WatchGuard Solutions Days
~最新IntelligentAVから多要素認証、無線LANセキュリティまで~

パスワードだけの危険な状態に "多要素認証"の導入で情報漏えいを防ぐ!

UTM（統合脅威管理）/NGFW（次世代ファイアウォール）といったセキュリティアプライアンス製品をメインに、数多くの企業向けセキュリティソリューションを提供するウォッチガードが、10月17日、東京都内で最新セキュリティセミナー「WatchGuard Solutions Days TOKYO」を開催。高度化したサイバー攻撃から企業を守るために必要な知識や技術、最新セキュリティソリューションの詳細を、セキュリティの最前線で活躍している登壇者たちが解説してくれた。本稿では、今回のセミナーで解説された最先端のサイバーセキュリティ技術・製品について、3回にわたってレポート。3回目は、ウォッチガードが提供するクラウドベースの多要素認証サービス「WatchGuard AuthPoint」のセッションの内容をお届けしたい。

パスワード認証の脆弱性を補う多要素認証ソリューションに注目が集まる

現代のビジネスにおいて、PCをはじめ、モバイルやクラウドといったITの活用はもはや必須といえる。テレワークやフリーアドレスなど場所や時間を問わないワークスタイルを実践する企業も増えてきており、企業ネットワークの外でも、デバイスやアプリ・サービスが活用されるようになった。このため、企業内に構築したセキュリティ対策だけでは対応できなくなり、外部に持ち出したデバイスに対応したセキュリティ対策が求められるようになってきている。

Verizonの「2016年度情報漏えい調査レポート」によると、2016年に発見された情報漏えい事件の63%が、強度の弱いパスワードあるいはパスワードの詐取に起因しているという。持ち出したデバイスが盗まれたり、悪意ある第三者に操作された場合、単なるパスワードひとつでは簡単に破られる可能性が高い。そこで注目されているのが「多要素認証（MFA）」だ。パスワードやPINなどの要素に、ユーザーの所持しているもの（専用ハードやスマートフォンなど）や、ユーザーの生体情報（指紋や虹彩など）などの要素を追加し、2つ以上の要素を組み合わせてユーザー認証を行う多要素認証ソリューションは、年の平均成長率が17.79% ～ 23%にも及ぶ成長市場となっている（成長率はグローバル市場の数値）。 今回開催されたセキュリティセミナー「WatchGuard Solutions Days TOKYO」では、ウォッチガードが提供を開始したクラウドベースの多要素認証ソリューション「WatchGuard AuthPoint」（以下、AuthPoint）についても紹介。「多要素認証ソリューション～クラウドベースの多要素認証によるセキュリティ強化」と題したセッションで、ウォッチガード・テクノロジー・ジャパンの猪股 修氏が登壇し、多要素認証の重要性からAuthPointの利用手順までを詳細に解説してくれた。

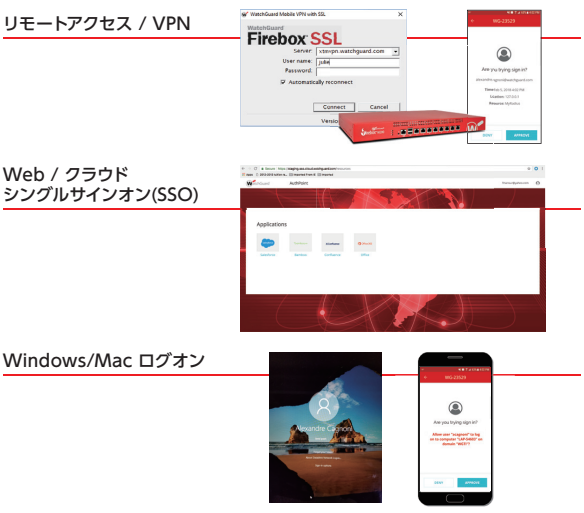
ウォッチガード・テクノロジー・ジャパン
システムエンジニア部
プリセールスエンジニア
猪股 修 氏

スマートフォンをトークンとして活用し、セキュリティを向上

AuthPointは、ビジネスに携わるユーザーのほとんどが活用している"スマートフォン"をセキュリティトークンとして利用する多要素認証ソリューションだ。クラウドベースのサービスとなっており、専用のハードウェアなどを用意しなくてもよいため、コストや手間をかけることなく導入できると猪股氏は語る。セッションでは、AuthPointの活用例として、リモートアクセス/VPN、Web/クラウドシングルサインオン、PC（Windows/Mac）ログオンが例として挙げられた。企業システムへのセキュアな接続を実現するVPNをはじめ、業務効率化に貢献する各種クラウドアプリ・サービスを使いやすくするシングルサインオン、そして不正利用を未然に防ぐためのPCログオンの強化と、どれもがワークスタイル変革にともなうセキュリティ上の課題を解決してくれるものとなっている。

AuthPointにおける多要素認証の仕組みは、第一要素がパスワード固定、第二要素として「プッシュ通知」「QRコード」「ワンタイムパスワード」を選択することができる。「プッシュ通知」は、認証時にスマートフォンへ送信された通知で「承認」をタップするだけの簡単操作、「QRコード」は、認証画面に表示されたQRコードをスマートフォンで読み取ることで表示されるコードを入力、「ワンタイムパスワード」はスマートフォ

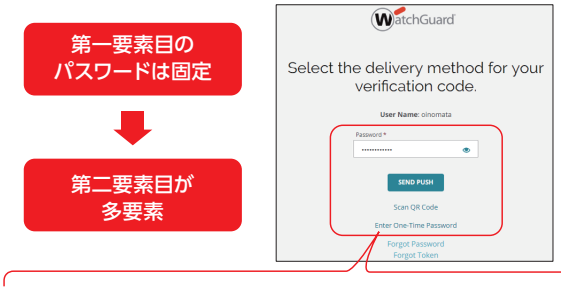
AuthPoint 使用例



パスワードだけの危険な状態に"多要素認証"の導入で情報漏えいを防ぐ!

ンに表示される6桁のパスワード（30秒で自動変更）を入力するだけと、どれもシンプルな操作で認証が行える。ユーザーの利便性を損なわずに、セキュアな多要素認証を導入することが可能と猪股氏。セッションでは、実際の活用事例として、Radius認証によるリモートアクセスVPN接続構成（AuthPointは単体のクラウドサービスとして提供されるため、Radiusサーバを用いたVPN認証に対応している場合Firebox以外のデバイスでも利用可能）や、SAMLに対応した複数のクラウドアプリ／サービスへのWeb SSO認証による接続構成、さらにオンライン・オフライン環境に対応したPCログオンの仕組み（エージェントをPCにインストールして利用）が解説された。

AuthPoint が提供する多要素認証の種類



プッシュ通知

スマートフォンに認証通知リクエストが送信され、"承諾"すると認証が成功します。ご自身のスマートフォンだけに通知されるので第三者によるログインを防げます。

QRコード

スマートフォンよりQRコードをスキャンし認証します。QRコードを読み取りパスワードを生成します。従って固定パスワードの管理は不要です。

ワンタイムパスワード

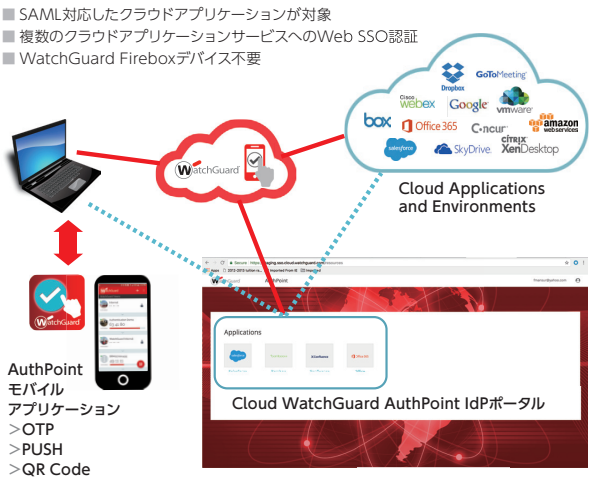
スマートフォンに表示されるワンタイムのパスワードを入力し認証します。
ワンタイムは30秒間隔でランダムに変更されるので固定パスワードではありません。従ってパスワード管理が不要です。

どれもが、認証時のセキュリティを高める事例で、特にWeb SSO認証では「WatchGuard AuthPoint IdPポータル」を経由することで、複数のアプリ／サービスを1回の認証で使えるようになり、セキュリティはもちろん、ユーザーの利便性も大幅に向上する。このほか、ダッシュボード・レポートやスケジュール・レポートなど、クラウドサービスならではの豊富なレポート機能も利用可能で、業務の"見える化"にも貢献するという。

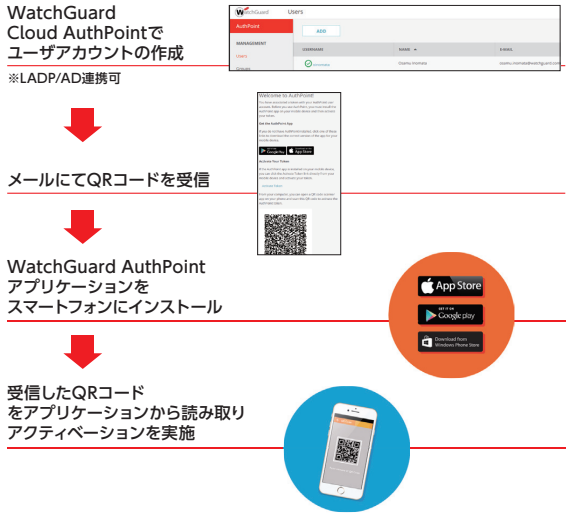
セッションでは、クラウド上でのユーザーアカウント作成から、スマートフォンにWatchGuard AuthPointアプリをインストールしてアクティベーションを行うまでの、AuthPoint利用の流れをデモンストレーションで解説。さらに、AuthPoint IdPポータルを利用したWeb SSO認証によるクラウドアプリへの接続手順や、オンライン／オフライン時のPCログオン手順なども猪股氏により詳細な説明がなされた。万が一、設定したスマートフォンを紛失した際も、クラウド上から迅速にアカウント削除が行えるなど、隙のないセキュリティソリューションであることも確認することができた。

本セミナーの参加者は、サイバーセキュリティを向上させたい企業担当者が中心となっていたが、特別なハードウェアや大掛かりなシステム変更などを必要とせず、コストを抑えながら強固なセキュリティ体制が構築できるAuthPointへの注目度は非常に高かった。グローバル市場と比較すると、中堅・中小企業ではまだまだ多要素認証の導入が進んでない日本だが、AuthPointのような低コストで容易に導入できるソリューションが登場してきたことで、今後は急速に普及が進むのではないだろうか。そんな期待を抱かせるセッションとなっていた。

AuthPoint Web SSO 認証による クラウドアプリケーションサービスへの接続構成例



ユーザ作成からモバイルアプリケーションの登録までの流れ



ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041　東京都港区麻布台 1-11-9 CR BPR プレイス神谷町ビル 5 階
Tel. 03.5797.7205
Fax. 03.5797.7207
URL https://www.watchguard.co.jp/
MAIL jpnsales@watchguard.com