

LAB LETTER

株式会社 デザインラボ
代表取締役 藤原 康孝

第195回 WannaCrypt ランサムウェアについて

5月12日からの WannaCrypt、WannaCry、WannaCrypto などと呼ばれるランサムウェア/ウイルス大流行との TV ニュースや各種メディアで報じられています。感染するとパソコンやサーバーのファイルを暗号化してしまい業務に使えなくなり、暗号化を解除するには身代金を支払わなければならないとのことです。ちなみに身代金(=ransom/ランサム)を払ったところで解除できる確約もありませんので、払うべきではありません。

今回の「WannaCrypt」については下記対策が必要です。

1. アンチウイルスソフトウェアを最新版としてウイルス定義を更新する。
2. 当ウイルスは Windows OS の脆弱性を利用して感染しますので、マイクロソフト社が用意した下記の対策プログラムをインストールする。
[WannaCrypt] MS17-010 の適用状況の確認方法について (WSUS)
<https://blogs.technet.microsoft.com/jpwsus/2017/05/15/wannacrypt-ms17-010-wsus/>
3. Windows のファイル共有やプリンタ共有機能の為の通信手段である「SMBv1」を無効化すること。

万一感染した場合は、元に戻せません。感染する前にバックアップを取っておき復旧するしか方法がありません。

感染源は、①メールの添付ファイルをクリック、②メールに記載の URL や感染している WEB サイトのリンクなどをクリック、③サーバーや自身の PC の共有フォルダに勝手に感染、④「SMBv1」が有効化されている場合、勝手に感染、以上のいずれかになります。

取りあえずは過去のウイルス同様、怪しい添付ファイルを開かない、怪しいサイトにアクセスしない、クリックしないことは同じですが、上記の③と④の理由でそれだけでは感染を防ぐことができません。

ランサムウェア自体はここ数年様々なウイルスが出現し、その度対策されてきましたが、今回特に大きなニュースとなったのは、原因と経緯にあります。

- 1) アメリカの情報機関である国家安全保障局(NSA)が Windows の脆弱性(SMBv1)を見つけ、マイクロソフト社へ知らせることなく、この脆弱性を利用して逆に情報収集する為の官製の盗聴ソフトウェア「ETERNALBLUE(エターナルブルー)」を開発。
- 2) 盗聴ソフトウェア「ETERNALBLUE」がハッカーにより NSA から流出。数ヶ月の間「シャドー・ブローカーズ」にて販売されていたものが、4月14日にネットに公開された。

- 3) マイクロソフト社は NSA からの流出を知り、本年 3 月に対策プログラム(セキュリティーパッチ)の配布を開始。
- 4) しかし対策プログラムを当てなかったパソコンの感染が急増。特にインターネットに直接接続しているサーバーやルーターに感染した為、世界的な規模に広がった。ユーザー自身が何もしなくとも脆弱性に問題ある機器は知らない内に感染してしまいます。
- 5) 本年 5 月 13 日に既にサポートを終了している Windows XP, 8 パソコンと Windows Server 2003 サーバー用の対策プログラムを配布開始。

WannaCrypt は感染すると予め設定されたサーバーへアクセスし、そこから感染ツールをダウンロードすることから、感染が拡大し始めた当初、そのサーバーを特定し一時期拡大を止めることができました。しかしその後 WannaCrypt の改造版が出ておりこの方法も効果がなくなっています。

「シャドー・ブローカーズ」はいわゆるハッカー集団で、アメリカ人、ロシア人、アジア人が関与している、あるいはそもそも NSA 内部にいるとも言われていますが不明です。

そもそも正義の味方であるべきと思われる NSA が Windows の脆弱性を発見した際にどうしてマイクロソフト社へ連絡し対策を取らなかったのか、その時点で対策していればこのような問題にはならなかったはずと感じる方も多いと思います。NSA の本来の目的は諜報活動であり、アメリカ合衆国国民をスパイすることは違法であっても、他国をスパイすることが大きな目的の1つであり、その一つの手段として盗聴ソフトウェアを開発することになります。NSA の立場としては盗聴することでテロを未然に防ぐことができるということになります。

マイクロソフト社も以前から企業や政府が発見したソフトウェアの脆弱性を開発者へ報告を義務づけさせる「デジタル版ジュネーブ条約」の必要性を訴えてきているわけですが、NSA からすれば、そもそもマイクロソフト社が今回感染拡大の一要因となった Windows XP のサポートを止めていたことが原因とも言えますので、今のところすぐに条約締結される方向にはありません。

マイクロソフト社が次々に Windows OS の最新版をリリース販売し、旧バージョンのサポートを終わらせ、旧バージョンを利用しているユーザーへアップグレードするように強引とも思える方法を取っているのは、売上云々の問題だけではなく、根本的にはやはりセキュリティー向上が最優先であるためです。今回のようなケースでは、旧バージョンを利用しているパソコンとネットワーク機器が牙を剥いてくるとも言えますので、やはりセキュリティー対策の一環として OS のバージョンアップは必須です。

(御参考まで)

DLAB System Integrator **デザインラボのご案内**

【業務内容】

1. パソコン・周辺機器などハードウェア、ソフトウェア販売、ネットワーク構築・サポート
2. 会計・生産管理・販売管理システムの販売、開発、サポート
3. インターネットサーバー構築、Web サイト開発、運用管理
4. システムコンサルティング
(社内システム部門として PC などの運用管理、Q&A 対応、システム評価を行います。)

0-2439-2663~4
 0-2439-2665
 Email : info@dlab.co.th

株式会社 デザインラボ (Design LAB Co., Ltd.) 連絡先: 藤原 康孝 (Yasutaka Fujihara)

LAB LETTER

株式会社 デザインラボ
代表取締役 藤原 康孝

第196回 AI について

本年5月下旬に囲碁の試合で Google の子会社である Deep Mind 社が開発した「アルファ碁」と呼ばれる人工知能が、中国の最強棋士に3局全勝したことがニュースになりました。その後、日本でも(6月20日時点において)若干14歳の藤井聡太四段が27連勝し、AI、ディープラーニングの手法により開発された将棋ソフトウェアとの対戦で実力をつけてきたとの報道もありましたが、この1~2年の間にAIに関するニュースを見かけない日はないほどのブームになってきました。

AIは、Artificial Intelligence(人工知能)の略で1940年代から開発が始まりましたが、今回のブームは「ディープラーニング」と呼ばれるコンセプトを中心にしたものです。「ディープラーニング」を一言でいうと画像、音声といったデータを入力するとそのデータから何らかの特徴を見つけ、同一性、差異性などを数値化して認識することにあります。

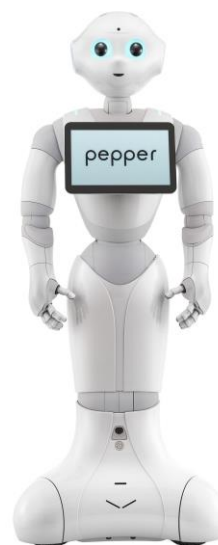
AIの目指すところとして、鉄腕アトムやドラえもんといった人間と同じ特徴を持ったロボットを作ることがある一つの目標と言えるかもしれませんが、鉄腕アトムやドラえもんの目であったり、耳となる機能が「ディープラーニング」と言えます。

「ディープラーニング」の目で碁盤を認識し、囲碁のルールに基づいて優勢劣勢の判断を行い、勝つための確立が最大となる次の一手を計算するロジックをプログラミングすることでAIによる囲碁ソフトウェアが開発されます。開発した後は過去の棋譜を数多く読み込ませることで優劣のパターンを認識する精度を高め、さらにはAI同士を対戦させることで人間の記憶力と判断力を超えたパターンを認識することが期待されます。つまりは最強の囲碁人間ロボットを作ることが可能になります。

しかしながら人間はもちろん囲碁だけを行っているわけではありませぬので、鉄腕アトムやドラえもんといった人間と同じ特徴を持ったロボットを作るには、さらに別次元のコンセプトが必要になると考えられます。

一般に市販されているAIロボットとしてソフトバンク社の「Pepper」ペッパーがあります。本体価格198,000円ですが、基本機能の会話、コミュニケーション機能に加え、追加料金で料理、英会話、クイズなどの機能を追加することができます。

一昔前にはSONYが販売していた犬型ロボット「AIBO」がありますがこれも同じような仕組みで動作していました。現時点ではあのシュワルツェネッガー主演の「ターミネーター」のようにロボットが人間を支配するようになるにはまだ越えなければならない壁がありそうです。



AIの世界では鉄腕アトムやドラえもんといった人間と同じ特徴を持ったロボット、つまり意思を持ったAIを「強い AI (Strong AI)」、強い AI の構成部品となる画像認識、音声認識といった機能を「弱い AI (Weak AI)」と呼んでいます。「ディープラーニング」も弱い AI になりますが、開発するにはプログラミングが必要になります。

現在ではマイクロソフト、Google などにより「ディープラーニング」を比較的容易に試すことができる API やライブラリと呼ばれるプログラムのセットが予め用意されており、プログラマーでなくとも、「ディープラーニング」を体験することができます。詳しくは下記ご参照ください。

「はじめての AI」

<http://www.itmedia.co.jp/news/series/5264/>

例えば、マイクロソフトの API を利用するには、マイクロソフトのクラウドサービス「Azure」に登録して、下記のような認識機能を利用することができます。

1. Computer Vision API
画像の分析、画像内のテキスト読み取り、著名人、有名な場所の抽出など。
2. Emotion API
画像から感情の読み取り、ビデオ画像から感情の読み取り。
3. Face API
似ている顔の検出、年齢、性別などの読み取り。
4. Translator Speech API
音声翻訳、書き起こしなど。

この他にも様々な API が用意されています。初期費用や認識件数が少なければ費用は掛かりません。当然のことながらクラウドサーバを利用しますのでハードウェアの費用も掛かりません。API をゼロから開発するには時間と費用が掛かりますが、まずはお試しください。

(御参考まで)



DLAB デザインラボのご案内
System Integrator

【業務内容】

1. パソコン・周辺機器などハードウェア、ソフトウェア販売、ネットワーク構築・サポート
2. 会計・生産管理・販売管理システムの販売、開発、サポート
3. インターネットサーバー構築、Web サイト開発、運用管理
4. システムコンサルティング
(社内システム部門として PC などの運用管理、Q&A 対応、システム評価を行います。)

0-2439-2663~4 0-2439-2665 Email : info@dlab.co.th

株式会社 デザインラボ (Design LAB Co., Ltd.) 連絡先: 藤原 康孝 (Yasutaka Fujihara)

LAB LETTER

株式会社 デザインラボ

代表取締役 藤原 康孝

第197回 オフィスの移転

IT 関連のサポート業の中でオフィスの移転時にインフラ構築を請け負うことがあります。今回はその中でも特に当地において非常に見落とししやすい項目と時間の掛かる項目について上げてみました。

様々な業者や入居先のビルとのやり取りが関わっていきますので、とにかく全体の進捗が遅れがちになります。最低でも2ヶ月前には着手する必要があります。大項目としては下記になります。

- ハードウェア関連
 - インターネット回線
 - 電話・FAX・セキュリティ回線
 - 社内 LAN
 - 既存の契約のキャンセルとその他
- ハードウェア関連
 - 移設前後で電源のオンオフを行い、正常に動作していることを確認。
 - 移送時に壊れることがないように十分な梱包が必要です。当地の場合、特に雨季になると IT 機器が雨に濡れて故障しますので要注意です。
 - サーバーラックや複合機など大きなハードウェアの移送は専門の業者に依頼した方が安心です。例えば Fuji Xerox の複合機は Fuji Xerox に依頼して手配していただくことが可能です。
 - オフィスビル間での移転では荷物専用のエレベーターしか使えないことが多いので予め移転元、移転先のビルに確認が必要です。工事と重なると予定通り進捗できません。
 - 高額な機器には移送時に損害保険を掛けておきましょう。
 - インターネット回線
 - 移転先で現在と同じインターネット環境が使えるとは限りません。バンコク市内の場合、回線業者は TOT、TRUE やその他ビル指定の回線業者がありますが、市内でも一部のエリアで光回線が使えないことがまだあります。回線の状況次第で逆に入居先のビルを選定するケースもあります。
 - 申請から開通まで 1 ヶ月近く掛かることがあります。インターネット回線がないと仕事になりませんので、先行して申込が必須です。
 - インターネットプロバイダーは、多くの場合、専用線は入居先のオフィスまで配線してくれることが多いようですが、ADSL、VDSL といった料金の安い回線は、ビルの MDF (配線盤) までしか配線してくれません。ビル階下から自社のオフィスまで自社でビルと連絡を取りながら配線する必要があります。
 - ビル内での配線は、ビルが業者を手配して代行してくれるケースと、自社で配線業者を手配しなければならないケースがあります。
 - いずれの場合でも、ビルに管理費として数千パーツ～数万パーツ以上のかかり想定外な費用を請求されます。デポジットなどの名目で請求されることがありますが、一般的には退去時にもこの費用は返却されません。予め移転費用に入れておく必要があります。

3. 電話・FAX・セキュリティ回線

- 1) これもインターネット回線と同様で、電話会社はビル階下の MDF までの配線となりビル内は自社で配線することが必要になります。
- 2) あるいはビルによっては予めビルが所有している電話回線を割り当てられ、入居者側で電話会社と直接契約できないことがあります。
- 3) 代表電話番号を取る場合は、一般的には電話会社へ設定を依頼します。名刺や会社案内に新しい電話番号と住所を入れて作成する必要がありますので、これも 2 ヶ月ほど前から電話会社へ申請し、一ヶ月前には電話番号、FAX 番号を決めておく必要があります。決まらなければ印刷物の手配が掛けられません。
- 4) セコム社などのセキュリティ回線は、FAX 回線を共有することがあります。FAX 回線とセコム社のセキュリティ設備への分岐の方法について予め確認が必要です。

4. 社内 LAN

- 1) 内装会社、工事会社に LAN ケーブル、電話線の種類と設置場所を指定します。LAN ケーブルは、AMP 社、LINK 社など特定のメーカー品を指定した方が長期的に安定します。
- 2) 電源コンセントも当地の場合、非常に抜けやすい、壊れやすいなどの問題が多発します。多少高価でもパナソニックなど日系製品がやはりお勧めです。移転後に毎日の使い勝手が大きく変わります。
- 3) 無線 LAN は鉄扉などを経ると非常に繋がりにくくなります。移転先の部屋割りを確認の上、配置がお勧めです。
- 4) LAN ケーブル長は余裕を見て長めに用意しておくこと、ケーブルの両端にはケーブル番号をつけること。

5. 既存の契約のキャンセルとその他

- 1) 移転元で利用しているインターネット回線や電話回線のキャンセル手続きをお忘れなく。ローカルスタッフに寄れば、キャンセルせず請求書が来て支払わなければ、自然とキャンセルされると言われることもありますが、電話局側ではキャンセル用の申請書を用意しています。利用しないサービス料を支払うことのないように予め届け出をすることが必要です。
- 2) 電源コンセントが不足することが多々あります。OA タップの必要数を予め計算しておきましょう。

基本的に内装会社、工事会社、IT 業者などは自社の請負業務の範囲内でしか移転作業を請け負いません。その狭間にある様々な移転項目に抜けがないように総務担当者中心に移転をプロジェクトとして管理する必要があります。

(御参考まで)

DLAB デザインラボのご案内
System Integrator

【業務内容】

1. パソコン・周辺機器などハードウェア、ソフトウェア販売、ネットワーク構築・サポート
2. 会計・生産管理・販売管理システムの販売、開発、サポート
3. インターネットサーバー構築、Web サイト開発、運用管理
4. システムコンサルティング
(社内システム部門として PC などの運用管理、Q&A 対応、システム評価を行います。)

0-2439-2663~4 0-2439-2665 Email : info@dlab.co.th

株式会社 デザインラボ (Design LAB Co., Ltd.) 連絡先: 藤原 康孝 (Yasutaka Fujihara)

LAB LETTER

株式会社 デザインラボ
代表取締役 藤原 康孝

第198回 サイバーリスクの対策

ニュースなどで顧客情報の流出などについて頻繁に記事が載るようになってきました。特に顧客のクレジットカード情報が流出し、第三者に使われてしまうと多額の被害が発生することがあります。

当地で多い日系製造業や商社ではいわゆる B2C として一般消費者の顧客情報を扱っているケースは少ないと考えられますが、逆に当地で考えられるサイバーリスクとしては下記のようなものがあります。

1. 顧客図面の流出
2. 得意先への売上単価、取引先からの仕入単価情報の流出
3. ウイルスメールを得意先、取引先へ送り受信者の感染による被害
4. ウイルス感染などによる社内データの消失
5. 自然災害(特に洪水、火災)による社内データの喪失

このようなリスクに対して、まず日常的にバックアップを取っておくことが基本ではありますが、日本などでは「サイバー保険」を利用されている企業があります。当地でも 2017 年 1 月に「三井住友海上火災保険、タイにサイバー保険投入」という記事が出ていました。

一般的なサーバー保険は、賠償、事故対応、利益損害、営業継続費用について対応されます。

1. 賠償、事故対応
賠償責任を負担する場合、予め決められた限度額内で保険金が支払われます。付帯的な費用としての、原因調査費用、訴訟費用、謝罪広告費用などに対応されるかどうかは予め確認が必要です。
2. 利益損害(オプション)
例えばウイルスに感染し、運営する WEB サイトから受注を受けられなくなった、工場のシステムが止まり生産ラインが停止するようなケースでは、予め決められた限度額内で保険金が支払われます。
3. 営業継続費用(オプション)
例えば、ネットワーク機器が停止することで営業活動ができなくなった場合、予め決められた限度額内で保険金が支払われます。

保険料の一例として、例えば製造業向けには、年間売上高が 10 億円以下の場合、保険金額を 1 億円と設定した場合、年間の保険料は 25 万円ほどになります。

ただし、下記のケースでは保険金は支払われません。

1. 被保険者に重大な過失がある場合
2. 被保険者が法令に違反した行為を行った場合
3. 被保険者が意図的に損害が発生する行為を行った場合

4. 被保険者が対象となる機器、設備を第三者に貸与していたケース
5. 災害と労働争議が原因である場合
6. サーバーが海外にあるケースなど。

日本の場合、保険会社では「ISMS 認証取得企業」の場合、保険料を割引することがあります。ISMS(情報セキュリティマネジメントシステム /Information Security Management System)とは、ISO 27001に規定されているマネジメントシステム規格のひとつです。

ISMS の概要は、「リスク」、「資産価値」、「脅威」、「脆弱性」を定義づけ、

リスクレベル＝資産価値×脅威×脆弱性

以上の方法で数値化された「資産価値」、「脅威」、「脆弱性」によってリスクレベルを算出します。後は ISO と同じで分析と評価を行い改善に繋がります。ISO 導入企業では比較的取り組みやすい点はあるかと思われますが、「情報セキュリティ」のノウハウが必要になります。

「情報セキュリティ」の主な 3 要素は、下記の通りです。

1. 機密性：許可されていない個人、組織に情報にアクセスさせない、開示しない特性。
2. 完全性：正確性、完全性の特性
3. 可用性：許可された個人、組織に情報にアクセス及び使用可能である特性。

実際のところ保険会社では、JQA 社、BSI-J 社等といった特定の ISO 認証機関から ISMS 認定を受けた企業へ保険料の割引を行っていますのでコンサルティングを受ける場合は、予め確認が必要です。

サイバーリスク対策については、今後 AI も含め IT システム化が進むにつれ必須事項になると思われます。概要だけでもご確認がお勧めです。

(御参考まで)

既に運用されているサイバー保険として、当地のローカル保険会社では AIG 社がサイバー保険を取り扱っています。 <http://www.aig.co.th/en/business/products/financial-insurance/cyber>

サイバーリスクについて詳しく調べたい方は、独立行政法人 情報処理推進機構 (IPA) 作成の下記の資料が参考になります。 <https://www.ipa.go.jp/files/000045629.pdf>



DLAB デザインラボのご案内
System Integrator

【業務内容】

1. パソコン・周辺機器などハードウェア、ソフトウェア販売、ネットワーク構築・サポート
2. 会計・生産管理・販売管理システムの販売、開発、サポート
3. インターネットサーバー構築、Web サイト開発、運用管理
4. システムコンサルティング
(社内システム部門として PC などの運用管理、Q&A 対応、システム評価を行います。)

0-2439-2663~4 0-2439-2665 Email : info@dlab.co.th

株式会社 デザインラボ (Design LAB Co., Ltd.) 連絡先: 藤原 康孝 (Yasutaka Fujihara)