Topics

欧米のヘルスデータプラットフォームにおける「セキュリティ・プライバシー」規制の概況について

医薬産業政策研究所　統括研究員　森田　正実
医薬産業政策研究所　主任研究員　佐々木隆之
医薬産業政策研究所　主任研究員　中塚　靖彦

“Data is the new oil（データは新しい石油）”。この概念が社会に浸透し、急激にデータ駆動型社会へと変化するなか、様々な産業でデータを活用したビジネスが生み出されている。医療・健康をとりまく産業においても電子カルテ等のEHR（Electronic Health Record）に始まり、レセプトデータ、DPCデータ、さらにはゲノム・オミックスデータ等、様々な医療を中心としたデータを活用する動きが活発化している。さらにIoTの進展やデジタルバイオマーカーの開発といったデジタル化の流れが加速するに伴い、mHealth（mobile Health）やヘルスケア向けウェアラブル製品等も普及し、日常の行動やバイタルデータ等を可視化・デジタル化することが可能となりつつあり、医療のスナップショットデータのみならず、日々の生活や健康に関する情報（PHR[1)]）の利活用についても著しい進展がみられる。

これらのデジタル化されたヘルスデータ（ゲノム、医療情報、生活情報などを含む）を最大限に活用し、精密医療や先制医療を実現していくためには、それぞれをバラバラに活用するのではなく、統合された「デジタルヘルスインフラ」として構築していく必要がある。デジタルヘルスへの注力を拡大しているWHOにあっても、2019年４月に発行されたデジタルヘルスガイドライン[2)]において、統合されたデジタルインフラが必要であることに言及されている。また、デジタル化された保健サービスの効果的な実施を支援するために組織され、世界23か国が参加する“Digital Health Partnership”においては、更に踏み込んで、デジタルヘルスインフラの重要な要素として「サイバーセキュリティ」「相互運用性（Interoperability）」「エビデンスと評価」「ポリシーの環境（Policy Environments）」「臨床・患者エンゲージメント」が提示され[3)]、それぞれについてホワイトペーパーも作成されている[4)]。

ヘルスデータは機微性の高い情報であり、それらを統合的に取り扱うプラットフォームには、セキュリティ確保とプライバシー保護の観点がまず重要である。本稿では、プラットフォームの構築が進む欧米を中心に、セキュリティ確保とプライバシー保護から、特に法規制がどのように整備されているかを概括したい。

※）医薬産業政策研究所ではビッグデータの医薬産業に関する課題を研究するために、所内に『医療健康分野のビッグデータ活用･研究会』を2015年７月発足させた。今回の報告は、弁護士法人漆間総合法律事務所　吉澤　尚先生の講演など、『研究会』の調査研究に踏まえてまとめたものである。

※）ヘルスデータプラットフォームとは：様々なヘルスデータ（生活・行動データなどを含む）を活用するための、収集、蓄積、流通、統合、解析、マネジメント等を実施する際の個別の基盤システムや環境などを指す。複数の基盤システムや環境などを纏めた総体としてプラットフォームと称することもある。

１）医療健康分野のビッグデータ研究会は、効果的な医療の実現だけでなくヘルスケア関連産業全体の振興に向けたデータ流通の観点も見据え、ゲノム、オミックスデータやEHR（Electronic Health Record）、モバイルアプリやウェアラブルデバイス等により医療機関以外で取得されるデータも含めた生涯にわたって蓄積される「ライフコースデータ」として定義している。

２）WHO Guideline：recommendations on digital interventions for health system strengthening

３）https://www.gdhp.org/（2019/10/４参照）

４）https://www.gdhp.org/media-hub/news_feed/gdhp-reports（2019/10/４参照）

ヘルスデータプラットフォームの構築状況

【米国】

米国ではGAFA（Google社、Apple社、Facebook社、Amazon社）等の民間ITプラットフォーマーを中心としてヘルスデータのプラットフォーム化が加速している。例えばAmazon社はMERCK社、Accenture社と連携してPrecision Medicineのためのクラウドプラットフォーム構築[5]をし、医薬品、バイオテクノロジーの研究開発の増大・多様化する研究データをプラットフォーム化により、迅速かつ効率的に研究を推進させ、新しい治療法の発見を促進させることを目指している。

一方Google社は、Deloitte社と提携して人工知能ソリューション、臨床データウェアハウス、ゲノミクス、及び画像といった様々なデータを医療機関とライフサイエンス企業に提供するためのヘルスケアクラウドプラットフォームの構築を進め[6]、早期診断等の推進を目指している。

また、IBM社は豊富な医療データを医療AIへと拡大し、ヘルスケアライフサイエンス企業がIoT、ビッグデータを利活用可能なプラットフォーム構築を目指している。例えば、Watson for Oncologyでは医療データ、医療文献、専門家からのガイドライン等を分析し、エビデンスに基づく治療方針作成を支援する取り組みを行っている[7]。

以上のように民間の取り組みが中心ではあるが、国としての動きもある。例えば、米国立がん研究所（National Cancer Institute：NCI）は2017年にクラウドベースのインフラを整備したNCI Cancer Research Data Commons（CRDC）を発表している。本構想は医師、研究者などがゲノム・オミックスデータ等にアクセスし、がん研究とPrecision Medicineの加速化を目指すもので、関連するデータプラットフォームの整備を目標として掲げている[8]。

米国ではPrecision Medicine Initiative等のヘルスケア関連の政府戦略をNIH等の国家機関が支えつつ、GAFA等の巨大プラットフォーマーやアカデミア、先端医療機関、製薬企業、IT企業などが連携して、プラットフォームを構築している動きが顕著である。

ヘルスデータは機微性の高いデータとなるため、プラットフォーマーはプラットフォーム構築にあたりセキュリティ対策を施し、医療・医薬品産業における各種規制、法律を遵守している。また、各国のプライバシーポリシーや個人情報保護法に準拠し対応することが必要となる。

例えばGoogle社においては「ユーザーとそのプライバシーの尊重」、「収集データ内容と目的の明確化」、「ユーザーの個人情報を販売しないこと」、「ユーザー自身の自己管理」、「ユーザーのデータ所有権」、「最高水準のセキュリティ技術導入」、「セキュリティ強化の模範化」の７つを「プライバシーとセキュリティ原則」に定めている。さらには医療に係るプライバシー、及びセキュリティ標準を一元的に規定している「HIPAA」の要件に準拠したシステムを構築している[9]。

５）https://newsroom.accenture.com/news/accenture-and-merck-collaborate-with-amazon-web-services-to-launch-a-research-platform-to-drive-innovation-in-drug-discovery-and-scientific-research.htm（2019/９/25参照）

６）https://cloud.google.com/blog/topics/partners/deloitte-and-google-cloud-expand-their-alliance-to-bring-the-cloud-to-more-industries（2019/９/25参照）

７）https://www.ibm.com/watson/jp-ja/health/（2019/９/25参照）

８）https://datascience.cancer.gov/data-commons（2019/９/25参照）

９）https://safety.google/principles/?hl=ja（2019/10/10参照）

【欧州】

欧州では国の戦略として医療・ヘルスケア分野のプラットフォームを構築する動きがある。2000年ごろから世界に先駆けてEHRネットワークの構築が取り組まれ、医療情報のプラットフォーム化が進められている。

フィンランドでは、新しい医療プラットフォームとビジネス創出を目的としたPersonalized Health Finlandプログラムという取り組みを2018年より行っており、個別化医療・予防の促進を目的として、バイオバンク、健康データ、診療データ、処方データ等様々なデータのプラットフォーム化が盛り込まれている[10]。このように国が中心となって医療情報を始めとするヘルスケアのデジタル化を進めている事例はエストニアや英国、北欧諸国等、欧州には散見される。

EUにおけるゲノム情報について、2018年4月にはEU加盟13カ国（イタリア、エストニア、キプロス、スロバニア、スペイン、スウェーデン、チェコ、フィンランド、ポルトガル、マルタ、リトアニア、ルクセンブルク、英国）は「2022年までにEU域内で100万人ゲノムにアクセス可能とする」という目標を掲げたゲノム情報の越境アクセスに関する宣言書を採択[11]した。英国バイオバンクではこれまでに英国全域の約50万人の遺伝子治療データを収集しているが、シーケンシングやバイオバンクの構築等において、既に実施された加盟国の施策を、この13カ国で活用・最大化することとしている。

併せて、欧州では研究者が国境を越えて、信頼できる環境で膨大な量の研究データを保存、管理、分析、再利用し、臨床試験や臨床研究にリアルワールドデータを活用できるような環境整備が進められている。さらに、EUでは、「GDPR（一般データ保護規則）」[12]や、標準化などの施策を進めるとともに、ゲノム情報の越境利用を含むEuropean Open Science Cloud（EOSC）を展開[13]し、ゲノムデータと医療データの統合を目指している。

10）https://www.businessfinland.fi/en/for-finnish-customers/services/programs/personalized-health-finland/（2019/9/25参照）

11）https://ec.europa.eu/digital-single-market/en/news/eu-countries-will-cooperate-linking-genomic-databases-across-borders（2019/9/25参照）

12）https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC（2019/9/25参照）

13）https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud（2019/9/25参照）

ヘルスデータ利活用に関係する欧米の法規制

セキュリティ/プライバシー

ヘルスケア領域のプラットフォームを構築するにあたり、データが蓄積され活用される仕組み（データエコシステム）を並行して作る必要がある。その仕組みにおいてはデータセキュリティやプライバシーに関する整備を始めとした法制度の対応（アーキテクチャ）なども併せて重要となる。ここでは米国と欧州のセキュリティやプライバシーに関する主な法規制・ガイドラインについて纏めた。日本の制度も参考として表１に掲載する。

表１　セキュリティ/プライバシーに関する主な法規制・原則

	名称	施行時期/改正時期（直近）	概要	罰則	分類
米国	HIPAA （The Health Insurance Portability and Accountability Act） 医療保険の相互運用性と説明責任に関する法律	1996年 /2006年	個人の医療情報のプライバシーを守りつつ、データを医療の進歩に役立てることを目的とした法律	有	P/S
	HITECH （The Healthcare Information Technology for Economic and Clinical Health Act） 経済的及び臨床的健全性のための医療情報技術に関する法律	2009年	医療 IT の導入に際して想定されるようなセキュリティ・プライバシー条項の適用拡大や罰則強化を盛り込んだ法律	有	P/S
	CSF （Cybersecurity Framework） 重要インフラのサイバーセキュリティを向上させるためのフレームワーク	2014年	IT 世界のセキュリティリスクに特化したフレームワークであり、セキュリティ対策の強化を目的としたガイドライン	－	S
欧州	NIS Directive （Network and Information Security Directive） ネットワークおよび情報セキュリティ指令	2013年	各国での法制化及び、デジタルサービス提供者と交通、水、金融、医療等、重要なインフラサービス提供者にセキュリティ対策の強化と義務を求める指令	－	S
	GDPR （General Data Protection Regulation） 一般データ保護規則	2018年	個人の権利を強化（情報への権利、アクセスの権利、処理の制限権、忘れられる権利、データポータビリティ権等）し、個人データ保護の調和と統一性の強化を図った規則	有	P
日本	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針	2006年 /2018年	情報セキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を実現するための指針	－	S
	サイバーセキュリティ基本法	2014年 /2018年	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、サイバーセキュリティ戦略の策定、及びその他当該施策の基本となる事項等を規定	有	S
	個人情報の保護に関する法律	2003年 /2017年	個人情報の適正かつ効果的な活用を目指し、かつ、個人の権利利益を保護することを目的とした法律	有	P
	医療分野の研究開発に資するための匿名加工医療情報に関する法律 （次世代医療基盤法）	2018年	医療分野の研究開発に資するための匿名加工医療情報に関し、事業を行う者の認定、情報等の取扱いに関する規制等を定めることにより、健康・医療に関する先端的研究開発及び新産業創出を促進し、健康長寿社会の形成に資することを目的とした法律	有	P

P：Privacy
S：Security

【米国】

米国では医療情報の機密性を踏まえ、1996年に「HIPAA」[14]を制定し、さらに医療IT化を目的に2009年に「HITECH」[15]を制定した。これらの法律では医療に係るプライバシー、及びセキュリティ標準を一元的に規定しており、医療情報の保護責任をもつ事業体がプライバシーとセキュリティを確保するための対策を講じることが義務づけられている。「HIPAA」は個人の医療データのプライバシーを守りつつ、データを医療の進歩に役立てることを目的とした法律となっており、医療データを取り扱うIT企業などが個人情報保護を重視した基準として活用されている。

「HITECH」は、医療ITの導入に際して想定されるようなセキュリティ・プライバシー問題への対応策が「HIPAA」に含まれていなかったことから、「HIPAA」をより実効的にするため、プライバシー条項の適用拡大や罰則強化が盛り込まれた。

米国国立標準技術研究所（National Institute of Standards and Technology：NIST）が2014年２月12日に公表した「CSF（サイバーセキュリティフレームワーク）」[16]は、IT世界のセキュリティリスクに特化したフレームワークであり、セキュリティ対策の強化を目的としたガイドラインである。米国のセキュリティについては、NISTによって様々規格化されているが、クラウドインフラを前提としたマルチステークホルダーエコシステムの構築と、重要なシステムに対しての直接攻撃や情報漏洩を避けるために多層の防御を行なう分野横断型の多層防御の考え方がとられている。この点は、集中クラウド層、フォグノード層、エンドデバイス層*のITインフラ基盤を前提として多くのITインフラ企業が関わってセキュリティについて適切な管理を行うこととなる。また、米国には脅威情報の収集、共有や警告などの業界別の情報共有分析組織（Information Sharing and Analysis Center：ISAC）が数多く存在しており、現在はさらに広範なカテゴリを網羅する情報共有分析機関（Information Sharing and Analysis Organization：ISAO）によって補完されつつある。なお、米国では国土安全保障省が業界横断的にセキュリティの管轄を行っている。

【欧州】

2018年５月25日に「GDPR」が施行され、企業による個人データの取得利用が規制された。個人の権利を強化（情報への権利、アクセスの権利、処理の制限権、忘れられる権利、データポータビリティ権等）し、個人データ保護の調和と統一性の強化がなされた。「GDPR」が適用されない地域の企業に対しても、「GDPR」と同レベルのデータ保護義務が課されることとなる。「GDPR」は個人データの処理に適用され、対象者としてはEU域内に拠点をもつデータ管理者と処理者に適用される[17]。また、EU域内の個人に対し商品、サービスを提供し、個人データを処理、または監視するデータ管理者、処理者にも適用される。

「GDPR」はEU域内の統一ルールであり、加盟国全体への拘束力を持っている。各国はこの統一ルールに則り各々法規制を定める必要がある。

「NIS指令（ネットワークと情報システムのセキュリティに関する指令）」[18]は2016年５月17日にEU理事会で採択され、同年８月８日に発効している。EUの全体的なサイバーセキュリティを高めるための指令で、EU加盟国の重要インフラ（エ

＊集中クラウド層、フォグノード層、エンドデバイス層：加工されたデータの活用や他サービスとの連携を担う集中クラウド層、デバイスから収集したデータの１次処理を担うフォグノード層、製品で構成されるエンドデバイス層

14）https://www.hhs.gov/hipaa/index.html（2019/９/25参照）

15）https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html（2019/９/25参照）

16）https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf（2019/９/25参照）

17）JETRO「EU一般データ保護規則（GDPR）について」 https://www.jetro.go.jp/world/europe/eu/gdpr/（2019/９/25参照）

18）https://eur-lex.europa.eu/eli/dir/2016/1148/oj（2019/９/25参照）

ネルギー、交通、金融等、）事業者など、社会基盤となるサービスを提供する組織にセキュリティ対策の強化と義務を求めるものである。ただし、本指令は法令そのものではなく、EU 加盟各国それぞれに対し国内法を定めるように指示するものとなる。そのため、各国における法制度については異なることに留意する必要がある。NIS 指令は欧州内のミニマムスタンダードであり、実際の法令設定や運用は各国当局に委ねられている。

例えば、EU 加盟国のドイツでは NIS 指令に先立ち2015年に「IT セキュリティ法」を制定[19]し、サイバーセキュリティに関する最低限の基準を満たしている証明を情報セキュリティ庁から得ること、セキュリティ監査を定期的（隔年毎）にうけること、サイバー攻撃を受けた際には情報セキュリティ庁へ報告することを主要・重要インフラ事業者に対して要求している。違反時の罰則規定もある。英国も「ネットワーク・情報システム法」を2018年に定め[19]、重要インフラ事業者に対し効果的なサイバーセキュリティ対策を講じることを求めており、GDPR だけではなくセキュリティにも厳しい課徴金制度があるので注意が必要である。

欧州のセキュリティについては、European Security Certification Framework（EU-SEC）[20]と呼ばれるセキュリティのフレームワークについての認証の仕組みが出来上がっており、このフレームワークは情報セキュリティマネジメントシステム（Information Security Management System：ISMS*）の延長線上での設計となっている。

まとめ

わが国においては内閣官房内閣サイバーセキュリティセンター（NISC）が「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）改定」（案）[21]の策定を行い、2019年４月19日には意見募集を行っている。(2019年９月25日現在、意見募集は終了している。)

３省（厚生労働省・総務省・経済産業省）ガイドラインにおける医療情報の取り扱いについても、各種指針において一部委託や第三者提供などの責任範囲の明確化はされているが、ヘルスデータの Application Programming Interface（API）にかかるセキュリティの議論は各種指針においても検討することが必要であろう。また、多層防御の考え方や、各層においてマルチステークホルダーによる対応も含めたセキュリティ対策の考え方についても検討が望まれる。欧州ではセキュリティに関する認証制度も取り入れられており、日本企業にとっても精査すべき認証であると考える。

データ駆動型の社会や研究の環境を整えるためにはプラットフォームの構築が重要であることに議論の余地はないが、データエコシステムが作られていることが併せて重要であり、さらにデータセキュリティやプライバシーに関する法制度の整備も同時に始めていく必要がある。

今後、プラットフォームの構築を行う上で、医療データベースが IT ネットワークや IoT デバイスにつながっていくと、API におけるセキュリティの対応がより厳格になるものと思われ、特に進化の速い米国のクラウド基盤技術を前提としたセキュリティの規格基準作りの動向は日本も早急にキャッチアップする必要があるものと思われる。

＊ ISMS：情報の「機密性」、「完全性」、「可用性」の確保からなる、情報セキュリティを管理する仕組み。

19）諸外国のサイバーセキュリティ、及び個人情報保護に関する法律まとめ　https://www.j-cic.com/pdf/report/Cybersecurity-Privacy-Law.pdf

20）https://www.sec-cert.eu/（2019/10/４参照）

21）重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）　https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf