# 博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　企業情報システムにおけるセキュアな情報共有モデルの研究
申請者　：　荒井正人
審査委員会　：　主査　教授　田中英彦
副査　教授　小柳和子
副査　教授　佐藤直
副査　教授　土井洋
副査　客員准教授　辻秀典

## Ⅰ．論文内容の要旨

本論文は、「企業情報システムにおけるセキュアな情報共有モデルの研究」と題し、7 章と付録などからなる。近年、社会インフラとして IT システムやインターネットの利用が拡大する一方で、社内機密情報や個人情報の漏洩といった問題が深刻化している。その原因には、紛失・置き忘れ、盗難、誤操作、ワーム・ウイルス、などがあり、PC、可搬記録媒体、インターネット、Email などを漏洩経路とするものが多い。この研究は、そのような状況への対策として、機密情報の保護と企業活動における情報共有の双方の両立を可能とするモデルを提案し、それを既存のクライアント PC へ容易に導入可能とする実現方式を考察したものである。

第１章は「緒言」で、本研究の背景と研究の範囲、目的、及び論文の構成についてまとめたものである。

第２章は「一般的な漏洩対策技術とその課題」で、企業の業務プロセスで収集、参照、生成される情報を公開可能な一般情報と機密情報とに分類し、プロセスに潜む情報漏洩問題を論じ、まず、それに対する従来技術として、アンチウイルスソフト、暗号化ツール、コンテンツフィルタリング、デジタル著作権管理システムを挙げ、それらの特徴と課題について整理している。その結果、それらの組み合わせで強固なセキュリティ対策にはなるものの、情報の保護と共有を両立させる上では多くの課題があることを指摘している。すなわち、既存のアンチウイルスソフトでは新種のワーム・ウイルスには効果が薄く、防止は不正なファイルアクセスのみである。また、情報の暗号化ツールは、情報を暗号化するか否かの区別が負担であり、逆に、すべてを暗号化すると業務における情報共有が阻害され、機密情報の安全な共有には、鍵の配布・共有手段の問題がある。コンテンツフィルタリングは管理者による機密性の分類が大きな負荷になる、またデジタル著作権管理システムは作業中文書の保護や共有には不向きであり、閲覧ソフトが限定されるという問題もある。

第３章は「セキュア情報共有モデルの提案」で、第２章の考察を踏まえ、情報の共有と保護のあり方を見直し、根本的な対策のモデルとして、セキュア情報共有モデルを提案している。その基本方針は、公開可能な情報と機密情報とを区別可能であること、一般情報の利用に制限はなく、機密情報についても専用応用プログラムを用いずとも利用・保護が可能であること、機密情報であっても可搬記録媒体やインターネットを利用しながら安全に共有可能であること、更に、共有と保護を両立するための保護ポリシーの設定が容易であることの 4 つである。その方針に従い、下位主体が上位対象を読み出しする場合、暗号化した形でそれを許可するというモデルを提案している。その結果、従来モデルの Bell-LaPadula モデルでは、上位と下位の間の情報流が一方向であるのに対し、提案モデルでは、情報流が双方向となり、上位の対象を下位主体が読み出し、インターネットなどを用いて拠点間や社外関係者へ情報伝播が可能となっている他、ウイルスに感染し易い下位の主体が上位の対象を破壊することを防いでいる。また、このモデルは

上位下位の 2 階層のみならず、3 階層以上にも容易に拡張可能である。

第 4 章は「実現方式」で、上記モデルを実現するための3機能、Work Space Segregation, Stored Data Encryption, Secure Communicatiaon の実現法を論じたもので、Work Space Segregation には Sandbox を用いたプログラムの実行環境分離を用いること、更に、デスクトップ間の情報分離を確実にするためクリップボード経由のデータ転送をクリアすること、Stored Data Encryption にはファイルシステム層でのアクセス制御と自動暗号化、更に、グループ暗号を用いた鍵管理を用いること、Secure Communication には暗号化した機密ファイルのアクセス制御とプログラム実行環境をまたがるデータ転送制御を、それぞれ提案している。更に、実用上の観点から詳細な実装法を検討するとともに、それらの要素を組み合わせた全体システムの構成とその利用手順を明らかにしている。

第5章は「マルチレベルセキュリティ」で、上記構造に加えて、企業内で更に詳細なセキュリティの区分を設けるための工夫について述べたもので、社外秘クラス、部課クラス、職位クラスなどに機密情報を区分し、各クラスに対応する宛先リストを工夫することにより、負担無くそれらの間の機密制御が可能となることを示している。

第 6 章は「考察」で、提案方式の効果について考察したもので、機密ファイルと一般ファイルの区別が容易となり、セキュリティポリシーはプログラム実行環境ごとに定義可能であること、機密ファイルは既存のプログラムから利用可能であること、社内および社外の関係者に機密情報を安全に伝達可能であることなどを述べている。また、既存技術と比較して、提案手法の優位性を示すとともに、使い勝手を評価し、従来の手順と殆ど手間が変わらないことを与えている。更に、提案手法の脆弱性を考察し、それらに対する対策の組み合わせを提案するとともに、実装時のオーバヘッド対策を考察している。

第 7 章は「結言」である。

## Ⅱ. 論文審査結果の要旨

これを要するに本論文は、企業活動で大きな問題である情報漏洩を減らすとともに、企業活動で重要な情報共有を阻害しないシステムのあり方を考察し、企業内情報を一般と機密に分け、それぞれを扱うデスクトップを切り替えて、一般のデスクトップからのみインターネット利用を可能とし、そのデスクトップからは機密情報のアクセスを許すが暗号化された形に限定するモデルを提案し、組織の部課や役職に応じたグループ暗号を採用することで利用の容易さを図り社外の関係者との情報共有も可能にすることによって、その有効性を示したもので、情報学に貢献するところ少なくない。

よって、本論文は、博士（情報学）の学位請求論文として合格と認められる。

## Ⅲ. 審査経過

本審査委員会は、2009 年 7 月 28 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。