中小企業 と サイバーセキュリティ

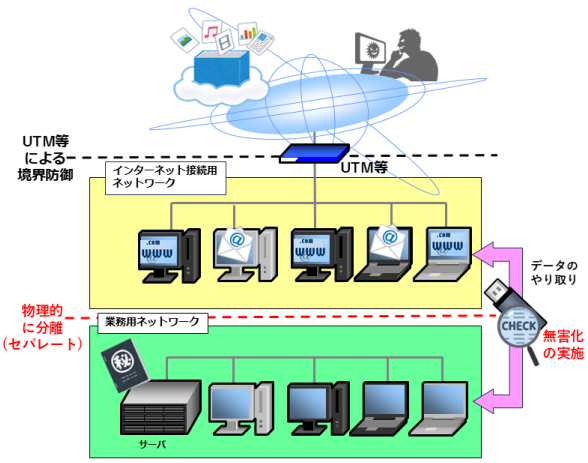
第2回 お手軽サイバー防犯対策①
「セパレート大作戦！！」

「サイバーセキュリティは利益にならない負の投資」と思われがちですが、費用を抑えて手軽に取り組めるサイバー防犯対策があったらどうでしょうか？

今回は「お手軽サイバー防犯対策」の第一弾として、ネットワーク分離によるリスク低減策「セパレート大作戦！！」をご紹介します。

ネットワーク分離（セパレート）とは、社内ネットワークを複数の独立したネットワークに分けて管理する手法です。

これにより、万が一、一つのネットワークが攻撃を受けても、他のネットワークへの影響を最小限に抑えることができます。



特にテレワークの普及に伴い、ネットワーク分離の重要性が高まっています。

ネットワーク分離の簡単な例としては、メールやWeb閲覧などのウイルス感染のリスクのあるインターネットを使う作業と業務処理を１台のパソコンで行うのではなく、インターネット用と業務用に別々のパソコンを用意した上で、それぞれをインターネット接続用システムと業務用システムとして物理的にネットワーク分離するというものです。　これによりウイルス感染や外部からの攻撃が業務に直接影響を与えるリスクを減らせます。

但し、物理的に分離した２つのシステム間でデータのやり取りを行う時にはウイルスチェック等の手間をかけて「無害化」する必要があります。
また、「業務上、物理的分離が難しい」場合は、ネットワーク間のデータ通信時の無害化と、「何も信頼しない厳格なアクセス制限（※注）」も必要です。

まずはコストをかけずに手間をかけて「セパレート大作戦！！」を実施し、その後、手間を省くために適切なセキュリティ製品等を導入する、つまり「**サイバー防犯対策のDX化**」を図ってみてはどうでしょうか？

※注　内部ネットワークも外部と同じように全てのアクセスを検証し、権限のあるユーザーやデバイスのみがアクセスできるようにする「ゼロトラスト」と呼ばれる考え方のことです。

神奈川県警察サイバーセキュリティ対策本部

※ この記事は川崎市産業振興財団機関紙「産業情報かわさき（2025年2月号）」に掲載されたコラムを再編集したものです。