オブジェクト指向分散環境 OZ++の セキュリティを考慮したサイト間通信の実装

3M－3

濱崎 陽一 (電子技術総合研究所)　鈴木 敬行* (シャープビジネスコンピュータ)
大西 雅夫* (東洋情報システム)　塚本 享治 (電子技術総合研究所)
*: 開放型基盤ソフトウェアつくば研究室研究員

1 はじめに

OZ++ は、ネットワーク上でクラスとオブジェクトの共有を可能とするオブジェクト指向分散処理環境である。本稿では、広域網を介したサイト間通信の実装について述べる。実装にあたっては、サイト間通信可能な OZ++ を導入する用いる事によりセキュリティレベルが低下することがないように留意した。

2 サイト間通信とセキュリティ

OZ++ でサイト間通信を設計する際に、インターネットセキュリティ要件を次のように設定した。OZ++ システムを導入することにより、1) 既存の情報の流出や破壊が発生しない、2)OZ++ で蓄えられた情報やサービスが不正にアクセスされない、3)OZ++ を利用して既存システムへの不正アクセスが起こらない [1]。

しかし、こうした不正なアクセスの有無を中継機構で判断する事は不可能であるので、オブジェクトの実行機構を組織外からのアクセスを特別に扱うように拡張し、中継機構には組織外からのアクセスであることが判断できるようにする機能のみを与えることとした。また、スケーラビリティや認証の時間的コストの点から、Kerberos のような広域認証システムは使わず、無認証で組織外のものは信頼しないポリシーを取った。

組織外部 (サイト外) からのアクセスは外来として扱い、上記のセキュリティ要件に対応して、1) ファイルへのアクセスを禁止、2)OZ++ ユーザ foreign 権限でのオブジェクトの実行と外部からアクセス可能なオブジェクトの生成禁止、3) ユーザ oznobody の権限での外部プロセスの実行という制限を設けた。

OZ++ のようなオブジェクトの実体が転送されるシステムでは、引数あるいは返り値としてサイト外からもたらされるオブジェクトの型はメソッド定義の型あるいはその子孫クラスである。そのため、親クラスのメソッドをウィルスのような悪意あるプログラムでオーバーライドしたようなクラスのオブジェクトが到来する可能性がある。このような悪意あるオブジェクトのメソッドは、どこから起動されたかにかかわらず制限付きで実行されるべきである。

こうした事から、サイト外からのメソッド起動 (スレッド) やサイト外からもたらされたオブジェクトは、外来のものとして管理することとした。オブジェクトとプロセスの外来性は次のようになる。

- サイト外からもたらされたオブジェクトは外来。
- 外来のプロセスが生成したオブジェクトは外来。
- サイト外からのメソッド起動のスレッドは外来。
- 外来スレッドから派生したスレッドは外来。
- 外来オブジェクトのメソッドを実行するスレッドは外来。

3 OZ++ のサイト間通信の実装

OZ++ のサイトはブロードキャストにより通信可能な物理的な範囲で、複数の計算機からなる。計算機上には、オブジェクトの実行実体であるエグゼキュータがいくつかとエグゼキュータを管理する一つのニュクリアスがある。これらによって、オブジェクトが相手のオブジェクトの位置を意識する事無くメソッドの起動を行なえる通信機構を提供している。

サイト内では、ニュクリアス間のブロードキャストによるエグゼキュータの通信アドレスの解決、エグゼキュータ間の TCP/IP によるオブジェクト間通信によりオブジェクト間通信が実現されている [2] が、広域網を介してはブロードキャストも IP 接続もできない。

サイト間通信を実現するためには、サイトをまたがる通信アドレスの解決とオブジェクト間通信の中継が必要である。そのために、組織のゲートウェイ計算機上に OZ++ のサイト間通信のためのゲートウェイ (OZAG) を設けることとした。またサイト内のブロードキャストを OZAG に中継する機能を備えたリレーニュクリアスをサイト毎に一つ設けることとした。

An Implementation of Inter-site communication with security in OZ++: An Object-Oriented Distributed Systems Environment

Yoichi Hamazaki(Electrotechnical Laboratory),
Takayuki Suzuki*(Sharp Business Computer Software, Co., Ltd.),
Masao Onishi*(Toyo Information Systems, Co., Ltd.),
and Michiharu Tsukamoto(Electrotechnical Laboratory)
*: Researcher, Tsukuba Laboratory, Open Fundamental Software Technology Project

3.1 サイト間でのアドレス解決

OZ++ではオブジェクトは全世界でユニークなID(OID)を持つ。OIDはその一部にサイトIDとエグゼキュータIDを含んでいる。よって、OIDからそのオブジェクトがサイト内にあるか否か、そのオブジェクトが存在するエグゼキュータのIDを知る事ができる。

サイトIDは集中管理されサイトIDとそのサイトを管理するOZAGの通信アドレスの対応表(サイト表)も集中管理される。各OZAGはサイト表のコピーを持っており、必要に応じて管理組織から再取得する。

サイト内ではブロードキャストによるアドレス解決が可能であるのでサイト毎にアドレス解決を行ない、OZAGはそれを利用する。サイトAのエグゼキュータEx-A3上のオブジェクトからサイトBのエグゼキュータEx-B3オブジェクトへメソッド起動のパケットを送る際のアドレス解決の手順は次のようになる。

サイトAでのアドレス解決 (図1) ①Ex-A3はEx-B3のアドレス解決をニュクリアスに要求し、②ニュクリアスはブロードキャストする。③リレーニュクリアスは他サイトであるのでOZAGに伝え、④OZAGは自分の通信アドレスを応える。⑤リレーニュクリアスはブロードキャストしたニュクリアスにOZAGからの応答を伝え、⑥Ex-A3はOZAGのアドレスをEx-B3宛のパケットを送る先として得る。

OZAG間のアドレス解決 サイトAのOZAGはサイト表からサイトBのOZAGのアドレスを得る。

サイトBでのアドレス解決 サイトBのOZAGはサイトBのリレーニュクリアスにEx-B3のアドレス解決を要求する。ブロードキャストによる問い合わせが行なわれEx-B3の通信アドレスが得られる。

OZAGはエグゼキュータIDとその通信アドレスあるいは中継するOZAGのアドレスの対応表をエグゼキュータ表として管理し、同一のアドレス解決を繰り返さないようにしている。

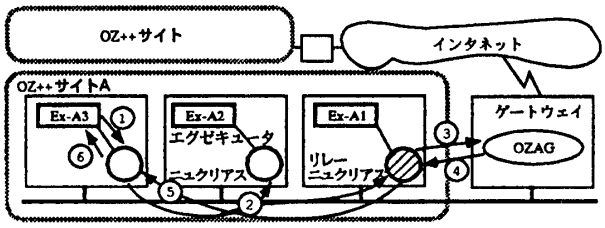

図 1: アドレス解決の手順

3.2 オブジェクト間通信の中継

オブジェクト間通信はメソッド起動によってなされる。メソッド起動は、最初にメソッドのcaller, calleeのOIDやメソッドのセレクタを含むパケットが送られ、ついで引数となるオブジェクトを含むパケットが送られる。メソッドの実行が終ると結果のパケットが返される。また、オブジェクト間通信のパケットにはメソッド起動毎にユニークなID (メッセージID: MID) が付与される。先ほどの例で、サイトAのOZAGの動作を示すと、次のようになる。

OZAGはメソッド起動の最初のパケットを受信すると、そこに含まれるcaller,calleeのOIDからそのパケットと同じMID(1234567)を持つパケットを中継する先をサイト表やエグゼキュータ表を参照して決定し、必要ならアドレス解決する。MIDと中継先の組はメッセージ表として管理する。

メッセージ表に従ってメソッド起動の最初のパケットはサイトBのOZAG(OZAG-B)に中継される。OZAG-Bに送られたパケットは同様に中継されてEx-B3に到達する。引数を含むパケットも同様にEx-B3まで到達する。

メソッドの実行が終了すると、その結果の種類と返り値は逆の経路でEx-B3からEx-A3に送られる。こうして両方向に中継をするためにMIDに対して二つの中継先がメッセージ表に記録されている。結果の最後のパケットを中継すると、そのMIDを持つパケットを中継する必要がなくなるので、エントリーはメッセージ表から削除される。

先に述べたように、パケットを中継する際には、外来である事を示すフラグを立てる。

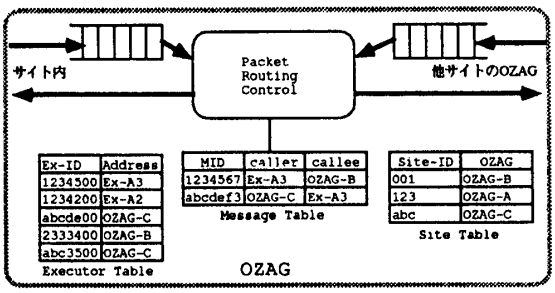

図 2: OZAGの構成とパケットの中継

4 まとめ

広域網を介したサイト間通信について、その構成、セキュリティ低下への対応策を示し、その実装を述べた。現在、その評価をすすめているところである。

本研究は、情報処理振興事業協会 (IPA) の「開放型基盤ソフトウェア研究開発評価事業」の一環として行われたものである。

参考文献

[1] 大西、濱崎、西岡、塚本：「オブジェクト指向分散環境OZ++におけるインターネットセキュリティ」、情処学会マルチメディア通信と分散処理ワークショップ、Oct. 1995.

[2] 濱崎、大西、鈴木、中村、塚本：「オブジェクト指向分散環境OZ++の通信機構の実装」、情処学会第49回全国大会、Oct. 1994.