SOLUTION BRIEF

CA API Gateway と CA Single Sign-On による API セキュリティ

クラウドおよびモバイル向けに、Web を超えて API に移行する

企業は従来、組織内のサービスや慎重に管理された Web ベースのアプリケーションを使って、データやアプリケーションを公開してきました。しかし現在では、モバイルとクラウドテクノロジの台頭により、企業は新しいチャネルを開くことが求められています。API は、モバイルアプリケーションやクラウドサービスを企業のデータおよびアプリケーションと接続する新しい基盤です。API は、新しい収益モデルを実現し、企業を BYOD（bring your own device）に対応させ、既存の顧客およびパートナーとの関係の価値を強化します。

企業のデータやアプリケーションに、クラウドやモバイルデバイスからアクセスできるようになると、アプリケーション連携、セキュリティ、サービス検出、開発者管理、SLA 達成、データ分析などで課題が生まれます。

CA API Gateway は、業界最先端の API プラットフォームを提供します。CA の API Management Suite は、API を介して組織が既存のリソースをモバイルアプリケーションやクラウドサービスに安全に開放できるようにします。CA API Gateway の技術は、組織がプロトコルの採用によって既存のアプリケーションへの投資をできるようにし、外部からの脅威や不正アクセスを防ぎ、API Developer Portal を通じて新しい市場やサードパーティ開発者のネットワークを開拓します。

主なメリット / 成果

CA API Gateway と CA Single Sign-On（CA SSO）が統合されたことで、以下が可能になりました。

- **組織内 SSO の拡張：**
  既存の ID ストアを使用して、API アクセスを管理できるようにする
- **モバイルおよび BYOD への対応：**
  OAuth および OpenID のモバイル・インタフェースを公開し、企業のデータ資産へのモバイル・インタフェースに接続して組織内のアイデンティティへブリッジできる機能を提供する
- **ID ポリシーの実施：**
  CA SSO からの ID 属性に基づいて、調整ポリシーを動的に実施する

API の管理とセキュリティにおける ID の役割

ID は、エンタープライズクラスの API 管理やセキュリティの基盤です。特にモバイルアプリケーションでは、モバイルエンドユーザ、アプリケーション開発者や組織内のデータにアクセスするユーザがそれぞれ固有の ID を持ち、その ID が認証、承認、マッピング、および管理される、レイヤ化した ID モデルが必要です。ID は、このようなアクセスのルールを定義するだけでなく、拡張ユーザプロファイルや可能なアクションを定義する基盤を形成します。ルーティング、バージョン管理、トラフィックコントロール、スロットリングや調整に関する決定は、関連の ID や、トランザクションのコンテキスト情報に基づいて、すべて動的に行うことができます。

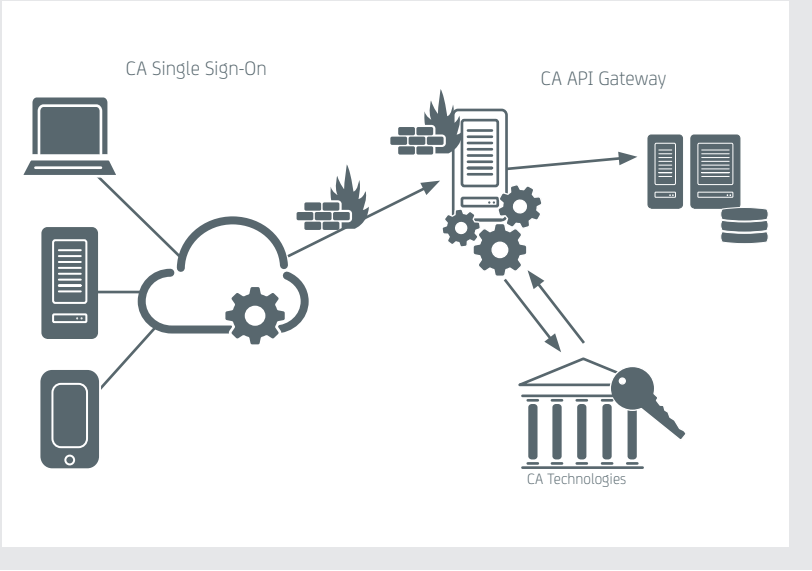
多くの企業が、安全なシングル・サインオン（SSO）を実現するため、企業内または Web ベースの ID 管理ソリューションに投資しています。CA Single Sign-On（CA SSO: 旧 CA SiteMinder）は、安全なインターネット規模の SSO および Web アクセス管理を提供し、企業がユーザを認証し、Web アプリケーション / ポータルへのアクセスを承認できるようにします。また、従業員、パートナー、サプライヤおよび顧客に、安全な SSO で、必要な情報およびアプリケーションを安全に提供できるようにします。

API 管理における ID の役割

CA API Gateway と CA SSO を合わせて使用すると、モバイルおよびクラウドを強化するイニシアチブとして、アイデンティティ中心の API 管理およびセキュリティ・インフラストラクチャを実現できます。一般的な使用事例を以下に紹介します。

- 既存の CA SSO フレームワークを使用して、Web、API、モバイル、およびクラウドで統一セキュリティ・ビューを作成する
- モバイル・アプリケーションに OAuth を公開し、ユーザ・トークンを CA SSO アイデンティティ・トークンにブリッジし、認証を委譲する

CA API Gateway と CA Single Sign-On のアーキテクチャ



CA API GatewayとCA Single Sign-Onの統合の主要な特長

アイデンティティとセキュリティ	
APIのセキュリティ	▪ APIへの脅威からの保護とデータの検証 ▪ エンドツーエンドのデータ保護とプロトコルのセキュリティ ▪ JSON/XMLコンテンツフィルタリング
拡張ID処理	▪ サービス/処理へのIDベースのアクセス ▪ APIプロバイダとサードパーティSaaSへのSSO ▪ SAML、X.509証明書、カスタムトークンのサポート ▪ OAuth連携のクライアントサポート ▪ 現在サポートされているCA Single Sign-Onの全バージョンと完全に統合 ▪ HTTPベーシック、ダイジェスト、相互SSL、Microsoft SPNEGOなどのサポート
ドキュメンテーションとリソース	▪ 開発者によるアプリケーション作成のスピードアップを助ける、インタラクティブAPIドキュメンテーション、APIエクスプローラ、サンプルコード、サンプルアプリケーション ▪ 告知、開発者サポート、FAQ、および開発者のコミュニティを育成するディスカッションフォーラムを提供
アプリケーション作成	▪ JavaScript、node.js、Python、Ruby、PHP、Objective C、JavaおよびCurlを含め、最も普及しているプログラミング言語でクライアント側コードを自動的に生成 ▪ 開発者が、1回のクリックでアプリケーションに複数のAPIの追加が可能
OAuthおよびOpenID Connect	
シナリオ・サポート	▪ 2-legged、3-legged OAuthの実装をサポート ▪ OAuthプロトコルフローのあらゆる段階（ユーザ、クライアント、認証サーバ、ランタイム、トークン検証、管理者トークン管理）に対応した機能
サポートされる標準	
XML、JSON、SOAP、REST、PCI-DSS、AJAX、XPath、XSLT、WSDL、XML Schema、LDAP、RADIUS、SAML、XACML、OAuth 1.0a/2.0、PKCS、Kerberos、X.509証明書、FIPS 140-2、XMLシグネチャ、XML暗号化、SSL/TLS、SNMP、SMTP、POP3、IMAP4、HTTP(S)、JMS、MQ Series、Tibco EMS、Raw TCP、FTP(S)、WS-Security、WSTrust、WS-Federation、WSSecureExchange、WSIL、WS-I、WS-Addressing、WS-Policy、SSecureConversation、WS-MetadataExchange、WS-SecurityPolicy、WSPolicyAttachment、WS-I BSP、UDDI、WSRR、MTOM、IPv6、WCF	

※製品の詳細情報については、弊社 Web ページ (www.ca.com/jp) をご覧いただくか、CA ジャパン・ダイレクト (0120-702-600) までお問い合わせください。

CA Technologies

〒 102-0093　東京都千代田区平河町 2-7-9　JA 共済ビル
お問い合わせ窓口：CA ジャパン・ダイレクト　0120-702-600
WEB サイト：www.ca.com/jp

お問い合わせ

2015 年 3 月現在

CS200-87730
Printed in JAPAN