



2026年3月30日

報道関係 各位

ネットアップ合同会社

## NetApp と Elastico、 ランサムウェアに対する多層防御型レジリエンスを提供する パートナーシップを発表

**強固なサイバーレジリエンスには、境界防御とストレージ層に組み込まれたセキュリティの両立が不可欠**

ネットアップ合同会社（本社：東京都中央区、代表執行役員社長：齊藤千春） - インテリジェントデータ インフラストラクチャ企業である NetApp®（NASDAQ: NTAP）と Elastico は、ランサムウェアに対する多層防御型レジリエンスを提供するパートナーシップを締結することを発表します。

セキュリティチームは、テクノロジースタックのあらゆるレイヤーにおける脅威に備える必要があります。これには、検知される前に本番環境を静かに横断し、スナップショットやバックアップの中に潜伏するランサムウェアも含まれます。高度化したランサムウェアは、既存の予防ツールを回避するよう設計されており、検知のしきい値を下回ったまま本番環境を移動し、アラートが発報される前にバックアップデータへ到達します。NetApp と Elastico は、本パートナーシップを通じ、本番ストレージからリカバリーデータに至るまでをカバーする多層防御により、企業のサイバーレジリエンス強化を支援します。

両社は、Elastico の Provable Recovery Control を「Powered by Elastico」として NetApp Ransomware Resilience Service に組み込み、スナップショットに対する Deep File Inspection（詳細ファイル検査）を追加します。これにより、ランサムウェアの検知から復旧まで、継続的に「クリーン」であることが検証された復旧ポイントを活用した、エンドツーエンドのレジリエンスを実現します。

### NetApp Ransomware Resilience Service における新たな防御層

#### ■ NetApp Ransomware Resilience Service

データレイヤーでランサムウェアをリアルタイムに検知・封じ込め、イミュータブルなスナップショットを取得し、復旧をガイドします。また、ONTAP® 環境全体にわたりランサムウェア対策状況を継続的に評価します。Autonomous Ransomware Protection（ARP）による振る舞い検知を含みます。

#### ■ Elastico Provable Recovery Control

ONTAP スナップショットに対する Deep File Inspection により、境界防御をすり抜けたゼロデイ・ランサムウェア、段階的に仕込まれたマルウェア、ステルス型のデータ破損を検知します。エージェント不要で、最

後に確認されたクリーンな復旧ポイントを継続的に特定します。

本協業により、Elastio Provable Recovery Control は 追加の調達やアーキテクチャ変更を必要とせず、NetApp Ransomware Resilience Service に直接組み込まれます。これにより、両社はお客様のサイバーレジリエンスをさらに強化します。

### 提供時期

Elastio 搭載 NetApp Ransomware Resilience Service (Powered by Elastio) は、近い将来の提供開始を予定しており、まずは Amazon FSx for NetApp ONTAP から提供を開始し、その後、他の ONTAP 環境へと展開される予定です。

Amazon FSx for NetApp ONTAP は、NetApp の広く利用されている ONTAP ファイルシステムを基盤とした、フルマネージド型のクラウドサービスであり、高い信頼性、スケーラビリティ、高性能、そして豊富な機能を備えたファイルストレージを提供しています。

アーリーアクセスに関心のある企業は、NetApp または Elastio の担当者までお問い合わせください。現在の復旧体制の評価を支援します。

NetApp シニア・バイスプレジデント 兼 データサービス担当ゼネラルマネージャーの Gagan Gulati は下記のようにコメントしています。

「包括的なサイバーセキュリティ戦略を定義するうえで、ストレージは不可欠な要素です。データが存在する場所で保護することで、ランサムウェアのようなサイバー脅威に対抗するための中核にストレージを位置付けることができます。しかし、事業のレジリエンスや業務継続にかかるリスクは非常に高く、単一の防御レイヤーに依存することはできません。Elastio との協業により、企業は最も重要な資産である『データ』を守るための新たな手段を手にすることができます。」

Elastio CEO である Naj Husain 氏は下記のように述べています。

「多くの組織が最悪のタイミング、つまりインシデント発生中に、復旧データが侵害されていることに気づきます。その時点では、バックアップがクリーンかどうかはもはや理論の話ではありません。本共同ソリューションは、その問いに対し、インシデントが起きる前から継続的に答えを提供します。」

Crane WW Logistics の VP IT Infrastructure 兼 CISO である Marc Crudgington 氏は下記のように述べています。

「インフラを移行するにあたり、バックアップのセキュリティと信頼性を十分に確保することは絶対条件でした。Elastio は初日からバックアップの継続的な検査を提供してくれたことで、確実に復旧できるという自信を持つことができました。これこそが、私たちが自らに課している基準です。」

### Elastio について

Elastio は、「復旧は定期的にテストするものでも、想定に頼るものでもなく、継続的に証明されるべきである」という一つの原則に基づく Active Cyber Resilience を提供します。Elastio Hunt Engine は、本番データ、レプリケーションデータ、バックアップ全体に対して Deep File Inspection を実行し、予防・検知ツールをすり抜けたランサムウェアやマルウェアを検出します。証明できる復旧（Recovery you can prove）を実現します。

## NetApp について

NetApp は 30 年以上にわたり、エンタープライズ ストレージの普及から、データと AI が定義するインテリジェント時代まで、世界のリーディング企業が変化を乗り越えるための支援を行ってきました。現在 NetApp は、データをイノベーション、レジリエンス、成長の原動力へと変えるインテリジェント データ インフラストラクチャ企業です。

その中核にあるのが NetApp データ プラットフォームです。これは、あらゆるクラウド、ワークロード、環境にわたりデータを接続・保護・活性化する、ユニファイドかつエンタープライズ グレードのインテリジェント基盤です。業界をリードするデータ管理ソフトウェア/OS である NetApp ONTAP の実績に基づき、AI Data Engine や AFX による自動化機能を備え、スケールに応じた可観測性、レジリエンス、インテリジェンスを提供します。

NetApp データ プラットフォームは、ストレージ、サービス、制御を分離設計することで、企業がより迅速にモダナイズし、効率的にスケールし、ロックインに縛られずイノベーションを加速できるようにします。さらに、世界最大のクラウドにネイティブ統合された唯一のエンタープライズ ストレージ プラットフォームとして、あらゆるワークロードを一貫したパフォーマンス、ガバナンス、保護のもとでどこでも実行できる自由を提供します。NetApp は、常にデータを「準備万端」に整え、脅威から守る準備、AI を駆動する準備、次のブレイクスルーを生み出す準備をしています。だからこそ、世界で最も先進的な企業が、インテリジェンスをアドバンテージへと変えるパートナーとして NetApp を信頼しています。詳細については、

<https://www.netapp.com/ja/>をご覧ください。ネットアップ合同会社は NetApp の日本法人です。また X、LinkedIn、Facebook、Instagram で NetApp をフォローしてください。

NetApp、NetApp のロゴ、および [www.netapp.com/TM](http://www.netapp.com/TM) に記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、各社の商標である場合があります。