VERITAS

ランサムウェア被害からの復旧をシンプルに確実に実現する

ベリタスのデータ保護ソリューション

ベリタステクノロジーズ合同会社

Agenda

- 背景と課題
- 課題解決のための要件とベリタスのソリューション
- 実現イメージ
- お客様のメリット
- まとめ

Agenda

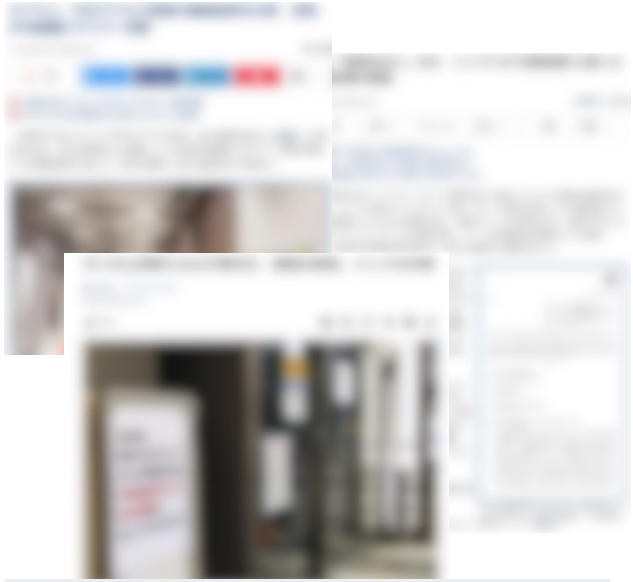
- 背景と課題
- 課題解決のための要件とベリタスのソリューション
- 実現イメージ
- お客様のメリット
- まとめ

サイバー犯罪者は今日もあなたの環境を狙っている

もはや、「もし」ではなく
「いつ？」の問題

日本でも拡大するランサムウェアの驚異

ランサムウェアが現実的な停止・データ損失リスクに



実際に事業停止が発生
バックアップシステムも攻撃対象

高まるランサムウェア被害の意識

IPA情報セキュリティ10大脅威 2023*1

順位	脅威（組織）	昨年順位
1	ランサムウェアによる被害	1
2	標的型攻撃による機密情報の搾取	2
3	サプライチェーンの弱点を悪用した攻撃	4
4	テレワーク等のニューノーマルな働き方を狙った攻撃	3
5	内部不正による情報漏洩	6
6	脆弱性対策情報の公開に伴う悪用増加	10
7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW

2021年から1位として脅威の
重大性に対する意識が高まる

求められる復旧手段

一般的なセキュリティ対策
ソリューションの投資領域

特定 → 防御 → 検知 → 対応 → **復旧**

- ☒ セキュリティ対策は必要。ただし侵入/感染を100%防ぐことは困難。
- ☒ 脆弱なバックアップシステムも狙われ、バックアップデータが感染してしまう。
- ☒ 身代金を支払ってもデータを回復できるとは限らない。さらなる資金源になりうる。

侵入・感染を前提とした
セキュリティ対策が必要

*1 出典：情報処理推進機構「情報セキュリティ10大脅威 2023」
URL https://www.ipa.go.jp/security/vuln/10threats2023.html

ランサムウェアの脅威が増大している要因

IT環境の複雑化

ランサムウェア攻撃の
ビジネス化

重要なインフラストラクチャに
対する攻撃の数が増加

新しいテクノロジーや
クラウドの活用が進む

サイバー犯罪者は、お互いに情報を
共有し、より精通し洗練化している

サプライチェーン攻撃は
2023年に300%増加

サイバー攻撃に耐える堅牢なバックアップシステムの構築が急務

サイバー犯罪者は、
最初のステップとして
バックアップを狙っている

しかしサイバー攻撃に対抗するためのバックアップ施策は多く複雑

Agenda

- 背景と課題
- 課題解決のための要件とベリタスのソリューション
- 実現イメージ
- お客様のメリット
- まとめ

サイバー攻撃から確実に復旧するために必要な要件

統合的、確実に保護し、クリーンなデータ回復を実現するためには？

1

IT環境全体の確実な保護

- どのシステムがサイバー攻撃に会うかわからないため、網羅的な保護が必要
- 網羅的保護のための複雑なシステムは非効率なため、シンプルな統合システムが求められる

2

不正侵入防止策

- 最後の砦であるバックアップシステムが無効化されるリスクを下げる必要がある

3

バックアップデータの改ざん・消去防止策

- 万が一バックアップシステムに不正アクセスされてしまっても、バックアップデータを改ざんされない対策が必要

4

ランサムウェア被害検知・検出

- ゼロデイ攻撃に気が付かないとすべての世代のバックアップデータが暗号化されたデータのバックアップデータになってしまう事を防ぐ必要がある
- リストアによるランサムウェアの拡散・再感染を防ぐ必要がある

5

RPO/RTOに応じた迅速・柔軟なリカバリ

- 大規模な被害に対応するため高速な回復が求められる
- 被害の状況に応じた柔軟な回復の選択肢が求められる
- 復旧単位、復旧先

１．IT環境全体の確実な保護

IT環境全体の保護に必要な要素

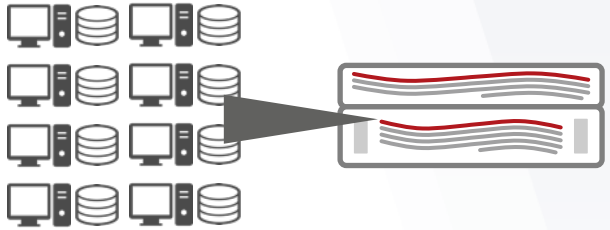
保護対象の幅広い対応

1つのデータ保護
プラットフォームで
企業の全データをカバー

高速なバックアップ

バックアップと
レプリケーションの
高パフォーマンス

シンプルな構成



少ないバックアップサーバ台数
プロキシサーバ不要
重複排除ストレージ不要

これらの特長を備えた NetBackupは、統合バックアップに最適

NetBackupは、企業のあらゆるデータを保護

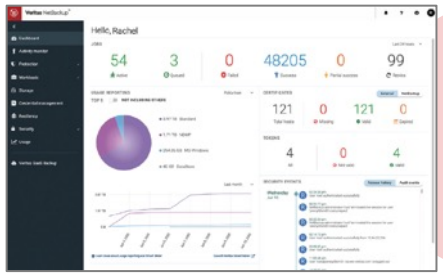
保護対象の幅広い対応

物理環境 | DB/アプリケーション | OSS/ビッグデータ

仮想環境/HCI | K8s/コンテナ | パブリッククラウド クラウドストレージ

aws Google Cloud

データソース (OS 100+) 800+



統合監視

SaaS アプリケーション

Microsoft 365 box salesforce

NetBackup / NetBackup Flexアプライアンス / Veritas Alta Data Protection

Veritas Alta SaaS Protection

ストレージターゲット 1400+

サードパーティ ストレージ/テープ

NetBackup Flex アプライアンス

Veritas Alta Recovery Vault

aws Google Cloud

クラウドストレージ オブジェクトストレージ

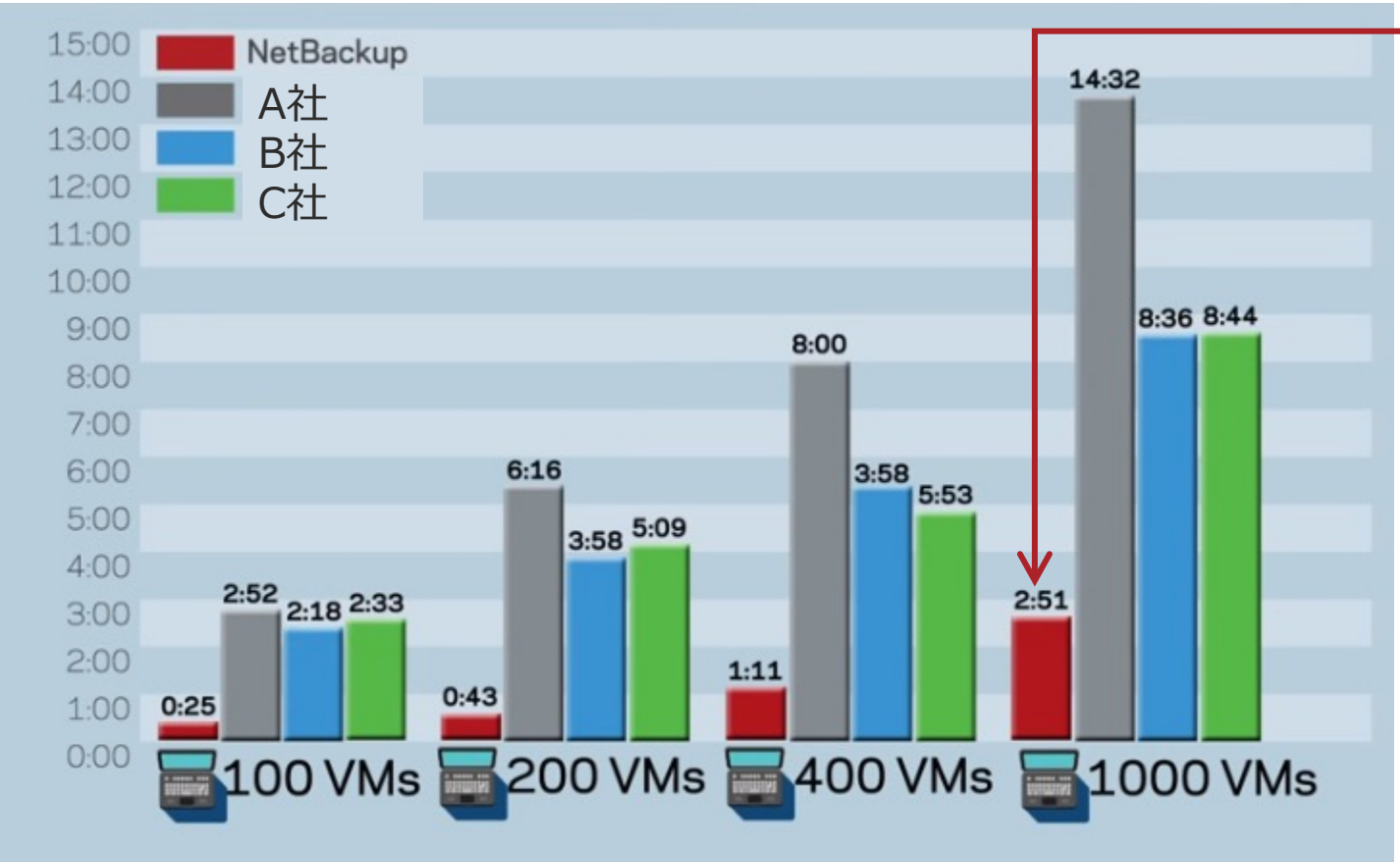
クラウドストレージ オブジェクトストレージ 60+

物理、仮想化、クラウド、SaaS まで、あらゆる環境 の あらゆるデータを NetBackup 1つのソリューションで統合バックアップ可能です

VERITAS

高速な
バックアップ

群を抜く ハイパフォーマンスなNetBackup



他社製品と比較して、

5倍高速！！

1000台2.5TBの仮想マシンを
2時間51分でバックアップ！！

同じ仮想マシンバックアップでも、
重複排除処理とバックアップのメタデータ操作が高速なので、
ここまで差が出る！！

https://www.youtube.com/watch?v=tprUkIXa9rE

NetBackup は **群を抜く超高速な** 重複排除・永久増分バックアップ

バックアップシステムの全ての役割を兼ね備えた シンプルなアプライアンス

シンプルな構成

セキュリティ強化済み専用OS

NetBackupソフトウェア
- ✓ BCP対策機能
- ✓ ランサムウェア対策機能など含む

バックアップ管理サーバ

バックアップ保存先管理サーバ

VADPプロキシサーバ

クラウドストレージ・ゲートウェイ

重複排除ストレージ

WORMストレージ

CIFS／NFSストレージ

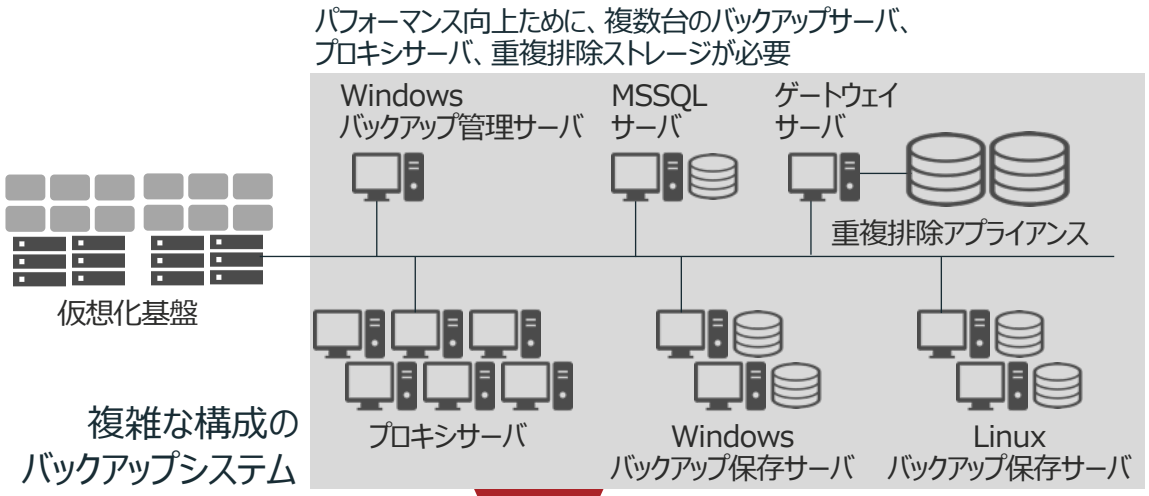
エージェントレス仮想マシン運用

NetBackup Flex アプライアンス

NetBackup Flex アプライアンスは 圧倒的なシンプル構成

シンプルな構成

バックアップソフトAとの比較

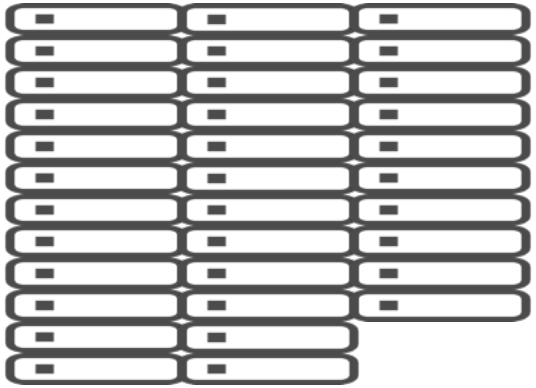


台数10分の1以下

NetBackup Flex アプライアンス

全ての役割を兼ね備えたシンプルなアプライアンス

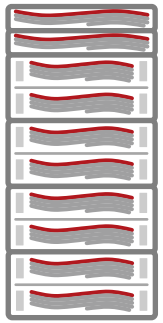
アプライアンスBとの比較（2PB）



ラックユニット　：**68U**
ネットワーク　：408ポート
電力消費　：**17,730W**
冷却熱量　：114,274 BTU/秒

さらに、クラウドストレージに複製するための追加ライセンスが必要

設置面積、電力消費に大きな差



NetBackup Flex アプライアンス

ラックユニット　：**24U**
ネットワーク　：28ポート
電力消費　：**5,800W**
冷却熱量　：25,152 BTU/秒

VERITAS

2．不正侵入防止策

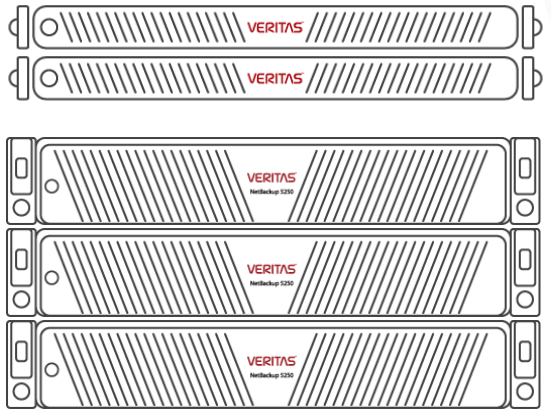
セキュアなバックアップ専用アプライアンス

汎用OS ＋ バックアップソフト

- バックアップソフト
- 汎用OS
- IAサーバ ｜ 仮想環境
- 重複排除ストレージ

VS

NetBackup Flex アプライアンス



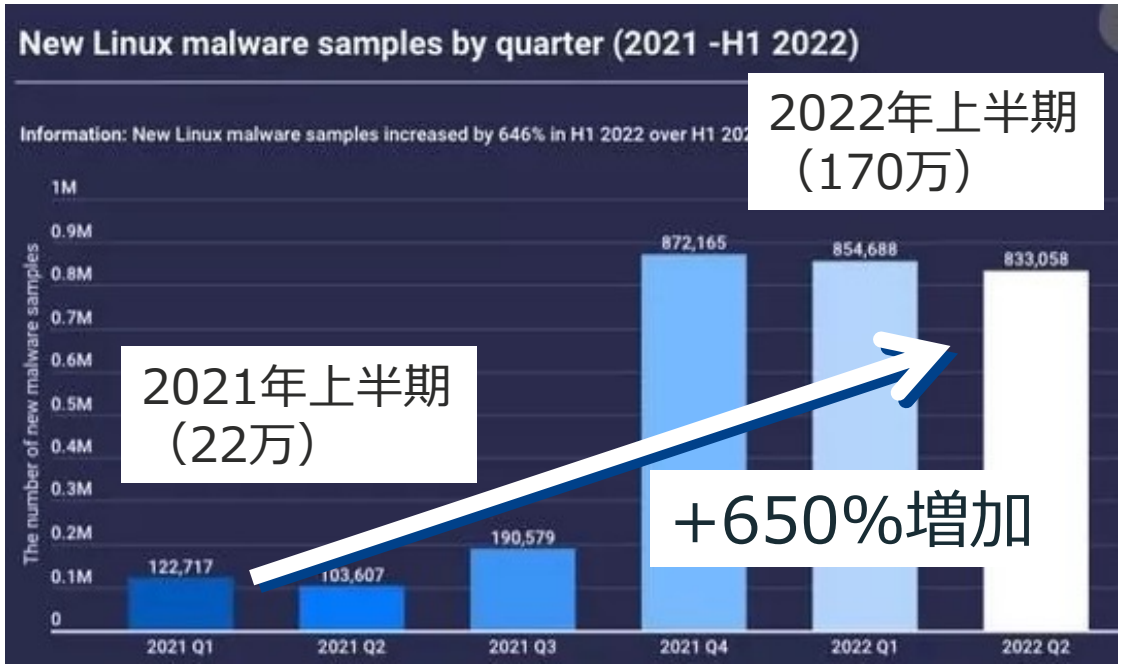
製品/パッチリリース時に
脆弱性チェックなどを実施

米国最大の
セキュリティカンファレンス
“Black hat”へ複数年出展し
全ての攻撃を防御

ランサムウェアは、バックアップサーバが稼働する汎用OSの脆弱性をついて侵入します。
ベリタスは
セキュアな専用OSのNetBackup Flex アプライアンス
を提供します

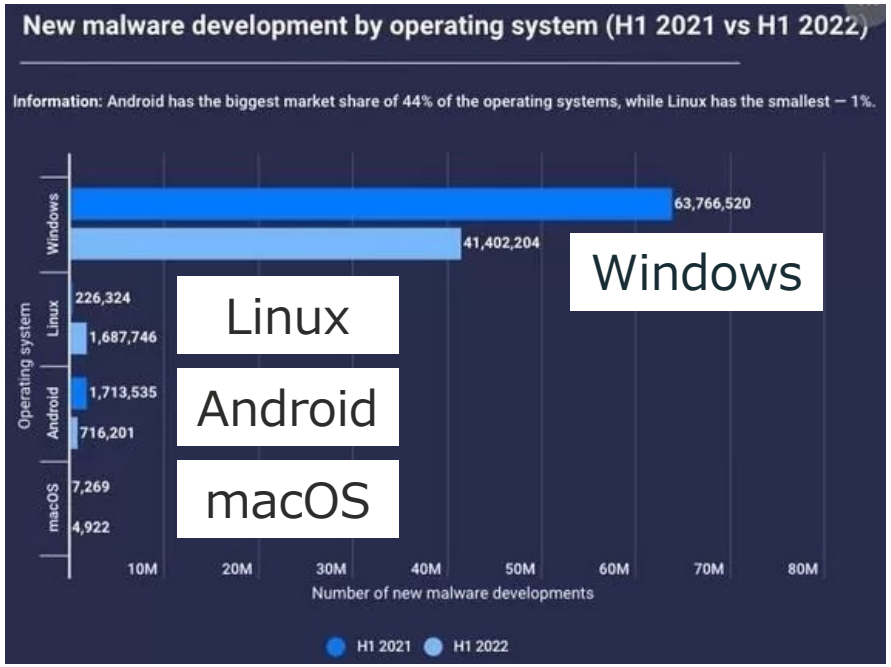
汎用OSが狙われています

Linuxの新規マルウェアが
前年比 +650%増加



Linuxの新規マルウェアのサンプル数

しかし、全体としては
依然としてWindowsが最も多い



OS毎の新規マルウェアのサンプル数

汎用OS（Windows、Linux）のバックアップサーバは、セキュリティリスク

【参考】https://news.mynavi.jp/techplus/article/20220730-2411054/

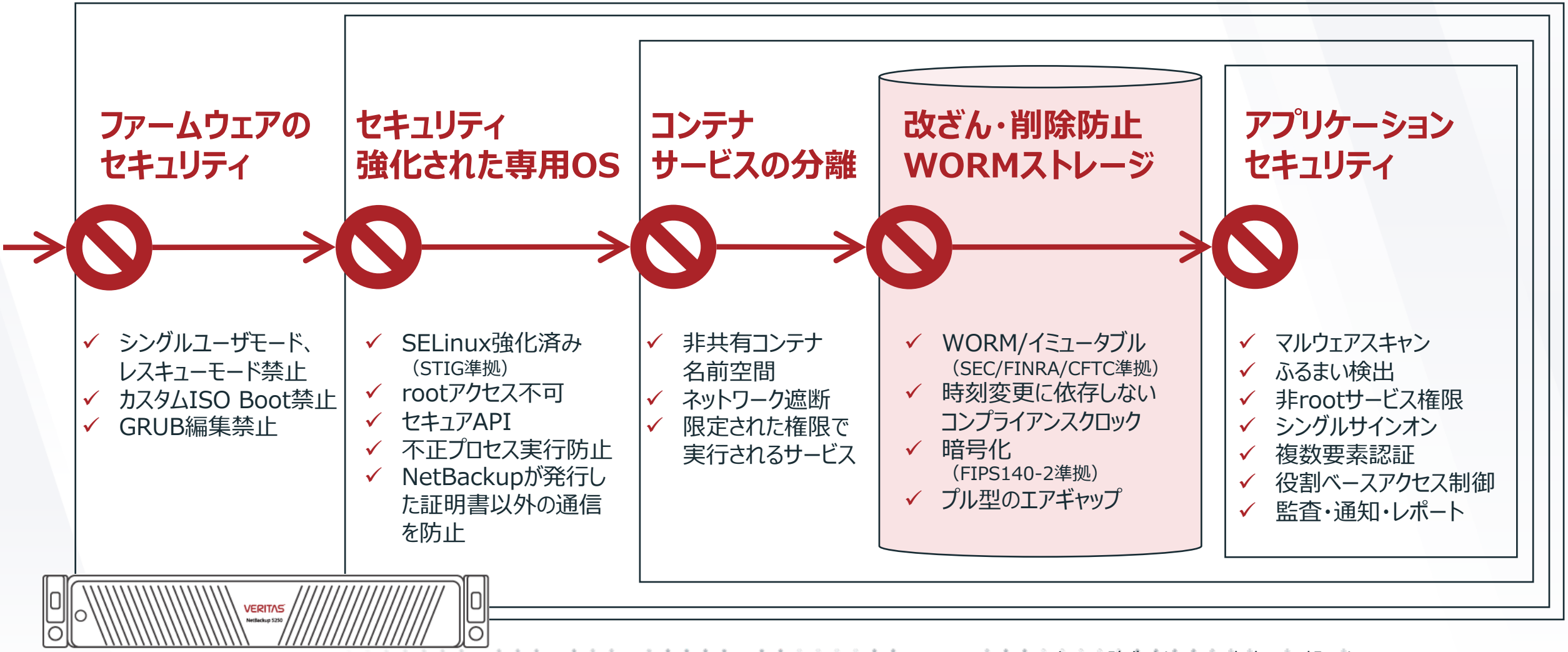
ゼロトラストの考えに基づくエンドツーエンドのサイバーレジリエンス

ゼロトラストアーキテクチャ

イミュータビリティ	分離	インテリジェンス	統合化されたセキュリティ	インサイト
イミュータブルストレージ WORMストレージ	分離された リカバリ環境	マルウェア検出 と異常検出	多層化された サイバーセキュリティ	セキュリティ制御 とインサイト

サイバー攻撃をシャットアウトする万全な実装

NetBackup Flex アプライアンス の多層防御

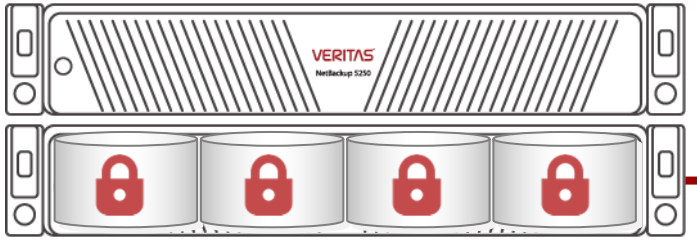


※上記は強化されている内容の一部です。

３．バックアップデータの改ざん・消去防止策

NetBackup Flex アプライアンスの堅牢な改ざん防止機能

NetBackup Flex アプライアンスは、ランサムウェアからバックアップデータを確実に保護します。



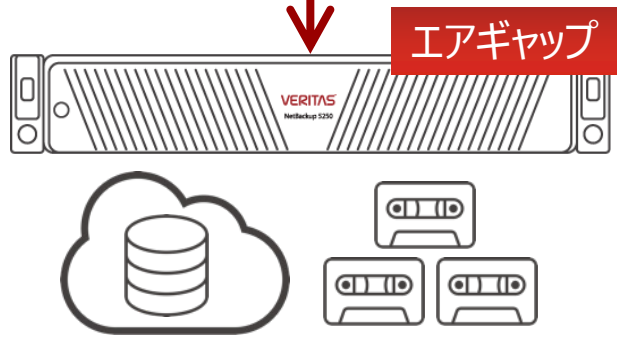
暗号化

データ転送時、データ保管時
- AES 256-bit
- FIPS 140-2
- 2048 bitキー
- TLS 1.2証明書

改ざん防止／削除防止

幅い広いWORM対応
- Veritas Flex アプライアンス
- クラウドストレージWORM機能
- サードパーティ製WORM

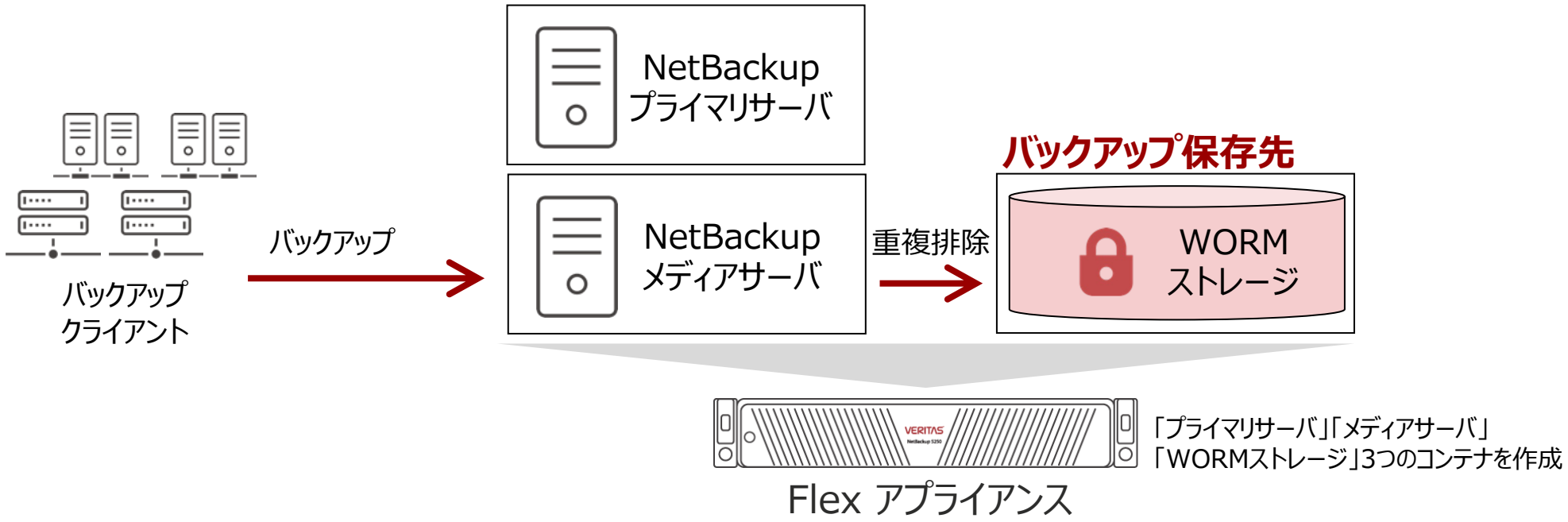
遠隔地への複製



レプリケーション、クラウド、テープ

NetBackup Flex アプライアンス：　WORMストレージ構成

Flex アプライアンスは、
1台のハードウェア上に、コンテナでNetBackupサーバとWORMストレージを構築できます。
コンテナで構成するため、セキュア、かつ、高速に構築／アップグレード可能です。



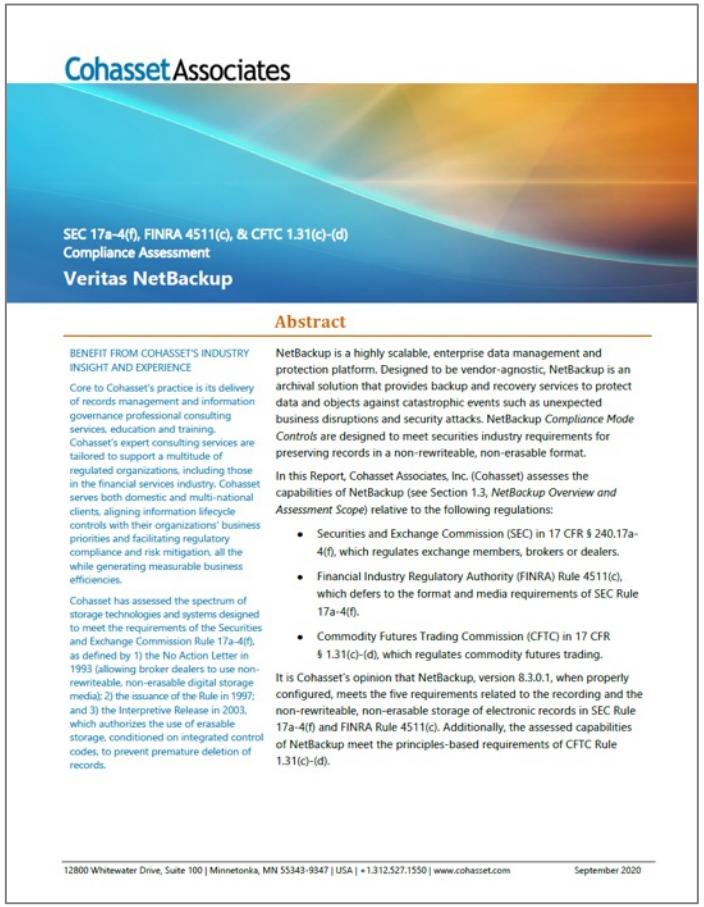
Flex Appliance 1台上に、バックアップサーバとWORMストレージを構成可能

セキュリティ要件（SEC、FINRA、CFTC）評価済み

Flex アプライアンス の WORM機能は、
下記のセキュリティ要件を満たしています。

- ✓ **SEC Rule 17a-4(f)**
- ✓ **FINRA Rule 4511(c)**
- ✓ **CFTC Rule 1.31(c)-(d)**

Cohasset Associates社により、評価・証明されています。
Cohasset Associates社は、記録管理と情報のガバナンスを専門とするマネジメントコンサルティング企業です。
Amazon S3オブジェクトロック（WORM）の規制対応を評価、証明している企業でもあります。



Cohasset Associates

SEC 17a-4(f), FINRA 4511(c), & CFTC 1.31(c)-(d)
Compliance Assessment
Veritas NetBackup

Abstract

BENEFIT FROM COHASSET'S INDUSTRY INSIGHT AND EXPERIENCE

Core to Cohasset's practice is its delivery of records management and information governance professional consulting services, education and training. Cohasset's expert consulting services are tailored to support a multitude of regulated organizations, including those in the financial services industry. Cohasset serves both domestic and multi-national clients, aligning information lifecycle controls with their organizations' business priorities and facilitating regulatory compliance and risk mitigation, all the while generating measurable business efficiencies.

Cohasset has assessed the spectrum of storage technologies and systems designed to meet the requirements of the Securities and Exchange Commission Rule 17a-4(f), as defined by 1) the No Action Letter in 1993 (allowing broker dealers to use non-rewriteable, non-erasable digital storage media); 2) the issuance of the Rule in 1997; and 3) the Interpretive Release in 2003, which authorizes the use of erasable storage, conditioned on integrated control codes, to prevent premature deletion of records.

NetBackup is a highly scalable, enterprise data management and protection platform. Designed to be vendor-agnostic, NetBackup is an archival solution that provides backup and recovery services to protect data and objects against catastrophic events such as unexpected business disruptions and security attacks. NetBackup *Compliance Mode Controls* are designed to meet securities industry requirements for preserving records in a non-rewriteable, non-erasable format.

In this Report, Cohasset Associates, Inc. (Cohasset) assesses the capabilities of NetBackup (see Section 1.3, *NetBackup Overview and Assessment Scope*) relative to the following regulations:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It is Cohasset's opinion that NetBackup, version 8.3.0.1, when properly configured, meets the five requirements related to the recording and the non-rewriteable, non-erasable storage of electronic records in SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the assessed capabilities of NetBackup meet the principles-based requirements of CFTC Rule 1.31(c)-(d).

12800 Whitewater Drive, Suite 100 | Minnetonka, MN 55343-9347 | USA | +1.312.527.1550 | www.cohasset.com September 2020

https://www.veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup

【参考】NetBackup Flex アプライアンス WORMストレージの安全性

NetBackup Flex アプライアンスでは、万が一、システムが起動不能になった場合でも、
バックアップデータを残したまま、アプライアンスを再インストールし、リストア可能です。

https://sort.veritas.com/doc_viewer/#/content?id=130821112-145890001-0%2Fv135697518-145890001

NetBackup管理者でも
WORM保持期間中はバックアップデータは**削除不可**

Image Expire Error

Backup ID	Copy Number	Error Message
kiji-media_1625015927	1	Expiration for Open Storage WORM cannot be shortened. (2530)

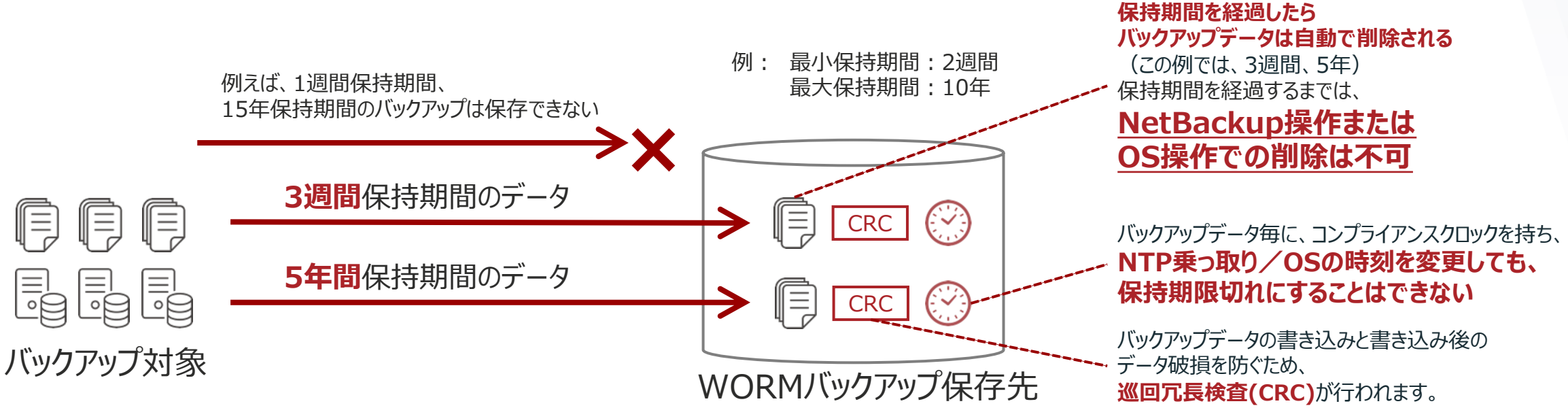
WORM内にバックアップデータがある状態では
WORMストレージインスタンスは**削除不可**

Messages

Sep 4 2021 18:43:01 Attempting to delete instance flexapp3.
Application name: NetBackup WORM Storage Server, version: 15.0
Sep 4 2021 18:43:07 Can't delete instance because locked backup images are present. You must wait for the retention period to end before you can delete this instance.
Sep 4 2021 18:43:07 Failed to delete instance flexapp3. Check /log/nodeworker/worker.log and VCS logs for more details.

WORM機能の動作概要

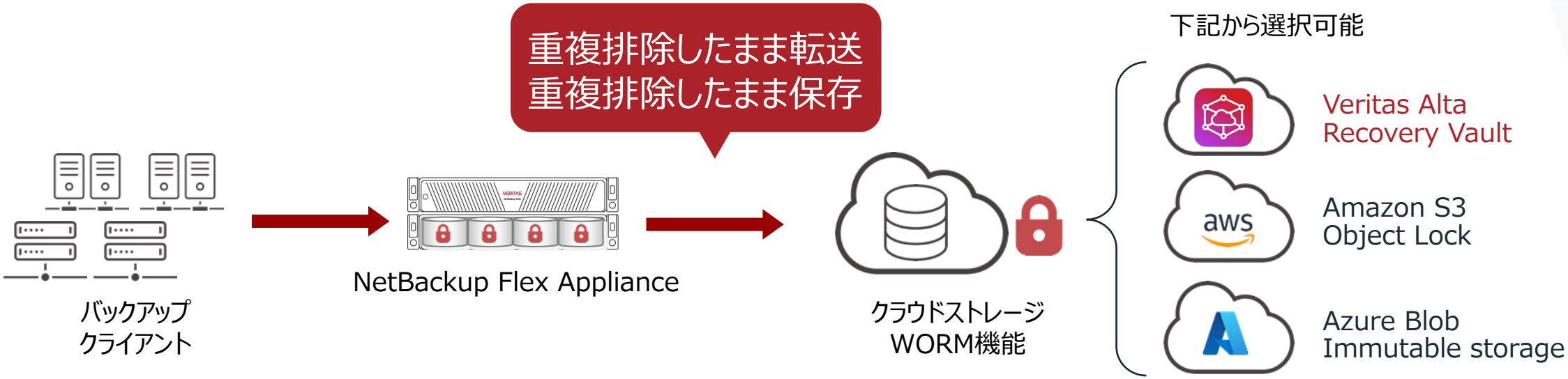
バックアップデータが永久に溜まり続けるわけではありません。
1つのWORMストレージに異なる保存期間のバックアップデータを管理できます



バックアップ保持期間中は、NetBackup管理者およびOSユーザから、
いかなる操作でも、バックアップデータを改ざん／削除することはできません。

クラウドストレージのWORM機能との連携

NetBackup Flex アプライアンスは、**クラウドストレージのWORM機能と連携可能**です。
コストをおさえたBCP対策とともに**ランサムウェア対策としての**3-2-**1**ルールの実現が可能です。



NetBackupユーザは、H/W、ライセンスの追加無く
クラウドストレージのWORM機能でランサムウェア対策を実現

Veritas Alta Recovery Vault

ベリタスが提供する クラウドストレージサービス

Veritas Alta Recovery Vault

※ 現在は、Azure Blob、Amazon S3 から
ベースのクラウドストレージを選択可能です。

シンプル運用

- NetBackup UIからの簡単操作

リストア費用の削減

- 重複排除後の使用容量にのみ課金
- サブスクリプションに契約容量20%のリストア費用を包含

ワンストップサポート

- NetBackupとクラウドストレージの一括サポート
- ストレージアカウントとアクセスキーを提供
- 契約／更新／ライセンス管理窓口一本化

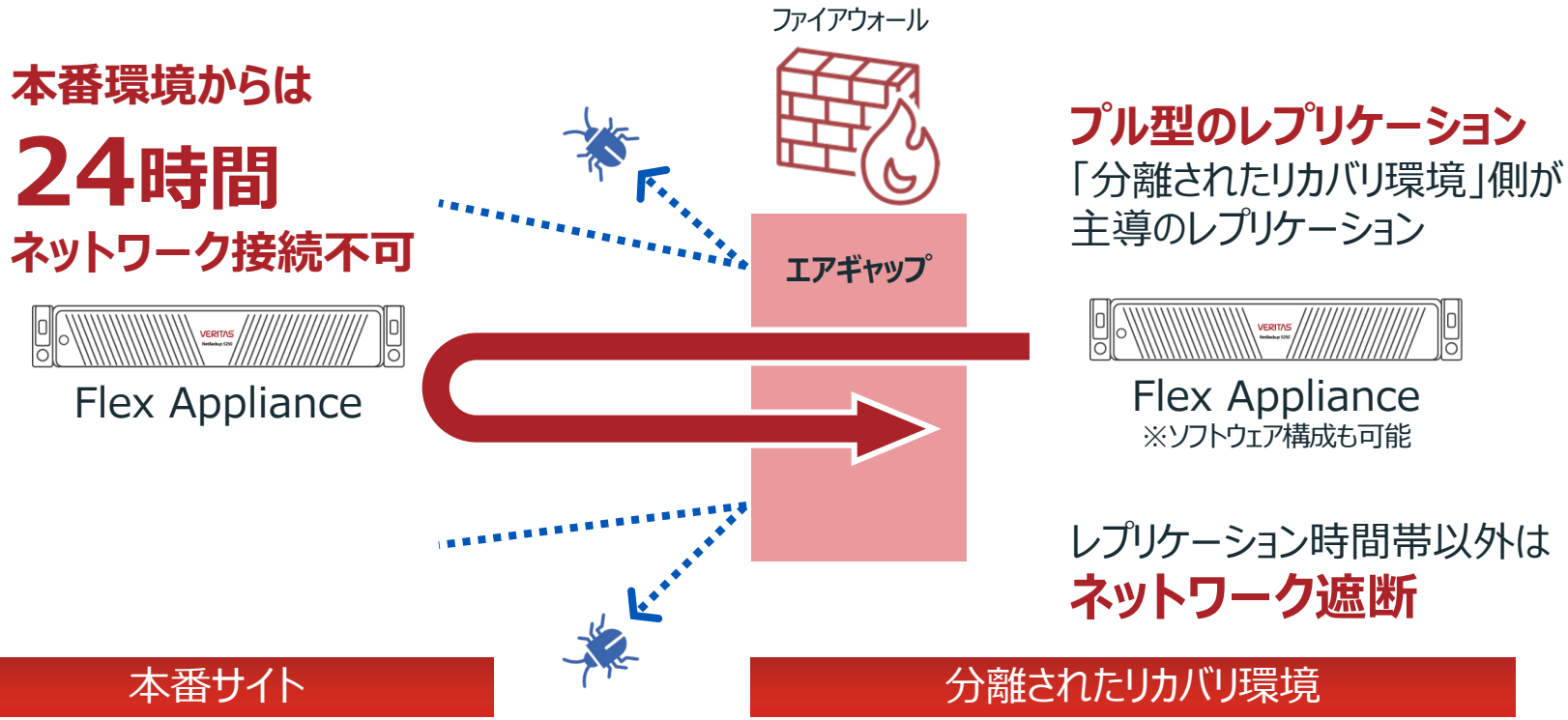
ランサムウェア対策

- WORMによるバックアップデータの改ざん／削除防止
- AWS、Azureの管理者でも削除不可

分離されたリカバリ環境（エアギャップ）でクリーンな復旧を担保

分離されたリカバリ環境は、本番環境とバックアップ複製データの間にエアギャップ（ネットワーク分離）を提供します。

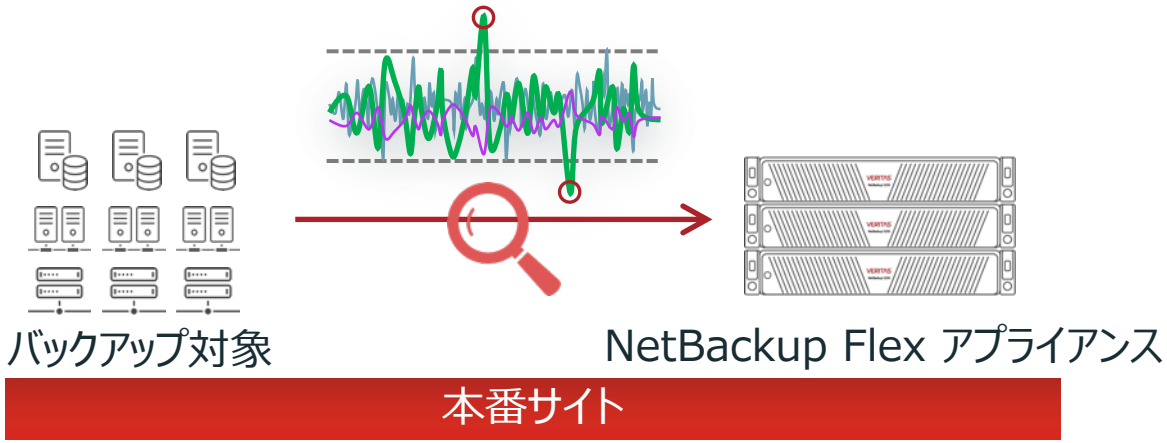
- **レプリケーション時以外のネットワーク遮断を実現**
- **プル型のレプリケーション＋ファイアウォールでレプリケーション中含む24時間の遮断が可能**



４．ランサムウェア被害検知・検出

ランサムウェア被害の可能性をふるまい検知（異常検知）

バックアップ取得時の統計情報をもとに、
本番サイトで、ほぼリアルタイムで、バックアップデータのふるまい検知できます。
AI／機械学習により、下記情報の異常な偏差（統計的なズレ）を検出します。



ふるまい検知にする統計情報

- ✓ バックアップデータのサイズ
- ✓ データ転送のサイズ
- ✓ バックアップファイルの数
- ✓ バックアップデータの重複排除率
- ✓ バックアップジョブの所要時間

攻撃の兆候	主なバックアップへの影響
ファイルの暗号化	バックアップ時の重複排除率が低下
ファイル名の変更	バックアップされるファイル数が増加
ファイルの削除	バックアップされるファイル数やサイズが減少
新しい拡張子の追加	バックアップされるファイル数やサイズが増加

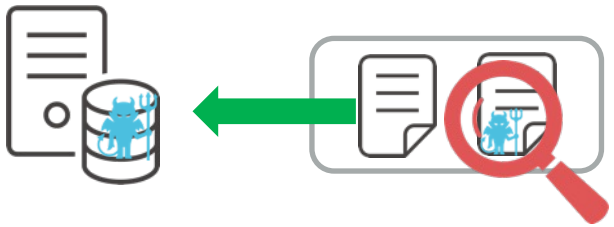
第三者視点のバックアップから被害の可能性を検知
あらゆるデータを保護できるNetBackupにより、
統合的なチェックが可能

ふるまい検知（異常検知）の必要性

- セキュリティーソフトのチェックをかいくぐるゼロデイ攻撃対策
  - 第三者視点のバックアップから被害の可能性を検知
- 感染直後の迅速な復旧を促す

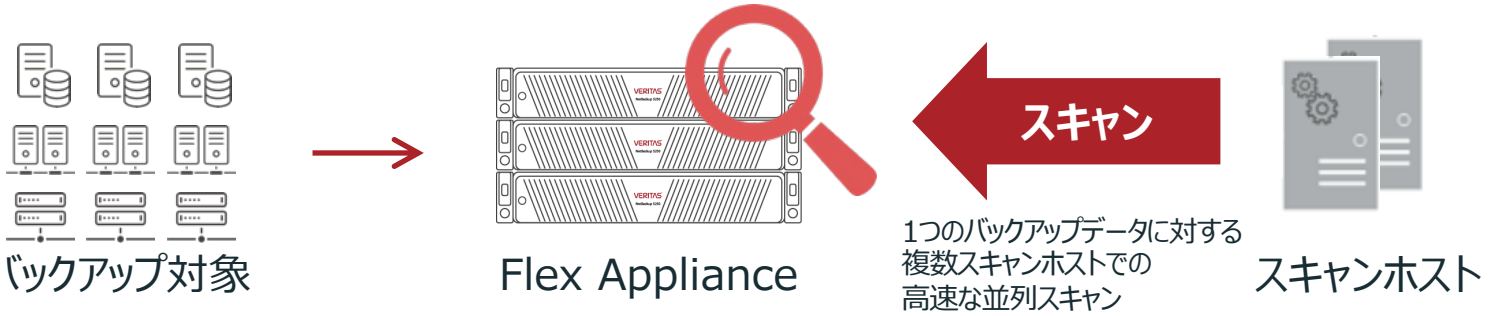
異常に気付かず、日数が経つと
- クリーンなバックアップが無くなってしまう
- 長期保存していても使い物にならない
  - 古い状態にしか復旧できない

データの異常を検知することで、
ランサムウェア被害前の最新状態に
復旧することができる



バックアップ保存データのマルウェア検出

本番サイトでのマルウェアスキャンにより、リストア前のバックアップデータの健全性の確認できます。
また、バックアップ保持世代数が、全てランサム被害で埋め尽くされてしまうリスクを低減します。
Flex アプライアンス以外に、スキャンホストのみ準備すればOK（シンプル構成）



対応マルウェアスキャナ
- ✓ **Microsoft Defender**
- ✓ **Symantec Protection Engine**
- ✓ **NetBackup Malware Scanner（Avira）**

本番サイト

マルウェア感染を検出した際の自動制御

- ✓ 感染したクライアントのバックアップデータ期限切れの一時停止
  → **正常なバックアップデータの期限切れを防止**
- ✓ 感染したクライアントのバックアップジョブの一時停止
- ✓ 感染したクライアントのバックアップ複製ジョブの一時停止
  → **感染バックアップデータの遠隔地複製を防止**

今後のロードマップ
- ✓ **スキャナーの追加：Crowd Strike、Cybereason、McAfee**
- ✓ Hosted マルウェアスキャンサービス
- ✓ 異常検出：ファイルベースの検出

NetBackup Malware Scanner のパターンファイル更新頻度

ID	XVDF バージョン	公開日	
67550	8.19.36.228	2023年3月20日月曜日	詳細
67549	8.19.36.226	2023年3月20日月曜日	詳細
67548	8.19.36.224	2023年3月20日月曜日	詳細
67547	8.19.36.222	2023年3月20日月曜日	詳細
67546	8.19.36.220	2023年3月19日日曜日	詳細
67545	8.19.36.218	2023年3月19日日曜日	詳細
67544	8.19.36.216	2023年3月19日日曜日	詳細
67543	8.19.36.214	2023年3月19日日曜日	詳細
67542	8.19.36.212	2023年3月19日日曜日	詳細
67541	8.19.36.208	2023年3月19日日曜日	詳細
67540	8.19.36.206	2023年3月18日土曜日	詳細
67539	8.19.36.204	2023年3月18日土曜日	詳細
67538	8.19.36.202	2023年3月18日土曜日	詳細
67537	8.19.36.200	2023年3月18日土曜日	詳細
67536	8.19.36.198	2023年3月18日土曜日	詳細
67535	8.19.36.196	2023年3月18日土曜日	詳細
67534	8.19.36.194	2023年3月18日土曜日	詳細
67533	8.19.36.192	2023年3月18日土曜日	詳細

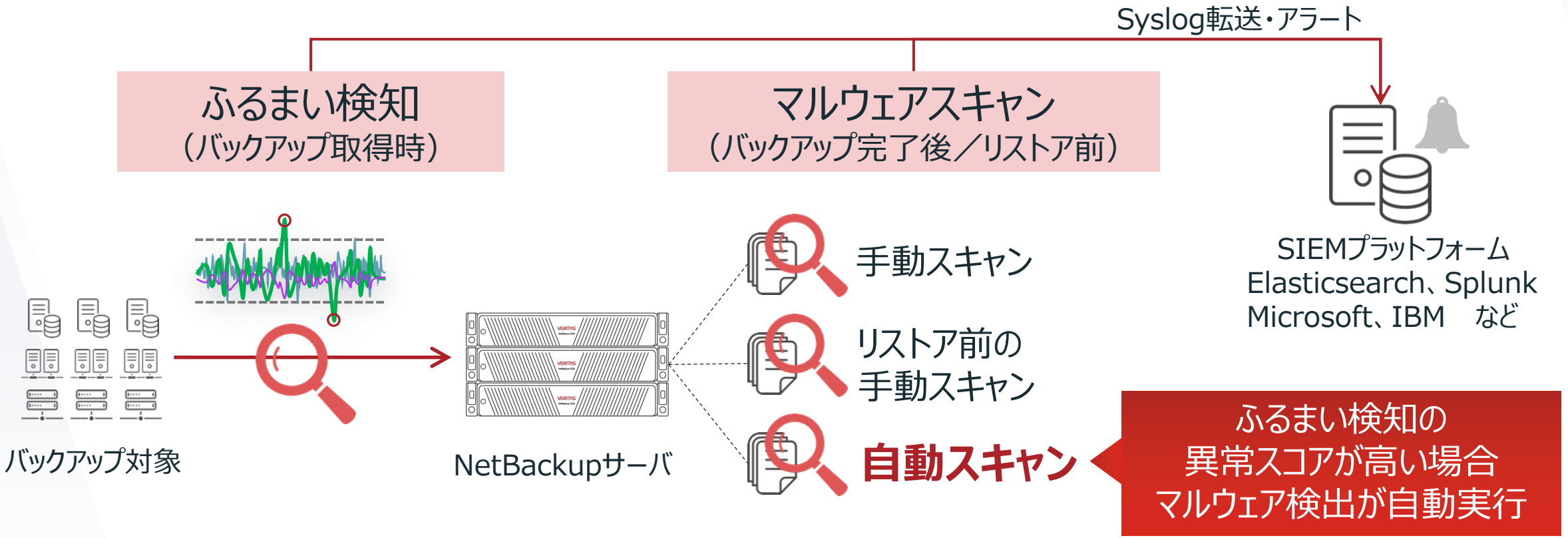
https://www.avira.com/ja/support-vdf-history

NetBackup Malware Scannerは、
Aviraセキュリティをベースとしており、
保守サポートはベリタス社が提供します。

Aviraセキュリティで最新の脅威の検知を継続できるよう、
Aviraでは**毎日数回VDFファイルの更新**を行います。

ふるまい検知 と マルウェアスキャン の自動連動

ふるまい検知で異常を検知した場合、マルウェアスキャンが自動実行されます。
ふるまい検知、マルウェア検出で脅威を検知した際は、Syslog転送やアラート通知が可能です。



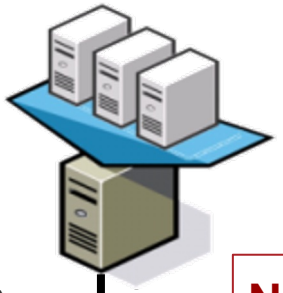
5．RPO/RTOに応じた迅速・柔軟なリカバリ

仮想マシンの短時間直接復旧

IO性能はいらないが、即時復旧が必要なシステム向け

NetBackupメディアサーバをNFSデータストアしてマウントし、**仮想マシンを即時起動**

② バックアップストレージの
VMDKファイルから
仮想マシンを起動します



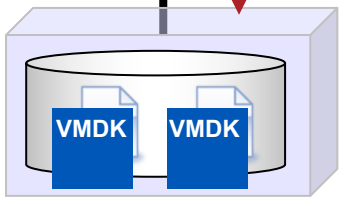
ESXサーバ

① バックアップサーバが
NFSデータストアして
マウントされる

NFSマウント

※RHELまたはFlex アプライアンスのメディアサーバが必要

③ バックアップストレージから
プライマリストレージへオンラインで
仮想マシンを移行できます
（**Online Storage vMotion**）



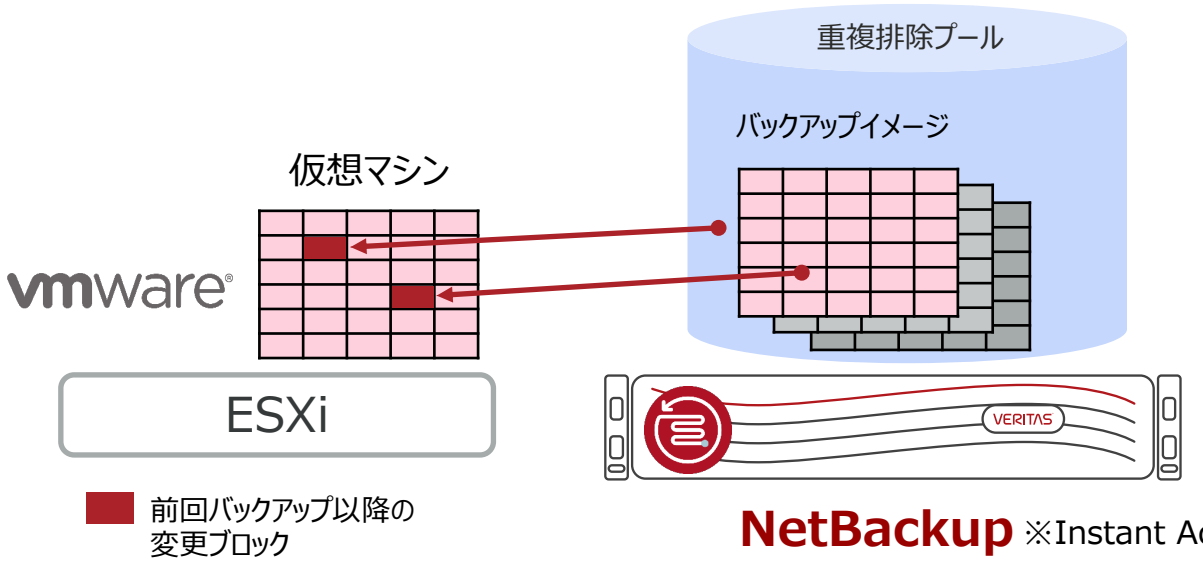
本番データストア

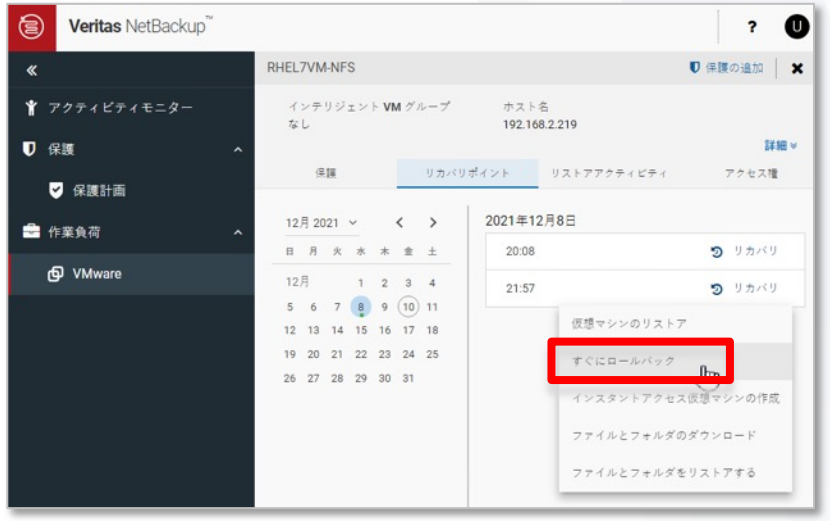
- バックアップ済みの仮想マシンイメージから直接を立ち上げ
- 同時立ち上げ最大50VM
- WebUIから簡単復旧
- 特定のユーザに特定のVM立ち上げ権限を委譲可能

既存環境に影響を与えず、新たな環境として仮想マシンを起動!!

仮想マシンの短時間差分リストア

本番のIO性能で短時間に復旧させたいシステム向け





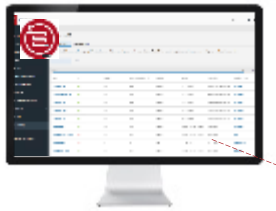
NetBackup ※Instant Access機能が動作する環境

- 本番ストレージへの仮想マシンのリカバリ時間短縮の選択肢
- VMwareのCBT(トラックログ)と連携、更新ブロックの差分のみをリストアすることでリカバリ時間を短縮
- ランサムウェアやその他のイベントからの回復 時間を数分に短縮
- 複数のVMを一括操作で復旧可能
- 特定のユーザに特定のVM復旧権限を委譲可能

オンプレミスの仮想マシンをクラウドで復旧

他拠点サイト

ブラウザの操作から簡単なステップでAzure/AWSへのリカバリが実現可能



本番拠点サイト

クライアント

VM VM VM

ESXi

バックアップ

NetBackupサーバ

重複排除

LSU

MSDPクラウド構成

重複排除複製

- 災害やランサムウェア被害発生後、別のクリアな環境で復旧させたい場合

クラウド

リストア専用
NetBackupサーバー

VM

カタログ
インポート

Read Only

VHD/AMI変換

復旧

クラウドストレージ
- Azure Blob
- Amazon S3

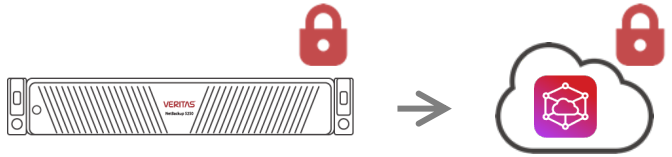
クラウド・インスタンス
- Azure VM
- AWS EC2

Agenda

- 背景と課題
- 課題解決のための要件とベリタスのソリューション
- 実現イメージ
- お客様のメリット
- まとめ

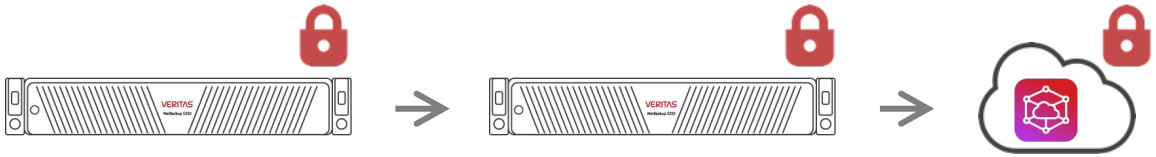
ベストプラクティス構成

1



NetBackup Flex アプライアンス　+ Veritas Alta Recovery Vault

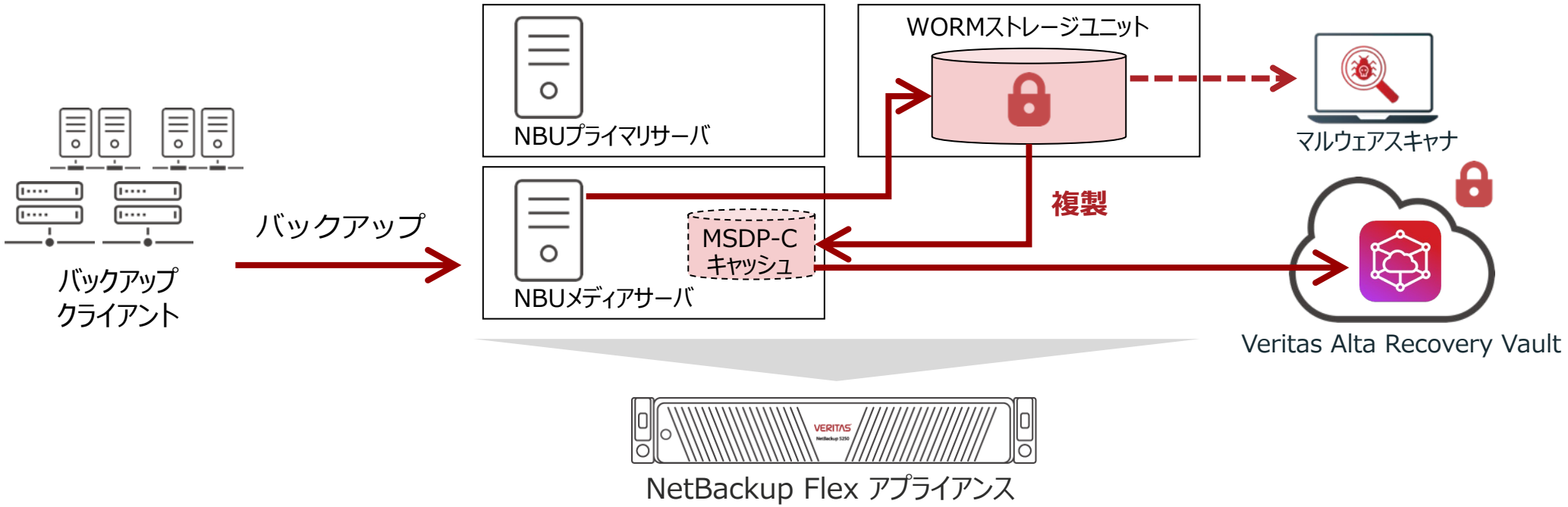
2



NetBackup Flex アプライアンス レプリケーション構成 + Veritas Alta Recovery Vault

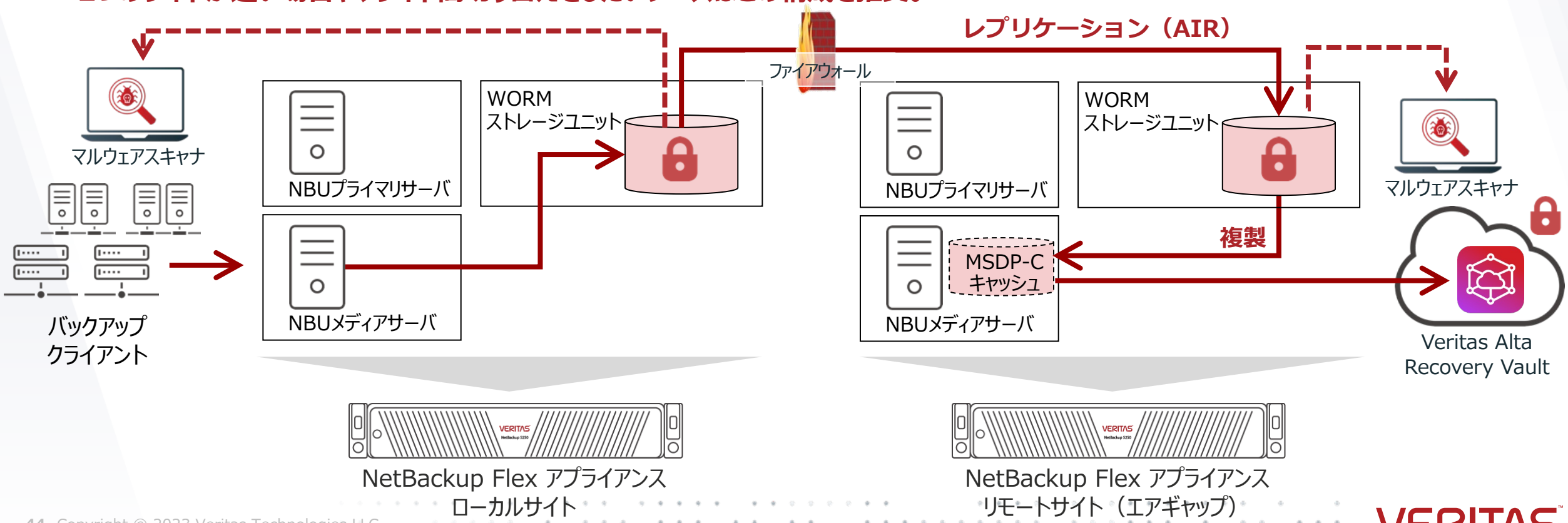
構成例①　NetBackup Flex アプライアンス + Veritas Alta Recovery Vault

バックアップデータをWORMストレージユニットに、Accelerator機能で永久増分バックアップします。
その後、MSDP-Cloud機能により、Veritas Alta Recovery Vaultに重複排除したまま複製します。
必要に応じてマルウェアスキャンを実施します



構成例②　NetBackup Flex アプライアンス レプリケーション構成 + Veritas Alta Recovery Vault

バックアップデータをWORMストレージユニットに、Accelerator機能で永久増分バックアップします。
その後、AIR機能でリモートサイト（エアギャップ）にレプリケーションします。
リモートサイトにて、MSDP-Cloud機能により、Veritas Alta Recovery Vaultに複製します。
必要に応じてマルウェアスキャンを実施します
2つのサイトが近い場合や、サイト間切り替えをしたいケースはこの構成を推奨。



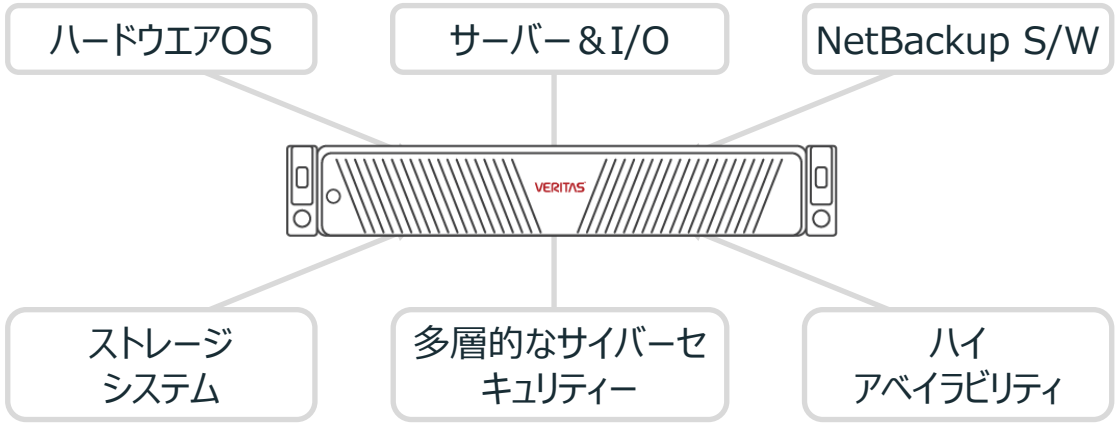
Agenda

- 背景と課題
- 課題解決のための要件とベリタスのソリューション
- 実現イメージ
- お客様のメリット
- まとめ

設計・導入・運用コストと導入時間を削減

NetBackup Flex アプライアンス

必要コンポーネントを全て搭載、最適化、テスト済み
NetBackup Flex アプライアンス

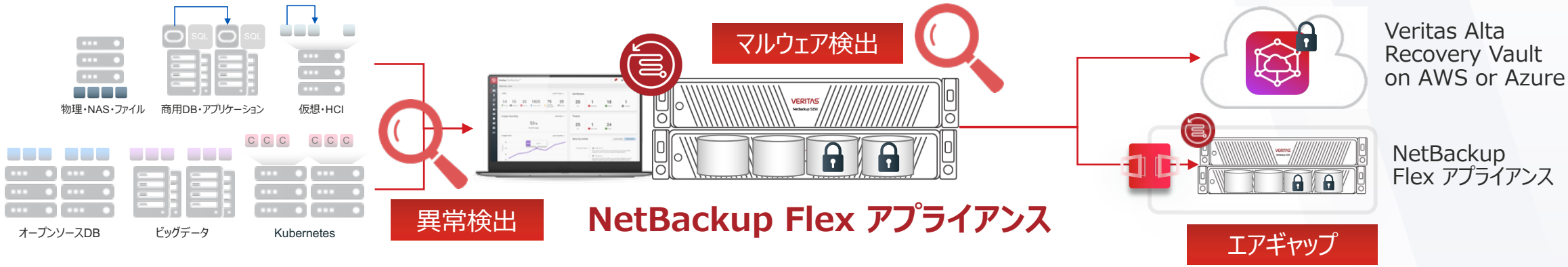


迅速な「ラック＆ロール」配備

納品後すぐに利用可能なバックアップ専用アプライアンス

ランサムウェア攻撃に対する万全な保護・復旧をシンプルに実現

統合的、確実に保護し、クリーンなデータ回復を実現



1 IT環境全体の確実な保護

- ✓ 多くのワークロードに対応
- ✓ バックアップ対象を検出しもれなくバックアップ
- ✓ 高速なバックアップ
- ✓ シンプルな統合管理・構成

2 不正侵入防止策

- ✓ セキュアな専用OS[*1]
- ✓ 不正侵入検知・防止機能
- ✓ 限定されたプロセス・通信
- ✓ 多要素認証
- ✓ 定期的なシステムの脆弱性評価と対処

3 バックアップデータの改ざん・消去防止策

- ✓ 管理者ですら改ざん不可なFlex Appliance内改ざん防止ストレージ
- ✓ クラウドストレージやオブジェクトストレージとのWOR連携制御
- ✓ 機能遠隔地への複製、エアギャップ保管

4 ランサムウェア被害検知・検出

- ✓ AIベースでバックアップ時にデータの異常を検知
- ✓ バックアップデータ上のマルウェアを検出

5 RPO/RTOに応じた迅速・柔軟なリカバリ

- ✓ 高速な回復
- ✓ 柔軟な回復オプション
- ✓ 統合化されたクラウド上へのリカバリ

30年以上の実績を誇る信頼のNetBackupで安心

Gartner
17x
LEADER

Gartner Magic Quadrant™ Leader
エンタープライズ向けバックアップ&リカバリーソフトウェアソリューション

ベリタスを使用している
Fortune 100 企業の割合

Gartner
15x
LEADER

Gartner Magic Quadrant™ Leader
エンタープライズインフォメーションアーカイブ

6,000+
グローバルの従業員

20,000+
グローバルパートナー

80,000+
グローバルの顧客

2,000+
グローバルの開発者

2,200+
グローバル特許数

800+
対応するワークロード

100+ EB
ベリタス製品によって管理されるデータ

VERITAS

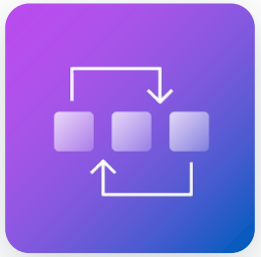
まとめ

1

ランサムウェア攻撃に対する備えは喫緊の課題

もはや、「もし」ではなく「いつ？」の問題

2



統合的、確実に保護し、クリーンなデータ回復を実現するデータ保護が必要

バックアップシステムに必要なランサムウェア対策は多く、実装が大変

3

NetBackup Flex アプライアンスなら万全なランサムウェア対策をシンプルに実現

- IT環境全体の確実な保護
- 不正侵入防止策
- バックアップデータの改ざん・消去防止策
- ランサムウェア被害の検知・検出
- RPO/RTOに応じた迅速・柔軟なリカバリ