法務の眼 Legal Eyesight

ランサムウエア攻撃と法務

KDDI 株式会社
総務本部法務部　法務部長
和田進太郎 (Shintaro Wada)

1　ランサムウエア攻撃の広がり

近年、企業をねらったサイバー攻撃、特にランサムウエア攻撃の報道を見る機会が増えている。本年10月31日付の日経の記事によると、本年１月～６月は国内でも116件のランサムウエア被害が発生し、世界の2025年のランサムウエア被害額は570億ドル（約８兆7000億円）に達する見込みとのことである。

そもそも、ランサムウエア攻撃とは何かということであるが、企業のシステムやネットワークの脆弱性をねらったランサムウエア犯罪者によるサイバー攻撃である。犯罪者が何らかの手段により社内のシステムやネットワークに入り込み、データを暗号化したり、データを盗んだりすることによって、企業を脅迫して、身代金（ランサム）を要求する。

世の中には DarkWeb という通常のブラウザではアクセスできない世界があり、そのなかで盗まれたデータが公開されたり売買されたり、ランサムウエア攻撃が宣言されたりするようである。また、RaaS（Ransomware as a Service）というランサムウエアをサービスとして提供する人たちがおり、それをアフィリエイトが利用して犯罪に利用するなど、ランサムウエアに関する分業と協業のビジネスモデルが構築されているケースもある。

2　ランサムウエア攻撃のおそろしさ

ランサムウエア攻撃は予測ができない。当社もいつ被害にあうかわからない。明日かもしれないし、１年後かもしれないし、被害を受けないかもしれない。しかも、いったん被害を受けてしまうと、企業の経営活動の根本であるオペレーションがとまってしまう。

当社であれば、最悪のケースであれば通信をとめてしまうおそれがある。それは企業経営にとって重大なリスクであり、サービスや商品を利用する人の生活にも大きな影響を与えてしまう。

当社は３年前に約2000万人以上のお客様に対して最長約61時間にもわたり大規模な通信障害を起こしてしまい、通信を提供できないことによって社会にご迷惑をかけたことがある。通信を提供できないということが、企業の経営だけでなく、いかに人々の生活に影響を与えるのか、身をもって経験した。あのときは、当事者として、いつ通信障害が終わるのか不安を感じていた。

法務部門としては、通信サービス約款上の位置づけの検討や損害賠償の検討などを実施したものの、通信障害中は技術部門を陰で応援するしかできず、通信障害の解決に直接貢献できないもどかしさを感じていた。

ランサムウエア攻撃の場合も通信障害と同様、いつ被害が回復するのか予想がつかない点においては大きな不安を与えるものである。また、ランサムウエア攻撃のときは、犯罪者がいるという点においては経営層や従業員への不安はより大きいものであるに違いない。

3　ランサムウエア攻撃対策の重要性と難しさ

このように、ランサムウエア攻撃を受けると、最悪の場合、ビジネスの継続性に支障が出てしまう。BCP を定めている企業も多いとは思うが、その一内容としてランサムウエア攻撃を受けたときの対策も事前に策定しておくことが、現在の企業に求められる要請なのだろう。

ランサムウエア攻撃対策としては、しっかりとしたセキュリティ対策やデータのバックアップ以上の特効薬はないようである。だが、いかにセキュリティ対策をしていても、システムの脆弱性が発見されるケースもあり、対策には限界がある。AI の発展により、AI を利用したラ

ンサムウエアが作成され、ランサムウエア攻撃対策としてもAIが利用され、専門外の人間からするとますます予測がつかない状況になりそうである。

また、特に大企業になると、日々のオペレーションで利用しているシステムは無数にあり、事前にどこのシステムがねらわれるのか予測するのは難しい。ランサムウエア攻撃にあった際の代替システムの検討を無数にすることも現実的ではない。そもそも基幹システムであればその代替システムは本当に存在するのか、どういう事象かわからないのにシステムの復旧時間を考えることはできるのか、課題も多そうである。ランサムウエア攻撃を受けた経験がある企業は少なく、経験したことのないことを想像しながら対策を考える難しさも無視できない。

ただ、このような状況でも検討できることはある。世界でおこっている実際の被害事例は、一部ではあるものの、日々報道はされており、ランサムウエアの攻撃者がどういった属性で、どういった手段をつかって、何をしてくる傾向があるのか分析をすることはできる。また、日本だけでなく、アメリカやEUもランサムウエア攻撃対策には力をいれており、各国政府が出す情報も重要なリソースだろう。このように情報を得ながら、少しずつランサムウエア攻撃発生時のイメージの解像度をあげて対策していくしかない。

4　ランサムウエア攻撃対策における法務部門の役割

ランサムウエア攻撃対策のメインはセキュリティ対策である以上、最も重要な部門は情報セキュリティ部門であることは確かだ。だが、情報セキュリティ部門だけでは解決できない重要な課題もある。

ランサムウエア攻撃は通常のセキュリティインシデントと異なる。一番大きいのは、犯罪者が現前にいるということである。たとえば、フィッシング詐欺などでは犯罪者は身を隠すのが通常である。他方で、ランサムウエア攻撃では、犯罪者が自らが犯罪者であると宣言する（それが本当の犯罪者かわからないことの難しさはあるが）。したがって、企業としては犯罪者との交渉というフェーズが必ず発生する。また、その犯罪者は外国に拠点を置くことが通常である。外国の犯罪者と交渉しなければならないという難しい局面において、経営層の意向、情報セキュリティ部門、捜査機関、法律事務所などと調整しながら交渉を支援できる能力があるのは法務部門であると考えている。

当社においても、情報セキュリティ部門と密に連携して、ランサムウエア攻撃があった際に当部が果たすべき役割について、想像力を働かせながら、細かく具体的に整理し、万が一の際に迅速に動けるように準備している。通信障害のような事態が起こるのは絶対避けたいところだが、ランサムウエア攻撃の被害にあってもその被害を最小限にできるよう万全の措置をとりたい。

そして、ランサムウエア攻撃があると多数の法律問題が発生する。個人情報保護法、官公庁対応、顧客との対応、公表のあり方、各国の規制、究極的には（各フェーズにおける）経営判断のあり方などをもれなく検討しなければならない。最近、森・濱田松本法律事務所外国法共同事業の蔦大輔弁護士ほか同事務所サイバーセキュリティ法研究チームが、『クロスセクター・サイバーセキュリティ法』（商事法務、2025年）で、横断的に検討、整理されているとおり、サイバーセキュリティには法務上検討しなければならない重要な話が多数ある。ランサムウエア攻撃に関しても、身代金の支払い是非に関する論点を含め対応すべき論点が網羅的に検討されており、ランサムウエア攻撃対策を検討する際に参照すべき必須の書籍である。また、サイバー攻撃はグローバルな事象であり、日本法における検討だけでなく、アジア、EU、アメリカなどの法規制も紹介されている点は大変ありがたい。

このように、ランサムウエア攻撃は企業に深刻な被害をもたらしうる事象である一方で、企業の法務部門として解決に貢献できることは大きいと信じている。企業の危機的な状況の解決に貢献できる法務部門であれば、それは価値のある法務部門であることにだれも異論をはさまないだろう。