(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6359227号
(P6359227)
(45)発行日　平成30年7月18日(2018.7.18)　(24)登録日　平成30年6月29日(2018.6.29)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/56 360

請求項の数 15 (全 30 頁)

(21)出願番号　特願2018-510034(P2018-510034)
(86)(22)出願日　平成28年4月4日(2016.4.4)
(86)国際出願番号　PCT/JP2016/061048
(87)国際公開番号　WO2017/175283
(87)国際公開日　平成29年10月12日(2017.10.12)
審査請求日　平成30年4月17日(2018.4.17)

早期審査対象出願

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　110002491
溝井国際特許業務法人
(72)発明者　片岡　えり
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　松本　光弘
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

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】プロセス探索装置およびプロセス探索プログラム

(57)【特許請求の範囲】
【請求項１】
対象装置に対する攻撃に関するプロセスを探索するプロセス探索装置であって、
順序を有する複数の攻撃のうちの検知された攻撃を識別する攻撃種類識別子と、攻撃が検知された時間帯に動作した動作プロセスの動作プロセス識別子とが互いに対応付けられた動作プロセスリストと、攻撃の検知が行われた時間帯に他のプロセスを操作した操作元プロセスの操作元プロセス識別子と、操作された他のプロセスである操作先プロセスの操作先プロセス識別子とが互いに対応付けられた操作プロセスリストとを記憶する記憶部と、
前記動作プロセスリストと前記操作プロセスリストとを用いて、攻撃種類識別子の１つである起点種類識別子に対応付けられた動作プロセス識別子と前記起点種類識別子と異なる攻撃種類識別子に対応付けられた動作プロセス識別子との組に該当し、操作元プロセス識別子と操作先プロセス識別子との組に該当する間接プロセス識別子の組を探索する間接プロセス探索部と
を備えるプロセス探索装置。
【請求項２】
前記間接プロセス探索部は、
前記動作プロセスリストに含まれる攻撃種類識別子から、それぞれの攻撃種類識別子に対応付けられた動作プロセス識別子の個数に基づいて、探索の起点となる攻撃種類識別子である起点種類識別子を選択し、

選択された起点種類識別子に対応付けられた動作プロセス識別子を用いて、前記間接プロセス識別子の組を探索する
請求項１に記載のプロセス探索装置。
【請求項３】
前記間接プロセス探索部は、前記動作プロセスリストに含まれる攻撃種類識別子のうち、対応付けられた動作プロセス識別子の個数が最も少ない攻撃種類識別子を、前記起点種類識別子として選択する
請求項２に記載のプロセス探索装置。
【請求項４】
前記間接プロセス探索部は、
前記動作プロセスリストから、前記起点種類識別子に対応付けられた動作プロセス識別子を、起点プロセス識別子として選択し、
前記動作プロセスリストから、前記起点種類識別子と異なる攻撃種類識別子を、探索種類識別子として選択し、
前記動作プロセスリストから、前記探索種類識別子に対応付けられた動作プロセス識別子を、探索プロセス識別子として選択し、
前記起点プロセス識別子と前記探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が前記操作プロセスリストに含まれるか判定する
請求項２に記載のプロセス探索装置。
【請求項５】
前記攻撃種類識別子は、攻撃の順序を示す番号であり、
前記間接プロセス探索部は、
前記起点種類識別子が示す番号の１つ前の番号を示す攻撃種類識別子を、前記探索種類識別子として選択する
請求項４に記載のプロセス探索装置。
【請求項６】
前記間接プロセス探索部は、
前記起点プロセス識別子と前記探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が前記操作プロセスリストに含まれ、前記探索種類識別子が示す番号が先頭番号である場合、前記起点プロセス識別子と前記探索プロセス識別子との組を、前記間接プロセス識別子の組として生成する
請求項５に記載のプロセス探索装置。
【請求項７】
前記間接プロセス探索部は、前記起点プロセス識別子と前記探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が前記操作プロセスリストに含まれるが、前記探索種類識別子が示す番号が前記先頭番号でない場合、
前記探索種類識別子に対応付けられた動作プロセス識別子を新たな起点プロセス識別子として選択し、
前記探索種類識別子が示す番号の１つ前の番号を示す攻撃種類識別子を新たな探索種類識別子として選択し、
前記新たな探索種類識別子に対応付けられた動作プロセス識別子を新たな探索プロセス識別子として選択し、
前記新たな起点プロセス識別子と前記新たな探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が前記操作プロセスリストに含まれ、前記新たな探索種類識別子が示す番号が前記先頭番号である場合、前記起点プロセス識別子と前記探索プロセス識別子との組と、前記新たな起点プロセス識別子と前記新たな探索プロセス識別子との組とを、前記間接プロセス識別子の組として生成する
請求項６に記載のプロセス探索装置。
【請求項８】
前記動作プロセスリストは、攻撃が検知された時間帯の始まりの時刻であって攻撃種類

識別子と動作プロセス識別子とに対応付けられた時刻である攻撃開始時刻を含み、
前記間接プロセス探索部は、
前記動作プロセスリストから、前記探索種類識別子に対応付けられた動作プロセス識別子のそれぞれを、攻撃開始時刻の早い順に、前記探索プロセス識別子として選択する
請求項５に記載のプロセス探索装置。
【請求項９】
前記間接プロセス探索部は、
前記探索プロセス識別子と同じ操作元プロセス識別子を前記操作プロセスリストから選択し、選択された操作元プロセス識別子に対応付けられた操作先プロセス識別子を前記操作プロセスリストから付加プロセス識別子として取得し、
前記起点プロセス識別子と前記探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が前記操作プロセスリストに含まれ、前記探索種類識別子が示す番号が先頭番号である場合、前記起点プロセス識別子と前記探索プロセス識別子と前記付加プロセス識別子との組を、前記間接プロセス識別子の組として生成する
請求項８に記載のプロセス探索装置。
【請求項１０】
前記間接プロセス探索部は、
前記探索プロセス識別子が、先に選択された探索プロセス識別子に対応する付加プロセス識別子と同じである場合、前記起点プロセス識別子と前記探索プロセス識別子との組に対する処理を省略する
請求項９に記載のプロセス探索装置。
【請求項１１】
前記間接プロセス探索部は、
前記起点種類識別子が示す番号の１つ後の番号を示す攻撃種類識別子を、新たな探索種類識別子として選択し、
前記新たな探索種類識別子に対応付けられた動作プロセス識別子を新たな探索プロセス識別子として選択し、
前記起点プロセス識別子と前記新たな探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が前記操作プロセスリストに含まれる場合、前記起点プロセス識別子と前記新たな探索プロセス識別子との組を、前記間接プロセス識別子の組として生成する
請求項６に記載のプロセス探索装置。
【請求項１２】
前記動作プロセスリストは、攻撃が検知された時間帯の始まりの時刻であって攻撃種類識別子と動作プロセス識別子とに対応付けられた時刻である攻撃開始時刻を含み、
前記間接プロセス探索部は、
前記動作プロセスリストから、前記探索種類識別子に対応付けられた動作プロセス識別子のそれぞれを、攻撃開始時刻の遅い順に、前記新たな探索プロセス識別子として選択する
請求項１１に記載のプロセス探索装置。
【請求項１３】
前記間接プロセス探索部は、
前記新たな探索プロセス識別子と同じ操作元プロセス識別子を前記操作プロセスリストから選択し、選択された操作元プロセス識別子に対応付けられた操作元プロセス識別子を前記操作プロセスリストから付加プロセス識別子として取得し、
取得された付加プロセス識別子を、前記起点プロセス識別子と前記探索プロセス識別子との組に加える
請求項１２に記載のプロセス探索装置。
【請求項１４】
前記間接プロセス探索部は、

前記新たな探索プロセス識別子が、先に選択された探索プロセス識別子に対応する付加プロセス識別子と同じ識別子である場合、前記起点プロセス識別子と前記新たな探索プロセス識別子との組に対する処理を省略する
請求項１３に記載のプロセス探索装置。
【請求項１５】
動作プロセスリストと操作プロセスリストと用いて対象装置に対する攻撃に関するプロセスを探索するプロセス探索プログラムであって、
前記動作プロセスリストは、順序を有する複数の攻撃のうちの検知された攻撃を識別する攻撃種類識別子と、攻撃が検知された時間帯に動作した動作プロセスの動作プロセス識別子とが互いに対応付けられたリストであり、
前記操作プロセスリストは、攻撃の検知が行われた時間帯に他のプロセスを操作した操作元プロセスの操作元プロセス識別子と、操作された他のプロセスである操作先プロセスの操作先プロセス識別子とが互いに対応付けられたリストであり、
前記プロセス探索プログラムは、
前記動作プロセスリストと前記操作プロセスリストとを用いて、攻撃種類識別子の１つである起点種類識別子に対応付けられた動作プロセス識別子と前記起点種類識別子と異なる攻撃種類識別子に対応付けられた動作プロセス識別子との組に該当し、操作元プロセス識別子と操作先プロセス識別子との組に該当する間接プロセス識別子の組を探索する間接プロセス探索処理
をコンピュータに実行させるためのプロセス探索プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、攻撃に関係するプロセスを探索する技術に関するものである。
【背景技術】
【０００２】
サイバー攻撃の対策として、ＩＰＳ（Ｉｎｔｒｕｓｉｏｎ　Ｐｒｅｖｅｎｔｉｏｎ　Ｓｙｓｔｅｍ）またはＩＤＳ（Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）などのシステムがある。
これらのシステムは、アプリケーションまたはプロセスの動きをマルウェアの既知のパターンと照らし合わせてマルウェアを検出するものであり、未知のパターンを持つマルウェアを検出することができない。
【０００３】
特許文献１～４には、未知のマルウェアを検出するために、標的型攻撃が段階的に進行することを利用する手法が開示されている。未知のマルウェアとは、未知のパターンを持つマルウェアである。
これらの手法では、既知の攻撃の組み合わせが攻撃シナリオとして定義される。そして、プロセスの発生順序を攻撃シナリオと比較して攻撃の進行が検知される。
攻撃シナリオを用いて検知を行うことで、未知のマルウェアの挙動を検知することができる。しかし、互いに関係がない攻撃が一連の攻撃として検知されてしまう場合があり、誤検知が多く含まれる可能性がある。
【０００４】
特許文献５、６には、未知のマルウェアを検出するために、プロセス間の関係に注目して、不正なプロセスの挙動を検出する手法が開示されている。プロセス間の関係とは、具体的には、ネットワークアクセスとファイルアクセスとの関係、プロセス間の呼び出しの関係などである。
これらの手法では、端末でプロセスが発生する度にプロセス間の関係が更新される。そして、不正なプロセスが検出された場合、プロセス間の関係が探索され、検出されたプロセスに関係があるプロセスが不正なプロセスとして検出される。検出された不正なプロセスは、一連の攻撃を構成する。

【０００５】
特許文献７には、不正なプロセスを判定するために、ネットワークアクセスのログと端末のログとを組み合わせ、プロセス間の関係を保持する手法が開示されている。
この手法では、通信を監視するだけでは検出できない不正なプロセスが検知される。
【０００６】
特許文献５～７に開示された手法では、プロセス間の関係を作成し、プロセス間の関係を更新して最新の状態を維持しなければならない。また、不正なプロセスの挙動が検出された場合にプロセス間の関係を探索する必要がある。
プロセス間の全ての関係が保持される場合には、プロセス間の関係が複雑化および巨大化するため、効率的な探索が必要となる。
一方、終了したプロセスがプロセス間の関係から削除されれば、プロセス間の関係の複雑化および巨大化が回避される。しかし、削除されたプロセスが攻撃または攻撃間をつなぐプロセスであると後に判明した場合、正確な検出が困難となる。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２０１５－１２１９６８号公報
【特許文献２】国際公開第２０１４／１１２１８５号
【特許文献３】国際公開第２０１５／０５９７９１号
【特許文献４】国際公開第２０１４／０４５８２７号
【特許文献５】特表２０１１－５０１２７９号公報
【特許文献６】特表２０１３－５４３６２４号公報
【特許文献７】特開２０１１－０５３８９３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
本発明は、攻撃に関係するプロセス間の関係を探索できるようにすることを目的とする。
【課題を解決するための手段】
【０００９】
本発明のプロセス探索装置は、
検知された攻撃の種類の攻撃種類識別子と、攻撃が検知された時間帯に動作した動作プロセスの動作プロセス識別子とが互いに対応付けられた動作プロセスリストと、攻撃の検知が行われた時間帯に他のプロセスを操作した操作元プロセスの操作元プロセス識別子と、操作された他のプロセスである操作先プロセスの操作先プロセス識別子とが互いに対応付けられた操作プロセスリストとを記憶する記憶部と、
前記動作プロセスリストと前記操作プロセスリストとを用いて、異なる攻撃種類識別子に対応付けられた動作プロセス識別子の組に該当し、操作元プロセス識別子と操作先プロセス識別子との組に該当する間接プロセス識別子の組を探索する間接プロセス探索部とを備える。
【発明の効果】
【００１０】
本発明によれば、攻撃に関係するプロセス間の関係を示す関係プロセス識別子の組を探索することができる。
【図面の簡単な説明】
【００１１】
【図１】実施の形態１におけるプロセス探索システム１００の構成図。
【図２】実施の形態１におけるプロセス探索装置２００の構成図。
【図３】実施の形態１におけるプロセス探索方法のフローチャート。
【図４】実施の形態１における動作ログファイル３１０の構成図。

【図５】実施の形態１における攻撃ログファイル３２０の構成図。
【図６】実施の形態１における動作プロセスリスト３３０の構成図。
【図７】実施の形態１における動作プロセス抽出処理（Ｓ１２０）のフローチャート。
【図８】実施の形態１における操作プロセスリスト３４０の構成図。
【図９】実施の形態１における操作プロセス抽出処理（Ｓ１３０）のフローチャート。
【図１０】実施の形態１における直接プロセスの再帰的探索の概要図。
【図１１】実施の形態１における直接プロセス探索処理（Ｓ１４０）のフローチャート。
【図１２】実施の形態１における間接プロセスファイル３６０の構成図。
【図１３】実施の形態１における間接プロセス探索処理（Ｓ１５０）のフローチャート。
【図１４】実施の形態１における前探索処理（Ｓ２１０）のフローチャート。
【図１５】実施の形態１における前探索処理（Ｓ２１０）のフローチャート。
【図１６】実施の形態１におけるデータ生成処理（Ｓ２３０）のフローチャート。
【図１７】実施の形態１における後探索処理（Ｓ２２０）のフローチャート。
【図１８】実施の形態１における後探索処理（Ｓ２２０）のフローチャート。
【図１９】実施の形態１におけるプロセス構成例を示す図。
【図２０】実施の形態１における間接プロセスデータ３６１の例を示す図。
【図２１】実施の形態２におけるプロセス探索方法のフローチャート。
【図２２】実施の形態２における間接プロセス探索処理（Ｓ３００）のフローチャート。
【図２３】実施の形態２における後探索処理（Ｓ３１０）のフローチャート。
【図２４】実施の形態２における後探索処理（Ｓ３１０）のフローチャート。
【図２５】実施の形態２における間接プロセスデータ３６１の例を示す図。
【図２６】実施の形態２における間接プロセスファイル３６０を示す図。
【図２７】実施の形態におけるプロセス探索装置２００のハードウェア構成図。
【発明を実施するための形態】
【００１２】
実施の形態１.
プロセス探索システム１００について、図１から図２０に基づいて説明する。
【００１３】
＊＊＊構成の説明＊＊＊
図１に基づいて、プロセス探索システム１００の構成について説明する。
プロセス探索システム１００は、対象装置１１０に対する攻撃に関係するプロセスを探索するシステムである。
プロセス探索システム１００は、対象装置１１０と攻撃検知装置１２０とプロセス探索装置２００とを備える。
対象装置１１０は、攻撃の検知の対象である。
攻撃検知装置１２０は、対象装置１１０に対する攻撃を検知する。
プロセス探索装置２００は、対象装置１１０に対する攻撃に関係するプロセスを探索する。
対象装置１１０、攻撃検知装置１２０およびプロセス探索装置２００は、ネットワーク１０１を介して、互いに通信を行う。
【００１４】
対象装置１１０は、プロセッサ、メモリおよび通信装置などのハードウェアを備えるコンピュータである。
対象装置１１０は、ログ収集部１１１を機能構成の要素として備える。ログ収集部１１１の機能を実現するプログラムは、メモリにロードされて、プロセッサによって実行される。
ログ収集部１１１は、従来の技術でログを収集して、後述する動作ログファイル３１０を生成する。
【００１５】
攻撃検知装置１２０は、プロセッサ、メモリおよび通信装置などのハードウェアを備え

るコンピュータである。
攻撃検知装置１２０は、攻撃検知部１２１を機能構成の要素として備える。攻撃検知部１２１の機能を実現するプログラムは、メモリにロードされて、プロセッサによって実行される。
攻撃検知部１２１は、対象装置１１０に対する攻撃を従来の技術で検知して、後述する攻撃ログファイル３２０を生成する。
【００１６】
図２に基づいて、プロセス探索装置２００の構成について説明する。
プロセス探索装置２００は、プロセッサ９０１とメモリ９０２と補助記憶装置９０３と通信装置９０４といったハードウェアを備えるコンピュータである。プロセッサ９０１は、信号線を介して他のハードウェアと接続されている。
【００１７】
プロセッサ９０１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）であり、他のハードウェアを制御する。具体的には、プロセッサ９０１は、ＣＰＵ、ＤＳＰまたはＧＰＵである。ＣＰＵはＣｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略称であり、ＤＳＰはＤｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒの略称であり、ＧＰＵはＧｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略称である。
メモリ９０２は揮発性の記憶装置である。メモリ９０２は、主記憶装置またはメインメモリとも呼ばれる。具体的には、メモリ９０２はＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）である。
補助記憶装置９０３は不揮発性の記憶装置である。具体的には、補助記憶装置９０３は、ＲＯＭ、ＨＤＤまたはフラッシュメモリである。ＲＯＭはＲｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙの略称であり、ＨＤＤはＨａｒｄ Ｄｉｓｋ Ｄｒｉｖｅの略称である。
通信装置９０４は、通信を行う装置であり、レシーバ９０５とトランスミッタ９０６とを備える。具体的には、通信装置９０４は通信チップまたはＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）である。
【００１８】
プロセス探索装置２００は、プロセスリスト生成部２１０と直接プロセス探索部２２０と間接プロセス探索部２３０と攻撃判定部２４０といった「部」を機能構成の要素として備える。「部」の機能はソフトウェアで実現される。「部」の機能については後述する。
【００１９】
補助記憶装置９０３には、「部」の機能を実現するプログラムが記憶されている。「部」の機能を実現するプログラムは、メモリ９０２にロードされて、プロセッサ９０１によって実行される。
さらに、補助記憶装置９０３にはＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）が記憶されている。ＯＳの少なくとも一部は、メモリ９０２にロードされて、プロセッサ９０１によって実行される。
つまり、プロセッサ９０１は、ＯＳを実行しながら、「部」の機能を実現するプログラムを実行する。
「部」の機能を実現するプログラムを実行して得られるデータは、メモリ９０２、補助記憶装置９０３、プロセッサ９０１内のレジスタまたはプロセッサ９０１内のキャッシュメモリといった記憶装置に記憶される。これらの記憶装置は、データを記憶する記憶部２９１として機能する。
なお、プロセス探索装置２００が複数のプロセッサ９０１を備えて、複数のプロセッサ９０１が「部」の機能を実現するプログラムを連携して実行してもよい。
【００２０】
メモリ９０２には、プロセス探索装置２００で使用、生成、入出力または送受信されるデータが記憶される。
具体的には、メモリ９０２には、動作ログファイル３１０、攻撃ログファイル３２０、動作プロセスリスト３３０、操作プロセスリスト３４０、直接プロセスファイル３５０、

間接プロセスファイル３６０、攻撃判定結果３７０等が記憶される。メモリ９０２に記憶されるデータの内容については後述する。

【００２１】

通信装置９０４はデータを通信する通信部２９２として機能し、レシーバ９０５はデータを受信する受信部２９３として機能し、トランスミッタ９０６はデータを送信する送信部２９４として機能する。

【００２２】

プロセッサ９０１とメモリ９０２と補助記憶装置９０３とをまとめたハードウェアを「プロセッシングサーキットリ」という。

「部」は「処理」または「工程」に読み替えてもよい。「部」の機能はファームウェアで実現してもよい。

「部」の機能を実現するプログラムは、磁気ディスク、光ディスクまたはフラッシュメモリ等の不揮発性の記憶媒体に記憶することができる。

【００２３】

＊＊＊動作の説明＊＊＊

プロセス探索装置２００の動作はプロセス探索方法に相当する。また、プロセス探索方法の手順はプロセス探索プログラムの手順に相当する。

【００２４】

図３に基づいて、プロセス探索方法について説明する。

ステップＳ１１０は受信処理である。

ステップＳ１１０において、受信部２９３は、対象装置１１０から動作ログファイル３１０を受信する。

動作ログファイル３１０は、動作時刻と動作プロセス識別子と親プロセス識別子とが互いに対応付けられて、操作元プロセスに該当する動作プロセスの動作プロセス識別子に操作先プロセス識別子が対応付けられたデータである。

動作時刻は、動作プロセスが動作した時刻である。

動作プロセスは、動作時刻に動作したプロセスである。

動作プロセス識別子は、動作プロセスを識別するプロセス識別子である。

プロセス識別子は、プロセスを識別する識別子である。

親プロセス識別子は、親プロセスを識別する識別子である。

親プロセスは、動作プロセスを生成したプロセスである。

操作元プロセスは、他のプロセスを操作するプロセスである。

操作先プロセス識別子は、操作先プロセスを識別するプロセス識別子である。

操作先プロセスは、操作元プロセスに操作されるプロセスである。

【００２５】

図４に基づいて、動作ログファイル３１０の具体的な構成を説明する。

動作ログファイル３１０は、１つ以上の動作ログ３１１を含む。図中の一行が動作ログ３１１に相当する。

動作ログ３１１は、動作時刻と動作プロセス識別子と親プロセス識別子と動作種類と操作先プロセス識別子とを互いに対応付けて含む。

動作種類は、動作プロセスの動作の種類を示す情報である。

【００２６】

図３に戻り、ステップＳ１１０の説明を続ける。

さらに、受信部２９３は、攻撃検知装置１２０から攻撃ログファイル３２０を受信する。

攻撃ログファイル３２０は、攻撃種類識別子と攻撃時間帯とが互いに対応付けられたデータである。

攻撃種類識別子は、検知された攻撃の種類を識別する識別子である。具体的には、攻撃の順序を示す番号である。

攻撃時間帯は、攻撃が検知された時間帯である。具体的には、攻撃時間帯は、攻撃開始

時刻と攻撃終了時刻とで示される。
攻撃開始時刻は、攻撃時間帯の始まりの時刻である。
攻撃終了時刻は、攻撃時間帯の終わりの時刻である。
【００２７】
図５に基づいて、攻撃ログファイル３２０の具体的な構成を説明する。
攻撃ログファイル３２０は、１つ以上の攻撃ログ３２１を含む。図中の一行が攻撃ログ３２１に相当する。
攻撃ログ３２１は、攻撃種類識別子と攻撃開始時刻と攻撃終了時刻と攻撃種類と通信元アドレスと通信先アドレスとを互いに対応付けて含む。
攻撃種類は、攻撃の種類を示す情報である。
通信元アドレスは、攻撃として検知された不審な通信の通信元のアドレスである。具体的には、通信元アドレスはＩＰアドレスである。ＩＰはＩｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌの略称である。
通信先アドレスは、攻撃として検知された不審な通信の通信先のアドレスである。具体的には、通信先アドレスはＩＰアドレスである。
【００２８】
図３に戻り、ステップＳ１２０から説明を続ける。
ステップＳ１２０は、動作プロセスリスト３３０を生成するためのプロセス生成処理である。以下、ステップＳ１２０を動作プロセス抽出処理という。
ステップＳ１２０において、プロセスリスト生成部２１０は、動作ログファイル３１０と攻撃ログファイル３２０とを用いて、動作プロセスリスト３３０を生成する。
動作プロセスリスト３３０は、攻撃種類識別子と、動作プロセス識別子と、攻撃時間帯とが互いに対応付けられたデータである。
【００２９】
図６に基づいて、動作プロセスリスト３３０の具体的な構成を説明する。
動作プロセスリスト３３０は、１つ以上の動作プロセスデータ３３１を含む。図中の一行が動作プロセスデータ３３１に相当する。
動作プロセスデータ３３１は、攻撃種類識別子と攻撃開始時刻と攻撃終了時刻と動作プロセス識別子とを互いに対応付けて含む。
図６の動作プロセスリスト３３０は、図４の動作ログファイル３１０と図５の攻撃ログファイル３２０とを用いて生成される。
【００３０】
図７に基づいて、動作プロセス抽出処理（Ｓ１２０）の手順を説明する。
ステップＳ１２１において、プロセスリスト生成部２１０は、動作ログファイル３１０から、未選択の動作ログ３１１を１つ選択する。
具体的には、プロセスリスト生成部２１０は、動作時刻の早い順に、動作ログ３１１を１つずつ選択する。
【００３１】
ステップＳ１２２において、プロセスリスト生成部２１０は、選択された動作ログ３１１に対応する動作プロセスが抽出対象プロセスであるかを判定する。抽出対象プロセスは、抽出される対象となる動作プロセスである。
具体的には、プロセスリスト生成部２１０は、選択された動作ログ３１１から動作時刻を取得する。そして、プロセスリスト生成部２１０は、攻撃ログファイル３２０を参照して、取得された動作時刻がいずれかの攻撃時間帯に含まれるかを判定する。取得された動作時刻がいずれかの攻撃時間帯に含まれる場合、選択された動作ログ３１１に対応する動作プロセスは抽出対象プロセスである。
選択された動作ログ３１１に対応する動作プロセスが抽出対象プロセスである場合、処理はステップＳ１２３に進む。
選択された動作ログ３１１に対応する動作プロセスが抽出対象プロセスでない場合、処理はステップＳ１２５に進む。

【００３２】
ステップＳ１２３において、プロセスリスト生成部２１０は、選択された動作ログ３１１に対応する動作プロセスデータ３３１を生成する。
【００３３】
具体的には、プロセスリスト生成部２１０は、動作プロセスデータ３３１を以下のように生成する。
まず、プロセスリスト生成部２１０は、選択された動作ログ３１１から、動作時刻と動作プロセス識別子とを取得する。
次に、プロセスリスト生成部２１０は、攻撃ログファイル３２０から、取得された動作時刻を含んだ攻撃時間帯を選択する。
次に、プロセスリスト生成部２１０は、攻撃ログファイル３２０から、選択された攻撃時間帯に対応付けられた攻撃種類識別子と攻撃開始時刻と攻撃終了時刻とを取得する。
そして、プロセスリスト生成部２１０は、取得された攻撃種類識別子と攻撃開始時刻と攻撃取得時刻と動作プロセス識別子とを互いに対応付けて、動作プロセスデータ３３１を生成する。
【００３４】
ステップＳ１２４において、プロセスリスト生成部２１０は、生成された動作プロセスデータ３３１を動作プロセスリスト３３０に追加する。
【００３５】
ステップＳ１２５において、プロセスリスト生成部２１０は、動作ログファイル３１０に、未選択の動作ログ３１１があるか判定する。
未選択の動作ログ３１１がある場合、処理はステップＳ１２１に戻る。
未選択の動作ログ３１１がない場合、動作プロセス抽出処理（Ｓ１２０）は終了する。
【００３６】
図３に戻り、ステップＳ１３０から説明を続ける。
ステップＳ１３０は、操作プロセスリスト３４０を生成するためのプロセス生成処理である。以下、ステップＳ１３０を操作プロセス抽出処理という。
ステップＳ１３０において、プロセスリスト生成部２１０は、動作ログファイル３１０を用いて、操作プロセスリスト３４０を生成する。
操作プロセスリスト３４０は、操作元プロセス識別子と、操作先プロセス識別子とが互いに対応付けられたデータである。
操作元プロセス識別子は、操作元プロセスを識別する識別子である。
操作元プロセスは、操作先プロセスを操作した動作プロセスである。
【００３７】
図８に基づいて、操作プロセスリスト３４０の具体的な構成を説明する。
操作プロセスリスト３４０は、１つ以上の操作プロセスデータ３４１を含む。図中の一行が操作プロセスデータ３４１に相当する。
操作プロセスデータ３４１は、動作時刻と操作元プロセス識別子と動作種類と操作先プロセス識別子とを互いに対応付けて含む。
図８の動作プロセスリスト３３０は、図４の動作ログファイル３１０を用いて生成される。
【００３８】
図９に基づいて、操作プロセス抽出処理（Ｓ１３０）の手順を説明する。
ステップＳ１３１において、プロセスリスト生成部２１０は、動作ログファイル３１０から、未選択の動作ログ３１１を１つ選択する。
具体的には、プロセスリスト生成部２１０は、動作時刻の早い順に、動作ログ３１１を１つずつ選択する。但し、プロセスリスト生成部２１０は、全体の攻撃時間帯に含まれる動作時刻を含んだ動作ログ３１１を対象にして、動作ログ３１１を選択してもよい。全体の攻撃時間帯は、攻撃ログファイル３２０に含まれる最も早い攻撃開始時刻から、攻撃ログファイル３２０に含まれる最も遅い攻撃終了時刻までの時間帯である。

【００３９】
ステップＳ１３２において、プロセスリスト生成部２１０は、選択された動作ログ３１１に対応する動作プロセスが抽出対象プロセスであるかを判定する。抽出対象プロセスは、抽出される対象となる動作プロセスである。
具体的には、プロセスリスト生成部２１０は、選択された動作ログ３１１に操作先プロセス識別子が含まれるかを判定する。選択された動作ログ３１１に操作先プロセス識別子が含まれる場合、選択された動作ログ３１１に対応する動作プロセスは抽出対象プロセスである。
選択された動作ログ３１１に対応する動作プロセスが抽出対象プロセスである場合、処理はステップＳ１３３に進む。
選択された動作ログ３１１に対応する動作プロセスが抽出対象プロセスでない場合、処理はステップＳ１３５に進む。
【００４０】
ステップＳ１３３において、プロセスリスト生成部２１０は、選択された動作ログ３１１に対応する操作プロセスデータ３４１を生成する。
【００４１】
具体的には、プロセスリスト生成部２１０は、操作プロセスデータ３４１を以下のように生成する。
まず、プロセスリスト生成部２１０は、選択された動作ログ３１１から、動作プロセス識別子を操作元プロセス識別子として取得する。
また、プロセスリスト生成部２１０は、選択された動作ログ３１１から、動作時刻と動作種類と操作先プロセス識別子とを取得する。
そして、プロセスリスト生成部２１０は、取得された動作時刻と操作元プロセス識別子と動作種類と操作先プロセス識別子とを互いに対応付けて、操作プロセスデータ３４１を生成する。
【００４２】
ステップＳ１３４において、プロセスリスト生成部２１０は、生成された操作プロセスデータ３４１を操作プロセスリスト３４０に追加する。
【００４３】
ステップＳ１３５において、プロセスリスト生成部２１０は、動作ログファイル３１０に、未選択の動作ログ３１１があるか判定する。
未選択の動作ログ３１１がある場合、処理はステップＳ１３１に戻る。
未選択の動作ログ３１１がない場合、操作プロセス抽出処理（Ｓ１３０）は終了する。
【００４４】
図３に戻り、ステップＳ１４０から説明を続ける。
ステップＳ１４０は直接プロセス探索処理である。
ステップＳ１４０において、直接プロセス探索部２２０は、動作プロセスリスト３３０と動作ログファイル３１０とを用いて直接プロセス識別子の組を探索し、直接プロセスファイル３５０を生成する。
直接プロセス識別子の組は、動作プロセス識別子と親プロセス識別子との組に該当し、動作プロセスリスト３３０に含まれる動作プロセス識別子の組に該当する。
直接プロセスファイル３５０は、直接プロセス識別子の組を示すデータである。
【００４５】
図１０に基づいて、直接プロセスを再帰的に探索する処理の概要を説明する。
プロセス間の親子関係（呼び出し関係）は木構造で表すことができる。木構造において、プロセスがノードに相当し、プロセス間の親子関係がエッジに相当する。図１０において、丸はノードを示し、ノード同士を結ぶ線はエッジを示す。
プロセスＢに対応する攻撃開始時刻がプロセスＡに対応する攻撃開始時刻よりも後である場合、直接プロセス探索処理（Ｓ１４０）では、プロセスＢから親プロセスを再帰的に辿ってプロセスＡに到達する。

【００４６】
図１１に基づいて、直接プロセス探索処理（Ｓ１４０）の手順について説明する。
ステップＳ１４１において、直接プロセス探索部２２０は、動作プロセスリスト３３０から、未選択の動作プロセス識別子を１つ選択する。
具体的には、直接プロセス探索部２２０は、攻撃開始時刻の遅い順に、動作プロセス識別子を１つずつ選択する。
選択される動作プロセス識別子を子プロセス識別子という。
【００４７】
ステップＳ１４２において、直接プロセス探索部２２０は、子プロセス識別子に対応する親プロセス識別子が動作ログファイル３１０にあるか判定する。
子プロセス識別子に対応する親プロセス識別子とは、子プロセス識別子と同じ動作プロセス識別子に対応付けられた親プロセス識別子である。
子プロセス識別子に対応する親プロセス識別子が動作ログファイル３１０にある場合、処理はステップＳ１４３に進む。
子プロセス識別子に対応する親プロセス識別子が動作ログファイル３１０にない場合、処理はステップＳ１４６に進む。
【００４８】
ステップＳ１４３において、直接プロセス探索部２２０は、子プロセス識別子に対応する親プロセス識別子を、動作ログファイル３１０から取得する。
【００４９】
ステップＳ１４４において、直接プロセス探索部２２０は、取得された親プロセス識別子が検出プロセス識別子であるかを判定する。
検出プロセス識別子とは、動作プロセスリスト３３０に含まれる動作プロセス識別子である。
具体的には、直接プロセス探索部２２０は、取得された親プロセス識別子と同じ動作プロセス識別子が動作プロセスリスト３３０にあるか判定する。当該動作プロセス識別子が動作プロセスリスト３３０にある場合、取得された親プロセス識別子は検出プロセス識別子である。
取得された親プロセス識別子が検出プロセス識別子である場合、処理はステップＳ１４５に進む。
取得された親プロセス識別子が検出プロセス識別子でない場合、取得された親プロセス識別子が子プロセス識別子となり、処理はステップＳ１４２に戻る。
【００５０】
ステップＳ１４５において、直接プロセス探索部２２０は、取得された親プロセス識別子と選択された子プロセス識別子との組を、直接プロセス識別子の組として、直接プロセスファイル３５０に含める。
具体的には、直接プロセス探索部２２０は、親プロセス識別子と子プロセス識別子との組を含んだ直接プロセスデータを生成し、生成された直接プロセスデータを直接プロセスファイル３５０に追加する。
直接プロセスデータの構成は、後述する間接プロセスデータ３６１の構成と同じであり、直接プロセスデータは、起点プロセス識別子と探索種類識別子と探索プロセス識別子と関係情報と付加プロセス識別子とを含む。
生成される直接プロセスデータにおいて、起点プロセス識別子、探索種類識別子、探索プロセス識別子、関係情報および付加プロセス識別子は、以下の通りである。
起点プロセス識別子は、子プロセス識別子である。
探索種類識別子は、動作プロセスリスト３３０のうち、親プロセス識別子と同じ動作プロセス識別子に対応付けられた攻撃種類識別子である。
探索プロセス識別子は、親プロセス識別子である。
関係情報は、関係ありを示す。
付加プロセス識別子は、空欄である。

ステップＳ１４５の後、取得された親プロセス識別子が子プロセス識別子となり、処理はステップＳ１４２に戻る。

【００５１】

ステップＳ１４６において、直接プロセス探索部２２０は、子プロセス識別子として選択されていない未選択の動作プロセス識別子が動作プロセスリスト３３０にあるか判定する。

未選択の動作プロセス識別子がある場合、処理はステップＳ１４１に戻る。

未選択の動作プロセス識別子がない場合、直接プロセス探索処理（Ｓ１４０）は終了する。

【００５２】

図３に戻り、ステップＳ１５０から説明を続ける。

ステップＳ１５０は間接プロセス探索処理である。

ステップＳ１５０において、間接プロセス探索部２３０は、動作プロセスリスト３３０と操作プロセスリスト３４０とを用いて間接プロセス識別子の組を探索し、間接プロセスファイル３６０を生成する。

間接プロセス識別子の組は、異なる攻撃種類識別子に対応付けられた動作プロセス識別子の組に該当し、操作元プロセス識別子と操作先プロセス識別子との組に該当する。

間接プロセスファイル３６０は、間接プロセス識別子の組を示すデータである。

【００５３】

間接プロセス探索処理（Ｓ１５０）は、以下のような特徴を有する。

間接プロセス探索部２３０は、動作プロセスリスト３３０に含まれる攻撃種類識別子から、それぞれの攻撃種類識別子に対応付けられた動作プロセス識別子の個数に基づいて、起点種類識別子を選択する。起点種類識別子は、探索の起点となる攻撃種類識別子である。

間接プロセス探索部２３０は、起点種類識別子に対応付けられた動作プロセス識別子を用いて、間接プロセス識別子の組を探索する。

【００５４】

間接プロセス探索部２３０は、動作プロセスリスト３３０に含まれる攻撃種類識別子のうち、対応付けられた動作プロセス識別子の個数が最も少ない攻撃種類識別子を、起点種類識別子として選択する。

【００５５】

間接プロセス探索部２３０は、動作プロセスリスト３３０から、起点種類識別子に対応付けられた動作プロセス識別子を選択する。選択される動作プロセス識別子を起点プロセス識別子という。

間接プロセス探索部２３０は、動作プロセスリスト３３０から、起点種類識別子と異なる攻撃種類識別子を選択する。選択される攻撃種類識別子を探索種類識別子という。

間接プロセス探索部２３０は、動作プロセスリスト３３０から、探索種類識別子に対応付けられた動作プロセス識別子を選択する。選択される動作プロセス識別子を探索プロセス識別子という。

間接プロセス探索部２３０は、起点プロセス識別子と探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれるか判定する。

【００５６】

攻撃種類識別子は、攻撃の順序を示す番号である。

間接プロセス探索部２３０は、起点種類識別子が示す番号の１つ前の番号を示す攻撃種類識別子を選択する。選択される攻撃種類識別子が探索種類識別子である。

【００５７】

起点プロセス識別子と探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれ、探索種類識別子が示す番号が先頭番号である場合、間接プロセス探索部２３０は、起点プロセス識別子と探索プ

ロセス識別子との組を、間接プロセス識別子の組として生成する。

【００５８】

起点プロセス識別子と探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれるが、探索種類識別子が示す番号が先頭番号でない場合、間接プロセス探索部２３０は、以下のように動作する。

間接プロセス探索部２３０は、探索種類識別子に対応付けられた動作プロセス識別子を選択する。選択される動作プロセス識別子は新たな起点プロセス識別子である。

間接プロセス探索部２３０は、探索種類識別子が示す番号の１つ前の番号を示す攻撃種類識別子を選択する。選択される攻撃種類識別子は新たな探索種類識別子である。

間接プロセス探索部２３０は、新たな探索種類識別子に対応付けられた動作プロセス識別子を選択する。選択される動作プロセス識別子は新たな探索プロセス識別子である。

新たな起点プロセス識別子と新たな探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれ、新たな探索種類識別子が示す番号が先頭番号である場合、間接プロセス探索部２３０は次のように動作する。間接プロセス探索部２３０は、起点プロセス識別子と探索プロセス識別子との組と、新たな起点プロセス識別子と新たな探索プロセス識別子との組とを、間接プロセス識別子の組として生成する。

【００５９】

間接プロセス探索部２３０は、動作プロセスリスト３３０から、探索種類識別子に対応付けられた動作プロセス識別子のそれぞれを、攻撃開始時刻の早い順に、探索プロセス識別子として選択する。

【００６０】

間接プロセス探索部２３０は、探索プロセス識別子と同じ操作元プロセス識別子を操作プロセスリスト３４０から選択する。

間接プロセス探索部２３０は、選択された操作元プロセス識別子に対応付けられた操作先プロセス識別子を操作プロセスリスト３４０から取得する。取得される操作先プロセス識別子を付加プロセス識別子という。

起点プロセス識別子と探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれ、探索種類識別子が示す番号が先頭番号である場合、間接プロセス探索部２３０は、間接プロセス識別子の組を生成する。間接プロセス識別子の組は、起点プロセス識別子と探索プロセス識別子と付加プロセス識別子との組である。

【００６１】

探索プロセス識別子が、先に選択された探索プロセス識別子に対応する付加プロセス識別子と同じである場合、間接プロセス探索部２３０は、起点プロセス識別子と探索プロセス識別子との組に対する処理を省略する。

【００６２】

間接プロセス探索部２３０は、起点種類識別子が示す番号の１つ後の番号を示す攻撃種類識別子を選択する。選択される攻撃種類識別子は新たな探索種類識別子である。

間接プロセス探索部２３０は、新たな探索種類識別子に対応付けられた動作プロセス識別子を選択する。選択される動作プロセス識別子は新たな探索プロセス識別子である。

新たな起点プロセス識別子と新たな探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれる場合、間接プロセス探索部２３０は、新たな起点プロセス識別子と新たな探索プロセス識別子との組を、間接プロセス識別子の組として生成する。

【００６３】

間接プロセス探索部２３０は、動作プロセスリスト３３０から、探索種類識別子に対応付けられた動作プロセス識別子のそれぞれを、攻撃開始時刻の遅い順に、新たな探索プロセス識別子として選択する。

【００６４】

間接プロセス探索部２３０は、新たな探索プロセス識別子と同じ操作元プロセス識別子を操作プロセスリスト３４０から選択する。
間接プロセス探索部２３０は、選択された操作元プロセス識別子に対応付けられた操作元プロセス識別子を操作プロセスリスト３４０から取得する。取得される操作元プロセス識別子を付加プロセス識別子という。
間接プロセス探索部２３０は、付加プロセス識別子を、起点プロセス識別子と探索プロセス識別子との組に加える。
【００６５】
新たな探索プロセス識別子が、先に選択された探索プロセス識別子に対応する付加プロセス識別子と同じ識別子である場合、間接プロセス探索部２３０は、起点プロセス識別子と新たな探索プロセス識別子との組に対する処理を省略する。
【００６６】
図１２に基づいて、間接プロセスファイル３６０の具体的な構成を説明する。
間接プロセスファイル３６０は、１つ以上の間接プロセスデータ３６１を含む。図中の一行が間接プロセスデータ３６１に相当する。
間接プロセスデータ３６１は、起点プロセス識別子と探索種類識別子と探索プロセス識別子と関係情報と付加プロセス識別子とを互いに対応付けて含む。
起点プロセス識別子と探索プロセス識別子と付加プロセス識別子との組が、間接プロセス識別子の組に相当する。
起点プロセス識別子は、起点プロセスを識別する識別子である。
起点プロセスは、探索の起点となるプロセスである。
探索種類識別子は、探索の対象となる攻撃種類識別子である。
探索プロセス識別子は、探索プロセスを識別する識別子である。
探索プロセスは、探索の対象となる動作プロセスである。
関係情報は、起点プロセスと探索プロセスとの間に関係があるか否かを示す情報である。起点プロセスと探索プロセスとの間に関係がある場合、起点プロセス識別子と探索プロセス識別子とは間接プロセス識別子の組に含まれる。
付加プロセス識別子は、付加プロセスを識別する識別子である。
付加プロセスは、探索プロセスとの間に関係があるプロセスである。
【００６７】
図１３に基づいて、間接プロセス探索処理（Ｓ１５０）の手順を説明する。
ステップＳ１５１において、間接プロセス探索部２３０は、動作プロセスリスト３３０に含まれる攻撃種類識別子から、起点種類識別子を選択する。
起点種類識別子は、探索の起点となる攻撃種類識別子である。
【００６８】
具体的には、間接プロセス探索部２３０は、それぞれの攻撃種類識別子に対応付けられた動作プロセス識別子の個数に基づいて、起点種類識別子を選択する。
より具体的には、間接プロセス探索部２３０は、動作プロセスリスト３３０に含まれる攻撃種類識別子のうち、対応付けられた動作プロセス識別子の個数が最も少ない攻撃種類識別子を、起点種類識別子として選択する。
【００６９】
ステップＳ１５２において、間接プロセス探索部２３０は、動作プロセスリスト３３０から、未選択の動作プロセス識別子を起点プロセス識別子として選択する。
起点プロセス識別子は、起点種類識別子に対応付けられた動作プロセス識別子である。
具体的には、間接プロセス探索部２３０は、攻撃開始時刻の遅い順に、動作プロセス識別子を起点プロセス識別子として選択する。
【００７０】
ステップＳ２１０は前探索処理である。
前探索処理（Ｓ２１０）については後述する。
ステップＳ２１０の後、処理はステップＳ１５３に進む。

【００７１】
ステップＳ１５３において、間接プロセス探索部２３０は、後述する後探索フラグの値が１であるか判定する。
後探索フラグの値が１である場合、処理はステップＳ２２０に進む。
後探索フラグの値が０である場合、処理はステップＳ１５４に進む。
【００７２】
ステップＳ２２０は後探索処理である。
後探索処理（Ｓ２２０）については後述する。
ステップＳ２２０の後、処理はステップＳ１５４に進む。
【００７３】
ステップＳ１５４において、間接プロセス探索部２３０は、Ｓ１５２で起点プロセス識別子として選択されていない未選択の動作プロセス識別子があるか判定する。
未選択の動作プロセス識別子がある場合、処理はステップＳ１５２に戻る。
未選択の動作プロセス識別子がない場合、間接プロセス探索処理（Ｓ１５０）は終了する。
【００７４】
図１４および図１５に基づいて、前探索処理（Ｓ２１０）の手順を説明する。
ステップＳ２１１において、間接プロセス探索部２３０は、起点種類識別子が示す番号が先頭番号であるか判定する。
先頭番号は、先頭の攻撃の順番を示す番号である。具体的には、先頭番号は、動作プロセスリスト３３０に攻撃種類識別子として含まれる番号のうちの最も小さい番号である。
起点種類識別子が示す番号が先頭番号である場合、処理はステップＳ２１１１に進む。
起点種類識別子が示す番号が先頭番号でない場合、処理はステップＳ２１２に進む。
【００７５】
図１５に基づいて、ステップＳ２１１１から説明を続ける。
ステップＳ２１１１において、間接プロセス探索部２３０は、前回以前のデータ生成処理（Ｓ２３０）で生成されて破棄されていない間接プロセスデータ３６１から、関係ありを示す関係情報を含んだ間接プロセスデータ３６１を選択する。
【００７６】
ステップＳ２１１２において、間接プロセス探索部２３０は、選択された間接プロセスデータ３６１を間接プロセスファイル３６０に追加する。
【００７７】
ステップＳ２１１３において、間接プロセス探索部２３０は、後探索フラグに第１のフラグ値を設定する。
第１のフラグ値は、後探索処理（Ｓ２２０）が必要であることを意味する値である。具体的には、第１のフラグ値は１である。
Ｓ２１１３の後、前探索処理（Ｓ２１０）は終了する。
【００７８】
図１４に戻り、ステップＳ２１２から説明を続ける。
ステップＳ２１２において、間接プロセス探索部２３０は、動作プロセスリスト３３０から、起点種類識別子とは異なる攻撃種類識別子を、探索種類識別子として選択する。
具体的には、間接プロセス探索部２３０は、起点種類識別子が示す番号の１つ前の番号を示す攻撃種類識別子を、探索種類識別子として選択する。
【００７９】
ステップＳ２１３において、間接プロセス探索部２３０は、動作プロセスリスト３３０から、探索種類識別子に対応付けられた動作プロセス識別子のうち、未選択の動作プロセス識別子を選択する。選択される動作プロセス識別子を探索プロセス識別子という。
具体的には、間接プロセス探索部２３０は、それぞれの動作プロセス識別子に対応付けられた攻撃開始時刻に基づいて、攻撃開始時刻の早い順に、動作プロセス識別子を探索プロセス識別子として選択する。

【００８０】
ステップＳ２３０はデータ生成処理である。
ステップＳ２３０において、間接プロセス探索部２３０は、起点プロセス識別子と間接プロセス識別子との組に対応する間接プロセスデータ３６１を生成する。生成された間接プロセスデータ３６１は記憶部２９１に記憶される。
データ生成処理（Ｓ２３０）の詳細については後述する。
【００８１】
ステップＳ２１４において、間接プロセス探索部２３０は、ステップＳ２１３で探索プロセス識別子として選択されていない未選択の動作プロセス識別子があるか判定する。
未選択の動作プロセス識別子がある場合、処理はステップＳ２１３に戻る。
未選択の動作プロセス識別子がない場合、処理はステップＳ２１５に進む。
【００８２】
ステップＳ２１５において、間接プロセス探索部２３０は、直接プロセスファイル３５０に含まれる直接プロセスデータとステップＳ２３０で生成された間接プロセスデータ３６１とを用いて、関係プロセスがあるか判定する。
関係プロセスは、起点プロセスに関係がある探索プロセスである。
具体的には、直接プロセスデータがある場合、間接プロセス探索部２３０は、間接プロセスがあると判定する。また、関係ありを示す関係情報を含んだ間接プロセスデータ３６１がある場合、間接プロセス探索部２３０は、関係プロセスがあると判定する。
関係プロセスがある場合、処理はステップＳ２１６に進む。
【００８３】
関係プロセスがない場合、記憶部２９１は、ステップＳ２３０で生成されて記憶されている間接プロセスデータ３６１を破棄する。
また、間接プロセス探索部２３０は、後探索フラグに第２のフラグ値（０）を設定する。第２のフラグ値は、後探索処理（Ｓ２２０）が不要であることを意味する値である。具体的には、第２のフラグ値は０である。
その後、前探索処理（Ｓ２１０）は終了する。
【００８４】
ステップＳ２１６において、間接プロセス探索部２３０は、未選択の関係プロセス識別子を１つ選択する。
関係プロセス識別子は、関係プロセスを識別する識別子である。
具体的には、間接プロセス探索部２３０は、それぞれの関係プロセス識別子と同じ動作プロセス識別子に対応付けられた攻撃開始時刻を動作プロセスリスト３３０から取得する。そして、間接プロセス探索部２３０は、攻撃開始時刻が早い順に、関係プロセス識別子を選択する。
【００８５】
ステップＳ２１７において、間接プロセス探索部２３０は、新たな起点種類識別子に探索種類識別子を設定し、新たな起点プロセス識別子に選択された関係プロセス識別子を設定する。
そして、新たな起点種類識別子と新たな起点プロセス識別子との組に対する前探索処理（Ｓ２１０）が実行される。
この前探索処理（Ｓ２１０）の後、処理はステップＳ２１８に進む。
【００８６】
ステップＳ２１８において、間接プロセス探索部２３０は、ステップＳ２１６で選択されていない未選択の関係プロセス識別子があるか判定する。
未選択の関係プロセス識別子がある場合、処理はステップＳ２１６に戻る。
未選択の関係プロセス識別子がない場合、前探索処理（Ｓ２１０）は終了する。
【００８７】
図１６に基づいて、データ生成処理（Ｓ２３０）の手順を説明する。
ステップＳ２３１において、間接プロセス探索部２３０は、探索プロセス識別子が探索

済みの付加プロセス識別子と同じであるか判定する。
探索済みの付加プロセス識別子は、前回以前に選択された探索プロセス識別子に対応する付加プロセス識別子である。
具体的には、間接プロセス探索部２３０は、前回以前のデータ生成処理（Ｓ２３０）で生成されて記憶されている間接プロセスデータ３６１に、探索プロセス識別子と同じ付加プロセス識別子があるか判定する。当該付加プロセス識別子がある場合、探索プロセス識別子は、探索済みの付加プロセス識別子と同じである。
探索プロセス識別子が探索済みの付加プロセス識別子と同じである場合、データ生成処理（Ｓ２３０）は終了する。これにより、ステップＳ２３２からステップＳ２３４までの処理が省略される。
探索プロセス識別子が探索済みの付加プロセス識別子と異なる場合、処理はステップＳ２３２に進む。
【００８８】
ステップＳ２３２において、間接プロセス探索部２３０は、起点プロセスと探索プロセスとの間に関係があるか判定する。
具体的には、間接プロセス探索部２３０は、起点プロセス識別子と探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれるか判定する。
起点プロセス識別子と探索プロセス識別子との組に該当する操作先プロセス識別子と操作元プロセス識別子との組が操作プロセスリスト３４０に含まれる場合、起点プロセスと探索プロセスとの間に関係がある。
【００８９】
より具体的には、間接プロセス探索部２３０は以下のように判定を行う。
まず、間接プロセス探索部２３０は、操作プロセスリスト３４０から、起点プロセス識別子と同じ操作先プロセス識別子を含んだ操作プロセスデータ３４１を検索する。
そして、間接プロセス探索部２３０は、いずれかの操作プロセスデータ３４１に含まれる操作元プロセス識別子が探索プロセス識別子と同じであるか判定する。
【００９０】
ステップＳ２３３において、間接プロセス探索部２３０は、探索プロセス識別子に対応する付加プロセス識別子を取得する。
具体的には、間接プロセス探索部２３０は、付加プロセス識別子を以下のように取得する。
まず、間接プロセス探索部２３０は、探索プロセス識別子と同じ操作元プロセス識別子を操作プロセスリスト３４０から選択する。
そして、間接プロセス探索部２３０は、選択された操作元プロセス識別子に対応付けられた操作先プロセス識別子を、操作プロセスリスト３４０から取得する。取得される操作先プロセス識別子が付加プロセス識別子である。
【００９１】
ステップＳ２３４において、間接プロセス探索部２３０は、間接プロセスデータ３６１を生成する。
具体的には、間接プロセス探索部２３０は、起点プロセス識別子と探索種類識別子と探索プロセス識別子と関係情報と付加プロセス識別子とを含んだ間接プロセスデータ３６１を生成する。関係情報は、ステップＳ２３２で判定された結果を示す。
記憶部２９１は、生成された間接プロセスデータ３６１を記憶する。
ステップＳ２３４の後、データ生成処理（Ｓ２３０）は終了する。
【００９２】
図１７および図１８に基づいて、後探索処理（Ｓ２２０）の手順を説明する。
後探索処理（Ｓ２２０）のステップＳ２２１からステップＳ２２８は、前探索処理（Ｓ２１０）のステップＳ２１１からステップＳ２１８に対応する。
【００９３】

ステップＳ２２１において、間接プロセス探索部２３０は、起点種類識別子が示す番号が最終番号であるか判定する。
最終番号は、最終の攻撃の順番を示す番号である。具体的には、最終番号は、動作プロセスリスト３３０に攻撃種類識別子として含まれる番号のうちの最も大きい番号である。
起点種類識別子が示す番号が最終番号である場合、処理はステップＳ２２１１に進む。
起点種類識別子が示す番号が最終番号でない場合、処理はステップＳ２２２に進む。
【００９４】
図１８に基づいて、ステップＳ２２１１から説明を続ける。
ステップＳ２２１１において、間接プロセス探索部２３０は、前回以前のデータ生成処理（Ｓ２３０）で生成されて破棄されていない間接プロセスデータ３６１から、関係ありを示す関係情報を含んだ間接プロセスデータ３６１を選択する。
【００９５】
ステップＳ２２１２において、間接プロセス探索部２３０は、選択された間接プロセスデータ３６１を間接プロセスファイル３６０に追加する。
ステップＳ２２１２の後、後探索処理（Ｓ２２０）は終了する。
【００９６】
図１７に戻り、ステップＳ２２２から説明を続ける。
ステップＳ２２２において、間接プロセス探索部２３０は、動作プロセスリスト３３０から、起点種類識別子とは異なる攻撃種類識別子を、探索種類識別子として選択する。
具体的には、間接プロセス探索部２３０は、起点種類識別子が示す番号の１つ後の番号を示す攻撃種類識別子を、探索種類識別子として選択する。
【００９７】
ステップＳ２２３において、間接プロセス探索部２３０は、動作プロセスリスト３３０から、探索種類識別子に対応付けられた動作プロセス識別子のうち、未選択の動作プロセス識別子を選択する。選択される動作プロセス識別子を探索プロセス識別子という。
具体的には、間接プロセス探索部２３０は、それぞれの動作プロセス識別子に対応付けられた攻撃開始時刻に基づいて、攻撃開始時刻の遅い順に、動作プロセス識別子を探索プロセス識別子として選択する。但し、間接プロセス探索部２３０は、起点プロセス識別子に対応付けられた攻撃開始時刻よりも早い時刻に対応付けられた動作プロセス識別子を選択しない。
【００９８】
ステップＳ２３０において、間接プロセス探索部２３０は、起点プロセス識別子と間接プロセス識別子との組に対応する間接プロセスデータ３６１を生成する。生成された間接プロセスデータ３６１は記憶部２９１に記憶される。
【００９９】
ステップＳ２２４において、間接プロセス探索部２３０は、ステップＳ２２３で探索プロセス識別子として選択されていない未選択の動作プロセス識別子があるか判定する。
未選択の動作プロセス識別子がある場合、処理はステップＳ２２３に戻る。
未選択の動作プロセス識別子がない場合、処理はステップＳ２２５に進む。
【０１００】
ステップＳ２２５において、間接プロセス探索部２３０は、直接プロセスファイル３５０に含まれる直接プロセスデータとステップＳ２３０で生成された間接プロセスデータ３６１とを用いて、関係プロセスがあるか判定する。判定方法は、前探索処理（Ｓ２１０）のステップＳ２１５と同じである。
関係プロセスがある場合、処理はステップＳ２２６に進む。
関係プロセスがない場合、記憶部２９１は、ステップＳ２３０で生成されて記憶されている間接プロセスデータ３６１を破棄する。そして、後探索処理（Ｓ２２０）は終了する。
【０１０１】
ステップＳ２２６において、間接プロセス探索部２３０は、未選択の関係プロセス識別

子を１つ選択する。
具体的には、間接プロセス探索部２３０は、それぞれの関係プロセス識別子と同じ動作プロセス識別子に対応付けられた攻撃開始時刻を動作プロセスリスト３３０から取得する。そして、間接プロセス探索部２３０は、攻撃開始時刻が遅い順に、関係プロセス識別子を選択する。
【０１０２】
ステップＳ２２７において、間接プロセス探索部２３０は、新たな起点種類識別子に探索種類識別子を設定し、新たな起点プロセス識別子に選択された関係プロセス識別子を設定する。
そして、新たな起点種類識別子と新たな起点プロセス識別子との組に対する後探索処理（Ｓ２２０）が実行される。
この後探索処理（Ｓ２２０）の後、処理はステップＳ２２８に進む。
【０１０３】
ステップＳ２２８において、間接プロセス探索部２３０は、ステップＳ２２６で選択されていない未選択の関係プロセス識別子があるか判定する。
未選択の関係プロセス識別子がある場合、処理はステップＳ２２６に戻る。
未選択の関係プロセス識別子がない場合、後探索処理（Ｓ２２０）は終了する。
【０１０４】
図１９に、プロセス群の構成例を示す。
図１９において、アルファベットが付された丸は、プロセスを示している。また、横軸は時刻を示し、縦軸は攻撃ステップの番号を示す。攻撃ステップは、攻撃種類識別子に相当する。
【０１０５】
攻撃ステップ「３」が起点となる場合、時刻の遅い順、つまり、プロセスＨ、プロセスＧの順に、起点プロセスが選択される。
攻撃ステップ「３」が起点となる場合、攻撃ステップ「２」が探索の対象となる。このとき、時刻の早い順、つまり、プロセスＤ、プロセスＥ、プロセスＦの順に、探索プロセスが選択される。
起点プロセスＨは探索プロセスＥと関係があるため、攻撃ステップ「２」が新たな起点となり、探索プロセスＥが新たな起点プロセスとなり、攻撃ステップ「１」が新たな探索の対象となる。このとき、時刻の早い順、つまり、プロセスＡ、プロセスＢ、プロセスＣの順に、探索プロセスが選択される。
起点プロセスＥは探索プロセスＡと関係があり、探索プロセスＡは付加プロセスＣと関係がある。また、起点プロセスＥは探索プロセスＢと関係がない。起点プロセスＥと探索プロセスＣとの関係については、プロセスＣが付加プロセスとして抽出されているため、探索が省略される。
攻撃ステップ「３」から攻撃ステップ「１」までの関係が抽出されたため、攻撃ステップ「４」が探索の対象となる。このとき、起点プロセスＥと探索プロセスＩとの間に関係はない。
その結果、プロセスＡとプロセスＣとプロセスＥとプロセスＨとの組が間接プロセスの組として抽出される。
【０１０６】
起点プロセスＧについても同様に探索が行われる。
攻撃ステップ「２」が探索の対象となり、時刻の早い順に、つまり、プロセスＤ、プロセスＥの順に、探索プロセスが選択される。プロセスＦは起点プロセスＧの後に動作したプロセスであるため、プロセスＦは探索プロセスとして選択されない。
起点プロセスＧと探索プロセスＤとの間に関係があるため、攻撃ステップ「２」が新たな起点となり、探索プロセスＤが新たな起点プロセスとなり、攻撃ステップ「１」が新たな探索の対象となる。このとき、時刻の早い順、つまり、プロセスＡ、プロセスＢの順に、探索プロセスが選択される。プロセスＣは起点プロセスＤの後に動作したプロセスであ

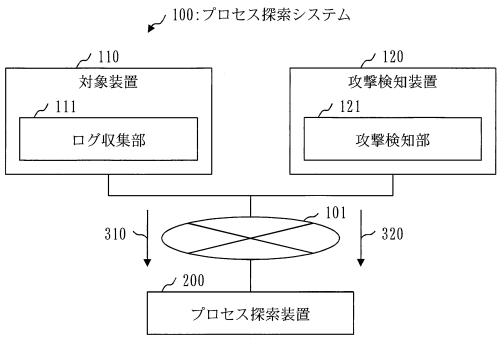
るため、プロセスＣは探索プロセスとして選択されない。
起点プロセスＤと探索プロセスＡ、Ｂとの間に関係がない。
その結果、攻撃ステップ「３」から攻撃ステップ「１」までの関係が抽出されず、プロセスＧを含んだ間接プロセスの組は抽出されない。
【０１０７】
図２０に、図１９のプロセス群を対象にして間接プロセス探索処理（Ｓ１５０）が行われた場合に生成される間接プロセスデータ３６１を示す。間接プロセスデータ３６１の一部は、直接プロセスデータである。
図２０の間接プロセスデータ３６１のうち、関係ありを示す関係情報を含んだ間接プロセスデータ３６１が、図１２の間接プロセスファイル３６０に登録される。
【０１０８】
図３に戻り、ステップＳ１６０から説明を続ける。
ステップＳ１６０は攻撃判定処理である。
ステップＳ１６０において、攻撃判定部２４０は、間接プロセスファイル３６０を用いて、攻撃に関係するプロセス間の関係を判定する。そして、攻撃判定部２４０は、攻撃判定結果３７０を生成する。
具体的には、攻撃判定部２４０は、間接プロセスファイル３６０から間接プロセス識別子の組を抽出し、間接プロセス識別子の組を示す攻撃判定結果３７０を生成する。間接プロセス識別子の組の一部は、直接プロセス識別子の組である。
【０１０９】
＊＊＊実施の形態１の効果＊＊＊
動作ログファイル３１０と攻撃ログファイル３２０とを用いて、攻撃に関係するプロセス間の関係を探索することができる。
選択された起点から探索が行われるため、探索経路が絞られて、効率的に探索が行われる。
【０１１０】
＊＊＊他の構成＊＊＊
プロセス探索システム１００において、対象装置１１０と攻撃検知装置１２０とプロセス探索装置２００とのうちの２つまたは３つの装置が１つの装置であってもよい。
【０１１１】
実施の形態２．
動作プロセスリスト３３０に含まれる全ての動作プロセス識別子を対象にして探索を行う形態について、図２１から図２６に基づいて説明する。但し、実施の形態１と重複する説明は省略または簡略する。
【０１１２】
＊＊＊構成の説明＊＊＊
プロセス探索システム１００の構成は、実施の形態１と同じである。
プロセス探索装置２００の構成は、実施の形態１と同じである。
【０１１３】
＊＊＊動作の説明＊＊＊
図２１に基づいて、プロセス探索方法について説明する。
ステップＳ１１０からステップＳ１４０まで、および、ステップＳ１６０は、実施の形態１と同じである。
ステップＳ３００は、実施の形態１におけるステップＳ１５０に対応する。
【０１１４】
ステップＳ３００は、間接プロセス探索処理である。
ステップＳ３００において、間接プロセス探索部２３０は、動作プロセスリスト３３０と操作プロセスリスト３４０とを用いて間接プロセス識別子の組を探索し、間接プロセスファイル３６０を生成する。
【０１１５】

図２２に基づいて、間接プロセス探索処理（Ｓ３００）の手順を説明する。
ステップＳ３０１において、間接プロセス探索部２３０は、動作プロセスリスト３３０に含まれる攻撃種類識別子から、起点種類識別子を選択する。
具体的には、間接プロセス探索部２３０は、先頭番号を示す攻撃種類識別子を、起点種類識別子として選択する。
【０１１６】
ステップＳ３０２において、間接プロセス探索部２３０は、動作プロセスリスト３３０から、未選択の動作プロセス識別子を起点プロセス識別子として選択する。
具体的には、間接プロセス探索部２３０は、攻撃開始時刻の早い順に、動作プロセス識別子を起点プロセス識別子として選択する。
【０１１７】
ステップＳ３１０は後探索処理である。
後探索処理（Ｓ３１０）については後述する。
ステップＳ３１０の後、処理はステップＳ３０３に進む。
【０１１８】
ステップＳ３０３において、間接プロセス探索部２３０は、ステップＳ３０２で起点プロセス識別子として選択されていない未選択の動作プロセス識別子があるか判定する。
未選択の動作プロセス識別子がある場合、処理はステップＳ３０２に戻る。
未選択の動作プロセス識別子がない場合、間接プロセス探索処理（Ｓ３００）は終了する。
【０１１９】
図２３および図２４に基づいて、後探索処理（Ｓ３１０）の手順を説明する。
ステップＳ３１１からステップＳ３１８までの処理は、実施の形態１において図１７に基づいて説明したステップＳ２２１からステップＳ２２８までの処理と同じである。
但し、ステップＳ３１１において、起点種類識別子が示す番号が最終番号である場合、処理はステップＳ３２１に進む。
また、ステップＳ３１５において、関係プロセスがない場合、処理はステップＳ３２１に進む。
【０１２０】
図２４に基づいて、ステップＳ３２１およびステップＳ３２２を説明する。
ステップＳ３２１およびステップＳ３２２は、実施の形態１において図１８に基づいて説明したステップＳ２２１１およびステップＳ２２１２と同じである。
【０１２１】
図１９のプロセス群を例にして、間接プロセス探索処理（Ｓ３００）の流れを説明する。
攻撃ステップ「１」が起点となり、時刻の早い順、つまり、プロセスＡ、プロセスＢ、プロセスＣの順に、起点プロセスが選択される。
攻撃ステップ「１」が起点となる場合、攻撃ステップ「２」が探索の対象となる。このとき、時刻の遅い順、つまり、プロセスＦ、プロセスＥ、プロセスＤの順に、探索プロセスが選択される。
起点プロセスＡは探索プロセスＥと関係があり、起点プロセスＡは付加プロセスＣと関係がある。
次に、攻撃ステップ「２」が新たな起点となり、探索プロセスＥが新たな起点プロセスとなり、攻撃ステップ「３」が新たな探索の対象となる。そして、プロセスＨが探索プロセスとして選択される。
起点プロセスＥは探索プロセスＨと関係があるため、攻撃ステップ「３」が新たな起点となり、探索プロセスＨが新たな起点プロセスとなり、攻撃ステップ「４」が新たな探索の対象となる。そして、プロセスＩが探索プロセスとして選択される。
起点プロセスＨは探索プロセスＩと関係がないため、探索は終了する。
この結果、プロセスＡとプロセスＣとプロセスＥとプロセスＨとの組が間接プロセスの

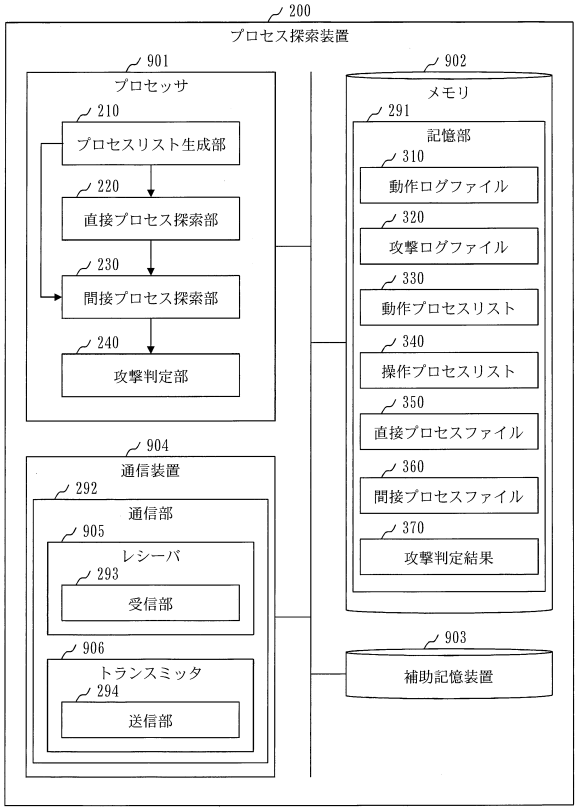
組として抽出される。
【０１２２】
起点プロセスＢについても同様に探索が行われる。
攻撃ステップ「２」が探索の対象となるが、起点プロセスＢは探索プロセスＦ、Ｅ、Ｄのいずれとも関係がない。そのため、探索は終了する。
【０１２３】
起点プロセスＣについても同様に探索が行われる。
攻撃ステップ「２」が探索の対象となり、プロセスＦが探索プロセスとして選択される。プロセスＤは起点プロセスＣよりも前に動作したプロセスであるため、プロセスＤは探索プロセスとして選択されない。また、プロセスＥは付加プロセスとして抽出されているため、プロセスＥは探索プロセスとして選択されない。
起点プロセスＣは探索プロセスＦと関係がないため、探索は終了する。
【０１２４】
図２５に、図１９のプロセス群を対象にして間接プロセス探索処理（Ｓ３００）が行われた場合に生成される間接プロセスデータ３６１を示す。
図２６に、図２５の間接プロセスデータ３６１から間接プロセスの組を示す間接プロセスデータ３６１が抽出されて、生成される間接プロセスファイル３６０を示す。
【０１２５】
＊＊＊実施の形態２の効果＊＊＊
先頭番号の攻撃種類識別子が起点となるため、動作プロセスリスト３３０に含まれる全ての動作プロセスを対象にして探索を行うことができる。
【０１２６】
＊＊＊実施の形態の補足＊＊＊
実施の形態において、プロセス探索装置２００の機能はハードウェアで実現してもよい。
図２７に、プロセス探索装置２００の機能がハードウェアで実現される場合の構成を示す。
プロセス探索装置２００は処理回路９９０を備える。処理回路９９０はプロセッシングサーキットリともいう。
処理回路９９０は、実施の形態で説明した「部」の機能を実現する専用の電子回路である。この「部」には記憶部２９１も含まれる。
具体的には、処理回路９９０は、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ロジックＩＣ、ＧＡ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。ＧＡはＧａｔｅ　Ａｒｒａｙの略称であり、ＡＳＩＣはＡｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔの略称であり、ＦＰＧＡはＦｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙの略称である。
なお、プロセス探索装置２００が複数の処理回路９９０を備えて、複数の処理回路９９０が「部」の機能を連携して実現してもよい。
【０１２７】
プロセス探索装置２００の機能は、ソフトウェアとハードウェアとの組み合わせで実現してもよい。つまり、「部」の一部をソフトウェアで実現し、「部」の残りをハードウェアで実現してもよい。
【０１２８】
実施の形態は、好ましい形態の例示であり、本発明の技術的範囲を制限することを意図するものではない。実施の形態は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。
【符号の説明】
【０１２９】
１００　プロセス探索システム、１０１　ネットワーク、１１０　対象装置、１１１

ログ収集部、１２０　攻撃検知装置、１２１　攻撃検知部、２００　プロセス探索装置、２１０　プロセスリスト生成部、２２０　直接プロセス探索部、２３０　間接プロセス探索部、２４０　攻撃判定部、２９１　記憶部、２９２　通信部、２９３　受信部、２９４　送信部、３１０　動作ログファイル、３１１　動作ログ、３２０　攻撃ログファイル、３２１　攻撃ログ、３３０　動作プロセスリスト、３３１　動作プロセスデータ、３４０　操作プロセスリスト、３４１　操作プロセスデータ、３５０　直接プロセスファイル、３６０　間接プロセスファイル、３６１　間接プロセスデータ、３７０　攻撃判定結果、９０１　プロセッサ、９０２　メモリ、９０３　補助記憶装置、９０４　通信装置、９０５　レシーバ、９０６　トランスミッタ、９９０　処理回路。

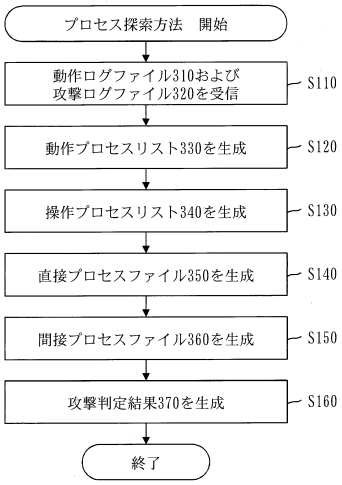
【図１】



【図２】



【図３】



【図４】

310:動作ログファイル

動作時刻	動作プロセス識別子	親プロセス識別子	動作種類	操作先プロセス識別子
18:00:01	413	0	起動	-
18:02:03	413	0	通信	-
18:04:14	24	375	通信	-
18:05:20	24	375	ファイル操作	375
18:05:28	154	413	通信	-
18:06:54	4	0	ファイル操作	4
18:06:55	154	413	終了	-
18:10:43	413	0	終了	-
18:11:44	1548	413	通信	-
18:12:34	1548	413	ファイル操作	375
18:13:55	375	1548	通信	-
18:21:11	126	4129	通信	-
18:25:09	375	1548	ファイル操作	552
18:28:51	552	4	起動	-
18:30:38	126	4129	終了	-
18:33:38	552	4	通信	-

311

【図５】

320:攻撃ログファイル

攻撃種類識別子	攻撃開始時刻	攻撃終了時刻	攻撃種類	通信元アドレス	通信先アドレス
1	18:02:00	18:02:10	侵入	192.168.1.1	192.168.1.3
	18:05:23	18:05:50	侵入	192.168.1.1	192.168.1.5
2	18:04:10	18:04:19	感染	192.168.1.1	192.168.1.5
	18:11:27	18:11:50	感染	192.168.1.1	192.168.1.3
3	18:21:05	18:21:29	探索	192.168.1.1	192.168.1.3
4	18:13:52	18:14:00	漏洩	192.168.1.1	192.168.1.7
	18:33:33	18:34:44	漏洩	192.168.1.1	192.168.1.3

321

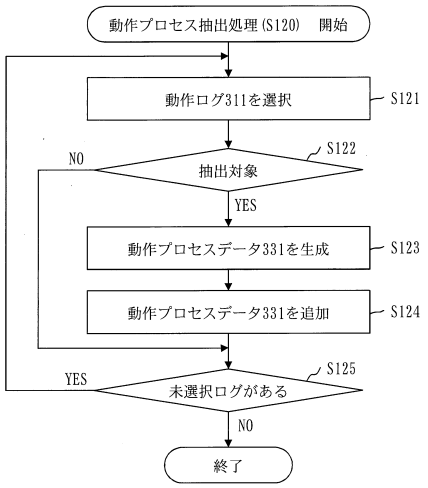
【図６】

330:動作プロセスリスト

攻撃種類識別子	攻撃開始時刻	攻撃終了時刻	動作プロセス識別子
1	18:02:00	18:02:10	413
1	18:05:23	18:05:50	154
2	18:04:10	18:04:19	24
2	18:11:27	18:11:50	1548
3	18:21:05	18:21:29	126
4	18:13:52	18:14:00	375
4	18:33:33	18:34:44	552

331

【図７】



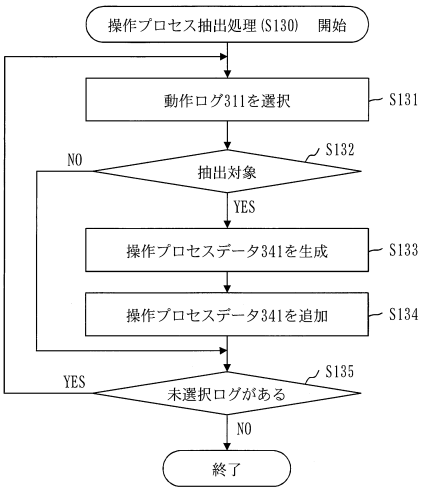
【図８】

340:操作プロセスリスト

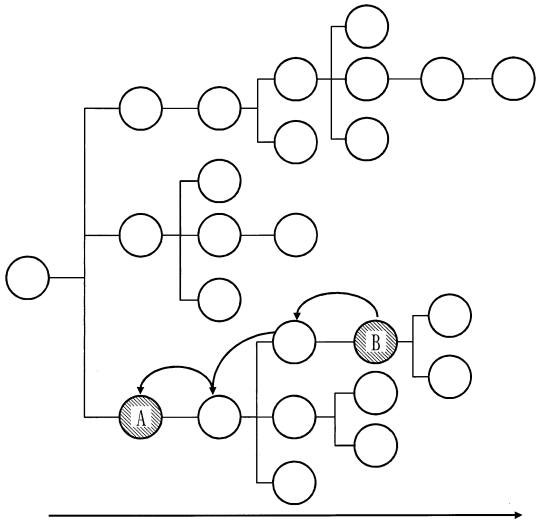
動作時刻	操作元プロセス識別子	動作種類	操作先プロセス識別子
18:05:20	24	ファイル操作	375
18:06:54	4	ファイル操作	4
18:12:34	1548	ファイル操作	375
18:25:09	375	ファイル操作	552

341

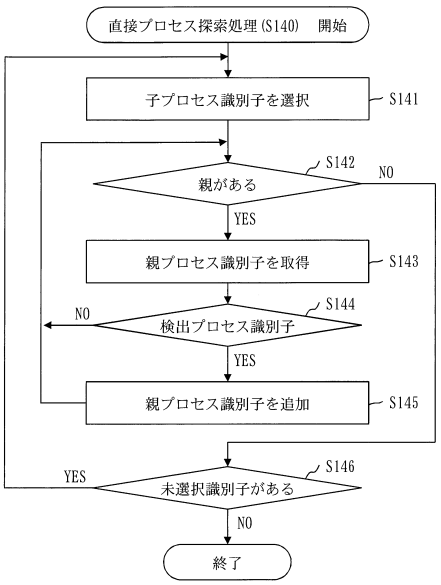
【図９】



【図１０】



【図１１】



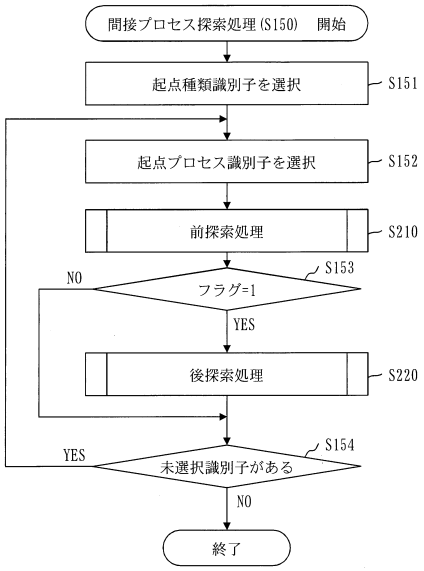
【図１２】

360:間接プロセスファイル

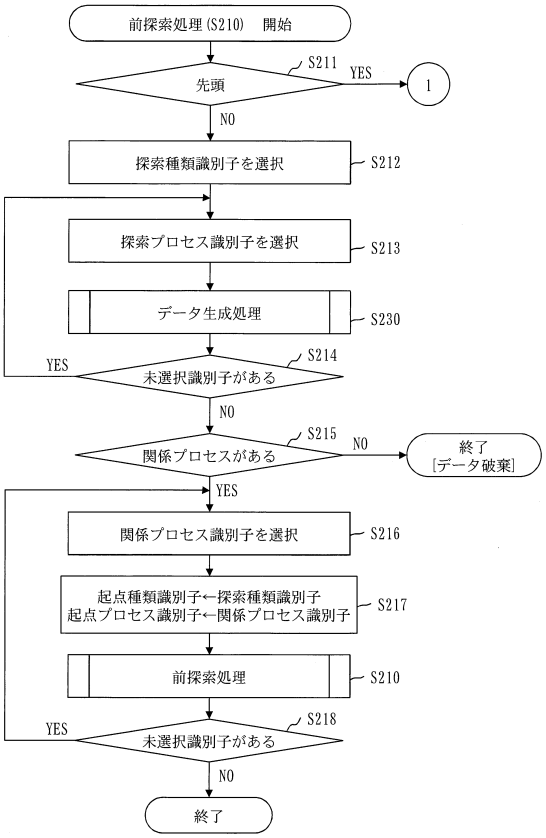
起点プロセス識別子	探索種類識別子	探索プロセス識別子	関係情報	付加プロセス識別子
H	2	E	あり	-
E	1	A	あり	C

361

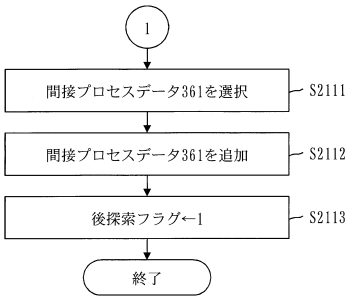
【図１３】



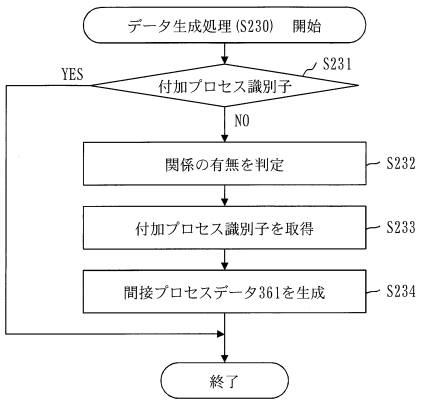
【図１４】



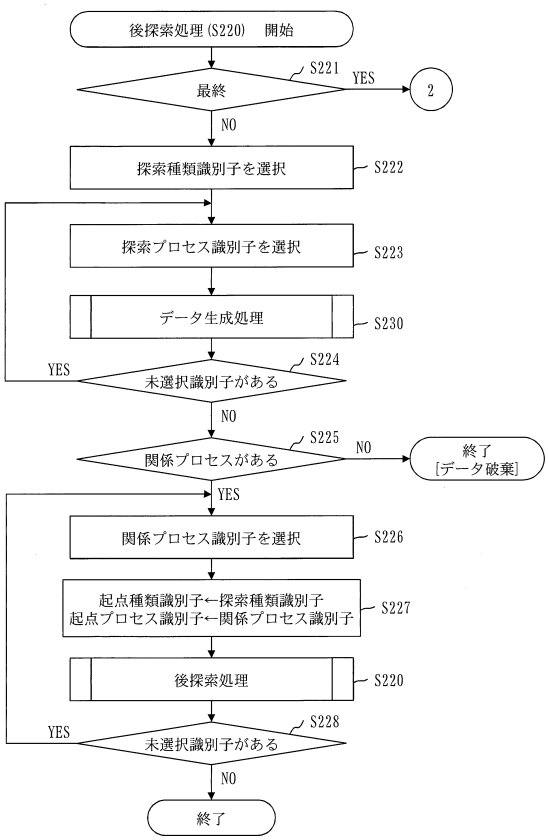
【図１５】



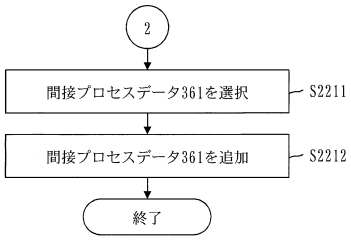
【図１６】



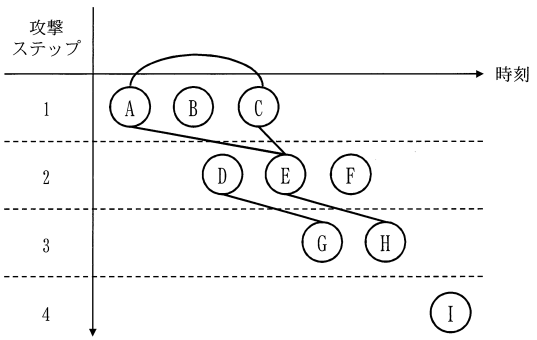
【図１７】



【図１８】



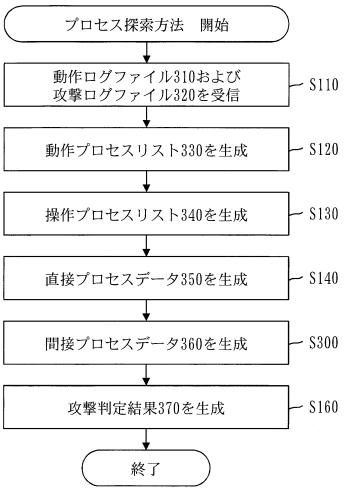
【図１９】



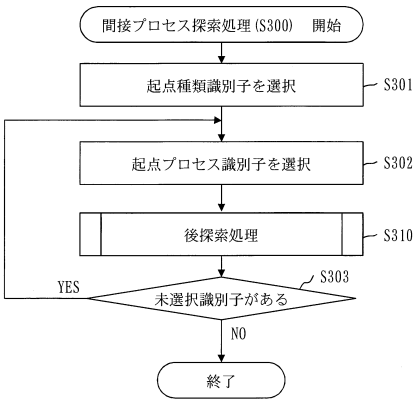
【図２０】

起点プロセス識別子	探索種類識別子	探索プロセス識別子	関係情報	付加プロセス識別子	
H	2	D	なし	-	361
H	2	E	あり	-	361
H	2	F	なし	-	361
E	1	A	あり	C	361
E	1	B	なし	-	361
E	1	C	-	-	361
H	4	I	なし	-	361
G	2	D	あり	-	361
G	2	E	なし	-	361
D	1	A	なし	-	361
D	1	B	なし	-	361

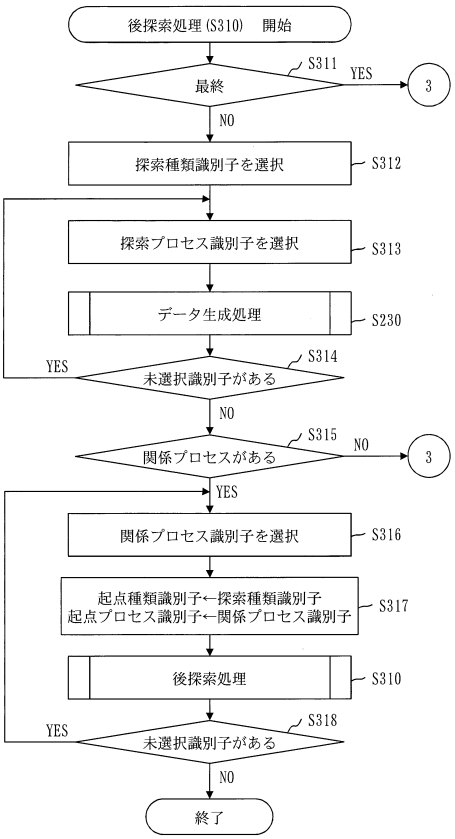
【図２１】



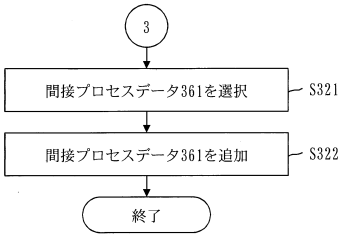
【図２２】



【図２３】



【図２４】



【図２５】

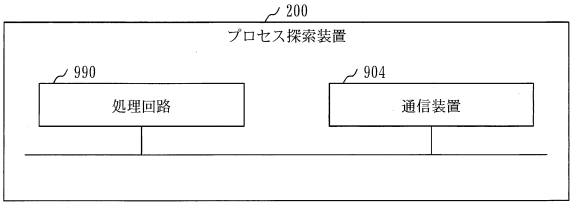
起点プロセス識別子	探索種類識別子	探索プロセス識別子	関係情報	付加プロセス識別子	
A	2	F	なし	-	361
A	2	E	あり	C	361
A	2	D	なし	-	361
E	3	H	あり	-	361
E	3	G	なし	-	361
H	4	I	なし	-	361
B	2	F	なし	-	361
B	2	E	なし	-	361
B	2	D	なし	-	361
F	3	H	なし	-	361
C	2	F	なし	-	361
C	2	E	-	-	361

【図２６】

360:間接プロセスファイル

起点プロセス識別子	探索ステップ	探索プロセス識別子	関係情報	付加プロセス識別子	
A	2	E	あり	C	361
E	3	H	あり	-	

【図２７】



フロントページの続き

(56)参考文献 特開２００６－１１９７５４（ＪＰ，Ａ）
特開２０１０－１８２０２０（ＪＰ，Ａ）
米国特許出願公開第２００７／０２５０８１８（ＵＳ，Ａ１）
国際公開第２０１４／０８７５９７（WO，Ａ１）
特開２００４－３０４７５２（ＪＰ，Ａ）
片岡　えり　Eri　Kataoka，攻撃間の関係を用いた標的型攻撃確定手法の提案　A method to determine targeted attacks using the relation between attacks，ＦＩＴ２０１６　第１５回情報科学技術フォーラム　講演論文集　第４分冊　査読付き論文・一般論文　ネットワーク・セキュリティ　ユビキタス・モバイルコンピューティング　教育・人文科学　情報システム　Forum on Information Technology 2016，２０１６年　８月２３日，pp.175-176

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６