

Zaif

管理者でもデータが改ざんできないRubrikで顧客の暗号資産をランサムウェアから守る

イミュータブル

管理者によるデータの改ざん・消去を徹底拒絶

論理的エアギャップ

完全に独立したクラウドでデータを隔離保護

クリーンな復旧

被害範囲を特定し、再感染リスクを排除して復旧

課題

- ✓ 厳格なセキュリティと内部統制への対応
- ✓ 進化するランサムウェアへの対策
- ✓ 顧客資産の保護と事業継続性の確保

ソリューション

- ✓ 機密性・完全性を担保したデータバックアップと即時復元
- ✓ データをイミュータブル(不変)な状態で保持
- ✓ 被害範囲の特定とクリーンな復旧ポイントの選定

効果

- ✓ クラウド上の自社環境が侵害されてもバックアップを保護できる
- ✓ ランサムウェアの手が及んでも、データ破壊や暗号化を拒絶する
- ✓ クリーンな復旧ポイントまで遡ることで、再感染リスクを防止

日本で歴史のある暗号資産交換所の一つとして、独自の事業やサービスを展開しているZaif(ザイフ)。ビットコインなどの暗号資産の売買サービスのほか、ユーザー同士が暗号資産を売買する取引所も運営しています。国の認可を受けてサービスを提供する暗号資産取引所は、ユーザーが取引口座に保有する資産や取引履歴などのデータを厳格に記録・保存し、取引のたびにいつでも利用できるようにしておかなければなりません。万が一、サイバー攻撃などによってデータが消失、あるいは改ざんされるといった事態が発生すると、ユーザーに大きな損失をもたらし、社会からの信頼を著しく損なってしまふ恐れがあります。そうした事態を避けるため、Zaifは、たとえ脅威に侵入されても、データを強固に守り、ビジネスを速やかに復旧できるRubrikを採用しました。

Zaif

社名
株式会社 Zaif

URL
<https://zaif.jp/>

業界
暗号資産取引所

従業員数
26名
※2025年9月30日現在

十数年にわたって暗号資産交換所を運営 業界に先駆けて革新的なサービスを生み出す

近畿財務局長第00001号として登録され、十数年にわたって事業運営してきたZaifは、日本で歴史ある暗号資産交換所の一つです。

老舗であるだけでなく、ユーザー同士が売買する「板取引」を長年にわたり提供するほか、コイン積立やステーキングなどといった新しいサービスも積極的に展開しています。そんなZaifのサービスをさらに進化させ、ユーザーを増やす追い風となりそうなのが、国による規制の枠組みの見直しです。

「現在、暗号資産の取引は資金決済法に基づき提供されていますが、暗号資産を新たな金融商品として位置づけ、金融商品取引法(金商法)の枠組みで規制すべきではないかという論議が国会で繰り返されています。早ければ、2027年度中にも、暗号資産取引の規制に金商法が適用される可能性も議論されています」と語るのは、同社 プロダクト企画開発部 部長の佐古夏樹氏です。

“

暗号資産取引が普及するためには、お客様に安全だと感じていただけることが不可欠です。ランサムウェア被害が多発する中、安全性を担保するためのソリューションとして選んだのがRubrikでした。

株式会社Zaif プロダクト企画開発部 部長 佐古夏樹氏

取引を規制する枠組みの移行によって セキュリティ対策の要求レベルが高まる可能性

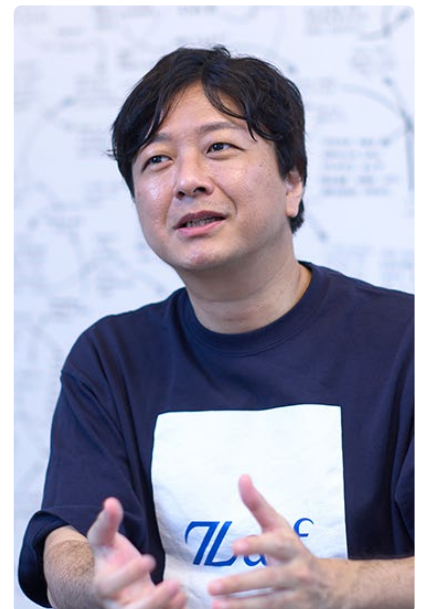
資金決済法の下では、暗号資産取引による利益は原則として雑所得と見なされ、最大55%の総合課税が適用されますが、現在、暗号資産交換業界全体で他の金融商品と同様の申告分離課税(20%)への移行が要望されており、実現すれば投資家の税負担が適正化されます。

その結果、市場参加者が増え、取引が活発化する可能性も高まるので、暗号資産取引所にとっては追い風となる可能性があります。

一方で、取引を規制する枠組みが資金決済法から金商法に移行すると、暗号資産取引所には、より厳格なセキュリティと内部統制が求められるようになるはずです。中でも要求レベルが格段に高まると見込まれるのがセキュリティ対策です。

「あらゆる操作や挙動をログとして記録し、後から確実にチェックや監査ができる体制を整える必要があると考えています」と語るのは、同社 プロダクト企画開発部 エンジニアリングマネージャの湯瀬淳也氏です。

ただし、新たな法令に準拠するだけでは、セキュリティ対策としては不十分です。なぜなら、サイバー攻撃の手口は刻一刻と巧妙化し、どんなに万全と言われる防御策を講じても、新たな技術や手法によって、いともたやすく打ち破られてしまうケースが後を絶たないからです。



管理者が意図的に削除することは不可能 完全に独立したアカウントにデータを保存できる

とくにZaifが懸念しているのが、近年激増しているランサムウェア被害です。

「厳格なアクセス制限を行っても、ランサムウェアが当社の人間になりすましてシステムに入り込んだら、お客様の資産データや取引履歴、残高情報といった重要な記録が失われたり、改ざんされたりする恐れがあります。これは絶対にあってはならないことです」(佐古氏)

そうした事態が起こればサービスが提供できなくなり、社会からの信用を失うことにもつながりかねません。「だからこそ、お客様からお預かりしている資産とデータを確実に守るため、進化する脅威に対して常に先手を打つことで、データ保護体制を強化するという経営判断に至りました」と佐古氏は説明します。

安全なデータ保護を目指してZaifが2026年1月からの検証を経て、現在導入を進めているのが、Rubrikです。

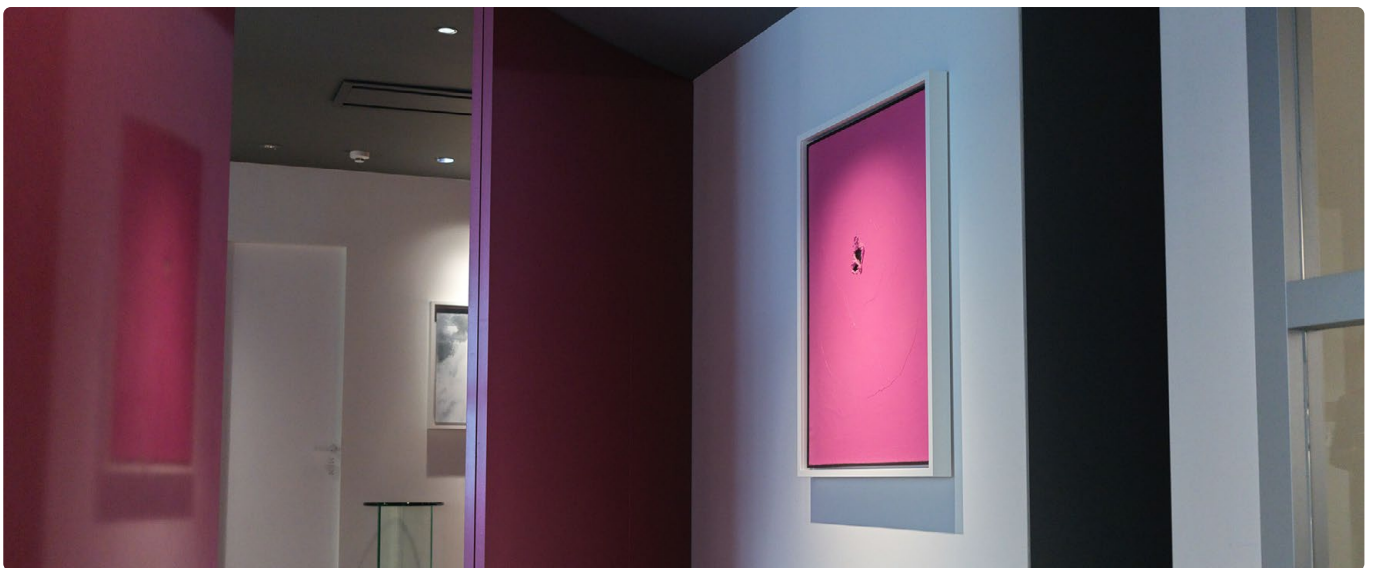
数あるデータ保護ソリューションの中からRubrikを採用した最大の決め手は、「管理者が意図的に削除しようとしてもできない仕組み」が実現できたことでした。そもそもRubrikは、ハイパースケーラーなどのクラウド上で保存したデータを、機密性と完全性を担保した状態でバックアップ・即時復元できるソリューションです。ハイパースケーラーが通常機能(ネイティブ)で提供するバックアップ機能は、データが自社アカウント内にとどまるため、ランサムウェアなどに管理者権限を奪取されると、データを消去・改ざんされてしまう恐れがあります。

「その点、Rubrikのバックアップ用クラウドストレージであるRCV(Rubrik Cloud Vault)は、同社が管理する完全に独立したアカウントにデータを保存するので、自社環境が侵害されてもバックアップには被害が及びません。この『論理的エアギャップ』を確保できる点が選定の決め手となりました」(湯瀬氏)

“

データをイミュータブル(不変)な状態で保持できるバックアップ製品で最も優位性が高いと判断したのが、Rubrikでした。

株式会社Zaif
プロダクト企画開発部
エンジニアリングマネージャ
湯瀬 淳也 氏



“

暗号資産は、預金や株と違って、一度流出したら取り戻すのが極めて難しい資産です。だからこそ、データ保護のための取り組みは徹底的に行わなければなりません。今後も Rubrik をさらに活用するなど、セキュリティの強化に取り組み続けます。

株式会社 Zaif プロダクト企画開発部 部長 佐古夏樹 氏

脅威検出や脅威ハンティングの機能が利用できる Enterprise Edition を採用

さらに Zaif が着目したのは、Rubrik には、万が一、RCV にまでランサムウェアの手が及んだとしても、データの破壊や暗号化を拒絶する技術が採用されている点です。「管理者になりすましてデータに手を加えようとしても、指示をすべて跳ねのけるので、二重、三重の防御の壁を築くことができます」(湯瀬氏)。

ちなみに Rubrik には、基本的なデータ保護および管理機能を提供するエントリーレベル Foundation Edition のほかに、より多彩で高度な機能が利用できる Enterprise Edition と呼ばれるサブスクリプションパッケージがあります。

Zaif は、Foundation Edition には含まれていない Anomaly Detection (ふるまい検知) や Threat Monitoring (脅威検出) そして、Threat Hunting (脅威ハンティング) という機能が利用できることから Enterprise Edition を採用しました。

これらの機能は、ハイパースケーラー上に保持しているバックアップデータにマルウェアや不審なファイルが潜んでいないかどうかを自動監視し、感染していた場合は、過去のバックアップに遡って、いつ感染したのか? どの範囲まで被害が及んでいるのか? といったことを特定します。これによって「クリーンな復旧ポイント」の選定が可能となり、再感染のリスクを抑えられるのです。

Zaif による Rubrik を活用したデータ保護の取り組みは、他の暗号資産取引所や金融業界全体にとっても、大いに参考になりそうです。

“

『改ざんされていないクリーンなデータが確実に存在する』と証明できることは、お客様への迅速な情報提供や、資産保護のためにも非常に重要です。そのため、我々のような暗号資産取引所にとっては必要不可欠な機能だと判断して、Enterprise Edition を選びました。

株式会社 Zaif
プロダクト企画開発部
エンジニアリングマネージャ
湯瀬淳也 氏



Rubrik Japan 株式会社
<https://www.rubrik.com/ja>

ご質問・お問い合わせ
<https://www.rubrik.com/ja/contact-sales>



サイバーセキュリティ企業である Rubrik は、世界のデータを安全に保護することをミッションとしており、The Zero Trust Data Security™ の先駆者として、企業がサイバー攻撃、悪意のあるインサイダー、および業務の中断に対するビジネスの回復力を達成できるよう支援します。機械学習を活用した Rubrik Security Cloud は、オンプレミス、クラウド、および SaaS アプリケーション全体のデータを安全に保護します。また Rubrik は、データの安全性を維持し、厳しい条件下でのデータの可用性を実現するとともに、データのリスクと脅威を継続的に監視し、インフラストラクチャが攻撃された場合でもデータと共にビジネスの復旧を支援します。

Rubrik は Rubrik, Inc. の登録商標です。本ドキュメント中に記載された会社名、製品名などは、各社の登録商標 または 商標です。