

セキュリティは「ブレーキ」でなく価値創出の原動力

NECが実現する クラウドセキュリティ運用変革

NEC

会社名

日本電気株式会社

産業

テクノロジー

リージョン

日本

WIZ製品

Wiz Cloud

ユースケース

Wiz Cloud

クラウドプラットフォーム

AWS

Azure

GCP

IaaS領域にてエージェントレスで導入でき、IT資産・リスク・攻撃診断からAIによるアクションまで一気通貫で高精度に可視化するWizの実力に驚いたというNEC。この導入により同社はマルチクラウド環境でのセキュリティ運用変革と「セキュリティの民主化」を加速しています。

セキュリティを一部の部門だけで守ることには限界があります。組織全体の意識を高め、開発や運用の中にセキュリティを自然に組み込んでいく文化の醸成こそが、今の時代には不可欠です。

日本電気株式会社 執行役 Corporate EVP 兼 CAXO 小玉 浩 氏

チャレンジ

- AWS、Azure、Google Cloudが混在する環境で、IT資産やリスクの全体像の正確な把握が困難
- CSPMなど複数ツールから大量のアラートが発生しており、優先的に対応すべきリスクの判断が困難
- システム開発スピードを維持しつつ、組織全体でセキュリティに取り組む体制づくりが必要に

解決

- パブリッククラウド個々のツールに依存せず、マルチクラウド環境全体のIT資産とリスクの可視化が容易に
- Wizの「セキュリティグラフ」によって複合的なリスクを可視化。AIによる修正提案で迅速な対応が可能に
- ダッシュボードでリスク状況を共有することで、開発・運用の垣根を超えて主体的に対応できる体制を強化
- AWS、AzureやGoogle Cloudなどのクラウド環境へ約3カ月で導入を進行
- 導入時に検知されたクリティカルな 이슈は約3カ月で10分の1程度に削減

1/10

導入時に発見された
クリティカル 이슈を
3カ月で大幅に削減

約1割

セキュリティ運用における
セキュリティ専任者の関与を
1割程度に低減

約3カ月

大規模な
マルチクラウド環境へ
迅速に展開

サイバー攻撃が高度化する時代に NEC が掲げる「セキュリティの民主化」

昨今ではAI技術の進展によって業務の利便性が向上する一方、サイバー攻撃の高度化によるセキュリティリスクの懸念も高まっています。このような状況の中、サイバーセキュリティ対策を経営の重要課題と位置づけているのが、日本電気 (NEC) です。同社 執行役 Corporate EVP 兼 CAXO の小玉 浩 氏は、「AI の登場によって脅威のレベルは大きく変わりました。企業は AI を前提としたガバナンスと防御の仕組みを整え、迅速に対応できる体制を構築する必要があります」と話します。

一方で、ビジネス環境が目まぐるしく変化する現状においては、システム開発のスピード、品質、セキュリティの3つを同時に実現しなければなりません。そのために NEC が重視しているのが「セキュリティの民主化」です。セキュリティを専門の部署だけが担うのではなく、開発や運用を含めた組織全体で取り組む体制をつくることで、スピードを維持しながらセキュリティレベルを高めていく考えです。



日本電気株式会社
執行役 Corporate EVP 兼
CAXO

小玉 浩氏

“

AI が前提となった世界では、セキュリティと AI ガバナンスはビジネスの根幹を成します。Wiz はその即戦力として期待できるツールです。セキュリティはブレーキではなく、成長のエンジンになると確信しています。



日本電気株式会社
Corporate Executive CISO

淵上 真一氏

“

脆弱性・設定ミス・権限過剰が重なると、攻撃リスクは一気に跳ね上がります。Wiz のセキュリティグラフはそうした複合的な関係性を直感的に可視化し、真に優先すべき対処を明確にしてくれます。

本当に対処すべきリスクを正しく見極める難しさ

このような目標を掲げる一方で、NEC では社内 IT 基盤の複雑さがセキュリティ運用における大きな課題になっていたといいます。同社ではプロジェクトごとに最適なクラウドを選択してきた結果、Amazon Web Services (AWS) や Microsoft Azure、Google Cloud などさまざまなサービスを利用し、1000 環境以上に達していました。クラウドごとに管理ツールや運用方法が異なっていたことも複雑さに拍車をかけていたと同社 Corporate Executive CISO の淵上真一氏は語ります。

「プロジェクトごとには完結していても、全体を管理する立場からすると、システムのモニタリングや管理を一元的に行うことが難しく、クラウド全体の状況を素早く正確に把握しにくい状態でした」

セキュリティに関しては、すでに CSPM (Cloud Security Posture Management) などのツールを活用し、クラウド設定の不備や脆弱性を検出する取り組みを進めてきました。しかし、複数のツールから多数のアラートが発生するため、その運用も一筋縄ではいきませんでした。

「膨大なアラートの中から、真に優先して対応すべきものはどれなのかを判断するのが難しい状況でした。見つけてから対応が完了するまで、数日で終わるケースもあれば、優先順位の判断に時間がかかり、1 カ月ほど要するケースもありました」(淵上氏)

判断が難しい要因には、「リスクは単独で存在するとは限らない」という点もあります。つまり、ある脆弱性そのものは重大ではなくても、過剰な権限設定など別の要因と組み合わせることで、実際の攻撃リスクが高まるケースがあります。「さまざまな要因や条件を加味した上で全体像を評価し、実際のリスクに応じて対処の優先順位を判断できる仕組みを必要としていました」と淵上氏は語ります。

複合的な要因によるリスクを可視化する機能に着目して Wiz を導入

こうした課題を受け、NEC では新たなソリューションの検討を開始しました。そこでは3つのポイントを重視したといいます。

「1つは、脆弱性や設定ミスなど複数の要因を踏まえ、リスクの優先順位を提示できることです。2つ目は、エンジニアを含めて誰にとっても分かりやすく状況を可視化できること。そして3つ目は、見つかった課題に対して現実的な修正方法を提示できることでした」(淵上氏)

その後、複数の製品を対象に PoV (価値実証) を行い、最終的に採用されたのが Wiz です。決め手となったのは、マルチクラウド環境横断でリスクを正確に可視化できる点でした。また、「セキュリティグラフ」機能による可視化の有用性も評価につながりました。クラウド資産や脆弱性、権限設定などの関係をグラフ構造で示すことで、複合的な要因によって生じるリスクを直感的に把握できます。

「加えて、AI による修正提案機能も評価ポイントでした。PoV の段階で詳細な検証を行った結果、Wiz から提示される修正方法が従来のツールに比べて実用性が高く、実際の運用にもそのまま活かせると判断しました」と淵上氏は語ります。

セキュリティの民主化と運用高度化へ確実な手応え

PoV はまず AWS 環境で実施され、その後 Azure や Google Cloud にも展開。全体として約3カ月で大規模なクラウド環境への導入が進みました。エージェントレスで迅速に接続・展開できることもスムーズな導入に貢献しました。さらに、NEC の経営ダッシュボードに Wiz を組み込むことで、昨今の情勢における大きな経営リスクの1つであるクラウドセキュリティを可視化しました。

現在では Wiz の導入により、これまでセキュリティ部門が中心に行っていた脆弱性対応は、システム管理部門との連携体制へと移行しています。導入時に検知されたクリティカルな 이슈 は約3カ月で10分の1程度に削減。実際の運用では、複数の要因が組み合わさったことで生じたリスクを特定できたケースや、管理の所在が不明確なクラウド資産が判明するケースもあり、リスク低減やガバナンスの強化に貢献しています。さらに、Wiz を活用したセキュリティ運用ではセキュリティ専任担当者の関与は全体の1割程度に抑えることができ、残りの8~9割はシステム管理や開発の担当者が対応。より幅広い担当者が関わる「セキュリティの民主化」を実現しつつあります。「Wiz の導入は、セキュリティがブレーキではなく価値創出の原動力となる大きな一歩として評価しています」と小玉氏は語ります。

NEC では今後も、クラウドにとどまらずより広い領域でのセキュリティ管理にも取り組んでいきます。ソースコードレベルでのリスク検知など、開発段階からセキュリティの文化を醸成することで、よりセキュアな IT 環境を整備していく方針です。