ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発
Research and Development on detection and prevention of information leakages through computer networks.

研究代表者　田代 勤　株式会社日立製作所

研究期間　　平成 19 年度～平成 21 年度

【Abstract】

This paper summarizes the final achievements of "R&D on detection and prevention of information leakages through computer networks".

This R&D is aimed at minimizing information leakages caused by P2P file-sharing applications, which does not have any functionalities to remove files once they are exposed to the Internet, without losing usefulness and effectiveness of the P2P technologies. Then, we have developed technologies that identify and control P2P traffic, and extract and remove packets that contain leaked information with specific characterestics.

We have completed this three-year R&D (from 2007 to 2010) with many benefical and useful achievements that will contribute to make the secure and reliable Internet by reducing risks of information leakages caused by P2P file-sharing applications.

This paper also lists intellectual properties, technical papers, and presentation materials that have been made through the R&D.

1　研究体制

○ **研究代表者**　　田代 勤（株式会社日立製作所）

○ **研究分担者**　　中田 登志之†（日本電気株式会社†）

○ **研究期間**　　平成 19 年度～平成 21 年度

○ **研究予算**　　総額　1,947 百万円

（内訳）

平成 19 年度	平成 20 年度	平成 21 年度
492,208,232	821,166,000	633,685,000

2　研究課題の目的および意義

近年、自動転送型ファイル共有ソフトに起因した情報の流出が多発し、個人・企業・行政における情報漏えい被害が社会問題として顕在化している。一方で、自動転送型ファイル共有ソフトは、情報流通に係わるコスト削減や負荷分散など、有用な特長も兼ね備えており、従来のクライアント・サーバ型通信に代わる方式として、新たなサービス市場の創造を含め、大いに期待されている技術である。

そのため、本施策では、自動転送型ファイル共有ソフトの優れた特長を損なうことなく、情報通信ネットワークを通じた情報漏えいの検知技術、及び当該漏えい情報の自動流通停止技術を確立し、安心・安全なネットワーク利用環境の実現に資する。

具体的な研究開発目標としては、情報通信ネットワークを通じた情報流出が起こってしまった場合の被害を最小限にとどめ、自動転送型ファイル共有ソフトに起因する情報漏えいのリスクを最小限にすることで、国民が情報通信ネットワークをより安心して利用可能とするため、すべてのトラヒックの中から自動転送型ファイル共有ソフトのトラヒックのみを抽出・制御する技術、また自動転送型ファイル共有ソフトにより交換される情報の中から、特定の特徴を有する情報を検知、削除する技術、および新たな自動転送型ファイル共有ソフトの出現を早期に把握可能とする技術を確立する。

３　研究成果

３．１　自動転送型ファイル共有ソフトトラヒック制御技術

３．１．１　自動転送型ファイル共有ソフト通信検知技術

すでに自動転送型ファイル共有ソフトに起因した情報の流出が多発し、情報漏えいリスクの低減が喫緊の課題となっていることから、既存の自動転送型ファイル共有ソフトの通信特性の分析については、まず初年度に国内で多く利用されている２種類以上のソフトについて実施し、それら自動転送型ファイル共有ソフトのトラヒックを検知する元となる基本データを抽出する。更に、２年目以降、国内で利用されているそれ以外の自動転送型ファイル共有ソフトや主に海外で利用されている５種類以上の自動転送型ファイル共有ソフトについてそれぞれの通信特性の分析を行い、自動転送型ファイル共有ソフトに共通の通信特性を導出することを目標とする。

また、国内外で利用されている自動転送型ファイル共有ソフトの種別やその利用状況の調査については、少なくとも５種類以上の自動転送型ファイル共有ソフトの調査を初年度に行い、２年目以降は、新たな自動転送型ファイル共有ソフトの出現など状況の変化に応じて適宜実施し、新たな自動転送型ファイル共有ソフトの出現を把握する技術を明確化することを目標とする。

上記目標を達成するために、第一年目に代表的な自動転送型ファイル共有ソフトを対象として、自動転送型ファイル共有ソフトのトラヒックの解析を行い、自動転送型ファイル共有ソフト通信検知・制御技術の基礎となる要素技術を確立し、第二年目に初年度に検討した基本方式・要素技術の汎用化(より多くの自動転送型ファイル共有ソフトへの適用)を目指すとともに、実ネットワークへの運用にも耐える基本技術の確立を行い、第三年目に大規模な実証実験を通して、開発技術が実ネットワーク環境においても性能面、機能面、コスト面から有効であることを検証した。以下、詳細について説明する。

(1) 自動転送型ファイル共有ソフト調査

① 自動転送型ファイル共有ソフトの動作原理、機能調査

国内外で利用されている主要なファイル共有ソフトの機能調査を実施し、当該ソフトの動作原理、機能を明確化した。具体的には、Winny、Share、LimeWire、Cabos、WinMX、Winnyp、BitTorrent、Perfect Dark の８種類の自動転送型ファイル共有ソフトの公開情報ファイル検索の方法やファイル送受信の方法、暗号化機能、匿名化機能、バージョン管理機能、流通ファイルの削除機能など、個々の自動転送型ファイル共有ソフトの動作原理やそれら自動転送型ファイル共有ソフトが持つ機能

について調査した。調査対象とした自動転送型ファイル共有ソフトは、後述する「③ 利用者アンケートによる自動転送型ファイル共有ソフトの利用状況調査」の調査結果に基づき、利用者の多い結果となった自動転送型ファイル共有ソフトから選定しており、本調査結果によると、国内で利用されている自動転送型ファイル共有ソフトの利用者カバー率 90%以上となる自動転送型ファイル共有ソフトの動作原理、機能が明らかとなった。

② トラヒック監視・分析に基づく自動転送型ファイル共有ソフトの利用状況調査

前述の「① 自動転送型ファイル共有ソフトの機能調査」の調査結果に基づいて、自動転送型ファイル共有ソフトの接続するネットワークの構成ノードや流通コンテンツを観測するための手法を確立し、P2P ネットワークを観測可能な観測用ツールを開発した。また、開発したツールを用いて、P2P ネットワークを構成するノードの数や流通コンテンツ、トラヒック量などの統計情報を定量的な調査を行った。

③ 利用者アンケートによる自動転送型ファイル共有ソフトの利用状況調査

自動転送型ファイル共有ソフトの利用者に対してアンケート調査を実施し、ファイル交換ソフトを通じた情報漏えいに関する現状を明らかにした。具体的には、3 カ年に渡り 60,000 以上のユーザを対象とした Web アンケートを実施し、自動転送型ファイル共有ソフトの利用の有無、主に利用している自動転送型ファイル共有ソフトの種類などの利用状況に関する定量的な分析および、年ごとの傾向など経年変化を分析した。また、アンケートだけでなく、実際の自動転送型ファイル共有ソフト利用者に対する聞き取り調査も実施することで、利用者の意識や利用環境について詳細な調査を実施した。さらに、国外のベンダを対象に自動転送型ファイル共有ソフトに関わるセキュリティ対策技術動向についてのヒアリング調査を行った。これにより、ファイル共有ソフトの利用に起因する情報漏えい被害に対する効果的な対策を研究するための基礎的データを集積した。

④ P2P 技術を利用したソフトウェア・サービスの調査

P2P 技術を有効活用しているソフトウェアやサービスの実態､また技術の有効性の調査を行った。P2P 技術の有効活用事例を参考に、P2P 技術を活用したサービスのあるべき姿、サービスモデルを検討した。

(2) 自動転送型ファイル共有ソフト通信特性の解析技術

① 自動転送型ファイル共有ソフトのプロトコル解析技術の確立

「(1) 自動転送型ファイル共有ソフト調査」の成果および、自動転送型ファイル共有ソフトの実行コードを解析する静的解析により、Winny、Share、LimeWire、Cabos、WinMX、Winnyp、BitTorrent、Perfect Dark の 8 種類の自動転送型ファイル共有ソフトの通信プロトコルを詳細に調査・解析し、IP パケットのペイロードに現れるそれぞれの特徴を導出した。前述の「③ 利用者アンケートによる自動転送型ファイル共有ソフトの利用状況調査」の調査結果によれば、国内で利用されている自動転送型ファイル共有ソフトの利用者カバー率 90%以上となる自動転送型ファイル共有ソフトのプロトコル解析が完了し、世の中のほぼ全ての自動転送型ファイル共有ソフトのプロトコルを解明したこととなる。

また、上記解析結果に基づき、各自動転送型ファイル共有ソフトの利用者端末に接続し、利用者情報を取得することによって P2P ネットワークの情報を収集する手法を確立した。

② 自動転送型ファイル共有ソフトのコネクション解析技術の確立

自動転送型ファイル共有ソフトによる通信とそれ以外のソフトウェアによる通信について、様々

な観点より解析を実施し、自動転送型ファイル共有ソフトに特有な通信の特徴を導出した。具体的には、(1)集約フローに基づく検知手法、(2)DNS 通信履歴に基づく検知手法、(3)接続確立成功割合に基づく検知手法、(4)クエリルーティングに基づく検知手法、(5)乱数検定に基づく検知手法の 5 種類のコネクション解析手法を確立した。

３．１．２　動的トラヒック制御技術

本事業の成果を既存の情報通信インフラに対してできるだけ容易に適用可能とするためには、既存インフラで使用されている機器自体を置き換えるのではなく、当該機器と連携して動作するアドオンモジュールとしての実装が望ましい。また、ISP レベルでの通信性能を考慮し、最終的にはハードウェア実装を目指す。

初年度は、トラヒックの通信特性を観測する機能、自動転送型ファイル共有ソフトの通信特性に合致するか否かを判定する機能、および判定結果にしたがってトラヒックの経路や流量の制御を動的に実行する機能の基本方式を確立するとともに、効率的にハードウェア実装するための設計指針を明確化する。また、2 年目以降のハードウェア実装を踏まえ、予備的な調査として、5000 台程度のユーザ利用端末等からなるネットワークシミュレーション環境を構築し、当該シミュレーション環境において、上記基本方式の機能や性能等の検証を行う。その際、既存の情報通信インフラで使用されている機器や構成についても調査し、実ネットワークへの最適配置などの検討も併せて実施する。

2 年目は、初年度のネットワークシュミレーション環境での検証結果にしたがって基本方式をブラッシュアップするとともに、当該基本方式を実装したハードウェアモジュールを試作する。更に、数十台程度のユーザ利用端末からなるリアルな実験ネットワーク環境を構築し、当該実験ネットワーク環境において、試作したモジュールの機能や性能等を確認する。本実験においては、トラヒックの通信特性の観測などがシステム全体に及ぼすオーバヘッドを検査し、利用者に不快感を与えることのないレベルの性能（通信特性を観測することによって生じる自動転送型ファイル共有ソフト以外のトラヒックのオーバヘッドが 1 秒程度）を達成することを目標とする。

更に、最終年度に向けて、試作モジュールの大規模対応化、処理の高速化等を図るとともに、初年度の実ネットワークへの最適配置に関する検討結果を利用して、より大きな規模での実証実験を実施し、試作モジュールの有効性（機能、性能、配置、コスト等）を検証する。最終的には本技術開発の成果を実ネットワークへ適用した場合のオーバヘッドを、1Gbps 回線で 5%以内、10Gbps 回線で 10%以内に抑えることを目標とする。

上記目標を達成するために、第一年目に各課題に関する基本方式の検討ならびに要素技術の開発を行い、第二年目に第一年目に開発した要素技術に基づく試作モジュールの開発を行い、第三年目に試作モジュールの処理の高速化を行うとともに、必要な機能拡張・強化を図り、大規模なネットワーク環境において実証実験を行った。以下、詳細について説明する。

(1) 自動転送型ファイル共有ソフトトラヒック検出技術

① プロトコル解析結果を利用したトラヒック検出技術の確立

前述したプロトコル解析で得られた個々の自動転送型ファイル共有ソフトの特徴を利用して、ネットワーク上を流れるトラヒックの中から自動転送型ファイル共有ソフトのトラヒックを検出する技術を開発した。具体的には、既存の自動転送型ファイル共有ソフトのバージョンアップや、新しい自動転送型ファイル共有ソフトへの対応を考慮し、検知エンジンを搭載したトラヒック検出モジ

ュールに対して個々の自動転送型ファイル共有ソフトの特徴から生成するパターンファイルを入力するような構成をとる検知システムのアーキテクチャを開発した。さらに、Winny、Share、LimeWire、Cabos、WinMX、Winnyp、BitTorrent、Perfect Dark の 8 種類の自動転送型ファイル共有ソフトに対応した検知パターンファイルと、監視対象トラフィックから自動転送型ファイル共有ソフトのトラヒックを検知する検知エンジンを開発した。また、1Gbps、10Gbps のトラヒックを処理可能な検知エンジンをハードウェア上に実装した。

② コネクション解析結果を利用したトラヒック検出技術の確立

前述したプロトコル解析で得られた 5 種類のコネクション解析手法に対応したコネクション検知モジュールを開発した。開発においては、コネクション解析で行った自動転送型ファイル共有ソフト以外のアプリケーションのコネクション特性の解析結果を盛り込み、より誤検知の少ないコネクション検知を実現した。また、AFM（Aggregated Flow Mining）を用いたコネクション検知機能を 10Gbps のトラヒックを処理可能なハードウェア上に実装した。

自動転送型ファイル共有ソフトの通信にみられるコネクション特性に着目したコネクション検知技術によって、既知・未知含めた自動転送型ファイル共有ソフトの通信を検知・把握することができる。またプロトコル検知技術によって既知の自動転送型ファイル共有ソフトを検知・把握することができる。このことから、両検知技術を実装した本研究開発システムでは、新たに出現した未知の自動転送型ファイル共有ソフトの存在を早期に発見することができる。なお、Parfect Dark を未知の自動転送型ファイル共有ソフトと仮定した実証実験では、Parfect Dark の検知パターンを無効化したプロトコル検知システムと、コネクション検知システムを組み合わせた環境を用いて、未知のものと仮定した Parfect Dark の通信を不明な自動転送型ファイル共有ソフトとして検知できることを確認した。

(2) 動的な自動転送型ファイル共有ソフトトラヒック制御技術

① トラヒック制御技術の確立

実ネットワークにおける運用を想定した、自動転送型ファイル共有ソフト検知・制御システムの基本アーキテクチャを確立した。このシステムは、トラヒックの監視・制御を行うスイッチや、自動転送型ファイル共有ソフトのトラヒックを特定する解析装置を、容易に拡張できる仕様となっており、ISP や企業の社内ネットワークなど様々な規模のネットワークに柔軟に対応が可能である。また、このシステムは、観測対象のトラヒックに影響を与えないように、観測対象トラヒックをミラーリングして解析を行う仕様となっており、実ネットワークへ適用した場合のオーバヘッドは発生せず、当初の目標を達成している。システムの構成要素として、IP アドレスをキーとしてトラヒックの監視を行うための選択的ミラーリングモジュール、対象のトラヒックに対して制御を実行する階層化シェイパモジュールのハードウェアを開発した。また、これらのハードウェアを制御するための制御モジュールを開発した。

② 広域ネットワークトラヒック制御技術の確立

観測・制御のための設備、自動転送型ファイル共有ソフト検知のための設備が広い地域に分散して配置されている場合に対応した、広域ネットワーク対応自動転送型ファイル共有ソフト検知・制御技術を確立した。帯域を圧迫しているトラヒックを自動的に検出する過大トラヒックの自動検出機能、離れた拠点にある解析装置にミラーリングを行うリモートミラーリング機能、解析結果を受けて該当するトラヒックの制御を行う帯域制御機能を開発した。

３．２　流出情報の検知・削除技術

３．２．１　情報マーキング技術

マークが付与される可能性のある情報としては、文書データや画像データ，音楽データなど様々な形式のものが想定されることから、元情報の種別に依存せずできるだけ汎用的に適用可能な情報マーキング技術が望ましい。そこで、本研究開発においては、利用される可能性の高い少なくても 10 種類以上の形式の情報に対して適用可能な情報マーキング技術の実現を最終的な目標とする。またその際に、マークが文書作成ソフトなど他のアプリケーションに影響を及ぼすことのないよう留意する。

一方、自動転送型ファイル共有ソフトが情報を暗号化して送受信する機能を有していた場合、マークの形式や元情報との関連付け方法、マークを付与するタイミングなどによっては、付与したマークを検知することができなくなってしまう恐れがある。

そのため、初年度は、暗号化機能のない自動転送型ファイル共有ソフトと暗号化機能を有した自動転送型ファイル共有ソフトそれぞれについて、最適なマークの形式や元情報との関連付け方法、マークを付与するタイミングなどに関する基本方針を確立する。その際、ユーザの意思確認方法については、利便性を損なうことなく、かつ誤設定等のリスクをできるだけ軽減したユーザインタフェースの実現を目指す。

2 年目以降は、初年度の結果にしたがい、少なくても 2 種類以上の自動転送型ファイル共有ソフトを対象として、情報マーキング機能を試作してその有効性を検証する。

上記目標を達成するために、第一年目に各課題に関する基本方式の検討ならびに要素技術の開発を行い、第二年目に第一年目に開発した要素技術に基づく試作モジュールの開発を行い、第三年目に試作モジュールの処理の高速化を行うとともに、必要な機能拡張・強化を図った。以下、詳細について説明する。

(1) 情報マーキング技術

① 機密属性に基づく保護マーク付与技術の確立

利用者端末において、自動転送型ファイル共有ソフトのネットワークに流出させたくないファイルに対し、ファイル形式に依存せず機密属性を付与するモジュールを開発した。機密属性の付与にあたっては一般利用者による利用を想定し、機密属性管理のための GUI を設計し開発した。機密属性の設定漏れによる情報漏えいを避けるため、全てのファイルに機密属性が付与されているものとし、自動転送型ファイル共有ソフトで共有したいファイルのみ機密属性を解除する仕組みとした。この機密属性に基づき、端末内のファイルアクセスを監視し、機密属性の付与されたファイルが自動転送型ファイル共有ソフトによって共有されるときにこれを検知し、共有を阻止するモジュールを開発した。

また、利用者端末における OS の機能呼び出しやファイルアクセスの監視により端末が暴露ウイルスに感染していることを検知するモジュール、暴露ウイルスなどに見られるアイコン偽装を行っている実行ファイルを検知するモジュールを開発した。

これらのモジュールによって端末の異常状態（機密属性の付与されたファイルが流出しそうになった、暴露ウイルスを検知した、など）が検知された場合に、利用者端末から送出されるパケットに保護マークを付与するモジュールを開発した。保護マークとして付与する情報は、利用者端末の異常状態に関する情報に加え、付与対象のパケットを送出しようとしているプログラムの情報とし

た。また、保護マークの付与方式は、付与による既存のプログラムの通信への影響がないようにするため、パケットのヘッダ部に付与する方式とした。

(2) 流出情報を解析し特定可能な特徴情報を抽出する流出情報特徴解析技術の研究開発

① 流出情報のフォーマットに応じた流出情報の内容解析技術の研究開発

企業内での情報交換によく利用されると考えられるファイルフォーマットの内容を解析する流出情報特徴解析技術を開発し、当初予定の２種類のファイル形式だけではワード、エクセルの２つのアプリケーションのファイル形式だけに限定してもバージョンによって複数のファイルフォーマットがあり、最終的にワード、エクセルそれぞれの 2000 形式、2002 形式、2003 形式、2007 バイナリ形式、2007ooxml 形式の合計１０種のファイル形式を解析し、特徴情報として抽出可能な特徴部分とそれ以外の無特徴部分とに分割する技術を確立した。

② 内容解析結果にもとづいて流出情報の特徴情報を抽出する技術の研究開発

流出情報の特徴情報を抽出する特徴情報抽出技術を開発し、流出したファイルと同じファイルだけでなく、何気ない操作によってオリジナルファイルから変化してしまった亜種ファイルに対しても同じシグネチャでファイルマッチングが可能な特徴情報を抽出する技術を確立した。

さらに、後述の流出情報を検知・削除する技術を用いて、Winny と Gnutella の２種類の P2P ネットワーク上で流出ファイルの検知・削除実験を行い。各ファイル形式に対して、18 種の亜種生成操作により生成できた 218 種のファイルの検知･削除実験を行い、２種の P2P ネットワークともに 218 種中 194 ファイルの検知・削除が可能であった。これは、全ファイル種別中の約 90%である。

３．２．２　マーク付き情報検知・削除技術

初年度は、上記 3.2.1 での検討結果を考慮して、ユーザ利用端末やネットワーク上に設置された特定の装置においてマーク付き情報を検知削除するための､少なくとも 2 種類以上の基本方式を確立し、それぞれの方式について比較・検討する。また、予備的な調査として、5000 台程度のユーザ端末等からなるネットワークシミュレーション環境を構築し、当該シミュレーション環境において、上記基本方式の機能や性能等の検証を行う。

2 年目は、初年度のネットワークシミュレーション環境での検証結果にしたがって基本方式をブラッシュアップするとともに、当該基本方式を実装したマーク付き情報検知・削除モジュールを試作する。

更に、数十台程度のユーザ利用端末からなるリアルな実験ネットワーク環境を構築し、当該実験ネットワーク環境において、試作したモジュールの機能や性能等を確認する。本実験においては、送受信されるデータを観測し、当該データがマーク付き情報であるか否かを判定する処理などがシステム全体に及ぼすオーバヘッドを検査し、利用者に不快感を与えることのないレベル性能（送受信されるデータを観測し、当該データがマーク付き情報であるか否かを判定する処理を追加することによるオーバヘッドが１秒程度）を達成することを目標とする。

更に、最終年度に向けて、試作モジュールの大規模対応化、処理の高速化等を図るとともに、より大きな規模での実証実験を実施し、試作モジュールの有効性（機能、性能、配置、コスト等）を検証する。最終的には、本技術開発の成果を実ネットワークへ適用した場合のオーバヘッドを、1Gbps 回線で 5%以内、10Gbps 回線で 10%以内に抑えることを目標とする。

上記目標を達成するために、第一年目に各課題に関する基本方式の検討ならびに要素技術の開発を行

い、第二年目に第一年目に開発した要素技術に基づく試作モジュールの開発を行い、第三年目に試作モジュールの処理の高速化を行うとともに、必要な機能拡張・強化を図り、大規模なネットワーク環境において実証実験を行った。以下、詳細について説明する。

(1) 保護マーク付き情報検知・削除技術

① ネットワーク上での保護マーク付き情報検知・削除技術の確立

前述した保護マークが付与されたパケットをネットワーク上の機器で検知しポリシに基づいて処理を行う技術を開発し、利用者がインターネットへの接続に用いるインテリジェントゲートウェイへのハードウェア実装を行った。数百台規模のネットワークでの実験により、インテリジェントゲートウェイの処理性能が、一般利用者のインターネット接続環境に適用するのに十分なスループットを実現できるものであり、オーバヘッドを1秒以内に抑えられることを確認した。

② 利用者端末上での保護マーク付き情報検知・削除技術の確立

保護マークが付与されたパケットを利用者端末上で検知しポリシに基づいた処理を行う技術を開発し、利用者端末上で動作するモジュールを開発した。

開発した保護マーク付与モジュール及びネットワーク上での保護マーク検知モジュール、利用者端末上での保護マーク検知モジュールについて、数百台規模のネットワークにおける有効性評価実験を実施し、これらのモジュールによる情報漏えい対策が有効に働くことを確認した。

また、ネットワーク上での保護マーク付き情報検知・削除技術、利用者端末上での保護マーク付き情報検知・削除技術での検知情報を「３．１．２ (2) ①トラヒック制御技術の確立」で述べた制御モジュールへと送信する機能を開発した。この機能により、10Gbps レベルのトラヒックが流れるネットワークの基幹部において、異常な状態にある端末のトラヒックをオーバヘッドなく制御することが可能となる。

前述した保護マークの付与およびネットワーク機器や利用者端末における保護マーク付きパケットの検知・処理による情報漏えい対策に加え、既に自動転送型ファイル共有ソフトのネットワークに流通している流出情報への対策を行う技術を開発した。具体的には、自動転送型ファイル共有ソフトのネットワークで流通しているファイルの属性情報（流出ファイルであるか、マルウェアが含まれているか、著作権を侵害したファイルであるか、等）を格納する P2P ファイル情報データベース、利用者端末でダウンロードされたファイルが流通してはならないファイルである場合に当該ファイルの削除を行うダウンロード検知モジュールを開発した。また、自動転送型ファイル共有ソフトのネットワークで流通している流出ファイルに関して自動的にファイル拡散抑止情報を送信するシステムを開発した。

また、「３．２．２ (2) 流出情報の検知にもとづいて特定情報の通信を遮断する流出情報通信遮断技術」との連携機能を開発し、利用者端末においても流出情報の亜種情報を検知・削除可能なようにした。この他、後述する「情報の来歴管理等の高度化・容易化に関する研究開発」との連携、DRM (Digital Rights Management) ソリューションとの連携について連携方式を開発した。

(2) 流出情報の検知にもとづいて特定情報の通信を遮断する流出情報通信遮断技術

① 高速パケット処理装置の検知結果から流出情報の通信パケット情報を構成する技術の研究開発

高速パケット処理装置からのパケットを受け取り前述の特徴抽出技術を用いて作成されたシグネチャと高速にマッチングを行うことで流出情報とその亜種ファイルを発見し、その通信を制限する

ための通信制限設定情報生成機能を開発し、マルチ Gbps のトラヒック中から流出情報もしくはその亜種ファイルが含まれているときに、ファイルを転送する通信を切断する設定を作成する技術を確立した。

② 通信パケット情報にもとづいて通信制限装置の通信制限設定情報を生成する技術の研究開発

高速パケット処理装置からのパケットを受け取り前述の特徴抽出技術を用いて作成されたシグネチャと高速にマッチングを行うことで流出情報とその亜種ファイルを発見し、その通信を制限するための通信制限設定情報生成機能を開発し、マルチ Gbps のトラヒック中から流出情報もしくはその亜種ファイルが含まれているときに、ファイルを転送する通信を切断する設定を作成する技術を確立した。

また、通信パケット情報生成機能を含む流出情報検知・削除システムを、インターネットのトラヒックを模した疑似インターネット環境の基幹部に相当するネットワークに接続し最大 2.4Gbps のトラヒックが処理できることを確認した。さらに、そのトラヒックに含まれる Winny、Gnutella の２種類の P2P ネットワークに対して流出情報やその亜種ファイルを流通させ、流通情報やその亜種ファイルが検出、削除できることを確認した。

３．３　その他の研究実績

(1) 他プロジェクトとの連携

総務省委託研究「情報の来歴管理等の高度化・容易化に関する研究開発」との連携について検討を行った。具体的には、上記プロジェクトが情報漏えいの未然の防止を目的としたものであること、本研究開発で開発した技術では既に自動転送型ファイル共有ソフトのネットワークに流通してしまった漏えい情報の流通抑止を実現できることから、来歴管理システムによって管理されている電子ファイルが故意もしくは過失により来歴管理システムの対象組織外へと漏えいし、そこからさらに自動転送型ファイル共有ソフトのネットワークへと流出してしまっている状況を想定し、それぞれのプロジェクトで開発した技術が連携し被害の最小化を図ることができるような連携方式を開発した。

(2) 研究成果の展開（普及・啓発）

初年度より国内の学会や国際会議等において対外的な研究発表を積極的に進めてきた。また、通信事業者およびセキュリティ技術や P2P 技術に精通した関連ベンダ等との連携を強化するため、安心・安全・便利に利用できるインターネット環境の実現を目的として活動している、安心・安全インターネット推進協議会　P2P 研究会を中心とした、関係者との情報・問題意識の共有を図ってきた。

また、学会や国際会議の場だけでなく、本研究成果を広く世の中に知らせ、P2P の現状に対する認識の共有、安心・安全な P2P 技術の開発・普及・発展を図るために、得られた知見や研究成果を発表した情報セキュリティセミナーを開催した。

(3) 研究成果の展開（製品化）

本研究で得られた成果のうち P2P トラヒックの帯域制御技術に関するノウハウを、トラフィック制御機能およびネットワーク・パーティションとの連携機能に活用し、AX6600S シリーズで製品化。

また、本研究を推進する過程で作成したネットワーク状況確認ツールのネットワーク装置からネットワーク情報を収集し、ビジュアルに管理する機能を製品化した。

(4)実証実験の実施

開発した各技術の有効性を評価するため、情報通信研究機構北陸リサーチセンターが運用する大規模汎用テストベッドである StarBED を利用し、大規模なネットワークにおける実証実験を行なった。

実証実験を行うにあたっては、アンケート調査結果に基づき、P2P ノードで稼働させる自動転送型ファイル共有ソフトの台数を決定し（1020 台の P2P ノードからなる実験環境を構築）、実際のインターネット環境を模擬するために、バックボーンルータ、エッジルータ、ホームルータから構成される 3 階層のネットワークトポロジを構築し、①ISP カスタマエッジ（ISP トラヒック調査を基にトラヒック量、トラヒックパターンを再現）、②大学 GW（某大学の GW に流れるトラヒックパターンを再現）、③架空の GW（未知の P2P 通信が存在するトラヒックパターンを生成）の 3 つの広域ネットワーク環境を模擬した実験環境を StarBED 上に構築した。

インターネットを模した環境でスループットの測定、性能評価を行い、課題 1 の目標である、10Gbps のバックボーンを持つネットワークにおいて情報漏洩発生件数を 10%以下に抑えること、課題 2 の目標である、2 種類以上のファイル形式での流出情報の発見・削除および、マルチ Gbps のトラヒック処理が可能であることが確認できた。この結果、自動転送型ファイル共有ソフトの優れた特長を損なうことなく、情報通信ネットワークを通じた情報漏えいの検知技術、及び当該漏えい情報の自動流通停止技術を確立した。

4　研究成果の更なる展開に向けて

本研究開発で確立した情報マーキング技術等の要素技術を IETF 等の国際標準化機関に提案し、本国産技術の国内外での普及展開を図る。

P2P 研究会の活動は、平成 22 年度以降も継続し、自動転送型ファイル共有ソフトの利用や著作権侵害に関する注意喚起などの対外的な情報発信を進めていくとともに、関連する団体（財団法人日本データ通信協会テレコムアイザック推進会議やサイバークリーンセンターなど）との連携を図っていく予定である。また、本研究成果である動的トラヒック制御技術、アラクサラ AX シリーズを中心に、キャリアユーザへの適用・展開を目指す。

本研究開発終了後も、自動転送型ファイル共有ソフトに関連する技術・社会動向の把握を進め、有効な対策技術の確立を目指すとともに、研究成果の利用を積極的に働きかけることにより、本研究開発で確立した技術の普及啓発を図っていきたい。

波及効果：自動転送型ファイル共有ソフトの特長の一つである匿名性が情報漏えいや著作権侵害の温床ともなっており、本技術による自動転送型ファイル共有ネットワークの透明性向上によって、自動転送型ファイル共有ソフトの利用抑止による情報漏えい事故の低減や、違法ファイルや漏えいファイルの収集家に対する抑止力の効果が期待できる。

５　査読付き誌上発表リスト

６　その他の誌上発表リスト

[1]古泉聡洋、“ネットワーク管理・運用負荷を軽減する「論理ネットワークビジュアルマネージャー」”、日立評論 Vol.91 No.11 pp822-825（2009 年 11 月 1 日）:

[2]仲小路博史、“社会イノベーションを支える先進セキュリティ技術”、日立評論 Vol.91 No.12 pp60-65（2009 年 12 月 10 日）:

７　口頭発表リスト

H19 年度

[1]寺田真敏、“P2P Network Observation using Crawling Method”、FIRST Technical Colloquium（マレーシア）（2007 年 8 月 22 日）

[2]寺田真敏、“ファイル交換ソフトの利用状況に関する調査報告”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2007 年 12 月 3 日）

[3]重本倫宏、“シミュレーションによる P2P ネットワークの調査報告”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2007 年 12 月 20 日）

[4] 寺田真敏、“トラヒック監視、流量調査に基づく P2P ソフトウェア利用状況調査”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 2 月 28 日）

[5] 寺田真敏、“トラヒック監視、流量調査に基づく P2P ソフトウェア利用状況調査”、JPCERT/CC CSIRT 関連組織会合（東京）（2008 年 3 月 5 日）

[6] 寺田真敏、“P2P ファイル交換ソフトウェア環境における情報流通対策アーキテクチャの検討”、DPS／CSEC 合同研究発表会（京都）（2008 年 3 月 7 日）

H20 年度

[7]寺田真敏、“P2P 通信検知ツール”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 4 月 17 日）

[8]仲小路博史、“Winny ネットワークの制御技術の検討 ～ポイズニング実験ほか～”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 4 月 17 日）

[9]寺田真敏、“Safeny 等 Winny に関するパッチについて”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 5 月 29 日）

[10]寺田真敏、“Winny の Port0 接続数の調査”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 5 月 29 日）

[11]鬼頭哲郎、“端末内での活動監視に基づく暴露ウイルス検知手法”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 5 月 29 日）

[12]大河内一弥、“サイバー攻撃対策技術”、日立製作所システム開発研究所 第 13 回テクノロジーコミュニティ（神奈川）（2008 年 6 月 6 日）

[13]仲小路博史、“サイバー攻撃対策技術”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2008 年 7 月 10 日）

[14]洲崎誠一、“セキュリティ技術最前線 2008”、日立製作所 uVALUE コンベンション 2008（東京）（2008

年 7 月 18 日）
[15]寺田真敏、鬼頭哲郎、仲小路博史、“P2P ファイル交換ソフトウェア環境におけるノード型情報流通防止機能の提案”、情報処理学会　第 42 回 CSEC 研究会（福岡）（2008 年 7 月 24 日）
[16]寺田真敏、“P2P ファイル交換ソフトウェア環境における情報流通対策向けデータベースの検討”、情報処理学会　第 42 回 CSEC 研究会（福岡）（2008 年 7 月 24 日）
[17]鬼頭哲郎、“端末内の動作監視に基づく情報漏えいウイルスの検知手法に関する検討”、情報処理学会 第 42 回 CSEC 研究会（福岡）（2008 年 7 月 25 日）
[18]重本倫宏、“コネクション解析による P2P 通信端末検知手法”、情報処理学会　第 42 回 CSEC 研究会（福岡）（2008 年 7 月 25 日）
[19]寺田真敏、鬼頭哲郎、仲小路博史、“IP マーキングによる不正活動ホストの広報機能の開発”、情報処理学会　第 42 回 CSEC 研究会（福岡）（2008 年 7 月 25 日）
[20]仲小路博史、“P2P ノードの分布傾向～P2P 型ファイル共有ネットワークの見える化～”、安心・安全インターネット推進協議会 第 1 回 情報セキュリティセミナー（東京）（2008 年 9 月 10 日）
[21]江頭徹、“P2P ファイル交換の選択的制限手法”、コンピュータセキュリティシンポジウム 2008（沖縄）（2008 年 10 月 8 日）
[22]寺田真敏、鬼頭哲郎、仲小路博史、“P2P ファイル交換ソフトウェア環境におけるノード型情報流通対策システムの実装”、コンピュータセキュリティシンポジウム 2008（沖縄）（2008 年 10 月 8 日）
[23]鬼頭哲郎、“端末内の動作監視に基づく情報漏えいウイルスの検知手法の実装と評価”、コンピュータセキュリティシンポジウム 2008（沖縄）（2008 年 10 月 8 日）
[24]寺田真敏、“P2P ファイル交換ソフトウェア Winny を対象としたオーバレイネットワークの制御実験”、北陸リサーチセンターワークショップ 第 2 回（東京）（2008 年 11 月 12 日）
[25]大河内一弥、“サイバー攻撃対応検知・分析技術”、北陸・日立グループフェア 2008（富山）（2008 年 11 月 20 日）
[26]寺田真敏、“Feasibility Study of DoS attack by P2P network”、2009 FIRST Symposium（ラトビア）（2009 年 1 月 20 日）
[27]寺田真敏、“P2P ファイル交換ソフトウェア Winny を対象としたオーバレイネットワークの制御実験”、NTT-CERT セキュリティワークショップ（東京）（2009 年 2 月 10 日）
[28]鍛忠司、“P2P ネットワークのセキュリティ”、電子情報通信学会　総合大会（愛媛）（2009 年 3 月 19 日）
H21 年度
[29]寺田真敏、“P2P ファイル交換ソフトウェア Winny を対象としたオーバーレイネットワークの制御実験”、第 164 回ソフトウェア工学・第 45 回コンピュータセキュリティ・第 13 回組込みシステム合同研究発表会（東京）（2009 年 5 月 29 日）
[30]重本倫宏、“Winny ネットワークにおけるファイルダウンロード時間の調査”、安心・安全インターネット推進協議会 P2P 研究会（東京）（2009 年 6 月 16 日）
[31]大河内一弥、“P2P ファイル交換ソフトウェアを対象としたトラヒック分析・制御システムの基本アーキテクチャの提案”、情報処理学会 第 46 回コンピュータセキュリティ研究発表会（秋田）（2009 年 7 月 3 日）
[32]洲崎誠一、“セキュリティ技術最前線 2009”、日立製作所 uVALUE コンベンション 2009（東京）（2009

年 7 月 22 日）

[33]川口信隆、大河内一弥、寺田真敏、“Detection of Peer-to-Peer Nodes based on Query Routing”、APSIPA Annual Summit and Conference 2009（札幌）（2009 年 10 月 4 日）

[34]寺田真敏、“P2P ファイル交換ソフトウェア環境向け注意喚起メッセージングシステムの提案”、コンピュータセキュリティシンポジウム 2009（富山）（2009 年 10 月 28 日）

[35]古泉聡洋、“ネットワーク管理・運用負荷を軽減する論理ネットワークオペレーティングシステム”、ITpro EXPO 2009（東京）（2009 年 10 月 28 日）

[36]重本倫宏、“P2P ファイル交換ネットワークの構築及びその活用事例”、StarBED Techinical Workshop 2009（東京）（2009 年 12 月 8 日）

[37]寺田真敏、“情報漏えい対策技術の研究開発”、安心・安全インターネット推進協議会 第 2 回 情報セキュリティセミナー（東京）（2010 年 3 月 2 日）

[38]寺田真敏、“Feasibility study of the control possibility of P2P network”、ICT システムテストベッドに関する国際シンポジウム（東京）（2010 年 3 月 30 日）

8 出願特許リスト

H19 年度

[1]仲小路博史、P2P 通信検出装置、及びその方法とプログラム、日本、2007 年 11 月 14 日

[2]江頭徹、島村英、ピアツーピア型通信制限装置及び 通信制限方法並びに通信制限プログラム、日本、2007 年 12 月 5 日

[3]鬼頭哲郎、情報流出検知方法、情報流出検知装置、情報流出検知システム、日本、2008 年 1 月 21 日

[4]寺田真敏、ファイルダウンロード観測装置、日本、2008 年 3 月 4 日

H20 年度

[5]重本倫宏、P2P 端末検知及び制御システム、並びにその方法、日本、2008 年 5 月 26 日

[6]重本倫宏、P2P 通信制御システム及び制御方法、日本、2008 年 6 月 2 日

[7]江頭徹、島村英、通信制限システム、通信制限装置、通信制限方法、および通信制限プログラム、日本、2008 年 9 月 16 日

[8]大河内一弥、トラヒック監視・制御システム及び方法、日本、2008 年 9 月 22 日

[9]鬼頭哲郎、不正プログラム検知方法、不正プログラム検知プログラムおよび情報処理装置、日本、2009 年 2 月 27 日

[10]大河内一弥、トラヒック観測・制御システム、日本、2009 年 3 月 11 日

[11]川口信隆、端末検出方法、端末検出プログラム、および端末検出装置、日本、2009 年 3 月 24 日

H21 年度

[12]川口信隆、端末検出方法、および端末検出装置、日本、2009 年 12 月 10 日

[13]榊啓、情報漏洩防止システム、情報漏洩防止方法及び情報漏洩防止プログラム、日本、2009 年 12 月 21 日

[14]榊啓、情報漏洩防止システム、情報漏洩防止方法及び情報漏洩防止プログラム、日本、2009 年 12 月 21 日

[15]重本倫宏、P2P 通信のコンテンツ制御装置、日本、2010 年 1 月 5 日

[16]大河内一弥、トラヒック制御システムおよびトラヒック制御データ生成プログラム、日本、2010 年 1

月 15 日

[17]鬼頭哲郎、ユーザ端末保護方法、およびシステム、日本、2010 年 3 月 8 日

[18]大河内一弥、トラヒック観測システム、日本、2010 年 3 月 9 日

[19]重本倫宏、P2P 端末検知装置、P2P 端末検知方法、および P2P 端末検知システム、日本、2010 年 3 月 24 日

９　取得特許リスト

１０　国際標準提案リスト

１１　参加国際標準会議リスト

[1]FIRST・FIRST Technical Colloquium、マレーシア、2007 年 8 月 22 日

[2]FIRST・2009 FIRST Symposium、ラトビア、2009 年 1 月 20 日

１２　受賞リスト

１３　報道発表リスト

H20 年度

[1]“「P2P 技術の“前向き”な活用方法を探る」――業界団体セミナーで総務省が講演”、ITpro、2008 年 9 月 12 日

[2]“P2P ソフトを解析し，活用に向けての可能性を探る「P2P の現状～Winny の解析と P2P ノードの見せる化～」セミナー・レポート”、ITpro、2008 年 9 月 22 日

[3]“P2P で流通するファイルの 20 ファイルにひとつがマルウェア（HIRT）”、Scan NetSecurity、2008 年 12 月 10 日

[4]“ファイル共有ソフトの「現在利用者」は 10.3%、ACCS などが調査”、Interenet Watch、2008 年 12 月 12 日

[5]“ファイル共有ソフトの「現在利用者」、1 割超える――ACCS など調査”、ITmedia、2008 年 12 月 12 日

[6]“初めて 1 割を超える、ファイル共有ソフト利用者―ACCS ら 3 団体が調査結果を公表”、japan.internet.com、2008 年 12 月 12 日

[7]“ファイル共有ソフトの現在利用者が 1 割を超える--ACCS などが調査”、Scan NetSecurity、2008 年 12 月 12 日

[8]“Winny を流れるファイルの 5%はウイルス”、ITpro、2008 年 12 月 12 日

[9]“Winny で流通するファイルの約 5%にマルウェアとの調査結果”、Interenet Watch、2008 年 12 月 12 日

[10]“ファイル交換ソフトによる情報漏えいの影響が増大--HIRT が調査”、Scan NetSecurity、2008 年 12 月 15 日

[11]“ファイル共有ソフト利用者の 3 人に 2 人は情報流出を心配”、Interenet Watch、2008 年 12 月 15 日

[12]“ファイル共有ソフト利用者の 4 人に 1 人は漏洩ファイルの入手経験あり--日立グループ調査”、CNET

Japan、2008 年 12 月 16 日
H22 年度
[13]“ダイナミック省電力機能を搭載した省スペース型高信頼コアスイッチ AX6600S シリーズを提供”、ZDNet Japan、2009 年 4 月 23 日
[14]“日立、GUI で VLAN 構成を可視化できるネットワーク管理ソフト”、Enterprise Watch、2009 年 10 月 26 日
[15]“日立、VLAN のネットワーク情報を可視化し管理作業を効率化する新製品”、ZDNet Japan、2009 年 10 月 26 日
[16]“P2P に流出したファイルの拡散を抑止する技術、NEC が開発”、ITmedia Enterprise、2010 年 3 月 2 日
[17]“NEC、P2P ソフトで漏えいしたファイルを特定/流通停止できる技術を開発”、Softbank ビジネス IT、2010 年 3 月 2 日
[18]“NEC、ネットワークへの情報漏洩後に状態が変化した派生ファイルでも特定・流通停止できる技術を開発”、Asahi.com、2010 年 3 月 2 日
[19]“NEC、PtoP での情報漏洩に歯止めをかける技術を開発--派生ファイルも特定可能”、Japan CNET、2010 年 3 月 2 日
[20]“NEC、PtoP での情報漏洩に歯止めをかける技術を開発--派生ファイルも特定可能”、ZDNet、2010 年 3 月 2 日
[21]“「悪意ある放流者は追い詰める」日本 IBM が Share 流出を振り返る”、Interenet Watch、2010 年 3 月 3 日
[22]“高木浩光氏「Winny は適法に使えない」”、Interenet Watch、2010 年 3 月 3 日
[23]“Winny などの P2P ソフトに流出したファイルを特定して流通停止できる技術が開発される”、GIGAZINE、2010 年 3 月 3 日
[24]“NEC、P2P 情報漏えいで派生ファイルも特定できる技術を開発”、Internet Watch、2010 年 3 月 3 日
[25]“高負荷ネットワークからファイル共有ソフト上の漏洩データを検出、削除する技術 - NEC が開発”、セキュリティネクスト、2010 年 3 月 3 日
[26]“ネット上の流出検知 「ウィニー」使用を抑止”、日刊工業新聞/20 面、2010 年 3 月 3 日
[27]“P2P ソフトの情報で漏えい対策技術開発 漏えいファイルを特定 流通停止を実証”、電波新聞/3 面、2010 年 3 月 3 日
[28]“ＮＥＣ、情報ネット漏洩防止、ファイル交換ソフト対策。”、SECURITY SHOW、2010 年 3 月 4 日
[29]“NEC 情報ネット漏洩防止 ファイル交換ソフト対策。”、日経産業新聞/12 面、2010 年 3 月 4 日

１４　ホームページによる情報提供

H19 年度
[1]“ファイル交換ソフトによる情報漏えいに関する調査結果”、http://www.hitachi.co.jp/hirt/publications/hirt-pub07012/index.html、インターネットユーザのファイル交換ソフト利用状況や意識に関して行った調査結果について紹介（2007 年 12 月 21 日）
[2]“クローリング調査を用いたファイル交換ソフトのノード数推定”、

http://www.hitachi.co.jp/hirt/publications/hirt-pub08001/index.html、クローリング調査を用いたファイル交換ソフトのノード数推定について紹介（2008 年 1 月 16 日）

H20 年度

[3]“P2P ファイル交換ソフト環境で流通するマルウェア”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub08007/index.html、2008 年に実施した P2P ファイル交換ソフト環境のコンテンツ流通実態調査結果について紹介（2008 年 12 月 10 日）

[4]“2008 年ファイル交換ソフトによる情報漏えいに関する調査報告”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub08008/index.html、インターネットユーザのファイル交換ソフト利用状況や意識に関して行った調査結果について紹介（2008 年 12 月 12 日）

[5]“ファイル交換ソフト環境の観測活動掲載の和（輪）”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub08006/index.html、安心・安全インターネット推進協議会と連携して進めている、ファイル交換ソフト環境に関連する研究活動について紹介（2009 年 3 月 9 日）

[6]“ファイル交換ソフトのノード数推定　～Winnyp ノード数～”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub08009/index.html、Winny と互換性のあるファイル交換ソフト Winnyp のノード数推定について報告（2009 年 3 月 23 日）

H21 年度

[7]“ダイナミック省電力機能を搭載した省スペース型高信頼コアスイッチ AX6600S シリーズ”、
http://www.alaxala.com/jp/news/press/2009/20090423.html、本研究開発成果を活用した製品化のニュースリリース（2009 年 4 月 23 日）

[8]“ファイル交換ソフトにおける流通ファイル数の推定”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub09005/index.html、ファイル交換ソフトにおける流通ファイル数の推定について紹介（2009 年 6 月 8 日）

[9]“ネットワーク管理・運用負荷を軽減する論理ネットワークオペレーティングシステム”、
http://www.hitachi.co.jp/New/cnews/month/2009/10/1026a.html、本研究開発成果を活用した製品化のニュースリリース（2009 年 10 月 26 日）

[10]“2009 年ファイル交換ソフトによる情報漏えいに関する調査結果”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html、インターネットユーザのファイル交換ソフト利用状況や意識に関して行った調査結果について紹介（2009 年 12 月 22 日）

[11]　“P2P ファイル交換ソフト環境で流通するマルウェア(2009 年)”、
http://www.hitachi.co.jp/hirt/publications/hirt-pub09007/index.html、2009 年に実施した P2P ファイル交換ソフト環境のコンテンツ流通実態調査結果について紹介（2010 年 3 月 1 日）

[12]“ネットワークへの情報漏洩後に状態が変化した派生ファイルでも特定･流通停止できる技術を開発”、
http://www.nec.co.jp/press/ja/1003/0203.html、本研究開発成果のニュースリリース（2010 年 3 月 2 日）

研究開発による成果数

	平成 19 年度	平成 20 年度	平成 21 年度
査読付き誌上発表数	0 件（0 件）	0 件（0 件）	0 件（0 件）
その他の誌上発表数	0 件（0 件）	0 件（0 件）	2 件（0 件）
口頭発表数	5 件（1 件）	21 件（1 件）	10 件（0 件）
特許出願数	4 件（0 件）	7 件（0 件）	8 件（0 件）
特許取得数	0 件（0 件）	0 件（0 件）	0 件（0 件）
国際標準提案数	0 件（0 件）	0 件（0 件）	0 件（0 件）
国際標準獲得数	0 件（0 件）	0 件（0 件）	0 件（0 件）
受賞数	0 件（0 件）	0 件（0 件）	0 件（0 件）
報道発表数	0 件（0 件）	12 件（0 件）	17 件（0 件）

	合計	（参考） 提案時目標数
査読付き誌上発表数	0 件（0 件）	4 件（0 件）
その他の誌上発表数	2 件（0 件）	0 件（0 件）
口頭発表数	36 件（2 件）	27 件（3 件）
特許出願数	19 件（0 件）	13 件（0 件）
特許取得数	0 件（0 件）	2 件（0 件）
国際標準提案数	0 件（0 件）	0 件（0 件）
国際標準獲得数	0 件（0 件）	0 件（0 件）
受賞数	0 件（0 件）	0 件（0 件）
報道発表数	29 件（0 件）	5 件（0 件）

注１：　（括弧）内は、海外分を再掲。

注２：　「査読付き誌上発表数」には、論文誌や学会誌等、査読のある出版物に掲載された論文等を計上する。学会の大会や研究会、国際会議等の講演資料集、アブストラクト集、ダイジェスト集等、口頭発表のための資料集に掲載された論文等は、下記「口頭発表数」に分類する。

注３：　「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等を計上する。