

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！



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／ NTT東日本株式会社／Intel Capital／ 株式会社シーティーエス／岡三キャピタルパート ナース株式会社／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



ニッセイ・キャピタル株式会社



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

12年



ご利用社数

25,000
社突破



使いやすさ、
サポート品質など

No.1
受賞



サービス継続率

99%
以上



サービスご利用実績

ご利用社数
25,000社
突破！
※OEM サービスなど含む

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。

HONDA

CITIZEN

Samantha Thavasa

Mary's

株式会社 いけうち

株式会社 **Deto**

EGURO

waazwiz
JAPAN

ピーエス・コンストラクション

100年をつくる会社
in 鹿島

Nishitetsu Construction
西鉄建設株式会社

岡本土木株式会社

JSTE

株式会社 守谷 商会

建装工業

Eisai

まだみぬ、世界は、美しい
SEED

Bushu
Pharma

真ん中に笑顔がある会社。
三笑堂

奈良県立医科大学附属病院
Nara Medical University Hospital

偕行会グループ

株式会社
あいらいふ

足立区社会福祉協議会

町田市
MACHIDA City

佐世保市
SASEBO CITY

育てよう明日を
JAグループ鹿児島

YAKO
MARKETPLACE

イオンイーハート

BOOK・OFF

あなたの会社に元氣と未来を届けます！
KODATO

朝日税理士法人

HINOMARU LIMOUSINE
株式会社 日の丸リムジン

MARUHAN

心に届く旅
阪急交通社
Direct to your heart

西遊旅行
SAIYU TRAVEL Co.,Ltd.

HIS

文藝春秋

KADOKAWA

Tokyofm
Life time audio 80.0

共テレ

ALPICO GROUP

株式会社 グランサクシード

WORKS APPLICATIONS

DmMiX

みどり会

TOYOTA TSUSHO SYSTEMS

RELO CLUB

オリエンタルエステの
スリムビューティハウス
SLIM BEAUTY HOUSE

FFG
FFGベンチャービジネスパートナーズ

ZENKANKYO REIWA SONPO
全管協利いわ損害保険株式会社

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 ——— P.6
- 2 従来のランサムウェア対策における課題 ————— P.9
- 3 ランサムウェア対策に最適なクラウドストレージ ————— P.10

①急増するランサムウェア・企業様への影響

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



金銭的被害（身代金、復旧費用）



社会的信用の低下

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）

①急増するランサムウェア・企業様への影響

国内セキュリティインシデントの原因

第1位は6年連続“ランサムウェアによる被害”



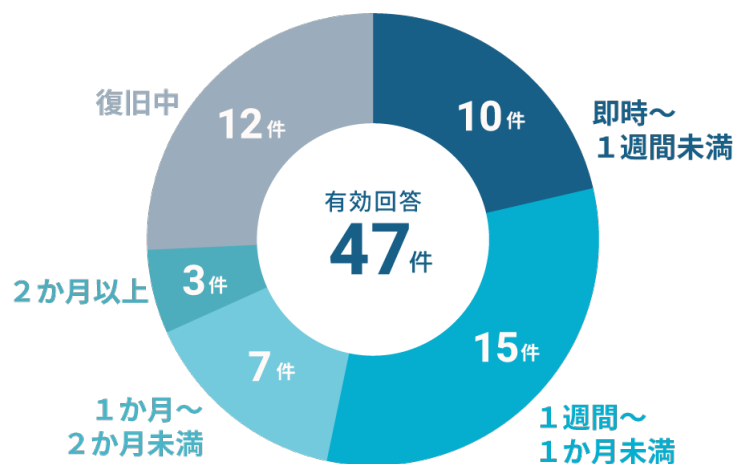
- 情報処理推進機構（IPA）の報告より、2021年～2026年で「国内セキュリティインシデントの原因第1位は6年連続で”ランサムウェアによる被害”」となっています。
- 社内のファイルサーバーやNAS、バックアップストレージ等、あらゆるデータが被害の対象となっています。

順位	2021年	2022年	2023年	2024年	2025年	2026年
1位	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	ランサムウェアによる被害	ランサム攻撃による被害
2位	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	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃
3位	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）	機密情報などを狙った標的型攻撃	AIの利用をめぐるサイバーリスク

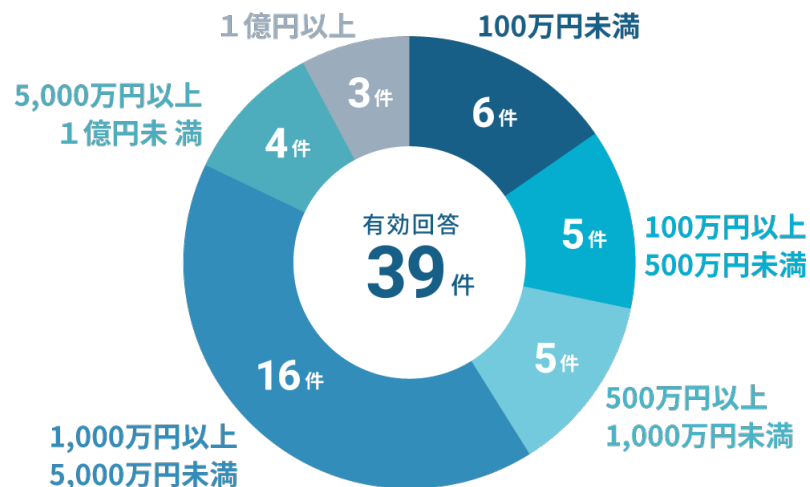
出処：独立行政法人 情報処理推進機構（IPA）：情報セキュリティ10大脅威（2021～2026）組織向け脅威

①急増するランサムウェア・企業様への影響

復旧に要した期間

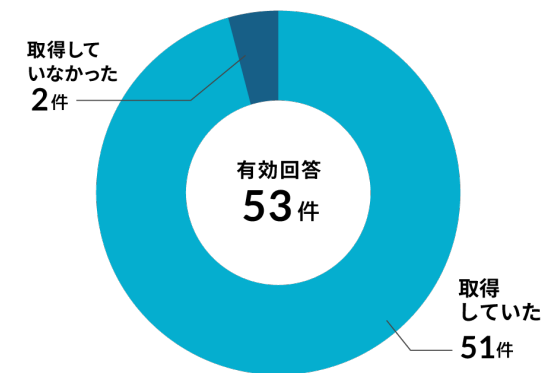


調査・復旧費用の総額



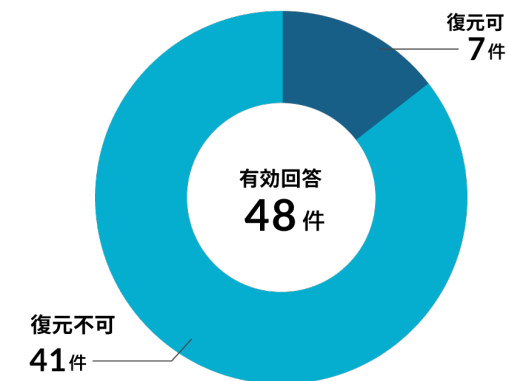
バックアップ取得の有無

9割以上がバックアップを取得



復元結果

9割近くが復元に失敗



出典：「令和7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）

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

②従来のランサムウェア対策における課題

バックアップがあるから万全？

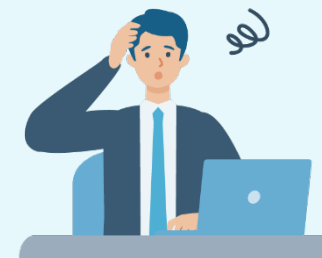
バックアップは、ある時点のデータを一括で復元する方法です。この場合は被害を受けていないファイルまで過去の状態に戻されてしまいます。

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。

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？



本資料で分かる3つのこと

③ ランサムウェア対策に最適なクラウドストレージ

専門知識や
追加コスト不要！
データ消失被害なし！



この機能があるクラウドストレージはFileforceだけ！

1 不審なプロセスの動きを検知して止める

2 被害ファイルを特定・復元

3 オプションではなく標準機能！

Fileforce ドライブ

独自の仮想 ファイルシステム

エクスプローラー/Finderからクラウドへのシームレスなアクセスを実現しつつ、OS機能を制御することでFileforce ドライブ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

ランサムウェアの可能性があるプロセスを検知、Fileforceドライブ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

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。



お客様の声を反映したランサムウェア対策機能



被害拡大を防止

ランサムウェアの可能性のあるプログラムを検知すると、組織内の全 Fileforce ドライブに情報が共有され、プロセスのアクセスを遮断します。

POINT

遮断するのはそのプログラム限定。業務に影響が無いよう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、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。

POINT

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。

POINT

バックアップからの復元と異なり、被害にあったファイルを特定し復旧。通常業務で更新したファイルを最新の状態で維持できます。



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。

POINT

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なし。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。

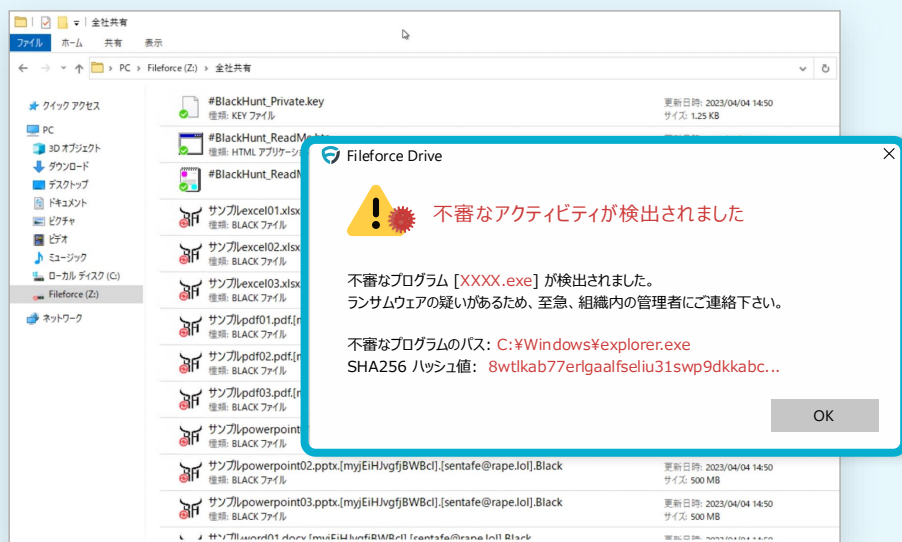
POINT

全ての料金プランで標準提供！ご利用規模や使い方に問わず、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/Finderでのふるまい検知

Fileforceドライブで不審な動きが
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

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ください。

ITmediaビジネスオンライン

<https://www.itmedia.co.jp/business/articles/2308/21/news016.html>

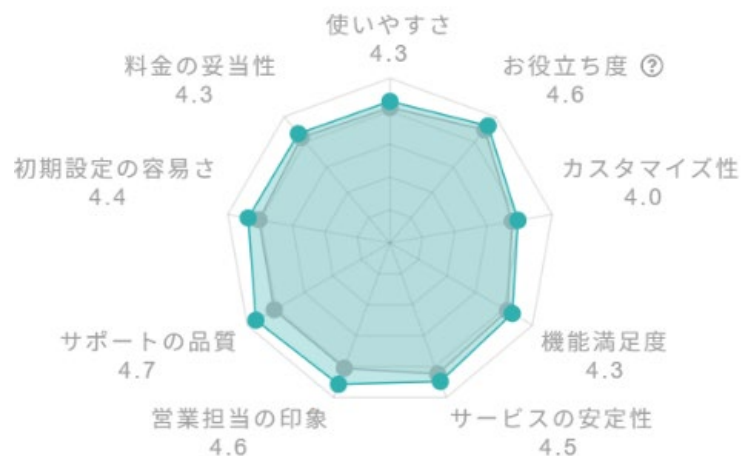
Fileforceオウンドメディア TeamDX

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 Autumn 2025」
オンラインストレージ部門で

13期連続で
「Good Service」受賞！



Fileforce

カテゴリ平均

受賞の詳細： <https://www.fileforce.jp/news/20250905news/>

「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



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/>