修士論文等にみる情報セキュリティ大学院大学のシステムセキュリティ研究動向

佐藤　直*

概 要

本論文では，情報セキュリティ大学院大学において開学以来提出された修士論文および特定課題研究報告のなかから，情報通信システムのセキュリティを課題としているものを調査し，それらの要点をまとめ研究動向として示した．調査の結果，関連する修士論文等は115 件あり，概ね 22 の分野に分類できることがわかった．特に，マルウェア，ネットワーク攻撃，Web，要求分析と設計開発，の 4 分野が継続的にとりあげられていることが分かった．

1　はじめに

情報セキュリティ大学院大学が 2004 年に開学して以来 10 年が経過し，2013 年度までに修士 249 名，博士 24 名が情報学の学位を取得し修了している．修士課程および博士課程（正確には博士前期課程および博士後期課程）を修了するには，指導教員の研究指導を受け，研究結果を修士論文および博士論文として提出し，審査に合格する必要がある．修士課程については，2005 年度から1年制の課程も設置しており，修士論文に相当する特定課題研究報告を同様に提出して審査を受ける必要がある．

修士論文，特定課題研究報告（以降，両者を合わせて修士論文等と呼ぶ），および博士論文は学生個人の成果と位置づけられるが，その計画立案から成果のまとめまで，各過程において，輪講（研究内容を発表する必修科目）や研究室ゼミでの討論が反映されることが多い．このため，これらの論文は大学としての研究成果ともいうことができ，大学における研究動向を知るよい資料でもある．

しかし，論文の内容が全て公開されているわけではない．博士論文の公開が義務付けらえている一方で，修士論文等については他大学と同様原則非公開扱いである．本学においては修士論文等についてもその成果を学会などで外部発表するよう推奨しているが，セキュリティという研究分野のため公開が憚れる，あるいは，社会人学生が多く，業務繁忙によりその機会に恵まれない，といった事情により，外部発表されない場合も多いようである．

個人的なことになるが，筆者は開学以来，研究指導や論文審査に関わってきた．このため，比較的多くの修士論文等を読ませていただいてはいるものの，時間的制限からすべて

* 情報セキュリティ研究科 教授

に目を通してきたわけではない. 専門領域である情報通信システムセキュリティ分野の論文等であっても内容を詳細に把握しているとはいえない, という反省の念を抱いている.

本学には, 育成する人材像の観点から, 暗号テクノロジ, システムデザイン, 法とガバナンス, セキュリティ/リスクマネジメントという4つのコースを設けており, 筆者はシステムデザインのコースリーダを仰せつかっている. 今回, コースリーダとして紀要を執筆するという良い機会を得たので, 研究テーマがシステムデザインとみなせる修士論文等を通読し, サーベイ論文として研究動向を紹介させていただくことにした.

以下, 2節では, 修士論文等でとりあげられてきた研究テーマを分類して全体的な動向を分析する. 3節では, 各分野の論文の要点を数行程度で紹介する. 最後に, 4節で, サーベイ結果を考察し, 所感を述べる.

2 全体動向

2005 年度から 2013 年度までに提出された修士論文等のうち, システムデザイン系のものは 115 件あった. 修士課程の修了生は 249 名であることから, 修士論文等の 46%はシステム系とみなすことができる. これらの修士論文等を通読し筆者の主観で以下の 22 に分類した.

脆弱性, マルウェア, セキュア OS, アクセス制御, 個人認証, 監視と検疫, フォレンジック, サイドチャネル攻撃, サイバー犯罪, ネットワーク攻撃, セキュリティ評価モデル, Web, 電子メール, P2P ネットワーク, 無線通信, モバイル, ネットワーク制御, 要求分析と設計開発, クラウド, 重要インフラ及び制御システム, 各種情報システム, プライバシー

上記分類は, 概ね, 脆弱性, 攻撃, セキュリティ対策, といったシステムセキュリティに関する要素的なテーマからシステム運用管理・設計開発, さらにセキュリティ関連課題, といった順で並べてある. 論文が複数分野にわたるものも少なくないが筆者の主観で一つの種類に分類した. 115 件を分類し修了年度別に件数を示すと表1のようになった.

表1から, 全体的な動向をまとめると以下のようになる. すなわち, 22 の分類のなかで, 研究テーマとして最もよく選択されているのは, マルウェア, ネットワーク攻撃, Web, および要求分析と設計開発, の 4 つである. さらに, 個人認証, 監視と検疫, と続いている. マルウェア, ネットワーク攻撃, Web, および要求分析と設計開発の 4 分野は年度によらずほぼ一定の割合でテーマとしてとりあげられており, 根強い人気のある研究分野といえるであろう. 件数的には個人認証, 監視と検疫も同程度であるが, 2008 年度までがピークであり, その後テーマとしてとりあげられることが少なくなっている. これはこれらの分野の研究開発が一段落したという現れとみることができる. また, 昨今, セキュリティ分野のバズワードとなっている, サイバー攻撃, ビッグデータとプライバシー, IoT に関する修士論文等は, 表1ではそれぞれ, 重要インフラおよび制御システム, プライバシー, 各種情報システムに該当するが, 件数的にはまだ少なく顕著な動向となっていないように見受けられる.

3 修士論文等の要点

前節では, システム系の修士論文等の傾向を俯瞰した. 本節では, 22 の分類ごと, 修

表1 システム系修士論文等の分類・年度別件数

分類＼年度		2005	2006	2007	2008	2009	2010	2011	2012	2013	計
1	脆弱性				2		1	1		1	5
2	マルウェア		1	2	1	2	1	1	1	1	10
3	セキュアOS					1				1	2
4	アクセス制御	1	2	1							4
5	個人認証	1	4	1	2		1				9
6	監視と検疫	4		1	3						8
7	フォレンジック			1		1				1	3
8	サイドチャネル攻撃					1					1
9	サイバー犯罪		1		2				1		4
10	ネットワーク攻撃		4	1	2			1	2		10
11	セキュリティ評価モデル	1					1				2
12	Web	1	2	2	1	2	1			1	10
13	電子メール		1			2			1	2	6
14	P2Pネットワーク		2		1						3
15	無線通信			1	1		2				4
16	モバイル						1	1	3		5
17	ネットワーク制御				1	1			1		3
18	要求分析と設計開発		2	1	2	3		1	1		10
19	クラウド					1				1	2
20	重要インフラ及び制御システム	1			1		2			2	6
21	各種情報システム			1		1				1	3
22	プライバシー			2				1	2		5

士論文等の中に記述されている要旨や外部発表文献をもとに，要点を 5 行から 7 行程度で示す．最初に，修了生氏名，「タイトル」，（修了年度）を示し，その後に要点を示す．なお，特定課題研究である場合はその旨を（修了年度）に示した．

（1）脆弱性

Web アプリケーション関連で 2 件，名前解決システム関係で 1 件，脆弱性検査で 2 件の修士論文があった．

下川 善久「テスティングフレームワークを活用した SQL インジェクション検出手法」（2008 年度）

SQL インジェクション対策としてエスケープ処理とバインドメカニズムがよく知られているが，前者はプログラマが記述するため対策漏れが生じやすく，後者は構文が動的変化する場合適用が困難であるという欠点がある．これらの問題を克服するため，本研究ではテスティングフレームワークを利用し，二つのクラス：攻撃者に相当するテストクラスと被害者に相当する検知クラスを設けることを提案している．これらのクラスを実装し評価したところ，誤検知するケースがあるものの，SQL インジェクションを起こす多くのケースに有効であることを示している．

伊波 源太「バインディング機構の導入による XSS 脆弱性対策の実装と評価」(2008 年)
DOM(Document Object Model)は HTML 文書または XML 文書を表示するための標準のオブジェクト・モデルである. 本研究では, DOM ツリーの改変を引き起こすことで不正なスクリプトを実行する XSS 攻撃に着目している. 具体的に, SQL のバインド機構の考え方を応用し, XSS 脆弱性対策に有効に対処することのできるバインド機構を提案している. 提案方式の実装と評価を行った結果, 従来手法を用いずに XSS 脆弱性対策を行うことができ, 既存の対策手法による問題点も解決できることを示している.

龍 浩一「DNS 権威サーバを DNSSEC に対応させるネットワーク機器の提案」(2010 年度)
名前解決システム DNS に対するポイズニング攻撃対策として電子署名を活用する DNSSEC の導入が促進されているが, 導入・運用のコストが高いという欠点がある. 本研究では, この課題を解決するため, 署名のみを行うアプライアンスを提案する. このような装置を既設の DNS サーバと組み合わせることで, DNSSEC の導入・運用のコストを下げることができる. さらに, 提案したアプライアンスを実装し, DNS サーバと組み合わせて機能検証を行った. その結果, 提案が実現可能であることが確認された.

山口 聖大「脆弱性検査ツール統合システムの提案」(2011 年度)
情報システムのセキュリティを確保するために, 脆弱性検査 (ペネトレーションテスト)を実施することが不可欠となっている. しかし, 検査を担当する組織内技術者は関係するツールについての膨大な知識を要求される. この課題を解決するために, 本研究では脆弱性検査ツールの統合について着目している. 検査を担当する技術者が検査ツールを統合したシステムを予備知識無しに, かつ簡易に操作可能にするためのツールの集約方法を検討しプロトコルを試作してその有効を検証した.

亀谷 直希「情報システムの脆弱性に対する客観的評価手法の提案」(2013 年度)
情報システムの利用環境に応じた脆弱性に対する影響を評価するシステムとして CVSS (共通脆弱性評価システム)の環境基準があるが, 脆弱性評価値の算出に主観的評価が含まれるため, 評価する人によって結果が異なる, という問題がある. そこで, 情報システムの脆弱性を客観的に評価する手法として, ペネトレーションテストにより攻撃成功時間を測定し, CVSS の基本値とこの攻撃成功時間から, 情報システム環境の脆弱性の実測値を算出する手法を提案している.

(2)マルウェア
ワーム等のマルウェアの検出に関するものが 5 件, 静的・動的解析や分類手法が 4 件あった. また, ワンクリック詐欺の検出が 1 件あった.

頼永 忍「ファイルアクセスログを用いたワームの検出」(2006 年度)
本研究では, ワーム検出法として適用されている振る舞い検出法にファイルアクセスログ情報を活用することにより検知率を高めることを提案している. 従来法は振る舞い検出法では主に振る舞い(What)情報にのみ着目していたが, アクセスログから抽出できる時間

(When), 場所あるいは対象(Where), 方法(How)の各種情報を加味して検知するという特徴を有する. 実験により, 提案法は特にマスメーリング型のワーム検出に一定の効果があることを示した.

髙木 祐輔「Wilcoxon 符号順位検定による性能特性比較での異常検知」(2007 年度)

マルウェアの亜種の出現数の増加と抗検知技術により従来のシグネチャマッチングのみの対策は限界となりつつある. そこで, 本研究ではシグネチャマッチングの補完的技術として, パーソナルコンピュータの異常な性能値を判定に利用する手法を提案している. パーソナルコンピュータの性能値は小規模かつ固定の使用用途であれば類似した傾向を示すと仮定し, その理想的な環境下で二端末間の情報を比較することにより異常な性能差を検知するシステムを構築し機能検証した. また, この検知には, 対応する一対の標本の性能差の検定法である Wilcoxon 符号順位検定を用いている.

柿本 圭介「自己組織化マップを用いた Windows システムサービスコールの分類によるマルウェア検出手法」(2007 年度)

自己組織化マップは, 多次元のデータの統計的性質を学習し, 類似した性質を持ったもの同士を 2 次元平面上へ写像する手法である. 本研究では, 未知のマルウェアを検出することを目的とした動的解析による検出手法としてこの自己組織化マップを適用し, マルウェア実行時に呼び出される Windows Native API 順序情報, および入出力パラメータに設定される文字列を特徴量として機械学習する方式を提案している. 10 種類の API コール, 100 の API コールログデータを用いて, 実証実験を行ったところ, 比較的良好な検出精度が得られることを示している.

浅田 武「ネットワークアクセス制御ログ活用によるワーム蔓延防止策の一考察」(2008 年度)

本研究では, LAN 環境におけるクライアント間の通信からワームの蔓延を検出する手法を検討している. 本提案実現のために必要な機能は, スイッチの通信制御, 共有デバイスへの折り返し通信制御, クライアント間通信のモニタリング, ログの定量出力機能, 汎用アプリケーションによるパケット再送間隔の異常(セキュリティ違反)検出機能である. これらの機能を搭載した検証システムで実証実験を行った. この結果, 1秒間に 2 件以上のセキュリティ違反ログの出力が検出された場合は, ワームによるスキャンパケットが増大している可能性が大きく, ワームの蔓延を検出可能であることが分かった.

山口 和晃「マルウェア動的解析の効率化手法についての検討」(2009 年度)

最近は仮想マシンで実行されているか否か, ネットワーク接続の有無, 日時などの動作環境要因から処理を分岐することで, 振る舞いを変化させる耐解析機能を備えたマルウェアが増えている. このことから, マルウェア自動的解析の精度の低下や解析効率の低下が起きている. 本研究では, マルウェア自動的解析の効率向上に向けて, 実行環境や実行方法の組み合わせを変えて解析を比較検討した. 結果, 実マシンでの解析の重要性を再確認した. また, 複数の実行環境と実行方法によるマルウェアの挙動の変化を検証した.

四本木 正男「P2P ファイル交換ネットワーク環境におけるマルウェアの検出手法の提案」(2009 年度)

P2P ファイル交換ネットワークで流通している実行ファイル形式のマルウェアは，同ネットワークで流通している他のコンテンツに偽装もしくは混入されていることが多い．一方，正常な実行ファイルは，通常，他のコンテンツに偽装もしくは混入されて流通することは少ない．本研究では，この違いを利用し P2P ファイル交換ネットワーク上で流通している実行ファイルがマルウェアか否かを自動判別する検出手法を提案している．提案手法を実装した結果，検出率 90%以上と良好な結果が得られた．

畑上 英毅「マルウェア動的解析に於ける自動分類手法の研究」(2010 年度)

本研究では，動的解析によるマルウェアの自動分類手法を提案している．具体的に，マルウェアを実行して得られるプロセスの起動情報，レジストリの改ざん情報，通信パケットの内容などといった動的な挙動から得られる情報の他，マルウェアの静的な情報を扱うことで，検知率の向上を試みている．マルウェアから得られる静的な情報を追加することで，従来の自動分類手法に比べ概ね 5 ポイント程の一致率の向上が確認された．また，従来法でマルウェアを検出できない場合でも，蓄積した既存のマルウェアの挙動と類似したマルウェアを抽出することで，約 75%以上の精度でその科名を自動的に提示可能となった．

松藤 達彦「静的解析の強化によるマルウェア自動分類システムの改善」(2011 年度)

本研究ではマルウェアの自動分類手法について，マルウェアを実行した際に得られるプロセスの起動情報，レジストリの改ざん情報，通信パケットの内容などといった挙動情報の他に，マルウェアに含まれる静的な情報をマルウェア解析のパラメータとして扱うことで，分類精度の向上を試みている．提案手法ではマルウェアをアンパックし，そこから得られる文字列を用いて自動分類することで．従来の手法に比べて，科名・亜種名共に 4．5%程度検知精度を向上することに成功した．

羽田 大樹「解析済みマルウェアとの差分抽出による静的解析の効率化手法の提案」(2012 年度)

マルウェアの挙動を正確に解析するためには，実行ファイルを逆アセンブルして実行コード列を読み解く静的解析が必要となる．これは熟練した技術者が時間をかけて行う必要があり，コストが高いという難点がある．本研究では，既に解析が完了した複数のマルウェアの情報を用いて，効率的に静的解析を行うアーキテクチャを提案している．具体的に，プログラムをグラフ構造で表現して 2 つのプログラムの差分を特定する．実際のマルウェア検体を用いてこの提案アーキテクチャを評価し，解析が完了した複数のマルウェアと対象とするマルウェアとの差分抽出が静的解析の効率化に有効となる事例を示している．

唐沢 勇輔「HTA ファイルの解析によるワンクリック詐欺の検出」(2013 年度)

パソコンのデスクトップ上に不正請求画面を表示するようなワンクリック詐欺手法では，HTA(HTML Application)形式のファイルが利用されている．本研究では，HTA 形式ファイルを用いたワンクリック詐欺を検出することを目的に3つの検出手法を提案している．サンプルを用いて評価した結果，3つの手法ともに悪性ファイルを 100%検出し，正規ファイ

ルの誤検出は 0 という良好な結果が得られた. 特に,「パソコンのデスクトップ上に不正請求画面を表示する」という感染行為自体のふるまいに着目して検出する手法は, 汎用性, 実装の難易度の点から優れていることが分かった.

(3)セキュア OS

SELinux 関連で 2 件の修士論文があった.

黒田 洋介「設定簡易化のための SELinux ポリシー記述言語の提案」(2009 年度特定課題研究)

セキュア OS はセキュリティ確保のために, 利用している既存のソフトウェアが利用できない, あるいは利用者に合わせた設定変更が複雑になる, という問題がある. 本研究では, セキュア OS のセキュリティレベルを落とすことなく設定を簡易化するためのポリシー記述言語を検討している. 具体的には, Apache を例にとり, デフォルトで設定されている SELinux ポリシーから, 類似性などをもとに統合を行うことでポリシーの削減が可能であることを示した.

滝澤 峰利「SELinux におけるアクセス制御方式の改良をユーザ空間で検証するツールの提案」(2013 年度)

本研究では, カーネルソースに含まれる SELinux のアクセス判定部分をユーザ空間に抽出し, 変更するツールを提案・開発している. ユーザ空間で SELinux の変更が可能になることにより, プログラムの変更後のシステムの再起動が不要になる, 既存のアプリケーション層のライブラリを利用できる, といった利点がある. 提案ツールを作成して評価した結果, カーネルソースを変更する場合に比べ容易に実現できることが分かった.

(4)アクセス制御

利用場所を考慮したアクセス制御, 分散システムにおけるアクセス制御, ソーシャルエンジニアリングの脅威に着目したアクセス制御, さらに, 暗号を用いたアクセス制御に関するものが各々1 件あった.

宗吉 隆行「ユーザとその居場所に応じたアクセス制御」(2005 年度)

企業などのイントラネットでアクセス制御を行う場合の主な方法として, ファイアウォール(FW)と各ユーザが持つアクセス権制御が挙げられる. FWは, 建物や部屋毎に設定されたセグメント間の通信を規定する. ユーザのアクセス権制御は情報サービス毎に設定される. 本研究では主に場所の要請で設定されているアクセス制御のポリシーにユーザのアクセス権を考慮したアクセス制御を加えることを提案している. 本提案によって, 場所に依存しないユーザ権限の行使, ユーザ権限に依存しない利用場所でのアクセス制御を実現することができる.

橋本 正樹「分散システムにおけるケイパビリティを用いた資源アクセス制御」(2006 年度)

ディペンダブルな分散システムの構築を目的に, システムソフトウェアによるアクセス権限

管理方式を提案している. その実装としてアクセス制御表を, Service をアクセス制御対象とした Capability によって記述する. ここで, Capability とは Service Object の Location と Access Mode を記述したデータ構造であり, システムの保護領域においてプロセス毎に関連付けられる. この Capability をローカルシステムに保持することにより, 分散システム内のあらゆる Object に対する認可問い合わせをローカルシステム内で完結できる.

矢竹 清一郎「Social Engineering の分析およびアクセス制御の提言」(2006 年度)

情報システムを利用する人間と情報システムとの間で, ソーシャルエンジニアリングを利用し情報を入手する脅威に着目し, ソーシャルエンジニアによる情報開示要求に対するシステム的対策を提案している. ユーザ・機密度・アクセスコントロール権限それぞれにおいてレベルをわけ, 定義したことにより従来のアクセスコントロールと比較し, より細かいアクセスコントロールが実現できる. さらに, 複数のポリシーを事前に用意することで業務効率も考慮したアクセスコントロールが可能となる.

谷内 崇浩「暗号を用いたファイルのアクセス制御についての研究」(2007 年度)

近年, 暗号技術を応用したアクセス制御製品が流通しているが, いずれも管理をサーバで行っており, ネットワークに依存する欠点がある. 本研究では, ネットワークに依存しないアクセス制御として, ユーザ保有の公開鍵をベースとするアクセス制御技術を提案し, 実装例を示している. 具体的には, ファイルの暗号化を共通鍵暗号で行い, 用いた共通鍵をユーザの公開鍵を用いた公開鍵暗号で暗号化することで, ファイルの本文, 及び暗号化された共通鍵は秘密鍵を持つ者にしか参照される恐れがなくセキュリティが確保される.

(5)個人認証

生体認証が 8 件, 画像選択型認証が 1 件あった. 生体認証の内訳は, 虹彩認証が 3 件, 網膜認証が 4 件と多く, 他に DNA 認証が 1 件であった.

齋藤 邦男「極座標センサーを用いた虹彩認証方式の実証実験」(2005 年度)

虹彩は, 何十年にもわたって変化がない, 非接触で利用者にとって煩わしくない, 高い認証精度を有する, といった特徴があり, 生体認証手段として優れているものの他の手段に比べて認証装置が高価であるという問題がある. この問題を解決するため, 本研究では, 虹彩認証に極座標センサーを利用することを提案している. 極座標センサーを搭載した試作装置を用いて虹彩画像を採取し, 判定閾値の設定やその重みづけ, 最適な認証パラメータの選択, などを変えて実験を行った. その結果, 試作装置が実用に耐えうる認証精度を有することを確認している.

溝口 正敏「測定楕円を導入した網膜認証方式」(2006 年度)

網膜認証は画像を用いる生体認証であり, 他の画像を用いる生体認証に比べ盗撮しにくいという特徴がある. 本研究では, 網膜認証として測定楕円を導入し, 眼底画像に写された静脈や動脈の血管パターンの交点を特徴点として個人識別を行う新たな方式を提案している. 実データによる実験を行い, 特徴点の類似度分布において画素の一致範囲を閾

値として与えて認証特性を調べた. 結果, 本人サンプルと他人サンプルを区別する場合については 82%の正答率を, 本人サンプル同士については 65%の正答率を得た.

村松 直紀「画像相関マッチングによる網膜認証方式」(2006 年度)

網膜画像に基づき個人認証を行なう方法として以下のようなステップを有するアルゴリズムを提案している. すなわち, 最初に, 撮影した網膜画像から視神経乳頭および黄斑部の位置を決定する. 次に, 視神経乳頭および黄斑部の位置に基づき網膜画像を正規化して, 正規化した画像データを作成する. 最後に, 正規化した画像データと基準画像データの相関を調べることにより個人認証を行なう. 提案アルゴリズムの精度は視神経乳頭の抽出精度に依存する. 検証実験を行い, 視神経乳頭を中心とした 192 ピクセルの G 成分画像が認証に適することを示している.

中嶋 崇泰「二点間の RGB 比較による網膜認証方式」(2006 年度)

本研究では, カラー画像を用いる二つの網膜認証方式を提案している. 一つめは, 血管データのパターン一致による網膜認証方式である. しかし, 本方式は血管の色情報を定義しパターン抽出をするのが難しいことが分かった. 二つめは, 二点間の RGB 比較による網膜認証方式である. これは, 血管にこだわらず直接 RGB 等の色情報を用いて認証を行うものである. 色情報に関する閾値を変化させ, 本提案法の実験を行った. 同一人物の網膜画像が少なく, 十分な精度検証ができなかったが, 網膜認証が可能であるという見通しが得られた.

斉藤 直 「DNA-SNP 個人識別方式の社会システムへの応用」(2006 年度)

DNA 情報による個人識別として, 従来法より分析時間が短縮かつ安価に実現できる SNP(Single Nucleotide Polymorphism)を用いた手法が提案されている. しかし, 社会システムへの応用はまだ本格的に行われていない. 本研究では, 電子パスポートへの DNA-SNP 識別の適用を中心に社会システムへの具体的実用化方法を検討している. また, SNP 識別による検証実験を行い, SNP データの識別精度評価を行った. その結果, 十分な識別精度が得られることを確認した.

石原 彰人「画像選択型認証方式における改善策」(2007 年度)

本研究では, 提示された画像から正しい画像を選択することによる認証を行う画像選択型認証方式を取り上げている. この画像選択型認証方式では推測攻撃が比較的容易に行える. 例えば, 正解と推測できる画像が少ない場合, 関連性のある画像が正解画像数とほぼ同じ枚数表示された場合等において推測攻撃が可能である. このような問題を解決するため, 関連性のある画像を囮として表示することで推測攻撃を難しくする改善策を提案し実験で効果を検証した.

堤 健泰「国際標準に準拠した網膜認証評価」(2008 年度)

国際標準評価測定方法 ISO/IEC 19795-1:2006 を参考に, 散瞳液の点眼が不要な眼底カメラを用いて網膜画像のデータベースを採取し, 2007 年に情報セキュリティ大学院大学で研究された画像相関法による網膜認証アルゴリズムの精度を評価した. すなわ

ち，網膜画像の特異点である視神経乳頭を自動抽出し，その付近の部分画像を切り出し，自動切り出しに成功した網膜画像について照合するよう試みている．180 人の網膜の特定の 1 ヶ所の部分画像の相関値を求める単純な方法により，他人からなりすまされることなく正しく確認（1:1 照合）が可能なことが確かめられた．

蘇 雷明「高精度虹彩認証の研究」（2008 年度）

本研究は虹彩による個人認証の精度向上を図っている．研究では，瞳孔の特定に「投票法」と「成長法」という二つの手法を考案してその実施手順を詳細に記述している．また，まつげがノイズとなるので，まつげの認識と除去について「除去円拒」という方法を考案した．本学で撮影したデータによる精度評価実験を行い，FAR（他人受入率）=10-6 の条件で FRR（本人拒否率）は 1．38%未満であった．また，この際の FER（登録失敗率）は約 0．02%であった．

小田島 広幸「虹彩認証アルゴリズムの精度向上に関する研究～画像品質・照合領域・特徴データ量の影響～」（2010 年度）

本研究では，虹彩認証の認証精度向上を目的に，新たに3つの照合アルゴリズムの改善を提案し，その効果を評価している．具体的には，画像品質については，ぼけた画像も照合できるように，意図的にぼかされた画像も照合データに加える．照合領域について，まつげによるノイズの影響を避けるため，比較的識別能力の高い領域を照合に使用する．虹彩の模様が少ないものやぼやけた画像を扱うために特徴データ量を増やす．提案を検証した結果，認証精度を 87．34%から 96．32%に上昇することができた．

（6）監視と検疫

検疫ネットワーク 2 件，侵入検知システム 1 件，ログ管理関連 2 件，情報漏洩検知 1 件，パケット監視 1 件，ホームセキュリティ監視 1 件，に関する研究調査が報告された．

田中 修「コンピュータウイルスに対する検疫ネットワークの考察」（2005 年度）

管理者が能動的にコンピュータウイルス対策を実施する手法である検疫ネットワークが注目されている．本研究では，コンピュータウイルスがネットワークにどのように拡散するか，また，検疫ネットワークの有効性について検証実験を実施した．近年猛威をふるった，CodeRed-I，Slammer，Nachi，Sasser を感染・発症させる環境を構築して検証した結果，Slammer，Nachi，Sasser について正しく検出でき，パケット通信を停止可能なことを確認した．なお，CodeRed-I は，感染先と TCP コネクションを確立することが必要であるが，検証環境にはこのコネクション接続機能がなく検証できなかった．

横山 恵一「イントラネットにおける IPv6 検疫ネットワークシステムの研究」（2005 年度）

本研究では，IPv4 による既存の検疫ネットワークシステムよりも，IPv6 でセキュアな検疫ネットワークシステムを実現することを提案している．提案方式の特徴は IPv6 の近隣探索プロトコル（NDP）の近隣要請やルータ広告の機能を検疫ネットワークシステムに応用することである．ABK（Address Based Keys）を実装し，MAC アドレスや IP アドレスを詐称できないようにすることでさらにセキュアなシステム構築を行う．また，具体的なシステム構成

法を与えるとともに具体的な実装手法を示している.

柏木 肇「侵入検知システムにおけるパケット・フラグメンテーションに対する脆弱性の検討」(2005 年度)

侵入検知システム IDS にはパケットの検出漏れが発生しやすいという弱点があり, 本研究ではこの弱点に着目している. 一般的に使用されている IDS 製品を対象に動作検証実験を行った. さらに, 実験結果を分析したうえで機器選択や導入時のポイント, 機器設定における注意点などをまとめている. 実験では, 検出漏れを調べるために, パケット・フラグメンテーション攻撃を疑似したトラヒック負荷をかけた. その結果, 検知率が低下してしまう場合があり, 改善が必要であることが分かった.

小野寺 栄吉 「モバイルエージェントによる新しいログ管理方式」(2005 年度)

本研究では, モバイルエージェント技術を適用して, 多様な OS およびサービスに対応したログ管理を, 簡易かつ高度に行うことのできるシステム構成を提案している. ログの管理におけるシステム管理者の負担を軽減し, かつサーバやサービスの種類・行いたい管理業務の変化などに柔軟に対応できるのが本提案の特徴である. 提案方式の構成要素の検討, 実験用システムの試作を通して, ログ管理を行う上での役割分担の明確化, モバイルエージェントによるシステム拡張の可能性や性能面での確認が行えた.

仙北谷 祐輔「ログに対する改ざん検知方法の提案」(2007 年度)

不正侵入者は不正侵入の発覚を防ぐためにログ情報を改ざんすることが多い. この問題に対して, 本研究は新たなログ情報改ざん検知方法を提案している. 本提案では, システムのバッファ内に保存するログと従来のログ情報を細かく分割し複製する. この複製したログ情報のハッシュ値を算出し, ログ情報の改ざん検知を行う. 本提案により, ログ情報が改ざんされたとしても迅速な検知が可能になる. また, ログ情報の出力先は従来と同じため, 従来の運用・管理方法を変更する必要がないという特徴を持つ.

傳法谷 悟史「自己情報報告方式による情報漏洩検知システムの構築」(2008 年度)

本研究は, 情報漏洩したファイルがアクセスされた際にその所在を管理元に報告(自己情報報告)することで漏洩を検知するシステムを提案している. 提案方式は, 境界セキュリティのようなファイルの流出入を監視する方式と異なり, 外部からのファイルアクセスをトリガに受動的に報告する. 具体的には, ファイルに ID を付与し, ファイル漏洩先ホストにおいて異常な ID を有するファイルを識別すると, 自己情報報告アプリケーションを用いて管理元に自動通報することを特徴としている.

小山 充芳「広帯域キャプチャ技術を用いた不正パケットの検出手法」(2008 年度)

ネットワークのトラヒック計測は通常フローベースのサンプリングで行われるが, フローベースのサンプリングではマルウェアのスキャンパケットなどショートフローを見過ごすことが多い. この問題を解決するため, 広帯域キャプチャ技術が注目されている. 本研究では, 広帯域キャプチャ技術を用いて, 不審なパケットの送信元を的確に把握することを目的に, 一つのパケットからなるフロー(One-packet Flow)の抽出方法を検討している. 実験によ

り，One-packet Flow の送受信 IP アドレス，送信先ポート番号，フロー数などの情報から不正パケットの発信元を特定可能なことを示した．

新谷 祐司「ホームネットワークにおける個人行動の機械学習に基づく異常検出の研究」（2008 年度特定課題研究）

本研究はホームセキュリティに関するもので，情報家電の操作行動の統計的特徴から異常検出することを提案している．具体的には，ITU-T によって勧告化されたホームネットワークアーキテクチャに基づく AV 家電系および白物家電・設備系家電のネットワークを想定し，機械学習法を用いて利用者の家電操作特性を学習し，異常発生を検出する．実際に，フィールド試験で得たデータに提案法を適用し，各種機械学習アルゴリズム（単純ベイズ分類器，ベイジアンネットワーク，決定木，サポートベクターマシン）による検出性能を比較した結果，決定木が有効であることが分かった．

（7）フォレンジック

インシデント検知へのフォレンジックの応用1件，ネットワークフォレンジックシステム１件，アンチフォレンジック1件であった．

越智 貴夫「インシデント検知へのデジタル・フォレンジック技術の応用」（2007 年度）

本研究は，インシデント対応の事前対処のバックアップと事後対処のデジタルフォレンジックを組み合わせることにより，取りこぼしと性能低下の課題を解決できる「ホットデジタルフォレンジック」というコンセプトを提案し，そのための要求条件を満たすシステムを検討している．「ホットデジタルフォレンジック」の監視範囲は，ホスト型 IDS よりも狭いが，ホスト型 IDS と併用することにより，セキュリティを強化，補完することができる．また，昨今，J・SOX 法により内部統制の強化が求められているが，従来のデジタルフォレンジックを強化する手法の一つとしても有効である．

金 東佑「第三者機関によるネットワークフォレンジックシステムの提案」（2009 年度）

デジタル・フォレンジックの証拠性として，正確な時刻，原本性証明，第三者への証明という三つの要素が求められる．従って，デジタル・フォレンジックシステムの機能として，ある時刻に確かにデータが存在し，かつ改ざんがされていないことを第三者へ証明できることが必要である．本研究では，特にネットワーク・フォレンジック技術に着目し，それに時刻認証技術を組み合わせることで，高い証拠生を持つ新たなネットワーク・フォレンジックシステムを提案している．

浦野 晃「アンチフォレンジックツール実行の痕跡検出方式に関する研究」（2013 年度）

証拠隠蔽やデータの改ざんなどを簡単に実行できるアンチフォレンジックツールが多数インターネット上に公開されている．デジタルフォレンジックにおいて，アンチフォレンジックツールがデータを操作したことを検出できなければ，重要な証拠を見落とし，間違った情報に基づく調査につながる．そこで，本研究では，アンチフォレンジック手法がデジタルフォレンジックの作業プロセスに与える影響を軽減させるための体制構築について考察した．また，分析作業に先だってアンチフォレンジックツール実行の痕跡検査を行うことで一定の

効果が期待できることを示した.

(8)サイドチャネル攻撃
漏洩電磁波による攻撃1件であった.

庄司 陽彦「漏洩電磁波の局所性を利用した電磁波解析に関する研究」(2009 年度)
本研究では, 暗号回路全体の変化量を均一化するサイドチャネル攻撃解析対策について, 漏洩電磁波の局所性を利用した解析手法を提案している. IC チップの内部情報に対して解析を行う観点から, FPGA のように内部の配線情報や演算回路のレイアウトを参照・変更できることが望ましいと考え, 解析プラットフォームとして, FPGA が搭載されている標準評価環境である SASEBO を用いる. この環境を用いて, FPGA 内部の配線情報や演算回路のレイアウトから得られる情報に対して, 漏洩電磁波の局所性を利用した解析が可能であることを示している.

(9)サイバー犯罪
ワンクリック詐欺 1 件, SPAM 電話 1 件, フィッシング 2 件であった.

名越 潤也「ワンクリック詐欺対策手法の提案」(2006 年度)
本研究では, ワンクリック詐欺の対策手法を二つ提案している. 一つは, スパムメールフィルタリングに使用されている機械学習(ベイズ理論)を利用したもので, Web ページ中の単語の出現確率によって詐欺ページを判別する手法を提案している. 二つめは, スクリプト解析に基づく判別手法である. これは, スクリプト中の特定の振る舞いを検出して判別する. 最終的に, 二つの手法を組み合わせた実験を行い, 詐欺ページで 99%, 非詐欺ページで 98%という高い精度で判別できることを示している.

松倉 俊介「SPIT 判別のためのチューリングテスト方式の研究」(2008 年度)
電話版 SPAM は SPIT(SPAM over IP Telephony)と呼ばれ. 新たなサイバー犯罪となることが懸念される. SPIT が発信から通話までをすべて自動(無人)で行われるものと仮定し, 質問応答による SPIT 判別を行うチューリングテストを提案している. SPIT 判別上望ましいと思われる質問構成法を考案し, 現状で利用可能な自動応答システムを用いて応答による自動編別特性を評価した. その結果, 本提案による質問構成法が SPIT の自動判別に有効であるという見通しを得た.

水野 浩三「利用者の入力情報に基づくホワイトリスト形式によるフィッシング対策手法の提案」(2008 年度)
現状のフィッシング対策はユーザへの注意喚起やツールを利用した対策が中心であり, 決め手になるような手法が確立されていない. この問題に対して, 本研究では, 個人情報と送信先の組み合わせをホワイトリストとして設定し, ホワイトリストを利用したフィッシング対策を提案している. ホワイトリストに定義されていない送信先に個人情報を送信しようとすると異常な通信として許可しない. 提案方式を実装し, 機密性, 可用性, 利便性, の諸点から評価・考察を行い, 有効性を検証している.

松ヶ谷 新吾「URL 情報分析に基づくフィッシング対策方式の検討」(2012 年度)
本研究では, 最初に, フィッシングの原因について動向を調査し, 従来に比べ, フィッシングサイトの URL が正常サイトの URL と判別しにくくなっていることを示した. また, 安価なレンタルサーバを利用するライトユーザの Web サイトがフィッシングに悪用されていることが分かった. そこで, サーバサイドの対策として, Web サイト運営者が自ら導入できるホワイトリストフィルタ方式を提案し, 実験と評価を行った. フィッシング URL と正規 URL の判別実験を行い, 提案の有効性を確認した.

(10)ネットワーク攻撃
ボット関連が 4 件, DoS 攻撃が 5 件と多かった. 他に, IP トレースバックが 1 件あった.

朝長 秀誠「Botnet の命令サーバドメインネームを用いた Bot 感染検出手法に関する研究」(2006 年度)
本研究では, ボットが DNS サーバに命令サーバの FQDN (Fully Qualified Domain Name)をクエリするという特徴を観測することでボットを検出する手法を提案している. 本研究では, ハニーポットで収集したマルウェアの事前解析から予め DNS サーバのブラックリストを作成しておく. 提案を実装して実験した結果, 複数のハニーポットでのマルウェア収集が効果的であることが分かった. 特に, 同じネットワークアドレスの範囲でハニーポットを 3 つ以上設置すると良好なボット検出率が得られることを示した.

窪田 豪史「リクエストの特徴検出によるアプリケーションレベル DDoS 攻撃の判別」(2006 年度)
現在発生している DDoS 攻撃はネットワークレベルの攻撃が多い. しかし, ネットワークレベルの攻撃に対する防御手法も充実しつつある. そこで, 本研究では, 攻撃の効果が見込め, 今後の増加が予想されるアプリケーションレベルの DDoS 攻撃に着目し, その検知手法を提案している. 具体的には, 攻撃ツールから発生するアプリケーションサービスのリクエストと一般ユーザがブラウザで Web ページの閲覧を行う場合に発生するリクエストの差異に基づいて検知する手法を提案している.

近藤 賢志「SVM を用いた C&C セッションの分類による Botnet の検出方法」(2006 年度)
ボットネットの特徴的な機能である遠隔制御セッション(C&C セッション)機能 に着目し, ネットワークレベルで C&C セッションを識別する事によってボットホストの検知を行う手法を提案している. セッション識別アルゴリズムに機械学習アルゴリズムであるサポートベクターマシン SVM を使用し, パケットサイズと到達間隔にもとづいたパケットヒストグラムによる特徴ベクトルデータを用いた場合, 未知の C&C セッションに対しても 95% という高い C&C セッション識別率が得られることを示した.

安齋 孝志「輻輳型 DoS 攻撃を対象にした優先制御・帯域制御の研究」(2006 年度)
大きなサイズのファイルをアップロードしてサーバを攻撃する輻輳型 DoS 攻撃を対象に,

TCP のフロー制御および再送・輻輳制御のメカニズムを用いて，攻撃を検知・防御する手法を提案している．提案法では，サーバ側から，上記制御を指示するプローブパケットを恣意的に送信者に送り，それに送信者が従うか否かで攻撃源かどうかを判定する．さらに，判定結果を用いて通信帯域を優先制御する．従来の DoS 対策では正常な利用者が犠牲になるという副作用があるが，本提案はこれを軽減できるという特徴を持つ．

阿部 義徳「挙動トラフィック分析によるボット検出手法の研究」(2007 年度)

ボットの検出方法として感染端末と C&C サーバ間のネットワークトラフィックの特徴を抽出し，正常な通信と比較することで，C&C セッションを検出することを提案している．具体的に，C&C セッションにおけるパケットサイズと応答時間，C&C セッションにおけるプロトコルの変化，を特徴量とした検出法を提案している．ボットで使用されている IRC セッションと通常の Web セッションを比較したところ，前者は応答時間が長く，送受信パケットサイズが大きく異なっており，C&C セッションの特徴量として利用可能なことを示した．

武藤 展敬「時間管理による SYN cookies の改良提案」(2008 年度)

代表的な DoS 攻撃である SYN Flood 攻撃への対策として SYN cookies が実用化されている．SYN cookies はキャッシュレスで相手が特定できるという利点があるが，逆に悪意で ACK パケットを送信されるとコネクションを確立してしまう危険性がある．本研究では，攻撃者がネットワーク上を流れる SYN-ACK パケットを観測し，サーバを攻撃する場合を想定し，上記問題に対する手段を提案した．具体的には，ACK パケットが多くなった場合 SYN cookies の振る舞いを変更し，SYN-ACK パケットの送信量を抑えることが有効であることを示した．

西川 康宏「私的セキュリティポリシを利用した NGN における DoS 対策の研究」
(2008 年度)

私的セキュリティポリシとして設定しているユーザ個々の DoS 対策をネットワーク側で実現することを提案している．ユーザが NGN を利用していることを例に，前述の私的セキュリティポリシを NGN のエッジルータに反映し，ネットワーク側で DoS パケットをフィルタリングすることによって，同ユーザのアクセス回線の正常性が維持できることを示した．その他，従来，直接の攻撃対象でないにもかかわらず DoS 攻撃の被害を蒙っていた他のユーザの帯域も確保できる利点があることを示している．

齊藤 純一郎「ネットワークにおける異常検出手法確立に向けた攻撃トラフィックの特徴抽出に関する考察」(2011 年度特定課題研究)

本研究では，トラフィックの異常性からネットワーク攻撃を検出する手法について研究している．具体的に，DARPA データを利用して，攻撃トラフィックの特徴抽出実験を行い，攻撃種別ごとの着目すべきパラメータを明らかにしている．一例として，DoS 攻撃や Probing においては，トラフィック量の他に SYN，FIN，RST，RST/ACK フラグによる異常検出が可能であり，脆弱性を突いた R2L(Remote to Local)攻撃では RST フラグに着目することで未知攻撃を含むネットワーク攻撃の検出が可能であることを示している．

仲間 政信「C&C サーバ振る舞い情報抽出システムの提案と分析手法の検討」(2012 年度)

近年のボットネットでは, C&C サーバの IP アドレスが短期間で変更されるため, 特定 IP アドレスをキーに C&C セッションを監視することが困難となっている. 本研究では, ボットクライアントが接続する C&C サーバの IP アドレスを特定・抽出し, 抽出した IP アドレスを用いて C&C サーバの振る舞い情報を自動的に抽出するシステムを提案している. 実際にボットネットクライアントを稼働させ, パケットキャプチャデータを分析し, C&C サーバと想定される IP アドレスの抽出に成功している.

佐々木 達典「DNS を用いた IP トレースバック情報連携方式の提案」(2012 年度)

外部ネットワークからサイバー攻撃を行う際, 攻撃者は送信元の IP アドレスを詐称することにより, 発信源の特定を困難とすることが多い. 本研究では, DNS を用いて ISP などのネットワーク組織間で情報連携を行い, IP トレースバックする手法を提案している. インターネットを模した環境を構築して提案方式の有効性を検証している. その結果, 提案方式の機能が検証された. また, 追跡所要時間や情報保有可能時間等の性能の面からも充分現実的な利用が見込めることを示している.

(11)セキュリティ評価モデル

セキュリティ対策選択のための意思決定モデルが 2 件報告された.

大村 博敏「企業のためのセキュリティ対策分析・評価手法に関する研究」(2005 年度)

一般に, セキュリティ対策の有効性は, セキュリティリスク発生確率あるいはセキュリティ対策費用といった諸量の実態値を絶対的な尺度で表し, 金額で評価することが行われている. しかし, 対象となる諸量の数が多く実態値を把握することが困難なため, 評価が実質的に行えないという状況が生じている. 本研究では, この課題に対し, セキュリティ対策を対比較し, 階層分析法(AHP)により相対評価することを提案している. 本提案により, コスト以外の価値を尺度として取り入れ, 体系的にセキュリティ対策を分析・評価することが可能になる.

鈴木 亜矢子 「セキュリティ攻撃・防御戦略のリアルタイム意思決定モデルの提案」(2010 年度)

本研究では, 外部からのセキュリティ攻撃を想定し, 攻撃の進行過程において, 攻撃者利得や防御者損失を動的に評価し, 攻撃策と防御策をリアルタイムに逐次決定するプロセスをモデル化している. このモデルを用いて, 効果的に攻撃および防御を行うための方法をゲーム理論の思考に基づいて評価・選択する. すなわち, 同モデルにおいては, 攻撃者は得られる利益の最大化を, 防御者は自身の損失の最小化を図るようそれぞれ攻撃策および防御策を交互に選択する. 最後に, 同モデルを定式化し適用例を示している.

(12)Web

Web サーバ・システムの要塞化 3 件, Web アプリケーションのセキュリティ対策 2 件, Web ユーザ認証 3 件, DB アクセス制御 2 件であった.

菱川 尚「Web サーバの実用的な要塞化」(2005 年度)

本研究では Web サーバのセキュリティ対策方針として, 構築時にコストをあまりかけず, セキュリティ事故が発生した場合に長時間(コスト)をかけて対策する, 逆に, 構築時にコストをかけてセキュリティを高めておき事故時には短時間で対応する, という二つの対称的なアプローチを比較検討した. 具体的に, SELinux の有無, IDS の有無, パーソナルファイアウォールの有無, Web アプリケーションファイアウォールの有無, の組み合わせについて, 両ポリシーを反映したシステム(Alternative Set)を比較した. 結果, 事後のフォレンジックへの対応を考えた場合, 前者の方が高コストになることを確認した.

吉濱 佐知子「Web アプリケーションにおける言語ベースの動的情報フロー制御」(2006 年度)

情報フロー制御とは複数の主体間の情報の流れにおいて機密性や完全性への要求を満たすよう制御することを指す. 本研究では, 情報フロー制御について, 動的なアプローチを採用することにより, 既存のソフトウェア資産に手を加えることなく制御を行う方式を提案している. 具体的には, Inline Reference Monitor(IRM)と呼ばれるセキュリティポリシーを反映した制御コードを Web アプリケーションプログラムに挿入し, 実行時に動的に情報フローの追跡と制御を行う. 本提案は, バイトコード書き換え手法を使用するため, ソフトウェアの改造が不要であり, 実行環境に依存しないという利点がある.

小野 雅章「細粒度 DB フィルタリングルール生成システム」(2006 年度)

近年, データベース(DB)と連携する Web アプリケーションが増えており, SQL インジェクションによる不正アクセスによる被害件数も増えている. そこで, 本研究では, DB からの情報漏洩を阻止するためのフィルタリングルールの生成システムを提案している. 同システムは, 特定の RDBMS に依存しないため, 広範囲の DB アプリケーションに適用可能である. また, 任意のカラムを組み合わせて検索する際のアクセス権を細かい粒度で設定できる. さらに, 実装したルール生成システムはブラックリスト・ホワイトリストの両タイプのフィルタリングシステムに広く応用できることを示した.

村田 薫「携帯電話用 Web ブラウザの安全性向上に関する提案」(2007 年度)

携帯電話用 Web ブラウザに入力されたパスワード等の情報がキャッシュされ, ログアウト後でも端末を入手した第三者が使用可能になる危険性がある. 本研究では, この対策として, 携帯端末と携帯電話向けサイトが連携する方式を提案している. 具体的には, 携帯電話向けサイト側では携帯電話の機種判別情報を登録しておき, ユーザがログアウトを選択した際に, キャッシュに残されたパスワード情報等を同機種判別情報で上書きすることで, キャッシュ削減機能と同等の機能を実現する. 本提案は, 現状実施されているサイト側の負荷を軽減しつつセキュリティを高められるという特徴を有する.

松岡 浩平「利用者発信情報を扱う Web サービスにおける認証方式の研究」(2007 年度)

本研究では, Web サービスにおいて利用者発信情報を第三者と共有する場合の利用

者認証方式を検討している. 具体的に, OpenID を用いて, シングルサインオンを拡張したトークン発行方式を提案している. また, トークンが漏洩した場合でも不正利用を検出可能な方式を提案している. 提案方式は, 第三者の Web アプリケーション上に署名サービスを追加し, トークンに署名を付与することによって実現される. これらの成果は, Web サービスにおける安全な情報交換の基盤構築に寄与できると考えられる.

関 和行「マルチホップ web サービスにおける XML 暗号化の影響を考慮したスキーマ検証法の検討」(2008 年度)

本研究では, マルチホップの Web サービスにおいて, XML 暗号化の影響を考慮したスキーマ検証の手法を提案している. 提案方式では, 事前情報としての XML 暗号化に関する情報を用いてスキーマ変換することでスキーマの制約が緩んでしまうというパーティクル統合の問題をなくすことが可能である. このため, 中継者において元スキーマの制約を損なうことなくスキーマ検証をおこなうことができる. このように正しくスキーマ検証が行えることでエンド・エンドにわたるセキュアな Web サービスの実現が可能になる.

日吉 康仁「Web システム開発工程への XSS ワーム対策の組み込み」(2009 年度)

本研究では, XSS ワーム対策として Web システム開発工程への組み込みする対策を検討している. 個々の対策が Web システム開発に及ぼす影響を考慮して, 開発工程のどの部分に対策を組み込めばよいかを検討し整理した. 整理結果を利用することにより, 対策の検討漏れが発生し手戻りするリスクを少なくすることが可能であり, 従来に比べ効率的にセキュアな Web システムを構築できることを示した.

磯貝 雄治「一般消費者向け Web サービスにおける認証情報の盗難を前提としたなりすまし対策に関する考察」(2009 年度)

本研究では, 認証情報がすでに盗まれてしまった場合を仮定して, なりすましによる被害を食い止めるための対策に焦点をあてている. なりすましが発生した時の対処法として, 以下の三つのタイプを明らかにしている. すなわち, ①利用者自ら利用スタイルに応じた対処のタイプの選択できる環境を提供する, ②利用者自らサービス利用時間帯を制限する環境を提供する, ③認証情報の盗難をチェックする機構を備える, である. 提案によれば, 犯罪やサービス提供者からの情報流出の早期発見が期待できるとしている.

武藤 幸一「Web ユーザ情報に基づく DB アクセス制御手法の提案-既存 Web アプリケーションの脆弱性対策-」(2010 年度)

本研究では, 使用している言語や DBMS に依存せずに Web アプリケーションのアクセス制御を行う手法を検討している. 具体的に, SQL 文にセキュリティコンテキスト情報を含めることで環境依存を排除し, アクセスルール記述も既存 DB に存在する情報をもとにした階層型のロールベースアクセス制御定義を作成することを提案している. さらに, 提案を実装し, モデルケースで評価した結果, 導入に必要な時間やパーフォーマンスの影響の点において問題がないことが分かった.

木村 勇一「既存 Web アプリケーションの入力処理の脆弱性調査と対策」(2013 年度)

Web アプリケーションの入力処理の脆弱性に注目し，現在の開発手法に適用可能な対策方法を検討した．本研究では Java で検証用 Web アプリケーション を構築し，これを用いて脆弱性の原因調査を行った．さらに，入力処理の脆弱性の対策方法を複数実装し検証を行った．その結果，単一の方法では十分な対策が困難な Web アプリケーションについては，対策方法を組み合わせることが重要であることが分かった．

(13)電子メール

スパムメール 3 件，誤送信 2 件，送信者認証 1 件について修士論文が提出された．

小池 隆司「ユーザ・プロバイダ連携によるスパムメールフィルタリングの研究」(2006 年度)

電子メールのユーザとプロバイダが協力してスパムメールをフィルタリングする方法を検討した．具体的には，従来利用されているグレイリスティングとベイジアンフィルタリングを組み合わせた手法を提案している．提案手法は，スパムメールによるネットワーク輻輳を回避できる，管理コストを低減できる，という特徴を有するほか，スパムメール受信者からのフィードバック情報を用いてスパムメール判別を行うため，通信の秘密の遵守という要求に適合しつつ，フィルタリングを実施できる．

嶋 浩紀「情報工学的手法を用いたメールの情報漏洩防止の対策」(2009 年度)

本研究では，電子メールの誤送信により情報漏洩するインシデントの防止策を検討している．具体的には，迷惑メールのフィルタリングに利用されている POPFile の自動メール振り分けツールを送信メールに適用して，ベイズ理論によりフィルタリングを機械学習させる手法を基本検討した．実メールを使って実験を行ったところ，テストメールについて正答率 55．5%，誤検知 44．5%という結果となり，期待通りの結果とはならなかったが，今後の検討の足掛かりが得られた．

本田 致道「配送情報を利用した迷惑メールのフィルタリング」(2009 年度)

ネットワークベースの迷惑メールフィルタリングは送信メールサーバの情報を利用し，迷惑メールを受信する前に排除することができるが，迷惑メールと正常メールを混在して送信するメールサーバに対して有効ではない．そこで，本研究では Naive Bayes 分類器を用いてメールの配送情報を機械学習するネットワークベースフィルタを提案している．提案フィルタの適用実験を行った結果，従来のネットワークベースフィルタによる場合と比較して，フィルタを通過する迷惑メールのサイズ数を 73．4%削減できるという効果を得た．

堀田 知宏「実運用を考慮した電子メール誤送信対策」(2012 年度)

本研究では，近年の主要なメール誤送信対策ソフトウェアにて実装されている，特定の機密情報を含むメールを外部へ送信不可とする機能に着目し，機密情報となりうる用語を運用者に自動的に提示する手法を提案している．提案手法では，機密情報となりうる用語は，組織全体のみでなく，部署やプロジェクトといった単位でも提示するため，細かなグループごとの機密情報送信制限に対応可能である．本提案の妥当性を模擬メールにより検証している．その結果，運用負荷の軽減，機密情報の製品への登録失念等による誤送信

発生リスクの低減が可能という見通しを得ている.

渡邊 隆志「特徴抽出によるスパムメールフィルタリング性能の向上」(2013 年度)
スパムメールがメーラのコンテンツベースフィルタを潜り抜けることがある. 本研究では, このフィルタ通過スパムメールには, 件名と本文が類似している, 本文中に URL が含まれ, 本文の文字数が少ない, といった特徴が見られる そこで, これらの特徴量を機械学習して分類する手法を提案している. 文字の類似度には, 文字列ベースで, 比較的人間の感覚に近い類似度が得られるJaro-Winkler距離を用いた. 実験の結果, 特に, 件名と本文の類似度が判別に大きく貢献し, 提案手法がフィルタ通過スパムメールの低減に有効である他, 従来のフィルタリング機能を代替可能なことを示した.

増渕 篤「メール送信者認証における検証機能の改善に関する研究」(2013 年度)
本研究では, メール送信者認証技術を用いた場合, メーリングリスト等で中継サーバが件名や本文を修正するため, 受信側の検証が失敗してしまうという問題を検討した. 中継サーバが修正した情報を送信時の情報に戻した上で検証する3つの方式を検討した. 電子署名を利用するタイプの送信ドメイン認証 DKIM を対象に仮想環境上で検証実験を行った結果, 件名へのメーリングリスト名と通番の付与, および定型文を本文の先頭と末尾へ付与することで解決できることを示した.

(14)P2P ネットワーク
ユーザやノードの信頼度に関するものが 2 件, データ取得性制御に関するものが 1 件であった.

伊勢路 真吾「P2P ネットワークにおける信頼度を用いたコンテンツ流通システムの研究」(2006 年度)
本研究では, P2P ネットワークでのコンテンツ情報の安全性の確保を検討している. 具体的に, コンテンツの売買の売り手と買い手が相互の信頼度をもとにして相手を信頼するかどうかを決定する枠組みを提案している. 提案により, 信頼性の高いコンテンツ交換, 悪質な売り手や劣悪なコンテンツの自然淘汰, などが可能になる. また, P2P ネットワークのノード管理方式として分散ハッシュテーブル DHT(Distributed Hash Table)を活用するというのも提案の特徴である.

笹村 直樹「データ取得性制御可能な P2P ネットワークアーキテクチャの提案」(2006 年度)
P2P ネットワークが普及するとデジタルデータの無制御な流通を招き, 著作権やセキュリティに関わる問題が発生する可能性がある. そこで, 本研究では, (k, n)閾値秘密分散法を使った配布データの符号化と, P2P ネットワークの各ノードの動作を制御することで, データの取得性を制御可能な P2P ネットワークアーキテクチャを提案している. シミュレーションにより, 配布データの分散データの種類の数などにより効率の違いはあるものの, 提案により, P2P ネットワーク内のデータの取得性制御が可能であることを確認している.

秋本 諭史「自律分散型ネットワークにおけるノード信頼度管理に関する研究」（2008 年度）

P2P ネットワークのような自律分散型ネットワークにおいて，個々のノードの信頼度を電子証明書の一属性として保持し交換し合うことで，信頼度の相互検証を行う方法を提案している．提案によれば，各ノードに対して統一的な方法で付与された信頼度をお互いに検証が容易な形で提示しあうことができる．また証明書の交換という形で信頼度を提示することに伴って想定される攻撃とその対処についての検討を行い，提案が有効であるという見通しを得た．

（15）無線通信

無線を使った被害者への駆けつけ方式が 2 件，MAC フレームのアクセス制御が 1 件，電波伝搬特性に基づく秘密鍵共有が 1 件であった．

石井 和行「無線アドホックネットワークにおける発信者探索アルゴリズム」（2007 年度）

災害発生時を仮定し，アドホックネットワークで受信信号強度(RSSI) を基に自律的に被災者（発信者）に駆けつける方法をけんとう提案している．提案手法によれば，電波の RSSI と通信距離の関係から，端末が移動中に取得可能な RSSI とその移動距離， さらに移動方向ベクトルを基に，最寄り端末へ駆けつけることができる．自由空間伝播モデル，2 波モデル，偶発ノイズモデルのそれぞれのモデルについて計算機シミュレーションを行い，提案手法の有効性を示した．

高木 敏幸「無線 LAN における利己的端末を無害化する MAC プロトコルの提案」（2008 年度）

無線 LAN ではユーザの善意を前提にアクセス制御を行っているため，悪意のあるユーザがチャネル帯域を占有することも可能である．この研究はこのような無線 LAN の利己的な振る舞いを無害化する MAC プロトコルを提案している．無線 LAN では，個々の端末はアクセスポイントの受信確認応答 ACK によって通信タイミングを制御されるが，提案によれば，ACK の返信タイミングを制御し，データフレーム受信と ACK フレーム返信の間に他の端末からのデータフレームを割り込ませ，チャネルを強制的に割り振ることによってチャネル帯域を公平に分配している．

小出 雄太「災害時におけるアドホックネットワークを利用した被害者駆け付け方式の検討」（2010 年度）

本研究は，電波強度(RSSI)が通信距離と関係することを利用し，災害発生時の被災者を救済するために駆け付ける方式を検討対象にしている．駆けつけ者は被災者からの電波の RSSI を逐次測定し被災者の位置を推定しながら駆け付ける．特に，本研究では複数の駆け付け者が協調することで駆け付ける時間の短縮を図っている．また，駆け付け者が通行できない障害物を仮定し，複雑な電波環境においても被災者の救済が可能な方式を示している．計算機シミュレーションにより，駆けつけ端末数が増える程，到着率が向上し平均移動距離も短縮できることを確認している．

若尾 聡「電波伝搬特性に基づく秘密鍵共有方式に関する一考察」(2010 年度)

移動体無線通信において，暗号化の安全性の根拠を情報理論におく研究が進展している．本研究では，電波伝搬特性を利用して秘密鍵の生成と共有を行う無線暗号通信方式を対象に，生成される鍵の乱数性に関する評価を実施した．具体的に，IC タグからの電波を使用した実環境下において，FIPS140-2 の規定に基づいて評価した．その結果，同規定の乱数検定をパスするような秘密鍵を生成するには，マルチパスフェージングの変動周期を加味する必要があることを示した．

(16)モバイル

モバイルセキュリティの分析が 1 件，覗き見攻撃対策が 1 件，リモートデスクトップを用いたスマートフォンの活用が 1 件，Android アプリケーションセキュリティが 2 件あった．

永田 大「モバイル端末におけるセキュリティ上の問題点の分析」(2010 年度)

本研究は，モバイル端末におけるセキュリティ対策の調査を行い，問題点を分析している．調査の結果，各プラットフォームにおけるセキュリティ対策の方針が異なっていることが分かった．さらに，今後発生しうるセキュリティ上の問題点として，フィッシングや USB メモリを利用したウィルス等が，モバイル端末の特有の機能を利用して，新たな形で広まる可能性があることを指摘している．また，モバイル端末では，バックアップ方法と，小さな画面等ユーザインタフェースに対する検討が必要であることも示している．

内山 毅「携帯端末における覗き見攻撃への安全性を向上させる入力方法の提案」(2011 年度)

覗き見攻撃とは端末を操作している人の肩越しに操作内容や表示されている情報を覗き見て，情報を盗む行為を指す．本研究では，携帯端末における覗き見攻撃対策として「2 面同時入力方式」を提案し，その有効性や実用性を検討している．提案方法を実装した端末を用いて評価し，情報セキュリティ上一定の効果があることを示している．他方，従来の 1 面操作に比べて，操作が複雑になる，というトレードオフがあり，パスワードの長さや，端末の表面および裏面のボタンの数を検討する必要があることも分かった．

西村 隆宏「リモートデスクトップを用いたスマートフォンの活用と課題」(2012 年度)

スマートフォンを安全かつ便利に低コストで利用するためのスマートフォン活用モデルを提案している．また，提案モデルを実装し接続実験を行って評価を行っている．提案モデルでは，スマートフォン本体にデータが残らないため，一定のセキュリティ効果が見込まれる．また，無料のアプリケーションソフトを利用しており，さらにサーバ等の専用設備も不要である．これらのことから，低コストで簡易に構築できることを示している．

林 里香「Android アプリケーション利用の安全性を高めるアプリケーション動作の「見える化」」(2012 年度)

ユーザの意図しない動作をする Android アプリケーションが問題になっている．そこで，本研究ではアプリケーション動作の「見える化」について検討している．具体的には，標準の Android プラットフォームに対して，重要な動作が生じたことをリアルタイムにユーザに

通知する機能，および重要な動作の履歴をユーザに提示する機能の追加を提案している．プロトタイプを作成し評価した結果，「見える化」システムが実現可能であること，一定の条件下において目的が達成できることが分かった．

河村 辰也「Android アプリ開発におけるセキュアコーディング環境構築に関する研究」（2012 年度）

モバイル向け OS である Android において，マルウェアの脅威と同時に開発者の知識不足が原因として発生するアプリの脆弱性も多数報告されている．この対策として Android 向けのセキュアコーディングガイドラインが出ている．本研究では，同ガイドラインの内容を自動チェックできるプラグインを提案し，実装，検証を行っている．提案したプラグインは開発者が上記ガイドラインを参照しながら，危険なコードの有無を容易に確認できるという特徴を有する．

（17）ネットワーク制御

セキュリティレベルによるネットワークの利用制御 1 件，位置アドレスを用いた経路制御 1 件，オニオンルーティングの経路制御 1 件であった．

堀 琢磨「ユーザの安全性評価に基づいたネットワーク利用制御」（2008 年度）

情報セキュリティの観点からユーザのネットワーク利用環境を評価し，その結果に基づいてネットワークの利用を制御することを提案している．ユーザのネットワーク利用環境のセキュリティレベルを共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）のような客観的な基準で数値化する．その結果を用いて，ネットワークの利用帯域を差別化することで，インターネットのような公衆ネットワークのセキュリティを確保可能としている．

岡崎 成寿「位置アドレスを用いた経路制御の基本検討」（2009 年度）

インターネットプロトコルをベースにしたパケットネットワークは，IP アドレスが論理的なアドレス体系をとっていることからルータ負荷の増大や，不正アクセスが頻発するなどの問題が発生している．本研究では，中継系ネットワークのエッジルータ間に限定し，IP アドレスに代え，GPS などより取得した緯度・経度・高度の位置情報をパケットのアドレス（以下位置アドレスと呼ぶ）として用いるパケット転送網を提案している．このパケット転送網に求められる機能要件を基本検討し，位置情報による送信エリア構成法，送信エリアを多段階層化する手法を示した．

李 岩「オニオンルーティングにおける経路制御の研究」（2012 年度）

匿名通信サービスとして利用されているオニオンルーティングは経路がランダムに生成されるため，接続性が保証されず，転送性能が最適化されないという欠点がある．そこで，本研究では，エニーキャストと最短経路制御を適用して，接続性の改善，転送遅延の減少を図る方式を提案し，これら通信性能向上の効果を明らかにしている．また，トラヒック特性の異なる複数のケースを対象に，従来法と提案法の経路匿名性を考察した結果，経路匿名性においても提案法が従来法と同等もしくは優れるという見通しを得ている．

(18)要求分析と設計開発

要求分析に関するものが6件と多い. 他に, セキュリティ保証パッケージ, オープンソース導入ガイドライン, アスペクト指向プログラミング, プラットフォーム完全性検証システムに関するものがそれぞれ 1 件あった.

伊藤 慶則「ゴール指向分析を用いた要求分析法についての研究」(2006 年度)

ゴール指向分析とは, システム開発には何らかの目標(ゴール)があり, ゴールを明確にして, さらにそれを部分ゴールに分解する過程を繰り返すことによって, 要求を詳細かつ明確化しようとする要求分析手法である. 本研究では, ゴール指向分析の課題とその解決について考察し, 以下の結論を得ている. すなわち, ゴール指向分析は分析者の知識, 経験, 能力に依存している, 全体的な評価判断を行うには部分の評価が必要である, システム開発に関与するステークホルダー(顧客, 供給者, 利用者)の立場を相互理解する必要がある.

棚橋 和也「システムのセキュリティ評価における保証パッケージの提案」(2006 年度)

本研究では, セキュリティ保証要件を選択するための指標を挙げ, それに基づいた保証パッケージの提案を行っている. 具体的に, ISO/IEC15408 と ISO/IEC TR 19791 で規定されたセキュリティ保証要件の保証パッケージを提案し, ISO/IEC TR 19791 を用いた運用システムのセキュリティ評価を実施する際のセキュリティ保証要件の指針を示した. 本提案により, 十分な知識や時間のないシステム運用者もしくはシステム開発者でも, 機械的に短時間でシステム評価に必要なセキュリティ保証要件を選択できるようになる.

大木 安紀「情報システムへのオープンソースソフトウェア導入に関するガイドライン策定」(2007 年度)

本研究では, オープンソースアプリケーションソフトウェアの組織内情報システムへの導入について考察している. ユーザ企業がオープンソースソフトウェアに対する主な懸念(人材不足・互換性・サポート・実績)を考慮し, ソフトウェアサイクルの各プロセス(取得プロセス, 供給プロセス, 開発プロセス, 運用プロセス, 保守プロセス)における検討事項や導入判断ポイントを考察している. さらに, 検討結果をもとにした導入ガイドライン策定の考え方を示した.

沖津 直樹「衝突時におけるアスペクトの手続き呼出し順番定義に関する提案」(2008 年度)

ソフトウェアの特定の振る舞いをアスペクトとして分離し, モジュール化するプログラミング技術が検討されている. このアスペクトの手続き呼び出しには, 衝突が発生した時に備えて実行順番を定義しておく必要がある. これを行わないと処理結果が予期しないものとなる. この問題の解決に向け, 衝突の検知や手続きの順番などを定義・設定する 4 つのデータベースを用いることを提案している. 本提案には, 知識不足や入力ミスを原因とする手続き誤りがなくなる, 開発要員に十分な完全な知識が無くても手続きの定義が可能になる, 手続きの配置忘れや取り外し忘れを防止できる, という利点がある.

前富 博「拡張ミスユースケース図を利用した既存システムのセキュリティ更改要件抽出/分析手法」(2008 年度)

本研究では，拡張ミスユースケース図を利用した，既存システムのセキュリティ更改要件の抽出／分析手法を提案している．提案では，設計書やマニュアルなどのドキュメントをもとに進める従来の要件抽出作業に対して，セキュリティ対策状況を図表を用いて視覚的に検討する，という特徴がある．このため，提案手法を適用することで，セキュリティ対策の検討作業の効率化，正確性の向上を図ることが可能である．また，セキュリティ技術に疎いステークホルダーにも受け入れやすいという特徴がある．

中尾 雅幸「ソフトウェアベースのプラットフォーム完全性検証システム」(2009 年度)

情報システムが改ざんされていないことを保証するため，セキュリティチップの Trusted Platform Module(TPM)を用いることが多い．しかし，この TPM はエラーや破損時の対応が困難であるなどの可用性に課題を抱えている．そこで，本研究ではこれをソフトウェアベースで実現するため，USB メモリと外部の認証システムで代替する方式を提案している．提案により，TPM が搭載されていない環境でもソフトウェアベースでプラットフォームの完全性の検証を実現することが可能であることを明らかにした．

武川 宏「漸進的分析による Web 予約システムセキュリティ要求分析手法の提案」(2009 年度)

従来のセキュリティ要求分析手法は導入コストが高く普及していないことを解決するため，本研究では漸進的なセキュリティ要求分析手法を提案している．提案では，基準となる Web 予約システムのセキュリティ要求分析結果を元に，UML ベースの開発で頻繁に導入されるユースケース図を利用してセキュリティ要求分析作業を行えること，セキュリティ要求分析結果の雛形である Web セキュリティ要求パターンを利用できることから，セキュリティが専門でない一般的なソフトウェア開発者でも容易にセキュリティ要求分析が可能となる．

金子 朋子「アクタ関係表に基づくセキュリティ要求分析手法(SARM)の提案」(2009 年度)．

代表的なゴール指向要求工学手法である i*フレームワークの SD 図に変換可能で，i*の表記の複雑さを解消した表記方法として，アクタ関係行列が提唱されている．本研究では，これを拡張しアクタ関係表に基づくセキュリティ要求分析手法(SARM)を提案している．提案手法は攻撃と通常のシステム機能との間のセキュリティ上の関係を分析するための要求分析手法であり，開発現場における要求分析の利便性を向上させ，セキュアなシステム開発を実現するため，攻撃者をアクタに追加し，セキュリティ機能の国際標準であるコモンクライテリア(ISO/IEC15408)を利用して，セキュリティ機能を統一的に表記する．

宇野 健二「Web アプリケーション開発におけるシステム機能ベースセキュリティ要求分析」(2011 年度)

セキュリティ要求分析について，守るべき資産の価値と，それに対する脅威・脆弱性の評価プロセスを表すセキュリティパターンが提案されている．しかし，プロセスの実行や，セ

キュリティ要求を導出する際に，セキュリティに関する知識が必要とされるため，実際の開発現場ではほとんど採用されていない．本研究では，脆弱性や解決策などが明らかになっている Web アプリケーションを対象に，通常の機能要求分析に対応付けることで，セキュリティに関する知識のない開発者でも，容易に利用可能なシステム機能ベースのセキュリティパターンの提案を行っている．

清水 啓人「複数のセキュリティ要求分析手法を組み合わせる枠組みの検討」
（2012 年度）

セキュリティ要求分析は分析者や開発手法によって適した手法が異なり，すべての人に適した手法を提案するのは困難である．また，一つの手法だけでは得られる情報が不十分である．そこで，本研究では，セキュリティ要求分析のコンセプト，および，分析者に適した手法を利用してセキュリティ要求を獲得するための枠組みを検討している．ケーススタディの結果，複数の分析手法を組み合わせて分析することは可能であるが，共通データ構造への保存や分析されていないコンセプトに対応することが難しいということも分かった．

（19）クラウド

セキュリティ SaaS，および ID 管理負荷軽減方式に関する修士論文が 1 件ずつあった．

小宮 康裕「クラウドコンピューティングにおけるセキュリティ SaaS の基本検討」
（2009 年度）

本研究では，クラウドコンピューティング環境下のセキュリティ対策を全て SaaS として提供することにより，ユーザの金銭的負担や労力的負担を減らしつつ，安心・安全に IP ネットワークが利用できることを提言している．提言によれば，端末（ユーザ）毎のセキュリティレベルの均一化が図られ，端末のセキュリティ検査の負担が軽減される，といった効果が生まれる．一方，SaaS 化が要因となって生じる新たな情報漏洩リスクや SaaS の信頼性保証が課題となることも示している．

岩渕 琢磨「クラウドサービス利用企業における ID 管理負荷軽減方式の研究」
（2013 年度）

クラウドサービスを利用している企業の ID 管理者の運用負荷を軽減する方策として，クラウド上での ID 管理と連携する方式（IdP-IdP 連携方式）を提案している．提案によれば，ユーザプロビジョニングの対象を最小化することによって，ID 管理者の運用負荷を軽減できることが分かった．さらに，業界標準として検討が進められているプロビジョニング用 API 標準規格である SCIM と合わせた利用も可能であることを示した．

（20）重要インフラ及び制御システム

医療システム 2 件，電力システム 1 件，鉄道システム 1 件，行政システム 1 件，産業制御システム 1 件の研究・調査結果が報告された．

井出 美緒 「情報漏洩防止のための医療情報システムにおけるアクセス権の検討」
（2005 年度）

本研究では，医療機関内におけるアクセス権，とくに医療従事者による情報の参照に関するアクセス権についてアンケート調査をもとに検討している．医療従事者の中でもリハビリテーション分野に絞り，情報の参照に関するアンケート調査を実施した．アンケートの結果，必ず参照する情報，参照しない情報などアクセスの必然性から情報を分類した．さらに，この結果を踏まえ，医療情報システムの画面における情報表示の仕方を検討している．本研究によれば不要な個人情報の表示・拡散を最小限に抑えることが期待される．

澤田 忍「医療分野における RFID タグシステムの情報セキュリティの確保」(2008 年度)

本研究では，医療分野における RFID タグ利用について情報漏洩や改ざんなどの脅威の洗い出しをおこない，ミスユースケース図を用いてセキュリティ分析する方法を提案している．提案による分析結果例として，RFID タグや IC カードに格納された ID の盗聴，漏洩・改ざんの脅威を軽減できる一方で，トレーサビリティ情報など ID 情報を追跡する脅威については，電波を遮断する，ID を固定化しない，暗号化の対策をとる，などの対策が必要となることを示している．

伊藤 義治「次世代電力システムに対応する電力通信ネットワークセキュリティの考察」(2010 年度)

近年の環境問題などを背景に次世代電力システムが検討されている．本研究では同システムの検討の一環として，電力通信ネットワークの構築について考察している．次世代電力システムではより細やかな電力系統の制御を行うため，配電系統についてセキュアな電力通信ネットワークが必要になるものと仮定して検討した．具体的には，インターネットと電力通信ネットワークの融合を想定し，IPv6 の基本的な機能を用いたネットワーク構築方法を検討している．

佐々井 憲之「鉄道系制御システムのセキュリティ運用設計について」
(2010 年度特定課題研究)

本研究では，鉄道系制御システムについて，セキュリティの観点から運用設計法を考察している．最初に，同システムの運用状況に基づいてセキュリティ脅威を抽出することで問題点を洗い出している．さらに，この問題点を運用の改善によって対応する際のポイントを整理している．最後に，実際の鉄道系制御システムに改善策を当てはめることをイメージし，具体的な提案を行っている．

吉岡 達宏「組織間データ連携を実現する効率的なポリシー管理方式に関する検討」(2013 年度)

行政機関の情報システムを例に，重要インフラ機関の情報システムが他の機関の情報システムとデータ連携する際のポリシー管理およびセキュリティ維持問題を取り上げている．具体的に，ポリシー記述の標準言語を用いて実現できるポリシー管理方式を導出し，定性的な評価を行った．その結果，提案方式は最低限の要件を満足でき，組織間データ連携のための基準となることを示した．

水沼 暁「産業制御システムに対するサイバー攻撃の調査」(2013 年度特定課題研究)

近年，重要インフラ業界で扱われる制御システムを標的としたサイバー攻撃によるインシデントが増加している．しかし，日本におけるサイバー攻撃報告件数は少なく，国内の制御システムインシデント状況が不透明である．本研究では，制御システム向けのハニーポットである SCADA HoneyNet を用いて，制御システムを偽装し，インターネットに公開することで第三者からのアクセス状況を調査した．その結果， 80 番および 1433 番のポートに対するアクセスが多いことが判明した．

(21)各種情報システム

デバイスドライバ，IC カード，ICT チェーンのセキュリティに関するものが各々1 件あった．

藤澤 一樹「デバイスドライバのセキュリティ強化」(2007 年)

デバイスドライバに起因するセキュリティ上の問題点に着目し，セキュリティ脅威から保護する機構を提案している．具体的には，デバイスドライバに対するリファレンスモニタを導入し，強制アクセス制御とリファレンスモニタを連携してデバイスドライバに対する攻撃を防ぐ保護機構を導入する．提案手法を x86 アーキテクチャの Linux と Xen に適用し，大きなパーフォーマンスの低下を起こさず，ほとんど全ての脆弱性に対応可能であることを確認した．

白子 惣一「非接触型 IC カードなどにおけるセキュリティレベル調査研究」
(2009 年度特定課題研究)

IC カードや RFID タグといった非接触デバイスは今後さらなる需要拡大が予想されているが，一方で，セキュリティ課題も多く挙げられている．これらの課題を解決するための手段として暗号技術は必要不可欠であり非接触デバイスの根底を支えている．本研究はこのような視点から非接触デバイスに関する暗号技術の調査研究を行っている．非接触デバイスについて，暗号の 2010 年問題を始め，リソースの限られた中での暗号技術の搭載，プライバシーの確保，さらに情報の匿名化まで，課題が多岐にわたっていることが分かった．

長内 仁「ICT チェーンのセキュリティレベル向上を実現するセキュリティ情報連携アーキテクチャ」(2013 年度)

ICT チェーンを構成する企業間で情報セキュリティ基準を共有して評価可能にする情報セキュリティアーキテクチャを提案した．提案アーキテクチャでは，情報セキュリティ標準規格を適用することで企業間の指標値を統一する．提案アーキテクチャにより，IT 機器や脆弱性などのセキュリティ情報の共有や分析の自動化・継続モニタが容易になり，システム管理者の負荷を軽減することができる．さらに，自組織の情報セキュリティを守る従来の対策から，ICT チェーン全体の情報セキュリティ対策が可能になる．

(22)プライバシー

データマイニング，位置情報提供サービス，位置情報証明，行動ターゲティング広告，センサデータの活用，の各視点からプライバシー保護が論じられた．

大栢 良介「効率的なプライバシー保護データマイニングアルゴリズムの研究」（2007 年度）

秘密情報を含むデータが複数ノードに分散しているときに，これを自身以外のノードやデータを集約するサーバには開示せずに，集約したデータ集合から計算可能な有用な知識を自動発見するための技術をプライバシー保護データマイニングと呼ぶ．本研究では，プライバシー保護データマイニングにおける相関ルール検出について，出現頻度など集計時の結託への耐性に確率的尺度を導入する手法を提案している．提案手法では，ある程度の結託耐性を保ちながら同時発生するメッセージを一つにすることが可能である．

永廣 悠介「プライバシを考慮した地理位置情報サービスの提案」（2007 年度）

地理位置情報サービスにおいて，提供者自身が情報の提供先を選択し，かつ提供する情報の開示レベルを選択可能とするサービスモデルを提案した．提案モデルでは移動体の認証にグループ署名を使用することで移動体固有の ID を秘匿可能とし，プライバシーを考慮した位置情報の取り扱いが可能である．また，複数のサービス事業者が共通の情報収集システム基盤を利用し地理位置情報を収集することで，個々のサービス事業者がそれぞれ独立して収集するよりも幅広い地理位置情報を収集することが可能となることを示した．

西村 俊介「行動ターゲティング広告におけるプライバシー保護方式の提案」（2011 年度）

行動ターゲティング広告とは，Web サイトの検索や閲覧の履歴など，インターネット利用上の行動履歴を収集，分析し，消費者の関心事にあった広告を適切なタイミングで配信する広告手法である．本研究では，プライバシー問題を解決しながら，現状の行動ターゲティング広告を維持する仕組みについて検討している．具体的に，プライバシーの保護を実現するために必要な要件と，実現に向けて取り組むべき課題の抽出を行った．

山口 正「スマートフォンの位置証明方式に関する提案」（2012 年度）

スマートフォンの位置情報サービスが様々提供されているが，スマートフォンの GPS 測位を行う部分と測位結果を位置情報サーバへ転送する部分が分離しており，この分離を利用した位置情報詐称が容易である．このような詐称・改ざんを検出・防止する方法が提案されているが，未だ有効な方式として確立していない．そこで，本研究では，GPS 機能と位置情報サーバが通信しながら測位情報を第三者の位置証明サービスに登録する方式を提案している．従来方式に比べ，提案方式は位置情報を生成／改ざんすることが困難であることを示した．

麻生 享路「センサデータを活用する社会に向けたプライバシーに係る課題の多角的考察」（2012 年度特定課題研究）

センサデータの活用に注目が集まっているが，センシングにより個人の行動や趣味などの情報が露呈する，いわゆるプライバシーに係る懸念があり，この懸念を払拭する必要がある．本研究ではプライバシーデータとセンサデータの関わりについて整理し，センサデータに係るプライバシーの懸念を明確にしている．具体的に，センサデータが他の情報と

容易に突合できるか否かを現す量である個人特定量を提案し，センサデータの特徴により，個人の特定され易さが異なることを述べている．また，プライバシーが露呈する過程を，例を挙げて考察し，それが容易でない点も指摘している．

4 おわりに

本論文では，2013 年度までに提出された情報セキュリティ大学院大学の修士論文および特定課題研究報告のなかから，情報通信システムのセキュリティを研究対象としたものを 115 件抽出し，その動向をサーベイしたものである．2 節にも示したように，研究テーマの動向をまとめると以下のようになる．すなわち，修士論文等の研究テーマは概ね 22 の分野に分けることができ，研究対象として最もよく選択されているのは，マルウェア，ネットワーク攻撃，Web，および要求分析と設計開発，の 4 分野である．これらの 4 分野は年度によらず継続的にとりあげられていることが分かった．

上記 4 分野は，ホストコンピュータおよびインターネットを二大要素とするコンピュータネットワーク時代の研究テーマであり，急速な進展が予想される IoT 時代においても，魅力的であり続けるかどうかは疑問である．現在，マイナーと見受けられる分野が今後注目を浴びる可能性も大いにある．しかし，対象が変わったとしても，マルウェア，ネットワーク攻撃，Web，および要求分析と設計開発，の検討の重要性が低くなることはないであろう．このような視点にたつとき，上記 4 分野に限らず修士論文等は研究のヒントが効率的に得られる貴重な情報源といえる．

修士論文等の要旨は在席していた研究室のホームページに掲載されているが，各分野の研究動向を横断的にとらえようとするとかなりの労力を要するし，教員が退任して研究室がなくなると，修士論文等の情報自体も喪失してしまうことが多い．このようなことから，本論文のような要旨集はこれから修士論文等の作成にとりかかろうとする学生諸君にも役立つと期待している．