監視系を安全に構築するための仮想分散環境

光来健一 †* 千葉滋 † 廣津登志夫 ‡ 菅原俊治 ‡

† 東京工業大学 情報理工学研究科 数理・計算科学専攻
‡ 日本電信電話株式会社 NTT 未来ねっと研究所

1 はじめに

クラスタなどの分散システムは外部からの要求を処理するサーバプログラムなどの計算系に加えて、分散システム全体を監視するための監視系を必要としている。監視系の役割の一つは計算系が外部から攻撃を受けていないかどうかを検出することである。このような監視系の代表的なものとして侵入検知システムがよく用いられている。侵入検知システムは分散システムに対する攻撃や侵入の徴候を発見すると、それを管理者に通知するシステムである。管理者が早めに攻撃の試みに対する対策を講じたり、侵入経路を割り出して再度の侵入を許さないようにすることができる。

監視系は常に分散システムを監視できなければならないが、従来のシステム構成では監視系が機能しなくなる場合があった。1 つは監視系が攻撃を受けた場合である。分散システムの監視系はホスト間で通信を行うため、その通信チャネルから攻撃を受ける危険性がある。また、攻撃を受けた計算系を経由して監視系が攻撃される危険性もある。別の問題としては、監視系のソフトウェアを一括してアップデートする際に一時的に監視系が停止し、その間に攻撃を受ける危険性がある。この危険性を避けるには監視系のアップデート中は計算系も停止させればよいが、分散システム全体の停止はできるだけ避けるべきである。

そこで、我々は図 1 のように監視系を仮想分散環境の中で動かす手法を提案する。仮想分散環境はポートスペース [1, 2] と呼ばれる各ホストで作られる仮想環境を仮想ネットワークを使って結合させたものである。ポートスペースは独自のファイルシステム空間、ネットワーク空間、プロセス空間を提供し、独自の仮想ネットワークを使用する。このようにして、仮想分散環境は監視系を計算系から分離する。そして、仮想分散環境は監視系に対して、計算系の使用する資源を監視する機能を提供する。

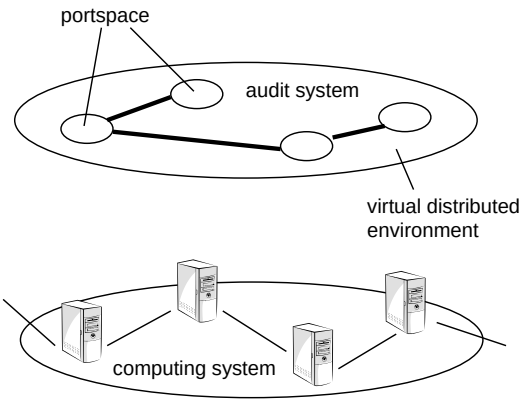

図 1: 分散システムにおける監視系と計算系の分離

仮想分散環境の中で監視系を動かすことにより、従来では監視系が機能を停止していた状況でも、監視を続けられるようになる。仮想分散環境は計算系から干渉されることはないので、監視系は攻撃を受けた計算系を経由した攻撃を受けずに済む。さらに、仮想分散環境はインターネットからも切り離されているので、監視系が信頼できない第三者から直接攻撃を受けることもない。また、監視系のソフトウェアをアップデートする際には、一時的に古いバージョンと新しいバージョンの監視系ソフトウェアを異なる仮想分散環境の中で同時に動かすことにより、監視系を停止させずにアップデートを行うことができる。

各ホストにおける侵入検知システムなどの監視系のソフトウェアは図 2 のようにポートスペースの中で動かされる。一方、サーバプログラムなどの計算系のソフトウェアは通常の実行環境（ベース環境）で動かされる。ポートスペースからはベース環境の

*kourai@is.titech.ac.jp

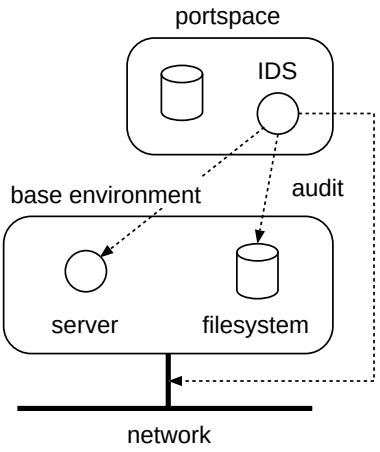

図 2: 各ホストの監視系の構成

ファイルシステムやネットワークなどを監視することができる。逆に、ベース環境はポートスペースの利用するファイルシステムやネットワークに一切アクセスすることができず、ポートスペース自体を終了させたりすることもできない。

2 現在のステータス

現在、我々は仮想分散環境を FreeBSD 4.9 に実装しているところであり、ポートスペースからベース環境のファイルシステム、ネットワーク、プロセスなどを監視できるようにしている。単一ホストでのファイルシステムとネットワークの監視についての基本的な部分は動いており、文献 [3] で既に報告している。今後はファイルシステムとネットワーク以外の監視への対応、および、分散システムにまたがる監視に対応していく予定である。

参考文献

[1] Kourai, K., Hirotsu, T., Sato, K., Akashi, O., Fukuda, K., Sugawara, T. and Chiba, S.: Secure and Manageable Virtual Private Networks for End-users, in *Proceedings of the 28th Annual IEEE Conference on Local Computer Networks*, pp. 385–394 (2003).

[2] 光来健一, 廣津登志夫, 佐藤孝治, 明石修, 福田健介, 菅原俊治, 千葉滋：VPN とホストの実行環境を統合するパーソナルネットワーク, ソフトウェア科学会論文誌 コンピュータソフトウェア：掲載予定.

[3] 光来健一, 廣津登志夫, 佐藤孝治, 明石修, 福田健介, 菅原俊治, 千葉滋：仮想環境を用いた侵入検知システムの安全な構成法, 第 5 回インターネットテクノロジワークショップ (2003).