



## 2006 年度下期未踏ソフトウェア創造事業 採択案件評価書

### 1. 担当PM

ウィリアム齋藤 PM (株式会社フォーバル 取締役副社長)

### 2. 採択者氏名

開発代表者:石井 充 (有限会社アペイロン)  
共同開発者:なし

### 3. プロジェクト管理組織

有限会社トリガーデバイス

### 4. 委託金支払額

8,000,000 円

### 5. テーマ名

BitTorrent 型分散システムと使い捨てパッドを用いた通信システムの開発

### 6. 関連Webサイト

<http://www.ipa.go.jp/jinzai/esp/index.html>

### 7. テーマ概要

ネットワーク上における通信の傍受・盗聴・改ざんなどの問題に対して、原理的に100%安全であることが数学的に証明されている、使い捨てパッド(One time pad)という暗号化手法が存在する。使い捨てパッドは、原理的に解読不可能であるものの、暗

号の鍵の長さが、暗号化前の平文データと同じ長さになるため、従来の単一の配信経路に依存した通信手段では鍵の配信問題が解決できなかった。

本プロジェクトでは、使い捨てパッドによって暗号化されたデータを BitTorrent と同様の方式でビット単位で複数のファイルに分割・混在させることにより、上記の問題を解決し、使い捨てパッドを用いた安全かつ実用的な通信システムを構築する。

分割された断片ファイルは中間サーバに一時的に保存されるが、通信の全てにおいて PKI を用いた認証を行うため、Man in the middle 攻撃を含むシステムのなりすましを行うには、関連する全サーバの証明書を不正に入手する必要があり、現実的には不可能となる。また、各断片ファイル・使い捨てパッドのハッシュ値も異なる通信経路で配信され、かつ断片ファイルは複数の経路で重複して送られるため、改ざんチェック及びデータの復元も容易に実現できる。

この他に本システムは以下の利点を有する。

- ・ 既存のシステムを変更することなく導入可能
  - メールサーバーや Proxy サーバーに本機能を付加するだけで運用が可能となり、既に運用されているシステム・個々の端末マシンに全く変更を加えることなく導入できる。
- ・ HTTPS, SSL/TLS, PGP, PKI などの既存の暗号化・認証・通信技術と両立可能
  - 本システムは SSL/TLS とは独立に実装される。このため、既存の全てのセキュリティー技術と両立が可能である。HTTPS 通信に、本システムをそのまま導入できるし、電子メールにおいては PGP と組み合わせるなどが可能である。

以上をメール及び Web に対して実装する。

## 8. 採択理由

ファイル分散をワンタイムパッドと組み合わせる本プロジェクトの提案はきわめて独創的であり、興味深い。ワンタイムパッドは鍵の配信方法やファイルサイズと秘密鍵のサイズを同一にすることに解決すべき問題点があるが、この提案方法を利用することにより、その問題点を解決することができると考えられる。ワンタイムパッドの基本的ルールを守りさえすれば有用に活用でき、実践的であると思われる。

## 9. 開発目標

暗号方式は主に 3 種類ある。一つは共通鍵暗号方式。2つめは公開鍵暗号方式。3

つめが使い捨てパッド(One Time Pad)方式である。

共通鍵方式は暗号化と復号化で同じ鍵を使う暗号方式である。あらかじめ安全な方法で相手に鍵を渡さなければならず、一度解読されてしまったら終わりである。

公開鍵方式は公開鍵と秘密鍵の対になる2つの鍵を使ってデータの暗号化/復号化を行う暗号方式である。共通鍵方式と比べ鍵の管理が容易で安全性が高い。しかしこれらの方式は数学的に暗号が解読されてしまう可能性がある。

One Time Pad 方式は乱数鍵を1回だけ使う暗号方式で、解読不可能な暗号であることが数学的に証明されている。しかし鍵の長さが平文データと同じであるために鍵の配送問題が解決できないなど、従来の単一経路による通信を用いたシステム上で使用するには適さない側面があり、これまで利用されてこなかった。

そこで、当該プロジェクトでは、インターネット上でのサーバー間通信においては、OTP で暗号化後に、データを BitTorrent 方式で断片化し、PKI で認証された複数のサーバーを経由して配信することによって、上記問題を解決することを目指した。

## 10. 進捗概要

本プロジェクトの本質はシステム利用の容易性を保ちながら、いかにセキュアなシステムを構築できるかである。

当該プロジェクトは当初、システムの技術的な面に重きが置かれ、使いやすさの観点からは十分に検討されていなかった。そこで当該プロジェクト全体の間段階で、組織内での通信をドライバーで行うことにより、組織内においても OTP で通信が可能になることを指摘した。OTP 暗号化を L2 で行うドライバーを開発することにより、組織内の通信がポートやプロトコルによらずに自動的に OTP で暗号化されるシステムの開発を提案した。

## 11. 成果

最終報告では、指摘した変更事項が盛り込まれており、組織外のインターネットにおける通信を暗号化する OTP 分割分散通信システムの開発に加え、ユーザビリティを考慮したフィルタードライバーが開発されていた。

## 12. プロジェクト評価

BitTorrent は、UP 帯域を有効に利用して大容量ファイルの配布効率を高める目的で作成した高速ファイル交換(P2P:Peer to Peer)ネットワークプロトコルである。音楽や

映画、商用アプリケーションを提供する為に、BitTorrent が利用されている。  
このような技術を利用し、OTP と組み合わせでシステムを開発するという発想は独創的かつ現実性があり、非常に興味深いプロジェクトであった。  
中間報告での指摘を受け、ユーザビリティを考慮したフィルタードライバーの開発や当初想定していなかったいくつかの問題を解決し実装した点は、非常に評価できる。  
最終的に完成度の高い、BitTorrent 型分散システムを用いたサーバー間OTP通信システムと Diffie-Hellman を用いた組織内 OTP 暗号化/復号化ドライバーの二種類を開発できた点も非常に満足のいくものであった。

### 13. 今後の課題

開発者は既に開発したシステムを実際に運用されているシステムで使用されるように、代理店と契約し、医療関係システムや、通信事業者などとの交渉を始めている。  
しかしながらビジネス面での展開を考えると、導入から保守なども考慮する必要がある、また様々なステークホルダー(サービスプロバイダ、社内の IT 部署、システム管理者、ユーザなど)を想定して考慮したシステム構築が今後の課題ではないか。  
ユーザビリティの観点からシステムをさらにブラッシュアップし、使いやすいOTPを用いた通信システムの開発に期待したい。