5Q-08 POLICYCOMPUTING™アーキテクチャによる情報セキュリティポリシーの実装と導入

坂田　祐司[†]、小熊　慶一郎[†]、田中　俊介[†]、菅野　政孝[††]、松田 栄之[†]
（株）NTT データ　情報科学研究所[†]、英国支店[††]
e-mail: {ysakata@rd,bak@rd,shun@rd, suganom@noanet,matu@rd}.nttdata.co.jp

1. はじめに

われわれはマスターポリシー(ポリシー策定者が理解しやすい表現形式のポリシー)によって情報システム内のすべてのリソース(ユーザ、サーバプロセス、ネットワーク機器など)を一元的に管理する仕組みである POLICYCOMPUTING™ を提案してきた[1][2]。

今回、情報セキュリティポリシーに対して POLICY COMPUTING™ を適応し、その有用性を検証した。

2. 情報セキュリティポリシーの導入

2.1. 情報セキュリティポリシー

一般的に企業など何らかの目的を持った組織はその内部で情報を積極的に共有し利用できるようにする一方、情報を適切に取り扱うことにより目的外の利用から保護することが求められている。そのための組織全体の決まりが情報セキュリティポリシーである。

2.2. アクセス制御ポリシー

情報セキュリティポリシーを遵守するにあたり、ユーザの教育や、管理体制や管理フローの決定などの運用による解決も重要であるが、どのような情報にどのような人をアクセス可能にすべきかというアクセス制御ポリシー(例を表 1 に示す)は、情報がWWWサーバやグループウェアサーバ等の、情報システム上に存在することが多い現在において、それらシステムよって解決されている場合が多い。

表 1: アクセス制御ポリシーの例

情報種別項目		セキュリティポリシー	
大項目	小項目	機密レベル	開示範囲
研究開発成果	研究成果	厳秘	グループ内
	研究テーマ	秘密	研究所内
	実験結果	秘密	研究所内
	報告書	社外秘	社員全員

現状、電子情報に対してのアクセス制御ポリシーを遵守するための仕組みや設定は、情報作成者(もしくは作成者に依頼された情報システム管理者)が行なうことが一般的である。

これは管理が分散しているクライアントサーバシステムにおいては管理業務を増大させる結果になっている。今回は管理業務増大の解決のために POLICY COMPUTING™ を導入する。これを用い、アクセス制御ポリシーをマスターポリシーとして定義し、個々のリソースがその定義に従い動作する環境を構築するものとする。

Implementation and deployment of Information Security Policy under the POLICYCOMPUTING™ Architecture
Yuji Sakata, Keiichiro Oguma, Shunsuke Tanaka,
Masataka Sugano, Shigeyuki Matsuda,
NTT DATA CORPORATION

3. POLICYCOMPUTING™ によるシステムの構築

情報作成者がアクセス制御ポリシーの情報種別項目を指定するのみで、個々の情報システムが定められたポリシーに従って、情報を扱うようにするために以下のようなシステムを構築した。

3.1. システムのアーキテクチャ

最初に明文化されたポリシーをコンピュータが理解できる形式で電子的に保存しなければならない。

POLICYCOMPUTING™ ではそのレポジトリとしてディレクトリサーバを用いる。 情報システムが存在するサーバに追加されるリソースエージェントは、ディレクトリサーバに蓄積されている情報を解釈し個別の設定がそのポリシーを満たすように自動的な変更を行なう。 またディレクトリサーバは通常変更の通知を行なう事が出来ないため、アクセスコントローラがディレクトリの変更情報を各リソースエージェントに通知する。 情報作成者は提供される UI により、情報の種別を選択するのみでポリシーが適用される。(図 1)

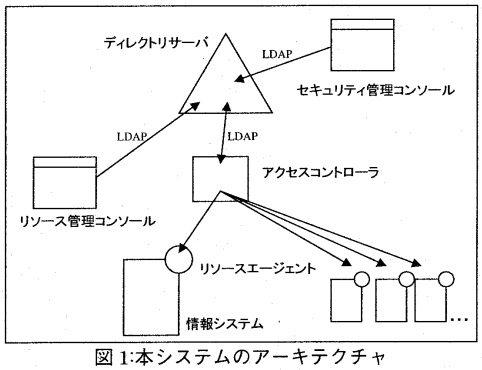

図 1:本システムのアーキテクチャ

3.2. アクセス制御ポリシーの変換

3.1 で述べたようにアクセス制御ポリシーはディレクトリサーバのエントリとして表現される。

(表 1)で示されるように、アクセス制御ポリシーは情報システムの設定に依存しない記述方法で記載されるものであり、そのような抽象的な記述を定義できるようにする必要がある。

アクセスコントロールの仕組みは認証(Authentication)と許可(Authorization)に分類する事ができる。

許可のための設定は一般的にアクセスコントロールリスト(ACL)で記述され、それはあるネームスペース内で認証されたあるユーザ(またはシステム)もし

くはロール(役割)ベースでグループ化されたユーザがある対象リソースに対する対象行為をある条件下(時間など)で許可/拒否されるという形式で記述されているものである。個々の情報システムにおいて、これらの設定方法は異なるが、その関係は同様であり、これらの情報をディレクトリのエントリとして定義するものとする。

また、エントリのためのスキーマ定義を検討するにあたり、以下のような点を考慮した。

(1). 同じ意味を持つ情報の冗長性の排除 例えば[秘密扱い]ポリシーの内容を変更した場合、この[秘密扱い]ポリシーを表現する情報のみを変更すれば[秘密扱い]ポリシーを採用している情報のポリシーが変更される。

(2) 責任範囲に従ったアクセス制御の指定: ドキュメント管理者、情報システム管理者、セキュリティ管理者などが異なる際に、管理範囲に応じて変更できるようにアクセス制御がなされる必要がある。

また、ディレクトリの主な特性から以下の点も考慮する。

(3). 変更頻度に応じたエントリ定義:
一般的にディレクトリは高速な検索が可能であるが、更新処理に時間がかかる。そのため、更新頻度が異なる情報を同じエントリで定義する事は全体的な性能低下をもたらす。(例えばポリシーの変更と人事異動の頻度は異なるため、ポリシーを示すエントリに人事異動毎に変更を必要とするような情報を含むべきではない。)

(4). 関連付けの定義方式の検討:
ディレクトリはその情報モデルからエントリの属性間の関係を示す事が難しい。そのため関係を示すための情報の持ち方を検討する必要がある。

このような検討課題を元にポリシー定義を行なった。 (図 2)

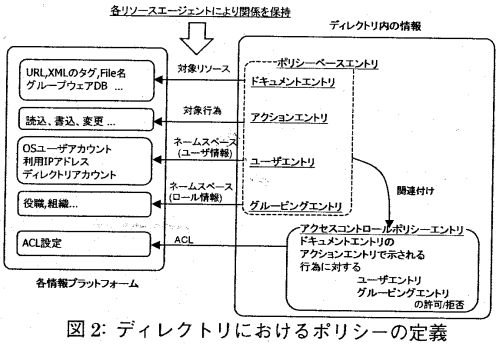

図 2: ディレクトリにおけるポリシーの定義

(図 3)は検討の結果、(表 1)で示されるようなポリシーを実際にエントリとして定義した例である。

これでわかるように、あるエントリが、その属性値として他のエントリを指定するという形式でポリシーの定義を行なっている。

このように定義する事により

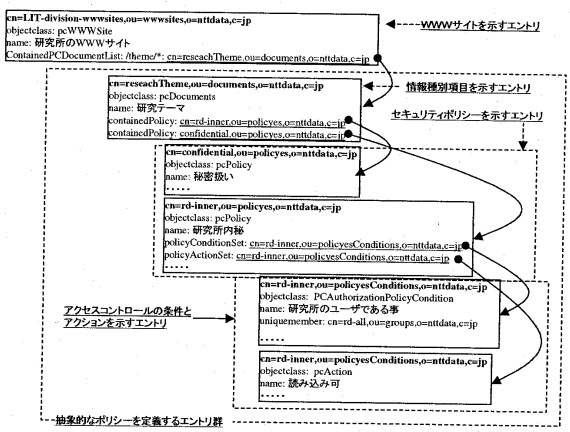

図 3: セキュリティポリシーエントリの例と
関連付けられる WWW サイトエントリの例

(1). リソースの種類によらないポリシー定義が可能になり、将来的に様々なリソース(XML 文書など)を追加可能となる。

(2).ユーザ情報を一元的にディレクトリに統一する事が可能となる。

(3).アクセス制御ポリシーを管理する管理者自身は個々の情報システムの設定を考慮する必要が無く簡単に設定が可能である。

等の利点を得る事が出来る。

3.3. リソースエージェントによる個別設定の変更

リソースエージェントはディレクトリサーバ上のポリシー情報を解釈し、個々の情報システムがそれに従い動作するように設定を変更するものである。今回、WWW サーバとして NETSCAPE ENTERPRISE SERVER、グループウェアサーバとして LOTUS 社の domino を用い、実装を行なった。

4. POLICYCOMPUTING™ の導入効果

アクセス制御ポリシー遵守のために情報作成者はポリシーの解釈、設計/設定、監査/保守を行なう必要がある。POLICYCOMPUTING™ の導入により、情報の情報種別項目を選択するのみでその遵守が可能であるため、管理業務が削減される。 その結果、情報作成者の管理業務の削減と同時に、その煩雑さのためアクセス制御ポリシーから逸脱するような設定がなされているような状況を回避する意味でセキュリティの向上も期待できる。

5. おわりに

アクセス制御ポリシー管理のための POLICY COMPUTING™ システムを検討し、構築した。 その結果情報作成者のポリシー遵守に必要な管理業務を減少させる事を可能とした。

[参考文献]

[1] 田中、菅野、他:情報ネットワークシステムのポリシー制御 POLICYCOMPUTING™ に関する一検討,情報研報 Vol99 , No18

[2] 菅野、坂田、他: POLICYCOMPUTING™ のセキュリティポリシーへの適用; 情処研報 Vol99、No.56