株式会社 ITS MORE

2020年4月始動

2020年4月13日 投稿者: YSATO@DELEGATE.ORG

危険なメールを根絶する技術

1993年は MIME メール (多目的インターネットメール拡張規格、Multipurpose Internet Mail extension）の第一版（ RFC1341, RFC1342）が出された年でもあり、一方（ほどなくMIMEを転送メッセージ形式とすることとなる）WWW（ウェブ、World Wide Web）、HTTP（Hyper Text Transfer Protocol）が勃興した年でもありました。

それらは世の中を変えました。 とっても便利に、同時にひどく危険に。

端末制御コードを細工した無邪気ないたずらメールやファイルは、はるか昔からありました。しかし MIME によるメールのマルチメディア化（特に添付ファイル）とウェブサイトとの連携を悪用して生まれた狂暴な危険・危機は笑いごとでは無く、今日も未だ収まることがありません。

しかし、そのような危機が顕在化した頃には既に、解決策も存在し、広く使われていました。それは公開鍵暗号を使った電子署名であり、そのデータ（たとえばメールやファイル）を誰が作ったものかを証明する技術です。主に使われていたツールは PGP（Pretty Good Privacy）でした。

メッセージやファイル、あるいはさらにその構成要素毎に署名をしてやり、信頼できる署名の無いものは利用（受け取りや開封など）しないようにすれば、全ては解決するだろうし、枯れた技術だからすぐに広まって、この危機は早晩終焉するだろう、と当時は素朴に考えていたものです。なのにあれからもう四半世紀が過ぎても、状況はそれほど改善しておらず、アンチウィルス業が盛んです。

これってマッチポンプなんじゃないの？と思うこともあります（笑）

ウェブやメールを代表とするアプリケーションの通信の世界では、通信路の暗号化や、サーバやクライアントの電子署名（認証）は早くに実現しました。特に SSL (Secure Sockets Layer) のお陰ですね。一方でコンテンツに対する電子署名は遅れていました。

プロフェッショナルが作るものについては、電子署名や暗号化の技術利用が進みました。一方、メールの大半は、素人エンドユーザが書くものです。素人の世界では、自分の書いたメールや資料に電子署名をして送ったり公開したりするためのインフラの普及が遅れていました。結果的に、受け取るほうも、電子署名を利用できない状態でした。

ですが、少しずつ状況は進歩し、インフラは整いつつあります。特にPDFに電子署名を行う技術はかなり普及しました。（領収書も電子署名されていると良いのに…）メールに署名する技術（特にS/MIME）も、多くのツールに実装されています。あとは、いつ大多数のエンドユーザがそれを使うようになるか、ですね。現状、電子署名用のデータをツールにインストールする作業はそれほどカンタンではなく、素人には少し敷居が高いレベルですが、これも早晩こなれて解決するでしょう。

ラストワンマイルは、ユーザ各人が自分の証明書を手に入れるところだと思います。気になる費用ですが、個人の証明書は一年あたり５千円くらいが昨今の最安値のようです。

> などと書いている私も最近まで前職にあった頃は、結構センシティブな情報をやり取りするのに、通常メールやファイルの署名は…。相手方も…でしたから。そもそも組織の人間としての業務には、組織の発行する公式な職員証たる証明書を使うべきですし。
> ですが今回、自分の仕事環境をまっさらから作るのを機に、電子署名の環境を整えることにしました。それで、キャンペーンにもつられて少しだけ安く、個人証明書を購入しました。（いや、ハンコを押すのも新鮮に感じられていいんですけどね…）

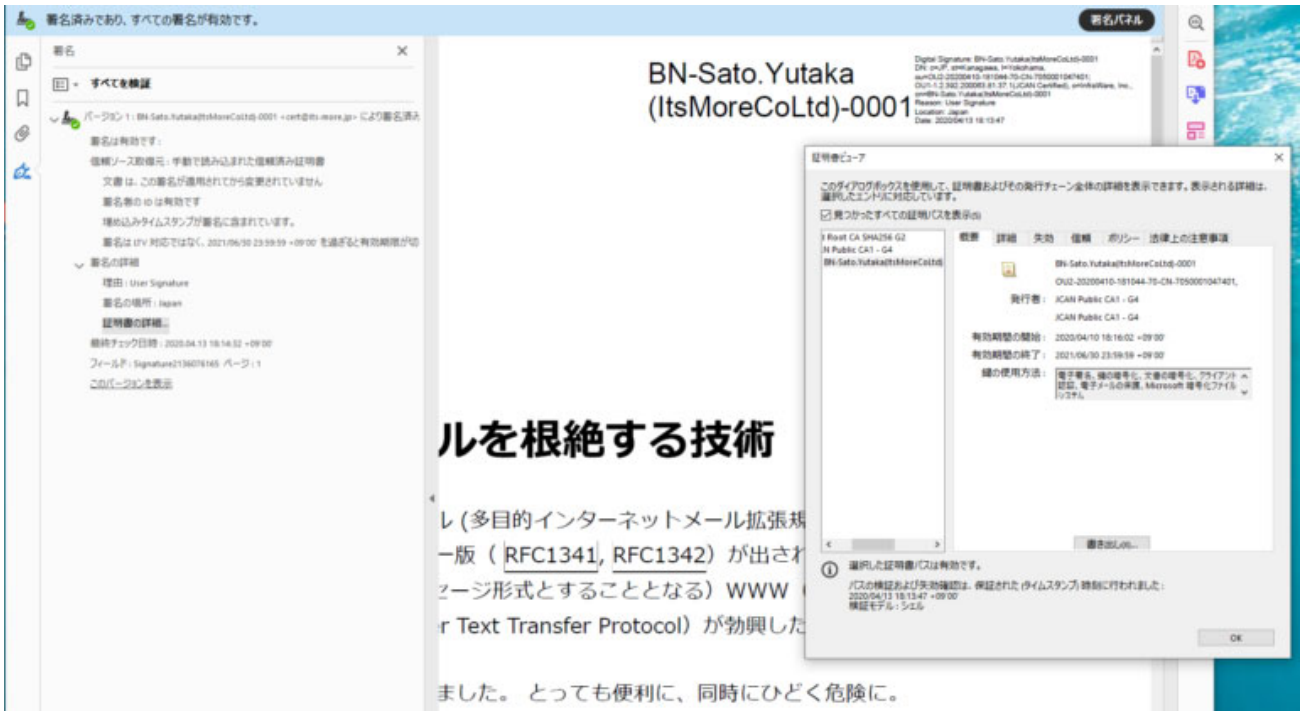
この費用をどう感じるかですね。また、素人（非営利個人）の場合にはあまり問題になりませんが、そのデータを「いつ」作ったのかが、「だれ」が作ったかと同時に重要になります。特に知的財産の保護のために。それを実現しているのが「タイムスタンプサービス」で、ある時点には既にそれが存在していいたことを証明します。これは署名＋時刻に対するさらなる署名で、ネットワーク経由の自動署名で精度は１秒程度のようです。ですが、これも結構お高い。安いところでも一件あたり10円くらいするようです。

> 自動生成した部品データにも署名したいと考えている、個人的な法人（笑）の私としては、ちょっと10円は厳しいかなと感じます。

自然なりゆきとして、ウェブ（HTTP）のメッセージにもS/MIMEが使われるようになるのか？に興味がありますが、そういう話は盛り上がっていないようです。そもそも、ページの中のこの部分は誰が書いたもの、たとえば許可を受けた引用部分とかを峻別するためには、MIME/HTTPではなく、コンテンツ（HTMLなど）に署名を仕込む必要があります。MIMEにもマルチパートというデータ型があって、それを使えば入れ子のS/MIMEもできるのですから、やればできるとは思いますが、今ではすっかり、マルチパートは廃れてしまった模様です。

2020-0413 sato@izmoh

そんな中、上記の個人証明書値引きキャンペーン打っている会社では並行して、無償で手軽にタイムスタンプを押してくれるサービスを提供しています。それがキャンペーンに乗った決め手でした。たとえばこの書き物のPDF版に対する署名は、以下のファイルの右肩に表示しています。PDFのリーダで開けば、その署名が本物か確認できますが、そのためにはご自身のPDFリーダに署名者の証明書をインストールする必要があります。自動化する方法もあるようですが、一件だけなら手動でも簡単です。 めっちゃメジャーな証明書業者から買えば、Adobeが証明書をプレインストールしてくれてて、その手間もいらないのかな？高そうだけど。ちなみに、Adobe自身が提供しているタイムスタンプサービスは、とても高価です。

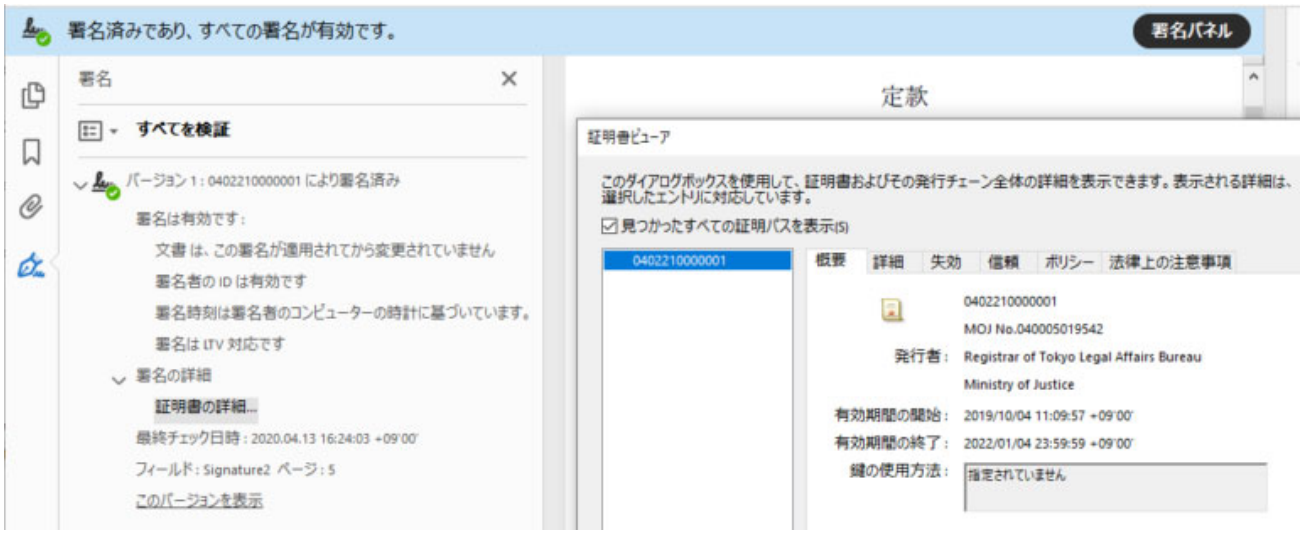


以下が上記PDFの原本です。暗号してますごめんなさい。ヒントは：

“2020/04/13 18:54:20 +09’00'”

保護された電子封筒001　　**ダウンロード**

いわゆる電子定款には、公証役場の公証人さんが電子署名します。たとえば、弊社の定款PDFをAcrobatで開くと、以下のように表示されます（この場合には、署名をPDF上に重ねていません）。発行者は Registrar of Tokyo Legal Affairs Bureau, Mnistry of Justice（法務省法務局）です。わが社は東京法務局ではないですけどね。



Googleさんはどうしてるかなと思ったら、DocuSignという、クラウド上で署名してくれるサービスと連携してますね。やはりそう来ましたか。零細企業向けプランだと$25/月だそうな。かなりリーズナブルだけど、うーん、むずがゆいところ。富士ゼロックスさんも最近DocuSignと連携してペーパレス化(^-^)始めたみたいだし（一件あたり387円～ってまじか？）。複合機で紙をスキャンすると署名付きでPDFに落ちたりして。
いずれにしても電子署名化は、時代の潮流みたいですね。

危険なメールを根絶する技術---ITS-more – DocuSign　　**ダウンロード**

とまあ、こういうふうに、まずはウェブページを題材に、ページの魚拓をとって電子署名して、同じページに挿入したりドライブに保存したりメールするフローを自動化・ワンクリック化したい、というのが、いまこれを試行している動機なんです。技術的には単純。このWordPressでもできるんじゃまいか。

最大のネックはタイムスタンプ代。技術的には応答時間…まあ、数秒なら我慢できます。任意のでデータに署名するには？例えばS/MIMEをエンベロープにするとか。

現状、各社のサービスは「大事な文書に人間が大事に署名する」ことを想定しているし、クラウドサービスと抱き合わせです。一方わが社の構想は、「今見ているもの（いろいろ）」の上でワンクリック、特にエクスプローラの上のアイコン

で右クリックとか、スマホで拇印押して指紋認証で捺印とか、さらに「機械的に生成したデータに自動的に署名する」というものです。私が証明書を購入した会社さんのコンセプトはそれに合っています。いずれ実現したいものです。
まあ、うちがやらなくても誰かがやる（やっている）でしょうけど…