情報量的安全性に基づくリアルタイム通信向け認証方式

Information-Theoretic Authentication Scheme for Real-Time Communication

片山　茂樹　　福嶋　和人　　関口　勝彦

■ KATAYAMA Shigeki　■ FUKUSHIMA Kazuto　■ SEKIGUCHI Katsuhiko

電力や交通など重要な社会インフラでは，情報ネットワークを活用することが増えつつあり，情報セキュリティ対策の重要性が高まってきている。一方，社会インフラ向け制御システムでは，リアルタイム性及び長期のメンテナンス性を考慮することが重要である。

東芝は，このような要件に応えるため新たな認証方式を開発した。この方式は，一般の情報システムで広く用いられている計算量的暗号と異なり，情報量的安全性に基づく認証タグを付加することでメッセージの認証を行う。この方式を電力系統の保護リレーシステムに適用して，期待どおりに動作することを確認した。

With the increasing dependence on information networks in social infrastructures such as power systems, transportation systems, and so on, safeguarding the security of information is now a crucial issue. In particular, a new security-enhancement technology with real-time responses and long-term maintenance of protection from threats and attacks is required to protect the control systems of these social infrastructures.

Toshiba has developed an authentication method that effectively applies information-theoretic cryptography to such real-time communication systems. Our method features a novel scheme based on unconditionally secure authentication codes (A codes) having short authenticators (authentication tags) and a feasible number of keys. We have developed a data format for the scheme, and confirmed its effectiveness through experiments using a protection relay in an electric power system.

1　まえがき

電力や交通など重要な社会インフラでも情報ネットワークが活用され，その依存度は増してきている。これに伴い情報セキュリティの確保の重要性は高まっている。このような社会インフラ向け制御システムの通信の特徴として，リアルタイム性や長期のメンテナンス性などが挙げられる。情報セキュリティの要件として情報の秘匿性（Confidentiality），一貫性（Integrity），可用性（Availability）などがあるが，社会インフラ向け制御システムが行うリアルタイム通信では，一貫性，特にメッセージ認証(注1)が重要であることは周知である。

そこで東芝は，長期にわたって安全なセキュリティを確保することを目的として，リアルタイム通信向けの認証方式を開発した。ここでは，その認証の方式と，一例として社会インフラ向け制御システムの一つである電力系統の保護リレーシステムに適用し，評価した結果について述べる。

2　情報セキュリティの安全性

情報セキュリティの実現手法は，計算量的安全性に基づく手法と，情報量的安全性に基づく手法の大きく二つに分類することができる。このうち，DES（Data Encryption Standard）やHMAC（Keyed-Hashing for Message Authentication Code）などに代表される計算量的安全性に基づく手法は，情報通信の分野で広く使われている。しかしこれらの手法は，計算機がその手法の核となっている計算問題を解くのに要する時間によって安全性を保証しているため，計算機性能が向上したり，問題をより高速に解くアルゴリズムが発見されると安全性の保証が困難になる。

一方，情報量的安全性に基づく手法はシャノンの情報理論に端を発している[1]。安全性はあらかじめ設定するパラメータによって明確に保証でき，計算機性能の向上や新しいアルゴリズムの発見には影響されない。ところが情報量に基づいたセキュリティ技術はこれまでのところあまり実用化されていない。その理由は，この技術に大量の鍵データが必要となるからである。

情報量的セキュリティ技術の代表例としてはワンタイムパッドがある。この方式では，メッセージを暗号化するために，メッセージと同じ大きさの暗号鍵を1回だけ使う。ワンタイムパッドは，暗号解読が不可能であることがシャノンによって証明されている反面，大きな暗号鍵が必要になる。

（注1）　メッセージの一貫性の保証で，セキュリティ攻撃によりメッセージが変更されていないことを保証するための手続き。

3　保護リレーシステムへの情報量的セキュリティ技術適用

ここでは，電力系統の保護リレーシステムを例に，開発した認証方式の社会インフラ向け制御システムへの適用について述べる。

3.1　保護リレーシステムの概要

発電した電力を利用するためには，発電所，送電線，変電所，配電線，受電設備及び電気利用設備などすべての電力設備を電気的に相互に連携して結ぶ必要がある。このような電気的ネットワークを電力系統と呼び，巨大なシステムが形成されている。しかし電力系統の各種設備は，雷や台風襲来などの自然災害あるいは火災，山火事などの人災にさらされている。保護リレーシステムは，これらの設備で故障が発生した際に，故障設備を電力系統から短時間内に切り離すことで故障の波及を防止したり範囲を限定する（**図1**）。

最近の保護リレーシステムでは通信を利用する場合が多く，その代表的なものとして送電線電流差動リレー方式がある。この方式では，保護対象とする送電線の両端の変電所に設置された保護リレー装置が自端子で検出した送電線の電流値をディジタル化して取り込み，2 ms以下の周期で相互に同期をとってこの電流データを送り合っている。そして，自端子と相手端子の電流を比較することで，送電線に事故が生じたことを精度よく高速に検出している。例えば雷事故が発生した場合に，リレー装置は通常数十 ms 以内に事故を検知する。

3.2　情報量的安全性に基づくメッセージ認証

従来，前述の電流データなどの保護演算用データを運ぶ伝送路は専用線であったが，今後はイーサネットに代表されるより汎用性の高いものに置き換えられ，より広範囲の通信接続が実現されていく可能性がある。また，電力会社が電力系統及び専用通信インフラを統合的に管理し運用しているわが国と違って，海外では電力系統と通信が異なる企業によって運用される場合がある。これらのことから，今後はこの分野でも情報セキュリティの関心が高まっていくと考えられる。

保護リレーシステムの通信内容は，時々刻々と変わる電流・電圧データが主である。情報セキュリティの要件を考えると，これらを盗聴しても利用価値は少ないが，データの改ざんやなりすましによる保護リレーの誤動作あるいは誤不動作は回避しなければならない。このことから，認証の機構は必要であるが，データ秘匿機構の必要性は低いと言える。

一方リレー装置は，信頼性を保つために装置内のアルゴリズム変更が容易に行えない組込みシステムであり，計算能力が限定されるなどの制約がある。更に，長期間（例えば15年）無停止での運用が課せられており，稼働率を下げられない。また伝送路は狭帯域の場合も多く，更に保護リレーの性格上リアルタイム性を最優先させる必要があることから，保護演算用データに付加するセキュリティ用データのオーバヘッドは小さいほどよい。したがって，計算量的セキュリティ技術は保護リレーシステムにはあまり親和性が高くないと考えられる。

そこで，式(1)で算出される情報量的安全性に基づく認証タグを保護演算用データに付加することでメッセージ認証を行う，A-code方式を開発した。

$$\boldsymbol{y} = \boldsymbol{x}\,\boldsymbol{U} + \boldsymbol{v} \qquad (1)$$

$\boldsymbol{x}$：送信メッセージを表すaビット長ベクトル
$\boldsymbol{U}$：固定鍵を表すa×b行列
$\boldsymbol{v}$：使い捨て鍵を表すbビット長ベクトル
$\boldsymbol{y}$：$\boldsymbol{x}$から算出される認証タグを表すbビット長ベクトル
＋：排他的論理和演算

A-code方式によるデータ認証方法を**図2**に示す。あらかじめ両端で行列$\boldsymbol{U}$及びベクトル$\boldsymbol{v}$の集合$\{v_1, v_2, \cdots\}$を秘密裏に共有しておく。これらは保護リレーの整定値と同等の扱いを

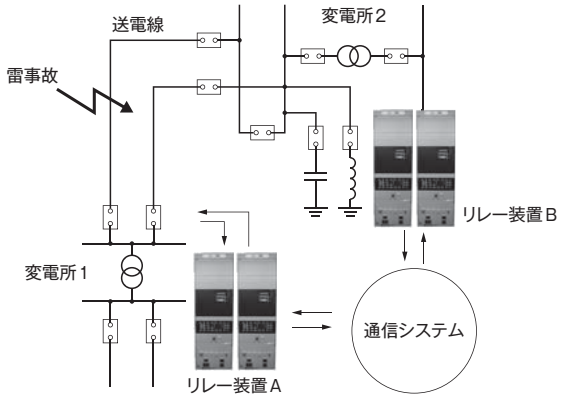

図1. 保護リレーシステム — 送電線の両端で計測した電気量データを相互に送り合うことで，雷などの送電線上の事故を瞬時に検出する。
Protection relay system

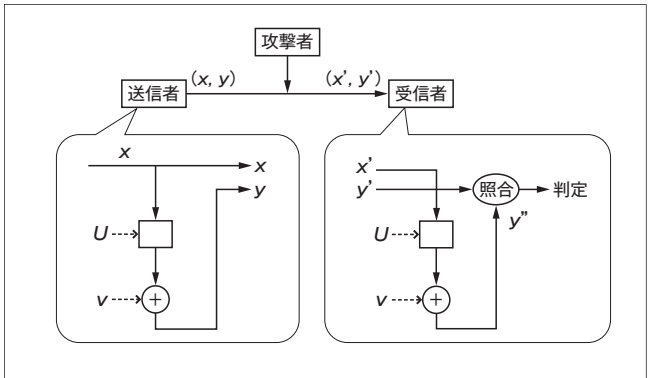

図2. 情報量的安全性に基づく認証方式 — メッセージの送受信者が同じ鍵$\boldsymbol{U}$, $\boldsymbol{v}$を使って認証タグを生成することで，通信路上でメッセージが書き換えられたことを検出できる。
Information-theoretic authentication scheme

一般論文

想定する。データ送信者はメッセージx_1を送信する際に，$\boldsymbol{U}$とv_1を使って式(1)から認証タグy_1を算出し，対（x_1，y_1）をデータ受信者に送付する。データ受信者は受信したデータ対（x_1'，y_1'）のうちx_1'とv_1，$\boldsymbol{U}$を使って式(1)から認証タグy_1''を算出し，これをy_1'と比較することでメッセージ認証を行う。このシステムでは，式(1)の演算に毎回同じ行列$\boldsymbol{U}$を使用するが，ベクトル$\boldsymbol{v}$はメッセージごとにv_1，v_2，..と変えていく。このシステムの安全性は，情報理論的に確率で評価できることが証明されており[2]，次のようになる。

(1) なりすまし攻撃（impersonation）　通信路にメッセージを挿入することが成功する確率は，$1/2^b$以下

(2) 改ざん攻撃（substitution）　通信路で伝送途中のメッセージを改ざんすることが成功する確率は，$1/2^b$以下

類似の技術として，メッセージのデータ化けを検出するための巡回冗長化符号（CRC）がある。しかし，CRCの場合はその算出式が公になっているので誰でもメッセージからCRCを生成し攻撃ができるのに対し，A-code方式は認証タグを生成する際に鍵データを用いるため，前記の確率以上の頻度で攻撃が成功する可能性がない。

3.3　保護リレーシステムへの適用

A-code方式は，前節で示したように，メッセージをいったん固定鍵行列$\boldsymbol{U}$によってタグ長の領域に線形写像したうえで，写像データに使い捨て鍵を適用して認証タグを生成する。したがって，必要な鍵データの量は認証タグの長さに依存するので，鍵データの量をメッセージごとに同じ長さの使い捨て鍵を必要とするワンタイムパッドよりも大幅に少なくできる。このことは，メッセージの秘匿を目的とするのでなく認証を必要とするシステムでは，情報量的セキュリティ技術の実用化の可能性があることを示唆している。

そこで，A-code方式を実際の保護リレーシステムに適用する場合について具体的な検討を行った。その構成と送信データの構成を**図3**に示す。

(1) 送信メッセージ長　2,048ビット

(2) 送信レート　600 Hz

(3) 認証タグ長　32ビット（すなわち攻撃成功確率$1/2^{32}$以下）

(4) システム運用期間　20年

この場合，なりすまし攻撃及び改ざん攻撃に成功される確率は$1/2^{32}$（$< 10^{-9}$）である。この確率は，現在の通信路で一般的に使われているCRC-16がランダムノイズを見逃す確率（1.53×10^{-5}）よりも十分小さい。また，このシステムで両端がそれぞれ保持しなければならない鍵データの容量は，次のようになる。

32ビット×（2,048 +「20年間のデータ送信回数」）
= 4バイト×（2,048 + 600×60×60×24×365×20）
≒1.5 T（テラ：10^{12}）バイト

保護リレー装置はその信頼性確保のために，記憶媒体として駆動部を持つ磁気ディスク装置（HDD）を搭載することはできず，フラッシュメモリなどの不揮発性記憶媒体を搭載することが多い。現在のメモリ容量を考えるとこの数値はやや多いが，近年の半導体技術の進展を考慮するとTバイトオーダのフラッシュメモリが実用化されるのも遠い未来ではない。

情報セキュリティ技術に対する保護リレーシステムからの要件と，各要件に対する計算量的セキュリティ技術及び情報量的セキュリティ技術それぞれの特徴を，**表1**に示す。これらの要件は，保護リレーシステムをはじめとする電力システムだけ

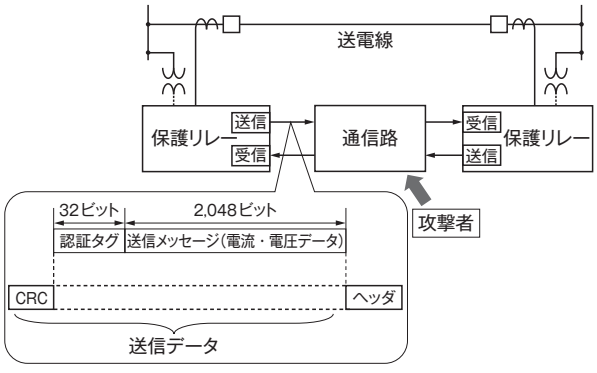

図3．保護リレーシステムへの適用例 — 保護リレーが送受信している電気量データに，これを元に算出した認証タグを付加している。
Application to protection relay system

表1．認証方式の比較
Comparison of authentication schemes

要　件	計算量的セキュリティ技術	情報量的セキュリティ技術	保護リレーシステムからの要求
計算機資源	計算量が膨大なため，FPGA（Field Programmable Gate Array）などを用いた専用の暗号回路が必要になる場合がある	計算量が少ないため，専用回路は不要	装置に搭載できるメモリ容量は小さく，またCPUパワーにも制約がある
可用性	アルゴリズムの脆弱（ぜいじゃく）性が見つかるとソフトウェアの更新が必要になる	ソフトウェアの更新は不要	システム稼働率の観点から，ソフトウェアの更新は好ましくない
通信帯域	SHA（Secure Hash Algorithm）-256の場合，認証タグ長として256ビット必要	ここでの例では32ビットの認証タグ長で十分である	通信容量が小さい伝送路を使う場合が多い
製品寿命	アルゴリズムの強度は徐々に弱くなる	アルゴリズムの強度は時間経過に依存しない	装置の使用期間は15年以上の場合が多い
信頼度	信頼度を設計者は設定できない	信頼度を設計者が設定可能	信頼度を設計者が明示的に設定できることが望ましい
リアルタイム通信	リアルタイム通信を実現するためには高性能なCPUが必要	低速なCPUでもリアルタイム通信が可能	リアルタイム通信を必要とするアプリケーションが多い
鍵の管理	鍵のサイズは小さいが定期的に更新する必要がある	鍵サイズが膨大になる（ここでの例では1.5 Tバイト）	装置にHDDが搭載できない場合が多く記憶容量は少ない

でなく，社会インフラ向け制御システムや組込みシステム共通の課題と言える。表に示すとおり，鍵の大きさを除いて，情報量的セキュリティが優れている。

3.4　評価結果

A-code方式が実際の保護リレーシステムに適用できることを検証するために，式(1)のアルゴリズムを実際の保護リレー装置に実装し，その演算時間を計測した。その結果，**図4**に示すとおり，将来のメッセージ長に対しても平均演算時間は数10μsであり，実用面でもほぼ問題ないことを確認した。また，この計測ではアルゴリズムをすべてソフトウェアで実装したが，式(1)に示すように非常に簡単な行列演算だけで実現できることから，ハードウェアでも実装できる。

またパソコン（PC）と乱数発生器を組み合わせた検証システムを構築した。検証システムでは両端の保護リレーをPCで模擬し，PC間を前節で示した送信データの内容で通信させた。両端のPCには乱数発生器によって生成した同じ鍵を持たせ，これを元に認証タグの生成及び照合に使用する。疑似乱数は攻撃者に鍵を想定される可能性があることから，当社が開発した，熱雑音の発生を利用した乱数発生器ランダムマスター$_{TM}$を用いて検証を行った。その結果，システムが期待どおりに動作することを確認した。

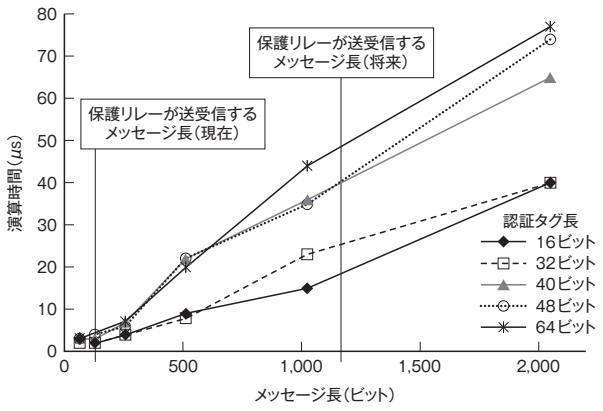

図4．CPU処理時間 — A-code方式による認証タグを実際の保護リレーに適用した場合，計算時間は平均数10μs程度で，実用可能な数値である。
Central processing unit (CPU) processing times

4　あとがき

社会インフラ向け制御システム全般に適用可能な認証方式の概要を述べた。開発したA-code方式は，アルゴリズムが陳腐化せずその効果を確率で示すことができ，また実装及び検証が容易であるため，CPU能力に制約のある組込みシステム全般に適用できると考えている。

今後，この方式の応用について検討を進めていく。

謝　辞

この開発を進めるにあたりご指導いただいた横浜国立大学 松本勉教授並びにご協力いただいた横浜国立大学 情報・物理セキュリティグループの関係各位に感謝の意を表します。

文　献

(1) Shannon, C. E. Communication theory of secrecy systems. Bell Systems Technical Journal. **28**, 1949, p.656－715.
(2) Matsumoto, T., et al. "Protection Relay Systems Employing Unconditionally Secure Authentication Codes". PowerTech. Bucharest, Romania, 2009-06, 07, IEEE Power & Energy Society. No.95.

片山　茂樹　KATAYAMA Shigeki
電力流通・産業システム社 府中事業所 電力システム制御部
主務。電力系統の保護制御システムの開発に従事。
Fuchu Complex

福嶋　和人　FUKUSHIMA Kazuto
電力流通・産業システム社 電力流通事業部 電力系統技術部
主務。電力系統の保護制御システムのエンジニアリング業務に従事。電気学会会員。
Transmission & Distribution Systems Div.

関口　勝彦　SEKIGUCHI Katsuhiko
電力流通・産業システム社 府中事業所 電力システム制御部
主幹。電力系統の保護制御システムの開発に従事。電気学会，IEEE，CIGRE会員。
Fuchu Complex