、攻撃知識105等に欠陥があることが推定される旨を通知するメッセージをディスプレイ907に出力する。

また、パス比較部1032は、ゴールドツリーに含まれる特定の攻撃パスに含まれる複数の攻撃ステップがゴールドツリーと同じ順序で評価ツリーには含まれていないが失敗ツリーには含まれている場合にも、当該特定の攻撃パスをディスプレイ907に出力する。更に、パス比較部1032は、述語論理を用いた推論の前提、すなわち、システム知識104、攻撃知識105等に欠陥がないことが推定される旨を通知するメッセージをディスプレイ907に出力する。

【0044】

動作の説明

図25は、本実施の形態に係るツリー比較部103の動作例を示す。

【0045】

まず、ステップS2031において、失敗ツリー生成部1033が、失敗ツリーを生成する。

評価ツリー生成部101の処理を修正することで、失敗ツリー生成部1033を実現することができる。評価ツリー生成部101では、システム知識104、攻撃知識105等を利用して、後ろ向き推論により攻撃目標が成立する全てのケース（攻撃パス）を導出する。評価ツリー生成部101は、図4と図5に記載した攻撃知識105及びシステム知識104を利用すると、図6の推論過程を経て、図7のアタックツリーを抽出することができる。ここで、図6の推論過程には推論失敗の過程も含まれている。このため、失敗ツリー生成部1033は、推論が失敗したパスのみを選び出すと、失敗ツリーを得ることができる。具体的には、評価ツリー生成部101は、Trueである推論過程ごとに推論過程の分割を行う。また、評価ツリー生成部101は、Failである推論過程は排除する。このようにすることで、評価ツリー生成部101は、評価ツリーを生成する。一方、失敗ツリー生成部1033は、Trueである推論過程ごとに推論過程の分割を行うのではなく、Failである推論過程ごとに推論過程の分割を行う。そして、失敗ツリー生成部1033は、Trueである推論過程を排除する。

図6のツリーから失敗のパスだけをピックアップして整形した失敗ツリーの例を図26に示す。失敗ツリー生成部1033は、失敗のパスのピックアップは最初に失敗（条件がFalseになる）が判明した時点で処理を終了する。図7の評価ツリーと図26の失敗ツリーを合わせると図6のツリーができ、評価ツリーと失敗ツリーは相補的であることがわかる。

【0046】

ステップS2032及びS2033において、パス抽出部1031が、ゴールドツリーと評価ツリーからパスを抽出する。ステップS2032及びS2033は、実施の形態1で説明したステップS1031及びS1032と同じであるため、詳細な説明を省略する。

【0047】

次に、ステップS2034において、パス抽出部1031が、失敗ツリーからパスを抽出する。ステップS2034の処理もステップS2032及びS2033と同等であるため、詳細な説明は省略する。

【0048】

次に、ステップS2035において、パス比較部1032が、ゴールドツリーと評価ツリーのそれぞれから抽出したパスを比較する。そして、パス比較部1032は、図23に示す比較手順を利用し、比較結果として`matchedAttackPathDict`を取得する。

【0049】

次に、ステップS2036において、パス比較部1032は、同様の方法で、ゴールドツリーと失敗ツリーのそれぞれから抽出したパスを比較する。ステップS2036の手順は基本的にはステップS2035と同様である。しかし、ステップS2036では、ゴールドツリーの攻撃パスに途中までマッチする失敗ツリーの攻撃パスと、ゴールドツリーの当該攻撃パスとの比較でもよいという点が異なる。失敗ツリーの攻撃パスの攻撃ステップを`fStep`（メンバーは`a`, `nf`, `nt`, `i`, `s`）と表す。パス比較部1032がゴールドツリーの攻撃パスと失敗ツリーの攻撃パスとを比較することで、ゴールドツリーの攻撃パスに対応する失敗ツリーの攻撃パスが辞書形式で出力される。このようなパス比較部1032の比較動作を`matchedFailedAttackPathDict`という。

図27に、パス比較部1032の比較動作を実現する疑似コード（`compareFailedPaths`）を示す。

【0050】

ステップS2037において、パス比較部1032は、`matchedAttackPathDict`および`matchedFailedAttackPathDict`を利用して評価結果を生成する。パス比較部1032は、`matchedAttackPathDict`から2種類の情報を得る。

1つ目の情報は、評価ツリーにおけるゴールドツリーをカバーする攻撃パスについての情報である。この攻撃パスについての情報は、`matchedAttackPathDict`における空集合（ ϕ ）ではない各エントリ（`gPath`）に定義された評価ツリーの攻撃パス（`aPath`）の集合（`COVERED__ATTACK__PATH__SET`）の情報である。この集合はゴールドツリーの攻撃パスと対応する評価ツリーの攻撃パスとのペア（（`gPath`, `aPath`））の集合として定義される。ゴールドツリーの1つの攻撃パスに評価ツリーの複数の攻撃パスが対応する場合は、評価ツリーの複数のペアが集合に含まれる（{（`gPath1`, `aPath1`）, （`gPath1`, `aPath2`）, （`gPath1`, `aPath3`）}）。

2つ目の情報は、評価ツリーではカバーしていない攻撃パスについての情報である。この攻撃パスについての情報は、`matchedAttackPathDict`において空集合（ ϕ ）となっている各エントリ（`gPath`）の集合（`UNCOVERED__PATH__SET`）の情報である。アタックツリー自動生成に必要な推論ルールや前提知識において、本来カバーしなくてもよい攻撃パスが含まれている可能性もあるが、推論ルールや前提知識の設定ミスによって本来カバーしなくてはならないパスが抜けている可能性もある。

`matchedFailedAttackPathDict`からは1種類の情報を得ることができる。`matchedFailedAttackPathDict`から得られる情報は、失敗ツリーにおけるゴールドツリーを途中までカバーする攻撃パスの情報である

。この攻撃パスの情報は、`matchedFailedAttackPathDict`における空集合(ϕ)ではない各エントリ(`gPath`)に定義された失敗ツリーの攻撃パス(`fPath`)の集合(`COVERED_FAILED_PATH_SET`)の情報である。この集合はゴールドツリーの攻撃パスと対応する失敗ツリーの攻撃パスとのペア(`(gPath, fPath)`)の集合として定義される。ゴールドツリーの1つの攻撃パスに失敗ツリーの複数の攻撃パスが対応する場合は、失敗ツリーの複数のペアが集合に含まれる(`{(gPath1, fPath1), (gPath1, fPath2), (gPath1, fPath3)}`)。

ここで、`UNCOVERED_PATH_SET`に含まれる`gPath`が、`COVERED_FAILED_PATH_SET`に含まれていれば、当該`gPath`は、対応する`fPath`における最後の侵攻手順(条件)が失敗した根拠(導出失敗の条件)となる。この`gPath`と`fPath`のペアの集合を`NORMAL_UNCOVERED_PATH_SET`という。

`UNCOVERED_PATH_SET`に含まれる`gPath`が、`COVERED_FAILED_PATH_SET`に含まれていなければ、推論エンジンに与える前提知識又は推論ルールに何かしらの不具合があることが予想される。この`gPath`の集合を`ABNORMAL_UNCOVERED_PATH_SET`という。

【0051】

最後に、ステップS2038において、パス比較部1032は、評価結果をディスプレイ907に出力する。

具体的には、パス比較部1032は、評価結果として、`NORMAL_UNCOVERED_PATH_SET`と`ABNORMAL_UNCOVERED_PATH_SET`を表示する。`NORMAL_UNCOVERED_PATH_SET`については、パス比較部1032は、失敗の根拠が存在する場合は失敗の根拠も表示する。`ABNORMAL_UNCOVERED_PATH_SET`については、パス比較部1032は、システム知識104、攻撃知識105等に欠陥があるために、該当するパスが評価ツリーから漏れている可能性があることをユーザに示すことができる。

【0052】

実施の形態の効果の説明

本実施の形態によれば、評価ツリーで網羅できていないパスが抽出された場合に、当該パスが評価ツリーで網羅できていない理由をユーザに示すことができる。つまり、`PATH_PAIR_SET2`に含まれるパスについては、システム知識104、攻撃知識105等に欠陥がなく、適正に評価ツリーから除外されていることをユーザに示すことができる。一方、`UNCOVERED_PATH_SET`が存在する場合は、システム知識104、攻撃知識105等に欠陥があるために、該当するパスが評価ツリーから漏れている可能性があることをユーザに示すことができる。

【0053】

その他

実施の形態1では、評価ツリー生成部101が評価ツリーを生成することになっている。これに代えて、網羅性評価装置100の外部の機器が、評価ツリー生成部101と同様の手法で評価ツリーを生成するようにしてもよい。この場合は、網羅性評価装置100には、外部で生成された評価ツリーを取得する構成(評価ツリー取得部)が設けられる。評価ツリー取得部は、第1のアタックツリー取得部に相当する。

【0054】

また、実施の形態2では、失敗ツリー生成部1033が失敗ツリーを生成することになっている。これに代えて、網羅性評価装置100の外部の機器が、失敗ツリー生成部1033と同様の手法で失敗ツリーを生成するようにしてもよい。この場合は、網羅性評価装置100には、外部で生成された失敗ツリーを取得する構成(失敗ツリー取得部)が設けられる。

【0055】

10

20

30

40

50

以上、本発明の実施の形態について説明したが、これら2つの実施の形態を組み合わせ
て実施しても構わない。

あるいは、これら2つの実施の形態のうち、1つを部分的に実施しても構わない。

あるいは、これら2つの実施の形態を部分的に組み合わせ実施しても構わない。

なお、本発明は、これらの実施の形態に限定されるものではなく、必要に応じて種々の
変更が可能である。

【0056】

ハードウェア構成の説明

最後に、網羅性評価装置100のハードウェア構成の補足説明を行う。

図1に示すプロセッサ901は、プロセッシングを行うIC(Integrated
Circuit)である。 10

プロセッサ901は、CPU(Central Processing Unit)、
DSP(Digital Signal Processor)等である。

図1に示す主記憶装置902は、RAM(Random Access Memory)
)である。

図1に示す補助記憶装置903は、ROM(Read Only Memory)、フ
ラッシュメモリ、HDD(Hard Disk Drive)等である。

図1に示す通信デバイス904は、データの通信処理を実行する電子回路である。

通信デバイス904は、例えば、通信チップ又はNIC(Network Inter
face Card)である。 20

【0057】

また、補助記憶装置903には、OSも記憶されている。

そして、OSの少なくとも一部が主記憶装置902にロードされ、プロセッサ901に
より実行される。

プロセッサ901はOSの少なくとも一部を実行しながら、評価ツリー生成部101、
ゴールドツリー生成部102及びツリー比較部103の機能を実現するプログラムを実行
する。

プロセッサ901がOSを実行することで、タスク管理、メモリ管理、ファイル管理、
通信制御等が行われる。

また、評価ツリー生成部101、ゴールドツリー生成部102及びツリー比較部103
の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、主記憶装
置902、補助記憶装置903、プロセッサ901内のレジスタ及びキャッシュメモリの
少なくともいずれかに記憶される。 30

また、評価ツリー生成部101、ゴールドツリー生成部102及びツリー比較部103
の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コ
ンパクトディスク、ブルーレイ(登録商標)ディスク、DVD等の可搬記録媒体に格納さ
れていてもよい。

【0058】

また、評価ツリー生成部101、ゴールドツリー生成部102及びツリー比較部103
の「部」を、「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。 40

また、網羅性評価装置100は、処理回路により実現されてもよい。処理回路は、例え
ば、ロジックIC(Integrated Circuit)、GA(Gate Arr
ay)、ASIC(Application Specific Integrated
Circuit)、FPGA(Field-Programmable Gate A
rray)である。

この場合は、評価ツリー生成部101、ゴールドツリー生成部102及びツリー比較部
103は、それぞれ処理回路の一部として実現される。

なお、本明細書では、プロセッサと処理回路との上位概念を、「プロセッシングサーキ
ットリー」という。

つまり、プロセッサと処理回路とは、それぞれ「プロセッシングサーキットリー」の具 50

体例である。

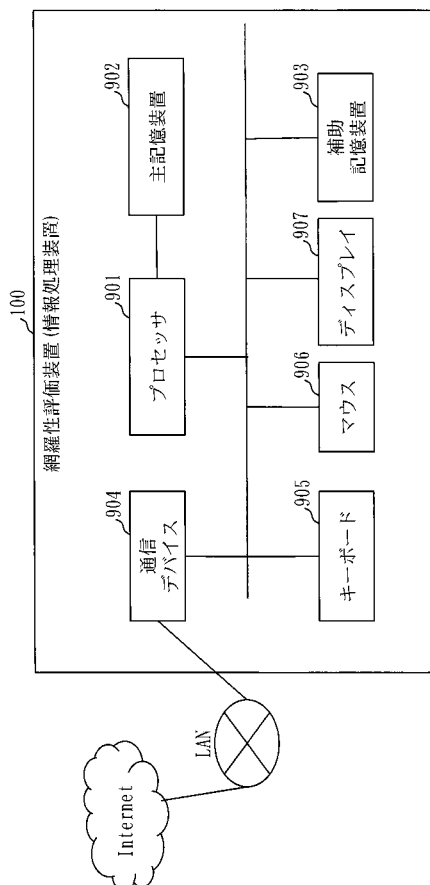
【符号の説明】

【0059】

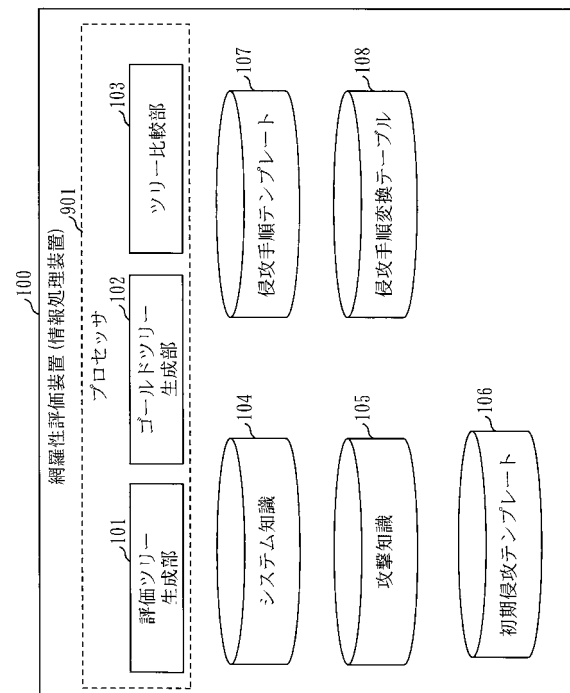
100 網羅性評価装置、101 評価ツリー生成部、102 ゴールドツリー生成部、103 ツリー比較部、104 システム知識、105 攻撃知識、106 初期侵攻テンプレート、107 侵攻手順テンプレート、108 侵攻手順変換テーブル、901 プロセッサ、902 主記憶装置、903 補助記憶装置、904 通信デバイス、905 キーボード、906 マウス、907 ディスプレイ、1021 ネットワーク網羅部、1022 テンプレート適用部、1031 パス抽出部、1032 パス比較部、1033 失敗ツリー生成部。

10

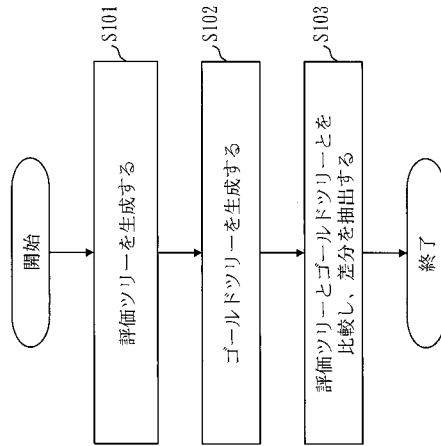
【図1】



【図2】



【図 3】



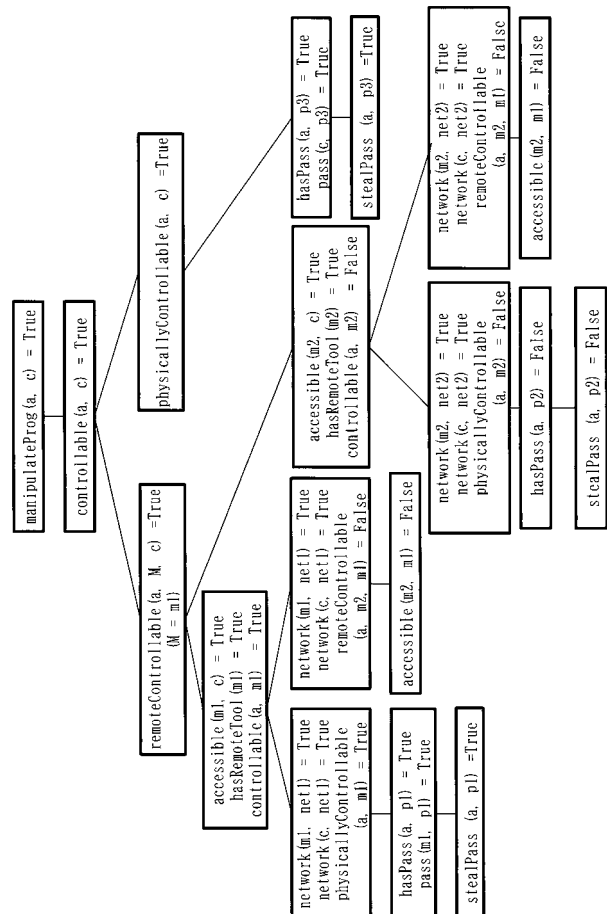
【図 5】

規則	説明
network(m1, net1)	マシンm1のネットワークアドレスはnet1
network(m2, net2)	マシンm2のネットワークアドレスはnet2
network(c, net1)	マシンcのネットワークアドレスはnet1
network(c, net2)	マシンcのネットワークアドレスはnet2
pass(m1, p1)	マシンm1のパスワードはp1
pass(m2, p2)	マシンm2のパスワードはp2
pass(c, p3)	マシンcのパスワードはp3
stealPass(a, p1)	攻撃者aはパスワードp1を盗んだ
stealPass(a, p3)	攻撃者aはパスワードp3を盗んだ
hasRemoteTool(m1)	マシンm1は遠隔操作ツールを持っている
hasRemoteTool(m2)	マシンm2は遠隔操作ツールを持っている

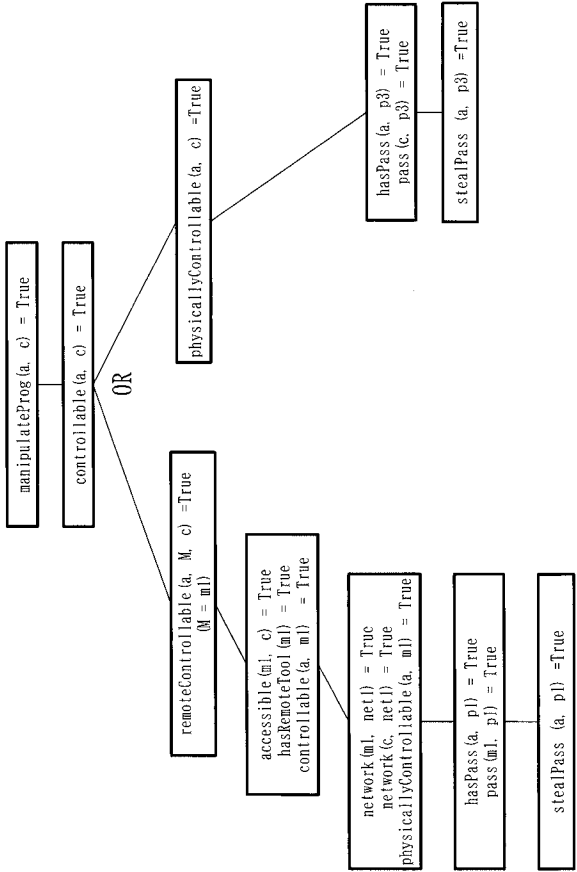
【図 4】

規則	説明
manipulateProg(A, M) :- controllable(A, M)	攻撃者AがマシンMをコントロールできる場合、攻撃者AはマシンMのプログラムを書き換えることができる。
controllable(A, M) :- physicallyControllable(A, M)	攻撃者Aが物理的にマシンMをコントロールできる場合、攻撃者AがマシンMをコントロールできる。
controllable(A, M) :- remotelyControllable(A, M1, M)	攻撃者Aが遠隔にあるマシンM1からマシンMをコントロールできる場合、攻撃者AがマシンMをコントロールできる。
remotelyControllable(A, M1, M2) :- accessible(M1, M2), hasRemoteTool(M1), controllable(A, M1)	マシンM1からマシンM2にアクセス可能で、マシンM1が遠隔操作ツールを持っていて、攻撃者AがマシンM1をコントロールできる場合、攻撃者Aが遠隔にあるマシンM1からマシンM2をコントロールできる。
accessible(M1, M2) :- network(M1, IP), network(M2, IP)	マシンM1のネットワークアドレスがIPで、マシンM2のネットワークアドレスもIPの場合、マシンM1からマシンM2にアクセス可能である。
physicallyControllable(A, M) :- hasPass(A, P), pass(A, P)	攻撃者AがパスワードPを持っていて、マシンMのパスワードがPの場合、攻撃者Aが物理的にマシンMをコントロールできる。
hasPass(A, P) :- stealPass(A, P)	攻撃者AがパスワードPを盗んだ場合、攻撃者AがパスワードPを持っている。

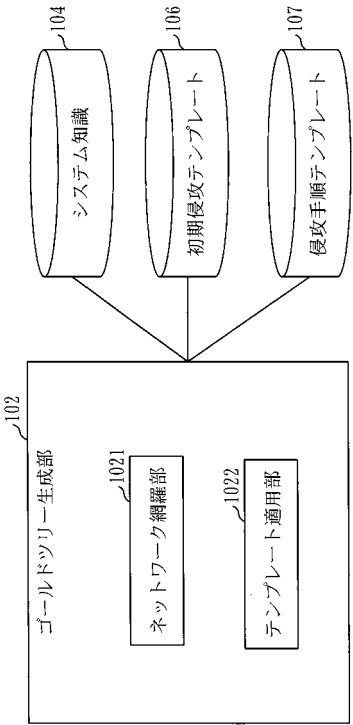
【図 6】



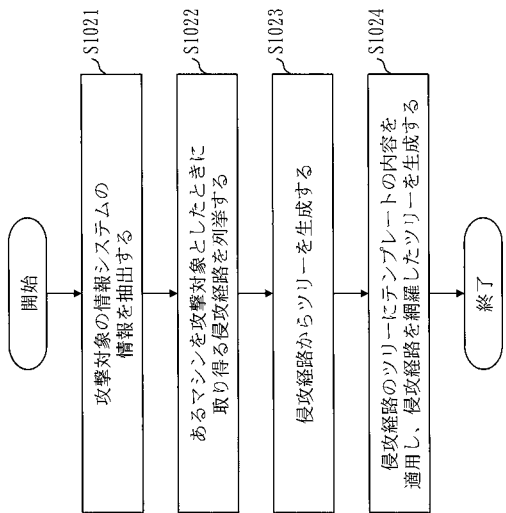
【図 7】



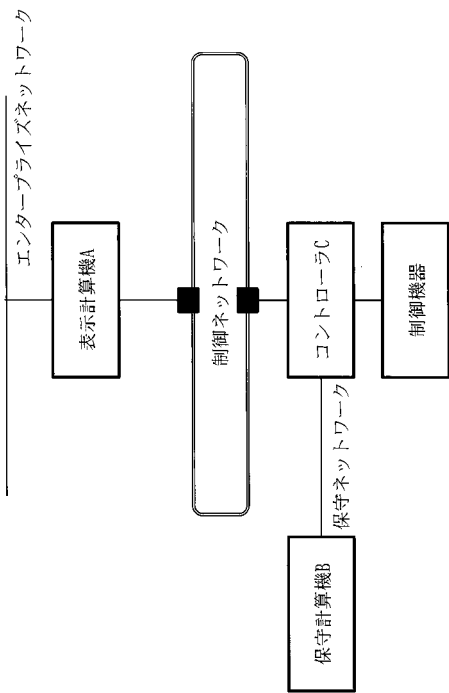
【図 8】



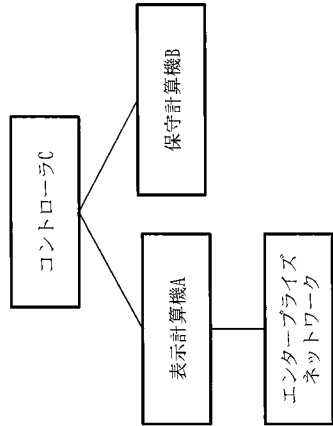
【図 9】



【図 10】



【図 1 1】



【図 1 2】

マシンタイプ OS (version), Application (version) ...	初期侵攻手順1	初期侵攻手順2	初期侵攻手順3	...	...
保守計算機	Initial_access1	Initial_access2	φ	φ	...
コントローラ	Initial_access2	Initial_access3	φ	φ	...
表示計算機	Initial_access1	Initial_access2	Initial_access4	φ	...

【図 1 3】

マシンタイプ OS (version), Application (version) ...	初期侵攻手順1	初期侵攻手順2	初期侵攻手順3	...	...
保守計算機	USB経由のマルウェア感染	盗んだパスワードを利用したログイン	φ	φ	...
コントローラ	USB経由のプログラム変更	盗んだパスワードを利用したログイン	φ	φ	...
表示計算機	USB経由のマルウェア感染	盗んだパスワードを利用したログイン	不正メール経由のマルウェア感染	φ	...

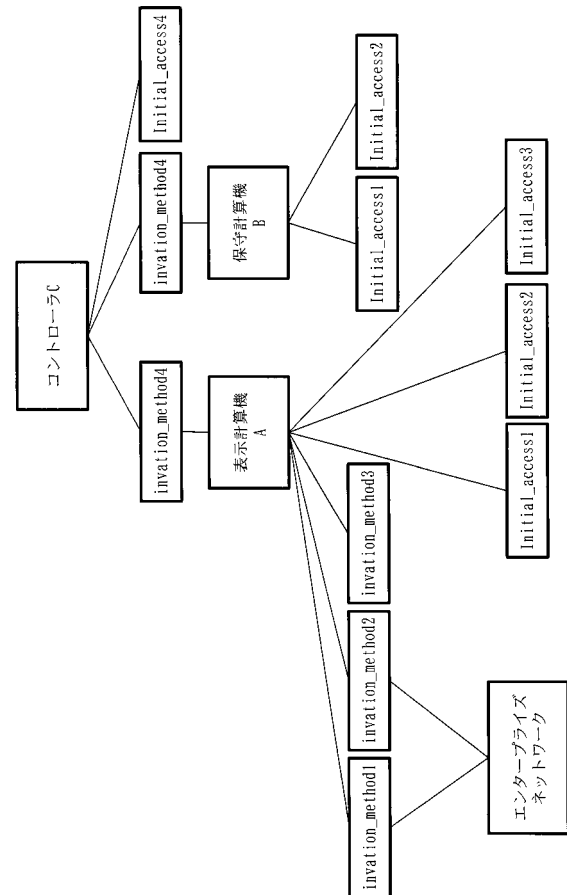
【図 1 4】

マシンタイプ OS (version), Application (version) ...	侵攻手順1	侵攻手順2	侵攻手順3	侵攻手順4	...
保守計算機	invation_method1	invation_method2	φ	φ	...
コントローラ	invation_method4	φ	φ	φ	...
表示計算機	invation_method1	invation_method2	invation_method3	φ	...

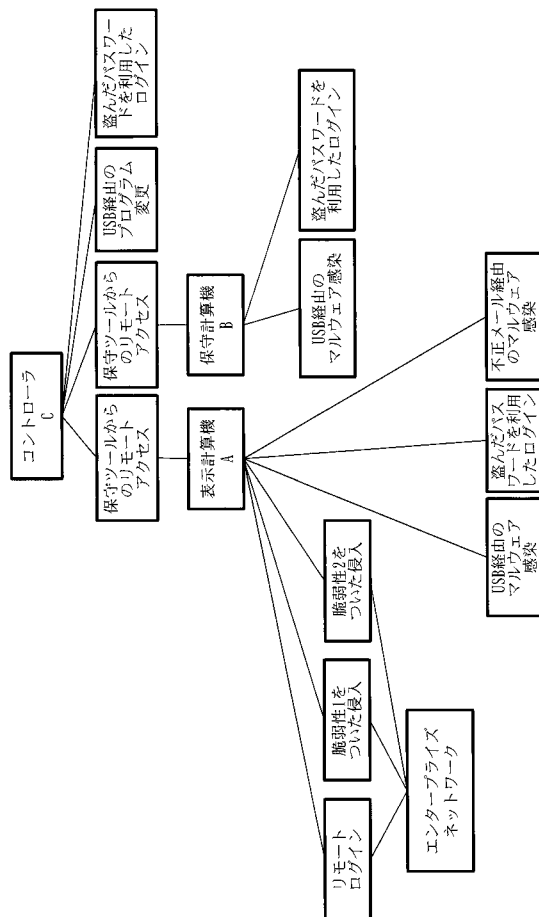
【図 15】

マシンタイプ OS (version), Application (version)...	侵入手順1	侵入手順2	侵入手順3	侵入手順4	...
保守計算機	リモートログイン	脆弱性1	φ	φ	...
コントローラ	保守ツールからのリモートアクセス	φ	φ	φ	...
表示計算機	リモートログイン	脆弱性1	脆弱性2	φ	...

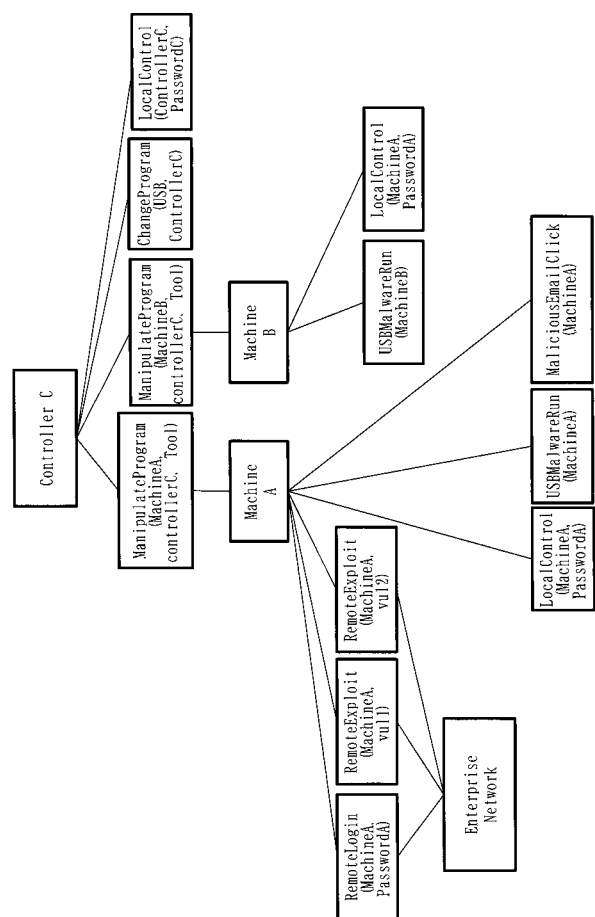
【図 16】



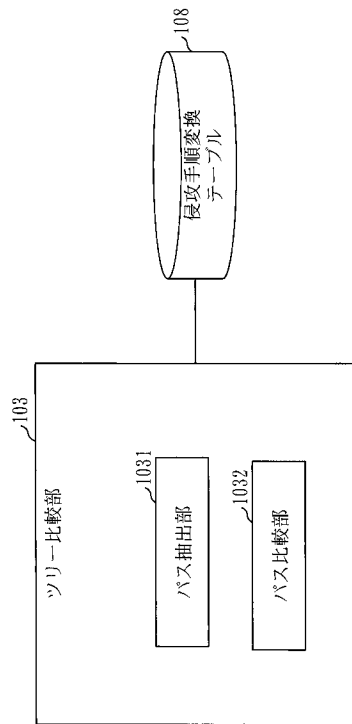
【図 17】



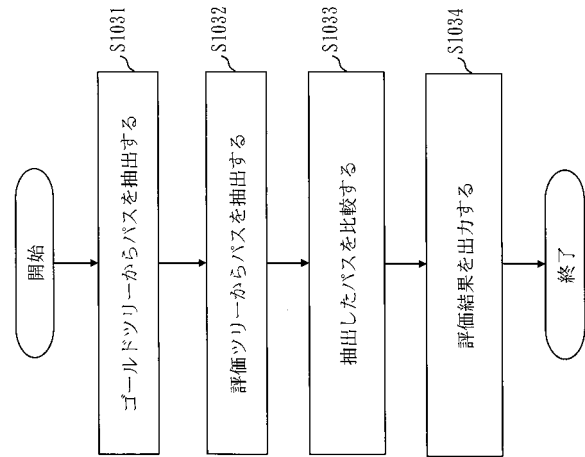
【図 18】



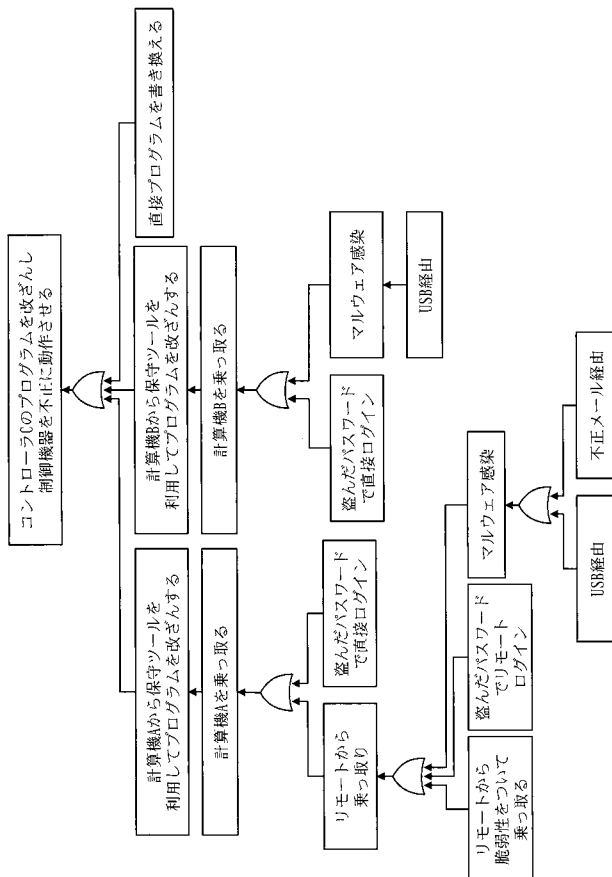
【 図 1 9 】



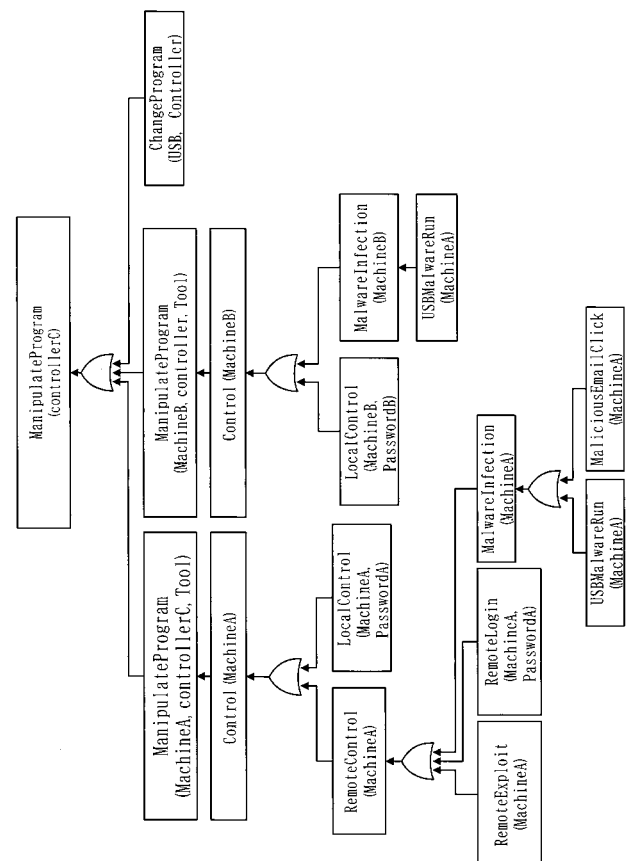
【図 20】



【图 2 1】



【图 2 2】



【図 23】

```

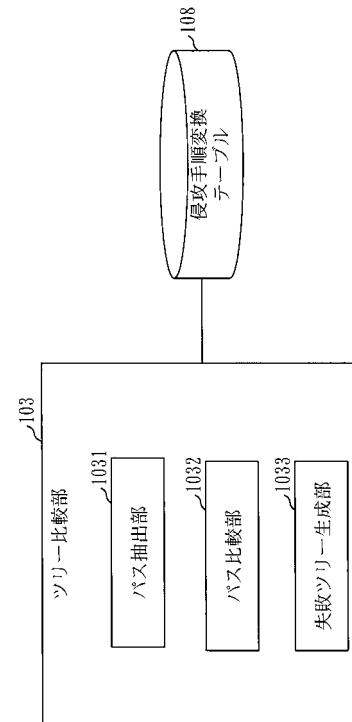
1: procedure compareAttackPaths(goldTreePathList, attackTreePathList):
  /* パスのリスト (配列) には、頂上から順にノードが記録されている */
2:   matchedPath = dict() /* 辞書初期化 */
3:   for each gPath in goldPathList
4:     for each aPath in attackTreePathList
5:       matchedPathDict[gPath] =
         matchedPathDict[gPath] ∪ matchPath (gPath, aPath)
6:   return matchedPathDict
  /* エントリーが空集合の gPath がマッチなかったパス */

1: procedure matchPath(gPath, aPath):
2:   matchedNum = 0
3:   aIndex = 0
4:   for (i = 0; i < length(gPath); i++)
5:     gStep = gPath[i]
6:     for (j = aIndex; j < length(aPath); j++)
7:       aStepSet = aPath[j]
8:       if matchStep(gStep, aStepSet)
9:         matchedNum = matchedNum + 1
10:        aIndex = j
11:        break
12:   if matchedNum >= len(gPath) /* len(gPath) gPath の長さ */
13:     return { aPath } /* 集合で返す */
14:   return ∅

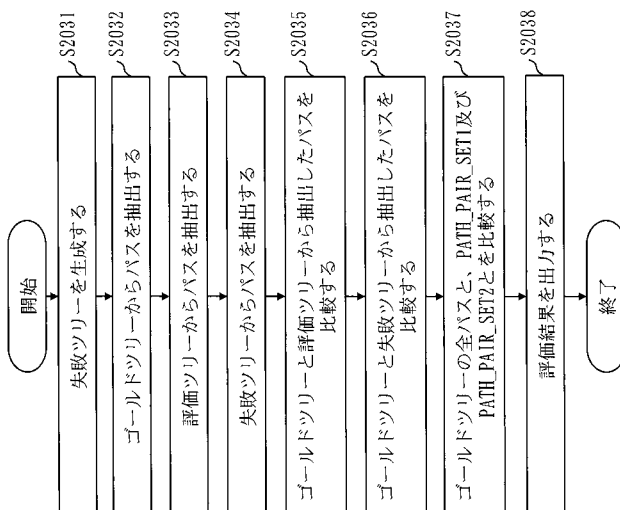
1: procedure matchStep(gStep, aStepSet):
2:   gStep2 = translate(gStep, table)
  /* 攻撃ステップを攻撃手口対応テーブル (table) で変換 */
3:   for each aStep in aStepSet
4:     if gStep2.a == aStep.a &&
       gStep2.nf == aStep.nf && gStep2.nt == aStep.nt
5:       /* gStep2.i == aStep.i && gStep2.s == aStep.s は適宜追加 */
6:       return True
7:   return False

```

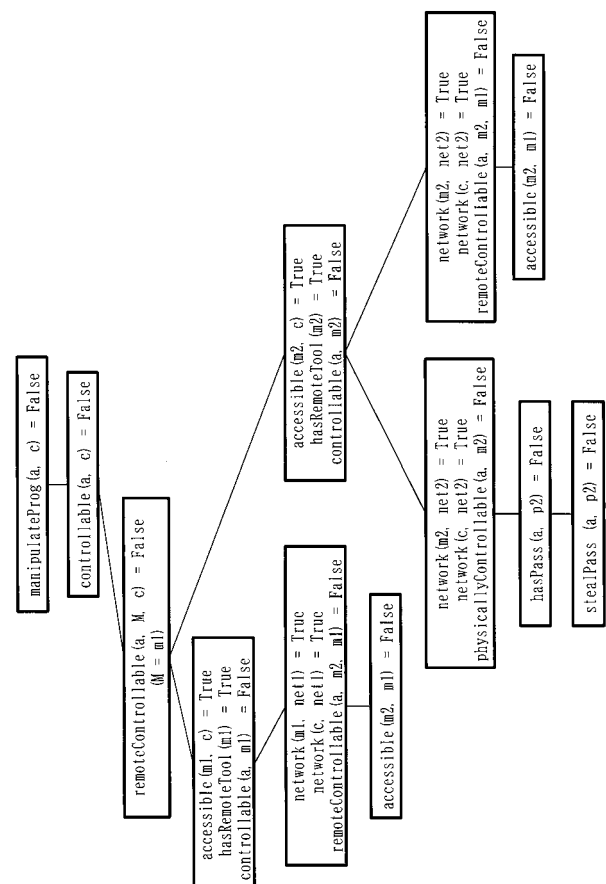
【図 24】



【図 25】



【図 26】



【図 27】

```

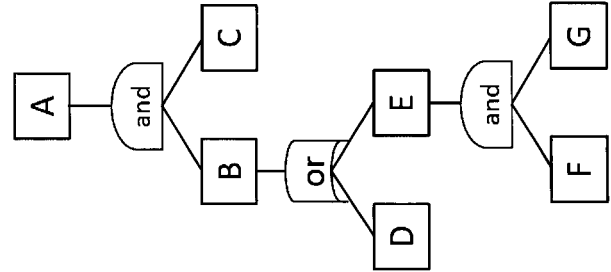
1: procedure compareFailedPaths(goldTreePathList, failedAttackTreePathList):
2:   matchedPath = dict() /* 辞書初期化 */
3:   for each gPath in goldPathList
4:     for each fPath in failedAttackTreePathList
5:       matchedPathDict[gPath] =
         matchedPathDict[gPath]
         ∪ matchFailedPath (gPath, fPath)
6:   return matchedPathDict
   /* エントリーが空集合の gPath がマッチなかったパス */

1: procedure matchFailedPath(gPath, fPath):
2:   matchedNum = 0
3:   fIndex = 0
4:   for (i = 0; i < length(gPath); i++)
5:     gStep = gPath[i]
6:     for (j = fIndex; j < length(fPath); j++)
7:       fStepSet = fPath[j]
8:       if matchStep(gStep, fStepSet)
9:         matchedNum = matchedNum + 1
10:        fIndex = j
11:        break
12:   if matchedNum > 0
13:     return { fPath }
14:   return φ

1: procedure matchStep(gStep, fStepSet):
2:   gStep2 = translate(gStep, table)
   /* 攻撃ステップを攻撃手口対応テーブル (table) で変換 */
3:   for each fStep in fStepSet
4:     if gStep2.ga == fStep.fa &&
       gStep2.nt == fStep.nf && gStep2.gnt == fStep.nt
       /* gStep2.i == fStep.i && gStep2.s == fStep.s は適宜追加 */
5:     return True
6:   return False

```

【図 28】



【手続補正書】

【提出日】令和2年10月22日(2020.10.22)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0034

【補正方法】変更

【補正の内容】

【0034】

ステップS1033において、パス比較部1032が、ゴールドツリーと評価ツリーのそれぞれから抽出したパスを比較する。そして、パス比較部1032は、ゴールドツリーのパス中にある攻撃ステップを必ず含むパスを評価ツリーから抽出する。

説明のために、ゴールドツリーから抽出される攻撃パスの攻撃ステップを $gStep$ (メンバーは a, nf, nt, i, s) と表す。攻撃ステップ $gStep$ は、主体 $gStep.s$ が、侵攻手順 $gStep.a$ を利用し、補足情報 $gStep.i$ を使って、攻撃元ノード $gStep.nf$ から攻撃先ノード $gStep.nt$ を攻撃することを意味する。

$malEmailClick(m1, x, \quad)$ の場合は、 $gStep.a$ が $malEmailClick$ である。 $gStep.nf$ は x である。 $gStep.nt$ は $m1$ である。 $gStep.i$ は「 」(ドントケア) である。 $gStep.s$ は「 」(ドントケア) である。

同様に、評価ツリーから抽出される攻撃パスの攻撃ステップを $aStep$ (メンバーは a, nf, nt, i, s) と表す。攻撃ステップ $aStep$ は、主体 $aStep.s$ が、侵攻手順 $aStep.a$ を利用し、補足情報 $aStep.i$ を使って、攻撃元ノード $aStep.nf$ から攻撃先ノード $aStep.nt$ を攻撃することを意味する。

$remExp(a, x, m1, vul1)$ の場合は、 $aStep.a$ が $remExp$ である。 $aStep.s$ は a である。 $aStep.nf$ は x である。 $aStep.nt$ は m

1である。aStep. iはvul1である。

「access(x, m1, __, __)、clickMalEmail1(a, x, m1, __)、control(a, x, __, __)」のように1つの攻撃ステップの中に複数の侵攻手順（もしくは条件）が含まれている場合がある。このような攻撃ステップは、要素の数に関係なく、侵攻手順の集合として扱う。

ゴールドツリーから抽出した各攻撃パスは攻撃ステップ（侵攻手順）が要素となる順序リストである。評価ツリーから抽出した各攻撃パスは攻撃ステップ（侵攻手順の集合）が要素となる順序リストである。パス比較部1032は、以下のように、ゴールドツリーの攻撃パスと評価ツリーの攻撃パスとを比較する。

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2018/040641
A. CLASSIFICATION OF SUBJECT MATTER Int.Cl. G06F21/57 (2013.01) i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) Int.Cl. G06F21/57		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2019 Registered utility model specifications of Japan 1996-2019 Published registered utility model applications of Japan 1994-2019		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/0325412 A1 (NORRMAN, K.) 23 December 2010, paragraphs [0005]-[0028], [0142] & JP 2011-519435 A, paragraphs [0005]-[0026], [0108], [0109]	1-9
A	US 2006/0021034 A1 (COOK, C. L.) 26 January 2006, paragraph [0054] (Family: none)	1-9
☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 09.01.2019		Date of mailing of the international search report 22.01.2019
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/040641

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2018-527672 A (RENESAS ELECTRONICS EUROPE LIMITED) 20 September 2018, paragraphs [0050], [0059]-[0063], [0082]-[0094], fig. 2, 5, 10, 11 & US 2018/0183826 A1, paragraphs [0064], [0075]-[0079], [0094]-[0103], fig. 2, 5, 10, 11 & WO 2017/032957 A1 & CN 108293038 A	1-9

国際調査報告		国際出願番号 PCT/J P 2 0 1 8 / 0 4 0 6 4 1	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G06F21/57(2013.01)i			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G06F21/57			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2019年 日本国実用新案登録公報 1996-2019年 日本国登録実用新案公報 1994-2019年			
国際調査で利用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリ *	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号	
A	US 2010/0325412 A1 (NORRMAN, Karl) 2010.12.23, 段落 [0005]-[0028], [0142] & JP 2011-519435 A, 段落 [0005]-[0026], [0108]-[0109]	1-9	
A	US 2006/0021034 A1 (COOK, Chad L.) 2006.01.26, 段落[0054] (フ ァミリーなし)	1-9	
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリ 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献			
国際調査を完了した日 09.01.2019		国際調査報告の発送日 22.01.2019	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 上島 拓也 電話番号 03-3581-1101 内線 3546	5 S 6 2 9 3

国際調査報告

国際出願番号 PCT/J P 2 0 1 8 / 0 4 0 6 4 1

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2018-527672 A (ルネサス・エレクトロニクス・ヨーロッパ・リミテッド) 2018.09.20, 段落[0050], [0059]-[0063], [0082]-[0094], 図 2, 5, 10-11 & US 2018/0183826 A1, 段落 [0064], [0075]-[0079], [0094]-[0103], 図 2, 5, 10-11 & W0 2017/032957 A1 & CN 108293038 A	1-9

フロントページの続き

(72)発明者 河内 清人

日本国東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内

(注) この公表は、国際事務局(W I P O)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。