(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5791814号
(P5791814)
(45)発行日　平成27年10月7日(2015.10.7)　(24)登録日　平成27年8月14日(2015.8.14)

(51)Int.Cl.　F I
G06F 21/41 (2013.01)　G06F 21/41

請求項の数 32　(全 14 頁)

(21)出願番号	特願2014-534730 (P2014-534730)
(86)(22)出願日	平成24年10月4日 (2012.10.4)
(65)公表番号	特表2014-529156 (P2014-529156A)
(43)公表日	平成26年10月30日 (2014.10.30)
(86)国際出願番号	PCT/US2012/058789
(87)国際公開番号	WO2013/052693
(87)国際公開日	平成25年4月11日 (2013.4.11)
審査請求日	平成26年4月3日 (2014.4.3)
(31)優先権主張番号	13/252,931
(32)優先日	平成23年10月4日 (2011.10.4)
(33)優先権主張国	米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ジェシカ・エム・フラナガン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】シングルサインオンドメインを信用情報漏洩から保護するための方法および装置

(57)【特許請求の範囲】
【請求項１】
シングルサインオンドメインを信用情報漏洩から保護するための方法であって、
認証サーバが認証クッキーをユーザブラウザクライアントに与えるステップであって、前記認証クッキーは前記シングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、前記シングルサインオンドメインの認証サブドメインに関連付けられる、与えるステップと、
前記認証サーバが前記ブラウザクライアントからのアクセス要求において前記認証クッキーを受信するステップであって、前記アクセス要求は、前記ユーザブラウザクライアントからのコンテンツ要求に応答して、前記シングルサインオンドメイン内のコンテンツサーバから前記ユーザブラウザクライアントによって受信された宛先変更に基づく、受信するステップと、
前記受信された認証クッキー内の前記ユーザ認証信用情報を認証すると、前記認証サーバが、前記ユーザブラウザクライアントに、前記シングルサインオンドメインのための限定利用クッキーを転送することによって、前記アクセス要求に応答するステップと、
前記認証サーバが、前記コンテンツサーバから前記限定利用クッキーのセッション識別子の妥当性を検証する要求を受信するステップであって、前記コンテンツサーバは前記ユーザブラウザクライアントから前記限定利用クッキーを受信した、受信するステップと、
前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記認証サーバが、前記コンテンツサーバに、前記コンテンツサーバが要求されたコンテンツを前記ユー

ザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えるステップとを含む、方法。
【請求項２】
前記限定利用クッキーは1回使用のクッキーを含む、請求項1に記載の方法。
【請求項３】
前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記認証サーバが前記限定利用クッキーを無効にし、前記限定利用クッキーのさらなる使用を禁止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】
前記限定利用クッキーは、短い満了時間を有する、請求項1に記載の方法。
【請求項５】
前記短い満了時間は約1分を含む、請求項4に記載の方法。
【請求項６】
前記コンテンツサーバは、前記シングルサインオンドメインのサブドメインを含む、請求項1に記載の方法。
【請求項７】
限定利用クッキーは、前記コンテンツサーバのサブドメインに対してのみ有効である、請求項6に記載の方法。
【請求項８】
前記セッション識別子は1回限りのセッションキーを含む、請求項1に記載の方法。
【請求項９】
認証サーバであって、
認証クッキーをユーザブラウザクライアントに与えるための手段であって、前記認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、前記シングルサインオンドメインの認証サブドメインに関連付けられる、与えるための手段と、
前記ブラウザクライアントからのアクセス要求において前記認証クッキーを受信するための手段であって、前記アクセス要求は、前記ユーザブラウザクライアントからのコンテンツ要求に応答して、前記シングルサインオンドメイン内のコンテンツサーバから前記ユーザブラウザクライアントによって受信される宛先変更に基づく、受信するための手段と、
前記受信された認証クッキー内の前記ユーザ認証信用情報を認証すると、前記ユーザブラウザクライアントに、前記シングルサインオンドメインのための限定利用クッキーを転送することによって、前記アクセス要求に応答するための手段と、
前記コンテンツサーバから前記限定利用クッキーのセッション識別子の妥当性を検証する要求を受信するための手段であって、前記コンテンツサーバは前記ユーザブラウザクライアントから前記限定利用クッキーを受信した、受信するための手段と、
前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記コンテンツサーバに、前記コンテンツサーバが要求されたコンテンツを前記ユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えるための手段とを備える、認証サーバ。
【請求項１０】
前記限定利用クッキーは1回使用のクッキーを含む、請求項9に記載の認証サーバ。
【請求項１１】
前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記限定利用クッキーを無効にし、前記限定利用クッキーのさらなる使用を禁止するための手段をさらに備える、請求項9に記載の認証サーバ。
【請求項１２】
前記限定利用クッキーは短い満了時間を有する、請求項9に記載の認証サーバ。
【請求項１３】

前記短い満了時間は約1分を含む、請求項12に記載の認証サーバ。
【請求項１４】
前記コンテンツサーバは前記シングルサインオンドメインのサブドメインを含む、請求項9に記載の認証サーバ。
【請求項１５】
前記限定利用クッキーは、前記コンテンツサーバのサブドメインに対してのみ有効である、請求項14に記載の認証サーバ。
【請求項１６】
前記セッション識別子は1回限りのセッションキーを含む、請求項9に記載の認証サーバ。
【請求項１７】
認証サーバであって、
プロセッサを含み、前記プロセッサは、
認証クッキーをユーザブラウザクライアントに与えることであって、前記認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、前記シングルサインオンドメインの認証サブドメインに関連付けられる、与えることと、
前記ブラウザクライアントからのアクセス要求において前記認証クッキーを受信することであって、前記アクセス要求は前記ユーザブラウザクライアントからのコンテンツ要求に応答して、前記シングルサインオンドメイン内のコンテンツサーバから前記ユーザブラウザクライアントによって受信される宛先変更に基づく、受信することと、
前記受信された認証クッキー内の前記ユーザ認証信用情報を認証すると、前記ユーザブラウザクライアントに前記シングルサインオンドメインのための限定利用クッキーを転送することによって、前記アクセス要求に応答することと、
前記コンテンツサーバから前記限定利用クッキーのセッション識別子の妥当性を検証する要求を受信することであって、前記コンテンツサーバは前記ユーザブラウザクライアントから前記限定利用クッキーを受信した、受信することと、
前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記コンテンツサーバに、前記コンテンツサーバが要求されたコンテンツを前記ユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えることと
を実施するように構成される、認証サーバ。
【請求項１８】
前記限定利用クッキーは1回使用のクッキーを含む、請求項17に記載の認証サーバ。
【請求項１９】
前記プロセッサは、
前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記限定利用クッキーを無効にし、前記限定利用クッキーのさらなる使用を禁止するように構成される、請求項17に記載の認証サーバ。
【請求項２０】
前記限定利用クッキーは短い満了時間を有する、請求項17に記載の認証サーバ。
【請求項２１】
前記短い満了時間は約1分を含む、請求項20に記載の認証サーバ。
【請求項２２】
前記コンテンツサーバは前記シングルサインオンドメインのサブドメインを含む、請求項17に記載の認証サーバ。
【請求項２３】
前記限定利用クッキーは、前記コンテンツサーバのサブドメインに対してのみ有効である、請求項22に記載の認証サーバ。
【請求項２４】
前記セッション識別子は1回限りのセッションキーを含む、請求項17に記載の認証サーバ。

【請求項２５】
コンピュータ可読記録媒体であって、前記コンピュータ可読記録媒体は、
コンピュータが、認証クッキーをユーザブラウザクライアントに与えるためのコードであって、前記認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、前記シングルサインオンドメインの認証サブドメインに関連付けられる、与えるためのコードと、
コンピュータが、前記ブラウザクライアントからのアクセス要求において前記認証クッキーを受信するためのコードであって、前記アクセス要求は前記ユーザブラウザクライアントからのコンテンツ要求に応答して、前記シングルサインオンドメイン内のコンテンツサーバから前記ユーザブラウザクライアントによって受信される宛先変更に基づく、コンピュータが受信するためのコードと、
コンピュータが、前記受信された認証クッキー内の前記ユーザ認証信用情報を認証すると、前記ユーザブラウザクライアントに前記シングルサインオンドメインのための限定利用クッキーを転送することによって、前記アクセス要求に応答するためのコードと、
コンピュータが、前記コンテンツサーバから前記限定利用クッキーのセッション識別子の妥当性を検証する要求を受信するためのコードであって、前記コンテンツサーバは前記ユーザブラウザクライアントから前記限定利用クッキーを受信した、コンピュータが受信するためのコードと、
コンピュータが、前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記コンテンツサーバに、前記コンテンツサーバが要求されたコンテンツを前記ユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えるためのコードとを含む、コンピュータ可読記録媒体。
【請求項２６】
前記限定利用クッキーは1回使用のクッキーを含む、請求項25に記載のコンピュータ可読記録媒体。
【請求項２７】
コンピュータが、前記限定利用クッキーの前記セッション識別子の妥当性を検証すると、前記限定利用クッキーを無効にし、前記限定利用クッキーのさらなる使用を禁止するためのコードをさらに含む、請求項25に記載のコンピュータ可読記録媒体。
【請求項２８】
前記限定利用クッキーは短い満了時間を有する、請求項25に記載のコンピュータ可読記録媒体。
【請求項２９】
前記短い満了時間は約1分を含む、請求項28に記載のコンピュータ可読記録媒体。
【請求項３０】
前記コンテンツサーバは前記シングルサインオンドメインのサブドメインを含む、請求項25に記載のコンピュータ可読記録媒体。
【請求項３１】
前記限定利用クッキーは、前記コンテンツサーバのサブドメインに対してのみ有効である、請求項30に記載のコンピュータ可読記録媒体。
【請求項３２】
前記セッション識別子は1回限りのセッションキーを含む、請求項25に記載のコンピュータ可読記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般にシングルサインオンドメインを信用情報漏洩から保護することに関する。
【背景技術】
【０００２】

シングルサインオン技法によれば、許可されたユーザが、共有ドメイン下の複数の保護されたサブドメインウェブサイトのうちの1つとの一度のサインオントランザクションに基づいて、保護されたサブドメインウェブサイトにアクセスできるようになる。通常のシングルサインオン技法では、保護されたサブドメインウェブサイトにアクセスするユーザは認証され、ユーザのブラウザにセッションクッキーを与えるウェブサイトに接続される。そのセッションクッキーによって、ユーザは、そのサブドメインウェブサイトに加えて、そのドメイン下のすべてのウェブサイトにアクセスできるようになる。

【０００３】

しかしながら、ユーザ認証の安全性を確保するために、サブドメインウェブサイトのすべてのホスト、およびすべてのホスト上で実行中のすべてのスクリプトは信頼されなければならない。保護されたドメイン下の別のサブドメインにおいて運営しており、ユーザによって訪問される不正ウェブサイトが、ユーザのブラウザからユーザのセッションクッキーを収集する可能性がある。セッションクッキーにおいて漏洩したユーザの信用情報は、そのドメイン下のサブドメインの他の保護された内部ウェブサイトに不法にアクセスするために、再利用される可能性がある。

【０００４】

したがって、シングルサインオンドメインを信用情報漏洩から保護するための技法が必要とされている。

【発明の概要】

【課題を解決するための手段】

【０００５】

本発明の一態様は、シングルサインオンドメインを信用情報漏洩から保護するための方法に属する場合がある。その方法では、認証サーバが認証クッキーをユーザブラウザクライアントに与える。認証クッキーはそのシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、シングルサインオンドメインの認証サブドメインと関連付けられる。認証サーバはブラウザクライアントからのアクセス要求において認証クッキーを受信する。アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求に応答して、シングルサインオンドメイン内のコンテンツサーバからユーザブラウザクライアントによって受信された宛先変更に基づく。受信された認証クッキー内のユーザ認証信用情報を認証すると、認証サーバは、シングルサインオンドメインのための限定利用クッキーをユーザブラウザクライアントに転送することによって、アクセス要求に応答する。認証サーバは、コンテンツサーバから、限定利用クッキーのセッション識別子の妥当性を検証する要求を受信する。コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した。限定利用クッキーのセッション識別子の妥当性を検証すると、認証サーバはコンテンツサーバに、コンテンツサーバが要求されたコンテンツをユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与える。

【０００６】

本発明の他のさらに詳細な態様では、限定利用クッキーは、1回使用のクッキーとすることができる。限定利用クッキーのセッション識別子の妥当性を検証すると、認証サーバは限定利用クッキーを無効にして、限定利用クッキーのさらなる使用を禁止する。限定利用クッキーは、短い満了時間を有することができる。短い満了時間は約1分を含むことができる。コンテンツサーバは、シングルサインオンドメインのサブドメインを含むことができる。限定利用クッキーは、コンテンツサーバのサブドメインに対してのみ有効とすることができる。セッション識別子は1回限りのセッションキーを含むことができる。

【０００７】

本発明の別の態様は認証サーバに属する場合があり、認証サーバは、認証クッキーをユーザブラウザクライアントに与えるための手段であって、その認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、シングルサインオンドメインの認証サブドメインに関連付けられる、与えるための手段と、ブラウザクライアントからのアクセス要求において認証クッキーを受信するために手段であって、アク

セス要求は、ユーザブラウザクライアントからのコンテンツ要求に応答して、シングルサインオンドメイン内のコンテンツサーバからユーザブラウザクライアントによって受信された宛先変更に基づく、受信するための手段と、受信された認証クッキー内のユーザ認証信用情報を認証すると、ユーザブラウザクライアントにシングルサインオンドメインのための限定利用クッキーを転送することによって、アクセス要求に応答するための手段と、コンテンツサーバから、限定利用クッキーのセッション識別子の妥当性を検証する要求を受信するための手段であって、コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した、受信するための手段と、限定利用クッキーのセッション識別子の妥当性を検証すると、コンテンツサーバに、コンテンツサーバが要求されたコンテンツをユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えるための手段とを備える。

【０００８】

本発明の別の態様は認証サーバに属する場合があり、認証サーバはプロセッサを備え、プロセッサは、認証クッキーをユーザブラウザクライアントに与えることであって、その認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、シングルサインオンドメインの認証サブドメインに関連付けられる、与えることと、ブラウザクライアントからのアクセス要求において認証クッキーを受信することであって、アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求に応答して、シングルサインオンドメイン内のコンテンツサーバからユーザブラウザクライアントによって受信された宛先変更に基づく、受信することと、受信された認証クッキー内のユーザ認証信用情報を認証すると、ユーザブラウザクライアントにシングルサインオンドメインのための限定利用クッキーを転送することによって、アクセス要求に応答することと、コンテンツサーバから限定利用クッキーのセッション識別子の妥当性を検証する要求を受信することであって、コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した、受信することと、限定利用クッキーのセッション識別子の妥当性を検証すると、コンテンツサーバに、コンテンツサーバが要求されたコンテンツをユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えることとを実施するように構成される。

【０００９】

本発明の別の態様はコンピュータ可読記録媒体を含むコンピュータプログラム製品に属する場合があり、コンピュータ可読記録媒体は、コンピュータが認証クッキーをユーザブラウザクライアントに与えるためのコードであって、その認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報を有し、シングルサインオンドメインの認証サブドメインに関連付けられる、与えるためのコードと、コンピュータがブラウザクライアントからのアクセス要求において認証クッキーを受信するためのコードであって、アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求に応答して、シングルサインオンドメイン内のコンテンツサーバからユーザブラウザクライアントによって受信された宛先変更に基づく、コンピュータが受信するためのコードと、受信された認証クッキー内のユーザ認証信用情報を認証すると、ユーザブラウザクライアントにシングルサインオンドメインのための限定利用クッキーを転送することによって、コンピュータがアクセス要求に応答するためのコードと、コンピュータがコンテンツサーバから限定利用クッキーのセッション識別子の妥当性を検証する要求を受信するためのコードであって、コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した、コンピュータが受信するためのコードと、限定利用クッキーのセッション識別子の妥当性を検証すると、コンピュータが、コンテンツサーバに、コンテンツサーバが要求されたコンテンツをユーザブラウザクライアントに転送できるようにするための有効セッションメッセージを与えるためのコードとを含む。

【図面の簡単な説明】

【００１０】

【図１】本発明による、シングルサインオンドメインを信用情報漏洩から保護するための

方法の流れ図である。
【図２】認証サーバおよび複数のコンテンツサーバと通信できるようにするインターネットに結合されるユーザブラウザクライアントを示すブロック図である。
【図３】は、認証サーバを実現するためのコンピュータの一例を示すブロック図である。
【図４】本発明による、シングルサインオンドメインを信用情報漏洩から保護するための方法の別の流れ図である。
【発明を実施するための形態】
【００１１】
「例示的な」という語は、本明細書において、「例、実例、または例示としての役割を果たすこと」を意味するために用いられる。本明細書において「例示的」として説明する任意の実施形態は、必ずしも他の実施形態よりも好ましいか、または有利であると解釈されるべきではない。
【００１２】
図1および図2を参照すると、本発明の一態様は、シングルサインオンドメインを信用情報漏洩から保護するための方法100に属することができる。その方法では、認証サーバ210が、ユーザブラウザクライアント220に認証クッキー102を与える(ステップ110)。認証クッキーは、シングルサインオンドメインのための少なくとも1つのユーザ認証信用情報112を有し、シングルサインオンドメインの認証サブドメインに関連付けられる。認証サーバは、ブラウザクライアントからのアクセス要求114において認証クッキーを受信する(ステップ120)。アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求118に応答して、シングルサインオンドメイン内のコンテンツサーバ230からユーザブラウザクライアントによって受信された宛先変更116に基づく。受信された認証クッキー内のユーザ認証信用情報を認証すると(ステップ130)、認証サーバは、ユーザブラウザクライアントに、シングルサインオンドメインのための限定利用クッキー132を転送することによってアクセス要求に応答する(ステップ140)。認証サーバは、コンテンツサーバから限定利用クッキーのセッション識別子の妥当性を検証する要求134を受信する(ステップ150)。コンテンツサーバは、ユーザブラウザクライアントから限定利用クッキーを受信した(ステップ160)。限定利用クッキーのセッション識別子の妥当性を検証すると(ステップ170)、認証サーバは、コンテンツサーバに、コンテンツサーバが要求されたコンテンツ184をユーザブラウザクライアントに転送できるようにするための有効セッションメッセージ182を与える(ステップ190)。
【００１３】
本発明のさらに詳細な態様では、限定利用クッキー132は1回使用のクッキーとすることができる。限定利用クッキーのセッション識別子の妥当性を検証すると(ステップ150)、認証サーバは、限定利用クッキーを無効にし、限定利用クッキーのさらなる使用を禁止することができる(ステップ180)。限定利用クッキーは、短い満了時間を有することができる。短い満了時間は約1分を含むことができる。限定利用クッキーは、特定のコンテンツサーバ230に特有とすることができる。コンテンツサーバは、シングルサインオンドメインのサブドメインを含むことができる。限定利用クッキーは、コンテンツサーバのサブドメインに対してのみ有効とすることができる。セッション識別子は1回限りのセッションキーを含むことができる。
【００１４】
図3をさらに参照すると、認証サーバ210を含むステーションが、プロセッサ320、メモリ330(および/またはディスクドライブ)、ディスプレイ340およびキーパッドまたはキーボード350を含むコンピュータ310とすることができる。同様に、ユーザクライアント220を含む別のステーションが、プロセッサ、メモリ(および/またはディスクドライブ)、ディスプレイおよびキーパッドまたはキーボードを含むコンピュータとすることができる。ユーザクライアントコンピュータは、マイクロフォン、スピーカ、カメラ、ウェブブラウザソフトウェア等も含む場合がある。さらに、そのステーションは、インターネット240のようなネットワークを介して通信するためのUSB、イーサネット(登録商標)および類似

のインターフェースも含む場合がある。

【００１５】

図4を特に参照すると、本発明は、シングルサインオンドメインを共有ドメイン名を使用する不正サーバへの信用情報漏洩から保護するための別の方法において具現化することができる。その方法は、ドメインレベル(たとえば、domain_name.com)クッキーを用いてサブドメインサーバを認証することができ、その後、別のサブドメイン特有のクッキーを生成することができる。シングルサインオンの場合、そのドメイン内のサブドメイン(たとえば、cs1.domein_name.com)において第1のコンテンツサーバ230‐1によってホスティングされたウェブサイトへのアクセスを要求するユーザブラウザクライアント220(ステップ410)は、サブドメイン:login.domein_name.comを使用する認証サーバ210に宛先変更することができる(ステップ414)。認証サーバは宛先変更要求を受信し、そのドメインのためのユーザの信用情報を入手することができる(ステップ418、422および426)。

【００１６】

理想的には、認証サーバは、特定の下位レベルサブドメイン(たとえば、cs1.domein_name.com)のためのクッキーを生成することができる。しかしながら、一致しないサブドメイン名に対するクッキーは設定することができない。代わりに、認証サーバは、ドメイン:domain_name.comのための限定利用クッキー(1回使用のクッキーなど)において1回限りのセッションキーを生成することができる。さらに、認証サーバは、サブドメイン:login.domein_name.comのための認証サーバ特有のクッキーを生成し、そのクッキーをブラウザクライアントに与えることができる(ステップ430)。ユーザのブラウザクライアントが最初に、アクセスすることを望むウェブサイトにdomain_name.comクッキーを与えるとき(ステップ434)、そのウェブサイトは、認証サーバとのセッションを調べる(ステップ438および442)。認証はそのセッションを無効にして、クッキーの再利用を防ぎ(ステップ446)、その後、そのセッションが有効であったことをウェブサイトに指示する(ステップ450)。その際、ウェブサイトは、ユーザブラウザクライアントに、その下位レベルサブドメインのためのセッションクッキーを与えても安全であることがわかる(ステップ454)。

【００１７】

ユーザブラウザクライアント220が、第2のコンテンツサーバ230‐2によってホスティングされる別のサブドメイン内のウェブサイトに対する認証を望む場合には(ステップ458)、認証サーバ210に宛先変更することができる(ステップ462)。ユーザブラウザクライアントが、早期に得られている(ステップ430)login.domein_name.comクッキーを認証サーバに与えることができ、認証サーバは、domain: domain_name.comのための新たな1回使用のクッキーを返送することができる(ステップ466および470)。第1のコンテンツサーバと同様に(ステップ434～454)、新たな1回使用のクッキーは、認証サーバへの照会によってユーザブラウザクライアントを認証し、要求されたコンテンツを与えるために第2のコンテンツサーバによって使用することができる(ステップ474～494)。ユーザブラウザクライアントが第2のコンテンツサーバからのサブドメインクッキーを有する今、第2のコンテンツサーバはセッション中にそのサブドメイン(cs2.domain-name.com)内で再認証する必要はない。

【００１８】

domain_name.comクッキーの限定利用の態様は、別のウェブサイトがdomain_name.comクッキーを再生し、保護されたウェブサイトにアクセスするのを防ぐ。無効にされたdomain_name.comクッキーが再利用される場合には、第2の認証試行が失敗することになり、そのユーザはその信用情報を与えるように促されることになる。

【００１９】

さらに、無効にされたクッキーを送信する時間を無駄にするのを防ぐために、domain_name.comクッキーは短い満了時間で生成される。本発明の方法はやりとりされるメッセージの数を増やすことができるが、ユーザに代わる任意のさらなる動作を必要としない。

【００２０】

2つ以上の接続に対して有効である唯一のクッキーはサブドメイン特有のクッキーであ

り、これらのクッキーはシングルサインオンドメイン内の他のサブドメインのウェブサイトに送信されないので、その方法はさらに安全にすることができる。したがって、login.domain_name.comサブドメインのためのクッキーが認証サーバ以外のいかなるウェブサイトまたはサーバにも与えられないので、たとえば、不正ウェブサイトへの信用情報漏洩を防ぐことができる。

【００２１】

本発明の別の態様は認証サーバ210に属する場合があり、認証サーバは、認証クッキー102をユーザブラウザクライアント220に与えるための手段310であって、その認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報112を有し、シングルサインオンドメインの認証サブドメインに関連付けられる、与えるための手段と、ブラウザクライアントからのアクセス要求114において認証クッキーを受信するために手段310であって、アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求118に応答して、シングルサインオンドメイン内のコンテンツサーバ230からユーザブラウザクライアントによって受信された宛先変更116に基づく、受信するための手段と、受信された認証クッキー内のユーザ認証信用情報を認証すると、ユーザブラウザクライアントにシングルサインオンドメインのための限定利用クッキー132を転送することによって、アクセス要求に応答するための手段310と、コンテンツサーバから限定利用クッキーのセッション識別子の妥当性を検証する要求134を受信するための手段310であって、コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した、受信するための手段と、限定利用クッキーのセッション識別子の妥当性を検証すると、コンテンツサーバに、コンテンツサーバが要求されたコンテンツ184をユーザブラウザクライアントに転送できるようにするための有効セッションメッセージ182を与えるための手段310とを備える。

【００２２】

本発明の別の態様は認証サーバに属する場合があり、認証サーバはプロセッサ320を備え、プロセッサ320は、認証クッキー102をユーザブラウザクライアント220に与えることであって、その認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報112を有し、シングルサインオンドメインの認証サブドメインに関連付けられる、与えることと、ブラウザクライアントからのアクセス要求114において認証クッキーを受信することであって、アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求118に応答して、シングルサインオンドメイン内のコンテンツサーバ230からユーザブラウザクライアントによって受信された宛先変更116に基づく、受信することと、受信された認証クッキー内のユーザ認証信用情報を認証すると、ユーザブラウザクライアントにシングルサインオンドメインのための限定利用クッキー132を転送することによって、アクセス要求に応答することと、コンテンツサーバから限定利用クッキーのセッション識別子の妥当性を検証する要求134を受信することであって、コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した、受信することと、限定利用クッキーのセッション識別子の妥当性を検証すると、コンテンツサーバに、コンテンツサーバが要求されたコンテンツ184をユーザブラウザクライアントに転送できるようにするための有効セッションメッセージ182を与えることとを実施するように構成される。

【００２３】

本発明の別の態様はコンピュータ可読記録媒体330を含むコンピュータプログラム製品に属する場合があり、コンピュータ可読記録媒体は、コンピュータ310が認証クッキー102をユーザブラウザクライアントに与えるためのコードであって、その認証クッキーはシングルサインオンドメインのための少なくとも1つのユーザ認証信用情報112を有し、シングルサインオンドメインの認証サブドメインに関連付けられる、与えるためのコードと、コンピュータ310がブラウザクライアントからのアクセス要求114において認証クッキーを受信するためのコードであって、アクセス要求は、ユーザブラウザクライアントからのコンテンツ要求118に応答してシングルサインオンドメイン内のコンテンツサーバ230からユーザブラウザクライアントによって受信された宛先変更116に基づく、コンピュータが受信

するためのコードと、受信された認証クッキー内のユーザ認証信用情報を認証すると、ユーザブラウザクライアントにシングルサインオンドメインのための限定利用クッキー132を転送することによって、コンピュータ310がアクセス要求に応答するためのコードと、コンピュータ310がコンテンツサーバから限定利用クッキーのセッション識別子の妥当性を検証する要求134を受信するためのコードであって、コンテンツサーバはユーザブラウザクライアントから限定利用クッキーを受信した、コンピュータが受信するためのコードと、限定利用クッキーのセッション識別子の妥当性を検証すると、コンピュータ310が、コンテンツサーバに、コンテンツサーバが要求されたコンテンツ184をユーザブラウザクライアントに転送できるようにするための有効セッションメッセージ182を与えるためのコードとを含む。

【００２４】

情報および信号が、種々の異なる技術および技法のいずれかを用いる表される場合があることは、当業者には理解されよう。たとえば、上記の説明全体にわたって参照される場合があるデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁界または磁性粒子、光場または光学粒子、あるいはそれらの任意の組合せによって表される場合がある。

【００２５】

本明細書において開示された実施形態に関連して説明された種々の例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実現される場合があることは、当業者にはさらに理解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、種々の例示的な構成要素、ブロック、モジュール、回路、およびステップが、上記でそれらの機能に関して包括的に説明された。そのような機能がハードウェアとして実装されるか、ソフトウェアとして実施されるかは、特定の応用形態およびシステム全体に課される設計上の制約よって決まる。当業者は、説明された機能を特定の応用形態ごとに様々なやり方で実施することができるが、そのような実施の決定は、本発明の範囲からの逸脱を生じるものと解釈されるべきではない。

【００２６】

本明細書において開示された実施形態に関連して説明された種々の例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタルシグナルプロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書において説明される機能を実行するように設計されたそれらの任意の組合せによって、実施または実行することができる。汎用プロセッサはマイクロプロセッサとすることができるが、代替形態では、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。また、プロセッサは、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、または任意の他のそのような構成として実現することもできる。

【００２７】

本明細書において開示された実施形態に関連して説明された方法またはアルゴリズムのステップは、直接ハードウェアにおいて具現化することができるか、プロセッサによって実行されるソフトウェアモジュールにおいて具現化することができるか、またはその2つの組合せで具現化することができる。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、取外し可能ディスク、CD-ROM、または当技術分野において既知である任意の他の形態の記憶媒体内に存在することができる。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替形態として、記憶媒体はプロセッサと一体にすることができる。プロセッサおよび記憶媒体はASIC中に存在することができる。ASICはユーザ端末中に存在することができる。代替形

態では、プロセッサおよび記憶媒体は、ユーザ端末内に個別構成要素として存在することができる。

【００２８】

1つまたは複数の例示的な実施形態では、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実現することができる。コンピュータプログラム製品としてソフトウェアにおいて実現される場合、それらの機能は、1つまたは複数の命令またはコードとしてコンピュータ可読記録媒体上に記憶することができる。コンピュータ可読記録媒体は、ある場所から別の場所へのコンピュータプログラムの移送を容易にするコンピュータ記憶媒体を含む。記憶媒体は、コンピュータによってアクセス可能である任意の入手可能な媒体とすることができる。例として、限定はしないが、そのようなコンピュータ可読記録媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、または命令もしくはデータ構造の形で所望のプログラムコードを記憶するために用いることができ、コンピュータによってアクセス可能である、任意の他の媒体を含むことができる。本明細書で使用する場合、ディスク(disk)およびディスク(disc)は、コンパクトディスク(CD)、レーザディスク、光ディスク、デジタル多用途ディスク(DVD)、フロッピー(登録商標)ディスク、およびブルーレイディスクを含み、ディスク(disk)は、通常、磁気的にデータを再生し、一方、ディスク(disc)は、レーザで光学的にデータを再生する。上記の組合せもコンピュータ可読記録媒体の範囲内に含まれるべきである。

【００２９】

開示される実施形態の上記の説明は、任意の当業者が本発明を実施または使用できるようにするために提供される。これらの実施形態への様々な変更が当業者には容易に明らかになり、本明細書において規定される一般原理は、本発明の趣旨および範囲から逸脱することなく他の実施形態に適用することができる。したがって、本発明は、本明細書に示される実施形態に限定されるものではなく、本明細書において開示される原理および新規の特徴に矛盾しない最も広い範囲を与えられるべきである。

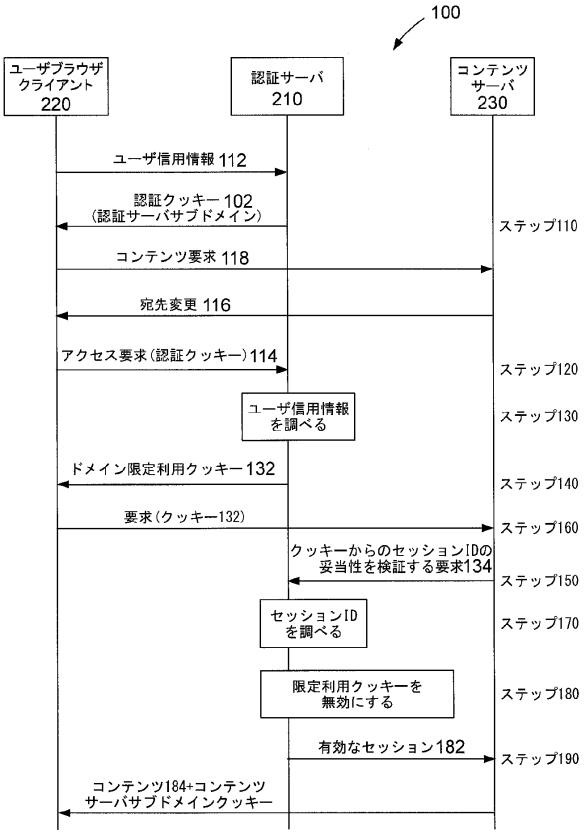
【符号の説明】

【００３０】

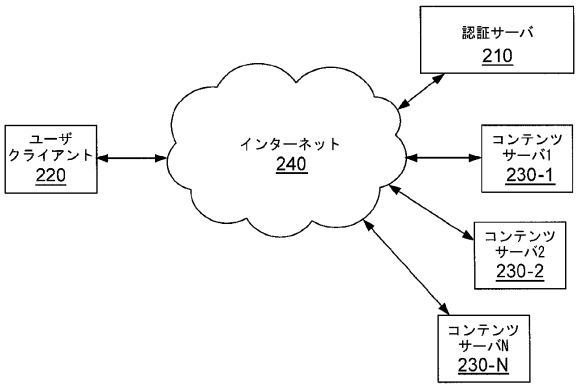
100 方法
102 認証クッキー
110 ステップ
112 ユーザ認証信用情報
114 アクセス要求
116 宛先変更
118 コンテンツ要求
120 ステップ
132 限定利用クッキー
130 ステップ
134 要求
140 ステップ
150 ステップ
160 ステップ
170 ステップ
180 ステップ
182 有効セッションメッセージ
184 コンテンツ
190 ステップ
210 認証サーバ
220 ユーザブラウザクライアント
230 コンテンツサーバ

230-1　第1のコンテンツサーバ
230-2　第2のコンテンツサーバ
240　インターネット
310　コンピュータ
320　プロセッサ
330　メモリ又はディスクドライブ
340　ディスプレイ
350　キーパッド又はキーボード
410　ステップ
414　ステップ
418　ステップ
422　ステップ
426　ステップ
430　ステップ
434　ステップ
438　ステップ
442　ステップ
446　ステップ
450　ステップ
454　ステップ
458　ステップ
462　ステップ
466　ステップ
470　ステップ
474　ステップ
478　ステップ
482　ステップ
486　ステップ
490　ステップ
494　ステップ

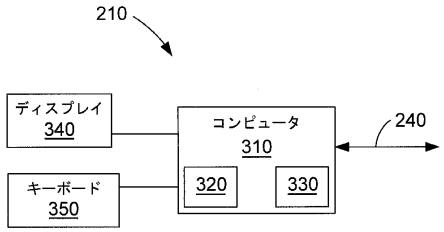
【図１】


100
ユーザブラウザ
クライアント
220
認証サーバ
210
コンテンツ
サーバ
230
ユーザ信用情報 112
認証クッキー 102
(認証サーバサブドメイン)
ステップ110
コンテンツ要求 118
宛先変更 116
アクセス要求(認証クッキー)114
ステップ120
ユーザ信用情報
を調べる
ステップ130
ドメイン限定利用クッキー132
ステップ140
要求(クッキー132)
ステップ160
クッキーからのセッションIDの
妥当性を検証する要求134
ステップ150
セッションID
を調べる
ステップ170
限定利用クッキーを
無効にする
ステップ180
有効なセッション182
ステップ190
コンテンツ184+コンテンツ
サーバサブドメインクッキー

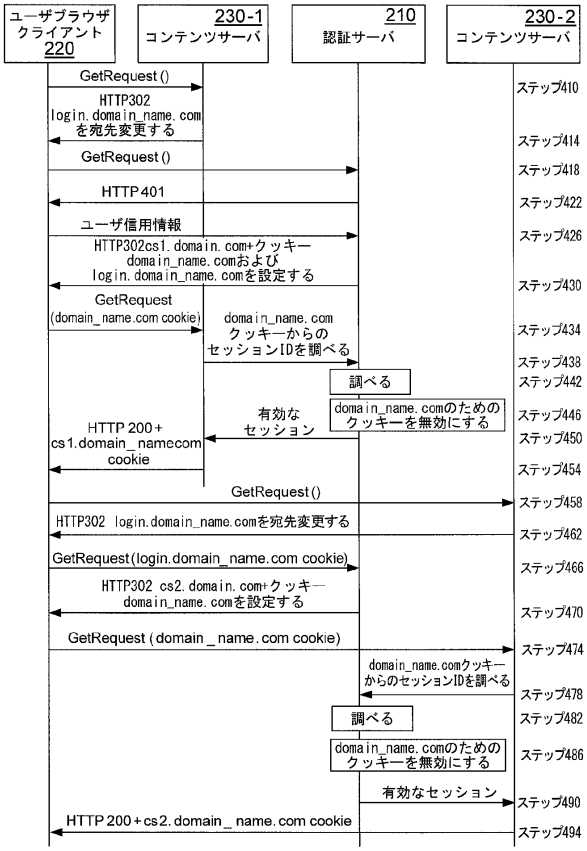
【図２】


認証サーバ
210
ユーザ
クライアント
220
インターネット
240
コンテンツ
サーバ1
230-1
コンテンツ
サーバ2
230-2
コンテンツ
サーバN
230-N

【図３】


210
ディスプレイ
340
コンピュータ
310
240
キーボード
350
320
330

【図４】


ユーザブラウザ
クライアント
220
230-1
コンテンツサーバ
210
認証サーバ
230-2
コンテンツサーバ
GetRequest()
ステップ410
HTTP302
login.domain_name.com
を宛先変更する
ステップ414
GetRequest()
ステップ418
HTTP401
ステップ422
ユーザ信用情報
ステップ426
HTTP302cs1.domain.com+クッキー
domain_name.comおよび
login.domain_name.comを設定する
ステップ430
GetRequest
(domain_name.com cookie)
ステップ434
domain_name.com
クッキーからの
セッションIDを調べる
ステップ438
調べる
ステップ442
有効な
セッション
domain_name.comのための
クッキーを無効にする
ステップ446
HTTP 200+
cs1.domain_namecom
cookie
ステップ450
ステップ454
GetRequest()
ステップ458
HTTP302 login.domain_name.comを宛先変更する
ステップ462
GetRequest(login.domain_name.com cookie)
ステップ466
HTTP302 cs2.domain.com+クッキー
domain_name.comを設定する
ステップ470
GetRequest(domain_name.com cookie)
ステップ474
domain_name.comクッキー
からのセッションIDを調べる
ステップ478
調べる
ステップ482
domain_name.comのための
クッキーを無効にする
ステップ486
有効なセッション
ステップ490
HTTP 200+cs2.domain_name.com cookie
ステップ494

フロントページの続き

(72)発明者　クレイグ・エム・ブラウン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　マイケル・ダブリュ・パドン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　平井　誠

(56)参考文献　特開２００４－１８５６２３（ＪＰ，Ａ）
特表２００５－５１９５０１（ＪＰ，Ａ）
国際公開第２００５／０１５４２２（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１