(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6053808号
(P6053808)

(45)発行日　平成28年12月27日(2016.12.27)　(24)登録日　平成28年12月9日(2016.12.9)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/62	345
G06F 12/00	(2006.01)	G06F	12/00	537A
G06F 21/10	(2013.01)	G06F	12/00	514M
		G06F	21/10	350

請求項の数 10　(全 21 頁)

(21)出願番号	特願2014-540051 (P2014-540051)
(86)(22)出願日	平成24年10月31日 (2012.10.31)
(65)公表番号	特表2015-501497 (P2015-501497A)
(43)公表日	平成27年1月15日 (2015.1.15)
(86)国際出願番号	PCT/US2012/062881
(87)国際公開番号	WO2013/067066
(87)国際公開日	平成25年5月10日 (2013.5.10)
審査請求日	平成27年10月29日 (2015.10.29)
(31)優先権主張番号	13/286,219
(32)優先日	平成23年11月1日 (2011.11.1)
(33)優先権主張国	米国(US)

(73)特許権者　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　98052　レッドモンド　ワン　マイクロソフト　ウェイ
(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　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修

最終頁に続く

(54)【発明の名称】セキュリティ・トリミングのためのインテリジェントなキャッシング

(57)【特許請求の範囲】

【請求項１】

サーバーにおいて、前記サーバー上のコンテンツにアクセスするための第１の要求をユーザーから受け取るステップと、

セキュリティ・データーストアから、前記受け取られた第１の要求に応答して前記要求されたコンテンツにアクセスするための前記ユーザーのアクセス特権の値を取得するステップと、

前記要求されたコンテンツにアクセスするための前記ユーザーの前記取得されたアクセス特権の値と、前記コンテンツにアクセスするための前記ユーザーの前記アクセス特権の値を受信した時刻に関連する１または複数のパラメーターとを、前記サーバー上のキャッシュに格納するステップであって、前記パラメーターの１つは、前記コンテンツに対する前記アクセス特権の値についての有効期限（ＴＴＬ）である、ステップと、

前記コンテンツにアクセスするための前記ユーザーの前記受信されたアクセス特権の値が所定の前の時間期間において肯定的である回数に基づいて、前記ＴＴＬの時間の長さを調整するステップと、

前記サーバーにおいて、前記サーバー上の前記コンテンツにアクセスするための第２の要求を前記ユーザーから受け取るステップと、

前記第２の要求を受け取ることに応答して、前記サーバーにおいて、前記コンテンツにアクセスするための前記ユーザーの前記アクセス特権の値についての前記ＴＴＬの値を評価して、前記コンテンツにアクセスするための前記ユーザーの前記格納されたアクセス特

権の値の有効性を判断するステップと、
前記コンテンツにアクセスするための前記ユーザーの前記格納されたアクセス特権の値が有効であると判断したときに、前記ユーザーが前記サーバー上の前記コンテンツにアクセスすることを可能にするステップと、
を含む方法。
【請求項２】
前記コンテンツに対する前記格納されたアクセス特権の値が無効であると判断したときに、前記コンテンツに対する更新されたアクセス特権の値を求める要求をセキュリティ・データーストアへ送るステップと、
前記コンテンツに対する前記更新されたアクセス特権の値を受け取るステップと、
前記要求に応答して、前記コンテンツに対する前記更新されたアクセス特権の値を伝達するステップと、
を更に含む、請求項１に記載の方法。
【請求項３】
前記コンテンツに対する前記格納されたアクセス特権の値を前記コンテンツに対する前記更新されたアクセス特権の値で更新するステップと、
前記コンテンツに対する前記アクセス特権の値を受信した時刻に関連する前記１または複数のパラメーターを更新するステップと、
を更に含む、請求項２に記載の方法。
【請求項４】
前記１または複数のパラメーターは、前記コンテンツに対する前記アクセス特権の値が最後に受信された時刻を含む、請求項１に記載の方法。
【請求項５】
前記セキュリティ・データーストアに要求を送るステップは、多数のセキュリティ・データーストアに要求を送るステップを更に含む、請求項２に記載の方法。
【請求項６】
コンピューター・システム上の計算プロセッサーによって実行された時に、前記計算プロセッサーにコンピューター・プロセスを実施させるコンピューター実行可能命令をエンコードした１または複数のコンピューター読み取り可能記憶デバイスであって、前記コンピューター・プロセスは、
前記コンピューター・システム上のコンテンツにアクセスするための第１の要求をユーザーから受け取るステップと、
セキュリティ・データーストアから、前記受け取られた第１の要求に応答して前記要求されたコンテンツにアクセスするための前記ユーザーのアクセス特権の値を取得するステップと、
前記要求されたコンテンツにアクセスするための前記ユーザーの前記取得されたアクセス特権の値と、前記コンテンツにアクセスするための前記ユーザーの前記アクセス特権の値に関連する１または複数のパラメーターとを、キャッシュに格納するステップであって、前記パラメーターの１つは、前記コンテンツに対する前記アクセス特権の値についての有効期限（ＴＴＬ）である、ステップと、
前記コンテンツにアクセスするための前記ユーザーの前記受信されたアクセス特権の値が所定の前の時間期間において肯定的である回数に基づいて、前記ＴＴＬの時間の長さを調整するステップと、
その後、前記サーバー上の前記コンテンツにアクセスするための第２の要求を前記ユーザーから受け取るステップと、
前記第２の要求を受け取ることに応答して、
前記コンテンツにアクセスするための前記ユーザーの前記アクセス特権の値に関連する、前記キャッシュに格納された前記ＴＴＬの値の評価を実施するステップと、
前記実施された評価に基づいて、前記コンテンツにアクセスするための前記ユーザーの前記格納されたアクセス特権の値の有効性を判断するステップと、

を含む、コンピューター読み取り可能記憶デバイス。
【請求項７】
計算プロセッサーと、命令を収容したメモリーとを有する計算システムであって、前記命令は、前記計算プロセッサーによって実行されると、前記計算プロセッサーに、
前記計算システムにおいて、あるコンテンツにアクセスするための第１の要求をユーザーから受け取るステップと、
セキュリティ・データーストアから、前記受け取られた第１の要求に応答して前記要求されたコンテンツにアクセスするための前記ユーザーのアクセス特権の値を取得するステップと、
前記要求されたコンテンツにアクセスするための前記ユーザーの前記取得されたアクセス特権の値と、前記コンテンツにアクセスするための前記ユーザーの前記アクセス特権の値を受信した時刻に関連する１または複数のパラメーターとを、前記計算システム上のキャッシュに格納するステップであって、前記パラメーターの１つは、前記コンテンツに対する前記アクセス特権の値についての有効期限（ＴＴＬ）である、ステップと、
前記セキュリティ・データーストアへの１または複数の以前の要求と、対応する取得された前記アクセス特権の値との履歴に基づいて、前記ＴＴＬの時間の長さを調整するステップと、
前記サーバーにおいて、前記コンテンツにアクセスするための第２の要求を前記ユーザーから受け取るステップと、
前記第２の要求を受け取ることに応答して、前記コンテンツにアクセスするための前記ユーザーの前記アクセス特権の値に関連する前記ＴＴＬの値に基づいて、前記キャッシュに格納されている前記ユーザーの前記アクセス特権の値の有効性を判断するステップと、
前記コンテンツにアクセスするための前記ユーザーの前記格納されたアクセス特権の値が有効であると判断することに応答して、前記ユーザーが前記コンテンツにアクセスすることを可能にするステップと、
を含むプロセスを実施させる、計算システム。
【請求項８】
前記コンテンツに対する前記アクセス特権の値に関連する前記１または複数のパラメーターは、前記要求されたコンテンツに対する前記アクセス特権の値を受信した時刻に関連する１または複数のパラメーターを含む、請求項７に記載の計算システム。
【請求項９】
前記１または複数のパラメーターは、前記要求されたコンテンツに対する前記アクセス特権の値が最後に受信された時刻を含む、請求項７に記載の計算システム。
【請求項１０】
前記計算プロセッサーによって実施される前記プロセスは、前記要求されたコンテンツに対する受信された前記アクセス特権の値が失敗値または不確定値のうちの少なくとも１つを示すことに応答して、次の要求が前記セキュリティ・データーストアへ送信される前の時間を示す要求カウンタまでの時間を更新するステップを更に含む、請求項７に記載の計算システム。
【発明の詳細な説明】
【背景技術】
【０００１】
[0001] インターネットおよびウェブは、コンテンツ供給者が彼らの顧客、パートナー、または他のユーザーと大量の情報を共有することを可能にする。例えば、医療(healthcare)供給者は、当の医療供給者によって提供されるサービス、種々の病気についての包括的情報、患者の予約についての日程計画情報等について、彼らの顧客と情報を共有する。通例、このような医療情報は、１つのデーターストアまたはサーバー上にホストされるデーターストアの集合体に格納される。ユーザーは、このような情報に、種々のアプリケーション、ウェブ・ブラウザー等を用いてアクセスすることができる。例えば、ユーザーが、医療供給者によって提供されるウェブサイトにログオンして、このような情報を見るこ

とができる。しかしながら、ユーザーが、種々のレベルのアクセス特権がある情報を含む文書またはコンテンツにアクセスしているとき、このユーザーがアクセス特権を有するコンテンツのみがこのユーザーに提供されることを判定する必要がある。例えば、患者が医療供給者からの医療情報にアクセスしているとき、この患者の予約およびその予約の理由、またはこの患者の予約に対する参照だけが、この患者に示されるのでなければならない。大量の情報が、医療情報供給者の患者のようなエンド・ユーザーに提供され、大量のソースにこのような情報およびその特権が格納されることを想定すると、ユーザーには特権情報(privileged information)のみが開示されることを確保することが課題となる。

【発明の概要】

【０００２】

[0002] 本明細書において記載し特許請求する実施態様は、セキュリティ・データーストアから受信されるセキュリティ・トリミング情報のインテリジェントなキャッシングを用いるセキュリティ・トリミング・システムを提供することによって、以上で述べた問題に取り組む。アクセス・キャッシュは、アクセス・データーストアから受信したセキュリティ・トリミング情報を、セキュリティ・トリミング情報の有効期限（ＴＴＬ：time to live）、セキュリティ・トリミング情報を求める要求の回数等というような、このようなセキュリティ・トリミング情報に関連する他のパラメーターと共に格納する。その後、セキュリティ・トリミング情報を求める要求に応答して、アクセス・キャッシュは、セキュリティ・トリミング情報のキャッシュされた値を、他の関連するパラメーターと共に用いて、コンテンツ供給者からの要求に対する応答を決定する。例えば、セキュリティ・トリミング情報に関連するＴＴＬが有効である場合、このようなセキュリティ・トリミング情報が、要求に対する応答において用いられる。そうでない場合、セキュリティ・トリミング情報の更新値を求める新たな要求がセキュリティ・データーストアに送られる。

【０００３】

[0003] 実施態様の中には、製造品目がコンピューター・プログラム生産物として提供される場合もある。コンピューター・プログラム生産物の一実施態様は、計算システムによって読み取り可能であり、プロセッサー実行可能プログラムをエンコードする有形コンピューター・プログラム記憶媒体を提供する。他の実施態様についても、本明細書において説明し、特許請求の範囲に記載する。

【０００４】

[0004] この摘要は、詳細な説明において以下で更に説明する概念から選択したものを、簡略化した形態で紹介するために設けられている。この摘要は、特許請求する主題の主要な特徴や必須の特徴を特定することを意図するのではなく、特許請求する主題の範囲を限定するために用いられることを意図するのでもない。

【図面の簡単な説明】

【０００５】

【図１】図１は、セキュリティ・トリミング・システムについてのデーター・ソースおよびフローの例を示す。

【図２】図２は、セキュリティ・トリミング・システムについてのデーター・ソースおよびフローの代替例を示す。

【図３】図３は、本明細書において開示するセキュリティ・トリミング・システムの動作例を示す。

【図４】図４は、本明細書において開示するセキュリティ・トリミング・システムの代替動作例を示す。

【図５】図５は、本明細書において開示するセキュリティ・トリミング・システムの使用例を示す。

【図６】図６は、説明する技術を実現するときに有用であると考えられるシステム例を示す。

【発明を実施するための形態】

【０００６】

[0012] 本明細書において説明するセキュリティ・トリミング・システムは、医療サービス供給者のような、コンテンツ供給者が、コンテンツに対してアクセス特権を有するユーザーだけにそのコンテンツが提供されることを確保することを可能にする。コンテンツ供給者は、多くの場合、セキュリティ・トリミング供給者を使用する。セキュリティ・トリミング供給者は、コンテンツに対するユーザーの特権を判定するために用いることができるセキュリティ・トリミング情報へのアクセスを付与する。このような場合、セキュリティ・トリミング供給者は、コンテンツまたはコンテンツに対する参照をユーザーに示す前に、ユーザーのアクセス特権を判定する。医療情報を患者に表示する医療供給者の場合、患者がアクセス特権を有さない医療情報はいずれも、完全にその患者から秘匿される、即ち、患者に表示される文書／コンテンツから「はじき出される」(trimmed out)。これを遂行するために、患者が医療情報を求める要求をウェブサーバーに送ったとき、ウェブサーバーはセキュリティ・トリミング供給者をコールして、この患者にコンテンツを提供する前に、要求されたコンテンツのコンポーネントに対するユーザーのアクセス特権を判定する。その後、ウェブサーバーは、ユーザーがアクセスすることができない特権情報を除外する(trim out)ことができる。

【０００７】

[0013] しかしながら、アクセス特権を判定する必要がある度に要求をセキュリティ・トリミング供給者に送ると、このような要求のボリュームが大量の通信帯域幅およびプロセッサー時間を消費するために、不経済になる可能性がある。セキュリティ・トリミング供給者に要求を過剰に送ることを回避するために、本明細書において開示するセキュリティ・トリミング・システムは、セキュリティ・トリミング情報のインテリジェントなキャッシングを設ける。具体的には、セキュリティ・トリミング・システムは、セキュリティ・トリミング情報を求めるあらゆる要求を、セキュリティ・トリミング供給者に送る必要がないように、セキュリティ・トリミング供給者から受信したセキュリティ・トリミング情報を格納するキャッシュを含む。加えて、セキュリティ・トリミング・システムは、キャッシュにおけるセキュリティ・トリミング情報の格納および処理にインテリジェンスを追加する。例えば、セキュリティ・トリミング・システムは、コンテンツ・セキュリティ情報に対する有効期限（ＴＴＬ）というような種々の他のパラメーターを、キャッシュに格納されたセキュリティ・トリミング情報に関連付けて、そのセキュリティ・トリミング情報に対するプロキシーまたは表現を生成する。

【０００８】

[0014] つまり、患者が何らかの特定のコンテンツにアクセスできるか否か判定することに、医療供給者が関心がある場合、この医療供給者のウェブサーバーは、セキュリティ・トリミング・システムに、患者のアクセス特権を判定することを求める要求を送る。セキュリティ・トリミング・システムは、最初に、このようなセキュリティ・トリミング情報、またはこのような情報の何らかのプロキシーをキャッシュに要求する。キャッシュの中で情報が見つからない場合、またはキャッシュ内に格納された情報が失効した情報(stale information)である場合、セキュリティ・トリミング・システムは要求をセキュリティ・トリミング供給者に送る。更に、セキュリティ・トリミング・システムがアクセスするおよび／またはセキュリティ・トリミング供給者から情報を受信する度に、要求時刻、特定のセキュリティ・トリミング情報を求めて要求を送った回数等というような他の情報も、キャッシュに格納する。したがって、医療供給者のウェブサーバーが、前週における日程計画情報 (scheduling information) を確かめるために特定の患者のアクセス特権を既に求めており、以前の要求によって応答が生成され、この特定の患者がこのような日程計画情報にアクセスすることをこの応答が可能にする場合、セキュリティ・トリミング・システムはこのような、キャッシュに保存されている以前の応答を用いて医療供給者に応答するので、セキュリティ・トリミング供給者に、費用がかかる要求を送る必要はない。

【０００９】

[0015] インテリジェント・キャッシュ・システムを設けることによって、本明細書において開示するセキュリティ・トリミング・システムは、要求を送る回数を減らし、した

がって、セキュリティ・トリミング供給者にかかる負荷も減らす。更に、このようなインテリジェント・キャッシュを利用することによって、セキュリティ・トリミング・システムは、医療サービス供給者のようなユーザーからの要求に応答するために要する時間も短縮する。このことから、これらのユーザーは、医療サービス供給者の患者のようなエンド・ユーザーに一層応答し易くなる。

【００１０】

[0016] 図１は、セキュリティ・トリミング・システム１００についてデーター・ソースおよびフローの例を示す。具体的には、セキュリティ・トリミング・システム１００は、患者Ｃ１０２、患者Ｄ１０４というような、医療供給者の種々のユーザーについてのセキュリティ特権情報を提供するために用いられる。患者１０２、１０４は、ウェブサイト１１０を用いて、医療供給者からの情報にアクセスする。ウェブサイト１１０は、特定の医者の予定、研究所の予定等についての情報を提供する医療供給者の予定表１１２を提示する。例えば、予定表１１２の各コンポーネントは、リンクによって示され、このリンクをユーザーが選択すると、そのコンポーネントに関係する追加情報を得ることができる。

【００１１】

[0017] 一実施態様では、医療供給者はウェブサーバー１２０上でウェブサイト１１０をホストする。患者１０２、１０４がウェブサイト１１０にアクセスすると、患者１０２、１０４を識別する種々の情報がウェブサーバー１２０にも送られる。例えば、患者Ｃ１０２が使用するコンピューターのブラウザーが、患者Ｃ１０２を識別する情報をウェブサーバー１２０に送る。あるいは、ウェブサーバー１２０が、患者Ｃ１０２に、ログインおよびパスワード、あるいは他の認証手段を用いて、予定表１１２上で認証するように要求する。

【００１２】

[0018] 一旦ウェブサーバー１２０が患者Ｃ１０２を認証したなら、ウェブサーバー１２０は、患者Ｃ１０２に提供することができる情報を判定する。例えば、患者Ｃ１０２が医療供給者の予定表１１２にアクセスしたとき、ウェブサーバー１２０は、予定表１１２へのアクセスを患者Ｃ１０２に完全に付与すべきか否か判断する。この判断を行うとき、ウェブサーバー１２０は、患者Ｃ１０２の素性(identity)を検証する。例えば、医療情報データーストア１２２は、種々の患者の素性についての情報、および予定表１１２を含む、医療情報に対する彼らのアクセス特権を格納する。加えて、ウェブサーバー１２０は、患者Ｃ１０２に示すべき予定表１１２の一部も決定する。例えば、予定表１１２は、所与の日における医者の予約全てをリストに纏め、このリストには患者の名前および予約の理由が含まれる。しかしながら、種々のプライバシーおよび法的な理由のため、ある患者の名前および予約理由が他の患者には示されないことが必要となる。つまり、午後１時に予約している患者Ｃ１０２が予定表１１２にアクセスするとき、名前Ｊｏｈｎ Ｂおよび予約理由「健康診断」だけが予定表１１２上で示される。

【００１３】

[0019] ウェブサーバー１２０は、予定表１１２の種々のコンポーネント・コンテンツに対する患者Ｃ１０２のアクセス権利を判定した後に、患者Ｃ１０２に示す情報についてこのような決定を行う。ウェブサーバー１２０は、セキュリティ・トリミング・プロセスを用いて、患者Ｃ１０２に表示される情報を決定する。セキュリティ・トリミングとは、ユーザーのコンテンツに対するアクセスを、このような情報に対する何らかの参照をユーザーに示す前に、決定するプロセスである。例えば、患者が基礎コンテンツにアクセスできる場合にのみ、予定表１１２におけるリンクがこの患者に示される。一実施態様では、予定表１１２の内容に関係するこのようなセキュリティ・トリミング情報は、セキュリティ・トリミング供給者１３０のような、セキュリティ・データーストアによって提供される。ウェブサーバー１２０は、セキュリティ・トリミング供給者１３０が基礎コンテンツに対する患者のアクセス権利を検証した場合にのみ、予定表１１２上にリンクを表示する。

【００１４】

[0020] 例えば、患者Ｃ１０２が予定表１１２にアクセスするとき、ウェブサーバー１２０からセキュリティ・トリミング供給者１３０への要求から、患者Ｃ１０２が午後１時の時間枠について患者の名前および予約理由のみにアクセス特権を有することを識別する。この場合、患者Ｃ１０２には予定の変更版１１６が提示される。一方、患者Ｄ１０４が予定表１１２にアクセスする場合、午後２時の時間枠についての変更予定１１８が患者Ｄ１０４に提示される。一方、病院の管理者、医者等のような医療供給者が予定表１１２にアクセスする場合、この医療供給者には予定表１１２全体についての情報が与えられ、この情報には予定表１１２上における全ての時間枠について患者の名前および予約理由が含まれる。

【００１５】

[0021] セキュリティ・トリミング・システム１００の一実施態様では、ウェブサーバー１２０がセキュリティ・トリミング供給者１３０に要求を送る度に、セキュリティ・トリミング供給者１３０によって生成された結果がキャッシュ１４０に格納される。更に、セキュリティ・トリミングを求める要求をセキュリティ・トリミング供給者１３０に送る代わりに、代替実施態様では、ウェブサーバー１２０がセキュリティ・トリミング情報を求める要求をキャッシュ１４０に送る。つまり、例えば、患者Ｃ１０２が予定表１１２にアクセスすることを求める要求を送ったとき、ウェブサーバー１２０は、最初に、予定表１１２の種々のコンポーネントに対するこの患者のアクセス特権を判定することを求める要求をキャッシュ１４０に送る。

【００１６】

[0022] キャッシュ１４０は、応答をウェブサーバー１２０に供給するために、要求されたセキュリティ・トリミング情報を有するか否か判定する。例えば、キャッシュ１４０は、キャッシュされたセキュリティ・トリミング・データーストア１４２に、ウェブサーバーに送られる応答を決定するように要求する。セキュリティ・トリミング・データーストア１４２は、セキュリティ・トリミング供給者１３０に対する過去の要求に基づいて、セキュリティ・トリミング情報を格納するように構成される。例えば、医療供給者の予定表１１２のコンポーネントに対する患者Ｃ１０２のアクセス特権を求める過去の要求に応答して、セキュリティ・トリミング供給者１３０が「アクセス」の値を返した場合、キャッシュされたセキュリティ・トリミング・データーストア１４２は、医療供給者の予定表１１２のそのコンポーネントに対する患者Ｃ１０２のアクセス特権の値として「アクセス」を格納する。セキュリティ・トリミング供給者１３０から戻される他の可能な値には、「アクセス禁止」、「不確定」、「失敗」等が含まれる。更にその代わりに、アクセス特権値は、コンテンツに対して可変レベルのアクセスを付与するために戻される。つまり、医者には、医療供給者の予定表１１２についての特定のコンテンツに対する「編集アクセス」が付与され、一方患者には、その特定のコンテンツに対する「視認アクセス」が付与される。

【００１７】

[0023] 一実施態様では、ウェブサーバー１２０のようなコンテンツ供給者がコンテンツの位置およびそのコンテンツに対するユーザーのアクセス特権を要求する場合、確定した「アクセス」または「アクセス禁止」結果がコンテンツ供給者に供給される。代替実施形態では、セキュリティ・トリミング供給者１３０が検索結果供給者である場合、セキュリティ・トリミング供給者１３０は、ユーザーがコンテンツにアクセスできる場合、「アクセス」の値を返す。しかしながら、このような場合、セキュリティ・トリミング供給者１３０は、ユーザーがアクセスできない場合、セキュリティ・トリミング供給者１３０がそのコンテンツを知らない場合、またはそのコンテンツが移動または削除されている場合、セキュリティ・トリミング供給者１３０は「未確定」値を戻す。同様に、セキュリティ・トリミング供給者１３０への要求をし損ねる可能性もあり、この場合、「失敗」値が戻される。セキュリティ・トリミング供給者１３０への要求失敗の原因になるイベントの例には、クエリー失敗、一時的ネットワーク接続問題による失敗、セキュリティ・トリミング供給者１３０が受ける要求の過剰負荷等が含まれる。

【００１８】
[0024] 一実施態様では、セキュリティ・トリミング供給者１３０が「アクセス」または「アクセス禁止」をセキュリティ・トリミング情報の値として戻す場合、キャッシュ１４０はこのような値を、キャッシュされたセキュリティ・トリミング・データーストア１４２に書き込む。セキュリティ・トリミング情報のこのような値は、ウェブサーバー１２０からの後続の要求に応答するために用いられる。しかしながら、セキュリティ・トリミング供給者１３０が確定的な「アクセス」または「アクセス禁止」値を戻さない場合、キャッシュ１４０は、ユーザーがコンテンツにアクセスできるか否か判断するために、受信した値の追加の解釈を引き受ける。
【００１９】
[0025] また、キャッシュ１４０はセキュリティ・トリミング推論エンジン１４４も含む。セキュリティ・トリミング推論エンジン１４４は、キャッシュされたセキュリティ・トリミング・データーストア１４２に格納されたセキュリティ・トリミング情報の値、およびセキュリティ・トリミング情報に関連する種々の他の関連パラメーターを用いて、ウェブサーバー１２０からの要求に対する応答を決定する。具体的には、セキュリティ・トリミング推論エンジン１４４は、セキュリティ・トリミング供給者１３０が確定的な「アクセス」または「アクセス禁止」値を返さないときに、ユーザーがコンテンツにアクセスできるか否か判断する。
【００２０】
[0026] 例えば、セキュリティ・トリミング供給者１３０がコンテンツについてセキュリティ・トリミング情報の値を「不確定」または「失敗」として戻した場合、キャッシュ１４０は、そのコンテンツについてのセキュリティ・トリミング情報の値を求めてセキュリティ・トリミング供給者１３０に送られる次の要求のタイミング、キャッシュ１４０がこのような要求をセキュリティ・トリミング供給者１３０に送った回数等というような、追加の情報を格納する。一実施形態では、次の要求までの時間のカウンタ、および要求回数のカウンタが、タイミング情報を格納するために用いられる。このような情報を格納することによって、キャッシュ１４０が、短い期間の内に同じセキュリティ・トリミング情報に対して余りに多くの要求がセキュリティ・トリミング供給者１３０に送られないことを確認することが可能になる。また、このような情報は、キャッシュ１４０がセキュリティ・トリミング情報の値について推論を行うことも可能にする。例えば、セキュリティ・トリミング供給者１３０に対する最後の３回の要求の各々が、コンテンツに対するユーザーのアクセス特権に対して「不確定」の値を戻した場合、キャッシュ１４０は、ユーザーはそのコンテンツにアクセスできないと判断し、ある時間期間そのコンテンツに対するセキュリティ・トリミング情報の値を「アクセス禁止」に設定する。このような場合、この時間期間が経過した後、キャッシュ１４０は、このコンテンツについての情報を求めるウェブサーバー１２０からの新たな要求に応答して、セキュリティ・トリミング供給者１３０に新たな要求を送る。
【００２１】
[0027] 一代替実施態様では、セキュリティ・トリミング推論エンジン１４４は、キャッシュされたセキュリティ・トリミング・データーストア１４２に格納されたセキュリティ・トリミング情報に関連する種々のパラメーターを用いて、このようなセキュリティ・トリミング情報の代表値を生成し、ウェブサーバー１２０に送る。また、セキュリティ・トリミング推論エンジン１４４は、他のこのようなパラメーターの値に基づいて、このようなパラメーターの値を設定する。例えば、セキュリティ・トリミング推論エンジン１４４は、セキュリティ・トリミング供給者１３０から最後に受信した特定のセキュリティ・トリミング情報、所定の時間期間にセキュリティ・トリミング供給者１３０が肯定的な値を送った回数等についての情報を格納する。その後、セキュリティ・トリミング推論エンジン１４４は、このような情報を用いて、セキュリティ・トリミング情報に関連するＴＴＬを設定する。
【００２２】

[0028] 一例として、キャッシュ１４０が、予定表１１２の特定のコンテンツに関連するセキュリティ・トリミング情報を求める要求を先週３回送り、その度にセキュリティ・トリミング供給者１３０が肯定的な値を生成した場合、セキュリティ・トリミング推論エンジン１４４は、その特定のセキュリティ・トリミング情報に関連するＴＴＬを「長」時間値に設定する。その後、そのセキュリティ・トリミング情報を求める要求がウェブサーバー１２０から受信されたとき、セキュリティ・トリミング推論エンジン１４４は、キャッシュされたセキュリティ・トリミング・データーストア１４２におけるセキュリティ・トリミング情報に添付されたＴＴＬを評価して、ウェブサーバー１２０に送る応答を決定する。例えば、セキュリティ・トリミング情報に対するＴＴＬが所定の閾値よりも大きい場合、セキュリティ・トリミング推論エンジン１４４は、そのセキュリティ・トリミング情報の代表値を、キャッシュされたセキュリティ・トリミング・データーストア１４２に格納されたものと同一に決定する。しかしながら、セキュリティ・トリミング情報に対するＴＴＬが所定の閾値未満である場合、セキュリティ・トリミング推論エンジン１４４は、セキュリティ・トリミング情報の現在値を求める新たな要求をセキュリティ・トリミング供給者１３０に送るように、キャッシュ１４０に命令する。

【００２３】

[0029] キャッシュ１４０は、セキュリティ・トリミング供給者１３０から受信したセキュリティ・トリミング情報の実際の値、またはこのようなセキュリティ・トリミング情報の代表値のいずれかをウェブサーバー１２０に戻す。一実施態様では、キャッシュ１４０は、その値が、要求されたセキュリティ・トリミング情報の実際の値か、または代表値かについても、ウェブサーバー１２０に伝える。一代替実施態様では、セキュリティ・トリミング推論エンジン１４４は、信頼度値も生成する。信頼度値は、セキュリティ・トリミング情報の代表値がセキュリティ・トリミング情報の実際の値と同じである確率(likelihood)を指定する。このような実施態様では、信頼度値は、ウェブサーバー１２０に、セキュリティ・トリミング情報の代表値と共に伝えられる。その後、ウェブサーバー１２０は、セキュリティ・トリミング情報の代表値を用いるか否か判断する。

【００２４】

[0030] キャッシュされたセキュリティ・トリミング・データーストア１４２が要求されたセキュリティ・トリミング情報の有効値を有していないため、そしてセキュリティ・トリミング推論エンジン１４４が要求されたセキュリティ・トリミング情報に対して有効な代表値を生成することができないために、キャッシュ１４０がウェブサーバー１２０からのセキュリティ・トリミング要求に応答できないと判断した場合、キャッシュ１４０は、更新されたセキュリティ・トリミング情報を得るために、セキュリティ・トリミング供給者１３０に要求を送る。代替実施態様では、キャッシュ１４０は、キャッシュされたセキュリティ・トリミング・データーストア１４２においてセキュリティ・トリミング情報に関連する他のパラメーターを分析して、セキュリティ・トリミング供給者１３０に更新を求める要求をいつ送るか決定する。

【００２５】

[0031] あるいは、キャッシュ１４０は、種々のセキュリティ・トリミング情報を求める周期的な要求を、セキュリティ・トリミング供給者１３０に送るように構成される。例えば、キャッシュ１４０は、キャッシュ１４０とセキュリティ・トリミング供給者１３０とを接続する通信ネットワークの輻輳が少ないとき、セキュリティ・トリミング供給者１３０が多数のセキュリティ・トリミング要求に応対するのに非常に忙しいのではないとき等に、毎日ある時刻にこのような要求を送る。一旦ウェブサーバー１２０がセキュリティ・トリミング情報またはセキュリティ・トリミング情報の代表値をキャッシュ１４０から受信したなら、ウェブサーバー１２０は、このようなセキュリティ・トリミング情報を用いて、ユーザーに示す予定表１１２の部分を決定する。

【００２６】

[0032] 一実施態様では、セキュリティ・トリミング・システム１００の種々のコンポーネントは、インターネット、仮想プライベート・ネットワーク（ＶＰＮ）、移動体通信

ネットワーク等のような通信ネットワークによって、通信可能に互いに接続される。一代替実施態様では、ウェブサーバー１２０に仮想メモリーを提供するクラウド・サーバー上というように、ウェブサーバー１２０に容易にアクセス可能なサーバー上に、キャッシュ１４０が配置される。あるいは、キャッシュ１４０上のコンテンツが、自動的に多数のウェブサーバーの仮想メモリー上にミラーリングされ、このようなウェブサーバーの各々が、公衆通信ネットワークを通じて通信する必要なく、キャッシュに要求を送ることを可能にする。

【００２７】

[0033] 図２は、セキュリティ・トリミング・システム２００についてのデーター・ソースおよびフローの例を示す。セキュリティ・トリミング・システム２００は、多数のセキュリティ・トリミング供給者にインテリジェントなキャッシングを提供するアクセス・キャッシュ２１０を含む。一実施態様では、ウェブサーバー２２０、２２２は、アクセス・キャッシュ２１０を用いて、セキュリティ・トリミング供給者２３０、２３２によって提供されるセキュリティ・トリミング情報に対するアクセスを得る。例えば、ウェブサーバーＩ２２０は、ウェブサイト上で開示されるコンテンツについてセキュリティ・トリミング情報を要求する医療サービス供給者のウェブサーバーである。一実施態様では、ウェブサーバーＩ２２０上のコンテンツは、セキュリティ・トリミング供給者２３０、２３２双方からのセキュリティ・トリミング情報を必要とする。同様に、ウェブサーバーＩＩ２２２も、セキュリティ・トリミング供給者２３０、２３２双方からのセキュリティ・トリミング情報を要求とする。セキュリティ・トリミング・システム２００の一実施態様では、セキュリティ・トリミング供給者Ｉ２３０は、主セキュリティ・トリミング供給者に指定され、セキュリティ・トリミング供給者ＩＩ２３２は副セキュリティ・トリミング供給者に指定される。このような実施態様では、主セキュリティ・トリミング供給者への要求が「不確定」応答を与えるとき、要求が副セキュリティ・トリミング供給者に送られる。代替実施態様では、主セキュリティ・トリミング供給者上のトリミング要求負荷についての観察に基づいて、要求が副セキュリティ・トリミング供給者に送られる。

【００２８】

[0034] ウェブサーバー２２０、２２２がセキュリティ・トリミング供給者２３０、２３２に直接アクセスして（破線で示すように）必要なセキュリティ・トリミング情報を得ることができる場合、セキュリティ・トリミング・システム２００は、必要なセキュリティ・トリミング情報を得るために、アクセス・キャッシュ２１０を用いて、ウェブサーバー２２０、２２２を図示する(illustrate)。例えば、ウェブサーバーＩ２２０が医療予定表上に表示されるコンテンツについてセキュリティ・トリミング情報を判定する必要があるとき、ウェブサーバーＩ２２０はアクセス・キャッシュ２１０を用いて、このようなセキュリティ・トリミング情報を得る。

【００２９】

[0035] アクセス・キャッシュ２１０は、セキュリティ・トリミング・データーストア２１２を含む。セキュリティ・トリミング・データーストア２１２は、セキュリティ・トリミング供給者２３０、２３２から受信したセキュリティ・トリミング情報を格納する。このようなセキュリティ・トリミング情報は、セキュリティ・トリミング供給者２３０、２３２に送られた以前のセキュリティ・トリミング要求の結果として収集することができる。ウェブサーバーＩ２２０から要求を受けると、アクセス・キャッシュ・インテリジェンス・エンジン２１４は、セキュリティ・トリミング・データーストア２１２が、ウェブサーバーＩ２２０からの要求に応答するために必要な情報を含むか否か判断する。含む場合、アクセス・キャッシュ２１０は、データーストア２１２においてセキュリティ・トリミング情報に関連する種々のパラメーターをチェックして、このようなセキュリティ・トリミング情報の有用性を判定する。

【００３０】

[0036] このような関連パラメーターの一例に、セキュリティ・トリミング情報に添付され、セキュリティ・トリミング・データーストア２１２に格納されたセキュリティ・ト

リミング情報の古さ(staleness)についての情報を提供するＴＴＬがある。このようなＴＴＬが期限切れになった場合、即ち、セキュリティ・トリミング情報が相当古い場合、アクセス・キャッシュ・インテリジェンス・エンジン２１４は、このようなセキュリティ・トリミング情報は使えないと判断する。このような場合、アクセス・キャッシュ２１０は、必要に応じて、セキュリティ・トリミング供給者２３０、２３２に新たな要求を送るか、新たな要求をスケジューリングする。

【００３１】

[0037] 図３は、本明細書において開示したセキュリティ・トリミング・システムの動作例３００を示す。例えば、動作３００は、医療日程計画情報を患者に提供する医療情報システムにおいて用いられる。受信動作３０２は、サーバーによって提供されるウェブサイトまたは他のリソースにおいて、コンテンツを求める要求を受ける。例えば、受信動作３０２は、医療情報供給者からの、特定の医者との患者の予約を求める要求を受ける。この患者がウェブ・ブラウザーを用いて医療情報予定表を訪問したとき、このような医療情報予定表をホストするサーバーは、最初に、患者に見せることができる医療情報予定表の部分、および予定表ページ上における他のコンテンツを決定する。

【００３２】

[0038] 要求評価動作３０４は、患者が要求したコンテンツを表示するには、何らかの種類のセキュリティ・トリミング情報が必要になるか否か判断する。医者の予定表ではその日に２０の予約がある場合、予定表を訪問する種々の患者の各々が、この医者の予定表の部分のみを見ることができる。同様に、医者が研究のためにその日の一部を休診する(block off)場合、医者は、患者が医者の予定表においてこのような研究時間を見ることができないことを確認することができる。予定表を見ることを求める患者からの要求の場合、要求評価動作３０４は、予定表における特定のコンテンツへのアクセスがこの患者に与えられるべきか否か判断する。一実施態様では、所与の医者に対して多数の患者の予約がある場合、要求評価動作３０４は、これらのコンテンツの内患者に表示してもよいものを決定するために、種々の時間枠の各々においてコンテンツに対するセキュリティ・トリミング要件を決定する。

【００３３】

[0039] 要求評価動作３０４が、患者によって要求された特定のコンテンツがセキュリティ・トリミング情報を全く必要としないと判断した場合、表示動作３０６が、このようなコンテンツを患者に表示する。例えば、予約予定表が医者の専門、医者の事務所の地図等についての包括的なコンテンツを含み、このコンテンツがセキュリティ・トリミング情報を全く必要としない場合、表示動作３０６は、このような包括的コンテンツを患者に表示する。一方、要求評価動作３０４が、要求されたコンテンツはセキュリティ・トリミング情報を必要とすると判断した場合、要求動作３０８が、そのコンテンツについてのセキュリティ・トリミング情報を求める要求を送る。

【００３４】

[0040] 一実施態様では、要求動作３０８は、セキュリティ・トリミング情報を求める要求をアクセス・キャッシュに送る。アクセス・キャッシュは、多数のセキュリティ・トリミング供給者のためにセキュリティ・トリミング情報を格納するように構成される。しかしながら、代替実施態様では、要求動作３０８は、このような要求を直接セキュリティ・トリミング供給者に送る。更にその代わりに、要求動作３０８は、このような要求をキャッシュおよびセキュリティ・トリミング供給者双方に送る。例えば、ユーザーからの要求に応答する際に時間が重要である場合、要求動作３０８は、素早い応答を確保するために、キャッシュおよびセキュリティ・トリミング供給者双方にこのような要求を送る。

【００３５】

[0041] その後、判定動作３１０が、要求されたセキュリティ・トリミング情報に対するエントリがアクセス・キャッシュ内にあるか否か判定する。アクセス・キャッシュにおいてセキュリティ・トリミング情報が見つからない場合、宣言動作３１２が、アクセス・キャッシュ・ミスを宣言する。代替実施態様では、宣言動作３１２はセキュリティ・トリ

ミング情報を求める要求の時刻というような、他のパラメーターをその特定のセキュリティ・トリミング情報に割り当てることも行う。あるいは、宣言動作３１２は、所与の時間期間において特定のセキュリティ・トリミング情報を求める要求が受けられた回数を追跡する要求カウンタの数値を調節する。このようなカウンタ情報は、その特定のセキュリティ・トリミング情報を求める要求が、アクセス・キャッシュからセキュリティ・トリミング供給者に送られる自動セキュリティ・トリミング情報要求に含まれるか否か判断するために、アクセス・キャッシュによって用いられる。

【００３６】

[0042] しかしながら、判定動作３１０が、要求されたセキュリティ・トリミング情報に対するエントリがアクセス・キャッシュ内にあると判定した場合、他の判定動作３１４が、アクセス・キャッシュにおけるセキュリティ・トリミング情報に関連するＴＴＬのような、種々のパラメーターを評価する。具体的には、判定動作３１４は、このようなＴＴＬの値を評価して、キャッシュに格納されているセキュリティ・トリミング情報の値の有効性を判断する。例えば、キャッシュ内で見つけられた特定のセキュリティ・トリミング情報が、セキュリティ・トリミング供給者からかなり以前に受信されたのであった場合、この特定のセキュリティ・トリミング情報に添付されたＴＴＬは、判定動作３１４によって評価されるときには、期限が切れているはずである。このような場合、宣言動作３１６が、アクセス・キャッシュにおけるこの特定のセキュリティ・トリミング情報エントリが、期限切れまたは無効であると宣言する。

【００３７】

[0043] 一方、このセキュリティ・トリミング情報のＴＴＬが期限切れでない場合、評価動作３１８は、このセキュリティ・トリミング情報についてアクセス・キャッシュ・エントリを評価する。例えば、医療予定表上における特定のコンテンツにアクセスしようとしている患者がそのコンテンツにアクセスできない場合、アクセス・キャッシュにおけるセキュリティ・トリミング・エントリは、「アクセス禁止」の値を有する。このような場合、制御は動作３２０に渡され、セキュリティ・トリミング情報を要求するサーバーに、この患者はコンテンツにアクセスできないことを通知する。その結果、サーバーはこのようなコンテンツを患者に表示しない。しかしながら、予定表上において特定のコンテンツにアクセスしようとしている患者がそのコンテンツにアクセスできる場合、アクセス・キャッシュにおけるセキュリティ・トリミング・エントリは、「アクセス」の値を有する。このような場合、制御は動作３２２に渡され、セキュリティ・トリミング情報を要求するサーバーに、患者はコンテンツにアクセスできることを通知する。その結果、サーバーはこのようなコンテンツを患者に表示する。

【００３８】

[0044] 状況によっては、アクセス・キャッシュにおけるセキュリティ・トリミング情報の値が、「不確定」または「失敗」となる可能性がある。例えば、アクセス・キャッシュからセキュリティ・トリミング供給者への、あるセキュリティ・トリミング情報を求める過去の要求が、各々、「不確定」応答を生じた場合、即ち、患者がコンテンツにアクセスできるか否かについて、セキュリティ・トリミング供給者が知らなかった場合、アクセス・キャッシュは、セキュリティ・トリミング情報に「不確定」の値を割り当てる。同様に、アクセス・キャッシュがセキュリティ・トリミング情報を得ようとする度にセキュリティ・トリミング供給者から応答がなかった場合、これは、セキュリティ・トリミング供給者に対する大量の需要(demand)、通信ネットワークの障害等で発生する場合があるが、アクセス・キャッシュはセキュリティ・トリミング情報に「失敗」の値を割り当てる。このように、セキュリティ・トリミング情報が「不確定」または「失敗」の値を有する場合、動作３２４はこのセキュリティ・トリミング情報に、再試行の印を付ける。

【００３９】

[0045] 動作３００の結果、アクセス・キャッシュにおいて特定のセキュリティ・トリミング情報が見つからない場合、特定のセキュリティ・トリミング情報のＴＴＬが期限切れであった場合、または特定のセキュリティ・トリミング情報の値が「失敗」または「不

確定」であった場合、要求動作３２６は、セキュリティ・トリミング供給者に、その特定のセキュリティ・トリミング情報の更新値または現在値を要求する。一実施態様では、このような要求は、セキュリティ・トリミング情報の値が見つからない、期限切れである、失敗または不確定であることが判明すると直ちにリアル・タイムで送られる。しかしながら、代替実施態様では、アクセス・キャッシュはこのようなセキュリティ・トリミング情報要求を、セキュリティ・トリミング供給者に対する他の保留の要求の一群に追加する。このような実施態様では、このような要求の一群が、所定の時間間隔でセキュリティ・トリミング供給者に送られる。しかしながら、代替実施態様では、セキュリティ・トリミング供給者に送られる要求の収集(batching)は、アクセス・キャッシュによって受けられる種々の要求に基づく。例えば、患者が予定表、検査結果、および診断を一度に全て医療供給者のウェブ・ページ上で見ることを望む場合、キャッシュは、予定表、検査結果、および診断の各々についてのセキュリティ・トリミング情報を求める要求を纏めて１つの集合にして、このような要求の集合をセキュリティ・トリミング供給者に送る。これによって、セキュリティ・トリミング・システム３００は貴重なネットワーク帯域幅を節約することが可能になる。

【００４０】

[0046] マッピング動作３２８は、アクセス・キャッシュにおいて、要求の結果をセキュリティ・トリミング供給者にマッピングする。一実施態様では、要求がセキュリティ・トリミング供給者に送られる前のセキュリティ・トリミング情報の値が「アクセス」であり、要求の結果、セキュリティ・トリミング情報の値が同様に「アクセス」であることが示された場合、このようなセキュリティ・トリミング情報に関連するＴＴＬには「長」の値が割り当てられる。このような場合、アクセス・キャッシュは、セキュリティ・トリミング情報の値が「アクセス」であることが改めて確認したので、アクセス・キャッシュはこの値を高い信頼度レベルでより長い時間期間用いることができる。同様に、アクセス・キャッシュにおけるセキュリティ・トリミング情報の現在値が「失敗」であり、要求の結果も、セキュリティ・トリミング情報の値が「失敗」であることが示す場合、アクセス・キャッシュはＴＴＬの値を「短」に設定する。このような場合、キャッシュは、短い時間期間の内に要求をセキュリティ・トリミング供給者に送るか、またはもっと積極的に、セキュリティ・トリミング情報の値についてもっと確定的な回答を得るための要求を送る。

【００４１】

[0047] 一方、要求がセキュリティ・トリミング供給者に送られる前におけるセキュリティ・トリミング情報の値が「不確定」であり、多数の要求が既にセキュリティ・トリミング供給者に送られており、更に要求の結果が、セキュリティ・トリミングの値が「アクセス禁止」であることを示す場合、このようなセキュリティ・トリミング情報に関連するＴＴＬに、「長」の値を割り当てる。このような場合、セキュリティ・トリミング情報の値を判定するための以前の試み全てにおいて「不確定」という結果となり、要求の結果、値が「アクセス禁止」となったとすると、今後長い時間期間にわたって、アクセス・キャッシュはこのセキュリティ・トリミング情報に「アクセス禁止」の値を用いる。長い時間期間にわたって値を「アクセス禁止」に設定すると、セキュリティ・トリミング供給者に要求が送られる頻度が下がり、したがって、ユーザーがアクセスを殆ど有しそうもないコンテンツのための、セキュリティ・トリミング供給者への、費用がかかるトラフィックが減少する。

【００４２】

[0048] 同様に、要求がセキュリティ・トリミング供給者に送られる前におけるセキュリティ・トリミング情報の現在値が「不確定」であり、比較的少数の要求が既にセキュリティ・トリミング供給者に送られており、要求の結果が、セキュリティ・トリミングの値が「アクセス禁止」であることを示す場合、このようなセキュリティ・トリミング情報に関連するＴＴＬには「短」の値が割り当てられる。この場合、アクセス・キャッシュは、セキュリティ・トリミング供給者に送られるセキュリティ・トリミング情報に対する試行回数の値を増加させる。アクセス・キャッシュにおいて要求の結果をセキュリティ・トリ

ミング供給者にマッピングした後、格納動作３２０が、受信したセキュリティ・トリミング情報の値をアクセス・キャッシュに格納する。

【００４３】

[0049] 図４は、本明細書において開示したセキュリティ・トリミング・システムの代替動作例４００を示す。具体的には、動作４００は、特定のセキュリティ・トリミング情報が「不確定」の値を有するときに、アクセス・キャッシュがセキュリティ・トリミング供給者に要求することを示す。例えば、患者が医者の予約予定表に最初にアクセスしようとしている場合、セキュリティ・トリミング情報を格納するアクセス・キャッシュは、予約予定表上のコンテンツに対する患者のアクセス権利についてのセキュリティ・トリミング情報を有しておらず、このセキュリティ・トリミング情報に対する値が「不確定」となる。このような場合、要求動作４０２が、このコンテンツに関連するセキュリティ・トリミング情報について、セキュリティ・トリミング供給者に要求する。この要求の結果は、評価動作４０４によって評価される。

【００４４】

[0050] セキュリティ・トリミング供給者が戻したセキュリティ・トリミングの値が「失敗」である場合、動作４０６はアクセス・キャッシュにおけるセキュリティ・トリミング情報の値を「失敗」に設定し、このセキュリティ・トリミング情報に関連するＴＴＬを「短」に設定する。このような場合、アクセス・キャッシュは、結果が「失敗」となった原因である問題は短い時間期間で補正することができると想定し、したがって、短い時間期間の内にセキュリティ・トリミング供給者に他の要求が送られると、セキュリティ・トリミング情報のこの値を受信することになる。しかしながら、セキュリティ・トリミング供給者が、セキュリティ・トリミング情報の値を「アクセス」にして戻した場合、動作４０８はアクセス・キャッシュにおけるセキュリティ・トリミング情報の値を「アクセス」に設定し、セキュリティ・トリミング情報に関連するＴＴＬを「長」に設定する。この場合、患者はコンテンツにアクセスできるので、表示動作４１０はコンテンツを患者に表示する。

【００４５】

[0051] しかしながら、セキュリティ・トリミング供給者がセキュリティ・トリミング情報の値を「不確定」にして戻した場合、評価動作４１２は、セキュリティ・トリミング供給者からセキュリティ・トリミング情報の値を得るためにアクセス・キャッシュによって行われた試行または要求の回数を評価する。このような試行の回数が閾値よりも多く、多数会の試行の後でも、セキュリティ・トリミング情報の値を得ることができなかったことを示す場合、動作４１４は、ユーザーがこのコンテンツにアクセスできないと推論し、したがって、アクセス・キャッシュにおけるセキュリティ・トリミング情報の値を「アクセス禁止」に設定し、このセキュリティ・トリミング情報に関連するＴＴＬを「長」に設定する。この場合、患者はコンテンツにアクセスできないので、表示動作４１６は、患者がアクセスできないコンテンツを除いて、予約カレンダを表示する。

【００４６】

[0052] 一方、セキュリティ・トリミング供給者からセキュリティ・トリミング情報の値を得るためにアクセス・キャッシュによって行われた試行または要求の回数が閾値よりも少ない場合、動作４１８は、アクセス・キャッシュにおけるセキュリティ・トリミング情報の値を「不確定」に設定し、セキュリティ・トリミング情報に関連するＴＴＬを「中間」に設定する。このような場合、動作４１８は、更に、セキュリティ・トリミング供給者からセキュリティ・トリミング情報の値を得るためにアクセス・キャッシュによって行われた試行または要求の回数を示すカウントを増加させる。

【００４７】

[0053] 図５は、本明細書において開示したセキュリティ・トリミング・システムの使用例を示す。具体的には、図５は、本明細書において開示したセキュリティ・トリミング・システムの使用中における、ウェブサーバー５０２、アクセス・キャッシュ５０４、およびセキュリティ・トリミング供給者５０６について種々の段階を示す。段階１において

、医療供給者の患者というようなユーザーが、ウェブサーバー５０２から患者予約予定表を表示するウェブ・ページというような特定の文書にナビゲートする。図示する例では、このような文書は、５つの可能なユニバーサル・リソース・ロケータ（ＵＲＬ）、ＵＲＬ１～ＵＲＬ５を含み、患者に予約予定表の一部として表示することができる。あるいは、ＵＲＬ１～ＵＲＬ５が患者予定情報、患者の診断、患者の検査結果等のような、ユーザーによって要求された５つの異なる情報を表す。段階１において、５１２に示すように、ウェブサーバー５０２は５つのＵＲＬの内どれを患者に表示することができるか判定する必要がある。この段階では、５１４に示すように、アクセス・キャッシュ５０４はＵＲＬ１～ＵＲＬ４についてセキュリティ・トリミング情報を有する。具体的には、アクセス・キャッシュ５０４は、患者がＵＲＬ１、ＵＲＬ２、およびＵＲＬ４にアクセスできるが、患者はＵＲＬ３にアクセスできないことを示す。この段階において、アクセス・キャッシュ５０４は、ＵＲＬ５について何のセキュリティ・トリミング情報も有していない。

【００４８】

[0054] 段階２において、ＵＲＬ１～ＵＲＬ５についてのセキュリティ・トリミング情報を求める要求５１６が、アクセス・キャッシュ５０４に送られる。その後、段階３において、アクセス・キャッシュ５０４は、ＵＲＬ１、ＵＲＬ２、およびＵＲＬ４についてのセキュリティ・トリミング情報と共に結果５１８をウェブサーバー５０２に戻す。その結果、５２０において、ウェブサーバー５０２は、要求されたＵＲＬについてのセキュリティ・トリミング情報を更新する。その後、段階４において、ウェブサーバー５０２は、５２２に示すように、ＵＲＬ１、ＵＲＬ２、およびＵＲＬ４を患者に表示する。ウェブサーバー５０２が、アクセス・キャッシュ５０４によって提供されたセキュリティ・トリミング情報を用いて、患者にコンテンツを表示している間、背景では、アクセス・キャッシュ５０４が、ＵＲＬ５についてのセキュリティ・トリミング情報を求める要求５２４をセキュリティ・トリミング供給者５０６に送る。５２６に示すように、セキュリティ・トリミング供給者５０６は、患者がＵＲＬ５にアクセスできることを示す。

【００４９】

[0055] 段階５において、セキュリティ・トリミング供給者５０６は、ＵＲＬ５についてのセキュリティ・トリミング情報と共に結果５２８をアクセス・キャッシュ５０４に送る。アクセス・キャッシュ５０４は、セキュリティ・トリミング供給者５０６からの結果に基づいて、ＵＲＬ５についてのセキュリティ・トリミング情報を更新する。その結果、５３０に示すように、アクセス・キャッシュ５０４は、この時点では、患者がＵＲＬ１、ＵＲＬ２、ＵＲＬ４、およびＵＲＬ５にアクセスできることを示す。

【００５０】

[0056] その後、段階６において、ユーザーは、予約予定表のような文書を表示するウェブ・ブラウザーをリフレッシュする。ユーザーが予約予定表をリフレッシュしたことに応答して、ウェブサーバー５０２はユーザーについての全てのセキュリティ・トリミング情報をリセットする。つまり、５３２に示すように、ウェブサーバー５０２はＵＲＬ１～ＵＲＬ５の各々についてセキュリティ・トリミング情報を決定する必要がある。その結果、ウェブサーバー５０２は、ＵＲＬ１～ＵＲＬ５についてのセキュリティ・トリミング情報を求める新たな要求５３４を、アクセス・キャッシュ５０４に送る。

【００５１】

[0057] 段階７において、アクセス・キャッシュ５０４は、更新したセキュリティ・トリミング情報５３６をウェブサーバー５０２に送る。尚、アクセス・キャッシュ５０４はＵＲＬ１～ＵＲＬ５についてのセキュリティ・トリミング情報を有するので、この段階ではセキュリティ・トリミング供給者５０６に要求が送られないことを注記しておく。この結果、セキュリティ・トリミング供給者５０６に送られる、費用がかかる要求が減少する。ウェブサーバー５０２は、５３８に示すように、ユーザーにＵＲＬ１、ＵＲＬ２、ＵＲＬ４、およびＵＲＬ５へのアクセスが付与されるように、そのセキュリティ・トリミング情報を更新する。代替実施態様では、更新されたセキュリティ・トリミング情報を求める新たな要求をウェブサーバー５０２から受けなくても、アクセス・キャッシュ５０４は、

周期的に更新されたセキュリティ・トリミング情報をウェブサーバー５０２に送るように構成される。

【００５２】

[0058] 図６は、以上で説明した技術を実現するのに有用であると考えられるシステム例を示す。以上で説明した技術を実現するための図６のハードウェアおよび動作環境例は、ゲーミング・コンソールまたはコンピューター２０の形態とした汎用計算デバイス、移動体電話機、パーソナル・データー・アシスタント（ＰＤＡ）、セット・トップ・ボックス、または他のタイプの計算デバイスというような、計算デバイスを含む。図６の実施態様では、例えば、コンピューター２０は、処理ユニット２１、システム・メモリー２２、およびシステム・バス２３を含む。システム・バス２３は、システム・メモリーから処理ユニット２１までを含む種々のシステム・コンポーネントを動作的に結合する。コンピューター２０のプロセッサーが、１つの中央処理ユニット（ＣＰＵ）、または、通常並列処理環境と呼ばれる、複数の処理ユニットを含むように、処理ユニット２１が１つだけであっても１つよりも多くてもよい。コンピューター２０は、従来のコンピューター、分散型コンピューター、または他のいずれのタイプのコンピューターでもよく、本発明はこのようなことに限定されない。

【００５３】

[0059] システム・バス２３は、メモリー・バスまたはメモリー・コントローラー、周辺バス、交換ファブリック(switched fabric)、二点間接続、および種々のバス・アーキテクチャーのいずれかを用いるローカル・バスを含む、様々なタイプのバス構造の内いずれでもよい。システム・メモリーは、単にメモリーと呼ばれることもあり、リード・オンリー・メモリー（ＲＯＭ）２４およびランダム・アクセス・メモリー（ＲＡＭ）２５を含む。基本入力／出力システム（ＢＩＯＳ）２６は、起動中のように、コンピューター２０内部にあるエレメント間で情報を転送するのに役立つ基本的なルーチンを収容し、ＲＯＭ２４に格納される。更に、コンピューター２０は、図示しないハード・ディスクからの読み取りおよびハード・ディスクへの書き込みを行うためのハード・ディスク・ドライブ２７、リムーバブル磁気ディスク２９からの読み取りまたはリムーバブル磁気ディスク２９への書き込みを行うための磁気ディスク・ドライブ２８、ならびにＣＤ ＲＯＭ、ＤＶＤ、または他の光媒体のようなリムーバブル光ディスク３１からの読み取りまたはリムーバブル光ディスク３１への書き込みを行う光ディスク・ドライブ３０も含む。

【００５４】

[0060] ハード・ディスク・ドライブ２７、磁気ディスク・ドライブ２８、および光ディスク・ドライブ３０は、システム・バス２３に、それぞれハード・ディスク・ドライブ・インターフェース３２、磁気ディクス・ドライブ・インターフェース３３、および光ドライブ・インターフェース３４を介して接続される。ドライブおよびそれらに付随するコンピューター読み取り可能媒体は、コンピューター２０のためのコンピューター読み取り可能命令、データー構造、プログラム・モジュール、およびその他のデーターの不揮発性ストレージを設ける。尚、磁気カセット、フラッシュ・メモリー・カード、ディジタル・ビデオ・ディスク、ランダム・アクセス・メモリー（ＲＡＭ）、リード・オンリー・メモリー（ＲＯＭ）等のような、コンピューターによってアクセス可能なデーターを格納することができるコンピューター読み取り可能媒体であれば、いずれのタイプでもこの動作環境例において使用してもよいことは、当業者には認められてしかるべきである。

【００５５】

[0061] オペレーティング・システム３５、１つ以上のアプリケーション・プログラム３６、他のプログラム・モジュール３７、およびプログラム・データー３８を含む多数のプログラム・モジュールは、ハード・ディスク、磁気ディスク２９、光ディスク３１、ＲＯＭ２４、またはＲＡＭ２５に格納することができる。ユーザーは、キーボード４０およびポインティング・デバイス４２のような入力デバイスを介して、コマンドおよび情報をコンピューター２０に入力することができる。他の入力デバイス（図示せず）は、マイクロフォン、ジョイスティック、ゲーム・パッド、衛星ディッシュ、スキャナー等を含むこ

とができる。これらおよびその他の入力デバイスは、多くの場合、システム・バスに結合されたシリアル・ポート・インターフェース４６を介して、処理ユニット２１に接続されるが、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）のような他のインターフェースによって接続されてもよい。モニター４７または他のタイプのディスプレイ・デバイスも、ビデオ・アダプター４８のようなインターフェースを介して、システム・バス２３に接続される。モニターに加えて、コンピューターは、通例、スピーカーおよびプリンターのような他の周辺出力デバイス（図示せず）も含む。

【００５６】

[0062] コンピューター２０は、リモート・コンピューター４９のような、１つ以上のリモート・コンピューターへの論理接続を用いて、ネットワーク接続環境において動作することもできる。これらの論理接続は、コンピューター２０に結合された通信デバイス、またはコンピューター２０の一部である通信デバイスによって行われるが、本発明は、特定のタイプの通信デバイスには限定されない。リモート・コンピューター４９は、他のコンピューター、サーバー、ルーター、ネットワークＰＣ、クライアント、ピア・デバイスまたは他の一般的なネットワーク・ノードであってもよく、通例、コンピューター２０に関して以上で説明したエレメントの多くまたは全部を含むが、図６には、メモリー記憶デバイス５０だけが示されている。図６に示す論理接続は、ローカル・エリア・ネットワーク（ＬＡＮ）５１およびネットワーク（ＷＡＮ）５２を含む。このようなネットワーク接続環境は、事務所ネットワーク、企業規模のコンピューター・ネットワーク、イントラネット、およびインターネットでは極普通である。これらは全てネットワークの種類である。

【００５７】

[0063] ＬＡＮネットワーク接続環境において用いられる場合、コンピューター２０は、ネットワーク・インターフェースまたはアダプター５３を介してローカル・ネットワーク５１に接続される。アダプター５３は、一種の通信デバイスである。ＷＡＮネットワーク接続環境において用いられる場合、コンピューター２０は、通例、モデム５４、ネットワーク・アダプター、ある種の通信デバイス、またはワイド・エリア・ネットワークワーク５２を通じて通信を確立する他の何らかのタイプの通信デバイスを含む。モデム５４は、内蔵型でも外付け型でもよく、シリアル・ポート・インターフェース４６を介してシステム・バス２３に接続される。ネットワーク接続環境では、コンピューター２０に関して図示したプログラム・エンジン、またはその一部が、リモート・メモリー記憶デバイスに格納されてもよい。尚、図示するネットワーク接続は例であり、コンピューター間で通信リンクを確立する他の手段および通信デバイスを用いてもよいことは認められよう。

【００５８】

[0064] 一実施態様例では、セキュリティ・トリミング・システムの種々のコンポーネントは、メモリー２２および／または記憶デバイス２９または３１に格納され処理ユニット２１によって処理される命令によって具体化することができる。コンテンツ・セキュリティ情報、セキュリティ・トリミング・データーストア、および他のデーターは、メモリー２２および／または記憶デバイス２９または３１に永続的データーストアとして格納されてもよい。更に、セキュリティ・トリミング・システムは、ネットワーク接続システムにサービス機能を提供するように構成されたハードウェアおよび／またはソフトウェアを表す。このようなサービスは、汎用コンピューターおよび特殊ソフトウェア（サービス・ソフトウェアを実行するサーバーのような）、特殊目的計算システムおよび特殊ソフトウェア（サービス・ソフトウェアを実行する移動体デバイスまたはネットワーク・アプライアンスのような）、あるいは他の計算構成を用いて実現することができる。代替実施態様では、セキュリティ・トリミング・システムおよびその種々のモジュールは、移動体データーストア、クラウド等に格納されてもよい。

【００５９】

[0065] 実施形態の中には、製造品目(article of manufacture)を構成するものもある。製造品目は、ロジックを格納する記憶媒体を含むことができる。記憶媒体の例には、電

子データーを格納することができる１つ以上のタイプのコンピューター読み取り可能記憶媒体が含まれ、揮発性メモリーまたは不揮発性メモリー、リムーバブルまたは非リムーバブル・メモリー、消去可能メモリーまたは消去可能でないメモリー、書き込み可能メモリーまたは再書き込み可能メモリー等が含まれる。ロジックの例には、ソフトウェア・コンポーネント、プログラム、アプリケーション、コンピューター・プログラム、アプリケーション・プログラム、システム・プログラム、機械プログラム、オペレーティング・システム・ソフトウェア、ミドルウェア、ファームウェア、ソフトウェア・モジュール、ルーチン、サブルーチン、関数、メソッド、手順、ソフトウェア・インターフェース、アプリケーション・プログラム・インターフェース（ＡＰＩ）、命令セット、計算コード、コンピューター・コード、コード・セグメント、コンピューター・コード・セグメント、ワード、値、記号、またはこれらのあらゆる組み合わせというような、種々のソフトウェア・エレメントを含むことができる。一実施形態では、例えば、製造品目は、実行可能コンピューター・プログラム命令を格納することもでき、この命令をコンピューターによって実行すると、以上で説明した実施形態にしたがって方法および／または動作をこのコンピューターに実行させる。実行可能コンピューター・プログラム命令は、ソース・コード、コンパイル・コード、インタプリター・コード、実行可能コード、スタティック・コード、ダイナミック・コード等のような、適したタイプのコードであればいずれでも含むことができる。実行可能コンピューター・プログラム命令は、既定のコンピューター言語、様式(manner)または構文(syntax)にしたがって、一定の機能を実行するようにコンピューターに命令するために、実装することができる。 命令は、適した高級プログラム言語、低級プログラム言語、オブジェクト指向プログラム言語、ビジュアル・プログラム言語、コンパイル型プログラム言語および／またはインタプリター型プログラム言語であればいずれを用いても実現することができる。

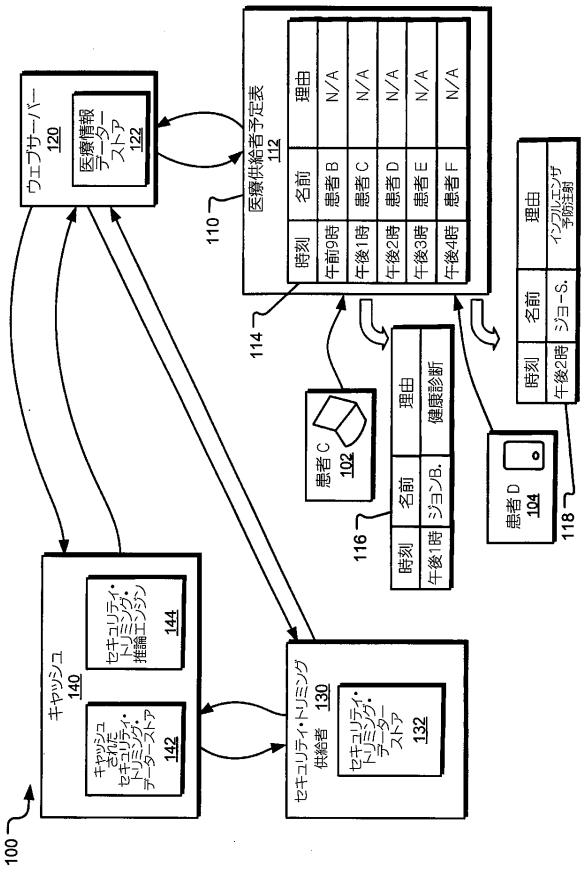
【００６０】

[0066] 本明細書において説明した発明の実施形態は、１つ以上のコンピューター・システムにおける論理ステップとして実現される。本発明の論理動作は、（１）１つ以上の計算システムにおいて実行するプロセッサー実施ステップのシーケンスとして、（２）計算システム内において相互接続された機械または回路モジュールとして実現される。実施態様は、本発明を実現する計算システムの性能要件に依存する選択事項である。したがって、本明細書において記載された発明の実施形態を構成する論理動作は、処理(operation)、構造的デバイス、動作(act)、またはモジュールと様々に呼ばれる。更に、別段明示的に特許請求されないなら、または特定の順序が請求項の文言によって本質的に必要とされないなら、論理動作はいずれの順序で実行してもよいことは、理解されてしかるべきである。

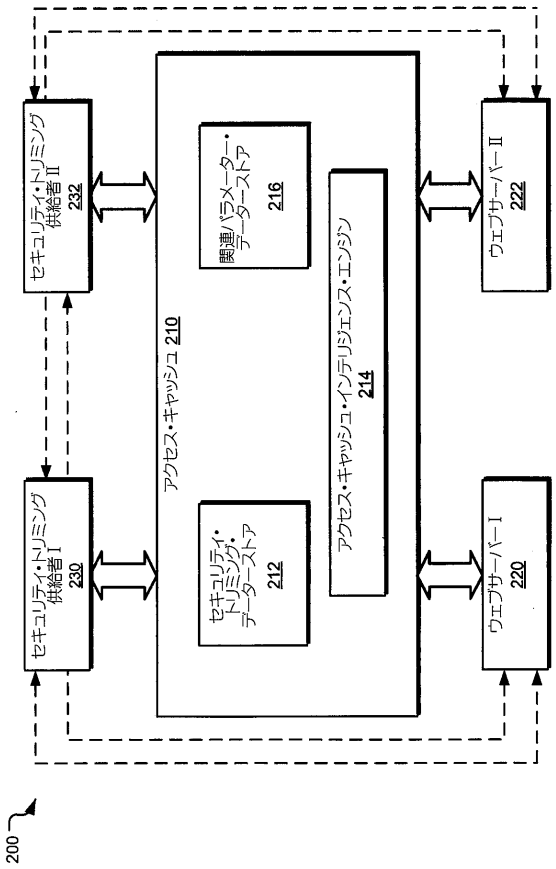
【００６１】

[0067] 以上の明細書、例、およびデーターは、本発明の組成(composition)の製造および使用の完全な説明に考慮している。本発明の主旨および範囲から逸脱することなく、本発明の多くの実施形態を形成することができるので、本発明は、以下に添付する特許請求の範囲に存在するものとする。更に、特許請求の範囲の記載から逸脱することなく、異なる実施形態の構造的特徴が更に他の実施形態において組み合わされてもよい。

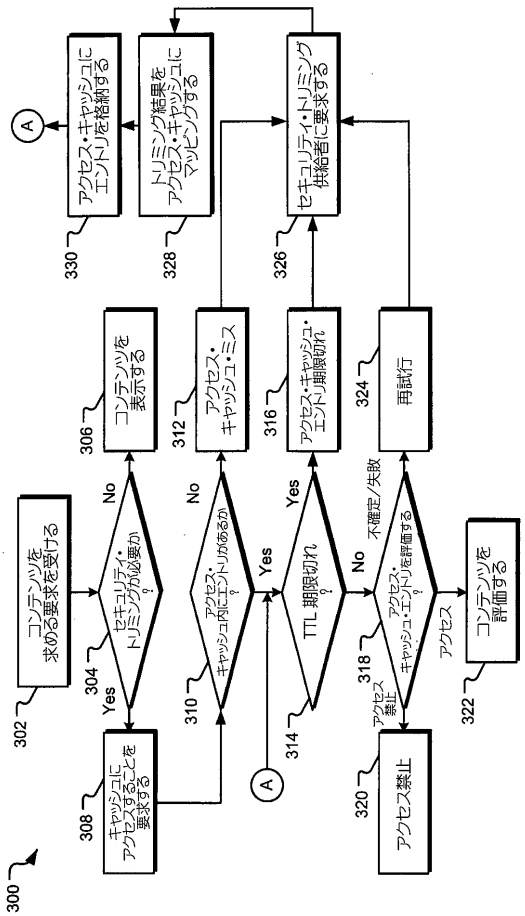
【図１】


ウェブサーバー 120
医療情報データーストア 122
医療供給者予定表 112
時刻 名前 理由
午前9時 患者B N/A
午後1時 患者C N/A
午後2時 患者D N/A
午後3時 患者E N/A
午後4時 患者F N/A
110
114
患者C 102
患者D 104
116
時刻 名前 理由
午後1時 ジョンB. 健康診断
118
時刻 名前 理由
午後2時 ジョーS. インフルエンザ予防注射
キャッシュ 140
セキュリティ・トリミング推論エンジン 144
キャッシュ済セキュリティ・トリミング・データーストア 142
セキュリティ・トリミング供給者 130
セキュリティ・トリミング・データーストア 132
100

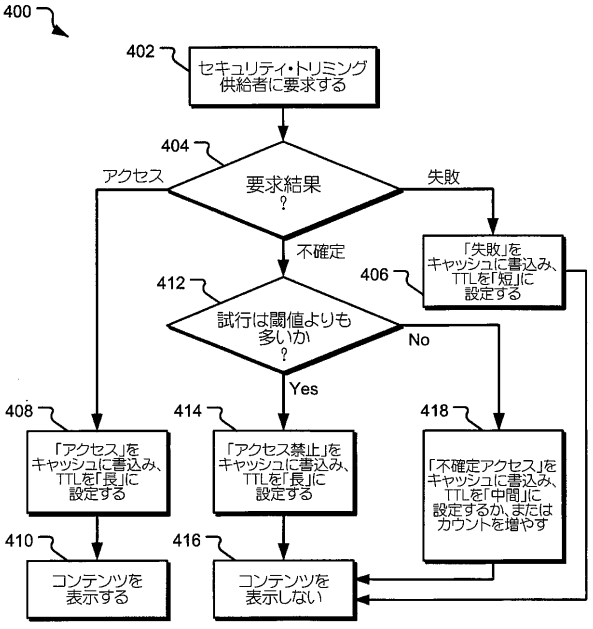
【図２】


セキュリティ・トリミング供給者II 232
アクセス・キャッシュ 210
関連パラメーター・データーストア 216
ウェブサーバーII 222
アクセス・キャッシュ・インテリジェンス・エンジン 214
セキュリティ・トリミング供給者I 230
セキュリティ・トリミング・データーストア 212
ウェブサーバーI 220
200

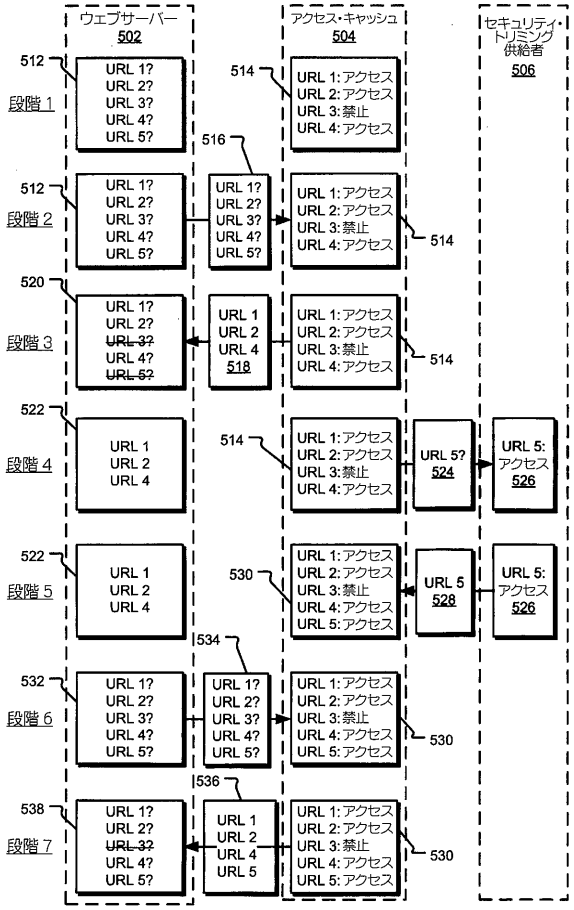
【図３】


コンテンツを求める要求を受ける
302
セキュリティ・トリミングが必要か？
304
Yes
No
キャッシュにアクセスすることを要求する
308
コンテンツを表示する
306
アクセス・キャッシュ内にエントリがあるか？
310
No
Yes
アクセス・キャッシュ・ミス
312
TTL 期限切れ？
314
No
Yes
アクセス・キャッシュ・エントリ期限切れ
316
アクセス・キャッシュ・エントリを評価する
318
不確定/失敗
アクセス禁止
320
再試行
324
アクセス
コンテンツを評価する
322
セキュリティ・トリミング供給者に要求する
326
トリミング結果をアクセス・キャッシュにマッピングする
328
アクセス・キャッシュにエントリを格納する
330
A
300

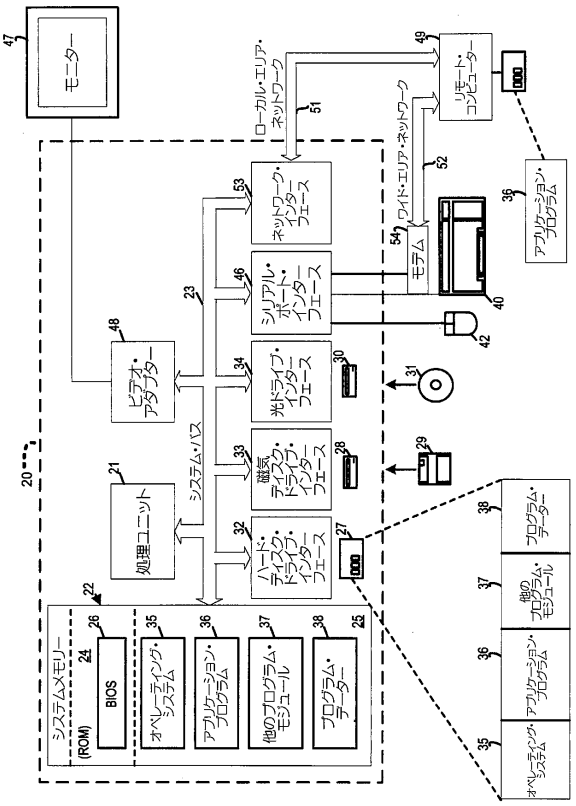
【図４】


400
402
セキュリティ・トリミング供給者に要求する
404
要求結果？
アクセス
失敗
不確定
「失敗」をキャッシュに書込み、TTLを「短」に設定する
406
412
試行は閾値よりも多いか？
No
Yes
408
「アクセス」をキャッシュに書込み、TTLを「長」に設定する
414
「アクセス禁止」をキャッシュに書込み、TTLを「長」に設定する
418
「不確定アクセス」をキャッシュに書込み、TTLを「中間」に設定するか、またはカウントアを増やす
410
コンテンツを表示する
416
コンテンツを表示しない

【図５】


ウェブサーバー
502
アクセス・キャッシュ
504
セキュリティ・アプリミング供給者
506
段階１
段階２
段階３
段階４
段階５
段階６
段階７
URL 1?
URL 2?
URL 3?
URL 4?
URL 5?
URL 1
URL 2
URL 4
URL 5
URL 1: アクセス
URL 2: アクセス
URL 3: 禁止
URL 4: アクセス
URL 5: アクセス
URL 5?
524
URL 5
528
512
514
516
518
520
522
526
530
532
534
536
538

【図６】


モニター
ローカル・エリア・ネットワーク
リモート・コンピューター
ネットワーク・インターフェース
ワイド・エリア・ネットワーク
モデム
アプリケーション・プログラム
シリアル・ポート・インターフェース
ビデオ・アダプター
光ドライブ・インターフェース
磁気ディスク・ドライブ・インターフェース
ハード・ディスク・ドライブ・インターフェース
システム・バス
処理ユニット
システムメモリー
(ROM)
BIOS
オペレーティング・システム
アプリケーション・プログラム
他のプログラム・モジュール
プログラム・データー
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
40
42
46
47
48
49
51
52
53
54

フロントページの続き

(74)代理人 100153028
弁理士 上田 忠
(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100196508
弁理士 松尾 淳一
(74)代理人 100147991
弁理士 鳥居 健一
(74)代理人 100119781
弁理士 中村 彰吾
(74)代理人 100162846
弁理士 大牧 綾子
(74)代理人 100173565
弁理士 末松 亮太
(74)代理人 100138759
弁理士 大房 直樹
(72)発明者 ロム，ロバート
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 ワイルド，ベンジャミン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 タヴィス，マイケル
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 エフドキーモフ，アレクセイ
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 シャー，スィッダールト・アール
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 ナルラ，プニート
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ

審査官 青木 重徳

(56)参考文献 特開２００７－４６９４（ＪＰ，Ａ）
特開２００９－１５１５３３（ＪＰ，Ａ）
米国特許出願公開第２００８／０１７２３７７（ＵＳ，Ａ１）
米国特許出願公開第２００８／０２４３６９９（ＵＳ，Ａ１）
米国特許出願公開第２０１０／００１７８７６（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ １２／００
Ｇ０６Ｆ ２１／１０