情報セキュリティ産業の現状と展望

国立国会図書館　調査及び立法考査局
専門調査員　文教科学技術調査室主任　　小林　信一

目　　次

【要　旨】
情報セキュリティ産業は、社会の情報セキュリティを日々支える役割を担っている。本稿は、情報セキュリティ産業の観点から情報セキュリティの現状を展望する。
情報セキュリティ産業は今後の成長産業として期待されている。しかし、日本の情報セキュリティ産業の市場規模は、2000年代の成長の後、2008年度以降7千億円程度で停滞している。ただし、市場規模に関するデータは未整備であり、市場規模はもっと大きい可能性もある。
情報セキュリティ市場の将来は、新しい種類の脅威の発生、IT環境の変化、法規制等の外部環境の変化に左右される。「モノのインターネット」化の進展は、情報セキュリティ市場を変質させる可能性がある。一方、マイナンバー制度の運用開始、2020年東京オリンピック等は、情報セキュリティ市場の拡大要因になりうる。情報セキュリティ産業は、ICT社会を陰で支える裏方的産業で、顕著な存在感はないが、その重要性は将来においても変わることはない。

はじめに

情報セキュリティ産業は、社会全体の情報セキュリティを日々支える役割を担っている。本稿は、情報セキュリティ市場や情報セキュリティ産業の実態を明らかにすることを通じて、産業活動の観点から日本の情報セキュリティの現状を展望することを目的とする。

サイバーセキュリティ上の脅威に対する取組には、基盤的で公共性の高い取組と、主として民間主導で行われる日常的、個別的な取組がある。ウイルス対策ソフト、ファイアウォール、暗号化、ユーザ認証等の一般ユーザにもなじみのある情報セキュリティソフトや機器の開発・供給は民間企業によって担われている。また、個々の組織の状況に適合させて情報セキュリティの方針を定め、その方針に則って個別の情報セキュリティソフト・機器を組み合わせて情報セキュリティシステムを構築し、運用・監視する活動、またはそれらを専門的に支援するサービスは、主として民間主導で行われている。これら以外にも、情報セキュリティに関する教育、研修、情報セキュリティシステムの監査、情報セキュリティに関する保険なども主として民間企業、民間団体が担っている。つまり、サイバーセキュリティへの日常的な取組のほとんどは産業界が担っている。

「サイバーセキュリティ基本法」（平成26年法律第104号）は、サイバーセキュリティに関連する産業が成長産業となるよう国が必要な施策を講じることを定めている(1)。情報セキュリティ産業の振興に関する議論のためには、まず情報セキュリティ市場や産業の実態把握が必要である。しかし、「日本の情報セキュリティ市場や産業の規模はどれくらいか」という初歩的な問いにさえ確信を持って答えられないのが現実である。

そこで本稿は、日本におけるサイバーセキュリティ対策の現状を産業活動の観点から見て、その市場規模や産業構造の実態を探る。以下、Ⅰでは情報セキュリティ市場の分類、典型的なデータ源とその特性を明らかにする。Ⅱではその結果を踏まえて、可能な範囲で情報セキュリティ産業の成長を描出するとともにデータの限界や妥当性について検討する。また、独自の調査結果も含めて、産業構造の特徴を描出する。Ⅲでは情報セキュリティ市場に影響を及ぼす要因について検討する。その中で、情報セキュリティ市場に影響を与える法制度についても整理する。また、日本の情報セキュリティ産業の今後の展開に関して、新市場の見通し、海外市場

＊　本稿におけるインターネット情報の最終アクセス日は、特に断りのない限り、2014年12月19日である。
(1)　サイバーセキュリティ基本法第19条。

との関連、他産業との関連、外的要因の影響などの面から展望する。

Ⅰ　情報セキュリティ対策と情報セキュリティ市場

1　サイバーセキュリティに関連する概念

サイバーセキュリティに関連する概念としては、情報セキュリティ、ネットワークセキュリティ、コンピュータセキュリティなどの語が用いられている。まず、これらの関係を整理する。

我が国においては、サイバーセキュリティについては、サイバーセキュリティ基本法第2条が定義している(2)。一方、情報セキュリティについては、明確に定義されずに用いられるケースも多いが、JIS Q 27000:2014が定義している(3)。平易な表現で要約すれば、サイバーセキュリティや情報セキュリティは、情報システムや情報通信ネットワークが安全で信頼性が確保され、情報が適切に扱われるよう管理されることを指している。ただし、JIS Q 27000:2014の情報セキュリティの定義は情報通信技術を用いない情報（例えば、紙片に書かれたメモなど）も含むものである。このことに着目すれば、情報セキュリティの方がサイバーセキュリティより広い概念であると理解できる。一方、サイバーセキュリティという表現が初めて公式に用いられた「サイバーセキュリティ戦略」(4)（平成25（2013）年6月10日情報セキュリティ政策会議決定）では、従来の情報セキュリティ確保のための取組に加えて、広くサイバー空間(5)に係る取組を推進する必要性と取組姿勢を明確化するために「サイバーセキュリティ戦略」の名称を用いる旨が述べられている(6)。即ち、日本の政策上では、サイバーセキュリティは情報セキュリティを包含する概念として導入されたという経緯がある。ここでは政策上のサイバーセキュリティ概念を「広義のサイバーセキュリティ」とする。

ネットワークセキュリティに関しては、必ずしも明確な定義が存在していない。情報通信ネットワークを介してユーザのコンピュータ等が晒される脅威（内部からの攻撃による情報漏えいやミスによる情報流出を除く）を管理し、情報通信ネットワークの安全性や信頼性の確保のために必要な措置を取ることを指して用いられる場合もあれば、単にネットワーク社会における情報セキュリティといった意味で用いられる場合もある。前者の場合は、ネットワークセキュリティはサイバーセキュリティに包含される概念となる。後者の場合は、ネットワークセキュリティは情報セキュリティの一面であり、広義のサイバーセキュリティに包含される。

コンピュータセキュリティも明確に定義されていない概念であるが、多くの場合はユーザの

(2)「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式…（中略）…により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置…（中略）…が講じられ、その状態が適切に維持管理されていること」

(3)「情報セキュリティ（information security）」（2.33）は「情報の機密性（2.12），完全性（2.40）及び可用性（2.9）を維持すること。」なお、「機密性（confidentiality）」（2.12）とは「認可されていない個人，エンティティ又はプロセス（2.61）に対して，情報を使用させず，また，開示しない特性」、「完全性（integrity）」（2.40）とは「正確さ及び完全さの特性」、「可用性（availability）」（2.9）とは「認可されたエンティティが要求したときに，アクセス及び使用が可能である特性」と定義されている。

(4) 情報セキュリティ政策会議「サイバーセキュリティ戦略」2013.6.10. <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>

(5) サイバー空間とは「情報システムや情報通信ネットワーク等により構成され、多種多量の情報が流通するインターネットその他の仮想的なグローバル空間」の意。同上, p.4.

(6) 同上, p.3.

コンピュータが脅威に晒されている状況を管理し、コンピュータ利用の安全性や信頼性の確保のための措置を取ることを指している。情報通信ネットワークを介した脅威だけでなく、機器や装置を介した脅威、内部からの情報漏えいなども対象とするセキュリティ概念と捉えることができる。これも広義のサイバーセキュリティ概念に包含される。

したがって、我が国においては、サイバーセキュリティ、情報セキュリティ、ネットワークセキュリティ、コンピュータセキュリティは、広義には、また政策上、ほぼ同じものを指している。ただし、サイバーセキュリティは新しい概念であるため、調査や統計には十分には反映されておらず、多くは情報セキュリティに関する調査や統計として発表されている。本稿は、各種の調査や統計に基づいて産業活動の側面からサイバーセキュリティにアプローチするものである。そこで本稿では、既存の調査や統計との関連性を明確にするため、情報セキュリティの表現を用いる。

2　情報セキュリティ対策と情報セキュリティ市場の構成

（1）情報セキュリティ対策のあらまし

一般のユーザは、情報セキュリティのための対策として、ウイルスその他の不正プログラムの侵入を検知し、排除するためのウイルス対策ソフトの導入や、パソコンやスマートフォンのOSやアプリ（アプリケーション）の脆弱性を改善するためのアップデートなどを思い浮かべるであろう。しかし、企業等の組織の場合には、インターネットやコンピュータのユーザであると同時に、組織内のユーザに対してネットワーク環境、コンピュータ環境を提供する立場でもある。そのため、情報セキュリティ対策ははるかに複雑なものになる。

組織における情報セキュリティ対策のあらましは以下のとおりである。まず、個別の対策の前に、組織とその情報システムが置かれている環境やリソースを分析し、どのような脅威や脆弱性があるかを明らかにし、その結果を踏まえて、どのような情報セキュリティ対策を講じるかに関する全社的方針、情報セキュリティシステムの構築方針、管理体制などを検討する必要がある。方針の大枠が決まると、想定される脅威やそれに対する技術的対応策を組み合わせるなどして、情報セキュリティシステムを設計、構築し、実際に運用していくことになる。

脅威としては、ウイルス、スパムメール、危険なウェブサイトへのアクセス、不正アクセス、データ改ざんやサーバへの攻撃などネットワークを介した脅威と、組織内のシステムや端末の不正使用、ウイルス感染、さらには機密情報の持出しや過誤による情報漏えいなど組織内部の脅威がある。これらの脅威から組織の情報システムを守るために、不正アクセスの検知技術・防御技術、組織内部のシステムや端末からのウイルス除去、ユーザ認証技術、情報が流出した場合でも被害を小さくするための暗号技術など多様な技術がある。

情報セキュリティ対策技術としては、ソフトウェアだけでなく、組織の情報システムと外部ネットワークとの間の通信経路上に設置して不正なアクセスを遮断する機能（ファイアウォール）等を組み込んだアプライアンス(7)と呼ばれる装置やユーザ認証用機器等のハードウェア製品もある。これらの技術を適切に組み合わせて情報セキュリティシステムを設計し、構築、さらには運用していくことになる。最近は、組織内に情報システムを構築せずに、クラウドコン

(7)　ハードウェアとソフトウェアを一体化して特定の機能を提供する製品のことをいう。

ピューティング技術を利用してクラウド側に必要な情報システム、データベースを構築することも可能になっており、その場合は情報セキュリティに関してもクラウド側にシステムを構築したり、クラウドの提供するセキュリティサービスを利用したりする。このような外部資源の利用も含めて、組織の情報セキュリティシステムを構築していく。

情報セキュリティの確保のためには、情報セキュリティシステムを構築し、運用するだけでは十分ではない。実際に防御できているか、新しい脅威はないか等、常に状況を監視し、必要な見直し、改善を行う必要がある。もし、セキュリティが破られて、ウイルスによる感染等のインシデントが生じた場合には、緊急に対応し、復旧させることも必要になる。

また、情報セキュリティの確保のためには、技術的対応だけでなく、組織内のユーザが情報セキュリティに関して必要な知識やスキルを習得すること、必要な情報を適時に組織内に周知すること等の人的対策も必要である。さらに、組織が対外的な取引等を行う場合など、当該組織の情報セキュリティシステムが十分に整備されていることを保証するために、第三者による認証を受けておくことが必要になる。

（2）情報セキュリティ市場の分類

情報セキュリティ対策を実現するために、一般のユーザは、自らの判断で必要なセキュリティ対策ソフトを購入したり、アプリをアップデートしたりすることで対応することができる。情報システムが比較的単純な組織であれば、組織内部に情報セキュリティの専門家さえいれば、必要なソフトウェアやハードウェアを購入して独自に情報セキュリティシステムを構築することは可能であろう。このような場合には、情報セキュリティシステムに関わるソフトウェアやハードウェアの市場が成立し、それらを供給する産業が成立することになる。

一方、巨大化・複雑化した情報システムが導入されている大規模組織の場合など、情報セキュリティシステム構築も複雑化し、内製できない可能性が高い。そのような場合も、外部の専門業者のコンサルテーションを受けたり、情報セキュリティシステムの設計、構築や、場合によっては運用も外部の専門業者に委託したりすることが現実的選択肢になる。情報セキュリティに関する教育や研修も外部に委託することが可能である。情報セキュリティシステムの認証は、その性質上外部に依頼することになる。この種の情報セキュリティに関するサービスについても市場が成立し、サービスを提供する産業が成立することになる。

情報セキュリティに関わる産業について論じるためには、これらの情報セキュリティに関する市場を定義し、その範囲を明確にする必要がある。表1は日本ネットワークセキュリティ協会（以下、JNSA）が定めた「情報セキュリティ市場分類区分定義表―2012年度版―」[8]の概要を整理したものである。後述するように、JNSAは経済産業省の委託調査として、日本における情報セキュリティ市場に関する調査を2004年度以来実施している。JNSAの独自調査として実施された2010年度以降の分も含めて最も長期にわたる公開データである。そこで、本稿では統計データの利用可能性にも配慮してJNSAの「情報セキュリティ市場分類区分定義表―2012年度版―」に準拠して、情報セキュリティ市場を定義する。なお、情報セキュリティに関するハードウェアやソフトウェアを総称して「情報セキュリティツール」と表現する。これ以外は、概ね前述の情報セキュリティ対策に対応したものである。

(8) 日本ネットワークセキュリティ協会「情報セキュリティ市場分類区分定義表―2012年度版―」2013.5.20. <http://www.jnsa.org/result/2013/surv_mrk/2012fymarketresearchreport_apx.pdf>

表1　情報セキュリティ市場の分類（大分類レベル）

市場区分	大分類	説明
情報セキュリティツール（情報システムに関するソフトウェア製品、ハードウェア製品の市場）	統合型アプライアンス	アプライアンス製品*1で、ネットワーク脅威対策又はコンピュータセキュリティ対策の機能のいずれか一方の機能を必ず含み、かつ情報セキュリティツールの以下の大分類のうち複数の大分類項目にまたがる機能を提供する製品。
	ネットワーク脅威対策製品	ネットワーク上の脅威に対応するために、ネットワークの境界に置いて通信の制御と管理を行う製品。ソフトウェア、アプライアンス製品の両方を含む。ファイアウォール、VPN*2、侵入検知・防止その他の不正侵入、不正プログラムの挿入、盗聴などの対策製品。
	コンピュータセキュリティ対策製品	ウイルスその他の不正プログラムやスパムメールの検出・排除・無害化・警告する製品や、有害なウェブサイトへのアクセス制御製品、情報流出防止機能製品。
	アイデンティティ・アクセス管理製品	個人認証のためのソフトウェアやハードウェア製品やアクセス管理機能を有する製品など。
	システムセキュリティ管理製品	コンピュータネットワークシステムの状態を監視、解析、管理する機能を持つ製品。
	暗号製品	データの暗号化機能を持つ製品。
情報セキュリティサービス（情報セキュリティに関するサービス市場）	情報セキュリティ・コンサルテーション	情報セキュリティポリシーや情報セキュリティ管理全般のコンサルテーション、情報セキュリティに関する診断や認証、監査及び認証取得の支援サービス。
	セキュアシステム構築サービス	情報セキュリティシステム又は情報システムのセキュリティに関する設計、仕様策定、導入・導入支援、セキュリティ製品の選定・選定支援などのセキュリティシステム構築サービス。
	セキュリティ運用・管理サービス	情報セキュリティシステム又は情報システムのセキュリティ対策機器等の運用、管理、セキュリティ状態の検査・監視を行うサービスのほか、電子証明書の発行、セキュリティ情報提供サービス及び緊急時の対応、復旧に関するサービス。
	情報セキュリティ教育	情報セキュリティに関する教育の提供、関連する資格の認定等のための研修など。
	情報セキュリティ保険	情報漏えい等、情報セキュリティに関する損害を補償する保険。

（注）*1　ハードウェアとソフトウェアを一体化して特定の機能を提供する製品。
*2　Virtual Private Network. ネットワーク上の通信に暗号処理をするなど、第三者による盗聴をできなくして、実質的に閉じたネットワークを構築する機能。
（出典）日本ネットワークセキュリティ協会「情報セキュリティ市場分類区分定義表―2012年度版―」2013.5.20. <http://www.jnsa.org/result/2013/surv_mrk/2012fymarketresearchreport_apx.pdf>を基に筆者作成。

個々の企業は、これらのうち1以上のツールやサービスを提供する。ただし、専ら情報セキュリティに関するツールやサービスの提供を業務とする専業企業もあれば、他の事業を展開する企業が情報セキュリティに関するツールやサービスを提供する場合もある。たとえば、一般の情報システムに関するコンサルテーションや構築支援を行う企業が、その一環として情報システムのセキュリティ面に関してツールやサービスを提供する場合、経営コンサルタント企業が情報セキュリティに関するコンサルテーションサービスを提供する場合、スマートフォンやタブレット端末及びそのアプリのベンダが情報セキュリティのためのソフトウェアなどを提供する場合、ネットワークを提供する電気通信事業者やクラウドサービスを提供する企業が情報セキュリティに関するツールやサービスを提供する場合など、多様な組合せがある。

（3）情報セキュリティ市場に関するデータ源

（i）富士キメラ総研「ネットワークセキュリティビジネス調査総覧」

情報セキュリティ市場に関する調査として最も早くから実施されてきたのは、1998年以来毎年発表されている富士キメラ総研の「ネットワークセキュリティビジネス調査総覧」であろう。2009年版からは市場編と企業編に分けて刊行されている。同資料は市場調査会社によるもので、聞き取り調査により事業者ごと、情報セキュリティに関するサービス（同資料では「ネットワークセキュリティサービス」という。）やツール（同資料では「ネットワークセキュリティ製品」という。）の種類ごとに詳細に市場動向を調査している。同資料は、関連企業への聞き取り調査に基づくため、対象企業等の捕捉が十分でない可能性がある一方、対象となる情報セキュリティサービス及びツールを、対象外のものと厳密に区別して把握できている可能性がある[(9)]。

本資料は非常に詳細で有益な面があるが、資料の性質上、利用には厳しい制限が課されている。そのため本稿では用いないこととする。

（ii）日本ネットワークセキュリティ協会「情報セキュリティ市場調査」

日本ネットワークセキュリティ協会（JNSA）による「情報セキュリティ市場調査」は2004年度以来、今日まで継続的に実施、公表されているものである。当初は経済産業省の委託調査として、「情報セキュリティ産業の実態を把握し、我が国における情報セキュリティの普及度と到達度を明らかにするための基礎データの提供を目的」[(10)]として開始された。調査は、「国内情報セキュリティ販売事業者に対するアンケート調査をベースに、官民の各種統計や分析資料ならびに国内事業者へのヒアリング結果を加味して、国内情報セキュリティ市場の市場規模実績並びに予測数字を導き出した」[(11)]ものである。ただし、2005年度からは、アンケート調査を実施しつつも、回答を得られなかった企業等のうち主要企業に関しては、サンプリング調査と称して、独自に有価証券報告書、ウェブページ、製品資料等の外部公表資料などから事業規模を推計している[(12)]。また、本調査は2009年度までは経済産業省の委託調査[(13)]として実施されたが、2010年度以降はJNSAの独自事業として継続している。ただし、2010年度と2011年度は東日本大震災があったことなどから、2か年分をまとめて発表している[(14)]。

JNSA独自調査における推計の範囲は「国内で情報セキュリティに関するツール、サービス等の提供を事業として行っている事業者（輸入販売、再販売を含み、輸出を含まない）」[(15)]で、国内情報セキュリティ市場の規模を供給事業者側から把握しようとしてきた従前の調査と実質的

⑼　これらの特性はともに、後述する他の調査に比べて市場規模を相対的に小さく推計する要因となりうる。あくまでも相対的なものであり、どちらが正しいといった判断はできない。なお、非常に詳細に調査しているものの、データの収集や推計の方法論については具体的に示されていない。

⑽　日本ネットワークセキュリティ協会「国内情報セキュリティ市場調査―調査報告書―」2005.3, p.1. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/16FY_ISmarket_research_report.pdf>

⑾　同上, p.2.

⑿　日本ネットワークセキュリティ協会「情報セキュリティ市場調査報告書」2006.3, p.12. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/17FY_ISmarket_research_report.pdf>

⒀　2007年度以降の報告書は、以下のURLから入手できる。なお、2006年度の調査報告書は発表されていない。2007年度版 <http://www.meti.go.jp/policy/netsecurity/downloadfiles/19FY_ISmarket_research_report.pdf>; 2008年度版 <http://www.meti.go.jp/policy/netsecurity/downloadfiles/20FY_ISmarket_research_report.pdf>; 2009年度版 <http://www.meti.go.jp/policy/netsecurity/downloadfiles/21FY_ISmarket_research_report.pdf>

⒁　日本ネットワークセキュリティ協会「2010～2011年度 情報セキュリティ市場調査報告書 v1.0 r1」2012.7.4. <http://www.jnsa.org/result/2010/surv/mkr/index.html>

⒂　同上, p.57.

には変わらない。しかし、調査方法に関しては変化がある。すなわち、経済産業省の委託調査であった2009年度まではアンケートの対象者の抽出方法を明確には示さず、「国内情報セキュリティ販売事業者」等と表現していた。独自調査になってからは、アンケート対象を「JNSA会員企業」と明記したが、結果としてアンケート調査の対象事業者数は、委託調査の時代に比較して大幅に減少した[16]。アンケート調査を補うために、「事業として何らかの形で情報セキュリティに関わっていると考えられる企業」について、有価証券報告書ウェブページ、製品資料等の外部公表資料などから事業規模を推計している点は、従前のサンプル調査と同じである。2012年度調査も2010、2011年度と同じ方法で推計した[17]が、2013年にはアンケート調査を見送り、サンプル調査（470社）のみに絞っている[18]。

（iii）ガートナー社による推計

経済産業省委託「情報セキュリティ市場調査」は、2010年度分はGartner Inc.[19]、2011年度分はガートナージャパン[20]（以下では、日本法人を含めて「ガートナー社」という。）が受託して実施している。いずれも、日本国内のみならず、世界の情報セキュリティ市場の動向も調査しており、両年度ともに米国ガートナー社（Gartner Inc.）が発表している市場動向報告[21]に基づいている。

市場分類は、JNSAが実施していた際の分類とは異なるが、ほぼ対応がつくように整理されている。ただし、JNSAが実施していた調査とは方法が全く異なるので、データの接続性は全く担保されていない。2010年度版のガートナー社の推計では、情報セキュリティサービス市場の規模は、JNSAの推計値とほぼ同じであるが、情報セキュリティツール市場の規模はJNSAの推計値の3分の1程度になっている。ガートナー社の2010年度版報告書は両者の差異とその要因を分析している。すなわち、JNSAが供給側からの推計であるため、代理店経由の場合など、本来は付加価値分（＝売上－仕入）を計上すべきところ、売上をそのまま計上しているので何重にも重複カウントすることになり、最終的なユーザの購入金額をはるかに上回る推計値になってしまう。ガートナー社はこれを回避するために、ベンダ側だけでなく、ユーザ側の調査も行いデータの検証を行っている。これが両者の違いの主要な要因ということになる。[22]

この分析には説得力がある。一方では、ガートナー社の推計にも弱点がある。第一に入手できるデータの期間が短い。経済産業省による委託調査は2011年度のガートナー社に対する委託調査までであり、その後のデータは公表されていない。ガートナー社も独自に推計して公表し

---

⑯　2009年度調査のアンケートの対象企業数は1,045社（有効回答133件）であったのに対して、2010、2011年度調査では145社（有効回答34件）になった。2009年度版　前掲注⑬, p.17; 同上, pp.57-58.

⑰　日本ネットワークセキュリティ協会「2012年度 情報セキュリティ市場調査報告書」2013.5, pp.53-54. <http://www.jnsa.org/result/2013/surv_mrk/>

⑱　日本ネットワークセキュリティ協会「2013年度 情報セキュリティ市場調査報告書 V1.0」2014.5, p.49. <http://www.jnsa.org/result/2014/surv_mrk/index.html>

⑲　Gartner Inc.「平成22年度コンピュータセキュリティ早期警戒体制の整備事業（各国情報セキュリティ政策等の動向に関する調査研究）―報告書（市場調査編）―」2011.3. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/22FY_ISmarket_research_report.pdf>

⑳　ガートナージャパン「平成23年度企業・個人の情報セキュリティ対策促進事業（情報セキュリティの市場調査）―調査報告書―」2012.3. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/23FY_ISmarket_research_report.pdf>

㉑　“Forecast: Security Software Markets, Worldwide”; “Forecast: Security Service Markets, Worldwide”; “Market Share: Security, Worldwide.” これらの市場動向報告は一般には公開されていない。

㉒　Gartner Inc.　前掲注⑲, pp.55-56.

ている様子はない。そのため入手できるデータは報告書2年分だけで、市場規模の実績の推計期間では2008年度から2010年度であり、市場規模の将来予測は2015年度までである。このため、特に実績に関して推計値が得られる期間が非常に短い。第二に、円ドル換算の困難がある。ガートナー社の推計は基本的にドル建てである。将来予測値を円換算する場合の換算レートが2011年以降は1ドル＝81.80円に固定して設定されている。しかし、2013年以降は円安が進み、1ドル＝100円以上の相場が続き、2014年末には120円に近い水準である。このような実勢レートで換算し直すと、極端な数字になり、見掛け上は日本の情報セキュリティ市場が急成長しているように見える。これが実勢を反映するものとは考えにくい。こうしたことから、ガートナー社のデータの利用には困難がある。

（iv）本稿で用いるデータ源

以上のほかにも、IDC Japanも2006年から、国内セキュリティ市場の分析と予測を実施し、一部についてはニュースリリースを発表している[23]。ただし、IDC Japanは市場調査会社であるので、報告書は一般公開されておらず、情報の入手は困難である。また、独立行政法人情報処理振興機構は「情報セキュリティ白書」を2006年から継続して出版しており、2009年度版からは情報セキュリティ産業の動向に1章を割いている[24]。そこでは情報セキュリティ市場の規模に関するデータを紹介しており、その典拠として、経済産業省調査の委託先がガートナー社に代わった後もJNSAの情報セキュリティ市場調査を用いている。

以上の調査データの特性に関する検討を踏まえ、本稿ではまず、JNSAの「情報セキュリティ市場調査」を基準データに位置付けて、情報セキュリティ市場の規模を推計する。その上で他のデータ源の推計値を対照データとして参照し、JNSAのデータの妥当性を評価する。

Ⅱ　日本の情報セキュリティ産業の現状

1　情報セキュリティ市場の実態

（1）情報セキュリティ市場の成長

JNSAの情報セキュリティ市場調査に基づいて、情報セキュリティ市場の規模の経年変化を推計する。JNSAの情報セキュリティ市場調査は、長期データとして公表されていないので、公開データから時系列データを推計する。

JNSAの情報セキュリティ市場調査の推定値には、売上実績推定値、売上高見込推定値、売上高予測値の三種類がある。JNSAの情報セキュリティ市場調査のt年度版は基本的には、t年度に調査が実施され、t+1年に発表されている。そのため基本的には、t年度版報告書の場合、t-1年度に関しては前期の売上実績が判明しており、t年度に関しては当期の売上高の見込が推計されている状況にあり、t+1年度以降に関しては売上高は来期以降の予測値となる。これらに対応するJNSAによる推定値が、t-1年度の売上実績推定値、t年度の売上高見込推定値、t+1年

⑵3　例えば、IDC Japan「国内セキュリティ市場予測を発表」（プレスリリース）2014.5.27. <http://www.idcjapan.co.jp/Press/Current/20140527Apr.html>

⑵4　情報セキュリティ産業の動向に関する記述は徐々に短くなり、2014年版では独立の章ではなく、章の中の一節に位置付けられた。情報処理振興機構「2.9情報セキュリティ産業の規模と成長の動向」『情報セキュリティ白書　2014』2014, pp.116-119.

度以降の売上高予測値である。当然ながら、売上高見込推定値、売上高予測値は後年度の調査によって売上実績推定値に変更されることになる[25]。

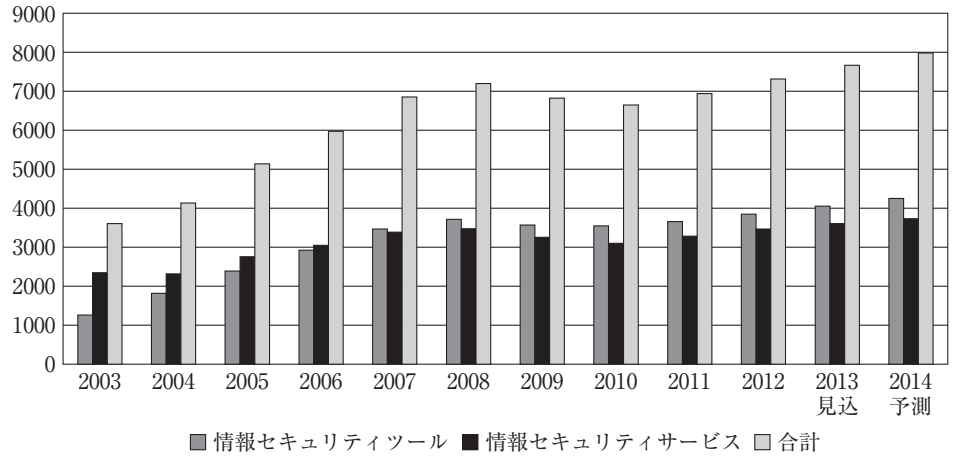
そこで、2003年度から2012年度までの売上実績推定値を各年の報告書から抽出する。その際に、後年度に売上実績推定値が改定された場合は、最新データを採用する。2013年度売上高見込推定値、2014年度売上高予測値については、「2013年度 情報セキュリティ市場調査報告書V1.0」の数値を採用する。こうして情報セキュリティ市場の規模の経年変化を推計した結果が、図1及び表2である。前述のように、この間に何度か推計方法が変わっているので、厳密にはデータの接続性はないことに留意する必要がある。もっとも、過去に遡って売上実績推定値を改定しているので、トレンドを大まかに把握する上では十分な精度であると思われる[26]。

図1、表2から理解できることは、日本の情報セキュリティ市場は2008年度までは順調に拡大し、その後は拡大が止まり、若干の減少も見られるが、ほぼ横ばいで今日に至るトレンドである。2008年にはリーマンショックがあり、2009年度、2010年度にわたり情報セキュリティ投資がやや後退したことがわかる。その後は緩やかな復調の兆しを見せている。2013年度、2014年度も拡大を続ける見込みである。

情報セキュリティツールと情報セキュリティサービスに分けると、2000年代前半の調査開始当時は、情報セキュリティサービスの方が市場の規模が大きかったが、情報セキュリティツールの拡大のペースが速く、2007年度以降は情報セキュリティツールの市場規模の方が若干大きくなっている。

表3には、2012年度の日本の情報セキュリティ市場の内訳を示した。分類別ではウイルス対策ソフトなどのコンテンツセキュリティ対策製品が最大である。これに並ぶのがセキュアシステム構築サービス、セキュリティ運用・管理サービスである。情報セキュリティシステムの設計、導入、構築などを行うセキュアシステム構築サービスは情報セキュリティシステム構築の

図1　日本の情報セキュリティ市場の規模（売上実績推定値、年度・億円）



（注）2012年度までは売上実績推定値、2013年度は売上高見込推定値、2014年度は売上高予測値。
（出典）日本ネットワークセキュリティ協会「情報セキュリティ市場調査報告書」（各年度版）を参考にして筆者作成。

⑵⑸　調査方法や推計方法の変更により、売上実績推定値も改定される場合がある。
⑵⑹　JNSA情報セキュリティ市場調査の枠組みの中でのトレンドを把握する上では問題ないが、後述するように、他のデータ源との比較においては規模感においてかなり隔たりがある。従って、規模感を把握する上では慎重に扱う必要がある。

表2　日本の情報セキュリティ市場の規模（売上実績推定値、年度・億円）

年度	情報セキュリティツール	情報セキュリティサービス	合　計
2003	1260	2347	3607
2004	1817	2316	4133
2005	2387	2752	5139
2006	2924	3047	5972
2007	3468	3387	6855
2008	3717	3476	7193
2009	3571	3250	6821
2010	3543	3100	6643
2011	3656	3285	6940
2012	3849	3465	7314
2013見込	4055	3607	7661
2014予測	4248	3730	7978

（注）2012年度までは売上実績推定値、2013年度は売上高見込推定値、2014年度は売上高予測値。
1億円未満を四捨五入しているため、内訳の計と合計が一致しない場合がある。
（出典）日本ネットワークセキュリティ協会「情報セキュリティ市場調査報告書」（各年度版）を参考にして筆者作成。

表3　日本の情報セキュリティ市場の分類別規模（売上実績推定値、2012年度・億円）

市場区分	大　分　類	金　額
情報セキュリティ市場 合計		7314
情報セキュリティツール　計		3849
	統合型アプライアンス	201
	ネットワーク脅威対策製品	521
	コンテンツセキュリティ対策製品	1470
	アイデンティティ・アクセス管理製品	688
	システムセキュリティ管理製品	551
	暗号製品	417
情報セキュリティサービス　計		3465
	情報セキュリティ・コンサルテーション	702
	セキュアシステム構築サービス	1389
	セキュリティ運用・管理サービス	1031
	情報セキュリティ教育	266
	情報セキュリティ保険	76

（注）1億円未満を四捨五入しているため、内訳の計と合計が一致しない場合がある。
（出典）日本ネットワークセキュリティ協会「2013年度 情報セキュリティ市場調査報告書 V1.0」2014.5, p.3. <http://www.jnsa.org/result/2014/surv_mrk/index.html>を基に筆者作成。

主要部分であり、従来から一定の規模を維持している。情報セキュリティシステムの運用や監視、診断やインシデントへの対応などのセキュリティ運用・管理サービスは成長が続いている分野であり、2012年度には主要分野になっている。次々と出現する脅威や脆弱性に対応するために、セキュリティ運用・管理サービスの重要性は今後も高まると思われる。

（2）情報セキュリティ市場データの妥当性の検討

JNSAの推計によると情報セキュリティ市場の規模は、2007年度以降はほぼ7000億円前後である。この推計値の妥当性について検討する。

まず、前述の他のデータ源と比較検討する。2009年度、2010年度はガートナー社の経済産業省委託調査報告書と、2012年度、2013年度はIDC Japanのニュースリリースの数値と比較が可能である[27]。そこで、これらの推計値を比較して表4に示した。

表4によると、情報セキュリティツールに関しては、JNSAの推計値がもっとも大きく、IDC Japanがその約6割、ガートナー社はJNSAの約3分の1である。一方、情報セキュリティサービスに関しては、JNSAがもっとも小さく、JNSAに対してガートナー社が1.2倍前後、IDC Japanが1.6倍強である。これらは、調査時期が異なるのみならず、調査方法や定義も異なる可能性があるので、あくまで目安である。しかし、この結果から、JNSAの推計値は、情報セキュリティツールに関しては最大3倍程度の過大推計になっている可能性があり、情報セキュリティサービスに関しては過小推計になっており、最大で1.6倍程度まで大きく見積もりうることがわか

表4　情報セキュリティ市場の推計値の比較

年度	データ源	情報セキュリティツール	情報セキュリティサービス	合　計
2009	JNSA*1	3571（100.0）	3250（100.0）	6821（100.0）
	Gartner Inc.*2	1140（ 31.9）	3820（117.5）	4960（ 72.7）
2010	JNSA*3	3543（100.0）	3100（100.0）	6643（100.0）
	ガートナージャパン*4	1253（ 35.4）	3883（125.3）	5136（ 77.3）
2012	JNSA*5	3849（100.0）	3465（100.0）	7314（100.0）
	IDC Japan*6	2227（ 57.8）	5701（164.5）	7928（108.4）
2013	JNSA*7	4055（100.0）	3607（100.0）	7661（100.0）
	IDC Japan*8	2476（ 61.1）	6043（167.5）	8519（111.2）

（注）数字は市場規模（億円）、カッコ内はJNSA（日本ネットワークセキュリティ協会）の推計値を100とした場合の指数。1億円未満を四捨五入しているため、内訳の計と合計が一致しない場合及び表中の数値を用いて計算した指数と指数として掲載されている数値が厳密には一致しない場合がある。

*1　日本ネットワークセキュリティ協会「2010～2011年度 情報セキュリティ市場調査報告書 v1.0 r1」2012.7.4, p.3. <http://www.jnsa.org/result/2010/surv/mkr/index.html>

*2　Gartner Inc.「平成22年度コンピュータセキュリティ早期警戒体制の整備事業（各国情報セキュリティ政策等の動向に関する調査研究）―報告書（市場調査編）―」2011.3, p.46. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/22FY_ISmarket_research_report.pdf>

*3　日本ネットワークセキュリティ協会「2012年度 情報セキュリティ市場調査報告書」2013.5, p.3. <http://www.jnsa.org/result/2013/surv_mrk/>

*4　ガートナージャパン「平成23年度企業・個人の情報セキュリティ対策促進事業（情報セキュリティの市場調査）―調査報告書―」2012.3, p.8. <http://www.meti.go.jp/policy/netsecurity/downloadfiles/23FY_ISmarket_research_report.pdf>

*5　日本ネットワークセキュリティ協会「2013年度 情報セキュリティ市場調査報告書 V1.0」2014.5, p.3. <http://www.jnsa.org/result/2014/surv_mrk/index.html>

*6　IDC Japan「国内セキュリティ市場予測を発表」（プレスリリース）2014.5.27. <http://www.idcjapan.co.jp/Press/Current/20140527Apr.html> の数値を基に推計。

*7　日本ネットワークセキュリティ協会　前掲注(*5)なお、2013年は売上高見込。

*8　IDC Japan　前掲注(*6)

（出典）上記資料を参考に推計して筆者作成。

27　JNSAの推定値は2013年度に関しては売上高見込。また、IDC Japanに関しては推計方法が示されていないので厳密な推論はできない。

る。少なくとも、JNSAの推計値は、情報セキュリティツールに関して過大推計、情報セキュリティサービスに関して過小推計になっている可能性があることは了解しておく必要がある。

このようなJNSAの推計値の特性は、どのような要因によるものと考えられるだろうか。情報セキュリティツール市場に関しては、前述のように、JNSAの推計値は販売ルートの途中に位置づけられる企業の売上が重複計上されている可能性がある。情報セキュリティサービス市場に関しては、JNSAの推計では、中小規模の独立系ソフトウェアハウス、システムハウス、システムインテグレータ等と呼ばれる企業群が、主たる業務であるソフトウェアやハードウェアの開発やインテグレーションとともに情報セキュリティサービスを扱っているケースを十分に捕捉できていない可能性がある。平成21（2009）年経済センサス（基礎調査）によれば、産業分類上のソフトウェア業及びインターネット附随サービス業[28]の2009年の事業所総数は、それぞれ31,031事業所、5,924事業所、このうち単独事業所が18,964事業所、4,724事業所、本所・本社・本店が3,187事業所、380事業所なので、企業数は22,151社、5,104社となる[29]。しかも、これらの企業の大多数は10人未満の小規模企業である。これらの企業の少なからぬ部分が、主業務のほかに情報セキュリティサービスを提供している可能性がある。JNSA調査はこれらの多数の、しかし小規模な企業による情報セキュリティサービスを捕捉できていない可能性が高い。もちろん、ガートナー社やIDC Japanの推計値も同じく過小推計の可能性がある。

情報セキュリティ市場規模をツールやサービスの供給側から調査することによる過小推計や過大推計を補正するには、需要側から市場規模を推計する方法がある。JNSAの情報セキュリティ市場調査報告書は、独自調査として実施された2010～2011年度版以降、経済産業省「情報処理実態調査」から得られる1社当たり情報セキュリティ対策費用[30]と調査回答企業数、調査対象企業数等を用いて、需要側から情報セキュリティ対策費用総額を推計している。「情報処理実態調査」の数値は概数であり、また情報セキュリティに関する支出項目が明確に定義されていないため非常に粗雑な推計になるが、市場の規模感を把握する方法としては意味がある。表5にJNSAによる需要側からの情報セキュリティ市場規模の推計を整理した。

表5の需要側からの情報セキュリティ市場規模の推計値は9300億円から9800億円で、3年ともJNSA調査による推計値の1.4倍前後に収まっている。3年とも約1.4倍であったことは偶然なのか、一定の傾向を示すものかは判断できないが、JNSAによる情報セキュリティ市場全体の推計値は過小推計になっていると判断してよいと思われる。

以上のことから、日本における情報セキュリティ市場の規模については以下のように総括できる。すなわち、①2000年代当初から2008年まで急速に拡大し、その後は比較的安定している、②2012年度の情報セキュリティツール市場の規模は約1350億円[31]ないし3850億円、情報セキュ

⑵8 「大分類G　情報通信業　説明及び内容例示」『日本標準産業分類（平成25年10月改定）（平成26年4月1日施行）』（総務省ウェブページ <http://www.soumu.go.jp/main_content/000290726.pdf>）によれば、小分類（391）ソフトウェア業はその下位分類に、受託開発ソフトウェア業（3911）、組込みソフトウェア業（3912）、パッケージソフトウェア業（3913）、ゲームソフトウェア業（3914）を含む。小分類（401）インターネット附随サービス業はその下位分類に、ポータルサイト・サーバ運営業（4011）、インターネット利用サポート業（4013）等を含む。ポータルサイト・サーバ運営業（4011）にはウェブ情報検索サービス業、インターネット・ショッピング・サイト運営業が、インターネット利用サポート業（4013）には、電子認証業、情報ネットワーク・セキュリティ・サービス業が例示されている。

⑵9 産業（小分類），従業者規模（15区分），本所・支所（3区分），経営組織（4区分）別民営事業所数及び従業上の地位（6区分），男女別従業者数－全国⑵F 電気・ガス・熱供給・水道業～K 不動産業，物品賃貸業「平成21年経済センサス―基礎調査―」2011.6.3. 政府統計の総合窓口 <http://www.e-stat.go.jp/SG1/estat/Xlsdl.do?sinfid=000012658614>

⑶0 選択肢に示された金額の階級の中間値の加重平均。

表5　情報セキュリティ市場規模の需要側からの推計

年　度	1社当たり情報セキュリティ対策費用（万円）	調査回答企業数（社）	調査回答企業全体の情報セキュリティ対策費用（億円）	回答率（%）	調査対象企業全体の情報セキュリティ対策費用（億円）［A］	JNSA調査による推計値（億円）［B］	［A］/［B］	JNSA報告書
2008年度	1030	5021	5172*1	52.9	約9800*2	7193	1.36	2010～2011年度
2010年度	1070	4537	4855	50.9	約9500	6643	1.44	2012年度
2011年度	979	4971	4867	52.3	約9300	6640*3	1.40	2013年度

（注）1社当たり情報セキュリティ対策費用、調査回答企業数、回答率は経済産業省「情報処理実態調査」に基づく。JNSA（日本ネットワークセキュリティ協会）報告書には誤記があるので改めて計算した。［A］の数値は概算値を掲載しているため、表中の数値を用いて計算した［A］/［B］と掲載されている［A］/［B］の数値が厳密には一致しない場合がある。
*1　JNSA報告書には6051億円と記載されているが、計算すると5172億円になる。
*2　JNSA報告書には示されておらず、独自に計算したもの。
*3　JNSA報告書は6643億円と記載しているが、6640億円が正しい。
（出典）日本ネットワークセキュリティ協会「2010～2011年度 情報セキュリティ市場調査報告書 v1.0 r1」2012.7.4, p.101. <http://www.jnsa.org/result/2010/surv/mkr/index.html>; 日本ネットワークセキュリティ協会「2012年度 情報セキュリティ市場調査報告書」2013.5, p.74. <http://www.jnsa.org/result/2013/surv_mrk/>; 日本ネットワークセキュリティ協会「2013年度 情報セキュリティ市場調査報告書 V1.0」2014.5, p.70. <http://www.jnsa.org/result/2014/surv_mrk/index.html> を参考に筆者作成。

リティサービス市場の規模は約3450億円ないし5700億円、情報セキュリティ市場全体では約4800億円ないし約1兆円[32]であると推計できる、③JNSAの推計方法は、情報セキュリティツール市場の規模は過大推計、情報セキュリティサービス市場の規模は過小推計、情報セキュリティ市場全体としては過小推計である可能性がある。

10兆円を超える売上の産業が多数あり、1企業で数兆円を売り上げる企業が存在する日本経済の中では、1兆円は産業規模としては決して大きくない。

2　情報セキュリティ産業の構造

次に、情報セキュリティ産業の産業構造について検討する。前述の経済センサスのデータが示唆するように情報セキュリティ市場には、小規模企業を含む多数のソフトウェア関連企業が関係する可能性がある。このことも情報セキュリティ産業の産業構造の特色の一つである。

多数の企業が関わる情報セキュリティ産業の全体像を明らかにすることは困難である。ただし、JNSAの情報セキュリティ市場調査の対象となっているような主要企業に関しては、どのような企業が参入しているのか、ある程度理解できる。表6はJNSAの2013年度調査のサンプリング調査の対象となった企業の業態を整理したものである。

表6は業態を8分類しているが、このうち情報セキュリティを主たる事業分野としている業態（以下、「情報セキュリティ専業」という。）は、海外ベンダまたはその日本法人、セキュリティサービス提供企業の2種類であり、残りの6種類は他の事業とともに情報セキュリティに関するツールやサービスを提供する業態である。国内のセキュリティツールベンダは専業の場合もあると思われるが、ソフトウェアハウス、システムハウス、その他の企業が情報セキュリティツール

⑶1　JNSAの2012年情報セキュリティツール市場の推計値3849億円に2010年のガートナー社との比率0.354を乗じて推計。
⑶2　JNSAの2012年情報セキュリティ市場全体の推計値7314億円に、表5から得られる1.4を乗じて推計。

表6　情報セキュリティ企業の業態別分布

業　　態	概　　要	会社数
海外ベンダまたはその日本法人	セキュリティツール･サービスを提供する海外ベンダまたはその日本法人。	79
国内のセキュリティツールベンダ	個人認証、暗号等のセキュリティツールのメーカ等。ベンチャー系のソフトウェアハウス、システムハウスも多く見られる。	97
総合商社、技術商社等の流通企業	海外セキュリティ企業のツールの代理店、販売店的な役割を果たす企業や技術的対応能力を有する販売特化型企業など。	56
セキュリティツールを代理店等として扱うシステムインテグレーション、ネットワークインテグレーション企業	システムインテグレーション、ネットワークインテグレーション企業がセキュリティツールの代理店、販売店として扱うケースや、技術商社がシステムインテグレーション、ネットワークインテグレーション業務に重点を置くようになり、セキュリティツールを扱うケース。	87
大手システムインテグレータ企業	メインフレームコンピュータメーカや通信事業者などの大手企業のほか、中小の独立系システムインテグレーション専業企業が、システムコンサルテーションの一環としての情報セキュリティコンサルテーションを行ったり、システムインテグレーションに際してセキュリティシステムの構築を担う。	28
コンサルティング企業	経営コンサルティング企業が情報セキュリティコンサルティングを行う。	24
セキュリティサービス提供企業	セキュリティサービスに特化したコンサルティング、情報セキュリティシステムの診断、運用・管理、インシデント対応など情報セキュリティの専門サービスを提供する。小規模企業が多い。海外事業者の参入もある。	73
その他	情報セキュリティ保険事業者など。	26
計		470

（出典）日本ネットワークセキュリティ協会「2013年度 情報セキュリティ市場調査報告書 V1.0」2014.5, pp.59-62. <http://www.jnsa.org/result/2014/surv_mrk/index.html>を参考に筆者作成。

も扱っているケースが多いと思われる。対象企業470社のうち情報セキュリティ専業は152社程度と見積もられる。これは全体の約3分の1に相当する。情報セキュリティ専業企業は必ずしも多くない。また、情報セキュリティ専業企業の半分以上はセキュリティツール・サービスを提供する海外ベンダ又はその日本法人である。また、セキュリティサービス提供企業にも海外企業の参入がある。つまり、情報セキュリティ専業企業のかなりの部分は海外企業に支えられている。このことも情報セキュリティ産業の顕著な特色の一つである。

情報セキュリティ産業の企業規模や創業時期にはどのような特色があるのだろうか。この点に関しては、JNSA情報セキュリティ市場調査からはわからないので、独自に情報セキュリティに関連する団体の会員リストなどから420社を抽出し、各社の企業規模、創業時期、情報セキュリティ専業企業か否かを調べた。企業規模としては、業態、業種に依存しない指標として従業員数を調べた(33)。

企業規模の分布を表7に示した。情報セキュリティ専業企業は非専業と比較して圧倒的に小規模企業が多い。従業員数301人以上は4社のみ（1千人以上は2社）であり、非専業の中には大手コンピュータメーカや通信事業者などの大手システムインテグレータ企業が多数含まれているのと比較して顕著に異なっている。

表8には創業時期別の分布を示した。情報セキュリティに関連する企業全般に若い企業が多い。2000年以降に創業した企業が4割程度を占める。特に情報セキュリティ専業企業に関しては2000年以降に創業した企業が多い。情報セキュリティ専業企業の7割程度は2000年以降に創業している。情報セキュリティに関する顕著な脅威が発生するようになったのが2000年以降であることを考えれば、当然の結果であるといえる。なお、詳細なデータは省くが、専業、非専

表7　情報セキュリティ企業の規模別分布（企業数）

従業員数	専　業	非専業	計
50人以下	30	67	97
300人以下	12	67	79
301人以上	4	166	170
不明	25	49	74
計	71	349	420

（出典）筆者作成

表8　情報セキュリティ企業の創業時期分布（企業数）

創業年	専　業	非専業	計
1999年まで	18	239	257
2000年以降	50	106	156
不明	3	4	7
計	71	349	420

（出典）筆者作成

業ともに、2005、2006年頃までの創業が多く、その後はペースは落ちたが創業は続いている。このような状況から、情報セキュリティ産業は新しい産業、成長途上の産業といえよう。

断片的なデータからの推計ではあるが、以上のように、情報セキュリティ産業の構造にはいくつかの特徴がある。すなわち、①小規模企業を含む多数のソフトウェア関連企業が情報セキュリティ市場に参入しており、情報セキュリティ専業企業は必ずしも多くない、②情報セキュリティ専業企業のかなりの部分が海外企業に支えられている、③情報セキュリティ専業企業は非専業と比較して圧倒的に小規模企業が多い、④情報セキュリティ市場に参入している企業には全般に若い企業が多く、特に情報セキュリティ専業企業に関しては2000年以降に創業した企業が多い、⑤専業、非専業ともに2005、2006年頃までに創業した企業が多いが、その後ペースは落ちているものの新規創業は続いている。

Ⅲ　日本の情報セキュリティ産業の展望

1　日本の情報セキュリティ産業を取り巻く環境

（1）情報セキュリティ市場に影響を及ぼす要因

情報セキュリティ市場に影響を及ぼす要因としては以下の事項が考えられる。

㉝　対象企業は以下の団体等の会員企業（個人経営等を含む）一覧から重複を除く420社を抽出した。日本ネットワークセキュリティ協会（調査対象企業等157社。以下同様）、日本スマートフォンセキュリティ協会（152社）、日本セキュリティ監査協会（84社）、データベース・セキュリティ・コンソーシアム（23社）、日本クラウドセキュリティアライアンス（16社）、セキュリティ・エデュケーション・アライアンス・ジャパン（正会員7社）、日本セキュリティ・マネジメント学会（賛助会員30社）、経済産業省平成26年度情報セキュリティ監査企業台帳（326事業所 <http://www.meti.go.jp/policy/netsecurity/is-kansa/download/is-kansa2014.xls>）。

抽出企業に関して、各社のウェブページを2014年11月の1か月間に閲覧し、企業概要等から従業員数、設立年を調査した。また、業務内容から情報セキュリティ専業企業か否かを推定した。情報セキュリティツール又は情報セキュリティサービス専業の企業のほか、それらから派生して一般的なシステムコンサルティング等を一部実施している場合も主要業務が情報セキュリティの場合は情報セキュリティ専業企業とした。記載方式が統一されていないので、厳密なデータではないが、大まかな傾向を把握することは可能である。

本稿が抽出した420社はJNSA2013年度情報セキュリティ市場調査のサンプリング調査の対象企業数の470社の約9割に相当し、主要な企業に関しては抽出できていると推測できる。一方、情報セキュリティ専業企業か否かに関しては、420社中71社が情報セキュリティ専業であると判定した。全体の6分の1である。JNSA情報セキュリティ市場調査では専業企業がおよそ3分の1であるので、その半分程度に相当する。判断基準が同じではないので単純に比較できないが、対象企業が異なっている可能性もある。以下の分析では、JNSA情報セキュリティ市場調査のデータと一貫性がないことに留意する必要がある。

（i）情報セキュリティに関する脅威

情報セキュリティ市場の消長を左右する直接的な要因は、情報セキュリティに関する脅威であることは言うまでもない。顕著なインシデントが発生すれば、組織には何らかの対策を取ろうというインセンティブが働く。次から次へと新しいタイプの脅威が登場するので、情報セキュリティツールや情報セキュリティサービスに対する需要が途絶えることはないだろう。

（ii）IT 環境の変化

企業等組織が業務で利用するサーバや端末機能を有するPC、プリンタその他のデバイスなどのコンピュータシステム[34]は、性能の変化や減価償却その他の理由で一定の年限を過ぎるとリプレースされる。ソフトウェアも、ビジネスの変容や新規事業等への対応のため、またハードウェアの進展に合わせるために一定の期間を経ると更新することになる。これらを支えるICT技術や通信環境などの変化もシステム更新やソフトウェア更新の引き金になる。これらのIT環境の変化は、微細な変化を積み重ねることもあれば、幅広い範囲をまとめて更新する場合もある。まとまった更新の場合には、情報セキュリティツールやシステムも併せて更新する可能性が高く、IT投資の動向は情報セキュリティに対する需要を左右するとみられる。

JNSAの情報セキュリティ市場調査報告書は、システムやパッケージのシステムライフサイクル、事業のライフサイクル、ハードウェアの性能のサイクル、通信ネットワークの容量拡大のサイクルなどがIT投資サイクルに影響を及ぼすとし、IT投資サイクルを概ね3〜5年とみなしている。このIT投資のサイクルは、情報セキュリティツールやサービスの需要にも影響を及ぼすとしている。[35]

（iii）企業の経営状況と景気動向

情報セキュリティ市場の動向を左右する第3の要因は、企業の経営状況であり、その総体としてのマクロな景気動向である。情報セキュリティ市場の規模拡大がリーマンショックを経て低迷した事実からも、企業の経営状況がよくない場合には、たとえIT投資はしても、情報セキュリティに関する投資を控える可能性は高いことが類推できる。

（iv）制度的要因

第4の要因は、情報セキュリティに関連する法制度や各種セキュリティ標準、認証制度などの制度的要因である。次項で紹介するように、情報セキュリティに関連する法制度は、さまざまなインシデントの発生の影響も受けながら、2000年前後以降に急速に整備されてきた。これらの法制度は、程度の差はあれ、企業等の情報セキュリティに対する対応を強化する方向に働くものと思われる。

⑶④　インターネットが発達する前から、企業等組織においてはコンピュータを中心に各種デバイスを組合せて業務用システムを構築し、これをコンピュータシステムと呼び習わしてきた。今日でも組織内のシステムの骨格はこのコンピュータシステムである。ただし、近年ではイントラネット、インターネットが必須の要素となったことから、ネットワーク機能に関わるルータ、サーバ等もコンピュータシステムの一部と捉えられている。そのため、実態としては情報ネットワークシステムと異なるものではないが、減価償却や税制上の取扱等の経営資源としての側面を表現する際に、コンピュータシステムの語を用いることが多い。

⑶⑤　日本ネットワークセキュリティ協会　前掲注⑴⑧, pp.66-67.

（v）日本企業の情報セキュリティに対する態度

最後に、企業の情報セキュリティに対する態度に言及しておく必要がある。すなわち、日本企業はセキュリティ投資に消極的であるという特徴があると言われている。

ガートナー社の平成23年度報告書は、海外諸国と比較した日本の情報セキュリティ市場の特性を分析している。それによると、2010年から2015年までの情報セキュリティ市場の成長に関して日本市場の年平均成長率は7%と見込まれ、世界全体の年平均成長率約10%、欧州9.0%、北米8.9%よりも低い(36)。また、インタビュー結果を踏まえて、欧米は情報セキュリティ上のインシデントが発生するリスクを前提として、それにどう対処するかというコンプライアンスガイドラインがしっかりしており、そのためリスク管理に関するツールなどの売上が大きいが、日本は攻撃に対する防御を重視する傾向があるとしている(37)。

また、MM総研が実施した日米の企業に対するアンケート調査(38)によると、ICT投資に占める情報セキュリティ投資の比率は、米国が7.2%、日本が5.7%で、1.5ポイントの差があるが、従業員数5千人以上の大企業では8.4%、6.4%と2ポイントの差がついており、日本企業の方が情報セキュリティ投資に対して消極的な様子が見られる。日本は情報セキュリティ上の脅威に対する重層的な対応、セキュリティ監視・運用サービスの利用などは進んでいない(39)。

このように、日本企業の情報セキュリティに対する取組の相対的消極性、アプローチの違いなどの情報セキュリティに対する態度には独自性がある。日本企業の情報セキュリティに対する態度が変われば日本の情報セキュリティ市場は新しい方向に向かう可能性がある。

（2）情報セキュリティ市場に影響を及ぼす法制度

情報セキュリティ市場に影響を及ぼす法律等には多様なものがある。表9は、情報セキュリティ市場に対する影響の及ぼし方に注目して、主要な法律を整理したものである。

表中の①は、サイバー犯罪、迷惑メール等の防止等を定める法律等である。これらは、サイバー犯罪、迷惑メール等の禁止や違反者に対する罰則を定めるものであるが、同時にそれらに対する防御措置の導入など、情報セキュリティ対策の根拠や誘因として機能している。例えば、「不正アクセス行為の禁止等に関する法律」（平成11年法律第128号）は、不正アクセス行為の禁止、違反した者に対する罰則を定めると同時に、アクセス管理者に不正アクセス行為から防御するために必要な措置を講ずることを求めるもので、企業が防御措置を講じる契機になる。また「電気通信事業法」（昭和59年法律第86号）は電気通信事業者による検閲の禁止、秘密の保護、差別的扱いの禁止を定めているが、「特定電子メールの送信の適正化等に関する法律」（平成14年法律第26号）第11条（電気通信役務の提供の拒否）は、電気通信事業者が迷惑メール等に対する対策を講じることを可能にする根拠となっている。サイバー犯罪、迷惑メール等の防止等を定める法律等はこのような形で情報セキュリティ市場の動向に影響を及ぼしうる。

---

(36)　ガートナージャパン　前掲注(20), pp.65-74.

(37)　同上, p.90.

(38)　渡辺克己ほか「日米企業の情報セキュリティ投資動向―多様化する情報セキュリティの脅威に関心高まるも、セキュリティ投資で後れをとる日本企業―」『M&D Report』No.213, 2014.3, pp.7-8.

(39)　導入しているツールやサービスに関しても、ウイルス対策製品、スパムメール対策製品は日米ともに導入率は約9割で高いが、Webアプリケーションファイアウォール（日41.8%、米70.9%）、統合型アプライアンス製品（日37.2%、米62.5%）、ウイルス対策のセキュリティ監視・運用サービス（日34.7%、米67.7%）、不正侵入検知システム・不正侵入予防システム（日32.7%、米62.5%）、スパムメール対策のセキュリティ監視・運用サービス（日30.1%、米64.1%）などでは、米国の方が導入が進んでいる。同上。

表9　情報セキュリティ市場に影響を与える法律等

法律の趣旨	法　　律
①サイバー犯罪、迷惑メール等の防止等	・不正アクセス行為の禁止等に関する法律（平成11年法律第128号） ・特定電子メールの送信の適正化等に関する法律（平成14年法律第26号） ・情報処理の高度化等に対処するための刑法等の一部を改正する法律（サイバー刑法）（平成23年法律第74号）［不正指令電磁的記録に関する罪（いわゆるコンピュータ・ウイルスに関する罪）を刑法（明治40年法律第45号）に新設］ ・サイバー犯罪に関する条約（平成24年条約第7号）
②企業の内部統制（J-SOX法）	・会社法（平成17年法律第86号） ・証券取引法等の一部を改正する法律（平成18年法律第65号）［金融商品取引法（昭和23年法律第25号）の一部改正］
③IT利用基盤の整備	・電子署名及び認証業務に関する法律（平成12年法律第102号） ・書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律（IT書面一括法）（平成12年法律第126号） ・個人情報の保護に関する法律（平成15年法律第57号） ・民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（e-文書法）（平成16年法律第149号）
④行政のICT基盤の整備	・行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号） ・行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）（平成25年法律第27号）
⑤その他（基本法）	・高度情報通信ネットワーク社会形成基本法（IT基本法）（平成12年法律第144号） ・サイバーセキュリティ基本法（平成26年法律第104号）

（出典）筆者作成

表中の②は、企業の内部統制に関する制度である。複数の法律により実現される制度で、厳密には法律ではないが、米国のSOX法（Sarbanes-Oxley Act of 2002, P.L. 107-204）に倣って、日本版SOX法、J-SOX法等と呼ばれる。株式市場等が健全であるためには、企業が粉飾決算、虚偽記載など不適切な情報を流さないことが前提である。また、不正取引や違法行為など不適切な方法で業務を行うことも市場の健全性を損なう。適正に業務が行われるように企業内部の体制を整備、維持することが内部統制であり、内部統制が適切であることを対外的に保証することが必要である。そのための枠組み等を示すのがいわゆるJ-SOX法である。今日の企業経営にITシステムは欠かせない。内部統制を行うためには、ITシステムが適切に運用されなければならない。そのためには、例えばITシステムに対する不正アクセスを許さないことが必要であり、ユーザ認証、アクセス管理が必要であり、また情報漏えいやデータ改ざんを防止する仕組みが必要である。結局、これらのことは情報セキュリティ対策そのものであり、内部統制のためには情報セキュリティの確保が前提になる。また、ITシステムのセキュリティ対策が適切であることを検証し、対外的に明示するために情報セキュリティ監査を受けることも有効である。このように、企業の内部統制の要請は、情報セキュリティ需要を生む要因となる。

③は、IT化の進展に伴いそれを活用するための根拠や手続を定めるものである。電子商取引などの場面で用いられる電子署名のルールを定める、書面による手続に代えて電子的に文書を送付することを認める、IT技術の進展に伴い利用が拡大している個人情報の利用と保護のルールを定める、文書を電子化する場合のルールを定める等、IT利用基盤を整備するものである。これらの法制度も認証技術、暗号、個人情報保護その他の情報セキュリティツールやサービスによって支えられるものであり、情報セキュリティ需要の拡大要因となる。

ITの利用は民間部門に限るものではなく、当然ながら行政部門でもIT利用が推進されている。

これが④である。行政機関等の保有する個人情報に関しても利用と保護のルールが必要となるし、さらには行政の効率化等のために個人情報の一層の活用も求められる。これらの基盤となる法律も整備されている。これらに伴って情報セキュリティ対策も必要になる。これらは、情報セキュリティに対する官需の拡大要因となる。

⑤はその他である。「高度情報通信ネットワーク社会形成基本法」（平成12年法律第144号）、サイバーセキュリティ基本法などは、直接情報セキュリティ需要を喚起するものではないが、ITの活用や情報セキュリティの政策基盤となり、長期的には情報セキュリティ需要の拡大に寄与するだろう。

これらの法律に基づく諸制度の運用は、情報セキュリティ需要、さらには情報セキュリティ産業の発展を左右する要因となる[40]。

2　日本の情報セキュリティ産業の展望

（1）新市場の発展

最後に日本の情報セキュリティ産業の今後の発展可能性について簡潔に検討する。今後出現する新市場や、現在はまだ萌芽段階にあるが今後著しい拡大が期待できる市場は何か、である。それは、情報セキュリティ上の新しい脅威が出現しつつある分野でもある。

近年の脅威の動向をみると、いくつかの新しい動きが見出せる。第1は、サイバー戦争、サイバーテロ、あるいはハクティビズム（hacktivism）などと呼ばれる国境を超えた攻撃である。攻撃手段は多様であるが、政府機関や特定の企業（多くの場合は、攻撃された場合の社会的影響の大きい基幹産業を担う企業が対象となる）、あるいは重要インフラ[41]などを標的にしたものであり、攻撃を防御できない場合には、経済活動や国民の生活に多大な影響を及ぼす可能性がある。

第2はIoT（Internet of Things）あるいは「モノのインターネット」化と呼ばれる動きである。重要インフラ以外でも、生産設備などはすでにIT化され、ネットワーク化されつつあるが、今後はさまざまな製品（モノ）もネットワークに接続することが構想されている。従来の製品はIT化されている場合でも、多くは組込みシステムによる製品単体でのIT化であったが、今後はそれらをインターネットに接続していくことが想定されている。インターネットに接続されるということは、単にインターネットを通じてモノが監視されたり、制御されるという上下関係による管理だけでなく、モノ同士のネットワークを介した情報のやり取りを通じて、自律的に判断してモノ同士が協調するといった水平的関係も生じてくる。

モノがインターネットに接続されるということは、ネットワークを介した攻撃の対象となりうることを意味する。モノに対する攻撃は、情報漏えいやサービス停止といったシステム上の影響だけでなく、モノ同士のネットワークを通じて、モノの制御の破綻やその連鎖など、実社会への顕著な影響も予想しうる。従来の組込みシステムは専用のOSを使用していたが、ネットワークに接続されるようになって以来、ネットワーク接続機能をサポートする汎用OSを使うことが多くなったため、脆弱性が判明した場合の影響や攻撃の可能性も大きくなるとみられ

⑷⓪　情報セキュリティ対策促進のための税制上の優遇措置も情報セキュリティ需要を喚起しうる。ただし、次第に縮小し、現在は中小企業を対象とする税制優遇制度の一部に残るのみである。

⑷①　日本では、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の13分野とされる。情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第3次行動計画」2014.5.19, p.8. <http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf>

る[42]。

これらの新しい脅威の出現は、新しいタイプの情報セキュリティツールやサービスを生む可能性がある。また、影響する範囲が大きくなるので、情報セキュリティの考え方そのものを従来とは異なる方向へ転回する契機になる可能性もある。

（2）日本企業の海外展開と海外企業の参入

日本企業がグローバル化を進める中では、情報セキュリティ産業も海外に進出する日本企業や海外市場に目を向けざるをえない。しかし、日本の情報セキュリティ産業は海外進出に対して必ずしも積極的ではないと言われる[43]。

一方では、前述のように日本の情報セキュリティ市場の中には少なからぬ海外企業が参入している。すでに情報システムへの攻撃は国境を越えている。世界規模で出現する情報セキュリティ上の脅威に対応するためには、国内企業、国内技術だけで対応しようとするのは現実的でなく、重層的なリスク管理を進める上でも、参入企業の多様性は歓迎すべきことであろう。

日本企業が海外進出するにせよ、海外企業の日本市場への進出がさらに進展するにせよ、国際化を通じた新しいリスク情報の入手や対策技術や対策製品の導入は今後とも必要であり、情報セキュリティ産業の国際化がさらに進展する可能性がある。

（3）情報セキュリティが支える新産業

IoTが進展すると、IoTを利用した新しいサービスが開発される。そのイメージはいまだ定まっていないが、多種多様な新サービスが出現することになるだろう。IoTが情報セキュリティによる支えられるべきことは前述の通りだが、IoTを活用した新サービスも情報セキュリティに裏打ちされたものであることが必要になる。そこにも新しい情報セキュリティ市場が開ける可能性がある。

すでに防犯や警備等の「セキュリティ産業」においてはIT機器やITシステムの活用が進んでいる。IT化されたセキュリティ産業は情報システムの防御等の分野にも進出し、情報セキュリティ産業との融合が進みつつある。例えば、ITシステムにおける物理的なアクセス管理（入退室管理等）は情報セキュリティの一分野だが、従来から建物等における物理的なアクセス管理を担ってきたセキュリティ産業が、IT関連の施設のアクセス管理を担う場合も少なくない。セキュリティ産業が情報セキュリティ市場に参入する動きが見られるとともに、セキュリティ産業が情報セキュリティツール等を活用して新サービスを開拓したり、サービスをさらに高度化していく可能性もある。このように既存の産業を情報セキュリティツールが支えることで新産業が出現する可能性がある。

3　情報セキュリティ市場に影響を及ぼす外的要因

情報セキュリティ産業を左右する制度的変化に関してはすでに予定されているものもあり、近未来の情報セキュリティ市場の動向をある程度見通すことができる。すでに日程が明らかに

⑷2　日本ネットワークセキュリティ協会　前掲注⑴8, pp.46-48.

⑷3　情報処理推進機構「情報セキュリティ産業の構造と活性化に関する調査」2011.6, pp.46-49. <http://www.ipa.go.jp/files/000024418.pdf>

なっているものを2点紹介しておく。

第1は、マイナンバー制度の運用開始である。マイナンバー制度は平成27（2015）年10月以降個人にマイナンバーが通知され、平成28（2016）年1月から社会保障、税等の行政手続での利用が始まり、その後地方自治体を含む情報提供ネットワークシステムの運用が開始される予定である。マイナンバー制度の運用のためには国の年金、税、その他のシステム、情報提供ネットワークシステム、地方自治体の関連システムの改修や新規開発のみならず、民間企業等でもシステム改修が必要になる。これらの関連市場の規模は総額3兆円になるとも言われ(44)、このうち一定割合が情報セキュリティ投資に向けられると想定される。情報セキュリティ投資がIT投資の5%とすれば1500億円になる。したがって、マイナンバー制度の導入は情報セキュリティ需要を平成26（2014）年度以降数年にわたって、毎年数百億円押し上げる効果がある。

第2は、2020年の東京オリンピック・パラリンピックの開催である。2012年のロンドンオリンピック・パラリンピックでは、英国政府はサイバーセキュリティ対策にオリンピック関連予算の4分の1相当額（約3000億円）を費やし(45)、開催期間中にはサイバー攻撃の兆候が23億件に上り、2億件以上の不正アクセスをブロックしたと言われている(46)。オリンピックと情報セキュリティ上の脅威に対する対策は切り離せないものとなっている。「世界最先端IT国家創造宣言」（平成25年6月14日閣議決定）の改定（平成26（2014）年6月24日閣議決定）では「東京オリンピック・パラリンピック等の機会をとらえた最先端のIT利活用による「おもてなし」の発信」の項目を追加し、その中にサイバーセキュリティを位置付けた(47)。今後、2020年の東京オリンピック・パラリンピックが終了するまで、集中的な攻撃等に対応するために、様々な分野で情報セキュリティ対策を構築し、運用していく必要がある。東京オリンピック・パラリンピックに対する直接的な攻撃対策だけでなく、外国人観光客用ネットワーク環境整備など付随的なIT環境整備も進むものと予想される。そこでも情報セキュリティ対策は必要になる。これらの総体は、今後の情報セキュリティ市場の拡大要因となると見込まれる。

これらの外的要因が日本の情報セキュリティ市場の拡大にどの程度の影響を及ぼすかは、厳密には予測できないが、相当規模の情報セキュリティ需要を喚起することになろう。

おわりに

本稿は、日本の情報セキュリティ市場がどの程度の規模なのかを探り、その産業構造の特徴を描出することを試みた。情報セキュリティ市場の規模に関する正確なデータは存在していないが、さまざまなデータを総合すると、日本の情報セキュリティ市場は2000年代当初から2008年頃まで拡大し、2012年現在では4800億円ないし1兆円程度の規模を有すると推測される。現時点では決定的なデータがないため、各種のデータを総合的に検討した結果、推計値には大きい幅が残されている。産業構造の点では、情報セキュリティ産業は小規模で若い企業が多く、情報セキュリティ専業企業は多くない、また、海外企業の参入が比較的多いという特徴がみられる。

---

(44)「マイナンバー受注に備え　自治体・民間にシステム構築　3兆円市場を争奪」『日経産業新聞』2014.6.20.
(45)「東京五輪　サイバー対策強化」『読売新聞』2014.2.10, 夕刊.
(46)「2020年東京　狙われる先端IT」『読売新聞』2014.9.17.
(47)「世界最先端IT国家創造宣言改定について」（平成26年6月24日閣議決定）, pp.12-13. <http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryou1.pdf>

情報セキュリティ市場の規模を左右する要因にはさまざまなものがあるが、当面はマイナンバー制度の導入、2020年の東京オリンピック・パラリンピック開催が情報セキュリティ需要を牽引していくことは確実であろう。そのような追加的な需要が生ずる際に、供給側がどのように対応していくべきかは、本稿の範囲を超える問題である。しかし、過去の延長上の情報セキュリティ対策に加えて、大型の案件が同時に複数登場する事態が、従来の情報セキュリティ産業の供給能力を超え、混乱を生じさせかねないことは容易に想像できる。最近数年間にわたって市場の顕著な拡大がなかった日本の情報セキュリティ産業にとってはチャンスであると同時にリスクを抱え込むことになる。とくにセキュリティ人材の不足は繰り返し提起される課題[48]であり、人材確保がリスク要因となる可能性は無視できない。

情報セキュリティ産業は、ICT社会を陰で支える裏方的産業で、市場規模も決して大きいとは言えず、顕著な存在感はない。しかし、その重要性は無視できない時代になっている。

（こばやし　しんいち）

[48] 例えば、情報セキュリティ政策会議　前掲注(4), pp.36-37.