STRATEGIC BUSINESS INSIGHTS

scan

2021 年 5 月

SoC1228

Growing Demand for Resilience

By Susan Leiby（Send us feedback）

レジリエンスの需要が増大

レジリエンス（回復力）の高いシステムの必要性が、政府機関、企業、個人にとって重要な意思決定要因になりつつある。厳しい気象条件、パンデミック、経済恐慌、テクノロジーの変化、サイバー攻撃など、多種多様な「予期せぬ」事象の発生によって、複雑なシステムが設計上の想定をはるかに超える混乱に陥り、壊滅的な機能停止につながる場合がある。グローバル経済の基盤となっている主要なインフラ・システムに関しては、レジリエンスの必要性はとりわけ明白である。このようなインフラ・システムは電力および燃料グリッド、交通運輸、廃棄物処理、通信、水道システムだけでなく、新興のモノのインターネット（IoT）ネットワークや、住宅・医療などの社会的基盤も含まれる。リスク要因の増大に応じて、重要システムの信頼性を確保するための対策をステークホルダーが講じなければならない。冗長性の確保やサプライチェーンの多角化などの対策を講じることで、短期的に不利益が生じるとしてもである。

リスク要因の増大に応じて、重要システムの信頼性を確保するための対策をステークホルダーが講じなければならない。

暴風雨、記録的な猛暑や寒波、干ばつ、山火事など、気候に関連する事象が世界各地で頻発するようになった。最近のテキサス州電力危機は、こうした事象を乗り切るための、相互接続されたインフラを整備する必要性をまざまざと見せつけた事例である。2021 年 2 月、テキサス州を激しい吹雪と寒波が襲い、同州の電力グリッドの相当な部分が機能停止に陥り、大規模な停電が起こるとともに、道路および鉄道網、上水道システム 、およびその他のシステムの障害が連鎖的に広がった。この停電とシステム障害により、数日間にわたって数百万人が影響を被った。テキサス州知事は、風力タービンと太陽光発電パネルの凍結が停電の原因だとして非難したが、その後、天然ガス発電所の不十分な寒波対策が第一の原因だったことが専門家によって明らかになった。同州の孤絶したグリッド設計も、不足した電力を近隣の州から補填する妨げとなった。テキサス州危機の注目すべき側面として、連邦規制当局は以前、異常気象の発生確率が高まっている現状から、地方政府および公益企業に対し、エネルギー・システムを堅牢化するよう警告を発していた。しかしながら、役人たちはコスト等の問題を理由に対策を講じていなかった。この無為無策は、対策を講じた場合のコストよりもはるかに高くついたと考えられる。大規模停電による経済的損失の総額を査定するのは難しいが、米国 Perryman Group の試算によると、テキサス大寒波の損害は最大 2,000 億ドルに達する見通しである。

現代経済の心臓部で電力の重要性がますます高まっている。米国のバイデン大統領が打ち出した 2 兆 2,500 億ドル規模のインフラ改造計画は、老朽化して信頼性が低下した米国の電力グリッドに気候耐性を持たせることを主眼とするものである。バイデン・プランには、グリッドの脱炭素化、効率化、最新化を迅速に進める狙いがある。多くの企業や自治体が、自分たちで消費する電力の信頼性を高め、停電時におけるエネルギーの自給自足を可能にする目的で、電池システムや太陽光発電を含む分散型マイクログリッドなどのソリューションを導入している。インフラ障害への対応に役立つ製品に対する消費者の需要も増大している。テキサス州危機の最中には、EV 車、屋上ソーラー・システム、家庭用予備バッテリー、あるいはピックアップ・トラックに備え付けのガス発電機を所有する多くの人が、各家庭で電力と暖房を手に入れるうえでこれらのシステムがどのように役立ったか、ソーシャル・メディアで盛んにレポートしていた。

Covid-19 パンデミックはグローバル経済に激震を走らせ、戦略的レジリエンスの必要性を浮き彫りにした。たとえば企業は、競争力を損なわずにサプライチェーンの弱点やリスクを減らすにはどうすればいいか、

という難題に直面している。この分野では、複数の参加企業がサプライチェーン・マネジメントを 1 つのプラットフォームで一元化する、マルチパーティ・ネットワーク・プラットフォームの人気が上昇している。企業中心型のサプライチェーン管理テクノロジーとは対照的に、ネットワーク・プラットフォームでは、参加企業が接続先のサプライチェーンに関するリアルタイム情報にアクセスし、素早く調整を行うことができるので、従来よりはるかに高いスピードと精度が約束される。このようなシステムでは、需要と供給の動的なマッチングや、自動的な調達など、かつてないレベルの最適化が可能である。ただし、こうした効率化には代償が伴う。サプライチェーンの機能停止に対する物理的な緩衝作用が失われることで、新たなレベルのサプライチェーン脆弱性が引き起こされる可能性がある。

さまざまな産業で必需品となった特殊なコンピューター・チップも、パンデミックの到来とともに世界的な供給不足に陥っている。2020 年前半、パンデミックによって海外への渡航や交易がほとんど途絶したため、自動車メーカー各社は自動車販売の低迷が長期化することを予測し、チップの発注量を晴らした。予想に反して消費者の自動車需要はすぐに回復したが、世界の半導体業界はすでに、自動車メーカー以外のバイヤーにチップを多く販売する態勢を整えていた。パンデミック中に消費者がインターネット・サービス用に依存度を高めた、サーバーやパーソナル・コンピューターなどの通信機器で使われるチップの需要を主に満たすためである。半導体の製造には大量の清浄水が必要だが、台湾の深刻な水不足によって、チップの供給はさらに逼迫している。最新世代のチップを大量に製造する能力のある台湾のチップ・メーカーは、グローバル・サプライチェーンにとって特に重要な存在だ。グローバル自動車メーカーの多くが、最新型の自動車に必要なコンピューター・チップが入手できないことを理由に、工場を一時閉鎖したり、生産量を減らしたりしている。チップをめぐる熾烈な競争は今後何年も続く可能性があり、すでに世界中でビジネスや政策についての判断に影響を及ぼしている。

多くのシステムが接続性を獲得する一方で、レガシー・ソフトウェアの欠陥が研究者によって続々と発見され、増加傾向にあるもう1つのリスク要因がサイバーセキュリティ脆弱性である。逆説的にも、多くの設計者が重要インフラのレジリエンスを高める目的で IoT ネットワークをインフラに組み込んでいるが、複数のシステムを安全かつ最新の状態に保つのは至難の業である。米国 Forescout Technologies のサイバーセキュリティ研究者が最近、7 つのオープンソース TCP/IP（Transmission-Control-Protocol/Internet-Protocol）スタックで、33 個の脆弱性を発見した。TCP/IP スタックは、各種デバイスとインターネット等のネットワークとの間で接続を仲介するネットワーク通信プロトコルの集合体である。これらの脆弱性が原因で、何百万台もの IoT デバイスが攻撃にさらされる可能性がある。技術的な観点では、個々の脆弱性にはパッチを適用することで簡単に対応できるが、無秩序に広がった IoT デバイスのサプライチェーンの性質に加え、オープンソース・ソフトウェアが多用されている現状から、特定のデバイスが脆弱かどうかを判断するのは非常に難しい。エンドユーザーは自分のデバイスにリスクがあるかどうかの判断をサプライヤーに頼っているが、IoT デバイスのメーカーは、自社の IoT デバイスに組み込まれたサードパーティ製ハードウェアまたはソフトウェア・コンポーネントに脆弱なオープンソース・スタックが使われていても、おそらく気付かない。デバイスのサプライヤーが仮にそうした問題を発見しても、サードパーティ側が信頼性の高い方法でパッチを提供できるとは限らない。結果的に、多くの欠陥が是正されないまま放置されることになりかねない。

重要なシステムの障害が増え続けている現在、あらゆるレベルの顧客や政府機関がレジリエンスを重視する傾向を強めていく可能性がある。信頼性を確保するには、予測しにくい破壊的事象に対するシステムの脆弱性を継続的に評価する必要がある。レジリエンスを効果的に改善することで、起こり得る突然の事態をシステムが予測し、耐え抜き、適応し、そこから迅速に回復する能力が強化される。

SoC1228

本トピックスに関連する Signals of Change		**関連する Patterns**	
SoC1225	ハードウェアの検証という難題	P1596	気候変動への適応
SoC1154	コロナウイルス後の生活	P1591	感染症の拡散を予測する
SoC1147	気候変動が市場リスクを変える	P1586	気候変動リスクのマネジメント