リモートアクセスを狙うランサムウェア攻撃から企業を守る多要素認証サービス「Soliton OneGate」

リモートワークやハイブリッドワークが標準的な働き方になるなか、リモートアクセス基盤の脆弱性・認証情報を悪用し、企業内ネットワークへの侵入を試みるランサムウェア攻撃が増えている。そうした攻撃への耐性を持った多要素認証サービスとして注目を集めているのがソリトンシステムズの「Soliton OneGate」だ。同サービスがなぜランサムウェアなどのサイバー攻撃に強いのか。ソリトンシステムズのエバンジェリスト、荒木 粧子氏に話を聞いた。

株式会社ソリトンシステムズ
IT セキュリティ事業部
エバンジェリスト
荒木 粧子氏

多要素認証を突破する攻撃への耐性を確保する

警察庁の報告[*1]によれば、ランサムウェア攻撃の侵入経路の83%がリモートアクセス経由のものであり、VPN機器やリモートデスクトップの脆弱性を突き、認証情報（ID、パスワード）が悪用されることが侵入の要因として考えられるという。

こうした攻撃への対策としては多要素認証が有効だ。ただし、認証アプリなどの簡易な多要素認証を突破する「AiTM（Adversary in the Middle）」攻撃も出現しており「多要素認証を行っているから安心というわけではありません」と、ソリトンシステムズのITセキュリティ事業部 エバンジェリスト、荒木 粧子氏は指摘する。

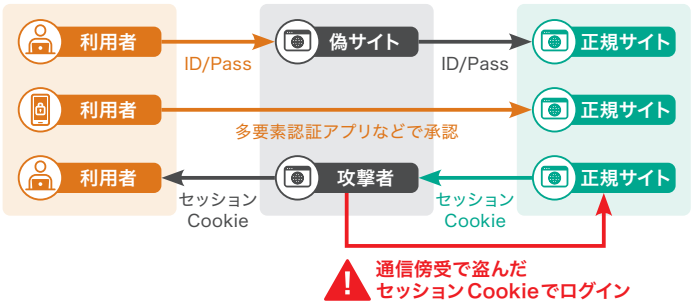
AiTMとは、フィッシングサイトにターゲットユーザーを巧みに誘導して認証情報を入力させ、その情報を悪用して正規サイトへの「セッションCookie」を盗み、認証情報を入力せずとも正規サイトにログインできる状態を確立する攻撃手法だ（図）。こうした攻撃への備えを固めるうえでは、AiTMに強い「フィッシング耐性の高い多要素認証」を採用する必要がある。そこで有効なのが、ソリトンシステムズの多要素認証サービス「Soliton OneGate」（以下、OneGate）である。

同サービスは、“なりすまし”による不正アクセスを防ぐ「デジタル証明書」によって多要素認証の攻撃耐性を強化し、クラウドサービスに点在する企業の情報資産をランサムウェア攻撃などのサイバー攻撃から守る仕組みだ。

「デジタル証明書を使うことで、（デジタル証明書を持たない）攻撃者はログイン画面に到達できず、AiTMは成立しなくなります。また、仮にログイン画面に脆弱性があったとしても、攻撃者による不正アクセスを阻止できるようになります。その意味でデジタル証明書はきわめてセキュリティ強度の高い認証手段といえます」（荒木氏）

OneGateの多要素認証では、デジタル証明書と生体認証やスマートフォン認証、パスワードなどと組み合わせることができ、「Microsoft 365」や「Google Workspace」をはじめとする多様なクラウドサービスと連携して、重要情報へのアクセスを信頼のおける利用者やデバイスに限定できるようになる。また、OneGateでは、システムへのアクセスに使用されているデバイスや位置情報などから、普段とは異なる不審なログインを検出し、追加認証を要求する「ポリシー／リスクベース認証」の機能も備えている。

図：AiTM攻撃のイメージ



デジタル証明書の運用も簡素化

デジタル証明書は、不正アクセス対策として有効な反面、運用に手間がかかるのが一般的だ。ただし、OneGateにはデジタル証明書の運用負担を低減する仕組みがある。例えば、マルチOSに対応した簡単・安全な証明書配布機能や、MDM連携による証明書配布に対応、有事の証明書失効も容易に運用できるなど、一人の社員が複数の端末を使用するような、DXが進んだ組織にも適した設計になっている。加えて、OneGateと主要なクラウドサービスのID情報を自動的に同期させることができるほか、SAML非対応の業務システムにも、ID・パスワードを代理入力するアプリでシングルサインオンを実現できる。これにより、パスワードの管理負担からエンドユーザーを解放し、かつパスワードの漏えいリスクを低減させることができる。

OneGateはすでに大手鉄道会社や証券会社など、多くの企業に導入され、不正アクセス対策の強化と運用負担の低減に役立てられている。リモートワーク、ハイブリッドワークが当たり前の今日において、サイバー攻撃から企業の情報を守るきわめて有効な手だてといえそうだ。

株式会社ソリトンシステムズ

URL …… https://www.soliton.co.jp/contact/
Tel …… 03-5360-3811
Email …… netsales@soliton.co.jp

*1 参考：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」（2023年3月公表）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf