川崎医療福祉学会誌　Vol. 26　No. 2　2017　264 − 272

短　報

アメリカで発生した医療提供者による個人情報に関する事故原因の図式化

品川佳満*1　橋本勇人*2

要　　約

本研究では，アメリカで発生した医療提供者による個人情報取扱い事故事例を分析することにより，事故原因の全体像を明らかにすることを目的とした．アメリカのHITECH法により報告が義務付けられている個人が識別可能な500人以上のPHI（Protected Health Information）が含まれていた事故事例を分析対象とし，事故原因のカテゴリを作成した．結果として「盗難」，「置き忘れ」，「紛失」，「廃棄関連」，「誤送付・誤配布・郵送中の事故」，「メール誤送信」，「設定ミス」，「不適切な持出し」，「意識的な開示，目的外使用，過剰な情報提供」，「不正アクセス」の10の事故原因カテゴリに整理できた．カテゴリ化された事故原因をもとに3つの視点（対象が財物か情報そのものか，引き起こした者が特定人か不特定人か，意識型かうっかり型の事故か）から事故原因の全体像を図式化した．図式化した事故原因の全体像は，事故防止策を考える上で役立つものになると思われる．

1．はじめに

全面施行から約10年が経過した2015年9月に個人情報保護法の改正が行われた．また，同年10月には個人情報保護法の特別法である番号法（マイナンバー法）が施行された．番号法は，現在「社会保障」，「税」，「災害対策」に利用が限定されているが，将来的には医療分野における活用も視野に入っている[1)]．私たちの個人情報は，「保護」のみならず，「利活用」する時代に入ってきたといえる．情報を守りながら安全に利用するためには，これらの法律やそれを受けたガイドラインを理解し，ルールを守ることが重要である．しかし，現状では，多くの個人情報に関する事故が発生している[2)]．

我が国では，事業分野ごとに個人情報の保護に関する法律が存在するわけではなく，個人情報保護法を受けた形で，分野ごとにガイドラインが定められている[3)]．これに対しアメリカでは，一般法としての個人情報保護法は存在せず，領域ごとにプライバシー保護に関する法律が制定されている．医療分野でいうと，1996年に「医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act of 1996（HIPAA; Pub. L.104–191）」が制定され，さらに，2009年の「アメリカ復興・再投資法（American Recovery and Reinvestment Act of 2009（ARRA; Pub.L.111–5）」の一部にHIPAA法を拡張した「経済的および臨床的健全性のための医療情報技術に関する法律（Health Information Technology for Economic and Clinical Health Act（HITECH）」が制定されている．

HIPAA法制定の背景には，医療費のコスト削減を，情報の電子化によって行おうとしたことにあり，同時に情報の取扱いルールを定めることでプライバシー保護をも行っている．またその後制定されたHITECH法では，HIPAAプライバシールールを拡張し，中でも情報漏えいなどの事故が起きた場合，患者への通知義務や，保健福祉省に対する報告義務，さらに違反に対する罰則を強化している[†1)]．この点，日本においては，個人情報保護法違反に対する罰則はあるものの，具体的なルールや，事故発生の際の報告や公表等については，ガイドライン（解説を含む）に委ねられており[†2)]，アメリカと比較

*1 大分県立看護科学大学　健康情報科学研究室
*2 川崎医療短期大学　医療保育科
（連絡先）品川佳満　〒870-1201　大分市廻栖野2944-9 大分県立看護科学大学
E-mail : shinagawa@oita-nhs.ac.jp

するとその法的強制力は低いと言わざるを得ない.

つまり, アメリカは, いち早く医療情報の標準化・電子化をすることにより, 情報の利活用を促進すると同時に, 安全保護措置とプライバシールールによる情報の保護を法レベルで実現し,「保護」と「利活用」のバランスを図ろうとしている. 日本においても, 一般法である個人情報保護法に加えて, 特別法であるマイナバー法を制定し同様の道筋にある. いち早く情報の保護と利活用に取り組んでいるアメリカの現状を踏まえ, そこで発生している事故の内容やその原因を知ることは, 日本で発生している個人情報の漏えい問題や今後の対策を考えていくうえで参考になる.

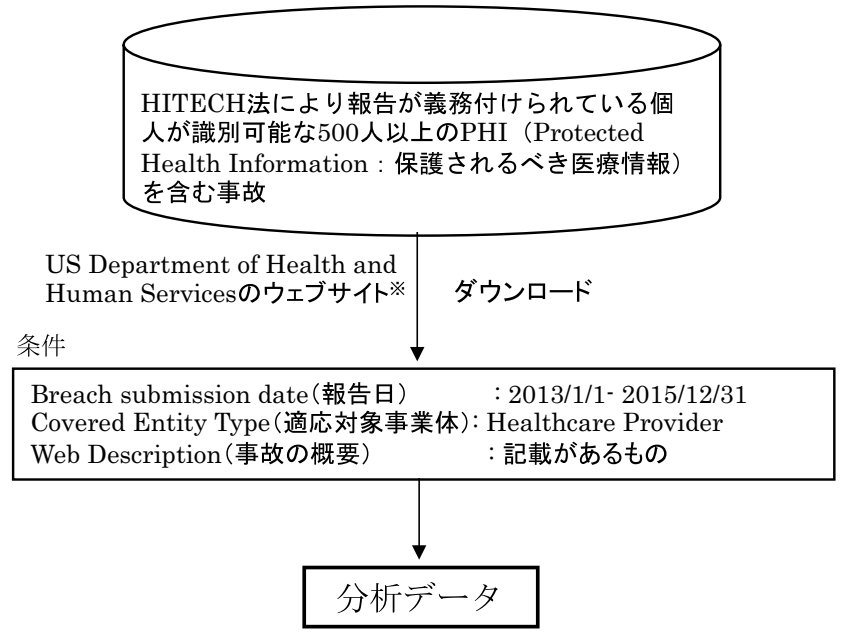
これまで, 日本で起きた医療分野における個人情報の取扱い事故については, その傾向や特徴等についての報告がある[4,5]. 筆者らも事故原因や媒体の現状[6], 経年変化[7], 事故パターン[8,9], 教育実践[10,11] について研究を行ってきた. また, アメリカの HITECH 法を受け, 事故が発生した際の対応や公表のあり方について, 日本の事故事例をもとに事故発生から公表までに要した日数を分析することで, 医療機関が適正な対応や公表を行うための基本的態度・姿勢を提案してきた[12]. このように日本の事故事例を対象にした研究は数多くされている. 一方, アメリカの個人情報に関する事故については, HIPAA 法に対する認識やセキュリティに対する実践状況[13], 規則への遵守状況に関する調査[14,15], 政府に提出された事故報告を単純集計したものは見受けられる[16]. しかし, 我が国の個人情報漏えい事故対策の参考となるような事故原因に着目した研究はほとんどない.

そこで本研究では, アメリカで発生した医療提供者による個人情報に関する事故事例を分析し, 事故原因の全体像を明らかにすることを目的とした.

2. 方法

2.1 データ収集と分析データの抽出手順

図1にデータ収集および分析データの抽出手順を示す. 分析対象は, HITECH 法で報告が義務付けられ, アメリカ合衆国保健福祉省のウェブサイトにリスト化されている個人が識別可能な500人以上の PHI（Protected Health Information：保護されるべき医療情報）が含まれていた事故とした[17]. ウェブサイトから表計算形式（Excel）でデータをダウンロードした後, 条件として, 報告日（Breach submission date） が2013/1/1 ～ 2015/12/31（3年間分）であり, HIPAA 法のプライバシールールが適用される機関（Covered Entity Type）が医療機関や医師などの「医療提供者（Healthcare Provider)」によるもので, さらに事故に関する概



※ US Department of Health and Human Services. “Breaches Affecting 500 or More Individuals.” https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

図1 データ収集および分析データの抽出手順

要（Web Description）の記載があるものを抽出し，本研究の分析データとした．

２．２　分析方法

ダウンロードしたデータ内には，原因に関する項目（Type of Breach）が存在する．そこでは事故原因を7分類（「Hacking/IT Incident」，「Improper Disposal」，「Loss」，「Theft」，「Unauthorized Access/Disclosure」，「Unknown」，「Other」）しているが，事故防止策を考えた原因を探る上ではアメリカの分類をさらに詳細に分ける必要があると考えた．そのため，本研究では事故の概要に基づき，個人情報の取扱い事故に関する研究歴のある研究者2名によって分類を行った．以下にその手順を示す．

① 分析データの中からサンプルとして2015年に報告された事故を抽出し，事故原因について暫定的なカテゴリを作成した．なお，事故の中には，複数の原因が関係するケース（例えば，ハッキング→マルウエア感染）があるが，原則として時間軸上の最初の原因をその事故の原因と判断した．

② 暫定的に作成したカテゴリを3年間分のすべての事例に対して当てはめを行い，該当するカテゴリがなかったもの，うまく当てはまらなかったもの，また暫定カテゴリ間に類似性があるものなどについて考慮しながら，カテゴリの新規，再作成，グループ化を繰り返し最終的な事故原因のカテゴリを作成した．

③ 最終カテゴリをもとに，その代表事例とともに表に整理した．

以上により分類した事故原因のカテゴリをもとに，医療提供者による個人情報に関する事故原因の全体像を図式化した．

３．結果

アメリカ合衆国保健福祉省のウェブサイトにリスト化されていた2013年～2015年の全事故データは838件であり，そのうち2.1で示した条件に合致し，本研究の分析対象となった事故事例は，221件であった．事故原因は，最終的に11のカテゴリに整理できた．表1に作成された事故原因のカテゴリ，代表事例，代表事例の報告年および州を示す．

PHI が記録されている物理的な媒体自身に対して起こるものとして，ノート PC や可搬型電子媒体の施設や車からの【盗難】，可搬型電子媒体や紙バインダーなどの【置き忘れ】や【紛失】，データの削除やシュレッダー処理をしなかったなど不適切な処分を行った【廃棄関連】の事故，宛名間違い等により関係ない人物へ情報を開示した【誤送付・誤配布・郵送中の事故】に分類できた．

ネットワークなど通信に関連するものとして，誤った人に PHI を含むファイルや情報を送った【メール誤送信】，サーバの設定ミスや，ファイルのアップロードなどによりインターネット上から PHI にアクセスできる状態になっていた【設定ミス】に分類できた．

必ずしも記録媒体や通信といった形式にとらわれない原因として，許可されていない情報を持出した【不適切な持出し】，情報へのアクセスは許可されているが，その情報を意図的に第三者へ開示したり，利用の範囲を超えた情報の利用（目的外使用）や過剰な提供を行った【意識的な開示，目的外使用，過剰な情報提供】に分類できた．また，情報へのアクセスが許可されていないにも関わらずアクセスした【不正アクセス】があった．

【不正アクセス】に関しては，手段やその目的により5つのサブカテゴリに分けることができた．コンピュータウイルスの感染により不正アクセスできる状態にされるなどした「マルウエア」による被害を受けたケース，サーバ等への「ハッキング」攻撃を受けたケース，「フィッシング」メールに応答したことにより情報漏えいが起きたケース，職務上必要のない情報へのアクセスをした「その他」の不正アクセスに整理できた．また，詐欺的な目的のために情報を取得するなど犯罪行為に関連した「identity theft 関連」の事故も見受けられた．

以上に挙げたもの以外として，最初の原因が不明だが，結果として情報への侵害が起きていた【結果的に開示】があった．

４．考察

４．１　事故原因を構成する3つの視点

アメリカで発生した医療提供者による個人情報取扱い事故の原因を分析した結果，原因が不明である【結果的に開示】を除くと10の事故原因に整理できた（表1）．この結果を踏まえ，事故原因の全体像を図式化するにあたり，本研究では，次の3つの視点が重要であると考えた．

①対象は，財物か情報そのものか

②引き起こした者は，特定人か不特定人か

③意識型かうっかり型か

①財物か情報そのものか

情報を記録する媒体には，紙などのアナログ系媒体から PC や可搬型電子媒体（USB メモリや外付けハードディスク等）といったデジタル系媒体まであるが，これらは，いずれも形ある財物である（≪物（財物）系≫と呼ぶ）．一方で，インターネット

表1　アメリカで発生した個人情報に関する事故から分析した事故原因のカテゴリ

原因のカテゴリ		代表事例	報告年(州)
盗難		従業員のノート PC と外付けハードディスクが盗まれ，外付けハードディスクには ePHI※1が含まれていた.	2015(TN)
		PHI※2を含む暗号化されていないノート PC が，従業員の車から盗まれた.	2015(TX)
置き忘れ		病棟で PHI を含むバインダーを置き忘れた.	2014(OH)
		事務室内で, ePHI を含むモバイルデバイスを置き忘れた.	2014(VA)
紛失		研修医が，患者の名前や臨床情報等を含んだ暗号化されていない USB フラッシュメモリを紛失した.	2015(AZ)
		PHI を含む救急部のログブックを紛失した.	2014(WY)
廃棄関連		コンピュータから ePHI を削除せずに，従業員の個人利用のために，旧式のコンピュータを配布した.	2015(FL)
		従業員がリサイクルセンターで PHI を含む手書きノートを処分していた.	2015(TN)
誤送付・誤配布・郵送中の事故		従業員がスプレッドシートエラーに起因する封筒の宛名間違いをしたため，PHI の許されない開示が起きた.	2013(FL)
		郵送の過程において，PHI を含む小包が損傷を受け開封されてしまった.	2015(KS)
メール誤送信		従業員が ePHI を含んだ添付ファイルを誤って送った.	2014(OK)
		従業員が，間違ったアドレスに ePHI を含む暗号化されていない電子メールを送った.	2015(MA)
設定ミス		PHI を含んだフォルダに対してデフォルトのパーミッション設定を変更しなかったため，インターネット上から見える状態になっていた.	2013(IL)
		うっかり ePHI を含む内部のデータベースをインターネットからアクセスできる状態にしてしまった.	2014(PA)
不適切な持出し		ePHI を含む電子メールを仕事用の電子メールアドレスから自宅の電子メールアドレスに送った.	2013(TX)
		従業員は，週末に仕事をするために PHI を含む紙のリストを持ち帰ったが，その情報の返却を忘れていた.	2014(OR)
意識的な開示，目的外使用，過剰な情報提供		医師が，元メディカルアシスタントへ FAX 経由で患者の PHI を許可なく開示していた.	2015(NY)
		従業員によって PHI の許可されていない利用があった.	2013(CO)
		従業員が，所期の目標を達成するために，必要以上の PHI を提供した.	2014(PA)
不正アクセス	マルウエア	ウイルス（トロイの木馬）がコンピュータデバイスに影響を与え，オンライン上で不正にアクセスできるようになっていた.	2015(NY)
		コンピュータがマルウエアに感染し，結果として，感染したコンピュータ上のデータが暗号化され，アクセスできなくなった.	2013(GA)
	ハッキング	ハッカーの疑いがある者が，コンピュータのハードディスクに不正アクセスを行い PHI に影響を与えた.	2015(TX)
		関係者以外の者がネットワークセキュリティーを回避し，ウェブサイトを操作するために使うマルウエアをコンピュータ上に置いた.	2013(MI)
	フィッシング	従業員が，フィッシングメールに応答してしまい，PHI を開示（暴露）してしまった.	2014(KY)
	その他	ベンダーの従業員が職務上の必要性がないにもかかわらず，PHI へアクセスしていた.	2015(MD)
	identity theft 関連	元従業員は，通常の職務上の義務に反して PHI にアクセスし，税金の還付詐欺にこの情報を利用した.	2014(VA)
		医学研修生は，PHI の写真を撮り，詐欺的な所得申告を提出する目的で，許可されていない第三者に電子メールで送った.	2013(FL)
結果的に開示（原因不明）		従業員が，自宅での仕事中に USB メモリを使った時，USB メモリの内容がインターネット上からアクセス可能な状態になっていた.	2014(AZ)

※1　ePHI: electronic protected health information
※2　PHI: protected health information

などの通信上の情報やサーバ等に保存されている情報など，情報そのものに対して起きる事故もある（≪ICT 系≫と呼ぶ）．現在の情報通信社会においては，情報の形態と事故原因は密接に関係しており，原因の全体像を示す一つの軸になると言える．

②特定人か不特定人か

事故には，従業員などの組織内部の人物や委託先などの特定の人物が関係した事故（≪特定人型≫と呼ぶ）と，外部の不特定の第三者が引き起こした事故とがある（≪不特定人型≫と呼ぶ）．内部の特定人による事故に対しては，組織のルールの強化や教育・研修の実施，外部の不特定人による事故には，技術的なセキュリティの強化といったことが事故防止につながる．つまり，事故防止策を考える上では事故を引き起こした人物の属性も重要な視点となる．

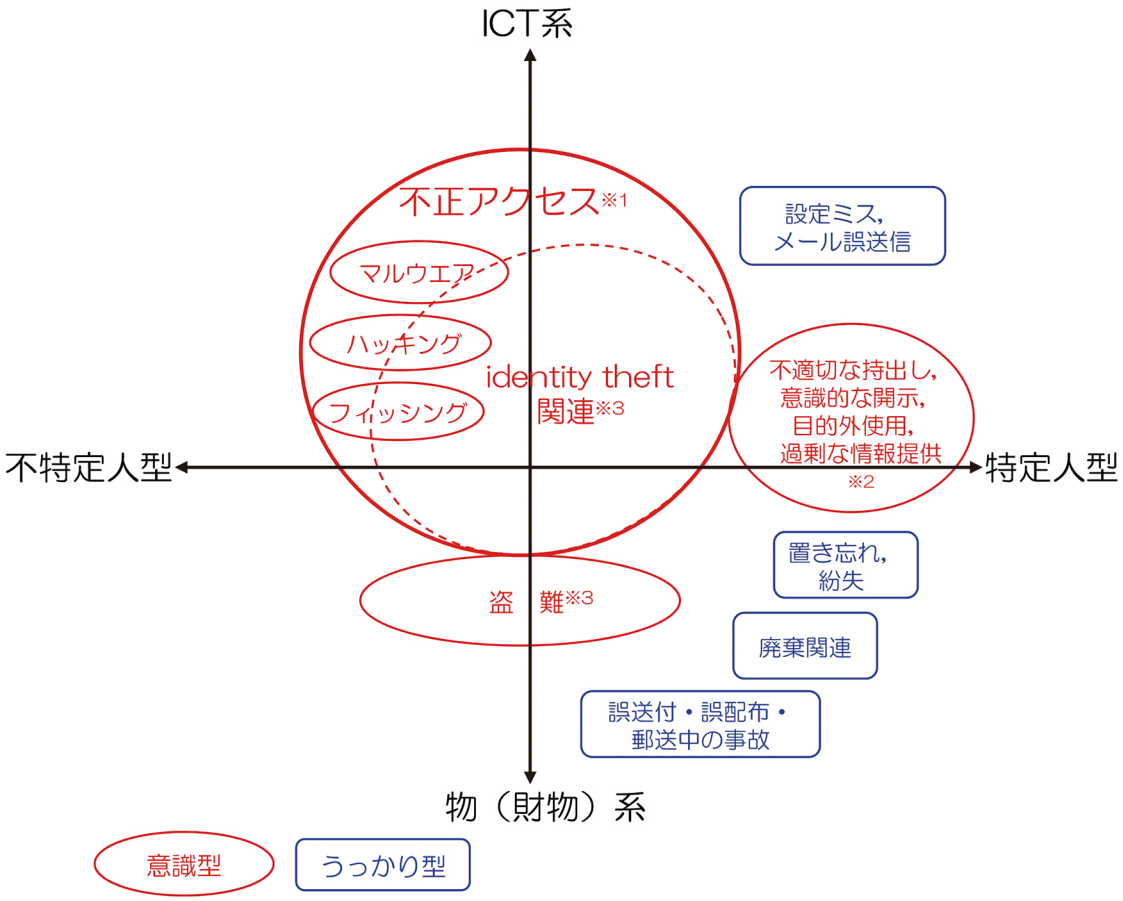
③意識型かうっかり型か

筆者らが行ってきた研究から，日本の医療機関で起きた個人情報の取扱い事故の中で，組織が定めたルールに違反していたケースが約半数あったことが明らかになっている[6]．この現状から，事故原因やパターンを考える上では，自らのミスなどにより発生した事故なのか（≪うっかり型≫と呼ぶ），刑法上の故意にあたる場合や民法上の悪意（知っていること）に基づく事故なのか（≪意識型≫と呼ぶ）という視点も重要となってくる．

4．2　3つの視点からみた事故原因の図式化

以上の3つの視点に基づいて事故原因の全体像を図式化したものが図2となる．縦軸が≪ICT 系／物（財物）系≫を示し，横軸が≪特定人型／不特定人型≫を示している．また，角丸四角形で示している原因が≪うっかり型≫，楕円形で示している原因が≪意識型≫となる．

設定ミスやメール誤送信は，情報そのものに影響する事故であり，自らのうっかりした誤操作に基づ



※1　許可されていない情報へアクセスした場合
※2　情報へのアクセスは許可されているが，その情報の不適切な持出し，意図的に第三者へ開示，目的外の使用，必要以上に提供した場合
※3　アメリカでは有体物，無体物に限らず ID 情報となるが，ここでは，不正取得した情報の移転，使用，所持といった犯罪に関連した行為があったものを不正アクセスの「identity theft 関連」とし，財物に対するもので identity theft 以外のものを「盗難」とした．

図2　図式化した個人情報の取扱いに関する事故原因

く事故であるため，≪ICT系，特定人型≫の領域に位置する≪うっかり型≫の原因となる．

置き忘れ，紛失，廃棄関連，誤送付・誤配布・郵送中の事故は，財物（紙，PC，USBメモリなど）に保存・記録されている情報に対して起きる事故である．また，関係した人物は組織内部や委託先の特定人であり，自らのうっかりに基づく事故である．そのため，≪物（財物）系，特定人型≫の領域に位置する≪うっかり型≫の原因となる．

不適切な持出し，意識的な開示，目的外使用，過剰な情報提供は，特定人の故意行為による事故である．情報の形態には，財物を介するケースだけでなく，仕事用のメールアドレスから，個人用のメールアドレスに情報を送るといった通信上の情報に関連するケースも存在する．そのため，これらの事故原因は≪特定人型≫の≪ICT系，物（財物）系≫の両領域に属する≪意識型≫の事故となる．なお，アメリカの事例では確認できなかったが，SNSを利用した情報漏えい事故は，この中に位置づくものとなる．

盗難は，外部の不特定人よる事故が中心となるが，内部の特定人によるケースもある．そのため，≪物（財物）系≫の≪特定人型，不特定人型≫の両領域に属する原因となる．なお，盗難は，故意や悪意に基づくものであるため≪意識型≫になることは言うまでもない．

不正アクセスは，≪特定人型，不特定人型≫，≪ICT系，物（財物）系≫のすべてのパターンが存在するため全領域に属する≪意識型≫の事故原因となる．ただし，不正アクセスを手段別にみた場合は，「マルウエア」，「ハッキング」「フィッシング」は情報そのものに対する第三者からの攻撃となるため≪ICT系，不特定人型≫の領域に位置づく．

不正アクセスの一部であるidentity theft関連の事故は，すべての領域に属する．アメリカの場合，ID情報そのものが犯罪の客体となり，不正に取得したIDを移転，使用，所持することは処罰の対象となる．通常，identity theftは情報そのものが対象となるため，先に述べた視点を考慮すると，ICT系のみに属すると言えるが，紙やPCの画面といった有体物の情報を写真に撮影するなどのケースもあるため本研究では，アメリカ法の概念とは異なり≪物(財物)系≫の領域にも属するように図式化した．

図式化した中の「不正アクセス」と「不適切な持出し，意識的な開示など」の区別は，「不正アクセス」は許可されていない情報へアクセスした場合となり，「不適切な持出し，意識的な開示など」は情報へのアクセスは許可されているが，許可されていない利用があった場合に該当する．

4．3　アメリカと日本の事故原因の違い

アメリカの事故事例をもとに作成した事故原因のカテゴリ（表1）と，筆者らが先行研究で集計した日本の事故原因との違いをみると[6,7]，日本の医療機関で発生した事故の場合，不特定人による不正アクセスを原因とする事故はほとんどみられていない．一方アメリカの場合は，ハッキング，フィッシング，マルウエアといった事故が多数発生している．アメリカでは，ID犯罪に対して1998年に制定された「Identity Theft and Assumption Deterrence Act of 1998（Pub.L.105-318)」，2004年に制定された「Identity Theft Penalty Enhancement Act of 2004（Pub.L.108-275)」などがありID情報の不正取得による移転，所持，使用などの行為が厳しく規制されている．一方日本においても，1999年に成立した不正アクセス禁止法が存在し，不正なアクセス行為に対する規制が存在する．しかし，日本とアメリカで違いがみられた背景には，アメリカの場合で言うと，ID情報の経済的な価値が広く認識されているため攻撃がシビアなのか，日本と比較して医療提供者側のセキュリティ対策が不十分なのかのいずれかということになる．

4．4　図式化した事故原因に基づく防止策への示唆

3つの視点に基づき図式化した事故原因の全体像は，自施設のリスク分析や事故防止策を考える上で役立つものになると思われる．例えば，≪ICT系≫の原因については，情報へのアクセス認証や制御などの技術的安全対策の強化，≪物（財物）系≫の原因は，入退室管理の実施や機器や装置の保護といった物理的安全対策の強化が必要となる．≪特定人型≫や≪うっかり型≫の原因については，規程の整備などの組織的安全管理対策の見直し，従業員や委託先に対しての教育・訓練といった人的安全対策の実施が必要となろう．つまり，もし事故が発生した場合，図のどの領域に属する原因に起因するものであったかを分析すれば，再発防止策や強化すべきポイントが見えてくる．その後の，原因にそった具体策をついては，ガイドラインが参考にできる[18]．

4．5　今後の課題

3年間分のアメリカの事故事例を分析対象とした本研究は，現在アメリカで起きている事故原因の大部分をカバーしたと思われる．しかし，500人以上のPHIを含む事故のみが対象となっており，少人数の事故事例が含まれていない．100人未満の事故も多く占める日本の現状を考慮すると[6,7]，今回整理した事故原因が日本の事例にうまく当てはまるか

今後確認する必要がある．そのうえで，日本とアメリカの事故原因や媒体の違いを量的に比較することで，法規制の影響をより深く考察できるものと思われる．

5．おわりに

アメリカのHITECH法で報告が義務付けられている医療提供者による個人情報に関する事故事例をもとに，事故原因の全体像を明らかにした．3つの視点≪ICT系／物（財物）系）≫，≪特定人型／不特定人型≫，≪意識型／うっかり型≫に基づき図式化した事故原因の全体像は，事故防止策を考える上で役立つものになると思われる．今後は，日本の事例へ適用可能か確認するとともに，アメリカと日本で発生した事故の原因や媒体の量的な比較を行い，法規制の違いがもたらす影響をみていくことが必要となる．

注

†1）HIPAA法に基づくプライバシールールについては，開原成允，樋口範雄編「医療の個人情報保護とセキュリティ―個人情報保護法とHIPAA法」[19]に詳しく述べられている．また，アメリカのプライバシー保護法制については，中川[20]，堀田[21]，湯淺[22]，石井[23]らの論文が参考になる．

†2）例えば，「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」[24]においては，『個人情報の漏えい等の問題が発生した場合には、二次被害の防止、類似事案の発生回避等の観点から、個人情報の保護に配慮しつつ、可能な限り事実関係を公表するとともに、都道府県の所管課等に速やかに報告する。』と規定している．

文　献

1）厚生労働省：医療等分野における番号制度の活用等に関する研究会. **http://www.mhlw.go.jp/stf/shingi/other-jyouhouseisaku.html?tid=197584**, 2015.（2016.9.1 確認）

2）NPO日本ネットワークセキュリティ協会：2014年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～第1.0版（2016年7月11日改定）. **http://www.jnsa.org/result/incident/data/2014incident_survey_ver1.1.pdf**, 2016.（2016.8.1 確認）

3）個人情報保護委員会：個人情報の保護に関するガイドラインについて（平成27年11月25日現在）. **http://www.ppc.go.jp/files/pdf/personal_guideline_ministries.pdf**, 2015.（2016.9.1 確認）

4）相澤直行：個人情報の事故事例から見た医療情報の安全管理．新医療，**35**(6)，121-124，2008.

5）相澤直行：医療情報の利活用と公認医療情報システム監査人．新医療，**39**(8)，106-111，2012.

6）品川佳満，橋本勇人：医療機関における患者の個人情報に関する事故の現状―電子媒体が関係したケースの分析―．医療情報学，**33**(6)，311-319，2014.

7）品川佳満，橋本勇人：医療機関における患者情報の取り扱い事故に関する経年変化―個人情報保護法制定後10年間の分析―．川崎医療福祉学会誌，**24**(1)，103-109，2014.

8）品川佳満，橋本勇人：患者の個人情報取扱い事故のパターンと違反したルールに関する分析．川崎医療福祉学会誌，**24**(2)，221-227，2015.

9）品川佳満，橋本勇人：看護師が関係した患者情報の取扱い事故の特徴に関する分析．日本医療情報学会看護学術大会論文集，**16**，188-191，2015.

10）橋本勇人，品川佳満：医療系学生による患者情報に関する事故の概要と対応―教育機関が把握しておくべき法的対応を中心として―．川崎医療短期大学紀要，**33**，49-54，2013.

11）橋本勇人，品川佳満：医療・福祉・教育系大学における個人情報保護教育の授業展開と改善：法教育と専門科目・卒後教育との連続性を見すえた実践．法と教育，**5**，19-29，2015.

12）品川佳満，橋本勇人：患者の個人情報取扱い事故に関する公表遅れの要因分析．日本医療マネジメント学会雑誌，**15**(4)，233-241，2015.

13）Kwon J and Johnson ME：Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*，**20**(1)，44-51，2013.

14）Firouzan PA and McKinnon J：HIPAA privacy implementation issues in Pennsylvania healthcare facilities. *Perspectives in Health Information Management*，**1**，2004.

15）Davis D and Having K：Compliance with HIPAA security standards in U.S. Hospitals. *Journal of Healthcare Information Management*, **20**(2)，108-115，2006.

16）Wikina SB：What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*，**11**(Fall)，2014.
17）US Department of Health and Human Services：“Breaches Affecting 500 or More Individuals.” **https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf**（2016.8.1 確認）
18）厚生労働省：医療情報システムの安全管理に関するガイドライン　第4.3版．平成28年3月．**http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000119598.pdf**, 2016.（2016.9.1 確認）
19）開原成允 , 樋口範雄編：医療の個人情報保護とセキュリティ　個人情報保護法と HIPAA 法．第2版，有斐閣，東京，2005.
20）中川かおり：米国における個人情報保護の動向―個人情報窃盗対策を中心に―．外国の立法，231，59-70，2007.
21）堀田周吾：個人識別情報の不正取得・不正使用に対する刑事訴追．駿河台法学，**23**(1)，214-192，2009.
22）湯淺墾道：アメリカにおける個人データ漏洩通知法制．日本セキュリティ・マネジメント学会誌，**26**(2)，24-34，2012.
23）石井夏生利：アメリカのプライバシー保護に関する動向．情報処理，**55**(12)，1346-1352，2014.
24）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24日（2010年9月17日最終改正）．**http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf**, 2010.（2016.8.1 確認）

（平成28年10月28日受理）

Schematization of the Cause of Data Breaches Involving Personal Health Information by Healthcare Providers that Occurred in the United States

Yoshimitsu SHINAGAWA and Hayato HASHIMOTO

（Accepted Oct. 28, 2016）

Key words : personal health information, data breach, HIPAA, HITECH

Correspondence to : Yoshimitsu SHINAGAWA Health Informatics and Biostatistics
Oita University of Nursing and Health Sciences
Oita, 870-1201, Japan
E-mail：shinagawa@oita-nhs.ac.jp
（Kawasaki Medical Welfare Journal Vol.26, No.2, 2017 264－272）