クラウドに適した
ワンタイムパスワードの
認証システム

会津大学
コンピュータ理工学部
コンピュータサイエンス部門
教授　林　隆史

セキュアなクラウド

認証 (authentication),

認可 (authorization),

課金(accounting)

上記3つが基本・根幹

認証・認可・課金　(AAA)と暗号、時刻

認証では、単に本人確認するだけではなく属性確認を行うことが必要である。属性:　アクセス状況、アクセスしている業務内容、立場

認可では、時間などの認可範囲を設定することが必要となる。

課金では、認証、認可された上でのサービス利用の時間や利用状況が必要となる。

これらに共通しているのは、secure なパスワードの必要性、secure な暗号と、正確な時間の必要性である。

ワンタイムパスワード

- 認証のために1回しか使えない「使い捨てパスワード」
- 繰り返し使わないため、安全性が高い
- 有効期限を設けて安全性を高める。
- モバイルなどからのアクセスに有用

技術的背景

ソフトウェア暗号は、プログラムのバグによる不具合、プログラムの交換が必要。

物理暗号であれば、故障しなければ、交換は不要

電波時計のユニットは、安価で超小型

物理乱数発生器の優位性

物理乱数発生器による乱数発生	ソフトウェアによる乱数発生
FIPSなどに合格・準拠した乱数を安定して生成	ソフトウェアに不具合が生じると安定動作できない
ハードウェア化されているので、安定性が高い	他のプログラムの影響を受けて動作が不安定になる可能性がある。
出力データそのもので動作検証できる。	一様乱数そのものを生成するわけではない。
ランダムネスの高い（FIPSレベル）の乱数を安定して生成	アルゴリズムとプログラム実装の両方のテストが必要

本研究の基礎となる部分

- セキュリティマネジメントに関する研究
- Enterprise Security Architecture, Enterprise Security Planning
- 情報セキュリティに関する社会情報学的研究
- クラウドに必要なサービス疎結合に関する研究
- 認証・認可・課金サービスに関する研究
- クラウドに関する社会情報学的研究
- 乱数に関する研究

電波時計、物理乱数発生器、パスワード発生器

電波時計、物理乱数発生器、パスワード発生器を内臓

- 電波状態が悪いときのために、内部時計で、定期的に時刻補正

物理乱数発生器は、IC化されたものを使用。物理乱数発生器は、一様乱数を継続的生成

パスワード発生器は、物理乱数発生器から生成される物理乱数と電波時計の示す時刻のデータを用いて、ワンタイムパスワードを生成

生成されたパスワード、パスワード生成時の時刻、パスワード生成に用いられた物理乱数、パスワード有効期限が、パスワード生成器に保持される。

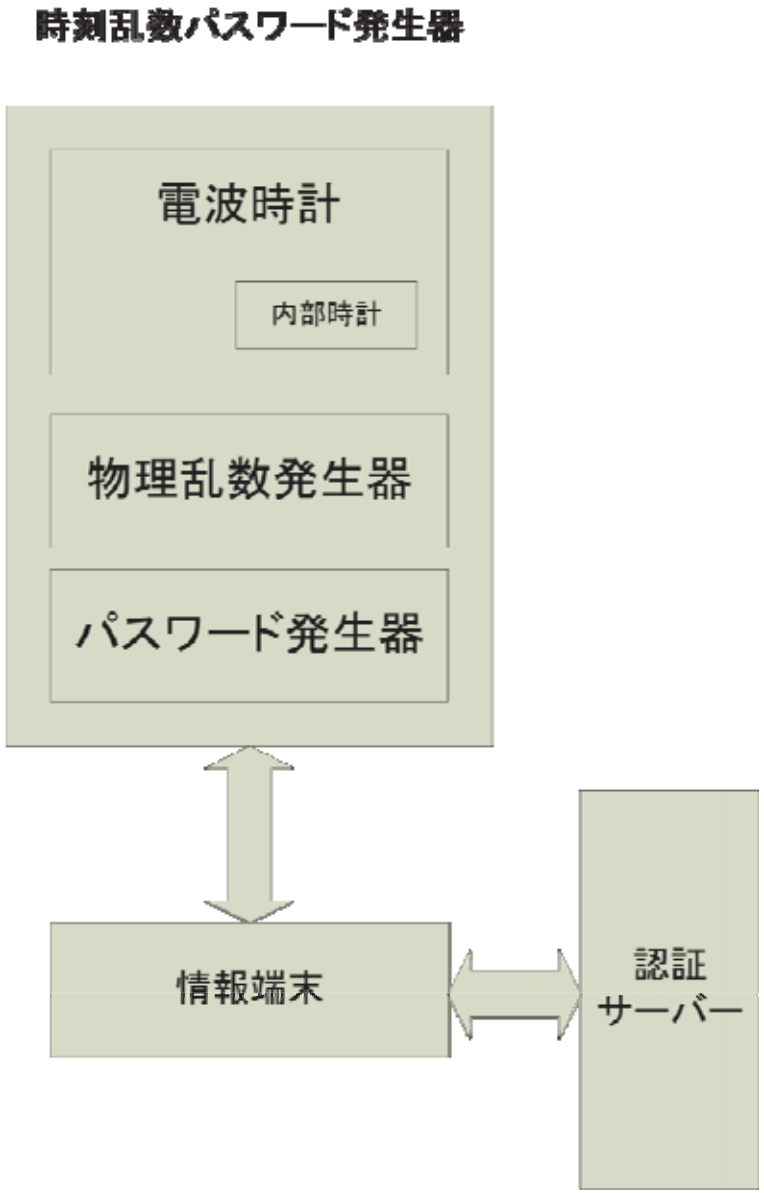
パスワード生成

パスワード生成器に保持されたパスワード、パスワード有効期限は、図中の情報端末を経て、認証サーバに伝送される

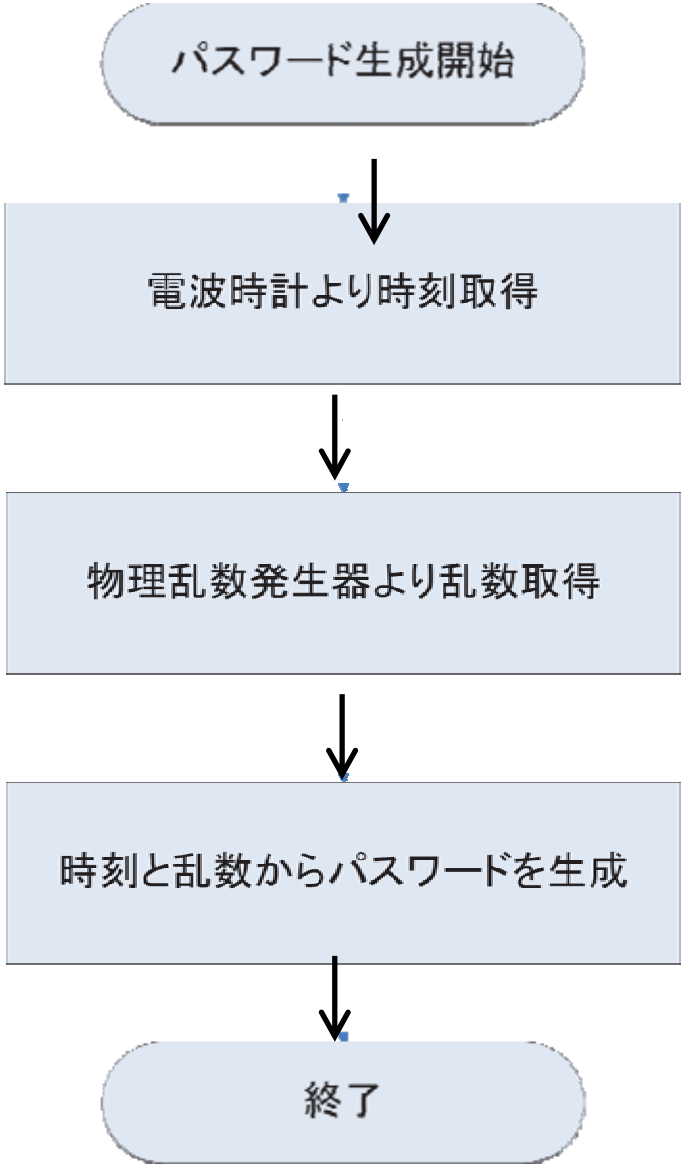
情報端末には、上記の情報は保持しない。

システムのアクセスには、パスワード生成器に保持されたワンタイムパスワードを、情報端末を経て、認証サーバに伝送して認証をうける。

システムの概略



処理の概略



パスワード生成（同時に物理乱数、生成時刻も生成）

↓

パスワード、パスワード生成時刻を情報端末を経由して暗号化して認証サーバに転送する

↓

パスワード生成器から直接認証サーバにパスワードを送り、認証を行う。
あらかじめ設定した時刻まで、パスワードを受け付ける。

従来法の課題1
ネットワークなどを介した時刻取得

時刻データ取得に遅延が生じる可能性

ウィルスなどによって、通信を傍受される可能性

時刻取得をしていることを検知されることによって、侵入者に情報を与える危険性がある。

ウィルスなどによって、通信を改竄される可能性

ネットワークへの過負荷攻撃などによって時刻データの取得を妨害される危険性。

時刻データ取得のためにネットワークへの接続が必要になるため、stand-aloneで利用ができない

ネットワークへの安全な接続が確保されない場所で利用ができない

従来法の課題2
乱数発生にソフトウェアを使用

乱数発生アルゴリズムが知られてしまうと、それを利用した攻撃の可能性

乱数発生アルゴリズムに不備が見つかった場合、生成方法の変更が必要

乱数発生プログラムの不具合が見つかった場合、ソフトウェアを交換する手間がかかる。

新技術の特徴

Network Time Protocol を使わず電波時計を使うことで、ネットワークアクセスを必要最小限にとどめることができる。

FIPSなどの規格に準拠した物理乱数発生ハードウェアを装置内に内蔵することで、ソフトウェア乱数の持つ問題点を解決する。

- プログラムのバグ
- アルゴリズムの弱点、誤り

時刻取得装置と、物理乱数発生装置を内蔵

- 安全なワンタイムパスワード発生を正確な時刻で生成できる

新技術の特徴

コンピュータやセンサーなどの機器の認証にも利用可能

時刻情報を用いた、クラウドの従量課金の利用時間測定に利用可能

きめ細かなアクセス制御が可能

想定される用途

- クラウドサービスの利用者の認証（本人確認＋属性確認）
- クラウドにおけるホスト認証
- センサーネットにおけるセンサー認証
  - 医療センサーの認証と利用者の認証を組合わせることによりセキュアな医療センサーネットが実現
  - 気象センサー
  - 防災センサー

想定される業界

- クラウドにおける認証サービス、認可サービス業者
- クラウド提供業者：　利用者の認証・認可・課金
- データセンター
- 電子自治体

実用化に向けた課題

- コスト
- パッケージ化
- 各種サービスとの連携部分

企業への期待

- パッケージ化を共同で検討してくれる企業があると、製品化が進むと考えています。
- サービス化を一緒に検討してくれる企業を求めています。

本技術に関する知的財産権

- **発明の名称**：

  ワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置

- **出願番号**　：**特願**2008-075279
- **出願人**　　：**公立大学法人会津大学**
- **発明者**　　：**林　隆史**

お問い合わせ先

会津大学
産学官連携コーディネーター（本杉 常治）

ＴＥＬ　０２４２－３７－２５１１
ＦＡＸ　０２４２－３７－２５４６
e-mail　ubic-adm@ubic-u-aizu.pref.fukushima.jp