KOKUSAI SHŌJI HŌMU

国際商事法務

JOURNAL OF THE JAPANESE INSTITUTE OF INTERNATIONAL BUSINESS LAW

Vol. 49, No. 10
(通巻712号)

経営判断を迫るサイバー攻撃・ランサムウェアの最新動向について

山岡裕明*

Ⅰ　ランサムウェアとは

ランサムウェアによるサイバー攻撃が世界中の企業にとって看過できないリスクとなりつつある。

ランサムウェアとはランサム（身代金）及びマルウェアから成る造語である。

従来ランサムウェアの攻撃手法は，端末内のデータを暗号化して利用できなくさせて，復号（復旧）の対価として身代金を要求するものであった。

ところが，昨今，ランサムウェアの攻撃手法に変化が見られている。すなわち，従来のデータの暗号化に加えて，端末内のデータを窃取したうえで，データの復号及び非公開の対価として身代金要求するという手法が確認されている（「二重の脅迫」型とも呼ばれている[1]。）。

Ⅱ　ランサムウェア攻撃の深刻化

調査[2]によると，2020年８月から2021年７月の間の12ヶ月間で，ランサムウェアによるサイバーインシデントは121件発生しており，前年比で64％増加している。

また，同調査によると，身代金として要求される金額も高額となっており，１件あたりの平均額は1,000万ドルをこえ，3,000万ドル以上のインシデントは30％となっている。

Ⅲ　ランサムウェア被害の実例

近時注目を集めた被害事例として，2021年５月に報道された米国の石油パイプラインの最大手 Colonial Pipeline Company（以下「コロニアル社」という。）におけるランサムウェア攻撃が挙げることができる。

同社において，2021年５月７日，ハッカー集団からランサムウェア「Darkside」による攻撃を受けたことが発覚した。この攻撃は，まさにデータの暗号化と窃取という二重の脅迫型とされており，身代金として75ビットコイン（当時の価値で $4.3 million）の要求をなされた。同社は米国東海岸の燃料消費の半分近くのシェアを占める社会的インフラを担う企業であるところ，このサイバー攻撃を受けてから全てのパイプラインが稼働するまでにおよそ約１週間掛かったとされており，ランサムウェアが引き起こす被害の深刻さが浮き彫りになった。

また，同事案の特筆すべき点として，同社がハッカー集団に身代金を支払った点を挙げるこ

*やまおか ひろあき，弁護士（八雲法律事務所），内閣サイバーセキュリティセンターSWGタスクフォース構成員（2019年～2020年），カリフォルニア大学バークレー校客員研究員（2019年～2021）を務める。

本稿は、去る８月27日に開催された「アメリカン・ロイヤーズ・クラブ」（(一社）国際商事法研究所）における筆者の講演の要旨である。

とができる。同社のCEOであるJoseph Blount氏は，同年6月8日の上院委員会での証人喚問において，「私は，パイプラインを早期復旧するために利用可能なあらゆるツールを入手すべく身代金を支払うという意思決定を行った（I made the decision that Colonial Pipeline would pay the ransom to have every tool available to us to swiftly get the pipeline back up and running」と述べて，その支払いを認めている[3]。

Ⅳ ランサムウェア増加の背景

経済産業省から2020年12月18日付で注意喚起（以下「経産省注意喚起」という。）がなされており[4]，「大企業・中小企業等を問わないランサムウェアによる被害の急増」の背景事情として，「RaaS（Ransomware as a Service）とも呼ばれる，マルウェアの開発者と当該マルウェアを使って攻撃を行う攻撃者などで構成される，ランサムウェアの提供や身代金の回収を組織的に行うエコシステムが成立したことにより，高度な技術を持たなくても簡単に攻撃を行えるケースが増えていることなどが挙げられる」という指摘がなされている。

このRaaSと呼ばれる一種のエコシステムにより，犯罪収益目的の実行犯（Affiliatorともいう。）が増え，その結果，ランサムウェアによるサイバー攻撃が増加しているという背景がある。

Ⅴ ランサムウェア攻撃を受けた場合の法的留意点

1 OFAC規制

上記の経産省注意喚起において，「国によっては，金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ，金銭の支払いを行った企業に対して制裁が課される可能性もある。」と言及されているところ，米国においては，まさにOFAC規制が身代金の支払いを厳しく規制している。

すなわち，財務省外国資産管理室（The U.S. Department of the Treasury's Office of Foreign Assets Control; OFAC）は，外国資産管理規則（Foreign Assets Control Regulations）に基づいて情報の提供，処罰の決定，違反者への制裁等を管轄する官庁で，同規則に基づいて制定される各種規制がOFAC規制と呼ばれている。2020年10月1日，OFACは，「ランサムウェアの支払いを助長することに関する潜在的制裁リスクについての勧告[5]」（Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments）を発表し，身代金の支払いについてOFAC規制が発動され得るとの解釈を示した[6]。

2 善管注意義務との関係

仮に，身代金の支払いがOFAC規制のようなハッカー集団への身代金の支払いを直接禁ずる法律に抵触しないとしても，身代金相当額の損害が会社に生じる以上，意思決定を下す経営層としては，経営判断原則（business judgement rule）を踏まえつつ，善管注意義務に違反しないかを注意する必要がある。

上述のコロニアル社のCEOであるJoseph Blount氏は，同証人喚問において，身代金を支払ったことに関して「人生で最も大変な意思決定の一つであった（It was one of the toughest decisions I have had to make in my life)」と述べていることからも，その意思決定の重大さが伝わってくる。

3 適時開示との関係

ランサムウェア攻撃については，サイバー攻撃を受けた時点で発生事実として，また，仮に身代金を支払うのであればその意思決定を下した点について決定事実として，適時開示の要否が問題となる。

かつては身代金の要求額が高くなかったため，決定事実との関係で適時開示が問題になることは少なかったが，上述のとおり昨今では身代金として要求される金額が増額しているため，適時開示の要否に留意する必要が生じている。

4 個人情報保護規制との関係

二重の脅迫型のランサムウェア攻撃では企業

が保有するデータの窃取を伴うため，窃取されたデータに個人データが含まれている場合には，各国の個人情報保護規制に沿った対応が必要となる。

欧州におけるGDPRや米国各州で制定されているPrivacy Actにおいては，個人情報の漏えい時に当局への報告及びその期限が既に法律上の義務として制定されている。

他方で，国内の個人情報保護法の下では，個人情報保護委員会への報告は努力義務にすぎなかった。しかし，2022年4月1日に施行される改正個人情報保護法の下では，一定の場合を除いて同委員会への報告が法律上の義務となり，また，速報及び確報という2段階において報告期限が定められた点に留意が必要となる。

Ⅵ 結びに代えて

コロニアル社の事案から分かるとおり，ランサムウェア攻撃は，もはや企業の事業継続を脅かすリスクとなっている。また，その増加背景を踏まえると，「When, not if（発生するかどうかの問題ではなく，発生することを前提としていつ発生するか）」というレベルのリスクとして認識する必要がある。

実際にランサムウェア攻撃を受けた企業のインシデントレスポンスに携わっている筆者の実務経験上，ランサムウェアへの対応は，身代金の支払い期限として指定された短期間での，経営層を中心とした総力戦となる。また，海外の関連会社が被害を受けた際には，留意すべきレギュレーションが増えるため，その対応は更に難易度が上がる。

ランサムウェア攻撃による被害実態と法的留意点の現状整理として本稿が国際法務担当者の一助となれば幸甚である。

〔注〕

1 2020年8月20日独立行政法人情報処理推進機構セキュリティセンター「事業継続を脅かす新たなランサムウェア攻撃について」(https://www.ipa.go.jp/files/000084974.pdf)

2 2021年8月23日付Barracuda Threat Spotlight (https://www.barracuda.co.jp/threat-spotlight-ransomware-trends/)

3 HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS, June 8, 2021. Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company (https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf)

4 2020年12月18日経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

5 OFAC, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," Oct 1, 2020, *available at* https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

6 詳細は拙稿「脅迫型サイバー攻撃の現状と企業対応の実務」会社法務A2Z 2021年4月号を参照されたい。

アクセス・ツー英米誤考 ㉚

1）秋始めの季語処暑（Latest summer和誤）8月27日夕刊朝日のコラム素粒子に「自宅療養」（Home stay family treatment care和誤）と書いて「キミンセイサク」と読むとあり，辞典にはギミン（義民）があるがキミンはなく，セイサクは政策のことのようだから，義民（我が身をかけて正義を守る人々（People fighting for justice和誤）の語は当用漢字にあるが，キミンを深く調べると棄民も（戦争や災害で苦しむ人々が頼りにしない（No rescue of people suffering for war etc.（和誤））とあるから，8.15敗戦戦没者のことになると国の責任者云々となり，国語辞典の当用漢字にないのは理解できる。

2）同じく秋の季語残暑（Early autumn和誤）の9月1日詠んだ俳歴2年目の「高層の物書き机残暑かな」の高層が具体的ではなく高層ビルのマンションのこと「ものを書く高層ビルの残暑かな」と指導者の先生が句会欠席の投句者（Haiku writer）不在のところで直されたこと，テレビで好評の夏井いつき先生の投句した出席できない人の気持の詠みの違いを改めて学習した。（小原三佑嘉）

事務局だより

本誌及び一般社団法人国際商事法研究所に関する情報をホームページでご覧いただけます。
http://www.ibltokyo.jp

※NY州CLE単位付与対象

当研究所の最近の事業の実績及び予定は下記のとおりです。なお，ビジネス・ロースクールは広く会員以外の方でも受講することができますのでご利用下さい。「会員」（表2参照）への入会手続きは，事務局までお問合せ下さい。

新型コロナウイルス感染症への対応のため，現在，WEBのライブ配信で開催しております。尚，今後の状況等により開催延期・中止することもありますが，この場合には，HP上にてお知らせいたします。

●月例会

10/13「中国の個人情報保護法へのコンプライアンス対応」　中国・英国弁護士　李 暁蓓氏
（ﾓﾃﾞﾚｰﾀ）日本・NY州弁護士　杉本武重氏
（WEB/ライブ配信）

10/21「COVID 19とAIが英国雇用法に与えている影響」　英国弁護士　A. フレデリック氏
英国弁護士　J. デイビス氏
英国弁護士　S. イリング氏
（ﾓﾃﾞﾚｰﾀ）弁護士　中田浩一郎氏
（WEB/ライブ配信）

●研究会

〔国際通商法研究会〕

10/28「中国の反外国制裁法について」
中国弁護士　李 美善氏
中国弁護士　李 敬花氏
（WEB/ライブ配信）

〔CIS・東中欧法研究会〕

（要請中）

〔中国法研究会〕

10/25「中国最新法令動向」
（WEB／ライブ配信）　弁護士　住田尚之氏

〔中東ビジネス法研究会〕

9/21「UAE・イスラエル・イランの関係と各国投資環境」弁護士（在ドバイ）　森下真生氏
（WEB／ライブ配信）月例会と共催

〔アメリカン・ロイヤーズ・クラブ〕

8/27「経営判断を迫るサイバー攻撃・ランサムウエアの最新動向」　弁護士　山岡裕明氏
（WEB／ライブ配信）

〔イングリッシュ・ロイヤーズ・クラブ〕

10/5「M&Aシリーズ④競争法，オークション，MBO/LBO」
ベーカー&マッケンジー法律事務所パートナー　乗越秀夫氏
（WEB／ライブ配信）

〔チャイニーズ・ロイヤーズ・クラブ〕

10/26「中国の個人情報保護法～本社と現地法人の留意事項」　弁護士　中川裕茂氏
（WEB/ライブ配信）

〔国際M&A契約研究会〕

9/16「M&A事例について」～補償条項の後半部分について　㈱リケン法務室長 臺 礼子氏
（WEB／ライブ配信）

●ビジネス・ロースクール

10/7「ビジネス法律英語入門」
弁護士　長谷川俊明氏
（WEB／ライブ配信）

10/29「国際取引に伴う税務基本講座」
税理士　牧野好孝氏
公認会計士　鈴木康二氏
（WEB／ライブ配信）

11/11「英文契約書作成の実務基本講座」
弁護士　長谷川俊明氏
（WEB／ライブ配信）

11/26「（中級）英文契約書作成の法務セミナー」
筑波大学教授・弁護士　大塚章男氏
（WEB／ライブ配信）

12/14「英文契約ドラフティングとアメリカ契約法」
中央大学教授・NY州弁護士　平野　晋氏
（WEB／ライブ配信）

●マテリアルズ

「中国への出向者のための講習」

●国際ビジネス法エグゼクティヴ・サマリー

No.51「オランダ・ハーグの地方裁判所がロイヤル・ダッチ・シェルにCO_2の純排出量を2030年までに2019年比で45%削減するよう命じた事例」
（HP上に掲載）　弁護士　江口尚吾氏

●英文契約法律実務相談室（WEB／ライブ配信）

10/6　（ご担当）弁護士　長谷川俊明氏

研究会参加のおすすめ

本欄に掲げてあります「国際通商法研究会」以下の『研究会』は，予め会員の中からメンバーを募り，Zoomのオンライン形式で運営しております。

会員の皆様は随時参加（無料）できますので，参加を希望される方は，事務局までご連絡下さい。