管理番号＃１８－２０２

平成１８年度
研究開発成果報告書

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１９年４月

情報通信研究機構

平成１８年度　研究開発成果報告書

（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。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 100 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。

移動端末管理の基本的な問題は「ネットワーク管理者の目が行き届かない状態」が存在することにある。さらに、移動端末の場合は 2 種類のネットワーク管理者が存在する。一方はその移動端末の管理者で、その本来の所属ネットワークの管理者であり、もう一方は、その移動端末が移動した先で接続する受け入れネットワークの管理者である。

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 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。

全体として、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入りつつあるといえる。それにともない周辺技術の研究開発も進んでいる。

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。移動体市場および関連技術の研究開発の活性化は、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。

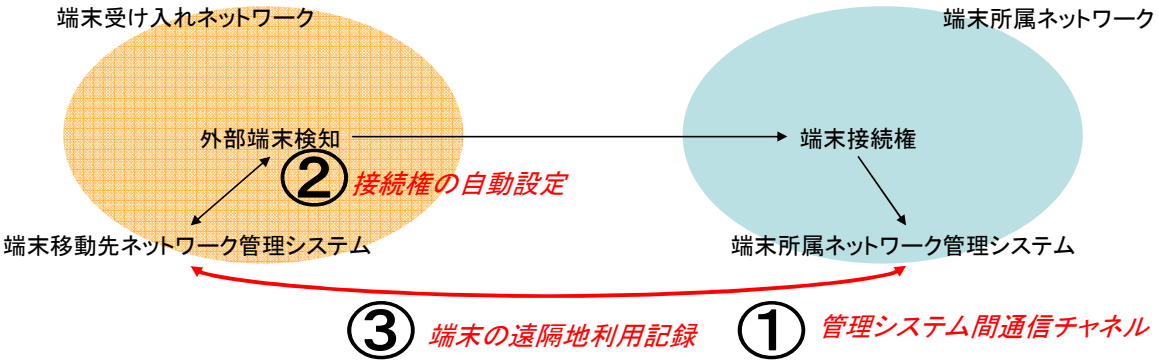


図 1 本研究開発の要素技術構成

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。

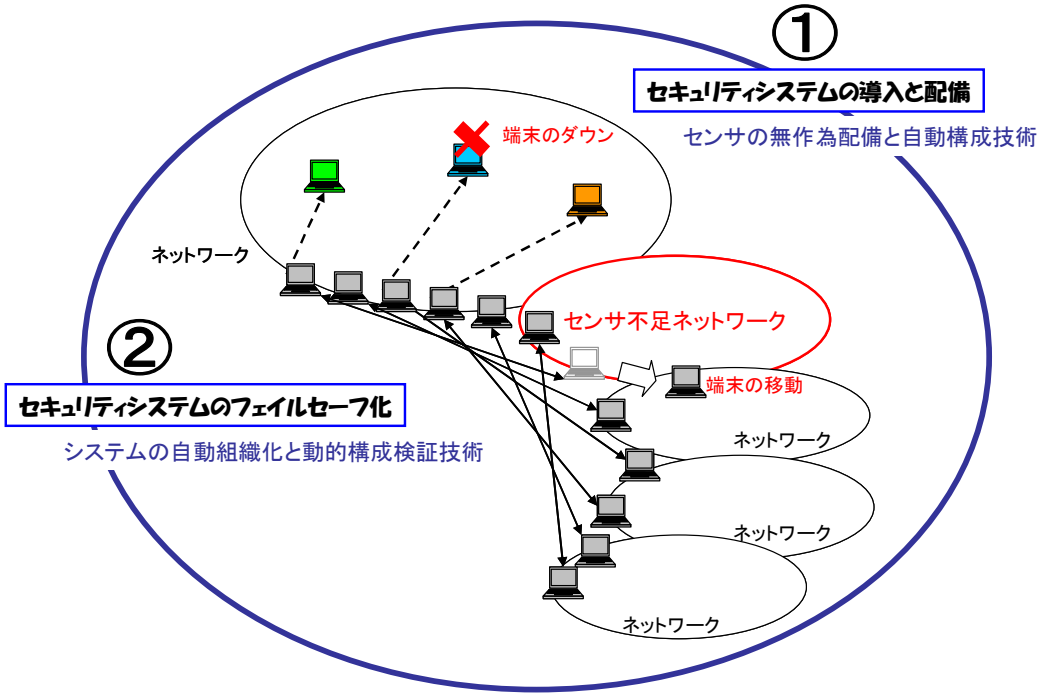


図 2 大規模ネットワークを柔軟に管理できる端末管理システム

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

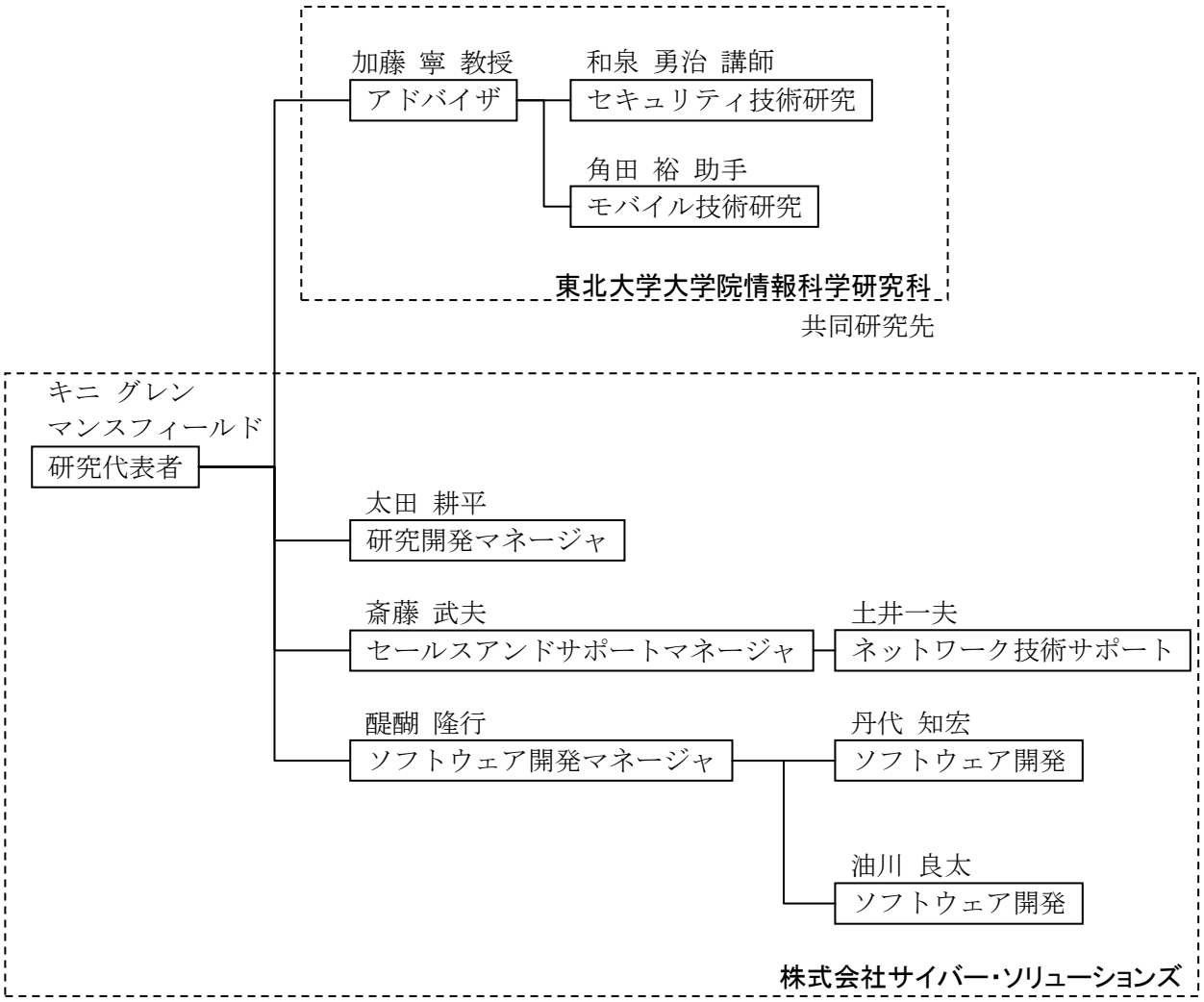
金額は非公表

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



４　研究開発実施状況

図 3に本研究開発の平成 18 年度末時点での実施状況を示す。

本研究開発では、基盤となる製品として主に固定端末の接続管理を実現する既存の NetSkateKoban を想定し、その上に提案した新技術を開発、製品化することで、研究開発後の素早い市場投入を実現する。

平成 18 年度は、19 年度に本格化する移動端末管理、および自動発見、自動構成技術の基盤となる端末の常時監視を実現するネットワーク管理機能の統合、および移動端末認証・制御の基盤となるマルチベンダ検疫機能を研究開発し、当初計画通りの目標を達成した。

また、19 年度の研究開発の基盤となる調査研究を実施し、移動端末および無線接続管理の現状と課題、さらには標準化動向との関連を明らかにし、今後の方向性を示した。

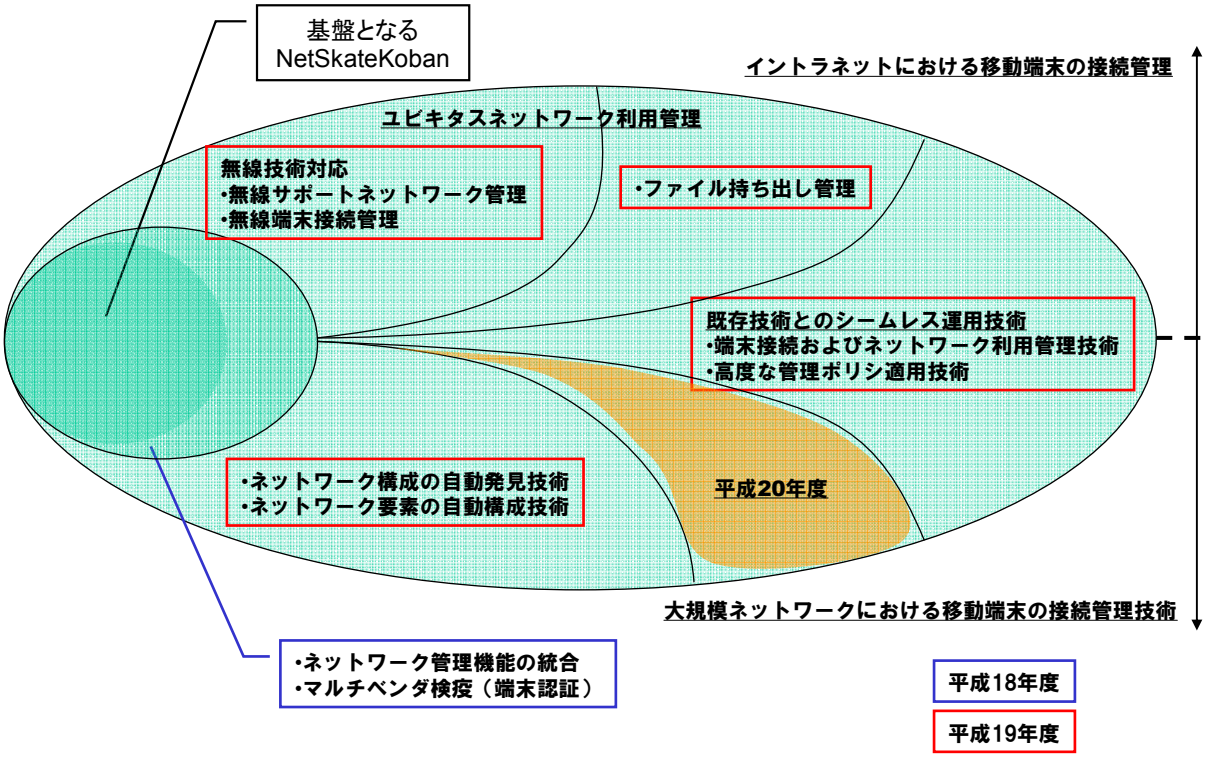


図 3 研究開発の実施状況

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を統合した。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 4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。

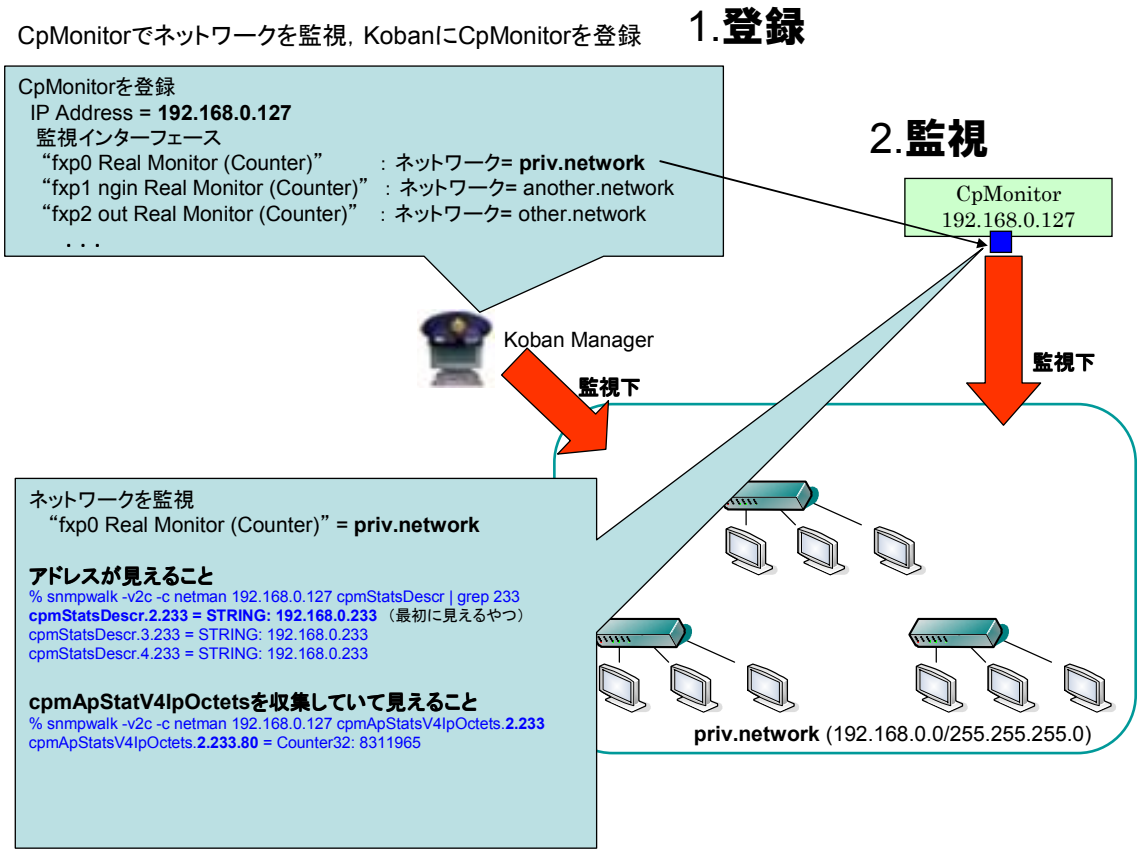


図 4 ネットワーク管理機能の統合

図 5に本研究開発によって実際に統合されたトラフィックセンサの画面例を示す。センサのタイプとして、新たに CpMonitor が追加され、従来の端末センサと同様に管理可能であることを示している。

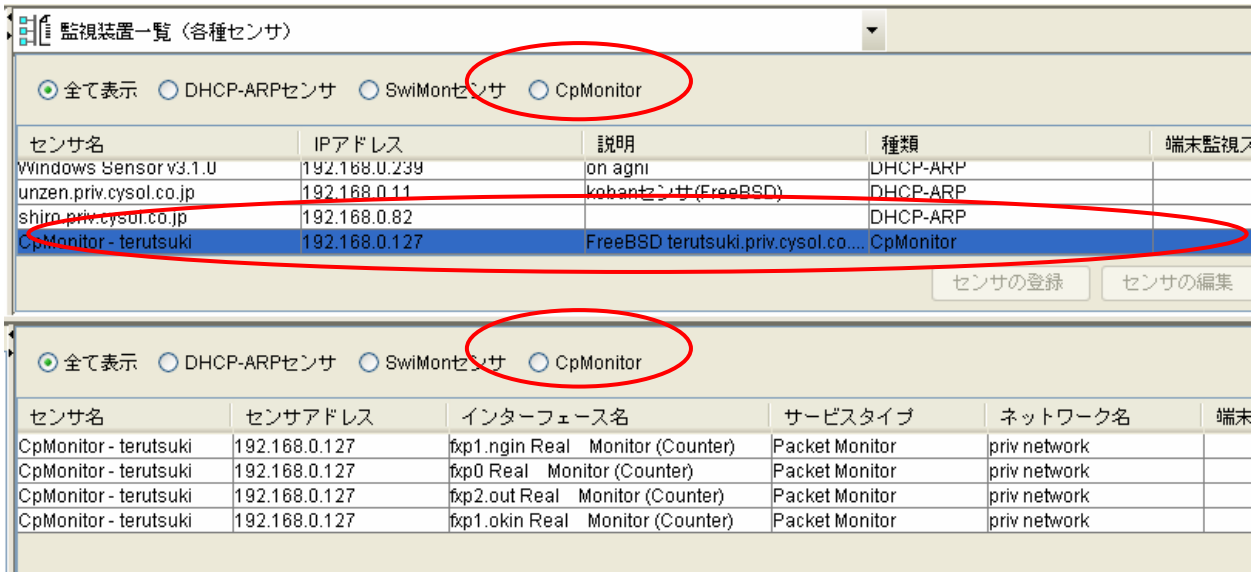


図 5 トラフィックセンサを統合した監視機能の画面例

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 6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、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、アクションの動作により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。

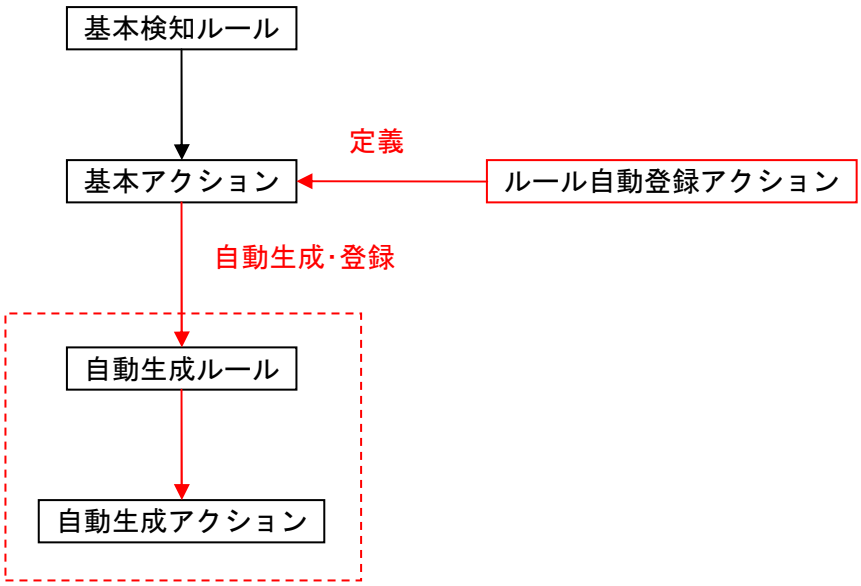


図 6 トラフィック情報に基づくポリシ設定の概要

図 7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。

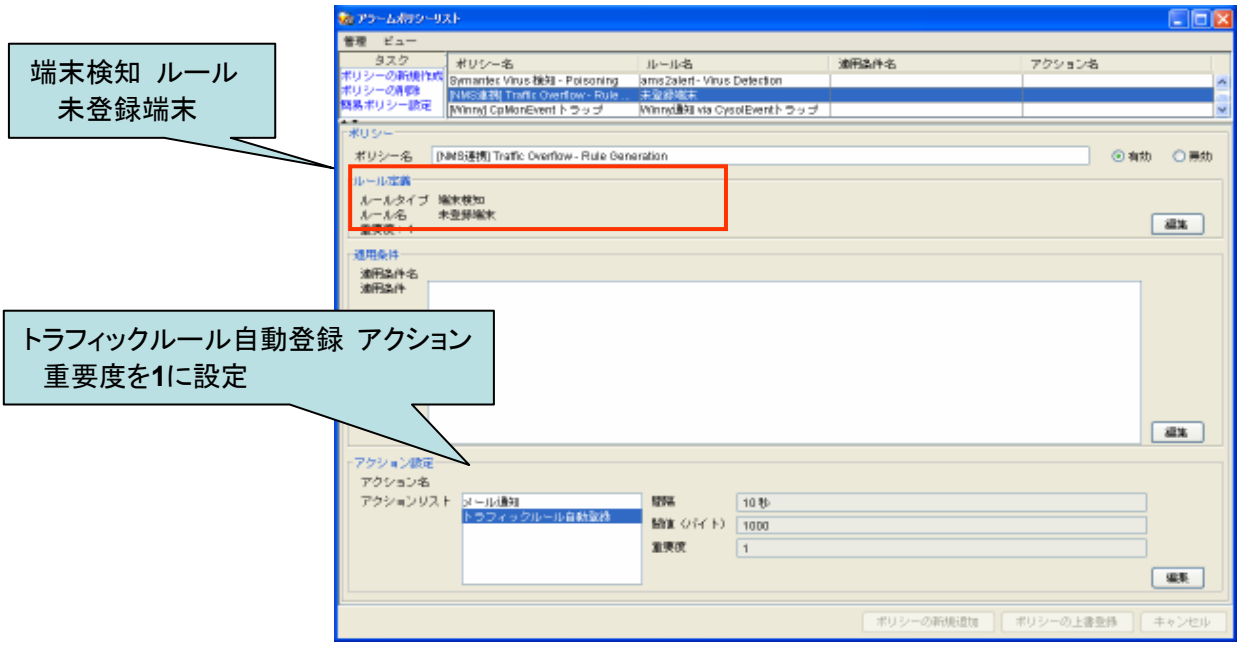


図 7 トラフィックルール自動登録の設定画面例

図 8に、ルール自動登録によって登録されたルールに対するアクションの定義例を示す。本定義（設定）によって、最終的なアクションを定義することとなる。

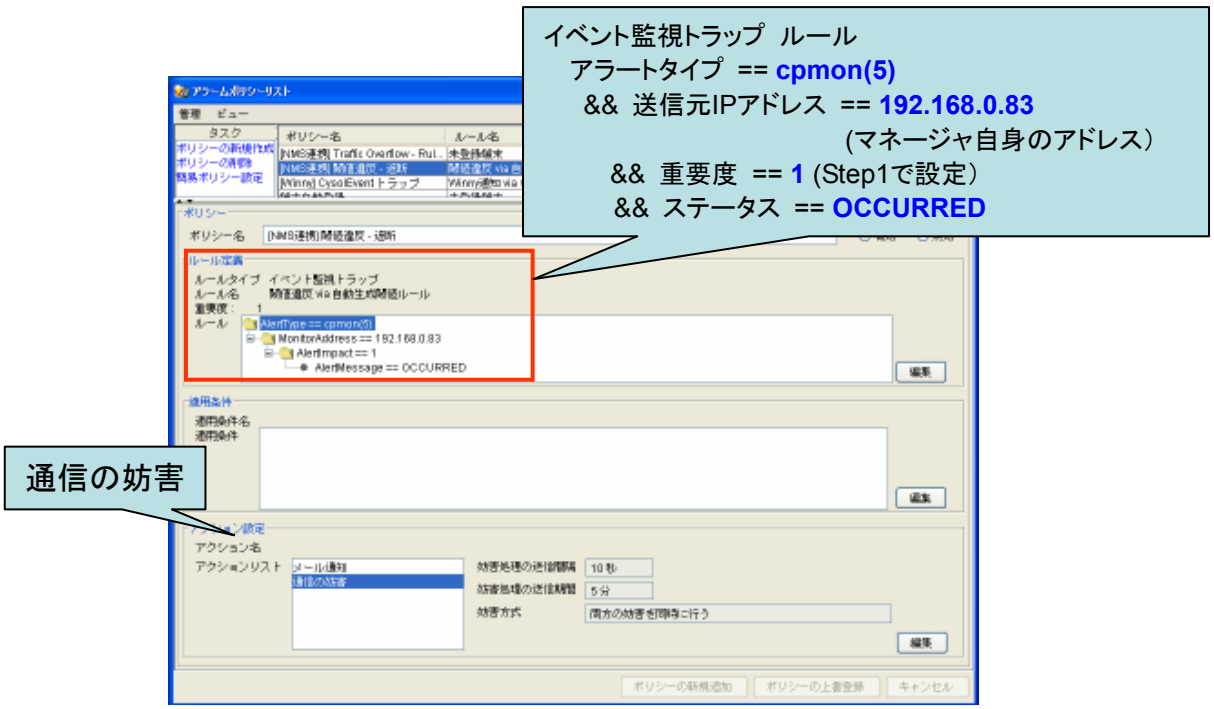


図 8 自動生成されるルールによって実行されるアクションの設定画面例

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 9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（トラフィック情報）をおこなっているか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、その両者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。

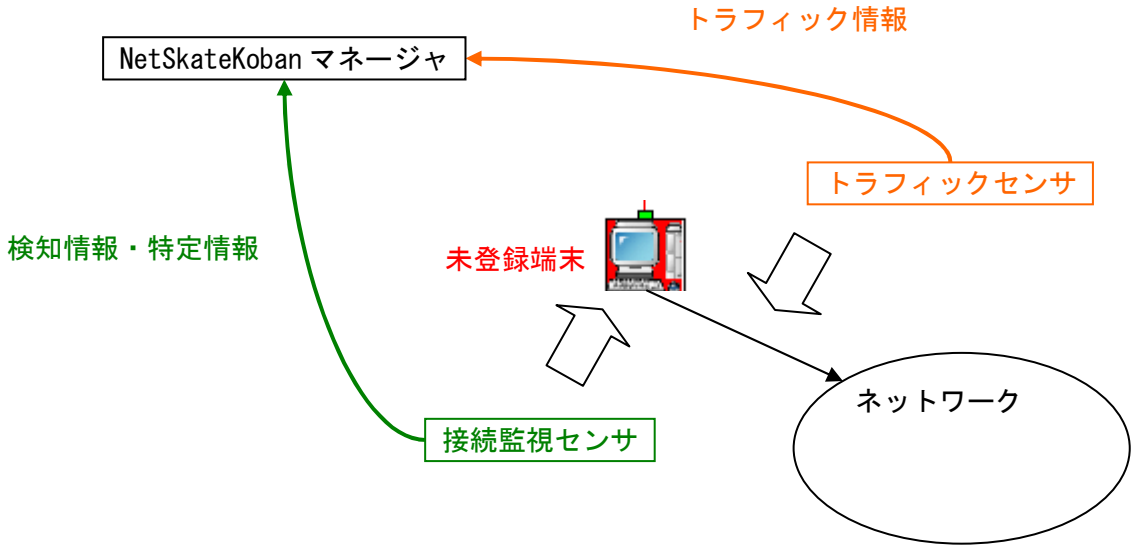


図 9 端末管理とネットワーク管理の協調動作の概要

図 10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。

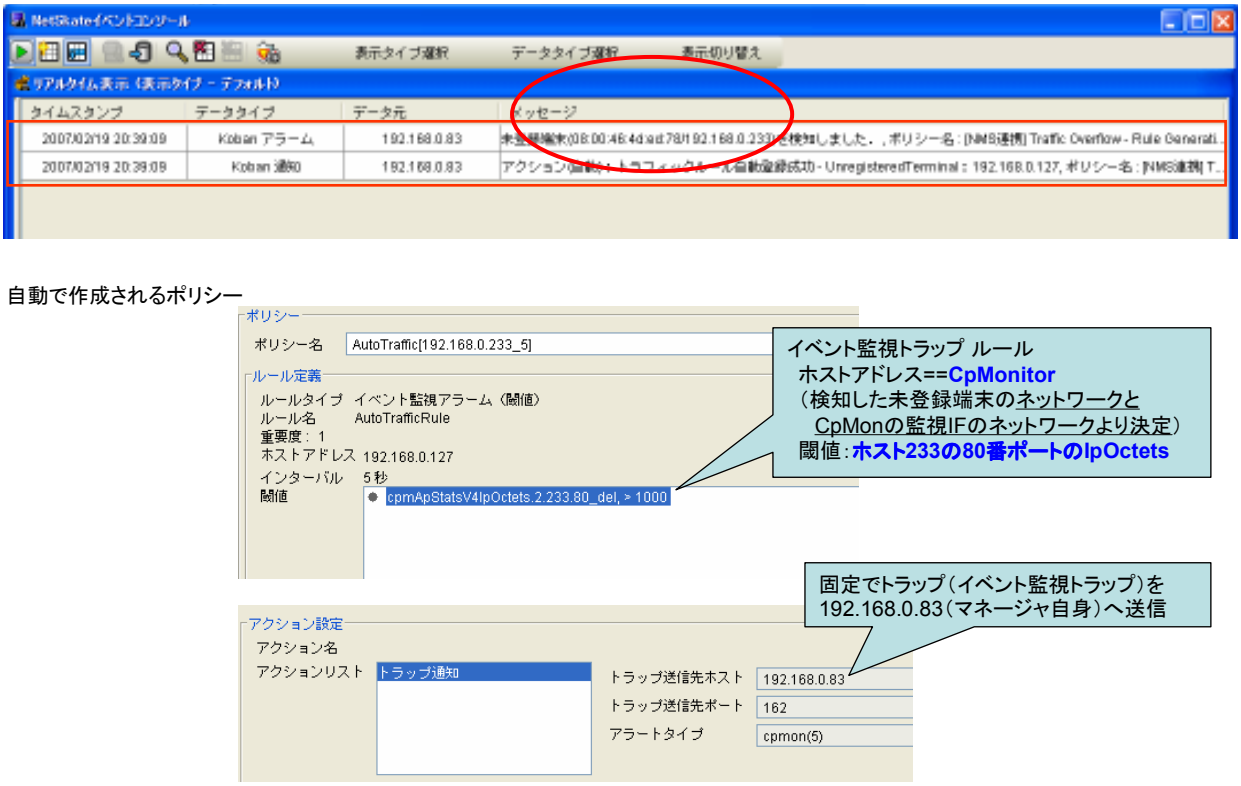


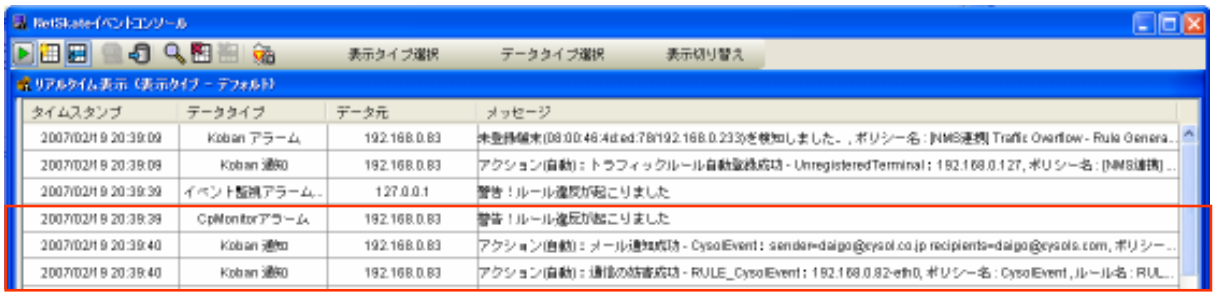
図 10 トラフィック監視と端末追跡・特定機能の動作例

図 11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

イベントコンソール



Kobanブラウザ ― 通信妨害中の端末一覧

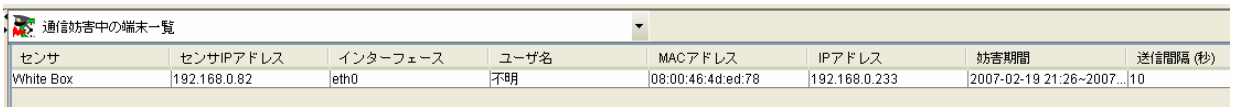
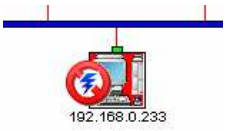


図 11 連動動作：未登録端末検知 → 自動トラフィック監視 → 自動遮断

図 12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。

ネットワークマップ



検知端末一覧

マネージャ動作ログ

図 12 管理状態の可視化および運用画面例

図 13に、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. 未登録端末を検知：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。

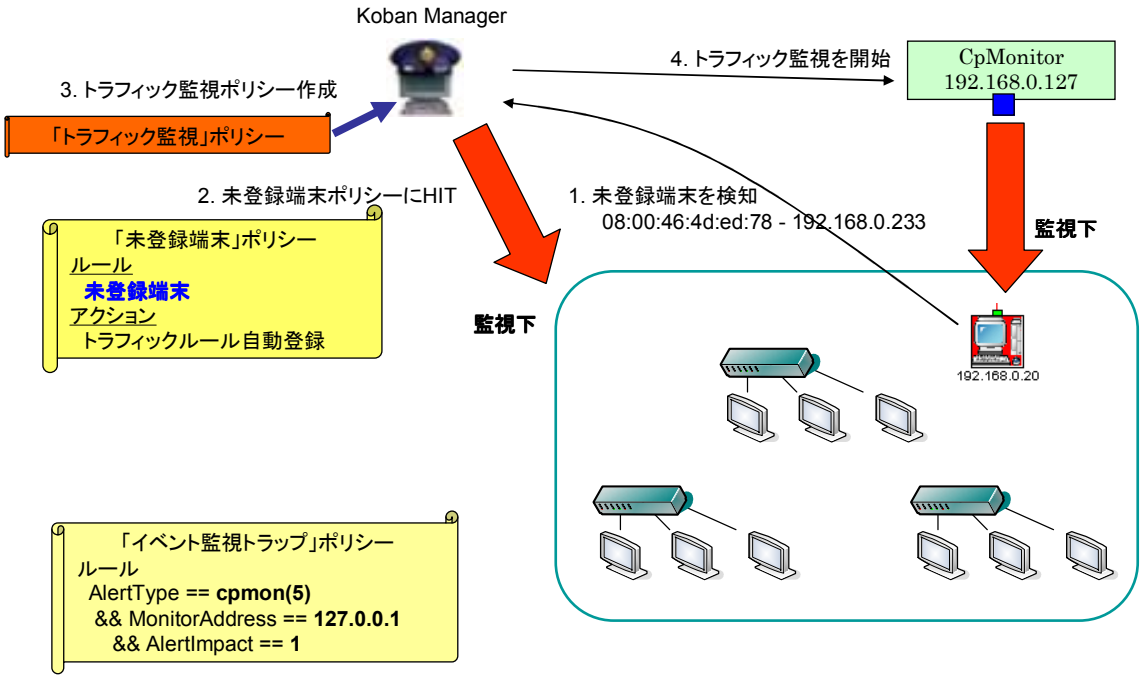


図 13 トラフィック監視機能の統合による動作例

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 14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。

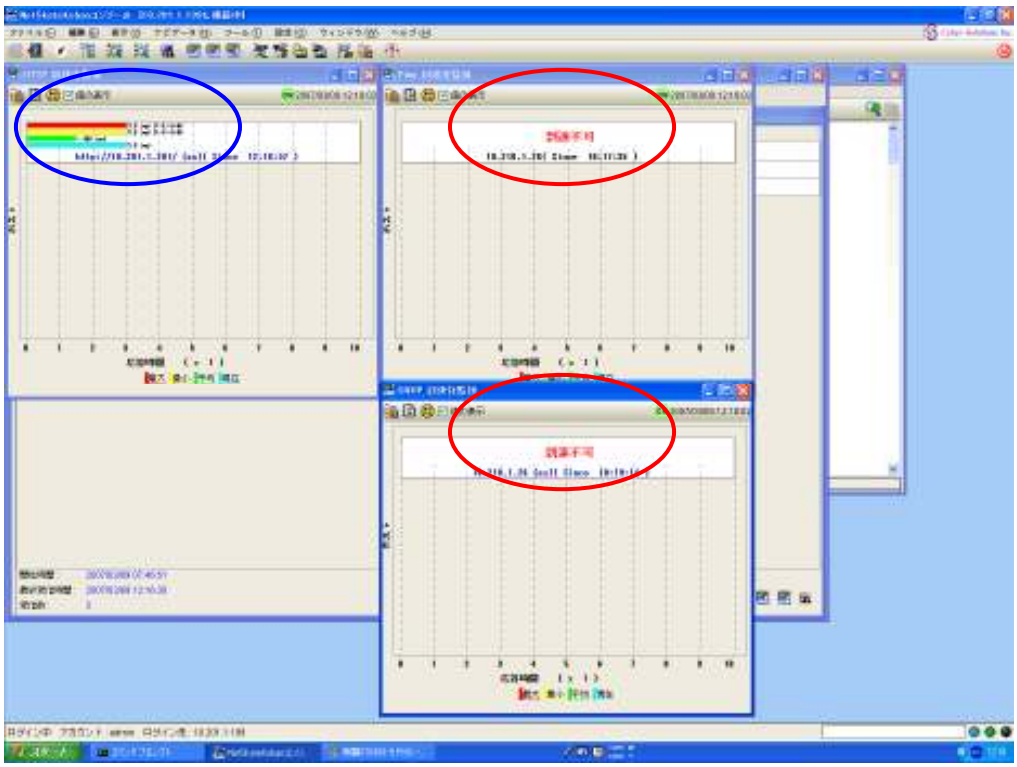


図 14 到達性管理の画面例

図 15に、統合されたネットワーク管理機能を用いたリソース管理の画面例を示す。図中の円グラフで示したものが、当該機器の HDD およびメモリの利用状況を示しており、青が使用されている分、黄色が空き部分を示している。

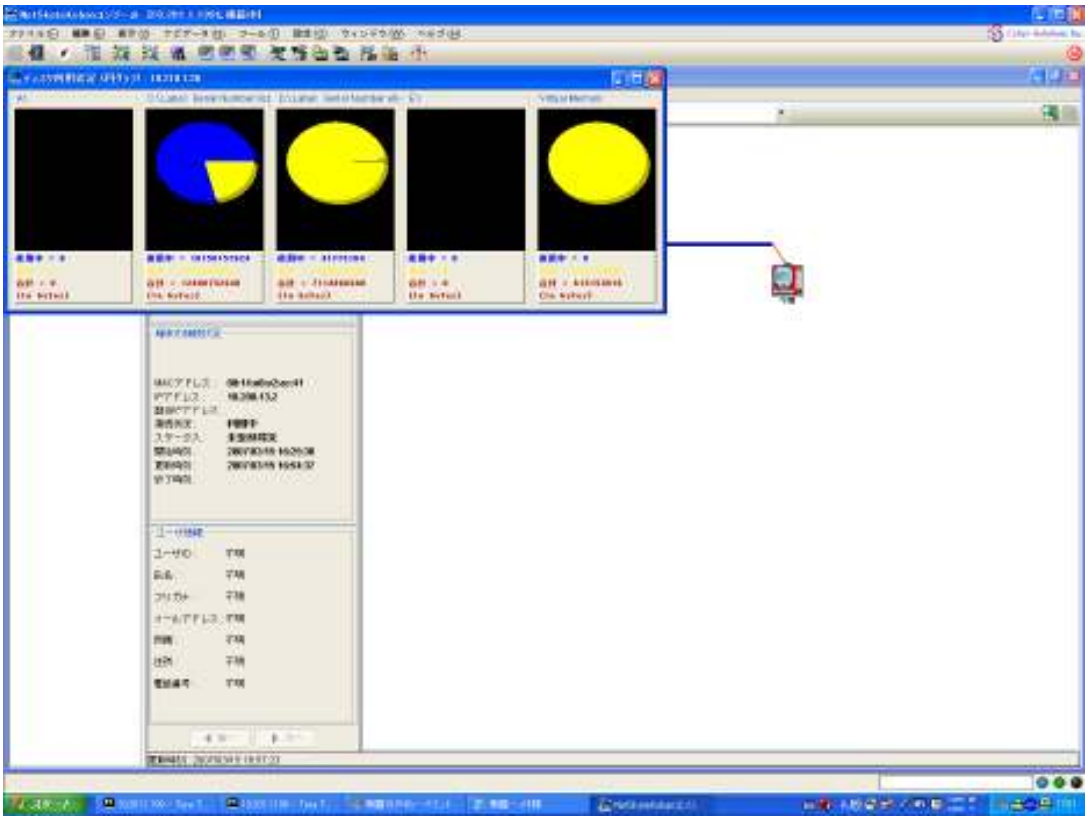


図 15 リソース管理の画面例

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。

- ■　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
- ■　トラフィック監視結果から、発信元の追跡・検索機能連携
- ■　セルフモニタリング、システムリソース管理機能統合

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には、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必要となる。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の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。

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 16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。

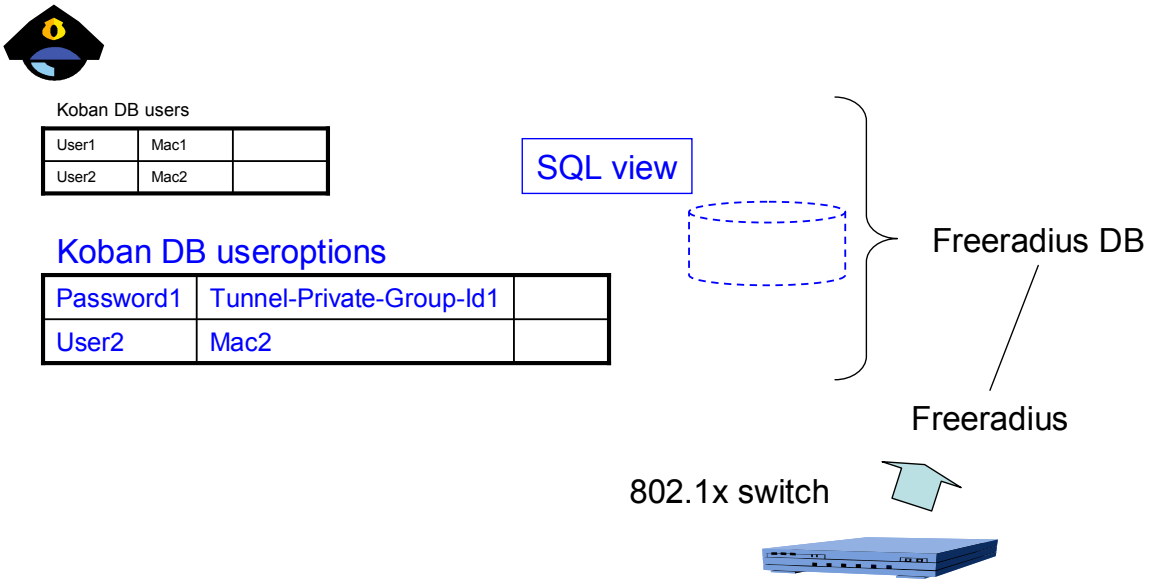


図 16 マルチベンダに対応するユーザ管理および認証技術の概要

図 17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。

---

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

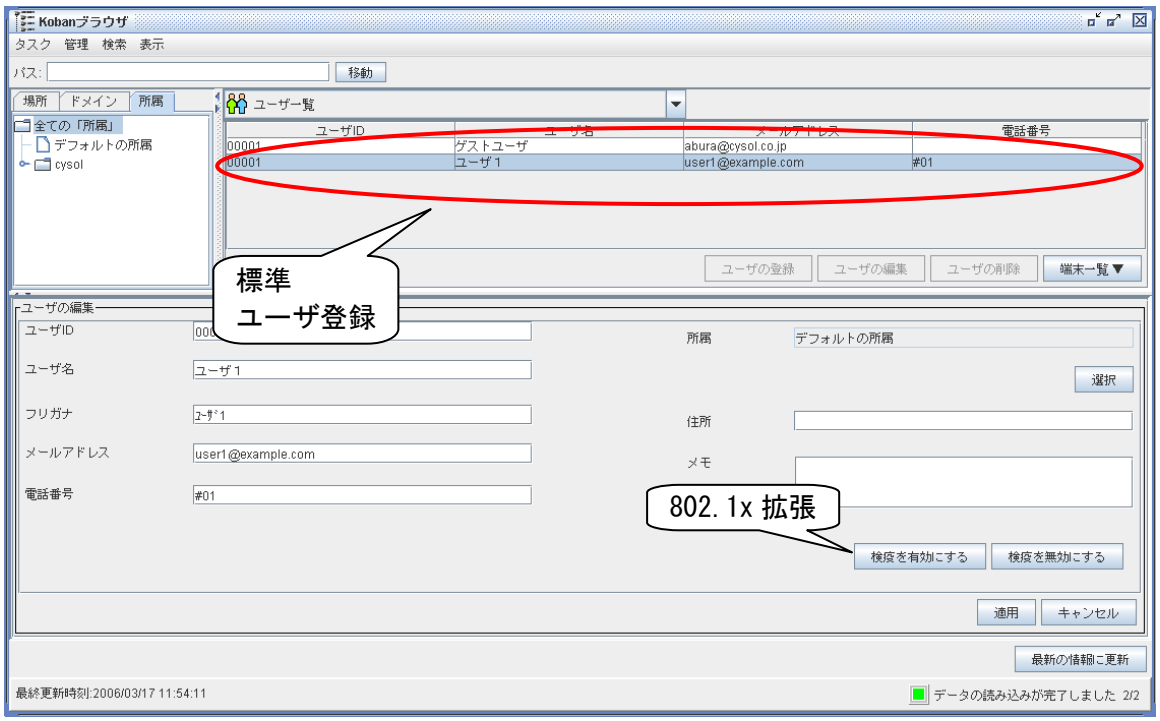


図 17 拡張ユーザ登録の画面例

図 18に図 17で示した拡張ユーザ登録画面で選択された 802.1x のための拡張ユーザ情報の編集画面例を示す。RADIUS で利用するアカウント、パスワード情報以外に、接続先のネットワーク情報を示す VLAN 情報、接続プロトコル情報などのフィールドが設けられている。これらの情報がデータベースに格納され、データベースレベルでの View を活用することで、端末管理システム、RADIUS 認証エンジンの双方から共通の情報にアクセスできる環境を実現した。

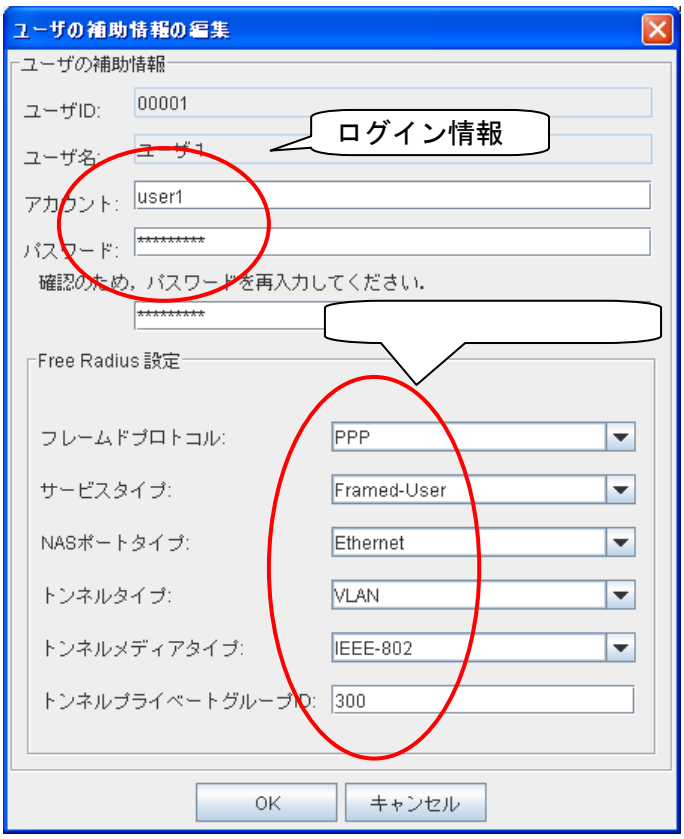


図 18 802.1x に対応したユーザ情報の編集画面例

図 19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。

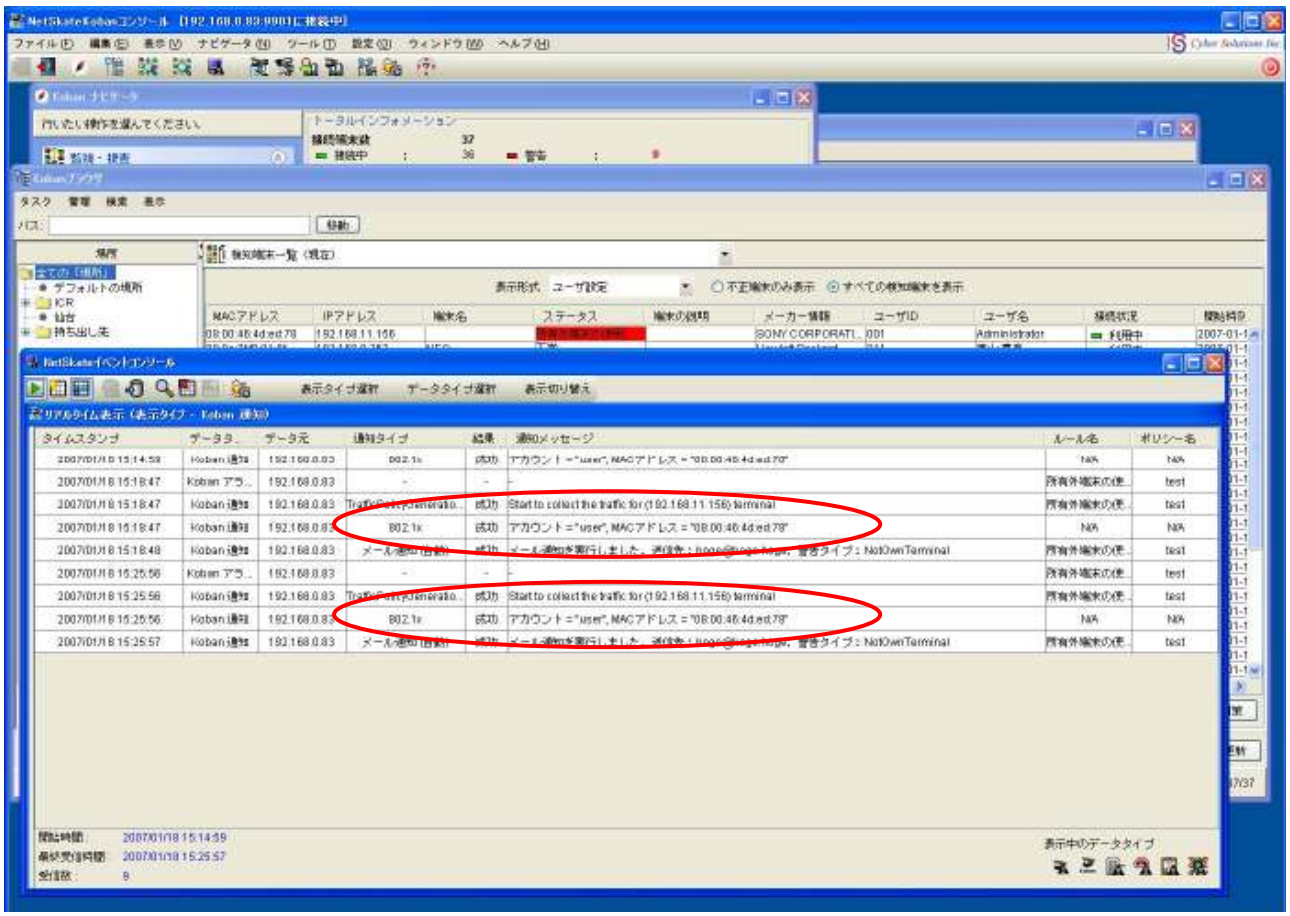


図 19 認証状態の管理画面例

図 20にネットワーク管理プロトコル SNMP を活用した再認証の動作概要を示す。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。

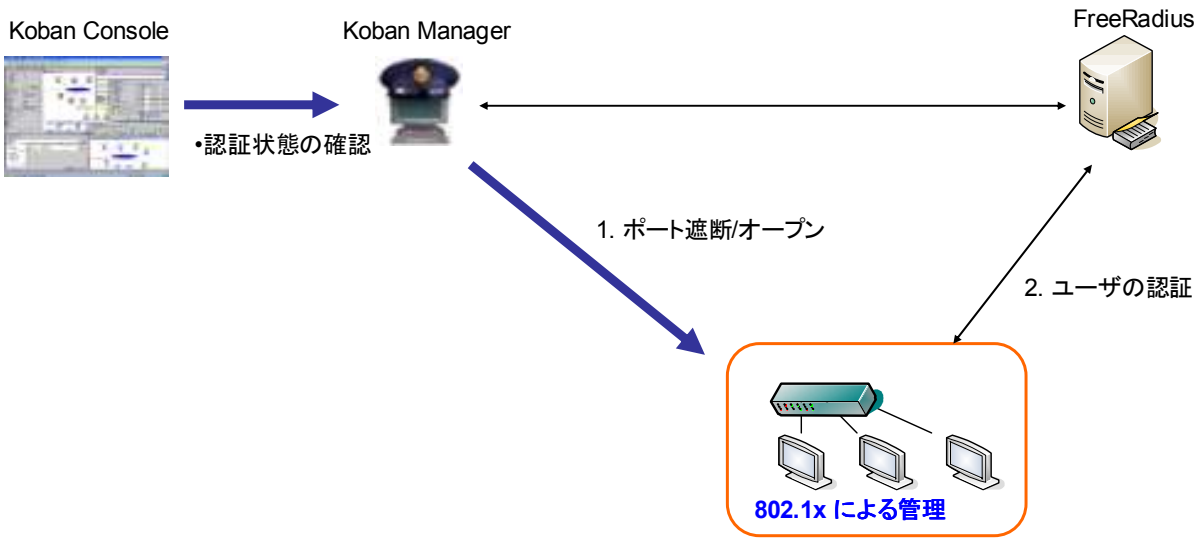


図 20 ユーザの再認証の動作概要

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 21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二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。

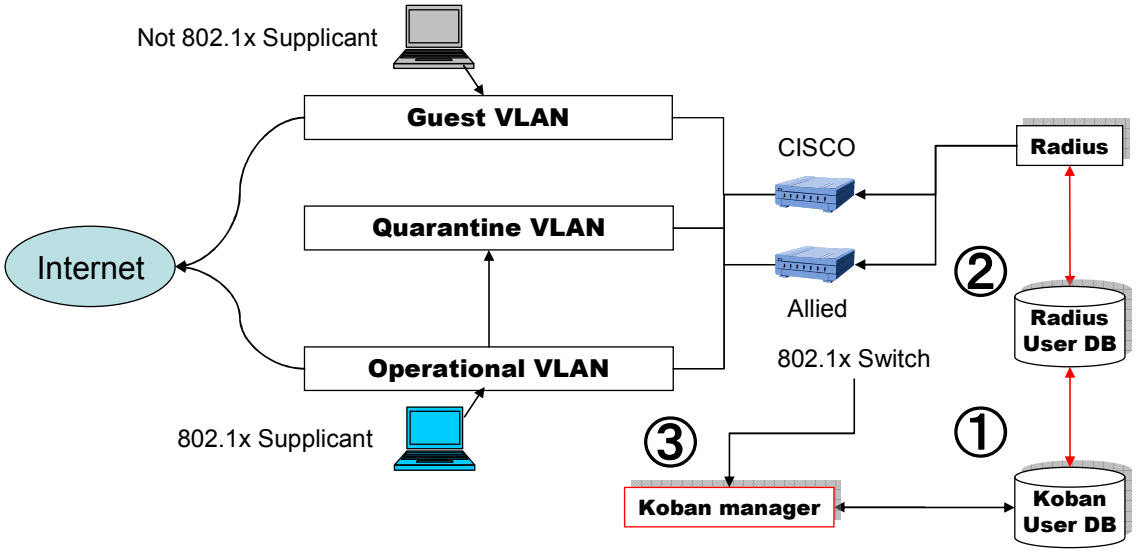


図 21 端末隔離技術の概要

図 22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. GuestVLAN 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

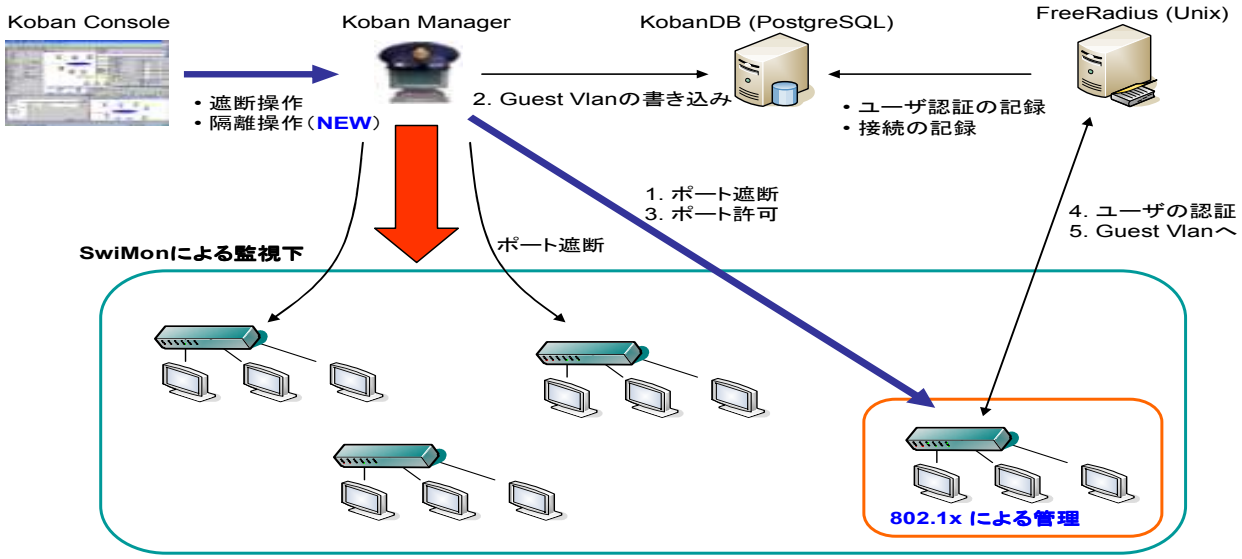


図 22 端末強制隔離のシステム要素概要

図 23に隔離動作のメニュー画面例を示す。画面では従来の「遮断」にかわる選択肢として用意されたメニューを示しているが、一般的な管理メニューにも同様の項目を実装した。

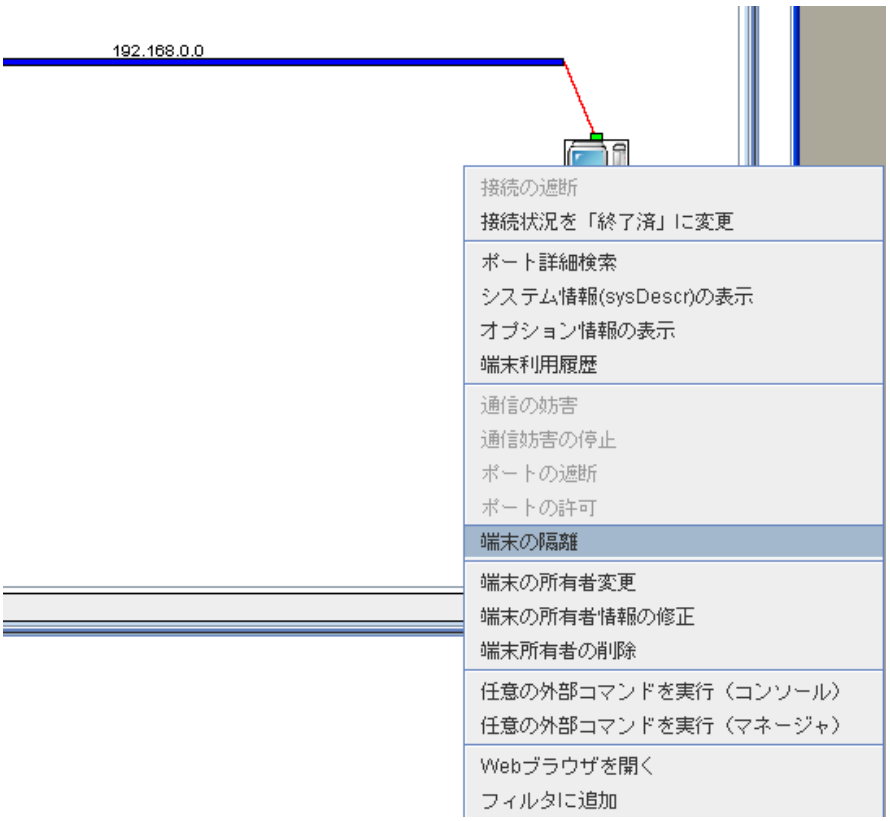


図 23 隔離操作のメニュー画面例

図 24に上記のメニューからよばれる隔離動作の例を示す。明示的に隔離先を指定することで、隔離を目的する場合以外にも、任意の VLAN に端末を移動させることが可能となっている。

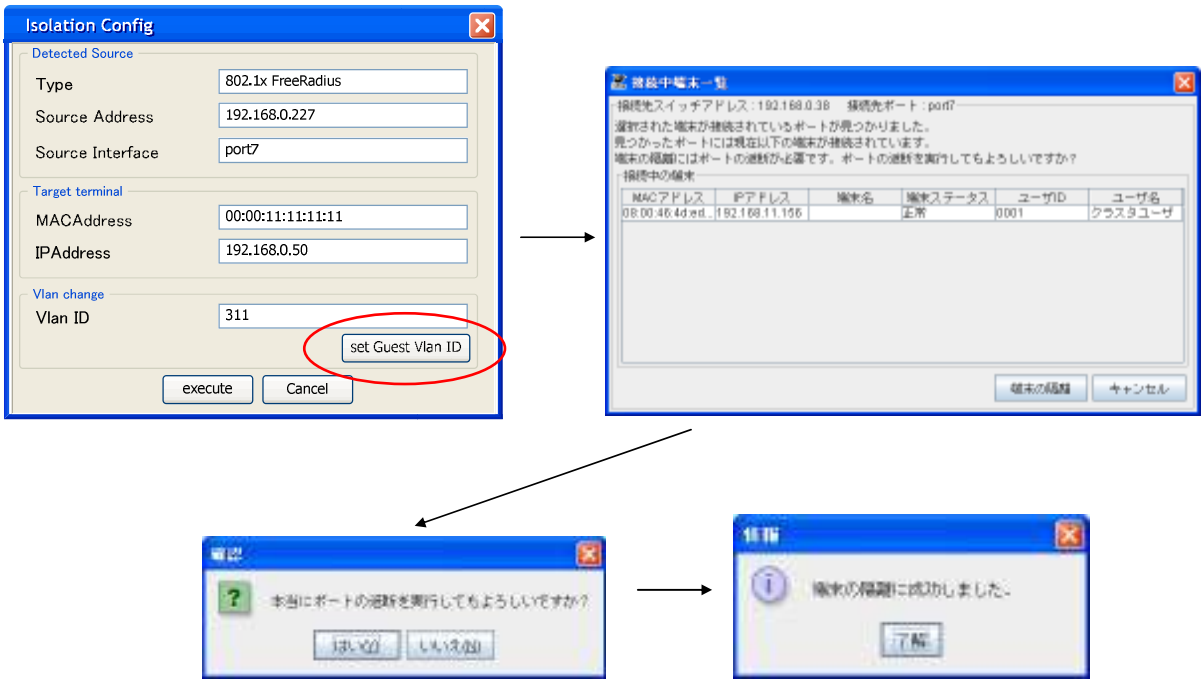


図 24 隔離操作の画面例

③ 不正検知機能と連動した自動端末管理機能

図 25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。

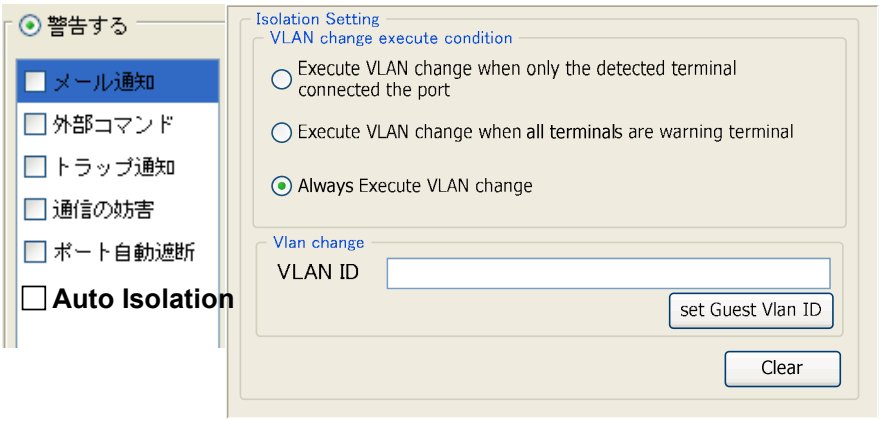


図 25 自動隔離機能の設定画面例

図 26に 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。

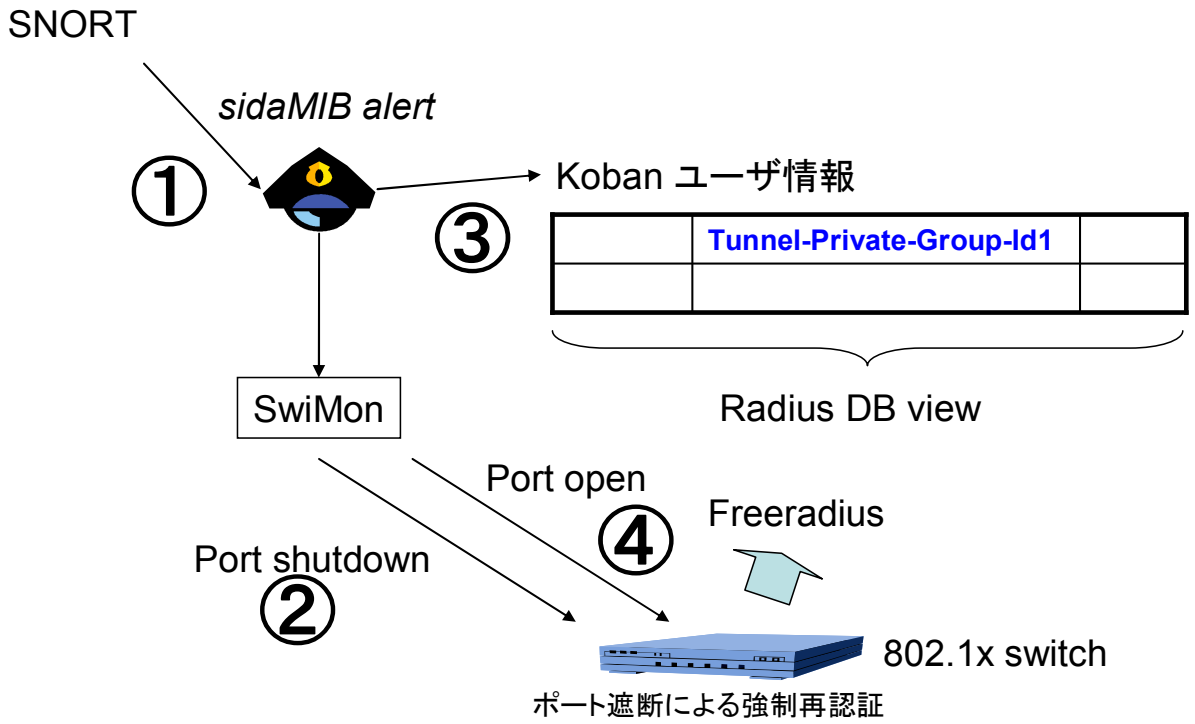


図 26 SNORT と連動した自動隔離機能

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。

- RADIUS 認証の統合および SNMP 管理技術による再認証機能
- SNMP 管理技術、および動的 VLAN 技術による遠隔（強制）隔離機能
- 不正検知と連動した自動遮断、隔離機能

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

４－３－１ 移動性を管理できる NetSkateKoban 実現のための設計要件調査概要

移動端末に関する技術の研究開発は、現在も進行中であり、将来の主流となる技術がどうなるかは、いまだ確定的ではない。一方で、携帯型デバイスは、従来のノート PC 以外にスマートフォンなどが台頭するとともに、構内電話、携帯電話などの従来はインターネット接続との接点は少なかったデバイスのインターネット接続も進んでおり、研究開発の方向性と優先度は慎重に検討されなければならない。

本研究開発は、以下の 2 点について調査研究することによって、次世代のイントラネットセキュリティシステムとして備えるべき機能の方向性を明らかにする。

1. ゲスト端末の安全な接続技術
   ゲスト端末等によって、動的に変化するネットワーク構成を管理し、様々な端末の接続を安全に管理する技術の設計要件を調査研究する。

2. Mobile IP 管理に関する標準化動向
   申請者らが提案し、標準案として RFC（Request For Comments）化された MobileIP 管理技術の応用の可能性と、他の標準化動向について製品化のための設計要件を調査研究する。

４－３－２移動性を管理できる NetSkateKoban 実現のための設計要件調査実施状況

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 を終身とした要件、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。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く、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ことなる無線アクセスポイントへのハンドオーバがおこっており、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

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

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

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

本研究開発サブテーマは当初の計画を 100%実施し、以下の調査研究を実施するとともに、具体的な課題および見通しを示した。

- 移動端末主体のネットワークの管理技術
- 管理対象としての移動 IP 端末の重要性

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。

４－４　総括

平成 18 年度の研究開発は、当初の計画通り進捗し、要素技術のみならずそれらを活用した具体的なアプリケーションを実現することができた。

1.　ネットワーク管理技術の統合

本研究開発によって、従来は独立に考えられ、製品化されていたネットワーク管理とセキュリティ管理を高いレベルで統合することができた。

本研究開発では、それぞれを単に統合するだけではなく、セキュリティ管理の観点から、リスクとしてのネットワーク管理の概念を全面的に導入し、管理可能とするとともに、両者の連携が新しいレベルの管理アプリケーションを生み出せることを示した。

具体的には、ネットワークおよびシステムに発生し得る「障害」をセキュリティ管理上のリスクとしてとらえ、ネットワーク上のサーバなど各要素への到達性、およびそれぞれのシステムが有しているリソースの利用率などを監視することで、ネットワークが全体として健全に動作しているかどうかを管理し、問題発生時には、セキュリティ上のリスクとしても捕らえることを可能とした。

また、端末管理技術のもつ端末特定および制御技術、ネットワーク管理技術のもつトラフィック管理、障害管理、リソース管理を連動させることで、ネットワーク現象として不正を検知するとともに、関係の端末を特定し、遮断するといった具体的な対策を可能とした点は世界でも最先端の技術といえる。

これらの技術によって、「外部への大容量トラフィック」といったそれだけでは不正かどうかわからないが、潜在的な情報漏洩の可能性のある現象をトラフィック監視技術で監視し、その発生時に当該端末を遮断する、といった具体的な運用を自動的に実施することも可能となった。

2.　マルチベンダ検疫技術の確立

本研究開発によって、移動する端末、複数の機器の接続管理の基盤となるユーザ認証技術および端末接続制御技術を確立した。

本技術は既存の標準、あるいはデファクトスタンダードとなっている技術のみを活用することで、ベンダに依存しないユーザ認証および機器制御技術を実現した。実現にあたっては、ベンダに依存する動作部分などは、全く別の独立した標準技術で、すでに広く普及しているネットワーク管理プロトコルで補い、同じ機能を複数のベンダで動作可能であることを確認した。

また、本年度に研究開発した統合されたネットワーク管理機能との連携動作も研究開発した。本研究開発によって、ユーザ認証時のみならず、トラフィック観測による不正の検知、侵入検知システムによる不正アクセスの検知時にも、本技術を利用した端末接続の制御を可能とした。

これらの技術によって、前述の「外部への大容量トラフィック」検知時にも遮断ではなく隔離することが可能になる。同様の動作はなんらかの原因で IDS 等に不正と判断される通信を発信した場合でも即座に遮断するのではなく、通信を制限する程度にとどめることができるため、誤検知などの問題に現実的なソリューションを与えるとともに、管理権限のいきとどかない移動端末に安全にネットワークアクセスを提供することも容易になる。

５　参考資料・参考文献

５－１　研究発表・講演等一覧

外国発表予稿

1. 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.

口頭発表

1. 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 ICICE Society Conference, BS-7-2, pp.S25-S26, 2006.

2. 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.

3. 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

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