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

特許第4644246号
(P4644246)

(45)発行日　平成23年3月2日(2011.3.2)　(24)登録日　平成22年12月10日(2010.12.10)

(51)Int.Cl.　F I
G06F 3/048 (2006.01)　G06F 3/048 651A
G06F 13/00 (2006.01)　G06F 13/00 550A

請求項の数 19　(全 13 頁)

(21)出願番号　特願2007-508321 (P2007-508321)
(86)(22)出願日　平成16年7月29日 (2004.7.29)
(65)公表番号　特表2007-533023 (P2007-533023A)
(43)公表日　平成19年11月15日 (2007.11.15)
(86)国際出願番号　PCT/US2004/024343
(87)国際公開番号　WO2005/109736
(87)国際公開日　平成17年11月17日 (2005.11.17)
審査請求日　平成19年7月27日 (2007.7.27)
(31)優先権主張番号　10/826,139
(32)優先日　平成16年4月15日 (2004.4.15)
(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　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アン　セルツァー
アメリカ合衆国　９８０５２　ワシントン州　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　コーポレーション内

最終頁に続く

(54)【発明の名称】セキュリティ要素をブラウザウィンドウと共に表示すること

(57)【特許請求の範囲】
【請求項１】
ブラウザウィンドウのためのセキュリティ機能を提供するための方法であって、
前記ウィンドウを開くためのコールを受信するステップと、
前記ウィンドウに関連付けられるセキュリティレベルを決定するステップであって、前記セキュリティレベルは、少なくとも１つの信頼されないセキュリティレベルおよび少なくとも１つの信頼されたセキュリティレベルから選択される、ステップと、
前記セキュリティレベルが、前記ウィンドウ内のコンテンツが信頼されないソースから来ることを指示するとき、ユーザが見て、前記ウィンドウ内の前記コンテンツが前記信頼されないソースから来ると判断することができるセキュリティ要素と共に前記ウィンドウを表示するステップとを備え
前記ウィンドウを開くための前記コールに関連付けられた属性を検査するステップと、
前記セキュリティレベルが、前記ウィンドウ内のコンテンツが信頼されないソースから来ることを指示するとき、信頼されないセキュリティ要素についての前記セキュリティ要素が表示されるように、前記コール内の前記属性の少なくとも１つを調整するステップと、
前記ウィンドウを開くための前記修正されたコールを送信するステップとを備えることを特徴とする方法。
【請求項２】
前記コール内の前記属性の少なくとも１つを調整するステップは、前記セキュリティレ

ベルが、前記ウィンドウ内のコンテンツが信頼されたソースから来ることを指示するとき、信頼されるセキュリティ要素についての前記セキュリティ要素が表示されないように、前記コール内の前記属性の少なくとも１つを調整することを含むことを特徴とする請求項１に記載の方法。

【請求項３】

前記ウィンドウに関連付けられた前記セキュリティレベルを決定するステップは、前記ユーザがインターネットゾーンおよび制限付きゾーンのうちの少なくとも１つにおいてナビゲート中であるとき、前記セキュリティレベルが前記信頼されないレベルであると決定するステップをさらに備えることを特徴とする請求項１に記載の方法。

【請求項４】

前記セキュリティ要素はステータスバーであることを特徴とする請求項１に記載の方法。

【請求項５】

前記ステータスバー内にゾーンを表示することを特徴とする請求項４に記載の方法。

【請求項６】

前記セキュリティ要素はタイトルバーをさらに備えることを特徴とする請求項４に記載の方法。

【請求項７】

ブラウザウィンドウのためのセキュリティ機能を提供するためのプログラムを有するコンピュータ可読記録媒体であって、前記プログラムは、コンピュータに、

前記ウィンドウを開くためのコールを受信するステップであって、前記コールは、前記ウィンドウの属性に関連付けられたパラメータを含む、ステップと、

前記ウィンドウに関連付けられたセキュリティレベルを決定するステップと、

前記パラメータを解析して、前記ウィンドウと共に表示されるときにユーザに、前記ウィンドウ内のコンテンツが信頼されないソースから来ることを指示する、セキュリティ要素に関連付けられた少なくとも１つのパラメータを探し出すステップと、

前記セキュリティレベルが、前記ウィンドウ内のコンテンツが信頼されないソースから来ることを指示するとき、前記ウィンドウが開かれるときに信頼されないセキュリティ要素についての前記セキュリティ要素が表示されるように前記少なくとも１つの探し出されたパラメータを調整するステップと

を実行させることを特徴とするコンピュータ可読記録媒体。

【請求項８】

前記少なくとも１つの探し出されたパラメータを調整するステップは、前記セキュリティレベルが、前記ウィンドウ内のコンテンツが信頼されたソースから来ることを指示するとき、信頼されるセキュリティ要素についての前記セキュリティ要素が表示されないように、前記少なくとも１つの探し出されたパラメータを調整することを含むことを特徴とする請求項７に記載のコンピュータ可読記録媒体。

【請求項９】

前記セキュリティレベルは、少なくとも１つの信頼されないセキュリティレベルおよび少なくとも１つの信頼されたセキュリティレベルから選択されることを特徴とする請求項７に記載のコンピュータ可読記録媒体。

【請求項１０】

前記ウィンドウに関連付けられた前記セキュリティレベルを決定するステップは、前記ユーザがインターネットゾーンおよび制限付きゾーンのうち少なくとも１つにおいてナビゲート中であるとき、前記セキュリティレベルが前記信頼されないレベルであると決定するステップをさらに備えることを特徴とする請求項７に記載のコンピュータ可読記録媒体。

【請求項１１】

前記セキュリティ要素はステータスバーであることを特徴とする請求項１０に記載のコンピュータ可読記録媒体。

【請求項１２】
前記ステータスバー内にゾーンを表示することを特徴とする請求項１１に記載のコンピュータ可読記録媒体。
【請求項１３】
前記セキュリティ要素はタイトルバーをさらに備えることを特徴とする請求項１１に記載のコンピュータ可読記録媒体。
【請求項１４】
ブラウザウィンドウのためのセキュリティ機能を提供するための装置であって、
プロセッサおよびコンピュータ可読記録媒体と、
前記コンピュータ可読記録媒体に格納され、前記プロセッサで実行されるオペレーティング環境と、
ディスプレイと、
前記オペレーティング環境の制御下で動作し、前記プロセッサにアクションを実行するように動作するアプリケーションとを備え、前記アクションは、
前記ウィンドウを開くためのコールを受信することであって、前記コールは、ステータスバーに関連付けられたパラメータを含むこと、
前記ウィンドウに関連付けられたセキュリティレベルを決定すること、および
前記セキュリティレベルが、前記ウィンドウ内のコンテンツが信頼されないソースから来ることを指示するとき、前記ウィンドウが開かれるときに前記ステータスバーが表示されるように、前記ステータスバーに関連付けられた前記パラメータを調整することを含むことを特徴とする装置。
【請求項１５】
前記パラメータを調整するステップは、前記セキュリティレベルが、前記ウィンドウ内のコンテンツが信頼されたソースから来ることを指示するとき、信頼されるセキュリティ要素についての前記セキュリティ要素が表示されないように、前記パラメータを調整することを含むことを特徴とする請求項１４に記載の装置。
【請求項１６】
前記セキュリティレベルは、少なくとも１つの信頼されないセキュリティレベルおよび少なくとも１つの信頼されたセキュリティレベルから選択されることを特徴とする請求項１４に記載の装置。
【請求項１７】
前記ウィンドウに関連付けられた前記セキュリティレベルを決定することは、前記ユーザがインターネットゾーンおよび制限付きゾーンのうち少なくとも１つにおいてナビゲート中であるとき、前記セキュリティレベルが前記信頼されないレベルであると決定することをさらに備えることを特徴とする請求項１６に記載の装置。
【請求項１８】
前記ステータスバー内にゾーンを表示することを特徴とする請求項１４に記載の装置。
【請求項１９】
タイトルバーを表示することをさらに備えることを特徴とする請求項１４に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザがウィンドウのソースを信頼し、知ることができるような方法でブラウザウィンドウを表示することによって、悪意あるアクティビティを抑制することを対象とする、セキュリティ要素を提供するための方法およびシステムを提供することを対象とする。
【背景技術】
【０００２】
インターネットサイトにアクセスするとき、コンピュータのセキュリティを保持するこ

とは、困難である場合がある。毎日、安全なタスクを実行するであろうとユーザが信じるアクションで、実際に実行するときにそのタスクが悪意あるものとなるアクションを選択させるようにユーザを欺く、新しい方法が存在する。例えば、悪意を有してブラウザウィンドウが描画されて、信頼されたソースに関連付けられたダイアログボックスまたはウィンドウが模倣される場合がある。このウィンドウを見るユーザは、自分が実際に別のサイトにリダイレクトされているか、あるいは悪意あるファイルをダウンロード中であるときに、そのウィンドウを閉じていると信じるように欺かれる場合がある。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

本発明は、ユーザがウィンドウのソースを信頼し、知ることができるような方法でブラウザウィンドウを表示することによって、悪意あるアクティビティを抑制することを対象とする、セキュリティ要素を提供するための方法およびシステムを提供することを対象とする。

【課題を解決するための手段】

【０００４】

本発明の一態様によれば、セキュリティ要素は、実際にはソースが信頼されないソースであるときに、ユーザが混乱されないこと、または信頼されたソースからウィンドウが発生すると信じるように欺かれない（「スプーフされない」）ことを確実にする助けとなるように、ウィンドウ上に表示される追加の情報および装飾を含む。

【０００５】

本発明の別の態様によれば、ブラウザウィンドウを開くためのコールが行われるとき、セキュリティ要素は、デフォルトにより表示されるステータスバーである。ステータスバーは、セキュリティゾーンなど、追加の情報をユーザに提供して、コンテンツのソースを決定する際にユーザを助けることができる。セキュリティゾーンはユーザに、コンテンツが発生中である元の場所を通知する。

【０００６】

本発明のさらに別の態様によれば、ユーザがナビゲート中であるセキュリティゾーンは、ブラウザウィンドウと共に表示されるべきセキュリティ要素を決定するために使用される。例えば、ソースが信頼されないソースであるとき、セキュリティ要素は常に表示される。ソースが信頼されるとき、セキュリティ要素は表示されてもされなくてもよい。

【発明を実施するための最良の形態】

【０００７】

一般に、本発明は、ユーザがウィンドウのソースを信頼し、知ることができるような方法でウィンドウを表示することによって、悪意あるアクティビティを抑制することを対象とする、セキュリティ機能を提供するための方法およびシステムを提供することを対象とする。追加の情報および装飾を含むセキュリティ要素は、ユーザが混乱されないこと、または、信頼されたソースからウィンドウが発生すると信じるように欺かれない（「スプーフされない」）ことを確実にする助けとなるように、ウィンドウ上に表示される。例えば、ユーザは、オペレーティングシステムなどの信頼されたソースから生成されたウィンドウを、外部ウェブサイトなどの信頼されないソースから生成されたコンテンツを有するウィンドウに対して、視覚的に区別することができるようになる。

【０００８】

本発明の一実施形態によれば、ブラウザウィンドウが開かれるとき、ステータスバーがデフォルトにより表示される。ステータスバーは、セキュリティゾーンなど、追加の情報をユーザに提供して、コンテンツのソースを決定する際にユーザを助ける。セキュリティゾーンはユーザに、コンテンツが発生中である元の場所を通知する。例えば、セキュリティゾーンは、コンテンツがインターネットから発生中であることを指示することができる。この追加の情報は、ソースを信頼するかどうかにかかわらず、ユーザが必要な情報を有することを確実にする助けとなる。

【０００９】
例示的オペレーティング環境
図１を参照すると、本発明を実施するための１つの例示的システムは、コンピューティングデバイス１００などのコンピューティングデバイスを含む。非常に基本的な構成では、コンピューティングデバイス１００は通常、少なくとも１つの処理装置１０２およびシステムメモリ１０４を含む。コンピューティングデバイスの正確な構成およびタイプに応じて、システムメモリ１０４を揮発性（ＲＡＭなど）、不揮発性（ＲＯＭ、フラッシュメモリなど）またはこの２つのある組合せにすることができる。システムメモリ１０４は通常、オペレーティングシステム１０５、１つまたは複数のアプリケーション１０６を含み、プログラムデータ１０７を含む場合がある。一実施形態では、アプリケーション１０６はウィンドウセキュリティプログラム１２０を含む場合がある。一般に、ウィンドウセキュリティプログラム１２０は、ユーザがウィンドウ内のコンテンツのソースを決定するために必要な視覚的合図および情報と共に、ウィンドウが開かれることを確実にするように構成される。この基本構成を図１で、破線１０８内のこれらのコンポーネントによって例示する。
【００１０】
コンピューティングデバイス１００は、追加の特徴または機能を有する場合がある。例えば、コンピューティングデバイス１００はまた、追加のデータストレージデバイス（リムーバブルおよび／または非リムーバブル）も含む場合があり、この追加のデータストレージデバイスは例えば、磁気ディスク、光ディスクまたはテープなどである。このような追加のストレージを図１で、リムーバブルストレージ１０９および非リムーバブルストレージ１１０によって例示する。コンピュータストレージメディアには、揮発性および不揮発性、リムーバブルおよび非リムーバブルメディアが含まれる場合があり、このメディアは、コンピュータ可読命令、データ構造、プログラムモジュールまたは他のデータなどの情報の格納のためのいずれかの方法または技術において実装される。システムメモリ１０４、リムーバブルストレージ１０９および非リムーバブルストレージ１１０はすべてコンピュータストレージメディアの例である。コンピュータストレージメディアには、それだけに限定されないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）もしくは他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または、所望の情報を格納するために使用することができ、またコンピューティングデバイス１００によってアクセスすることができる他のいかなるメディアもが含まれる。いかなるこのようなコンピュータストレージメディアも、デバイス１００の一部となることができる。コンピューティングデバイス１００はまた、キーボード、マウス、ペン、音声入力コンポーネント、タッチ入力デバイスなど、入力デバイス１１２も有する場合がある。ディスプレイ、スピーカ、プリンタなど、出力デバイス１１４もまた含まれる場合がある。
【００１１】
コンピューティングデバイス１００はまた通信接続１１６も含む場合があり、通信接続１１６は、デバイスがネットワークを介するなどして他のコンピューティングデバイス１１８と通信することができるようにする。通信接続１１６は通信メディアの一例である。通信メディアは通常、搬送波または他の移送メカニズムなどの変調データ信号におけるコンピュータ可読命令、データ構造、プログラムモジュールまたは他のデータによって実施することができ、いかなる情報配信メディアもが含まれる。「変調データ信号」という用語は、信号における情報を符号化するような方法でその特性の１つまたは複数が設定または変更されている信号を意味する。限定ではなく、例として、通信メディアには、有線ネットワークまたは直接有線接続などの有線メディア、ならびに、音響、ＲＦ、赤外線および他の無線メディアなどの無線メディアが含まれる。本明細書で使用されるとき、コンピュータ可読メディアという用語には、ストレージメディアおよび通信メディアが含まれる。

【００１２】
セキュリティ要素を含む例示的ウィンドウ
図２は、本発明の態様による、ユーザがアクセス中である可能性のある異なるゾーンを例示する、例示的ウィンドウを示す。セキュリティゾーンは、ユーザが出会う可能性の高い様々なタイプのコンテンツについて適切なレベルのセキュリティを提供する際に支援するために使用される。多数の異なるセキュリティゾーンを実施することができ、これらのゾーンは、そのゾーンに関連付けられた様々な程度の信頼性を有する。本発明の一実施形態によれば、５つの異なるゾーンがあり、ローカルマシンゾーン（２０５）、信頼されたサイトゾーン（２３０）、ローカルイントラネットゾーン（２４０）、インターネットゾーン（２５０）および制限付きゾーン（２６０）が含まれる。これらの異なるゾーンは、そのゾーンに関連付けられた様々なレベルのセキュリティを有する。本発明の一実施形態によれば、ステータスバー２２０などのセキュリティ要素は、常にウィンドウと共に表示される。
【００１３】
現在のゾーン（２２５、２３５、２４５、２５５および２６５）は、ステータスバー２２０の右下側に表示される。ユーザは、コンテンツ２１５に関連付けられたリスクを、ゾーンを参照することによって容易に査定することができる。ユーザが異なるゾーンにナビゲートするときは常に、そのゾーンはステータスバー内に表示される。
【００１４】
本発明の一実施形態によれば、各ゾーンに関連付けられたデフォルトセキュリティ設定がある。しかし、これらのセキュリティ設定を変更し、組織およびそのユーザのニーズに基づいた設定に構成することができる。
【００１５】
例えば、組織は、ブラウザがコンテンツの表示、プログラムおよびファイルのダウンロードを処理する方法についての設定を、コンテンツまたはファイルが来る元のゾーンに応じて指定することができる。例えば、組織は、その企業イントラネット内でダウンロードされたいかなるものも安全であると確信することができる。したがって、ローカルマシンゾーン（２２５）またはローカルイントラネットゾーン（２４５）など、いくつかのゾーン用のセキュリティ設定を、プロンプトをほとんどなしに、あるいはまったくなしにダウンロードを可能にする低レベルに設定することができる。しかし、インターネットゾーンまたは制限付きサイトゾーンからのコンテンツなど、信頼されないソース用のセキュリティ設定を、より厳しくすることができる。例えば、より多くの情報をユーザに表示して、コンテンツに関連付けられたリスクを指示することができる。
【００１６】
ウィンドウ２０５によって例示されたローカルマシンゾーンは、ユーザのローカルコンピュータ上に存在するコンテンツ用のゾーンである。ユーザのコンピュータ上で発見されたコンテンツは、信頼されないソースからローカルシステム上にキャッシュされる可能性のあるコンテンツを除いて、高いレベルの信頼を有して扱われる。例えば、ブラウザは、インターネットから得られた信頼されないソースからのコンテンツをキャッシュする可能性がある。一般に、ローカルコンピュータ上にすでにあるいかなるファイルも大変安全であると仮定され、したがって、最小限のセキュリティ設定がこれらのファイルに割り当てられる。一実施形態によれば、ナビゲートされているゾーンがローカルマシンゾーンであるとき、セキュリティ要素をオフにすることができる。
【００１７】
ウェブサイトを、信頼されたサイトゾーン（２３５）および制限付きサイトゾーン（２６５）に対して追加および削除することができる。信頼されたサイトゾーン（２３５）および制限付きサイトゾーン（２６５）には、インターネットゾーンまたはローカルイントラネットゾーン内のサイトより多少信頼されるサイトが含まれる。
【００１８】
信頼されたサイトゾーン（２３５）は、有害でないと思われるサイトを指す。例えば、

ユーザは「信頼されたサイトゾーン」内に含まれたサイトからのファイルを、データの信頼性について心配することなく安全にダウンロードまたは実行することができると思われる。このゾーンは、信頼されたビジネスパートナーのサイトなど、大変信頼されたサイト向きである。一実施形態によれば、ナビゲートされているゾーンが信頼されたサイトゾーンであるとき、セキュリティ要素をオフにすることができる。

【００１９】

制限付きサイトゾーン（２６５）は、信頼されず、高いセキュリティレベルに割り当てられるサイト用である。ユーザが制限付きサイトにいるとき、十分な情報がウィンドウ２６０と共に提供されて、ユーザは、そのコンテンツが信頼されないソースからのものであることを知るようになる。一実施形態によれば、ステータスバー（２２０）およびタイトルバー（２１０）は、ユーザが制限付きゾーン内でナビゲート中であるとき、常に表示される。

【００２０】

ローカルイントラネットゾーン（２４５）は通常、システムアドミニストレータによって定義されたようなプロキシサーバーを必要としない、任意のアドレスをも含む。これらには通常、ネットワークパス（＼＼コンピュータ名＼フォルダ名など）およびローカルイントラネットサイト（通常、ピリオドを含まないアドレスであり、ｈｔｔｐ：／／ｉｎｔｅｒｎａｌなど）によって指定されたサイトが含まれる。ローカルイントラネットゾーン２４５は一般に信頼することができ、これは、イントラネット上の情報はユーザの会社から来るからである。例えば、ユーザの会社のイントラネット上のサイトを信頼することができるので、組織は通常、ユーザがこの場所からのすべてのタイプのアクティブなコンテンツを実行することができることを望む。本発明の一実施形態によれば、ユーザがローカルイントラネットゾーン（２４５）内で操作中であるとき、タイトルバー（２１０）およびステータスバー（２２０）をオフにすることができる。

【００２１】

インターネットゾーン（２５５）は、ユーザのコンピュータ上、会社のローカルイントラネット上に含まれていないウェブサイト、または、信頼されたサイトゾーンもしくは制限付きサイトゾーンに割り当てられていないサイトからなる。インターネット上に位置するサイトは一般に信頼できない。したがって、より高いレベルのセキュリティがインターネットゾーンに適用される。このより高いセキュリティレベルは、ユーザがアクティブなコンテンツを実行することおよびコードを自分のコンピュータにダウンロードすることから、ユーザを助ける。ユーザがインターネットゾーン（２５５）にナビゲートしているとき、ウィンドウ２５０は、コンテンツがどこから来ているかをユーザが知るために必要な、十分な情報を有するようになる。例えば、一実施形態によれば、ウィンドウ２５０は、タイトルバー（２１０）およびステータスバー（２２０）を含み、イントラネットゾーン（２５５）がステータスバー（２２０）内で指示される。

【００２２】

図３は、本発明の態様による、信頼されたブラウザウィンドウ内に表示された、信頼されないコンテンツを例示する。

【００２３】

信頼されたブラウザウィンドウ３００は、タイトルバー３１０、ステータスバー３３０、ゾーン情報３４０および信頼されないコンテンツ３４５を含む。信頼されないコンテンツ３４５は、タイトルバー３５０を、閉じるボタン３５５と共に含み、閉じるボタン３５５をクリックするときにそのブラウザウィンドウ３１０が閉じると信じるように、ユーザをスプーフするように意図されている。本発明の一実施形態によれば、信頼されないゾーン内にあるいかなるウィンドウも、ステータスバー（３３０）と共に表示される。最も信頼されたゾーン内では、ブラウザのステータスバー（３３０）およびタイトルバー（３１０）をオフにすることができる。もう１つの実施形態によれば、セキュリティ要素が決してオフにされないようにすることができる。

【００２４】

コンテンツ３４５は、例示的広告ウィンドウとして描画される。コンテンツ３４５は、閉じるボタン３２０をクリックする代わりにコンテンツ３４５内の閉じるボタン３５５をクリックするように、ユーザを欺こうとして描画される。閉じるボタン３５５をクリックすると、ユーザに対して悪意ある状況になる可能性がある。例えば、ユーザが架空の閉じるボタン３５５をクリックするとき、ブラウザがそうするようにウィンドウを閉じるのではなく、ユーザは別のウィンドウにナビゲートされる場合があり、さらに悪い場合は、ウィルスがユーザのコンピュータにダウンロードされる可能性がある。ステータスバー（３３０）を、信頼されないコンテンツに対して強制的に表示させることは、コンテンツがどこで発生するかを見分けるために必要な情報をユーザに提供する際に助けとなる。図３を参照することによってわかるように、コンテンツ３４５は明らかに、ステータスバー（３３０）を有する信頼されたブラウザウィンドウ内にあり、ステータスバー（３３０）上で明らかにユーザに、このウィンドウがインターネットソース（３４０）からきたことを通知する。

【００２５】

ステータスバー３３０はデフォルトにより、コンピュータのオペレーティングシステムなどの信頼されたソースによって生成されたウィンドウと、信頼されないソースによって生成されたコンテンツとを区別する助けとするために表示される。

【００２６】

追加の情報および装飾をブラウザウィンドウ３００上に表示して、エンドユーザがコンテンツ３４５によって混乱されないことまたは欺かれないことを確実にする助けとすることによって、悪意あるアクティビティは抑制される。本発明の一実施形態によれば、追加の情報および装飾は、コンテンツ３４５がウェブページウィンドウ内にあるように見えるようにするための視覚的合図である。この実施例では、例えば、ステータスバー３３０が表示されなかった場合、ユーザは、コンテンツ３４５が、外部のソースではなくオペレーティングシステムによって作成されたウィンドウであると信じるように導かれる可能性がある。

【００２７】

タイトルバーを有するブラウザウィンドウが開かれるとき、ステータスバーはデフォルトにより、ステータスバー内の情報がユーザに見えることを確実にするために表示される。セキュリティゾーン（３４０）がステータスバー３３０内に表示されて、ユーザに、例えば、自分がインターネット上にいるのか、ローカルイントラネット上にいるのかが通知される。

【００２８】

図４は、本発明の態様による、ブラウザウィンドウのためのセキュリティを向上させるためのプロセスを例示する。開始ブロックの後、プロセスはブロック４１０に流れ、新しいウィンドウを開くためのコールが受信される。ウィンドウを開くためのコールは一般に、ウィンドウの特性を定義する、関連付けられたウィンドウ設定を有する。これらの設定には一般に、高さ、幅、場所、スクロールバー情報、タイトルバー、ステータスバー関連情報などが含まれる。

【００２９】

ブロック４２０に移ると、セキュリティゾーンに関連付けられたセキュリティ設定が決定される。一般に、セキュリティ設定は、ユーザが現在ナビゲート中であるゾーンに関係する（図５および関連する考察を参照）。セキュリティ設定を使用して、セキュリティ要素を表示するかどうかを決定することができる。

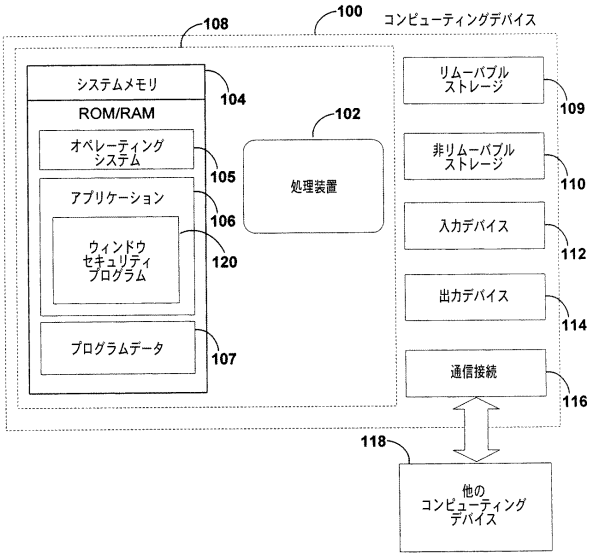
【００３０】

ブロック４３０に移行すると、ウィンドウ設定を、セキュリティ設定に基づいて修正することができる。一般に、ユーザが信頼されないコンテンツを認識できるようにするために十分な情報および装飾がウィンドウ上にあるように、ウィンドウ設定が構成されるように、パラメータが修正される（図６および関連する考察を参照）。例えば、ステータスバーが表示される。

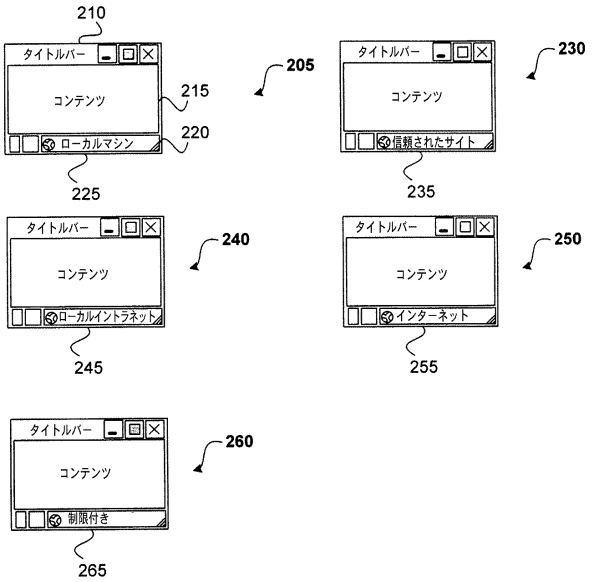
【００３１】
ブロック４４０に流れると、ウィンドウが表示される。一実施形態によれば、ウィンドウは、タイトルバーおよびステータスバーをオンにして表示され、コンテンツが明らかにウェブページウィンドウから区別可能であるようにされる。
【００３２】
図５は、本発明の態様による、セキュリティ設定を決定するためのプロセスを示す。開始ブロックの後、プロセスはブロック５１０に流れ、セキュリティゾーンが決定される。一実施形態によれば、セキュリティゾーンは、ローカルマシンゾーン、信頼されたサイトゾーン、ローカルイントラネットゾーン、インターネットゾーンおよび制限付きゾーンを含む、５つのゾーンのうち１つにすることができる。
【００３３】
判断ブロック５２０に移ると、ゾーンが信頼されるかどうかについての判断が行われる。信頼されたゾーンは、信頼されたコンテンツを常に有すると見なされるゾーンである。すなわち、信頼されたゾーンから検索されたコンテンツは悪意あるものではない。ゾーンが信頼されないとき、プロセスはブロック５３０に流れ、開かれるように要求されたウィンドウには、コンテンツの場所が信頼されないソースからのものであるとユーザが判断するために必要な装飾および情報が含まれるようになる。一実施形態によれば、タイトルバーおよびステータスバーは、信頼されないゾーンからのコンテンツを含むいかなるウィンドウに対しても表示される。ゾーンが信頼されるとき、プロセスは終了ブロックに流れ、処理は終了する。もう１つの実施形態によれば、ゾーンが信頼されるときでも、ウィンドウには、コンテンツの場所が信頼されないソースからのものであるとユーザが判断するために必要な装飾および情報が含まれる。次いで処理は終了ブロックに進み、他のアクションの処理へ戻る。
【００３４】
図６は、本発明の態様による、セキュリティ要素に関連付けられたウィンドウパラメータを調整するためのプロセスの流れを例示する。開始ブロックの後、プロセスはブロック６１０に流れ、ウィンドウパラメータが得られる。上述のように、ウィンドウパラメータは、幅、高さ、スクロールバー、色、タイトルバー（オン／オフ）、ステータスバー（オン／オフ）など、ウィンドウに関連付けられたいかなる属性にも関係する可能性がある。
【００３５】
ブロック６２０に移行すると、ウィンドウパラメータが解析されて、ステータスバーに関係する属性が探し出される。一実施形態によれば、タイトルバー属性もまた探し出される。
【００３６】
ブロック６３０に流れると、ステータスバー属性がオンに設定される。これは、ウィンドウパラメータが、ステータスバーを表示しないように設定された場合でも、ステータスが表示されるようになることを確実にする助けとなる。
【００３７】
次いで、プロセスはオプショナルブロック６４０に流れ、タイトルバーもオンにされる。他の属性または情報をオンにして表示することもでき、ウィンドウ内のコンテンツがウィンドウ自体でないとユーザが判断するために十分な装飾および情報がウィンドウに含まれることを確実にする助けとすることができる。例えば、特殊な境界をウィンドウの周囲に配置することができる。次いで、プロセスは終了ブロックに流れ、他のアクションの処理に戻る。
【００３８】
上記の仕様、実施例およびデータは、本発明の構成の製造および使用の完全な説明を提供する。本発明の多数の実施形態を、本発明の精神および範囲から逸脱することなく作成することができるので、本発明は、以下の付属の特許請求の範囲内に存在する。
【図面の簡単な説明】
【００３９】

【図１】本発明の例示的実施形態で使用することができる例示的コンピューティングデバイスを例示する図である。
【図２】ユーザがアクセス中である可能性のある異なるゾーンを例示する、例示的ウィンドウを示す図である。
【図３】信頼されたブラウザウィンドウ内に表示された、信頼されないコンテンツを例示する図である。
【図４】ブラウザウィンドウのためのセキュリティを向上させるためのプロセスを例示する図である。
【図５】セキュリティ設定を決定するためのプロセスを示す図である。
【図６】本発明の態様による、セキュリティ要素に関連付けられたウィンドウパラメータを調整するためのプロセスの流れを例示する図である。
【符号の説明】
【００４０】
１００　コンピューティングデバイス
１０２　処理装置
１０４　システムメモリ
１０５　オペレーティングシステム
１０６　アプリケーション
１０７　プログラムデータ
１０９　リムーバブルストレージ
１１０　非リムーバブルストレージ
１１２　入力デバイス
１１４　出力デバイス
１１６　通信接続
１１８　他のコンピューティングデバイス
１２０　ウィンドウセキュリティプログラム
２１０　タイトルバー
２１５　コンテンツ
２２０　ステータスバー
３００　ブラウザウィンドウ
３１０　タイトルバー
３３０　ステータスバー
３４０　ゾーン情報
３４５　コンテンツ

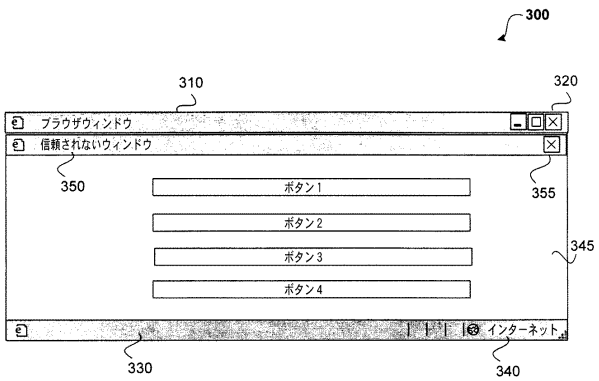
【図１】


100
コンピューティングデバイス
108
システムメモリ
104
ROM/RAM
オペレーティングシステム
105
アプリケーション
106
ウィンドウセキュリティプログラム
120
プログラムデータ
107
102
処理装置
リムーバブルストレージ
109
非リムーバブルストレージ
110
入力デバイス
112
出力デバイス
114
通信接続
116
118
他のコンピューティングデバイス

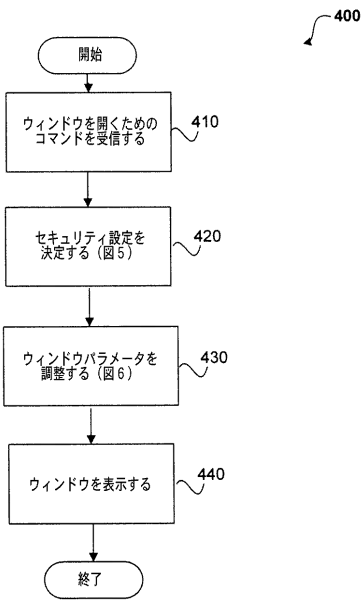
【図２】


210
タイトルバー
コンテンツ
215
ローカルマシン
220
225
205
タイトルバー
コンテンツ
信頼されたサイト
235
230
タイトルバー
コンテンツ
ローカルイントラネット
245
240
タイトルバー
コンテンツ
インターネット
255
250
タイトルバー
コンテンツ
制限付き
265
260

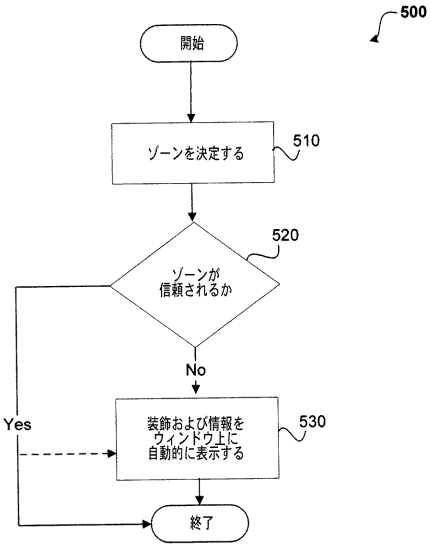
【図３】


300
310
320
ブラウザウィンドウ
信頼されないウィンドウ
350
355
ボタン1
ボタン2
ボタン3
ボタン4
345
インターネット
330
340

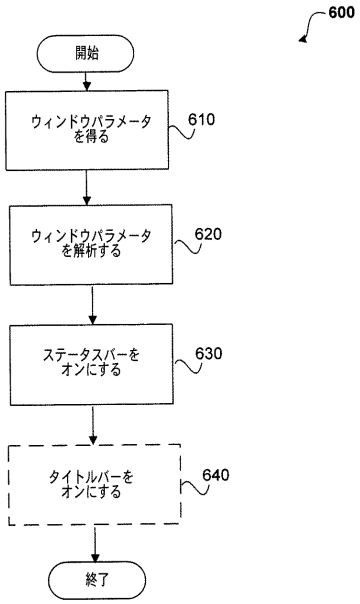
【図４】


400
開始
ウィンドウを開くためのコマンドを受信する
410
セキュリティ設定を決定する（図5）
420
ウィンドウパラメータを調整する（図6）
430
ウィンドウを表示する
440
終了

【図５】


500
開始
ゾーンを決定する
510
520
ゾーンが
信頼されるか
No
Yes
装飾および情報を
ウィンドウ上に
自動的に表示する
530
終了

【図６】


600
開始
ウィンドウパラメータ
を得る
610
ウィンドウパラメータ
を解析する
620
ステータスバーを
オンにする
630
タイトルバーを
オンにする
640
終了

フロントページの続き

(72)発明者　ロバート　スティーブン　ディリクソン
アメリカ合衆国　９８０５２　ワシントン州　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　コーポレーション内
(72)発明者　ローランド　トクミ
アメリカ合衆国　９８０５２　ワシントン州　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　コーポレーション内
(72)発明者　ロベルト　エー．フランコ
アメリカ合衆国　９８０５２　ワシントン州　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　コーポレーション内

審査官　竹中　辰利

(56)参考文献　特開２００３－２１８８５９（ＪＰ，Ａ）
このままだとあなたのＰＣはウイルス＆ハッカーに殺される　ハードでタフなネット時代、強くなくては生きていけない　ハッカーに唾をかけろ，ネットランナー，日本，ソフトバンクパブリッシング（株），２００３年１２月　１日，第5巻　第12号，p.178-180

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　3/048
G06F　13/00