ソフトウェア工学 123－7
（1999．5．14）

オブジェクト指向セキュリティポリシー開発

鵜飼孝典[1]

ugai@flab.fujitsu.co.jp
株式会社富士通研究所

概要 ： セキュリティポリシーを分散オブジェクトシステムとする "ポリシーオブジェクトネットワーク" というモデルを提案し，既存のオブジェクト指向分析，設計法を用いてセキュリティーポリシーの分析設計を行う．"ポリシーオブジェクトネットワーク" では通常のサービスを提供するサービスオブジェクトのセキュリティを管理するオブジェクトをセキュリティポリシーオブジェクトとし，セキュリティポリシーオブジェクト同士あるいは,セキュリティポリシーオブジェクトとサービスオブジェクトがコミュニケーションを行なってシステム全体のセキュリティポリシーを構成する．最後に文書管理システムについてセキュリティ要求の分析,設計を行なった例を示す．

Object Oriented Security Policy Analysis and Design

Takanori Ugai
ugai@flab.fujitsu.co.jp
Fujitsu Laboratories Limited

Abstract: We propose policy object network that is a model for security policy analysis and design. In the model a security policy which controls system functions is a distributed object network system collaborating with functional objects which provide system's functions. Using this model we can analyze and design a system with OOA/OOD. In this paper we apply an object-oriented method to analysis and design of a document management system and its security policy.

[1] 本研究は ANSA program (http://www.ansa.co.uk/) の一部として行われました

1. はじめに

これまでの firewall 技術, 暗号技術によって情報を外からの攻撃から守るという要求から，情報公開の手続きやデータのバックアップのスケジューリングなどの複雑なセキュリティポリシー管理技術が要求されてきている[3]. 情報管理のセキュリティポリシーに沿って実際にどのようにシステムにセキュリティポリシーを設定するかという技術，すなわちセキュリティポリシーの分析，設計のためのモデル，方法論が必要になってきている. とくに Internet, Intranet の普及によって分散システムのセキュリティポリシーの技術が重要課題となっている.

これまで利用されてきたセキュリティポリシーのモデルは，一つの大域的なポリシーによって全体を管理する中央集権的なものであり，Internet のようなお互いに独立のポリシーによって運営されるサイトの接続によって一つの大きなシステムが構成される場合には適用が困難である. またユーザのセキュリティに関する要求は複雑化してきており，アクセスコントロールリストやアクセスメトリックスに基づいたこれまでのセキュリティポリシーの表現モデルは不十分である. 例えば，バックアップデータを作ることはセキュリティに関する要求の一つであるが，これまでの設計ではセキュリティの一部としてではなくシステムの機能として設計しなければならない.

本稿ではセキュリティポリシーをオブジェクトシステムとする "ポリシーオブジェクトネットワーク" というモデルを提案し，既存のオブジェクト指向分析，設計法を用いてセキュリティーポリシーの分析設計を行う. "ポリシーオブジェクトネットワーク" のモデルでは，一つのオブジェクトをサービスを提供するサービスオブジェクトとそのサービスオブジェクトを管理するセキュリティポリシーオブジェクトからなる仮想オブジェクトとしてモデル化する. さらにポリシーオブジェクトネットワークの要素となるセキュリティオブジェクト同士あるいは,セキュリティポリシーオブジェクトとサービスオブジェクトがコミュニケーションを行なってシステム全体のセキュリティポリシーを構成する. セキュリティーポリシーをオブジェクトとして設計することで動的に変化するポリシーやバックアップなどの機能的なセキュリティポリシーを記述することが可能になる.

本論の第2章ではポリシーオブジェクトネットワークモデルを説明し，第 3 章ではそのモデルに基づいて，試験問題作成システムのセキュリティポリシーの設計を，オブジェクト指向を用いて行なった例を示す. さらに第 4 章では，セキュリティポリシーの設計とソフトウェアの設計に関する考察を述べる.

2. ポリシーオブジェクトネットワーク

本章では，ポリシーオブジェクトネットワークのモデルについて説明する.

2.1. 中央集権ポリシーと分散ポリシー

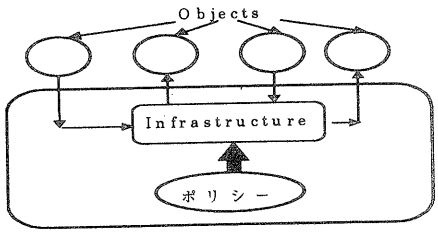

図 1:中央集権ポリシーモデル

図 1は古典的な中央集権ポリシーモデルを示す. このモデルではセキュリティーポリシーが設定された OS やシステムなどのインフラストラクチャによってそれぞれのオブジェクトの振る舞いが管理，監視される.

オブジェクトが置かれるサイトごとに異なるポリシーで運用される分散システムにおいてはこのモデルで設計される大域的な

ポリシーはサイトごとの局所的なポリシーと矛盾し機能しないことがある.

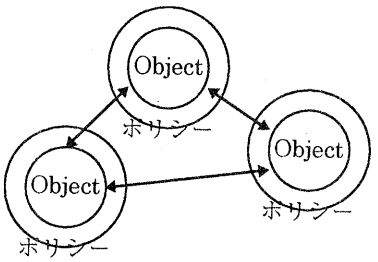

図 2: 分散ポリシーモデル

図 2は, それぞれのオブジェクトがポリシーをもって自分の振る舞いを管理するモデルを示す. このモデルでは個々のオブジェクトのコミュニケーションが必ずそのオブジェクトのポリシーに従う. このモデルではオブジェクト間にまたがる大域的なセキュリティポリシーもここのオブジェクトのセキュリティポリシーに分散される.

本論で提案するポリシーオブジェクトネットワークはこの分散ポリシーモデルに基づく.

2.2. 自己防衛オブジェクト

2.1節で述べた分散ポリシーを構成するそれぞれのオブジェクトのセキュリティは次の自己防衛モデル[5]に基づく. このモデルでは, オブジェクトは [7] で定義されるようにインターフェイスを通してコミュニケーションを行なうことで他のオブジェクトにサービスを提供する.

自己防衛モデルは実際の社会における個々のセキュリティポリシーを反映したモデルで, 次の2つの原理を持つ.

- カプセル化 : オブジェクトはそのオブジェクトが提供するインターフェイスを通してのみコミュニケーションを行なう. これを保証することがそのオブジェクトが実装されるインフラストラクチャに対して要求される.
- 自己責任 : オブジェクトはそのオブジェクトへのアクセスに対して自らが責任を持つ. そのオブジェクトへのアクセス元の認証,承認, 監視,その他すべてのセキュリティポリシーの設計, 実装はそのオブジェクト毎に行なう. セキュリティ機能の一部をそのオブジェクトが信頼する別のオブジェクトに委任することは可能であるが, それもそのオブジェクト自身の責任で行われる.

2.3. サービスとポリシーの分離

オブジェクトはその振る舞いに対して自分で責任を持っていることから, 他のオブジェクトとどのようにコミュニケーションするかというポリシーも, 通常はオブジェクト内にその振る舞いとして設計される. しかし実際のシステム設計,実装運用においてはセキュリティの基準は, サービスに依存せず独立に設定され, サービスの設計とは別の部署によってセキュリティポリシーの設計が行われることが多いので, サービスとセキュリティポリシーが独立に設計されるモデルが必要である..

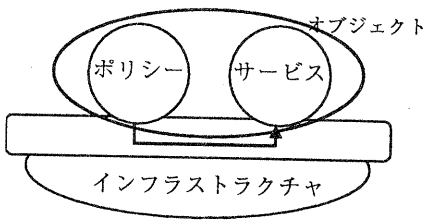

図 3: サービスとポリシーの分離

ひとつのオブジェクトのサービスとポリシーを図 3のように分離して,2つの側面が協調して動作しているオブジェクトとしてモデル化すると, オブジェクトの振る舞いについてサービス, セキュリティポリシーのそれぞれの部分にフォーカスを当てることができるようになる.インフラストラクチ

ャはセキュリティポリシーとサービスを結合する機能を提供し，サービスにアクセスする要求がセキュリティポリシーにしたがっているかどうかをチェックする．

2.4. サービスオブジェクトとポリシーオブジェクト

サービスとセキュリティポリシーはそれぞれあるオブジェクトの特定の側面にフォーカスを当てるものであるが，それらもまたそれぞれオブジェクトとしてモデル化される．

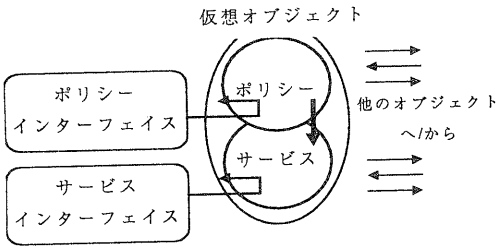

図4:サービスオブジェクトとポリシーオブジェクト

オブジェクトのサービスとセキュリティポリシーをそれぞれオブジェクトとして分離したものが図4のモデルであり，ひとつのオブジェクトは，ポリシーオブジェクトとサービスオブジェクトから構成される仮想的な複合オブジェクトとしてモデル化される．このモデルではポリシーオブジェクト，サービスオブジェクトに関してそれぞれにインターフェイスが定義される．サービスオブジェクトのインターフェイスは仮想オブジェクトのサービスを利用するものであり，ポリシーオブジェクトのインターフェイスはその仮想オブジェクトのポリシーを外部から変更することを可能にする.このモデルによってポリシーは認証，承認などの外部サービスを利用することも可能になる．さらにポリシーオブジェクトもまた再帰的にサービスオブジェクトとポリシーオブジェクトとしてモデル化され，ポリシーオブジェクトがまた別のポリシーオブジェクトとコミュニケーションを行なうことが可能である．

サービスをひとつのオブジェクトとすることによって，サービスの設計とセキュリティポリシーの設計を独立に行うことが容易になり，特にサービスオブジェクトの設計はセキュリティポリシーの存在を意識することなく進められる．

2.5. ポリシーオブジェクトネットワーク

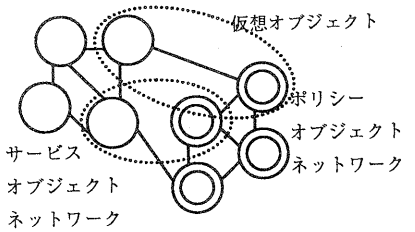

図 5 ：サービスオブジェクトネットワークとポリシーオブジェクトネットワーク

図 5のように提供されるサービスに関連するポリシーオブジェクトも，他のサービスオブジェクトによって提供されるサービスを呼び出すことも可能である．またあるポリシーオブジェクトが別のポリシーオブジェクトとコミュニケーションを行ない，ポリシーオブジェクトもネットワークを形成する．図 5は実際の状態を簡単化し，オブジェクトの配置を考慮していないが，分散オブジェクトシステムでは実際には図 6のようにポリシーオブジェクトはローカル，リモートの何処からでもサービスオブジェクトを管理しポリシーオブジェクトとサービスオブジェクトの関係は複雑になる．

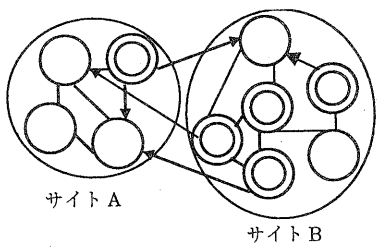

図 6：複雑なポリシーオブジェクトネットワーク

2.6. オブジェクト開発技法を用いたポリシーの設計の方法

前節までに述べたポリシーオブジェクトネットワークのモデルに基づいて，セキュリティポリシーをオブジェクト指向開発技法によって開発するとき，

- 一つのサービスオブジェクトに対し一つのポリシーを付随させる．一つのオブジェクトをサービスとセキュリティポリシーの 2 つの側面から同時に設計することもセキュリティポリシーをオブジェクトの機能とは独立に設計することも可能である．
- 一つのセキュリティポリシーは複数のオブジェクトからなるシステムとして設計する．

3. 例題 ―試験作成システム―

本章ではセキュリティポリシーの設計の例題として[1] で示される文書管理システムの一つである試験作成システムのセキュリティポリシーを設計する．

3.1. 仕様概要

この節では，システム全体の仕様とセキュリティポリシーを概説する

試験を作る作業グループはボードメンバーと呼ばれ， Chair, と Ex1 と呼ばれる Examiner, それと若干名の external Examiner から構成される．それぞれは次のような役割を果たす．

- Ex1 が試験の最初の版を作成し，Chair と他の Examiner がそれに対してコメントをつけ，Ex1 がコメントをもとに試験を更新する．
- ボードメンバーは作成されている試験に対してつけられたコメントを読むことができる．
- ボードメンバーは試験の作成を終了できる．

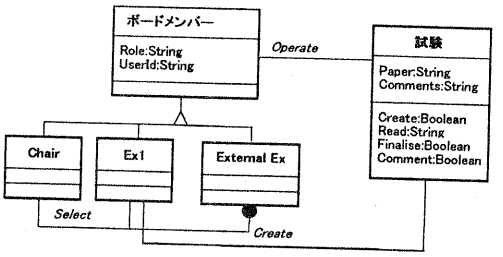

図 7 試験作成システムのオブジェクト図

以上のようにして作成される試験は次のポリシーを満足するようにして作成されなければならない．

- ボードメンバー以外は試験の状態を見ることができない．
- 試験は，適切な役割の人かその人に委任された人によってのみ作成され，更新される．
- 委任は一段階のみ許される．
- 試験の作成は複数人によって終了されなければならない．
- 役割を委任される人は Chair によってあらかじめ選ばれたグループから選ばれなければならない．
- 試験作成に対するすべての作業は記録されなければならない．
- 作成される試験は一定期間ごとにバックアップを取らなければならない．

3.2. 試験作成システムの実装環境

試験作成システムは， 試験問題を管理する試験問題サーバに，ボードメンバーのクライアントシステムがアクセスするサーバ／クライアントの分散システムで実装され，サーバ/クライアント間は， Internet のような秘密に関して信頼できないネットワークであり，公開暗号を用いることとする．

3.3. 試験問題サーバのセキュリティポリシー設計

本節では，設計された試験問題サーバのセキュリティポリシーを示す．

1. 試験は Ex1 によって作成されなければならない．Ex1 以外の人によって作成されようとするときにはそれを拒否しなければならない．
   - 試験作成のメッセージは Ex1 のサインがついていなければならない
   - サインは試験問題サーバ自身か試験問題サーバが信頼する認証サーバによって認証されなければならない．
2. Ex1 から送られる試験はボードメンバー以外からは秘密でなければならない．
   - 試験のデータは，Ex1 の鍵かボードメンバーの鍵によって暗号化されなければならない．
3. コメント，読み出し，終了の要求はボードメンバーからのものでなければならない．
   - クライアントから送られるメッセージは送信者のサインが付いていなければならない．
   - メッセージについているサインはサーバ自身か,サーバによって信頼される認証サーバによって認証されなければならない．
4. コメントと試験の更新のデータはボードメンバー以外には秘密でなければならない．
   - 試験の更新のデータは Ex1 かボードメンバーの鍵によって暗号化されなければならない
   - コメントはコメントをつけた人の鍵かボードメンバーの鍵によって暗号化されなければならない．
5. Chair は試験問題作成が始まる前に external examiner を決めておかなければならない．
   - external examiner からのメッセージは，そのメッセージの作成者が試験作成開始前に試験問題サーバ自身によって認識されているか，試験問題サーバが信頼する認証サーバによって，それが保証されなければならない．
6. 試験問題作成サーバは，1 段階委任されたメッセージを受け付ける．
7. 試験に対するすべての操作を記録し，一定期間保存する．
8. 試験問題に関するすべてのデータは一定期間ごとにバックアップを保存する．

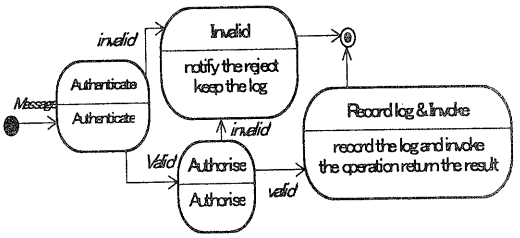

図 8 セキュリティーポリシーの状態遷移図

図 8は試験問題サーバのセキュリティーポリシーの状態遷移図の一部を示すものであり，データがその権利を持たないものによって変更されたり破壊されない性質を保つためのポリシーである．

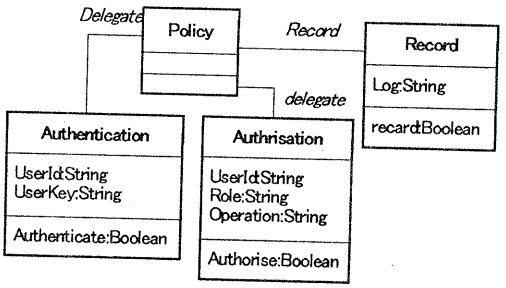

図 9 セキュリティポリシーのオブジェクト図

図 9は試験問題サーバのセキュリティポリシーのオブジェクト図の一部である．ひとつのポリシーが認証，承認，記録の３つのオブジェクトから構成される．

3.4. オブジェクトの分割，詳細化

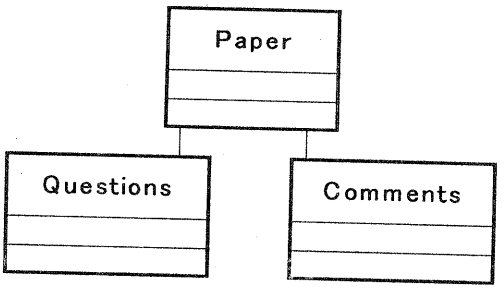

図 10：試験問題オブジェクトの詳細化

試験問題オブジェクトが問題オブジェクトとコメントオブジェクトから構成される複合オブジェクトとして詳細化され，問題オブジェクトとコメントオブジェクトは試験問題オブジェクトのサブクラスとして設計されるとする．また試験問題オブジェクト，問題オブジェクト，コメントオブジェクトがそれぞれ異なる分散オブジェクトとして設計される場合，問題オブジェクトとコメントオブジェクトはそれぞれ試験問題オブジェクトのセキュリティポリシーによって管理され，さらにそれぞれのセキュリティポリシーを持つことができる．

例えば，問題オブジェクト独自のセキュリティポリシーは，

- 問題オブジェクトへのアクセスは試験問題オブジェクトを通してのみ行われ，ユーザから直接アクセスされない．
- 試験問題オブジェクトと問題オブジェクトの間の通信はその内容を他人に知られてはならない．
- 試験問題オブジェクトを通して行われる問題オブジェクトへのアクセスに関する認証と承認は試験問題オブジェクトに委任される．

問題オブジェクトは試験問題オブジェクトのセキュリティポリシーを継承するため，問題オブジェクトは自分で呼び出し元を認証し，承認しなければならないが，この場合，試験問題オブジェクトに認証,承認を委任し，自らは行わない．

4. ソフトウェア開発とセキュリティポリシー開発に関する考察

現在プログラマが

- プログラミング言語で
- エディタ，コンパイラ，デバッガなどのツールを使って
- OOA/OODやJSDなどの方法論を用いて
- ソフトウェアアーキテクチャの下に

ソフトウェアを開発しているが，セキュリティマネージャがセキュリティポリシーを管理するために利用できる技術は少ない．今後は，セキュリティマネージャが

- セキュリティポリシー記述言語を用いて
- セキュリティポリシーエディタやセキュリティポリシーデバッガを用いて
- セキュリティ開発方法論やサポートツールを使って

- セキュリティアーキテクチャに基づいて

セキュリティポリシーを管理することが考えられ，これらの技術の開発が必要とされている．

5. 結論

本論では分散システムのセキュリティポリシーを分散オブジェクトシステムとする"ポリシーオブジェクトネットワーク"というモデルを提案し，既存のオブジェクト指向分析，設計法を用いてセキュリティーポリシーの分析設計を行うことを提案した．

"ポリシーオブジェクトネットワーク"ではセキュリティポリシーを，サービスを管理するオブジェクトとして捉え,セキュリティポリシーオブジェクト同士あるいは,セキュリティポリシーオブジェクトとサービスオブジェクトがコミュニケーションを行なってシステム全体のセキュリティポリシーを構成する．ポリシーオブジェクトネットワークは，セキュリティメカニズムを備えた古典的な大型システムの OS やハードウェアを仮定したものではなく，それぞれのオブジェクトを守る最小限の機能のみを前提としている．このため本論で示した設計を Internet などで行われる商取引などに広く利用することができる．

例題として文書管理システムについてセキュリティ要求の分析,設計を行なった．設計されたセキュリティポリシーに関しては ISO などによって定められたセキュリティ基準などによってそのポリシーが意図したものであるか,ある基準を満たしたものであるかを検証する必要がある．今後，オブジェクト指向開発で形式的に記述された部分に関しては，そのポリシーが満たすべき性質を機械的に示すことができれば，セキュリティポリシーの設計をより容易にすることになる．

6. 参考文献

[1] Marie Rose Low "Expressing a Policy" (to be published) University of Hertfordshire.

[2] Rumbaugh J. Blaha M. Premerlani W. Eddy F. Lorensen W., "Object-Oriented Modeling And Design", Prentice-Hall International Editions.

[3] Emil C. Lupu, Damian A. Marriott, Morris S. Sloman and Niholas Yialelis, "A POLICY BASED ROLE FRAMEWORK FOR ACCESS CONTROL", Role Based Access Control Workshop, ACM/NIST, Dec. 1995

[4] R.T.O.Rees, J.A.Bull, "A Framework for Federating Secure Systems", Architecture Projects Management Ltd., Cambridge(UK), May 1993

[5] J.A.Bull "ANSA Security Services", Architecture Projects Management Ltd., Cambridge(UK), May 1993

[6] T. Ugai "Security Policy Objects and RM-ODP", November '97,OMA/ODP workshop in Cambridge, England

[7] International Standards Organisation "Open Distributed Processing - Reference Model. Sep. 1995 http://www.iso.ch:8000/RM-ODP