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

阿倍 博信[†]，若土 剛之[†]，中島 宏一[†]，小林 信博[†]

本稿では，ID ベース暗号を用いて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安全な設定を実現するプロファイル設定方式について述べる．方式設計にあたり，プロファイル設定処理を ID ベース暗号の処理性能と使用頻度を考慮し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一回実行し，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．

Secure Profile Setting Method for Network Camera using the Identity-Based Encryption

Hironobu Abe[†], Takayuki Wakatsuchi[†],
Koichi Nakashima[†] and Nobuhiro Kobayashi[†]

In this paper, the profile setting method where a safe 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 designing, the profile setting processing 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.

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．特に，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）を機器毎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プロファイル管理システムの開発を行っている[2].

また，監視カメラのネットワーク対応により，入退室管理システム等の関連システムとネットワークを共有したいという要求も高い．この場合，複数のシステムでネットワークを共有する必要があるため，情報漏えい対策が課題となっている[3].

本稿では，上記課題に対応して，ネットワークカメラプロファイル管理システムを拡張し，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安全に設定する方式について述べる．

今回，我々は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からネットワークカメラの各種プロファイルの設定を安全に行う方式を設計し，その結果に基づきネットワークカメラプロファイル管理システムの評価システムを開発した．評価システムを用いてシステムの基本性能を評価した結果，その有効性について確認することができた．

2. 技術課題

従来から広く使用されてきた公開鍵暗号を用いた PKI による暗号化通信では，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り，複雑な運用が必要となっていた．

例えば，組込み機器に予め公開鍵証明書を発行する方式では，各組込み機器の証明書を利用者へ配布する為にディレクトリサーバ等のリポジトリを常時運用させる必要がある．しかし，我々がターゲットとする映像監視システムのネットワークでは，情報漏えい対策に代表されるセキュリティポリシー上の理由により，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ず，プロファイル管理サーバが設定対象とするネットワークカメラの証明書を取得できない恐れがあった．

また，機器内部から証明書を入手する方式の場合，ネットワーク経由では機器と証明書の結びつきが確認できずセキュリティ上の問題であり，オフラインでは多数の機器から証明書を取り出す作業が煩雑なため，利便性やコストの面でマイナスとなる．同様に，個々の機器に個別の共通鍵を手作業で設定する方式の場合も，利便性やコストの面からデメリットが指摘されている．

† 三菱電機株式会社
Mitsubishi Electric Corporation

これに対して ID ベース暗号では，機器に固有の ID を公開鍵として使用できるため，簡易にシステムを構築することが可能である．一般的に ID ベース暗号処理は他の公開鍵暗号処理と比較して演算量が大きくなる，という課題があり，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[4].

今回，組み込み機器であるネットワークカメラに ID ベース暗号を実装するにあたり，ID ベース暗号の処理負荷への対策がポイントとなる．

3. セキュアプロファイル設定方式

3.1 概要

2. で設定した技術課題に対して，ID ベース暗号の適用によるネットワークカメラを対象とする安全なプロファイル設定方式を検討した．具体的には，フェーズ毎に要件分析を行った結果，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に分割し，処理負荷の高い ID ベース暗号処理は初期設定時のみ一回実行し，通常設定機能は処理負荷の高い ID ベース暗号の代わりに共通鍵暗号（MISTY[5] ）を用いる方針とした．以下，各フェーズにおける処理概要について示す．

(1) 工場設定

機器製造時に，工場にて 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ともに，同時に共有鍵の作成，共有，あわせて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 回動作させれば良い．

(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プロファイルの暗号化を行い，ネットワークカメラのプロファイルの設定を安全に行う．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．

3.2 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* からマスターパブリックキー*PKm* と，マスターシークレットキー*SKm* を関数 *SETUP( )* により生成する．

次に，PKG がマスターシークレットキー*SKm*,プロファイル管理サーバ PMS の ID である *IDpms* を入力として関数 *DERIVATIONs( )* により PMS のプライベートキー*SKpms* を生成する．

また，PKG が *SKm*,ネットワークカメラ NC の ID である *IDnc* を入力として関数 *DERIVATIONe( )* により NC のプライベートキー*SKnc* を生成する．

最終的に，PMS には，PKG のマスターパブリックキー*PKm* および PMS のプライベートキー*SKpms* を配布し，NC には，PKG のマスターパブリックキー*PKm* および NC のプライベートキー*SKnc* を配布する．

3.3 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 にてプロファイル初期設定要求を生成し，HTTP/POST 経由にて 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，初期設定処理を行うとともに，その結果を元に応答を作成し，PMS に応答送信する（STEP2）．最後に，PMS にて NC から応答内容に基づき，処理を行う（STEP3）．プロファイル初期設定の流れについて図 1 に示す．

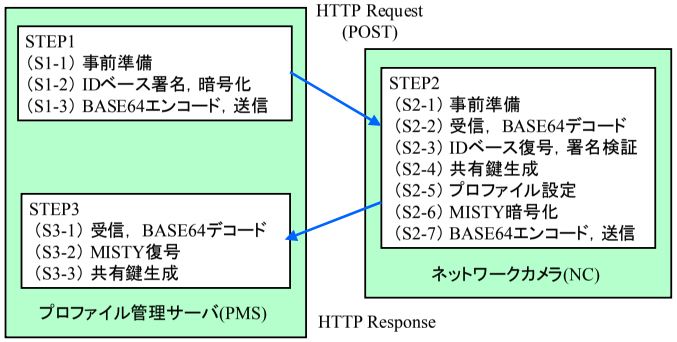

図 1　プロファイル初期設定処理の流れ

以下，STEP 毎に，処理内容の詳細について説明する．

3.3.1 STEP1

（S1-1）事前準備

PMS では，予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 *PROFnc* および NC の *IDnc* 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 *PROFnc* および *IDnc* と結合してメッセージ *M* に設定する．

$$NONCE1 = rand\ (\ ) \tag{1}$$

$$M \leftarrow [\ NONCE1,\ IDnc,\ PROFnc,\ DATE\ ]$$

続いて，マスターパブリックキー*PKm*，PMS のプライベートキー*SKnc*，メッセージ *M* を入力として ID ベース署名関数 *IBsign( )* により署名 *SIGpms* を生成する．

$$SIGpms = IBsign(\ PKm,\ SKnc,\ M\ ) \tag{2}$$

更に，メッセージ *M*，署名 *SIGpms* および PMS の *IDpms* と結合してメッセージ *M'* に設定するとともに，マスターパブリックキー*PKm*，NC の *IDnc* を入力として ID ベ

ース暗号化関数 *IBenc( )* により暗号化データ *Cpms* を生成する．

$$M' \leftarrow [\, M, SIGpms, IDpms \,] \quad (3)$$
$$Cpms = IBenc(\, PKm, IDnc, M' \,)$$

（S1-3）BASE64 エンコード，送信

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

3.3.2 STEP2

（S2-1）事前準備

NC では，製造時の初期値として *DATEinit* が設定されたタイムスタンプ *DATEnc* 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 *Cpms* を取得する．

（S2-3）ID ベース復号，署名検証

暗号化データ *Cpms*，PKG のマスターパブリックキー*PKm*，NC のプライベートキー *SKnc* を入力として ID ベース復号関数 *IBdec( )* によりメッセージ *M'* を復号する．

$$M' = IBdec(\, PKm, SKnc, Cpms \,) \quad (4)$$

続いて，メッセージ *M'* から，メッセージ *M*，署名 *SIGpms*，PMS の *IDpms* を抽出し，ID ベース検証関数 *IBvrf( )* により，PMS の署名を検証する．

$$[\, M, SIGpms, IDpms \,] \leftarrow M' \quad (5)$$
$$IBvrf(\, PKm, IDpms, M, SIGpms \,) \Rightarrow OK/NG$$

（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無いことを確認する為，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 *DATEnc* より新しいことを検証する．

$$[\, NONCE1, IDnc, PROFnc, DATE \,] \leftarrow M \quad (6)$$
$$DATEnc < DATE \Rightarrow OK/NG$$

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 *CKnc* を生成する．そして，受信した *DATE* により *DATEnc* を更新するとともに，プロファイル通常設定で使用する為に *CKnc* を保存する．

$$NONCE2 = rand( ) \quad (7)$$
$$CKnc = KDF(\, NONCE1, NONCE2 \,)$$
$$DATEnc \leftarrow DATE$$

（S2-5）プロファイル設定

受信した *PROFnc* の内容に従い，NC のプロファイル設定を行い，その結果を *RESnc* に出力する．

（S2-6）MISTY 暗号化

PMS の *IDpms*，NC の生成した *NONCE2*，プロファイル設定結果 *RESnc* を結合して応答メッセージ *Mres* に設定する．そして，*NONCE1* と *Mres* 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 *Cnc* を生成する．

$$Mres \leftarrow [\, NONCE2, IDpms, RESnc \,] \quad (8)$$
$$Cnc = MISTY(\, NONCE1, Mres \,)$$

（S2-7）BASE64 エンコード，送信

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

3.3.3 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 *Cnc* を取得する．

（S3-2）MISTY 復号

暗号化データ *Cnc* を STEP1 で生成した *NONCE1* を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 *Mres* を入手する．

$$Mres = MISTY(\, NONCE1, Cnc \,) \quad (9)$$

（S3-3）共有鍵生成

復号された応答メッセージ *Mres* から *NONCE2*，*IDpms*，*RESnc* を抽出し，抽出した *IDpms* と保有する *IDpms* 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 *CKnc* を生成し，プロファイル通常設定にて使用する為に *CKnc* を保存する．

$$[\, NONCE2, IDpms, RESnc \,] \leftarrow Mres \quad (10)$$
$$CKnc = KDF(\, NONCE1, NONCE2 \,)$$

3.4 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，3STEP から構成され，PMS と NC の通信は HTTP/POST 経由となる．プロファイル通常設定の流れについて図 2 に示す．

以下，STEP 毎に，処理内容の詳細について説明する．

3.4.1 STEP1

（S1-1）事前準備

PMS では，予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 *PROFnc* 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 *PROFnc* および *DATE* と結合してメッセージ *M* に設定する．

$$NONCE1 = rand\ (\ ) \tag{11}$$
$$M \leftarrow [\ PROFnc,\ DATE\ ]$$

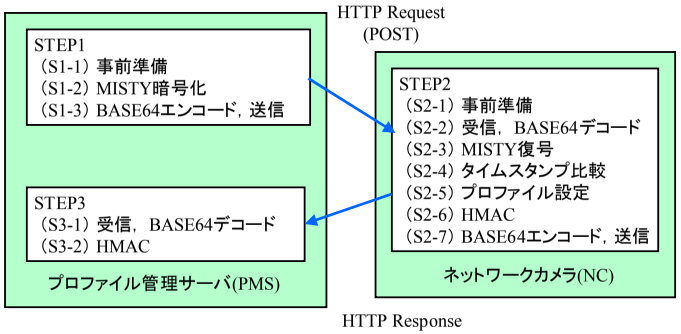

図 2　プロファイル通常設定処理の流れ

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 *Cpms'*を生成する．更に共有鍵 *CKnc* と *NONCE1* を入力として，*MISTY( )* を用いて暗号化データ *Cpms"*を生成する．そして，*Cpms'*と *Cpms"*を結合して暗号化データ *Cpms* に設定する．

$$Cpms' = MISTY(\ NONCE1,\ M\ ) \tag{12}$$
$$Cpms'' = MISTY(\ CKnc,\ NONCE1\ )$$
$$Cpms \leftarrow [\ Cpms',\ Cpms''\ ]$$

（S1-3）BASE64 エンコード，送信

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

3.4.2　STEP2

（S2-1）事前準備

NC では，予めタイムスタンプ *DATEnc* 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 *Cpms* を取得する．

（S2-3）MISTY 復号

暗号化データ *Cpms* を暗号化データ *Cpms'*と暗号化データ *Cpms"* に分割する．そして，プロファイル初期設定にて保存した共有鍵 *CKnc* を用いて暗号化データ *Cpms"* 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．更に，この *NONCE1* を用いて暗号化データ *Cpms'* 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 *PROFnc* および *DATE* を抽出する．

$$[\ Cpms',\ Cpms''\ ] \leftarrow Cpms \tag{13}$$
$$NONCE1 = MISTY(\ CKnc,\ Cpms''\ )$$
$$M = MISTY(\ NONCE1,\ Cpms'\ )$$
$$[\ PROFnc,\ DATE\ ] \leftarrow M$$

（S2-4）タイムスタンプ比較

抽出した *DATE* と *DATEnc* 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 *DATEnc* を更新する．

$$DATEnc < DATE \Rightarrow OK/NG \tag{14}$$
$$DATEnc \leftarrow DATE$$

（S2-5）プロファイル設定

PROFnc 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 *RESnc* 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*, *RESnc* 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 MAC 値 *MACnc* を生成する．

$$NONCE2 = rand(\ ) \tag{15}$$
$$M' \leftarrow [\ NONCE2,\ RESnc\ ]$$
$$MACnc = HMAC(\ NONCE1,\ M'\ )$$

（S2-7）BASE64 エンコード，送信

MAC 値 *MACnc* 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．

$$M'' \leftarrow [\ MACnc,\ M'\ ] \tag{16}$$

3.4.3　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 *MACnc* を抽出する．更に，メッセージ *M'*を分割し，*NONCE2* と *RESnc* を抽出する．そして，*NONCE1* を用いて関数 *HMAC( )* により MAC 値 *MACnc'* を生成し，*MACnc* と *MACnc'* を比較する．比較結果が OK であれば，*RESnc* を確認する．

$$[\ MACnc,\ M'\ ] \leftarrow M'' \tag{17}$$
$$[\ NONCE2,\ RESnc\ ] \leftarrow M'$$
$$MACnc' = HMAC(\ NONCE1,\ M'\ )$$

$$DATEnc = DATEnc' \Rightarrow OK/NG$$

4. 評価システムの開発

4.1 システム構成

図 3 に開発したネットワークカメラプロファイル管理システムの評価システムのシステム構成について示す.

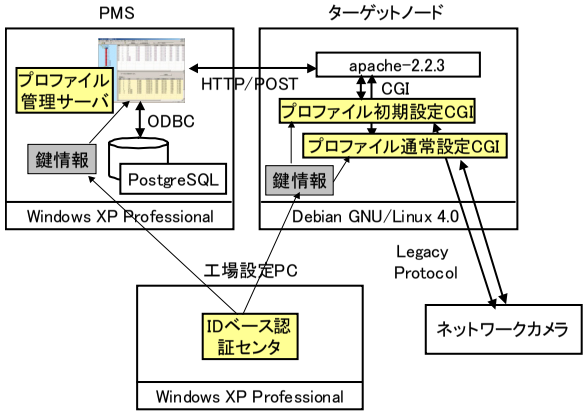

図 3　評価システム構成

評価システムでは，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 性能を持つ組み込み Linux 環境をターゲットノードとして選択し，必要な機能をターゲットノード上に実装した．表 1 にターゲットノードの仕様について示す.

表 1　ターゲットノードの仕様

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

また，PMS 及び工場設定 PC として Windows XP 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.

4.2 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布する機能を実現した.

4.3 PMS

PMS では，各カメラのプロファイルを PostgreSQL にて管理し，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つプロファイル管理サーバを実装した．また，今回設定対象としたプロファイル例について表 2 に示す.

表 2　設定プロファイル例

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

4.4 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 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．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.

5. 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.

5.1 目標性能

プロファイル初期設定機能は，ネットワークカメラの設置時に一回動作させる機能であり，使用頻度が低くかつ応答時間に対する性能要求は低い．そのため，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（プロファイル設定作業時に負担とならない時間）に設定した.

プロファイル通常設定機能は，初期設定後に設定変更を行う毎に動作させる必要がある機能であり，応答時間に対する性能要求は高い．そのため，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（プロファイル設定作業時に負担とならない時間）に設定した.

5.2 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 3STEP 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

・ID ベース署名，暗号化

(2) STEP2：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 3 に示す.

表 3　プロファイル初期設定機能の評価結果

	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

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処理は 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.

5.3 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，プロファイル初期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 3STEP 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：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 4 に示す.

表 4　プロファイル通常設定機能の評価結果

	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

表 4 の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処理は 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，本処理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.

5.4 考察

5.1 で設定した目標性能を踏まえて，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処理時間が 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処理時間が 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満足し，設定プロトコルを分割した効果について確認できた.

6. 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安全に設定する方式を設計し，その評価システムの開発を行った.

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，プロファイル管理サーバからネットワークカメラの各種プロファイルの設定を安全に行う方式を設計した．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一回実行し，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処理が 20.8 秒，使用頻度の高いプロファイル通常設定処理が 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 の搭載 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 4E-2，pp.3-53-3-54 (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 2006 年 10 月号，pp.27-30 (2006).
4)　Luther Martin : Introduction to Identity - Based Encryption, Artech House (2008).
5)　Mitsuru Matsui : New Block Encryption Algorithm MISTY,　Fast Software Encryption Workshop FSE1997,　pp.54-68 (1997).