NII

A New Approach to Cyber Resilience in Healthcare

Hiroki Takakura

National Institute of Informatics, Japan

takakura@nii.ac.jp

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

IARIA

Hiroki Takakura

NII

- **Education**

  1990: Bachelor of Science, Kyushu University, Japan

  1992: Master of Science, Kyushu University, Japan

  1995: Ph.D., Kyoto University, Japan

- **Professional Experiences**

  1995: Researcher, Kyoto University

  - Visiting scholar, University of Illinois at Urbana-Champaign

  1995-1997: Assistant Professor, Nara Institute of Science and Technology

  1997-2009: Lecturer/Associate Professor, Kyoto University

  2010-2016: Professor, Nagoya University

  2016-Present: Professor, National Institute of Informatics,

  Director, Center for Strategic Cyber Resilience Research and Development

- **Social Contribution in Healthcare**

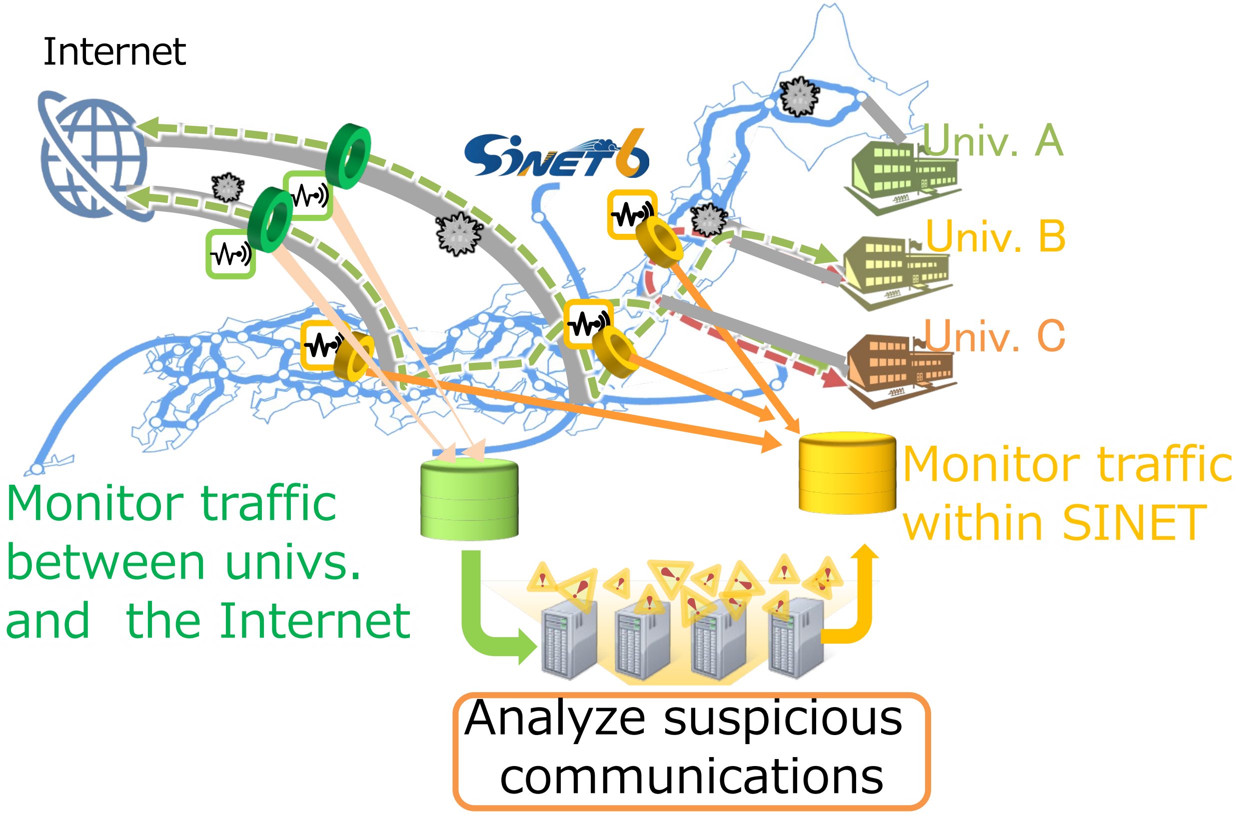
  - Ministry of Health, Labour and Welfare (MHLW), Japan

My current duty...interests

NII

NII Security Operation Collaboration Services (NII-SOCS)

- Monitors 3.5 billion suspicious communications daily across 100 national universities.
- Data is collected and analyzed in near real-time using advanced threat intelligence and machine learning techniques.



Vigilance still critical in highly encrypted networks
https://www.nature.com/articles/d42473-023-00326-y

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 National Institute of Informatics

My Current Interests

NII

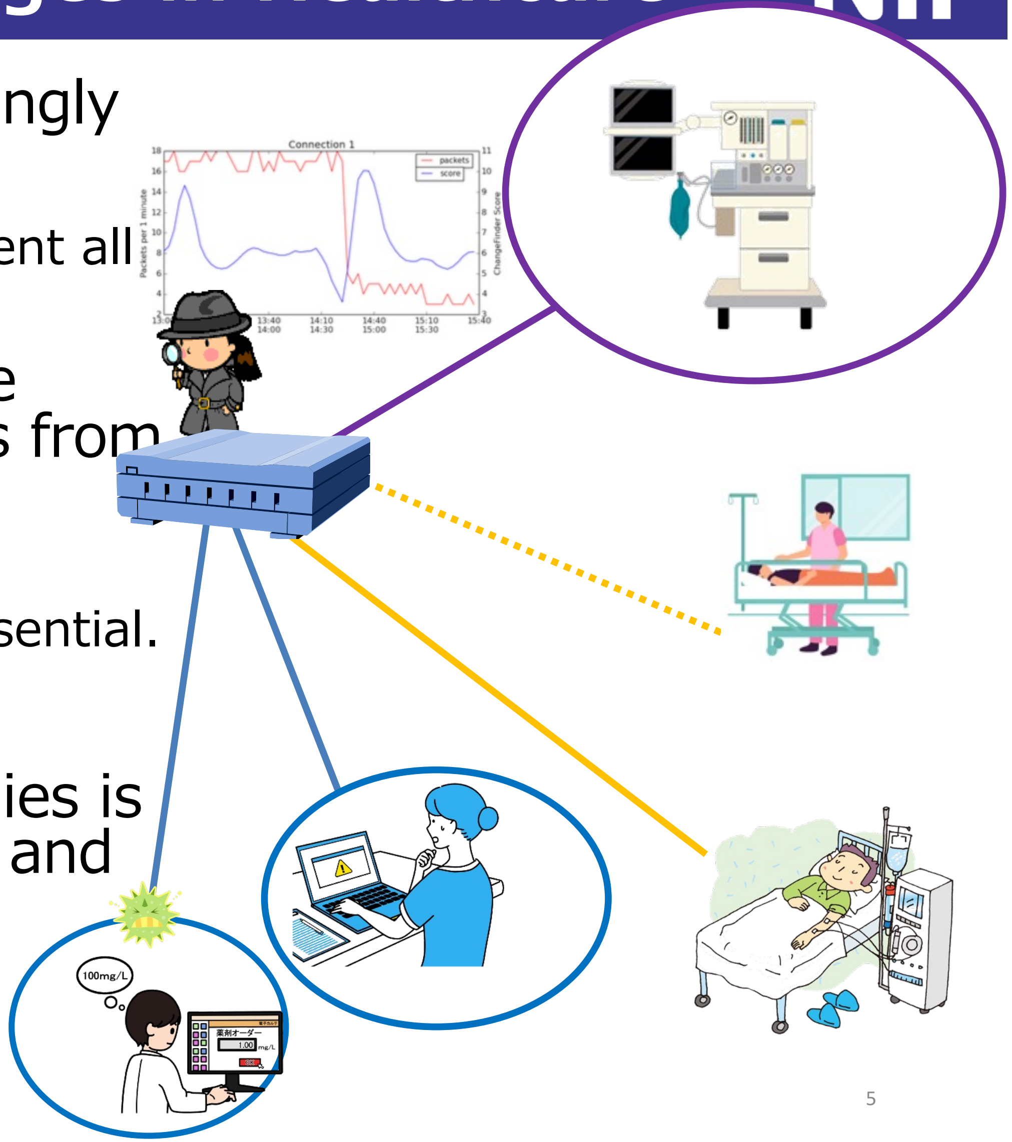
- Resilience Against Diverse Incidents
  - Includes cyberattacks and system malfunctions
- Many critical infrastructures require control over physical and chemical processes.
  - While control systems can be shut down immediately, most infrastructures cannot be stopped instantly.
- Service outages disrupt essential operations and can cause people to wait in line for an extended period.

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Cybersecurity Challenges in Healthcare

NII

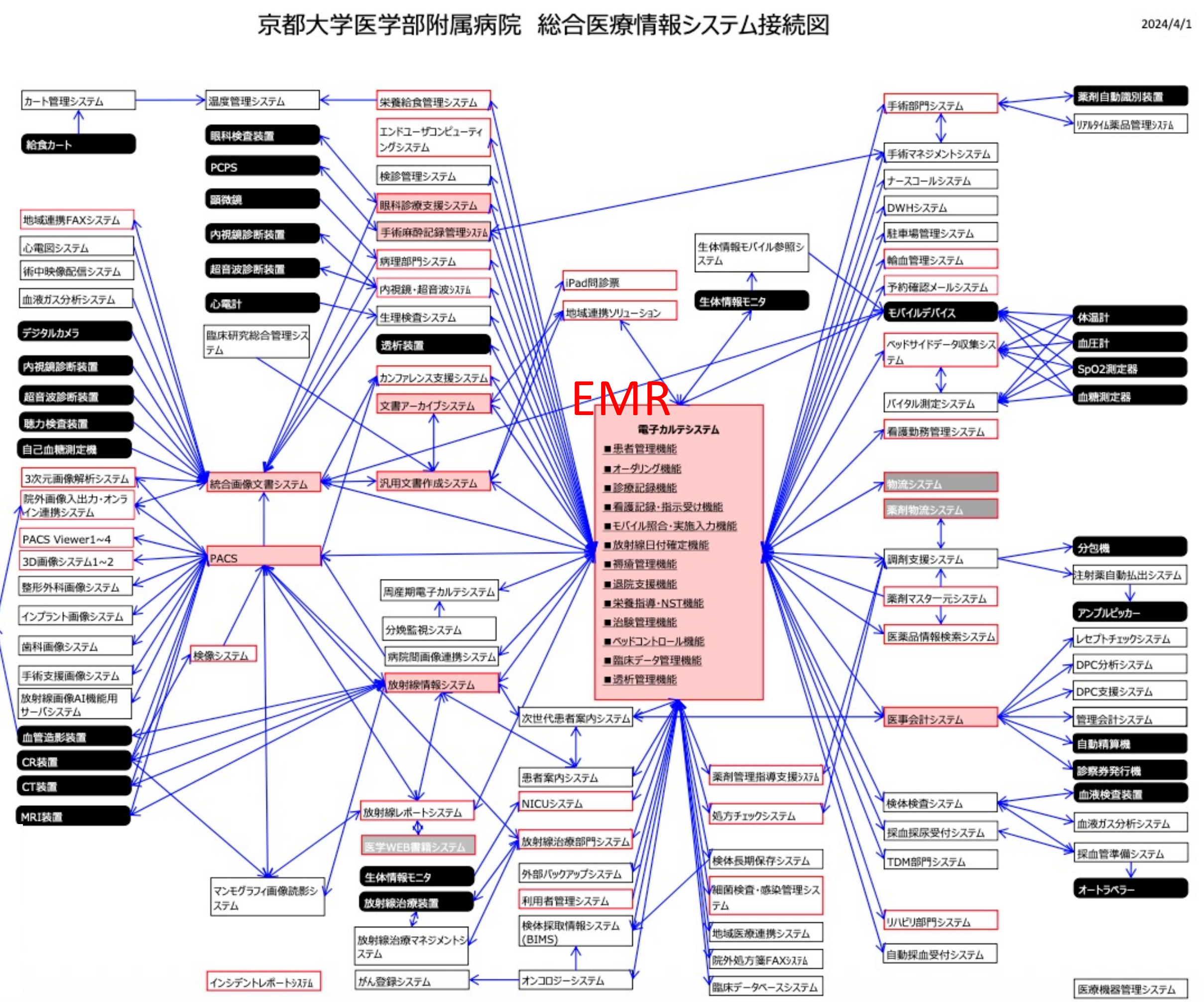
- Cyberattacks are becoming increasingly sophisticated
  - Even security experts cannot fully prevent all attacks
- Traditional countermeasures involve disconnecting compromised devices from the network
  - Preventive cybersecurity is limited, as continuous access to medical data is essential.
    - ”Safety first” is mandatory
- Integrating cybersecurity technologies is crucial for protecting patient safety and ensuring uninterrupted medical operations.



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

NII

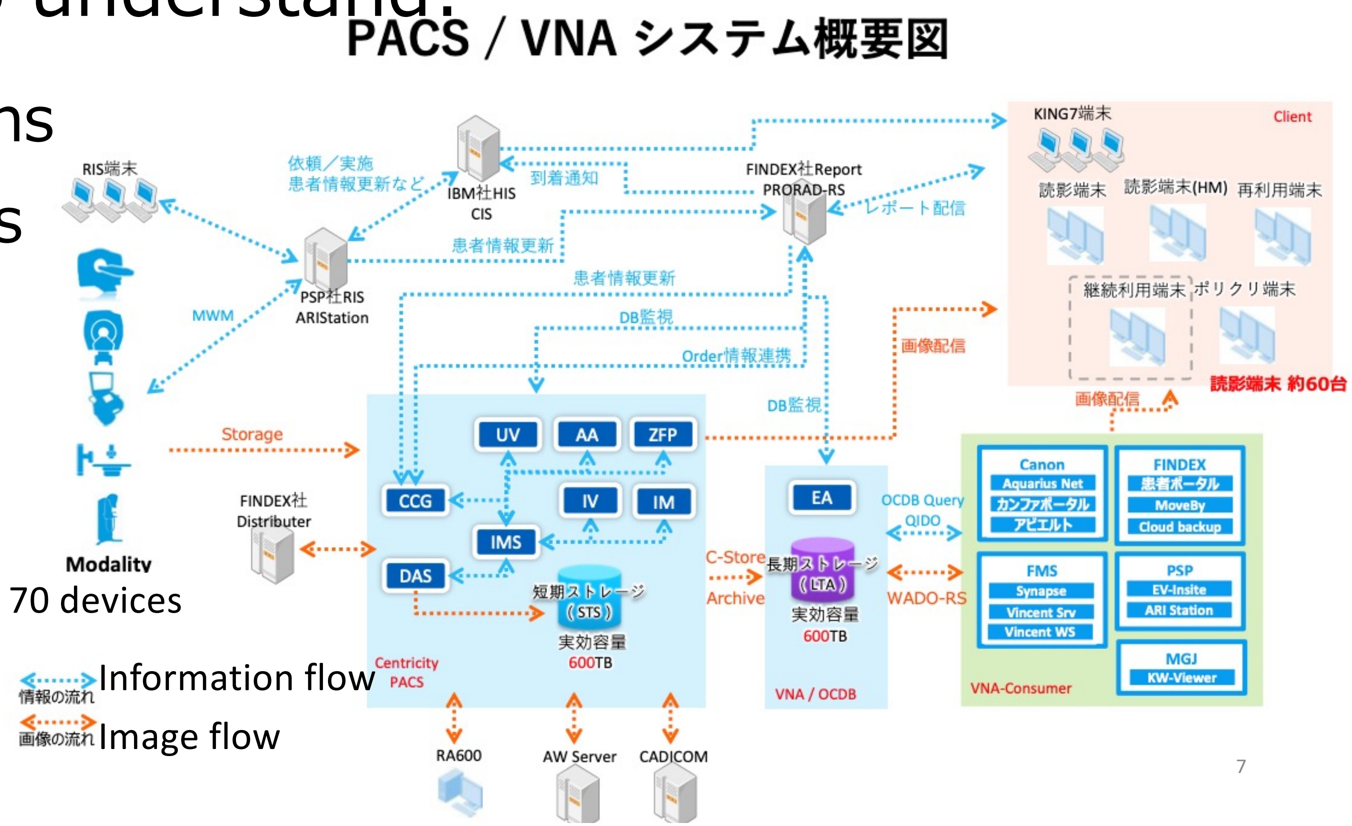
- Healthcare systems heavily rely on electronic medical records (EMRs), making data integrity crucial for maintaining continuous patient care.
- The healthcare information network is an environment where the EMR system is highly integrated with multiple other systems.
  - Asynchronous system replacements make it difficult to fully understand all system dependencies.



Medical Device Management Challenges

NII

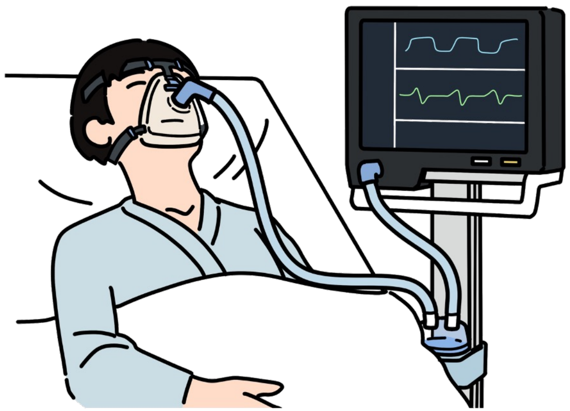
- The large variety and number of medical devices, even in one system, complicate system management
- It is necessary to understand:
  - Physical connections
  - Logical connections
  - Dependencies among devices
    - Information flow
    - Data volume

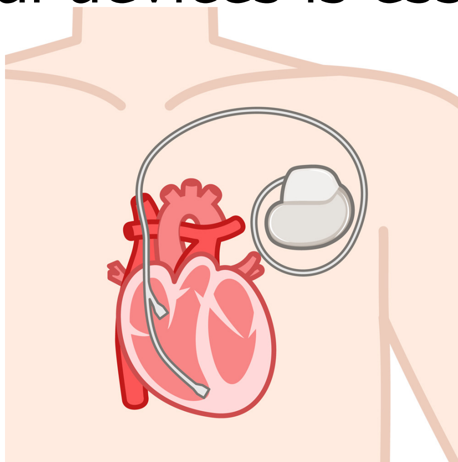


大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Critical Device Identification

- Even a small number of device malfunctions can lead to critical situations.
  - E.g., Class III and IV devices require immediate attention.
- Support systems are needed to ensure continuity of medical services.
  - Identifying such critical medical devices is essential.





Key Functions of the Support Systems

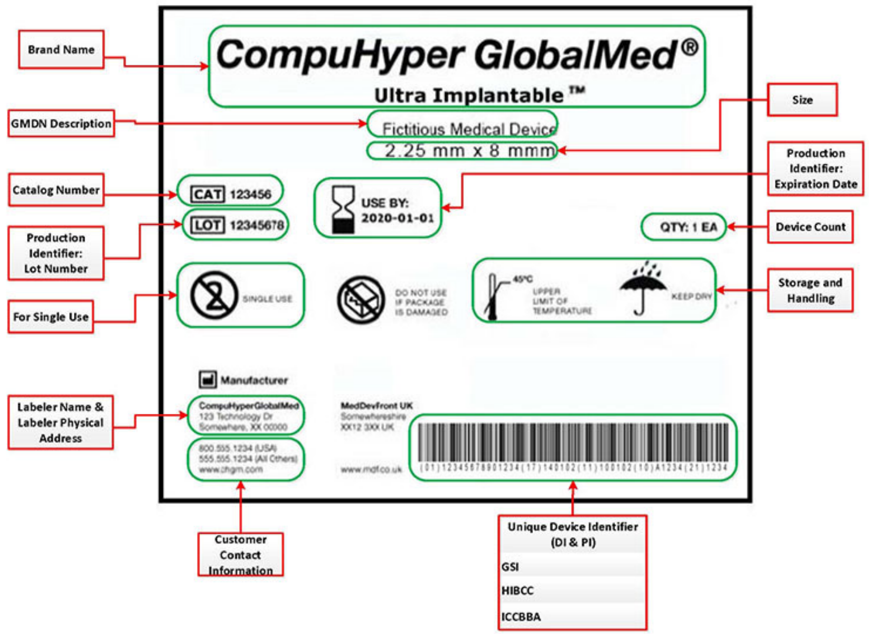
NII

- Critical Medical Device Management
  - Identifies and manages Class III and IV devices that require immediate attention during anomalies.
- Device-Patient Mapping with Unique Device Identification (UDI)
  - Utilizes UDI and network information to map devices to patients accurately.
- Software Inventory and Vulnerability Management
  - Supports Software Bill of Materials (SBOM) for detailed software inventory and vulnerability management.
- Network Traffic and Threat Detection
  - Integrates traffic monitoring, anomaly detection, and honeypot technologies for real-time threat detection.

Device and Vulnerability Identification

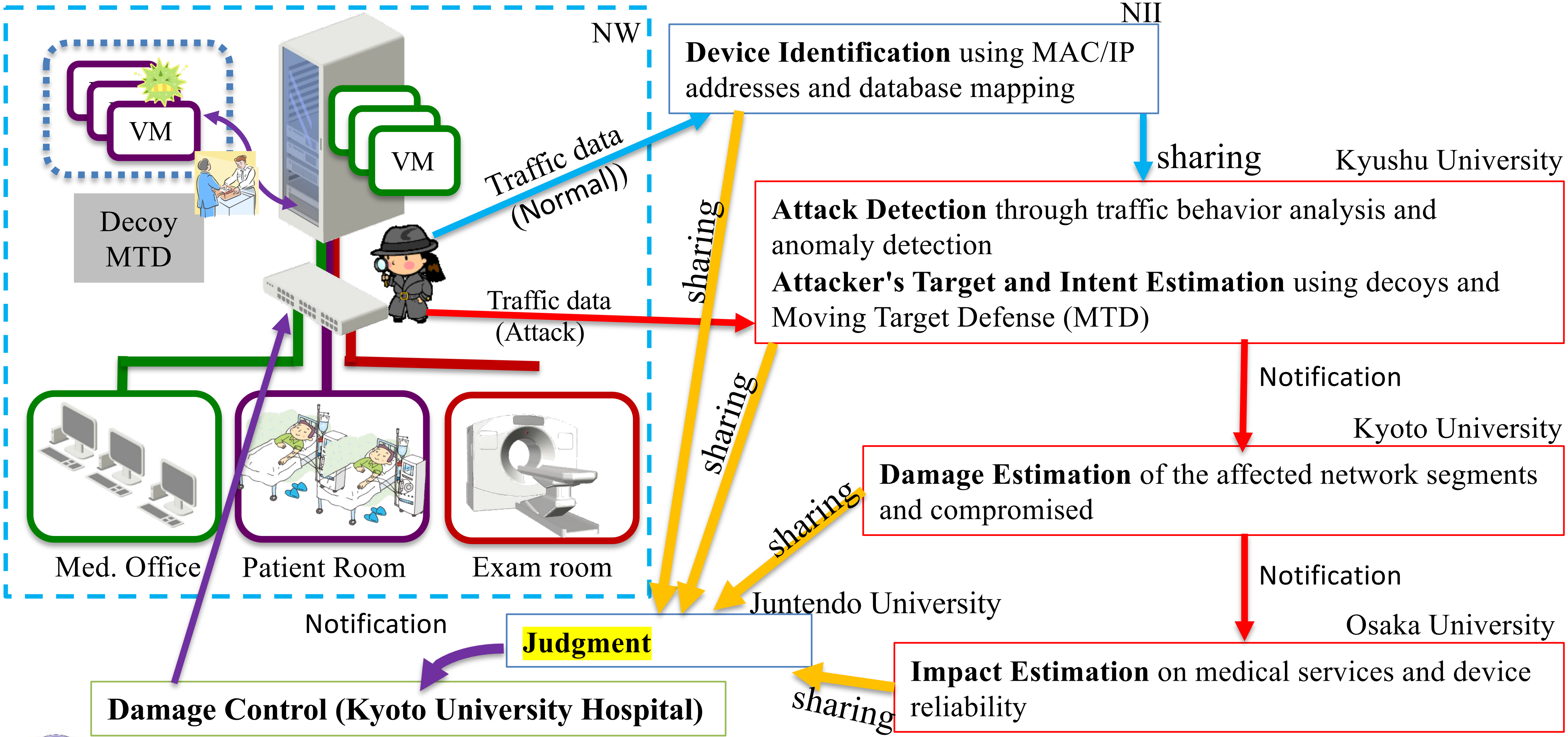
NII

- Software Bill of Materials (SBOM) (IEC 81001-5-1)
  - Identifies devices with potential vulnerabilities
    - Unique Device Identification(UDI)
      - Device ID + Production ID
        - E.g., serial number
  - Patient DB
    - Wristband ID, UDI,
  - IT DB
    - MAC address/IP address



- By combining these data sources, we can identify patients who may be at risk due to device vulnerabilities

Basic Concept of Medical Resilience Support System

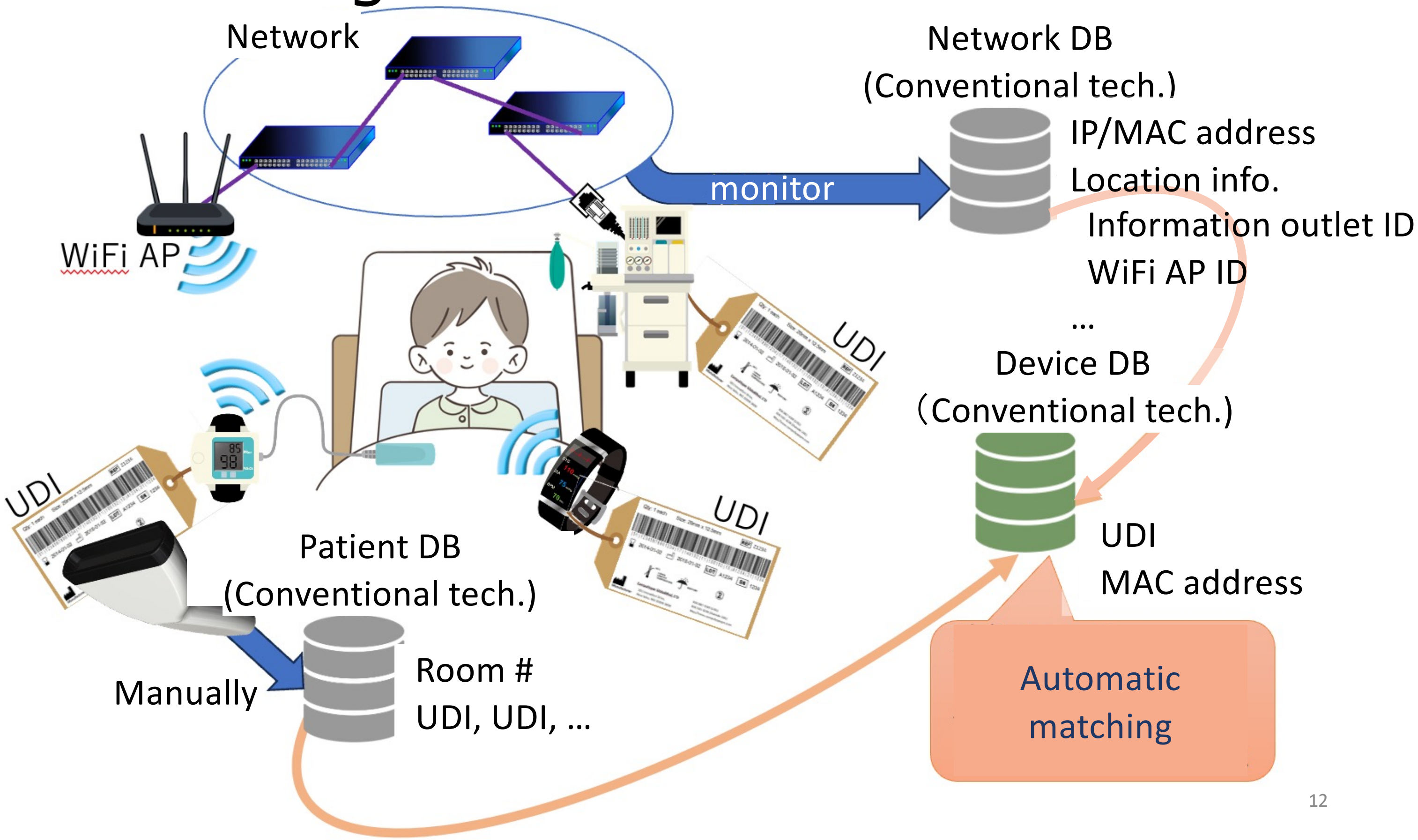


Data sharing and notification mechanisms are employed during both normal operations and attack scenarios.

Device Identification

NII

- The system monitors network traffic and matches device information using:
  - Network DB
  - Patient DB
  - Device DB



Attack Detection

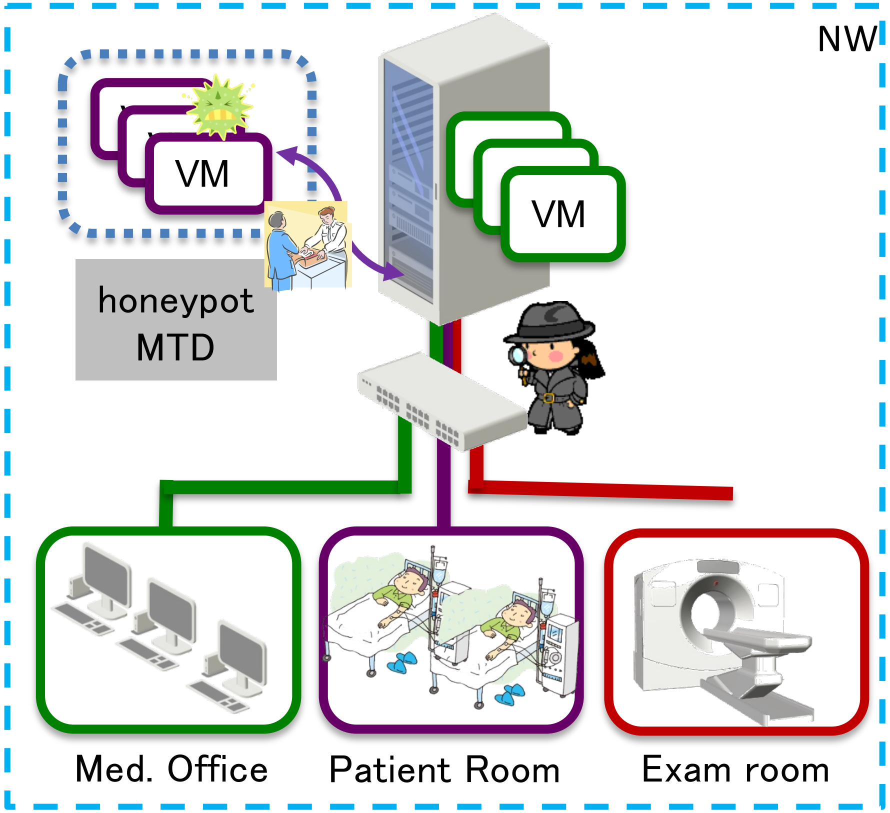
NII

- Assessment
  - Capture network traffic to analyze communication patterns and volumes during normal operations.
  - Derive dependencies among devices.
  - Pre-calculate the impact on medical services if devices become unavailable.
- Attack estimation
  - Detect anomalies and suspicious activities in real-time
    - Conventional anomaly detection techniques can be adopted.
  - Identify affected devices
    - Estimate the likelihood of device compromise or malfunction.

Attacker's Target and Intent Estimation

NII

- Honeypots and Moving Target Defense (MTD)
  - Trap and delay attackers for effective threat analysis.
    - Profile attackers to infer intent, skill level, and tactics.
  - Identify evidence of compromise to investigate affected devices.
    - Attacked vulnerability estimation.



Damage and Impact Estimation

NII

- Ensure security
  - Implement device and user authentication.
- Assess device security using SBOM (Software Bill of Materials)
  - Identify potentially affected devices and alternative devices.
- Evaluate the trustworthiness of network segments and potential threat propagation
  - Impact estimation helps prioritize response actions and containment strategies.

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Judgement and Damage Control

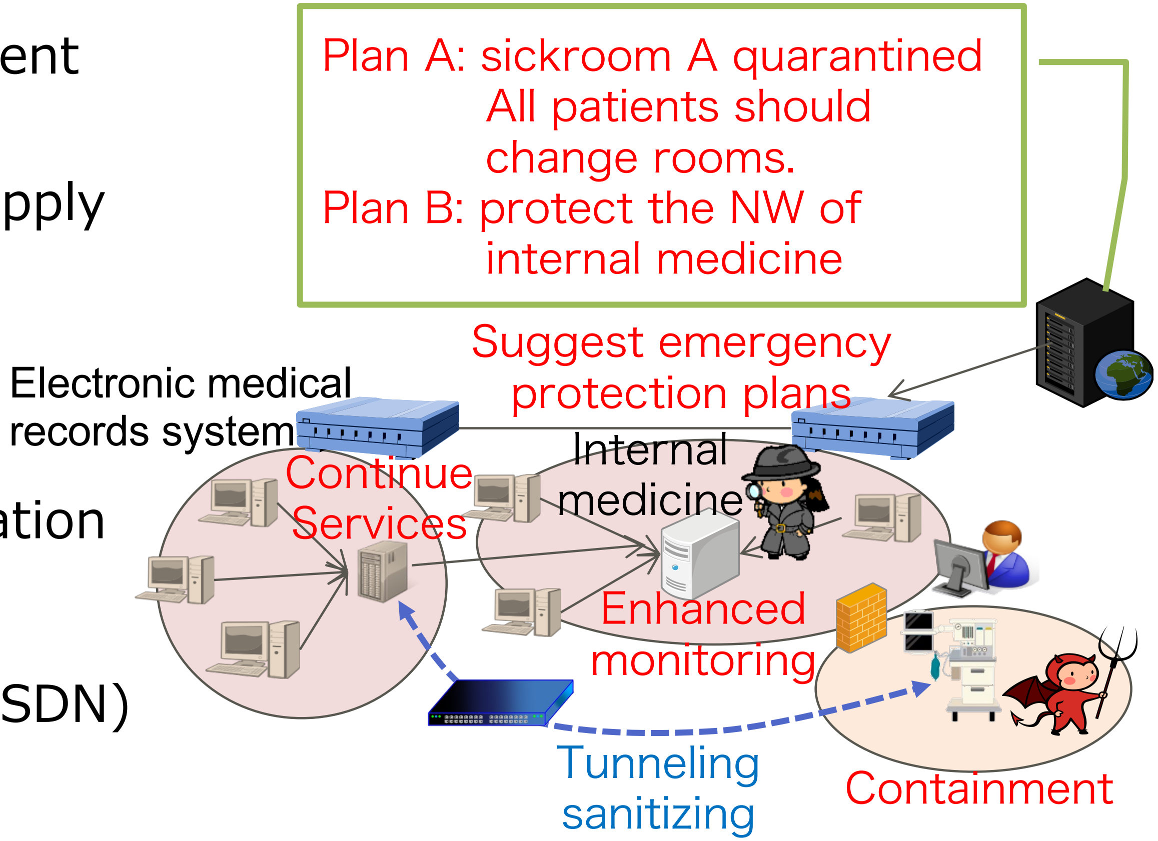
NII

■Availability Assurance

- ◆Minimize residual risk and prevent further damage.
  - Using the attacker's profile, apply proactive defense

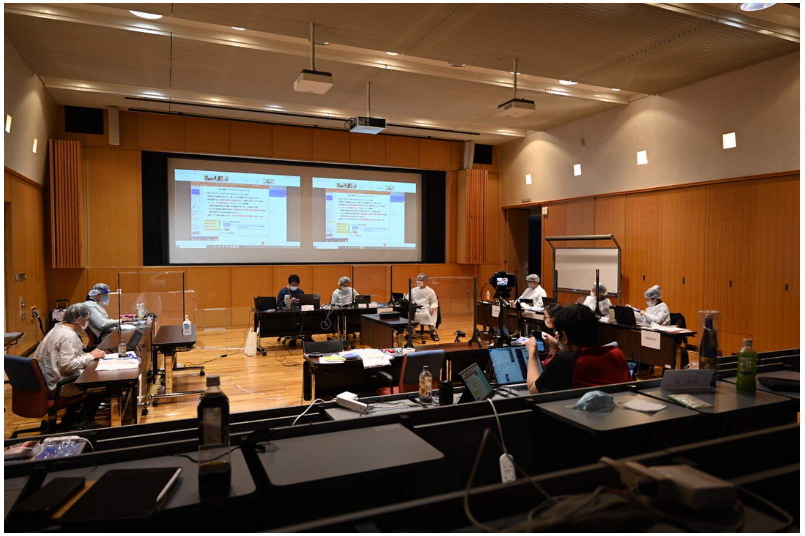
■Maximize availability while minimizing risk

- ◆Use tunneling and data sanitization
  - Rescues surviving data
- ◆Software Defined Networking (SDN)
  - Enables real-time network segmentation.



Attack Detection and Impact Assessment

- Assessment of potential impact on medical services
  - Identify devices that are inoperable or at high risk of becoming inoperable due to attacks.
  - Identification of medical services at risk of interruption and patients likely to be significantly affected
- Appropriate network segmentation and access restrictions
  - Maintain continuity of care during incidents.



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Staff Notification and Data Protection

NII

- Balancing Security and Patient Safety
  - Promptly notify relevant medical staff.
  - Apply safe data handling protocols to prevent further damage
  - Ensure essential services remain operational
- If alternatives are unavailable, provide swift and sufficient information to support decisions about transferring patients to nearby facilities.

Summary

Importance of resilience

- Cyber resilience is essential for maintaining safety and continuity in healthcare operations.
- Resilient infrastructure, including cyber components, offers practical solutions for critical infrastructures
- Achieving resilience requires integration of both conventional and advanced technologies