of standard DICOM servers and a Client's computer with LAN and the INTERNET. The DICOM-NAS was able to communicate with both the DICOM servers and the Client's computer. After transferring the images from the DICOM servers to the Client's computer, it will immediately delete all of the images. The downloading time, defined as the time needed for downloading 45 slices (12.8 MB) of CT images (abdomen, 512 × 512, 8 bit, 292 kB/slice) from the DICOM servers to the Client's computer, is measured in four kinds of network configurations (Fig. 6). This time period is 10 times.

3. Result

3.1 Performance

The DICOM-NAS was connected to two different DICOM servers, the Image Central Test Node (distributed by Kuratorium OFFIS e. V., University of Oldenburg) and DgS Image server (provided by DgS Computer Co., Ltd.). The Client was connected to the DICOM-NAS through the LAN or the INTERNET. After receiving a request for images from the Client's computer, the DICOM-NAS was able to download the DICOM images from each of the servers, and then sent the images to the Client's computer. When the Image Central Test Node and DgS Image server were both used, the DICOM-NAS was still able to download and transfer the DICOM images. Furthermore, the DICOM-NAS would immediately delete all of the images downloaded from the DICOM servers after the transfer was completed.

3.2 Measurements

The time required to download 45 CT image slices from the DICOM servers to the Client was measured in this study. The average and standard deviation of the

downloading times are listed in Fig. 7. These images were transferred from the DICOM servers to the DICOM-NAS using DICOM protocol, and were then transferred to the Client using HTTP, excluding the LAN1 that the Client was directly connected to DICOM servers and was used for downloading the images with HTTP. When the Client was directly connected to the DICOM servers with a 10 Mbps line (LAN1), the downloading time was 16.92 sec (SD: 0.3438 sec). When the Client was connected to the DICOM servers through the DICOM-NAS using cable lines of 10 Mbps (LAN2) or 100 Mbps (LAN3), the downloading times for these images were 32.86 sec (SD: 0.3298 sec) in LAN2 and 23.45 sec (SD: 0.2119 sec) in LAN3, respectively. When the DICOM-NAS was connected to the Client through a 24 Mbps (max) ADSL line and connected to the DICOM servers through a 10 Mbps lines (INTERNET), the downloading time was 46.82 sec (SD: 3.250 sec). The standard deviation of the INTERNET was the largest in four network configurations. A comparison of the connecting methods LAN1 and LAN2 revealed that the downloading time increased by 94.2%. However, a comparison between LAN2 and LAN3 revealed that the downloading time decreased by 28.6% when a faster network was used. A comparison between LAN3 and the INTERNET showed that the standard deviation of the INTERNET was larger than that of LAN3, and that the downloading time increased by 42.5% when the INTERNET was used.

4. Discussion

Today, many web-based DICOM servers and viewers can share images from anywhere using Internet Technology (IT) and browsers; some of the images are distributed for free. However, many of them only have the function to display the DICOM images and do not have the Query/Retrieve function [3-7]. Others may have both

functions, but the Query/Retrieve function depends on particular image databases [8-13]. In general, a patient's original images generated by CTs or MRs in hospitals are stored in DICOM servers. Therefore, extra servers that have large storage devices for image storage must be installed anywhere inside or outside a hospital, and this (using IT, but that) would cost a large amount of money. As an alternative method, a web-based server could be used to store the patients' original images to reduce the installation cost; however, the threatening risks of invading the patient's privacy are higher because an attacker can steal and modify the images via the INTERNET. We therefore designed and developed the DICOM-Network Attached Server to solve the cost and security problems. The DICOM-NAS can communicate with two different DICOM servers, and it enables the Client to obtain medical information and images from the DICOM servers. The DICOM-NAS plays an important bridge role between the DICOM protocol and HTTP and can immediately delete all information and images downloaded from the DICOM server after transferring them to the Client's computer. Since the DICOM-NAS only temporarily stores the requested images, and the DICOM servers keep all of the original DICOM images, unwanted outsiders attempting to access the DICOM-NAS cannot access any patients' medical information.

Figure 7 illustrates that the downloading time increases when the DICOM-NAS is used. After the Client requests to download the images, all of the images are temporarily stored in the DICOM-NAS. This extra information transfer and temporary downloading time increases the total working time. However, using faster cable lines can reduce this increase. According to our experience, the increased time by DICOM-NAS could be very small when the FTTH (Fiber To The Home), a faster ADSL, or a faster PC is used.

5. Conclusion

The DICOM-NAS developed in the present study has the following features: (a) It plays a bridge role between the DICOM protocol and HTTP. (b) It does not require a large amount of storage and can improve information security to better protect patients' privacy. (c) It can easily install, transfer, and distribute information and images stored in the DICOM servers. When medical images are transferred from the DICOM-NAS to the Client, image confidentiality can be improved on the INTERNET using VPN (Virtual Private Network) technology [18].

The DICOM-NAS program can be downloaded for free from the website http://umeken3.ahs.kitasato-u.ac.jp, and can be easily installed. In conclusion, the DICOM-NAS is useful because of the above-mentioned advantages, and it does not generate much cost.

6. Acknowledgement

This study was partially supported by a Grant-in Aid for Exploratory Research, No. 40142319, 2002-2003, and a Grant-in Aid for Scientific Research (A), 15209022, 2003-2005 from the Japan Ministry of Education, Culture, Sports, Science, and Technology.

References

[1] Ministry of Health, Labor, and Welfare of Japan, http://www1.mhlw.go.jp/toukei-i/isc99_8/index.html.

[2] T. Umeda, K. Inamura, K. Inamoto, *et al.*, Development and evaluation of oral reporting system for PACS. Comput. Meth. Prog. Bio. 43 (1994) 115-123.

[3] T. Osaki, H. Ban, H. Matsuo, *et al.*, A teleradiology system with realtime and E-mail-based operating modes. Med. Imag. Tech. 16(6) (1998) 615-621.

[4] A. Alaoui, J. Collmann, D. Nguyen, *et al.*, Implementing a secure teleradiology system using the Internet. CARS 2003, (2003) 803-808.

[5] N. Yokohama, Construction of DICOM-WWW gateway by open source, and application to PDAs using the high-speed mobile communications network. Jpn. J. Radiol. Technol. 9(9) (2003) 1155-1163.

[6] Johannes Bernarding, Andreas Thiel, and Alexander Grzesik, A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption. Int. J. Med. Inform. 64(2-3) (2001) 429-438

[7] Pengyu Cao, Masao Hashiba, Kouhei Akazawa, *et al.*, An integrated medical image database and retrieval system using a web application server. Int. J. Med. Inform. 71(1) (2003) 51-55

[8] http://mars.elcom.nitech.ac.jp/dicom.

[9] K. Muto, Y. Emoto, K. Anami, *et al.*, Low/No cost DICOM server which is integrated with JAVA viewer and reporting system on a web browser. RSNA 2001 Supplement to Radiology 221 (2001) 739.

[10] Shawn P. Laird, Johnny S. K. Wong, William J. Schaller, *et al.*, Design and implementation of an Internet-based medical image viewing system. J. Syst. Software

66(2)15 (2003) 167-181.

[11] H. Munch, U. Engelmann, A. Schroeter, *et al.*, Web-based distribution of radiological images from PACS to EPR. CARS 2003, (2003) 873-879.

[12] G. C. Sakellaropoulos, G.. C. Kagadis, C. Karystianos, *et al.*, An experimental environment for the production, exchange and discussion of fused radiology images, for the management of patients with residual brain tumor disease. Med. Inform. 28(2) (2003) 135-146.

[13] J. Bernarding, A. Thiel, I. Decker, *et al.*, Implementation of a dynamic platform-independent DICOM-server. Comput. Meth. Prog. Bio.65(1) (2001) 71-78

[14] Kuratorium OFFIS e. V., University of Oldenburg, http://www.offis.de/index_e.php

[15] DICOM Supplement 23 Structured Reporting Object, http://medical.nema.org/medical/Dicom/Final/sup23_ft.pdf.

[16] K. Inamura, DICOM Structured Reporting. Med. Imag. Tech. 19(2) (2002) 101-107.

[17] H. H. Hawkins, Jr., Clinical Information System for a Multi-disciplinary Breast Center: Integration of Structured Reporting, Activity-Based Costing, and Continuous Quality Improvement. RSNA 2001 Supplement to Radiology 221 (2001) 741.

[18] H. Tachibana, T. Umeda, Y. Iwata, Secure web-based teleradiology system with integrated structured reporting and VPN technology on a web browser. Med. Imag. Tech. 22(1) (2004) 26-34.

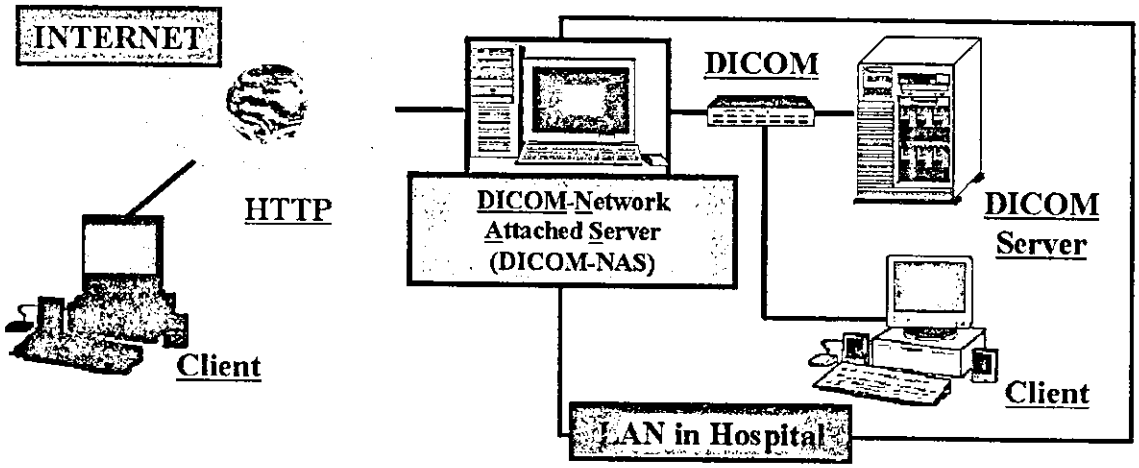

Fig.1 Scheme of DICOM-Network Attached Server

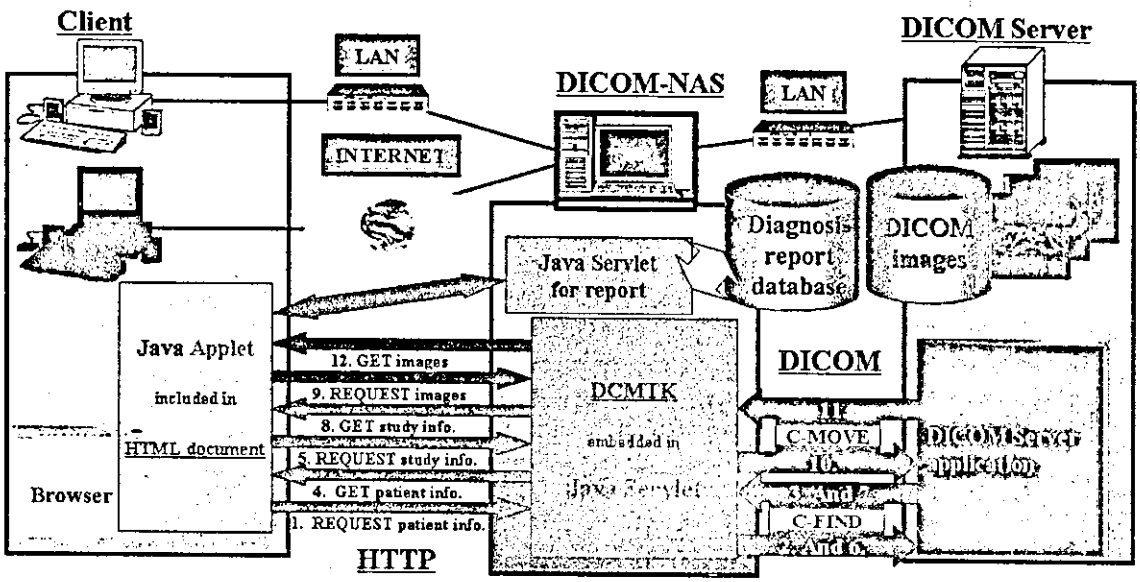

Fig.2 System configuration of DICOM-NAS, and data flow after downloading Java Applet that have the functions of Query / Retrieve and display of DICOM images from DICOM-NAS

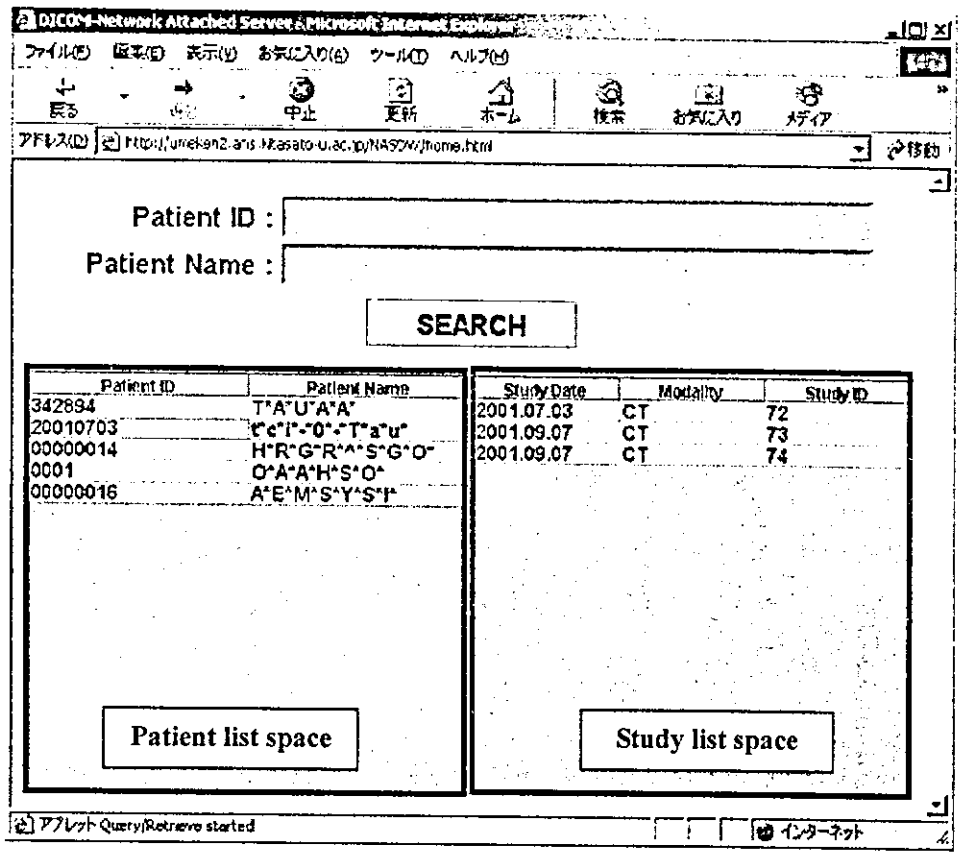

Fig.3 GUI of DICOM-NAS (Query/Retrieve)

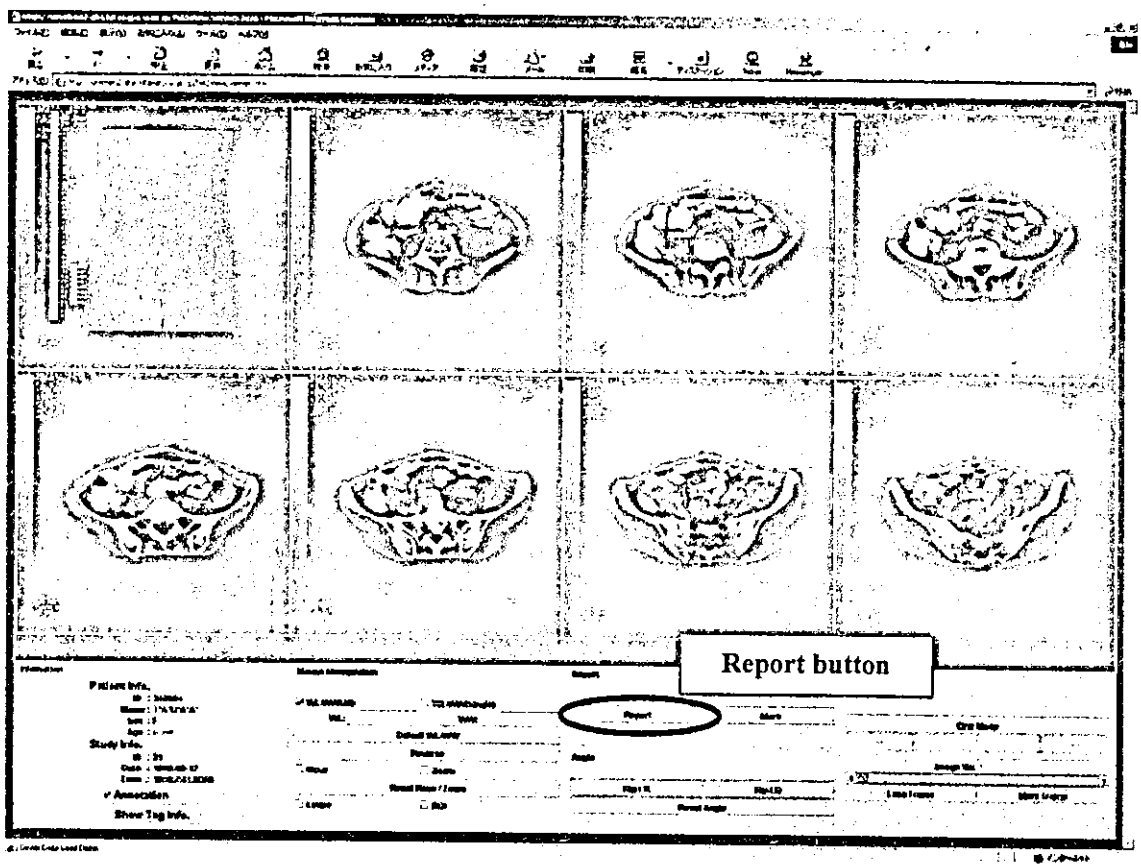

Fig.4 GUI of DICOM-NAS (DICOM web viewer)

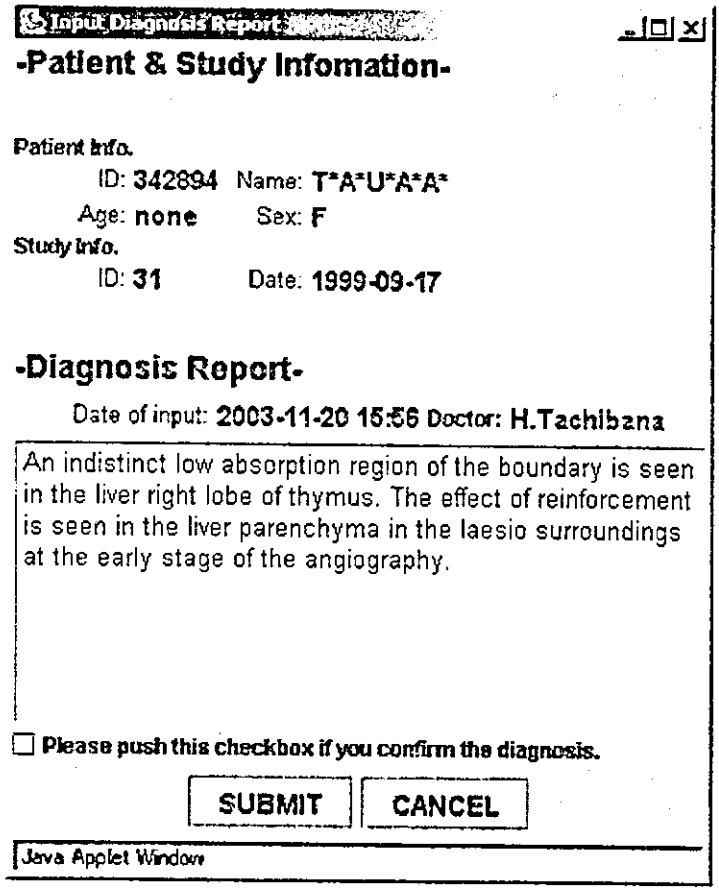

Fig.5 Screenshot of a window for inputting diagnosis report

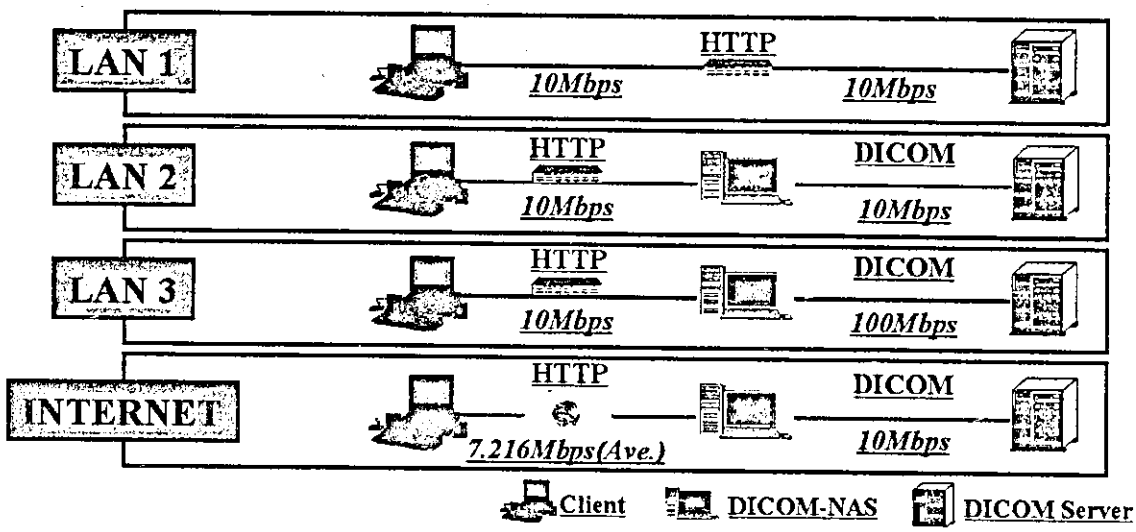

Fig.6 Network configurations for measuring the downloading time

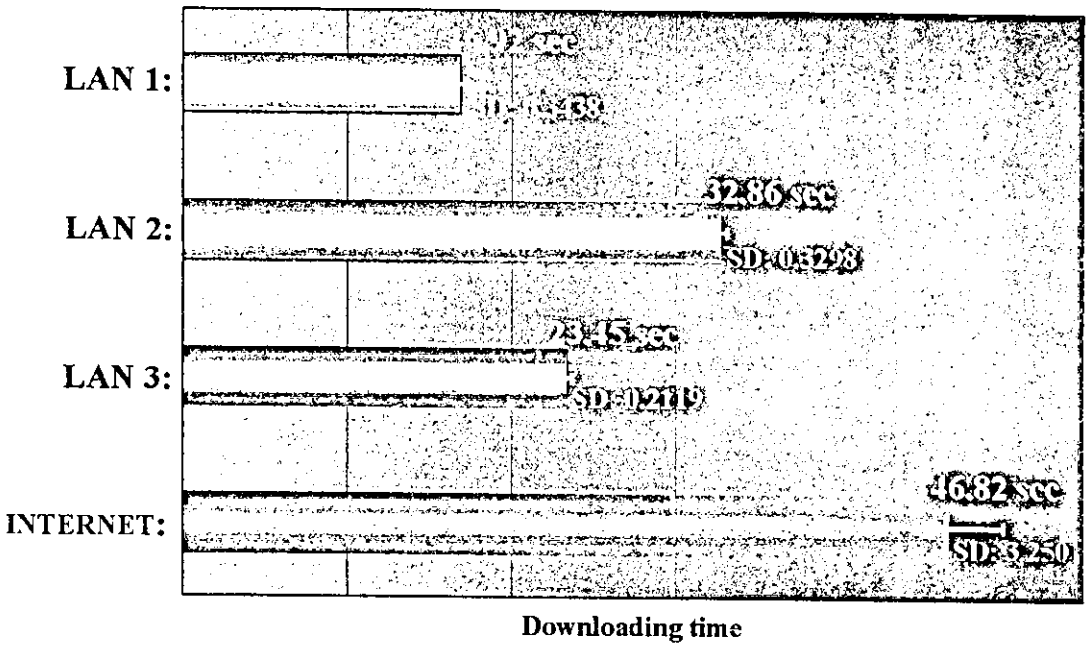

Fig.7 Total downloading time on four kinds of network configurations

電子透かし付 QR コードを用いた
セキュアなネットワーク認証システムの構築

樋口　江，橘　英伸，梅田徳男
北里大学大学院医療系研究科

Development of a Secure Network Authentication System using QR Code with Digital Watermark

Ko Higuchi, Hidenobu Tachibana, Tokuo Umeda
Kitasato University Graduate School of Medical Sciences

【はじめに】

近年の医療における IT（Information Technology）化はめざましく，院内ネットワークにおける Web ベースの医事会計システム，電子カルテシステムなどの構築が急速に進んでいる．その際，多くの場合はシステムにアクセスしてきた人物を本人として認証し，目的のアプリケーションへと導くために，ID，Password を入力させる“フォーム認証”の技術が用いられている．しかしながら，ID，Password を覚える煩雑さのため ID, Password を付箋紙に記入し Personal Computer に直接貼り付けていたり，ブラウザのキャッシュをこまめに消去しないため，ID や Password の履歴が残っていたりと，ずさんな認証管理が目立つ．それによって不正アクセスや情報の漏洩，なりすましなどの問題が増えてきている．これらの問題に対し，近年では，静脈や声紋などを用いて認証する“生体情報認証技術（バイオメトリクス）”を取り入れ，より簡便で秘匿性の高い認証技術も普及してきてはいるが，その分のコストは無視することはできない．

そこで本研究では，電子透かし技術を応用した Quick Response（以下 QR と称す）コードを用いて，簡便で秘匿性が高い，ネットワーク認証システムを構築する．また，他の Web ベースシステムとの連結を行い本システムの運用提案を行う．

【方法】

QR コードデコードライブラリ(SUNMORETEC 社製)，電子透かしデコードライブラリ(SOFTADVANCE 社製)を，Java 言語を用いて作成したプログラムに組み込み，システム（Web アプリケーション）を構築した．

【結果・考察】

本構築システムでは Client が ID，Password を入力，記憶せずにすむように QR コードにそれらの情報を変換して認証に用いた．しかしこれでは QR コードを読み取るリーダやカメラ付携帯電話があれば情報を読み取られてしまう可能性がある．そこで新たに Secret_Password（以下 S_ Password）という項目を設定し，電子透かし技術を利用した透かし情報を QR コードに付帯させた．したがって，本システムは ID，Password，S_ Password の 3 つの情報が入った QR コードを Server に Upload することで，それらの情報を読み取り，自動で認証できる新しいタイプのネットワーク認証システムとなった．S_ Password は電子透かし技術を利用しているので，QR コードからは S_ Password の存在そのものが分からない．

他の Web ベースシステムとの連結に関しては，連結しようとするシステムが認証に用いていた ID，Password の情報を本システムのデータベース（以下 DB）に追加するだけで容易に連結可能である．本システムは連結しようとするシステム（Server）に情報を橋渡しするだけなので，連結しようとする Server 環境（Operating System）に依存しない．

また，本構築システムは DB に Client の個人情報（名前，住所，身長，体重，血液型，アレルギーの有無，既往歴など）を登録，変更できるようなインターフェースも有しているので，Client が自身の健康管理を行える簡易的なチェックシートとしても運用可能である．

【結論】

本システムは認証情報入りの QR コードを Server に Upload するだけで認証が完了する．また，認証情報の一部を電子透かし技術を用いて不可視にしているので，情報の存在そのものを隠蔽できるため，秘匿性がより高まった．さらに，既存の Web ベースシステムとの連結も容易で汎用性が高い．よって本構築システムはセキュアで新しいタイプのネットワーク認証システムとなり得る．

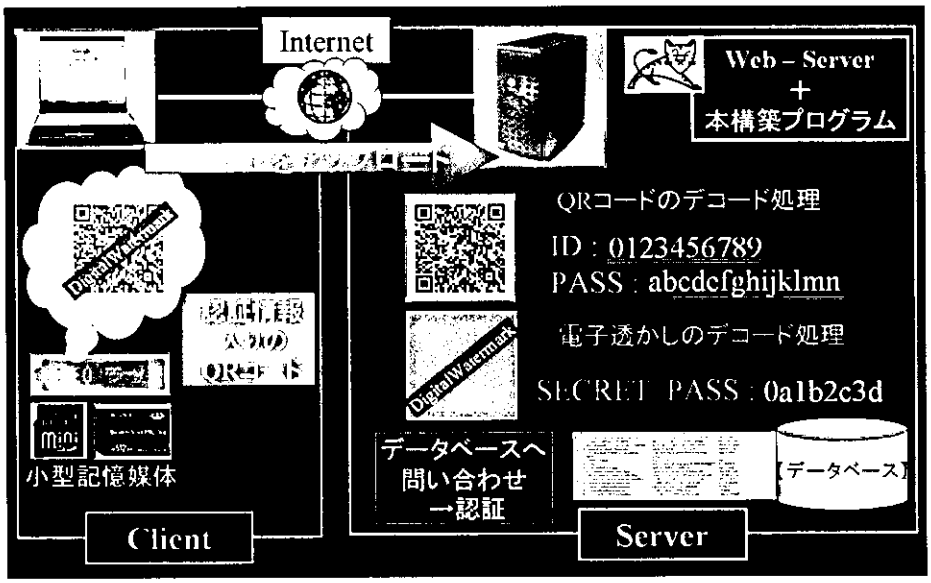

Fig.1　System configuration

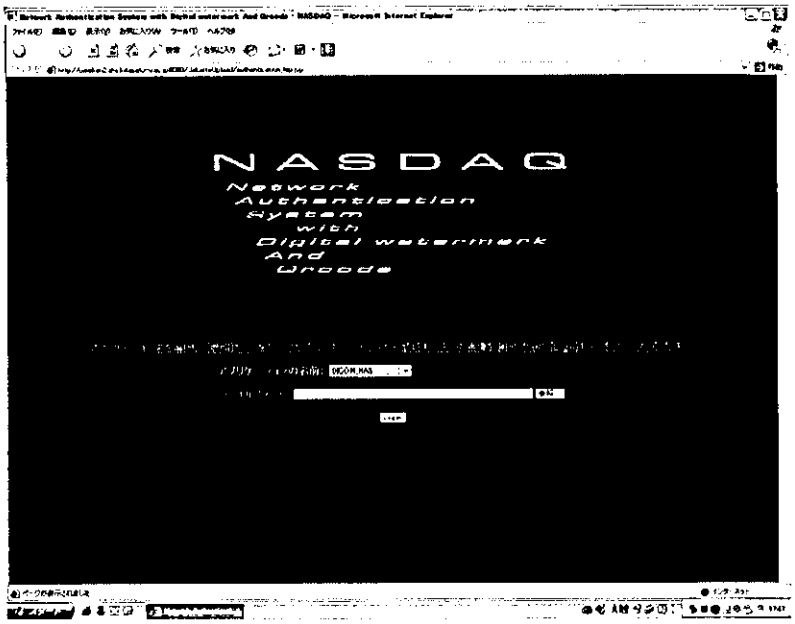

Fig.2　Front page of the system