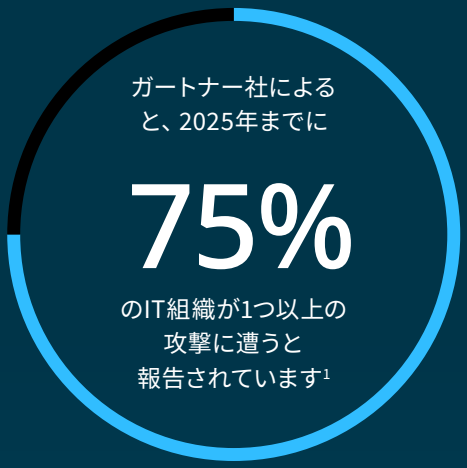
COHESITY

ランサムウェアから

レジリエンスへ

ITリーダーたちが最新のデータセキュリティとデータ管理で
どのようにビジネスを継続させたのかをご紹介します

ランサムウェアへの備えは、これまで以上に急務になっています



ランサムウェアは、サイバー犯罪の中で最も急増している形態の犯罪です。

Gartner社によると、「**2025年までにIT組織の少なくとも75%が1つ以上の攻撃に遭う。**というのも、自由裁量権をもつ研究者が、2020年にランサムウェア攻撃が劇的に増加し、7倍以上の増加率を示したことを明らかにしているからだ」[1]と報告しています。そして、サイバー犯罪者が成功するたびに、組織は経済的に、そしてしばしば評判的にもダメージを受けることになります。Cybersecurity Venturesによると、2031年までに、ランサムウェアは2秒に1回、企業、顧客、デバイスを攻撃し、被害者は年間約2,650億ドルの損害を受けると予想されています。どの業界も無関係ではありません。企業は、ランサムウェアの攻撃を阻止するための惜しみない努力は行っても、警戒を怠ることはできません。なぜなら、サイバー犯罪者は常に革新的だからです。彼らは、新たな攻撃手段を生み出し続けています。そして、その攻撃はより頻繁に、より巧妙に、より標的を絞るようになっています。しかし、攻撃の仕方はそれぞれ異なっていても、攻撃者は皆同じ目標を持っています: それは、事業運営を妨害し、秩序を回復するために被害者にお金を支払わせることです。

このような大きなリスクがあるため、企業はセキュリティ体制を進化させ、境界やアクセスのセキュリティに加え、データセキュリティを優先していく必要があります。

本当の意味での備えには、下記を含む必要があります:

- 攻撃対象領域を小さくする
- 机上演習で対応策を計画し、訓練を行う
- 漏洩したデータと潜在的な損害のリスクレベルをどのように把握するかを決定する
- あらゆるデータ環境の可視化を向上 - 見えないデータ、管理できていないデータを守ることはできない

ランサムウェアへの備えは、前もって行うことが重要です。

[1] Gartner®, Minimize Risk by Better Knowing and Managing Your Data, Michael Hoeck, Gartner IT Infrastructure, Operations & Cloud Strategies Conference, Nov 2022
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

お客様、セキュリティパートナー、第一線のセキュリティ専門家から話を聞く

幸いなことに、セキュリティ体制を改善できるベストプラクティスとソリューションが存在します。おそらくサイバー犯罪者を撃退することさえできます。

私たちは、この新しい時代にふさわしいモダンデータセキュリティとデータ管理ソリューションを提供する信頼できるパートナーです。私たちのソリューションをご利用いただいている人たちのお話を直接聞いてください。

このeBookでは、私たちのお客様が下記について語ります:

- ランサムウェア攻撃に関する体験談
- 侵害のメカニズムに関する彼らの見解
- どのようにして復旧に成功したのか
- 今後に向けて、どのようにセキュリティ体制を強化したのか

最後に、Cohesityのデータセキュリティアライアンスと Cohesityセキュリティアドバイザリーカウンシルのパートナーからのお話を聞いてください。これらの専門家はサイバーセキュリティの真の著名人で、ランサムウェアとの戦いに勝利するための鍵となる方法を明らかにします。

業種: 教育
所在地: テキサス州ヒューストン
設立: 1935年

独立学区の事前準備が功を奏す

背景:

ヒューストン地域のスプリング独立学区 (ISD) は、他の学区と同様に、増大するサイバーセキュリティの脅威に対する防御を強化していました。

「毎月140万件の攻撃をブロックし、定期的に脆弱性テストや侵入テストを行い、スタッフには1年を通してサイバーセキュリティトレーニングを提供しています」とアプリケーションサポート担当ディレクターのBobby LaFleur氏は言います。

加えて、ヒューストンの近隣の学区では、2020年3月に破壊的なランサムウェア攻撃に遭い、20万ドル以上の身代金を支払っていました。

スプリングISDは、同じ運命を辿りたくなかったのです。

攻撃:

11月、LaFleur氏の警戒心と準備が功を奏しました。

「午後8時頃、パンデミックの時に使用していたシステムにエラーが発生したという連絡がありました」とLaFleur 氏は語ります。ITエンジニアがファイルサーバーが暗号化されていることを確認すると、LaFleur 氏と彼の同僚はオフィスに駆けつけ、ネットワークを一時的に停止させました。

復旧:

幸いなことに、スプリングISDは先だって、重要な切り替えを行っていました。

彼らは以前、別の2種類のバックアップ製品を使用していました。その2つの異なるバックアップサーバープラットフォームは、災害復旧用に使用していた近くのコロケーション施設にセットアップ全体を複製していました。しかし、コロケーション施設のリース契約を更新することになったとき、ITチームはCohesityを採用しました。データセンター内のCohesityのバックアップはイミュータブル (変更不可) で、攻撃者がそれらを暗号化または削除しようとするのを防ぐことができます。「仮想マシンやSQL Serverが攻撃で暗号化されても、スナップショットで即時に任意の時点に復元することができます」とLaFleur氏は言います。

攻撃に遭った時、Cohesityのデータセキュリティとデータ管理プラットフォームがすでに導入されていました。スプリングISDは、仮想マシン (VM) とデータベースのイミュータブルコピーをオンプレミスに1つ、AWSにもう1つ保存していました。 攻撃の翌日、学校が始まる前に、ITチームはすでにActive Directoryサーバーと重要な学習用サーバーを復旧していました。財務と生徒情報のシステムも2日以内に復旧しました。学習への支障はなく、給与支払いへの影響もなく、身代金の支払いも行いませんでした。残りの200台のサーバー (ほとんどがセカンダリーシステムでした) は、計画的にオンラインに戻していきました。

「ランサムウェア対策のおかげで、サイバーセキュリティ保険の更新と増額を行った時、有利な料率を得ることができました。他の学区の仲間から、データ保護に何を使っているのかと聞かれたら、Cohesityだと答えます。選んだパートナーにとても満足しています!」

スプリング独立学区 アプリケーション サポート担当ディレクター
Bobby LaFleur氏

「ランサムウェア攻撃後、Cohesityは本当に学区を救ってくれました。ローカルのActive Directoryサーバーがロックされ、ローカルのバックアップからデータをリストアすることができませんでしたが、AWS内のCohesityのバックアップから重要なサーバーを迅速に復旧することができました。教師たちは翌日から通常通りオンライン授業を行い、給与の支払いが滞ることもありませんでした」

Bobby LaFleur氏
スプリング独立学区
アプリケーションサポート担当ディレクター

spring ISD

結果:

身代金の支払いなし

100% 復旧

有利なサイバーセキュリティ保険料率

業種: ヘルスケア
所在地: オレゴン州クラマス・フォールズ
設立: 1968年

データのセキュリティと復旧が命を救う

背景:

スカイレイクスメディカルセンターは、オレゴン州中南部とカリフォルニア州北部で8万人以上の人々にサービスを提供している非営利の教育病院です。

以前使用していたレガシーバックアップ製品が老朽化し、更新が近づいた時、スカイレイクスインフォメーションサービス (IS) チームは、より使いやすく、さらなる効率化を促進することができる新しいデータセキュリティとデータ管理ソリューションを評価しました。この時は、Cohesityのセキュリティとランサムウェア保護機能が、患者様の治療だけでなく、ISチームにとっても救いの手になるとは、まったく思っていませんでした。

攻撃:

2020年10月、スカイレイクスは思いがけず大規模なランサムウェア攻撃の標的にされ、侵入されました。

地域医療のリーダーである同社は、Ryukランサムウェアの亜種による攻撃を受け、レガシーバックアップを含むSky LakesのITオペレーションの70%に影響を及ぼしました。

復旧:

Cohesityは、スカイレイクスがランサムウェアからデータを守るために、迅速な対応を行うデータ管理チームを務めました。

ランサムウェアの攻撃を食い止め、検知し、迅速な大規模データ復旧を可能にするCohesityのイミュータブル (変更不可の) バックアップスナップショットやDataLock、その他搭載の保護機能は、ISチームがサイバー犯罪者の要求にノーと言うことを可能にしました。

Cohesityのデータセキュリティとデータ管理プラットフォームを通じて、ISスタッフが組織のActive Directoryデータベースの詳細なバージョンにアクセスできるようになりました。また、Sky Lakesは、Cohesity SmartFilesのユニークな機能により、ファイルサービスを即座に復元することができました。迅速でシンプルなデータ復旧により、スカイレイクスがん治療センターを定期的に利用している多くの患者様が、不便を感じたり、他の場所に移動したりすることもなく、治療の中断を最小限にとどめることができました。「今回、Cohesityが命を救ってくれたと言っても過言ではありません」と、スカイレイクスのテクノロジーソリューション担当マネージャーであるNick Fossen氏は語ります。

「Cohesityのおかげで、ランサムウェアの恐喝者を追い出すことができました」

スカイレイクス・メディカルセンター
情報システムディレクター **John Gaede氏**

「私たちの組織は、重大なランサムウェアの攻撃を受け、実質インフラ全体が機能不全に陥りました。Cohesityのおかげで、マシンやファイル共有の復旧、クリーンデータの確認、そしてアプリケーションのオンライン化を実現することができました。Cohesityは、文字通り何百時間もの作業時間を節約し、実際に身代金を支払う必要もなくしてくれました」

John Gaede氏
情報システムディレクター
スカイレイクス・メディカルセンター

SKY LAKES MEDICAL CENTER

結果:

身代金の支払いなし

データ損失なし

データ復元にかかる時間を100時間短縮

業種: 不動産
所在地: タイ、バンコク
設立: 2009年

身代金を拒否し
データを高速にリストア

背景:

タイのオリジン・プロパティ (Origin Property Public Company Limited) は、タイ全土で多数の不動産を管理する不動産開発会社で、データ保護と復旧をレガシーソリューションに頼っていました。

2022年、ITチームは拡大を続ける中、バックアップ時間の短縮、データセキュリティの向上、拡張性のシンプル化、迅速な復旧を実現するため、新しいデータセキュリティとデータ管理ソリューションを探すことにしました。

システムインフォメーションテクノロジー担当シニアバイスプレジデントのSirawut Chanthasangsawang氏は、「私たちは、ERP (企業資源計画) ソフトウェア、顧客データベース、開発データ、その他コアビジネスのアプリケーションなど、さまざまな種類のデータを社有施設に保管しています。もし、これらのデータのいずれかを失うことがあれば、当社にとって大惨事になり得ます」と語ります。

攻撃:

チームが新しいソリューションを積極的に調査している間に、ランサムウェアに攻撃され、既存のソリューションが障害を起こし、Originのデータベース、サーバー、アプリケーションのすべてが停止してしまいました。

「ランサムウェアは、APIを使用してプライマリストレージを攻撃し、すべてのボリュームを完全に削除してしまいした。侵入者は、以前のバックアップソフトウェアからすべてのデータリポジトリを暗号化し、完全に復旧に使えなくしました。彼らの身代金要求に応えない限り、復旧は不可能と思える状況でした」とChanthasangsawang氏は説明します」

復旧:

幸運なことに、オリジンはCohesityでPoCを開始していました。

オリジンはPoCの間にCohesityのデータセキュリティとデータ管理プラットフォームにデータをバックアップしていたため、すべての顧客と企業データを守り、3時間以内にリストアすることができ、身代金の支払いを免れることができました。

それ以来、オリジンはデータのバックアップ時間を20時間から3時間弱に短縮することができ、85%の削減を実現しました。セキュリティ体制の強化に加え、Cohesityのソリューションで、以前のベンダーのデータ保護ソフトウェアよりもはるかに低いTCOを実現することができました。

「Cohesityは、私たちの環境全体の復旧と復元に絶対的な力を発揮しました。Cohesityがなければ、データを取り戻すために身代金を支払う羽目になっていたでしょう」

オリジン・プロパティ システム情報技術担当 SVP、Sirawut Chanthasangsawang氏

「Cohesityのインスタントリカバリ機能により、ランサムウェアの攻撃から3時間以内にすべてのデータを取り戻すことができました。Cohesityがなければ、データを取り戻すために身代金を支払わなければならなかったでしょう」

Sirawut Chanthasangsawang氏
オリジン・プロパティ システム情報技術担当SVP

ORIGIN

結果:

身代金の支払いなし

3時間でデータ復旧

データ損失なし

SiteOne LANDSCAPE SUPPLY

業種: 小売業
所在地: ジョージア州アトランタ
設立: 2013年

販売業者は、サイバー攻撃から24時間後にオペレーションを再開

背景:

サイトワン・ランドスケープ・サプライは、アトランタに本社を置く35億ドル規模のフォーチュン1000企業です。

米国とカナダに600以上の拠点を持ち、過去5年間に買収によって大きな成長を遂げ、売上は倍増しています。

攻撃:

2020年7月14日午前3時、テクノロジーサービス担当副社長のDavid Bannister氏は、自社の情報技術システムに対する攻撃を危惧したシニアエンジニアのひとりに起こされました。

環境は完全に停止し、ITチームは社内のサーバーやサービスにアクセスすることができなくなっていました。サイトワンは調査を開始し、法執行機関に通知し、法律顧問やその他のインシデント対応専門家に依頼し、ランサムウェアの拡散を防ぐために一連の封じ込め措置と修復措置を迅速に実施しました。

復旧:

サイトワンは、重要な業務データをすべて復旧させ、業務オペレーションへの大きな影響を防ぐことができました。

- Cohesityのデータセキュリティとデータ管理プラットフォーム上のファイル共有は、数分でリストアすることができました。
- VMを暗号化前の時点にリストアしました。そして、ラボ環境でデータを分離し、暗号化される前と暗号化されている間にどのような活動が行われていたかを特定しました。
- 本番稼働前の環境には、リアルタイムのデータレプリケーションがないサービスが多数ありました。これらのシステムをCohesityで復旧できたことは、ビジネスオペレーションの再構築に大きく貢献しました。
- サイトワンは、多数の独自およびカスタムアプリケーションを含む、コアアプリケーションとサービスのホットデータコピーとウォームスタンバイデータコピーを持っていました。

「Cohesityのスナップショットビューは有用で、私たちのフォレンジックチームに深い洞察をもたらし、サイトワンが規制要件を満たすために必要な対策を決定することができました。ランサムウェア攻撃の全体像を把握できるCohesityの機能は、ITやセキュリティチームだけでなく、法務やコミュニケーション部門も前進させ、次の対策を見極めるのに役立ちました。Cohesityの管理画面がなければ、迅速に調査し、必要なフォレンジック活動を行うことはできませんでした」とBannister氏は語ります。

「Cohesity DataLockでバックアップを固定/ロックする機能がなければ、サイバー攻撃後にこれほど早くデータを復旧することはできませんでした」

サイトワン・ランドスケープ・サプライ、
テクノロジーサービス担当副社長、David Bannister氏

「Cohesityのおかげで、私たちは24時間で復旧し業務を再開することができ、1週間以内に社内チームによって、何も複合化することなくデータを完全に復元することができました」

David Bannister氏
サイトワン・ランドスケープ・サプライ
テクノロジーサービス担当副社長

SiteOne LANDSCAPE SUPPLY

結果:

身代金の支払いなし

24時間以内に業務再開

データの復号化必要なし

コラボレーションの重要性

私たちは、ランサムウェアの惨劇と単独で戦うことはできないことを認識しています。

エコシステムは、力を増幅させることができます。そのため、私たちはデータセキュリティアライアンスを設立し、サイバーセキュリティの”真の著名人”と提携し、包括的なセキュリティ、データ保護、レジリエンス戦略のために、最も優秀な頭脳と最も大胆なソリューションを結集しています。

データセキュリティアライアンス

paloalto NETWORKS
CROWDSTRIKE
tenable
okta
MANDIANT
cisco
pwc
splunk>
securonix
CYBERARK
BigID
Qualys

“セキュリティ業界のほとんどの人は、私たちの誰もが、自分たちだけでお客様の問題を解決することはできないと認識しています。私たちは協力し合う必要があり、それがTenableのプラットフォームの重要な部分です。Cohesityやその他の業界リーダーと連携することで、お客様が攻撃対象領域を評価する機能を強化し、露出やサイバーセキュリティに対し最も重要なリスクに優先順位をつけて注力できるようにします」

テクニカルアライアンス担当副社長 Ray Komar氏

tenable

“エンドポイント、ワークロード、ユーザーを抱える組織が障壁なく業務を継続し、ランサムウェアによる窃取を含む侵害や内部脅威からデータが継続的に保護されるよう、継続的に取り組んでいます」

グローバルアライアンス担当副社長 Michael Rogers氏

CROWDSTRIKE

私たちはまた、Mandiant、Netflix、Facebook、Microsoft、国家安全保障局など、多くの企業からセキュリティに関する深い専門知識を持つ先見性のある人材を集め、Cohesity セキュリティアドバイザリーカウンシルを設立しました。

Cohesityの取締役会メンバーであるKevin Mandiaが率いるこのカウンシルは、Cohesityチーム、お客様、パートナーに、セキュリティのトレンドや、新たなサイバー脅威、脆弱性について助言を行っています。

「近年、悪質なランサムウェア攻撃が爆発的に増加しています。サイバー犯罪者はより賢くなり、企業の活動を停止させ、支払いを強要するために、しばしばレガシーバックアップを掌握しています。データセキュリティとデータ管理のリーダーは、手を取り合って、犯罪者を排除する必要があります」

Kevin Mandia, CEO

MANDIANT

Cohesityでは、最新のデータセキュリティとデータ管理プラットフォームと、協業によるエコシステムアプローチによる組み合わせの利点をお客様に提供できることを誇りにしています。

一緒にランサムウェアと戦いましょう。

COHESITY

Cohesity.com/jp | Cohesity Japan 株式会社 | 東京都千代田区大手町1-6-1 大手町ビル4F

6100020-001 JP 9-2023