しろねこ通信

Lsys News Vol.4
2014.09.20 発行

特集　大解説！！インターネットショッピングを支える暗号技術！

みなさんはインターネットでお買い物をしたことがありますか？支払いにクレジットカードをお使いになることも多いと思います。インターネットは、本来誰であっても見ることができるものです。しかしインターネットショッピングではクレジットカード番号のような個人情報をやりとりしています。これを安全に行うために使われているのが暗号技術です。

anazon　Racuten　YAFOO! JAPAN ショッピング

今回はこの暗号技術の仕組みににについて、解説してみたいと思います。現在多くのショッピングサイトで使われている技術が、SSL（Secure Sockets Layer）と呼ばれるものです。それを提供する仕組みとして世界中で広く使われているのが、OpenSSL です。OpenSSL は今年 4 月と 6 月に脆弱性が見つかり大騒ぎになりましたね。今や暗号化技術は世界的なインパクトをもたらす重要事項なのです。

この OpenSSL では公開鍵暗号方式という方法で暗号化を行います。暗号化を行う鍵が公開されているのです。なぜ公開されているのでしょうか？どうやって安全性を担保しているのでしょうか？公開されていることによって私たちはどのような恩恵を受けているのでしょうか？気になる方は裏面へどうぞ！

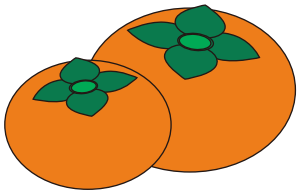
もっと詳しく！
裏面へ→

ほっと♪(´▽`) 健康

秋の味覚
柿の健康効果

豊かで深い甘みの柿、実はビタミン C を多く含む果物です。100g あたりの含有量はなんと 70mg、レモンやイチゴにも引けをとりません。

抗酸化作用のあるβカロチンも豊富に含まれており、風邪などの予防に効くと考えられています。気温の変化で体調を崩しやすいこの季節にぴったりの果物ですね。



また、柿をお酒のお供にすると悪酔いしないとも言います。利尿効果のあるカリウムやビタミン C や渋みの成分であるタンニンがアルコールの排出を助けるためです。

果糖も酔いを早く覚ます効果があるそうです。秋の夜長に深酒しても安心ですね。

パソコン＆スマートライフ教室
エルシス
Powered by RomeoLynx!

☎(0794)-88-8283（※日建学院さんと共通です）
〒675-1378　兵庫県小野市王子町 13　プリンスガーデンビル 1F
FAX:(0794)-88-8284　Mail: ono@l-sys.jp　URL: http://l-sys.jp
小野市　エルシス　検索

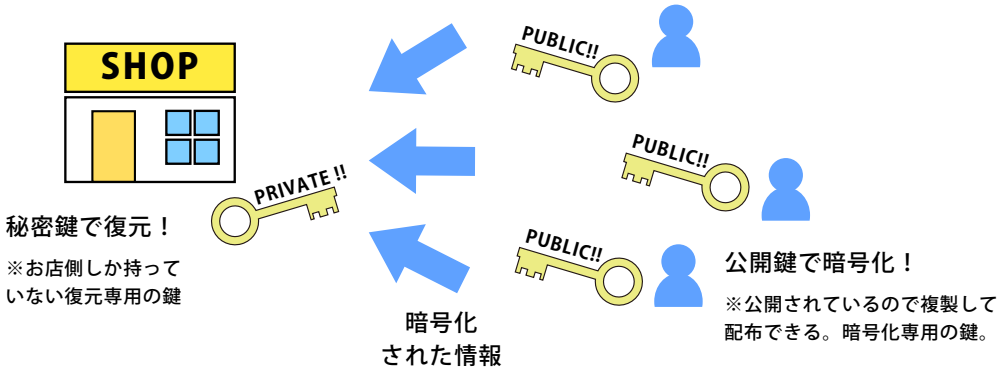
小野郵便局横！ P あり。日建学院さんと同じフロアです。

もっと詳しく！裏面

素数で守られる！？公開鍵暗号の仕組み！！

一昔前まで暗号化と暗号を復元する復号化の方法はどちらも非公開とされていました。これを秘密鍵暗号方式といいます。この方法は、鍵の受け渡しの手間や、鍵自体の漏洩の危険性があり使い勝手がとても悪いものでした。

そこで暗号化する鍵だけを公開する方法が考案されました。ショッピングサイトにはこの暗号化鍵が組み込まれていて、誰でも買い物できるのは鍵が公開されているおかげなのです（※ 暗号化の仕組みのあるサイトはアドレスが、https://www.○○○.com となっています）。一方、暗号を復元する鍵は秘密のままにします。これによりお店に送った情報はお店の人しか見ることができません。



ではここで公開されている鍵を使って暗号が破られることはないのか？という疑問が浮かびます。はい。理論的には可能です。しかしそれを行うには何百桁もの数字を素因数分解しなければならず、現在のコンピュータを用いても数百年かかります。つまり理論的には総当たり的に計算すれば暗号は破ることができますが実質的には不可能なのです。この暗号方式を RSA 暗号といいます。

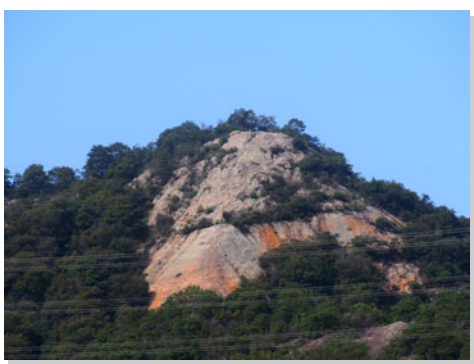
[PR]

エルシスでは毎週日曜（10:00 ～ 12:00）パソコン・スマートフォン何でも無料相談会を開催しております (※要予約)。セキュリティに関する疑問・質問、日頃不安に思われていることなどありましたら、お気軽にお声かけください。

地域の話題

紅山
(小野市来住町)

秋。行楽の季節ですね。山歩きなどはいかがですか？紅山とそれに連なる山々は小野アルプスと呼ばれています。特に紅山は岩場を登る楽しみや、標高が 200m に及ばないとは思えないほどの眺望で人気の山です。写真は加古川市側から紅山の露出した岩肌を撮影したものです。



楽技（ラク ワザ！）

エクセル操作の要！！マウスカーソルの形

Excel はひとつの動作（クリック、ドラッグなど）で様々な機能を使うことができます。今どの機能が有効になっているかは、マウスカーソルの形を見ると分かります。

同じように操作してもなぜかうまくいかないときときは落ち着いてマウスカーソルの形を確認してみてください。

下に基本的なものを掲載します。

基本の形。クリック操作、ドラッグ操作でセルを選択することができる状態です。

選択したセルの右下隅をポイントしすると表示されます。ドラッグ操作で連続したデータを入力するオートフィル機能が使える状態です。

選択したセルの枠をポイントすると表示されます。ドラッグ操作でセルの内容を別のセルに移動させることができる状態です。

行番号や列番号の境をポイントすると表示されます。ドラッグ操作で行や列の幅を変更できる状態です。

行番号や列番号をポイントすると表示されます。クリック操作で行や列を選択できる状態です。