Appendix

1. Technical details on H-LINCOS

In H-LINCOS, medical record data is backed up using secret sharing as depicted in Figure 2. First, medical record data is converted to SS-MIX data. Next, the original SS-MIX data is converted into multiple data called shares, each of which is of no use on its own. Finally, the shares are distributed to remote data servers via secure communication channels and stored in those data servers.

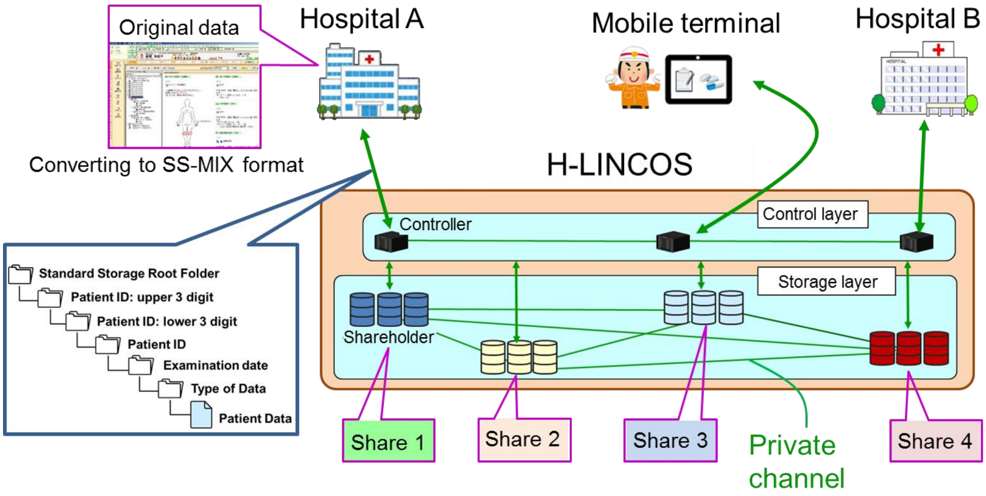


Figure 2: Conceptual structure of H-LINCOS

With this method, even if some servers have crashed or are lost, the original data can be restored from the remaining servers. On the other hand, the original data cannot be restored unless a certain number of distributed data are gathered. Therefore, the confidentiality of the data can be enhanced, enabling ***secure backup***. In addition, by conforming to SS-MIX, it is possible to ***cross-reference medical record data***. Moreover, we developed data access technology for high-speed search, a so-called fast secret sharing driver, and realized ***rapid restoration of important data items of medical records required in disaster situations***.

In our implementation, the SS-MIX data provided by KHSC was first transmitted over an 800 km secure channel to the Koganei access point on JGN. It was then converted to shares. They were then distributed to data servers in the Osaka, Nagoya, and Otemachi access points via secure communication channels, and stored there.

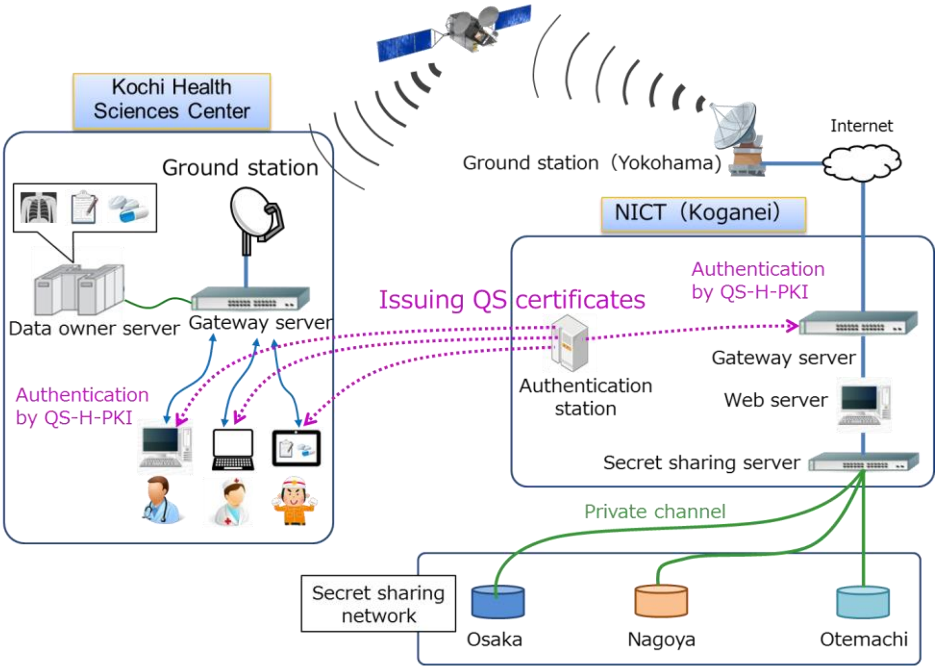


Figure 3: Configuration of access control scheme based on quantum-safe PKI

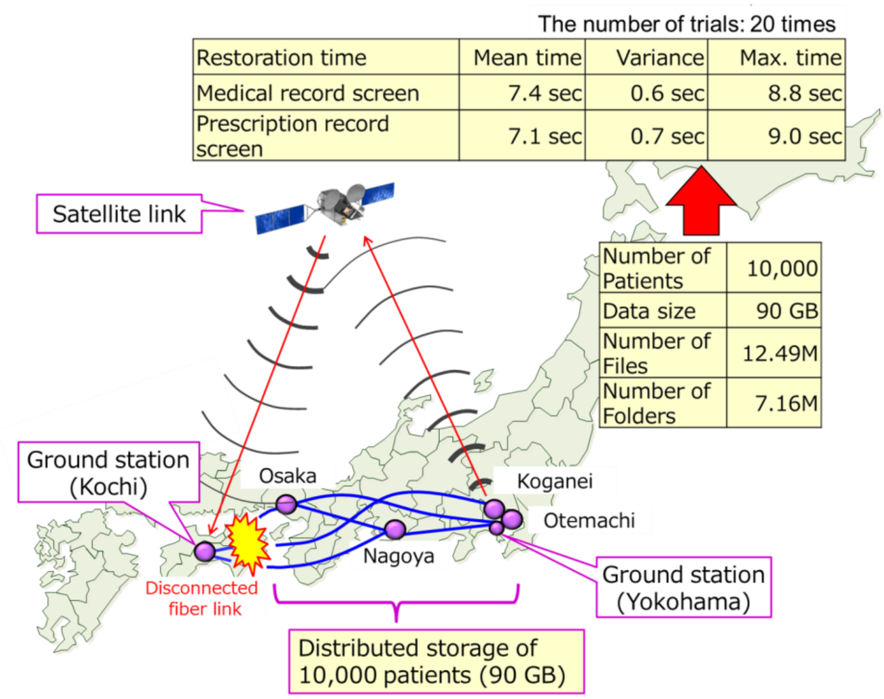
The secret communication channel consists of a symmetric key cipher seeded with a pre-shared physical random number pair. Its security is "quantum-computer resistance", which is difficult to decrypt even with quantum computers. In the KHSC and Koganei access points, NEC's symmetric key cipher system was installed, which enables high-speed encryption at the data link layer. In addition, in the 100 km area of Tokyo, including Otemachi and Koganei, a quantum key distribution network was used to realize secure communication, which allows secret sharing with "information theoretical security" that cannot be decrypted by any computer.

Access control for the H-LINCOS is executed by using highly secure user authentication and access right management based on national qualifications for healthcare workers. More precisely, the access control scheme is designed by following the Healthcare Public Key Infrastructure (H-PKI) recommended by the Ministry of Health, Labor and Welfare. Furthermore, a next generation scheme of PKI based on quantum-safe public-key cryptography is newly introduced to increase the security to a level of quantum-computer resistance, making it difficult to decipher even with a quantum computer. This so-called quantum-safe H-PKI (QS-H-PKI) is depicted in Figure 3.

As quantum-safe public-key cryptography, we selected seven schemes that are expected to be promising in the standardization process currently underway by the National Institute of Standards and Technology (NIST). Specifically, combining two hash-based schemes for issuing root certificates, two schemes (lattice-based and isogeny-based) for key exchange, and three schemes (two lattice-based and one multivariate-based) for digital signature, a total of 12 types of cryptographic tool sets (so-called cipher suites) were prepared. These were implemented in compliance with the Internet standard Transport Layer Security (TLS). It was confirmed that all cipher suites operate normally with a processing time of about 100 to 250 ms. Although this processing speed is about 10 times that of the existing TLS, it is sufficiently practical for our purpose. In our SS-MIX data restoration experiment using a satellite link, the fastest cipher suite was adopted for access control.

In restoring SS-MIX data assuming a disaster situation, two data servers in Osaka, Nagoya, or Otemachi, were selected, and data items such as prescription records and allergy information were restored in the Koganei server. The data was then sent to the SKY Perfect JSAT ground station in Yokohama via a secret communication channel on the Internet, transmitted to the KHSC ground station via the satellite link, and finally restored in the medical viewer terminal in KHSC.

2. Experimental results



The number of trials: 20 times

Restoration time	Mean time	Variance	Max. time
Medical record screen	7.4 sec	0.6 sec	8.8 sec
Prescription record screen	7.1 sec	0.7 sec	9.0 sec

Number of Patients	10,000
Data size	90 GB
Number of Files	12.49M
Number of Folders	7.16M

Figure 1: Network configuration of H-LINCOS and experimental results. (An enlarged version)

Conducting 20 restoration campaigns, we confirmed that the average time from entering the patient ID to displaying the medical record viewer screen was 7.4 seconds, the maximum was 8.8 seconds, and the time from clicking the prescription record selection button to displaying the contents was 7.1 seconds on average, and the maximum was 9.0 seconds (see Figure 1).

< Technical Contact >

Masahide Sasaki
Advanced ICT Research Institute
NICT
Tel: +81-42-327-6524
E-mail: psasaki@nict.go.jp

Kazuyuki Kitamura
Medical Information Center
KHSC
Tel: +81-88-837-3882
E-mail: kazuyuki_kitamura@khsc.or.jp

Manabu Ichikawa
Planning, Architecture and Environmental Systems
Shibaura Institute of Technology
Tel: +81-48-720-6234
E-mail: m-ichi@shibaura-it.ac.jp

Tetsuya Miyagishima
Medical Business Department
SBS Information Systems
Tel: +81-54-283-1450
E-mail: t_miyagishima@sbs-infosys.co.jp

Kota Suzuki
Space & Satellite Business Group
Enterprise Business Division
SKY Perfect JSAT
Tel: +81-3-5571-1646
E-mail: Suzuki-kota@sptvjsat.com

Hiromi Iizuka
National Security Solution Division
NEC Corporation
Tel: +81-42-333-5591
E-mail: qkd-inquiry@nss.jp.nec.com

Atsushi Yamada
Research and Development
ISARA Corporation
Tel: +1-226-972-1792
E-mail: atsushi.yamada@isara.com

Prof. Johannes A. Buchmann
Department of Computer Science
Technische Universität Darmstadt
Tel: +49-6151-16-20660
E-mail: buchmann@cdc.informatik.tu-darmstadt.de

< Media Contact >

Sachiko Hirota
Press Office
Public Relations Department
NICT
Tel: +81-42-327-6923
E-mail: publicity@nict.go.jp

Izumi Matsukura
Public Relations and Marketing
ZenmuTech
Tel: +81-3-5436-6541
E-mail: press@zenmutech.com

Atsumi Shibata
Planning and Public Relations Section
Shibaura Institute of Technology
Tel: +81-3-6722-2900
E-mail: koho@ow.shibaura-t.ac.jp

Minoru Teramoto
Medical Business Department
SBS Information Systems
Tel: +81-54-283-1450
E-mail: m_teramoto@sbs-infosys.co.jp

Takeshi Hamada
Public Relations Office
Corporate Communications Division
NEC Corporation
Tel: +81-3-3798-6511
E-mail: press@news.jp.nec.com

Andrea Hruska
Marketing, PR and Communications
ISARA Corporation
Tel: +1-905-749-3595
E-mail: andrea.hruska@isara.com