ChaosWare Inc.

プレスリリース

平成 22 年 11 月 19 日

ファイル転送サービス「暗号便」で送信される全てのファイルに無償で送信証明書（タイムスタンプ）を付与
－暗号便送信内容の電子署名検証サービスを開始－

株式会社カオスウェア（代表取締役社長　梅野健）は、ファイル転送サービス暗号便(http://www.angobin.jp/)で送信される全てのファイルに 2048 ビット公開鍵暗号に基づく電子署名による送信証明書の付与を開始しましたのでお知らせします。

この送信証明書発行により、暗号便を利用してファイルが、送信または受信したユーザの双方で暗号便を経由して送信されたファイルであること（送信日時を含む送信内容の真正性）を電子署名技術に基づき、確実に証明することができます。

背景:

Webによるファイル転送サービスや電子メールが普及し、ファイルのやりとりや、Webサイトへのアップロードは日常的に行われる様になりましたが、送信されるファイルの真正性を証明する電子証明は特殊なタイムスタンプサービスを利用する以外は普及しておらず、日常的にインターネット上で送信されるファイルや送信日時の改竄を防止することは困難でした。 また、当社では、
ファイル転送サービス「暗号便」(http://www.angobin.jp/)を運営しており、大型ファイルのSSL暗号化技術による安全なファイル送信を実現し、多くのユーザが日々利用されておりました。ここで、暗号便を経由してファイルの送信が行われた場合、送信者の方には送信確認、受信者の方にはファイルを受け取るためのファイルのダウンロード URL が記載されたメールが送信されますが、これらの情報だけでは第 3 者の方へ、暗号便を経由して、いつどの様なファイルが送付されたか、を証明することができませんでした。

このたび、既に公開中の電子署名検証用公開鍵（2048 ビット。2010年11月5日プレスリリース参照。）に対応する暗号便専用秘密鍵(2048 ビット)を用いてファイル送信時に作成される電子署名が含まれた送信証明書を作成し、全ファイルに無償で自動付与することで、全てのユーザが簡単に、いつ、どの様なファイルが暗号便を経由して送付されたかを確認することができる様になりました。

暗号便で付与される送信証明書について:

電子署名による送信証明書は暗号便を経由して送付されるファイル全てに自動的に付与されます。送信証明書自体は、テキストファイルの形式でファイルの送信者及び、受信者へファイルの転送が行われる際に暗号便から送付されるメールに添付されます。 送信証明書には、以下の情報が記載されています。

- 送信証明書 ID
- ファイル送信日時
- ファイル送信時にファイルの送信者が設定したメッセージ
- 送信ファイルの一覧
  - 送信ファイル毎に更に以下の情報を記載
    - ファイル名
    - ファイルサイズ
    - SHA256 アルゴリズムによるファイル本体のハッシュ値
- 暗号便によって送付されたことを示す電子署名情報

なお、送信証明書に記載されているファイル送信日時については、通常の原子時計に基づくタイムスタンプではありませんが、暗号便のサービスを提供する www.angobin.jp サーバにファイルがアップロードされた時点の時刻を、www.angobin.jp サーバが独立行政法人情報通信研究機構が公開する NTP サーバから発信される日本標準時と同期することにより取得しています

送信証明書を受け取ったユーザは、暗号便が提供する送信証明書検証ページ（https://www.angobin.jp/proof/ ）を利用することで、送信証明書をアップロードするだけで簡単に送信証明書が正当なものであるかどうかを証明することができます。

また、本年 11 月 5 日より公開中の、電子署名検証用公開鍵（2048ビット）を利用することにより、暗号便とは独立して送信証明書の正当性を確認することもできます。

暗号便が提供する送信証明書検証ページを介しての送信証明書の検証は、暗号便の有償暗号便アップローダー以外の無償サービスによるファイルアップロードの場合、ファイル送信時から 2 週間以内に限り、検証を行うことが出来ます。2 週間を超えて、引き続き暗号便を介して送信証明書の検証を行うためには、1 送信証明書あたり 100 円(税抜き)にて、期限無しで送信証明書の検証が行える様になります。

暗号便 送信証明書検証ページ https://www.angobin.jp/proof/ 暗号便 電子署名用公開鍵閲覧ページ（2010 年 11 月 5 日公開） https://www.angobin.jp/publickey/

本送信証明書の特徴:

- 暗号便で送付される全てのファイルに電子署名による送信証明書を付与
- 送信証明書は暗号便が提供する送信証明書検証ページを利用することによって、簡単に送信証明書に含まれる電子署名の検証が可能
- 暗号便での無償の送信書証明期間が過ぎた場合でも 1 送信証明書あたり 100 円で送信証明書の検証が可能

今後の展開：

送信内容のタイムスタンプに関しては、現在のNICTの提供するNTPサーバだけでなく、NTPサーバに乱数を付与することにより，NICTのNTPサーバから配信される時刻をスタンプしていることを証明可能にするNICTの持つ新技術（特開 2009-253860）や他社タイムスタンプサービスとの連携検証実験、及びサービス連携を積極的に推進し、今後より利便性が高く正確なタイムスタンプを付与し普及させていきます。

また、今回証明する内容に加えて送信者のなりすましを防ぐ送信者証明を可能とするため、現在提供中の有償版暗号便アップローダー、CIPHERON、VSC-P2P シリーズ等のアプリケーションを介して暗号便にファイル送信された場合、送信者の証明を行えるための情報を送信証明書に付与し、暗号便を中心とした認証クラウドコンピューティング環境の構築を進めていきます。また、有償 Web サービスである暗号便私書箱(http://www.angobin.jp/pb/)のオプション機能として、この電子署名サービスに基づき送信証明書を提供し、私書箱を介して私書箱契約中の企業ユーザ様へ送信されたファイルの内容及び、送信時刻証明に活用してまいります。

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: 送信証明書検証ページ（https://www.angobin.jp/proof/ ）

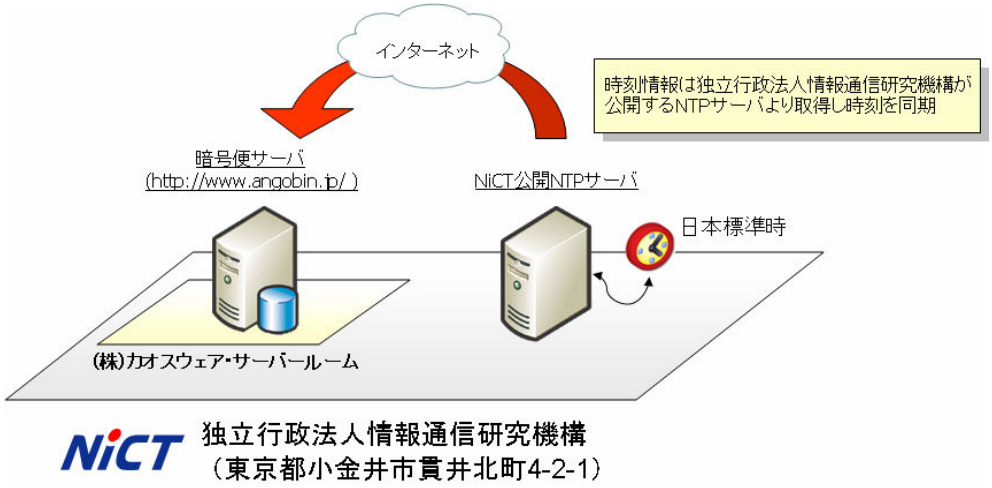

図 2: 送信証明書で利用される時刻についての概要図

((株)カオスウェア・サーバールームは独立行情報通信研究機構本所内に設置されている NTP サーバとほぼ同じ場所（半径 1Km 以内）にあります）

サンプルファイルは以下の URL からダウンロードできます。

http://www.angobin.jp/?action_dlstatic=true&target=tssample

表 1: 送信証明書サンプルファイルの内容

①正当な送信証明書ファイル	ts-normal.txt
②改ざんされた送信証明書ファイル	ts-interpolation.txt

※ ②の改ざんされた送信証明ファイルは、①の正当な送信証明ファイルに記載されている送信日時に記載されている時間を 1 秒早い時間ものに書き換えたものです。

※ ダウンロードしたファイルを暗号便 送信証明書検証ページ (https://www.angobin.jp/proof/)からアップロードすることで送信証明書の内容が正しいかどうかを確認することができます。
(②のファイルをアップロードした場合は、改ざんされている可能性がある旨のメッセージが表示されます)

図 3: 送信証明書検証結果(検証成功時)

図 4: 送信証明書検証結果(検証失敗時)

＜作成される送信証明書の例＞

```
----------------------------------------
 暗号便.jp 送信証明書
----------------------------------------

この送信証明書は、以下のファイルが記載された送信日時に
www.angobin.jp を経由してファイルが送付されたことを証明するものです。

送信証明書の正当性は、https://www.angobin.jp/proof/ を
利用して暗号便上で簡単に検証することができます。
また、https://www.angobin.jp/publickey/ で公開されている
公開鍵を利用して暗号便とは独立に送信証明書の検証を行うことも可能です。

＜送信証明書 ID＞
7887b5f0715288034499439f5ba9606906602d3a

＜送信内容＞
送信日時:
2010/11/18 17:47:19 +0900

メッセージ:
暗号便・送信証明書（電子署名）付与サービスのテストです。

送信ファイル一覧:
No.40596-1
 * ファイル名
    Examples.zip
 * ファイルサイズ
    21.8Mb
 * SHA256 ダイジェスト
    ed0abc1b7a9df9b1fca69bc55a4bc2795a9517ce4f8057ceb633dfafb5724b87

＜送信証明期限（無償利用の場合)＞
2010/11/19 17:47:19 +900


*** 送信日時について ***
angobin.jp サーバの時刻は、独立行政法人情報通信研究機構が公開する
NTP サーバを利用して日本標準時と同期されています。
タイムスタンプされる日時はこのサーバから取得された時間で記録されています。
```

*** 送信証明期限について ****
無償で当証明書を暗号便で検証できる期限となります。
期限を過ぎた場合でも、検証を暗号便で行える様にしたい場合は、
1 送信証明書あたり 100 円で永続的に検証を行うことができる様になります。

以下のフォームより、引き続き暗号便上で検証ができる様に変更したい
送信証明書 ID を記載の上、ご連絡ください。

https://www.angobin.jp/contactus/

--
 暗号便 angobin.jp - Authentication Cloud Computing Platform
 http://www.angobin.jp/

------- BEGIN ANGOBIN DIGITAL SIGNATURE -------
XzoSajJUQj44LWTBnxVTVpLO815Z9Yd9Nfn42mLSLsqOLAuOA+q68myHQMfOxke9xHCj9zsDu
rSIUdz3yGDTAq1euv+eS7dQIINi4kMAwHs3qpMdaZXIwcGAeycYwjzwqQhf7kOaVkwZl7RsC1
3ApDWxrJk3QW28EUnXf3w29+kL6PF4AOGmi8ayqqx+FDUEC3F/qhMUHVtFx/wOUKafxsukLxO
YnORf4DDlme5LnGiBS/PCmOUZFhKfMclRbzfZsMju+V94Xpuir68E23cH/NJgMrHpudQqzOoH
4nO1OUsNLNBt6kbQLHW6OqVbf8lTsByAkaRALRfnELq6asOwwg==
------- END ANGOBIN DIGITAL SIGNATURE -------

------- BEGIN ANGOBIN PUBLIC KEY -------
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxH7YBlj68Ck7llK+FHpc
85zU3fHP82Zeroeq2nQDuQqGbNCYxrgtqlRNvfRtc1MUKy6Moee46oVC9N7ilYuF
yEqRSxZKFZlJBAVkHwx5M7EOOhdxwrWATefPuoNBH4rnHn2PqhS7PMiZuPmJPteW
HgetvCuaeqBXlDUH/J9QLhhvRp5dLlxxxUM6RpWaEEqglV19fNNgFefS+Wi0ok6F
fGdnW55hdXohfUqLW8VYT1AY/Hb+Vr6h13vvtzRilhtFij3gm8ZaRK/rxZx1QAyh
YsvZkgNuaZDeJY8Q3VBqgMaMvjSIW+nv1sX8xpqStvWQTz9ON5NErRVVsCWaFApA
FwIDAQAB
------- END ANGOBIN PUBLIC KEY -------