

サステナビリティ ERPを守る、クラウドセキュリティ BoostがWizで実現した アジリティと信頼の両立



会社名

Boost株式会社

産業

ソフトウェア

リージョン

日本

WIZ製品

Wiz Cloud

クラウドプラットフォーム

AWS

サステナビリティ領域のSaaSを提供するBoostは、クラウド環境のセキュリティ管理で生じていた複数ツールによる分断と可視性の欠如という課題を解消するためにWizを導入。リスクを迅速に把握でき、開発のアジリティを損なわないクラウド環境を実現しています。

アジリティは競争を勝ち抜くための力、セキュリティはビジネスを持続させるための土台。ビジネスを前進させるにはその両立が不可欠です。

Boost 株式会社 取締役 CTO 高塚 智敬 氏

チャレンジ

- 顧客ごとに異なる認証・セキュリティ要件への対応で、クラウド環境が複雑化
- 脆弱性や設定不備の確認に複数ツールを使い、全体の把握が困難
- 人員が限られている中で、セキュリティと開発スピードの高度な両立に苦心

解決

- AWS 環境全体をスキャンしてリスクの全体像を単一プラットフォームで可視化
- 発見した脆弱性に対する適切な優先順位付けと対処方針が得られるように
- セキュリティ領域専門でないエンジニアでも、セキュリティへの対応がより容易に

80% 削減

PoV 期間（3 週間）で
クリティカル 이슈を
80% 以上削減

SOC2 取得に貢献

脆弱性の対応プロセスを
証跡として活用し
コンプライアンスを確保

優れた UX

セキュリティ専門の
エンジニアでなくとも
扱いやすい UX

サステナビリティの領域で企業の信頼に応える ERP を提供

昨今、ESG や温室効果ガス排出量の開示義務化など、世界各国でサステナビリティに関する規制が急速に整備されつつあります。Boost 株式会社は、サステナビリティ領域に特化したクラウド型 ERP ソリューションを大企業向けに提供しており、時価総額1兆円を超える規模の企業を中心に、ESG 対応を支援しています。同社 取締役 CTO の高塚 智敬氏は、同社の立ち位置について「サステナビリティ領域では各国で規制が整備されつつあり、企業側には対応のための業務プロセス構築が求められています。そこで当社ではその管理を効率化する仕組みをクラウドから提供しています」と話します。

同社は単に汎用的なソリューションを提供するのではなく、大企業特有の複雑なプロセスにも深く対応できる点が強みです。「各社の業務プロセスは複雑ですが、その要請に耐えられるソリューションを開発していきたいというのが当社の考えです」と高塚氏は語ります。

こうした背景から、同社にはサービス開始当初からセキュリティへの高い要求が課せられてきました。「当社のお客様はエンタープライズ規模であることから、当然ながらセキュリティに対する要求は高いものがあります。当初は企業ごとに個別にインフラ環境をご用意するところから始まり、よりスケールしていくために、クラウド技術を使いながらさまざまな施策を実施してきました」と高塚氏は話します。

確かなセキュリティは「継続的に成長し続ける土台」

同社にとって、サービス開発やリリースのアジリティ（迅速性）は事業の根幹をなす要素です。「サス



Boost 株式会社
取締役 CTO
高塚 智敬氏

“

専門知識を持ったセキュリティエンジニアでなくとも、直感的なインターフェースのおかげでインフラ・SREのチームが十分に活用できる。それがWizを選んだ理由の1つです。

テナビリティという新たな領域でビジネスを行うスタートアップ企業として、スピーディにサービスを提供し、お客様と一緒に価値を検証することを繰り返すのがカギだと考えています」と高塚氏は語ります。一方で、高塚氏はセキュリティとアジリティの双方を欠かすことができないと話します。「アジリティは、いわば日々の競争を勝ち抜く『明日を生きる力』です。それに加えて、ビジネスを継続させる、すなわち『生き続ける力』をつけるにはセキュリティが不可欠です」（高塚氏）

大企業の顧客に対する信頼の担保という観点からも、セキュリティは重要な意味を持ちます。「お客様が私たちのサービスを安心してご利用いただく上で、セキュリティが担保されていることは非常に重要です。当社がどのような体制で取り組んでいるかを社外に対して示す必要があり、顧客データを安全に管理するために現在ではSOC2などの第三者認証も取得しています」（高塚氏）

こうした考えのもと、同社はセキュリティを「コスト」や「ブレーキ」ではなく、事業の継続性と顧客との信頼を支える基盤として位置づけ、創業当初から継続的に取り組みを進めてきました。

複数ツールの使用が生んだ分断と可視性の欠如

一方、エンタープライズ企業のニーズに対応し、AWSをベースに構築されたクラウド環境でサービスを開発・展開する中で、同社はクラウド環境の複雑化という課題がありました。

「お客様は、グループ会社や関連企業、さらにはサプライヤーまでが当社のサービスを利用するケースもあり、それぞれに異なる認証要件やセキュリティ条件への対応が必要でした。利用者のカテゴリごとにセキュリティ条件が異なるため、それらすべてに対応できる対策を講じてきました」（高塚氏）こうした環境でのセキュリティ管理における最大の課題が「複数ツールの分断」です。例えば、脆弱性のチェックは、複数種類のツールを使って異なる観点ごとに実施していました。高塚氏は、「それぞれ分断された形での対応になっているため、全体として対応にどれくらい時間がかかっているかを正確に把握できない状況でした」と従来の課題を振り返ります。

さらに「自社が行っているセキュリティ対策は本当に十分なのか」という懸念もありました。「複数実施する対策はそれぞれタイミングもバラバラになりますし、環境全体を統合して見たときに、いつの時点で100点の出来にできるかのコントロールが非常に難しい状態でした。そのため、対策が本当に問題ないと言うにはまだ不安が拭いきれませんでした」（高塚氏）

セキュリティの民主化へWizにより少人数でも回る運用が可能に

こうした背景から、Boostではクラウドセキュリティ対策の見直しに着手。複数の製品を比較する中で評価したのが、Wizの可視化と優先順位付けの仕組みです。「すべてのアラートを追うのは現実的ではありません。その中で、どの順番でどう対処すべきかを提示してくれる点がWiz選定の大きな決め手となりました」と高塚氏は評価します。

導入前のPoV（価値検証）では、当初100件以上検出されていた 이슈が3週間後には20件以下に削減しています。「Wizはダッシュボードの見た目のインパクトが大きく、私自身エンジニアとして触っていて楽しい製品だと感じました」と高塚氏は振り返ります。実際の改善効果と高いUXが、導入の決め手となりました。

Wiz導入後、Boostのセキュリティ運用は「現場主導」へと変化しつつあります。導入当初は、同社にはまだ専任のセキュリティエンジニアがいなかったものの、Wizのわかりやすいダッシュボードを活用することで、インフラやSREチームが主体的に対応できる体制が構築されました。セキュリティを一部の専門チームだけが担うのではなく、開発・運用の現場全体で扱う「セキュリティの民主化」を実現する基盤となっています。

さらに、SOC2対応においても、Wizは重要な役割を果たしています。「脆弱性の検知から対応までのプロセスを証跡として活用できるため、コンプライアンス確保にもつながっています」と高塚氏は語ります。

今後同社は、開発の初期段階から脆弱性を排除する「シフトレフト」を推進する考えです。「セキュリティの検証期間を短縮することで開発リリースを早め、お客様への価値還元のスピードを上げていきたい」と高塚氏は語ります。アジリティとセキュリティの両立を追求するBoostにとって、Wizを軸としたクラウドセキュリティの高度化はその挑戦を支える確かな土台となっています。