clinical information. Among the data mining approaches, we employed machine learning approach and back propagation neural network approach.

3 Results

Towards the construction of the information infrastructure for genome medicine, we implemented some software components for PKI and HL7. Then we developed a prototype system based on the architecture that was described in the above and evaluated it.

3.1 PKI Components

3.1.1 Configuration of the root CA

The root CA was installed in The Medical Information System Developing Center (MEDIS-DC). The X.500 distinguished name (DN) for it was set to 'c=JP, o=MEDIS-DC, cn=MD-HPKI-01-MEDIS -TopCA-for-CAs-and-TSAs'. The DN is a structured data type that supports a hierarchical naming system. The most common X.500 naming attributes are 'c' (country), 'o' (organization), 'ou' (organization), and 'cn' (common name).

The primary functions of the root CA are 1) issue of the certificate signing certificate to the root CA (the root CA signing certificate), 2) issue of the certificate signing certificates to the sub CAs (the sub CA signing certificates), 3) revocation of the sub CA signing certificates, 4) distribution of the authority revocation list (ARL) that lists the revoked sub CA signing certificates, and 5) distribution of the certificate revocation list (CRL) that lists the end entity signing certificates that are revoked by each sub CA. The certificate validity period of the root CA signing certificate is set to 8 years. That of the sub CA signing certificates is also set to 8 years. Distribution of ARLs and CRLs are made via HTTP protocol. The distribution points of ARL and CRL are http://repository.medis.or.jp/crl/root.crl and http: //repository.medis.or.jp/crl/, respectively.

The system architecture of the root CA is illustrated in Figure 1. Since it shall be operated in top level secure way, the CA system that generates PKCs and ARL is installed on the private network that is isolated from either the intranet of MEDIS-DC or the Internet. The web server for distributing ARLs and CRLs is installed on the demilitarized zone (DMZ).

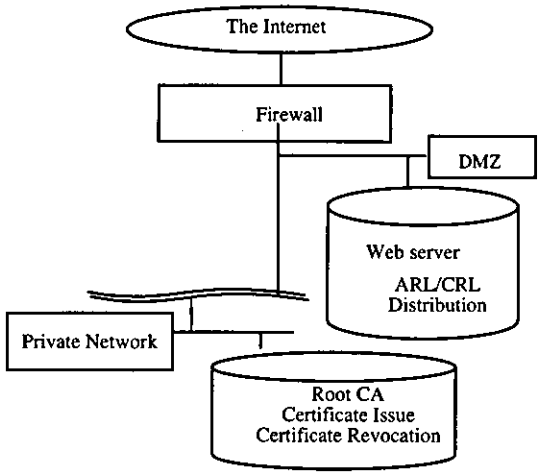


Fig. 1. The system architecture of the root CA installed in MEDIS-DC

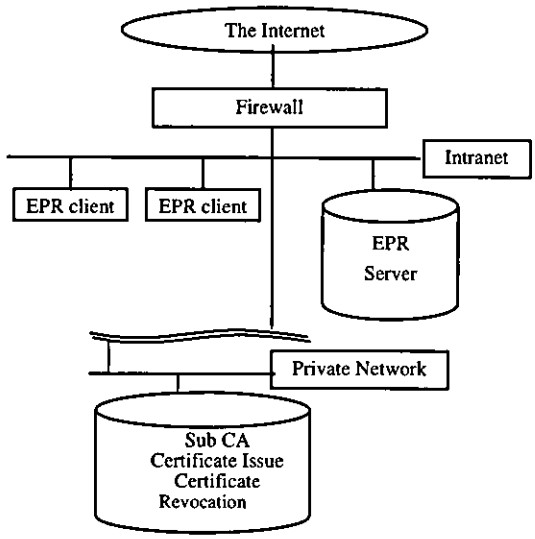


Fig. 2. The system architecture of the sub CA installed in Kobe University Hospital.

3.1.2 Configuration of the sub CA

The sub CAs were installed on the private networks in Kobe University Hospital and Kobe Translational Research Informatics Center. For example, The DN for Kobe University Hospital was set to 'c=JP, o=Kobe University Hospital, ou=Kobe University Hospital, cn=MD-HPKI-01-KUH-CA-for-non -Repudiation'. The DN of the end entities were, for example, identified by a DN like 'c=JP, o=Kobe University Hospital, ou= regulated health professional, cd=Real Name' where 'Real Name' is a doctor's real name.

The primary functions of the sub CA are 1) issue of the clinical document signing certificates to end entities (the end entity signing certificate), 2) revocation of the end entity signing certificates, 5) registration of the CRL to the CRL distribution point on the web server of the root CA. The certificate validity period of the end entity signing certificate is set to 4 years that is a half of that of the sub CA signing certificates.

The system architecture of the sub CA is illustrated in Figure 2. The CA system that generates PKCs and CRLs is installed on the private network that is isolated from either the intranet of each EPR project where EPR servers and EPR clients are running or the Internet.

3.2 HL7 Components

The clinical documents including individual genome information are composed of two components. The first component is clinical information and genome information itself. We designed the format of those information of a patient according to the Japanese Set of Identifiers for Medical Record Information Exchange (J-MIX) [14] and HL7 Version 3. The items and their XML elements are listed in Table 1. We exchanged the clinical information and the genome information as an XML document in conformity to J-MIX and HL7 HMD.

The second component of the clinical documents is a digital signature and its related information. Digital signatures are usually transferred with the signer's PKC that is used for verifying the digital signature and the CA PKCs that are necessary for building the certification path to validate the signer's PKC.

There are various choices regarding the format of the digital signatures and signed document formats. An XML signature is one of the most possible choices because we use J-MIX and HL7 Version 3 in an XML format. However, the implementation of the XML format is not straightforward. For example, it requires a lot of preprocessing of XML documents such as canonicalization. PKCS #7 is another possible choice. It is the de facto standard specification for protecting information with digital signature.

The basic PKCS #7 message format has two fields: the content type and the content. The content types defined by PKCS #7 are data, signedData, envelopedData, signedAndEnvelopedData, digestedData, and encryptedData. Since PKCS #7 is a basic building block for cryptographic applications, such as the S/MIME v2 electronic mail security protocol, there are already a lot of libraries or modules available on may platforms. Since this means the ease of implementation, we chose PKCS #7 as the signature format in this study.

A part of the XML scheme for the clinical information and genome information described in HL7 Version 3 format with a digital signature is illustrated in Table 2.

Table 1. J-MIX items that are used for the description of clinical information and genome information

Item code	XML element name	Data type
MD0010050	Patient.WholeName	String
MD0010110	Patient.Birthday	Date
MD0010120	Patient.Sex	Category
MD0010150	Patient.WholeAddress	String
MD0020180	Referral.Date	Date
MD0020220	Referring.Provider. Name	String
MD0020410	Referring.Physician. WholeName	String
MD0020480	ReferredTo.Provider. Name	String
MD0020670	ReferredTo.Physician. WholeName	String
MD0020730	ReferralNote	Text

3.3 Prototype System

We developed a prototype system by using the above components and evaluated it in Kobe University Hospital, Kyoto University Hospital, Osaka University Hospital and Kobe Translational Research Informatics Center. The system was developed using with Microsoft Internet Information Servers, Microsoft InfoPath, and Microsoft .Net C#. The overall system architecture was illustrated in Figure 3.

About 60 users participated in using the prototype system. First they applied for registration through the registration web page to the sub CA either in Kobe University Hospital or Translational Research Informatics Center depending on their affiliation. The sub CA verified the registration and issued a private key and the corresponding public key certificate stored in a USB token. The users generated pieces of translational research information that contained SNP information in some cases in an HL7 Version 3 format and signed it with the USB token. The signed documents were uploaded through the Internet by using SSL to the Translational Research Information System that was maintained in Translational Research Informatics Center.

The system was running successfully and the system architecture we proposed in this paper was evaluated to be appropriate.

Table 2. A part of XML scheme for a clinical document described in HL7 Version 3 format with a digitall signature

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <xs:schema targetNamespace="urn:hl7-org:v3"
elementFormDefault="qualified"
xmlns:fo="http://www.w3.org/1999/XSL/Format"
xmlns:msg="urn:hl7-org:v3/mif" xmlns:hl7="urn:hl7-org:v3"
xmlns:voc="urn:hl7-org:v3/voc" xmlns="urn:hl7-org:v3"
xmlns:my="http://schemas.microsoft.com/office/infopath/2003/myXSD/200
4-02-20T09:07:01" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:include schemaLocation="datatypes.xsd" />
  <xs:include schemaLocation="voc.xsd" />
  <xs:import
namespace="http://schemas.microsoft.com/office/infopath/2003/myXSD/20
04-02-20T09:07:01" schemaLocation="my.xsd" />
  <xs:element name="OutcomeResearchReport"
type="UUDD_MT990100.OutcomeResearchReport" />
- <xs:group name="UUDD_MT990100">
- <xs:sequence>
  <xs:element name="OutcomeResearchReport"
type="UUDD_MT990100.OutcomeResearchReport" />
  </xs:sequence>
  </xs:group>
- <xs:complexType name="UUDD_MT990100.OutcomeResearchReport">
- <xs:sequence>
  <xs:element name="id" type="II" />
  <xs:element name="recordTarget" type="UUDD_MT990100.RecordTarget" />
  <xs:element name="component" type="UUDD_MT990100.Component"
minOccurs="0" maxOccurs="unbounded" />
  <xs:element name="signature" type="my:SignatureType" />
  </xs:sequence>
  <xs:attribute name="classCode" type="ActClass" />
  <xs:attribute name="moodCode" type="ActMood" />
  </xs:complexType>
- <xs:complexType name="UUDD_MT990100.RecordTarget">
- <xs:sequence>
  <xs:element name="patient" type="UUDD_MT990100.Patient" />
  </xs:sequence>
  <xs:attribute name="typeCode" type="ParticipationType" />
  </xs:complexType>
```

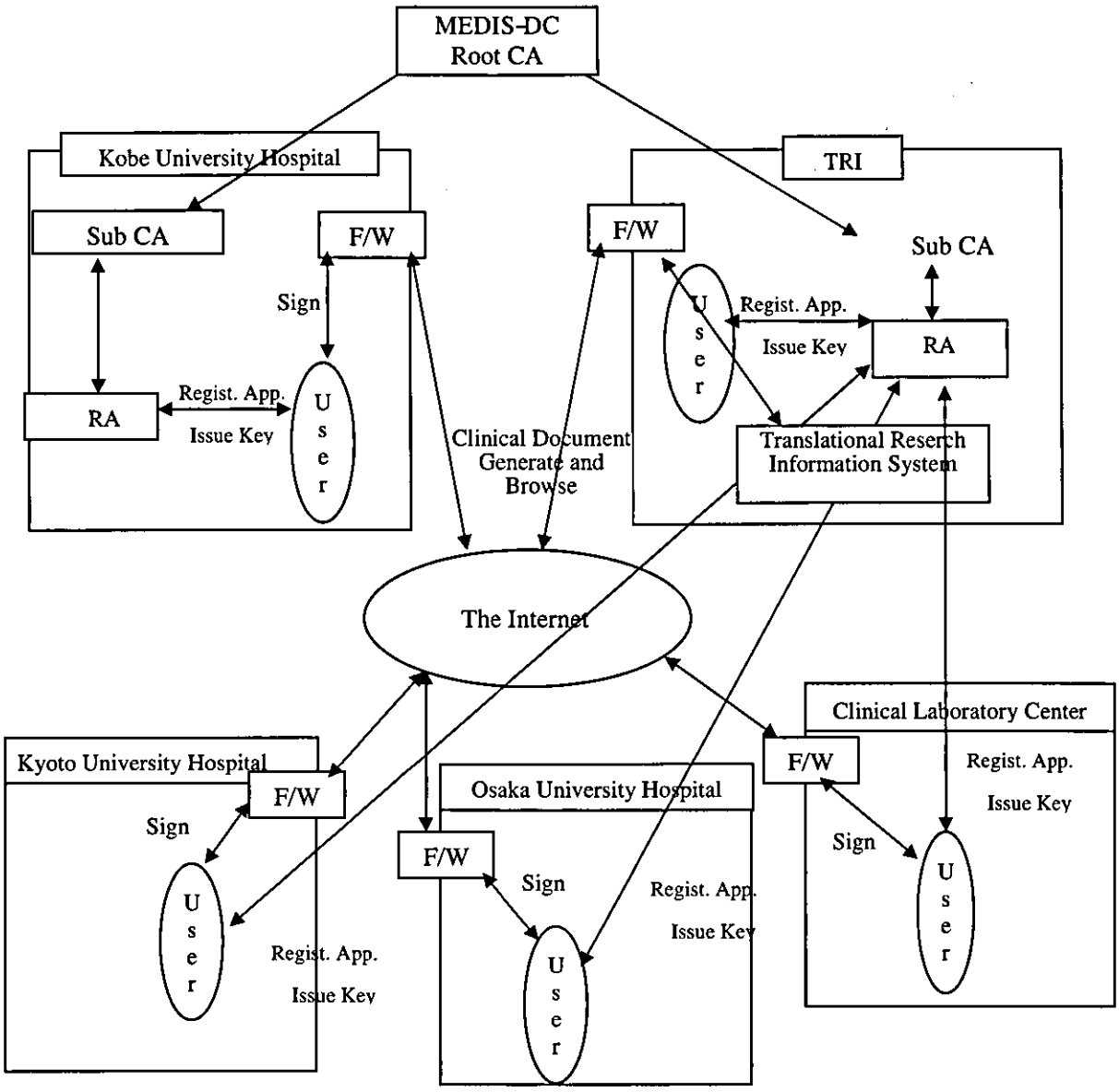


Fig. 3. The overall system architecture of the prototype system. The users in Kobe University Hospital posses the PKC that was issued by the sub CA installed in Kobe University Hospital while the other users possess the PKC that was issued by the sub CA installed in TRI.

4 Discussion

During the evaluation process of the prototype system, we had no technical problems and the system was running without any troubles. The most difficult part of the process was in the steps of registration of users and issuing their public key certificates because these steps required a lot of collaboration of the users who didn't know much about PKI. We needed to ask them to bring forward their resident's card for

the personal identification and their medical license for conformation of their qualification, This procedure put a burden on the users and it took about seven day for half of them to get a complete set of the papers. In order to make these steps much speedier and easier, social infrastructure for digital application should be developed. Especially, the development of nation wide PKI that is specific for the healthcare field and assert healthcare professionals is a pressing issue.

The cost of issuing the public key certificate is another serious problem. One PKC stored in a USB token cost about 24,000 yen or 220 USD. It is obviously higher compared to current seals and handwritten signature. .Though this problem about the cost is the one that is expected to be solved as PKI becomes popular and the number of the PKC in use increases, it is another pressing issue.

We succeeded in the development of the comprehensive information models for clinical information and genome information on a basis of HL7 Version 3. However, the more comprehensive the information models are getting, the more complicated the implementations becomes. In the development of the prototype system, the implementation of the clinical document of HL7 Version 7 XML format took the longest time (man month) in the whole implementation processes. A development of a set of software tools that supports the HL7 Version 3 is an urgent business for the construction of the information infrastructure for genome medicine.

We pointed out the importance of the intelligent analyzers that provide a lot of statistical functions for the information infrastructure for genome medicine and its essential components. However, its implementations are still in progress and were not included in the prototype system. In order to make the prototype system much more practical, we need to work hard for its implementations.

5 Conclusion

The Internet is providing the powerful foundation for the construction of the information infrastructure for genome medicine because the Internet is now stable, trustworthy and fast. The Public Key Infrastructure is adding another good feature, namely security, to the Internet. PKI is expected to be more popular through the Internet society in the near future, which will provide more sound foundation for the construction of the information infrastructure for genome medicine.

Though PKI is one of the key technologies that is critical for all of those who want to use the Internet in safety, other methods that are specific for the development of genome medicine should be devised by the research community of clinical genome informatics. Among those methods, comprehensive information models and intelligent analyzers are most essential. In this paper, we proposed an implementation of the information models based on the HL7 Version 3 and demonstrated the integrated architecture of the models and the PKI. The architecture was evaluated to work well and we consider that the architecture gives the basis for the construction of the information framework for genome medicine.

Acknowledgment

This work was partially supported by the research fund of the Japanese Ministry of Health, Labor, and Welfare. We thank Dr. Gou Masuda for his great support for HL7 Version 3 Modeling and Implementation.

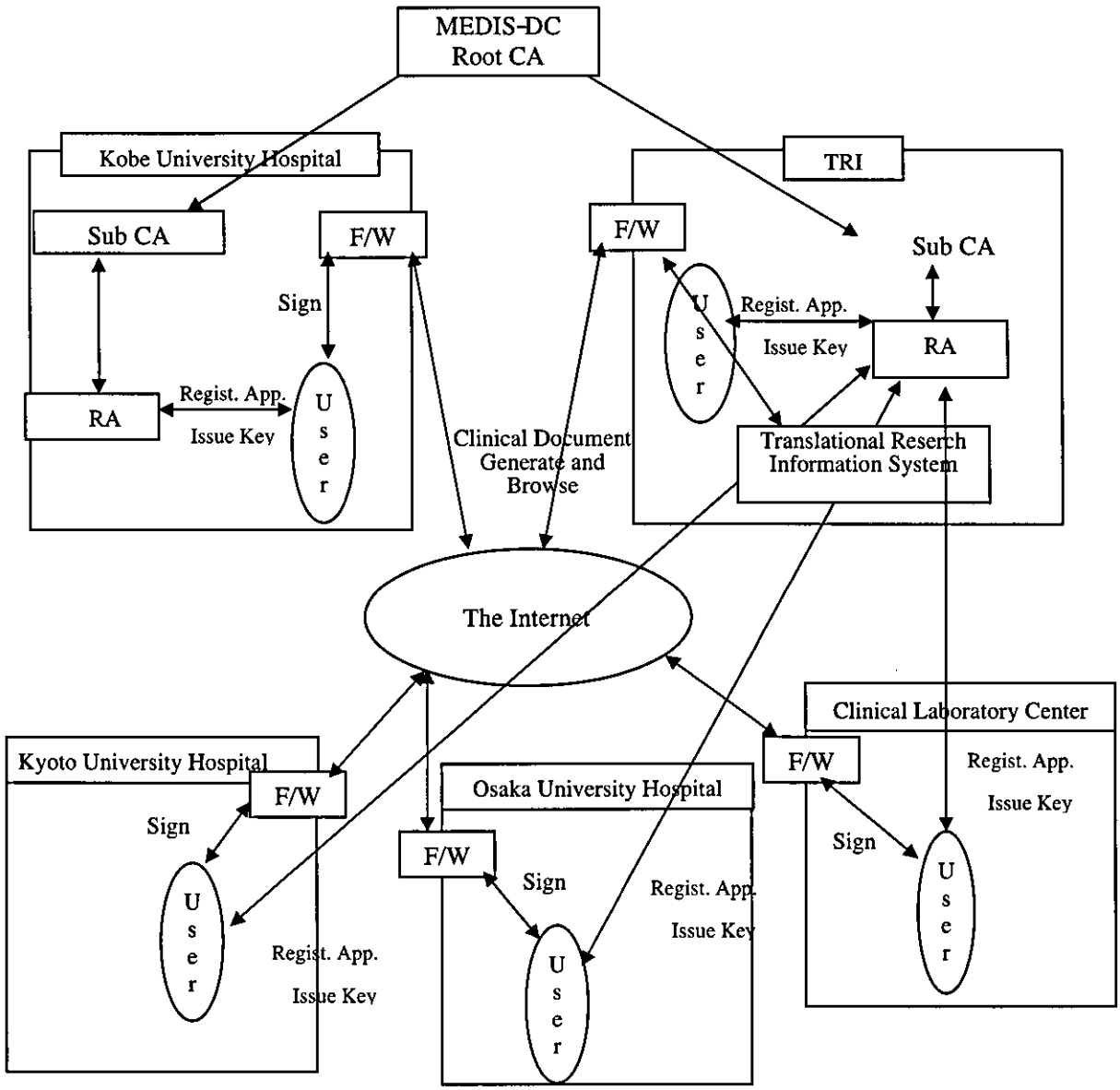
References

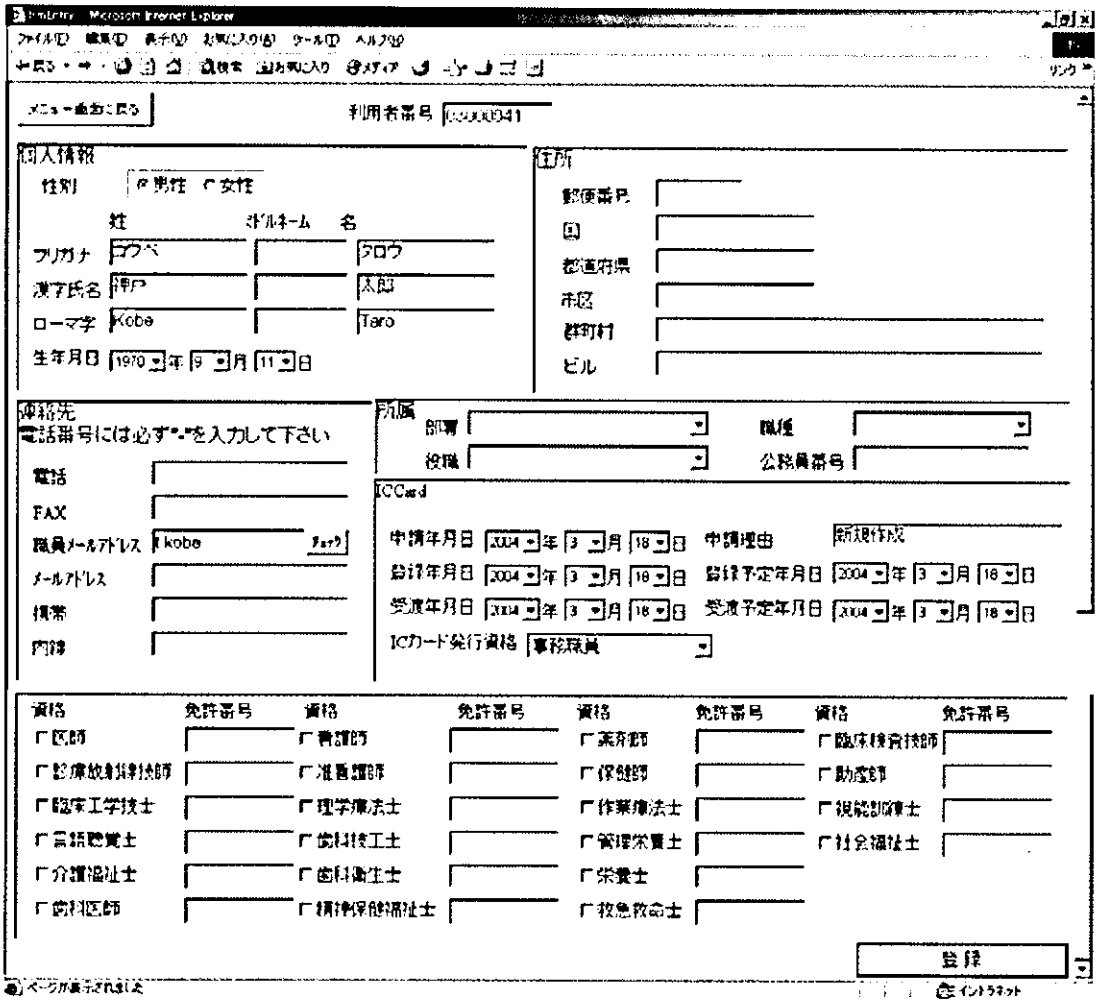
1. Nawata, H., et. al: Genome-wide linkage analysis of type 2 diabetes mellitus reconfirms the susceptibility locus on 11p13–p12 in Japanese. Journal of Human Genetics, Online First (http://springerlink.metapress.com/app/home/contribution.asp?wasp=e05d2179wm4jnnba1gdh&referrer=parent&backto=issue,3,11;journal,1,63;browsepublicationsresults,281,533) (2004)
2. Parsaye, K., Chignell, M.: Intelligent Database Tools & Applications: Hyperinformation Access, Data Quality, Visualization, Automatic Discovery. New York: John Wiley & Sons, Inc. (1993)
3. Parsaye, K., Chingnell, M.H., Khoshafian, S., Wong, H.K.T.: Intelligent Databases: Object-Oriented, Deductive Hypermedia Technologies. New York: John Wiley & Sons (1989)
4. Takeda, H., Matsumura, Y., Kuwata, S., Nakano, H., Yamamoto, R., Sakamoto, N.: Architecture for networked electronic patient record system. International Journal of Medical Informatics Vol. 60, No.2 (1999) 161-167
5. Blobel, B.: Advanced tool kits for EPR security. International Journal of Medical Informatics Vol.60, No.2, (1999) 169-175.
6. Park, Y.M., Lee, K.H., Jeong, C.K., Choi, J.W., Cho, H.I., Min, B.G.: A Method to Implementing the Extended Order Communication System Using the Public Key Infrastructure (PKI) through the Patient Certification System (PCS), Proceedings of The Second-China-Japan-Korea Joint Symposium on Medical Informatics (CJKMI '2001 Tokyo, Japan, 2001)
7. Sakamoto, N.: The Construction of a Public Key Infrastructure for Healthcare Information Networks in Japan. MEDINFO 2001, V.Patel et al. (Eds), Amsterdam IOS Press, © 2001 IMIA (2001) 1276-1280
8. Housley, R., Ford, W., Polk, W., Solo, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999 (1999)
9. Hinchley, A.: Understanding Version 3: A primer on the HL7 Version 3 Communication Standard. Munich, Germany: Alexander Moench Publishing (2003)
10. Jones, T.: NPfIT interoperability - the role of HL7 version 3. HL7 UK 2003, 2003. Available at http://www.hl7.org.uk/HL7UKConferenceSite/HL7UK2003Papers.htm. Accessed Dec 12, 2004 (2003)
11. The NeCST Progress Report. 2003. Available at http://secure.cihi.ca/cihiweb/en/downloads/infostand_eclaims_prog2003_e.pdf. Accessed Dec 12, 2004. (2003)

12. de Jong, T.: Medication Supply Registry Project and Demonstration in the Netherlands. HL7 UK 2003, 2003. Available at http://www.hl7.org.uk/HL7UKConferenceSite/HL7UK2003Papers.htm. Accessed Dec 12, 2004. (2003)

13. William, B.L., Trigg, B.K.: Information System Architectures for Syndromic Surveillance. Morbidity and Mortality Weekly Report. 2004; 53(Suppl) (2004) 203-208

14. The Medical Information System Development Center: The Japanese Set of Identifiers for Medical Record Information Exchange (J-MIX) (in Japanese) http;//www.medis.or.jp/ Accessed Dec 12, 2004 (2000)


MEDIS-DC
Root CA
Kobe University Hospital
Sub CA
F/W
Sign
RA
Regist. App.
Issue Key
User
TRI
F/W
Sub CA
User
Regist. App.
Issue Key
RA
Translational Reserch
Information System
Clinical Document
Generate and
Browse
The Internet
Kyoto University Hospital
F/W
Sign
User
Regist. App.
Issue Key
Osaka University Hospital
F/W
Sign
User
Regist. App.
Issue Key
Clinical Laboratory Center
F/W
Regist. App.
Issue Key
Sign
User


メニュー画面に戻る
利用者番号
個人情報
性別
男性
女性
姓
ミドルネーム
名
フリガナ
漢字氏名
ローマ字
Kobe
Taro
生年月日
1970
年
9
月
11
日
住所
郵便番号
都道府県
市区
郡町村
ビル
連絡先
電話番号には必ず"-"を入力して下さい
電話
FAX
職員メールアドレス
kobe
チェック
メールアドレス
携帯
内線
所属
部署
職種
役職
公務員番号
ICCard
申請年月日
2004
年
3
月
18
日
申請理由
新規作成
登録年月日
登録予定年月日
受渡年月日
受渡予定年月日
ICカード発行資格
事務職員
資格
免許番号
医師
歯科医師
薬剤師
准看護師
理学療法士
歯科技工士
歯科衛生士
精神保健福祉士
看護師
保健師
作業療法士
管理栄養士
栄養士
救急救命士
臨床検査技師
助産師
視能訓練士
社会福祉士
介護福祉士
臨床工学技士
言語聴覚士
診療放射線技師
登録
ページが表示されました
インターネット

厚生労働科学研究費補助金
医療技術評価総合研究事業

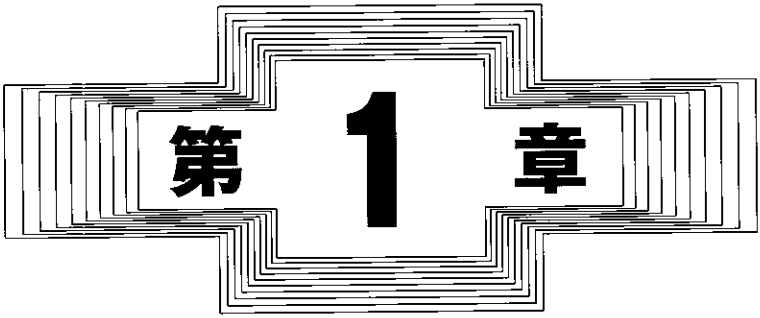
電子カルテの相互運用に向けたHL7メッセージの開発および管理・流通手法に関する研究

(H14－医療－004)

平成15年度　成果資料

主任研究者　坂本　憲広
神戸大学医学部附属病院医療情報部

CONTENT



はじめに

■

Introduction

1.3　本書は何を扱っていないか

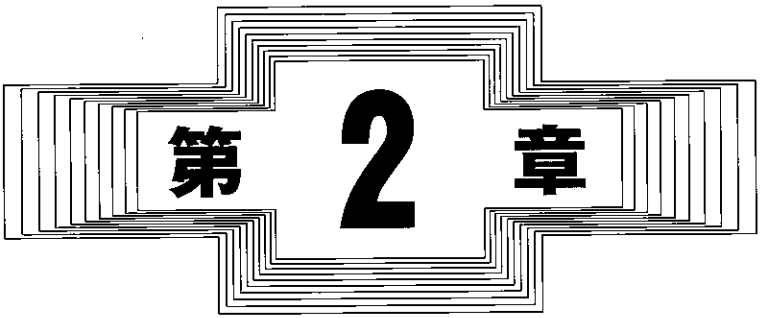
本書は現行のHL7 V3方法論について，完全な解説文書を提供することは目的としていません。HL7協会は方法論に関する最も包括的な文書である“Version 3 User Guide”を公表しており，www.hl7.orgから入手可能です。

本書は主要な概念と主要な用語の大部分を紹介していますが，完全な方法論を理解するには上記のユーザーガイドが必要となるでしょう。

1.4　本書の利用の仕方

本書は，方法論の主要な部分それぞれについて，章を分けて解説しています。さらに，巻末の用語集は，本書で紹介した用語の定義を提供しています。

本書は順を追って通して読むように構成されており，用語はそれ以前の章で紹介した後に限って，使用するようにしています。



背景

Background

2.3 HL7 V2の成功

1980年代後半に誕生して以来，HL7 V2は米国を始め，国際的に広く使用され続けています。特に，病院の中での通信に使用され，多くのベンダーからなるシステムのシステム間通信に成功を収めています。

2.4 HL7 V3の必要性

HL7 V2は成功を収めましたが，HL7は，真に相互運用可能なシステムを支援するためには，より強力な方法論が必要であると数年前に気づきました。さらに，さまざまな施設や，各国から寄せられる多岐にわたる詳細な要求事項の結果，HL7 V2標準化規格に膨大な数の選択項目ができ，実装を扱いにくくしてしまいました。そこで，HL7は以下の特徴を有する新しいバージョンの標準化規格を開発することを決定しました。

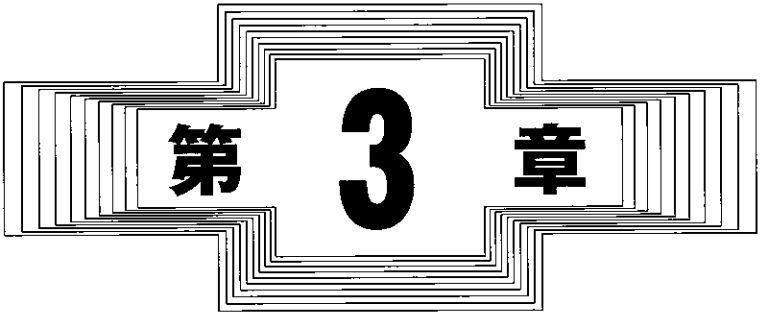
- システムの相互運用性の動向を反映していること。
- 選択性（optionality）をできる限り排除すること。
- 当初から国際的な要求事項を含んでいること
- プラグ･アンド･プレイにできる限り近づけること。

これらの結果こそが，HL7 V3なのです。

2.5 HL7 V3の優位点

V2と比較したV3の主な優位点は，以下のとおりです。

- 実装の再利用性
- 世界規模の相互利用可能性
- プラグ･アンド･プレイへの移行
- 最新のシステム開発技術との互換性
- 実装コストの削減



V3方法論の主要概念

The Key Concepts of the V3 Methodology

- アプリケーションロール（Application Role）：メッセージの送信システムと受信システムの責務を定義します。
- トリガイベント（Trigger Event）：何がメッセージの送信を引き起こすかを定義します。
- ストーリーボード（Storyboard）：システム利用者（すなわち，人間）の視点から見て，何が起こるかを定義します。

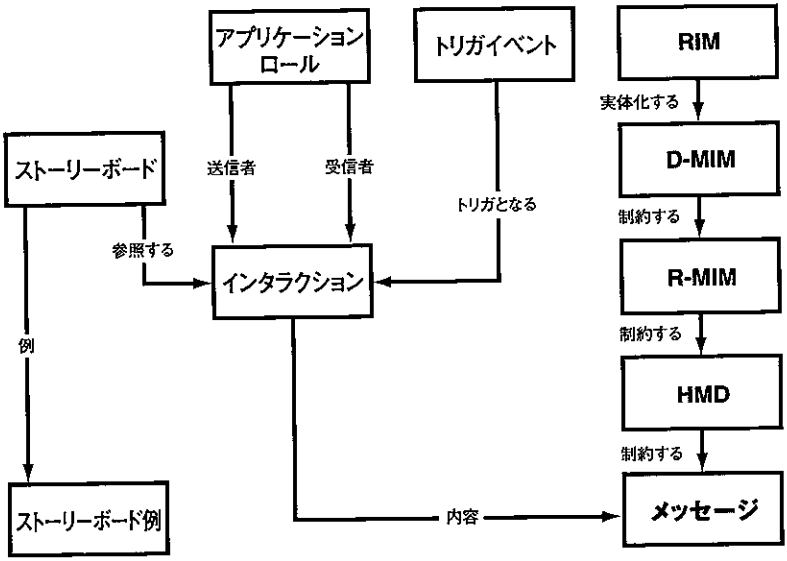


図1　HL7 V3メッセージの開発過程