日本アイ・ビー・エム

深刻化するセキュリティー人材不足 変革への道筋を「Watson」が指し示す

多くの企業でセキュリティー担当部門は負荷の増大と人材不足の板挟みになっている。こうした課題に対して抜本的な解決アプローチを示すのが、セキュリティー分野に特化したコグニティブシステム「Watson for Cyber Security」である。インシデント対応をはじめとするセキュリティー業務において、インテリジェンスとスピード、正確性を高めるソリューションへの期待は大きい。

日本アイ・ビー・エム
IBMセキュリティー事業本部
セキュリティー・インテリジェンス営業部
テクニカルセールス
丸茂 武彦 氏

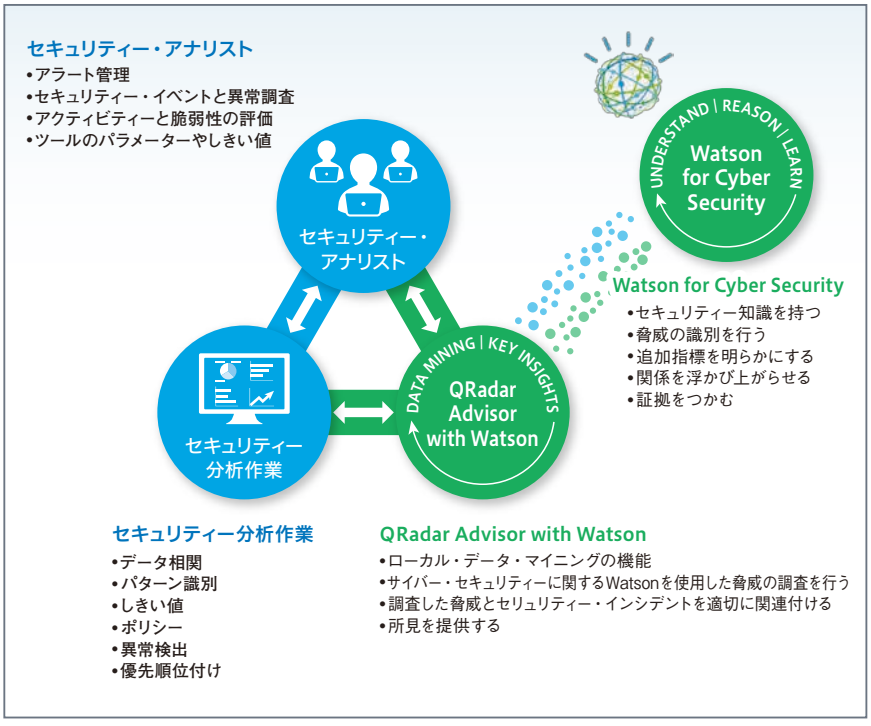
サイバー攻撃の脅威が増大する中で、セキュリティー人材の負荷は高まるばかりだ。セキュリティーを担う部門からは悲鳴にも似た声が聞こえてくる。日本IBMの丸茂武彦氏は、課題の背景にある3つの要因を指摘する。

第1はセキュリティーデータの増大である。企業内のデバイスが増え続け、それに呼応してセキュリティー機器が次々に導入されている。このため、インシデント発生時、分析すべきデータは急増している。

2番目はインテリジェンスの不足または欠如の問題だ。サイバー攻撃を受けたとき、適切な情報をタイムリーに取得できれば、攻撃を阻止したり、被害を最小限に食い止めることができる。しかし、インテリジェンスを得られないために被害の拡大を許してしまうケースは少なくない。インテリジェンスを提供する仕組みを整えていなかったり、仕組みは持っていてもアナリストが使いこなしていない企業が少なくないという。

3番目の要因は人材のスキルギャップである。「日本では以前からセキュリティー人材の不足が叫ばれていますが、残念ながら改善が進んでいるとはいえません。人材の教育も追いついておらず、スキルギャップが生まれています」（丸茂氏）。

図1 QRadar Advisor with Watsonがセキュリティー・アナリストの活用をサポート



セキュリティー人材の質と量の課題に対し、日本IBMは2016年12月、パソナとの協業でセキュリティー人材を育成するプログラム「Cyber Security Intelligence Academy」を開始した。こうした地道な活動の一方で、テクノロジーを活用した解決策への期待も高まっている。同社が提供しているソリューションの1つが、「コグニティブ・セキュリティー」である。

「壁」による防御から学習を基にした対処へ進化

企業のセキュリティー対策は、サイバー環境の変化に呼応して進化を続けてきた。2005年ごろまではファイアウォールやウイルス対策ソフトなどを用いて「壁」を作り、外部からの攻撃を防ぐ手法が主流だった。その後、ログなどリア

ルタイムデータを収集・分析し、イベントに優先順位をつけてリスクの高い脅威を検出、対処する手法が広がった。

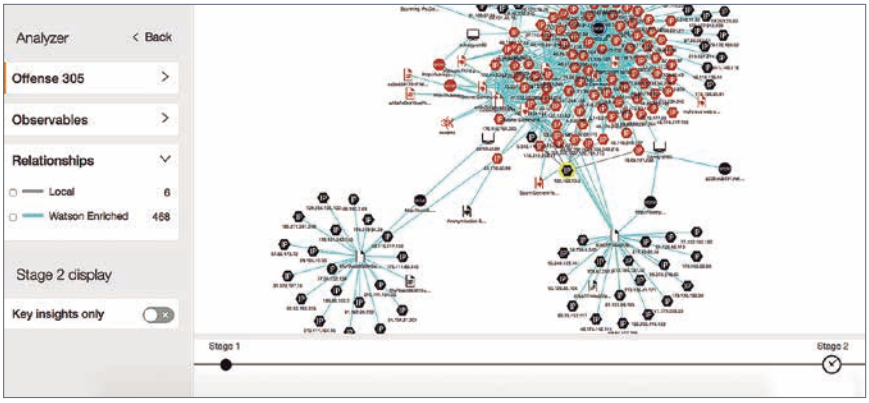
現在では、新たにコグニティブ・セキュリティーが現実的な選択肢として注目を集めている。セキュリティーに関する膨大な情報を学習しながら、目の前の脅威への対策を実行する。コグニティブテクノロジーの発展が、こうした手法を実現した。

「2016年に全世界700人のCISO（情報セキュリティー最高責任者）を対象とした調査を実施したところ、回答者の3分の2が、前述のスキルギャップを埋めてくれる技術としてコグニティブ・セキュリティーへの期待を示していました。また、コグニティブ・セキュリティーのメリットとして、多くの人が『インテリジェンス』『スピード』『正確性』を挙げていました」（丸茂氏）。

コグニティブ・セキュリティーという新しい世界への先導役を担う日本IBMのソリューションが、「Watson for Cyber Security」と「IBM QRadar Advisor with Watson」だ。

「今年2月に市販を開始したWatson for Cyber Securityの開発段階では、Watsonに基礎からセキュリティーの知識を与え、膨大なコーパス（全集）を持つまでに育てました。コーパスには脅威データベースや調査レポート、セキュリティー教本、脆弱性報告などが含まれており、現在も継続的に成長しています。人間なら見逃してしまう経路、関連性を見いだし、それを記録して次の発見につなげます」と丸茂氏は言う。

図2 コグニティブ・セキュリティーにより、複雑な攻撃の解析も可能に



「数日から数週間」を「数分から数時間」に短縮

一方のIBM QRadar Advisor with Watsonは、Watsonの持つ膨大なセキュリティー知識を活用し、セキュリティー分析プラットフォーム「IBM QRadar」が収集したインシデントデータを分析できる。アナリストに代わってインシデントの調査・検証を行うとともに、インシデントに関する洞察を生み出す。また、アナリストのスキル不足、インシデント対応の遅れなどの課題を洗い出し、改善を促すことも可能だ。このアプリケーションは、IBM QRadarのユーザーであれば30日間の無償利用が可能で、最新版を自由に試用できる。

IBM QRadar Advisor with Watsonの特長について丸茂氏は、アナリストによる分析時間が大幅に短縮されることを挙げる。「従来型のオペレーションでは、インシデントの仕分けから調査・影響評価、対応までに数日から数週間かかっていました。IBM QRadar Advisor with Watsonを活用すれば、数分から数時間で完了します。ベータ版を提供したお客様の実績では、50分間かかっていた分析が10分間に短縮されました」（丸茂氏）。

時間短縮の一方で、問題のあるIPやマルウエアの関係性など、分析によって得られるフィードバックは豊富だという。ベータ版を利用した企業によると、アナリストが従来型の方法で5つの知見を得たのに対して、IBM QRadar Advisor with Watsonは同一のインシデントに対し、50の知見を提示したという。

セキュリティーに特化したWatsonは、セキュリティー対策を大きく変えようとしている。サイバー攻撃の実態を可視化でき、これまでの分析方法では追うことが事実上、不可能だった攻撃ルートや、各要素の関係性を分かりやすく表示することができる。丸茂氏は、セキュリティー人材不足に悩む企業にとって、コグニティブ・セキュリティーのもたらす価値は少なくないと強調して講演を終えた。