rubrik

ランサムウェア対策を強化したプライベートクラウド「USiZE」が実現する日本企業のための「データ主権」

SCSK

業界:テクノロジー

導入前の課題:

- SCSKのクラウドサービス「USiZE」のリニューアル
- USiZEバックアップサービスの品質・性能に関する課題の解消
- バックアップソリューションに対する国内サポート

導入効果:

- 高度なサイバーセキュリティレジリエンスが担保されたバックアップを実現
- Anomaly Detectionによりランサムウェアの迅速な検知が可能に

ITトランスフォーメーションの成果:

USiZEのバックアップサービス基盤をRubrikアプライアンスにより刷新し、バックアップ取得時間を大幅に削減するとともに、上書きや削除ができないイミュータブル(変更不可)なファイルシステムによりバックアップデータの保護を強化。さらに、Rubrik Security Cloudを活用し、ランサムウェアによる被害の検知・初動対応を自動化する「USiZEランサムウェア対応サービス」の提供を開始しました。Threat Hunting(脅威ハンティング)を活用し影響範囲の特定から復旧までを網羅するサービスも計画中です。

2024年4月、SCSK のクラウドサービス「USiZE」がリニューアルしました。ブランドロゴも一新したUSiZEは、「ソブリンクラウド」「ハイブリッドクラウド」の2軸でより顧客価値の高いサービスへの進化を指向しています。新たにRubrikを採用することで、SCSKがソブリンクラウドの要件として考えるデータセキュリティを大幅に強化。SCSKはRubrikのテクノロジーを全面的に活用し、顧客のバックアップデータを対象に、攻撃されたデータやファイルを検出・対処する「USiZEランサムウェア対応サービス」の提供を開始しました。

Rubrikを採用しUSiZEのバックアップサービス基盤を刷新

2004年にリソース占有型マネージドクラウドとしてサービスを開始した「USiZE」は、常に最新のテクノロジーを採り入れながら進化し、多様化する顧客ニーズに応え続けています。SCSKは、USiZEのサービス開始20年を機に大幅なリニューアルを行い、サービスの強化・拡充を図る戦略を打ち出しました。USiZEサービス部 部長の豊口博文氏は次のように話します。

「企業が自社のデータを自社の意思で管理・コントロールできる『データ主権』の確保は、経営課題として広く認識されるようになりました。サイバー攻撃による被害の増大、地政学的リスクの高まりなど、様々な環境変化がその背景にあります。国内の事業者が運営してセキュリティ面での安全性が確保され、他国の法令の影響を受けない『ソブリンクラウド』へのニーズはますます高まっていくものと考えています」

国内企業であるSCSKによる運営、最高水準のファシリティを備えた自社データセンター「netXDC」、高速かつセキュアな閉域網「SCNX」、強化されたデータ保護とランサムウェア対策など――USiZEが備える資質は、まさに日本企業の「データ主権」へのリアルな要求に応えるものです。USiZEサービス部 第一課の藤田利一氏は次のように話します。

「リニューアルに先立って『Rubrikバックアップアプライアンス』を導入し、USiZEのバックアップサービス基盤を刷新しました。これにより、データ保護とランサムウェア対策を大幅に強化しています。データバックアップの高速化と安全性・確実性の向上を図るとともに、上書きや削除ができない『イミュータブルなファイルシステム』を利用してランサムウェアによる暗号化を不可能にしたことがポイントです」

さらにSCSKは「Rubrik Security Cloud」を活用した革新的なサービスを開発。2024年5月に「USiZEランサムウェア対応サービス」として提供を開始しました。

「USiZEランサムウェア対応サービス」を新たに開発

Rubrik Security Cloudは、最先端のデータ保護、バックアップデータの脅威分析、データセキュリティ耐性、サイバーリカバリ機能を備えたサイバーレジリエンスソリューションであり、Rubrikによるクラウドサービス(SaaS)として提供されます。これを

活用した「USiZEランサムウェア対応サービス」は、USiZEにおけるデータ保護をいっそう強固なものにしました。USiZEサービス部 第一課の田中直樹氏は次のように説明します。

「ソブリンクラウドを実現する上で、データセキュリティの強化、中でも近年の最も大きな脅威であるランサムウェアへの対策は必須でした。私たちが着目したのは、Rubrik Security Cloudが提供する『Anomaly Detection（機械学習による異常検知）機能』です。バックアップデータを分析し、ランサムウェアによる被害を受けたデータが存在することを検知していち早く通報することで、お客様のビジネス影響を最小化できると考えました」

Anomaly Detectionでは、Rubrikが取得したバックアップのメタデータを独自の機械学習モデルが分析し、ランサムウェアにより暗号化されたシステムやファイルを高精度に検出・可視化。これにより、ユーザー企業の迅速なデータ復旧に大きく貢献します。

「通報を受けたお客様は、USiZEの管理ポータルからバックアップの実行停止、バックアップデータの保持、ネットワークの遮断を行っていただけます。これらの手順を自動化するサービスの提供の準備も進めています。Rubrikより提供されたテスト環境とシミュレーションツールを利用することで、Anomaly Detectionの評価やサービスプロセスの開発を効率的に進めることができました」（田中氏）

「次のステージでは、Rubrikの『Threat Hunting機能』を利用して、SCSKグループのセキュリティチームと連携し、『データ復旧支援サービス』の提供を目指しています。Threat Huntingでは、最初に感染したのがどのファイルか、いつ感染したのかを明らかにし、データ復旧に使用可能なクリーンなバックアップデータを正確に特定できます。この優れた機能をUSiZEのサービスとして作り込み、新しい価値としてお客様に提供していく計画です」と豊口氏は話します。

「ハイブリッドクラウド」で柔軟にバックアップ先を選ぶ

データ転送利用料が不要な「USiZEクラウドストレージサービス」、閉域網からセキュアにパブリッククラウドを活用できる「USiZE Cloud Extension」など、SCSKは「ハイブリッドクラウド」を強化するサービスの拡充にも積極的です。

「Rubrikアプライアンス、USiZEクラウドストレージサービス、パブリッククラウドなど、バックアップデータの置き場所をお客様がより柔軟に選択できるようにしていきたいと考えています。それぞれにRubrik Security Cloudを適用して、サイバーレジリエンスを強化することがポイントです」（豊口氏）

データバックアップは、様々なリスク・脅威に晒されている企業にとって、ビジネス継続のためのまさに「最後の砦」です。Rubrikは、強固なデータ保護と最先端のサイバーレジリエンスソリューションの提供を通じて、リニューアルしたUSiZEの顧客価値向上に貢献しています。豊口氏は、「生まれ変わったUSiZEはさらにビジネス成長を加速させていく」と話しつつ次のように結びました。

「USiZEランサムウェア対応サービスの報道発表では、お客様から想像以上の反響をいただきました。Rubrikのソリューションは、USiZEにおけるデータ主権を確保するとともに、高い性能と品質でデータ保護の安心・安全を支えており、『攻めと守り』を両立させたUSiZEへの信頼感をさらに高めてくれるものと期待しています。Rubrik Japanには、これからも適切なアドバイスと継続的な技術支援を期待しています」

SCSK株式会社
ソリューション事業グループ
クラウドサービス事業本部
USiZEサービス部
部長　豊口博文氏

SCSK株式会社
ソリューション事業グループ
クラウドサービス事業本部
USiZEサービス部 第一課
藤田利一氏

SCSK株式会社
ソリューション事業グループ
クラウドサービス事業本部
USiZEサービス部 第一課
田中直樹氏

ルーブリック・ジャパン株式会社
〒105-0001
東京都港区虎ノ門1-10-5
KDX虎ノ門1丁目ビル11F

お問い合わせ先
japan-info@rubrik.com
050-3733-1850
www.rubrik.com/ja/

ルーブリックは、インスタント・アプリケーション・アベイラビリティにより、ハイブリッド・クラウド環境における確実なリカバリやデータ検索、そしてクラウド化への対応が可能となります。市場をリードするCloud Data Management プラットフォームは、わずか数秒でセルフサービスによるアクセスや、自動的な保護ポリシーの適用、大規模なアプリケーションデータの検索や分析、さらにはランサムウェアからのリカバリなどを実現し、エンタープライズ環境におけるデータ保護やアプリケーションのさらなる活用をもたらします。

202409-01