情報処理学会論文誌 Vol.54 No.2 561–570 (Feb. 2013)

ネットワークカメラシステムにおける セキュアなプロファイル設定方式の提案

阿倍 博信[1,a)] 若土 剛之[1] 中島 宏一[1] 小林 信博[1]

受付日 2012年4月24日, 採録日 2012年11月2日

概要：本論文では，ネットワークカメラの動作に必要な各種プロファイルのネットワーク経由での設定を ID ベース暗号の適用によりセキュア化する方式について述べる．提案にあたり，プロファイル設定機能を ID ベース暗号の処理性能と使用頻度を考慮して初期設定と通常設定に分割した．本方式では，処理負荷の高い ID ベース暗号処理は初期設定時のみ 1 回実行し，通常設定時には共通鍵暗号を使用する．評価システムを開発し，システムの基本性能について評価を行ったところ，その有効性について確認できた．

キーワード：ネットワークカメラ，ID ベース暗号，プロファイル設定

Proposal of a Secure Profile Setting Method in the Network Camera System

Hironobu Abe[1,a)] Takayuki Wakatsuchi[1] Koichi Nakashima[1] Nobuhiro Kobayashi[1]

Received: April 24, 2012, Accepted: November 2, 2012

Abstract: In this paper, the profile setting method where secure setting by way of the network of various profiles necessary for the operation of the network camera are achieved by using the identity-based encryption is described. When the proposal, the profile setting function was divided into initialization and a usual setting in consideration of the processing performance and the operation frequency of the identity-based encryption. In this method, the identity-based encryption processing with a high processing load executes once only when initializing it, and uses the common-key encryption when usually setting it. When the evaluation system was developed, and the basic performance of the system was evaluated, the effectiveness was able to be confirmed.

Keywords: network camera, identity-based encryption, profile setting

1. はじめに

近年のセキュリティ意識の高まりにより，監視カメラを用いた映像監視システムの市場規模が拡大している．その中でも，IP ネットワークに直結可能なネットワークカメラの普及が著しい [1]．

ネットワークカメラの普及により映像監視システムの大規模化が可能となり，数百～数千台規模のカメラを設置したシステムが一般的になりつつある．ネットワークカメラはネットワークや画像データの符号化に関するパラメータ（以下プロファイル）を機器ごとに設定管理する必要があるが，我々はシステムの運用コスト削減を目的として，複数のネットワークカメラのプロファイルを 1 台のサーバで一括管理するネットワークカメラのプロファイル管理システムの開発を行っている [2]．

また，ネットワークカメラシステムの大きな流れの 1 つとして，入退室管理システムなどの関連システムとのシステム連携に対する要求の高まりがある．たとえば，駅の改札やサーバ室への入室の際に，システム連携により入退室情報と顔画像を同時に記録するなどの用途が考えられる．従来のネットワークカメラシステムでは，専用の IP ネッ

[1] 三菱電機株式会社
Mitsubishi Electric Corporation, Kamakura, Kanagawa 247–8501, Japan
[a)] Abe.Hironobu@cs.MitsubishiElectric.co.jp

トワークを構築して使用してきたため，特に情報セキュリティ対策は不要とされてきたが，他システムとの連携を前提とするシステムの場合，情報漏えい対策をはじめとするセキュリティ面での信頼性（ディペンダビリティ）の課題が指摘されている [3].

上記課題に対応して，本論文では，ネットワークカメラのプロファイル管理システムを拡張し，公開鍵暗号の 1 つである ID ベース暗号 [4] を用いてネットワークカメラのプロファイルをセキュアに設定する方式について提案する．

本論文では，2 章でセキュア化の課題，3 章でプロファイル設定機能の性能要件分析，4 章でネットワークカメラの ID としてカメラの MAC アドレスを，プロファイル管理サーバの ID として顧客 ID を使用し，プロファイル管理サーバ（以下 PMS）からネットワークカメラの各種プロファイルの設定をセキュア化する方式の提案，5 章で本方式を適用した評価システムの開発，6 章で評価システムを用いたシステムの基本性能の評価結果，7 章で考察について述べ，最後にまとめを行う．

2. セキュア化の課題

ネットワークカメラの PMS のセキュア化の従来方式では，TLS [5]（Transport Layer Security）をはじめとする公開鍵暗号を用いた PKI による暗号化通信が広く使用されてきた．従来方式では，暗号化の際に用いる公開鍵の正当性保証のために公開鍵証明書を使用する必要がある．

たとえば，リポジトリの設置が不要であり，現状ネットワークカメラで最も広く使用されている方式である機器内部から証明書を入手する方式では下記の課題があげられる．

- **課題 1**　ネットワーク経由で機器と証明書の結び付きが確認できないため，セキュリティ面での課題がある．
- **課題 2**　機器の製造時に証明書を発行することができないため，ネットワークカメラの設置時に，オフラインで証明書を取り出す作業が発生し，設置コストがかかる．

課題 1 への対応として，認証局などのリポジトリを設置する方式が考えられるが，ネットワークカメラの前提とするネットワークは，情報漏えい対策に代表されるセキュリティポリシ上の理由より，リポジトリの設置されたネットワークとの接続が保証されない場合が多く，ネットワークカメラに適用するのは困難である．

以上より，セキュア化の検討にあたり，従来方式である TLS 以外のアプローチについて検討していく必要がある．

3. プロファイル設定機能の性能要件分析

映像監視システムでは，対象分野によって，ネットワークカメラの設置台数が異なる [6]．PMS はその中でも，設置コストと運用コストとのバランスがとれた 50〜100 台程度の中大規模システムを対象としている．そこで，本論文では，PMS 1 台で管理対象とするネットワークカメラの台数を 100 台に設定する．

PMS におけるプロファイル設定機能はネットワークカメラの制御 API を使用して実現する．従来，ネットワークカメラの制御 API は各社独自のプロトコル（レガシープロトコル）が長く使用されてきたが，2008 年にネットワークカメラ製品のインタフェース規格標準化フォーラムとして ONVIF [7]（Open Network Video Interface Forum）が設立され，現在，標準化が進んでいる．

ONVIF も含め，一般的にネットワークカメラの制御 API は，大きく以下の 3 種類に分類することができ，PMS においてもそれぞれサポートしている．

(1) **プロファイル設定**
　ネットワークカメラの動作に必要なプロファイルを設定する．

(2) **プロファイル取得**
　ネットワークカメラに設定されているプロファイルを取得する．

(3) **カメラ制御**
　パン，チルト，ズームなどネットワークカメラの制御を行う．

今回，PMS のプロファイル設定機能のセキュア化検討にあたり，ONVIF 規格書 [8]（Version 1.02）で規格化されているネットワークカメラの制御 API（152 個）を上記 3 種類に分類し，使用するタイミング（システム構築時/システム運用時），使用頻度（高/低）[*1]，同時実行数，の観点から，性能要件分析として，通信時間を含むプロファイル設定機能の目標応答時間を検討した．

一般的にシステム構築時に使用するプロファイル設定 API は使用頻度は低く，システム運用時に使用する API は使用頻度は高くなる．また，システム構築時におけるプロファイル設定は，カメラ設置工事と並行してネットワーク関連のプロファイルを設定する場合など，人手で 1 台ずつ実施されるため，同時実行数を 1 に設定した．システム運用時におけるプロファイル設定はアラームイベント発生により関連するネットワークカメラの画像符号化関連のプロファイルを自動的に変更する場合など自動実行が中心となるため，同時実行数を 4 に設定した．また，プロファイル取得やカメラ制御などのカメラからの応答が必須である API は性能要件が高くなる．

性能要件の分析結果について**表 1** に示す．

表 1 に示したプロファイル設定機能の性能要件について下記のとおり分析した．

(1) **システム構築時**
　ネットワーク関連のプロファイルの設定など，基本的にシステム構築時に 1 回だけ設定すればよいネット

[*1] 使用頻度として，1 日に平均 1 回以上使用するものを高，それ以下のものを低に分類した．

表 1 ネットワークカメラ制御 API の性能要件分析結果
Table 1 Performance requirement analysis result of network camera control API.

使用するタイミング	システム構築時			システム運用時		
機能	プロファイル設定	プロファイル取得	カメラ制御	プロファイル設定	プロファイル取得	カメラ制御
使用頻度	低	低	低	高	高	高
同時実行数	1	100	1	4	100	1
目標応答時間 (秒)	30	1	1	1	1	1
調査 API 数	56	7	3	11	64	11

ワークカメラ API．使用頻度が低く，同時実行数が 1 で人手での作業を前提とするため，PMS とネットワークカメラでの処理時間と通信時間を加えた目標応答時間を 30 秒に設定した．

(2) システム運用時
画像データの符号化関連のプロファイルの設定など，システム運用時に頻繁に発生するネットワークカメラ API．使用頻度が高く，同時実行数が 4 であり，アラームイベント処理など性能要件が高いため，PMS とネットワークカメラでの処理時間と通信時間を加えた目標応答時間を 1 秒に設定した．

また，本論文では対象としていないが，プロファイル取得機能，カメラ制御機能は使用するタイミングや使用頻度と関係なく性能要件が高いことが分かった．

4. セキュアプロファイル設定方式の提案

4.1 方針

これまでの検討結果を考慮し，本論文では ID ベース暗号を用いたセキュア化について検討していく方針とする．ID ベース暗号では，機器の製造時に生成した機器固有の ID を公開鍵として使用できるため，公開鍵の正当性保証のための認証局の設置が不要となり，簡易にシステムを構築することが可能である [9]．

一方で，ID ベース暗号処理は演算量の大きいペアリング暗号をベースとしており，他の公開鍵暗号処理と比較して演算量が大きくなる，という課題がある．文献 [10] では，ペアリング暗号処理は RSA 暗号や楕円曲線暗号と比べて 5 倍以上遅いことが報告されている．このような理由から，ID ベース暗号は，従来は電子メールシステムなどの PC ベースのシステムを中心に適用されてきた [11]．

また，ID ベース暗号を PC より処理性能の低い組み込み機器に適用する取り組みは新しい試みであり，ネットワークカメラへの ID ベース暗号の実装例はない．関連研究としては，携帯電話を対象としたペアリング暗号の高速実装に関する研究があるが，まだ研究途上ということもあり [12], [13]，今回，携帯電話よりさらに処理性能の低いネットワークカメラに ID ベース暗号を実装する必要があるため，ID ベース暗号の適用方式からのアプローチによる処理負荷対策がポイントとなる．

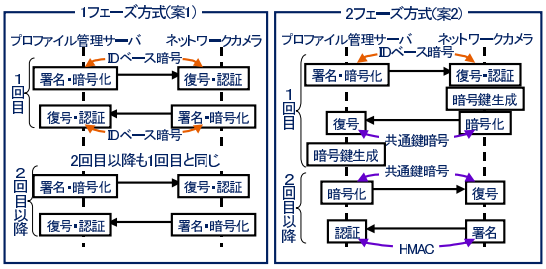

図 1 セキュアプロファイル設定機能の概要
Fig. 1 Outline of secure profile setting function.

4.2 提案の概要

設計方針に基づき，ID ベース暗号を適用によるネットワークカメラのセキュアプロファイル設定機能の実現方式について検討した．本論文では，ID ベース暗号として，Boneh らの方式 [14] を前提として検討を行い，下記の 1 フェーズ方式（案 1）と 2 フェーズ方式（案 2）について比較検討を実施した（**図 1**）．

- **1 フェーズ方式（案 1）**
  案 1 は ID ベース暗号のみを用いてプロファイル設定機能のセキュア化を実現する方式である．ネットワークカメラに対してプロファイル設定機能を行う際に，PMS とネットワークカメラの双方で相互に ID ベース暗号処理を行うことによりセキュア化を実現する．
- **2 フェーズ方式（案 2）**
  案 2 は，3 章の結果をもとにプロファイル設定機能を 2 フェーズに分割し，ID ベース暗号と共通鍵暗号を組み合わせる方式である．プロファイル設定機能を使用頻度と ID ベース暗号の処理負荷を考慮して初期設定と通常設定に分割し，処理負荷の高い ID ベース暗号処理は初期設定で 1 回のみ実行し，2 回目以降は通常設定として ID ベース暗号のかわりに共通鍵暗号（MISTY [15]）を用いる [16], [17], [18]．

案 1 では，プロファイル設定を行うごとに，処理負荷の高い ID ベース暗号処理を組み込み機器で動作させる必要があり，ID ベース暗号の処理負荷による応答性の課題がある．一方，案 2 は共通鍵暗号との組合せを前提とする方

式であり，ID ベース暗号の処理負荷対策も実現できていることから，本論文では，案 2 を選択することとした．

以下，案 2 を用いたセキュアプロファイル設定機能の処理概要について示す．

(1) 工場設定
機器製造時に，工場で ID ベース暗号に必要なパラメータを設定する．

(2) プロファイル初期設定
システム構築時に，ID ベース暗号を用いてネットワークカメラの認証を行うと同時に共有鍵の作成，共有，およびプロファイルの初期設定を行う．この処理はシステム構築時に 1 回動作させればよい．この処理を機器製造時に行う案も考えられるが，通常，機器製造時には PMS とネットワークカメラの組合せが決まっていないため，運用上の課題がある．

(3) プロファイル通常設定
システム運用時に，プロファイル初期設定時に共有した共有鍵を用いて暗号化を行い，ネットワークカメラのプロファイル設定機能をセキュア化する．この処理はシステム運用時に必要に応じてユーザが使用する．

4.3 工場設定

工場において，事前に鍵生成センタ PKG（Private Key Generator）のセキュリティパラメータ k からマスタパブリックキー PK_m と，マスタシークレットキー SK_m を関数 $SETUP()$ により生成する．

次に，PKG がマスタシークレットキー SK_m，プロファイル管理サーバ PMS の ID である ID_{pms} を入力として関数 $DERIVATION_s()$ により PMS のシークレットキー SK_{pms} を生成する．

また，PKG が SK_m，ネットワークカメラ NC の ID である ID_{nc} を入力として関数 $DERIVATION_e()$ により NC のシークレットキー SK_{nc} を生成する．

最終的に，PMS には，PKG のマスタパブリックキー PK_m および PMS のシークレットキー SK_{pms} を配付し，NC には，PKG のマスタパブリックキー PK_m および NC のシークレットキー SK_{nc} を配付する．

4.4 プロファイル初期設定

プロファイル初期設定における処理フローは，まず，PMS でプロファイル初期設定要求を生成し，HTTP/POST 経由で NC に送信する（STEP1）．NC では，受信したプロファイル設定要求を解析し，初期設定機能を行うとともに，その結果をもとに応答を作成し，PMS に応答送信する（STEP2）．最後に，PMS で NC から応答内容に基づき，処理を行う（STEP3）．**図 2** にプロファイル初期設定処理の流れについて示す．

以下，STEP ごとに，処理内容の詳細について説明する．

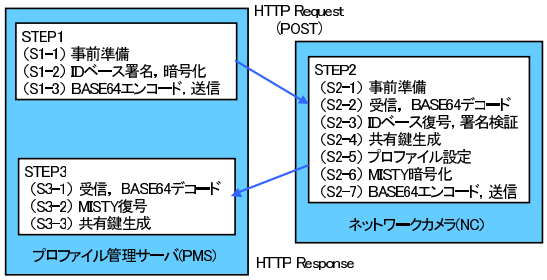

図 2 プロファイル初期設定機能の流れ
Fig. 2 Flow of profile initialization function.

4.4.1 STEP1

(S1-1) 事前準備

PMS では，あらかじめ設定対象のネットワークカメラ NC に設定すべきプロファイル $PROF_{nc}$ および NC の ID_{nc} を準備しておく．

(S1-2) ID ベース署名，暗号化

乱数生成関数 $rand()$ を用いて $NONCE1$ を生成するとともに，タイムスタンプ $DATE$ を取得する．そして $PROF_{nc}$ および ID_{nc} と結合してメッセージ M に設定する．

$$NONCE1 = rand(), \tag{1}$$
$$M \leftarrow [NONCE1, ID_{nc}, PROF_{nc}, DATE]$$

続いて，マスタパブリックキー PK_m，PMS のシークレットキー SK_{pms}，メッセージ M を入力として ID ベース署名関数 $IB_{sign}()$ により署名 SIG_{pms} を生成する．

$$SIG_{pms} = IB_{sign}(PK_m, SK_{pms}, M) \tag{2}$$

さらに，メッセージ M，署名 SIG_{pms} および PMS の ID_{pms} と結合してメッセージ M' に設定するとともに，M'，マスタパブリックキー PK_m，NC の ID_{nc} を入力として ID ベース暗号化関数 $IB_{enc}()$ により暗号化データ C_{pms} を生成する．

$$M' \leftarrow [M, SIG_{pms}, ID_{pms}], \tag{3}$$
$$C_{pms} = IB_{enc}(PK_m, ID_{nc}, M')$$

(S1-3) BASE64 エンコード，送信

暗号化データ C_{pms} を BASE64 [19] エンコードし，その結果を HTTP/POST 経由で NC に送信する．

4.4.2 STEP2

(S2-1) 事前準備

NC では，製造時の初期値として $DATE_{init}$ が設定されたタイムスタンプ $DATE_{nc}$ を読み込んでおく．

(S2-2) 受信，BASE64 デコード

PMS から受信したデータを BASE64 デコードし，暗号化データ C_{pms} を取得する．

（S2-3）ID ベース復号，署名検証

暗号化データ C_{pms}，PKG のマスタパブリックキー PK_m，NC のシークレットキー SK_{nc} を入力として ID ベース復号関数 $IB_{dec}()$ によりメッセージ M' を復号する．

$$M' = IB_{dec}(PK_m, SK_{nc}, C_{pms}) \tag{4}$$

続いて，メッセージ M' から，メッセージ M，署名 SIG_{pms}，PMS の ID_{pms} を抽出し，ID ベース検証関数 $IB_{vrf}()$ により，PMS の署名を検証する．

$$[M, SIG_{pms}, ID_{pms}] \leftarrow M', \tag{5}$$
$$IB_{vrf}(PK_m, ID_{pms}, M, SIG_{pms}) \Rightarrow OK/NG$$

（S2-4）共有鍵生成

署名検証結果が OK であれば，通信データの再送によるリプレイアタックでないことを確認するため，メッセージ M から抽出したタイムスタンプ $DATE$ がタイムスタンプ $DATE_{nc}$ より新しいことを検証する．

$$[NONCE1, ID_{nc}, PROF_{nc}, DATE] \leftarrow M, \tag{6}$$
$$DATE_{nc} < DATE \Rightarrow OK/NG$$

タイムスタンプ検証結果が OK であれば，乱数生成関数 $rand()$ を用いて $NONCE2$ を生成し，受信した $NONCE1$ と組み合わせて共有鍵導出関数 $KDF()$ から共有鍵 CK_{nc} を生成する．そして，受信した $DATE$ により $DATE_{nc}$ を更新するとともに，プロファイル通常設定で使用するために CK_{nc} を保存する．

$$NONCE2 = rand(), \tag{7}$$
$$CK_{nc} = KDF(NONCE1, NONCE2),$$
$$DATE_{nc} \leftarrow DATE$$

（S2-5）プロファイル設定

受信した $PROF_{nc}$ の内容に従い，NC のプロファイル設定を行い，その結果を RES_{nc} に出力する．

（S2-6）MISTY 暗号化

PMS の ID_{pms}，NC の生成した $NONCE2$，プロファイル設定結果 RES_{nc} を結合して応答メッセージ M_{res} に設定する．そして，暗号鍵とする $NONCE1$ と M_{res} を入力として，共通鍵暗号方式である暗号関数 $MISTY()$ を用いて暗号化データ C_{nc} を生成する．

$$M_{res} \leftarrow [NONCE2, ID_{pms}, RES_{nc}], \tag{8}$$
$$C_{nc} = MISTY(NONCE1, M_{res})$$

（S2-7）BASE64 エンコード，送信

暗号化データ C_{nc} を BASE64 エンコードし，その結果を HTTP 経由で PMS に送信する．

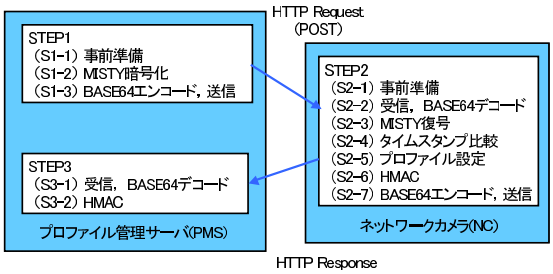

図 3 プロファイル通常設定機能の流れ

Fig. 3 Flow of usual profile setting function.

4.4.3 STEP3

（S3-1）受信，BASE64 デコード

PMS では STEP1 の HTTP 応答として受信したデータを BASE64 デコードし暗号化データ C_{nc} を取得する．

（S3-2）MISTY 復号

暗号化データ C_{nc} を，STEP1 で生成した $NONCE1$ を復号鍵として用いて共通鍵暗号方式である暗号関数 $MISTY()$ により復号し，応答メッセージ M_{res} を入手する．

$$M_{res} = MISTY(NONCE1, C_{nc}) \tag{9}$$

（S3-3）共有鍵生成

復号された応答メッセージ M_{res} から $NONCE2$，ID_{pms}，RES_{nc} を抽出し，抽出した ID_{pms} と保有する ID_{pms} の比較検証を行う．比較検証結果が OK であれば，受信した $NONCE2$ と $NONCE1$ を組み合わせて共有鍵導出関数 $KDF()$ から共有鍵 CK_{nc} を生成し，プロファイル通常設定で使用するために CK_{nc} を保存する．

$$[NONCE2, ID_{pms}, RES_{nc}] \leftarrow M_{res}, \tag{10}$$
$$CK_{nc} = KDF(NONCE1, NONCE2)$$

4.5 プロファイル通常設定

プロファイル通常設定における処理フローも，プロファイル初期設定の処理フローと同様に，3 STEP より構成され，PMS と NC の通信は HTTP/POST 経由となる．**図 3** にプロファイル通常設定機能の流れについて示す．

以下，STEP ごとに，処理内容の詳細について説明する．

4.5.1 STEP1

（S1-1）事前準備

PMS では，あらかじめ設定対象のネットワークカメラ NC に設定すべきプロファイル $PROF_{nc}$ を準備しておく．

（S1-2）MISTY 暗号化

乱数生成関数 $rand()$ を用いて $NONCE1$ を生成するとともに，タイムスタンプ $DATE$ を取得する．そして $PROF_{nc}$ および $DATE$ と結合してメッセージ M に設定する．

$$NONCE1 = rand(), \quad (11)$$
$$M \leftarrow [PROF_{nc}, DATE]$$

続いて $NONCE1$ と M を入力として，共通鍵暗号方式である暗号関数 $MISTY()$ を用いて暗号化データ C'_{pms} を生成する．さらに暗号鍵とする共有鍵 CK_{nc} と $NONCE1$ を入力として，$MISTY()$ を用いて暗号化データ C''_{pms} を生成する．そして，C'_{pms} と C''_{pms} を結合して暗号化データ C_{pms} に設定する．

$$C'_{pms} = MISTY(NONCE1, M), \quad (12)$$
$$C''_{pms} = MISTY(CK_{nc}, NONCE1),$$
$$C_{pms} \leftarrow [C'_{pms}, C''_{pms}]$$

（S1-3）BASE64 エンコード，送信

暗号化データ C_{pms} を BASE64 エンコードし，その結果を HTTP/POST 経由で NC に送信する．

4.5.2 STEP2

（S2-1）事前準備

NC では，あらかじめタイムスタンプ $DATE_{nc}$ を読み込んでおく．

（S2-2）受信，BASE64 デコード

PMS から HTTP/POST 命令経由で受信したデータを BASE64 デコードし，暗号化データ C_{pms} を取得する．

（S2-3）MISTY 復号

暗号化データ C_{pms} を暗号化データ C'_{pms} と暗号化データ C''_{pms} に分割する．そして，プロファイル初期設定で保存した共有鍵 CK_{nc} を復号鍵として用いて暗号化データ C''_{pms} を共通鍵暗号方式である暗号関数 $MISTY()$ により復号し，$NONCE1$ を入手する．さらに，この $NONCE1$ を復号鍵として用いて暗号化データ C'_{pms} を暗号関数 $MISTY()$ により復号し，メッセージ M を入手する．そして，メッセージ M から $PROF_{nc}$ および $DATE$ を抽出する．

$$[C'_{pms}, C''_{pms}] \leftarrow C_{pms}, \quad (13)$$
$$NONCE1 = MISTY(CK_{nc}, C''_{pms}),$$
$$M = MISTY(NONCE1, C'_{pms}),$$
$$[PROF_{nc}, DATE] \leftarrow M$$

（S2-4）タイムスタンプ比較

抽出した $DATE$ と $DATE_{nc}$ のタイムスタンプ検証を行い，タイムスタンプ検証結果が OK であれば，$DATE$ により $DATE_{nc}$ を更新する．

$$DATE_{nc} < DATE \Rightarrow OK/NG, \quad (14)$$
$$DATE_{nc} \leftarrow DATE$$

（S2-5）プロファイル設定

$PROF_{nc}$ の内容に従い，ネットワークカメラ NC のプロファイル設定を行いその結果を RES_{nc} に出力する．

（S2-6）HMAC

次に，乱数生成関数 $rand()$ を用いて $NONCE2$ を生成する．生成した $NONCE2$, RES_{nc} を組み合わせてメッセージ M' に設定し，$NONCE1$ を用いて関数 $HMAC()$ により HMAC [20] を実行し，MAC 値 MAC_{nc} を生成する．

$$NONCE2 = rand(), \quad (15)$$
$$M' \leftarrow [NONCE2, RES_{nc}],$$
$$MAC_{nc} = HMAC(NONCE1, M')$$

（S2-7）BASE64 エンコード，送信

MAC 値 MAC_{nc} とメッセージ M' を結合しメッセージ M'' に設定し，BASE64 エンコードし，その結果を HTTP 経由で PMS に応答送信する．

$$M'' \leftarrow [MAC_{nc}, M'] \quad (16)$$

4.5.3 STEP3

（S3-1）受信，BASE64 デコード

PMS では STEP1 の HTTP 応答として受信したデータを BASE64 デコードしてメッセージ M'' を取得する．

（S3-2）HMAC

メッセージ M'' を分割し，メッセージ M' と MAC 値 MAC_{nc} を抽出する．さらに，メッセージ M' を分割し，$NONCE2$ と RES_{nc} を抽出する．そして，$NONCE1$ を用いて関数 $HMAC()$ により MAC 値 MAC'_{nc} を生成し，MAC_{nc} と MAC'_{nc} を比較する．比較結果が OK であれば，RES_{nc} を確認する．

$$[MAC_{nc}, M'] \leftarrow M'', \quad (17)$$
$$[NONCE2, RES_{nc}] \leftarrow M',$$
$$MAC'_{nc} = HMAC(NONCE1, M'),$$
$$MAC_{nc} == MAC'_{nc} \Rightarrow OK/NG$$

5. 評価システムの開発

5.1 システム構成

図 4 にセキュアなプロファイル設定機能を実装したネットワークカメラのプロファイル管理システムの評価システム構成について示す．

評価システムでは，プロファイルをセキュアに設定するために新たにネットワークカメラへ搭載する機能をターゲットノード上に実装した．ターゲットノードには，将来的なネットワークカメラへの搭載を想定して，一般的なネットワークカメラと同等の CPU 性能を持ち，組み込み Linux 環境が動作する CPU ボードを選択した．**表 2** にターゲットノードの仕様について示す．

また，PMS および工場設定 PC として Windows XP

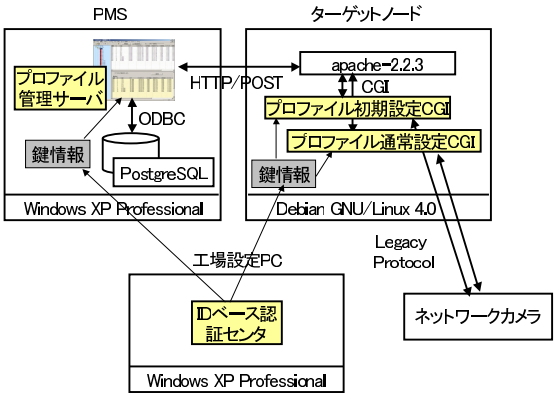

図 4 評価システム構成
Fig. 4 Evaluation system configuration.

表 2 ターゲットノードの仕様
Table 2 Specification of target node.

プロセッサ	Cirrus Logic EP9315（ARM9）
システムクロック	200 MHz
SDRAM	64 MB
OS	Debian GNU/Linux 4.0

表 3 ID ベース暗号ライブラリのパラメータ
Table 3 Parameters of identity based encryption library.

マスタパブリックキー	PK_m	104 バイト
マスタシークレットキー	SK_m	28 バイト
シークレットキー（NC）	SK_{nc}	312 バイト

Professional が動作する PC を準備し，これらの装置を 100BASE-TX ネットワークで接続する構成とした．

5.2 ID ベース暗号・署名ライブラリの実装

評価システムの構築の際に実装して使用した ID ベース暗号・署名ライブラリの仕様について以下に示す．方式の選定にあたり，ペアリング暗号処理に関する個別の高速化実装手法は利用せず，組み込み機器，PC への適用を考慮して一般的な方式，パラメータを選定した．

5.2.1 ID ベース暗号ライブラリ

本ライブラリは，プロファイル初期設定の際に，ID ベース暗号化関数 $IB_{enc}()$（S1-2），ID ベース復号関数 $IB_{dec}()$（S2-3）で使用する．ID ベース暗号方式として，境・笠原方式 [21] を採用した．また，暗号・復号処理の際に使用する各パラメータを**表 3** のとおり定義した．

5.2.2 ID ベース署名ライブラリ

本ライブラリは，プロファイル初期設定の際に，ID ベース署名関数 $IB_{sign}()$（S1-2），ID ベース検証関数 $IB_{vrf}()$（S2-3）で使用する．今回は，Certificate-based 方式 [22] を採用した．また，署名・署名検証処理の際に使用する各パラメータについて**表 4** のとおり定義した．

表 4 ID ベース署名ライブラリのパラメータ
Table 4 Parameters of identity based signature library.

マスタパブリックキー	PK_m	48 バイト
マスタシークレットキー	SK_m	24 バイト
シークレットキー（PMS）	SK_{pms}	120 バイト
署名	SIG_{pms}	144 バイト

表 5 PMS の仕様
Table 5 Specification of PMS.

プロセッサ	Intel Pentium M
システムクロック	1400 MHz
RAM	1024 MB
OS	Windows XP Professional SP3

表 6 プロファイル例
Table 6 Example of profiles.

プロファイル名	プロファイル内容	サイズ (bytes)	対象
ipaddress	カメラの IP アドレス	16	初期設定
control_port	カメラの制御ポート	4	初期設定
compress_rate	映像データの圧縮率	4	通常設定
frame_rate	映像データのフレームレート	4	通常設定

5.3 工場設定 PC

工場設定 PC では，PKG 機能を持つ ID ベース認証センタを実装し，ID ベース暗号処理に必要な鍵情報を PMS，ターゲットノードに配付する機能を実現した．

5.4 PMS

各カメラのプロファイルを PostgreSQL [23] で管理し，必要に応じて提案したプロファイル設定方式を用いて対象とするカメラに対してプロファイルの初期設定，通常設定を行う機能を持ったプロファイル管理サーバ PMS を実装した．**表 5** に PMS の仕様を，**表 6** に今回対象としたプロファイル例について示す．

5.5 ターゲットノード

ターゲットノードでは，Web サーバとして apache [24] を使用し，提案したプロファイル初期設定，通常設定機能を apache と連携する CGI プログラムとして実装した．HTTP 経由で受信したデータを処理してプロファイルを抽出し，レガシープロトコル経由でネットワークカメラに設定できるようにした．評価システムではターゲットノードとネットワークカメラの組合せを 4 セット準備した．

6. 評価

開発した評価システムを用いて，プロファイル初期設定，通常設定機能の性能評価を行った．

表 7 プロファイル初期設定機能の評価結果
Table 7 Evaluation result of profile initialization function.

	STEP1 (sec)	STEP2 (sec)	STEP3 (sec)	合計 (sec)
カメラ 1	0.832	19.708	0.240	20.780
カメラ 2	0.711	19.839	0.260	20.810
カメラ 3	0.451	20.069	0.280	20.800
カメラ 4	0.852	19.688	0.270	20.810
平均	0.712	19.826	0.263	20.801

表 8 プロファイル通常設定機能の評価結果
Table 8 Evaluation result of usual profile setting function.

	STEP1 (sec)	STEP2 (sec)	STEP3 (sec)	合計 (sec)
カメラ 1	0.020	0.070	0.020	0.110
カメラ 2	0.180	0.220	0.010	0.410
カメラ 3	0.020	0.110	0.010	0.140
カメラ 4	0.020	0.090	0.020	0.130
平均	0.060	0.123	0.015	0.198

6.1 目標性能

3 章で設定した性能要件分析の結果をふまえて，今回の評価におけるプロファイル初期設定機能，プロファイル通常設定機能の目標性能について下記のとおり設定した．

3 章で，プロファイル初期設定機能の目標応答時間は，30 秒に設定している．その内容をふまえて，今回の評価では，プロファイル初期設定機能の応答時間の目標性能値を，サーバ：1 秒，ターゲットノード：20 秒に設定した．また，サーバとターゲットノード間の通信時間はターゲットノード側に含めることとした．また，組み込み機器であるターゲットノード上での ID ベース暗号処理は，処理負荷が高くなることが予想されるため余裕時間を 9 秒に設定した．

3 章で，プロファイル通常設定機能の目標応答時間は，1 秒に設定している．その内容をふまえて，今回の評価では，プロファイル通常設定機能の応答時間の目標性能値を，サーバ：0.5 秒，ターゲットノード：0.5 秒に設定した．こちらも，サーバとターゲットノード間の通信時間はターゲットノード側に含めることとした．

6.2 プロファイル初期設定機能の評価

評価システムを用いて，プロファイル初期設定機能の性能評価を行った．プロファイル初期設定機能を以下の STEP1，STEP2，STEP3 の 3 STEP に分割し，各 STEP の処理時間を測定した．

(1) STEP1：PMS での処理
- ID ベース署名，暗号化

(2) STEP2：通信時間を含めたターゲットノードでの処理
- ID ベース復号，署名検証，共通鍵暗号化

(3) STEP3：PMS での処理
- 共通鍵復号

プロファイル初期設定機能の評価結果について**表 7** に示す．

上記評価結果について確認したところ，プロファイル初期設定機能は 20.8 秒かかっており，そのうちサーバの処理時間が 0.98 秒，ターゲットノードの処理時間が 19.8 秒であることが確認できた．

6.3 プロファイル通常設定機能の評価

評価システムを用いて，プロファイル通常設定機能の性能評価を行った．プロファイル通常設定機能を以下の STEP1，STEP2，STEP3 の 3 STEP に分割し，各 STEP についての処理時間を測定した．

(1) STEP1：PMS での処理
- 共通鍵暗号化 × 2

(2) STEP2：通信時間を含めたターゲットノードでの処理
- 共通鍵復号 × 2，HMAC

(3) STEP3：PMS での処理
- HMAC

プロファイル通常設定機能の評価結果について**表 8** に示す．

上記評価結果について確認したところ，プロファイル通常設定機能は 0.2 秒という結果が得られ，そのうちサーバの処理時間が 0.08 秒，ターゲットノードの処理時間が 0.12 秒であることが確認でき，また，本機能はほぼリアルタイムで完了する処理であることが確認できた．

7. 考察

7.1 性能評価に対する考察

6.1 節で設定した目標性能をふまえて，評価結果を確認したところ，使用頻度の低いプロファイル初期設定機能が 20.8 秒（サーバ：0.98 秒，ターゲットノード：19.8 秒），使用頻度の高いプロファイル通常設定機能が 0.2 秒（サーバ：0.08 秒，ターゲットノード：0.12 秒）となっており，どちらも目標性能を達成していることを確認できた．この結果は，3 章で設定した性能要件を満たしていることから，システム構築時とシステム運用時に設定プロトコルを分割した効果を確認できた．

また，本論文では対象としていないが，性能要件の高いプロファイル取得機能，カメラ制御機能についても，プロファイル通常設定機能と同様の方式により，セキュア化の見込みが立ち，これにより，PMS 全機能についてセキュア化の見込みが立った．

7.2 システムのスケーラビリティに対する考察

3 章で，PMS 1 台で管理対象とするネットワークカメラの台数を 100 台に設定したが，性能要件分析において，プ

ロファイル設定機能の同時実行数は，システム構築時は 1，システム運用時は 4 に設定しているため，基本的には 100 台以上となるシステムにも適用可能な方式と考える．

6.2 節の結果より，システム構築時におけるプロファイル初期設定機能については，同時実行数が目標値である 1 に対して 4 までは性能要件を満たしていることが確認できた．

6.3 節の結果より，システム運用時におけるプロファイル通常設定機能については，同時実行数が目標値である 4 まで性能要件を満たしていることが確認できた．ただ，システムの規模が大きくなるにつれ，システム運用時ではアラームイベントの輻輳が発生する確率が高くなるため，この点について考慮していく必要がある．

また，プロファイル取得機能は必要に応じて全カメラに対していっせいにプロファイル取得処理を行うため，システムが大規模になるにつれ，同時実行数が大きくなることが予想される．現状，PMS ではスレッド処理により並行動作に対応しているが，この点について考慮していく必要がある．

7.3 システム運用時のネットワークカメラやネットワークの負荷に対する考察

システム運用時は，ネットワークカメラが稼働中にプロファイル設定処理を行う必要があるが，この際のネットワークカメラやネットワークの負荷について考察する．

ネットワークカメラの負荷については，セキュア化により，通常のプロファイル設定処理に共通鍵復号処理 × 2，HMAC が追加した形となる．表 8 の結果を見ても分かるとおり，セキュア化によるネットワークカメラの負荷向上は，実運用上問題ない範囲であると考察する．

ネットワークの負荷については，プロファイル設定時に，ネットワークで伝送するデータ量は通常のプロファイル設定処理とほぼ変わらないため，セキュア化によるネットワークの負荷向上について，実運用上問題ない範囲であると考察する．

8. おわりに

本論文では，ID ベース暗号を用いてネットワークカメラのプロファイルをセキュアに設定する方式を提案し，その評価システムを開発した．

本開発において，ネットワークカメラの ID としてカメラの MAC アドレスを，プロファイル管理サーバの ID として顧客 ID を使用し，PMS からネットワークカメラの各種プロファイルの設定をセキュアに行う方式を提案した．その結果，プロファイル設定機能を使用頻度と ID ベース暗号の処理負荷を考慮して，初期設定と通常設定の分割し，処理負荷の高い ID ベース暗号処理は初期設定時のみ 1 回実行し，通常の設定機能は共通鍵暗号の MISTY を選択する方針とした．

上記結果に基づき，評価システムを開発し，システムの基本性能について評価を行った．評価結果を確認したところ，使用頻度の低いプロファイル初期設定機能が 20.8 秒，使用頻度の高いプロファイル通常設定機能が 0.2 秒という結果が得られ，有効性について確認することができた．

また，今回ターゲットノードの CPU として採用した ARM 環境はネットワークカメラ以外にも様々な SoC における内蔵 CPU として採用されており，本方式はネットワークカメラ以外にも様々な組み込み機器に広く適用が可能である．

参考文献

[1] 矢野経済研究所：2008～09 年版ビジュアル・コミュニケーションシステム市場 Vol.1 ネットワークカメラ編 (2007).

[2] 三浦健次郎，杉野幸正，阿倍博信：構内デジタルカメラのポリシー制御機能の検討と実装，情報処理学会第 69 回全国大会，pp.3-53–54 (2007).

[3] 山口晃由，山田敬喜，松井　充：ユビキタスセキュリティ—監視映像情報セキュリティ—，三菱電機技報，Vol.80, No.10, pp.631–634 (2006).

[4] Martin, L.: *Introduction to Identity – Based Encryption*, Artech House (2008).

[5] Dierks, T. and Rescorla, E.E.: The Transport Layer Security (TLS) Protocol Version 1.2, RFC5246 (2008).

[6] 電子情報技術産業協会監視カメラシステム WG：監視カメラシステム分野別モデル (2010).

[7] Open Network Video Interface Forum, available from ⟨http://www.onvif.org/⟩.

[8] Open Network Video Interface Forum: ONVIF Core Specification, Ver.1.02 (2010).

[9] CRYPTREC ID ベース暗号調査 WG：ID ベース暗号に関する調査報告書 (2009).

[10] Barreto, P., Kim, H., Lynn, B. and Scott, M.: Efficient Algorithms for Pairing-based Cryptosystems, *Proc. CRYPTO2002*, LNCS 2442, pp.354–368 (2002).

[11] 高島克幸，坂上　勉：ID ベース暗号アルゴリズムと暗号メールシステム，三菱電機技報，Vol.82, No.5, pp.301–304 (2008).

[12] 吉富　基，高木　剛，清本晋作，田中俊昭：BREW 携帯電話でのペアリング暗号の高速実装，情報処理学会研究報告 2006-CSEC-35, pp.19–24 (2006).

[13] 川原祐人，高木　剛，岡本栄司：Java を利用した携帯電話上での Tate ペアリングの高速実装，情報処理学会論文誌，Vol.49, No.1, pp.427–435 (2008).

[14] Boneh, D. and Franklin, M.: Identity based encryption from the Weil pairing, *Proc. CRYPTO2001*, LNCS 2139, pp.213–229 (2001).

[15] Matsui, M.: New Block Encryption Algorithm MISTY, *Proc. Fast Software Encryption Workshop FSE1997*, pp.54–68 (1997).

[16] 若土剛之，阿倍博信，小林信博，中島宏一：映像監視システムにおけるセキュアなプロファイル設定機能の開発，第 8 回情報科学技術フォーラム FIT2009，pp.4-323–324 (2009).

[17] 阿倍博信，若土剛之，中島宏一，小林信博：ID ベース暗号を用いたネットワークカメラ向けセキュアプロファイル設定方式，情報処理学会第 17 回マルチメディア通信と分散処理ワークショップ DPSWS2009，pp.55–60 (2009).

[18] 阿倍博信，若土剛之，中島宏一，小林信博：ネットワーク

カメラシステムにおけるセキュアなプロファイル設定方式，情報処理学会マルチメディア，分散，協調とモバイルシンポジウム DICOMO2010，pp.907–913 (2010).
[19] Josefsson, S. (Ed.): The Base16, Base32, and Base64 Data Encodings, RFC3548 (2003).
[20] Krawczyk, H., Bellare, M. and Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, RFC2104 (1997).
[21] 境 隆一，笠原正雄：楕円曲線上のペアリングに基づく二，三の暗号方式（その 2），電子情報通信学会技術報告 ISEC2002–52, pp.131–138 (2002).
[22] Bellare, M., Namprempre, C. and Neven, G.: Security proofs for identity-based identification and signature schemes, *Proc. Eurocrypt 2004*, LNCS 3027, pp.268–286 (2004).
[23] PostgreSQL, available from ⟨http://www.postgresql.org/⟩.
[24] The Apache Software Foundation, available from ⟨http://www.apache.org/⟩.

阿倍 博信 （正会員）

昭和 63 年慶應義塾大学理工学部計測工学科卒業，平成 2 年同大学院理工学研究科修士課程修了，同年三菱電機株式会社入社．以来，グループウェアシステム，マルチメディア応用システムの研究開発に従事．平成 17 年慶應義塾大学大学院理工学研究科後期博士課程修了．博士（工学）．電子情報通信学会，日本ソフトウェア科学会，映像情報メディア学会，画像電子学会，教育システム情報学会各会員．

若土 剛之

平成 18 年大阪大学基礎工学部システム科学科卒業，平成 20 年同大学院生命機能研究科前期博士課程修了，同年三菱電機株式会社入社．以来，映像や音声を中心とした，メディア処理システムの研究開発に従事．

中島 宏一

昭和 59 年早稲田大学理工学部電気工学科卒業，同年三菱電機株式会社入社．以来，テレビ会議システム，映像監視システム等のマルチメディア応用に関わる研究開発に従事．映像情報メディア学会会員．

小林 信博 （正会員）

平成 2 年早稲田大学理工学部機械工学科卒業，同年三菱電機株式会社入社．以来，情報技術総合研究所で情報セキュリティシステムの研究開発に従事．情報処理学会第 63 回全国大会優秀賞受賞．