(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5346374号
(P5346374)
(45)発行日　平成25年11月20日(2013.11.20)　(24)登録日　平成25年8月23日(2013.8.23)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 560A

請求項の数 20　(全 20 頁)

(21)出願番号	特願2011-523887 (P2011-523887)
(86)(22)出願日	平成21年8月14日 (2009.8.14)
(65)公表番号	特表2012-500441 (P2012-500441A)
(43)公表日	平成24年1月5日 (2012.1.5)
(86)国際出願番号	PCT/US2009/053851
(87)国際公開番号	WO2010/021926
(87)国際公開日	平成22年2月25日 (2010.2.25)
審査請求日	平成24年7月3日 (2012.7.3)
(31)優先権主張番号	12/193,587
(32)優先日	平成20年8月18日 (2008.8.18)
(33)優先権主張国	米国 (US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
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
(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
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】ウェブページプライバシーリスク保護方法及びシステム

(57)【特許請求の範囲】
【請求項１】
ウェブページに関連付けられているＨＴＭＬコードを受信するステップと、
前記ウェブページにコンテンツを提供している一つ以上の第三者を識別するために前記ＨＴＭＬコードを処理するステップと、
個々に識別された第三者に対し、前記第三者がコンテンツを提供している１つ以上のウェブページに前記第三者を関連付けるためのデータをストアするステップと、
特定の第三者が、前記特定の第三者に関連しストアされているデータに従ってユーザーの閲覧傾向を観測できる立場にあるか否か検出するステップと、
前記検出するステップに応答し前記ユーザーが、前記特定の第三者からのコンテンツに関して１つ以上の動作を前記ユーザーに実行させ得るユーザーインターフェース手段を出力するステップと、を含む計算機実行方法。
【請求項２】
前記検出するステップ及び出力するステップが、ウェブブラウザーによって実行されることを特徴とする請求項１記載の計算機実行方法。
【請求項３】
前記ユーザーインターフェース手段が、ポップアップウィンドウを含むことを特徴とする請求項１記載の計算機実行方法。
【請求項４】
前記ユーザーインターフェース手段が、前記コンテンツをブロックするか又は許可する

か指定するための入力を前記ユーザーに提供できる１つ以上の選択可能なボタンを含むことを特徴とする請求項１記載の計算機実行方法。
【請求項５】
前記ユーザーインターフェース手段が、前記特定の第三者に関する付加的な情報を前記ユーザーが取得できる選択可能なリンクを含むことを特徴とする請求項１記載の計算機実行方法。
【請求項６】
前記選択可能なリンクが選択されたとき、前記特定の第三者から前記付加情報を前記ユーザーが取得できるように前記特定の第三者のウェブサイトへリダイレクトさせることを特徴とする請求項５記載の計算機実行方法。
【請求項７】
前記検出するステップが、異なるウェブページに前記特定の第三者が関連付けられるたびに、前記特定の第三者に関連付けられているカウンターを増やすステップを含むことを特徴とする請求項１記載の計算機実行方法。
【請求項８】
更に、
前記ユーザーインターフェース手段を介し前記ユーザーからの入力を受信するステップと、
前記ユーザーからの前記入力に従って、前記特定の第三者からの前記コンテンツをブロックするか又は許可するステップと、を含む請求項１記載の計算機実行方法。
【請求項９】
ウェブページに関連付けられているＨＴＭＬコードを受信するステップと、
前記ウェブページに含まれている第三者のコンテンツソースからのコンテンツを識別するために前記ＨＴＭＬコードを処理するステップと、
前記第三者のコンテンツソースからのコンテンツが、アプリケーションによってナビゲートされたウェブページにおいて遭遇した回数を計算するステップと、
計算された回数に基づいて、前記第三者のコンテンツのソースが、前記アプリケーションの前記ユーザーの閲覧傾向を観測できる立場にあるか否か確認するステップと、を含む計算機実行方法。
【請求項１０】
更に、前記確認するステップに応答し、検出された第三者のコンテンツソースの前記ユーザーに通知するためのユーザーインターフェース手段を出力するステップを含む請求項９記載の計算機実行方法。
【請求項１１】
更に、
前記計算された回数に基づいて、知覚された危険水準を第三者のコンテンツソースに割り当てるステップと、
前記検出された第三者のコンテンツソースの前記ユーザーに通知するための前記ユーザーインターフェース手段出力を介し、前記知覚された危険水準を提示するステップと、を含む請求項１０記載の計算機実行方法。
【請求項１２】
前記ユーザーインターフェース手段が、前記アプリケーションのメニューバー内にメニューバー項目形式で出現することを特徴とする請求項１０記載の計算機実行方法。
【請求項１３】
更に、前記確認するステップに応答し、前記検出された第三者のコンテンツソースに関する行動を前記ユーザーが実行できる複数の選択可能な部分を有するユーザーインターフェース手段を出力するステップであって、前記複数の選択可能な部分が、
前記第三者のコンテンツソースからのコンテンツをブロックするための選択可能なボタンと、
前記第三者のコンテンツソースからのコンテンツを許可するための選択可能なボタンと

、を少なくとも含む請求項９記載の計算機実行方法。
【請求項１４】
前記アプリケーションが、ウェブブラウザーであることを特徴とする請求項９記載の計算機実行方法。
【請求項１５】
前記確認するステップが、前記第三者のコンテンツソースからのコンテンツが遭遇した前記計算された回数を、知覚された危険水準を示す１つ以上の閾値と比較するステップを含むことを特徴とする請求項９記載の計算機実行方法。
【請求項１６】
１つ以上の処理装置と、
１つ以上の計算機可読記憶媒体と、
前記１つ以上の計算機可読記憶媒体上に具体化された計算機可読命令であって、前記１つ以上の処理装置によって実行されるとき、
第三者のコンテンツソースが、ウェブブラウザーによってナビゲートされるウェブページに対するコンテンツを提供する回数を計算し、
計算された回数に基づいて、前記第三者のコンテンツソースがユーザーの閲覧傾向を観測できる立場にあるときを決定し、
前記第三者のコンテンツソースが、前記ユーザーの閲覧傾向を観測できる立場にあることを通信するための通知を出力するように、前記ウェブブラウザーを動作させるもの、を含むシステム。
【請求項１７】
前記ウェブブラウザーが、ポップアップウィンドウとして前記通知を出力することを特徴とする請求項１６記載のシステム。
【請求項１８】
前記ウェブブラウザーが、前記ウェブブラウザーのメニューバー項目として前記通知を出力することを特徴とする請求項１６記載のシステム。
【請求項１９】
前記出力される通知が、閲覧傾向を観測できる立場にあることを決定された前記第三者のコンテンツソースをユーザーが許可、ブロック、又は無視できる複数の選択可能部分を含むことを特徴とする請求項１６記載のシステム。
【請求項２０】
前記ウェブブラウザーが、更に、
第三者のコンテンツソースからの複数のコンテンツ項目とのウェブページにおける遭遇を記述しているデータベースを維持し、前記データベースが、前記コンテンツ項目と遭遇するウェブページと、前記コンテンツ項目それぞれのユニフォーム・リソース・インジケーター（ＵＲＩ）とを一致させるためのデータをストアするように構成されているものと、
前記第三者のコンテンツソースがウェブページにコンテンツを提供する前記計算された回数に達した前記コンテンツ項目のＵＲＩの類似性に関する少なくとも一部に基づいて、前記データベース内のコンテンツ項目をマージするように動作することを特徴とする請求項１６記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ウェブシステムに関し、具体的には、ウェブシステムのウェブページ利用時のプライバシーリスク保護に関する。
【背景技術】
【０００２】
[0001]ウェブページは、ユーザーにとって有用であり得、多くの異なるタイプのコンテンツを含み得る。典型的なウェブページは、様々な固有のコンテンツ（例えば、ウェブペ

ージの本来のプロバイダーからの直接的なコンテンツ）と、１つ以上の第三者のコンテンツソースからの第三者のコンテンツと、から構成され得る。例えば、ニュースウェブページは、ニュースプロバイダーからのニュース記事、リンク、及び画像などの固有コンテンツ、並びに様々な第三者のコンテンツソースから提供される広告、リンク、（スポーツチッカー、気象トラッカーなどの）プラグインのような第三者のコンテンツなど、を含むように構成され得る。

【０００３】

[0002]ニュースウェブページを見るためにブラウザーをナビゲートするユーザーは、ニュースウェブページとの対話を意識する。しかしながら、ユーザーは、ニュースウェブページに関するコンテンツを提供している第三者のコンテンツソースとも生じる対話は意識し得ない。その上更に、複数のウェブページを介しアクセスされる第三者のコンテンツソースは、ユーザーの閲覧傾向を観測できる立場にある。かくして、第三者のコンテンツソースは、ユーザーにプライバシーリスクを提示し得る。しかし、第三者のコンテンツソースとの対話に関する知識がないユーザーは、ユーザーの閲覧傾向を観測し得るこれらの第三者のコンテンツソースに対する行動を実行できる立場にない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

本発明の目的は、プライバシーリスクをもたらし得るウェブページに関する第三者のコンテンツソースを検出するシステムを提供することである。

【課題を解決するための手段】

【０００５】

[0003]この「課題を解決するための手段」は、「発明を実施するための形態」に更に後述される概念のいくつかを簡易化した形式で紹介するために提供される。この「課題を解決するための手段」は、請求対象項目の重要な機能も本質的な特徴も特定するように意図されておらず、請求対象項目の範囲を限定するために利用されることも意図されていない。

【０００６】

[0004]様々な実施形態が、ユーザーにプライバシーリスクをもたらす第三者のコンテンツソースの検出を可能にする。少なくともいくつかの実施形態の中には、ブラウザーを介しナビゲートされるウェブページが処理され得、ウェブページにコンテンツを提供している第三者のコンテンツソースを識別する。第三者のコンテンツと遭遇するウェブページを第三者のコンテンツソースに関連付けるデータがストアされる。データはその後、解析され、特定の第三者がユーザーの閲覧傾向を観測できる立場にあるときを決定し得る。一例において、同一のコンテンツ及び／又は第三者のコンテンツソースに関連付けられたウェブページの数が、構成可能な閾値を超えたとき、プライバシーリスクが決定される。プライバシーリスクの決定に応答し、潜在的な危険を伴うコンテンツをユーザーに知らせるための通知が様々な方法で出力され得る。

【０００７】

[0005]別の少なくともいくつかの実施形態の中には、ユーザーに自動的に提示される通知が、ユーザーインターフェース手段を介し実行され得、潜在的な危険を伴う第三者のコンテンツソースをユーザーに知らせ得るものもある。場合によっては、ユーザーインターフェース手段が、ウェブページに関する危険を伴う第三者のコンテンツに遭遇したとき自動的に提示される警告メッセージ形式であるものもある。更に、ユーザーインターフェース手段が場合によっては、第三者のコンテンツソースからのコンテンツをブロックするか又は許可するような様々な動作を実行するための選択可能な機能性にユーザーがアクセスできる１つ以上の選択可能な部分を組み込み得るものもある。

【０００８】

[0006]

同様の特徴を参照するために同一の数字が図面内で使用されている。

【図面の簡単な説明】
【０００９】
【図１】[0007]１つ以上の実施形態による本発明の原理が使用され得る動作環境を例示している。
【図２】[0008]１つ以上の実施形態による方法のステップを説明する流れ図である。
【図３】[0009]１つ以上の実施形態による方法のステップを説明する流れ図である。
【図４】[0010]１つ以上の実施形態によるウェブブラウザーユーザーインターフェースを例示している。
【図５】[0011]１つ以上の実施形態によるウェブブラウザーユーザーインターフェースを例示している。
【図６】[0012]１つ以上の実施形態によるシステムブロック図である。
【発明を実施するための形態】
【００１０】
概要
[0013]様々な実施形態は、ユーザーにプライバシーリスクをもたらす第三者のコンテンツソースの検出を可能にする。少なくともいくつかの実施形態の中には、ブラウザーを介しナビゲートされるウェブページが処理され得、ウェブページにコンテンツを提供する第三者のコンテンツソースを識別するものもある。第三者のコンテンツと遭遇するウェブページに第三者のコンテンツソースを関連付けるためのデータがストアされ得る。データは、その後、解析され、特定の第三者がユーザーの閲覧傾向を観測できる立場にあるときを決定し得る。一例において、同一のコンテンツに関連付けられたウェブページ及び／又は第三者のコンテンツソースの数が、構成可能な閾値を超えたとき、プライバシーリスクが決定される。プライバシーリスクの決定に応答し、潜在的な危険を伴うコンテンツをユーザーに知らせるための通知が様々な方法によって出力され得る。
【００１１】
[0014]別の少なくともいくつかの実施形態の中には、潜在的な危険を伴う第三者のコンテンツソースをユーザーに知らせるための通知が、ユーザーに自動的に提示されるユーザーインターフェース手段を介し、実行され得るものもある。ユーザーインターフェース手段は、場合によっては、ウェブページの危険を伴う第三者のコンテンツが遭遇したときに自動的に提示される通知メッセージ形式で常駐し得る。更に、ユーザーインターフェース手段は、場合によっては、様々な第三者のコンテンツソースからのコンテンツをブロックするか又は許可するような動作を実行するための機能性にユーザーがアクセスできる選択可能な１つ以上の選択可能部を組み込み得る。
【００１２】
[0015]次に続ける論述において、「動作環境」と題するセクションは、一環境を説明しているが様々な実施形態が使用され得る。これに続いて「プライバシーリスク検出例」と題するセクションは、ウェブページの第三者のコンテンツが識別され得、プライバシーリスクが決定され得る実施形態を説明している。次に「リスク通知例」と題するセクションは、ユーザーにとって潜在的な危険を伴う第三者のコンテンツをユーザーに知らせるための通知が出力され得る実施形態を説明している。最後に「システム例」と題するセクションが提供されていて、１つ以上の実施形態を実装するために使用され得るシステム例を説明している。
【００１３】
動作環境
[0016]図１は（１００）において、１つ以上の実施形態に従った通常の動作環境を例示している。環境（１００）は、１つ以上のプロセッサー（１０４）、１つ以上の計算機可読媒体（１０６）、及び計算機可読媒体に常駐するプロセッサー（単数又は複数）によって実行可能な１つ以上のアプリケーション（１０８）を有する計算装置（１０２）を含む。アプリケーション（１０８）は、非限定の例として、リーダーアプリケーション、電子メールアプリケーション、インスタントメッセージアプリケーション、及びその他の様々

なアプリケーションのような適切な任意のタイプのアプリケーションを含み得る。
【００１４】
[0017]計算装置（１０２）は、インターネットのようなネットワーク（１１２）を介し、そこからコンテンツが受信され、そこへ送信される１つ以上のウェブサイト（１１４）へナビゲートするための、計算装置（１０２）のユーザーが利用可能な機能性を提供するウェブブラウザー（１１０）形式のアプリケーション（１０８）を含む。ウェブブラウザー（１１０）は、様々なユーザーインターフェース（１１６）を提供するように作動し得、それを介しユーザーは１つ以上のウェブサイト（１１４）から利用可能なコンテンツと対話し得る。
【００１５】
[0018]ウェブサイト（１１４）は、本来のコンテンツソース及び第三者のコンテンツソースを含み得る。本明細書に使用される本来のコンテンツソースは、ユーザーが肯定的及び／又は意図的にナビゲートされるウェブサイト（１１４）に関連付けられたドメインからのコンテンツソースを参照する。本来のコンテンツソースは、ブラウザーがユーザーによって方向付けられるユニフォーム・リソース・インジケーター（ＵＲＩ）ドメインと緊密な関係を有していて、及び／又はそのドメインプロバイダーと同一のプロバイダーを有し得る。本明細書に使用されている第三者のコンテンツソースは、本来のコンテンツソース以外のコンテンツソースである。言い換えると、第三者のコンテンツソースは、ブラウザーがユーザーによって方向付けられたドメインの外部からのソースであって、通常、ドメインのプロバイダーと異なるプロバイダーを有し得る。
【００１６】
[0019]更に、ウェブブラウザー（１１０）は、前述及び後述したように作動するプライバシーモジュール（１１８）を含み得るか又はそうでなければ利用し得る。プライバシーモジュール（１１８）は、１つ以上のウェブサイト（１１４）と対話するときにユーザーに提供され得る様々なプライバシー機能を代表している。例えば、プライバシーモジュール（１１８）は、ウェブサイト（１１４）から取得されるウェブページコンテンツを提供している第三者のコンテンツソースの識別を可能にし得る。プライバシーモジュール（１１８）は、第三者のコンテンツソースによって提示されるプライバシーリスクも決定し得る。具体的には、プライバシーモジュール（１１８）は、第三者のコンテンツソースが計算装置（１０２）のユーザーの閲覧傾向を観測できる立場にあるときを決定するように作動し得る。
【００１７】
[0020]実施形態において、プライバシーモジュール（１１８）の機能性は、様々なサブモジュールを介し提供され得る。図１の例において、プライバシーモジュール（１１８）は、ログ記録モジュール（１２０）及び検出モジュール（１２２）を含むように例示されている。ログ記録モジュール（１２０）は、ウェブページ内の第三者のコンテンツを識別する機能性を代表している。ログ記録モジュール（１２０）は、ウェブサイト（１１４）と関連するコンテンツとのウェブブラウザー（１１０）の対話を記述するデータを登録するか又はそうでなければ蓄積するためのデータベースも維持管理し得る。ログ記録モジュール（１２０）を介し蓄積された様々なデータは、図１に例示したようなデータストア（１２４）に維持管理され得る。
【００１８】
[0021]検出モジュール（１２２）は、ログ記録モジュール（１２０）によって様々な方法で蓄積されたデータを処理するために作動可能な機能性を代表している。この処理を介し、検出モジュール（１２２）は、第三者のコンテンツソースとウェブブラウザー（１１０）との対話を監視し、特定の第三者のコンテンツソースが潜在的なプライバシーリスクをもたらすときを決定し得る。検出モジュール（１２２）は、更に、第三者のコンテンツが潜在的な危険を伴う決定に応答し、通知を出力させるように作動し得る。
【００１９】
[0022]計算機可読媒体（１０６）は、非限定の例として、揮発性及び不揮発性メモリー

及び／又は典型的に、計算装置に関連する記憶媒体すべての形式を含み得る。そのような媒体は、ＲＯＭ、ＲＡＭ、フラッシュメモリー、ハードディスク、取り外し可能媒体などを含み得る。特定の計算装置の一例が図６に示され、後述されている。

【００２０】

[0023]計算装置（１０２）は、非限定の例として、デスクトップコンピューター、ポータブルコンピューター、携帯情報端末（ＰＤＡ）のような携帯型計算機、携帯電話など、適切な任意の計算装置として具体化され得る。

【００２１】

[0024]動作環境の例を考察してきたので、ここで今から第三者のコンテンツソースからのコンテンツに関連するプライバシーリスクを検出し得る実施形態の論述を考えられたい。

【００２２】

プライバシーリスク検出例

[0025]１つ以上の実施形態において、ウェブページ上に出現するコンテンツに関連する第三者のコンテンツソースを識別する技法が使用され得る。前述したように、第三者のコンテンツソースからのコンテンツと遭遇するウェブページに第三者のコンテンツソースを関連付けるための様々なデータが蓄積され、ストアされ得る。第三者のコンテンツソースとウェブページとを関連付けているデータが処理され、プライバシーリスクをもたらす、それらの第三者のコンテンツソースを検出し得る。

【００２３】

[0026]図２は、１つ以上の実施形態による方法のステップを説明している流れ図である。本方法は、適切な任意のハードウェア、ソフトウェア、ファームウェア、又はその組み合わせと関連し実行され得る。少なくともいくつかの実施形態の中には、図１に前述したウェブブラウザー（１１０）のような適切に構成されたウェブブラウザーによる方法が実行され得るものもある。

【００２４】

[0027]ステップ（２００）が、ウェブページに関連付けられているＨＴＭＬコードを受信する。このステップは、ウェブブラウザーが特定のウェブページへナビゲートしたときに実行され得る。ステップ（２０２）がＨＴＭＬコードを処理し、ステップ（２０４）が第三者のコンテンツソースからのウェブページのコンテンツを識別する。このステップは、適切な任意の方法で実行され得る。例えば、ウェブページに関連付けられているＨＴＭＬコードが、ユーザーが契約し得るウェブページに含まれているコンテンツを識別し得る。これが実行され得る方法に関する一例は、ＨＴＭＬコードに埋め込まれているコンテンツのＨＴＭＬタグ、ＵＲＩ、及びその他適切な識別子を介することである。識別は、ＨＴＭＬコードの処理がウェブページに包含するためのコンテンツをダウンロードするためのリクエストをもたらすときには常に、生じ得る。

【００２５】

[0028]前述したように、ウェブページのコンテンツは、本来のコンテンツソース及び第三者のコンテンツソース双方から提供され得る。かくして、ステップ（２０４）において識別は、本来のコンテンツソースと第三者のコンテンツソースとの間の区別を含み得る。１つ以上の実施形態において、リクエストしたコンテンツの経路と、コンテンツが現れるウェブページの経路との間の比較が実行され得、リクエストしたコンテンツのソースが、同一ドメイン内にあるか否か、及び／又はウェブブラウザーが向けられた先のウェブページと同一のプロバイダーを有しているか否か、を決定し得る。ドメイン及び／又はプロバイダーが異なることが決定されたとき、リクエストされているコンテンツが、第三者のコンテンツソースからのコンテンツとして識別され得る。

【００２６】

[0029]１つ以上の第三者のコンテンツソースの識別に応答し、ステップ（２０６）が、１つ以上の第三者のコンテンツソースをウェブサイトに関付けるためのデータをストアする。その後、ステップ（２０８）が、１つ以上の第三者のコンテンツソースとの対話を監

視し、潜在的なプライバシーリスクを決定する。

【００２７】

[0030]例えば、第三者のソースからのコンテンツの識別に基づいて図１のデータストア（１２４）内のログなどのデータが、データベースにおいて蓄積され、ストアされ得る。第三者コンテンツソースが最初、識別されたとき、第三者のコンテンツソースに関するレコードがデータベースに追加され得る。レコードが、第三者のコンテンツソースを第三者のコンテンツソースからのコンテンツと遭遇するウェブサイトに関連付ける。その後、データベースのレコードは、ウェブブラウザーによって第三者のコンテンツソースと遭遇するたびに更新され得、ブラウザーがナビゲートされる先の別のおそらくウェブページの更なる遭遇を反映する。

【００２８】

[0031]１つ以上の実施形態において、データベースに維持保守されているレコードは、第三者のコンテンツソースが異なるウェブサイト／ドメインと遭遇した回数に関するログを記録するか又はそうでなければトラッキングするように作動する。例えば、特定の第三者のコンテンツソースに関するレコードは、特定の第三者のコンテンツソースが異なるウェブサイト及び／又はドメインと遭遇するたびに増加され得るカウンターフィールドを含む。第三者のコンテンツソースと遭遇した回数は、第三者のコンテンツソースがユーザーにどのくらいのプライバシーリスクを提示するか決定する基盤であり得る。

【００２９】

[0032]ウェブページにおいて遭遇する特定の第三者のコンテンツソースは、ウェブブラウザー（１１０）を介し出力されるものとして考慮されたい。第三者のコンテンツソースと遭遇したとき、プライバシーモジュール（１１８）などのウェブブラウザー（１１０）は、第三者のコンテンツソースに関するレコードが存在するか否か決定するためにデータストア（１２４）を参照し得る。レコードが既に存在していると仮定すると、ウェブブラウザー（１１０）は更に、第三者のコンテンツソースが既にウェブページに関連付けられているか否か決定するように作動する。第三者のコンテンツソースが既にウェブページと関連付けられていないと仮定すると、ウェブブラウザー（１１０）はレコードを更新し得、更なる遭遇を反映し得、第三者のコンテンツソースが異なるウェブサイト及び／又はドメインと遭遇した回数を示し得るレコードに関連付けられているカウンターも増やし得る。

【００３０】

[0033]１つ以上の実施形態において、ウェブブラウザーは、第三者のコンテンツソースと遭遇する回数に関する少なくとも一部に基づいて、第三者のコンテンツソースによって提示されるリスクを決定する。今説明したように、カウンターを増やすことは、ウェブブラウザーがその回数に達し得るやり方の一例である。例えば、コンテンツ項目「ｓｏｕｒｃｅ１．ｘｙｚ．ｆｏｏ．ｊｓ」がサイトＡ及びサイトＢ双方で遭遇した場合、「ｓｏｕｒｃｅ１．ｘｙｚ．ｆｏｏ．ｊｓ」のソースは、少なくともウェブブラウザーがサイトＡ及びサイトＢを訪問したことを知る十分な情報を有している。ＩＰアドレス、ブラウザーの設定、優先順位などの別の情報も第三者のソースとの対話を介し交換され得る。この例において、カウンターの値は、「ｓｏｕｒｃｅ１．ｘｙｚ．ｆｏｏ．ｊｓ」が遭遇した異なるサイト数に相当する「２」に設定される。

【００３１】

[0034]１つ以上の実施形態において、ウェブブラウザーは、カウンターの値（例えば異なるサイト数）を知覚された１つ以上の危険水準に関連付けるために使用され得る構成可能な閾値を実装し得る。異なる危険水準に関連付けられる単一の閾値か又は複数の範囲の値が使用される。非限定の例として、以下の表１は、知覚された危険水準を決定するために使用される異なる危険水準に関連付けられた複数範囲の値の一例を提供している。

【００３２】

【表１】

表１：知覚された危険水準　対　第三者の遭遇

危険水準	遭遇回数
低	０～５
中	６～１０
高	１１以上

【００３３】

[0035]かくして、前述及び後述した方法によって、図１に前述したウェブブラウザー（１１０）のような適切に構成されたウェブブラウザーが、第三者のコンテンツソースとの対話を監視し、第三者のコンテンツソースに関連付けられているプライバシーリスクを決定し得る。以下、図３の論述は、第三者のコンテンツソースに関連付けられているプライバシーリスクを決定するために使用され得る付加的な技法の例を提供している。

【００３４】

[0036]図３は、１つ以上の実施形態に従った方法のステップを説明する流れ図である。本方法は、適切な任意のハードウェア、ソフトウェア、ファームウェア、又はその組み合わせに関連し実行され得る。少なくともいくつかの実施形態の中には、本方法が前述した図１のウェブブラウザー（１１０）のような適切に構成されたウェブブラウザーによって実行され得るものもある。

【００３５】

[0037]ステップ（３００）が、ウェブページにおいて遭遇した第三者のコンテンツソースを識別する。このステップは、適切な任意の方法によって実行され得る。このステップは、ウェブブラウザーが特定のウェブページのＨＴＭＬコードを処理し、１つ以上のコンテンツソースからコンテンツをダウンロードするリクエストを生成するとき、実行され得る。例えば、ウェブページに関連付けられているＨＴＭＬコードが、ウェブページに含まれるコンテンツを識別し得る。これが実行され得る方法の一例は、ＨＴＭＬタグ、ＵＲＩ、及びＨＴＭＬコードに埋め込まれているコンテンツの別の適切な識別子を介することである。少なくともいくつかの実施形態の中には、第三者のコンテンツの識別が、代替としてウェブページがレンダリングされた後に生じ得るものもある。この技法は、ウェブページをレンダリングし、性能損失に対応している間のリソース処理の消費を回避するために使用され得る。

【００３６】

[0038]ステップ（３０２）は、第三者のコンテンツソースにウェブページを関連付けるために維持保守されているデータベースを更新する。具体的には、図１のログ記録モジュール（１２０）などを介しウェブブラウザーが、データベース内の第三者のコンテンツソースに対応するレコードを更新し、第三者のコンテンツソースがウェブページと遭遇したことを反映し得る。第三者のコンテンツソースに関するレコードがまだ存在しない場合、新しいレコードが生成され得る。

【００３７】

[0039]その後、ステップ（３０４）がデータベースを解析し、第三者のコンテンツソースによってもたらされるプライバシーリスクを決定する。具体的には、ウェブブラウザーが、図１の検出モジュール（１２２）などを介し様々な方法によってデータベースのデータを解析し得、第三者のコンテンツソースがユーザーの閲覧傾向を観測できる立場にあるか否か決定する。

【００３８】

[0040]１つ以上の実施形態において、データベースの解析は、データベース中の同様項目を１つにまとめることを含み得る。様々なロジックが適用され得、同様の項目を１つにまとめ得る。項目を１つにまとめることは、異なるコンテンツ項目に関する経路データに基づいて実行され得る。非限定の例として、経路データは、ＵＲＩ、ファイル名、クエリー文字列、パラメーター、本来のドメイン名、及びその組み合わせを含み得る。２つのコ

ンテンツ項目に関する経路データの比較が実行され得る。コンテンツ項目が十分類似しているとき、コンテンツ項目に関するデータが一緒に分類され得、プライバシーリスクを提示している第三者のコンテンツソースか否か決定し得る。

【００３９】

[0041]例えば、ｈｔｔｐ：／／ｗｗｗ．ｔｒａｃｋｕ．ｃｏｍ／１２３４／ｆｏｏ．ｊｓの経路を有する１つの第三者のコンテンツ項目と、ｈｔｔｐ：／／ｗｗｗ．ｔｒａｃｋｕ．ｃｏｍ／５６７８／ｆｏｏ．ｊｓの経路を有する第２の第三者のコンテンツ項目と、を考慮されたい。この例において、ドメイン「ｗｗｗ．ｔｒａｃｋｕ．ｃｏｍ」及びファイル名「ｆｏｏ．ｊｓ」は同一である。これらの類似性に基づいてデータベースを解析するために適用されるロジックが、２つの項目に関するデータを１つにまとめ得る。具体的には、双方のコンテンツ項目が、同一の第三者のコンテンツソース、例えば、「ｗｗｗ．ｔｒａｃｋｕ．ｃｏｍ」に関連付けられ得る。同様の項目を１つにまとめるための様々な異なる技法及びアルゴリズムが想定される。

【００４０】

[0042]１つ以上の実施形態において、データベース解析は、第三者のコンテンツソース及び／又は項目と遭遇した回数を決定することも含み得る。回数を決定する一例は、既に説明したように、第三者のコンテンツソースが異なるウェブサイト及び／又はドメインと遭遇するたびに、カウンターフィールドを増やすことによるものである。通常、カウントが多ければ多いほど、潜在するプライバシーリスクが高い。第三者のコンテンツソース及び／又は項目と遭遇した回数に達する適切な様々なアルゴリズムが想定されている。非限定の例として使用され得るリスク検出のアルゴリズムの一例が以下、表２に提供されている。

【００４１】

表２：リスク検出アルゴリズム例

コンテンツを本来のウェブサイト「ｆ」に提供したとき、所与のデータベース「ｄ」、本来のウェブサイト「ｆ」、及び第三者のコンテンツソース「ｔ」が識別され、データがペア（ｆ，ｔ）として「ｆ」と「ｄ」とを関連付ける「ｄ」にストアされ得る。

【００４２】

【表２】

```
Select all third parties from d where tracker.FQDN equals t.FQDN
    If third parties is empty, add t as a new item to d, with a count of 1.
    Else
        For each third party T in third parties
            If T matches the regex "t.FQDN/.*\/t.filename"
                Set Boolean match equal to false
                For each primary website F in T.PrimaryWebSites
                    If f equals F
                        Set match equal to true
                If match equals false
                    Add f to T. PrimaryWebSites
                    Increment T. PrimaryWebSites
                Else discard (f,t) and quit
            Else discard (f,t) and quit
```

【００４３】

[0043]データベース解析に基づいてステップ（３０６）が、第三者のコンテンツソース

がプライバシーリスクをもたらすか否か決定する。これが実行され得る方法に関する一例は、前述した１つ以上の閾値を介することである。ステップ（３０６）において、十分なプライバシーリスクが決定されなかったとき、ステップ（３０８）は、プライバシーリスクを検出するウェブページ及び／又は第三者のソースを監視し続ける。例えば、更なるウェブページがウェブブラウザーを介しレンダリングされたとき、前述及び後述した様々な技法が使用され得、これらのウェブページにおいて遭遇した第三者のコンテンツソースからプライバシーリスクを検出し得る。

【００４４】

[0044]ステップ（３０６）において、十分なプライバシーリスクが決定されると、ステップ（３１０）がユーザーに知らせるプライバシーリスクの通知を出力する。第三者のコンテンツソースによってもたらされるリスクをユーザーに知らせ得る適切な任意の通知が使用され得る。１つ以上の実施形態において、潜在的な危険があることが決定された第三者のコンテンツソースをユーザーに知らせるための通知が、ユーザーインターフェース手段を介し実行され得、自動的にユーザーに提示される。少なくともいくつかの実施形態の中には、ユーザーインターフェース手段が自動的に潜在的な危険を伴う第三者のコンテンツソースの検出に応答し出力されるポップアップウィンドウ又はダイアログボックス形式で出力され得るものもある。別の実施形態において、ウェブブラウザーのメニューバー内に出現し得るメニューバー項目形式の通知が出力され得る。出力され得る適切ないくつかの通知例に関する更なる議論が「リスク通知例」と題するセクション以下において見出され得る。

【００４５】

[0045]１つ以上の実施形態において、通知を出力するためのユーザーインターフェース手段は、第三者のコンテンツソースに関する行動をユーザーが実行できる１つ以上の選択可能な部分を含み得る。例えば、ポップアップウィンドウ又はダイアログボックス形式の通知は、ユーザーによって選択できる１つ以上の選択可能なボタン又は適切な別のコントロールを含み得、第三者のコンテンツソースからのコンテンツをブロックするか及び／又は許可するために作動可能な機能性にユーザーがアクセスできる。かくして、ユーザーは、ユーザーインターフェース手段との対話を介し、潜在的な危険を伴う第三者のコンテンツソースに対する様々な動作を起動する入力を提供し得る。

【００４６】

[0046]ステップ（３１２）が、潜在的な危険を伴う第三者のコンテンツソースの通知に応答し、受信され得るユーザー入力を決定する。第三者のコンテンツソースを許可するためのユーザー入力が受信されたとき、ステップ（３１４）が、第三者のコンテンツソースコンテンツを許可する。同様に、第三者のコンテンツソースブロックするためのユーザー入力が受信されたとき、ステップ（３１６）が、第三者のコンテンツソースからのコンテンツをブロックする。

【００４７】

[0047]コンテンツの許可及びブロックグが生じ得る一方法は、ウェブブラウザーによって許可され、ブロックされるコンテンツソースを記述している１つ以上のコントロールリストを介するものである。特定の第三者のコンテンツソースがブロックされるか又は許可されるか否か示すためのコントロールリストは、受信されるユーザー入力に基づいて更新され得る。１つ以上の実施形態において、コントロールリストは、ユーザーの閲覧傾向に従って、ユーザーによって投入され得る。したがって、いくつかの従来システムにおいて使用されるときに、事前投入されるコントロールリストを生成し維持管理する時間及び費用は、回避され得る。説明した実施形態に従ったコントロールリストは、図１に示したデータストア（１２４）のようなデータベースに維持管理され得る。ウェブブラウザーは、コンテンツをレンダリングするとき、コントロールリストを参照し利用し得、コントロールリストに指定された許可及び／又はブロックされたコンテンツに従った動作をし得る。

【００４８】

[0048]コンテンツを許可するか又はブロックするユーザー入力が上記の例に記載されて

いるが、潜在的な危険を伴うものとして検出された第三者のコンテンツソースに関し別の様々なユーザー入力及び対応する動作が使用され得ることが想定される。非限定の例として、適切なユーザー入力を介し開始され得る別の動作の例は、第３のコンテンツに関する詳細情報を取得することと、コンテンツに関するリマインダーを設定することと、推薦用にソーシャルネットワークにアクセス及び／又は通知を無視する（例えばどんな更なる行動を実行しない）ことと、を含み得る。

【００４９】

[0049]潜在的な危険を伴う第三者のコンテンツの検出が生じ得る実施形態例を説明してきたので、ここで今、潜在的な危険を伴う第三者のコンテンツソースの通知がユーザーへ出力され得る別の実施形態を考慮されたい。具体的には、今から後述する実施形態において、ユーザーインターフェース例が記載されていて、潜在的な危険を伴う第三者のコンテンツソースの検出に応答し出力され得るリスク通知の読み手の利益に関する具体例を提供する。

【００５０】

リスク通知例

[0050]既に論じたように、ウェブブラウザーは、閲覧傾向を観測できる立場にあり得る第三者のコンテンツソース、例えば、潜在的な危険を伴う第三者のコンテンツソースを検出するための様々な前述及び後述した技法を実装し得る。この検出に応答し、潜在的な危険を伴う第三者のコンテンツソースをユーザーに知らせるための通知が出力され得、第三者のコンテンツソースに関する行動をユーザーが実行できる。

【００５１】

[0051]図４は、（４００）において、通常のウェブブラウザーのユーザーインターフェースを例示していて、レンダリングされるウェブページ（４０２）が示されている。例示したユーザーインターフェースは、１つ以上のウェブサイト（１１４）から利用可能なコンテンツと様々なユーザー対話可能なように出力され得る図１のユーザーインターフェース（１１６）の一例に過ぎない。既に論じたように、提示されたウェブページ（４０２）は、本来のコンテンツソースと、１つ以上の第三者のコンテンツソースと、を含む様々なソースからのコンテンツを含み得る。例示した例において、「トップニュース」部分（４０４）及び様々なリンク（４０６）は、ウェブブラウザーが方向付けられている先のウェブページ（４０２）のプロバイダーなどの本来のコンテンツソースからのコンテンツを示している。自動車の画像（４０８）、ゴルフ関連広告（４１０）、及び気象情報プラグイン（４１２）は、１つ以上の第三者のコンテンツソースから取得されたウェブページ（４０２）のコンテンツを示している。

【００５２】

[0052]ウェブページ（４０２）をレンダリングするためのウェブブラウザーが、ウェブページ（４０２）に関連付けられているＨＴＭＬコードを処理し得る。前述及び後述した技法に従って適切に構成されているウェブブラウザーが、潜在的な危険を伴う第三者のコンテンツソースを検出するように作動し得る。関連付けられているウェブページのＨＴＭＬコードの処理を介したそのような検出は、少なくとも一部において生じ得る。潜在的な危険を伴うコンテンツの検出に応答し、ユーザーに知らせ潜在的な危険を伴うコンテンツに関する動作可能にするための通知が、出力され得る。

【００５３】

[0053]図５を参照すると、図４のユーザーインターフェース（４００）及びウェブページ（４０２）が再び示されている。この例において、ウェブブラウザーが、プライバシーリスクをもたらし得るウェブページ（４０２）のコンテンツを検出している。したがって、潜在的なリスクをユーザーに知らせる通知が出力されている。

【００５４】

[0054]この場合、通知の出力は、ユーザーインターフェース手段を介し提供され、ウェブブラウザーを介し表示され得るように例示されている。そのような通知を提供するための適切な任意のユーザーインターフェース手段が、使用され得る。例示した例において、

プライバシー警告を表示するためのポップアップウィンドウ（５０２）形式のユーザーインターフェース手段が存在する。より具体的にはプライバシー警告が、コンテンツ項目「ｂａｎｎｅｒａｄ．ｐｓ」が潜在的な危険を伴うものとして検出されたことを示している。この例において、項目「ｂａｎｎｅｒａｄ．ｐｓ」は、第三者のコンテンツソース、例えば「ａｄｓｅｒｖｅｒ．ｃｏｍ」から取得されたゴルフ関連広告（４１０）に対応している。通知の出力は、「ａｄｓｅｒｖｅｒ．ｃｏｍ」がユーザーが訪問した異なる複数のウェブサイトにおいて遭遇している、という決定に応答し発生している。例えば、プライバシー警告の例は、遭遇が「６」回あったことを示していて、危険水準「中」を割り当てたことを示している。遭遇回数及び危険水準の割り当ての決定は、本明細書に記載したカウンター及び構成可能な様々な閾値に従って、生じ得る。

【００５５】

[0055]ポップアップウィンドウ（５０２）は、第三者のコンテンツソースに関する行動をユーザーが実行できる様々な選択可能な部分の例を含むように示されている。具体的には、ポップアップウィンドウ（５０２）の例は、許可（Ａｌｌｏｗ）ボタン（５０４）、ブロック（Ｂｌｏｃｋ）ボタン（５０６）、無視（Ｉｇｎｏｒｅ）ボタン（５０８）、及び詳細リンク（Ｍｏｒｅ　Ｉｎｆｏ）（５１０）を含む。

【００５６】

[0056]許可ボタン（５０４）上でクリックすることによってユーザーは、項目「ｂａｎｎｅｒａｄ．ｐｓ」及び／又は「ａｄｓｅｒｖｅｒ．ｃｏｍ」が許可されたコンテンツとして識別されることをもたらすための入力を提供し得る。これが生じ得る一方法は、許可されたコンテンツコントロールリストにこれらの項目を追加することによる。同様に、ブロックボタン（５０６）上でクリックすることによってユーザーは、項目「ｂａｎｎｅｒａｄ．ｐｓ」及び／又は「ａｄｓｅｒｖｅｒ．ｃｏｍ」がブロックされるコンテンツとして識別されることをもたらすための入力を提供し得る。また一方、これは、ブロックコンテンツコントロールリストにこれらの項目を追加することによって生じ得る。無視ボタン（５０８）上でクリックすることによってユーザーは、通知の出力を無視するための入力を提供し得る。この場合、ユーザーは、コンテンツが再び遭遇する別の時までコンテンツに対する決定を延期し得る。

【００５７】

[0057]詳細リンク（５１０）は、検出された第三者のコンテンツソースに関しユーザーに知らせ、その結果、第三者のコンテンツソースを許可するか又はブロックする否か決定する際にユーザーを支援する、より多くの情報を取得し得るための機構を提供し得る。詳細リンク（５１０）を選択することによってウェブブラウザーは、潜在的な危険を伴う第三者のコンテンツソースに関する様々な情報ソースにリダイレクトされ得る。一例として、ユーザーによる詳細リンク（５１０）の選択が、様々な第三者のコンテンツソースに関する情報を収集し提供するサービスへウェブブラウザーをリダイレクトし得る。別の例において、ユーザーによる詳細リンク（５１０）の選択が、第三者のコンテンツソースに関するユーザーコミュニティからの推薦を蓄積しているソーシャルコミュニティーサイトへウェブブラウザーをリダイレクトし得る。

【００５８】

[0058]更に別の例において、ユーザーによる詳細リンク（５１０）の選択が、第三者のコンテンツソースによって提供されているウェブページへウェブブラウザーをリダイレクトし得る。この例において、第三者のコンテンツソースは機能性を提供していて、それを介し第三者のコンテンツソースは、それらがウェブページに提供しているコンテンツに関する付加的な情報を提供し得る。これが生じる一方法は、第三者のコンテンツソースからのコンテンツ、又は特定のフラグ、ＨＴＭＬタグ、付加情報が利用可能であることを示すためのその他の適切なデータと、を関連付けるＨＴＭＬコードを構成することによる。付加的な情報へのウェブブラウザーのリダイレクションをもたらすための経路の名前もコンテンツに関するＨＴＭＬコード内に埋め込まれ得る。ウェブブラウザーは、特定のフラグ、ＨＴＭＬタグ、又は利用可能な付加的な情報を示すその他の適切なデータを認識し得る

。ウェブブラウザーは、その後、第三者のコンテンツソースによって指定される経路の名前へウェブブラウザーをリダイレクトするための詳細リンク（５１０）を構築し得る。この様にして第三者のコンテンツソースは、ユーザーが第三者のコンテンツソースによって提供されるコンテンツ、第三者のコンテンツソースによって収集される情報、第三者のソースによって収集される情報がどのように使用されているかなど、より理解する際の支援をし得る。この情報に関する少なくとも一部に基づいてユーザーは、潜在的なリスクとして検出されているコンテンツ又はコンテンツソースをブロックするか又は許可するかに関する詳細な情報を得た上で決断を下し得る。

【００５９】

[0059]図５は、リスク通知を提供するための適切な別のユーザーインターフェース手段の代替例として、メニューバー項目（５１２）も示している。メニューバー項目（５１２）が、潜在的な危険を伴う１つ以上の第三者のコンテンツソースの検出に応答し、ウェブブラウザーのメニューバー内に自動的に出現し得る。メニューバー項目（５１２）が、ポップアップウィンドウ（５０２）のような別のユーザーインターフェース手段に加えるか又はその代わりに出現し得る。メニューバー項目（５１２）は、ドロップダウンボックス機能を含み得、それを用いてユーザーは対話し得、検出されたリスクに関する情報を取得し得る。例えば、メニューバー項目（５１２）とのユーザーの対話が、ポップアップウィンドウ（５０２）に提示されているような、例示した情報及びコントロールと同様のプライバシー警告表示をドロップダウンボックス内にもたらし得る。

【００６０】

[0060]ポップアップウィンドウ（５０２）及びメニューバー項目（５１２）の例が論述されているが、様々な別のリスク通知が実行され得るユーザーインターフェース手段も想定される。非限定の例として、ウェブブラウザーのタブ、ウェブブラウザー情報のウィンドウ枠、ツールバー若しくはサイドバーに出現するオペレーティングシステムメッセージ、及び／又はウェブページ内で遭遇するコンテンツに関連したリスク通知を提示するための適切な別の任意のユーザーインターフェース手段を介し、リスク通知が実行され得る。インスタントメッセージ又は電子メールのような別の通信タイプによっても通知は実行され得る。１つ以上の実施形態において、ユーザーは、潜在的な危険を伴う第三者のコンテンツソースの検出に応答し、所望する１つ以上のタイプの通知を選択し得、受信し得る。

【００６１】

[0061]プライバシーリスクをもたらし得る第三者のコンテンツソースを検出するための技法が使用される、様々な実施形態を説明してきたので、ここで今から前述した実施形態を実装するために利用され得るシステム例を考察されたい。

【００６２】

システム例

[0062]図６は、前述した様々な実施形態を実装し得る計算装置（６００）の例を示している。計算装置（６００）は、例えば、図１の計算装置（１０２）か又はその他の任意の適切な計算装置であり得る。

【００６３】

[0063]計算装置（６００）は、１つ以上のプロセッサー若しくは処理ユニット（６０２）、１つ以上のメモリー及び／又はストレージコンポーネント（６０４）、１つ以上の入力／出力（Ｉ／Ｏ）装置（６０６）、並びに様々なコンポーネント及び機器が相互に通信可能なバス（６０８）、を含む。バス（６０８）は、メモリーバス、又はメモリーコントローラー、周辺機器用バス、アクセラレイティッドグラフィックスポート、及び様々な任意のバスアーキテクチャを利用したプロセッサーバス又はローカルバス、を含むいくつかのバス構造タイプのうち１つ以上のどれかを示している。バス（６０８）は、有線及び／又は無線バスを含み得る。

【００６４】

[0064]メモリー／ストレージコンポーネント（６０４）は、１つ以上の計算機記憶媒体を表す。コンポーネント（６０４）は、（ランダムアクセスメモリー（ＲＡＭ）のような

）揮発性媒体及び／又は（読み出し専用メモリー（ＲＯＭ）、フラッシュメモリー、光学式ディスク、磁気ディスクなどのような）不揮発性媒体を含み得る。コンポーネント（６０４）は、（例えばＲＡＭ、ＲＯＭ、固定型ハードドライブなどの）固定型媒体及び（例えばフラッシュメモリードライブ、取り外し可能ハードドライブ、光学式ディスクなどの）取り外し可能媒体を含み得る。

【００６５】

[0065]１つ以上の入力／出力装置（６０６）は、ユーザーが計算装置（６００）にコマンド及び情報を入力可能にして、情報がユーザー、及び／又はその他のコンポーネント又は機器に提示され得るようにする。入力装置の例は、キーボード、カーソル制御装置（例えばマウス）、マイクロフォン、スキャナーなどを含む。出力機器の例は、表示装置（例えば、モニター又はプロジェクター）、スピーカー、プリンター、ネットワークカードなどを含む。

【００６６】

[0066]様々な技法は、ソフトウェア又はプログラムモジュールに関する一般的な文脈で本明細書に記述され得る。通常、ソフトウェアは、特定のタスクを実行するか又は特定の抽象データタイプを実装しているルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。これらのモジュール及び技法の実装は、いくつかの計算機可読媒体形式を介しストアされ得るか又は送信され得る。計算機可読媒体は、計算装置によってアクセスされ得る利用可能な任意の単一の媒体又は複数の媒体であり得る。非限定の例として、計算機可読媒体は、「計算機記憶媒体」を含み得る。

【００６７】

[0067]計算機記憶媒体は、計算機読込可能命令、データ構造、プログラムモジュール、又はその他のデータのような情報の記憶に関する任意の方法若しくは技術によって実装される揮発性媒体及び不揮発性媒体、並びに取り外し可能媒体及び媒体取り外し不可能媒体を含む。計算機記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリー、若しくはその他のメモリー技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、若しくはその他の光学式記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置、若しくはその他の磁気記憶装置、又は所望した情報をストアするために利用され得、計算機によってアクセスされ得るその他任意の媒体、を含むがこれらに限定しない。

【００６８】

結論

[0068]プライバシーリスクをもたらし得るウェブページに関する第三者のコンテンツソースを検出可能にする様々な実施形態を本明細書に記述している。

【００６９】

[0069]対象項目が構造的な機能及び／又は方法論的な動作に対し特定の言語で記載されているが、添付した請求項に定義した対象項目が、記載した特定の機能又はステップに必ずしも限定されるわけではないことを理解されよう。もっと具体的に言うと、特定の機能及びステップは、本請求対象項目の実装形式の例として開示されている。

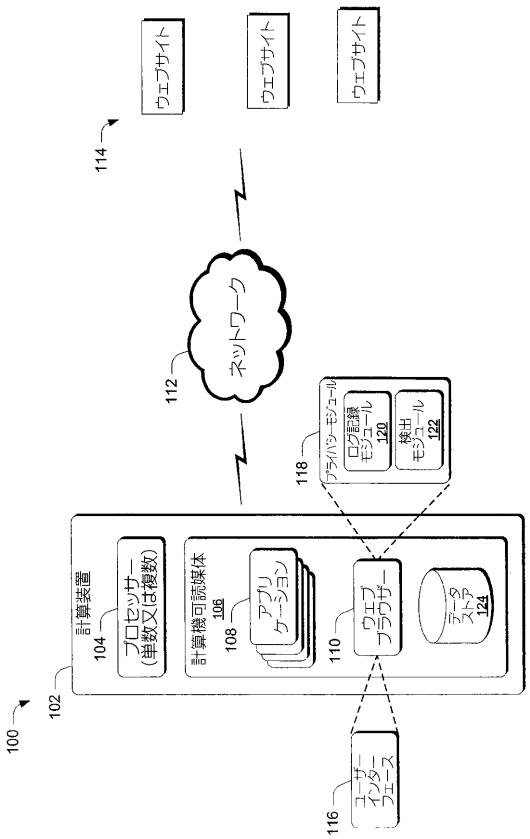
【符号の説明】

【００７０】

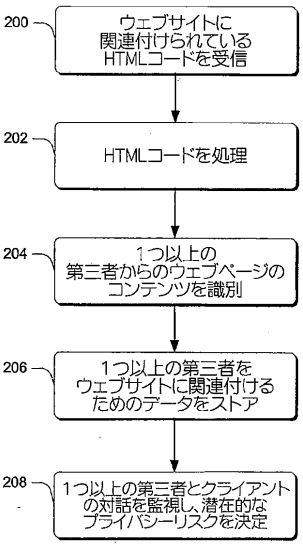
１００　動作環境
１０２　計算装置
１０４　プロセッサー
１０６　計算機可読媒体
１０８　アプリケーション
１１０　ウェブブラウザー
１１２　ネットワーク
１１４　ウェブサイト
１１６　ユーザーインターフェース
１１８　プライバシーモジュール

１２０　ログ記録モジュール
１２２　検出モジュール
１２４　データストア
４００　ユーザーインターフェース
４０２　ウェブページ
４０４　「トップニュース」部分
４０６　リンク
４０８　自動車の画像
４１０　ゴルフ関連広告
４１２　気象情報プラグイン
５０２　ポップアップウィンドウ
５０４　許可ボタン
５０６　ブロックボタン
５０８　無視ボタン
５１０　詳細リンク
５１２　メニューバー項目
６００　計算装置
６０２　処理ユニット
６０４　メモリー／ストレージ
６０６　入力／出力装置
６０８　バス

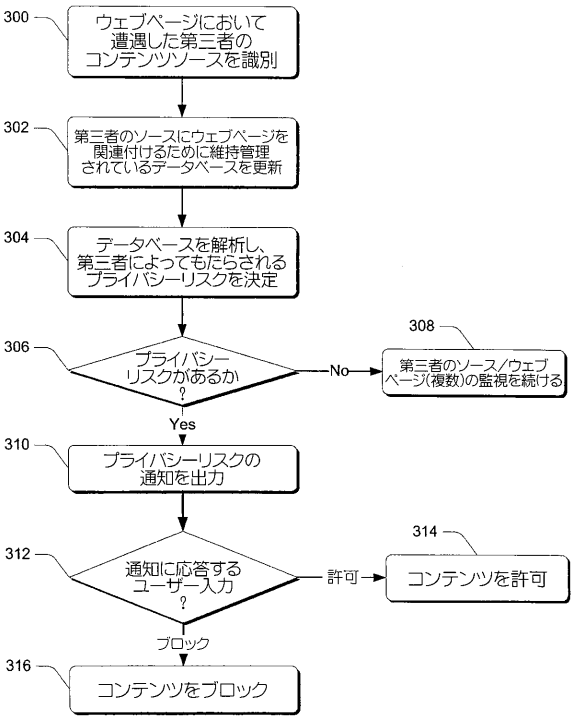
【図１】



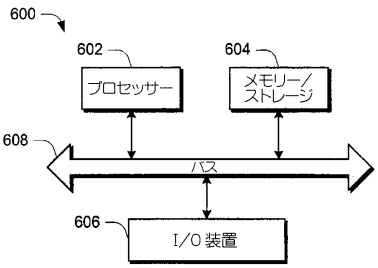
【図２】



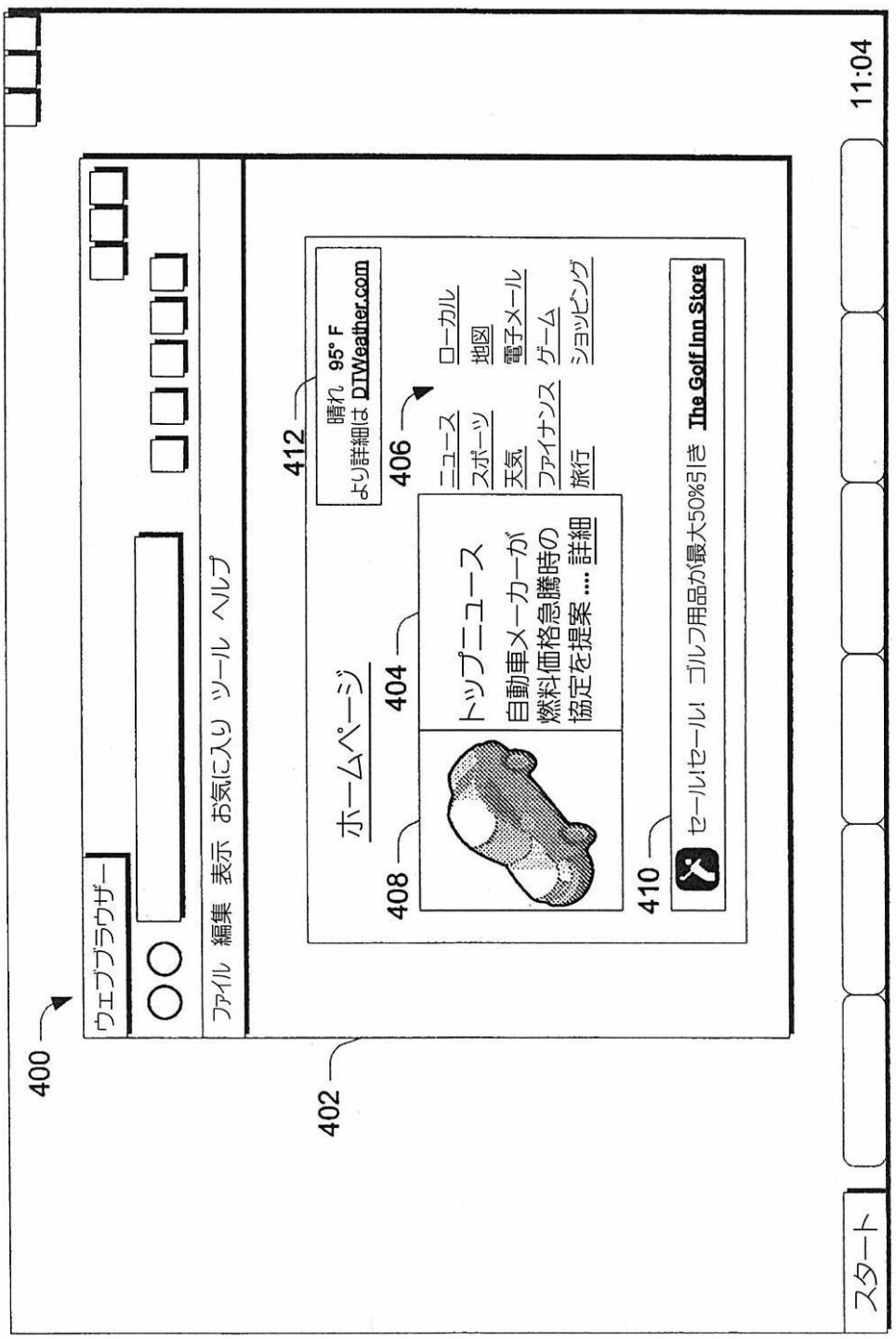
【図３】


300
ウェブページにおいて遭遇した第三者のコンテンツソースを識別
302
第三者のソースにウェブページを関連付けるために維持管理されているデータベースを更新
304
データベースを解析し、第三者によってもたらされるプライバシーリスクを決定
306
プライバシーリスクがあるか？
No
308
第三者のソース/ウェブページ(複数)の監視を続ける
Yes
310
プライバシーリスクの通知を出力
312
通知に応答するユーザー入力？
許可
314
コンテンツを許可
ブロック
316
コンテンツをブロック

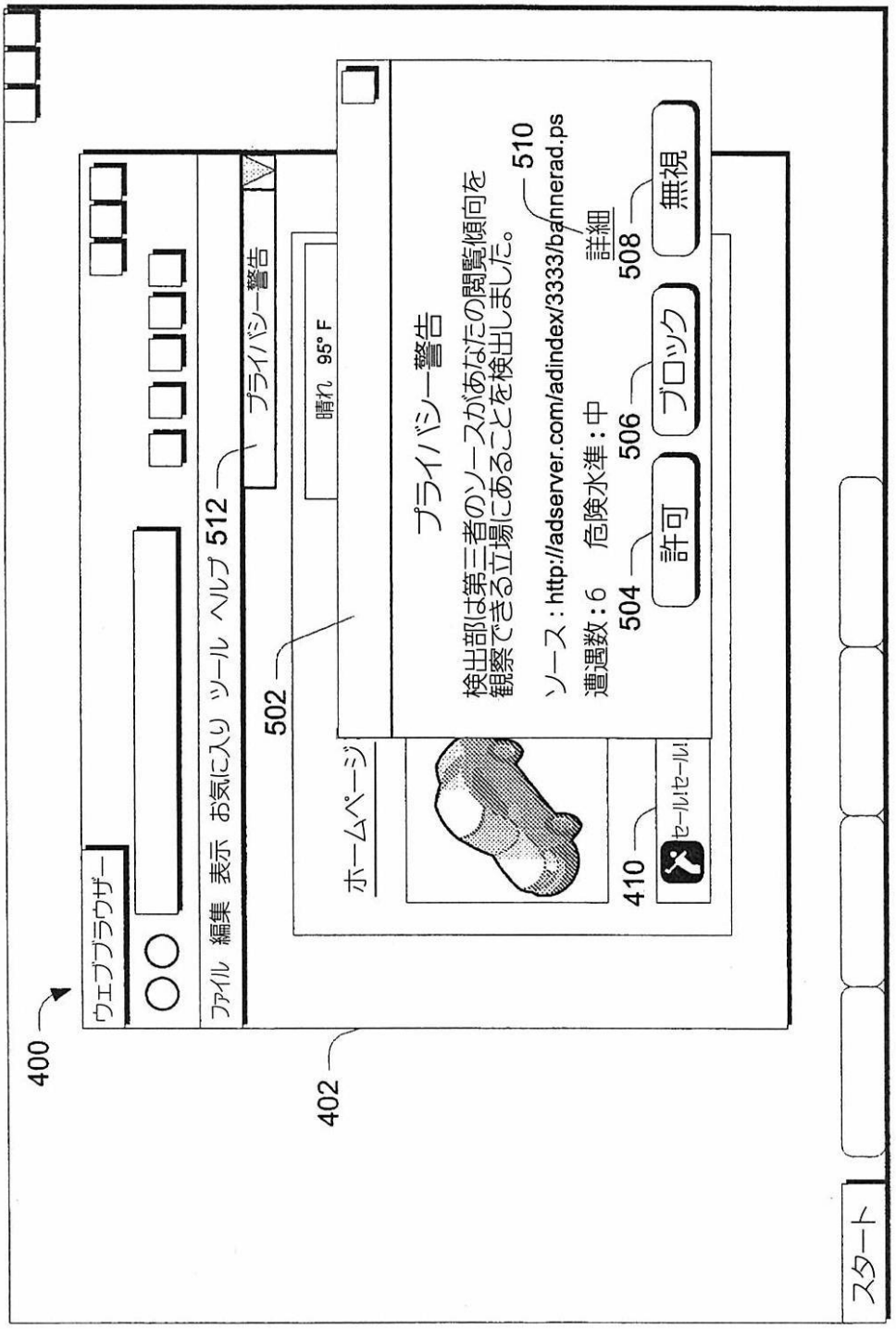
【図６】


600
602
プロセッサー
604
メモリー/ストレージ
608
バス
606
I/O装置

【図４】


400
ウェブブラウザー
ファイル 編集 表示 お気に入り ツール ヘルプ
402
ホームページ
404
トップニュース
自動車メーカーが
燃料価格急騰時の
協定を提案.... 詳細
408
ニュース
スポーツ
天気
ファイナンス
旅行
ローカル
地図
電子メール
ゲーム
ショッピング
406
412
晴れ 95° F
より詳細は DTWeather.com
410
セールはセール! ゴルフ用品が最大50%引き The Golf Inn Store
スタート
11:04

【図５】


400
402
ウェブブラウザー
ファイル 編集 表示 お気に入り ツール ヘルプ 512
プライバシー警告
晴れ 95° F
502
ホームページ
プライバシー警告
検出部は第三者のソースがあなたの閲覧傾向を観察できる立場にあることを検出しました。
510
ソース：http://adserver.com/adindex/3333/bannerad.ps
遭遇数：6 危険水準：中 詳細
504 506 508
許可 ブロック 無視
410
セールセール
スタート

フロントページの続き

(72)発明者 ジーグラー，アンドリュー
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 ガンジャム，アナンサ・ピー
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 パットン，マラ・ビー
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 ヒッチコック，ジェシカ・エイ
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 ハチャモヴィッチ，ディーン・ジェイ
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 コール，アンソニー・ティー
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 田上 隆一

(56)参考文献 特開２００５－３５３０３８（ＪＰ，Ａ）
笹川，Buyer's Guide，ＡＳＣＩＩ ｎｅｔｗｏｒｋ ＰＲＯ，日本，株式会社アスキー，２００年 1月 1日，第5巻 第1号，ｐ．８１～９０

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １３／００