SAS-L を用いた動画像暗号通信方式の研究

1275105　高原 成功　【 セキュリティシステム研究室 】

A Study on Secure Video Communication Methods Using SAS-L

1275105　TAKAHARA, Nao　【 Security Systems Lab. 】

1　はじめに

近年，IoT の普及により，個人情報などの様々な情報がインターネット上でやり取りされるようになってきている．その中で，身近な IoT 機器として Web カメラが挙げられ，Web カメラは防犯用の監視カメラとしての利用や，産業・医療にも用いられている．インターネット上で操作できるため，利便性は高いが，Web カメラに映っている利用者の行動や個人情報を保護するため，通信を暗号化する必要がある．しかし，IoT 機器に使用される Web カメラには，処理能力の低い物や，メモリの容量に制約があるため，セキュリティ対策が十分に行えない場合も存在する．特に，カメラ撮影から得られる動画像は，データサイズが大きいため，暗号化の工夫や，暗号鍵の安全性についての検討が必要である．

本研究では，処理能力の低い Web カメラでも，安全な動画像暗号通信を行えるような方式を提案する．それに付随し，プライバシ保護のため，動画像の映し方についても検討を行う．

2　従来方式

2.1　事前共有鍵による暗号化

事前共有鍵方式（Pre-shared Key, PSK）は，通信を行う双方が事前に共有した対称鍵を用いて暗号化および復号化を行う方式である．本方式では，通信開始前に安全な経路を用いて暗号鍵を共有し，以降の通信を AES（Advanced Encryption Standard）等の安全な暗号方式を用いて動画像を保護する．しかし，事前共有鍵方式では，暗号鍵の更新が困難であるため，一度鍵が漏洩すると全ての通信が解読される危険性がある．そのため，鍵更新が必要となるが．多数の IoT 機器に対する更新作業は煩雑となる．

2.2　セッション鍵による暗号化

事前共有鍵方式の課題を解決する手法として，鍵交換プロトコルを利用したセッション鍵方式がある．セッション毎に異なる暗号鍵を生成し，その鍵を用いて通信データを暗号化および復号化する方式である．RSA や DH 法といった公開鍵暗号方式を応用した鍵交換プロトコルを利用して，セッション鍵を安全に交換した後，AES などの共通鍵暗号方式で暗号通信を行う．安全性が向上した一方で，処理負荷の大きい鍵交換プロトコルが利用されるため，リソースの限られた IoT 機器では，実装が困難であったり，リアルタイム性が損なわれるといった課題が発生する場合がある．

3　提案方式

従来方式の問題点を解決する方式として，SAS-L2 を鍵交換に用いた動画像暗号化システムを提案する．提案方式の概要を図 1 に示す．

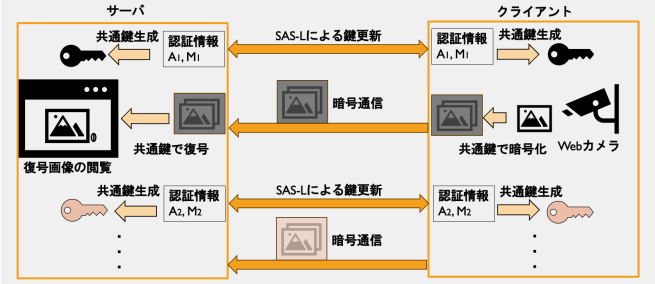

図 1　提案方式の概要図

3.1　SAS-L2

SAS-L2 はサーバ・クライアントのいずれかでハッシュ関数の適用を必要としない，処理負荷が限りなく 0 に近いワンタイムパスワード認証方式である [1]．SAS-L2 の認証フローを図 2 に示す．

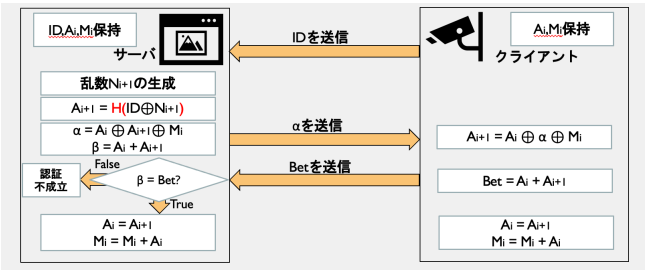

図 2　SAS-L2 の認証フロー

サーバは検証子とクライアントからの受信内容が一致していれば認証成立で，認証情報を次回用に更新する．一致していなければ，認証不成立となる．

提案方式では，SAS-L2 の各認証情報をもとにして，共通鍵を生成する鍵交換方式として利用する．

3.2　動画像の暗号化

3.2.1　JPEG 圧縮

JPEG 圧縮は，画像の視覚的品質を保ちながらデータ量を削減できるため，動画像の効率的な伝送に適している．特に，IoT 機器やネットワーク帯域が限られた環境では，JPEG 圧縮によるデータ量削減が通信負荷の軽減に寄与する．提案方式では，まず動画像をフレーム単位で JPEG 圧縮し，暗号化処理の対象とすることで効率的な通信を実現する．

3.2.2　バーナム暗号

バーナム暗号（Vernam Cipher）は，一度限りのパッド（OTP: One-Time Pad）を用いた暗号化方式であり，シャノンにより理論的には完全な安全性を持つと証明されている [2]．暗号化の際，平文と同じ長さのランダムな鍵をビットごとに排他的論理和（XOR）演算で組み合わせることで暗号文を生成する．復号時には，同じ鍵を再度使用して XOR 演算を行うことで平文を復元する．提案方式では，動画像を暗号化する際に，フレーム単位で SAS-L2 で鍵を交換し，バーナム暗号を適応することで，安全かつ高速な暗号通信を実現する．

4　結果と考察

4.1　速度評価

表 1 は，AES の同一鍵を用いる方式と，AES，XOR に対してそれぞれ SAS-L2 鍵更新を行った際の fps 計測結果（ 画像を 1000 フレーム送信した際のもの）である．同一鍵を使い続ける方式では，15.32fps，SAS-L2 で鍵更新を行う AES 暗号化では 11.03fps となった．同一鍵を用いる方式よりも鍵更新を行っている分，低速になったが，速度減衰を約 28 %に抑えて，より安全な動画像の通信が可能である．また，AES 暗号化では，Web カメラの処理能力が低い場合や，ライブラリに対応していない機器の場合は，実装が難しくなるのに対し，XOR 暗号化では，単純な論理演算のみで行っているため，処理能力の低い機器にも実装可能であると言える．

表 1　fps 比較

方式	[fps]
AES 暗号化（同一鍵）	15.32
AES 暗号化と SAS-L2 鍵更新	11.03
XOR 暗号化と SAS-L2 鍵更新	13.42

4.2　鍵更新による比較

表 2 は，動画像を XOR 演算で暗号化し，鍵更新に SAS-L2 と DH 法を使用したときの fps と，鍵交換 1 回にかかる平均時間を計測したものである．SAS-L2 鍵更新では，鍵交換の時間が 0.014s なのに対し，DH 法では 5.16s となっており，大幅な差が出ていることが確認できる．また，DH 法を使用した時の fps は，0.02fps という結果になった．日本防犯設備協会の防犯カメラ撮影機能では，最低でも 2〜3fps で記録できる性能が条件とされており，リアルタイム性の観点から見ても，SAS-L2 を用いた動画像通信は有用であると言える．

表 2　鍵更新の性能比較

方式	[fps]	鍵交換の平均時間 [s]
XOR 暗号化と SAS-L2	13.42	0.014
XOR 暗号化と DH 法	0.02	5.16

4.3　部分的暗号化

元画像図 3 に対し，特定のピクセル領域に対して部分的暗号化を行なったものが図 4 である．JPEG 圧縮されたフレームデータ内のピクセル範囲を指定し，XOR で暗号化を行なった．暗号化されたピクセル値は，元画像にランダムなノイズを与え，さらに対象領域のピクセルブロックを平均化することで，視覚的な加工を行なっている．これにより，カメラに映っている対象人物の行動を監視すると同時に，プライバシの保護を行うことができる．

図 3　元画像

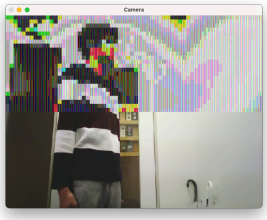

図 4　特定領域の暗号化

5　まとめ

本研究では，ワンタイムパスワード認証方式である SAS-L2 を鍵更新に用いた，動画像暗号通信を提案した．動画像の通信は，カメラから得られるデータサイズが大きいため，鍵更新も含めると処理が大きくなってしまうが，軽処理な SAS-L2 を鍵更新に用いることで，処理能力の低い機器にも対応可能であることを示した．また，動画像の部分的な暗号化により，プライバシ保護も実現した．

参考文献

[1] 溝口洸熙，清水明宏，”IoT 環境に適したワンタイムパスワード認証方式”，電子情報通信学会技術研究報告，vol. 124, no. 257, LOIS2024-43, pp. 112-117, 2024 年 11 月．

[2] Claude E. Shannon, ”Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.