StellarLink 隔月連載 第24回

Information Point！

意外と知られていないお得な情報や
今ICT業界で話題になっている事をご紹介！！

「ランサムウェア」ご注意ください！

『第18回 Information Point!』でもお伝えしました『ランサムウェア』
まだまだ感染の猛威は続いておりますので、再びのご紹介です！

ランサムウェアとは？

ランサムウェアとは、感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。
身代金要求型不正プログラムとも呼ばれますが、ほとんどの場合「身代金」を支払っても暗号化を解く事は出来ないようです。

感染すると・・・

一例ですが、ランサムウェアの「Locky」に感染するとデスクトップ上に以下のような赤字の警告文が表示され、デスクトップやマイドキュメント、アクセスしたサーバーなどに置いてあったWordやExcelと言ったファイルが暗号化され開けなくなります。

```
        !!! 重要な情報 ！！！！

すべてのファイルは、RSA-2048およびAES-128暗号で暗号化されています。
RSAの詳細については、ここで見つけることができます:
    http://ja.wikipedia.org/wiki/RSA暗号
    http://ja.wikipedia.org/wiki/Advanced_Encryption_Standard

あなたのファイルの復号化は秘密鍵でのみ可能であり、私たちの秘密のサーバー上にあるプログラムを、復号化します。
あなたの秘密鍵を受信するには、リンクのいずれかに従います:
    1. http://i3ezlvkoi7fwyood.tor2web.org/AAF92AC
    2. http://i3ezlvkoi7fwyood.onion.to/AAF92AC57C
    3. http://i3ezlvkoi7fwyood.onion.cab/AAF92AC

このすべてのアドレスが使用できない場合は、次の手順を実行します。
    1. ダウンロードして、Torのブラウザをインストールします: https://www.torproject.org/download/download-easy.html
    2. インストールが正常に完了したら、ブラウザを実行し、初期化を待ちます。
    3. アドレスバーにタイプ: i3ezlvkoi7fwyood.onion/AAF92AC57C
    4. サイトの指示に従ってください。

!!! 個人識別ID: AAF92AC57C          !!!
```

警告文を読むとどこかのサイトにログインし、操作すると暗号化を解除できるような事が記載されていたりしますが、実際に解除できる事はありません。
それだけでなく、記載されているサイトにアクセスしてしまうだけでも以下のリスクが生じます。

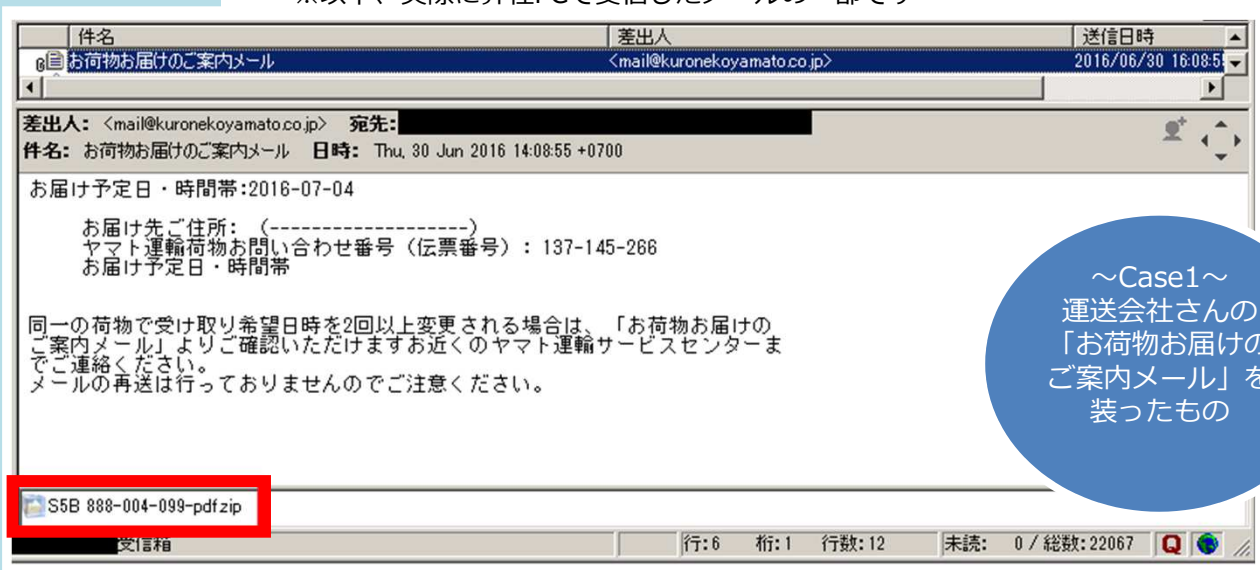
- **各種マルウェアがインストールされてしまう**
- **個人情報を盗まれる**
- **ウィルスなどが再侵入するための裏口（バックドア）を仕込まれる**

※最近では「Locky」だけでなく「Zepto」と言うランサムウェアが流行しているようです。
名前は違えども動作的には同じものなので注意が必要です。

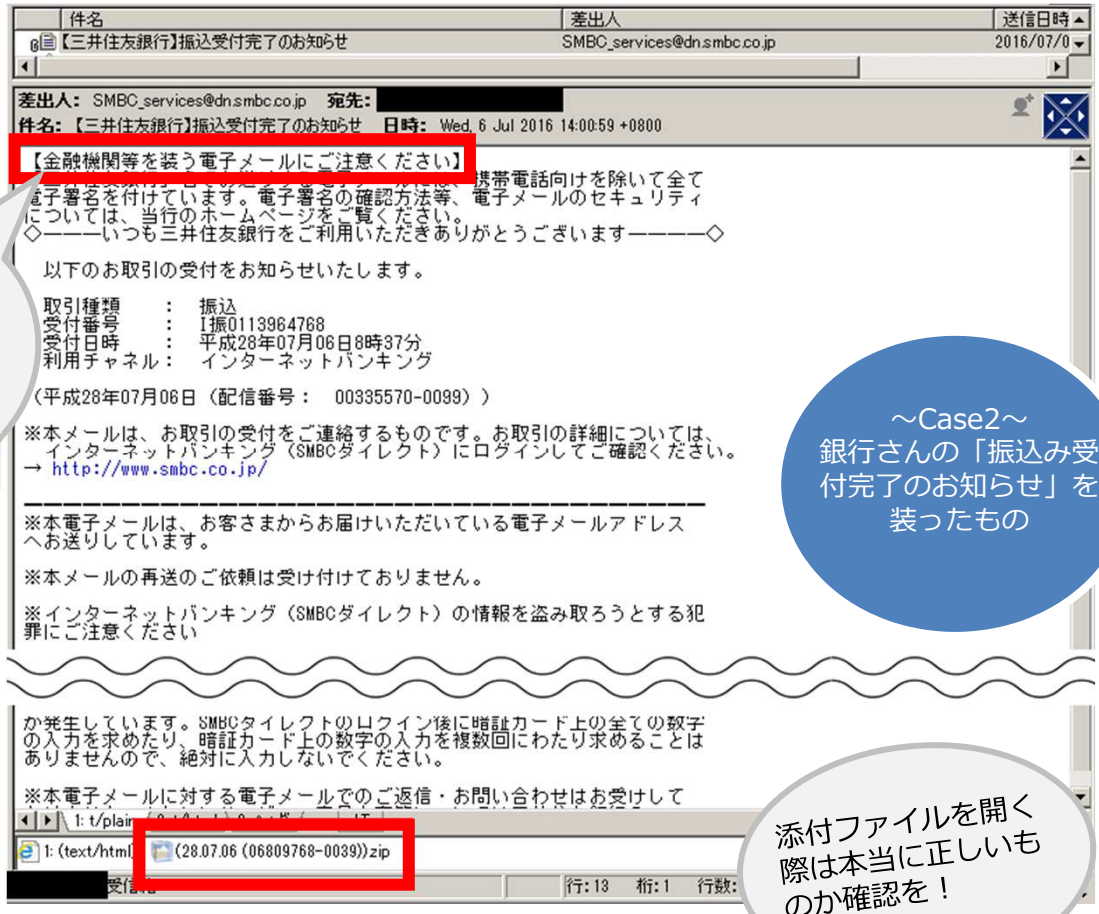
どうやって感染するの？

『ランサムウェア』は、**メールに添付されたファイルを開いたために感染**してしまうことが多いのです。
　最近では、セキュリティ意識の向上により、多くの方は身に覚えのないファイルは開く事が少なくなってきているせいか、**巧妙なメール**が多くなってきております。

※以下、実際に弊社PCで受信したメールの一部です



～Case1～
運送会社さんの「お荷物お届けのご案内メール」を装ったもの



～Case2～
銀行さんの「振込み受付完了のお知らせ」を装ったもの

添付ファイルを開く際は本当に正しいものか確認を！

心当たりがある場合、うっかり開いてしまいそうな件名と内容に見えますが、
どちらも添付ファイルが付いていますので、圧縮ファイルを解凍した時点で自動的にランサムウェアに感染し被害に遭う事になります。

ご注意ください！