自己防犯システムの開発

都築　佳生† 村田　嘉利† 佐藤　文明‡　水野　忠則‡

E-mail: † yoshio@docomo-tokai.co.jp, ymurata@docomo-tokai.co.jp,
‡ sato@cs.info.shizuoka.ac.jp, mizuno@mizulab.net

あらまし　警察庁の統計によると 2002 年1～5 月における重要窃盗犯の件数は 20 万件に迫ろうとしており、年々増加傾向にある。その一方で検挙件数は低下傾向にある。窃盗犯やストーカに対抗するため、一人暮らしの女性を中心にビデオカメラ付きインターフォンを利用して帰宅前に訪問者を確認したい等の自己防犯システムへの要求が強まっている。ビデオインターフォンとｉモード端末とをサーバを介して接続した上で、ビデオカメラ付きインターフォンと PHS を組み合わせた CTI 技術の適用により、高セキュリティーを確保しつつリモート通話、自宅周辺の映像モニタリングおよび施錠状況等の遠隔確認を可能とする防犯システムを開発したので報告する。

Development of the Residential Self-Security System

Yoshitoshi Murata†, Yoshio Tsuduki†, Fumiaki Sato‡ and Tadanori Mizuno‡

Abstract; According to the National Police Agency's statistics, the number of serious thefts is increasing each year and nearly 200,000 thefts occurred between January and May 2002. On the other hand, the number of arrests is decreasing. A demand for the residential self-security system such as interphones with video cameras that verify visitors to a residence before returning home is increasing especially among women who live alone to protect themselves from thieves and stalkers.

This report describes the development of the residential self-security system that enables remote communication, image monitoring around homes, and a remote verification of windows/doors locked to ensure high security. This system utilizes CTI technology that combines a video interphone and PHS by connecting video interphones and IP mobile phones (DoCoMo's i-mode terminals, etc.) through servers.

1. はじめに

警視庁の統計によると 2002 年1～5 月までの侵入盗、自動車盗、ひったくりといった重要犯罪件数は、20 万件に迫ろうとしており、5 年前に比べて５０％近い増加となっている[1]。その一方、その検挙件数は 5 万件弱であり、年々減少している。ストーカ犯罪も社会問題化しており、2000 年 5 月にはストーカ規正法が成立した。これらの犯罪に対処方法するため、警備保障会社への依頼の他、外出時における訪問者を確認した上でのモバイル通話、不審者が近づいたことの状況確認、施錠状況の遠隔確認および施錠実施、等といった自己防犯システムへの要望が強まっている。

これらの要望に応えるため、インターネットビデオカメラが複数の会社から発売されており、インターネット経由で映像モニター可能となっている。また、松下通信工業からモバイル通話および施錠状況等のモバイルセンサー監視可能なビデオインターフォン[2]が発売されている。これらの装置の多くが、カメラやインターフォンの親機がサーバとなっており、認証 ID とパスワードで外部からアクセス可能である。これは第三者も容易にアクセス可能であることを意味し、犯罪を助長することになりかねない。

筆者らは、これまでセンサー監視に対するＡＳＰとしてサービス提供するモバイルリモート監視システムを開発した[3]。本システムでは、センサーデータの情報量が少ないことから、データロガーとセンターサーバ間の通信回線として、セキュリティーに優れた無線パケットシステム（DoCoMo PDC-Packet）を適用した[4]。しかしながら、画像モニタリングでは取り扱うデータが画像データと非常に多い

†株式会社ＮＴＴドコモ東海
‡静岡大学

ことから、セキュリティー的には弱いが伝送情報量当たりの通信料金が安価なＡＤＳＬ等のインターネットを使うことが望ましい。

今回、ビデオインターフォンをビデオモニタリングのクライアント端末の位置付けとし、全ての情報をサーバ上に蓄積した上で、ｉモード等のIP携帯電話からサーバにアクセスすると共に、クライアント端末にＰＨＳを組み込み発信者番号を利用することにより、非常に高いセキュリティーを確立した防犯システムを開発したので、その主要技術とシステム構成を紹介する。第 2 章では自己防犯システムに要求される機能を整理する。第 3 章ではセキュリティーやリモートコントロールの実現方式について提案する。それに基づいて開発した自己防犯システムの構成を第 4 章で紹介する。また、そのシステムの基本データを第 5 章で紹介する。

2. 自己防犯システムに求められる機能

自己防犯システムへの要望を整理すると、

- 施錠状況やガス器具の消火状況を外出先において確認したい。施錠し忘れが見つかればその場で施錠や消火をしたい。
- 鍵ではなく、携帯電話で鍵の施錠／開錠を実施したい。(鍵穴のない鍵)
- 帰宅前に訪ねてきた人の確認や自宅周辺に不審者がいないか確認したい。
- 訪問者があった場合に、外出時においても相手の顔を見た上で話をしたい。
- 外出時に何らかのトラブルが発生した場合には、緊急連絡して欲しい。
- 防犯ではないが、要介護者やペットを自宅に残してきた場合、外出先から状況をビデオモニタリングしたい。

に集約されると考えられる。それらの要望に応える機能としては、

- 異常 (不審者侵入、自動車への危害、火災、等) 検知時の警報音の発出とアラームのリモート通知
- 屋内外の画像モニタリング
- 扉や窓の施錠状況、ガス器具等の消火状況のリモートモニタリングとリモートコントロール
- 相手の顔を確認した上でのリモート通話

がある。更にシステムとして提供するためには、それらに加えて、

- システムへの第3者による侵入禁止
- アラームの送出先の切り替え、モニタリング画像の選択等の各種設定および変更をリモート環境から実施

できるようにする必要がある。

3. 主要技術

3.1 リモート通話におけるセキュリティー技術

相手の顔を確認した上でのリモート通話を実現するためには、

Step1；ビデオインターフォン子機のボタンが押下されたことをトリガーにビデオ画像あるいは静止画像を撮影

Step2；上記撮影データをビデオインターフォンの親機からテレビ電話機能付き携帯電話あるいは静止画表示機能付き携帯電話に送信

Step3；送信されてきた画像を見た上で通話モードに移行

という手順を短時間に実施する必要がある。通話に至るまでに何十秒もかかるようでは、訪問者は不在とみなして立ち去ってしまう。現在市販されているテレビ電話機能付き携帯電話としてドコモの FOMA 端末があるが、FOMA 端末間でのテレビ電話に限られている上に発信してから TV 電話できるようになるまでに３０秒程度かかり、サービス提供条件を満足しない。また、静止画の場合では、ビデオインターフォンのカメラで取得した映像を WWW サーバにアップロードし、それに携帯電話からアクセスにいくことにより訪問者を確認することになる。この場合、訪問者を確認後、ビデオインターフォン親機に再接続する必要があり、数十秒以内に接続することは困難といえる。

それ故、今回は相手の顔を確認した上でのリモート通話の実現は見送り、インターフォンのボタン押下の後、即、携帯電話を呼び出す構成とした。実現に当たっては、図1のようにビデオインターフォンの親機に PHS を取り付け、携帯電話を呼び出す構成とした。

その際、顔によって相手を確認することなく、通話モードに移行することから、以下の要件を満足する必要がある。

- 通常の電話機からの着信と間違えて不用意な応答を避けるため、ビデオインターフォンからの呼び出しであることを事前に認識できる。
- 話中あるいは圏外が電源断時のトーキが流れることによる外出中であることを認識されないようにする。

その実現のため、今回は、ビデオインターフォン子機のボタンが押下されたことに伴い、

Step1;ビデオインターフォン子機と PHS 間の通話路を保留する。

Step2;携帯電話を呼び出す。

Step3;携帯ユーザの応答に対して、ビデオインターフォンの親機からの呼び出しである旨のトーキを流す。

Step4;ビデオインターフォンからの呼び出しであることを認識した上で、“＃”ボタン（他のキーでも良い）なりを押下する。

Step5;ビデオインターフォン子機と PHS 間の通話路を接続

の手順により、高いセキュリティーを保ちながらリモート通話可能とした。TV電話の接続処理時間が短縮された場合においても、相手も顔を確認した上で通話路を接続する必要がある。

3.2 画像リモートモニタリングにおけるセキュリティー技術

インターネット上における第三者の侵入を防ぐセキュリティー技術としては、Firewall や VPN が一般的である。これらの技術は LAN に対する侵入を防止するものであり、単体として設置されたインターネットカメラやインターフォンシステムに適用するには高価であり、適用困難といえる。

セキュリティーの問題を引き起こす大きな原因の1つが、インターネットカメラやインターフォンシステムをサーバにインターネット上におけるサーバに位置付けることである。常時インターネットに接続されており、クライアント端末からアクセスする構成では、第三者からの侵入を容易にする。

一方、インターネットカメラやインターフォンシステムをクライアント端末と位置付けることにより常時IPアドレスを持っているのではなく、必要時のみインターネットに接続することにより、第三者による侵入機会を大幅に低減可能となる。今回のシステムでは、リモート通話機能を実現するために PHS を搭載していることから、発IDを利用したCTI技術と一時蓄積サーバを組み合わせることにより実現した。

訪問者がビデオインターフォン子機のボタンを押下した場合、リモート通話した後、通話中に撮影した画像情報をサーバにアクセスし、一時蓄積する。サーバは、新規データが蓄積されたことをメール形式でIP携帯電話に通知する。連絡を受けたユーザはサーバにアクセスし、Webベースで画像情報を見る。

ユーザサイドからリモート画像端末にアクセスする場合、まず、サーバにアクセスし、携帯上の操作画面を利用しておこなう。指示を受けたサーバは、PHSに電話をかけ発IDを送った後、切断する。起動指示を受けたリモート画像端末はサーバにアクセスし、画像情報をサーバに転送する。

サーバに対するインターネットからの侵入に対しては、既存技術である Firewall およびSSLで対応する。

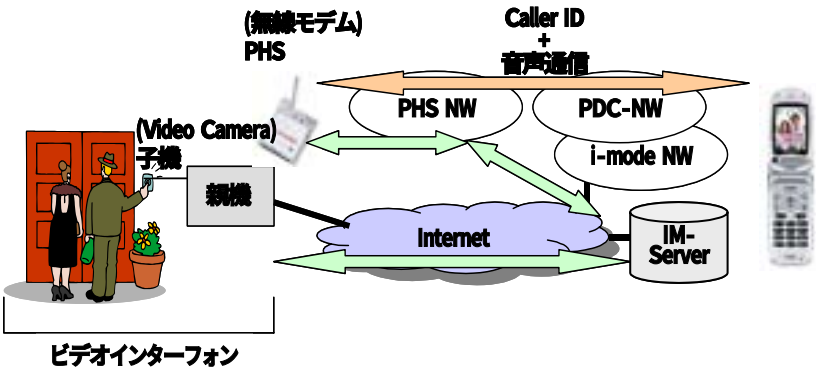

図 1. ビデオインターフォンを利用した自己防犯システム

3.3 リモートコントロール技術

従来のホームテレメトリーでは、電話のPB信号の組み合わせを利用するものがほとんどであった。

しかしながら、この構成では管理装置に専用の電話回線を用意すると共に音声応答機能を搭載する必要があった。また、操作的にも音声による指示とダイヤルキーの押下であることから、操作性に優れていると言いがたい。また、四国電力のOpenPlanetのようにJavaを利用したものも出てきている[5]。

今回は、モニタリング端末としてブラウザを搭載したIP携帯電話を利用した。インターホン親機にJVMを搭載することが困難であったことから、リモート端末～サーバ間、サーバ～モニタリング端末間共にWebインタフェースのみを実装し、リモート端末側に実行させたいＵＲＬ(=CGIプログラムのパス)をサーバからリモート端末に転送することによりＯＳに依存することなくリモートコントロールを実現する方式を考案した。具体的なシーケンスは、図2に示すようにIP携帯電話からサーバにアクセスし、最新画像情報の転送指示等をブラウザ画面から行う(①)。その指示を受けたサーバはインターホン親機に装着されているＰＨＳに対して電話をかけることにより発IDを送信した後、発信を中止する(②)。ＰＨＳ経由で受け付け許可した発IDを受信したビデオインターフォン親機はインターネットアクセス回線あるいはＰＨＳ回線を利用してサーバとの間にセッションを確立し(③)、サーバからの要求が何であるのかを知るために、HTTP要求でサーバへ問合せを行う(④)。問合せを受けたサーバはインターホンが実行すべき画像アップロード用のＵＲＬをHTTP応答で送信する(⑤)。インターホン親機は、受け取ったＵＲＬに適切な引数(送信する画像ファイル名など)を付加した上で、サーバへアクセスすることにより所定の処理(画像情報の転送や設定値の変更、等)を実現する(⑥)。

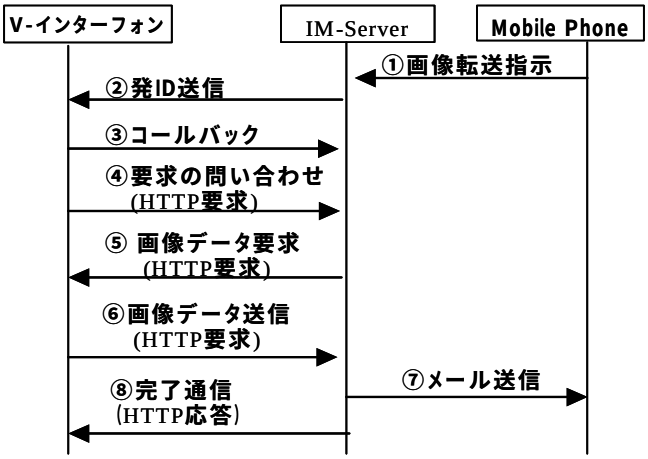

図2. リモートコントロール制御方式

4. システム概要

業務用機器に対するリモートセンサー監視を主目的とするモバイルリモートモニタリングシステムとは異なり、自己防犯システムは個人用途を中心とする構成とする必要がある。センターサーバは、監視端末としてビデオインターフォンだけでなく監視カメラにも対応できるように設計した。

4.1 オブジェクト管理モデル

筆者らは、センサー監視システムについては、クライアント／データロガー／デバイス／センサーの各レイヤーから成る4階層オブジェクト管理モデルが適していることを述べた[3]。

自己防犯システムでは、センサーとしてドアの施錠状態表示センサーや各種機器のＯＮ／ＯＦＦ表示センサーに加えてビデオカメラが加わる点を除けば、違いはない。デバイスレイヤーについては、一戸建てでは不要かもしれないが、工場等の監視の場合、系統別に複数のカメラやセンサーが設置することが想定され、有用である。データロガー層については、センサー監視システムと何ら変わることはない。クライアント層については、サーバへのアクセス件の管理が中心であることから、アクセス者が企業の保守監視者ではなく、個人や個人事業者になるが、クライアント層の機能は必要である。

以上のことから、自己防犯システムにおいてもモバイルリモート監視システムと同じく4階層オブジェクト管理モデルを採用した。

4.2 ノード構成

自己防犯システムでは、監視者は企業のシステム保守担当者より個人が圧倒的に多い。それ故、システム構成としては図3に示すように

- リモート端末;ビデオインターフォン
- 画像監視センター(Image Monitoring Center; IM Center)
- モニタリング端末(Monitoring Terminal);業務用と個人用で2種類の監視端末を用意。

- PC ベース
- IP携帯電話ベース

の大きく 3 つのノードから構成する。ビデオインターフォンは、

- 親機;画像データの一時蓄積メモリ、各種センサーとの接続ポートおよびＰＨＳの接続インタフェースを有する。
- 子機 (カメラ付き)

から構成する。機能としては、

- サーバに対する各種設定操作
  - 通話転送先
  - メール送信先
  - センサーの異常判定の設定
- 通話転送時、子機のボタン押下に応じて、ＰＨＳを利用して転送先に電話発信
- 上記と平行して、子機のカメラを利用して所定の要領に従って写真を撮影
- 撮影したビデオデータを IM Center に転送
- 接続ポートが異常感知した場合のメール送信

である。

IM Center は、

- アプリケーションサーバ
- WWW／ＳＭＴＰサーバ
- アドミニストレーション端末

から構成する。機能としては、

- 画像データの一次蓄積;リモート端末からのビデオデータをサムネイル形式に変換･保存後、保守監視者等にアラーム信号を携帯メールで保守者に周知
- ユーザ登録／解除;接続するシステムの構成、リモート等にデータ変換し一時蓄積
- アラーム通知;アラーム情報を受信した場合、あるいは受信データの閾値が特定の値を超えた場合端末に接続されたＰＨＳの電話番号、転送先電話番号、転送先メールアドレス、モニタリング端末、等の登録
- モニタリング端末に対する操作インタフェース (cgi) の提供
- リモート端末に接続されたＰＨＳへの発信制御
- オペレーション操作インタフェースの提供

4.3 通信プロトコル

リモート端末と IM Center 間は、物理回線としてＰＨＳ電話回線とインターネットアクセス回線の 2 系統を用意した。但し、ＡＤＳＬ回線を引けないことを考慮し、画像伝送を含めた全ての機能をＰＨＳのみでも実現可能としている。IM CEnter とモニタリング端末間は、モバイルインターネット回線 (ドコモの場合は、i モードシステム) を利用した。セッションの確立･維持については、標準的なプロトコルである TCP/IP および HTTP を利用した。

各ノード間の通信プロトコルを図4に示す。

5. システムデータ

5.1 通話転送遅延特性

インターフォン子機のボタンを押下された後、ＰＨ

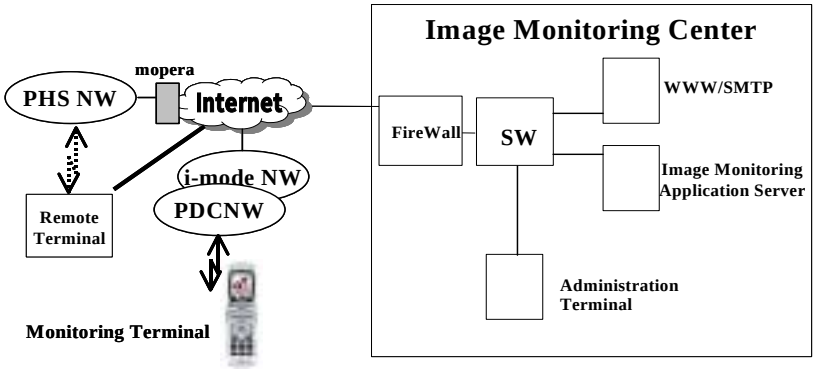

図3．自己防犯ステムの構成

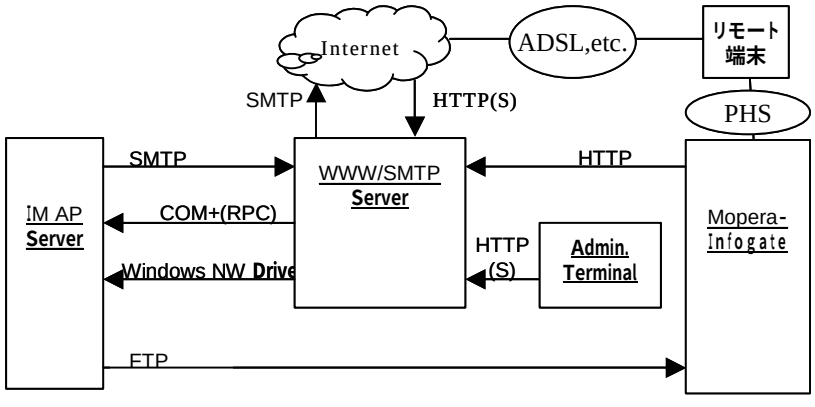

図4．通信プロトコル

Sを起動して携帯電話を呼び出すまでの時間を測定した。その分布を図5に示す。ほぼ 10 秒以内でIP携帯電話のリンギングが始まっており、インターホンからの着信である旨のトーキを確認しても 15 秒程度で応答可能なことから、使用上の問題点はないと判断できる。

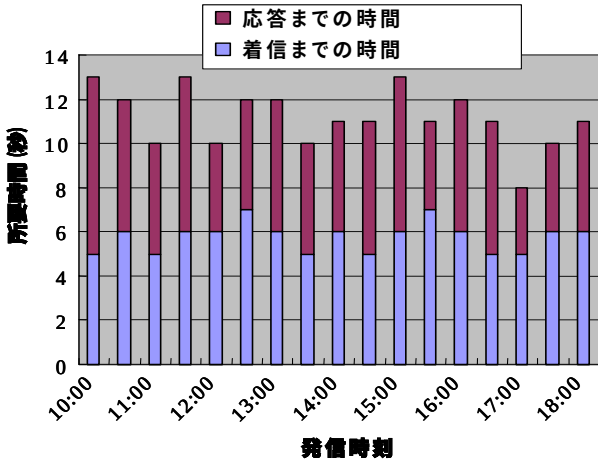

図5. 子機ボタン押下からの着信時間特性

5.2 画像伝送完了時間特性

実際のサービスでは、インターホン子機のボタン押下後、1, 5, 9, 13 秒のタイミングで計 4 枚の写真をとり、一時蓄積した上で、サーバに送信する。送信される画像データは、画像サイズが 640×480 ドット、ファイルサイズが 25KB 前後の JPEG ファイルである。

画像データを受信するとサーバは、IP携帯電話のディスプレイへの通常表示やサムネイル表示に最適な画像サイズとファイルサイズに画像データを変換する。また画像形式も JPEG 以外に GIF 形式の生成も行う。これらの変換作業が完了すると、サーバは画像受信完了メールをIP携帯電話にメールする。写真を撮影後、画像受信通知メールを送るまでの時間を測定した。その結果を図6に示す。インターネット経由のアクセス回線としては NTT 西日本のフレッツ ISDN の 64kbps 回線、プロバイダとしては NTT コミュニケーションズの OCN ダイヤルアクセス「フラットプラン」を利用した。ISDN-64 の利用でも十数秒で画像伝送が完了しており、ADSLを利用すれば数秒で画像伝送完了すると想定され、より快適に利用可能になると考えられる。

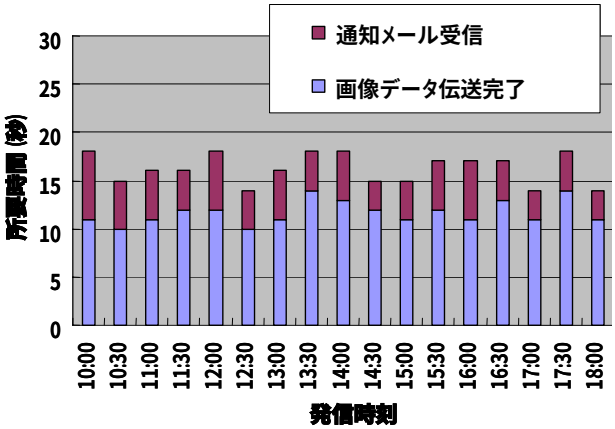

図6. 画像伝送時間特性 (ISDN回線時)

6. まとめ

今回、自己防犯システムの必要性とシステムに求められる機能の提唱を行い、その一例としてビデオインターフォンをクライアント端末とし、PHS を組み込むことにより高いセキュリティー性を確立した防犯システムの紹介を行った。また、システムの応答時間を測定し、実用レベルに達していることの検証も行った。

代表的なインターフォン機器メーカであるアイホン社と、今回のシステムを使った市場調査を共同で行ったところ、ユーザはリモートコミュニケーション機能よりもセキュリティー機能に対する関心を強く持っていることが判明した。今後は今回のシステムをベースに PHS を使わず、より低コストでセキュリティー機能を拡充したシステムの開発を進めていきたいと考えている。

参考文献

[1] http://www.npa.go.jp/police_j.htm

[2]http://www.ipa.go.jp/NBP/ITX2001-1/result/katei/katei.htm

[3] Murata, “Design Scheme of Shared Mobile Remote Monitoring System”ACIS, 2002, pp.115-121

[4] 大貫, “Mobile Packet Communication System Special”, NTT DoCoMo Technical Journal Vol.5, No.2 (July 1997)

[5] http://www.openplanet.co.jp/