M-2

権限管理に対応した認証・アクセス制御技術

Authentication And Access Control Technology Corresponding To Authority Management

柳原 秀明† Hideaki Yanagihara
西田 廣治‡ Hiroji Nishida

1．はじめに

IT化の進展に伴い、インターネットやイントラネットを介して膨大な情報から必要なデータに迅速にアクセスできる環境となってきている反面、不正アクセスによる機密情報の漏洩といった情報セキュリティ上の犯罪が後を絶たないのが現状である。また、既存の業務アプリケーションに加え、電子決裁など新たな業務アプリケーションが増えるに従い、情報システム利用者のログイン操作が煩雑になり、安易な文字列の使用やメモ書き等によるパスワードのずさんな管理によって、成りすましによる不正アクセスの温床が多々存在しているのも非常に問題となっている。

そのため、組織・個人の権限管理、権限に応じたアクセス制御、一回の認証で複数のアプリケーションを利用可能とするシングルサインオンやバイオメトリクスによる個人識別を行える情報システム利用環境が求められる。

本稿では、これら要件に応じたWeb業務アプリケーションの認証・アクセス制御システムに要する技術の抽出と実現方式について報告する。

2．所要技術項目

図1に、当方で構築した認証・アクセス制御システムの利用イメージを示す。

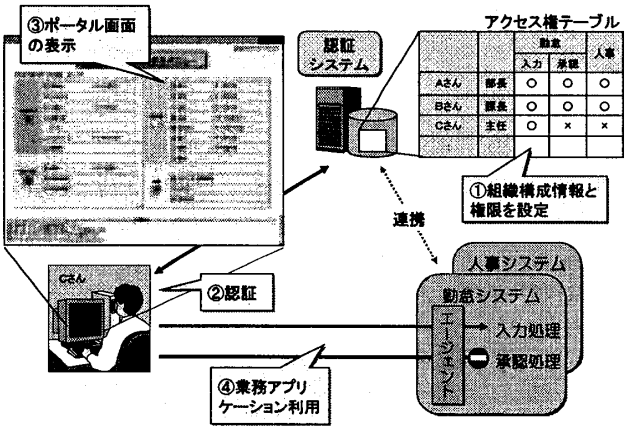

図1　システムの利用イメージ

認証・アクセス制御システムにおける、所要技術の概要を以下にあげる。

(1) 世代管理に対応した組織情報設定と所属部署、役職、分類や個人等に応じた権限設定
(2) ユーザID・パスワードまたは指紋による一回の認証で、複数の業務アプリケーションを利用可能とするシングルサインオン
(3) 既存の業務アプリケーションの改造の必要がなくシングルサインオンへの対応を可能とする
(4) 職員／社員がアクセス可能な業務アプリケーションとその機能の一覧や決裁待ち案件等の件数を統合的に表示するポータル画面
(5) 権限に応じた業務アプリケーション、ディレクトリ及びファイル単位のアクセス制御
(6) 離席中のセキュリティ確保に対応した自動ログアウト
(7) パスワードの連続失敗回数の制限、有効期間や設定文字制約等のパスワードポリシー設定
(8) 認証情報APIを用いた業務アプリケーションによる利用者情報の取得

3．技術の実装

図2に認証・アクセス制御システムにおける機能関連図を示す。図中の網掛け部分が、認証・アクセス制御システムの範囲である。

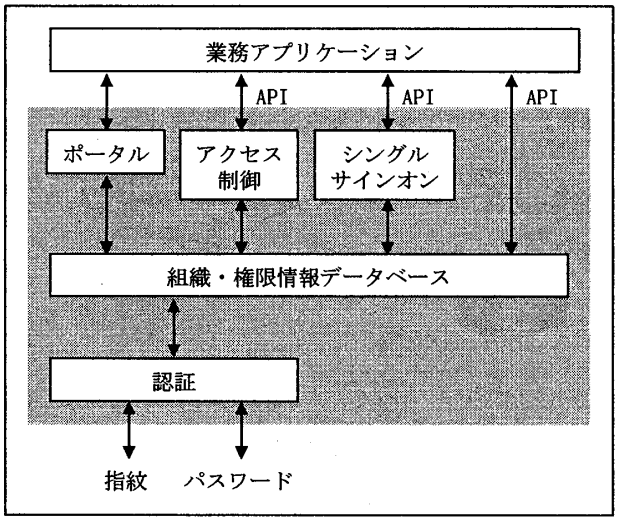

図2　機能関連図

認証・アクセス制御システムの所要技術について、その実現方式を以下に説明する。

† 富士電機(株) 事業開発室
‡ 富士電機(株) 事業開発室

3.1 権限設定と世代管理

利用者の所属部署、役職、補職、役割、分類や個人の単位でアクセス権の付与・抹消が行え、それらの AND／OR 条件の重複による木目細やかな設定を可能とする。部署に対しアクセス権を付与した場合は、その下位の部署に所属する職員／社員も対象とする。例えば、A課に所属する係長全員とB課全員は基本的にアクセス可能だが、ただし正社員でない利用者はアクセス不可といった複雑な設定にも柔軟に対応することが可能である。

図３に利用者の権限情報生成の方式を示す。

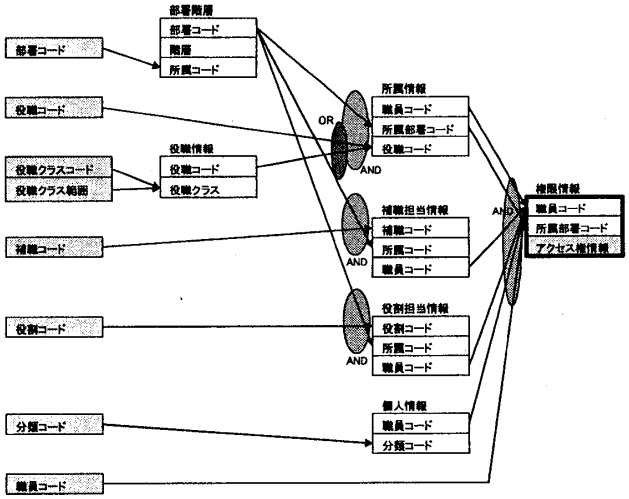

図３　利用者の権限情報生成

組織・個人情報は、世代管理を行うことで過去の組織情報の参照や組織変更のスムーズな対応を可能とする。

図４に、組織・個人情報の世代管理方式を示す。

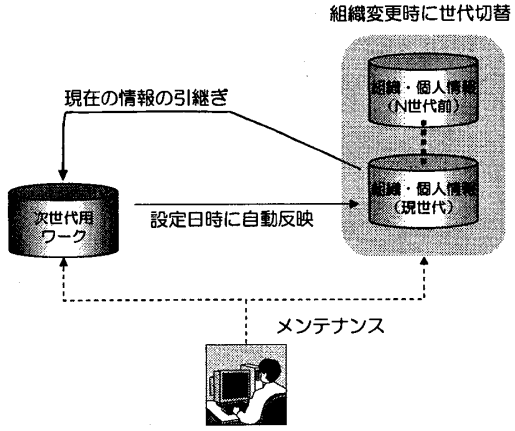

図４　組織・個人情報の世代管理

3.2 処理権限チケット

認証完了時に、利用者の権限情報を処理権限チケットとして利用者に発行する。処理権限チケットは Web の Cookie としてクライアント側に保存され、同一ドメインに属する Web サーバで参照可能である。

処理権限チケットには、表１に示すように、権限情報やアクセス権情報以外に、利用者の氏名・職員コード等の業務アプリケーションで共通に利用する情報も含む。さらに、クライアント固有の情報を付加し、処理権限チケット自体を暗号化することで、盗聴等による情報漏洩、改竄や成りすましへの利用を防止する。

表１：処理権限チケットの内容

分類	内容
認証情報	ユーザ ID
利用者情報	職員／社員コード、氏名 所属部署コード、所属部署名 役職コード、役職名 補職コード、補職名 役割コード、役割名 所属の兼任数
クライアント情報	IP アドレス等
その他	チケット発行日時等

この処理権限チケットは、業務アプリケーションの Web サーバに適用するエージェントモジュールにより参照され、認証済みであるかまたはアクセス権限があるかの判別に利用する。

3.3 業務アプリケーションとの連携

認証情報 API により、業務アプリケーション側で利用者の氏名、所属、役職、役割やユーザ ID 等の情報を取得することができ、業務アプリケーションにおける各種処理に利用することを可能としている。

また、業務アプリケーションに必要な認証情報をあらかじめ定義しておくことで、業務アプリケーションへのアクセス時の HTTP リクエストメッセージに認証情報を自動的に付加することができる。これにより、業務アプリケーションの改造なくシングルサインオンへの対応を可能としている。

4．まとめ

本稿では、業務遂行と密接に関連した権限情報をもとにした認証・アクセス制御を行うための技術の実装方式について報告を行った。本方式により、複数の業務アプリケーション利用環境における権限情報の一元化、シングルサインオンとアクセス制御への対応を実現でき、利便性とセキュリティの両立を図ることが可能となる。

今後は、ポータル画面の個人カスタマイズ、個人属性情報をもとに X.509 フォーマットの属性証明書を用いたアクセス制御等により、様々なシステム利用環境への対応とそのセキュリティ強化に向けた取組みを実施していく計画である。

参考文献

[1] 西田,柳原,近藤：自治体のセキュリティを守る電子認証ソリューション,富士時報,Vol.74 No.3, pp192-195 (2001)