管理番号＃１８－２０２

平成２０年度
成果報告書

移動端末を安全に管理できるスケーラブルな
次世代イントラネット端末接続管理技術の研究開発

委託先：　㈱サイバー・ソリューションズ

平成２１年４月

情報通信研究機構

平成２０年度　成果報告書

（地域中小企業・ベンチャー重点支援型）

「移動端末を安全に管理できるスケーラブルな
次世代イントラネット端末接続管理技術の研究開発」

目　次

1　研究開発課題の背景

近年のウィルス感染や情報漏洩事件の多くは、外部からの巧妙な侵入等ではなく、組織的な管理を離れた移動端末を経由している。そのため情報の出入り口としての端末接続管理の重要性が増している。

安全な企業内/組織内ネットワークを実現するために、端末が移動することを前提とした次世代のイントラネット端末管理技術を研究開発する。セキュリティの確保には、端末の接続管理などの内部ネットワーク（イントラネット）のセキュリティが鍵となる。特にノート PC などの移動端末は、情報漏洩、外部からのウィルス持ち込みなど、大きなリスク要因となっており、現状では持ち出し、移動を禁じるなどの本来の利便性を無視した運用を余儀なくされている。このことは、現状の技術および資産の活用を阻害しているばかりか、これから到来するモバイル情報社会の大きな障害となっている。

そのような中、イントラネット内の端末接続を監視し、不正な接続を自動的に排除/隔離する技術および製品が登場し、市場での存在感を増している。現在の技術では、特定の端末があらかじめ割り当てられたネットワークに接続することを前提にその接続を監視しており、固定端末を想定したものである。しかし、ノート PC などの個人端末は、人事異動や、新型への置き換え、会議などでのプレゼンテーション、さらには部署を横断する共同業務などの現実的な理由のために、実際には移動している。

現状の端末管理システムは、端末の移動の度に、登録情報の書きかえ、ネットワークアクセスの設定変更などの変更を要求する。企業内で、技術者が、研究所と工場を行き来する場合、移動するためにそれぞれの場所で以前の登録が必要になる。多国籍企業で、日本の営業担当者が海外の事業所を訪れる場合、会社単位を超えて事前に手続きをおこなっておく必要がある。

結果として、現状の技術では、不正な端末の接続を阻止できるが、自由な移動を認められないために、これからのモバイル情報社会に応えられるものとなっていない。

もうひとつの大きな問題は、現在のような端末管理システムは、ネットワークの規模に対してまったくスケールしないことである。端末とその接続可能なネットワークが厳密に関連付けられており、新しくネットワークを拡張するときには、中央の管理システムに新たに登録し、必要な監視体制を拡張しなければならない。組織改変などにより、数百人単位の人の移動があり、ネットワーク構成の変更があった場合、それにともなって登録情報の変更と、ネットワーク変更に合わせた監視システムの再構成が必要となる。このことは、柔軟な拡張と運用が可能なインターネット技術の長所をスポイルしている。

本研究開発では、

端末の移動、およびネットワーク構成の変更を前提にした安全な端末管理技術

を確立し、端末とネットワークの構成変更に対応できる次世代の端末接続管理システムを実現する。

研究開発分野の現状

IP 接続される移動可能な端末の数は増加の一途を辿っており、IT インフラとしてのイントラネットは拡大し続けていることから、この技術範囲の研究開発が急務である。一方で、公衆ネットワークでの移動管理は、MobileIP の実用化研究が進められている。本研究開発では、公衆ネットワークでの移動端末管理ではなく、現在まったく整備されていないイントラネットでの安全な移動端末管理技術を研究開発する。またその技術を公衆ネットワークでも利用できるように MobileIP 技術への適用も可能な技術とする。

2007 年 3 月の WIDE（Widely Integrated Distributed Environment）プロジェクトによる”Mobile IPv6 を用いた IPv6 移動通信サービスの実験運用開始”のアナウンスに続いて、インターネット技術の標準化を議論する IETF（Internet Engineering Task Force）でも IPv6 の配備が本格的に開始されることがアナウンスされた。

全体として、本文やの現状は、移動体に関する研究分野や、基礎的な研究の段階から、具体的なサービスを踏まえた実用化の時期に差し掛かり、本研究開発提案時の期待通り、世界的な動きも加速しつつあるといえる。

一方で市場の状況は、当初の予想通り活性化が進んでおり、その規模も拡大を続けている。本研究開発を通して、機能強化を図ってきた基盤となるイントラネットセキュリティ製品 NetSkateKoban は、平成 19 年度を通して大きく成長し、市場でもその存在感を増している。特に平成 19 年度後半には、無線接続端末だけではなく、パートナー企業から IPv6 対応に関する計画についての具体的な問い合わせをうけるなど、ニーズが顕在化しつつあり、次世代の接続管理技術としての本研究開発の重要性を大きく拡大するものとなっている。

２　研究開発の全体計画

２－１　研究開発課題の概要

ステップ１：イントラネットにおける移動端末の接続管理技術

受け入れネットワークでも移動端末を外部から管理可能とし、所属ネットワークでは、受け入れ先での利用状況を正確に知ることを可能とするために、本研究開発では、管理システム間の通信チャネルを確保する技術を確立する。

移動端末を経由しない、管理システム間の直接チャネルを利用することで、移動端末管理者の自己責任に依存しない、安全な移動端末管理を実現する。図 1に本研究開発の要素技術の構成を示す。

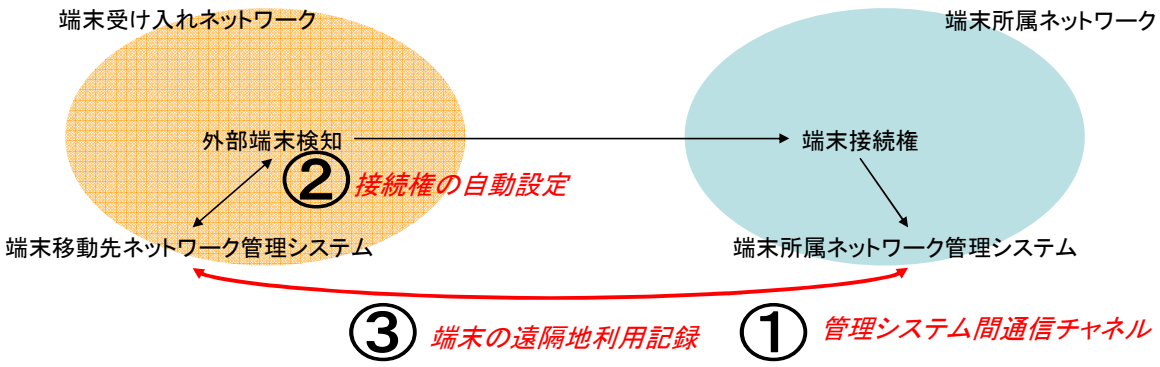


図 1 本研究開発の要素技術構成

ステップ 1 は、以下の 3 つの要素技術から構成される。まず、端末接続時にその所属ネットワークの管理システム情報を抽出し、管理システム間の直接通信チャネルを確立する技術を研究開発し、次にそのチャネルを利用して、移動端末からではなく、その所属ネットワークから得られた情報に基づいて、そのアクセス権に応じた接続を自動的に実現する技術を研究開発する。また受け入れネットワーク側で監視された移動端末のネットワーク利用情報を管理システム間の通信チャネルを利用して送信する技術を研究開発する。

①. **管理システム間通信チャネル構築技術**

②. **移動端末のアクセス権自動設定技術**

③. **移動端末のネットワーク利用管理技術**

ステップ 2：大規模ネットワークにおける移動端末の接続管理技術

端末接続管理の基本機能は、接続を監視するセンサによって実現されている。現在は、このセンサをネットワーク毎に配備し、管理システムに登録する必要があり、ネットワーク構成の変更時にはセンサ配備も再設計が必要となることから、部署毎の登録変更や、大規模ネットワークへの導入が困難になっている。

本研究開発では、このセンサ機能を自動的に配備することを可能とする技術を確立する。センサの機能を利用者の端末に無作為に配備し、自動構成することで、事前の詳細なシステム設計と運用時の厳密な（コストのかかる）システム管理を不要とする。

一方で、自動的に構成され、配備されるセンサは、端末の移動、予期しない障害等によって常に全体の配備状況が変化する。変化するネットワークに追随してシステムを再構築する技術を確立する。図 2に本研究開発の要素技術を示す。

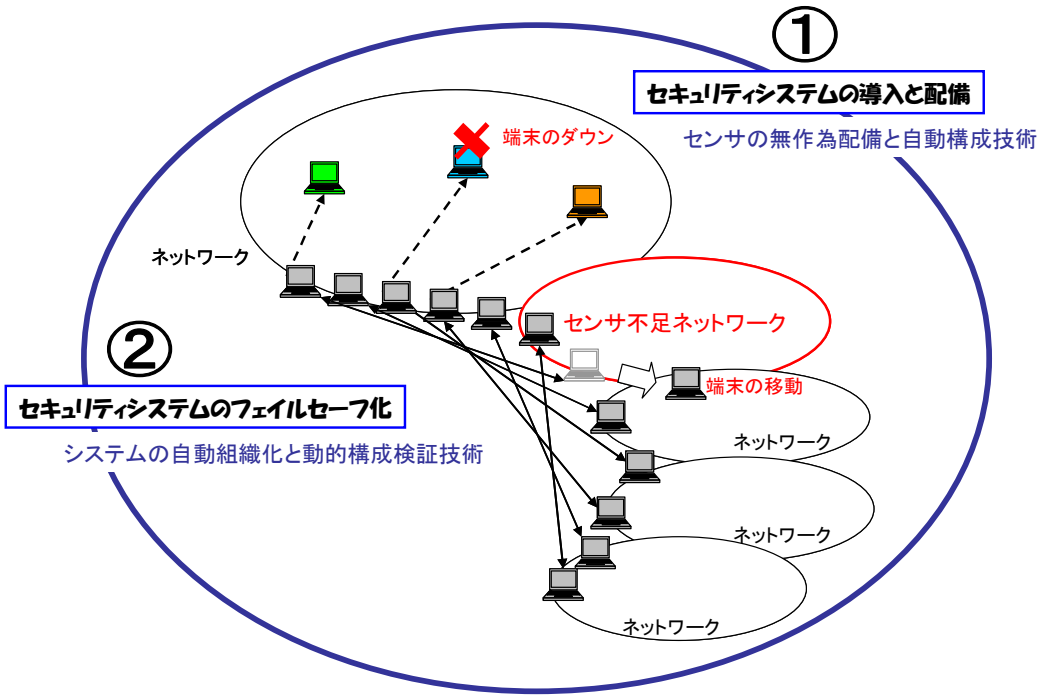


図 2 大規模ネットワークを柔軟に管理できる端末管理システム

ステップ 2 は以下の二つの要素技術から構成される。まず候補となる端末群から、センサとなる端末を自動的に抽出する技術を研究開発する。次に、センサとなった端末を監視し、それらの移動、ダウン時に自動的に他の端末をセンサとする技術を研究開発する。

２－２　研究開発の最終目標（平成 20 年 8 月末）

本研究開発の成果物によって実現される次世代の端末管理システムによって、以下を達成する。

イントラネットにおける移動端末の接続管理技術

- 機能目標
  - 端末をイントラネット内の部局毎に独立して管理可能とする
    会計、営業、研究開発など、本来、異なるポリシによって運用され、業務毎に異なる管理体制、アクセス制御が必要であるが、現在の端末接続管理技術は、それらの業務実態と関係なく集中管理を必須としている。そのことが柔軟な運用と、移動端末の管理を阻害していることから、その解決のために分散管理アーキテクチャを許容する技術の確立を目標とする。
  - 移動端末接続時に、その移動端末の過去の接続履歴を参照可能とする
    移動端末の場合は、その端末が継続的に受け入れネットワークで許容できる管理体制下にあったかどうかが、接続を許可する際に、大きなポイントなる。本機能の実現には、所属ネットワークからの移動端末管理、受け入れネットワークの移動端末検証、両ネットワーク間の安全な通信等の本研究開発の要素技術のすべてが必要となるため、受け入れ側ネットワークで利用できる機能の代表として目標とする。
  - 移動端末のイントラネット内の他のネットワーク利用状況を検証可能とする
    移動端末が、所属ネットワークに戻ってきたときに、再接続を認める際には、端末が移動先でも管理ポリシを遵守していることを、客観的に確認すること必要が

あり、受け入れネットワークの管理システムからの当該端末ではない、第三者のレポートが必要となる。本機能の実現には、所属ネットワークからの移動端末管理、受け入れネットワークの移動端末検証、両ネットワーク間の安全な通信等の本研究開発の要素技術のすべてが必要となるため、所属ネットワークで利用できる機能の代表として目標とする。

- 性能目標
  - 端末から得られる情報を直接管理に利用しない耐詐称端末管理技術を確立する
    端末自身によってのみ管理されている情報は、IP アドレスや、MAC アドレスなどの情報であっても詐称可能であるため、端末接続管理の代表的なセキュリティ上の脅威である成りすまし対策の実現を目標とする。
  - 移動端末の問題をリアルタイムに所属ネットワークに通知する技術を確立する
    受け入れネットワーク管理者は、管理権限等の問題から、問題発生時には当該端末を遮断するしか対応法がない。一方で所属ネットワーク管理は配下の移動端末の問題をリアルタイムで知ることができず、問題発生時の迅速な対応ができない。本研究開発で実現する「端末を常に管理下におく」を実現する代表的機能として目標とする。
- 技術目標
  - 端末へのエージェント搭載の可否に依存しない耐詐称端末管理技術を確立する
    セキュリティの現場では、端末への付加的なプログラムの搭載を許容するポリシと許容しないポリシはそれぞれの現場によって使い分けられており、どちらか一方のみの対応では、潜在的な市場が大きく制限されることから、両者の実装技術を確立することを目標とする。
  - 標準化され、普及した技術のみを活用したアクセス制御技術を確立する
    本研究開発の成果を、実用的にするためには、既存のネットワークでも利用可能とすることが重要となる。そのため専用の機器、ソフトウェアに依存せずマルチベンダ環境での利用を実現できる技術の確立を目標とする。

大規模ネットワークにおける端末接続管理システムの導入・管理技術

- 機能目標
  - 端末接続を監視するセンサの明示的な配備が不要なシステム構成技術を確立する
    センサを配備するために、ネットワーク毎に異なる物理、論理構成にあわせた事前の設定を必要とするアーキテクチャが大規模なセンサ配備を妨げているため、個別の詳細な設定なしにセンサを配備運用できるセキュリティシステムの確立を目標とする。
- 性能目標
  - ネットワーク内のセンサのダウン時に自動的に代替センサを選出する技術を確立する
    本技術開発により、センサの役割を担う端末は動的に変化する。この新しい機能により、センサの不在の状態が起こり得るため、それを防ぐフェイルセーフ実現を目標とする。
- 技術目標
  - 標準化され、普及した技術のみを活用した管理技術を確立する
    本研究開発の成果を、実用的にするためには、既存のネットワークでも利用可能とすることが重要となる。そのため専用の機器、ソフトウェアに依存せずマルチベンダ環境での利用を実現できる技術の確立を目標とする。

２－３　研究開発の年度別計画

（金額は非公表）

研究開発項目	H18 年度	H19 年度	H20 年度	計	備　考
移動端末を安全に管理できるスケーラブルな次世代イントラネット端末管理技術の研究 イントラネットにおける移動端末の接続管理技術 大規模ネットワークにおける端末接続管理システムの導入・管理技術 実証実験	→	→	 → →	－ － －	
間接経費	－	－	－	－	
合　　計	－	－	－	－	

注）１　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の３０％を上限として計上（消費税を含む。）。
　　２　備考欄に再委託先機関名を記載
　　３　年度の欄は研究開発期間の当初年度から記載。

３　研究開発体制

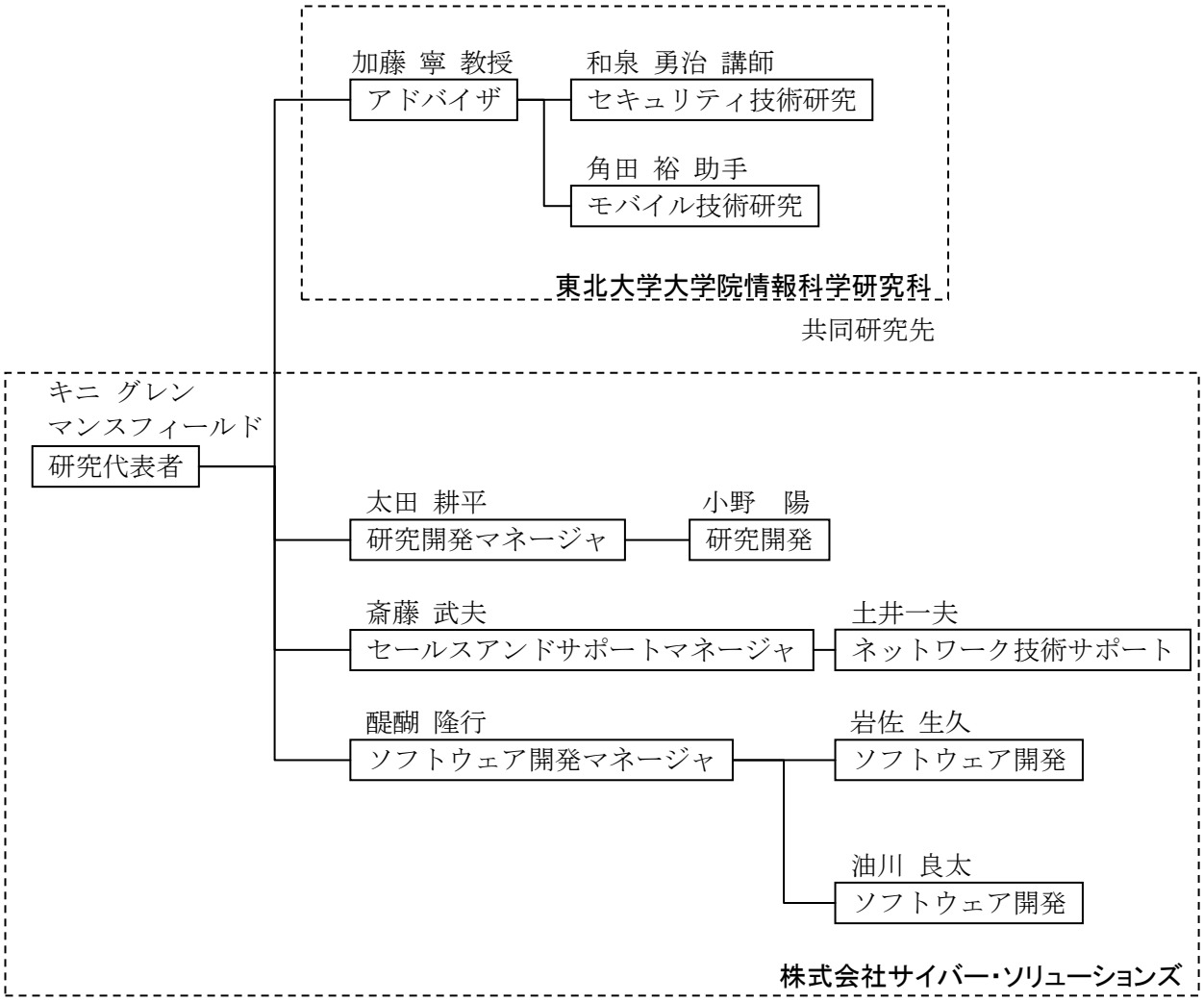
３－１　研究開発実施体制

研究開発は、受託者である株式会社サイバー・ソリューションズを中心に実施し、最先端の技術動向について、適宜、東北大学情報科学研究科の支援を仰ぐ。また実ネットワークを想定した実験環境についても、ノウハウ、実績のある東北大学の設備を活用する。

具体的には、モバイル、動的ネットワーク構成技術（Ad-hoc ネットワーク技術）等の全般的技術動向について、東北大学情報科学研究科の加藤 寧教授のアドバイスを仰ぎ、セキュリティ分析技術について、同研究科の和泉 勇治講師、移動管理技術について、同研究科の角田 裕助手に支援を依頼する。さらに、同研究科の実践的な実験ネットワーク設備を活用して、研究開発した技術を実験的に評価する。

また、事業化パートナーである NTT 東日本-宮城との連携の向上を図り、開発された技術の速やかな市場投入を促進する。

本研究開発の成果を製品化する際のプラットフォームとなる製品を有するサイバー・ソリューションズ社が、端末接続管理、大規模ネットワークでの導入・管理技術を研究開発する。



「大規模ネットワークにおけるセキュリティシステムの自動最適化技術」の研究開発では、太田 耕平、小野 陽が研究および開発のサポートを行い、醍醐隆行、岩佐生久、油川良太がソフトウェア開発を担当する。

「ネットワーク資産の自動発見技術」の研究開発では太田 耕平、小野 陽が研究および開発のサポートを行い、醍醐隆行、岩佐生久、油川良太がソフトウェア開発を担当する。

「実証実験」では齋藤武夫、土井一夫が実証実験環境となるネットワーク技術に関する技術開発およびサポートを担当する。

４　研究開発実施状況

４－１　ネットワーク管理機能のセキュリティ管理への統合の研究開発

４－１－１　ネットワーク管理機能のセキュリティ管理への統合技術の概要

包括的なイントラネットセキュリティ実現のために、ネットワーク管理機能を統合し、従来の未登録端末の発見と排除を中心とした端末管理だけではなく、一般的なセキュリティインシデント、ネットワーク障害に起因するインシデント、さらには明らかな不正ではないが、潜在的な問題であると考えられるネットワーク現象の網羅的な監視を実現する。

本研究開発は以下の 3 つの要素技術を確立し、それらを連係させることで具体的な機能として実現する。

1. （不正）端末のトラフィック、経路制御などのネットワーク活動管理機能
   従来のセキュリティ管理は、侵入検知システムで検知される攻撃や、ウィルスなどの明確な不正を対象としているが、起こりえるあらゆる事態に対応するには「管理」こそが基本となる。本技術開発では、申請者らのもつネットワーク監視技術をセキュリティ管理に統合する。
2. （不正）トラフィック発信元端末の追跡機能
   端末のセキュリティ管理には、問題のある現象を検知するだけでは十分ではなく、その発信元を迅速に特定するとともに、継続的に監視することが必要となる。本技術開発では、既存の端末管理機能と連携することで、特定のトラフィックの発信元を追跡管理する機能を実現する。
3. セキュリティシステム（NetSkateKoban）の状態およびリソース監視機能
   セキュリティシステムは、本来もっとも可用性が要求されるものであるが、これまでは付加的な機能として、対症療法的に利用されている現実もあり、現実の可用性は十分に確保されているとはいえない。本技術開発では、ネットワーク管理分野で確立されている監視機能をセキュリティシステムに統合することで、高い信頼性をもつセキュリティシステムを実現する。

４－１－２　ネットワーク管理機能のセキュリティ管理への統合技術の実施状況

本研究開発によって、これまでは独立し監視を主体としていたネットワーク管理を、その原因となる端末の特定､自動/手動排除､まで全自動でおこなうことが可能となった｡また、システム自身の管理を統合することでセキュリティシステムとしての信頼性を大幅に向上させた。

端末の接続管理に､ネットワーク構成管理機能､トラフィック監視機能の統合を実現した。具体的には、NMS（Network Management Station）モジュールを開発し、既存の研究開発プラットフォームである NetSkateKoban に統合することで、以下の 2 つのこれまで同分野では実現されていない機能を実現した。

1. 組織外への大容量通信などの､不正と断定はできないが情報漏洩などの可能性がある通信の検知と、その即時遮断
2. 狭義にはセキュリティインシデントではないが､その原因となり得る､あるいは未知の攻撃の結果として起こり得るリソース不足､ノードのダウンなどの検知､およびその通知

以下に４－１－１で述べた 3 つの要素技術毎の実施状況を示す。

①（不正）端末のトラフィック、経路制御などのネットワーク活動管理機能

トラフィック監視装置を統合し、端末管理との統合を実現した。管理機能として、すでにある多くの製品や技術を有効に活用できるようにするために、管理情報の収集および、制

御には、インターネット標準の管理プロトコルとして広く普及した SNMP（Simple Network Management Protocol）を全面的に採用した。

端末管理システムである NetSkateKoban に SNMP による管理機能を統合するために、NetSkateKoban に汎用的な SNMP マネージャ機能を実装し、各種の SNMP 対応機器との通信を担う機能を配備することで、特定のベンダに依存しないネットワーク管理機能を統合することを狙う。

図 3にトラフィック監視機能（CpMonitor）を管理機能の一つとして統合した場合の例を示す。本例では、従来は端末を検知することを目的とした「センサ」のみを登録し利用していた NetSkateKoban マネージャに、トラフィック情報を監視する「センサ」を登録するケースを示している。

「1. 登録」によって対象となる監視装置の IP アドレス、インタフェース、および管理上のラベル情報を登録する。NetSkateKoban マネージャは、新たに統合された SNMP マネージャ機能を介して、本登録情報に基づいて「2. 監視」を開始することができる。

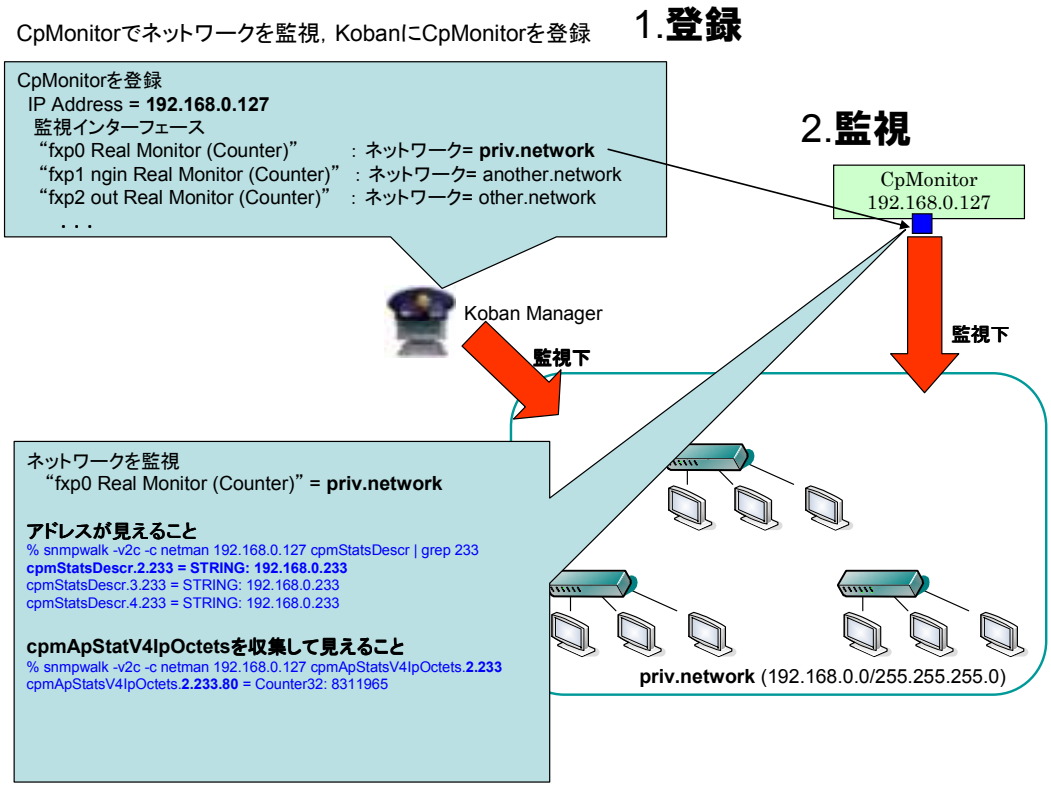


図 3 ネットワーク管理機能の統合

次に、本研究開発によって統合された CpMonitor を運用時に自動的に利用するためのポリシ設定機能の拡張を示す。図 4に本機能統合の概念図を示す。従来は未登録端末検知 → 遮断といった単純なルール設定を基本としていたが、それを拡張し、未登録端末の検知という従来のアクションに加え、その検知後にトラフィック情報を監視し、その状況によってあらためてアクションを選択することを可能とする。

具体的には、遮断等の最終的な対策を定義する「アクション定義」を拡張し「新たなルールを生成する」という動作をアクションとすることで、拡張性のある柔軟な条件を設定することが可能としている。

このような拡張によって、未登録端末検知時にも、それを即座に遮断するのではなく、一定のルールの下での利用を認めつつ、その通信状況に問題があったときに初めて実際の遮断をおこなう、といった高度な利用が可能となる。

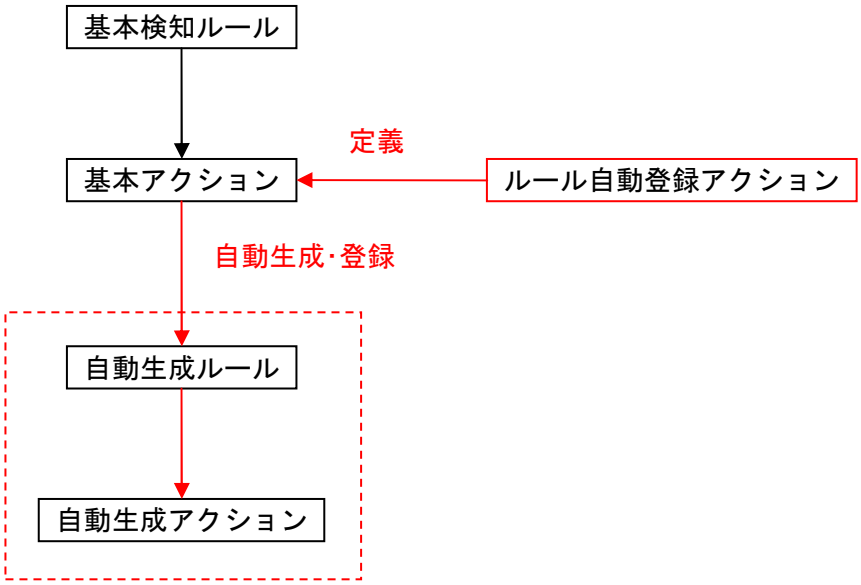


図 4 トラフィック情報に基づくポリシ設定の概要

図 5に上記の開発したシステムでのルール自動登録アクションを実際に適用している例を示す。アクションとして、従来にはなかった「トラフィックルール自動登録」を登録可能となっている。また自動登録されるトラフィックに対する閾値となるルールテンプレートを監視間隔、基準値、重要度で定義する。

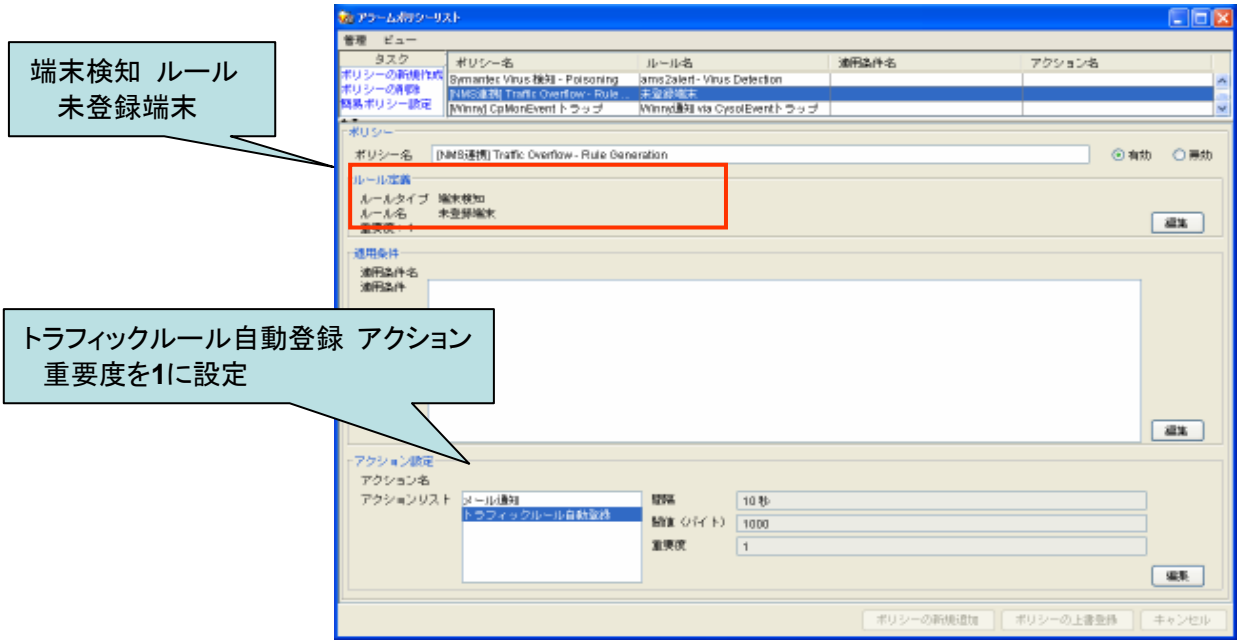


図 5 トラフィックルール自動登録の設定画面例

②（不正）トラフィック発信元端末の追跡機能

従来の端末管理とネットワーク管理機能を統合することで、ネットワーク管理の観点から

みても、従来にはない新しい機能を実現することが可能となった。従来のネットワーク管理は受動的なもので、監視によって問題の発生を検知し、通知することが主な任務となっているが、実際には通知をうけた管理者が具体的な対策をとるまで「管理」はおこなわれないことになる。

本研究開発によって、端末管理機能とネットワーク管理機能を統合し、協調動作させることで、問題を検知した際には、当該端末の遮断や、隔離（後述）といった具体的な対策まで自動的にとることが可能となった。

図 6に端末管理とネットワーク管理の協調動作によるトラフィック発信元端末の追跡機能の概要を示す。図中、赤で示す未登録端末に対して、新たに統合されたトラフィックセンサによって、その端末がどのような通信をおこなっているか（トラフィック情報）を知ることができるようになった（図中、橙）。一方で、図中、緑で示す従来の接続監視センサは、トラフィック情報を監視することはできないが、未登録端末を検知するとともに、その接続情報を取得できる。

本研究開発では、その両センサの協調動作によって、トラフィックセンサによって検知された異常についても、端末監視センサの機能を活用してその発信元を特定することが可能となった。

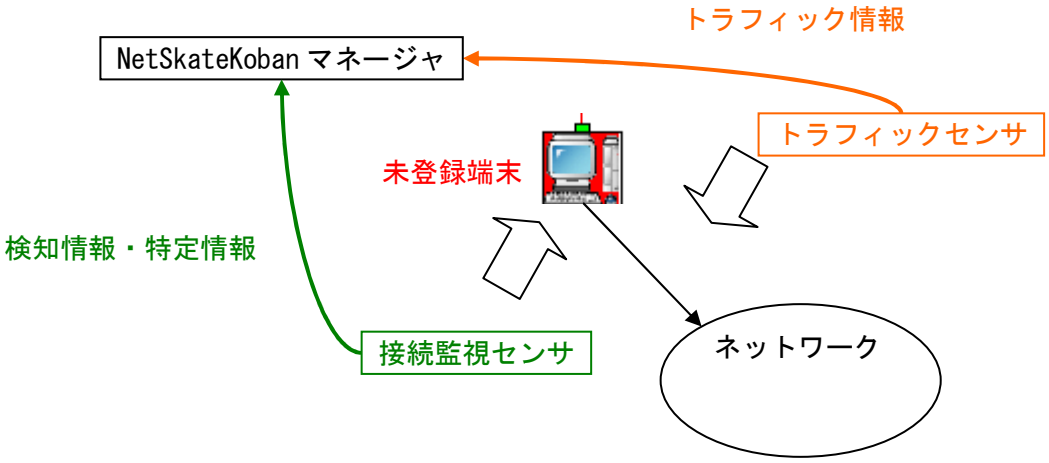


図 6 端末管理とネットワーク管理の協調動作の概要

図 7にトラフィック監視と端末追跡・特定機能の動作例を示す。図中、上部の表の 1 行目は接続監視センサによる未登録端末の検知情報が示されており、MAC アドレス、IP アドレスによって当該端末が特定されている。また 2 行目では動的に生成されたルールによって特定された端末情報とともに、トラフィック監視を開始していることが示されている。これらの動作によって、異常トラフィックの検知時に、その発信元を特定することが可能となっている。

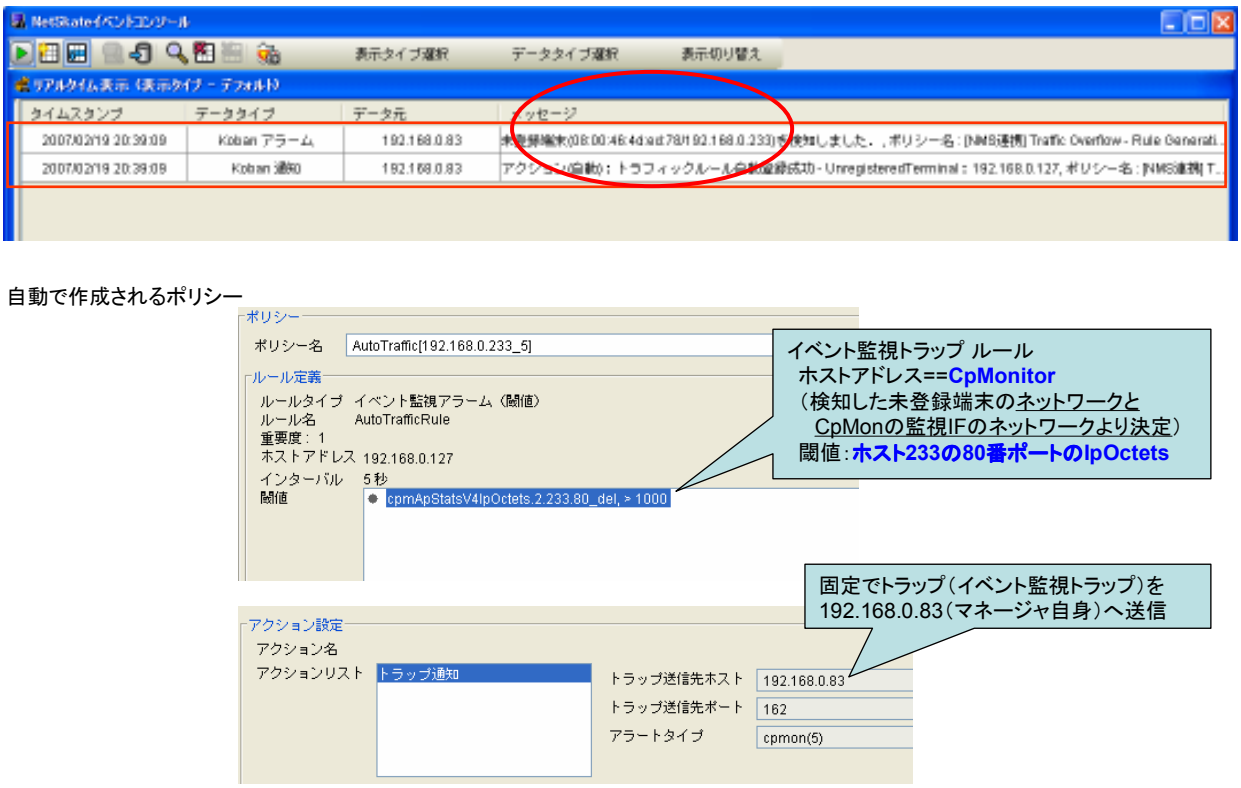
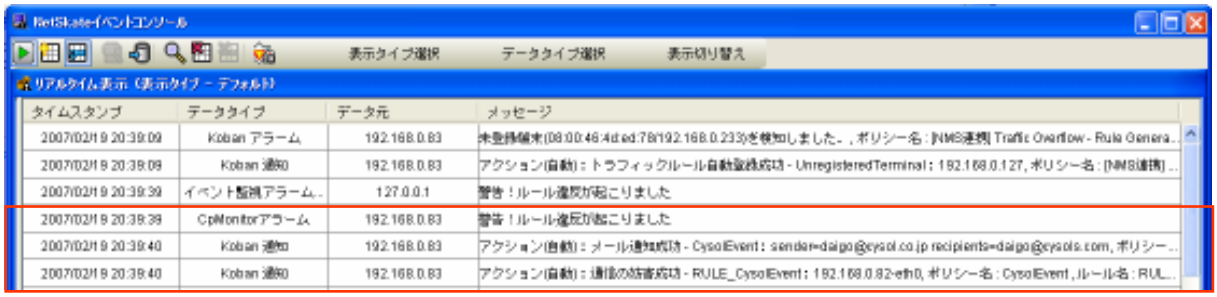


図 7 トラフィック監視と端末追跡・特定機能の動作例

図 8に特定された端末情報を基に、具体的な対策として、通信の妨害（端末の遮断）を実施することができた状況を示している。このことはネットワーク管理と端末管理の融合および連携の大きな成果のひとつであり、ネットワーク管理、端末管理双方にとって以下のようなこれまでにない利点をもたらした。

- ネットワーク管理にとって、管理者が不在時でも、監視、検知後の具体的な対策をとることが可能となった
- 端末管理にとって、利用者のなんらかのミス、あるいは悪意のある行為によって、正規の端末を不正に利用された場合の問題に対応することが可能となった



Kobanブラウザ ― 通信妨害中の端末一覧

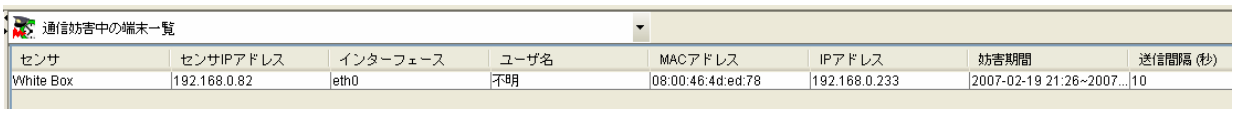


図 8 連動動作：未登録端末検知 → 自動トラフィック監視 → 自動遮断

図 9に、これまでに実現された機能によって、実際に端末の妨害が実施された場合の管理画面例を示す。当該端末は図中左上に示したアイコンのように地図上に一目でわかるように表示され、未登録端末であることを赤い PC のアイコンで、当該端末の通信が妨害され、ネットワークから遮断されていることをその上に表示したアイコンによって示している。

また現実の運用管理の観点から、図中右上のように一覧表示として、さらに後の調査に必要な履歴管理のために、図中下のような動作記録としても表示および管理可能としている。

図 9 管理状態の可視化および運用画面例

上述したネットワーク管理機能の動的な適用によって可能となる新しい動作シナリオを示す。

1. 未登録端末ポリシを設定：従来の検知ルールを基本検知ルールとして任意に設定
2. 未登録端末ポリシに HIT：端末監視センサが未登録端末として検知
3. トラフィック監視ポリシ作成：当該端末のトラフィックを監視するポリシを自動生成
4. トラフィック監視を開始：生成したポリシをトラフィック監視センサに適用

これらの一連の動作によって、外部組織からの移動端末なども一律に排除するだけではなく、必要に応じて利用を許可しながら、極端な通信時に遮断する、といった柔軟な運用が可能となる。

③ セキュリティシステム（NetSkateKoban）の状態およびリソース監視機能

本研究開発では、端末管理機能とネットワーク管理機能を統合することによって、外部からの侵入者や、未登録端末の持ち込みといった明らかな不正に対応するだけではなく、ミスによる不作為の不正、あるいは正規の利用者の悪意による不正などの、容易には予測できないが、実際にはもっともあり得るシナリオに対応することが可能となった。

しかし、最も根本的な問題はこれらのシステムが常に健全に動作することである。セキュリティシステムの障害による監視体制の穴は、致命的な問題を引き起こす。真に悪意のある攻撃者なら、目標を攻撃する以前に、セキュリティシステムを無力化することを狙うの

は当然であり、現実には、それらに対する高い対応能力が求められる。本研究開発では、統合されたネットワーク管理機能をさらに積極的に活用し、システムの各要素に対する到達性、およびそれらのリソースの状態を管理することで、システムの健全性を監視する。

図 10に、統合されたネットワーク管理機能を用いた到達性管理の画面例を示す。図中、青丸で示した部分が到達性の状況を示しており、応答時間を最大、最小、平均などの統計量で示すことで性能上の問題も推測することを可能としている。赤丸部分は到達性が失われており、なんらかの対策が必要であることを示している。

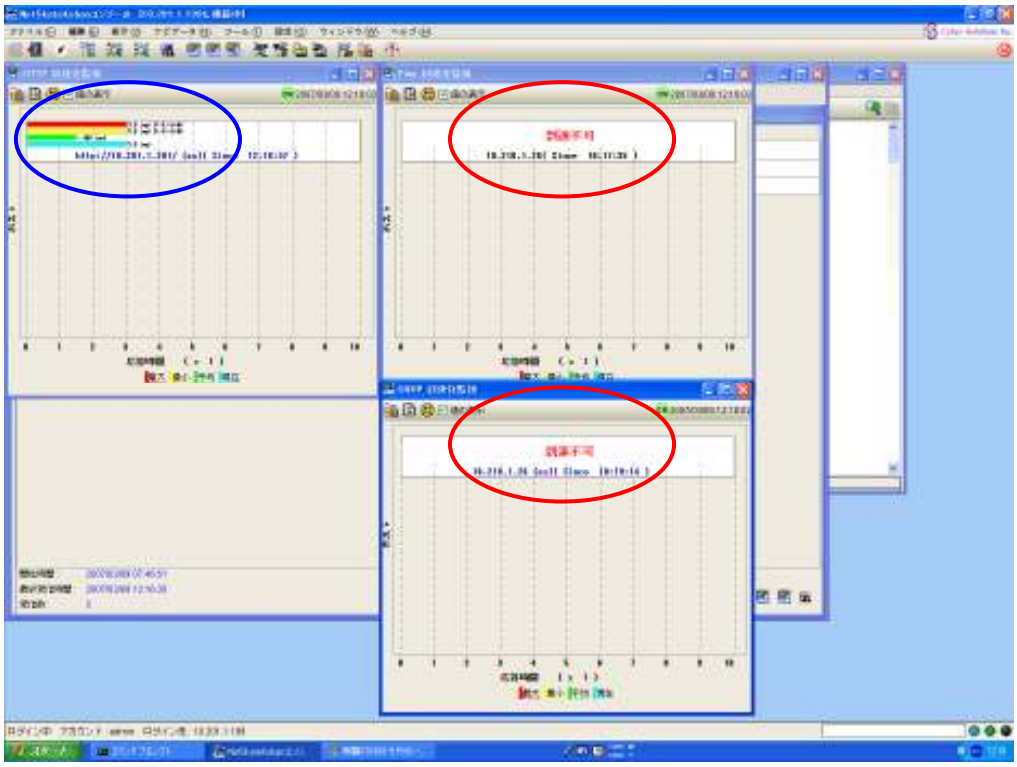


図 10 到達性管理の画面例

４－１－３　ネットワーク管理機能のセキュリティ管理への統合技術のまとめ

本研究開発サブテーマは当初の計画を 100%実施し、以下の技術を確立するとともに、具体的な製品としての統合を実現した。

本研究開発によって、これまでは独立し監視を主体としていたネットワーク管理を、その原因となる端末の特定、自動/手動排除、まで全自動でおこなうことが可能となった。また、システム自身の管理を統合することでセキュリティシステムとしての信頼性を大幅に向上させた。

４－２　マルチベンダに対応する基礎的検疫管理技術

４－２－１　マルチベンダに対応する基礎的検疫管理技術の概要

管理状態を制御できない外部組織に所属する移動端末なども対象とでき、日常の業務およびネットワークの運用にスムーズに統合できるネットワークおよび端末制御技術が必要である。一方的な遮断だけではなく、必要に応じて遮断のレベルを選択するとともに、全面的な遮断ではなく対策や、緊急避難的なアクセス経路を残すといった、柔軟なアクセス制御が重要となる。一方で、特定のベンダの機器や技術に依存した制御技術では、マルチベンダ化の進む現実の市場に受け入れられるものとするのは困難である。

本研究開発は、以下の 3 つの要素技術を確立し、それらの組み合わせによって既存のあらゆるネットワークに対応できる柔軟なネットワークおよび端末制御機能を実現する。

1. インターネット標準および業界標準技術を利用したマルチベンダユーザ認証機能
   同等の機能を実現する既存の市場製品は、特定のベンダ、機器に依存するものがほとんどである。本技術開発では、特定の製品機能に依存しない、標準化された、あるいはすでにデファクトスタンダードとなっている技術のみを利用することで、ベンダに依存しないユーザ認証を実現する
2. インターネット標準を利用した端末の強制隔離機能
   ユーザ認証による端末接続管理では、許可されていないユーザの接続を制御することができるが、許可されているが悪意のあるユーザの接続に対して無力である。本技術開発では、正当に認証され接続した端末に対して、強制的にそれを排除、隔離するための技術を開発し、インターネット標準技術のみでそれを実現することで、ベンダに依存しない強制隔離を実現する
3. 不正検知機能と連動した自動端末管理機能
   ユーザ認証、端末認証による端末接続管理は、不正接続を排除するための第一歩である。本技術開発では、ネットワーク管理機能と連動することで正当な権限のもとに接続した端末の不正行為を検知し、上記の強制隔離技術を利用することで、当該端末を自動的に排除する技術を開発する。

４－２－２　マルチベンダに対応する基礎的検疫管理技術の実施状況

本研究開発によって、標準化の進んでいる動的 VLAN 技術、RADIUS 認証技術、SNMP ネットワーク管理技術の組み合わせにより、市場に広く普及している複数のベンダの機器で共通の検疫機能を実現するとともに、統合されたネットワーク管理機能とも連携して検疫を実現する技術を確立した。

従来の端末管理機能を機器管理だけではなくユーザ管理の対応へと拡張し、業界標準、およびインターネット標準を組み合わせることで、ベンダ独自の技術および機能に依存しない動的なネットワークおよび端末制御技術を実現した。

① インターネット標準および業界標準技術を利用したマルチベンダユーザ認証機能

本研究開発によって、端末の移動、複数機器の利用などのモバイル機器利用に対応し、利用者自身の認証と機器の接続管理を連動させることが可能となった。本研究開発では、ベンダに依存しないユーザ認証技術の基盤として、以下の標準化されたあるいはデファクトスタンダードとなった技術を活用した。

- ネットワーク接続の認証：IEEE 802.1x
- 802.x1 におけるユーザ認証：RFC3580
  IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

また、既存の NetSkateKoban との連携を実現するためのデータベースを設計した。

マルチベンダを検証するための研究開発および実証は、CISCO 社およびアライドテレシス社の両機器で検証を実施するものとした。

図 11に、本研究開発で実現する端末管理システムへのマルチベンダ対応ユーザ認証機能の概要を示す。ユーザ認証のコア部分には広く活用されている RADIUS を活用し、かつそのエ

ンジンの実装として FreeRADIUS[1]を利用した。既存の端末管理との融合はデータベース管理レベルで実現し、以下の 2 点の要件を実現した。

- 既存の端末管理システム独自のデータベースを拡張したユーザ管理
- FreeRADIUS あるいは他の認証エンジンをそれぞれに対する変更を加えることなく統合

二つの異なるデータベース定義を SQL の View を用いて融合させることで、端末管理システムと FreeRADIUS でそれぞれの異なるデータベース定義を両立し、双方から整合のとれたデータベース設計とした。

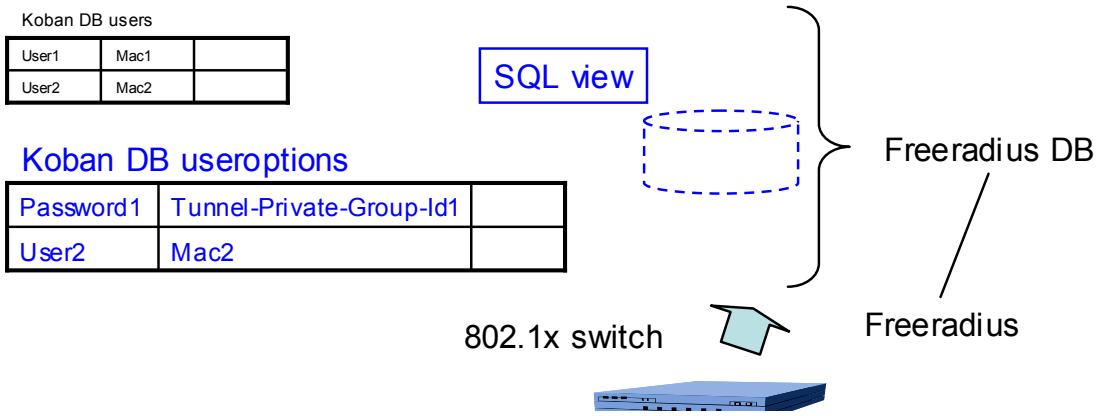


図 11 マルチベンダに対応するユーザ管理および認証技術の概要

図 12に上記にコンセプトに基づいて実現されたユーザ管理（登録）画面の例を示す。ユーザ情報として従来の端末管理システムに登録された情報を 802.1x に対応できるように拡張することで、マルチベンダに対応したユーザ認証情報を生成する。

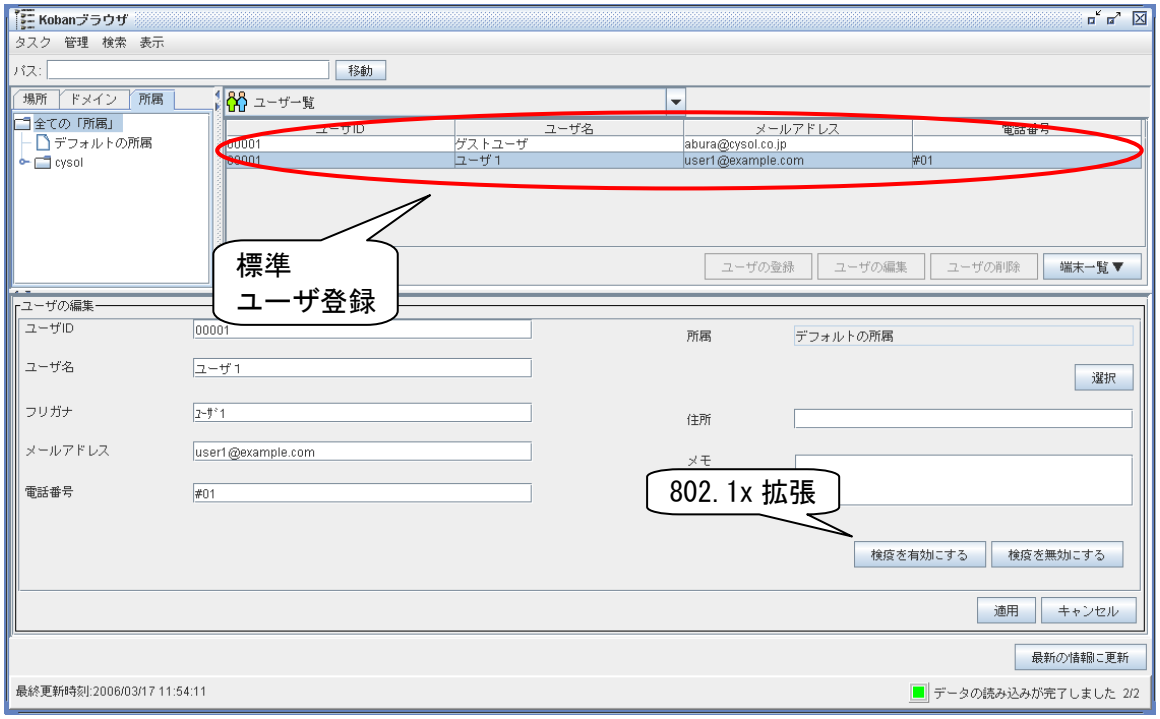


図 12 拡張ユーザ登録の画面例

[1] The FreeRADIUS Server Project, http://www.freeradius.org/

図 13に本研究開発で実現したユーザ認証実行時の画面例を示す。ユーザ認証の結果はイベントとして通知され、誰がログインを試み、成功したか、失敗したかなどの情報を他のイベントとともに一元管理することが可能となっている。

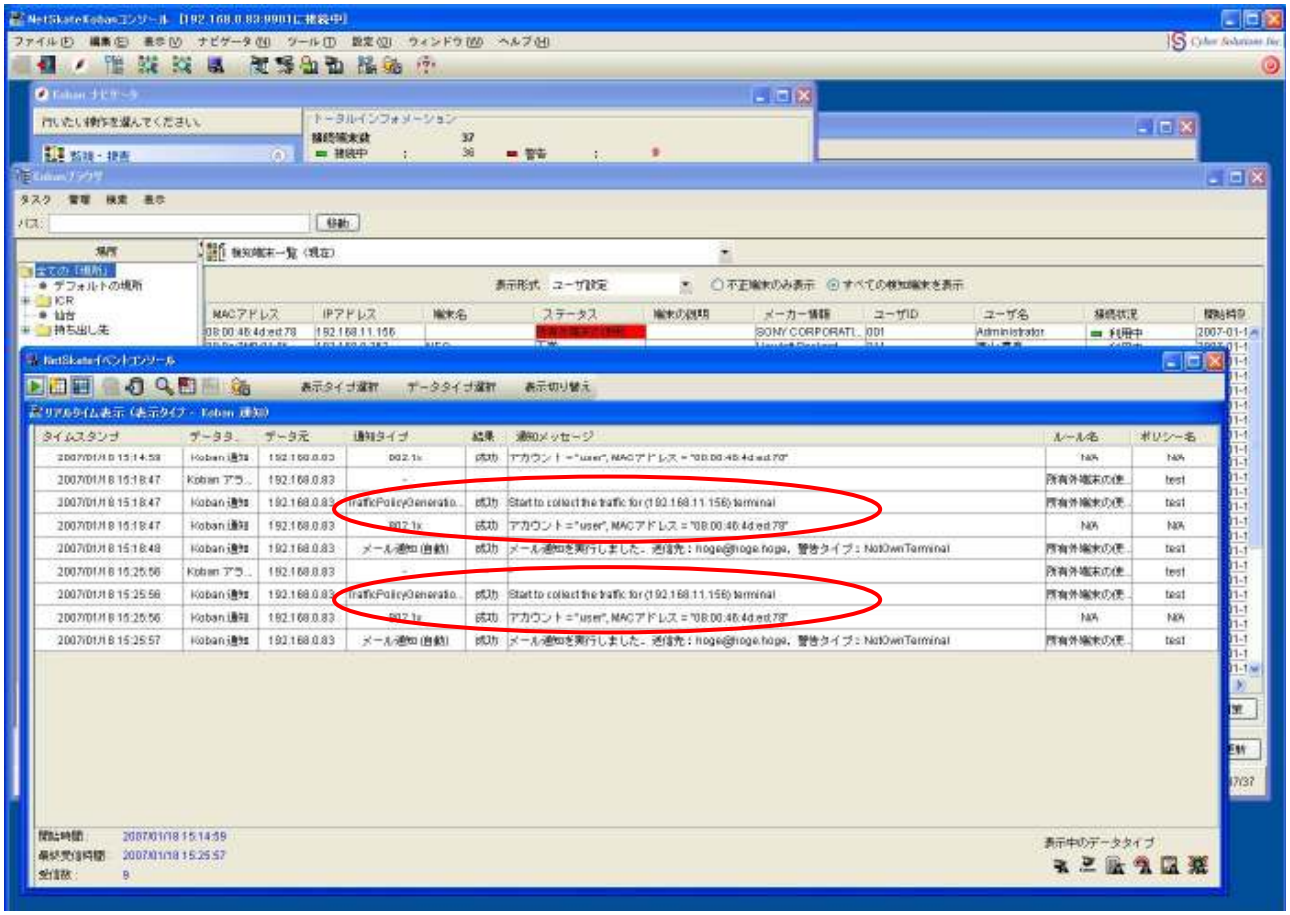


図 13 認証状態の管理画面例

ネットワーク接続者のなりすましを防ぐためにも初回の認証以外に、常に定期的に再認証を実施する必要があるが、再認証のタイミング、および実装はベンダによって異なる部分が多く、現在の標準的な方法を全面的には信頼することができない。

本研究開発では、それらの実装上の違いに依存せず、管理することが前提となっているネットワークスイッチなら標準的に備えているネットワーク管理情報ベース（MIB）経由で強制的に再認証を実行する技術を開発し実現した。マネージャから当該ポートを強制的に遮断およびオープンすることで、接続を初期化し、認証を促すことができる。

② インターネット標準を利用した端末の強制隔離機能

図 14に、強制的な隔離を実現するためのシステム要素および構成の概要を示す。端末は通常は図中の Operational VLAN として示された 802.1x を運用しているネットワークに接続するものとし、隔離を実行すると同じく図中の Quarantine VLAN に移動することで、他の端末との接触のない環境に移動させる。隔離は図中にも示した以下の三つのステップで実施される。

1. 前節のユーザ管理によって統合された端末管理（Koban）データベースと RADIUS データベースに対して、ユーザアカウントとともに、当該端末が本来所属すべき VLAN 情報を設定する。
2. 強制隔離時には、Quarantine VLAN として設定された VLAN ID を、ユーザ管理データベ

ース上の本来所属すべき VLAN 情報のかわりに設定し、SNMP によって当該ポートを制御することで、強制的に接続先 VLAN を変更する。

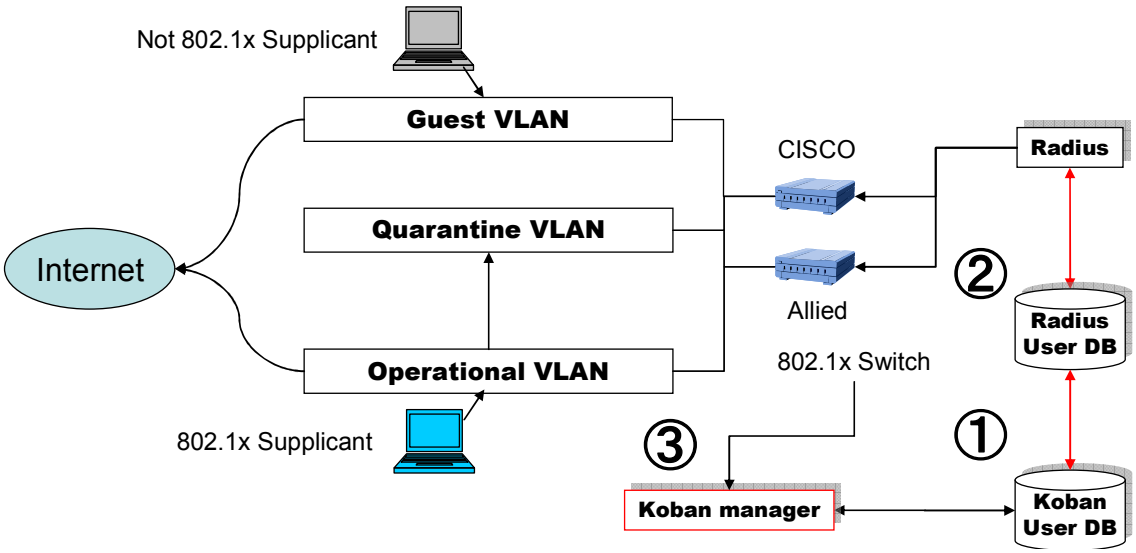


図 14 端末隔離技術の概要

図 15に強制隔離を実現するステップと要素の関係を示す。

1. ポート遮断：当該端末が接続しているポートを標準管理プロトコルによって強制遮断
2. Quarantine VLAN の書き込み：隔離先にあたる VLAN の情報をデータベースに格納
3. ポート許可：1 で遮断したポートを許可（オープン）する
4. ユーザの認証：端末が再接続された状態になり、認証を要求される
5. GuestVLAN へ：正しく認証されれば、2 で書きこまれた VLAN 情報により接続が変更

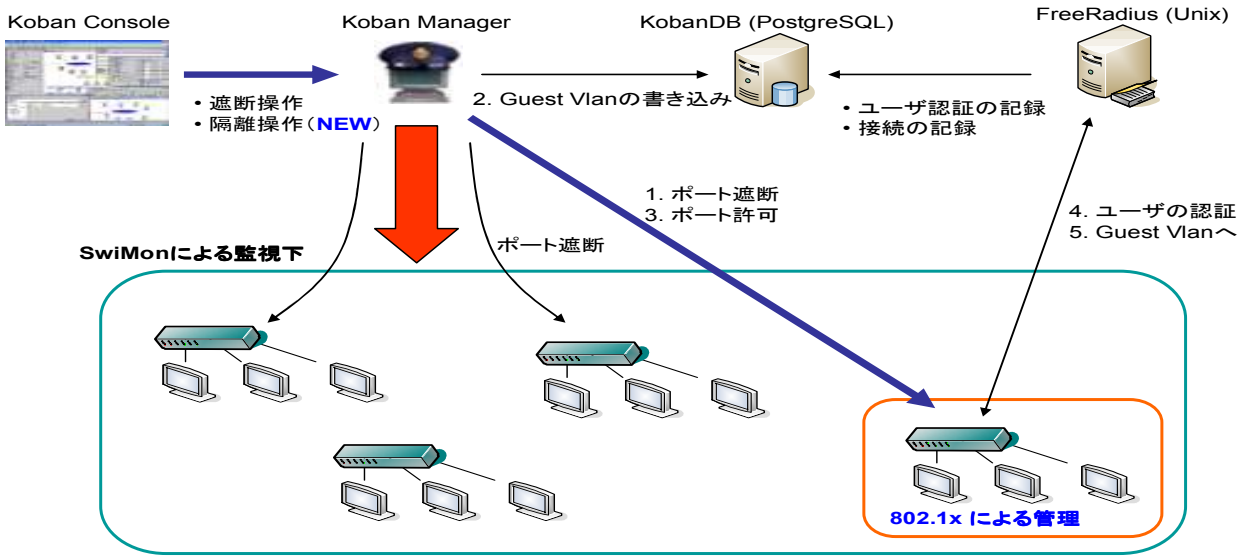


図 15 端末強制隔離のシステム要素概要

③ 不正検知機能と連動した自動端末管理機能

図 16に検知された端末を自動隔離するための設定画面例を示す。本設定によってイベントに対応して自動的に隔離を実行することが可能となる。その結果、従来の遮断とはことなり、隔離された端末にはある程度のネットワークアクセスを認めることができるため、必要なセキュリティ対策、あるいは移動端末として、認められたゲストアクセスのみを許可するといった柔軟な運用が可能となる。

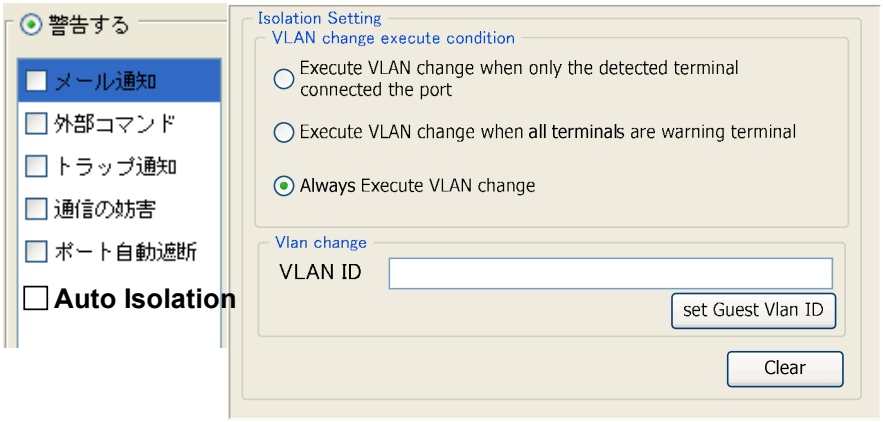


図 16 自動隔離機能の設定画面例

図 17にオープンソースの IDS 侵入検知システムである SNORT と連動した自動隔離機能の概要を示す。未登録端末として検知された端末に対する強制隔離機能以外に、侵入検知システム（IDS: Intrusion Detection System）と連動した隔離機能を実現した。本機能によって、未登録端末だけではなく、IDS に検知される利用者のミスあるいは不作為によるウィルス等への感染、あるいは悪意のある行為も隔離の対象とすることが可能となり、従来にはない高度なセキュリティ管理を実現することが可能となる。

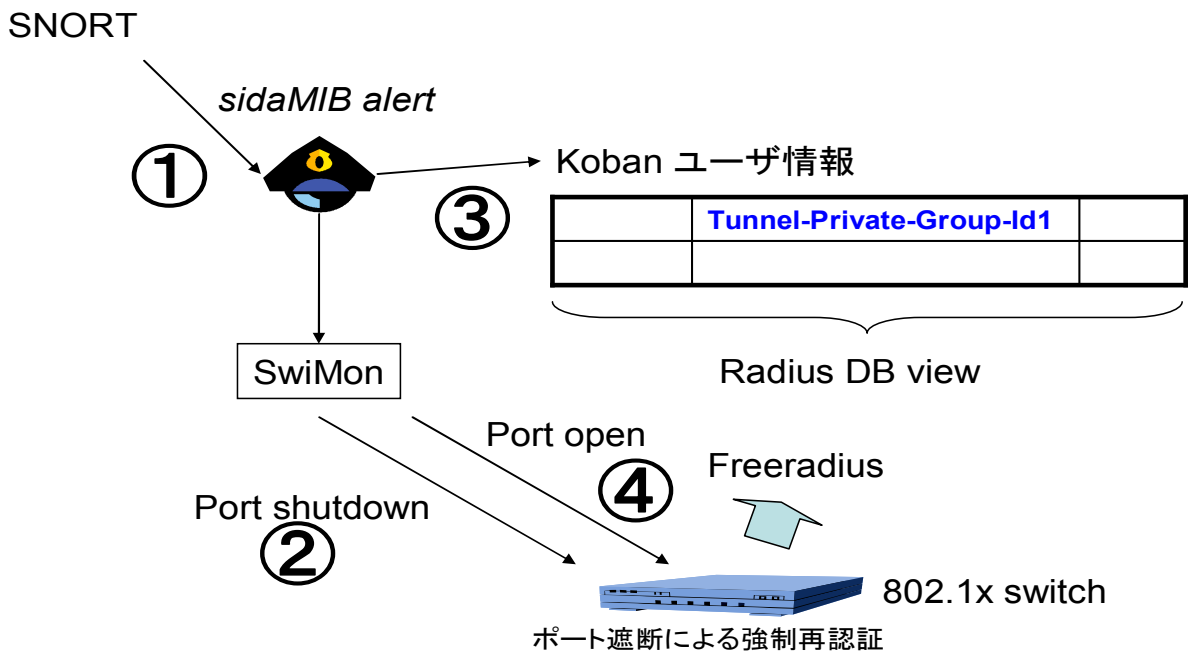


図 17 SNORT と連動した自動隔離機能

４－２－３　マルチベンダに対応する基礎的検疫管理技術研究開発のまとめ

本研究開発サブテーマは当初の計画を 100%実施し、以下の技術を確立するとともに、具体的な製品としての統合を実現した。

本研究開発によって、標準化の進んでいる動的 VLAN 技術、RADIUS 認証技術、SNMP ネットワーク管理技術を組み合わせることによって、市場に広く普及している複数のベンダの機器で共通の検疫機能を実現するとともに、統合されたネットワーク管理機能とも連携して検疫を実現する技術を確立した。

４－３　移動性を管理できる NetSkateKoban 実現のための設計要件調査

本調査研究によって、本格的な移動端末環境を管理するには、端末が移動することによる物理的な接続切り替えを効率よく処理する技術が不可欠であることを明らかにした。シミュレーションによって同性能の特性を定量的に明らかにすることができ、今後の開発の重要な指標を確立できた。また管理対象として、VoIP を使った移動 IP 電話を検討することが、市場の大きな部分をカバーするために重要となることが明らかになった。

接続するネットワーク組織の管理がおよばない移動端末を安全に接続させるための要件、および将来の普及が見込まれるインターネット標準の移動管理プロトコル MobileIP を中心とした要件、および標準化動向を調査研究した。

① ゲスト端末の安全な接続技術

移動性の管理は、まったく新しい環境の管理であり多くの課題が存在している。既存の固定端末の接続をすべての無線接続に移行していくような利用も進み、新しいデバイスとして無線 VoIP デバイスなども現実のものとなってきている。本調査研究ではこれらの新しい環境に対して、協力関係にある研究開発パートナ等を通じて現場レベルの調査を実施し、以下のような知見を得た。

■　非常に多くの無線アクセスポイントの監視

従来は、論理セグメント単位での監視をおこなうことで、そのネットワークに接続される全ての端末を監視することが可能であったため、大規模ネットワークであってもその数は数百のレベルであった。

しかし、無線ネットワークでは同一論理セグメント内であっても接続点が刻々と移動する可能性があるため、その直接の接続先である無線アクセスポイントの監視は欠かせない要素となる。このとき問題となるのは、無線アクセスポイントの数である。従来、論理セグメントの設計は、収容可能なデバイスの数を論理アドレス数、帯域などの性能的な側面から設計し、スイッチング技術の進歩によって同時接続による帯域的な問題は大きくない。その規模、数は規模に対してほぼ線形となることから、監視システムが備えるべきスケーラビリティも線形として、実用上の問題はなかった。

しかし、無線アクセスポイントは、各アクセスポイントがカバーすべき物理的な場所によってその範囲が制限され、多くの端末が接続する可能性があるエリア、建物の影響をうけるエリアなどではきめ細かな配備がおこなわれる。結果として監視対象となる無線アクセスポイントは、従来の固定ネットワークの場合に対して飛躍的に大きくなり、本調査研究で調査した、現在日本最大規模の無線アクセスポイントの配備を進めている企業でもそれらの管理に現実的な問題がでていることが明らかになっている。具体的には従来は数百であった単位が容易に数千の規模になることがわかった。

■　非常に多くの無線接続デバイスの監視

大規模な無線インフラの整備は、その上で利用される各種の端末の増加も意味する。無線VoIP 端末などが普及すると、従来は PC 端末の接続のみに利用されていた無線接続も、用途に応じて、音声通信用、ノート PC 用、あるいは将来的には個人が身につけるウェアラブル端末など、多様化することが予想できる。本調査研究では、無線アクセスポイントが数千のオーダとなったとき、管理対象となる端末は少なくとも 1 万以上を想定しておくべきことがわかった。無線アクセスポイントとともにこれだけの数の端末を常時監視するためには、多くの性能上の向上が必要であることが明らかになった。

■　新しい「移動」の概念の導入

端末管理技術にもまったく新しい概念の導入が必要となる。これまでは端末は一定の場所に比較的長時間接続されることを前提としており、端末あたりの接続および切断は一日数回のレベルで十分実用的であった。しかし端末が移動することを前提とすると、この仮定は大きな修正を余儀なくされる。無線接続のローミング技術によって、端末利用者は無線レベルのハンドオーバを意識することなく、シームレスに接続を維持することが可能なっているが、物理メディアのレベルでは異なる無線アクセスポイントへのハンドオーバが起こっており、これは端末の切断と再接続が繰り返されることを意味している。

このことはたとえ短時間であっても端末の利用者が廊下を数 10m 移動する、部屋を移動する、階を移動するといった日常的な移動で頻繁に接続と切断が発生することを意味しており、イベントおよびその履歴の管理に大きなリソースが必要となること示している。具体的には、従来の 1 日数回のレベルではなく、ほぼ無限に増加することを前提とした設計が必要となることが明らかになった。

また、上記のように移動するような利用形態では、一回の接続時間が見かけ上非常に短くなるため、適切な接続管理なしには、処理がおいつかず、同時に複数の接続が、異なる場所に存在しているようなケースが発生し得ることが明らかになった。無線アクセスポイントおよび端末管理の性能問題と併せて、リアルタイムで高精度な接続管理技術が必要であることがわかった。

■　新しい管理アプリケーションの研究

VoIP 端末等で利用が広がっている SIP プロトコルでは「プレゼンス」の概念を積極的に利用することが提案されている。「プレゼンス」の概念は、無線環境のアプリケーションに大きな可能性を開くものとして期待されているが、そのことは無線端末の状態管理に課題をもたらすこともまた明らかである。今後の接続管理はより上位のアプリケーションが「移動」の概念を備えてくるにつれて、その管理および活用に大きな研究、および事業化の余地が生まれることが明らかになった。

■　ネットワークをまたがる接続の管理

本研究開発の主要な課題は、移動端末の管理にはネットワークをまたがる端末の移動をいかにして管理するが重要な要素であるが、なかでも以下のふたつの要素は、特に今後の研究を要するものとなる。

1. Mobile IPv4 と Mobile IPv6 の両方のネットワークおよび端末の管理
2. ローカルに接続されていない端末の検知

1 については複数のプロトコルが共存する環境での接続管理であり、2 は、Mobile IP を活用して、外部に持ち出されている端末を検知することが課題となる。Mobile IP の管理は大きな課題であり、ホームエージェント管理技術などの研究開発および事業化余地が大いにあることが明らかになった。

② Mobile IP 管理に関する標準化動向

移動性をサポートする次世代インターネットプロトコルである Mobile IP は実用化にむけて多くの標準化、実装、実証実験が進められている。本研究開発ではその中でもネットワーク管理に関する側面に焦点をあてており、以下の標準技術を主導している。

RFC 4295: Mobile IPv6 Management Information Base

本研究開発では上記の標準を基盤として、外部ネットワークに接続している端末の管理を実現する。

また、2007 年 3 月 29 日には、WIDE（Widely Integrated Distributed Environment）プロジェクトによって”Mobile IPv6 を用いた IPv6 移動通信サービスの実験運用開始”がアナウンス[2]され、次世代プロトコルである MobileIPv6 の実用化も着々と進行中である。

一方で、移動体からの情報収集については、十分な技術がなく、課題があることが明らかになっている。具体的には、移動体が本質的にもつ、通信品質の不安定さを前提とした情報収集技術の欠如である。

本調査研究によって、RFC として発行された以下の技術を活用して、インターネット標準技術による情報収集の効率化の可能性が大きいことを明らかにした。

RFC4498: Managed Object Aggregation MIB and the technique

これらは優秀賞を受賞した以下の研究の延長上に調査研究されたものである。

“A Bulk-Retrieval Technique for Effective Remote Monitoring in a Mobile Environment” Glenn Mansfield Keeni, Kazuhide Koide, Takeo Saitoh, Norio Shiratori ,Proceeding of The IEEE 20th International Conference on Advanced Information Networking and Applications, 18-20, April, 2006

４－４　ユビキタスネットワーク利用管理技術の研究開発

平成 18 年度に確立した、端末を管理下に置くための技術を活用し、端末が移動することを前提とするネットワークの管理技術を確立する。

４－４－１　ユビキタスネットワーク利用管理技術の概要

端末接続がダイナミックに変化する無線接続の移動端末を主体とするネットワーク管理技術を研究開発する。研究開発は接続を受け入れるネットワーク側、および接続する端末、さらにはその上で利用するファイルを管理する技術で構成される。

本研究開発では、無線接続をサービスするネットワークの管理技術を確立する。無線接続のサービスは AP（アクセスポイント）と呼ばれる無線接続機器によって提供される。本研究開発では、自由度の高い無線アクセスポイントトポロジの適切な管理、大規模ネットワ

[2] プレスリリース：http://www.wide.ad.jp/news/press/20070329-MobileIPv6-j.html

ークに対応できる無線アクセスポイント管理の拡張性の課題を解決し、無線接続端末が前提の接続を受け入れる側のネットワーク管理技術を確立する。

次に、無線接続端末の管理技術を確立する。無線接続は、端末が移動することを前提とするため、有線ネットワークと異なり、ネットワークへの接続箇所を特定のネットワーク、ポートなどのように固定することができない。また端末の移動によって、端末の接続箇所も移動し、ネットワークへの接続・離脱が頻繁に発生する。本研究開発では、定常的な接続、離脱を管理可能な、論理的にも物理的にも動的に接続される無線接続端末の管理技術を確立する。

さらに、端末レベルを超えた新しい移動性をサポートする技術を確立する。移動端末によって、場所やネットワークに束縛されない新たな情報環境を構築可能であるが、このことは情報そのものを管理する単位となるファイルのレベルでは、機密情報ファイルの持ち出しの管理という新たな課題が発生する。本研究開発では、機密情報の持ち出しをイントラネット管理として統合するとともに、持ち出されたファイルの利用状況をリアルタイムに監視し、記録することで、監査可能なファイル利用管理技術を確立する。

４－４－２　ユビキタスネットワーク利用管理技術の研究開発実施状況

本研究開発では、まず無線接続端末を収容する無線 AP（Access Point）の管理技術を開発した。従来は、端末はスイッチの特定のポートに接続され、それが移動することはないため、端末の接続、切断の管理は個々のポート毎に管理することで実現されていたが、移動端末の管理を考えると、それでは十分ではない。無線接続の端末は、移動することによってその接続先となる AP が変わり、さらに結果としてそれらを収容しているポートも変化する。従来の方式ではこれらは特定の端末がネットワークから離脱し、新たな端末がネットワークに接続した、として解釈されるが、本研究開発によって、無線接続端末を収容するネットワーク側を連携管理する技術を確立し、これらを同一端末の移動として管理する技術を確立した（図 18）。本技術によって、移動端末管理の基礎的要素が拡張され、ユビキタスなネットワーク利用を管理する技術が確立された。

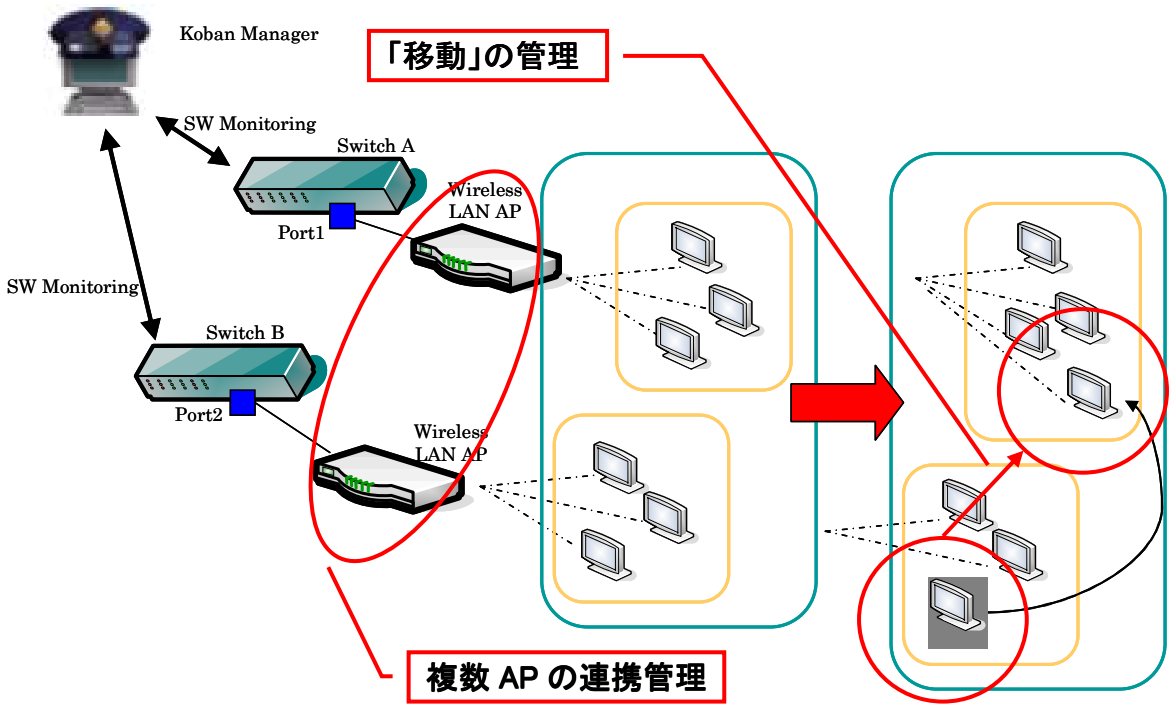


図 18 無線接続端末の「移動」管理の実現

次に、上記技術によって拡張された端末側の管理技術を開発した。「移動」をサポートすることで移動端末管理の基盤が整備されたため、その接続管理に新たなレベルをもたらすことか可能となった。具体的にはこれまで場所や部署ごとに個別に行ってきたアクセス制御に移動の概念を考慮することが可能となり、移動端末による不正な接続の試みがあった場合でも、その端末がどのようにネットワークにアクセスしてきたかを参照して、管理することが可能となった。図 19に移動端末の接続管理例を示す。この例では営業部門への接続を禁止した研究開発部門に接続していた端末が営業部門に移動するケースを示している。

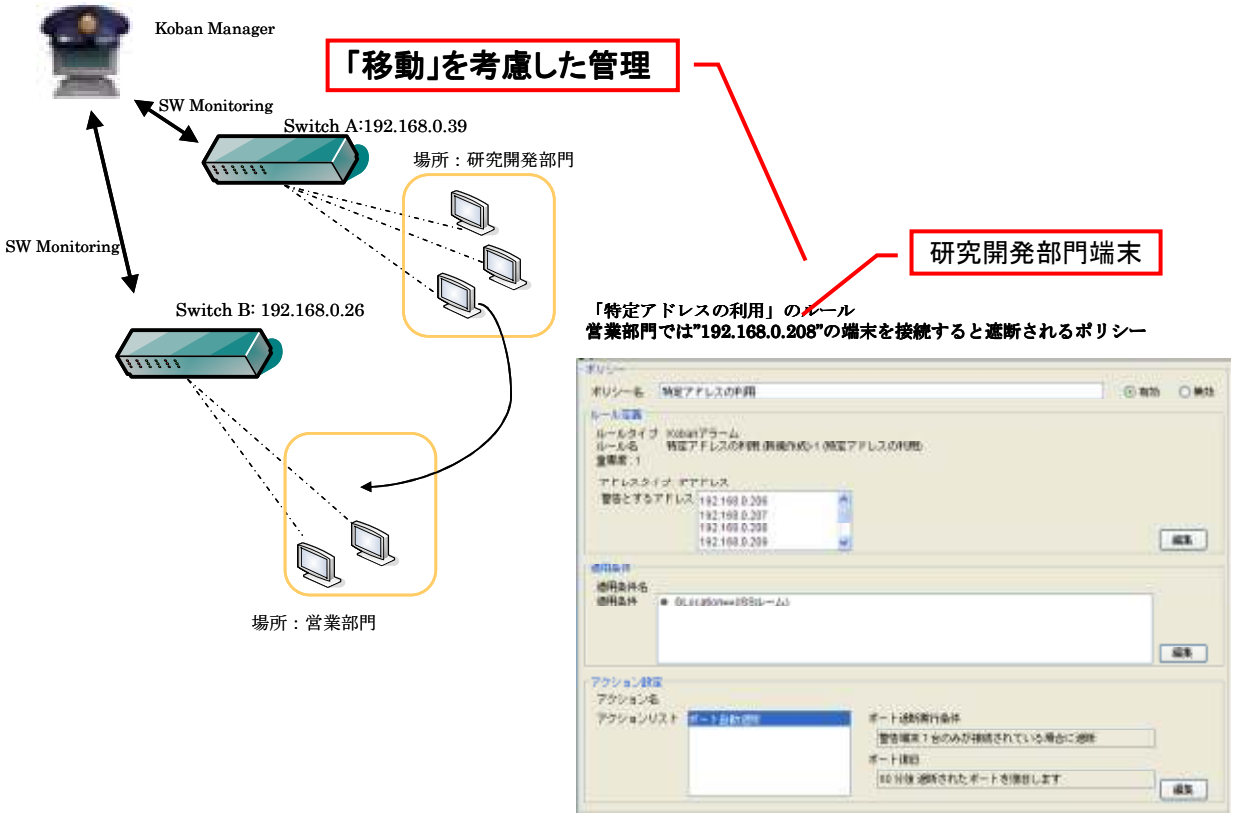


図 19 移動端末の接続管理例

図 20は移動元での接続管理例を示している。この場合は当該端末の接続は許可されており、正常な接続として管理されている。

図 20 移動元での接続管理例

図 21は移動先での接続管理例を示している。この部署では当該端末の接続は禁止されているため接続の検知と同時に遮断されている。従来は図 20のケースと図 21のケースはそれぞれ独立であり、実際の運用時には、営業側で、この端末はなぜここに接続しようとして

いるのかを一から調査する必要があったが「移動」を適切に管理することで当該端末が直前まで研究開発の部署で正常に接続していたことがわかる。そのため調査時にも、研究開発部門に問い合わせる、といった現実的な運用を実施することができる。

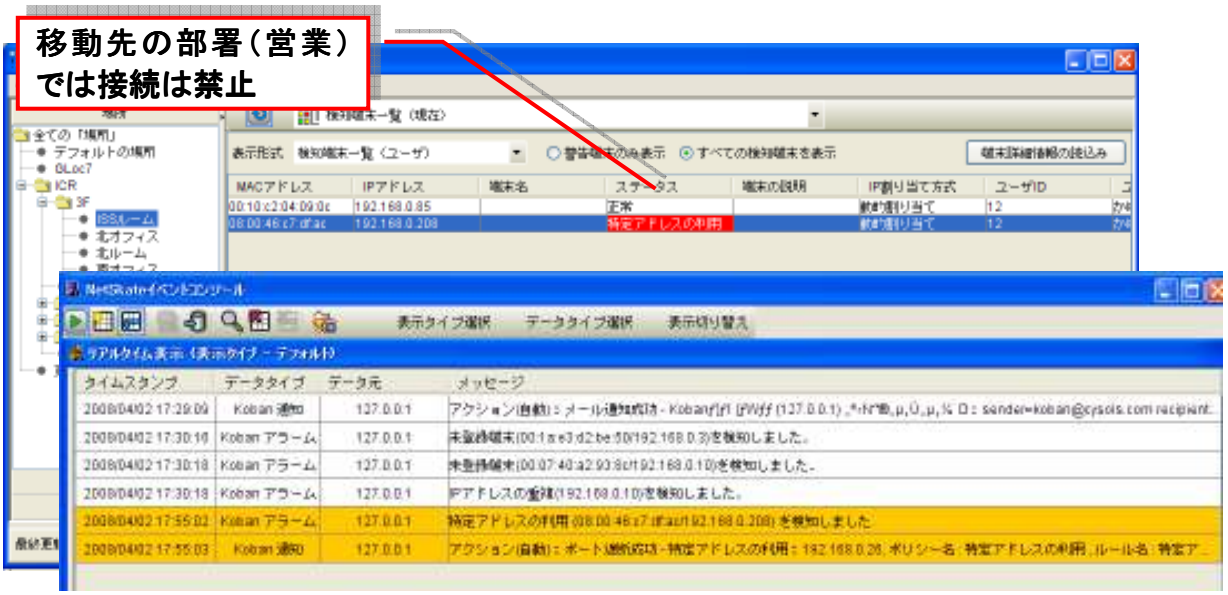


図 21 移動先での接続管理例

さらにより上位レベルの概念として、機密情報の持ち出しをイントラネット管理として統合するとともに、持ち出されたファイルの利用状況をリアルタイムに監視し、記録することで、監査可能なファイル利用管理技術を確立した。図 22に端末上のファイルレベルの移動管理の例を示す。本技術により、端末だけではなく、ファイルレベルの移動管理が実現し、端末に依存しない機密情報管理を実現できる。

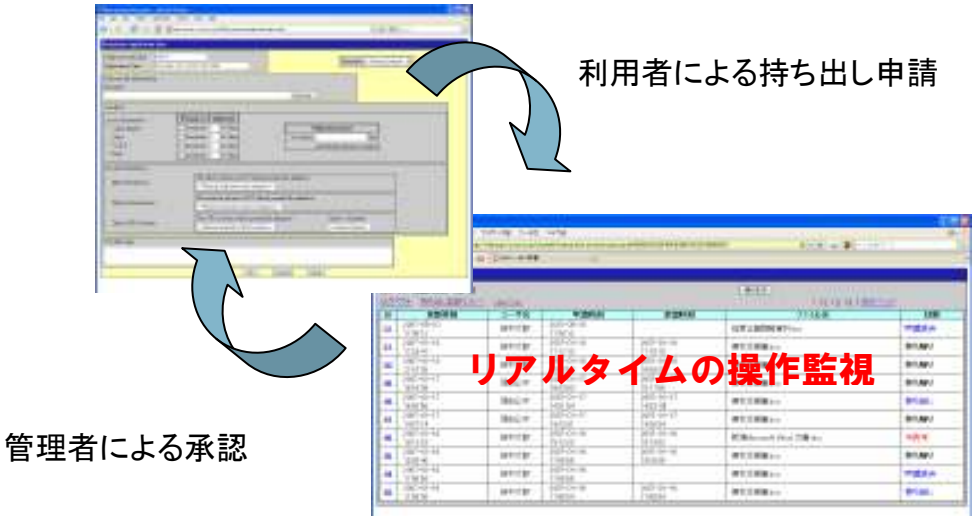


図 22 端末上のファイルレベルの移動管理の例

４－４－３　ユビキタスネットワーク利用管理技術の研究開発のまとめ

本研究開発によって、ユビキタスネットワーク利用の基盤となる「移動」の概念を包括的に管理する技術を確立できた。無線接続端末に関する研究開発では、仮想的に構築した大規模環境を利用し、大規模ネットワークでも実用的に利用できる技術であることを確認できた。ファイル持ち出しは技術の確立が完了し、結合試験を通じて実用化にむけた実用面での課題を明らかにできた。

４－５　既存技術とのシームレス運用技術の研究開発

本研究開発では、従来の固定ネットワークと今後の移動体管理を統合し、運用管理をシームレスに拡張できる技術を確立する。

４－５－１　既存技術とのシームレス運用技術の概要

本研究開発では、従来の有線ネットワーク管理技術と、移動端末を前提とする新しいネットワークの管理技術のシームレスな統合と拡張を実現する技術を確立する。従来の有線ネットワーク管理では、ネットワークを構成する端末の役割や利用目的は原則として固定的であるため、あらかじめ設定された管理基準に従って、全体として管理することが可能であったが、移動端末を前提とするネットワークでは、端末の役割、利用目的は常に変化するため、各端末の管理はそれらの変化に応じた柔軟さが必要となり、以下のような課題をもたらす。

- ユーザ端末認証技術のシームレスな統合
- 有線環境と無線環境のシームレスな統合

本研究開発では、前節の研究開発で確立される有線、無線の統合環境を活用した新しい端末管理技術を確立する。ユーザ端末認証となる登録情報を有線、無線で統合するとともに、端末の移動性を管理し、端末の総合的な利用状況を活用する以下の技術を研究開発する。

- ユーザアカウント情報の統合管理
- 高度な端末履歴の管理

４－５－２　既存技術とのシームレス運用技術の研究開発実施状況

本研究開発では、今後の移動体管理を既存の固定ネットワーク管理のフレームワークに統合する技術を研究開発し、ユーザレベルの管理単位、無線・有線を問わない運用管理を実現する技術を確立した。

図 23に端末認証とユーザ認証のシームレスな統合例を示す。図では MAC アドレス認証による端末認証によって接続された端末とユーザ認証によって接続された端末を同じ管理画面上でシームレスに管理している。本技術によって多様化する接続認証方式に対応し、移動端末を効率的に管理することが可能となる。

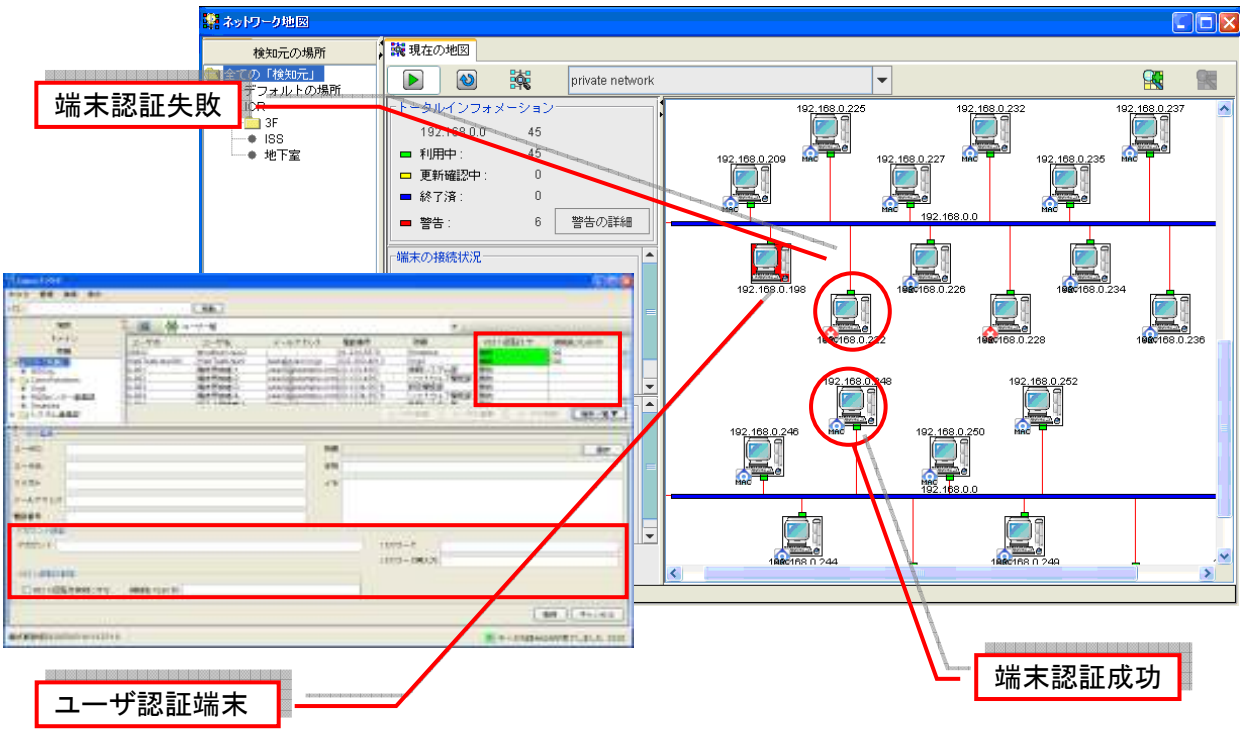


図 23 端末認証とユーザ認証のシームレスな統合例

図 24に有線環境と無線環境のシームレスな統合の例を示す。図のように従来の有線接続のネットワーク構成図と同様に無線 AP 接続を可視化・管理する技術を確立できた。

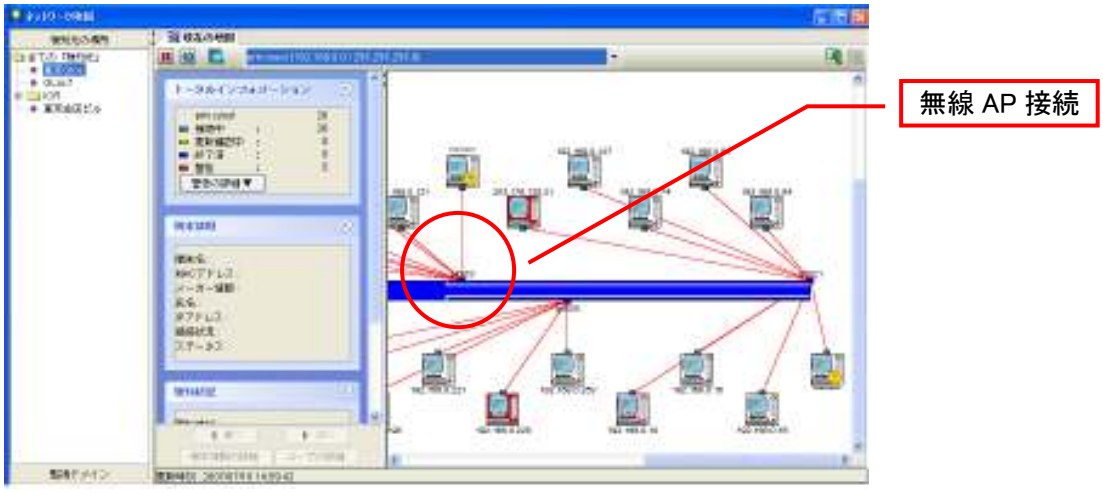


図 24 有線環境と無線環境のシームレスな統合

本研究開発では、端末の接続管理、有線および無線接続を実際の運用に即して管理するために、ユーザ情報による管理技術を統合した。本技術によって、端末利用の管理をより抽象化し、接続方式、移動/固定の違いに関わらず追跡管理することを可能とした。図 25にユーザ毎の利用履歴管理例を示す。本機能によって端末ではなく利用者による接続管理が可能となり、実際の運用現場での利用シーンに沿った管理が可能となる。

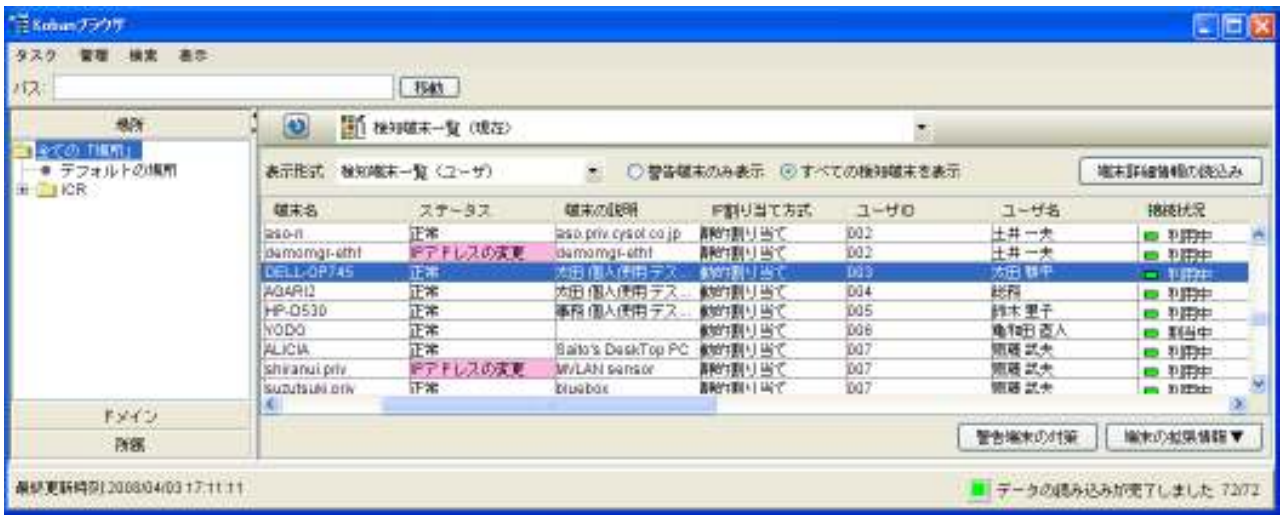


図 25 ユーザ毎の利用履歴管理例

図 26に図 25の機能をユーザが複数の端末を利用している場合の管理に拡張した例を示す。図 25と同様にユーザレベルでの管理が可能となり、かつ、複数端末を対象とすることで、デスクトップとノート PC の利用といった実際の業務に即した管理を実現した。

図 26 ユーザによる複数端末利用管理例

図 27に図 26で示した複数端末の管理をより直感的に理解できる形とした表示例を示す。複数の端末の利用をグラフ化して示すことによって、利用状況の管理をより容易にできた。

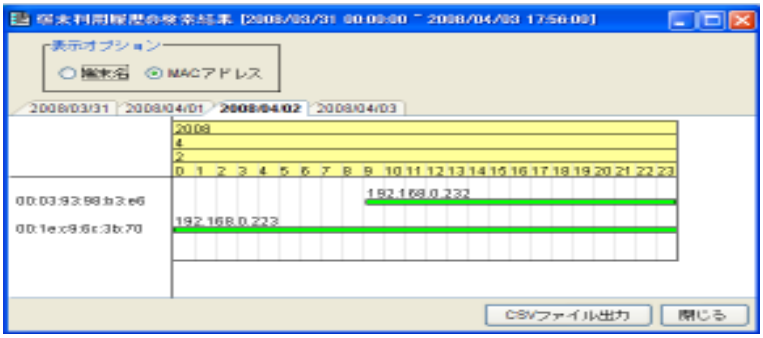


図 27 複数端末利用履歴管理例

４－５－３　既存技術とのシームレス運用技術の研究開発まとめ

ユーザ端末認証技術のシームレスな統合と有線環境と無線環境のシームレスな統合を実現し、従来の有線接続との統合を実現するとともに、端末接続とユーザ認証の統合によってネットワーク利用レベルでの管理を実現した。

ユーザアカウント情報の統合管理と高度な端末履歴の管理を実現することによって、従来は端末管理、ユーザ管理と分かれていたものの統合を実現し、それらを一体化したポリシ管理技術を確立した。移動端末接続の管理にその長期的な利用履歴を活用することを実現した。

４－６　次世代ネットワーク活用技術の研究開発

次世代ネットワーク技術である IPv6 は長い研究開発期間を経て標準化が進んできたが、近年の IPv4 アドレスの枯渇問題などから、その普及が急務となっている。一方で端末の OS として普及しているマイクロソフト社の Windows も VISTA で IPv6 を標準サポートするなど、実際の運用への機運が高まっている。

４－６－１　次世代ネットワーク活用技術の概要

本研究開発では、次世代インターネット技術として、標準化および実装が進んでおり、今後の移動ネットワークを実現する重要な要素となる IPv6 を活用するための技術を確立する。次世代のインターネット技術として徐々に導入が進んでいる IPv6 について以下の課題を研究開発する。

- IPv6 ネットワーク管理
- IPv6 端末管理

４－６－２　次世代ネットワーク活用技術の研究開発実施状況

本研究開発では、管理対象となる端末の IPv6 接続を管理する技術を予定通り確立した。IPv6 ネットワーク管理のために、現在 IPv4 アドレスで表現されているネットワークの論理構成を IPv6 でも扱える技術を開発した。具体的には接続された端末の IPv6 アドレスを自動的に取得し、そのアドレス構造を分析することで、ネットワーク構成を可視化するとともに、IPv4 との混在環境でもシームレスに管理、表示する技術を実現した。図 28に開発したIPv6 ネットワーク管理の例を示す。

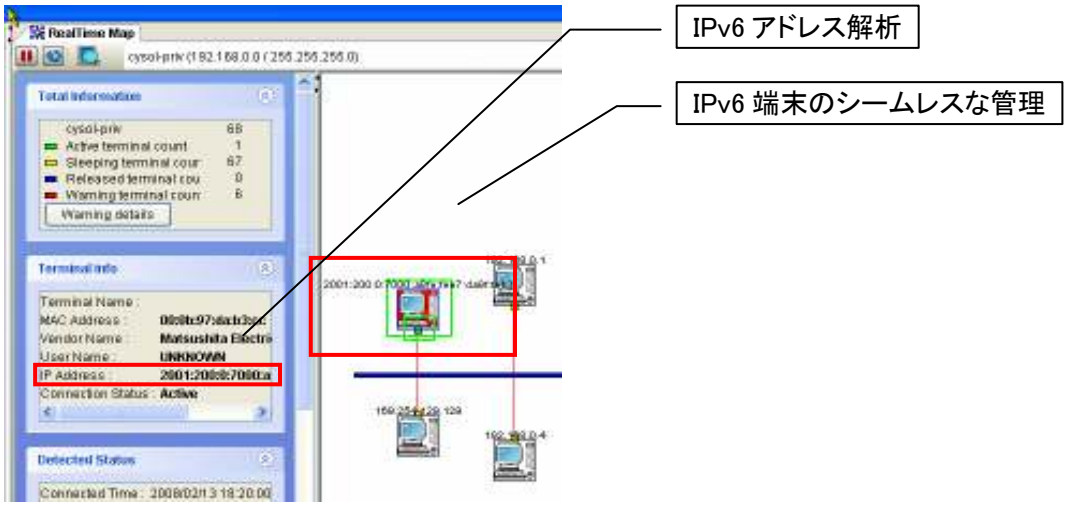


図 28 IPv6 ネットワーク管理の例

また､インターネットのネットワーク管理プロトコルとして広く普及しているSNMP(Simple Network Management Protocol）の IPv6 化も重要な要素である。本研究開発グループは同プロトコルの IPv6 化に早い段階から取り組んでいたが、本研究開発によって、それを実用技術として確立した。図 29に開発したシステムでの管理プロトコルでの IPv6 アドレスの扱い例を示す。

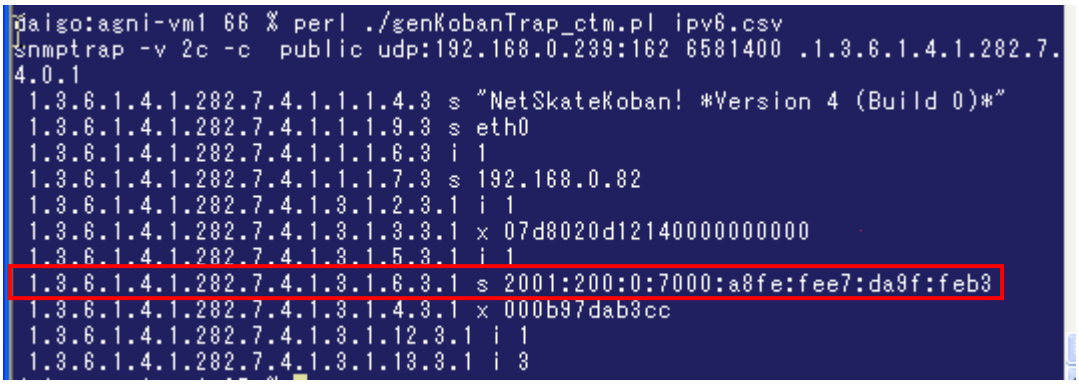


図 29 管理プロトコルでの IPv6 アドレスの扱い例

４－６－３　次世代ネットワーク活用技術の研究開発まとめ

最新のインターネット技術 IPv6 および移動端末対応プロトコル MobileIPv6 に対応したネットワーク管理、および端末管理技術を確立し、従来の IPv4 端末管理技術とのシームレスなシステム化を実現した。本技術、およびシステムの実現によって、今後ニーズが立ち上がってくることが予想される次世代ネットワーク技術においても市場をリードしていくことを期待できる。

４－７　ネットワーク構成の自動発見技術の研究開発

本研究開発では、大規模ネットワークへのセキュリティシステムのスムーズな導入という現実の課題に対する技術の確立を目指し、導入対象となるネットワーク側の状況を自動的に取得、分析する技術を研究開発する。

４－７－１　ネットワーク構成の自動発見技術の概要

本研究開発では、監視対象となるネットワーク構成を自動的に発見し、管理すべき対象および情報を自動的に認識する技術を確立する。大規模ネットワークでは、セキュリティシステムに必要なセンサ網の事前設計および配備に多大なコストを要するが、それらの自動化には以下のような課題の解決が必要となる。

- ネットワークトポロジの自動発見
- 管理システムおよびセンサの自動構成

４－７－２　ネットワーク構成の自動発見技術の研究開発実施状況

本研究開発では、流動的に構成が変化する大規模ネットワークでのセキュリティシステムの自動構成技術を研究開発し、予定通り技術の実用化を実現した。

図 30では、本研究開発で確立したネットワークトポロジの自動発見技術の核となるネット

ワーク構成の分析例を示している。分析は情報収集、情報分析、分析結果に基づく更なる情報収集、という再帰的なプロセスで構成されている。また既存のあらゆるネットワークで利用できるシステムとするために、すでに標準化され、広く普及した管理情報のみを利用している。

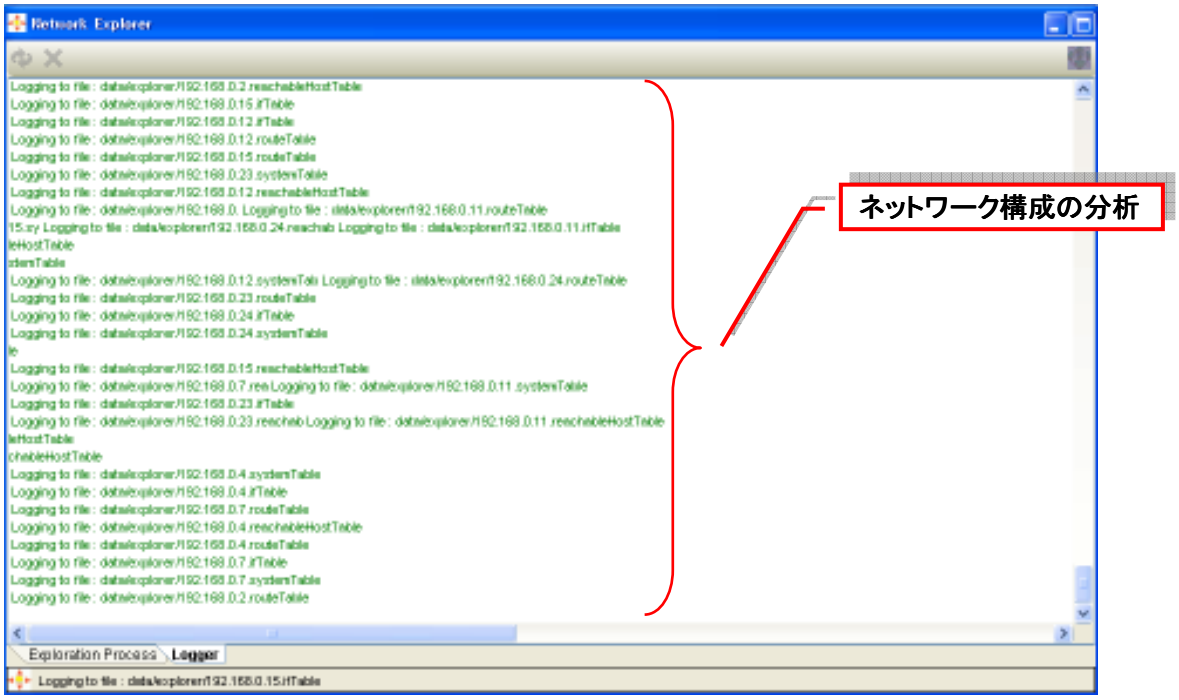


図 30 ネットワークトポロジの分析例

図 31はネットワークトポロジの自動発見例を示している。図 30の例で示したようなネットワーク情報の分析結果から、ネットワーク構成要素の接続関係を自動的に発見できるが、それらを人がみてわかるように可視化するために、それらを最適にレイアウトする技術を確立した。

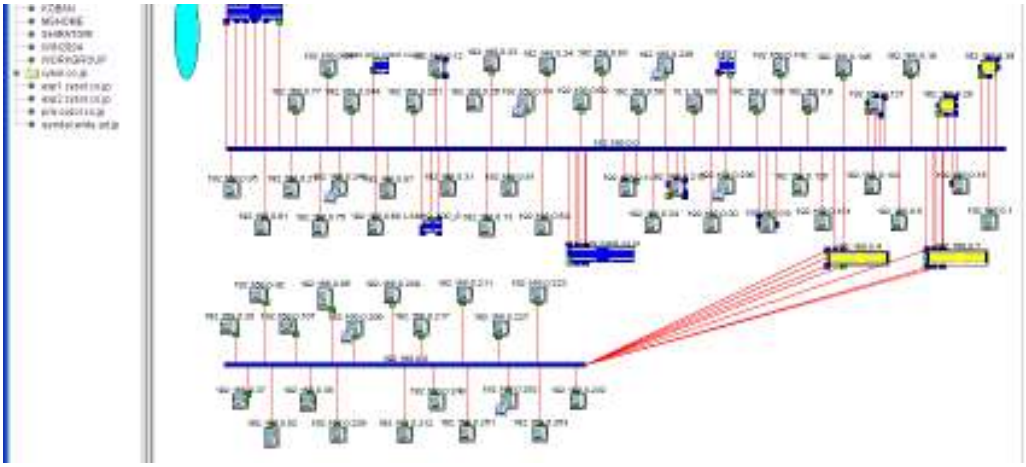


図 31 ネットワークトポロジの自動発見例

さらに、自動発見されたネットワーク構成に対して、センサの配備及び設定を追随させる技術を研究開発し、センサの遠隔構成技術を確立した。図 32はマネージャ<->センサ構成例を示している。

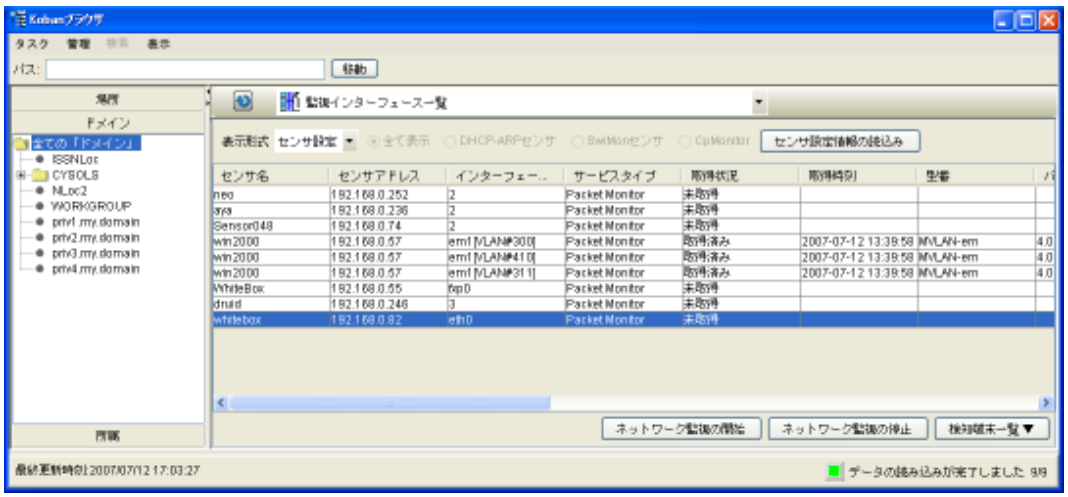


図 32 マネージャ<->センサ構成例

上記の技術を組み合わせることで、ネットワークトポロジを自動発見し、管理者に対してわかりやすく提示するとともに、その構成にあわせて、センサシステムを遠隔から動的に構成することが可能となる。本技術と次に述べるネットワーク要素の自動構成技術を利用することで大規模ネットワークでのセキュリティシステムの導入が大幅に簡素化され、結果として、セキュアなネットワーク構築をより容易にすることができる。

４－７－３　ネットワーク構成の自動発見技術の研究開発まとめ

ネットワークトポロジの自動発見技術、および管理システムおよびセンサの自動構成技術を確立し、大規模ネットワークにおけるセキュリティシステム自動構成の基盤技術を確立した。本技術はシステムそのものの自動化よりもシステムの導入の自動化に重点を置いたものであり、現在のセキュリティシステムの抱えている現実の課題の解決に大きな貢献となるものである。

４－８　ネットワーク要素の自動構成技術の研究開発

本研究開発では、大規模ネットワークへのセキュリティシステムのスムーズな導入という現実の課題に対する技術の確立を目指し、セキュリティシステムとしての構成を自動化する技術を研究開発する。

４－８－１　ネットワーク要素の自動構成技術の概要

本研究開発では、管理システム、センサおよび各種監視エージェントの自動構成技術を確立する。セキュリティシステムには、新しい機能、脅威への対応など日常的な更新が必要とされるが、大規模ネットワークでは、セキュリティシステムの更新にも多大なコストを要するため、分散配備される各種センサおよびエージェントの自動更新技術が重要となり、以下の課題の解決が必要となる。

- セキュリティシステム自体の管理
- セキュリティシステムの自動更新

４－８－２　ネットワーク要素の自動構成技術の研究開発実施状況

セキュリティシステムには、高い信頼性と可用性が要求されることから、システム全体の常時監視が重要な課題となっている。本研究開発では、本システムのすべての基盤であるセンサシステムの監視技術を確立した。図 33は監視のための基本となるインタフェースの実装を示している。

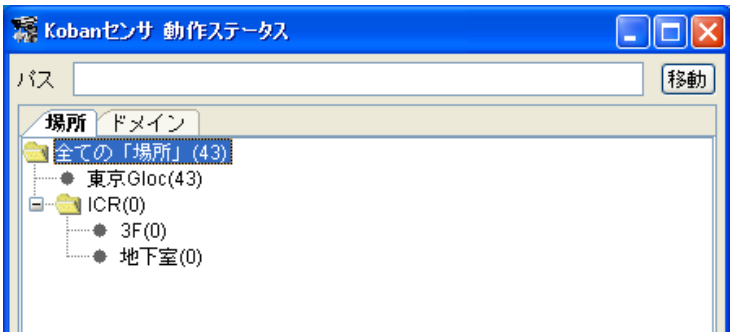
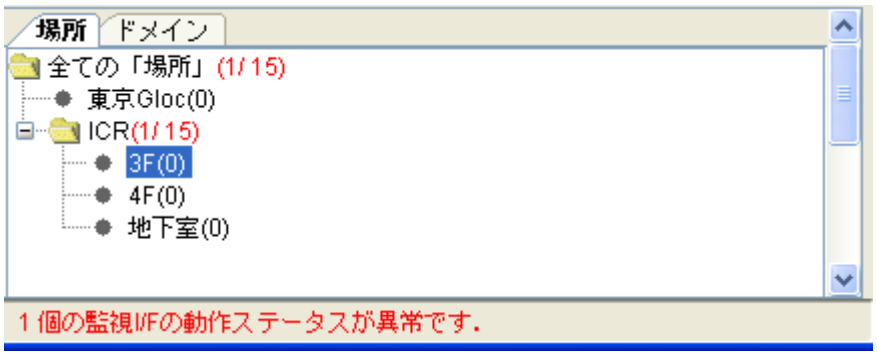


図 33 センサ動作ステータス

センサでは、2 種類のプロセスが動作しており、このどちらかのプロセスが停止してしまった場合や、ネットワーク接続障害等で Koban マネージャと NetSkateKoban センサが通信できなくなった場合は、赤色で障害のある場所のセンサ数と画面下部のメッセージで通知される。



また、図 34にセンサが監視を行っているインタフェースの一覧を表示する機能を示す。本機能によって、本システムの運用状況を一目で把握することが可能となり、システム全体の可用性の管理を実現できた。

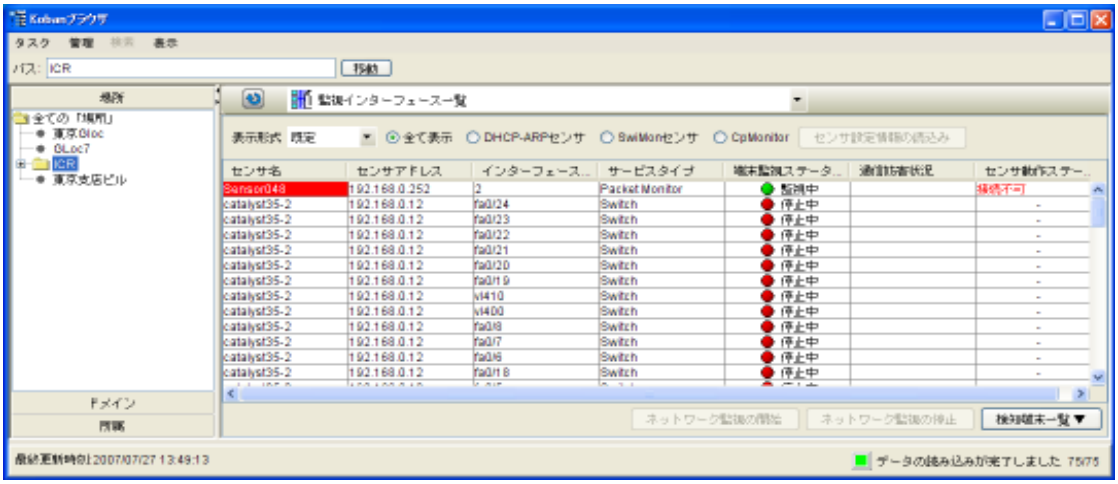


図 34 Koban ブラウザ（監視インタフェース一覧）

次に、研究開発したネットワーク中に配備されたセンサの構成を一括更新する技術を示す。大規模ネットワークでは、センサの配備が物理的にも広範囲にわたることがめずらしくなく、それらの運用管理に関するコストが現実的な課題となる。また大規模ネットワークではその構成の変更も相対的に多くなるが、それにあわせてセンサの構成を変更するのは容易ではない。本研究開発では、配備済みのセンサのソフトウェアおよび設定を一括更新する技術を確立した。

４－８－３　ネットワーク要素の自動構成技術の研究開発まとめ

セキュリティシステム自体の管理技術、セキュリティシステムの自動更新技術を確立し、セキュリティシステムの一部であるセンサの信頼性の向上と可用性の確保を実現し、ネットワーク中に多数配備されたセンサシステムの更新技術を確立することで、超大規模ネットワークでの本システムの運用の実用性を大幅に高めることができた。

４－９ 大規模ネットワークにおけるセキュリティシステムの自動最適化

高信頼な大規模ネットワークの管理には、セキュリティシステム自体についても、多数のセンサの配備、管理システムの並列化、データベースシステムの最適配置、およびそれらのシステムの冗長化などの要素を考慮したシステム設計が重要な要素となる。しかし大規模ネットワークでは、その各所で日常的に部分的なシステムの更新、構成の変更、機器およびソフトウェアの更新、追加などが行われるため、それらに追随してセキュリティシステムを再設計、再配備することは非常に困難となり、国際的な広がりを持つような組織では事実上不可能となっている。

４－９－１ 大規模ネットワークにおけるセキュリティシステムの自動最適化の概要

本研究開発では、18 年度、19 年度に確立したネットワーク構成の自動発見技術、およびネットワーク要素の自動構成技術を基盤として、それらを統合し、ネットワーク構成にあわせたシステム設計を自動的に実現する技術を確立する。

４－９－２ 大規模ネットワークにおけるセキュリティシステムの自動最適化の実施状況

常に局所的な変更があることを前提とする必要がある大規模ネットワークでは、ネットワーク中のリソースの状況を自動的に取得し、障害等を含め、その状況にあわせた動的再構成が必要となる。

図 35にネットワークリソースを自動的に取得する機能の実行例を示す。ネットワーク接続された機器、およびセキュリティシステムを検索し、その利用状況を取得する。

図 35 ネットワークリソースの自動検索

取得された情報を基に、最適化を実現する。以下に障害等で問題が発生した場合の自動リカバリ機能の実行例を示す。

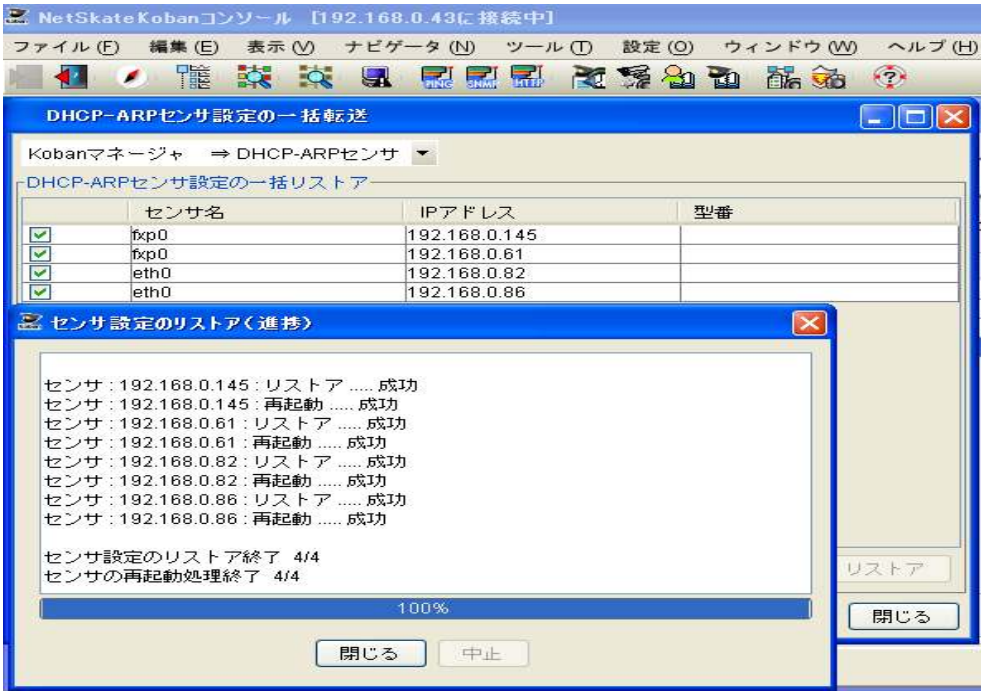


図 36 システム全体のリカバリ実行例

４－９－３ 大規模ネットワークにおけるセキュリティシステムの自動最適化のまとめ

本研究開発によって、障害発生時等に、センサ、マネージャ双方のフェイルオーバを実現する技術を確立した。サーバおよびセンサの両方をバックアップシステムに移行することで、ダウンタイムを最小化し、可用性を大幅に引き上げる技術を確立した。また平成 19 年度までに確立したネットワーク構成の自動取得、センサの遠隔設定などの技術と統合することで、導入および運用管理全体のコストの大幅な削減と省力化を実現し、大規模ネットワークでのセキュリティシステム導入をより現実的なものとすることが可能となる。

４－１０ ネットワーク資産の自動発見技術

情報システムへのセキュリティ要件は日増しに高度になっており、セキュリティ監査の範囲も拡大および詳細化している。現状では組織の利用する機器、ソフトウェアの管理には多大なコストがかかっており、その自動化は大きな課題となっている。

４－１０－１ ネットワーク資産の自動発見技術の概要

本研究開発では、19 年度に確立されたネットワーク構成の自動発見技術を基盤として、ネットワークで利用される情報資産を自動発見する技術に拡張する。19 年度までにネットワーク接続される機器、および利用されるファイルの管理技術が確立されるため、それを拡張し、さらに以下の技術課題を解決することでこれまでは容易ではなかった「情報資産」の管理まで可能とする技術とする。

４－１０－２ ネットワーク資産の自動発見技術の実施状況

図 37にネットワーク上のハードウェア資産を自動的に検知し、その基本情報を自動取得する機能の実現例を示す。本機能によって端末だけではなく、ネットワーク接続された情報設備資産を統合管理することが可能となり、包括的なイントラネット資産管理システムとして大きな拡張となる。

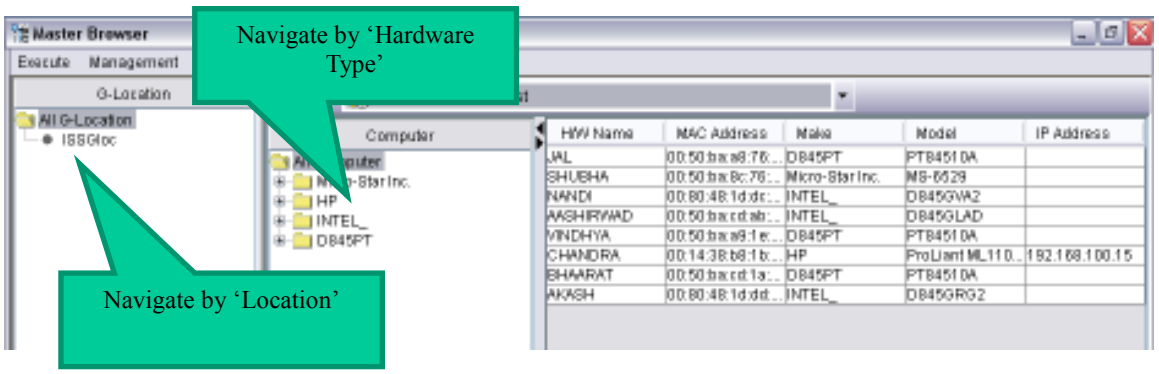


図 37 ハードウェア資産管理機能

図 38にネットワーク上のソフトウェア資産を自動的に発見し、管理する機能の実現例を示す。本機能により、ハードウェアだけではなくソフトウェア資産の管理を実現し、台帳として管理するだけではなく、ソフトウェアインストールに関するポリシの実現状況、違法コピーの有無などの全ネットワーク的な管理を実現している。

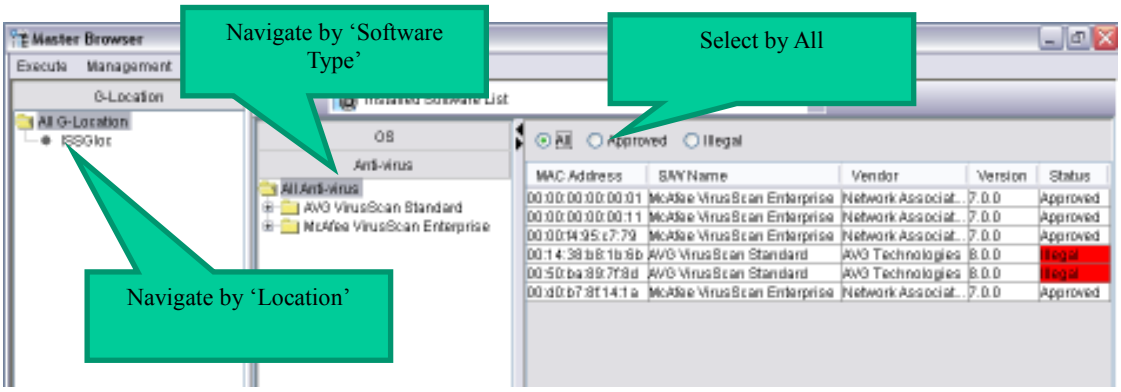


図 38 ソフトウェア資産管理機能

４－１０－３ ネットワーク資産の自動発見技術のまとめ

本研究開発によって、管理対象を端末だけとするのではなく、イントラネットで利用されている情報資産全体に拡張するための、基礎部分が確立された。実質的なセキュリティレベルを高めるためにも、運用を含めたネットワーク管理の効率化は急務であり、本機能は今後大きく発展することが予想される統合運用管理システムの基盤となる。

４－１１ 実証実験

研究開発の成果を実用的な技術として確立するため、大規模ネットワークを想定した運用実験を実施する。

４－１１－１ 実証実験の概要

平成18年度および19年度に確立される上記課題を実際のネットワークに適用することで、実証実験をおこなう。実証実験は、共同研究先、および事業化パートナーの協力を得て、実験ネットワークおよび、実際に運用されているネットワークの双方で実施し、現実的な課題の洗い出しおよび性能評価をおこなう。

４－１１－２ 実証実験の実施状況

実証実験は、大規模ネットワークでの運用を想定した性能評価を中心に実施した。

表 1 大規模ネットワークにおける性能計測（サーバ仕様）

CPU	Intel Core2 Duo E8200 @ 2
RAM	4.00GB
OS	Windows Vista Business
Database	MSSQLServer2005

本システムは、通常の運用時は、センサから送られてくる様々な情報をマネージャが処理、分析し、利用者が直感的に理解できる形で表示することを基本としている。管理対象のネットワーク規模が大きくなるにつれて、収集される情報が増大し、その処理性能がシステム全体の性能を決定する。そこで本実証実験ではその基本性能を実験で評価した。

図 39は、本実験で測定した性能と結果の概要を示している。それぞれの部分での所要時間を分析した。

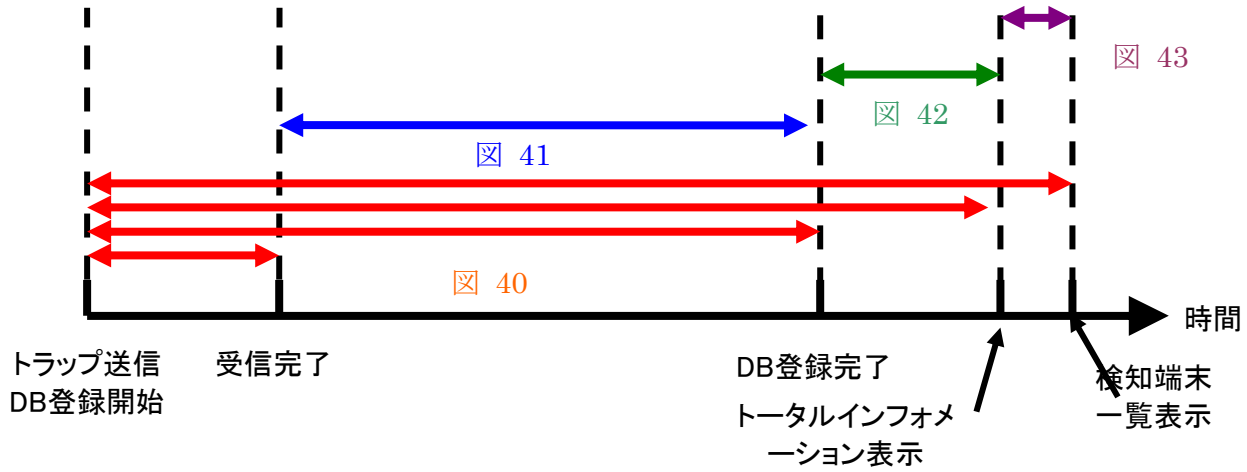


図 39 性能評価概要

図 40にトラップを受信してから、最終的な表示までの所要時間を示している。図からトラップ受信性能が端末数の増加に対して一定であるのに対して、それ以外の所要時間はリニアに増加しており、なかでも DB 登録がその支配的要因であることがわかる。

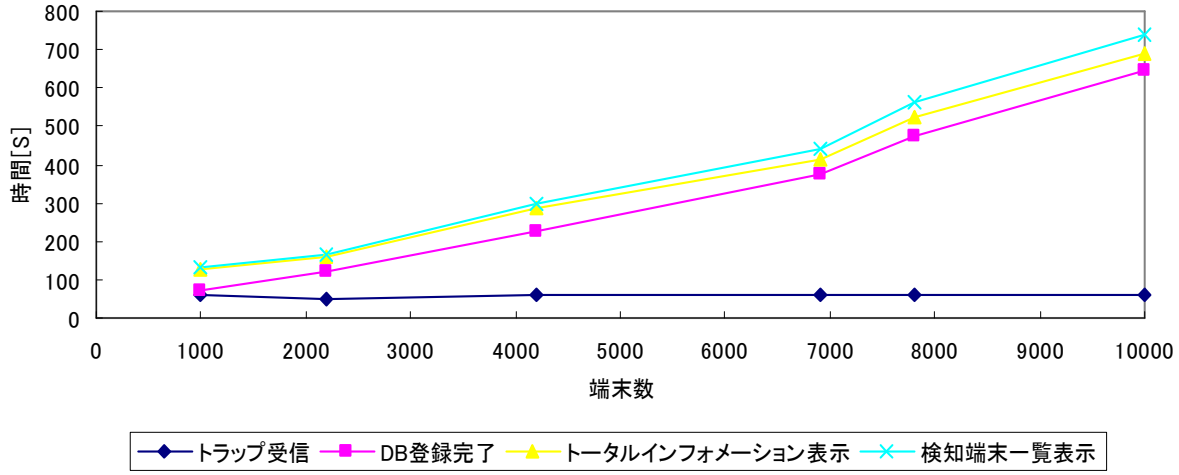


図 40 イベント検知の所要時間

図 41はトラップ受信完了-DB 登録完了所要時間を抽出したグラフである。図から DB 登録は端末数の増加に対してリニアであることがわかる。

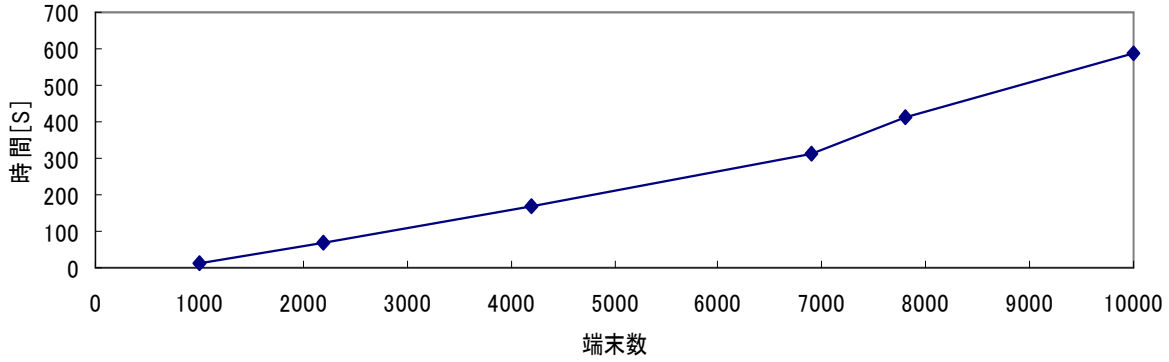


図 41 トラップ受信完了-DB 登録完了所要時間

図 42はDB 登録完了-インフォメーション表示所要時間を抽出したグラフである。インフォメーション表示は 30 秒ごとに更新されるため、周期的に所要時間が変動しているが、端末数の増加に対する影響はないことがわかる。

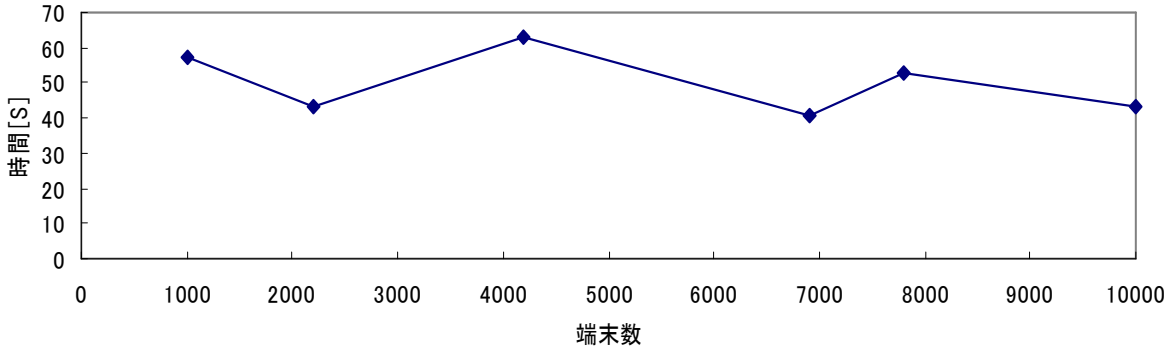


図 42 DB 登録完了-インフォメーション表示所要時間

図 43はインフォメーション表示-検知端末一覧表示所要時間を抽出したグラフである。最終的な一覧表示は、端末数の増加に対してリニアな特性を示すことがわかる。

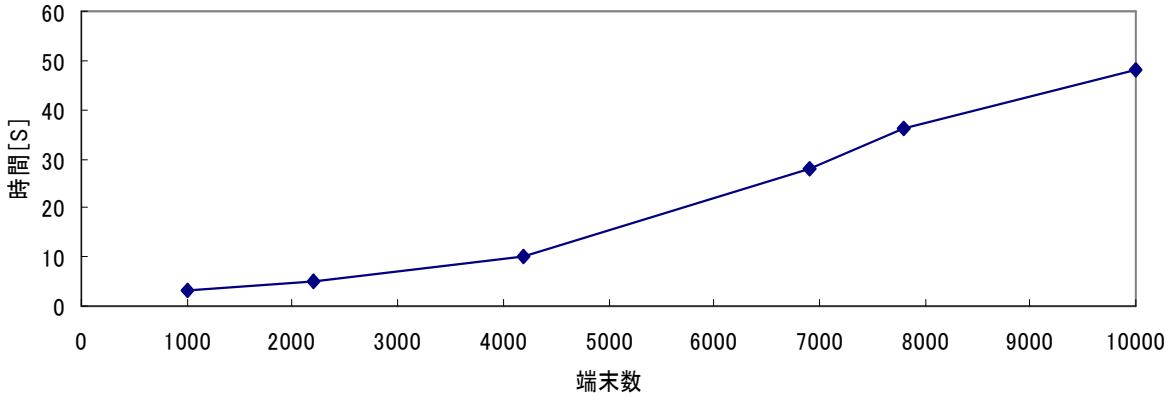


図 43 インフォメーション表示-検知端末一覧表示所要時間

４－１１－３ 実証実験のまとめ

平成18年度および19年度に確立される上記課題を実際のネットワークに適用することで、実証実験をすすめている。実証実験は、共同研究先、および事業化パートナーの協力を得て、実験ネットワークおよび、実際に運用されているネットワークの双方で実施しており、当初予定していた、拡張性を考慮した性能試験が 19 年度に完了した。

全体の性能は対象となるネットワーク規模に対してリニアであり、特定的なボトルネックが存在しないことが確認されたが、その中でも DB 登録が支配的な要素であることが明らかになったため、その最適化によって、全体性能を向上させることが可能であることがわかった。

４－１２ 総括

４―１２―１ イントラネットにおける移動端末の接続管理技術

本研究開発項目では、固定端末の接続を管理する基盤となる既存製品 NetSkateKoban™ を基盤として、**移動端末の接続および移動環境での安全な情報利用を実現する技術**を研究開発した。主な研究開発要素は以下の通り。

- アドレス詐称に対応する端末管理
- 無線ネットワーク/端末の管理
- ファイル持ち出しの管理
- 次世代ネットワークIPv6接続の管理
- 既存技術とのシームレスな運用

各要素の位置づけを図 44に示す。

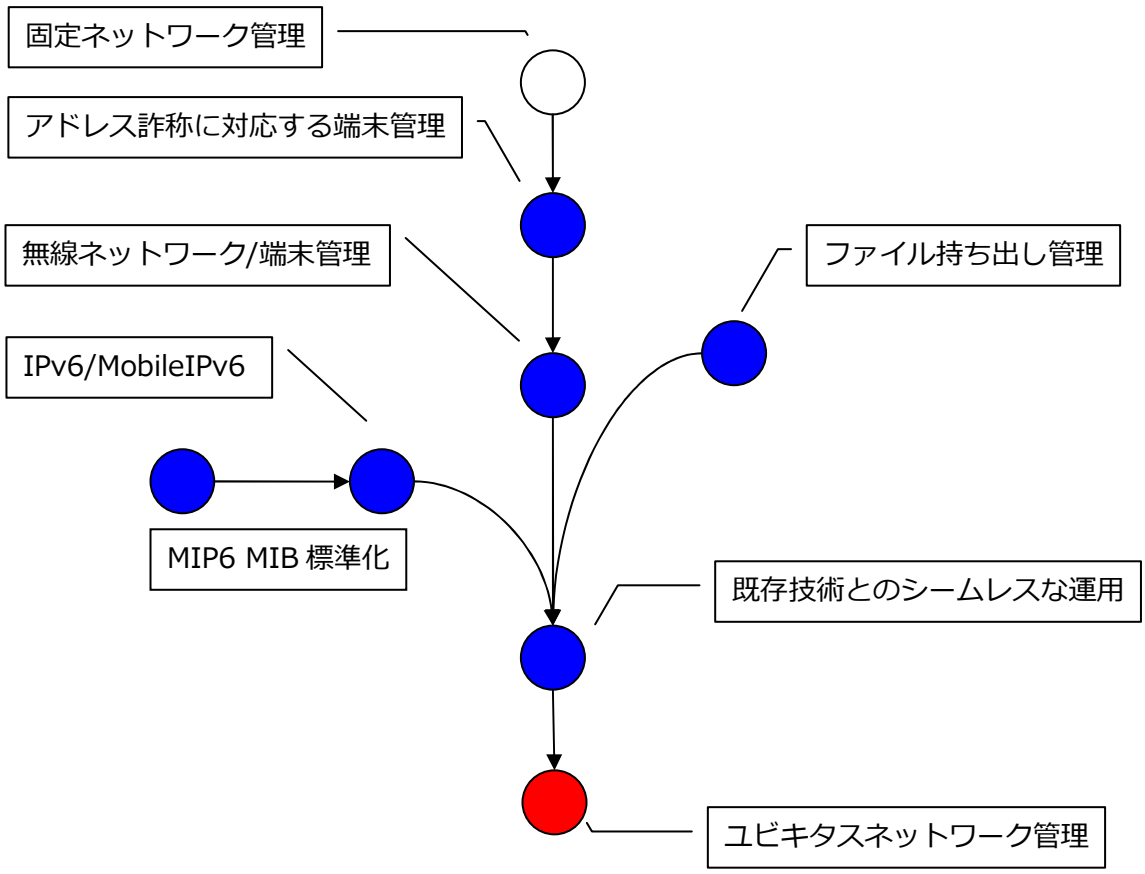


図 44 イントラネットにおける移動端末の接続管理技術の研究開発概要

本研究開発によって、今後の移動端末を主体とした端末接続の管理技術を確立した。端末管理の基盤となる

アドレスの詐称に対応する端末管理技術

を確立し、それらを

無線接続端末の移動分析技術

によって管理可能とした。さらに端末上で利用するコンテンツの安全性管理について、

安全なファイル持ち出し管理技術

を確立した。また、製品としての市場性を考慮し、

既存技術とシームレスに運用できる統合技術

を開発するとともに、将来の

次世代ネットワークIPv6に対応できる

システムとした

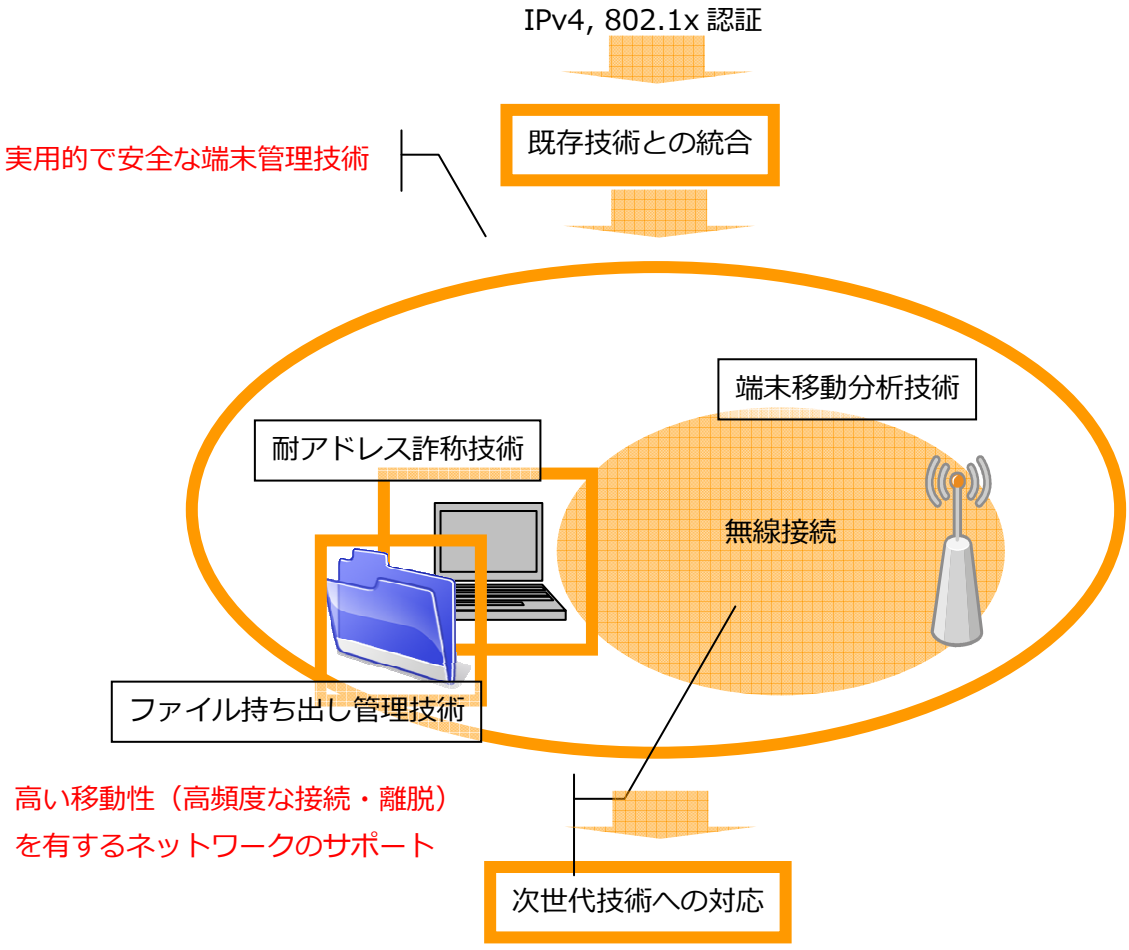


図 45 確立したイントラネットにおける移動端末の接続管理技術の概要

４―１２―２ 大規模ネットワークにおける端末接続管理システムの導入・管理技術

数十万以上の端末を擁するような大規模ネットワークでは、セキュリティシステムの導入にも莫大なコストと手間がかかるため、**導入そのものが大きな技術課題**となっている。本研究開発項目では、大規模ネットワークへのセキュリティシステムの導入およびその管理技術を研究開発した。主な研究開発要素は以下の通り。

- ネットワーク資産の自動発見技術
- 大規模ネットワークにおけるセキュリティシステムの自動最適化技術
- ネットワーク要素の自動構成技術
- ネットワーク構成の自動発見技術

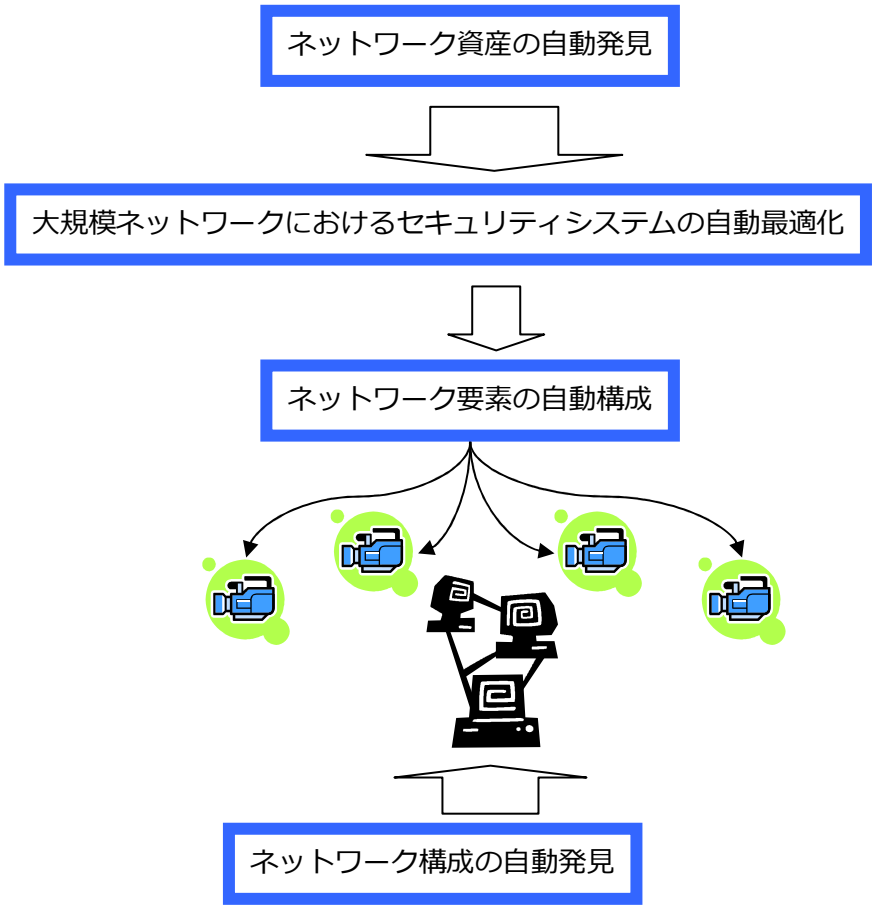


図 46 大規模ネットワークにおける端末接続管理システムの導入・管理技術の研究開発概要

本研究開発によって、大規模ネットワークでのセキュリティシステム導入の大きな障害になっていた導入コストを大幅に削減することが可能なった。

大規模ネットワークの構成情報を取得・分析する技術

によって、導入対象となっているネットワークの情報を自動的に取得し、配備される大量のセンサに対する適切な構成を生成するとともに、

ネットワーク要素の自動構成技術

によってネットワーク中のセンサを遠隔から設定することで導入コストを大幅に削減

できた。また運用開始後は、システム全体を監視するとともに、問題発生時は、

によって、サーバおよびセンサの両方をバックアップシステムに移行することで、ダウンタイムを最小化し、可用性を大幅に引き上げる技術を確立した。またハードウェア、ソフトウェアを含めた総合的な資産管理技術によって管理すべき対象の一元化を実現した（図 47）。

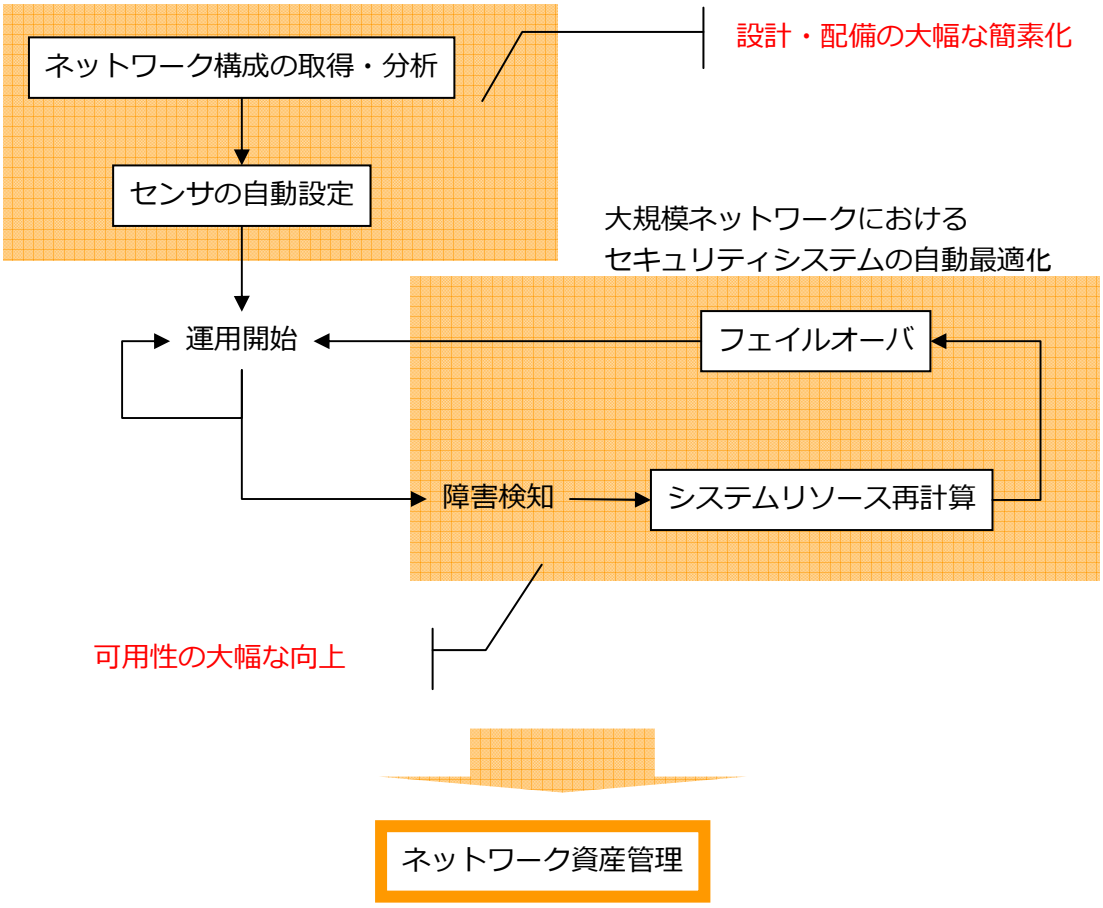


図 47 大規模ネットワークにおける端末接続管理システムの導入・管理技術の研究開発成果

本研究開発によって、大規模ネットワークにおける情報収集能力を大幅な向上を実現し、数十万端末以上のネットワークで実用的な性能と負荷のリニアな特性が得られることを確認し、大規模ネットワークでの基本性能と、サーバ機の増設によって容易にシステムを拡張できる拡張性を確保できた。以下にその計測結果の一例を示す。

表 2 大規模ネットワークにおける性能計測（サーバ仕様）

CPU	Intel Core2 Duo E8200 @ 2
RAM	4.00GB
OS	Windows Vista Business
Database	MSSQLServer2005

表 3 大規模ネットワークにおける性能計測（例）

10万端末を想定した実証実験の計測内容	結果
ネットワーク地図の呼び出しから絞込み画面の表示まで	1秒
絞込み画面の表示よりネットワーク地図（サマリ）が表示されるまで	18秒
ネットワーク地図(サマリ)から詳細の地図が表示されるまで	4秒
詳細地図の更新の開始から絞り込み画面の表示まで	1秒
絞り込み画面の表示より更新の完了まで	29秒

５　参考資料・参考文献

５－１　研究発表・講演等一覧

外国発表論文

Kazuhide KOIDE, Glenn Mansfield Keeni, Nguyen Thanh Trung,Norio Shiratori,"A New Concept in Ubiquitous Network Management: Guest Node Monitoring -Applications of the MobileIPv6-MIB -," The 2007 International Symposium on Applications and theInternet(SAINT2007), Hiroshima, Jan. 2007.

Egon Hilgenstieler, Elias P. Duarte Jr., Glenn Mansfield Keeni, Norio Shiratori, "Improving the Precision and Efficiency of Log-based IP Packet Traceback," 50th IEEE Global Communications Conference (IEEE GLOBECOM'2007), pp. 1-5, Washington D.C., U.S.A., 2007.

口頭発表

- Masahiro Nagao, Glenn Mansfield Keeni, Takuo Suganuma, Kazuhide Koide and Norio Shiratori, "Detecting and Diagnosing Events from Monitored Data in a Wide Area Network", Proceedings of the 2006 IEICE Society Conference, BS-7-2, pp.S25-S26, 2006.

- Glenn Mansfield Keeni, Masahiro Nagao and Norio Shiratori, "Event Based Management",第３回先端的ネットワーク&コンピューティングテクノロジワークショップ予稿集, pp.76-79, 2006.

- 反射型 DoS 攻撃のための Hash-based Traceback 方式の拡張, 佐藤良信・大森孝雄（NTT 東日本）, 角田　裕（東北大）, 太田耕平, Glenn Mansfield Keeni（サイバー・ソリューションズ）, 加藤　寧, 根元義章（東北大）, 2007 年電子情報通信学会総合大会 B-7-123

- 福田啓一、小出和秀、グエン　タン　チュン、キニ　グレン　マンスフィールド、白鳥則郎、“MobileIPv6 ネットワーク管理における移動端末情報の監視手法”、電子情報通信学会 IN 研究会（仙台）（2007 年 9 月 20 日）

- 福田啓一、小出和秀、キニ　グレン　マンスフィールド、白鳥則郎、“ネットワークモ

ビリティをサポートするネットワーク監視技術の開発”、平成 19 年度情報処理学会東北支部研究会（仙台）（2008 年 2 月 15 日）

- 小出和秀、他、“IP ネットワーク管理の新しいフレームワーク”（ポスター発表）、2008 年春 WIDE 合宿（浜松）（2008 年 3 月 3-6 日）

- Kazuhide Koide, Masahiro Nagao, Satoshi Utsumi, Glenn Mansfield Keeni, Norio Shiratori, “Sifting through Monitored Data: the Difficulties and the Workaround”, 第 6 回情報科学技術フォーラム(FIT2007), 2007 年 9 月

- Kohei OHTA, Glenn Mansfield KEENI, “Building secure and reliable network for regional health care system“, 2008 Sendai International Workshop on New Information Technologies and Related Health and Welfare Topics, 6th, Feb. 2008, Hotel Sendai Plaza

報道発表

「情報通信分野の研究開発委託　仙台の 2 ベンチャー採択」平成 18 年 9 月 7 日　河北新報