別添４

厚生労働科学研究費補助金（長寿科学政策研究事業）
分担報告書

EUにおける介護事業所の情報安全管理措置に関する研究

研究分担者　大寺　祥佑　　国立長寿医療研究センター医療経済研究部・副部長
大西　丈二　　国立長寿医療研究センター老年内科部・医長

研究要旨

本研究では、EUにおける介護事業所の情報安全管理措置を対象に、制度的枠組みと実践的対応の実態を文献により調査した。GDPRやNIS2に基づく個人情報保護義務、ENISAや欧州委員会による中小事業所支援策を整理し、加えてフィンランドの「Kanta」システムを先進事例として情報を整理した。その結果、EUにおいては法制度・技術支援・教育を組み合わせた多層的対策が実装されていることが確認された。日本においても、介護分野における情報基盤の整備とセキュリティ強化に向け、EUの知見が有用な示唆を与えるものと考えられた。

Ａ．研究目的

ICT（情報通信技術）の進展に伴い、個人情報の管理と保護は、EU 全体で極めて重要な課題となっている。介護や医療を扱う小規模な事業所では、限られた人的・物的・経済的リソースの中で、情報の安全管理を確保する必要があり、配慮を要する。

本研究では、EU における介護事業所の情報安全管理措置について、WEB 調査およびヒアリング調査を行い、法的な枠組み、リスク、ガイドライン、実践的対応策等を収集し、対策について検討する。

Ｂ．研究方法

文献検索によって、EU における小規模の医療・介護事業所での情報安全管理措置に関する指針、規程、調査等を調査した。また先進的な事例のひとつとしてフィンランドにおける医療介護情報基盤である Kanta について調べた。

（倫理面への配慮）

本研究は個人の情報を一切扱わず、人を対象とする生命科学・医学系研究に関する倫理指針の対象外である。

Ｃ．研究結果

1. EU における介護事業所の個人情報保護とサイバーセキュリティ政策

欧州連合（EU）は、介護・医療分野における個人情報保護とサイバーセキュリティの強化に積極的に取り組んでいた。2018 年に施行された一般データ保護規則（General Data Protection Regulation, GDPR）は、介護事業所を含むすべての組織に対して個人情報の厳格な管理を義務付けており、透明性、正当性、データ主体の権利保護を基本原則としていた[1]。

加えて、重要インフラ事業者を対象とした「ネットワーク・情報システム指令（NIS2)」が 2023 年から施行され、介護事業所のような社会福祉サービス提供機関もその対象とされるようになった[2]。この制度は、サイバーインシデントへの対応能力向上、インシデント報告義務、組織的なリスク管理体制の構築を求めていた。さらに、欧州委員会による包括的なサイバーセキュリティ政策[3]や、ENISA による年次の脅威分析[4]は、介護を含む社会的サービス領域におけるリスク認識の向上に貢献していることがわかった。

患者・利用者の機微な個人情報を多数取り扱う介護事業所にとって、これらの制度は単なる規制ではなく、信頼性と質の高いサービス提供の前提条件である。最近の研究では、患者データ保護の強化が、ケアサービスの質向上にも寄与することが指摘されていた[5]。

2. EU における中小介護事業所の課題と支援策

EU 内の介護事業所の大多数は中小規模であり、こうした事業所では情報安全管理に関する人材・予算の確保が困難な場合が多いとの指摘があった。ENISA は中小事業者向けに特化した支援ガイドラインを発行し、アクセス制御、データ暗号化、職員教育など、基本的な対策の実施を促していた[6]。また、Segovia らの研究では、こうした中小介護施設が情報セキュリティの実装において直面する技術的・組織的障壁が明らかにされていた[7]。

ENISA の中小企業向けサイバーセキュリティガイド[8]や、eHealth Action が発表した共通セキュリティフレームワーク[9]は、介護を含む地域密着型サービス提供者にとって有用な参考資料となっていた。さらに、2025 年には EU 委員会が病院や介護施設を含む医療・福祉機関向けのサイバーセキュリティ行動計画を打ち出し、支援体制の整備と資金的支援が開始された[10]。

3. 介護事業所におけるリスク管理とインシデント対応

介護施設では、日常的に高齢者の健康情報、生活状況、家族関係に関するデータを取り扱うため、データ流出・改ざん・不正アクセスのリスク管理は不可欠である。ENISA は、介護を含む社会福祉分野向けのリスク管理ガイドラインを提供し[11]、資産の特定、脅威分析、脆弱性評価と対応優先順位設定を推奨していた。

また、インシデント発生時の対応についても、ENISA は対応マニュアル[12]を公開し、封じ込め、復旧、再発防止策までを網羅した対応フローの整備を支援していた。EDPB による中小事業者向けガイドライン[13]は、介護事業所が個人情報保護を確保するための具体的手順を示しており、ECSO（欧州サイバーセキュリティ機構）は人的リソースやコンサルティング支援も行っていた[14]。

さらに、欧州委員会が策定した医療・介護分野横断のサイバーセキュリティ行動計画[15]は、介護事業所のデジタルインフラ整備と職員の IT リテラシー向上を促進するための包括的戦略を示していた。

4. フィンランドにおける先進的な介護情報基盤の整備

フィンランドでは、医療と福祉を統合する全国情報基盤「Kanta」が整備されており、介護分野においても高度な情報連携が実現していた[16]。電子処方（ePrescription）、診療・福祉記録の統合リポジトリ、国民向けポータル「MyKanta」などを通じて、国民は自身の健康・介護情報にアクセス可能であり、関係者間での情報共有が暗号化・認証付きで行われていた。

2023 年の制度改革により、福祉サービス提供体制が 22 の福祉サービス県（Wellbeing Services Counties）とヘルシンキ市に統合され、医療・福祉・救急サービスが一体運営される仕組みが導入された。これに伴い、介護記録の全国的な標準化・共有も進んでおり、2026 年までに完全な情報一体化が計画されていた。

Kanta の設計思想は「患者・利用者中心」「一元的記録管理」「国民のアクセス権の保障」にあり、将来的には AI を活用した意思決定支援や国際的な情報連携（MyHealth¥@EU）との統合も見据えられていた。

さらに、EU の「Health Data Access Body」について調査した。Health Data Access Body の主体は国によって異なり、これらをまとめた概要が表である。EU においては、EHDS が開発され、各国の「Health Data Access Body」がインターフェースとなって EHDS にデータ提供およびデータ参照を行っている。

（表１）

国名	実施機関	内容
アイルランド	アイルランド保健省（Department of Health） 健康情報と品質機関（HIQA: Health Information and Quality Authority） 健康研究委員会（HRB: Health Research Board）	HealthData@IE プロジェクトでは、データアクセス申請管理システム（DAMMS）、安全なデータ処理環境（SPE）、国家健康メタデータカタログの構築が進められています。
ドイツ	連邦保健省（Bundesministerium für Gesundheit, BMG） ドイツデータ保護監督機関（Federal Commissioner for Data Protection and Freedom of Information, BfDI）	データアクセス条件の公開、データの匿名化、セキュアな処理環境の構築が検討されています。
ルクセンブルク	ルクセンブルク保健省（Ministère de la Santé, Luxembourg） eHealth Agency Luxembourg（Agence eSanté Luxembourg）	患者が自国の医療記録に外国からもアクセスできる仕組みを整備し、患者のエンパワーメントを促進しています。
フランス	フランス国立健康データ研究所（Health Data Hub, HDH） フランス保健省（Ministère des Solidarités et de la Santé）	電子健康記録（EHR）の相互運用性の向上を目指し、EHDS の規則に適合するためのデータ基盤を強化しています。患者が自分の健康データにアクセスし、情報を修正したり、医療従事者へのアクセスを制限したりできるシステムを開発中です。
ベルギー	ベルギーeHealth プラットフォーム（eHealth Platform Belgium） ベルギー連邦公衆衛生省（FPS Public Health, Food Chain Safety and Environment）	EHDS のガバナンスに積極的に関与し、EU のルール策定にも貢献しています。データアクセスを管理する中央機関を設置し、透明性の向上とデータの可視化を進めています。
フィンランド	Findata（Sosiaali- ja terveysalan tietolupaviranomainen, Social and Health Data Permit Authority）	データ許可の発行：研究者、政策立案者、企業が医療および福祉データにアクセスできるようにデータ許可証を発行します。 データ管理の効率化：データの収集、連携、事前処理を行い、データ利用者が分析に使用できるように準備します。 技術サポート：Findata はセキュアな処理環境（Secure Processing Environment,

		SPE)を運用し、Kapseli と呼ばれるデータ処理プラットフォームを提供しています
スウェーデン	Swedish eHealth Agency (eHälsomyndigheten)	電子処方箋のクロスボーダー管理を行い、HDAB としての役割を果たしています。スウェーデンの MyHealth@EU への参加により、EU 加盟国間の医療データの円滑な共有を促進しています。
オランダ	MedMij (データ交換標準化機関) Zorginstituut Nederland (保健研究所)	患者が自らの健康データにアクセスできるデジタル環境の構築を行い、データ共有を可能にする MedMij フレームワークを開発しています。国際的な医療データの標準化と相互運用性の確保に取り組んでいます。
スペイン	Ministerio de Sanidad (保健省)	EHDS の枠組みに基づき、国家的な HDAB の設立を行っています。 医療機関や研究機関にデータアクセスを提供するため、セキュアな処理環境を構築しています。

D．考察

本研究では、EUにおける介護事業所を対象とした情報安全管理措置の制度的枠組みと実装状況を整理し、特にGDPR、NIS2、ENISA等の施策が中小規模の介護事業者に与える影響と支援の実態に焦点を当てた。EUの制度設計では個人情報保護とサイバーセキュリティを一体化した包括的な枠組みを構築しており、かつ現場実装に向けて多様な支援策を伴っていた。これにより、介護現場でのリソース不足、技術力不足といった構造的課題に対して、制度と運用の両面から対応する基盤が整備されていた。

特に、GDPRが定める「データ主体の権利」や「目的限定性」等の原則は、介護事業所が利用者情報を取り扱う際の実務的ガイドラインとなり得る。またNIS2では、社会福祉領域を含む重要サービス事業者として介護事業所を対象とし、リスク評価、セキュリティ対策、インシデント報告といった対応能力を制度的に求めている点が新しい。こうした政策的枠組みに対し、ENISAやEDPB、ECSOといった専門機関がガイドラインやツールを通じて現場支援を行っており、政策実装のための中間支援インフラが制度的に位置づけられていることが、EUの大きな特徴と言える。

一方、日本では介護事業所の情報化は進んできたものの、セキュリティ対策は未だ施設間格差が大きく、支援制度も限定的と考えられる。科学的介護情報システム（LIFE）を含む匿名介護保険等関連情報データベース（介護保険総合データベース、介護DB）などデータ基盤の活用が広まりつつあるが、それらを支える制度的セキュリティ設計や運用ガイドラインは発展途上にある。EUのように「制度」「実装支援」「教育・人材育成」が連携した枠組みを構築することが、日本の今後の政策課題といえる。

また、フィンランドの事例が示すように、介護と医療を統合した情報基盤の構築は、ケアの質向上と業務効率化、国民のデータアクセス権を同時に実現する可能性を示している。Kantaは、全国的に一元化された構造化データの運用と、市民ポータルを通じた当事者アクセスを実現しており、これは高齢化が進む日本にとって極めて有用な参考事例である。

さらに、日本の制度設計においては、セキュリティ対策を「現場負担」ではなく「公共的インフラ整備」と捉える視点の転換が求められる。EUの取り組みに学ぶことで、技術的・財政的支援、標準化、研修制度の整備などを通じて、情報安全管理を介護現場に浸透させる仕組みの設計が可能となる。

以上より、EUの制度的取り組みと先進事例は、単なる法制度の比較を超えて、介護の質と情報の保護を同時に達成するための実装モデルを提示しており、日本にとって有効な戦略構築の基盤となり得ると考えられる。したがって、今後は日本の制度と現場の特性に適応させた形で、EUを含む諸外国の知見も取り込む体系的な政策設計とエビデンスに基づく支援体制の整備が求められる。

E．結論

EUにおける介護事業所の情報安全管理は、法的・技術的・教育的支援が統合された多層的な枠組みにより支えられていた。中小介護事業所に対しては、ENISAやEDPBによる具体的ガイドラインや支援制度が充実しており、介護現場の実情に即した対応が可能になっていた。

また、フィンランドのKantaシステムに見られるように、介護と医療を一体化した情報基盤と市民ポータルの整備は、個人情報の保護とケアの質向上を両立させるものである。日本においても、介護保険データやLIFEを活用した情報統合の動きが進む中で、EUの制度的アプローチと標準化の経験は重要な指針となると考えられる。

今後は、個人情報保護とサービスの質の向上を同時に実現する観点から、日本の介護事業所にお

ける情報安全管理の戦略を再構築し、EUとの制度比較を通じて最適な実践モデルを構築していく必要がある。

1. GDPR.eu. General Data Protection Regulation (GDPR). https://gdpr-info.eu/ (2025/3/30 アクセス)

2. Network and information systems (NIS), 2 Directive. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333. (2025/3/30 アクセス)

3. European Commission. Cybersecurity Policies | Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. (2025/3/30 アクセス)

4. ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. (2025/3/30 アクセス)

5 van Kessel R, Haig M, Mossialos E
Strengthening Cybersecurity for Patient Data Protection in Europe
J Med Internet Res 2023;25:e48824

6, ENISA. Cybersecurity for SMEs - Challenges and Recommendations. 2022. https://www.enisa.europa.eu/publications

7.Segovia P, et al. Barriers to Cybersecurity in Small Healthcare Providers. Comput Secur. 2023;129:102889.

8. ENISA. Cybersecurity guide for SMEs. 2021. https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

9. eHAction. Common Security Framework for eHealth. 2021. https://ehaction.eu/wp-content/uploads/2021/06/eHAction-D7.3.pdf

10. Sidley Austin LLP. EU Commission Launches Cybersecurity Action Plan for Hospitals. 2025. https://datamatters.sidley.com

11. European Union Agency for Cybersecurity (ENISA). Risk Management Guidelines. 2022. https://www.enisa.europa.eu/topics/risk-management

12. ENISA. Incident Response Plan Guide. 2022. https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management

13. EDPB. Data Protection Guide for Small Businesses. 2023. https://www.edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business_en

14. European Cybersecurity Organisation (ECSO). Cybersecurity Support Services. 2023. https://ecs-org.eu

15. European Commission. Digital Health and Cybersecurity in EU. 2024. https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers

16. 木村映善, 大寺祥佑, 佐々木香織, 黒田知宏. フィンランドにおける医療分野レジスタとデータ提供の状況. 日本統計学会誌 2020;50(1):47-80.

F．研究発表

1. 論文発表
該当なし

2. 学会発表
該当なし

G．知的財産権の出願・登録状況

該当なし