セキュリティ対策をムダにしないために

セキュリティシステムの注意点

現場の利便性を維持できるか？
最新技術や事例を調査して検討できているか？
投資に対するリスクヘッジの効果があるか？

総務省が 2017 年度から約 18 億円をかけて導入した、サイバー攻撃対策としてインターネットから遮断されたうえで、強固なセキュリティ対策が施されている「セキュアゾーン」というシステムが、一度も使用されないまま 2019 年 3 月に廃止されていました。
もともと 2015 年に日本年金機構から基礎年金番号などの個人情報約 125 万件が流出したサイバー攻撃を受けて導入が決まったものの、使い勝手の悪さやコスト面から各府省庁が使用を見合わせたことと、会計検査院の調査を受け、今後も利用の見込みがないことや、年間 3 億 6 千万円程度の維持・管理費がかかることから、廃止したとのことです。
セキュアゾーンの高度なセキュリティーは、各府省庁は専用回線で機密情報を閲覧できるが、ダウンロードはできない仕組みだったようで使い勝手が悪く、保管されたデータの出し入れや訂正には、各府省庁の職員が設置場所まで足を運ぶ必要があり、使用にあたっては負担金が生じる可能性もあったとのことで、そもそも、計画段階から利用を希望していなかったようです。
こうしたことは、お役所仕事にありがちな内容で責任の所在が不明瞭ですが、このようなムダな投資を許していたら、業者に対する単なる利益供与と疑われても仕方ありません。
このセキュリティシステムは、私たちのセキュリティ投資に関して考えさせられる重要な事例です。
セキュリティ強化は、業務の効率化とは真逆で、その多くは使い勝手を悪くし、チェックの負荷や場合によってはこの例のように手間を増やすものになります。それでも、行うべきなのがリスク回避のためのセキュリティ対策です。
今回は、各府省庁がハードウェアなどを共通で整備・運用する「政府共通プラットフォーム」の中に置かれていたとのことですが、果たしてセキュアゾーンの設置が最良の策だったのでしょうか？もし、そうであれば強制的にでも使わせるべきだったのではないでしょうか？このあたり、企業であれば、使用される見込みがないセキュリティシステムは絶対作らないでしょう。詳細がわからないので、判断はできませんが、インターネット遮断の方法も日進月歩で、様々な方法があります。閲覧だけでダウンロードできない仕組みにこんなに投資することが必要だったのでしょうか？
セキュリティ対策を施したシステムの作成には、現場とのコンセンサスと、最新技術を入手した上での投資対効果の算定が、特に重要です。