「守り」から「早期復旧」へかじを切った経営の決断

SBSホールディングスが貫く「物流を止めない」覚悟

サイバー攻撃の「真の恐怖」は、業務が一時的に停止して売り上げが減ることではない。復旧が大幅に遅れれば、事業そのものが立ち行かなくなり、「倒産」の２文字が現実味を帯びる。かつてランサムウェア被害に遭い、「倒産リスク」の大きさを思い知った総合物流企業のSBSホールディングスは、従来の「防御」を中心とするサイバーセキュリティから、「迅速な復旧」を柱とするサイバーレジリエンスへとかじを切った。

メーカーの物流子会社を積極的に買収 非連続な成長を遂げる

2003年の株式上場以来、20年余りで年間売上高が25倍以上、営業利益は53倍と急成長を遂げている総合物流企業のSBSホールディングス。大手メーカーの物流子会社などを30社以上もM&A（合併・買収）して、非連続的な成長を遂げてきた。

「物流業務を切り離して効率化したい大手メーカーから子会社を取得し、当グループの洗練された物流オペレーションを移植する。その繰り返しによって、非連続的な成長を遂げてきました。合併・買収した物流会社の企業価値が高まり、グループシナジーが生まれれば、オーガニックな成長も促進されるという好循環がもたらされます」

そう語るのは、同社 グループITインフラ統括部長の宮崎 健氏である。

リコー、東芝、NSK（日本精工）、ブリヂストンなど、名だたるメーカーの物流子会社を買収してきたが、それが実現できたのは、元の親会社から「安心して譲渡できる」という高い信頼を得たからにほかならない。

「買収した物流会社の大半は、その後も元の親会社の物流を請け負うことになりますが、サービスの質の低下を招いてしまっては、売ってくださる企業にとって何の価値もありません。我々としては、売り手側の期待に十分応えられる体制を整え、安心していただく必要があるわけです」と宮崎氏は説明する。

その「安心」を担保するために、中でも重要となるのが、「物流を止めない」ためのサイバーセキュリティ対策だ。

ランサムウェア攻撃を受けた苦い経験を基にセキュリティを高度化

SBSホールディングスは、過去に１度ランサムウェア攻撃を受け、危うく事業が停止しかけた苦い経験がある。これが、強固なサイバーセキュリティ体制の重要性を再認識する大きなきっかけとなった。

攻撃が発覚したのは、17年のある日のことである。その日の未明、宮崎氏は、会

SBSホールディングスが貫く「物流を止めない」覚悟

社支給の携帯電話が何度も鳴り響くのを聞いて目を覚ました。携帯を開くと、よく分からないエラーメールやアラートが大量に転送されていた。

「メールを見ても状況が分からないので、リモートPCを立ち上げ、社内ネットワークに入ろうとしたが、全くつながりません。相当大きな事故が起きているな、と感じて、すぐ会社に駆けつけました」と、宮崎氏は振り返る。

会社に着くと、早朝にもかかわらず、すでに何人かの社員が来ていた。「システムがまったく動いていない」と大騒ぎしているので、調べてみると、複数台のクライアントPCにランサムウェアの脅迫メッセージが表示されているのが見つかった。

「これでランサムウェア攻撃が原因であることが特定できました。まだ出社時間前だったので、PCを立ち上げることを全面禁止し、ネットワークやサーバーもすべて遮断しました。判断が早かったおかげで、被害の拡大は何とか食い止められたと思います」（宮崎氏）

しかし、業務に欠かせないデータがランサムウェアの“人質”にされたことで、ほぼ1週間、システムが動かない状況が続いてしまった。

「幸いなことに、ランサムウェアの侵入経路と時期は特定できたので、影響を受けていないバックアップデータを使って、1週間程度で何とか大半の業務を復旧することができました。けれども、これはあくまで不幸中の幸い。どの範囲のデータが影響を受けているのかを特定できず、まっさらな状態からハードウェアやシステムを組み直したとしたら、復旧までに数カ月かかっていたかもしれません」と宮崎氏は語る。

実際に数カ月も業務が止まってしまったら、会社としての存続そのものが危うくなる。売上の減少や、信頼の低下といった生易しいリスクではなく、「倒産リスク」が現実味を帯びることになるのだ。

被害から9年が経過し、近年のサイバー攻撃は、急速に進化するAIの技術を採り入れることなどで、高度化、巧妙化が飛躍的に進んでいる。

「侵入経路や時期の特定はますます困難になっており、次に襲われたら、数カ月にわたって業務が復旧できなくなる恐れがあります。当グループの経営層も、サイバー攻撃による倒産は『十分に起こり得るリスクである』という認識を強くし、対策強化のために積極的な投資を行いました」と宮崎氏は明かす。

ここ数年、大手通販サイトや大手飲料メーカーなどが、相次いでランサムウェア攻撃を受け、業務停止状態に追い込まれたことも、経営層の危機意識を高めたようだ。

ランサムウェア対策を念頭に置いたバックアップソリューション

M&Aを重ねながら、非連続的な成長を継続するため。そして何より、業務停止による「倒産リスク」を回避するため。この2つの大きな目的を果たすべく、SBSホールディングスは継続的にサイバーセキュリティ対策の強化を図ってきた。

「ランサムウェア攻撃を受けた17年以降、ファイヤーウォールを先進的なものに入れ替えたほか、SOC（セキュリティ・オペレーション・センター）への委託、EDR（エンドポイント監視・検知）ソリューションの導入など、検知と防御に関するサービスや

SBSホールディングス株式会社
グループITインフラ統括部長

宮崎 健 氏

SBSグループのITインフラ、セキュリティ戦略を統括。M&AにおいてはITインフラ、セキュリティ領域のデューデリジェンスからPMIまでをリード、グループ全体のITガバナンス高度化を推進してきた。クラウド活用、サイバーレジリエンス強化、事業継続性向上を通じて、持続的な成長を支えるIT基盤づくりに取り組んでいる。

ソリューションを積極的に採り入れてきました。しかし、業務を早期復旧させるには、“守り”を固めるだけでなく、侵入されることを前提としたリカバリー策をしっかり打っておかなければなりません。いわゆるサイバーレジリエンス対策です。防御の高度化がある程度進んだ23年ごろから、本格的にその取り組みを開始しました」と宮崎氏は語る。

同社は当初、メインのデータセンターのほかに「第2センター」を設け、そこで毎日バックアップデータを取って、万一の際には第2センターで早期復旧することを検討した。しかし、社内ネットワーク上にウイルスが潜んだままの状態でデータを戻しても、第2センターにも感染してすぐに使い物にならなくなるのは目に見えている。

「第2センターにバックアップを取るというのは、金融機関などでよく用いられる手法ですが、本来、地震や火災といった災害時への対応を念頭に置いたソリューションなので、サイバー攻撃への対応にはあまり適していません。かといって、他に選択肢がなかったので、すべてのウイルスを駆除できた可能性に賭けて第2センターを設けるつもりだったのですが、Rubrikの担当の方から話を聞いて、考えを改めたのです」と宮崎氏は明かす。

その担当者から説明を受けるまで、宮崎氏はRubrikに関する知識をほとんど持っていなかった。話を聞いて強く興味を持ったのは、Rubrikがランサムウェア対策を念頭に置いて開発を重ねているバックアップソリューションだということだった。

「『ランサムウェアによる攻撃があったかどうか』さらに、『いつ攻撃を受けたのか』といったことを可視化できるソリューションだと聞いて、正直、驚きました。他のバックアップソリューションで、そこまでの機能を持つものは見たことがありませんでしたし、仮にそれが実現できるのなら、どのタイミングまで戻れば安全なデータが利用できるのかが分かり、業務の早期復旧が可能になるからです」（宮崎氏）

使える状態のデータを速やかに戻せる数少ないソリューションと高く評価

宮崎氏がRubrikを評価したポイントは、他にもいくつかある。

1つは、サイバー攻撃によって壊されにくい独自のOSを採用していること。他のバックアップ製品は、WindowsやLinuxなどの汎用OS上で動くものが多く、OSがランサムウェアに感染して壊されると、バックアップシステムそのものが動かなくなってしまう恐れがある。その点、Rubrikは独自のOS上で動くので、システムが影響を受ける可能性は極めて低く、復旧に支障を来す心配は少ない。

またRubrikには、一度バックアップデータを取得すると、物理的に変更・削除できないようにする改ざん防止（イミュータブル）機能も備わっている。

さらに、バックアップの設定を変更する場合、管理者だけでなく承認者による2段階の承認が必要とされ、両方のアカウントを奪わないと攻撃できない仕掛けになっていることなども、宮崎氏は高く評価した。

「ランサムウェア対策を念頭に置いているというだけあって、非常によく考えられたバックアップソリューションだと思いました。PoCをしてみたところ、UIも非常に優れていて使いやすかったので、採用を決定しました」と宮崎氏は語る。

SBSホールディングスが貫く「物流を止めない」覚悟

手始めに、オンプレミスで運用している仮想基盤のバックアップ／リカバリー用として24年に採用。同社はこのほか、仮想基盤とクライアントPCのネットワークを分離して外部からの侵入が仮想基盤に及ばないようにするランサムウェア対策も講じているが、Rubrikは、万が一、それをすり抜けられた場合の“保険”として運用している。

「仮に侵入されてデータが“人質”に取られても、3日以内にデータを復旧させるという目標を定めています。Rubrikがあれば実現不可能な目標ではないと信頼しており、『倒産リスク』を最小化できる頼もしい“保険”が手に入ったと思っています」（宮崎氏）

その後、SBSホールディングスは、26年2月にファイルサーバーのバックアップ用、同年6月にはMicrosoft 365のSharePointのバックアップ用としてRubrikを採用。さらにActive Directoryのバックアップ用としても導入準備を進めている。

「ランサムウェア被害の95％以上は、ローカルのActive Directoryを狙ったもの、または経由したものなので、そのバックアップ／リカバリーをいかにしっかり行えるかは非常に重要です。今後も、あらゆる方面でRubrikの活用を検討していきたい」と宮崎氏は語る。

AIを活用したサイバー攻撃の高度化、巧妙化によって、もはや防御策を講じるだけではランサムウェア攻撃による「倒産リスク」の回避は困難になっている。

最後に宮崎氏は、「業務を早期復旧させるには、“使える状態”のデータを速やかに戻せる仕組みを採用するのが有効です。Rubrikは、それを実現できる数少ないソリューションであり、『倒産リスク』を回避するという観点では、防御をさらに積み増すよりも投資対効果の高い選択肢だと言えそうです」と高く評価した。

rubrik

https://www.rubrik.com/ja