ネットワークシステムの可視化

可視化してセキュリティポリシーを展開し セキュリティ運用を自動化・効率化する

セキュリティポリシーを策定しているが、それが有効に機能しているか、現状の自社ネットワークとどのようなギャップがあるか、を可視化できている日本企業は少ない。しかし、このネットワークの可視化は、セキュリティ運用の自動化・効率化やサイバー攻撃を受けた際の迅速な復旧を可能にするものであり、特にケーブルテレビ・放送局などのインフラ事業者には必須だ。（本誌編集部）

内田正文
NTT Com DD株式会社
GTM本部 副本部長
パートナー営業部 部長

自社ネットワークシステムの ルールと通信経路を把握する

現在、企業にコーポレートガバナンスとして透明性が求められている。この透明性をネットワークシステムにおいても実現できている企業がどの程度あるだろうか。多くの企業は、ネットワークシステムの透明性とは何か、という問いを持っている。

ネットワークの透明性とは可視化である。このネットワークシステムの可視化を解決することなく、今、多くのネットワークシステムに求められている自動化、効率化を実現することはできない。

では、ネットワークシステムの可視化とはどういうものなのか。それは、「自社のネットワークシステムの通信経路ルールと通信経路をいつでも提示できること」である。

当然、ネットワークシステム管理運用担当者は自社のネットワークシステムの通信経路ルールと通信経路を把握しているが、経営層も瞬時に答えられるだろうか。ある海外のセキュリティベンダーと話した際に、海外では経営層が自社ネットワークのコンプライアンス状況を常に把握している、と言っていたのは驚きであった。海外では当たり前のことなのである。

可視化の観点は「誰と誰が通信可能か」 「通信できるアプリケーションは何か」

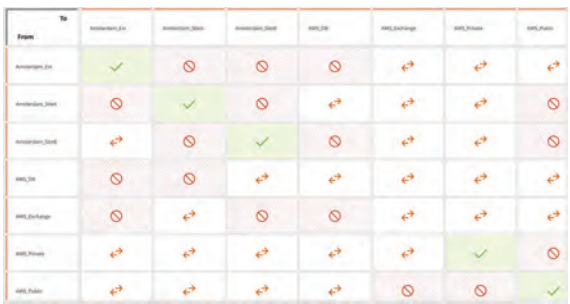
セキュリティインシデントが発生した際に、被害の状況と範囲をすぐさま報告することで、企業としての情報セキュリティポリシーを正しく運用していると証明できる。しかし、多くの日本企業では被害に遭った際、被害の状況と範囲を把握できないため、復旧にどれだけ時間を要するのかさえもわからないのが現状ではないだろうか。この状況が、一般の民間企業ではない、医療機関などの公共施設でも多々発生している。

では、この可視化をどのように行えばよいのか。それは、「誰と誰が通信可能か？」と「通信できるアプリケーションは何か？」という観点でファイアウォールの管理を見直すことで、先述したような通信経路ルールと通信経路を明示できるようにすることである（**図1・2**）。

セキュリティポリシーの一元管理で 大きな運用効率が得られる

これにより、セキュリティポリシーと現状のギャップも明確になる。さらにセキュリティポリシーを

【図1】 理想的と思われる通信経路のルールマトリックス図



【図2】 理想的と思われる通信経路図