管理番号＃１８－２０２

平成１９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２０年４月

情報通信研究機構

平成１９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 月の 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、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。

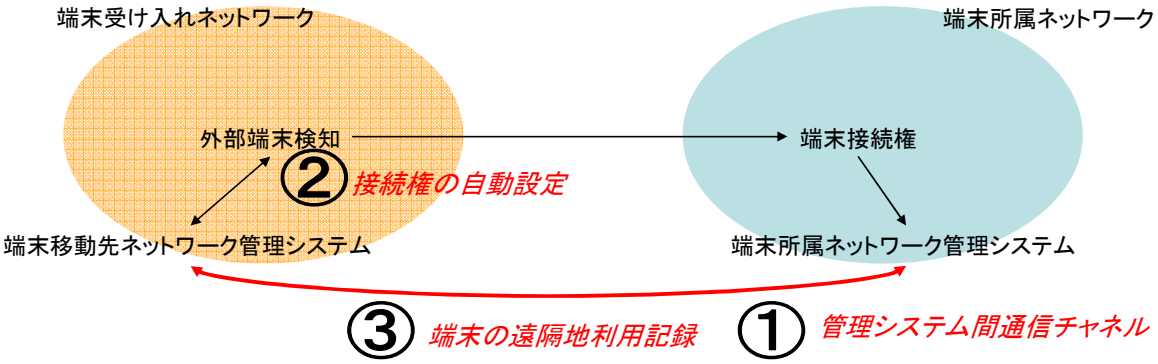


図 1 本研究開発の要素技術構成

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。

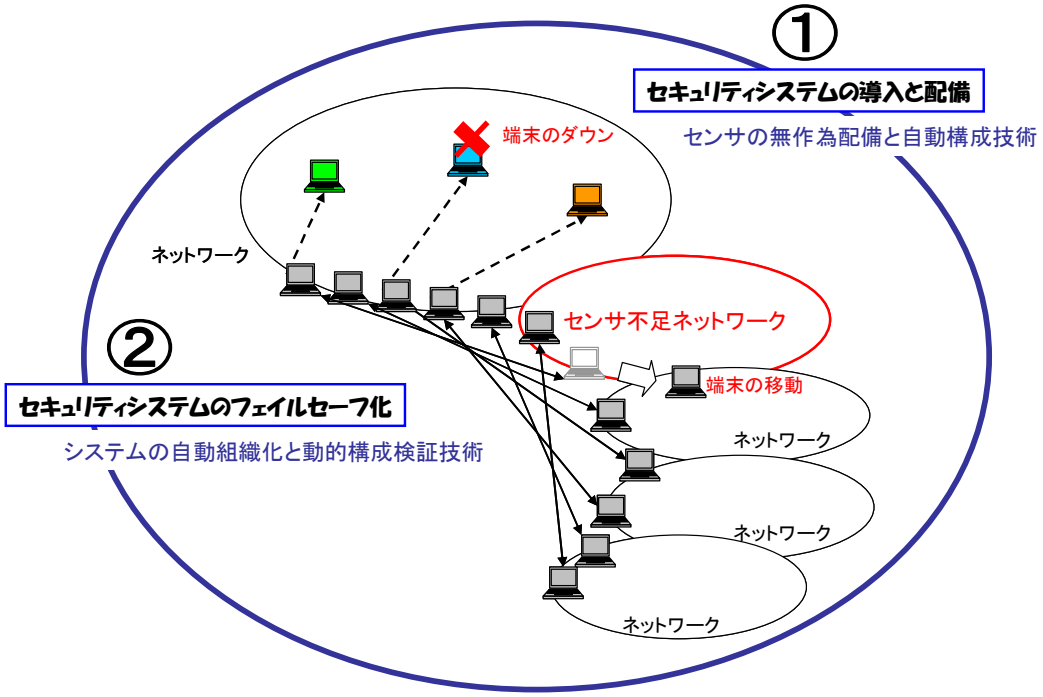


図 2 大規模ネットワークを柔軟に管理できる端末管理システム

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

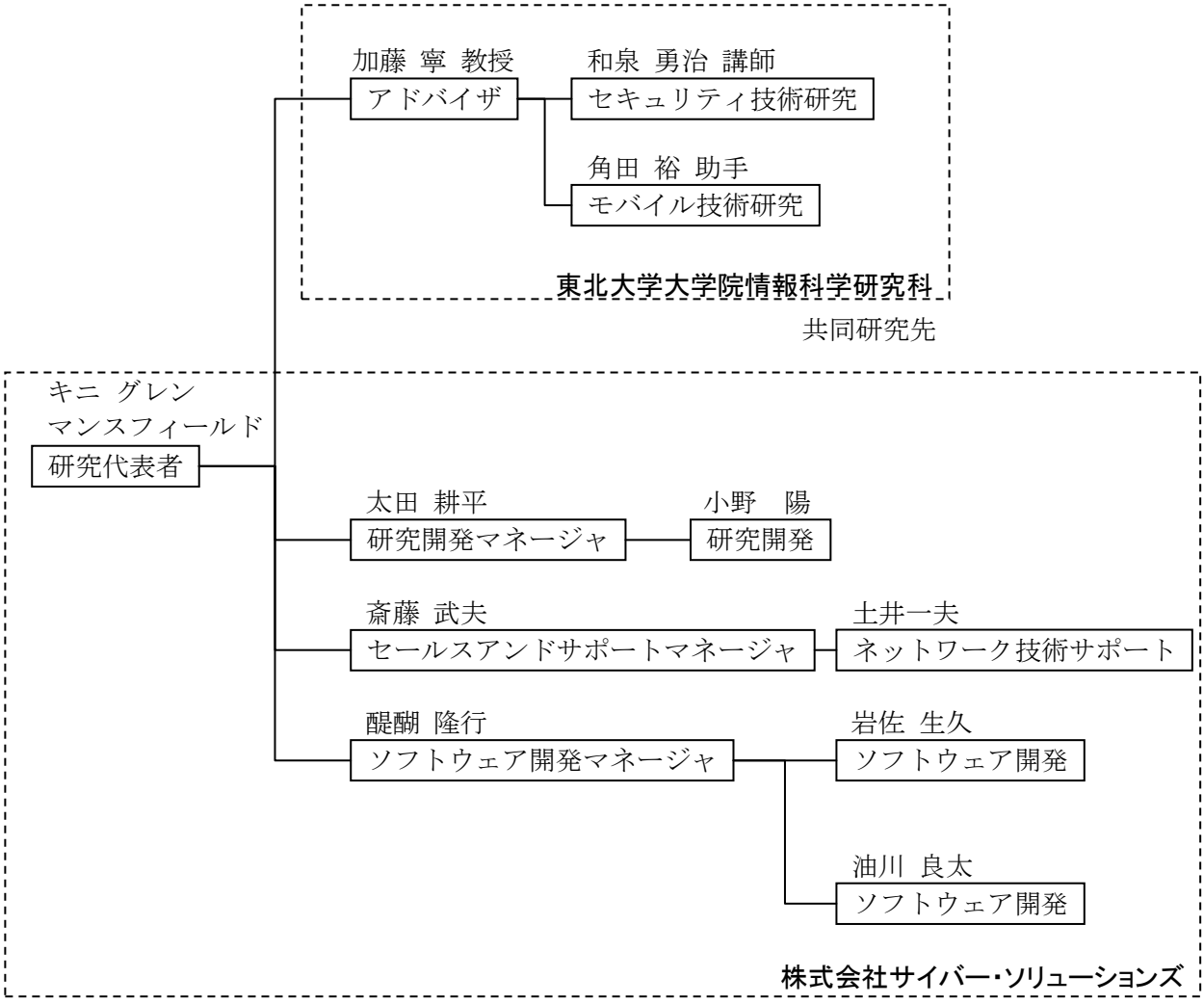
3－1　研究開発実施体制

研究開発は、申請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

図 3に本研究開発の平成 19 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 19 年度は、18 年度に整備された基盤を基に、無線接続端末、ファイル持ち出し管理、既存技術とのシームレスな運用、および次世代に向けた IPv6 への対応を実施し、さらに大規模化にむけた、自動発見、自動構成技術を研究開発し、当初計画通りの目標を達成した。

また、大規模化に対する現実的な対応を検証するために継続的な実証実験を行い、管理のために必要な各種性能の評価を実施した。

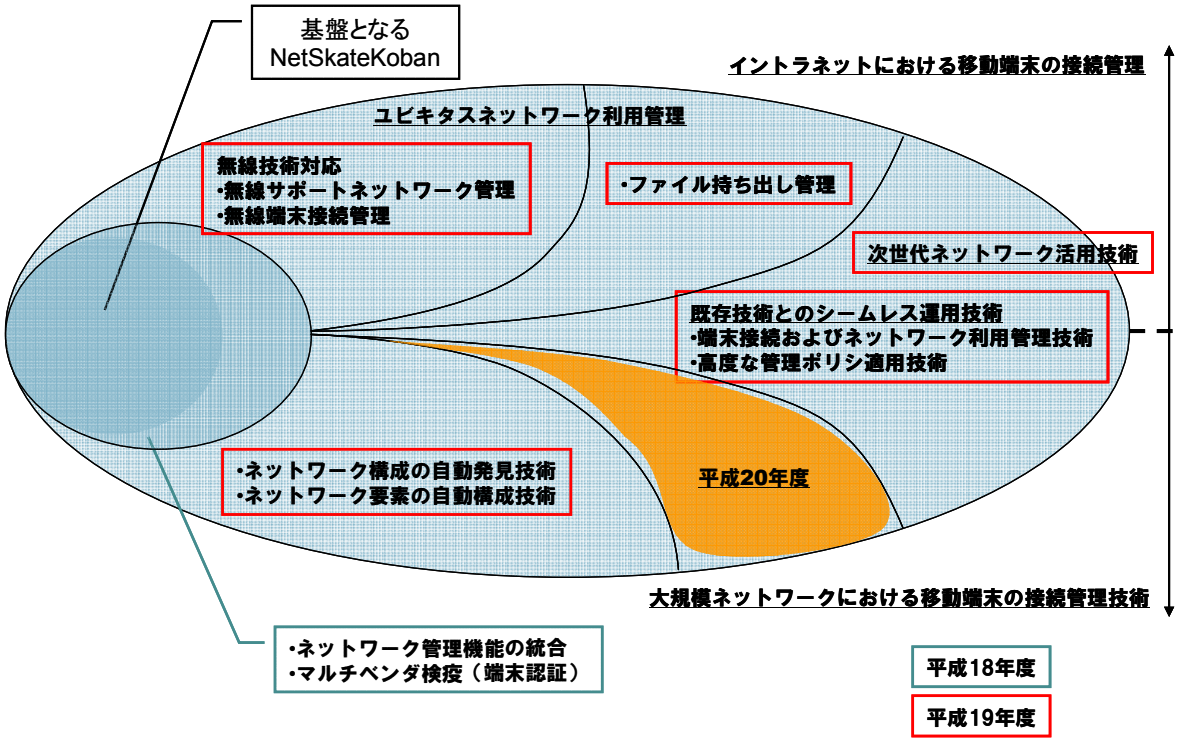


図 3 研究開発の実施状況

４－１　　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、端末を管理下にお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。

４－１－１　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、優先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、離脱を管理する可能な、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。

４－１－２　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

本研究開発によってユビキタスネットワーク利用管理技術を予定通り確立できた。

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 4 無線接続端末の「移動」管理の実現)。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。

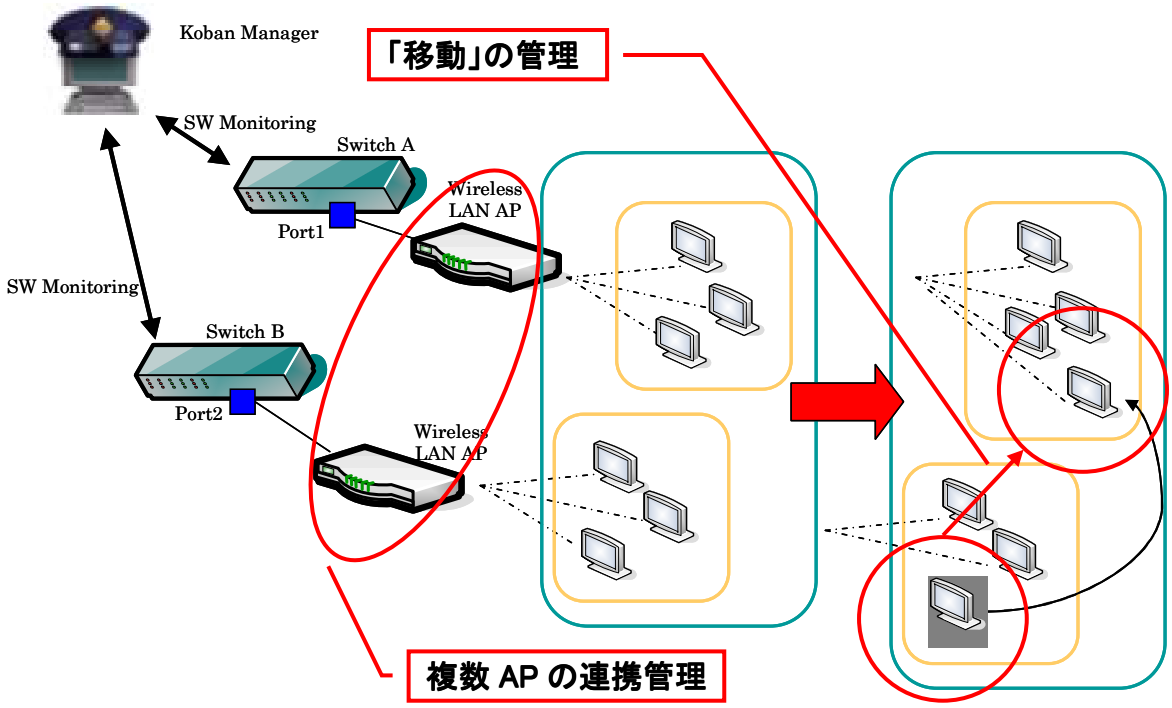


図 4 無線接続端末の「移動」管理の実現

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 5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移動するケースを示している。

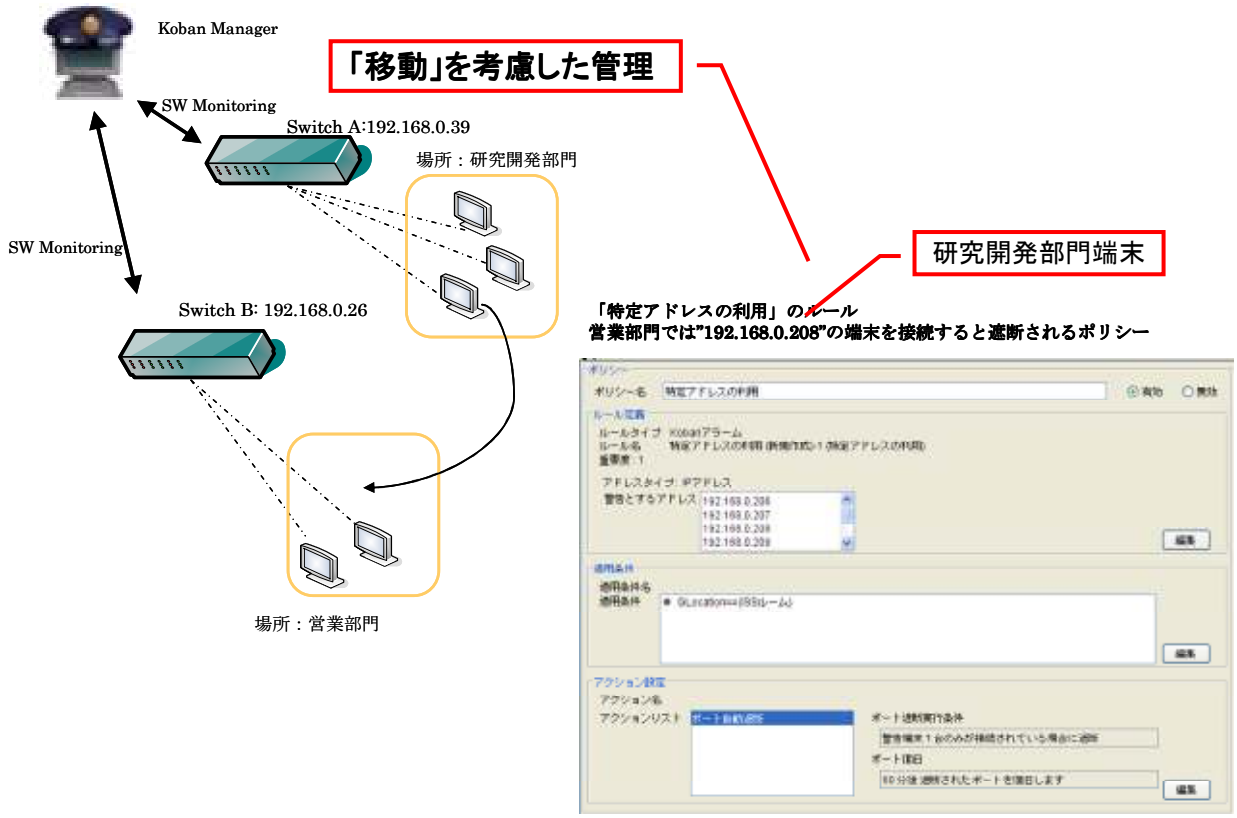


図 5 移動端末の接続管理例

図 6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 6 移動元での接続管理例

図 7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 6のケースと図 7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 7 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 8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。

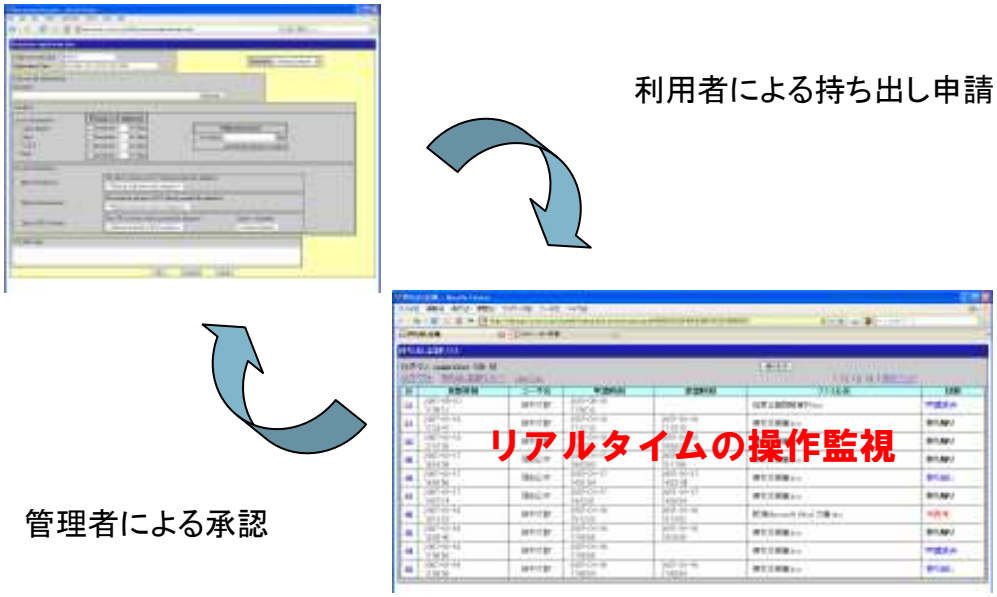


図 8 端末上のファイルレベルの移動管理の例

４－１－３　ユビキタスネットワーク利用管理技術の研究開発まとめ

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。

４－２　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。

４－２－１　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 NetSkateKoban 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

４－２－２　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 9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。

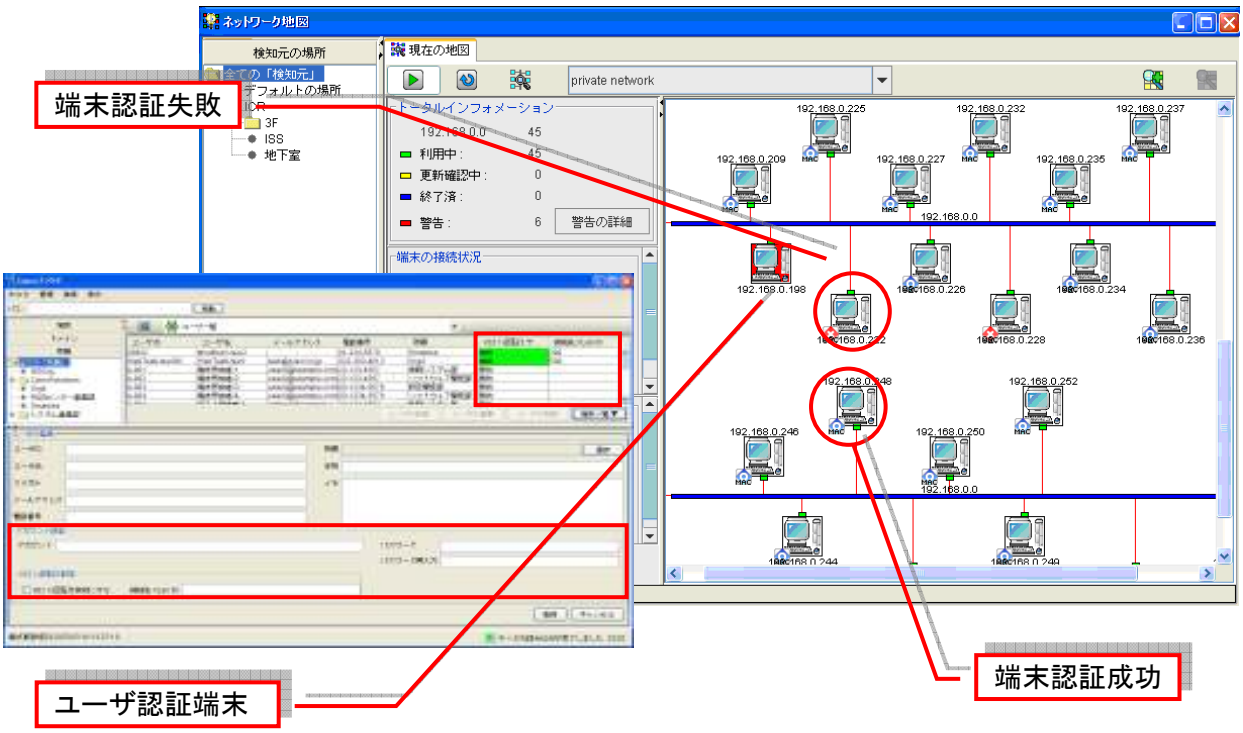


図 9 端末認証とユーザ認証のシームレスな統合例

図 10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。

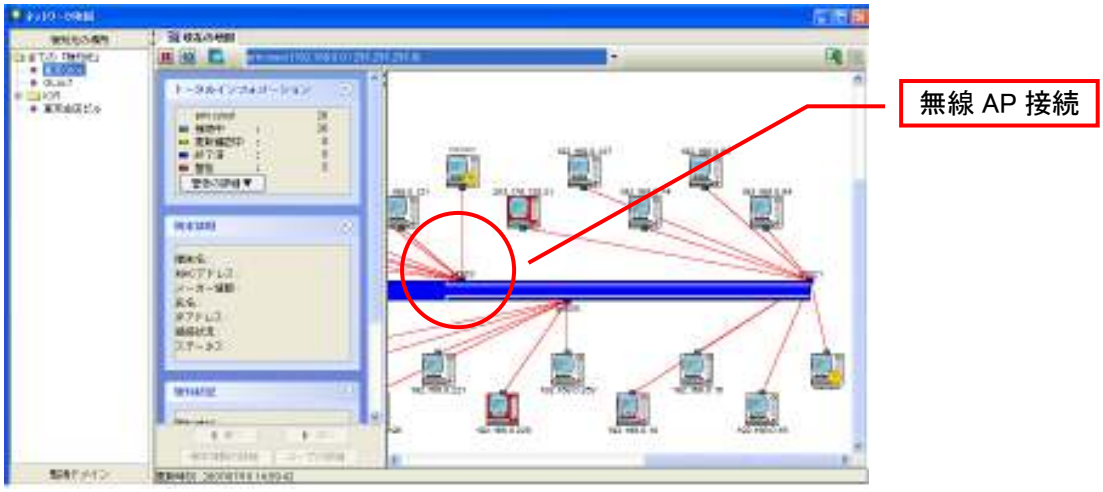


図 10 有線環境と無線環境のシームレスな統合

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 11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 11 ユーザ毎の利用履歴管理例

図 12にユーザによる端末利用履歴例を示す。図 11の例でユーザ情報から抽出された利用端末の履歴を示す。これによって当該ユーザの利用状況を追跡することが可能となり、セキュリティインシデント発生時にも物理的管理における入退館管理に相当する管理の実現が可能となる。

図 12 ユーザによる端末利用履歴例

図 13に図 11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 11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 13 ユーザによる複数端末利用管理例

図 14に図 13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。

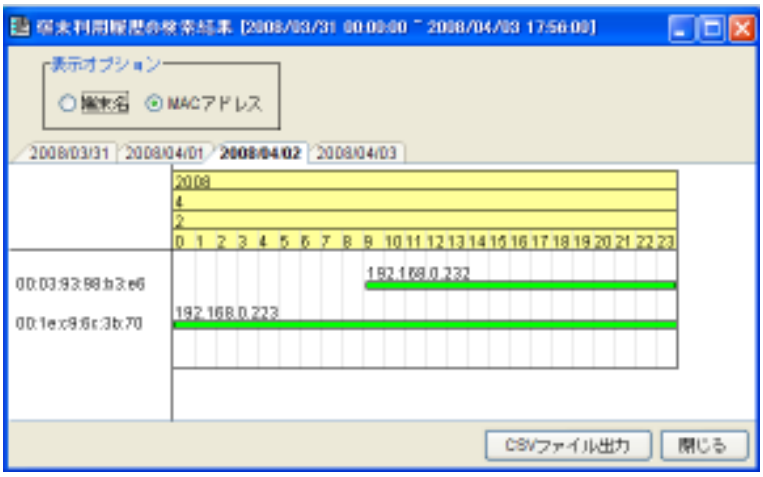


図 14 複数端末利用履歴管理例

４－２－３　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。

４－３　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。

４－３－１　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

４－３－２　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 15に開発したIPv6 ネットワーク管理の例を示す。

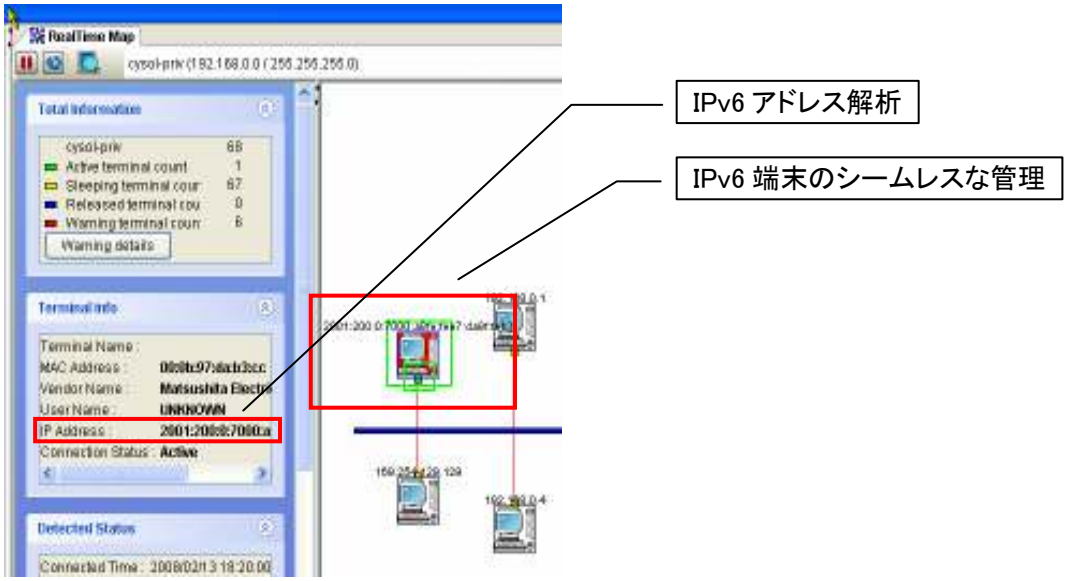


図 15 IPv6 ネットワーク管理の例

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 16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。

```
daigo:agni-vm1 66 % perl ./genKobanTrap_ctm.pl ipv6.csv
snmptrap -v 2c -c  public udp:192.168.0.239:162 6581400 .1.3.6.1.4.1.282.7.
4.0.1
 1.3.6.1.4.1.282.7.4.1.1.1.4.3 s "NetSkateKoban! *Version 4 (Build 0)*"
 1.3.6.1.4.1.282.7.4.1.1.1.9.3 s eth0
 1.3.6.1.4.1.282.7.4.1.1.1.6.3 i 1
 1.3.6.1.4.1.282.7.4.1.1.1.7.3 s 192.168.0.82
 1.3.6.1.4.1.282.7.4.1.3.1.2.3.1 i 1
 1.3.6.1.4.1.282.7.4.1.3.1.3.3.1 x 07d8020d12140000000000
 1.3.6.1.4.1.282.7.4.1.3.1.5.3.1 i 1
 1.3.6.1.4.1.282.7.4.1.3.1.6.3.1 s 2001:200:0:7000:a8fe:fee7:da9f:feb3
 1.3.6.1.4.1.282.7.4.1.3.1.4.3.1 x 000b97dab3cc
 1.3.6.1.4.1.282.7.4.1.3.1.12.3.1 i 1
 1.3.6.1.4.1.282.7.4.1.3.1.13.3.1 i 3
```

図 16 管理プロトコルでの IPv6 アドレスの扱い例

次に、IPv6 アドレスによって接続された端末の管理技術の開発状況を示す。

IPv6 による端末接続は、IPv4 とは大きく異なるものとなる。IPv4 では ARP（Address Resolution Protocol）によって接続されていたため、そのプロトコルの通信を監視することで接続を管理することができたが、IPv6 では ARP に相当する異なるプロトコル Neighbor Discovery を管理することが重要となる。またアドレスを割り当てる DHCP(Dynamic Host Configuration Protocol)についても IPv6 対応が必要となる。図 17に本研究開発で実現したIPv6 端末の検知例を示す。

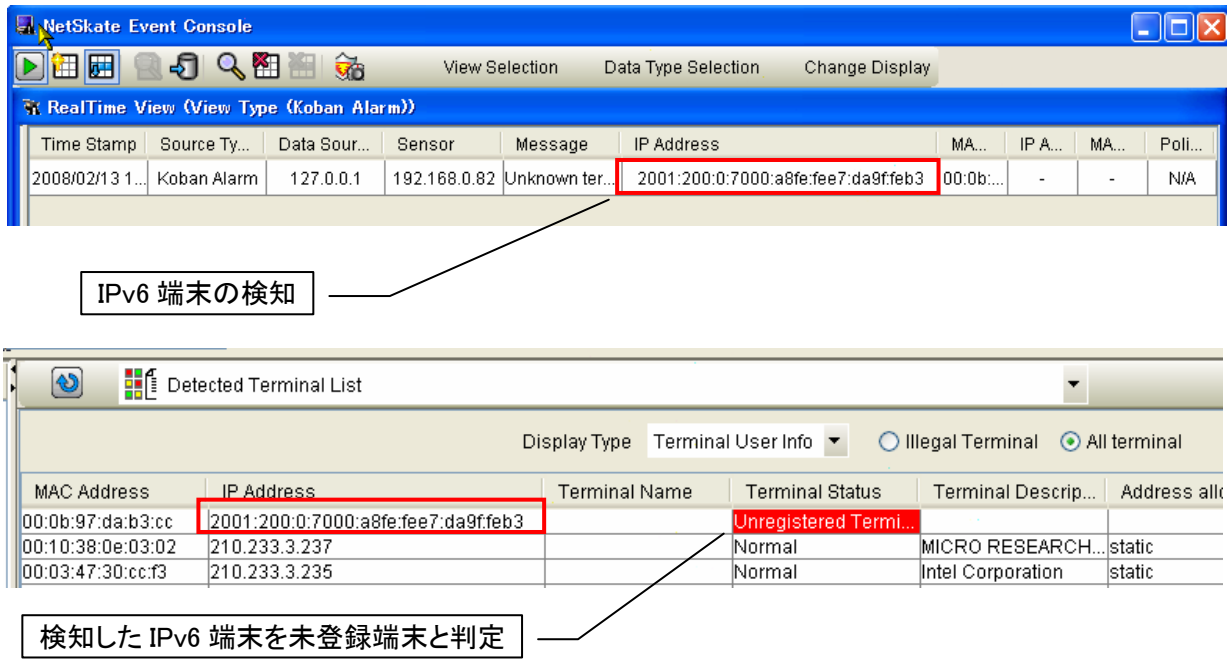


図 17 IPv6 端末の検知例

図 17で検知された端末はデータベース中で IPv4 端末と同様に管理される（図 18 IPv6 端末の内部管理例）。

77	00:0b:97:da:b3:cc	1	2001:200:0:7000:a8fe:fee7:da9f:feb3	<NULL>	1	192.168.0.0	255.255.255.0
9	00:60:67:30:6b:af	1	210.233.3.226	<NULL>	1	210.233.3.224	255.255.255.248
32	00:02:b3:a1:7c:48	1	210.233.3.227	<NULL>	1	210.233.3.224	255.255.255.248
17	00:03:93:f4:21:0c	1	210.233.3.228	<NULL>	1	210.233.3.224	255.255.255.248
48	00:02:b3:a6:15:64	1	210.233.3.229	<NULL>	1	210.233.3.224	255.255.255.248
50	00:03:47:31:09:47	1	210.233.3.234	<NULL>	1	210.233.3.232	255.255.255.248
75	00:03:47:30:cc:f3	1	210.233.3.235	<NULL>	1	210.233.3.232	255.255.255.248
26	00:10:38:0e:03:02	1	210.233.3.237	<NULL>	1	210.233.3.232	255.255.255.248
78	00:c0:9f:1d:77:d8	1	fe80::2c0:9fff:fe1d:77d8	<NULL>	1	192.168.0.0	255.255.255.0

図 18 IPv6 端末の内部管理例

４－３－３　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。

４－４　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。

４－４－１　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

４－４－２　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 19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。

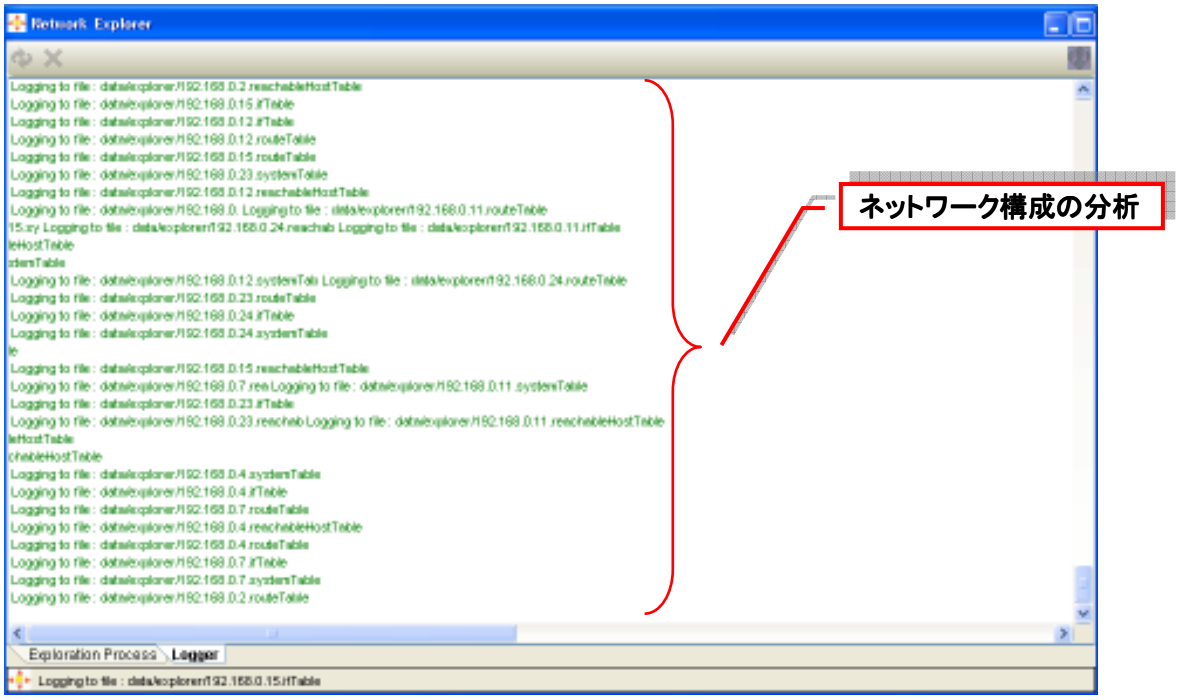


図 19 ネットワークトポロジの分析例

図 20はネットワークトポロジの自動発見例を示している。図 19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。

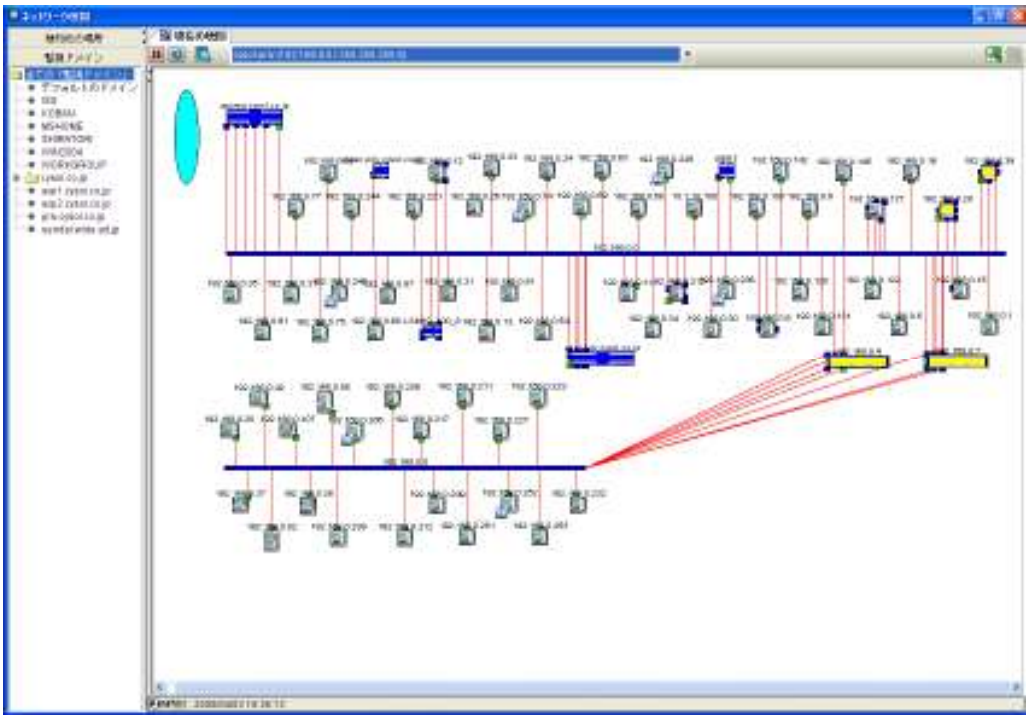


図 20 ネットワークトポロジの自動発見例

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 21は管理システム<->センサ構成例を示している。

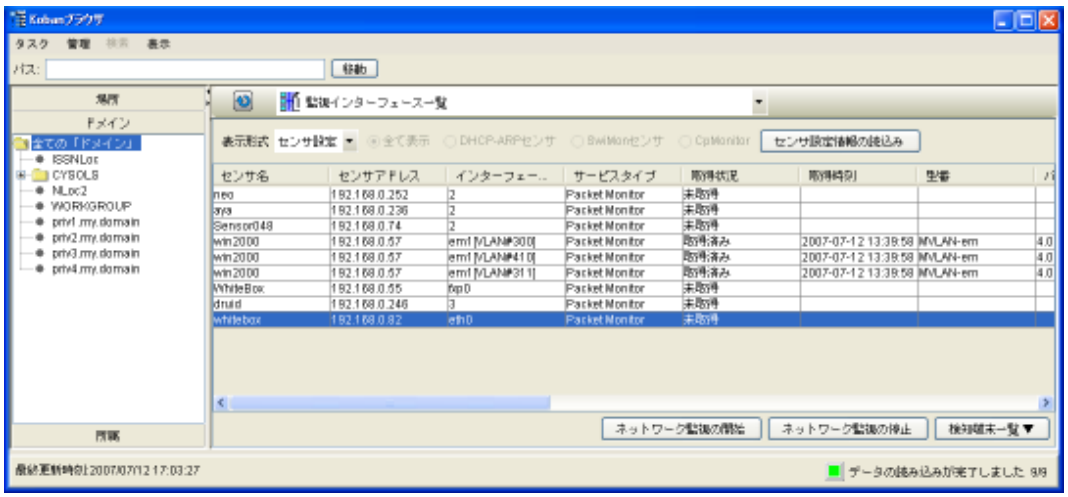


図 21 管理システム<->センサ構成例

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、センサシステムを動的、かつ遠隔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。

４－４－３　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。

４－５　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。

４－５－１　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

４－５－２　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 22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。

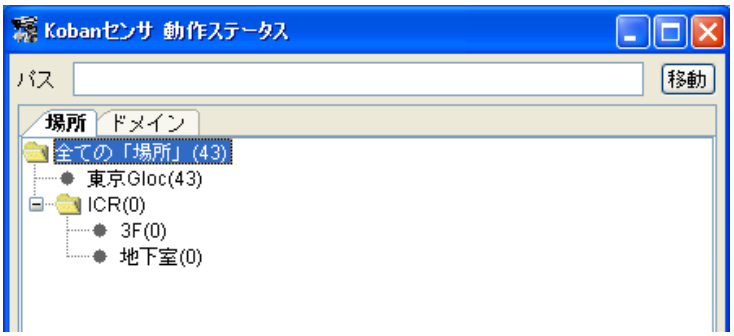
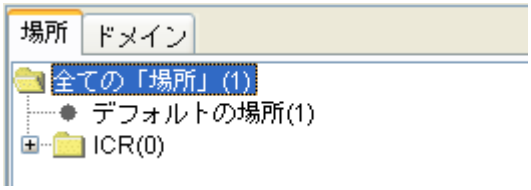
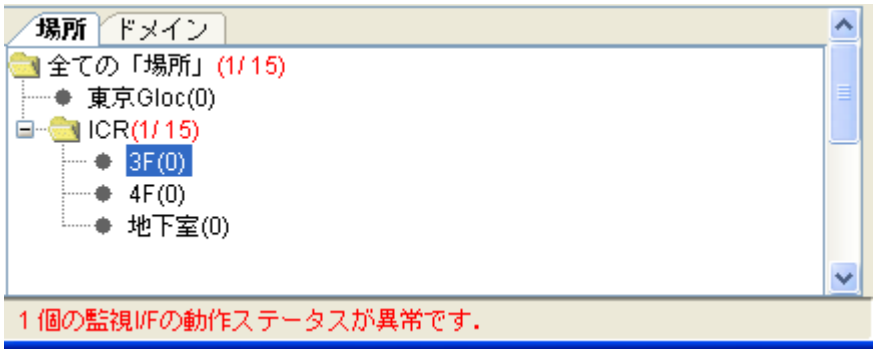


図 22 Koban センサ動作ステータス

監視結果として、センサ数がロケーション（場所）毎に表示されます。センサが正常に動作している場合、黒色でセンサ数が表示される。



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 23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。

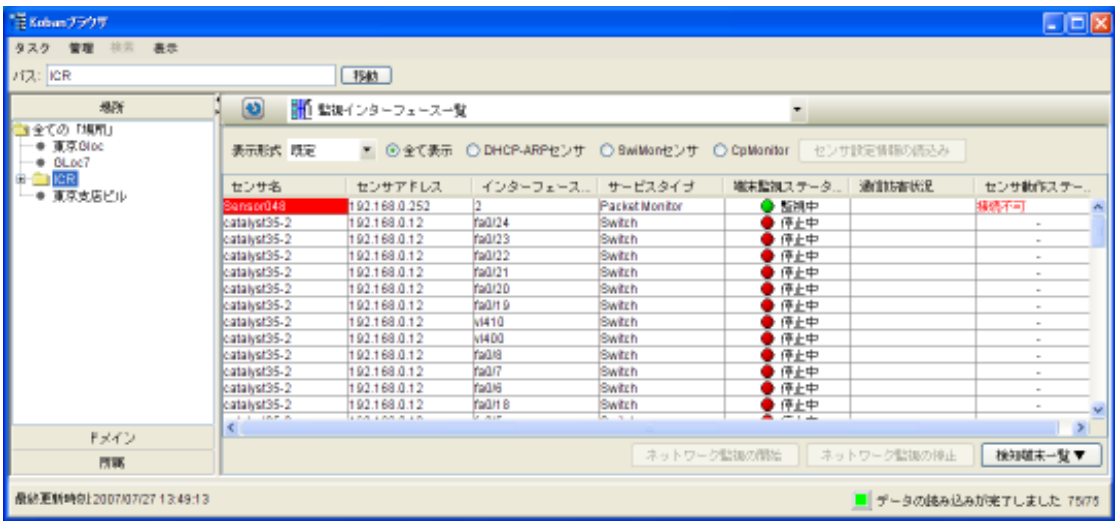


図 23 Koban ブラウザ（監視インタフェース一覧）

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。

更新対象となるセンサを選択すると以下のような GUI を備えた更新管理が利用できる。更新するファイルおよびセンサを選択することで、任意のセンサ群に対して遠隔・一括更新が可能となる。

４－５－３　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。

４－６ 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。

４－６－１ 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。

４－６－２ 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。

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 24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、性能向上の可能性を検討した。

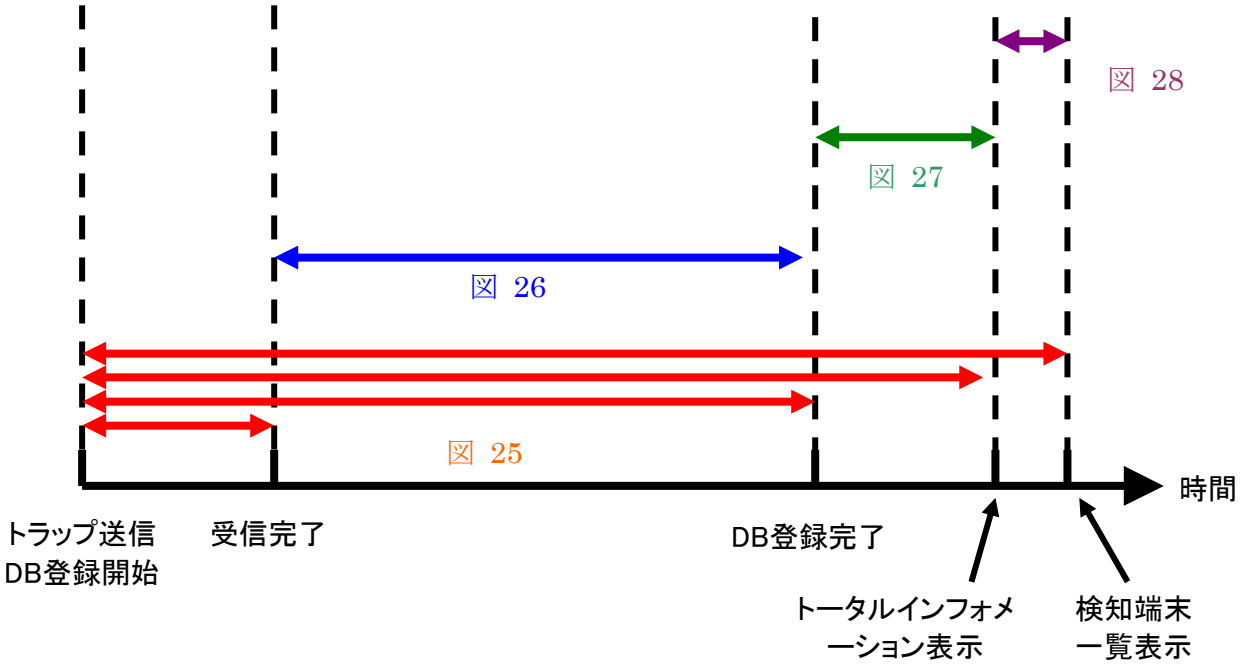


図 24 性能評価概要

図 25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。

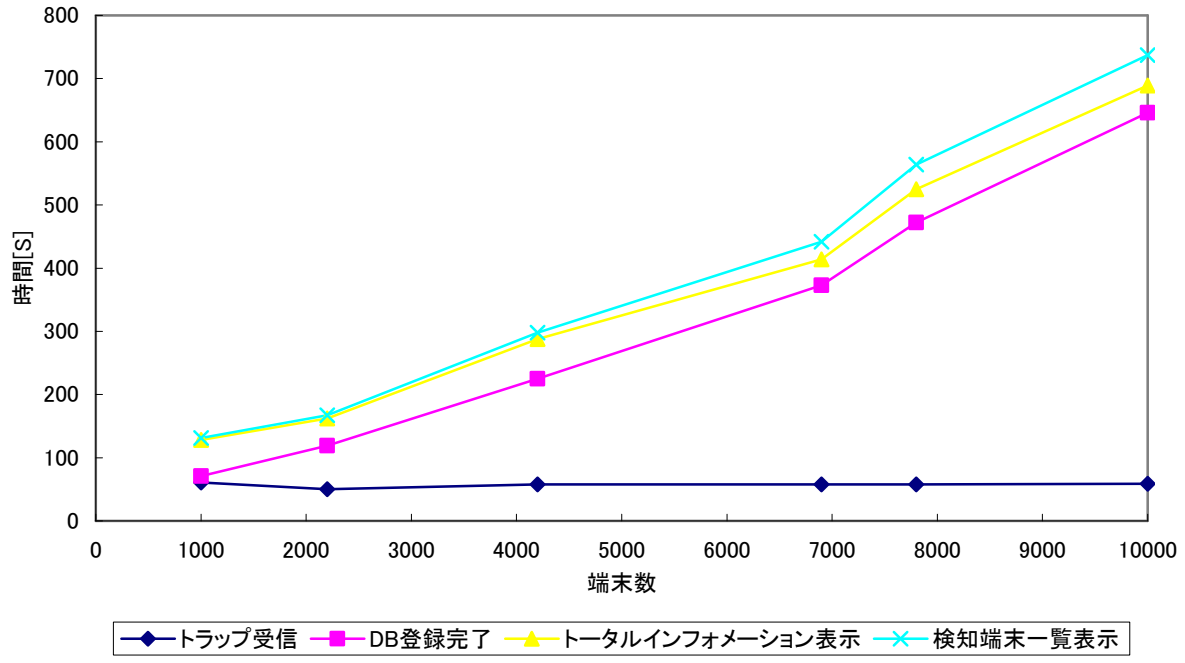


図 25 イベント検知の所要時間

図 26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。

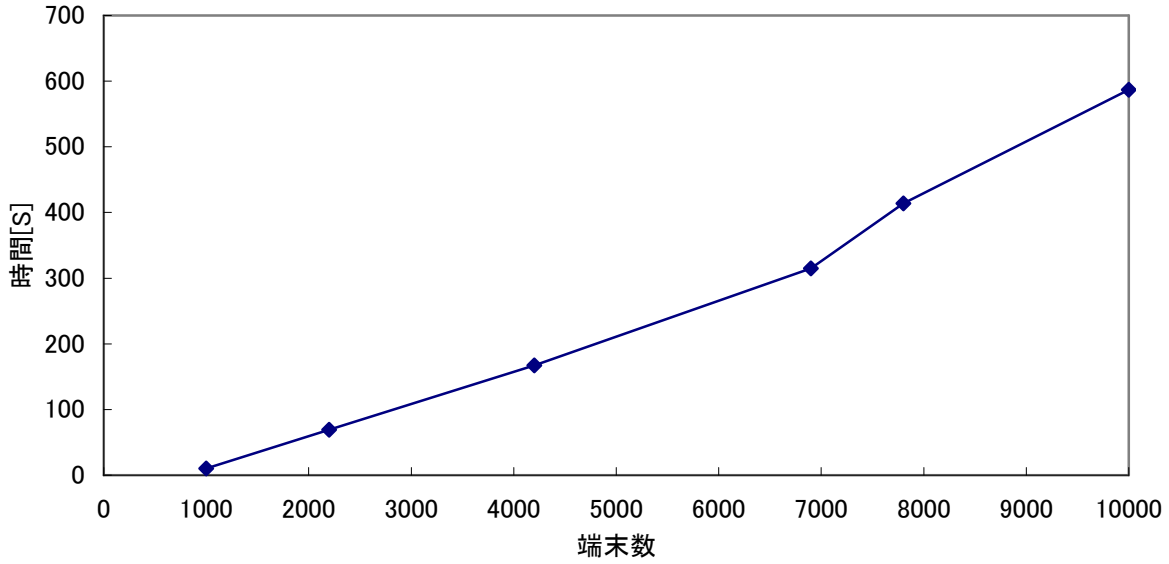


図 26 トラップ受信完了-DB 登録完了所要時間

図 27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。

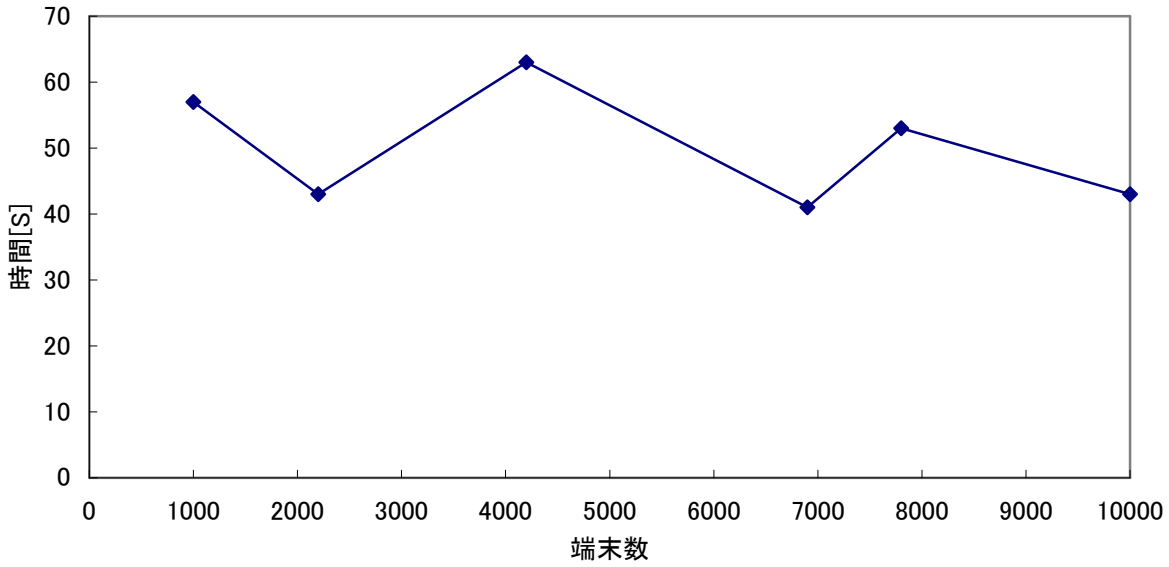


図 27 DB 登録完了-インフォメーション表示所要時間

図 28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。

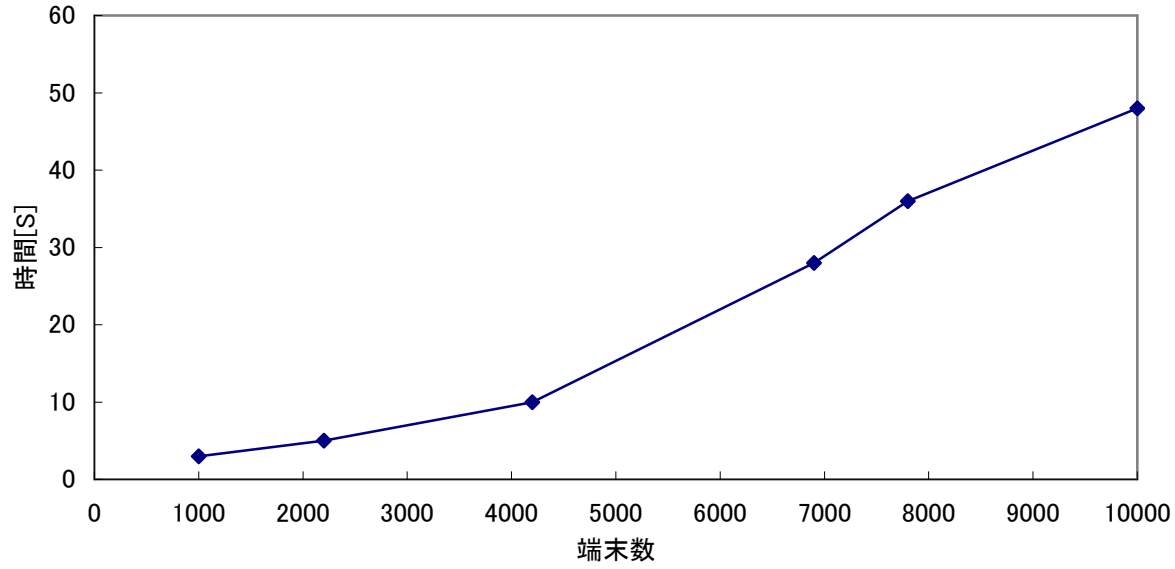


図 28 インフォメーション表示-検知端末一覧表示所要時間

４－６－３ 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。

４－７　総括

平成 19 年度の研究開発によって、当初計画した以下の研究開発大項目の主要要素技術を確立することができた。

- 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移動端末の接続管理技術

移動端末の管理については、有線、無線による端末の接続に関する問題点を解決し、新たな管理技術を実現することができた。また端末レベルではなく、ユーザレベル、さらにはファイルレベルの管理を実現することによって、従来のハードウェア毎の管理ではなく、現実の管理単位である、人、および情報にフォーカスした管理を実現する技術を確立した。また、移動体ネットワークについてはインターネット技術そのものの新しいフェーズへの移行が始まっており、それらにいち早く対応できるように IPv6 および MobileIPv6 も視野にいれた研究開発を実施し、市場ニーズに対して即応できる体制を整えた。

大規模ネットワークでの接続管理については、システムの自動構成、遠隔構成の技術を確

立し、セキュリティシステムの現場で大きな問題となる「導入」に関わる課題を大幅に簡略化することが可能となった。またさらにセキュリティシステム固有の問題として、その信頼性、可用性に対する要求が非常に高いことを指摘し、システム自身のセルフチェックとなる監視機構を実現した。本監視機構は、個々のシステムだけではなく巨大なネットワークシステム内のすべての要素を管理することを可能としており、セキュリティシステム自体に発生する問題の「検知」「通知」そして必要に応じた「対策」を遠隔での実行を可能とした。

上記二つの大項目で示される研究開発結果の実用化には、本当の大規模環境での実証試験が欠かせない要素となる。本研究開発では、実証実験のための大規模ネットワークを模した環境を人工的に構築し、繰り返し試験できる体制を整えた。またその環境を利用して想定される大規模環境での性能評価を実施した。本性能評価の結果は、技術開発に即座に反映され、これまで明確になっていなかった大規模ネットワークでの性能のボトルネックの改善を実現できた。

本研究開発は、予定通り研究開発が進み、要素技術の研究開発の段階から、これまで欠けていた補完的な技術開発の段階に入るとともに、実用化を踏まえた現実的な改良、改善の段階に入っている。平成 20 年度は商品としての完成度を踏まえた研究開発を推進していく予定である。

５　参考資料・参考文献

５－１　研究発表・講演等一覧

外国発表論文

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

- 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