@ITセキュリティセミナーリポート

働き方改革に欠かせない認証基盤とは？

クラウドサービスとレガシーWebアプリケーションのシームレスなSSOの実現に向けたNTTコムウェアの取り組み

2018年夏、@ITセキュリティセミナー 東京・大阪・福岡・札幌ロードショーが開催されました。6月22日の東京会場では、NTTコムウェア ネットワーククラウド事業本部 サービスプロバイダ部 CLS-BU 担当課長の野呂昌哉が「多様化する働き方、変革期の企業システムに求められる認証基盤について」と題し、NTTコムウェアにおける働き方改革とクラウドサービスとレガシーWebアプリケーションのシームレスなシングルサインオンを実現する認証基盤について講演しました。

働き方改革推進の過程で見えてきた3つの課題

育児や介護などの社会的課題を背景として、働き方改革が注目されています。NTTコムウェアでも、ICTソリューションによって働き方改革を加速していこうと取り組んでいます。

その一環として、自社ビルでの業務だけでなく、在宅勤務やお客さま先ビルなどのロケーション、営業・開発・保守運用などの職種で分類し、業務の現状調査を行いました。その結果、浮かび上がってきたのは、社内IT環境における3つの課題でした。

第1の課題は「コミュニケーション環境」です。社内外との連絡手段はメールや電話が主流であり、限定的であるため、連絡がとりにくい状況です。第2の課題は「ナレッジ環境」です。社内のナレッジ環境は組織ごとに分散されており、探しにくく、期待したほどには有効活用されていない現状があります。第3の課題は「パソコン環境」です。社員の端末はシンクライアントであり、強固なIT統制が効いているため、セキュリティー面でのメリットはあります。その半面、ツールが自由にインストールできないという問題があります。また、パソコンであるがゆえに、お客さま先でプレゼンがスマートにできないといった声があがっています。

図1：NTTコムウェアの「社内IT環境」の整備

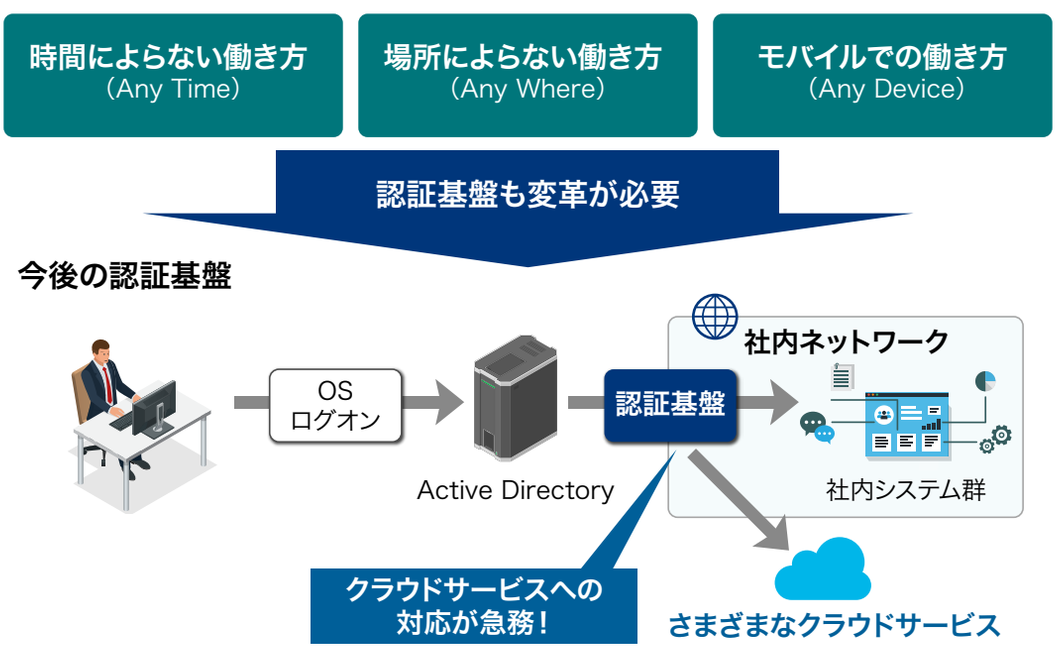
浮かび上がってきた認証環境の課題

これらの改善策を検討していく過程で浮かび上がってきたのは、認証環境に関する課題でした。端末起動時のOSへのログオン後、社内システムが使えるようになるまでに、ユーザーは何度も認証が必要となっており、利用者目線で考えると利便性が悪く非効率であることも事実です。

一方、クラウドサービスの導入も進んできています。しかしクラウドサービスと社内システムで認証方式が統一されていないため、パスワードやアクセス権限を個別に管理しなければならないといった課題が分かってきました。

NTTコムウェアはこのような背景から、「時間や場所やデバイスによらない働き方」を実現するためには、認証基盤も変革が必要であると考えました。

図2：認証基盤も働き方改革対応



従来の認証基盤でもシングルサインオン（SSO）は実現していましたが、対応していたのは社内システムだけでした。しかし将来を見据えると、社内システムだけでなく、クラウドサービスへのSSO対応も急務でした。

クラウドサービスのフェデレーションと従来の独自認証の両方に対応するには？

ここでNTTグループ全体の施策について触れたいと思います。NTTグループでは、各社で個別に運用されている認証機能を「NTTグループ統合認証基盤」に集約する施策を推進しています。このNTTグループ統合認証基盤は、グループ各社のActiveDirectoryとAD FS（Active Directory Federation Services）でフェデレーション（ユーザー認証の連携）することで認証を一元的に行い、グループ共通で利用する仕組みで、SAML（Security Assertion Markup Language）プロトコルを用います。

NTTコムウェアも、このNTTグループ統合認証基盤システムを自社の社内システムの認証基盤として活用することとしました。

ところが、NTTコムウェアの従来の認証基盤は、SAMLではなく、独自認証方式を採用していました。社内システムは50以上存在するため、それらすべてをSAMLに対応させる改修には莫大なコストがかかります。

そこで、NTTグループ統合認証基盤とはSAML認証を行い、社内システムであるレガシーWebアプリケーションには従来方式で認証を行える、新たな認証基盤を構築する方向で検討しました。

クラウドサービスと従来の社内システムの両方の認証方式に対応するWAMの導入

SAMLと従来の社内システムの両方の認証方式に対応できるソリューションとして採用したのが、EVIDIAN-BULL JAPANが提供するEvidian Web Access Manager（WAM）です。

野呂 昌哉
NTTコムウェア株式会社
ネットワーククラウド事業本部
サービスプロバイダ部 CLS-BU
担当課長

WAMを採用した第1の理由は「認証要件」です。SSOにはいくつかの方式がありますが、NTTコムウェアの従来の認証基盤は、認証サーバーを経由するリバースプロキシー方式でした。しかし、クラウドサービスでは、サービスを提供するプロバイダーは認証機能を持たずに、外部のIDプロバイダーに認証を委ねるフェデレーション方式がよく使われています。

WAMはリバースプロキシー方式とフェデレーション方式の両方に対応していました。WAMを導入すれば、社内システムであるレガシーWebアプリケーションの認証はそのままにして、クラウドサービスの認証もできるようになります。

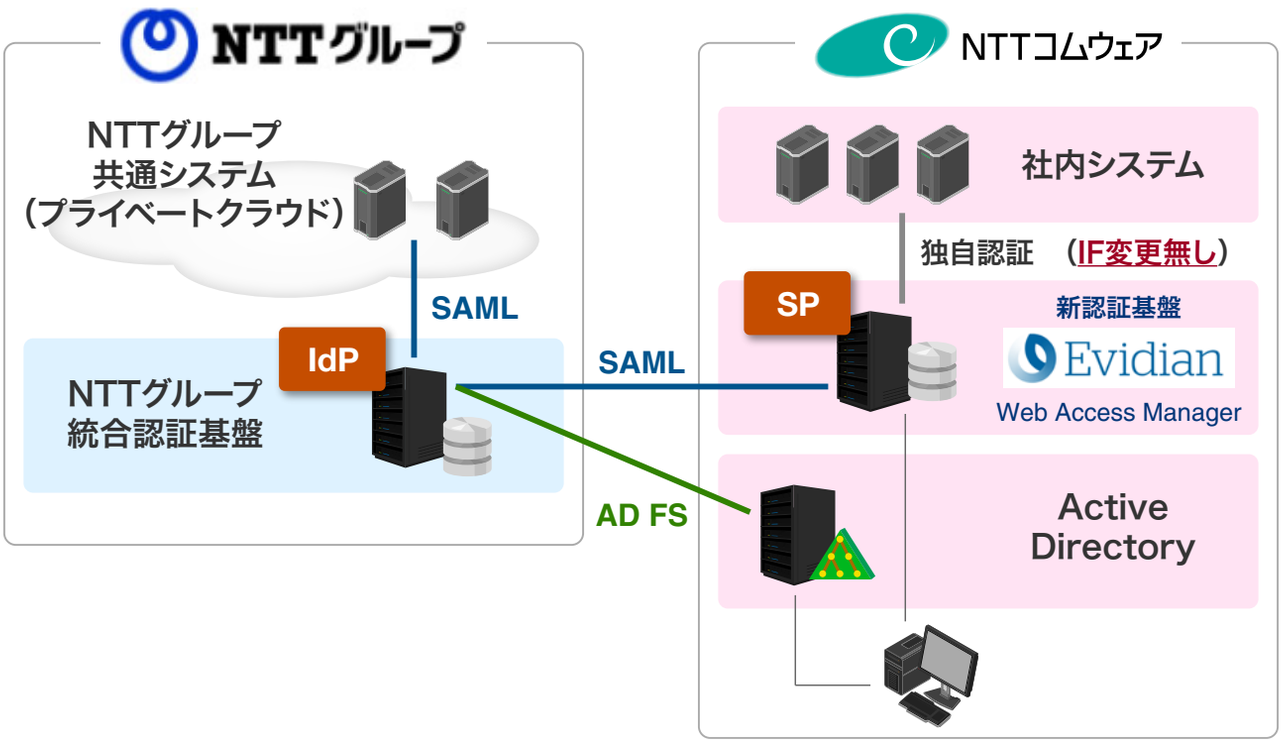
第2の理由は「アクセス権限」、つまり「認可制御」です。NTTコムウェアでは、「営業部の社員であれば営業部のシステムにアクセスできるが、他部署の社員はアクセスできない。そして承認処理は権限のある管理者にのみ許可される」などの細かい制限を設けていました。そのため従来の認証基盤は部署や役職といったロールを設定し、社内システムのURL単位に接続制限をかけていたのです。

また、社内システム側での認可制御が必要であるため、社員のアカウントの属性情報を流通する必要がありました。流通とは、業務システムに対して、アカウントの属性情報を送って認可制御に利用することを意味しています。これにはCookieを利用することで対応していました。これらの属性情報の流通に関する制御はWAMでも実現可能でした。

第3の理由が「可用性」です。従来の認証基盤は、認証サーバーを経由するリバースプロキシーサーバー方式であるため、認証サーバーがすべてのシステムへの中継ポイントになります。そのため認証サーバーがダウンすると、すべてのシステムが利用できなくなる危険性があるため、認証サーバーのダウンはなんとしても回避しなくてはいけません。もちろん従来の認証基盤でも可用性を考慮して、サーバーを二重にし、ロードバランサーを設置するなどの対策を施してはいました。

当然、新しい認証基盤においても可用性の確保は求められます。これについては冗長構成を確保するソフトウェア「Evidian SafeKit」によって、認証サーバーの二重化が実現できます。ロードバランサーが不要になり、シンプルで低コストな冗長構成を実現できるというメリットがありました。

図3：Evidian Web Access Managerの採用



認可情報の同期には苦労もあった

ただし、WAMの導入に関して一筋縄ではいかず、苦労した場面もあったのも事実です。それは、認可制御の設定でした。

社内システムでは以前から認可制御を実現しており、認可に用いるアクセス制御情報は、従来の認証基盤のリポジトリ（ユーザーディレクトリ）内に格納していました。一方で、WAMの認可制御では、WAM独自のWAM Directoryというリポジトリに認可情報を格納する必要があります。

つまり、従来の社内システムの認可情報、WAMの認可情報が、別々の場所に存在することになるため、2つのディレクトリを同期しなくてはいけません。

同期には、Evidian ID Synchronizationという便利なツールが利用できました。ところが、この同期の設定は簡単ではありませんでした。WAM Directoryの内部構造を深く理解した上で、どの項目をどのように同期するかを設計する必要があったのです。この設計と実装は非常に苦労しましたが、何とか達成することができました。お客さまの会社でも新しい認証基盤を導入される際には、アカウント情報の移行については十分考慮されるとよいと思います。

@ITセキュリティセミナーリポート **働き方改革に欠かせない認証基盤とは？**

SSOによってICTの利便性を高め、働き方改革を推進する

WAMの利用によって、以前から活用していたレガシーWebアプリケーションに加えて、クラウドサービスに対して、SSOを実現する基盤を構築できました。

これにより、社員は、社内にいるときはもちろん、出先、自宅などさまざまな場所にいても、自分のアカウントでOSにログオンするだけで、必要なすべてのサービスにSSOできる仕組みが実現できたわけです。

いつでもどこでもICT機器が使え、利便性が高まったことで、コミュニケーションやナレッジ環境の共有がますます進み、NTTコムウェアの働き方をより推進するための道筋が開けました。ここで蓄積した知見は、お客さまの認証基盤の構築・改善に貢献できると考えています。ぜひ、お客さまの会社でもSSOを始めてみませんか？

Column

ATAWAD
(Any Time, Any Where, Any Device)
をめざして

@ITセキュリティセミナー 東京・大阪・福岡・札幌ロードショーでは、野呂の講演に先立ち、NTTコムウェアが導入したWAMを提供している、EVIDIAN-BULL JAPAN株式会社 日本統括マネージャー／最高技術責任者 オリビエ・イサテル氏の講演も行われました。

ウイークポイントはユーザー自身。だから認証システムが重要

Evidianは、ID管理とアクセス制御において20年以上の経験を持つ、フランスに本社を置くソフトウェアメーカーです。Evidianの製品は1,000社以上のお客さまにご使用いただいております。

企業は、ワークスタイルの変化、働き方の変化、クラウドサービスの活用、デジタル技術の活用などによって、デジタルトランスフォーメーションに取り組もうとしています。これらの取り組みによって、企業の情報システムを利用するユーザーは、いつでも、どこからでも、さまざまなデバイスを利用して、企業の情報システムにアクセスできるように変わりつつあります。

Evidianではこのような世界を「ATAWAD（Any Time, Any Where, Any Device）」という言葉で表現しています。この「ATAWAD」の環境により、ユーザーの利便性、そして、ユーザーの業務生産性は、大きく向上すると考えます。

しかしATAWADは、外部の不適切なユーザーはもちろん、悪意をもった社内ユーザーが、情報システムにアクセスできるリスクも内包しています。そのためユーザーのアクセス権限を管理する、アイデンティティー管理と、ユーザーのアクセスを制御するユーザー認証の仕組みが、もっとも基本的、そして重要なセキュリティー対策となります。

@ITセキュリティセミナーリポート　働き方改革に欠かせない認証基盤とは？

認証基盤の課題を放置すると、企業競争力の足かせになりかねない

総務省の調査では約50%の企業が既に何らかのクラウドサービスを利用されている状況にありますが、多くの企業においては、まだオンプレミス上に重要な情報システム資産があるはずです。クラウドサービスだけにクローズした認証機能を利用する場合、オンプレミスとクラウドサービスの認証基盤がサイロ化することになります。

オリビエ・イサテル氏
EVIDIAN-BULL JAPAN株式会社
日本統括マネージャー／最高技術責任者

それを放置すると、ユーザーの利便性が低下するだけでなく、将来の変化に対応できない情報システムになる危険性があり、将来的に企業競争力の足かせを作ることにもなりかねません。システム環境によらないシームレスなアイデンティティー管理、ユーザー認証の仕組みの構築が、今後のデジタルトランスフォーメーションに対応するために重要な視点となります。

Evidianでは、さまざまなID管理基盤製品、そしてアクセス制御製品を用意しています。これらEvidianのソリューションによって、お客さまのビジネスの発展に貢献していきたいと考えています。

NTTコムウェア株式会社
URL：https://www.nttcom.co.jp/
WEB 掲載：2018.7