宮崎大学
University of Miyazaki

大学関係者 1 万ユーザを対象に、スマートフォンを活用したクラウドベースの多要素認証ソリューションで認証強化を実現

国立大学法人 宮崎大学

国立大学法人 宮崎大学は平成 15 年 10 月に旧宮崎大学と宮崎医科大学が統合し、平成 16 年 4 月から国立大学法人宮崎大学（以下宮崎大学）になりました。「世界を視野に地域から始めよう」のスローガンのもと、生命科学、環境科学、エネルギー科学、食の科学の分野を筆頭に、国際的に通用する特色ある高度な学術研究結果を世界に発信しています。

課題

学外に対して大量のスパムメール送信や Web サイトの改ざん等、アカウントの不正使用によるインシデントが過去に発生しました。学生を含む構成員（約 1 万人）に対して、情報セキュリティ教育を毎年行っており、特に脆弱なパスワードは変更する、パスワードの使い回しは行わないことを指導してきましたが、徹底できていませんでした。こうした理由により、情報セキュリティ教育を充実させると同時に、システム的な認証強化対策を実施することが急務となっていました。また、文部科学省から「大学等におけるサイバーセキュリティ対策等の強化」方針がまとめられ、この中でアカウント管理の徹底、多要素認証（MFA）システムの導入等が定義されたことも認証強化を図る要因の一つでした。

ソリューション

そこで宮崎大学ではセキュリティ体制の強化の一環として、多要素認証（MFA）を提供する複数のベンダーの検討を 2018 年より本格的に開始しました。「ウォッチガードの多要素認証（MFA）ソリューション「WatchGuard AuthPoint（オースポイント）」の存在を初めて知ったのは、宮崎で同年の 11 月に開催されたセミナーがきっかけでした」と今回の導入指揮を執った宮崎大学の情報基盤センター 技術専門職員の園田 誠（そのだ まこと）氏は振り返ります。

「多要素認証（MFA）システムをオンプレミスで導入するには、導入コストや運用管理／保守費用が高額になるのではないかといった印象がありました」（園田氏）。その点 WatchGuard AuthPoint は、ウォッチガードが提供する WatchGuard Cloud と呼ばれるクラウド上に置かれている管理共有基盤で管理することができるため、オンプレミスでの管理負荷を軽減し、コストも抑制できるといったメリットが考えられました。また、クラウドサービスが日本国内で展開されていることも安心要素の 1 つでした。さらに園田氏は「現在ほとんどの学生がスマートフォンを利用しているため、各個人が所有するスマートフォンをトークンとして代用することで、従来発生していたトークンの購入費用をゼロにすることができると考えました」と説明しています。

WatchGuard AuthPoint の選定の決め手となったのは、その他に認証手法として（1）プッシュベース認証をサポートしていることからワンタイムパスワード入力の手間を省くことができる（2）外資系ベンダーにありがちなローカライズ未対応のマイナス要素もなく、スマートフォンにインストールするトークンアプリが日本語化されており、ユーザフレンドリーなインターフェイスが採用されている（3）スマートフォンへのトークンアクティベーションにメールと Web（IdP ポータル）のいずれかを活用できる（4）初期導入時は VPN と Office365 に対する認証強化のみだが、今後その他のクラウドサービスを導入した場合に追加コストが発生しない（5）ベーシック認証を無効とし、二要素目のみ有効とすることができ、パスワードレスにすることもできる（6）クラウドアプリケーション（SAML ベース）の SSO 機能を搭載していること等が挙げられています。

また、宮崎大学の情報基盤センター 技術専門職員の黒木 亘（くろぎ わたる）氏は次のようにコメントしています。「スマートフォンの機種変更時に利用者自身でトークンの移行ができるため、運用管理負荷の軽減につながるとともに、日常運用で管理者が利用状況や利用者のステータス管理を行うため、管理機能が充実していることも大きなメリットになります。」

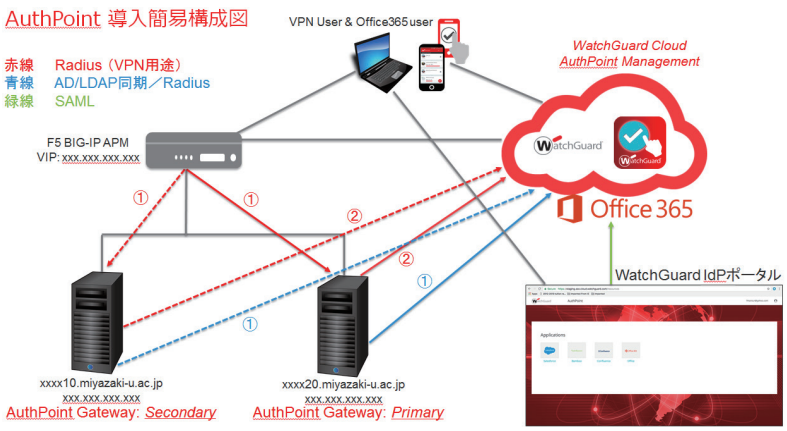
顧客
国立大学法人
宮崎大学

ユーザ数
約 10,000

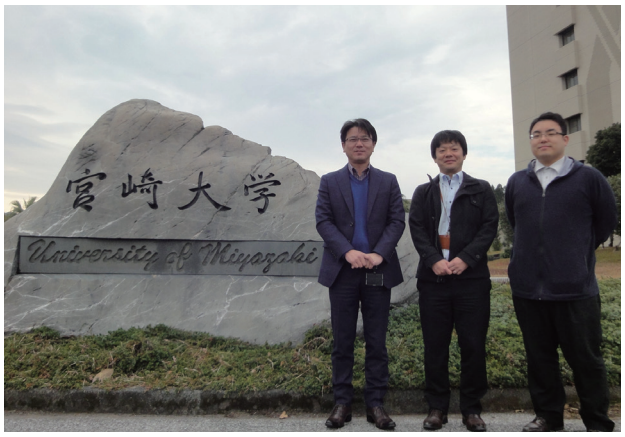
業種
教育

地域
宮崎県

導入製品
WatchGuard
AuthPoint



多要素認証（MFA）のシステム構成図



宮崎大学 情報基盤センター
（園田 誠 氏／黒木 亘 氏／川畑 圭一郎 氏）

導入

宮崎大学は WatchGuard AuthPoint のこうした特長を高く評価し、2019 年 9 月に同製品の導入を決定しました。導入時のインプリメンテーションにおけるオンプレミスでの作業は、AD ユーザの同期や Radius 中継目的のアプリケーションインストールのみで、残りは全てクラウド環境での作業となり、同年の 12 月にカットオーバーすることができました。

効果

WatchGuard AuthPoint を導入したことで、容易な操作で不正ログインを防止し、エンドポイントのセキュリティが強化されたことは言うまでもなく、運用面においても、アカウントのステータス毎に抽出が可能など充実したユーザアカウントの検索機能や、スマートフォンの機種変更時にトークンの移行を各ユーザで実施することが可能であることから、情報システム部門の手間を省くことができるといった効果がありました。「既存の認証基盤（LDAP/AD）に特別な変更を必要とせず、WatchGuard Cloud、AuthPoint、AD/LDAP サーバを同期させているため、アカウント管理は基本的に AD/LDAP サーバのみで非常に助かっています」と宮崎大学の情報基盤センター 技術職員の川畑 圭一郎（かわばた けいいちろう）氏は述べています。

既存認証基盤（LDAP/AD）に登録されているユーザで、多要素認証を使う人、使わない人を多要素認証のシステム側で設定することができます。また、セーフロケーション機能を利用することにより、信頼の置ける IP アドレスからの二要素認証を不要とし、ベーシック認証のみのアクセスが可能になります。さらに様々な通知機能があり、異常や障害が発生した場合にリアルタイムに管理者へ通知されるため、モニタリングにも負荷がかかりません。併せてレポート機能も充実しており、認証統計情報やサービスに対するアクセス統計をクラウド経由で確認することができます。

WatchGuard AuthPoint について

クラウドベースの多要素認証ソリューションとして、クラウドアプリケーション（SAML ベース）、リモートアクセス VPN、PC ログイン時の認証強化を図ることができます。クラウドベースによって全て管理することができるため、管理コストも削減することができます。また、スマートフォンにトークンアプリをインストールし、プッシュベース認証、ワンタイムパスワード、あるいはオフライン時に QR コードを読み取ることで認証を強化することが可能になります。

【WatchGuard Technologies について】

WatchGuard® Technologies は、ネットワークセキュリティ、セキュア Wi-Fi、多要素認証、そしてネットワークインテリジェントを提供するグローバルリーダとして、全世界で約 10,000 社の販売パートナーとサービスプロバイダより 80,000 社以上の企業にエンタープライズクラスのセキュリティ製品とサービスを提供しています。ウォッチガードのミッションは、中堅・中小企業や分散型企業を含むすべての企業がエンタープライズレベルのセキュリティをシンプルに利用できるようにすることです。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、数多くのパートナーを通じて、国内で拡大する多様なセキュリティニーズへのソリューションを提供しています。詳細は https://www.watchguard.co.jp をご覧下さい。

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 BPR プレイス神谷町 5 階
TEL：03-5797-7205　EMAIL：jpnsales@watchguard.com www.watchguard.co.jp