ネットワークカメラ映像のセキュアな転送方式に関する研究

1140318　釜山瑠梨

1　はじめに

近年，監視カメラの市場は拡大している．市場拡大の理由として，ネットワークカメラの普及によりネットワークを用いた遠隔管理を行える点が挙げられる．監視カメラの導入の多くの目的として防犯が挙げられる [1]．このことからネットワークカメラを用いた映像転送を行うと秘匿でなければならない映像がネットワークに流れる．よってネットワークを流れる映像は悪意のある第３者から保護する必要がある．既存のシステムには情報セキュリティ技術が使われているがこれらの技術には脆弱性や高コストといった問題点がある．本研究では，安全性を高めるためワンタイムパスワード認証方式 SAS-2(Simple And Secure password authentication protocol ver.2)[2] を用いた映像転送方式を提案する．

2　既存方式における問題点

ネットワークカメラの映像閲覧における情報セキュリティの各方式の問題点を挙げる．

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る．しかしながら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　既存のワンタイムパスワード認証の問題点

ネットワークカメラにおける既存のワンタイムパスワード認証既存の方式では，通常の ID パスワード認証後，認証が成立した場合のみあらかじめ登録したメールアドレスへワンタイムキーが送られ，もう一度認証を行う．しかしながらこの方式は, コンピュータウイルスによってワンタイ ムキーを抜き取られてしまっている．つまり脆弱性のある方式である．

2.3　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．SSL の導入には，証明書発行によるコストと通信速度の低下が伴う．また証明書には維持のコストもかかる．

3　提案方式

図１に提案システムの流れを示す．ネットワークカメラにプログラマブルなものがあかったので RaspberryPi という小型コンピュータと USB カメラをつなぎ仮想ネットワークカメラとした．ネットワークカメラはクライアントがアクセス要求をしてきた場合，そのとき持っている認証情報を元に鍵を作成し画像を暗号化する. 暗号化した画像と送信用情報をクライアント端末に送信する．クライアント端末は送信情報から生成した認証情報で復号の鍵を作成, 画像を復号する．また，認証が不成立であれば，ネットワークカメラから送られる画像は 0 KB になる．認証が成立し画像の復号処理が終われば画像を閲覧する事ができネットワークカメラに認証情報を返す．

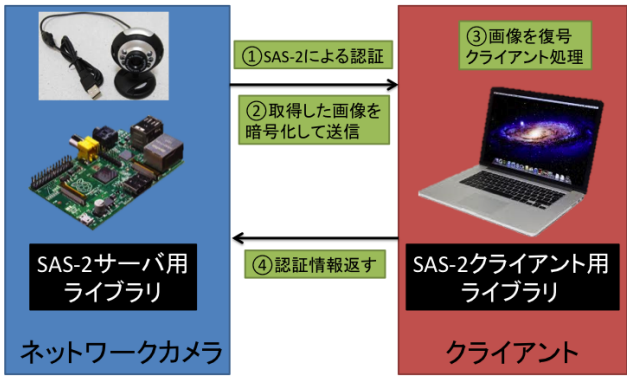

図 1　提案方式の流れ

4　評価

提案手法が既存方式である SSL と比べて処理速度が高速であるかを評価する．評価項目は実際に通信を行いかかった処理時間である．それぞれ１０回ずつ処理を行い，平均した値である．　この結果より，提案方式は既存方式である SSL より認証暗号化が行えることを示した．また認証局が不要なため SAS には維持コストがかからない．よって提案手法は高セキュリティかつ処理速度が早く，低コストな手法である．今後の展望として静止画像から動画への適応を考える．

表 1　実験結果

SAS	SSL
141ms	160.7ms

5　まとめ

本研究では，ネットワークカメラ映像の映像配信 SAS-2 を用いた認証及び映像暗号化を行うことによって高セキュリティかつ低コストで処理の早いの映像転送方式を提案し実証した．

参考文献

[1] 日経 BP 半導体，スマホカメラセンサ市場を切る TSR レポート, http://techon.nikkeibp.co.jp/article/COLUMN/20130701/290519/,（2013/10/11 アクセス）

[2] 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.