分散オブジェト指向ネットワークセキュリティに関する一考察

6F－2

今田美幸
NTT光ネットワークシステム研究所

1　はじめに

近年、分散処理を主体としたネットワークの検討が進められている。その1つに、今後のネットワークに必要とされる経済化、柔軟性、高性能化、高機能化等の多様な要求に答えるための新しい分散オブジェクト指向ネットワークアーキテクチャ(DONA)がある[1]。

セキュリティを構築する際に重要なことは、通信路上での情報の改竄や破壊、盗聴や改竄が発生しないセキュリティメカニズムを提供することである。

近年は、ネットワークを利用して、分散化した商品情報やシンクタンク等で独自に調査した企業情報などを契約者にのみ公開するといったような場合のセキュリティの検討が、特に重要な課題となってきている。

分散処理環境において、クライアントが利用したいサービスを提供するターゲットサーバを検索したい場合、トレーダサーバ（以下トレーダと呼ぶ)[2]を使用する方法がある。名前サーバが、サービスを提供しているターゲット名から、通信に用いる物理的なアドレスを提供するのに対し、トレーダはコスト等のサービス特性からターゲット名を検索するメカニズムを提供するサーバである。

筆者は、セキュリティサーバに、トレーダの保持する機能（トレーディング機能）を持たせたセキュア・トレーダを提案した[3]。

以下にセキュア・トレーダの特徴を4点示す。

・集中管理機構を持つ分散型データベースを基本とした情報管理をもつ。

・トレーダで管理するターゲット情報をセキュリティサーバ内で管理することにより、情報管理の安全性が高まる。

・トライアントが、中継するサーバの数が少ない。これは、までの通信回数の削減、通信中の危険の軽減、トレーダの保持する情報の保護等の効果が得られることを意味する。

・木構造を利用して、複数のセキュア・トレーダ間で情報を安全に共有できる。

一方、実際のシステムでは、セキュリティをそれほど必要としないトレーダとセキュア・トレーダが共存することになる。

本稿では、DONAプラットフォーム分散処理環境での既存のトレーダとセキュア・トレーダと効率的に使用する方法について述べる。

2　現状の問題点

より高いセキュリティを確保するためには、トレーダの保持するすべてのターゲット情報をセキュア・トレーダ内部で保護する方式がよい。しかし、個々のシステムのセキュリティ要求条件を考慮すると、実現は困難である。

一方、セキュア・トレーダが存在することにより、トレーダの種類が増加することになる。これは、クライアントにとって、自分の検索したい情報を保持するトレーダが機能分散し、オペレーションをセキュア・トレーダとトレーダのいずれに発行すればいいのかわからなくなるため、ターゲット名検索のための処理がかえって複雑になる。

3　解決策

上記の問題を解決するために、トレーダオペレーションに使用しているセキュリティメカニズムに着目したトレーダへの通信切り分け方法を提案する。

これは、クライアントがターゲット情報を登録する際、セキュア・トレーダにはセキュリティ条件の厳しいものを、一般のトレーダには、ネット検索ツールを使用するときのようなセキュリティ条件が厳しくないものを登録するということが想定される点を利用する。

Security Services for Distributed Object-oriented Network Systems
Miyuki Imada
NTT Optical Network Systems Laboratories
9-11, Midori-Cho 3-Chome, Musashino-Shi, Tokyo 180, Japan.

具体的には、クライアントが高いセキュリティメカニズムを使用してトレーダオペレーションを発行した場合にのみ、セキュア・トレーダのトレーディング機能で検索し、それ以外は、トレーダへ送信する。

処理概要を図１に示す。いずれのトレーダに要求した情報があるかの切り分けは、クライアント毎に生成されるインタフェースエージェント機能[4]を用いて行う。インタフェースエージェント機能は、クライアントが要求したターゲットとのオペレーションに必要なセキュリティ処理やトレーディング機能への処理依頼をクライアントに代わって行う機能とする。クライアント毎に生成されたインタフェースエージェントは、トレーダとの通信が終了すると消滅するものとする。

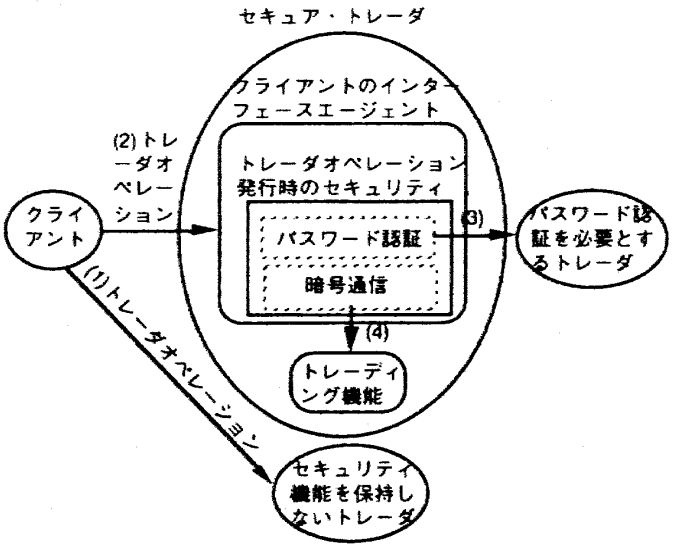

図１　提案方式の概要

以下に、トレーダへアクセスする際のセキュリティレベルが３レベルある場合の例を示す。

レベル１：セキュリティを全く必要としない場合

クライアントは、セキュア・トレーダを介することなく、トレーダにトレーダオペレーションを送信する（図１の(1)）。

レベル２：パスワード認証レベルのセキュリティが必要な場合

クライアントは、ID、パスワード、トレーダオペレーションをセキュア・トレーダのインタフェースエージェントに送信する。インタフェースエージェントは、トレーダへのオペレーションであることとパスワード認証を要求していることから、自トレーディング機能の検索は行わず、パスワードでクライアント本人であることを確認したら、トレーダにオペレーションを発行する（図１の(2)、(3)）。

レベル３：暗号レベルのセキュリティが必要な場合

セキュア・トレーダが、クライアントからの暗号処理したトレーダオペレーションを受け取ると、インタフェースエージェントはセキュア・トレーダ内部の暗号処理機能で復号化し、それをトレーディング機能に送信する（図１の(1)、(3)）。

4　効果

提案方式により、以下の効果が期待できる。

（１）クライアントに対する効果

・セキュア・トレーダの保持する情報かあるいはトレーダの保持する情報かの一次切り分けが可能となるため、セキュア・トレーダとトレーダ双方に検索依頼を出さなくてよい。

・トレーダオペレーションとセキュリティメカニズムが１対１に対応する場合に有効である。

・トレーダで使用しているセキュリティのレベルを階層化し、セキュア・トレーダで管理することで、クライアントは各トレーダのセキュリティを意識する必要はなくなる。

（２）トレーダ提供者に対する効果

トレーダでどのようなサービスを検索できるか把握しなくてよい。

5　まとめ

筆者が提案したセキュア・トレーダと既存のトレーダが共存するシステムにおいて、クライアントからのトレーダオペレーションを効率よく処理できる方式として、トレーダオペレーションに使用しているセキュリティメカニズムに着目した切り分け方法を提案した。

今後は、本方式を実装し、性能評価等を行う。

[参考文献]

[1]鈴木滋彦, 山田茂樹, 岡田忠信: "分散処理ネットワークアーキテクチャDONAの基本構想", 信学技報, SSE96-63, IN96-47, CS96-71 (1996-09).

[2]OMG RFC 5 Submission Trading Object Service, OMG Document orbos/96-07-08, July 1996.

[3]今田美幸: "分散システムにおけるセキュリティについて",信学技報, SSE96-130, CQ96-40(1996-12).

[3]西田豊明: "ソフトウェアエージェントとその周辺",Vol.78, No.11, pp1252-1259, 電子情報通信学会誌, 1995.