

# H-ISAC Japan Council



日米合同ワークショップ 2024

U.S.-Japan Joint Workshop 2024

2024 年 6 月 15 日 (土)

Saturday, June 15, 2024

## アジェンダ

08:50 - 09:05	Room1	開会あいさつ＋基調講演1「最近の脅威情勢と Health-ISAC の最新情報」 Health-ISAC デニス・アンダーソン
09:05 - 09:15	Room1	基調講演2「日本の医療機関におけるサイバーセキュリティ 2024」 医療 ISAC 深津博
09:15 - 09:55	Room1	基調講演3「米国におけるヘルスケア領域のサイバーインシデントの現状と FBI の取り組み」 FBI 特別捜査官 リリー・チェン
10:00 - 10:45	Room1	探索し対策せよ！アプリケーションリスクのマネジメント Texas Health Resources ロジャーズ・ニュンジャ (Web)
11:00 - 11:40	Room1	医療機関におけるランサムウェア対策(仮題) 警察庁サイバー警察局 澄川拓巳
11:45 - 12:15	Room1	サイバーリスク検出を目的とした機械学習アルゴリズムの構築 Cardinal Health スリニ&アナ (Web)
12:15 - 13:00		(昼食)
	Room1	ランチョンパネルディスカッション「医療安全と医療サイバーセキュリティ」 東京工科大学 田仲浩平／デニス・アンダーソン／深津博
13:00 - 13:45	Room1	JIS T 81001-5-1 へのコンプライアンスの確保:医療機器ソフトウェアセキュリティの成功戦略 日本ベクトン・ディッキソン 岡山太郎
	Room2	医療分野における重要インフラ防護の在り方 ～地域型官民連携の重要性の台頭～ 名古屋工業大学 渡辺研司
13:50 - 14:35	Room1	タケダの AI テクノロジーおよびサイバーリスク 武田薬品工業 笹山明 (Web)
	Room2	ランサムウェア対策としてのバックアップ Cohesity Japan 磯辺真／春日井市民病院 馬場隼人
14:40 - 15:25	Room1	医療機器のプロダクトセキュリティにおける主要な課題 Cybellum 池川史憲
	Room2	医療セキュリティにおける<BCP>とは何か 医療 ISAC 江原悠介
15:30 - 15:25	Room1	喫緊の課題 脆弱性対策・ランサムウェア対策を進めるには ジュピターテクノロジー 太田 道子
	Room2	医療機関におけるサイバー保険の選び方 あいおいニッセイ同和損保 神山太朗
16:20 - 17:05	Room1	医療機関におけるサイバーセキュリティ対策チェックリスト(令和 6 年度版対応)への具体的な 対応方法 パーソルプロセス&テクノロジー 谷昌行
	Room2	医療機関におけるゼロトラストとは ～ユースケースから見るゼロトラスト思考の活用例～ Zscaler 井上尚人
17:10 - 17:30	Room1	閉会挨拶 医療 ISAC 舟橋真

※Room1 のセッションは同時通訳となります

## Agenda

08:50 - 09:05	Room1	Opening Remarks & Keynote Speech 1 : The Recent Threat Landscape and H-ISAC Update Denise Anderson, President, Health-ISAC
09:05 - 09:15	Room1	Keynote Speech 2 : Cyber Security for Medical Sector 2024 Hiroshi Fukatsu, Medical ISAC Japan
09:15 - 09:55	Room1	Keynote Speech 3 : Status Quo of Cyber Security in US Healthcare and the Assault by FBI Lily Chen, Special Agent, Federal Bureau of Investigation (FBI)
10:00 - 10:45	Room1	Look for it, Do Something!: Managing Application Risks Rogers Nyunja, Texas Health Resources (Web)
11:00 - 11:40	Room1	Ransomware Countermeasures in Healthcare Organizations (Variable) Takumi Sumikawa, Japan Police Agency
11:45 - 12:15	Room1	Build machine learning algorithms to detect cybersecurity risks Srini Balasubramanian & Ana Carmela, Cardinal Health (Web)
12:15 - 13:00		(Lunch Time)
	Room1	Luncheon Mini Panel Discussion ; Medical Safety and Medical Cyber Security Kohei Tanaka, Tokyo University of Technology / Denise Anderson / Hiroshi Fukatsu
13:00 - 13:45	Room1	Ensuring Compliance with Japan IEC 81001-5-1: Strategies for Success in Medical Device Software Security Taro Okayama, Nippon Beckton Dickinson
	Room2	Critical Infrastructure Protection in the Healthcare Sector Kenji Watanabe, Nagoya Institute of Technology
13:50 - 14:35	Room1	AI Technology & Cyber Risk in Takeda Akira Sasayama, Takeda Pharmaceuticals (Web)
	Room2	Ransomware Backup Solutions Makoto Isobe, Cohesity Japan/Hayato Baba, Kasugai Municipal Hospital
14:40 - 15:25	Room1	Key challenges in medical device product security Fuminori Ikegawa, Cybellum
	Room2	What is “BCP” in medical security? Yusuke Ehara, Medical ISAC Japan
15:30 - 15:25	Room1	How Should Medical Institutes address 2 Pressing Cybersecurity Issues, Vulnerabilities and Ransomware attacks? Michiko Ota, JupitarTechnology
	Room2	How to Choose Cyber Insurance for Your Medical Organization Taro Kamiyama, Aioi Nissay Dowa Insurance
16:20 - 17:05	Room1	Specific measures to be taken in response to the Checklist of Cyber Security Measures for Medical Institutions (2024 version) Masayuki Tani, Persol Process & Technologies
	Room2	What is Zero Trust in Healthcare Organizations? Naoto Inoue, Zscaler
17:10 - 17:30	Room1	Closing Remarks Makoto Funahashi, Medical ISAC Japan

※Simultaneous interpretation will be available for Room1 sessions only.

## 登壇者のプロフィールと講演要旨

### Speaker Profiles & Abstract

8:50-9:05 Room1 241A1

基調講演 1: 最近の脅威情勢と Health-ISAC の最新情報

Keynote Speech 1: The Recent Threat Landscape and Health-ISAC Update

Health-ISAC 代表 デニス・アンダーソン

Denise Anderson, President of Health-ISAC

#### Profile

デニス・アンダーソン(MBA)は、信頼できるタイムリーな情報の発信を通じて、物理的およびサイバー攻撃やインシデントから医療セクターを保護することを目的とした非営利団体の Health Information Sharing and Analysis Center (H-ISAC) のプレジデントを務めます。

デニスは現在、National Council of ISACs の議長を務め、Global Resilience Federation (GRF) の理事を務めるほか、多くの業界団体やイニシアチブに参加しています。最近では、健康・公衆衛生セクター調整協議会のサイバーワーキンググループ執行委員会の3年任期に選出されました。

また、国際的なクレジット協会の役員および社長を務め、世界各地のイベントで講演を行っています。

バージニア州で20年間、救急救命士(B)、消防士 I/II、指導員 I/II の資格を取得し、バージニア州フェアファックス郡の消防救助アカデミーで10年間、非常勤講師を務めていました。

海軍大学院の国土防衛・安全保障センターでエグゼクティブ・リーダーズ・プログラムを修了。



Denise Anderson, MBA, is President of the Health Information Sharing and Analysis Center (H-ISAC), a non-profit organization dedicated to protecting the health sector from physical and cyber attacks and incidents through dissemination of trusted and timely information.

Denise currently serves as Chair of the National Council of ISACs, sits on the Board of Directors for the Global Resilience Federation (GRF) and participates in a number of industry groups and initiatives. She was recently elected to a 3-year term on the Cyber Working Group Executive Committee for the Health and Public Health Sector Coordinating Council. In addition, she has served on the Board and as Officer and President of an international credit association, and has spoken at events all over the globe.

Denise was certified as an EMT (B), and Firefighter I/II and Instructor I/II in the state of Virginia for twenty years and was an Adjunct Instructor at the Fire and Rescue Academy in Fairfax County, Virginia for ten years. She is a graduate of the Executive Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.

#### Abstract

デニスの講演では、第1四半期の Health-ISAC 活動について簡単な最新情報を提供した後、最近の統計や活発な脅威行為者グループなど、現在の世界的な脅威の状況について簡単な概要を説明するとともに、今後の規制とサイバーセキュリティ部門、特に CISO への影響についても触れます。

Ms. Anderson will provide a brief update on first quarter Health-ISAC activities and will then offer a brief overview of the current global threat landscape including recent statistics and active threat actor groups. She will also touch on upcoming regulation and implications for cybersecurity departments, especially CISOs.

9:05-9:15 Room1 241A2

## 基調講演 2: 日本の医療機関におけるサイバーセキュリティ 2024

### Keynote Speech 2: Cyber Security for Medical Sector 2024

医療 ISAC 代表理事 深津 博

Hiroshi Fukatsu, Representative Director of Medical ISAC Japan

#### Profile

医療 ISAC 代表理事

愛知医科大学医療情報部特任教授、放射線科専門医、  
社会医学専門医・指導医

1985 年 名古屋大学医学部卒業

2000 年より名古屋大学医学部附属病院准教授

2006 年より日本医療コンシェルジュ研究所代表

医療コンシェルジュの育成(1000 名以上)

医師事務作業補助者の基礎知識研修

(2000 名以上)を実施。

2009 年より現職

2014 年より一般社団法人メディカル IT セキュリティフォーラム

代表理事に就任

2019 年 10 月、団体名を一般社団法人医療 ISAC に改名

同年米国 Health ISAC と包括業務提携を締結



Hiroshi Fukatsu MD, Medical ISAC Japan Representative Director, Professor & Manager of Medical Informatics Division, Aichi Medical University Hospital, Certified Radiologist, Certified Social Medicine Trainer

Graduated from Nagoya University school of Medicine in 1985.

Became Assistant Professor, Nagoya University Hospital in 2000.

Shifted to the current status since 2009.

Also plays a role as the representative director of Japan Medical Concierge Research Institute in 2006

Offered medical concierge training course for more than 1000 students, also offered basic training for medical clerk for more than 4000 students.

Founded Medical IT Security Forum in 2014 and became the representative officer.

Organization name changed to Medical ISAC Japan in October 2019

Established a comprehensive alliance with Health ISAC in 2019.

#### Abstract

2021-2023 年の日本の医療機関におけるランサムウェア被害の多発を受けて、国主導の様々な動きが急速に進行している。またランサムウェア以外の被害也多発している。

本講演では現状認識の共有し、今後の対策方法についての考え方を提案する。

Various measures for cybersecurity driven by the government are promoted after multiple cyber attacks on medical facilities from 2021 to 2023. Also many non-ransomware victims are reported.

In this report, we will share the current situation and suggest the future concept for cybersecurity management.

**9:15-9:55 Room1 241A3 (Materials are not open to the public, so projection only.)**

**基調講演 3: 米国におけるヘルスケア領域のサイバーインシデントの現状と FBI の取り組み**

**Keynote Speech 3: Status Quo of Cyber Security in US Healthcare and the Assault by FBI**

**FBI 特別捜査官 リリー・チェン**

**Lily Chen, Special Agent, Federal Bureau of Investigation (FBI)**

Profile

FBI(連邦捜査局) 特別捜査官

駐日米国大使館 法務官事務所 副法務官

Special Agent, Federal Bureau of Investigation (FBI)

The U.S. Embassy, Tokyo, Legal Attache Office, Assistant Legal Attache

Abstract

重要インフラは、現在もサイバー犯罪の標的となっている。医療業界におけるサイバー攻撃の脅威に対する理解を深めることは、パートナーの皆さまがネットワーク保護を可能な状態にするための必要不可欠なものである。本講演では、直近の医療業界に影響を与える犯罪トレンドと犯罪統計、情報共有の重要性とその方法、重要インフラの脆弱性と保護するための緩和策、ベストプラクティス、重要インフラの保護するために利用可能なリソース等を説明します。

Critical infrastructure continues to be a target for cyber criminals. Understanding the current top healthcare cyber threats is essential for industry partners to be able to safeguard their networks. This presentation will cover recent crime statistics and trends affecting the healthcare industry, the importance and methods of information sharing, vulnerabilities, and mitigation measures to protect critical infrastructure, best practices, and resources available to help protect critical infrastructure.

**10:00-10:45 Room1 241A4**

**探索し対策せよ！アプリケーションリスクのマネジメント**

**Look for it, Do Something! Managing Application Risks**

**Texas Health Resources ロジャーズ・ニュンジャ**

**Rogers Nyunja, Texas Health Resources**

Profile

Texas Health Resources のアプリケーション・セキュリティ、およびデジタル・エクスペリエンス担当ディレクターで、組織内のアプリケーション・セキュリティとビジネス情報セキュリティを統括しており、サイバーセキュリティとテクノロジーにおける熟練したエグゼクティブリーダーです。

同社のアプリケーション・セキュリティ、およびビジネス情報セキュリティ・プログラムを一から構築。ビジョン、イノベーション、オペレーショナル・エクセレンスを融合させ、組織の卓越性を推進しています。

金融、小売、そして現在ではヘルスケアなど、さまざまな業界で実績のあるロジャーズは、変革的なイニシアチブをリードし、インパクトのある結果を出す能力を発揮しています。



Rogers Nyunja is the Director of Application Security and Digital Experience at Texas Health Resources, leading application security and business information security within the organization. Rogers is an accomplished executive leader in Cybersecurity and Technology. He has built the application security and business information security program for Texas Health Resources from the ground up. He brings a blend of vision, innovation, and operational excellence to drive organizational excellence. With a proven track record across diverse industries including finance, retail and currently healthcare, Rogers demonstrates my ability to lead transformative initiatives and deliver impactful results.

#### Abstract

「Look for it, Do something」は、リスク・エクスポージャーを見つける方法と、見つけた時に何をすべきかについて考察します。これはアプリケーション・リスク・マネジメントの実践であり、職場や生活における日常的な状況に関連づけながら、実践的な方法を考えます。より安全にリスク・エクスポージャーを発見し、それに対して何かをすることができるようになることを実感しながら、楽しく軽快な雰囲気の中で進めていきます！

Look for it, Do something looks into how to find risk exposures and what to do when we find them. This is Application Risk Management in practice, considering practical ways to go about while relating it to our everyday situation in your workplace and in life. This is going to be fun and lighthearted, knowing you are safer finding risk exposures and doing something about it!

**11:00-11:40 Room1 241A5**

#### **医療機関におけるランサムウェア対策(仮題)**

#### **Ransomware Countermeasures in Healthcare Organizations (Variable)**

**警察庁サイバー警察局 澄川拓巳**

**Takumi Sumikawa, Japan Police Agency**

#### Profile

警察庁サイバー警察局サイバー企画課サイバー事案防止対策室対策推進第一係 課長補佐

Assistant Director, Cyber Incident Prevention Office, Cyber Planning Division, Cyber Police Bureau,

National Police Agency

**11:45-12:15 Room1 241A6**

#### **サイバーリスク検出を目的とした機械学習アルゴリズムの構築**

#### **Build machine learning algorithms to detect cybersecurity risks**

**Cardinal Health スリニ&アナ**

**Srini Balasubramanian & Ana Carmela, Cardinal Health.**

#### Abstract

特注の機械学習アルゴリズム(RFC や DBSCAN など)を活用して、サイバーセキュリティのリスクを検出します。洗練された脅威検出システムを構築しながら、サイバーセキュリティと機械学習の重要な結びつきを調査する。絶えず変化するサイバー脅威に対してデジタルセキュリティを強化するための有用な戦術を学ぶ。

このコースでは、基本的な考え方の理解から最先端の ML アプローチの適用まで、現代のサイバーセキュリティの複雑な世界を横断するために必要な知識とスキルを身につけることができます。

このイベントは、専門家、エンジニア、CISO、SOC 管理者、学生、ペンテスター、サイバーセキュリティ専門家、


脅威エンジニア、その他現代のサイバー時代におけるデジタルエコシステムの保護に関心のあるすべての人にとって不可欠です。

実践的なアプリケーション、倫理的考察、プロアクティブな防御戦略について学びましょう。

Utilizing bespoke machine learning algorithms (like RFC and DBSCAN) to detect cybersecurity risks.

Investigate the crucial nexus between cybersecurity and machine learning as we build sophisticated threat detection systems. Learn useful tactics to strengthen digital security against ever changing cyberthreats.

This course gives participants the knowledge and skills they need to traverse the complicated world of contemporary cybersecurity, from comprehending fundamental ideas to applying cutting-edge ML approaches. This event is essential for professionals, engineers, CISOs, SOC managers, students, pentesters, cybersecurity professionals, threat engineers, and anyone else interested in protecting digital ecosystems in the modern cyber age. Learn about practical applications, ethical considerations, and proactive defense strategies.




## Srini – Srinivasan Balasubramanian Thimma

Singapore

**Speak:** 12 global languages


**Hobbies:** Hiking, Swim, Sauna, Jacuzzi, Research (Cybersecurity, Math's & Science)

**Strengths :** Value oriented, Creativity, Cultural fit and empathy-relationship, Detail oriented and pictorial



**20 years of Information Security experience & Volunteer**

Worked in USA, Japan, UK, Singapore, ANZ and India




**Platinum member of ISACA Japan – 15 years**

Speaker for 100+ events in Asia Pacific region. Consulting to 500+ customers.




**Design thinking and Innovation program**

Design thinking and innovation research programs, Masters in Computer Science.




**Ph.D. – Doctor of Philosophy in Cybernetics**


Research in threat intel, Human and machine interface.




**CGEIT** Certified in the Governance of Enterprise IT  
An ISACA Certification




**CDPSE** Certified Data Privacy Solutions Engineer  
An ISACA Certification



**CISM** Certified Information Security Manager  
An ISACA Certification




**Stanford ENGINEERING**



**University of Reading**

1 © 2022 Cardinal Health. All Rights Reserved. FOR INTERNAL USE ONLY.



## Ana Carmela Arcillas

Philippines

**Hobbies:** Solving puzzles and Sudoku, planting, sketching

**Strengths :** Analytical, Value-oriented, Learner

- More than 10 years of experience in Information security (network and web application security, client data protection, third party risk assessment)
- Mathematic major from the University of the Philippines
- Supervisor, New APAC and EMEA Vendors in CHIP

**Exams passed:**

Certified Information Security Auditor(CISA)

CompTIA Security+

Certified in Cybersecurity

2 © 2022 Cardinal Health. All Rights Reserved. FOR INTERNAL USE ONLY.



12:15-13:00 Room1 241A7

ランチョン・ミニパネルディスカッション「医療安全と医療サイバーセキュリティ」

Luncheon Mini Panel Discussion; Medical Safety and Medical Cyber Security

座長：東京工科大学 田仲浩平

Chairman: Kohei Tanaka, Tokyo University of Technology

パネリスト：Health-ISAC デニス・アンダーソン

Panelists: Denise Anderson, President of Health-ISAC

パネリスト：医療 ISAC 深津 博

Panelists: Hiroshi Fukatsu, Medical ISAC Japan

#### Profile

田仲 浩平

[学歴]

徳島大学大学院 先端技術科学教育部 知的力学システム工学専攻卒

[所属]

東京工科大学 医療保健学部 臨床工学科 教授 / 博士(工学) / 臨床工学技士

大学院医療技術学研究科

片柳研究所 デジタルヘルス・イノベーションセンター/センター長

[専門分野]

医療機器安全工学、医療 AR グラス、医療 VR シミュレータ、XRトレーニング

[学会等]

日本医療安全学会理事(医療機器安全部会長)

日本医療安全推進学会理事

日本保健情報コンソシウム学術顧問

合同会社 society5.0 特別顧問



Kohei Tanaka,

[Academic Background]

Graduated from the Department of Intelligent Mechanics and Systems Engineering, Graduate School of Advanced Technological Sciences, Tokushima University.

[Affiliation]

Professor, Ph.D, CE, Department of Clinical Engineering, Faculty of Medical and Health Sciences, Tokyo University of Technology

Graduate School of Medical Technology

Center Director, Digital Health Innovation Center, Katayanagi Institute

[Area of Expertise]

Research and development of medical device safety engineering, research and development of medical augmented reality (AR) glasses and medical virtual reality (VR) simulators.

[Academic conferences, etc.]

Director, Japan Society for Medical Safety (Chair, Medical Device Safety Section)

Director, Japan Society for the Promotion of Medical Safety

Academic Advisor, Japan Health Information Consortium

Senior Advisor, society5.0, LLC

#### Abstract

医療安全とサイバーセキュリティは医療機関にとって重要な課題であり、事故事例の分析と情報・教訓の共有が重要な点も共通している。

本セッションでは日米の事例を紹介し、座長である日本医療安全学会の田仲理事の指南の元、問題提起を行う。

Medical safety and cybersecurity are both critical matters for medical facilities and share the importance of information and lessons sharing.

In this session, panelists will introduce the examples in the US and Japan, and Dr. Tanaka, director of the Japan Society of Medical Safety will promote the discussion and problem presentation.

#### **13:00-13:45 Room1 241P1**

##### **JIS T 81001-5-1 へのコンプライアンスの確保:医療機器ソフトウェアセキュリティの成功戦略**

##### **Ensuring Compliance with Japan IEC 81001-5-1: Strategies for Success in Medical Device Software Security**

**日本ベクトン・ディッキンソン 岡山太郎**

**Taro Okayama, Nippon Beckton Dickinson**

#### Profile

日本ベクトン・ディッキンソン株式会社

薬事部 シニアマネージャー

現在は、主に MD や IVD の厚生労働省への製品登録業務と、製品ライセンスの維持管理を担当しています。

私は東京大学を卒業し、獣医師免許と博士号を取得し、キャリアの初期はドイツとカナダで血液学/腫瘍学のポスドク研究者として勤務したあと、帰国後は、ベンチャー企業、国内製薬企業、CRO で研究開発、臨床研究に携わりました。

やりがいを感じるのは、どんな役割であれ、新しい価値のある製品を市場に送り出すことに貢献できたときです。

趣味は弓道、ガーデニング、旅行、飲食、愛猫との時間です。



Taro Okayama, DVM, Ph.D.

Senior Manager/Regulatory Affairs

Nippon Beckton Dickinson Company, Ltd.

In my current role, I am mainly in charge of local product registration to PMDA/MHLW on MDs and IVDs and maintaining product licenses. I graduated Tokyo University and granted a veterinary license and Ph.D. In my early carrier, I worked in Germany and Canada as a post-doctoral researcher in hematology/oncology. After returning to Japan, I took roles in R&D and clinical research in a start-up, domestic pharma, and CRO. I feel mostly rewarded when I contribute in bringing a new product with new value to the market, whatever

the role is. I enjoy Kyudo (Japanese archery), gardening, travelling, food and drinking, and time with my cat.

#### Abstract

急速に進化する今日の医療現場では、医療機器ソフトウェアのセキュリティを確保することが最も重要です。本講演では、JIS T 81001-5-1 (IEC 81001-5-1)が定める重要な規格と、医療機器業界に対するその影響について掘り下げます。

コンプライアンスを達成するには、リスク管理、安全なソフトウェア開発ライフサイクル (SDLC) の実践、効果的なインシデント対応プロトコルに焦点を当てた一連の包括的な戦略が必要です。参加者は、これらの標準を組織のプロセスに統合することで、サイバーセキュリティの脅威が増大する中で医療機器の信頼性と安全性を高めるための実用的な洞察を得ることができます。

In today's rapidly evolving medical landscape, ensuring medical device software security is paramount. This presentation delves into the critical standards JIS T 81001-5-1 (IEC 81001-5-1) set forth and their implications for the medical device industry. Therefore, achieving compliance requires a series of comprehensive strategies focusing on risk management, secure software development lifecycle (SDLC) practices, and effective incident response protocols. Attendees will gain actionable insights into integrating these standards into their organizational processes, thereby enhancing the reliability and safety of medical devices in the face of growing cybersecurity threats.

**13:00-13:45 Room2 242P1**

**医療分野における重要インフラ防護の在り方 ～地域型官民連携の重要性の台頭～**

**Critical Infrastructure Protection in the Healthcare Sector ～Emerging Importance of Regional Public-Private Partnerships～**

**名古屋工業大学大学院工学研究科社会工学専攻 防災安全部門長 教授 渡辺研司**  
**Prof. Kenji Watanabe, Head of Disaster & Safety Management Div., Nagoya Institute of Tech**

#### Profile

富士銀行、PwC コンサルティング、IBM ビジネスコンサルティングサービス  
長岡技術科学大学を経て 2010 年より現職。

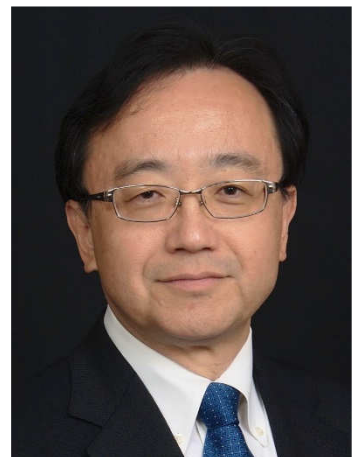
重要インフラ専門調査会会長、ISO/TC292 (セキュリティ・レジリエンス技術委員会) エキスパート等を兼務。

工学博士、MBA。

Prof. Kenji Watanabe has worked for Fuji Bank, PwC Consulting, and IBM Business Consulting Services Nagaoka University of Technology before assuming his current position in 2010.

He also serves as Chairman of the Critical Infrastructure Technical Committee and Expert of ISO/TC292 (Security and Resilience Technical Committee).

He holds a doctorate in engineering and an MBA.



#### Abstract

医療分野における DX の急速な進展は、利便性の向上と同時に、サイバーセキュリティ上の脆弱性も増加するという構造的な脆弱性を生み出している。所管省庁は集中的に現状の把握と事態の改善を行っているが、実効性を確保するためには各地域における官民連携の枠組みが不可欠である。本セッションでは中部での取り

組みや米国の InfraGard の仕組みを参照しながら、医療分野における重要インフラ防護の在り方について議論する。

The rapid development of DX in the healthcare sector has brought us many conveniences but also but also increase structural cybersecurity vulnerabilities. While responsible ministries and agencies are working intensively to understand the current situation and remedy the situation, a framework of public-private partnerships in each region is essential to ensure effectiveness. In this session, the state of critical infrastructure protection in the healthcare sector will be discussed, referring to the efforts in Chubu and the InfraGard mechanism in the United States.

**13:50-14:35 Room1 241P2 (Materials are not open to the public, so projection only.)**

**タケダの AI テクノロジーおよびサイバーリスク**

**AI Technology & Cyber Risk in Takeda**

**武田薬品工業株式会社 Information Security Leads - APAC 笹山 明**

**Akira Sasayama, Information Security Leads - APAC, Takeda Pharmaceutical Company Limited**

#### Profile

武田薬品の情報セキュリティ・リーダーとして、アジア太平洋地域のサイバーセキュリティを担当しています。IT セキュリティソリューション企業にてセキュリティエンジニアとして 9 年、コールセンタープロバイダーにてサイバーセキュリティマネージャーとして 5 年半、様々なサイバーセキュリティプロジェクトを担当していました。CISSP、CCSP、CISM の認定を所持しており、継続的に学習し専門的な能力を開発しています。

Akira Sasayama is an Information Security Lead at Takeda, overseeing cybersecurity in APAC. With 9 years of experience as a security engineer in IT security solutions company and 5 and a half years of experience as a Cyber Security Manager in a call center provider, handling critical cybersecurity projects. Certified in CISSP, CCSP, and CISM, to continuous learning and professional development.



#### Abstract

この度、武田薬品工業は、ソーシャルエンジニアリングに基づくサイバー攻撃の人的側面に焦点を当て、AI に基づくセキュリティの脅威とリスクについて講演させていただくことになりました。

ディープフェイクやマルウェアベースの攻撃は、ジェネレーティブ AI の活用により、ますます巧妙になってきています。武田薬品は、このようなグローバルの脅威において、どのような攻撃を確認しているのか、また、人的要素に焦点を当ててサイバー防御を強化することで、増大する脅威にどのように対処しているのか共有いたします。

We are delighted to present on AI based security threats and risks to Takeda, with a focus on the human side of social engineering based cyber-attacks.

Deepfake and malware-based attacks have become increasingly sophisticated by use of Generative AI.

Takeda is a target in this global threat landscape; We will discuss the types of attacks we are identifying and how we are addressing this growing threat by strengthening our cyber defence with a focus on the human element.

13:50-14:35 Room2 242P2

**診療報酬改定対応に向けた医療データを守るランサムウェア対策**

**Ransomware countermeasures to protect medical data in response to the revision of medical reimbursement**

**Cohesity Japan 株式会社 磯辺 真／春日井市民病院 馬場隼人**

**Makoto Isobe, Cohesity Japan K.K. / Hayato Baba, Kasugai Municipal Hospital**

Profile

磯辺 真(いそべ まこと)

Cohesity Japan 株式会社 営業本部 第二営業部 シニアセールス

診療報酬改定対応に向けた医療データを守るランサムウェア対策

Makoto Isobe, Cohesity Japan K.K.

Mr.Isobe will explain about ransomware countermeasures to protect medical data in preparation for the revision of medical reimbursement.



馬場隼人(ばば はやと)

春日井市民病院 医療情報技術センター事務局管理課情報担当

Hayato Baba, Kasugai Municipal Hospital, Kasugai Municipal Hospital,

Medical Information Technology Center, Administration Division,

Information



Abstract

磯辺さんは、診療報酬改定対応に向けた医療データを守るデータセキュリティとしてのオフラインバックアップに関して説明します。

そして、馬場さんからは、ランサムウェアの脅威から診療データを守り、医療現場を止めないセキュリティ対策と、BCP 対策としても有効な、安全な環境整備の実現について解説していただきます。

Mr. Isobe will explain about offline backup as a data security to protect medical data for responding to the revision of medical reimbursement.

And, Mr. Baba will explain how to realize a secure environment that protects medical data from ransomware threats, security measures that do not stop medical practices, and is also effective as a BCP measure.

14:40-15:25 Room1 241P3

## SBOM 作成で終わらない法規対応で求められるプロダクトセキュリティとデータ品質の課題

### Going beyond the SBOM: Product security in the age of regulations and data quality challenge

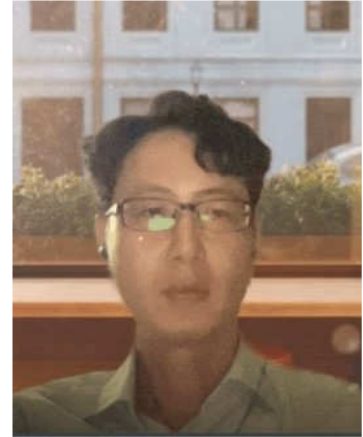
サイベラム・テクノロジーズ合同会社 Principal Sales Engineer 池川史憲

Fuminori Ikegawa, Principal Sales Engineer, Cyberum Technologies, G.K.

#### Profile

サイベラム・テクノロジーズ合同会社で 2022 年から Principal Sales Engineer として日本市場を担当し、自動車、医療、製造業の接続デバイスに対するセキュリティを推進している。25 年にわたるサイバーセキュリティおよび IT セキュリティ領域で様々な役職の経験を持ち、前職に引き続きサプライチェーンセキュリティへ取り組んでいる。

Mr. Ikegawa has been working as a Principal Sales Engineer at Cybellum Technologies G.K. since 2022, responsible for the Japanese market, promoting security for connected devices in the automotive, medical, and manufacturing industries. With 25 years of experience in various roles within the cybersecurity and IT security fields, he continues to focus on supply chain security, following his previous positions.



#### Abstract

世界中の医療機器メーカーとサプライヤーに勤務する従業員を対象に行った調査をもとにしたデータおよび日米のプロダクトセキュリティの状況を考察し、医療機器メーカーの課題を取り上げます。

プロダクトセキュリティを取り巻く課題とプロダクトセキュリティ成熟度向上の必要性、成熟度に伴うビジネス価値の向上、ソフトウェアサプライチェーンとデータ品質の課題など、SBOM 作成で終わらない医療機器メーカーが解決すべき課題を考察していきます。

Based on data from a survey conducted among employees of medical device manufacturers and suppliers worldwide, we will consider the state of product security in Japan and the United States, and address the challenges faced by medical device manufacturers. We will explain the challenges surrounding product security, the necessity of improving product security maturity, the enhancement of business value that comes with increased maturity, and issues related to the software supply chain and data quality. We will also discuss the various challenges that medical device manufacturers need to solve, beyond just creating an SBOM (Software Bill of Materials).



14:40-15:25 Room2 242P3 (Materials are not open to the public, so projection only.)

## 医療セキュリティにおける<BCP>とは何か

What is “BCP” in medical security?

医療 ISAC ステアリングコミッティ委員 江原悠介

Yusuke Ehara, Medical ISAC Japan Steering Committee Member

### Profile

医療機関や情報処理事業者に対するガイドライン・指針に基づく態勢整備/セキュリティ監査、患者個人情報等の二次利用に際したプライバシーガバナンスの整備支援等、ヘルスケア分野のセキュリティ/コンプライアンスや医療 DX に伴うガバナンス設計の知識・経験を有する。医療サイバーに関する各種講演・セミナー、寄稿・執筆等に加え、四病院団体協議会や保険団体連合会等、国内医療関係組織へのサイバーアンケートに基づく調査・分析・提言等も行う。

Mr. Yusuke Ehara has knowledge and experience in security/compliance in the healthcare field and governance design for medical DX, such as maintenance of systems and security audits based on guidelines and guidelines for medical institutions and information processing businesses, and support for privacy governance for the secondary use of personal patient information, etc. He has knowledge and experience in security/compliance in the healthcare field and governance design for healthcare DX.

He also conducts surveys, analysis, and recommendations based on cyber surveys of domestic healthcare-related organizations such as the Japan Federation of Four Hospital Associations and the Japan Federation of Insurance Organizations.



### Abstract

医療機関へのサイバー攻撃が発生する中で、サイバーBCP の重要性が論じられ、医療法 25 条 1 項に基づく医療監視においても対応状況の確認が行われている。

ただし、こうしたコンテキストにおいては、医療セキュリティにおける IT-BCP/サイバーBCP の異同点の説明どころか、本来あるべき BCP の観点から一般的に検討すべき基本ポイントの整理、あるいは BCM の運用の重要性も特にフォーカスされず、単なるサイバー攻撃で利用不可になったシステムの復旧手順が BCP と論じられている状況である。

本講演では、本来あるべきサイバーBCP、ひいては BCM も含め、医療セキュリティにおいて検討すべき業務継続性の確保に本当に検討すべきポイントが何であるのかについて概括的に解説し、無駄のないサイバー BCP を確立するためのヒントを紹介する。

Amid cyber attacks on medical institutions, the importance of cyber BCP has been discussed, and the status of response has been confirmed in medical surveillance based on Article 25.1 of the Medical Care Act.

However, in this context, rather than explaining the differences between IT-BCP and cyber-BCP in medical security, there is no particular focus on the basic points that should be generally considered from the perspective of BCP as it should be, or the importance of BCM operations. Instead, BCP is simply a procedure for restoring a system that has become unusable due to a cyber attack.

In this lecture, the speaker will give a general explanation of the points that should be considered in medical

security to ensure business continuity, including cyber BCP and BCM, and will introduce hints for establishing a lean cyber BCP.

**15:30-16:15 Room1 241P4**

**喫緊の課題 脆弱性対策・ランサムウェア対策を進めるには**

**～医療法 25 条に基づく立ち入り検査チェックリストを踏まえて～**

**How Should Medical Institutes address 2 Pressing Cybersecurity Issues, Vulnerabilities and Ransomware attacks?**

**～ Proposal Based on On-site Inspection Checklist under Article 25 of the Medical Care Act～**

**ジュピターテクノロジー株式会社 太田 道子**

**Michiko Ota, Jupiter Technology Corp.**

#### Profile

ジュピターテクノロジー BU3 技術・プリセールス

取得資格

- ・情報セキュリティマネジメント
- ・教育情報化コーディネーター2級

10 年間、学校現場の ICT 機器の導入、保守を経験(院内学級含む)。特別支援学校の ICT 活用支援員として児童・生徒の教育に ICT を活用頂く取り組みを行う。

導入機器研修担当、児童・生徒・教諭への情報モラル研修講師を経て、現在はセキュリティ製品の検証、拡販を担当。

Jupiter Technology BU3 Technical and Pre-Sales

Certifications

- ・ Information Security Management
- ・ Educational Informatization Coordinator Level 2

10 years of experience in the introduction and maintenance of ICT equipment at schools (including in-hospital classes). As an ICT utilization support staff at special-needs schools, she has worked on the utilization of ICT in the education of children and students.

After working as a training instructor of ICT equipment, and as an instructor of information morality training for students and teachers, he is currently in charge of verifying and expanding sales of security products.



#### Abstract

医療法施行規則の改正により、保健所の立ち入り検査にてサイバーセキュリティ対策が検査対象となり、医療情報システムのサーバー・端末における、セキュリティパッチ適用が必須となりました。数百台規模のサーバー・端末の状況の把握とパッチ適用は手動では自ずと

限界があるため、半自動化が望まれます。また関連する課題としてパッチ適用による医療情報システムの動作検証など、周辺課題も無視できません。

本講演ではこれらの課題を、パッチ管理システムがどのように解決できるかをご紹介します。

As a result of the amendments to the Enforcement Regulations on the Medical Care Act, the medical institutes' cybersecurity measures are now subject to inspection conducted on-site by the public health



centers and they must implement the security patches on the servers and endpoints on their medical information systems.

Manual patching is resource-intensive, requiring significant time and manpower. It can be easily imagined that manual tracking update status and patching on time hundreds of servers and endpoints across their environment is not feasible and automated (semi-automated) patching is strongly required.

In addition, it cannot be ignored that the related issues patch management has, such as patch testing on the medical information systems before applying patches to avoid compatibility issues and potential system disruptions.

In this session, we present how the patch management system can solve these issues.

**15:30-16:15 Room2 242P4**

### **医療機関におけるサイバー保険の選び方**

#### **How to Choose Cyber Insurance for Your Medical Organization**

**あいおいニッセイ同和損害保険株式会社新種保険部 サイバー・特殊リスクG**

**サイバー保険担当 神山太朗**

**Taro Kamiyama, Deputy General Manager, Cyber, D&O, E&O Underwriting Group,**

**Casualty Insurance Underwriting Department,**

**Aioi Nissay Dowa Insurance Co., Ltd.**

#### Profile

損害保険業界の商品開発部門に 20 数年に渡り在籍。90 年代後半より IT 関連の保険 (現在のサイバー保険) の企画・開発等に携わる。

保険業界ほかセキュリティ業界でも活動。

日本ネットワークセキュリティ協会 (JNSA) 幹事、調査研究部会インシデント被害調査 WG リーダー

Mr. Taro Kamiyama has worked in the product development department of the non-life insurance industry for more than 20 years, and has been involved in the planning and development of IT-related insurance (currently cyber insurance) since the late 1990s.

He is active in the security industry as well as the insurance industry.

Secretary of the Japan Network Security Association (JNSA), and leader of the Incident Damage Investigation WG of the Research and Survey Subcommittee.



#### Abstract

徳島半田病院、大阪急性期・総合医療センターの事例からもわかるように、ランサムウェア感染により発生する損失は非常に高額となる。フォレンジック調査、システム復旧、診療停止期間の逸失利益などの各種損害を考慮するに、診療所で数千万円、大病院で数億円規模の被害が発生し得る。

このような損失に備え、医療機関でサイバー保険の加入が加速しているが、改めてサイバー保険の必要性、サイバー保険の機能について説明したい。

As the cases of Tokushima Handa Hospital and Osaka Acute & General Medical Center show, the losses incurred due to ransomware infection are extremely high. Considering various types of losses such as forensic

investigation, system restoration, and lost income during the period of medical treatment suspension, damage in the tens of millions of yen for a clinic and hundreds of millions of yen for a large hospital can be incurred. To prepare for such losses, medical institutions are increasingly purchasing cyber insurance. We would like to reiterate the necessity of cyber insurance and explain its functions.

**16:20-17:05 Room1 241P5**

**医療機関におけるサイバーセキュリティ対策チェックリスト(令和6年度版対応)への具体的な対応方法  
Specific measures to be taken in response to the Checklist of Cyber Security Measures for Medical  
Institutions (2024 version)**

**パーソルプロセス&テクノロジー株式会社 谷 昌行  
Masayuki Tani, Persol Process & Technology co., Ltd.**

Profile

政府機関の情報システムおよびセキュリティ担当を経て、サイバーセキュリティ業務を行う企業でコンサルタントを務め、2023年より現職。

Mr. Masayuki Tani has worked in information systems and security for a government agency, and then as a consultant for a company that provides cybersecurity services, where he has been in his current position since 2023.



Abstract

セキュリティの専門的な知識を持つ人材は社会全体でも不足しており、医療機関が単独で確保することが難しい状況にあります。

そこで弊社は、専門知識を広く共有していただく方策として、「医療機関におけるサイバーセキュリティ対策チェックリスト」への対応を主眼に置いたセキュリティ対策に関するサービス「SharedCISO」を提供しております。

今回はこのサービス事例から、「チェックリストをどのように解釈するか」「どこまで対策すれば「はい」と答えてよいか」「本当にチェックリストだけ対策すれば十分か」等について、弊社コンサルタントが数点例を挙げながら、サービス内容を紹介いたします。

There is a shortage of personnel with specialized security knowledge in society as a whole, and it is difficult for medical institutions to secure such knowledge on their own.

To address this situation, we offer “SharedCISO” a security measures service that focuses on the “Cyber Security Measures Checklist for Medical Institutions” as a way to widely share expertise.

In this case study, our consultant will introduce our service with some examples, such as “how to interpret the checklist,” “how far to go to get a ‘yes’ answer,” and “is it really sufficient to take measures only on the checklist?”

16:20-17:05 Room2 242P5

医療機関におけるゼロトラストとは ～ユースケースから見るゼロトラスト思考の活用例～

What is Zero Trust in Healthcare Organizations? ~Examples of Zero Trust Thinking from Use Cases~

ゼットスケーラー株式会社 セールスエンジニア 井上 尚人

Naoto Inoue, Sales Engineer, Zscaler K.K.

#### Profile

SI、セキュリティ機器メーカーのプリセールス SE 業務に従事。  
その後 Zscaler の SE として国内顧客への提案・評価・導入支援を行っている。  
Naoto Inoue worked as a pre-sales SE for a SI and security equipment manufacturer. Then, as SE of Zscaler, he has been proposing, evaluating, and supporting implementation to domestic customers.



#### Abstract

2022 年に医療業界で発生したランサムウェア攻撃は前年比で 650%増加したといわれています。

また国内でも様々な医療機関で攻撃被害が発生し、厚労省からは「医療情報システムの安全管理に関するガイドライン第 6 版」が昨年公開されました。

このガイドライン内にゼロトラスト思考といったキーワードが出ていますが、具体的に何をすればよいかの記載はなく、各機関に任されている状況かと思います。

そこで本セミナーでは、ゼロトラスト思考を取り入れた医療システムの活用例を、ユースケース・事例をもとにご紹介したいと思います。

It is said that the number of ransomware attacks that occurred in the healthcare industry in 2022 increased by 650% compared to the previous year.

In Japan, various medical institutions have also suffered attacks, and the Ministry of Health, Labor, and Welfare (MHLW) released the “Guidelines for the Safe Management of Medical Information Systems, 6th Edition” last year.

Although the guideline includes keywords such as “Zero Trust Thinking,” it does not specifically state what to do, leaving it up to each institution.

Therefore, in this seminar, we would like to introduce some examples of medical system applications that incorporate Zero Trust Thinking, based on use cases and case studies.

17:10-17:30 Room1 241P9

閉会のあいさつ

Closing Remarks

医療 ISAC ステアリングコミッティ委員 舟橋 真

Makoto Funahashi, Medical ISAC Japan Steering Committee Member

#### Profile

警察庁情報管理課長、警察庁技術審議官等を歴任。

2001 年 3 月、警察庁を退官し、財団法人未来工学研究所等に所属して危機管理やサイバーセキュリティに関する研究に従事。

2004 年 8 月、デジタル・フォレンジック研究会の設立に参画、デジタル・フォレンジックの普及・啓発、および資

格認定の制度設計に取り組んでいる。

また、2011 年 6 月、株式会社セキュリティ工学研究所の設立に参画、国内外のセキュリティに係わるコンサル業務に携わっている。

この間、1996 年度、「マルチベンダによる大規模情報通信ネットワークの開発とその実用化」により、電子情報通信学会業績賞(第 34 回)及び森田賞(第 2 回)を受賞。

【政府関係委員会】

- ・ 2007 年度、総務省消防庁国民保護室「国民保護における避難施設検討会」座長
- ・ 2010 年度～2012 年度、海上保安庁「情報流出再発防止対策検討委員会」委員
- ・ 2012 年度～2022 年度、「海上保安庁情報セキュリティアドバイザリー会議」委員
- ・ 2016 年度～2018 年度、内閣府「総合科学技術・イノベーション会議・重要課題専門調査会「地域における人とくらしのWG」」専門構成委員

【著書】

- ・ 2014 年 4 月、「改訂版 デジタル・フォレンジック事典」共著
- ・ 2019 年 5 月、「基礎から学ぶデジタル・フォレンジック: 入門から実務での対応まで」共著

Mr. Funabashi served as Director of the Information Management Division of National Police Agency and as Councillor for Science and Technology Affairs of National Police Agency.

In March 2001, he retired from National Police Agency and joined The Future Engineering Research Institute, where he was engaged in research on crisis management and cyber security.

In August 2004, he participated in the establishment of The Institute of Digital Forensics and has been involved in the promotion and awareness of digital forensics and the design of certification systems.

In June 2011, he participated in the establishment of The Security Engineering Laboratory, Inc. and has been engaged in consulting services related to domestic and international security.

In 1996, he received the 34th Achievement Award and the 2nd Morita Award from The Institute of Electronics, Information and Communication Engineers (IEICE) for the “Development and Practical Application of a Large-Scale Information and Communication Network with Multiple Vendors”.

【Government Committees】

- ・ FY2007: Chairperson of the “Committee to Study Evacuation Facilities for the Protection of the People”, Civil Protection Office, Fire and Disaster Management Agency
- ・ FY2010 – FY2012: Member of “Information Leakage Recurrence Prevention Measures Review Committee”, Japan Coast Guard
- ・ FY2012 – FY2022: Member of the “Information Security Advisory Board”, Japan Coast Guard
- ・ FY2016–FY2018: Expert Member of “Council for Science, Technology and Innovation, Specialist Committee on Key Issues, Working Group on People and Life in Local Communities”, Cabinet Office, Government of Japan

【Publications】

- ・ Co-author of “Revised Handbook of Digital Forensics”, April 2014
- ・ Co-author of “Basics of Digital Forensics: From Introduction to Practical Application”, May 2019





Canon

世界を繋ぐ、医療を描く。



キヤノンの医療情報ソリューション“Abierto”は、  
莫大なデータの検索に最適なデータベースを採用した集める Abierto VNA と、  
効率的に観せる Abierto Cockpit に加え、データを活用し、  
画像診断業務のワークフローを改善する新しいソリューションです。

読影支援ソリューション

# Abierto

## Reading Support Solution

【一般名】 読影支援業務ワークステーション用プログラム 【販売名】 読影支援業務ワークステーション用プログラム Abierto SCAP IAP  
【登録番号】 302A9BZX00004000 【製造販売元】 キヤノンメディカルシステムズ株式会社 / 栃木県大田原市下石上1385番地

D000248

キヤノンメディカルシステムズ株式会社 <https://jp.medical.canon>

Made For life

Marubeni  
Group

デジタル眼底カメラ  
&  
AI眼底写真解析

AI胸部X線画像  
肺結節検出支援



大切な人へ、  
未来の医療を、共に

AI統合認知  
評価ツール

MR画像変性脳疾患  
定量解析

AI医用画像  
整理・正規化、  
匿名化ツール

総合商社 丸紅の持つ130拠点（67か国・地域）のネットワークで  
優れた技術をいち早く発掘し提供していきます

## クエアボ・テクノロジーズ株式会社

([www.clairvotech.com](http://www.clairvotech.com))

設立： 2020年 4 月

株主： 丸紅株式会社 100%出資

事業： 1)AI やその他先端技術を適用した医療機器・  
サービスの開発、製造、販売・貸与、輸出入  
2)その他医療機器 及びヘルスケア関連商品の開  
発、製造販売、販売・貸与、輸出入

資格： 第一種医療機器製造販売業

(許可番号 13B1X10341)

高度管理医療機器等販売業・貸与業

(第4501210013号)

医療機器修理業

(許可番号 13BS201699)

古物商

(東京都公安委員会 第301012415492号)



# ハイムダル Heimdal® パッチ・脆弱性管理

Heimdal パッチ・脆弱性管理は、クライアント PC やサーバーの脆弱性を可視化し、提供元が配布する正式な修正パッチを自動で適用する製品です。

◇パッチ適用、管理の自動化

◇OS 更新と200種類以上の  
アプリケーション更新に対応

◇閉鎖環境でも運用可能

※プロキシサーバー使用環境



**STC-i** ジュピターテクノロジー

【本社】

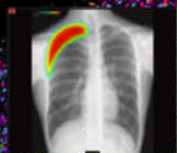
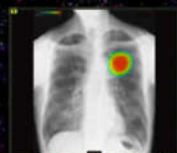
〒183-0023 東京都府中市宮町一丁目 40 番地

KDX 府中ビル 6F

TEL:042-358-1250(代表) FAX:042-360-6221

胸部X線画像病変検出ソフトウェア

## CXR-AID



90  
100

AI技術<sup>®</sup>を活用して胸部単純X線画像の「結節・腫瘤影」「浸潤影」「気胸」診断を支援

※ AI技術のひとつであるディープラーニングを設計に用いた。導入後に自動的にシステムの性能や精度が変化することはない。



胸部X線画像病変検出ソフトウェア CXR-AID

販売名: 胸部X線画像病変検出(CAD)プログラム LU-AI689型

承認番号: 30300BZX00188000

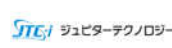
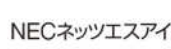
※ご利用いただくにはアプリケーションがインストールされた高度処理ユニットが必要です。

製造販売業者: 富士フイルム株式会社

販売業者: 富士フイルム メディカル株式会社

〒106-0031 東京都港区西麻布2丁目26番30号 富士フイルム西麻布ビル

TEL.03-6419-8040(代) URL <https://fujifilm.com/fms/>



**一般社団法人 医療 I S A C**

〒103-0021 東京都中央区日本橋本石町 3-3-8 日本橋優和ビル 5F  
電話 : 03-3527-9528 FAX : 03-3527-9950

URL : <https://m-isac.jp/>  
Facebook : <https://www.facebook.com/medical.isac/>