コンピュータセキュリティ 19－2
（２００２．１２．２０）

ネットワーク上の戸下通信システムの提案

富田哲也　　村山優子

岩手県立大学大学院 ソフトウェア情報学研究科

「戸」は住居や居宅への入り口であるだけではなく，住人と訪問者等との様々な情報の交換の媒体ともなる．本研究では「戸」のメタファを利用したコミュニケーションを「戸口通信」と呼びネットワーク上に実現している．本稿では「戸下通信」に着目し，そのモデル，設計，実装についての報告を行うとともに,「戸下通信」に求められるセキュリティ機能について考察する．

Proposal for Uunder The Door Communication on the network

Tetsuya Tomita　　Yuko Murayama

Graduate School of Software and Information Science
Iwate Prefectual University

In this research we try and implement communication systems using the metaphor of a door on the World Wide Web (WWW) as a media for informal communications. We call those informal communications through a door "on-door-communications". This paper introduces a system for the under-the-door communication. We present its model design and implementation. Finally, we discuss on its security issues.

1　はじめに

学生寮などの個人の部屋の「戸」は部屋への入り口であるだけではなく，部屋の住人と他の住人との様々な情報交換の媒体でもある．

「戸」を利用したコミュニケーションには，部屋の戸口に設置された伝言板にその部屋の住人宛のメッセージを書き込むコミュニケーションや，訪問者が部屋の戸を叩くことにより音で通信の意思を伝えるコミュニケーションがある．さらに，学生が教官の研究室の戸の下へ提出物を挿入したり，ホテル等の宿泊客への緊急あるいは秘密のメモなどを部屋の戸の下から入れるような戸下通信もある．

本研究では，このような「戸」をメタファとするコミュニケーションを「戸口通信」と呼び，ネットワーク上にこのような通信を行うためのシステムを構築し，コミュニケーションメディアとしての可能性を探る [1].

本稿では特に，戸の下から書類を差し入れる戸下通信に着目し，ネットワーク上での実現手法，技術の検討を行い，コミュニケーションモデル，システム設計およびプロトタイプの実装について報告する．さらに，本システムに必要なセキュリティについて考察する．

2　関連研究

戸を通して行われるコミュニケーションについての研究の多くは，戸の開閉状態などを WWW 上に取り込み提供する Door Awareness System[2]，また WWW 上から戸に掲げた掲示板などに対して情報を伝える Dynamic Door Displays[3] など

現実世界の戸とのインタフェースを実現している．本研究 [1] では WWW 上のホームページをその所有者とのコミュニケーション空間への入り口ととらえ，そこに戸のメタファを用いて新しいコミュニケーション媒体の構築を目的としている．

戸下通信のように個人からある個人に電子化された情報を伝えるシステムにはレポート提出システム [4] が挙げられる．このシステムはフォーマルな情報のやり取りに利用され情報を伝える者は事前に登録を行うなど身分が明らかである．戸下通信では情報を伝える者は不特定で扱われる情報も特定しないインフォーマルなコミュニケーションに利用される．

また，電子メールなどを利用した場合，戸下通信で行われているようなコミュニケーションが可能であり，電子メールとの差異についての調査は今後行う．

3　戸下通信のモデル

戸下通信では，戸を通して不特定多数の人々と部屋の住人との間でコミュニケーションが行われる．メモを渡したい相手の部屋の場所を知っていれば，誰でもその場所を訪問し，その戸の下から自由にメモなどを入れることができる．部屋とは戸下通信のコミュニケーション空間で住人は部屋の戸の鍵を所有し，部屋に自由に出入りできる．住人は部屋の中に入り，訪問者が残したメモの存在に気付き，それを読む．

図１に示すように戸下通信の構成要素には部屋の戸，訪問者，部屋の住人，通りすがりの人々，メモ，部屋の所有者，部屋の鍵などがある．

戸は訪問者から部屋の住人だけへメモを伝えるためのインタフェースであり，次のような機能がある．訪問者からメモを受け取り，保存管理する．部屋の中に入らなければ誰もメモの存在に気付くこともメモを読むこともできない． このアクセス制御を戸が行う．

通りすがりの人々は偶然に部屋の前を通った人々で訪問者と同じようにメモを部屋の住人に残すことが可能である．

部屋の所有者は住人に部屋を貸し，戸のマスター鍵を所有し，管理のために入室できる．

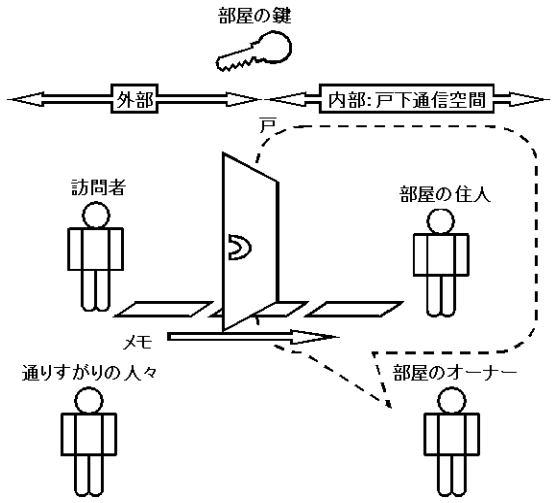


図 1: 戸下通信のモデル

4　戸下通信システムの設計

本研究では，部屋を WWW 上のホームページととらえ，そこへの入り口となるポータルサイトのページを「戸」と考える．WWW 上での部屋の住人は自分の戸のページに残されたメモを読むためのアクセス権を持つ．

不特定多数の訪問者は，何らかの方法で WWW 上の住人の「戸」の頁の存在を知りアクセスする．メモは訪問者が住人に渡したい情報であり，テキストデータの他，画像や音声なども含むマルチメディア情報とする．

戸下通信システムはクライアントサーバ型である．サーバはメモの保存管理を行う戸下通信空間を提供しクライアントがその空間への「戸」を提供する．戸の所有者は戸下通信サービス提供を行う ASP(Application Service Provider) で，戸下通信サーバを管理し,「戸」の利用権を住人に与える．住人は，自分のホームページ上に，戸下通信サーバへのリンクを設定する．このリンクを通して，住人や訪問者は戸下通信のクライアントの機能を取得する．

通信は部屋の住人と不特定多数の人々と行われる一対多の非同期コミュニケーションである．戸下通信の設置されているホームページを訪れた訪問者は誰でもメモを残すことが可能であり，住人が戸下通信にアクセスしているかどうかに関わらずメモを残すことが可能である．

4.1 ユーザインタフェースの設計

ユーザインタフェースについての本研究の方針は，ユーザに説明を必要としない直感的な操作を提供することである．ユーザはホームページ上の戸下通信へのリンクを通してサービスを利用することができる．戸の機能はサブウインドウで提供される．戸は戸下通信空間へのアクセス機能を持つ（図２）．

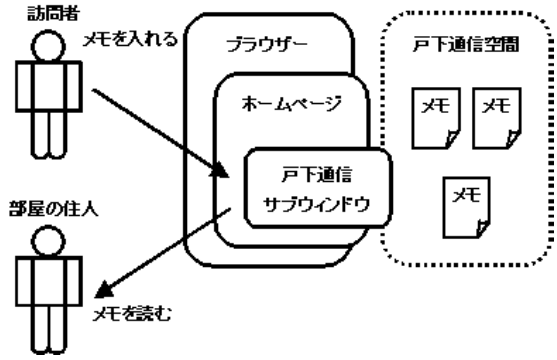


図 2: インタフェース概念図

4.2 システム構成

戸下通信システムはWWW上のクライアント/サーバ型システムとする（図３）．

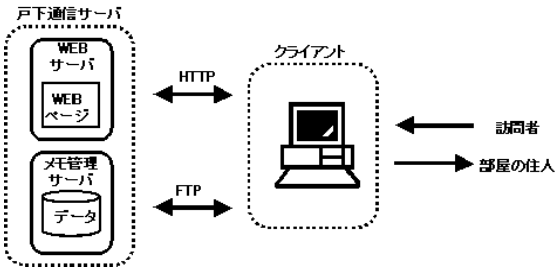


図 3: システム構成図

クライアント端末は，WEBサーバに対して戸の機能の要求や，ユーザからの入力に従いメモ管理サーバに対してメモデータの送受信要求を行う．またユーザの認証を行いメモ管理サーバに対するアクセス制御を行う．訪問者にメモ管理サーバへのメモデータの送信，部屋の住人にメモ管理サーバからのメモデータの受信を許可する．

戸下通信サーバはWEBサーバとメモ管理サーバにより構成される．WEBサーバはクライアント端末から要求された戸の機能をクライアント端末に送り，メモ管理サーバはクライアント端末からのメモデータの受信，保存，管理，クライアント端末へのメモデータの送信を行う．

今回，戸の機能の送受信にはHTTPプロトコルを用いた，またメモデータの送受信にはFTPプロトコルを用いる．

5 プロトタイプの実装

クライアントの実装は，Java言語で行いJavaアプレットを用いた．サーバが提供する機能のメモ管理にはFTPサーバを用いた．実装に使用したソフトウェアを表１に示す．

表 1: 実装に使用したソフトウェア

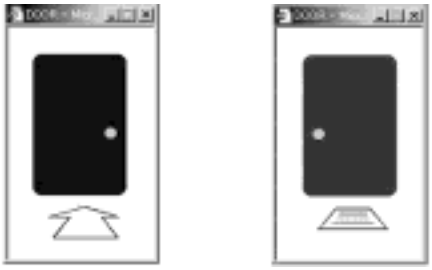
OS	Linux version2.4.18
HTTP デーモン	apache-1.3.26
FTP デーモン	proftpd-1.2.4
Java	1.4.0

クライアントにJavaアプレットを用いることで，ユーザはソフトウェアのインストールが不要となる．Javaアプレットは自動的にサーバからクライアントの端末に読み込まれ実行される．クライアントの端末にJavaアプレットの実行が可能なブラウザーとインターネットへの接続環境があればどこからでもメッセージを届けたり，読んだりすることが可能となる．

アプレットが実行されるとメモデータをクライアント端末からメモ管理サーバに送信する機能，部屋への入室認証機能が提供される．クライアント・サーバ間のFTPコネクションはアプレット実行時に確立され，アプレットが終了するまで維持される．FTPサーバとのコネクション確立に必要なID，パスワードはアプレット内で保持している．

メモ管理サーバに対するアクセス制御はアプレットの機能を訪問者用（戸の外側）と部屋の住人用（戸の内側）（図４）で切り替えることによって行っている．訪問者にはメモ管理サーバにメモデータを送信する機能，部屋の住人にはメモ管理

サーバよりメモデータを受信する機能が提供される．部屋の住人用の機能は入室認証により認証されたユーザのみに提供される．入室はユーザが入力したパスワードがアプレット内に保持されている認証パスワードと一致した場合に許可する．入室認証により部屋への入室が許可されるとメモをメモ管理サーバからクライアント端末に受信する機能が提供される．



外側　　内側

図 4: 戸下通信空間（部屋）

メモの存在の有無はメモアイコンにより確認ができる．メモアイコンはメモデータがメモ管理サーバに存在する場合に表示される．

6　戸下通信における脅威と対策

6.1　戸下通信における脅威

戸下通信では，訪問者からのメモが紛失したり，改ざんされたり，宛先の住人以外に読まれたりすることなく宛先の住人に伝わるようにする必要がある．本システムは現実の戸下通信をモデルとしていることから，まず現実の戸下通信の脅威を挙げ，次に WWW での戸下通信の脅威について考える．

6.1.1　現実の戸下通信における脅威

戸下通信ではメモ，部屋の鍵，部屋の住人が守るべき対象となる．これらの対象は次のような脅威にさらされる．

1. メモの盗難やすりかえ.
2. 部屋の鍵の盗難や紛失.
3. 住人に対するメモによる迷惑.

メモは訪問者が訪問の途中にメモを盗まれたり，いつの間にかすりかえられることが考えられる．にせ金庫事件 [5] のように部屋番号などをすりかえ訪問者を他の部屋に誘導しメモを奪う方法がある．また，戸が消された事件 [6] のように部屋の戸を隠しメモが相手に渡ることを妨害することも可能である．内部のメモも戸のピッキングによる部屋への侵入や窓など他の出入り可能な場所からの侵入により盗まれたりすりかえられたりすることがあるだろう．また部屋への侵入を行わなくとも道具を使用してドアの下の隙間からメモなどを取り出し奪うなどの方法もある．また管理者が貸し出した部屋のマスター鍵により侵入しメモを盗み見る可能性もある．

部屋の住人や管理者の鍵の盗難や紛失は部屋への侵入につながる可能性がある．鍵が盗難や紛失した場合にはそのことに気付き鍵の付け替えなどの処置をとるだろう，しかし鍵の複製などを作成された場合にはその事実に気付くまで侵入を許すこととなる．

住人に対するメモは本人が望むものとは限らない．大量のダイレクトメールなどは住人にとって迷惑なものであろう．また危険物が差し入れられる可能性もある．

6.1.2　WWW の戸下通信における脅威

WWW の戸下通信ではメモデータ，パスワード，部屋の住人のクライアント端末が守るべき対象となる．これらの対象は次のような脅威にさらされる．

1. メモデータの盗聴や改ざん.
2. パスワードの漏洩.
3. 不正なメモデータによる迷惑.

メモデータは訪問者からメモ管理サーバへの通信路やメモ管理サーバから部屋の住人への通信路で盗聴，改ざんされることが考えられる．また WEB サーバをなりすまし訪問先のものではない不正な戸アプレットを訪問者のクライアント端末に送りメモデータを自身に送らせ盗聴する方法などもある．メモ管理サーバのメモデータもパス

ワードクラックやセキュリティホールからのメモ管理サーバに対する不正アクセスにより盗聴や改ざんが行われる可能性がある．またサーバにトロイの木馬やバックドアを仕掛けそれを利用しメモデータを盗聴する方法もあるだろう．またシステム管理者によるメモデータの盗聴，改ざんも考えられる．

部屋の住人やシステム管理者のパスワードの漏洩はメモデータの盗聴や改ざんの可能性につながる．

訪問者からのメモデータが安全なものであるとは限らないスパムやウイルスやなど部屋の住人にとって迷惑なものが送りつけられる可能性もある．

6.1.3 現実と WWW の戸下通信における脅威の比較

このように現実と WWW の戸下通信には，共に多くの脅威が考えられる．しかし次に述べるようなことにより WWW では現実の戸下通信にくらべより多くの脅威にさらされると考えられる．

WWW ではクライアント上で起動された戸アプレットが部屋への入り口となる．そのためメモ管理サーバ，クライアントとメモ管理サーバ間の通信も部屋の中での出来事と考えられる．現実の世界では安全と考えられる部屋の中に多くの脅威がある．

現実の戸下通信では訪問者が部屋にメモを入れる際に奪われたり，すりかえられたりすることはメモを狙う者にとっても危険が大きくよほどのことがなければ発生するとは考えにくい．また部屋の住人は部屋に入った時点で確実にメモを受け取ることが出来るだろう．しかし WWW では訪問者のメモがメモ管理サーバにたどり着くまでには盗聴や改ざんなどの脅威があり，部屋の住人がメモを受け取るまでにも同様の脅威にさらされてしまう．

また現実の世界ではメモを狙う者や部屋の管理者が部屋に侵入する場合は部屋の住人や他の住人に目撃される可能性がある．しかし WWW では利用者がサーバのシステム管理の権限をもつことはなく自身のメモデータが何者かにより盗聴されたことを知るすべがなくシステムの管理者が利用者に知られることなくメモデータを盗み見ることが容易に行えるであろう．

現実世界では誰かに目撃される恐れや危険物を入手することが困難であることから，危険物がメモとして届けられる可能性は低いのではないかと考える．しかし WWW では匿名性が高くまたコンピュータウイルスなどの入手も可能であることから，部屋の住人のクライアント端末が危険にさらされる可能性が高いと考える．

6.2 問題点と対策

戸下通信で訪問者からの情報を盗聴，改ざんされることなく確実に部屋の住人に伝えるためには戸下通信空間の安全性をいかに高めるかが重要である．そのために求められるセキュリティ対策について考えた．

6.2.1 通信路について

戸下通信ではクライアントとメモ管理サーバ間でのメモデータに対する機密性，完全性を確保する必要がある．また FTP セッション確立時に利用される ID，パスワードに対する機密性の確保も必要である．そのためには通信データの暗号化，メモ管理サーバのなりすまし防止の必要がある．その対策として SSL によるサーバ認証や暗号化通信路の確保が考えられる．

6.2.2 メモ管理サーバについて

メモ管理サーバに対する不正アクセスや管理者からメモ管理サーバ内のメモデータに対する機密性，完全性を保つためにはあらかじめクライアントにてメモデータを暗号化し送信するなどの方法が考えられる．

暗号化の方法としては部屋の住人の公開鍵を用いる方法などがある．しかしユーザの端末を特定しない戸下通信では鍵の管理をどのように行うかが問題となる．

6.2.3 ユーザ認証について

本システムでは部屋に入室するための認証に用いられるパスワード検証をクライアント端末のア

プレット内で行っている．

認証パスワードはアプレット内にコードとして保持されるためコード解析などによりパスワードの漏洩などの恐れがある．また，FTP サーバへの認証 ID，パスワードも同様にアプレット内にコードとして保持されるため同様の危険性がある．対策としてはコード内の ID，パスワードの暗号化や認証をクライアントではなくサーバ側で行うなど認証プロトコルの変更などが考えられるだろう．

6.2.4 Java アプレットの認証

本システムではクライアントシステムに Java アプレットを用いる．このためクライアントが提供する訪問者によるメモデータ送信や部屋の住人によるメモデータ受信の機能が Java アプレットのセキュリティにより規制される．これは，Java アプレットは必要となった時に Web から自動的にクライアントに読み込まれ実行されるため，悪意のある不正なアプレットによりクライアントのデータが漏洩や改ざんなどの危険にさらされることを防ぐためである．

これらの規制を回避するには，ユーザからアプレットのローカル資源へのアクセスやネットワークへの接続に対する許可を得る必要がある．ユーザから許可を受ける方法としてアプレットが実行されるクライアントの Java セキュリティポリシーの変更や，アプレットに署名を付け発行元を示しユーザに認証を受ける方法がある．本システムでは署名付きアプレットによりユーザに対し許可を求めることとした．

プロトタイプシステムでは証明書はアプレット製作者のものを利用している．今後，戸下通信を多くの利用者に提供する場合，利用者個人の証明書を利用し誰の戸であるかを証明する方法が考えられる．

7 まとめ

本稿では，戸下通信モデルを基にしたコミュニケーションシステムの設計，実装とセキュリティの考察について述べた．

現実の戸下通信では，戸締りのされた部屋には容易に侵入出来ないという安全性により，訪問者からのメモが宛先の住人以外に読まれたり，紛失や改ざんされることなく宛先の住人に伝えることを可能にしている．

WWW 上の戸下通信でも戸下通信空間に対するセキュリティ対策が重要である．今後は戸下通信空間でのメモデータの盗聴や改ざんに対するセキュリティ対策の改善を進めて行きたい．

参考文献

[1] 権藤広海，鈴村圭史，瀬川典久，山根信二，村山優子，宮崎正俊：ネットワーク上の戸口通信システムの構築，情報処理学会 第 43 回グループウェアとネットワークサービス研究会報告，Vol.2002，No.31，pp.79-84,（2002）

[2] J. Nichols, J. O. Wobbrock, D. Gergle, and J. Forlizzi：Mediator and Medium，In Proc. of DIS'2002，pp.379-386，(2002)

[3] D. Nguyen, J. Tullio, T. Drewes, E. Mynatt：Dynamic Door Displays，http://www.cc.gatech.edu/grads/t/Joseph.Tullio/doorshort.htm （2002・11 参照）

[4] 広島大学 情報メディア教育研究センター：レポート提出システム，http://www.riise.hiroshima-u.ac.jp/service/report/ （2002・11 参照）

[5] にせ夜間金庫事件，昭和 48 年大阪の梅田で発生，http://www.atmarkit.co.jp/fsecurity/special/24gpki/gpki01.html（2002・11 参照）

[6] MIT で学長室の戸が消された事件，http://hacks.mit.edu/Hacks/by-year/1990/vest-bboard/ （2002・11 参照）

[7] 瀬川典久，村山優子，権藤広海，山根信二，宮崎正俊：戸口伝言板における匿名化の提案，情報処理学会 情報処理学会論文誌 第 43 巻 3 号，pp.815-824，(2002)