テレワーク時代のインシデント対策 ～境界型セキュリティから ゼロトラストセキュリティへ～

株式会社ディアイティ
JNSA 理事　青嶋　信仁

テレワークによる業務環境が一気に進みだしたその変化の結果として通信経路が多様化する中、従来、セキュリティ対策の考えで主流であった境界型セキュリティの限界を迎え、通信経路の守りが十分ではないことを前提としたゼロトラストセキュリティへの移行が注目されています。

従来、業務で取り扱われる情報は、境界に置かれたゲートウエイ製品などによるセキュリティ対策を主体に行われており、エンドポイント側ではウイルス対策ソフトレベルで補完的に守られているという状況でした。境界が分散して多様化する環境においては、エンドポイントでの自立した単独でのセキュリティ対策が必要になり、従来の教科書や試験にもできたような境界型を基本としたセキュリティ対策の考え方の変更が求められる時期が来たといえます。

このような変化において、表立って議論されることは少ないものの非常に影響が大きいのが、テレワーク環境における分散したエンドポイントに対するインシデント対応です。インシデント対応をフェーズ毎でみていくと、「検知」段階においては、従来の境界におかれた検知機能が必ずしも有効に働かず、個々のエンドポイントの機能に依存する問題があります。また、「受付/トリアージ」の段階においては、一般社員と同じようにテレワーク環境に置かれたシステム管理者やCSIRTに対して必要な通知や報告が届くのか、コミュニケーションの連携に支障がないかが問題になります。さらに「インシデントレスポンス」段階では、コンピュータフォレンジックを行わないと解決できない場面において、テレワーク環境にある解析対象機器から必要なデータや各種情報をすぐに入手できないことも想定しておかなければなりません。併せて、解析対象機器の回収と代替機提供といった物流の問題も考えておかなければなりません。これらの問題は従来のインシデントレスポンスに比べて対処の遅れと被害の拡大を招きます。このような問題に対する解決策としてEDR（Endpoint Detection and Response）などのインシデント対応を考慮したエンドポイント製品が注目を集めています。EDRは、その機能から初期対応への効果が高く、従来製品が苦手であった大量のエンドポイント機器への監視やインシデント対応が可能となるなど、状況によっては従来より素早い対応が期待できるレベルになっており、日本でも導入が進み実績を積んでいるところです。

日本のセキュリティ対策は、欧米から常に4，5年は遅れていると言われていますが、世界で一斉にテレワーク環境が利用されるようになっている状況にある今、この機会に弾みをつけて一気に進化してほしいと期待しています。