世界同時多発ランサムウェア攻撃（5 月 13 日）と企業の対応

日本時間 2017 年 5 月 13 日から、世界各国で同一種類のランサムウェア「WannaCry」感染による被害が相次いでいる。ランサムウェアとは、電子データ等を暗号化し、暗号化の解除と引き換えに「身代金」を要求する不正プログラムである。推定される被害規模は調査機関・時期によって幅があるものの、150 カ国以上で 30 万件以上との見方もある。医療、通信、鉄道・物流等の公共性が高い（攻撃者に「身代金」支払の要求に応じると思われている）セクターを中心に WannaCry の被害が報告されている。他方、WannaCry は保守サポート対象の Windows OS では既にセキュリティの更新プログラムが公開されたものであり、ソフトウェア等の情報インフラに対する適切な投資とセキュリティ上の運用を徹底していれば被害を極小化できた可能性が高い。

本稿では、5 月 13 日の世界同時多発ランサムウェア攻撃の概要と対策について紹介する。

1. 世界同時多発ランサムウェア攻撃（5 月 13 日）の概要

（1）ランサムウェア「WannaCry」の概要

ランサムウェア（ransomware）とは、「身代金（ransom）」を要求するマルウェア（malware／不正プログラム）の総称である。ランサムウェアは、感染したパソコン、サーバー、スマートフォン等の端末をロックしたり、それらの端末に保存されているファイルを暗号化[1]したりすることで使用不能にした上で 、元に戻すことと引き換えに仮想通貨「ビットコイン（Bitcoin）」等で「身代金」を要求する。

■図 1： WannaCry に感染した場合に表示されるメッセージの例

出典：IPA ウェブサイトより抜粋

[1] WannaCry では 166 種類のファイル拡張子が対象となっており、感染すると拡張子「WNCRY」として暗号化される。

5 月 13 日に世界で同時多発被害を引き起こしたランサムウェアは、「WannaCry」との呼び名が付けられている[2]。今回のランサムウェア WannaCry では、300 ドル相当（場合によっては 600 ドル相当）のビットコインが要求されていることが多い。

WannaCry によるサイバー攻撃の原因は、Windows の脆弱性「CVE-2017-0144」[3]であり、これは「Shadow Brokers」と呼ばれるハッカー集団が 2017 年 4 月に米国の国家安全保障局（National Security Agency: NSA）から窃取したハッキングツールに含まれていたとみられる。

この脆弱性は Windows10 には存在せず、保守サポート対象の Windows OS では上記の更新プログラムが公開されていた。しかし、保守サポート切れの Windows OS が現在もアプリケーションソフトウェアの制約等から多く使用されていたため、サポート対象外の Windows OS を使用する企業・組織を中心に WannaCry の被害が広がっている。マイクロソフトでは今回の感染事案を受け、Windows XP、Windows 8、Windows Server 2003 といったサポート切れ OS を対象とした緊急の更新プログラムを公開した。つまり、保守サポート対象の OS を用いて、セキュリティプログラムを最新化していれば、WannaCry による被害はなかった、あるいは極小化された可能性が高い。

WannaCry の被害は週明け 15 日以降、日本や東アジア各国での被害拡大が確認されている（欧米では 12 日（金）午後以降に被害が発生した）。WannaCry による被害規模は、調査機関によって調査範囲・時期が異なり、ばらつきがあるが、15 日の米ホワイトハウスの国土安全保障・テロ対策担当の大統領補佐官ボサート（Thomas Bossert,）氏は、WannaCry の被害は 150 ヶ国で 30 万件以上と発表している[4]。

（2）世界と日本におけるランサムウェア「WannaCry」の被害事例

WannaCry による世界同時攻撃は計画的なものであった。攻撃は日本時間の 5 月 13 日、被害の中心となった欧州では 5 月 12 日（金）の午後から夕方に発生した。週末直前に攻撃を仕掛けたのは、「（「身代金」を支払ってでも）当日中にランサムウェア被害を何とかしたい」という被害者心理を狙った可能性がある。

ランサムウェア攻撃が日本時間で 5 月 13 日（土）未明であったことから、多くの企業・組織は休業中であり、15 日（月）の勤務開始以降の感染・被害の発覚が懸念されていた。こうした状況をふまえて、独立行政法人 情報処理推進機構（IPA）は 14 日 に記者会見を開き、WannaCry に対して週明けの就業前に対応をとるように注意喚起を行った[5]。

WannaCry の被害は世界各地で確認されている。WannaCry の「身代金」要求画面の多言語対応が進み、28 カ国語で表示されていることが世界的な被害拡大につながったと考えられる。西欧では医療、通信、鉄道・物流、金融機関等の社会インフラ企業が攻撃対象となっている。これらの公共性の

---

[2] WannaCry は「泣きたくなる」を意味する。なお、マイクロソフトおよび情報セキュリティ大手等の呼称は Win32/WannaCrypt（マイクロソフト）、RANSOM_WANA.A および RANSOM_WCRY.I（トレンドマイクロ）、Ransom.Wannacry（シマンテック）、WanaCrypt0r 2.0 (aka WCry)（アバスト）、WannaCryptor（IPA）等、さまざまである。

[3] コードネーム「Eternal Blue（エターナルブルー）」。

[4] Thomas Bossert, Assistant to the President for Homeland Security and Counterterrorism, Press Daily Briefing by Press Secretary Sean Spicer #48: (May 15, 2017)
https://www.whitehouse.gov/the-press-office/2017/05/15/press-daily-briefing-press-secretary-sean-spicer-48

[5] 独立行政法人 情報処理推進機構（Information-technology Promotion Agency: IPA）「世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について」（2017 年 5 月 15 日）。

高いセクターは、「身代金」支払いが社会的に許容されうる側面があるため、「身代金」を支払う可能性が高いとみられている。英国国民保健サービス（National Health Service: NHS）に代表されるように、医療セクターは今回の事案だけでなく、ランサムウェア攻撃の中長期的な主要ターゲットとなっている[6]。

欧州各国では、ランサムウェア感染とともに、実際の事業への影響が発生している（表 1）。例えば、英国 NHS への攻撃により、英国内の複数の医療機関で診療が行えなくなり、予定の手術が中止となり、救急車の行先変更が必要となった。また、スロベニアの自動車工場では生産ラインが停止し、ロシアの通信会社ではコールセンター業務に支障が生じ、中国のガソリンスタンドでは電子決済が利用不能となった。

日本国内でも複数のランサムウェア感染および被害が確認されている（表 2）。一般社団法人 JPCERT コーディネーションセンターの調査・分析によれば、国内では IP ベースで約 600 カ所、約 2,000 端末の感染が判明したとしている（5 月 13 日午前 0 時から約 12 時間分の分析）。事業に影響が及んだ被害事例はほとんど報道されていないが、大手電機メーカーではメールの送受信に障害が発生し、同グループ会社では受発注システムに障害が生じている。

[6] こうした状況は、米国の 15 のインテリジェンス機関を束ねる国家情報長官による年次議会報告「世界規模での脅威評価」にも反映されている。2017 年 5 月のコーツ（Daniel R. Coats）国家情報長官の報告によれば、グローバルな脅威の筆頭はサイバーリスクであり、サイバー攻撃の主体として 4 つの国家、テロリスト、犯罪組織を列挙している。コーツ国家情報長官によれば、「犯罪組織は情報の摂取、金銭要求、その他犯罪行為の促進等、さまざまな目的にサイバーツールを発展・利用している。ユーザーがデータにアクセスできないように暗号化するマルウェア、すなわち「ランサムウェア」は金銭要求の特筆すべきツールとなっている。2016 年、犯罪集団は医療セクターに焦点を当ててランサムウェアで攻撃し、患者のケアを妨害し、医療制度の公的信頼を貶めている（下線強調は引用者）」。Daniel R. Coats, Director of National Intelligence, “statement for the Record: Worldwide Threat Assessment of the US Intelligence Community,” Senate Select Committee on Intelligence (May 11, 2017), p.2.

■表１：ランサムウェアによる攻撃または被害が発生したと報道された事案（世界）

国	セクター	概要（報道内容）
イギリス	医療	NHS248 団体中、48 団体で端末が使用不能となったため、複数の医療機関で診療が行えなくなり、予定の手術が中止となり、救急車の行先変更が必要となった。NHS 内の約 9 割のコンピュータで Windows XP が使用されていたことが原因の1つと見られている。
イギリス	自動車	日系自動車工場で生産ラインが一時停止する影響が発生したが、広報担当者によれば事業への影響はない。
スロベニア	自動車	フランスの自動車メーカーの子会社本社のコンピュータが被害に遭い、12 日夜に生産ラインが稼働停止した（13 日時点でも停止）。
ドイツ	鉄道	フランクフルト等、複数の駅で列車の発着時刻表示の電光掲示板に障害が発生したが、列車運行には直接的な影響は生じていない。
スペイン	通信	大手通信会社のワークステーションの約 85%に被害が発生し、拡声器を使って従業員に使用の即時停止を呼びかけた。
ポルトガル	通信	大手通信会社が攻撃を受けたが、事業に影響はないとしている。
ロシア	行政	内務省の Windows OS 搭載のコンピュータ約 1,000 台が攻撃を受けたが、同省で使用される全体の約1%に満たない。これ以外にも非常事態省、保健省等、一部官庁でも攻撃が確認された。
ロシア	通信	大手通信会社が攻撃により、コールセンター業務に支障が生じた。
アメリカ	運輸	Windows をベースとしたシステムの一部でランサムウェアによる障害が発生した。
中国	エネルギー	天然ガスの生産・販売会社の直営ガソリンスタンドで電子決済が利用不能となる障害が発生した。
中国	大学	北京大学、上海交通大学、山東大学、南昌大学、大連海事大学、桂林航天工業学院等で攻撃が確認される。

※　上記のほか、スペインのガス会社・銀行、ロシアの銀行・鉄道会社、インド、インドネシア、ベトナム等でも行政機関や病院等で感染が確認された、あるいは被害が発生したと報じられている。

■表２：ランサムウェアによる攻撃または被害が発生したと報道された事案（日本）

セクター	概要（報道内容）
病院	警察による被害聞き取り調査で発覚したものの、業務への影響は生じていない。
鉄道	群馬県内の事業所でパソコン1台が感染したが、社内ネットワークに接続しておらず、運行システムや利用者へのサービスへの影響はない。
鉄道	東京都本社内のパソコン1台が感染していたが、社内ネットワークに接続しておらず、運行システム等に影響はない。
電機	感染により社内システムに障害が発生しており、メールの送受信が停滞したほか、メールの添付ファイルが開けない等の被害が出ている。また、子会社の1社でも同様の障害が発生している。同社はサイバー攻撃の被害が大きかった英国で鉄道事業を手がけているため、被害の有無等の確認を急いでいる。さらに、調査を進めた結果、家電量販店等との受発注で使用するシステムにも障害が見つかり、被害が拡大している。
自治体	上下水道局のパソコン1台が感染したが、内部のネットワークに接続しておらず、被害は広がっていない。同局は国際事業も担当し、海外も含めて大容量データの送受信を行うため、庁内ネットワークから独立した専用パソコンを使用していた。
自治体	県内の消防指令センターの出動現場から動画をリアルタイム伝送する専用タブレット端末 1 台が感染したが、感染拡大はなく、データ流出等の被害はない。

出典：表１・表２とも各種報道をもとに弊社作成

2. ランサムウェア攻撃への対策と対応

以下に WannaCry 事案から示唆されるランサムウェア攻撃への対策と対応を紹介する。

（1）ランサムウェア攻撃への予防策

平時からの予防策として、①ランサムウェアの侵入・感染を防ぐこと、②ランサムウェアに感染し、ファイルが暗号化されても復旧できるよう、ファイルのバックアップをとっておくこと、③暗号化等による実害が生じても適切な危機管理・事業継続を行うこと が挙げられる。

自社システムの開発・運営を IT 企業に委託している中堅・中小企業では、対策ソフトの適用やバックアップの設定等のランサムウェア攻撃対策が不十分となっていることも多く、また、自社システムのネットワークの構成がシンプルなため、対策未実施で感染した場合、被害が重要なファイルまで及ぶ可能性が高くなる。業種や規模を問わず、あらゆる企業がランサムウェア攻撃のリスクに晒されている中、特に中堅・中小企業においては、委託先の IT 企業・セキュリティベンダーと自社システムの契約内容を確認した上で、早急に対策を講じることが望ましい。

a. ランサムウェアの感染防止策

ランサムウェアに限らないが、一般的なマルウェア予防策の例は表 3 のとおりである。

WannaCry 事案では、（保守サポート対象の）Windows OS を用いて、OS およびウイルス対策ソフトを最新にアップデートしていれば、被害は極小化できた可能性が高い。企業・組織にとって、ソフトウェア等の情報インフラとセキュリティに対する一定の投資（予算、運用を支える要員手配）は不可欠である。

ランサムウェア被害が生じた企業では、業務で使用するアプリケーションやシステムの関係で、OS の切り替えやセキュリティ更新が徹底されていない、必要な予算がないとの理由から保守サポート外の OS を使っていたという事情が推察される。自社業務や予算の関係で、適切な最新化ができない企業であっても、経営者や（ICT やセキュリティ部門のみならず）経営管理部門は少なくとも、自社の端末 OS やブラウザのバージョンやそれらの脆弱性を把握しておく必要がある。

■表３：ランサムウェア等のマルウェア感染予防策の例

対策	概要
ソフトウェア等の最新化の徹底	端末の OS、ウェブブラウザや、ウェブで多用する Flash、Java、PDF 等のソフトウェアの最新化を徹底する。ランサムウェアに限らず、マルウェア対策に共通するものである。
ふるまい検知機能をもつアンチウイルスソフトの適用	不審なファイルの添付されたメールの受信をブロックし、マルウェア感染を防ぐ。
URL フィルタリングソフトの導入	リスクの高いウェブサイトの閲覧をブロックし、マルウェアのダウンロードを防ぐ。
管理者権限の実行者の限定	重要ファイルが保存されているサーバー等にアクセスできる者を限定することで、当該ファイルの暗号化リスクを低減する。
従業員へのセキュリティ教育・訓練の徹底	不審メールに添付されたファイルの開封や、危険サイトへのアクセスしないように周知・徹底する。

出典：弊社作成

b. データのバックアップ

ランサムウェアに感染し、必要なデータが暗号化されたとしても、バックアップを保存しておくことでデータは復元できる。バックアップの頻度や期間は企業の業態や対象情報量等をふまえて検討する必要があるものの、必要な措置の例は表 4 のとおりである。

■表４：データのバックアップ措置の例

分類	概要
安全な領域でのデータのバックアップ保存	重要なファイルをネットワーク外（別ネットワーク、外部媒体、クラウド上）またはサーバー内の非共有領域に保存する。
Windows Server OS のシャドウコピー設定	Windows Server OS の「シャドウコピー機能」を活用して、共有フォルダのコピー生成を行う。
端末の Windows OS の復元ポイント設定	Windows OS では、復元ポイントを有効としておくことでファイルの復元が可能となる[7]。

出典：弊社作成

c. コンティンジェンシープラン・事業継続計画の策定

ランサムウェアに感染し、必要なデータにアクセスできなくなったとしても、停止することができない業務は継続する必要がある。WannaCry 事案でも、一部企業ではオフラインで重要事業を継続した。コンティンジェンシープランは、自社のネットワーク構成・システム構成と事業特性をふまえて、複数のリスクシナリオを想定して作成することが望ましい。

ランサムウェア感染時や情報漏えい時のインシデントハンドリングを定めている企業・組織は少なくないが、事業部門におけるオフラインでの事業継続計画は未着手であることが多い。企業・組織はデータやシステム等の情報インフラのみが利用不能な場合の対応計画を策定することが必要である。

（２）ランサムウェア感染時の対応策

a. 被害拡大防止

ランサムウェア感染時、最も重要なことは被害の拡大を防止することである。ランサムウェアに感染した場合、直ちに全てのデータが暗号化されるわけではない。暗号化には一定の時間を要する。ランサムウェア感染を確認した場合、社内の ICT・セキュリティ部門や委託先と連携しながら、感染した端末・サーバーとその他データをネットワーク上あるいは物理的に分離することが重要である。

b.「身代金」支払要求に対する対応：原則、「身代金」支払要求には応じない

ランサムウェアに感染し、重要なファイルが暗号化された場合、身代金要求に応じるかどうかは極めて慎重な判断を要するが、原則として金銭の支払いに応じないことが推奨される。その理由は、

① 金銭支払いに応じても、暗号化が解除される保証はない

② 金銭支払いに応じた企業・組織の「リスト」に掲載され、今後も攻撃者のターゲットにさ

[7] Windows7、Windows10 の場合、「システムの復元」機能で作成された複数の復元ポイントから任意のファイルを復元することができる「以前のバージョン機能」がデフォルトで有効となっているが、それ以外の OS では予め手動で設定を有効にしておくことが推奨される。

れるおそれがある

③　反社会的勢力に金銭を支払い、攻撃者の資金源となることで、社会的批判を免れない

これまで、③については人命にかかわる事業者や公益性が高い事業者は社会的批判に晒されず、むしろ身代金支払いに応じるべきであるとされることも少なくなかった[8]。しかし、WannaCry でランサムウェアの脅威がかつてないほど注目を浴びる中、ランサムウェア対策投資を怠った結果、将来、感染・被害に遭い、「身代金」支払いに応じたとなれば、社会的批判は免れないだろう。

c. データの復号・復旧

ランサムウェアの種類によっては、暗号化されたデータを復号するツールが開発されている。一般財団法人 日本サイバー犯罪対策センター（Japan Cybercrime Control Center: JC3）では、ランサムウェアに対応する復号ツールとして、①トレンドマイクロ株式会社、②欧州刑事警察機構のサイバー犯罪対策機関である EC3（European Cybercrime Centre）のファイルの復号ツールを公開している。暗号化されたデータの復号プロセスの詳細は、JC3「ランサムウェア対策について」（2017 年 2 月 23 日）【 https://www.jc3.or.jp/info/nmransom.html 】を参照すると良い。

以上（本稿は 2017 年 5 月 16 日時点の情報にもとづくものである）

（2017 年 5 月 18 日発行）

[8] 「身代金」支払に応じた例は以下のとおりである（①は DDoS 攻撃、②③④はランサムウェア攻撃による「身代金」支払要求）。①2015 年 11 月、スイスの通信会社 Proton Technologies は DDoS 攻撃を回避したければ、「身代金」を払えという脅迫を受けた。同社のメールサービスは人権活動家等の多くが利用し、ユーザーからの業務継続（≒身代金支払い）要請を受けて、約 6,000 ドルのビットコインを支払った。②2016 年 2 月、米国南カリフォルニアの病院 Hollywood Presbyterian Medical Center がサイバー攻撃により患者の情報にアクセスできなくなり、「院内緊急事態」を発令する事態となった。病院は人命への影響を最小化するため「身代金」支払要求に応じた。③2016 年 5 月、カナダの University of Calgary の端末がランサムウェアに感染し、身代金支払の要求があった。研究機関として保有する重要機密の損失・漏えい回避という観点から、100 台の PC 端末と電子メール復旧のため、身代金 2 万カナダドル（約 170 万円）を支払った。④2017 年 1 月、オーストリアの 4 つ星高級ホテル Romantik Seehotel Jaegerwirt で客室のカードキーシステム等がランサムウェアに感染し、宿泊客が客室から閉め出される事件が起きた。当日の宿泊客は約 180 人で、ホテルは攻撃者の要求に従い、1,500 ユーロ相当のビットコインを支払った。

東京海上日動リスクコンサルティング株式会社

To Be a Good Company

ビジネスリスク本部
〒100-0004 東京都千代田区大手町 1-5-1 Tel. 03-5288-6556　Fax. 03-5288-6625
http://www.tokiorisk.co.jp/

