安全・安心なサービスを提供するアズビルのクラウド運用基盤

Azbil's cloud operation infrastructure for providing safe and secure services

野間　節 Takashi Noma
鈴木　唯一 Tadakazu Suzuki
岸　勝 Masaru Kishi
関　英信 Hidenobu Seki

キーワード
SaaS，サイバーセキュリティ，ISMS，ITIL，DevSecOps，DX

クラウドを活用したSaaS（Software as a Service）としての価値提供が増えているが，サイバーセキュリティのリスクは日々増大しており，常に変化する。リスクに応じたセキュリティ対策，そして，運用上のセキュリティ対策が必須となる。しかし，セキュリティを十分考慮したクラウドサービスを個別に構築するのは容易ではない。そこで，セキュリティ対策が整備され常にアップデートされるクラウドサービス開発・実行の共通基盤を構築した。また，運用面でのセキュリティを確保するためにクラウド運用の専門組織を設置し，ITサービスマネジメントフレームワークの活用や情報セキュリティマネジメントシステム認証取得により，常に運用上のセキュリティ向上にも努めている。さらに，商品開発プロセス全般でのセキュリティ確保，実施状況審査のための専門組織も設置した。これらクラウド運用基盤整備の取組みにより，アズビルの安全・安心なサービスが提供できており，さらに強化を続けている。

As the provision of value in the form of cloud-based software as a service (SaaS) increases, cyber security risks are also increasing day by day, and they are assuming new forms. Commensurate measures to maintain secure operation are indispensable. However, it is not easy to build an individual cloud service that adequately addresses security. For that reason we have built a common platform for cloud service development and implementation that is equipped with security measures and is constantly updated. In addition, by establishing a specialized organization in charge of cloud operational security, by utilizing IT service management frameworks, and by acquiring information security management system certifications, we are constantly striving to improve operational security. Additionally, a specialized organization has been set up to ensure security in the overall product development process and to monitor its progress. Through these efforts to enhance our cloud operation infrastructure, we have been able to provide the safety and security of Azbil's services, which we continue to strengthen.

1. はじめに

第4次産業革命やSociety5.0といわれるように，社会・産業の在り方，ニーズが大きく変化している。さらに，新型コロナウイルス感染拡大により，解決すべき様々な課題が顕在化し，新たに出現してきている。azbilグループが果たすべき役割は拡大し，価値創造の機会が増加している。azbilグループとしては，SDGsを道標として，持続可能な社会へ「直列」に繋がる貢献を目指している。

IoT，AIといった先進技術も活用した高付加価値なサービスをお客さまに素早く，ライフサイクルに応じて提供するため，そして，お客さまのシステム運用・保守コストを削減するため，azbilグループとしてクラウドを活用した価値提供を推進している。一方，クラウド上のサイバーセキュリティのリスクは日々増大し，常に変化する。リスクに応じたセキュリティ対策，運用上のセキュリティ対策が必須となる。

本稿では，安全・安心なサービスを提供するアズビルのクラウド運用基盤，およびその上で提供されているアズビルのクラウドソリューションについて述べる。

2. アズビルの取組み

クラウドサービスを安全・安心に提供するためには，まず，セキュリティ対策が十分整備された開発・実行基盤が必須である。そして，運用面でのセキュリティ対策，商品開発プ

ロセス全般でのセキュリティ確保·審査機能も極めて重要である。これらの取組みについて説明する。

2.1　クラウドサービス開発·実行の共通基盤

情報セキュリティの3原則である，可用性，機密性，完全性の要件を満たすシステム構成を，アプリケーション開発プロジェクトごとに設計，構築することは，アプリケーション開発者にとって大きな負担となるばかりでなく，設計漏れ，構築不備などを引き起こすリスクとなる。まして，クラウド利用環境でそれらを設計，構築していくことは，専門の知識を要し，アプリケーション開発における大きな足かせとなる。そこで，アズビルでは，アプリケーションの基盤となる部分を共通に設計し提供することで，アプリケーション開発時に考慮すべき構成範囲を限定させ，可用性，機密性，完全性を担保しつつ，アプリケーション開発にかかる工数の削減と，開発期間の短縮を実現している。また，この共通基盤を利用することは，運用設計，および実運用の共通化による，運用面での効率化にもつながっている。

共通基盤で提供される機能は，エンジニアリングプラットフォームとランタイムプラットフォームに大別される。本稿では，「安全·安心なクラウドサービスを提供」へ直接的に寄与する，ランタイムプラットフォーム部分について説明する。ランタイムプラットフォームでは，安全に，かつ高可用性を担保するコンテナ（Docker）オーケストレーション環境を提供している。アプリケーションサービスとして作成されたコンテナは，この基盤上で動作させることにより，安定稼働のための構成とコンテナ管理の機能が享受される。

次に，安定稼働のために欠かせないセキュリティリスクに対する基盤側の対策としては，サービス提供の外界との境界線である，入口と出口に徹底した入口対策と出口対策を共通基盤として構築し，運用での監視，管理を行っている。これらの入口，出口対策は，設計や構築が難しいばかりでなく，徹底したセキュリティ対策を行うためには大きな初期導入コストと運用コストを必要とする。これらを単独のアプリケーションで実施することは，そのためのコストがアプリケーションサービス提供コストにそのまま反映されてしまい，ビジネス面での重荷になりかねない。そこを共通基盤として提供することで，複数のアプリケーションで分割して負担することが可能になり，セキュリティとコストの相反する2つの要求を同時に実現している。

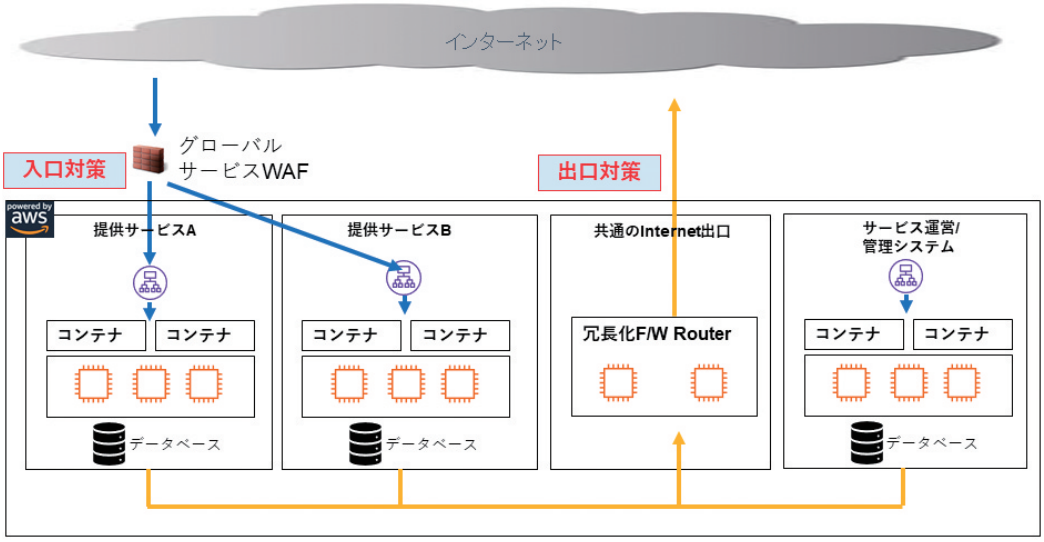

図1　全体構成図

2.2　クラウド運用センター

クラウドサービスは，従来の売り切り型の商品とは異なり，サービスを提供した後もお客さまが安全·安心にサービスを利用し続けられるよう維持する必要がある。これまでアズビルではクラウドサービスの運用を各部門が実施しており，そのノウハウも各部門内に閉じていた。この状況は，個別最適の観点では有効に機能していたが，今後クラウドサービスを拡充していく中では，アズビルとしてお客さまに均質なサービスを提供する，という観点で課題が残る。この課題を解決し，azbilグループのクラウドサービスをより安全·確実に提供可能とするための専門組織としてクラウド運用センターを2019年4月に設置した。

均質なサービスを提供するための取組みの一例として，プロジェクトの企画段階で運用に関する機能要求を提示するという活動を行っている。従来，企画段階では運用に関する機能要求が明確になっておらず，そのため，運用に関する機能の実装状況は各サービスにより異なっていた。各サービスの運用差異は人手でカバーすることとなり，運用コストの増大はもちろんのこと，作業ミスによるインシデント発生のリスクも大きくなる。運用機能を統一することで各サービスの運用品質を均質化することができ，その結果，サービス提供開始時から安全·安心にサービスを提供することが可能となる。また，これらの活動を通じて，運用業務の重要性を関係者に周知することにより，運用部門にも適切に情報が展開され，お客さまからの問い合わせ情報の集約やインシデント発生時の迅速な対応などを可能としている。

そのほかにも，各種セキュリティ施策や運用施策を実施することで，確実な運用を担保している。これらの概要を図2，図3に示す。

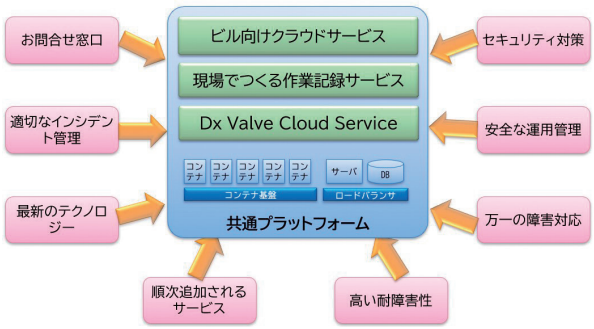

図2　共通基盤運用イメージ

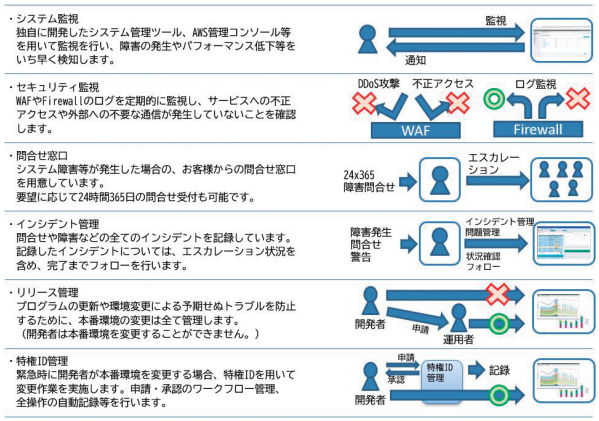

図3　主な運用業務

2.3　ITIL（ITサービスマネジメントフレームワーク）

顧客が安心してサービスを利用可能とするためには，各種の運用業務を確実に遂行する必要がある。そのため，クラウド運用センターではITIL（IT Infrastructure Library）を参考にして各種運用業務の設計を行っている。 ITILとはITサービスマネジメントのベストプラクティスを体系化したガイドラインであり，ITILを参考にすることにより短期間で効率的に運用体制や仕組みの構築が可能となる。

ITILは戦略・設計・移行・運用・継続的な改善という，ITサービスのライフサイクル全体を視野に入れているため，運用に適用するだけではその効用を十分に享受できない。そこでクラウド運用センターでは，ITILの知見を企画・開発などの関係者に対しても展開し，ITサービス全体でITILを活用可能とするための活動も行っている。当初はITILという言葉も知らない状態であったが，現在ではサービスカタログの作成など具体的な活動が行われる状況になりつつある。ITILの知見が浸透することで，ITサービス全体として，顧客満足度の向上を図ることが可能となると考えている。

2.4　ISMS（情報セキュリティマネジメントシステム）

クラウドサービス利用者の最大の懸念事項として情報セキュリティが挙げられる。サービス提供者は，利用者の不安を解消する取組みを実現し，明示することが重要である。そのため，クラウド運用センターでは情報セキュリティの国際規格であるISMS認証（ISO27001）およびクラウドセキュリティ認証（ISO27017）を取得している。認証の取得にあたっては，適合状況の確認，各種セキュリティ対策の拡充，関連ドキュメント類の整備，利用規約内容の調整など，整備には多くの時間を費やしたが，その結果として，よりセキュアな運用が行える状態を実現することができたと考えている。

情報セキュリティインシデントは，万が一にも発生してはならないものであり，各種認証を取得すれば大丈夫というものではない。時間の経過とともに，情報セキュリティを担保するための運用が形骸化してしまいインシデントを防止できなくなる恐れもある。そのため，クラウド運用センターでは，ISMS教育の実施や，定期的な改善活動を行うことで，情報セキュリティに対しての高い意識を維持し，よりセキュアな運用を目指す活動を行っている。

CLOUD 722670
IS 722669

図4　ISMS 27001，27017認証取得

2.5　サイバーセキュリティ審査室

当社が販売しているまたは今後販売予定の商品（製品やクラウドサービス等）のサイバーセキュリティ確保を確実に遂行していくための専門組織として，商品サイバーセキュリティ審査室を2019年4月に設置した。商品のサイバーセキュリティの確保とは，「サイバー空間における，商品の可用性，完全性，機密性，真正性，責任追跡性，否認防止，信頼性などを喪失しないよう保護し，また維持すること」と定めている。

この組織を中心とした商品のサイバーセキュリティ確保の取組みは，

①商品におけるライフサイクル全般でのサイバーセキュリティ確保を実践していくための規則および方針の整備
②商品開発プロセスにおけるサイバーセキュリティ確保活動およびその実施状況の審査
③販売商品における脆弱性情報の収集および対応の推進

などである。商品のサイバーセキュリティ確保を適切かつ効率的に実現するためには，商品企画から開発・保守へと長期間にわたるライフサイクル全般に関わるすべての担当者にサイバーセキュリティ確保の重要性を認識してもらい，それぞれの業務タスクの中でサイバーセキュリティ確保を意識した活動を実施し，一丸となって取り組む必要がある。

まず商品開発プロセスにおいて，従来の開発プロセス標準や実践活動に加えて，サイバーセキュリティ確保を意識した継続的なプロセスの見直しを実施した。見直し項目は，サイバーセキュリティリスクアセスメントに基づく，サイバーセキュリティ要件の検討，セキュアな設計および実装，それらの妥当性検証，含有するサードパーティコンポーネント等の脆弱性情報対応など，多岐にわたる。プロセスの標準化については，様々な規格やガイドラインを参照し，作成した。これらの方針や標準は，定期的に開催している全社的な，商品のサイバーセキュリティを強化する会議で随時展開している。

次に商品のライフサイクル全般におけるサイバーセキュリティ審査については，当社で開発·販売しているクラウドサービスを中心にまずは実施している。このクラウドサービスについては，サービス提供開始後の運用上のセキュリティが特に重要であると考えている。

商品に含まれるサードパーティコンポーネントの脆弱性情報については，脆弱性情報対応要領標準を策定し，これに沿った活動が定期的に実施されている。

以上，これまでの取組みの中で見えている次のような課題に対して，PDCAをしっかり回しながら，改善していく。

- サイバーセキュリティ確保の対策実装および検証が効率的に開発プロセスに組み込めていない。
- 商品企画開発者のサイバーセキュリティ確保の意識向上への活動がまだまだ不足している
- 商品リリース後のサイバーセキュリティ確保の維持·向上活動についての認識が薄い

これらの改善とともに，商品開発·改善スピードを加速していくために，図2のイメージ図にも示しているように，商品の開発や運用の企画設計段階からセキュリティを考慮するDevSecOpsの導入·実践，開発プロセスにサイバーセキュリティ診断ツールを組み込み，さらなる自動化の推進，サイバーセキュリティ確保を意識して実現できる人材の育成，情報処理安全確保支援士資格取得の加速化などを進めている。今後もお客さまに安心して当社商品をご利用していただけるよう，改善していきたい。

3. アズビルのクラウドサービス

次に，アズビルのクラウド運用基盤上で提供されている，クラウドサービスについて紹介する。エネルギー，設備，品質の監視·管理クラウドサービスとして，ISMS27017クラウドセキュリティ認証を取得している。

3.1 ビル向けクラウドサービス

クラウドサービスの特長を活かし，ビルオーナーだけではなく，オフィスで働く人々やビル管理者等，ビルに関わるあらゆる人々がそれぞれの目的に合わせて，時間や場所を選ばずにサービスを利用することができ，関係者間での情報共有も促進できる。

ビルオーナーやビル管理者には，ビルのエネルギー管理や設備管理業務の効率化を提供し，管理コストの削減を実現する。居住者にとっても，空調·照明のON/OFF，設定変更等をPC，タブレット，スマートフォンから簡単に行うことができる。居住者の「暑い」「寒い」といった温冷感に基づいて設定温度を変更することもでき，執務環境の向上を支援する。また，エネルギーの見える化により省エネ活動促進，意識の啓もう活動に役立てることができる。

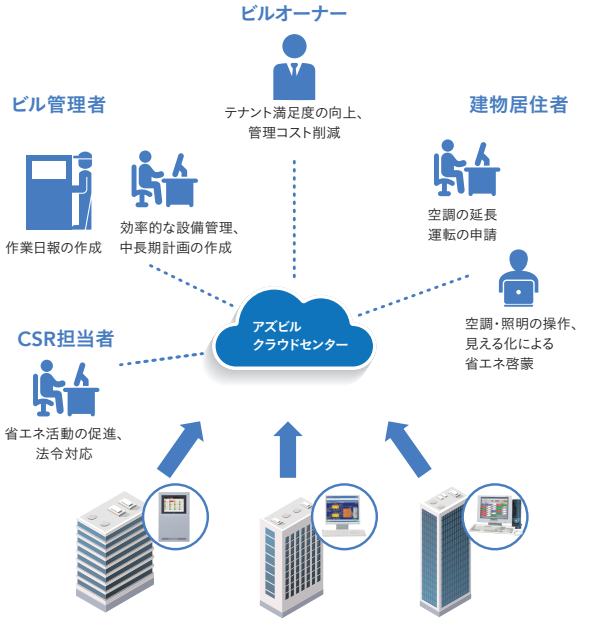

図5　ビル向けクラウドサービスの利用場面

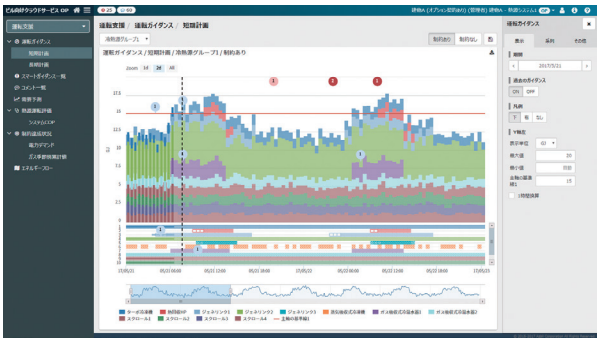

図6　エネルギー管理画面事例(熱源最適運用)

3.2 現場でつくる作業記録サービス[注1]

現場に数多く残る，紙に手書きで記録している作業を，簡単，スマートにデジタル化するためのクラウドサービスである。クラウドサービスの特長である，ハードウェア資産が不要で，自社に運用者を必要とせず，必要なときにすぐに始められるという柔軟性を活かしたサービスである。

製造·メンテナンスの現場などをはじめとする，幅広い各種業務での手書き作業を，PC，スマートフォンやタブレットを使ってその場でデジタル化し，そしてクラウドに保存できる。テキスト，数値，日時などのデータに加えて，その場で撮影して画像として記録することができる。

注1　詳しくは本冊子p.23をご覧ください

図7　手書き記録作業をデジタル化

それぞれの業務用途に合わせた記録画面の構築を，ドラッグアンドドロップ・文字入力といった簡単な操作だけで実現できる。また，紙の記録では不可能だったQRコードやバーコードからのデータ取得，画像の記録など，モバイルならではの多彩な入力フォーマットによる情報収集機能を利用することが可能である。

直感的な操作で記録を行えるので，ミスの削減や作業時間短縮につながる。その場でデータ化し，クラウド保存することで，リアルタイムに情報共有し現場の状況を把握することができる。データを活用することで現場の状況を正しく把握でき，業務の改善やDXに繋げることができる。

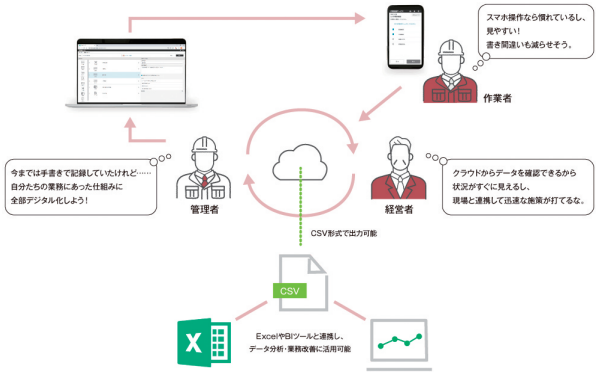

図8　作業記録サービスの利用場面

3.3　Dx Valve Cloud Service[注2]

調節弁メンテナンスサポートシステム PLUG-IN Valstaff（以下Valstaff）で収集したバルブの稼働データをクラウド上に自動送信・解析を実施する。顧客は，クラウドサービスの特長を活かし，「必要なトキに」「必要なカタチで」「必要なシーンで」診断結果を確認できる。従来，日常的にバルブの健全性を確認するためには，Valstaffに蓄積する稼働データを顧客が日々確認や評価をする必要があった。Dx Valve Cloud Serviceは，顧客が稼働データの確認や評価をしなくても診断データからバルブの異常早期発見や異常進行予測の確認が可能となり，生産設備の安定化や保安力強化に貢献する。概要を図9に示す。

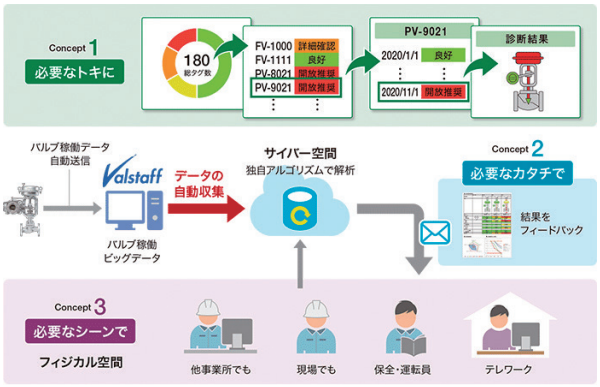

図9　Dx Valve Cloud Serviceの利用場面

4. おわりに

azbilグループ各社ではクラウドサービスを活用した価値提供をさらに加速している。そのために必須となるクラウド運用基盤を，継続的にさらに強化していく。

そして，アズビルのクラウドサービスをより多くのお客さまに安全・安心にご活用いただければと願っている。お客さまのパートナーとしてデジタルトランスフォーメーション（DX）推進をサポートし，事業環境の変化に迅速に対応できるよう貢献したい。

＜著者所属＞
野間　節　　アズビル株式会社
クラウド運用センター
鈴木　唯一　アズビル株式会社
クラウド運用センター
岸　勝　　アズビル株式会社
IT開発本部 IT開発1部
関　英信　　アズビル株式会社
商品サイバーセキュリティ審査室

注2　詳しくは本冊子p.30をご覧ください。