Vol.2011-UBI-32 No.12
2011/11/24

「覗き込み」を利用した直感的な外部ディスプレイアクセス方式の提案

小木真人[†1] 清水裕基[†1] 三好健文[†1]
吉永努[†1] 入江英嗣[†1]

本論文では，携帯端末とディスプレイ端末を連携するため,「覗き込む」ことによって携帯端末からディスプレイ端末に無線環境でアクセスするシステム UDU を提案する．携帯端末とディスプレイ端末を連携するためには，簡単に携帯端末とディスプレイ端末を接続できることが必要である．また，携帯端末が不特定多数が使う公共のディスプレイ端末と連携する場合でも，安全に通信できる必要がある．そこで，UDU では通信したいディスプレイ端末に表示した識別子を携帯端末のカメラで読み込むことにより，簡単かつセキュアに携帯端末とディスプレイ端末の連携を実現する．本システムの初期実装では，ディスプレイ端末を携帯端末のカメラで「覗き込む」だけで，簡単にディスプレイ端末との通信が確立できた．

Proposal of External Display Access Using "Looking into the Display"

MASATO KOGI,[†1] HIROKI SHIMIZU,[†1]
TAKEFUMI MIYOSHI,[†1] TSUTOMU YOSHINAGA[†1]
and HIDETSUGU IRIE[†1]

This paper proposes a system named UDU that enables mobile devices to access external displays in a wireless environment with just "looking into the display" for use the large screen. The UDU provides a simple connection procedure in order to cooperation between a mobile device and an external display easily. In addition, UDU also provides a secure connection mechanism in order to employ both of private and public displays. The key idea of UDU is a scheme to provide these two features by a camera embedded the mobile devices. By capturing a displayed identifier on a target display via the camera, UDU connects the device to the display in a secure manner. In this paper, it is shown that the preliminary implementation of the the proposed system enables a mobile device to connect an external display.

1. はじめに

近頃の携帯端末の処理速度は向上しているが，持ち運び可能でなければならないため，携帯できる物理的な大きさには制約がある．そのため，表示できる情報は画面のサイズに制限されてしまい，ユーザビリティが損なわれている．その代表例として，スマートフォンでの Web 閲覧では，文字や図が小さく表示され PC ほどの識別性を得られない．一方ディスプレイ端末側を見ると，駅や繁華街などには周辺地図などを表示する大型のデバイスが普及してきている．そこで，携帯端末とこれらのディスプレイ端末が通信でき，外部ディスプレイ端末として利用できれば，外出先でも大型のディスプレイ端末を得られる．その結果スマートフォン上での情報の識別性が高まり，ユーザビリティが増す．加えて，近年ディスプレイ端末の高性能化によって，従来にはなかった映像を用いたサービスが提供されている．例として次世代放送用の高解像度ディスプレイ向けサービスや，3D ディスプレイ用の立体的なコンテンツの提供がある．しかし，これらのサービスはディスプレイ端末側の機能に依存するため，専用のデバイスを所持していなければ利用することはできない．そこで，これらのようなディスプレイ端末が共用で使用できる環境があり，自分の持っている携帯端末と連携可能ならば，デバイスを所持していなくともそれらのサービスを利用することができる．

携帯端末とディスプレイ端末を接続する技術は，PAN[4] や PN[5] のようにさまざまなものが提案されている．しかし現状の方法で通信する場合，通信相手を検出し手動で設定する必要があるため煩雑であり，外出先などでの使用は難しい．ディスプレイ端末を使いたいとき，その場で簡単に接続できるシステムがあれば，携帯端末とディスプレイ端末の連携は容易に実現できる．また，ディスプレイ端末との連携においては，重要な個人情報を盗聴されないために，セキュリティも簡単さと同様に重要な要素である．

そこで本論文では，携帯端末のカメラで対象のディスプレイ端末を「覗き込む」ことによって，容易かつセキュアに外部ディスプレイ端末と連携できるシステム UDU を提案する．UDU では,「覗き込む」という直感的な操作により，使用するディスプレイ端末を指定し自動的にセキュアな通信を確立する．そのため，複雑な操作無しで携帯端末とディスプレイ端末の連携を実現できる．

†1 電気通信大学大学院情報システム学研究科
Graduatc School of Information Systems The University of Electro-Communications

以下に本論文の構成を示す．2 章では関連研究と本研究の課題について述べる．3 章では，本システムの概要を述べ，4 章では本システムの詳細について述べる．5 章では本システムの初期実装とその評価について述べ，6 章で結論とする．

2. 携帯端末とディスプレイ端末連携に向けて

2.1 関 連 研 究

近くにある機器同士で通信する技術としては，Personal Area Network(PAN)[4] がある．PAN は，ユーザの周辺にあるデバイス同士で通信を行うためのネットワークである．機器同士の通信には，Bluetooth や IrDA などの技術が利用されている．PAN の特徴は，近接したデバイス同士がケーブルで直接通信するように，一対一で情報を共有できることである．また PAN では，エリア内にあるデバイスの中から通信を行わないデバイスを選択でき，通信を拒否できる．これにより，PAN を構成しているデバイス以外との通信をユーザ側から遮断でき，PAN の範囲内にある関係のないデバイスによるネットワークへの不必要な干渉や無許可のアクセスを防ぐことができる．

この PAN を拡張した研究として，Personal Network(PN)[5] がある．PN は，自分の所有するデバイスが手元に無い場合でも，インターネットなどを通じて手元のデバイスと連携するシステムである．PN の種類には，Fednets[6] ，MAGNET[7] [8] などがある．MAGNET では,「Group Security Access」を用いてセキュリティを確保している．例えば，PAN を構成するあるデバイスが通信の暗号化に対応していない場合，そのデバイスを含む PN では暗号化した通信を行うことが出来ない.「Group Security Access」では，PAN の中心デバイスを決め，それを master デバイスとする．それ以外のデバイスは，master デバイスを通じてインターネットにアクセスする．master デバイスは，PAN を構成するデバイスの中からユーザ側で任意に設定できる．この master デバイスに暗号化に対応した機器を設定し，外部との通信を暗号化して行うことで，デバイス間の機能差によるセキュリティの問題を解決している．

2.2 技術的課題

携帯端末とディスプレイ端末を実現する上で重要なことは，容易なデバイス連携と，セキュリティを高い状態に確保することである．UDU は，利用シーンとして外出先などに設置されている公共のディスプレイ端末に接続することを想定しているが，この時容易にかつセキュアに接続できなければ利便性や秘匿性を損なうためである．2.1 節ではデバイスの接続方式として PN の概要を示したが，本稿の提案する利用シーンには適さないことが分かった．以下に課題となる点をまとめる．

まず，デバイス連携は容易にできなければならない．従来の方法では，外出先で携帯端末から目の前にあるディスプレイ端末を使用したい場合，設定が煩雑で，使いたいときに使えない．例えば MAGNET で通信する場合は，PAN の設定をすることと，master デバイス同士が通信するように設定することが必要がある．携帯端末とディスプレイ端末を連携するには，携帯端末と使用するディスプレイ端末をそれぞれを PAN の master デバイスに接続し，master デバイス同士が通信するように設定する必要がある．また登録したデバイスが多くなると，登録デバイスのリストから目当てのデバイスを探すのにも大きな労力がかかり，スケーラブルではない．つまり，携帯端末とディスプレイ端末の連携を考えると，ユーザの意思で簡単に接続できる直感的なシステムが必要である．

次にセキュリティについて考える．セキュリティで必要となるのは，個人情報などの重要な表示情報が流失しないために，携帯端末とディスプレイ端末間通信に秘匿性があることである．MAGNET では，先述のように「Group Security Access」によってデバイスの性能差によって生じるセキュリティの低下の対策をしており，インターネットを介した通信は VPN で暗号化している．しかし，この秘匿性が確保された通信を行うためには，PAN の master デバイスの設定と，master デバイス同士の通信を VPN で暗号化するという二重の設定が必要であり煩雑である．またパスコードなどの入力ミスなど，ユーザの操作ミスによりセキュリティが保たれない場合も考えられる．ユーザの操作を単純かつ直感的にすることで，セキュリティが低下する操作を排除することができる．

以上のように，UDU の利用シーンを考慮すると，使いたいときに目の前のディスプレイ端末を利用できるような連携手法と，複雑な操作なしに強固なセキュリティを確保できることが必要であるとわかった．

3. システム UDU

3.1 アイデア

本論文では,「覗き込み」を利用した直感的なリモートディスプレイアクセス方式 UDU を提案する．これは広く（Universal) ディスプレイを (Display) を使用する (Usage) システムとしてそれぞれの頭文字をとったものである．

3.2 節で述べたように，携帯端末とディスプレイ端末の連携を行うには，接続が容易に行えることと，セキュアなことが重要である．デバイス同士を接続する方法は既に存在するが，ユーザが望むような簡単にデバイス同士を接続するには煩雑な設定が必要で，容易に使用できない．例えば，Bluetooth で接続する場合，次のような手順が必要である．

(1) 接続する端末をペアリングモードにする
(2) 接続される側の機器でペアリング操作を行い，接続する端末を検索する
(3) 接続される側の機器上で，接続する端末を指定する
(4) 接続される側の機器上で，パスコードを入力し，接続を確認する

このように，デバイス同士の接続は多くの手順を必要とし煩雑である．また，特定の端末であれば一度の登録で使用できるが，複数台の端末を使用する場合には端末分の設定が必要となる．接続する端末が少ない場合はユーザの負担も小さいが，接続できるデバイスが多くなれば，目当てのデバイスを探すのにも大きな労力がかかってしまう．そこで，簡単に接続でき，かつユーザの意思を明確に示す方法として，携帯端末のカメラで対象のディスプレイ端末を「覗き込む」ことによって，容易かつセキュアに外部ディスプレイ端末と連携できるシステム UDU を提案する．UDU では，次の二つの手順で接続できる．

(1) ディスプレイ端末になんらかの識別子を表示しておく
(2) 携帯端末のカメラで「覗き込み」，識別子を得る

このように，UDU は従来の手法と比べて容易である．また，Bluetooth におけるパスコードのようなものを，ユーザが入力することなくセキュアに通信をおこなえる．

3.2 接続の容易さ

提案手法 UDU の利点は，使い方が直感的なことであること，使用状況が分かりやすいことの二点である．直感的な操作で接続することにより，ユーザはディスプレイ端末を使いたいときに容易に接続できる．

ディスプレイ端末の使用状況を考慮し，本稿では待ち受けモードと表示モードの二種類を用意する．待ち受けモードはディスプレイ端末が携帯端末の接続を待ち受けている状況で，ディスプレイ端末は接続のための識別子を表示しておく．表示モードは表示端末に携帯端末が接続している状況で，携帯端末の情報を表示する．この時待ち受けモード時に表示していた接続のための識別子は表示しない．そのため，複数携帯端末が同時にディスプレイ端末にアクセスすることはできない．この識別子をわかりやすいものに設定することで，ユーザは表示端末が現在使用中であるか否かを容易に判断することができる．

待ち受けモードのディスプレイ端末への携帯端末の接続は，端末のカメラを用いて接続したいディスプレイ端末を捉える動作を行うことで確立する．このカメラを用いた「覗き込み」を行うことで，接続したいディスプレイ端末を直感的に指定することができ，デバイス指定を間違えること無く使用できる．

3.3 セキュリティ

携帯端末とディスプレイ端末の連携では，容易さと同時にセキュリティが重要である．セキュリティでは，ディスプレイ端末と通信経路の二点を考慮する必要がある．

まずディスプレイ端末のセキュリティを考える．UDU で使用するためにディスプレイ端末側に求められる最低限必要な機能は，情報を表示する機能とネットワークに接続する機能である．この表示する情報のフォーマットを最も単純な画像フォーマットである BITMAP に限定することを考える．BITMAP はデータの圧縮解凍などの必要がないため，デコーダなどの特殊な処理を必要としない．そのため端末に余計なメモリ領域を用意する必要が無く，またデコーダのバグなどによる端末への不正侵入を防ぐことができる．このことから，本提案手法は単純なシステム構成であると同時に外部からの不正アクセスなどに対して強固である．また，ディスプレイ端末の同時接続による情報流出も考えられるが，これは 3.2 節で説明の通り，待受モードと表示モードの切り替えによって排除できる．

次に通信経路について考える．通信経路のセキュリティで問題となるのは，非正規のディスプレイ端末と通信してしまうこと，正規端末だが悪意あるユーザに占拠されたディスプレイ端末と通信してしまうことの二点である．まず，非正規のディスプレイ端末との通信防止を考える．UDU では，ディスプレイ端末の管理サーバを設置し，管理サーバで作成した秘密鍵と公開鍵を用いてディスプレイ端末の認証を行う．ディスプレイ端末はあらかじめ管理サーバから秘密鍵を受け取っておき，待ち受けモード時，画面上に認証局とディスプレイ端末自身の IP アドレスを表示する．携帯端末側は管理サーバに接続し，読み込んだディスプレイ端末の IP に対応する公開鍵を得て，ディスプレイ端末と鍵交換方式による認証を行う．この認証を行うことで，ディスプレイ端末が管理サーバによって認められた正規の端末であることが判別できる．次に悪意あるユーザに占拠された正規端末との通信を考える．ディスプレイ端末に表示する情報が固定である場合，情報は悪意あるユーザによって複製される可能性がある．鍵交換認証により，使用したディスプレイ端末が正規端末であるかどうかは判別できる．しかし，悪意あるユーザは，占拠した端末の接続情報を複製して他端末に表示することできる．これによって，接続者は期待したディスプレイ端末と異なる端末に接続し，

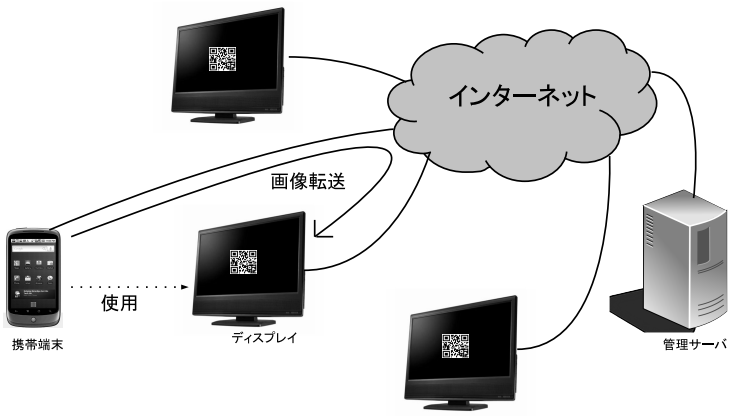

図 1 UDU の構成図

通信内容を盗聴されてしまう．UDU では，悪意あるユーザに占拠された正規端末との通信を防ぐために，待受モードのデバイスの画面に表示する情報に，一定時間で変化する値を付与する．このことで表示している情報に鮮度を加えることができ，情報のコピーを難しくし，正規端末の成りすましを防止する．また，通信を開始する直前にディスプレイ端末側に通信の開始を通知する画面を一定時間表示し，使用するディスプレイ端末をユーザ自身が確認できるようにする．このようにすれば，意図したディスプレイ端末に確認画面が表示されない場合，ユーザ側が直接通信を切断することで，意図しないディスプレイ端末との通信を防止できる．

4. システムの詳細

4.1 システム構成

3.1 節で述べたシステム UDU の詳細を説明する．**図 1** に UDU の構成図を示す． UDU は，ディスプレイ端末とディスプレイ端末の管理サーバで構成される．また，各々のデバイスと管理サーバはインターネットで接続されている．ディスプレイ端末は，接続に必要な情報を識別子にして画面上に表示する．携帯端末は，接続したいディスプレイ端末を「覗き込む」ことで接続相手を指定し，識別子を取得することで接続のための情報を得る.「覗き込む」ことによるディスプレイ端末の指定と識別子を捉える動作には，携帯端末のカメラ機能を用いる．カメラ機能は携帯端末に標準的に内蔵されているため，特殊な機材などを用意する必要はない．またディスプレイ端末と携帯端末間の通信を保護するために，暗号復号化のための資源が必要である．しかし最近の携帯端末には，暗号復号化に十分な計算資源を有しているため，特殊な機材は必要ない．

管理用サーバは，携帯端末と表示デバイスが接続する際に，表示デバイスが正規の端末であることを認証するための認証局の役割をする．管理用サーバから，ディスプレイ端末に秘密鍵，携帯端末に公開鍵を渡すことで携帯端末と表示デバイスの公開鍵認証を行う．これによりディスプレイ端末が正規の端末であるか否かを判断できる．表示デバイスは様々な場所に置かれることを想定しているが，それぞれ設置した人だけが正規の端末であることを判断できる．そのため，管理サーバはディスプレイ端末を設置した人ないし団体単位で設置する．管理サーバにディスプレイ端末を設置した人が鍵を設定することにより，他のディスプレイユーザもディスプレイが正規端末であることを判断できる．

4.2 接　　続

帯端末ディスプレイ端末の接続手順を**図 2** に示す．各手順については以下に述べる．

(1) 管理用サーバから，ディスプレイ端末に予め秘密鍵を渡す
(2) 待ち受けモードのディスプレイ端末が，画面上に接続のための識別子を表示する
(3) 携帯端末のユーザは，接続したいディスプレイ端末が待ち受けモードになっていることを確認し，ディスプレイ端末に表示されている識別子を携帯端末のカメラで読み取る
(4) 携帯端末がカメラで読み取った識別子に含まれている管理サーバの IP アドレスを使い管理用サーバに接続する
(5) 携帯端末が，管理用サーバから接続したい表示ディスプレイ端末の持つ秘密鍵と対応する公開鍵を取得する
(6) 携帯端末から公開鍵を使い，表示端末の鍵交換認証を行う
(7) ディスプレイ端末の認証後，携帯端末とディスプレイ端末間で通信を行う

これら手順で，実際にユーザが行う作業は，(3) の接続したいディスプレイ端末が表示している識別子を携帯端末のカメラで読み取るだけである．その他の手順は，得られた識別子の情報を用いることで自動的に行われる．そのため，人間の操作ミスなどに起因する情報漏えいなどの心配がなく，高いセキュリティ性能を有することができる．

ユーザがこのディスプレイ端末を使い終わり，接続を切断するか，通信中にユーザが他のディスプレイ端末を覗き込んだ場合は通信路を切断する．通信が切断されると，通信してい

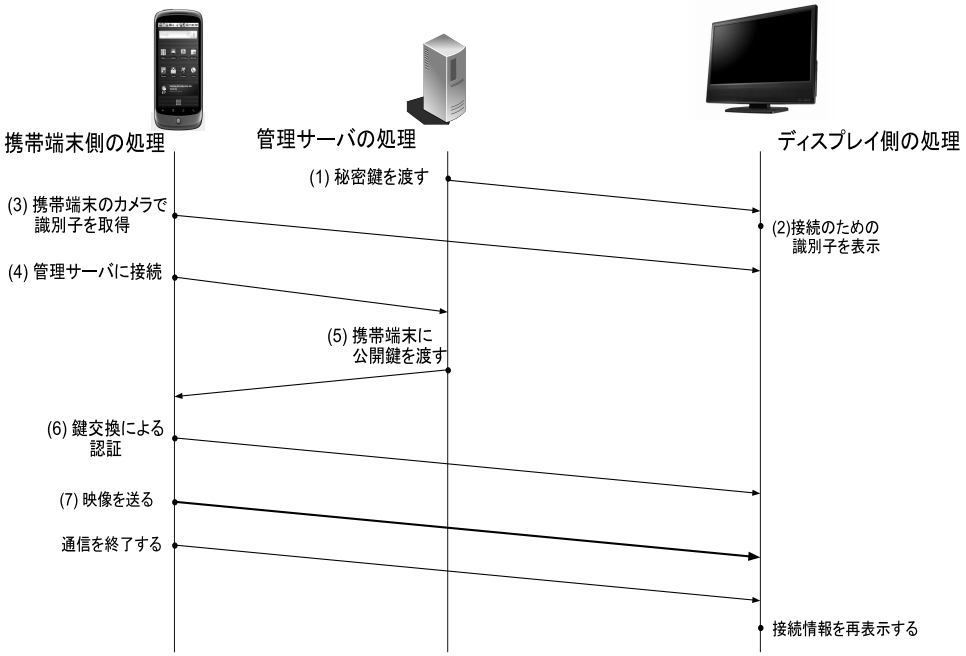

図 2 システムの接続手順

たディスプレイ端末は待ち受けモードに戻る．

4.3 識 別 子

ディスプレイ端末の画面上に表示する接続に必要な識別子は，識別子であることを人間が容易に判断できること，携帯端末のカメラで撮影する程度で解析可能であること，接続に必要な情報を詰め込むのに十分な容量があることが求められる．識別子であることが人間によって容易に判断できることで，UDU の待ち受けモードと表示モードどちらの状況にあるかが容易に判断可能になる．したがって，ディスプレイ端末を利用したいユーザに使用可能か否かを容易に知らせることができる．また，携帯端末のカメラの性能は機種に依存するため，どのようなカメラで読み取っても解析可能である識別子が必要である．加えて，どのような識別子であっても，接続情報を埋め込むのに十分な容量がなければならない．この条件

図 3 ランダムキーを入れたコードの生成

に適する識別子として，光学式マークがある．光学式マークはバーコードなどの総称で，識別子をカメラなど光学式マーク読取装置を用いて読み取ることで情報を得ることができる．これらはカメラの性能差に依存して読み取り精度が低下しないよう工夫がされている．また識別子として一般的に普及しているため，人間が容易に識別子と判断できる．このため，光学式マークは提案手法 UDU における識別子の用途として十分な性能を有しているといえる．

識別子には，ディスプレイ端末への接続に必要な情報を埋め込む．UDU では，ディスプレイ端末の IP アドレス，管理サーバの IP アドレス，時間などに起因して変化するランダムなキーを埋め込む．これら情報は光学式マークに埋め込み可能な情報量である．また，IP アドレスなどを識別子に埋め込むことで，人間の目による読み取りを難しくする．このことで識別子自体を盗むことを難しくしている．ランダムなキーはディスプレイ端末が生成し，一定時間などに起因して変化するようにする．そのため，万一識別子が何らかの手法で複写されてしまった場合でも，識別子に含まれるキーと現在ディスプレイ端末が有しているキーを比較することで有効な識別子か否かを判断することができる．画面に表示する識別子の例を**図 3** に示す．

4.4 管理用サーバ

UDU では，表示端末の認証のために管理用サーバを設置する．ディスプレイ端末の管理にサーバー使用する理由は，セキュリティの向上である．前述のように，携帯端末とディスプレイ端末の通信では，ディスプレイ端末が正規端末と証明できることが必要である．この管理サーバでは，秘密鍵と公開鍵のペアを生成する．この生成した秘密鍵を，ディスプレイ端末を設置するときに秘密鍵を渡す．この秘密鍵をもっていることが，正規端末の証明とな

る．ディスプレイ端末側は，管理用サーバの IP アドレス，ディスプレイ端末自身の IP アドレス，時間変化するランダムキーを光学的マーク認識に変換して表示する．携帯端末は，表示された管理用サーバの IP アドレスに接続し，公開鍵を取得する．その公開鍵を用いて鍵交換認証をディスプレイ端末と行い，正規端末であるか判断する．このように管理サーバを設置することで，ディスプレイ端末が正規端末であると証明できる．

5. 性能評価

5.1 初期実装

提案するシステムの初期実装について述べる．この初期実装では，ディスプレイ端末にノート PC を使用し，ノート PC の画面上に通信に必要な識別子を表示させ，携帯端末側のカメラで識別子を読み込むだけで通信できるシステムを実装した．この初期実装では，携帯端末の画面を画像データとしてディスプレイ端末に送信することを想定し，画像を送信した際の経過時間，暗号化を行った際の通信時間の変化，識別子をカメラで読み込むだけで通信を行えるかを評価した．通信する画像データは，どのディスプレイ端末でも使用できるように BITMAP を使用した．実験環境は表 1 にまとめる．

まず，ディスプレイ端末の画面上にノート PC の IP アドレスを含む識別子を表示させる．この識別子は QR コードとした．次に，表示された QR コードを携帯端末のカメラを使い読み取る．読み取った IP アドレスを使用し，携帯端末からディスプレイ端末側に接続して通信を行う．この通信で，携帯端末内の画像をディスプレイ端末側に送信する．その様子を**図 4**，**図 5** に載せる．図 4 は待ち受けモードで，図 5 は接続モードの様子である．図 4，図 5 では，携帯端末の画面を送信ために，VNC サーバソフト droid vnc[2] を使用した．**図 6** に通信比較の概要図を載せる．

表 1 実験環境

使用携帯端末	Nexous One
携帯端末の CPU	Qualcomm QSD8250 Snapdragon 1GHz
携帯端末の Memory	512MB
携帯端末のカメラの画素値	500 万画素
SSH クライアントソフト	Connect bot
SSH サーバソフト	freeSSHd1.2.6
通信環境	Wi-fi IEEE802.11g 54Mbps

図 4 待ち受けモード

5.2 評　　価

- 「覗き込み」を利用した携帯端末からディスプレイ端末通信

本実装では，「覗き込む」だけで携帯端末からディスプレイ端末に画像を送信することができた．携帯端末側は，ディスプレイ端末に表示されたコードをカメラで認識するだけで接続を確立できている．ディスプレイ端末画面の QR コードの認証は，QR コードの大きさが一辺 20(cm)，携帯端末のカメラ画素が 500 万画素，室内の環境下で表示端末から約 1.5m の距離まで行えた．また，複数のディスプレイ端末を置いた場合，QR コードを読み込むだけでシームレスにディスプレイ端末を切り替えることができた．

- 画像データ送信の経過時間

表 2 暗号化の有無による通信時間の比較

転送画像の解像度 (pixel)	転送画像のサイズ (MB)	暗号化無しの転送時間 (ms)	暗号化した転送時間 (ms)
800 × 480	1.09	1064	1729
1024 × 1080	3.75	3165	4943
1920 × 1080	7.91	6806	10355

図 5 表示モード

表 2 に通信時間の測定結果を載せる．本実装では，送信する画像は BITMAP 形式で送り，解像度が 800 × 480，1280 × 1024，1920 × 1080 の三種類の画像を使用した．この解像度は，スマートフォンの画面，17〜19 インチディスプレイの解像度，フル HD の規格，にそれぞれ対応している．各画像について，計 5 回送信に要した時間を計測しその平均を送信時間とした．通信時間の測定には java の timer 関数を用いた．結果，スマートフォンの画面サイズである 800 × 480 の場合は 1 秒で送信できた．また，フル HD 規格の 1920 × 1080 のサイズの場合は 6 秒で送信できている．この結果から，携帯端末内のデータを大きな画面で確認したい場合など，簡単かつ短時間でディスプレイ端末で表示できる．例えば，携帯端末のカメラで撮影した高解像度の写真を，その場で大きなディスプレイで観賞したい場合には，UDU を使用すれば使いたいディスプレイ端末の識別子をカメラで写すだけで，その写真を観賞できる．よって，現時点の無線環境でも静止画の観賞といった用途には十分使用できる．

- 暗号化による通信時間の変化

暗号化を行った場合の通信時間の変化を見る．本実装では，暗号化を行った際の通信速度を見るために，SSH 通信で暗号化を行い画像をノート PC 側に送信し，暗号化した場合としていない場合の画像送信にかかる時間を測定した．暗号化は，android 端末側に SSH クライアントソフト Connect Bot[1] を使い，ノート PC 側には SSH サーバとして Free SSH[3] を使用し，SSH 通信を行った後で port forwarding 用いてソケット通信を行うことで暗号化し，BITMAP 画像を送信した．その結果，表 2 より 1.5 倍程度通信時間が増加した．この場合でも，800 × 480 の画像を 2 秒で送信できており，暗号化して通信しても十分使用できる．

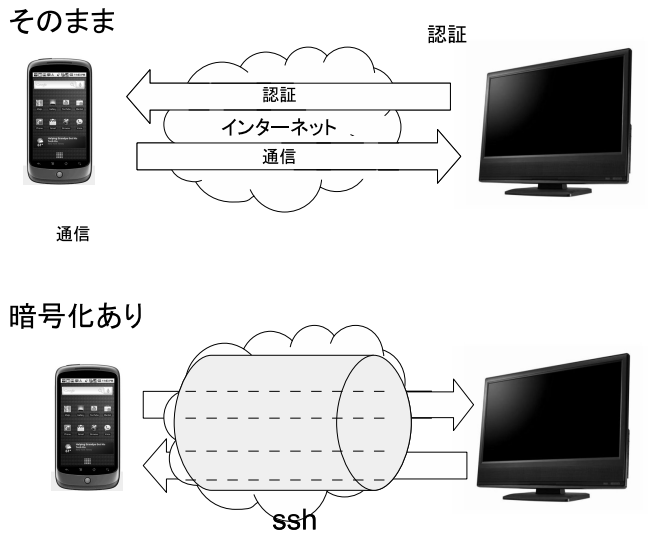

図 6 通信時間比較実験の概略図

5.3 動画像に関する考察

表 2 より，現時点の実装でも静止画の観賞は十分に行えるとわかったが，この環境で動画を転送した場合を考える．5.1 節で行った実装から得られた送信画像のサイズとフレームレートで表したグラフを図にのせる． 表 2 の画像サイズと転送時間を用いてフレームレートを計算すると，**図 7** のようになる．解像度 800 × 480 の画像サイズは 1.09(MB) で，このときのフレームレートは 0.9(fps) であった．例えば，テレビ放送の場合はフレームレート 30(fps) なので，リアルタイムでテレビ放送なみのフレームレートには足りていない．本実装で使用した無線環境の理論値 54Mbps でデータを送信できたとしても，フレームレー

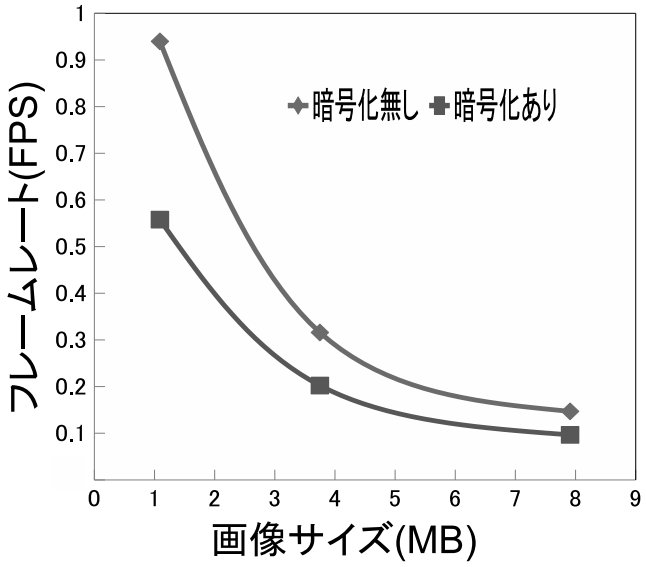

図 7 転送サイズとフレームレートの比較

トは 6.2(fps) なので，現時点での動画転送のボトルネックは通信帯域のバンド幅と考える．しかし，今後高速な無線環境が普及すれば動画の転送も十分可能である．次に，暗号化による通信時間増加について，常時暗号化による通信を行うのではなく，個人情報が含まれる重要な通信の際のみ暗号化で通信を行えばよい．つまり，重要度の高くない通信は暗号化を行わないなど，場面によって暗号化の on/off をシステム側が自動で切り替えるシステムの実装を行えばよい．このような実装にすれば，暗号化する必要の無い通信はそのまま通信することで，すべての通信内容を暗号化する場合と比べて，暗号化による通信時間の遅延の影響を減らすことができ，かつ重要な情報の流失を防ぐことができる．

6. ま と め

本論文では，携帯端末のカメラを利用し,「覗き込む」ことによって携帯端末とディスプレイ端末を連携するシステム UDU を提案した．このシステムでは，カメラで対象を写すだけで通信し画像の表示を行うことで，直感的で簡単に携帯端末とディスプレイ端末を実現できる．携帯端末とディスプレイ端末間通信のセキュリティは，直接 BITMAP イメージを受け取ること，ディスプレイ端末が正規のものであるとを認証できること，確認画面を表示しユーザ自身が確認すること，携帯端末とディスプレイ端末間通信を暗号化することの四点で枠組みを示した．システムの初期実装では，ディスプレイ端末上の QR コードを携帯端末のカメラで「覗き込む」だけで，ディスプレイ端末との通信が確立できた．さらに複数のディスプレイ端末をシームレスに切り替えることができた．今後の課題は，通信の方式などを最適化することによって，リアルタイムに動画の転送を行えるシステムにすることである．

参 考 文 献

1) *Connect bot.* https://market.android.com/details?id=org.connectbothl=ja.
2) *droid vnc.* https://market.android.com/details?id=org.onaips.vnchl=ja.
3) *freeSSHd.* http://www.freesshd.com/.
4) *IEEE 802.15.* http://www.ieee.org.
5) *Personal Networks: An Overlay Network of Wireless Personal Area Networks and 3G Networks*, july 2006.
6) *Reputation-Based Service Management and Reward Mechanisms in Fednets to Improve the Quality of Cooperation between Personal Networks*, june 2010.
7) M.Bauer, R.L. Olsen, M.Jacobsson, L.Sanchez, J.Lanza, M.Imine, and N.Prasad. Context management framework for magnet beyond, 2006.
8) DCalin, ARMcGee, UChandrashekhar, and RPrasad. MAGNET: An approach for secure personal networking in beyond 3G wireless networks. *BELL LABS TECHNICAL JOURNAL*, Vol.11, No.1, pp. 79–98, SPR 2006.