fileforce®

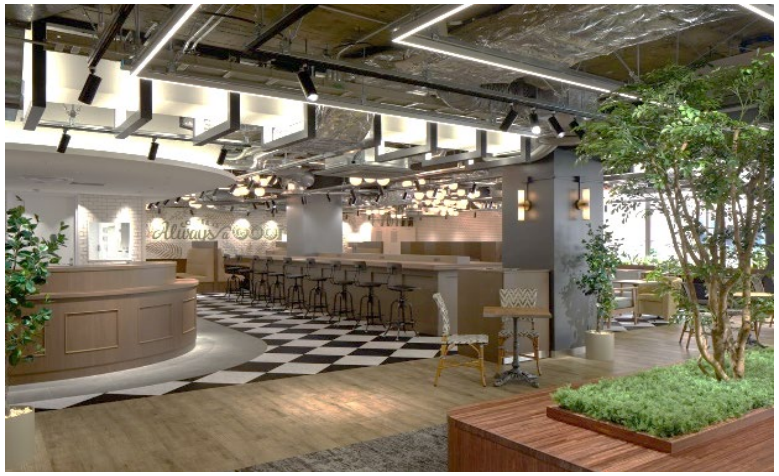
最新の“ランサムウェア”被害の現状

クラウドストレージでの対策最前線！

2025_v2

会社概要

社名	ファイルフォース株式会社
提供サービス	Fileforce®（法人向けクラウドストレージ）
サービス開始	2014年4月
所在地	東京都千代田区丸の内3丁目3-1 新東京ビル4F
資本金	100,000,000円
代表取締役	サルキシャン アラム
主要株主	株式会社NTTドコモ・ベンチャーズ／東日本電信電話株式会社／Intel Capital／株式会社シーティーエス／岡三キャピタルパートナーズ株式会社／ニッセイ・キャピタル株式会社／アーキタイプベンチャーズ株式会社



Fileforceとは

ファイルサーバーとしての利用に特化した「クラウドストレージサービス（Saas）」です

サービス
提供開始
11年

ご利用社数
23,000
社突破

使いやすさ、
サポート品質など
No.1受賞

ITreview オンラインストレージ
カテゴリーレポート 2025 Spring

サービス継続率
99%
以上

サービスご利用実績

ナショナルクライアントをはじめ
様々な規模・業種の企業様に導入いただいております。

ご利用社数
累計23,000社突破！
※OEM サービスなど含む

100年をつくる会社 鹿島
CITIZEN
Daiichi-Sankyo
KADOKAWA
文藝春秋
TOYOTA TSUSHO SYSTEMS
まだみぬ、世界は、美しい SEED
HIS
Mary's
YAOKO MARKETPLACE
イオンイーハート
Bushu Pharma
心に届く旅 阪急交通社 Direct to your heart
Tokyofm Life time audio 80.0
SUCREY AOYAMA
オリエンタルエステの スリムビューティハウス SLIM BEAUTY HOUSE
HINOMARU LIMOUSINE 株式会社 日の丸リムジン
偕行会グループ
みどり会
ALPICO GROUP
DmMiX
WORKS APPLICATIONS
株式会社Deto
朝日税理士法人
あなたの会社に元気と未来を届けます！ KODATO
足立区社会福祉協議会
建装工業
真ん中に笑顔がある会社。 三笑堂
BM
Nishitetsu Construction 西鉄建設株式会社
信金キャピタル株式会社

一部抜粋

本資料で分かる３つのこと

1. 急増するランサムウェア。企業様への影響と被害の現状
2. 従来のランサムウェア対策における課題
3. ランサムウェア対策に最適なクラウドストレージ

ランサムウェアが及ぼす企業様への影響

- ⚠ **業務停止、事業停止**
- ⚠ **情報漏えい、データ損失**
- ⚠ **社会的信用の低下**
- ⚠ **金銭的被害（身代金、復旧費用）**

ランサムウェアとは…

“身代金”という意味の「Ransom（ランサム）」と「Software（ソフトウェア）」を合わせた造語。
パソコン等の端末に**保存されているファイルやデータを暗号化**したり、端末自体をロックしたりして利用できない状態にし、その**暗号化またはロックを解除する交換条件として金銭を要求するマルウェア**（悪意のあるソフトウェアプログラム）

国内セキュリティインシデントの原因第１位は
４年連続”ランサムウェアによる被害”！

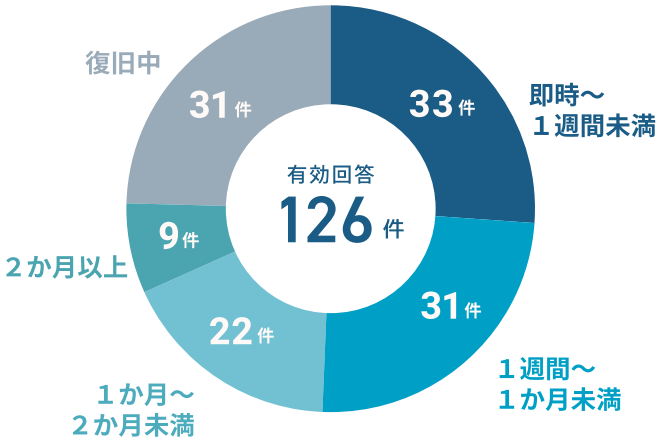
- 情報処理推進機構（IPA）の報告より、2021年～2024年で
  「国内セキュリティインシデントの原因第１位は４年連続 ”ランサムウェアによる被害”」となっています。
- 社内のファイルサーバーやＮＡＳ、バックアップストレージ等、あらゆるデータが被害の対象となっています。

順位	2020年	2021年	2022年	2023年	2024年
1位	標的型攻撃による機密情報窃取	**ランサムウェアによる被害**	**ランサムウェアによる被害**	**ランサムウェアによる被害**	**ランサムウェアによる被害**
2位	内部不正による情報漏洩	標的型攻撃による機密情報窃取	標的型攻撃による機密情報窃取	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃
5位	**ランサムウェアによる被害**	ビジネスメール詐欺による金銭被害	内部不正による情報漏洩	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

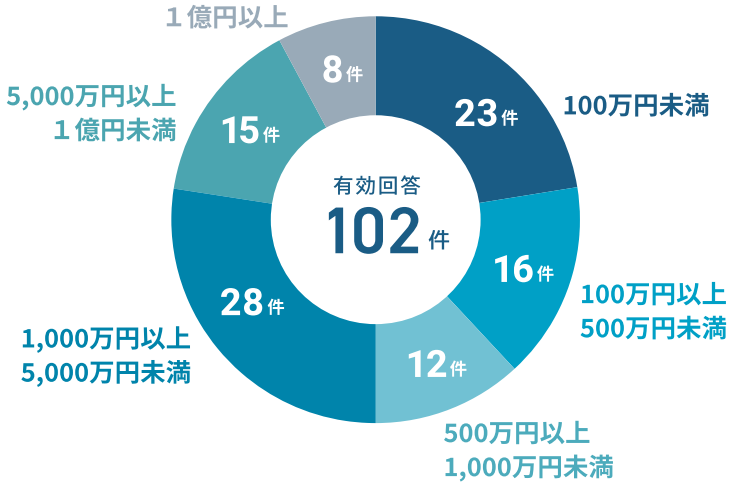
出処：独立行政法人 情報処理推進機構（IPA）：情報セキュリティ10大脅威（2020～2024）組織向け脅威

①急増するランサムウェア被害の現状

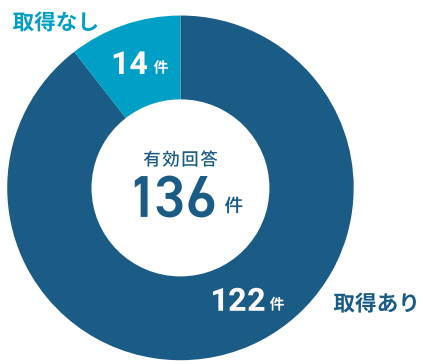
復旧に要した期間



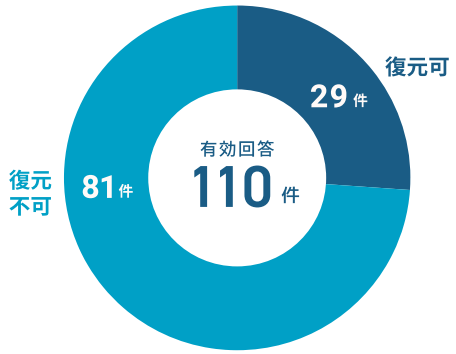
調査・復旧費用の総額



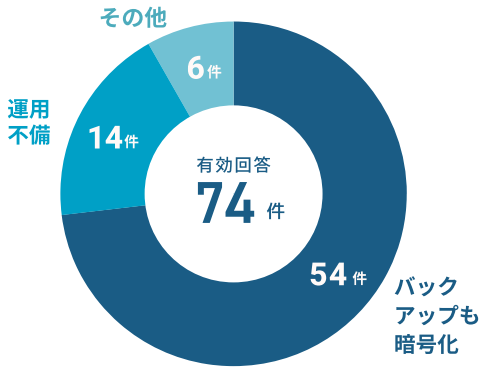
バックアップの取得状況



バックアップからの復元結果



バックアップから復元できなかった理由



ランサムウェア被害の対応には、企業様の貴重な経営資源の投入が不可避。
一方で被害のあった企業様の多くは復元に失敗。

これらのデータは氷山の一角。一部企業様の回答に過ぎず、実際の被害件数は計り知れません

出典：「令和６年上半期におけるサイバー空間をめぐる驚異の情勢等について」（警視庁）

②従来のランサムウェア対策における課題

1 バックアップがあるから万全…？

バックアップは、ある時点のデータを一括で復元する方法です。この場合は**被害を受けていないファイルまで過去の状態に戻されてしまいます。**
また、日頃からバックアップデータを取得する**手間や費用がかかる**だけでなく、**バックアップデータ自体がランサムウェアに暗号化される可能性**もあり必ずしも万全とは言えません。

2 ランサムウェアを検知、でもその後は‥？

ランサムウェア検知ツールは、ランサムウェアの侵入やその経路を分析して管理者に対処を促しますが、**ファイル自体を暗号化の被害から守り切れるわけではありません。**また、ツールの運用には**専門知識を必要**とし、ランサムウェアの**被害を受けたデータの特定や復旧対応のためには人的リソースや費用がさらにかかります。**

データ消失の被害には対処しきれない、
調査や対処の**コスト**が必要、**専門知識やノウハウ**も不足。
本当に必要な対策とは…？

③ランサムウェア対策に最適なクラウドストレージ

この機能があるクラウドストレージはFileforceだけ！

- **不審なプロセスの動きを検知して止める**
- **被害ファイルを「特定」「復元」できる**
- **オプションではなく標準機能！**

Fileforceのランサムウェア対策機能なら

手間なし！コストなし！被害なし！

対策から対処まで**一貫して「専門知識」や「追加コスト」不要。**
「データ消失被害」なし！

3つの防御壁がデータを守りぬく

Fileforce Drive

独自の仮想ファイルシステム

仮想ファイルシステムによって、エクスプローラーからクラウドへのシームレスなアクセスを実現しつつ、ランサムウェアが拠り所とするOSの機能を制御することで、Fileforce Driveへのアクセスを防止します。

ふるまい検知のヒューリスティックなアルゴリズム

ヒューリスティックなアルゴリズムで、ランサムウェアの可能性があるプロセスを検知してFileforce Driveへのアクセスを遮断します。
※100%の検知を保証するものではありません。

Fileforce Cloud

高機能なファイル変更管理システム

高機能なファイル変更管理システムにより、ランサムウェアが書き換え・暗号化したファイルをピンポイントで特定し、元の状態に戻します。

ランサムウェア対策に最適なクラウドストレージ

被害拡大を防止する

ランサムウェアの可能性のあるプログラムを検知した場合、組織内にあるすべてFileforceDriveに情報が共有されてプロセスのアクセスを遮断します。

▼ここが違う！
遮断するのはあくまでもそのプログラムに限定。
業務に極力影響が無いように、ユーザーの操作によるFileforceへのアクセスは止めません。

被害範囲がすぐわかる

被害を受けた可能性のあるファイルはワンクリックで自動的にリスト化でき、被害状況の把握や確認、報告といった業務負担を圧倒的に軽減します。

▼ここが違う！
ランサムウェア被害の際の、慣例法令対応やステークホルダーへの報告業務をスムーズにします。

ワンクリックで復旧

組織全体の被害にあったファイルは、管理者のワンクリックで「暗号化前の状態」に戻すことが可能です。

▼ここが違う！
バックアップからの復元と異なり、被害に合ったファイルを特定して復旧します。そのため通常業務で更新したファイルは最新の状態を維持することが可能です。

ゼロデイ攻撃に強い

未知や新種のランサムウェアを含め、検知できるヒューリスティックなアルゴリズムが標準で実装されています。

▼ここが違う！
管理者による事前設定は一切不要。ランサムウェア検知アルゴリズムはファイルフォース社側で自動メンテナンスされます。

標準機能として提供

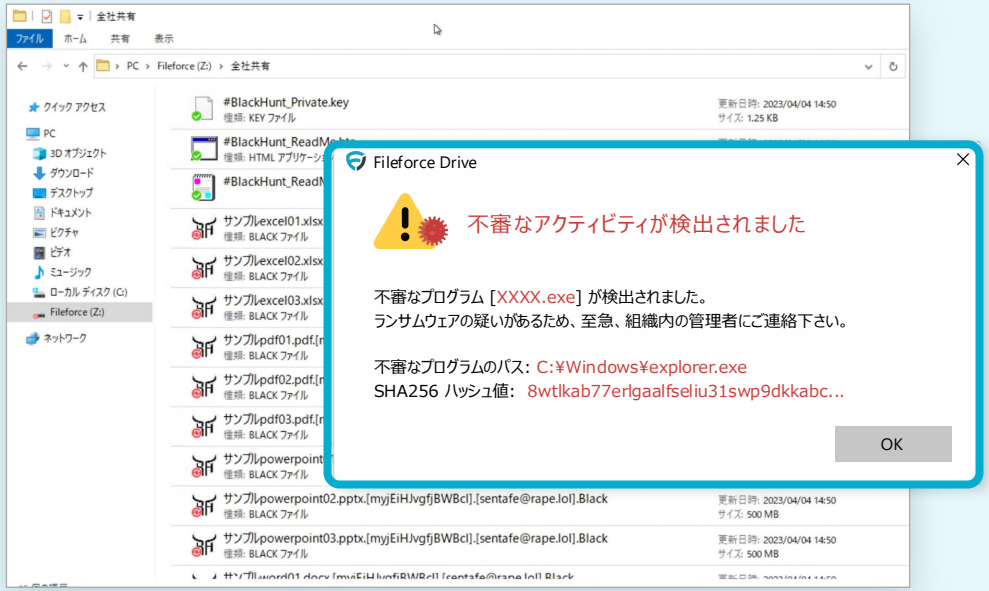
ランサムウェア対策機能のご利用には追加費用が発生しません。Fileforceにファイルを保管するだけで、ランサムウェアからファイルを守ります。

▼ここが違う！
全ての料金プランで標準提供！利用規模や使い方に関わらず、安心してファイルを保管いただけます。

ランサムウェア対策機能の画面

エクスプローラーでのふるまい検知

Fileforce Driveで不審な動きが
あった際に検知



インシデント管理画面

検知後は管理者画面で対処
（被害ファイルを一括で復旧）

事例

ITmediaビジネス ONLINE Special

ITmedia ビジネスオンライン > ランサムウェア被害から「25分で1万3000ファイル」を復旧！　事例...

PR

ランサムウェア被害から「25分で1万3000ファイル」を復旧！　事例から学ぶ、これからのデータの守り方

2023年08月21日 10時00分 公開　[ITmedia]

印刷　見る　Share　B!

企業を取り巻くリスクは多様だが、サイバー攻撃――特にランサムウェア攻撃は極めて危険な脅威として知られるようになった。ランサムウェア攻撃とは感染したデバイスをロックしたりデータ／ファイルを暗号化したりして“人質”にとり、その復旧と引き換えに金銭を要求する手口で、その被害は近年拡大の一途をたどっている。

警視庁が2023年3月に発表した「令和4年におけるサイバー空間をめぐる脅威の情勢等について」によれば、警察庁に報告されたランサムウェア被害件数は20年下半期から右肩上がりに上昇しており、22年の被害件数は230件と、前年比57%増となった。また、情報処理推進機構（IPA）が発表した最新版の「情報セキュリティ10大脅威 2023」でも「ランサムウェアによる被害」が3年連続で1位となっている。

ランサムウェア攻撃は業種や企業規模にかかわらず、どんな企業でもターゲットになるため対策は必須といえる。しかし一口に対策と言っても方法はさまざまある。

事例記事

ランサムウェア被害から「25分で1万3000ファイル」を復旧！

以下から記事をご覧いただけます。

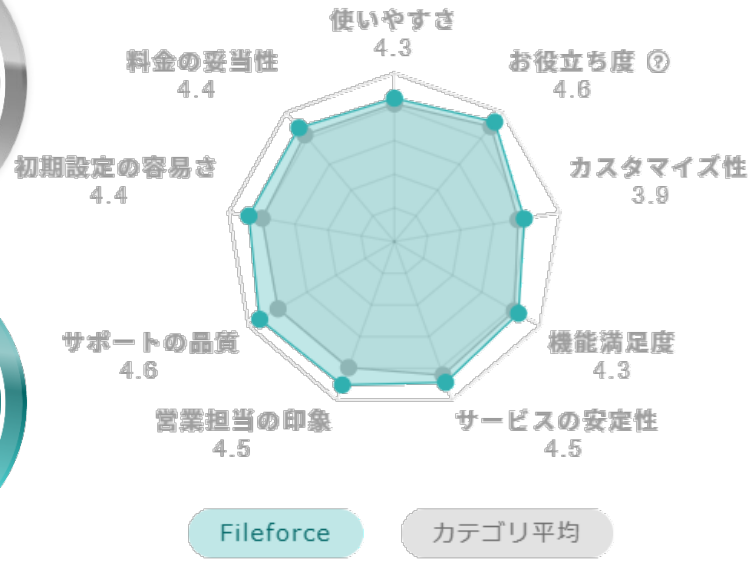
ITmediaビジネスオンライン
https://www.itmedia.co.jp/business/articles/2308/21/news016.html

Fileforceオウンドメディア TeamDX
https://www.fileforce.jp/teamdx/a_22908/

クラウドストレージFileforceは以下で受賞しています

「BOXIL SaaS AWARD Summer 2025」
オンラインストレージ部門で

12期連続で
「Good Service」受賞！



受賞の詳細：https://www.fileforce.jp/news/20250603news/

「ITreviewカテゴリーレポート2025 Spring」
オンラインストレージ部門

使いやすさ・サポート品質など
6項目でNo.1に選出！

使いやすさ　サポート品質　バージョン管理
アクセス制御　ログ管理　管理のしやすさ

ITreview オンラインストレージ
カテゴリーレポート 2025 Spring

ITreview オンラインストレージ
カテゴリーレポート 2025 Spring

受賞の詳細：https://www.fileforce.jp/news/20250514news/

導入からご利用開始までの流れ

STEP1	STEP2	STEP3	STEP4	START
情報収集 ・資料ダウンロード ・サービス確認（お打ち合わせ）	30日無料 トライアル	導入前 質疑応答	ご利用 申し込み	ご利用 開始

検討から導入・活用まで
多くのノウハウを元に支援いたします

クラウド化へご不安な企業様でもご安心頂けるような
サポート・支援を行いますので是非ご利用くださいませ。

30日間無料トライアルの申込はこちら ▶ https://www.fileforce.jp/trial/

最後までご覧頂きまして
ありがとうございました。

https://www.fileforce.jp/