TOKIO MARINE

リスクマネジメント最前線

2022 | No.4

高まるランサムウェアの脅威と企業の備え *

ビジネスリスク本部 兼 戦略・政治リスク研究所 主席研究員 川口 貴久
専門分野：リスクマネジメント、国際政治・安全保障、サイバーセキュリティ

今日、サイバーセキュリティは企業経営やガバナンス・リスク管理のあらゆる領域に係わる。それゆえ、サイバーセキュリティは IT・セキュリティ担当役員や担当部門だけでの問題ではない。この点を改めて強調したのは、米国内で公開されたものを翻訳し、2019 年 10 月に経団連が公開した「サイバーリスクハンドブック」である[1]。これは一義的には取締役（業務執行を管理監督する立場）向けのものだが、業務執行側にも同様の示唆がある。

「ハンドブック」は原則の第一で「サイバーセキュリティを、単なる IT の問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要」を説く。このほか、全ての取締役に対してビジネスが依存する IT システムやサイバーセキュリティ関連の法規制の理解、M＆A や新製品開発などの意思決定におけるサイバーセキュリティ側面の検討を期待する。こうした理解がなければ、妥当な意思決定や投資判断ができないと考えてよい。

2019 年 7 月、あるスマートフォン決済サービスの不正利用が発覚した。不正利用が可能だった主な原因の一つは、同サービスが「二要素認証」を備えていなかった点である。しかし、その後の記者会見からは当該事業会社の社長が「二要素認証」を理解していない様子が伝わった。経営層が細かいサービス設計やサイバーセキュリティ技術まで把握している必要はない。だが、二要素認証のような、ビジネスモデルやサービス設計の「核心」となるようなセキュリティ施策・技術に関する知識は必須だ。そうでなければ、新規事業展開に関する意思決定や必要なセキュリティ投資に関する妥当な判断は下せない。経営層に期待されるサイバーセキュリティ知識は時代・状況とともに変化するため、不断にアップデートしなければならない。

そこで本稿では、世界で大きな脅威となっている「ランサムウェア」（身代金要求型ウイルス）について扱う。**ランサムウェアの脅威と必要な備えについて、経営層、経営企画・リスク管理・総務・広報・渉外といったコーポレート部門および事業部門が把握すべき点を紹介**する。

本稿は以下の報告・レポートを大幅に改変したものである。川口貴久「米コロニアル・パイプライン事案にみるランサムウェア攻撃対応の教訓」公益財団法人笹川平和財団 第２回 サイバーセキュリティセミナー2021 日本企業を狙うランサムウェアの脅威 ～安心・安全を脅かすサイバー攻撃の動向と対策～（2021 年 9 月 8 日）；川口貴久「"国家"に狙われる日本企業 経営層の意識変革は待ったなし」『Wedge』（2021 年 12 月）、33-35 頁。

[1] 全米取締役協会（NACD）が 2014 年に公開した米国版を日本語訳にしたものである。一般社団法人 日本経済団体連合会（経団連）『サイバーリスクハンドブック：取締役向けハンドブック日本版』（2019 年 10 月 31 日）。
https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.pdf

1. ランサムウェア攻撃の概要と特徴

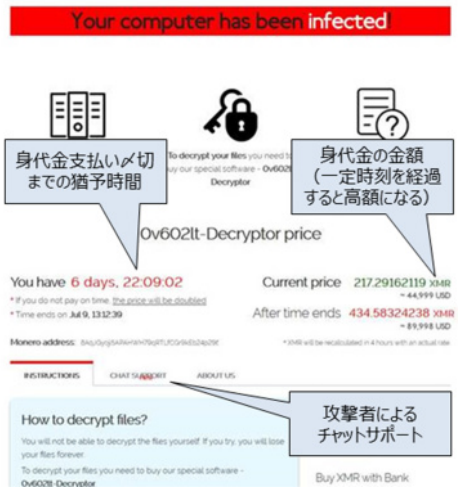
（1）ランサムウェア攻撃

ランサムウェアとは、身代金（ransom）を要求するマルウェア（malicious software：ウイルス等の不正やプログラムの総称）を指す。このタイプのコンピュータウイルスは約 10 年前から流行している。金銭目的の犯罪グループは解散・再結成・リブランディングを繰り返し[2]、2021 年 9 月時点で、全世界で約 20 のグループが積極的に活動中とみられる。

最近のランサムウェア攻撃のプロセスは次の通りである。まず、企業のネットワークに侵入する。その後、高次権限を奪取し、ネットワークを内で横展開しながら、機密情報やランサムウェアの展開方法を調べ上げる。個人データや営業秘密などのデータ窃取が完了すれば、データを暗号化する。多くの企業はバックアップをとっているので、攻撃者は可能であればバックアップを削除するか、これも暗号化する。最後は身代金を支払えと脅迫する（図 1）。

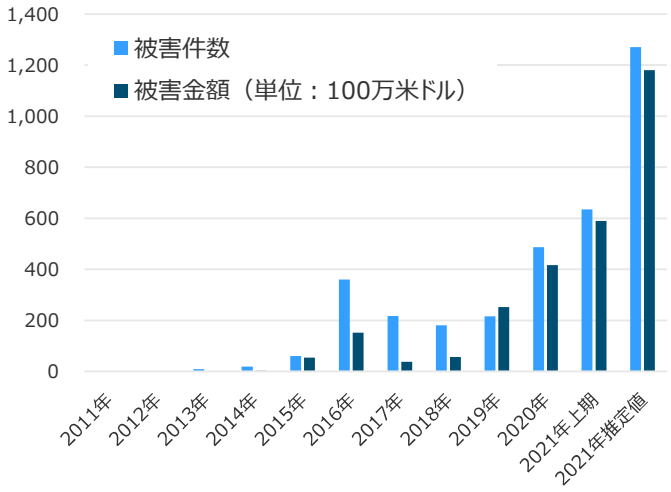
こうしたランサムウェア攻撃の被害は増加傾向にある。警察庁によれば、企業・団体等におけるランサムウェア被害の報告件数は、2020 年度下期の 21 件から、2021 年度上期には 61 件に増加した[3]。これはあくまでも警察庁への報告分であり、実際にはより多くの企業・組織が被害にあっていると推察される。また、米財務省によれば、2021 年上半期に報告されたランサムウェアの被害額（支払額）は 5.90 億ドルに達し、2020 年通年の 4.16 億ドルを上回った。2021 年通年（推定値）は過去 10 年間の総額を上回るペースである（図 2）。

■ 図 1 ランサムウェア感染時の表示例



出典：Mark Loman (@markloman), July 3, 2021 のツイートより抜粋。
https://twitter.com/markloman/status/1411053456983564300

■ 図 2 ランサムウェア被害の件数と金額の推移（米財務省）



出典： Financial Crimes Enforcement Network(FonCEN), Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data between January 2021 and June 2021, the United States Department of the Treasury, Oct 15, 2021. ※数値は報告日（Filing Date）ベースのもの。

[2] "Ransomware Gangs and the Name Game Distraction," Krebs on Security, August 5, 2021. https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/#more-56464

[3] 警察庁「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」2021 年 9 月 9 日、4-7、23-25 頁。https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

（２）ランサムウェア攻撃の被害と影響

ランサムウェア攻撃による被害と影響は以下に大別できる。

- 情報・データにアクセスできない、またはシステムを利用できないことによる事業・サービスの中断
- 機密情報の漏洩・暴露（個人情報や営業秘密・知的財産等の漏洩、暴露）
- レピュテーションの悪化（事業・サービス中断、情報漏洩、身代金支払い等）
- 直接・間接的な経済的損失（事業・サービス中断による逸失利益、情報インフラの復旧に関わる費用、企業価値の毀損等）

ランサムウェア攻撃によって、経営・事業に大きな影響が生じた事案もある。米国では、東部地域のエネルギー供給の約 45%を担うコロニアル・パイプライン社がランサムウェアに感染し、エネルギー供給が 6 日間途絶し、完全復旧に約 2 週間を要した。このほか、国内外の多くの大手企業が被害にあっている（表 1）。

■ 表 1 ランサムウェア攻撃による大規模被害例

被害企業・発生時期	被害の概要と影響
エネルギー大手 コロニアル・パイプライン （米国） 2021 年 5 月	• 米国東部のエネルギー供給量全体の約 45%を担う同社パイプラインによるエネルギー供給が 6 日途絶（完全復旧・通常化に約 2 週間を要する）。 • 同社は 440 万 USD の身代金を支払う。 • 同社最高経営責任者（ＣＥＯ）は連邦議会公聴会に召喚され、上下院で計 4 時間超の証言・質疑応答を求められる。
食肉大手ＪＢＳ （米国他） 2021 年 5 月	• ブラジル JBS の米国子会社 JBS USA は 1,100 万 USD 相当の身代金を支払う。 • 米国と豪州の IT システムを支えるサーバに影響が生じ、全世界の生産拠点 10 か所が操業停止。
ソフトウェア大手 Kaseya 及び顧客（米国他） 2021 年 7 月	• 同社のリモート監視製品「Kaseya VSA」のオンプレミス版の利用顧客でランサムウェア被害。Kaseya 社は念の為、オンプレミス版のみならず、クラウド版（SaaS）についても利用停止措置を講じる。 • 同製品の利用顧客のマネージドサービスプロバイダ（MSP 事業者） 40～60 社、MSP の顧客 800～1,500 社で被害。
ゲーム大手（日本） 2020 年 11 月	• 報道によれば、約 11 億円の身代金を要求されたが、応じず。 • 顧客・従業員・採用応募者等の個人情報や営業秘密（販売レポート、財務情報、取引先情報、営業資料、開発資料等）が暴露。
精密化学大手（日本） 2021 年 6 月	• ランサムウェア感染 3 日後からシステム等を順次復旧。完全復旧までに 2 週間を要する。 • 比較的早い段階でランサムウェア攻撃を検知し、被害拡大防止のためにネットワーク遮断やシステム停止を行ったとみられる。
食品大手（日本） 2021 年 7 月	• 基幹システムを格納するファイルサーバ、財務会計システム（国内グループ会社 26 社利用）、販売管理システム（同 11 社利用）が暗号化・停止。バックアップも被害。 • 2021 年第 1 四半期決算報告書提出が 3 か月遅延。

出典：筆者作成。

（３）近年のランサムウェア攻撃の特徴

ここ数年のランサムウェア攻撃には、標的、侵入経路、脅迫手法の観点でいくつかの変化・特徴がみられる。

特徴①標的：「ばらまき」型から「標的」型へ

これまでに拡散したランサムウェア CryptoLocker（2013 年）や WannaCry（2017 年）は世界中の不特定多数の企業・組織が被害にあった。しかし、最近のランサムウェア攻撃は、このような不特定多数への「ばらまき」型から、有名企業や脆弱性のある企業・箇所を狙った「標的」型に移行している。いくつかの攻撃者は標的企業の財務諸表を調査して支払能力を確認している。しかし、攻撃者にとっては何よりも、その企業に侵入口があるかどうかが重要だと考えられる。

特徴②侵入経路：「ネットワーク貫通」型

侵入口・侵入経路という点では、不審な添付ファイルや URL 付きのフィッシングメールによる ID/PW の窃取は引き続き懸念すべき脅威である。しかし、最近では、これに加え、社外から社内ネットワークに接続するための「仮想プライベートネットワーク（VPN）」機器等の脆弱性をついた「ネットワーク貫通」型の攻撃が増加している。既に公開済の「既知の脆弱性」が悪用されるケースが多く報告されている。表 1 のコロニアル・パイプライン社の事案では、会社が把握・管理できていない VPN 機器からの侵入が端緒だった。

一般にいう「ネットワーク貫通型」とは異なるが、ソフトウェアの更新機能やクラウドサービス経由での侵入も確認されている。2017 年にウクライナを中心に拡散した NotPetya では、税務・会計ソフト「M.E.doc」の更新機能が悪用された。表 1 の Kaseya 事案では、IT 機器・端末の遠隔監視を委託する事業者経由でのランサムウェア感染であった。

特徴③脅迫手法：「二重脅迫」型

最近の攻撃者は、データやシステムの暗号化に加えて、標的の機密情報を窃取している。ランサムウェア攻撃者は「復号化キーが欲しければ、また機密情報を暴露されたくなければ、身代金を支払え」と脅迫する（二重脅迫）。一部では、「三重脅迫」の攻撃も確認されている。例えば、暗号化、情報暴露に加えて、ホームページや EC サイトに DDoS 攻撃（標的対象の公開サーバに大量の情報を送り付けるサイバー攻撃）を行い、機能を停止する、と脅迫するものである。

2. ランサムウェア攻撃発生への備え

このようにランサムウェア攻撃が増加し、経営・事業への影響も大きいことから、ランサムウェア攻撃とその備えに対する経営の関心は非常に高い。ここでは、ランサムウェア攻撃への備えの考え方と準備事項を整理したい。

第一に、ランサムウェア攻撃**だけ**に特化した備えは存在せず、必要なことは自社のサイバーセキュリティ態勢そのもの・全体を向上させることである。前述のとおり、ランサムウェア攻撃のプロセス・構成要素のうち、侵入、高次権限奪取による横移動、マルウェア感染等はサイバー攻撃全般に共通する要素である。それゆえ、**ランサムウェア攻撃を予防するためには、サイバーセキュリティ態勢全般を向上**させる必要がある。

第二に、サイバーセキュリティへの投資は重要だが、**サイバーリスクはゼロにはならない**。なぜ、サイバーリスクはゼロにならないのか。米サイバー軍初代司令官・元国家安全保障局長官だったアレグザンダー（Keith Alexander）は 3 つの脆弱性で説明する。すなわち、①未だ公開されていない「未知の脆弱性（ゼロデイ）」、②公開済の「既知の脆弱性」への対応の遅れ、③設定ミスや不適切なパスワード管理などの「人間の脆弱性」である[4]。これら脆弱性がある限り、侵入を予防することは極めて困難だろう。それゆえ、企業は、サイバーセキュリティ分野への十分な**投資を通じて、サイバーリスクを許容レベル以下に抑えるとともに、残余リスクへの備えとしてサイバー攻撃発生時の対応態勢を整備**すべきである。

（1）ランサムウェアを含むサイバー攻撃全般への対応

実際問題として、ランサムウェア攻撃への備えの多くはサイバー攻撃全般への備えと共通する。とはいえ、各国の政府機関・サイバーセキュリティ機関は（恐らく企業・組織の関心に訴える目的もあって）「ランサムウェア攻撃対策」と銘打って様々な情報を公開している。例えば、米国国立標準技術研究所（NIST）は、ランサムウェア攻撃の「予防」の 8 つのポイントと、万が一、ランサムウェアに感染した場合の「復旧」の 3 つのポイントを以下のとおり公開している。

■ 表 2 米 NIST「ランサムウェア対応のヒント」（2021 年 5 月 13 日）

予防	1. ウイルス対策ソフトウェアを常時使用する 2. 全てのセキュリティパッチを適用する 3. 既知のランサムウェアサイトへのアクセスをブロックする 4. 承認されたアプリケーションのみを実行する 5. 個人所有デバイスの使用を制限または禁止する 6. （可能な限り、管理者権限を持つアカウントではなく）標準ユーザアカウントを使用する 7. 私用のアプリケーションや Web サイト（メール、SNS 等）を使用しない 8. 不明なソースからのファイルやリンクを開かない
復旧	1. インシデント復旧計画を策定し実装する 2. データのバックアップと復元の戦略を慎重に計画、実装、検証する 3. 法執行機関を含む組織内外の連絡先リストを更新・維持する

出典： “NIST Releases Tips and Tactics for Dealing With Ransomware,” National Institute of Standards and Technology, May 13, 2021.
https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

[4] Rt. Gen. Keith B. Alexander, “Securing the Cybersecurity Future of Japan: Leader’s Role in Cyber Incident Response” 経団連主催 第 3 回サイバーセキュリティ経営トップセミナー（2018 年 10 月 31 日）。

前述のとおり、表 2 で掲げられた対策はランサムウェア攻撃に特化したものではなく、多くのサイバー攻撃の予防・復旧に貢献するものである。ここでは、NIST でいう「復旧」の 3 点について補足する。

①緊急時の対応計画の策定

ランサムウェア攻撃をはじめとするサイバー攻撃が発生した場合、これを検知し、緊急性を判断した上で、脅威の封じ込め・除去、復旧するための体制・手順・ツールを定めておく必要がある。これらは、IT・セキュリティ面での対応体制（CSIRT）や対応手順（インシデント対応手順）に加えて、会社全体の危機管理・事業継続という観点から、ランサムウェア攻撃をはじめとするサイバー攻撃への危機対応計画や事業継続計画（BCP）が必須である。

緊急時の対応計画には少なくとも以下の要素を含む必要がある。

- IT・セキュリティ部門だけではない全社的な指揮命令・対応体制
- 感染・被害拡大を防止するための選択肢
- IT インフラが使えない場合の事業継続策
- 身代金支払い脅迫に対する方針・手順（もちろん、身代金支払いには応じない、ということ）
  ※この項目はランサムウェア攻撃に特化したもの。
- 対外発信・広報に関する方針・手順
- 自力でのシステムやデータの復旧可否の見極め手順、復旧工程　等

また、JPCERT/CC が公開する「侵入型ランサムウェア攻撃を受けたら読む FAQ」も事前に確認しておくとよい[5]。

②バックアップ

データやシステムのバックアップは重要であり、一般的に「321 ルール」に準拠すべきと考えられている。

「321 ルール」とは、

- 3 つのデータコピーを持つ（2 つのバックアップ）
- 2 種類の異なるメディアで保管する
- 1 つは違う場所（遠隔地で保管されるクラウドサービス等を含む）で保管する

ことを指す。もちろん、バックアップの範囲や頻度はコストに直結するため、経営判断を要する。

③緊急時連絡先

ランサムウェア攻撃をはじめとするサイバー攻撃や大規模システム障害の発生時、社内ネットワークにアクセスできず、連絡先を確認できない可能性、メールやオンライン会議ツールが使えない可能性がある。そのような場合に備えて、オフラインでの連絡先（下記例）や連絡手段を準備しておくことが望ましい。

- 社内の関係部門（トップマネジメント、危機対応チーム、CSIRT、システムオーナー部門、事業部問等）
- 主要な顧客、仕入先、業務委託先
- 法執行機関、規制当局、法律上必要な報告先（少なくとも、個人情報保護委員会、証券取引所（適示開示）等）
- 主要なソフトウェア等の開発会社、セキュリティ会社、インシデント対応専門会社
- 公的なサイバーセキュリティ団体（サイバーセキュリティ協議会、IPA、JPCERT）、サイバーセキュリティ関連の業界団体（業界 ISAC）

[5]「侵入型ランサムウェア攻撃を受けたら読む FAQ」JPCERT/CC（2022 年 1 月 13 日）
<https://www.jpcert.or.jp/magazine/security/ransom-faq.html>

（２）ランサムウェア対応に固有の対応： 脅迫対応

ランサムウェア攻撃発生時に固有の対応は、身代金要求への対応である。言うまでもなく、**身代金要求は、支払わないことが大原則**である。その理由は以下のとおりである。

- 日本はランサムウェア攻撃に対して身代金を支払う率が他の先進国に比べて低い[6]。これは、日本国内では、公序良俗に反する観点から、身代金支払いに対する社会の許容度は低いことの結果と考えられる。
  なお、2021 年 12 月時点で、日本の大企業が多額の身代金を支払ったと報じられた例は確認できない。
  万が一、日本国内で最初の大規模支払い事例と報じられた場合、その後、攻撃者がますます日本企業・市場を狙う可能性がある。特に大手企業は、自社の身代金支払いは将来の日本企業へのランサムウェア攻撃を増加させうるという認識を強く持つ必要がある。
- 攻撃者が盗んだ情報を暴露するかしないかに関わらず、情報が漏洩した事実は変わらない。
- 身代金支払いによって、攻撃者から提供される複合化ツールが十分に機能するかは分からない。
- 一度身代金を支払うことによって、将来、再び標的となる可能性がある[7]。
- 米国財務省外国資産管理室（OFAC）等がランサムウェア攻撃グループを金融制裁指定している場合、支払った企業が諸外国の二次制裁の対象となる恐れがある[8]。

身代金を支払わないことが前提としても、留意すべき点がある。顧客や投資家等のステークホルダーは、「事業・サービス中断の長期化や不特定多数への情報暴露は、被害企業の意思決定・判断（身代金を支払わなかったこと）の結果」と認識する恐れがある。従って、支払わないことを選択するとしても、支払い要否の判断根拠・判断プロセスを残すことが重要である。経営会議での承認、臨時取締役会の開催、持株会社/事業会社一体での対応を検討する会社もある。

身代金支払い要求を受けた事実や支払い要否に関する判断結果については、企業は積極的かつ広く対外開示する必要はないが、場合によっては、ステークホルダーに対する説明責任を問われる場合がある。身代金支払い要求の対応は、危機対応・事業継続の中でも、特に対外的なアカウンタビリティが期待されると考えるべきである。

---

[6] Yukimi Sohta「身代金を支払うのは正解か？ランサムウェア支払い結果 7 か国比較から考えるサイバー犯罪エコシステムへの対処」ProofPoint、2021 年 7 月 5 日。https://www.proofpoint.com/jp/blog/threat-insight/is-it-right-to-pay-the-ransom

[7] 同上。

[8] 他方、一般論として支払い要否を検討するケースがあることも事実である。例えば、
① 事業**継続の期待度が極めて高い**場合（例：エネルギー供給等の社会生活にかかわる場合、医療等の人々の生命に直結する場合等）
② 結果的に情報が暴露されたとしても、**暴露タイミングを遅らせることで被害拡大防止**に資する場合
③ 自力での**復旧が極めて難しい・不可能**な場合 等
である。しかし、いずれの場合であっても、日本国内では一定のレピュテーション悪化を前提としつつ、経営判断を下すべきであろう。

[2022年2月4日発行]

To Be a Good Company

東京海上ディーアール株式会社

ビジネスリスク本部　兼　戦略・政治リスク研究所　主席研究員　川口　貴久（専門分野：リスクマネジメント、国際政治・安全保障、サイバーセキュリティ）

〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594　Fax. 03-5288-6626 www.tokiorisk.co.jp