Deloitte.

「2017年に最も注目を集めた情報セキュリティインシデント」と聞いて、皆さんはどのような事例を想像されるでしょうか。恐らく、「ランサムウェア」という単語を想像される方は少なからずいらっしゃるのではないかと思います。「身代金ウィルス」と言ったほうがピンとくる方が多いかもしれません。「ランサムウェア」とは、コンピュータウィルスの一種であり、感染したパソコン、あるいはパソコンに保存されたデータを使用不能にすることで、これを「人質」として「身代金」を要求する、といった挙動をするものです。

2017年5月には、欧米およびロシアに於いて、「WannaCry」と呼ばれるランサムウェアによる大規模なサイバー攻撃が発生したと報じられました。特に英国では、国民保健サービス（ＮＨＳ）がその被害を受けて、一部の医療機関に於いて診察や手術を行えない状況に陥ったと伝えられています。また、被害は日本とオーストラリアを含む世界中に広まっており、その影響力を改めて痛感させられる事態となっております。

ランサムウェアの被害を防ぐために必須の対策

◆こまめなバックアップ：
一度、ランサムウェアによって暗号化されたファイルを元に戻すことはかなり困難です。クラウドや外付けハードディスクなどの複数の場所に重要なファイルのコピーを常に予備として保管しておきましょう。

◆ファイルの開封やリンクへのアクセス：
今回のランサムウェアの感染には細工したメールの添付ファイルを開封させる等の方法が用いられていると報道されています。また、不審なメールを確認した場合はシステム管理者等に問題ないか確認してください。

◆ＯＳやソフトの脆弱性：
パソコンのＯＳやソフトの脆弱性を残していると、脆弱性攻撃を受けてランサムウェアに感染してしまう可能性があります。Windows Updateなどのソフトウェアの自動更新を有効にするなど、ＯＳやソフトの開発元から更新プログラムが提供されたら速やかに適用し、脆弱性を修正してください。

もしもランサムウェアに感染したときには？

◆金銭の支払い：
ランサムウェアに感染して金銭を要求されても決して言いなりになってはいけません。支払ったところで犯罪者が暗号化したファイルを確実に元に戻してくれる保証はない上、ランサムウェアの拡散にうまみを感じたサイバー犯罪者の攻撃を助長してしまうことにもなります。

◆感染端末：
ネットワークでほかの端末とファイル共有などをしている場合には、他の端末が感染したり暗号化されるデータが増えてしまったりするリスクがあります。気付いたタイミングによっては被害を抑えることもできるので、有線であればＬＡＮケーブルを外す、無線の場合はWi-Fiをオフにし、感染した端末をネットワークから外しましょう。

◆サポート窓口：
上記の対処策と並行して、ランサムウェアの感染が疑われる場合には、まずはご利用のセキュリティソフトを提供する企業のサポート窓口に問い合わせることをおすすめします。

PROFILE
Wenda Gumulya
(wgumulya@deloitte.com.au)
2009年四大会計事務所日本法人に入所。日本での上場企業ＩＴ全般統制監査や金融企業技術アドバイザリー業務に従事。2011年には同会計事務所メルボルン事務所に場所を移し、豪州上場金融企業に対する同種業務やセキュリティーアドバイザリー・サービスを提供。2015年豪州Deloitteシドニーに入所。豪州上場企業ＩＴ全般統制監査やオペレーション監査、技術アドバイザリー業務に従事。公認情報システム監査人。