(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-507271
(P2009-507271A)
(43)公表日　平成21年2月19日(2009.2.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560B	5B017
H04L 9/32	(2006.01)	H04L	9/00	675A	5B276
G09C 1/00	(2006.01)	G09C	1/00	660D	5B285
G06F 21/22	(2006.01)	G06F	9/06	660N	5J104
G06F 21/20	(2006.01)	G06F	15/00	330A	

審査請求 未請求　予備審査請求 未請求　（全 55 頁）　最終頁に続く

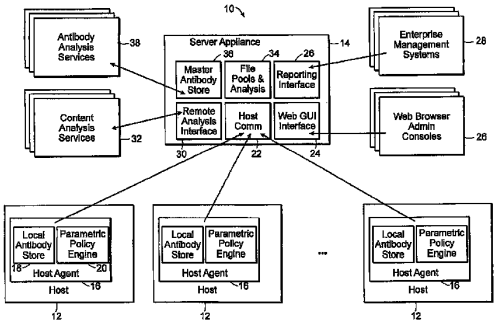
(21)出願番号　特願2008-524253 (P2008-524253)
(86)(22)出願日　平成18年7月27日 (2006.7.27)
(85)翻訳文提出日　平成20年3月19日 (2008.3.19)
(86)国際出願番号　PCT/US2006/029714
(87)国際公開番号　WO2007/016478
(87)国際公開日　平成19年2月8日 (2007.2.8)
(31)優先権主張番号　11/193,292
(32)優先日　平成17年7月29日 (2005.7.29)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/193,295
(32)優先日　平成17年7月29日 (2005.7.29)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/194,075
(32)優先日　平成17年7月29日 (2005.7.29)
(33)優先権主張国　米国 (US)

(71)出願人　508029778
ビットナイン・インコーポレーテッド
アメリカ合衆国マサチューセッツ州０２１４１，ケンブリッジ，テン・カナル・パーク
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行

最終頁に続く

(54)【発明の名称】ネットワーク・セキュリティ・システムおよび方法

(57)【要約】
セキュリティシステムは、知られているおよび知られていないウィルス、ワーム、スパイウェア、ハッカ、ならびに非所望または知られていないソフトウェアからの防御を提供することができる。システムは、管理者がファイル動作を承認、ブロック、隔離、または記録することを可能にする集中ポリシーを実施できる。システムはホスト内とサーバ内とにファイルメタ情報を維持する。ホストは、ファイルコンテンツまたはファイル名に変更を引き起こすことが可能なファイル動作を検出して、結果として、ホストおよび／またはサーバのメタ情報を更新する。サーバのメタ情報内の変更はホストに利用可能にされる。



【特許請求の範囲】
【請求項１】
サーバと、１つまたは複数の関連するホストコンピュータ（ホスト）とを有するシステム内で使用するための方法であって、
各独自のファイルに関して、コンテンツ署名と、前記ファイルの前記コンテンツの署名と、前記ファイルまたは前記署名が初めてサーバに報告された日と、ある種のファイル動作が前記ファイル上でホストによって実行され得るか否かおよび何の条件によるかを表示する状態データとを含めて、複数のファイルに関して前記サーバ上に前記サーバのメタ情報のセットを維持するステップと、
各ファイルに関し、前記ファイルコンテンツの前記状態データと前記署名とを含めて、複数のファイルに関して前記ホスト上にメタ情報を維持するステップと、
前記ホスト上にファイルコンテンツまたはファイル名に対する可能な変更を検出して、ホストおよび／またはサーバのメタ情報を更新するステップと、
前記サーバが前記ホストに前記サーバのメタ情報内の変更を提供するステップと、
を含む方法。
【請求項２】
前記コンテンツの前記署名は、前記ファイルの前記コンテンツの１つまたは複数の暗号ハッシュの結果を含む、請求項１に記載の方法。
【請求項３】
各ホストに関して、ファイル名と状態データとを有する個々の名前キャッシュを維持するステップをさらに含む、請求項１に記載の方法。
【請求項４】
前記ファイルのファイル動作に対する要求に応答して、前記ホストは、前記ファイル動作が許可されるか否かを決定するために前記名前キャッシュにアクセスし、前記名前キャッシュ内に、前記ファイル動作が許可されるか否かの表示が存在しない場合、前記ファイルの前記コンテンツをハッシュさせて、前記ファイル動作が許可されるか否かを決定するために前記ファイルの前記ハッシュを前記ホストキャッシュ内の前記メタ情報と比較する、請求項３に記載の方法。
【請求項５】
前記ホストキャッシュは、前記ファイル動作が許可されるか否かを決定するためのデータを有さない場合、前記ホストが前記サーバに問い合わせる、請求項４に記載の方法。
【請求項６】
アップロードされたファイルまたは前記ファイルの前記コンテンツの署名に応答して、アンチウィルス走査またはアンチスパイウェア走査を含めて、１つまたは複数の分析を実行させる、請求項５に記載の方法。
【請求項７】
前記分析が完了する前に前記ファイル動作が継続することが許可される、請求項６に記載の方法。
【請求項８】
前記分析がある種のファイル動作が許可されるべきでないことを表示する場合、前記サーバは、その後の試みについて、前記一定のファイル動作が前記ファイルに関して許可されないことを表示するために前記ホストにそのメタ情報を更新させる、請求項６に記載の方法。
【請求項９】
前記分析がある種のファイル動作が許可されるべきであることを表示する場合、前記サーバは、その後の試みについて、前記ある種のファイル動作が前記ファイルに関して許可されることを表示するために前記ホストにそのメタ情報を更新させる、請求項６に記載の方法。
【請求項１０】
ある種のファイル動作が許可されるべきであるか否かが未決定である場合、前記ホスト

は、一定の条件下でのみ、その後の試みについて、前記ファイルに関して前記ある種のファイル動作が許可されることを表示するためにそのメタ情報を更新する、請求項６に記載の方法。

【請求項１１】

ファイル内の埋込み動作状態のコンテンツに関して、前記ファイルから前記コンテンツを抽出して、前記コンテンツの暗号ハッシュを実行し、前記動作状態のコンテンツの前記ハッシュを保存するステップとをさらに含む、請求項２に記載の方法。

【請求項１２】

暗号ハッシュを実行するステップに先立って、縮小ファイルを作成するために、前記動作状態のコンテンツが有効なフォーマット済みファイル内に提供される、請求項１１に記載の方法。

【請求項１３】

前記動作状態のコンテンツはマクロを含み、前記有効なフォーマット済みファイルはワードプロセッシング文書を含む、請求項１２に記載の方法。

【請求項１４】

前記ホストが前記動作状態のコンテンツをそこから前記動作状態のコンテンツが抽出された前記ファイルと関連付ける、請求項１１に記載の方法。

【請求項１５】

ホストがファイルに関するファイル動作の要求を受信するステップに応答して、前記ホストが前記状態を決定するために前記ホストキャッシュにアクセスし、キャッシュの失敗が存在する場合、前記システムがさらなる分析を実行する間に、前記ホストは前記ファイル動作を遅らせる、請求項１に記載の方法。

【請求項１６】

前記ファイル動作は、実施と、ファイル読取りと、ファイル書込みとを含む、請求項１５に記載の方法。

【請求項１７】

前記さらなる分析は、アンチウィルス走査、スパイウェア走査、知られているファイルまたはコンテツのリストに対する比較、およびその他のサーバによって提供された結果に対する比較のうちの１つまたは複数を含む、請求項１５に記載の方法。

【請求項１８】

前記状態データは、前記ファイルの前記コンテンツに基づいてファイル動作が禁止されるか、前記ファイルの前記経路および名前に基づいて禁止されるか、承認されるか、前記ホストによって局所的に承認されるか、またはさらなる分析をペンディングして許可もしくは禁止されるかを含む、請求項１に記載の方法。

【請求項１９】

前記サーバは、前記ファイルまたは前記ファイルコンテンツの前記ハッシュが前記サーバによっていつ初めて参照されたかを表示するデータをさらに維持する、請求項１に記載の方法。

【請求項２０】

前記サーバは、前記ファイルが修正された最後のときを表示するデータをさらに維持する、請求項１に記載の方法。

【請求項２１】

前記状態データは、ファイル動作がいくつかのホストに関して禁止され、その他のホストに関して許可されることを表示するデータを含む、請求項１に記載の方法。

【請求項２２】

前記サーバは、いくつのホストがファイルの複写を有するかのカウントを維持する、請求項１に記載の方法。

【請求項２３】

前記サーバは、いくつのホストがファイルの複写を有するのかのカウントを使用して、前記カウントを閾値と比較し、前記カウントが閾値を超えた後にホストにファイル動作を

禁じる、請求項２２に記載の方法。
【請求項２４】
前記サーバは、分析結果と、勧告される状態とを表示するデータを維持する、請求項２３に記載の方法。
【請求項２５】
前記ホスト内に保存された前記メタ情報は、ファイル経路名と、初めて参照された日と、修正された最後の日とをさらに含む、請求項１に記載の方法。
【請求項２６】
ホスト記憶装置上のすべてのファイルは、変更が各ファイルに関して発生した場合と同様に分析され、前記分析がホスト状態をサーバ状態と同期化するために自動的にトリガされている、請求項１に記載の方法。
【請求項２７】
前記サーバ上の各ファイルに関する前記メタ情報は、前記ファイルの前記名前に関するデータを含む、請求項１に記載の方法。
【請求項２８】
前記サーバは、前記ホストによってアクセス可能なようにメタ情報内の変更を書き込むことによって、前記メタ情報内の変更を前記ホストに提供し、前記ホストが前記書き込まれた変更にアクセスして、前記ホスト上の前記メタ情報を修正する、請求項１に記載の方法。
【請求項２９】
サーバと、関連するホストコンピュータ（ホスト）とを有するシステム内で使用するための方法であって、
各独自のファイルに関して、コンテンツ署名と、前記ファイルの前記コンテンツの署名と、ある種のファイル動作が前記ファイル上でホストによって実行され得るか否かおよび何の条件によるかを表示する状態データと、前記ファイルまたは前記署名が初めて参照された時間とを含めて、複数のファイルに関してサーバ上にメタ情報のセットを維持するステップと、
各ファイルに関して、前記状態データと、前記ファイルコンテンツの前記署名と、前記ファイル経路名とを含めて、複数のファイルに関して前記ホスト上にメタ情報のセットを維持するステップと、
ホストがファイルコンテンツまたはフィルタ名に対する可能な変更を検出して、ホストおよび／またはサーバのメタ情報を更新するステップと、
前記サーバが前記ホストに前記サーバのメタ情報内の変更を提供するステップと
を含む方法。
【請求項３０】
前記サーバは前記ファイルに関してメタ情報をすでに有していない場合、前記ファイルが前記サーバにアップロードされる、請求項２９に記載の方法。
【請求項３１】
前記ホストは、前記ファイル名に基づいて情報を記憶する第１のキャッシュと、前記ファイルコンテンツのハッシュに基づいて情報を記憶する第２のキャッシュとにアクセスする、請求項２９に記載の方法。
【請求項３２】
前記サーバは、前記ファイルの前記コンテンツの１つまたは複数のハッシュを実行して、前記１つまたは複数のハッシュを前記ホストによって実行された前記ハッシュと比較する、請求項３０に記載の方法。
【請求項３３】
サーバと、関連するホストコンピュータ（ホスト）とを有するシステム内で使用するための方法であって、
各独自のファイルに関して、コンテンツ署名と、前記ファイルに関連するある種の動作が禁止されるか、許可されるか、またはまだ完全に決定されていないかおよび何の条件に

よるかを表示する状態データとを含めて、複数のファイルに関してサーバ上にメタ情報のセットを維持するステップと、
各ファイルに関して、前記状態データを含めて、複数のファイルに関して前記ホスト上にメタ情報のセットを維持するステップと、
前記ホスト上にファイルコンテンツまたはファイル名に対する可能な変更を検出して、ホストおよび／またはサーバのメタ情報を更新するステップと、
前記サーバが前記ホストに前記サーバのメタ情報内の変更を提供するステップと、
前記サーバ内に前記ファイルに関する入力が存在していないこと、または状態がまだ完全に決定されていないことに応答して、前記サーバが前記ファイルの分析を実行するステップと
を含む方法。
【請求項３４】
前記サーバは１つまたは複数のアンチウィルス走査またはアンチスパイウェア走査を引き起こす、請求項３３に記載の方法。
【請求項３５】
前記サーバは、特定のファイルに関してファイル動作が禁止されるべきかまたは許可されるべきかを後に決定し、前記サーバが状態のこの変更を前記ホストに伝播させる、請求項３４に記載の方法。
【請求項３６】
前記サーバは、前記ホストが前記変更にアクセスして、前記変更を取り出すようにメタ情報内の前記変更を書き込むことによって伝播する、請求項３５に記載の方法。
【請求項３７】
サーバと、
前記サーバに関連する複数のホストコンピュータ（ホスト）とを含むシステムであって、
前記サーバは、各ファイルに関して、前記ファイルの前記名前に関するデータと、前記ファイルの前記コンテンツの署名と、前記ファイルに関連するある種の動作が禁止されるか、許可されるか、またはまだ完全に決定されていないかおよび何の条件によるかを表示する状態データとを含めて、複数のファイルのメタ情報のセットを維持するためのサーバメモリを有し、
前記ホストの各々は、各ファイルに関して、前記状態データと前記署名とを含めて、複数のファイルに関してメタ情報のセットを維持するための局所メモリを有し、
前記ホスト上にファイルコンテンツまたはファイル名に対する可能な変更を検出して、ホストおよび／またはサーバのメタ情報を更新し、
前記サーバは前記ホストに前記サーバのメタ情報内の変更を提供する、
システム。
【請求項３８】
前記サーバは、前記ホストによってアクセス可能なように前記変更を書き込むことによって、変更を前記ホストに提供し、前記ホストが前記ホスト上の前記メタ情報を修正できるように、前記ホストが前記書き込まれた変更にアクセスすることを可能にする、請求項３７に記載の方法。
【請求項３９】
前記コンテンツの前記署名は、前記ファイルの前記コンテンツの１つまたは複数の暗号ハッシュの結果を含む、請求項３７に記載のシステム。
【請求項４０】
各ホストはファイル名と状態データとを含む個々の名前キャッシュを有する、請求項３７に記載のシステム。
【請求項４１】
ホストはファイルに関するファイル動作の要求を受信するステップに応答して、前記ホストが前記状態を決定するために前記ホストキャッシュにアクセスし、キャッシュの失敗

が存在する場合、前記システムがさらなる分析を実行する間、前記ホストは前記ファイル動作を遅らせる、請求項３７に記載のシステム。
【請求項４２】
前記サーバは、前記ファイルまたは前記ファイル・コンテンツ・ハッシュが前記サーバによっていつ初めて参照されたかを表示するデータをさらに維持する、請求項３７に記載のシステム。
【請求項４３】
前記サーバは、前記ファイルが修正された最後のときを表示するデータをさらに維持する、請求項３７に記載のシステム。
【請求項４４】
前記サーバは、いくつのホストがファイルの複写を有するかのカウントを維持する、請求項３７に記載のシステム。
【請求項４５】
前記ホスト内に保存された前記メタ情報は、ファイル経路名と、初めて参照された日と、最後に修正された日とをさらに含む、請求項３７に記載のシステム。
【請求項４６】
複数のホストコンピュータ（ホスト）と、前記ホストに関連するサーバとを有するコンピュータシステムと共に使用するための方法であって、
前記サーバが、ファイル動作に関連するポリシーと、少なくともこのような動作が許可されるかまたは禁止されるかおよび何の条件によるかを表示するポリシーオプションとのマスタセットを前記ホストに伝播するステップと、
前記サーバが値を前記ホストに伝播するステップと
を含み、
前記ホスト上に記憶された前記値は、ポリシーおよびポリシーオプションの前記マスタセットからどのポリシーおよびポリシーオプションのサブセットが前記ホスト上で実施するかを表示し、
前記ホストは前記値によって表示された前記ファイル動作ポリシーを実施する
方法。
【請求項４７】
各ポリシーは、前記ポリシーオプションのうちの１つを表示する単一の構成パラメータを有し、伝播された前記値が、いくつかのポリシーの各々に関して前記ポリシーオプションを選択する、請求項４６に記載の方法。
【請求項４８】
前記マスタセットは、ポリシーおよびオプションのリストを含み、伝播された前記値が前記リストのうちの１つを選択する、請求項４６に記載の方法。
【請求項４９】
前記ポリシーは、ファイル動作を実行するためのホストの能力を増分的に増加または削減する順序付けされた規制のセットを構成する少なくとも３つのオプションを有する、請求項４６に記載の方法。
【請求項５０】
前記サーバは、管理者による手動の変更に応答して前記値を変更する、請求項４６に記載の方法。
【請求項５１】
前記サーバは、人間の管理者からのインプットなしに自動的に前記値を変更する、請求項４６に記載の方法。
【請求項５２】
前記自動サーバ値変更は、検出されたセキュリティイベントまたはＳＮＭＰメッセージもしくはシスログメッセージならびに報告書またはネットワークメッセージもしくは電子メールメッセージに応答する、請求項５１に記載の方法。
【請求項５３】

前記ホストは、人間からのインプットなしに、または前記サーバからのコマンドなしに、前記値を自動的に変更する、請求項４６に記載の方法。

【請求項５４】

前記ホストは、同じホストに関するポリシー報告書に応答して、もしくは前記ホスト上で検出されたイベントに応答して、または前記ホスト上で実施されたコマンドに応答して、前記値を自動的に変更する、請求項４６に記載の方法。

【請求項５５】

前記ポリシーオプションは、実施および／または読取り動作が承認されることを表示する関連するメタ情報状態を有するファイルのこのような動作を自動的に許可する、請求項４６に記載の方法。

【請求項５６】

前記ポリシーオプションは、実施および／または読取りが禁止されることおよび／または前記サーバに報告書を送ることを表示する関連するメタ情報状態を有するファイルのこのような動作をブロックするステップを含む、請求項４６に記載の方法。

【請求項５７】

前記ポリシーオプションは、実施および／または読取りが許可されるかまたは禁止されるかがまだ決定されていないことを表示する関連するペンディングメタ情報状態を有するファイルのこのような動作をブロックするステップを含む、請求項４６に記載の方法。

【請求項５８】

前記ポリシーオプションは、実施および／または読取りが許可されるかまたは禁止されるかがまだ完全に決定されていないことを表示する関連するペンディングメタ情報状態を有するファイルのこのような動作をブロックするステップを含む、請求項４６に記載の方法。

【請求項５９】

前記ポリシーオプションは、ある動作が許可されるかまたは禁止されるかがまだ完全に決定されていないことを表示する関連するペンディングメタ情報状態を有するファイルに関するこのような動作の要求の場合に、報告書を前記サーバに送信するステップを含む、請求項４６に記載の方法。

【請求項６０】

前記ポリシーオプションは、関連するペンディングおよび／または禁止メタ情報状態を有する新ファイルの作成もしくは修正または初めての実施を検出および追跡するステップを含む、請求項４６に記載の方法。

【請求項６１】

前記ポリシーオプションは、関連するペンディングメタ情報状態を有するファイルの作成または修正をブロックするステップを含む、請求項４６に記載の方法。

【請求項６２】

前記ポリシーオプションは、関連する禁止メタ情報状態を有するファイルの自動削除または自動移動を含む、請求項４６に記載の方法。

【請求項６３】

前記ポリシーオプションは、承認のために、新たに作成または修正されたファイルのメタ情報状態を前記ホストに自動的に設定するステップを含む、請求項４６に記載の方法。

【請求項６４】

前記ポリシーオプションは、承認のために、前記ホスト上で新たに作成または修正されたファイルのサーバのメタ情報状態を設定するステップを含む、請求項４６に記載の方法。

【請求項６５】

前記ホストは前記ホスト上の前記ファイルの各々に関してメタ情報を維持し、前記メタ情報が少なくとも３つの可能な値、すなわち、承認、禁止、およびペンディングを有する状態を含む、請求項４６に記載の方法。

【請求項６６】

許可するための表示は、さらなる監視なしに動作を許可する、請求項６５に記載の方法。

【請求項６７】

前記ポリシーオプションは、前記ホストおよび／または前記サーバが前記ファイルを分析する間、ファイル動作を遅らせるステップを含む、請求項６５に記載の方法。

【請求項６８】

サーバはファイルに関連するメタ情報を有さないことを決定した場合、前記サーバは前記ペンディング状態を前記ファイルと関連付ける、請求項６７に記載の方法。

【請求項６９】

ホストがファイルに関連するメタ情報を有さないことを決定した場合、前記ホストが前記ペンディング状態を前記ファイルと関連付ける、請求項６７に記載の方法。

【請求項７０】

前記サーバは、ファイルが任意のホストによっていつ初めて参照されたかを表示するメタ情報を維持する、請求項４６に記載の方法。

【請求項７１】

前記ポリシーおよび前記ポリシーオプションのうちの少なくともいくつかは、ファイルの前記名前に基づいて動作動作を表示する、請求項４６に記載の方法。

【請求項７２】

前記ポリシーおよび前記ポリシーオプションのうちの少なくともいくつかは、ファイルの前記コンテンツに基づいて動作を表示する、請求項４６に記載の方法。

【請求項７３】

前記ポリシーおよび前記ポリシーオプションのうちの少なくともいくつかは、ファイルの前記名前および前記コンテンツの組合せに基づいて動作を表示する、請求項４６に記載の方法。

【請求項７４】

前記サーバは、前記ファイルのコンテンツのハッシュを含めて、ファイルに関するメタ情報を維持する、請求項４６に記載の方法。

【請求項７５】

前記ファイルの前記コンテンツの前記ハッシュが前記ファイル内の前記当該コンテンツのハッシュである、請求項７４に記載の方法。

【請求項７６】

前記ポリシーは、新ファイルの実施と、ファイルに対する書込みアクセスと、ファイルに対する読取りとを含み、前記オプションが、前記動作が発生することを可能にすること、前記動作を禁止すること、またはさらなる監視により前記動作を承認することを含む、請求項４６に記載の方法。

【請求項７７】

前記さらなる監視は、１つまたは複数の追跡記録と、報告書を提供することとを含む、請求項７６に記載の方法。

【請求項７８】

前記値のうちの１つはすべての新実行可能を禁止する、請求項４６に記載の方法。

【請求項７９】

前記値のうちの１つはすべてのファイル動作を可能にする、請求項４６に記載の方法。

【請求項８０】

前記サーバは、前記ホストによってアクセス可能なように新しい値を書き込むことによって前記値を変更し、前記ホストが前記新しい値にアクセスし、前記新しい値を前記ホストが有する前記値と比較して、その値を前記新しい値に変更する、請求項４６に記載の方法。

【請求項８１】

値ならびに関連するポリシーおよびポリシーオプションの順序付けされたセットが存在し、前記ホストがその他の中間値により増分的に前記新しい値に変更する、請求項８０に

記載の方法。
【請求項８２】
前記ホストの各々は、複数のホストグループのうちの１つに配置され、前記サーバは、ホストグループが異なる値を有するように、前記ホストグループのすべてではなくホストグループの少なくとも１つに関して前記値を変更する、請求項４６に記載の方法。
【請求項８３】
前記サーバは、前記新しい値を前記ホストに送信することによって前記値を変更する、請求項４６に記載の方法。
【請求項８４】
サーバファイルのメタ情報状態に対する変更がホストに利用可能にされかつ／またはホストに伝播する、請求項５４に記載の方法。
【請求項８５】
複数のホストコンピュータ（ホスト）と、
ファイル動作に関連するポリシーと、このような動作が許可されるかまたは禁止されるかおよび何の条件によるかを表示するポリシーオプションとのマスタセットを前記ホストに伝播するためのサーバであって、
値を前記ホスト上の記憶のために前記ホストにさらに伝播するためのサーバと
を含み、
前記ホスト上に記憶された前記値がポリシーおよびポリシーオプションの前記マスタセットからどのポリシーおよびポリシーオプションのサブセットが前記ホスト上で実施するかを表示し、
前記ホストが前記値によって表示された前記ファイル動作ポリシーを実施する、
コンピュータシステム。
【請求項８６】
前記サーバによって伝播された前記情報は、いくつかの異なるポリシーの各々に関してポリシーオプションのセットを表示する値を含む、請求項８５に記載のシステム。
【請求項８７】
前記ホストは複数のホストグループに編成され、前記サーバは前記値内の変更を前記ホストグループのすべてではなく前記ホストグループの１つまたは複数に伝播する、請求項８６に記載のシステム。
【請求項８８】
前記ファイル動作がファイルに対する書込みアクセスと、ファイルの実施とを含み、前記オプションが、ファイル動作を実行するためのホストの能力を増分的に増加または削減する順序付けされた規制のセット内に複数のオプションを有する、請求項８５に記載のシステム。
【請求項８９】
前記マスタセットがポリシーのリストとポリシーオプションとを含み、前記サーバは前記リストのうちの１つを表示する値を含む情報を提供する、請求項８５に記載のシステム。
【請求項９０】
前記サーバは、前記ホストによってアクセス可能な場所の中に前記情報を書き込み、前記ホストは前記情報にアクセスして、それらの値を更新する、請求項８５に記載のシステム。
【請求項９１】
サーバと、前記サーバに関連する複数のホストコンピュータとを有するシステム内で使用するための方法であって、
前記サーバはファイルに関してメタ情報問合せを特定するステップと、
ホストの１つまたは複数のグループに前記メタ情報問合せを配信するステップと、
前記ホストがメモリ内に記憶された局所ホストのメタ情報から前記メタ情報問合せを実行するステップと、

前記ホストは、メタ情報の前記問合せからの結果を前記サーバに送信するステップであって、前記結果が前記ホスト上のファイルに関する情報を含むステップと、
前記サーバは前記ホストからの前記結果を受信および記憶するステップと
を含む方法。
【請求項９２】
前記サーバは、規則のセットからセキュリティポリシーを設定して、前記サーバは、前記ホストから受信された前記問合せの前記結果に応答して、前記ホストのうちの少なくともいくつかに適用可能な前記規則を自動的に変更する、請求項９１のシステム。
【請求項９３】
前記サーバは、前記結果に応答して、セキュリティ警告を自動的にトリガする、請求項９２に記載の方法。
【請求項９４】
前記サーバは、前記ホストから結果が受信されると、統合報告書を作成するために前記結果を併合する、請求項９１に記載の方法。
【請求項９５】
前記サーバは前記問合せを各ホストに送付する、請求項９１に記載の方法。
【請求項９６】
前記サーバは各ホストによるアクセスのために前記問合せを書込み、各ホストは前記サーバによって書き込まれた前記問合せを取得する、請求項９１に記載の方法。
【請求項９７】
ホストのグループに関して問合せされ得るファイルに関する前記メタ情報は、
ファイル名に関する正規表現パターン仕様と、
ファイル経路に関する正規表現パターン仕様と、
ファイルの当該コンテンツのハッシュと、
ファイルまたは前記ファイルの前記ハッシュが前記ホストによって初めて参照されたときの時間範囲と、
前記ホストのＩＰアドレスと、
前記ファイルのタイプと、
少なくとも３つの状態、すなわち、承認、禁止、ペンディングの分析のセットから前記ファイルに関連する１つまたは複数のホストファイル状態と、
ある種のファイル動作が前記ファイル上の前記ホスト、およびホストグループによって実行されているかどうかと、
のうちの１つまたは複数を含む、請求項９１に記載の方法。
【請求項９８】
前記問合せは識別されたファイル名前を有するファイルに関する、請求項９７に記載の方法。
【請求項９９】
前記問合せは識別されたファイル経路を有するファイルに関する、請求項９７に記載の方法。
【請求項１００】
前記問合せはそのコンテンツの識別されたハッシュを有するファイルに関する、請求項９７に記載の方法。
【請求項１０１】
前記問合せは、前記ファイルが前記ホストによって初めて参照されたときの識別された時間範囲を有するファイルに関する、請求項９７に記載の方法。
【請求項１０２】
前記問合せは、ファイル動作の識別された状態を有するファイルに関し、前記状態が、ファイル動作が承認されているかまたは禁止されているかを示す、請求項９７に記載の方法。
【請求項１０３】

前記問合せは項目（１）から（６）のうちの２つ以上を含む、請求項９７に記載の方法。

【請求項１０４】

前記問合せは項目（１）から（６）のうちの３つ以上を含む、請求項９７に記載の方法。

【請求項１０５】

前記サーバに対して前記ホストによって識別された各ファイルに関する結果は、

ファイル名と、

ファイル経路と、

ファイルの当該コンテンツのハッシュと、

ファイルまたは前記ファイルの前記ハッシュが前記ホストによって初めて参照された時間と、

前記ホストの名前と、

前記ホストのＩＰアドレスと、

前記ファイルのタイプと、

少なくとも３つの状態、すなわち、承認、禁止、ペンディングの分析のセットからの前記ファイルに関連する１つまたは複数のファイル状態と、

ある種のファイル動作が前記ファイル上の前記ホスト、およびホストグループによって実行されているかどうかと

を含む、請求項９１に記載の方法。

【請求項１０６】

前記サーバはメタ情報の記憶装置を維持し、前記サーバはホストメモリ内に記憶されたメタ情報を変更するために前記ホストに更新を提供する、請求項９１に記載の方法。

【請求項１０７】

前記ホストは最後に知られている修正されたメタ情報時間を用いて調査し、前記サーバはメタ情報の局所ホスト記憶装置に対する更新がペンディングされるか否かの表示を送り返す、請求項９６に記載の方法。

【請求項１０８】

ホストのメタ情報はカーネル内およびユーザ領域内の複数の永続キャッシュ内に記憶される、請求項９６に記載の方法。

【請求項１０９】

ファイルまたは前記ファイルに関する前記メタ情報は、前記ファイルが前記サーバによって初めて参照された後、定義された期間削除される、請求項９６に記載の方法。

【請求項１１０】

前記サーバ内に維持された前記メタ情報は、コンテンツ署名と、ホストの前記１つまたは複数のグループによって初めて参照された日／時間と、最近の分析結果の履歴と時間とを含む、請求項９６に記載の方法。

【請求項１１１】

前記サーバ内に維持された前記メタ情報は、最近の状態変更の履歴と、変更の理由と、前記メタ情報が最後に変更された時間とをさらに含む、請求項１１０に記載の方法。

【請求項１１２】

いくつかのホストコンピュータと、

前記ホストコンピュータに関連するサーバと

を含み、

各ホストコンピュータは、名前情報と、コンテンツ情報と、前記コンテンツのハッシュと、いくつかのファイルの各々に関するセキュリティ情報とを含むメタ情報データ記憶装置を有し、前記ホストコンピュータが、定義された基準に基づいて前記メタ情報を探索して、前記基準を満たすファイルのリストを提供するために前記サーバからの問合せに応答する、

コンピュータシステム。

【請求項１１３】
前記問合せは管理インターフェースを通じて前記サーバに提供される、請求項１１２に記載のシステム。
【請求項１１４】
前記ホストコンピュータは、メタ情報更新を取得するために周期的に前記サーバを検査する、請求項１１２に記載のシステム。
【請求項１１５】
ホストのグループに関して問合せされ得るファイルに関する前記メタ情報は、
ファイル名に関する正規表現パターン仕様と、
ファイル経路に関する正規表現パターン仕様と、
ファイルの当該コンテンツのハッシュと、
ファイルまたは前記ファイルの前記ハッシュが前記ホストによって初めて参照されたときの時間範囲と、
前記ホストの名前と、
前記ホストのＩＰアドレスと、
前記ファイルのタイプと、
少なくとも３つの状態、すなわち、承認、禁止、ペンディングの分析のセットからの前記ファイルに関連する１つまたは複数のホストファイル状態と、
ある種のファイル動作が前記ファイル上の前記ホスト、およびホストグループによって実行されているかどうかと
のうちの１つまたは複数を含む、請求項１１２に記載のシステム。
【請求項１１６】
前記問合せは識別されたファイル名前を有するファイルに関する、請求項１１２に記載のシステム。
【請求項１１７】
前記問合せは識別されたフェイル経路を有するファイルに関する、請求項１１２に記載のシステム。
【請求項１１８】
前記問合せは当該コンテンツの識別されたハッシュを有するファイルに関する、請求項１１２に記載のシステム。
【請求項１１９】
前記問合せは、前記ファイルまたは前記ファイルハッシュが前記ホストによって初めて参照されたときの識別された時間範囲を有するファイルに関する、請求項１１２に記載のシステム。
【請求項１２０】
前記問合せは、ファイル動作に関して識別された状態を有するファイルに関し、前記状態がある種のファイル動作が一定の条件に基づき承認されているかまたは禁止されているかを表示する、請求項１１２に記載のシステム。
【請求項１２１】
前記問合せは項目（１）から（６）のうちの２つ以上を含む、請求項１１２に記載のシステム。
【請求項１２２】
前記問合せが項目（１）から（６）のうちの３つ以上を含む、請求項１１２に記載のシステム。
【請求項１２３】
サーバと、関連するホストのグループと共に使用するための方法であって、
前記サーバのメタ情報内に、前記ホスト上で決定されたファイルに関連する状態を記憶するステップであって、前記メタ情報が前記ファイルの前記コンテンツの署名を含むステップと、
各署名に関して初期時間を記憶するステップと、

前記初期時間に関連する定義された期間に、前記ファイルの少なくとも１つのセキュリティ分析、または前記ファイルコンテンツの前記署名の分析を実行するステップと、
前記ファイル状態を変更して、前記変更された状態に関連する情報を前記ホストに提供するステップと
を含む方法。
【請求項１２４】
前記実行するプロセスは、アンチウィルス走査およびアンチスパイウェア走査のうちの１つを実行するステップを含む、請求項１２３に記載の方法。
【請求項１２５】
前記署名が前記コンテンツの１つまたは複数の暗号ハッシュを含み、前記サーバが独自のハッシュを有する各ファイルの単一の複写を記憶する、請求項１２３に記載の方法。
【請求項１２６】
ある種のファイル動作が前記ファイルに関して前記ホストによって実行され得るか否かおよび何の条件によるかを表示する状態を記憶するステップをさらに含み、前記実行するプロセスは、それに関してある種のファイル動作が一定の条件に基づいて承認または禁止されている署名の１つまたは複数のリストを検査することを含む、請求項１２３に記載の方法。
【請求項１２７】
前記初期時間に関連する前記定義された期間が、前記ファイルまたは前記署名が定義された期間内に前記ホストおよび／または前記サーバによって初めて参照された日を有するすべてのファイルである、請求項１２３に記載の方法。
【請求項１２８】
ある種のファイル動作は前記ファイルに関して前記ホストによって実行され得るか否かおよび何の条件によるかを表示する状態を記憶するステップをさらに含み、前記状態が、禁止、許可、または一定の条件に基づいてある種のファイル動作に関してさらなる監視の許可を含む、請求項１２３に記載の方法。
【請求項１２９】
前記さらなる監視は、追跡記録するステップまたは報告書を提供するステップを含む、請求項１２８に記載の方法。
【請求項１３０】
前記サーバ上の各メタ情報記録に関して、各分析に関連する追加の記録を記憶するステップをさらに含む、請求項１２３に記載の方法。
【請求項１３１】
前記追加の記録は、分析を実行するアクタと、分析時間と、分析結果とに関連するデータを含む、請求項１３０に記載の方法。
【請求項１３２】
前記追加の記録は、勧告される状態と、分析結果情報ストリングとをさらに含む、請求項１３１に記載の方法。
【請求項１３３】
前記分析に応答して、シスログメッセージおよび／または統計更新および／または警告を生成するステップをさらに含む、請求項１２３に記載の方法。
【請求項１３４】
前記分析は、コンテンツ転送、メタ情報転送、分析転送、およびセキュリティ規則の変更のうちの１つまたは複数を引き起こす、請求項１２３に記載の方法。
【請求項１３５】
請求項１に記載の動作は、もう１つの当事者のホストコンピュータへの外部委託サービスとして実行される、請求項１２３に記載の方法。
【請求項１３６】
前記サーバは、禁止または承認されるとして設定されたある種の動作を有するファイルのリストに対する変更をその他のネットワークデバイスに自動的に通知する、請求項１３

５に記載の方法。
【請求項１３７】
前記サービスは、年齢と分析結果とに基づいて、最近のメタ情報をその他のサーバとネットワークデバイスとに転送する、請求項１３５に記載の方法。
【請求項１３８】
前記セキュリティ分析は、最近の分析結果をその他のサーバの最近の分析結果と比較するステップを含む、請求項１２３に記載の方法。
【請求項１３９】
前記セキュリティ分析はユーザ定義されたコンテンツ分析を含む、請求項１２３に記載の方法。
【請求項１４０】
前記サーバは前記初期時間に基づいて複数の時間に実行される複数の分析のセットを有する、請求項１２３に記載の方法。
【請求項１４１】
前記複数の時間のうちの１つは、前記初期時間の翌日未満であり、前記複数の時間のうちのもう１つは、前記初期時間の翌日を超える、請求項１４０に記載の方法。
【請求項１４２】
前記複数の時間のうちの１つは、前記初期時間の翌日未満であり、前記複数の時間のうちのもう１つが、前記初期時間の翌週を超える、請求項１４０に記載の方法。
【請求項１４３】
前記初期時間は、前記ファイルまたは前記ファイルコンテンツの前記ハッシュがホストによって前記システム内で初めて参照された時間に関連する、請求項１２３に記載の方法。
【請求項１４４】
前記初期時間は、前記ファイルまたは前記ファイルコンテンツの前記ハッシュがサーバによって前記システム内で初めて参照された時間に関連する、請求項１２３に記載の方法。
【請求項１４５】
前記サーバは、ポリシーのセットを前記ホストに伝播し、前記サーバが、前記ポリシーのうちのどれが前記ホストによって実施されるかおよびどの条件に基づくかを表示する情報も提供する、請求項１２３に記載の方法。
【請求項１４６】
前記ホストは第１のファイルを受信し、前記第１のファイル内の当該コンテンツを抽出し、縮小ファイルを作成するために前記当該コンテンツを有効なフォーマット済みファイル内に再パッケージ化し、前記縮小ファイルにハッシュを適用するステップをさらに含む、請求項１２３に記載の方法。
【請求項１４７】
前記ファイルの少なくとも１つのセキュリティ分析を実行する前記プロセスは、前記ファイルをもう１つのコンピュータシステムに提供して、そこから分析結果を受信するステップを含む、請求項１２３に記載の方法。
【請求項１４８】
ある種のファイル動作が前記ファイルに関して前記ホストによって実行され得るか否かおよび何の条件によるかを表示する状態を記憶するステップをさらに含み、前記サーバが、前記状態に変更が存在する場合、ホストにメタ情報を伝播する、請求項１２３に記載の方法。
【請求項１４９】
前記サーバは、前記メタ情報が前記ホストによってアクセスおよび取得されるように、前記メタ情報を書き込むことによって伝播する、請求項１４８に記載の方法。
【請求項１５０】
前記サーバは、前記コンテンツのハッシュを実行し、前記ハッシュを前記ホストのうち

の少なくとも１つによって実行されたハッシュと比較する、請求項１２３に記載の方法。
【請求項１５１】
前記サーバは、複数のハッシュを実行する、請求項１５０に記載の方法。
【請求項１５２】
ホストは、前記署名および／または前記ファイルコンテンツを前記サーバにアップロードする前に前記サーバが特定のファイルに関してメタ情報を有するか否かを決定するために前記サーバに問い合わせる、請求項１２３に記載の方法。
【請求項１５３】
前記サーバは、署名または名前が承認されたファイルのホワイトリストに対応するか否かを決定するために遠隔ネットワークデバイスに問い合わせる、請求項１２３に記載の方法。
【請求項１５４】
前記サーバは、署名または名前が禁止されたファイルのブラックリストに対応するか否かを決定するために遠隔ネットワークデバイスに問い合わせる、請求項１２３に記載の方法。
【請求項１５５】
前記サーバは、署名または名前が新ファイルもしくは分類されていないファイルのペンディングリストに対応するか否かを決定するために遠隔ネットワークデバイスに問い合わせる、請求項１２３に記載の方法。
【請求項１５６】
前記サーバは、ファイルと署名をその他のファイルと署名のグループと関連付ける情報を記憶する、請求項１２３に記載の方法。
【請求項１５７】
前記サーバは、ファイルと署名をその他のサーバ上に記憶された情報に関する統計と関連付ける情報を記憶する、請求項１２３に記載の方法。
【請求項１５８】
前記署名は、前記コンテンツの１つまたは複数の暗号ハッシュを含み、前記サーバが、関連する製品と、前記ファイルハッシュに関連する前記製品に対応するその他のファイルとを識別する目的で、知られている製品分類データベースに対してハッシュを調査するために遠隔ネットワークデバイスに問い合わせる、請求項１２３に記載の方法。
【請求項１５９】
前記サーバは前記ネットワーク上のもう１つのデバイスに問い合わせることにより、前記サーバが、コンテンツの問合せ、メタ情報の問合せ、分析結果の問合せ、およびセキュリティ規則の問合せのうちの１つまたは複数を実行する、請求項１２３に記載の方法。
【請求項１６０】
各ファイルに関して、ある種のファイル動作が前記ファイルに関してホストによって実行され得るか否かおよび何の条件によるかを表示する状態を含めて、サーバに関連する前記ホスト上で決定されたファイルに関連するセキュリティ関連のメタ情報を記憶するためのメモリを含むサーバを含むコンピュータシステムであって、
前記サーバは、前記ファイルまたは前記ファイルの署名が前記ホストおよび／または前記サーバによって受信されたときの初期時間に基づく定義された期間に、前記ファイルの少なくとも１つのセキュリティ分析を引き起こし、
少なくともいくつかの分析に応答して、前記状態を変更して、前記変更された状態に関連する情報を前記ホストに提供する
コンピュータシステム。
【請求項１６１】
前記サーバに関連するホストのグループをさらに含む、請求項１６０に記載のシステム。
【請求項１６２】
前記サーバは、ある種のファイル動作が前記ファイルに関して前記ホストによって実行

され得るか否かおよび何の条件によるかを表示する状態を記憶し、前記実行するプロセスが、それに関してファイル動作が承認または禁止されたファイルの１つまたは複数のリストを検査するステップを含む、請求項１６１に記載のシステム。

【請求項１６３】

前記サーバは、禁止または承認されるとして設定された動作のリストに対する変更をその他のネットワークデバイスに自動的に通知する、請求項１６０に記載のシステム。

【請求項１６４】

前記サーバは、年齢と分析結果とに基づいて、最近のメタ情報をその他のサーバとネットワークデバイスとに転送する、請求項１６１に記載のシステム。

【請求項１６５】

前記初期期間は、前記ファイルまたは前記ファイルコンテンツの前記ハッシュが前記サーバによって前記システム内で初めて参照された時間に関連する、請求項１６０に記載のシステム。

【請求項１６６】

前記サーバは前記ホストにポリシーのセットを伝播し、前記サーバは、前記ポリシーのうちのどれが前記ホストによって実施されるかおよびどの条件に基づくかを表示する情報も提供する、請求項１６１に記載のシステム。

【請求項１６７】

前記サーバは、ある種のファイル動作が前記ファイルに関して前記ホストによって実行され得るか否かおよび何の条件によるかを表示するファイルに関する状態を記憶し、前記サーバが、前記状態に変更が存在する場合、ホストにメタ情報を伝播する、請求項１６１に記載のシステム。

【請求項１６８】

前記サーバは、前記メタ情報が前記ホストによってアクセスおよび取得されるように、前記メタ情報を書き込むことによって伝播する、請求項１６７に記載のシステム。

【請求項１６９】

前記署名は、前記コンテンツの１つまたは複数の暗号ハッシュを含み、前記サーバが、前記コンテンツのハッシュを実行して、前記ハッシュを前記ホストのうちの少なくとも１つによって実行されたハッシュと比較する、請求項１６１に記載のシステム。

【請求項１７０】

前記サーバは、署名を取得するために複数のハッシュを実行する、請求項１６９に記載のシステム。

【請求項１７１】

第１のファイルを受信するステップと、

前記第１のファイル内の当該コンテンツを抽出するステップと、

縮小ファイルを作成するために前記当該コンテンツを有効なフォーマット済みタイプの１つまたは複数のファイル内に再パッケージ化するステップと、

前記縮小ファイルに署名を適用するステップと、

前記署名を記憶して、前記署名を第１のファイルと関連付けるステップと

を含むコンピュータで実施される方法。

【請求項１７２】

第２のファイルに関して、請求項１に記載の動作を実行して、前記第１の縮小ファイルの前記署名と前記第２の縮小ファイルの前記署名とが同じであるか否かを決定するために、それらを比較するステップをさらに含む、請求項１７１に記載の方法。

【請求項１７３】

前記署名は、前記ファイルコンテンツの１つまたは複数の暗号ハッシュを含む、請求項１７２に記載の方法。

【請求項１７４】

請求項１に記載の動作がホストコンピュータ上で実行され、前記第１の縮小ファイルが、さらなるコンテンツ分析のために前記ホストコンピュータに関連するサーバに転送され

る、請求項１７１に記載の方法。
【請求項１７５】
前記当該コンテンツはマクロを含む、請求項１７１に記載の方法。
【請求項１７６】
前記当該コンテンツはワードプロセッシング文書として再パッケージ化される、請求項１７５に記載の方法。
【請求項１７７】
前記ハッシュを記憶するステップが、前記縮小ファイルまたはその署名が前記サーバによって初めて参照された日を記憶するステップをさらに含む、請求項１７１に記載の方法。
【請求項１７８】
前記第１のファイルはプレゼンテーションスライドを含むプレゼンテーションファイルである、請求項１７１に記載の方法。
【請求項１７９】
前記第１の縮小ファイルを電子メール添付ファイルとして送信するステップをさらに含む、請求項１７１に記載の方法。
【請求項１８０】
前記電子メールは、電子メール添付書類のためのウィルス走査能力を有するゲートウェイに送信される、請求項１７８に記載の方法。
【請求項１８１】
前記当該コンテンツは、実行可能、スクリプト、アーカイブ、またはインストーラのうちの１つを含む、請求項１７１に記載の方法。
【請求項１８２】
前記当該コンテンツは、ワードプロセッシング文書またはアーカイブファイルとして再パッケージ化される、請求項１７１に記載の方法。
【請求項１８３】
前記署名は前記ファイルコンテンツの１つまたは複数の暗号ハッシュを含む、請求項１７１に記載の方法。
【請求項１８４】
各ファイルに関して、前記コンテンツの署名を含む、ファイルに関するメタ情報と、ある種の特定ファイル動作が実行され得るか否かおよび何の条件によるかを表示する状態情報とを含むメモリと、
第１のファイル内の当該コンテンツを抽出するために前記第１のファイルを受信するステップ、
第１の縮小ファイルを作成するために前記当該コンテンツを有効なフォーマット済みタイプの１つまたは複数のファイル内に再パッケージ化するステップと、
署名またはハッシュを前記第１の縮小ファイルに適用するステップと、および
前記署名または前記ハッシュを記憶して、前記署名または前記ハッシュを前記第１のファイルと関連付けるステップに応答するホストコンピュータと、
を含むコンピュータシステム。
【請求項１８５】
前記署名は前記ファイルコンテンツの１つまたは複数の暗号ハッシュを含む、請求項１８４に記載のシステム。
【請求項１８６】
複数のホストコンピュータと、前記複数のホストコンピュータに関連するサーバとが存在し、前記ホストコンピュータが記憶のために前記署名を前記サーバに提供する、請求項１８４に記載のシステム。
【請求項１８７】
前記メタ情報は、各ファイルに関して、ファイル名と、前記縮小コンテンツの署名と、ある種の特定ファイル動作が実行され得るか否かおよび何の条件によるかを表示する、承

認または禁止されるもしくは知られていない状態情報のうちの少なくとも１つとを含む、請求項１８４に記載のシステム。
【請求項１８８】
前記メタ情報は、実施および書込み動作を含めて、異なる動作に関して複数の承認または禁止状態を有する、請求項１８７に記載のシステム。
【請求項１８９】
前記サーバはデータ記憶装置内にメタ情報を記憶し、前記ホストコンピュータは前記データ記憶装置内に前記データのキャッシュを記憶し、前記サーバは更新を前記ホストコンピュータキャッシュに提供させる、請求項１８８に記載のシステム。
【請求項１９０】
前記サーバは、コンテンツハッシュと、ファイル名と、承認された状態および禁止された状態と、前記ファイルまたは前記ファイルの前記ハッシュが前記サーバによって初めて参照された日とを記憶する、請求項１８８に記載のシステム。
【請求項１９１】
前記サーバは、その中で前記状態に対する変更が許可または禁止されるためのさらなる分析をペンディングして動作が許可されるペンディング状態を記憶することができる、請求項１９０に記載のシステム。
【請求項１９２】
前記ホストコンピュータは、ファイルの前記コンテンツおよび／または前記名前を変更することができる動作を検出することによって前記第１のファイルを受信し、
前記ホストコンピュータは、局所メタ情報記憶装置上のファイル名またはファイル名の署名によってファイルのメタ情報を調査し、
前記ファイル名または前記署名が探索されない場合、コンテンツの前記ハッシュに基づいて前記サーバに問合せを提供し、
前記ファイル名または前記署名が探索された場合、ある種の特定ファイル動作が実行され得るか否かおよび何の条件によるかを決定するために前記メタ情報にアクセスする、請求項１８６に記載のシステム。
【請求項１９３】
前記署名は前記ファイルコンテンツの１つまたは複数の暗号ハッシュを含む、請求項１９２に記載のシステム。
【請求項１９４】
前記ホストは、メタ情報更新を取得するために周期的に前記サーバを検査する、請求項１９２に記載のシステム。
【請求項１９５】
前記ファイルは初めて参照された後の定義された期間、前記ファイルのさらなる分析を自動的に実行するステップをさらに含む、請求項１８６に記載のシステム。
【請求項１９６】
前記サーバ内に維持される前記メタ情報は、最近の状態変更の履歴と、変更の理由と、前記メタ情報が最後に変更された時間とをさらに含む、請求項１８９に記載のシステム。
【請求項１９７】
サーバのメタ情報に基づいて、ファイルがホストからサーバに自動的に転送される、請求項１９４に記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
大企業は、多額の情報技術（ＩＴ）セキュリティ予算と階層的なＩＴセキュリティシステムとを有しつつも、ネットワークはウィルスおよびワームからの損害の危険にさらされ、スパイウェア問題は普及している。現在のＩＴセキュリティ技術は、維持に費用がかかり、多くの新しいまたは知られていない脅威に対して保護を提供せず、一方、新たな脅威は増加速度で広がり、検出され、報告されている。

【０００２】
ファイアウォールなど、ネットワーク境界に配置されるセキュリティ解決法は、それらを直接通過するネットワークトラフィックに限られる可視性を有する。電子メール、ウェブブラウザ利用、無線アクセス、ＶＰＮ、インスタントメッセージ、およびファイル共有などの入力ベクタは、これらの技術を迂回する、ますます多孔性の境界を生み出している。十分な制御と可視性とを提供する現代のネットワークで境界を定義することは困難である。多くの攻撃は、機械またはネットワークを汚染した後で初めてネットワークトラフィックを生成する。例えば、ウィルスがネットワーク内の機械から電子メールを開始するまでに、その機械はすでに汚染されている。実施する前に攻撃を止めるためには、ネットワークトラフィックだけでなく、ファイルを保護することが全体的に必要である。

【０００３】
可視性と保護とは、ネットワーク内の複数の個々のコンピュータ「ホスト」上で動作する、ハードウェアと共に使用されることもあるソフトウェアであるホストエージェントによって提供されることが可能である。ホストエージェントは、背景でセキュリティ機能を実行するためにホストの資源のいくつかを使用して、同時に全体的に動作する。ホストの重要な内部機能すべてに対するアクセスを潜在的に有することによって、ホストエージェントは、理論上、何らかの損害が与えられる前にホスト上の脅威を検出および停止することができる。ホスト・エージェント・セキュリティ・システムは、ネットワークの「終端」で動作するため、エンドポイント・セキュリティ・システムと呼ばれる。

【０００４】
現在の企業のエンドポイント・セキュリティ・システムは、多くの場合、アンチウィルス（ＡＶ）走査およびアンチスパイウェア（ＡＳ）走査など、知られているビットパターンを用いて攻撃を検出およびブロック（ｂｌｏｃｋ）する。パターン走査は、不良として予め識別されるパターンのブラックリストを使用する。同様に、いくつかのセキュリティシステムは、不良行動様式パターンのブラックリストと説明されることができる、検出された、知られている行動様式プロフィールを使用する。いずれの場合も、ブラックリストは永久に古いものであり、新しいまたは知られていない攻撃に応答することができない。ブラックリストはまた、ブラックリスト更新を誘出、試験、および配信するための能力よりも速く広がることが可能な新しいウィルスなどの攻撃に対して効果がない。毎週、数十もの新しいウィルスが探索されるため、すべての種類のブラックリストは、ますます効果のないものになっている。開発および試験を行うには行動様式パターンは複雑であり、結果として、高い誤報率を有する。すなわち、行動様式パターンは、実際に、動作に害がない場合に行動様式は不良であるという結論を誤って下す。新しい攻撃が展開すると、行動様式は変化し、その代わりに、的外れの検出の誤りにつながる。ウィルスのように、攻撃まで待つことによって、不良行動様式を示し、影響を受けた機械はすでに汚染されている可能性がある。要約すれば、不正であるものは絶えず変わるのに、ブラックリストは不正であるとすでに知られているものを追跡しようと試みる。

【０００５】
もう１つの企業のエンドポイント技術は、異常検出である。これは、経時的に行動様式を観察することによって統計的に決定される行動様式ブラックリストとみなされ得る。行動様式ブラックリストの欠点を受け継ぐことに加えて、異常検出は、良い行動様式と不良行動様式の両方が統計的に評価されるときに新たな誤りモードを加え、したがって、評価誤りが必ず存在する。このプロセスは、多くの場合、受け入れ不可能なほど高い誤報と、損なわれた検出をもたらす。

【０００６】
エンドポイント・セキュリティ・システムのもう１つのクラスは、知られている良いプログラムのパターンのリストであるホワイトリスト上にあるプログラムだけに実施を限定する。プログラムがそのリスト内に含まれていない場合、プログラムは実行しないことになる。かかるシステムは、典型的な現代の企業にとって十分に柔軟ではなく、結果として、ホワイトリストは維持が困難である。例えば、ほとんどの大企業は、社内で開発され、

頻繁に変更できるカスタムプログラムを配備する。さらに、これらのプログラムは、第三者に公開されるべきでない、慎重を期する知的財産とセキュリティリスクとを含む可能性がある。ホワイトリストのサプライヤが時宜を得た方法でこのソフトウェアを事前承認するためのアクセスを有することはあり得ない。その他の例は、オペレーティングシステムおよびその他の更新である。この場合も、いくつかのプログラムまたは更新がすべてに企業にとって望ましいものであることを証明するための中央クリアリングハウスまたは中央権限は存在しない。ホワイトリストシステムの故障モードは深刻であり、重要であるが、まだ承認されていないアプリケーションおよびビジネス機能へのアクセスをブロックする。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

結果として、ファイル・コンテンツ・アクセスを１つまたは２つの状態、すなわち、承認と禁止とに中央分類するシステムは、競争（タイミング）条件を含む課題を有することになる。大量のソフトウェアは、いずれの部類にも明瞭に当てはまらず、企業内のすべてのソフトウェアに関して広く一般に信頼されることになる中央権限は存在しない。これが要因でないとしても、中間ソフトウェアを分類するには時間がかかる。新しいウィルスの場合、新しいウィルスを不良として分類するためには６～４８時間かかる場合があり、その時までに発生は全域にわたる可能性がある。したがって、ホストから中央承認権限に強力なネットワーク接続性を用いても、新しいソフトウェアを検出および分析するためには数分を超える時間がかかる。このコンテンツベースの許可を背景内のオペレーティングシステムに透過的に加えるためには、遅延は、一般に、１分未満でなければならず、さもないとファイルシステムは時間切れになり、誤ったアクセスブロックエラーが発生する可能性がある。

【課題を解決するための手段】

【０００８】

本明細書で説明されるセキュリティシステムは、管理者がコンピュータの大規模なネットワーク上にインストールされたファイルを検出、管理、所在確認、識別、および管理することを可能にする。システムは、知られているおよび知られていないウィルス、ワーム、スパイウェア、ハッカ、非承認／非所望ソフトウェア（例えば、事業使用ポリシーに反するソフトウェアアプリケーション）およびソーシャルエンジニアリング攻撃からの防御を提供することができる。管理者は、新実行可能、スクリプト、および埋込みスクリプトがネットワーク化されたシステムに出現および伝播すると、それらに関する詳細な情報および統計にアクセスすることができる。システムは、管理者がファイル動作を承認、ブロック、隔離、または記録することを可能にする集中ポリシーを実施できる。システムはまた、問題のファイルまたは攻撃を診断および所在確認するために有用な詳細な情報を収集することも可能である。システムは、大規模なコンピュータ設定のための可視性、制御、および保護を提供する。

【０００９】

システムアーキテクチャは、保護された各ホスト上で実行するエージェントソフトウェアと、集中ポリシー管理を提供する、「サーバ」と呼ばれるサーバと、イベント監視と、エージェント調整と、ウィルス走査とを含むことが好ましい。サーバは、（より限定された機能性デバイスを全体的に示唆する）装置として実施されてもよい。単一の装置は、多くのホスト（例えば、１０，０００個のホスト）をサポートすることが可能である。「スーパサーバ」と呼ばれることもある、さらなるサーバまたは装置は、複数の装置を監視することができる。

【００１０】

保護された各ホストコンピュータ上で実行するエージェントソフトウェアは、ファイルシステム動作を分析して、サーバに関して構成されたポリシーに基づいて処置を取る。一実施形態では、ホストがファイルを開くことまたはファイルに書き込むことを試みる場合

、ファイルのコンテンツのハッシュを計算して、システムに対してファイルを独自に識別する。エージェントソフトウェアは、このハッシュを使用して、そのファイルに関して状態とポリシーとを調べる。この情報に基づいて、エージェントソフトウェアは、動作をブロックし、イベントを記録し、ファイルを隔離し、または（１つもしくは複数の）その他の指定された処置を取ることが可能である。

【００１１】

システムはまた、アーカイブからファイルを抽出する能力、ファイルからマクロを抽出する能力、集中的なコンテンツ追跡および分析、ならびに本明細書で説明される「ファイル調査」機能を含めて、組合せでまたは個々に有用な多くのその他の特徴も含む。

【００１２】

本明細書で説明されるシステムは、少なくとも２つの追加の状態を使用することができる。すなわち、定義の程度が低い中間の脅威水準を表すペンディングと、１つのホストに関して承認されるが、中央権限（したがって、すべてのその他のホスト）に関して承認されるとは限らない局所承認とである。後者は、ホストが基本線から若干それることを可能にする。ペンディング状態は、ホストが様々な脅威水準と企業の利用ポリシーとに基づいて新コンテンツへのアクセスをブロックまたは許可することを可能にする。一般的なバイナリ承認専門用語、すなわち承認と禁止とを使用するが、３～４つの状態に承認を分割することは、結果として、各個々の状態に関して改善された、異なる能力をもたらす。一般に、新しく、まだ分類されていないソフトウェアは、ペンディングである。ソフトウェア用の伝統的なバイナリアクセス状態（禁止／承認）は十分に柔軟ではなく、かかる分類システムは拡張可能ではない。

【００１３】

新／ペンディングとしてのソフトウェアの指定は有用である。ほとんどの企業は、「従業員は承認されていないソフトウェアをインターネットからダウンロードおよび実行することを許可されない」など、何らかの形で「新実行可能拒否」ポリシーを有する。それでもなお、企業は、新しいソフトウェアが伝播しているときに、手遅れになるまで、そのソフトウェアを検出することができず、企業のポリシーがいつ侵害されたのかを知らず、企業のポリシーを効果的に強化する手段を持たない。電子メール、インスタントメッセージ、ダウンロード、ＵＳＢ鍵、移動ラップトップなどにかかわらず、新コンテンツはほとんどいかなる手段からもネットワークに入り込むため、新プログラムが変更され／ファイルシステムに書き込まれている間に、ペンディングとしてその新プログラムを追跡することによって、ホストエージェントは、リアルタイムで新コンテンツを検出および報告することができる。ペンディングとしてプログラムを識別することによって、「許可するが、ホストが新実行可能を実行する場合、警告する」または「非承認プログラムはホストのこのグループによってインストールまたは実行されることができない」または「２４時間以内にＮ個を超えるホスト上に同じ新しい非承認プログラムが出現した場合、警告する」など、いくつかの拡張可能な簡単かつ効果的なポリシーが可能である。それにより、新プログラムは、ブロックされている間に、安全に所在確認、追跡、および分析され得る。その他の承認されたビジネス用ソフトウェアは、引き続き実行することになる。ＡＶ更新またはセキュリティパッチなど、承認された新しいソフトウェアは、インストールおよび実行されることが可能である。この手法は先行型の対応であり、生産性を可能にする間に、知られていない、場合によっては、悪意のあるソフトウェアを防ぎ、時間が重視される任意のブラックリスト更新またはホワイトリスト更新を要求せずに、分析時間を得る。

【００１４】

中央で多くの個々のリスト（各ホストに関して１つ）を維持することは困難であるため、既存のファイル・ホワイトリスト・システムおよびファイル・ブラックリスト・システムは、本質的に世界的な傾向がある。本明細書で説明されるように、ホストは、中心リストと異なる可能性がある独自のリストを維持することができる。特に、これは局所承認状態およびペンディング状態の場合である可能性があり、名前禁止および名前承認など、名前ベースの状態の場合に当てはまることが多い。「名前」は一般に局所プロパティである

ため、これらの状態は中央管理された状態と異なる可能性がある。例えば、ファイル「ｆｏｏ」がホスト上にあるハッシュ＝ｘと中央サーバペンディング状態とを有する場合、ファイルは局所承認または名前禁止もしくは名前承認である可能性があり、後者の２つはホスト上のファイルの局所名に応じる。本明細書で説明されるシステムは、すべてのホスト上のすべてのファイルに同時に応用される数千もの名前プロパティの効率的な管理とポリシー実施とを可能にする。名前承認は、ホスト上のどこにファイルが作成されているかに基づいて、柔軟な局所承認能力と中央承認能力とを可能にする。ホストグループと共に、これは、どのホストのどこに新コンテンツが承認されるかの正確かつ柔軟な効果的仕様を可能にする。

【００１５】

この新しい柔軟なポリシーシステムを用いてさえ、企業は、通常、異なる任務および状況に関して異なるポリシーを実行する必要がある。例えば、ＩＴアドミニストレータおよび社内のソフトウェア開発者は、新しいソフトウェアを慎重に実行する必要がある可能性があるものの、その他の従業員は比較的静的なアプリケーションの小さな基準一式だけを必要とする。攻撃を受けると、この状況は速やかに変化する可能性がある。例えば、ウィルスがＮ個を超えるホスト上で検出される場合、「新実行可能拒否」ポリシーの範囲を拡張することは道理に適う場合がある。企業内の変化するポリシーに、そして異なる状況に対して適合できない固定システムと比較して、この柔軟性および増分対応は、本明細書で説明される「パラメータコンテンツ制御」システムの利点である。「パラメータコンテンツ制御」は、中央管理されて、ネットワーク条件とホスト条件とに基づいて速やかに変わることが可能である柔軟な封鎖モードを可能にする。これは増分ファイルコンテンツおよび／またはファイル名ベースの規制と承認とを可能にする。

【００１６】

ホストユーザ資格証明、プロセス識別子、データソース（ＵＲＬ）、ディレクトリ構造、およびオペレーティングシステムのセキュリティ記述子を処理するその他のエンドポイントセキュリティ技術と異なり、本明細書で説明されるシステムは、ホストポリシーの一部としてこれらの要因を利用する必要がない。ホスト上で、これらの要因は、信頼できず、汚染に無防備である可能性があり、拡張性を妨げる可能性がある。きめ細かなポリシーは、複雑な方法で様々なホストの全域で相互に作用できるため、これらの要因は、結果として、拡張可能性がより少ないポリシーをもたらす。オペレーティングシステムが汚染され、攻撃が管理上の特権とすべての関連するセキュリティ記述子を得たとしても、本明細書で説明される「新実行可能拒否」ポリシーは、実質的な保護を提供することになる。

【００１７】

「コンテンツ追跡」システムは、新コンテンツがネットワークを進むにつれて、新コンテンツを監視および分析するために、ペンディングなどの追加の状態を利用する。現在の技術は、多数のホストの全域で、すべての新しい実施可能ファイルのリアルタイムでの世界的な中央可視性と追跡とを可能にしない。ＡＶスキャナなど、ファイルシステム走査に依存するエンドポイントシステム、およびＴｒｉｐｗｉｒｅなどのホストアプリケーション在庫管理は、新ソフトウェアまたは変更されたソフトウェアを探して多数のファイルシステムの中を周期的にゆっくりと這って進む。これは、一般に、ホストに悪影響を及ぼし、時間がかかる場合があり、通常、多くても１日に１度予定される。何が新しいかに重点を置き、その情報をメモリ内に記憶することによって、コンテンツ追跡システムはより拡張可能かつ反応性である。大きなグループＮ内の任意のホストによって決定されたことがない新ソフトウェアが到着することは稀であり、多くのホストＭが短期間にその新ソフトウェアを出現させることは稀であるため、報告、応答、および分析はこの区別によって容易にされる。

【００１８】

新ソフトウェアが検出されると、時宜を得た方法でそのソフトウェアを所在確認および識別することは有用である可能性がある。いくつかの新ソフトウェアが新たな攻撃であり、かつ広がっていることが判明した場合、極めて素早く対応することが所望される。この

場合も、現在の技術は、数分から数時間のうちに、ネットワーク上の単一のホスト上の単一の新ファイルを所在確認することができる。単一のホスト上であっても、名前またはコンテンツによって非常に新しいファイルを探索することは１５～１６分かかる場合があり、問合せが処理されている間にホストのディスク性能に悪影響を与えることになる。過去２０年にわたって、ハードディスクは、さらに大量のバイト記憶容量を得ているが、速度は比例して増加していない。「分散型メタ情報問合せ」特徴は、ホストディスクに影響をほとんどまたはまったく与えずに、中央指定された問合せと、中央報告された結果とにより、多数（数千）のホストの全域で、キーファイル属性の所在確認および識別を数秒で加速する。変更されていないものを含めて、すべてのファイルを追跡する伝統的な追跡技術と異なり、本明細書の本発明はファイルが変更するとメモリ内のファイル変更を追跡し、これはメモリからのファイルのメタ情報に関してホストに問い合わせるための効果的な手段を提供する。この情報を中央処理することは、ホストファイルシステムの収集物全体にわたって個々のファイルの動きの反応性の世界的な視野を初めて提供する。最終的に、セキュリティサービスとして、ホストが中央サーバに接続し、書込み、中央サーバから問い合わせることが重要である。これはホストが１つもしくは複数のファイアウォールまたはＮＡＴデバイスによってサーバから分離されることを可能にし、受入れ／聴取モードで追加のホスト・ネットワーク・ソケットを確保する困難な問題を回避するという点で、これは本発明の重要部分である。

【００１９】

コンテンツ分析を使用する現在のエンドポイント・ホスト・エージェント・システムは、ホストエージェントの更新を伴う課題を有する。例えば、ＡＶスキャナが最も効果的になるためには、利用可能にされている数時間または数分の更新範囲内に更新されなければならない。遅れるＡＶを有する任意のホストは危険な状態にあり、多くのＡＶシステムは、不適切に構成されており、結果として、更新遅延をもたらす。ＡＶスキャナは、効率的にファイル変更を追跡しないため、ＡＶスキャナは、一般に、ファイルシステムに書き込まれた新コンテンツに対応するのに比較的長い時間をかける。また、現在のホストコンテンツ分析技術は、セキュリティ要因を考慮に入れずに、ファイルを不必要に再分析する。例えば、新コンテンツ、すなわち、より新しいコンテンツをより頻繁に分析することが重要である。ファイルがネットワーク内で２年間まったく変更されていない場合、１０分ごとに走査されなくてよい場合がある。しかし、新ファイルが１０分間に始まってネットワーク全体にわたって広がる場合、初めの２日間、新ファイルを頻繁に走査することは道理に適う可能性がある。一般に、時間が進むと、新しい悪意のある実施可能なファイルに関する新しい情報は次第に少なくなる。「時間設定された集中分析」特徴は、これらの課題に対処する。１つの分析エージェント（中心のもの）だけ更新される必要があり、すべてのホストは速やかに利益を得る。ホスト構成がコンテンツ分析更新を妨げることができる可能性はより少ない。新ファイルだけを追跡して、ネットワークに発表された年齢（時間）に基づいて分析を予定することによって、新しい不良コンテンツは効率的かつより速やかに所在確認および識別され得る。最終的に、ＡＶなど、多くのエンドポイントコンテンツ分析技術は、オペレーティングシステムと密に統合される。結果として、異なるサプライヤからのいくつかのコンテンツ点検エージェントをホスト上に配置することは困難な可能性がある。分析技術の多様性は、検出および分類の正確さを改善する。この場合も、本発明は、必要に応じて、分析を異なるサーバに発送するために中央サーバを使用することによってこの問題を解決する。

【００２０】

実施可能なコンテンツ（ｅｘｅファイル）および埋込みマクロ（Ｍｉｃｒｏｓｏｆｔ Ｏｆｆｉｃｅ文書内に埋め込まれたマクロ）は、クラスタまたはグループにおいて伝播する傾向がある。ワードプロセッシング文書は、１０個のマクロを含み、サイズが３０ＭＢを超える場合があるが、マクロはその領域の一部だけを占有する。大型のインストールパッケージは、サイズが数百ＭＢである場合があるが、その内部アーカイブの実施可能な部分は、一般に、総サイズの小さな部分を占有する。ウィルスは、多くの場合、検出を回避

するために、ジップファイルなど、アーカイブ添付ファイルとして電子メールを介して移動する。これらのアーカイブの内部では、ウィルスペイロードは小さい可能性がある。これらの事例すべてに関して、より大きな「コンテナ」ファイルは、場合によっては所望されない新しい符号の伝播を隠すことができる。「コンテンツエキストラクタ」特徴は、（入れ子型の）コンテナ関係を保存することによって、様々な現在の制限に対処し、同時に、コンテンツを追跡し、類似コンテナを追跡し、製品関連付けを追跡し、不要な再分析を最小限に抑え、ファイル転送帯域幅を最小限に抑え、コンテンツをその他の知られているファイルタイプと再パッケージ化することによって、その他の分析技術との互換性を維持することを円滑にする。新コンテンツの中央記憶および中央追跡、ならびにコンテンツの初めての出現時間に関連する分析の中央スケジューリングは、セキュリティ、世界的な可視性、企業管理システム統合、および将来の拡張の観点から、強力な利点を提供する。

【００２１】

本明細書で説明されるシステムは、その他のシステムと区別されているが、かかる区別はそれらのシステムに対する特許請求の範囲対象を放棄することを意味しない。本明細書で説明されるシステムおよび特徴は、グループでまたは個々に提供されることが可能であり、多くの場合、上で識別されたものを含めて、先行システムおよび知られているシステム内に統合されることが可能である。

【００２２】

その他の特徴および利点は、添付の図面、詳細な説明、および特許請求の範囲から明らかになるであろう。

【発明を実施するための最良の形態】

【００２３】

図１を参照すると、デジタル抗体（アンチボディ）システム（ＤＡＳ）１０とも呼ばれるシステムは、管理者がコンピュータの大型ネットワーク上にインストールされたファイルを監視、理解、および制御することを可能にし、知られているおよび知られていないウィルス、ワーム、スパイウェア、ハッカ、およびソーシャルエンジニアリング攻撃、ならびに非承認ソフトウェア（例えば、ビジネス用途でないファイル共有ソフトウェア）からの防御を可能にする。システムは、そのうちの１つが、本明細書でサーバ１４（装置）として示される、１つまたは複数のサーバを含む。このサーバは、集中ポリシー管理と、イベント監視と、エージェント調整と、コンテンツ分析（例えば、スパイウェアおよびウィルスの走査）とを提供する。単一のサーバは、多くのホスト１２（例えば、数百または数千のホスト）をサポートすることができる。サーバはまた、ファイルとプログラムとに関して、走査履歴および承認状態など、分析に関連するメタデータのデータベースを維持する。このメタデータは、ファイルおよびプログラムの各々のための「抗体」と呼ばれる。

【００２４】

保護された各ホスト１２は、ソフトウェアとして実施されることが好ましいホストエージェント１６を有する。ホストエージェント１６は、ファイルシステム動作を分析して、サーバ上に構成されたポリシーに基づいて処置を取る。以下により詳細に説明されるこれらのポリシーは、ファイルアクセスおよび実行可能の実施などの動作をブロック、記録、許可、または隔離するか否かを識別する。各ホストエージェント１６は、ファイルに関連するメタ情報のキャッシュである局所「抗体」記憶装置１６と、サーバ１４からポリシーを実施するためのパラメータ・ポリシー・エンジン２０とを有する。

【００２５】

サーバ１４は、いくつかの機能とインターフェースとを有する。インターフェースは、ホストと通信するためのホスト通信インターフェース２２と、ウェブブラウザ管理コンソール２６と通信するためのウェブベースのグラフィカル・ユーザ・インターフェース（ＧＵＩ）と、企業管理システム２８に対するインターフェースとしての機能を果たす報告インターフェース２６と、コンテンツ分析サービス３２（例えば、ウィルススキャナおよびスパイウェアスキャナ）と通信するための遠隔分析インターフェース３０とを含む。サーバ１４は、分析ブロック３４および抗体分析サービス３８と通信して、関連するホストに

関して抗体のマスタリストを記憶するマスタ抗体記憶装置３６も有する。サービス３８は、抗体に関連する追加の情報（例えば、Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅなどのある製品パッケージのメンバーとしての抗体の分類）を有するオフサイト証明権限を含んでよい。

【００２６】

図２は、システムおよび、サーバ１４と、ユーザ位置とカーネル位置とを含むホスト１２と、その他のネットワークおよびウェブサーバ４０とを含むその構成要素の拡張図を示す。本明細書で示されるように、サーバは、ネットワーク上に出現した最近のファイルの複写を含む新ファイル処理およびファイル・プール・ブロック４２と、分析されることになるファイルおよびハッシュを識別するためのスケジュールされた分析エンジン４６と、ＭＤ５およびＳＨＡ－１などのアルゴリズムを使用してコンテンツの暗号ハッシュを作成するためのコンテンツ署名者４６と、マスタ抗体記憶装置３６と、構成管理５０と、追跡記録および報告５２とを含む。サーバは、ネットワークおよび、分析５４と、ＡＶ（またはその他のコンテンツ）スキャナ５６と、管理サービス５７とを含むウェブサービス４０と相互に作用する。

【００２７】

ホスト１２のユーザ部分６０は、名前とデータの両方によってデータベース３４からの更新を保持するための抗体キャッシュ６４と、ファイルおよびイベント処理６６と、分析エンジン６８と、パッケージ内の当該コンテンツと個々のコンテンツの関連するグループとを抽出するためのコンテンツエキストラクタ７０と、コンテンツの暗号ハッシュを作成するためのコンテンツ署名者７２と、抗体に関して抗体キャッシュ６４を検査して、抗体に関してサーバを検査するためのサーバのメタ情報（ＭＩ）状態リゾルバ７４と、サーバへのコンテンツのアップロードの進展を検査して、アップロードの証明書に関してサーバを検査するためのファイル状態リゾルバ７６とを有する。

【００２８】

ホスト１２のカーネル部分８０は、ファイル名によって編成された抗体を保存するためのキャッシュ８２と、最近のファイル動作およびファイル情報のキャッシュ８４とを有する。カーネルはまたは、ファイル動作要求を受信および傍受して、これらの要求を、初めに最近のファイル動作のキャッシュ８４を検査するステートフル（ｓｔａｔｅｆｕｌ）フィルタ８８に提供する傍受／ブロック機能８６も有する。一致が存在しない場合、カーネルは、セキュリティポリシーを維持するトリガおよび動作ブロック９０を検査する。このブロック９０は、システム用のセキュリティ水準を表示する値を有する「デフコン」ブロック９２と、実施、ファイル読取り、ファイル書込み、およびその他の動作を含めて、様々なファイル動作を制御するためにブロック８２、９０、および９２を支配するポリシーエンジン９４とに結合される。トリガおよび動作ブロック９０は、その名前に基づいてファイルに関するメタ情報を探す抗体キャッシュ８２と通信する。ポリシーエンジン９４はまた、ブロック、報告、またはファイル動作の許可、およびユーザへの報告などの動作を制御する。

【００２９】

システムは、このセキュリティシステムを使用するための多数の方法と態様とを含み、その多くは、単独でまたはその他のシステムと組み合わせて使用されることが可能である。これらの方法および態様は、以下により詳細に説明される。

【００３０】

一態様は、文書または実行可能を検査して、そのデータが予め検査されているかどうかを表示するハッシュを維持するための集中的走査の使用である。ハッシュ値は、データベース内に記憶され、やはり局所ホスト内にキャッシュされることも可能である。

【００３１】

もう１つの態様は、ホストのポリシーを制御する、「Ｄ」または「デフコン」と示される、中央設定されたパラメータの使用にある。この集中的なポリシーとパラメータとは、すべてのホストに、またはホストの選択されたグループに適用されることが可能である。

パラメータは、オペレータによって手動で設定されてよく、または、一般に、何らかのイベントに応答して、人間の介入なしにシステムによって調整されてもよい。ポリシーは、ある種の動作をブロックまたは許可することを含んでよく、または、動作を追跡記録などのさらなる監視を条件に許可するペンディングにすることも可能である。ペンディング状態は、システム内の待ち時間を考慮に入れること、ならびに伝統的なバイナリ承認／禁止モデルに適合しないポリシーを実施することを含めて、複数の利点を有する。これらの待ち時間は、有害な符号が識別される前の時間、システム内の機能不全の間、またはホストがネットワークから切り離されている時間を含む。

【００３２】

さらにもう１つの態様では、中央サーバはメタ情報の問合せを特定して、その問合せをホストのすべてグループまたは選択されたグループに配信することができる。これらのホストは、メタ情報の局所記憶装置から問合せを実行し、サーバにパラメータを調整させることができる結果をサーバに戻す。

【００３３】

さらにもう１つの態様では、システムは、その他の文書内に埋め込まれることが可能なマクロウィルスの拡散を防ぐための方法を含む。この機能性は、ビジュアルベーシックマクロを用いて使用され得るが、この方法は、ビジュアルベーシック以外のその他のマクロ言語に適用することが可能である。

【００３４】

もう１つの態様では、新ファイルのすべての複写は、サーバ４２内の特別なディレクトリ内に維持される。さらなる分析はタイマに基づいて実行されてよく、ファイルが初めて参照されてから何日も経過した後で実行されてもよい。３０日など、ファイルの初めての出現からある期間の後、ファイルは、ウィルス、スパイウェア、またはその他の問題に関して再度走査されることが可能であり、システムはその結果に応じて処置を講じることができる。例えば、ウィルスがファイル内に含まれていることを示す分析は、次いで、禁止状態を含むためにこのファイルに対して対応する抗体・データベース３６の入力を引き起こす。その他の抗体・データベース変更と共に、この変更は、ホストに伝播されることになる。

【００３５】

中央設定されたパラメータおよびパラメータ・コンテンツ・ポリシー

システム内のセキュリティは、各サーバ内で定義されるポリシーに基づき、プッシュおよび／またはプル技術を介して関連するホストまたはホストのグループに伝播される。これらのポリシーは、読取り、実施、および書込みなど、実行可能およびファイルにより行われることができるもの、それらがホストによって作成また変更された場合に何をするか、走査がどのように実行されるか、追跡記録がどのように行われるか、および多くのその他の機能に関連し、各ポリシー（例えば、新たに決定された実行可能により何の動作が行われ得るか）に関して、（禁止、許可、または許可および記録など）いくつかのポリシーオプションが存在してよい。ポリシーは、ファイル内のコンテンツ（データ）もしくはファイルの名前、またはそれらの組合せに基づいてよい。コンテンツは、１つまたは複数の暗号ハッシュなど、署名によって定義されてよい。サンプルポリシーの非排他的リストは以下を含む。

【００３６】

１．新実行可能および切離しスクリプト（例えば、＊．ｅｘｅまたは＊．ｂａｔ）の実施をブロック／記録する
２．新しい埋込みコンテンツ（例えば、＊．ｄｏｃ内のマクロ）の読取り／実施をブロック／記録する
３．ウェブコンテンツ（＊．ｈｔｍｌまたは＊．ｃｇｉファイル内のコンテンツの変更）のインストール／修正をブロック／記録する
４．上の（３）などのポリシーに関して更新を許可する
５．２つのウィルス走査を通過したファイルを自動承認する（例えば、対応するファ

イル状態を承認に設定する）
６．管理者によって具体的に禁止されたファイルのインストール／実施をブロック／記録する
７．感染したファイルをデータで隔離／削除／記録する
８．感染したファイルを名前で隔離／記録する
９．管理上「クラス」と定義された新ファイルの実施をブロック／記録する（例えば管理者はスクリーンセーバ（＊．ｓｃｒ）をブロックすることを望むが、実行可能（＊．ｅｘｅ、＊．ｄｌｌ、＊．ｓｙｓなど）のクラス全体をブロックすることは望まない場合がある）
１０．特定されたファイルが取り外し可能媒体に結合された場合、記録する
１１．一定のディレクトリを除いて、新の実行可能、スクリプト、および埋込みコンテンツの実施をブロック／記録する（すなわち、ユーザが特別なディレクトリ内で新のスクリプトまたは実行可能を作成することを可能にするが、その他のファイルシステムは保護する）
１２．オフライン、遠隔で接続されるまたは局所的に接続される場合、ホストに関して異なるポリシー
１３．特定のファイルを含むホスト／経路を日付でまたは名前で列挙する
１４．ブロックされた実行可能、スクリプト、および埋込みスクリプトを有するホストを列挙する
１５．感染したまたは禁止されたファイルを有するホスト／経路を列挙する
１６．定義された更新サービスからのファイルを自動承認する（例えば、信頼されたソースからである場合）
１７．特定のホストグループに関して管理者によって具体的に禁止されたファイルの実行をブロック／記録する（すなわち、１つ以上のグループが存在する）
１８．性能の理由および試験のためにホストシステムを完全に非動作化する
１９．ある期間後にファイルを自動承認する（ユーザ構成可能）
２０．新ファイルが最高でｘ回までインストール／実施されることを可能にする（ユーザ構成）。承認されるまで、それ以上のインストールおよび／または実施はロックする。
２１．書き込まれるとき新ファイルを局所承認する
２２．書き込まれるとき新ファイルを中央承認する

【００３７】

サーバは、各ホストグループに関して１つまたは複数のポリシーを維持することができ、各ポリシーは中央設定され、ポリシー用に関してオプションを表示するパラメータに従って可変的に実施される。これらのポリシーとオプションとは、パラメータが、事実上、１つの次元に沿って移動して様々なポリシーに関してオプションを選択する２次元アレイとして論理的に編成されることが可能である。このパラメータは、本明細書でＤ値と呼ばれる。すべてのホストは、Ｄに関して１つの値を有してよく、またはホストの論理サブグループは独自のＤ値を有する。例えば、営業部のホストにはＤ＝１が割り当てられてよく、マーケティング部のホストには同時にＤ＝２が割り当てられてよい。一実施形態では、ホストはサーバを検査（調査）して、Ｄの値が変更されたかどうかを決定する。各ホストは、Ｄが変更されたことを探索すると、各々、新しいＤ値に「移動」し始める。この移動は段階的に行われてよい。これらの調査は、ホストからサーバへのネットワークメッセージとして提供され得る。Ｄ値はポリシー動作を制御する。所与のポリシー（例えば、「新実行可能拒否」または「新スクリプト拒否」）に関して、Ｄ＝２は動作を侵害するポリシー（この場合、「新実行可能」の実施）をブロックする。Ｄ＝４は警告（サーバに対するサイレント警告）するが許可し、Ｄ＝６は許可して警告はまったくしない。Ｄ＝２、４、または６であるかにかかわらず、ホストは、新実行可能が書き込まれると、新実行可能を引き続き通知および記録することが好ましい。本明細書での例は、Ｄに関して数値を使用するが、Ｄは文字、言葉、または文字と数字の任意の組合せで表現される「値」を有して

よい。

【００３８】

Ｄ値はまたポリシー動作化を制御する。所与のポリシー（例えば、「新実行可能拒否」または「新スクリプト拒否」）に関して、Ｄ＝１は「書込み保護」ポリシーを可能にし、したがって、新実行可能はまったく書き込まれることができず、一方、Ｄ＝８はすべてのポリシーを完全に動作不能にし、Ｄ＝２、４、および６の事例は上で提示されたようであり得る。この場合、Ｄ＝８は、新実行可能がファイルシステムに書き込まれる場合、通知のポリシーさえ動作不能にすることができる。

【００３９】

Ｄの値はサーバ内で中央設定されることが可能であるが、ホスト上では局所的に実施される。この値は、サーバに接続されたブラウザを使用することによって、または簡易ネットワーク管理プロトコル（ＳＮＭＰ）を経由して、管理コンソール上のグラフィカル・ユーザ・インターフェース（ＧＵＩ）を介して管理者によって設定されてよい。Ｄ値は「目標」値とみなされる。ホストは可能な限りこの値に近づくことを試み、これは数秒または数分かかる可能性がある。場合によっては、ホストは、サーバによって特定された目標値から局所的にそれることが可能である。コマンド・ライン・プログラムがホスト上で呼び出されることが可能であり、またはユーザは一定のＤ値について促されることが可能であり、Ｄの目標値は取り消されることが可能である。この特徴は、例えば、個人の機械をセキュリティ動作不能（Ｄ＝８）にする必要があり、サーバとのネットワーク接続性が存在しない場合に有用である。許可されたプログラムからの更新（例えば、アンチウィルス更新）の検出など、ある種の動作はホスト上のＤの値を自動的に変更する可能性がある。

【００４０】

ポリシーは、セキュリティと使いやすさの間のトレードオフを反映する。上の例では、Ｄ＝８は、最大限に有用であり、最小限に安全である。すなわち、何のポリシーも動作化されず、ホストエージェントはブロックおよび追跡から効果的に動作不能にされる。Ｄが最大セキュリティ（Ｄ＝１）に近づくと、ますます多くの規制ポリシーが動作化され、ポリシーが侵害された場合に実行される動作は、ますます厳しいものになる。順序付けされた状態は可視化および試験が容易であるという点で、所望される（一般に、Ｄ＝１およびＤ＝８など、試験される必要のある終端だけを試験することができる）。順序付けされた状態により、ファイルおよびユーザの数は、値が増加または減少するにつれて、連続的によりアクセス可能またはより制限的になる。これらの順序付けされた状態は、当然、セキュリティと使いやすさの間のトレードオフを反映する。

【００４１】

Ｄがライブシステム上で変更されると、競争状態が発生する可能性がある。基本的な問題は、プログラムをインストールする間にＤの値が８から１に変更されたとした場合、複数のファイルのインストールは「半分ブロック」または「半分インストール」になる可能性があることである。結果として、一定のＤ遷移は、ファイルの抗体状態の再分析と、ファイルの抗体バルク状態変換をトリガする可能性がある。

【００４２】

局所的なＤ変更は、時々、局所的なポリシートリガによって引き起こされる場合がある。通常、Ｄは、サーバ上で中央設定される。しかし時々、局所ホストポリシーがトリガされ、このポリシーは、次いで、局所ホストＤ値を変える。これは、例えば、ロックされたシステム（Ｄ＝２）上でインストールを完了するために有用である。この例を続けると、Ｄ＝２でプリンタドライバをインストールすることは、パックが解かれた新インストールファイルのいくつかはインストールを完了するために実施される必要があるため、通常なら問題をまねく可能性がある。さらに、異なるホスト機械は、インストールを完了するために異なるプログラムのパックを解いて、実施する必要がある場合がある（例えば、Ｗｉｎｄｏｗｓ（登録商標）２０００およびＷｉｎｄｏｗｓ（登録商標）ＸＰ）。この場合、ある種の抗体ファイルタイプ（承認されたプログラム「ｐｒｉｎｔｅｒ＿ｓｅｔｕｐ．ｅｘｅ」）の実施は、そのホストの局所Ｄを２から、それらの新しいインストールファイ

ルとその子孫だけを自動的かつ局所的に承認するわずかに弱い３に移動させる。

【００４３】

Ｄ値は、（配線式ＬＡＮ上の）局所であるか、電話モデムもしくは仮想私設ネットワーク（ＶＰＮ）を介してなど遠隔であるか、または完全に切断されているか、接続性のタイプに応じて変更されてよい。ホストエージェントは、したがって、これらのタイプの接続性に関して特定されたＤ値のセットを記憶し、次いで、例えば、ユーザがＬＡＮからホストを切断した場合、変更に応答して、そのセットから自動的に選択することになる。また、異なるＤ値は、結果として、詳細の報告、追跡記録、および追跡に際して減少または増加をもたらすことが可能である。

【００４４】

ポリシーはまた、多くのサーバを制御できる、「スーパサーバ」と呼ばれることがある中央サーバから設定されてもよい。各サーバが２，０００個のホストを制御し、１，０００個のスーパサーバが存在すると想定すると、Ｄ＝１を設定するためのスーパサーバコマンドが２，０００，０００個のホストすべてに適切になることはありそうもない。代わりに、スーパサーバは、局所的に許可される限り強いＤを有するようにすべてのサーバとホストとに命令することができる。したがって、いくつかのサーバと、それらの接続されたホストとは、例えば、Ｄ＝２の限界まで進むことになる。その他のサーバは、Ｄ＝１に進むことが可能であるが、その場合、それらのホストグループのいくつかは、Ｄ＝４に制限されることになり、したがって、それらのホストはＤ＝４まで強くなるが、Ｄ＝４より強くはならないことになる。同じ制限は、スペクトルのもう１つの端についても当てはまる。スーパサーバがＤ＝８を命令する場合、いくつかのサーバとホストとは、代わりにＤ＝６にだけ進む可能性がある。Ｄは順序付けされた状態であるため、これらの制限は単なる整数範囲（最大および最低）である。

【００４５】

Ｄの値は、ファイルの広がりなど、ある種のイベントの検出に基づいて変更できる。新ファイルの多すぎる複写がサーバのホスト間で伝播される場合、サーバは、広がりを止めるためにＤをオプションで増加する（例えば、Ｄ＝２に進む）ことができる。このイベントは、ある種の名前が多すぎる（例えば、名前による上位１０のリスト）または独自のコンテンツで多すぎる（例えば、データのハッシュによる上位１０のリスト）として特定されてよい。

【００４６】

値はまた、新しい着信ファイルまたは潜在的なウィルス攻撃など、サーバによって認められた新しいイベントに応答してサーバ要求により変更されることも可能である。ほとんどの場合、計画されたユーザ動作に続いて、またはある種のファイルイベントの観測に基づいてＤの変更を開始するのは管理者（人物）である。Ｄは、例えば、動作のプロセスの間に自動的に変更されることが可能であり、その場合、ホスト／サーバは、動作が終了した後でＤの値をその元の水準に戻すことになる。ＳＮＭＰなどの外部トリガはＤの値を変更できる。

【００４７】

もう１つの対応は、サーバが一定の閾値数のホストより少ないホスト上でコンテンツを自動的に承認するが、ホスト数がその数を超えた場合、コンテンツへのアクセスを禁止することである。かかるポリシーは、ネットワーク内の任意のコンテンツまたは任意のファイルの複写数を制限するために使用されることが可能である。また、かかるポリシーは、一定のホスト数を超えるコンテンツだけを報告するために使用されることも可能である。

【００４８】

サーバは、営業ホスト、マーケティングホスト、およびエンジニアリングホストなど、ホストの各論理グループに関してポリシーセットを個々に維持することができる。ポリシーセットは、抗体のバージョン番号に類似する独自の識別番号を有してよい。違いは、配備されると、ポリシーセットはポリシーセットを用いて後の問題を照合調整して問題配備を取り消すために「読取り専用」になることである。これは、Ｕｎｉｘ（登録商標） ユ

ーティリティ「差異（ｄｉｆｆ）」および「パッチ（ｐａｔｃｈ）」に類似した技術を使用して、異なる構成およびその他の更新に対して行われることも可能である。ホストはそのグループ用の現在のポリシーセットＩＤ番号に関してサーバに問い合わせることができ、不一致が存在する場合、ホストはサーバに「ポリシーセット取得（ＧｅｔＰｏｌｉｃｙＳｅｔ）」問合せを送信することができる。

【００４９】

ポリシーセットは、「新実行可能」ポリシーおよび「新スクリプト」ポリシーなど、複数のポリシーを含んでよい。各ポリシーは、動作状態（オン）、非動作状態（オフ）、または（ブロックが許可されるが、「ブロックされたであろう」メッセージがサーバに送信される）試験モードであってよい。各ポリシーは、各規則が基本的な「トリガと動作」モデルを有する複数の規則を有してよい。トリガは試験されるパターンである。パターンが一致する場合、結果として生じる動作が実行される。例えば、「Ｄ＝２で新実行可能の実施をブロックする」は以下のように特定され得る:

トリガ＝（Ｄ＝２　＆　ファイル動作＝実行　＆　状態＝ペンディング　＆　ファイル実行クラス＝実行可能クラス　ここで、実行可能クラス＝（*.exe |*.sys |*.dll | ...）

動作＝（ブロック＆報告＆通知（Ｐ））であり、「ブロック」は動作を停止し、「報告」はサーバに通知を送り、「通知」はパラメータセットＰを用いてユーザに警告する。

【００５０】

この構造により、カーネル抗体キャッシュ更新、Ｄ更新、およびポリシーセット更新の場合を除いて、カーネルは、ユーザ領域との相互作用なしに、すべてのポリシーを実施することができる。ポリシーセットは、１つの場所の中だけに記憶される必要があり、この実施に際してだけカーネル内で解釈される必要がある。ポリシーセットは、１つの安全なコンテンツ（カーネル）内で認証および記憶され、結果として、不正変更に対してより多くのセキュリティをもたらすことができる。

【００５１】

Ｄは異なる規則を異なるトリガと一致することを可能にするため、ポリシーおよび動作はＤによってパラメータ化される。ある状態を有するファイルは、ある動作をブロックされる場合がある。これらの状態は名前プロパティとデータプロパティの組合せであってよい。これらの状態は、ユーザ領域内で決定され、カーネル領域内でミラー化され、最終的に、これらの状態はサーバによって決定される。１つの有用なポリシーは、禁止されたファイルをブロックし、いくつかのＤ値で、ペンディング（新）ファイルのファイル実施をブロックすることである。

【００５２】

ポリシーは、アクセス可能性とセキュリティの間のトレードオフにより範囲全体にわたってポリシーのリストのセットとして提供され得る。サーバは、次いで、ホストにリストのうちの１つを選択させるために情報を提供することができる。リストをホストに提示させて、ホストが「プル」手法を使用してポリシーを更新することを可能にすることによって、ホストはサーバの制御のもとでセキュリティポリシーを好都合に更新することができる。

【００５３】

以下の表は、Ｄ値がマスタポリシーセット内の様々なポリシーにどのように影響を及ぼすことが可能であるかの例を示す。行はマスタセット内のポリシーであり、列は動作であり、セルは動作を表示するためのＤの数値範囲を有する。表内に特定された動作とその他の詳細とは下で要約される。

【００５４】

【表１】

D値に対するポリシー名	D=10 グローバル承認	D=8 保護が動作不可能にされる	D=6 追跡だけ	D=4 サイレント警告	D=3 局所承認	D=2 封鎖	D=1 書込み保護
新規／ペンディング エキュセキュータブル *.exe, *.sys, ...	新規の自動的かつグローバル承認、報告	許可	許可	実施許可、報告	新規の自動的かつ局所的な承認、報告	実施ブロック、通知、報告	書込み／実施ブロック、通知、報告
新規／ペンディング 独立型スクリプト *.vbs, *.bat, ...	新規の自動的かつグローバル承認、報告	許可	許可	実施許可、報告	新規の自動的かつ局所的な承認、報告	実施ブロック、通知、報告	書込み／実施ブロック、通知、報告
新規／ペンディング 埋込みスクリプト *.doc, *.xls, ... で	新規の自動的かつグローバル承認、報告	許可	許可	実施許可、報告	新規の自動的かつ局所的な承認、報告	実施ブロック、通知、報告	書込み／実施ブロック、通知、報告
新規 ウェブコンテンツ *.html, *.asp, ...	新規の自動的かつグローバル承認、報告	許可	許可	書込み許可、報告	書込み許可、報告	書込み保護、報告	書込み保護、報告
承認 (ハッシュおよび／または名前) 実施／スクリプト／埋込み	許可	許可	許可	許可	許可	許可	許可
禁止／非承認 (ハッシュで) 実施／スクリプト／埋込み	許可	許可	実施ブロック、通知、報告	実施ブロック、通知、報告	実施ブロック、通知、報告	実施ブロック、通知、報告	実施ブロック、通知、報告
禁止／非承認 (名前で) 実施／スクリプト／埋込み	許可	許可	実施ブロック、通知、報告	実施ブロック、通知、報告	実施ブロック、通知、報告	実施ブロック、通知、報告	実施ブロック、通知、報告
コンテンツ変更およびコンテンツ作成の追跡	追跡、報告	許可	追跡、報告	追跡、報告	追跡、報告	追跡、報告	追跡、報告

【００５５】

（１）許可。動作を許可し、そうでない場合はサイレント

（２）ブロック。動作をブロックし、そうでない場合はサイレント。

（３）追跡。動作と（コンテンツがペンディングまたは禁止である場合）結果として生じるコンテンツを追跡し、そうでない場合はサイレント。承認されたコンテンツは一般に追跡されない

（４）報告。サーバに通知を送信する

（５）通知。動作がなぜブロック／割り込みされたのかをホストの終端ユーザに知らせる

（６）自動的な局所承認。局所ホスト状態＝ペンディングを有する新ホストファイルおよび／または新コンテンツは、ファイル／コンテンツが作成／変更されると、局所ホスト上だけでホスト状態＝承認または状態＝局所承認に局所的に設定される。

（７）自動的かつ世界的な承認。局所状態＝ペンディングを有する新ホストファイルおよび／または新コンテンツは、ファイル／コンテンツが作成／変更されると、サーバ上でサーバ状態＝承認に世界的に設定される。

【００５６】

抗体の導入、ファイルのメタ情報

具体的に図２を参照すると、許可される動作に関して、システム内のサーバは、ファイルの走査履歴と各ファイルに関する承認状態とを追跡するために主に使用される抗体データベース３６を含む。抗体は、以下のフィールドの一部またはすべてを含む可能性がある、ファイルに関するデータ（すなわち、メタデータまたはメタ情報）のブロックである。

【００５７】

・初めて参照された時間。ファイルまたはハッシュがホストによって初めて参照され、サーバに報告されたとき。
・ファイルＩＤ。ＭＤ５、ＳＨＡ－１、およびＯＭＡＣなど、コンテンツの１つまたは複数のハッシュを含めて、ファイルに関する独自の識別子。
・ファイルタイプ。ファイルクラス（例えば、実行可能、スクリプト、オフィス文書、アーカイブなど）。これは、初めて参照されたファイル名から、かつファイルコンテンツの分析から導出される。
・状況／状態。承認、ペンディング、または禁止を含めて、現在のファイル状況。
・方法。サーバがファイルについて学習する方法（自動、手動など）。
・ファイル名。初めて参照されて、サーバに報告されたファイルの名前。これはファイルの現在の名前ではなく、ネットワーク上で参照された初めての事例の正に名前である可能性がある。
・ファイル経路。初めて参照されて、サーバに報告されたファイルの経路。
・初めて参照／報告されたときのホストファイル名／経路／拡張子。
・最後に参照／報告されたときのホストファイル名／経路／拡張子。
・初めて参照／報告されたときのホストＩＰアドレス。
・初めて参照されたホスト。その上でファイルまたはハッシュが初めて参照および報告されたホストの名前。
・分析結果。最後の走査またはその他の分析の結果。
・最初の分析。ファイルの最初の走査／分析の時間。
・最後の分析。ファイルが最後に走査／分析された時間。
・最後の更新。ファイル状態が最後に変更された時間。
・親コンテナ。ファイルに関連したその他のファイルへのリンク。
・親コンテナ属性。ファイル名、初めに決定された時間、初めに決定されたホスト、ファイル経路、製品分類、および１つの関連するコンテナファイルの状態。
・ルートコンテナ。ファイルに関連したその他のファイルへのリンク。ルートコンテナは、もう１つのコンテナ内に含まれないコンテナである。
・ルートコンテナ属性。ファイル名、初めに決定された時間、初めに決定されたホスト、ファイル経路、製品分類、および１つの関連するルートコンテナファイルの状態。
・知られている場合、基準親ファイルコンテナ。これらは、「ハッシュ＝ｘのアーカイブファイル内部でこのハッシュ＝ｙのファイルが観測された」など、包括する関連性を維持するために使用される。
・実行可能、スクリプトファイル、埋込みマクロなど、（コンテンツ分析によって決定される）ファイルコンテンツタイプ。

【００５８】

サーバは、システムに関してシステムの完全な抗体セットを有する。各ホストは、ユーザキャッシュ６４内とカーネルキャッシュ８２内とに抗体の局所サブセットを含むことができ、一方、サーバは一定の状態に設定および変更するための権限である。例えば、サーバは、ペンディングから承認または禁止（これらの３つの状態はコンテンツハッシュに関連付けられることが好ましい）の状態遷移を含めて、変更を中央で開始して、（ホストに）伝達する権限であり、一方、ホストは、局所的に承認されるように状態を設定できる唯一の権限である。データベース３６内の各入力は、永続的であり、好ましくは、ファイルデータハッシュ索引により簡単にアクセス可能である。管理者が容易に抗体データベースをブラウズできるように、データベースは、ファイル名、初めて参照された日、状態、分析結果、ホストＩＤ、またはホストカウントなど、その他の鍵によって任意選択で索引付けされてよい。

【００５９】

抗体を有するデータベースはサーバ内またはサーバ上にあるものとして説明されるが、これはデータベースがサーバに関連することを意味する点を理解されたい。抗体を有するデータベースは、同じボックス内およびサーバの処理機能性内に物理的に存在することが

可能であり、または異なるボックス内または遠隔位置内にさえ存在することができる。遠隔の場合、データを取得するために適切な有線接続または無線接続が存在すべきである。

【００６０】

抗体（ＡＢ）追跡の導入

新ファイルが作成されると、または既存のファイルが変更されると、追跡ポリシーがトリガされることが可能であり、それにより、ファイルおよび抗体の分析イベントのチェーンを始める。まず、ホストは一連のステップを実行して、すでに分析されたコンテンツに対応し、それに関して抗体がホストキャッシュ内にすでに記憶されているコンテンツに重要な変更が存在するか否かを決定する。コンテンツの抗体がホストキャッシュ内にない場合、サーバは問合せされて、サーバがすでにそのコンテンツを分析したか否かを決定する。サーバが対応する抗体を有さない場合、コンテンツはさらなる分析のためにサーバにアップロードされる。サーバが状態を確定的に決定できるまで、コンテンツに関連する状態はペンディングに設定される、すなわちまだ決定されない。ペンディングのコンテンツに対するその後のアクセスは限定され得る。サーバは、コンテンツがサーバ上で初めに参照されてからの時間に基づいてコンテンツに関する分析を実行する。分析またはその他の外部決定に基づいて、サーバは状態の変更を確定的に決定することができる。これらの変更は、後の取り出しのためにホストによって表示されることが可能であり、したがって、ホストは変更された状態を用いてその抗体キャッシュを更新することができる。

【００６１】

ホスト抗体追跡

図３を参照すると、ホストは、実施、読取り、名前変更、または書込みを含めて、ファイル動作を傍受して（５０１）、ステートフルファイル動作フィルタ（５０２）に動作を提供する（５０２）。ファイル名がカーネルキャッシュ内になく、カーネルキャッシュの間違いが存在し（５１０）、可能なファイル修正またはコンテンツ修正が存在する場合（５１１）、状態は無効にされる。次いで、ファイルは、以下により詳細に説明されるように、縮小ファイルを作成するために動作状態の当該コンテンツを抽出するコンテンツエキストラクタに進み（５０３）、コンテンツ署名者に縮小ファイルを提供する（５０４）。コンテンツ署名者は、ＭＤ５などの暗号ハッシュを縮小ファイルに応用する。このハッシュはファイルとファイル名とに関連付けられる。ハッシュおよびその他の分析（キャッシュの間違え解決）が完了する間、ファイル動作は遅延／機能停止されてよい。

【００６２】

ホストはまた、ハッシュコンテンツに基づいてを行い、状態を取得しようと試みる（５０５）。コンテンツと状態とが探索されない場合、状態はペンディングに送られる。これは、ファイル動作は進むことが許可されることを意味するが、追跡記録など、さらなる監視が発生してもよい。コンテンツが探索された場合、名前と、コンテンツと、コンテナ（動作状態のコンテンツを含むファイル）と、状態とはすべて共に関連付けられる（５０７）。そうでなければ、ホストはサーバがそのメモリ内のコンテンツを調査する（５０６）ことを要求する。そこで探索された場合、名前と、コンテンツと、コンテナ（動作状態のコンテンツを含むファイル）と、状態とはすべて共に関連付けられる（５０７）。コンテンツと状態とが探索されない場合、状態はペンディングに設定され、コンテンツはサーバにアップロードされ（５０８）、サーバはアップロードを確認する（５０９）。サーバはまた、いくつかのサーバに関連する「スーパサーバ」に注意を向けることもできる。コンテナ関係は記憶されて、ファイルおよびその他のコンテナと関連付けられる。コンテナ情報はまた、サーバおよびホストに送られると同様に分析のために送られる。「ルートコンテナ」は、もう１つのコンテナによって含まれないコンテナである。コンテナはその関連するファイルによって、ならびに暗号ハッシュによって識別される。

【００６３】

一般に、抗体状態は、ファイルコンテンツの「動作状態の」部分またはファイルコンテンツの全体のハッシュまたは署名に関連付けられる。したがって、一般に、ハッシュ（ファイルデータ／コンテンツ）は状態である。これはデータを状態にマップする。状態（Ｓ

）は、「承認」（ホワイトリスト）もしくは「禁止」（ブラックリスト）または「ペンディング」（まだ完全に分析されていない新たに決定されたファイルなどの「グレイリスト」）など、情報の多くの断片を含む。

【００６４】

このシステムの利点は、名前状態とコンテンツ状態との組合せである。例えば、サーバは、＊ｍｓｂｌａｓｔ．ｅｘｅなど、複数の名前禁止を特定および記憶することができる。サーバは、正規表現および関連するメタ情報のリストとして名前状態ポリシーを記憶する。正規表現に一致する任意のファイルドライブ／経路／名前／拡張子（ｅｘｔ）は、次いで、名前のメタ情報を引き継ぐ。この情報は、ファイル名が変更されるときまたは名前のメタ情報仕様が変更するときはいつでも更新される。名前状態とポリシーとは、サーバからホストに伝播される。例えば、＊ｍｓｂｌａｓｔ．ｅｘｅを名前禁止に追加することによって、サーバは新ポリシー／状態を検出することになり、その仕様をホストに伝播することになる。ホストは、次いで、＊ｍｓｂｌａｓｔ．ｅｘｅとの一致に関してそれらの名前のメタ情報キャッシュを調べ、一致するファイルは名前禁止状態を引き継ぐことになる。ホストファイル状態は、名前状態およびデータ状態の重ね合わせである。例えば、ｔｅｍｐ＿ｍｓｂｌａｓｔ．ｅｘｅがコンテンツ状態＝ペンディングを有する場合、名前禁止はペンディングより優位であるため、その組み合わされた状態は禁止される。名前承認状態は、同様の形で処理される。

【００６５】

抗体は、データベース内で階層的に処理される。上に示されたように抗体に関して４つの主な記憶場所が存在する。ホストエージェントで、カーネル抗体キャッシュ８２は、ファイル名を抗体状態にマップする。例えば、名前＝ｃ：＼ｗｉｎｄｏｗｓ（登録商標）＼ｂａｒ．ｅｘｅ→状態＝承認。要するに、このマッピングは名前→状態である。カーネルは、ファイルコンテンツへのアクセスの必要なしに、状態に基づいてポリシーを実施することができ、これを行う。ファイルはカーネル内で暗号化されることが可能であるが、より高い非暗号化の形態で可視的であるため、これは有用である。カーネルは名前に対して直接的なアクセスを有するが、ハッシュに対してはアクセスを有さない。長い待ち時間（数秒、数分、数時間、数日）が存在する可能性があるという点で、カーネルキャッシュは、その他のキャッシュ、および最終的にはサーバと弱く一貫する可能性がある。

【００６６】

ホストエージェントは、ユーザ抗体の名前キャッシュ（ＵＮ）と、ユーザ抗体のデータキャッシュ（ＵＤ）６０とを有する。ＵＮは、ファイル名をファイルコンテンツ（データ）のハッシュにマップする。すなわち、ＵＮはＮをデータにマップする。同様に、ＵＮは、データを状態にマップする（データ→Ｓ）。一般に、Ｎ→データのマッピングは、多対１であり、ＵＮは局所ファイルシステムの構造をミラー化する。ＭＤ５など、使用されることが好ましい強いハッシュの場合、ハッシュ衝突は稀であるため、データ→Ｓのマッピングは、一般に、１対１である。ＵＮキャッシュおよびＵＤキャッシュもサーバと弱く一貫するが、カーネルキャッシュがそうであるように、ＵＮとＵＤは両方とも局所ホストファイルシステムと強く一貫する。ＵＮとＵＤとは、以下のように組み合わされることができる。Ｎ→データ→Ｓ＝Ｎ→Ｓ。

【００６７】

サーバは、そのホストのいずれかによってこれまで報告された、一般にすべての独自のハッシュの抗体・データベース３４を有し、（１個存在する場合）スーパサーバは、そのサーバのいずれかの上で決定された、一般にすべての独自のハッシュの抗体・データベースを有する。独自のハッシュに限定することは、記憶と処理とを限定するが、記憶および処理におけるさらなる改善により、より多くが記憶され得る。また、独自のハッシュに限定することは、結果として、より効果的な分析とより低いネットワークトラフィックとをもたらす。

【００６８】

一般に、新ファイルは、「新ファイル」イベントまたは「汚染ファイル」イベントに応

答して、ホストからサーバ、スーパサーバに伝播し、新たに計算された抗体状態は、抗体更新の形で、スーパサーバから、サーバ、ホストユーザ、ホストカーネルに逆に伝播する。このように、抗体は、中央で制御、管理、および検証される。サーバは抗体を「所有」および証明し、サーバは、抗体が変更または偽造されていないという認証を提供する。ホストは、一般にサーバ上の抗体に対応するが、必ずしもそうであるとは限らない独自の抗体を維持する。したがって、汚染されたホストまたは機能不全のホストは、サーバまたはスーパサーバの抗体収集物を劣化することはできず、汚染されたホストは、その他のホストの抗体を劣化することもできない。

【００６９】

抗体がハッシュ／データと関連付けられず、むしろ名前によって関連付けられるように、ホスト上で抗体状態が記憶されることが好ましい。カーネルは、ポリシーを解析、解釈、および実施し、ファイルの状態は名前で調べられる。好ましい実施形態は、カーネル内でポリシーを実施するが、その他の実施形態はユーザ領域でポリシーを実施できる点を理解されたい。ユーザ領域内またはカーネル内で状態を調べる場合、それは、実際には、結果として生じる状態を決定する混合物である。例えば、ｆｏｏ．ｅｘｅのデータの抗体はペンディングであるが、名前の抗体がその名前に基づいて禁止される場合、ＡＢ状態取得（ＧｅｔＡＢＳｔａｔｅ）（ｆｏｏ．ｅｘｅ）は、「名前で禁止」の結果を戻す。抗体状態＝名前禁止を有するファイルの実施をブロックするための個々のポリシーが存在する。そのポリシーに関する動作は、上記のようにＤの値によってパラメータ化される。１つの差異は、「名前で禁止」をブロックするポリシーは、より低いＤセキュリティ設定で動作状態にある点である。例えば、Ｄ＝４で、「ペンディング」ファイルは、（サイレント警告により）実施することになるが、禁止されたファイルは実施されないことになる。

【００７０】

名前禁止は、正規表現のリストとして表され、サーバ上にワイルドカード（＊）（例えば、「＊ｏｏ．ｅｘｅ」または「＊ｍｓｂｌａｓｔ．ｅｘｅ」）を含んでよい。これらのリストは、バージョン番号を有する。ホストが調査するとき、ホストはそれらのバージョン番号を検査する。ホストが不一致を検出する場合、ホストは、次いで、名前禁止取得（ＧｅｔＮａｍｅＢａｎｓ）問合せをサーバから送信する（すなわち、ホストはサーバから新禁止データをプルする）。次いで、これらの正規表現は、名前の抗体に対して再評価される。名前禁止は状態の属性であり、名前禁止リストが変更する場合またはファイル名が変更する場合のみ再度計算されなければならない。ワイルドカードリストは、すべてのファイル動作に関して比較されなくてよい。したがって、データの抗体および名前の抗体の二重性が有用である。また、数百または数千の名前の正規表現は、法外に費用がかかる可能性がある、各ファイル動作に関してカーネル内で数千の正規表現の一致計算を要求せずに、同時に実施されることが可能である。

【００７１】

ファイルコンテンツの追跡

図２に戻ると、傍受／ブロック機能８６は、ファイルアクセス要求を傍受して、読み取ることができる。この機能は、ポリシー情報を取得する間に要求を一時停止し、カーネル内のポリシーに基づいて要求をブロックし、ブロックされた要求に関して適切な誤りコードを戻すことができる。機能８６は、ファイルアクセス要求から、要求プロセス名と、要求の局所システム時間と、（全経路を含む）要求されたファイルと、要求された動作（例えば、読取り、書込み、または実施）を読み取る。一実施形態では、機能８６は、すべてのファイルアクセス要求を「ステートフルフィルタ」８８に供給し、フィルタ８８が動作はブロックまたは許可されたことを表示するフラグを戻すまで、すべての動作はブロックされる。

【００７２】

フィルタ８８は、ファイルアクセス要求を機能８６から傍受して、ほとんどのファイルアクセス要求に対して「ブロック」または「許可」の動作を戻す。すでに承認されているファイルアクセス要求に関連付けられることができない任意のファイルアクセス要求は、

カーネルトリガおよび動作モジュール９０に転送され、カーネルトリガおよび動作モジュール９０は、「ブロック」または「許可」の動作を戻す。この動作は、フィルタ８８によって記憶されて、好ましくは、任意のその後の関連する類似ファイルアクセス要求のために機能８６に戻される。

【００７３】

フィルタ８８は、（全カーネルの独自の識別子（例えば、Ｗｉｎｄｏｗｓ（登録商標）ＮＴ内のカーネルファイルハンドル）によって索引付けられた）すでに開かれたファイルのキャッシュ８４を維持する。各キャッシュ入力は、ファイル識別子（カーネルファイルハンドル）と、読取り、書込み、もしくは実施に関してブロックまたは許可の許可とを含む。

【００７４】

複数のプロセスが同じファイルにアクセスする場合、各々は、その独自のキャッシュ入力を有することになる。所与のプロセスが新ファイルアクセスを試みる場合、ステートフルフィルタは、そのファイルに関してキャッシュの失敗を経験することになり、これはステートフルフィルタにファイルアクセス要求をトリガおよび動作モジュールに提出させることになる。モジュール９０がそれを許可する場合、要求された動作（読取り、書込み、または実施）用のフラグは、「許可」に設定されるべきである。そうでなければ、「ブロック」に設定されるべきである。１種類の許可（例えば、読取り）だけを取得したプロセスが、次いで、もう１つの種類のアクセス（例えば、書込み）を試みる場合、モジュール９０は、再度、接触されることになる。

【００７５】

その年齢が一定の値（例えば、６０秒）を超えるキャッシュ入力は削除されることが可能である。これは、何らかの理由で、除去されない入力を取り除くことを可能にする。これはまた、モジュール９０によってファイルの周期再検査も可能にする。

【００７６】

この例では、ファイル書込み動作は、ファイル「ｆｏｏ．ｅｘｅ」に関して、ブロックシム８６内のカーネル内でホスト・エージェント・カーネル・プログラム（ＨＫ）によって捕らえられる。Ｄ＝４の値で、ファイル動作、この場合、ファイル書込み動作は、動作化された「汚染追跡」ポリシーによって捕らえられ、これは、ホスト・カーネル・プログラムからホスト・エージェント・ユーザ領域プログラム（ＨＵ）に「汚染」イベントを開始させる。このイベントは、ファイル名と汚染動作とを特定する。汚染追跡ポリシーはそのフィールドを無効にしたため、カーネルキャッシュ８２は、この動作に関して調査されない。

【００７７】

ＨＵは、次いで、ファイル内ならびにイベント処理６６内および分析エンジン６８内でｆｏｏ．ｅｘｅに関して様々な局所分析動作を実行する。まず、ｆｏｏ．ｅｘｅは、それが存在するか、それが読取り可能であるか、それが実際に実施可能であるかを決定するために検査される。フィルタ８８内の「当該データ」の抽出など、その他の動作が実行され得る。例えば、ファイルがｆｏｏ．ｂａｔであった場合、スクリプト注釈は除去されることができる。ｆｏｏ．ｅｘｅの抽出データは、次いで、暗号的にハッシュされ、このハッシュはＨＵ抗体キャッシュ６０内の調査を試みるために使用される。名前とデータとがすでに存在する場合、その他には何も行われない。名前は新しいが、データが知られている場合、新しい名前の抗体がＵＮキャッシュ内で作成される。このプロセスはすべて、「段階１分析待ち行列」と呼ばれるものの一部である。多くのファイルは、ホスト上の段階１待ち行列内でハッシュされるのを待って列に並べられることができる。データはまだ知られていないまたはまだ分析されていないため、段階１待ち行列は、名前の抗体とメタ情報とだけを有する。

【００７８】

ホストがこのファイルデータとハッシュとを決定した場合、そのハッシュに関して対応する、知られているメタ情報は、そのファイルに関するホストファイルのメタ情報に関連

付けられ、ＵＤ局所メモリまたは局所ディスク記憶装置から取り出される（この順序で行われる）。ホストがこのデータを決定していない場合、ＵＤキャッシュは「失敗する」。ハッシュは、段階２分析待ち行列に入れられる。現実には、データの抗体、すなわち、「承認される」、「禁止される」、または「ペンディング」など、論理的にデータを追跡する状態が存在し、名前の抗体（例えば、「名前で禁止」）も存在する。例えば、サーバが「＊ｏｏ．ｅｘｅ」を禁じる場合、ｆｏｏ．ｅｘｅ用の名前の抗体は「名前禁止」を表示することになり、名前禁止ポリシーはそれに基づいてブロックすることができる。したがって、キャッシュが、ｆｏｏ．ｅｘｅが（名前で）すでに禁止されていることを知っている可能性があるとしても、汚染追跡解決は依然として継続する。名前とデータの抗体のこの区別は、個々のホストに対する範囲において局所的であるが、（下で説明される）ファイル探索機能およびポリシー実施にとって重要になる。データの抗体は、それにより、段階２待ち行列に入れられる。

【００７９】

段階２分析は、まずメモリキャッシュから、次いで、局所ディスクベースの記憶装置から、次いで、サーバから局所状態情報を解決することを試みることになる。サーバが接続される場合、メタ情報は解決されるため、段階２待ち行列は空になる。ｆｏｏ．ｅｘｅがこの待ち行列から除去されると、サーバは、このデータハッシュを決定したか否か、そのハッシュが局所的に探索されていないかどうかをたずねられる。答えが「いいえ」である場合、ｆｏｏ．ｅｘｅとそのハッシュとその他のメタ情報とは、サーバにアップロードするために段階３待ち行列に入れられる。加えて、サーバが前にそのハッシュを決定していない場合、またはサーバ分析がその他の状態を決定するためにまだ十分完了されていない場合、サーバは、「ペンディング」規定の抗体状態をホストに送ることになる。サーバがすでに有効な抗体と状態とを計算した場合、サーバはこの抗体のメタ情報を戻す。サーバがｆｏｏ．ｅｘｅに関してこのデータを決定したことがない場合、サーバの経験においてすべての機械はこのファイルを決定していないという意味で、それは新しい。

【００８０】

ｆｏｏ．ｅｘｅが段階３待ち行列から除去される場合、ｆｏｏ．ｅｘｅは暗号化された一方向転送を使用して、サーバにアップロードされる。すなわち、ＦＴＰＳ（セキュアファイル転送プロトコル）と書込み専用サーバディレクトリとを使用して、ファイルはサーバにアップロードされることが可能であるが、ダウンロードされることはできない。アップロードが首尾よく完了すると、ホストはｆｏｏ．ｅｘｅが転送されたことをサーバに通知する。情報漏れを最低限に抑えるため、および追加のセキュリティのために、この転送はハッシュに参照される。

【００８１】

サーバが、ｆｏｏ．ｅｘｅがアップロードされたことを学ぶと、サーバは、ホストが行うように、いくつかの段階を通じてファイルを分析することで開始する。この場合、サーバがその初めての出現にタイムスタンプを押すためにその同期化された検証クロックを使用することにより、新抗体が作成される。また抽出およびハッシュが実行され、それらの結果はホストの結果に取って代わる。

【００８２】

サーバ分析は、サーバ上で特定および記憶されるスケジュールに従う。このスケジュールは、サーバ上でのファイルまたはそのハッシュの初めての出現時間に関連する。例えば、ファイルが正午に到着し、スケジュールが「＋０でハッシュ調査、および＋０でＡＶ走査、ならびに＋２時間でＡＶ走査」である場合、正午に、ファイルハッシュは、外部ハッシュ調査サービスを使用して計算および調査されることになる。次いで、ＡＶ走査が実行される。２時間後の午後２時に、そのファイルのもう１つのＡＶ走査が実行される。スケジュールを説明するためのもう１つの方法は、スケジュールを「サーバ上のファイル年齢」と関連付けることである。

【００８３】

抗体がサーバ上の状態を変更する場合、増分カウンタ値が抗体に書き込まれる。このカ

ウンタは、任意の特定のホストまたはスーパサーバがチェックインされてから変更された抗体の範囲だけを選択するために使用される。例えば、先の抗体変更が、ペンディングから承認へのｇｌｏｒｐ．ｂａｔ変換であり、世界的な抗体バージョンのカウンタが２７７であった場合、ｇｌｏｒｐ．ｂａｔのハッシュに対応するサーバの抗体は、バージョン番号２７７を取得することになり、カウンタは２７８になる。したがって、抗体ｆｏｏ．ｅｘｅに対応するバージョン番号は２７８であり、カウンタは２７９である。

【００８４】

ホストが周期的に調査する場合、ホストはその最後の抗体のバージョン番号を提供し、サーバは、最後の調査から変更されたすべての抗体を送ることになる。サーバは現在の番号を送り、ホストが不一致に気づいた場合、ホストは抗体更新をサーバに要求し、データの抗体リストが戻ることが好ましい。それらの抗体は、次いで、ホストの抗体に併合され、変更はカーネルにも送られる。ホストは、いまだかつて決定されていないデータに関していくつかの抗体を取得および記憶することができるが、一般に、既存のホストファイルに対応する抗体だけが併合される。その他は、通常、破棄される。サーバは、更新の最後の数分をキャッシュして、すべての更新を各ホストに対して特別に調整することの影響を最低限に抑える。この場合も、ホストは、一般に、必要とするより多くの抗体を取得するため、そして新抗体は稀であるため、このトラフィックは限定される。抗体更新は、その他のメッセージの大部分と同様、小さい。

【００８５】

抗体は、類似の形で依然としてスーパサーバと同期化されることが可能である。ここで、スーパサーバは、サーバを調査して、抗体更新リストを取得することができる。スーパサーバは、これらを併合して、各サーバに関して特別に調整した更新を送る。これらの更新はすべて、数分または数日だけ遅れる可能性があるという点で弱く一貫するが、更新内の「穴（ｈｏｌｅ）」を回避するために連動および保護が存在しなければならない。

【００８６】

抗体の併合に関してその他の態様および特徴が存在する。例えば、いくつかのサーバは、スーパサーバからある種の抗体更新を受け入れない場合がある。また、ホストは、ある種の局所状態をある種のサーバ特定された状態に変更することを許可しないことになる。

【００８７】

１つの課題は、キャッシュの初期状態と初期ポリシーとを含む。サーバキャッシュは、知られている良いハッシュ抗体と不良ハッシュ抗体により事前ロードされることが可能であり、またはサーバキャッシュは空である可能性があり、すべて正しい。しかし、ホストは、時折「細流充電」しなければならない。例えば、ホストが初めてあるサーバに接続する場合、この事実は検出され、ホストファイルシステム上のすべての当該ファイルが段階１待ち行列に挿入されるときはいつでも、ホストは細流充電を実行することになる。このプロセスの間、中間キャッシュが問題を引き起こさないことを確実にするために、Ｄの特別値が使用される。抗体は、一般に、すべて状態「ペンディング」で開始し、サーバとゆっくり同期化する。また、ホストのすべて抗体と、待ち行列情報と、関連する大域とは、周期的にかつ再ブートを経て維持される。

【００８８】

カーネルキャッシュの一貫性

ホストエージェントのブート時またはその他の初期化時に、カーネルは、有効なメタ情報を有するすべての知られている既存のホストファイルに関して、ユーザ領域から知られているすべての有効な抗体によりロードされる。いくつかの抗体更新は、サーバから、またはユーザ領域内の分析待ち行列から受信されるとカーネルに送られる。しかし、いくつかの更新は、カーネルキャッシュの失敗の結果である。ポリシーが動作状態であると決定され、抗体状態が必要であり、その状態が利用不可能である場合、カーネルは、しばらくの間、動作を全体的に停止して、カーネルの失敗イベントをユーザ領域に送る。いくつかのイベントは、抗体がすぐに必要でないとしても停止される可能性がある。これは、ポリシーが、ホストユーザがユーザインターフェース（メッセージボックスの出現）と相互作

用すること（例えば、ブロックされたペンディング動作を取り消すため、およびしばらくの間、ブロックすることなしに、その後の制限された動作を続けるために「はい」をクリックすること）によって抑制状態（ペンディング）を取り消すことを許可する場合である。

【００８９】

一例では、インストールプログラムは、ｉｎｓｔ．ｅｘｅと呼ばれる新プログラムのパックを解いて、次いで、名前を変更して、それを実施する。カーネルは、解析が実行される間、名前変更を展開して、実施を展開することによって一時的な不一致を回避することになる。結果として生じる抗体は、ユーザ領域から非同期的に送り出され、次いで、非同期的更新が完了するとすぐに、ペンディング動作はブロックが取り除かれて、ポリシーが要求される状態情報を用いて評価される。

【００９０】

カーネルキャッシュは、初期化時にファイルシステム内のほとんどすべてのファイルに関して抗体を含む。カーネルキャッシュ内に穴またはその他の不一致を残す可能性のある動作は、短い時間であっても、遅延およびインターロックされ、その結果、一貫性が維持される。ユーザ領域キャッシュは、非常に低い待ち時間を用いてカーネルの失敗を解決するために最適化される。カーネルキャッシュとユーザ領域キャッシュとは、サーバ側の待ち時間に極めて敏感ではなく、一方、カーネルキャッシュはインターロックと適切な永続性に敏感である。

【００９１】

ファイル探索

ＵＮキャッシュとＵＤキャッシュとは低い待ち時間調査のために最適化されることが好ましいため、これらのキャッシュは、何のホストに何のファイルがあるかの一覧を作成するために、本明細書で「ファイル探索」と呼ばれる、サーバから配信された抗体問合せの一部として使用されることが可能である。ファイル探索要求は、サーバまたはスーパサーバ上でウェブインターフェースを経由してウェブブラウザ書式を提供することによって管理者によって特定されることが可能である。例えば、以下のクオリファイヤ（修飾子）が一緒に特定され得る。

【００９２】

（１）ファイル名のための正規表現パターン仕様、
（２）ファイル経路のための正規表現パターン仕様、
（３）ファイルの当該コンテンツのハッシュ、
（４）ファイルに関連するコンテナのハッシュまたはその他のＩＤ、
（５）ファイルまたはファイルのハッシュがホストによって初めて参照されたときの時間範囲、
（６）ホストの名前、
（７）ホストのＩＰアドレス、
（８）ファイルのタイプ、
（９）少なくとも３つの状態、すなわち、承認、禁止、ペンディングの分析のセットからのファイルに関連する１つまたは複数のホストファイル状態。例えば、ＡＩ禁止＝（名前禁止、ハッシュで禁止）のセット。
（１０）ある種のファイル動作がそのファイルに関してホストによって実行されているかどうか、そして
（１１）ホストグループ。

【００９３】

図４を参照すると、サーバは特定されたホストによる後の取出しのために要求を送るという点で、完全なファイル探索要求は電子メールに類似する。ホストがチェックインすると、ホストは、ホストを待つ、サーバからのファイル探索メッセージが存在するか否かを知る。ホストが未処理のファイル探索要求を有することを知ると、図４で線（１）として示されるように、ホストはファイル探索要求取得（ＧｅｔＦｉｎｄＦｉｌｅＲｅｑｕｅｓ

ｔｓ）を使用して要求を取り出す。すなわち、要求はサーバからの「プル」として達成されることが好ましい。これは、リスニング・ホスト・ソケットを必要とせずに、より安全な実施を可能にする。

【００９４】

接続されたホストは、各々、その抗体キャッシュから、適用可能なデータにアクセスすることによって、そのファイル探索要求を処理して、戻された各ファイルに関して、以下の情報の一部またはすべてを含めて、ファイル探索結果通知（ＰｏｓｔＦｉｎｄＦｉｌｅＲｅｓｕｌｔｓ）として示される結果のリストを結果データベースに書き込む（図４の線（２））。

【００９５】

（１）ファイル名、

（２）ファイル経路、

（３）ファイルの当該コンテンツのハッシュ、

（４）ファイルまたはファイルのハッシュがホストによって初めて参照されたときの時間範囲、

（５）ホストの名前、

（６）ホストのＩＰアドレス、

（７）ファイルのタイプ、

（８）ファイル向けのコンテナ情報、

（９）少なくとも３つの状態、すなわち、承認、禁止、ペンディングの分析のセットからのファイルに関連する１つまたは複数のホストファイル状態、

（１０）ある種のファイル動作がそのファイルに関してホストによって実行されているかどうか、そして

（１１）ホストグループ。

【００９６】

一実施形態では、（ファイル探索だけでなく）ホストとサーバの間のすべての通信は、ホストが初めにサーバに接続して、１つまたは複数のネットワークメッセージを送信し、切断前に、そのホストメッセージに関してサーバ応答を受信することによって達成される。この場合も、リスニング・ホスト・ソケットが必要でないという点で、これはより安全であるという利点を有する。ホストのアドレス指定、経路を維持して、かかるホスト情報の探索の必要性を削減するのではなく、サーバのアドレス指定および経路だけが維持される必要があるという点で、追加の利点が存在する。

【００９７】

サーバは、ホストからのファイル探索結果リストのマスタリストを併合および蓄積する。これらのリストの結合は、完全なファイル探索要求応答であり、経時的に蓄積し、通常、１分未満で完了する。局所ホスト処理は抗体キャッシュだけにアクセスし、ホストファイルシステムにはアクセスしないため、これらの問合せは高速であり得る。名前とデータの抗体との関連性の二重システムとキャッシュとが、これを可能にする。サーバは、次いで、例えば、ウェブインターフェースを介して、結果を管理者に送出する。また、一定のファイル探索結果は、ＳＮＭＰ、シスログ、警告、およびその他の通知システムに影響を及ぼし、これらをトリガすることができる。

【００９８】

スーパサーバはまた、類似の形でサーバによってアクセスされるように要求を送ることもでき、またはスーパサーバは、ファイル探索要求をサーバに直接的に提出することが可能である。次いで、サーバは、併合された結果をスーパサーバに戻すことができ、スーパサーバは、次いで、これらの結果をより大きなマスタ結果に併合することが可能である。これは、ファイル探索要求を処理する場合のサーバとホストの間の関係に類似する。

【００９９】

タイマトリガされた中央分析

図５を参照すると、サーバは、イベントに基づいて分析（例えば、ホストがコンテンツ

を更新するたびに分析）を行うことができ、またはシステムは、時間に基づいてこれらの分析を行うことができる。上で示されたように、新コンテンツは、サーバにアップロードされることが可能であり、データベース内に記憶されるメタデータまたはメタ情報を作成するために、分析は外部および／または内部の分析エージェントにより実行される。システムは、次いで、例えば、新コンテンツが更新された場合、ファイルの第１の考察に関連して一定時間後に、さらなるスケジュールされた分析に関して検査することができる。サーバとスーパサーバとは、多くのタイプのさらなる時間ベースの分析を実行することが可能である。

【０１００】

図６を参照すると、ファイルが初めて参照されて、その抗体がサーバのデータベースに加えられると、効果は、タイマが各ファイルに関して開始される場合と同様である。したがって、例えば、時間間隔は（第１の目撃またはサーバへの報告後、ｔ＝０＝即時、ｔ＝１２時間後、ｔ＝２日後、およびｔ＝３０日後）である可能性があり、サーバのクロックに基づく可能性がある。１回だけの時間設定された動作に加えて、周期的な動作が特定され得る。本明細書で示されるように、アンチウィルス（ＡＶ）スキャンおよびアンチスパイウェア（ＡＳ）スキャンは、異なる時間に実行されることが可能であり、その他の分析が実行されることが可能である。後の期間の場合、これは、ファイルを考察した可能性があるその他のサーバに対する比較であってよい。一般に、後の分析は、ある期間内に初めて参照されたすべてのファイルに基づくことになる。例えば、１時間以内に初めて参照されたすべてのファイルは、その期間内の最後のファイルから１２時間後に１２時間の分析を得ることになる。

【０１０１】

図７を参照すると、システムは分析のためにファイルを選択して、特定された分析を実行するためにそのファイルを送信する。各時間間隔に関して、異なる動作が特定されてよい。ファイルはサーバ上にしばらく維持されるため、これらの時間動作化された分析は、元のホストが依然として接続されているか否かにかかわらず続行することが可能である。実行され得る中央時間設定されたサーバ分析の例は以下を含む。

【０１０２】

（１）（例えば、ＭＤ５アルゴリズムまたはＳＨＡ１アルゴリズムを使用して）交互に並ぶハッシュを計算し、報告されたハッシュを検証して、ハッシュのすべてを記憶する。

（２）サーバ資格証明またはその他の第三者資格証明を用いてコンテンツを認証または署名する。

（３）局所的にまたはもう１つのサーバの問合せを経由して、知られている不良データベース（ブラックリスト）に対してハッシュを調査する。

（４）局所的にまたはもう１つのサーバの問合せを経由して、知られている良いデータベース（ホワイトリスト）に対してハッシュを調査する。

（５）　知られている製品分類データベースに対してハッシュを調査して、ファイルのハッシュに対応する製品（およびその他の情報）を識別する。

（６）（例えば、ＭＩＭＥ添付ファイルとして、ＦＴＰまたはＳＭＴＰによる）ウィルス走査のためにファイルを送信する、または局所的に実行する。

（７）（４）のようにスパイウェア走査のためにファイルを送信する、または局所的に実行する。

（８）（４）のようにサイト特定のカスタム分析のためにファイルを送信する、または局所的に実行する。

（９）ネットワークファイルサーバ（例えば、認証サンバまたはＦＴＰＳ）上の特別な限定ネットワーク・アクセス・サブディレクトリにファイルを送出する。

（１０）新ファイルが分析を必要とするというＳＮＭＰトラップを送信して、それらの位置を特定する。

（１１）新ファイルが分析を必要とするというシスログメッセージまたは電子メールメッセージを送信して、それらの位置を特定する。

（１２）もう１つのシステムがファイルを承認したかまたは非承認したかを決定するためにいくつかのディレクトリを検査する。
（１３）サーバ上でカスタム分析を実行する。
（１４）第１の分析の結果に基づいて調整された第２の分析を自動的に実行する。
（１５）外部分析システムからの分析結果を含む認証ネットワークメッセージを受信する。

【０１０３】
上の分析の結果はサーバ上で要約され、サーバは、メタ情報記憶装置（１２４）内の状態、特に、ホストに対するブロードキャストに関して状態を更新する。サーバは、ファイルが承認されるべきか、または禁止されるべきかについて勧告する。情報は要約されて、その結果、管理者は、１つのウェブブラウザ動作によりファイルのグループを承認または禁止することができる。任意選択で、上の分析からの結果は、ある抗体によりファイルを自動的に承認または禁止するために使用されてよい。サーバは、報告、警告、または別の情報を提供することができ、ホストのすべてまたは１つもしくは複数のグループに関してパラメータのＤ値を変更できる。サーバは、好ましくは、ホストがサーバから更新をプルする方法で、更新を通じて後の配信に関して状態変更を警告する（１３０）。

【０１０４】
抗体分析／承認サービス

システムは、新ファイルに焦点を当てるため、外部委託されたファイル分析サービスは実際的かつ有用にされ得る。これらのサービスは、（例えば、ＳＯＡＰ／ウェブサービス呼出しにより）自動化されてよく、または手動（サービスプロバイダのサーバへの認証リンクに従う）であってもよい。局所的にまたは遠隔サーバを使用してオフサイトで実行されることが可能なこれらのサービスは以下を含んでよい。

【０１０５】
（１）ハッシュを手動で入力して、または事前計算されたウェブリンクに従って、知られている良いデータベースおよび不良データベースの調査の問合せ結果を取得する。企業などの実体は、世界的なホワイトリストまたはブラックリストを維持することを所望する可能性がある。後者はあまりにも多いため、ハッシュに関して役に立たないことになる。様々な企業は、「良い」プログラムに資格を与える、異なるポリシーを有するため、前者は役に立たないことになる。これらのサービスは、下で示されるように、ホワイト／ブラック／グレイリストと投票とを処理する。
（２）特定の抗体に関する抗体（例えば、同じアプリケーションまたは類似のアプリケーションに関連するファイルのグループ）を探索する。
（３）ハッシュに関連するサプライヤとアプリケーションとを識別する。
（４）どれだけ多くの企業とコンピュータとが、どれだけ長い間そのファイルを持っているかを見つけ出す。これらの企業は、名前であると識別されるのではなく、単にカウントされることになる。サービスプロバイダは、このサービスの一環として内密にこの情報を収集することになる。サービスプロバイダは、結果とサービスの二重のブラインド（ｂｌｉｎｄ）データベースを作成する。
（５）どれだけ多くの企業がそのファイルを禁止または承認したか、それらの企業がそれに沿ってどのファイルを承認したかを見つけ出す。この場合も、エンドユーザの観点から、これらはすべてブラインドであり、ハッシュによって行われる。サービスプロバイダは、ファイル名またはファイルデータを収集または記憶する必要はなく、抗体の形でメタ情報を収集するだけである。実際に、ファイル名、および当然、ファイル自体は専有情報とみなされるべきである。
（６）上の問合せの結果に基づく、ならびにサーバ側の分析にも基づく自動化されたサーバ側の承認。

【０１０６】
コンテンツエキストラクタ（ＣＥ）

コンテンツは、通常、コンテンツのグループまたはパッケージを形成する。この例は、

実施可能なプログラムおよびジップファイル内のウィルス、またはＭｉｃｒｏｓｏｆｔＯｆｆｉｃｅ文書内のマクロ（例えば、Ｗｏｒｄ、Ｅｘｃｅｌ、およびＰｏｗｅｒｐｏｉｎｔのファイル）もしくはＭｉｃｒｏｓｏｆｔ　．ｍｓｉファイルなど、インストールパッケージ内のファイルを含む。図８を参照すると、ファイルが受信されて、コンテンツエキストラクタは埋め込まれたコンテンツタイプ（例えば、Ｏｆｆｉｃｅ文書内のマクロ）を探す。コンテンツのかかる「動作」タイプだけが抽出されることが好ましい。

【０１０７】

可能なファイルまたは知られていない状態の修正検出（６００）後に、エキストラクタは、（１つまたは複数の）抽出された部分を取り出し、それらを有効なコンテンツファイルタイプ（例えば、テキストまたは図が伴わないＷｏｒｄ（．ｄｏｃ）ファイル）に変換して、これらを再パッケージ化する。このプロセスは、ステップ６００～６０５として例示される。結果として生じる再パッケージ化されたファイルは、一般に、元のファイル（「コンテナ」）よりもずっと小さく、「縮小」と呼ばれる。縮小のハッシュが計算されて（６０３）、縮小ハッシュはコンテナハッシュと関連付けられる（６０４）。コンテナは入れ子型であってよく、その上、それらの関連性が追跡される。後でコンテンツがアップロードされる必要がある場合、縮小だけがアップロードされる。任意選択で、コンテナファイルとそのメタ情報とは、抽出の分析の結果に基づいてアップロードされることが可能である。ルートコンテナとそれらのメタ情報とは、抽出の分析の結果に基づいてアップロードされ得る。例えば、ファイルｓｅｔｕｐ．ｅｘｅはファイルｍａｉｎ．ｃａｂを含み、ファイルｍａｉｎ．ｃａｂは、ファイルｉｎｓｔａｌｌ．ｅｘｅを含む。ｉｎｓｔａｌｌ．ｅｘｅに関連して、ｍａｉｎ．ｃａｂはｉｎｓｔａｌｌ．ｅｘｅ用の親コンテナであり、ｓｅｔｕｐ．ｅｘｅは、ｉｎｓｔａｌｌ．ｅｘｅ用のルートコンテナならびに、ｍａｉｎ．ｃａｂ用の親コンテナである。これらの関連性はすべて記憶され、好ましくは、個々のファイルのハッシュ間の関係として保存される。

【０１０８】

このプロセスは、ネットワークトラフィックと、分析段階のフットプリントとを削減し、その他のファイルに関連するマクロ（例えば、継承された文書テンプレート）ではなく、埋込みコンテンツだけの追跡を可能にする。これは、マクロらのローディング時にマクロを傍受する方法には当てはまらない。エキストラクタは、場所に依存しない埋込みマクロ検出と追跡とを可能にする。

【０１０９】

その他の有効なファイルタイプとしての縮小の再パッケージ化は、第三者分析システムと互換性があるという利点を有する。例えば、小さいＷｏｒｄ文書として再パッケージ化されたマクロは、電子メールの添付ファイルとしてウィルス走査電子メールゲートウェイに送られることが可能である。もう１つの例は、そのうちの１つだけが動作状態（ｆｏｏ．ｅｘｅ）である５つのファイルを含むジップファイル、ｔｅｍｐ．ｚｉｐである。ｔｅｍｐ．ｚｉｐの縮小は、その中にｆｏｏ．ｅｘｅだけがあるジップファイルｆｏｏ．ｚｉｐであってよく、または縮小は、ｆｏｏ．ｅｘｅ自体であってもよい。ｆｏｏ．ｚｉｐの署名またはｆｏｏ．ｅｘｅの署名は、ｔｅｍｐ．ｚｉｐに対応する署名として関連付けられることが好ましい。縮小は、この場合も、ＡＳ走査電子メールゲートウェイに電子メールで送られることが可能である。いくつかのコンテナは、動作状態のコンテンツを欠いており、したがって、追跡されることができない。縮小の追跡には効率の利点が存在するが、新コンテンツだけを検出および分析するための利点も存在する。このように、より正確な統計、警告、および分析が生み出されことが可能である。ペンディング状態ファイルなどの分類されていないコンテンツの自動的かつ特定の早期検出は、強力なポリシーとコンテンツ管理とを可能にする。

【０１１０】

サーバ・ユーザ・インターフェース

サーバのためのユーザインターフェースは、その各々がシステムの異なる態様の構成と管理とを可能にするいくつかの「パネル」を提供する。このセクションでは、用語「ユー

ザ」は、サーバ・ユーザ・インターフェースへのアクセスを有する管理者を示すために使用される。ユーザインターフェースは、ＳＳＬ暗号化接続を経由して、標準ウェブブラウザを通じてアクセス可能であってよい。サーバの完全性を維持して、特定のユーザの特権水準を決定するために、認証とアクセス制御とが提供される。

【０１１１】

ユーザが初めてシステムにアクセスする場合、ユーザは認証され、この認証に基づいて特権水準を割り当てられる。この特権水準は、ユーザが無制限のアクセスを許可されるか、または読取り専用アクセスを許可されるかを決定する。アクセスのより細かい粒度も提供され得る。ユーザ動作は、ユーザ名と時間とによって追跡および記録される。サーバ上にインストールされた証明書は、ユーザインターフェースへのアクセスの制御および暗号化の両方を行うため、ならびにホストに対する署名およびホストに戻される情報の可能な暗号化を提供するために使用されことが可能である。これらの証明書は、保守パネル内でインストールおよび更新され得る。インターフェースへのすべての入力は、サーバがその構成内で正確な情報をホストに供給していることを確実にするために、適切に確認されるべきである。

【０１１２】

ネットワーク状態インターフェースは、名前および独自の識別子の両方によって識別された、独自のファイル識別子、イベントタイムスタンプ、イベントタイプ、イベント優先順位、ファイルタイプとファイル名、およびホストシステムを含めて、最近のイベントと関連情報とを含む、実行システムの概要を提供する。インターフェースはまた、一定の期間（例えば、最後の１時間、前日）の間のシステムの状態に関する要約情報も提供する。より詳細な情報は、統計パネル内で利用可能である。ここで表示される情報は、検出された多数の新実行可能と、検出された新スクリプトと、新埋込みコンテンツと、非承認ファイルと、感染ファイルとを含む。

【０１１３】

統計パネルは、システムによって収集されたより詳細な統計を表示する。この情報は、様々な期間（例えば、最後の１時間、最後の２４時間、先週）の以下のイベントの数を含む。この情報は、例えば、ネットワーク上で決定された多数の新実行可能と、新スクリプトと、新埋込みコンテンツを有するファイルと、新ウェブファイル（ＨＴＭＬ、ＡＳＰなど）と、手動でまたは走査によってまだ承認されていないファイルと、走査プロセスによって承認されたファイルと、手動でまたは自動承認を経由して承認されたファイルと、走査に失敗したファイルと、ブロックされている、感染していることが知られているファイルと、禁止されてブロックされた実行可能と、初めてインストールされてからサーバによって処理されたイベント全体と、最後の再始動以来のイベントとを含む。

【０１１４】

各範疇に関する統計と共に、ユーザは、サーバによって管理されたすべてのホストを通して各々の最も頻繁に決定されたイベントを浮き彫りにする、項目の「上位１０のリスト」を閲覧することができる。上位１０のリストの例は、いくつのホストがそのファイルの少なくとも１つの複写を有するかのカウントによって並べられた最近探索されたファイルの上位１０を含み、このリストの変形は、独自のハッシュによるカウントと、独自のファイル名によるカウントと、ハッシュによって禁じられたカウントと、名前によって禁じられたカウントと、最近禁じられたカウントと、最近更新／修正されたカウントと、独自のグループ／コンテナ／ルートコンテナ／製品とを含む。上位１０のリストは、ＳＮＭＰを経由して更新および送出される。構成パネルは、上位１０のカウントとその他の更新された変数に基づいて、警告と自動応答とを構成するために使用され得る。警告は、ログ報告と、ＳＮＭＰトラップと、シスログメッセージと、電子メール通知と、その他のネットワークメッセージとを含む。応答は、ファイルの禁止と、ファイルの承認と、１つまたは複数のホストグループ向けのパラメータＤの変更と、１つまたは複数のホストグループ向けのポリシーの変更と、１つまたは複数のホストのホストグループ割当ての変更と、ファイルの分析とを含む。

【０１１５】
統計パネルは、このサーバによってサービス提供されたホストの総数と、動作状態および非動作状態による内訳（非動作状態のホストは、最近サーバに接触していないホストである）と、サーバデータベース内の抗体の総数と、動作可能時間（すなわち、最後の再起動からどれだけ長い間システムが作動しているか）とを含めて、システムに関する全体的な情報も含む。
【０１１６】
このパネル上に表示される統計情報は、ネットワーク管理システムとの統合を可能にして、サーバに対するＳＮＭＰ（簡易ネットワーク管理プロトコル）問合せを経由して利用可能でもある。
【０１１７】
プロットパネルは、ユーザが最近の動作のグラフおよびチャートをプロットおよび印刷することを可能にする。このパネルは、統計パネルと組み合わされてよい。プロット情報は、外部アプリケーション内での表示のためにＸＭＬ形式で利用可能であってもよい。プロットされ得るグラフの例は、最近の期間（分単位で１時間、時間単位で１週間など）に対する動作、または「上位１０のリスト」のグラフ表示を含む。
【０１１８】
サーバによって維持される統計情報に関する制約により、利用可能な様々なプロットに関して何らかの制限が存在する場合がある。管理者がＳＮＭＰ管理システムを使用している場合、そのシステムも組織内ですでに使用中の形で統計プロットを提供することが可能な場合がある。
【０１１９】
抗体データベースパネルは、ユーザがサーバ上に記憶された抗体データベースと直接的に相互作用することを可能にする。データベースのコンテンツが表示されて、ユーザは異なる基準によって表示を選択もしくは分類することができ、またはフィルタパターンを選択することによって表示を制限することができる。ユーザは、抗体自体と相互作用することも可能である。これらの動作は下で説明される。
【０１２０】
サーバは、メイン抗体データベース内で要求されないフィールドを含む、補助的情報データベースを使用することも可能である。このデータベース内のフィールドの例は、決定された第１のファイル名または初期ファイルクラスであってよい。
【０１２１】
各ファイルに関して、以下の情報がこのパネル上に表示される。
・初めて参照された時間。ファイルまたはハッシュがホストによって初めて参照され、サーバに報告されたとき。
・ファイルＩＤ。ＭＤ５、ＳＨＡ－１、およびＯＭＡＣなど、コンテンツの１つまたは複数のハッシュを含めて、ファイルに関する独自の識別子。
・ファイルタイプ。ファイルクラス（例えば、実行可能、スクリプト、オフィス文書、アーカイブなど）。これは、初めて参照されたファイル名から、およびファイルコンテンツの分析から導出される。
・状況／状態。承認、ペンディング、または禁止を含めて、現在のファイル状況。
・方法。サーバがファイルについて学ぶ方法（自動、手動など）。
・ファイル名。初めて参照されて、サーバに報告されたファイルの名前。これはファイルの現在の名前でなく、ネットワーク上で決定された初めての事例の正に名前である可能性がある。
・ファイル経路。初めて参照されて、サーバに報告されたファイルの経路。
・初めて参照されたホスト。その上でファイルまたはハッシュが初めて参照および報告されたホストの名前。
・分析結果。最後の走査またはその他の分析の結果。
・最初の分析。ファイルの最初の走査／分析の時間。

・最後の分析。ファイルが最後に走査／分析された時間。
・最後の更新。ファイル状態が最後に変更された時間。
・親コンテナ。ファイルに関連したその他のファイルへのリンク。
・親コンテナ属性。ファイル名、初めに決定された時間、初めに決定されたホスト、ファイル経路、製品分類、および１つの関連するコンテナファイルの状態。
・ルートコンテナ。ファイルに関連したその他のファイルへのリンク。ルートコンテナは、もう１つのコンテナ内に含まれないコンテナである。
・ルートコンテナ属性。ファイル名、初めに決定された時間、初めに決定されたホスト、ファイル経路、製品分類、および１つの関連するルートコンテナファイルの状態。
以下の動作は、リストから選択されたファイルに関して実行され得る。
・ファイル詳細。これは、ファイルを承認または禁じたインターフェースユーザと、どこでファイルが初めて参照されたかと、ユーザによって加えられた任意の注釈とを含めて、抗体・データベースからファイルに関する追加の情報を提供する。
・承認。現在選択されたファイルを明示的に承認する。このオプションは、すべてのホストを通してファイルを承認することになるため、このオプションはユーザに十分な警告を提供すべきである。
・非承認。好ましくは、状態をペンディングに遷移して、すでに承認されているファイルを明示的に非承認する
・禁止。ファイルを明示的に禁止する。これはすべてのホスト上でファイルを禁止させる。
・分析／ウィルス走査。選択されたファイルに関して分析／走査のスケジューリングを強要する。
・削除。このファイルに関する情報を除去する。これは次に決定されたときに、サーバに新しいものとしてファイルを扱わせることになる。
・ホスト上のファイルの探索。この動作は、ファイルファインダに連結し、入力されると、選択されたファイル名を提供する。
・コンテナの探索。ファイルに関する可能なコンテナと、それらのコンテナに関する情報とを調査する。
・ルートコンテナの探索。ファイルに関する可能なルートコンテナと、それらのコンテナに関する情報とを調査する。
・ウェブサービス情報の探索。ファイルおよび／またはそのコンテナ／製品に関する追加の情報を見つけ出すために様々なその他のネットワークサーバに問い合わせる。

【０１２２】
ファイル・ファインダ・パネルは、ユーザが管理されたすべてのホスト上の特定のファイルの位置を探索する最善努力式のプロセスを開始することを可能にする。このプロセスは、時間がかかる可能性があるため、ユーザは新しい探索を開始する前に通知されることになる。ファイルファインダは、製品のすべてのバージョンで実施されなくてもよい。ファイル探索の進度は、問合せの部分完成の間に報告されてよい。

【０１２３】
プロセスは、特定の１つまたは複数のファイルを選択することによって抗体データベースパネル（セクション０を参照）から開始されてもよく、次いで、適切な情報を自動的に記入することにより、ユーザをファイル・ファインダ・パネルに導く。

【０１２４】
このプロセスは、サーバと通信しているすべてのホストが非同期的に状態を戻すことを要求し、したがって、パネルは結果が受信されるとその結果を動的に表示するために新しいビューを開くことになる。ユーザがもう１つの探索を開始する場合、現在の探索は終了されることになる。複数のファイル探索は、将来のバージョンで可能にされ得る。

【０１２５】
ホストグループパネルは、サーバによって知られているホストが特定の論理グループと関連付けられることを可能にする。全面的なグループ機能性は、インターフェースの初期

バージョンで利用可能でない可能性があり、その場合、このスクリーンはこのサーバによってサポートされる単一のグループに関する情報を表示することになる。

【０１２６】

パネルは、以下を含めて、グループメンバーシップを操作することをサポートする。

・新しいグループの追加。

・既存のグループの除去。グループが除去される場合、ホストはサーバのデータベースから除去されないが、規定のグループに再度割り当てられる。

・ホストを１つのグループからもう１つのグループに移動する。

【０１２７】

各ホストに関して、以下の情報がこのパネル上で表示される。

・ホスト。ホストのＤＮＳ名。

・独自のＩＤ。ホストの独自の識別子。

・ＩＰアドレス。このホストの最後の知られているＩＰアドレス。

・状態。ホストのオンライン状態。

・最後に参照されたとき。最後にホストがサーバにチェックインしたとき。

・オペレーティングシステム。ホストのオペレーティングシステムのバージョン。

・バージョン。ホスト上のオペレーティングシステムのバージョン。

【０１２８】

ファイル・クラス・パネルは、各クラスにマップされるファイル拡張子の閲覧および編集を可能にする。下記のように、いくつかのクラスは、拡張子によって定義される。その他のクラスは、コンテンツの分析によって決定される。いくつかのクラスは、拡張子および分析の両方によって決定される。これらの拡張子は、読取り専用である。

【０１２９】

いくつかの事前定義された拡張子クラスは、

・実行可能。ｅｘｅ、ｃｏｍ、ｄｌｌ、ｐｉｆ、ｓｃｒ、ｄｒｖ、およびｏｃｘを含む拡張子。

・スクリプト。ｖｂｓ、ｂａｔ、およびｃｍｄを含む拡張子。

・埋込みマクロコンテンツ。ｄｏｃ、ｄｏｔ、ｘｌｓ、ｘｌａ、ｘｌｔ、ｘｌｗ、ｐｐｔ、ｐｐｓ、およびｐｏｔを含む拡張子。

・ウェブコンテンツ。ｈｔｍ、ｈｔｍｌ、ａｓｐ、およびｃｇｉを含む拡張子。

【０１３０】

ポリシーパネルは、サーバの構成の中心である。ユーザは、ホストグループによってグループ化された、すべての管理ホスト上で強要されるポリシーを表示および編集することができる。このパネルは、現在選択されたグループに関して現在の世界的なＤ設定も表示する。

【０１３１】

この選択は、ユーザが現在選択されたグループに関して世界的なＤ水準を定義することを可能にする。新しいＤ水準が選択される場合、変更は速やかに適用されないが、明示的に選択されなければならない。提案された新しいＤ水準を選択することは、ポリシー情報および動作の表示を変更し、この新しい水準に関してポリシー情報と動作とを示す。パネルから離れて移動することは、それらの変更を適用しないことになる。

【０１３２】

ポリシーリストは、特定のファイルクラス（例えば、実行可能、スクリプトなど）に関して特定のＤ水準の様々な動作と効果を表示する。ポリシーは、動作可能にされることも動作不可能にされることも可能であるが、編集されることはできない。以下のポリシーがリスト上に含まれる。

【０１３３】

・新実行可能

・新独立型スクリプト

・新埋込みスクリプト

・新ウェブコンテンツ
・非承認ファイル
・更新エージェントを無視（一定の更新ソース／プロセス／位置からの新コンテンツを自動的に承認）
・ウィルス／スパイウェア感染ファイル
【０１３４】
ポリシーが動作不能にされるときはいつでも、そのクラスのファイルの追跡は依然として続くが、影響を受けたホストシステムによって何の処置も取られない。
各ポリシーに関して、動作グリッドが表示される。グリッドは、どのポリシー設定が現在選択されたＤ水準で適用されるかを表示する。
【０１３５】
・動作
・実施ブロック。このファイルクラスの実施はブロックされることになるか。
・書込みブロック。このファイルクラスのファイルへの書込みはブロックされることになるか。この設定は、ウェブコンテンツおよび非承認ファイルだけに使用される。この設定は、厳重に制御されたシステムだけに使用され、通常の動作には使用されない。
・隔離。このクラスのファイルは隔離されるか。ファイルは、個々のディレクトリに移すのではなく、読取りをブロックすることによって隔離されることが可能である。ウィルス感染ファイルの場合、これらは書き込まれてよいが、後に削除される。しかし、この機能性は、当初実施されなくてもよい。
・記録。このクラスのファイルへのアクセスは記録されることになるか。
・承認
・暗黙的な承認。ファイルはこのＤ水準で暗黙的に承認されることになるか。暗黙的な承認は、適切な走査および待ち時間の後にファイルの承認状態を変更する。
・明示的な承認。ファイルはこのＤ水準で明示的に承認されることになるか。
【０１３６】
上で例示されたものに類似した動作グリッドは、ユーザに、予め作られたポリシーと組み合わせて特定Ｄ水準の効果の表現を示す。下の表は、様々なＤ水準（ゼロから７）で動作と予め作られたポリシーの組合せの例を示す。
【０１３７】
通知パラメータ
コンテンツアクセスがブロックされる場合、ホストユーザは通知される。リスト上の各ポリシーに関して、および各ホストグループに関して、以下の設定が利用可能である。
・表示されたメッセージ。ユーザ・インターフェース・ダイアログ上に表示されたテキスト。複数のメッセージがリストボックス内に挙げられる。
・ボタンテキスト。ユーザ・インターフェース・ダイアログ上の単一ボタン上に表示されるテキスト。
・タイムアウト。ダイアログはどのくらい長くユーザに表示されることになるか。ユーザによって受け入れられるまで、ゼロのタイムアウトは示し、ダイアログは無期限に表示し続ける。
・任意選択で、Ｄの一定値に関して、一時期、コンテンツ制限を取り消すためのボタン。
・ポリシーに関してより多くの情報を有するＵＲＬリンク。
【０１３８】
通知パラメータは、通知メッセージと共にホストで表示される画像を定義する世界的な設定も含む。これらの設定は、予め作られた個々のポリシーの各々に関して構成可能である。通知パラメータは、サーバ管理インターフェース内で編集される。それらのパラメータは、ポリシーと関連付けられ、ポリシーはホストグループに割り当てられて、ポリシーが変更するとホストに伝播される。
【０１３９】
年齢走査パラメータ

このセクションは、ユーザが、ファイルが初めて参照されて承認（自動承認走査）される時間と、第２の（承認）走査が実行される時間および第３の（繰返し）走査が発生する時間の間の時間を構成することを可能にする。より多い走査と時間とは、図７で特定されることができる。

【０１４０】

保守

保守セクションは、ユーザがサーバ自体に関して世界的な設定を構成することを可能にする。

・システム構成。局所ネットワークおよびホストシステムとのサーバの相互作用に関する設定。

・ＩＰアドレスおよびサブネットマスク。サブネットマスクは、ホストの遠隔タイプと局所タイプへの分類を可能にする。遠隔ホストは、帯域幅を保存するためにより制限された通信を有する。ホストグループは、各接続タイプ、すなわち、遠隔、局所、または切断に関して特定される、異なるポリシーセットとＤパラメータ設定とを有する可能性ある。遠隔ホストは、より少ないネットワークトラフィック（例えば、より少ないサーバ報告書）を生成することになる。また遠隔ホストは、サーバに新コンテンツのハッシュを報告するが、コンテンツをアップロードしないことが好ましい。

【０１４１】

・ＩＰ経路指定情報。

・パスワード。サーバインターフェースへのアクセスのための設定パスワードまたは再設定パスワード。

・証明書。リムーバブル媒体（および、任意選択で、ネットワーク）から証明書をインストールする。これらは、サーバの識別性を検証するため、およびサーバに対するＳＳＬインターフェースのためにユーザによって使用される。

・ＳＮＭＰ。トラップを受信して、サーバの構成を問い合わせることが可能にされるようにＳＭＭＰサーバのリストを設定する。

・ＳＮＭＰトラップ選択。どのイベントタイプが、どのトラップを引き起こすか、どのＳＮＭＰサーバに対してトラップが送られることになるか（および優先順位が重要、高い、中間、低い、情報など）を選択する。

・シスログ。様々なイベントタイプと優先順位に関してシスログを経由して記録情報を受信するためにサーバのリストを設定する。

・ＮＴＰ時間同期化サーバ。時間同期化に関してサーバのリストを設定する。サーバ上の時間は、起動時にその内部クロックから取得され、次いで、この外部ＮＴＰ時間ソースにより同期化される。サーバ時間からのホスト偏差は、サーバによって追跡されることになる。

【０１４２】

・システム状態（サーバ）

・動作可能時間。最後のシステム再起動からの時間を表示する。

・ソフトウェアバージョン。サーバソフトウェアに関するバージョン情報を表示する。

・ディスク領域。サーバに関してローカルディスクと記憶統計とを表示する。

【０１４３】

・ウィルス／スパイウェア署名更新

・最後の署名の更新。最後の署名更新の時間。

・サービス構成の更新。ダウンロード場所とスケジュールとを含めて、インストールされたアンチウィルスソフトウェア向けの更新サービスを構成する。

・スキャナの更新。ウィルス・スキャナ・ソフトウェアを更新する。

・署名更新。ウィルス署名の更新を強要する。

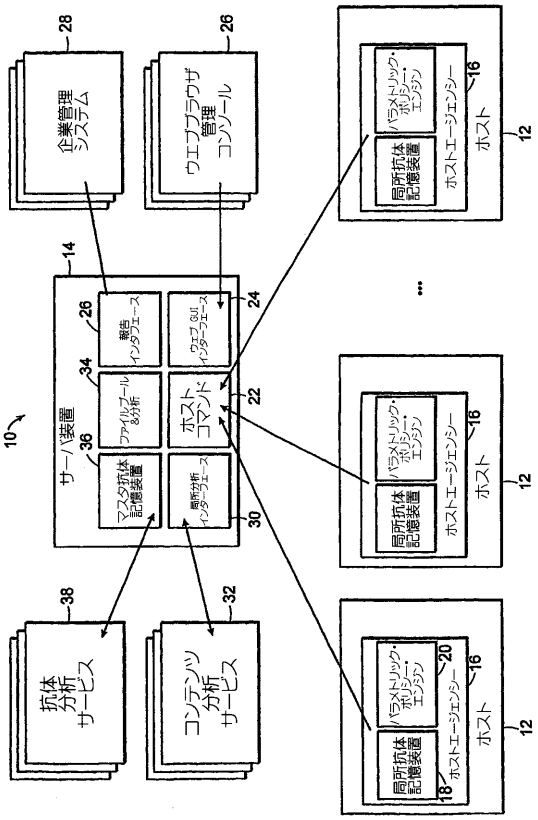
【０１４４】

・サーバソフトウェア更新

・現在のバージョン。現在のサーバソフトウェアバージョンを表示する。

・再起動。現在インストールされている画像を使用してサーバを再起動する。
・新画像のロード。リムーバブル媒体またはネットワーク（例えば、ＦＴＰ）から新ソフトウェア画像をサーバにロードする。
・先のバージョンへの復帰。予め使用されたソフトウェア画像に復帰する。
【０１４５】
・外部サービス構成
・コンテンツ走査システム向けのネットワークアドレス、サービスタイプ、および承認権限。
・メタ情報共有サービス向けのネットワークアドレス、サービスタイプ、および承認権限。
・外部コンテンツ転送向けおよびユーザ定義された分析向けの外部ファイルサーバアドレス、プロトコル、ログイン、およびディレクトリ。
・ＳＮＭＰ、シスログ、電子メール、および新コンテンツのＳＯＡＰ通知のための外部コンテンツ通知サービス構成。
【０１４６】
・バックアップ。リムーバブル媒体への（およびネットワークへの）構成のバックアップおよび回復。
・構成とデータベースの保存。（例えば、ＸＭＬを経由して）構成と抗体・データベースとを保存する。
・構成とデータベースのロード。（例えば、ＸＭＬで）構成と抗体・データベースとをロードする。
【０１４７】
サーバは、プログラム式マイクロプロセッサ、デジタル信号処理装置（ＤＳＰ）、または特定用途向け処理およびメモリなどの処理能力を含む。ホストは、パーソナルコンピュータもしくは類似コンピュータ、またはハンドヘルド、ＰＤＡ、もしくはネットワーク上のその他のデバイスを含めて、その他の処理デバイスを含んでよい。
【０１４８】
本明細書で発明の実施形態を説明することにより、主張される本発明の範囲から逸脱せずに、修正形態が行われ得ることが明らかであろう。
【図面の簡単な説明】
【０１４９】
【図１】本明細書で説明されるセキュリティシステムの概要を示すブロック図である。
【図２】図２Ａ、図２Ｂ、図２Ｃの配置図である。
【図２Ａ】図１のシステムの構成要素を示すより詳細なブロック図である。
【図２Ｂ】図１のシステムの構成要素を示すより詳細なブロック図である。
【図２Ｃ】図１のシステムの構成要素を示すより詳細なブロック図である。
【図３】図３Ａ、図３Ｂの配置図である。
【図３Ａ】分析を実行するためのプロセスを例示する流れ図である。
【図３Ｂ】分析を実行するためのプロセスを例示する流れ図である。
【図４】システムによって実行されるプロセスの概略図である。
【図５】システムによって実行されるプロセスの概略図である。
【図６】時間設定された分析の例を示すチャートである。
【図７】時間設定された分析の間に実行されるステップの流れ図である。
【図８】コンテンツ抽出プロセスの概略図である。

【図１】



【図２】

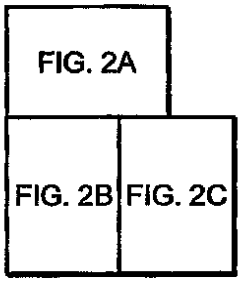
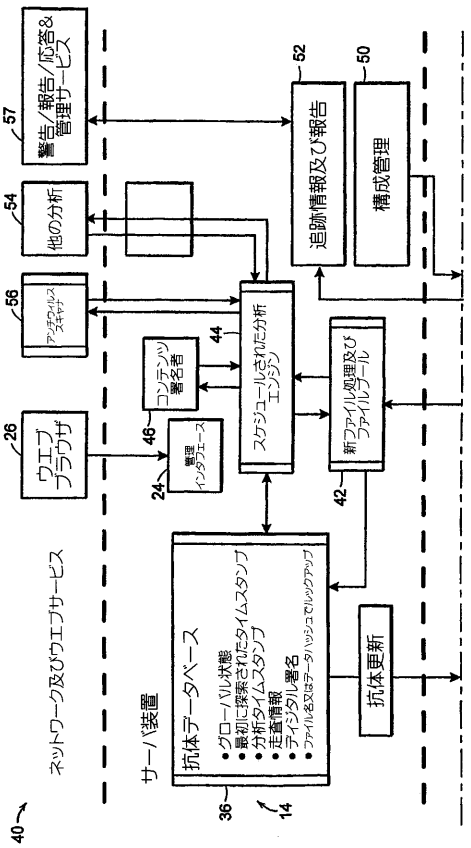
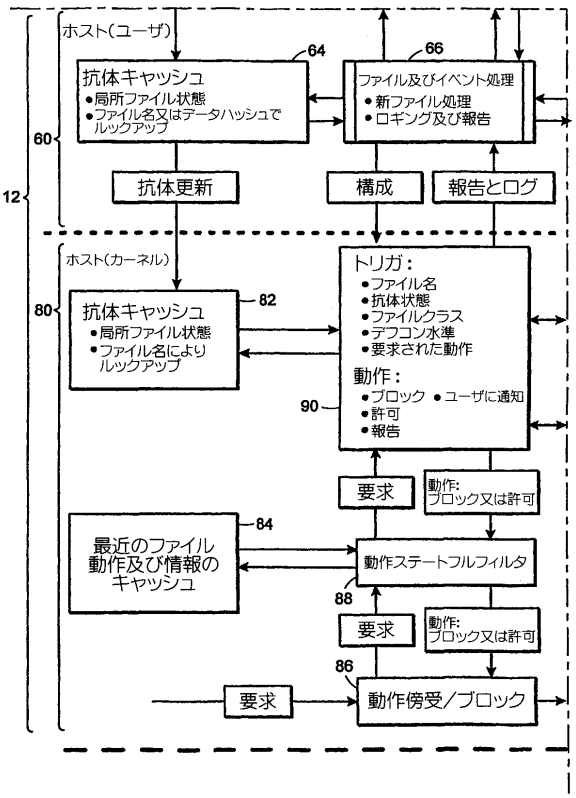


FIG. 2

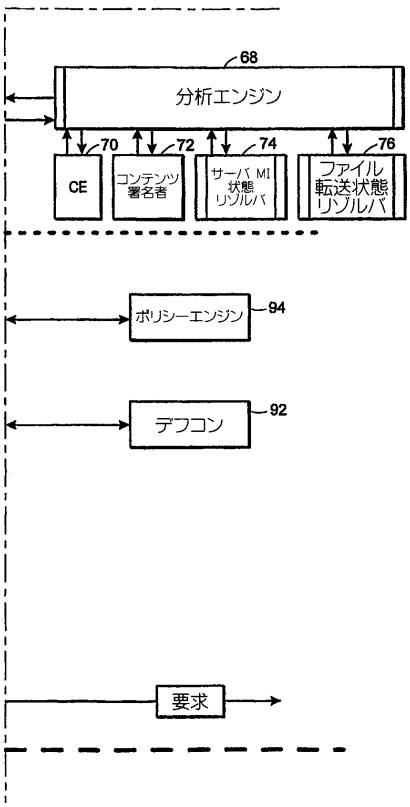
【図２Ａ】



【図２Ｂ】



【図２Ｃ】



【図３】

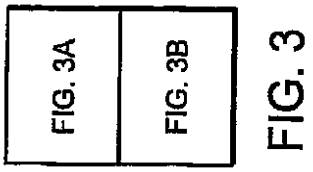
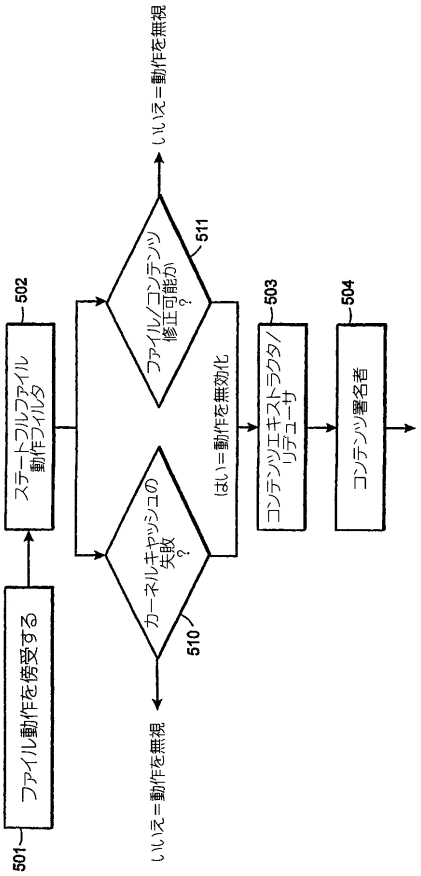
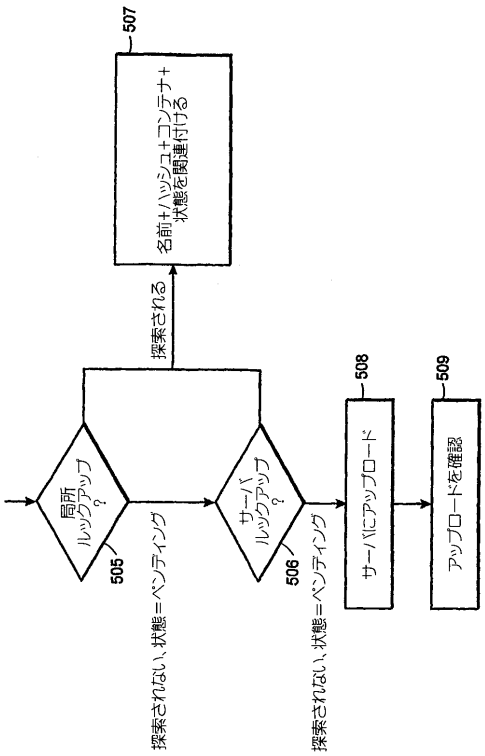


FIG. 3

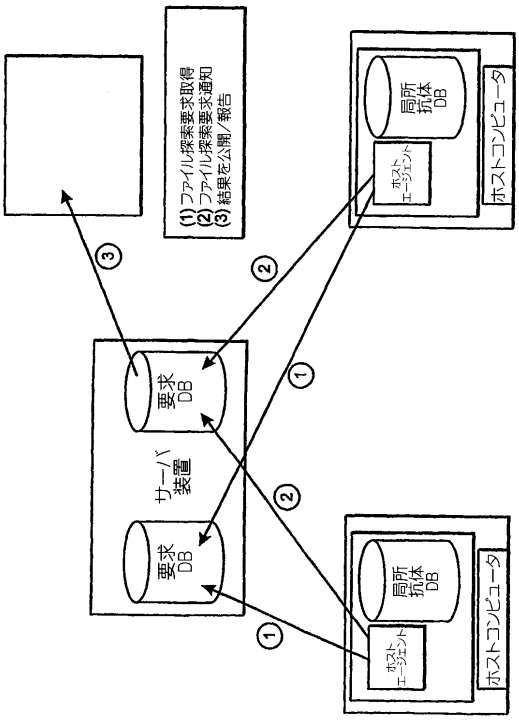
【図３Ａ】



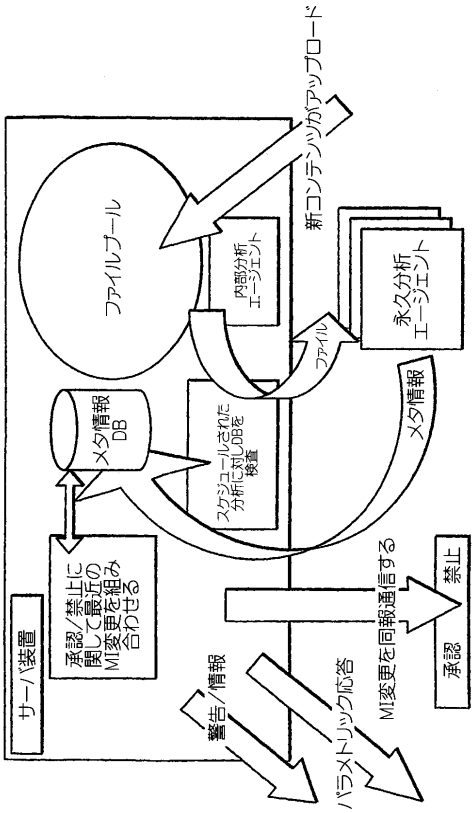
【図３Ｂ】



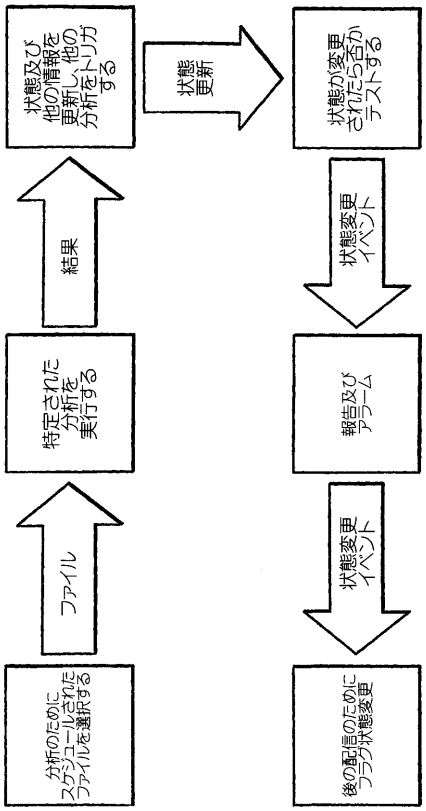
【図４】



【図５】



【図６】

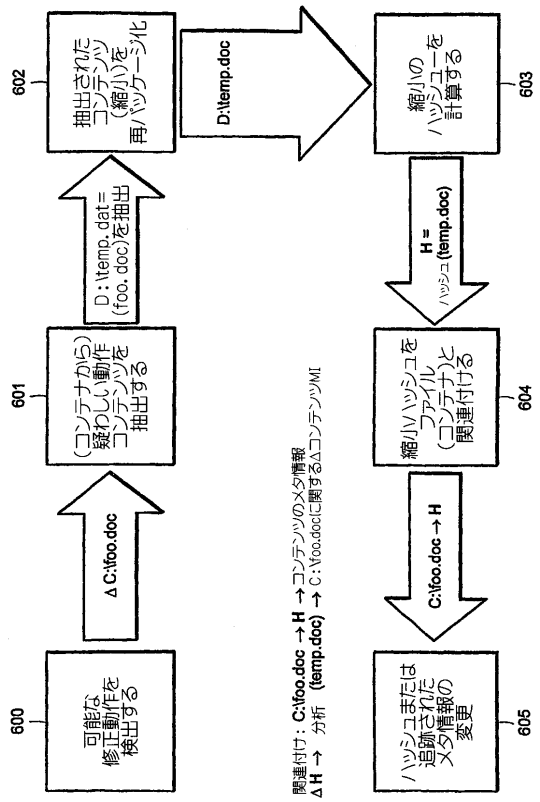


【図７】

$\Delta t = t_{current} - t_{the\_first\_seen\_on\_network}$

Δt=0	Δt=12 時間	Δt=2 日	Δt=30 日	
ハッシュ証明				
AV 走査 #1 AV 走査 #2	AV 走査 #1 AV 走査 #2	AV 走査 #1 AV 走査 #2	AV 走査 #1 AV 走査 #2	
AS 走査 #1 AS 走査 #2	AS 走査 #1 AS 走査 #2	AS 走査 #1 AS 走査 #2	AS 走査 #1 AS 走査 #2	
その他の分析 #1 (新を分析)		その他の分析 #2 (永続を分析)		その他の分析 #2 (永続を分析)

【図８】


600
可能な修正動作を検出する
Δ C:\foo.doc
601
(コンテナから)疑わしい動作コンテンツを抽出する
D:\temp.dat = (foo.doc)を抽出
602
抽出されたコンテンツ(縮小)を再パッケージ化
D:\temp.doc
603
縮小のハッシュを計算する
H = ハッシュ(temp.doc)
604
縮小ハッシュをファイル(コンテナ)と関連付ける
C:\foo.doc → H
605
ハッシュまたは追跡された メタ情報の変更
関連付け：C:\foo.doc → H →コンテンツのメタ情報
ΔH → 分析 (temp.doc) → C:\foo.docに関するΔコンテンツMI

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	G06F 12/14 560C	

(31)優先権主張番号 11/193,291
(32)優先日 平成17年7月29日(2005.7.29)
(33)優先権主張国 米国(US)
(31)優先権主張番号 11/194,078
(32)優先日 平成17年7月29日(2005.7.29)
(33)優先権主張国 米国(US)

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100107696
弁理士 西山 文俊
(72)発明者 ブレナン，トッド・エフ
アメリカ合衆国マサチューセッツ州０２４１３，サマヴィル，ビーコン・ストリート ９
(72)発明者 ヒラリー，アレン
アメリカ合衆国テキサス州７７０３０，ヒューストン，シェイクスピア ２５１５ ナンバー３
(72)発明者 ハンラティ，ジョン
アメリカ合衆国マサチューセッツ州０２１４０，ケンブリッジ，マウント・ヴァーノン・ストリート １５ ナンバー７

Ｆターム(参考) 5B017 AA02 AA08 BA09 CA01 CA16
5B276 FD08 FD09
5B285 AA05 BA03 CA36 CA38
5J104 AA08 AA16 AA26 EA08 LA05 NA12 NA38 PA07