【産業競争力懇談会2011年度　プロジェクト　最終報告】

【個人情報や企業情報を活用するための クラウドコンピューティング基盤の整備】

２０１２年３月６日

産業競争力懇談会 COCN

【エクゼクティブサマリ】

１．本プロジェクトの基本的な考え方

昨今、ICT ベンダ各社が個人や企業に対してクラウドサービスを本格的に提供し始めている。しかしながら、利便性を向上させるために必要となる、共通番号で紐付けられた個人情報や企業情報を安心・安全に共有するための共通基盤がいまだ存在していない。不特定多数の利用者のプライバシーや、やり取りされる様々な情報に対するセキュリティを担保しながら、個人情報や企業情報を収集・管理・共有するための基盤を構築して、これらの情報を共有できれば、種々の新たなサービスやサービス間連携を生み出すことができ、日本の産業競争力強化につながる。

また、このような情報を安全にクラウド上で管理し、必要に応じて連携して取り出せる仕組みを実現すれば、東日本大震災時に見受けられた様々な個人の生活に必要な情報を記録した書類（身分証・通帳、戸籍、住民票、健康保険証、処方箋 等）を紛失した場合にも、迅速な再発行、あるいは紛失時における柔軟な対応が可能となる。このような基盤を構築することにより、種々の災害に対して対応可能な Resiliency を有する ICT 基盤の構築を目指す必要がある。COCN は、個人情報や企業情報を活用するためのクラウドコンピューティング基盤の整備について、情報の利活用を促進するために検討が必要な法制度や、開発・構築が必要な技術・システムについて提言する。

２．今年度の活動

昨年度検討を行った内容をもとに、具体的な基盤のあり方についての検討や、新しいユースケースについての検討を行った。特に今年度は、平成 23 年 3 月に発生した東日本大震災により引き起こされた様々な事象も踏まえ、昨年度検討したクラウドコンピューティング基盤が、防災や減災にもつながるものとなるような議論も行った。なお、今年度は、医療分野、セキュリティ分野、製品安全分野の 3 分野で検討した。

（１）　医療分野

医療分野の検討においては、昨年度の検討内容をベースに、平常時はもとより大規模災害時においても有効に機能する「災害医療支援基盤」について検討した。本基盤を実現することにより、東日本大震災で明らかになった医療分野における様々な課題や、生活面での課題の克服に寄与することができる大規模災害時においても現地・遠隔地のリソースを最大限に活用して、医療の継続性を確保できる。また国民・個人のメリットとしては、被災により様々な不便を強いられた場合に、被災直後から復興時までの長い期間、その時々のニーズに応じて医療・介護や生活面等での様々な支援サービスを受けることが可能となる。また、クラウドコンピューティング基盤で共有した医療情報の利活用例として、治験分野での二次利用や、医療分野以外での活用についても検討した。治験分野で医療情報を二次利用することにより、わが国の医薬品や医療機器開発における国際競争力の向上や、医療現場におけるより良い医療の提供などに繋がる。さらに医療情報を医療分野以外で活用（三次利用）することにより、既存の製品・サービスに新たに「健康機能」を追加できるだけでなく、全く新しい ICT ビジネス領域を切り開くことにも繋がりうる。また国民・個人のメリットとしては、このような治験環境の改善や健康機能を取り込んだ新サービスにより、日々の生活をより健康的に過ごすことが可能となる。

（２）　製品安全分野

製品安全分野の検討においては、昨年度の検討内容をベースに、クラウド基盤化のメリットの訴求と東日本大震災で明らかになった課題や状況変化の反映を目的に、まずクラウド基盤上のサービス（SaaS：Software as a Services）としての視点で「製品安全情報管理クラウド基盤」について深堀を行い、ニーズ、必要な機能および技術、さらにそれらの有用性、実用性を検証するための観点などについて検討を行った。本基盤を実現することにより、製品の一連のライフサイクルを共通インフラで管理できるようになり、製品の価値を高めることにつながる。また国民・個人のメリットとしては、製品安全に関する情報提供を迅速かつ正確に受け取ることが可能となるとともに、被災時における各種製品の所有者情報の確認等も可能となる。

（３）　セキュリティ分野

セキュリティ分野の検討においては、昨年度の検討内容をベースに、権限保有者による不正を抑止するための第三者機関によるセキュリティ監査技術のあり方について検討した。第三者機関によるセキュリティ監査技術を確立することにより、番号制度を民間利用する上で、国民が不安に思っている権限保有者による目的外利用や、本人の許可なしでの情報流通などを抑止することが可能となる。これにより、番号制度の民間利用への国民の不安感を取り除くことに寄与できる。またそのほかの活動として、昨年度の検討成果について学会発表を行った。

３．クラウドコンピューティング基盤の整備に向けた提言

（１）　番号制度の民間活用に基づく、情報共有による産業競争力強化

産業競争力を強化するために、個人情報や企業情報を安全に組織間で共有するクラウドコンピューティング基盤の構築により、種々の社会システムを効率化すると共に、種々の新サービスを構築し、新たな社会基盤を早期構築すること。また、様々な分野における多種多様な情報の連携性を高め、各種の情報を紐付けするための個人番号の民間活用を早期に実現するためにも、社会保障･税番号大綱の適用領域の拡大について、より早期に検討着手すること。

（２）　震災対応に向けての基盤整備

首都圏直下型地震ならびに東海・南海・東南海地震による災害が今後 10 年以内に発生する可能性が極めて高いことを鑑み、災害医療支援基盤ならびに、製品安全情報共有クラウド基盤を早期に構築し、次なる大震災への備えとすること。

（３）　医療関連情報の利活用による産業競争力の強化

医薬品、医療機器の開発に必要な治験環境を充実させることができる、あるいは他の産業にも応用可能とすることで、医療分野の産業のみならず他の多くの産業分野において、健康を日本の産業の強みにすることができる、医療関連情報を利活用できる情報基盤を実現すること。

（４）　情報の利活用が正しく行われていることを確認できる監査システムの実現

個人情報が安全に利活用されるためには、不正利用されていないか確認できる仕組みが必要である。そのための監査システムは大量の監査ログを処理する必要があるため、監査機能の標準化とクラウドにより高速処理できる監査システムを実現すること。

【目　次】

【はじめに】

ブロードバンドインフラストラクチャの充実やIP化の進展に伴い、種々のサービスがインターネット上で提供されるクラウドコンピューティングの時代が到来しつつある。しかしながら、情報通信分野に関する国際競争力比較では、日本は高速性や利用料金といったハードウェアインフラの面では世界最先端であるにも関わらず、その普及度や電子政府といった利活用面においては低い評価となっている。つまり、ハードウェアインフラの整備は進んでいるが、それが十分に有効活用されていないことにより、消えた年金や社会保障の不正受給等、国民一人ひとりの権利が損なわれる事態を生じさせている。この利活用が進んでいない原因の一つに、個人情報や企業情報の有効な活用が進んでいないという課題がある。また、プライバシーと個人情報の保護が過度に強調される結果、その活用が限定的になってしまうことも懸念されている。この問題を解決するためには、個人情報や企業情報を安全に組織間で共有するための技術開発と、その活用を妨げている要因を取り除くことを併せて進める必要がある。COCNは、個人情報や企業情報を活用するためのクラウドコンピューティング基盤の整備について、情報の利活用を促進するために検討が必要な法制度や、開発・構築が必要な技術・システムについて提言する。

これからのインターネットサービスは、特定の企業が提供する特定のクラウド上で提供されるサービスではなく、金融や医療など異なる分野の企業や機関による複合的なサービスや、さらに政府や自治体といった公共機関とも連携した総合的・統合的なサービスがマルチクラウド環境で提供されていくものと考えられる。その際、クラウド間でサービスを連携するためには、それぞれのクラウドが有する情報を相互に関連付けることが重要な課題になってくる。本プロジェクトでは情報を関連付ける手段として、国の番号制度で検討されている個人を個々に識別することができる番号を、公的分野のみならず民間サービスも含めて利用すべきとした。この番号による情報の関連付けは、国民生活を豊かにし、より便利にする新たなサービスを生み出すと期待される。同時に、各種情報を関連付けることによるセキュリティ上の問題については十分な配慮と対策が必要である。今年度は、医療分野、製品安全分野、セキュリティ分野の3つのワーキンググループで検討している。また、平成23年3月に発生した東日本大震災により引き起こされた様々な事象も踏まえ、昨年度検討したクラウドコンピューティング基盤が、防災や減災にもつながるものとなるような議論も行った。

本プロジェクトが目指す、複数のクラウドが連携して、個人情報や企業情報を活用することを可能にするクラウドコンピューティング基盤は、国民生活における国民負担を軽減し利便性を大幅に向上させ、様々な新たなサービスを実現する基盤となるものである。そして、その結果として国民一人ひとりの権利を守り、公平・公正な社会を構築することに資するとともに、新産業の創出、および既存産業の活性化を通して我が国の産業競争力強化につながると考えられる。官民を挙げてその実現に向けて取り組むことを期待する。

産業競争力懇談会
会長（代表幹事）
榊　原　　定　征

【プロジェクトメンバー】

プロジェクトリーダー：	日本電気株式会社	江村　克己	
サブ・リーダー：	日本電気株式会社	中田　登志之	
メンバー：	日本電気株式会社	青木　英司	岩本　真治
		佐古　和恵	側高　幸治
		三宮　禎資	高島　洋典
		名倉　賢	宮内　幸司
		宮川　伸也	山田　達也
		山中　勝文	吉本　明平
		伊藤　直子（9 月まで参画）	
		佐治　信之（12 月まで参画）	
	株式会社　日立製作所	小島　啓二	堀田　多加志
		尾内　享裕	洲崎　誠一
		赤津　雅晴	畠山　靖彦
		藤城　孝宏	坂崎　尚生
		神山　卓也	及川　道雄
		安細　康介	
	富士通株式会社	吉川　誠一	渋谷　俊昭
		阪井　洋之	佐々木　繁
		加藤　雅之	松田　竜太
		野村　昌弘	内藤　洋二
		五十嵐　俊哉	中川　昌彦
		御魚谷　武	下江　達二
		鳥居　直也	島田　宏
		長谷部　高行（9 月まで参画）	
	株式会社　東芝	内平　直志	西川　武一郎
	東芝ソリューション株式会社	岩崎　元一	守安　隆
		山田　朝彦	
	産業技術総合研究所	関口　智嗣	渡邊　創
		大岩　寛	田中　良夫
	第一三共株式会社	松下　泰之	古賀　貞一郎
		高鳥　登志郎	
	中外製薬株式会社	安達　秀樹	佐藤　隆司
		相川　仁（5 月まで参画）	
	早稲田大学	松島　裕一	中島　徹
	ソニー株式会社	星野　真由美	

１．本プロジェクトの概要

総務省により公開されている情報通信分野に関する国際競争力比較では、日本は高速性や利用料金といったハードウェアインフラの面では世界最先端であるにも関わらず、その普及度や電子政府といった利活用面においては低い評価となっている。具体的には、主要 30 ヶ国中、基盤（整備）面では第 1 位（総合）ながら、基盤（普及）面では第 12 位（総合）、利活用面では第 18 位（総合）という結果が示されている[1]。特に、普及において携帯電話普及率が第 25 位、携帯電話利用料金が第 27 位、利活用において個人の利活用は第 12 位、政府の利活用は第 23 位と、極めて低い順位となっている[1]。これはつまり、ハードウェアインフラの整備は進んでいるが、それが十分に有効活用されていないことを意味している。

このような、国民や政府による ICT の利活用が進んでいない原因の 1 つとして、個人情報や企業情報の有効な活用が進んでいないという課題がある。また、プライバシーと個人情報の保護が過度に強調される結果、その活用が限定的になってしまうことも懸念されている。このことが巡り巡って、消えた年金や社会保障の不正受給等、国民一人ひとりの権利が損なわれる事態を生んでいる。この情報活用問題を解決するためには、個人情報や企業情報を安全に組織間で共有するための技術開発と、その活用を妨げている要因を取り除いていくことを併せて進める必要がある。

我々は、上記の課題解決に向け、個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備について、情報の利活用を促進するために検討が必要な法制度や、開発・構築が必要な技術・システムについて提言することを目的に、平成 22 年度より本プロジェクトをスタートさせ、提言を行ってきた。

今年度は、昨年度の提言をベースに、以下の 4 点を産業競争力強化のための目標として具体的な実証実験の内容についての検討・提案活動を継続した。

（１）東日本大震災等の災害の復興時に種々の災害対応サービスを提供することにより、罹災した方々への支援を迅速に行うとともに、種々の産業の復興にも貢献できるような ICT 利活用の仕組みを作り上げること。ポスト震災時代に必要とされる、Resiliency を有する ICT 基盤を構築すること。

（２）他国に比べて様々な課題を持つ日本の治験環境について、医療情報を活用することにより充実させる仕組みを作り上げること。また、医療情報を医療分野以外の産業へと応用可能とすることにより、医療分野の産業のみならず他の多くの産業分野において、健康を日本の産業の強みとできるような仕組みを作り上げること。

（３）製品に関する一連のライフサイクル（製造情報、試験情報、使用状況、修理・保守状況、廃棄情報等）をクラウド基盤上で共有し、平時にも有事にも対応可能な品質情報管理システムを共通サービスとして提供する仕組みを作り上げること。

（４）クラウドコンピューティング基盤を用いて個人情報を安全に利活用するために、権限保有者による不正利用が行われていないかどうかを第三者機関により監査する仕組みを作り上げること。

２．昨年度の成果

昨年度、我々は個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤において情報の利活用を促進するために検討が必要な法制度や、開発・構築が必要な技術・システムについて検討を行い、最終報告として以下の 5 つの提言を取りまとめた。

（１）官の管理する個人番号、個人情報の民間活用

（平成 22 年度最終報告書作成時点において）国で検討されている国民 ID あるいは共通番号制度の個人を特定することができる番号、および官の管理する個人情報を、民間のサービスにおいても個人を特定するために利用できるようにすること。それにより、民間のサービスにおいて住民票、戸籍等で行っていた本人確認が容易かつ信頼性の高いものとなり、サービスの提供者、および利用者双方に大きなメリットをもたらす。また民間および官民連携の新たな利便性の高いサービスを生み出す基盤ともなり得る。

（２）個人番号管理センターの設立

国の番号制度や官の管理する個人情報を民間で利用するための機関（個人番号管理センター）を設立すること。このセンターは、クラウドコンピューティング基盤がこの個人番号を利用する場合、国の番号制度を運用しているシステムと民間サービスを直接接続するのではなく、個人番号や個人情報の安全な取り扱いや、国や自治体等の公的機関のもつ信頼性を保つために双方のシステムを中継する機関である。

（３）第三者機関の設置

本プロジェクトで提案するクラウドコンピューティング基盤やその上で実現されるサービスにおいて、個人番号や個人情報の利用が正しく行われているかを監査する第三者機関を設置すること。その機関は、番号の取り扱いを監査する機能を持ち、個人番号および個人情報について個人の意図しない利用がされていないことを担保する機関である。

（４）関連する法制度、ガイドラインの検討

国の番号制度や官の管理する個人情報を民間活用するために法制度の見直しやガイドラインについての検討を行うこと。そのなかで、個人番号や個人情報の不正行為に対する罰則や個人情報、個人番号を扱う担当者の責任範囲を定める制度の制定に関連する検討も必要となる。また、それに加えて個人番号管理センターや第三者機関を設置するための制度の制定が必要である。

（５）官民連携しての技術開発およびシステムの開発、実証

サービスを実現する上での技術課題については、以下に挙げる技術開発を進めていくことやシステムの実現性を実証するための実験を通じて解決していくこと。

- 本人の意思を反映した情報アクセス制御が可能なシステムの開発と実証。
- 大量、かつ長期にわたる安全な情報のライフサイクル管理を可能とするシステムの開発と実証。
- 確実に情報を匿名化する技術の開発。
- 長期間（無期限で）データを安全に保存、簡単に利用できる技術の開発。
- 膨大な時系列データの効率的処理技術の開発。

３．東日本大震災からの教訓

平成 23 年 3 月 11 日に発生した、マグニチュード 9.0 という日本観測史上最大の巨大地震とそれに起因する大規模な津波によって、社会を支えるほとんどのインフラが大きな打撃を受けた。想定を遥かに超える揺れと津波であったことは事実であるが、十分に整備したつもりの社会インフラが、思いのほか脆弱なものであったことを強く印象付ける結果となった。地震発生による主な被害状況について表 ３－１－１に示す。

表 ３－１－１　東日本大震災による主な被害状況（被災直後～復旧初期）[2]

分野	内容
電気	停電戸数：約 466 万戸（東北電力管内）、約 405 万戸（東京電力管内）
ガス	供給停止戸数（岩手県、宮城県、福島県）：約 42 万戸（都市ガス）、約 166 万戸（LP ガス）
水道	供給停止戸数：約 229 万戸（19 県）
下水道等	【下水道】稼動停止：下水処理施設 48 箇所、ポンプ施設 78 箇所（1 都 11 県） 【集落排水】被災：403 地区（11 県）
通信	【固定回線】不通：約 100 万回線 【携帯電話】基地局停波：約 14,800 局
銀行	東北 6 県および茨城県に本店のある 72 金融機関の営業店約 2,700 中 280 が閉鎖
流通業	被災地の総合スーパーの約 3 割、コンビニ店舗の 4 割強が営業停止
宅急便	震災直後から 1 週間程度、全サービス休止（岩手県、宮城県、福島県）
放送	テレビ中継局停波：120 箇所 ラジオ中継局停波：4 箇所
道路	通行止め：高速道路 15 路線、直轄道路 69 区間、都道府県等管理国道 102 区間、都道府県動等 539 区間
鉄道	運行休止：東北・山形・秋田新幹線を含む、23 社 66 路線
バス	車両損害：196 両（東北 3 県）
航空	使用不能：1 空港、施設損壊：2 空港
港湾	港湾機能停止：国際拠点港湾及び重要港湾 14 港、地方港湾 19 港
文教施設	施設の倒壊、半焼、津波による流出： 国立学校施設 76 校、公立学校施設 6,414 校、社会教育・体育、文化施設 2,928 施設
医療施設	381 病院中、全壊 11 病院、一部損壊 296 病院（岩手県、宮城県、福島県）

一部のインフラについては、強靭な耐性や迅速な回復力を示したものも存在する。

- 運転中の 27 本の東北新幹線はいずれも安全に停止し、脱線・転覆等の事故を防止した。
- 通信規制のかかった固定通信・移動通信の代わりに、Twitter や Facebook など、インターネットを介した SNS による情報交換が行われた。
- 震災後 6 日で高速道路が復旧した。

しかしながら全体としては、想定外の地震規模であったことと複合的な被害が発生したことにより十分な対応ができていない。今後の災害対策のあり方としては、耐震性や多重性、代替性の向上などをも考慮した、Resiliency を有するインフラとするべく、抜本的な見直しが必要であるとの感が否めない。

また、地震や津波による一次的な被害が想定を超えた大規模なものであったこともさることながら、被災の範囲があまりにも広かったこと、十分な通信が確保できず、情報が不足または錯綜し対応が後手後手に回ったこと、支援物資や人的リソースが有効に活用しきれなかったことなどにより、復旧・復興に時間がかかり、二次的な被害も深刻なものとなった。

以下に、今年度の検討対象となる医療、製品安全に関連する具体的な被災事例についてクローズアップする。

３－１．医療分野

表 ３－１－１に示したように、医療施設については岩手県、宮城県、福島県の三県にある病院の実に 8 割が全壊または一部損壊している。これは、地震と津波による直接的な被害である。この後、問題を抱えながらもかろうじて病院機能を維持できていた病院についても、二次被害に襲われることになった。まず、水道や電気などのライフラインが途絶えたことにより、診療も手術も、入院患者が使用している各種医療装置の維持もできなくなった。自家発電や備蓄物資で持ちこたえようとしたものの、ライフラインの停止が想定を超えた長期に及んだことから備蓄が底を突いてしまった。さらには、通信網、交通網が壊滅的状況にあったため、外部との連絡が取れず、補給物資の入手も患者の搬送も不可能な状況となった。その後、東京消防庁、自衛隊、DMAT（災害派遣医療チーム）などの到着・救援により徐々に解消されていったが、これら二次被害の想定が甘かったことが初動対応の遅れにつながったといえよう。

被災した病院の中には災害拠点病院も含まれていたが、災害時に拠点として活動できることを期待されていた災害拠点病院でさえ、耐震性、備蓄物資の確保、通信手段、搬送手段が確保できないケースがあった。それほどに想定を超えた被害が発生していたことは事実であるが、国や省庁で定めた災害拠点病院の基準が不十分なものであったこともまた事実である。

このようなインフラ的な被害のほかにも、医療の継続を困難にさせる被害が発生している。病院施設の破壊とともに、押し寄せる津波が院内の紙のカルテを押し流し、泥濘に埋もれさせ、紛失あるいは使用不可能な状態にした。受診前の健康状態や投薬状況が分からない状態では診断・処方が困難となる。当人の記憶を頼りにするしかなくなるが、患者が自身の処方を正確に記憶しているケースはまれである。また、被災当日の当直者以外は地震で被災したことにより、病院に

辿りつけなくなるなどし、病院は人員不足に見舞われた。自宅や家族の安否も分からない中、当直スタッフの心労・疲労は増す一方であったという。

なお、時間の経過と共に、被災地と被災者のニーズは変化していく。以下に、大規模災害が発生した場合における、生活面と医療面に関して時間経過とそれに伴う地元ニーズの変化についてまとめた。ここでは、時間経過の区分を「平常時」「被災時」「復興期」の 3 つに分け、さらに復興期を「初期」「中期」「後期」の 3 つに分けて整理した。

表３－１－１　時間経過とそれに伴う地元ニーズの変化（生活面）

	生活面での課題	ニーズ
平常時	予測不可能な災害への備え	大規模な災害にも対応できるようにしたい
被災時 （72h 以内）	近辺状況の正確な把握が困難 避難所に関する情報が得られない 　ーオーバフローした場合どこへ？ 　ー家族・知人の所在が不明 避難できない場合どうすればよい？	どこに行けば安全なのか早急に知りたい 家族・知人の安否を早急に確認したい 避難経路が確保できない場合どうすればよいのか知りたい
	物資の不足	必要物資を入手したい
復興初期 （数週間）	物資の不足、または過集中（被災地） ボランティアの不足、または過集中 被災地のニーズが正確に伝わらない	必要物資を入手したい ボランティアの手を借りたい 不要なものを送ってこないで欲しい
	自治体機能の回復が困難 　ー人的リソースの問題 　ーシステム・機器の問題	自治体の機能を早急に回復したい
復興中期 （1､2 ヶ月） ～ 復興後期 （数年）	生活物資の不足（限定的） 　ー物資供給にムラが発生 　ー避難所では現金を持ちにくく､買い物が不便 　ー交通手段が確保できない 　ー需要がなく支援物資が余る	必要物資を入手したい 安心して買い物をしたい 交通手段を確保したい
	仕事の再開が困難（金、場所、人員）	仕事を再開したい（雇用者、被雇用者とも）
	要介護者・アレルギー体質者の食事 　ー炊出しが受けられず、要自炊 　ー立地が不便な場合が多い	介護者やアレルギー体質者など､特別な事情を持つ場合でも食事の支援を受けたい
	ボランティアへの依存過多の是正	地元の雇用をボランティアや支援企業に奪われたくない
平常時	次なる災害への備え	被災により経験したことを災害対策に反映したい

表 ３－１－２　時間経過とそれに伴う地元ニーズの変化（医療面）

	医療面での課題	ニーズ
平常時	災害への備え	大規模な災害にも対応できるようにしたい
被災時 （72h 以内）	カルテの喪失 緊急医療のニーズ激増 医療機関自体の被災による診療不能 被災した医師が行方不明 後方病院への搬送手段・人員の不足・欠乏	プライバシーを保護したい 緊急時に患者のカルテを活用したい 場所を選ばず診療を行いたい 医師の所在や医療提供場所を伝達したい 周辺自治体からの支援リソースを適切に配分したい
復興初期 （数週間）	避難所・被災地域での感染症の発生・拡大 被災者の PTSD、精神的ストレス	感染症等の流行を防止したい 精神的ケアを行いたい
	生産・配送停止による医薬品・医療機器の欠乏	支援物資を適切に配給したい 生産・配送拠点を迅速に復旧したい
	地元の診療体制の復旧	医療支援チームに頼りきりになりたくない
復興中期 （1、2 ヶ月）	避難所でのエコノミー症候群の発生 仮設住宅入居者の不便 　－自発的な情報収集が必要に 　－生活支援が受けにくい	できるだけ体を動かすようにしたい 被災者向けの情報を入手しやすくしたい
	医療支援チーム・ボランティアスタッフの減少 　－地元の医療スタッフの負荷増 地元の診療体制の復旧・確立	医療支援チーム撤退後に向け、地元の医療体制を整えておきたい
復興後期 （数年）	リハビリ医療のニーズ増 在宅医療のニーズ増	避難所、仮設住宅、自宅療養を問わず、必要とする医療を受けたい
	医療支援チーム・ボランティアスタッフの撤退 　－手厚い支援が得られた時期とのギャップ	医療支援チームやボランティア存在時とのギャップを感じたくない
平常時	次なる災害への備え	被災により経験したことを災害対策に反映したい

物資の不足という一事を取ってみても、被災直後は交通網の寸断により配送が滞り、かなりの広範囲にわたって物資不足が発生する。その後交通網が徐々に復旧し、配送可能となったところから物資不足が解消されていくが、被災の中心部の物資不足は長く続くことになる。また、被災地に生産拠点や配送拠点が含まれる場合は、かなりの長期間にわたり、物資不足が継続することにもなる。

また医療支援という観点で見た場合にも、被災直後は広範囲で怪我人が多発し、救急医療のニーズが爆発的に高くなる。が、時間の経過にともない救急医療のニーズは減少し、かかりつけの病院や診療所を失った慢性患者などの診療ニーズが高くなる。また、大多数の年齢や健康状態も異なる人々が、電気、ガス、水道の使用に制限がある避難所に集まることにより、避難所内での感染症が発生することも危惧され、その予防へのニーズが高まる。さらに、避難生活が長期化することで、被災による PTSD 等に加え、思うに任せない生活を強いられることによる精神的スト

レスが募る、あるいは窮屈な姿勢をとり続けることによるエコノミー症候群の発生なども懸念されることから、これらのケアへのニーズも高まっていく。

このように、時間の経過と共に被災地でのニーズは次々と変化していく。硬直的な支援システムを構築しても、一過性の支援になってしまう。被災者のニーズの変化に柔軟に対応できるような支援システムを構築することが望ましい。

３－２．製品安全分野

製品安全分野における東日本大震災からの教訓としては、①廃棄物の処理・リサイクルの問題、②復旧時の製品安全確認の問題、③サプライチェーンの問題の 3 点に言及する。

（１）廃棄物の処理・リサイクルの問題

東日本大震災では、地震により引き起こされた津波により、家屋、船舶、自動車、家電製品など様々なものが大量に押し流され、海洋に流出したり、もとあった場所を遠く離れ、他人の敷地内に流れ着いたりしている。そのほとんどは使用不可能となってしまったが、漂着先の人々は漂着物が他者の所有物であることから、財産権の侵害やリサイクル法の違反などを恐れ、勝手に廃棄するわけにもいかず、困惑するというケースが頻発した。

家電については、国や自治体からはできるかぎりリサイクル法の遵守を求めつつも、災害廃棄物としての一括処理も含めた柔軟な対応も可とする姿勢が示されている。自動車については一定期間自治体が預かり、所有者を捜索し、所有者が見つからなければ自治体により処分手続きが行われることになる。

（２）復旧時の製品安全確認の問題

震災後、各種製品を再稼動するにあたり、大きく 2 つの問題がある。1 つは、停電後の通電時における製品からの出火の危険性問題であり、もう 1 つはエレベータや半導体製造装置などの復旧問題である。前者に関しては、公的機関や報道機関が注意喚起を呼びかけている。後者に関しては、その典型例としてエレベータの復旧がある。エレベータを再稼働させるためには昇降機検査資格者による安全点検が必要となるが、震災時は膨大な数のエレベータを点検する必要があり、実際には故障していなかったとしても復旧するまでに時間がかかっている。

この点について、製品安全情報のモニタリング技術を適用することで、再稼働までの時間を短縮する効果がある。

（３）サプライチェーンの問題

東北地方には自動車や半導体、その他様々な製品の部品を製造する工場や、薬品の精製工場が多数存在していた。それらの工場が被災し、操業不能になったことにより、被災地とは遠く離れた地域において、場合によっては国内にとどまらず海外においても、部品の不足による製造の遅れや、重要な医薬品の欠乏といった問題を生じることにつながった。

４．個人情報や企業情報を活用するためのクラウドコンピューティング基盤整備のあり方

3 章に示したように、昨年度末に東日本大震災が既存の社会システムに与えた影響は甚大なものであった。今年度、クラウドコンピューティング基盤整備のあり方について検討するにあたっては、震災により得られた様々な教訓をもとに、防災・減災に向けてどのような社会システムとすべきか、あるいは安全性を維持しつつ、生活の利便性を高めることができるかについて考慮することを避けて通ることはできないと考えられた。

このため、震災の影響を色濃く受けた医療分野と製品安全分野については、情報利活用についての深掘りや、利活用するためのシステムについての具体的な検討を進めると同時に、防災・減災に役立つクラウドコンピューティング基盤についても検討を行った。また、情報利活用の安全性を担保する仕組みについてセキュリティ面の検討も継続して行った。

以降、5 章～7 章に分けて、医療分野、セキュリティ分野、製品安全分野のそれぞれにおいて検討を行った、本プロジェクトが想定するクラウドコンピューティング基盤整備のあり方について詳述する。

５．医療分野についての検討

昨年度は、病院にある患者情報や医療関連機関にある医療関連情報や健康情報を集約する仕組みとして、個人情報を関連付けるキーの導入やシステムの形態について検討し、昨年度政府で導入が決まったマイナンバー利用や社会基盤としてのクラウドコンピューティング基盤の構築に関する提言を行った。その後、東日本を中心に未曾有の大震災に見舞われ、被災地では住民や社会基盤、医療機関等にも大きな被害が及び、それまでには明らかになっていなかった様々な課題が顕在化した。

今年度は、東日本大震災等の災害の復興時に種々の災害対応サービスを提供することにより、罹災した方々への支援を迅速に行うと共に、種々の産業の復興にも貢献できるような ICT 利活用の仕組みを作り上げること、ポスト震災時代に必要とされる、Resiliency を有する ICT 基盤を構築することを目標に加え、検討を進めた。東日本大震災で明らかになった医療分野における課題や、生活面での課題の克服に寄与する仕組みの必要性を痛感し、災害医療支援基盤に必要な要件の洗い出しを行った。

また昨年度、医療情報の二次利用に関する課題について検討し、匿名化技術の開発や ID による情報の連結についての提言を行った。今年度は、医療と密接な製薬産業における医療情報の利活用についての検討を行った。製薬産業において医療情報の活用は企業活動として必須の事柄であり、質の良い多くの情報を低コストで利用できるようにすることは重要な課題である。日本は薬を開発できる技術を有する世界でも数少ない技術力の高い国とされているが、日本の治験は品質が高いものの、コストが高い、時間が掛かるといった問題があり、薬の開発における国際競争力が低下している。今年度は、現在病院で使われているシステム全体と、治験業務に利用されている EDC（Electronic Data Capture）システム等の統合について検討した。

さらに、医療情報を他の産業に生かすための課題についても検討した。

最後に、以上を通して、医療情報を利活用するためのシステムを実現化するために解決しなければならない課題を整理し提言とした。

５－１．医療情報利活用例：災害時にも有効利用できる情報利活用基盤

医療分野の情報利活用において、東日本大震災で明らかになった医療分野における課題や、生活面での課題の克服に寄与することを目的に、昨年度検討した「医療連携サービス」「PHR 一次利用サービス」「PHR 二次利用サービス」の 3 つのユースケースをベースとして、平常時から大規模災害時においても有効に機能する医療向けクラウドコンピューティング基盤で必要となる機能とそれを実現するためのシステムについて検討を行った。

５－１－１．検討内容

東日本大震災において、地震、あるいは津波の影響により、被災地の医療機関は深刻かつ複合的なダメージを負った。その時の課題を次項でまとめた。

今回の震災により、医療現場においても様々な問題が惹起したが、今後も同規模の災害が発生する可能性は残されており、そのときにこのような被害を減少させる（減災）ために、今回顕在化された課題を分析し、Resiliency を有する仕組みを早急に実現する必要がある。

このような仕組みについて、昨年度検討した「医療連携サービス」「PHR 一次利用サービス」「PHR 二次利用サービス」をベースに、その必要性や有用性、求められるサービス、さらにそのサービスを実現するためのシステムについて検討を行った。以降、この仕組みを「災害医療支援基盤」と呼ぶ。

５－１－２．東日本大震災時に明らかになった医療分野に関連する課題

東日本大震災において、医療分野で明らかになった課題について大きく分類すると、以下の４つに集約できる。

１．診断・治療情報の露出、喪失

被災した医療機関で保管していた紙のカルテや医療情報の保持されたパソコンが津波により流出し散逸した。これにより、診断・治療情報が露出するというリスクが発生した。運よく回収されても水や泥を被り、紙のカルテは判読不能に、パソコンは故障し機能しないなどの事態も発生し、診断・治療情報が喪失された状況が生じた。患者の診療・治療情報を喪失したことにより、被災直後に診療活動を実施することが困難になるという問題が発生した。

２．継続的、偏在的な診断・治療情報の集積・管理利用

糖尿病や高血圧、不整脈など診療・治療の継続が必要な慢性疾患の患者については、服薬情報などが極めて重要である。１．で述べた震災による診断・治療情報が喪失だけでなく、震災により医療機関を移らなければならない場合にも問題が生じた。これまで診療・治療を受けてきた医療機関の被災により診断・治療ができなくなった、あるいは患者が自宅から離れた避難所や仮設住宅、親戚宅に転居したため、他の医療機関での診断・治療を受けなければならなくなることがしばしば発生した。

医療機関では初見の患者本人に聞き取りを行っても、こうした患者には高齢者が多いこともあり、患者自身が診療・治療に関する情報を知らない・覚えていないケースが多数見受けられた。その結果、継続的な診療や処方を行うことが非常に困難になった。医療機関が替わっても継続的に診断・治療を続けられるように、継続的で地域や医療機関に依存しない偏在的な患者の診断・治療情報の集積と管理が必要である。

３．医療機関に関する情報の伝達・展開が困難

災害発生時には平時に比べ、被災による傷病、災害後の生活の困難さによる病気の発生など、医療機関の必要性は常にも増して高くなる。今回の震災では医療機関や医療従事者も被災し、診断・治療などを行える医療機関が限定されるということが発生した。

また、再開した医療機関でも医療機器の故障、被災した専門の医療従事者が出勤できない、医薬品の供給が滞った、などにより、被災前に比べ、診断・治療が一部に限定されるという事態が発生することがあった。

今回の震災では被害が大きく広範囲に及び、自宅だけでなく地域の避難所に指定されていた公民館や学校までもが津波の被害にさらされ、安全な避難所が地域外に設置されることもあった。復旧に時間を要するため、避難所を移る、あるいは仮設住宅に移り住むなど、長年住み慣れた地域から離れ、馴染みの薄い土地を移り住むことになった被災者もいる。また転居の必要が無くても、身近な診療所や病院が被災し、罹患した傷病の診断・治療が可能な医療機関がどこにあるのか、いつどのような医療機能が復旧するのか、被災者は正確な情報を得ることが困難になった。医療機関とその機能についての情報の伝達・展開は、被災後の被災者の健康を守るために極めて大きな課題である。

4．医療ニーズが変化

被災直後から時を経るに従い、現場での医療ニーズが変化して行き、供給支援とのギャップを生じるようになった。具体的には、被災直後は外科処置などの緊急医療のニーズが高かったが、その後避難所などにおいて、慢性疾患を持つ患者に対する定期処方のニーズが高くなった。また、避難所には年齢も健康状態もまちまちの多数の被災者が集まっており、時間の経過と共に感染症対策のニーズが高くなった。さらに時が経過すると、様々な被災のストレスに起因する心不全やPTSD、鬱病などのケアのニーズが高まった。ある程度落ち着きを取り戻し、避難所から自宅へ戻る人が増えると、帰宅者に含まれる高齢患者などからの在宅医療へのニーズが高まった。

５－１－３．課題解決のための要件

５－１－２．に示した課題を解決するために、災害医療支援基盤は、以下の要件を満たす必要がある。

1．三次医療圏を跨った広域での情報連携を可能とする仕組み

患者の医療情報・健康情報を電子化し、遠隔地においてバックアップすることにより、大災害時においても遠隔地にあるデータにアクセスすることで現地での診療を継続可能にする。またこれにより、今回の震災で発生した紙のカルテの流出のような患者のプライバシーの流出の防止に貢献する。

2．減災を考慮した支援計画の策定（BCP）と演習の実施

様々な災害を考慮し、災害時の医療支援をスムーズに行うために支援計画を事前に策定する。また策定した支援計画について、関係地域で演習し災害に備える。さらに、支援計画を実施するために必要となる各種システムを構築する。

３．医療機関までたどり着けない被災者への支援

携帯端末を使った医療相談システムを構築することにより、被災により交通手段を失った、あるいは怪我、障害、重い病などの理由により医療機関まで自力でたどり着くことができない被災者を支援することを可能とする。また同システムにより、復興時や被災状況が長引く時の精神的なケア等も可能とする。

４．復興時に必要となる医療・介護支援、生活支援等の支援

慢性病を有する患者や介護が必要な患者を対象とした帰宅支援、さらには帰宅後の訪問診療や遠隔サポート等を可能とする。また、仮設住宅に入居した高齢者等への生活支援のための情報発信とニーズの吸い上げを可能とする。

５．被災時における診療目的の医療情報参照を妨げないような本人確認の仕組み

被災時には、従来本人確認のために必要としていた品物を常に携行できるとは限らないため、被災時における情報アクセスを目的とした本人確認手段の多様化（携帯電話、生体情報、IC カード、番号制度等）を実現する。

６．監査機関による適正利用の監査機能

医療情報は利用状況に応じた適切な取り扱いが行われる必要があるため、平常時と被災時において、その場に応じた適切な医療情報の取り扱いがなされているかを監査可能とする。

これらの要件を満たす、大規模災害時の減災に寄与する災害医療支援基盤についての具体的な検討内容について、次項以降に述べる。

５－１－４．災害医療支援基盤に求められるサービス

災害医療支援基盤に求められるサービスのイメージを図　５－１－１に示す。

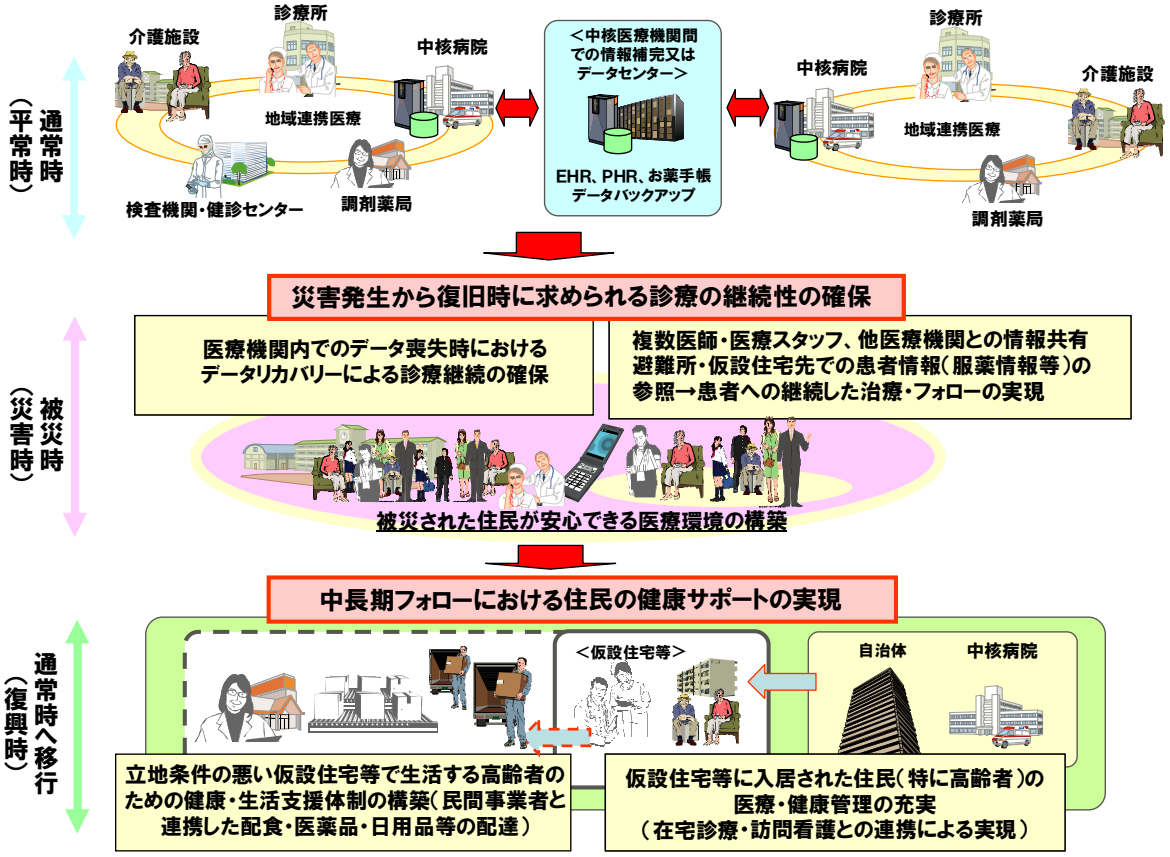


図　５－１－１　災害医療支援基盤に求められるサービス

通常時から被災時を経て、再び通常時へと移行するまでの一連の流れにおいて、クラウド基盤上の情報を共有することにより、診療・治療を途切れることなく継続して提供可能とするとともに、中長期における地域住民の健康サポートをも可能とする仕組みの構築が必要である。

５－１－５．災害医療支援基盤を実現するシステム

災害医療支援基盤を実現するシステム構成について表　５－１－１に示す。

表　５－１－１　災害医療支援基盤のシステム一覧

項目	システム	機能	説明
（１）	災害医療支援準備システム（BCP）	支援情報管理機能	災害時において、適切かつ効率の良い医療支援ができるように、通常時に必要な情報を収集し、想定される様々な災害に対応する施策を事前に計画するシステム
		災害時医療対策計画機能	
		医療情報匿名化機能	

（２）	現地医療支援システム	医療情報バックアップ機能 診療業務継続機能	災害時に医療機関（避難所、仮設医療機関を含む）において、医療支援チームが患者の医療情報を収集し、診療を継続するためのシステム
（３）	災害時医療相談システム	医療者登録機能 患者個別相談機能 相談・診察記録管理機能 相談内容サマリ公開機能	遠隔地の医師が、現地で治療を受けられない被災者もしくは軽症者からの医療相談を受けるシステム
（４）	在宅医療・生活支援システム	患者管理機能 遠隔状態監視機能 生活情報提供・収集機能	自宅に戻った、あるいは仮設住宅等に入居した住民（特に高齢者）の在宅医療・健康管理の充実と日常生活を支援するシステム
（５）	被災時本人確認システム	本人確認機能	被災時における（診療目的の医療情報参照を妨げない）多様な本人確認を行うシステム
（６）	監査用ログシステム	監査ログ収集管理機能 監査ログ分析機能	医療情報だけでなく生活支援に関する個人情報のプライバシーを保護するシステム

災害医療支援基盤のシステム構成を図　５－１－２に示す。

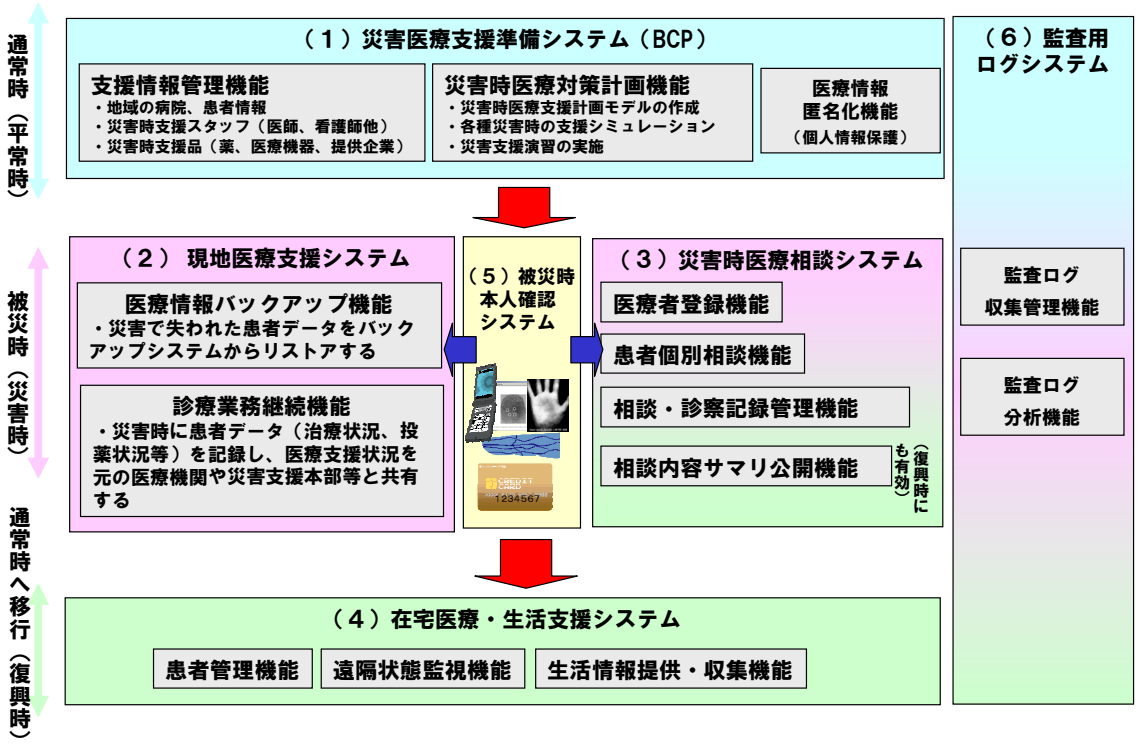


図　５－１－２　災害医療支援基盤のシステム構成図

５－１－６．災害医療支援基盤を構成する各システムの検討内容

以下に災害医療支援基盤を構成する各システムの検討内容を述べる。

（１）災害医療支援準備システム（BCP）

（ア）システム概要

災害時において、適切かつ効率の良い医療支援ができるように、通常時に必要な情報を収集し、想定される様々な災害に対応する施策を事前に計画するシステム（BCP）である。

システムの構成要素として、支援計画を立てる際に使用する各種情報を収集し管理するデータベースと分析・計画立案するための理論（モデル）が必要となる。

災害医療支援準備システム（BCP）のイメージを図 ５－１－３に示す。

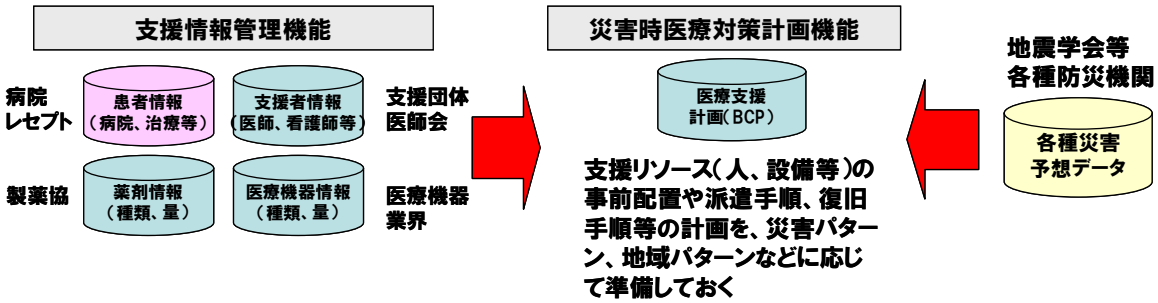


図 ５－１－３　災害医療支援準備システム（BCP）のイメージ

（イ）機能

災害医療支援準備システム（BCP）は、表 ５－１－２に示す機能を有する。

表 ５－１－２　災害医療支援準備システム（BCP）の機能

No	機能	概要
1	支援情報管理機能	各情報を各機関が入力するポータルとそれぞれのデータを管理する
2	災害時医療対策計画機能	支援情報管理システムおよび防災機関からの災害予想データより、医療支援モデル計画を作成管理する
3	医療情報匿名化機能	平常時と震災時の傾向分析を行うために医療情報の匿名化をする

（ウ）効果

地域の医療体制の実情の把握や、予想される災害の特質に合わせた医療災害を想定し、全国からの医療支援が有効に働く支援計画を事前に策定することで、実災害に向けての準備が可能となる。

（２）現地医療支援システム

（ア）システム概要

現地医療支援システムは、災害時に医療機関（避難所、仮設医療機関を含む）で、医療支援チームが患者の医療情報を収集し、診療業務を継続するためのシステムである。情報提供と情報収集の 2 つの役割を持つ。

情報提供については、医療機関施設内の医療情報（電子カルテ、処方情報等）を平常時に外部のデータセンターにコピーし、災害時であっても Web 環境で診療情報を参照可能とする。

情報収集については、患者の診療継続ができるようシステム被災時に他の医療機関（避難所、仮設医療機関を含む）が診療結果を書き込み、システム復旧後、元の医療機関が参照する。現地医療支援システムのイメージを図 ５－１－４に示す。

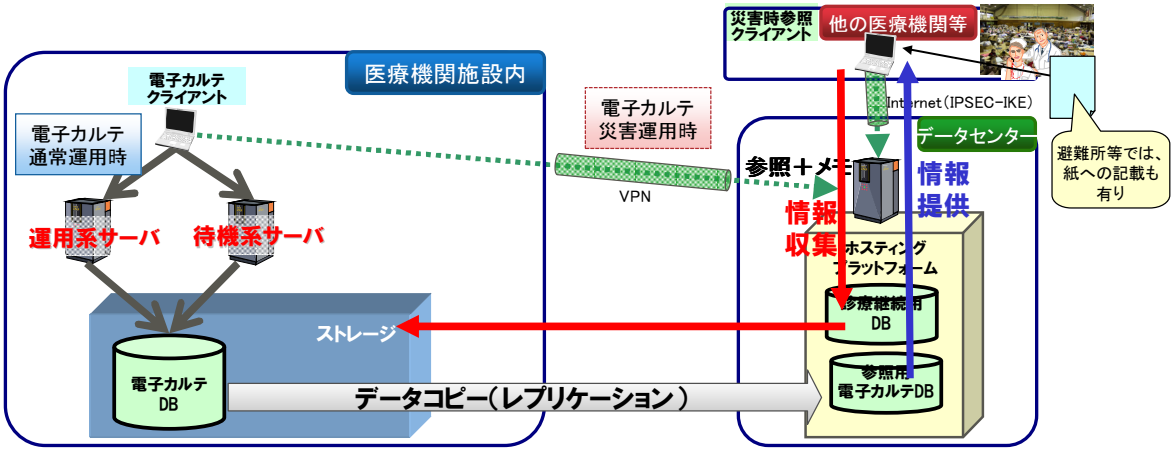


図 ５－１－４　現地医療支援システムのイメージ

（イ）機能

現地医療支援システムは、表 ５－１－３に示す機能を有する。

表 ５－１－３　現地医療支援システムの機能

No	機能	概要
1	診療情報バックアップ機能	医療機関にある電子カルテの医療情報を、データセンター等の参照用電子カルテ DB へ定期的にバックアップする

2	診療業務継続機能	他の医療機関（避難所、仮設医療機関を含む）が、患者の診療を継続するための情報の収集・提供をする

（ウ）効果

現地医療支援システムを構築することにより、診療データ参照のタイムラグをほとんどなくすことが可能となる。また、電子カルテシステム上にあるほとんどの情報が参照可能となるため、速やかに診療再開が可能となる。さらに、他の医療機関（避難所、仮設医療機関を含む）が、継続的に診療結果を書き込むことにより、システム復旧後に元の医療機関が継続して診療を行える。

（３）災害時医療相談システム

（ア）システム概要

病院が被災し支援チームが到着してない地域、病院まで行けない人、軽症で治療の順番がなかなか来ない場合等のために、インターネットを通して全国の医師への相談を可能とする。支援初期の混乱時期のみならず、復興時においても、医療施設および医師の治療が万全になるまでの間、有効な支援システムである。

また、被災時に支援活動を行った全国各地のボランティア医師によるインターネットを介した医療相談システムの課題（被災者がシステムの存在を知らない、回答者の身元が不明である、相談者の正確な医療情報が不明）を解決し、より有効な支援を可能とする。

なお、このシステムはクラウド上に構築し、PC、携帯等からサービスを利用できるようにする。

（イ）機能

災害時医療相談システムは、表 ５－１－４に示す機能を有する。

表 ５－１－４　災害時医療相談システムの機能

No	機能	概要
1	医療者登録機能	災害時に医療相談支援を行う意志のある医者の事前登録により、医師であることを確認する 医療相談を行うことが可能な日時、手段の登録をする
2	患者個別相談機能	患者に電話、メール、Web でのアクセス手段を提供する 次の機能との連携で、患者本人の相談、診察内容を参照できるようにする 患者の相談に対する、回答、診察結果を伝える（表示する）

3	相談・診察記録管理機能	相談・診察記録を保管し、他の医師・患者本人が参照できるようにする 他の医師に患者を引き継ぐための記録を管理する
4	相談内容サマリ公開機能	医師が受けた相談のうち一般的な内容として確認されたものを匿名化して公開する

（ウ）効果

以下のような効果を想定している。

- 医療を待つ被災者への安心感を与える。
- 現地で緊急災害医療に当たっている医師の負担を減らし、緊急・重傷者への治療に重点をおける。
- 現地入りしていない全国の医師の支援を活用できる。
- 患者からの情報を得ることで被災地の状況を把握できる。
- 相談を受けた医師から現地で治療する医師へ相談情報を渡すことで、治療の継続性が高まる。
- 復興時期の自宅療養者への支援が可能となる。
- 事前に連絡先（アドレス、URL や電話番号など）を周知させることができる。これは、存在の周知、臨時設営のため連絡先が定まらないことに対する解決策となる。
- 相談者が本当に医療資格者かどうかを事前にチェック可能となる。
- 一定のルールに従った支援が可能（例えば、相談ログの管理、治療者への引き継ぎなど）となる。
- システムのセキュリティ等、一定の機能を有した支援システムが準備できる。

（４）在宅医療・生活支援システム

（ア）システム概要

仮設住宅等に入居した高齢者等の医療・健康管理の充実と生活を支援するシステムである。在宅医療・生活支援システムのイメージを図 ５－１－５に示す。

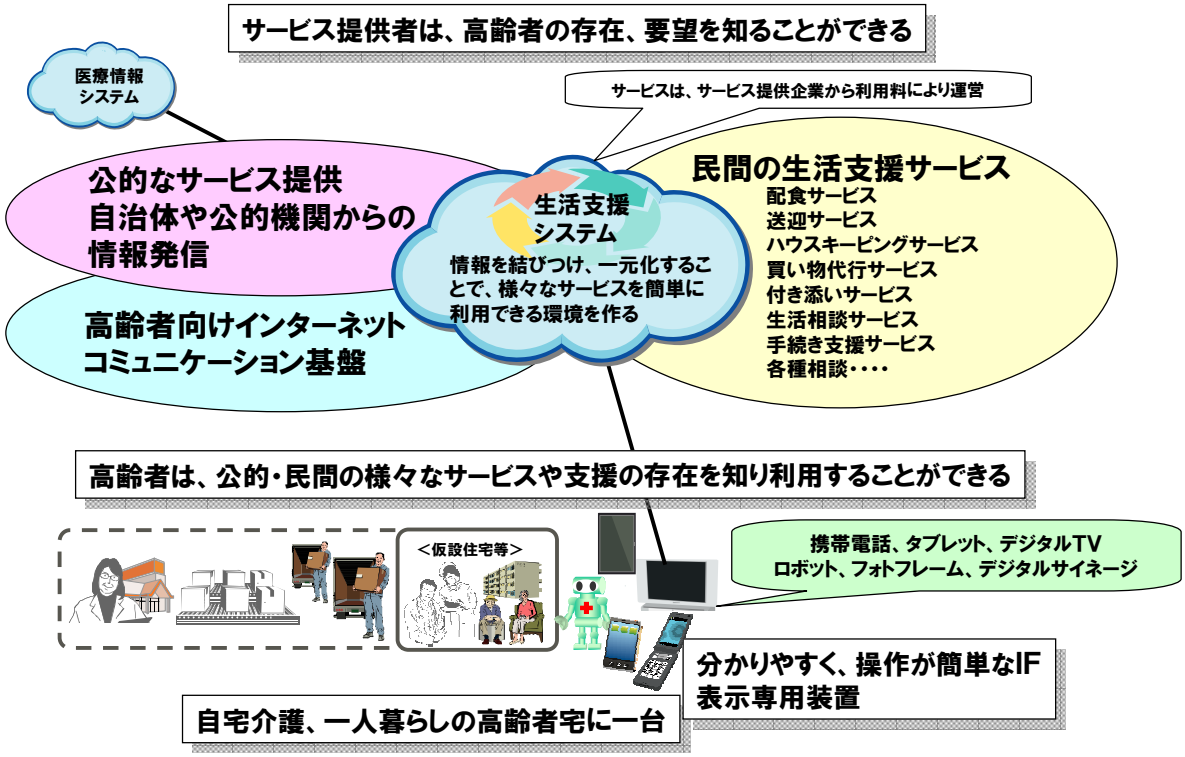


図　５－１－５　在宅医療・生活支援システムのイメージ

（イ）機能

在宅医療・生活支援システムは、表　５－１－５に示す機能を有する。

表　５－１－５　在宅医療・生活支援システムの機能

No	機能	概要
1	患者管理機能	在宅診療による医療情報と訪問看護による介護情報を連携させる
2	遠隔状態監視機能	自宅介護、一人暮らしの高齢者宅のモニタリングを行う
3	生活情報提供・収集機能	生活支援情報を結び付け一元化することで、様々なサービスを簡単に利用できる環境を作る 分かりやすく操作が簡単な利用者インターフェースを提供する

（ウ）効果

生活支援サービスを一元化することにより、サービスを受けやすい環境を提供可能とする。例えば、利用者の情報をサービス提供者と共有することで、利用者に適したサービスを提供する、あるいは医療情報や介護情報と連携し、利用者の健康状態に即した減塩、低カロリー、

アレルギー食物除去等を考慮した食事サービスの提供などを可能とする。また、利用者が受けることができるサービスを知らせる『提供（プッシュ）型サービス』を実現できる。

次に、自治体や公的機関からの情報を入手しやすい環境を提供可能とする。例えば、自治体や公共機関から発信される生活に必要な情報を伝える手段（メディア）を整備する、あるいは仮設住宅の集会所にデジタルサイネージモニターで生活情報を表示する、あるいは個人宅にフォトフレームやタブレット端末を使って伝達する手段を設けるなど、プッシュ型での情報提供を行う。

さらに、高齢者を孤立させないコミュニケーション環境を提供可能とする。例えば、インターネットのコミュニケーション手段である Twitter、Facebook 等を、高齢者の孤立を防ぐ手段として利用できる環境を整備することで、不特定ではあるが、多くの人の係わり合いを通じて、社会が自分をフォローしてくれていると感じてもらうことができる。

（５）被災時本人確認システム

（ア）システム概要

被災時に診療目的の医療情報参照を妨げないように本人確認手段の多様化を実現するためのシステムである。本人の希望する本人確認のための登録情報を、平常時にあらかじめ患者本人が登録しておく（オプトイン方式）。共通診察券番号（患者が複数の医療機関で受診する場合に、それら医療機関の間で診療情報を共通的に利用・管理するために用いる、患者本人を識別するための番号）を元に、本人登録情報と医療情報等を紐付け、登録済みの情報を利用可能とする。被災時本人確認システムのイメージ（被災時）と被災時本人確認システムのイメージ（オプトイン方式）を図 ５－１－６および図 ５－１－７に示す。

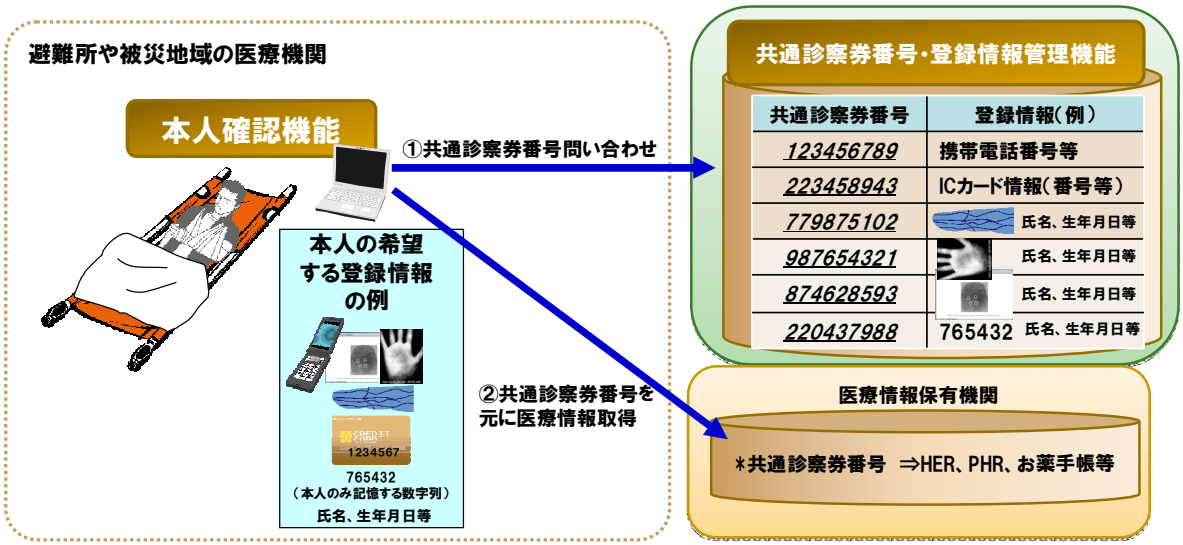


図 ５－１－６ 被災時本人確認システムのイメージ（被災時）

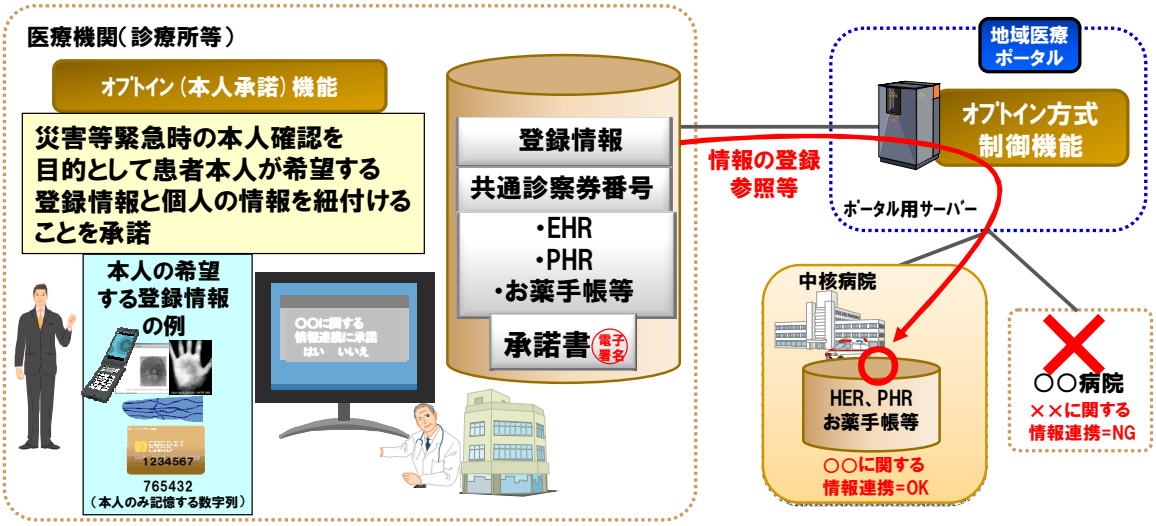


図　５－１－７　被災時本人確認システムのイメージ（オプトイン方式）

（イ）機能

被災時本人確認システムは、表　５－１－６および表　５－１－７に示す機能を有する。

表　５－１－６　被災時本人確認システム（被災時）の機能

No	機能	概要
1	本人確認機能	登録情報を使って本人を確認し、共通診察券番号を取得する
2	共通診察券番号・登録情報管理機能	共通診察券番号と登録情報を管理する

表　５－１－７　被災時本人確認システム（オプトイン方式）の機能

No	機能	概要
1	オプトイン（本人承諾）機能	本人の登録情報と共通診察券番号、本人の EHR、PHR、お薬手帳の連携、また他の医療機関と連携するかを本人に承諾させる
2	オプトイン方式制御機能	本人のポリシー（承諾内容）に応じて情報連携を制御する

（ウ）効果

救急搬送時や被災時における診療目的の医療情報参照を妨げないような本人確認手段の多様化を実現できる。

（６）監査用ログシステム

（ア）システム概要

医療情報だけでなく、生活支援に係る個人情報のプライバシーを保護するためのシステムである。監査用ログシステムのイメージを図 ５－１－８に示す。

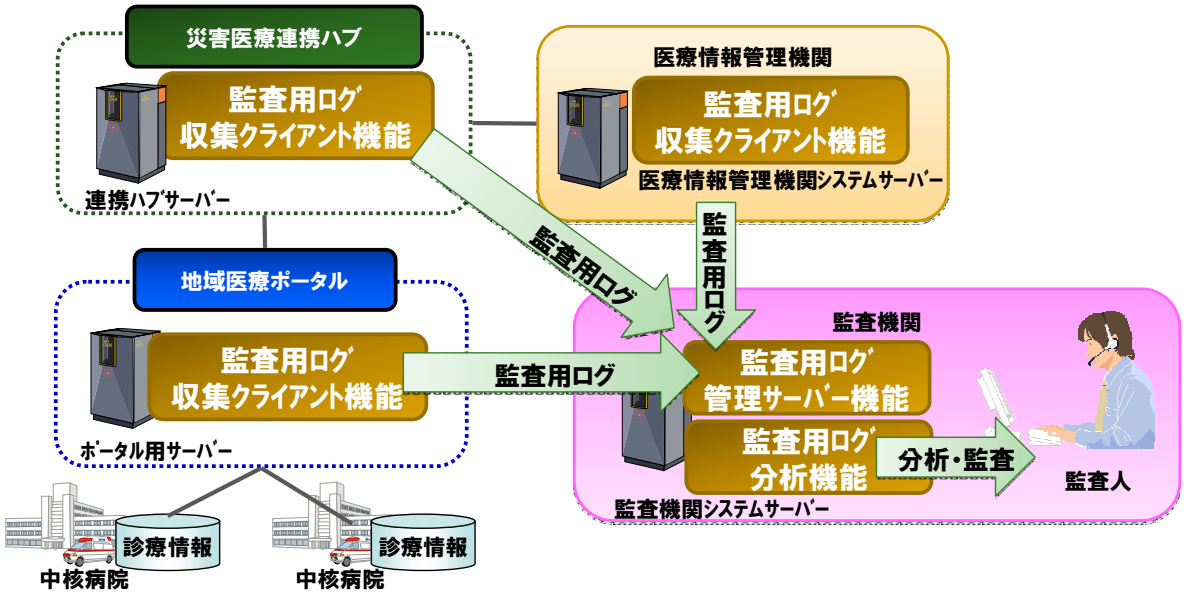


図 ５－１－８　監査用ログシステムのイメージ

（イ）機能

監査用ログシステムは、表 ５－１－８に示す機能を有する。

表 ５－１－８　監査用ログシステムの機能

No	機能	概要
1	監査用ログ収集クライアント機能	ポータル用サーバー等に設置し、監査に必要なログを収集する
2	監査用ログ管理サーバー機能	上記クライアントから送られてくる監査用ログを一元管理する
3	監査用ログ分析機能	収集された監査用ログを分析し、監査作業を支援する

（ウ）効果

医療情報だけでなく、生活支援に係る個人情報のプライバシーを保護できるようになる。

５－２．医療情報利活用例：治験と医療の情報統合と利活用

昨年度、医療情報の二次利用に関する課題について検討し、匿名化技術の開発や ID による情報の連結についての提言を行った。今年度は、医療と非常に密接な製薬産業における医療情報の利活用について、本プロジェクトに参加していない製薬会社の方々にも議論に参加していただき検討を行った。製薬産業において医療情報の活用は企業活動として必須の事柄であり、質の良い多くの情報を低コストで利用できるようにすることが重要課題の１つである。

図　５－２－１は、製薬業界における医療情報の利用目的を示した図である。

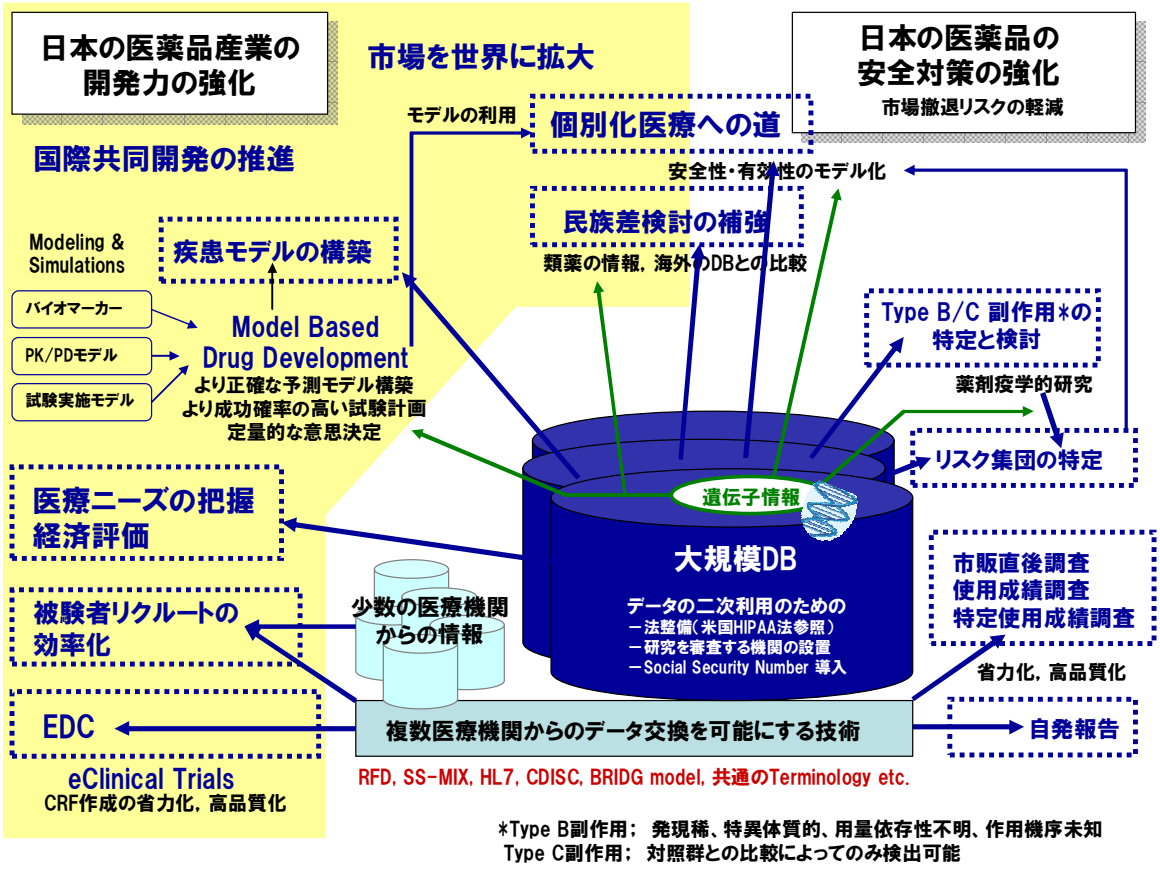


図　５－２－１　製薬業界における医療情報の利用目的

図　５－２－１では、遺伝子情報等を含む大規模情報を、病院や医療研究機関等の多くの医療情報が集められた情報を蓄積したイメージとしているが、実態としては集中して大きな DB として管理する情報もあれば、各機関において保持し適切な情報交換の仕組みにより相互に利用できる情報もあり、すなわちクラウド上の仮想的な大規模 DB のイメージである。このようなシステムを一気呵成に構築するのは難しいことであるが、技術やシステムの開発、医療情報を取り扱う法整備を進め、将来において実現すべき社会基盤であると考えている。ここでは、このシステムが存在するとした場合に、どのような目的でその情報を利用するのかについて整理している。大きく、医薬品の安全対策の分野と医薬品開発の分野において利用されることが示されている。

ここでは、医薬品開発分野の中の点線で囲まれた「被験者のリクルートの効率化」、「EDC（Electronic Data Capture）」に関連する治験について検討を進めた。日本は薬を開発できる技術を有する世界でも数少ない技術力の高い国とされているが、日本の治験については、品質は高いものの、コスト、期間がかかるといったことにより、医薬品の開発において国際競争力が落ちてきているとされている。このような課題を解決する提案の 1 つとして、治療や診断に使われている医療システムや、患者や医薬品等の管理などに利用されている病院システムといった、現在病院で使われているシステム全体と、治験業務に利用されている EDC システム等を統合化することで、解決できないかについて検討した。

５－２－１．日本の治験の状況

病気治療に新薬や新しく開発された医療機器を利用するためには、その効果、安全性を確認、保証するため、治験制度が定められている。しかし、日本の治験実施環境は他国に比べて様々な課題があり、日本における医薬品や医療機器の開発において国際競争力の低下を招いたり、他国で使われている医薬品や医療機器の導入が遅れたりすることで、日本国内の患者に対して効果的で適切な医療を提供できていないのではないかと懸念されている。このような状況を改善するため、国や医薬関係者により治験の活性化に向けての施策が行われている。具体的には、平成 15 年に「全国治験活性化 3 カ年計画」が策定されたのを始めとして、平成 19 年に「新たな治験活性化 5 カ年計画」が策定され、継続的な施策が実施されてきた。「新たな治験活性化 5 カ年計画」では、治験等の中心的役割を担う中核病院・拠点医療機関の体制整備が進められ、その大規模治験ネットワークを通じて治験参加への意思、具体的な候補者数に応じるシステムが構築されている[3]。さらに、現在残った以下の課題については、完全解決に向けた取り組みを継続していくこととしている[4]。

① 症例集積性の向上
② 治験手続きの効率化
③ 医師等の人材育成
④ 国民・患者への普及・啓発
⑤ コストの適正化
⑥ ICT 技術の更なる活用　等

５－２－２．治験における情報基盤の構築と活用

治験を効率的に進める方策の 1 つとして、治験を取り巻く環境の ICT 化を実現することが挙げられる。単に治験に利用される EDC（Electronic Data Capture）のシステムを活用するというのではなく、電子カルテや患者管理システム、治験薬のオーダシステムなど、病院や薬局に関連するシステムとの統合化、少なくとも情報の連携活用を実現したシステムが必要である。

厚生労働省の治験等適正化作業班がまとめた「治験等の効率化に関する報告書」[5]では、治験の国際化、および大規模化が進む昨今、アジア諸国での治験実施医療機関は 2,000 床以上の規模

を有する、いわゆる「メガホスピタル」が多く、1 つの医療機関で高い症例集積性を上げているのに対して、我が国の治験実施医療機関は 400～500 床規模であることが多く、1 つの医療機関でアジア諸国と同等の症例集積を行うことは困難である、としている。また、治験集積性を向上させるために、国内において複数の医療機関が連携し、「あたかも 1 つの医療機関のように機能すること」によってメガホスピタルと同等の治験集積性が可能となる「治験ネットワークモデル案」が提唱されている。

症例をより迅速に集めるためには、それぞれの医療機関側が治験参加候補者をより迅速に見出すことも重要である。「小児治験ネットワーク」では各施設の電子カルテにアクセス可能な閲覧システムを導入している[6]。このように、現状では各施設の電子カルテに治験ネットワークがアクセスして治験参加候補者を検索している状況であるが、クラウド ICT 基盤を活用することにより、あたかも“1 つのネットワーク”が“1 つの医療機関”であるかのように機能して、治験の活性化に寄与するものと考える。

また、モニタリングの効率化の観点から、EDC の積極的な活用が挙げられ、医療機関が電子カルテを導入していれば、単一医療機関での電子カルテから EDC へ自動的にデータを取り込むことも可能になってきている。EDC の運用を考慮すると、患者をその 1 つの医療機関に集めることは効率的と考えられるが、移動時間やコストの面で患者にとって負担が大きく、できるだけ患者の居住地に近い病院で治験に参加できることが望ましい。

この点について、多くの医療機関に EDC と連携可能なインターフェースを有する電子カルテが導入され、様々な仕様の電子カルテと EDC の相互連携ができ、クラウド基盤技術を活用した EDC を利用することにより、端末の整備に対応する程度で中核病院・拠点医療機関を軸とした治験ネットワークに参加でき、中小病院における患者の治験参加が期待できる。このことは症例集積性向上にも寄与するものと考えられる（図 ５－２－２）。

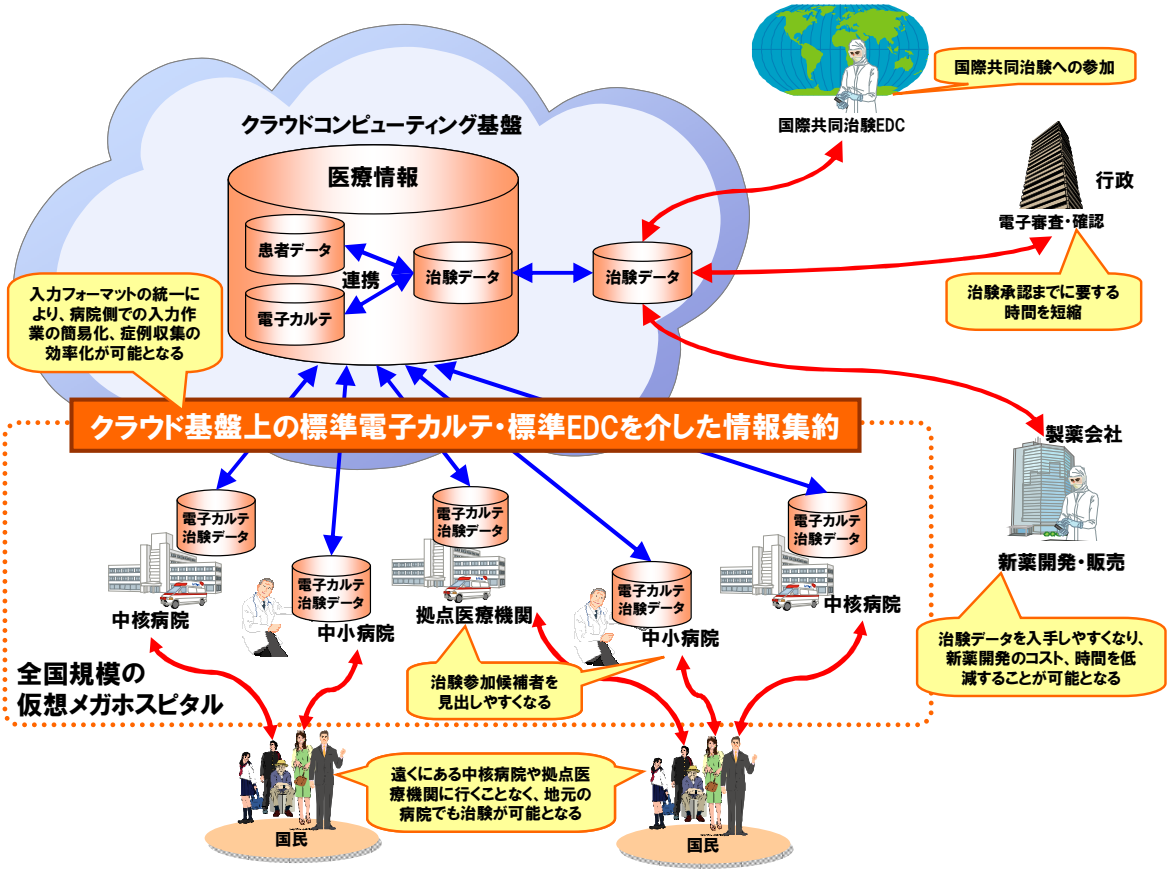


図　５－２－２　治験の側面から見た医療クラウド

５－２－３．システムの要件

５－２－２．で検討したようなシステムについては、以下のような機能や要件が必要であると考えられる。

（１）治験参加候補となる患者情報の集約

治験依頼者が治験を実施しようと考えた時に、その治験の対象となる患者が、どこの病院にどのくらいいるのかを詳細に把握する必要がある。例えば、以下のような情報を効率よく得られるとすれば、治験を効率的に進めることが可能になると考えられる。

- 全国規模の患者情報。
- 各患者の性別、年齢、居住地域等の患者情報。
- 各患者の罹患している病気情報や診療、治療状況。
- 治療を受けている病院、医師の情報。

（２）治験データの集約

治験では、患者への有効性や安全性を確認するために、治療状況や状態を医師の診断や各種の検査数値を蓄積し、分析していく作業が主な活動になる。そのため、通常の病院における治療、診察、検査といった病院システムに蓄積される情報と、治験特有の検査、診断によって得

られた情報とを集約管理できるシステムが必要となる。現状では、治療は治療、治験は治験と、医師の作業や病院のシステムがそれぞれ異なるため、データ管理や入力の負担を病院の医師やスタッフ等が負うことで進められている。

（３）利用者（医療機関）の利用環境の標準化

近年、病院の ICT 化の進展にともない、電子カルテの普及が進んでいるが、メーカーにより仕様が異なることや、治療や検査の仕方が病院ごとに異なり、それに合わせてシステムを個別にカスタマイズしていることにより、医療システムの統合化が難しく、地域医療として医療機関同士が連携して医療を進める際の課題の 1 つになっている。当然ここで検討しているシステムも現状のシステムを統合した形態を想定しているため、メーカーや利用機関に関係なく、同じ目的を持ち、同じ業務を行うためのシステムであれば同じ使い方、同じ解釈ができるシステムであることが望ましい。そのためのシステムの標準化が必要であると考えられる。

また、国際治験の実施についても同じ手順、操作で可能とするために、国際標準に準拠する必要がある。例えば、2012 年に ISO 標準化を目指している BRIGE プロジェクトの成果を取り込むべきである。

（４）システムの連携の要件

統合化したシステムで治験を実施する際には、電子カルテと同期することで電子カルテから得られる情報は自動的に集約され、治験独自の項目のみ入力すれば良い方式とすべきである。それに加え、検査機器とも連携した上で、医療用のデータであるか、治験用のデータであるかはシステムにより的確に判断されるようにし、医療関係者の負担を極力無くすものであるべきである。このようなシステム連携を構築する上で、以下の課題解決が必要である。

- 治験ネットワークに参加するすべての医療機関の電子カルテの共通のクラウド化が必要。
- 治験ごとに EDC にデータを流し込むシステム連携の構築が必要。

（５）被験者管理

治験に参加している患者は、病院の治療とは別に治験のための診察や検査を受けてもらう必要がある。通常の病院の患者予約システムと連動した、治験のための通院管理機能が必要である。具体的な例としては、間違いなく通院してもらうために、通院のリマインダーメールを送付するなどの機能が考えられる。

５－２－４．システムが可能にするメリット

５－２－３．に示すようなシステムが構築され利用されることにより、治験に関わるそれぞれの分野において、以下のようなメリットが創出される。このことがひいては、日本の医薬品や医療機器開発における国際競争力を高め、日本の患者により良い医療を提供することに繋がっていくものと考えている。このような情報基盤の早期の構築を望むものである。

（１）データ入力時間、コストの削減

日本では、1 施設あたりの症例数が少なく、目標症例数を獲得するために多くの病院を対象にする場合がある。多くの施設で、EDC システムを導入し、各施設でデータ入力のための人員を確保することは、コスト増につながる。このため、EDC システムの導入、EDC のデータ入力コスト（入力の手間）をできるだけ抑え、医療機関側の負担を下げることが必要である。

（２）治験依頼者側のメリット

- 日本全国の病院から標準化された治験データを入手できる。
- 治験の標準化と効率化で治験コストを低減し、医薬品の国際競争力の強化につながる。
- EDC システムの医療現場での利用には、メーカー毎のインストラクションが必要なほど手間が掛かるという課題を解決できる。
- 電子カルテとの連携を高めることで、電子カルテと EDC とに同じデータを繰り返し入力する手間や、入力ミスの問題を解消できる。
- 国際共同治験にスムーズに参加できるようになる。
- クラウド基盤の活用により、EDC 導入における初期投資を少なくできる。

（３）病院のメリット

- 電子カルテと EDC の連動により、必要最小限のコストで治験が実施できる。
- クラウド基盤の活用により、多くの医療機関で効率的に EDC による治験を実施でき、中小病院の電子カルテ導入の契機にもなる。
- 中小病院、診療所において、診療報酬以外に治験報酬を得ることで病院経営の安定につながる。手間（コスト）が掛からない治験業務が可能な電子カルテ＋EDC のクラウドサービスで実現する。
- （治験報酬）＞（電子カルテ）＋（EDC 運用コスト）であれば、電子カルテの普及促進につながる。

（４）ICT 企業のメリット

- 中小病院のメリットが小さくなかなか普及しない状況にある電子カルテについて、普及の一因になると期待される。
- EDC の国際治験対応システムを国内病院だけでなく海外病院へ展開できる。

（５）日本社会のメリット

- 日本人による治験がより早く進むことで日本での医薬品の開発が促進され、ドラッグ・ラグの解消にもつながる。電子カルテの普及で医療コストの削減が見込まれる。
- 治験ネットワークに参加している身近な病院で治験に参加することができる。
- 電子化された医療情報の利活用が見込まれる。
- 日本人向けの新薬の恩恵、医療情報電子化による恩恵を受けられる。

５－３．医療情報利活用例：医療情報の他産業分野での利活用

医療関連機関内の情報利用だけでなく、医療や健康情報を他の産業分野においても活用できるような仕組みについても検討が必要である。これから日本が迎える高齢化社会の中で、国民が健康で元気に生活していくためには、医療、製薬等の医療分野のみならず、医療に近い健康に関わる産業分野や、食品や住宅などの生活全般に関わる産業分野においても、健康を意識した製品、サービスを開発し提供していくことが重要になってくる。そのとき、健康や医療に関する情報をもとにして、質の高い、利用者の状況に即した製品やサービスを提供するためには、健康や医療関連情報を一般の産業へ提供し利活用を可能とする仕組みが必要になってくると考えられる（図５－３－１）。

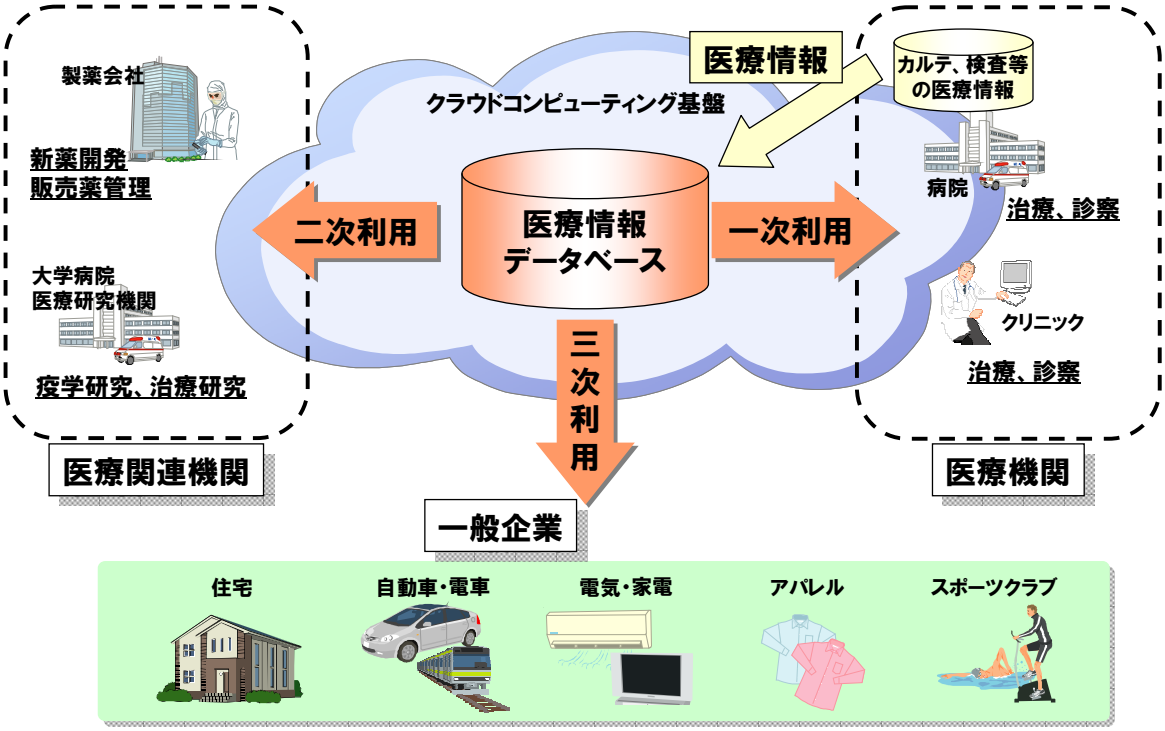


図　５－３－１　医療情報の他産業での利活用

５－３－１．三次利用の目的とメリット

一般的に、医療情報の利用の目的において、患者本人の治療や診療に用いることを「一次利用」、患者本人とは直接関係しない疫学や研究を目的として用いることを「二次利用」と呼んでいる。ここでは、医療情報を医療分野外の産業分野のために用いることを「三次利用」と呼ぶこととし、医療分野以外の一般産業における医療・健康情報利用であることを明確にして検討する。

なお近年、健康食品やフィットネス、スポーツクラブ等健康関連産業への医療情報利用について議論されるようになってきているが、ここでは住宅、交通、アパレル等、医療とは距離のある産業分野について、医療情報の活用におけるメリットや課題を検討する。

（１）一般企業が医療情報を利用する目的

高齢化社会を向える日本にとって、健康・医療に関しては社会全体の大きな関心事である。医療および介護・看護の質や量、およびコストの問題は様々な方策をとって解決していかなければならない状況である。そのような状況の中では、日常の生活を健康で過ごすことが重要なことであり、健康で過ごすための手段を求めるのは世の中の当然の動向である。このような環境において、日常生活の製品やサービスに健康志向が求められる、もしくは健康を促進するための日常的な製品、サービスを提供することが必要になってくる。多少イメージ先行的なところもあるが、例えば居住しているだけで健康になる“健康住宅”、着用しているだけで病気が軽減される“健康衣服”、毎日の通勤で健康が増進される“健康通勤電車”など、日本に住むことで健康になるという健康立国を目指すためにも、健康を軸とした製品・サービスを提供する必要がある。

健康を軸とした製品・サービスの開発には、その製品やサービスがどのように健康に寄与するのか、疾病にどのくらい効果があるのかについての研究を進める必要がある。その研究を支えるもとになるのは、病院や医療関係機関の保有する医療関連情報である。これらの情報を有効活用して研究を進めることなくしては、健康を増進させる、あるいは維持する製品やサービスの開発は進まないと考えられる。

（２）健康を促進させる製品・サービス開発を促進するメリット

従来は、開発した製品が健康に及ぼしている影響に関するデータを収集するためには、莫大なコストを必要としていた。この点について、製品を使っている人、使っていない人の健康に関する情報を、統計的にかつ低コストで得ることができれば、企業の製品開発が促進されるというメリットが生まれる。また、その効果について客観的なデータに基づいて確認できることにより、利用者も安心してその製品の効果に期待することができるようになる。

（３）多くの産業が健康分野と結びつくメリット

今まで、医療とはあまり結びつかなかった業種や分野の産業が提供する製品やサービスについて、コストをかけることなく健康との関連情報を得られるようになれば、製品やサービスの機能の１つとして健康に関する機能を研究し付加することが始まるのではないかと期待される。

（４）健康機能による産業強化

日本製品の特徴として、“高品質”であるということは世界的に認識されている。高品質、すなわち精度の高さや性能の高さといった元来の特色に、“健康”という新たな特色を加えて、他国の製品やサービスとの差異化を図り、訪れつつある世界的な高齢化社会に適した製品やサービスを提供することにより、日本製品の優位さを維持できるのではないかと考える。具体的にどのような健康機能を製品やサービスに付加するかについては、それぞれの産業、企業による研究努力の結果によるが、どのようなものを追加するとしても、研究を促進するためには、医療・健康情報の三次利用が欠かせない。

５－３－２．三次利用を実現するための課題

三次利用を実現するためには、昨年度のプロジェクトにおいて二次利用について検討した課題に加えてさらに別の課題が存在すると考えられる。昨年度二次利用についての検討で挙げた主な課題としては、データの統合化（紐付け）の課題、プライバシー保護の問題、大規模情報の処理、管理の課題などがある。ここでは、三次利用に特有と考えられる課題について考察した。

（１）医療情報の専門性の問題

病院、特に大病院や大学病院には、カルテ情報や検査情報など様々な医薬に関する多くの情報が収集され蓄積されている。医療情報であるこれらの情報の取り扱いには厳重な注意を要するものであり、病院外もしくは病院の中であっても、基本的に関係者以外は持ち出すことができないものである。しかし、医療技術の発展に役立てることを目的として、厳密な手続きに従って研究機関等が利用できる制度が発足し運用が始まった。今後、この医療情報を利活用する仕組みを拡張して、医療周辺の健康産業や生活一般のより広い範囲の産業分野での利用を進めていくことを考えると、情報をより利用しやすい形にすることが重要になると考えられる。医療機関でない分野の企業にとって、例えば病気や治療に関する情報を得ることで、新製品や新サービスの開発が可能になることが分かったとしても、医療という専門性の高い分野の情報を自分たちの研究開発に使えるものにするためのハードルは非常に高いものであると思われる。

（２）情報処理技術の問題

多種多様、かつ膨大になるであろう集積された医療情報を効率的に分析する情報技術は、情報工学を得意とするICT企業の有する技術であると言える。

（３）法律等の整備

法律や取り扱いに関する規制を整備するにあたって、医療分野以外での利用を前提とすると、医療分野における二次利用以上に慎重な情報の取り扱いが必要である。しかしながら、制限を掛けすぎると情報の利用価値が下がり、かえって産業の発展を阻害することにもなりかねないと考えられる。

５－３－３．三次利用を実現するための新しいICTビジネス領域

医療情報を他の産業分野で利用しようとする場合、前述したような専門性の課題が存在するため、医療分野および利用しようとする産業分野、双方についての専門的な知識が必要となる。特に医学的な知識は非常に専門性が高いため、医療関係者でない他の産業分野の技術者が必要な知識を身につける場が必要となると考えられる。また、膨大かつ多種多様なデータを取り扱い、分析することになるため､情報処理分野に関する知識と技量も求められることになる｡このように、3つの分野に通じた高度なスキルを有する人材をどのように育成するかは大きな課題である。ま

た、医療データを他の産業分野で利用可能とするようなICTの技術開発を進め、膨大で多種多様な医療関連データを分析し、適切な形で他の産業分野で利用できる形態にすることも進める必要があると考える。この領域は、3つの分野を結ぶ領域であり、多くの産業分野に健康化をもたらすキーとなる領域であると考えられる。ICTを駆使し、多くの企業に医療情報を提供する新しいビジネスの１つになると考えられる（図 ５－３－２）。

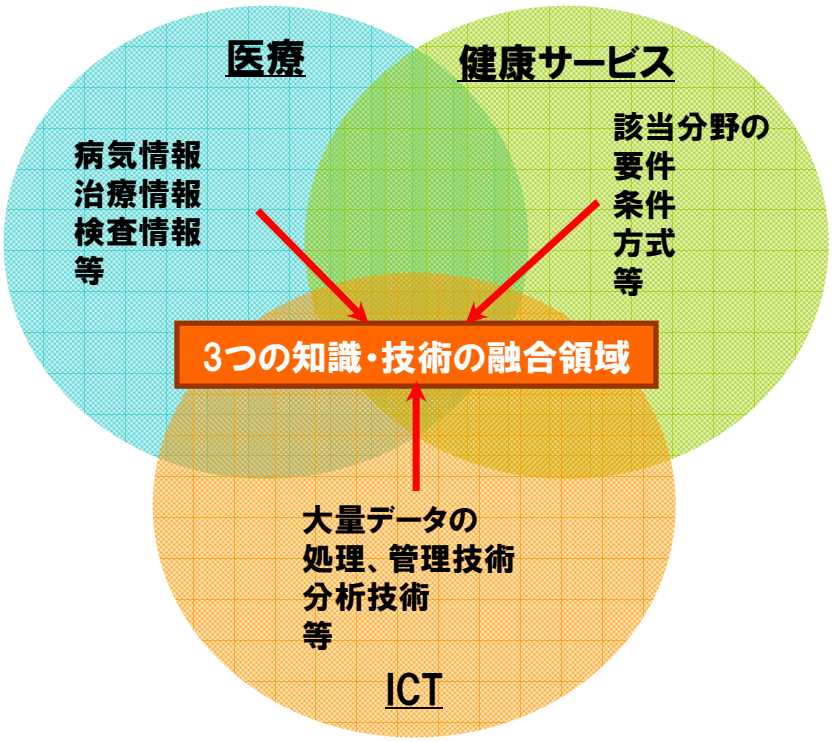


図 ５－３－２　異なる分野のノウハウの融合

５－４．医療分野における提言

東日本大震災の経験から、平常時にも災害時にも対応できる医療環境が求められる。そこで、被災に対応できる医療分野のBCP策定と災害医療支援基盤の構築を提案する。実現のためには以下が必要である。

- 今後発生が予想される東海、東南海、南海地域における災害を想定した、医療分野におけるBCPの策定。
- BCPを支える災害医療支援基盤の構築による、医療分野における減災の実現。
- 被災時における診療の継続と二次的な患者の発生を抑制するための、平常時における医療情報のバックアップ。
- 番号制度の利用や共通診察券・被災時本人確認の仕組みの導入による、本人と情報の紐付け。
- 医療情報に限らず生活支援に係る個人情報を含めた、プライバシー保護の確立。

治験を含む医療統合システムの実現については、以下の課題解決が必要である。

- 治験のみならず医療や医療関連機関との統合にあたって、従来から十分配慮されている個人情報の取り扱いについて、より厳密かつ効率のよい手法、ならびに技術の開発導入。
- 医療機関や治験依頼者の利用負担コストを下げるためのシステム、およびサービスの実現。
- 国際共同治験も実施可能な、国際標準への対応。
- 病院や医療関係システムとの統合化についての課題解決（例えば、医療情報の形式の統一化、操作の一元化）。

医療情報を他の産業分野で利用するためには、次のような課題解決が必要である。

- 医療・情報活用産業・ICT 技術の 3 つの分野を見通せる人材育成。
- 医療・情報活用産業間の知識ギャップを埋める知的情報処理技術の開発。
- 大規模情報に対して情報漏えいや紛失等を起こさない、高度な情報処理・管理技術。
- 医療情報を他の産業分野で利用可能にする法的整備。

６．製品安全分野についての検討

製品安全分野の検討においては、クラウド基盤化のメリットの訴求と東日本大震災で明らかになった課題や状況変化の反映を目的に、昨年度検討したユースケースについてクラウド基盤上のサービス（SaaS : Software as a Services）の視点で深堀を行い、「製品安全情報共有クラウド基盤」を提唱する。具体的には、製品安全情報共有クラウド基盤のニーズ、必要な機能およびそれを実現する技術、について検討を行う。特に、クラウド特有の課題であるセキュリティに関して踏み込んで整理する。

６－１．昨年度の検討と課題および東日本大震災で明らかになった課題や状況変化

昨年度は、共通番号の民間活用の視点で製品安全分野における個人番号・法人番号を用いたユースケースについて検討した。具体的には、個人番号・法人番号管理センター、製品安全センター、製品情報管理機関の三層アーキテクチャ（図　６－１－１）に基づき、4 つのユースケースの検討を実施した。

① 製品リコール対応
② 事故未然防止
③ 保守継続性
④ 製品リユースにおける品質管理・保証

この三層アーキテクチャでは、個人番号・法人番号管理センター、製品安全センターを公的なクラウド基盤として導入する一方、各機関の所有する製品情報管理システムにおいて、ユースケースによっては製品情報を提供する共通インターフェースを提供する必要があった。

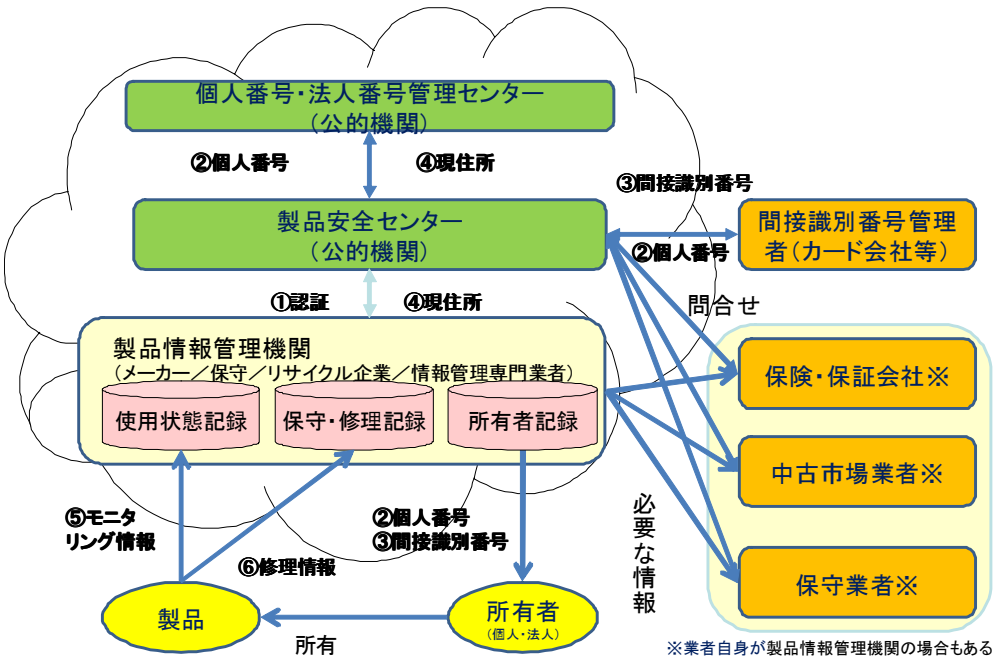


図　６－１－１　製品安全クラウド

昨年度の検討時の課題としては、個人番号・法人番号により、製品の所在把握率が向上する期待があるものの、各製品情報管理機関における製品情報管理システムの成熟度には企業によってばらつきがあり、共通インターフェースを作るというインセンティブが弱いという問題点があった。また、製品安全分野の対象機器がネットワークに接続される時代においては、製品のトレースやモニタリングが直接可能となり、必ずしも個人番号や法人番号による所有者のトレースが必須ではないという議論もあった。

その後発生した東日本大震災では、自動車や家電製品などの膨大な量の廃棄物の処理に伴う所有者把握の必要性の再確認とともに、復旧時の製品安全確認の効率化の必要性が明らかになった。また、電力不足解消および自然エネルギー活用が優先度の高い課題と認識され、スマートグリッドなどの製品をネットワークに接続し、モニタリングするインフラの整備の機運が高まった。

今年度は、上記の検討結果あるいは状況変化を受けて、国民 ID から検討範囲を広げるとともにクラウド基盤の原点に戻り、「製品安全情報共有クラウド基盤」のコンセプトを示し、その実現可能性について検討した。以下では、製品安全情報共有クラウド基盤のニーズを明確にし、その実現に必要な技術および制度的課題を明確にする。

６－２．基本コンセプト：製品安全情報共有クラウド基盤

ここでの製品安全情報とは、製品の出荷前の製造および試験情報と製品出荷後の稼働、使用状況、修理、保守状況、廃棄の製品ライフサイクルでの情報を意味する。

「製品安全情報共有クラウド基盤」とは、各メーカーが持っている／持とうとしている品質情報管理システムを、クラウド上の共通サービス（SaaS）として提供する基盤である（図 ６－２－１）。製品安全情報共有クラウド基盤は、金融機関の共同センターと同様のコミュニティクラウドに分類できる。

製品安全情報共有クラウド基盤は、基盤として表 ６－２－１に示す機能を持つ。

- 品質情報のフォーマット／テンプレート。
- 製品の使用者および使用状況をモニタリングする機能。
- 品質情報を解析する製品安全解析機能群（故障予測、故障解析など）。
- 統計的および個別の品質／製品安全情報をサービスとして提供する機能（リコールや震災等の有事際には、公的機関に必要な情報を提供する機能を含む）。
- 製品の品質情報および製品使用者の個人情報のセキュリティを担保する機能。

現状では、品質情報管理システムが十分整備されていない企業が多い。それらの企業では、独自に開発するより、本クラウド基盤の共通サービスを利用するインセンティブはある。また、データや解析ツールの標準化・共通化および有事対応など、公益性もある。さらに、震災後のエネルギーマネジメントの状況変化を受け、ネットワーク経由の製品モニタリングのインフラも急速に整備が進むことが期待できる。

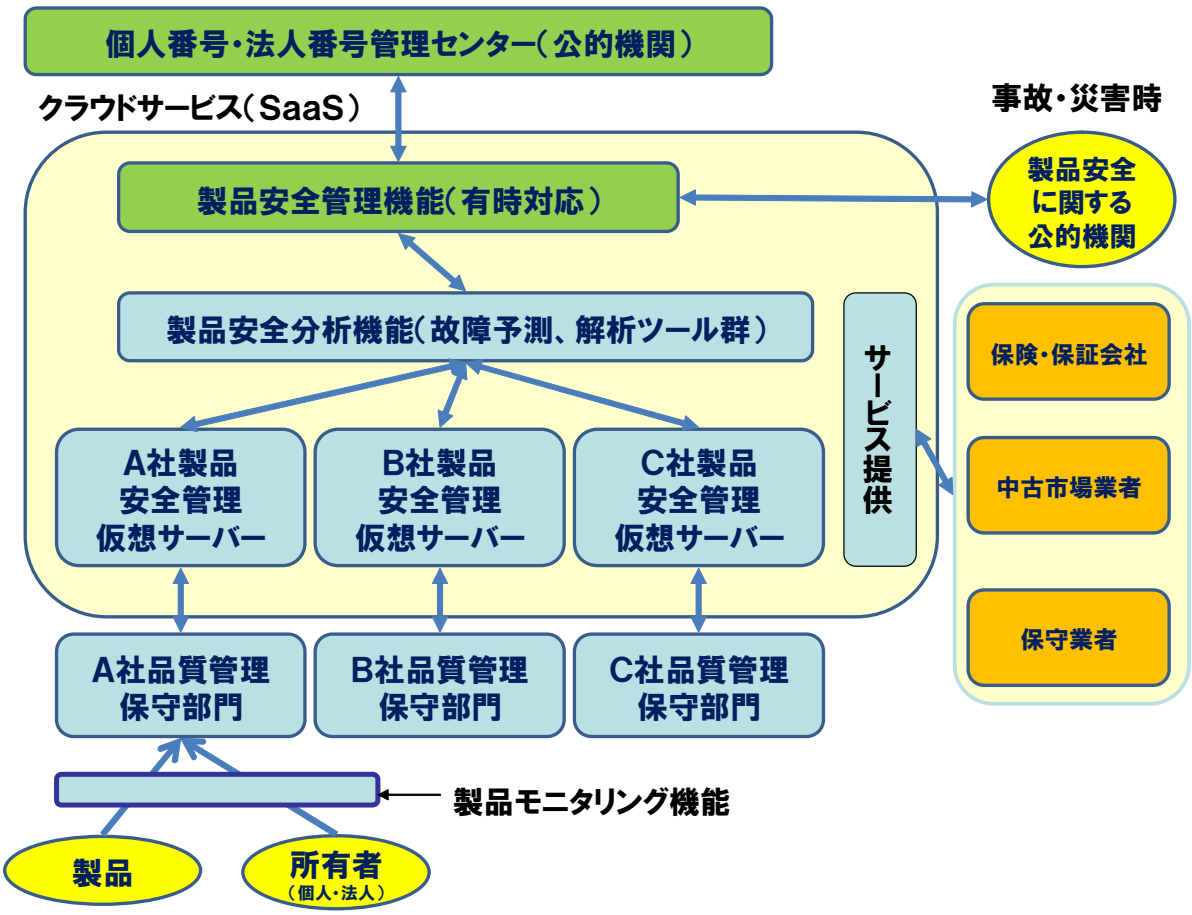


図　６－２－１　製品安全情報共有クラウド基盤

表　６－２－１　製品安全情報共有クラウド基盤の機能

No	機能	概要
1	製品安全情報フォーマット／テンプレート	製品安全情報のモニタリングおよび解析を行うための共通フォーマット／テンプレート。
2	製品モニタリング機能	ネットワークに接続された製品安全情報（使用状況、劣化状況）をモニタリングする機能。IPPC、eSHIPS などの成果を活用。
3	製品安全情報分析機能	品質情報を分析するためのツール／ライブラリ群（故障予測、故障解析など）。
4	セキュリティ管理機能	製品の品質情報および製品使用者の個人情報のセキュリティを担保する機能。
5	製品安全情報提供機能	統計的および個別の品質情報をサービスとして提供する機能（リコールや震災等の有事の際には、公的機関に必要な情報を提供する機能を含む）。

６－３．関連する既存の取り組み、およびニーズ調査

関連する既存の取り組み、およびニーズ調査の結果について以下に整理する。なお、電気・電子情報連携協議会（IPPC）における製品トレーサビリティに関する先導的な取り組み、特に通信ネットワークを介してリコール情報を対象機器に通知する「リコール情報告知システム」に関しては、昨年度の最終報告書で言及しており、ここでは省略する。

（１）先行企業の取り組みと製品安全情報共有クラウド基盤へのニーズ

製品の運用時のモニタリング機能を持つ品質管理システムを自社で開発し運用している先行企業として、富士ゼロックス株式会社（以降、富士ゼロックス）の品質管理システム「TQMS[16]」や株式会社　東芝（以降、東芝）の「PC ヘルスモニタ[17]」がある。富士ゼロックスの TQMS は、品質管理機能に加えてリモート監視機能および保守支援機能を持っている。東芝の PC ヘルスモニタは、PC に内蔵されたセンサーから PC の健康状態を診断しユーザに情報提供するとともに、ネットワーク経由で収集したデータを用いて様々なサービスを提供することを検討している。

これらの先行メーカーは独自にシステムを構築しているが、そのようなメーカーは多くはない。特に、品質管理部門のリソースが不足している場合には、製品安全情報共有クラウド基盤のようなサービスへのニーズがあると思われる。また、経時劣化の品質管理に関しては他分野でも共通化できる部分が多い。実際に、富士ゼロックスでは、自社だけでなく他業種のメーカーへのコンサルティングやシステムの展開を、すでに「お客様共創ラボラトリー」という形で取り組んでいる[18]。

（２）製品安全に関する公的機関の取り組みとサービス連携の可能性

製品評価技術基盤機構（NITE）製品安全センターでは、消費生活用製品（家庭用電気製品、燃焼器具、乗物、レジャー用品、乳幼児用品等）の製品事故に関する情報の収集と原因究明および調査結果の情報提供を行っている[19]。なお、製品に欠陥があった場合だけでなく、未然防止を目的として誤った使用方法や不注意による製品事故の情報提供も行っている。また、事業者等が行った社告・リコール情報を収集しており、データベース化するとともにリーフレットやチラシを作成している。製品安全情報共有クラウド基盤が構築された場合には、NITE 製品安全センターのような公的機関とも積極的にサービス連携することで、より一元的な製品安全の仕組みが実現できると思われる。具体的には、製品安全情報共有クラウド基盤で管理されている製品が、社告・リコール対象となった場合には、ネットワーク経由で状況把握および管理する、使用状況のモニタリングにより誤った使用方法に対する把握および警告を行う、などが考えられる。

（３）スマートハウス情報活用基盤整備フォーラム（eSHIPS）の取り組み

eSHIPS は、スマートハウスに係る「市場創り」に向けて、異業種が集まり、家庭エネルギー情報を活用する新事業を創出できるオープンな仕組みを実現することを目的に設立された

[20]。昨年度の活動の中で、新サービス創出 WG では、家庭内でのエネルギー利用状況などのセンシング、モニタリングと、ICT を組み合わせ、低炭素時代のスマートな暮らしを実現する“スマートハウス”の機能を活用し、新たな付加価値を生むサービス事業としてどのようなモデルが考えられるかなどが検討された[21]。B2C 事業領域では、「販促・需要開拓」に加えて、「エネルギー利用効率化」や「故障・不具合予兆検知」などの価値を創出する「家電使い方サービス」や「家財管理サービス」など製品安全に関するモデルが構想された。東日本大震災以降、エネルギー消費の可視化サービスの必要性が増しており、可視化サービスのためのスマートハウスの情報利活用インフラの整備が進むと思われるが、次のステップとしてそのインフラを活用した製品安全に関するサービスも進展することが期待できる。特に、長期間の実績データが少ない家庭用の太陽光発電や蓄電池などの新しいスマートハウス関連機器に関しては、製品品質モニタリングへの期待は大きい。製品安全情報共有クラウド基盤構築にあたっては、スマートハウスのインフラの活用を前提とするとともに、eSHIPS で検討されてきたスマートハウスのサービスニーズを参考にする必要がある。

６－４．開発すべき技術の要件

開発すべき技術に求められる要件について、以下に述べる。

（１）大規模データ処理

膨大な数の製品の時系列のログ情報をクラウドで収集・分析するための技術が不可欠となる。大規模データ処理技術には、①サーバーに蓄積された膨大な製品ログデータをバッチ処理する技術と、②時系列で収集される製品ログデータを逐次的に処理する技術がある。前者の技術としては、Google の検索エンジン用に開発されたバッチ処理システムをオープンソース化した「Hadoop」が注目されており、企業での利用が進んでいる。後者は、CEP（Complex Event Processing）と呼ばれる分野であり、近年研究開発が進んでいる。

（２）異常検知・故障診断

製品の異常検知、故障診断に関しては、統計的品質管理など多くの研究開発があり、個別の分野・製品に関しては既に実践されている。一例として、株式会社　小松製作所の「KOMTRACKS」、富士ゼロックスの「TQMS」、東芝の「PC ヘルスモニタ」、などがある。また、国立大学法人　電気通信大学（以降、電気通信大）　鈴木和幸研究室では、高品質・高信頼性を実現するための情報の収集・蓄積・構造化・最適化・還元を行う統合情報システムとして、「次世代信頼性・安全性情報システム（QRIS : Quality and Reliability Information System）」を開発している。次世代信頼性・安全性情報システムの構成を図　６－４－１に示す。これは、コミュニティクラウド上の SaaS を想定したものではないが、製品安全情報共有クラウド基盤の製品安全分析機能としては、これらの既存技術をツール／ライブラリ群として組み込む必要がある。また、単純にソフトウェアを共同利用するだけでなく、コミュニティクラウドのユーザ企業間で知識を共有する仕掛けこそが、製品安全情報共有クラウド基盤の肝となる。例えば、

過去に販売経験のない新興国における、従来の想定と異なる使用環境に起因する品質問題を、故障モードや故障メカニズムとして共有化することは、日本の産業競争力強化にも貢献するものと思われる。

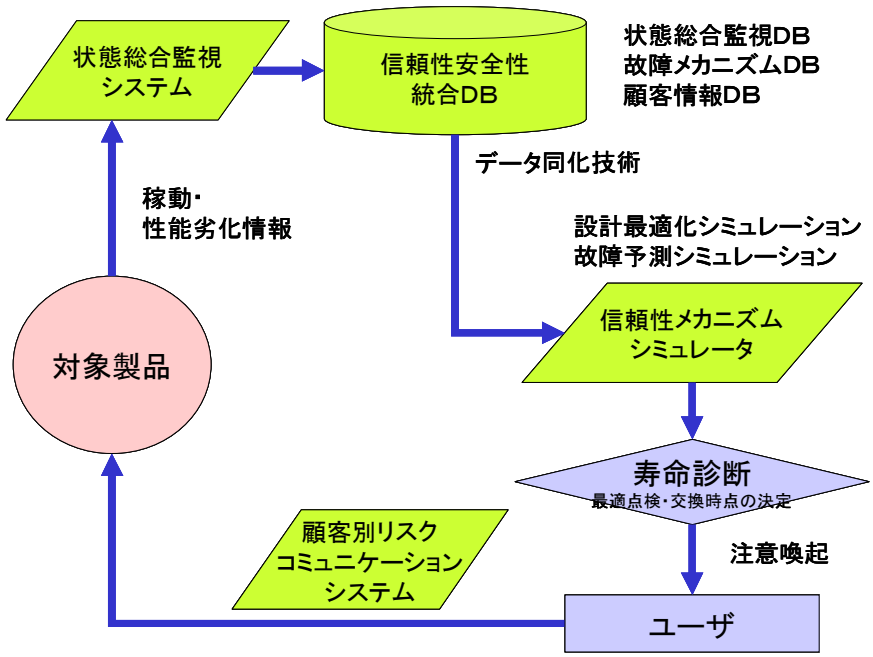


図　６－４－１　次世代信頼性・安全性情報システム（電気通信大学　鈴木和幸研究室）[22]

（３）セキュリティ管理

コミュニティクラウドの SaaS としての製品安全情報共有クラウド基盤において、セキュリティ管理は重要な課題である。セキュリティ管理の対象、場所および想定されるリスクおよび技術要件について整理する。

（ア）セキュリティ管理の対象

- 製品使用者の個人情報
  製品安全情報としては個人を直接特定されるような情報は集めないとしても、個人番号とセットにすることで、その個人が製品をどのように使用しているか（使用頻度、使用時間、使用機能など）が把握可能となる。この情報は、クレジットカードの購買履歴などと同様に一種の個人情報であり、セキュリティ管理の対象である。
- 製品の品質情報（企業情報）
  製品の平均使用時間や故障確率などの品質に関する統計情報は企業の機密情報である。また、生情報も大量に漏れる場合は統計情報に変換可能であり、セキュリティ管理の対象である。

（イ）セキュリティ管理の場所とリスク

- 品質情報収集時（第三者への漏えいリスク）
  ネットワーク経由で製品モニタリング情報を吸い上げる際に、ネットワークを物理的に共有する第三者に品質情報が漏えいしないためのネットワークセキュリティ管理が必要である。特に、製品モニタリングにスマートホーム／スマートグリッドのインフラであるスマートメータを利用する場合は、様々なサービスが同居するため、統合的な管理が必要となる。
- 品質／製品安全情報保存時（コミュニティクラウドユーザ間の漏えいリスク）
  収集された製品の品質情報をコミュニティクラウドで管理する際に、各企業の情報が他の企業や外部に漏れないようにするためのセキュリティ管理が必要である。
- 品質／製品安全情報分析時（分析者およびクラウドユーザ間の漏えいリスク）
  収集された各社の製品の品質情報を統計的・データマイニング的に分析する際に、分析者（分析ツール）への不必要な情報漏えいを避けたいならば、分析データの匿名化等の処置が必要となる。また、コミュニティクラウドユーザ企業の情報を統合して分析する場合、各企業に分析結果をフィードバックする際に、各社の製品品質情報および製品使用者の個人情報が特定できないかのチェックが必要である（例えば、ある分類に属する製品が１つだけである場合は、その分類の統計データはその製品の情報であることがわかってしまう）。さらに、製品の品質／製品安全情報の分析結果は、各企業の企業秘密であり、漏えいすることで不利益が発生する可能性がある。例えば、寿命モデルや故障確率モデルの漏えいにより、ネガティブな面だけを捉えた誤解や悪用が懸念される。
- 品質／製品安全情報使用時（品質情報参照者への漏えいリスク）
  保守業者（修理センター）や保険・保証会社等の品質情報参照者が、その業務に不必要な情報（例えば、修理対象以外の製品の品質情報）を参照できないようにするセキュリティ管理が必要である。

６－５．セキュリティ管理に必要な具体的な技術

上記の要件の中で、大規模データ処理、異常検知・故障診断に関しては、クラウド基盤とは独立な要件であり、すでに技術開発は進んでいる。一方、製品品質／安全情報管理のコミュニティクラウドでの実現は未検討な部分が多く、特にセキュリティ管理は最も重要な要件であると思われる。また、医療分野などの他のユースケースと共通の項目も少なくない。以下では、製品安全分野のセキュリティ技術に関する具体的な検討を進めていく（表 ６－５－１）。

（１）スマートメータのセキュリティ技術（品質情報収集時）

スマートグリッドのセキュリティ要件は、NIST IR7628（米国国立標準技術研究所 Interagency Report 7628）にまとめられており、関連する技術開発が進められている[23]。製品

安全情報共有クラウド基盤においても、スマートグリッドのインフラを利用する場合は、これらの標準化された技術に基づいたセキュリティ管理を行う必要がある。

（２）製品安全情報匿名化技術（品質／製品安全情報分析時）

品質情報を統計的／データマイニング的に解析するためのツール／ライブラリ群を開発する（故障予測、故障解析など）ためには、製品や個人の特定は必要ではない。開発に必要な情報以外を匿名化する技術が必要である。さらに、個人を直接特定する情報を削除するだけでは対策として不十分であり、複数の情報を組み合わせることで個人を特定できる可能性があるため、k-匿名化技術等の検討が必要である。

（３）プライバシー保護データマイニング（品質／製品安全情報分析時）

プライバシー保護データマイニングは、秘密情報を含むデータが複数ノード（各社の仮想サーバー）に分散しているときに、これを自身以外のノードやデータを集約するサーバーには開示せずに、集約したデータ集合から計算可能な有用な知識を自動発見するための技術である[24]。プライバシー保護データマイニングには、匿名化技術の他にも様々な研究開発段階の技術があり、セキュリティ管理として導入を検討する必要がある。

（４）製品品質情報参照時オプトイン技術（品質／製品安全情報使用時）

品質情報参照者が製品所有者の許可に基づき、製品安全情報を参照する技術を開発する。特に品質情報参照者が、業務に不必要な情報（例えば、修理対象以外の製品の品質情報）を参照できないようにするアクセス制御の仕組みが必要となる。

（５）第三者監査技術（品質／製品安全情報分析時、品質／製品安全情報使用時）

データ分析および参照時のアクセス状況を監査する技術／仕組みを開発する。生データの目的外使用を抑止する。特に、品質監査時に生のアクセス情報を解析するのは現実的ではないため、保護すべき情報を明確にした上で、モニタリング項目をどのように設定するかが鍵になる。

表 ６－５－１　製品安全情報共有基盤のセキュリティの開発項目

No	開発項目	概要
1	スマートメータのセキュリティ技術	製品品質／安全情報をスマートメータ経由で収集する場合の標準化されたセキュリティ管理技術を適用する。
2	製品安全情報匿名化技術	品質情報を解析するためのツール／ライブラリ群を開発する（故障予測、故障解析など）ためには、個人の特定は必要ではない。開発に必要な情報以外を匿名化する技術を開発する。
3	プライバシー保護データマイニング	プライバシー保護データマイニング技術の製品品質／安全情報分析に適用する。

4	製品品質情報参照時オプトイン技術	修理時等の製品所有者の許可に基づき、製品品質情報を提供する技術を開発する。
5	利用アプリケーション第三者監査技術	データ分析および参照時のアクセス状況を監査する技術を開発する。生データの目的外使用を抑止する。

６－６．製品安全分野における提言

個人情報や企業情報に紐付けることができる製品品質／安全情報を管理し活用するシステムをコミュニティクラウド上の SaaS として提供する「製品安全情報共有クラウド基盤」を構築することで、出荷前の製造情報や試験情報から、使用状況、修理・保守状況、廃棄状況に至るまで、一連のライフサイクルを管理する仕組みを共通インフラとして提供できる。これは、製品販売時の低価格競争に陥ることなく、ライフサイクルを通じて製品の価値を高めるものであり、我が国の産業競争力強化にも貢献するものである。また、スマートグリッドやスマートハウスなどの製品の使用状況をモニタリングするインフラが整いつつあり、製品安全情報共有クラウド基盤導入に向けた大きな変化点を迎えている。その実現に向けての主な課題は以下である。

- 製品安全情報のモニタリングおよび解析を行うための共通フォーマット／テンプレートの整備。
- スマートグリッドやスマートハウスなどの国のインフラ整備事業における、ネットワークに接続された製品安全情報（使用状況、劣化状況）をモニタリングする機能の埋め込み。
- 品質情報を分析するために必要なツール／ライブラリ群（故障予測、故障解析など）の産学連携による研究開発の加速。
- 共有することでメリットがある製品品質／安全情報（故障モードや故障メカニズム、および統計モデル）をサービスとして提供する仕組みの開発と情報提供者へのインセンティブの設計、および社会的認知の形成。
- 製品の品質情報、および製品使用者の個人情報のセキュリティを担保する技術の開発。具体的には、スマートメータのセキュリティ技術、製品安全情報匿名化技術、プライバシー保護データマイニング、製品品質情報参照時オプトイン技術、利用アプリケーション第三者監査技術の開発の推進。

７．セキュリティ分野についての検討

本プロジェクトで提案している「個人情報や企業情報を活用するためのクラウドコンピューティング基盤」が、社会基盤として広く利用されるためには、適切な法制度の下で国民にとって安心・安全を感じられる基盤として構築され、正しく運用される必要がある。特に個人情報等を安全に活用するための基盤として番号制度を広く民間にも利用する場合、番号制度に携わる組織や人の数も多くなることから、一般的にセキュリティの脅威が増大する。また、情報の利用範囲も広くなることから、個人情報の漏えい、プライバシー侵害という問題だけでなく、犯罪への情報利用や金銭がらみの被害など、脅威の種類・程度も多種多様化し、リスクも大きくなると考えられる。

昨年度は上記状況を鑑み、個人情報や企業情報を利活用するために解決しなければならないセキュリティ上の課題や脅威について、医療、製品安全、金融分野でのユースケースを例として議論し、その議論から出てきた課題とその課題を解決する技術的・制度的な対応策を纏めた[7]。さらに、技術的・制度的な対策を講じることはもちろん、それらの対策により、「安心安全な情報の利活用がどのように実現されるか」ということを分かりやすく説明するために国民目線での回答例としても纏めた。

しかしながら昨年度の検討結果に基づけば、番号制度の民間活用において、悪意のある第三者からの不正アクセス等による情報漏えい、情報改竄に関する脅威は、現在のセキュリティ対策でおおむね対抗することができるが、権限保有者による目的外利用や本人の許可なしでの情報流通に関する脅威に関しては、必ずしも対策が施されているとは言えず、それが国民の不安につながっているのではないかと考えられる。それゆえ、番号制度の民間活用において、それらの脅威への対策を講じることが重要である。権限保有者による不正を抑止するための対策としては、利用履歴を記録していることを権限保有者に知らせることが効果的であり、それには対象となるシステムに対して、どのようなログを取得管理すべきかを検討し、権限保有者が行った処理を確認できる仕組みを整備する必要がある。また、権限保有者による不正がないことを国民に証明するために、第三者機関を設置し、第三者によるセキュリティ監査・監視を行うことも重要と考える。

今年度は上記状況を鑑み、権限保有者による不正を抑止するための対策として、番号制度の民間活用を念頭に入れた第三者機関によるセキュリティ監査技術のあり方について検討した。

７－１．第三者監査の概要

昨年度の検討内容に基づけば、安心安全な番号制度の民間活用には、現在のセキュリティ対策に加え、以下の仕組みを整備する必要がある（2010 年度報告書[8]抜粋）。

① 番号制度に則った正しい運用の実現
② 不特定多数の組織への番号提供及び情報提供の防止
③ 権限保有者による不正の抑止
④ 不正がないことの国民への証明
⑤ その他

ここでは、昨年度の検討結果を踏まえ、我々が考える第三者機関の概要を記す。

我々が考える第三者機関は、具体的に表　７－１－１に示す業務を行う組織として定義する。

表　７－１－１　第三者機関の役割

目的	業務	概要
①番号制度に則った正しい運用の実現	ガイドライン策定、評価基準策定	●ガイドライン・評価基準策定
②不特定多数の組織への番号提供及び情報提供の防止	認定業務	●システムにおける情報保護評価 ●組織・人の認定と失効
③権限保有者による不正の抑止	**セキュリティ監査業務**	●書類監査 **●監査用ログの監査**
	セキュリティ監視業務	●個人情報へのアクセスに関する監視 ●立ち入り調査
④不正がないことの国民への証明	情報公開、問い合わせ対応	●不正組織の公表 ●国民（被害者）への通知 ●苦情受付
⑤その他	国際協力等	●個人情報取り扱いに関する国際協力 ●個人情報保護の普及啓発

表　７－１－１に示すように、番号制度の民間活用における第三者機関の業務は多岐に渡るが、本報告では、この内、第三者機関の主要な業務であり、これらの業務を支える上での出発点でもあるセキュリティ監査業務、特に「監査用ログの監査」について的を絞り、番号制度の民間活用を念頭に入れた監査技術のあり方について検討した（図　７－１－１）。

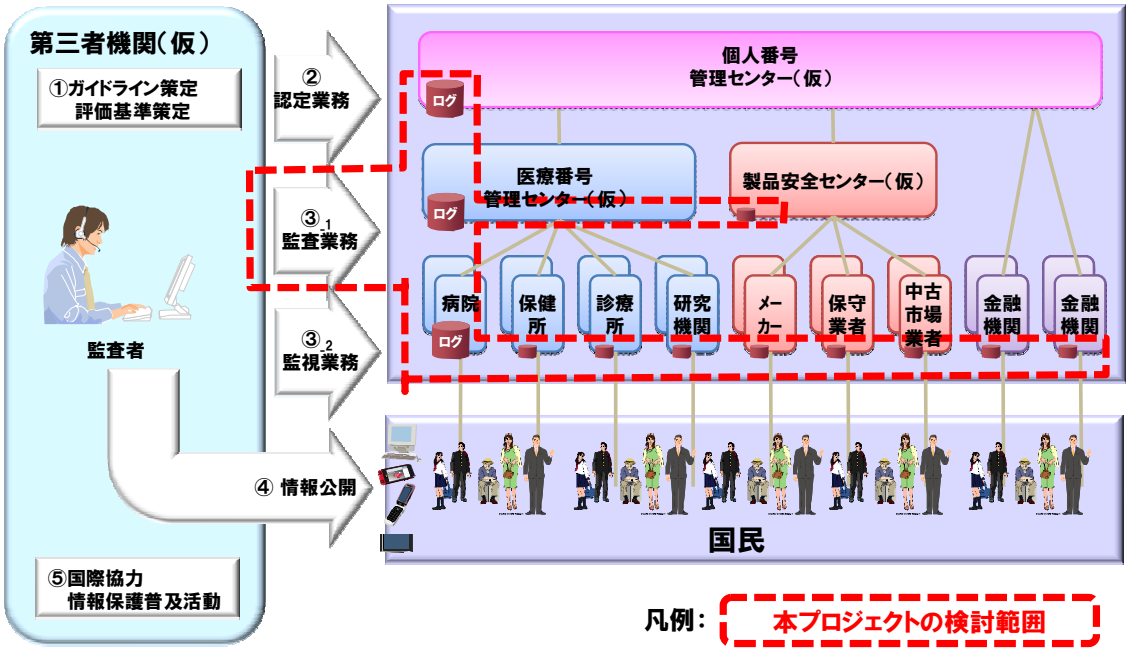


図　７－１－１　第三者機関の業務イメージと検討範囲

７－２．セキュリティ監査（監査用ログの監査）に関する課題

本検討では、監査技術のあり方を検討するにあたり、昨年度の検討結果より、権限保有者による脅威を分類した。その結果、権限保有者による個人番号に関する脅威は、職員による個人番号に紐付いた個人情報の不正閲覧等「組織内部に閉じる脅威」と、個人番号を媒介とした不正なデータ連携等「組織内では閉じない脅威」とに分類することができた(表 ７－２－１)。どちらも権限保有者による脅威であるが、前者の個人情報不正閲覧等の脅威は、個人番号に特化した脅威ではなく、個人情報保護そのものに関するものと考えられる。それゆえ、それらの脅威に対する監査は、経済産業省発行の「情報セキュリティ管理基準[9]」や「情報セキュリティ監査基準[10]」に基づいて運営される情報セキュリティ監査制度や一般的なシステム監査制度等に委ねることにし、ここで言うセキュリティ監査とは、後者の番号制度の民間活用により顕著に表れる個人番号を媒介とした不正なデータ連携等の脅威を中心に、従来の組織毎に行われる監査では対処することが難しい組織間を跨った監査に注目して議論を行う。

表 ７－２－１　権限保有者による脅威の分類

脅威の分類	例
組織内部で閉じる脅威	● 個人番号に紐付いた個人情報の不正閲覧 ● 個人番号に紐付いた個人情報の改竄 ● 個人番号に紐付いた個人情報の不正な持ち出し etc
組織内では閉じない脅威	● 個人番号を媒介とした不正なデータ連携 ・ 個人番号をキーとした不正なデータ収集（名寄せ） ・ 目的外でのデータ連携（目的外利用） ● 本人の許可なしでの情報流通 etc

個人番号を媒介とした不正なデータ連携等の対策として、セキュリティ監査では、データ連携先とデータ連携元の監査用ログの付き合わせ等、組織間を跨った監査を新たに行う必要がある。

また、番号制度の民間活用では利用範囲拡大に伴い、セキュリティ監査に必要な監査用ログが大量に発生することが予想される。

それゆえ、大量の監査用ログからデータ連携先と連携元の情報を検索し、その整合性を確認するためには、人手による監査では困難であり、監査作業の自動化が必須と考える。

本検討では、上記状況を鑑み、監査作業の自動化という観点で、監査用ログによるセキュリティ監査を実現する上での検討すべき課題について論ずる。

（１）監査用ログに求められる要件と監査項目

権限保有者による不正なデータ連携等を監査するために、監査用ログとして、どのような内容を記録するべきかを定義する必要がある。

不正なデータ連携とは、その処理が目的の範囲外で行われたものであり、監査用ログとしては目的外のデータ入出力の有無を記録する必要がある。より具体的には、「外部入力」「外部出力」各イベントにおいて、目的外利用でないことを証明するために「何時」「誰が」「何のために」「なんの情報を」「どこからどこへ」「どうしたか」を監査用ログとして取得し、以下のような項目を監査する必要がある。

- データ入出力の目的。
- 目的遂行における職員の権限の有無。
- 本人の許可の有無。
- 目的遂行のために個人情報にアクセスした回数の妥当性。
- 目的遂行のためにアクセスした個人情報の種類の妥当性。
- 目的遂行におけるデータ入出力先の妥当性。
- データ連携の際、連携元の監査用ログと連携先の監査用ログとの整合性。

また、上記の項目に加え、取得した監査用ログの正当性についても監査する必要がある。

- 監査用ログの正当性。

なお、上記セキュリティ監査は全ての関係組織にて行われることを前提にしており、それゆえ、監査用ログは全ての関係組織より出力されることから、大量のデータ数になると想定される。したがって、大量の監査用ログに対し、監査をスムーズに実施するためにはシステム・アプリケーション毎にバラバラの監査用ログではなく、フォーマットの統一をしておく必要がある（図　７－２－１）。

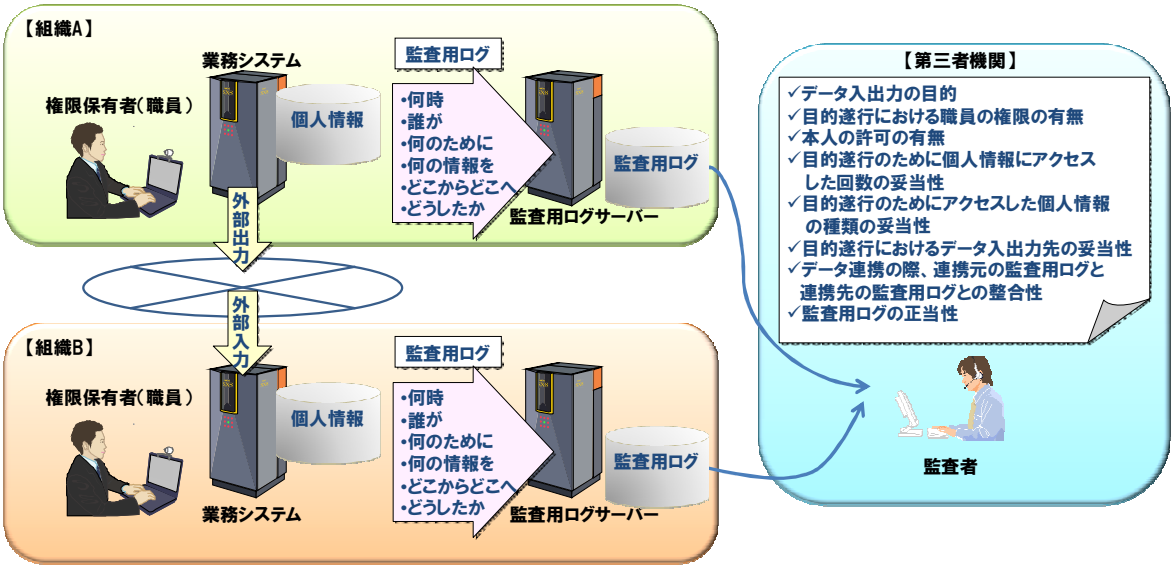


図　７－２－１　監査用ログの要件と監査項目

（２）各組織におけるセキュリティ監査制度に向けた課題

監査用ログには、データ連携等を監査するため、「データ入出力の目的」の記載が求められる。また、監査機関はデータ連携の際の連携元監査用ログと連携先監査用ログとの整合性をチ

ェックするため、関連する監査用ログのレコードを一意に定める識別子も必要になる。これらの情報は、通常のシステムログ等では取得困難な場合が多いため、各組織は、セキュリティ監査制度実施に備え、監査用ログとしてそれらの情報を取得できる仕組みを新たに導入することになると考える。また、監査用ログを取得する仕組みを回避して、不正なデータ連携ができてしまっては、セキュリティ監査制度が意味を持たなくなってしまう。

それゆえ、監査用ログを取得できる仕組みを導入する際、確実に必要な項目の監査用ログを取得できるように既存システムの改修が求められ、各組織にとっては、かなりの負担となる可能性が高い。したがってセキュリティ監査制度を実現するためには、上記状況も考慮し、何らかの方法で各組織の負担を軽減させる措置を講じる必要があると考える。

（３）監査用ログのセキュリティに関する課題

監査用ログは、権限保有者の不正を抑止するものであるので、権限保有者等によって書き換えられては意味をなさない。それゆえ、取得された監査用ログは、電子署名等の技術を用いて真正性を確保する必要がある。

また、監査用ログに、該当者の個人番号も記載された場合、監査用ログを参照することで個人の行動がトレースできる可能性が秘められている。それゆえ、第三者機関が監査用ログを監査すること自体、プライバシー侵害にならないかという課題も生じる。このように監査用ログはプライバシー侵害の危険性を帯びているため、暗号技術等を用いて監査用ログに含まれた個人情報に対し、適切な処置を施す必要がある。

（４）監査機関における監査方法について

監査用ログを監査する方法として、第三者機関の監査者が該当組織に出向き監査用ログを監査する方法や、第三者機関が監査用ログを各組織からネットワーク等を介して収集し、監査する方法などが考えられる。

総務省統計局発行の「平成 21 年経済センサス基礎調査[11]」によると、医療福祉関係の事業所数は 38,217 であり、製造業関係の事業所数は 401,365 ある。また金融保険業関係の事業所数は 65,151 である。仮に監査員が出向いてこれら全ての事業所を監査する場合※1、監査員は年間約 50 万件（1 日あたり約 1,380 件）の事業所を監査しなければならない。また、監査員の日当を仮に 1 件あたり 10,000 円×2 人とすると※2、監査にかかる人件費は年間 100 億円となり、費用対効果として合理的か考えざるを得ない。また、セキュリティ監査では、データ連携先とデータ連携元の監査用ログの付き合わせ等、組織間を跨った監査を新たにする必要があるため、監査員が出向いて監査をする方法では、一つの監査項目に対して何度も複数組織に出向く場合も生じ、不正なデータ連携に関する監査の作業効率が悪化する可能性が高い。

それゆえ、番号制度の民間活用におけるセキュリティ監査では、ネットワーク技術や ICT 技術を用いて監査用ログを収集し、監査する仕組みが必要と考える。

（５）監査用ログデータ量について

番号制度の民間活用では利用範囲拡大に伴い、セキュリティ監査に必要な監査用ログが大量に発生することが予想される。そこで我々が想定する監査用ログのデータ量について概算した（表 ７－２－２）。

総務省統計局発行の「平成 19 年国民生活基礎調査[12]」によると、医療分野における通院者数は述べ 42,066,000 人/年であり、仮に医療連携サービスにおいて、通院者の情報を他の医療機関に平均 5 回データ連携したと仮定すると※3、医療連携サービスにおけるデータ連携の総数は約 2 億件/年である。この時、監査用ログのレコード数は連携元と連携先それぞれ出力されるので、約 4 億件/年となる。ここで高度な検索手法等を用いず、単純に全件探索にて連携先の監査用ログに対応する連携元の監査用ログとの整合性を確認した場合、その整合性確認に費やす処理数は、2 億×(2 億÷2※4)=2 京件/年となる。

また、電子情報技術産業協会（JEITA[13]）によると 2010 年民生用電子機器※5 の生産実績は 52,229,196 台であり、産業用電子機器※6 の生産実績は 72,982,288 台である。計 125,211,484 台の製品に対し、製品リコールサービスの登録をするために平均 1 回データ連携したと仮定すると※3、データ連携の総数は、約 1 億件/年である。この時、監査用ログのレコード数は 2 億件/年であり、整合性確認に費やす処理数は 0.5 京件/年となる。

また、金融庁発行の「平成 23 年銀行免許一覧[14]」によると都市銀、信託、その他の銀行数は 40 行であり、信用金庫一覧によると信用金庫は 272 行ある。また、住信 SBI ネット銀行によると[15]、2011 年 6 月での口座数は 1,149,000 であり、仮に上記計 312 行が住信 SBI ネット銀行クラスの口座数を持つと仮定すると※7、金融関係の権限保有者が年 1 回現況確認で全口座を検索・更新し平均 2 回データ連携したと仮定すると※3、データ連携の総数は約 7 億件/年である。この時、監査用ログのレコード数は 14 億件/年であり、整合性確認に費やす処理数は 24.5 京件/年となる。

上記は各分野の 1 サービスを例にとった仮定上の概算値である。本プロジェクトでは番号制度を広く民間サービスに活用し、より便利にする新たなサービスを生み出すことを期待しており、それゆえ、新たなサービスの数に比例して監査用ログは増大すると予想される。また、セキュリティ監査では、データ連携先とデータ連携元の監査用ログの付き合わせ等を行うため、それに伴う処理は、その組み合わせの分に応じて増大すると考える。

それゆえ、並列分散処理の仕組みを導入する等、監査用ログを大量に効率良く処理できるようにすることが重要と考える。

表 ７－２－２　監査用ログの想定レコード数

分野	サービス	想定母数	平均データ連携数	データ連携総数	処理件数
医療	医療連携サービス	42,066,000 人	5 回(想定)	約 2 億件/年	2 京件/年
製品安全	製品リコールサービス	125,211,484 台	1 回(想定)	約 1 億件/年	0.5 京件/年
金融	現況確認サービス	1,149,000 口座×312 行	2 回(想定)	約 7 億件/年	24.5 京件/年

【注意】

※1　全事業所を監査しなければならないかは、監査内容にもより、今後の課題である。

※2　日当および人数に関しては、調査に基づくものではなく、本検討における想定である。

※3　平均アクセス数に関しては、調査に基づくものではなく、本検討における想定である。

※4　平均 N/2（N=連携先の監査用ログの数）の照合で連携元の監査用ログに対応する連携先の監査用ログが検出されると仮定する。

※5　民生用電子機器内訳：TV、DVD、ビデオカメラ、デジカメ、カーナビ、オーディオ、補聴器。

※6　産業用電子機器内訳：通信機器、電子計算機、電子応用装置、計測器、事務用機械。

※7　調査に基づくものではなく、他の銀行の口座数の平均を住信 SBI ネット銀行の口座数と仮設定した想定である。なお、ゆうちょ銀行などは数億口座保有している可能性が高い。

７－３．セキュリティ分野における提言

番号制度の民間活用により顕著に表れる脅威として、個人番号を媒介とした不正なデータ連携等が挙げられる。それらの対策として第三者機関による監査が効果的であり、それゆえ、データ連携先とデータ連携元の監査用ログの付き合わせ等、組織間を跨った新たなセキュリティ監査制度を整備する必要があると考える。また、番号制度の民間活用では利用範囲拡大に伴い、上記セキュリティ監査に必要な監査用ログが大量に発生することが予想される。

それゆえ、大量の監査用ログからデータ連携先と連携元の情報を検索し、その整合性を確認するためには、人手による監査では困難であり、セキュリティ監査制度の実現には、監査作業の自動化に向けた技術開発が必須と考える。

組織間を跨ったセキュリティ監査における監査作業の自動化に向けた技術的な課題は以下である。

- 監査用ログの記載内容およびフォーマットの定義。
- 各組織における監査用ログ取得機能の整備とそれに伴う負担軽減措置。
- 監査用ログの真正性確保とプライバシー保護。
- ネットワークを介した監査用ログの収集。
- 大量データ処理技術。

８．クラウドコンピューティング基盤の整備に向けた提言

（１）災害医療支援基盤の構築

広範囲に及ぶ災害時において、現地での診察だけでなく、遠隔地からのサポートにも対応可能な広域での情報活用を実現しうる災害医療支援基盤を構築すること。これは、医療環境が壊滅した災害地域の復興に必要であるばかりでなく、将来の災害に備える医療基盤として必要なことである。

（２）医療情報の二次利用・三次利用

医療関連産業の活性化や国際競争力の強化のため、クラウドコンピューティング基盤を用いた医療情報の二次利用を可能とすること。また、医療分野と他業種とのコラボレーションによる新産業創出に向け、三次利用を可能とすること。

（３）製品安全情報共有クラウド基盤の構築

製品の品質情報を製品安全情報共有クラウド基盤上で管理し、出荷前の製造情報や試験情報から、使用状況、修理・保守状況、廃棄状況に至るまで、一連のライフサイクルの管理を可能とすること。

（４）組織間を跨ったセキュリティ監査作業の自動化

番号制度を用いたクラウドコンピューティング基盤を運用するためには、様々な分野の様々な組織間での情報連携が行われ、それにともない膨大な監査用ログが発生することになる。この膨大なログを正確にかつ効率的に処理するための監査作業の自動化技術を開発すること。

９．まとめ

本プロジェクトでは 2 年間にわたり、マルチクラウド時代のコンピューティング基盤の有るべき姿や、情報共有の基本となる番号制度などについて検討してきた。また、その間におきた、東日本大震災を契機に、このようなコンピューティング基盤を震災被害軽減に向けて適用するための検討を行ってきた。本テーマは、技術的な検討だけでなく、種々の制度や、法律などの検討も含めて、じっくりと検討すべきもので、この 2 年間ではまだその緒に着手したところである。今後は、本プロジェクトで検討した事項を、プロジェクトに参加したメンバーが種々の場面で関係する府省などに働きかけると共に、技術課題の解決に向けた研究開発を行っていくことが必要である。その中で、特に大きな提言として、以下の 2 点について、まとめておく。

９－１．震災対応に向けての基盤整備の重要性

震災から 1 年が経とうとする今、すでに東北地方は復興期に入っており、今年度検討したシステムの適用フェーズとしては、最終段階に入っている。そのため、今年度の検討は後ろ向きなものととらえられる可能性があるが、実際はそうではない。COCN が今年度開催した、「レジリエントエコノミー研究会」ワークショップでは、過去二千年の間、東日本太平洋側でマグニチュード 8.0 以上の地震がおきた 4 つの例（貞観地震（869 年）、慶長三陸地震（1611 年）、明治三陸地震（1896 年）、昭和三陸地震（1933 年））において、いずれも 10 年以内に首都圏直下型地震が連動して発生しており（相模・武蔵地震（878 年）、江戸地震（1615 年）、明治東京地震（1894 年）、関東大震災（1923 年））、さらに 4 例中 3 例については 18 年以内に東海・南海・東南海地震が連動して発生している（仁和地震（887 年）、慶長地震（1605 年）、昭和南海・東南海地震（1944-46 年））ことが発表されている[25]。すなわち今後 10 年以内に、首都圏直下型地震ならびに東海・南海・東南海地震が発生する可能性は極めて高いと考えざるを得ない。これを考慮すれば、今年度本プロジェクトにおいてとりまとめた災害医療支援基盤ならびに、製品安全情報共有クラウド基盤を早期構築し、次なる大震災への備えとすることが望まれる。

９－２．番号制度の民間活用に基づく、情報共有による産業競争力強化

昨今、日本国内では円高、高法人税率、労働規制、自由貿易協定への対応の遅れ、温室効果ガス抑制、電力不足、という「六重苦」が叫ばれ、企業の海外流出や国内産業の空洞化につながるものとされている。さらにこれらに加え、少子高齢化、電力料金の値上げ、復興財源を確保するための増税、などの「苦」も考慮すると、産業活性化のために、あらゆる手を早急に打たなければ、国内産業の空洞化がより一層進むことになってしまう。

本プロジェクトでは、個人情報や企業情報を安全に組織間で共有するクラウドコンピューティング基盤の構築により、種々の社会システムを効率化すると共に、種々の新サービスを構築することによる、産業活性化について検討してきた。これらを用いた新たな社会基盤の早期構築が望まれる。そのためには、様々な分野における多種多様な情報の連携性を高めるために、各種の情報を紐付けするための個人番号の民間活用を早期に実現することが不可欠となる。

その一方で、民間利用を実現するために解決しておくべき技術的課題も多々あり、それらを確実に解決しなければならない。特に、世の中全体の ICT 依存度が高まる中で、近年サイバーテロの脅威が益々高まっている。個人情報や企業情報を安全に組織間で共有するクラウドコンピューティング基盤の構築のためには、このような問題にも正面から取り組む必要がある。

１０．参考文献

[1] 平成 23 年度版　情報通信白書（総務省）

[2] 今回の地震・津波による主な被害等（東北地方太平洋沖地震を教訓とした地震・津波対策に関する専門調査会第１回会合）
http://www.bousai.go.jp/jishin/chubou/higashinihon/1/3-1.pdf

[3] 「新たな治験活性か 5 カ年計画の中間見直しに関する検討会」報告（平成 22 年 1 月 19 日）
http://www.mhlw.go.jp/shingi/2010/01/s0119-10.html

[4] 「臨床研究・治験活性化に関する検討のための論点及びそれらに対する意見」より。
http://www.mhlw.go.jp/stf/shingi/2r9852000001td1v-att/2r9852000001td6z.pdf

[5] 治験等の効率化に関する報告（平成 23 年 5 月）
http://www.mhlw.go.jp/topics/bukyoku/isei/chiken/dl/110630b.pdf

[6] 第 3 回臨床研究・治験活性化に関する検討会（平成 23 年 10 月 28 日） 特定領域治験基盤整備事業-小児治験ネットワーク-
http://www.mhlw.go.jp/stf/shingi/2r9852000001td1v-att/2r9852000001td6d.pdf

[7] 個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備プロジェクト、産業競争力懇談会、http://www.cocn.jp/common/pdf/thema30.pdf

[8] 坂崎 尚生、側高 幸治、長谷部 高行、山田 朝彦、大岩 寛、
"個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備"、
情報処理学会コンピュータセキュリティ研究会：コンピュータセキュリティシンポジウム 2011(CSS2011)、論文集、p259-265

[9] 情報セキュリティ管理基準、経済産業省、
http://www.meti.go.jp/policy/netsecurity/docs/isaudit/IS_Management_Standard.pdf

[10]情報セキュリティ監査基準、経済産業省、
http://www.meti.go.jp/policy/netsecurity/docs/isaudit/IS_Audit_Annex04.pdf

[11]平成 21 年経済センサス基礎調査、総務省統計局、
http://www.stat.go.jp/data/e-census/2009/kakuho/gaiyou/gaiyou.htm

[12]国民生活基礎調査、厚生労働省、http://www.mhlw.go.jp/toukei/list/20-19.html

[13]電子工業生産実績表、電子情報技術産業協会(JEITA) 、
http://www.jeita.or.jp/japanese/stat/electronic/2011/index.htm

[14]免許・許可・登録等を受けている業者一覧,金融庁、
http://www.fsa.go.jp/menkyo/menkyo.html

[15]口座数・預金残高の推移、住信 SBI ネット銀行、
https://www.netbk.co.jp/wpl/NBGate/i900500CT/PD/corp_koza_zandaka

[16]高野ほか、TQMS による機能連携品質マネジメント、富士ゼロックステクニカルレポート No.20, 2011.
http://www.fujixerox.co.jp/company/technical/tr/2011/pdf/s_6.pdf

[17]西川、原、市場品質の監視による早期対策からプロアクティブな品質保全とサービスへ、東芝レビュー、Vol.64, No8, 2009.
[18]http://www.fujixerox.co.jp/company/technical/laboratory/
[19]http://www.jiko.nite.go.jp/
[20]スマートハウス情報活用基盤整備フォーラム 平成23年度eSHIPS活動計画
http://www.jipdec.or.jp/dupc/forum/eships/aboutus/h23plan.pdf
[21]スマートハウス情報活用基盤整備フォーラム スマートハウス情報活用基盤に関する検討活動中間報告書
http://www.jipdec.or.jp/dupc/forum/eships/results/doc/eships_fy22_sum_report.pdf
[22]http://www-suzuki.inf.uec.ac.jp/index.php?Research#f20e3a85
[23]神田ほか、相互認証と暗号化処理を統合するスマートメータ用統合鍵管理技術ＡＭＳＯ, 東芝レビューVol.65、No.10、2010.
[24]佐久間ほか、プライバシ保護データマイニング、人工知能学会学会誌、2009.
[25]徳山 日出男、東日本大震災の経験から学ぶ社会インフラ・レジリエンスの重要性.
http://www.cocn.jp/common/pdf/0913-01.pdf
[26]社会保障･税番号大綱（案）
http://www.cas.go.jp/jp/seisaku/bangoseido/youkouan_honbun.pdf

１１．付録１　情報処理学会コンピュータセキュリティ研究会：コンピュータセキュリティシンポジウム 2011(CSS2011)　論文集　P.259-265　掲載論文

個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備

坂崎 尚生 ‡,†　　側高 幸治 ‡,††　　長谷部 高行 ‡,†††　　山田 朝彦 ‡,††††
大岩 寛 ‡,†††††

‡ 産業競争力懇談会 (COCN)
100-8280 東京都千代田区丸の内一丁目 6 番 6 号日本生命丸の内ビル 株式会社日立製作所内

†(株) 日立製作所
hisao.sakazaki.qc@hitachi.com
†† 日本電気株式会社
k-sobataka@bx.jp.nec.com
†††(株) 富士通研究所
hasebe.takayuki@jp.fujitsu.com
†††† 東芝ソリューション (株)
Yamada.Asahiko@toshiba-sol.co.jp
††††† 独立行政法人産業技術総合研究所
y.oiwa@aist.go.jp

あらまし　2011 年 6 月 30 日に政府・与党社会保障改革検討本部から社会保障・税番号大綱 (案)[2] が示された。社会保障・税番号制度は，社会保障や税制を一体的に捉え，社会保障給付の効率性・透明性・公平性を高めようという観点から導入が検討されてきた社会基盤である。上記番号制度は社会保障・税分野で利用することを目的とした制度であり，民間への利活用は現段階では検討範囲外である。そこで，産業競争力懇談会 (COCN) では，民間への利活用をテーマに，番号制度が国民に安心・安全な社会基盤として受け入れられるように，番号制度の民間利用に関する脅威分析を行い，セキュリティ対策を検討した。本論文では，医療，金融，製品安全の分野での想定したユースケースを基に，課題とその課題を解決する為の技術的・制度的対応策を纏めたものである。

Inter-cloud Information Sharing Foundation for Secure Utilization of Personal and/or Enterprise Information

Hisao Sakazaki‡,†　　Koji Sobataka‡,††　　Takayuki Hasebe‡,†††
Asahiko Yamada‡,††††　　Yutaka Oiwa‡,†††††

‡Council on Competitiveness-Nippon(COCN)
Nippon Life Marunouchi Building, 1-6-6, Marunouchi, Chiyoda-ku, Tokyo-to, 100-8280

†Hitachi, Ltd
hisao.sakazaki.qc@hitachi.com
††NEC Corporation
k-sobataka@bx.jp.nec.com
†††FUJITSU LABORATORIES LTD.
hasebe.takayuki@jp.fujitsu.com
††††TOSHIBA Solutions Corporation
Yamada.Asahiko@toshiba-sol.co.jp
†††††National Institute of Advanced Industrial Science and Technology
y.oiwa@aist.go.jp

Abstract　We discuss the threat analysis in the national number system. In this paper, we describe security countermeasures of the national number system based on the medical treatment usage, the financial usage and the distribution industry usage.

1 はじめに

2011 年 6 月 30 日に政府・与党社会保障改革検討本部から社会保障・税番号大綱 (案)[2] が示された。社会保障・税番号制度は，社会保障や税制を一体的に捉え，社会保障給付の効率性・透明性・公平性を高めようという観点から導入が検討されてきた社会基盤である。上記番号制度は社会保障・税分野で利用することを目的とした制度であり，民間への利活用は現段階では検討範囲外である。番号制度の民間利用については，「2018 年を目途にそれまでの番号法の執行状況等を踏まえ，利用範囲の拡大を含めた番号法の見直しを行うことを引き続き検討する」と述べられている。上記状況を鑑み，産業競争力懇談会 (COCN) では，番号制度が個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤として広く民間にも利用される為に，基盤の構築・運用に関して網羅的・体系的な脅威分析を行い，その脅威に対して効果的なセキュリティ対策を検討した。本論文では，政府検討の番号制度における議論との混同を避ける為，上記政府検討の番号制度とは別に仮の番号制度 (以下，個人番号と称する) を想定し，医療，金融，製品安全の分野でのユースケースを基に，課題とその課題を解決する為の技術的・制度的対応策を纏めた。尚，国として情報利活用を進めるための社会保障・税番号制度については，内閣官房社会保障改革担当室 [1] や国際公共政策研究センター（CIPPS）[4] 等，様々なところで議論されているので，それらの報告書を参考にされたい。

2 番号制度の民間活用について

番号制度を民間利用するということは，番号制度に携わる組織や人の数も多くなることから，一般的にセキュリティの脅威が増大する。また，情報の利用範囲も広くなることから，個人情報の漏洩，プライバシー侵害という問題だけでなく，犯罪への情報利用や金銭がらみの被害など，脅威の種類・程度も多種多様化し，リスクも大きくなると考えられる。従って，番号制度を民間利用し，個人情報や企業情報の利活用を図っていく為には，内閣官房社会保障改革担当室 [1] や CIPPS[4] 等での検討事項に加え，民間利用による新たな脅威に対する対策を講じ，番号制度の民間利用における障害を取り除いていくことが重要である。それ故，本論文では，番号制度の民間利用により生じる新たな脅威とその対策を中心に検討する。

表 1: 保護対象資産と脅威の主体

保護対象資産 (what)	(A) 個人番号 (B) 基本情報 (氏名，性別，住所，生年月日，他) (C) その他，紐付けられた関連情報
脅威の主体 (who)	(a) 悪意の第三者 (悪意を持った外部犯) (b) 管理機関等の権限保有者 （悪意を持った内部犯，または過失の内部者）

3 番号制度の民間利用における脅威分析

3.1 脅威分析手法

脅威分析を行う手法の一つとして，5W1H 法がある。5W1H 法は「いつ (when)[1]」「どこで (where)」「誰が (who)」「何を (what)」「どのように (how)」「何を目的とした (why)」被害であるかを洗い出す手法である。本検討では 5W1H 法を採用し，3.2 節に示す医療，製品安全，金融のユースケースに沿って，「何を (what)」「だれが (who)」を定義し，各ユースケースにおける脅威を分析した。具体的には，「個人の情報」を保護すべき資産 (what) と捉え，「(A) 個人番号」，「(B) 基本情報（氏名，性別，住所，生年月日，他)」，「(C) その他紐付けられた関連情報」の 3 つを保護すべき資産とし，番号制度の民間利用における脅威を分析した。また，脅威を引き起こす可能性のある主体 (who) としては，「(a) 悪意の第三者（悪意を持った外部犯)」，「(b) 個人番号管理センターやその他民間管理機関の権限保有者（悪意を持った内部犯，または過失の内部者)」の二通りに分類し，脅威分析を行った (表 1)。

3.2 民間利用ユースケース

本検討では番号制度を民間利用した際，利便性が高く国民の生活が豊かになると思われる医療，製品安全，金融の 3 分野を例に挙げ 10 個のユースケースを設定した [3]。表 2 にて各ユースケースの概要を示す。

[1]「いつ (when)」に関して，本検討では，個人情報および企業情報の民間利用時全体を対象にしている。

表 2: ユースケース概要

	医療分野	
	医療連携サービス	各医療機関で持っている診療情報を医療機関の間で個人番号を媒介して連携させ，患者に対し地域で一貫した治療を施す為のサービス
	PHR 一次利用サービス	母子手帳から健診カルテ，死亡診断書までを電子化し，健康時から病気の時まで一貫して身体の情報を管理し，健康維持や診療支援をするサービス
	PHR 二次利用サービス	医療研究機関等が当事者の為だけでなく，公共の利益の為に蓄積情報をプライバシを保ちつつ二次的に利用し，医療の質向上に役立てるサービス
	製品安全分野	
	製品リコールサービス	製品リコールが発生した場合に，製品番号と個人番号を連携して製品の所有者情報を取得し，製品リコール情報を所有者に通知するサービス
	事故未然防止サービス	製品の使用状況をインターネット経由でモニタリングし，リスクを未然に通知するサービス
	保守継続性サービス	製品を中古で転用する場合やメーカーと異なる業者が保守を行う場合において，必要な保守情報を継承し継続性のある品質管理を支援するサービス
	製品リユースにおける品質管理・保障サービス	製品が中古市場等で取引される場合に，製品番号と個人番号を用いて必要な情報を入手し適正価格を算出するとともに，製品情報と一緒に売買することを支援するサービス
	金融分野	
	本人確認サービス	口座開設時の本人確認において，身分証の提示の代わりに，個人番号カードの認証機能等より個人番号に紐付いた本人確認を実施するサービス
	現況確認サービス	結婚や引越等で氏名・住所が変更となった場合に金融機関側で個人番号より住民登録情報を参照することで変更届提出等の手間を削減するサービス
	各種証明書手続サービス	個人が税務署に提出する各種証明書類を個人番号を用いて金融機関から税務署に直接提出することで個人での証明書の管理を軽減させるサービス

3.3 各ユースケースにおける脅威分析

本検討では，3.2 節のユースケース毎に 5W1H 法を用いて脅威分析を行い，118 個の脅威を洗い出した [3]。これらの脅威は，脅威の主体者により大きく **T1**～**T3** に大別することができ，さらに詳しくは以下のようにまとめることができる。

T1：悪意の第三者による脅威
- **T1-1**：悪意の第三者による情報漏洩
- **T1-2**：悪意の第三者による情報改竄
- **T1-3**：個人番号をキーにした名寄せ
- **T1-4**：匿名化データからの個人推定

T2：権限保有者による脅威[2]
- **T2-1**：権限保有者による情報漏洩
- **T2-2**：権限保有者による情報改竄
- **T2-3**：個人番号をキーにした名寄せ
- **T2-4**：匿名化データからの個人推定
- **T2-5**：権限保有者による目的外利用
- **T2-6**：本人の許可なしでの情報流通

T3：その他の脅威
- **T3-1**：情報の劣化消失によるサービス不履行

[2]「T2:権限保有者による脅威」には，「組織による脅威」と「組織内のある権限保有者による脅威」とがある。

また，これら **T1**～**T3** の脅威は，主に以下のような手段 (how) で引き起こされる。

【不正アクセス】正規のアクセス権を持たない人が，ソフトウェアの不具合等を悪用してアクセス権を取得し，システムに侵入して保護対象資産に漏洩や改竄等の危害を加える。
【成りすまし】個人番号を記載したカードの盗難紛失，あるいは個人番号の盗み見などにより，第三者に個人番号を取得され，その者がその個人番号を使って本人に成りすまし，本人の保護対象資産に対して漏洩や改竄等の危害を加える。
【ネットワーク盗聴】ネットワークを流れるデータを盗聴することにより，不正に個人番号や基本情報，関連情報等の保護対象資産を取得する。
【不正な情報持ち出し】システムへのアクセス権を持っている者が，不正に情報を持ち出すことにより，保護対象資産に漏洩の危害を加える。
【不正な情報処理】システムへのアクセス権を持っている者が，不正に情報を処理することにより，保護対象資産に改竄の危害を加えたり，目的外の利用を行ったりする。
【誤操作】システムへのアクセス権を持っている者が，誤操作により保護対象資産に漏洩や改竄等の危害を加える。
【個人番号をキーとした情報の収集】公開されている情報やネットワークを流れるデータ等，正規/不正に限らず，個人番号をキーとして個人情報を収集する。
【データ分析】公開情報やネットワークを流れるデータ等，正規/不正に限らず，何らかの手段でデータを大量に取得し，それらのデータを分析することにより，個人を特定する。
【その他】天災などによるデータの消滅等。

尚，表 3 は，3.3 節のユースケースから導かれた脅威に対し，その脅威を引き起こす上記攻撃手段 (how) との対応関係を纏めたものである。

4 安心安全な情報利活用の為のセキュリティ対策

一般的にセキュリティ対策は，技術的対策と制度的対策に大別することができる。技術的対策はセキュ

表 3: 脅威と攻撃手段 (how)

脅威	攻撃手段 (how)
T-1:悪意の第三者による情報漏洩	不正アクセス, 成りすまし, ネットワーク盗聴等
T1-2:悪意の第三者による情報改竄	不正アクセス, 成りすまし等
T1-3:個人番号をキーとした名寄せ	番号をキーとした情報収集等
T1-4:匿名化データからの個人推定	データ分析等
T2-1:権限保有者による情報漏洩	不正な情報持出し, 誤操作等
T2-2:権限保有者による情報改竄 **T2-3**:番号をキーとした名寄せ	不正な情報処理, 誤操作等 番号をキーとした情報収集等
T2-4:匿名化データからの個人推定	データ分析等
T2-5:権限保有者による目的外利用	不正な情報処理等
T2-6:本人の許可なしでの情報流通	不正な情報処理等
T3-1:情報消失等でサービス不履行	大災等によるデータの消滅等

リティを守る為の直接的な対策であり，制度的対策は運用管理面における間接的な対策である。セキュリティ対策というと技術的対策ばかりが注目される傾向にあるが，技術的セキュリティ対策は強化すればするほど費用がかさみ，時には利便性が悪化する場合もある。従って，技術的対策だけでなく，制度的な対策も強化し，両方でバランスの良い対策をとることが重要である。本検討では各ユースケースから抽出した番号制度の民間利用における脅威に対してセキュリティ要件を定義し，その要件に対して技術的面と制度面の両面からセキュリティ対策を検討する。

4.1 セキュリティ要件

3 章にて，番号制度の民間利用における脅威とその脅威の攻撃手法が洗い出された。特に攻撃手法がわかれば，その攻撃を成功させない為の要件を導くことができる。故に本検討では，3 章で洗い出した結果から，それらの脅威に対抗する為のセキュリティ要件を導いた。以下にその結果を記す。**R1**〜**R23** が導かれたセキュリティ要件である。

T1-1 悪意の第三者による情報漏洩に対するセキュリティ要件
R1 第三者からの不正アクセスを防止できること
R2 成りすましを防止できること（本人性を証明できること）
R3 本人または本人が許可した者以外は利用できないこと
R4 個人番号カード紛失等の際，カード利用を停止できること
R5 保護対象資産が管理されている DB から漏洩しないこと
R6 保護対象資産がネットワークから漏洩しないこと
R8 万一危害があった場合，可能な限り補償がされていること
T1-2 悪意の第三者による情報改竄に対するセキュリティ要件
R1 第三者からの不正アクセスを防止できること
R2 成りすましを防止できることと（本人性を証明できること）
R3 本人または本人が許可した者以外は利用できないこと
R4 個人番号カード紛失等の際，カード利用を停止できること
R7 保護対象資産の改竄を検知できること
R8 万一危害があった場合，可能な限り補償がされていること
T1-3 個人番号をキーとした名寄せに対するセキュリティ要件
R20 個人番号と基本/関連情報とは，分割管理されていること（個人番号漏洩がダイレクトに個人情報漏洩に繋がらないこと）
T1-4 匿名化データからの個人推定に対するセキュリティ要件
R21 データを二次利用する際，データが匿名化されていること
R22 複数の匿名化データを集めても個人が推定できないこと
T2-1 権限保有者による情報漏洩に対するセキュリティ要件
R9 提供サービスを利用できる組織人を認定できること
R10 権限保有者を認証できること
R11 権限保有者の役割 (ロール) を定義できること
R12 必要最小限のデータを除き，秘匿 (暗号化) すること
R17 権限保有者の誤操作が起きにくい仕組みにすること
R8 万一危害があった場合，可能な限り補償がされていること
T2-2 権限保有者による情報改竄に対するセキュリティ要件
R9 提供サービスを利用できる組織人を認定できること
R10 権限保有者を認証できること
R11 権限保有者の役割 (ロール) を定義できること
R17 権限保有者の誤操作が起きにくい仕組みにすること
R7 保護対象資産の改竄を検知できること
R8 万一危害があった場合，可能な限り補償がされていること
T2-3 個人番号をキーとした名寄せに対するセキュリティ要件
R20 個人番号と基本/関連情報とは，分割管理されていること（個人番号漏洩がダイレクトに個人情報漏洩に繋がらないこと）
T2-4 匿名化データからの個人推定に対するセキュリティ要件
R21 データを二次利用する際，データが匿名化されていること
R22 複数の匿名化データを集めても個人が推定できないこと
T2-5 権限保有者による目的外利用に対するセキュリティ要件
R13 権限保有者が行った処理を確認できること
R14 権限保有者の目的外利用を抑止できること[3]
R15 本人又は第三者により自己に関する情報を確認できること
R16 権限保有者の不正行為に対して罰則があること
T2-6 本人の許可なしでの情報流通に対するセキュリティ要件
R18 本人の許可なしで情報が流通しないこと
R19 本人が承諾していることを証明できること
T3-1 情報消失等でサービス不履行に対するセキュリティ要件
R23 バックアップがとられていること

4.2 セキュリティ対策

セキュリティ技術の進歩により，今日では様々な技術的対策が存在する。これらセキュリティ技術に

[3]医療分野ユースケースの緊急を要する場合については要検討

表 4: 技術的対策の概要

攻撃を防止する対策	効果
C1 端末認証, C2 ユーザ認証, C3 アクセス制御	利用者を認証し，成りすましを防止することができる。悪意の第三者等から保護対象資産への不正アクセスを防止することができる。
C4 通信路の暗号化	ネットワークを流れる情報の盗聴をを防止することができる。
C5 自己情報コントロール技術 C6 本人の承諾による処理技術	本人に関わる情報を本人がコントロールし，本人了承なしの情報流通を防止することができる。
C7 複数人による操作	権限保有者単独での誤操作を防止することができる。
C8 匿名化技術	データの二次利用の際，匿名化により個人推定ができないようにすることができる。
攻撃を抑止する対策	**効果**
C9 アクセスログ管理 C10 マイ・ポータル技術	権限保有者による目的外利用を抑止する為に，権限保有者が行った処理をログとして管理する。また，国民自身が本人に関する情報に対し権限保有者が行った処理を確認することができる
被害を最小化する対策	**効果**
C11 蓄積データの暗号化 (保護対象資産の暗号化)	万が一，第三者が保護対象資産にアクセスできた場合でも，データ自身を暗号化することで情報漏洩を防止することができる。
C12 電子署名	万が一，保護対象資産を書き換えられた場合でも改竄を検知し，改竄されたことを証明することができる。
C13 ロールベース アクセス制御	各権限保有者のアクセス権限をロールに応じた必要最低限のものとし，権限以上の不正アクセスを防止することができる。
C14 カード失効・再発行	新たな個人番号を発行する仕組みを整備し，問題の発生した個人番号を無効化することができる。
C15 分散管理技術	クレジットカード仕様の PCIDSS [5] が推奨している様に，個人番号と基本情報・関連情報とを分割管理することで万が一，情報流出した時に被害を最小化することができる。
C16 バックアップ技術	複製をあらかじめ作成し，例え問題が起きてもデータを復旧できるように備えておく。

表 5: 制度的対策の概要

制度的対策	効果
C17 第三者認定機関 ・監査機関の設置	個人番号を利用する組織を認定する機関及び，個人番号を利用する組織を監査する機関を設置する。 これにより番号制度に則った正しい運用を実現できる。
C18 認定制度策定	番号制度を利用することを認められた組織・人を認定する制度を策定する。これにより闇金融など，不特定多数の組織への番号提供および情報提供を防止することができる。
C19 監査制度策定	認定制度が正しく運用されているかを監査する監査制度を策定する。 個人番号の目的外利用等の履歴を監査することで権限保有者による目的外利用を抑止することができる。
C20 罰則制度策定	権限保有者が不正（目的外利用，情報漏洩等）を行った場合の罰則規定を策定。これにより不正に対する抑止効果が期待できる。
C21 補償制度策定	番号制度に関連し情報管理側の不備により被害（金銭被害，情報漏洩）が生じた場合の補償規定を策定。 これにより，国民は万が一の被害に対して補償を受けることができる。
C22 不正アクセス禁止法 平成 11 年 8 月 13 日法律 128 号	インターネット等のコンピュータネットワークでの通信において不正アクセス行為とその助長行為を規制。
C23 個人情報保護法 平成 15 年 5 月 30 日法律 57 号	個人情報を個人情報データベース等として所持している事業者に対し，主務大臣への報告やそれに伴う改善措置に従わない等，適切な対処をしなかった場合に刑事罰が科される。

よる対策は，主に「攻撃を防止することを目的とした技術」「抑止効果を狙った技術」「被害を最小化するための技術」の 3 つに大別することができる。また，制度的な対策は，より安心安全な番号制度を実現する為に技術的な対策を補完するものである。本検討では，上記観点の基，主要な技術的対策と制度的対策を整理し，4.1 節で挙げた要件を満たす為のセキュリティ対策について検討を行った。以下，技術的対策と制度的対策の概要をそれぞれ表 4,5 に纏める。また，表 6 にて 4.1 節で挙げたセキュリティ要件と表 4,5 のセキュリティ対策との関係を示す。

5 安心安全な番号制度の民間利用の実現に向け，さらに検討すべき技術的対策と制度的対策

表 6 から分かるように，悪意ある第三者からの不正アクセス等による情報漏洩，情報改竄に関する脅威 (R1～R7) は，現在確立されている技術的・制度的対策により概ね対抗することができる。しかし，権限保有者による目的外利用や本人の許可なしでの情報流通に関する脅威 (R13～R19) に関しては，必ずしも対策が確立されているとは言えず，それが国民の不安につながっていると考える。また，個人番号を騙った成りすましによる脅威 (R2,R3) や匿名化データによる個人推定の脅威 (R21,R22) も個人番号を民間利用した個人情報利活用の特徴的な脅威であり，現在のセキュリティ対策で十分とはいいきれない。それ故，安心安全な番号制度の民間利用の実現に向けて，以下のセキュリティ対策の検討を深めることが重要と考える。

【権限保有者による目的外利用に対するセキュリティ対策（R13～R17）】

権限保有者の認証などは現在の技術で確立できるが，権限保有者による目的外利用や誤操作による脅

表 6: 技術的対策と制度的対策の概要

要件	現在確立されている対策		さらに検討すべき対策	
	技術的対策	制度的対策	技術的対策	制度的対策
R1	C2,C3	C22		
R2	C2		C2	
R3	C2		C2	
R4		C14		
R5	C11	C23	C11	
R6	C4	C23		
R7	C12			
R8				C21
R9	C2			C18
R10	C1,C2			
R11	C13			
R12	C11	C23	C11	
R13			C9	
R14		C23	C7,C9	C19,C20
R15			C10	C19
R16				C20
R17			C7	C21
R18		C23	C5,C6	
R19				C19
R20	C15			
R21	C8		C8	
R22	C8		C8	
R23	C16			

威が残っている。権限保有者による目的外利用を抑止する為には，利用履歴を記録していることを知らせることが効果的である。それには対象となるシステムに対して，どのようなログを取得管理すべきかを検討し，権限保有者が行った処理を確認できる仕組みが必要である。また，権限保有者による不正がないことを国民に証明するために，第三者監査機関を設置し，第三者による監査を行うことが重要である。また，第三者による監査だけでなく，国民自身が自己の情報に関する処理を確認できる仕組みを確立することで，国民が安心して番号制度を利用できるようになる。このような仕組みは，本人に関する情報を集約したサイト,「マイ・ポータル」をインターネット上に設け，個人情報が利用された履歴を自身で把握できるようにすることで実現できる。しかし，このようなマイ・ポータルを設置するだけでは，自分の情報が目的外利用されていないかどうかを国民が日々チェックしなければならず，国民にとって負担となる可能性がある。それ故，自動的に目的外利用の疑いがある処理を監視し，その結果を本人に通知する仕組みなども考慮されるべきと考える。主な検討課題を以下に示す。

- 第三者監査機関の設立，監査制度の策定
- 監査用ログの取得・管理方法の検討
- 権限保有者の不正行為に対する罰則制度の策定
- 国民自身が個人情報の利用履歴を確認できるマイ・ポータル技術の確立（自動的に目的外利用の疑いがある処理を監視し，その結果を本人に通知する仕組みを含む）
- 万が一の被害に対する補償のあり方の検討

【本人の許可なしでの情報流通に関する脅威に対するセキュリティ対策（R18，R19）】

国民は，本人の知らないところで自分の情報が流通することに対して不安を抱いている。それ故，本人の許可なしでは情報流通ができない仕組みについて検討する必要がある。また，サービス提供者側の説明の不備で，よく分からないうちに承諾してしまうケースも考えられる。「国民は何に対して了承したのか？」,「承諾しなければどうなるのか？」,「紙面による承諾書か？電子による承諾システムか？」など，どのようにして本人が承諾したのかを証明できるような制度設計が必要である。一方，本人の許可なしで情報が流通することは問題ではあるが，医療分野ユースケースにおける緊急を要する場合のように，本人の承諾なしで診療記録を連携できる仕組みについても検討が必要である。したがって，このような例外のケースも考慮し，柔軟な制度設計をすることが重要である。主な検討課題を以下に示す。

- 国民自身が自己の情報を管理できる自己情報コントロール技術の確立
- 本人の承諾による処理方法の検討及び制度設計
- 例外処置の検討

【悪意の第三者による脅威（個人番号を騙った成りすましによる脅威）に対するセキュリティ対策（R2～R5）】

番号制度の民間利用において，本人が個人番号を提示して各サービスを受ける場合がある。その際，成りすましなど第三者による不正を防止する為に，本人が本人であることを証明することが重要になってくる。現在，IC カード等の認証技術を用いて本人確認をすることができるが,「IC カードインフラのない場所での使用はどうするのか？」,「IC カードが盗難された場合どうなるのか？」「万が一，成りすましによる被害があった場合，どうなるのか？」など国民が不安に感じる課題が残されている。また，本人確認方法を IC カードによる認証ではなく，携帯電話などを用いて認証する方法も考えられる。番号制度の利便性向上の為，それらのデバイスでの本人確認方法についても今後検討する必要がある。主な検討課題を以下に示す。

- カード運用ガイドラインの策定（カード失効再発

行の手順およびカード利用方法の確立）
● カードインフラのない場所での本人確認方式
● 携帯電話等，他のデバイスを用いた本人確認方式
● 万が一の被害に対する補償のあり方の検討

【匿名化データによる個人推定の脅威に対するセキュリティ対策（R21〜R22）】

医療分野ユースケース（PHR 二次利用）に見られるように，個人情報を統計情報として扱う場合もある。このように個人情報を集め統計情報として利用する場合，収集された情報から個人が推定されないように匿名化処理を施すことが重要である。また，名前や住所等，直接個人を特定する情報を削除しても，そこに含まれる情報を分析することで個人を推定できてしまっては，匿名化の意味を成さない。それ故，たとえ複数の匿名化情報が集まっても個人を推定できないような匿名化技術が望まれる。主な検討課題を以下に示す。

● 匿名化方式の検討
● 複数の匿名化情報が集まっても個人を推定できないような匿名化技術

【その他特記すべきセキュリティ対策 (R12)】

個人情報や企業情報の民間活用に関する新たな情報漏洩対策として，蓄積データの完全なエンドツーエンド暗号化（プロキシ再暗号化技術など）が必要となってくる。通常，情報漏洩対策としてはデータの暗号化が一般的であるが，医療連携や PHR 一次利用等では，現在普及している暗号技術だけでは要件を満たさない。医療連携や PHR 一次利用では，診療情報等を暗号化して医療情報を管理する機関で管理し，必要に応じて診療情報を復号して利用することを想定しているが，暗号化する時点では，その診療情報等を次に利用する病院や医師等は決まっていない。つまり，通常の暗号化技術は，相手の暗号化鍵で暗号化し情報共有をするが，医療連携や PHR 一次利用等では，次にそれらの診療情報を利用する相手が決まっていない為，診療情報を暗号化するための暗号化鍵を定めることができない。それ故，最終利用者が予め決まっていなくても，医療情報管理機関等で診療情報等が復号されることなく，最終利用者に暗号化データを送付することが可能な暗号化技術（プロキシ再暗号化技術など）が必要となってくる。主な検討課題は以下である。

● プロキシ再暗号化技術（暗号化したままで別の復号鍵に付け替えられる技術）

6 まとめ

本論文では，政府検討の番号制度とは別に仮の番号制度 (以下，個人番号と称する) を想定し，医療，金融，製品安全の分野でのユースケースを基に，課題とその課題を解決する為の技術的・制度的対応策を纏めた。具体的には 5W1H 法を用いて，各ユースケースにおける脅威分析を実施し，各ユースケースにおいて，保護対象資産及びその管理場所，脅威の主体者，サービスシーン等により，様々な脅威が存在することが分かった。更に我々はそれらの脅威に対して，セキュリティ要件を導き出し，技術的面と制度面の両面から対策を纏めた。また，安心安全な番号制度の民間利用の実現に向けさらに深堀すべき技術的対策と制度的対策を検討した。

参考文献

[1] 社会保障・税に関わる番号制度, 内閣官房, http://www.cas.go.jp/jp/seisaku/bangoseido/index.html

[2] 社会保障・税番号大綱, 政府・与党社会保障改革検討本部, http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/honbun.pdf

[3] 個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備プロジェクト, 産業競争力懇談会, http://www.cocn.jp/common/pdf/thema30.pdf

[4] 共通番号制度の早期実現に向け 民本位の社会基盤づくり, 国際公共政策研究センター共通番号制度に関する研究会, http://www.cipps.org/img/news/100701/ID number proposals.pdf

[5] PCIDSS, PCI Security Standards Council, https//www.pcisecuritystandards.org/

１２．付録２　情報処理学会コンピュータセキュリティ研究会：コンピュータセキュリティシンポジウム 2011(CSS2011)　発表資料

個人情報や企業情報を安全に活用する為のクラウドコンピューティング基盤の整備

産業競争力懇談会（COCN）

株式会社　日立製作所
坂崎 尚生

1

目次

1. 産業競争力懇談会（COCN）について
2. 番号制度の民間活用について
3. 番号制度の民間活用における脅威分析
4. 安心安全な情報利活用の為のセキュリティ対策
5. 更に検討すべき技術的対策と制度的対策
6. まとめ

2

1. 産業競争力懇談会（COCN）について

■目的

日本の産業競争力の強化に深い関心を持つ産業界の有志により国の持続的発展の基盤となる産業競争力を高める為、科学技術政策、産業政策などの諸施策や官民の役割分担を産官学協力のもと、合同検討により政策提言として取り纏め、関連機関への働きかけを行い、実現を図る活動を行っている

詳しくは
COCN 検索

■2011年度推進テーマ

【継続テーマ】
- 個人情報や企業情報を安全に活用する為のクラウドコンピューティング基盤の整備
- 微細藻類を利用した燃料の開発
- 都市づくり・社会システム構築
- 企業活動と生物多様性

【新規テーマ】
- 災害対応ロボットと運用システムのあり方
- 次世代医療システム
- 半導体戦略「産業競争力強化の為の先端研究開発」
- 希少金属の安定確保に向けた資源循環システム
- グローバルもの（コト）づくり
- グローバルなリーダー人材の育成と活用
- 強靭な（Resilient）社会システムと産業の構築
- HPC（High Performance Computing）の応用

1. 産業競争力懇談会（COCN）について

■本プロジェクトの活動

個人情報や企業情報を安全に活用する為のクラウド基盤を整備する際に解決しなければならない課題（特に番号制度の民間活用）について検討した。

■本プロジェクトに関連する国内外の調査
■実現されるサービスの検討
- 医療分野、製品安全分野、金融分野における情報利活用のユースケースの検討

■番号制度に関する検討
- 番号の対象者、保持期間、番号の表現形式、利用方法、付番方法などの検討

■セキュリティに関する検討
- 番号制度を民間に拡げていく上でのセキュリティ課題とその対策についての検討

■法律・制度に関する検討
- 番号制度を民間に拡げていく上で必要となる規制緩和などについての検討

クラウドコンピューティング基盤整備のために必要となる提言

■体制図

2. 番号制度の民間活用について

■背景

- 2011年6月30日、与党社会保障改革検討本部より社会保障・税番号大綱(案)が公示
- 上記番号制度は社会保障・税分野で利用することを目的とした制度であり、民間活用への検討は現段階では先送り
- COCNでは、番号を民間でも活用できれば、より便利にする新たなサービスを生み出し、国民の生活が豊かになり、また企業活動が効率化できると考え、個人情報や企業情報を安全に活用する為のクラウドコンピューティング基盤を検討
- 個人情報等を安全に活用する為の基盤として番号制度が広く民間にも利用される為にはセキュリティが重要と考え、基盤の構築・運用に関して、脅威分析を行い、セキュリティ対策を検討
- 本論文(発表)では番号制度の民間活用にターゲットを絞り、政府検討の番号制度における議論との混同を避ける為、政府検討の番号制度とは別に仮の番号制度(以下、個人番号と称する)を想定し、医療、金融、製品安全の分野でのユースケースを基に課題を検討

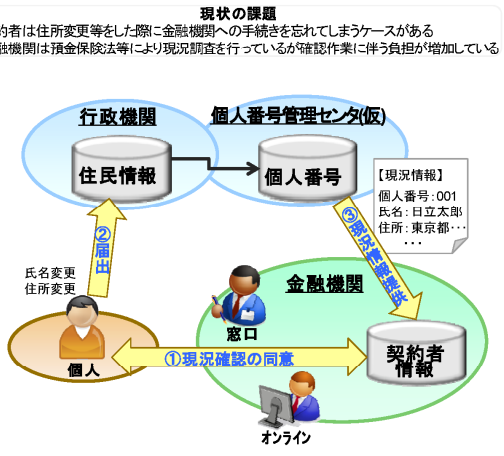
5

2. 番号制度の民間活用について

■ユースケース

本検討では番号制度を民間利用した際、利便性が高く国民の生活が豊かになると思われる、医療、金融、製品安全の3分野を例に挙げ、10個のユースケースを設定

医療分野	医療連携サービス
	PHR一次利用サービス
	PHR二次利用サービス
金融分野	本人確認サービス
	現況確認サービス
	各種証明書手続きサービス
製品安全分野	製品リコールサービス
	事故未然防止サービス
	保守継続性サービス
	製品リコールにおける品質管理・保障サービス

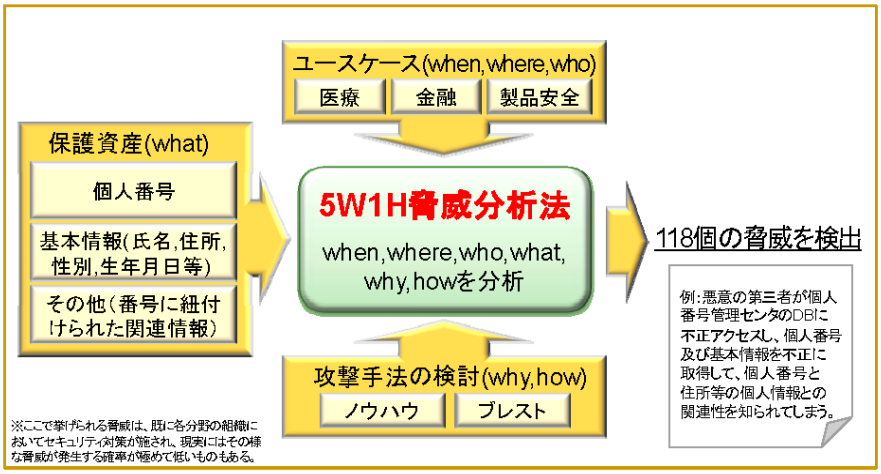


【金融分野:現況確認サービスイメージ】

3. 番号制度の民間活用における脅威分析

■脅威分析手法

・5W1H脅威分析法にて各ユースケースに対して脅威分析を実施（118個の脅威を検出）



3. 番号制度の民間活用における脅威分析

■各ユースケースにおける脅威分析

・抽出した118個の脅威を、脅威の主体者により大別

・更に詳しく、攻撃手法や被害の種類などから体系的に分類

T1:悪意の第三者による脅威
- T1-1:悪意の第三者による情報漏洩
- T1-2:悪意の第三者による情報改竄
- T1-3:個人番号をキーにした名寄せ
- T1-4:匿名化データからの個人推定

T2:権限保有者による脅威
- T2-1:権限保有者による情報漏洩
- T2-2:権限保有者による情報改竄
- T2-3:個人番号をキーにした名寄せ
- T2-4:匿名化データからの個人推定
- T2-5:権限保有者による目的外利用
- T2-6:本人の許可なしでの情報流通

T3:その他の脅威
- T3-1:情報の劣化・消失によるサービス不履行

8

3. 番号制度の民間活用における脅威分析

■脅威と攻撃手段

・脅威分析結果より、分類した脅威がどのように発生するのか攻撃手法を整理

脅威	攻撃手段(how)
T1-1:悪意の第三者による情報漏洩	不正アクセス，成りすまし，ネットワーク盗聴等
T1-2:悪意の第三者による情報改竄	不正アクセス，成りすまし等
T1-3:個人番号をキーとした名寄せ	番号をキーとした情報収集等
T1-4:匿名化データからの個人推定	データ分析等
T2-1:権限保有者による情報漏洩	不正な情報持出し，誤操作等
T2-2:権限保有者による情報改竄	不正な情報処理，誤操作等
T2-3:番号をキーとした名寄せ	番号をキーとした情報収集等
T2-4:匿名化データからの個人推定	データ分析等
T2-5:権限保有者による目的外利用	不正な情報処理等
T2-6:本人の許可なしでの情報流通	不正な情報処理等
T3-1:情報消失等でサービス不履行	天災等によるデータの消滅等

4. 安心安全な情報利活用の為のセキュリティ対策

■セキュリティ要件

・洗い出した脅威に対抗する為のセキュリティ要件を導出(23要件)

（攻撃手法がわかれば、その攻撃を成功させない為の要件を導くことが可能）

T1-2悪意の第三者による情報改竄に対するセキュリティ要件

- R1　第三者からの不正アクセスを防止できること
- R2　成りすましを防止できること（本人性を証明できること）
- R3　本人または本人が許可した者以外は利用できないこと
- R4　個人番号カード紛失等の際，カード利用を停止できること
- R7　保護対象資産の改竄を検知できること
- R8　万一危害があった場合，可能な限り補償がされていること

T2-5権限保有者による目的外利用に対するセキュリティ要件

- R13　権限保有者が行った処理を確認できること
- R14　権限保有者の目的外利用を抑止できること
- R15　本人又は第三者により自己に関する情報を確認できること
- R16　権限保有者の不正行為に対して罰則があること

T2-6本人の許可なしでの情報流通に対するセキュリティ要件

- R18　本人の許可なしで情報が流通しないこと
- R19　本人が承諾していることを証明できること

10

4. 安心安全な情報利活用の為のセキュリティ対策

■セキュリティ対策

・導き出したセキュリティ23要件に対し、主要な技術的対策と制度的対策を整理

セキュリティ要件		現在考えられるセキュリティ対策		さらに検討すべきセキュリティ対策	
		技術的対策	制度的対策	技術的対策	制度的対策
R1	第三者からのアクセスを防止できること	ユーザ認証, アクセス制御	不正アクセス禁止法		
R2	成りすましを防止できること	ユーザ認証		本人確認方式の高度化	
R3	本人または本人が許可した者以外は利用できないこと	ユーザ認証		本人確認方式の高度化	
R4	カードの盗難・紛失の際、カード利用を停止できること		カード失効・再発行		ガイドライン策定
R5	保護対象資産が管理されているDBから漏洩しないこと	蓄積データの暗号化	個人情報保護法	ｴﾝﾄﾞﾂｰｴﾝﾄﾞの暗号化	
R6	保護対象資産がネットワークから漏洩しないこと	通信路の暗号化	個人情報保護法		
R7	保護対象資産の改竄を検知できること	電子署名			
R8	万が一の場合、補償がされていること				補償制度策定
R9	提供サービスを利用できる組織・人を認定できること	ユーザ認証			認定制度策定
R10	権限保有者を認証できること	端末認証、ユーザ認証			
R11	権限保有者の役割(ロール)を定義できること	ロールベースアクセス制御			
R12	必要最小限のデータを除き、秘匿（暗号化）すること	蓄積データの暗号化	個人情報保護法	ｴﾝﾄﾞﾂｰｴﾝﾄﾞの暗号化	
R13	権限保有者が行った処理を確認できること			アクセスログ管理	
R14	権限保有者の目的外利用を抑止できること		個人情報保護法	アクセスログ管理 複数人による操作	監査制度策定、 罰則制度策定
R15	本人または第三者により、自己情報を確認できること			マイポータル技術	監査制度策定
R16	権限保有者の不正行為に対して罰則があること				罰則制度策定
R17	権限保有者の誤操作が起きにくい仕組みにすること			複数人による操作	補償制度策定
R18	本人の許可なしでは情報が流通しないこと		個人情報保護法	自己情報ｺﾝﾄﾛｰﾙ技術 本人承諾処理技術	
R19	本人が承諾していることを証明できること				本人承諾制度の設計
R20	個人番号と他の情報が分割管理されていること	分割管理技術			
R21	個人が特定されないように匿名化すること	匿名化技術		匿名化技術の高度化	
R22	複数の匿名化データを集めても個人が推定できないこと	匿名化技術		匿名化技術の高度化	
R23	バックアップがとられていること	バックアップ技術			

手薄と考えている範囲

5. 更に検討すべき技術的対策と制度的対策

■権限保有者による目的外利用に対するセキュリティ対策(R13～R17)

・利用履歴を記録していることを権限保有者に知らせることが効果的
・監査用ログの取得・管理方法の検討(権限保有者が行った処理を確認できる仕組)
・第三者監査機関の設立、監査制度の策定(不正がないことの証明)
・国民自身が個人情報の利用履歴を確認できる技術の確立(マイ・ポータル※1)

■本人の許可なしでの情報流通に対するセキュリティ対策(R18,R19)

・国民自身が自己の情報を管理できる技術の確立（自己情報コントロール技術）
・本人の承諾による処理方法の検討および制度設計（オプトイン方式※2）

■その他特記すべきセキュリティ対策

・大規模災害時など、ｶｰﾄﾞｲﾝﾌﾗのない場所での本人確認技術(R2～R5)

※1 この様な利用履歴を確認できるポータルサイトを設置するだけでは，自分の情報が目的外で利用されていないかを日々チェックしなければならず，国民にとって負担となる可能性がある。
それ故，自動的に目的外利用の疑いがある処理を監視し，その結果を本人に通知する仕組みなども考慮されるべきと考える

※2 一方，本人の許可なしで情報が流通することは問題ではあるが，医療分野において緊急を要する場合など，本人の承諾なしで診療記録を連携できる仕組みについても考慮し，柔軟な設計をすることも重要と考える。

12

6. まとめ

■政府検討の番号制度とは別に仮の番号制度を想定し，医療，金融，製品安全分野でのユースケースを基に5W1H脅威分析法を用いて脅威分析を実施

■洗い出された脅威を体系的に纏め、各々の脅威に対しセキュリティ要件を導出

■各セキュリティ要件に対し技術的面と制度面の両面からセキュリティ対策を検討

■安心安全な番号制度の民間利用の実現に向け、さらに深堀すべき技術的対策と制度的対策を整理

■COCNでは、上記深掘りすべき対策について継続検討中

13

産業競争力懇談会（ＣＯＣＮ）

東京都千代田区丸の内一丁目６番６号　〒100-8280
日本生命丸の内ビル（株式会社日立製作所内）
Tel：03-4564-2382　Fax：03-4564-2159
E-mail：cocn.office.aj@hitachi.com
URL：http：//www.cocn.jp/
事務局長　中塚隆雄