

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号  
特許第6510040号  
(P6510040)

(45) 発行日 令和1年5月8日 (2019. 5. 8)

(24) 登録日 平成31年4月12日 (2019. 4. 12)

(51) Int. Cl.

F I

GO 6 F 16/00 (2019. 01)

GO 6 F 16/30 (2019. 01)

GO 6 F 17/30 2 1 O D

GO 6 F 17/30 1 7 O A

GO 6 F 17/30 3 4 O A

請求項の数 13 (全 21 頁)

|               |                               |           |                       |
|---------------|-------------------------------|-----------|-----------------------|
| (21) 出願番号     | 特願2017-518999 (P2017-518999)  | (73) 特許権者 | 506344309             |
| (86) (22) 出願日 | 平成27年10月5日 (2015. 10. 5)      |           | クラウドマーク インコーポレイテッド    |
| (65) 公表番号     | 特表2017-530481 (P2017-530481A) |           | アメリカ合衆国 カリフォルニア州 9 4  |
| (43) 公表日      | 平成29年10月12日 (2017. 10. 12)    |           | 1 0 7 サンフランシスコ キング スト |
| (86) 国際出願番号   | PCT/US2015/054014             |           | リート 1 2 8 セカンド フロア    |
| (87) 国際公開番号   | W02016/057401                 | (74) 代理人  | 100108855             |
| (87) 国際公開日    | 平成28年4月14日 (2016. 4. 14)      |           | 弁理士 蔵田 昌俊             |
| 審査請求日         | 平成29年6月6日 (2017. 6. 6)        | (74) 代理人  | 100103034             |
| (31) 優先権主張番号  | 14/508, 400                   |           | 弁理士 野河 信久             |
| (32) 優先日      | 平成26年10月7日 (2014. 10. 7)      | (74) 代理人  | 100153051             |
| (33) 優先権主張国   | 米国 (US)                       |           | 弁理士 河野 直樹             |
|               |                               | (74) 代理人  | 100179062             |
|               |                               |           | 弁理士 井上 正              |
|               |                               | (74) 代理人  | 100189913             |
|               |                               |           | 弁理士 鵜飼 健              |

最終頁に続く

(54) 【発明の名称】 不審なホストネームを識別するシステム及び方法

(57) 【特許請求の範囲】

【請求項 1】

入力インターフェースを介して、ホストネームに対応するストリングを受信することと、

コンピューティングデバイスにおいて、第1のストリングのセット中の複数のnグラムのそれぞれの発生の頻度を示すデータ構造を識別することと、

前記コンピューティングデバイスにおいて、前記ストリングを潜在的に不審であるとして分類するか否かを決定するためのフィルタを適用することであって、前記フィルタは、エントロピーフィルタと少なくとも1つの他のフィルタとを含み、ここにおいて、前記フィルタは、前記ストリングが潜在的に不審であるとそれぞれ示している前記エントロピーフィルタと前記少なくとも1つの他のフィルタとにตอบสนองして、前記ストリングを潜在的に不審であるとして分類するように構成され、ここにおいて、前記エントロピーフィルタは、前記ストリングのnグラムエントロピーに基づいて、前記ストリングが潜在的に不審であることを示すように構成され、ここにおいて、前記ストリングのnグラムエントロピーは、前記ストリング中の各nグラムに対して前記データ構造によって示される前記発生の頻度の関数であり、および、

前記ストリングが潜在的に不審であるとして分類されたことにตอบสนองして、前記コンピューティングデバイスにおいて、前記ストリングに関係付けられた少なくとも1つのドメインネームシステム (DNS) レコードを検索することと、ここにおいて、前記少なくとも1つのDNSレコードは、前記ホストネームに関係付けられたネットワークアクセス可能

なエンティティを識別し、前記コンピューティングデバイスにおいて、前記少なくとも1つのDNSレコードによって識別された前記ネットワークアクセス可能なエンティティに対する1つ以上のルールの適用に基づいて、前記ストリングを不審なストリングのセットに付加するか否かを決定するために、ルールベースのエンジンを実行することと、  
を備える、方法。

【請求項2】

前記少なくとも1つの他のフィルタは、

前記ストリングが国際化されたドメインネーム（IDN）プレフィックスで開始することを決定することに応答して、前記ストリングが潜在的に不審であることを示すように構成されたIDNフィルタと、

前記ストリングがトップレベルドメイン（TLD）であると決定することに応答して、前記ストリングが潜在的に不審であることを示すように構成されたTLDフィルタと、

前記ストリングの長さが、長さしきい値を満たすと決定することに応答して、前記ストリングが潜在的に不審であることを示すように構成された長さフィルタと、

しきい値時間期間内で、前記コンピューティングデバイスによって、前記ホストネームが登録されたか又は遭遇されたことを決定することに応答して、前記ストリングが潜在的に不審であることを示すように構成された最新のフィルタと、又は、

これらの組み合わせと、を含む、請求項1に記載の方法。

【請求項3】

前記少なくとも1つのDNSレコードに基づいて、第2のストリングを識別することと、  
、ここにおいて、前記第2のストリングは、前記ストリングとは異なり、

前記第2のストリングに関係付けられた少なくとも1つの第2のDNSレコードを検索することと、

前記少なくとも1つの第2のDNSレコードに対する前記1つ以上のルールの適用に基づいて、前記第2のストリングを前記不審なストリングのセットに付加するか否かを決定するために、前記ルールベースのエンジンを実行することと、をさらに備える、請求項1に記載の方法。

【請求項4】

前記少なくとも1つの第2のDNSレコードに基づいて、第3のストリングを識別することと、ここにおいて、前記第3のストリングは、前記ストリングと前記第2のストリングとは異なり、

前記第3のストリングに関係付けられた少なくとも1つの第3のDNSレコードを検索することと、

前記少なくとも1つの第3のDNSレコードに対する前記1つ以上のルールの適用に基づいて、前記第3のストリングを前記不審なストリングのセットに付加するか否かを決定するために、前記ルールベースのエンジンを実行することと、をさらに備える、請求項3に記載の方法。

【請求項5】

前記少なくとも1つのDNSレコードは、外部のDNSデータベースから検索され、アドレス（A）レコード、カノニカルネーム（CNAME）レコード、又は、ネームサーバ（NS）レコードのうちの少なくとも1つを備える、請求項1に記載の方法。

【請求項6】

前記少なくとも1つのDNSレコードは、前記ホストネームを前記ネットワークアクセス可能なエンティティにマッピングし、前記ルールベースのエンジンによって、前記ネットワークアクセス可能なエンティティが前記不審なストリングのセット中に含まれる第2のストリングに関係付けられたと決定することに応答して、前記ストリングを前記不審なストリングのセットに付加することをさらに備える、請求項1に記載の方法。

【請求項7】

前記少なくとも1つのDNSレコードは、前記ネットワークアクセス可能なエンティティを前記ホストネームにマッピングし、前記ルールベースのエンジンによって、前記ホス

10

20

30

40

50

トネームにマッピングするしきい値パーセンテージを上回るDNSレコードが、前記不審なストリングのセット中に含まれる1つ以上の第2のストリングに関係付けられたと決定することに応答して、前記ストリングを前記不審なストリングのセットに付加することをさらに備える、請求項1に記載の方法。

【請求項8】

前記第1のストリングのセットは、不審であると決定されているホストネームを除外し、又は、前記第1のストリングのセットは、不審でないと決定されているホストネームを除外する、請求項1に記載の方法。

【請求項9】

前記エントロピーフィルタは、nグラムエントロピーしきい値に対する前記ストリングのnグラムエントロピーの比較に基づいて、前記ストリングを分類するように構成されている、請求項1に記載の方法。

10

【請求項10】

nグラムエントロピーによって前記第1のストリングのセットをソートすることと、前記第1のストリングのセットの、少なくとも特定のパーセンテージが、前記nグラムエントロピーしきい値を満たすことができないように、nグラムエントロピーしきい値を選択することとによって、

前記nグラムエントロピーしきい値を決定することをさらに備える、請求項9に記載の方法。

【請求項11】

20

前記nグラムエントロピーは、前記ストリング中に含まれるnグラムに対応する前記データ構造のエントリの、合計、加重和、平均、又は、加重平均を備える、請求項1に記載の方法。

【請求項12】

潜在的に不審なストリングのセットを記憶するように構成されたメモリと、プロセッサと、

フィルタリングモジュールであって、

ホストネームに対応するストリングを受信し、

第1のストリングのセット中の複数のnグラムのそれぞれの発生の頻度を示すデータ構造を識別し、

30

前記ストリングを前記潜在的に不審なストリングのセットに付加するか否かを決定するためのフィルタを適用するように、前記プロセッサによって実行可能なフィルタリングモジュールと、を備えるシステムであって、前記フィルタは、エントロピーフィルタと少なくとも1つの他のフィルタとを含み、ここにおいて、前記フィルタは、前記ストリングが潜在的に不審であるとそれぞれ示している前記エントロピーフィルタと前記少なくとも1つの他のフィルタとに応答して、前記ストリングを前記潜在的に不審なストリングのセットに付加するように構成され、ここにおいて、前記エントロピーフィルタは、前記ストリングのnグラムエントロピーに基づいて、前記ストリングが潜在的に不審であることを示すように構成され、ここにおいて、前記ストリングのnグラムエントロピーは、前記ストリング中の各nグラムに対して前記データ構造によって示される前記発生の頻度の関数であり、

40

ここにおいて、前記メモリは、不審なストリングのセットを記憶するように構成され、

前記システムは、

前記ストリングを前記潜在的に不審なストリングのセットに付加するフィルタリングモジュールに応答して、前記ストリングに関係付けられた少なくとも1つのドメインネームシステム(DNS)レコードを、外部のデータベースから検索するように、前記プロセッサによって実行可能なDNSモジュールと、

前記少なくとも1つのDNSレコードに対する1つ以上のルール適用に基づいて、前記ストリングを前記不審なストリングのセットに移動するか否かを決定するように、前記プロセッサによって実行可能なルールベースのエンジンと、をさらに備える、

50

システム。

【請求項 1 3】

分散型サービス妨害（DDoS）緩和アプリケーションに対して、DNSセキュリティアプリケーションに対して、又は、両方に対して、前記不審なストリングのセットを提供するように構成された出力インターフェースをさらに備える、請求項 1 2 に記載のシステム。

【発明の詳細な説明】

【関連出願への相互参照】

【0001】

[0001] 本出願は、2014年10月7日付けで提出された、共通して所有される米国仮出願番号 14 / 508、400 からの優先権を主張し、この内容は、その全体において、参照によって明確にここに組み込まれる。

【背景】

【0002】

[0002] インターネットは、多くの異なるタイプの通信のための好ましい媒体となってきた。例えば、人気のあるウェブサイトは、一日に何億ものユーザにサーブし得る。インターネットが増大するにつれて、悪意あるインターネットユーザの頻度及び複雑性も増大する。例えば、情報技術（IT）管理者は、悪意ある攻撃から企業のコンピューティング資産を保護するために、インターネットセキュリティアプリケーション、アンチマルウェアアプリケーション、アンチスパムフィルタ、アンチフィッシングフィルタ等が企業において配備されることを必要とし得る。インターネット上の多数のウェブサイトによって、そして、新たなウェブサイトが登録される容易さによって、ウェブサイト（又は、関係付けられたホストネーム又はインターネットプロトコル（IP）アドレス）が悪意のあるものか否かを決定することは、困難であり得る。説明するように、マルウェア、スパム、フィッシング、分散型サービス妨害（DDoS）攻撃、又は他の悪意あるアクティビティに関連して使用するために、ランダム化されたホストネームを生成するためのドメイン生成アルゴリズム（DGA）を実行するボットネットによって、ホストネームが生成されているか否かを自動的に又はプログラムで決定することは困難であり得る。

【概要】

【0003】

[0003] 不審なホストネーム（例えば、DGAによって作られたホストネーム、及び／又は、DGAによって作られたホストネームに関連したホストネーム）を決定するシステム及び方法が開示される。システムは、セキュリティフィードやDNSクエリフィード等を含んでいるが、これらに限定されないさまざまなソースからのストリングを受信し得る。ストリングは、IPアドレス、ホストネーム、ドメイン、ネームサーバ、及び／又は、他のインターネットアクセス可能なデバイス又は位置に関係付けられた情報を含み得る。システムは、ストリングの入力セットにおける「不正」ストリングを識別するための2段階のプロセスを実現し得る。第1段階において、システムは、入力セットを、「興味がある」と決定されたストリングの、より小さなサブセットに低減し得る。例えば、システムは、興味があるストリングのサブセットを識別するために、ストリングの入力セットをフィルタリングし得る。ストリングの入力セットは、nグラムエントロピーに基づいてフィルタリングされ得る。代替的に又は追加的に、ストリングが、しきい値期間内のシステムによって登録されたホストネーム、又は、初めに遭遇されたホストネームに対応する場合、ストリングは、興味があるとして識別されることができる。

【0004】

[0004] 第2の段階において、アルゴリズム的に生成されると予測されるホストネームに位相的に又はアルゴリズム的に関連付けられたホストネームに対応するストリングのような、「不正」（例えば、不審な）ストリングを識別するために、システムは、ルールベースのエンジンを使用して、興味のあるストリングを評価し得る。ルールベースのエンジンによって使用されるルールは、1つ以上の「ギルト・バイ・インダクション（guilt

10

20

30

40

50

by induction)」ルールを含み得る。例示的で限定的でない例として、ホストネームのDNSレコードが、アルゴリズム的に生成されたと既に予測された別のホストネームにマッピングする場合、ホストネームは、不審であり得る。システムは、「不正」ストリングのセットを構築するために、再帰的にDNSレコードを調べ得る。「不正」ストリングのセットは、セキュリティを高めるために、モバイルセキュリティアプリケーション、Eメールセキュリティアプリケーション、DDoS緩和アプリケーション、及び、DNSセキュリティアプリケーションを含んでいるが、これらに限定されないさまざまなアプリケーションによって使用され得る。

【図面の簡単な説明】

【0005】

10

【図1】 [0005] 図1は、不審なホストネームを識別するシステムの特定の実施形態を説明するためのダイアグラムである。

【図2】 [0006] 図2は、図1のシステム中に含まれ得るフィルタリングモジュールの特定の実施形態を説明するためのダイアグラムである。

【図3】 [0007] 図3は、図1のシステム中に含まれ得るルールベースのエンジンの特定の実施形態を説明するためのダイアグラムである。

【図4】 [0008] 図4は、図1のシステムによってアクセスされ得るDNSレコードの例を説明するためのダイアグラムである。

【図5】 [0009] 図5は、不審なホストネームを識別する方法の特定の実施形態のデータフローダイアグラムである。

20

【図6】 [0010] 図6は、不審なホストネームを識別する方法の別の特定の実施形態を説明するためのフローチャートである。

【図7】 [0011] 図7は、本開示の態様を実現するのに使用され得るコンピューティングデバイスの特定の実施形態のダイアグラムである。

【詳細な説明】

【0006】

[0012] 図1を参照すると、システム100の特定の実施形態が示されている。システム100は、コンピューティングデバイス110を含む。例示的な例において、コンピューティングデバイス110はサーバである。ここでさらに説明されるように、コンピューティングデバイス110は、「不正」（例えば、不審な）ストリングを識別するために、2段階のプロセスを実行し得る。例えば、コンピューティングデバイス110は、「不正」ストリングのセットを生成して更新し得る。セットの初期シード(seed)は、アルゴリズム的に生成されると予測されたホストネームに対応するストリングであり得る。シードに関係付けられたDNS情報は、位相的に又はアルゴリズム的にシードに関連付けられた付加的な不審なホストネームを識別するために調べられ得る。2段階のプロセスにおいて、第1の段階は、「興味がある」ストリングのサブセットを生成するために、ストリングの入力セットをフィルタリングすることを含んでもよく、第2の段階は、ルールベースのエンジンの実行に基づいて、興味があるストリングを評価することを含み得る。

30

【0007】

[0013] コンピューティングデバイス110は、1つ以上の入力インターフェース111、1つ以上の出力インターフェース112、1つ以上のプロセッサ113、及びメモリ120を含み得る。例えば、入力インターフェース111と出力インターフェース112は、コンピューティングデバイス110が、ローカルエリアネットワーク(LAN)やインターネット等のようなネットワークを介してデータを通信できるようにする、ユーザ入力/出力インターフェース、及び/又は、ネットワークインターフェースを含み得る。ネットワークインターフェースは、イーサネット(登録商標)のような有線インターフェースとともに、第3世代(3G)、第4世代(4G)、ロングタームエボリューション(LTE(登録商標))、LTEアドバンスド、及び、電気電子技術者協会(IEEE)802.11のような無線インターフェースを含み得る。プロセッサ113は、中央処理ユニット(CPUs)、デジタル信号プロセッサ(DSPs)、ネットワーク処理ユニット(

40

50

N P U s ) 等を含み得る。プロセッサ 1 1 3 は、シングルスレッド、マルチスレッド、シングルスレッド、マルチコア、又は、これらの組み合わせであり得る。メモリ 1 2 0 は、ランダムアクセスメモリ ( R A M ) 、ディスクベースのメモリ、光ディスクメモリ、ソリッドステートメモリ、別のタイプのメモリ、又はこれらの組み合わせに対応する。

#### 【 0 0 0 8 】

[0014] コンピューティングデバイス 1 1 0 は、複数のソースからデータを受信し得る。例えば、コンピューティングデバイス 1 1 0 は、ホストネーム登録フィールド 1 0 1 とホストネーム遭遇フィールド 1 0 2 から、ストリングを受信し得る。ホストネーム登録フィールド 1 0 1 は、インターネットドメインネーム登録エンティティで登録されたホストネームに対応するストリングを提供し得る。ホストネーム遭遇フィールド 1 0 2 は、インターネットトラフィックの送信、受信、及び／又は処理の間に、特定のデバイス又はデバイスのグループ (例えば、メールサーバ、ウェブサーバ、ネームサーバ、企業のファイアウォール等) によって遭遇されたホストネームに対応するストリングを提供し得る。

10

#### 【 0 0 0 9 】

[0015] コンピューティングデバイス 1 1 0 は、スパムフィルタリングフィールド 1 0 3、モバイルセキュリティフィールド 1 0 4、Eメールセキュリティフィールド 1 0 5、及び／又は、DNSクエリフィールド 1 0 6 から、ストリングを受信し得る。スパムフィルタリングフィールド 1 0 3 は、ウェブメールサーバ又は企業メールサーバにおいて実行するスパムフィルタリングアプリケーションのようなスパムフィルタリングアプリケーションによって、Eメールにおいて検出されたホストネームに対応するストリングを提供し得る。代替的に、又は追加的に、スパムフィルタリングフィールド 1 0 3 によって提供されるストリングは、企業において「悪用ボックス (abuse box)」に送られたEメールに基づいて識別されたホストネームに対応し得る。例えば、企業の被雇用者は、価値がない、又は悪意がある (例えば、フィッシング) と決定されたEメールを、悪用ボックスに転送し得る。

20

#### 【 0 0 1 0 】

[0016] モバイルセキュリティフィールド 1 0 4 は、1つ以上のモバイルデバイス (例えば、携帯電話、タブレットコンピュータ等) 上で、及び／又は、企業サーバにおいて実行するモバイルセキュリティアプリケーションのような、モバイルセキュリティアプリケーションによって識別されたホストネームに対応するストリングを提供し得る。Eメールセキュリティフィールド 1 0 5 は、アンチマルウェア走査や、他のEメールセキュリティ動作を実行するために、個人用コンピューティングデバイス、企業のサーバ、及び／又は、メールサーバにおいて実行しているアプリケーションのような、Eメールセキュリティアプリケーションによって識別されたホストネームに対応するストリングを提供し得る。

30

#### 【 0 0 1 1 】

[0017] DNSクエリフィールド 1 0 6 は、(例えば、DNSクエリの処理の間に) DNSサーバによって処理されるホストネームに対応するストリングを提供し得る。DNSクエリフィールド 1 0 6 によって提供されるストリングはまた、DNSサーバにおいて (又は、DNSサーバにアクセス可能なデータベースにおいて) 記憶されたDNSレコードから読み取られ、及び／又は、DNSレコードに書き込まれるホストネームに対応し得る。

#### 【 0 0 1 2 】

40

[0018] コンピューティングデバイス 1 1 0 は、第3者DGAリスト 1 0 7からのストリングをさらに受信し得る。例えば、コンピューティングデバイス 1 1 0、又は、これに関係付けられたエンティティは、DGAによって出力されていると疑われる又は確認された、ホストネームのリストを提供するサービスに加入し得る。

#### 【 0 0 1 3 】

[0019] 代替の実施形態において、図 1 において図示されたものよりも多い、より少ない、及び／又は、異なるデータソースからの潜在的なホストネームに対応するストリングを、コンピューティングデバイス 1 1 0 が受信し得ることは留意されるべきである。システム 1 1 0 において利用可能な特定のデータソースに関わらず、コンピューティングデバイス 1 1 0 は、ストリング 1 2 1 の入力セットとして図 1 において図示された、多数の

50

ストリングを受信し得ることが認識される。例えば、人気のあるDNSサーバの場合、ピークのトラフィック期間に、DNSクエリフィールド106は、コンピューティングデバイス110に1秒毎に100万を超すストリングを提供し得る。

#### 【0014】

[0020] コンピューティングデバイス110は、受信されたストリング121のセットを処理するように構成されたコンポーネントを含み得る。図示された例において、コンピューティングデバイス110は、フィルタリングモジュール114、DNSモジュール115、ルールベースのエンジン116、及び、走査／分類モジュール117を含む。フィルタリングモジュール114、DNSモジュール115、ルールベースのエンジン116、及び、走査／分類モジュール117は、ハードウェア、ソフトウェア（例えば、プロセス113によって実行可能な命令）、又は、両方を使用して実現され得る。フィルタリングモジュール114は、受信されたストリング121のセットを、「興味がある」ストリングに対応すると決定されたストリングの、より小さなサブセット122にフィルタリングするように構成され得る。特定の実施形態において、フィルタリングモジュール114は、例示的で限定的でない例として、複数のフィルタを、nグラムエントロピーに基づいたフィルタとストリング長に基づいたフィルタとを含む、ストリング121のセットに適用するように構成される。フィルタリングモジュール114によって実行される動作の例は、図2を参照してさらに説明される。

10

#### 【0015】

[0021] DNSモジュール115は、サブセット122のストリングに関係付けられたDNS情報を検索するように構成され得る。例えば、DNSモジュール115は、特定のホストネームに関係付けられたDNS情報を検索するために、DNSデータベース130において記憶されたDNSレコード131にアクセスし得る。DNSレコード131の例は、図3を参照してさらに説明される。

20

#### 【0016】

[0022] ルールベースのエンジン116は、サブセット122のストリングが「不正」ストリングか否かを決定し得る。例えば、ストリングが、アルゴリズム的に生成されている（例えば、DGAによって出力されている）と予測されるホストネームに、又は、アルゴリズム的に生成されることになると予測されるホストネームに関連付けられたホストネームに対応する場合、ストリングは、「不正」ストリングであり得る。ルールベースのエンジン116は、ストリングが「不正」ストリングかどうかを決定するために、1つ以上のルールを、ストリングに関係付けられたDNS情報に適用し得る。図1において、ルールベースのエンジン116は、「不正」ストリングのセット123を生成する。「不正」ストリングのセット123中に含まれるアイテムは、ホストネーム、IPアドレス、ネームサーバ、及び、他のインターネットアクセス可能なエンティティを含み得る。ルールベースのエンジン116によって実行される動作の例が、図4を参照してさらに説明される。

30

#### 【0017】

[0023] 動作の間、コンピューティングデバイス110は、ストリング121のセットを受信してもよく、フィルタリングモジュール114は、興味のあるホストネームに対応すると決定されたストリングのサブセット122を生成するために、1つ以上のフィルタを、ストリング121のセットに適用し得る。DNSモジュール115は、サブセット122のストリングに関係付けられたDNS情報を検索してもよく、DNS情報に対する1つ以上のルールの適用に基づいて、ストリングを「不正」ストリングのセット123に付加するか否かを決定するために、ルールベースのエンジン116は実行され得る。プロセスは、「不正」ストリングのセット123のメンバーシップを拡張するために再帰的に実行され得る。例えば、コンピューティングデバイス110は、第1のストリング（例えば、第1のホストネーム）に関係付けられたDNS情報に基づいて、第2のストリング（例えば、ホストネーム）を識別し得る。応答において、第2のストリングについてのDNS情報が検索されて、第2のストリングを「不正」ストリングのセット123に付加する

40

50

か否かを決定するために、ルールベースのエンジン 116 に提供され得る。再帰的なプロセスは、付加的なストリング（例えばホストネーム）が遭遇されたときに継続し得る。

#### 【0018】

[0024] 特定の実施形態において、「不正」ストリングのセット 123 は、アルゴリズム的に生成されたホストネームであると予測される「シード」を識別することによって、初期形成される。例示的な限定的でない例として、シードは、 $n$  グラムエントロピーフィルタを使用して識別され得る。 $n$  グラムエントロピーフィルタの使用は、結果として、「不正」ホストネームのセット 123 中に「ランダム」のホストネームを十分に含み得る。フィルタリングモジュール 114 によって適用され得る  $n$  グラムエントロピーフィルタと他のフィルタの例は、図 2 を参照してさらに説明される。図 2 において、フィルタリングモジュール 114 は、 $n$  グラムエントロピーフィルタ 210、最新のフィルタ 220、国際化されたドメインネーム (IDN) フィルタ 230、2 ポートトップレベルドメイン (TLD) フィルタ 240、及び、長さフィルタ 250 を含む（例えば、これらを適用するように構成されている）。代替的な実施形態において、より多い、より少ない、及び／又は、異なるフィルタが、フィルタリングモジュール 114 によって適用され得る。

10

#### 【0019】

[0025] 特定の実施形態において、フィルタリングモジュール 114 は、2 つのフィルタリング動作、すなわち「不正」ストリングのセット 123 を初期構築するためのシードを識別するために、「既知」のホストネームのデータベース 202（例えば、リレーショナル・データベース）をフィルタリングすることと、ストリングのサブセット 122 を生成するために、ストリング 121 のセットをフィルタリングすることと、を実行するのに使用される。

20

#### 【0020】

[0026] 特定の実施形態において、「不正」ストリングのセット 123 に対するシードを識別することは、 $n$  グラムエントロピーフィルタ 210、IDN フィルタ 230、2 ポート TLD フィルタ 240 及び長さフィルタ 250 を、データベース 202 中に記憶されたストリングに適用することを含み得る。 $n$  グラムエントロピーフィルタ 210 はデータベース 202 にアクセスし得、データベース 202 は、（例えば、悪意のあるアクティビティに関係付けられた「不正」ホストネームとともに、正当なインターネットウェブサイトに対応する「良い」ホストネームの両方を含んでいる）コンピューティングデバイス 110 に対して処理される一部又はすべてのホストネームを記憶し得る。代替的に、 $n$  グラムエントロピーフィルタ 210 は、「不正」ホストネームのみ、又は、「良い」ホストネームのみを評価し得る。 $n$  グラムエントロピーフィルタ 210 は、データベース 202 中に記憶されたホストネームの少なくともドメイン部分に渡るすべての  $n$  グラムの頻度を計算し得る。説明される例において、 $n=3$ 、 $n$  グラムエントロピーフィルタ 210 は、3 グラム（例えば、aaa、aab、aac、… zzz）の頻度を示す頻度テーブル 212 を生成する。代替的な実施形態において、 $n$  は、異なる値を有し得る。頻度テーブル 212 を生成することは、一回の動作であってもよく、頻度テーブル 212 は、その後の使用のために記憶され得る。

30

#### 【0021】

[0027] 頻度テーブル 212 を生成した後、 $n$  グラムエントロピーフィルタ 210 は、特有のホストネームの  $n$  グラムエントロピーが、 $n$  グラムエントロピーしきい値 214 を満たすか否かを決定し得る。特定のストリングの  $n$  グラムエントロピーは、特定のホストネーム中に含まれる  $n$  グラムの発生の頻度の関数（例えば、合計、加重和、平均、加重平均等）であり得る。例として、ストリング「exampledomain.com」について、 $n$  グラムエントロピーは、（頻度テーブル 212 において示されるような） $n$  グラム：「exa」、「xam」、「amp」、「mpl」等の発生の頻度の関数であり得る。 $n$  グラムエントロピーしきい値 214 は、プログラムの、又は、ユーザ入力を介して決定され得る。特定の実施形態において、 $n$  グラムエントロピーしきい値を下回る、ホストネームの少なくとも特定のパーセンテージ（例えば、95%、99%、又は、他の何

40

50

らかの値)が、「不正」ストリング(例えば、ランダムに生成されたホストネーム)であると見えるように、 $n$ グラムエントロピーによってデータベース202のホストネームをソートし、 $n$ グラムエントロピー値を識別することによって、 $n$ グラムエントロピーしきい値214が生成される。 $n=3$ についての例示的な例において、他の実施形態においては異なる値が使用され得るが、 $n$ グラムエントロピーしきい値は、おおよそ0.00035である。

#### 【0022】

[0028] IDNフィルタ230は、ホストネームがIDNであるか否かを決定し得る。特定の実施形態において、IDNフィルタ230は、ホストネームが「xnー」のようなIDNプレフィックスで開始するかどうかをチェックする。2パートTLDフィルタ240は、ホストネームが「example.com」のような2パートTLDであるか否かを決定し得る。他の実施形態において、異なる長さしきい値が使用され得るが、長さフィルタ250は、ホストネームが、例えば10文字の長さのような長さしきい値よりも長いかなかを決定し得る。

10

#### 【0023】

[0029] 特定の実施形態において、ホストネームの $n$ グラムエントロピーが $n$ グラムエントロピーしきい値214よりも低く、ホストネームが2パートTLDであり、ホストネームがIDNではなく、そして、ホストネームが長さしきい値252よりも長い場合、データベース202からのホストネームは、「不正」ストリングのセット123に対するシードとして使用され得る。代替的な実施形態において、異なるフィルタの組み合わせが、「不正」ストリングのセット123をシードするのに使用され得る。

20

#### 【0024】

[0030] フィルタリングモジュール114はまた、ストリング121のセットを、興味のあるホストネームに対応するストリングのサブセット122に低減するのに使用され得る。例えば、最新のフィルタ220が、ストリングが登録最新しきい値222、又は、遭遇最新しきい値224を満たすことを決定した場合、ストリング121のセットのストリングは、サブセット122中に含まれ得る。したがって、しきい値時間期間内で(例えば、インターネットドメインネーム登録エンティティで)登録された、又は、しきい値時間期間内でコンピューティングデバイス110によって初めに遭遇されたホストネームに対応するストリングは、サブセット122に付加され得る。別の例において、ストリング121のセットからのストリングは、ストリングが、前述されたシード条件(例えば、ストリングが、 $n$ グラムエントロピーしきい値214と長さしきい値252を満たし、2パートTLDであり、IDNでない)を満たす場合、サブセット122に付加され得る。代替的な実施形態において、異なるフィルタの組み合わせは、ストリング121のセットを、興味のあるホストネームに対応するストリングのサブセット122に低減するために適用され得る。

30

#### 【0025】

[0031] ストリングが興味のあるホストネームであると識別されたとき、興味のあるホストネームの「ネイバー(neighbor)」が識別され得る。例えば、DNSモジュール115は、付加的なホストネームを識別するために、興味のあるホストネームに関係付けられたDNSレコード131にアクセスし得る。図3は、本開示にしたがって使用され得るマッピング情報(例えば、DNSレコードと、他のマッピング情報)の例を説明している。図3において、第1のDNS情報310は、「examplehostname.com」に対応し、第2のDNS情報320は、(ホストネーム95.160.243.23.in-addr.arpaと表現される)IPアドレス23.243.160.95に対応する。

40

#### 【0026】

[0032] ホストネームについてのDNS情報は、さまざまなDNSレコードを含み得る。図3において、「examplehostname.com」についてのDNS情報310は、ホストネームをインターネットプロトコルバージョン4(IPv4)アドレス

50

にマッピングするアドレス (A) レコード 3 1 1、ホストネームを別の (例えば、エイリアス) ホストネームにマッピングするカノニカルネーム (CNAME) レコード 3 1 2、及び、ホストネームを信頼できるネームサーバにマッピングするネームサーバ (NS) レコード 3 1 3 を含む。DNS レコードの付加的な例が、ここでさらに説明される。

#### 【0027】

[0033] IP アドレスについての DNS 情報は、ホストネームに対する、IP アドレスの逆 DNS マッピングに対応するポインタ (PTR) レコードを含み得る。例えば、DNS 情報 3 2 0 は、IP アドレス 2 3 . 2 4 3 . 1 6 0 . 9 5 をマッピングする PTR レコード 3 2 1 を含み、これは、ホストネーム `residential-DNS-customer84848.socal.res.examplehost.com` に対して、ホストネーム `95.160.243.23.in-addr.arpa` と表現される。

10

#### 【0028】

[0034] さまざまなタイプのレコードが、IP アドレス (例えば、`a.b.c.d`) をドメイン名 (`d.c.b.a.in-addr.arpa`) が付けられたドメインにマッピングするように、IP アドレスに対して記憶され得る。例えば、レコードは、例示的で限定的でない例として、PTR レコード、NS レコード、及び／又は、ゾーン情報 (例えば、スタートオブオーソリティ (SOA) レコードを含み得る。(例えば、コンピューティングデバイス 1 1 0 によって) クエリが発行されたとき、クエリは、さまざまなレコードタイプを応答として生成し得る。あるレコードタイプは、将来の使用のために保持され得る。例えば、CNAME レコード、A レコード、NS レコード、SOA レコード、テキスト (TXT) レコード、メール交換 (MX) レコード、及び／又は、PTR レコードが、例示的で限定的でない例として保持され得る。さらに、クエリ結果中に含まれるドメイン及び／又は IP アドレスは、クエリされたドメイン／IP アドレスと、結果となるドメイン／IP アドレスとの間の関係を追跡するために保持され (例えば、関連性データベースに付加され) 得る。

20

#### 【0029】

[0035] IP アドレスをホストネームにマッピングする PTR レコードの場合において、IP アドレスに対する逆 DNS が、ホストネームの一部として IP アドレスオクテットを含み得る (例えば、IP アドレス `a.b.c.d` は、`d.c.b.a.example.com` にマッピングし得る) ので、IP アドレスからホストネームのベースドメイン部分へのマッピングも保持され得る。ある状況において、全ホストネームは興味がないが、ホストネームの一部分は興味があることがあり得る。説明するように、「`example.com`」は、悪意のあるエンティティに関係付けられると知られ、スパム又はフィッシング等のために使用されると知られ得る。この状況において、全ホストネームではない、ホストネームのベースドメイン部分「`examplehost.com`」が、悪意のあるエンティティに関係付けられるので、全ホストネームにマッピングする PTR レコードは、有用でないかもしれない。例えば、「`95.160.243.23.in-addr.arpa`」からベースドメイン部分「`examplehost.com`」へのマッピング 3 2 2 が記憶され得る。したがって、ここで使用されるような、「不正」ストリングを識別するのに使用される「DNS 情報」及び「DNS レコード」は、登録リソースレコード (RR) タイプとともに、登録されていないレコード／マッピング (例えば、ベースドメインマッピング 3 2 2 に対する IP アドレス) を含み得る。

30

40

#### 【0030】

[0036] DNS モジュール 1 1 5 によって検索された DNS レコードは、ルールベースのエンジン 1 1 6 に提供され得る。例えば、図 4 において示されるように、ルールベースのエンジン 1 1 6 は、1 つ以上のルールを、ストリングが「不正」ストリングのセット 1 2 3 に付加されるべきか否かを決定するために、DNS モジュール 1 1 5 によって検索された DNS レコード 1 3 1 に適用し得る。ルールベースのエンジン 1 1 6 は、したがって、図 2 を参照して説明されたように、「不正」ストリングのセット 1 2 3 がシードされた後に、「不正」ストリングのセット 1 2 3 のメンバーシップを「育てる (grow)」のに

50

使用され得る。

#### 【0031】

[0037] ルールベースのエンジン116によって適用されたルールは、ストリングのDNSレコードが、「不正」ストリングのセット123中に既に含まれた別のストリングに関係付けられたアイテム（例えば、ホストネーム又はIPアドレス）にマッピングするとき、ストリングが「不正」ストリングのセット123に付加されることを示すルールを含み得る。例えば、第1のルール401は、ストリングが「不正」IPアドレスになる（例えば、ストリングのAレコードが、「不正」ストリングのセット123中に含まれるIPアドレスになる）場合、ストリングが「不正」ストリングのセット123に付加されることを示す。第2のルール402は、ストリングが「不正」ホストネームになる（例えば、ストリングのCNAMレコードが、「不正」ストリングのセット123中に含まれるホストネームになる）場合、ストリングが「不正」ストリングのセット123に付加されることを示す。第3のルール403は、ストリングの逆DNSルックアップが「不正」ホストネームになる（例えば、ストリングのPTR又はPTRDレコードが、「不正」ストリングのセット123中に含まれるホストネームになる）場合、ストリングが「不正」ストリングのセット123に付加されることを示す。第4のルール404は、ストリングが「不正」ネームサーバになる（例えば、ストリングのNSレコードが、「不正」ストリングのセット123中に含まれるネームサーバになる）場合、ストリングが「不正」ストリングのセット123に付加されることを示す。

10

#### 【0032】

[0038] ルールは、ストリングにマッピングするしきい値パーセンテージを超えるDNSレコードが、セット123中に既に含まれた「不正」ストリングに関係付けられたとき、ストリングが「不正」ストリングのセット123に付加されることを示すルールも含み得る。図4において、代替的な実施形態において異なる値が使用され得るが、しきい値パーセンテージは80%である。したがって、5番目のルール405は、ネームサーバによってサーブされるホストネームの少なくとも80%が「不正」である（例えば、ネームサーバにマッピングするNSレコードの80%が、「不正」ストリングのセット123中に含まれるアイテムに対応する）場合、ネームサーバが「不正」ストリングのセット123に付加されることを示す。6番目のルール406は、IPアドレスになるホストネームの少なくとも80%が「不正」である（例えばIPアドレスにマッピングするAレコードの80%が、「不正」ストリングのセット123中に含まれるアイテムに対応する）場合、IPアドレスが「不正」ストリングのセット123に付加されることを示す。7番目のルール407は、ホストネームとしてエイリアスする他のホストネームの少なくとも80%が「不正」である（例えば、ホストネームにマッピングするCNAMレコードの80%が、「不正」ストリングのセット123中に含まれるアイテムに対応する）場合、ホストネームが「不正」ストリングのセット123に付加されることを示す。

20

30

#### 【0033】

[0039] 図4において説明されたルールは例のためだけのものであり、限定的であると考えられるものではないことが留意されるべきである。ルールベースのエンジン116は、代替的な実施形態において、ルールの異なる組み合わせを使用し得る。ルール401～407の適用に基づいて、ルールベースのエンジン116は、興味のあるホストネームに対応するストリングのサブセット122中の「不正」ストリングを識別し得る。識別された「不正」ストリングは、「不正」ストリングのセット123に付加され得る。特定の実施形態において、「不正」ストリングが識別されて、「不正」ストリングのセット123に付加される度に、「不正」ストリングについてのDNS情報が検索されて、ルールベースのエンジン116が、DNS情報を処理して「不正」ストリングのセット123に付加するための付加的な「不正」ストリングを識別するために、反復的に実行される。

40

#### 【0034】

[0040] 図1に戻ると、ホストネームが「不正」ストリングのセット123に付加されたとき、走査／分類モジュール117は、ストリングに関係付けられた付加的な情報を

50

決定し得る。例えば、走査／分類モジュール 117 は、どのように「不正」ストリングを分類するかを決定するために、「不正」ストリングに関係付けられたウェブサイトやアクセス DNS 情報等にアクセスし得る。説明するように、ホストネーム、IP アドレス、ネームサーバ等は、マルウェアカテゴリ、スパムカテゴリ、フィッシングカテゴリ等において分類され得る。

#### 【0035】

[0041] 特定の実施形態において、メモリ 120 は、「不正」ストリングのセット 123 に関係付けられた付加的な情報を記憶する。例えば、アイテムが「不正」ストリングのセット 123 に付加されたとき、メモリ 120 は、アイテムがセット 123 に付加された理由を記憶し得る。説明するように、メモリ 120 は、アイテムによって満たされた、  
10 ルールベースのエンジン 116 によって実行される特定のルールを識別するデータを記憶し得る。メモリ 120 は、「ブレッドクラム」アイテム（例えば、ホストネーム、IP アドレス等）を識別するデータも記憶し得、そのアイテムに導かれる DNS 情報はセット 123 に付加される。したがって、メモリ 120 は、ユーザ又は管理者が、なぜ特定のアイテムが「不正」ストリングのセット 123 に付加されたかを、その後決定するのを可能にするデータを記憶し得る。

#### 【0036】

[0042] 「不正」ストリングのセット 123 は、コンピュータセキュリティを改善するのに使用され得る。例えば、コンピューティングデバイス 110 は、「不正」ストリングのセット 123 を、モバイルセキュリティアプリケーション 141 に、Eメールセキュリティアプリケーション 142 に、DDoS 緩和アプリケーション 143 に、DNS セキュリティアプリケーション 144 に、及び／又は、他のアプリケーション／デバイスに提供し得る。アプリケーション 141～144 は、アプリケーション 141～144 によって処理されるインターネットトラフィックに関するセキュリティ決定を行うために、「不正」ストリングのセット 123 を使用し得る。例として、モバイルセキュリティアプリケーション 141 は、「不正」ストリングのセット 123 中に含まれるアイテムに関係付けられるように決定されるトラフィック上の増加されたセキュリティ測定を、制限するか、又は設置し得る。別の例として、Eメールセキュリティアプリケーション 142 は、「不正」ストリングのセット 123 中に含まれるソースから到来する Eメールをブロックし得る。また別の例として、DDoS 緩和アプリケーション 143 は、「不正」ストリングの  
20 セット 123 中に含まれるアイテムに関係付けられた DNS クエリを無視するか、又はそうでなければ処置してもよく、これは、「不正」ホストネーム又はサーバに関係付けられた多数のクエリを受信することによって引き起こされる DDoS 攻撃を緩和するのを可能にし得る。また別の例として、DNS セキュリティアプリケーション 144 は、DNS データベース（例えば、DNS データベース 130）において、「不正」ストリングのセット 123 中に含まれるアイテムに関係付けられたクエリ／要求に基づいて、レコード（例えば、DNS レコード 131）のアクセス又は修正をディセーブルし得る。  
30

#### 【0037】

[0043] 図 1～4 を参照して説明されたシステム 100 は、したがって、正当なネームサーバと IP アドレスを不審であるとして分類することなく、不審なアイテムのクラス  
40 タ（例えば、セット）を自動的に識別し得る。例えば、ホストネームのような不審なアイテムは、位相的に及び／又はアルゴリズム的に関連付けられ得る。さらに、システム 100 は、さまざまなソースから受信された入力データに基づいて不審なホストネームを識別してもよく、識別されたホストネームをさまざまなコンピュータセキュリティアプリケーションに提供し得る。

#### 【0038】

[0044] 図 5 は、不審なホストネームを識別する方法 500 の特定の実施形態を説明するデータフローダイアグラムである。方法 500 は、501 において開始する。502 において、1 つ以上のホストネームソースは、アルゴリズム的に生成され得る、又は、生成され得ないホストネームに対応する候補ストリング 503 を提供する。504 において  
50

、候補ストリング503が興味のあるホストネームであるか否かについての決定がなされ得る。例えば、候補ストリング503が興味のあるホストネームであるか否かは、図2のnグラムエントロピーフィルタ210を参照して説明された候補ストリング503のnグラムエントロピーに基づいて決定され得る。候補ストリング503が興味のあるホストネームでない場合、方法500は、510において停止する。

#### 【0039】

[0045] 候補ストリング503が興味のあるホストネームである場合、興味のあるホストネームに対して、DNS情報が利用可能（例えば、コンピューティングデバイス110のようなコンピューティングデバイスにおいてキャッシュされる）か否かについて、505において決定がなされてもよい。DNS情報が利用可能でない場合、DNS情報は、DNSルックアップ動作を使用して、DNSデータベース507から検索されてもよく、これは、図1のDNSデータベース130に対応し得る。DNS情報が利用可能である場合、又は、DNSルックアップ動作が実行された後、方法500は、506において、興味があるホストネームのDNS「ネイバー」（例えば、すべてのDNS「ネイバー」）を調べることを含む。説明するように、ホストネームのDNS「ネイバー」は、ホストネームの少なくとも1つのDNSレコードによって識別された、別のホストネーム、IPアドレス、ネームサーバ、又は別のインターネットアクセス可能なエンティティに対応し得る。

#### 【0040】

[0046] 509に続いて、DNS「ネイバー」のいずれかを、セット（例えば、「不正」ストリングのセット123）に付加するか否かに関して、決定がなされる。例示的な例において、図4においてルールベースのエンジン116の動作を参照して説明されるように決定がなされる。DNS「ネイバー」のいずれもセットに付加されない場合、方法500は、510において停止する。1つ以上のDNS「ネイバー」がセットに付加される場合、方法500が508に続行して、（セットに付加される「ネイバー」の）付加的な候補「ネイバー」が識別されて調べられる。方法500又はこの部分は、付加的な候補「ネイバー」が識別されるときに反復され得る。ホストネームソースからのすべての候補「ネイバー」と候補ストリングが処理されたとき、方法500は、510において終端し得る。

#### 【0041】

[0047] 図6は、不審なホストネームを識別する方法600の、別の特定の実施形態を説明するためのフローチャートである。例示的な実施形態において、方法600は、図1のコンピューティングデバイス110によって実行される。

#### 【0042】

[0048] 方法600は、602において、ストリングのセットを受信することを含み得る。ストリングは、候補及び／又は識別されたホストネームに対応し得る。例えば、図1において、コンピューティングデバイス110は、ストリング121のセットを受信してもよく、これは、ホストネーム登録フィールド101、ホストネーム遭遇フィールド102、スパムフィルタリングフィールド103、モバイルセキュリティフィールド104、Eメールセキュリティフィールド105、DNSクエリフィールド106、及び／又は、第3者リスト107によって提供されるストリングを含み得る。

#### 【0043】

[0049] 方法600はまた、604において、興味のあるストリングのサブセットを生成するために、1つ以上のフィルタをストリングのセットに適用することを含み得る。例えば、図1のフィルタリングモジュール114は、ストリングのサブセット122を生成するために、ストリング121のセットをフィルタリングしてもよく、これは、図2のフィルタ210、220、230、240、250のうちの1つ以上の適用に基づいて、興味があると決定されるホストネームを含み得る。

#### 【0044】

[0050] 方法600は、606において、サブセットのストリングに関係付けられた

10

20

30

40

50

DNS情報を検索することをさらに含み得る。例えば、図1のDNSモジュール115は、DNSデータベース130からDNS情報を検索し得る。例示的な実施形態において、検索されたDNS情報は、図3を参照して説明されるような、Aレコード、CNAMEレコード、NSレコード、PTRレコード、PTRDレコード、及び／又は、他のタイプのDNSレコードを含み得る。

#### 【0045】

[0051] 方法600は、608において、DNS情報に対する1つ以上のルールの適用に基づいて、ストリングを「不正」ストリングのセットに付加するか否かを決定するために、ルールベースのエンジンを実行することを含み得る。例えば、ルールベースのエンジン116は、ストリングを「不正」ストリングのセット123に付加するか否かを決定するために、図4のルール401～407のうちの1つ以上のような、1つ以上のルールを適用し得る。

10

#### 【0046】

[0052] 方法600はまた、610において、DNS情報に基づいて識別された、付加的なストリングのサブセット、及び／又は、付加的なストリングを、「不正」ストリングのセットに付加するか否かを決定するために、ルールベースのエンジンを再帰的に実行することを含み得る。例えば、「不正」ストリングがセット123に付加されたとき、DNSモジュール115は、「不正」ストリングに関係付けられたDNS情報を検索してもよく、ルールベースのエンジンは、DNS情報中に含まれる、又はDNS情報に関連付けられた、任意の付加的なストリングも「不正」ストリングであるか否かを決定するために、ルール401～407を適用し得る。方法600は、したがって、不審なホストネーム、このようなホストネームに関係付けられたIPアドレス、このようなホストネームに関係付けられたネームサーバ等のような「不正」ストリングの、自動化された識別を可能にし得る。

20

#### 【0047】

[0053] 図7は、本開示の実施形態によって使用され得るコンピューティングデバイス701の実施形態を図示している。コンピューティングデバイス701は、プロセッサ703を含むコンピュータ、サーバ、又は他のデバイスであり得る。メモリ705、記憶装置711、ディスプレイ制御装置709、通信インターフェース713、及び、入力／出力制御装置715は、バス707に結合されている。

30

#### 【0048】

[0054] コンピューティングデバイス701は、通信インターフェース713を通して、外部のシステム及びデバイスにインターフェース接続し得る。通信インターフェース713は、イーサネットインターフェース、IEEE802.11インターフェース、3Gインターフェース、4Gインターフェース、LTEインターフェース、LTEアドバンスドインターフェース等のような、有線及び／又は無線ネットワークインターフェースを含み得る。

#### 【0049】

[0055] 特定の実施形態において、通信信号725は、（例えば、クラウドコンピューティング環境に対応する）通信インターフェース713とクラウド730との間で受信／送信され得る。通信信号725は、コンピュータデバイス701を、別のコンピュータシステム、ゲートウェイ、サーバ、ルータ、又はこれに類するものとインターフェース接続するのに使用され得る。

40

#### 【0050】

[0056] 特定の実施形態において、プロセッサ703は、マイクロプロセッサであり得る。メモリ705は、ダイナミックランダムアクセスメモリ（DRAM）、スタティックランダムアクセスメモリ（SRAM）等のような、機械読み取り可能な（例えば、コンピュータ読み取り可能な、又は、プロセッサ読み取り可能な）記録媒体又は記録デバイスであり得る。機械読み取り可能な媒体又はデバイスは、信号ではない。

#### 【0051】

50

[0057] ディスプレイ制御装置709は、ディスプレイ719を制御してもよく、これは、液晶ディスプレイ（LCD）、テレビジョンモニタ、又は、別のタイプのディスプレイであり得る。入力／出力制御装置715に結合された入力／出力デバイス717は、キーボード、ディスクドライブ、プリンタ、スキャナ、マウス、トラックボール、トラックパッド、又は、別の入力及び／又は出力デバイスを含み得る。

#### 【0052】

[0058] 記憶装置711は、機械読み取り可能な媒体又はデバイスを含んでもよく、これは、磁気ハードディスク、フロッピー（登録商標）ディスク、光ディスク、スマートカード、又はデータのための記憶装置の別の形態を含み得るが、これらに限定されない。特定の実施形態において、記憶装置711は、取り外し可能な媒体、読み取り専用媒体、及び／又は、読み取り可能な／書き込み可能な媒体を含む。コンピューティングデバイス701によるソフトウェアの実行の間、データの一部は、ダイレクトメモリアクセスプロセスによってメモリ705中に書き込まれ得る。ソフトウェアは、記憶装置711、メモリ705中に存在してもよく、あるいは、モデム又は通信インターフェース713を介して送信されるか又は受信され得る。記憶装置711は、図5の方法500及び／又は図6の方法600のすべて又は一部分のような、ここで説明された1つ以上の動作又は方法を実行するために、プロセッサ703によって実行可能な命令を記憶し得る。説明するように、記憶装置711は、フィルタリングモジュール114と、DNSモジュール115と、ルールベースのエンジン116と、走査／分類モジュール117とに対応する命令を記憶し得る。

#### 【0053】

[0059] 本開示のさまざまな実施形態によると、ここで説明される方法、機能及びモジュールは、コンピュータシステムによって実行可能なソフトウェアプログラムによって実現され得る。さらに、例示的な実施形態において、インプリメンテーションは、分散型処理、コンポーネント／オブジェクト分散型処理、及び、並行処理を含むことができる。例えば、コンピューティングデバイス110及び／又はコンピューティングデバイス701は、分散型様式及び並行様式において動作を実行する複数の個々のコンピューティングデバイスを含むクラウドコンピューティング環境に対応し得る。代替的に、仮想コンピュータシステム処理は、ここで説明された方法又は機能性のうちの1つ以上を実行するのに使用されることができる。

#### 【0054】

[0060] 特定の実施形態は、ここで開示された方法又はコンピュータベースの機能のうちの任意の1つ以上を、コンピュータシステムに実行させる命令のセットを実行するコンピュータシステムを使用して、実現されることができる。コンピュータシステムは、ラップトップコンピュータ、デスクトップコンピュータ、携帯電話、タブレットコンピュータ、又はこれらの任意の組み合わせを含み得る。コンピュータシステムは、例えばネットワークを使用して、他のコンピュータシステム又は周辺のデバイスに接続され得る。例えば、コンピュータシステム又はそのコンポーネントは、図1～7において図示された、又は、図1～7を参照して説明された、デバイス、システム、モジュール及び／又はコンポーネントのうちの任意の1つ以上を含む、又は、これらの内に含まれることができる。ネットワーク化された配備において、コンピュータシステムは、サーバとして、又は、サーバクライアントユーザネットワーク環境におけるクライアントユーザコンピュータとして、又は、ピアツーピア（又は分散型）ネットワーク環境においてピアコンピュータシステムとして、動作し得る。用語「システム」は、1つ以上のコンピュータ機能を実行するための命令のセット又は複数のセットを、個々に又は共同で実行する、システム又はサブシステムの任意の収集を含むことができる。

#### 【0055】

[0061] 特定の実施形態において、命令は、集中型又は分散型データベース、及び／又は、関係付けられたキャッシュ及びサーバのような、1つ以上のコンピュータ読み取り可能な又はプロセッサ読み取り可能なデバイスにおいて具現化されることができる。用語

「コンピュータ読み取り可能なデバイス」と「プロセッサ読み取り可能なデバイス」はまた、ここで開示された方法又は動作のうちの任意の1つ以上を、プロセッサによって実行するか、又は、コンピュータシステムに実行させるための命令を記憶することができるデバイスを含む。このようなデバイスの例は、ランダムアクセスメモリ（RAM）、フラッシュメモリ、読み取り専用メモリ（ROM）、プログラム可能な読み取り専用メモリ（PROM）、消去可能なプログラム可能な読み取り専用メモリ（EPROM）、電氣的に消去可能なプログラム可能な読み取り専用メモリ（EEPROM（登録商標））、登録ベースのメモリ、ソリッドステートメモリ、ハードディスク、取り外し可能なディスク、ディスクベースのメモリ（例えば、コンパクトディスク読み取り専用メモリ（CD-ROM））、又は、他の任意の形態の記憶デバイスを含むが、これらに限定されない。コンピュータ読み取り可能なデバイス又はプロセッサ読み取り可能なデバイスは、信号ではない。

10

#### 【0056】

[0062] ここで記述された実施形態の説明は、さまざまな実施形態の構造の一般的な理解を提供するように意図される。説明は、ここで記述された構造又は方法を利用する装置及びシステムの、要素及び特徴のすべての完全な記述として役立つようには意図されない。他の多くの実施形態が、開示をレビューする際に当業者にとって明らかとなり得る。他の実施形態は、開示の範囲から逸脱することなく、構造上及び論理上の代用及び変更がなされ得るように利用されて、開示から導出され得る。したがって、開示及び図面は、制限よりも説明として見なされるべきである。

#### 【0057】

20

[0063] 特定の実施形態がここで図示されて説明されてきたが、同一の目的又は同様の目的を達成するために設計された任意の後続の構成が、示された特定の実施形態に対して代用され得ることが認識されるべきである。本開示は、さまざまな実施形態の、任意の及びすべての、後続の適応又は変動をカバーするように意図される。上の実施形態の組み合わせと、ここで特に説明されていない他の実施形態は、明細書をレビューする際、当業者にとって明らかとなる。

#### 【0058】

[0064] 要約は、特許請求の範囲又はその意図を解釈又は限定するのには使用されないという理解とともに提出される。さらに、先述の詳細な説明、さまざまな特徴は、開示を合理化する目的で、単一の実施形態において、ともにグループ化又は説明され得る。本開示は、特許請求の範囲に記載された実施形態が各請求項において明示的に規定されるものより多くの特徴を要求する意図を表わすとして解釈されるべきでない。むしろ、以下の特許請求の範囲が表わすように、進歩的な主題事項は、開示された実施形態のいずれかの特徴のすべてよりも少ないものに向けられ得る。

30

#### 【0059】

[0065] 上で開示された主題事項は、例示的、かつ、限定的でないと考えられるべきであり、添付される特許請求の範囲は、本開示の実際の範囲内に含まれる、すべてのこのような修正、エンハンスメント、及び、他の実施形態をカバーするように意図される。したがって、法によって認められる最大の範囲まで、本開示の範囲は、以下の特許請求の範囲とそれらの均等物の最も広い許容可能な解釈によって決定されるべきであり、先述の詳細な説明によって制限又は限定されるべきではない。

40

以下に、本願出願時の特許請求の範囲に記載された発明を付記する。

〔1〕プロセッサを備えるコンピューティングデバイスにおいて、ストリングのセットを受信することと、

興味のあるストリングに対応するように決定されるストリングのサブセットを生成するために、前記ストリングのセットに1つ以上のフィルタを適用することと、

前記サブセットの第1のストリングに関係付けられたドメインネームシステム（DNS）情報を検索することと、

前記DNS情報に対する1つ以上のルール of 適用に基づいて、前記第1のストリングを不審なホストネームのセットに付加するか否かを決定するために、ルールベースのエンジ

50

ンを実行することと、を備える方法。

〔2〕前記第1のストリングに関係付けられた前記DNS情報に基づいて、第2のストリングを識別することと、

前記第2のストリングに関係付けられた第2のDNS情報を検索することと、

前記第2のDNS情報に対する前記1つ以上のルール適用に基づいて、前記第2のストリングを前記不審なホストネームのセットに付加するか否かを決定するために、前記ルールベースのエンジンを実行することと、をさらに備える、〔1〕に記載の方法。

〔3〕DNS情報に基づいて識別された1つ以上の付加的なストリングを前記不審なホストネームのセットに付加するか否かを決定するために、前記ルールベースのエンジンを再帰的に実行することをさらに備える、〔2〕に記載の方法。

〔4〕前記1つ以上のフィルタを適用することは、前記第1のストリングが、エントロピーしきい値未満であるnグラムエントロピーを有するか否かを決定するために、エントロピーフィルタを前記第1のストリングに適用することを含む、〔1〕に記載の方法。

〔5〕識別されたストリングのセットにおいて、複数のnグラムのそれぞれの発生の頻度を決定することをさらに備え、ここにおいて、前記第1のストリングのnグラムエントロピーは、前記第1のストリング中に含まれる前記複数のnグラムのうちの1つ以上のnグラムの発生の頻度に基づく、〔4〕に記載の方法。

〔6〕前記1つ以上のフィルタを適用することは、前記第1のストリングが、しきい値時間期間内に登録された又は遭遇されたホストネームに対応するか否かを決定するために、最新のフィルタを前記第1のストリングに適用することを含む、〔1〕に記載の方法。

〔7〕前記DNS情報は、DNSレコードを備える、〔1〕に記載の方法。

〔8〕前記DNSレコードは、アドレス(A)レコードを備える、〔7〕に記載の方法

。

〔9〕前記DNSレコードは、カノニカルネーム(CNAME)レコードを備える、〔7〕に記載の方法。

〔10〕前記DNSレコードは、インターネットプロトコル(IP)アドレスをホストネームにマッピングするポインタ PTR)レコードを備える、〔7〕に記載の方法。

〔11〕前記DNSレコードは、インターネットプロトコル(IP)アドレスをホストネームのベースドメイン部分にマッピングする、〔7〕に記載の方法。

〔12〕前記DNSレコードは、ネームサーバ(NS)レコードを備える、〔7〕に記載の方法。

〔13〕前記1つ以上のルールは、前記第1のストリングに関係付けられたDNSレコードが、前記不審なホストネームのセット中に含まれる第2のストリングに関係付けられたアイテムにマッピングするとき、前記第1のストリングが前記不審なホストネームのセットに付加されることになることを示しているルールを含む、〔1〕に記載の方法。

〔14〕前記1つ以上のルールは、前記第1のストリングにマッピングするしきい値パーセンテージを上回るDNSレコードが、前記不審なホストネームのセット中に含まれる第2のストリングに関係付けられたとき、前記第1のストリングが前記不審なホストネームのセットに付加されることになることを示しているルールを含む、〔1〕に記載の方法

。

〔15〕命令を備えるコンピュータ読み取り可能な記録デバイスにおいて、前記命令は、コンピュータによって実行されるとき、前記コンピュータに、ストリングのセットを受信することと、

興味のあるストリングに対応するように決定されるストリングのサブセットを生成するために、前記ストリングのセットに1つ以上のフィルタを適用することと、

前記サブセットの第1のストリングに関係付けられたドメインネームシステム(DNS)情報を検索することと、

前記DNS情報に対する1つ以上のルール適用に基づいて、前記第1のストリングを不審なホストネームのセットに付加するか否かを決定するために、ルールベースのエンジンを実行することと、を備える動作を実行させる、コンピュータ読み取り可能な記録デバ

10

20

30

40

50

イス。

〔16〕前記動作は、前記第1のストリングを1つ以上の複数の分類カテゴリに分類することをさらに備え、ここにおいて、前記複数の分類カテゴリは、少なくともマルウェアカテゴリとフィッシングカテゴリとを含む、〔15〕に記載のコンピュータ読み取り可能な記録デバイス。

〔17〕前記ストリングのセットは、モバイルセキュリティフィード、スパムフィルタリングフィード、Eメールセキュリティフィード、DNSクエリフィード、又は、これらの任意の組み合わせから受信された少なくとも1つのストリングを含む、〔15〕に記載のコンピュータ読み取り可能な記録デバイス。

〔18〕ストリングのセットを受信するように構成された入力インターフェースと、メモリであって、

前記ストリングのセットと、  
興味のあるストリングに対応するように決定されるストリングのサブセットと、  
及び、

不審なホストネームのセットと、  
を記憶するように構成されたメモリと、

プロセッサと、  
前記興味のあるストリングに対応するように決定されるストリングのサブセットを生成するために、1つ以上のフィルタを適用するように、前記プロセッサによって実行可能なフィルタリングモジュールと、

前記サブセットの第1のストリングに関係付けられたドメインネームシステム（DNS）情報を検索するように、前記プロセッサによって実行可能なDNSモジュールと、

前記DNS情報に対する1つ以上のルールの適用に基づいて、前記第1のストリングを前記不審なホストネームのセットに付加するか否かを決定するように、前記プロセッサによって実行可能なルールベースのエンジンと、を備えるシステム。

〔19〕モバイルセキュリティアプリケーションに対して、Eメールセキュリティアプリケーションに対して、又は、両方に対して、前記不審なホストネームのセットを提供するように構成された出力インターフェースをさらに備える、〔18〕に記載のシステム。

〔20〕分散型サービス妨害（DDoS）緩和アプリケーションに対して、DNSセキュリティアプリケーションに対して、又は、両方に対して、前記不審なホストネームのセットを提供するように構成された出力インターフェースをさらに備える、〔18〕に記載のシステム。

10

20

30

【図 1】

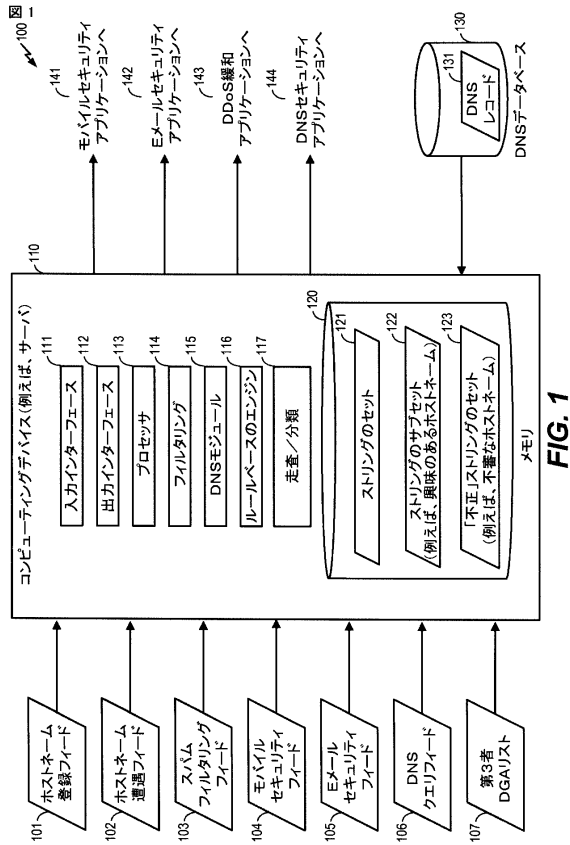


FIG. 1

【図 2】

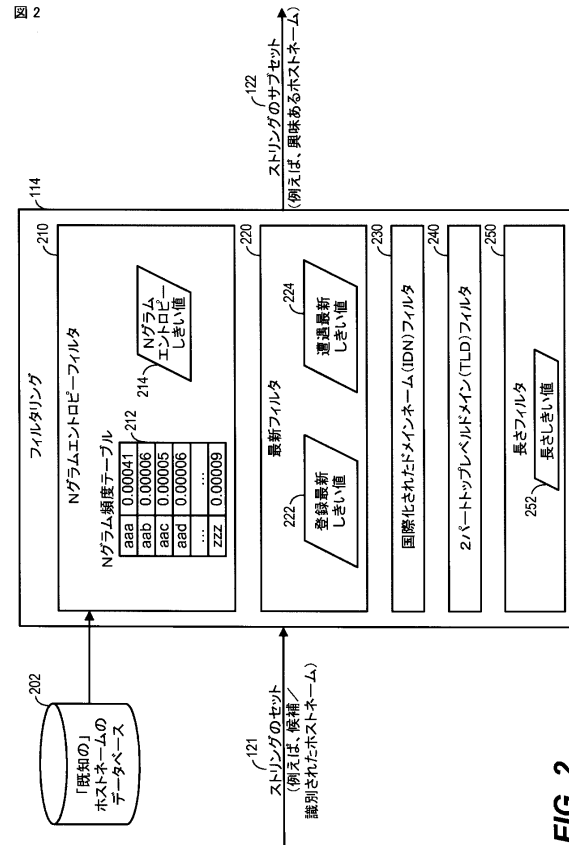


FIG. 2

【図 3】

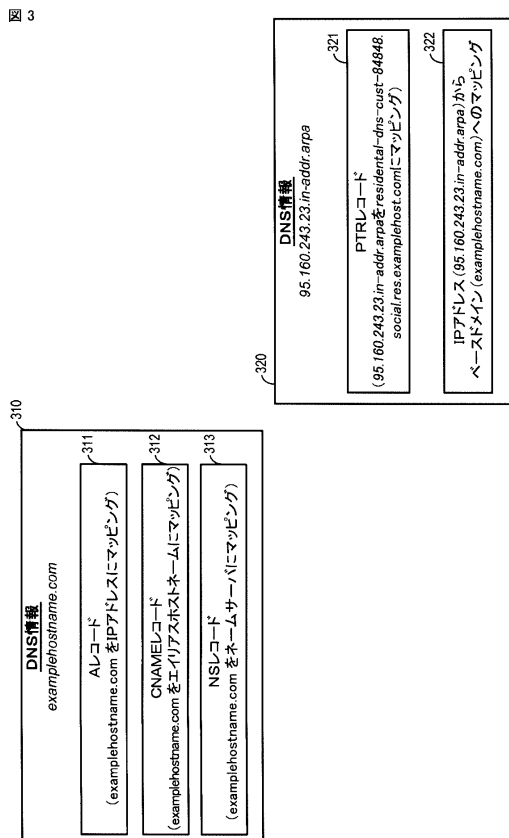


FIG. 3

【図 4】

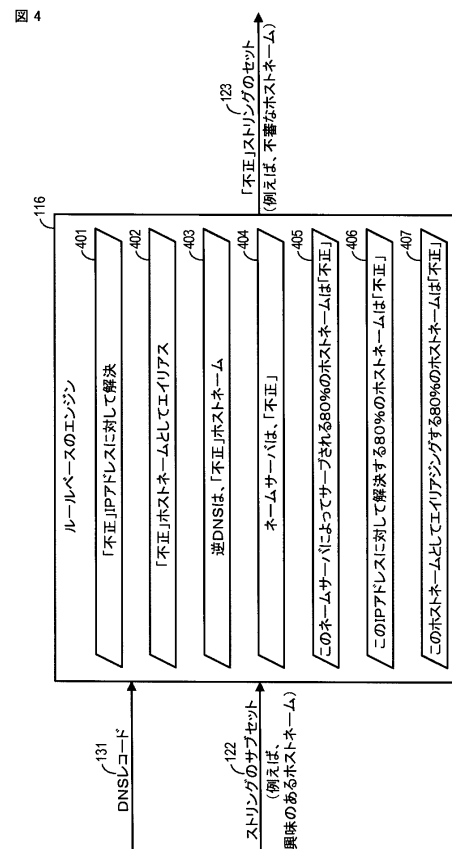


FIG. 4

【図 5】

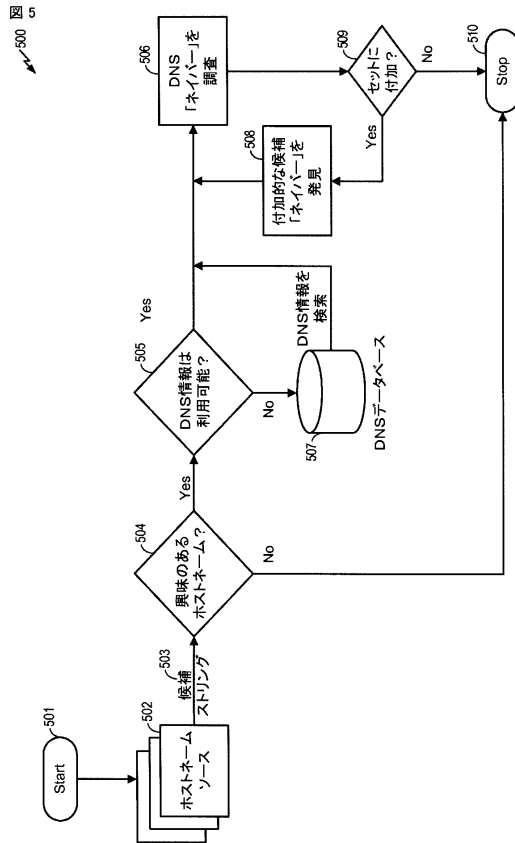


FIG. 5

【図 6】

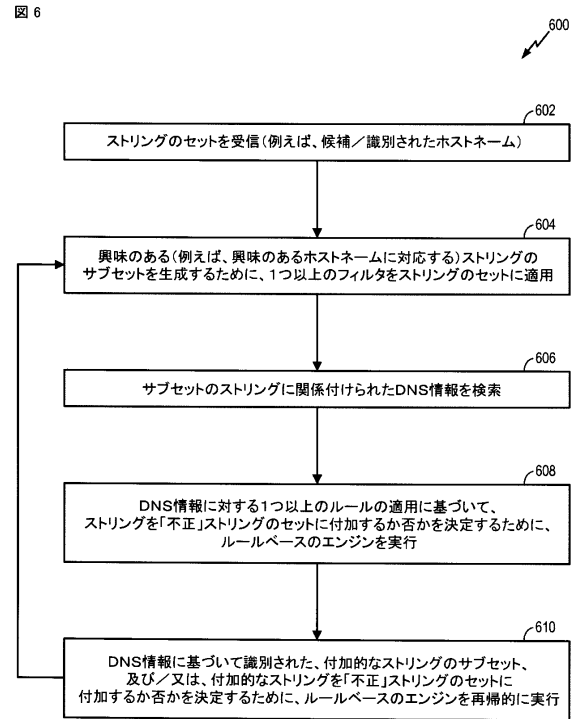


FIG. 6

【図 7】

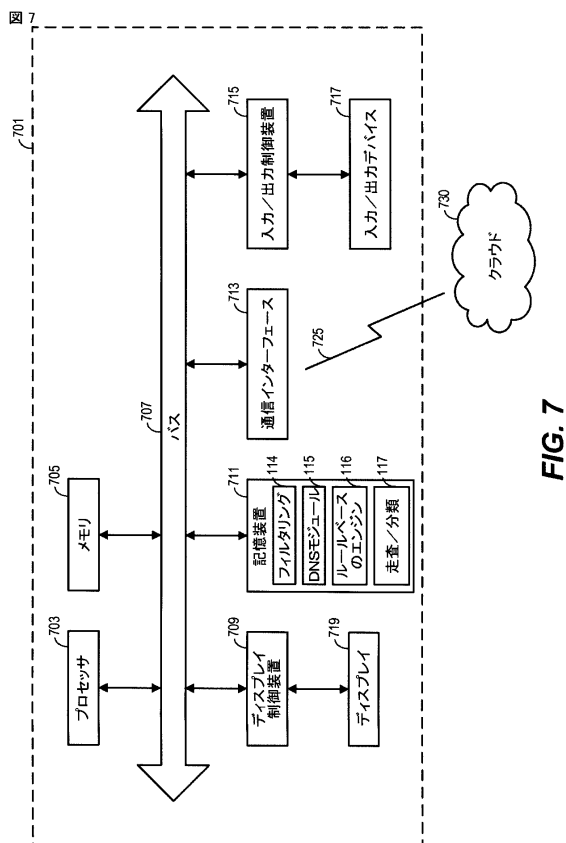


FIG. 7

---

フロントページの続き

(74)代理人 100199565

弁理士 飯野 茂

(72)発明者 スティーム、マーク・リチャード

アメリカ合衆国、カルフォルニア州 90403、サンタ・モニカ、フィフティーンズ・ストリート 848 ナンバー 5

(72)発明者 ジョーンズ、アーリン・ロバート

アメリカ合衆国、カルフォルニア州 94610、オークランド、ウォーフィールド・アベニュー 915

審査官 吉田 誠

(56)参考文献 特開2005-018745 (JP, A)

特開2012-118577 (JP, A)

特開2007-025789 (JP, A)

特開2008-250597 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 16/00 - 16/958

G06F 13/00