

厚生労働科学研究費補助金（安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究事業）

分担研究中間報告書

産業保健医療に関わる個人情報管理の実施方策の調査・検討

研究分担者 八幡勝也 産業医科大学産業生態科学研究所作業病態学 准教授

研究要旨

H20年度より始まった特定健診・特定保健指導は、従来の定期健康診断とその事後措置という、安全衛生行政の枠組みから大きく広がった。また、PHR(Personal Health Record)の検討が行われており、さらに取り扱う機関が広がる可能性が高くなった。

そこで、企業と従業員の個人情報の関係について考察した。

企業における従業員の個人情報については、幾つかの指針が出されているものの法的な裏付けはない。今後、雇用契約の一環に盛り込む必要がある。

A. 研究目的

2008年4月に始まった、特定健診・特定保健指導を機に、従来では産業保健の健康情報とは関係の無かった機関との情報連携が課題となる。特に、個人情報保護に関しては、産業保健は異なる法体系となっているために、注意が必要である。本調査ではその課題の基礎情報を整理した。

B. 研究方法

産業保健の健康情報を関連する機関で利用する際の、起業における個人情報保護の関わりについて調査した。

C. 研究結果および考察

産業保健の特殊性

産業保健は、通常の医療とは異なり、医療行為を中心とした業務よりは企業活動の基盤やリスクマネジメントの面が強い。よって、健康診断も通常の医療関係者が考えるような個人健康管理よりは、事業主の業務遂行のために行われる。

産業保健業務の4管理1教育

産業保健業務は、総括管理、作業管理、作業環境管理、健康管理、健康教育の4管理1教育に整理される。この内、健康診断は、健康管理の一貫として行われる。しかし、健康診断の主目的は、生活習慣病のような個人の疾病管理ではなく、事業主が従業員の健康状況を把握し、必要があれば配置転換や休養などの措置を講じるためである。

つまり、事業主の安全衛生配慮義務を遂行するためである。また、従業員個人は個人の責任において自己の健康を管理する義務がある。よって、個人健康指導もその点を配慮して実施することとなる。

そのために、業務による従業員への影響の検討が中心で、有害業務・過重労働対策の一環として健康診断の情報が使われる。

従業員個人に対しては、業務との関連して適正業務、適正配置が主体となり、次いで個人健康指導となる。また、効率性からも集団での健康教育が主体となる。

使用者の安全衛生配慮義務

労働者が労務提供のため設置する場所、設備もしくは器具等を使用し又は使用者の指示のもとに労務を提供する過程において、労働者の生命及び身体等を危険から保護するよう配慮すべき義務を負っている。

健康診断については、事業所単位で結果の集計の報告義務がある。

労働者の自己保健義務

労働者自身が自己の健康を管理し、その保持を図り、使用者の行う健康管理措置に協力して、債務の本旨に従った心身ともに完全な労務を提供するために自己の健康状態の維持を図っていく義務。

健康情報管理の動向

次に産業保健関連で従業員健康情報に関する勧告やガイドラインを列挙する。

従業員の健康情報管理に関する国際的動向

1992年国際労働衛生委員会(ICOH)「産業保健専門職の倫理コード」

1996年国際労働機関(ILO)「労働者個人情報の保護実施要項」

1998年「労働者の健康サーベイランスのための技術・倫理ガイドライン」

いずれも、労働者の個人情報である健康情報の取り扱いを医療職に限定し、非医療職は医療内容に立ち入らないことを勧めている。

産業保健の専門家集団であるロンドン王立内科医会産業医部会の「産業医の倫理ガイドライン」では、

「個人の健康情報は守秘義務が保たれる現職の産業保健専門職に直接手渡されて保管されるべきである。この性質の医学記録は、人事担当者や

他の非医療関係の部門で扱われたり保管されたりしてはならない。」とあり、

こちらでも従業員の健康情報の保管・管理は医療職が行うべきであるとしている。

日本国内

2000年「労働者の健康情報に係わるプライバシー保護に関する検討会」中間報告

2000年「労働者の個人情報保護に関する行動指針」

2004年「労働者の健康情報の保護に関する検討会報告書」

2004年「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について」

基本的に医療職による管理を勧めている。

しかし、法令上産業医の選任の義務のない中小事業場においては、企業内での取り扱いに一定のルールを明確にすることを求めている。

従業員の健康情報

企業における従業員の個人情報は個人情報保護法での個人情報取り扱い事業者の扱いとは異なる。

厚生労働省から2004年に「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針について」と「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項」が出されて、個人情報としての管理が明確となった。

健康診断結果情報に関する矛盾

安全配慮義務があるので、事業主は健康診断結果に基づいた、配置転換や休養を指示しなければならない。

↑↓

健康情報はセンシティブな個人情報であるので、事業主にも開示されるべきではない。

→産業保健スタッフが仲介する

関係機関・スタッフ

事業所の医療職特に産業医

厚生労働省、安全衛生法における定期健康診断等に関する検討会報告書、2007.3

厚生労働省、労働者の健康情報の保護に関する検討会報告書、2004年9月

産業保健専門職の倫理コード、2002年

労働者個人情報の保護実施要項、ILO 労働者のための技術・倫理ガイドライン/労働者個人情報の保護実施要項、P65、労働基準調査会、1999年

ILO 労働者のための技術・倫理ガイドライン、ILO 労働者のための技術・倫理ガイドライン/労働者個人情報の保護実施要項、P1、労働基準調査会、1999年

ロンドン王立内科医会産業医部会、産業医の倫理ガイドライン、健康開発科学研究会誌、2001年

健診機関

健診機関は、基本的に医療機関である。よって、通常の医療機関としての個人情報保護が適応される

厚生労働省、医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン、2004年12月

医療保険者

厚生労働省、健康保険組合等における個人情報の適切な取扱いのためのガイドライン、2004年

厚生労働省、国民健康保険組合における個人情報の適切な取扱いのためのガイドライン、2005年

代行機関

厚生労働省告示第百七十九号、特

定健康診査及び特定保健指導の実施に関する基準第16条第3項の規定に基づき厚生労働大臣が定める者

事業運営上開示すべき重要事項の概要

2 特定健康診査及び特定保健指導の結果等の情報の取扱いに関する基準

(1) 代行業務を行うに当たっては、法第30条に規定する秘密保持義務を遵守すること。

(2) 個人情報の保護に関する法律（平成15年法律第57号）及びこれに基づくガイドライン等を遵守すること。

(3) 電子情報処理組織（代行業務を行う者が使用する電子計算機（入出力装置を含む。以下同じ。）と保険者が使用する電子計算機及び実施機関が使用する電子計算機とを電気通信回線で接続した電子情報処理組織をいう。以下同じ。）により代行業務を行う場合には、電子情報処理組織の使用に係る安全管理（組織的、物理的、技術的、人的な安全対策等）を徹底すること。

アウトソーシング機関

標準的な健診・保健指導プログラム

第6章保健指導の実施に関するアウトソーシング

(3) 保健指導アウトソーシングの留意事項

8) 個人情報の管理

保健指導は対象者の生活そのものを把握することになり、その情報は個人として知られたくない情報であることもある。このため、保健指導を行った場合の記録の漏洩防止や、保健指導実施者に守秘義務をかけるなど、個人情報の管理が重要である。アウトソーシングを行う場合は、事業者がこのような規定を有しているか確認するとともに、情報の管理状況を定期的に確認する必要がある。

○ 個人情報については、その性格と重要性を

十分認識し、適切に取り扱われなければならない、特に、医療分野は、「個人情報の保護に関する基本方針」等において、個人情報の性質や利用方法等から、特に適正な取扱いの厳格な実施を確保する必要がある分野の一つとされており、委託先の事業者は個人情報を適切に取り扱わなければならない。なお、保健指導の記録等の情報を取り扱う業務のみを委託する場合にも、委託先の事業者は2)④に定める保健指導の記録等の情報の取扱いに関する基準を遵守することが求められる。

E. 結論

健康分野においては従来の企業、従業員、健診機関といった単純な構図ではなく、保険者、保健指導受託事業者などの非医療機関の関与が広がる可能性が高い。

これらの機関で健康情報を取り扱う際には、管理責任と利用責任の分離の教育が必要である。

それには、健康情報を取り扱うための組織体および運用の取り決めが必要となる。特に複数の機関で情報の共有を検討する際には、その機関の特性と利用形態にを診査する必要がある。

F. 健康危険情報

特になし

G. 研究発表

1. 論文発表

- 1). 八幡勝也、産業保健と特定健診・特定保健指導、総合臨床、57, 7, 1533-1535, 2008
- 2). 八幡勝也、産業保健での遠隔保健相談ための検討、日本遠隔医療学会雑誌、4, 2, 117-120, 2008

2. 学会発表

- 1) 「産業保健における特定健診・特定保健指導」、シンポジウム1「特定健診と産業保健の情報共有・利用のあり方」、第28回

医療情報連合大会、2008年11月

- 2) 産業保健における個人情報保護、チュートリアル「特定保健指導のシステム」、第28回医療情報連合大会、2008年11月
- 3) 八幡勝也、産業保健のためのリスク記述モデリング、第28回医療情報連合大会、2008年11月
- 4) 八幡勝也、稲田紘、吉田勝美、藤野善久、鹿妻洋之、特定健診と産業保健の情報共有・利用のあり方、第28回医療情報連合大会、2008年11月

H. 知的財産権の出願・登録状況

特になし

参考文献

1. 厚生労働省、安全衛生法における定期健康診断等に関する検討会報告書、2007.3,
<http://www.mhlw.go.jp/houdou/2007/04/h0402-4.html>
2. 標準的な健診・保健指導プログラム,
<http://www.mhlw.go.jp/bunya/kenkou/seikatsu/index.html>
3. 小規模事業所における総合的健康管理の方策に関する調査研究、1996年2月,
http://www.iph.pref.osaka.jp/report/busins96/bsns96_2.html
4. 過重労働による健康障害防止のための総合対策について、2005年3月,
<http://www.mhlw.go.jp/topics/bukyoku/roudou/an-eihou/dl/ka060317008a.pdf>
5. 産業保健専門職の倫理コード、2002年,
http://www.icohweb.org/core_docs/code_ethics_jpn.pdf
6. 労働者個人情報の保護実施要項、ILO労働者のための技術・倫理ガイドライン/労働者個人情報の保護実施要項、P65、労働基準調査会、

1999年

7. ILO 労働者のための技術・倫理ガイドライン, ILO 労働者のための技術・倫理ガイドライン/労働者個人情報の保護実施要項, P1, 労働基準調査会, 1999年

8. ロンドン王立内科医会産業医部会, 産業医の倫理ガイドライン, 健康開発科学研究会誌, 2001年

9. 厚生労働省労働基準局安全衛生部労働衛生課, 労働者の健康情報の保護に関する検討会報告書, 2004年9月,
<http://www.mhlw.go.jp/shingi/2004/09/s0906-3a.html>

10. 厚生労働省労災補償課医療係, 二次健康診断等給付について,
<http://www.roudoukyoku.go.jp/seido/rousai/rousai-2ji.htm>

11. 厚生労働省, 医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン, 2004年12月,
<http://www.mhlw.go.jp/topics/bukyoku/seisaku>

[u/kojin/dl/170805-11a.pdf](http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf)

12. 厚生労働省, 健康保険組合等における個人情報の適切な取扱いのためのガイドライン, 2004年,

<http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161227kenpo.pdf>

13. 厚生労働省, 国民健康保険組合における個人情報の適切な取扱いのためのガイドライン, 2005年,

<http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170401kokuhoh.pdf>

14. 日本産業衛生学会, 衛則改正に関わる省令案の実施に関する要望書について, 2007年7月,
<https://www.sanei.or.jp/#line>

15. 日本産業衛生学会産業医部会, 特定健康診査、特定保健指導に関して、産業医業務における位置づけ、日本産業衛生学会産業医部会としての意見, 2007年6月,

<http://www.on-top.net/ibukai/bukai/kanjikai070627.doc>

電子私書箱と連携した保健医療情報の安全な利活用を促進する
医療情報ネットワーク基盤整備の技術的方策に関する研究
分担研究報告書

医療機関内部における個人情報管理に関する調査・検討

研究分担者 秋山 昌範 (東京大学政策ビジョン研究センター)

研究要旨

医療機関相互の連携を行うために必要な医療機関内部における医療情報管理の実施形態を検討し、医療情報ネットワークによる電子カルテ連携実現に必要な要件を明らかにする。また、ITによる電子認証等を用いて、医療情報へのアクセスコントロールを実施するにあたっての課題を検討した。

本研究では医療機関が提供するサービスの方向性の変化とそれに対応していくための一般的なセキュリティ対策について検討した。本年は、実際に運用が想定される現場調査を行い、法的面と制度的面から検討した。その結果、情報を共有するニーズとプライバシー情報の漏えいの懸念とのトレードオフの問題が指摘された。これは、患者の安全とプライバシーの保護とのバランスの問題と言い換えることもでき、今後の検討が必要と思われた。

A. 研究目的

電子私書箱等の情報共有の仕組みを利用して、医療機関相互の連携を行うために必要な医療機関や介護・福祉機関内部における医療情報管理の実施形態を検討し、医療情報ネットワークによる電子カルテ等の病院内のシステムを連携するための実現に必要な要件を明らかにする。

B. 研究方法

電子私書箱を利用して、医療機関相互に連携するために診療記録の外部保存、保険統計情報の分析および遠隔医療への取り組みは、近い将来にネットワーク型医療サービスの出現が推測されるものである。また、従来は院内で独立・隔離して管理されていた情報が関連組織間で共有化されていくことを意味している。こうした提供サービスの変化は情報保護(セキュリティ)面における詳細なセキュリティポリシーの策定と関連組織間での合意・順守体制が求められることになる。またサービス内容としてリアルタイム性が追求されることにもなり、患者情報の保護だけではなくネットワークシステム全体のセキュリティも検討していく必要があると考える。

これに加え、介護・福祉の現場では、さらに他職種の人材が働いており、守秘義務の規定があいまいな職種やボランティアも含まれてくる。そこで、医療機関において必要となる課題を明らかにする。

(倫理面への配慮)

本研究は、個人情報を扱うものではないので、問題はないと考えられる。

C. 研究結果

1) 医師法上の問題

1. 医師法20条(無診療治療等の禁止)の適用

厚生労働省医政局「情報通信機器を用いた診療(いわゆる「遠隔診療」)について」の一部改正について～医政発第0331020号平成15年3月31日～は十分に機能しているかを検討した。

具体的には、以下の3点である。

- ・患者さんへの説明
- ・テレビ電話利用時における患者さんのプライバシー保護
- ・システムダウンについて患者さんの危険の引き受けを前提としているが、十分に理解されているのか?

2. 医師法17条(医師以外の医業の禁止)の適用問題

在宅の場合、医師だけでなく医師以外のコメディカルの関与も重要であり、遠隔診療だけでなくオンライン・メディカルコントロールの応用も検討課題と思われた。

2) 患者の安全とプライバシーの保護とのバランスの問題

テレビ電話を利用した遠隔診療以外の部分でも、患者のプライバシーの保護のあり方は重要である。

個人情報という形でひとくくりにしないうで、情報の内容やコンテキストを考慮できないかを検討する必要がある。たとえば、「排泄・性」に関連する情報などは、「特定の個人であれば、知ら

れても問題ないが、医療サービスの提供者でも、その他の人には知られたくない」という意見があった。つまり、情報共有するに当たっては、人対人の関係性に依存することが指摘された。

また、現状では、医療現場における各種記録用紙やメモだけでなく、在宅患者宅における申し送りノートなど、定型化されていない紙情報が主たる情報共有手段であった。高度のテクノロジーを駆使することで、服薬等の在宅医療の状態を常時監督しつつ、患者さんとその家族のプライバシーを十分に保護できないかも検討課題に挙がった。

D. 考察

情報提供サービスの変化は、情報保護（セキュリティ）面における詳細なセキュリティポリシーの策定と関連組織間での合意・順守体制が求められることになる。またサービス内容としてリアルタイム性が追求されることにもなり、患者情報の保護だけでなくネットワークシステム全体のセキュリティも検討していく必要があると考える。これは医療・健康分野のシステムが金融系・通信事業系システムと同様のミッションクリティカル性を帯びてきており、体系化されたシステムのセキュリティデザインを確立していくべきである。

さらに、医療情報を連携・ネットワーク化するには、相互運用性を可能にする技術も重要であるが、組織や情報コンテンツの信頼も重要である。この場合、デジタル・フォレンジック技術は、当事者間の信頼関係を確立するためのツールとして役立つ、正確性の証拠となるものである。いわばトラブルとなったときの担保といえる。もし、トラブルの際に証拠能力がないと、そのシステムは担保としての意味をなさない。現状では、医療現場へのフォレンジックの導入に対して否定的な意見もあるが、前述したように施設を超えて連携するためには、施設間に情報の正確性、信頼性がないとその仕組みは活かされない。連携するためには、情報インフラであるネットワークシステムへの信頼のほか、情報源への信頼とコンテンツの信頼のどちらもが必要である。

院内のみならず、病院と病院、病院と診療所間、さらに、在宅医療まで連携するには、在宅医療に対応した電子カルテシステム等の構築が非常に重要な課題になる。在宅での診療では、診療所と異なり、医療従事者が移動する必要があり、診療情報をどのように把握する手段は非常に重要である。診療情報は、情報の正確性を担保する上でも、また2度入力を省く意味でも発生時点での入力が望ましい。また、高齢者への医療はこれまで

の医療のあり方とは異なる異なった性格を持っている。高齢社会においては、横断的な連携が不可欠となってくる。高齢者は、複数の疾患を抱えている場合は多く、複数の診療科やリハビリへの通院は日常的なものである。また、中核病院だけでなく、長期療養型病院や診療所、介護福祉施設、在宅での診療や看護、介護を行う必要があり、相互の情報連携が不可欠となる。診療科や施設の連携が重要な鍵となっている。

今回の研究では、情報共有のニーズはますます高まる一方で、情報漏えいへの危険が懸念され、さらに、医師法20条の問題など、さらに改善すべき問題も散見された。特に、在宅医療では、まだ実用化されておらず、システムダウン対策も不十分と思われた。

これらの課題の解決に有効であると考えられるのが、Web型の電子カルテである。Web型の電子カルテは、ネットワークに接続する環境を整えば、端末を問わず、電子カルテにアクセスすることが可能である。この性質は、在宅での発生時点での情報入力や病診連携において非常に重要である。また、診療所においては、情報化の費用は非常に重荷になるものであるが、Web型の電子カルテであれば、既存の端末の有効利用なども計れるため、費用面からも非常に優れている。しかし、現状ではWeb型の電子カルテは一部の例外を除いてほとんど運用されていない。その理由としては、セキュリティ上の問題点や技術的な問題点などがあげられる。これらを解決するためにも、技術面のみならず、法的・制度的面も研究を進める必要がある。すなわち、電子私書箱等の情報共有の仕組みを利用した保健医療情報の安全な利活用を促進する医療情報ネットワーク基盤整備が求められると考えられた。

E. 結論

医療機関が提供するサービスの方向性の変化とそれに対応していくための一般的なセキュリティ対策について検討した。実際に運用が想定される現場調査を行い、法的面と制度的面から検討した結果、情報を共有するニーズとプライバシー情報の漏えいの懸念とのトレードオフの問題が指摘された。これは、患者の安全とプライバシーの保護とのバランスの問題と言い換えられ、今後の検討が必要と思われた。

F. 研究発表

1. 論文発表

秋山昌範「電子カルテと医療画像データベースの未来」消化器内視鏡 Vol.21 No.7 1-10 2009

秋山昌範「クラウドコンピューティング時代に必要
なデジタル・フォレンジック」日本セキュリティ・
マネジメント学会誌 Vol.23 No.1 61-67
2009

秋山昌範「医療安全における医薬品等のトレーサ
ビリティの役割」医療の質安全学会誌 第4巻第
1号:41-47、2009

小塩篤史・秋山昌範「血液製剤の履歴管理と医療
IT - AIDC(Auto Identification and Data
Capturing)と患者安全・プロセスの可視化」医療
情報学 29(Suppl.) 799-803, 2009

秋山昌範・小笠原克彦・奥田保男・岡崎宣夫「医
療情報が支える医療マネジメント-放射線部門を
例とした情報連携と最適化-」医療情報学
29(Suppl.) 321-323, 2009

Koshio A., Akiyama M. Blood Transfusion and
Patient Safety with IT - Minimizing risk of
transfusion with Point-of-Act-System.
Proceedings of Asia Pacific Medical
Informatics Association 2009:46-53.

2. 学会発表

秋山昌範・中安一幸・古川俊治・佐々木良一 「医
療におけるデジタルフォレンジック」第29回医
療情報学連合大会 29th JCMI (Nov., 2009)

小塩篤史・秋山昌範「血液製剤の履歴管理と医療
IT - AIDC(Auto Identification and Data
Capturing)と患者安全・プロセスの可視化」第
29回医療情報学連合大会 29th JCMI (Nov., 2009)

秋山昌範・小塩篤史 「医療安全における IT の
重要性~特に5つの"Right"について」第29回医
療情報学連合大会 29th JCMI (Nov., 2009)

秋山昌範・小笠原克彦・奥田保男・岡崎宣夫 「医
療情報が支える医療マネジメント-放射線部門を
例とした情報連携と最適化-」第29回医療情報
学連合大会 29th JCMI (Nov., 2009)

Koshio A., Akiyama M. Blood Transfusion and
Patient Safety with IT - Minimizing risk of
transfusion with Point-of-Act-System. Asia
Pacific Medical Informatics Association 2009
Akiyama M. World Alliance for Patient Safety-
Japanese Contribution. Asia Pacific Medical
Informatics Association 2009

秋山昌範 「WHOの医療安全プロジェクトの紹介」
医療の質安全学会 第4回学術総会 2009

秋山昌範 「患者安全のための5つの的確さ-注
射認証システムでの検証」医療の質安全学会
第4回学術総会 2009

秋山昌範・小塩篤史 「注射リスクマネジメント
システムのログデータ解析による注射エラーの

現状・原因分析」医療の質安全学会 第4回学
術総会 2009

小塩篤史・秋山昌範 「注射リスクマネジメント
システムのログデータ解析による注射混注エラ
ーの現状・原因分析」医療の質安全学会 第4
回学術総会 2009

小塩篤史・秋山昌範 「トレーサビリティと患者
安全-電子タグを用いた血液製剤管理」第13
回日本医療情報学会春季学術大会大会 2009

秋山昌範・鈴木明彦・高野長邦・小塩篤史・名和
肇 「血液製剤のトレーサビリティ-電子タグを
用いた血液製剤管理」第57回日本輸血・細胞
治療学会総会 April 2009

G. 知的所有権の取得状況

1. 特許取得
なし。
2. 実用新案登録
なし。
3. その他
なし。

健康情報を利用した遠隔医療の在り方に関する考察

研究分担者 安藤 裕 放射線医学総合研究所 重粒子医科学センター 医療情報課長

研究要旨 健康情報を利用した遠隔医療で問題となるのは、(1) セキュリティと(2) 認証方法である。本研究では、この2点について考察を行った。特に、画像診断の面から問題点を検討し、セキュリティ面では、暗号化により個人情報の保護が可能となるが、個人IDの管理において、どのような名寄せを行うかが問題となる。

A. 研究目的

健康情報を利用した遠隔医療で問題となるのは、(1) セキュリティと(2) 認証方法である。本研究では、この2点について考察を行った。特に、画像診断の面から問題点を検討し、その解決策があれば、解決策の可否を検討した。

B. 研究方法

健康情報および医療情報を利用して画像の遠隔診断を行う『Teleradiology』をモデルにして検討する。

このモデルは、一般病院(A)で撮影したCT画像やMRI画像を、一般ネットワークを用いた通信回線で遠隔地にある読影センター(B)に転送する。読影センターでは、送られてきた画像を画像診断医が読影を行い、読影レポートを再び通信回線を用いて、依頼元の病院(A)へ転送する。

この場合、使用するネットワークは、一般病院(A)と読影センター(B)との接続には、VPN(Virtual Private Network)を用いることとする(図1を参照)。画像を転送する場合は、画像フォーマットは、DICOM規格のフォーマット[1]を用いて、DICOM規格のプロトコールによる転送を

行う。

この場合の、(1) セキュリティ面の課題、(2 a) システム利用者の認証方法、(2 b) 読影対象となる患者の確認方法について検討を行い、問題点を探る。

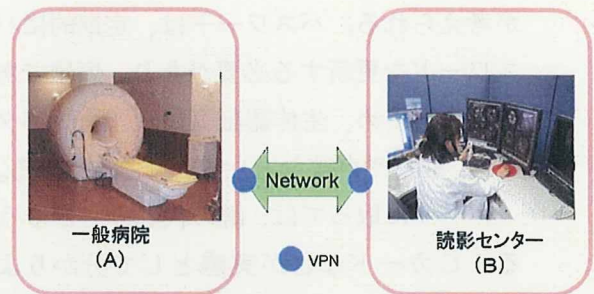


図1 一般病院と読影センターの構成

C. 研究結果

C. 1 セキュリティ面の課題

セキュリティの面から検討した結果は、以下に示すような問題点がある。

表1 セキュリティの問題点

NO	項目	内容
1	検査依頼情報	検査依頼情報には、患者名、性別、年齢や病名が含まれる。また、

		依頼元の施設名。
2	画像情報	画像情報には、個人情報（氏名、生年月日、性別、病院名）が含まれる。
3	読影結果報告書	患者名、病名や病院名が含まれる。

表1に示すような、情報をいかに保護して、通信を行うかが課題となる。一般的なVPNの強度で十分なのか、また、どのような暗号強度を用いるべきなのかを検討する必要がある。

現在、一般に市販されているVPNを利用して遠隔画像診断を行うことが、どのようなセキュリティー上のリスクを負うのか、各事業者は検討する必要がある。

C. 2 システム利用者の認証方法

利用者の認証方法には、図2に示す方法が考えられる。パスワードは、定期的にパスワードを更新する必要がある、煩雑である。そのため、生体認証（指紋、静脈パターン、虹彩や声紋など）が検討されている。

ユーザにとって、鍵の代わりとなりうるICカードなどが実感として分かりよいと思われる。また、PKI個人認証等の技術を用いる必要がある。施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとることが重要である。セッション乗っ取り、IPアドレス詐称等のなりすましを防止する対策も必要となろう。

医療情報システムの安全管理に関するガイドラインによれば、上記を満たす対策として、例えばIPSecとIKEを利用することによりセキュアな通信路を確保することがあげられる。

各装置には、利用者認証のログを記録できるような機能が必要である。IHE（Integrating the Healthcare Enterprise）[2]のATNA（Audit Trail and Node Authentication）[3]機能を使用することが望まれる。

利用者認証

- ユーザのみが知っているもの(パスワード)
- ユーザが所有するもの(鍵やカード)
- ユーザの特徴を表すもの(指紋、静脈パターン、虹彩などのバイOMETリックス)
- ワンタイム・パスワード
- 医療用PKI個人認証

図2 利用者認証の種類

C. 3 読影対象となる患者の確認方法

読影対象となる患者の確認方法として、過去の検査データとの比較参照が望ましい。同一の医療機関から依頼された画像検査であれば、同じ患者IDを使用しているために、過去の検査を参照することは容易いが、複数施設からの依頼で同一患者の名寄せを行うことは、標準的な手段がなく困難が予想される。しかしながら、同一患者の過去画像を参照して読影することは、読影精度の向上につながるため、複数医療機関をまたいだ名寄せ機能を検討すべきである。また、地域や市町村単位での患者の統一医療IDの確立が望まれる。

C. 4 患者の過去検査履歴

個人が長期間に渡って健康診断や病院における診断・治療を行っている場合に、そのデータのある特定の個人に結びつけ、名寄せをする必要がある。医療IDの検討をすべきであると考え（図3）。

画像読影の場合でも、読影対象となる患者の過去における検査を参照することにより、読影精度の向上が可能となる。

- ・名寄せの方法論
 - ・名寄せのセキュリティー
 - ・名寄せにより可能となるメリット
- －被曝管理
- －患者のフォローアップ
- －検査結果の有効活用

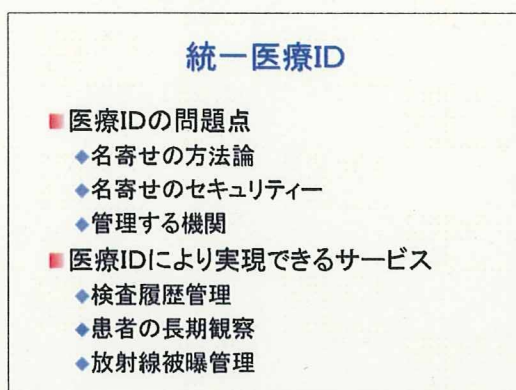


図3 統一医療ID

D. 考察

インターネットに代表されるネットワークを利用して患者の個人情報を取り扱う時代になりつつある。この場合に、暗号化技術やユーザの認証技術を用いて安全・安心な遠隔画像診断システムを構築することが急務である。実際に、ネットワークを利用して、システムを構築する場合に、どのくらいの強度の暗号ならば良いのか、また、どのようなVPNを使用すべきなのかを示すときに来ていると考える。

医療機関が限られた資源（人材やコスト）で情報システムを構築する際に問題になるのは、そのシステムの管理や説明責任に耐えるだけのコストである。このようなコストをいかに低減して、医療に活用するかが緊急の課題である。

医療IDについて、外国では、スウェーデンやノルウェーなどでは、医療IDが確立している。また、アメリカでもソーシャル・セキュリティー番号を名寄せに利用することが可能である。日本でも、早く医療関連の情報を一元的に扱えるような機構が必要と思われる。

日本でも社会保障ファイナンスを一元化し、社会保障番号で管理する案が提案された経緯があるが、税金や年金などの番号とは、共通にせず、医療だけに特化したID番号を創設するべきであろう。現在の情報技術を利用すれば、医療ID番号を税金の納税者番号や社会保障番号とリンクすることは、技術的に容易である。国民の医療福祉の推進のためにも、早急に医療ID制度確立すべきと考える。

E. 結論

健康情報を利用した遠隔医療で問題となる（1）セキュリティーと（2）認証方法について検討した。この2点について考察を行い、画像診断の面から問題点を検討し、セキュリティー面では、暗号化により個人情報の保護が可能となるが、個人IDの管理において、どのような名寄せを行うかが課題である。

F. 参考文献

- [1] DICOM : Digital Imaging and communications in medicine <http://dicom.nema.org/>
- [2] IHE <http://www.ihe.net/>
- [3] ATNA, Audit Trail and Node Authentication, http://www.ihe.net/Technical_Framework/index.cfm#IT

G. 研究発表

1. 論文発表

なし

2. 学会発表

なし

H. 知的財産権の出願・登録状況

なし

電子私書箱と連携した保健医療情報の安全な利活用を促進する医療 情報ネットワーク基盤整備の技術的方策に関する研究

(H20-医療-一般-030)

個人医療情報の安全性確保に関する調査・検討

研究分担者 山本 隆一 (東京大学大学院 情報学環)

研究要旨

情報システムの安全管理の基本である監査証跡について、厚労省の基準である安全管理 GL を精査し、要件を抽出した上で、全数監査については東京大学付属病院の実際の操作ログにおいて実現可能性を検討し、またサンプリング監査については文献を含め考察した。現実的にはサンプリング監査を行わざるを得ないが、全数検査も不可能ではないことを示し、そのための要件を整理できた。

A. 研究目的

一般に情報セキュリティは可用性、機密性、完全性、責任追及性を確保することで達成されるとされており、利用者の認証と監査が重要と言われている。その意味で病院情報システム (以下 HIS) の様々な操作の監査証跡は定型文書の電子化にとどまらず、扱う情報を安全に管理する上できわめて重要と考えられている。その一方で HIS の操作きわめて多数の利用者が頻回にアクセスすることが一般的であり、その操作ログは膨大な量に達する。本研究では安全性の確保に資するために、その膨大な操作ログを効率よく解析する手法について考察することにある。

B. 研究方法

厚生労働省が個人情報保護に関する法

律を実施するために大臣が斟酌すべき指針の一つとして公表している医療情報システムの安全管理に関するガイドライン⁽¹⁾ (以下安全管理 GL) の監査証跡に関する部分を精査し、要件を抽出した上で一般の医療機関にとって合理的な監査のあり方をサンプリング調査および全数調査に分けて考察する。

(倫理面への配慮)

今回の作業に用いたデータは、現実の患者データではあるが、患者識別情報はまったく用いていなく、また利用者情報を職種以外は用いていないため、患者ならびに利用者ともに個人が識別できる可能性はなく、倫理面への配慮は特に必要なかった。

C. 研究結果

C-1 安全管理 GL

安全管理 GL では6章の情報システムの基本的な安全管理の項に利用者認証と操作ログについて記載されている。

6.5 技術的安全対策のB項で、認証についてはIDとパスワードによる認証も現時点で禁止はしていないものの、ICカード等の所持情報、生体計測認証、パスワード等の認証手段から2つ以上を組み合わせる2要素認証を強く推奨している。またアクセスログについては「個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。

また、アクセスログの証拠性確保のためには、記録する時刻は重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取らなければならない。」とされており、定期的な監査を求め、さらに正確な時刻情報の必要性について言及している。実際の基準であるC項では次に示すようにC-5からC-8に詳細に記載している。

5. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人

事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。

6. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。
7. アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。
8. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。

ただし、C項ではアクセスログの確認という表現が用いられ、厳密な監査は求めている。

C-2 操作ログの監査の方法

操作ログの監査は2つの方法が考えられる。一つは全数監査であり、すべての

ログを監査する方法である。ただし一般に HIS の操作ログは膨大な数になる。2005 年の東京大学付属病院の入院患者に対する HIS の操作ログを実際に収集したところ、10 月一ヶ月間で約 300 万レコードに達した。これは利用者が特定の患者を選択し、何らかの操作を行い、ログアウトするか、別の患者の選択までを 1 レコードと数えた数で、実際の詳細な操作ログはこの 10 数倍に達する。これをすべて人手で監査することは事実上不可能であり、まず、具体的な指示を含むアクセスを除き、参照のみのアクセスの内、アクセスの時点からさかのぼって 48 時間以内に同一利用者による指示を含むアクセスがある場合を従属アクセスとして除いた。この時点は全アクセスログレコードを 84% が除かれた。残ったアクセスを独立アクセスとし、利用者と患者の関係を、主治医グループ、入院病棟勤務看護師等の合理的にアクセスの必要性を推測できる関係があるものを除外した。なお、看護師等では実際の勤務状況を反映させた。その結果全アクセスログレコードの 98% が除外された。その結果人手で監査が必要なアクセスログは約 6 万レコードとなった。これを実際に人手監査したところ、ほぼすべてが中央診療部門のスタッフによるアクセスであった。

次にサンプリング監査について述べる。これは多くの機関で実施されており、大きくランダムサンプリングと特定属性の患者の操作ログの二つに分類することができる。後者の例は岸らが報告しているような職員の家族が入院した場合⁽²⁾や、いわゆる VIP 患者である。岸らはこの方

法でも一定の効果を認めている。

D. 考察

監査はセキュリティの基本ではあるが、実際には実施が容易ではない。監査証跡を確実に保存することで正規の利用者による不正アクセスあるいは不要アクセスを抑止する効果があることは容易に想像できるために、安全管理 GL では収集を必修としているのであろうが、やはり監査は行うべきである。現実的にはサンプリング監査が主体にならざるを得ないが、本研究で示したように、十分な情報が収集できれば全数監査も不可能ではない。ただしそのためには職員の勤務状況をほぼリアルタイムに把握することが必要で、また実際には本研究で 1 レコードと定義した、ある患者に対する連続の操作を一レコードとするためには単一のシステムのログでは不可能で複数のシステムのログを関連づけて収集しなければならない。DICOM や JAHIS 規格に、このような目的のログの標準化に関する規格があり、これに準拠することが必須である。さらにある程度自動的に問題のないログレコードを分類できるログ管理サーバの開発が急がれる。

参考文献

1. 医療情報システムの安全管理に関するガイドライン（厚生労働省）
<http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html>（2010 年 3 月確認）
2. 電子カルテシステム利用者に対する患者情報アクセス記録通知，岸真司，永野泰之，餅井美愛，沢田潔，浅井広，板津武晴，第 25 回医療情報学連合大会論文

集, 平成 17 年

なし

E. 結論

情報システムの安全管理の基本である監査証跡について、厚労省の基準である安全管理 GL を精査し、要件を抽出した上で、全数監査については東京大学附属病院の実際の操作ログにいて実現可能性を検討し、またサンプリング監査については文献を含め考察した。現実的にはサンプリング監査を行わざるを得ないが、全数検査も不可能ではないことを示し、そのための要件を整理できた。

F. 健康危険情報

本研究において、生命、健康に重大な影響を及ぼすと考えられる新たな問題、情報ななかった。

G. 研究発表

H. 知的財産権の出願・登録状況

なし

電子私書箱との連携に関する調査・検討

研究分担者 小尾 高史 東京工業大学大学院総合理工学研究科准教授

研究要旨 我々は、国民が自らの情報を簡単に収集管理可能な仕組みである「電子私書箱（仮称）」に関して、その具体的な実現方策について検討を進めており、それを利用した安全・安心なIT社会の実現を目指している。さらに、本年4月のデジタル新時代に向けた新たな戦略～三か年緊急プラン～では、従来の「電子私書箱」に対して、様々な電子行政サービスを実現するための機能を追加した「国民電子私書箱（仮称）」構想が提案され、あらゆる公共サービスに対する総合口座を実現することが求められるとともに、今後は、次世代電子行政サービス、社会保障カード、（従来の）電子私書箱を一体化した議論をすることが要求されている。これに対して、本研究は、「国民電子私書箱」を利用する社会保障分野のワンストップサービスの実現方法を整理し、退職時の様々な手続きを例として、具体的な国民電子私書箱の利用方法を検討した。

A. 研究目的

現在、国民の社会保障、行政情報などに関する個々の情報は、医療機関や保険者、地方自治体等、機関毎において個別管理されており、これらは国民自らの情報であるにも関わらず、本人が必要に応じて自由にアクセスし、利活用できる状態にはない。このような状況の下、平成19年4月にIT戦略本部より発表されたIT新改革戦略 政策パッケージ[1]において、国民視点の社会保障サービスの実現に向け、電子私書箱（仮称）の創設が記載された。これを受けて、平成20年8月に発表された重点計画2008[2]では、「国民が自己の情報を安全かつ簡便に入手、閲覧及び活用することができる社会保障サービスを実現するため、医療機関や保険者等に個別管理されている情報を、希望する国民が自ら入手・管理できる電子私書箱（仮称）を検討し、2010年頃のサービス開始を目指す」とされたことを受け、我々は、これまで社会保障サービスに資する電子私書箱の基本機能の検討を行ってきた[3,4]。

しかし、平成21年4月に発表されたデジタル新時代に向けた新たな戦略～三か年緊急プラン～[5]において、希望する個人又は企業に提供される高度なセキュリティ機能を持った電子空間上のアカウントとして、従来の「電子私書箱（仮称）構想」及び「社会保障カード（仮称）構想」[6]を発展させ、社会保障分野のみならず、広い分野でのワンストップの行政サービスを提供するために提供される国民電子私書箱（仮称）が提案された。

そして、平成21年7月のi-Japan戦略2015[7]において、「国民電子私書箱は、希望する国民・企業等に提供される、電子空間上で安心して年金記録等の情報を入手し、管理できる専用の口座であり、社会保障分野のみならず幅広い分野でワンストップの行政サービスを提供するものである。」と再定義され、「「国民電子私書箱（仮称）」を、広く国民・企業等の間に普及、定着させることなどにより、顧客である国民に対し、以下に掲げる行政サービスを提供する。」とされたサービスの1つとして、幅広い分野におけるワンストップ行政サービスが挙げられることとなった。

我々はこのような状況の下、新たな私書箱構想である国民電子私書箱に関する技術的要求項目を明らかにし、要求定義をまとめる作業を行っている[8]が、本研究では、これら状況を踏まえ、「国民電子私書箱」を利用するワンストップサービスの実現方法を整理し、退職時の様々な手続きを例として、具体的な国民電子私書箱の利用方法を検討したのでその結果を報告する。

B. 研究方法

ワンストップサービスには、様々な提供形態が考えられるが、本章では、公共的分野に関連するワンストップサービスの考え方を整理するとともに、電子私書箱を利用したワンストップサービスの考え方についてまとめる。

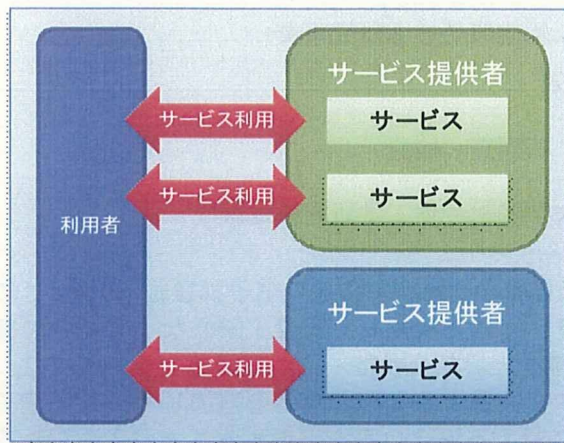


図1 従来型のサービス利用・提供

一般的に、ワンストップサービスとは、利用者が一か所もしくは一度の手続きで必要とする関連作業を一括して完了できるように設計されたサービスのことを指し、従来は利用者がサービス提供者との間で個別に行っていた手続きなどのサービス利用を（図1参照）一括して行えるようにするものである。

ワンストップサービスの最も代表的な例としては、引っ越しなど住民のライフイベントに沿って必要となる複数の機関等にまたがる様々な申請・届出を一括して手続きできるようにしたものがあり、引っ越し手続き、結婚手続き、出生手続き、退職手続きなどがその対象として挙げられている。

ここで、今回の国民電子私書箱構想によるワンストップサービスの検討を待つまでもなく、従来からワンストップサービスを実現するための検討は行われてきた。先に述べたように、ワンストップで取り上げられる手続きには、ライフイベントに関するものが多いため、住民などの利用者から見た際には、自治体等を直接の窓口としたものが多い。自治体等で提供されるサービスの内容は様々であるが、ワンストップサービスとしては、大きくは「申請手続き型」「情報照会型」の二つに分類することができる。

「申請手続き型」は、従来行政サービスの申請手続きをベースとしてワンストップ化を図ったものであり、申請や届出を受け、決められた業務の流れに従って処理を行うサービスである。具体的には、利用者からの複数のサービスに対する申請・届出を一括して手続きするものであり、ポータルサイトにおいて利用者の申請や届出を受けて、処理の結果を返すものである。手続き例としては、引っ越し、結婚、出生など、ライフイベントに沿って必要となる複数の申請・届出を、一括して行う手続きがあり、一種のワークフローに従って、順次処理が行われるため、各サービス提供者による作業が順次必要となる手続きでは、申請から結果

通知という一つのワンストップサービスが完了するまでに時間がかかる場合も考えられる。

「情報照会型」は、利用者が、一度に複数のサービスから情報を照会または検索するものであり、複数のサービス提供者から、同時に情報を収集し、利用者に対して必要な情報を返すものである。このサービスは、利用者からの情報取得の要求に応じて複数のサービスから情報を取得し、これら情報を合わせて提供するサービスであり、利用者に対する新たな付加価値をもったサービス提供の可能性を含んでいる。手続き例としては、複数のサービス提供者や複数の業務で管理されている情報について、新たな観点や別の視点から関連する情報をまとめて利用者に表示したり、検索結果を返還するものなどが考えられ、現状の考えられるものとしては、地域の図書検索サービスなどがある。

その他に、これらをまとめた総合的なワンストップサービスも考えられるが、ここでは省略する。

このようなワンストップサービスを実現するために必要となる技術要素として、「ポータル」、「認証・署名」、「バックオフィス連携」、「標準化」が挙げられており、従来型ワンストップサービスにおいては、特に、「バックオフィス連携」を充実させることにより、行政機関間の連携を実現し、添付書類などを省略することを目指している（図2参照）。

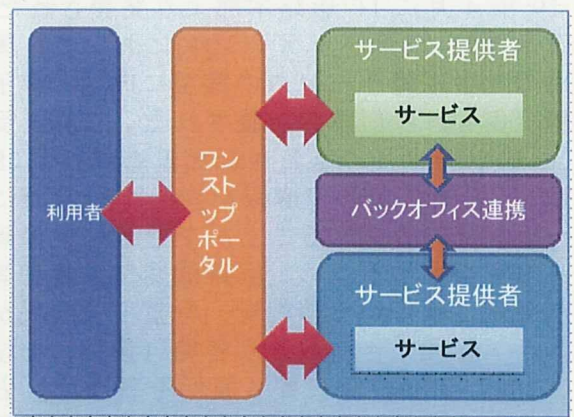


図2 従来型ワンストップサービスの考え方

しかしながら、現在ワンストップの対象となる様々なサービスは、サービス提供者ごとに独自のシステムを利用して行っており、関係する機関間で連携できる既存の仕組みは存在しない。このため、バックオフィス連携を実現するためには、すべてのサービス提供者間で新たなインターフェース仕様を決める必要があるだけでなく、以下のような課題を解決する必要がある。

1. バックオフィス連携を効率的に実施するためには、行政機関等のサービス提供者におけるデータ等の標準化を進める必要がある。

2. セキュリティリスクを考慮して、取り扱う情報は一カ所に蓄積して集中管理せず各機関で保有し、各機関が保有するデータベース間の連携は疎結合により実現することが望まれる。
3. サービス提供者で個人情報を共同利用する際は、必ず利用者本人の同意を得る必要がある。
4. 利用者が自分の情報がいつ、どこからどこへ送付されたか確認できる仕組みが必要である。
5. 利用者の情報を共同利用する機関に対して、バックオフィス連携のための機関（電子行政分野では、「行政情報の共同利用支援センター（仮称）」などが提案されている）を介して得た情報の蓄積および目的外の利用を禁止する必要がある。

ここで、課題2から5は、利用者の情報を利用者が直接関与しない状態で共有することにより発生する問題であると考えられる。そこで我々は、ワンストップサービスを実現するために必要となる技術要素としてあげた「ポータル」、機能を「国民電子私書箱」に置き換えることにより、これら課題を解決することを考えている。

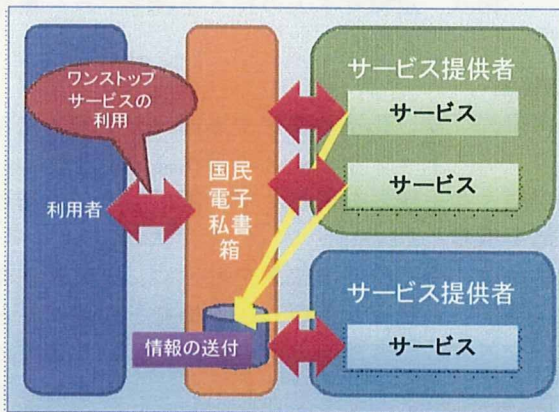


図3 国民電子私書箱を利用したワンストップサービスの考え方

例えば、バックオフィス連携ができない機関がある場合には、図2に示すワンストップサービスを提供できない。そこで、連携に必要な情報を電子的に国民電子私書箱に交付し、電子私書箱を起点としてワンストップサービスを行う仕組みを提供する。さらに、国民電子私書箱側に情報を交付することにより、国民電子私書箱の有するコンセルジュ機能を用いて利用者が気付いていない手続を利用者に提示するなど、付加価値の高いサービスを提供可能となり、利便性の高いワンストップサービスを実現できる。また、利用者が自分の情報の制御に積極的に関与することになるため、従来問題になっていた、利用者に対する自己情報コントロール権付与の問題を解決できる可能性があると考え

られる。

このように、従来型電子行政サービスで考えられていたポータル機能を国民電子私書箱に置き換えることにより、国民電子私書箱を経由して得られる情報や私書箱内に保存された情報を利用して、これら情報を起点とする新たな付加価値を有するサービスを展開することが可能となる。

C. 研究結果

電子私書箱を利用した退職ワンストップサービスの実現

現在、企業は従業員の退職に伴い、年金、医療保険、雇用保険、国税、地方税に関する手続をそれぞれ別々に行う必要がある。これら手続は、非常に煩雑であることが知られており、企業担当者、退職者は、社会保険事務所や健康保険組合など6ヶ所以上の機関を訪問し、健康保険被保険者証や出勤簿、賃金台帳など15種類以上の書類を添付した申請などを行う必要がある。

このようなことから、退職者自身は、自分の退職に際して、何のために何をしなければならないのかを正確に把握することは困難であり、企業でも退職者への説明にかなりの時間が割かれているのが現状である。

このような現状を受け、平成19年10月に設置され、様々な行政手続を基本的にワンストップで簡便に行える次世代の電子行政サービス基盤の検討を行っている「次世代電子行政サービス基盤等検討プロジェクトチーム」では、平成20年6月の「次世代電子行政サービス（eワンストップサービス）の実現に向けたグランドデザイン」において、優先的に検討すべきワンストップサービスの具体例として、退職手続を挙げている。

しかしながら、現在までの検討では、主にバックオフィス相互間の連携やフロントオフィスとバックオフィス、民間手続との連携等を図ることにより、それを実現するものとしており、前章で述べた利用者主体の情報管理によるワンストップサービスを実現する方法は明らかになっていない。

本章では、我々が検討を進めている国民電子私書箱の有する機能[8]を利用して、どのように退職ワンストップを実現するかを示す。

電子私書箱の機能構成についての検討を別途進めているが、基本的なシステム構成は、図4で示すものになると考えられる。基本システムを構成する各機能は、利用者が電子私書箱へアクセスするために利用する認証機能、電子行政、社会保障サービス等の入り口となるポータル機能、利用者の情報の制御及び送受信を行う私書箱サービス機能、公的情報保有機関と電子私書箱との関連づけを行う私書箱プラットフォーム機能の4つとなり、公的情報保有機関からは、基本機能

に対して直接またはプラットフォーム機能を介して送付される。

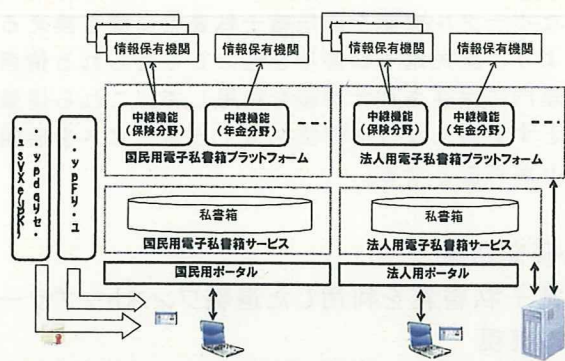


図4 国民電子私書箱のシステム構成

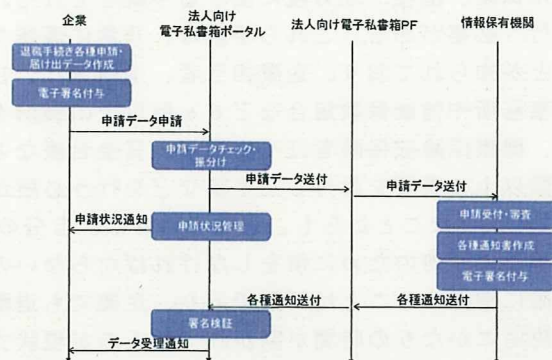


図5 企業の行う手続きのフロー概略

さらに、企業等については、国民向けと同等の機能を有する法人向け電子私書箱が提供され、企業と情報保有機関間の情報のやり取りには、法人向け私書箱が利用され、法人から国民への情報送付は、法人向け私書箱プラットフォームと国民向け私書箱プラットフォームが連携することで行われる。

まず、退職時の企業が行う退職手続き（図5）は、企業内で一括して申請書類を作成したのち、これらをまとめて法人向け電子私書箱ポータルに送付することにより行われる。このとき私書箱ポータルは、ポータル利用者を支援するコンセルジュ機能を有しており、送られてきた情報をもとに振り分け、適切な情報保有機関へ送付する働きをする。これにより、企業側は必要な処理をワンストップで行えるようになり、事務処理等の負担は大きく減ることになる。

次に退職者本人の手続き（図6）だが、電子私書箱を利用することで、従来退職時の会社経由で入手しなければならなかった各種通知書は、情報保有機関から直接退職者に送付されることになるため、何らかの理由による会社経由でのこれら通知書の入手が困難な場合でも、退職者はその後の処理に必要な書類等を入手することができる。また、私書箱ポータルの有するコンセルジュ機能により、退職者に対して、送付された

情報をもとにその後、どのような手続きをどのような理由で行うのか、必要な手続きにはどのようなものが存在するかを適切に提示することができ、退職者は、必要な手続きを正しく正確に実行できるようになると予想される。



図6 退職者本人の行う手続きフロー概略

D. 結論

本研究では、我々が想定する国民電子私書箱を利用したワンストップサービスの実現方法を整理し、退職時の様々な手続きを例として、国民電子私書箱の利用方法を検討した。

今後は、今回の検討結果をもとに、国民電子私書箱が具備すべき機能を整理し、各機能を利用してどのようにシステムを構築するかの検討を行い、実際に退職ワンストップをデモンストレーションするためのシステムを構築する予定である。

E. 研究発表

1. 小尾高史・谷内田益義・李 中淳・本間祐次・山本寛繁・大山永昭：国民電子私書箱を利用した退職ワンストップサービスの検討；コンピュータセキュリティシンポジウム CSS2009, E9-3, 2009
2. 小尾高史・谷内田益義・李 中淳・本間祐次・大山永昭：サーバ連携型 IC カードシステムを利用した公的分野別個人識別番号導入の検討, 3E3-1, SCIS2010, 2010
3. 小尾高史・谷内田益義・李 中淳・本間祐次・大山永昭：国民電子私書箱を利用した退職ワンストップサービスの実装；電子情報通信学会総合大会講演論文集, D-9-4, 2010