

携帯端末におけるセキュアな画像モニタリングに関する研究

1130321 小椋 智泰 【 清水研究室 】

1 はじめに

近年、ネットワークカメラの需要が拡大している。国内市場規模は、2015 年には 219 億円となる見込みである [1]。需要拡大の理由として、今まで使われてきたアナログカメラよりも金銭的なコストが低いことや、高画質化や高画角化といった性能向上があげられる。また、幼稚園や保育所のカメラを保護者がいつでも見られたり、ペットや要介護者の様子を遠方から携帯端末で確認するといった画像モニタリングサービスも増えている [2]。カメラで撮影された画像は、個人情報や企業機密の情報である。画像情報を送信する通信路のセキュリティには、パスワード認証や SSL、IPsec が用いられており、これらには問題がある。

そこで本稿では、携帯端末における画像モニタリングに適したセキュリティの提案・開発の実験結果の報告をする。

2 携帯端末における画像モニタリングのセキュリティ

遠隔監視サービスは、フィーチャーフォンやスマートフォンなどでブラウザを用いて閲覧する。閲覧する画像はパスワードによる認証や SSL もしくは IPsec によってセキュリティを確立している。以下に、各セキュリティの問題点を述べていく。

2.1 パスワード認証の問題点

パスワード認証とはあらかじめ本人が登録した単一の固定文字列を使う認証である。これは数字や記号を複雑な組み合わせの文字列を用い、また、定期的に文字列を変更しなければ悪意ある人物による辞書攻撃や総当たり攻撃によって解読される恐れがある。

2.2 SSL の問題点

SSL(Secure Socket Layer) とは電子証明書による公開鍵暗号方式と共通鍵暗号方式を併用して、認証及び暗号通信を行う方式である。この方式では、正当な利用者であることを示す証明書を証明局が発行する必要がある。そのため導入コストや維持コストなどが必要である。

2.3 IPsec の問題点

IPsec とはネットワーク層で認証や暗号化を行いセキュリティを実現する技術である。この方式では、認証方式によっては既に解読装置が開発されており、認証局を導入するコストがかかる恐れがある。

提案方式ではこれらの問題を解決するワンタイムパスワードである SAS-2 を使ってセキュアな画像モニタリングを実現する [3]。

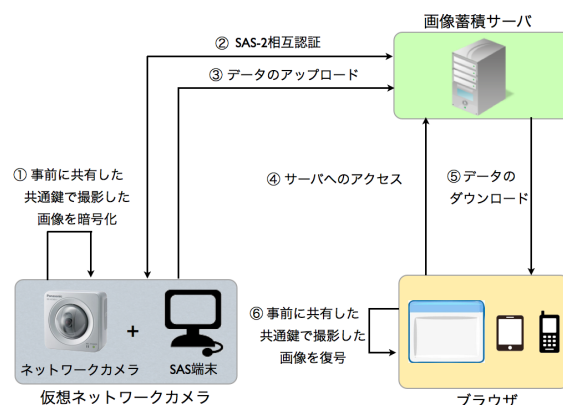


図 1 提案システムの流れ

3 提案方式

図 1 に提案システムの流れを示す。今回、ネットワークカメラにプログラマブルなものがなかったため SAS-2 をかける端末と合わせて仮想ネットワークカメラとした。また、仮想ネットワークカメラとブラウザ側であるユーザは共通鍵を共有する。

まず、仮想ネットワークカメラで共通鍵を用いて画像を暗号化する。そして仮想ネットワークカメラと画像蓄積サーバを SAS-2 で認証し、正しい通信先かを確認する。その後、暗号化したデータをアップロードする。

ユーザはブラウザからサーバへアクセスし、暗号化されたデータをダウンロードする。そのデータを事前に共有していた共通鍵でデータを復号して画像を復号する。

4 まとめ

本研究では既存の画像モニタリングの問題であるセキュリティと認証局の導入・維持コストを SAS-2 を用いた提案手法によって解決し、セキュアで認証局のいらぬ方式を実装した。今後は速度評価やパケットサイズの評価を行ない、SAS-2 のもっとも負荷がかからない鍵交換のタイミングを検討する。

参考文献

- [1] 国内のセキュリティ関連市場を調査, "https://www.fuji-keizai.co.jp/market/12090.html," 株式会社富士経済
- [2] 監視カメラソリューションと活用事例—HD&メガピクセルネットワークカメラ, 日本工業出版
- [3] 大垣文誉, 小西竜也, 辻貴介, 清水明宏, "SAS を用いた Web 通信方式," 電子情報通信学会技術研究報告, OIS2003-6, vol.103, no.44, pp.31-35, 2003.