資料2

IoT社会への対応に向けた
データ利活用・セキュリティ強化施策の論点

平成27年8月19日

商務情報政策局

情報経済小委員会中間取りまとめ（概要）

方向性Ⅰ：制度を変える

【課題】
- ITの技術進歩を前提としていない現行制度が新たなビジネスモデルの創出を躊躇させ、企業間のデータ流通を萎縮させている。

例えば、
- 自動運転と道路交通法との関係、シェアリングビジネスと既存業法との関係など既存規制に抵触する可能性
- セキュリティやプライバシーへの懸念

新ビジネス創出のための制度を整備

－データを活用したビジネス創出のための枠組
－セキュリティリスクへの対応力向上のための枠組み
－上記を含めた情報処理促進法の見直しや執行体制の整備を検討

方向性Ⅱ：チャレンジを促す

【課題】
- 自前主義に固執し、自社の強みを生かした他社との連携によるエコシステムの構築、参画ができていない。
- ベンチャーを含め、ゲームチェンジを起こすチャレンジが限定的

企業間連携により新たな産業モデルを生み出す

－CPSをビジネス化する具体事例を各分野で展開
　・特区活用も含め、規制改革と一体的に推進
　・プライバシー、標準、セキュリティ等のルール策定
－企業間連携の中核拠点として「CPS推進協議会（仮称）」を年内に創設

企業がCPSにチャレンジする環境を抜本的に強化

－攻めのデータ経営への転換を市場が評価する仕組みの構築（情報開示の推進等）
－ゲームチェンジを起こすITスタートアップ企業創出に向け、企業成功者が起業家を育てるスタートアップアクセラレータ組織を組成

方向性Ⅲ：基盤を整備する

【課題1：セキュリティ】
- サイバー攻撃の高度化により、サイバーセキュリティリスクが深刻化。

国がイニシアティブを取った企業等のサイバーセキュリティリスクが深刻化

－CPSの到来を見据えた「セキュリティ経営ガイドライン」策定
－第三者認証の強化による企業等の取り組みを「見える化」、同認証の国際標準化
－サイバー攻撃情報や対応策に関する、官民及び業種の垣根を越えた情報共有の仕組づくり

【課題2：技術】
- CPSの実現を支えるコアテクノロジーの蓄積が不十分

CPSのコアテクノロジーを世界最先端に

－人工知能（AI）の実用化と基礎研究の進展の好循環を生むプラットフォーム機能を果たす人工知能の研究センターを産総研に整備
－外部電源が不要な自立センサシステムや大容量データの処理技術等の研究開発を強化

【課題3：人材】
- IT人材が質・量ともにCPSに対応できていない。下請構造による低い生産性

CPS関連のIT人材確保強化

－インド、ベトナム等の優れたIT人材活用に向け、日本への留学、就職等を支援するための官民の枠組みを構築
－非効率でセキュリティリスクも高い「丸投げ下請」を防止するための「下請ガイドラインの強化
－ITとビジネスの両方がわかるCPSビジネス拡大のための人材確保・育成

今回の討議事項

◆これまでの情報経済小委員会では、データ駆動型社会の実現に向けて必要な施策の方向性について議論をしてきた。中間取りまとめを踏まえ、必要な施策の具体化を図っているところ、今後の委員会においては、施策の進捗の報告とともに、一部論点について更なる深掘りを実施。

＜深掘りが必要な論点＞

利活用

- 論点１：　データを活用した産業モデル創出の戦略的展開
- 論点２：　AI等の技術深化を睨んだ、データの収集を促進する仕組みの構築

セキュリティ

- 論点3(1)：高まるサイバーセキュリティのリスクへの対応　→ ユーザ側
- 論点3(2)：標的となりやすい機関等の対策強化　→ ユーザ側
- 論点3(3)：重要インフラの対策強化　→ ユーザ側
- 論点3(4)：企業のセキュリティ対策強化　→ ユーザ側
- 論点４　：ソフトウェア製品・IoT製品の安全性・信頼性強化　→ ベンダ側
- 論点５　：セキュリティ人材の能力評価制度の在り方　→ ユーザ側・ベンダ側共通
- 論点６　：サイバーセキュリティ産業の成長産業化　→ その他

＜経過報告＞

- 「セキュリティ人材の確保に関する研究会」の設置
- 企業間連携の中核拠点の創設と、ビジネスモデルの発掘
- 市場を活用したIT経営の促進
- 国立研究開発法人産業技術総合研究所人工知能研究センターの整備
- IoT推進に不可欠なコアテクノロジーの技術開発、先進モデル創出

論点

＜深掘りが必要な論点＞

データ利活用

・論点１：　データを活用した産業モデル創出の戦略的展開
・論点２：　AI等の技術深化を睨んだ、データの収集を促進する仕組みの構築

セキュリティ

・論点3(1)：高まるサイバーセキュリティのリスクへの対応
・論点3(2)：標的となりやすい機関等の対策強化
・論点3(3)：重要インフラの対策強化
・論点3(4)：企業のセキュリティ対策強化
・論点４　：ソフトウェア製品・IoT製品の安全性・信頼性強化
・論点５　：セキュリティ人材の能力評価制度の在り方
・論点６　：サイバーセキュリティ産業の成長産業化

論点１　データを活用した産業モデル創出の戦略的展開

◆ あらゆる産業で、付加価値の源泉がデータの利活用に移行し、産業構造が大きく変化。
◆ 企業による新たな産業モデルの創出を加速していくことが必要。

このために、重要分野ごとの課題や状況に応じて、**将来像を共有した上**、**民間やベンチャー等の先駆的なチャレンジの支援**と**官民で規制改革や新たな規格形成を目指した実証的な取組**を展開し、**革新的な産業モデルの創出**を行うべきではないか。

将来像の共有

民間やベンチャー等の先駆的な
チャレンジを支援する取組

官民で規制改革と新たな規格形成を
目指した実証的な取組

あらゆる分野で革新的な産業モデルの創出

例：**自動走行技術を活用した新たなサービスの創出**　（自動タクシー、自動物流　など）

論点２　AI等の技術深化を睨んだ、データの収集・分析を促進する仕組みの構築

◆ データの有効な利活用には、従来からデータの収集・蓄積が重要であったが、人工知能等の開発競争の激化により、その重要性と緊急性が一層増している。

◆ 日本では様々な主体（企業・行政機関・医療機関等）にデータが一定程度蓄積されているものの、その蓄積量は限定的であったり、各機関に分散されているため、統合的な解析ができず、**データが有効に活用されていない**。

AI等を活用しビッグデータ解析を進め、より高度な成果を得るためには、プライバシーに配慮しつつ、**分散したデータの分野を超えた統合、解析を促進する仕組みを構築するべき**ではないか。

強みを生かし、他社との提携を進める国内ベンチャー

自動運転

ロボット開発

iPS細胞研究

AIを用いた
データ解析サービスの開発

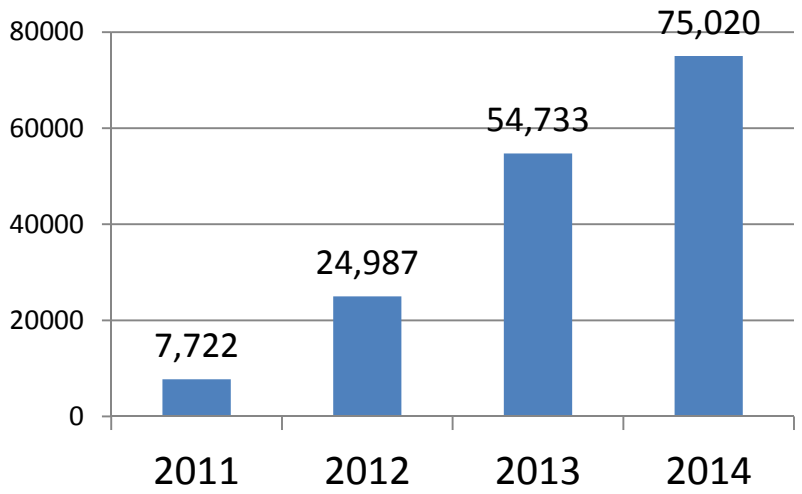
学習済NWを登録・利用・交換する仕組みを開発中

論点3（1） （ユーザ側）高まるサイバーセキュリティのリスクへの対応

◆ 我が国へのサイバー攻撃は、増加傾向・手口も巧妙化。さらに、今後のIoT社会の進展により、脅威も増大。
◆ 政府関係機関や企業への標的型サイバー攻撃により大量の重要情報漏えい事案も発生
◆ 企業規模等に応じて具体的にどの程度のレベルの対策を講じればよいか必ずしも明らかではない。

今後の、政府機関、独立行政法人・特殊法人については総合的な対策強化を図り、対策の不断の見直しが必要ではないか。重要インフラ事業者、民間企業においては、それぞれの持つ情報の性質を踏まえつつ、セキュリティ対策を促す取組を推進すべきではないか。

＜インシデント件数（2011年～の累計）＞



○インシデントの報告受付数は増加傾向。

（出典）JPCERT/CCｲﾝｼﾃﾞﾝﾄ報告対応ﾚﾎﾟｰﾄにおけるｻｲﾊﾞｰ攻撃の報告受付数より経済産業省作成

＜現行のセキュリティ対策の概要＞

国の行政機関	○情報システムへの不正活動の監視 ○対策状況の監査 ○インシデント発生時の原因究明調査 ○サイバー攻撃情報のNISCへの報告義務
独法・特殊法人等	○サイバー攻撃情報の監督官庁への報告
重要インフラ	○NISCの基準（行動計画）による体制整備 ○サイバー攻撃の監督官庁への報告 ○攻撃情報の共有（IPA）
民間企業	○自発的対策の促進 ○ガイドライン等による情報提供、人材育成支援等（IPA）

（出典）サイバーセキュリティ基本法等より経済産業省作成

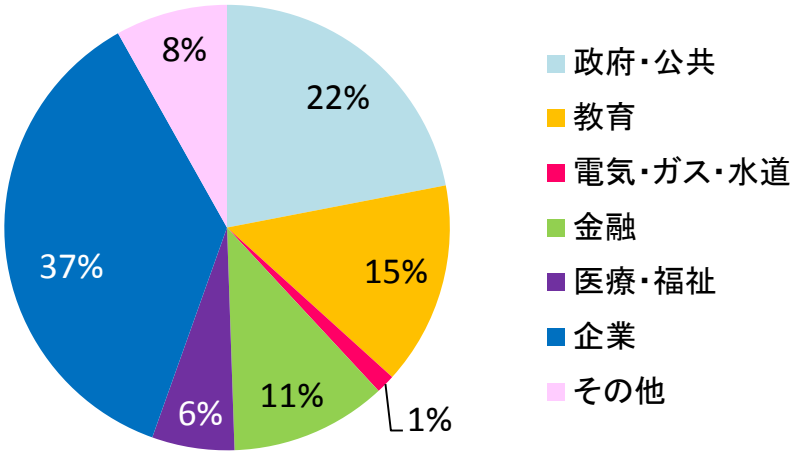
論点3(2)　(ユーザ側)標的となりやすい機関等の対策強化

◆国民生活・経済社会活動の基盤である機能やサービスを提供し、支障が生じると重大な悪影響が生じる可能性がある政府機関や重要インフラなど、標的となりやすい機関におけるセキュリティ強化が必要。

標的となりやすい機関の対策強化にあたり、独法や、府省庁と一体となって公的業務を行う特殊法人等も国の行政機関に準ずる対策を講ずるなど、国全体として対策強化すべきではないか。その中で、適切な役割分担の下、これまで大規模なサイバー攻撃への対処などの機能を提供してきたIPAも、その知見・経験を活かし、積極的に貢献していくべきではないか。

＜情報セキュリティインシデントの発生状況＞

○政府・公共、教育、電気・ガス・水道、金融、医療・福祉に対するインシデントが過半数。



(出典)IPA「情報セキュリティ白書2015」より経済産業省作成

＜ 政府、独法等、企業等に対するのIPAの支援＞

○情報セキュリティに関するガイドライン等を通じた情報提供

○政府、独法・特殊法人等、民間企業に対する重大なサイバー攻撃事案が生じた際のサイバーレスキュー隊による支援（2014年～）

○IPAがサイバー情報共有イニシアティブ(J-CSIP)を運営。重要インフラ等企業（6業種61組織）に対するサイバー攻撃の情報共有体制を強化（2011年～）

論点3（3） （ユーザ側）重要インフラの対策強化

◆ 2020年の東京オリンピックを控え、重要インフラ事業者のセキュリティ対策の強化が重要。
◆ ロンドンオリンピックでは、開会式直前に電力網を対象としたサイバーテロの予告があり、開会式での照明システムへのDoS攻撃が40分間続くなど、サイバー攻撃のリスクが高まった。

重要インフラ事業者に関し、平時における情報共有体制を強化するとともに、緊急時における被害拡大を防ぐことが重要。このため、平時、緊急時それぞれぞれのセキュリティ対策の実効性を高めることを検討すべきではないか。

＜2012年ロンドン・オリンピックで発生した事案＞

○2億件の不正通信をブロック。毎秒約1万件の不正通信があった。

○開会式当日にオリンピックスタジアム等の電力供給の監視制御システムに対するサイバー攻撃。万が一に備え手動での発電に切り替えるべく準備。

（出典）IPA「IPAサイバーセキュリティシンポジウム2014」
オリバー・ホーア氏講演録

＜諸外国における取組＞

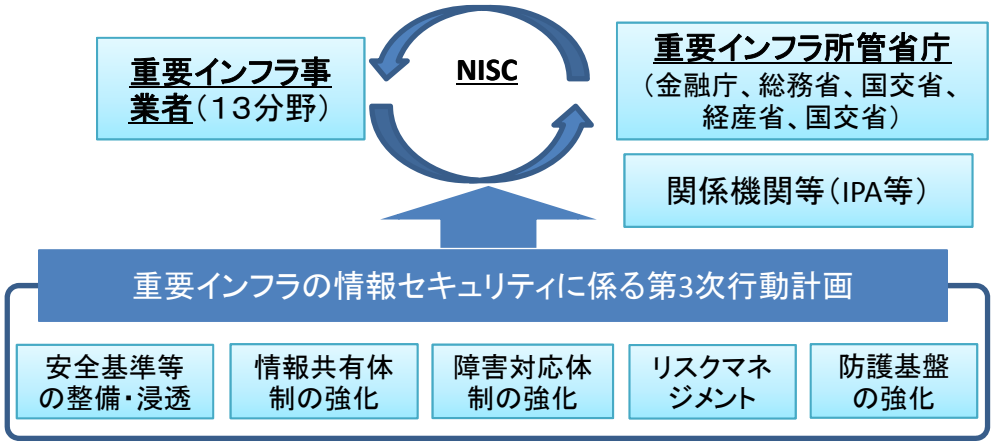
○米国の電力分野では、FERC（連邦エネルギー規制委員会）が、各電力会社に対し、セキュリティ監査等を行うNERC（北米電力信頼度協議会（民間団体））の活動を監督。違反があれば、各電力会社はNERCに対し、罰金を支払う必要あり。

○ドイツでは、重要インフラ事業者に対して、基準に基づく対策を義務づける法律が成立。（2015年）

＜我が国おける取組＞

政府機関は、重要インフラ事業者自らの責任で行う情報セキュリティ対策に対し、以下の支援を実施。

○重要インフラの情報セキュリティに係る第3次行動計画の枠組み（2015年5月改訂）



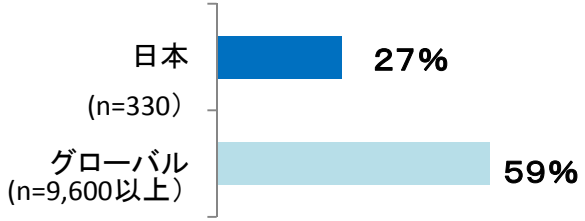
○サイバー情報共有イニシアティブ（J-CSIP）（再掲）

論点3（4） （ユーザ側）企業のセキュリティ対策強化

◆ 我が国においては、経営層のセキュリティ意識が低いことが課題。
◆ また、中小企業においては、セキュリティ対策に割けるランニングコストの余力も少ない。

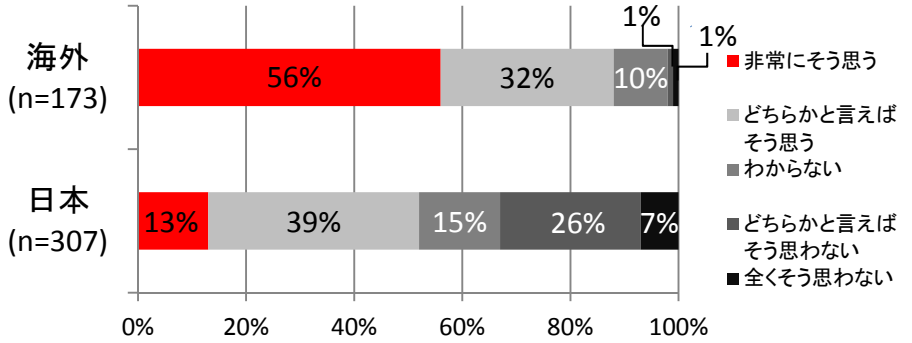
民間のセキュリティ経営の基準となるガイドライン等の整備を加速すべきではないか。また、経営層が主導してセキュリティ対策を積極的に強化する企業が市場から評価される枠組みとしての第三者認証制度の確立などにより、国は、経営層のセキュリティ意識の向上を促していく必要があるのではないか。また、中小企業においては、必ずしも専門家が企業内にいないことも踏まえ、より分かりやすく丁寧な支援を進めるべきではないか。

＜積極的にセキュリティ対策を推進する経営幹部がいる企業＞



（出典）PwC「2014 Global State of Information Security Survey」より経済産業省作成（n=不明）

＜サイバー攻撃の予防は取締役レベルで議論すべきか＞



（出典）KPMG「セキュリティサーベイ2013」より経済産業省作成

日本再興戦略2015

○民間企業における対策の促進

・<u>サイバーセキュリティを確保するために、企業経営上行うべき事項を明確化したガイドラインを策定</u>する。また、サイバーセキュリティ確保に向けた企業の取組に対する<u>第三者評価を促進</u>する。

論点4　（ベンダ側）ソフトウェア製品・IoT製品の安全性・信頼性強化

- ◆ IoTが進む中で、ソフトウェアの欠陥等が与える社会的影響は更に増大。あらゆるモノがつながることで、ソフトウェア単体を超えて、システム全体での安全性・信頼性を検証していくことも重要に。
- ◆ これまで、ソフトウェアの脆弱性については、経済産業省において規定を定め、情報収集や、開発者との調整、公表等の規定を整備。一方、脆弱性のみならず、データの外部送信、システム障害等のソフトウェアリスクや、システム開発・運用における取引の安全性確保の問題も課題となっている。

ソフトウェア製品・IoT製品・システム開発等の広範な安全性・信頼性上の問題に対し、リスク情報取扱制度や安全基準、ガイドライン等の整備を行っていくべきではないか。

＜ソフトウェアの安全性・信頼性上の問題＞

1．脆弱性

サイバー攻撃により機能等を損なう原因となる欠陥

（事例）

2015年7月、クライスラーの自動車に搭載されたシステムに脆弱性が発見され、ブレーキやエンジンのオン/オフが遠隔から操作できることが発覚。47万台超に影響が及んだ。

2．データの外部送信

ユーザに無断でデータの外部送信が行われる問題

（事例）

2013年12月、バイドゥ（株）が提供している日本語入力システムが、ユーザに無断で入力情報を外部サーバに送信していることが判明。

3．瑕疵（バグ）

システム障害の原因となる欠陥

（事例）

2015年4月、米国情報会社ブルームバーグの取引システムに障害が発生し、英国債の入札が延期になるなど世界金融市場で広範な影響が出た。

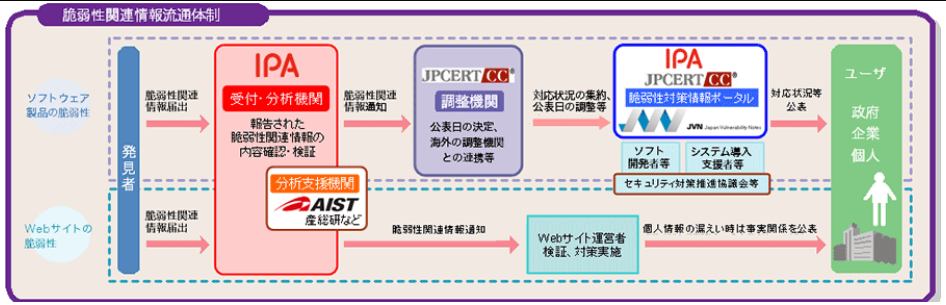
＜システム開発・運用における安全性・信頼性上の問題＞

丸投げ下請によるリスク増大

適切に管理されていないソフトウェア開発・運用の多重下請契約が、個人情報漏洩等セキュリティリスクの増大につながっている事例が存在。

＜ソフトウェア脆弱性の取扱フロー＞

- ➢ ソフトウェア脆弱性については、平成16年に経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」を定め、IPAを窓口とした情報収集等の取り扱いが定められている。



（出典）一般社団法人JPCERTコーディネーションセンター、産業技術総合研究所作成

論点５　（共通）セキュリティ人材の能力評価制度の在り方

◆ 日本企業のセキュリティ対策において不足している人材は約8万人であり、さらに、現在、企業でセキュリティ対策に取り組む人材のうち16万人はスキル不足と試算されている。（2011年時点データでのIPA推計）

◆ ユーザ側、ベンダ側双方で、セキュリティ人材の育成、登用、活用を進めていくことが必要。そのためには、社会におけるセキュリティ人材の能力を評価する仕組みが必要。

情報処理技術者試験を改革し、必要とされる人材像に基づいた試験創設や、常に能力を評価・担保できる更新制の仕組みの導入が必要ではないか。（「セキュリティ人材の確保に関する研究会」（P15参照）で検討中）

人材像

情報セキュリティマネジメント人材

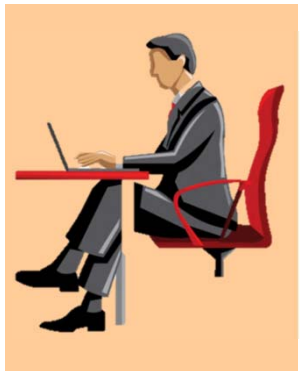
（情報セキュリティを利用者側の現場で管理する者）

（典型的な人材像：事業部門セキュリティ管理者）

- 事業部門でITを活用した事業の企画・推進等を担当しつつ、**平時においてはセキュリティポリシーの運用を行いつつ、トラブル発生時においては部門長やセキュリティ技術者と連携して被害の最小化を図る。**

情報セキュリティスペシャリスト人材

（安全な情報システムを作る者）



（典型的な人材像：セキュリティ技術者）

- 情報セキュリティ分野を専門とするIT技術者であり、**情報システムのセキュリティ機能を実装し、**また、**情報セキュリティ技術の専門家として情報セキュリティ管理を支援する。**
- **高度化するサイバー攻撃やITの技術革新などの動向を常に情報収集し、セキュリティ対策のアップデートを図っていく。**

（参考）
米国の民間セキュリティ資格CISSPでは、資格登録後、3年ごとに、講習等を受けることを登録更新要件として義務付け。（情報処理技術者試験には、更新の仕組みなし）

ユーザ企業においてセキュリティ対策のマネジメントをできる人材の評価の基準となる新試験を来年春に導入。

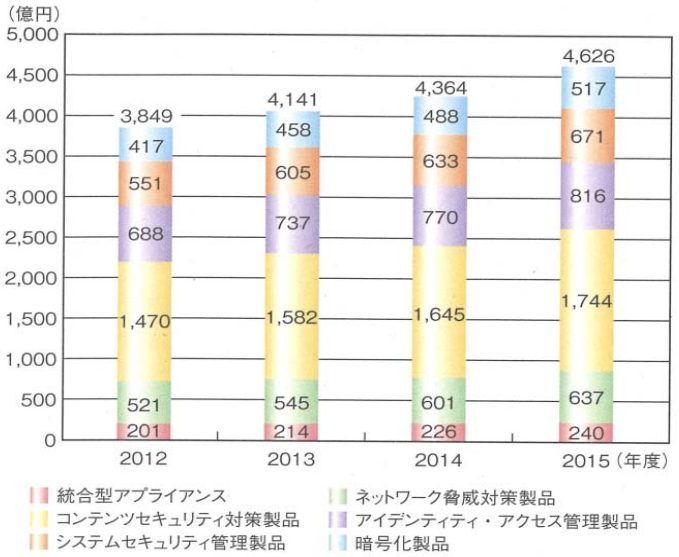
登録更新制の導入等により、能力を適時適切に評価できる試験制度の充実にむけた検討を行う。

論点6　（その他）サイバーセキュリティ産業の成長産業化

- ◆ 今後、コンサルティングや人材育成ビジネスを含むサイバーセキュリティ関連産業に対する需要が一層増加することが見込まれる。
- ◆ サイバーセキュリティ分野では、激しい変化に対する機動性が求められるところ、革新的な新規事業や技術開発に挑戦するベンチャー企業等の活性化が重要。

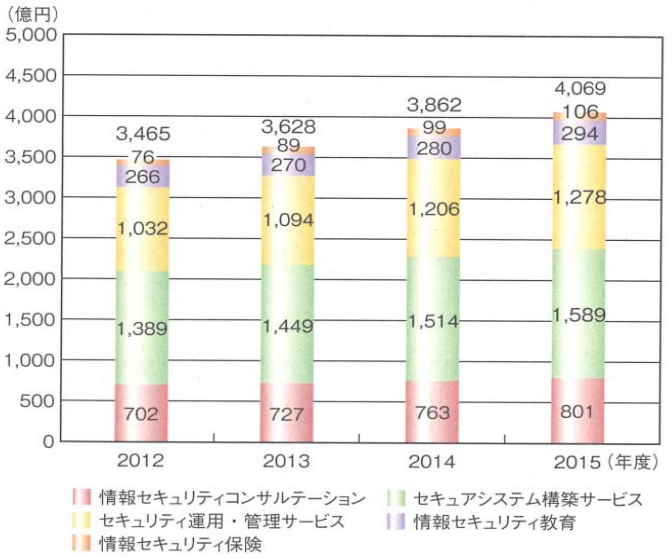
サイバーセキュリティ産業の成長産業化に向けて、政府系ファンド等を活用した投資などにより、国内外で大規模に活躍できるベンチャー企業等の振興が必要ではないか。

＜国内情報セキュリティツール市場規模の推移＞



（出典）IPA「情報セキュリティ白書2015」

＜国内情報セキュリティサービス市場規模の推移＞



（出典）IPA「情報セキュリティ白書2015」

経過報告

・「セキュリティ人材の確保に関する研究会」の設置
・企業間連携の中核拠点の創設と、ビジネスモデルの発掘
・市場を活用したIT経営の促進
・国立研究開発法人産業技術総合研究所人工知能研究センターの整備
・IoT推進に不可欠なコアテクノロジーの技術開発、先進モデル創出

報告　「セキュリティ人材の確保に関する研究会」の設置

◆ セキュリティ関連人材の実践的な能力を客観的かつ継続的に保証できるような制度について専門的な検討を行うため、研究会を設置する。

＜メンバー構成＞

有賀貞一	AITコンサルティング（株）代表取締役
岩丸良明	東京工業大学特任教授（情報処理技術者試験委員長）
鵜飼裕司	（株）FFRI代表取締役社長
富永由加里	（株）日立ソリューションズ 常務執行役員
浜田達夫	（一社）日本情報システム・ユーザー協会常務理事
原田要之助	情報セキュリティ大学院大学 教授
三谷慶一郎	（株）NTTデータ経営研究所 情報戦略コンサルティングユニット長
三輪信雄	S＆J（株）代表取締役社長
オブザーバ	内閣サイバーセキュリティセンター 文部科学省（専門教育課）

＜スケジュール＞

- 平成27年8月設置
- 研究会において集中的に検討を行い、その結果は9月上旬までにとりまとめ、産業構造審議会の関係会議体に報告する。

＜庶務＞

経済産業省商務情報政策局情報処理振興課
（独）情報処理推進機構

＜主な論点＞

（論点1）
登録制導入の意義について

（論点2）
登録制の対象となる試験や資格の範囲・名称

（論点3）
登録制の導入方法について
- ✓ 登録条件（取消条件）
- ✓ 更新条件、更新年限　等

（論点4）
試験・資格の普及・活用方策について

（論点5）
登録制導入に対しての経過措置

報告　企業間連携の中核拠点の創設と、ビジネスモデルの発掘

IoT推進の新たな枠組み

狙い

- AI・IoTを活用した革新的なプロジェクトの創出
- これを実現するために必要な規制改革の提言とルール形成
- グローバルかつ業界横断的な企業間連携の促進
- 価値創造型IoT投資への企業マインドの変革

チャレンジ促進のための規制改革等の提言

- 将来像を議論するとともに、それを実現するために必要な規制改革等について政府へ提言を行う場を設置。

セキュリティ・プライバシー等の基盤整備

- セキュリティ、プライバシー等、IoT推進のための基盤整備を行う専門家WGを設置。

IoT プロジェクトの発掘・実現

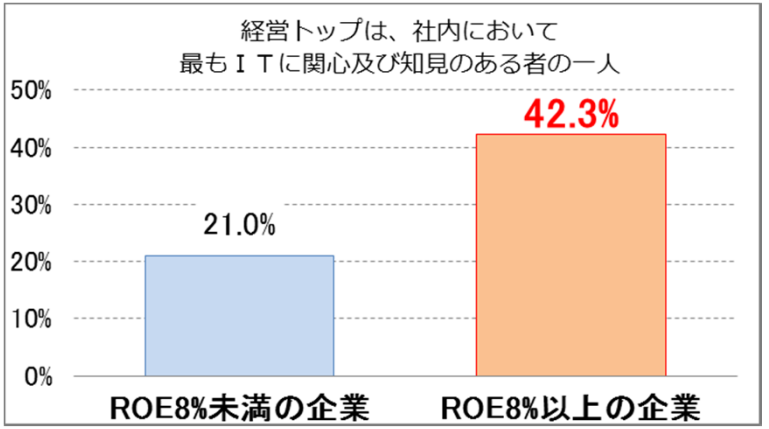
- 民間主導のユースケースを掘り起こし、その実現に必要な具体的なプロジェクトを立ち上げ。

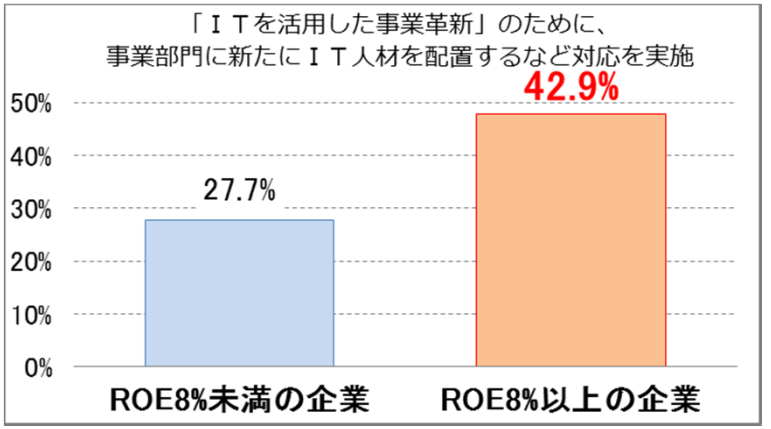
報告　市場を活用したIT経営の推進

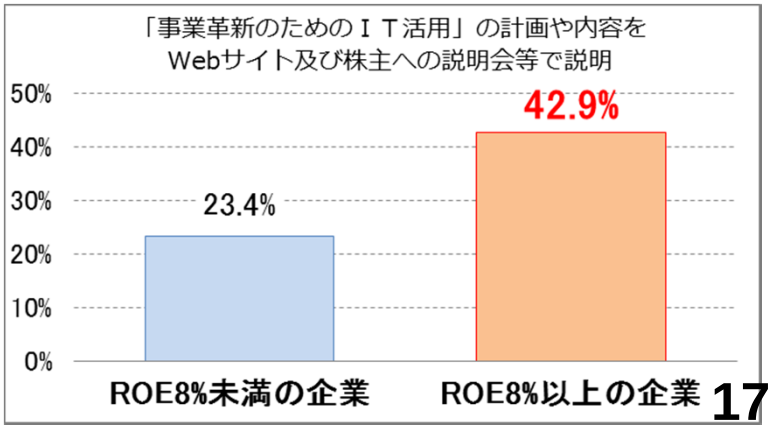
- ビジネスモデルを改革する戦略的IT投資の促進に向け、経済産業省・東京証券取引所が共同で「攻めのIT経営銘柄」を選定。平成27年5月28日公表。（下表）
- 本銘柄の選定の過程で、東証に上場する全企業を対象としIT活用のアンケートを行ったところ、210社から回答があり、ROEが高い企業では、積極的にIT活用の体制をとっている等の共通する特徴を確認。（右グラフ）

＜攻めのIT経営銘柄選定企業＞（全33業種のうち18業種について各1社選定）

選定された企業一覧	業種
積水ハウス株式会社	建設業
アサヒグループホールディングス株式会社	食料品
東レ株式会社	繊維製品
株式会社エフピコ	化学
株式会社ブリヂストン	ゴム製品
JFEホールディングス株式会社	鉄鋼
株式会社小松製作所	機械
株式会社日立製作所	電気機器
日産自動車株式会社	輸送用機器
株式会社ニコン	精密機器
トッパン・フォームズ株式会社	その他製品
大阪ガス株式会社	電気・ガス業
東日本旅客鉄道株式会社	陸運業
株式会社アルファポリス	情報・通信業
三井物産株式会社	卸売業
株式会社三井住友フィナンシャルグループ	銀行業
東京海上ホールディングス株式会社	保険業
東京センチュリーリース株式会社	その他金融業



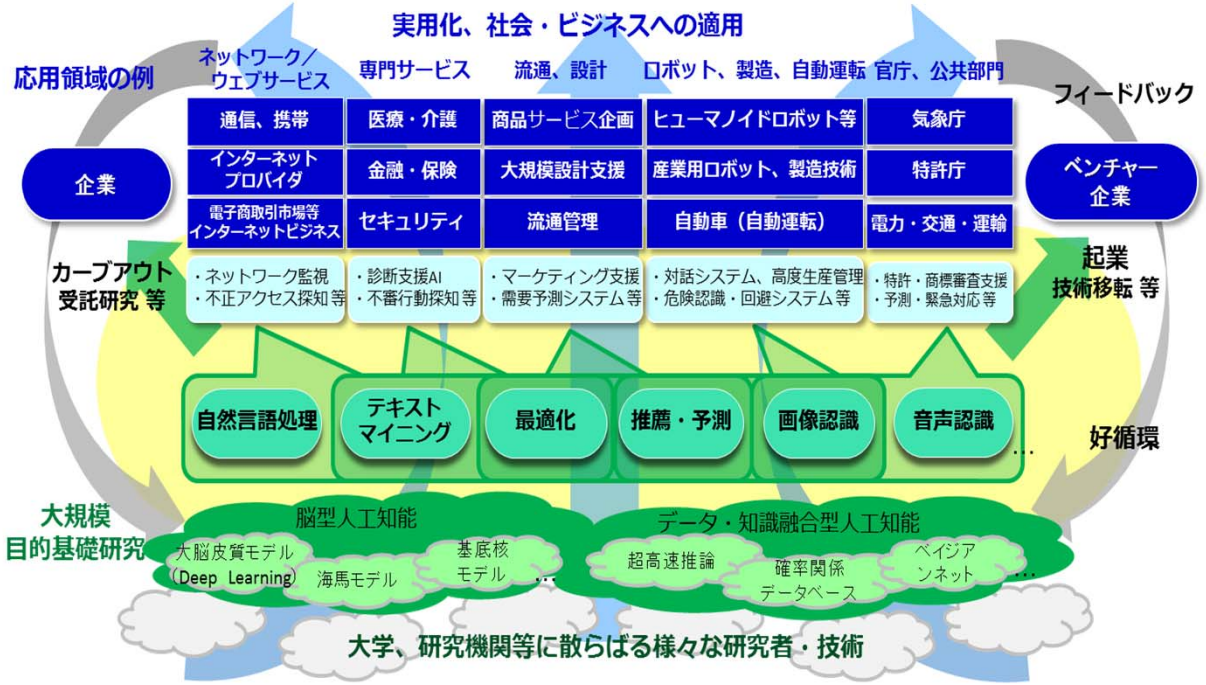




報告　国立研究開発法人産業技術総合研究所人工知能研究センターの整備

- ◆ 人工知能分野で、基礎研究と実用化等の好循環を生むことを目指して、平成27年5月に国立研究開発法人産業技術総合研究所に人工知能研究センターを設立。
- ◆ 国内外の優れた研究者・技術を集結し、ビッグデータを活用した研究、人材育成等も推進していく。

名称：人工知能研究センター
センター長：辻井 潤一（前マイクロソフト・リサーチ・アジア首席研究員）
設立：平成27年5月
場所：産業技術総合研究所臨海副都心センター内（東京都港区台場）
　一部つくばセンターとも連携
体制：100名超（産総研常勤研究員、招聘研究員（クロスアポイントメント等含む）、客員研究員等合わせて）

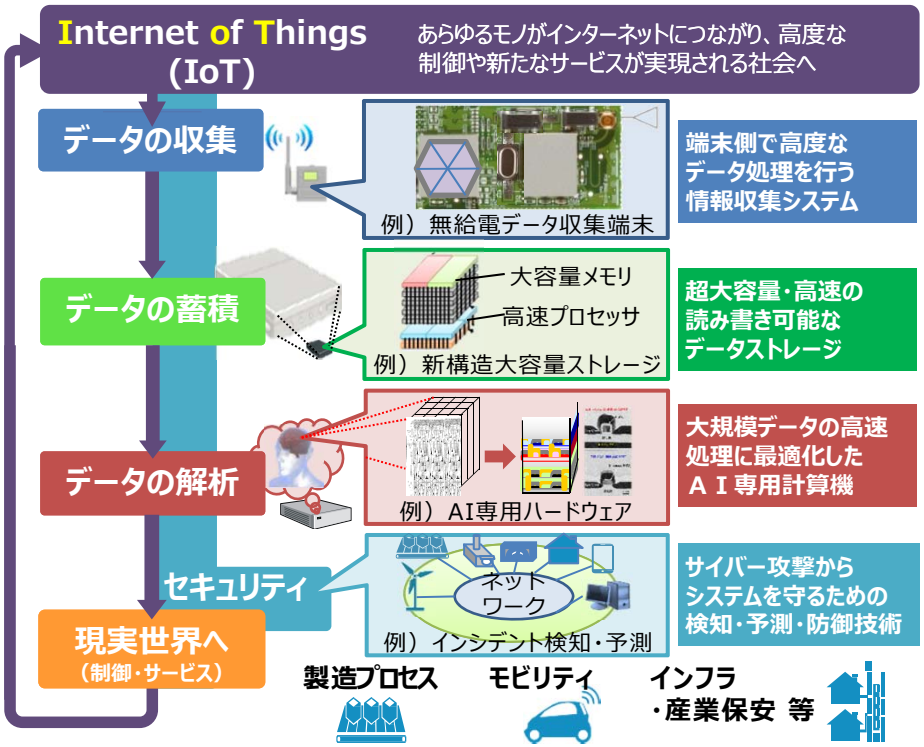


報告　IoT推進に不可欠なコアテクノロジーの技術開発、先進モデル創出

◆ IoTによる効率的で高度なデータ利活用を実現するため、端末（センサー）側でのデータ処理技術を始め、データの収集・蓄積・解析技術といった分野横断的に活用可能な共通基盤技術の研究開発を推進。

◆ また、モビリティ、製造・工場、行政・インフラ等の各分野におけるデータを活用した先進モデルを創出する。課題となる規制・制度や民間企業のビジネスモデル・商慣習等を見直すとともに、行政及び民間企業のデータ利活用を推進。

IoT推進のための横断技術開発プロジェクト



IoT推進のための社会システム整備等

各分野における先進モデル創出

○自動走行（モビリティ）

地図情報や、センサーから取得した信号、自動車の位置情報等を蓄積、解析し、その結果を反映することで、自動走行の実現とそれによる交通事故の減少や環境負荷の低減を実現

○製造・工場

設備の稼働状況や在庫状況など、設計～生産～販売部門から取得したデータ等を蓄積、解析し、その結果を反映することで、需要を予測した効率的な工場生産を実現

○行政・インフラ

各設備の稼働状況や保安点検記録データ、過去の気温と需要データ等を蓄積、解析し、その結果を反映することで、最適な設備更新とインフラ運営を実現