2Y-9

インシデント管理に必要なポリシー違反のログを履歴属性で管理することによるログ検索の高速化

伴　拓也†　　白石　善明†　　毛利　公美‡　　福田　洋治††　　野口　亮司†††

名古屋工業大学†　　岐阜大学‡　　愛知教育大学††　　（株）豊通シスコム†††

1.　はじめに

組織内情報システムでは，アクセス制御ポリシーとユーザ属性を基にユーザ毎にサービスへのアクセス制御を行う．ポリシー違反により，アクセスが拒否された場合，ポリシー違反のログが生成される．ポリシー違反はユーザの操作ミスで発生する場合もあるが，悪意のあるアクセスにより発生する場合もある．このような悪意のあるアクセスをセキュリティインシデント[1](以下インシデント)という．インシデント管理では，ポリシー違反のログの中から悪意のあるアクセスを探し，インシデントログを生成する．そして，インシデントログはユーザ属性として，ユーザのサービスに対するアクセス可否を決定するのに利用される．

インシデントによる被害拡大を抑制するためには，ポリシー違反のログの中から素早くインシデントを見つけ出さなければならない．それには，高速なログの読み出しが必要となる．特にプライベートクラウドの環境においては，アクセス制御とインシデント管理がより複雑になり，その上で速度が要求されることから，ログの読み出しの高速化が望まれる．

そこで本稿では，迅速なインシデント対応のために，高速にログを読み出すための手法を提案する．そして，提案手法が既存の手法と比較して優れていることを示す．

2.　アクセス制御とインシデント管理

2.1 アクセス制御とインシデント管理

アクセス制御システムの流れを図 1 に示す．

ユーザがサービスへアクセスを試みた場合，PEP(ポリシー強制点)が PDP(ポリシー決定点)にアクセス主体であるユーザの情報を送り，アクセス可否の判断を要求する．PDP ではユーザに与えられた権限と PIP(ポリシー情報点)から得られるユーザの情報を基にアクセス可否を判断する．PDP は PEP に判断結果を渡し，PEP はその結果に基づきアクセス制御を行う．

ここでのインシデントとは，コンピュータまたはネットワークのセキュリティを脅かす，またはその可能性のある，あらゆる敵対的なイベントを指す．インシデント管理は，インシデントに事前に対応する，または解決するための活動である．

2.2 インシデント管理とアクセス制御ポリシー違反のログ管理

インシデント管理を行うシステムの流れを図 2 に示す．ポリシー違反により PDP でアクセスが拒否された場合，PDP はポリシー違反のログを生成する．インシデント管理システムでは，ポリシー違反のログをすべて調べ，インシデントを検出し，インシデントログを残す．生成されたインシデントログは PDP でアクセス可否を決定するための情報となる．

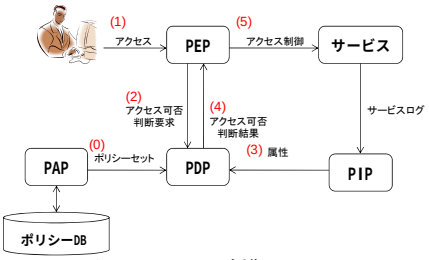

図 1　アクセス制御システム

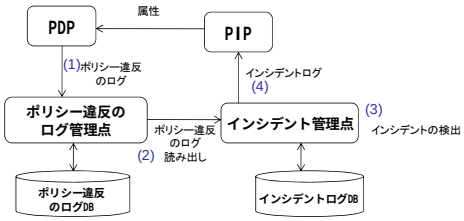

図 2　インシデント管理システム

2.3 ログ管理の方法

一般的なログ管理の方法として，ファイルシステムによる管理と，データベースによる管理がある．

ファイルシステムでログを管理する場合，一つのログデータを一つのファイルで管理することになる．ログデータを読み出す場合，ファイルオープンの操作を読み出すログの数だけ行うことになるため，読み出し効率が悪くなり，速度が低下する．

リレーショナルデータベース(RDB)では，内部的に複数のデータを一つのファイルに保存する．よって，一つのファイルに複数のログデータを保存することになり，ファイルシステムでのログ管理と比較して効率が良い．

しかしながら，RDB でログを管理する場合，ユーザ情報テーブルとログデータテーブルを用意し，ログデータテーブルにログデータを追加することでログを生成する．ログを読み出す際には，ユーザ情報テーブルとログデータテーブルを結合しデータを取り出す．そのため，RDB でログを管理する場合，システムを運用していくうちにログデータが単調増加することで，検索時の結合コストが増加していく．

2.4 インシデント管理における課題

インシデント管理システムでは，ポリシー違反のログから悪意のあるアクセスによるインシデントを高速に検出し，被害拡大を抑制しなければならない．しかし，特にプライベートクラウドの環境においては，サービスの種類は増え，さらにサービスが仮想化されるため，アクセス制御やインシデント管理はより複雑になり，インシデント管理システムの処理速度が低下することが予想される．不正アクセスによる被害拡大抑制のため，インシデント管理における処理速度低下への対応が望まれる．このような，インシデント管理システムの処理速度低下は，ポリシー違反のログの読み出しを高速化することで抑えることができると考えられる．したがって，ポリシー違反のログの管理方法を工夫し，ログの読み出しを高速化することが課題となる．

Speedup of Log Search by Managing Policy Violation Log Required for Incident Management as History Attribute

† Takuya Ban and Yoshiaki Shiraishi・Nagoya Institute of Technology

‡ Masami Mohri・Gifu University

†† Youji Fukuta・Aichi University of Education

††† Ryoji Noguchi・Toyotsu Syscom Corp.

3. オブジェクト指向データベースを利用したログ管理

3.1 RBAC とポリシー検索

組織内の情報システムでは，アクセス制御ポリシーによってユーザ毎のアクセス制御を行う．ユーザ毎にアクセス権を与えるアクセス制御方法として RBAC がよく利用されている．RBAC ではアクセス対象のアクセス権限をロールに割り当て，そのロールを適切なユーザに割り当てる．

RBAC を実現する上で，アクセス制御ポリシーを管理するためのデータベースが必要となる．データベースの一つに，オブジェクト指向データベース(OODB)がある．OODB は保存されているデータがオブジェクトの構造を持つ．[2]では，OODB を利用して，ユーザとロールのデータをオブジェクトとして扱う．そして，権限データと権限データ操作用のメソッドを同一クラス内で扱うことにより，柔軟な権限の変更を可能にしている．

この他にも OODB でアクセス制御ポリシーを管理する場合，ロールオブジェクト内でアクセス権を扱うことで，ロールとアクセス権は結合された状態で保存されるという特徴がある．すなわち，OODB では，オブジェクト毎にまとまめられたデータを検索する際に結合処理が不要となる．したがって，高速なポリシーの読み出しが可能になると考えられる．

3.2 提案手法：OODB によるログ管理

2.2 で述べたポリシー違反のログはユーザ毎に管理する必要のあるデータである．OODB を導入することで，ポリシー違反のログをユーザオブジェクト毎に分割して管理することで，ポリシー違反のログの高速な読み出しが可能になると考えられる．

そこで，以下の OODB によるログの管理手法を提案する．

まず，OODB でログを管理するためのクラス定義を図 3 に示す．ログクラスには，ログ生成日時を表す日時情報と，ログ内容を表すログデータの属性を持たせる．ユーザクラスには，ユーザを一意に特定するための ID などのユーザ情報とログオブジェクトを複数保持するためのログ履歴リストを持たせる．

そして，各クラスには次のようなメソッドを定義する．ログクラスには，日時情報とログデータに対する読み出しメソッドを持たせる．日時情報とログデータは変更不可能なデータであることから，変更メソッドは持たせないこととする．ログクラスの属性に対応するデータは，コンストラクタにより一度だけ書き込み可能とする．一方のユーザクラスには，ユーザ情報とログ履歴に対する変更メソッドと読み出しメソッドをそれぞれ持たせる．

ログの書き込みは次のようになる．OODB には予め，アクセス可能なユーザのユーザオブジェクトを格納する．あるユーザがポリシー違反を犯した場合，PDP ではアクセス制御ポリシー違反のログを生成する．ポリシー管理点は，ログ情報をもとにログオブジェクトを生成し，当該ユーザのユーザオブジェクトに追加する．

ログの読み出しは次のようになる．インシデント管理点でインシデントの検出のために，全ユーザオブジェクトのポリシー違反のログを調べる．このとき，全ユーザオブジェクトを調べ終わるまで，メモリ容量が許す限り多くのユーザオブジェクトをメモリ上に読み込む操作を繰り返す．そして，各ユーザオブジェクトからログデータを読み出し，インシデントの検出を行う．

OODB と RDB のデータの構造を図 4 に示す．OODB ではデータが各ユーザに分割され保存される．それに対して，RDB では正規化がなされ，ユーザとログの情報で分けられる．したがって， RDB ではデータの検索の際に結合処理が必要となり，ユーザ毎のデータを検索する場合は OODB の方が高速になると期待される．

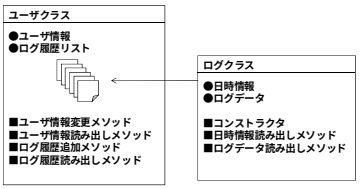

図 3　クラス定義

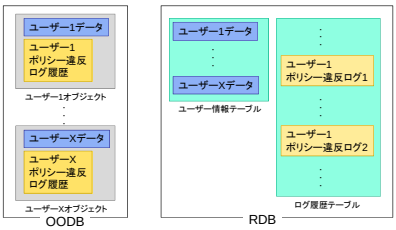

図 4　OODB と RDB のデータの構造

4. OODB によるログ管理の評価

OODB を利用したログ管理が汎用的なデータベースである RDB で管理するよりも検索が高速であることを示すために評価を行う．

4.1 評価方法

ユーザ数を 250 人，500 人，…，2,000 人と 250 人ずつ増加し評価を行うことで，人数が増加しても，検索速度が高速であるかどうかを確かめる．ユーザ一人当たりに 30 個のログを追加し，さらに，不正アクセスを行った者として 10 名をランダムに選び，その 10 名のみにログを 100 個追加することでログ数に偏りを持たせる．そして，すべてのユーザのログを検索するのにかかる時間を比較する．

4.2 結果

実験結果を図 5 に示す．RDB と比較して OODB では短時間ですべてのログを読み出していることがわかる．OODB ではデータベース内部で既にユーザーデータとログデータが結びついており，それらの結合処理が必要な RDB よりも検索が高速になることが確認された．

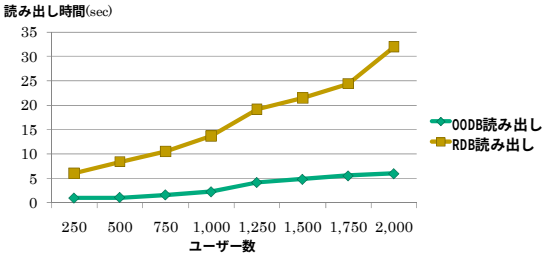

図 5　RDB と OODB でログ検索コストを比較した結果

5. おわりに

特にプライベートクラウドの環境でインシデント管理を行う場合，従来よりも高速なポリシー違反のログの読み出しが必要となる．その課題に対して， OODB を導入して各ユーザオブジェクトにログデータの履歴属性を持たせるという管理手法を提案した．提案手法が， RDB によるログ管理よりもログの読み出しが高速であることを示した．

参考文献

[1] Nevil Brownlee, Erik Guttman, “Expectations for Computer Security Incident Response”

[2] Raymond K. Wong, “RBAC Support in Object-Oriented Role Databases”, Department of Computing School of MPCE, Macquarie University Sydney, NSW 2109, Australia, 1997