

PRESS RELEASE (2013/2/26)

九州大学が WisePoint Shibboleth の全面運用を開始

～世界に先駆けて、安全かつ強固な多要素認証シングルサインオンを共同開発で実現～

概要

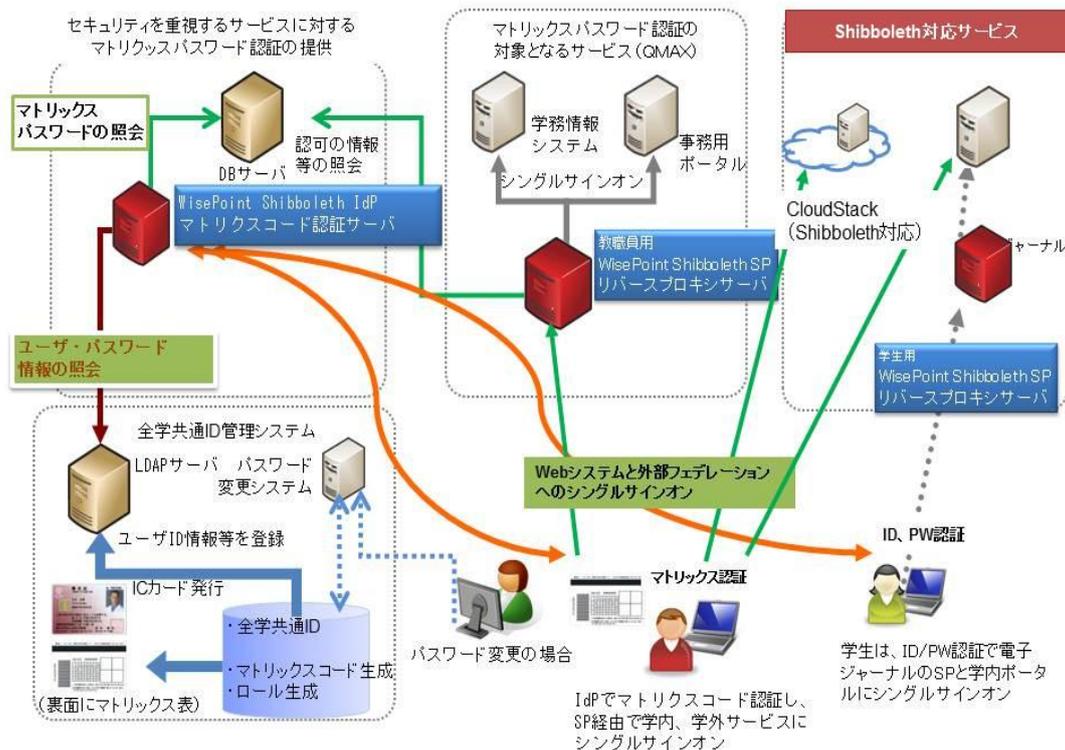
国立大学法人 九州大学(福岡県福岡市、総長:有川節夫、以下 九州大学)情報統括本部(本部長:藤村直美)は、2013年1月より認証基盤システム「WisePoint Shibboleth」の全面運用を開始しました。本システムの運用開始により、Shibboleth(シボレス)シングルサインオンにおいて、強固な多要素認証方式を備えた利用者認証方式を実現できるようになりました。

内容

九州大学ではこれまで、学務情報システム等の安全性重視サービス利用時には強い認証機能を持つファルコンシステムコンサルティング株式会社(本社:神奈川県川崎市、代表取締役:高橋正迪、以下ファルコン SC)のWisePointを導入し、WisePointが持つマトリックスコード認証¹⁾を適用することで安全性を確保していました。WisePointはリバースプロキシ型のWebシングルサインオンを実現し、かつマトリックスコード認証等の強固な認証方式を備えた製品です。

一方、電子メールや電子ジャーナル等、利便性重視のサービスでは個別のID・パスワードで認証していました。Web系の情報サービスでは、利用者認証時の手間を削減するため、一度の認証で複数のサービス利用が可能になるシングルサインオン(SSO)を進めており、その方式として学術系で普及している Shibboleth(シボレス)認証²⁾を採用しています。Shibbolethを使うことにより、国内および世界の学術認証フェデレーションに参加でき、学術機関向けサービスの多くを利用できるようになりました。

▼九州大学における WisePoint Shibboleth 導入イメージ



■ WisePoint Shibboleth の主な機能

- ・ワンタイムパスワード認証機能
マトリックスコード認証、イメージングマトリクス認証、J パスワード認証に対応。
- ・SP (Service Provider) 機能
SAML2.0 対応。ShibbolethSP、Non-ShibbolethWeb アプリケーションへのシングルサインオン機能。
リバースプロキシ機能。アクセスコントロール機能。
- ・IdP (Identity Provider) 機能
認証機能 (ID、パスワード、マトリックスコード認証、イメージングマトリクス認証、J パスワード認証)。LDAP 連携。

■効果

SSO 対応のサービスが増えるにつれ、安全上の問題も出ていました。認証方式が ID・パスワードだけの場合、パスワードを破れば他人になりすまして SSO 対応の全サービスを利用できてしまいます。この問題を防ぐため、パスワード以外の認証方式を併用する多要素認証³⁾が求められていました。また、Shibboleth 認証装置と、WisePoint マトリックスコード認証装置を複数運用するコストも問題になっていました。そこで、今回、多要素認証方式による Shibboleth 認証を実現する「WisePoint Shibboleth」を開発することになりました。

WisePoint Shibboleth は、九州大学とファルコン SC の連携により、2011 年 2 月から共同開発したものです。実際に九州大学附属図書館のサービスで実験を重ね、実験で得られた不具合部分を調整しつつ、今回の全面運用に至りました。本開発により、多要素認証による Shibboleth SSO を実現できるだけでなく、認証装置の維持コスト削減も実現できました。今後、クラウドサービスや外部フェデレーションサービスが追加される際にも、WisePoint Shibboleth の多要素認証とシングルサインオンにより安全性を確保しながら利用者の利便性を損なうことなく、サービスを提供していくことが可能となります。

■今後の展開

九州大学情報統括本部は、今後も安全性に留意しつつ、様々な学内向け情報サービスを提供していきます。また Shibboleth を経由して、国立情報学研究所の学術認証フェデレーション (学認)⁴⁾に関連するサービスの拡充を行います。ファルコン SC は、WisePoint Shibboleth の販売により、多くの学術機関における情報サービス利用の安全化を実現するとともに、Shibboleth による学認参加の支援や、全国および世界での大学間認証連携による学術サービス連携を支援していく予定です。

■用語説明

- 1) **マトリックスコード認証**: パスワードの代わりに行列のマス目に記入した数値・文字列のコードを利用者認証に用いる。サービス側が指定する座標のコードを、利用者がパスワードとして入力する。
- 2) **Shibboleth 認証**: 米国の Internet2 プロジェクトで開発された Web 系情報サービスシステムの分散シングルサインオン方式。内部では SAML を用いる。
- 3) **多要素認証**: 利用者認証時に、パスワードだけでなく、他の要素 (マトリックスコード、秘密の質問、ワンタイムパスワード等) を併用する認証方式。
- 4) **学認**: 学術認証フェデレーションの略称で、国立情報学研究所が推進する、全国の大学や研究機関および学術機関向けサービス提供者での共通認証機構に関する連携。各機関の構成員は、加盟機関が提供するサービスを、学内サービスと同様にシングルサインオンで利用可能になる。

【本件に関するお問い合わせ先】

九州大学情報統括本部情報環境整備推進室
認証基盤事業室 [担当:尾花]
〒812-8581 福岡市東区箱崎 6-10-1
TEL: 092-642-7234 E-Mail: id-room@iii.kyushu-u.ac.jp

【本件に関するお問い合わせ先】

ファルコンシステムコンサルティング株式会社 営業本部[担当:山下]
〒213-0012 神奈川県川崎市高津区坂戸 3-2-1
かながわサイエンスパーク西 612
TEL: 044-814-2512 E-Mail: sales@falcons.com
URL: <http://www.falcons.com/>

*本文中に記載の製品名はファルコンシステムコンサルティング(株)の登録商標または商標です。