Information-technology
Promotion
Agency, Japan

情報セキュリティ産業の構造と活性化に関する調査

概要報告書

2011年6月

独立行政法人情報処理推進機構

全体概要

背景

第一次産業構造調査

情報セキュリティ対策の一層の高度化と普及が必要

対策を支える情報セキュリティ産業の発展と強化が必要

情報セキュリティ対策の必要性の認知の浸透

情報セキュリティ脅威・情報漏洩リスクの増大

情報セキュリティ産業の構造と活性化に関する調査

実態調査と分析

1. 本調査の内容
2. 日本の情報セキュリティ産業の状況と特性 －海外諸国の事例と比較を踏まえての分析－
2.1. 日本の情報セキュリティ産業の現況
2.2. 日本の情報セキュリティ産業の特性
2.2.1. 市場と顧客
2.2.2. 研究開発と産業技術力
2.2.3. 人材の確保と育成
2.2.4. 起業家とベンチャーキャピタル
2.2.5. 国際化と海外進出
3. 情報セキュリティ産業に関わる政策・施策 －海外諸国の事例と比較を交えての分析－
3.1. 技術開発に関わる政策
3.2. 政府調達に関わる政策
3.3. 人材育成に関わる政策
3.4. 海外進出・輸出振興に関わる政策
3.5. その他の産業活性化政策

産業活性化施策の提起

4. 日本の情報セキュリティ産業の発展と活性化に向けて
4.1. 情報セキュリティ産業の活性化に向けて
4.2. 産業振興に有効と考えられる政策・施策
4.3. 産業界および民間における努力・改善要素
4.4. 産業振興手段としての海外進出
4.5 課題別取組み主体

1.本調査の内容

1.1.本調査の目的

本調査は、情報セキュリティ対策の一層の普及と高度化が望まれるところ、そのためには供給側である情報セキュリティ産業の発展と強化が必要であるという視点に立ち、産業実態の整理と、必要と考えられる課題、施策の検討に取組んだものである。その結果として、我が国の情報セキュリティ対策の推進と普及、浸透と高度化に資することを目指している。

1.2.本調査の概要

本調査においては、国内外の情報セキュリティ分野における技術と産業と普及の連関に関する分析と検証に必要となる、国内外の産業、ユーザ、政策に関する実態調査を行い、諸外国の状況に照らして、日本の情報セキュリティ産業にどのような構造的特徴があり、その発展と活性化のためにはどのような課題があるのかの分析を行った。更に、それら実態調査と分析結果を踏まえ、国内情報セキュリティ産業の発展と活性化のために有効と考えられる事項や施策についての検討を、有識者により組織する検討委員会の指導の下に行った。

1.3.本調査の実施事項

【実態調査】

国内および海外の事業者や政策関係機関、有識者等へのインタビュー調査、および文献調査を実施。

調査期間：2010年7月～2011年6月

対象国・地域：日本、米国、欧州、韓国

調査項目：

①情報セキュリティ産業調査（調査対象：日本、米国）

②海外情報セキュリティユーザ実態調査（調査対象：米国、欧州）

③情報セキュリティ政策の国際比較（調査対象：米国、欧州、韓国）

・政府調達に関する調査

・技術開発支援に関する調査

1.本調査の内容

実態調査の内容と対象国は以下のとおり。

	情報セキュリティ産業調査	海外情報セキュリティユーザ実態調査	政府調達に関する調査	技術開発支援に関する調査
日本	○	－	－	－
米国	○	○	○	○
欧州	－	○	○	○
韓国	－	－	○	○

【活性化施策を検討するための調査】

- 情報セキュリティ産業の活性化に資すると考えられる施策検討のため、実態調査の内容も踏まえつつ、施策仮説に示す、事例調査・調査分析・有効性評価及び施策検討の参考になる情報の収集を行い、仮説の肉付けや検証に資する情報の整理を行った。

【検討委員会の設置ならびに運営】

- 検討委員会を設置し、調査計画・調査結果・結果報告書の評価並びに施策検討を行った。
- 実態調査の結果の分析・整理および活性化のための課題の整理については、全5回開催された委員会において議論し、評価を行った。

「情報セキュリティ産業の構造と活性化検討委員会」委員（敬称略・役職は委嘱当時）

委員長	中島　一郎	早稲田大学	研究戦略センター　教授
委員	田中　秀幸	東京大学大学院	情報学環・学際情報学府　教授
（50音順）	谷川　徹	九州大学	産学連携センター　教授／副センター長
	三輪　信雄	S＆Jコンサルティング株式会社	代表取締役社長
	渡部　章	株式会社アークン	代表取締役社長

1.2.1. 実態調査詳細

- 国内情報セキュリティ産業調査

日本の情報セキュリティ産業調査実施状況

	アンケート調査	インタビュー調査
調査期間	2010年10月27日（水）～11月9日（火）	2010年11月25日（木）～12月7日（火）
調査対象	日本国内で展開している情報セキュリティ事業者を抽出し、113社に送付	アンケート回答企業でヒアリングに協力可能な企業を中心に17社に対して実施
回収数	37社（回収率32.7%）	17社（うちアンケート回答企業16社）

日本の情報セキュリティ産業調査回答業種内訳

	アンケート	インタビュー
1．国産ベンダ	12社	7社
2．外資ベンダ	7社	3社
3．システムインテグレータ	7社	3社
4．サービスプロバイダ	8社	4社
5．付加価値再販事業者（VAR）	3社	0社
合　計	37社	17社※

※インタビュー対象企業17社のうち1社はアンケート回答企業以外（国産ベンダ）

- 米国情報セキュリティ産業調査
- 文献調査・web調査
- アンケート調査

米国の情報セキュリティ産業調査実施状況

調査期間	2010年10月21日（木）～12月10日（金）
調査対象	情報セキュリティ事業者20社
回収数	20社

- 海外情報セキュリティユーザ実態調査
- 文献調査・web調査
- インタビュー調査

米国・欧州の情報セキュリティユーザ実態調査実施状況

米国	IT（製造）1社、通信1社、航空1社	3社
欧州	ドイツ系製造1社、英国系製造1社、フランス系製造1社、北欧系IT1社、在欧日系金融2社（英国、フランス）	6社

- 情報セキュリティ政策の国際比較
- 文献調査・web調査
- インタビュー調査

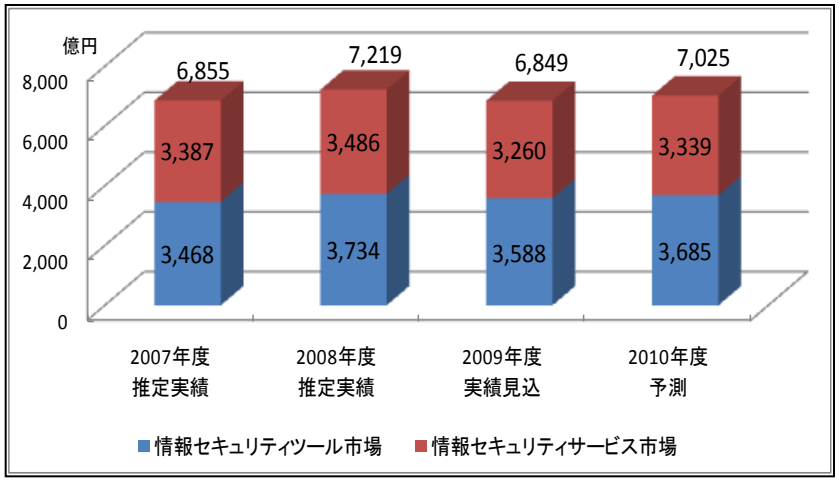
米国・欧州・韓国の情報セキュリティ政策調査実施状況

	実施方式	調査対象
米国	インタビュー調査 文献調査	NVLAP担当者、MITRE 政府および公的機関の情報セキュリティ関連研究開発および調達基準を調査。
欧州	インタビュー調査 文献調査	FP7、ENISA、フラウンホーファー研究所、フランス系製造、英国系製造、北欧系IT各1社 EU、英国、フランス、ドイツ、北欧（フィンランド、スウェーデン）の政府および公的機関の情報セキュリティ関連研究開発、調達基準、その他の産業支援の取組を調査。
韓国	インタビュー調査 文献調査	韓国調達庁、KISA、KISIA、ETRI、ベンダ3社 政府および公的機関の技術開発、調達基準、その他の産業支援の取組を調査。

2.日本の情報セキュリティ産業の状況と特性
－海外諸国の事例と比較を踏まえての分析－
2.1 日本の情報セキュリティ産業の現況

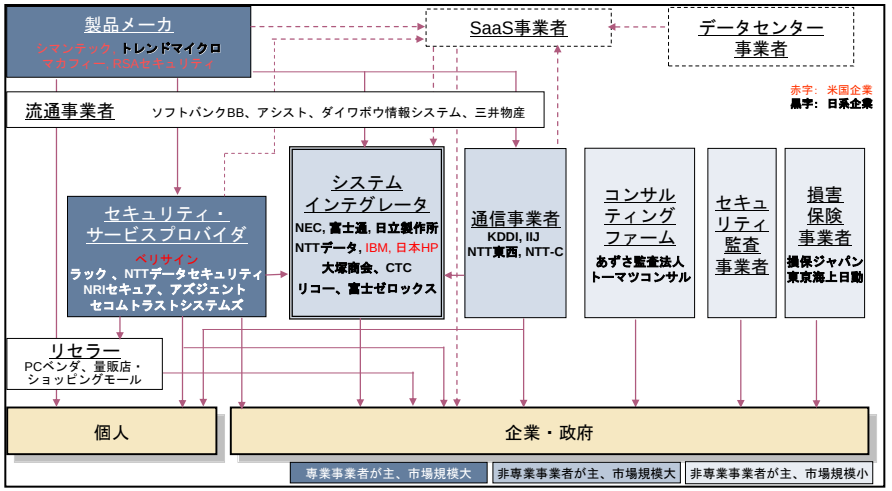
- 日本の情報セキュリティ産業の現況としては、経済産業省「平成21年度情報セキュリティ市場調査報告書」およびIPA「情報セキュリティ産業の構造に関する基礎調査」等から以下のようなことがいえる。
  - ① 製品供給において一部分野を中心にアメリカ企業の参入数が多い。
  - ② 日本の市場規模約7000億円の一方、日本で事業を営む情報セキュリティ関連の事業者の事業規模は1社あたり約19億円と小規模である。日本で比較的大手である情報セキュリティ事業者の年間売上はトレンドマイクロを除けば40～70億円規模である。一方、米国ではシマンテックが5500億円、マカフィーが1800億円の売上規模である。
  - ③ システムインテグレータが流通や情報セキュリティシステムの構築・実装・運用に占める役割が大きい。

国内情報セキュリティ市場規模の推移



（出所：経済産業省「平成21年度情報セキュリティ市場調査報告書[1]」）

日本の情報セキュリティ産業の役割構造



（出所：IPA「情報セキュリティ産業の構造に関する基礎調査」2009年12月）

- 経済産業省の同市場調査報告書では、「1 社当りの情報セキュリティの事業規模が20 億円を切るレベルでは、事業採算性を考えた時に、研究開発投資や人材育成等の面に十分に資金を割けない可能性がある。特に製品の開発や検証に際して、ベンチャー企業への支援の仕組の整備は課題となる可能性が高い。」と指摘されている。

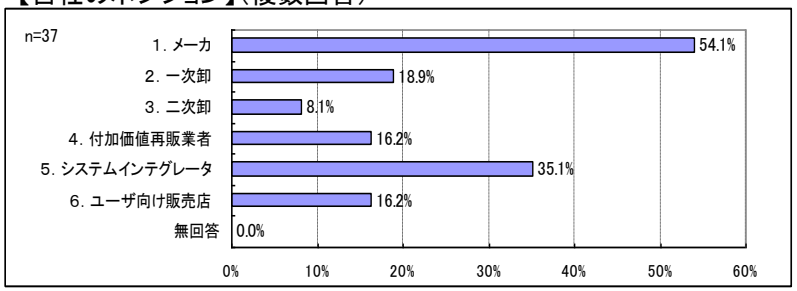
[1] http://www.meti.go.jp/policy/netsecurity/downloadfiles/21FY_ISmarket_research_report.pdf

2.2. 日本の情報セキュリティ産業の特性
2.2.1. 市場と顧客

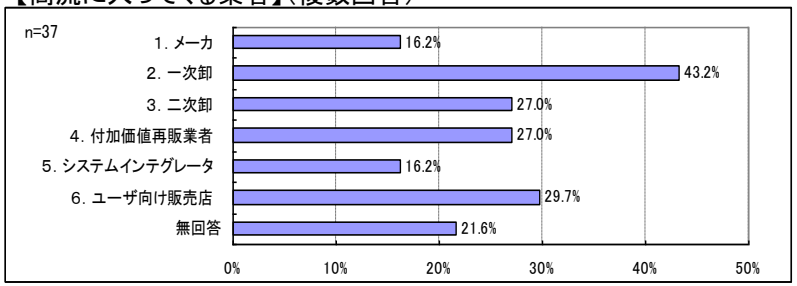
- 日本の商流の特徴

日本情報セキュリティ産業の流通構造

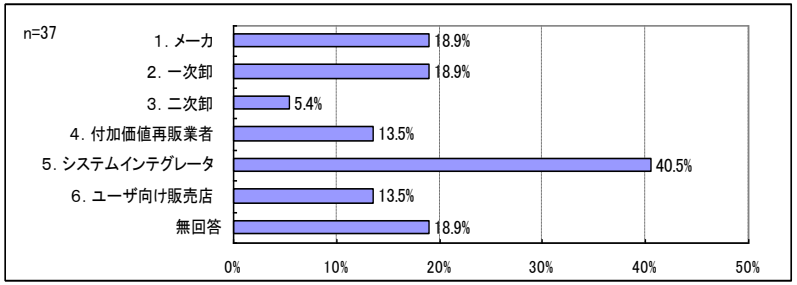
【自社のポジション】(複数回答)



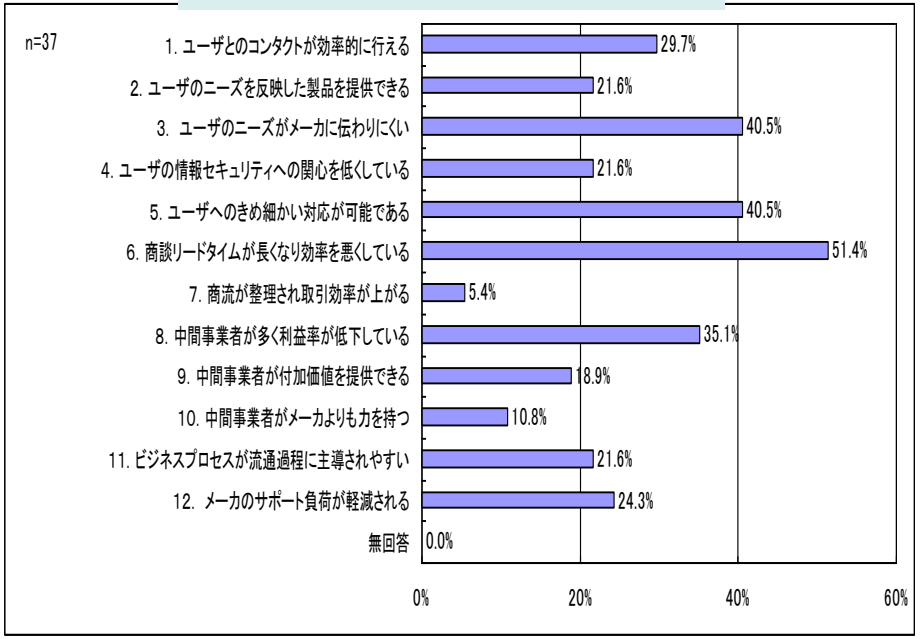
【商流に入ってくる業者】(複数回答)



【商流に入ってくるなかでポイントとなる業者】(複数回答)



日本流通構造におけるメリット・デメリット



- 日本のユーザの特徴

<u>日本産業アンケートの自由回答および産業インタビュー</u>

- 特に中小企業以下の規模ではセキュリティ知識が乏しく意識が低い（国産ベンダ、システムインテグレータ）
- 情報セキュリティ対策の投資効果・費用対効果の明確化が困難なため、エンドユーザの投資優先度が低い。投資というよりコストと認識されている。（国産ベンダ、システムインテグレータ、サービスプロバイダそれぞれ複数）
- 情報システム部門、情報セキュリティ部門の会社組織内の位置づけが低い。（サービスプロバイダ、システムインテグレータ）

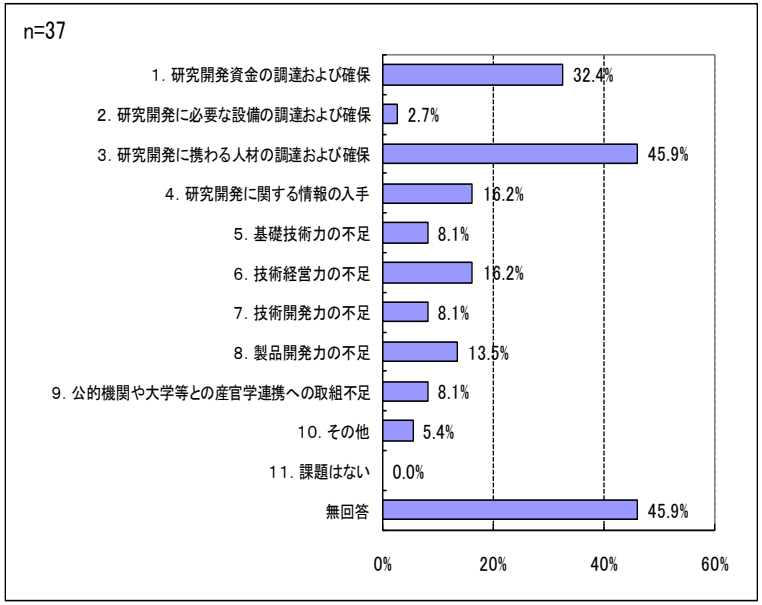
2.2. 日本の情報セキュリティ産業の特性
2.2.1. 市場と顧客

- 米国の市場と顧客の特徴
  - 仲介機能を持つチャネルがあるが、ユーザへの影響力はベンダの提案内容である。
  - β版ユーザ、ベンチャー製品購買など意欲があり、ユーザがリスク評価に基づき購買を決定する。
- 欧州の市場と顧客の特徴
  - F-SecureやSophosなど欧州ベンダもあるが、主なベンダとしては米国製品が強い。サービス地域密着型で日本と似た状況が確認できる 。
  - 情報セキュリティ技術担当をおき、製品の費用対効果評価を行い主導的に製品選定を行っている。
- 韓国の市場の特徴
  - 韓国市場では、ツール、サービスともAhnlab、IGLOOなど、韓国企業の存在感が大きい。
- 日本の市場と顧客の特徴と課題
  - 日本においては、商流に参加する業態が他国・地域よりも多く、複雑性・多様性を有する。
  - 流通構造は歴史的な商慣行や地域特性によるものも多く、ベンダから見たときに、ビジネス･プロセスの主導権を握れないというフラストレーションの原因ともなるが、流通を束ねる存在に依存できることは営業効率を高める面も否定できない。企業はこれらのメリット・デメリットを把握して商流を活かすことを考える必要がある。
  - 日本ユーザ企業の特徴として、品質追及に対する厳しさと、他社での導入実績を重視する指向が、日本産業アンケート・インタビューおよび有識者インタビューで多く挙げられた。
  - 日本ユーザ企業は、法令等が情報セキュリティ対策の動機となる要素が強い。費用対効果の議論は出るが、情報資産の価値や事故発生時のダメージの評価が確立していないことにより、効果の測定ができないというジレンマのレベルにとどまっているように見える。

2.2. 日本の情報セキュリティ産業の特性
2.2.2. 研究開発と産業技術力

- 日本の弱み
  - 技術が競争の鍵を握る市場において、研究開発に振り向けるべき資金と人材の不足に悩まされる実態がある。一方、米国企業の技術優位は確たるものがある。
  - 製造業のような産業技術力による差別化要素も少なく、独自技術があってもグローバル展開にまで至らない。
- 米国産業の技術優位の背景
  - コンピュータ、ネットワーク技術の発祥の地であり、十分な国内市場規模、豊富な人材供給、連邦政府の政策的注力（研究開発、産学連携、人材育成）に加え、企業の積極的R&D戦略に支えられて技術優位を維持している。

日本企業　国内における研究開発の課題



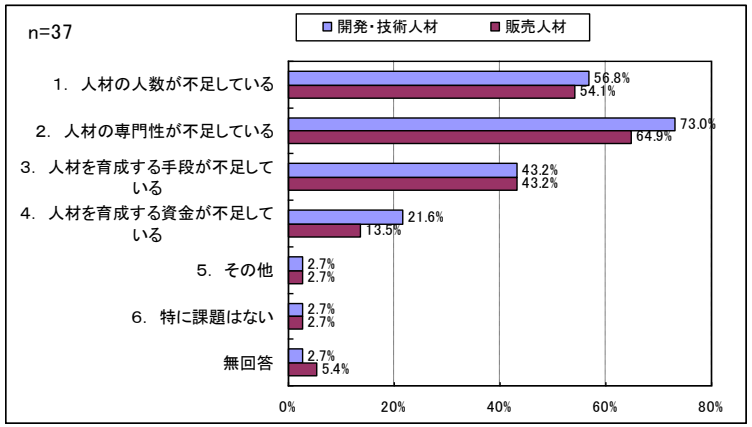
日本産業インタビュー
製品において米国技術が日本技術より優性である理由

- 日本発の要素技術はかなり難しい。また要素技術がでてもビジネスモデルへの組込みがないと成功しないが、日本はビジネスの構想力が弱いと感じている。（外資ベンダ）
- 要素技術が現状、ほとんど存在しない。大学発の技術は実用性に乏しく、米国ほど開発費がつかない。いい技術が出てくるためには、数が出てくるようにしなければだめだと思うが、日本はそのような状況にはない。（国産ベンダ）
- 日本にコア技術がない状況で利益が薄くては研究開発にお金を掛けられない。（国産ベンダ）
- 日本発のオープンソースがなく、調べてゆくと欧米になる。もっと公的機関の成果のオープンソース化があってもよいのでは。（国産ベンダ）
- ソフト、ＩＴの分野で日本発の技術がない。バグなどが有っても出すなどの視点がいるのかもしれない。（サービスプロバイダ）

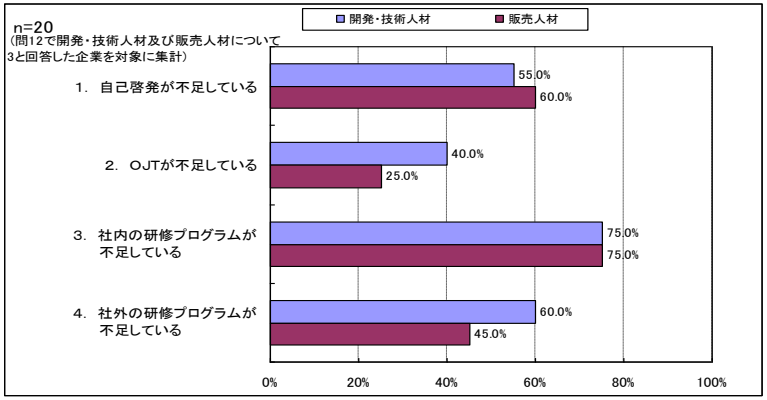
2.2. 日本の情報セキュリティ産業の特性
2.2.3. 人材の確保と育成

- 日本の情報セキュリティ事業者においては人材が量的にも質的にも不足している。
- 国内情報セキュリティ産業対象のアンケート調査において、人材の数、専門性、育成手段のいずれについても、不足感が多く回答されている。
- 特に、研究開発を担う人材の専門性について73%の企業が課題として挙げている。

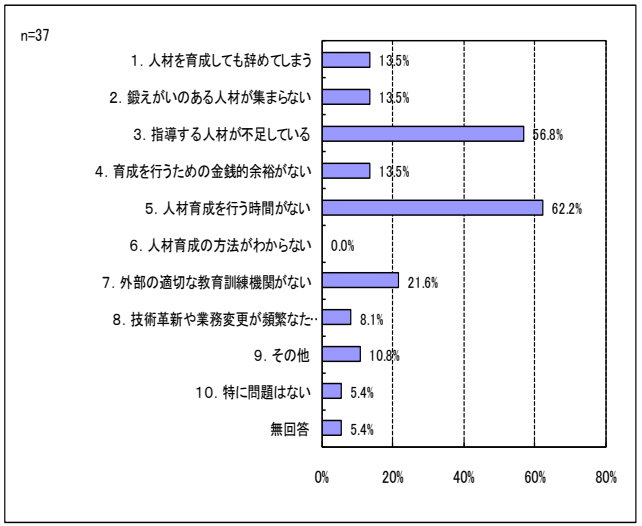
情報セキュリティ分野における人材の課題



人材育成上の課題



人材に関する具体的な課題



- ユーザにおける人材不足も指摘されており、その課題対処も必要。

有識者インタビュー

- ユーザ企業にセキュリティを担当する人材がいて初めてセキュリティ産業が必要とされる。、ユーザ企業の社員にセキュリティ担当者となる教育と任務を与えることが肝要であり、ユーザ側に対しても政策による支援が必要になる。

2.2.　日本の情報セキュリティ産業の特性
2.2.3.　人材の確保と育成

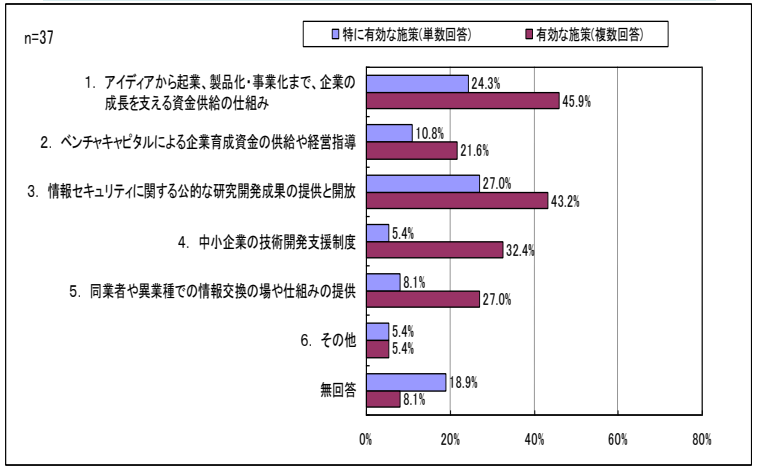
- 米国
  - 政府の人材対策強化の動きがあり、民間の需要も高いので、人材需要引き続き旺盛と予想される。
  - IT技術者への就職意欲が高く、政策的な人材育成策、奨学金制度等も強化されており、供給面での対応も手が打たれている。
- 欧州
  - 英国　情報セキュリティ技術者向けのトレーニング機関（民間非営利団体のCREST：The Council for Registered Ethical Security Testers）の教育の活用。
  - ドイツ、英国等の大学教育による情報セキュリティコースの提供
- 韓国
  - しばらく前は人材を比較的容易に採用できたが、現在は難しいとの指摘がある。
  - 高等教育機関や資格制度を充実させている。国民の資格取得熱が高く受験者が増えている。

- 日本の課題解決に向けて
  - 高等教育機関において情報セキュリティ専攻の教育を受けた新卒人材の供給は限定的であり、優秀な新卒人材の供給環境を整備することが重要である。
  - 情報セキュリティに多くの学生が魅力を感じるために、「魅力ある就職先」となることも重要である。
  - 経験者人材が情報セキュリティ産業に流入する環境を整える必要がある。
  - グローバルな人材確保を、企業にとって現実味を帯びたものにしていく必要がある。
  - ユーザ人材の育成についても人材育成のテーマの１つとする必要がある。

2.2. 日本の情報セキュリティ産業の特性
2.2.4. 起業家とベンチャーキャピタル

- 日本の情報セキュリティ産業における産業資金確保の状況

日本の情報セキュリティ産業の活性化に必要な環境

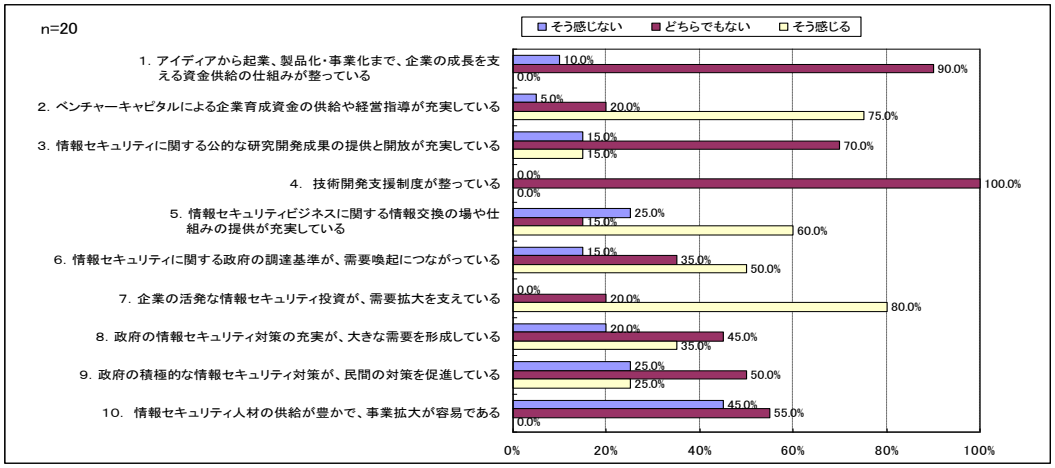


日本産業インタビュー

- 政府では産業振興のために補助金や開発援助が行われてきたが、むしろマーケティング的な支援が必要である。（外資ベンダ）
- 日本でのベンチャー育成においては、アイディアがあっても資金がない状況もある。ただ、ベンチャーキャピタルに「晴れの日には傘は貸すが、雨の日には貸さない」傾向があり、最も資金援助が欲しいときに得られないという状況はよく聞く。ここに公的な資金や仕組みがあれば有効と思う。（外資ベンダ）
- 情報交換の場があれば、救いの手が見つかることもある。但し、場を作った場合は意思と資金のある者が長期に渡り責任を持って場を継続する必要がある。（外資ベンダ）
- 日本の大手は「自前開発主義」であり、ベンチャーの技術を買うことはしない。（国産ベンダ）（外資ベンダ）

- 米国における情報セキュリティ産業の事業環境に対する評価

米国の情報セキュリティ産業の事業環境



– ベンチャーキャピタル等に接する中で経営指導が充実していることの実感を得ていると考えられる。
– 「情報セキュリティビジネスに関する情報交換の場や仕組みの提供が充実している」について「そう感じる」を選択した企業が60%を占めた。

2.2. 日本の情報セキュリティ産業の特性
2.2.4. 起業家とベンチャーキャピタル

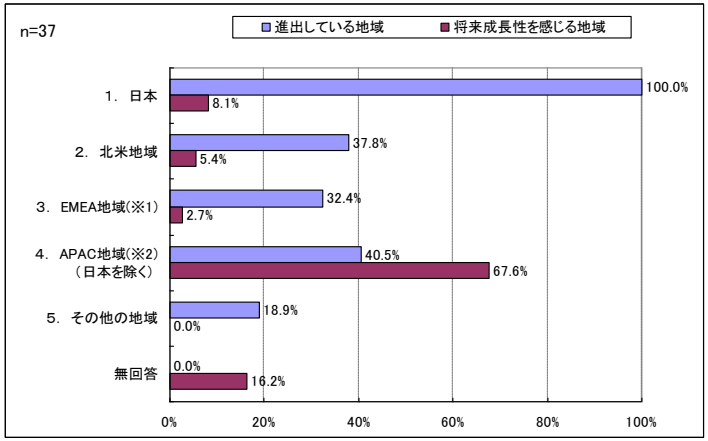
- 2007年3月　総務省情報通信政策局「ICT ベンチャーの実態把握と成長に関する調査研究（平成19年3月）」
  - 2000年から2006年までの日本と米国とのベンチャーキャピタルの投資額比較「アメリカのVC投資額の10分の1程度のリスクマネーしかVC経由でベンチャー企業に流入していない。」
  - 2000年～2003年のGDP比での国際比較では、米国が対GDP比0.37%であるのに対し、韓国0.27%、英国0.22%、EU全体0.13%、フランス0.11%、ドイツ0.10%、日本が0.03%となっている 。
- 2008年　独立行政法人情報通信研究機構　情報通信ベンチャー支援センター 「情報通信分野における経営者実態調査」
  - 経営者になった時点で「十分に計画して起業・独立した」53.1%に対して、「なんとなく起業・独立した」32.9%、失職などの事情により必要に迫られて起業した」14.0%との結果であった。
- 2011年3月　経済産業省「平成22年度アジア各国のベンチャー企業投資事例調査～アジアからの持続的なイノベーション創出とベンチャーファイナンス～」
  - 「我が国のベンチャー輩出やイノベーション創出に関する循環モデルは、時代や環境の変遷に合わせて再構築すべき段階に至っていると考えられる。」と評価している。

- 日本においては、産業活性化のために起業を促す仕組みを主に行政が中心となって整備しているものの、米国などのように起業が一般的となる土壌が育っていないとの評価がある。
- 日本においては、ベンチャーキャピタルが機能していない、との問題意識があるものの、実際には様々な投資活動が行われ、エンジェル優遇税制など制度としては整備されてきているといえる。問題はそれが実際産業育成に有効に機能しているかである。
- 日本の強みとして、公的に活用できる補助金等の資金供給施策が多いことがあげられる。このような日本の事情を鑑みた上で、製品化・事業化を多く行うための資金供給手段を確保するという役割を担う主体と必要な仕組みについて、特に金融機関の役割について検討することが課題である。
- また、日本の大企業の「自前主義」によりベンチャーでは太刀打ちできないとの指摘もある。このような風土において、ベンチャー企業が開発した技術を育成し活用する方向で機能する、金融機関、技術移転機関・知財取引仲介機関、大企業等の役割を充実させていくことが今後の課題である。

2.2. 日本の情報セキュリティ産業の特性
2.2.5. 国際化と海外進出

- 日本の情報セキュリティ事業者における海外展開の意向
  - 市場としての将来性をアジア地域に感じてはいるものの、積極的に進出する企業が多くない傾向にある。

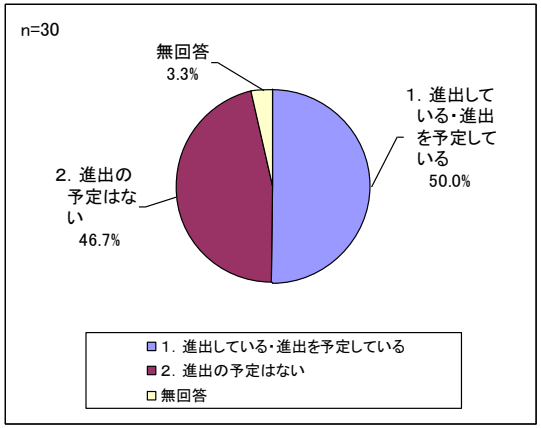
現在進出している地域、将来性を感じる地域[1]



現在進出している地域、将来性を感じる地域名

	進出している地域 ()内数値は回答数	将来成長性を感じる地域 ()内数値は回答数
2．北米地域	アメリカ(6)、カナダ(2)	アメリカ(1)
3．EMEA地域(	イギリス(3)、フランス(1)、スペイン(1)、ポーランド(1)	イギリス(1)
4．APAC地域(※2)（日本を除く）	中国(5)、韓国(3)、台湾(2)、シンガポール(2)、オーストラリア(1)、ベトナム(1)、マレーシア(1)、タイ(1)	中国(11)、インド(4)ベトナム(2)、タイ(1)、韓国(1)、オーストラリア(1)
5．その他の地	ロシア(1)	ー

海外市場への進出の意向



日本産業インタビュー　海外展開の困難を挙げる意見

- 既に英国に進出している。一方、アジア地域は商習慣についても難しい一面があると聞いており、中小企業である当社には難しいと思っている。（国産ベンダ）
- アジア市場は情報セキュリティに関する文化的背景や、そもそも商慣習が違うため、積極的な進出が難しい。（国産ベンダ複数）
- 将来的には海外展開もしたいが、現在の企業体力からは時期尚早と思っている。（国産ベンダ）
- 優秀なパートナー、有能な拠点の責任者を見つけることが成功するために重要であるが、それができるかどうか。（外資ベンダ複数）
- 日本発製品を海外に売るためにはローカリゼーションが課題である。（国産ベンダ）

[1] EMEA地域：欧州・中東・アフリカ地域、APAC地域：アジア太平洋地域

2.2.　日本の情報セキュリティ産業の特性
2.2.5.　国際化と海外進出

- 米国の情報セキュリティ事業者の特徴
  - グローバルに活発な活動を行っていることが確認されており、本調査においても企業規模の大小によって国外拠点数も多い・少ないの差はあるが、なんらかの形で国外に拠点を設け、事業を展開している。
- 欧州の情報セキュリティ事業者の特徴
  - 欧州企業でも北米の売上比率が高い等国際展開に積極的事例も見られる。
  - 北欧企業全体が、「ボーン・グローバル」であり、国内国外市場を区別せず、会社設立当初から国外への参入を想定し人的資源、物的資源を投入する経営戦略を取る。
- 韓国の特徴
  - 韓国の国内市場が小さいとして、他産業と同様に国外への展開が活発、特に日本進出が活発。情報セキュリティ事業者は、日本を海外進出の足がかりとして考える傾向がある。

- 日本の課題
  - 日本の情報セキュリティ事業者のグローバル展開に関する課題として、海外展開に商機を見いだす意識や、知識・情報の不足があるといえそうである。
  - 韓国や北欧諸国では政府が強く海外展開を支援する施策が明確。日本においても、海外展開の利点や意義を見出し、サポートする体制が必要である。
  - 事業者の海外展開に対する知識・情報の不足を補うこと、日本の政府施策としての取組みも、知られていないことも理由となって活用が十分であるとはいえない。海外展開を考えている企業が出られない、ということがないように、公的機関の支援の充実に加えて、情報提供機能が重要になる。

3.情報セキュリティ産業に関わる政策・施策
－海外諸国の事例と比較を交えての分析－
3.1. 技術開発支援政策

日本
- 公的研究開発機関：産総研、NICT、JSTによる研究開発が中心
- 公的研究資金利用、共同・委託研究には民間企業が消極的
  - 大学研究テーマのビジネス指向不足、研究費の使い勝手の悪さ（柔軟性・資金規模など）
- 日本の情報セキュリティ研究開発予算2006年度91.2億円→2010年度48.6億円（NISC「情報セキュリティ研究開発戦略（案）」2011.6）

米国
- NITRDで省庁横断プログラム・予算管理を行い、ITのR&Dに注力
- FFRDC等の仕組みにより、官のイニシアティブ・資金と民の技術・経営を融合
- 各省庁に技術移転窓口があり、公的開発技術の民間移転を積極展開
- 米国の情報セキュリティ研究開発予算2007年度約$213M→2010年度約$407M（NISC上記資料による）

欧州
- FP7による欧州横断プログラム・予算管理（域外にも解放）。成果は受託者に帰属
  - 2007年～13年　予算ICT　€9.05B（1兆円）　セキュリティ　€1.4B（1460億円）
  - 1つの国際協力研究開発プロジェクトに対し、2ヵ年で4億円程度の助成金
- 英国：R&D税制、開発支援資金、技術移転等の仕組みが充実
- ドイツ：フラウンホーファー研究所による技術開発と移転の仕組みが充実（1955年からの取組み）

韓国
- ETRIによる技術開発と民間移転、KISAによる開発支援・技術移転

3.情報セキュリティ産業に関わる政策・施策
－海外諸国の事例と比較を交えての分析－
3.2. 政府調達に関わる政策

日本

- 従来の政府調達は、調達仕様におけるセキュリティ要件の曖昧さや過不足の発生が「不公平な調達」、「過度なセキュリティ対策」、運用開始後の「セキュリティ事故」と言った結果を招く可能性もあった。
- 2011年4月、NISCが「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を公表。付録「対策要件集」において各対策項における機能要件が具体的に記述された。
- 政府機関および民間のセキュリティ対策のレベルアップと調達の活発化・積極化に貢献することが期待される。

米国
- NISTの定める標準に対する認定制度があり、認定製品が調達対象になる。
- 政府調達対象品の製品検査機関を認定するプログラムNVLAPをベースとして、評価機関の民間委託、標準策定時の民間参加等、民間を活用した仕組みが機能している。
- GSAによる一括調達や包括契約、統一約款等、効率性・一貫性を確保する仕組みも整っている。

欧州
- 英：政府調達のための評価基準を、通信機器セキュリティグループ（CESG）が所管。政府統一契約・価格設定のシステムがあり、透明性・公平性を確保している。Framework Agreementは、中小が入る余地があり、調達プロセスを効率化するとともに透明化し、不必要な競争や異常なダンピングを防いで調達品の品質確保にも資する。
- 仏：国家情報通信システム安全庁（ANSSI）が統括。調達基準のベースはCC
- 独：政府による技術基準があり、ドイツ連邦情報セキュリティ庁（BSI）が所管。CCも活用。

韓国
- 独自基準（KISAが評価）である＜Kシリーズ＞からCCベースの認証体系へ移行中。
- 中小企業育成のための優遇政策。韓国調達庁の目標として中小企業からの購買が挙げられている。
  - 政府調達における中小企業枠、大企業が応募する際に中小企業の参加とを必須とする枠など。

3.情報セキュリティ産業に関わる政策・施策
－海外諸国の事例と比較を交えての分析－
3.2.　政府調達に関わる政策

日本の課題

- 政府調達と産業活性化の関係
  - 政府調達がイノベーションを促進するという考え方は存在する。第3期科学技術基本計画 において「公的調達を通じた新技術の活用促進は、公的部門の活動の機能の充実や効率性向上等のみならず、研究成果の社会還元の促進の観点からも重要である」している。
  - JST　2007年8月「イノベーション指向型の公共調達にむけた政策課題の検討：欧米との比較調査を踏まえて」報告書において、特にイノベーションの促進を阻害している要素として「競争入札資格が、研究開発型ベンチャー企業にとって非常に不利な仕組みであり、入札機会が著しく限定されている。」と言及している。
  - 経済産業省経済産業政策局「ベンチャー企業からの公的調達の促進に向けた研究会」報告書（2007年3月）「どのような商品、サービスを提供するベンチャー企業がどこに所在しているか、調達機関の側で十分に把握できていないこと、性能や安全性など、ベンチャー企業が提供する商品等の信頼性が十分把握できないことが最大のネックである」との議論がなされた。
- 政府調達によってイノベーションが促進される、ベンチャー等への発注がなされることで、ベンチャーによる産業活性化がなされる、という点について、様々な検討が既になされている。政府調達の役割を、より積極的な見地から評価する必要がある。イノベーション促進、ベンチャー育成の機能を果していない。

- 政府機関に共通の調達基準がなく、製品評価基準は一部にCCが指定されるも、他に基準がない。
  - 負担になるだけではないかとの事業者の懸念、活性化につながっているのかとの有識者指摘

3.情報セキュリティ産業に関わる政策・施策
3.3.　人材育成に関わる政策

- 日本　情報セキュリティ人材の供給量の充足感には程遠い
  - 日本における高度ITおよび情報セキュリティ人材に関する主な施策
    - 先導的ITスペシャリスト育成推進プログラム（文部科学省）、情報通信人材研修事業支援制度（総務省）、公認情報セキュリティ監査人資格制度（経済産業省）、情報処理技術者試験（経済産業省）、ITスキル標準（経済産業省）、セキュリティ＆プログラミングキャンプ（経済産業省）
  - 大学・大学院等の高等教育の情報セキュリティ関連学部・学科・専攻が主な整備状況
    - 情報セキュリティ大学院大学（2004年開学）、中央大学博士課程情報セキュリティ科学専攻の設置（2007年）・21世紀COEプログラム「電子社会の信頼性向上と情報セキュリティ」申請拠点、奈良先端科学技術大学院大学、大阪大学、京都大学、北陸先端科学技術大学院大学の4校によるIT-Keysプロジェクト、産業技術大学院大学（東京都公立大学法人・2006年開学）に「情報アーキテクチャ専攻」情報セキュリティ専攻。

- 米国　著名大学・大学院の専攻カリキュラムに加え、サイバーセキュリティ人材育成に注力
  - 情報セキュリティ専攻大学・大学院が数多くカリキュラムを提供し、MITなど情報セキュリティに関する研究機関を有している著名大学もある。
  - 連邦政府のサイバーセキュリティ人材の育成を目指す計画。

- 欧州　大学等のプログラム提供と社会人向けプログラム提供、その中で資格や経験を評価するプログラムがある。
  - 英国は、大学・大学院における情報セキュリティ教育カリキュラム、CESG、CREST等が公的機関と連携して提供するプログラム。
  - ドイツ　ヘッセン州による大学情報セキュリティ学部への公的資金拠出、社会人コースの整備。

- 韓国　知識経済部による「産業振興」の一環としての人材育成施策の展開と資格制度の運用。
  - 知識経済部（Ministry of Knowledge and Economy 以下MKE）は、「韓国経済を牽引する新成長エンジン」の政策テーマの1つが「ソフトウェア」であり、その中にセキュリティがある。特定の分野の専門家を育成し、海外進出を活性化することを政策目標においている。
  - 情報セキュリティ認定国家資格　SIS（Specialist for Information Security）
    - 専門性が高く合格率10%程度。2010年は5つの地域（ソウル、釜山、大田、大邱、光州）で試験が実施された。SIS資格は認定国家資格であるが、エントリークラス向けの試験も開始。1回当たり700-800名が受験し、合格率は30-40%程度。

3.情報セキュリティ産業に関わる政策・施策
3.4. 海外進出・輸出振興に関わる政策

- 日本 JETRO（独立行政法人日本貿易振興機構・海外55カ国に73事務所）が主な役割
  - アジア（タイ）での進出ビジネス検討時のオフィス無償提供、有償での海外進出コンサルティング、進出・法制度・知的財産・市場に関する情報提供
  - 先端技術分野を対象とした「ベンチャーインキュベーションinUSA」インキュベーションプログラムの活用。卒業生36社（2010年12月1日現在・公表ベース）→2011年4月より「ビジネスサポートinシリコンバレー」事業に引き継がれた。

「ベンチャーインキュベーション in USA」概要

期間	1年間
支援内容	西海岸（シリコンバレーおよびロサンゼルス）の有力インキュベータと提携し、マッチング、オフィス貸与、ビジネス立ち上げ支援、ネットワーク紹介を行う。
選考過程	JETROとインキュベータによる書類審査
費用	157,500円（企業負担実費を除く）
支援状況	5社（2010年12月1日現在・公表ベース）
卒業生	36社（2010年12月1日現在・公表ベース）

「ビジネスサポートinシリコンバレー」概要

期間	3ヵ月（最大9ヵ月まで延長可）
支援内容	ジェトロがシリコンバレーに設置したBIC（US-Japan Business Innovation Center）のオフィススペースとソフトサービスの活用。渡航後の生活立上げ支援（車、住居等）、一般的な現地ビジネス関連情報の提供、ネットワーク構築支援、専門家の紹介、無償コンサルティングサービス
選考過程	JETROとインキュベータによる書類審査
手続費用	131,500円（企業負担実費を除く）

  - 財団法人海外職業訓練協会（以下OVTA）による海外進出や海外研修制のセミナー等の支援
- 米国 雇用創出のための経済活性化輸出支援策および中小企業の輸出支援策を実施。
- 欧州 欧州域内自由貿易。域外への輸出促進策をとっている。
  - 英国（UK Trade & Investment：英国貿易投資機構）によるサポート。日本では英国大使館商務部が定期的にセミナーを開催し、英国から担当官や有識者を招聘し、英国の情報セキュリティベンダやその日本代理店にも発表・アピールの機会を与える 。（IPAも参加している）
  - ドイツ連邦経済技術省では、IT産業の大規模システムの輸出のために、プラットフォームを形成し、中小ベンダ等であっても一定の基盤を利用してシステム構築できる仕組みをもつ。
- 韓国 国を挙げて国外の市場を獲得するための施策を多く行っている。
  - KOTRA（国外72カ国・99拠点。日本は4拠点と東京IT支援センター・東京輸出インキュベーターセンター）。情報セキュリティに関しては、東京IT支援センターが活動し韓国企業16社が入居。
  - KISIAによる支援（輸出向けの翻訳・ローカライズ費用の50%を公的資金が負担する支援など）

4.日本の情報セキュリティ産業の発展と活性化に向けて
4.1情報セキュリティ産業の活性化に向けて

4.1.1 民間における情報セキュリティの向上

- 情報セキュリティに対する経営上の価値の認識と企業戦略上の位置付けをさらに高め、より一層の体系的な対策の構築に取り組む必要がある。
- その実装や実践を支える情報セキュリティ事業者の技術力、経営体力、国際競争力の向上を実現するための、情報セキュリティ産業の活性化は、日本にとって重要な政策課題と言える。

4.1.2 政府における情報セキュリティの認識 「情報セキュリティ2010」より

- 大規模サイバー攻撃事態への対処態勢の整備等
- 新たな環境変化に対応した情報セキュリティ政策の強化

4.1.3 情報セキュリティ産業の活性化に関わる要素

① 社会全般において情報セキュリティに取り組む動機が強いこと。

- 国においては情報セキュリティが国家安全保障の一環と認識されていること、民間においては情報セキュリティリスクを経営リスクと位置付け、企業価値を守るための積極的課題と認知されていることが実現すれば、社会全体として情報セキュリティに取り組む動機が強いと言える。
- その結果、情報セキュリティに対する投資が積極的に行われ、情報セキュリティマネジメントが徹底し、経営課題の一環として位置づけられることにより、情報セキュリティガバナンスが確立する。
- その過程で情報セキュリティ製品への技術評価も厳密に行われることからベンダに対する要求も高まり、よりよい技術や製品の開発・供給を促すことになる。その結果より高度な対策が可能になり、情報セキュリティへの取組みのレベルアップを実現するという好循環を生んでいる。

② 安全保障や電子政府等、国家戦略の一環をなすものとしての位置付けがある。

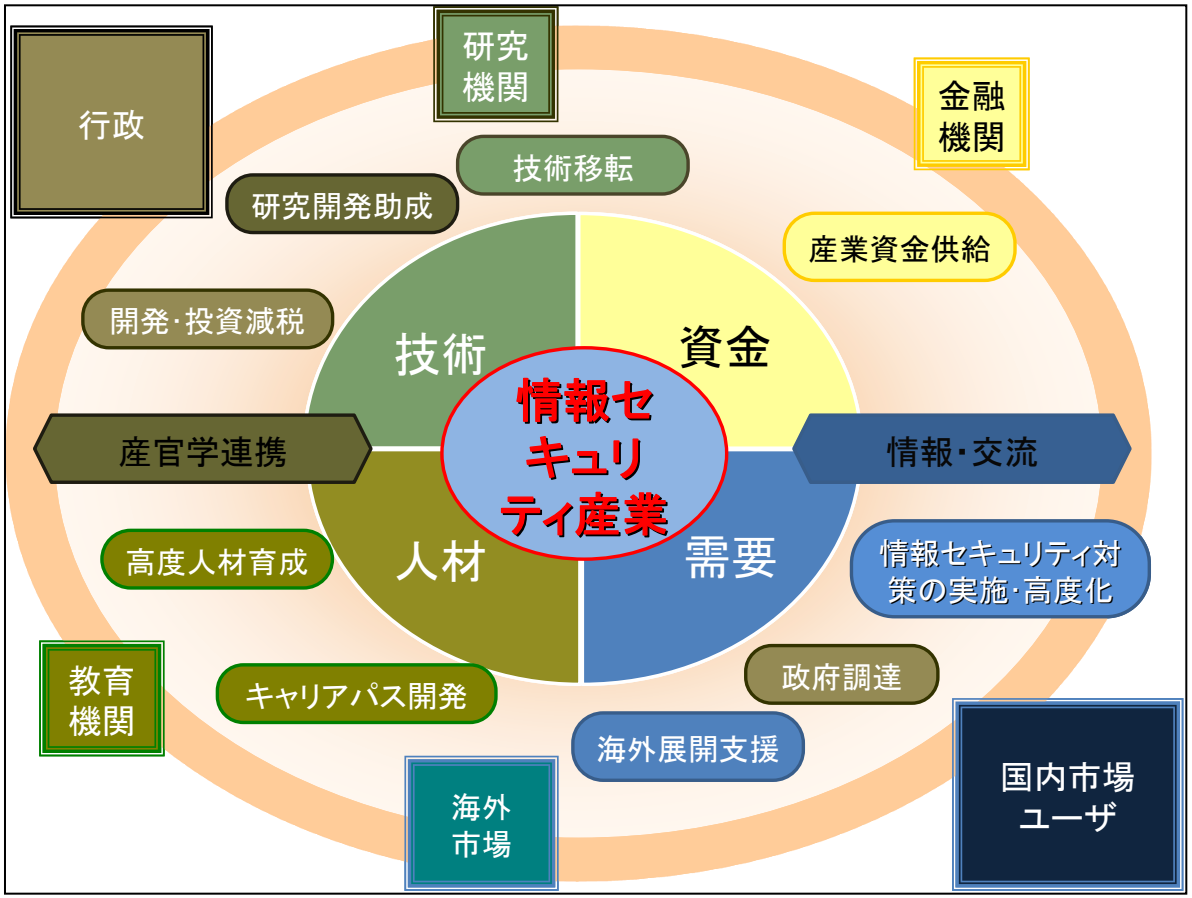
③ 情報セキュリティ技術人材の供給源が豊富である。

④ ベンチャー企業など、企業の起業と育成を支える社会的仕組みが存在する。

⑤ 海外市場に展開し、市場を拡大している。

4.日本の情報セキュリティ産業の発展と活性化に向けて
4.1情報セキュリティ産業の活性化に向けて

- 産業業活性化がもたらされ、好循環を生むための施策要素の連関を模式化すると以下のようになる。



4.日本の情報セキュリティ産業の発展と活性化に向けて（取組例は表にて後掲）

4.2.産業振興に有効と考えられる政策・施策（政府が中心となる施策）

- 技術開発における産官学連携の推進と成果の「産」における活用枠組みの拡大・柔軟化
- 企業・組織の情報セキュリティ対策の総点検の枠組みの整備
- 政府機関、重要インフラ等における情報セキュリティ対策整備ロードマップの策定や、それに基づく調達基準の考え方等の提示
- 情報セキュリティ人材の育成と確保
- 情報セキュリティ対策推進・支援税制の検討

4.3.産業界および民間における努力・改善要素（産業界・民間が中心となって取組むべき要素）

- 企業・組織の情報セキュリティ対策の総点検の実施
- サプライチェーン管理における情報セキュリティ対策の連関実現の促進・支援
- 情報セキュリティ産業への産業資金供給の誘導・促進
- IT業界・情報セキュリティ業界における相互交流の促進
- 独自技術開発への積極的取組み

4.4.産業振興手段としての海外進出

- ASEANセキュリティ政策会議、ASEANセキュリティセミナー等、政府のアジア連携政策と連携した、日本のセキュリティ産業のアジア進出・アジア支援
- サプライチェーン管理における情報セキュリティ対策の連関の、アジアにおける実現の促進と、そのための支援の提供
- オフショアリングの活用推進
- 海外進出に際しての公的支援と民間のサポートの充実

4.日本の情報セキュリティ産業の発展と活性化に向けて
取組主体別　検討する具体的施策の例（1）

テーマ	検討課題	主体	検討する具体的施策の例
技術開発	•産官学連携の推進 •成果の「産業」における活用枠組みの拡大・柔軟化 •独自技術開発への積極的取組み	公的機関	•研究開発における公的機関・産官学連携 •公的機関等の開発成果の民間移転活発化 •情報セキュリティ分野の国産技術取組みの強化 •開発された技術の国産製品への搭載支援
		事業者	•独自技術開発への積極的取組み •イノベーションへの取組み強化 •製品化・事業化ノウハウの向上
		金融等	•IT業界・情報セキュリティ業界への投資や融資の活発化 •製品化・事業化時の資金供給と事業化ノウハウ等の指導
		産業全体	•情報セキュリティ産業と産業を取り巻く関係者の相互交流の「場」の創出 •ビジネスチャンス拡大施策としてのマッチング活動 •ユーザも含めた相互交流
情報セキュリティ対策の総点検 （サプライチェーン管理を含めて）	•企業・組織の情報セキュリティ対策の総点検の枠組み整備 •企業・組織の情報セキュリティ対策の総点検の実施 •サプライチェーン管理における情報セキュリティ対策の連関の促進 •アジア諸国展開する日系企業のサプライチェーン管理支援	公的機関	•最新の脅威への対応を可能とするセキュリティ対策の基準やそれに基づく点検・評価の仕組みの再整備 •具体的な、何をどこまで等必要量への踏み込み（日本版FDCCの検討） •「政府機関統一基準」の民間活用のための実装ガイド等の開発、や政府機関の情報セキュリティ対策整備 •情報セキュリティ監査制度の展開
		事業者	•脅威情報の把握とそれらへの対応、政府支援の活用 •「中小企業の情報セキュリティ対策ガイドライン」などに基づく点検・評価および「委託関係における情報セキュリティ対策ガイドライン」による委託先点検・評価に関し、ユーザ企業の実施支援 •上記支援の実効性強化のための技術・サービス開発 •情報セキュリティ技術・管理・サービス・人材の総合的水準向上・レベルアップ •専門知識（コンサルタント・委託先監査等）の展開 •情報セキュリティ監査制度の活用促進
		産業全体	•情報セキュリティ対策の総点検の枠組みへの取組み整備

4.日本の情報セキュリティ産業の発展と活性化に向けて
取組主体別　検討する具体的施策の例（2）

テーマ	検討課題	主体	検討する具体的施策の例
政府機関、重要インフラ等における情報セキュリティ対策整備	•対策整備ロードマップの策定 •調達基準の考え方の提示	公的機関	•「政府機関統一管理基準」「技術基準」の活用 •社会的に重要な位置を占めるものとして、政府機関・重要インフラ等の情報セキュリティ積極投資 •重要インフラにおける情報セキュリティ整備計画の策定と公表
		事業者	•政府・重要インフラの情報セキュリティ整備に向けての中長期的技術開発、マーケティング戦略の強化 •事業者側からの公的機関への提案や計画策定サポート
情報セキュリティ産業を担う人材の育成	•スキルを持った人材育成の促進（人材供給源およびキャリア提示） •資格制度の周知活用 •途上国向け研修とのタイアップ	公的機関	•大学・大学院、高専等の高等教育における情報セキュリティ専攻の充実 •グローバル人材の輩出を念頭においた、実践的カリキュラム開発 •継続的教育への支援（民間教育機関や産業が提供する教育カリキュラム等） •人材育成費用負担軽減施策 •教育機関における情報セキュリティの高度知識・実践的なスキルの提供 •教育機関等における学生などへのキャリアパスの提示 •資格制度やスキル標準と連携した、セキュリティ専門キャリアマップの見直し・開発促進
		事業者	•情報セキュリティの専門知識を持った人材の積極的な育成 •グローバル人材の採用や育成 •オフショア開発、海外採用など、海外の人材活用
		産業全体	•産業における教育カリキュラムの検討、教育機関との連携 •優秀な人材を得るためのキャリアプランの形成と提示 •情報セキュリティ産業人材の教育カリキュラム充実と資金の確保 •産官学共同等による最先端人材・イノベーションを担う人材の育成 •教育機関を通じて、情報セキュリティの高度知識・実践的なスキルの提供
税制等の財政支援	•情報セキュリティ対策推進・支援税制の検討	公的機関	•中小企業をターゲットとした、情報セキュリティ導入負担軽減のための、減税策の維持
産業資金供給の誘導・促進	•情報セキュリティ産業への供給の誘導・促進	公的機関	•情報セキュリティ産業の中長期的見通し提示など、投資を促進する情報発信 •産業発展・市場発展のシナリオの提示 •より積極的な公的産業資金の活用
		事業者	•積極的な製品化への取組みと様々な資金活用の検討 •技術経営力の強化 •ベンチャーキャピタルや公的資金導入に関する情報収集
		産業全体	•魅力的な技術を持った企業の存在のアピール

4.日本の情報セキュリティ産業の発展と活性化に向けて
取組主体別　検討する具体的施策の例（3）

テーマ	検討課題	主体	検討する具体的施策の例
業界における相互交流の促進	•IT業界・情報セキュリティ業界における相互交流の促進	公的機関	•IT業界全体の相互交流の場の提供 •スタートアップ企業グループに対する、展示会の共同出展支援 •公的機関による展示・アピール等の機会提供、展示会等の質的向上 •「未踏プロジェクト」等の情報セキュリティ版などの横展開検討 •金融機関、教育機関、ユーザも巻き込んだ様々なマッチング企画支援
		事業者	•ベンダ・システムインテグレータなど業態や情報セキュリティ業界以外のIT業界全体など、業態や業種を超えた事業定型の活発化 •エンドユーザへの技術アピールの機会の設定
		産業全体	•業界を挙げてのエンドユーザへの技術アピールの機会の設定 •スタートアップ企業グループの展示会共同出展促進 •金融機関、教育機関、ユーザも巻き込んだ様々なマッチング企画
海外特にアジア進出支援	•政府のアジア連携政策との連携 •オフショアリングの活用推進 •アジア進出企業のサプライチェーン支援 •海外進出の公的支援と民間サポート充実	公的機関	•アジアを中心とした情報セキュリティ国際協力の充実（ASEANとの関係強化等） •海外進出のユーザ企業に対する情報セキュリティ取組み支援 •海外情報セキュリティ関連組織との連携強化による海外進出支援・環境整備 •オフショアリング、現地採用、グローバル採用など多様な人材活用法の支援 •情報セキュリティに関し、公的機関によるアジア・アセアン等との情報交換・連携施策の活発化 •公的機関が行うアジア等との連携施策への日本企業の参加促進 •留学・研修制度等の活用支援
海外特にアジア進出支援	•政府のアジア連携政策との連携 •オフショアリングの活用推進 •アジア進出企業のサプライチェーン支援 •海外進出の公的支援と民間サポート充実	事業者	•グローバル化・ボーダレス化への積極的な取組み（輸出、オフショア開発、現地法人設立等の戦略強化） •日系企業の事業展開に合わせた進出検討 •オフショア開発の積極的な取組み（日本の人材不足の補完等） •留学・研修制度の活用
		産業全体	•海外の情報セキュリティ事情や市場動向に関する情報収集と経営戦略上の検討 •グローバル展開をしている日本ユーザ企業へのマーケティング

Information-technology
Promotion
Agency, Japan

「情報セキュリティ産業の構造と活性化に関する調査」
概要報告書

作成：2011年6月

公表：2011年9月

独立行政法人情報処理推進機構
技術本部セキュリティセンター

Tel 03-5978-7530
Fax 03-5978-7546
Isec-info@ipa.go.jp