M2M通信システム向けグループ鍵管理技術

Group Key Management Technology for Machine-to-Machine Communication Systems

花谷　嘉一　■HANATANI Yoshikazu
上林　達　■KAMBAYASHI Toru
大場　義洋　■OHBA Yoshihiro

東芝は，センサやスマートメータなど自立して他の機器と情報のやり取りを行うM2M（Machine to Machine）機器をインターネットプロトコルを利用して有機的に接続できる通信システム（M2M通信システム）の研究開発を行っている。スマートコミュニティなど，数多くのM2M機器から構成される大規模なM2M通信システムにおいては，通信量を抑えるため，一度に複数の機器に対して送信できるグループ通信技術が不可欠な要素技術となる。

当社は，グループ管理を容易にするグループ通信技術を開発し，IEEE 802.21d（電気電子技術者協会規格 802.21d）の標準化を検討する委員会において国際標準規格の策定を推進している。

Toshiba has been engaged in the research and development of technologies for machine-to-machine (M2M) communication systems that can organically connect various types of M2M devices including smart meters by means of the Internet Protocol (IP). To construct a large-scale M2M communication system consisting of more than 1,000 M2M devices, a group communication technology to maintain interoperability among multiple vendors' products is essential.

With this as a background, we have been participating since 2012 in the Institute of Electrical and Electronics Engineers (IEEE) 802.21 Task Group d in order to provide an efficient and secure group key management system for large numbers of M2M devices, and are actively promoting the standardization of IEEE 802.21d as a key specification for M2M group communication.

1　まえがき

スマートメータをはじめとするセンサ機器など，処理の途中で人が介在しないM2M（Machine to Machine）機器においては，インターネットプロトコルを利用して有機的に接続できる通信システム（M2M通信システム）が不可欠である。

東芝は，1,000台以上のM2M機器から構成される大規模M2M通信システムの構築に不可欠な要素技術として，グループ通信技術の研究開発を行っている。グループ通信は，同一の情報を複数の機器から構成される機器グループに対して一斉に配信する通信（マルチキャスト通信）技術であり，個別に配信するユニキャスト通信と比べて，配信時間の短縮とネットワーク負荷の低減が期待される。更に，ルーティングやネットワークアクセス認証など，M2M通信システムを構成する他の技術要素と同様に，グループ通信においてもマルチベンダー間の相互接続性を維持することが重要になる。

当社は，著作権保護技術を応用し，多数のM2M機器を効率的かつ安全に管理するためのグループ管理技術を開発し，2012年からIEEE 802標準化委員会において，M2Mグループ管理規格であるIEEE 802.21dの標準化に積極的に取り組んできた[1]。

IEEE 802.21dは，多数のM2M機器を効率的かつ安全に管理する機能を提供する国際標準規格である。提供される機能は，M2M機器グループを動的に生成，更新，及び削除するグループ操作機能，並びに生成されたグループに属するM2M機器を一括操作するグループコマンド機能である。

ここでは，当社がM2M通信システム向けに開発したグループ鍵管理技術と，国際標準規格の概要について述べる。

2　効率的で安全なグループ鍵管理技術

M2M機器をグループで管理することにより，膨大な数のM2M機器であっても，効率的な運用と制御が可能になる。管理者が機器グループを指定する方法として，グループに所属する機器（グループメンバー）にだけグループ鍵（GK：Group Key）を配布する方法がある。この方法では，既に存在する機器グループであっても，新しいGKをグループメンバーとする機器に送付することで，グループメンバーの動的な変更を行うことができる。

一方，GKが第三者に漏えいすると，その鍵を利用してメンバーでない者がグループに参加するおそれがある。そのため，GKをグループメンバー以外から秘匿し，安全に配布する必要がある。しかし，グループメンバーが個別に持っている鍵を単純に使って，GKを暗号化して送付する方法では，グループメンバーの数が膨大となったときに通信量が多くなり，対応が困難である。

当社は，マルチキャスト通信に著作権保護技術を応用したGKブロック（GKB：Group Key Block）と呼ばれる鍵配布方法

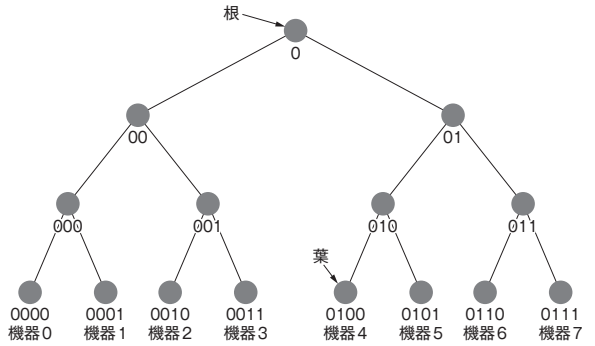


図1．機器数8の管理木の例 — 機器数が8の場合の管理木で，各ノードにインデックスと鍵が割りふられている。

Example of management tree for eight devices

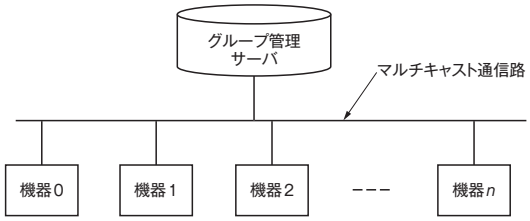


図2．M2Mシステムモデル — グループ管理サーバと各機器が，マルチキャスト通信路で結ばれているシステムを想定している。

Newly developed system model based on group key block (GKB)

により，前記の課題を解決できる独自のGK管理技術を開発した。

2.1 GKB

GKBは，Blu-ray Disc™ (注1)で採用されている著作権保護技術（AACS：Advanced Access Control System）[2]でも使われている鍵管理技術で，機器の無効化機能を備えることを特徴とする。

GKBの実現法の一つであるCS（Complete Subtree）法では，グループメンバーとなりうる全てのメンバーを**図1**のような二分木構造の管理木で管理する。管理木の各ノードには，ノードを識別するためのインデックスと鍵が割りふられている。例えば根にあたるノードには，インデックス0と鍵k0が割りふられるとする。

各メンバーには，各々固有の葉が割り当てられ，根から葉への経路上のノードに割りふられたインデックスと鍵の組をデバイス鍵として保持する。例えば，図1の機器2はデバイス鍵として（(0,k0)，(00,k00)，(001,k001)，(0010,k0010)）の四つの鍵を持っている。

グループを生成するときには，GKを生成するとともに，グループに所属させるメンバーに対応した葉だけを含む部分木の根を求め，それに対応するノード鍵でGKを暗号化することによりGKBを求める。例えば，機器0，機器1，及び機器4をグループメンバーとする場合，k000とk0100でGKをそれぞれ暗号化し，暗号文の組をGKBとする。このようにすることで，機器0，機器1はk000で暗号化されたGKを，機器4はk0100で暗号化されたGKをそれぞれのデバイス鍵で復号することによって，特定のデバイス鍵を保持するメンバーだけにGKを送信でき，かつ，個別に暗号化したGKを送信するよりもデータサイズを抑えることができる。

（注1） Blu-ray Disc™，Blu-ray™は，ブルーレイディスクアソシエーションの商標。

CS法によるGKBは，次の三つのアルゴリズムで構成されている。

(1) GKB_Setup　管理対象となるメンバーの総数nを入力として，管理木と各メンバーのデバイス鍵の集合を出力する。

(2) GKB_Enc　管理木とグループメンバーのデバイス鍵を入力とし，GKとGKBを出力する。

(3) GKB_Dec　GKBとデバイス鍵を入力として，GK又は無効との判定結果を出力する。

2.2 グループ操作法

ここでは，GKBを用いてグループメンバーを変更する方法（グループ操作法）について述べる。グループ操作法では，**図2**のように，コマンドを発行するグループ管理サーバとそれを処理する機器が，マルチキャスト通信路で結ばれるシステムモデルを想定している。この方法のグループ操作コマンドは，グループの新規生成，既存グループの削除，及び既存グループのメンバー構成の変更といったグループ操作を動的に実行できる。

GKBの性質により，このグループ操作コマンドからは，グループ管理サーバにより指定された機器だけがGKを取り出せるため，グループに属すべきでない機器にコマンドが届く状況においても，GKをグループに属する機器だけに配布できる。

2.2.1 グループ操作コマンドの発行　グループ操作のためのコマンドの発行は，管理木，全てのデバイス鍵，及びグループに加えるメンバーの識別子を入力として，次の手順でグループ操作コマンドを生成することで行う。

(1) 機器グループ識別子（GID）を決定する。

(2) グループに属する全てのメンバーの識別子（グループメンバー識別子）を特定する。

(3) 管理木と，グループメンバーのデバイス鍵をGKB_Encに入力し，GKとGKBを求める。

(4) GIDとGKBをグループ操作コマンドとして，マルチキャスト通信で各機器に送付する。

2.2.2 グループ操作コマンドの処理　グループ操作コマンドが発行されると，それを受信した機器は，機器固有の

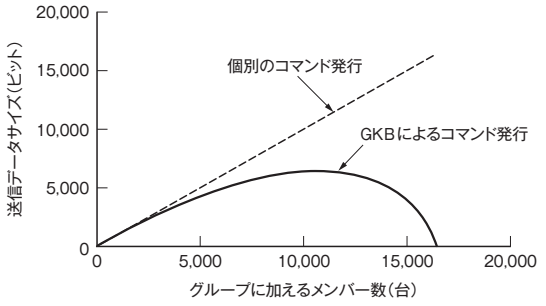


図3．グループ操作コマンドのデータサイズ ― グループに加えるメンバーをランダムに選択した際のグループ操作コマンドのデータサイズを，シミュレーションにより求めた結果である。

Superiority of data size of group manipulation command in newly developed system

デバイス鍵を用いて，次の手順でGKを計算する。

(1) グループ操作コマンドをGIDとGKBに分ける。

(2) GKBと自身のデバイス鍵をGKB_Decに入力し，GK又は無効との判定結果を得る。

(3) 以下の各場合に応じて，グループへの所属や離脱を決定する。

(a) グループに所属していない状態で，そのグループのGKを得た場合，グループに所属するように記録

(b) グループに所属している状態で，そのグループのGKを得た場合，グループに所属するように記録を更新

(c) グループに所属している状態で無効との判定結果を得た場合，グループに所属しないように記録

2.2.3 実験結果 グループ操作法により発行されるコマンドの送信データサイズを，シミュレーションにより求めた結果を**図3**に示す。

このシミュレーションでは，メンバーの総数を16,384台とし，ランダムに選択したn台のメンバーをグループに加えるコマンドのデータサイズを評価した。縦軸は送信データサイズで，横軸はグループに加えるメンバー数である。図3において，実線はGKBによるコマンドのデータサイズを表し，破線は個別にGKを配布するコマンドのデータサイズを表す。グループに加えるメンバー数が増えるに従って，GKBによるグループ操作法のほうがより効率的であることが確認できた。

シミュレーションの結果は，グループに加入したり離脱する機器をシステム構築時にいっさい予測できないというもっとも厳しい状況においても，グループ操作法が効果的であることを示している。

3 IEEE 802.21dへの応用

2章で述べたグループ操作法は，無線通信において受信すべき機器グループの管理法（マルチキャストグループ管理法）として，IEEE 802.21d委員会で議論されている。

IEEE 802.21dは，異種網間ハンドオーバ（MIH：Media Independent Handover）規格化グループのIEEE 802.21ワーキンググループ（WG）に属するタスクグループd（TGd）を指す。MIHとは，ある通信方式のアクセスポイントと通信中のデバイスの接続先を，異なる通信方式のアクセスポイントに変更する処理（ハンドオーバ）を指す。IEEE 802.21dの親規格であるIEEE 802.21 Std-2008[3]は，MIHをシームレスに実現するために，近接ネットワークの情報，リンク状態の早期通知，及びネットワーク又は通信ノードの能力といった機器のハンドオーバに先立って必要となる情報を，それらの情報を提供する機器（PoS：Point of Service）からハンドオーバする機器に提供する機能を定義している。MIHを用いることで，実行中のアプリケーションに影響を与えることなく，通信方式に依存しないアクセスポイントの変更を実行できる。

IEEE 802.21の通信方式への非依存性は，アクセス網が無線マルチホップや，PLC（Power Line Communication），携帯電話網など複数種類の通信方式から構成される，AMI（Advanced Metering Infrastructure）のような異種網統合システムに対しても有効である。

IEEE 802.21dは，IEEE 802.21 Std-2008をマルチキャスト通信に対応するよう拡張した規格で，安全なグループ管理機能を提供する。以下に，IEEE 802.21dが想定するユースケースと，セキュアなグループ管理機能の概要を述べる。

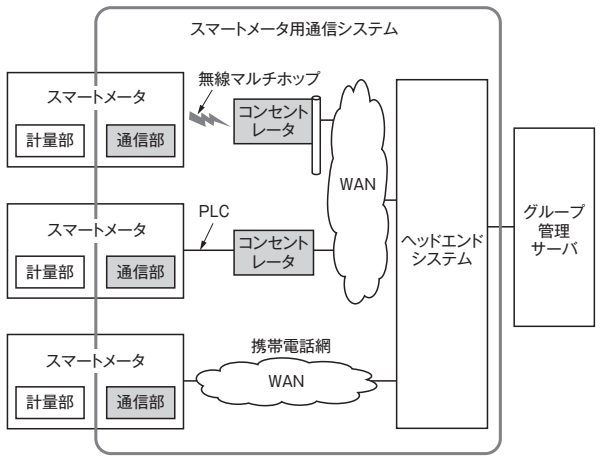
3.1 IEEE 802.21dの適用例

IEEE 802.21dを用いると，膨大な数の機器に対して動的にグループを設定でき，グループで管理される多くの機器に対して，ハンドオーバや機器へのコマンドの送付を効率的に行うことができる。ここでは，**図4**に示すようなAMIシステムにおけるIEEE 802.21dの適用例について述べる。

スマートメータは，無線マルチホップ，PLC，及び携帯電話網の3種の通信方式を用いて，コンセントレータなどの中継器を経て，ヘッドエンドシステムなど上流のシステムに接続される。コンセントレータには，数多くのスマートメータが接続されている。ヘッドエンドシステムは，スマートメータから消費電力情報を受け取ったり，スマートメータへの制御命令を発行したりするなど，スマートメータ群を管理する機能を備えている。

IEEE 802.21dを用いることで，状況に応じて，数多くのスマートメータに対して効率的かつ安全にグループを設定できる。このグループを利用することで，次のようなことが可能になる。

3.1.1 コンセントレータの負荷分散 スマートメータの新規設置や周辺環境の変化などが要因となり，特定のコンセントレータへの通信負荷が増大する状況が考えられる。この場合，過負荷のコンセントレータに接続されるスマートメータのグループに対して，別のコンセントレータへのハンドオーバを命じること



WAN：Wide Area Network

図4．AMIシステムの構成例 ― スマートメータは，コンセントレータをアクセスポイントとし，複数の通信方式でヘッドエンドシステムと接続される。

Example of architecture of advanced metering infrastructure (AMI) system applying IEEE 802.21d

で，その負荷を軽減できる。

3.1.2　コンセントレータの障害迂回（うかい）及び復旧

コンセントレータの故障や保守作業など周辺環境の一時的な変化により，一定期間にコンセントレータが使用不能になる状況が考えられる。このとき，そのコンセントレータに接続されているスマートメータのグループを，一時的に別のコンセントレータにハンドオーバし，コンセントレータが使用可能になったら元のとおりにハンドオーバできる。

3.1.3　スマートメータのファームウェアのアップデート

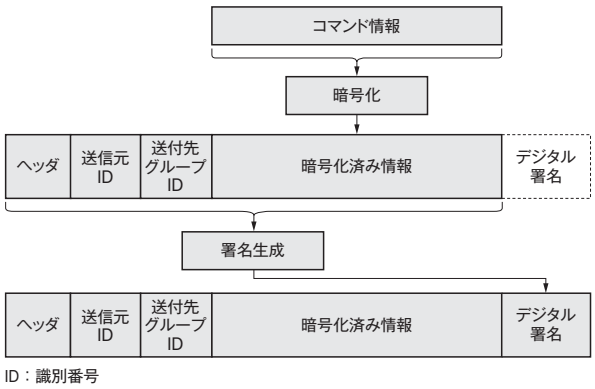
ファームウェアは，スマートメータの機種や既にインストールされているファームウェアのバージョンに応じて，適切に更新されなければならない。更に，安全性の観点では，ファームウェアは第三者から秘匿されることが望ましい。機種と現在のファームウェア バージョンによってスマートメータをグループに分け，そのグループごとにファームウェアを暗号化することで，安全かつ効率的にファームウェアを配布できる。

3.2　IEEE 802.21dにおけるコマンド保護の仕組み

IEEE 802.21dでは，2.2節のグループ操作法を用いてGKを配布するコマンドと，配布されたGKによるその他のコマンドの保護方法が定義されている。ここでは，コマンドの保護方法について述べる。

図5は，マルチキャスト通信路を介して送付されるコマンドに対し，IEEE 802.21dで提供される保護を示したものである。

配布されたGKを用いて各コマンドに特有のコマンド情報を暗号化することにより，グループメンバー以外のメンバーに対してコマンド内容を秘匿する。更に，コマンドに対して発行元のデジタル署名を付すことで，コマンドの正当性を検証できるようにしている。



ID：識別番号

図5．マルチキャストコマンドの保護方法 ― マルチキャストされるコマンド内容は暗号化され，発行者を検証するためのデジタル署名が付される。

Protection mechanism for multicast commands

4　あとがき

GKによる効率的かつ安全なグループ管理技術と，異種網間ハンドオーバの標準規格であるIEEE 802.21dへの応用について適用例を含めて述べた。この技術を用いることで，膨大な数のM2M機器を安全かつ効率的に管理できる。

今後は，GKの適切な更新を含めて安全性を高めた技術を開発し，AMIシステムをはじめ，多くのセンサから成るシステムへの応用を目指す。

文　献

(1) IEEE P802.21d. "IEEE 802.21 Task Group d (TGd)". IEEE 802 homepage. <http://www.ieee802.org/21/TGd.html>, (accessed 2013-12-19).
(2) AACS LA. "AACS Specifications". <http://www.aacsla.com/specifications/>, (accessed 2013-12-19).
(3) IEEE 802.21:2008. IEEE Standard for Local and metropolitan area networks - Media Independent Handover Services.

花谷　嘉一　HANATANI Yoshikazu, Ph.D.
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー，博士（工学）。暗号・情報セキュリティ技術の研究・開発に従事。日本応用数理学会，IACR（国際暗号学会）会員。
Computer Architecture & Security Systems Lab.

上林　　達　KAMBAYASHI Toru
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー研究主幹。セキュリティ技術の開発に従事。
Computer Architecture & Security Systems Lab.

大場　義洋　OHBA Yoshihiro, D.Eng.
研究開発センター ネットワークシステムラボラトリー研究主幹，博士（工学）。スマートグリッド・スマートコミュニティシステムの国際標準化業務に従事。IEEE会員。IEEE 802.21 TGd議長。
Network System Lab.