10

ITBL セキュア VPN とポータルサイト

鶴岡信彦、渡辺勝弘、黒川原佳、福井義成、姫野龍太郎（理化学研究所）

ITBL secure VPN and portal site

Nobuhiko Tsuruoka, Katsuhiro Watanabe, Motoyoshi Kurokawa, Yoshinari Fukui, Ryutaro Himeno

Abstract

This paper describes the concept and design of virtual computing environment project ITBL. The goal of ITBL project is the mutual utilization of computing-resources among multiple organizations and the convenient environment for users to access resources or to develop user application. For this purpose, ITBL project is not based on only GRID technology. To realize the concept, we propose several infrastructure models. We developed three independence technologies ITBL-VPN, PitSaw and ITBL portal. At present we almost finish these developments and ITBL experimental system works shortly. A further direction of this study will be to evaluate these implementations.

1．はじめに

近年，ネットワークを有効に利用し組織や分野の枠組みを越えて利用できる仮想計算環境，仮想実験環境（Grid 環境）を構築しようとする試みが活発に行われている。ITBL もこのようなプロジェクトの一つの形である.

ITBL は複数参加機関が研究資源の相互利用を行い、仮想研究環境を構築するプロジェクトである。ITBL ではこの目的を達成するために、一般的に Grid 環境を構築するために使用される Globus toolkit にとらわれず、状況に応じて既存技術と新規開発技術を統合することにより高度な分散環境を構築する。ITBL における分散環境構築のコンセプトは高いセキュリティを保ち、資源(計算資源、データベース等)の相互利用や共同研究用コラボレーションツール等の基盤技術をユーザに負担を求めない方法で開発することである。

本論文では，これら ITBL プロジェクトで開発した基盤技術の内、研究機関間を接続する閉鎖系ネットワークであるセキュア VPN、分散ログ収集解析システムによる仮想計算環境，仮想実験環境の構築におけるセキュリティの問題を解決する手段について述べる。また、Web から仮想計算環境，仮想実験環境を簡単に利用することができるポータルシステムのプロトタイプの構築について述べる。

2．セキュア VPN

2．1　VPN の概要

近年、多数のコンピュータをインターネットに接続して利用することは必須であるが、接続されたコンピュータは、ネットワークを利用して cracking(5,6,7)される。cracking 対策として多くの組織ではFireWallのようなセキュリティ機器を導入し、TCP/IP プロトコルに対して特定のアドレスグループ、TCP/UDP サービスに対して制限を行なっている。この手法は想定したユーザを組織内資源に安全にアクセスできるようにすることを目的としている。しかし、FireWall による以下に示すプロトコルへの制限には利便性や安全性に問題がある場合が多い。

- FTP や X session のように TCP/UDP session がコールバックされる
- Sun RPC のようにポートが動的である
- NFS、NIS のように OS に直接攻撃が行ないやすい
- telnet に見られるように通信内容が plain text により送信される

これらは HPC 環境で一般的に使用されるプロトコルであるが、FireWall では不十分な防御しか行えず、制限すれば極端に不便に、解放すれば容易に攻撃される。FireWall の設置による取り扱いの難しいプロトコルに対して、他の手法を援用することによって問題の解決を図ることも可能である。例えばパスワードの推測に対しては Kerberos、S-Key、SecurID 等の手法、データそのものの改竄、盗聴に対しては SSH、SSL 等の TCP サービスレベルの暗号化手法が有効である。しかし，複数手法の組み合わせによって資源提供を行うことは運用コストの上昇を伴い、またその複雑さ故にシステムにセキュリティホールが生まれる原因ともなる。特に ITBL プロジェクトのような複数機関による計算機の共同利用や共同研究などのセキュリティを考慮した場合、複数手法の組み合わせによるシステムの複雑さは顕著なものとなり、より直接的な解決方法が求められる。

本提案では VPN(Virtual Private Network)技術の 1 種である IP Security Protocol (IPsec) (1,2,3)を利用して、複数機関間を接続する閉鎖系ネットワークを構築し、上記のような問題を解決する枠組みを提案する。

2．2 ITBL-VPN

ITBL-VPN は IPsec を使用した閉鎖ネットワークであり以下の特徴を持つ。

- ITBL-VPN ノード間通信は全て IPsec を使用して行なう。これによりインターネット上での通信傍受は困難となる。
- 原則として参加機器に特別な設定を行なう必要はない。
- HPC の利用形態を考慮し、最大で 1Gbps のスループットが提供可能である。
- 接続機器は接続速度に応じた価格選択が可能である。
- 同一機器により ITBL－VPN 内に閉鎖ネットワークを複数持つことができる。これにより相互に接続すべきでないプロジェクトを容易に分割することができる。
- ITBL-VPN 外からのセキュアな接続方法を提供する。

ITBL-VPN 全体の接続方法を図 1 に示す。VPN ルータは主に 2 種類から構成される. 基幹 VPN ルータはフルメッシュ IPsec tunnel 構成、エッジ系 VPN ルータはいずれかの基幹系 VPN ルータに IPsec tunnel で接続する構成となる。原理上 1 基幹 VPN ルータで数千の IPsec tunnel が扱えるため、この構成により大規模な VPN を構築することが可能となる。

また図 2 に示すように、Multi-tenant 機能を使用することにより一つの VPN ルータを使用して複数の分離した閉鎖系ネットワークを構成することも可能である。これにより複数組織に跨る複数プロジェクトへの対応も可能となる。

2．3 ITBL-VPN の現状と今後

原則として ITBL-VPN ネットワークに参加するユーザは、安全なネットワーク環境でプロトコル制限等に煩わされることなく様々な機関に分散した資源にアクセスすることが可能となる。現在 ITBL-VPN は構築中であり、提案を実証する段階であるが、現段階でも以下の問題がある。

(ア) 内部からの攻撃への対処が難しい

(イ) IPsec による遅延がアプリケーションに与える影響とその対策

(ウ) ワークステーション等も含めた single sign on ができない

（ア）に対しては同時に開発している DNIDS との連係で対応可能であると考えられる。（イ）に対しては常時アプリケーション通信の遅延、利用帯域等を測定する方法を開発し対策する予定である。また（ウ）に関しては GRID 認証技術(4)との連係も検討している。

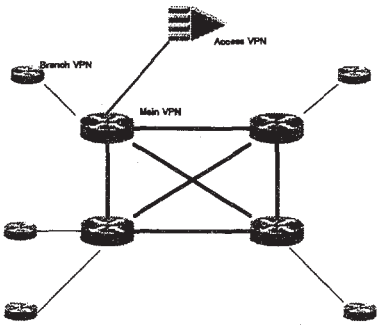


図 1 ITBL-VPN Topology

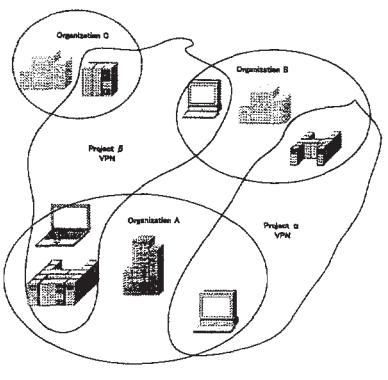


図 2 VPN for Multi-Organization

3. 分散コンピューティングにおけるログ収集解析システムの構築

3. 1 概要

多数の計算機・ネットワーク機器が展開される分散コンピューティング環境下においては，ログの収集・監視作業は管理者へ大きな負担を与える．これまで UNIX 系オペレーティングシステムに実装される Syslogd や互換ソフトウェアのログ転送機能によってログ収集を行ってきた．これらは数百台以上の規模からなる分散コンピューティング環境を考慮した設計がされてない．このため多数の計算機の監視や，監視サーバを分散化させることが困難である．またログの監視作業は人間による手作業に多くを委ねるにも拘わらず，単調な作業になる傾向が強く，見逃しや誤認などのエラーを発生させる．

今回提案するログ収集・解析システム「PitSaw」では，P2P 技術を基にした柔軟性・拡張性の高いログの配送機能を提供する．またログの自動監視機能も提供する．自動監視機能では，単純なログ監視機能のほかに，複数の計算機・ネットワーク機器を包括的に監視・分析可能な相関分析機能を持つ．

これにより分散コンピューティング環境におけるログ監視の効率化と，精度の高いログ解析を実現し，管理者の負担を低減する．

3. 2 ログ収集解析システム PitSaw

PitSaw では，ログを他の PitSaw ノードへ配送する機能，およびプログラムされた手順に従いログを解析・加工する機能を持つ。現在の実装では Solaris 8, RedHat Linux 7.x, Debian linux 2.x, OpenBSD 2.8/i386, FreeBSD 4.1, NetBSD/i386 1.5.2 の主要な UNIX 系 OS 上で動作する．

3. 2. 1. システムの構成

PitSaw システムは，ログを格納するためのレコード，ログを配送するための PitSaw ノード，ログの配送情報を管理する PitSaw サーバの要素から構成される．

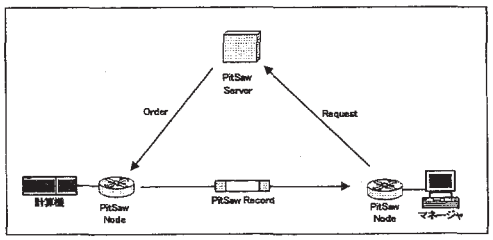


図 3 PitSaw システム

ログは PitSaw ノードで PitSaw の基本フォーマットであるレコードに変換される．レコードは複数項目から構成され，各項目は整数，文字列の型を持つ． PitSaw ノードはサーバの指示を受け，他の PitSaw ノードにレコードを転送する．以下に Syslog を Pitsaw レコード形式に変換した例を示す．実際に個々の項目はテキストではなくバイナリ形式で保持される．

```
Syslog {
        Host = 192.168.1.1:IPv4;
        Created = 2002/08/22 13:11:10:time;
        Message = "Failed password":string;
        PID = 2082:int;
}
```

PitSaw Record の例

3. 2. 2. レコードの転送とリクエスト形式

PitSaw システムにおいてレコード転送は，受信 PitSaw ノードのリクエストに応える形式により行われる．送信 PitSaw ノードが受信 PitSaw ノードからリクエストを受けた場合，送信 PitSaw ノードでは該当するリクエストに対するレコードをネットワークポートに送り出す．受信 PitSaw ノードは送信 PitSaw ノードのネットワークポートに現れたレコードを読み取ることで転送処理が完了する．(図 2.) 同一のリクエストを持つ複数の受信 PitSaw ノードが存在する場合，送信 PitSaw ノードのネットワークポートに現れたレコードを，それぞれの受信 PitSaw ノードが読み出す．これにより送信 PitSaw ノード上の実行プロセス数を節約できる．

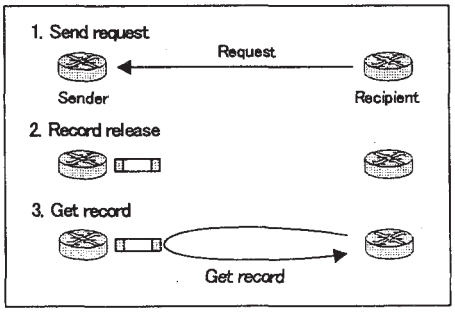


図 4 レコード転送の流れ

リクエストは必要とするレコードの条件、address or address range、record type、group から構成される．これをリクエスト tuple と呼ぶ．以下は「192.168.0.0/24 のネットワークレンジ上に存在する syslog を扱う総て」の条件を記述したリクエスト tuple の例である．

```
( 192.168.0.0/24 , syslog , * )
```

図 5 リクエスト Tuple の例

3. 2. 3. PitSaw サーバ

PitSaw システムでは計算機・ネットワーク機器の増加，ネットワークの規模の拡大に伴って PitSaw ノードが増加する．PitSaw サーバでは，受信 PitSaw ノードの要求するリクエストを正しく送信 PitSaw ノードに転送する機能を提供する．

PitSaw ネットワークに対して送信 PitSaw ノードが JOIN した際に，送信 PitSaw ノードの送信可能なログに関する情報が PitSaw サーバに記録される．受信 PitSaw ノードで発行されたリクエスト tuple によるリクエストは，PitSaw サーバに送信され，リクエスト tuple と送信 PitSaw ノードの情報から条件に一致する送信 PitSaw ノードを決定し，レコードの転送指示が適切な送信 PitSaw ノードに転送される．

3. 2. 4. レコードの解析機能

全ての PitSaw ノードはレコードを転送する際に，あらかじめプログラムされた手順に従い単一のレコードを解析・加工する機能を持つ．レコード解析部では複数レコード間の相関関係を分析することができる．例えば計算機 A において検出されたイベント A と計算機 B において検出されたイベント B が特定の時間帯にあった場合に管理者に通知するといった処理が可能となる．

3. 3 適用例

以下に不正アクセスの監視と計算機のログ収集に PitSaw を適用した例を示す．

3. 3. 1 分散設置された NIDS のアラートを収集する例

ネットワーク上に分散設置された不正アクセス検知システム(NIDS)のデータ(アラート)を，PitSaw のレコード転送機能と解析機能により統合することができる．それぞれの NIDS で検出されたアラートの相関分析を行うことで，ネットワーク上で発生する異常状態を包括的に監視することができる．(図 6) これによりネットワーク全体に対する不正アクセス等を正しく検知することができる．

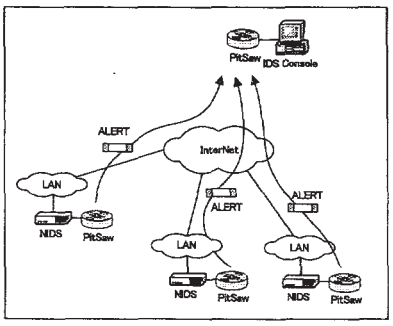


図 6 PitSaw により NIDS を統合する例

3. 3. 2 分散設置された計算機のログを収集する例

PitSaw を用いてインターネット上に分散設置された計算機のログの収集・監視を行う例を図 7 に示す．PitSaw を利用した場合，Syslogd のログ転送機能に比べ，ファイアーウォールを跨いだログ転送が容易に実現できる． PitSaw ではログ転送の要求があったノードに対してログが転送される．これにより，固定的なログ受信サーバを持つ必要が無くなる．またログサーバの分散化も容易に実現できる．

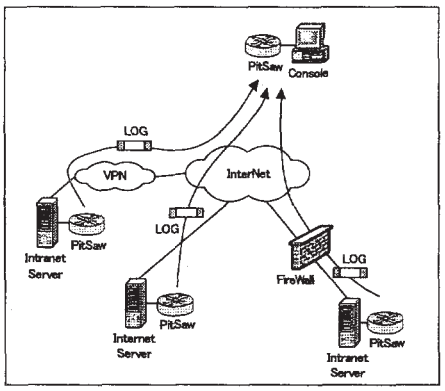


図 7 PitSaw によるログ監視の例

3. 4 現状と今後の課題

PitSaw を利用することにより，さまざまなネットワーク環境に対応できるログ収集システムを構築できることが分かった． IDS と組み合わせることにより，検知精度の向上に貢献することも分かった．今後は PitSaw ノード間通信に暗号化と認証機能を持たせる予定である．また，数万台にも及ぶような PitSaw ノードを制御するために，各 PitSaw ノードが自立的に動作するような次世代 P2P 技術の摘要を検討している．

4. Web Portal の構築

4. 1 はじめに

本節では，Web を用いた ITBL Portal システムの概要・目的について説明する。ITBL Portal システムのプロトタイプを構築することにより，Portal システムの設計・構築指針を示す。

4. 2 概要

ITBL Portal は，Grid 環境を科学者や技術者が簡便に利用するために提供するシステムである．ITBL Portal システムは大きく 3 つのパートに分かれる．第 1 は共同研究の

調整や研究資料等のグループウェア・データベース部である．第2はITBLの計算リソースを容易に用いるためのジョブハンドリング部である．第3は計算リソースを用いたISV(Independent Software Vendor)のアプリケーション試用/評価部である．

ITBL Portalは Webシステムを用いるため，

- 世界中どこからでもアクセス可能
- 計算機システムに不慣れなユーザのユーザビリティーの向上
- ターミナルでの複雑なコマンド操作からの解放
- HTTP/SSLを用いることでセキュリティを確保
- Web サービスは独立のため，計算ジョブインタフェースの更新が容易

等の利点がある．

4．3 構築ツール

ITBL Portalシステムは前述のように3つのパートからなるが，アプリケーション試用/評価部はジョブハンドリング部と同じ機構を用いるため，2つのパートを構築する必要がある．Portalシステムの構築には標準技術であり，ハードウェア依存性のない可搬性が高い方法を用いた．

グループウェア・データベース部の構築はJavaをベースとした．Javaを用いることでソフトウェアのハードウェア依存がなくなり，ソフトウェアの整備性や可搬性が向上する．Java環境はTomcatを用いた．Tomcatは JSP(Java Server Page)環境を実現するソフトウェアである．

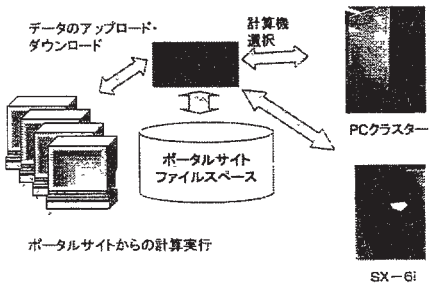
ジョブハンドリング部はWebのインタフェース部と計算ジョブ管理部がある．ジョブハンドリングにおけるWebインタフェース部の構築方法はCGIやJavaを用いるToolkitや独自実装が数多く存在する．ITBL PortalではGridPort Toolkitをベースとして用いた．GridPort Toolkitは Perl/CGIによるGlobusベースのGrid環境における Web Portal構築のためのToolkitである．ただし，GridPortもToolkitとして不十分なものであり，ITBL Portalでは非常に多くの部分が独自仕様である．

計算ジョブ管理部はユーザジョブのハンドリングを行うツールである．ツールとしてSGE(SUN Grid Engine)，LSF(Load Sharing Facility)やGlobusが存在する．どれも計算ジョブを広域に分散した計算リソースに投入することが可能であり，コマンドベースのツールである．ハードウェア依存性や可搬性は，どれも同等であるが，LSFやオープンソース版SGEは十分セキュリティを考慮していない．また，Grid環境において，Globusは事実上の標準技術である．ITBL Portalのジョブ管理はGlobusを用いた．このため，Globusを導入した計算リソースはITBL Portalシステムとして追加・削除等が自在に可能である．

4．4 バックエンドの計算機

ITBL Portalから利用可能な計算リソースは，PCクラスタとベクトル型計算機である．各計算リソースにはGlobusが導入され，Grid環境での計算機利用が可能である．現在、計算リソースやISVアプリケーションソフトウェアの利用は無償である。

PCクラスタはGatewayノードと多数の計算ノードからなる，SCore型PCクラスタである．計算ノードはNEC製Express5800/54Weである．諸元はCPU：Pentium4 2.2GHz，主記憶容量：RDRAM(PC-800)1GB，ディスク容量：36.3GB，ネットワーク：100Base-TXと1000Base-Tの2系統である．計算用通信はGigabit Ethernet，制御用通信は100Mbps Ethernetで接続されている．OS(Operating System)は全てLinuxである．コンパイラはGCC，PGI，Intelの各コンパイラを使用可能である．並列計算のための通信ライブラリはMPI(Message Passing Interface)を使用可能である．



ベクトル型計算機はNEC製SX-6iである．諸元はCPU:理論性能8GFLOPSのベクトルプロセッサ，主記憶容量：8GB，ディスク容量：73GBである．SX-6iはGatewayサーバを介して外部から利用可能である．ソフトウェアはNEC製のSX用ソフトウェアが利用可能である．Gatewayサーバと SX-6iは1000Base-SXで接続されている．

4．5 アプリケーションソフトウェアのショウルーム

ITBL Portalは，Web環境からのシミュレーションの可能性を実証するためプロトタイプである．シミュレーショ

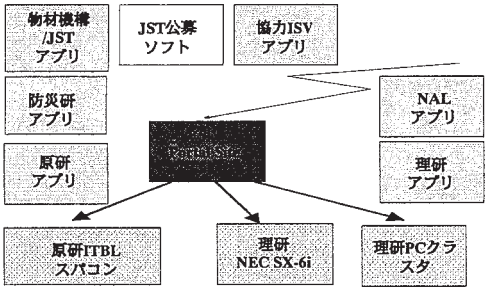
ンのユーザには次の２つのタイプが存在する．

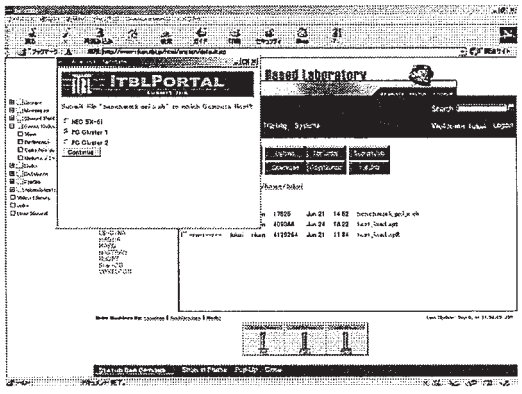
・　ソースプログラムからの実行

・　汎用アプリケーションソフトウェアの利用者

前者はポータルサイトの計算リソースと開発言語を用いるだけでシミュレーションが可能であるが，後者の場合は汎用アプリケーションソフトウェアの準備が必要である．その場合，同じ分野でも数種類のアプリケーションソフトウェアが存在し，ユーザ自身がアプリケーションソフトウェアを試用しない限り，ユーザ自身の問題を解く最も適しているアプリケーションソフトウェアを特定することは困難である．本ポータルサイトでは，主要なISVのアプリケーションソフトウェアを試用できる環境を準備している．いわばアプリケーションソフトウェアのショールームである．すでに，10を越す主要なISVから賛同を得ている．

ユーザは最適なアプリケーションソフトウェアを決定するまで費用と計算リソースの準備作業が発生しないというメリットがある．ISV にとっては，各自のアプリケーションの宣伝・拡販の機会を拡大でき，常時同一の計算資源を用いるため試用段階でのサポート負荷を低減できるメリットがある．





5．おわりに

ITBL プロジェクトにおける主要技術である ITBL-VPN と PitSaw および ITBL Portal を説明し，それらシステムの有用性および構築に対する指針を示した．ITBL-VPN は機関(計算リソース)間に高いセキュリティレベルの閉鎖系ネットワークを構築可能であり，ネットワーク構成の変更が非常に容易に行える．PitSaw は広域分散化した計算リソース環境において，各計算リソースのログ出力の種類依存しないログ監視と異常検出が可能であり，分散環境下での計算リソース管理・運用において非常に有効な手段である．ITBL Portal は総合的な研究者・技術者支援システムあり，ユーザフレンドリな Web ベースのシステムとして構築した．また，計算シミュレーション Portal システムとしての設計指針を示し，実際に構築したシステムでは ISV アプリケーションの試用環境も設けることで幅広いシミュレーションユーザが ITBL Portal を利用することが期待できる．

参考文献

(1) RFC2401 Sewcurity Architecture for the Internet Protocol, S. Kent, R. Atkinson

(2) RFC2408 Internet Security Association and Key Management Protocol, D. Maughan, M. Schertler, M. Schneidr, J. Turner

(3) RFC2409 The Inetrnet Key Exchange, D. Harkins, D. Carrel

(4) Globus Toolkit 1.1.3 System Administration Guide, the globus project

(9) A Security Architecture for Computational Grids

(10) ハッカー・プログラミング大全, UNYUN

(11) Maximum Security, Anonymous

(12) Snort Lightweight Intrusion Detection for Network , Martin Roesch.

(13) A Real-Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations , Nei Kato , Hiroaki Nitou , Kohei Ohta , Glenn Mansfield , Yoshiaki Nemoto.

(14) The Objective Caml system , Xavier Leroy.

(15) プロトコル構文規定言語 ASN-1 , 森野 和好 , 戸部 美春.

(16) Grid Port: https://gridport.npaci.edu/

(17) Globus: http://www.globus.org/

(18) SGE: http://www.sun.com/software/gridware/sge.html

(19) SGE: http://gridengine.sunsource.net/

(20) LSF: http://www.platform.com/