IT資産／セキュリティ統合管理システム ManagementCore®の開発

杉本恵俊*・金子博之・水谷　功
吉江信夫

Development of Integrated System for IT Asset/Security Management “ManagementCore®”—— by Shigetoshi Sugimoto, Hiroyuki Kaneko, Isao Mizutani and Nobuo Yoshie —— The demand to manage computers as enterprise information asset has further increased with the recent rise in awareness of corporate compliance and information security. The authors have developed “ManagementCore®/IT Asset Management”, a management system software that provides comprehensive support to various missions, ranging from network management to security management. This product is an amalgam of Sumitomo Electric’s software agent technology cultivated while developing network management software, and is a true all-in-one system that maximizes operation management efficiency with its extensive controlling functions. These functions include inventory management for managing computers as IT asset, patch management indispensable for securing security, license management for preventing unauthorized copying, PC operation log recording and external device management for preventing information leaks, quarantine to restrict access to corporate network resources by unauthorized PCs, and statistical reporting for efficient management of these functions.

1. 緒　言

近年オフィスにおいては、コンプライアンス重視や情報セキュリティ意識の高まりに伴い、業務と共に生成される各種情報に対し、資産として管理する要求が一段と高まってきている。当社はネットワーク管理ソフトウェアの開発で培った独自のエージェント※1技術を基に、ネットワーク管理からセキュリティ管理までのIT資産情報を統合的にサポートする管理システム「ManagementCore®/IT資産管理」の開発を行った。

特に本システムでは、運用管理の効率化を最大限に引き出す真のオールインワンを目指し、

・コンピュータやネットワーク機器などの所在や構成の台帳管理を行う、IT資産管理の基本機能とも言えるインベントリ※2管理。
・コンピュータの基本ソフトの脆弱性をなくして組織のセキュリティを維持、運用するためには必須のパッチ※3管理。
・ソフトウェアの不正コピーを防止し、正規購入ライセンスとの対応付けを行うためのライセンス管理。
・不正なコンピュータ操作による情報漏洩を防ぐためのPC操作ログ／外部デバイス管理や、不正PCの社内ネットワークへの接続を抑制するためのネットワーク検疫※4。
・これらの管理を効率的に行うための統計レポート。

といった豊富な管理機能を搭載するとともに、次のような特徴を有している。

・PC、ネットワーク機器、什器といったIT資産情報を一元管理することが可能。
・1億件のログを数秒で検索することができる抜群の検索性能。
・1つのサーバで5万台のPCの監視ができる高いスケーラビリティ。
・操作範囲をユーザごとに制限する機能の搭載。
・クライアントPCへの負荷を極小化するなど運用を重視した設計。
・信頼性の高いセキュリティ機能の実現。
・Webブラウザ画面での直感的な操作が可能。

2. 開発の背景

ManagementCore®/IT資産管理は汎用管理プラットフォームのManagementCore®上に構築している。ManagementCore®は**図1**に示す通り、LAN（Local Area Network）の管理システムであるDr_Net®の後継として当社で完全自社開発し、LANのみならずキャリア通信網、ADSLといった特定の通信機器管理、FDDI光ファイバの芯線管理※5といった幅広い管理に応用できる基盤システムとして、これまでに約1600システムが納入されている。

2003年に当社内でソフトウェアのライセンス管理のニーズが高まり、ManagementCore®上での開発が決定した。翌2004年にはManagementCore®/IT資産管理として外販を開始した。IT資産管理の競合製品は多数あり、その起源から

分類すると、ネットワーク管理、資産管理、セキュリティ管理に分かれるが、ManagementCore®/IT資産管理は、このようにネットワーク管理を基盤とする最も長い歴史を有する製品に分類される。

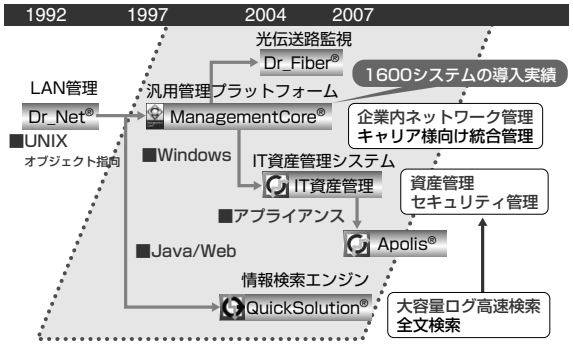

図1　ManagementCore®の歩み

3. IT資産管理

ManagementCore®/IT資産管理は、ManagementCore®で培ったエージェントに基づく機器情報の収集の仕組みを、IT資産情報の管理に応用した製品である（**図2**）。また、**図3**に示すように、ネットワーク管理をベースに、インベントリ管理やライセンス管理などのIT資産情報の管理、セキュリティパッチの管理など情報漏洩対策、そして不正接続を防ぐためのネットワーク検疫といった、組織のあるべき資産状態を実現するためのシステムである。このためシステムの機能は多岐に渡り、壮大なハイアラーキーを構成している。次節以後にその全容を説明する。

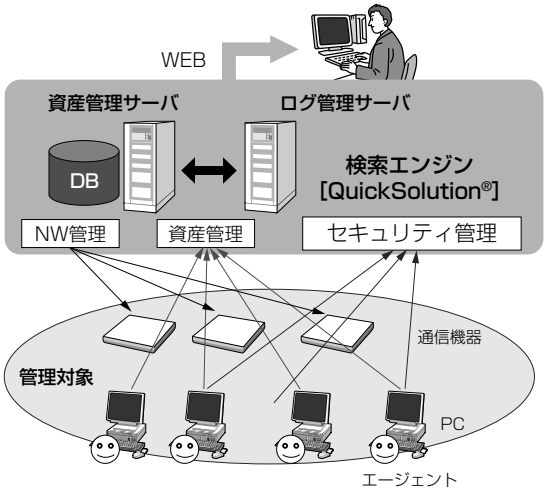

図2　漏れのない機器情報収集

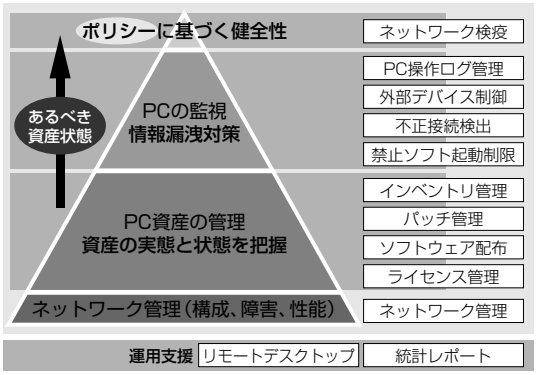

図3　情報資産管理階層

3－1　ネットワーク管理　ManagementCore®/IT資産管理ではManagementCore®が有するネットワーク管理機能を拡張しており、ネットワーク管理装置として利用することができる。SNMP(1)※6というIETF※7のRFC※8で規定された、その名の通りのシンプルな通信プロトコル※9を使用し、スイッチ※10やルータ※11など各種のネットワーク機器の構成、障害、性能といった管理機能を実現している。

SNMPによるネットワーク管理においては管理対象の通信機器にエージェントと呼ぶ小さなプログラムを搭載し、エージェントが採取する各種情報をネットワーク経由で管理装置に収集する。このエージェントが管理している通信機器の情報をMIB※12といい、機器ごとに取得できる情報を定義できる柔軟な構造を持っている。

さらにディスカバリ※13と呼んでいるオンライン機器探索機能を使うことで、ネットワークに接続されている通信機器やPCを検出し、管理することができるので、管理者は新たにネットワークに接続された機器の確認や既存機器の利用状況の把握を、洩れなく容易に管理することができる。

3－2　インベントリ管理　管理対象のPC端末のハードウェア情報やソフトウェア情報を総称してインベントリと呼ぶ。システム管理者はどのような機器、什器があるのか、資産契約情報との関連、ウィルス対策状況などを一括管理する事でセキュリティリスクを正しく把握することができる。

ManagementCore®/IT資産管理は管理対象PCのインベントリをエージェントソフトを使ってサーバに収集するという方法により、確実に資産情報を管理することができるようになっている。各エージェントにはエージェントIDという一意の番号が振られており、収集されるインベントリはエージェントIDと共にサーバに集められ、データベースに格納される。エージェントIDに基づきデータを収集、管理することでホスト名※14、IPアドレス※15、MACアドレス※16などが変更されても、あるいはデュアルブートPC※17や仮想環境※18であっても一意に追跡することができる。また1台の管理対象からは少なくとも1日1回定期的に10Kバイト程度のインベントリが集められるので、大規模な組織で

は相当なデータがサーバ上に集められることになり、効率的な処理が必要となる。ManagementCore®/IT資産管理は、エージェントがインベントリを送信するタイミングをスケジュールするなどして、サーバの負荷を分散させるようにしている。

さらにエージェント間で親子関係を設定することで負荷分散を実現する機能も提供している。専用の中継サーバが不要であり、直接ManagementCore®/IT資産管理サーバと通信できないPCであっても、親子関係を使用してサーバにデータを収集する、もしくはファイルを配信することが可能になっており、組織内のさまざまな端末が持つ膨大な機器情報を業務ネットワークに余分な負荷をかけることなく集配信することができる。

３－３　セキュリティパッチへの対応　セキュリティ意識の高まりと共に、インベントリのなかで各PC端末のOS※19に適用されているセキュリティパッチ情報が重要な意味を持つようになってきた。1台のパッチ未適用PCによってネットワーク全体がコンピュータウィルス※20や情報漏洩の危険にさらされるということが現実に発生している。Microsoft WindowsはWindowsUpdate機能※21により自動的にセキュリティパッチを適用する仕組みを提供しているが、WindowsUpdateが必ずしもセキュリティパッチのみを配信しているわけではないこと、WindowsUpdateの自動更新によってOSが起動しなくなるなどの問題が発生したこともあり、自動更新の機能を各PCの管理者が停止させていることも珍しくない。組織によってはWindowsUpdateの自動更新の機能の禁止をしているところすらある。

ManagementCore®/IT資産管理では管理者がWindows Updateの最終更新日、適用済みのHotfix※22番号、適用日時を確認することができ、またレジストリ※23情報だけでなくファイル単位でのパッチの適用確認をしているので、不足している未適用パッチが、各端末が適切な状態で運用されているのかを監視することができる。さらに必要なHotfixが未適用の端末に対して、ソフトウェア配布機能を使って強制的に適用させることも可能であり、ネットワーク内のセキュリティレベルの維持に有効である。

３－４　ソフトウェアライセンス管理　コンプライアンスの視点からすると使用するソフトウェアのライセンスを購入することは当然であるが、現実には使用するソフトウェアと保有しているライセンスをきちんと対応付けて管理することは、管理者にかなりの負担をかけることになる。

ManagementCore®/IT資産管理では使用しているソフトウェアの名前やバージョンはインベントリとして自動的に収集することが可能であるが、例えば同じMicrosoft Wordであってもバージョンやライセンス形態、パッチの適用具合によってソフトウェアの名称は様々なバリエーションが存在する。このためこうしたバリエーションを一つにまとめて同一のソフトウェアとしてカウントし、ソフトウェアごとの使用ライセンス数を数えることが現実的である。ManagementCore®/IT資産管理では、**写真１**のようにソフトウェアカタログという概念を導入し、バージョンの違いだけといった類似名称のソフトウェアをひとまとめにし、この単位で管理方針を指定できるようにしている。またボリュームライセンス※24など購入しているライセンスは必ずしもPC端末に対応づくものではないため、部門単位での使用ライセンス数と購入ライセンス数の管理、割当、残数管理が必要になる。ManagementCore®/IT資産管理は、不正コピーに対抗してどのPCがどのライセンスを使用しているか把握するための紐付け機能、使用者単位に集計が必要なユーザライセンスやPCに情報を持たないクライアントライセンスなど幅広くライセンス管理をする機能を持っている。こうした機能により適切なライセンス管理を行うことが可能となる。

写真１　ソフトウェアカタログ

３－５　操作ログ管理　個人情報や機密情報など外部に漏洩することにより、企業の社会的信用は大きく失墜する。残念なことにこうした情報の漏洩は組織内部の人間によって故意にあるいは無意識的になされる事が殆どであり、モラルの向上を謳うだけでは防ぎきれないのが現実である。ManagementCore®/IT資産管理では個々の端末にインストールされたエージェントがユーザによる様々な操作のログを収集し、サーバで蓄積、管理する機能を提供している。

操作ログはファイルのコピーやプログラムの起動、デバイスの接続などオペレーティングシステムの機能に介入して採取し、日々管理サーバに送付している。こうしたログの量は例えば500台程度の端末を持つ組織の場合で1週間に約1千万件にも上る膨大なものである。こうした大量の操作ログを効率的に検索を行うため、ManagementCore®/IT資産管理では住友電工情報システム㈱製のQuickSolution®という類似情報検索※25エンジンを組み込んでいる(2)。1億件のログを数秒で検索できるというQuickSolution®により、大量の操作ログの中から短時間で目的のログを見つけ出す

ことが容易になっている。過去のログをバックアップから戻して高速検索することも可能であり、定常的な監査にも有効である。

３－６　デバイス制御　操作ログの採取からさらに踏み込んでManagementCore®/IT資産管理では、外部デバイスの制御機能も提供している。ここで主な対象となるのはUSBメモリ※26に代表される持ち出し可能な外部記憶デバイスである。

こうしたデバイスは組織内部の重要な情報を故意に漏洩させる際に使用されるだけでなく、物理的に離れていて、しかもネットワークでは直接アクセスできないPC間での情報の配布のためにも使用されるが、その中で紛失、盗難などの不可抗力によって情報漏洩を引き起こす点において特に慎重に扱う必要がある。人による扱いが容易なこうしたデバイスの利用は規則だけでは抑制が現実には困難であり、システム側がこうしたデバイスの利用に対して歯止めをかける必要が出てくる。ManagementCore®/IT資産管理ではUSBメモリ、リムーバブルディスク※27といった外部デバイス毎に、接続の禁止やファイルのコピー／参照の禁止など、事前に管理者が設定した制御ポリシーに従って動作を制御する機能を提供している。さらにWinny※28など不適切な利用の恐れのあるソフトウェアの起動を禁止する機能もあり、これらによって、情報の漏洩を抑制する環境を提供している。

３－７　ネットワーク検疫　内部統制ニーズが強まる中、社内のセキュリティポリシー※29に不適合な機器を自動的にネットワークから切り離す、ネットワーク検疫が注目を集めている。ManagementCore®/IT資産管理では各端末にエージェントソフトをインストールしている事を利用し、例えばアンチウィルスソフト※30のパターンファイルが最新であるかどうか、スクリーンセーバ※31が設定されているかどうか、といった管理者が定めた検疫ポリシーに沿ってエージェントが各端末の検疫チェックを行い、検出した検疫ポリシー違反端末や、そもそもエージェントソフトがインストールされていない端末をネットワークから隔離する機能を提供している。端末をネットワークから切り離すには、**図４**に示すように、認証機能を有した認証スイッチや、

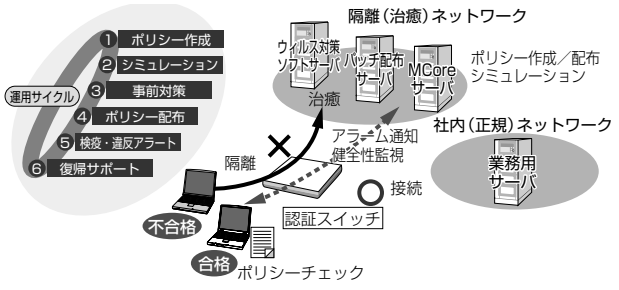

図４　ネットワーク検疫

IPゲートウェイ※32と言われる専用機器と連携する必要があるが、既存のネットワーク設備の変更を嫌う顧客は多い。このため、新たにManagementBox®（**写真２**）という簡便なネットワーク検疫装置の自社開発を行った。ネットワーク上につながった機器間の通信を行う場合、通信相手のIPアドレスをEthernet※33の機器アドレス（MACアドレス）に変換した上でEthernet上に流されるが、初めて通信を行う時点では相手のIPアドレスに対応するMACアドレスは不明な状態にある。通常はEthernet上のブロードキャストを使ってMACアドレスの問合せにより解決を行う。この一連の手続きはARP(3)※34というプロトコルで定義されている。ManagementBox®はEthernet上のARPパケットを監視し、エージェントが保持している検疫ポリシーを参照して、もし不適合な機器を検出した場合、隔離対象機器が関わるARPプロトコルによるアドレス解決※35に介入し、通信不能にする機能を提供している。既存のネットワークのスイッチの1ポート※36にManagementBox®を接続し、管理画面で必要な設定を行うだけで、ネットワーク構成を変更することなく検疫を行うことができるという手軽さと、ManagementBox®1個あたり20万円弱という低コスト性により、容易に導入することを可能としている。

写真２　ManagementBox®

３－８　統計レポート　IT資産の管理を行う上で日毎、月毎といった定期的な報告は、状況の適切な把握と変化への対処のための重要なベースラインとなる。しかしながら膨大な管理データの取りまとめ、整理は管理者への大きな負担となることを避けられない。ManagementCore®/IT資産管理はレポート機能により、PC稼動レポート、セキュリティレポート、ソフトウェアライセンスレポート、アラームレポートなど目的に応じたレポートを出力することにより、管理者の負担の軽減を図っている。多彩なグラフィカルな表現により素早く状況や問題の把握が可能で、各種サマリや履歴情報により変化や割合の分析も可能になる。ソートによる柔軟なベスト／ワースト表示、各種機能

と連携したドリルダウンなど管理者にとってより効率の良い運用管理を支援している。

特にPC稼動レポートは、PCでの操作の有無を5分単位で収集し、利用頻度の少ないPCや終日電源の入っているPCの抽出、勤惰管理への応用等で活用されている（**写真3**）。

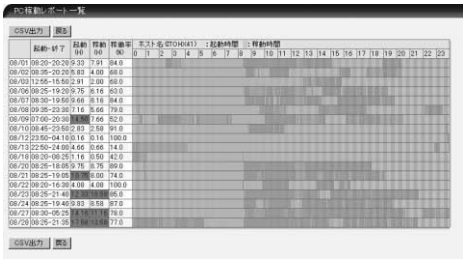

写真3　PC稼働レポート

4. ManagementCore® Apolis®

ManagementCore®/IT資産管理は非常に多機能、高性能であり、そのため主に大規模な企業ユーザを中心に導入が進んできた。しかしながら日本版SOX法※37の施行が始まって従来以上に情報資産の適切な管理が求められるようになってきたこと、セキュリティリスクが必ずしも大企業だけのもので無くなってきたこと等により、中小規模のユーザにおいてもこうしたシステムの導入意欲が高まってきている。こうしたニーズに応えるべく、新たに中小企業向けIT資産管理アプライアンス製品ManagementCore® Apolis®の開発を行った（**写真4**）。中小規模ユーザが専従の管理者を置きづらい点を考慮し、ManagementCore® Apolis®は導入しやすいハードウェア一体型で、機能を絞った見やすい画面、企業や部署のセキュリティ状態を一目で判断できる診断機能といった特徴を有している。

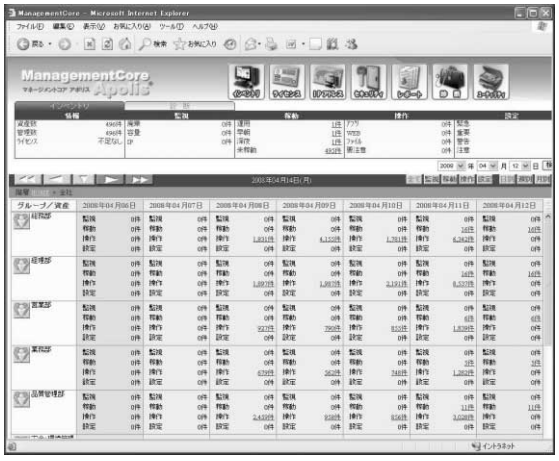

写真4　ManagementCore® Apolis®

5. 結　　言

完全なIT資産の管理、完全なセキュリティはシステムだけで実現できるものではなく、組織が意識的、継続的に取り組むことによって、有効なレベルを維持することが可能となる。管理を厳しくすれば業務効率が落ちるといったトレードオフにならないように、また運用者の負担が大きくならないように、システムがバックアップしていく必要がある。ManagementCore®/IT資産管理はこうした組織に対する手助けとなるよう今後も機能、性能、品質の強化を継続して行く予定である。

用 語 集

※1　エージェント

ユーザーや他のソフトウェアとの仲介的関係において動作するソフトウェアを指す計算機科学上の抽象概念。

※2　インベントリ

企業などで使用されている情報機器の資産情報。コンピュータのハードウェア情報や、ネットワーク機器情報など。

※3　パッチ

コンピュータのプログラムの一部分を更新して欠陥の修正や機能変更を行うためのデータのこと。

※4　ネットワーク検疫

ネットワークに接続した機器がコンピュータウイルスに感染していないか、ネットワークに不正に侵入された形跡はないか等を確認し、該当機器を隔離すること。

※5　芯線管理

通信事業者において通信用のケーブル（光ファイバなど）の個々の線がどことどこを接続しているのかを管理すること。

※6　SNMP

Simple Network Management Protocol：IPネットワーク上のネットワーク機器を監視・制御するための情報の通信方法を定める通信規約。

※7　IETF

Internet Engineering Task Force：TCP/IPなどのインターネットで利用される技術を標準化する組織。

※8　RFC

IETFによる技術仕様の保存、公開形式。

※9　通信プロトコル

ネットワーク上での通信に関する規約を定めたもの。

※10　スイッチ
OSI参照モデルのデータリンク層の情報を基に、フレームの送信ポートを決定し転送するコンピュータネットワーク機器。

※11　ルータ
コンピュータネットワークにおいて、2つ以上の異なるネットワーク間を相互接続する通信機器。

※12　MIB
Management Information Base：SNMPによって管理する情報の表現形式。

※13　ディスカバリ
ManagementCoreがネットワーク上に接続された機器を自動検出する機能。

※14　ホスト名
コンピュータ等ネットワークに接続された機器につけられる名前。

※15　IPアドレス
Internet Protocolに基づくネットワークにおいて、送受信する機器を判別するための番号。

※16　MACアドレス
Media Access Control address：LANカードなどのネットワーク機器のハードウェア固有の物理アドレス。OSI参照モデルの第2層のアドレスにあたる。

※17　デュアルブートPC
1台のコンピュータに2つのOSを組み込み、選択したいずれか一方のOSが起動するようにしたもの。

※18　仮想環境
ハードウェアプラットフォーム上でホストプログラム（制御プログラム）が擬似的なコンピュータ環境を生成し、ゲストソフトウェアに対して「仮想機械」を提供するもの。

※19　OS
Operating System。コンピュータにおいて、ハードウェアを抽象化したインターフェースをアプリケーションソフトウェアに提供するソフトウェアであり、基本ソフトウェアの一種。

※20　コンピュータウィルス
コンピュータに被害をもたらす不正なプログラムの一種。

※21　WindowsUpdate機能
マイクロソフトが提供するWindows関連ソフトウェア、およびデバイスドライバのダウンロードと更新を行う機能。

※22　Hotfix
ソフトウェアに致命的なセキュリティ上の脆弱性など深刻な不具合が発見された場合に、通常のリリース手順を踏まず緊急に発行される修正プログラム。

※23　レジストリ
Windowsの基本情報やソフトウェアの拡張情報などが保存される場所。

※24　ボリュームライセンス
1つのソフトウェア製品に複数の利用権（ライセンス）をまとめて、割引価格で提供する販売形態。あるいはそのライセンス自身。

※25　類似情報検索
キーワードやキーフレーズに対して、完全には一致しないが比較的似ていると思われる文章を検索すること。

※26　USBメモリ
Universal Serial Busを用いてデータの読み書きを行う記憶装置。

※27　リムーバブルディスク
ディスクドライブからディスクを取り出し交換することが可能なディスクドライブ、あるいは当該ドライブに対応したディスク。

※28　Winny
P2Pの技術を利用したファイル共有ソフトの一種。

※29　セキュリティポリシー
情報資産の取り扱いについて定めたルール。

※30　アンチウィルスソフト
コンピュータウイルスを検出・除去するためのソフトウェア。

※31　スクリーンセーバ
コンピュータのコンソールに一定時間ユーザによる入力がなかったとき、ディスプレイを保護するために自動的にアニメーション等を表示させるユーティリティソフトウェア。

※32　IPゲートウェイ
IPの規約に基づき、ネットワーク間を接続する機器。

※33　Ethernet
コンピュータネットワークの規格のひとつで、世界中のオフィスや家庭で一般的に使用されているLANで最も使用されている通信技術規格。

※34　ARP

Address Resolution Protocol：イーサネット環境において、IPアドレスからMACアドレスを得るために用いられる通信規約。

※35　アドレス解決

IPアドレスからMACアドレスを得ること。

※36　ポート

ここではスイッチングハブのケーブルを接続する部分。

※37　日本版SOX法

相次ぐ会計不祥事やコンプライアンスの欠如などを防止するため、米国のサーベンス・オクスリー法（SOX法）に倣って整備された日本の法規制のこと。

参　考　文　献

(1) RFC1157 Simple Network Management Protocol (SNMP). J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin. May 1990.
(2) 武並佳則、岸田正博、田辺泰夫、「エンタープライズサーチ･エンジンQuickSolution®の開発」、SEIテクニカルレビュー第172号（2008年1月）
(3) RFC826 Ethernet Address Resolution Protocol：Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware. David C. Plummer. November 1982.

執　筆　者

杉本　恵俊*：住友電工システムソリューション㈱　ネットワークシステム事業部　技術部長
金子　博之：住友電工システムソリューション㈱　ネットワークシステム事業部　営業部　主査
水谷　　功：住友電工システムソリューション㈱　ネットワークシステム事業部　営業部長
吉江　信夫：住友電工システムソリューション㈱　ネットワークシステム事業部　部長

＊主執筆者