TechTarget Japan SPECIAL

キーマンズネット SPECIAL

HITACHI Inspire the Next

今ある資産をつないで価値を生む

DX推進の要、API活用のセキュリティリスクと解決策は

金融機関や自治体、公共サービスなどを中心に自社システムの API 公開を進める動きが活発だ。ユーザーのインテグレーションを阻害せず、セキュリティを維持して運用するにはどういった方法があるだろうか。

日本は官民を挙げてデジタルトランスフォーメーション（DX）を急ぐ状況が続く。例えば 2019 年 12 月に改訂された内閣府「デジタル・ガバメント実行計画」に見られるように、行政機関も DX 実現を掲げて既存 IT 環境の刷新を本格化させ、民間企業にも DX 推進を促すルール作りを勧める。

サービス品質向上や外部とのコラボレーションを可能にする DX 推進で重要になるのは、確実なセキュリティ対策や安全なサービス提供だ。金融・公共機関などの組織は各監督省庁が定めるルールに準拠した運用にも対応しなければならない。ここでポイントとなるのが API を介したシステム間連携だ。重要システムへのアクセスも考えられることから、API の運用・管理には細心の注意が求められる。こうした状況に対して、積極的にグローバルな技術コミュニティーと連携し、安全な API 管理のアプローチを提案する日本企業を取材した。

API活用の2つの意義

直近で API を介したシステム連携の採用が進むのが金融業界だ。銀行などのように古くから IT を活用してきた企業では、業務の核を担うシステムがモノリシック構造だったり、改修を積み重ねたため複雑な構造になっていたりするため、モダナイズが困難といわれてきた。それでも FinTech の隆盛を受け、サービス開発の機動力を上げて DX を推進するため、コンテナ基盤を活用したシステムのマイクロサービス化やクラウドの利用、DevOps の導入といった改革が徐々に進む状況にある。


レッドハット　杉本 拓氏

2017 年 5 月に成立した改正銀行法もこうした状況を後押しする。もともとは外部アプリケーションを使ったスクレイピングによる非公式なデータ連携のリスクを回避する目的で、銀行自身に API を介した外部事業者との安全なデータ連携の基盤構築を義務付けたものだ。だがひとたび API を公開できれば、外部システムだけでなく自社も API を活用した新しいサービスやアプリケーションを迅速に開発できるようになる。

ここでは金融業界の DX の例を示したが、同じように古いシステムを抱える企業の DX は API の運用が成功のカギを握る。ポイントは API 全体をどう一元的に管理し、セキュリティやサービス品質を維持できるかだ。

こうした API 連携を支えてきたのが Red Hat と日立製作所（以下、日立）だ。Red Hat は API 連携のためのソリューション「Red Hat Integration」を世界各国の金融・公共機関などの組織に提供してきた。日立は IT ベンダー大手として金融機関をはじめ、多様な企業の重要システムの設計や運用を担ってきた。信頼性や安全性が重視されるシステムにおいて、Red Hat Integration を軸にセキュアで高信頼な API 環境を構築するソリューションを提供してきた。

レッドハットの杉本 拓氏（シニアソリューションアーキテクト）が「API はデジタル化を進める上での必須要素。企業の俊敏性を高め、市場競争力を強化します。また銀行のオープン API などからも分かるように、法律に準拠するための必須要素でもあります」と説明するように、API 連携は金融だけでなく製造、流通、サービスといったあらゆる企業にとって競争力に関わる重要なテーマだ。

API連携のための基盤製品「Red Hat Integration」

API を自社のシステム開発に組み込み、レガシーシステムのモダナイズやデジタル化による競争力強化につなげるには、どうすればよいのか。

デジタル化を推進する上での代表的な課題は「既存システムのデータを活用できない」「チャネルごとの情報に一貫性がない」

「データにリアルタイム性がない」「顧客やパートナーとの接点が限定的でビジネスの拡大が難しい」といったものだ。これらはデジタル化に限らず、何か新しい取り組みを進めるたびに直面する悩みでもある。

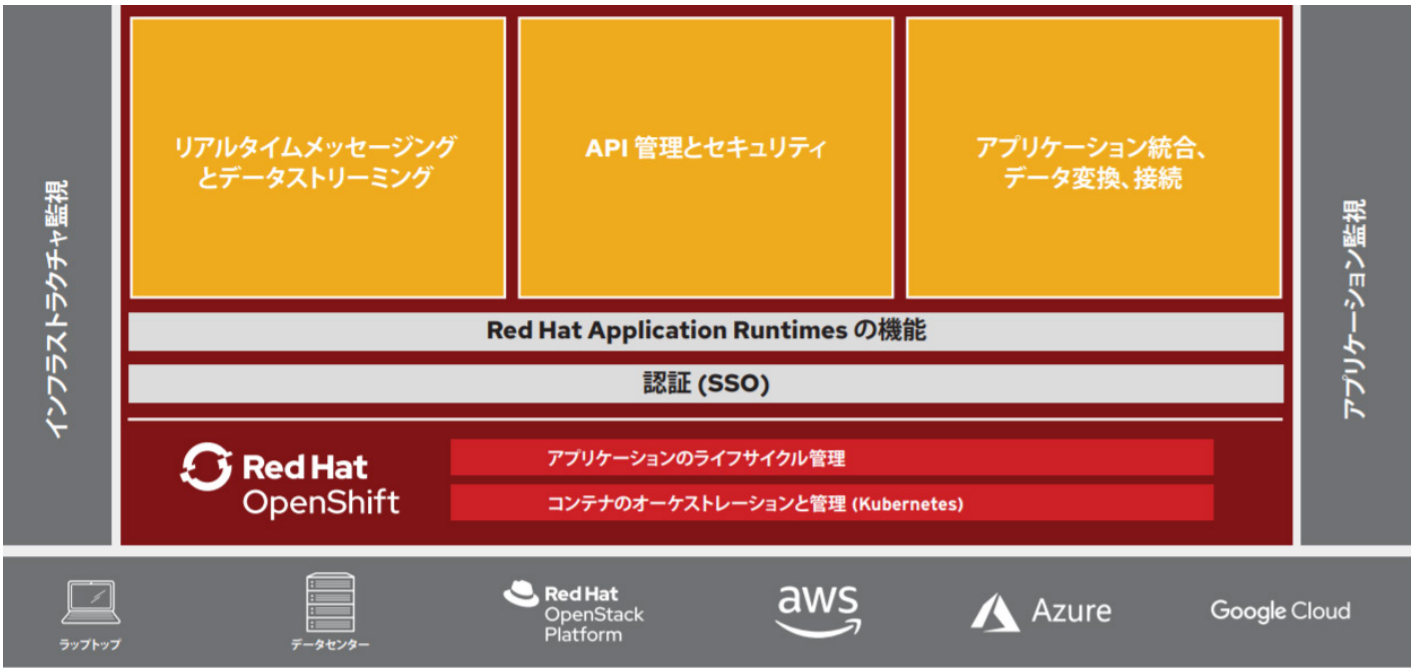
「これらの課題の根源にあるのは、システムの肥大化や複雑化、サイロ化、ブラックボックス化といった問題です。現実的な解決策は、重厚長大なシステムリプレースプロジェクトを立てるのではなく、今あるシステムを安全に運用しながらAPIによるシステム間連携を促進し、変化に対する柔軟性を高めることです」（杉本氏）

システム間連携は外部向けのAPIだけではない。同様の仕組みを社内のシステム間でも活用できれば、疎結合を維持したまま機能を活用して新しいアプリケーションを素早く開発できるようになる。

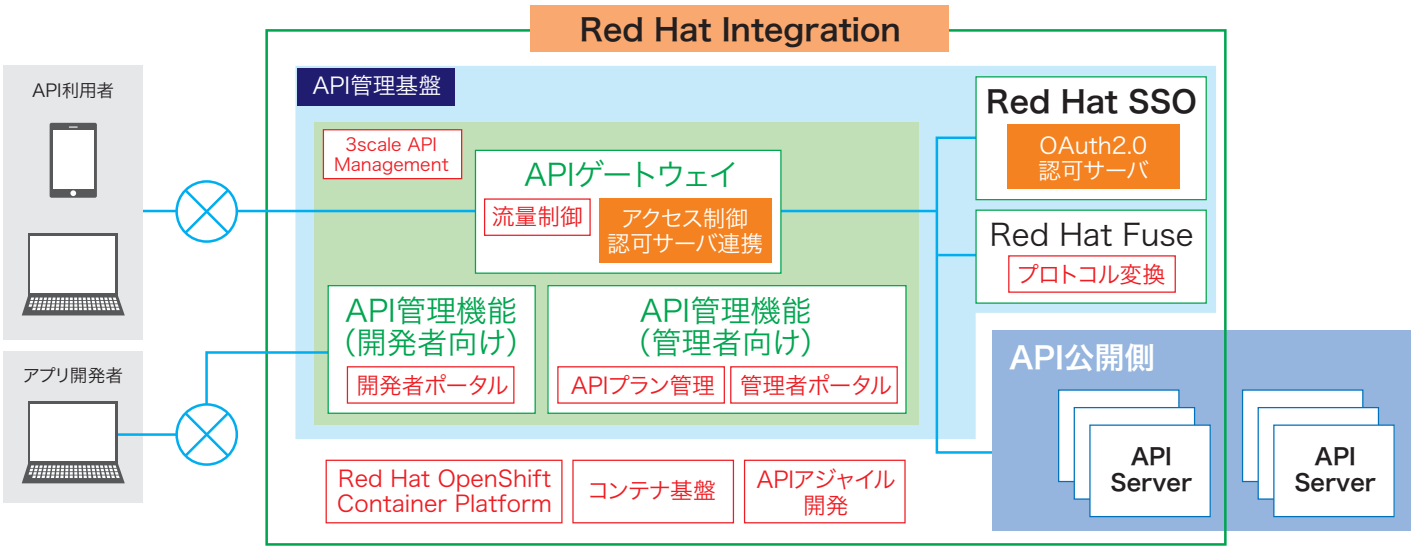
「DevOpsのようにサービスを速くリリースできるアプローチを採用し、それを実現するためのデジタル基盤に移行することも必要です」（杉本氏）

これらを実現するために、Red Hatはさまざまなミドルウェア製品を提供する。中でもAPIインテグレーションを実現するミドルウェアがRed Hat Integrationだ。

Red Hat Integrationは、サービスのメッセージを処理する「Red Hat AMQ」、サービスを連携させるハブの役割を担う「Red Hat Fuse」、APIを管理する「Red Hat 3scale API Management」の3製品とID管理製品「Red Hat Single Sign-On」（Red Hat SSO）などの周辺機能群で構成される。これらに「Red Hat OpenShift」などのコンテナプラットフォームや各種開発ツール、ビ



Red Hat Integrationの機能構成イメージ（出典：Red Hat）



Red Hat Integrationを採用したAPI管理基盤の例（出典：日立）

ジネスプロセスの自動化ツールなどを組み合わせてAPIインテグレーションを実現する。

「サービス全体のモダナイズを検討するならば、オンプレミスの既存システムだけでなく、複数のクラウドに展開するアプリケーションやサービスも含めてAPIのライフサイクル全体をカバーする必要があります。こうした運用は、基盤技術があればできるものではなく、技術を適用するためのノウハウや経験、法規制や安全性に関する規定などへの深い業界知識が重要です。この点においてRed Hatは金融、公共サービスなどで多数の実績があります」（杉本氏）

API管理や認証・認可などのセキュリティ機能開発でSSOに貢献、OAuth 2.0の課題を解決

Red Hat Integrationを活用して多くの企業のAPIインテグレーションを支援してきたのが日立だ。パートナーとしてユーザー企業の取り組みを支援するだけでなく、顧客の要望に応じてRed Hat Integrationのベーステクノロジーの開発コミュニティーにも直接携わってきた。

例えば、3scale API Managementの由来であるオープンソースソフトウェア（OSS）「3scale」やRed Hat SSOのOSS版である「Keycloak」の開発では日立の技術者が重要な貢献をしている。とりわけAPI接続時の認証手続きの実装で日立が果たした役割は大きい。

APIを活用する上で欠かせないのがセキュリティ対策だ。金融業界のオープンAPIやFinTechの取り組みでは、API公開に向けたセキュリティを確保するためにOAuth 2.0を使ったAPI連携を進めてきた経緯がある。ただ、OAuth 2.0はフレームワークであり実装方法は利用者に任されている。そのため、OAuth 2.0を実務で採用するには業界ごとの規制やセキュリティ基準に準拠した仕組みを別途構築する必要があり、リスクにもなり得る。

日立の中村雄一氏（OSSソリューションセンタ 主任技師（博士（工学））はこの点ついて「日立はOpenID Foundationが定める『Financial-grade API』（FAPI）へのKeycloakの対応に向けた実装を主導しています。FAPI対応を始めとして日本の顧客が求める安全性を実現する目的で開発したものを、KeycloakのOSSコミュニティーに還流する関係です」と技術的な優位性を強調する。


日立　中村雄一氏

日立はこうした技術的な裏付けを基に、Red Hat Integrationを使って自身の知見やノウハウを織り込んでセキュアなAPI公開基盤を日立独自の付加価値として提供している。具体的には、Red Hat Integrationを軸に、既存システムと接続するための典型的な拡張パターンをテンプレート化して提供するなどの取り組みを進める。さらに拡張のうち汎用（はんよう）的なものはOSSコミュニティに還元している。

日立とOSS開発コミュニティーとの関わりは古く、社内の技術者も積極的に開発に参加する。中村氏自身もセキュアLinuxである「SELinux」の開発メンバーであり、セキュリティとOSSの知見を生かして社内のKeycloak開発チームを率いている。

「OAuth 2.0は枠組みにすぎず、ユーザーIDだけで認証するような実装もできるため、重要システムの接続では考慮すべき点が多数あります。セキュアなAPI連携のためには、APIゲートウェイによる負荷分散や集中的なアクセス制御、適切な実装による認証および認可の仕組みが欠かせません。われわれは直接実装に携わってきた経験を生かしてニーズに沿ったセキュアなAPI公開を実装できます」（中村氏）

API連携基盤に最適なコンテナ基盤OpenShiftの魅力とは？


日立　戸部和政氏

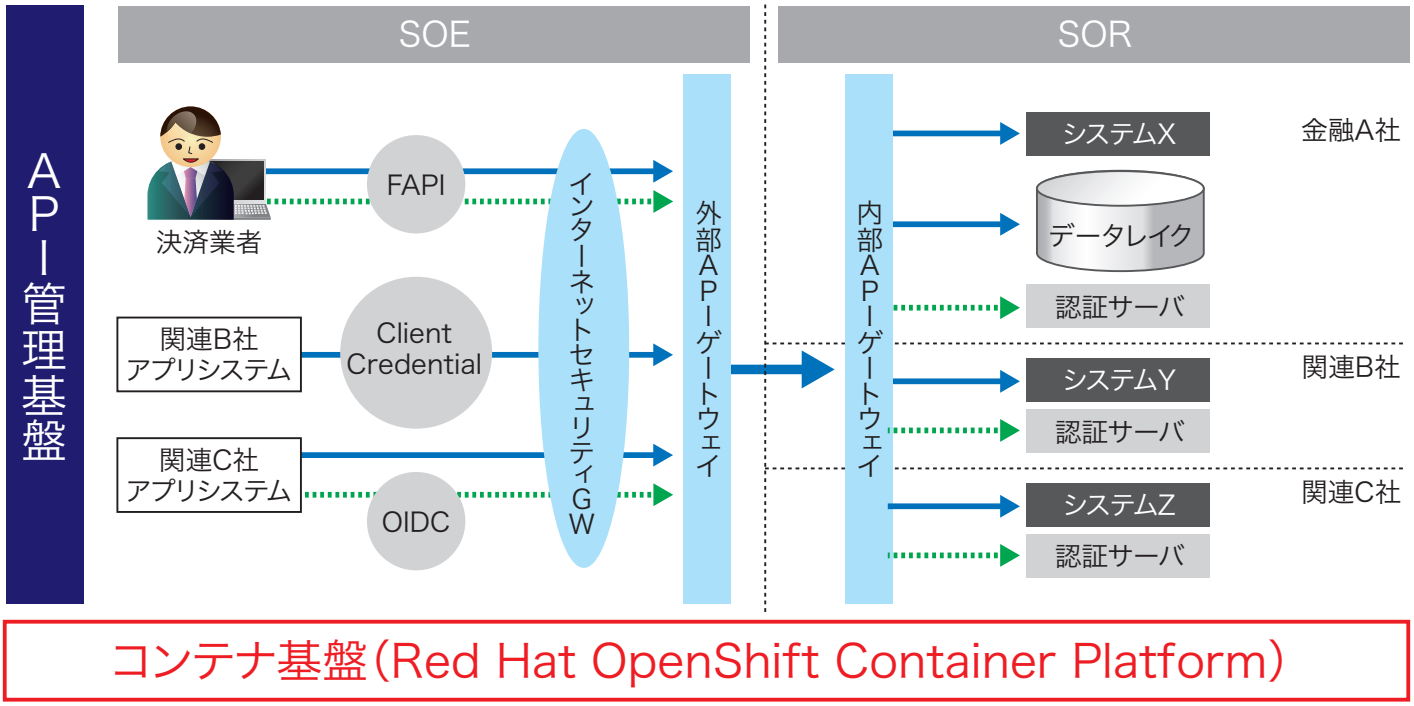
日立の戸部和政氏（プラットフォームサービス部 担当部長）はOpenShiftの魅力についてこう話す。

「DXによる新しいサービスを実現するためのシステムでは、従来型の特定の業務を密接な連携で実現するモノリシックなアーキテクチャではなく、汎用的なサービスを疎結合で連携して実現するマイクロサービスアーキテクチャ（MSA）が採用されます。MSAを採用することで、DXで求める俊敏性や変化への迅速な追従が実現できます」（戸部氏）

だたし、APIには新しいサービスを外部に公開するための外部APIと、インターネットを介さないシステム間連携をするための内部APIがあり、DXでは双方を連携しなければ企業資産を生かせない。

「SoR（Systems of Record）領域とMSAで構成するSoE（Systems of Engagement）領域のAPI公開は、それぞれ個別の取り組みではありません。DXを推進する場合、レガシーシステムと外部をつなぐ内部向けAPIと、外部の取引先とサービスをつなぐ外部向けAPIも連携を進める必要があります。こうした連携を容易にするのがOpenShiftです」（戸部氏）

内部向けAPIと外部向けAPIを異なる基盤で構築すると、両者の連携は難しくなる。特定のクラウドで特有のAPI管理ツールを用いることでそのクラウドにロックインされるリスクもある。これに対し、OpenShiftは、ハイブリッドクラウドに対応しており、HCI（ハイパーコンバージドインフラ）のようなオンプレミス環境で稼働



API 環境構築ソリューションの概要（出典：日立）

させることはもちろん、「Amazon Web Services」（AWS）や「Microsoft Azure」といったパブリッククラウドで稼働させることも可能だ。

「API とコンテナを OpenShift で統合的に管理することで、可搬性、柔軟性、拡張性、俊敏性といったコンテナのメリットを最大限に生かした API 連携が可能になります。例えば、固定的なワークロードを処理する API はオンプレミス環境で処理し、需要の変動が大きい API はパブリッククラウドにリフトするといった、クラウドリソースの活用が容易になります。さらに『JP1』と組み合わせれば、マルチクラウド、ハイブリッドクラウドでのコンテナ基盤を含む業務システム全体の稼働監視やトラブルシューティングまでの統合管理が実現します」（戸部氏）

企業が保有する IT 資産を生かしながら DX を推進したり顧客に素早く新しい価値を提供したりするのに、API を使ったシステム間連携は一つの解決策となり得る。特にビジネス環境の変化が激しい現代においては、コンテナアプリケーションへの段階的な移行と併せて API を活用するアプローチも機動力を高めるには重要な視点だ。このとき、日本企業に関する深い業務知識を持ち、開発コミュニティーに貢献して豊富なセキュリティの知識と技術力を持つ日立は大きな助けとなるだろう。

●お問い合わせ
株式会社 日立製作所 サービスプラットフォーム事業本部
〒244-0817 神奈川県横浜市戸塚区吉田町 292
http://www.hitachi.co.jp/Prod/comp/soft1/openshift/

※この冊子は、TechTarget ジャパン（https://techtarget.itmedia.co.jp/）とキーマンズネット（https://www.keyman.or.jp/）に 2020 年 6 月に掲載されたコンテンツを再構成したものです。
https://techtarget.itmedia.co.jp/tt/news/2006/16/news05.html