反脆弱性のセキュリティシステム

反脆弱性の考え方

- ブラックスワンを予測することは無理
- 脆さはかなりのところまで測定できるが、リスクは測定できない
- 耐久力のあるものは衝撃に耐えるが、反脆弱性は衝撃を糧にする
- 失敗は学習を促し、創造性を高める

反脆弱性の例

- 炎上マーケティング
- 筋トレ負荷で強くなる身体
- 節水栽培で甘くなる野菜
- 木組みの五重塔
- 反社会的勢力デモ

堅牢な IT セキュリティを意図したシステムを構築する場合、誰しも過去のセキュリティ事故とかを参考に、あらゆるセキュリティリスクに対処できるような強靭なシステムをイメージして、様々なセキュリティ対策を施すことが多いです。
しかしながら、強靭なシステムを目指せば目指すほどセキュリティの投資は膨らみ、ユーザの利便性は損なわれていく場合が多く、その上対処すべきセキュリティリスク対策はつきません。
こうした状況に対して、参考になる考え方として、「反脆弱性（Antifragile）」という言葉が、アメリカの作家である Nassim Nicholas Taleb 氏の同名タイトルの著書に登場します。
脆弱（Fragile）の対義語は、頑強（Robust）という感じがしますが、脆弱性が「外圧によってパフォーマンス低下する性質」であれば、それに対置するのは「外圧によってかえってパフォーマンスが高まるような性質」なのではないかという考えによって、反脆弱性という言葉が使われています。
エラーや負荷によってかえって、システムが強靭になるということはなかなかイメージしにくいのですが、「脆弱に見えるけれども実は反脆弱なシステム」と「堅牢にみえるけれど実は脆弱なシステム」の例であればわかりやすいです。
たとえば、自転車とトラックであれば、後者の方が堅牢にみえます。しかしそれは、通常の運転を前提にしている場合で、地震で交通網がマヒした場合などでは、自転車の方がパフォーマンスを発揮できます。
Taleb 氏の著書で、ありえないような事象が発生すると、非常に強い衝撃を与えることを「ブラック・スワン」という言葉で表しています。これは白鳥は白いと思われていたのに、黒鳥が発見され衝撃を与えたことに由来するようですが、そうしたありえない事象は、予測したり、リスクを計算したりすることは無理だというブラック・スワン問題があり、危うさを測ることがこの問題の解決策になるとのことです。
IT セキュリティを構築する場合においても、システムに対してどのような事象が発生して、どのようなリスクが生じるのかを予測することはとても難しいです。それに対して、システムが危ういかどうかを見分ける方がずっと楽だという考え方です。
必ずしも当てはまる環境ばかりではないと思われますが、危うさは測れるけれど、リスクは測れないという考え方をもとにして、セキュリティシステムを見直してみるのもいかがでしょうか？