図2-20 XMLファイルを受信後メール通知するための情報を設定するファイル(DTD)

●DTDファイル

```
<!DOCTYPE MailTemplate[
        <!ELEMENT MailTemplate (SMTPHost, To ,From ,Subject , Body)>
        <!ELEMENT SMTPHost   (#PCDATA)>
        <!ELEMENT To                    (#PCDATA)>
        <!ELEMENT From                  (#PCDATA)>
        <!ELEMENT Subject               (#PCDATA)>
        <!ELEMENT Body                  (#PCDATA)>
]>
```

●DTDファイルの例

```
        <?xml version="1.0" ?>
        <MailTemplate>
                <SMTPHost>smtp.xxxxx.co.jp</SMTPHost>
                <To>recipient@xxxxx.co.jp</To>
                <From>protmet@xxxxx.co.jp</From>
                <Subject>診療情報を受信</Subject>
                <Body><![CDATA[
診療情報を受信しました
タイトル=${SUBJECT}
種別=${FUNCTION}
確認してください
]]>     </Body>
        </MailTemplate>
```

表2-12 XMLファイルを受信後メール通知するための情報を設定するファイル(DTD)

項番	タグ名	説　明
1	SMTPHost	SMTPメールサーバーのアドレス(FDQN)を指定する
2	To	レポートの宛先メールアドレス
3	From	レポートの差出人メールアドレス
4	Subject	メールタイトル
5	Body	メール本文 ${SUBJECT}はxmlファイルの「タイトル」に置換される ${FUNCTION}は追加時は「新規」、変更時は「変更」の文字列に置換される

参考文献

［1］ 工藤 道治. 情報セキュリティ技術最前線"暗号とアクセス制御".
http://www-06.ibm.com/jp/developerworks/evangelist/events/pdf/ed050120-02.pdf
［2］ 林 隆志. セキュリティポリシーの策定・実施・改善に関する社会工学的研究.
http://research.nii.ac.jp/kaken-johogaku/reports/H17_A06/A06-15.pdf
［3］ 丸山 宏, XMLとWebサービスのセキュリティ—XMLデジタル署名と暗号化. 1st ed. 東京: 共立出版; 2004.

第3章

Webサービスを利用したXMLセキュリティシステムの実用化研究

本多正幸・中山良幸・梁瀬和夫

第3章　Webサービスを利用したXMLセキュリティシステムの実用化研究

主任研究者　本多　正幸
（長崎大学大学院・医歯薬学総合研究科医療情報学講座　教授）
分担研究者　中山良幸
（株式会社日立製作所・公共システム事業部　主任技師）
分担研究者　梁瀬和夫
（ケービーソフトウエア株式会社　代表取締役社長）

研究要旨

前年度に引き続き XML 文書の部分暗号化技術を利用し診療情報提供書をやり取りする医療機関間暗号化 XML 文書送受信システムを構築した。IPsec や SSL/TSL では実現が困難なエンドツーエンドのセキュアな送受信システムを部分暗号化 XML セキュリティで実装し、Web サービスによる職位によるエレメント暗号化、診療科によるアクセス制御機能の動作確認及び医療機関をフィールドにした実証試験を実施した。その結果、本システムの有効性を確認しするとともに、今後は、診療情報提供書入力インターフェースのブラウザ化、パッシブ・モードでの FTP 通信機能の追加等の改良が必要になることに言及した。

A. 研究目的

コンピュータ・システムは非常に広い領域で攻撃者から守られる必要がある。「エンドツーエンド・セキュリティ」という言葉を広い意味で使用する場合は、これらの前線が「端から端まで守れている」ことを指す。この広義の意味での「エンドツーエンド・セキュリティ」の観点からは、XMLのデジタル署名や暗号化は、これらの前線のごく一部の守りであることに注意する必要がある。すなわち XML 暗号化はシステム全体のセキュリティの重要であるがひとつの要素に過ぎない。

一方、コンピュータ・システム全体のセキュリティでなく、通信のセキュリティだけを考える「エンドツーエンド」の考え方があることは前章で述べた。この狭義の「エンドツーエンド」は、通信において情報の発信者から情報の受信者までの間に、情報が適切に守られていることを指す。通信における情報セキュリティの用件は主に次の4点に集約される。

（1）秘匿性（Confidentiality）：情報が発信者から受信者に渡るまでに他人に盗まれない

（2）完全性（Integrity）：情報が途中で改ざんされない。

（3）認証（Authentication）：発信者・受信者が確かに本人であり、他人が装っているのではない

（4）否認不能性（Non-repudiation）：発信者が情報の発信の事実を否定できない。

発信者と受信者の間にいかなる攻撃者を

仮定しても、これらの用件が成立するとき、その通信はエイドーツーエンドのセキュリティを持つという（ポリシーによっては、これらの要件のすべてが成立しなくともよい。例えば、SSL/TLS の場合は否認不能性は成立しないし、認証も通信の一方だけの認証が行われるのは普通である。

インターネットの通信モデルは

1．ホスト間の通信：IP アドレスによる IP データグラムの配信（ネットワーク層）

2．アプリケーション間の通信：IP アドレス＋ポート暗号による TCP/IP あるいは UDP/IP による通信（トランスポート層）

という２つの相から構成される。即ち、IP アドレスがわかっていれば、世界中のどのホストとも直接通信できる。あるいは IP アドレスとポート番号が判明すれば、どのホストの上で動いているアプリケーションとも直接通信できる。

このモデルに対応して、ネットワーク層でのセキュリティの標準として IPSec、トランスポート層のセキュリティとして SSL がある。これらはどちらも、それぞれの通信モデルに関してエンドツーエンドである。即ち、IPSec は、ホスト間のセキュアな IP データグラムの配信を可能にする。相手に直接 IP データグラムを送ることができる（IP-Reachable であるという）限り、間にどんな通信路があろうと、データの秘匿性、完全性が保たれ、相手の認証が正しく行える。通信は発信側のホストで暗号化され、受信側のホストで復号されるので、経路中はデータは適切に保護される。従って、IPSec は IP 接続が可能ホスト間でのエンドツーエンド・セキュリティを提供する。

しかしながら IP データグラムによってホストに配達されたデータは、多くの場合、特定のアプリケーションに配達されるため、IPSec は認証されたホストまでの送達を保護するが、ホストにデータが到着してから目的のアプリケーションに配達する部分は保護しない。従って、ホストに複数のアプリケーションがあり、それぞれのアプリケーションに対するセキュリティ上の信頼関係が異なる場合には IPSec はエンドツーエンドのセキュリティを提供しない。なぜならデータはホストについてから、間違ったアプリケーションに送達されるかも知れないし、アプリケーションに配達さえる前にコピーや改ざんの可能性もある。これに対して SSL/TLS は、トランスポート層のセキュリティ・プロトコルなので、アプリケーション間にエンドツーエンドの保護を提供する。

インターネットにおける医療機関間の通信は急速に発展している。これらの通信において特徴的なのは、１つの診療情報トランザクション（本研究の場合、診療情報提供書の送受信）が 2 者間で終ることはまずない、ということである。診療情報のやり取りについては医師が、患者基本情報や診療情報、保険情報については医事課職員が、検査結果については検査室職員が通信を行わなければならない。このように診療情報トランザクションの中には、各種のデータが含まれており、それぞれの特定の組合せでエンドツーエンドの保護が必要になる。例えば、診療情報提供書による患者紹介・逆紹介における紹介元医師は診療内容を照会先医師以外に開示する必要がない。一方、医事課職員は保険証番号のみ必要になるかも知れない。しかしながら医療情報トラン

ザクション全体としては、１つのトランザクションであり、１つの診療情報が複数の参加者の間でやり取りされることになる。従って、診療情報の中に選択的な保護が必要になってくる。

さらに診療情報のトランザクションは、後の監査のために保存されなければならない。仮にあるトランザクションに関して疑義が発生した場合には、トランザクションに参加したメンバはそれぞれのログを証拠として参照する。これらのログが、適切に保護されていなければ、改ざんされてしまった可能性があるので証拠性が薄くなるかも知れない。2000 年に可決された電子署名法ではある一定の条件を満たすデジタル署名に、署名・捺印と同様の商法上の効力を認めている。同時にこれらのログには機密性のある情報が含まれるので必要に応じて暗号化するなどの保護策が必要になる。

このように永続的なデータに関する保護も要求されているが、残念ながら IPSec や SSL/TLS などの通信プロトコルでは、データは通信路上だけで保護されていて、一度データが受け取り手に届いてしまうと保護は解除されてしまう。永続的なデータに関して言えば、情報の発信者と受信者が時間軸上で離れた２点間にいると考えることができ、この２点間でエンドツーエンドの保護が必要とされているのである。単なるプロトコルのフォーマットとしてだけでなく、永続性のある文書やデータのフォーマットである必要がある。このような時間軸上での保護を可能にする技術としてＸＭＬセキュリティ、しかも部分的に暗号化する技術はきわめて有効であろうと考えられる。

本章では前年度に引き続き診療情報提供書（XML 文書）をやり取りする医療機関間暗号化 XML 文書情報連携システムを試作し、職位によるエレメント暗号化、診療科によるアクセス制御機能の動作確認及び医療機関をフィールドにした実証試験を実施し、本システムの有効性を確認した。

B. 研究方法

B-1.研究環境

本研究に用いたシステムの概要を図 3-１に示した。またシステムにおけるコンピュータ環境を以下に記載した。

【Client】

①OS：Microsoft Windows XP Service Pack2

②ハードウェア：HITACHI FLORA310DA8 クラス

③メモリ容量：256MB

【Server】

①OS：Microsoft Windows 2003 Server

②ハードウェア：HITACHI HA8000/110GE クラス

③メモリ容量：2GB

④DBMS：SQL server 2005 express

また、XML ドキュメントの取り扱いには XML 統合開発環境である Altova XML Suite 2004 Enterprise Edition(Altova 社製)を使用した。

C. 研究結果及び考察

C-1.医療情報連携システムのシステムテスト概要

これまでの調査結果、検討結果を踏まえて医療情報連携システムに求められるシステムテスト必要事項の全体概要を表 3-1 に整理した。医療機関間送受信の対象となる診療情報提供書は XML 形式でテストに供試した（図 3-2、3)。もちろん、CSV 形式でもバイナリ形式のいずれでもよい。

所定のエレメントを暗号化した診療情報提供書は Web サービスまたは FTP プロトコルを利用してデータセンタ、若しくは医療情報交換先の医療機関へ送受信される。

システムテストで利用する診療情報提供書の送受信シナリオを図 3-4 に示した。

C-2.暗号化 XML 文書の送受信機能評価

（1）基本機能

基本機能としてはシステム上に用意した診療情報提供書表示画面で、紹介目的、経過、患者の症状などを記入・暗号化することが出来る。また、将来的には診療情報提供書を作成するときに再度入力する必要を無くすため、患者情報は電子カルテ等のデータベースから引き出すことが出来るようにする予定である。

（2）診療情報提供書送付機能

本機能は、患者紹介を行う際使用する機能であり、提供先地域医療機関コード、患者の症状をテキストデータで入力できる機能を有し、そのデータを地域医療連携データセンタに送付する機能である。診療情報提供書を送付するには、診療情報提供書作成画面からホスト一覧画面に遷移し、目的のホスト(FTP サイト、Web サービス)を選択・接続し、保存ボタンを押下することで実施する（図 3-5)。この時点で、XML 形式で作成した暗号化診療情報提供書をデータセンタに送受信することができる。

また当該システムは診療情報提供書が紹介先医療機関に到着するとメールで案内する機能を有している。到着案内メールの例を図 3-6 に示した。

C-2.XML ドキュメント（診療情報提供書）の暗号化・復号化手順

前章で設計・開発した診療情報提供書送受信システムは XML ドキュメントを読み込み、特定の要素全体（ルート要素も指定可）または要素内容を暗号化し、結果を別の XML ドキュメントとして生成する。また、暗号化された XML ドキュメントの復号化も行うプログラムのプロトタイプである。

ユーザ ID、パスワードを入力しシステムにログインすると、top 画面が出現する。通常、XML ドキュメントは表示されていないが、上部プルダウンメニューからドキュメントを選択し、上部ペインにある「表示」をクリックすると診療情報提供書が現れる。上部プルダウンメニューから「XML 表示」をクリックすると XML ドキュメントとして表示され、「暗号化」をクリックすると表示項目左部にあるチェックボックスにチェックを入れた情報が「●」印で暗号化される（図 3-7(1)、(2))。

C-3.暗号化 XML 文書の完全性評価

一般に情報の完全性とは、「情報及び処理方法が、正確であること及び完全であるこ

とを保証すること」である。言い換えれば、情報の改ざんや間違いから保護することを指すが、ここでは構築システムにおける診療情報提供書の送受信機能を評価するために用語として用いている。

本章では送受信・暗号化前の診療情報提供書の内容と送受信・復号化後のそれをテキストレベルでチェック可能なプログラムを開発した。この差分チェックプログラムにより、送受信前後の診療情報提供書内容に変化が無いことを確認している(図 3-8)。

C-4.暗号化 XML 文書の送受信におけるレスポンス・スループット評価

筆者らは前年度 XML スキーマにおける暗号化エレメント数を変化させ、処理時間に与える影響を評価した。同時に CPU 負荷(%)、メモリ使用状況(MB)を計測し、ハードウェアとの関連性も検討し、Triple-DES は共通鍵であるにも関わらず、処理時間が公開鍵以上に必要になることが確認するとともにセキュリティの面を考慮しても公開鍵の利用が望ましいことを報告している。また鍵長と暗号化・復号化処理時間の関係についても検討し、システム化する上で指摘鍵長が存在することも言及している。

今回、前章にて設計・開発したシステムを用いて HTTP、FTP プロトコル各々の場合における暗号化項目数とレスポンス時間の関係を検討した。暗号化を施す項目数は全て平文の場合 (A)、名前、生年月日、住所等の患者基本情報のみの場合 (B)、全項目を暗号化した場合(C)に分けて検討した。このときレスポンス時間とは upload の場合は紹介先医療機関のサーバに送受信するまでの時間、download の場合は紹介先医療機関の医師または事務員（地域連携室職員または医事課職員）が診療情報提供書を参照するまでの時間を表している。また同様の条件下にて診療情報提供書を繰り返し送受信させて負荷をかけた場合のレスポンス時間に与える影響も検討している。

その結果、診療情報提供書の upload に与える暗号化の影響については、HTTP プロトコルは暗号化項目数によらず平均してレスポンス時間が FTP プロトコルに比較して短い傾向にあるが、FTP プロトコルに比較して暗号化項目数の影響を受け易いことが解る（表 3-2、図 3-9)。一方、download 時は HTTP、FTP プロトコルともに暗号化項目数の影響に差はないことが解る。しかしながら upload 時に比較して HTTP プロトコルは FTP プロトコルに比較してレスポンス時間を要することが判明した(表 3-3、図 3-10)。従って診療情報提供書の送受信時にＷｅｂサービス（HTTP プロトコル）を利用する際には、可能な限り暗号化項目数を絞り込む必要がある。

診療情報提供書の upload を繰り返し実施し、レスポンス時間に与える影響を検討した。その結果、FTP プロトコルの場合は患者基本情報のみであれば、暗号化なしの場合とほとんど変わらないレスポンス時間を示すことが解る(表 3-4、図 3-11)。HTTP プロトコルの場合は、患者基本情報のみの暗号化でもレスポンス時間に影響が出ることが解る(表 3-5、図 3-12)。一方、download の場合、FTP プロトコルは暗号化の影響が実施した試験条件の範囲では認められなかったのに対して（表 3-6、図 3-13)、HTTP プロトコルは upload の場合と同様に暗号

化の影響が顕著であった(表3-7、図3-14)。従って、レスポンス時間の観点からはHTTPプロトコルに比較してFTPプロトコルの方が高効率であることが判明した。

医療機関や企業では内部 LAN とインターネットとの間にファイアウォールを設置するのが一般的である。ファイアウォールでは TCP/IP のヘッダをチェックして、LAN からインターネットへの通信は通過させるものの、インターネッからLANへの通信は予め設定したもの意外は拒否するのが通常である。当該システムではこの問題に対応するために今後は制御コネクションと同様にデータ・コネクションもFTPクライアントから FTP サーバに解説を要求する「パッシブ・モード」の実装も必要であろうと考えられる。

診療情報提供書の入力項目を全て暗号化して送受信テストを実施した際のシステム・リソースの変化の例を図3-15～18に示した。これらの結果から繰り返しupload操作して負荷をかけた場合に FTP プロトコルはメモリ使用量が増加する傾向があった。一方、download時は反対にHTTPプロトコルを使用した場合にメモリ使用量を始めとするシステム・リソースが増加した。従ってプロトコルの使い分けも考慮した運用及び運用設計も今後、必要になるものと推測している。参考までに表3-8にシステム・リソースのボトルネック判断基準を示した。

C-5. 地域医療とセキュリティの確保

質の高い地域医療を提供するために、医療の機能分化に伴って地域における情報の共有が必要となっている。われわれはそれを支援する手段としての地域医療用ネットワークシステムを長崎県下の病院で開発してきた。このようなシステムにおいてセキュリティの確保は最重要課題の1つである。

インターネットを利用して地域医療情報システムを構築する場合には、セキュリティ確保のため VPN が利用されていることが多い。日本医療情報学会会員の間では、このようなシステムにおける VPN の利用についてはコンセンサスが得られつつある。しかしながら VPN で問題になるのは NAT トラバーサル（NAT：network address translation とは、インターネットで利用するグローバル IP アドレスと、LAN 内で使うプライベート IP アドレスを相互転換する機能のことであり、ここではNAT環境でLAN内からVPN通信を行うために必要な機能の意味）の実装に制約が多く、現実問題として VPN を利用できないユーザ（医師）が存在することである。このような環境ではIPsecVPNの利用は断念せざるおえない。セキュリティを重視する場合にはVPN ゲートウェイの背後にも別途ファイアウォールを配置し、再度アクセスをコントロールする必要性も出てくるが、運用面では実用的でないと考えられる。従って、実運用を考えると本研究で採用した部分暗号化による診療情報提供書の送受信が最もセキュリティが確保できるものと考えられる。

D. 結論

XML 文書をやり取りする診療情報提供書（XML 文書）送受信システムを試作し、職位によるエレメント暗号化、診療科によ

るアクセス制御機能の動作確認を行うとともに実環境を利用した送受信テストを実施した。その結果、実装した各機能は問題なく動作することを確認した。今後は診療情報提供書入力インターフェースのブラウザ化、パッシブ・モードでのFTP通信機能の追加等の改良が必要である。

E. 研究発表

なし

F. 知的財産権の出願・登録状況

1. 特許取得

なし

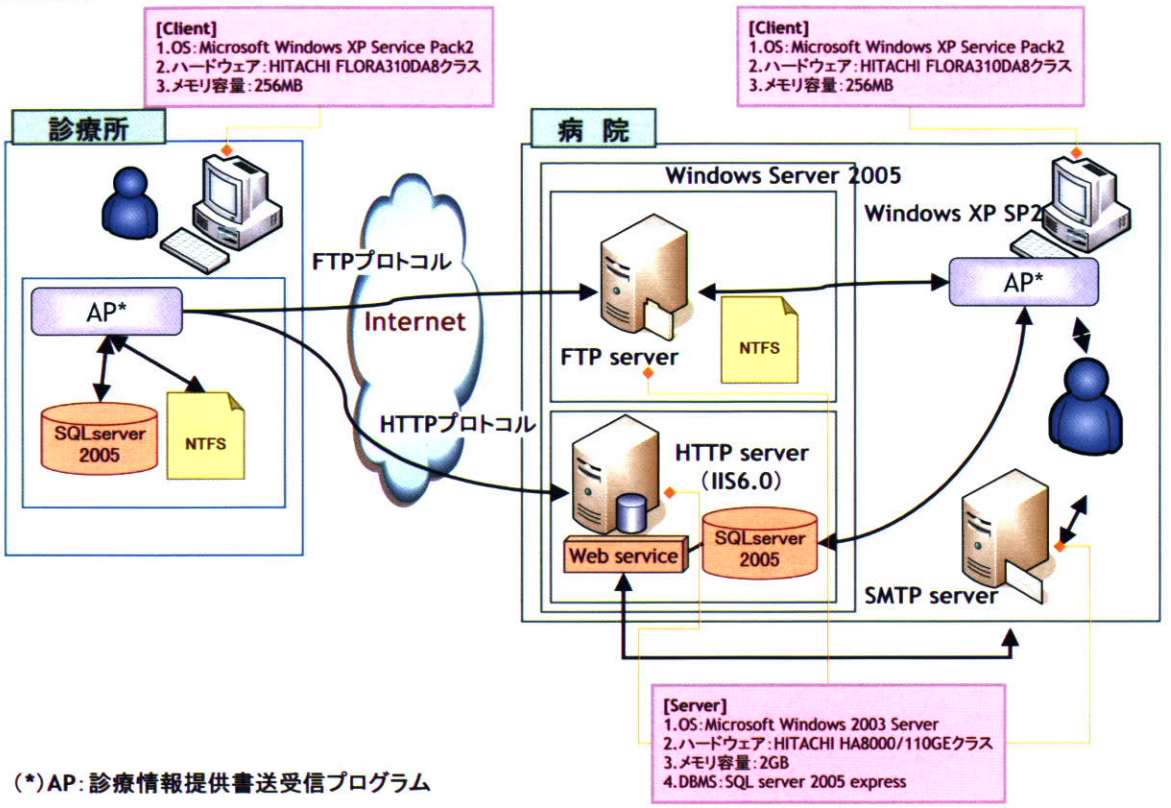
2. 実用新登

なし

3. その他

なし

図3-1 システムテストの環境



(*)AP:診療情報提供書送受信プログラム

表3-1 システムテスト考え方と実施項目

No.	項目	テスト方針	テスト項目及び内容
1	通常運用	(1)SMTPサーバからメールが送信されるか (2)送信された紹介状の内容に偏差がないか。 (3)各職位で正確に暗号化・復号化できるか。	(1)動作確認のみ (2)UNIXのdiffコマンド相当の内容でチェックする。 (3)職位の組み合わせを変化させ紹介状の内容に偏差がないことを確認する。
2		・紹介状を時間帯(朝、昼、夜)を変えて送信する	→動作確認のみ。各種テストは時間帯を可能な限り統一する。
3		・紹介状送信時にWeb閲覧が影響を受けるか	→紹介状送信時と非送信時で特定Webサイトの表示速度を計測する。CPU負荷(注3)を目安に負荷を変化させ、表示速度を計測する。
4	特異運用	・サーバ/クライアントの立上順序を変化させた場合、紹介状送信に影響はあるか	→動作確認のみ
5	性能	・紹介状を送信した場合のレスポンスはどのくらいか(暗号化項目を増減した場合)?	→暗号化項目数を変化させレスポンス(注1)を測定する。
6		・紹介状を送信し、SMTPサーバからメールが到着するまでのレスポンス・スループットはどのくらいか(送信数を増減した場合)?	→決められた時間(例えば1分間)での紹介状送信数を変化させ、レスポンス/スループット(注2)を測定する。
7		・紹介状送信時にクライアント、サーバで以下のリソースを計測する。Windows server 2003の管理ツール>パフォーマンスを利用する。 (1)CPU利用率 (2)回線利用率 (3)メモリ使用量	→項目3、5、6を測定する際に計測する。
8		・以下の紹介状送信手段の場合のレスポンス・スループットを計測する。評価基準は送信紹介状の数と暗号化項目の数とする。 (1)FTP (2)Webサービス	→項目3、5、6を測定する際に計測する。
9	既稼働業務/ネットワークへの影響	・暗号化データ項目数を変化させた(注4)ときの回線使用率への影響を計測する。回線使用率はWindows server 2003の管理ツール>パフォーマンスを利用する。	→項目3、5、6を測定する際に計測する。
10	高負荷テスト	・Webサービスでの紹介状送信ではFirewallの有無の影響を測定	→Firewall有り無しの場合に上記第8項を測定する。
11	性能	・セキュリティスキャンソフト(AntiVirus)起動の有無が紹介状通信に与える影響をみる	→AntiVirus起動の有り無しの場合に上記第8項を測定する。

(注1)レスポンス:ここでは入力画面で保存ボタンを押してから完了画面が返ってくるまでとする
(注2)スループット:ここでは決められた時間(例えば1分間)で送信可能な紹介状の数。J-Meterでのhttp、FTP送信の負荷(スレッド数)で調整する。
(注3)CPU負荷を目安に10%程度、50%程度、85%以上の3段階。
(注4)暗号化項目数は紹介状を①全く暗号化していないもの、②患者氏名から保険情報までを暗号化したもの、③全て暗号化したもの、の3段回に変化させることで設定する。

図3-2 診療情報提供書の例

診療情報提供書

平成 20 年 1 月 1 日

○○○○○○○ 医院
○○ ○○先生 御侍史

長崎大学医学部歯学部附属病院
○○○○科
TEL 095-819-7263 FAX 095-819-7267
松本 武浩（内線 7529）

下記の患者様を紹介します。どうぞよろしくお願いいたします。

【患者氏名】 ○○○○ ○○○○様 男性
【生年月日】 昭和１８年０２月１０日 満 ６４歳

【診断名】
＃１ Ｃ型慢性肝炎
＃２ 高血圧症
＃３ 腎石症

【症状経過・検査結果・治療経過】
いつも大変お世話になります。 ご多忙中強縮ですが○○氏をご紹介いたします。
○○氏は当院にて＃１にて外来経過観察中です。 2000 年に IFN 治療を受けましたが、HCV は消失しなかったものの、その後は Ib 型高ウイルスタイプですが、肝機能正常です。
一方、以前より高血圧があり下記内服にて○○病院にて治療を受けておられましたが、今回、担当医が代わられたとのことで、お住まいの近くの医院にかかりつけ医をお願いした方が良いだろうと今回ご紹介する次第です。高血圧症に関して御高診御治療をお願いいたします。
当方は＃１に関して引き続き経過観察させていただきたいと思います。
よろしくお願いいたします。

【処方】
１．ノルバスク ５ｍｇ １ｘｍ

図3-3 診療情報提供書のXMLファイルフォーマット

```
<?xml version="1.0" encoding="Shift_JIS"?>
<!-- 長崎大学医学部・歯学部附属病院 診療情報提供書 XML ドキュメント例(J-MIX 参考) 2006/07/26 -->
<PATIENT-REFERRAL>
    <HEADER>
        <情報提供 発効日>
            <年号>平成</年号>
            <年>18</年>
            <月>7</月>
            <日>26</日>
        </情報提供 発効日>
        <情報提供 目的>一般診療依頼</情報提供 目的>
        <情報提供先 医療機関 名称>○○病院</情報提供先 医療機関 名称>
        <情報提供先 医師姓>山田</情報提供先 医師姓>
        <情報提供先 医師名>三郎</情報提供先 医師名>
        <情報提供先 医師カナ姓></情報提供先 医師カナ姓>
        <情報提供先 医師カナ名></情報提供先 医師カナ名>
        <情報提供先 医療機関 郵便番号>852-8501</情報提供先 医療機関 郵便番号>
        <情報提供先 医療機関 住所>長崎県長崎市坂本１丁目７番１号</情報提供先 医療機関 住所>
        <情報提供先 医療機関 名称>長崎大学医学部・歯学部附属病院</情報提供先 医療機関 名称>
        <情報提供先 医療機関 電話番号>095(849)7200</情報提供先 医療機関 電話番号>
        <情報提供先 医療機関 電話番号>095(849)</情報提供先 医療機関 電話番号>
        <情報提供先 医療機関 FAX 番号>095(849)</情報提供先 医療機関 FAX 番号>
        <情報提供先 診療科 名称>第一内科</情報提供先 診療科 名称>
        <情報提供先 医師姓>長崎</情報提供先 医師姓>
        <情報提供先 医師名>太郎</情報提供先 医師名>
        <情報提供先 医師カナ姓></情報提供先 医師カナ姓>
        <情報提供先 医師カナ名></情報提供先 医師カナ名>
    </HEADER>
    <PATIENT-INFO>
        <患者 姓>患者</患者 姓>
        <患者 名>太郎</患者 名>
        <患者 カナ姓>カンジャ</患者 カナ姓>
        <患者 カナ名>タロウ</患者 カナ名>
        <患者 性別>M</患者 性別>
        <患者 郵便番号>000-0000</患者 郵便番号>
        <患者 住所>長崎県長崎市１町</患者 住所>
        <患者 電話番号>000-000-0000</患者 電話番号>
        <患者 生年月日>
            <年号>昭</年号>
            <年>62</年>
            <月>3</月>
            <日>9</日>
        </患者 生年月日>
        <患者 職業>大工</患者 職業>
    </PATIENT-INFO>
    <DISEASE-INFO>
        <現疾患 診断 名称>慢性胃炎</現疾患 診断 名称>
        <現症歴>特記すべきことなし</現症歴>
        <家族歴></家族歴>
        <現病歴>症状経過は別紙参照。</現病歴>
    </DISEASE-INFO>
    <PRESENT-INFO>
        <現病歴所見要約 自由記載>2006.7.1 GOT-23 GPT-16 γ-GTP-20</現病歴所見要約 自由記載>
        <現投与 薬剤商品名>ロペミンカプセル</現投与 薬剤商品名>
        <現投与 薬剤一般名></現投与 薬剤一般名>
        <現投与 薬剤用量>1mg 2カプセル</現投与 薬剤用量>
        <現投与 薬剤用量基準時間></現投与 薬剤用量基準時間>
        <現投与 薬剤単位></現投与 薬剤単位>
        <現投与 薬剤用法>1 日 2 回朝夕食後に</現投与 薬剤用法>
        <現投与 薬剤適用備考></現投与 薬剤適用備考>
    </PRESENT-INFO>
    <SUMMARY>
        <診療要約>下記処方は常空のものです。</診療要約>
    </SUMMARY>
    <備考>特記すべき事はありません。</備考>
</PATIENT-REFERRAL>
```

図3-4 XMLセキュリティシステム —診療情報提供書(紹介状)運用—

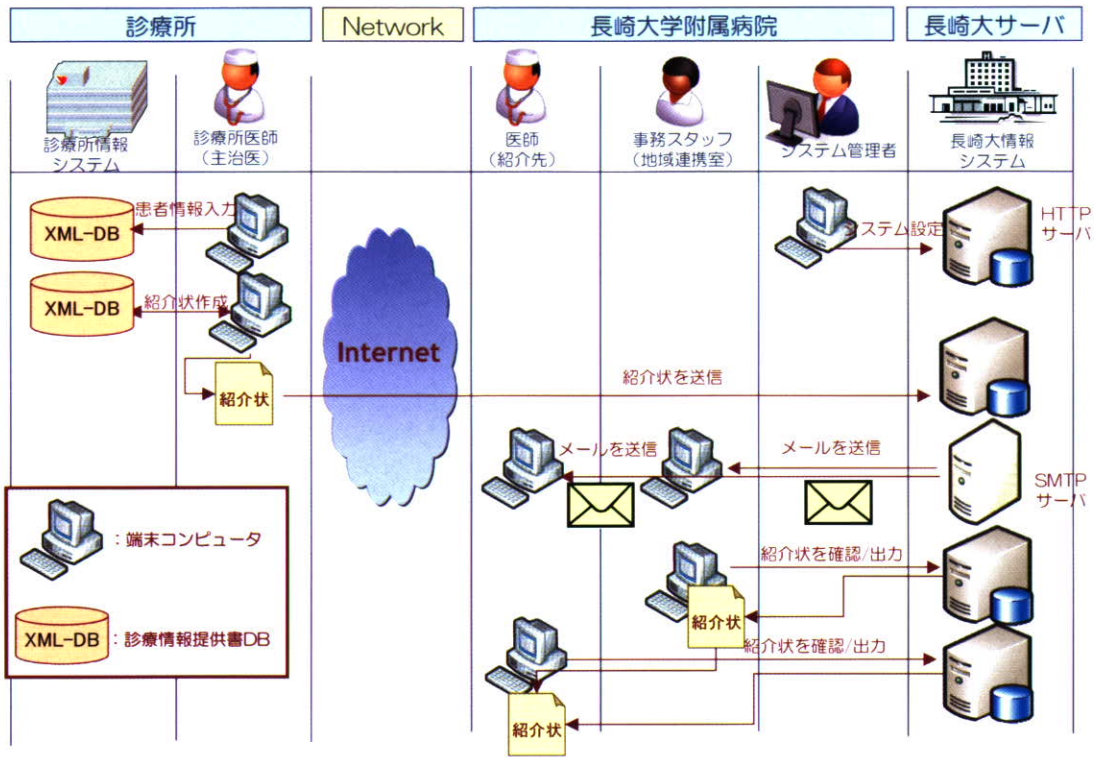


図3-5 XML形式で作成した暗号化診療情報提供書の送信手順(Webサービスの場合)

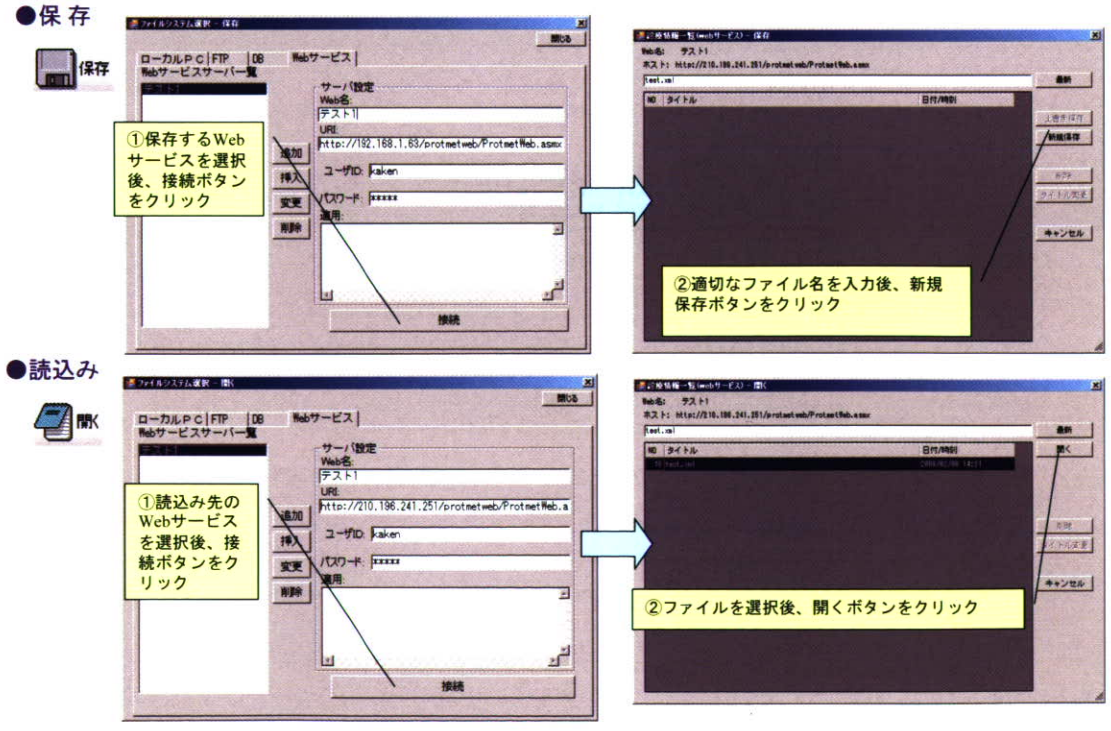


図3-6　到着案内メールの例

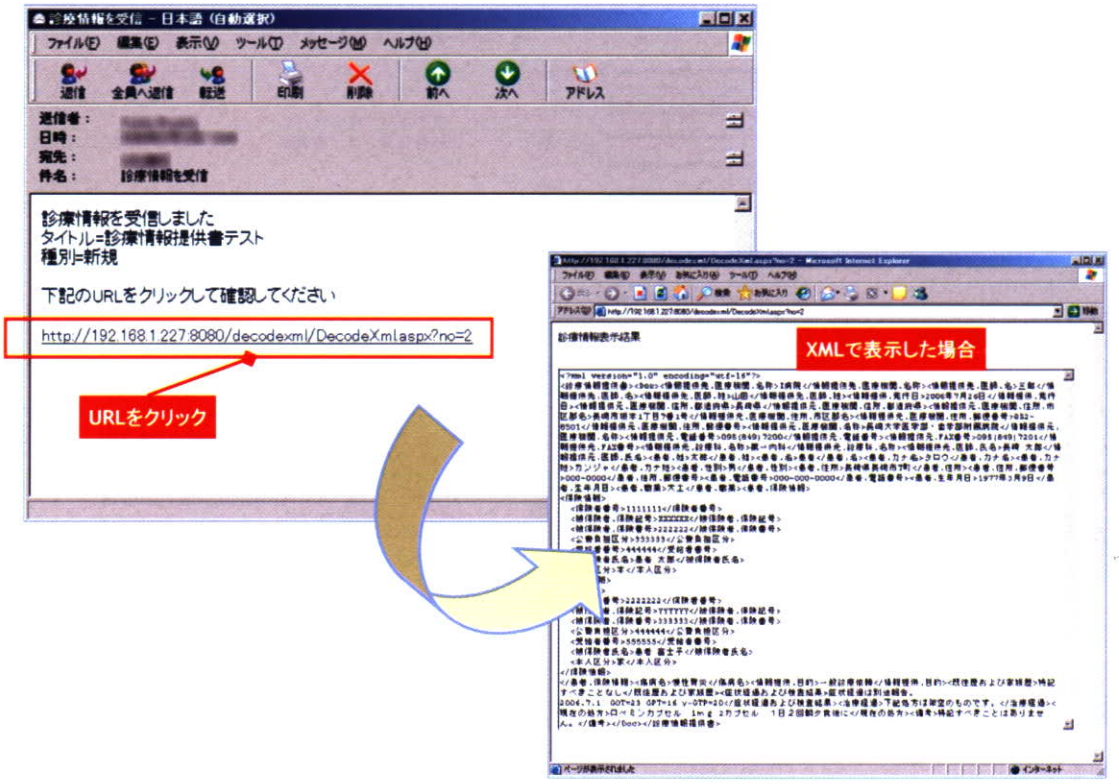
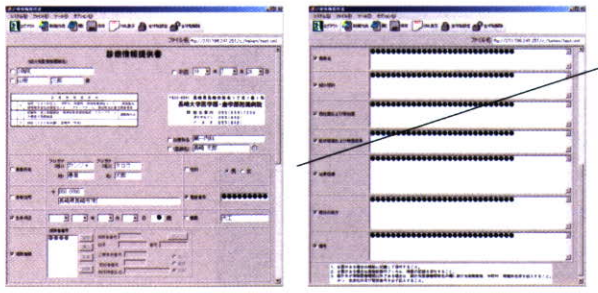


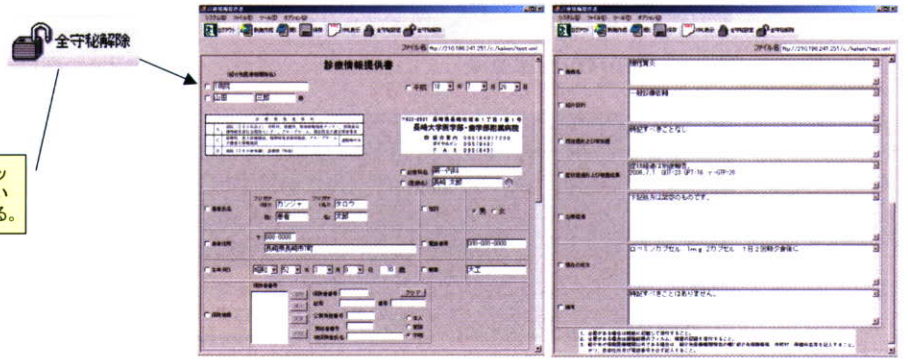
図3-7(1)　XMLドキュメント(診療情報提供書)の暗号化・復号化手順

● 診療情報提供書の復号化　－全項目閲覧可能なユーザーの場合－

⇨ 全ての項目を閲覧可能なユーザー(ここでは例として「doctor」)でログイン後、診療情報提供書の読込みを行う。



一部の項目が暗号化されている。
※暗号化部分は「●●●・・・」といった文字列で表示されている。

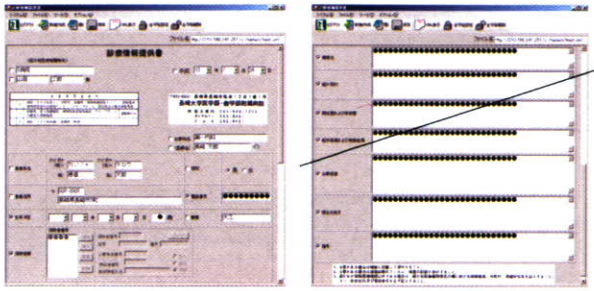


全守秘解除ボタンをクリックすると、暗号化されている項目が全て復号化される。

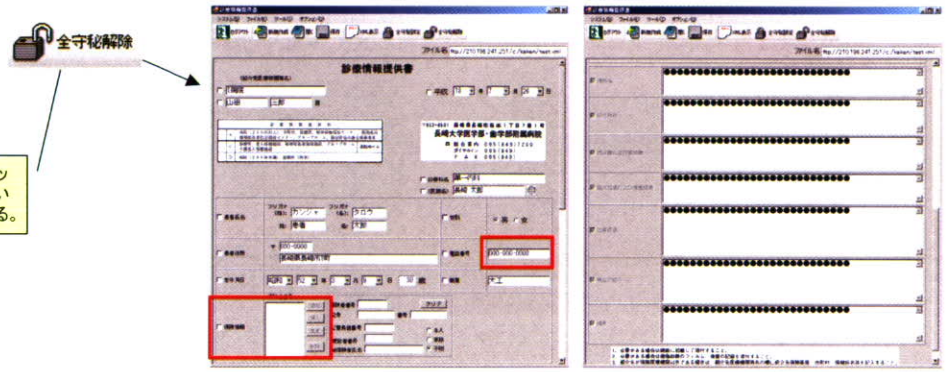
図3-7(2)　XMLドキュメント(診療情報提供書)の暗号化・復号化手順

● 診療情報提供書の復号化　－１部の項目が閲覧可能なユーザーの場合－

⇨ 1部の項目を閲覧可能なユーザー(ここでは例として「jimu」)でログイン後、診療情報提供書の読込みを行う。



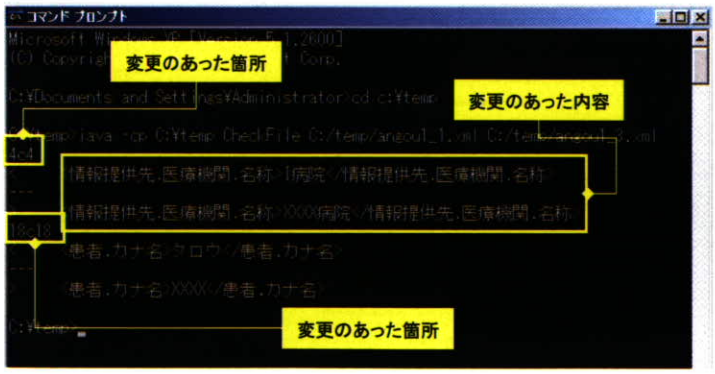
一部の項目が暗号化されている。
※暗号化部分は「●●●・・・」といった文字列で表示されている。



全守秘解除ボタンをクリックすると、暗号化されている項目が一部復号化される。

図3-8　差分チェックプログラム

● 比較文書に差異があった場合



● 比較文書に差異がなかった場合

表3-2 診療情報提供書送信に与える暗号化子項目数の影響-upload-

● 暗号化項目数によるレスポンス時間の測定－FTP－

	A [暗号化なし]	B [基本情報のみ]	C [全て]
1回目	906	1063	1110
2回目	797	968	1000
3回目	828	1000	1047
4回目	922	969	1281
5回目	890	1000	1063
平均	868.6	1000	1100.2

● 暗号化項目数によるレスポンス時間の測定－HTTP－

	A [暗号化なし]	B [基本情報のみ]	C [全て]
1回目	531	750	969
2回目	672	1000	1063
3回目	719	891	1047
4回目	735	938	1125
5回目	782	1094	1078
平均	687.8	934.6	1056.4

図3-9 診療情報提供書送信に与える暗号化子項目数の影響-upload-

図　診療情報提供書送信(upload)に与える暗号化の影響(FTPの場合)

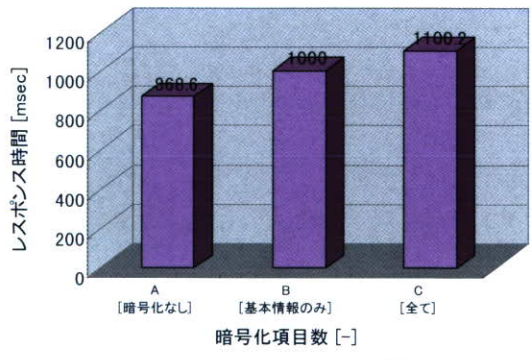


図　診療情報提供書送信(upload)に与える暗号化の影響(HTTPの場合)

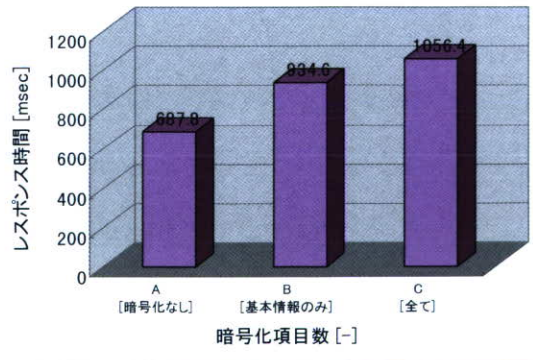


表3-3 診療情報提供書送信に与える暗号化子項目数の影響-download-

● 暗号化項目数によるレスポンス時間の測定－FTP－

	A［暗号化なし］	B［基本情報のみ］	C［全て］
1回目	740	780	805
2回目	470	558	607
3回目	508	598	657
4回目	500	531	672
5回目	516	640	719
平均	546.8	621.4	692

● 暗号化項目数によるレスポンス時間の測定－HTTP－

	A［暗号化なし］	B［基本情報のみ］	C［全て］
1回目	593	687	766
2回目	572	610	765
3回目	422	671	781
4回目	609	718	750
5回目	562	672	734
平均	551.6	671.6	759.2

図3-10 診療情報提供書送信に与える暗号化子項目数の影響 -download-

図　診療情報提供書送信(download)に与える暗号化の影響(FTPの場合)

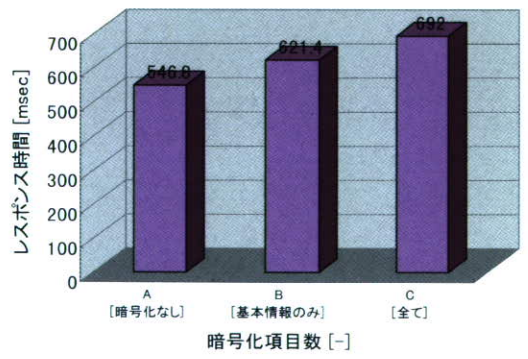


図　診療情報提供書送信(download)に与える暗号化の影響(HTTPの場合)

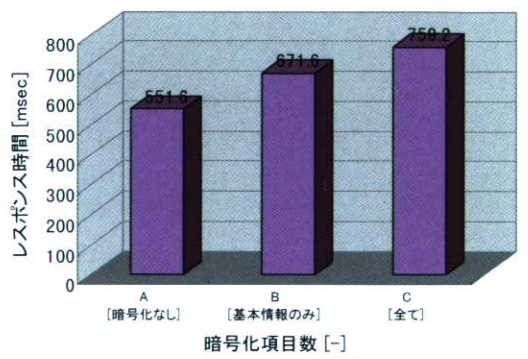


表3-4 診療情報提供書送信(upload)に与える送信メール数の影響(FTPの場合)

送信メール数[-]	1	3	5	10	15	20	25	30	45	60
A[暗号化なし]	938	2468	4250	8345	12641	17531	21251	25594	37546	45468
B[基本情報のみ]	859	2766	4110	8156	12267	16687	21313	25062	38686	52734
C[全て]	1047	3157	5314	10518	15832	21036	26350	31554	47386	63218

(注)5回計測した値の平均値msec

送信メール数[-]	1	3	5	10	15	20	25	30	45	60
A[暗号化なし]	0.938	2.468	4.25	8.345	12.64	17.531	21.251	25.594	37.546	45.468
B[基本情報のみ]	0.859	2.766	4.11	8.156	12.27	16.687	21.313	25.062	38.686	52.734
C[全て]	1.047	3.157	5.314	10.518	15.83	21.036	26.35	31.554	47.386	63.218

(注)5回計測した値の平均値 μ sec

図3-13 診療情報提供書送信(upload)に与える送信メール数の影響(FTPの場合)

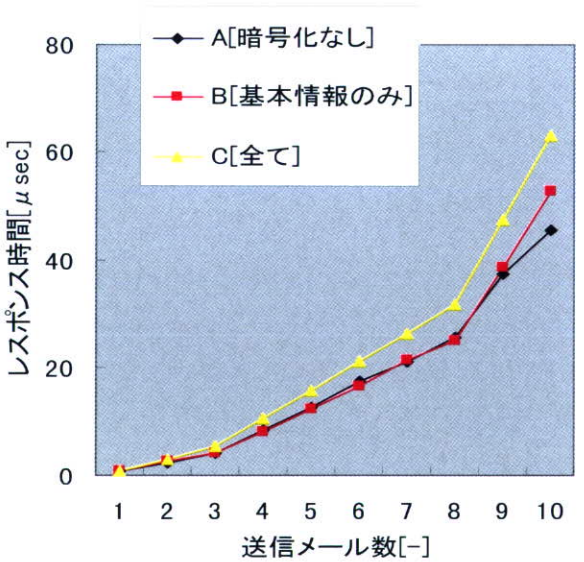


図　診療情報提供書送信(upload)に与える送信メール数の影響(FTPの場合)

表3-5　診療情報提供書送信(upload)に与える送信メール数の影響(HTTPの場合)

送信メール数[-]	1	3	5	10	15	20	25	30	45	60
A[暗号化なし]	31	141	218	531	609	767	1030	1155	1862	2452
B[基本情報のみ]	94	266	438	875	1563	1922	2250	2858	4172	5858
C[全て]	109	313	594	1125	1733	2298	2983	3840	5576	6912

(注)5回計測した値の平均値msec

送信メール数[-]	1	3	5	10	15	20	25	30	45	60
A[暗号化なし]	0.31	1.41	2.18	5.31	6.09	7.67	10.3	11.55	18.62	24.52
B[基本情報のみ]	0.94	2.66	4.38	8.75	15.63	19.22	22.5	28.58	41.72	58.58
C[全て]	1.09	3.13	5.94	11.25	17.33	22.98	29.83	38.4	55.76	69.12

(注)5回計測した値の平均値10μsec

図3-14　診療情報提供書送信(upload)に与える送信メール数の影響(HTTPの場合)

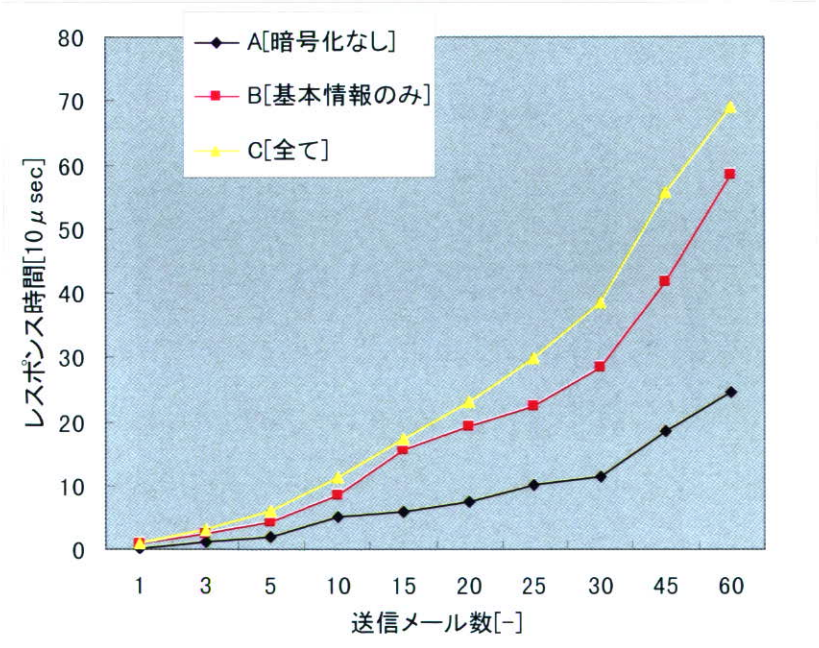


図　診療情報提供書送信(upload)に与える送信メール数の影響
(HTTPの場合)

表3-6 診療情報提供書送信(download)に与える送信メール数の影響(FTPの場合)

送信メール数[-]	1	3	5	10	15	20	25	30	45	60
A[暗号化なし]	219	516	1266	2062	3314	4329	5358	6453	9641	13252
B[基本情報のみ]	190	594	1313	2125	3483	4250	5672	6923	9922	13579
C[全て]	265	719	1141	2188	3265	4609	5796	6421	10407	14672

(注)5回計測した値の平均値msec

送信メール数[-]	1	3	5	10	15	20	25	30	45	60
A[暗号化なし]	2.19	5.16	12.66	20.62	33.14	43.29	53.58	64.53	96.41	132.52
B[基本情報のみ]	1.9	5.94	13.13	21.25	34.83	42.5	56.72	69.23	99.22	135.79
C[全て]	2.65	7.19	11.41	21.88	32.65	46.09	57.96	64.21	104.07	146.72

(注)5回計測した値の平均値10μsec

図3-15 診療情報提供書送信(download)に与える送信メール数の影響(FTPの場合)

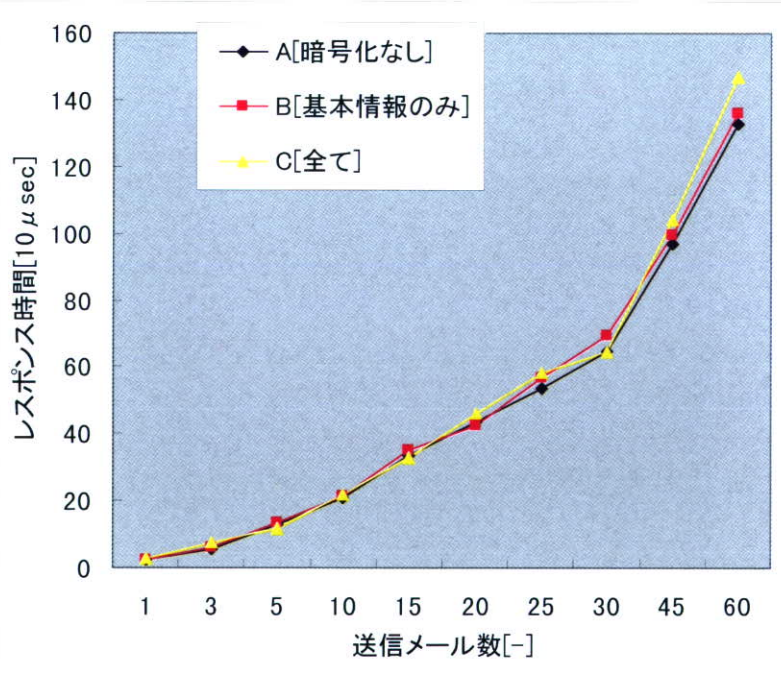


図　診療情報提供書送信(download)に与える送信メール数の影響
(FTPの場合)