株式会社 ITS MORE
2020年4月設立

2020年9月11日 投稿者: SATOXITS

GShell 0.3.8 – HTML署名

社長：今日は何から行きましょうか。

開発：きのうはSSL関係の調べ物とかトライアルで数時間、非常に疲れました。今日はぼちぼちやりたいですね。

社長：でもやはりHTML署名が軸ですね。

固まるライトセール

基盤：ところで先ほどから当社LSムンバイ支部に繋がらなくなっています。dfに応答しないので、リブートを掛けたら立ち上がらなくなりました。ping には反応するのですが、ssh というか 22番に繋がらない。

開発：NFSの関係ですかね。

基盤：確かにmountで見るとシドニーへのマウントが残ってはいたのですが、永続的なNFS設定ではないので、リブートすればきれいさっぱりするはずなんですが…　今、VMレベルでの再起動を掛けているところです。

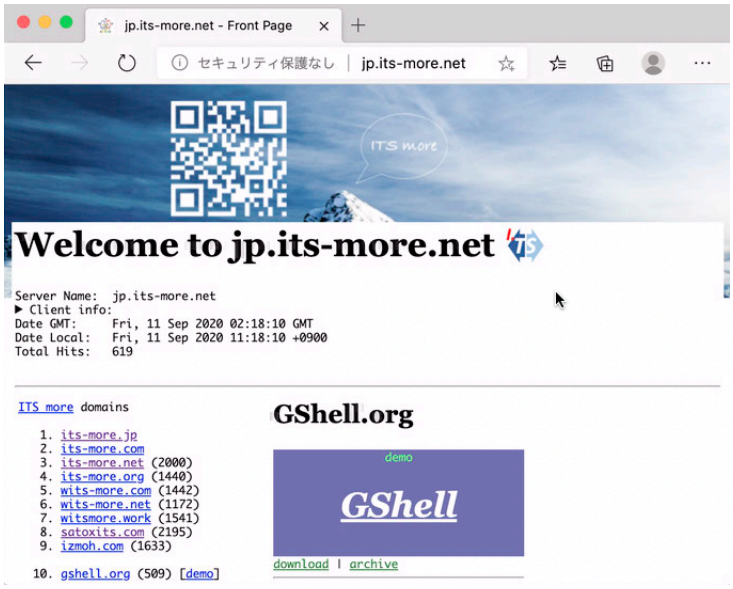
社長：他のポートはどうですかね。HTTPとか。

基盤：satoxits.comから行きます。うーん、どうしてこのサイトをポルトガル語だと思

いたがるんですかね？前々から。ASCIIしか無いのに。あれ？in.its-more.net、つながりました。…　そうこうするうちにSSHも。

開発：ライトセールは、自前でリブートすると繋がらなくなる事が良くありますね。VMインスタンスとファイアウォールとの連携がうまく行ってないのかも。

基盤：おっと、its-more.netフロントページがちょうど2000PVになってます。記念写真をパシャ。



基盤：それで、先ほどのリブートの件、ブートのログを見ると、外から繋げなくなっただけでなくて、実際に立ち上がって無かったようです。少なくとも、ユーザのcronが実行されるフェーズまでは至ってません。

```
in1% date
Fri Sep 11 02:39:24 UTC 2020
in1% boots
2020-0911-01:37:48 #0.0 Trigger reboot
2020-0911-01:37:48 #0.1 Sync before reboot
2020-0911-01:37:48 #0.2 Now sudo reboot
2020-0911-02:05:04 #1.0 Start Daemons on Reboot
2020-0911-02:05:09 #1.1 Finished Starting Daemons
```

開発：dmesg的にはどうですかね？

基盤：その後にリブート成功した時にきえちゃってますからね…　このリブートでは…　dmesgは6.3秒で終わってます。1.6秒経過時点のログがこれ。

```
[    1.622002] rtc_cmos 00:02: setting system clock to 2020-09-11 02:00:34 UTC (1599789634)
```

開発：システム起動時が02:00:34 で、ユーザの cron まで回ってきたのが、02:05:04。4分半かかってますね。

基盤：ライトセールに限らず、AWSは再起動に非常に時間がかかる事があります。その時の /var/log/messages …

```
Sep 11 02:00:39 ip-172-26-6-121 kernel: [    6.327890] Key type id_legacy registered
Sep 11 02:00:39 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 1080ms.
Sep 11 02:00:40 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 2080ms.
Sep 11 02:00:42 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 4120ms.
Sep 11 02:00:46 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 8020ms.
Sep 11 02:00:54 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 15760ms.
Sep 11 02:01:10 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 30480ms.
Sep 11 02:01:40 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 63530ms.
Sep 11 02:02:44 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 110750ms.
Sep 11 02:04:35 ip-172-26-6-121 dhclient[2236]: XMT: Solicit on eth0, interval 125610ms.
Sep 11 02:05:02 ip-172-26-6-121 acpid: starting up with netlink and the input layer
```

開発：なんにしろネットワーク関係の待ちのようですね。dhclient て DHCP？

基盤：そもそも 01:37にリブートを掛けた後に止まるところ停滞してます。

```
Sep 11 01:37:49 ip-172-26-6-121 ntpd[2587]: 139.59.15.185 local addr 172.26.6.121 -> <null>
Sep 11 01:39:30 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 130290ms.
Sep 11 01:39:44 ip-172-26-6-121 kernel: [4790565.233505] nfs: server au1 not responding, tim
Sep 11 01:39:44 ip-172-26-6-121 kernel: [4790565.241018] nfs: server au1 not responding, tim
Sep 11 01:41:40 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 112280ms.
Sep 11 01:43:33 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 128540ms.
Sep 11 01:44:52 ip-172-26-6-121 kernel: [4790872.441814] nfs: server au1 not responding, sti
Sep 11 01:45:41 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 125010ms.
Sep 11 01:47:46 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 111000ms.
Sep 11 01:49:37 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 131290ms.
Sep 11 01:51:49 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 120850ms.
Sep 11 01:53:50 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 116270ms.
Sep 11 01:54:25 ip-172-26-6-121 kernel: [4791445.897443] nfs: server au1 not responding, tim
Sep 11 01:55:46 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 120760ms.
Sep 11 01:57:47 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 108420ms.
Sep 11 01:59:35 ip-172-26-6-121 dhclient[2243]: XMT: Solicit on eth0, interval 124260ms.
Sep 11 02:00:38 ip-172-26-6-121 kernel: imklog 5.8.10, log source = /proc/kmsg started.
Sep 11 02:00:38 ip-172-26-6-121 rsyslogd: [origin software="rsyslogd" swVersion="5.8.10" x-p
Sep 11 02:00:38 ip-172-26-6-121 kernel: [    0.000000] Linux version 4.14.181-108.257.amzn1.
0170915 (Red Hat 7.2.1-2) (GCC)) #1 SMP Wed May 27 02:43:03 UTC 2020
Sep 11 02:00:38 ip-172-26-6-121 kernel: [    0.000000] Command line: root=LABEL=/ console=tt
Sep 11 02:00:38 ip-172-26-6-121 kernel: [    0.000000] x86/fpu: Supporting XSAVE feature 0x0
```

開発：au1向けのNFSも何か悪さをしてたですかね。

基盤：au1側のファイアウォールでNFS制限しちゃってますからね。でこの in1 での Solicit on eth0 ですが、IPv6が無いのに取りに行くと出るという説明があります。メッセージがそれっぽく無いですが。

開発：アマゾン純正Linuxなのにこういうのは困りますね。

社長：これも面白そうですが、いずれ時間がある時に。

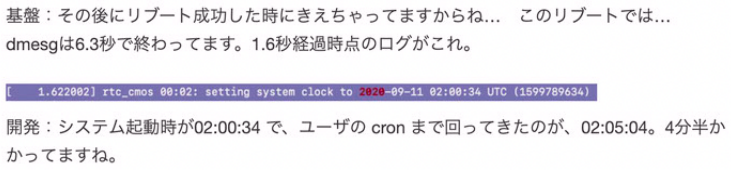
WordPressのブロックのセンタリングって

社長：ところで、TwentySeventeenをシングルカラム表示する機能が無いと、もはや非常に不便なので、とりあえず GShell HTML を貼り付けます。

開発：いずれこの機能だけ切り出してプラグインか何かにしてサイドバーにでも貼り付けましょう。ミニマムGShellウィジェットみたいな。

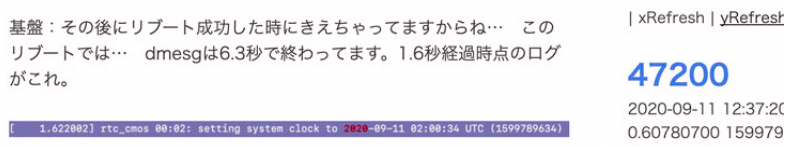
基盤：WordPressのブロックエディタって、編集状態で図のセンタリングの表示実際と全然不整合なのも気持ち悪いですね。

社長：現行版になってから特にそうですね。デフォでセンタリング表示されてしまっている。実際には左寄せ。これもシングルカラムにして見ないと確認できない事が多いです。例えばこの記事にしたって、編集中の action=edit で見るとこう。



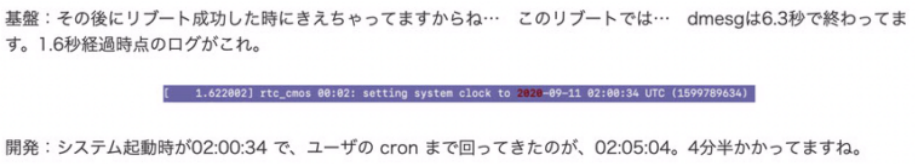
基盤：左寄せに見えます。

社長：公開状態で見るとこう。



開発：表示幅を使い切ってるので、センタリングされてるのかどうかわからないですね。

社長：で、シングルカラム表示にするとこう。



基盤：センタリングされてます。

開発：表示カラム数というより、現在の、というか、全体と primary のパートの幅を調整する機能があると良いのかも知れません。

社長：これも面白そうですが、いずれ時間のある時に。食事に行ってきます。

ほうとうの空.net

社長：ただいま。かき氷を買ってきました。

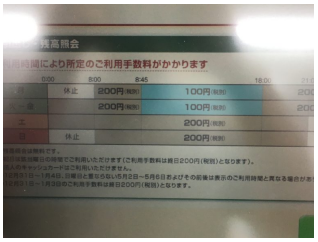
基盤：ゲッツ！

社長：今日はあちらこちらに「ほんとうの空」が出てました。

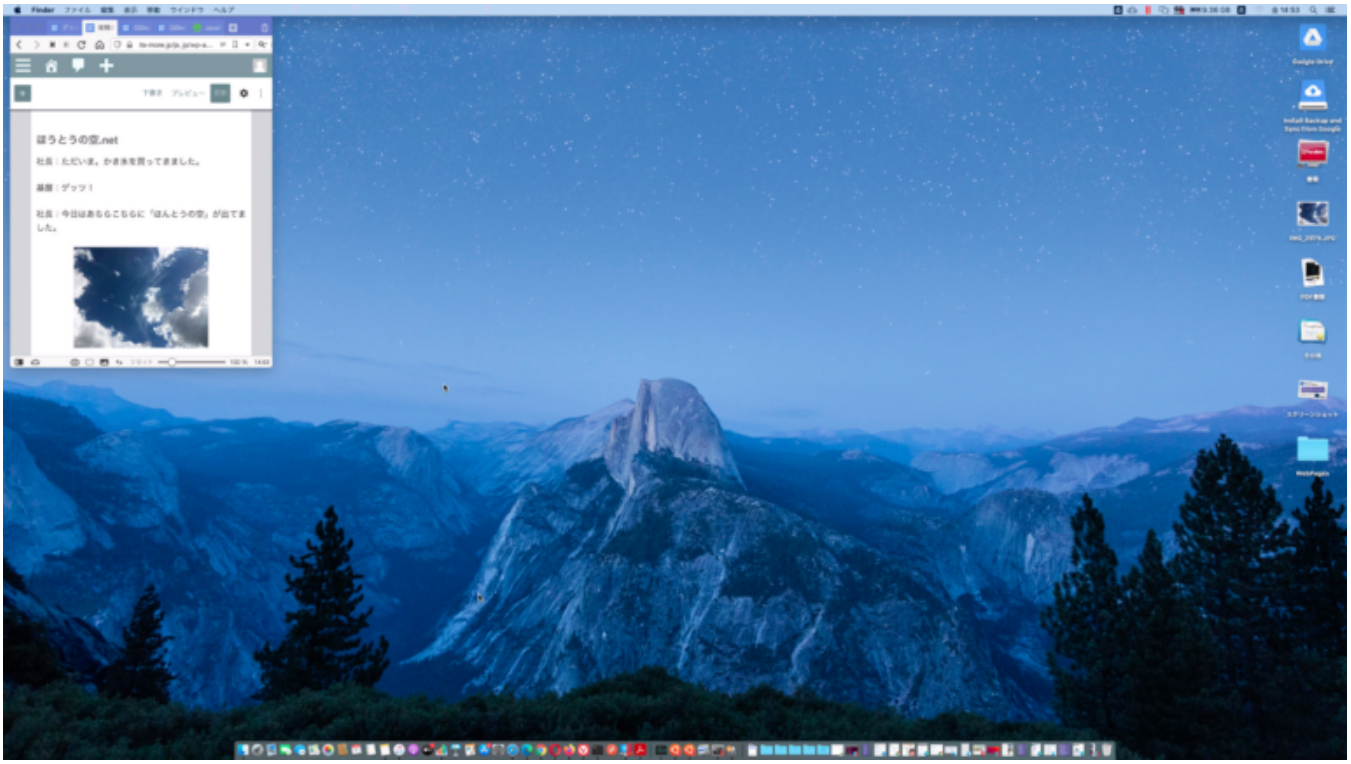




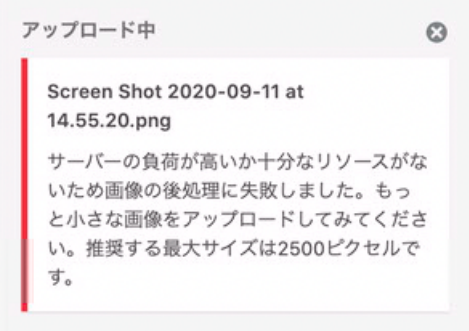




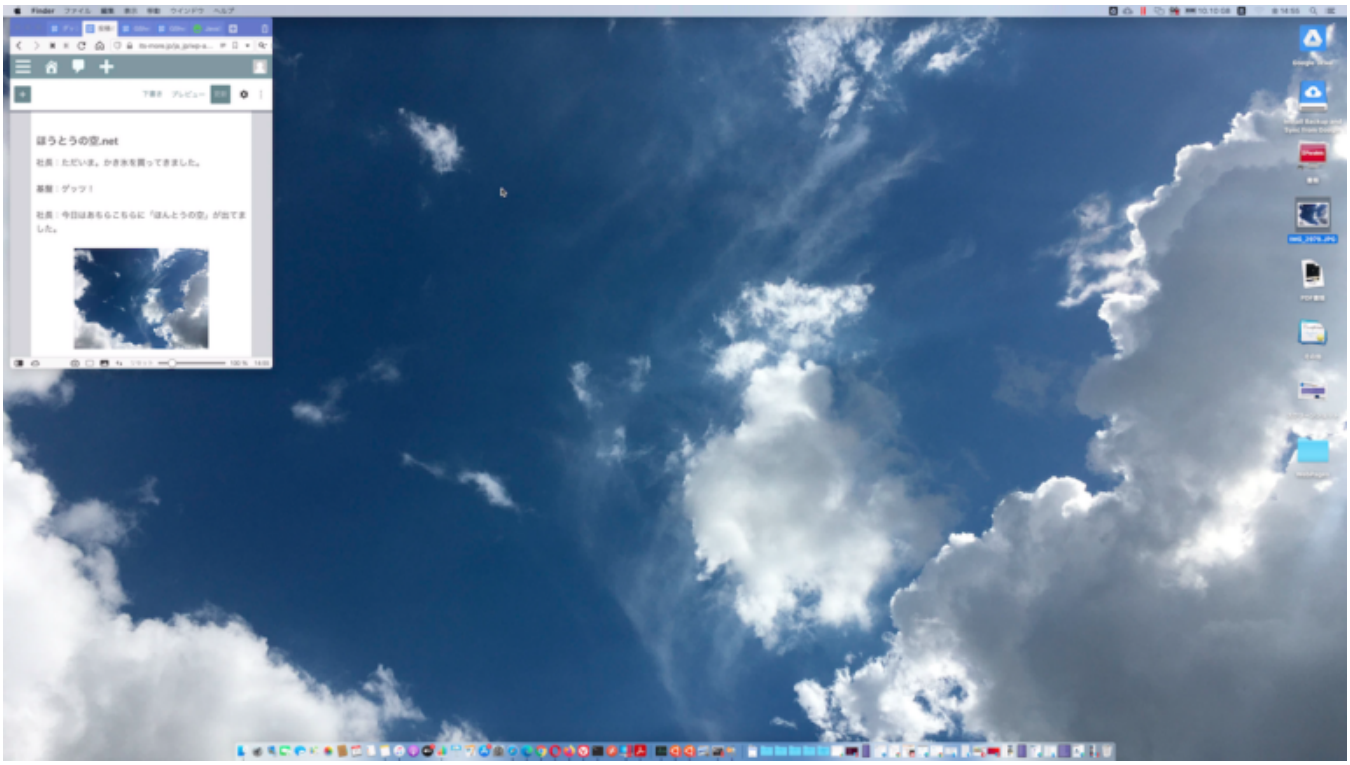
社長：ちょっと壁紙にしてみます。これがCatalinaオリジナル。



社長：そしてこれが・・・あれ？



社長：6MB程度でへこたれますかね。仕方がない、じぶんで圧縮してアップロード…



開発：これは気分が上がります。

基盤：NASAが宇宙から送ってくる画像に引けを取らないです。

開発：まあ、宇宙で一番綺麗な星からから宇宙を見てるわけですしね。

社長：ついでにサイトの背景も変えましょう。うーん、印刷も考えると、吹き出しの調整が難しいですね。ここかな？フォントはお気に入りのBradley Hand。

開発：体裁のために作ったサイトでしたが、あの山に吹き出しを付けた時から愛着がわきました。

社長：吹き出しの魔力ですね。

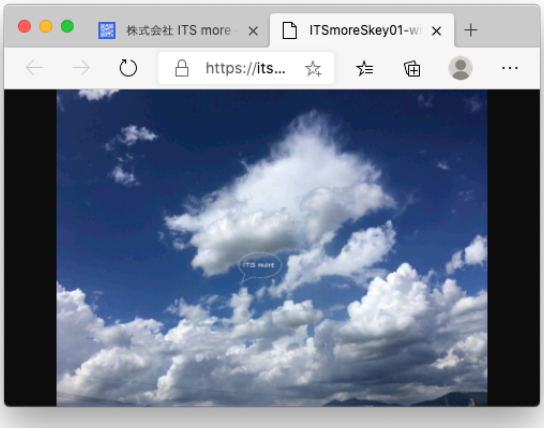
基盤：吹き出しの出どころの雲が消え入りそうな雲ですね。

社長：まあうちはそういう存在です。

開発：クラウドの巨人にモノ申すみたいな。

基盤：画面サイズを大きくすると左下に電線が映ります。

社長：画像だけで見ると舞台裏全景が見えるという嗜好です。



開発：地上が映ると突然日常的な風景に見えるのが面白いですね。

社長：下向きに日常を送っていると気づかない、その上にはいつもこんな、ほんとうの空が出ていたんだなと思いました。

開発：そういえば子供の頃は空をよく見てましたね。

社長：育った家のあたりの空は圧巻というか壮観というか、そういうふうに見える事がよくありました。今帰ると、そうも思わないのですが。

基盤：空に憧れて〜♪

社長：子供とか新人さんの目が輝いて見えるのは、顔を上向きにしてるからだと思うんですよね。まだよく知らない世界だから、顔を前か上に向けて周囲を観察しないと暮らしていけない。だから目に入った光線が反射して輝いて見える。これ、昔からの持論です。

HTML署名の表現形式

開発：それで、HTML署名を何処にどう入れるかなのですが。

社長：span に data-* で入れるという話でしたね。

開発：見苦しても良いかなと思ったのですが、色々属性を追加したいとなると、やはり見苦しすぎるように思えて来ました。こんなふうです。

```
/*<span
 id="gsh-digest"
 class="_digest_"
 data-target-id="gsh"
 data-crc32u="3302073024"
 data-length="194682"
 data-lines="6943"
 data-time="1599817503504"
 ></span>
*/
/*<html>
<span id="gsh">
<span id="gsh-digest" class="_digeste_" data-target-id="gsh" data-crc32u="150472587" data-length="194686" data-lines="6943" data-time="1599815435485">
</span>
```

開発：上のように人間がテンプレートを書いても、DOMではタグの中の改行情報とか保存されませんから、一行で生成してしまうわけです。人間が読み書きするHTMLの中にこういうのが混じってるのは嫌だなと。

社長：いっそRFC822形式にするというのはどうでしょう。S/MIME互換にしちゃう。

開発：全体に対する署名だけなら良いですが、内部の部品単位に署名する時にはやはり、multipart形式は厳しいかなと。Go や HTML と混在するのは見た目が痛すぎるかと。

基盤：RSAで署名したデータは256バイトになるんですかね。base64にしたらその4/3倍。これもかなり見た目に痛くないでしょうか？

開発：まあ72文字で折り返せば四行ですね。

基盤：同じエレメントに複数人が署名するというケースもありますよね。

開発：・・・

社長：data URL 以外で、属性って途中で折り返しても良いのでしょうか？

開発：属性値のクオートの中なら自由なのでは。で、base64文字列の中に改行が入ってたら無視するで良いかと思います。もちろん、innerHTMLの中なら無問題なのですが。うーん、やっぱりHTMLで書いてタグでhiddenにするのが良いのかな・・・

基盤：XMLかJSONで書くとか。

社長：見た目の問題は、やって見て、実際に見て感じてみないと何ともですね。

開発：そうですね。

S/MIMEにならう

社長：署名をどう表現するかとは別に、どういう情報を入れるかですが。これは、S/MIMEにならうのが良いのではないかと思います。

開発：そうですね・・・ S/MIME… RFC… おや、最近は CMS (Cryptographic Message Syntax) って呼ぶんですかね。どういう関係なのやら。えーと、S/MIME の最新の規格はv4.0、RFC8551のようです。2019年4月発行。メッセージの見た目はこんな感じ。

```
A sample message would be:

Content-Type: application/pkcs7-mime; smime-type=signed-data;
   name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

MIIDmQYJKoZIhvcNAQcCoIIDijCCA4YCAQExCTAHBgUrDgMCGjAtBgkqhkiG9w0BBw
GgIAQeDQpUaGlzIGlzIHNvbWUgc2FtcGxlIGNvbnRlbnQuoIIC4DCCAtwwggKboAMC
AQICAgDIMAkGByqGSM44BAMwEjEQMA4GA1UEAxMHQ2FybERTUzAeFw05OTA4MTcwMT
EwNDlaFw0zOTEyMzEyMzU5NTlaMBMxETAPBgNVBAMTCEFsaWNlRFNTMIIBtjCCASsG
ByqGSM44BAEwggEeAoGBAIGNze2D6gqeOT7CSCij5EeT3Q7XqA7sU8WrhAhP/5Thc0
h+DNbzREjR/p+vpKGJL+HZMMg23j+bv7dM3F9piuRx0DcMkQiVm96nXvn89J8v3UOo
i1TxP7AHCEdNXYjDw7Wz41UIddU5dhDEeL3/nbCElzfy5FEbteQJllzzflvbAhUA4k
emGkVmuBPG2o+4NyErYov3k80CgYAmONAUiTKqOfs+bdlLWWpMdiM5BAI1XPLLGjDD
HlBd3ZtZ4s2qBT1YwHuiNrhuB699ikIlp/R1z0oIXks+kPht6pzJIYo7dhTpzi5dow
fNI4W4LzABfG1JiRGJNkS9+MiVSlNWteL5c+waYTYfEX/Cve3RUP+YdMLRgUpgObo2
OQOBhAACgYBc47ladRSWC6l63eM/qeysXty9txMRNKYWiSgRI9k0hmd1dRMSPUNbb+
VRv/qJ8qIbPiR9PQeNW2PIu0WloErjhdbOBoA/6CN+GvIkq1MauCcNHu8Iv2YUgFxi
rGX6FYvxuzTU0pY39mFHssQyhPB+QUD9RqdjTjPypeL08oPluKOBgTB/MAwGA1UdEw
EB/wQCMAAwDgYDVR0PAQH/BAQDAgbAMB8GA1UdIwQYMBaAFHBEPoIub4feStN14z0g
vEMrk/EfMB0GA1UdDgQWBBS+bKGz48H37UNwpM4TAeL945f+zTAfBgNVHREEGDAWgR
RBbGljZURTU0BleGFtcGxlLmNvbTAJBgcqhkjOOAQDAzAAMC0CFFUMpBkfQiuJcSIz
jYNqtT1na79FAhUAn2FTUlQLXLLd2ud2HeIQUltDXr0xYzBhAgEBMBgwEjEQMA4GA1
UEAxMHQ2FybERTUwICAMgwBwYFKw4DAhowCQYHKoZIzjgEAwQuMCwCFD1cSW6LIUFz
eXle3YI5SKSBer/sAhQmCq7s/CTFHOEjgASeUjbMpx5g6A==
```

開発：署名情報は MIME ヘッダの中に分離してあるのかと思っていましたので、意外です。

社長：クリア署名のサンプルはないんですかね？

開発：ないですね。というかこれ、MIME形式に署名するには何がどうという話がほとんどなので、ちょっとペンディングかなと思います。

社長：正規化の件は、HTMLの署名でもDOMダンプというかプリティプリントというかの違いによるので、気になるところではあります。

基盤：DOMの内部表現が一定だとすると、それが正規化なんじゃないですかね。だとすれば自前でツリーをトラバースして署名を作るとか。

社長：まあそうかも知れません。ただ、HTML/JavaScriptではなく、Goでも署名・検証はしたいんですよね・・・

開発：ともかく、やることは、ダイジェストデータを公開鍵の一方で暗号化する、つまり署名するということだけなんです。で、検証する時にはそれをもう一方の鍵で復号する。復号できたらOK。それだけのはずです。

社長：とりあえず独自路線で行きますか。かき氷でも食べましょう。

社長：そういえば今日これをゥエルシァで購入して会計する時に、ちょっと店員さんの対応に感動しました。コンシェルジェですかみたいな気配り感で。レジ袋についても当然ですが、かき氷にもスプーンを付けますかとかちゃんと聞いてくれるし。

基盤：てかこれ、木のサジがかき氷一つ一つに載ってますね。

社長：それもびっくりですが、帰って来て気付いたんですが、3箱買ったマルボロがちゃんと輪ゴムでまとめてあるんです。

基盤：プロの仕業ですね。

社長：ちなみに、若くて美人さんでした。

開発：あそこは学習させてないロボットみたいな店員も居るし、人材が豊富ですねw

基盤：バイトのロボット野郎と美人コンシェルジェおねえさんは10倍は給料差がないと

納得できませんね。

新しい認証方式

開発：独自路線でという話なので、この際新しい認証方式を考えたいと思います。

社長：そこまで独自でなくても…

開発：基本は共通鍵なのですが、その鍵はそのデータを暗号化するためだけの使い捨てである、という感じのものです。要はパスワードなんですが、対象データとパスワードを合わせてハッシュして、そのハッシュ値でデータを暗号化する。処理はXORで十分と思います。

社長：認証は？

開発：そのパスワードを知っているのはその人だけだというところです。もし証明を求められたら、そのパスワードを開示する。

基盤：開示しちゃった後はもう使えないというか、他の人にも使えちゃうので証明にならないですね。

開発：それで、パスワードのハッシュを多段階にするわけです。100万段階とか。ハッシュでなくても、秘密の逆関数でもよいかもしれません。

社長：データでなくてアルゴリズムを秘密にすると。まあでもそれも、関数の引数というデータなのかも知れませんが。

開発：まあアルゴリズムもデータですけどね。

基盤：何回分ハッシュした値はなーんだ、って感じでチャレンジレスポンスするとよいかもですね。

開発：たとえば処理時間的に毎回10000回のハッシュが許容されるとすると、予めそれをそれを10000段階ぶん作ってスタート地点として記憶しておけば、1億通りの使い捨

てパスワードになります。

基盤：出発点が人間の入れたパスワードでなくても良さそうですね。ただの乱数。そのファイルにアクセスする権限だけで認証する。

社長：なんか面白いので飲みながら考えましょう。

＊　＊　＊

社長：久しぶりに飲み屋のはしごというものをしました。で考えたんですが、パスワードをハッシュして、っていう件は、そもそも太古よりパスワードはハッシュして記憶しておくのが普通で、これは当たり前すぎる技術。生のパスワードを送らないというのも、APOPとかダイジェスト認証でやっている技術。パスワードを繰り返してハッシュするという話は無限長の乱数の何番目というものとの違いがわからない、ということになりました。

開発：まあそんなことのような気はしていましたw

社長：以前考えたテラビット長の鍵というのもこれの親戚だと思います。まああれは盗んで運び出すのに物理的に時間がかかるっていうところがミソなわけですが。

開発：おとなしく非対称鍵暗号技術を使いましょうって事ですかね。

— 2020-0911 SatoxITS

http-im3-gsh-gsh-0.3.8.go_ ダウンロード

```
/* */ /*
GShell version 0.3.8 // 2020-09-11 // 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 | Digest | Source | */ /*

▶ Statement

/ /

▶ Features

/ /

▶ Index

*/ //

▶ Go Source

//

▶ Considerations

// /*

▶ References

/ /

▶ Raw Source

/ /

*///