5G時代に重視すべきセキュリティーオーケストレーションとは

～高度セキュリティーを自動化するSOAR（ソアー）～

インターネットに接続されるデバイスが急増すると同時に、セキュリティー対策も日々進化しています。
特に、まもなく訪れる5G時代においては、IoTの普及がより加速し、セキュリティー対策や考え方も、より進化していくでしょう。
5Gの特徴ともいえる通信速度の高速化と多数同時接続、超低遅延が、今、セキュリティーの考え方に革新的な変化をもたらそうとしているのです。

5G時代がIoTの普及を加速する

日本では2020年から5Gのサービスが正式に開始される予定です。

5Gは現行の4GLTEに比較すると、同時に接続できる端末の数が100倍以上になり、データ通信の遅延もほぼなくなると言われています。そのため、物流管理や工場のオートメーション、自動運転自動車、遠隔治療など、広範囲にわたって活用されることが見込まれています。

このことは同時に、セキュリティー対策も広範囲になることを示しています。

実はこうしたIoT機器へのセキュリティー攻撃の割合は既に大きくなっています。

国立研究開発法人の情報通信研究機構（NICT）の発表によると、2017年にNICTER（Network Incident analysis Center for Tactical Emergency Response）が観測したポート別の攻撃対象では、54.7％と半数以上がIoT機器となっています。（NICTER観測レポート2017の公開 ¦ NICT-情報通信研究機構）

この傾向は今後も進むことが予想されます。たとえば総務省がIHS Technologyから引用した数値では、2017年に274.9億台であった世界のIoTデバイスは、2020年には403億台になると予測しています。（『総務省 | 平成30年版 情報通信白書 | IoTデバイスの急速な普及』）

そのため、5G時代を見据えたセキュリティー対策「セキュリティーオーケストレーション（Security Orchestration, Automation And Response：SOAR）」という考え方が注目されています。

SOARが実現すること

SOARとは、米国の調査会社Gartner社が提唱する概念で、さまざまなIOT機器から収集した脅威情報のビッグデータを一つのプラットフォームに集約し、人工知能（AI）や機械学習により高速かつ自動的に分析して意思決定を行う技術です。

そのためSOARは、5G時代に大規模化する通信システムのセキュリティー管理に有効であると期待されています。

5G時代に重視すべきセキュリティーオーケストレーションとは

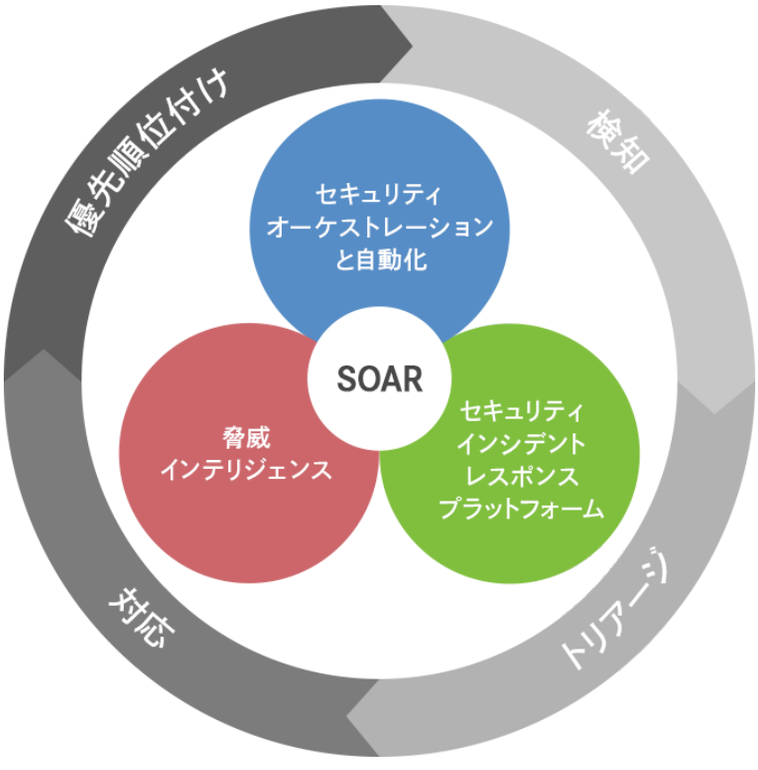

図:SOARの概念

SOARを導入することで、以下のようなメリットがあります。

●インシデントへの自動対処

想定されるインシデントごとに対応手順をワークフローとして組み込んでおくことで、インシデントへの対応を自動化することができます。このことで、セキュリティー担当者は手作業を軽減でき、より高度な分析作業などに注力することができます。

●インシデント情報の共有

SOARはインシデント情報の関係者間での共有を自動化します。このことで、担当者が関係者にいちいち手動でメール連絡したり電話連絡したりする手間が省け、連絡ミスも防げます。

●インシデント対処が自動的に記録される

SOARのプラットフォーム上にはインシデントへの対処が自動的に記録されます。そのため、後で確認することが容易であり、全ての対応が証拠として残されます。

●セキュリティー運用チームの品質を高められる

SOARにはセキュリティー運用チームのパフォーマンスを測定する機能があるため、作業分担の状況や各人の作業効率などを自動的に集計して可視化できます。これにより、運用チームのボトルネックを特定して改善策を立てるために役立てることができます。

5G時代のセキュリティー対策

SOARは大規模なネットワークのセキュリティーを、AIと機械学習により自動化することができるため、通信速度の高速化と接続デバイスが大規模化される5G時代のセキュリティー対策に大変有効であると期待できます。

また、SOARにより、高度セキュリティー人材の不足を補うことができ、人的資源をより高度な専門性を必要とする業務に配分することも可能になります。

5G時代の到来に向けて、セキュリティー対策の強化を検討する際には、SOARの導入を検討する動きも増えてくるでしょう。

【 制作／ブレイン 】

NTTコムウェア株式会社
URL：https://www.nttcom.co.jp/
WEB 掲載：2020.01