CUSTOMER SUCCESS STORY

学生と教職員10,500ユーザーが使うファイルサーバーをオールフラッシュ化し、最先端のAIテクノロジーによりサイバーセキュリティ対策を強化

NetApp

芝浦工業大學
SHIBAURA INSTITUTE OF TECHNOLOGY

標的型メールやマルウェアによる攻撃に備える NetApp Anti-Ransomware Suiteによる多層防御を実装

芝浦工業大学が、学生と教職員およそ10,500ユーザーが利用する統合ファイルサーバーを刷新しました。3世代15年にわたりNetAppストレージが担ってきた本環境に、新たに「NetApp AFF A400」オールフラッシュアレイが導入され2022年9月より運用を開始しています。注目すべきは、「NetApp Anti-Ransomware Suite」というAIベースのストレージセキュリティ機能の実装です。

標的型メールやランサムウェアなど、サイバー攻撃はますます複雑化・巧妙化しています。芝浦工業大学は、ネットアップのAIテクノロジーを活用して様々な脅威をいち早く検知し、瞬時にSnapshotを取得し、直近のリカバリポイントから復旧できる体制を整えました。ストレージセキュリティという「多層防御の最後の砦」はいかに強化されたのか――芝浦工業大学の先進的な取り組みに迫ります。

データ保護よる

リスク最小化

“定期バックアップに加え、「不審な挙動を検知した瞬間にSnapshotを取得」できるようになりました。瞬時に論理バックアップを取得できるONTAPの「Snapshot機能」をフルに活用しています”

芝浦工業大学
情報システム部 情報システム課
佐藤 剛 氏

「理工系×グローバル」という個性を備えた人材の育成

2022年9月、芝浦工業大学・豊洲キャンパスに14階建ての本部棟がオープンし、豊洲キャンパスの全体計画がいよいよ完成しました。新しい教育の場としての「アクティブラーニング教室」、研究室の枠組みを超えた活動を促進する「オープンラボ」などの環境が整備され、世界レベルでの研究拠点形成に向けた学部・大学院教育がさらに加速するものと期待されています。情報システム部 情報システム課の佐藤剛氏は次のように話します。

「芝浦工業大学は、創立100周年を迎える2027年までに『アジア工科系大学トップ10』としてのポジションを獲得すべく大学改革を推進しています。建学の精神である『社会に学び、社会に貢献する技術者の育成』をさらに発展させ、『理工系×グローバル』という個性を備えた優秀な人材を数多く送り出していくことを目指します」

芝浦工業大学では、改革の一環として、特定分野の専門性を磨く「学科制」から、複数分野の知識を習得できる「課程制」への移行を表明しています。

芝浦工業大学
情報システム部 情報システム課
佐藤 剛 氏

「より幅広い知識の取得や実践的な学びに取り組めるよう、学部やカリキュラムは今後さらに変化・進化していくことになるでしょう。情報システム部は、幅広い専門知識と技術をあわせ持ち、世界で活躍できる人材を育成するための環境整備にいっそう力を注いでいきます」（佐藤氏）

2022年9月、芝浦工業大学は、学生と教職員およそ10,500ユーザーが利用する新しい統合ファイルサーバーの運用を開始しました。ここに採用されたのは、最新のオールフラッシュアレイ「NetApp AFF A400」と、AIベースのストレージセキュリティ機能を提供する「NetApp Anti-Ransomware Suite」です。

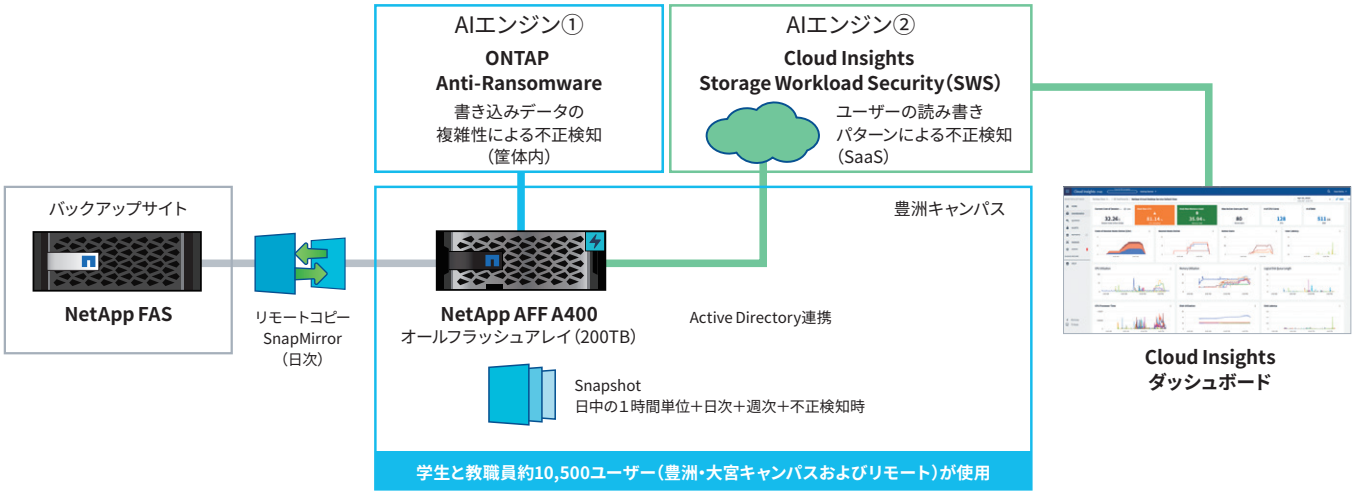
「オールフラッシュ化」と「セキュリティの強化」

芝浦工業大学では、全学を統合するファイルサーバー環境を2004年に整備し、以来5年ごとに最新化しながら運用しています。2016年に導入した第3世代の統合ファイルサーバーでは、NetApp FAS 8000が全学およそ10,500ユーザーへ高品質なストレージサービスを提供してきました。

「2022年の最新化のポイントは『オールフラッシュ化』と『セキュリティ強化』です。ユーザーのニーズに合わせた容量を確保しながら、より快適な性能・レスポンスを提供するためには、オールフラッシュ化が最も効果的でした。また、2016年にランサムウェアの被害を受けたことから、サイバーセキュリティ対策の強化は必須と考えていました」と佐藤氏は話します。

芝浦工業大学では、ネットワークからサーバーサイド、エンドポイントまで多層的なセキュリティ対策を施しており、最新のアンチウイルスソフトウェアも導入されています。ストレージ環境では、ONTAPのFPolicyを利用してランサムウェアが利用する拡張子を除外し、ファイルへの書き込みを制限しています。しかし、狡猾に進化し続けるサイバー攻撃に対しては、どんな組織であろうと完璧な備えはあり得ません。様々な脅威に侵入されるリスクを考慮しながら、問題に直面したときの組織のレジリエンス（回復力・適応力）をいかに高めるかが重要になっています。

「統合ファイルサーバーにおいて、データを破壊・暗号化するようなランサムウェアへの現実的かつ最も有効な対策は、不審な挙動をいち早く検知することと、検知から最短時間でバックアップを取得することです。改ざんされる直前のデータを保護しておくことで、ユーザーへの影響を伴うリスクを最小化できます」（佐藤氏）



統合ファイルサーバーでは、「日中の1時間単位」「日次」「週次」というきめ細やかさで定期的にバックアップを取得しており、バックアップデータはリモートサイトで保護する仕組みも整えられています。最新化された環境ではこの体制がさらに強化されました。

「これまで通りの定期バックアップに加え、『不審な挙動を検知した瞬間にSnapshotを取得』できるようになりました。瞬時に論理バックアップを取得できるONTAPの『Snapshot機能』をフルに活用しています。これにより、データ棄損のリスクを大幅に低減することに成功しました」(佐藤氏)

不審な挙動を検知した瞬間にSnapshotを取得

NetApp Anti-Ransomware Suiteは、①ストレージOSであるONTAPが備える「Anti-Ransomware」と、②クラウドベースの統合的なモニタリング環境NetApp Cloud Insightsから提供されるユーザー単位の行動分析(UBA)機能「Cloud Insights Storage Workload Security(SWS)*」から構成されます。(*旧名称:Cloud Secure)

「2つの異なるレイヤーでストレージ上の不審な挙動や異常を検知し、検知したその瞬間にSnapshotを取得する仕組みを整えました。検知から瞬時のデータ保護までを、ネットアップのAIテクノロジーが自動的に実行することがポイントです」と佐藤氏は話します。

①ONTAPのAnti-Ransomwareでは、AIエンジンがファイルサーバーに対する「データの読み書きパターン」を学習し、データの複雑性(エントロピー)としてスコア化します。書き込みやリネームの頻度が通常のスコアと大きく乖離するなど、AIエンジンが不審と判断したときに管理者へアラート通知するとともにSnapshotを取得します。

「一方、②Cloud Insights SWSでは、『ユーザーごとのアクセスパターン』を学習したAIエンジンが、大量のファイル削除や持ち出しといった通常とは異なるユーザーのふるまいを検知するとアラートを発し、同時にSnapshotを自動取得します。Active DirectoryのID情報と紐づけてログを確認できますので、学内のユーザーであれば連絡・報告など即座に適切なアクションをとることが可能です」

Cloud Insights SWSのAIエンジンは、運用を進める過程で学習を繰り返すため問題検知の精度向上が期待できます。

「Cloud Insights SWSのログデータはクラウド上に13か月分が保持され、必要な分だけCSV形式でダウンロードしてレポートに活用できるので安心です。不正アクセスやサイバー攻撃に対するフォレンジック(法的証拠の保全)に活用できるメリットが大きいですね」と佐藤氏は話します。

NetApp Cloud Insightsは、クラウドベースのモニタリング・運用監視ツールであり、優れた分析機能を備えたオブザーバビリティツールでもあります。ユーザー行動分析(User Behavior Analysis)を実行するAIエンジンを備えたCloud Insights SWSは、NetApp Cloud Insightsの多様な機能セットのひとつとして提供されるものです。

「NetApp Cloud InsightsからオンプレミスのNetApp AFF A400の状況を俯瞰的に把握し、アラートがあれば詳細まで掘り下げて確認することができます。NetApp AFF A400の設定や操作は、使い慣れたONTAP System Managerやコマンドコンソールを使い分けています」(佐藤氏)

高性能オールフラッシュアレイならではの安心

NetApp AFFは、業界をリードするパフォーマンスとONTAP 9のデータ管理機能が高く評価されているオールフラッシュアレイです。新しい統合ファイルサーバーとして採用された「NetApp AFF A400」は、4Uの筐体でデュアルコントローラーをActive-Activeで稼働させ、高いパフォーマンスと優れた耐障害性を実現します。

また、NetAppストレージ搭載するONTAPは、サイバー攻撃に強いという評価もあります。ONTAP自体が攻撃を受けて、第三者によるリモート操作やコマンド実行が行われるようなインシデントを発生させたことはありません。

「オールフラッシュ化による効果は幅広い範囲に及びました。アクセスが集中して高負荷になっても、レスポンスを悪化させない性能の高さは期待通りでした。予想を大きく上回ったのはデータ量の削減です。NetApp AFF A400では、ボリューム単位でなくストレージシステム全体で重複排除・圧縮が効くため、60%近いデータ削減効果が得られました」と佐藤氏は笑顔を見せます。

芝浦工業大学の新しい統合ファイルサーバーは「オールフラッシュ化」と「セキュリティ強化」という進化を果たし、2022年からの5年間を安心して運用できる環境が万全に整えられました。佐藤氏は次のように結びました。

「長年にわたりNetApp製品を活用してきましたが、世代交代の度に大きな進化を遂げていることを実感しています。特に、クラウドサービス、クラウド連携製品の充実には目を見張るものがあります。今回採用したNetApp Cloud Insightsは、私たちにとって最使い勝手の良いクラウドサービスのひとつではないかと思っています。芝浦工業大学の環境も、クラウドとオンプレミスのハイブリッド化が進んでいます。ネットアップのテクノロジーが、複雑になりがちなハイブリッド環境の統合的かつシンプルな管理を実現してくれるものと期待しています」

NetApp products

NetApp AFF

NetApp FAS

NetApp Cloud Insights

Protocols

NFS、SMB