PURESTORAGE®

Pure Storage の

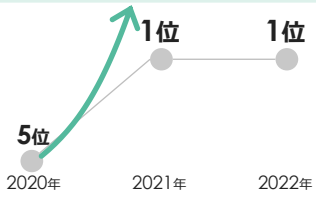
高速リストア可能なオフラインデバイス

SafeModeで安心・安全なランサムウェア対策を実現

Pure Storage ランサムウェア対策ソリューション

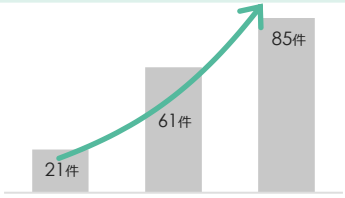
ランサムウェアによる被害は
数年にわたり
セキュリティリスクの上位
かつ**近年ではトップ**に

情報セキュリティ 10 大脅威



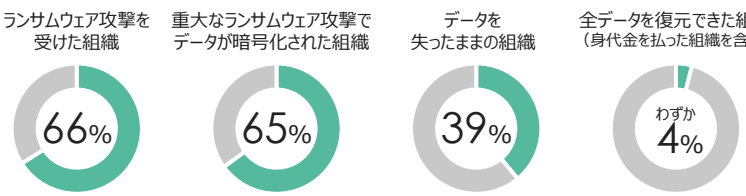
出典：IPA「情報セキュリティ 10 大脅威」
https://www.ipa.go.jp/files/000096258.pdf

ランサムウェア件数の推移



SOPHOS ホワイトペーパー 「ランサムウェアの現状 2022年版」

調査対象
5,600社の
IT意思決定者

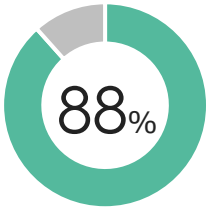


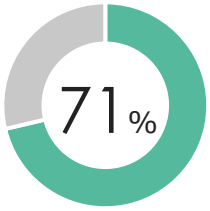
出典：https://assets.sophos.com/X24WTUEQ/at/jcn5nw9bmk433pnhvg46h3/sophos-state-of-ransomware-2022-wpja.pdf

ランサムウェア対策
としての
バックアップの
重要性が高まる

単純な
バックアップ では
不十分

バックアップ取得状況





復元結果

出典:「令和３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」(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf を一部加工

攻撃者は**バックアップ**も
破壊するため
"オフラインデバイス" が
重要

NISC ランサムウェアによるサイバー攻撃について

- ランサムウェア感染時でもバックアップが保護されるように留意する
- ネットワークからアクセスできないようにする等の対策を講じる

事例（2022年1月）

- 社内ネットワークに侵入後、**管理者権限を奪ってID/パスワードを窃取**
- 最終的に9台の機器へ不正接続され、内6台がランサムウェアによってファイルを暗号化された

管理者権限が奪われ
管理配下の機器に
不正接続されるケースも

出典:「コンピュータウイルス・不正アクセスの届出事例［2022年上半期（1月～6月）］」(IPA)
https://www.ipa.go.jp/files/000100440.pdf より一部抜粋

バックアップ用オフラインデバイスとしての
"テープ"は 「復旧に時間がかかる」
「確実性に懸念が残る」

Pure Storage の SafeMode で
ランサムウェアからの確実な保護と
大量データの高速リストアを実現

PURESTORAGE®

Pure Storage の SafeMode でいかなる状況でもリストア可能に
管理者権限でもアクセス不可能な領域を標準機能で確保

通常のスナップショット機能では

オペレーションミスには対応できるが
ランサムウェアには対応できない

- 削除されたオブジェクトは Destroyed Objects で一時的に保持
- その後オブジェクトは完全に削除され容量を解放

Snapshotは

管理者による操作

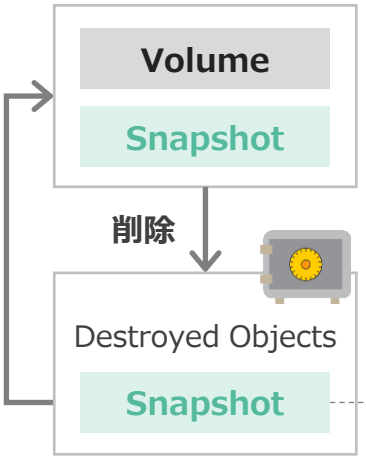
または

保持期間経過後

24時間で自動的に削除される

SafeMode 有効時は

管理者権限から削除権限を剥奪し
ランサムウェアにも対応



- 悪意ある攻撃者であっても、Snapshotを削除できない
- 万が一攻撃が遂行されても、迅速にリカバリ

Snapshotは

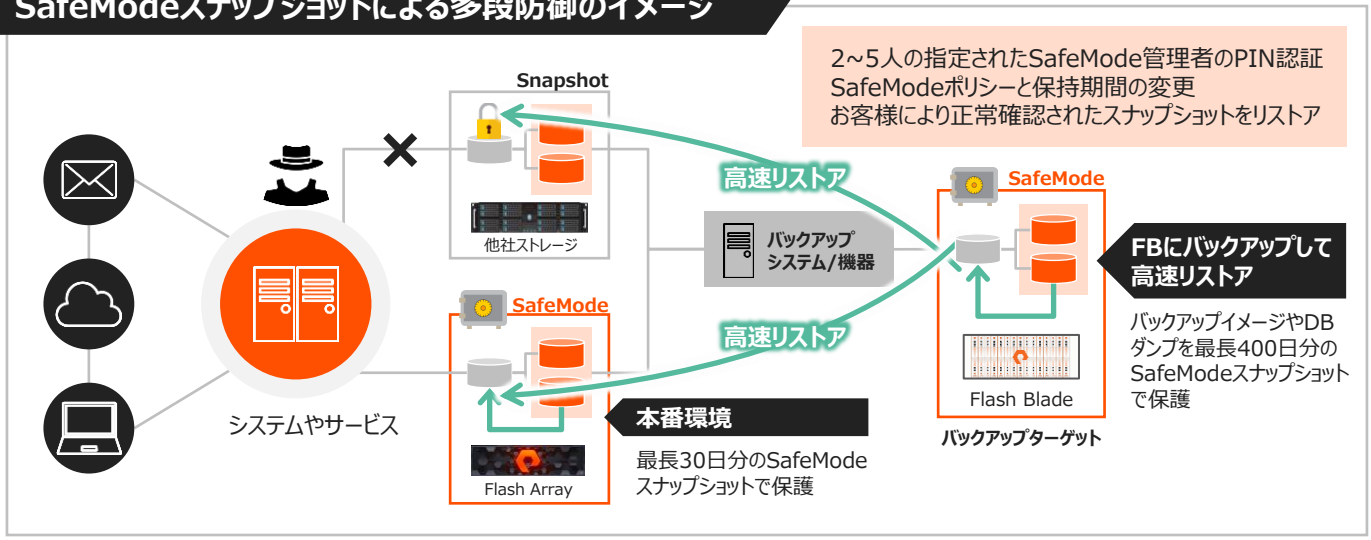
管理者による操作

であっても**削除不可**

保持期間経過後

でなければ
完全に**削除されない**

SafeModeスナップショットによる多段防御のイメージ



PURESTORAGE®