手間なくセキュアに外部ネットワークへ認証・接続
SAML認証にも対応した「eFEREC v1.2」

エンドポイントアクセス制御装置「eFEREC v1.2」では、SAML認証によるログイン機能が新たに追加されました。オープンな標準規格であるSAML認証は様々なクラウドサービスに対応しており、eFERECにおいてそれらと連携したシングルサイオンオン認証が可能になります。

セキュリティが重要なネットワーク認証にシングルサインオンを取り入れたい

組織のネットワークでは、不正な端末や不正なユーザーによるネットワーク利用を防ぎ、セキュリティを担保するため、ネットワーク接続へのエンドポイント認証（端末やユーザーの認証）を行うことが少なくありません。

このネットワーク認証には、様々な認証方式があります。これまで主流だった多くの方法では、ユーザーがネットワークに接続しようとしたとき、あらかじめ管理者が認証キー（ID・パスワードまたはデジタル証明書など）を設定した上で該当ユーザーに提供する必要がありました。そして認証キーの提供を受けたユーザーも、その認証キーを端末に入力ないし設定し、まずネットワークにログインした上で、続いて利用するサービスにログインすることになり、二度手間となっていました。

この二度手間を省く手段としては、シングルサインオン（SSO）が効果的です。システム間で認証結果の情報を連携させる仕組みを設けることにより、1つのシステムにログインすれば他のシステムにもログインできるようになります。ただしこれまでのSSOは、同じドメイン内に限られるのが通例でした。別ドメインの組織に端末を持ち込んで利用する場合などは、いったん訪問先ネットワークにゲストアカウント等でログインし、改めて自組織のサービスにログインする二度手間が発生していました。

しかし近年では、多くの組織でクラウドサービスの利用が拡大するなど、ネットワークの使い方にも変化が出ています。最近の主要なクラウドサービスは、多くがSAML（Security Assertion Markup Language、現在ではSAML2.0）認証に対応しています。このSAML認証は、異なるインターネットドメイン間でユーザー認証を行うための標準規格で、これまでの手法と比較して容易に、より多くのサービスとの間にSSOを実現できることが特徴です。SAMLにおいては、認証をつかさどる「IdP（Identity Provider）」、実際のサービスを提供する「SP（Service Provider）」の2つの役割が規定されており、ユーザーがSPにアクセスしてログインしようとした際、いったんIdPで認証が行われ、その結果を受けてSPからのサービスが提供されるようになっています。

バージョンアップで新たにSAML対応 IdPでの認証でネットワークも利用可能に

ネットスプリングが開発・販売するエンドポイントアクセス制御装置「eFEREC」は、ネットワーク内部からのアクセスに対するユーザー認証やアクセス制御を行う製品で、

1. 利用者がブラウザで任意のWebサービスに接続しようとする
   - ●eFERECのログイン画面に強制的にリダイレクト
   - ・最初のWebサービスがHTTPSの場合、eFERECへのリダイレクト時に「不正な証明書」の警告が表示される
2. 利用者のブラウザにeFERECの画面が表示される
3. eFERECのログイン画面でログイン開始
   - ●IdPのログイン画面にリダイレクト
   - ・IdPが複数存在する場合は、IdPの前にDS（Discover Service）の画面が表示され、DSでIdPを選択することによってIdPのログイン画面に遷移
4. 利用者のブラウザにIdPのログイン画面が表示される
5. 利用者はIdPでユーザ認証を行う
   - ●ユーザ認証に成功すると、eFERECにログイン
6. eFERECのログイン済み画面が表示される

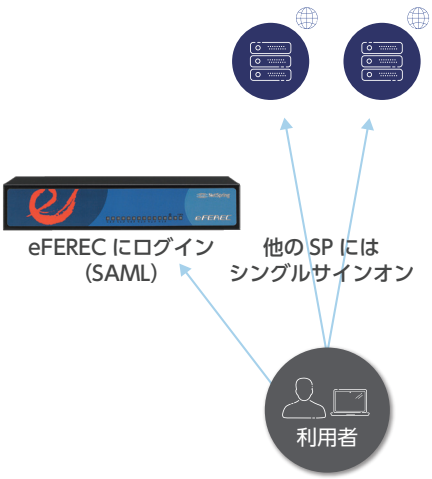

図1：eFEREC v1.2におけるSAML認証の流れ

本製品に接続された有線LANスイッチや無線LANアクセスポイントからのアクセスを管理します。コンパクトなアプライアンス製品となっており、ネットワークブリッジとして設置するため既存ネットワーク環境に大きな変更を加えることなく導入でき、例えば組織外のユーザーが多い会議室などに限ってネットワーク認証を実施するような使い方も可能です。応用範囲の広さから、様々な企業をはじめ、大学、図書館や病院などで採用されています。

ネットスプリングでは、eFERECの使い勝手や機能の向上を継続的に行っています。例えば、スマートデバイスでのログイン操作を容易にする専用アプリ「SmartSignOn for eFEREC」のAndroid版およびiOS版の各版を提供しています。

eFEREC バージョン1.2においては、新たにSAML認証によるログインに対応しました。「SAMLオプション」を追加することで、オープンソースのソフトウェアパッケージ「Shibboleth」のSP機能が利用可能となります。これにより、eFERECのネットワーク認証に、ネットスプリングの認証アプライアンス「AXIOLE」も含め自組織や外部の連携組織が持つIdPの認証結果を利用できるようになります。 また、Office 365やG Suiteなどのクラウドサービス、あるいは大学等で広く使われている学術認証フェデレーション「学認」やその他のSAMLに対応したWebサービスとeFERECとのSSOが可能になります。

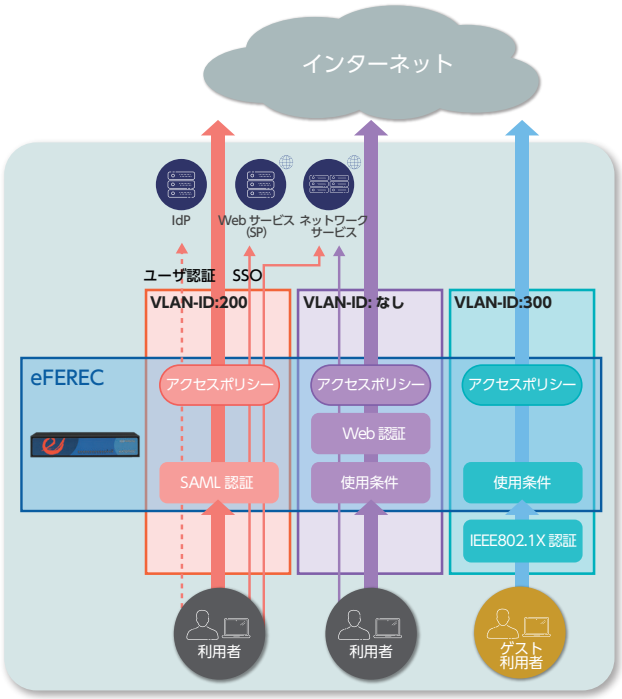

図2：大学におけるeFEREC v1.2の活用例

実際の利用イメージは図1あるように、ネットワークにアクセスすると、まずeFERECの認証画面が表示されます（ここまでは、eFERECの他の認証手段でも同様です）。ここでユーザーがSAML認証で使うIdPを選んでログインすると、IdPでの認証結果がeFERECに伝わり、ネットワークにもログインできるという流れです。ユーザーにとっては、実質的にネットワークへのログイン操作を行う必要も、そしてネットワークへのログインID・パスワードなどがなくても、自身が利用するサービスへのログインだけでネットワークを利用できるようになります。

単に便利なだけでなくセキュリティも向上
今後さらなる機能強化を計画

なお、eFEREC Ver.1.2では最大3つのVLANにユーザー認証を求める機能（認証ゲートウェイ）を設定できる（内SAML認証は最大1つ）ため、異なる認証方式を併用することができます。

また、eFERECはユーザー認証に成功した利用者にアクセスポリシーを設定することができます。アクセスポリシーは、認証ゲートウェイごとに異なる設定をすることができます（Web認証のみ、さらにユーザーごとにアクセスポリシーを指定することも可能です）ので、例えば図2のように、従来からのWeb認証とSAML認証、そして単なるゲストユーザー向けといった形で、きちんと分けて管理することが可能です。

さらに、SAML認証では、IdP側が多要素認証に対応していればそれが適用されるため、ID・パスワードのみの認証よりもセキュリティ水準が向上します。このように、eFERECとSAMLの組み合わせでは、利便性とセキュリティの両方をより高めることが可能になります。

ネットスプリングでは、今回のSAML認証対応に続き、eFERECのさらなる機能向上を進めていきます。現在のところ、クラウド版のActive Directoryへのネイティブ対応や、生体認証も可能となる新標準の認証技術FIDO2への対応などを計画中です。こうした新機能は、準備が整い次第ソフトウェアのバージョンアップで利用できるようにする計画です。

株式会社ネットスプリング
http://www.netspring.co.jp/
eFEREC 製品サイト：https://www.eferec.jp/
スマートアプリサイト：https://eferec.smartsignon.jp/
〒108-0073　東京都港区三田 3-12-16 山光ビル 2F
TEL：03-5440-7337　　FAX：050-3737-1458