NTTアドバンステクノロジ　セキュリティ診断サービス

クラウド環境やWeb・社内システムの弱点を発見 進化し続けるNTT-ATのセキュリティ診断サービス

DX（デジタルトランスフォーメーション）の取り組みにより、多くの企業・団体がWebシステムやクラウドサービスを利用し、事業や業務の改革を推進しています。その一方で、標的型サイバー攻撃やサプライチェーンへのリスクなど、サイバーセキュリティの脅威も今まで以上に高まってきています。
NTTアドバンステクノロジ（以下、NTT-AT）では、NTTグループを支えるセキュリティエンジニアの豊富な経験と、グローバルベンダーの技術や製品を組合せることにより、幅広く柔軟なセキュリティソリューションを提供しています。
今回は、セキュリティ診断に関する4つのサービスを紹介します。

AWS利用ユーザーの課題に応える「クラウドセキュリティ設定診断サービス」

NTT-ATのセキュリティ事業本部では、セキュリティコンサルティングや教育、組織内CSIRT（コンピュータセキュリティ事故に対応するチーム）の運用支援、UTM（統合脅威管理）やDDoS（分散型サービス拒否攻撃）対策などのソリューションの提供に加え、監視・運用やインシデント対応まで、広範囲なセキュリティソリューションを展開しています。

そのなかでもセキュリティ診断サービスは、1999年から開始しており、時代に応じて新たな脅威に対応し、2022年3月末現在、1000社以上（約72000台の端末）の診断実績があります。2022年9月にはAmazon Web Services（以下、AWS）の環境の脆弱性を診断する「クラウドセキュリティ設定診断サービス」を開始しました。

ここ数年クラウドサービスの普及が進んでおり、AWSはその先駆者として多くの利用者に支持されています。いつでも必要なだけITリソースを活用できるクラウドサービスは便利ですが、セキュリティに関しては、利用者とAWSなどのクラウド事業者がその責任を共有して双方でセキュリティ確保を行う必要があり、利用者側にも適切な設定管理が求められています。

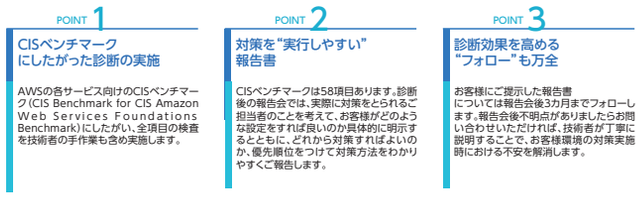

図1　クラウドセキュリティ設定診断サービスのポイント

NTT-ATはAWS Partner Network ADVANCEDの認定を受けており、有資格者が100名以上、上位資格保持者も数十名が在籍し、高度なセキュリティ資格を持つ人材を有しています。クラウドセキュリティ設定診断サービスはスタートしたばかりのサービスですが、すでにお客様に利用いただいております。あるお客様においては、セキュリティ設定のうち約7割に不備が見つかりました。この診断サービスでは不適切な設定について、具体的な対策方法を報告書にまとめて提示します。お客様からは「どのように対策すればいいか方向性をつかめた」「報告の説明がていねいでわかりやすい」といった評価をいただいています。

Webシステムを守る「プラットフォームセキュリティ診断サービス」と「Webセキュリティ診断サービス」

NTT-ATのセキュリティ診断サービスのうち、最も長く提供しているのが、1999年から提供している「プラットフォームセキュリティ診断サービス」です。これは、Webシステムが動作する、サーバーやOS、ミドルウェア層についてのセキュリティを診断するサービスです。ネットワーク越しに想定されるサイバー疑似攻撃を実施してリスクを分析・洗い出し、対処法を報告書にまとめます。このサービスでも「説明がわかりやすい」、「リスクの高い脆弱性を把握することができた」や「レポートに記載されたログなどの証跡が確認する際に役立つ」といった評価を得ています。

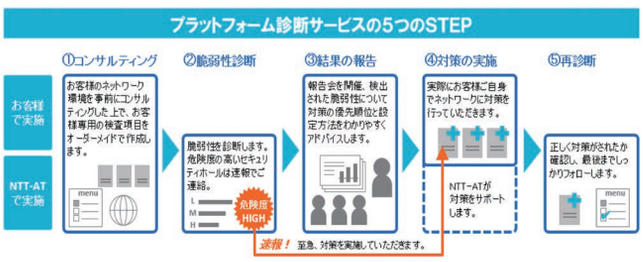

図2　プラットフォームセキュリティ診断サービスの流れ

Web ブラウザからアクセスできるアプリケーション層に対して診断するのが「Web セキュリティ診断サービス」です。独自ツールや市販ツールに加え、高度セキュリティ精鋭部隊の手作業により、詳細に脆弱性を診断します。発見した脆弱性に対する対策後の再診断も提供しています。オプションメニューでは、脆弱性を悪用した侵害リスクの検査も可能です。高度なスキルを保有するセキュリティチームが手作業で確認するので、ツールが見落とすような複雑な脆弱性も検知可能です。納入業者が検査をしていたにもかかわらず、私どもが受け入れ側のお客様の立場で検査することで、気づかなかった新たなリスクが見つかるケースも多く見られるため、好評を得ています。

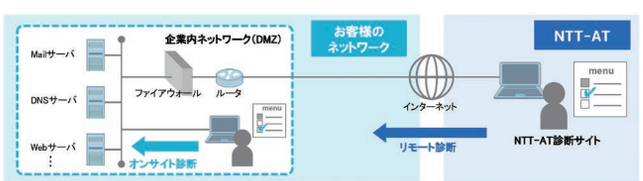

図3　Web セキュリティ診断サービスの実施イメージ

攻撃・侵入・内部感染への耐性を確認できる「標的型攻撃シミュレーションサービス」

特定の個人や組織を狙い、機密情報を盗み出そうとする標的型サイバー攻撃があります。その可能性を把握するための診断サービスが「標的型攻撃シミュレーションサービス」です。外部からの Web やメールを経由した攻撃の耐性や、内部不正やマルウェア感染など、内部起因のリスクを検知・確認することができます。

標的型サイバー攻撃のシミュレーションは、Cymulate 社製（イスラエル）のプラットフォームを使用します。これは、攻撃者視点でのサイバー攻撃を自動化して診断できるものです。このプラットフォームは、ワールドワイドでは金融機関を中心に 450 社以上が利用しており、NTT-AT では 2021 年 2 月からサービスを開始し、製造業や建設業、金融業などのお客様にご利用

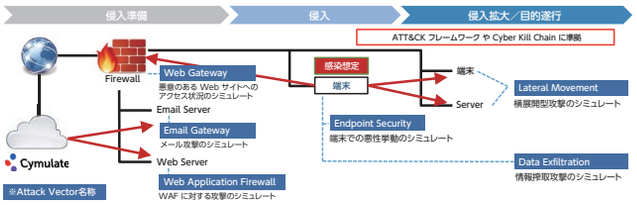

図4　標的型攻撃シミュレーションサービス

いただいています。

最新の標的型サイバー攻撃の手法が常にアップデートされ 1 万以上の攻撃による評価が可能です。シミュレーションですので、サーバーや PC 機器の破壊活動は行いません。お客様環境のデータや設定ファイルの書き換えなどは発生せず、トラフィックの負荷も低く、業務への影響を最小化して実施することができます。シミュレーション結果に基づき、セキュリティ対策上の良い点や改善すべき点を評価した日本語のレポートを提出いたします。また Cymulate 社のライセンス購入により常時シミュレーションすることも可能です。

進化し続けるサイバー攻撃の脅威に対応

インターネットの利用拡大とテクノロジーの進化によって、サイバー攻撃も凶悪化・巧妙化しています。被害の影響範囲も年々エスカレートしており、一企業だけでなく、事業に関連した複数の企業を巻き込むほど大きな影響を及ぼすようになっています。NTT-AT では、1999 年のセキュリティサービスセンタ開設以降、長期にわたり、サイバーセキュリティの技術やノウハウに磨きをかけてきました。これからもより一層お客様のセキュリティレベル向上に貢献いたしますので、各種セキュリティ診断サービスを用途に合わせて活用ください。

NTT-AT は、国や NTT グループに寄与する形で、NTT 研究所とも連携し技術やテクニカル部分をサポートし、いろいろな商材の創生、事業化を進めています。

NTT アドバンステクノロジ株式会社
セキュリティ事業本部
（右）セキュリティ診断＆運用サービスビジネスユニット
担当課長　**中川 貴之**
（左）セキュリティサービス＆ソリューションビジネスユニット
主幹技師　**小河原 成哲**