3A-5

情報漏洩防止ソリューション(2)
- アクセス制御情報統合管理 -

小宮　崇†　　大沼　聡久†　　近藤　誠一†　　遠藤　淳‡
三菱電機株式会社†　　三菱電機インフォメーションシステムズ株式会社‡

1. はじめに

近年、企業の機密情報が外部へ流出する事件が多発しており、企業として確固たる対策が必要となっている。情報漏洩防止ソリューションは、その対策を実現するセキュリティのトータルソリューションである。

本ソリューションでは、情報漏洩を防止する複数のセキュリティコンポーネントを提供する。各コンポーネントで使用するユーザ情報とアクセス制御情報を、LDAP ディレクトリを用いて統合管理する。その結果、ユーザ情報散在防止、ソリューション全体のセキュリティポリシー統一、管理コストの低減といった効果を得ることができる。

2. ディレクトリ構成

本ソリューションで管理する情報の構成を図 1 に示す。

(1)ユーザ情報と組織情報

ユーザ情報と組織情報を独立させて、相互リンクを張る構造とした。その結果、配属の変更が容易となり、人事異動・組織改変時の管理負荷低減が可能となった[1]。

(2)アクセス制御情報とロール情報

アクセス制御情報は、制御の対象となるコンテンツとそのアクセス条件から成る。アクセス条件はアクセス可能ユーザ、アクセス可能時間、有効時間等から成る。アクセス可能ユーザは、ユーザのグループを定義するロールを用いて表現する。コンテンツは上下関係を有するメニュー、Web コンテンツを考慮して階層構造とし、下位へのアクセス条件の継承を可能とした。ロールはアクセス制御情報と別に管理し、フラットに配置することにより被参照性能の向上を実現した。

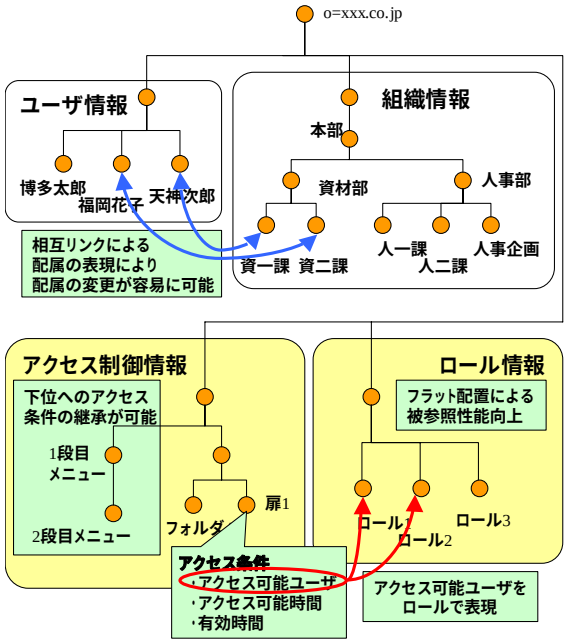

図 1. ディレクトリ構成

3. 課題

3.1 課題１：人事異動や組織改変時のロール再定義

一般的に、ロールはアクセス性能を考慮して構成するユーザを羅列して定義する方式を取ることが多い。その場合、人事異動や組織改変時にユーザ情報の変更にあわせてロールのグループ内容の再設定が必要となり、その作業負荷の大きさが課題である。

3.2 課題２：アクセス条件の表現方法

アクセス制御情報の統合管理では、用途が異なるセキュリティコンポーネントのアクセス条件を管理するため、様々なアクセス条件の実現が必要となる。

ロールによるアクセス管理を行うセキュリティ製品[2]では、1 つのアクセス条件を 1 つ以上のロールの論理和で組み合わせて表現する。しかし、論理和のみでの表現では多数のロールが必要となる点が課題である。

Information Leak Prevention Solution (2) – Integrated management of user information and access control information -

Takashi Komiya†, Akihisa Oonuma†, Seiichi Kondo† and Jun Endo‡
† Mitsubishi Electric Corporation.
‡ Mitsubishi Electric Information Systems Corporation.

4. 課題の解決方法

上記課題の解決のために、以下の 2 つの手法を取った。

4.1 課題の解決方法１

本ソリューションでは、抽象ロールを提供することにより、人事異動・組織改変時のロール再設定の作業負荷低減に対応した。抽象ロールは、一般的なロールとはユーザグループ定義方法が異なり、ユーザ属性情報を用いてロールを構成するユーザを定義する。図 2 に抽象ロールを用いたアクセス条件の実現方式を示す。

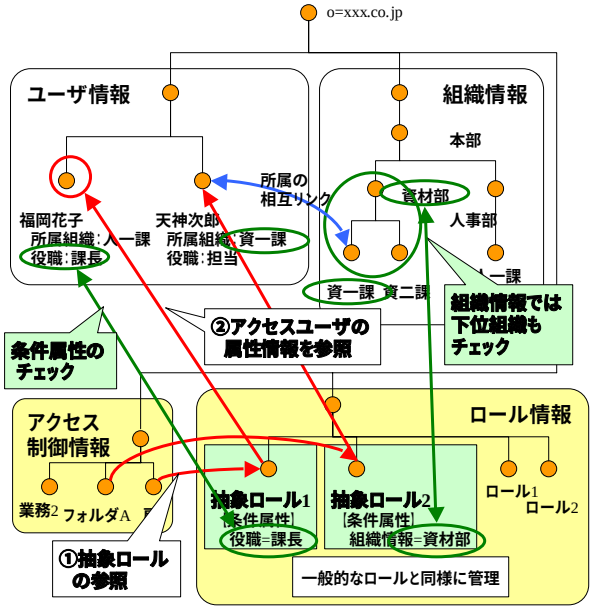

図 2．抽象ロールを用いたアクセス条件の実現

抽象ロールは条件属性としてユーザ情報の属性名と値の対を持ち、所属するユーザの条件を示す。抽象ロールは一般のロールと同様に管理し、アクセス条件の指定時に混在可能とした。

抽象ロールは、実行時にアクセス条件から参照されると、アクセスしたユーザの属性情報を参照する。次にその属性情報と条件属性を比較し、条件属性を満たすか判定する。条件属性に組織情報が定義されている場合には、下位組織へのアクセス権限継承をサポートし、アクセスユーザが条件の組織以下に所属する場合に条件属性を満たすと判定する。

本方式によって、抽象ロールは実行時にユーザ情報・組織情報を参照するため、人事異動に即座に追随可能である。

また、日本企業では組織主体のユーザ管理が行われるため、組織に結びつけたアクセス制御が行われる。そこで、組織情報の抽象ロールを自動的に生成して提供することにより、組織改変に即座に対応可能とした。

4.2 課題の解決方法２

本ソリューションでは、アクセス条件を表現するためのロールの組み合わせ方法に論理積と否定を追加することにより、ロール数の削減に対応した。追加の有無での必要ロール数の比較例を図 3 に示す。

登録ユーザ	所属組織	役職	登録ユーザ	所属組織	役職
A	資一課	課長	C	資二課	課長
B	資一課	担当	D	資二課	担当

以下のアクセス条件を表現する

ロールによるアクセス条件の表現

アクセス条件	論理和のみで表現	論理和･論理積･否定で表現
課長	A,C	A,C
課長以外	B,D	¬A,C
資一課 課長	A	A,B ∩ A,C

A A,C B,D
3つのロールが必要

A,B A,C
2つのロールが必要

図 3．必要ロール数の比較

図 3 の例では、論理和のみで表現した場合では 3 つのロールが必要であるのに対し、論理積・否定を追加することで 2 つのロールで表現することができる。このように、アクセス条件の表現方法の充実により、ロール管理負荷の低減を実現した。

一方で、アクセス条件の判定のためにユーザ属性や多段階にわたる組織情報の参照が必要となり、実行性能に影響を及ぼす。本ソリューションでは、LDAP ディレクトリを採用し、参照順のリンクを予め定義しておくことにより、高速化を図った。

5. おわりに

本稿では、情報漏洩防止ソリューションのアクセス制御情報の統合管理に関する課題と解決方法について述べた。その結果、人事異動・組織改変時の運用コスト低減と、ロール管理負荷の低減を実現した。

今後の課題として、独立性の高いシステムに対応するためのユーザ情報、アクセス制御情報のプロビジョニングが挙げられる。

参考文献

[1]五月女他、”金融情報システム向けセキュア情報活用ソリューション”、三菱電機技報 Vol.77,No.4,2003.

[2]IBM WebSphere Portal http://www-6.ibm.com/jp/domino07/lotus/home.nsf/Content/wp