【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2004-533075(P2004-533075A)
【公表日】平成16年10月28日(2004.10.28)
【年通号数】公開・登録公報2004-042
【出願番号】特願2003-504584(P2003-504584)
【国際特許分類】
Ｇ０６Ｆ　21/20　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　　３３０Ａ

【手続補正書】
【提出日】平成17年5月26日(2005.5.26)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
クライアントが保護されたリソース又はアプリケーションにアクセスすることを可能にするセキュリティシステムであって、
保護されたアプリケーションへのアクセスについての、クライアントからの要求を受け取り、前記要求をセキュリティサービスに伝えるアプリケーションインターフェース機構を備え、
前記クライアントが、アプリケーションコンテナに対して前記要求を作成し、前記アプリケーションコンテナが、前記要求及びコールバックで、セキュリティサービスを呼び出し、さらに、
前記要求を許可又は拒否する判定を行うセキュリティサービスを備え、
前記セキュリティサービスが、該セキュリティサービス内に差し込むことのできる複数のセキュリティプロバイダーを含み、かつ、前記セキュリティプロバイダーが、前記要求のために前記アプリケーションコンテナから状況情報を要求するために、コールバックハンドラを使用し、かつ、前記セキュリティプロバイダーからの出力に依って、前記セキュリティサービスが、前記クライアントが前記保護されたアプリケーションを使用するための権限の付与を定め、さらに、
許可されたアクセス要求を前記保護されたアプリケーションへ伝えるリソースインターフェース、
を備えるセキュリティシステム。
【請求項２】
前記アプリケーションインターフェース機構が、アプリケーション配置記述を読み取り、前記配置記述をセキュリティサービス内に登録するためのアプリケーションコンテナを含む、
請求項１記載のセキュリティシステム。
【請求項３】
前記アプリケーションコンテナが、EnterpriseJavaBeansコンテナである、
請求項２記載のセキュリティシステム。
【請求項４】
前記アプリケーションコンテナが、WebAppコンテナである、

請求項２記載のセキュリティシステム。
【請求項５】
前記セキュリティサービスが、アクセスポリシーを定義し、前記アクセス要求を許可、拒否、又は保留の寄与判定を定めるための複数のアクセス判定機構を含む、
請求項１記載のセキュリティシステム。
【請求項６】
前記セキュリティサービスが、前記アクセス要求を前記複数のアクセス判定機構に転送し、前記寄与判定を合体させて、前記アクセス要求を許可又は拒否するセキュリティサービスによる一つの全体判定とするアクセス制御装置をさらに含む、
請求項５記載のセキュリティシステム。
【請求項７】
前記アクセス判定が、ビジネス機能に関連するアクセスポリシーを表すものである、
請求項５記載のセキュリティシステム。
【請求項８】
アクセスポリシーにおける変更を反映するために、アクセス判定がセキュリティサービスに付加される、
請求項５記載のセキュリティシステム。
【請求項９】
前記保護されたリソースに前記クライアントがアクセスすることができる権限の付与を定義するために、前記アクセス判定機構が使用される、
請求項５記載のセキュリティシステム。
【請求項１０】
前記アクセス判定機構のいずれか一つによる拒否又は保留によって、セキュリティサービスがアクセス要求を拒否するようになった、
請求項５記載のセキュリティシステム。
【請求項１１】
前記アクセス判定機構のいずれか一つによる保留によっては、セキュリティサービスがアクセス要求を拒否しないようになった、
請求項５記載のセキュリティシステム。
【請求項１２】
前記セキュリティサービスが、前記複数のアクセス要求に対する判定を検査するための検査メカニズムをさらに含む、
請求項５記載のセキュリティシステム。
【請求項１３】
前記リソースインターフェースが、保護されたリソースへの要求、又は保護されたリソースからの要求を通すためのインターフェース機構を含む、
請求項１記載のセキュリティシステム。
【請求項１４】
前記インターフェース機構が、JavaJ2EEセキュリティインターフェースを含む、
請求項１３記載のセキュリティシステム。
【請求項１５】
前記インターフェース機構が、セキュリティプロバイダーインターフェースを含む、
請求項１３記載のセキュリティシステム。
【請求項１６】
前記インターフェース機構が、前記リソースインターフェースの中にプラグインとして含まれる、
請求項１３記載のセキュリティシステム。
【請求項１７】
セキュリティサービスがさらに、前記保護されたリソースから前記クライアントへの、前記アクセス要求に対する応答を許可するか又は拒否するかを判定する、

請求項１記載のセキュリティシステム。
【請求項１８】
クライアントが保護されたアプリケーションにアクセスすることを可能にする方法であって、
保護されたアプリケーションへのアクセスについてのクライアントからの要求を、アプリケーションコンテナで受け取るステップと、
前記要求を、コールバックと共に、前記アプリケーションコンテナからセキュリティサービスに伝えるステップと、
前記セキュリティサービス内に差し込むことのできる複数のセキュリティプロバイダーを含む該セキュリティサービスにおいて、前記アクセス要求を許可するか、又は拒否するかを判定するステップと、
前記要求のために前記アプリケーションコンテナから状況情報を要求するために、各セキュリティプロバイダーにおいて、コールバックハンドラを使用するステップと、
前記セキュリティサービスからの出力に依って、前記クラインとが前記保護されたアプリケーションを使用するための権限の付与を定めるステップと、
許可された要求を、前記保護されたアプリケーションへ伝達するステップと、
を含む方法。
【請求項１９】
前記アプリケーションインターフェース機構が、アプリケーション配置記述を読み取り、前記配置記述をセキュリティサービス内に登録するアプリケーションコンテナを含む、
請求項１８記載の方法。
【請求項２０】
前記アプリケーションコンテナがEnterpriseJavaBeansコンテナである、
請求項１９記載の方法。
【請求項２１】
前記アプリケーションコンテナがWebAppコンテナである、
請求項１９記載の方法。
【請求項２２】
複数のアクセス判定機構を介して前記セキュリティサービス内にアクセスポリシーを定義するステップと、
各アクセス判定機構において、前記アクセス要求を許可、拒否、又は保留するための寄与判定を定めるステップと、
をさらに含む、請求項１８記載の方法。
【請求項２３】
前記アクセス要求を、アクセス制御装置を介して、前記複数のアクセス判定機構に転送し、前記アクセス要求を許可又は拒否するために、前記寄与判定を合体させてセキュリティサービスによる一つの全体判定とするステップ、
をさらに含む請求項２２記載の方法。
【請求項２４】
前記アクセス判定が、ビジネス機能に関連するアクセスポリシーを表すものである、
請求項２２記載の方法。
【請求項２５】
アクセスポリシーにおける変更を反映するために、アクセス判定がセキュリティサービスに付加される、
請求項２２記載の方法。
【請求項２６】
前記保護されたリソースに前記クライアントがアクセスすることができる権限の付与を定義するために、前記アクセス判定機構を使用するステップ、
をさらに含む、請求項２２記載の方法。
【請求項２７】

前記アクセス判定機構のいずれか一つの拒否又は保留によりセキュリティサービスがアクセス要求を拒否するようになった、
請求項２２記載の方法。
【請求項２８】
前記アクセス判定機構のいずれか一つの保留によってはセキュリティサービスがアクセス要求を拒否しないようになった、
請求項２２記載の方法。
【請求項２９】
検査機構を介して前記複数のアクセス要求の判定を検査するステップ、
をさらに備える、請求項２２記載の方法。
【請求項３０】
リソースインターフェースを介して伝達する前記ステップが、インターフェース機構を介して、保護されたリソースへの、あるいは保護されたリソースからの要求を通すステップを含む、
請求項１８記載の方法。
【請求項３１】
前記インターフェース機構がJavaJ2EEセキュリティインターフェースを含む、
請求項３０記載の方法。
【請求項３２】
前記インターフェース機構がセキュリティプロバイダーインターフェースを含む、
請求項３０記載の方法。
【請求項３３】
前記インターフェース機構が、前記リソースインターフェースの中でプラグインとして含まれる、
請求項３０記載の方法。
【請求項３４】
前記保護されたリソースから前記クライアントへの前記アクセス要求に対する応答を、許可するか、又はは拒否するかの判定を行うステップ、
をさらに備える、請求項１８記載の方法。
【請求項３５】
セキュアな環境における保護されたリソースへのユーザーのアクセス権限の付与を定める方法であって、
前記アクセス要求及びコールバックで、セキュリティサービスを呼び出すことにより、保護されたリソースへのアクセスについてのユーザーアプリケーションからのアクセス要求を受け取るステップと、
前記セキュリティサービス内に差し込むことのできる複数のセキュリティプロバイダーをポーリングすることを含む、前記保護されたリソースへのアクセスについてのユーザーの権限付与を定めるステップと、
を含み、前記セキュリティプロバイダーは、前記要求のために前記アプリケーションコンテナから状況情報を要求するために、コールバックハンドラを使用し、さらに、
前記セキュリティサービスにおいて、前記ユーザーへの権限付与に基づき、前記アクセス要求を許可、又は拒否する判定を行うステップと、
(a)許可されたアクセス要求を前記保護されたリソースへ伝えるステップ、又は(b)拒否されたアクセス要求を前記保護されたリソースに与えないステップ、のいずれか一方のステップと、
を含む方法。
【請求項３６】
前記権限付与が、前記保護されたリソースのユーザーに利用可能なアクセスの形式を定めるものである、
請求項３５記載の方法。

【請求項３７】
前記アクセスの形式が、前記保護されたリソースの一部又は全部を、開く、修正する、削除する、コピーする、のいずれかを含む、
請求項３６記載の方法。
【請求項３８】
前記ユーザーの権限付与についての情報を、第一のセキュリティ領域から第二のセキュリティ領域へ伝えることができる、
請求項３５記載の方法。
【請求項３９】
前記ユーザーの権限付与についての情報を、前記第一のセキュリティ領域から前記第二のセキュリティ領域へ伝える前に、前記第一のセキュリティ領域からの付加的情報を使用してユーザーの権限付与を修正することができる、
請求項３８記載の方法。