

統治型アーキテクチャの提案

ーシステム全体の整合性維持を自動化する仕組みー

稲垣嘉信[†] 坂本久[†] 島津秀雄[†]

[†]NECシステムテクノロジー株式会社 システムテクノロジーラボラトリ

1 はじめに

今日、多数の各種端末や装置から構成された、サーバクライアント型の IT システムが普及している。これら端末や装置は、利用者の利用状況の変化に応じて頻繁に、サーバ側に接続したり、切断したりされる。そうすると、システム全体で統一したルールに基づいて動作させ、統治する場合に、その末端の端末や装置までの、ルール伝達が困難になる。一部のアプリケーションでは、内部でルールを最新版に維持する仕組みを持つものもあるが、独自にこの仕組みを持つことは困難かつ非効率である。本稿では、これを解決する「統治型アーキテクチャ」という新概念を提案する。

2 IT システムの変遷

サーバコンピュータに接続される全クライアントコンピュータを統治するという観点から見ると、IT システムは次のように変遷してきたということが分かる (図 1)。

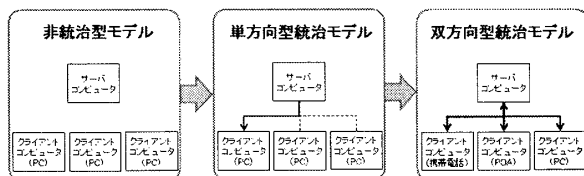


図 1 IT システムの変遷

1) 非統治型モデル

統治をする仕組みを持たないモデル。今日の一般的なシステムはこの形態をしている。

2) 単方向型統治モデル

サーバコンピュータからクライアントコンピュータに対して、一方的に指示が送信され、クライアントコンピュータはそれに従う。

3) 双方向型統治モデル

サーバコンピュータから各種端末によるクライアントコンピュータに対して、統治の指示(ポリシー)が送信され、クライアントコンピュータはそれに従う[1]。その後、クライアントコンピュータは、ポリシーを実行した結果で

ある状態情報をサーバに返信する。サーバはそれらを集約し、必要に応じて新たなポリシーを送信することを続けていく。

従来の先進的アプリケーションでは、独自に双方向型統治モデルの仕組みを実装していた。しかし独自に実装することは、困難かつ非効率的である。また、各アプリケーションで双方向型統治モデルの仕組みが異なるため、アプリケーションを超えた横断的な統治ができなかった。そこで、双方向型統治モデルの仕組みを各アプリケーションで持つのではなく、アーキテクチャの要素として組み込み、各アプリケーションは、その機能呼び出すことで、統一規格の双方向型統治モデルを比較的容易に実現する。このアーキテクチャを「統治型アーキテクチャ」と呼ぶ。

3 統治型アーキテクチャ

ここでは、統治型アーキテクチャの構成を図 2 を用いて説明する。

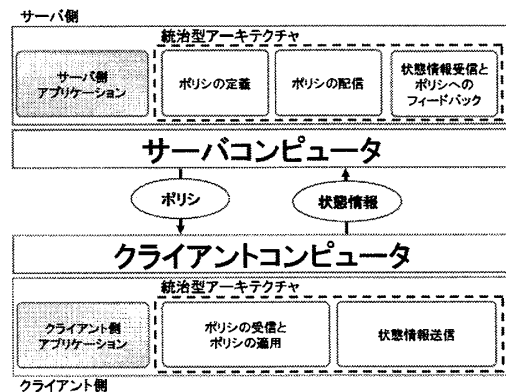


図 2 統治型アーキテクチャの構成

サーバコンピュータとクライアントコンピュータには、統治を実現するアプリケーションが導入されており、アプリケーションは統治型アーキテクチャを用いて、双方向型統治モデルを実現している。統治型アーキテクチャは、アプリケーションに双方向型統治モデルの機能を提供するため、次の 5 つの機能を備える。

1) ポリシーの定義

クライアントコンピュータへ配信するためのポリシーを定義する。ポリシー内容はアプリケーションにより異なるが、システム全体を統治

Proposal of the governance architecture
Yoshinobu INAGAKI[†], Hisashi SAKAMOTO[†],
Hideo SHIMAZU[†]
[†]NEC System Technologies, Ltd.

するため、クライアントコンピュータが行うべき動作が記述される。

2) ポリシの配信

定義されたポリシをサーバコンピュータからクライアントコンピュータへ配信する。

3) 状態情報受信とポリシへのフィードバック
クライアントコンピュータからサーバコンピュータへ送信された状態情報を受信する。収集した状態情報を総合的に判断した上で、次に配信すべきポリシの内容を決定し、その内容をポリシへフィードバックする。

4) ポリシの受信とポリシの適用

サーバコンピュータからクライアントコンピュータへ配信されたポリシを受信し、ポリシに記述された指示を実行する。

5) 状態情報送信

クライアントコンピュータでポリシを適用した結果である状態情報を、サーバコンピュータへ送信する。

4 統治型アーキテクチャの適用例

ここでは、統治型アーキテクチャを用いて、ウイルス対策アプリケーションが、シグナチャファイル（ウイルス検出パターンを記述したデータ）を、ポリシとして配信する適用例を紹介する。

図 3 を用いて統治型アーキテクチャの適用例を説明する。サーバコンピュータ上では、ウイルス対策アプリケーションサーバプログラムが、統治型アーキテクチャを用いて動作している。また、クライアントコンピュータ上では、ウイルス対策アプリケーションクライアントプログラムが、統治型アーキテクチャを用いて動作している。ウイルス対策アプリケーションは、統治型アーキテクチャを用いて、次の①～⑤の動作を継続的に行うことで、双方向型統治モデルを実現する。

- ①ウイルス対策アプリケーションサーバプログラムは、クライアントコンピュータへ配信するポリシを「ポリシの定義」により定義する。
- ②ウイルス対策アプリケーションサーバプログラムは「ポリシの配信」を用いて、①で定義したポリシをクライアントコンピュータへ配信する。
- ③ウイルス対策アプリケーションクライアントプログラムは、②で配信されたポリシを、「ポリシの受信とポリシの適用」を用いて受信し、最新のポリシとしてクライアントコンピュータに適用する。
- ④ウイルス対策アプリケーションクライアントプログラムは、③でポリシを適用した結果、

現在適用中のポリシのバージョンを状態情報として、「状態情報送信」を用いてサーバコンピュータへ送信する。

- ⑤ウイルス対策アプリケーションサーバプログラムは、④で送信された状態情報を「状態情報受信とポリシへのフィードバック」を用いて受信する。状態情報を総合的に判断した上で、次に配信すべきポリシの内容を決定し、その内容をポリシへフィードバックする。

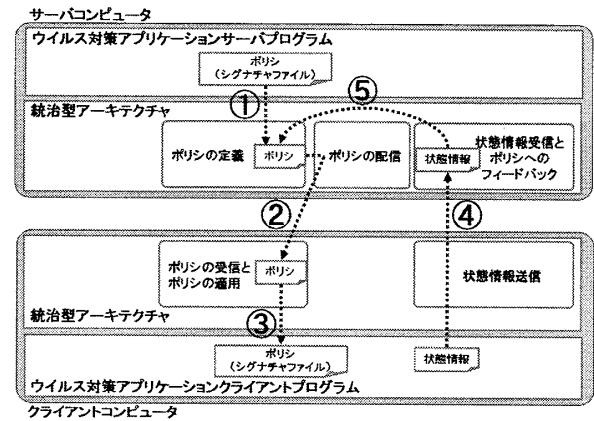


図 3 統治型アーキテクチャの適用例

このように、アプリケーションは、統治型アーキテクチャを用いることで、容易に双方向型統治モデルを実現することが可能になる。

5 むすび

本稿では、統治型アーキテクチャの概念を紹介した。従来の情報セキュリティシステムには、独自に双方向型統治モデルの仕組みを持つものもあった[2] [3]。今後、システム同士の緊密な連携が必要になるときに、個々のアプリケーションを超えた横断的なポリシ制御ができれば、セキュリティ強度の向上に貢献できる。また、今後は情報セキュリティシステム以外にも双方向型統治モデルが適用されていくと考えられる。このような場合に、統治型アーキテクチャを用いれば、様々なシステムに対して統一規格の双方向型統治モデルを比較的容易に適用でき、各アプリケーション間で状態情報を共有できるため、各アプリケーションを超えたポリシ制御も可能になると考えられる。

参考文献

- [1]小泉,平島,三宅：ポリシベースによる QoS 制御, オーム社 2001
- [2]足尾他：企業におけるコンテンツセキュリティ, 情報処理学会 第 70 回全国大会 2008
- [3]坂本他：コンテンツセキュリティにおける網羅性の実現, 情報処理学会 第 70 回全国大会 2008