平成３０年０３月３１日
リーダー　八田　崇史

３月度活動報告

平成３０年3月２４日（土）（第２３９回目）
１３：３０～１６：３０
参加者１１名

◆１時間目　ネット時代のセキュリティ護身術　　１３：３０～１６：１０　　１６０分
最終の６回目「万一に備え機密情報は暗号化で守る」
資料 2016.3.28　　89～92p　　4 ページ

★　パソコンやスマホ等の情報機器には、重要なデータが多く保存されている。万が一第三者の手に渡っても、情報漏洩対策の一つが「暗号化」である。

暗号化の技術では「暗号鍵」という秘密のデータを使い、データを決まったルールで変換するが、「暗号鍵」が判らないと正しい手順で元のデータに戻らないので「復号」が出来ない。

この暗号化ルールを「暗号アルゴリズム」と呼び、「ＡＦＳ」や「ＲＳＡ」等がある。アルゴリズムは、第三者が暗号鍵を割り出したり、元のデータを取り出したりする「解読」が通常では困難で、暗号化には２つの方式がある。

１．共通鍵暗号方式（AFS）
１つの暗号鍵を「暗号化」と「復号」の両方に使う従来の方法。

２．公開鍵暗号方式（RSA）
暗号化では、暗号鍵の秘密を守る点では「パスワード」と同じだが、暗号化したデータを渡す場合は、相手に暗号鍵を伝えないと相手は復号が出来ない様に考案されたのが「公開鍵暗号化方式」だ。

公開鍵暗号化方式では、ユーザが入力した暗号化の「公開鍵」と復号する「秘密鍵」のペアで利用する。「公開鍵」で暗号化したデータは、対になる「秘密鍵」でしか復号が出来ない。この様により大きなカギデータの「公開鍵暗号方式」の方が安全である。

注１．「ＡＦＳ」
128bit 以上の長い鍵を使って暗号強度を高め、シンプルなアルゴリズムで高速処理を可能としている。

注２．「ＲＳＡ」
公開鍵暗号の１つで３人の発明者の頭もじで命名。
文書を閉める鍵が「公開鍵」で、文書を開ける鍵が「秘密鍵」で、これをペアで使う。

データの暗号化として覚えておきたいのが「フアィルの暗号化」と「通信の暗号化」である。

★「フアィルの暗号化」と「通信の暗号化」

１．「フアィルの暗号化」
データの保存をする時に暗号化し、データフアィルを開いて表示や編集をする時に復号する。マイクロソフトのＯｆｆｉｃｅの各ソフト（ワードやエクセル等）には作成した書

類を暗号化して保護する機能がある。

文書を開いておいて

２０１０では「フアイル」→「情報」→「文書の保護」→表示されたドロップメニューの中の「パスワードを使用して暗号化」をクリックする。

２０１３・２０１６では「フアィル」→「情報」→「ブックの保護」→表示されたドロップメニューの中の「パスワードを使用して暗号化」をクリックする。

ソフトで暗号化できない時は、複数のフアィルやフォルダーをまとめて、１つの暗号化された圧縮ソフトの「Lhaplus（ラプラス）」を使う。

Windws10 には、ドライブに保存するデータ全てを自動的に暗号化する（デバイスの暗号化）機能がある。

設定→システム→バージョン情報→画面表示の［デバイスの暗号化］がある。

２．「通信の暗号化」

Ｗｅｂブラウザーやメールソフト等、通信機能を持つ個々のソフトウエアで幅広く利用されているのがＳＳＬやＴＬＳ技術。

インターネットにアクセスすると、アドレスが「https」で始まり「鍵マーク」表示されているので、ＳＳＬ／ＴＬＳで通信されているのが判る。

※　例　　Web ブラウザーやフアイル開示用のＵＲＬをコピーペーストした時、この表示が出来ません。

ヤフー画面（https）を開いて、別のブラウザーやフアィルのＵＲＬをコピーして貼り付けをしても（コピーしたＵＲＬが http なら）暗号化されてないので、アクセスできなく表示できません　になる。

何故なら暗号化のブラウザー画面で、暗号化されてないものを開くことが出来ないからです。

電子メールの送受信でもＳＳＬやＴＬＳが使われているが、Ｗｅｂと扱いが異なる。

ユーザのパソコンとメールサーバー間の通信は暗号化されているが、メールサーバー間や相手側のパソコンの送受信は暗号化されているとは限らない。

機密性の高い情報の場合は、添付フアィルは暗号化が必要だ。

◆２時間目　コンピュータの基礎講座　　１３講座の７回目　１５：０５～１５：２５　２０分

「どうしてメールにフアイルを添付できるの？」

資料日経ﾊﾟｿｺﾝ　2014.7.14　82p～83　２枚

インターネットのメールでは、半角英数しか使えない。

しかも多くのメールソフトがあり個々にソフトが異なっており、全角文字入力や画像や音声もフアィル添付も送ることが出来るのは、「エンコード」という変換信号処理をして送受信しているからです。

いわゆる入力したアナログ信号をコンピュータ処理に適したデジタルデータに変換しています。アナログ信号を６ビット６４通りのＡＣＣⅡコードに割り当てて、瞬時に変換して送受信されています。

この文書の生のメールのソースを見る事で、半角英数に変換されているのが判ります。
見る方法は
　メールの本文を開いて→プロパティ→詳細タブ　をクリックすると、表示された画面にヘッダー、ボディ等で半角英数のエンコードが表示されている。

◆３時間目　３０年度計画の説明　　１５：２５～１５：４０　１５分
２月度に提案された各テーマを月度別に割り当て配分して、記載した年間活動計画をプロジェクターに映して説明をして了解を得た。

◆４時間目　その他パソコン全般
１．メールのタイムアウトで通信エラーが発生
サーバーのタイムアウト時間の設定を長くする。
　メールを開いて「フアィル」タブを選択→「詳細設定」タブを押し、画面の中でタイムアウト時間を現状より長くする→ 適用 →ＯＫ で終了。

２．近頃話題の「仮想通貨」の解説　　資料日経ﾊﾟｿｺﾝ　2018.2.16　62p　１枚
「仮想通貨」とは「暗号通貨」とも呼ばれ、データ通信で不特定多数に支払いを出来るお金の性質を持っている。「円」や「ドル」等の公的通貨でなく、電子マネーの「Suica」とも異なる。
　国家や企業の後ろ盾がない独自の電子通貨で、最近では「ビックカメラ」等で支払いが出来る店舗が増えてきている。
　仮想通貨のビットコインでの支払いや受け取りには「ウオレット（財布）」というアプリを使う。専門の取引所に口座開設すると、円やドルの交換や売買が出来る。
　この「暗号通貨」である「仮想通貨」は、取引を記録する「ブロックチエーン」構造を採用しており、一旦記録された取引は後から無効化するのは困難で、不正送金されても取り戻せない場合がある。

―以上―