公益財団法人　セコム科学技術振興財団
研究成果報告書

研究課題名

情報法学・マネジメント論と侵入防止技術の融合による超セキュア情報システム

Ultra-Secure Information Systems by Integrating Information Laws, Management Methodologies and Invasion Prevention Technologies

研究期間

平成 25 年　4 月　～　平成 29 年　3 月

報告年月

平成 29 年　6 月

研究代表者
東京大学　情報理工学系研究科　電子情報学専攻　教授
坂井　修一

Professor
Department of Information and Communication Engineering,
Graduate School of Information Science and Technology,
The University of Tokyo
Shuichi Sakai

概　要

社会インフラとしての情報システムが定着・高度化するにつれ，情報セキュリティの確保が喫緊の課題となっている．近年では，ゼロデー攻撃や標的型攻撃による重要情報の流出や乗っ取り，個人情報流出とプライバシーの侵害が特に問題となっている．本研究は，これらの問題に対して，文理それぞれの分野で革新的な技術・政策・マネジメントシステムを提案・検証するとともに，文理融合によって総合的に解決していく手法を研究開発することを目的として進められた．

ここで対象とする分野は，情報法学，マネジメントシステム，情報システム工学とした．

準備段階では，それぞれの分野において調査を行って最重要課題を具体的に分析するとともに，政策・技術等の要件を整理し，基礎となるアイディアを文理両面に渡って提案・予備評価し，解決にあたっての道筋を示した．また，文理融合について検討し，サイバー攻撃防止と個人情報保護のそれぞれに事例研究を行って，本研究全体の成果見通しを立てた．

情報法については，個人の尊重という普遍的な価値を基礎に，第三者委員会（個人情報保護委員会）を中心として，ＥＵ及び米国等とのプライバシー・個人データ保護のルールの国際的調和を図り，各国間での執行協力体制を構築するところを目指した日本の個人情報保護法制のあり方を検討しながら改正の方向性を提案した．

一方，日本は，少子高齢・人口減少社会を背景に，社会保障制度の維持が構造的に困難になってきており，本人負担が日々増していく中，各人の生存権が脅かされつつある．

社会保障制度の維持のためにも経済成長を通じた税収の増加，財源の確保は大きな課題であり，その一つとして期待されるいわゆるビッグデータビジネスの振興を図るには，情報技術（IT）等の研究開発を通じた技術革新が求められている．すなわち，学問の自由，研究活動の自由を担保し支援し，それを産業に生かせる法制度の整備，国内はもとより国境を越えた情報の流通を担保する法制度の整備が前提となっている．これらの要請もまた個人情報保護法改正案に反映され実現されなければならない．そうした前提のもと，本研究では，新しい法制度について検討し，具体的な方法論と法律の基盤を示した．

マネジメントシステムについては，2000 年前後より急速に整備の進む ISMS 規格を中心に情報セキュリティ関連の国際標準を主な情報源としつつ，他方では国内の企業実態調査を行い，情報セキュリティの基本要件・課題・方策を整理した．また，エンタープライズアーキテクチャにおけるセキュリティの扱いについて TOGAF などの国際標準を参照し，組織の業務と IT を総合的に描写するエンタープライズアーキテクチャの情報セキュリティに対する応用の方策を検討した．そして，リスク分析手法の整備と情報セキュリティマネジメントにおける経営陣の役割の強化が課題解決の基盤になると判断し，数理的なリスク分析手法の開発と具体的なガバナンスプロセスの策定を行った．議論の妥当性を検証するために，既存の情報セキュリティ標準や類似研究，日米両政府における行政機関の情報セキュリティマネジメント体系，インシデント事例等を参照し，我々の着眼が普遍性を持つものであることを確認した．以上を総合して，情報セキュリティガバナンスの体系を新たに提案した．我々の成果は従来の取り組みにおける空隙を埋めるものであり，業務にとっての情報セキュリティの意義を明らかにし，かつ，技術の弱点を補う情報セキュリティマネジメント手法の強化に資する．なお，米国オバマ政権のサイバーセキュリティ指令に代表される最新のセキュリティ対策の情勢についても参照したが，サイバーセキュリティ指令などは主たる目的が重要インフラ保護であり，内容もそのための情報共有網整備に焦点を当てる

ものであった．行政機関の情報セキュリティマネジメントは，本研究で取り上げた FISMA（Federal Information Security Modernization Act）に基づく取り組みとして推進されている．

セキュリティ技術（特にここでは侵入防止技術）では，過去から直近までの侵入事例・情報漏洩事例について分析を行い，またコンピュータの異常状態の観測データ収拾を行った．これらをもとに，侵入検知システム・情報漏洩防止プラットフォームの原理を確立するとともに，万が一侵入された場合の検知法と対策について具体的に検討した．すなわち，データ流出・改竄を包括的に防止するために以下の三つのルートに着目し，研究を行った．

一つ目はシステムの管理者とデータの権利者が異なる場合についてのセキュリティ確保である．クラウド業者によるクライアント情報の盗聴改竄や，ユーザシステムによる DRM コンテンツの不正複製などが該当例として挙げられる．本研究ではこのような課題を解決するためのセキュアプロセッサ技術に着目し，特に近年の VM 技術をベースとした VM セキュアプロセッサ「Sharkcage」の機能・構造を開発した．コンピュータシステムの中核となるプロセッサを信頼の基点とすることで，正当な権利者の意志がきちんと処理に反映されることを保証することができる．プラットフォームの正当性認証や外部データの機密性・完全性保証を適切な暗号技術により実現し，かつ暗号処理のオーバヘッドをアーキテクチャ技術により軽減して実用的な処理速度と安全性を両立する．

二つ目は管理者やプログラマの不注意につけ込んだ侵入である．脆弱性によるウィルス感染やデータ改竄，フィッシングサイトによるデータ盗みだしやトロイの木馬によるシステムのっとり，ランサムウェアなど，この攻防は激しさを増し続けている．基本的な対策技術は攻撃信号のビットパターンや振る舞いのパターンを覚えてデータベース化し，水際で検疫することであったが，ゼロデー攻撃や標的型攻撃など，特に危険度の高い意図を持った攻撃には対処しきれない現状がある．本研究では，「情報フロー追跡技術」を発展させ，コンピュータが行おうとしている操作が，正当な権利者が意図したものかをコンピュータ自身が常に検査し，攻撃を検知するシステムを実現した．

三つ目はユーザの使い方につけ込んだソーシャルハックである．不用意にメモ書きされていたり，IoT センサ等で入力値を推測できてしまったりするパスワードや，正当なサービスのふりをした悪質な無線ルータなど，システム技術上は正しくセキュリティ対策がなされていても，物理世界・仮想世界の界面からユーザの使い方につけ込んだ攻撃によって侵入を許すケースが増えてきている．この攻撃は情報プラットフォームの小型化無線化とともに普遍化，高度化が進むことが予想される．本研究では，この解決策の一つとしてユーザにとって直観的に IoT 機器やコンピュータシステムにログイン・接続できるインタラクション技術の開発を行った．ユーザの位置情報やジェスチャに基づき，無線ルータや IoT 機器・家電などにパスワードを打つこと無く安全に接続する．

分野融合については，ゼロデー攻撃，標的型攻撃，個人情報漏洩，著作権侵害のそれぞれについて，情報法学，マネジメント，セキュリティ技術がおのおの何をすればよいか，それぞれの最新の成果をもとに，新たな役割分担と連携について検討を行った．