株式会社 ITS MORE
2020年4月設立

2020年9月3日 投稿者: SATOXITS

GShell 0.3.0 – 電子署名付きHTML5

社長：さて、今日は署名をやりましょうか。

開発：まずは JavaScript で出来ることが重要と思いますが、普通にRSAのライブラリとかあるみたいですね。Goにももちろんあります。

Multi Purpose な使い倒し

社長：せっかくなら、コードの正本証明以外にも使いたいですね。

開発：一粒で何度も美味しい。

社長：せっかく精神は我社の基本精神です。一つの技術、一つのコードを多目的に使い倒す。more with lessです。

基盤：フッ素ひとすじみたいなやつですね。

開発：アクセス権の制御というか、ライセンスキー的なものはやってみたいですね。キーをもってないとしかるべく実行できない。HTMLの一部のエレメントを表示できないとか。class で制御する。

基盤：それをやるには、HTMLソースでも見えないように暗号化する必要がありますよね。

社長：まあROT13みたいなもんですね。いっそdata URI にするという手もあります。href やら src やらで、URLとして自分のHTML内のエレメントIDを使えると良いのですけどね。dom:elmentId.innerHTML みたいな。

基盤：エレメント id は IPv6アドレスなんていうのが面白いですね。

開発：Goコードにしても、ソースでは配布するんだけれど、デフォでは読めないようにするには、暗号化する以外の道は無いですよね。

社長：なんか電子署名より暗号化のほうが面白そうな気がして来ました。

基盤：画像ならモザイクをかけるとか面白そうですね。

社長：プログラムなら、それが利用できるリソースとか実行性能を制御する感じでしょね。あるいは機能の一部を無効化する。

基盤：ありがちな手口ですねw

開発：チャンレンジアンドレスポンスで、簡便なワンタイムパスワード的なものもやりたいです。

基盤：クライアント側もチャレンジすると面白いんではないかと。

開発：SSLってそんな感じになってないんでしたっけ？

自前タイムスタンパー

開発：コードの電子署名では、何しろタイムスタンプを押すところがヤマだと思います。どこで押してもらうか。

社長：タイムスタンプの無い署名とか、知財保護の用途では意味が無いですね。

基盤：骨董品とかもそうですね。

開発：昔から電子署名技術があったら鑑定士も失職ですね。

社長：鑑定…　って、いいキーワードのような気がします。証明とかよりいい。

経理：タイムスタンパーって月1万円くらいかかるって聞きましたが。

開発：一発乱数生成するだけの証明書発行と違って、ずっとインフラ運用にコストが掛かりますからね。

社長：あれ、鍵を生成するのが証明書屋だっていうのが、全く理解できないです。

開発：実印と同じじゃないですかね。ハンコを彫った人は同じハンコを作れますから。

基盤：昔なら、機密兵器を作った技術者は、作り終えたら生き埋めにされちゃったりしてましたね。

社長：まあ、印鑑証明ってのは今の時代全く意味が不明なものの一つです。

基盤：でも社長がいつも使ってるタイムスタンパーは無償ですよね。

社長：なもので、QOSとかは無保証だと思うんです。それに、機械生成で1日に何百回も何万回を押したら怒られるか、サーバがダウンするか、ではないかと。

基盤：まあ、ファイアウォールでフィルタされておしまいでしょうけど。

開発：そういう使い方をしたら、有償のサーバでも落ちそうです。

経理：といいますか、タイムスタンプ代で一日に数万円飛びそうですね。

開発：なもので、タイムスタンパーも自前で立てる、何かの形で、1時間に1度くらいで、公式のタイムスタンパーに証明してもらう、というのが良い線だと思います。

社長：毎時間、自前タイムスタンプをするための鍵を作って、それを証明してもらう感じですかね。

基盤：有効期限が1時間の証明書みたいな感じですかね。

かぼちゃでGo

開発：おっと、吉田拓郎の夏休みがYouTubeから。

社長：麦わら帽子っていったら吉田拓郎ですよね。

基盤：それにしてもしょぼい演奏と録音ですね。

開発：なんせ1971年だそうですから。

社長：これは、聴かなかったほうが良かったかな (^-^; 想い出の中にしまって。

経理：そろそろまた血圧のサンプリングを。

社長：そうですね。24時間の変動のグラフを作って明日お医者さんに見せたい。ていうか、最近どうもクスリが効かないように思ってたんですが、一粒追加投与したらテキメンでした。

開発：仕事中、特に盛り上がってる時に血圧が下がるのは不自然じゃないかと思いますが。

基盤：めっちゃ血圧が下がったら死にますかね？

開発：思考する葦としては死んだも同然ですね。

社長：血圧が下がったせいか、イマイチ仕事する気にならないです。お腹もすいてきました。でも天気がぱっとしないので外出する気にもならない。

開発：カットかぼちゃがありますね。チンしましょう。

レンジ：ゴー…　ぱぺぽ、

開発：どれどれ。あー、さすがにかぼちゃは強靭ですね。延長。

基盤：チューリップのデビュー当時のも悲惨ですが。

社長：財津さんは年食ってからのほうが圧倒的に良いですね。

基盤：ヒジョーに、きびしーいっ。

レンジ：ぴぺぱ、

開発：どれどれ。あーもう少しかな。延長。

レンジ：ぱぺぽ、

開発：どれどれ。あーいい感じですね。90度で15分。もぐもぐ。うん、旨い。

基盤：はぐはぐ…。あまーい。

社長：うーん、もぐもぐ。

基盤：電子レンジって最高ですね。もぐもぐ。

経理：これ、業務用ですか？もぐもぐ。

社長：そうだったかも。回らないで大きなガラス鍋がまるごと入るという基準で選んだんですが。

開発：震災の時に足のゴムがひとつどっかに飛んじゃって不安定なんですよねｗ　もぐもぐ。

経理：そんなに古い機械には見えないですね。もぐもぐ。

開発：栄養価からして、かぼちゃは完全食みたいなもんですね。あなたは万能ですかって。

基礎：馬車も作れるくらいですからね。

社長：multi purpose 過ぎる。

開発：わたしはこれは「カロチン」だと思うですよ。「カロティン」ならまだしも「カロテン」て何だそれ？って。

基盤：でもWikiでは「カロテン」ですね。綴りは carotene（英）、carotin（独）。

開発：あそう。もぐもぐ。完食。

社長：あーおなかいっぱい。これで222円とは！

開発：まるごと買ってきてチンしたら爆発しますかね。

基盤：生状態だと自力ではまずカットできないですよね。

社長：ドリルで空気抜き開ければいいかも。

開発：ハロウィンのかぼちゃてそういういう起源だったのかも知れませんね。

経理：電子レンジはまだなかったんじゃないでしょうか？

基盤：ようやく洗濯物が少したまりました。60度温水泡洗浄でGo！

フルスクリーンShellの夢

開発：ふあぁ…　よく寝ました。

基盤：午睡をしたのは久しぶりですね。

社長：今日は夢に ESC [が出てきました。部分スクロールとか。cosmosの画面とか。

開発：そういえばもうずっと、ステータス行のあるshellを使ってないですね。

社長：macOSのターミナルでステータス行って出せるんですかね？画面の一番下に。

開発：特定のターミナルソフトに期待したり依存せずに、自前でステータス行を作った

ほうが良いのではないかと思います。部分スクロールで良いのでは。

基盤：Goでcurses ライブラリパッケージを作っている人は居ますね。goncurses とか gocurses とか。

開発：あれ？これって単に import “C” すればCのライブラリが使えるという事のようですが。。。pkg/C … おや、golang.org/cmd/cgo に飛ばされました。

社長：そういえばそれ、Cgo ってものがあるって事は覚えています。

開発：げげ、普通に Go の中に C が書けるんですね。どれどれ、Hello World…

```
iMac% cat hello-cgo.go
package main
// #include <stdio.h>
// void hello(void){ printf("Hello, World!\n"); }
import "C"
func main(){
        C.hello()
}
iMac% go run hello-cgo.go
Hello, World!
iMac%
```

社長：感動した。

開発：つまり、GoはCコンパイラとしても使えると。

社長：さらばVC！

基盤：Cの部分をコメント扱いにしちゃってるのが悲しいような。

開発：で、バイナリサイズは…

```
iMac% go build hello-cgo.go
iMac% ls -l hello-cgo
-rwxr-xr-x  1 ysato  staff  1516328 Sep  3 17:34 hello-cgo
iMac% file hello-cgo
hello-cgo: Mach-O 64-bit executable x86_64
iMac% size hello-cgo
__TEXT   __DATA   __OBJC  others  dec     hex
856064  225280  0       67305472        68386816        4138000
iMac%
```

社長：Goのでっかいしっぽは付いてくるんですね。

開発：で、逆は…　なるほど、Goの関数はこうやってCにexportするのか…

基盤：どんどんCに戻っていきそうですがw

開発：全然構いません。実際、可変長データ、スライスを扱うのにGoは便利ですけど、あとは普通にC風言語としてしか使ってないですからね。型宣言とforの構文がちょっと違うだけみたいな。IMEの入力部分は最初Cで書いた版を取り込むのに、自分で fprintf とか互換関数を書いたんですが、あれ必要なかったのか (; _ ;)。

社長：curses を使ってたのは30年前あたり…　というか主に学生時代です。最初は termcap だけで、いずれ curses を使うようになったような。あの頃のコードから骨を拾ってきますかね。

開発：まあ、我々のCUIの環境は当時より明らかに退化してますよね。

社長：といいますか、たとえばブラウザの窓とかフォームとかでテキストを入力する時、あれはGUI世界の中に分散したミクロなCUI世界だと思うのですが、とても貧しいCUIを使わされている感じがします。

開発：GUIでもテキスト入力をするところ全般にGShellを突っ込みたいですね。

基盤：ブラウザのURL窓とかフォームでshellコマンドが打てたらびっくりです。

開発：実際、ターミナルでコマンドを実行した結果を張ることはよくありますよね。

社長：要はIMEですね。分散したCUI世界を、裏で一つに繋ぐ。

基盤：CUI vs GUI だと、C vs Go みたいですｗ

開発：CとGoのIntegrationでCGIかなｗ

社長：ところで、Gshellはずっと1ファイルでいけますかね。

開発：今6,000行くらいですが、10万行くらいはへっちゃらな感じがします。

```
iMac% wc gsh.go
    6181   18652  170060 gsh.go
iMac% time go build gsh.go
go build gsh.go  0.13s user 0.13s system 166% cpu 0.155 total
```

開発：ただ、ユーザが特定の関数をカスタマイズしやすいように、主だった関数はプラグインで置き換えられるようにはするべきかと思います。

社長：実行時に生成したプログラムをプラグインできると良いですね。

開発：そこはちょっと…　たぶん、動的リンクは一回しかできないので。でも exec しちゃえばいいのかな。実行状態は継承して。

＊　＊　＊

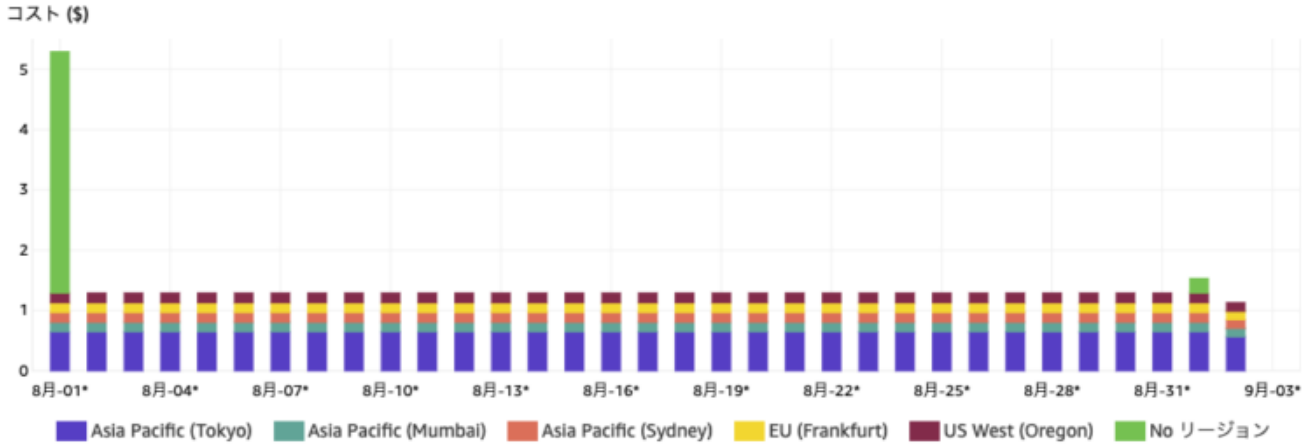
基盤：それはそうと今日は、HTML署名の作業は何かしないんでしょうか？

開発：ん、まー、一日一善、何かやりますかね。

社長：善かどうかはわかりませんけど、コードレベルでも前進はしたいですね。

経理：アマゾンから請求書が…　ああ、ライトセール代ですね。

基盤：これ以上無い明朗会計です。



基盤：Tokyoぶんは使わなくなったインスタンス２つ、40円/日削れるんですが、インスタンスを捨てる前の確認がまだできていません。

経理：水道代も来てますね。PayB でぴっ。快感〜。パスコードを。

社長：ぷちぷちっと。

携帯：ぶーっ。

Mac：ぽーん。

経理：納付完了しました。

開発：これ、よく出来てますよね。

基盤：しかしこれ、2ヶ月で4,851円。上水道代3,300円、下水道代1,551円て、サービスとしてどうなんでしょうね？1日80円。こちらにはサービス業者の選択肢が無い。

社長：一日50円で霞ヶ浦のおいしい水が飲み放題みたいな。

開発：ここで飲んだことないですけどね。

社長：昔はブリタでよく飲んでました。

基盤：げっ、もうこんな時間に…

社長：血圧を測定…　よた話を書いてる時は上がらないみたいですね。

JavaScriptでRSA

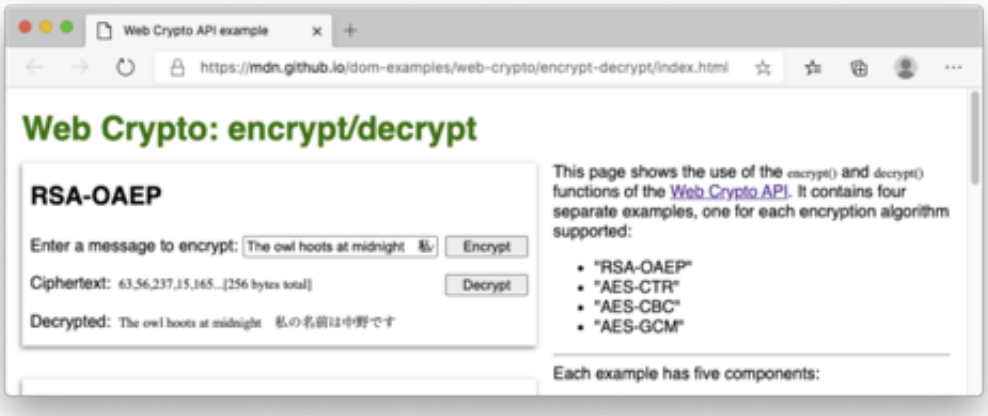
開発：それでは電子署名の件をやりましょう。まずはやはり、JavaScriptにて。この SubtleCrypto.encrypto() ってやつですかね。

社長：HTTPSのコンテクストでしか使えないってありますね。オフラインでは使えないですかね。ローカルファイルに使えれば。

開発：そもそもJavaScriptではローカルファイルへのアクセスはできないんじゃないですかね。GShellをHTTPSサーバにすれば良いのではないかと。

社長：extension 使ってもだめなのかなぁ。

開発：で、これがデモページ。



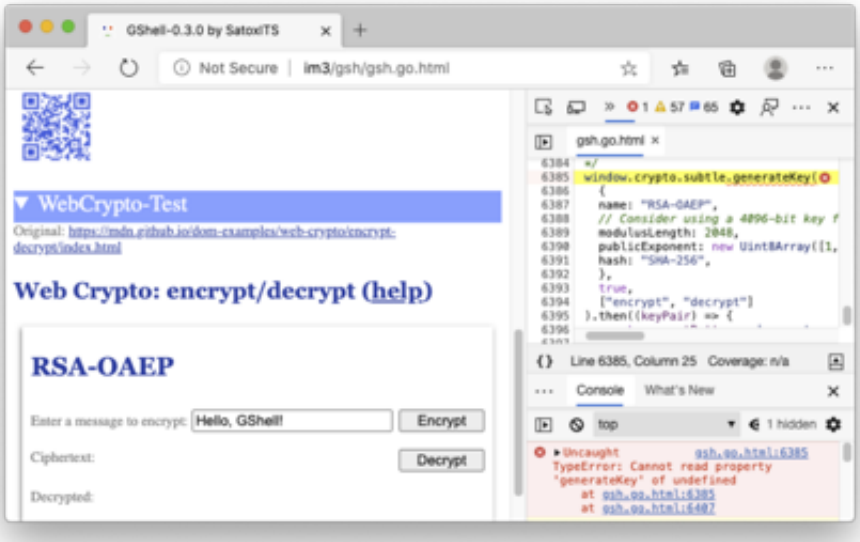
開発：View Page Source…

社長：簡単過ぎて意味がわかりません。

開発：まあここはHTMLの箱を定義しているだけですからね。JavaScriptはこちら。

社長：ああ、ほっとしますね。でもやっぱり簡単。

開発：ちょっとこのブログサイトにコピーしてテストしてみましょう。というか、まずgsh.html に組み込んじゃって…



社長：HTTPSじゃないので、きっちり怒られますね。

開発：で、これをこのブログ記事に貼り付ける…

基盤：おお！表示がきちゃないけど、ばっちり機能してますね。

開発：このCSS書いた人も、こんなふうに埋め込まれるとは想像しなかったでしょうね

w

社長：ちょっと興奮したので血圧を測定…　ありゃりゃ、大台を突破してます。

開発：行儀正しいCSSなんだと思いますが、スマホ時代のモノではないなと思います。

基盤：なんか、こんな副作用も出てますね。

開発：このCSSは全削除します。

＊　＊　＊

社長：思うに、ブログには載せたいけど、この部分は検索サイトにキャッシュされたくないなという部分はあると思うんですよね。そういう場合に、一部を暗号化して置くのは便利だと思います。

開発：すごい昔に、通信を暗号化しちゃいかんみたいな法があったような記憶もありますけどね。

社長：あるいは匿名で書きたいけど、後で誰が書いたのか証明する必要が出てきた時には出来るとか。

基盤：タイガーマスクのタカハシナオトみたいな。

開発：普通、平文の全文をRSAすることは無いと思いますが、ショートメッセージならRSAで暗号化が管理がシンプルで良いかもですね。暗号化して公開側の鍵も添付しちゃう。

社長：クリアテキストで署名はダイジェストに適用して別添ていうのが普通だとは思いますけどね。ただ、クリアテキストの部分が伝達経路で一部機械的に変わってしまう可能性は、現代でも考慮しておく必要はあるのかなと思います。

＊　＊　＊

社長：明日は定期検診なのでそろそろ終わりましょう。血を抜かれる予定でもあり。

開発：そうですね。今こんな状況です。

社長：これを見て思ったんですが。GShell をやめて GShe!! にしようかなって。あと、この日本語入力がGShell IMEで実現できたらって。

基盤：暗号文が256バイトブロックに収まらない場合には何が起こるんでしょうか。

開発：・・・たぶん対処してないです。明日検討します。

開発：ともかく、これをやってて色々びっくりしました。まず、CSSで上書きをする !important を何時の頃からか !import だと思ってしまっていたんです。なんだか効かないなーと思ってましたw。それと、e.innerHTML=xxx を e.innnerHTML=xxx とか　打ち間違えてしまったんですが、通っちゃうんですね。

社長：クォートしなくていいんで、タグの属性名って予約語的なものかと思ってました。

開発：つまり、一つエレメントを作っておけば、その属性値として何でもぶちこめる。コーディングの見た目もごちゃごちゃしなくていいかなと思います。

基盤：ということは、e.digest とか e.esign なんて属性を決めて、そこにダイジェストや電子署名を入れておけばよいということでしょうか？

開発：・・・そういうことになりますね。明日もう一度確認します・・・

社長：・・・思い違いでないとすると、ちょっと劇的な展開ですね・・・

開発：style とかは出来たと思いますが、 onclick とかも全部 JavaScript で押し込めるとすると、書き方が劇的に変わりますね・・・

社長：あとは document.getElementById(“*name*“) なんていう長たらしいのを書かずにすんだら、もっとスッキリするのにね。

開発：そこは我慢して一度だけ var *name* = document.getElementById(“*name*“) をするとします。var は参照されるたびに評価されるみたいなんで、いろんな処理が名前だけで参照できて、”.” でつなげるんだと思います。

社長：ダイナミックなマクロみたいですね。

開発：処理の結果を次の処理に渡す記法という意味でも便利ですよね。GShell もこういうふうにすると良いのかなとも思います。scanf().printf() みたいな。

社長：逆にshellのパイプで数珠つなぎにする的なのが JavaScript で書ければ良いと思うのですが。

開発：あと、今日はWordPressの拡張HTMLブロックの中でJavaScriptコードを開発するという妙な実験をしたわけです。ちょこちょこっといじる分にはまあ良いのですが、長いのになるとつらい。特に行数が12行程度で固定されているのが。タブも入れられない。もちろん、vi でも無く。

基盤：vi 互換のブロックエディタがあると良いですね。

開発：あと、そのブロックを独立なURLとしてダウンロードできると良いです。まあ、NFSでファイルとして見えたら最高かも。

開発：それと、ブラウザ内蔵のデベロッパーツールでは、Edgeが一番見やすいかなと思っています。

社長：MSのブラウザが最高とは。時代が変わりましたね。

— 2020-0903 SatoxITS

http-im3-gsh-gsh-0.3.0.go_.htmlrusage ダウンロード

```
/*
                                        GShell version 0.3.0 // 2020-09-03 // SatoxITS
```

GShell // a General purpose Shell built on the top of Golang

```
It is a shell for myself, by myself, of myself. -SatoxITS(^-^)

0 | | Fork | Stop | Unfold | Cksum | */ /*
▶ Statement
*/ /*
▶ Features
*/ /*
▶ Index
*/ //
▶ Go Source
//
```

▶ Considerations

// /*

▶ References

/ /

▶ Raw Source

/ /

▼ WebCrypto

Reference: https://mdn.github.io/dom-examples/web-crypto/encrypt-decrypt/index.html

Web Crypto – RSA-OAEP

Plain text:

Cipher text:

Decrypted text:

PublicKey…

*///