ChaosWare Inc.

プレスリリース

平成 22 年 11 月 5 日

暗号便の電子署名検証用公開鍵情報の公開について
―暗号便以外でも電子署名の検証を可能に―

株式会社カオスウェア（代表取締役社長　梅野健）は、暗号便が電子署名で利用する 2048 ビットの公開鍵情報をホームページでの公開を開始しましたのでお知らせします。

この公開情報を利用することで、ユーザは暗号便サービスの提供状況や運用状況に問わず、過去に暗号便が提供する電子署名機能を利用し、暗号便名義で付与された電子署名の検証を行うことができる様になります。

背景：

暗号便では、これまでファイル暗号化転送サービス暗号便(http://www.angobin.jp/)で、安全なファイルの転送と併せて提供させていただいております電子署名技術(署名 Web)を広くご利用いただいておりました。

暗号便で作成される電子署名は、電子署名の正当性を確認する作業を Web 上で行うことができるため、電子署名で利用される鍵情報について特に意識をする必要がありませんでしたが、電子認証（電子署名の検証）の仕組みは暗号便の Web サービスに依存するものでした。

本電子署名用公開鍵情報の公開により、全てのユーザが、暗号便のサービス及び、暗号便運営企業=カオスウェアとは独立に電子署名の検証が可能となります。

電子署名用公開鍵閲覧ページについて：

暗号便電子署名用公開鍵閲覧ページは、誰もが暗号便が電子署名を行う際に利用する公開鍵を閲覧することができるページとなります。閲覧ページでは、以下の情報を閲覧・取得することができます。

- 電子署名アルゴリズム
- 電子署名用公開鍵情報
- RSA Modulus
- 公開鍵ビット長
- 公開鍵利用開始日時
- 公開鍵有効期限

暗号便で付与された電子署名情報を検証したい場合、検証者は電子署名用公開鍵閲覧ページで公開されている公開鍵の情報を利用することで、暗号便サービスとは独立して電子署名情報の正当性を確認することができる様になります。

暗号便 電子署名用公開鍵閲覧ページ https://www.angobin.jp/publickey/

今後の展開:

本公開鍵情報を Twitter や、その他公開媒体を通して幅広く公開していき、より暗号便の認証基盤を強固・完全にいたします。

今後、暗号便アップローダー、CIPHERON、VSC-P2P にも本電子署名の技術を採用していき、暗号化のみならず電子認証サービスの提供、認証クラウドの構築を進めていきます。

連絡先:

株式会社カオスウェア
梅野 健
〒184-8795
東京都小金井市貫井北町 4-2-1
TEL: 042-359-6299
FAX: 042-359-6339
E-Mail: info@chaosware.com
URL: http://www.chaosware.com/

付属資料:

図 1: 暗号便の電子署名用公開鍵閲覧ページの概観