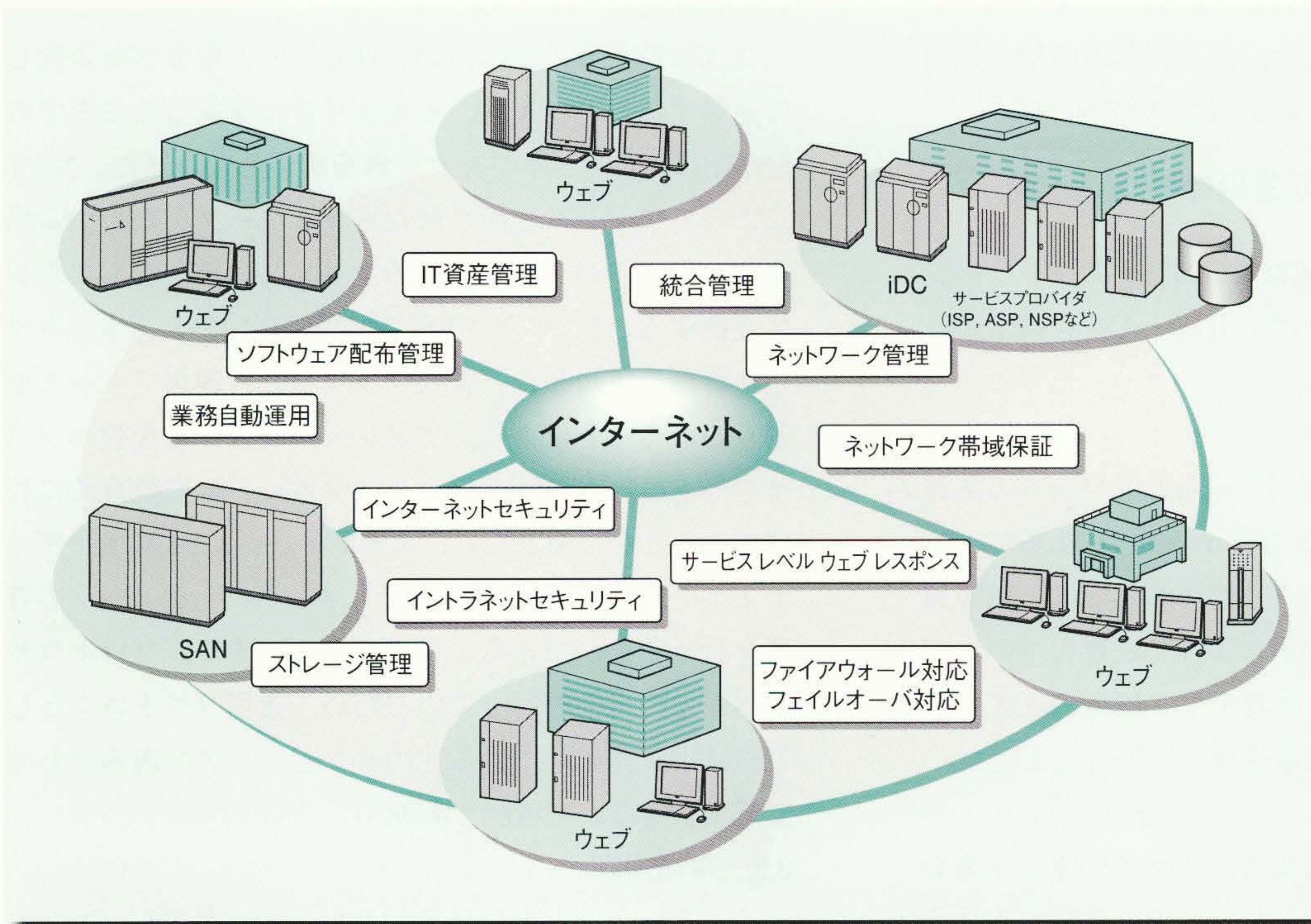


インターネットビジネスのシステム運用を支援する 統合運用管理“JP1”

Integrated Management System for Internet Businesses

平林元明 *Motoaki Hirabayashi*
大矢雅章 *Masaaki Ôya*

高山聡一郎 *Sôichirô Takayama*
佐藤俊夫 *Toshio Satô*



注：略語説明

IT (Information Technology)
iDC (Internet Datacenter)
ISP (Internet Service Provider)
ASP (Application Service Provider)
SAN (Storage Area Network)
NSP (Network Service Provider)

インターネットビジネス環境に対して“JP1”が提供する運用管理機能

インターネットビジネスの世界では、ネットワーク管理やセキュリティ管理、サービスレベル管理などが重要になる。

インターネットを中心としたビジネス環境へと社会の流れが大きく変化するのに伴い、情報システムに求められる運用管理の要件も質的に変化している。特に、インターネットビジネスでは、ECサイトのサービス品質がビジネスそのものの品質として評価される。また、iDCやASPは従来の情報システムよりも大規模であり、ネットワークやセキュリティなどの面でも従来とは異なる管理手法を必要とする。

日立製作所は、eマーケットプレイスが求めるサービスレベルを実現し、iDC・ASPなどのために強化した運用管理ソフトウェア“JP1 Version 6i”を発表した。“JP1 Version 6i”は、単にファイアウォールやNATなどのインターネット接続のための機能に対応するだけでなく、ビジネスポリシーに合わせたQoS制御やエンドユーザーの視点から見たウェブ性能の監視など、SLAで規定された管理機能を提供する。これらの機能により、運用管理ソフトウェアそのものをビジネス価値を創造するツールとして活用することができるようになる。

1 はじめに

社会の流れがインターネットを基盤としたビジネス環境へと大きく変化している。情報システムどうしがインターネットを通して相互に接続されることにより、B2B (Business to Business) や G2B (Government to Business) によるビジネス価値の拡大、B2C (Business to Consumer), G2C (Government to Consumer) による顧客サービスの提供が可能となり、情報システムが企業活

動の中心となってきた。

これに伴い、それを支える情報システムにも従来とは異なる要件が求められつつある。特に最近では、iDC (Internet Datacenter) や ASP (Application Service Provider) などのサービスを積極的に活用していこうという動きが進んでいる。これら情報システムを支える運用管理システムも、これまでのシステムの監視やスケジューリングといったリアクティブ(受動的)な管理だけでなく、ビジネス価値を創造するツールとして運用管理シス

テムそのものを活用していこうという動きが広がってきている。特にインターネットビジネスでは、EC (Electronic Commerce) サイトのサービス品質がビジネスそのものの品質として評価されるため、信頼できるサービスを提供することが重要になる。

ここでは、iDCやASPのためにインターネットビジネス環境を中心に対応を強化した、日立製作所の統合運用管理ソフトウェア“JP1 Version 6i”について述べる。

2 iDC・ASPにおける運用管理上の特徴

情報システムの管理を外部に委託する「アウトソーシング」という従来の形態と比べて、iDC・ASPには次の特徴がある。

(1) ネットワーク管理上

セキュリティやIP (Internet Protocol) リソースの関係で、NAT (Network Address Translator) によるアドレス変換を使用する場合も多い。これに対しては、顧客側の情報システムとの連携や管理によってこれらへの対応を図ることができる。また、業務データ配送の優先度をQoS (Quality of Service) による帯域保証で可能とした。

(2) セキュリティポリシー上

インターネットに直結するため、ファイアウォールなどの設置はもちろんのこと、iDC・ASPで管理する対象には、ウェブサーバをはじめとするオンラインデータベースなどさまざまなものがある。ここでの外部不正アクセスに対応するためにファイルアクセス制御や外部アクセス管理により、セキュリティ管理機能を強化している。

(3) サービス品質の保証

iDC・ASPが提供する付加価値の違いは、サービスレベルの違いと言ってもよい。故障通知時間や故障回復時間といった障害に関するもの、伝送遅延、安定したレスポンス性能といった性能に関するものなどがある。さらに、顧客満足度の測定や問題点の具体化による切り分けなどを支援することも必要になる。これらの分析により、ウェブサイトの最適化やパフォーマンスを向上させるための改善策を発見する。

ネットワーク管理とセキュリティ管理およびサービス管理での、製品による具体的な対応と顧客メリットについて以下に述べる。

3 ネットワークの管理

3.1 ファイアウォールとNATへの対応

ネットワーク管理では、SNMP (Simple Network

Management Protocol) を利用した管理が一般的である。しかし、ファイアウォールを介してネットワーク管理を行う場合、SNMPのポートを透過させる必要があり、ネットワークのセキュリティが低下する。このため、従来は、ネットワークの管理が企業内LANや専用線による接続の範囲に限定されていた。

これに対して、SNMPの管理パケットをカプセル化して通信することにより、セキュリティを保ったままのSNMPによるネットワーク管理を実現した。また、NATによってアドレス変換されたネットワークを監視する場合に、SNMPパケット内のIPアドレスのデータもアドレス変換することで、NAT環境でのSNMPによるネットワーク管理を実現した。監視マップ上で管理用アドレスを割り当てることにより、アドレスが競合する複数のプライベートネットワークを一つのマネージャで統合的に管理することが可能となり、スタティックNAT環境やダイナミックNAT環境のいずれでもネットワークノードの管理を行うことができるようになった。また、プロトコルレベルでの変換を行っているため、通信プロトコルとしてSNMPを採用している他のソフトウェアと組み合わせで適用することも可能である。

3.2 帯域保証

インターネット上には多数のルータが存在し、エンドトゥー エンドの通信は複数のルータを使って行われる。QoSを保証するためには、ネットワークに点在する複数のルータに対して統合的にQoSを制御するように設定しなければならない。従来のネットワークでは、コネクション単位でパケットを制御することによってQoS制御を行っていた。しかし、インターネットでは、単にコネク

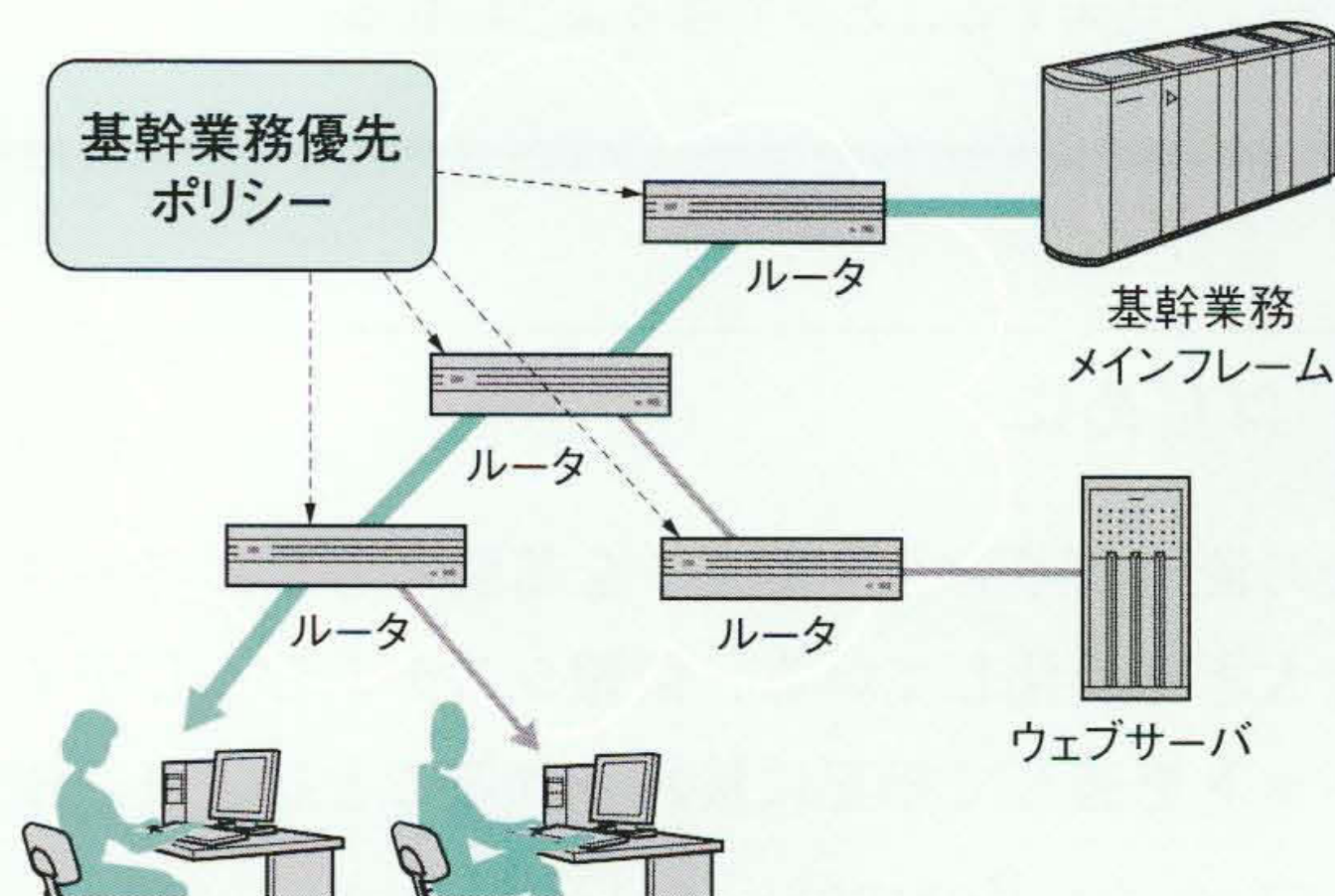


図1 基幹業務データの伝送例

ウェブサーバへのアクセスが頻繁に行われても、基幹業務の通信レスポンスの悪化を防ぐことができる。

ション単位での制御では複数のルータに対して一貫して効率的な制御をすることが難しい。これに対して「基幹業務優先ポリシー」という考え方を導入した(図1参照)。

ポリシーとは、どの業務データを優先的に配送するかという方針である。具体的には、IPパケットの先頭に、配送の優先度や帯域の大きさのグループを識別するための部分を設け、そのグループに従ってQoSを保証する。これにより、重要な業務アプリケーションに対する必要な帯域の保証や優先的な配送、メールやファイル転送のようなトラフィックに対しては優先度を下げたり、輻輳(ふくそう)時に廃棄したりするなどの制御が可能となる。

4 セキュリティの管理

セキュリティポリシーの違いを意識したアクセスの管理を行うためには、これまではOSで提供されていたアクセス制御を、運用管理の観点から、外部不正アクセスを含めた統合的なセキュリティ管理機能として体系化する必要がある。

4.1 アクセス制御

ファイアウォールなどインターネットとの接続部分でのセキュリティは一般的によく行われているので、セキュリティに関する問題は少ない。しかし、ログインが可能なユーザーや日時、端末を指定することにより、勤務時間外に裏口の外部接続回線を使った不当なログインなどを防止する必要がある。また、ファイルアクセスの制御によって不当なアクセスを防いだり、一般ユーザーが管理者権限を不当に行使することを防止することができる。このように、管理権限や監査権限などを複数のユーザーに分散することは、内部不正の抑止などに効果がある。

4.2 外部アクセス管理

ファイアウォール外のログ分析により、不正なアクセスを検知できるようになる。外部からの不正アクセスでは、異なるMAC(Media Access Control)アドレスが同一のIPアドレスを持つ「IPスプーニング攻撃」や、DoS(Denial of Service)攻撃、ポートスキャンなどが有名である。また、短時間に多数の認証が失敗しているような場合も注意する必要がある。外部アクセス管理では、これらの情報について、ルール・ポリシー設定に基づいた防御動作を起動させる(図2参照)。

5 サービスレベルの管理

ネットワークやデータベース、アプリケーションといったシステムの個々のコンポーネントの性能監視は従来行われていた。しかし、これらは、エンドユーザーから見たサービスレベルを直接監視するものではないので、インターネットビジネスでのサービスレベル管理を行うためには、それに合わせた方法が必要である。

5.1 ウェブサイトの性能管理

この機能では、エンドユーザーの視点から見たウェブサイトの性能を直接監視する。擬似的なアクセス要求を実際に発行して測定することにより、ウェブサイトの性能のボトルネック(障害)を検出し、ウェブサイトの性能改善を行うための情報を提供する。

このために、まず、URL(Uniform Resource Locator)ごとのページ表示速度や、CGI(Common Gateway Interface)の実行速度などを測定する。さらに、ウェブサイト利用者がどのURLトランザクションを切断したか、どのURLにアクセスを集中させたか、どのURLにど

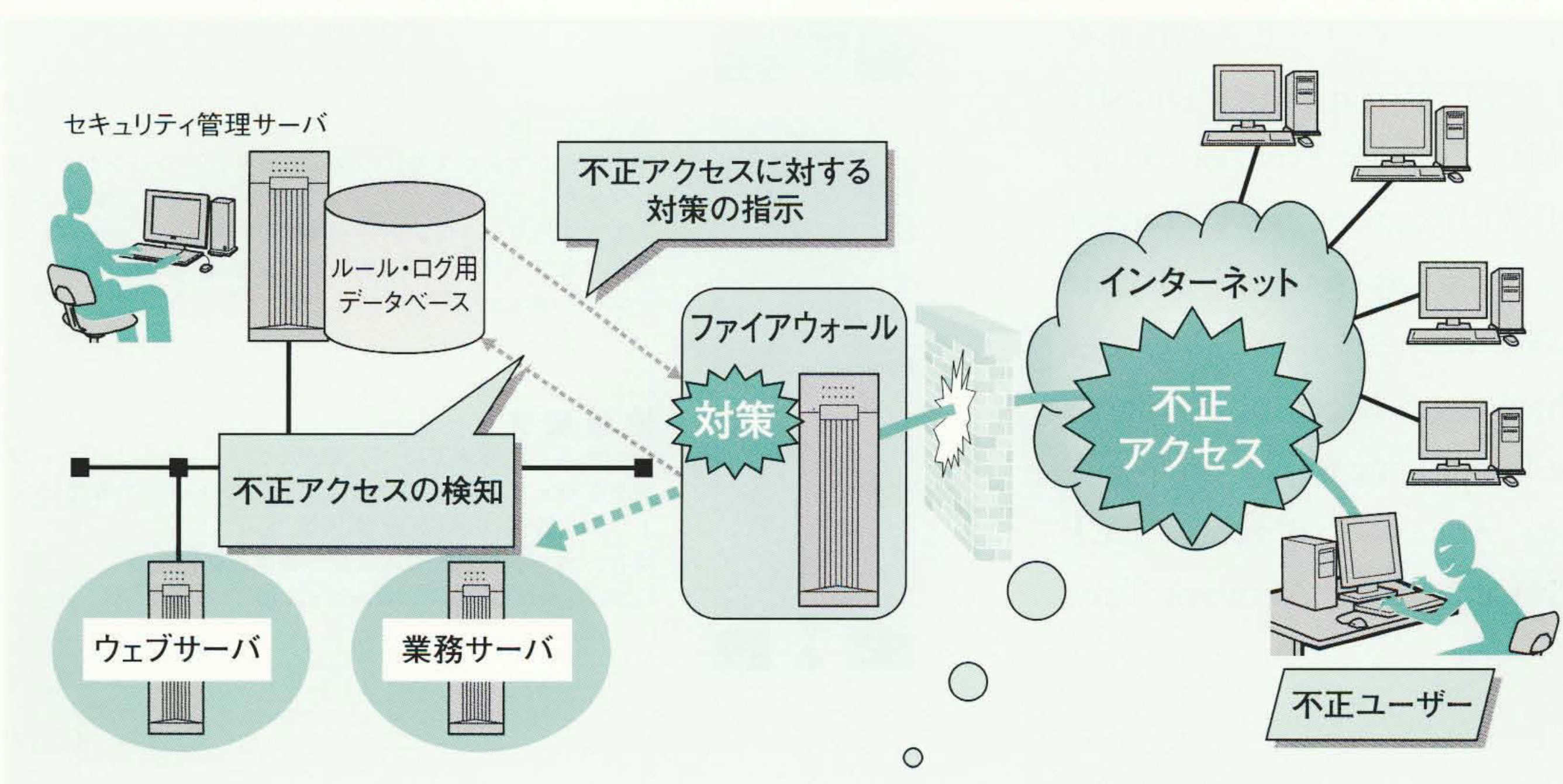


図2 外部不正アクセスの検知と防御動作

ファイアウォールのログ情報をルールに従って分析し、不正アクセスに対処するアクションを起動する。

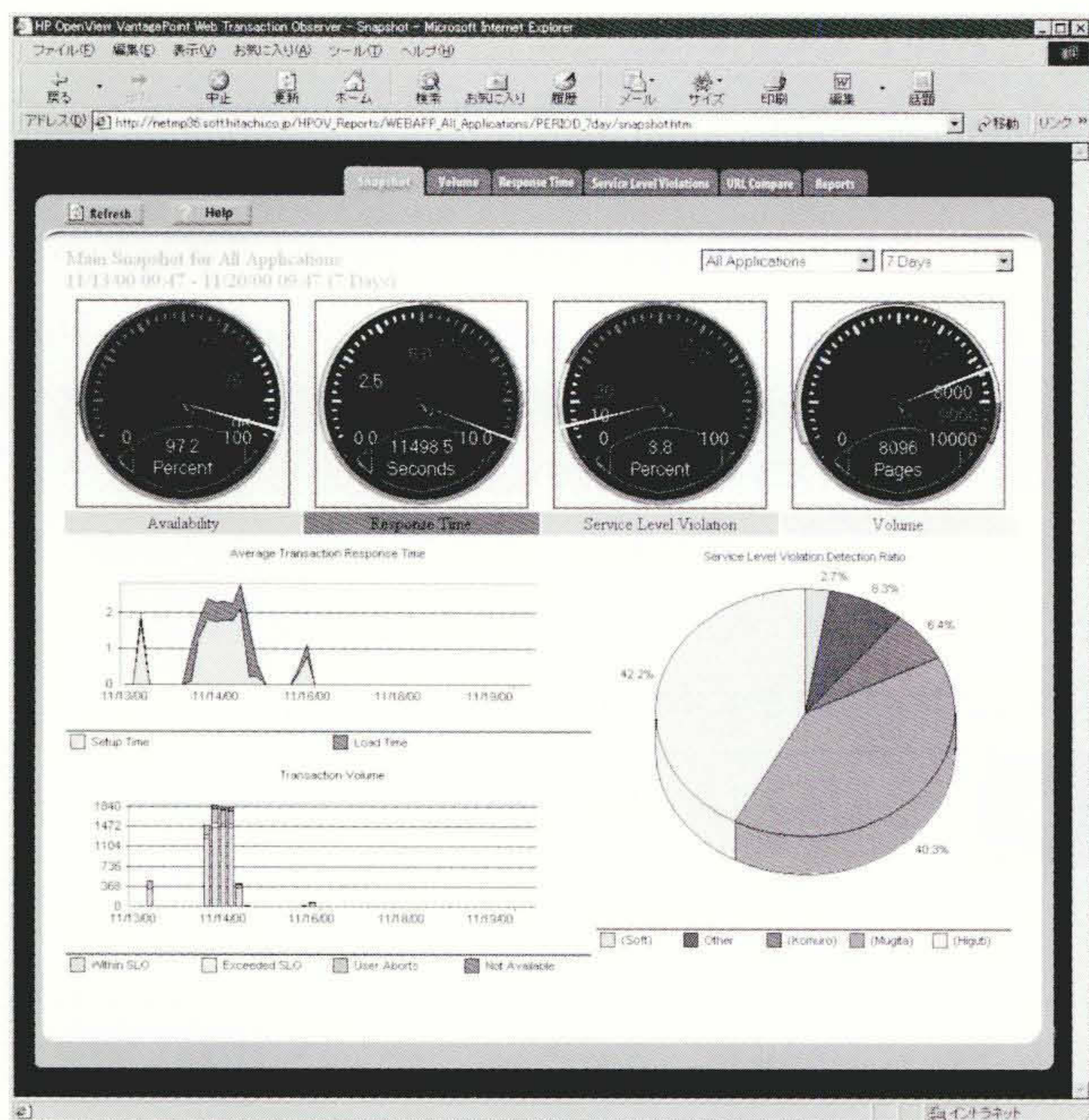


図3 ウェブサイトのパフォーマンス測定画面例
グラフィカルな画面でボトルネックの分析などができる。

のくらいの時間とどまっていたかなどを測定をすることにより、ウェブサイトの性能のボトルネックを検出し、ウェブサイトの性能改善を行うための情報を提供する(図3参照)。

5.2 インターネットサービスの性能管理

この機能では、インターネットサービス利用者の視点から見たインターネットサービスの性能を監視し、ISP (Internet Service Provider) や情報システム部門が提供する各種インターネットサービスがSLA (Service Level Agreement) に基づいて行われているかを検証するための情報を提供する。これを実現するためには、インターネットサーバの性能ではなく、以下のサービスの性能を監視することによって行う：HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3), NNTP (Network News Transfer Protocol), DNS (Domain Name System), FTP (File Transfer Protocol), ICMP (Internet Control Message Protocol), LDAP (Lightweight Directory Access Protocol), DHCP (Dynamic Host Configuration Protocol), IMAP (Internet Message Access Protocol), TCP (Transmission Control Protocol), NTP (Network Time Protocol) など

6 おわりに

ここでは、インターネットビジネス時代に対応し、iDC・ASPなどのためにネットワーク管理やセキュリティ管理、サービスレベル管理などを強化した“JP1 Version 6i”について述べた。

今後は、グローバルビジネスの時代に向けて、異種システムとの連携や管理がますます重要になってくる。新世紀は、ビジネスとの一体化だけでなく、複数の企業が一体となって、統合された情報システムを作る時代でもある。

日立製作所は、新世紀に向けて、“Business Quality Management”をキーワードに、新しい運用管理製品やサービスを提案していく考えである。

参考文献

- 1) 大矢，外：統合システム運用管理“JP1 Version 6”—ASPやデータセンターなどの運用管理を支える技術—日立評論，2000-9増刊，7～12(平12-9)

執筆者紹介



平 林 元 明

1980年日立製作所入社，システムソリューショングループソフトウェア事業部 システム管理ソフトウェア本部 システム管理ソフト設計部 所属
現在，統合システム運用管理“JP1”の事業推進に従事
情報処理学会会員
E-mail: hirabaya@itg.hitachi.co.jp



大 矢 雅 章

1984年日立製作所入社，システムソリューショングループソフトウェア事業部 システム管理ソフトウェア本部 システム管理ソフト設計部 所属
現在，統合システム運用管理“JP1”の事業推進に従事
E-mail: ohya_m@itg.hitachi.co.jp



高山聡一郎

1986年日立製作所入社，システムソリューショングループソフトウェア事業部 システム管理ソフトウェア本部 ネットワーク管理ソフト設計部 所属
現在，セキュリティ関連製品の事業推進に従事
E-mail: taka_so@itg.hitachi.co.jp



佐 藤 俊 夫

1984年日立製作所入社，システムソリューショングループソフトウェア事業部 システム管理ソフトウェア本部 ネットワーク管理ソフト設計部 所属
現在，ネットワーク管理製品の事業推進に従事
E-mail: sato_to@itg.hitachi.co.jp