CRYPTREC提出資料8
説明会発表資料

無限ワンタイムパスワード認証方式

Infinite OneTime Password：IOTP

平成22年 2月 1日

日本ユニシス株式会社
八津川　直伸

UNISYS

UNISYS

目次

1．既存ワンタイムパスワード方式の課題

既存のチャレンジ＆レスポンス方式、カウンタ同期方式、時刻同期方式にはいずれも以下の課題がある。

(1) 共有シークレットの漏洩
第三者または悪意の内部者による「なりすまし」が可能。

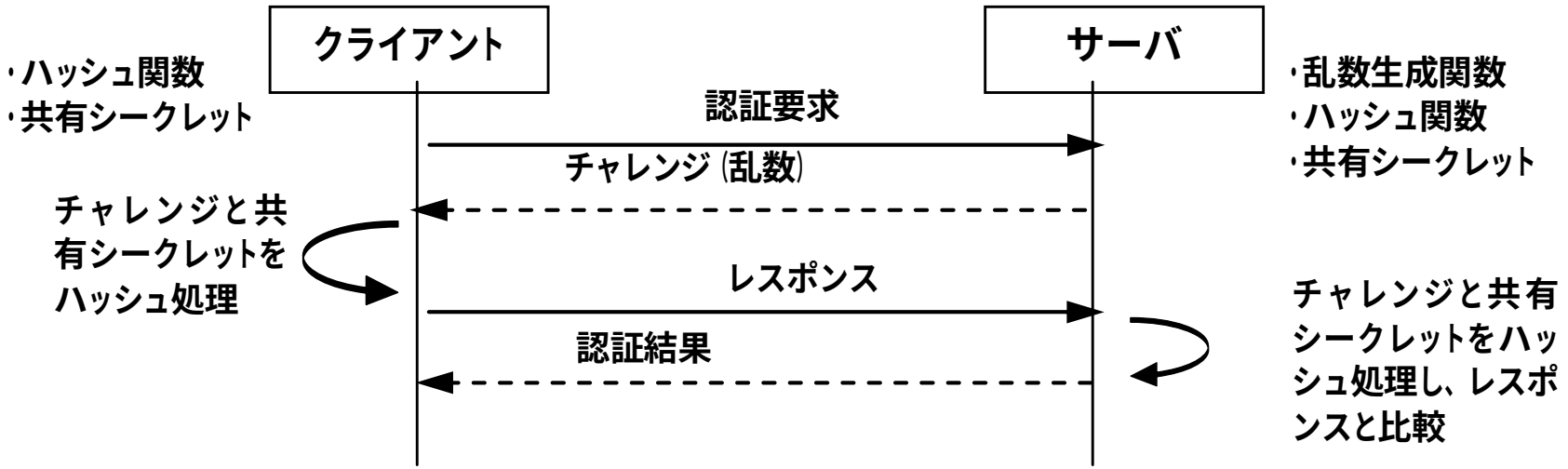
(2) オフライン鍵検索攻撃の脅威
第三者が盗聴等で入手したパスワードから共有シークレットを推測可能。

(3) 許容ウィンドウ管理が必要
カウンタ同期方式、時刻同期方式は、カウンタ、時刻の許容ウィンドウ管理が必要。

(4) 許容ウィンドウ逸脱時の機能不全（致命的同期はずれ）
許容ウィンドウを逸脱すると認証処理が不能となる。

(5) その他
時刻同期方式のSecurIDは仕組みが非公開なので安全性不明。上記の課題は同様にあると推察される。なお、RFC3552にオフライン鍵検索攻撃に対して脆弱性であるとの記述あり。

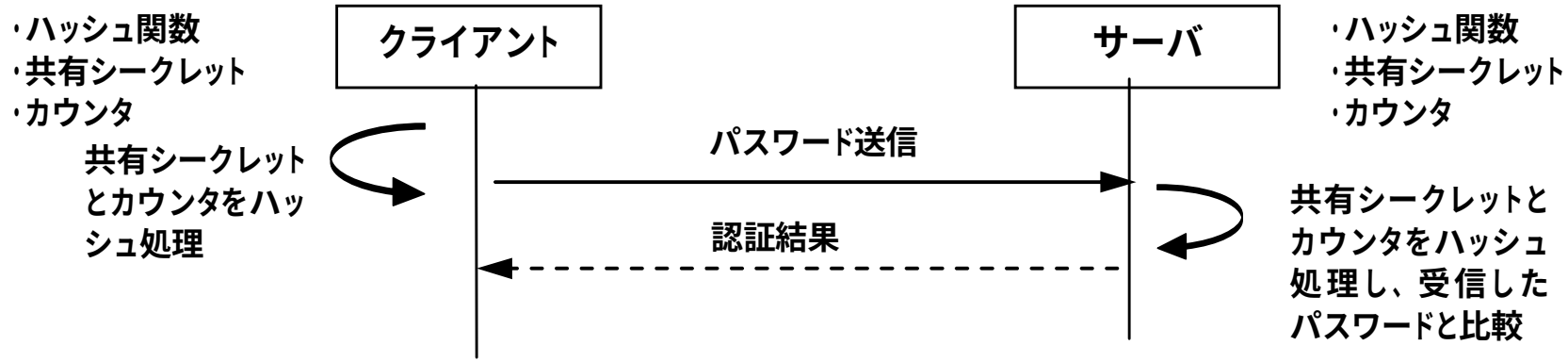
1．既存方式の課題（チャレンジ＆レスポンス方式：CHAP）



➢**共有シークレットの漏洩**

サーバ上に共有シークレットが保存されているので、第三者がなんらかの方法でサーバに侵入し、あるいはサーバ管理者が悪意でこの情報を得ることができれば、チャレンジに対する正しいレスポンスが生成できるので、クライアントになりすますことができる。

1．既存方式の課題（カウンタ同期方式：HOTP）

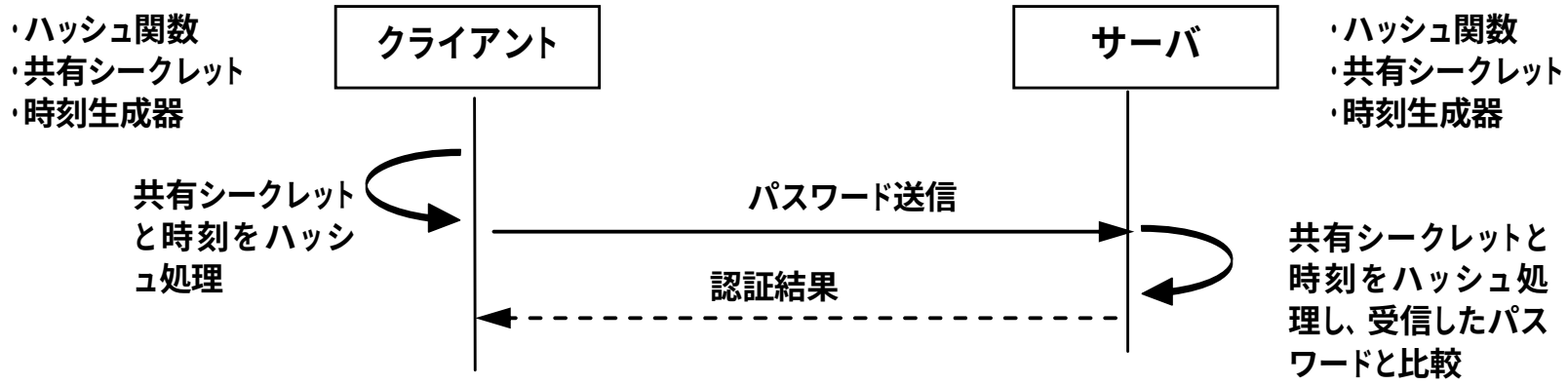


(a)クライアントの利用者は、カウンタを任意に進めることが可能なので、サーバはカウンタの先取り同期ウィンドウ（the look-ahead synchronization window）を管理する必要がある。

(b)先取り同期ウィンドウを逸脱すると致命的な同期はずれとなり、以降認証処理が不能となる。

(c)サーバ上に共有シークレットが保存されているので、CHAPと同様の課題がある。

1．既存方式の課題（時刻同期方式：TOTP）



(a)クロック精度の違いによりクライアントとサーバ間で時刻が前後にずれるので、前方および後方の許容時間ステップウィンドウ（the forward and backwards time-step window）を管理する必要がある。

(b)時刻のずれがこのウィンドウ値を超えると致命的な同期はずれとなり、以降認証処理が不能となる。

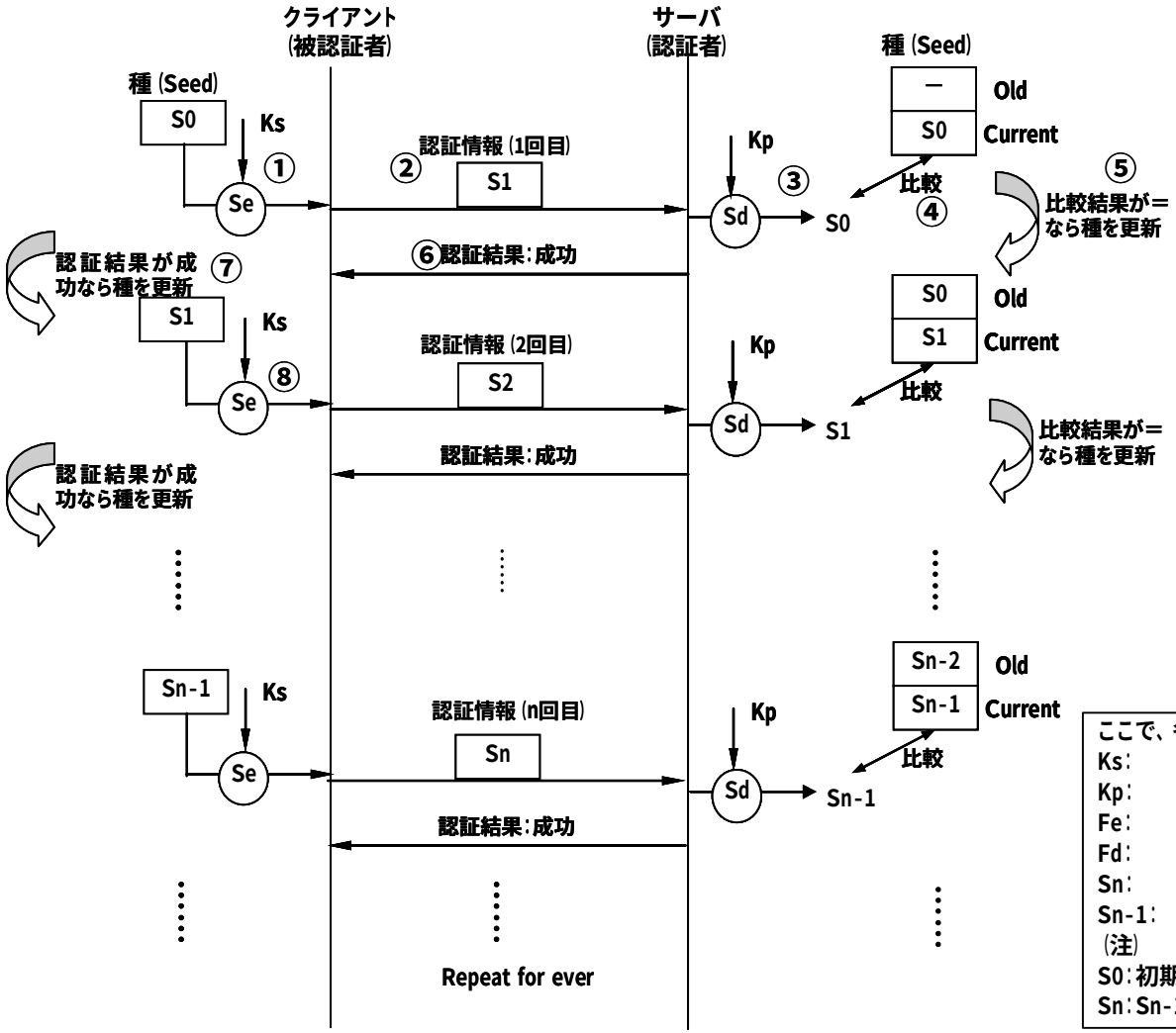
(c)たとえクライアントとサーバ間で時刻が正確に同期していたとしても、時間ステップ切り替わり直前に生成されたパスワードがサーバに到達したとき、ネットワークの伝送遅延等によって次の時間ステップに切り替わっていると認証が失敗する。

(d)サーバ上に共有シークレットが保存されているので、CHAPと同様の課題がある。

2．IOTPの特徴

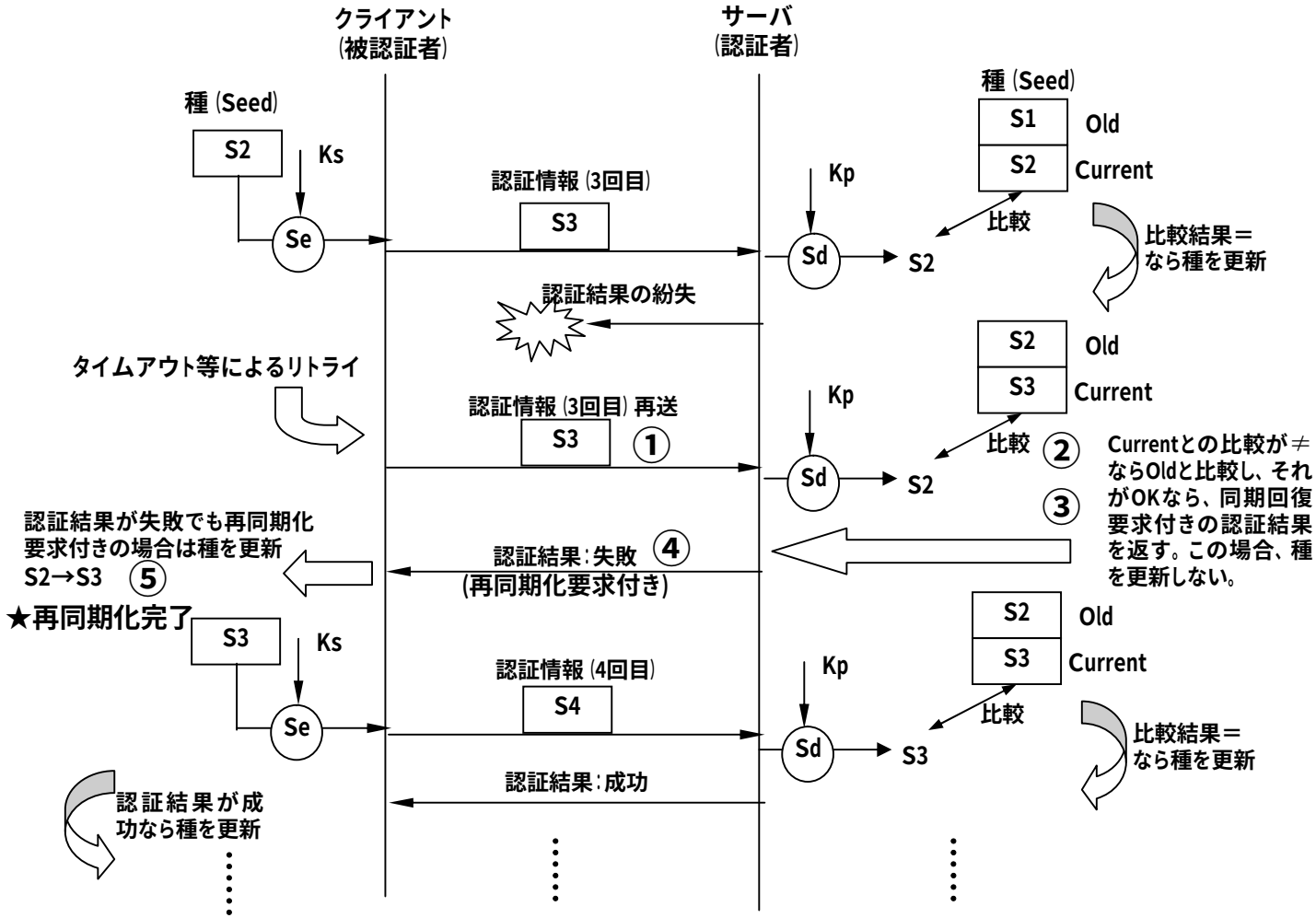
- 公開鍵暗号を利用したワンタイムパスワード認証方式。
- 盗聴などによって得たパスワードを再利用できない。
- 認証サーバに秘密の情報がないので、パスワードクラックが不可能。
- 悪意の内部者による内部犯罪をも防止。
- パスワードに対しオフライン鍵検索攻撃が現実的に不可能。
- パスワードの計算量的安全性が保証されている。
- IOTP認証方式の仕組み自体は未来永劫陳腐化することがない。
- 一回限り有効なパスワードを無限に生成できる。
- 簡単な認証処理シーケンス
- 再同期化が確実に行える。（既存方式のような致命的同期はずれが無い）
- 様々なプラットフォームに適用可能

3．IOTPの仕様 (基本認証処理)



ここで、各記号の意味は次のとおりである。
Ks:　　クライアントの秘密鍵
Kp:　　クライアントの公開鍵
Fe:　　公開鍵暗号アルゴリズムの暗号化関数
Fd:　　公開鍵暗号アルゴリズムの復号関数
Sn:　　n回目の認証時においてクライアントがサーバに送信する認証情報
Sn-1:　n回目の認証時においてクライアントとサーバが共有する種
(注)
S0:初期登録値
Sn:Sn-1 を Ks で暗号化したもの (但し, ∞＞n＞1) である。

3．IOTPの仕様（再同期化処理）



4．安全性、可用性評価（1／2）

□安全性

(1) 盗聴した認証情報の再利用が不可能

盗聴などによって得たパスワードを再利用できない。

(2) サーバ情報の奪取による「なりすまし」が不可能

認証サーバにはパスワードを生成するための情報がないので、パスワード解析アタックが不可能。

(3) 認証者側の内部犯罪防止

認証サーバに存在する全ての情報を得ても、次回のパスワードを生成することができないので、悪意の内部者による内部犯罪も防止できる。

(4) オフライン鍵検索攻撃が通用しない

パスワード生成に用いる種はランダムなビット列なので、辞書攻撃を併用したオフライン鍵検索攻撃が通用しない。

(5) 計算量的安全性の保証

IOTP方式で生成したパスワードを偽造するには、生成に使用する公開鍵暗号の秘密鍵を推測するしか方法がない。

4．安全性、可用性評価（2／2）

□可用性

(1) 毎回異なる一回限り有効な認証情報を無限に生成可能
クライアントは無限に一回限り有効な認証情報を生成できる。

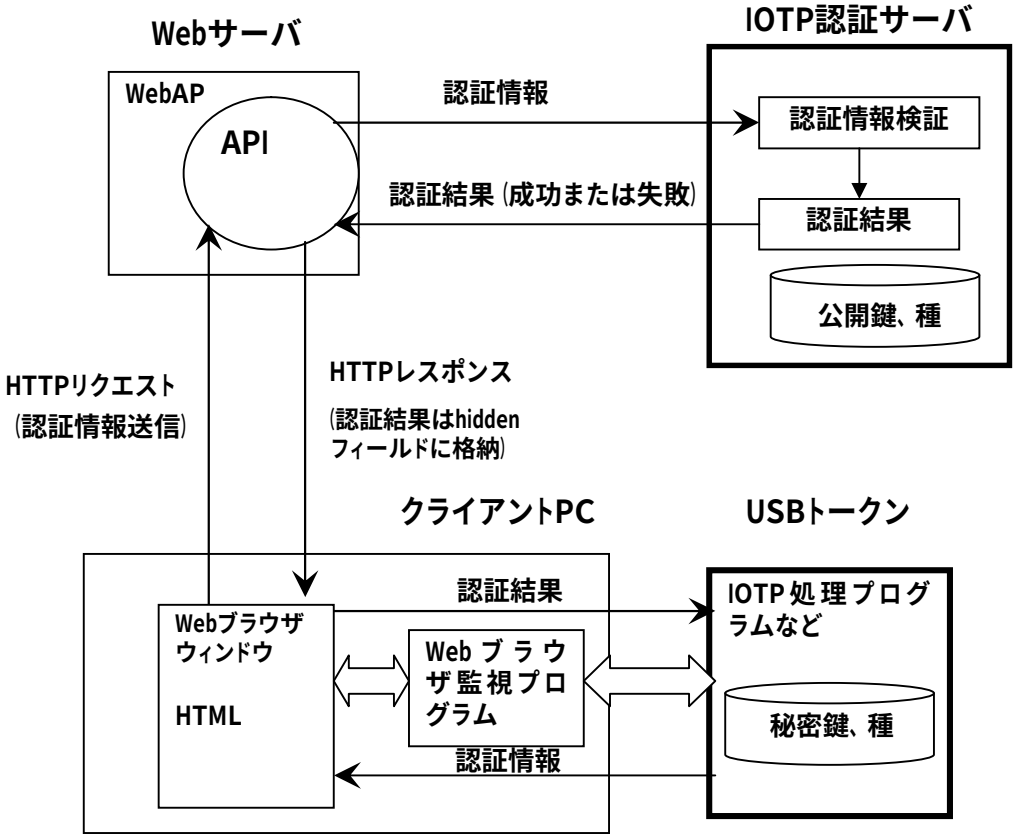
(2) 簡単な認証処理シーケンス
認証処理は一往復で完結。チャレンジ＆レスポンス方式のような複数の対話シーケンスを持たない。また、カウンタ同期方式における先取りウィンドウ（the look-ahead synchronization window）管理や、時刻同期方式における前方および後方の許容時間ステップウィンドウ（the forward and backwards time-step window）管理が不要である。

(3) 再同期化が確実で容易
カウンタ同期方式や時刻同期方式における致命的同期はずれが無く、確実な再同期化が可能。

(4) 様々なプラットフォームで利用できる。
IOTPの認証APIをアプリケーションに提供することにより、様々なプラットフォーム上でIOTP認証方式が利用可能。

(5) IOTP認証方式の仕組み自体は未来永劫陳腐化しない。

5．実施例



USBトークンには、秘密鍵、種、公開鍵暗号プログラム、IOTP処理プログラム、Webブラウザ監視プログラムなどを格納。

認証サーバには利用者毎に公開鍵と種が登録されており、認証サーバ（認証者）～USBトークン（被認証者）間で認証処理を行う。

6．知的所有権情報

□特許権に関する事項

1．日本国特許：第3595109号（2004年9月10日登録）
2．米国特許　：第6148404号（2000年11月14日登録）

□ライセンス方針

上記特許に関しては、本件応募技術（無限ワンタイムパスワード認証方式）を使用するものに対して、相互主義の下、非排他的に、公益を考慮した妥当な条件にて実施許諾する方針です。

7．まとめ

(1)既存方式の課題を全て解決し、高い安全性と可用性を備えたワンタイムパスワード認証方式。

(2)使用する暗号アルゴリズムの強度に等しい計算量的安全性が保障されたワンタイムパスワードを生成。

(3)毎回異なる一回限り有効なワンタイムパスワードを無限に生成可能。

(4)認証者側には各利用者固有の秘密情報が不要。

→ 外部の第三者のみならず認証サーバ側の内部悪意者による不正行為をも防御可能

(5)処理シーケンスが簡単であるため、様々なプラットフォームにおいて利用可能。

(6)IOTP認証方式の仕組み自体は未来永劫、陳腐化しない。