M2Mにおいてk平均法を用いたグループ鍵管理端末の効率的な配置手法

陳　致豪†　豊田 健太郎†　朴　美娘†　岡崎　直宣‡

†神奈川工科大学
243-0292 神奈川県厚木市 下荻野 1030

‡宮崎大学
889-2192　宮崎県宮崎市学園木花台西 1-1

あらまし スマートグリッドをはじめとしたM2M (Machine-to-Machine)において，安全性のためにデータを暗号化する必要がある．端末の計算量の観点から共通鍵暗号が用いられるが，鍵数の増大のため，階層的に鍵を管理するグループ鍵を用いた手法が検討されている．しかしながら, グループ鍵を管理する端末 (SGM:Sub Group Management node)は通常のセンサよりも高価であることから，センサとの通信範囲などを考慮して最適に配置される必要がある．そこで本研究では, センサ端末の通信量を低減するためにk平均法を用いたSGM配置手法を提案し，その有効性を示す.

An Efficient Group Key Management Devices Deployment Scheme using k-means in M2M

ChihHao Chen†　Kentaroh Toyoda†　MiRang Park†　Naonobu Okazaki‡

†Kanagawa Institute of Technology
1030 Shimo-Ogino, Atsugi-city, Kanagawa 243-0292, JAPAN
‡University of Miyazaki
1-1 Gakuenkibanadai-Nishi, Miyazaki-city, Miyazaki 889-2192, JAPAN

Abstract In M2M (Machine-to-Machine), a symmetric key encryption scheme is suited to encrypt sensory data. Recently, a hierarchical group key management system has been proposed to decrease the number of keys to be managed. However, since group key management devices are more expensive than sensor devices they should be efficiently deployed. In this paper, we propose an efficient group key management devices deployment scheme with k-means clustering algorithm.

1　はじめに

近年，様々な社会基礎産業サービスとしてM2M 通信システムが利用されている．M2M 通信システムは膨大な数のデバイス（センサなど）からデータを収集し分析するシステムである．例えば多種・多様なデバイスによって観測されたデータを，ネットワークを介して収集し，高度な交通管理サービス，防災，監視，在庫管理サービスなどを実現する．しかし，M2M 通信システムには，外部からの攻撃者や中継ノードのなりすましによるデータの傍受・改ざんなどの脅威があり，データの暗号化や送信元確認など機器間での安全な通信が必要になる．

M2M ネットワークは，安価かつ小型であるため計算資源が限られており，暗号化処理に計算量の多い公開鍵暗号方式を用いることは困難である[1]．そこで共通鍵暗号方式を用いたデータの暗号化が必要である．しかし，M2M ネットワークにおいてノード数は非常に多いため，各端末が管理する共通鍵の数を低減する必要がある．そこで LKH（Logical Key Hierarchy）と呼ばれるグループ鍵管理手

法が注目されている[2,3]．他にも，様々なグループ鍵管理手法が提案されている[4~6].

LKH は鍵木と呼ぶ木構造に基づいて，ボトムアップに各ノードのグループ鍵を更新する手法である．ここで各ノードのグループ鍵は，子ノードの鍵を用いて暗号化し，各ノードでの末端ノードに配布する．この手法により，暗号化した鍵のサイズや鍵配布に要する通信回数を削減できるため，効率的に鍵更新を行うことができる．しかし，ノードの離脱のたびにサーバは鍵更新を行う必要があるため，ノード数が多いほど鍵更新回数が増え，サーバの負荷が大きくなる．例えば規模の大きいスマートメータのようなネットワークを考慮した場合，LKH を用いた場合ノードの離脱／新規加入の度に多くの鍵の再配布が必要となる．

そこで，我々は計算資源に余裕があり信頼できる SGM (Sub Group Management)ノードを配置することでグループ鍵の更新時に配布する鍵数を低減させる方式を提案している[7]．そこで本研究では，配置できる SGM ノード数を制限した際に，k 平均法を用いて SGM の配置場所を効率的に決定する方式について検討する．しかし，SGM ノードは一般的なデバイスノードに対して高価であり，また多くのノードと通信を行うため，より効率的な配置を行うことが求められている．これにより，無駄な SGM の配置を避け，各 SGM ノードが配下のノードと通信を行う際に必要とする電力量を低減し，通信距離およびホップ数を改善することが期待される．最後に計算機シミュレーションにより，本方式の有効性を示す.

2　M2M のセキュリティ要求条件

2.1　暗号化方式

M2M 通信システムにおけるデータの暗号化方式には共通鍵暗号方式と公開鍵暗号方式が考えられる．共通鍵暗号方式は，暗号化に伴う処理を高速に行うことができる一方，サーバは各センサノードに対して個別に鍵を用意する必要がある．一方，公開鍵暗号方式を用いた場合，サーバは自身の秘密鍵と公開鍵のみを管理すればよいが，暗号化速度が遅いという欠点がある．

一般的なセンサデバイスは CPU が 4MHz, 512bytes の RAM と ROM，8Kbytes のキャッシュデータ空間と挙げられている[1]．従って計算資源の限られたセンサ端末において，公開鍵暗号方式の利用は不適である．

2.2　グループ鍵管理手法

共通鍵暗号方式を利用する際に，サーバが管理しなければならない鍵数を低減するために，LKH と呼ばれるグループ鍵管理手法が提案されている[2,3]．グループ鍵暗号方式において，サーバはネットワーク全体で共通のグループ鍵を用いてデータを暗号化し，各ノードに送信する．しかし，グループメンバーの加入・離脱のたびにグループ鍵を更新する必要がある．

最も単純なグループ鍵の更新方法として，各ノードにあらかじめ鍵を内蔵させ，それを用いて新しいグループ鍵を暗号化して送信する方式が考えられる．この手法はノード数が N 個の場合に N 回の配布処理が必要となり非効率である．そこで，サーバは各ノードをいくつかの階層によりグループ化し，階層毎にサブグループ鍵を生成する．まず離脱の発生したグループの端末に対しては個別の鍵で暗号化した，末端に最も近い新しいサブグループ鍵を配布する．次にそのサブグループ鍵で暗号化した，上位の階層の新しいサブグループ鍵を配布するという操作を繰り返し行うことで，階層数を d としたとき，$d\log_d n$ 回の処理で全ノードに新しい鍵を配布することが可能となる．

図 1 に 8 個のノードを用いた LKH グループ鍵管理手法の例を示す．図 1 において，末端の灰色の端末はノード N_1~N_8 を表し，各グ

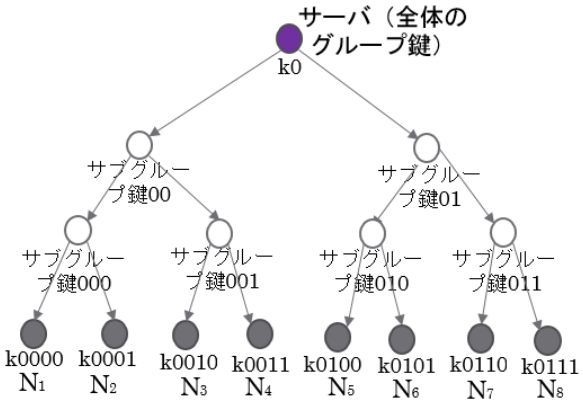

図 1．LKH グループ鍵管理手法

ループの頂点に仮想ノードを設けて，仮想ノードにサブグループ鍵を設ける．

各ノードは自身の鍵と自身が属するサブグループ鍵を持つ．サーバは全てのグループ鍵と全てのノード鍵を管理する．ノード N_1 が離脱する際，ノード N_1 が持っている鍵 k0000，k000，k00，k0 を更新する．

まず新しいサブグループ鍵 k000 を N_1 と同じグループに属していた N_2 の鍵 k0001 で暗号化し，N_2 に送信する．その後，さらに上位のサブグループの新しい鍵 k00 を k000 で暗号し，N_2 に送信する．そして，新しいサブグループ鍵 k00 を鍵 k001 で暗号化し，N3 および N4 にブロードキャストする．最後に全体のグループ鍵 k0 を k00 と k01 でそれぞれ暗号化し，各サブグループに送信する．上記のサーバがブロードキャストするデータの総数は 5 個であり，対称鍵で 1 対 1 に送信する手法と比較して，3 個だけ低減させることがわかる．

LKH と類似の仕組みをスマートメータに適用した手法が提案されている[5]．しかし，この手法はサーバが全てのグループ鍵を作成･管理しているため，サーバの負荷が重い．

Eschenauer 等が提案した EG プロトコル[6]はサーバが事前に要素鍵プールを作成し，鍵プール中の鍵をランダムに各ノードに送信する．そして，ブロードキャストを行う際に，各ノードがランダムに配布された鍵の最適な組み合わせによって，ブロードキャストする．本方式ではサブグループに依存せずに，目的のノードに直接データを送信することが可能であるが，事前に全てのノードに大量の要素鍵を格納する必要がある．また，グループ外のノードがグループ鍵を用いて復号できるという問題もある．金子等[4]はサーバが幾何学的性質を利用することで，単一のメッセージ送信のみで，各ノードに鍵配送を行う方式を提案している．ノードが固有鍵 1 つを持ち，サーバがグループ鍵を配送するノードの数によらず，1 つメッセージのみな容易にグループ鍵を配送ができる．しかしながら，サーバおよびノードの両端末において計算量が多く，解析攻撃に弱いというセキュリティ上の問題もある．

本研究では，安全性が保証されているという観点から，LKH に着目する．しかしながら，上述のように，LKH はサーバの負荷とグループ鍵の更新に時間がかからという問題点がある．そこで， 我々は LKH におけるサーバの負荷とグループ鍵を更新する即時性を改善する手法について検討する．

3　分散型グループ鍵管理手法

3.1　SGM（Sub Group Management）

本論文では，LKH における問題点を解決するために，任意のグループ毎にサーバの役割に代わりの SGM ノードを導入する．SGM ノードは一般的なデバイスノードに対して高価で，コンセントレータのような高計算能力を持つデバイスのため，サブグループ鍵を生成し，グループメンバーを管理することができ，低価格の通信装置を管理する装置である．

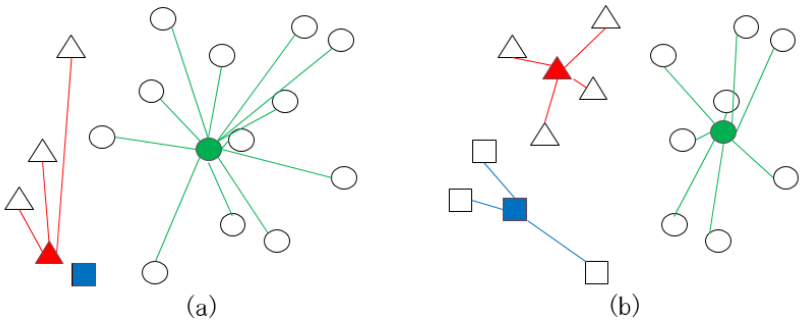

図2. (a) ランダムに3つのクラスタの重心が選択された場合
(b) k平均法によって3つのクラスタの重心が選択された場合

3.2　k 平均法を用いた SGM 配置手法

k 平均法は与えられた n 点を k 個のクラスタに分類するクラスタリングアルゴリズムのひとつである．最初に k 点をランダムに選択し，n 個のノードを k 個のうち最も近傍に位置する点のクラスタに分類する．その後分類された各クラスタの重心までのユークリッド距離の和が極小となるような k 点の位置を得ることができる．

図 2 に，(a)ランダムに 3 つのクラスタの重心が選択された場合と，(b)k 平均法によって 3 つのクラスタの重心が選択された場合の例を示す．図中において，丸，正方形と三角型は各クラスタを示し，色が塗られた記号は各クラスタの重心の位置を示す．ここで白抜きの記号をセンサノード，色で塗られた記号を SGM ノードとみなす．図 2 からわかる通り，k 平均法を用いることにより，センサノードと SGM ノード間の距離を短くすることができ，通信に必要な消費電力を低減できることが期待される．

- **k 平均法を用いた SGM 配置アルゴリズム**

(1) 配置する SGM ノードの数 k を定め，ランダムに k 点の SGM ノードを初期配置する．
(2) 各ノードを自身に一番近いクラスタに所属させる．
(3) 各クラスタの重心を計算し，それらの点に SGM ノードを再配置する．
(4) (2)に戻って繰り返しに計算する．各ノードの所属するクラスタおよび重心に変化がなくなった場合，操作を終了する．

これを利用し，n 点のノードが配置された M2M ネットワークに対し，k 平均法を用いることで得られる k 点に SGM ノードを配置し，各センサノードは自身の所属する SGM ノードクラスタと通信を行う．これにより，各 SGM ノードをランダムに配置した場合と比較し，距離を短くできるため，通信に伴う消費電力量を低減することが可能となる．

3.3　分散型グループ鍵管理手法

図 3 に，3.1 で K 平均法に基づき SGM を配置した分散型グループ鍵管理手法の全体像を示す．サブグループを管理する SGM ノードは，ルータ（コンセントレータ）であり，自身に隣接するノードと共にサブグループを形成する．図中において，S はサーバ，N_1〜N_{12} はセンサノードを示し，SGM ノードは N_1, N_5, N_9 とする．K_i はノード N_i の固有鍵を示す．SGM ノードは予めサブグループ内の全ノードの固有鍵を所持していることを前提とする．

SGM ノードがグループ鍵管理者になることで，各 SGM ノードは子ノードとともに，自身を根とするサブグループを形成する．SGM ノードがグループ鍵管理者になることで，各 SGM ノードは子ノードとともに，自身を根とするサブグループを形成する．そして，サブグループ内でノードの加入・離脱が

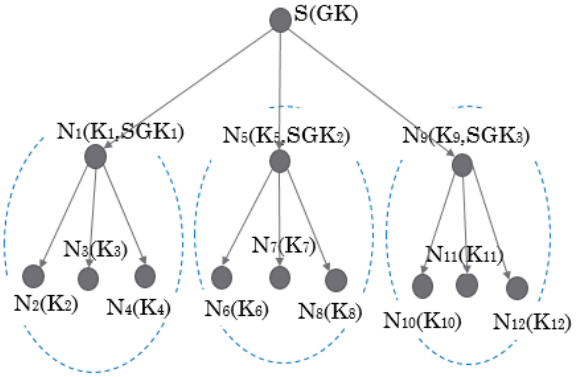

図 3. 分散型グループ鍵管理手法

あった際, サブグループ鍵 (SGK) を作成し, サブグループ内に配布する. サーバは全ノードに一般通信するとき（例えばバージョンアップ）, グループ鍵（GK）で暗号化を行い. 一方, サーバは各サブグループと通信するとき, サブグループ鍵を使用し, 1 対 1 通信するのは各ノードの固有鍵（K_i）を使用する. サーバは, サブグループにデータを送信する前に, グループ鍵を更新し, サブグループ鍵で暗号化し, サブグループ内にグループ鍵を配布する.

センサノードの離脱および新規加入におけるグループ鍵管理について, 以下にそれぞれ述べる. 例えば, 図 3 でノード N_2 が離脱するときの鍵更新プロトコルを図 4 に示す.

● **センサノードの離脱**

(1) SGM ノード N_1 はノードの定時連絡（ビーコン信号）を受信しなかった場合, SGM ノードはノード N_2 の離脱を判断し, 新しいサブグループ鍵（SGK'）を生成する.

(2) SGM ノード N_1 は, 新しいサブグループ鍵（SGK'）をサブグループ内の各ノードに対し, それぞれの固有鍵で暗号化して配布する. 同時に, サーバにそのノード N_2 が離脱したことを伝えるため, 新しいサブグループ鍵をサーバに送信する.

(3) サーバは, 全体用の新しいグループ鍵（GK'）を生成し, SGM ノードに対し, それぞれの新しいサブグループ鍵で暗号化して配布する.

(4) 各 SGM ノードはサブグループに所属する各ノードに自身のサブグループ鍵で暗号化した新しいグループ鍵を送信する.

● **センサノードの新規加入**

(1) 加入するノードはビーコン信号を発信し, それを受信した SGM ノードは応答信号を返信する. 加入するノードは受信した応答信号の受信時刻と信号強度により, 最も近隣に位置する SGM ノードを判断する.

(2) 加入するノードは, (1)で選択した SGM ノードに加入要求を自身の固有鍵で暗号化して送信する.

(3) 加入要求を受け取った SGM ノードは, サーバに加入要求を転送する.

(4) サーバは, 加入要求を復号することにより,

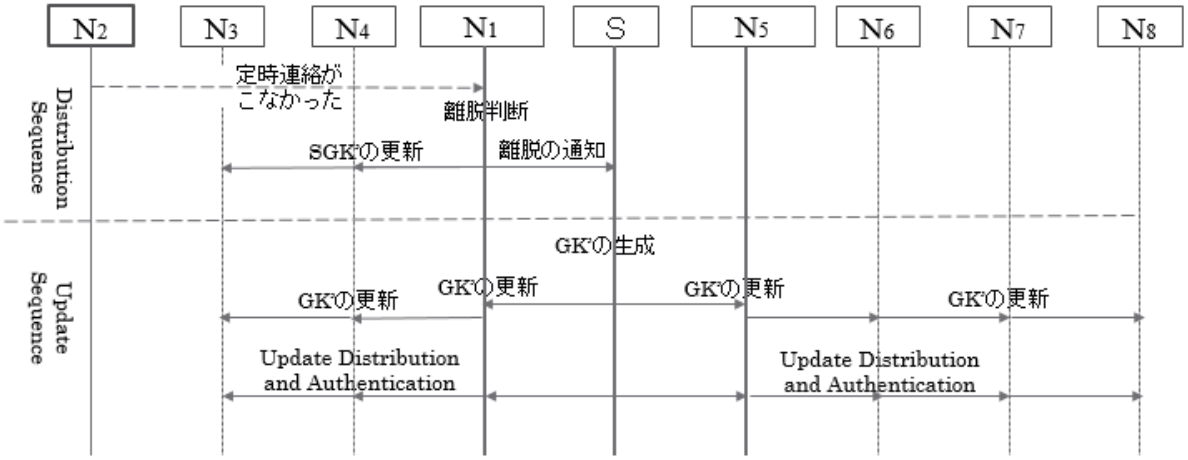

図4. ノードN_2の離脱プロトコル

表 1：SGM ノードのランダム配置と k 平均法を用いた通信距離の比較

センサ ノード数	SGM ノード数	ランダム配置		k 平均法配置	
		距離の二乗和 平均値	標準偏差	距離の二乗和 平均値	標準偏差
1,000	10	359.775	345.2511	165.1883	109.2805
	100	30.888	29.18382	14.14284	12.52476
5,000	10	392.8678	362.9496	170.5069	107.9234
	100	36.2246	40.05011	16.51841	12.24052
10,000	10	385.6642	393.4227	169.2803	110.3956
	100	39.7515	48.44475	16.45647	11.11673

シミュレーションの仮想環境は 100x100 平方メートルの正方形地域

加入ノードの正当性を判断し, 加入するノードの固有鍵を加入先の SGM ノードの固有鍵で暗号化し, SGM ノードに送付する.

(5) SGM ノードは，暗号化されたノードの固有鍵を自身の固有鍵で復号し, 加入するノードの固有鍵を取得する.

(6) SGM ノードが SGK を更新する手順は次のように 2 つに分けられる.

(i) SGK を更新しない場合（加入）

(1) SGM ノードは，現在使用しているサブグループ鍵をそのノードの固有鍵で暗号化し配布する.

(2) グループ鍵について同様に送る.

(ii) SGK を更新する場合（加入）

(1) SGM ノードは，新しいサブグループ鍵（SGK’）を生成し，加入したノードを含む サブグループ内の各ノードに対し，それぞれの固有鍵で暗号化して配布する.

(2) SGM ノードは，サーバにノードが加入したことを通知すると共に新しいサブグループ鍵をサーバとの固有鍵で暗号化して送る.

(3) センサノードの離脱 (3) と (4) . □

SGM ノードを導入することにより, サーバはデータ送信時にグループ鍵を更新するだけで良いため，ノードの加入・離脱が頻繁に行われても，サーバが処理しなければならない処理を低減することが可能となる.

4 評価

表 1 に, SGM ノードをランダムに配置した場合と k 平均法を用いた際の，各センサノードと自身に最も近い SGM ノードまでの距離の二乗の平均およびその標準偏差を示す．距離の二乗で評価を行った理由として，送信電力は距離の二乗に比例して減衰するためである.

本シミュレーションにおいて，シミュレーションエリアは 100m×100m とし，センサノードはいずれの方式に対してもランダムに配置する. センサノード数を 1,000, 5,000, 10,000 と SGM ノード数を 10 と 100 で行った．表 1 より，k 平均法を用いた場合，いずれの SGM ノード数の組み合わせにおいても，約 55%の低減となることがわかるため, SGM 通信に必要な消費電力を低減できる.

そして，ネットワーク内にノードが離脱／加入することと比べて鍵更新の容易性は SGM ノードが提案したため, 通信の回数も低減して，新たなサブグループが必要な場面が想定される．従来の LKH 手法はサブグループ鍵により, 効率にグループ鍵を更新するが, ノードの離脱／加入するとグループ鍵まで更新する必要がある．これに対して，提案手法は SGM ノードがマルチホップ数を減少する

表 2：LKH との比較

	LKH 方式[1]	提案方式
サーバの通信回数	$d\log_d n$	1
SGM の通信回数	-	n/m
グループ鍵更新の通信回数	$d\log_d n$	1+ (n/m)
SGM の鍵管理数	-	2+ (n/m)
ノードの鍵管理数	d	3

n: number of group member, d: number of degree, m: number of SGM

同時に，無駄なグループ鍵更新回数を抑えることもできるため，提案方式では，グループ鍵の変更を容易に行えると言える．さらに，LKH はノード数が多いほど, 鍵が配布しにくくなる．提案手法は SGM ノードの導入することにより，サブグループ鍵を即時かつ効率的に更新できる上で，k 平均法により，LKH 管理に対して，通信回数も軽減できる．

本研究での提案方式は M2M 通信システムにおける鍵管理サーバの負荷集中の低減と鍵更新時間の短縮を目的とし, SGM でサーバの負担を軽減し，表 2 に，鍵管理数および再通信回数の有無に LKH 方式と提案方式について比較を行う. LKH の通信回数は鍵木の深さに依存し, グループ鍵の更新回数は $d\log_d n$ である．一方，提案手法はサーバがグループ鍵の生成と配布を担当しないため，通信回数は 1 回であり, 各ノードを管理する SGM ノードの通信回数の (n/m)との和となるため，1+ (n/m) になる．また，LKH 方式の各ノードは鍵木の深さと等量のグループ鍵，サブグループ鍵および自身の固有鍵を管理するため，管理すべき鍵数は木の深さ d と等しい．一方，提案手法の各ノードはグループ鍵，自身が属するサブグループの鍵，自身の固有鍵の 3 つのみを管理するばよい.

これらのことから，k 平均法を用いて SGM ノードを配置することにより，再送処理および通信回数を改善できることが期待される．

5 まとめ

本研究では，M2M 通信システムで安全で効率的な鍵管理のための分散型グループ鍵管理手法について提案した．各 SGM ノードは多くの配下のセンサノードと通信する必要があるため，通信距離を短くするように配置される必要がある．そこで k 平均法を用いて SGM ノードの配置位置を決定する方式を提案する．計算機シミュレーションにより，ランダムに SGM ノードを配置した場合と比較して k 平均法を用いることにより約 55%だけ通信距離を低減することを明らかにしたため, 容易にグループ鍵を配送することができ, M2M 通信ネットワークに適したものとなっている．

今後の課題としては，ネットワークシミュレータを用いて実際に SGM ノードの消費電力がどの程度低減されるかを明らかにする．

参考文献

[1] Perrig A, Szewczyk R, Tygar J.D., Wen V, Culler D.E,“SPINS:Security Protocols for Sensor Networks,” Wireless Network Journal, pp.521-534, 2002.

[2] C.K. Wong, M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” IEEE/ACM Trans. Netw., vol. 8, no.1, pp.16-30, 2000.

[3] 土江 康太, 楫 勇一“センサネットワークにおける LKH グループ鍵配送について,” 第 31 回暗号と情報セキュリティシンポジウム(SCIS2014), 3D5-4, pp.1-8, 2014.

[4] 金子 良, 岩村 恵市“センサネットワークに適したグループ鍵配送方式の提案,” 第 32 回暗号と情報セキュリティシンポジウム誌(SCIS2015), 3B3-3, pp.1-6, 2015.

[5] 花谷 嘉一, 上林 達, 大場 義洋 “M2M 通信システム向けグループ鍵管理技術,” 東芝レビュー, 69(1), pp.14-17, 2014.
[6] 村上大樹, 双紙正和“ワイヤレスセンサネットワークにおけるグループ鍵分配プロトコルの考察,” 第 48 回コンピュータセキュリティ研究会(CSEC), No.27, pp.1-8, 2007.
[7] 陳 致豪, 喜多 義弘, 朴 美娘 “安全な M2M 通信システムのためのグループ鍵管理手法に関する一検討, ” 情報処理学会第 77 回全国大会(IPSJ2015), 6W-01, pp.1-2, 2015