サイバーセキュリティ最前線

「コンティニューエンジン」を活用し巨大災害の時代の障害対策に備える!!

今号の第2特集で紹介した通り、能登半島地震の復興は遅々としてすすまず、依然として課題が山積している。その影響はITなどの分野にもおよんでおり、多くの通信キャリアやデータセンターが甚大な被害をこうむった。そこで、今号ではその状況を概観しつつ、巨大災害にかぎらず発生する障害への対策を紹介したい。

能登半島地震で顕在化した多様な阻害要因

2024年1月に発生した能登半島地震では、もともと災害対策に力を入れてきた通信キャリアすら被害を免れることができなかった。事実、NTTドコモ、KDDI、ソフトバンクといった主要キャリアも震災による交通遮断や積雪によって復旧が思うようにすすまない状況に陥ったという。また、データセンターのなかには物理的な被害を免れ、事業継続計画（BCP）にもとづいた点検リスト共有や訓練といった備えを活用した例もみられたが、一方で大渋滞によるスタッフ不足など、想定外の課題が顕在化した。

この震災はコンピューターシステムの稼働確保を見直す大きなキッカケになったが、実は震災以外でも思いがけない障害が発生するケースは多々ある。たとえば、24年7月19日には米国のクラウドストライク社製のセキュリティ製品がオンラインでの更新時に不具合を起こし、世界中で850万台のWindows機器に障害をおよぼした。しかも調査が難航し、修正策が公表されるまでに3日を要したという。更新プログラムに不具合が起きた例はここ最近頻出しており、マイクロソフトのWindows Serverの更新でも障害を招く不具合が発生している。

旧式の障害対策から脱却し「コンティニューエンジン」に

コンピューターシステムを継続稼働できなくなるケースはほかにもある。ハードウェア機器の故障、プログラム自体のバグ、データを暗号化してしまうランサムウェア（身代金要求型ウイルス）などのサイバー攻撃、さらにはネットワーク障害など、要因は多岐にわたる。

では、こうした障害対策にはどのような措置がとられているのか。その点について、長年にわたってITセキュリティに取り組む㈱ブロード（東京都千代田区）は「障害対策といえば、古くからあるバックアップをとる方法がある。ところが、この方法だとバックアップをとった時点にしか戻せないし、かつ複雑なシステムの場合はすぐに再稼働させることができない」と指摘する。

もちろん、そのほかにも予備のコンピュータを用意して常時「同期」しておき、いざというときに切り替える方法などもある。だが、「自動切り替えの場合、ハードウェアやWindowsなどのOSレベルの異常しか検知せず、実際にユーザーが使用するアプリケーションが停止しても反応してくれないことが一般的だ」という。さらに、こうした仕組みは事前に意図した動作になることを検証する必要があるため、なかなか導入するのが難しい。しかも、設計や組み込みに時間を要するといった難点もある。

こうした状況にあって、ブロードがイチオシするのが、本コーナーの2023年10月号で紹介したNeverfail社の「コンティニューエンジン」だ。このソリューションを活用すれば「すでに稼働中のシステムであっても、シンプルな手順で組み込むことができるし、有事の場合も数分単位で自動切り替えが完了する」とブロードは説明する。まさに停止が許されないシステムにとって、心強い味方といえるソリューション、巨大災害の時代の障害対策として検討してみてはどうだろうか。