(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7084778号
(P7084778)

(45)発行日　令和4年6月15日(2022.6.15)

(24)登録日　令和4年6月7日(2022.6.7)

(51)国際特許分類

Ｇ０６Ｆ　21/56　(2013.01)	Ｇ０６Ｆ	21/56	３７０
Ｇ０６Ｆ　21/55　(2013.01)	Ｇ０６Ｆ	21/56	３６０
	Ｇ０６Ｆ	21/55	３４０

ＦＩ

請求項の数　20　外国語出願　（全25頁）

(21)出願番号　特願2018-95395(P2018-95395)
(22)出願日　平成30年5月17日(2018.5.17)
(65)公開番号　特開2019-82989(P2019-82989A)
(43)公開日　令和1年5月30日(2019.5.30)
審査請求日　令和2年10月5日(2020.10.5)
(31)優先権主張番号　2017133842
(32)優先日　平成29年9月29日(2017.9.29)
(33)優先権主張国・地域又は機関
ロシア(RU)
(31)優先権主張番号　62/573,830
(32)優先日　平成29年10月18日(2017.10.18)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　15/923,581
(32)優先日　平成30年3月16日(2018.3.16)
最終頁に続く

(73)特許権者　515348585
エーオー カスペルスキー ラボ
ＡＯ Ｋａｓｐｅｒｓｋｙ Ｌａｂ
ロシア国、１２５２１２ モスクワ、レニングラドスコ ショス ３９エー／３
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　セルゲイ ヴィー．ゴルジェーチク
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内
(72)発明者　コンスタンティン ヴィー．サプロノフ
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内
最終頁に続く

(54)【発明の名称】　標的型攻撃をクラウド型検出、探索および除去するシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

ハードウェアプロセッサを用いて、ネットワーク内のコンピュータのオブジェクトに関する情報を収集し、

前記オブジェクトとともにセキュリティ通知を前記ネットワーク内のオブジェクトデータベースに保存し、

前記ネットワーク内の脅威データベースで前記オブジェクトを検索し、

前記脅威データベース内で前記オブジェクトが発見された場合に前記オブジェクトに１以上のタグを付与して、前記オブジェクトデータベース内のレコードと脅威データベースとの対応付けを付与し、

前記１以上のタグがコンピュータ攻撃データベース内の１以上のシグネチャに対応する場合、コンピュータ攻撃が発生したと判定し、

前記シグネチャそれぞれは、前記オブジェクトに関する少なくとも一つのレコード、前記セキュリティ通知に関する少なくとも一つのレコード、および前記オブジェクトの少なくとも一つのタグを含み、

前記１以上のタグに基づいて不審動作データベース内で不審動作を検索し、

前記不審動作データベース内で不審動作のサインを発見した場合、第２のタグを前記セキュリティ通知に付与し、前記第２のタグは、前記不審動作データベースから取得し、少なくとも一つの不審動作の存在を示す、

ことを含む、コンピュータ攻撃検出方法。

【請求項２】
前記コンピュータ攻撃データベース内で前記オブジェクト、前記オブジェクトに付与された前記１以上の第１のタグ、および前記第２のタグが発見された場合、コンピュータ攻撃が発生したと判定する
ことをさらに含む請求項１に記載の方法。
【請求項３】
前記第２のタグは、不審動作のサインである所定イベントおよび所定動作がそれぞれ前記コンピュータ上で発生または実行された場合にのみ付与される、請求項２に記載の方法。
【請求項４】
前記コンピュータ攻撃の判定が不確実である場合、前記コンピュータ攻撃の判定を確認するためのコンピュータのメモリダンプ、および、前記コンピュータ攻撃を検出するロギングステップのいずれかを実行することをさらに含む、請求項２に記載の方法。
【請求項５】
前記オブジェクトに関する情報は、前記オブジェクトの動作、前記コンピュータのオペレーティングシステムにおけるイベント、ネットワーク間の前記オブジェクトのインタラクションに関する情報、侵入の痕跡（indicators of compromise）、および前記オブジェクトのメタデータのうち１以上を含む、請求項１に記載の方法。
【請求項６】
前記対応付けは、前記脅威データベースの前記オブジェクトのチェックサムと前記オブジェクトデータベースの前記オブジェクトのチェックサムとの一致によって規定される、請求項１に記載の方法。
【請求項７】
前記タグは、前記オブジェクトや前記オブジェクトによって実行されるイベントまたは前記オブジェクト上で実行されるイベントに関連する特徴である、請求項１に記載の方法。
【請求項８】
前記オブジェクトは、ファイル、当該ファイルのハッシュ、プロセス、ＵＲＬアドレス、ＩＰアドレス、証明書およびファイル実行ログのうち１以上を含む、請求項１に記載の方法。
【請求項９】
前記セキュリティ通知は収集された前記オブジェクトに関する情報を含む、請求項１に記載の方法。
【請求項１０】
前記セキュリティ通知はタイムスタンプを含む、請求項１に記載の方法。
【請求項１１】
ハードウェアプロセッサ上で実行されるコンピュータ保護モジュールであって、
ネットワーク内のコンピュータのオブジェクトに関する情報を収集し、
前記オブジェクトともにセキュリティ通知を前記ネットワーク内のオブジェクトデータベースに保存する、前記コンピュータ保護モジュールと、
ハードウェアプロセッサ上で実行される標的型攻撃防御用モジュールであって、
前記ネットワーク内の脅威データベースで前記オブジェクトを検索し、
前記脅威データベースで前記オブジェクトが発見された場合に前記オブジェクトに１以上のタグを付与して、前記オブジェクトデータベース内のレコードと前記脅威データベースとの対応付けを付与し、
前記１以上のタグがコンピュータ攻撃データベース内の１以上のシグネチャに対応する場合、コンピュータ攻撃が発生したと判定し、
前記シグネチャそれぞれは、前記オブジェクトに関する少なくとも一つのレコード、前記セキュリティ通知に関する少なくとも一つのレコード、および前記オブジェクトの少なくとも一つのタグを含み、
前記１以上のタグに基づいて不審動作データベース内で不審動作を検索し、
前記不審動作データベース内で不審動作のサインを発見した場合、第２のタグを前記セ

キュリティ通知に付与し、前記第２のタグは、前記不審動作データベースから取得し、少なくとも一つの不審動作の存在を示す、前記標的型攻撃防御用モジュールと
を備える、コンピュータ攻撃検出システム。
【請求項１２】
コンピュータ攻撃のデータベース内で前記オブジェクト、前記オブジェクトに付与された前記１以上の第１のタグ、および前記第２のタグが発見された場合、コンピュータ攻撃が発生したと判定する、請求項１１に記載のシステム。
【請求項１３】
前記第２のタグは、不審動作のサインである所定イベントおよび所定動作がそれぞれ前記コンピュータ上で発生または実行された場合にのみ付与される、請求項１２に記載のシステム。
【請求項１４】
前記コンピュータ攻撃の判定が不確実である場合、前記コンピュータ攻撃の判定を確認するためのコンピュータのメモリダンプ、および、前記コンピュータ攻撃を検出するロギングステップのいずれかを実行する解析センターをさらに含む、請求項１２に記載のシステム。
【請求項１５】
前記オブジェクトに関する情報は、前記オブジェクトの動作、前記コンピュータのオペレーティングシステムにおけるイベント、ネットワーク間の前記オブジェクトのインタラクションに関する情報、侵入の痕跡（indicators of compromise）、および前記オブジェクトのメタデータのうち１以上を含む、請求項１１に記載のシステム。
【請求項１６】
前記対応付けは、前記脅威データベースの前記オブジェクトのチェックサムと前記オブジェクトデータベースの前記オブジェクトのチェックサムとの一致によって規定される、請求項１１に記載のシステム。
【請求項１７】
前記タグは、前記オブジェクトや前記オブジェクトによって実行されるイベントまたは前記オブジェクト上で実行されるイベントに関連する特徴である、請求項１１に記載のシステム。
【請求項１８】
ハードウェアプロセッサを用いて、ネットワーク内のコンピュータのオブジェクトに関する情報を収集し、
前記オブジェクトとともにセキュリティ通知を前記ネットワーク内のオブジェクトデータベースに保存し、
前記ネットワーク内の脅威データベースでオブジェクトを検索し、
前記脅威データベース内で前記オブジェクトが発見された場合に前記オブジェクトに１以上のタグを付与して、前記オブジェクトデータベース内のレコードと脅威データベースとの対応付けを付与し、
前記１以上のタグがコンピュータ攻撃のデータベース内の１以上のシグネチャに対応する場合、コンピュータ攻撃が発生したと判定し、
前記シグネチャそれぞれは、前記オブジェクトに関する少なくとも一つのレコード、前記セキュリティ通知に関する少なくとも一つのレコード、および前記オブジェクトの少なくとも一つのタグを含み、
前記１以上のタグに基づいて不審動作データベース内で不審動作を検索し、
前記不審動作データベース内で不審動作のサインを発見した場合、第２のタグを前記セキュリティ通知に付与し、前記第２のタグは、前記不審動作データベースから取得し、少なくとも一つの不審動作の存在を示す、
ことを含むコンピュータ攻撃検出方法を、ハードウェアプロセッサによって実行された場合に実行するコンピュータ実行可能命令を格納した非一時的コンピュータ可読媒体。
【請求項１９】

前記コンピュータ攻撃のデータベース内で前記オブジェクト、前記オブジェクトに付与された前記１以上の第１のタグ、および前記第２のタグが発見された場合、コンピュータ攻撃が発生したと判定する
ことをさらに含む請求項１８に記載の媒体。
【請求項２０】
不審動作のサインである所定イベントおよび所定動作がそれぞれ前記コンピュータ上で発生または実行された場合にのみ、前記第２のタグが付与されることをさらに含む、請求項１９に記載の媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概してコンピュータセキュリティの分野に関し、特に、標的型攻撃をクラウド上で検出、探索および除去するシステムおよび方法に関する。
【背景技術】
【０００２】
従来の悪性ソフトウェア（ウィルス、インターネットワーム、キーロガー、エンクリプタ等）に加えて、現在コンピュータ攻撃が広がっている。特に、情報システム（コンピュータ装置と当該コンピュータ装置同士を接続するために使用される通信とを含む全体；情報システムは統合的インフラストラクチャとしても知られている。）に対する標的型攻撃（targeted attacks; TA）および高度持続型脅威（advanced persistent threats；APT）が広がっている。ハッカーは、従業員の個人データの単純な盗取から産業スパイまで様々な目的を持っている。多くの場合ハッカーは、企業ネットワークのアーキテクチャ、内部ドキュメントフローの仕組み、および、ネットワークやコンピュータ装置の保護に利用される手段に関する情報や、情報システムに固有のその他の情報を持っている。こうした情報により、ハッカーは既存の防御手段を潜り抜けることができる。既存の防御手段は、情報システムのニーズを全て満たすほど設定上の柔軟性を有していないことが多い。
【０００３】
悪性ソフトウェアや、シグネチャ解析、ヒューリスティック解析、およびエミュレーションなどの、コンピュータ脅威を防ぐ既存の技術には多くの欠点があり、標的型攻撃やその他のコンピュータ攻撃に対して適切なレベルの防御を提供する妨げとなっている。たとえば、既存の技術では、これまで知られていない脅威、悪性ソフトウェアを使用しないコンピュータ攻撃、（防御手段を潜り抜ける技術を使用した）複合攻撃および（数日から数年にわたる）長期持続攻撃を検出および探索することができない。こうした脅威のサインは所定期間後になってようやく分かるようになる。
【０００４】
このように、情報システムに対するコンピュータ攻撃のサインを判定する性能が低いという技術的課題が生じる。
【０００５】
しかし、従来技術で知られている方法では、コンピュータ攻撃とそのサインを特定できない場合が多い。これは、特定のためには実行可能ファイルをサーバに送信する必要があるが、標的型攻撃をはじめとする多くのコンピュータ攻撃は悪性ソフトウェアを使用せずに実行されるためである。よって、上述の方法では提示した技術的課題を解決することができない。たとえば、今日の標的型攻撃は、悪性コードを動的に生成しハードディスクにアーチファクトを残すことなくコンピュータメモリに直接ダウンロードするためにPowerShell（登録商標）を使用する場合がある。この場合、悪性ソフトウェアのコピーはなく、PowerShellインタプリタ自体は悪性ソフトウェアではない。別の例では、悪意で正規ツールを使用する場合がある。すなわち、侵入したコンピュータを遠隔制御するためにRemote Administration Utility（LiteManager、 TeamViewer等）を使用したり、侵入したコンピュータに悪性ソフトウェアをロードするために正規Windows（登録商標）ユーティリティ（bitsadmin、certuil等）を使用したり、コマンドを遠隔起動する管理ツール（w

mic、 psexec等）を使用したり、ハッカーがドメイン管理者のアカウントデータを取得して侵入したインフラストラクチャに統合するため、ネットワーク内のユーザのアカウントデータを繰り返しハッキングするラテラルムーブメント型攻撃が使用される場合がある。

【発明の概要】

【０００６】

本開示は、標的型攻撃をクラウド上で検出、探索および除去するシステムおよび方法に関する。

【０００７】

一例示的側面として、コンピュータ攻撃の検出方法を提供する。この方法では、ハードウェアプロセッサを用いて、ネットワーク内のコンピュータのオブジェクトに関する情報を収集し、オブジェクトとともにセキュリティ通知をネットワーク内のオブジェクトデータベースに保存し、ネットワーク内の脅威データベースでオブジェクトを検索し、脅威データベース内でオブジェクトが発見された場合に当該オブジェクトに１以上のタグを付与して、オブジェクトデータベース内のレコードと脅威データベースとの対応付けを付与し、当該１以上のタグがコンピュータ攻撃データベース内のシグネチャに対応する場合、コンピュータ攻撃が発生したと判定する。

【０００８】

別の側面では、この方法はさらに、１以上のタグに基づいて不審動作データベース内で不審動作を検索し、不審動作データベース内で不審動作のサインを発見した場合、第２のタグをセキュリティ通知に付与し、コンピュータ攻撃データベースでオブジェクト、第１のタグ、第２のタグが発見された場合、コンピュータ攻撃が発生したと判定する。

【０００９】

別の側面では、第２のタグは、不審動作のサインであるコンピュータ上の所定イベントの発生や所定動作の実行があった場合にのみ付与される。

【００１０】

別の側面では、コンピュータ攻撃の判定が不確実である場合、この方法では、コンピュータ攻撃の判定を確認するためのコンピュータのメモリダンプ、および、攻撃を検出するロギングステップのいずれかを実行する。

【００１１】

別の側面では、オブジェクトに関する情報は、オブジェクトの動作、コンピュータのオペレーティングシステムにおけるイベント、ネットワーク間のオブジェクトのインタラクションに関する情報、侵入の痕跡（indicators of compromise）、およびオブジェクトのメタデータのうち１以上を含む。

【００１２】

別の側面では、対応付けは、脅威データベースおよびオブジェクトデータベースのオブジェクトのチェックサム同士の一致によって規定される。

【００１３】

別の側面では、タグは、オブジェクトやオブジェクトによって実行されるイベントまたはオブジェクト上で実行されるイベントに関連する特徴である。

【００１４】

別の側面では、オブジェクトは、ファイル、当該ファイルのハッシュ、プロセス、ＵＲＬアドレス、ＩＰアドレス、証明書およびファイル実行ログのうち１以上を含む。

【００１５】

別の側面では、セキュリティ通知は、収集されたオブジェクトに関する情報を含む。

【００１６】

別の側面では、セキュリティ通知はタイムスタンプを含む。

【００１７】

一例示的側面では、コンピュータ攻撃を検出するシステムが提供される。このシステムは、ネットワーク内のコンピュータのオブジェクトに関する情報を収集し、オブジェクトとともにセキュリティ通知をネットワーク内のオブジェクトデータベースに保存するコンピ

ュータ保護モジュールと、ネットワーク内の脅威データベースでオブジェクトを検索し、脅威データベースでオブジェクトが発見された場合に当該オブジェクトに１以上のタグを付与して、オブジェクトデータベース内のレコードと脅威データベースとの対応付けを付与し、１以上のタグがコンピュータ攻撃のデータベース内のシグネチャに対応する場合、コンピュータ攻撃が発生したと判定する標的型攻撃防御用モジュールとを備える。

【００１８】

一例示的側面では、コンピュータ実行可能命令を格納した非一時的コンピュータ可読媒体が提供される。この命令は、ハードウェアプロセッサによって実行された場合、ハードウェアプロセッサを用いて、ネットワーク内のコンピュータのオブジェクトに関する情報を収集し、オブジェクトとともにセキュリティ通知をネットワーク内のオブジェクトデータベースに保存し、ネットワーク内の脅威データベースでオブジェクトを検索し、脅威データベース内でオブジェクトが発見された場合に当該オブジェクトに１以上のタグを付与して、オブジェクトデータベース内のレコードと脅威データベースとの対応付けを付与し、当該１以上のタグがコンピュータ攻撃のデータベース内のシグネチャに対応する場合、コンピュータ攻撃が発生したと判定する、というコンピュータ攻撃検出方法を実行する。

【００１９】

上記の例示的側面の簡単な概要により、本開示を基本的に理解できるであろう。この概要は、想定されるすべての側面の包括的な概観ではなく、全ての側面の主要または必要不可欠な要素を特定するものでも、本開示の側面の一部または全部の範囲を画するものでもない。本概要は、単に、以下の本開示の詳細な説明の前置きとして、１以上の側面を簡単に述べるものである。本開示の１以上の側面は、請求の範囲において説明され例示的に提示されている特徴を含む。

【図面の簡単な説明】

【００２０】

本明細書に組み込まれて本明細書の一部を構成する添付の図面は、本開示の１以上の例示的側面を図示し、詳細な説明とともにその原理および実施形態を説明する。

【図１】図１は、本開示の一例示的側面に係る、標的型攻撃をクラウド上で検出、探索および除去するシステムを示すブロック図である。

【図２】図２は、本開示の一例示的側面に係る、コンピュータ保護モジュールの想定されるモジュール例を示す図である。

【図３】図３は、本開示の一例示的側面に係る、標的型攻撃防御用コンピュータ保護モジュールの想定されるモジュール例を示す図である。

【図４】図４は、本開示の一例示的側面に係る、オブジェクトタグをセキュリティ通知に付与する処理を示す図である。

【図５】図５は、本開示の一例示的側面に係る、標的型攻撃を検出、探索および除去する方法の一例を示す図である。

【図６Ａ】図６Ａは、本開示の一例示的側面に係る、オブジェクトタグをセキュリティ通知に付与する一例を示す図である。

【図６Ｂ】図６Ｂは、本開示の一例示的側面に係る、オブジェクトタグをセキュリティ通知に付与する一例を示す図である。

【図７】図７は、本開示の一例示的側面に係る、汎用コンピュータシステムの一例を示す図である。

【発明を実施するための形態】

【００２１】

標的型攻撃をクラウド上で検出し、探索し、除去するためのシステムおよび方法、ならびに、当該システムおよび方法のためのコンピュータプログラムプロダクトについて、例示的側面を説明する。当業者であれば、以下の説明が単に例示的なものであって限定的なものではないことが理解できるであろう。他の側面についても、本開示の利益を享受する当業者は容易に理解できるであろう。以下、添付の図面に示す、例示的側面に係る実施形態を詳しく参照する。図面および以下の説明では、同じ又は同様の要素については可能な限

り同じ参照符号を使用する。
【００２２】
以下の用語は、本明細書、図面、および請求の範囲を通して使用される。
【００２３】
侵入の痕跡（indicators of compromise；IOC）は、フォレンジックアーチファクト、侵入のレムナントとも呼ばれ、ホストまたはネットワーク上で特定され得る。一般的なIOCは、ウィルスシグネチャ、IPアドレス、ファイルのチェックサム、URLアドレス、および従来のコンピュータ攻撃で知られているボットネットコマンドセンターのドメイン名などである。IOCには複数の規格がある。具体的には、OpenIOC（https://community.rsa.com/docs/DOC-62341、https://web.archive.org/web/20160401023434、http://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/、http://openioc.org/）、STIX（https://stix.mitre.org/）、CybOX（https://cybox.mitre.org）等である。
【００２４】
コンピュータ攻撃とは、ネットワークに侵入して組織や自然人に様々な危害を加えるために、当該組織や自然人の情報システムを対象とした、ハッカーが隠れて実行する長期間にわたる一連のステップのことを言う。
【００２５】
標的型攻撃（targeted attacks）またはTAとは、ネットワークに侵入して特定の組織や自然人に様々な危害を加えるための、当該組織や自然人の情報システムを対象としたコンピュータ攻撃のことを言う。
【００２６】
高度持続型脅威（advanced persistent threats）またはAPTとは、複雑な悪性ソフトウェア、ソーシャルエンジニアリング手法、および攻撃対象の情報システム上のデータを利用した、複雑で長期間にわたる巧みに計画された多面的なコンピュータ攻撃のことを言う。
【００２７】
ファジーハッシュ（フレキシブルフィンガープリントまたは局所鋭敏型ハッシュともいう。）とは、ファイルのフィンガープリントであって、ファイルのわずかな変更によってフィンガープリントが変わらないよう生成されているもののことを言う。つまり、悪性ファイルのフィンガープリントの値を用いて当該悪性ファイルを検出しようとすると、複数の類似した（おそらく未知の）悪性ファイルが検出される。このようなフィンガープリントの主な特徴は、ファイルに軽微な変更があっても変わらない点である。
【００２８】
ファジー判定（fuzzy verdict）とは、悪性ファイルの特徴など、ファイルの不審動作を検出する際のアンチウィルスアプリケーションの応答のことを言う。たとえば、フレキシブルフィンガープリントによってファイルを検出する際にファジー判定が返される。ファジー判定は、検出されたファイルが、ある程度の確率で悪性であることを示す。
【００２９】
図１は、本開示の一例示的側面に係る、標的型攻撃をクラウド上で検出、探索および除去するシステムを示すブロック図である。情報システム１００（または統合的インフラストラクチャ）は、コンピュータネットワーク１０５によって接続された一群のコンピュータ１０１を含む。コンピュータ１０１は、概括的に任意の計算装置およびセンサを指し、特に、パーソナルコンピュータ、ノート型パソコンおよびスマートホン、並びに、ルータ、スイッチおよびコンセントレータなどの通信デバイスを指す。情報システム１００は、従来技術で知られている任意のネットワーク１０５トポロジを使用して構成される。たとえば、完全接続型、point-to-point型、バス型、スター型、リング型または円型、メッシュ型、ツリー型、デイジーチェーン型あるいはハイブリッド型のうちいずれか一つを使用できる。コンピュータ１０１の一部には、コンピュータ保護モジュール１０２がインストールされている。コンピュータ保護モジュール１０２は、所定のコンピュータ１０１にはイ

ンストールされない場合がある。情報システム１００は、標的型攻撃防御用モジュール１０３を含んでもよく、標的型攻撃防御用モジュール１０３は、別のサーバなどに配置してもよい。評価サーバ１０４は、情報システム１００内に配置してもよく、（検出モジュール１１０に接続された）サービスプロバイダのクラウドサービス内に配置してもよい。コンピュータ１０１は、物理装置または仮想マシンのいずれであってもよい。ネットワーク１０５によってコンピュータ１０１をインターネットおよび検出モジュール１１０に接続するために、代理サーバ（図示せず）を使用してもよい。

【００３０】

コンピュータ保護モジュール１０２は、また、必要に応じて標的型攻撃防御用モジュール１０３は、コンピュータ１０１上のオブジェクトおよびネットワーク１０５内のオブジェクトに関する情報を収集する。コンピュータ保護モジュール１０２および標的型攻撃防御用モジュール１０３は、保護モジュール１０２，１０３とも呼ぶ。特定の例示的側面では、オブジェクトは、ファイル、当該ファイルのハッシュ、プロセス、URLアドレス、IPアドレス、証明書、ファイル実行ログ、またはコンピュータ１０１上で検出されるその他のオブジェクトでもよい。収集される情報は、コンピュータ１０１上のオブジェクトおよびネットワーク１０５内のオブジェクトに接続する不審なイベントに関する情報である。その後、コンピュータ保護モジュール１０２は、ネットワーク１０５によってセキュリティ通知を検出モジュール１１０（サービスプロバイダのクラウドサービス）に送信する。セキュリティ通知は、具体的には、保護モジュール自体に関する情報（識別子等）および収集されたオブジェクトに関する情報を含んでもよい。特定の例示的側面では、セキュリティ情報はタイムスタンプ（オブジェクトに関する情報が収集される時間または時間幅）を含んでもよい。特定の例示的側面では、保護モジュール１０２，１０３は、オブジェクトに関する以下の情報を収集するために使用される：

・プロセスの動作（実行トレース等）
・オペレーティングシステム（OS）におけるイベント－OSのイベントログのレコード
・ネットワーク間のインタラクションに関する情報
・侵入の痕跡（indicators of compromise）
・保護モジュールまたは保護モジュールが含む複数のモジュールの判定（ファジー判定を含む）またはテストシグネチャ
・オブジェクトのメタデータ、たとえばオブジェクトのチェックサム

【００３１】

標的型攻撃防御用モジュール（または標的型攻撃保護モジュール）１０３は、ネットワーク１０５を介してコンピュータ保護モジュール１０２に接続され、情報システム１００のネットワーク動作の解析を行う。また、標的型攻撃保護モジュール１０３は、（一部の側面では）「サンドボックス」、プロセスを安全に行うためのコンピュータ環境、およびその他の検出手法（詳しくは、図２～３）を使用してコンピュータ１０１のオブジェクトを検出することにより、情報システム内の標的型攻撃を検出する。

【００３２】

標的型攻撃防御用モジュール１０３は、ネットワークトラフィックで送信された情報を収集する。このように、標的型攻撃防御用モジュール１０３は、コンピュータ１０１（コンピュータ保護モジュール１０２がインストールされていないコンピュータ１０１を含む）からネットワーク１０５を介して送信されるすべてのオブジェクトの情報を収集する。

【００３３】

ネットワーク１０５内のオブジェクトに関する情報は、標的型攻撃防御用モジュール１０３の判定、ネットワークトラフィック内およびDNSトラフィック内の不審動作、および、電子メールやインターネットからのオブジェクトのエミュレーション結果を含んでもよい。

【００３４】

特定の例示的側面では、保護モジュール１０２，１０３は、上述のオブジェクトすべての情報を収集する。別の例示的側面では、保護モジュール１０２，１０３は、（悪性でも不審でもないことが正確に把握されている）安全な（正規）オブジェクトの一覧、および、

悪性かつ不審なオブジェクトの一覧（図示せず）を含んでもよい。この例では、保護モジュール１０２，１０３は、悪性かつ不審なオブジェクトの一覧の中のオブジェクトだけでなく、（安全なオブジェクトの一覧にも、悪性かつ不審なオブジェクトの一覧にも存在しない）不明なオブジェクトに関する情報も収集する。

【００３５】

さらに別の例示的側面では、保護モジュール１０２，１０３は、情報の収集が必要な補足オブジェクトの一覧を含んでもよい。このようなオブジェクトの一覧は、管理者１０６などが作成する。さらに別の特定の例示的側面では、管理者１０６は、一覧にオブジェクトを追加したり、一覧からオブジェクトを削除したりして、悪性かつ不審なオブジェクト（動作など）の一覧や安全なオブジェクトの一覧を作成してもよい。

【００３６】

たとえば、管理者１０６は、禁止動作の一覧および許可動作の一覧を示してもよい。たとえば、情報システム１００では、「psexec」ユーティリティはハッカーがリモート管理に使用する可能性があるため、一部のコンピュータ１０１での使用が禁止される場合がある。禁止動作に関連するオブジェクトの情報は、保護モジュール１０２，１０３が収集する。よって、特定のコンピュータ１０１やネットワーク１０５内でpsexecユーティリティが実行された場合、その使用に関する情報は検出モジュールに送信されその使用に応じたマーカが付与される。禁止動作および許可動作の一覧は、情報システム１００または検出モジュール１１０のいずれかに保存される。標的型攻撃防御モジュール１０３が、コンピュータ保護モジュール１０２がインストールされていないコンピュータ１０１上でpsexecユーティリティの使用を検出した場合、当該コンピュータ上での「psexec」の使用が許可可能かの確認および対応するタグの付与は、禁止動作の一覧を用いて標的型攻撃防御モジュール１０３または検出モジュール１１０のいずれかが行う。さらに別の特定の例示的側面では、禁止動作の一覧または許可動作の一覧に情報がない場合、解析センター１１５は、検出された動作が許可可能であるか管理者１０６に確認し、当該動作が許可可能ではない場合、対応するタグを付与する。

【００３７】

検出モジュール１１０は、受信したセキュリティ通知をオブジェクトデータベース１１２内に格納し、脅威データベース１１１内を検索してセキュリティ通知内のオブジェクトが脅威データベース１１１内にあるか判定する。検出モジュール１１０は、セキュリティ通知からのオブジェクトを脅威データベース１１１内に発見すると、発見したオブジェクトにつきオブジェクトデータベース１１２内にタグを付与し、脅威データベース１１１内に発見されたオブジェクトとの対応付けを付与する。対応付けは、たとえば脅威データベース１１１およびオブジェクトデータベース１１２内のオブジェクトのチェックサムの一致によって規定される。

【００３８】

オブジェクトのタグは、コンピュータ１０１で発生するイベントの特徴、発見されたオブジェクトに関連する特徴、あるいは、オブジェクトによって実行されたイベントまたはオブジェクト上で実行されたイベントに関連する特徴である。よって、コンピュータ１０１上で特定のイベントが発生した場合、または、オブジェクトに関する特定の動作が行われた場合にのみ、オブジェクトのタグがオブジェクトに付与される。特定の例示的側面では、オブジェクトのタグは、保護モジュール１０２，１０３の判定および（オブジェクトの情報に基づく）オブジェクトの不審動作に関する情報などを特徴づける。したがって、オブジェクトのタグは具体的に以下のイベントを含む（以下、所定のオブジェクトに関連し、オブジェクトについて得られた情報に基づいて検出されたイベントがコンピュータ１０１上で発生した場合にのみ、タグがオブジェクトに付与されるものと想定する）：

・コンピュータ上でのDNSサーバの置換
・オペレーティングシステムの自動更新の切断
・ネットワークファイアウォールの切断
・保護モジュールの切断

・UAC（User Account Control；Windows（登録商標）OSのコンポーネント）の切断
【００３９】
さらに別の特定の例示的側面では、検出モジュール１１０によってオブジェクトに付与されるオブジェクトのタグは、以下のイベントも含む：
・オブジェクト名とそのチェックサムとの不一致に関する情報（たとえば、リモートアクセスアプリケーションである実行可能ファイルTeamViewerが名称変更された場合）
・コンピュータ上の認証プロファイル違反（一定期間（１日間、２日間、またはそれ以上）にわたりオブジェクトに関する情報が収集されてコンピュータ１０１上で特定のユーザリストについて認証が実行された後、当該リストに存在しないユーザがコンピュータ１０１上で認証された場合）
・プロセスのネットワーク動作プロファイル違反（一定期間（１日間、２日間、またはそれ以上）にわたりオブジェクトに関する情報が収集されてプロセスがインターネットの特定のIPアドレス一覧とネットワーク内で相互作用した後に、プロセスがリストにないIPアドレスにネットワークによって接続された場合）
・所定の情報システム１００内で一意であり、許可タスクの一覧にないscheduler／Auto Runsettings／OS service／driver処理。
・外部のサイバー脅威インテリジェンスのソースから得たオブジェクトを検索した結果に関連するタグ
・キーロガー、リモートアドミンツールおよびモニタとして分類されるファイルが少数のコンピュータ１０１上で発見される場合に、当該ファイルが検出されるコンピュータ１０１
【００４０】
特定の例示的側面では、オブジェクトが悪性オブジェクトの一覧にない場合、検出モジュール１１０はオブジェクトに対してフレキシブルフィンガープリントを算出してもよい。その後、検出モジュール１１０は、このフレキシブルフィンガープリントが悪性オブジェクトのいずれかに対応しないか確認し、対応する場合、元のオブジェクトも検出モジュール１１０は悪性としてマークする。さらに、所与のファイルに対して判定（verdict）が作成され、検出モジュール１１０によってコンピュータ保護モジュール１０２に送信される。
【００４１】
検出モジュール１１０を使用して、受信したセキュリティ通知および当該セキュリティ通知に含まれるオブジェクトに付与されたタグに基づいて、不審動作データベース１１３内の不審動作のサイン（すなわち、コンピュータ攻撃の特徴的サイン）を検索する。不審動作のサインを発見すると、不審動作データベース１１３に含まれるタグが検出モジュール１１０によってセキュリティ通知に付与される。タグは、発見された不審動作のサインがあることを示す。その後、コンピュータ攻撃データベース１１４からコンピュータ攻撃のシグネチャを特定することにより、取得したオブジェクトおよびセキュリティ通知、ならびに、オブジェクトデータベース１１２内の当該オブジェクトおよびセキュリティ通知のタグの中から、コンピュータ攻撃のサインを検出する。
【００４２】
コンピュータ攻撃のサインが特定されることで、解析センター１１５が、標的型攻撃について詳細な探索および確認または標的型攻撃ではないとの証明を開始する条件が満たされる。特定の例示的側面では、コンピュータ攻撃のシグネチャを特定すると、解析センター１１５による探索を要することなく、コンピュータ攻撃のサインだけでなくコンピュータ攻撃も明確に特定し確認できる。別の例示的側面では、コンピュータ攻撃のシグネチャを特定することでは標的型攻撃を明確に確認することはできず、この場合、解析センター１１５によるさらなる探索が必要である。
【００４３】
タグは、オブジェクトおよびセキュリティ通知の両方に付与される。ここでタグは、コンピュータ１０１（セキュリティ通知に含まれる情報の収集元であるコンピュータ１０１）上で発生しているイベント、または、コンピュータ上で実行される動作の特徴である。よ

って、タグがセキュリティ通知に付与されるのは、不審動作のサインと定義される特定のイベントや特定の動作がコンピュータ１０１上で行われた場合のみである。

【００４４】

セキュリティ通知のタグは以下のような不審動作のサインを含む：

・ユーザが初めてコンピュータ上で認証を行ったこと。

このような不審イベントを発生させるスクリプトの一例を以下に説明する。保護モジュール１０２は、コンピュータ１０１上で認証に成功したユーザアカウントレコードの一覧を一月間収集する。その後、こうして作成されたアカウントレコードの一覧に含まれていないアカウントレコードでユーザがコンピュータ１０１上で認証される。

・オブジェクト（ファイル／プロセス）のリモート起動が発生したこと。

このような不審イベントを発生させるスクリプトの一例を以下に説明する。オブジェクトのリモート起動は、Windows Management Instrumentation（WMI）インフラストラクチャまたはOS Windowsサービスによって発生する。

・イベントログからレコードが削除されたこと。

・ブラウザではないアプリケーションからネットワーク内でファイルが起動されたこと。

・ホワイトリストに存在しないファイルが不審なディレクトリから起動されたこと。

・シャドウコピーが削除されたこと（たとえば、vssadmin.exeユーティリティによって削除される－これは、システムの復元を妨げる多くの悪性暗号化アプリケーションの特徴である）。

・名称変更されたリモート管理者のユーティリティが検出されたこと（AmmyyAdmin、TeamViewer等）。

・管理者のネットワークフォルダにファイルがコピーされたこと（C$、ADMIN$）。

・bcdedit.exeユーティリティを使用してOSコンポーネントスタートアップ修復が停止されたこと。

・lsass.exeシステムプロセスがディスク上でファイルを開いたりファイルを変更したりしたこと。

・難読化されたPowerShellスクリプトが実行されたこと。

・Windows API関数が呼び出されたこと（不審なPowerShellコマンド－Windows API関数が実行されている）。

・ライブラリRundll32によって不審な経路からのファイルが開かれたこと。

【００４５】

特定の例示的側面では、一部のオブジェクトのタグとセキュリティ通知のタグ（すなわち、不審動作のサイン）とは同時に生じる。たとえば、オブジェクトの名前とそのチェックサムとが対応しない場合、不審動作のサインであるとともに、タグがオブジェクトに付与される状況でありうる。

【００４６】

コンピュータ攻撃（特に標的型攻撃等）のシグネチャは、一側面において、オブジェクトの一覧、セキュリティ通知、および、特定のコンピュータ攻撃（特に標的型攻撃）の特徴である当該オブジェクトおよびセキュリティ通知のタグといった一連のレコードを含む。よって、標的型攻撃のシグネチャから特定のレコードの組合せを発見することで、攻撃（またはそのサイン）の発見を確認することができる。特定の一例示的側面では、コンピュータ攻撃のシグネチャは、オブジェクトに関する少なくとも一つのレコード、セキュリティ通知に関する少なくとも一つのレコード、オブジェクトの少なくとも一つのタグ、および、セキュリティ通知の少なくとも一つのタグを同時に含む。別の特定の例示的側面では、コンピュータ攻撃のシグネチャは上述のレコードのうち一つまたは複数のレコードを含んでもよい（たとえば、一つのオブジェクトに関するレコード、または、オブジェクトおよびオブジェクトのタグに関するレコードを含んでもよい）。さらに別の特定の例示的側面では、コンピュータ攻撃のシグネチャはセキュリティ通知の少なくとも一つのタグを含む。

【００４７】

不審動作（プロセスやコンピュータのネットワーク動作のプロファイル違反、ネットワーク入力のプロファイル違反等）のあらゆる種類のサインを発見するため、教師なし機械学習のシステムが使用されてもよい（このシステムは、送信されてくるセキュリティ通知および付与されたタグに基づいて自律的に学習する）。学習後、システムは、不審動作データベース１１３内でタグが付与されていないセキュリティ通知にタグを割り当てる。さらに、教師あり機械学習のシステムは、プロセスまたはコンピュータの動作を分類するという問題を解決するために使用されてもよい。この場合、因子は不審動作のサインであり、検出された既知のコンピュータ攻撃のデータによって学習が行われる。

【００４８】

オブジェクトデータベース１１２は、オブジェクトに関する情報を含むセキュリティ通知、ならびに、オブジェクトに付与されたタグおよびセキュリティ通知に付与されたタグを記憶する。

【００４９】

脅威データベース１１１は、既知の脅威に関するデータを含む。具体的には、脅威データベース１１１は、脅威のサインであるオブジェクトの識別子及び情報を含む。脅威データベース１１１内の各オブジェクトは対応するタグがラベル付けされる。たとえば、悪性オブジェクトには「悪性オブジェクト」タグが対応する。オブジェクトが特定の標的型攻撃で使用された場合、対応するタグが割り当てられる。

【００５０】

既知の標的型攻撃「Turla」の一例について検討する。これに関するURLアドレスが知られている。よって、実行可能ファイルであるオブジェクトがこのアドレスにアクセスした場合、そのオブジェクトにはその動作を示すタグが付与される（たとえば、「APT『Turla』につながるURLアドレスへのアクセス」タグがオブジェクトに付与される）。

【００５１】

さらに別の例では、「Naikon APT」標的型攻撃が既知のIPアドレス群に関連し、オブジェクトがこのアドレスにアクセスした場合、「『Naikon』APTにつながるURLアドレスへのアクセス」を示すタグがオブジェクトに付与される。

【００５２】

不審動作データベース１１３は、不審動作のサイン一覧を含む。不審動作の各サインには、当該不審動作のサインに対応する標的型攻撃を示す特別なタグがラベル付けされる（不審動作のサインの例は上述の通りである。）。

【００５３】

特定の例示的側面では、オブジェクトに特定のタグ群がラベル付されている場合、その状態を示す追加のタグがそのオブジェクトに付与されてもよい。よって、タグ群にさらにタグがラベル付されてもよい。

【００５４】

コンピュータ攻撃データベース１１４は、コンピュータ攻撃または標的型攻撃のシグネチャ一覧を含む。

【００５５】

図２は、コンピュータ保護モジュールの想定されるモジュール例を示す図である。コンピュータ保護モジュール１０２は、オンアクセススキャナ、オンデマンドスキャナ、Ｅメールアンチウィルス、ウェブアンチウィルス、プロアクティブ保護モジュール、HIPS（Host Intrusion Prevention System）モジュール、DLP（data loss prevention）モジュール、脆弱性スキャナ、エミュレータ、ネットワークファイアウォール等、コンピュータ１０１のセキュリティを確保するよう構成されたモジュールを含む。特定の例示的側面では、これらのモジュールはコンピュータ保護モジュール１０２の一部である。さらに別の例示的側面では、これらのモジュールは個々のソフトウェアコンポーネントとして実行される。

【００５６】

オンアクセススキャナは、ユーザのコンピュータシステムで開けられ、実行され、記憶さ

れるすべてのファイルの悪性動作を検出する機能を含む。オンデマンドスキャナは、ユーザの要求に応じて、ユーザが指定したファイルやディレクトリをスキャンするという点でオンアクセススキャナと異なる。

【００５７】

Ｅメールアンチウィルスは、送受信されるＥメールに悪性オブジェクトがないかをチェックするために必要である。ウェブアンチウィルスは、ユーザがウェブサイトにアクセスした時に、当該ウェブサイトが含んでいる可能性がある悪性コードの実行を防止し、また、ウェブサイトを開けないようブロックする。HIPSモジュールは、望ましくない悪性なプログラムの動作を検出し、実行時にこれをブロックする。DLPモジュールは、コンピュータやネットワークからの機密データの漏えいを検出して回避する。脆弱性スキャナは、コンピュータ上の脆弱性（たとえば、コンピュータ保護モジュール１０２の特定のコンポーネントが停止されていること、ウィルスデータベースが古いこと、ネットワークポートが閉じていること等）を検出するために必要である。ネットワークファイアウォールは、所定のルールに則ってネットワークトラフィックの制御およびフィルタリングを行う。エミュレータの機能は、エミュレータ内のコード実行中にゲストシステムのシミュレーションを実行することである。プロアクティブ保護モジュールは、実行可能ファイルの動作を検出して信頼度に応じて分類するために動作シグネチャを使用する。

【００５８】

悪性ソフトウェア（不審動作、スパム、およびその他のコンピュータ脅威のサイン）を検出する上述のモジュールは、（後にコンピュータ保護モジュール１０２の判定に変換されてもよい）対応する通知を生成し、発見した脅威およびその脅威を除去する処理（ファイルの削除や変更、実行の禁止など）の必要性について保護モジュールに通知する。特定の例示的側面では、悪性なソフトウェアを発見したモジュール自体が脅威を除去する処理を実行する。さらに別の例では、（判定は誤検知の可能性があるため）判定はファジーまたはテストでありうる。この場合、保護モジュールは脅威を除去する処理を行わずに検出モジュール１１０に通知を渡す。なお、コンピュータ保護モジュール１０２の判定は、オブジェクト（ファイル、プロセス）に関する情報の一部であり、後にセキュリティ通知の形式で検出モジュール１１０に送信される。

【００５９】

図３は、標的型攻撃防御用モジュールの想定されるモジュール例を示す図である。標的型攻撃防御用モジュール１０３は、たとえば、「サンドボックス」、侵入検出システム（Intrusion Detection System；IDS）、評価サーバ、YARAルールチェックモジュール、およびその他の検出モジュールなどの保護モジュールを含む。

【００６０】

サンドボックスモジュールは、コンピュータ保護モジュール１０２のエミュレータと同様の機能を有しているが、標的型攻撃防御用モジュール１０３はコンピュータ保護モジュール１０２に固有の時間制限がないため、サンドボックスは追加のコンピュータ性能を使用することができ、長時間作業を行うことができる。

【００６１】

サンドボックスは、プロセスを安全に実行するためのコンピュータ環境であり、ファイルから起動されたプロセスの実行中に不審動作を判定する。

【００６２】

サンドボックスは、たとえば、ファイルシステムおよびレジストリの部分仮想化、ファイルシステムおよびレジストリへのアクセスのルール、または、ハイブリッド手法に基づき、仮想マシンの形で実現してもよい。

【００６３】

侵入検出システムは、コンピュータシステム１０１またはネットワーク１０５への不正アクセスやその不正制御があったことを特定する。

【００６４】

評価サーバは、評価サーバ１０４のミラーコピーまたはキャッシュコピーでもよく、コン

ピュータ１０１上のオブジェクトの評判に関する情報（オブジェクトが存在するコンピュータ１０１の数、オブジェクトが起動された回数など）を含む。

【００６５】

YARAルールチェックモジュールは、YARAシグネチャ（シグネチャのオープンフォーマット）をチェックするために使用される（http://yararules.com/参照）。

【００６６】

DLPモジュールは、コンピュータやネットワークからの機密データの漏えいを検出して回避する。

【００６７】

TI（threat intelligence）解析器は、コンピュータ攻撃に関する報告のオブジェクトと、オブジェクトおよび不審動作のサインに関する情報とを照合するモジュールである。たとえば、TI解析器は、既知のコンピュータ攻撃に加わる指令センターのIPアドレス一覧を判定する。TI解析器は取得した情報をスコア化モジュールに送信し、スコア化モジュールは、オブジェクトや不審動作のサインに関する情報をコンピュータ攻撃に該当する確率に応じてランク付けする。

【００６８】

図４は、オブジェクトタグをセキュリティ通知に付与する処理を示す図である。保護モジュール１０２，１０３の少なくとも一つがオブジェクト４０１に関する情報を収集し、セキュリティ通知４０２を検出モジュール１１０に送信する。検出モジュール１１０は、受信したセキュリティ通知４０２からオブジェクト４０１を抽出し、脅威データベース１１１内でオブジェクト４０１を検索する（レベル１）。肯定の判定結果の場合、検出モジュール１１０は、脅威データベース１１１内の、このオブジェクト４０１に対応するタグ４１０を付与する。特定の一例示的側面では、上述のオブジェクト４０１にタグを付与する際に、収集された当該オブジェクトに関する情報が読み出される。たとえば、（脅威データベース１１１内に示されるように）規定されたIOCに対応するオブジェクト４０１がコンピュータ上で検出された場合、タグが付与される。しかし、同じオブジェクト４０１が検出されていても規定されたIOCが発見されない場合は、タグは付与されない。次に、検出モジュール１１０は、受信したセキュリティ通知４０２とオブジェクト４０１に付与されたタグ４１０とに基づいて、不審動作データベース１１３に含まれる不審動作のサインを検索する（レベル２）。不審動作のサインが発見された場合、検出モジュール１１０は、不審動作データベース１１３に含まれるタグ４１１をオブジェクトデータベース１１２（特にセキュリティ通知４０２）に付与する。

【００６９】

その結果、検出モジュール１１０は、オブジェクトデータベース１１２から受信したオブジェクト４０１、セキュリティ通知４０２、当該オブジェクトのタグ４１０、および、当該セキュリティ通知のタグ４１１の中から、コンピュータ攻撃データベース１１４の標的型攻撃のシグネチャを特定することにより、標的型攻撃の検出（レベル３）４０３を行う。

【００７０】

特定の例示的側面では、コンピュータ攻撃を確認すると、その情報が解析センター１１５へ送信されてもよい。解析センター１１５はこれに応じて、具体的には電気通信ネットワーク１２０またはネットワーク１０５を利用して、情報システム１００の管理者１０６に攻撃を検出した旨の警告を出す。

【００７１】

別の特定の例示的側面では、コンピュータ攻撃を確認するため、同様に情報が解析センター１１５へ送信される。これに応じて解析センター１１５は、具体的には電気通信ネットワーク１２０またはネットワーク１０５を利用して、情報システム１００の管理者１０６に攻撃を検出した旨の警告を出す。そして、管理者１０６が、コンピュータ脅威のシグネチャの特定の原因となった動作が正規の動作であると通知した場合、コンピュータ攻撃が反証される。

【００７２】

しかし、管理者１０６が、コンピュータ脅威のシグネチャの特定につながった動作は許容されるものではないことを通知した場合、および、オブジェクトデータベース１１２内の１以上のレコードにおいてコンピュータ攻撃データベース１１４からの標的型攻撃のシグネチャが特定できない場合は、解析センター１１５を使用して管理者１０６に追加情報を要求する。追加情報は、具体的に、１以上のコンピュータ１０１のファイル、コンピュータ保護モジュール１０２のログレコード（ネットワークファイアウォールログまたはプロアクティブ保護モジュールのログなど）、１以上のコンピュータ１０１のメモリダンプ、または、１以上のコンピュータ１０１のディスクダンプを含んでもよい。

【００７３】

解析センター１１５によって管理者１０６に追加情報を要求する例を以下の表１に示す。

【００７４】

たとえば、ウィルスシグネチャがメモリについてのファジー判定を含む場合、コンピュータ攻撃を確認するためにメモリダンプが必要となる（例１）。他の例については表１で詳しく説明する。

【表１】

番号	条件	要求された情報
1.	メモリに関するファジー判定 （アクセススキャナモジュール）	a）メモリダンプ
2.	フラグメントがメモリで発見され、 このフラグメントから指令サーバのアドレスが抽出される。標的型攻撃防御用モジュール103のログまたは代理サーバのログ（図示せず；代理サーバは、ネットワーク105内のコンピュータ101をインターネットおよび検出モジュール110に接続するために使用される）は、発見された指令サーバにアクセスしたコンピュータ101に関するレコードを含む。コンピュータ保護モジュール102はこれらのコンピュータ101にインストールされていない場合がある。	a）標的型攻撃防御用モジュール103のログ； b）代理サーバのログ； c）検出されたコンピュータ101のメモリダンプ
3.	（安全なファイルの一覧および悪性ファイルの一覧に存在しない）不審なファイルが発見される。さらに、評価サーバ104のデータによると当該ファイルは評価が低い。当該ファイルは自動実行で登録されている。解析センター115による当該ファイルの解析の結果、ファイルには以下の機能があることが発見された。ファイルから起動された場合、プロセスは特定のディレクトリからテキストファイルを読み出し、PEフォーマットに復号化し、そのコンテキストで実行を起動する。 攻撃を探索するには、解析センター115は管理者106に対し、不審なファイルが発見されたコンピュータ101の特定のディレクトリにコンテンツを要求する。	a）ファイルが検出されたコンピュータ101に、当該検出されたファイルを要求する。 b）特定のディレクトリのコンテンツを要求する。
4.	以下の悪性動作が検出される：Microsoft WordでDOCフォーマットのファイルを開けるプロセスにより、PEフォーマットの実行ファイルが生成され、実行のために起動される。実行可能ファイルは既知のAPT攻撃と関連付けられるC＆C（command and control）サーバのHTTPプロトコルによりアクセスされる。 ただし、オブジェクトデータベース112には、DOCフォーマットの初期ファイルのソースに関する情報は何もない。情報システム100の最初の侵入のベクトルを判定するため、解析センター115は、APT攻撃が発見されたコンピュータ101のハードディスクダンプを要求した。	a）APT攻撃が検出されたコンピュータ101のハードディスクのダンプを要求する。

【００７５】

特定の例示的側面では、不審動作のサインはコンピュータ攻撃（特に標的型攻撃）の戦術、技術および手順（tactics, techniques and procedures; TTP）に依拠している。

【００７６】

ここで、TTPの一例を挙げる。ユーザがＥメールの添付ファイル形式でオフィス文書を受信したとする。文書にはマクロが含まれ、ユーザはマクロを始める同意をした。開始されたマクロはPowerShellインタプリタを起動し、これにより、Base64でエンコードされているコンテンツがサイトからダウンロードされ、ディスク上にファイルを作成せずに起動された。起動されたコードは、PowerShellプロセスのコンテキスト内で実行され、レジスタHKEY_CURRENT_USER＼Software＼Microsoft＼Windows＼CurrentVersion＼Run内にレコードを生成することによってコンピュータシステムに埋め込まれ、ユーザがログオンするたびに当該コードが確実に起動されるようにする。このコードはクライアントTeamViewerと名称変更され、侵入したシステムにハッカーがリモート入力する際に使用する。

【００７７】
この例では、不審動作の以下のサインが役立つ：
・オフィスアプリケーションからのPowerShellインタプリタの起動；
・PowerShellパラメータの難読化（圧縮、BASE64でのエンコード等）に対するヒューリスティックなファジー判定；
・PowerShellインタプリタからのＨＴＴＰリクエスト；
・添付ファイルのダウンロード元のサイトが、（悪性オブジェクト一覧に含まれる）悪性ソフトウェアの拡散時に検出済であること；
・アクセススキャナによる、ダウンロードされた添付ファイルに対するファジー判定（フレキシブルフィンガープリントの機能から得られる結果と同様）；
・ダウンロードされた添付ファイルについて評価サーバの評価または評判が低いこと；
・サイトから悪性なコンテンツをダウンロードした後、コンピュータ保護モジュール１０２がPowerShellプロセスのメモリのスキャン時にファジー判定または確認済みとの判定を行うこと；
・PowerShellによる自動実行の登録鍵の変更；
・自動実行で登録されたファイルのハッシュが名前と一致しないこと（たとえば、ファイルのハッシュがTeamViewerアプリケーションのハッシュと一致するが、ファイル名が異なる）。
【００７８】
さらに別の例示的側面では、不審動作のサインは、侵入テスト(penetration test)（「pentest」と略称。）実行中に得られた標的型攻撃に関する情報に依拠する。たとえば、侵入テスト団体がSMBプロトコルの脆弱性によって管理者のコンピュータへのアクセス権限を得、正規のユーティリティによってlsass.exeプロセスのメモリダンプを生成する。権限データはこのダンプから抽出され、ネットワーク内の他のコンピュータにアクセスするために使用され、ここからメモリダンプが取得され権限データも抽出される。このプロセスは、Windowsドメインの管理者の権限データにアクセスできるまで何度も繰り返される。
【００７９】
なお、不審動作のサインの例は上記図１の説明の中で列挙した。
【００８０】
図５は、本開示の一例示的側面に係る、標的型攻撃を検出、探索および除去する方法５００の一例を示す図である。ステップ５０１において、コンピュータ保護モジュール１０２および／または標的型攻撃防御用モジュール１０３は、コンピュータ１０１上でオブジェクト（ファイル、プロセス等）に関する情報を収集する。次に、ステップ５０２において、これらの保護モジュールは検出モジュール１１０に対し、特に保護モジュールそのものに関する情報や収集されたオブジェクトに関する情報を含むセキュリティ通知を送信する。検出モジュール１１０は、受信したセキュリティ通知をオブジェクトデータベース１１２に記憶する。
【００８１】
ステップ５０３において、検出モジュール１１０は、脅威データベース１１１内にセキュリティ通知からのオブジェクトがあるか検索する。ステップ５０４において、検出モジュール１１０は、脅威データベース１１１内の当該オブジェクトに対応づけて、発見されたオブジェクトに対してオブジェクトデータベース１１２内でタグを付与する。ステップ５０５において、検出モジュール１１０は、受信したセキュリティ通知およびセキュリティ通知に含まれるオブジェクトに付与されたタグに基づいて、不審動作データベース１１３に含まれる不審動作のサインを検索する。ステップ５０６において、不審動作のサインを発見すると、検出モジュール１１０は不審動作データベース１１３に含まれるタグをオブジェクトデータベース１１２（特に、セキュリティ通知）に付与する。
【００８２】
ステップ５０７において、検出モジュール１１０は、オブジェクトデータベース１１２か

ら受信したオブジェクト、セキュリティ通知、当該オブジェクトのタグ、および当該セキュリティ通知のタグの中から、コンピュータ攻撃データベース１１４からのコンピュータ攻撃のシグネチャを特定することにより、コンピュータ攻撃のサインを発見する。コンピュータ攻撃のサインを発見した後、それ以降の攻撃の探索は解析センター１１５のコンピュータセキュリティ専門家が管理者１０６と共同して行う。特定の例示的側面では、コンピュータ攻撃のシグネチャを特定することで、コンピュータ攻撃のサインだけでなくコンピュータ攻撃の存在を解析センター１１５の探索を要することなく明確に確認できる。別の例示的側面では、コンピュータ攻撃のシグネチャを特定することでは、標的型攻撃を明確に確認することができない。この場合は、解析センター１１５による詳しい探索が必要となる。

【００８３】

このように、情報システムに対するコンピュータ攻撃のサインを判定する性能が低いという技術的課題を解決し、上述の技術的結果を実現する。すなわち、上記目的が達成され、さらに、オブジェクトデータベースから取得したオブジェクト、セキュリティ通知、当該オブジェクトのタグ、および当該セキュリティ通知のタグの中からコンピュータ攻撃のシグネチャを特定することにより、既知の解決法と比べ、情報システムに対するコンピュータ攻撃のサインを特定する性能が向上する。

【００８４】

なお、標的型攻撃を含む一定の攻撃は、保護モジュール１０２および１０３によって検出される。この場合、図５による方法が実行され、（攻撃で使用されたファイルの削除、トラフィックの遮断、その他の処理などによって）保護モジュール１０２，１０３によって攻撃が回避される。

【００８５】

特定の例示的側面では、ステップ５０１において、保護モジュール１０２および１０３は特に以下のオブジェクトに関する情報を収集する：

・プロセスの動作；
・オペレーティングシステムにおけるイベント；
・ネットワーク間のインタラクションに関する情報；
・侵入の痕跡（indicators of compromise; ＩＯＣ）
・保護モジュールの判定（モジュールの例は図２～３に図示）

【００８６】

特定の例示的側面では、不審動作のサインを発見すると、不審動作データベース内のタグが上述のセキュリティ通知に情報が含まれる保護モジュールに追加される。そして、標的型攻撃は、当該保護モジュールに付与されたタグとコンピュータ攻撃データベース１１４からのコンピュータ攻撃のシグネチャとの比較に基づいて検出される。

【００８７】

別の特定の例示的側面では、オブジェクトに関する情報は特に以下のいずれか一つをさらに含む：

・オブジェクトまたはその一部のチェックサム（たとえば、ファイルまたはその一部のチェックサム）（CRCや、MD5、SHA-1、SHA-2、Kessak、GOST R34.11-2012などのハッシュ関数）；
・オブジェクトの出現元（たとえば、オブジェクトのダウンロード元であるリソースのＩＰアドレス）；
・オブジェクト実行のエミュレーション結果；
・（オブジェクトがプロセスの場合）オブジェクトからのオペレーティングシステムのＡＰＩ関数呼び出しのログ；
・コンピュータ装置内のオブジェクト出現時間；
・ネットワーク内のオブジェクトが送信したデータ。

【００８８】

別の特定の例示的側面では、ステップ５０２において、オブジェクトや当該オブジェクト

に関する追加情報を提示する必要性を示すタグを脅威データベース１１１のオブジェクトに付与すると、検出モジュール１１０は、保護モジュール１０２，１０３の少なくとも一つに対し、オブジェクトまたは当該オブジェクトに関する追加情報を要求する。そして、要求したオブジェクトまたは当該オブジェクトに関する追加情報を保護モジュールから取得した後、新たに取得したオブジェクトまたは当該オブジェクトに関する追加情報についてステップ５０３～５０４が実行される。

【００８９】

さらに別の特定の例示的側面では、ステップ５０６において、セキュリティ通知に含まれる少なくとも一つのオブジェクトまたは当該オブジェクトに関する追加情報を提示する必要性を示すタグをセキュリティ通知に付与すると、検出モジュールは情報システム１００の少なくとも一つの保護モジュールに対し、オブジェクトまたは当該オブジェクトに関する追加情報を要求する。そして、要求したオブジェクトまたは当該オブジェクトに関する追加情報を保護モジュールから取得した後、新たに取得したオブジェクトまたは当該オブジェクトに関する追加情報についてステップ５０３～５０６が実行される。

【００９０】

図６Ａ～６Ｂは、図５の方法に係る、オブジェクトタグをセキュリティ通知に付与する例を示す図である。

【００９１】

ステップ５０２では、検出モジュール１１０は、保護モジュールからセキュリティ通知を取得した後、セキュリティ通知をオブジェクトデータベース１１２に保存する。この例では、２つのオブジェクトについて４つのセキュリティ通知が受信される（図６Ａのオブジェクトデータベース１１２の状態６０１参照）。

【００９２】

ステップ５０３において、検出モジュール１１０は、セキュリティ通知のオブジェクトが脅威データベース１１１内にあるか検索する。この例では、オブジェクト１のみが脅威データベース１１１に含まれる。オブジェクト１は、オブジェクトタグＯＴ１、ＯＴ４、ＯＴ５に対応する。これらのタグは、ステップ５０４において検出モジュール１１０によりオブジェクトデータベース１１２に付与される。その結果、オブジェクトデータベース１１２は状態６０２となる。

【００９３】

ステップ５０５において、検出モジュール１１０は、受信したセキュリティ通知と付与されたオブジェクトタグに基づき（すなわち、状態６０２のオブジェクトデータベース１１２に基づき）、不審動作データベース１１３に含まれる不審動作のサインを検索する。オブジェクトについての情報はセキュリティ通知に含まれている。この例では、不審動作データベース１１３中の不審動作の第１および第２のサインとの一致が発見される。よって、ステップ５０６では、不審動作データベース１１３の通知タグＮＴ１がオブジェクト１の通知２に付与され、通知４には通知タグＮＴ２が付与される。オブジェクトデータベース１１２は、図６Ｂの状態６０３となる。

【００９４】

ステップ５０７において、検出モジュール１１０は、（状態６０３の）オブジェクトデータベース１１２から受信したオブジェクトおよびセキュリティ通知、ならびに、当該オブジェクトおよびセキュリティ通知のタグの中から、コンピュータ攻撃データベース１１４に含まれるコンピュータ攻撃のシグネチャを特定することによって、コンピュータ攻撃のサインを検出する。この例では、オブジェクトデータベース１１２はオブジェクト１、タグＯＴ１、通知２および通知タグＮＴ１を同時に含んでいる（すなわち、第１のシグネチャを含んでいる）ため、コンピュータ攻撃の第１のシグネチャが検出される。また、第２のシグネチャが検出される。さらに、第２のシグネチャが検出される。よって、オブジェクトデータベース１１２において同時に２つのシグネチャが発見され、情報システム１００にコンピュータ攻撃のサインが存在することが証明される。

【００９５】

図７は、標的型攻撃をクラウド上で検出、探索および除去するシステムおよび方法の側面が例示的側面に応じて実施される、汎用コンピュータシステムの図である。

【００９６】

図示されているとおり、コンピュータシステム２０（パーソナルコンピュータまたはサーバでもよい）は、中央処理装置２１、システムメモリ２２、および、中央処理装置２１に対応するメモリを含む様々なシステムコンポーネントを接続するシステムバス２３を備える。当業者に理解されるとおり、システムバス２３は、バスメモリまたはバスメモリ制御部、周辺バス、および他のバスアーキテクチャと相互作用可能なローカルバスを含む。システムメモリは、永久メモリ（ＲＯＭ）２４およびランダムアクセスメモリ（ＲＡＭ）２５を含む。基本入力／出力システム（basic input／output system；ＢＩＯＳ）２６は、ＲＯＭ２４を使用してオペレーティングシステムをロードする時などの、コンピュータシステ２０の要素間の基本的な情報転送手順を記憶する。

【００９７】

コンピュータシステム２０は、さらに、データの読み取りおよび書き込みを行うハードディスク２７、取り外し可能な磁気ディスク２９の読み取りおよび書き込みを行う磁気ディスクドライブ２８、ならびに、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭおよびその他の光学媒体等の取り外し可能な光学ディスク３１の読み取りおよび書き込みを行う光学ドライブ３０を含む。ハードディスク２７、磁気ディスクドライブ２８、および光学ドライブ３０は、それぞれ、ハードディスクインタフェース３２、磁気ディスクインタフェース３３、および光学ドライブインタフェース３４を介して、システムバス２３に接続されている。ドライブおよびそれに対応するコンピュータ情報媒体は、コンピュータ命令、データ構造、プログラムモジュールおよびその他のコンピュータシステム２０のデータを記憶するための独立電源型モジュールである。

【００９８】

コンピュータシステム２０は、コントローラ５５を介してシステムバス２３に接続される、ハードディスク２７、取り外し可能な磁気ディスク２９、および取り外し可能な光学ディスク３１を含む。コンピュータによって読み取り可能な形式でデータを記憶できる媒体５６（ソリッド・ステート・ドライブ、フラッシュメモリカード、デジタルディスク、ランダムアクセスメモリ（ＲＡＭ）等）であればどのようなものでも利用できることは、当業者であれば理解できるであろう。

【００９９】

コンピュータシステム２０は、オペレーティングシステム３５が記憶されるファイルシステム３６、ならびに、追加プログラムアプリケーション３７、その他のプログラムモジュール３８およびプログラムデータ３９を有する。コンピュータシステム２０のユーザは、キーボード４０、マウス４２、または当業者に知られているマイク、ジョイスティック、ゲームコントローラ、スキャナ等（これらに限定されない）のその他の入力装置を使用して命令や情報を入力する。これらの入力装置は、通常、シリアルポート４６を介してコンピュータシステム２０に差し込まれ、システムバスに接続される。ただし、当業者であれば、入力装置は、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（ＵＳＢ）（これらに限定されない）を介するその他の方法でも接続され得ることがわかるであろう。モニタ４７やその他のタイプの表示装置も、ビデオアダプタ４８などのインタフェースを介してシステムバス２３に接続されてもよい。モニタ４７に加え、パーソナルコンピュータは、ラウドスピーカやプリンタ等のその他の周辺出力装置（図示せず）を装備していてもよい。

【０１００】

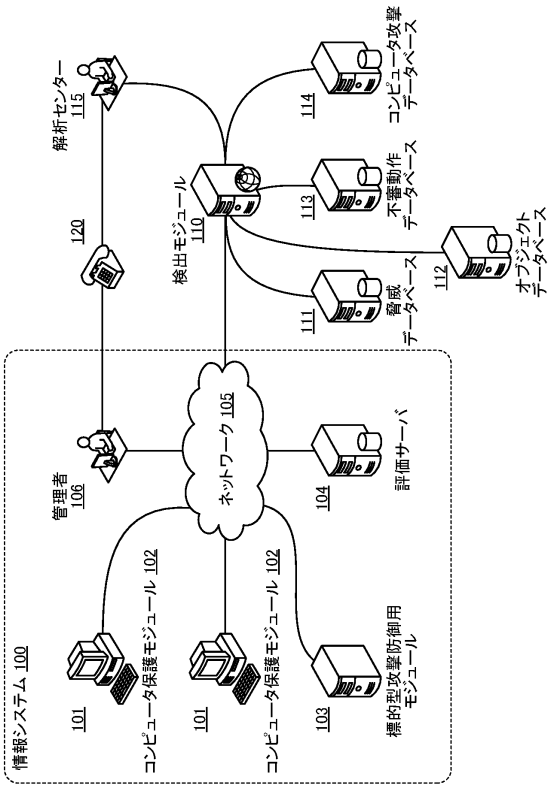
コンピュータシステム２０は、１以上のリモートコンピュータ４９へのネットワーク接続を使用して、ネットワーク環境で動作してもよい。一台（または複数）のリモートコンピュータ４９は、上述のコンピュータシステム２０の性質で説明した要素の大部分もしくはすべてを含むローカルコンピュータワークステーションまたはサーバでもよい。以下に限定されないが、ルータ、ネットワークステーション、ピア装置またはその他のネットワー

クノードなど他の装置も、コンピュータネットワーク内に存在してもよい。
【０１０１】
ネットワーク接続により、ローカルエリア・コンピュータネットワーク（ＬＡＮ）５０およびワイドエリア・コンピュータネットワーク（ＷＡＮ）が形成される。これらのネットワークは、企業コンピュータネットワークおよび社内ネットワークで使用され、通常はインターネットにアクセスできる。ＬＡＮまたはＷＡＮネットワークでは、パーソナルコンピュータ２０は、ネットワークアダプタまたはネットワークインタフェース５１を介して、ローカルエリア・ネットワーク５０に接続されている。ネットワークが使用されると、コンピュータシステム２０は、モデム５４、または、インターネットなどのワイドエリア・コンピュータネットワークによって通信を可能にする、当業者に周知のその他のモジュールを使用する。内部装置または外部装置であるモデム５４は、シリアルポート４６によってシステムバス２３に接続される。このネットワーク接続が、通信モジュールを使用して一つのコンピュータを別のコンピュータに接続させる数々の周知の方法の非限定的な例であることは、当業者であればわかるであろう。
【０１０２】
種々の側面において、ここに記載するシステムおよび方法は、ハードウェア、ソフトウェア、ファームウェアまたはその組み合わせにおいて実行される。ソフトウェアで実行される場合、この方法は１以上の命令またはコードとして非一時的なコンピュータ可読媒体に記憶されてもよい。コンピュータ可読媒体はデータ記憶装置も含む。一例では、このコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、フラッシュメモリ、その他の電気、磁気または光学記憶媒体、あるいは、命令やデータ構造の形式で所望のプログラムコードを伝達または記憶するために使用し、汎用コンピュータのプロセッサからアクセス可能な、その他の媒体を含んでもよいが、これらに限定されない。
【０１０３】
種々の側面において、ここに記載したシステムおよび方法は、モジュールによって処理することができる。「モジュール」という用語は、たとえば、application－specific integrated circuit（ＡＳＩＣ）またはfield－programmable gate array（ＦＰＧＡ）などのハードウェア、あるいは、モジュールの機能を実行するマイクロプロセッサシステムおよび命令一式などのハードウェアとソフトウェアとの組み合わせによって実行される、実装置、コンポーネントまたは一組のコンポーネントのことを指しており、これらは（実行中に）マイクロプロセッサシステムを専用装置に変換する。モジュールは、一部の機能をハードウェアのみで実行させ、他の機能をハードウェアとソフトウェアの組み合わせによって実行させるという、２つの組み合わせで実行させることもできる。特定の実施例では、モジュールの少なくとも一部、または、場合によってすべてが、汎用コンピュータのプロセッサで実行される（上記図３で詳しく説明）。よって、各モジュールは、様々な適切な設定で実行されるものであって、ここで例示した特定の実施例に限定されるものではない。
【０１０４】
なお、明瞭化のため、各側面の一般的な特徴すべてについては開示しない。本開示の実際の実装を開発する際、開発者の具体的な目的を達成するためには実装に応じた数々の決定を行わなければならず、具体的な目的は実装や開発者によって異なることに留意されたい。こうした開発上の取り組みは、複雑で時間を要するものであるが、本発明の利益を享受する当業者にとっては日常の作業であることを理解されたい。
【０１０５】
更に、ここで使用する用語又は表現は、あくまでも説明のためであり、限定するものではないことを理解されたい。よって、本明細書の用語又は表現は、関連技術の熟練者の知識と組み合わせて、本明細書に示す教示及び指針に照らして当業者によって解釈されたい。明細書又は特許請求の範囲における用語はいずれも、特に明記していない限り、一般的でない意味や特別な意味をもつものではない。
【０１０６】

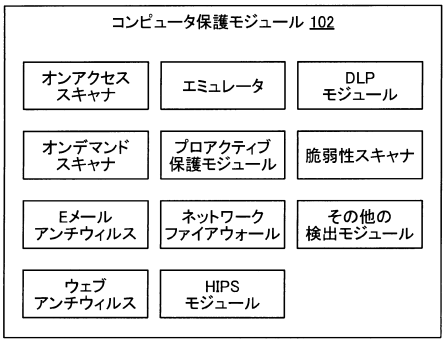
本明細書で開示した様々な側面は、本明細書で例示した既知のモジュールの、現在及び将来の既知の均等物を包含する。本明細書では、複数の側面及び応用例を示して説明したが、本明細書に開示した発明の概念の範囲内で、上記よりも多くの変形例が可能であることは、本発明の利益を享受する当業者にとって明らかであろう。

【図面】

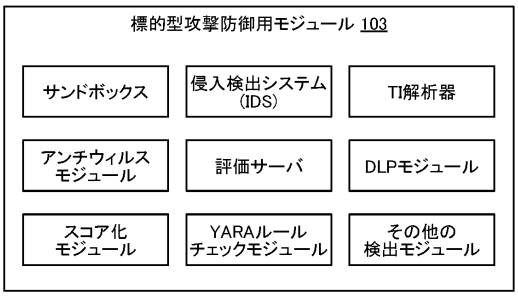
【図１】



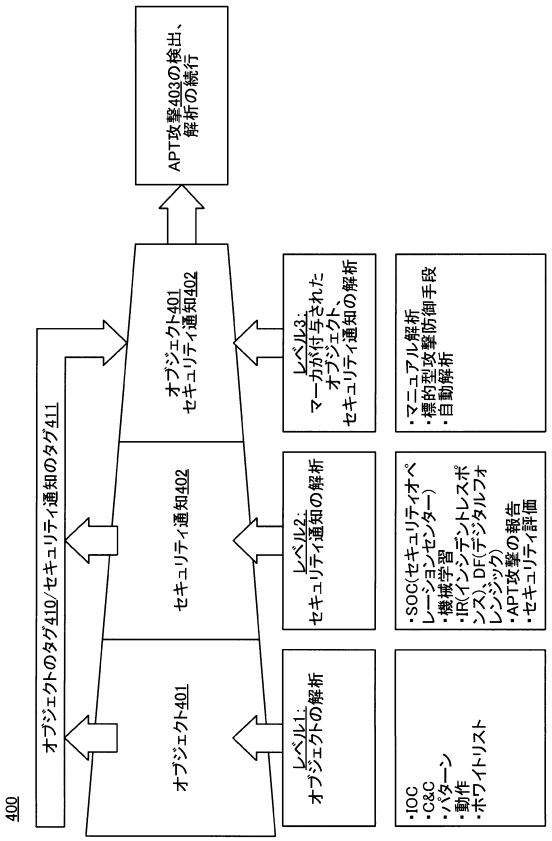
【図２】



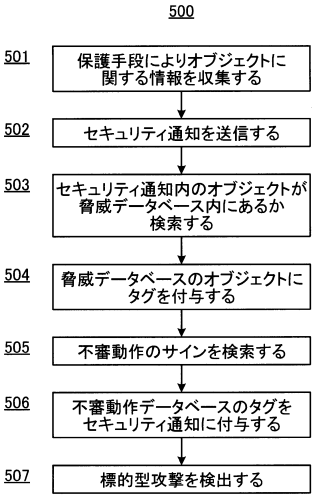
【図３】


標的型攻撃防御用モジュール 103
サンドボックス
侵入検出システム (IDS)
TI解析器
アンチウィルス モジュール
評価サーバ
DLPモジュール
スコア化 モジュール
YARAルール チェックモジュール
その他の 検出モジュール

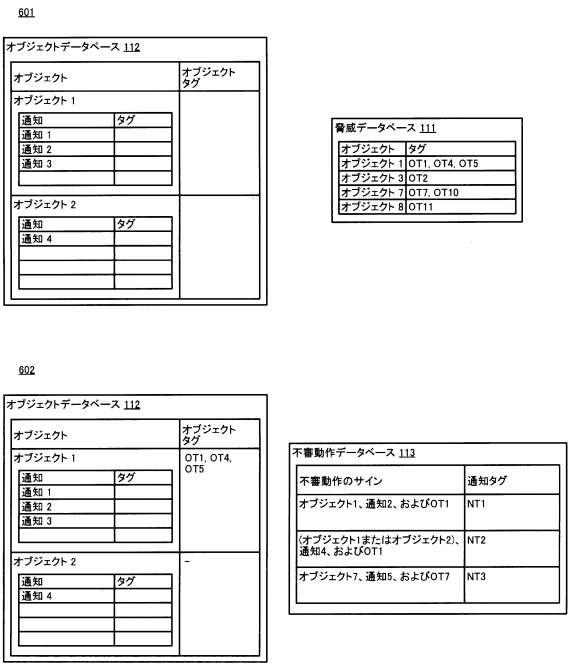
【図４】


APT攻撃403の検出、解析の続行
オブジェクト401 セキュリティ通知402
セキュリティ通知402
オブジェクト401
オブジェクトのタグ410/セキュリティ通知のタグ411
400
レベル3: マーカが付与されたオブジェクト セキュリティ通知の解析
レベル2: セキュリティ通知の解析
レベル1: オブジェクトの解析
・マニュアル解析
・標的型攻撃防御手段
・自動解析
・SOC(セキュリティオペレーションセンター)
・機械学習
・IR(インシデントレスポンス)、DF(デジタルフォレンジック)
・APT攻撃の報告
・セキュリティ評価
・IOC
・C&C
・パターン
・動作
・ホワイトリスト

【図５】


500
501
保護手段によりオブジェクトに関する情報を収集する
502
セキュリティ通知を送信する
503
セキュリティ通知内のオブジェクトが脅威データベース内にあるか検索する
504
脅威データベースのオブジェクトにタグを付与する
505
不審動作のサインを検索する
506
不審動作データベースのタグをセキュリティ通知に付与する
507
標的型攻撃を検出する

【図６Ａ】


601
オブジェクトデータベース 112
オブジェクト
オブジェクト タグ
オブジェクト 1
通知
タグ
通知 1
通知 2
通知 3
オブジェクト 2
通知
タグ
通知 4
脅威データベース 111
オブジェクト
タグ
オブジェクト 1 OT1, OT4, OT5
オブジェクト 3 OT2
オブジェクト 7 OT7, OT10
オブジェクト 8 OT11
602
オブジェクトデータベース 112
オブジェクト
オブジェクト タグ
オブジェクト 1
OT1, OT4, OT5
通知
タグ
通知 1
通知 2
通知 3
オブジェクト 2
-
通知
タグ
通知 4
不審動作データベース 113
不審動作のサイン
通知タグ
オブジェクト1、通知2、およびOT1
NT1
(オブジェクト1またはオブジェクト2)、通知4、およびOT1
NT2
オブジェクト7、通知5、およびOT7
NT3

【図６Ｂ】

603

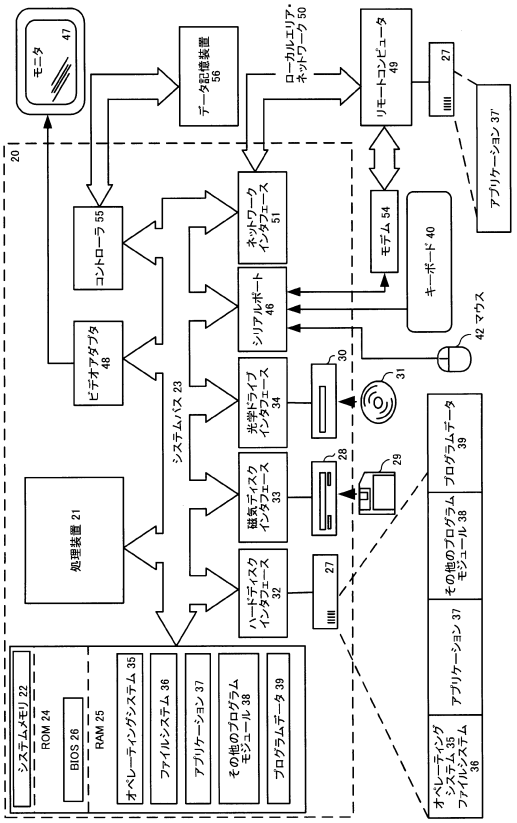
オブジェクトデータベース 112

オブジェクト		オブジェクトタグ
オブジェクト 1		OT1, OT4, OT5
	通知 / タグ	
	通知 1 /	
	通知 2 / NT1	
	通知 3 /	
オブジェクト 2		–
	通知 / タグ	
	通知 4 / NT2	

コンピュータ攻撃データベース 114

コンピュータ攻撃シグネチャ
オブジェクト1、OT1、通知2、およびNT1
(オブジェクト1またはオブジェクト2またはオブジェクト3)、(OT2またはOT4)、(通知1または通知4)および(NT2またはNT3)
オブジェクト7およびOT7

【図７】



フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(72)発明者 ユーリー ジー． パルシン
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内
(72)発明者 チェムール エス． ヘイルハバロフ
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内
(72)発明者 セルゲイ ヴィー． ソルダトフ
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内
審査官 吉田 歩
(56)参考文献 国際公開第２０１６／０６１０３８（WO，Ａ１）
特開２０１７－０２１７７７（ＪＰ，Ａ）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５６
Ｇ０６Ｆ ２１／５５