DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

DITTA Activities in Cybersecurity & Update on IMDRF Work Item on Cybersecurity

Keiichiro Ozawa

Vice-chair, DITTA Cybersecurity WG

24th AHWP Annual Meeting
12 November 2019, Muscat, Oman

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA Medical Imaging & Technology Alliance · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

DITTA GLOBAL PRESENCE

2018: DITTA as a recognized non state actor in official relations with WHO
2016: DITTA MoU with the World Bank
2015: DITTA was granted a NGO status with WHO
2014: DITTA has official liaison with AHWP

DITTA: 9 WORKING GROUPS

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. Regulated Product Submission (RPS) Working Group — MITA
2. Medical Device Single Audit Program (MDSAP) Working Group — MITA
3. Unique Device Identification (UDI) Working Group — MITA
4. Standardisation (STA) Working Group — COCIR
5. Clinical Evaluation — COCIR
6. Global Health (GH) Working Group — COCIR
7. Environmental Policy (ENVI) Working Group — COCIR
8. Good *Refurbishment Practice (GRP) Working* Group — JIRA
9. Cybersecurity Working Group — MITA

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

TABLE OF CONTENTS

COCIR Advancing Healthcare | JIRA | Medtech Canada | MITA Medical Imaging & Technology Alliance | THAIMED | IMEDA | 中国医疗器械行业协会 China Association for Medical Devices Industry | abimed | Kmdica Korea Medical Devices Industrial Coop. Association | ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

TABLE OF CONTENTS

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. Activities in IMDRF

COCIR Advancing Healthcare | JIRA | Medtech Canada | MITA Medical Imaging & Technology Alliance | THAIMED | IMEDA | 中国医疗器械行业协会 China Association for Medical Devices Industry | abimed | Kmdica Korea Medical Devices Industrial Coop. Association | ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-1 Promotion of Digital Health and Cybersecurity

1. Support and promotion of IMDRF SaMD work item
   – DITTA has been proposing the convergence of digital health regulation.
   – DITTA submitted the New Work Item Proposal of SaMD for IMDRF in 2013.
   – DITTA has been supporting the IMDRF activities since then.

2. IMDRF SaMD guidance document (IMDRF/SaMD WG/N12, SaMD: Possible Framework for Risk Categorization and Corresponding Considerations*) describes the importance of **information security** with respect to safety considerations.

** http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf*

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-2 Need for the Global Convergence of Cybersecurity

1. Cybersecurity guidance of US (2014)
   - Content of Premarket Submissions for Management of Cybersecurity in Medical
2. **DITTA held the 1st workshop on cybersecurity accompanying IMDRF meetings** (Brasilia, 2016).
3. Cybersecurity guidance of US (2016)
   - Postmarket Management of Cybersecurity in Medical Devices
4. Cybersecurity guideline of China (2017)
   - Medical Device Network Security Registration on Technical Review Guidance Principle

1. ACTIVITIES IN IMDRF

1-3 Development of New Work Item Proposal of IMDRF

1. **DITTA held the 2nd workshop on cybersecurity accompanying IMDRF meetings** (Shanghai, March 2018).
   - Raising the cybersecurity awareness of both regulators and industries in the medical device field
   - New Work Item Proposal was suggested from regulators.
2. DITTA Developed the New Work Item Proposal (March – May)
3. Submission of NWIP to IMDRF Management Committee (June)
4. Approval of NWIP by IMDRF MC (Beijing, September)

1. ACTIVITIES IN IMDRF

1-4 Contents of the New Work Item Proposal

Three important topics (NWIP)

Topic 1: Shared responsibility among stakeholders

Recognize that cybersecurity is a shared-responsibility among all stakeholders, including manufacturers, healthcare providers, regulators, patients, and others.

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

Three important topics (NWIP)

Topic 2: Information sharing

Promote broad information-sharing policies to have clearly established legal guardrails and create incentives for participation. Information-sharing requirements, if implemented, should also extend to owners/users of medical devices.

Topic 3: Definition

Define the terms and clarify the current understanding on medical device cybersecurity. Medical device cybersecurity should be based on the safety and performance of medical device. It is necessary to clarify and define that medical device cybersecurity is different from information security which maintains confidentiality, integrity and availability.

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-5 Activity of IMDRF Cybersecurity WG

1. **WG Name**: Medical Device Cybersecurity Guide WG
2. **Leadership**: USFDA and Health Canada (Co-chairs):
3. **Members**: Australia, Brazil, Canada, China, European Union, Japan, Russia, Singapore, South Korea, United States, **DITTA**, GMTA
4. **Timeline**:

Jan. 2019	Kick-off meeting
June	In-person meeting for the proposed draft (Arlington)
July	Submitting the draft to Management Committee
Sep.	Review and approval by MC (Yekaterinburg)
Oct. - Nov.	Public consultation on IMDRF website*

** http://www.imdrf.org/consultations/cons-ppmdc.asp*

1. ACTIVITIES IN IMDRF

1-5 Activity of IMDRF Cybersecurity WG

5. **Goals**

- To facilitate international regulatory convergence on medical device cybersecurity with open discussion and sharing best practices that are understandable and feasible for all stakeholders.
- Specifically, the WG goal is to produce a document providing medical device cybersecurity guidance for all responsible stakeholders, including manufacturers, healthcare providers, regulators, and users across the entire device lifecycle.

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-5 Activity of IMDRF Cybersecurity WG

6. **The process of drafting the guidance document**

Conference calls every two weeks

- Jan. 2019, Kick-off meeting
- Feb., Drafting table of contents
  Assigning sections to members
- Mar., Drafting pre-market section
- Apr., Post-market section
- May, Document structure
  Internal consultation
- June, Meeting in Arlington

Table of Contents

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-5 Activity of IMDRF Cybersecurity WG

7. **Public consultation**

- IMDRF Website: ***http://www.imdrf.org/consultations/cons-ppmdc.asp***
  - Draft guidance documents in PDF and Docx.
  - Comment sheet
- Document title: Principles and Practices for Medical Device Cybersecurity
- Activity update material in Yekaterinburg meeting
  - IMDRF Website: ***http://www.imdrf.org/docs/imdrf/final/meetings/imdrf-meet-190916-russia-yekaterinburg-32.pdf***

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-5 Activity of IMDRF Cybersecurity WG

7. Public consultation

Please send your comments to

aftin.ross@fda.hhs.gov (official)

or

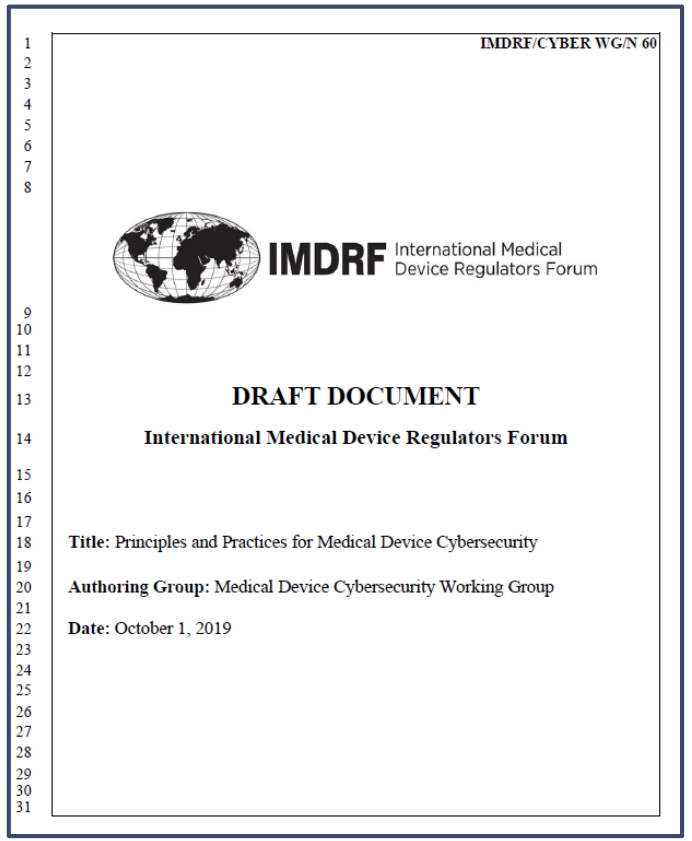
keiichiro.ozawa@fujifilm.com (my address)

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-6 Contents of IMDRF Cybersecurity Guidance Draft

- Document structure is **4 main components**:
  - Definitions
  - General Principles
  - Pre -market Considerations
  - Post -market Considerations
- All definitions add to **N47** terms/definitions, Generally align with **internationally recognized standards**, and include key terms such as: ‘ cybersecurity’, ‘ compensating control ’, ‘legacy device’, ‘ patch ’ and ‘privacy’



IMDRF/CYBER WG/N 60

IMDRF International Medical Device Regulators Forum

DRAFT DOCUMENT

International Medical Device Regulators Forum

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: October 1, 2019

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-6 Contents of IMDRF Cybersecurity Guidance Draft

- **General Principles** section covers:
  - Requirement for total product life cycle approach (TPLC)
  - Concept of shared responsibility among stakeholders
  - Global harmonization and concept of information sharing

- **Pre-market section** covers:
  - Recommendations for manufacturers only
  - Recommendations include: good design, risk management, security testing, labelling, and regulatory submission requirements

1. ACTIVITIES IN IMDRF

1-6 Contents of IMDRF Cybersecurity Guidance Draft

- **Post -market** section covers:
  - Recommendations for all stakeholders including manufacturers, healthcare providers and patients (users), regulators, and security researchers
  - Includes 'best practices' for healthcare
  - Provides guidance on information sharing and vulnerability disclosure along with remediation and incident response
  - Proposes level of regulatory oversight required for different categories of software maintenance
  - Recommends best practices for Legacy devices (devices that cannot be reasonably protected against current cybersecurity threats)

1. ACTIVITIES IN IMDRF

1-7 DITTA Perspective on the IMDRF Cybersecurity Activity

1. DITTA has been and will be supporting the IMDRF activity
   - DITTA organizes mirror groups and supports the activities in IMDRF!

2. **Scope and definition**
   - The scope is well described in the Guidance Document. But it is still somewhat unclear about the **difference between "medical device cybersecurity" and "information security"** and whether the latter is included in the scope or not.

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-7 DITTA Perspective on the IMDRF Cybersecurity Activity

3. Feasibility of the Guidance Document

- Currently the implementation of IMDRF all work items attracts much attention from stakeholders. The key is the feasibility of the guidance document in each work item. The development of guidance documents should consider member jurisdictions' regulatory systems, background of the regulation and so on. DITTA would suggest the members' discussion.

4. Cybersecurity requirements of N47, Essential Principles

- DITTA concerns about the newly added security requirements in Essential Principles, N47, such as ones in section 5.8. DITTA would recommend to present practical resolution for them on the assumption that it could be included in the pre-market submission.

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

1. ACTIVITIES IN IMDRF

1-8 Next Steps

Nov.-Dec.	Closing public consultation and consolidating comments
Jan. 2020	In-person meeting of WG for comment resolution (Eysins, Switzerland)
Feb.	Submitting the final document to Management Committee
Mar.	Document review by MC in IMDRF meetings (Singapore)
Mar.	**DITTA plans the 3rd workshop on cybersecurity accompanying IMDRF meetings. (Singapore)**
Apr.	**Publishing official guidance document**

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

2. Publishing Whitepapers

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

2. PUBLISHING WHITEPAPERS

2-1 DITTA White Paper on Cybersecurity of Medical Imaging Equipment

- Issued in November, 2016
- Based on NEMA/MITA Cybersecurity for Medical Imaging
- Detailed cybersecurity best practices for manufacturers, suppliers and healthcare providers

http://www.globalditta.org/fileadmin/user_upload/Level_home/Press_releases/2016/DITTA_Cybersecurity_paper_29_Nov._2016_final_clean.pdf


DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

DITTA White Paper on Cybersecurity of Medical Imaging Equipment[1]

[1] The DITTA White Paper on Cybersecurity of Medical Imaging Equipment is derived from NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging. Reprinted by permission of the National Electrical Manufacturers Association, Medical Imaging & Technology Alliance.

1 OF 9 30 NOVEMBER 2016

COCIR Advancing Healthcare JIRA Medtech Canada MITA THAIMED IMEDA 中国医疗器械行业协会 abimed Kmdica ITAC

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

2. PUBLISHING WHITEPAPERS

2-1 DITTA White Paper on Cybersecurity of Medical Imaging Equipment

- Manufactures should manage security risk by illustrating various ports, protocols and services with data flow diagrams…
- Manufacturers should plan to continually monitor device vulnerability to identify and provide patches and updates…
- Manufacturers' field service representatives should be aware of their customers' specific security requirements…

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

2. PUBLISHING WHITEPAPERS

2-2 DITTA Whitepaper on Cybersecurity: Best Practices in the Medical Technology Manufacturing Environment

- Issued in February, 2019
- Based on NEMA CPSP 2-2018 Cyber Hygiene Best Practices
- A set of industry best practices and guidelines within the medical technology manufacturing facility and engineering processes

https://www.globalditta.org/uploads/media/DITTA_White_paper_on_Cybersecurity_-_Feb._2019_-_Final.


DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

DITTA White Paper on Cybersecurity:

Best Practices in the Medical Technology Manufacturing Environment

8 February 2019 *Page 1 of 23*

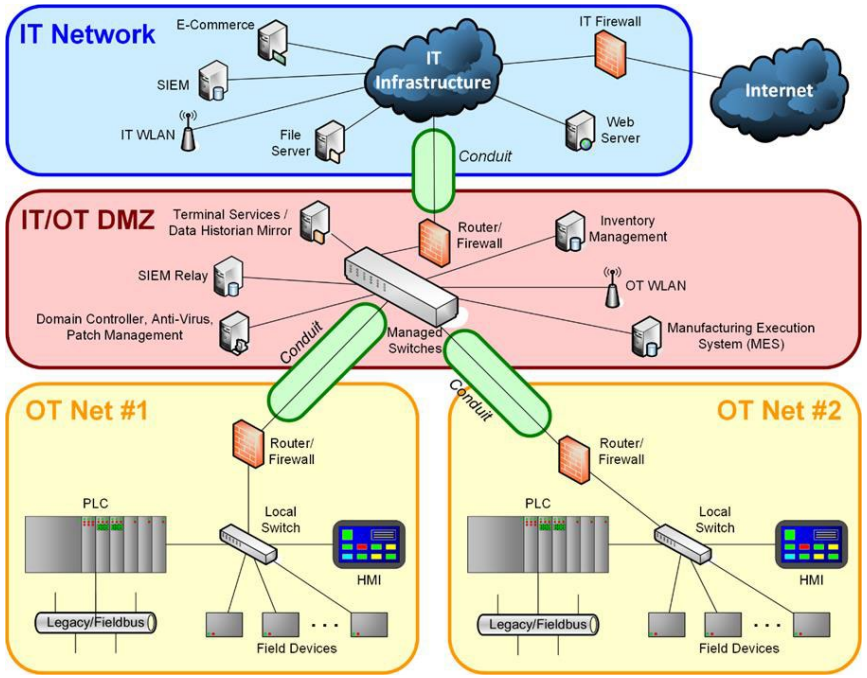
COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA Medical Imaging & Technology Alliance · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

2. PUBLISHING WHITEPAPERS

Seven fundamental principles for manufacturing facility and engineering process

1. Segmenting Networks
2. Understanding Data Types and Flows
3. Hardening Devices
4. Monitoring Devices and Systems
5. User Management
6. Updating Devices
7. Providing a recovery plan/escalation process



Segmenting networks

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA Medical Imaging & Technology Alliance · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · ITAC Information Technology Association of Canada

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

3. Activities in Member Associations

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

3. ACTIVITIES IN MEMBER ASSOCIATIONS

3-1 MDS2: MITA (DITTA member association, USA)

- Manufacturer Disclosure Statement for Medical Device Security
  - Official release of revision in Oct. 2019 (previous version in 2013)
    https://www.medicalimaging.org/2019/10/09/mita-releases-national-standard-for-medical-device-security/
- Four categories have been newly added

1. RMOT: Remote Service and Administration
2. **SBOM: Software Bill of Materials**
3. CONN: Connectivity Capabilities
4. MPII: Management of Personally Identifiable Information


ANSI/NEMA HN 1-2019

American National Standard—
Manufacturer Disclosure Statement for Medical Device Security

Published by

National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

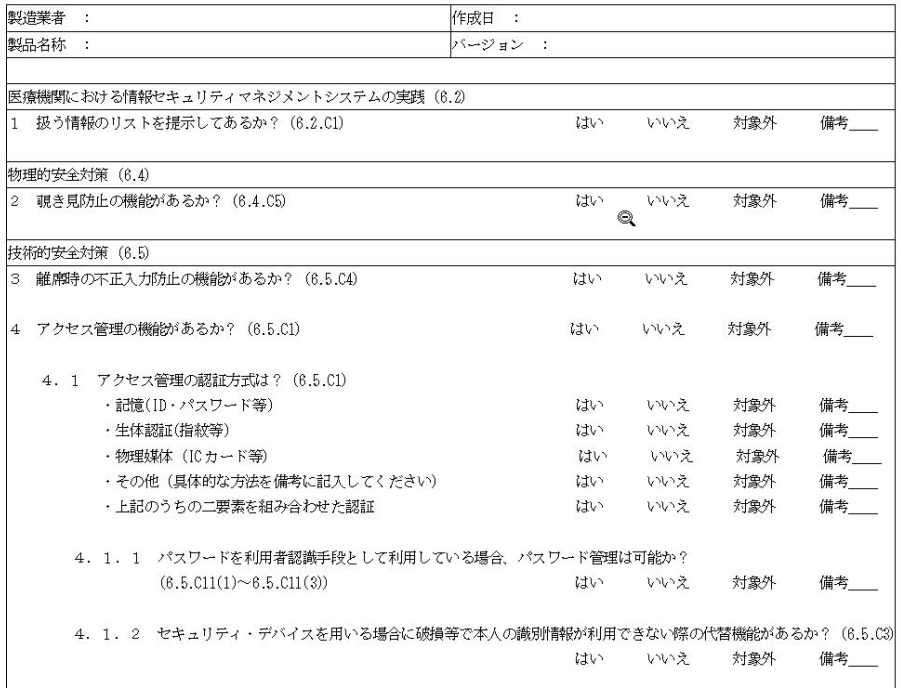
www.nema.org

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

3. ACTIVITIES IN MEMBER ASSOCIATIONS

3-2 MDS: JIRA (DITTA member association, Japan)

- Manufacturer Disclosure Statement
- A Check list of the device security following the concept of MDS2
- The list items are quite different from MDS2 based on the information security regulation of Japan.



製造業者　：	作成日　：
製品名称　：	バージョン　：

医療機関における情報セキュリティマネジメントシステムの実践（6.2）

1　扱う情報のリストを提示してあるか？（6.2.C1）　はい　いいえ　対象外　備考___

物理的安全対策（6.4）

2　覗き見防止の機能があるか？（6.4.C5）　はい　いいえ　対象外　備考___

技術的安全対策（6.5）

3　離席時の不正入力防止の機能があるか？（6.5.C4）　はい　いいえ　対象外　備考___

4　アクセス管理の機能があるか？（6.5.C1）　はい　いいえ　対象外　備考___

4．1　アクセス管理の認証方式は？（6.5.C1）
- ・記憶（ID・パスワード等）　はい　いいえ　対象外　備考___
- ・生体認証（指紋等）　はい　いいえ　対象外　備考___
- ・物理媒体（ICカード等）　はい　いいえ　対象外　備考___
- ・その他（具体的な方法を備考に記入してください）　はい　いいえ　対象外　備考___
- ・上記のうちの二要素を組み合わせた認証　はい　いいえ　対象外　備考___

4．1．1　パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？（6.5.C11(1)～6.5.C11(3)）　はい　いいえ　対象外　備考___

4．1．2　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？（6.5.C3）　はい　いいえ　対象外　備考___

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

4. DITTA Perspective on Cybersecurity

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

4. DITTA PERSPECTIVE ON CYBERSECURITY

As an international trade association we can contribute to medical device cybersecurity in terms of manufacturers by

1. Continuing development of **best practice documents** which are practical, feasible and promising quick effect
2. **Recognizing significant international standards**
3. Encouraging **information sharing** between manufacturers and healthcare providers by MDS2

DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

THANK YOU!

Keiichiro Ozawa

FUJIFILM Corporation

www.globalditta.org

Follow us on @DITTA_online

COCIR Advancing Healthcare | JIRA | Medtech Canada | MITA Medical Imaging & Technology Alliance, A Division of NEMA | THAIMED | IMEDA | 中国医疗器械行业协会 China Association for Medical Devices Industry | abimed Associação Brasileira da Indústria de Alta Tecnologia de Produtos para Saúde | Kmdica Korea Medical Devices Industrial Coop. Association | ITAC Information Technology Association of Canada