

情報セキュリティ分析機能強化に係る基礎調査

- 調査報告書 -

2008年4月

IPA[®] 独立行政法人 情報処理推進機構
セキュリティセンター

目次

1. 本調査について.....	3
1.1. 背景	3
1.2. 目的	4
1.3. 特色	5
2. 調査実施方法.....	6
2.1. 国内調査	6
2.1.1. インタビュー（情報セキュリティ関係機関）.....	6
2.1.2. インタビュー（経済・金融・社会等分析機関）.....	6
2.1.3. インタビュー（情報セキュリティセキュリティ分析手法に係る有識者）..	6
2.1.4. Web 調査	6
2.1.5. 統計調査.....	6
2.2. 海外調査(米国)	8
2.2.1. インタビュー（情報セキュリティ分野）.....	8
2.2.2. インタビュー（経済・社会分析関連分野）.....	8
2.2.3. Web 調査	8
2.2.4. 統計調査.....	8
3. 国内外の情報セキュリティ分析関連組織・機関.....	9
3.1. 国内調査結果.....	9
3.1.1. 情報セキュリティ関連組織・機関	10
3.1.2. 経済・金融・社会等の分析組織・機関	19
3.1.3. 国内調査結果のまとめ	29
3.2. 海外調査結果(米国)	31
3.2.1. 情報セキュリティ関連組織・機関	31
3.2.2. 経済・金融・社会等の分野の組織・機関.....	49
3.2.3. まとめ	52
4. 情報セキュリティ事象および対策等の実施状況に関するデータ.....	54
4.1. IT 化の進展に関するデータ	54
4.1.1. 国内の調査レポート.....	54
4.1.2. 国内の調査レポートでの把握可能データ.....	56
4.1.3. 米国の調査レポート.....	61
4.1.4. 米国の調査レポートでの把握可能データ.....	62
4.2. 情報セキュリティ事象および対策等の実施状況に関するデータ	66
4.2.1. 国内の調査レポート.....	66
4.2.2. 国内の調査レポートでの把握可能データ.....	68
4.2.3. 米国の調査レポート.....	72

4.2.4.	米国の調査レポートでの把握可能データ.....	79
5.	情報セキュリティ分析手法.....	84
5.1.	有識者インタビュー調査.....	84
5.1.1.	調査概要.....	84
5.1.2.	調査結果.....	86
5.2.	統計データの入手方法.....	88
5.2.1.	政府の統計調査.....	88
5.2.2.	民間の統計調査.....	89
5.3.	情報セキュリティ分析手法のトレンド.....	91
5.3.1.	有識者における研究トレンド.....	91
5.3.2.	海外での研究トレンド.....	95
5.3.3.	分析手法の全体像.....	104
6.	まとめ.....	106
付録.	調査レポート/参照元一覧.....	108

1. 本調査について

1.1. 背景

2007年5月に取りまとめられた、産業構造審議会情報セキュリティ基本問題委員会報告書「グローバル情報セキュリティ戦略」において、「情報セキュリティ対策を、国内・外の経済社会システムの構造の多面的変化に迅速かつ適切に対応したものとしていくため、データ収集・分析等を実施するための組織「情報セキュリティ分析ラボラトリー(仮称)」の創設を、独立行政法人情報処理推進機構(以下「IPA」)等の国内関係機関に対して求める」とされた。

こうしたデータ収集・分析組織を求めるニーズが高まる一方で、情報セキュリティに関する分析が整備途上である現状に鑑みて、脅威情報およびセキュリティインシデントを軸とした集計、分析はこれまでも行われてきた。個別のリスク、脅威の分析基盤が整備された現在、経済・社会システムと情報セキュリティとの関連性を考慮した多角的視野からの分析が求められている。

こうした背景を踏まえて、情報セキュリティ分析機能強化に係る基礎調査(以下「本調査」)は2007年の7月から12月にかけて実施された。

1.2. 目的

本調査は、国内および米国の情報セキュリティ関係機関の有する知見や執務経験に基づく生の声と情報を得ることによる組織の面からの課題分析や、国内外での情報セキュリティあるいは周辺のIT関連統計の現状を整理することによるデータ基盤の整備状況調査、国内外の学術的な取り組みとしての研究テーマ動向調査、分析手法等のトレンド分析等を並行して進めることによって、IPA において分析機能や組織のあり方を検討する際の一助となるべく開始された。

本調査では、IPA における情報セキュリティ分析機能強化に向けたデータ収集・分析手法の整理、検討を主目的としているが、同時に、IPA として同手法を活用する際の基盤となる組織の機能、体系についても整理することも目指した。

こうした手法や機能、組織体系の整理にあたり、国内外の既存の情報セキュリティ関係機関が持つ各種の分析機能を整理することで、IPA の新たな活動領域の定義に資するものとするを旨とした。さらに、情報セキュリティを活動の主要領域としない分析機関についても、情報セキュリティの経済・社会学的分析の過程でどのように両者の連関性を見出していくかというプロセス構築において参考になるものと考え、調査対象に加えた。

これらの議論を基に国内外の情報セキュリティに関する統計基盤の現状を把握することで、分析活動の際にどのような統計を活用することができるのか、統計基盤の活用によってどのような経済・社会学的分析が可能と考えられるかを検討した。

1.3. 特色

Web からの情報収集に加え、特に組織・機能面を対象に、情報セキュリティ分野を中心として国内外の幅広い関係機関に対するインタビューを実施し、その成果を盛り込んだのが本調査の特色である。

また、分析機能についても、政府関係機関が現時点において採用している基礎調査的手法と、専門の学会で報告された、研究領域における最新の分析手法や検討テーマの両方を整理することで、今後情報セキュリティ分析と経済・社会システムとの接点が現在どのような段階にあり(As-Is)、今後どのような方向に向かっていく可能性があるのか(To-Be)について、本報告書の幅広い読者にイメージを描いてもらえることを企図している。

最後に、本調査で海外事例調査対象とした米国の現況について、同国における官民でのデータ分析面での密な連携や、政策目的での柔軟な調査項目設定といった特色は、日本での組織、機能検討の拡大と深化が進む過程において有用な参考情報となると考えられる。

2. 調査実施方法

2.1. 国内調査

2007年8月から10月にかけて、情報セキュリティあるいは社会・経済分析に関するインタビューを実施するとともに Web やインタビューで入手した情報、討議内容を盛り込んだものである(各組織の詳細は第3章参照)。

情報セキュリティ関係機関については5機関、経済・金融・社会等分析機関については1機関、分析手法に関する知見を持つ有識者として2氏を調査対象とした。

2.1.1. インタビュー (情報セキュリティ関係機関)

括弧内はインタビュー実施日(いずれも2007年)

- 日本銀行金融研究所情報技術研究センター (8月15日)
- 有限責任中間法人 JPCERT コーディネーションセンター
(8月22日)
- 財団法人金融情報システムセンター(FISC) (8月28日)
- 電力分野におけるIT障害に係る情報共有・分析機能
(8月23日)
- 警察庁サイバーフォースセンター (9月11日)

2.1.2. インタビュー (経済・金融・社会等分析機関)

- 財団法人日本エネルギー経済研究所 (8月24日)

2.1.3. インタビュー (情報セキュリティセキュリティ分析手法に係る有識者)

- 東京大学生産技術研究所 松浦幹太准教授 (9月27日)
- 東京大学大学院情報学環・学際情報学府 田中秀幸准教授
(10月3日)

2.1.4. Web 調査

今回の調査の取りまとめに当たっては、調査対象として国内外の Web 情報を幅広く収集し、調査結果をまとめる際に活用した(巻末参照)。

2.1.5. 統計調査

国内外の情報セキュリティ、あるいはITの経済・社会面に係る種々の統計資料

を参照し、特色を整理した(調査対象統計一覧は第4章参照)。

2.2. 海外調査(米国)

情報セキュリティ関係機関については 4 機関、経済・金融・社会等分析機関については 1 機関を調査対象とした。インタビューはいずれも 2007 年 10 月から 11 月の期間に実施した。

2.2.1. インタビュー (情報セキュリティ分野)

- Computer Security Online (10 月 5 日)
- Computer Security Institute(CSI) (11 月 21 日)
- インターネット犯罪苦情センター (Internet Crime Complaint Center)
(11 月 26 日)
- Computer Economics (10 月 15 日)

2.2.2. インタビュー (経済・社会分析関連分野)

- 社会保障庁(SSA)、保険計理長室 (Office of the Chief Actuary)
(10 月 12 日)

2.2.3. Web 調査

今回の調査の取りまとめに当たっては、Web 情報を幅広く調査対象として収集し、報告書の中に活用した(巻末参照)。

2.2.4. 統計調査

国内外の情報セキュリティあるいは IT の経済・社会面に係るさまざまな統計資料を参照し、特色を整理した(調査対象統計一覧は第 4 章参照)。

3. 国内外の情報セキュリティ分析関連組織・機関

国内外の情報セキュリティ分析関連組織・機関について、日本国内および米国における現状を調査し、調査から得られた結果を整理した。

3.1. 国内調査結果

調査対象とした組織・機関に対して、Web 調査、文献調査およびインタビュー調査を通じて、以下の項目について調査を実施した(米国調査もほぼ同様)。

- (1) 組織の概要
 - 組織の設立背景・活動目的、活動内容
 - 組織の運営形態、運営資金
 - 組織の構成(部門構成、人員配置、従業員数、雇用形態) 等
- (2) 情報収集の詳細
 - 情報収集における情報源
 - 情報収集における収集データ(データ種別、収集項目、収集量) 等
- (3) 情報分析の詳細
 - 情報分析の対象・テーマ
 - 情報分析の方法(活用ツール、モデル) 等
- (4) 情報提供の詳細
 - 情報提供の目的
 - 情報提供の方法(対象、内容、媒体) 等
- (5) 外部とのチャンネル
 - 国内外の関係組織・機関との協力体制 等
- (6) 現在の課題と今後の方向性
 - 現在の課題認識
 - 今後の計画・方向性 等

3.1.1. 情報セキュリティ関連組織・機関

(1) 日本銀行金融研究所 情報技術研究センター (CITECS)

(A) 組織の概要

ホームページ URL

<http://www.imes.boj.or.jp/citecs/>

設立背景、役割

情報技術研究センター (CITECS: サイテックス) は、金融業界が情報化社会において直面する新たな課題に適切に対処していくことをサポートするために、1.国際標準化の推進、2.金融業界内の情報共有体制の整備、3.新しい情報セキュリティ技術の研究開発という3つの役割を担うことを目的として、2005年4月1日付けで設立された。

組織の運営形態

日本銀行金融研究所内に設置された常設組織(日本銀行は、特別の法律(日本銀行法)により設立された「認可法人」)。

CITECS のメンバー

10名程度のメンバー(日本銀行職員)によって構成され、半数程度が情報セキュリティに関する研究に従事している。

(B) 情報収集の詳細

CITECS では、情報セキュリティに関する論文、公開された脆弱性情報や、インシデント情報に加え、関係組織との情報交換や有識者との意見交換を通じて情報収集を行っている。もっとも、こうした情報は玉石混交にもたらされることが多いため、そうした中から取捨選択して有益な情報を抽出することに配慮している。

(C) 情報提供の詳細

学術的な知見に基づいて情報セキュリティのあるべき姿を提示し啓発することを目的として、「ホームページでの情報発信」「セミナーの開催」「シンポジウムの開催」を中心に情報提供を行っており、情報の内容と提供対象者層に応じて提供手段を設定している。

(2) 有限責任中間法人 JPCERT コーディネーションセンター (JPCERT/CC)

(A) 組織の概要

ホームページ URL

<http://www.jpcert.or.jp/>

設立背景

日本国内のセキュリティに関する事件・事故の調査や対策支援、セキュリティ情報の収集・提供、セキュリティ関連技術の調査研究等を行うことを目的に、1996年に任意団体として発足し、2003年3月に中間法人格を取得した。

活動内容

インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、1.日本国内のサイトに関する報告の受付、2.対応の支援、3.発生状況の把握、4.手口の分析、5.再発防止のための対策の検討や助言等を、技術的な立場から行う組織である。

運営形態

常設組織であり、官民連携組織である。有限責任中間法人であるため民間主管組織となるが、その活動は政府の事業の代行的な側面を有している。

雇用形態、従業員数

従業者は40名程度であり、そのうち10名程度はアドバイザー(技術専門委員)である。アドバイザー(技術専門委員)は、学識経験者、ベンダ、インターネットサービスプロバイダ等の専門家である。

(B) 情報収集の詳細

情報源

「ホームページ経由で受ける報告」「協力企業から提供される情報」「公知情報から収集する情報」等がある。

協力企業から提供される情報には、JPCERT/CC のサービスに登録をしているベンダ企業との情報交換や、「日本 CSIRT 協議会」等の会議体における情報交換によって提供される情報も含まれる。

収集データ

定量データ・定性データを含む、多岐にわたるデータを収集している。収集したデータは膨大な量になるが、全ての情報に目を通し、マネージャクラスの担当者がデータの取捨選択をしており、一連の収集作業を 365 日体制で実施している。

(C) 情報分析の詳細

分析方法

収集したデータを分析する際には、「概要分析」と「詳細分析(スコアリング等)」といった形で、2段階の分析を行っている。

分析実施者ごとに分析結果が異なることがないように、統一的な分析方法として「KENGIN」という分析ツールを独自に開発して使用し、企業へのインシデントハンドリング支援等に活用している。

(D) 情報提供の詳細

提供内容

提供内容は、分析結果や研究成果、ノウハウ等である。

提供方法

情報提供における提供方法としては、「メールマガジンでの情報発信」「ホームページでの情報発信」「各種メディアでの情報発信」が中心である。

情報提供する際には、その情報を誰が閲覧するのかを想定し、情報に応じて提供内容や提供方法、表現方法等を工夫している。

(3) 財団法人金融情報システムセンター (FISC: The Center for Financial Industry Information Systems)

(A) 組織の概要

ホームページ URL

<https://www.fisc.or.jp/>

組織の設立背景、活動内容

重要な社会インフラである金融情報システムの安全性確保のための自主基準の策定や普及啓発活動を行うとともに、金融機関における情報システムの活用や安全性を巡る諸問題について調査・研究を行う組織である。

組織の運営形態

常設組織である。有会員企業からの出捐によって設立され、会員の年会費により運営されている。所管府省は金融庁となっている。

従業者の雇用形態、従業員数

職員のうち、プロパー社員は数名であり、他 30 名程度は会員企業等からの出向社員(出向期間は原則 2 年間)である。

出向職員のバックグラウンドは、金融機関、保険会社、証券会社、コンピュータメーカー、情報処理サービス企業等、多様である。

組織の部門構造

「調査部」「監査安全部」「総務部」の 3 つの業務分野別に部門を設けている。「調査部」は、金融情報システムの国内外の動向等を調査する部署であり、「監査安全部」は、安全対策基準等の自主基準策定等をする部署である。

(B) 情報収集の詳細

情報源

情報収集における情報源としては、「アンケート調査で収集する情報」「インタビュー調査で収集する情報」「公知情報から収集する情報」等があり、アンケート調査よりも詳細な内容を収集する場合には、インタビュー調査を活用している。

収集データ

情報収集時には、アンケート調査による定量データや、インタビュー調査による定性データ等、多岐にわたるデータを収集している。

定量データの例としては、(システム化動向の調査の一環として)情報システムへの投資額といったものがある。

(C) 情報分析の詳細

分析の方法

アンケート調査で収集したデータを分析する際には、調査項目ごとの単純集計やクロス集計を中心に行っている。

ただし、セミナーや講演会でデータを使用する場合には、単純集計やクロス集計に加えて、相関分析等の多変量解析も行っている。

(D) 情報提供の詳細

提供内容

情報提供は主に会員企業に向けて行われており、提供内容は調査・分析結果や研究成果、ノウハウ等である。

提供方法

提供方法としては、「刊行物(機関誌等)の提供」「情報交流(説明会等)の実施」が中心である。

また、その他の提供方法として、「メール配信サービスの提供」「ホームページでのコンテンツ提供」「訪問サービスの提供」「セミナーの開催」等がある。

(4) 電力分野におけるIT障害に係る情報共有・分析機能(電力 CEPTOAR)

(A) 機能の概要

機能の設立背景、活動内容

「電力におけるIT障害に係る情報共有・分析機能」については、「重要インフラの情報セキュリティ対策に係る行動計画」(2005年12月13日情報セキュリティ政策会議決定)における「情報共有体制の強化」への対応として、電力業界における既存の取り組みを活用し、一般電気事業者10社、電源開発(株)、日本原子力発電(株)、電力中央研究所、電気事業連合会を参画機関として、情報共有・分析体制を整備し、電気事業連合会情報通信部が事務局を務めている。

また、情報収集・情報共有については、電気事業連合会が担当しており、情報分析は電力中央研究所が担当している。

<参考>

電気事業連合会ホームページ URL

<http://www.fepec.or.jp/index.html>

機能の運営形態

情報セキュリティに関する議題については、電気事業連合会内の会議体において、CEPTOAR参画機関が会議等によるFace to Faceを含め、情報交換等の諸活動を行っている。

(B) 情報収集の詳細

情報源

情報の収集源としては、「参画機関に対するアンケートにより収集する情報」と「公知情報により収集する情報」が中心である。

収集データ

会議体における議論・共有のための情報として、セキュリティ対策情報や障害情報等IT障害の未然防止や拡大防止等に資すると判断した情報を収集し、共有している。

(C) 情報分析の詳細

分析の方法

参画組織数が多くないため、各社における対策状況等を意見交換する程度である。

(D) 情報提供の詳細

提供内容

IT障害の未然防止や拡大防止に資する情報、その他電力業界として必要とする公知情報である。

提供方法

情報は主にメールで連絡しており、確実に伝達したい場合には、メール・FAX送付後に確認の電話を入れるようにしている。また、情報に応じては、会議体を活用し、情報共有している。

(E) 現在の課題と今後の方向性

CEPTOAR 事務局としての課題

CEPTOAR の仕組みの中では、電気事業連合会は事務局であり、実際の対策等のアクションをとるのは事業者であるため、受信した情報の精査、および共有すべき情報の発信については配慮している。

なお、重要インフラ分野といっても、金融、通信分野等のシステム = サービスの分野と、システム サービスの分野があるので、システムの位置づけによって各 CEPTOAR の取り組みや役割は異なる。

(5) 警察庁サイバーフォースセンター

(A) 組織の概要

ホームページ URL

<http://www.cyberpolice.go.jp/> (@police の HP)

組織の設立背景

警察庁は、サイバーテロの予兆把握、被害の拡大防止のための緊急対応に係る都道府県警察への技術支援等を行うために2001年4月、警察庁情報通信局技術対策課(現情報技術解析課)にサイバーテロ対策技術室を設置したほか、警察庁および管区警察局情報通信部の技術対策課(現情報技術解析課)に、サイバーテロ対策に当たる専門の技術部隊であるサイバーフォースを創設した。

組織の活動内容

サイバーフォースセンターは、各地のサイバーフォースの司令塔として東京に設置されている。インターネット上の治安情勢を24時間体制で監視することで、関連情報を収集・分析するとともに、さまざまな研究やサイバーテロ対策要員の教育訓練が実施可能な設備を備えている。

組織の運営形態

常設組織であり、政府主管組織(所管:警察庁)である。

(B) 情報収集の詳細

情報源

情報収集の情報源としては、「公知情報から収集する情報」が中心であり、「他組織との情報交換による情報」も活用している。

収集した情報の一部はデータベース化しており、それ以外の情報はテキストベースで保管している。

収集データ

情報収集における収集項目は、公知情報による定量データや、情報交換による定性データ等、多岐にわたるデータを収集している。

(C) 情報分析の詳細

分析の方法

収集したデータを対象に分析を実施しているが、統計処理的なトレンド

分析より個別の事象の分析に重点を置いている。

(D) 情報提供の詳細

情報提供における提供対象

さまざまな組織に情報を提供しているが、その中でも特に「重要インフラ事業者」への提供に注力している。

提供内容

重要インフラ事業者のシステムを守るためには何が必要かという観点で情報を収集しており、収集・分析した情報に基づいて、サイバー被害の予兆情報を中心に、多岐にわたる情報を提供している。

また、重要インフラ事業者に共通した一般的な情報だけでなく、個別の事業者特有の情報も提供している。

提供方法

重要インフラ事業者に対して、事業者特有の情報を提供する場合には、各都道府県警を通じた提供を行っている。

また、重要インフラ事業者に対して、情報セキュリティ全般の情報を提供する場合には、メールによる配信を行っている。

その他の提供方法としては、セミナーの開催、ホームページでの提供、個別の訪問等がある。

(E) 外部とのチャンネル

国際協力の状況

FIRST(Forum of Incident Response and Security Teams)への加盟や海外関係機関(法執行機関、情報セキュリティ機関等)との協力を行っている。

官民連携の状況

重要インフラ事業者と協力してサイバーテロ対策を行っている。

3.1.2. 経済・金融・社会等の分析組織・機関

(1) 日本銀行

ホームページ等の公知情報をもとに活動内容を整理したもの。

(A) 組織の概要

ホームページ URL

<http://www.boj.or.jp/> (日本銀行)

<http://www.imes.boj.or.jp/> (日本銀行金融研究所)

組織の設立背景・活動内容

日本銀行は日本で唯一の中央銀行であり、日本銀行法によりそのあり方が定められている認可法人となっている。日本銀行法では、日本銀行の目的を、「我が国の中央銀行として、銀行券を発行するとともに、通貨および金融の調節を行うこと」および「銀行その他の金融機関の間で行われる資金決済の円滑の確保を図り、もって信用秩序の維持に資すること」と規定している。

名称	主な担当事務の内容
政策委員会室	政策委員会の議事の運営 / 国会との連絡 / 報道機関を通じた広報 / 重要な文書に関する法令面の審査 / 役員に関する諸般の事務 / 監事の監査に関する補佐
検査室	事務処理の検査
企画室	金融政策に関する基本的事項の企画・立案
金融市場局	金融調節の実施 / 為替介入 / 国内金融・資本・外国為替市場の整備 / 国内外の金融・資本・外国為替市場の調査分析
調査統計局	国内の経済および財政の調査・分析 / 統計の作成
信用機構室	信用秩序の維持に資する施策に関する基本的事項の企画・立案
考査局	考査の実施 / オフサイト・モニタリングの実施 / 最後の貸し手としての貸出に関する具体的事項の決定
国際局	外国の中央銀行等との連絡・調整 / 外国中央銀行等への金融面の協力 / 海外経済・国際金融の調査・分析 / 国際収支統計等の作成
発券局	日本銀行券の発行、流通および管理に関する事務 / 貨幣の受払・鑑査等
業務局	手形割引・貸付 / 手形・国債等の売買・貸借(オペ) / 預金取引 / 国庫金の取扱い / 国債に関する事務
システム情報局	事務処理のシステム化 / コンピューター・システム(日銀ネット等)の運行
情報サービス局	一般広報 / 資料・図書の保管 / 貯蓄広報運動
経営企画室	組織や経営資源に関する基本的事項の企画・立案 / 会計に関する事務
人事局	人事制度、職員の人事、能力開発に関する事務
文書局	不動産および動産の取得・処分・管理、職員の福利厚生、警備、輸送、出資証券などに関する事務
金融研究所	金融経済の基本問題に関する研究 / 金融経済に関する歴史的資料の収集・保管・公開 / 学界との交流

図表 3-1 日本銀行の組織構成(出典:新しい日本銀行 その機能と業務

< <http://www.imes.boj.or.jp/japanese/pf.html> >)

(B) 情報収集の詳細

情報源

日本銀行で作成している各種の統計を含むさまざまな金融・経済統計の活用だけでなく、金融機関や事業法人、各種の業界団体やシンクタンク、政府や外国の中央銀行・国際機関等といったさまざまな相手との意見交換や、これらの組織が開催する各種のセミナー等への出席、広報活動を通じた人々の意見の聴取といった、多種多様な方法により情報収集を行っている。

収集データ

収集データは、政策や各業務の内容・目的に応じて多岐にわたる。

【収集データの例】

- 銀行券が全国に円滑に行きわたるよう準備するため、本店や支店での銀行券の受払の変化を把握する
- 日銀ネットをより効率的で安全なものとするよう、決済システムに関する技術革新の動向をフォローする
- 適切な金融調節を行うため、金融市場の動向をモニターし、金融機関と意見交換する
- 国庫金に関する事務の効率化を図るため、諸外国の動向を調べる

(C) 情報分析の詳細(金融政策に関連する調査・分析活動を対象)

分析の対象

金融政策を適切に運営していくことを目的とする調査分析としては、景気動向調査、金融動向調査等を実施している。

分析の方法

【景気動向調査】

景気動向の調査は、各種の統計を用いて経済状況をマクロ的な視点から分析するマクロ調査と、主として各種企業に対するヒアリングを通じて得た情報をもとに分析を行うミクロ調査からなる。

マクロ調査においては、財・サービスの需要動向(投資や消費、政府支出や輸出入)、企業活動(生産や雇用、収益等)、そして物価動向が主たる調査の対象となる。

- サービスの需要動向や企業活動に関しては、自ら作成している短観(全国企業短期経済観測調査)や国際収支統計に加え、国

民経済計算、鉱工業生産指数、家計調査、機械受注統計調査、住宅着工統計調査等、各省庁や各種団体によって作成される統計を用いて分析している

- 物価動向に関しては、自ら作成する各種の価格指数(卸売物価指数、企業向けサービス価格指数、製造業部門別投入・産出物価指数)のほか、消費者物価指数、国内外の商品市況、地価等をきめ細かくモニターし分析している

一方、ミクロ調査は、マクロ調査で捉えきれない景気の変化を把握したり、統計調査の時間的遅れをカバーしたりするほか、景気動向の背景をより細かく分析するために行われるものである。

- ミクロ調査は、主として各企業を対象とするヒアリングを通じて行われる。その対象は、鉄鋼、機械、建設、大型小売店、商社等といった広範な業種の主要企業から、全国各地の中堅・中小企業まで幅広いものとなっており、ヒアリングを通じて、各業界および各地の景気動向、生産、設備投資、収益、輸出入、資金調達等の動向を把握している

【金融動向調査】

金融動向の調査としては、国内の通貨の量を示すマネーサプライの動きを密接にモニターしているほか、貸出市場や債券・株式市場における企業の資金調達に関する動向を把握したり、主要金融機関に対し貸出量や貸出金利の変動の背景等についてヒアリングを実施したりすることで、通貨の需要と供給に関する情報の収集・分析を行っている。

(D) 情報提供の詳細

提供内容

透明性の高い政策・業務運営体制の確立を目指して、法律上求められる諸資料等の公表はもちろん、政策委員会の決定事項の公表や、日々の金融調節の内容、日銀当預残高の増減の実績・予想、決済動向・主要勘定等といった業務の実績、各種のオペレーションの相手先を選定するための基準、最後の貸し手の機能や考査の運営方針等の公表を行っている。

提供方法

調査活動の成果は、政策委員会や関連する業務部門に対して随時報告されるとともに、金融政策決定会合において金融政策の運営を決定す

る際に活用され、『金融経済月報』として毎月公表されている。

(E) 外部とのチャネル

研究活動における交流

国内外の学者や実務家を招聘して客員研究員を委嘱したり、各種の研究会やワークショップ、コンファレンス等を開催したりすることで、外部研究者との研究活動の交流を図っている。

(2) 財団法人日本エネルギー経済研究所

(A) 組織の概要

ホームページ URL

<http://eneken.ieej.or.jp/index.html>

組織の設立背景

「エネルギー諸般の問題を客観的に分析することにより、政策立案の基礎データ、情報、レポート等を提供し、日本のエネルギー産業、エネルギー需要産業の健全な発展および国民生活の向上に寄与するために国民経済全般の観点から専門的な研究を目指すこと」が設立目的である。

社会的ニーズはその後多様化し、エネルギーと密接に関連した環境問題や国際協力等まで研究分野が広がっている。

組織の活動内容

本研究所の役割は、産業や国民の期待に応えるべく調査、研究活動に取組、単に一産業や一国経済の範囲にとどまることなく、世界的視野で問題点の解明や対応策についての提言を行うことである。

組織の運営形態

経済産業省所管の純民間組織(常設)であり、付置機関として、石油情報センター、アジア太平洋エネルギー研究センターの2機関が設置されている。

従業者の雇用形態、従業員数

研究所には約100名の研究員が在籍し、その4割弱が石油、電力、ガス、商社、金融等の会員企業からの出向者で構成されている。

また、客員研究員制度があり、大学教授や各分野の専門家にアドバイスを求めることが可能である。

組織の部門構造

研究所本部の部門構造は、2グループ(開発調査グループ、戦略研究グループ)、4ユニット(企画事業ユニット、戦略・産業ユニット、計量分析ユニット、地球環境ユニット)、1センター(中東研究センター)となる。

このうち計量分析ユニットは、情報収集活動を中心に担当するグループ(統計情報グループ)と予測・分析活動を中心に担当するグループの2グループからなる。

(B) 情報収集の詳細

情報源

汎用的に活用される経済データは、研究所で一括購入して資料室に保管されている。情報源は新聞、雑誌、刊行物等である。

マーケット分析に必要となるデータについては、東京工業品取引所やNYMEX(ニューヨーク マーカントイル取引所)から提供を受けている。

収集データ

収集している定量データとしては、国内・海外のエネルギー需給データや、エネルギー関連指標、GDP等の経済関連指標がある。

また、エネルギー分野では一般消費者の動向が一番手薄であるため、従来は紙面でのアンケート調査を行っていたが、現在は回答率を考慮して、委託によるWebアンケート等を実施することもある。

(C) 情報分析の詳細

活動内容

主に、エネルギー需給構造の総合的な分析や分析に必要な経済モデル、エネルギーモデルの開発を行っている。

分析の方法

計量分析モデルでは、過去のデータから将来を予測するのが主体であり、分析・予測には、計量経済モデルを取り扱う特殊なツールを利用する一方、モデルに取り込む前の作業については主にエクセルを用いて実施している。

分析上の留意点

分析結果の妥当性を判断する能力が極めて重要であり、研究所員単独で判断がつかない場合には、出向者等有識者の見解や支援を得て妥当性を判断している。

分析時には、収集するデータの信頼性と分析精度のバランスに特に留意している。

(D) 情報提供の詳細

提供内容

エネルギー需給動向、経済・産業動向、研究成果(エネルギー政策)等の情報を提供している。

提供方法

提供方法としては、主に「オンラインデータベース」「報告書」「報告会」を活用している。

オンラインデータベースでは、国内外の月次および年次エネルギー経済データが、インターネットを通じて、データバンク会員にオンラインで情報提供されている(EDMC データバンク)。

留意点

対外的に提供される情報については中立性を特に重視しており、媒体を利用して情報を発信する際には、広報委員会において審査が行われている。

(E) 外部とのチャンネル

国内連携の状況

短期のエネルギー需給動向委員会を設立して、そこに石油、電力、ガスの専門家を集めてヒアリングを実施することがある。

国際協力の状況

APEC エネルギー統計・予測専門家会合の事務局を担当しており、各国政府からエネルギー統計を収集して「APEC エネルギーデータベース」を構築するとともに、インターネットを通じたネットワーク化を進めている。

(F) 現在の課題と今後の方向性

エネルギー消費が多い中国・インド等の海外の研究所とのアライアンスを強化し共同研究を進めていきたい。国内では、技術の分野を深く調査している機関や環境系の調査機関等とのアライアンスを深めていきたい。

(3) 国民生活センター

(A) 組織の概要

ホームページ等の公知情報をもとに活動内容を整理したもの。

ホームページ URL

<http://www.kokusen.go.jp/>

設立背景

国民生活の安定および向上に寄与するため、総合的見地から、国民生活に関する情報の提供および調査研究を行うことを目的として、国民生活センター法に基づき 1970 年 10 月に発足した。

活動内容

全国の消費生活センター等から収集された消費者相談情報を分析し消費者被害を未然に防止するための情報提供を行うとともに、消費生活相談、商品テスト、教育研修、消費者問題に関する調査研究等を活動の中心としている組織であり、消費者問題に関する中核的機能を担っている。

運営形態、従業員数

常設組織であり、常勤職員数職員 114 名(平成 19 年 6 月 1 日現在)が在籍している。

部門構造

7 部 4 課 5 室 1 館(2007 年度)による部門構成となり、情報収集および分析機能は、情報分析部が担っている。

(B) 情報収集の詳細

情報源

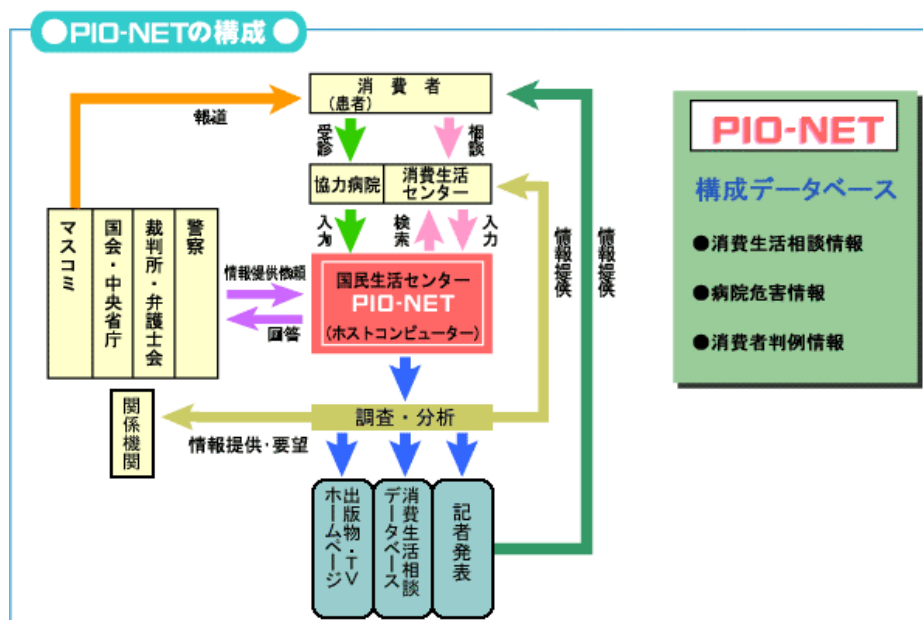
苦情相談等の消費者トラブル情報の情報源は、国民生活センターや各地域の消費生活センターにおける相談窓口、電話窓口およびホームページ上の消費者トラブルメール箱である。

また、主婦を対象として商品やサービスに対する不満・被害を調査した「国民生活動向調査」等の生活面の調査結果を利用している。

収集方法

消費生活に関する相談は、紙媒体の「消費生活相談カード」に直接情報を記入するか、相談窓口に設置された「直接作成システム」を利用してデータ化される。

データ化された情報は、国民生活センターと全国の消費生活センターをオンラインネットワークで結び、消費生活に関する情報を蓄積・活用している「PIO-NET」に登録される。



図表 3-2 PIO-NET のシステム構成 (出典:国民生活センター HP)

(C) 情報分析の詳細

分析の方法

情報分析部では、消費者から寄せられた情報について、消費者被害の未然防止・拡大防止を目的として、問題性、緊急性の高い消費者問題を見極めつつ調査・分析を行っている。

(D) 情報提供の詳細

提供内容

消費者トラブル関連情報、商品テスト情報、調査報告書等

提供方法

適宜、記者発表やホームページ、定期刊行物「たしかな目」「国民生活」「消費生活年報」、テレビ番組「ご存知ですか消費者身に情報」、啓発用リーフレット等を通じて消費者に情報提供している。

また、商品別・商法別で相談件数等を抽出・検索できる「消費生活相談データベース」をホームページで公開している。

3.1.3. 国内調査結果のまとめ

国内の情報セキュリティ分析組織・機関の活動状況について、情報セキュリティ分析ラボラトリー（以下、「情報分析ラボ」）のあり方や活動方針に資するポイントを整理した。

(1) 組織の活動目的

今回、調査対象とした組織・機関の多くでは、「誰に」「何を」提供するのかという2つの観点から組織の注力領域が示されており、これを軸足として活動目的(ミッション)や具体的な活動内容が定められていた。

(2) 組織の役割(機能)

(A) 収集機能

ミクロ的な個社事例を収集する場合と、マクロ的な市場動向を収集する場合に大別され、対象に応じて情報収集源や収集方法が大きく異なる。ミクロ的な情報を収集する場合には、会員企業・協力組織との情報交換が、マクロ的な情報を収集する場合には、公知情報やアンケート調査等が主流となっている。

また、収集した情報を分析等に活用するにあたり、担当者が妥当性を確認することで、情報の信頼性を確保している組織も存在する。

(B) 分析機能

情報セキュリティ分析組織・機関の多くでは、それほど高度な分析手法は採用しておらず、平均、単純集計、クロス集計等、比較的単純な統計処理による分析を行っている。

(C) 提供機能

広く多くの対象に提供される場合には、ホームページやセミナー等の方法によって提供される傾向にあり、特定の対象にプッシュ型で提供される場合には、メールや個別訪問等の方法によって提供される傾向にある。

(3) 組織の体制

(A) 組織構成

活動内容や調査研究テーマに応じた部門構成の組織が多く、情報収集専門部門等の機能別の部門構成は見られない。これは、調査研究テーマ等に応じた部門構成にすることで、バックグラウンドや分析テーマへの理

解が深まることによる各機能自体の効率性の向上や、機能間の連携が見込まれるためと想定される。

(B) 従業員人数

収集・分析・提供をフルラインで実施している組織・機関では、概ね 30～50 名程度が上記業務に従事している。一方で、収集や提供・分析活動以外の活動を主体としている組織・機関では、わずか数名程度の従業員しか従事していないことから、分析作業や分析データの整備には他の活動と比して多くのリソースが必要と想定される。

(C) 人材

内部リソースでカバーしきれない専門知識については、会員等の団体構成組織や学識経験者等の協力者によって対応している組織が目立つ。

(4) 関係機関との連携

組織単独では収集できないデータの入手、マイクロ情報の収集、個社単位での情報提供等を目的として、外部機関と協力関係を構築している組織が多い。

3.2. 海外調査結果(米国)

3.2.1. 情報セキュリティ関連組織・機関

(1) Computer Security Online(CXO Media)

(A) 組織の概要

ホームページ URL

<http://www.csoonline.com/>

設立背景、活動内容

「Computer Security Online(CSO)」とは、CXO Media 社の CSO 部門から出版されている雑誌のことである。CXO Media 社は、300 種以上の雑誌を出版し、その他、イベント主催、調査等も手がけている International Data Group (IDG) 社の傘下の一社である。

同社は、「CSO」「CIO」といった雑誌の出版をはじめ IT 全般および情報セキュリティコミュニティをターゲットとしたイベントも開催している。同社の CSO 部門の役割は、企業のセキュリティ部門の幹部に対して、あらゆる分野に関するセキュリティ関連の問題について出版物、イベント、調査等を通じて情報発信することで、企業内において的確な判断ができるようサポートすることである。

CXO Media 社の CSO 部門の主な活動は以下のとおり。

(出版)

- 情報セキュリティ関連のニュースと分析に関する雑誌「CSO」の出版
- オンライン版「CSO」の Web サイト(1 月間あたり約 9 万人が閲覧(版元公称値))

(イベント)

- 情報セキュリティコミュニティに関するイベントを主催(2007 年には、事業継続、ID 管理に関する専門的なトピックをカバーした情報セキュリティ関連の会議を開催した)

(調査)

- 情報セキュリティに関する調査を行い、その結果を雑誌「CSO」で公表
- CSO 読者アンケート調査を実施し、結果を読者に配布

運営形態

民間企業であるが、調査実施のために第三者機関と定期的に提携関係を築いているのが特徴的である。

例えば、CERT/CC は、過去に内部脅威に関する調査をした経験を持つことから、質問リストの作成や結果の分析で CSO 部門をサポートしている (CERT/CC は、「e-Crime Watch Survey」にも協力)。

2002 年から実施されている年次調査「State of Information Security Survey」では、PrinceWaterhouseCoopers (PWC) 社がパートナーとして、調査票の作成や調査の実施、結果分析といった一連の作業をサポートするとともに、調査票を、PWC 社の顧客の情報セキュリティ関係者に配布している。

従業員の雇用形態、従業員数

上記運営形態からわかるように同社は情報セキュリティに関する調査業務において常設組織体制をとっていないが、CSO 部門には、フルタイムスタッフ 2 人で構成される社内調査ユニットがあり、出版物作成のための調査を行っている。

(B) 調査活動全般

CSO 部門は情報セキュリティ関連のトピックについて以下のような調査を行っている。

「State of Information Security」(年次調査)

- 世界消費者市場や民間セクターにおける情報セキュリティ管理の調査
- PWC 社の協力を得て実施

「e-Crime Watch Survey」(年次調査)

- サイバー犯罪とその対応に関する米国動向に焦点をあてた調査で、最初に実施されたのは 2003 年
- 米検察局 (U.S. Secret Service) (以下、「検察局」と CERT/CC の協力を得て実施
- 検察局は、CSO 部門のリーダーシップで実施される調査に協力することで、サイバー犯罪の動向、情報セキュリティ部門の幹部によるサイバー犯罪への対処、その効果等に関する重要な情報が得られると考えた
- 検察局は、サイバーセキュリティに対する内部脅威の技術的専門知識を持つ CERT/CC にも同調査への参加を奨励し、出資を行わせた

- CSO 部門と CERT/CC、米検察局の三者が共同出資して実施したが、最近になって、Microsoft 社の出資も得た(全体額および出資額は非公表)

その他

- 情報セキュリティスタッフである読者が興味を有する特定のトピックについて、もしくは、情報セキュリティ部門のエグゼクティブが最も重視している内容に関する調査を実施している
- 第三者が依頼あるいは出資するカスタム調査も実施している

(C) 情報収集の詳細 (「e-Crime Watch Survey」の場合)

- 質問項目、内容の検討手順は以下のとおり
IT コミュニティがどのようなトピックに興味をもっているかを担当人員が特定し、参加者から最も効果的な回答が得られるような調査票を準備する
CSO 部門、CERT/CC、検察局の間で、調査票に取り上げられるべき質問の内容について電話会議を行う
電話会議の参加者は、情報セキュリティに関して今最も重要と考えられるトピックを持ち寄り、情報をアンケート調査から得る方法について議論する
特に前年の調査票の内容の中で大きく変化していることが予測される情報セキュリティ分野に関する議論を行う(2007 年は、ターゲット攻撃や不特定多数に対する攻撃に関する新しい質問が追加された)

(回答者に関する質問項目)

- 業種(公共、民間企業、重要インフラセクタ関連)
- 組織(従業員数、役職)
- セキュリティ予算
- セキュリティイベント数
- セキュリティイベントの原因(内部者、外部者、不明)
- セキュリティイベントの種類(ターゲット攻撃もしくは不特定多数)
- ターゲット攻撃数の変化
- ターゲット攻撃による金銭的被害
- 全イベントにおける実際の(e-Crime)の比率
- 電子犯罪の種類、損失規模、メカニズム

(セキュリティ手段の効果に関する質問項目)

- 正式なポリシー
- 記録の保管期間

- c) サイバーセキュリティ技術の効果度
- d) セキュリティポリシーの効果度
- e) セキュリティポリシーの見直し、アップデートの頻度
- f) サイバーセキュリティへの懸念に関する経年推移

以上のような調査票の構成作業は約 2 週間で終わる。

調査票の送付、回収

- 完成した調査票を、電子メール経由で雑誌「CSO」の読者と検察局の電子犯罪タスクフォースのメンバーに送信する(回答期間 3 週間以内)
- 親会社(IDG 社)が、CSO 部門が行う調査の質問リストの作成や配布作業をサポートしている
- 最新のケースでは、2007 年 7 月 26 日、1 万 5 千人に電子メールで調査票が送信され、671 人から回答を得た

(D) 情報分析の詳細

- CSO 部門の調査ユニットは、調査票の回収後に回答を集計し、各質問への回答の分布に関する基本的な数値データを作成する
- 特別な分析ソフトウェアや分析用ソフトウェア等は使用しない
- 集計結果は、CSO 部門、CERT/CC、検察局の参加者に配布され、それぞれの分析作業に利用する
- 分析結果を話し合うための電話会議を開催する(約 2 週間)

(E) 情報提供の詳細

提供方法

- 調査結果とその分析結果を含んだ内容の概要をプレスリリースとして発表し、さらに詳細な内容については、雑誌「CSO」に記事として掲載する
- IT および情報セキュリティ関連の外部メディアに対しても、こうしたプレスリリースや詳細記事を PR する
- CSO 部門、CERT/CC、検察局の参加者は調査結果について、会議の講演者として、あるいは、ポッドキャストにて講演することもある
- CERT/CC は自らの Web サイトにおいても同調査の結果を公表する

効果

- CSO 部門は、これまでに企業の情報セキュリティ担当幹部から良いフィードバックを得ており、企業によっては調査結果を自社の情報セキュリティプラクティスの基準として活用している例もある
- セキュリティイベントに関する調査結果については、情報セキュリティに対する投資の価値を決定するのにも役に立つとの声も寄せられている
- 情報セキュリティ幹部へ警鐘を鳴らす役割も果たしている(最近、大々的に報道される広範囲に及ぶ攻撃数が減っているため、組織は深刻なサイバー犯罪に対する心配の必要がなくなったと捉えられがちであったが、2007 年調査によると、企業が受けた攻撃の多くは、内部者による攻撃を含むターゲット型攻撃であり、サイバー犯罪の脅威は依然深刻であることが明らかとなった)

(2) Computer Security Institute (CSI)

(A) 組織の概要

ホームページ URL

<http://www.gocsi.com/>

設立背景、活動内容

サイバーセキュリティ分野に特化した調査や出版、イベント等を実施する企業で、サイバーセキュリティの重要さへの認識と、企業におけるサイバーセキュリティ導入のニーズを高めるために 1974 年に設立された。

世界的な活動を展開し、情報セキュリティに関するイベントの主催やテクノロジー業界を対象としたマーケティング調査等を行う CMP Technology 社の子会社である。

調査活動に加え、「CSI 会議 (CSI Conference)」（CSI が主催する最大の会議。「CSI Survey」の発表後 1 ヶ月以内に開催）や「セキュリティエクスチェンジ (Security Exchange)」（500 人ほどの参加者が情報共有や人的ネットワークの構築を行うことができる比較的インフォーマルなイベント）といったイベントの開催、あるいは、月刊ニューレター「コンピュータセキュリティアラート (Computer Security Alert)」、季刊誌「コンピュータセキュリティジャーナル (Computer Security Journal)」の出版等にも取り組んでいる。

組織の運営形態

個人会員形態をとっており、会員は、同社が出版する雑誌を受け取ることや、同社が主催する会議に割引価格で参加することができる。会員は、個人のみ（年会費は 224 ドル）で、現在の会員数は 3,500 人である。

大企業からの会員が大部分を占めており、米国経済全体の動向の分析とは位置づけが異なる。一方、会員構造は長年あまり変化していないことから、サイバーセキュリティ動向の経年モニタリングに適している。

従業員の雇用形態、従業員数

スタッフの多くは親会社の社員で、主なユニットは営業、イベント、会員サービスの 3 つである。

CSI 社の常任幹部は CSI のディレクタ、教育ディレクタ、編集者の計 3 名となっており、年次調査「CSI Survey」への取り組みの中心人物である。

(B) 調査活動の概要

「CSI Survey」(年次調査)

CSI社とFBIのサンフランシスコ犯罪班との間のインフォーマルな取り決めにより「CSI/FBI Survey」として1996年に開始した。

CSI社は当初、資金やリソースの大部分を提供し調査内容に対する責任を担い、FBIは質問の選択の支援や、調査結果の分析を行う支援役という役割分担となっており、調査タイトルに「FBI」という名前を添えることによって、FBIは調査結果へより多くの関心を引くことに貢献した。

このように調査費用はCSI社から提供されており、FBIから直接的な資金提供は行われていないことから、2007年にFBIが公的資金を投資していないことを明確にするために、調査名から「FBI」の名前が除かれた。

この結果、同社は営利活動を積極的に行うことができるようになった。今後は、調査結果を無料で提供し続ける一方、調査結果を利用したベンチマーキングツールやコンサルティングサービスの提供等、付加価値サービスを有料で提供する可能性もある。

その他の調査

定期的に他の組織と提携し、サイバーセキュリティに関する特定のトピックに集中した調査を実施している。

例えば、Webセキュリティの調査担当者がWeb2.0テクノロジーを活用した構築されたWebサイトにおけるセキュリティ脆弱性を報告するのを妨げる法的・倫理的・社会的・技術的障害に関する調査を行うために、CSI社は米司法省(U.S. Department of Justice)と2007年6月に提携関係を築いている。

(C) 情報収集の詳細(「CSI Survey」の場合)

収集テーマ

- 主にサイバー犯罪とサイバーセキュリティマネジメント

実施主体

- FBIだけでなく、メリーランド大学ビジネススクール、その他のサイバーセキュリティ専門家もパートナーとして参加

収集作業の手順、特徴

- CSI社とパートナーで質問を選定する(新しい質問の追加は、質問数増による回答率急落、調査結果価値下落を避けるため稀である)

- 調査票準備プロセス全体で 2 週間
- 調査対象者は会員および CSI 社の会議に参加した者で、調査票は郵便または電子メールで配布(電子メール版には、回答者が回答を電子的に送信することができる Web サイトへのリンクが含まれる)

調査票の主な質問

(回答者プロフィールに関する質問項目)

- a) 業界セクター、従業員数、売上、役職名

(サイバーセキュリティマネジメントに関する質問項目)

- b) サイバーセキュリティに費やす IT 予算の比率
- c) トレーニングに費やす予算の比率
- d) 投資利益率 (Return on Investment: ROI)、正味現在価値 (Net Present Value: NPV)、内部利益率 (Internal Rate of Return: IRR)
- e) アウトソースしているサイバーセキュリティ機能の比率
- f) サイバーセキュリティ保険
- g) 利用している技術および効果測定手法の種類
- h) トレーニングの効果を評価するための技術
- i) サイバーセキュリティ情報共有組織 (ISAC、Infragard 等) への参加

(サイバー犯罪に関する質問項目)

- a) 過去 12 ヶ月に経験したインシデントの内容や数
- b) 内部者が原因となった損失の比率
- c) 過去 1 年間に検知した攻撃の種類、Web サイトインシデントの経験
- d) 攻撃の種類別、損失金額、攻撃あたりの平均損失
- e) ターゲット攻撃の経験
- f) 法執行機関にインシデントを報告しなかった理由
- g) サーベンス・オクスリー法 (米国企業改革法) の影響

回収結果

- 2007 年は、約 5,000 人の個人に調査票を送り、494 人 (約 10%) から回答があった

(D) 情報分析の詳細

- 回答は、CMP Technology 社の社員により自社のデータ入力ツールに入力され、回答を分析する第 1 アナリストが分析作業を行う
- 平均、パーセンテージ等、基礎的分析を用いている(過去には SPSS 等、高度な分析ソフトウェアを利用していたが、多くの機能は不要となった)
- 分析結果をパートナーが共有し、パートナーで独自の分析を行う
- 学术界のパートナーからの分析結果を受け取る時間がかかり、分析作業にかかる時間は最終的に 1~2 ヶ月間に至ることもある

(E) 情報提供の詳細

提供主体

- 報告書のハードコピー版の作成および配布は親会社が実施
- 自社のホームページに掲載

提供方法

- ハードコピー版は、会員および CSI 社の会議参加者に配布している
- プレスリリースの公表に加え、技術関連のメディアに直接コンタクトし、同調査の発表を知らせている
- 自社 Web サイト上で報告書を無料公開し、また、報告書の内容を紹介する Web キャストもホストしている
- 教育者や研究者が教育、研究のために「CSI Survey」の報告書の中の情報を制限なく引用できるようにしている。一方、その他の目的での報告書の利用は、一定の制限のもと許可されている

効果

- サイバー犯罪インシデントによる損失金額は、ジャーナリストやその他の読者からの関心を集める最も人気のあるデータである
- ジャーナリストによる引用実績が豊富で、サイバー犯罪やサイバーセキュリティに関する統計を含む記事を執筆する場合に同調査から情報が頻繁に引用されている

(3) インターネット犯罪苦情センター (Internet Crime Complaint Center: IC3)

(A) 組織の概要

ホームページ URL

<http://www.ic3.gov/complaint/>

設立背景、活動内容

連邦捜査局 (Federal Bureau of Investigations: FBI) と、全米ホワイトカラー犯罪センター (National White Collar Crime Center: NW3C) とのパートナーシップによって 1998 年に設立された。

設立目的は、法執行機関の捜査対象となるケースを確立できるよう、複数のサイバー犯罪の間のパターンを特定することである。サイバー犯罪に関する苦情を集約、分析して、共通する悪事を特定してサイバー犯罪全体の大きな損失金額を法執行組織に提示し、捜査を促している。

主な活動内容は、サイバー犯罪苦情処理と、関係機関等との情報共有の 2 つ。

(サイバー犯罪苦情処理の手順)

- a) サイバー犯罪被害者は、IC3 に Web サイトを通じて、苦情を報告する
- b) IC3 は、受け取った苦情を分析、分類し、複数のサイバー犯罪を連結するパターンを特定し、共通する犯罪を法執行組織に報告する

(情報共有の手順)

- c) 法執行機関、企業、業界団体で、苦情分析に必要な情報を IC3 に提供
(例)
盗難、または、詐取されたクレジットカードで購入された商品が海外に流出する場合、荷物配送業界は IC3 に対して、再配送の可能性のある配送に関する情報を自発的に提供する
- d) FBI の Infragard 等の官民パートナーシップを情報共有チャンネルとして利用し、サイバー犯罪に関する動向を民間セクターに知らせる
- e) サイバー犯罪イニシアチブに参加し、特定した動向に関する情報を、連邦、州、地方レベルの法執行機関に提供する
(例)
フィッシングスキームを捜査するための法執行機関と民間セクターの共同イニシアチブである「デジタル・フィッシュネット (Digital Phishnet)」に参加し、情報共有する

組織の運営形態

FBI によって管理されており、FBI 職員が、IC3 のディレクタを務める。

5 つのチームから構成されており、各チームは、監視役である FBI エージェント 1 人と NW3C からのアナリスト複数名によって構成される。

5 つのチームのうち 4 つはサイバー犯罪に関する苦情を受付、分析する役目を果し、残りの 1 チームは、IC3 が、他の官民セクターの組織と一緒に行うアウトリーチ活動やタスクフォースに関する責任を担っている。

FBI 監督管理プログラムアナリストによると、苦情を処理する 4 チームは、金融、オークション、インターネットサービスプロバイダ、国際といった 4 分野を主な専門としている。

通常、提出された苦情は、その苦情が関連する分野の専門家がいるチームに転送される。一方で、普段は金融チームが処理する苦情を、他のチームが処理するといったことも珍しくなく、チーム間における形式的な要件はない(どのチームもあらゆる苦情を処理できる能力を備える)。

従業者の雇用形態、従業者数

FBI から連邦職員約 6 人、NW3C によってスポンサーされている業界および学术界のアナリスト 40 人、米郵政省検査サービス (U.S. Postal Service Inspection Service: USPIS) の職員 1 人で構成されている。

アナリストは多様な経歴、専門分野から抜き出された面々である。

運営資金

FBI と NW3C から共同で資金を受けているが、FBI が主な出資元である。

(B) 情報収集の詳細(インターネット犯罪苦情処理)

目的

- サイバー犯罪に関する苦情を取りまとめて分析し、法執行機関の捜査対象となりえるケースを確立すること(法執行機関の捜査をサポートするのに役立つ、一般非公開の機密情報も含まれている)

収集対象

- サイバー犯罪またはその可能性のあるものに関する苦情
- 被害者または犯罪者のどちらかの一人が米国内にいる限り、IC3 に苦情を提出可能である
- 民間セクターからもサイバー犯罪情報を入手している。企業は、一般市民が入手できない情報にアクセスできることもあり、それらの情報が IC3 の分析や法執行機関の捜査の手助けとなりうるためである

収集対象情報

- 苦情を提出する者(被害者)の名前、住所、連絡情報
- サイバー犯罪を行った(犯罪を試みた)個人や企業の名前、所在地、連絡情報
- 損失金額
- サイバー犯罪者への支払方法
- インシデントの説明
- 最初のコンタクト方法
- 最初のコンタクトは悪事を誘うものであったか
- 犯罪前の被害者とサイバー犯罪者の関係
- 犯罪前に被害者がサイバー犯罪者に関する調査を行ったことがあるか
- 犯罪が起こってから経過した時間
- 目撃者の名前、住所、連絡情報
- 犯罪に関する報告を受け取った組織の名前、所在地、連絡情報

収集方法

- 苦情フォームは、法執行機関の捜査官を支援するために必要とされるサイバー犯罪に関する情報すべてを収集できるように構成されている

(C) 情報分析の詳細

目的

- 別々に提出された苦情にみられるパターンを特定し、それらの苦情をつなぐ共通の犯人や犯罪の手口を特定すること

ツール

- カスタマイズされた分析ソフトウェア、ChoicePoint や LexisNeis 等のデータベース、FBI によって提出された「疑わしい行動に関する報告 (Suspicious Activity Report)」等のクローズドソースを含め、さまざまなツールを利用している

関係機関(CIRFU)による協力

- 法執行機関による捜査が実行可能となるためのケースを確立できない場合、潜在的なケースを FBI のサイバーインシデント・リソースフュージョンユニット(Cyber Initiative and Resource Fusion Unit: CIRFU)に報告する
- CIRFU は、潜在的なケースを分析して、サイバー犯罪者の割り出しや、その犯罪の防止方法を特定することができる
- CIRFU は独自の分析を終えると、法執行機関にそれらの結果を報告し、捜査または犯罪者の逮捕を促す。また、分析結果の IC3 への報告、サイバー犯罪の手口や防止方法についての IC3 のアナリストの教育、さらに、自らの情報配布チャンネルを通した民間セクターや一般市民向けの分析・捜査結果の公表を行っている

(D) 情報提供の詳細

法執行機関または CIRFU に報告するケースに加え、法執行機関に提供される月間レポートも作成している。

月間レポートには、新しいマルウェアの種類や、新しいソーシャルエンジニアリングの方法等、新しいサイバー犯罪の動向に関する情報が含まれる(一般には非公開)。また、年次レポートも作成(一般公開可能)し、最近のサイバー犯罪に関するパターンや年々の動向、個人がサイバー犯罪を予防するための方法を幅広く報告している(以下は報告データの例)。

- a) 苦情数
- b) 合計損失金額、苦情 1 件あたりの平均損失金額
- c) サイバー犯罪の種類
- d) 被害者がコンタクトされた方法、犯罪者の居場所

(4) Computer Economics

(A) 組織の概要

ホームページ URL

<http://www.computereconomics.com/>

設立背景、活動内容

1979年に設立されたIT市場調査・コンサルティング企業で、調査や出版、評価、コンサルティング等が主な活動である。

企業のIT利用状況やITハードウェアの市場動向に関する調査を実施し、その結果を顧客に有料で提供している(顧客には、北米および海外30カ国以上における主要IT組織やコンサルティング企業等が含まれる)。

IT予算ベンチマーク、IT管理動向、情報セキュリティ、ITインフラ、給与調査といった既存のサービス分野に集中し、かつソフトウェアアプリケーションのコストやメリットに関する分析を強化している。

(調査の方法)

- ITマネジメント関連のさまざまなトピックに関する調査・分析を実施する。中でも、年次調査では、エンドユーザーである企業のIT幹部に対して定期的な調査を行い、そこから得られるデータを基に分析を行っている
- 米国の官民両セクターにおける、ITコスト、人材、技術等の動向に焦点を当てた年次調査「ITコスト、人材、技術動向(IT Spending, Staffing, and Technology Trends)」で知られている
- 特定のIT市場や、IT購入者の購買パターン(PC機種、リース状況等)に関する動向調査も実施している

(出版の方法)

- 調査結果を、月刊ニュースレターや年次報告として出版している

(評価の方法)

- ITハードウェアの妥当な市場価値、残存価値、ITベンダによる価格設定や割引価格等のデータを収集して、「IT Valuations Database」と呼ばれるデータベースに保存し、定期購読者に提供している

運営形態、雇用形態、従業員数

非公開

(B) 調査活動の概要

ITセキュリティ脅威動向 (Trends in IT Security Threats)

- IT の意思決定者たちが、IT セキュリティに対する投資を慎重に決定するためのデータを必要としていることを認識したのがきっかけに、IT セキュリティ脅威に関する調査報告として「マルウェアに関する報告 (Malware Report)」を 1999 年から発行
- IT セキュリティ脅威を包括的に取り上げた「IT セキュリティ脅威動向 (Trends in IT Security Threats)」という新しい調査報告を 2007 年から追加で実施 (今後毎年報告予定)
- 「IT セキュリティ脅威動向」では、各種の脅威に対して事前に知覚されたリスク (Perceptive Risk: 必ずしも物理的に起こりうるわけではないが個人が漠然と認識しているリスク) と、実際に生じたインシデントの比率を測定

ITセキュリティ調査 (IT Security Study)

- サイバーセキュリティの管理面に焦点を当てた調査として「IT セキュリティ報告 (IT Security Report)」を 2006 年に開始 (毎年実施予定)
- サイバーセキュリティ分野のコスト、人材、技術の動向に特化
- IT の意思決定者が、自社のサイバーセキュリティに関する予算、人材、技術導入レベルを、米国全体または同規模の他の企業と比較することで、自社標準を適切に設定すること、また、サイバーセキュリティに対する他社の取り組みやベストプラクティスの導入状況等を理解することで、自社の取り組みを評価することを支援するもの

(C) 情報収集の詳細 (Trends in IT Security Threats)

基本方針

- CERT/CC や CSI 社によるサイバーセキュリティ関連の報告書等を基に選定。対象となる脅威は、読者によって理解しやすく、かつ、企業に対し財務的・業務的に大きな影響をもたらすもの

作業主体

- 選定作業は、同社スタッフと、コンサルタントとして同社を支援している外部の調査アナリストが実施
- 調査対象者として、同社の過去の調査に参加し、役立つ回答を提供してくれた企業の IT 関係幹部、同社と過去に接触したことがない企業を

抽出し、電子メールまたは郵送によって調査票を配布する。 の選定は、企業の規模や業界を考慮して行われる

収集方法

- 無記名で回答できるオプションが設けられており、実際に企業が被害を受けたセキュリティ関連のインシデントに関する内容を報告しやすいものとなっている

収拾対象(2007年の調査対象となった脅威)

- a) マルウェア
- b) フィッシング
- c) ファーミング
- d) スпам
- e) DoS 攻撃
- f) 外部者による不正アクセス
- g) 破壊行為(Vandalism) / 怠業(Sabotage)
- h) サイバー恐喝(Extortion)
- i) 不正取引
- j) 物理的損失
- k) 内部者による不正アクセス
- l) 内部者による悪用

(D) 情報収集の詳細 (IT Security Study)

- 自社の IT コスト、人材、技術動向等に関する過去の調査結果を基に、調査対象となるサイバーセキュリティ技術と管理プラクティスを特定
- 特定されたプラクティスは、企業の IT 意思決定者が社内で導入すべきかどうか決断するのが難しい可能性のあるもの
- 調査対象プラクティスは、関心の高いものと言えるが、推奨しているものとは限らない

(回答者に関する質問項目)

- a) 業種(公共か民間か重要インフラ)

(IT セキュリティの予算に関する質問項目)

- b) IT 予算全体の中の比率とその推移、金額、カテゴリー別金額
- c) 予算の妥当額に関する考え

(IT セキュリティの人材に関する質問項目)

- d) IT スタッフ全体における IT セキュリティスタッフの比率
- e) デスクトップ 1,000 台に対する人数
- f) IT セキュリティ管理の報告体制

(IT セキュリティ技術の適用動向に関する質問項目)

- g) スпамフィルタ、VPN、無線 LAN、WiFi 保護アクセス、サーバアクセスコントロール
- h) 侵入検知システム、侵入防止システム
- i) 暗号化、公開鍵暗号基盤(PKI)、パスワード管理
- j) スマートカード、パスワードトークン、バイオメトリクスの適用

(IT セキュリティ管理実施の動向に関する質問項目)

- k) IT セキュリティポリシーと処置
- l) 物理的セキュリティアクセスコントロール
- m) 文書破棄ポリシー
- n) アプリケーションとデータアクセスコントロール
- o) パスワードの生成に関する要請事項
- p) パスワード変更の強制
- q) 退職した従業員のパスワード無効処理
- r) デスクトップ管理権
- s) 全従業員を対象とした定期 IT セキュリティトレーニング
- t) PC ソフトウェア監査
- u) IT セキュリティ監査
- v) セキュリティスタッフのための IT セキュリティ認証
- w) IT セキュリティインシデント
- x) 原因別の IT セキュリティインシデントの数
- y) エントリーポイント(侵入口)別の IT セキュリティインシデントの比率
- z) Web サイトにおける IT セキュリティインシデントの影響

(E) 情報分析の詳細 (両調査共通)

収集結果レビュー

- 調査参加者から回答を得ると、回答の質をレビューする
- 具体的には、同社アナリストが、回答が未回答、不明、あるいは矛盾があ

るものを特定する。未回答または不明の場合は、参加者にやり直してもらおうよう依頼する一方、回答内容が矛盾している場合は、信用性が低いとして集計対象から除外される

ツールの活用

- 有効回答は SPSS 社の統計ソフトから入力される。このソフトウェアを利用することで、基礎的な統計データを簡単に算出することができる

取りまとめ

- 統計データをもとに、社内のアナリストは分析結果のドラフトを作成して、外部の調査アナリストに送り、情報追加や改訂を依頼する
- 最終的に、外部の調査アナリストからのコメントをもとに、報告書最終版を完成させる
- 調査の全工程はおよそ 3 ヶ月間である
- 外部の調査アナリストを含め、約 8 人が本工程にかかわっている

(F) 情報提供の詳細(両調査共通)

- 最終報告書が完成すると、Computer Economics 社は、調査からの主要成果をプレスリリースで発表する
- 同社 Web サイトに、報告書概要とオンライン購入用のフォームを掲載するとともに、社内のアナリストは、顧客からの質問に対応できるよう準備する

3.2.2. 経済・金融・社会等の分野の組織・機関

(1) 社会保障庁(SSA)、保険計理長室(Office of the Chief Actuary)

(A) 組織の概要

ホームページ URL

<http://www.ssa.gov/OACT/>

設立背景、概要

社会保障庁(Social Security Administration:SSA)は、老齢、遺族、身体障害者年金(Old Age, Survivors, and Disabilities Insurance:OASDI)プログラムを通じて、受給者に給付金を支払っている。給付金は、SAA が管理している 2 つの信託基金である、老齢および遺族年金(Old Age and Survivors Insurance Trust Fund:OASI)信託基金と、身体障害年金(Disabilities Insurance:DI)信託基金から出資されている。

SSA の保険計理長室(Office of the Chief Actuary:OACT)には、人口統計、経済動向、プログラムの条件等の分析に基づいた信託基金の財務状況を年次報告する義務がある。また、信託基金の財務状況に関して、OASDI のプログラムの条件を変更したときに起こりうる影響を予測することも保険計理長(Chief Actuary)の責務の一つである。

運営形態

保険計理長は、SSA のトップである社会保障庁長(Social Security Commissioner)から指名され、その直下に位置する。

OACT は、短期保険計理見積室(Short-Range Actuarial Estimates)と長期保険計理見積室(Office of Long-Range Actuarial Estimates)の 2 つに分かれている。短期保険計理見積室では、向こう 10 年間の信託基金の財務状況を予測し、長期保険計理見積室では、向こう 75 年間の同基金の財務状況を予測する役割を担っている。

雇用形態、従業者数

保険経理士、経済学者を含む 55 人のスタッフを擁する。

資金源

OACT の予算は年間約 500 万ドルで、大部分は人件費に割り当てられている。

(B) 調査活動の概要 -短期保険金計理見積

短期保険計理見積とは、この先10年間に於いて、毎年最初の時点における各信託基金の資産と、その年に受給者に支払う額との比率を算出し10年後の財務状況を予測するもので、SSAが受給者に対する義務を果たすためには何らかの法的措置が必要かどうかを連邦議会や大統領を含むSSAの監視者たちが検討する材料として利用される。

OACTは、10年後までの経済、人口統計、プログラムの給付金に関する動向を予測し、信託基金比率を算出する。また、その動向を予測するために、過去の経済、人口統計、プログラムの給付金に関する動向についても分析している。

(C) 情報収集の詳細

入手対象情報収集

- 経済と人口統計に関する推定に必要なデータ
- プログラムの給付金推定に必要なデータ

入手方法

- 経済と人口統計に関する推定に必要なデータは、商務省の経済分析局(Bureau of Economic Analysis)や国勢調査局(Census Bureau)、労働省の労働統計局(Bureau of Labor Statistics)等から、SSAとの省庁間の同意により提供される
- プログラムの給付金推定に必要なデータには、自庁の給付金プログラムの定期的な管理を通じて得られる庁内の情報が利用される
- これとは別に、SSAでは、「Master Earnings File(MEF)」と呼ばれる、社会保障制度に加入している労働者によって報告される収入に関するデータベースと、社会保障制度の受給者に支払われた給付金の記録として、「Master Beneficiary Record(MBR)」と呼ばれる別のデータベースを管理しており、これらの2つのデータベースからエントリー数の1%分に相当するサンプルを収集する

(D) 情報分析の詳細

実施主体

将来の経済と人口統計に関する推定値を創出するために必要となる過去の経済、人口統計、およびプログラムに関する傾向の分析は、OACTの保険経理士および経済学者が行う。

分析手法、ツール

- 分析の多くに定量的手法が用いられている
- OACTは最近のデータを計算し、各分野における推定を創出するための独自の方式を開発している。この方式には、OACTが独自に開発した「マイクロシミュレーションモデル」と呼ばれる方式も含まれており、同モデルを利用して、人口統計学的に異なる個々のグループの単位、または、米国全体人口の単位における動向を分析することができる
- 市販の分析ソフトウェアはカスタマイズしたうえで分析活動に利用されている

最終決定

- 複数の推定を理事会に報告し、理事会はこれらの推定をレビューし、どの推定が最も現実的であるかを投票によって決定する(中間推定)
- 中間推定とは、最も起こりうる予測で、社会保障信託基金をうまく維持するために低コストでも高コストでもない経済・人口傾向を反映したもの

(E) 提供方法の詳細

- 中間推定を決定したのちに信託基金比率が算出され、その結果を、理事会の意見を代表するものとして年次報告書の中で一般公開する
- SSAの広報は、新しく年次報告書がリリースされたときに、メディアへの報告も行っている。これは、社会保障プログラムの重要性と社会保障改革に関して国民からの関心が高まっているためである
- 同報告書はSSAのOACTのWebサイト上でも公開される

3.2.3. まとめ

海外の官民の今回の調査対象機関の組織の概要、取り組み内容から得られた示唆は以下のとおりであった。

(1) 組織の活動目的

国内機関と同様、「誰に」「何を」提供するのかという 2 つの観点から組織の注力領域が示されていた。本調査の対象とした民間の調査機関においては、特に企業の IT 部門の幹部をターゲットとして想定しているものが中心であった。

(2) 組織の役割(機能)

(A) 収集機能

情報収集方法はアンケートが主流であることが分かった。また、米国において活動成果がひろく一般に提供される調査の特徴は、アンケートの調査票の設計を毎回、数週間にわたって外部の有識者や関係機関を交えつつ詳細に実施していることである。

これは、毎年セキュリティ上のホットピックがかわるため、こうした情報を取り込むための設問を新たに設けるニーズと調査の継続性や回答数(率)を確保するための、設問の絞り込みニーズを同時に満たす必要性があるためである。

(B) 分析機能

今回調査した情報セキュリティ分析組織・機関の多くでは、単純な集計を除く複雑な分析については外部の専門家等に委ねている例が多く見受けられ、SPSS 社の統計分析ツールについては自ら活用する例も見受けられた。また、利用範囲を組織内に限定した独自ツールの導入例もある。

いずれにせよ分析結果の公開に至る過程では、内外の専門知識を有するアナリストの見解を求め、一定程度の調査品質や客観性を確保する配慮がなされている。

(C) 提供機能

概要についてはホームページ等からプレスリリースとして簡単に伝える一方、詳細情報については有料の雑誌購読者や会員向けのみへの情報提供とするといった差別化を図っているところが目立った。

(3) 組織の体制

(A) 組織構成

今回の調査の中で、IC3 では金融、オークション、ISP、国際といったテーマに基づくチーム編成とする例が見受けられた。ただし、各チームとも明確な区分がされているというわけではなく、全員がどのテーマにも対応できるスキルを有していることからトピックに応じて柔軟な対応をとっているようだ。

(B) 従業員人数

今回の調査対象組織では数人の小規模のところが目立った。こうした小規模組織では、外部(有識者や政府機関)との質問票作成等の場面で適宜連携することによって対応している。

(C) 人材

組織内に専門家を抱える場合でも外部人材との交流が積極的に行われている。

(4) 関係機関との連携

情報収集のみならず、調査票の作成や分析、検証といった実作業でも外部有識者、機関等が積極的に携わっていることが確認できた。

4. 情報セキュリティ事象および対策等の実施状況に関するデータ

IT 化の進展に関するデータ、情報セキュリティ事象および対策等の実施状況に関する主なデータについて、文献や Web 等を使用して調査を行い、経年的に把握可能なデータを中心に整理を行った。

4.1. IT 化の進展に関するデータ

4.1.1. 国内の調査レポート

国内における IT 化の進展に関するデータでは、以下の 5 種類の報告書・調査レポートを調査対象とした。

本調査では以下の報告書や調査レポートを対象としたが、この他に、経済産業省が実施している特定サービス産業実態調査等の大規模調査が存在する。

(1) 情報化白書 2006 (財団法人日本情報処理開発協会(JIPDEC))

我が国の情報化動向を総合的に紹介するものであり、情報化動向を概観し、ユーザーの IT 活用動向や情報政策と電子政府・電子自治体の動きを紹介するとともに、情報セキュリティ、法制度の整備状況等をまとめた報告書である。

更新頻度は年単位で、公表されている既存のデータ(以下、「二次データ」)である。

(2) 平成 19 年情報通信白書(総務省)

我が国の情報通信の現状、情報通信の政策の動向について、広く国民の理解を得ることを目的とした実態報告を行うとともに、毎年の特集テーマによる情報通信に関する新たな調査・分析を行っている報告書である。

更新頻度は年単位で、二次データが中心で、独自に調査を実施したデータ(以下「一次データ」)も一部含まれている。

(3) 企業 IT 動向調査 2007(社団法人日本情報システム・ユーザー協会(JUAS))

国内企業の約 4,000 社(有効回答は約 800 社)の IT 部門や、約 4,200 社(有効回答は約 810 社)の社内 IT 利用部門を対象にアンケート調査を行い、企業における IT 投資、IT 利用の現状と経年変化を明らかにしている報告書である。

更新頻度は年単位で一次データである。

- (4) 2006年ITサービス・ユーザー動向調査 / 2006年セキュリティ・ソフトウェア市場動向(ガートナージャパン)

国内企業の約 3,500 社の情報システム責任者を対象にアンケート調査を行い(有効回答は約 530 社)、ユーザーの IT 投資動向、システム化状況、ベンダ選択基準等を明らかにしているレポート(有料レポート)である。

更新頻度は年単位で、一次データである。

- (5) 2006年国内 / 世界の IT サービス市場規模予測(ガートナージャパン)

ユーザー企業が属する業種を産業別に 11 区分し、各産業における IT サービス市場規模と今後 5 年間の予測、トレンド等を分析しているレポート(有料レポート)。

更新頻度は年 2 回で、一次データである。

4.1.2. 国内の調査レポートでの把握可能データ

国内の各報告書・調査レポートで把握可能なデータを、情報化投資動向、市場動向、政策動向、技術開発動向、企業意識／消費者意識、情報資産に関わる動向に分けて掲載状況や具体的なデータの種類、データの入手範囲を整理した。

(1) 調査レポートの対応分野

国内のIT化の進展に関するデータとして、情報化投資動向、市場動向、企業意識／消費者意識は、掲載されている報告書・調査レポートが多く、経年データについても比較的容易に把握可能である。

一方、他の動向は掲載されている報告書・調査レポートがあるものの、経年データでの把握は難しいと考えられる。

調査レポート	調査項目					
	情報化投資動向	市場動向	政策動向	技術開発動向	企業意識／消費者意識	情報資産に関わる動向
情報化白書2006						
平成19年情報通信白書						
企業IT動向調査2007						
2006年ITサービス・ユーザー動向調査 2006年セキュリティ・ソフトウェア市場動向						
2006年国内／世界のITサービス市場規模予測						

* :該当データが掲載されており、経年データ(5年間程度)の取得が可能
 :該当データが掲載されており、単年データの取得が可能
 :該当データに類するデータのみ取得が可能

図表 4-1 調査レポートの対応分野一覧(国内、IT化関連)

(2) 把握可能データ的具体例

調査対象とした国内におけるIT化の進展に関する報告書・調査レポートにおいて、把握可能なデータの種類を例示する。

調査項目	具体的に把握可能なデータ(一例)
情報化投資動向	<ul style="list-style-type: none"> 情報化投資額の推移(情報化白書2006、平成19年情報通信白書) 企業の情報化投資目的の推移(企業IT動向調査2007) 企業の売上高に対する情報化投資割合の推移(企業IT動向調査2007)
市場動向	<ul style="list-style-type: none"> 情報通信産業の国内生産額の推移(平成19年情報通信白書) 世帯のIT関連消費額の推移(情報化白書2006) 日本/世界のITサービスの市場規模予測(2006年国内/世界のITサービス市場規模予測)
政策動向	<ul style="list-style-type: none"> ソフトウェア/情報サービス産業の変遷と国の政策(情報化白書2006) 情報セキュリティ対策に関する国内/海外の政府方針(情報化白書2006) 情報セキュリティ対策に関する経済産業省・総務省の取組(情報化白書2006、平成19年情報通信白書)
技術開発動向	<ul style="list-style-type: none"> ソフトウェア製品/Webアプリケーションの脆弱性届出の取扱状況(情報化白書2006) 情報通信産業の研究費/技術貿易額の推移(平成19年情報通信白書) 日本/世界のセキュリティ・ソフトウェアの新規ライセンス収益(2006年セキュリティ・ソフトウェア市場動向)
企業意識/消費者意識	<ul style="list-style-type: none"> 世帯の情報セキュリティに関する対策の実施状況(情報化白書2006) 企業の情報システムの信頼性に対する評価(企業IT動向調査2007) 企業の情報セキュリティに関する対策の実施状況(企業IT動向調査2007)
情報資産に関わる動向	<ul style="list-style-type: none"> 企業の情報システムの導入状況(情報化白書2006、平成19年情報通信白書) 企業の情報マネジメント体制・プロセスの整備状況(平成19年情報通信白書) 企業の情報セキュリティ体制・要員の確保状況(企業IT動向調査2007)

図表 4-2 把握可能データの例(国内、IT化関連)

(3) 各データから得られる特色

(A) 情報化投資動向

国内の調査レポートから得られる情報化投資動向データとして、産業全体の投資傾向を捉えた市場動向に関するデータでは「情報化投資額の推移」「情報通信資本ストックの推移(産業別・業種別)」等が、各企業の投資活動の傾向を捉えた企業活動に関するデータでは「情報化投資目的の推移」「情報化投資分野の推移」「情報化投資の効果」「売上高に対する情報化投資比率の推移」等が挙げられる。

「平成19年情報通信白書」によると、2005年の実質情報化投資額は約17兆円、民間企業設備投資に占める情報化投資比率は約21%となっている。実質情報化投資額は2002年から順調な成長を遂げているが、ここ数年では成長が鈍化しつつある。また、実質情報化投資額の内訳を分野別に見ると、「電気通信機器」が約10%、「電子計算機本体・同付属装置」が約42%、「ソフトウェア」が約48%となっており、それぞれの構成比の推移を

見ると、近年の成長は「電子計算機本体・同付属装置」「ソフトウェア」によるところが大きいことがわかる。

「企業 IT 動向調査 2007」によると、2006 年時での企業の情報投資目的（情報化投資で解決したい経営課題）は「業務プロセスの改革」「経営トップによる迅速な業績把握・情報把握」「経営の透明性の確保」等が高い比率を占めている。このうち、近年の推移を見ると、「業務プロセスの改革」「経営の透明性の確保」は解決したい経営課題としての比率が増加傾向にあり、情報化投資に対する期待も大きいと考えられる。

(B) 市場動向

国内の調査レポートから得られる市場動向データとしては、「情報通信関連指標（生産・設備・投資等）の推移」「IT サービスの市場規模予測（～2010 年）」「情報通信産業の国内生産額の推移」「情報通信産業の雇用者数の推移」「世帯の IT 関連消費額の推移」等が挙げられる。

「情報化白書 2006」では、情報通信に関連した指標を企業、家計、政府に分けており、企業の供給面として「生産」「サービス」、企業の需要面として「設備投資（民需）」、家計の需要面として「消費」、政府の供給面として「設備投資（官公需）」、外国部門として「輸出」「輸入」の分野を取り上げ、それぞれの市場成長性を表す総合指数、IT と関連した品目のみを抽出した IT 関連指数、および総合指数の増減に対する IT 関連指数の寄与度が示されている。

各指数の近年の動向を見ると、IT 関連指数の前年同期比は「輸入」「生産」「サービス」で高く、これらの分野では、IT と関連した品目の市場が活況を呈していると考えられる。この結果、総合指数の増減に対する IT 関連指数の寄与度も、「輸入」「生産」「サービス」は他の分野に比べて高くなっており、「輸入」では寄与度が 1.6%（2005 年）となっている。

(C) 政策動向

国内の調査レポートから得られる政策動向データとしては、「ソフトウェア / 情報サービス産業の変遷と国の政策の推移」「IT 政策に関する政府方針」「情報セキュリティに関する政府方針」等が挙げられる。なお、これらのデータにおいては経年の動向が俯瞰して整理されているものは少なく、現在取り組んでいる政策を中心に整理されている。

「情報化白書 2006」および「平成 19 年情報通信白書」では、「IT 政策に関する政府方針」として「IT 新改革戦略」の概要や、「重点計画 2006」の概要、「u-Japan 政策」の概要等が整理されている。

また、同調査レポートでは、「情報セキュリティに関する政府方針」として「第1次情報セキュリティ基本計画」の概要や、「セキュア・ジャパン」の概要等が整理されている。この他に、警察庁、防衛省、総務省、経済産業省における個別の施策についても整理されている。

(D) 技術開発動向

国内の調査レポートから得られる技術開発動向データとしては、「情報通信産業の研究費の推移」「情報通信産業の技術貿易額の推移」「情報通信産業の研究者数の推移」「ソフトウェア製品・Web アプリケーションの脆弱性届出の取扱状況」「セキュリティ・ソフトウェアの新規ライセンス収益」等が挙げられる。

「平成19年情報通信白書」によると、2005年度の企業等の研究費(12兆7,458億円)のうち、情報通信産業が占める比率は約36%(4兆5,713億円)となっており、情報通信産業の中でも「情報通信機械器具工業」や「電気機械器具工業」の業種分野で高い比率を占めていることがわかる。また、2005年度の技術貿易輸出額(2兆283億円)に占める情報通信産業の比率は約18%(3,619億円)、技術貿易輸入額(7,037億円)に占める情報通信産業の比率は約60%(4,200億円)となっており、情報通信産業では輸入超過となっている。

(E) 企業意識 / 消費者意識

国内の調査レポートから得られる企業意識 / 消費者意識データとして、企業に関するデータでは「情報システムの信頼性に対する評価」「情報セキュリティに関する対策の実施状況」「ウイルス・不正アクセスに関する対策の実施状況」「顧客の個人情報の保護のために採っている対策」等が、世帯に関するデータでは「情報セキュリティに関する対策の実施状況」「ウイルス・不正アクセスに関する対策の実施状況」「個人情報の保護のために採っている対策」等が挙げられる。

「企業IT動向調査2007」によると、企業の情報セキュリティに関して、対策が十分に進められているのは「ワクチンソフトの定期的更新等のウイルス対策」「ファイアウォール等のネットワーク上の情報アクセス制限」等である一方、対策が進んでおらず不安が強いのは「コンティンジェンシープランの確立等の事業継続対策」「コンプライアンス教育体制の確立」「PC持ち出し等の利用者の情報管理対策」等である。

「情報化白書2006」によると、世帯の情報セキュリティに関して、「怪しい電子メール・添付ファイルの削除」「セキュリティ対策ソフトの導入」

「WindowsUpdate 等による更新」は何らかの対策を行っている比率が約 80%であり、比較的対策が進んでいる。一方で、「パスワードの定期的な変更」は対策を行っている比率が約 40%に留まっており、対策が十分ではないと考えられる。また、情報セキュリティ対策を行う上での問題点としては、「費用がかかる」「手間がかかる」等の理由が挙げられている。

(F) 情報資産に関わる動向

国内の調査レポートから得られる情報資産に関わる動向データとして、企業に関するデータでは「情報システムの導入状況」「情報システム導入による業務・組織改革効果」「情報マネジメント体制・プロセスの整備状況」「情報セキュリティ体制・要員の確保状況」等が挙げられる。

「平成 19 年情報通信白書」によると、情報システムの導入が進んでいるのは、基幹業務では「全社的な共通基幹系データベースの構築」「販売先からの受注」等、間接業務では「管理会計システム」「グループウェア」等であり、どれも導入率が 70%を超えている。また、基幹業務における導入効果としては「業務の正確性が向上した」「オペレーションの速度が上がった」が、間接業務における導入効果としては「社内で周知すべき情報の浸透度・共有度が向上した」が、比較的効果の高い項目として挙げられている。

「企業 IT 動向調査 2007」によると情報セキュリティの体制(部署・担当等)がある企業は 9 割にのぼるものの、専門部署がある企業は約 1 割となっている。情報セキュリティ対策の専任要員が確保されているのは約 2 割の企業に留まる一方で、兼任要員が確保されているのは約 8 割の企業にのぼっており、多くの企業が兼任要員を配置していると考えられる。

4.1.3. 米国の調査レポート

米国における IT 化の進展に関するデータでは、以下の 7 種類の報告書・調査レポートを対象に調査を行った。

- (1) 2007 Enterprise Software Customer Survey (McKinsey and Co. and Sand Hill Group)

IT 業界とその他企業の幹部を対象に、ソフトウェア予算、ソフトウェア購入の意思決定、ビジネスへのインパクト等について調査したレポートである。

単独での調査で、調査の継続性は確認できない。

- (2) 2007 State of the CIO (CIO Magazine)

CIO の役割、IT 予算、IT マネジメント、重要な IT 事項等に関する調査レポートである。

更新頻度は年単位である。

- (3) 50 Technologies: Where CIOs are Spending Their Money (CIO Insight)

企業内の IT 部門幹部を対象とした IT 予算、労働力、重点課題に関する調査レポートである。

更新頻度は不明である。

- (4) IT Spending, Staffing, and Technology Trends (Computer Economics)

企業内の IT 部門幹部を対象とした IT 予算、労働力と重点課題に関する調査レポートである。経済的なセクター毎に報告されている。

更新頻度は年単位である。

- (5) Managing IT Costs in a Weakened Economy (CIO Insight)

企業内の IT 部門幹部を対象に IT コストの管理に関する戦略について調査したレポートである。

更新頻度は不明である。

- (6) Software as a Service (InformationWeek)

IT 部門幹部を対象に SaaS の採用理由、ターゲット、セキュリティ上の問題点や課題を調査したレポートである。

更新頻度は不定期である。

(7) Trends in Telephony Service (Federal Communications Commission)

電話産業の収入、シェア、通話時間、加入者、料金、インフラ投資について調査したレポートである。

更新頻度は年2回である。

4.1.4. 米国の調査レポートでの把握可能データ

米国の各報告書・調査レポートで把握可能なデータを、情報化投資動向、市場動向、政策動向、技術開発動向、企業意識/消費者意識、情報資産に関わる動向に分けて掲載状況やデータの入手範囲を整理した。

(1) 調査レポートの対応分野

米国のIT化の進展に関するデータとして、情報化投資動向、市場動向、企業意識/消費者意識、情報資産に関わる動向は、掲載されている報告書・調査レポートが多く、十分なデータの把握が可能である。一方、他の動向は掲載されている報告書・調査レポートが少なく、十分なデータの把握は難しいと考えられる。

調査レポート	調査項目					
	情報化投資動向	市場動向	政策動向	技術開発動向	企業意識 / 消費者意識	情報資産に関わる動向
2007 Enterprise Software Customer Survey						
2007 State of the CIO						
50 Technologies: Where CIOs are Spending Their Money						
IT Spending, Staffing, and Technology Trends						
Managing IT Costs in a Weakened Economy						
Software as a Service						
Trends in Telephony Service						

* :調査項目を十分にカバー
 :調査項目を部分的にカバー

図表 4-3 調査レポートの対応分野一覧(米国、IT化関連)

(2) 各データから得られる特色

(A) 情報化投資動向

米国の調査レポートから得られる情報化投資動向データは、各調査のサンプル数が必ずしも多くない一方、会社の責任者による IT 投資判断の意思決定の支援という調査趣旨を踏まえた項目が目立つのが特徴であり、「対前年度比の IT 予算の増減」「主な投資対象ソフト・インフラ」等がカバーされている。

「Managing IT Costs In a weakened Economy」によると、2007 年に IT 投資額を増加させた会社の比率は 58%、前年並みが 30%、減少の 12%となっている。ただし、社内的にはコスト削減のプレッシャーが増しているとの回答も多い。また、自社の情報化投資の最適化を計るため ROI 計算ソフト(22%)、コスト管理ソフト(17%)が活用されている。

また、「IT Spending, Staffing & Technology Trends」によると、分野別で見ても新システムの開発に次ぎ、情報セキュリティへの投資も重視されている。

(B) 市場動向

日本のような行政、消費者を含む市場動向については、十分な情報が見当たらない。

なお、「IT Spending, Staffing & Technology Trends」によると、2006 年との比較でどのような業種での IT 市場の伸びが期待できるかの示唆が示されており、流通、ヘルスケア、公共、資源を中心に幅広い分野での伸びが期待されると考えられる。

(C) 政策動向

今回リストアップした各調査には、政府の IT 投資に影響を与える政策動向に関する質問項目、集計結果等は存在しなかった。

(D) 技術開発動向

今回入手できた統計情報は、情報システムを開発する事業者ではなく、ユーザー企業を対象としたものであるため、技術開発動向そのものに対する項目は盛り込まれていなかったが、企業側の関心という点から今後の注目動向が浮かび上がってきた。「2007 Enterprise Software Customer Survey」によると、今後の注目テーマは SOA が 23%で 1 位、続いて組み込みソフト、オープンソース等となっている。

(E) 企業意識 / 消費者意識

米国の関連調査は、読者を企業の CIO あるいはそれに近い IT 部門の管理責任者と想定していることもあり、企業意識についてはさまざまなものが含まれる一方、今回の調査対象では一般消費者に関するものは含まれていない。

「Managing IT Costs In a weakened Economy」によると、IT 部門の戦略上の目的には(企業全体としての)コスト削減に貢献することと売り上げ増に寄与することの 2 つが挙げられているが、特に後者についてはさらなる IT 投資が不可欠との認識が持たれている。また、アウトソーシングによるコスト削減の意欲も高い。なお、このアウトソーシングについては「State of the CIO」の 2006 年版でも米国企業の今後の意向として、アプリケーションの開発、保守を対象に米国内(57%)に次ぎインド(18%)を活用する意向の多さが目立っている。

「Software as a Service」では、いわゆる SaaS に対する企業側の関心や課題が整理されており、検討していない企業が 36%、導入中あるいは何らかの形で導入済みが 64%と高い一方、大規模な導入はまだ先のことで、データの安全性、SaaS と非 SaaS アプリケーションの統合、ROI の明確化等が今後の懸案事項であるとの声が寄せられている。

(F) 情報資産に関わる動向

情報資産についても、米国全体としてのマクロデータというより、企業の IT 部門としての情報資産管理に関する方針、見解がまとめられているのが特色である。

「Managing IT Costs In a weakened Economy」において、特に情報資産管理のコスト削減のために効果的な技術や手法について統計が取りまとめられており、仮想化技術(サーバ、ストレージ)やデータセンターの統合等への企業の積極的な取り組みが窺える。ガバナンス体制についても 6 割が自社の取り組みに満足している。

「50 Technologies」でも、情報資産関連での企業の取り組みでは、IT インフラの統合やレガシーシステムの見直しが課題として上位に挙げられている。というのも、ハードウェア・ソフトウェア支出で IT 全体費用の 4 割弱を占めるためである。

(3) 日米における収集データの特徴

IT化の進展に関するデータについて、日本では政府・公共機関が主体となって、統計基盤の整備という点で、幅広くデータを収集しているのに対して、米国では政府・公共機関が主体となってデータを収集しているものは少なく、民間調査企業を中心となってデータを収集しているものが多い。

このような収集主体の違いにより、日本ではデータ規模も比較的大きい。一例を挙げれば、「企業IT動向調査2007」では約8,000社へのアンケート調査を実施している。一方、米国ではデータ規模が比較的小さく、データの内容に関しても、マクロ動向よりも企業のIT部門の幹部あるいは政府関係者を対象とした意思決定に係るものが中心となっている。したがって日米ではデータ収集・提供の目的が大きく異なるため、データを比較・検証することは難しい。

しかし、企業のIT部門の幹部あるいは政府関係者を対象としたデータの活用という点を考えると、特定の目的に対して米国のデータは非常に有用と考えられる。即ち、ある時点における企業のIT投資判断(例:情報セキュリティ投資をどの程度重視しているか)やITインフラ整備の実情、IT投資を取り巻く環境といったメッセージが比較的分かりやすいためである。したがって米国の統計を活用する際には、マクロ動向の把握や数字の妥当性の検証よりも、経年でのトレンドや企業での実態把握といった点での利用が期待される。

4.2. 情報セキュリティ事象および対策等の実施状況に関するデータ

4.2.1. 国内の調査レポート

国内における情報セキュリティ事象および対策等の実施状況に関するデータでは、以下の6種類の報告書・調査レポートを対象に調査を行った。

本調査では、以下の報告書・調査レポートを対象としたが、この他に、IPA が定期的に発表している脆弱性やウイルス・不正アクセスに関する届出の受付・処理状況、日本ネットワークセキュリティ協会(JNSA)が実施している情報セキュリティインシデントに関する調査等も存在する。

(1) 情報処理実態調査（経済産業省）

IT の利活用の現状を把握するために実施している統計法に基づく承認統計であり、企業における情報セキュリティトラブル、対策状況、対策費用等について調査した報告書である。

更新頻度は年単位で、一次データである。

(2) 情報セキュリティに関する新たな脅威に対する意識調査（IPA）

PC からのインターネット利用者への Web アンケートを通して、新たな脅威に対する認知度、理解度、対策の実施状況等の実態を調査した報告書である。

更新頻度は年2回(2006年度)で、一次データである

(3) 国内におけるコンピュータ・ウイルス被害状況調査(国内調査)（IPA）

1年間における、ウイルスに感染または発見した状況、ウイルスの名称、種類数、ウイルス対策ソフトの導入状況、セキュリティパッチの適用状況、組織的な管理状況等を調査した報告書である。

更新頻度は年単位で、一次データである。

(4) 企業における情報セキュリティ事象被害額調査および国内における情報セキュリティ事象被害状況調査(IPA)

企業における情報セキュリティ事象被害額調査は、ウイルスや不正アクセス、情報漏えいといった情報セキュリティ事象が企業に与えるインパクトとして、被害額、被害率を調査し、被害額算出モデルを用いて復旧費用・逸失売上を推計・算出した報告書である。2005年に実施された単独調査であり、一次データである。

国内における情報セキュリティ事象被害状況調査は、最新の情報セキュリティ関連の被害実態および対策の実施状況を把握するため、企業・自治体を対象とし

て実施しているアンケート調査である。1989年から毎年1回実施されており、一次データである。

- (5) 2006年日本の情報セキュリティ管理におけるコンプライアンスの現状と課題(ガートナージャパン)

情報セキュリティ管理における対策、ポリシーの策定状況、管理における課題等について企業ユーザーの視点から定量的、定性的に調査分析したレポート。

単独での調査で、一次データである。

- (6) 「Japan Security and Continuity 2007」(関係資料) (インターナショナルデータコーポレーションジャパン株式会社)

インターナショナルデータコーポレーションジャパン株式会社(IDC)が主催するセミナーであり、IDCの海外、国内のアナリストと国内外のセキュリティに関するリーディングベンダーによる講演を通じて、セキュリティ分野の市場動向にあわせて、企業における脅威や対策の動向が紹介された。

更新頻度は年単位(2007年度は第2回目)で、一次データである。

4.2.2. 国内の調査レポートでの把握可能データ

国内の各報告書・調査レポートで把握可能なデータを、脅威・脆弱性に関わる動向、被害に関わる動向、対策・投資に関わる動向、に区分し、掲載状況や具体的なデータの種類、データの入手範囲を整理した。

(1) 調査レポートの対応分野

国内の情報セキュリティ事象および対策等の実施調査のうち被害に関する動向と対策・投資に関する動向は、取り上げている報告書・調査レポートが多く、経年データでの把握も可能である。

一方、脅威・脆弱性に関する動向は、今回対象とした調査レポートにおいては、一部のレポートでのみ経年データの把握が可能となっている。

調査レポート	調査項目		
	脅威・脆弱性に関わる動向	被害に関わる動向	対策・投資に関わる動向
情報処理実態調査			
情報セキュリティに関する新たな脅威に対する意識調査			
国内におけるコンピュータウイルス被害状況調査(国内調査)			
企業における情報セキュリティ事象被害額調査(被害額調査)			
2006年日本の情報セキュリティ管理におけるコンプライアンスの現状と課題			
「Japan Security and Continuity 2007」関係資料			

* :該当データが掲載されており、経年データ(5年間程度)の取得が可能
 :該当データが掲載されており、単年データの取得が可能
 :該当データに類するデータのみ取得が可能

図表 4-4 調査レポートの対応分野一覧(国内、情報セキュリティ)

(2) 把握可能データ的具体例

調査対象とした情報セキュリティ分析事象および対策等の実施状況に関する報告書・調査レポートにおいて、把握可能なデータの種別を例示する。

調査項目	具体的に把握可能なデータ(一例)
脅威・脆弱性に関わる動向	<ul style="list-style-type: none"> 情報セキュリティに関する言葉の認知度(情報セキュリティに関する新たな脅威に対する意識調査) スパイウェアの被害の有無(国内におけるコンピュータウイルス被害状況調査) スパイウェア対策ツールの有無(国内におけるコンピュータウイルス被害状況調査)
被害に関わる動向	<ul style="list-style-type: none"> 情報セキュリティトラブルの経験の状況(情報処理実態調査) 遭遇したウイルスの種類数(国内におけるコンピュータウイルス被害状況調査) 遭遇したウイルスの名称(国内におけるコンピュータウイルス被害状況調査) 情報セキュリティに関する被害経験、被害時の対処方法(情報セキュリティに関する新たな脅威に対する意識調査)
対策・投資に関わる動向	<ul style="list-style-type: none"> 情報セキュリティの対策状況(情報処理実態調査) 情報セキュリティ対策費用(情報処理実態調査) 情報セキュリティに関する最新情報や対策情報の収集状況(情報セキュリティに関する新たな脅威に対する意識調査)

図表 4-5 把握可能データの例(国内、情報セキュリティ関連)

(3) 各データから得られる特色

(A) 脅威・脆弱性に関する動向

「情報セキュリティに関する新たな脅威に対する意識調査」によると、2006年11月調査におけるインターネット利用者の情報セキュリティに関する言葉の認知度は、「コンピュータ・ウイルス」が98.7%と最も高く、「ファームウェア」が10.3%で最も低いという結果となった。前回調査(2006年2月)と比較すると、セキュリティホールの認知度が10%以上の上昇となっている。

一方で、情報セキュリティに関する事象の理解度をみると、事象を完全に理解している利用者の比率は、コンピュータ・ウイルスやスパイウェアがそれぞれ63.8%と52.5%で5割を超えているが、その他の事象では、言葉の理解や事象の認知にとどまっておき、特徴や問題点の理解には至っていないことがわかる。刻一刻と変化する脅威から利用者を保護し、適切なセキュリティ対策を促すためにも、新たな情報提供手段の確保等の認知度向上策が必要なものと考えられる。

「国内におけるコンピュータ・ウイルス被害状況調査」によると、2006年に新たな脅威として認識されはじめたスパイウェアについては、既に31.4%の企業が「スパイウェアの侵入を受けた・実行された」または「スパイウェアを発見したが侵入や実行にいたらなかった」と回答している。一方で、対策

については 32.5%の企業が対策ソフトを導入しておらず、「専用ツールを導入している」企業は 6.2%にとどまっている。今後、スパイウェアの脅威が広まるにつれ、ツールの導入が進んでいくものと想定される。

(B) 被害に関する動向

「平成 17 年度情報処理実態調査」によると、平成 16 年度における情報セキュリティトラブルの経験状況については、「コンピュータ・ウイルスに関するトラブル」、特に「ウイルスやワームによるトラブル」を経験した企業が 81.2%と最も多く、次いで「システムに関するトラブル」の 39.7%となっている。前年比で見ると「ノートパソコンおよび携帯記憶媒体等の盗難紛失による重要情報の漏洩」が 19.2%と大きく増加しており、ネットワーク経由等の技術的な面に加え、人間の活動に基づいた事故が原因となるケースが増加していることが窺える。

「国内におけるコンピュータ・ウイルス被害状況調査」によると、2005 年において、企業が遭遇したウイルスの種類数は、「5 種類以上」が 42.2%と最も多く、次いで、1 種類の 23.3%となっている。2001 年からの経年で見ると「5 種類以上」の比率が徐々に上昇しており、コンピュータ・ウイルスの脅威が拡大していることがわかる。

また、遭遇したウイルスの種類としては、「W32/Netsky」「W32/Klez」「W32/Mydoom」が上位 3 となっており、メールの添付ファイルを介して感染を拡大するウイルスが大半を占めている。

「情報セキュリティに関する新たな脅威に対する意識調査」によると、2006 年 11 月調査におけるインターネット利用者の情報セキュリティに関する被害経験としては、「ウイルス感染」の経験が 41.1%と最も多く、次いで「パソコン起動以上やシステムの不備」が 33.9%と続いている。前回調査（2006 年 2 月）と比較すると、全ての被害について経験率が上昇しており、特に「パソコン起動以上やシステムの不備」の上昇が著しい。

また、被害時の対処方法としては、「自力で対処」「家族や知人に相談」がそれぞれ 52.1%、27.9%と上位を占めており、パソコンメーカーやセキュリティ対策ソフトメーカー等の専門組織に協力を求めるユーザーは少ない。

(C) 対策・投資に関する動向

「平成 17 年度情報処理実態調査」によると、平成 16 年度における情報セキュリティトラブルの対策の実施状況としては、「既に対策している」または「実施を検討している」と回答した企業の比率が、すべての対策項目について前年比で上昇している。特に「セキュリティポリシー」に関連する対

策や「責任・教育体制」に関する対策についての増加率が高くなっており、個人情報保護法の施行を前に、組織的な対策の意識が高まっていたことが想定される。

また、情報セキュリティ対策において、外部を活用している企業の比率は 57.6%となっている。この比率は資本規模が大きくなるほど上昇しており、資金が豊富な企業ほど積極的に外部を活用する傾向にあると言える。この内訳を見ると、防衛措置が54.0%と半数を占めており、監視体制や教育等の組織面での活用よりも、社員用 IC カードや防衛措置等の物理面での活用が中心となっていることが窺える。

「情報セキュリティに関する新たな脅威に対する意識調査」によると、2006 年 11 月調査における、インターネット利用者の情報セキュリティに関する最新情報や対策情報の収集状況については、「収集を行っている」と回答した利用者の比率は 40.3%となっており、半数にも満たない。また、その入手経路としては、「セキュリティ対策ソフトメーカーの Web サイト、メールリスト等」「パソコンメーカー、プロバイダ等の Web サイト、メールリスト等」の利用者がそれぞれ 64.7%、54.1%となっている。

4.2.3. 米国の調査レポート

米国における情報セキュリティ事象および対策等の実施状況に関するデータでは、以下の 33 種類の報告書・調査レポートを対象に調査を行った。

- (1) Information Security Awareness Report (SecureInfo Corp.)
連邦政府職員の法律「Federal Information Security Management Act (FISMA)」に対する認知、態度、対応に関する調査レポートである。
単独での調査である。
- (2) Datagate: The Next Inevitable Corporate Disaster? (McAfee Corp. and Datamonitor)
欧米大企業における、データ遺漏に関する認識、発生頻度、予防措置に関する調査レポートである。
単独での調査である。
- (3) Internet Security Threat Report, June, 2006 – December, 2006 (Symantec)
脆弱性、攻撃に関するグローバルな傾向分析(6 ヶ月間調査)を行った調査レポートである。
更新頻度は半年単位である。
- (4) 2006 Annual Study: Cost of a Data Breach (Ponemon Institute, Vontu Corp. and PGP Corp.)
データ遺漏の被害を受けた 31 組織の被害額や予防措置に関する調査レポートである。
単独での調査である。
- (5) 2007 Annual Study: U.S. Encryption Trends Study (Ponemon Institute and PGP Corp.)
暗号化(encryption)のための要因、戦略、技術に関する米国企業の調査レポートである。2007年の調査は、2006年のデータ遺漏調査のフォローアップとして実施された。
単独での調査である。

- (6) 2007 North American Virtual Criminology Report (McAfee Corp.)
近年のサイバー犯罪の分析(犯罪者とそのツールに関する議論を含む)に関する調査レポートである。法執行部門と企業による対応の意味についても議論されている。
更新頻度は年単位である。
- (7) Data Loss Prevention and Endpoint Security (Vontu Corp. and Forrester Consulting)
北米企業のデータ紛失や末端のセキュリティへの認識、脅威、対応の状況に関する調査レポートである。
単独での調査である。
- (8) Global Information Security Survey 2006 (Ernst and Young)
情報セキュリティを実施するにあたっての要因、投資、ガバナンスに関する企業調査レポートである。
更新頻度は年単位である。
- (9) Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior (Cisco Systems and Insight Express)
リモートで働く人を対象とし、情報セキュリティの脅威に関する認識度や情報セキュリティに影響を及ぼしうる行為について評価した調査レポートである。
単独での調査である。
- (10) National Survey on the Detection and Prevention of Data Breaches (Websense and Ponemon Institute)
データ遺漏に対する認知、脅威、反応、予防に関する調査レポートである。データ遺漏を防止するためのIT投資やセキュリティ面での取り組みに関する議論も含まれている。
単独での調査である。

(11) 2006 CSI/FBI Computer Crime and Security Survey (Computer Security Institute and the Federal Bureau of Investigations (FBI))

国内の官民組織を対象とした調査レポートである。被害を受けたコンピュータのセキュリティインシデントとその要因、情報セキュリティ戦略の予算、予防措置等についての内容が盛り込まれている。

更新頻度は年単位である。

(12) FBI Computer Crime Survey (FBI)

サイバー犯罪の事件と法執行部門への報告内容についての調査レポートである。FBIでは、毎年の調査(CSI/FBI Computer Crime and Security Survey)も同時に行っている。本調査は1回限りの調査で、2,000人の個人を対象に行ったものである(CSI/FBI surveyの約4倍の規模)。

単独での調査である。

(13) Enterprise Security Survey (Apani Networks)

特にネットワークセキュリティを中心とする、脅威、セキュリティ戦略についての調査レポートである。多様なユーザーへのアクセスを与えつつ、アクセスコントロールを維持するという課題にフォーカスを当てている。

更新頻度は年単位である。

(14) 2006 Technology, Media, and Telecommunications Security Survey (Deloitte Touche Tohmatsu)

IT、メディア、通信部門での国際企業を対象にし、企業のセキュリティ脅威、インシデント、セキュリティ戦略、予算、技術を調査したレポートである。また、米、日、EUにおける情報セキュリティ関係の規制の及ぼす影響についても議論を実施している。

更新頻度は年単位である。

(15) Security Trends Report, 2Q07 (Websense)

情報セキュリティ面での脅威に関して、四半期毎に分析した調査レポートである。

更新頻度は四半期単位である。

(16) Information Security Awareness Survey (Business Software Alliance and Forrester Consulting)

情報セキュリティの要因(drivers)、内部サポート、連邦政府の法律や施策への見解に関する調査レポートである。

単独での調査である。

(17) Insider Threat Study: Computer Sabotage in the Critical Infrastructure Sectors (U.S. Secret Service and CERT Coordination Center)

内部関係者によって引き起こされたサイバーセキュリティアタックに関する調査レポートである。金融部門(レポート1)、重要インフラ(レポート2)の企業をケーススタディとして調査した結果が含まれている。

単独での調査である。

(18) Top 20 Internet Security Attack Targets (SANS Institute and FBI)

情報セキュリティのエキスパートの合意による、最も危機的な脆弱性に関する調査レポートである。脆弱性に加え、救済のあり方に関する助言も含まれている。

更新頻度は年単位である。

(19) E-Crime Watch Survey 2006 (Computer Security Online, US Secret Service, CERT Coordination Center, and Microsoft Corp.)

企業のセキュリティ部門の幹部と法執行関係者を対象とする、情報セキュリティ上の脅威、インシデント、戦略、予算、技術に関する調査レポートである。

更新頻度は年単位である。

(20) Global Information Security Survey (InformationWeek and Accenture)

米国と中国の組織を対象としたもので、幅広い情報セキュリティを取り扱っている調査レポートである。トピックとしては脅威、インシデント、戦略、予算および技術等を取り扱っている。

更新頻度は年単位である。

(2 1) Information Security: A CompTIA Analysis of IT Security and the Workforce
(CompTIA and TNS Prognostics)

情報セキュリティの脅威、インシデント、予算、トレーニングに関する調査レポートである。主なポイントは、インシデントにおいて人間のミスが及ぼした影響とセキュリティのトレーニングの重要性等を取り扱っている(なお、調査レポート本体はCompTIAのメンバーのみが入手可能であり、本記述はサマリーに記載されている内容に基づくものである)。

単独での調査である。

(2 2) Committing to Security: Fourth Annual Benchmark Survey (CompTIA and TNS Prognostics)

情報セキュリティ、特に研修と認定に関する調査レポートである。インシデント、セキュリティポリシー、情報セキュリティのアウトソーシング、研修・認定の有効性に関する質問が盛り込まれている(なお、調査レポート本体はCompTIAのメンバーのみが入手可能であり、本記述はサマリーに記載されている内容に基づくものである)。

更新頻度は年単位である。

(2 3) The Global State of Information Security 2006 (CIO Magazine, Computer Security Online, and Pricewaterhouse Coopers)

情報セキュリティ部門の官民の幹部を対象とし、情報セキュリティの戦略や予算に関するグローバルの調査レポートである。本調査レポートには、情報セキュリティ関係の規制の遵守の役割に関する簡単な議論が含まれている。

更新頻度は年単位である。

(2 4) State of Internet Security: Protecting Enterprise Systems (Webroot Software)

情報セキュリティのインシデント、法律、ポリシー、技術に関するグローバルの調査レポートである。

単独での調査である。

(25) IT Risk Management Report (Symantec)

IT リスクマネジメントの傾向に関する調査レポートである。世界の IT およびビジネス分野の専門家に対するインタビューによる内容が盛り込まれている。リスクの種類、リスクマネジメントポリシー、リスクの技術・プロセス面でのコントロール等が議論されている。

更新頻度は年単位である。

(26) 2006 Global Security Survey (Deloitte Touche Tohmatsu's Global Financial Services Institutions Group)

主要金融機関の IT 関連幹部に対するグローバルな調査レポートである。情報セキュリティ上の脅威、戦略、予算、技術等をカバーしている。

更新頻度は年単位である。

(27) Network Attacks: Analysis of Dept. of Justice Prosecutions from 1999 2006 (Phoenix Technologies and Trusted Strategies)

米国司法省によりサイバー犯罪として訴追を受けた案件を対象し、サイバー犯罪の原因とコストについて整理した調査レポートである。

単独での調査である。

(28) Cost of Spam (Ferris Research)

スパムのコスト、ビジネスでの電子メールの利用者数、最もよく使われているメールのプラットフォーム、電子メールのセキュリティ市場規模等に関する議論が盛り込まれている。

更新頻度は不定期である。

(29) Digital Confidence Index (Computer Security Industry Association)

インターネットのセキュリティ、現行法の適正性、オンライン取引の利用意向に関する市民の動向を調査したレポートである。

更新頻度は半年単位である。

(3 0) 2007 Consumer Survey on Data Security (Ponemon Institute and Vontu Corp.)

個人情報セキュリティ、最も情報保護への関心が高い情報カテゴリー、個人の機密情報を最も保護するのはどのような組織かといったことに関する市民の意向を調査したレポートである。

単独での調査である。

(3 1) Online Fraud Report (National Cyber Security Alliance and Bank of America)

オンライン取引を行った人数、個人情報安全性に関する個人の見解、個人情報を保護するための技術や対応に関する人々の知識等を調査したレポートである。

単独での調査である。

(3 2) Internet Fraud Survey Report (Javelin Research)

インターネット上の詐欺、犯罪の方法、犯罪防止のための手段等について調査したレポートである。

単独での調査である。

(3 3) Internet Crime Report (Internet Crime Complaint Center (IC3))

IC3 に対するサイバー犯罪の報告の数と種別、被害の種類、犯罪者の種類、IC3 が取った対応等について整理した調査レポートである。

更新頻度は年単位である。

4.2.4. 米国の調査レポートでの把握可能データ

脅威・脆弱性に関する動向、被害に関する動向、対策・投資に関する動向に区分し、各データの掲載状況やデータの遡及入手範囲を整理した。

(1) 調査レポートの対応分野

全ての動向について、掲載されている報告書・調査レポートは多いものの、経年データでの把握が可能な報告書・調査レポートは一部に限られる。

調査レポート	調査項目		
	脅威・脆弱性に関わる動向	被害に関わる動向	対策・投資に関わる動向
Information Security Awareness Report			
Datagate: The Next Inevitable Corporate Disaster?			
Internet Security Threat Report, June, 2006 – December, 2006			
2006 Annual Study: Cost of a Data Breach			
2007 Annual Study: U.S. Encryption Trends Study			
2007 North American Virtual Criminology Report			
Data Loss Prevention and Endpoint Security			
Global Information Security Survey 2006			
Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior			
National Survey on the Detection and Prevention of Data Breaches			
2006 CSI/FBI Computer Crime and Security Survey			
FBI Computer Crime Survey			
Enterprise Security Survey			
2006 Technology, Media, and Telecommunications Security Survey			
Security Trends Report, 2Q07			
Information Security Awareness Survey			

* :該当データが掲載されており、経年データ(5年間程度)の取得が可能
:該当データが掲載されており、単年データの取得が可能
:該当データに類するデータのみ取得が可能

図表 4-6 調査レポートの対応分野一覧(米国、情報セキュリティ)

調査レポート	調査項目		
	脅威・脆弱性に関わる動向	被害に関わる動向	対策・投資に関わる動向
Insider Threat Study: Computer Sabotage in the Critical Infrastructure Sectors			
Top 20 Internet Security Attack Targets			
E-Crime Watch Survey 2006			
Global Information Security Survey			
Information Security: A CompTIA Analysis of IT Security and the Workforce			
Committing to Security: Fourth Annual Benchmark Survey			
The Global State of Information Security 2006			
State of Internet Security: Protecting Enterprise Systems			
IT Risk Management Report			
2006 Global Security Survey			
Network Attacks: Analysis of Dept. of Justice Prosecutions from 1999 – 2006			
Cost of Spam			
Digital Confidence Index			
2007 Consumer Survey on Data Security			
Online Fraud Report			
Internet Fraud Survey Report			
Internet Crime Report			

* : 該当データが掲載されており、経年データ(5年間程度)の取得が可能
: 該当データが掲載されており、単年データの取得が可能
: 該当データに類するデータのみ取得が可能

図表 4-7 調査レポートの対応分野一覧(米国、情報セキュリティ)

(2) 各データから得られる特色

米国の情報セキュリティ事象および対策等の実施状況に関するデータのうち、規模、内容等の面で特に鍵となる「Internet Crime Report」(IC3)、「CSI Survey 2007」(CSI)、「2006 Global Information Security Survey」(Ernst & Young)および「Enterprise Security Survey」(Apani)を対象としてポイントを整理した。

いずれも、各企業のCIO等の情報システム責任者を対象読者として想定し、単にデータを提供するのではなく、情報セキュリティ対策の必要性、緊急性を強く訴える内容のものとなっている。

(A) 脅威・脆弱性に関する動向

一般企業にとって、脅威や脆弱性に関する最新の情報を独力で入手し、対応策を講じるのは容易ではない。こうした前提の下、「CSI Survey 2007」では情報共有組織に所属しているかどうかをアンケートで尋ねているが、調査結果によるとInfragard(各地のFBIフィールドオフィスが、その地域の民間セクターと協力してサイバー犯罪に取り組むための、官民セクターのパートナーシップの全国ネットワーク。メンバー同士が認知したサイバー犯罪に関する情報を定期的に共有)に所属している回答者が34%、ISACが17%、その他が22%であるが、どこにも所属していないとする企業も50%にのぼる。

他方、脅威や脆弱性の把握だけでは個別の企業の潜在的リスクに対応することが難しくなっているのも事実である。「Internet Crime Report」でもリストアップされているオークション詐欺のような事象への対策をとるのは、技術的対応だけでは難しい。

なお、企業側の今後の懸念については、「Enterprise Security Survey」によると、データの盗難が最も大きな課題となっており、続いて、「ワームやウイルス」「アプリケーションの脆弱性」「内部からのアタック」の順となっている。

(B) 被害に関する動向

「Enterprise Security Survey」によると、前年に受けた内部からのアタックの数は0件とした回答者が62%であるものの、5回以上攻撃を受けたとする企業も12%にのぼっており、データの盗難も25%の企業が経験している。また、「Internet Crime Report」によると、政府当局(IP3)へのインターネット犯罪の報告数も増加を続けている。

アタックの種別については、「CSI Survey 2007」では、アタックで最も多かったのは、社内からのネットアクセスによる攻撃で59%、次いでウイル

スが 52%、端末盗難が 50%となっている。

なお、情報セキュリティの被害の近年の特色は、経済的な被害額が急激に大きくなっており、攻撃側も情報システムのみならず事業そのものにダメージを与えようとしていることである。

「CSI Survey 2007」による企業の被害金額ではその傾向が特に顕著であり、同調査では 1 企業当たり被害額は 35 万 424 ドルと前年に比べ 16 万 8,000 ドルも増えており、経済的ダメージが大きくなっていることが確認された。

また、ターゲット型の攻撃が増えた結果、アンケート実施者が正確な被害の規模や内容を把握するのが一層難しくなっている。

(C) 対策・投資に関する動向

セキュリティポリシー策定や内部監査体制等については、「Enterprise Security Survey」で 72%の企業が策定済みと回答しており、一定程度の取り組みが進んでいることが窺える。こうした取り組みの背景としては、「2006 Global Information Security Survey」によるとデータ保護のニーズ以上にコンプライアンスという一面もあるようだ。

BCP を全社で策定する際にも情報セキュリティは重要要素となっている。「2006 Global Information Security Survey」によると BCP 策定時に 75%の企業が IT リスクを管理対象としている。

対 IT 予算総額でみたセキュリティ関係の投資額は「CSI Survey 2007」で取りまとめられており、全体の 3～5%とした回答が最も多く 26%、1～2%が 23%となっている。

具体的にどのようなツールを用いて対策を講じているかについては、「CSI Survey 2007」によると、アンチウイルスソフトは 98%、ファイアウォールは 97%で、外部からのアクセスでも VPN の活用は 84%と高い比率となっている。一方、スマートカードや PKI、ワンタイムパスワード・トークンといったものについては利用率が 50%を割っており今後の課題となっている。

さらに、「Enterprise Security Survey」では、社内ネットワークやアプリケーションへのアクセス時に複数のセキュリティツール(スマートカードやデバイス)を組み合わせている比率について、「20%を超えている」との回答はわずか 22%に過ぎないことがわかった。また「CSI Survey 2007」でも、社内のトレーニングへの投資比率について、「セキュリティ投資全体の 1%未満」との回答が 48%となっており、今後は改善が求められると考えられる。

IT 部門としては情報セキュリティのリスク対策を企業全体のリスク対策

にさらに組み込んでほしいというニーズが高く、「2006 Global Information Security Survey」では半数以上がその必要性を指摘している。

(3) 日米における収集データの特徴

情報セキュリティ事象および対策等の実施状況に関するデータについてもIT化の進展と同様の傾向がみてとれる。

日本では、政府・公共機関が主体となって、統計基盤の整備という点で調査が行われており、経済産業省の「情報処理実態調査」(約 4,200 社)やIPAの「情報セキュリティに関する新たな脅威に対する意識調査」(約 5,300 人)等、調査規模が大きなレポートも存在する。

米国では民間企業が調査の主体となっており調査規模も小さいものが多いが、情報セキュリティについては、「Internet Crime Report」、「CSI Survey 2007」、「2006 Global Information Security Survey」および「Enterprise Security Survey」をはじめ比較的整備されたものも存在する。

他方、両者に共通的な特徴としては、情報セキュリティ分野では、時間がたつごとにアタックの目的や被害内容・種別が変化していくことが予想されるが、これらの状況についても調査項目にタイムリーに反映されているレポートが多い点である。

上記の理由により、継続性が確保されていないデータが多いことから、個別事象の経年変化等の統計的な分析に使用するのは困難であるが、脅威や脆弱性の動向、情報セキュリティ上の経済的な被害額のトレンド、企業側の取り組み状況等、特定の実施項目に着目して把握するうえではある程度の基盤が整備されている。

5. 情報セキュリティ分析手法

情報セキュリティ分析手法の現状動向を把握し、定量的な分析手法や定性的な分析手法がどのようなケースで活用されているのかを把握するため、有識者へインタビューを実施し、有識者の見解や近年のトレンドを整理した。

5.1. 有識者インタビュー調査

5.1.1. 調査概要

情報セキュリティの分析手法について、学際的な場での実績を有しており、新たな分析手法の開発も行っている有識者に対して、インタビュー調査を実施した。

(1) 有識者の概要

本インタビュー調査の対象とした有識者について、所属組織、主な研究テーマ等の概要を示す。

(A) 松浦 幹太

所属組織

- 東京大学 生産技術研究所 准教授

ホームページ

- http://kmlab.iis.u-tokyo.ac.jp/index_j.html

個人・研究室の研究テーマ

- 暗号技術とその応用
(属性ベース暗号、電子証拠物、高機能署名 等)
- ネットワークセキュリティ
(迷惑メール対策、不正者追跡、サービス妨害対策 等)
- セキュリティマネジメント
(IT プロジェクトマネジメント、IT 投資評価、経済学的リスク管理 等)

リスク定量化ワークショップにおけるテーマ

- 題名:
情報セキュリティ分野におけるリスク定量化とその応用に関する研究動向
- 概要:
情報セキュリティ分野におけるリスク定量化に関する研究について、情報セキュリティ研究対象と定量化の適用範囲、研究具体例、定量化研究における課題等についての国際的動向をまとめた研究

(B) 田中 秀幸

所属組織

- 東京大学大学院 情報学環・学際情報学府 准教授

所在地

- 東京都文京区本郷 7-3-1 東京大学大学院 情報学環・学際情報学府
田中秀幸研究室

ホームページ URL

- <http://h-tanaka.iii.u-tokyo.ac.jp/>

個人・研究室のテーマ

- 情報セキュリティ投資の経済分析
- 先端産業のイノベーションと中間組織の機能
- 電子自治体等の地域情報化
- 情報セキュリティ研究については、情報科学分野との共同研究による実証分析を中心に実施している

リスク定量化ワークショップにおけるテーマ

- 題名：
情報セキュリティ対策と企業価値
- 概要：
情報セキュリティ対策が企業価値の向上に結びつくかどうかについて、日本企業を対象とした定量的なデータに基づき、実証的に明らかにすることを目的とした研究

(2) 調査項目

本インタビュー調査では、経済・金融・社会等の視点から情報セキュリティ分析を行う際の示唆、およびそのような分析を情報分析ラボで実施する際の期待等について、有識者の見解を調査した。

(A) 経済・金融・社会等の視点からの分析可能性

分析の有用性

分析の方法(定量分析)

分析の方法(定性分析)

(B) 情報分析ラボへの期待

組織のあり方

期待する収集・分析・提供機能

(C) 情報セキュリティ分析時の留意点

分析に活用可能な統計データ

5.1.2. 調査結果

情報セキュリティ分析手法に関する有識者の見解を踏まえて、情報分析ラボにおける今後のあり方や分析方針に資するポイントを整理した。

(1) 経済・金融・社会等の視点からの分析可能性

(A) 分析の有用性

- 情報セキュリティの技術面だけでなく、経済的な動機付けや社会制度との関連を考えて行くことは非常に有用である
- 実際に分析を行う際には、「確立された科学的アプローチ(研究手法)を活用した分析」と「公的機関の立場・規模・強制力があればこそ可能な実務上の調査・分析」の2つのアプローチ方法が考えられる

(B) 分析の方法(定量分析)

- 情報セキュリティの定量分析は、IT投資額(情報セキュリティ投資額)を分析対象としたものが現状では主流である
- 日本については情報処理実態調査で情報セキュリティ投資額が把握できるため、諸外国よりも定量データの整備が進んでいる
- 確立された科学的アプローチを活用した分析としては、次の3つのアプローチが主なものとして想定される
 - 文献計量分析:
文献による情報セキュリティ関連組織の連携状況分析等
 - 計量経済分析:
経済的な事象と情報セキュリティとの間の因果関係分析等
 - 金融工学的アプローチ:
デリバティブの価格プロセスを観測することによる情報セキュリティのリスク尺度分析等

(C) 分析の方法(定性分析)

- 災害対策やBCPの観点で情報セキュリティ対策のベストプラクティスをモデル化する分析は既に行われている
- IT投資全体の中で、情報セキュリティ対策をどのように位置づけるか(目的、効果等)を定性分析することは有用である
- 定性分析はセカンダリアプローチであり、数字による説得力のある定量分析をプライマリアプローチとして、分析を実施するべきである

(2) 情報セキュリティ分析ラボラトリーへの期待

(A) 組織のあり方

- IPA(情報分析ラボ)で分析データの基盤を固め、そこに有識者がテーマに応じて参画する形で分析の充実化を図る体制を期待する
- 情報分析ラボが直に分析に用いる情報を収集するのはリソース的に困難である(経済分野の論文等は特殊なルートでしか入手できない)ため、他の研究・分析組織と連携し、学術研究グループとして情報分析ラボを育てて行くことに期待する

(B) 期待する収集・分析・提供機能

- 情報セキュリティ対策の実施有無だけでなく、投資額まで入手できれば分析の幅が広がるため、IPAの収集力に期待する
- 情報セキュリティ対策は、長期的に見れば企業価値を上げる施策であることを、経営層に情報提供することは有用である
- 近年の研究では地域による情報セキュリティ対策の差異が認められており、政策提言として情報提供することは有用である

(3) 情報セキュリティ分析時の留意点

(A) 分析に活用可能な統計データ

- 情報処理実態調査の個票は分析データとして有用である
- ただし、情報セキュリティ関連の設問は今後の拡充が必要である
- IPAが実施しているインシデントに関する調査は規模が大きく、情報セキュリティ分析への活用も検討すべきである
- 警察庁や総務省等が実施している情報セキュリティ関連の調査データ(個票)を共有できると、深堀分析が可能になる

5.2. 統計データの入手方法

5.2.1. 政府の統計調査

総務大臣の承認が必要な統計調査(指定統計・承認統計・届出統計)に関して、個票データの入手可否に関する現状、および情報分析ラボによる入手可能性を整理した。

(1) 個票データの入手可否

個票データの入手可否は、各統計情報を実施している部局の判断にもよるが、情報分析ラボのような立場を勘案すると、比較的入手が容易であると考えられる。

- 入手の可否は、各統計調査を実施している部局単位で確認が必要であり、利用主体や利用目的等を勘案して判断がなされている
 - 例示：
「情報処理実態調査」の個票データは、調査主体である経済産業省 商務情報政策局 情報経済課の判断によって入手の可否が決定される。
- 指定統計の場合、データの厳秘性が高い(公益性の高い統計調査では回答者に回答義務が発生する)ため、個票データの入手は難しい
- 承認統計・届出統計の場合、データの厳秘性が指定統計ほどではない(回答者は任意の判断で回答)ため、個票データの入手はそれほど難しくはない
- いずれの統計に関しても、単なる興味や、個別の企業活動に利用する場合には、入手はまず不可能である
- 逆に、公共用途で行われる事務・業務の一環(情報分析ラボのような立場)として利用する場合には、各部局の判断にもよるが、入手は容易となると考えられる

(2) 個票データの整備状況

- 2007年5月に統計法が改正され、2009年春に新統計法が施行予定
- 旧統計法では、企業情報・個人情報をもスキングした個票データの整備が統一化されておらず、各部局の判断に委ねられていた
- 新統計法では、企業情報・個人情報をもスキングした個票データの整備が統一化され、開示請求への対応に備えて行く予定

5.2.2. 民間の統計調査

民間企業・法人団体が独自に実施・編纂している統計調査・レポートに関して、個票データの入手可否に関する現状、および情報分析ラボの入手可能性を整理した。

(1) 個票データの入手可否

(A) 社団法人情報システム・ユーザー協会

取り扱っている主な統計調査・レポート名

- 企業IT動向調査

各社の見解

- アンケート実施時に利用目的を本調査に限定しているため、他の機関への個票の提供は難しい
 - 業界によりサンプル数が数社程度のものもあるため、仮に個票データを提供できたとしても、有効な分析結果が得られるとは限らない
 - 調査内容や調査設計に関する意見交換については、対応が可能

(B) 株式会社インプレス R&D

取り扱っている主な統計調査・レポート名

- インターネット白書
- ケータイ白書
- インターネット利用動向調査報告書(企業編 / 個人編)
- 企業システム担当者意識動向調査報告書

各社の見解

- 同社の発行する白書やインターネット利用動向調査報告書に掲載されているデータは、毎年独自に実施している利用動向調査の結果をベースとしており、調査結果のローデータの販売も行っている
 - インターネット白書に掲載している企業動向調査のローデータの場合で 150 万円(章、節単位での販売も可能)
 - 2006 年度の企業動向調査では有効回答数が約 1500 サンプル

(C) 株式会社シーメディア

取り扱っている主な統計調査・レポート名

- 電子決済総覧
- ICカード総覧

各社の見解

- 消費者を対象としている総覧ではないためアンケート調査は行っていないが、電子決済の技術動向等定性情報についての意見交換やデータ提供は可能である
 - 独自のヒアリング調査により個別企業の動向等のデータを収集しているが、整理して保管しているわけでないため、即座に提供することは難しい
 - 提供時の条件(出展の要否、作業費用)については、ケースバイケースで対応が可能である

5.3. 情報セキュリティ分析手法のトレンド

5.3.1. 有識者における研究トレンド

情報セキュリティの分析手法のトレンドについて、有識者インタビュー調査の対象である松浦准教授の研究テーマ(発表論文)を整理した。

(1) 松浦准教授の研究テーマ

情報セキュリティ分析について、暗号・ネットワーク・マネジメントのすべてのアプローチで研究をしている松浦准教授が、経済・金融・社会等の視点から研究しているテーマの論文をいくつか抜粋して整理した。

(A) Public Acceptance Issues Surrounding the Implementation of New Election Technology for Philippines

- フィリピンでは海外在住者の在外投票プロセスの最新化が課題となっており、それに対する一つの対応策として、本人確認時のバイオメトリクスの活用がある
- 本報告は、フィリピンにおけるバイオメトリクスを中心とするITを活用した本人確認の(実証実験含む)歴史を整理し、(特に在外投票での)必要性和、実用化へ向けて解決すべき課題を明らかにしている(定性調査)
- 性急な導入は裁判所にて却下されたものの、フィリピン政府は、革新的な在外投票システム整備に係る調査分析結果を国会報告に盛り込む等、積極的に検討を進めている

(B) University Industry Collaboration Networks in the Information Security Field In Japan: Problems and a Particular Success

- 日本における産学の連携が情報セキュリティ分野で十分に進んでいるかどうかについて調査したもの
- 調査は、日本における特許出願情報分析や、当該分野の論文における共著パターンに着目した文献計量分析のアプローチによって行われた。今後の情報セキュリティ分野におけるイノベーション基盤を活性化するための課題として、他の分野と比較した相対的な意味で、大学と産業界をつなぐリサーチのネットワークをより充実させることを挙げている(定量調査)

(C) A Derivative of Digital Objects and Estimation of Default Risks in Electric

Commerce

- オンライン上でのデジタル取引が持つ価値は、(取引される)額面の価格以外にもさまざまなバリューを持つ場合がある(例えば、デジタルイメージの著作権やサービス品質といったもの)
- 本論文は、そうした付加価値の損失リスクをコントロールするために、金融工学でも用いられている「デリバティブ」をあてはめたモデルを検討している(定量調査)

(D) Cross Sector Collaboration in Japanese Information-Security Industry and the Shock of Personal Information Protection Laws

- 上記(B)の報告の続編に当たるもので、個人情報保護法完全施行に沿って関連する論文を対象に追加の分析を行ったもの
- 2005年の1月以降の動きを見ると、情報セキュリティに係る論文、レポートの数が急激に増加していることが分かった(産学連携の比率に大きな変化はないが数は増えている)著者は、こうした個人情報保護法をきっかけとする研究の高まりは、産学連携にプラスをもたらすと期待している(定量調査)

(E) Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms

- 経済産業省の承認統計「情報処理実態調査」のデータを利用し、情報セキュリティ面での脆弱性を定量的に把握する技法を示し、その技法を情報セキュリティ実施効果の実証分析に応用したもの
- 分析結果によると、脆弱性の代理変数として電子メールのアカウント数を用いれば、最新の最適投資モデルに対する一定の実証サポートを得られることが示された。また、同様の技法を応用し、セキュリティ投資の相補性(対策技術の導入、セキュリティポリシーの策定、人員教育のすべてに取り組まなければ有効でないこと)と、セキュリティ投資を継続させることの有効性を実証することができた(定量調査)
- いくつかの会議発表成果を、論文誌の正論文として発展的にまとめたものである

- (F) Risk Assessment Model using Threat Probability depending on Classified Information Security Measures
(分析された情報セキュリティ対策に依存する脅威発生率を導入したリスクアセスメントモデル)
- リスクアセスメントに用いられる脅威発生率は、投資によって変化し、最適投資に影響を与える。本研究では、投資後の脅威発生率低減を反映して、セキュリティに対する最適投資を調整する手法が提案されている
 - 本研究は「情報処理実態調査」のデータを参考にパラメータをセットしたシミュレーションによって行われた。評価の結果、提案手法によって、9種類の脅威のうち6種類について情報セキュリティ投資に関する意志決定における正解選択率が上昇することが確認できた(定量調査)
- (G) An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan
- 情報セキュリティ対策については、さまざまなものを組み合わせることによってその効果(インシデントの削減等)を高めることができることを実証しようとしたもの
 - 対策は単に技術的なものへの投資に限らず、情報セキュリティポリシー策定や関係者への研修・教育を併用することによって、情報セキュリティ対策の効果を一層高めることができることが確認された。一方、ダミー変数として業種による制御をしなければ現在のデータでは証明が難しいとされている(定量調査)
- (H) The Challenge of Providing a Voter Registration System for Millions of Filipinos Living Overseas
- 今後導入が期待される情報システムを活用した海外在住者用在外投票システムについて記したもの
 - バイオメトリクスについては、期待しつつも、修正されたデータが犯罪に悪用されるリスクがある点、海外投票者への対応をどうするかという点、利便性をどうするかといった課題が残されており、段階的に導入していくことを推奨している(定性調査)

- (I) University-Industry Collaboration in the Information Security Field: An International Comparison
- 産学の連携の進捗状況について、SCIS (Symposium on Cryptography and Information Security) での論文における引用、出典を分析した上で検討したもの
 - 今回は、日本のみならず国際比較を行ったのが特色だが、調査結果によると、海外でも日本と同様に産学の連携は思ったほど進捗していないことが判明した。また、電気、機械といった伝統的分野に比べた遅れも確認できた (定量調査)
- (J) The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market
- 情報セキュリティ面でのニュース、インシデントが株価に及ぼす影響について、米国と比較しつつ分析を行ったもの
 - 日本は米国と比べ、市場が反応する速度は遅いことが分かった。また、企業規模との関係、無形資産が占める比率が高い企業ほど影響が大きいことも判明した (定量調査)
- (K) Vulnerability and Information Security Investment : An Empirical analysis of e-local government in Japan
- 「地方自治総覧」のデータを用いて、日本国内の地方自治体における情報システムへの投資と脆弱性との関係について計量経済学的分析を行ったもの
 - 情報化経費で制御した分析結果によると、ネットワーク態様によって脆弱性レベルを分類すれば、中程度の脆弱性へ重点的に投資するという有力な最適投資モデルを実証できることが分かった

5.3.2. 海外での研究トレンド

情報セキュリティの分析手法のトレンドについて、松浦准教授が参加している国際会議(WEIS)の検討テーマを整理した(なお、ホームページ上で公開されているもののみを対象に、本調査の観点から整理したものであり、調査・研究の趣旨を必ずしも正確に反映したものでない)。

(1) WEIS2007 の概要

情報セキュリティの経済・社会的分析に関して、研究成果のグローバルな公表の場(2007年の時点で、当該分野のトップコンファレンス。日本からの研究成果採録の実績は、松浦准教授らによる2006年の論文採録があるのみ)である「WEIS2007」の概要を示す。

(A) 講演会名

- WEIS(Workshop on the Economics of Information Security)2007

(B) 開催日時

- 2007年6月6日(水)～8日(金)(年1回開催)
- 次回は2008年6月25日～27日にかけて、米国ダートマス大(ニューハンプシャー州)にて開催

(C) 開催場所

- 米国カーネギーメロン大学(米・ペンシルバニア州ピッツバーグ)

(D) 講演内容

- 情報セキュリティと経済、社会との関係に関する定量分析や理論モデルを中心に約25の講演

(E) ホームページ

- <http://weis2007.econinfosec.org/program.htm>

(2) WEIS2007 での検討テーマ

「WEIS2007」での検討テーマのうち、Web サイトから入手可能な講演内容(講演テーマ、講演者、講演概要)を整理した。

(A) The Legitimate Vulnerability Market

講演者

- Charles Miller

講演概要

- ベンダ以外の第三者の専門家が、公開されていない脆弱性情報を見つけた場合に、それをベンダ側に販売するマーケットメカニズムが働くかどうかに関する考察

- 公正な市場価格を算定する第三者の存在が不可欠であるが、発見者側の情報の出し惜しみ(ただ乗り防止)により、その価格を決定することが難しいこと、購入者を見つけることが難しい等の理由で、現時点では難しいと結論付けている模様

(B) Inadvertent Disclosure-Information Leaks in the Extended Enterprise

講演者

- M.Eric Johnson and Scott Dynes

講演概要

- PtoP のファイル交換による、(過失による)ビジネス上の被害について、企業の属性との関係を分析したもの
- 結果として、企業規模(従業員数)が多いところほどその被害レベルが大きくなるというリスクを抱えていることが伺えた。同時に、対応策として、専用ソフト、従業員教育、モニタリングといったものが掲げられている

(C) Network Security: Vulnerabilities and Disclosure Policy

講演者

- Jai Pil Choy,Chaim Fershtman,Neil Gandal

講演概要

- ソフトウェアベンダーを対象に、自社製品のセキュリティ上の問題点について公表すべきかどうか、また公表する際のインセンティブ付与について、政府規制の影響や、経済的観点から効果等を検証したもの
- 「Bug Bounty Program」と呼ばれる脆弱性を発見、報告した人に対して報奨金を提供するというスキームに対して、高い評価を与えている

(D) The Countervailing Incentive of Restricted Patch Distribution:Economic and Policy Implications

講演者

- Mohammad S. Rahman, Karthik Kannan, Mohit Tawarmalani

講演概要

- ソフトウェアベンダーが、自社製品のパッチを(海賊版利用者を含む)すべての利用者に公開すべきか、正規品ユーザーのみに提供すべきかについて、社会的厚生観点から経済的分析をおこなったもの
- 政府が海賊版防止に積極的に関与する場合としない場合でシナリオを区分している。政府が対策を取らない場合は正規ユーザーのみにしたほうがよく、また、企業活動は社会的厚生上の最適解と一致しない

(E) On the Viability of Privacy-Enhancing Technology in a Self Regulated Business-to-Consumer Market

講演者

- Rainer Bohme, Sven Koble

講演概要

- プライバシーを高める技術導入の経済効果について分析したもの
- プライバシー技術は電子取引上の顧客と企業の関係に大きな影響を持っている。即ち、プライバシーを気にかける消費者が存在する限り、技術の導入は収入を増やす効果がある。また、価格の差別化要因としても活用できる(価格が安くてプライバシー保護不要とする消費者は依然として存在する)

(F) When 25 Cent is too much: An experiment on willingness-to-sell and willingness-to-protect personal information

講演者

- Jens Grossklags, Alessandro Acquisti

講演概要

- 個人情報保護 1 件当たりの価値(金額)がどの程度かについて、情報の保護の観点と情報販売の観点から分析を行ったもの
- 販売する際に許容できる(最低限の)単価が、保護する際の単価を上回っていることが確認できた

(G) Optimally Securing interconnected information systems and assets

講演者

- Vineet Kumar, Rahul Telang, Tridas Mukhopadhyay

講演概要

- 情報セキュリティへの投資による効果、影響についてモデル化を図ろうとしたもの
- 例えば、脅威や対抗策についていくつかに分類を行っている。発見事項として、セキュリティ保護対策は他の企業の戦略の影響を受けないとしており、支援施策としては補助金が最も好ましいとしている

(H) Interdependence of Reliability and Security

講演者

- Peter Honeyman and Galina A.Schwartz

講演概要

- 製造業者が、製品に用いるソフトウェアの信頼性およびセキュリティ面の欠陥について明確な区分ができるわけではないため、対応策を講じる際のメカニズムも明確ではない
- また、外部環境として、ただ乗り(フリーライダー)という問題や、社会的厚生からみた全体最適との不一致という問題を整理した

(I) A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision Making

講演者

- Rachel Rue, Shari Lawrence Pfleeger, David Ortiz

講演概要

- 情報セキュリティへの投資の決定に当たっては、リソース配分の観点から(効果等の)定量化のためのモデルの活用が不可欠であり、現在あるさまざまな手法の比較をおこなったもの(input/output モデル、ゲーム理論モデル、会計学モデル等)
- 本論文は、すべてに適用可能なモデルがあるわけではなく、ケースにより適用可能なモデルが異なるとしている。また、いずれのモデルにせよデータの精度を高めることが不可欠であり、そのためにもモデルは必ずしも精緻なものである必要はないとしている

(J) Growth and Sustainability of Managed Security Service Networks: An Economic Perspectives

講演者

- Alok Gupta, Dmitry Zhdanov

講演概要

- 企業のネットワークが外部接続されるに伴い、セキュリティ対策も自社のみでの対応では十分に行えないようになってきている
- 「MSSP (Managed Security Service Provider)」と呼ばれる、セキュリティのアウトソーシング事業者が果たす役割について、企業間のコンソーシアム方式と比べた費用面等での優位性について説明している

(K) Will Outsourcing IT Security Lead to Higher Social Level of Security

講演者

- Brent Rowe

講演概要

- 情報セキュリティのアウトソーシングについて、(主に肯定的な観点から) 外部環境、コスト、効果、種別等を整理したもの
- 結論としては、費用削減、セキュリティ向上の面から企業はアウトソーシングに積極的であるとする一方、発生が不確定であることによる課題や、企業行動と社会から見た最適解との不一致についても触れている。政府の役割についても、補助金の果たす役割を評価している

(L) Measuring Security Investment Benefit for OFF the Shelf Software Systems-A Stakeholder Value Driven Approach

講演者

- Yue Chen, Barry Boehm, Luke Sheppard

講演概要

- 情報セキュリティ上の脅威分析を定量的に行うモデル「T-MAP (Attacking Path Analysis)」について分析をおこなったもの
- 同手法は、そもそもはパッケージ製品(COTS)のセキュリティについて、セキュリティアタックのルートから分析を加えたものだが、T-MAPではそれに加え、企業およびステークホルダのバリューへの影響ルートについてもモデル化している。今後はデータを精緻化させより優れたモデルを構築していく

(M) Incentive Design for Free but No Free Disposal Services: The Case of Personalization under Privacy Concerns

講演者

- Ramnath K. Chellappa, Shivendu Shivendu

講演概要

- 個人のホームページ上でカスタマイズ可能なツールバーのような、パーソナライゼーションツールとセキュリティ上の課題について整理したもの
- パーソナライゼーションによってベンダに追加コストが発生するわけではないが、契約としては固定契約と利用契約が双方必要であるとしている (Pick and Choose)。一方で、クーポン提供も一つのパーソナライゼーションのパターン (Amazon) として認知している

(N) The Effect of Online Privacy Information on Purchasing Behavior :An Experimental Study

講演者

- Janice Tsai, Serge Egleman, Lorrie Cranor, Alessandro Acquisti

講演概要

- BtoC での個人情報のベンダでの扱いが消費者から必ずしも十分に見えていないことが消費者の不安要素となっていることから、企業側が個人情報の保存、管理状況について適切に評価・公表することが消費活動にどのような影響を及ぼすかを調査したもの
- 調査結果では、積極的公表が消費活動を刺激することが分かり、さらに、公表する事業者に対しては高い値段であっても支払う消費者層が存在することも判明した

(O) Economics of User Segmentation, Profiling, and Detection in Security

講演者

- Srinivasan Raghuathan, Huseyin Cavusoglu, Byungwan Koh

講演概要

- User Profiling とは、アクセスするユーザーを、属性に応じて危険度の観点からいくつかのクラスに分類し、安全なユーザーには簡素な手続を、危険度の高いユーザーには厳重な本人確認を行い、犯罪を防止しようというもの
- 本論文はその効果を認めつつ、外部の不正なアクセスが、自らを偽ることに伴うリスクを指摘し、バイオメトリクスのような、成りすましに大きなコストを伴う手段を用いる有効性を指摘している

(P) Deterrent Effect of Enforcement Against Computer Hackers: Cross Country Evidence

講演者

- Ivan Png, Chen Yu Wang

講演概要

- 政府のセキュリティ犯罪への政策面での取り組みがどの程度抑止効果を持つかについて検証したもの
- アタックの 36% 削減という効果が発揮され、特に罰金よりも収監 (imprisonment) の効果が大きかったとしている。ただし、中長期的な効果については今後検証を続けていく必要がある

(Q) An Empirical Analysis of the Current State of Phishing Attack

講演者

- Tyler Moore, Richard Clyaton

講演概要

- フィッシングサイトの現状について調べたもの。フィッシングサイトの寿命（サイトが何日間アクティブな状態か）、フィッシングにより生じるコスト（毎年 3 億 5000 万ドル）、一日当たりどの程度のフィッシングサイトが検知、除去されているか等について統計を取り分布を整理したもの
- フィッシングサイトの除去は必要ではあるが、十分に効果を発揮できているわけではないとしている

(R) Privacy Protection and Technology Diffusion: The case of Electronic Medical Records

講演者

- Amalia R. Miller, Catherine E. Tucker

講演概要

- EMR(Electronic Medical Record Technology)により医療記録を電子的にやり取りする動向に対して、プライバシーの観点から反対する動きが生じている
- 本論文では、そうした反対の動きのマイナス効果について指摘している。例えば州政府によるプライバシー規制で 25%の利用が制約を受け、また、州政府間のソフトウェアの互換性も 33%が阻害されるとしている

(S) Building (and estimating) Economic Models

講演者

- Neil Gandal

講演概要

- 経済モデルをセキュリティ分析に用いる際のポイントの説明
- 基本として、既に確立した経済モデルを用いることを推奨している。まずは、簡単なモデル(Reduced Form)を適用し次第に「前提条件」を解除し精緻化する(Structural Model)ことをすすめている。政府の政策も現実性のある者とならないものの区分、消費者余剰と社会余剰の違いの理解、外部環境との相互影響の考慮等にも触れている

(T) Mental Model of Computer Security Risks

講演者

- Farzaneh Asgharpour, Debin Liu, L. Jean Camp

講演概要

- セキュリティ対策としては、単に事業者や専門家の取り組みでなく、専門家でない一般人と適切なコミュニケーションがとられることが不可欠
- 今回の調査では、専門家と一般人にさまざまな事象を例にセキュリティ認識を調査したところ、両者には認識モデルに大きなギャップがあることが伺えた。今回の定量調査に加え、今後はインタビュー等の定性調査行っていく、両者のギャップを埋めるためのコミュニケーションのあり方を探っていく

(U) Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management

講演者

- Hemantha S.B. Herath, Tejaswini C. Herath

講演概要

- 近年、実務家および専門家からも必要性を指摘する声が多い、サイバー保険について、専門のモデルを用いて、価格決定方法(Pricing)のあり方を整理したもの
- インターネット上のリスクは実社会の保険と比べ、頻度、被害額、可視化等から異なる点が多い。アタックによる直接の被害額に加え、ケーススタディも交えつつ、企業全体の被害額まで考慮した保険料を算出するモデルを整理している

(V) Strategic Defense and Attack of Complex Networks

講演者

- Kjell Hausken

講演概要

- 企業の情報システムは複雑化し、ネットワークによってさまざまなコンポーネントが互いにリンクし影響しあっている
- 本論文では、そうした環境下での、情報システムを守る側とアタックする側のアクションの関係について、投下されるコスト、システムの機能への評価、システムの環境等による影響を整理している。今後は現実のケースの情報を適用してより現実性を高めていくとのこと

(3) WEIS2007 から得られる示唆

「WEIS2007」での検討テーマから、情報分析ラボにおける分析機能の検討に資するポイント(分析テーマ案)を整理した。

(A) アドホックなテーマ

- PtoP のファイル交換によるビジネスへの影響

(B) 政策との関連

- セキュリティ事故、リスク、個人情報取扱に関する(企業側の)情報公開の支援や政策上の措置
- 企業等へのセキュリティ対策への補助金導入の有効性
- 政府の採る対策によるセキュリティ犯罪抑制効果レベル

(C) 経済学の観点

- 企業にとっての最適化(となる行動)と個人、政府、外部環境を含む社会にとっての最適解との差異
- セキュリティ対策へのただ乗り(フリーライダー)の問題

(D) 消費者の観点

- 消費者にとっての情報セキュリティの安全性への評価
- 個人情報の市場価格
- カスタマイズ・ツール(Yahoo!他)と個人情報
- ベンダと消費者のコミュニケーションギャップの分析

(E) 企業経営の観点

- 情報セキュリティへの投資の費用対効果
(数値およびその算定モデル、必要となるデータ等)
- 情報セキュリティアウトソーシングのあり方
- 情報システム保険

(F) 情報システムの観点

- 企業の情報システムの複雑化(スタンドアロンからネットワークによる外部との相互接続、影響)に伴うセキュリティ上の影響、リスク

5.3.3. 分析手法の全体像

現在の情報セキュリティ分析手法に関する鳥瞰図を、定量分析か定性分析か(分析の種別)、また経済活動かその他か(分野の種別)の2つの軸から整理したところ以下のとおりとなった。

(1) 鳥瞰図

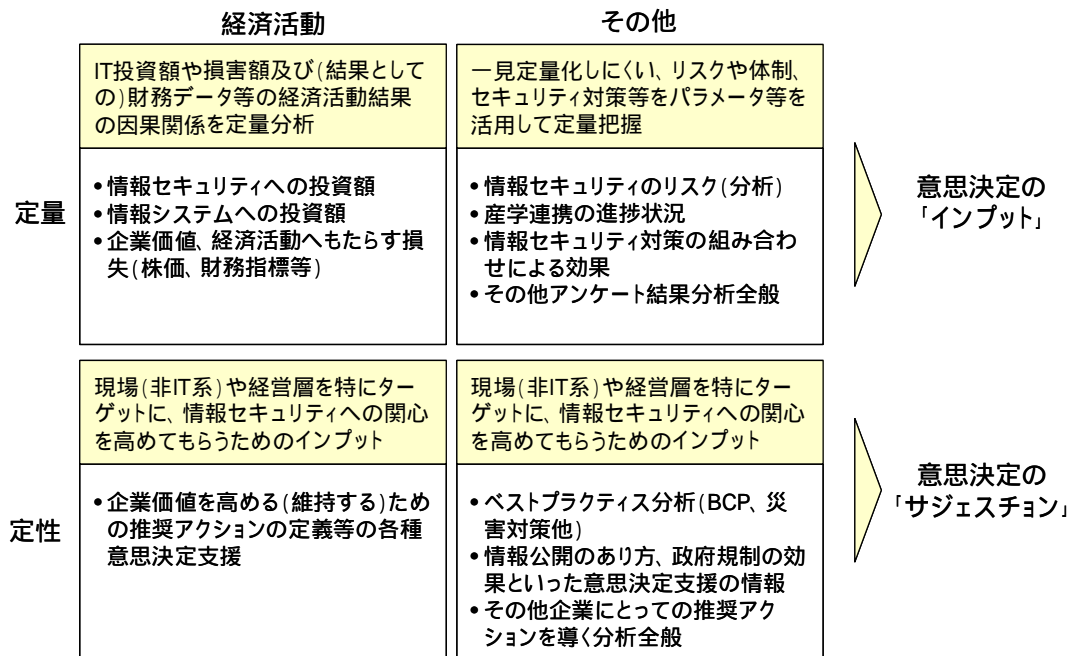


図 5-1 分析手法の鳥瞰図

ここで注目したいのは、定量分析・定性分析が排他的で別々のケースとしてもちいられるという側面ではなく、両方を組み合わせることで実務面での効果が発揮されるという点である。

即ち定量分析は、情報システムあるいは情報セキュリティという、経営や政策立案の視点から目に見えにくいものを、データとその因果関係として可視化するものである一方、定性分析はこうしたインプットを踏まえて行う意思決定を、事例の提供やアクションメニューの提供といったかたちで支援するものである。

(2) 企業・政府からのニーズと分析手法の現状

以上のような情報セキュリティ分析手法における定量分析および定性分析の現状を踏まえ、次の課題としては企業・政府側のニーズから、(有識者、専門機関等を中心とする)分析手法の最新状況を見た場合の課題について以下のとおり整理した。

まず、分析手法については企業・政府側のニーズは、高レベルな分析手法ではなく、(ハンドリング可能な)アンケートでの集計結果等の比較的単純な分析レベルに留まる。一方、専門機関では高レベルな分析手法の開発・活用が進められており、専門家による研究内容や分析手法に関する最新の動向を企業責任者、政府政策立案者に情報提供するとともに、現場の課題解決に少しでも活用できるよう分析手法を簡素化する、分かり易くする、あるいはツール化するといった橋渡しの機能も必要と考えられる。

一方、定性分析については、最新研究では必ずしも中心ではないとされるものの、実務レベルでは意思決定に資するものとしての期待が大きいようだ。

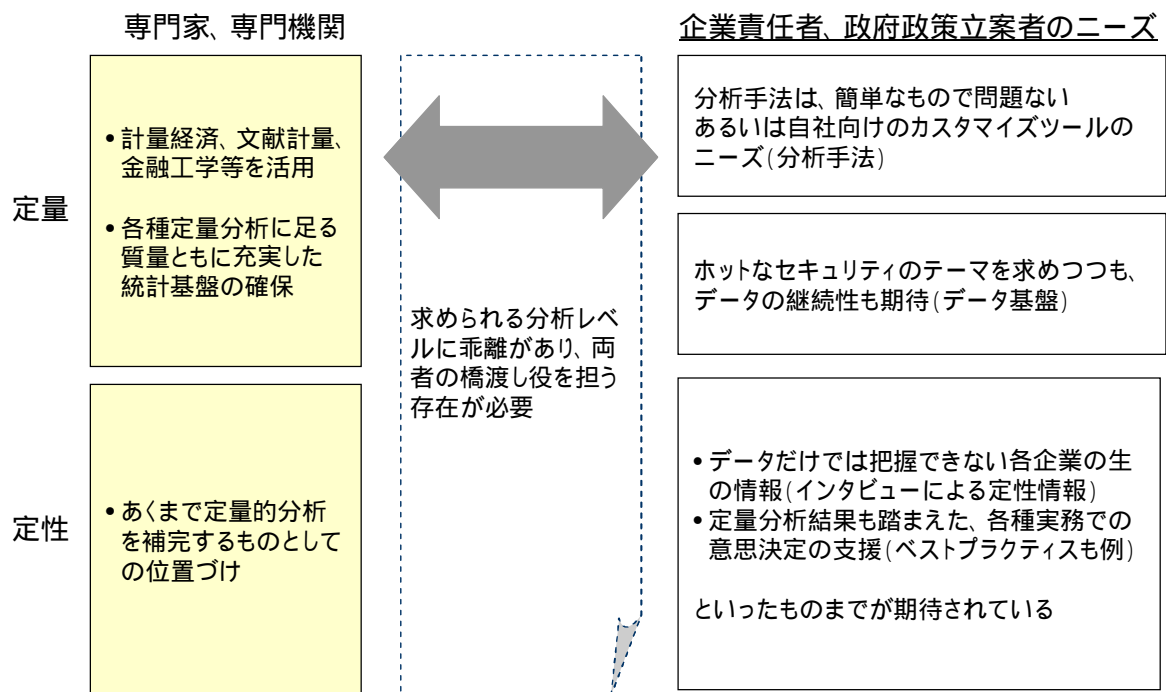


図 5-2 分析手法へのニーズ

6. まとめ

今回の調査における、国内外の幅広い情報セキュリティおよび経済社会分析に係る関係機関、有識者等を対象としたインタビュー等を踏まえると、分析手法、組織機能等の現状および今後については以下のように整理できる。

(1) 用途および利用主体に応じた分析手法

分析手法の現状については、利用者および利用目的によって大きく区分でき、互いに対照的であることがわかった。

すなわち、情報セキュリティに関する分析および研究成果を企業や市民を含む幅広い関係者に提供することを主たる目的としている場合においては、アンケート結果の集計が中心であり、分析手法についても平易なものが多い。一方、政策過程・市場動向把握、個別の投資決定といった、情報提供でなく内部での研究や分析を主目的とする場合には、平易な手法に加え多変量解析、さらには金融工学的アプローチの援用を視野に入れていることが窺える。

(2) 官民連携の重要性

米国では情報セキュリティに関する民間の調査分析を政府がスポンサーしたり、調査結果の分析で官民が連携するという動きが見られた。日本でも統計基盤の確立やデータ収集といった面で官民が連携する必要性があり、官民連携の重要性については、日米とも共通している。これは研究者と政府との関係構築についても同様と言える。

(3) 整備されつつある統計面でのインフラ

有識者の話でも、情報処理実態調査をはじめとする日本の政府が公式に(承認統計等の方式で行う統計調査については、海外の民間調査会社が行う調査と比べても母集団数やその(統計学的)品質という点で優れたものであることが分かった。また、今後は統計法の改正により、調査研究目的であれば個別の回答内容の明細等も幅広い関係者で共有する仕組みが構築されていくこともあり、こうした統計インフラの活用は期待されることである。

(4) 効果的な情報提供の実施

調査分析した結果を、国民および関係者に分かりやすい形で提供することの重要性は国内外とも同じである。本件においても、IPA のホームページでの提供(専門家向けの情報と一般向けの情報で、情報の粒度に差をつけることも考えられ

る)、関係機関ホームページでの提供、多言語での情報提供、学会等での冊子での配布等を適宜組み合わせていくことになる。

付録 調査レポート／参照元一覧

調査レポート／参照元	調査主体／著者	URL
第3章		
日本銀行金融研究所 情報技術研究所 ホームページ	日本銀行金融研究所	http://www.imes.boj.or.jp/citecs/
JPCERT / CC ホームページ	JPCERT コーディネーションセンター	http://www.jpccert.or.jp/
FISC ホームページ	(財)金融情報システムセンター	https://www.fisc.or.jp/
電気事業連合会 ホームページ	電気事業連合会	http://www.fepc.or.jp/index.html
サイバーフォースセンター (@police) ホームページ	警察庁	http://www.cyberpolice.go.jp/
日本銀行 ホームページ	日本銀行	http://www.boj.or.jp/
日本銀行金融研究所 ホームページ	日本銀行金融研究所	http://www.imes.boj.or.jp/
新しい日本銀行 その機能と業務	日本銀行金融研究所	http://www.imes.boj.or.jp/japanese/pf.html#chapter1
日本エネルギー経済研究所 ホームページ	日本エネルギー経済研究所	http://eneken.ieej.or.jp/index.html
国民生活センター ホームページ	国民生活センター	http://www.kokusen.go.jp/
Computer Security Online	CXO Media	http://www.csoonline.com/
Computer Security Institute ホームページ	Computer Security Institute (CSI)	http://www.gocsi.com/
インターネット犯罪苦情センター ホームページ	インターネット犯罪苦情センター (IC3)	http://www.ic3.gov/complaint/
Computer Economics ホームページ	Computer Economics	http://www.computereconomics.com/
保険計理長室 (Office of the Chief Actuary)	社会保障庁	http://www.ssa.gov/OACT/
第4章		
情報化白書2006	日本情報処理開発協会 (JIPDEC)	http://www.jipdec.jp/chosa/hakusho2006/index.htm
平成19年情報通信白書	総務省	http://www.jphoto.usintokei.soumu.go.jp/whitepaper/ja/h19/index.html
企業行動調査2007	日本情報システム・ユーザー協会 (JUAS)	http://www.juas.or.jp/project/survey/it07/index.html
2006年ITサービスイラストユーザー動向調査	ガートナー	
2006年セキュリティ・ソフトウェア市場動向	ガートナー	

第4章	調査レポート / 参照元	調査主体 / 著者	URL
	2006年国内 / 世界のITサービス市場規模予測	ガーートナー	
	2007 Enterprise Software Customer Survey	McKinsey and Co. and Sand Hill Group	http://software2007.com/grafix/pdf/Enterprise-Software-Customer-Survey-2007.pdf
	2007 State of the CIO	CIO Magazine	http://www.cio.com/state-of-the-cio/2007/index
	50 Technologies: Where CIOs are Spending Their Money	CIO Insight	http://www.cioinsight.com/article2/0,1540,2094439,00.asp
	IT Spending, Staffing, and Technology Trends	Computer Economics	http://www.computereconomics.com/page.cfm?name=IT%20Spending%20and%20Staffing%20Study
	Managing IT Costs in a Weakened Economy	CIO Insight	http://www.cioinsight.com/article2/0,1397,2181433,00.asp
	Software as a Service	InformationWeek	http://i.cmpnet.com/bmighy/research/Software.as.a.Service.pdf
	Trends in Telephony Service	Federal Communications Commission	http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-270407A1.pdf
	情報処理実態調査	経済産業省	http://www.meti.go.jp/statistics/zyo/zyouhou/index.html
	情報セキュリティに関する新たな脅威に対する意識調査	情報処理推進機構 (IPA)	http://www.ipa.go.jp/security/fy18/reports/ishiki01_press.html
	国内におけるコンピュータ・ウイルス被害状況調査	情報処理推進機構 (IPA)	http://www.ipa.go.jp/security/fy18/reports/virus-survey/index.html
	企業における情報セキュリティ被害被害額調査	情報処理推進機構 (IPA)	http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html
	2006年日本の情報セキュリティ管理におけるコンプライアンスの現状と課題	ガーートナー	http://www.gartner.co.jp/index.html
	Japan Security and Continuity 2007	IDC	http://www.idcjapan.co.jp/top.html
	Information Security Awareness Report	SecureInfo Corp.	http://www.fcw.com/images/st_images/SecureInfo_06_04_07.pdf
	Datagate: The Next Inevitable Corporate Disaster?	McAfee Corp. and Datamonitor	http://www.mcafee.com/us/local_content/misc/dlp_datagate_research.pdf
	Internet Security Threat Report, June, 2006 December, 2006	Symantec	http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport
	2006 Annual Study: Cost of a Data Breach	Ponemon Institute, Vontu Corp. and PGP Corp.	http://download.pgp.com/pdfs/Ponemon2-Breach-Survey_061020_F.pdf
	2007 Annual Study: U.S. Encryption Trends Study	Ponemon Institute and PGP Corp.	http://www2.csoonline.com/whitepapers/2007study061207.pdf
	2007 North American Virtual Criminology Report	McAfee Corp.	http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtuallCriminologyReport07.pdf?cid=3

第4章	調査レポート / 参照元	調査主体 / 著者	URL
	Data Loss Prevention and Endpoint Security	Vontu Corp. and Forrester Consulting	http://www.vontu.com/uploadedfiles/global/VontuDataLossPreventionEndpointSurvey.pdf
	Global Information Security Survey 2006	Ernst and Young	http://www.ey.com/Global/download.nsf/International/TSRS_-_GISS_2006/\$file/EY_GISS2006.pdf
	Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior	Cisco Systems and Insight Express	http://www.cisco.com/application/pdf/en/us/guest/netso/ns413/c654/cdccont_0900aecd8054581d.pdf
	National Survey on the Detection and Prevention of Data Breaches	WebSense and Ponemon Institute	http://www.csoonline.com/features/ponemon/ponemon102306.html
	2006 CSI/FBI Computer Crime and Security Survey	Computer Security Institute and the Federal Bureau of Investigations (FBI)	http://i.cmpnet.com/goCSI/db_area/pdfs/fbi/FBI2006.pdf
	FBI Computer Crime Survey	FBI	http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm
	Enterprise Security Survey	Apani Networks	http://www.apani.com/surveys/enterprise-security-survey-2006
	2006 Technology, Media, and Telecommunications Security Survey	Deloitte Touche Tohmatsu	http://www.deloitte.com/dtt/research/0,1015,cid%253D122104,00.htm
	Security Trends Report, 2Q07	WebSense	http://www.websense.com/securitylabs/docs/Security_Labs_Report_07Q2.pdf
	Information Security Awareness Survey	Business Software Alliance and Forrester Consulting	http://www.bsa.org/country/Research_and_Statistics/ /media/F4424D20D994429D88073C75DF6F3AC9.ashx
	Insider Threat Study: Computer Sabotage in the Critical Infrastructure Sectors	U.S. Secret Service and CERT Coordination Center	http://www.secretservice.gov/ntac.shtml
	Top 20 Internet Security Attack Targets	SANS Institute and FBI	http://www.sans.org/top20/?ref=3706
	E-Crime Watch Survey 2006	Computer Security Online, US Secret Service, CERT Coordination Center, and InformationWeek and Accenture	http://www2.csoonline.com/info/release.html?CID=24531
	Global Information Security Survey		http://www.informationweek.com/story/showArticle.jhtml?articleID=201001203
	Information Security: A CompTIA Analysis of IT Security and the Workforce	CompTIA and TNS Prognostics	http://www.comptia.org/sections/research/research%20docs/securitysummary407.pdf
	Committing to Security: Fourth Annual Benchmark Survey	CompTIA and TNS Prognostics	http://www.comptia.org/sections/research/research%20docs/securitysummary3-06.pdf
	The Global State of Information Security 2006	CIO Magazine, Computer Security Online, and Pricewaterhouse Coopers	http://www.cio.com/article/24979/The_Global_State_of_Information_Security_
	State of Internet Security: Protecting Enterprise Systems	Webroot Software	http://www.webroot.com/pdf/StateofInternetSecurity_Enterprise0307.pdf
	IT Risk Management Report	Symantec	http://eval.symantec.com/mktginfo/enterprise/other_resources/enterprise_risk_management_report_02-2007.en-us.pdf

調査レポート / 参照元	調査主体 / 著者	URL
第4章		
2006 Global Security Survey	Deloitte Touche Tohmatsu's Global Financial Services Institutions Group	http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006_Global_Security_Survey_2006-06-13.pdf
Network Attacks: Analysis of Justice Prosecutions from 1999 2006	Phoenix Technologies and Trusted Strategies	http://www.net-security.org/dl/articles/Report-DOJ_Computer_Crime_Prosecutions.pdf
Cost of Spam	Ferris Research	http://www.ferris.com/research-library/industry-statistics/
Digital Confidence Index	Computer Security Industry Association	https://www.csalliance.org/publications/publications/surveys_and_pols/ddi_survey_May2006/
2007 Consumer Survey on Data Security	Ponemon Institute and Vontu Corp.	http://www.vontu.com/uploadedfiles/global/2007_Data_Security_Consumer_Survey.pdf
Online Fraud Report	National Cyber Security Alliance and Bank of America	http://staysafeonline.org/news/onlinefraudreportfinal.pdf
Internet Fraud Survey Report	Javelin Research	http://www.javelinstrategy.com/idf2007
Internet Crime Report	Internet Crime Complaint Center (IC3)	http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf
第5章		
Public Acceptance Issues Surrounding the Implementation of New Election Technology for Philippines	Kanta Matsuura, Jose Luis Lacson, Congressman Teodoro Locsin, Jr.	
University Industry Collaboration Networks in the Information Security Field In Japan: Problems and a Particular Success	Kanta Matsuura, Ken Ebato	
A Derivative of Digital Objects and Estimation of Default Risks in Electric Commerce	Kanta Matsuura	
Cross Sector Collaboration in Japanese Information-Security Industry and the Shock of Personal Information Protection	Kanta Matsuura	
Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms	Wei Liu, Hideyuki Tanaka, Kanta Matsuura	
Risk Assessment Model using Threat Probability depending on Classified Information Security Measures	Takayasu Yamaguchi, Hiroshi Aono, Sadayuki Hongo, Kanta Matsuura	
An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan	Wei Liu, Hideyuki Tanaka, Kanta Matsuura	
The Challenge of Providing a Voter Registration System for Millions of Filipinos Living Overseas	Kanta Matsuura, Jose Luis Lacson	
University-Industry Collaboration in the Information Security Field: An International Comparison	Kanta Matsuura	
The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market	Masaki Ishiguro, Hideyuki Tanaka, Kanta Matsuura, Ichiro Murase	
Vulnerability and Information Security Investment : An Empirical analysis of e-local government in Japan	Hideyuki Tanaka, Kanta Matsuura, Osamu Sudoh	

第5章	調査レポート / 参考文献	調査主体 / 著者	URL
	The Legitimate Vulnerability Market	Charles Miller	http://weis2007.econinfosec.org/program.htm
	Inadvertent Disclosure-Information Leaks in the Extended Enterprise	M.Eric Johnson and Scott Dynes	http://weis2007.econinfosec.org/program.htm
	Network Security: Vulnerabilities and Disclosure Policy	Jai Pii Choy,Chaim Fershtman,Neil Gandal	http://weis2007.econinfosec.org/program.htm
	The Countervailing Incentive of Restricted Patch Distribution:Economic and Policy Implications	Mohammad S. Rahman, Karthik Kannan, Mohit Tawarmalani	http://weis2007.econinfosec.org/program.htm
	On the Viability of Privacy-Enhancing Technology in a Self Regulated Business-to-Consumer Market	Rainer Bohme, Sven Koble	http://weis2007.econinfosec.org/program.htm
	When 25 Cent is too much: An experiment on willingness-to-sell and willingness-to-protect personal information	Jens Grossklags, Alessandro Acquisti	http://weis2007.econinfosec.org/program.htm
	Optimally Securing interconnected information systems and assets	Vineet Kumar,Rahul Telang, Tridas Mukhopadhyay	http://weis2007.econinfosec.org/program.htm
	Interdependence of Reliability and Security	Peter Honeyman and Galina A.Schwartz	http://weis2007.econinfosec.org/program.htm
	A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision Making	Rachel Rue,Shari Lawrence Pfleeger, David Ortiz	http://weis2007.econinfosec.org/program.htm
	Growth and Sustainability of Managed Security Service Networks:An Economic Perspectives	Alok Gupta,Dmitry Zhdanov	http://weis2007.econinfosec.org/program.htm
	Will Outsourcing IT Security Lead to Higher Social Level of Security	Brent Rowe	http://weis2007.econinfosec.org/program.htm
	Measuring Security Investment Benefit for OFF the Shelf Software Systems-A Stakeholder Value Driven Approach	Yue Chen, Barry Boehm, Luke Sheppard	http://weis2007.econinfosec.org/program.htm
	Incentive Design for Free but No Free Disposal Services: The Case of Personalization under Privacy Concerns	Ramnath K. Chellappa, Shivendu Shivendu	http://weis2007.econinfosec.org/program.htm
	The Effect of Online Privacy Information on Purchasing Behavior :An Experimental Study	Janice Tsai,Serge Egleman, Lorrie Cranor, Alessandro Acquisti	http://weis2007.econinfosec.org/program.htm
	Economics of User Segmentation,Profiling,and Detection in Security	Srinivasan Raghathath, Huseyin Cavusoglu, Byungwan Koh	http://weis2007.econinfosec.org/program.htm
	Deterrent Effect of Enforcement Against Computer Hackers:Cross Country Evidence	Ivan Png, Chen Yu Wang	http://weis2007.econinfosec.org/program.htm
	An Empirical Analysis of the Current State of Phishing Attack	Tyler Moore, Richard Clyaton	http://weis2007.econinfosec.org/program.htm
	Privacy Protection and Technology Diffusion: The case of Electronic Medial Records	Amalia R. Miller, Catherine E. Tucker	http://weis2007.econinfosec.org/program.htm
	Building (and estimating) Economic Models	Neil Gandal	http://weis2007.econinfosec.org/program.htm

調査レポート / 参照元	調査主体 / 著者	URL
第5章		
Mental Model of Computer Security Risks	Fairzaneh Asgharpour, Debin Liu, L. Jean Camp	http://weis2007.econinfosec.org/program.htm
Cyber - Insurance Copula Pricing Framework and Implications for Risk Management	Hemantha S.B. Herath, Tejaswini C. Herath	http://weis2007.econinfosec.org/program.htm
Strategic Defense and Attack of Complex Networks	Kjell Hausken	http://weis2007.econinfosec.org/program.htm