A1データ株式会社
〒358-0055 埼玉県入間市新光 182 番地
TEL(04)2932-6365

2017年7月3日

ランサムウェア「WannaCry」に感染した PC からのデータ復旧サービスを開始

データ復旧のトップ企業であるA1データ株式会社（本社：埼玉県入間市　取締役社長　本田　正）オントラック事業部（事業部長：　溝呂木　清）は、ランサムウェア「WannaCry」に感染したPCからのデータ復旧サービスを2017年7月3日より開始しました。

ランサムウェアに感染し、データにアクセスできない事態に陥っていませんか？当社のエンジニアリング・エキスパートができるだけ早くデータを復旧し、ユーザーの不安を解消します。

【ランサムウェアの概要】

マルウェアの一種で、これに感染するとコンピュータがロックされたり、ファイルを暗号化したりすることによって利用者のシステムやデータへのアクセスが制限されます。この制限を解除する引き換えとして、マルウェアの作者に身代金（ransom、ランサム）を支払うよう要求する不正なプログラムのことを指します。

【ランサムウェアのタイプ】

ランサムウェアには主に 3 つのタイプがあります。

1. スケアウェア：
   ランサムウェアの中でも最も単純な形式。偽のアプリケーションやプログラムで構成され、これらは主にウイルス対策ソフトウェア等になりすましてインストールさせ、偽の警告で金銭の請求を行ったり、個人情報を盗み出したりします。
2. ロックスクリーンウイルス：
   2 番目に危険なランサムウェアタイプ。感染すると、ウイルスはユーザーのコンピュータをロックし、フルサイズのウィンドウを表示し、この PC にサイバー犯罪が起こったというメッセージを表示します。ユーザーは、コンピュータのロックを解除するために身代金を支払う必要があります。
3. 新しい暗号化ランサムウェア：
   最も危険なランサムウェアタイプ。被害者のコンピュータにアクセスした後、攻撃者はコンピュータのデータとファイル構造に侵入し、コンピュータ上のすべてのファイルとフォルダを暗号化します。

【WannaCryの特徴】

WannaCry（ワナクライ）は、ネットワークの脆弱性を突いてファイルをダウンロードし、SMB サービスとして実行され、感染します。SMB サービスはファイル共有するために使われるので、法人組織の場合、ネットワーク上で感染が拡大し、被害が甚大となる恐れがあります。

感染されるとファイルが拡張子「WNCRY」として暗号化されます。暗号化されるファイルは様々で、Microsoft Office やデータベース関連、圧縮ファイル関連、マルチメディア関連、さまざまなプログラミング言語関連のファイル等も含まれます。

そして暗号化を解除するための身代金を要求します。時間が経つごとに金額は上がり、最後はファイルを消去するという警告が表示されることもあります。

【WannaCryに感染してしまった場合の対処法】

1. まずは落ち着きましょう。性急な判断はデータの紛失を招く可能性があります。
2. PC のシャットダウンは行わないでください。
   WannaCry は PC のメモリー上に展開された素数を使用して復号用のキーを生成します。しかしながら、PC のシャットダウンや再起動を行うと、メモリー上にある素数がクリアされ、複合キーも消滅してしまいます。
3. 感染の拡大を防ぐため、LAN ケーブルを抜き、WiFi（無線 LAN）のスウィッチを OFF（無効）にし、PC をネットワークから切り離してください。
4. 最新のバックアップを確認してください。
5. アドバイスや復旧のオプションについては、オントラックへお問い合わせください。

【ランサムウェアの暗号化方法】

ランサムウェアがデータへのアクセスを制限する方法は、主に暗号化をすることですが、ランサムウェアによって暗号化方法は異なります。

1. 原本のファイルを暗号化する
2. 原本のファイルを暗号化してからその原本のファイルを削除し、別のファイルで上書きを行う
3. ファイルを複製してその複製ファイルを暗号化し、原本のファイルを削除する

ランサムウェアからデータ復旧するには、これらの中からどのように暗号化されたかを判別し、正しい手順と方法によってデータを復旧する技術が必要となります。

【ランサムウェアからの復旧実績】

オントラックグループでは現在確認されているランサムウェア220種のうち、感染した98種に対応しています。

主な実績として、Nemocod, Cryptolocker, Apocalypse, DMALocker, Globe 等があります。

解読ツールと非暗号化ファイルを検索と復旧する世界トップのデータリカバリーツールの両方を揃えることにより、成功率８０％を誇る復旧実績があります。

オントラックは WannaCry に感染した PC でもデータを復旧します。

WannaCry 及びその他のランサムウェアに感染した場合、まずはオントラックへご相談ください。

【媒体種別】

ランサムウェアにより失われたデータは、どのメディアでも復旧します。

ハードディスクドライブ、ノートパソコン、デスクトップ PC、モバイル、サーバー、SAN、NAS、仮想等

【その他のランサムウェア対応】

ランサムウェアは WannaCry だけではありません。また、パッチで穴をふさいでもすぐに亜種が発生し、世界にはたくさんのランサムウェアが蔓延しています。

全世界で500，000件以上と世界 No.1 のデータ復旧実績があるオントラックグループでは、随時ランサムウェアの調査を継続し、日夜全世界でランサムウェアからのデータ復旧技術も研究しています。

素直に身代金を支払えば必ず暗号は解除されるでしょうか。ランサムウェアをばらまく者が約束を守り、ファイルを戻してくれるとは限りません。感染させたランサムウェアの開発者を信じるか、世界 No.1 のデータ復旧実績があるオントラックを信じるか。信頼性は一目瞭然です。

WannaCry 及びその他のランサムウェアに感染した場合、まずはオントラックへご相談ください。

◆ A1データ株式会社 オントラック事業部について

1994 年に世界 No.1 のデータ復旧実績を持つ Kroll Ontrack 社と技術提携し、日本で初めてデータ復旧サービスを開始いたしました。以来 23 年間、50,000 件以上にわたってサービスを提供し、2007 年に国内大手のデータ復旧企業初の公的セキュリティー認証 ISO27001（ISMS）を取得し、万全のセキュリティ対策と徹底した機密保持体制を構築し、信頼感ある日本のトップサプライヤーとして実績を積み重ねています。当事業部は、データ復旧ソフト Ontrack EasyRecovery、インターネットを利用して素早くデータ復旧を行うリモートデータ復旧、当社でお預かりしてデータを復旧するラボラトリデータ復旧など、豊富なサービスと、多種多様の記憶メディア／OS に対応できる、高品質で迅速な業界随一のサービスを提供しております。

以上

【お問い合わせ先】

株式会社 A1データ株式会社 オントラック事業部
電話： (04)2931-2340（ダイヤルイン） FAX： (04)2932-6370
E-Mail： sales@ontrack-japan.com URL： https://www.ontrack-japan.com