拠点マネージャ

広域化，大規模化したネットワークでは，1台の統合監視マネージャで直接すべてのネットワークを管理していては，増大するネットワーク管理の負荷に耐え切れません。このような場合には階層型分散管理が有効で，拠点マネージャを配置して階層型の分散管理形態をとる必要があります。拠点マネージャは，統合監視マネージャに代わって各拠点ネットワークの定期的な監視を行い，障害通知をフィルタリングすることで，重要なトラップだけを統合監視マネージャに中継します。これにより，ネットワーク管理のためのトラヒックが抑えられ，効率的な管理が行えます。このように階層型の分散管理形態をとる場合には幾つかの拠点ではオペレーターを確保できないことも考えられますが，拠点マネージャではGUI操作を行わない無人運転が可能なことから，オペレーターなしの拠点も含めた階層型分散管理が行えます。

セキュリティポリシー

企業の情報資産を適切に保護するための，その企業の統一された基本方針のことです。どのような情報リソースを保護の対象とし，どのような行為を不正アクセスと見なすか，また万が一，情報の漏えいや改ざんがあった場合はどう対処するかなどの方針を，各企業が包括的に規定した文書を指します。システム設計や構築は，セキュリティポリシーに従って行われます。運用もセキュリティポリシーに従います。セキュリティポリシーを作らずにセキュリティ製品を導入しても，目的のない単なる対症療法でしかありません。また，運用に入った後も，システムのセキュリティが頻繁に侵害される場合には，セキュリティポリシーの一部を変更して制限を厳しくするなど，システムの目的や状況の変化に応じて，セキュリティポリシーの見直しや修正を継続的に行っていく必要があります。

ファイアウォール

元来は「防火壁」のことで，組織内部のローカルなネットワークと外部のインターネットとの間に，外部からの不正なアクセスを防ぐ目的で設置されるルータやサーバなどを指します。ファイアウォールでは，内外からの通信パケットをすべて捕そくし，パケットを通過させたり，禁止したりすることによって必要なサービスだけをユーザーに提供し，セキュリティを確保します。必要なサービスだけを通過させる方法として，アプリケーションからの操作を中継する「アプリケーションゲートウェイ」や，IPヘッダに含まれているポート情報などを基に通信を制御する「パケットフィルタリング」などの方式があります。

ストレージバーチャリゼーション

専用サーバによって複数メーカーの多種類のストレージ装置を仮想的に一つの大きなストレージプールとし，一元管理することにより，ストレージ資源を有効利用する技術です。業務サーバに論理ボリュームを割り当てる方式が一般的です。

DMZ

Demilitarized Zone(非武装中立地帯)の略で，インターネットなどの外部ネットワークと社内ネットワークなどの内部ネットワークとの中間に位置し，二つのファイアウォールによって隔離された区域を指します。

DMZには，ウェブやDNS(Domain Name System)，FTP(File Transfer Protocol)などの外部に公開するサーバを配置します。そのように配置することで，一段目のファイアウォールによって外部からの不正なアクセスを保護でき，もし公開したサーバが乗っ取られたとしても，内部ネットワークにアクセスするには，さらに二段目のファイアウォールがあるため内部ネットワークまで被害が及ぶことはなくなり，安全性が高まります。一つのファイアウォールとなるマシンにネットワークインタフェースを三つ装備し，外部ネットワークとDMZおよび内部ネットワークを接続する構成もあります。

IPv6

Internet Protocol Version 6の略で，現在標準的に使用されているIPv4(Internet Protocol Version 4)の次期バージョンのプロトコルです。インターネットの急速な普及により，IPアドレスの不足を解消するために作られました。IPv4は32ビットで，最大43億のアドレスが利用できますが，IPv6では，128ビット

のアドレス空間を持ち，1兆の1兆倍のアドレスの利用が可能になります。このため，家電製品をはじめとするさまざまな機器に固有のアドレスを付加することができるようになり，ネットワーク上での管理が可能になります。

e/Eビジネス

“e”は電子商取引という意味のelectronic businessのことであり，“E”は既存の企業（Enterprise）内のマーケティング部門や決済部門などの基幹系業務のIT化を意味するenterprise businessのことです。e/Eビジネスは，ネットワークによるノウハウ・知識の蓄積と活用を行うナレッジマネージメントなど，eビジネスとEビジネスを融合したビジネスを意味します。

MSP

Management Service Providerの略で，顧客システムの運用管理業務を担う事業者を指します。主に顧客システムの障害・稼動監視や障害時の復旧支援，定期的な稼動報告などを行うことにより，顧客システムの安定稼動とTCO（総経費）削減を図るのが目的です。通常は，データセンターを利用したホスティングサービスとセットで提供する場合と，ホスティングを行わずにリモート監視だけを行う二つの提供形態があります。

監視対象はMSP事業者によって大きく異なり，情報基盤部分にとどまらず，業務アプリケーションやセキュリティ，IT資産まで範囲を広げてサービスを提供するケースもあります。

NAT

NAT（Network Address Translation）は，社内のプライベートアドレスとグローバルIP（Internet Protocol）アドレスを相互に変換する機能です。グローバルIPアドレスはインターネット上ではユニークなIPアドレスですが，世界中のネットワーク機器にユニークなIPアドレスを割り振ることができないため，社内など組織内のネットワークでは一般的にプライベートアドレスを用いています。NATを利用することで，社内のネットワーク機器から透過的にインターネットにアクセスすることができます。

SAN

SAN（Storage Area Network）は，磁気ディスクや磁気テープ装置などのストレージ機器をLANから切り離し，ファイバチャネルという高速通信技術で接続した，ストレージ専用のネットワークです。従来はLAN上に分散したサーバ1台ごとにストレージが接続されていたので，データ共用が困難なうえ，バックアップなどで大容量のデータを転送する際にLANの帯域を占有してしまうことや，管理費がかさむなどの問題がありました。

SANでは，サーバやバックアップ装置へのデータ転送に高速な専用ネットワークを使用するので，LANへの負荷が軽減されます。また,複数のサーバがどのストレージへもアクセスできる構成とすることによってデータが共有でき，さらに，ストレージを1か所に集中して管理することでコストを削減できるという長所があり，需要が急速に高まっています。

SNMP

Simple Network Management Protocolの略で，TCP/IP（Transmission Control Protocol/Internet Protocol）の簡易ネットワーク管理プロトコルです。SNMPは，IETF（Internet Engineering Task Force）で仕様が標準化されています。ネットワークの構成情報や障害情報などを収集することができ，ネットワーク機器の監視や各種設定を行うために用いられます。

SNMPゲートウェイ

広域化したネットワーク環境でインターネットを経由する場合，統合監視マネージャと拠点マネージャとの間にファイアウォールを挟むことが想定されます。そのようなネットワーク構成に対しても，SNMP（Simple Network Management Protocol）ゲートウェイ機能により，SNMPパケットをカプセル化して通すことで，ファイアウォールのセキュリティを保持したまま，離れたネットワークを管理することができます。また，SNMPゲートウェイ機能では，それぞれの拠点がアドレスの重複する複数のプライベートネットワークで構成しているので，NAT（Network Address Translation）でアドレス変換されていても，一つのマネージャで統合的に管理することができます。