インターネットイニシアティブ エンドポイント向けの セキュリティサービスに Acronis Cyber Protect Cloud + EDRを採用

IIJセキュアエンドポイントサービスに復旧機能を実装。高度なセキュリティ機能によってバックアップの安全性を高め、ランサムウェアやラテラルムーブメントへの対応を可能にしました。

事業の概要

株式会社インターネットイニシアティブ（以下、IIJ）は日本で初めての本格的商用インターネットサービスプロバイダー(ISP)として1992年に誕生。以降、さまざまなサービスの原型を生み出し、ISPからトータルネットワークソリューションプロバイダーとして成長を続けてきました。

業務内容はインターネット接続サービスやネットワークシステムの構築など多岐にわたります。その一つが、法人向けのセキュリティソリューションの提供です。IIJは独自のセキュリティオペレーションセンター（SOC）を保有するほか、高い技術力と総合力を活かして多様なセキュリティソリューションを開発、提供しています。2018年にはクラウドによる統合型エンドポイントサービス「IIJセキュアエンドポイントサービス」（以下、セキュアエンドポイントサービス）の提供を開始しました。

当初は既知、未知のマルウェアの侵入を防ぐアンチウイルスとIT資産管理を主な機能として提供していましたが、2024年4月に「Acronis Cyber Protect Cloud + EDR」を導入したことで有事の迅速なデータ復旧が可能になるなど、さらにセキュリティ機能が充実。顧客ニーズに応じた柔軟なカスタマイズが可能になっており、規模の大小や業種を問わず幅広い企業の利用が期待されています。

ビジネス上の課題

「アクロニスの採用に関しては、これまで対応できていなかった復旧機能の実装を主眼においていました」

セキュアエンドポイントサービス開発を主導したIIJセキュリティ本部セキュリティビジネス開発部企画開発1課の砂田真志氏はこう説明します。

米国の科学技術に関連する研究を行う政府機関であるアメリカ国立標準技術研究所（NIST）は、サイバーセキュリティ対策の評価指標「サイバーセキュリティフレームワーク（CSF）」のなかで、「識別」「防御」「検知」「対応」「復旧」「ガバナンス」の6項目を、組織の種類や規模を問わない共通のセキュリティ対策として提示しています。従来のセキュアエンドポイントサービスはこのうち「識別」「防御」「検知」「対応」までをカバー。バックアップなどが必要なユーザー企業に対しては、別サービスでデータのバックアップやリストアを提供していました。

業種・業態
情報・通信業

主な課題
- 復旧機能によるNISTフレームワーク対応

主な要件
- 安全な復旧のためのセキュリティとバックアップ
- 自社クラウドストレージへのバックアップ
- サードパーティ製品との親和性

保護対象リソース
- Windows/MacのOSを搭載したPC

主なメリット
- 複層的な防御機能の実装
- 日本語のわかりやすいUI
- ユーザーの選択肢の拡大

IIJ
Internet Initiative Japan

「ただしバックアップとして提供しているのが主にサーバーに保管しているデータ向けサービスであったために、従業員が利用しているPCの復旧には不向きな面もあり、使い勝手にも課題がありました」と砂田氏。

「かねてからセキュアエンドポイントサービスに復旧機能を加える必要性は感じていました。またユーザーからも『マルウェア感染が起きた場合であっても、安全に、かつ迅速に業務環境を復旧できるか』というお問い合わせが増えるなど、復旧への関心は高まっていました」

こうしたなかで、IIJではいち早くセキュアエンドポイントサービスに復旧機能を追加、統合していくことを目指し、複数の製品で検討を開始しました。最終的にAcronis Cyber Protect Cloud + EDRの採用に至った理由は「高度なセキュリティに、使い勝手のよいバックアップという両輪を備えていた点にあります」と砂田氏は評価します。

ソリューション

「インシデントからの復旧では、普段からセキュアな状態で顧客の端末データをバックアップしておくこと、そして有事にはバックアップから安全な状態でお客様の端末を迅速に復旧できることが必要条件となります。バックアップからの復旧をいかにセキュアに実行するかという点において、網羅的な防御機能を備えたアクロニスは非常に頼もしい存在でした」

> 「いかにセキュアに復旧できるかという点において、高度なセキュリティに使い勝手のよいバックアップという両輪を備えていたAcronis Cyber Protect Cloud + EDRは非常に頼もしい存在でした」

株式会社インターネットイニシアティブ
セキュリティ本部
セキュリティビジネス開発部 企画開発1課
砂田真志氏

Acronis Cyber Protect Cloud + EDRは、従来型のパターンマッチングに加えて、振る舞い検知を含むAIおよび機械学習ベースのヒューリスティック検知などを備えた次世代ウイルス対策（NGAV）で、データ、アプリケーション、システムをプロアクティブに保護します。アプリケーションやバックアップデータを破壊しようとする攻撃に対する事故防御の仕組みを搭載したバックアップ機能との統合によって、バックアップデータの安全性を確かなものにしています。

また、独自の高度なランサムウェア対策機能であるActive Protectionが、システム上のデータファイルを変更するプロセスを監視します。ランサムウェアがファイルを暗号化しはじめると、すぐに検知してそのプロセスを遮断し、遮断前に暗号化されたデータをキャッシュから自動的に復元することも可能です。

さらに、万一マルウェアや攻撃者がシステムに侵入した場合にも、サイバーセキュリティ、データ保護、エンドポイントセキュリティ構成管理の統合を活用したEDRでインシデントに対応できます。簡単なクリック操作で、エンドポイントや脅威の隔離、リモート接続やフォレンジックバックアップを用いた調査、脆弱性の修復、攻撃に対するロールバックを実行し、被害を最小限に抑えるとともに将来の脅威を未然に防止することができます。

「IIJセキュアエンドポイントサービス IT資産保護」では、IIJのクラウド上のデータセンターにバックアップデータを保存しています。「アクロニスであれば、弊社独自のクラウドストレージへのバックアップが可能。このバックアップデータはサイバーインシデントのみならず、災害時や監査などさまざまな場面での利用が想定されています。セキュアな復旧機能を提供することは、ユーザーのあらゆるニーズに応えるものになるはずです」と砂田氏は語ります。

アクロニスの防御機能を評価し、セキュアエンドポイントサービスでは復旧のみならず防御においてもアクロニスを導入。アンチウイルスソフトとしてアクロニスを含めた3種類のソフトを提供しており、どれを利用するかはユーザーが自由に選択可能です。

「アクロニスはサードパーティ製品との親和性も高く、セキュアエンドポイントサービスの持つ柔軟性を損なうことなく、機能面の拡充に貢献してくれています。例えば防御と資産管理はA社ソフト、復旧はアクロニスといった具合に、ユーザーの事情に応じた組み合わせが、セキュアエンドポイントサービス上で実現できます。また他社製品ではユーザーの既存環境のリプレースが必要なケースが多くありましたが、アクロニスは既存環境に手を入れずにユーザーに復旧機能を提供できた点も大きなメリットだったと感じます」

効果と展望

砂田氏は「アクロニスは当初の想定以上に多様なセキュリティ機能を備えており、ユーザーに対してこれまで以上に幅広いソリューションを提案できるようになりました。今後はアクロニスを含めてセキュアエンドポイントサービスの有する複数の機能を組み合わせるメリットを、よりユーザーに分かりやすく説明していきたいと思っています」と語ります。

セキュアエンドポイントサービスが対象としているのはWindowsとMacのOSを搭載したPCですが、「IIJセキュアエンドポイントサービス IT資産保護」では今後はサーバーなど他の領域も対象に広げ、より多彩なサイバー攻撃に対応できるようにしていく考えです。

Acronis

詳細はwww.acronis.comをご確認ください。