Veritas Vibe Webinar

VERITAS

株式会社mizkan様向けの事例から学ぶ

すぐに導入できる
サイバーレジリエンスソリューション

工藤　陽平

ベリタステクノロジーズ合同会社

Veritas Vibe Webinar へようこそ！

本日のセッションは
ライブセッション

ご質問はQ&A
ボックスにいつでもOK

資料は後日公開

VERITAS

注意

製品の計画に関する将来的な記述は、仮のものです。
将来のリリース日は、確定したものではなく、変更されることがあります。

今後の製品のリリースや予定されている機能修正について、
ベリタスは継続的な評価を行っており、実装されるかどうかは確定していません。
したがって、購入の意思決定の判断材料にすべきではありません。

本書に記載されている情報は、予告なく変更されることがあります。

Agenda

- ランサムウェア攻撃の現状
- 課題解決のための要件とベリタスのソリューション
- ベストプラクティス
- 株式会社mizkan様の事例をご紹介
- まとめ

VERITAS

Agenda

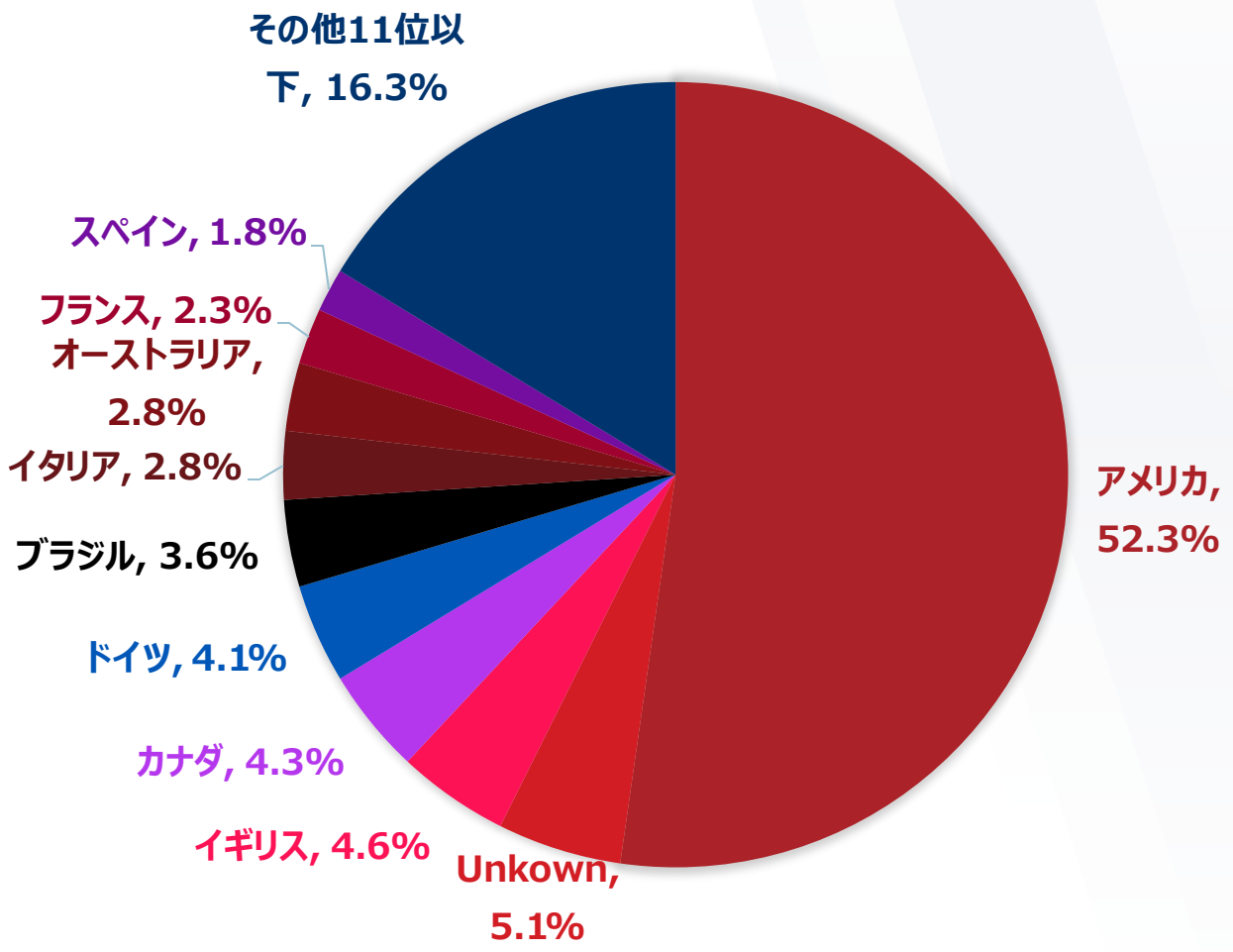
- ランサムウェア攻撃の現状
- 課題解決のための要件とベリタスのソリューション
- ベストプラクティス
- 株式会社mizkan様の事例をご紹介
- まとめ

VERITAS

2024年4月も引き続きランサムウェア攻撃が行われている

国名	件数	割合	前月比
アメリカ	205	52.3%	+12
Unkown	20	5.1%	+9
イギリス	18	4.6%	-5
カナダ	17	4.3%	-10
ドイツ	16	4.1%	-7
ブラジル	14	3.6%	+8
イタリア	11	2.8%	+3
オーストラリア	11	2.8%	-7
フランス	9	2.3%	+8
スペイン	7	1.8%	-1

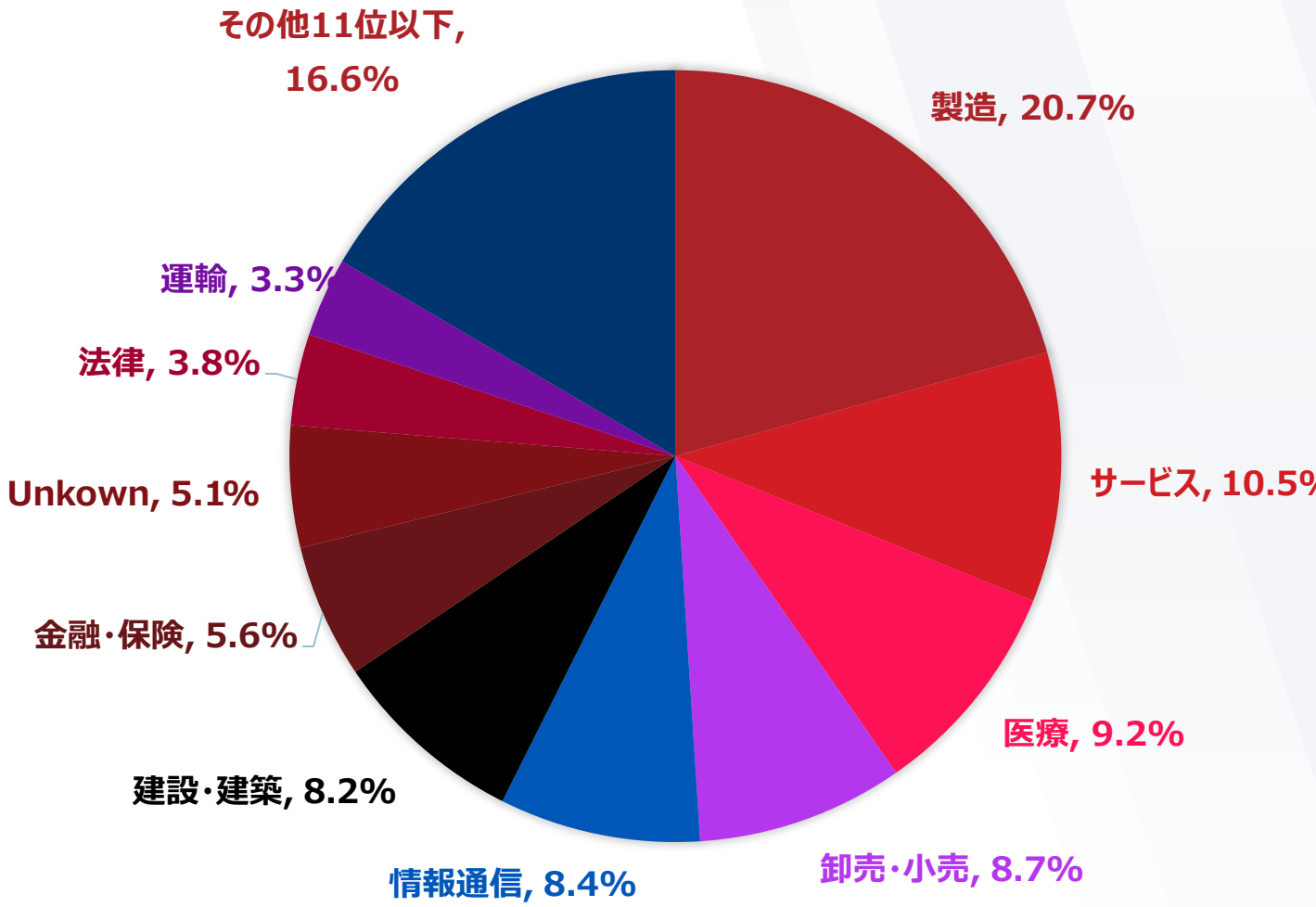
Source: MBSD Cyber Intelligence Group (CIG)



業種別では製造業がトップ

国名	件数	割合	前月比
製造	81	20.7%	+4
サービス	41	10.5%	+1
医療	36	9.2%	-1
卸売・小売	34	8.7%	-1
情報通信	33	8.4%	-5
建設・建築	32	8.2%	-7
金融・保険	22	5.6%	+3
Unkown	20	5.1%	+6
法律	15	3.8%	+2
運輸	13	3.3%	-1

Source: MBSD Cyber Intelligence Group (CIG)



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2024*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	サプライチェーンの弱点を悪用した攻撃	2
3	内部不正による情報漏洩	4
4	標的型攻撃による機密情報の窃取	3
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6
6	不注意による情報漏えい等の被害	9
7	脆弱性対策情報の公開に伴う悪用増加	8

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

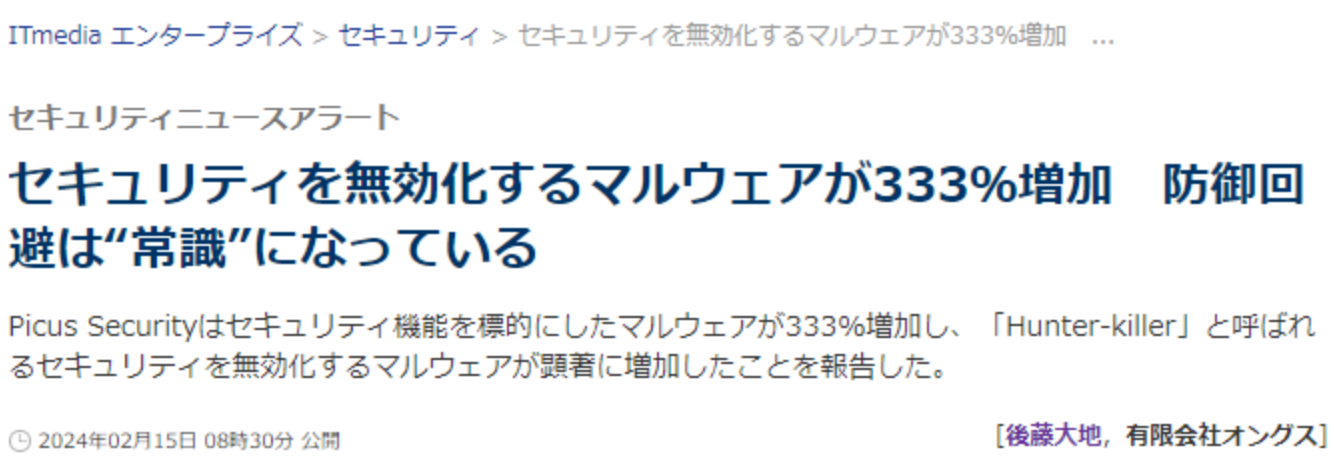
特定 → 防御 → 検知 → 対応 → **復旧**

- 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 2024」
URL https://www.ipa.go.jp/security/10threats/10threats2024.html

セキュリティを無効化するマルウェアが増加中



ITmedia エンタープライズ > セキュリティ > セキュリティを無効化するマルウェアが333%増加 ...

セキュリティニュースアラート

セキュリティを無効化するマルウェアが333%増加　防御回避は“常識”になっている

Picus Securityはセキュリティ機能を標的にしたマルウェアが333%増加し、「Hunter-killer」と呼ばれるセキュリティを無効化するマルウェアが顕著に増加したことを報告した。

2024年02月15日 08時30分 公開　　[後藤大地，有限会社オングス]

また、Picus Securityは「セキュリティツールが期待通りに機能しているように見える可能性があるため、サイバー攻撃によってセキュリティツールが無効化または再構成されたかどうかを検出するのは非常に難しい」とし、多層防御のアプローチで複数のセキュリティ制御を使用する必要があると指摘した。

IT Media エンタープライズの記事一覧より抜粋

セキュリティツールでの対策だけではなく、

大切なデータを守り切ることができる

「セキュアなOS」と、
「改ざん防止のWORM」を備えた、、、

バックアップシステムを、導入することが必須となります！！！

ランサムウェア攻撃とその背景

近年は下記の要因でランサムウェア攻撃が流行っています

攻撃が容易

- ✓ RaaS
- ✓ 人員が集めやすい
- ✓ 労力がかからない

儲かるビジネスモデル

- ✓ 初期投資が少ない
- ✓ 身代金をもらいやすい

脆弱性対応の遅れ・不足

- ✓ リモートワークによる機器整備で脆弱性対策が追い付いていない
- ✓ システムの複雑化
- ✓ ITスタッフのスキル・リソース不足

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

- ランサムウェア攻撃の現状
- 課題解決のための要件とベリタスのソリューション
- ベストプラクティス
- 株式会社mizkan様の事例をご紹介
- 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

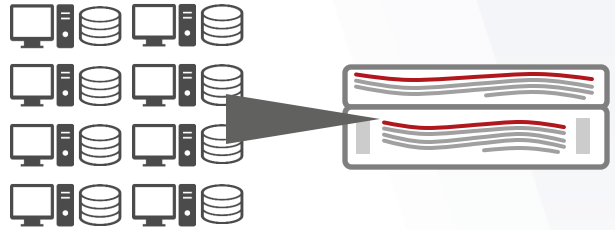
保護対象の幅広い対応

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

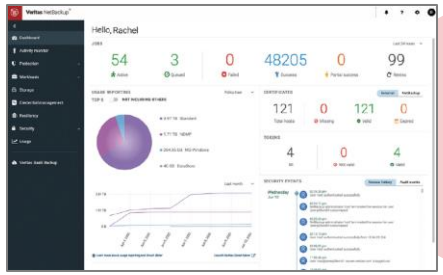
保護対象の幅広い対応

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

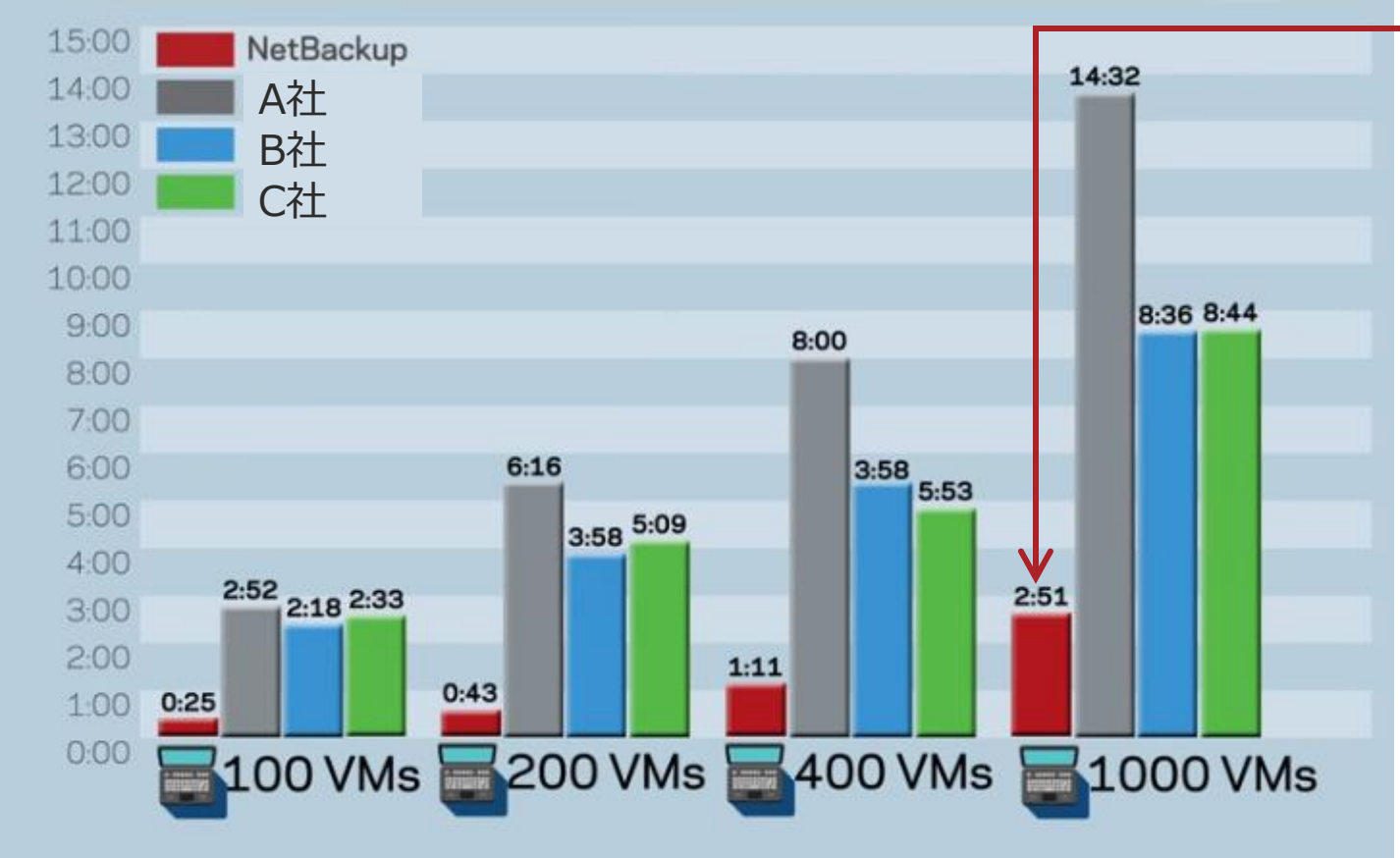
クラウドストレージ オブジェクトストレージ 60+

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

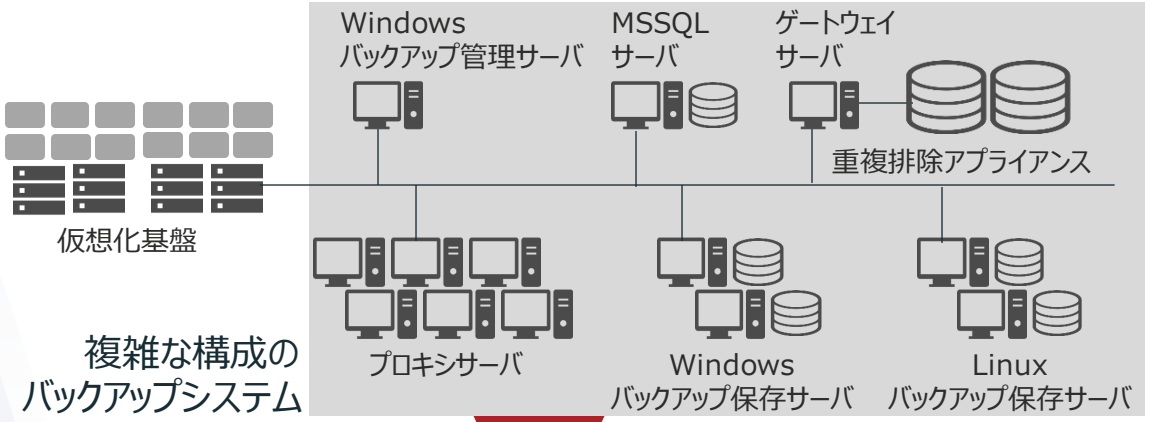
NetBackup Flex アプライアンス

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

パフォーマンス向上ために、複数台のバックアップサーバ、
プロキシサーバ、重複排除ストレージが必要



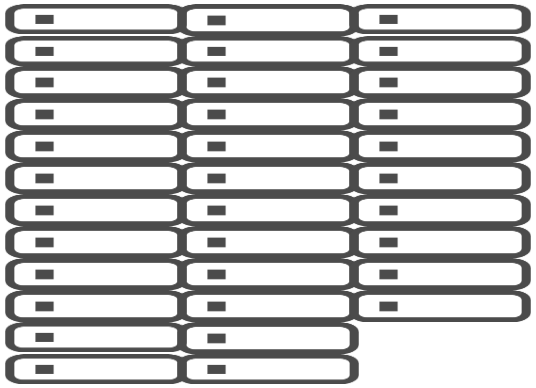
複雑な構成の
バックアップシステム

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

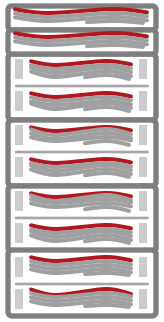
アプライアンスBとの比較（2PB）



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

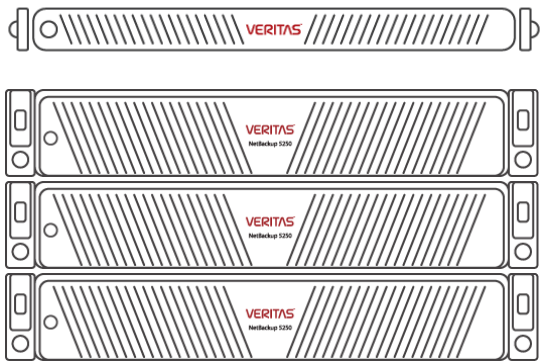
セキュアなバックアップ専用アプライアンス

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



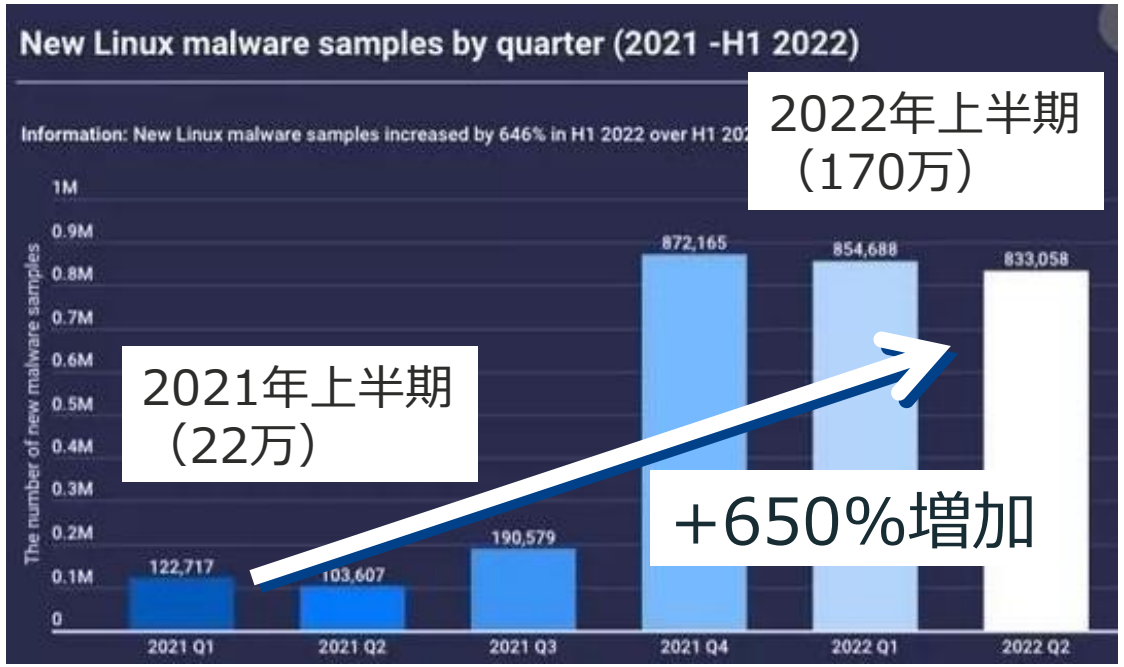
製品/パッチリリース時に
脆弱性チェックなどを実施

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

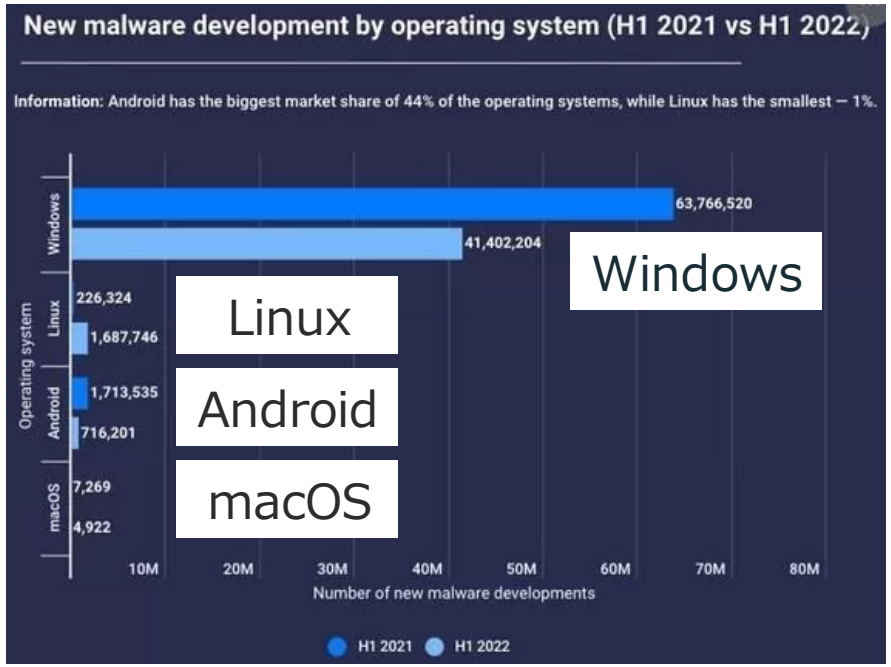
汎用OSが狙われています

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/

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

NetBackup Flex Applianceは導入済み！

ファームウェアのセキュリティ

- ✓ シングルユーザモード、レスキューモード禁止
- ✓ カスタムISO Boot禁止
- ✓ GRUB編集禁止

セキュリティ強化された専用OS

- ✓ SELinux強化済み（STIG準拠）
- ✓ rootアクセス不可
- ✓ セキュアAPI
- ✓ 不正プロセス実行防止
- ✓ NetBackupが発行した証明書以外の通信を防止

コンテナサービスの分離

- ✓ 非共有コンテナ名前空間
- ✓ ネットワーク遮断
- ✓ 限定された権限で実行されるサービス

改ざん・削除防止WORMストレージ

- ✓ WORM/イミュータブル（SEC/FINRA/CFTC準拠）
- ✓ 時刻変更に依存しないコンプライアンスクロック
- ✓ 暗号化（FIPS140-2準拠）
- ✓ プル型のエアギャップ

アプリケーションセキュリティ

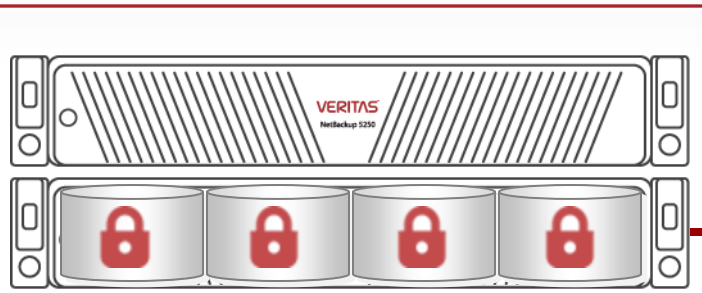
- ✓ マルウェアスキャン
- ✓ ふるまい検出
- ✓ 非rootサービス権限
- ✓ シングルサインオン
- ✓ 複数要素認証
- ✓ 役割ベースアクセス制御
- ✓ 監査・通知・レポート

※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

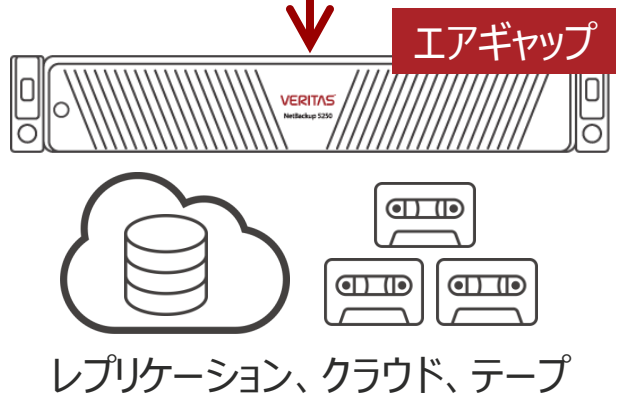
- AES 256-bit
- FIPS 140-2
- 2048 bitキー
- TLS 1.2証明書

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

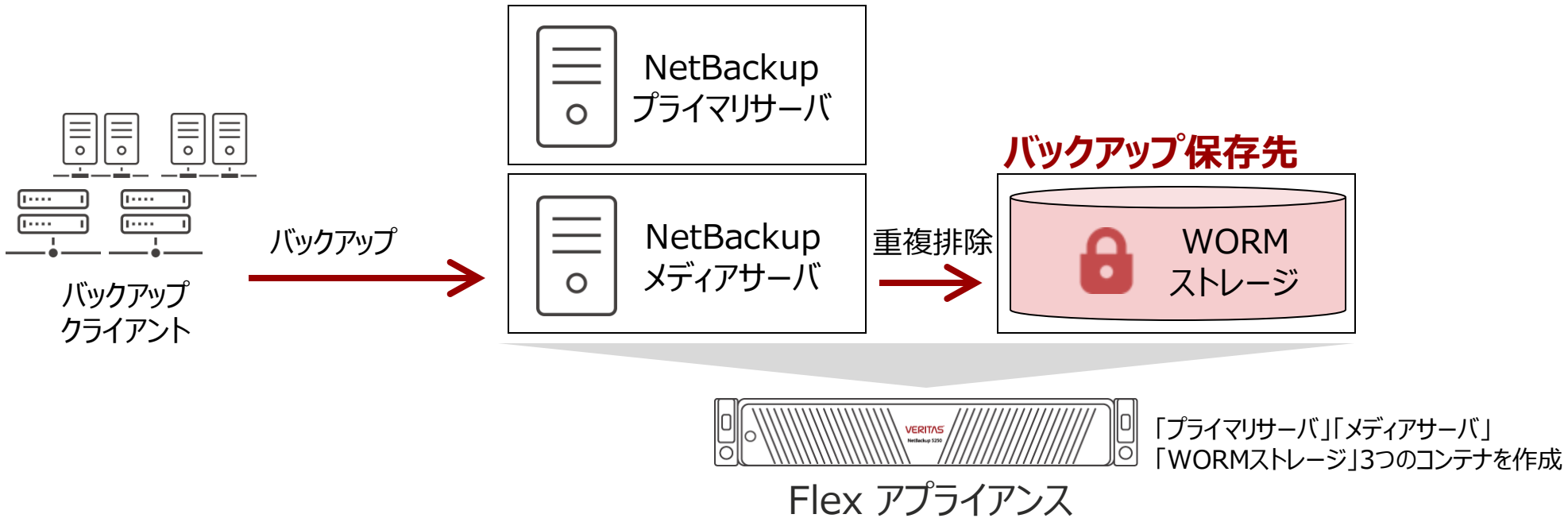
遠隔地への複製



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。



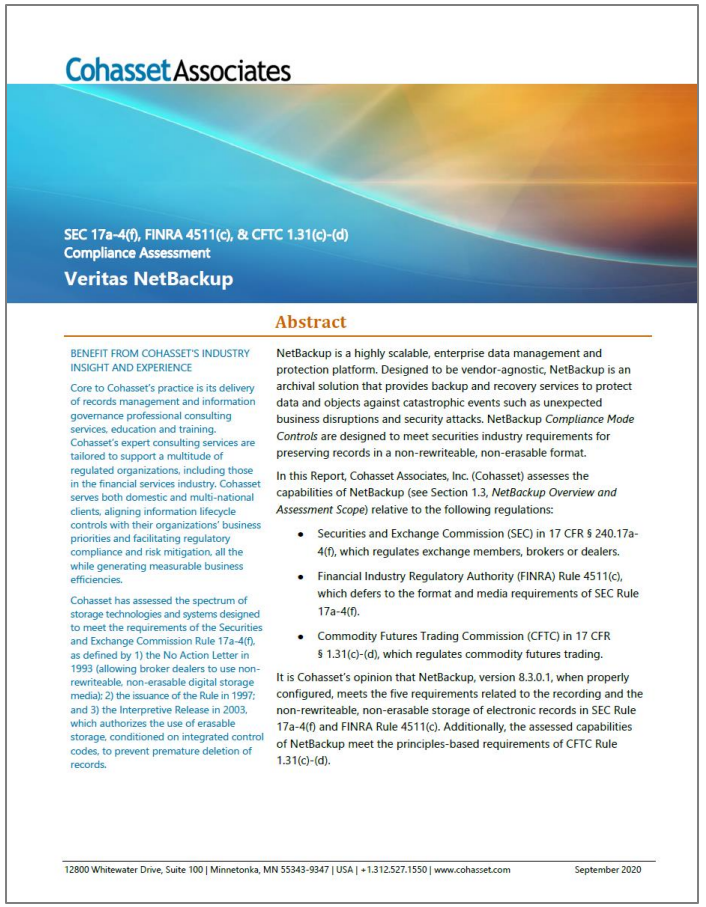
Flex Appliance 1台上に、バックアップサーバとWORMストレージを構成可能

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.

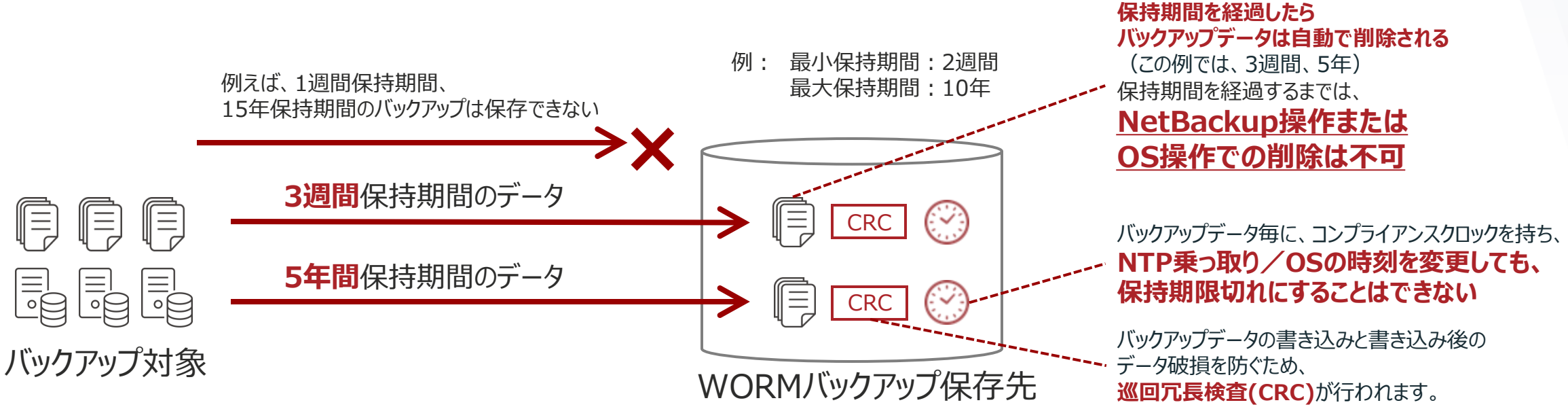
It is Cohasset's opinion that NetBackup, version 8.3.0.1, when properly configured, meets the five requirements related to the recording and the non-rewriteable, non-erasable storage of electronic records in SEC Rule 17a-4(f) and FINRA Rule 4511(c). Additionally, the assessed capabilities of NetBackup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

WORM機能の動作概要

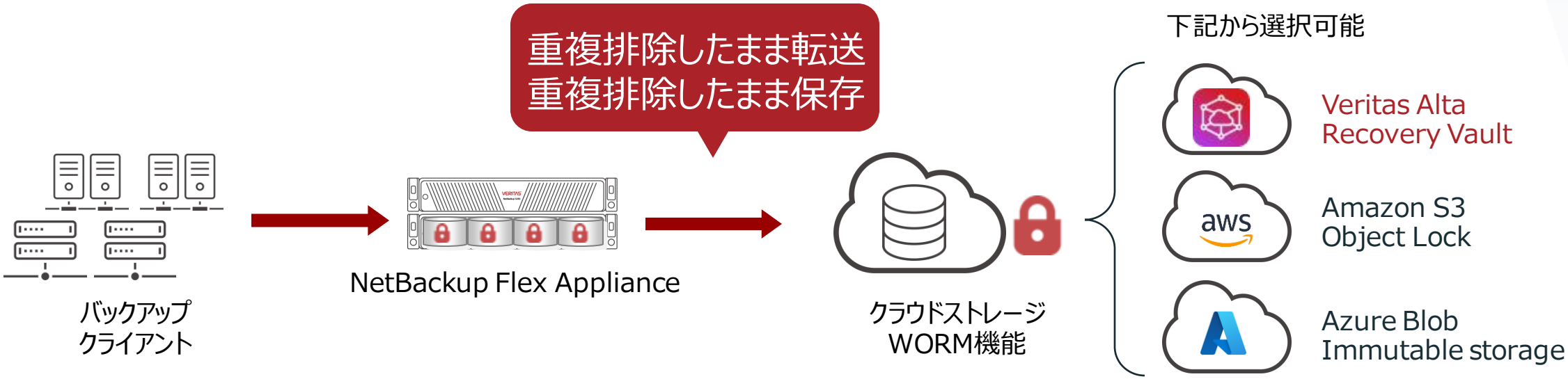
バックアップデータが永久に溜まり続けるわけではありません。
1つのWORMストレージに異なる保存期間のバックアップデータを管理できます



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

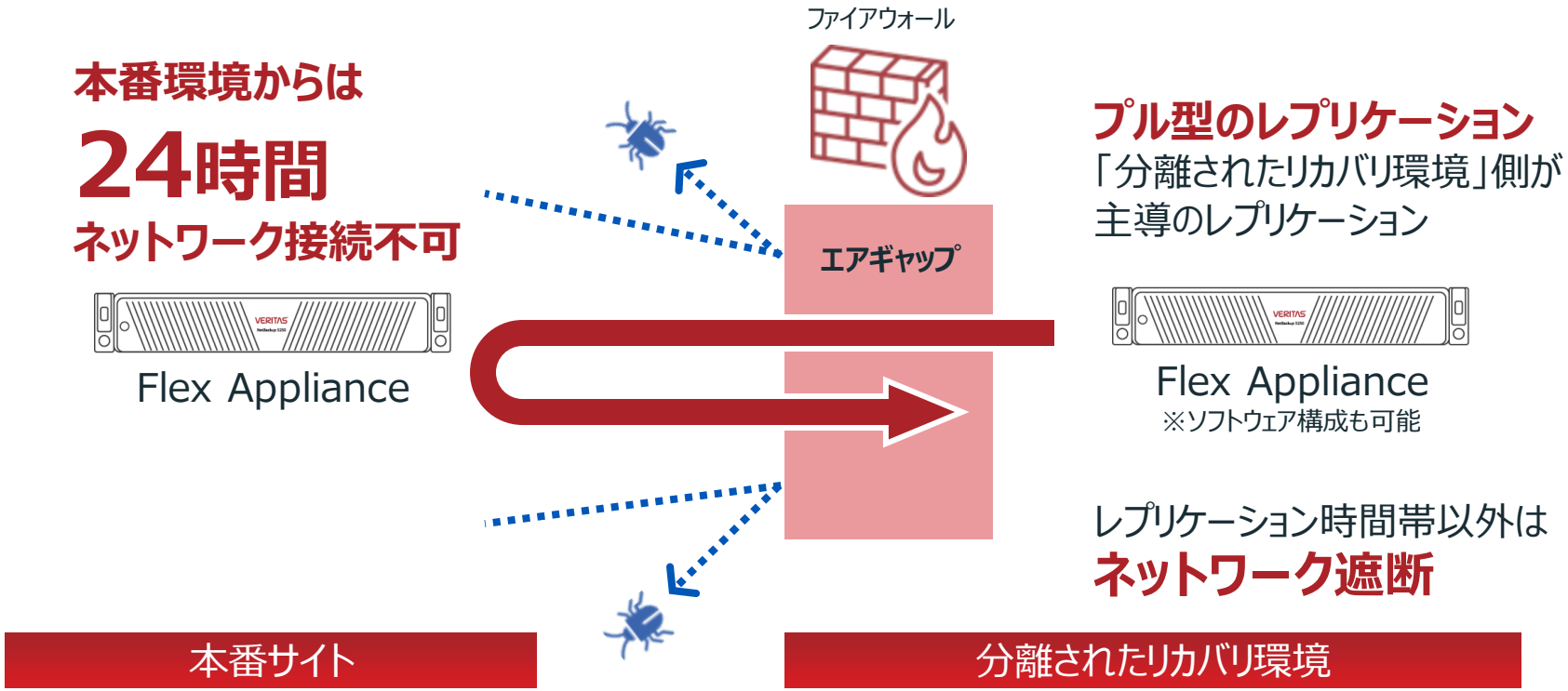
- NetBackupとクラウドストレージの一括サポート
- ストレージアカウントとアクセスキーを提供
- 契約／更新／ライセンス管理窓口一本化

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

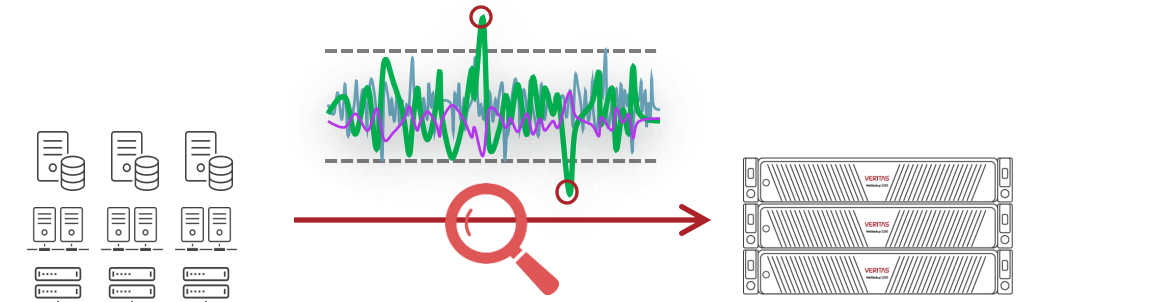
エアギャップとは、ネットワーク遮断機能です。
本番サイトから災対サイトへアクセス不可という状況を実現することが可能です。



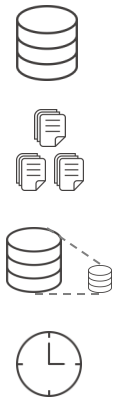
４．ランサムウェア被害検知・検出

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。



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



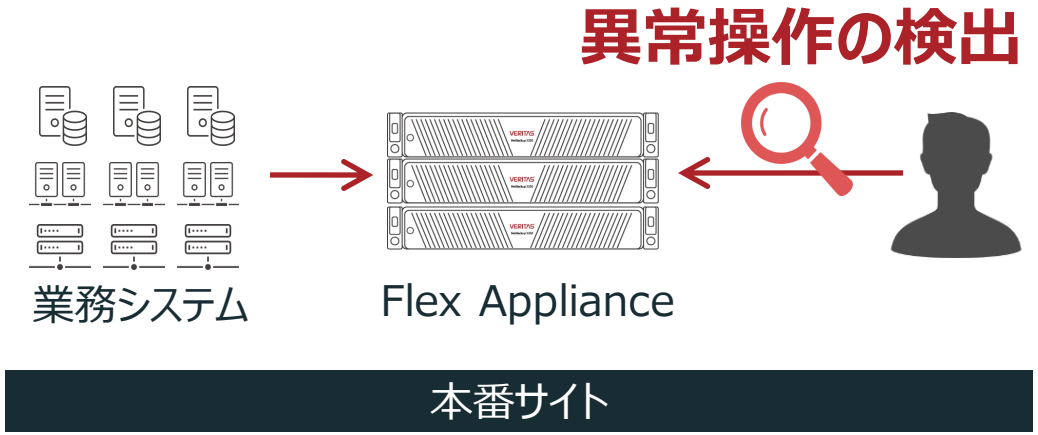
ふるまい検知にする統計情報

- ✓ 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
- ✓ ランサムウェア対策ファイルの拡張子

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

異常検出 - バックアップシステムの異常操作の検出

バックアップデータ喪失につながる危険な操作を異常操作として検出することができます。



右記以外の操作についても、監査ログとして記録され、
syslog転送で、SIEMサーバと連携可能です。

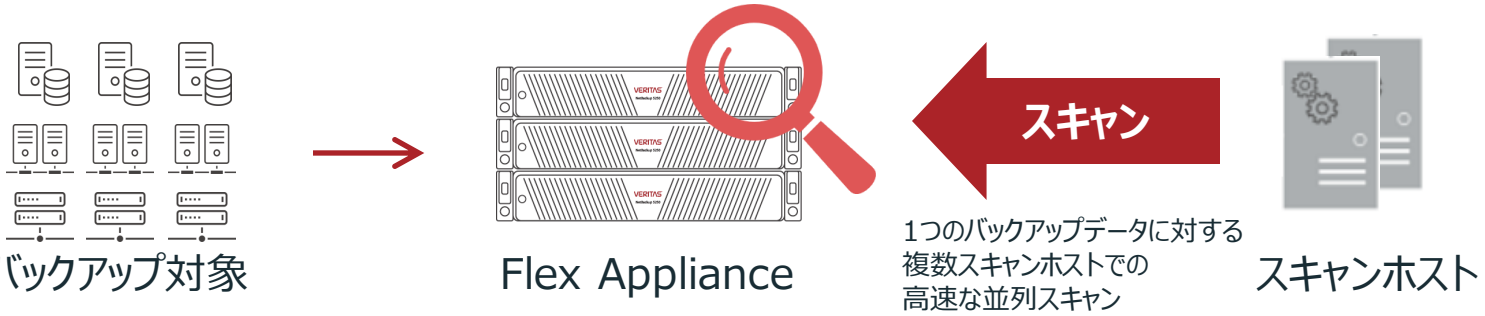
検出対象の危険な操作（異常検出ルール）

- ✓ バックアップデータの削除
- ✓ バックアップジョブ設定の変更
  - ✓ バックアップ対象クライアントの除外
  - ✓ バックアップ対象ファイルの除外
- ✓ バックアップジョブの削除、無効化
- ✓ トークンの再作成
- ✓ バックアップストレージ設定の削除
- ✓ バックアップ複製設定の変更、削除、無効化

など

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）



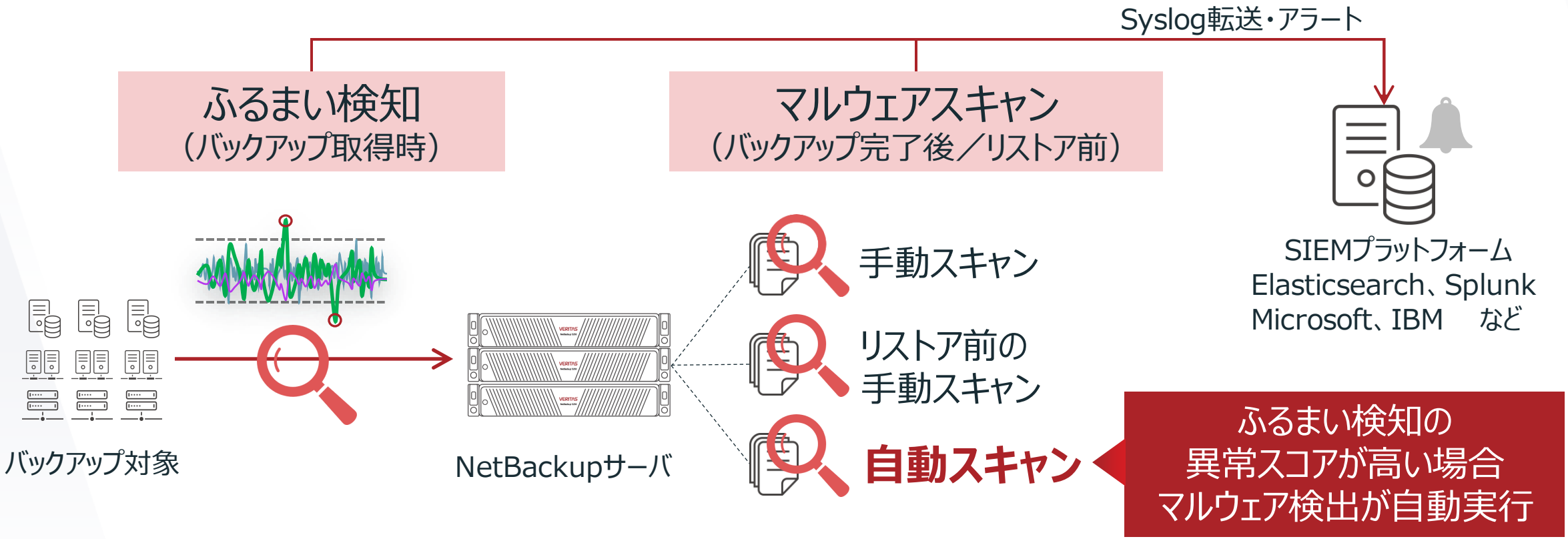
対応マルウェアスキャナ
- ✓ **Microsoft Defender**
- ✓ **Symantec Protection Engine**
- ✓ **NetBackup Malware Scanner（Avira）**

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**

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

リストア時の2次感染を防ぐ、安心・安全なリストア

NetBackupには、リストア時の2次感染を防ぐ、安心・安全なリストア機能を備えています。
リストア時にマルウェアを含むデータのリストアを防止する機能がデフォルトで有効です。

① リストア前のマルウェアスキャン

② リストアデータの選択時にスキャン状況を確認できる

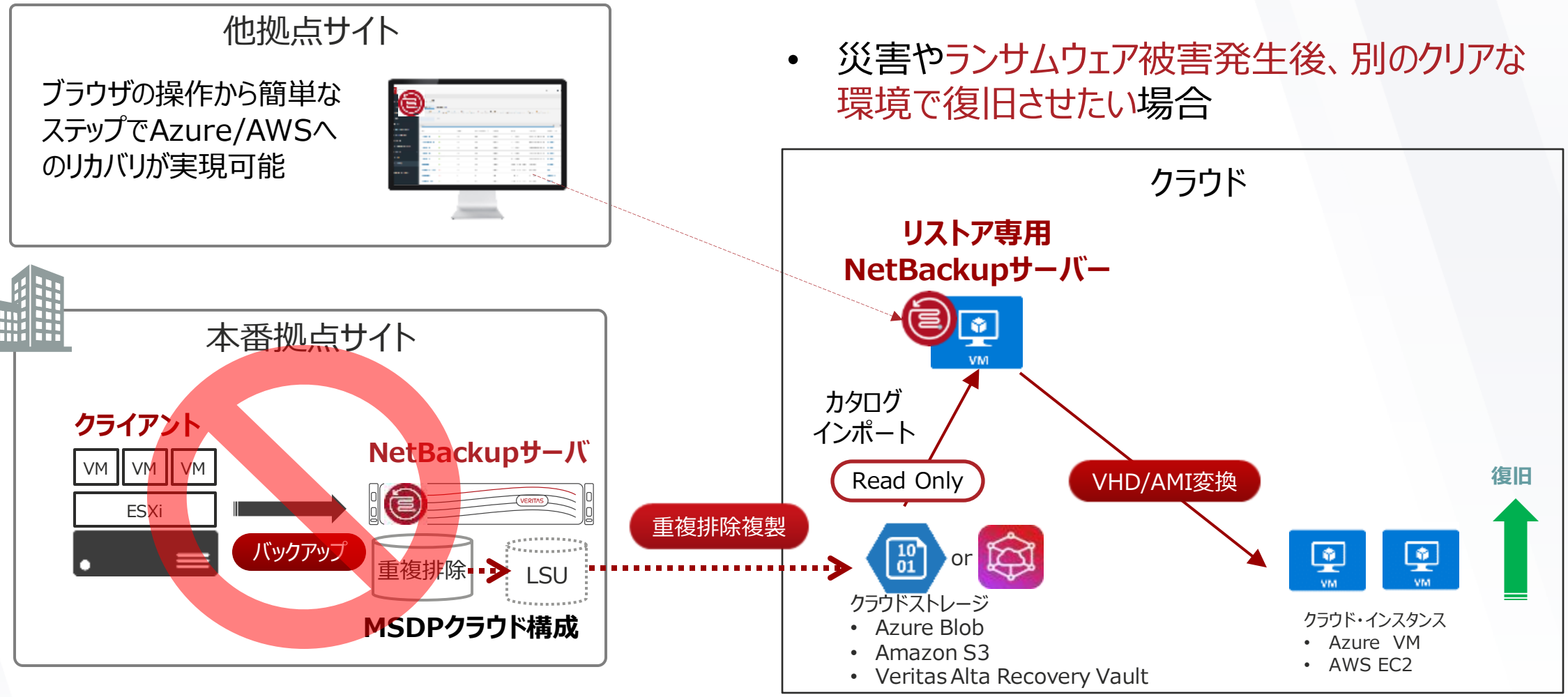
③ マルウェアに感染したバックアップデータはデフォルトでは、リストア不可

④ マルウェア感染したファイルを除外したリストア

⑤ ネットワークを分離した状態で仮想マシンを動作確認

オンプレミスの仮想マシンをクラウドで復旧

- 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



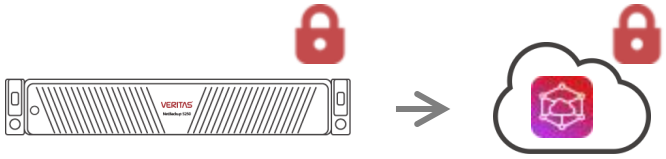
Agenda

- ランサムウェア攻撃の現状
- 課題解決のための要件とベリタスのソリューション
- ベストプラクティス
- 株式会社mizkan様の事例をご紹介
- まとめ

VERITAS

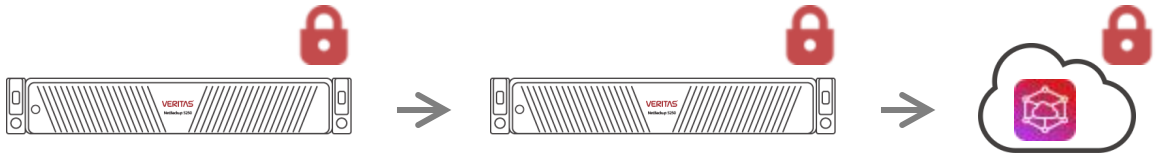
ベストプラクティス構成

1



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

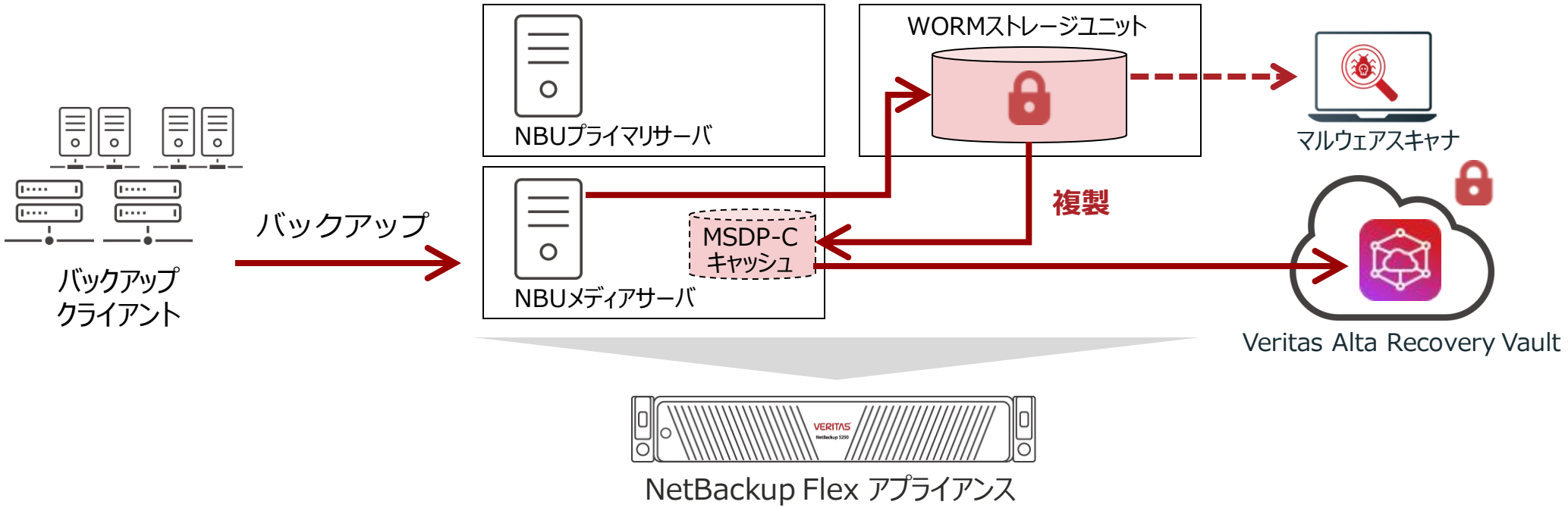
2



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

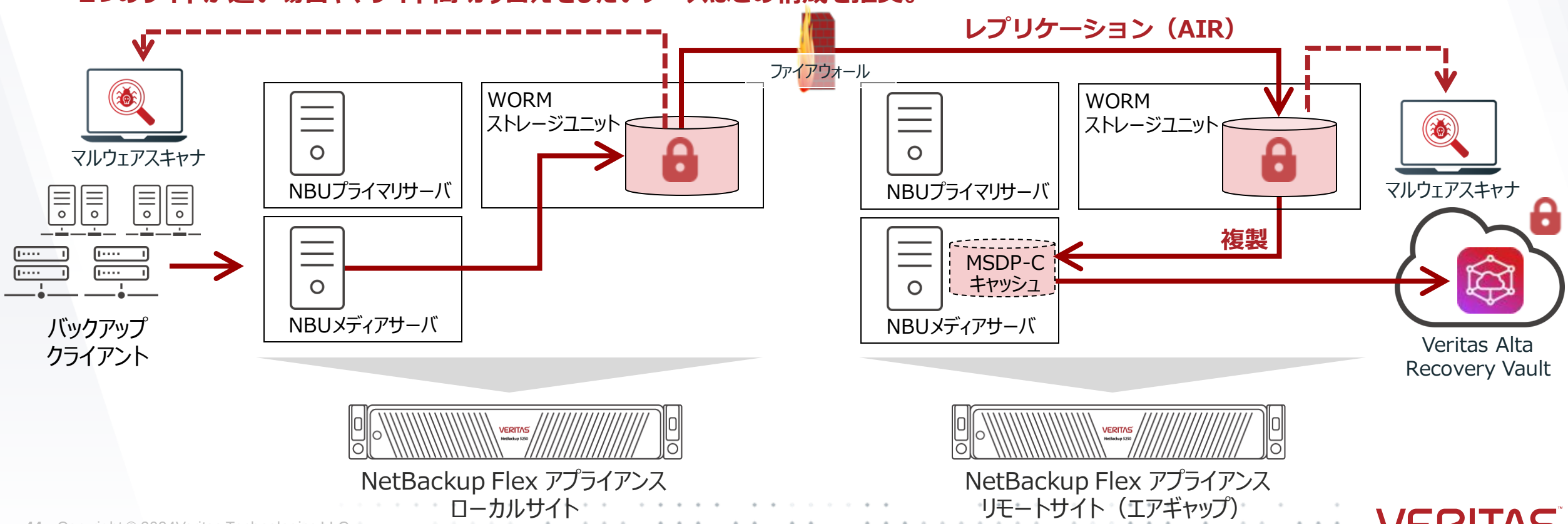
構成例①　NetBackup Flex アプライアンス
+ Veritas Alta Recovery Vault

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

- ランサムウェア攻撃の現状
- 課題解決のための要件とベリタスのソリューション
- ベストプラクティス
- 株式会社mizkan様の事例をご紹介
- まとめ

株式会社mizkan様

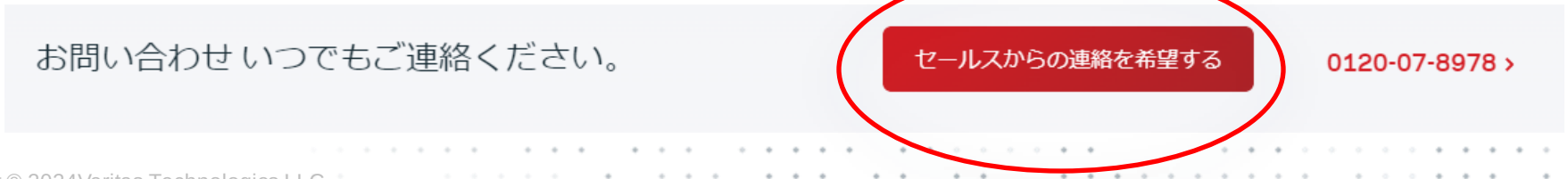
- 会社概要
  従業員数：約3700名
  （グループ全体、2023年4月1日現在）

  業種：食品

  業務概要：酢やぽん酢など家庭用／業務用調味料や
  加工食品、納豆の企画開発・製造販売を展開。
  海外ブランドで展開するパスタソースやスイートピクルスなど
  グローバルにビジネスを展開。

最初のMTGにつながったきっかけ

こちらのWebサイトから、
製品紹介をしてほしいとお問い合わせを、
いただきました！！！



導入ソリューション決定までのポイント

積極的な情報提供の実施

mizkan様の場合、コンタクトのはじめから直接やり取りが可能でした。
そのため、ソリューションの紹介にとどまらず、ランサムウェア対策のバックアップとして、
何を検討しなければいけないのかといった情報提供も実施したことで、
mizkan社内での勉強会もやりやすく、評価いただきました。

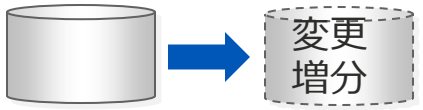
QA対応などの継続的なフォロー

お客様がソリューションを導入する上で疑問に思った点も、
頻繁にMTGを開催したり、資料を作成してお渡ししたことで疑問点がすぐに解消し、
mizkan社内でのNetBackup製品についての理解や、どのソリューションにするかの検討を加速する結果となりました。

既存バックアップの課題

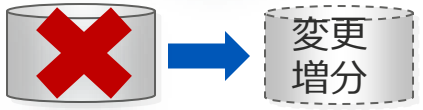
既存バックアップ

ストレージの機能によるスナップショットを取得している状況



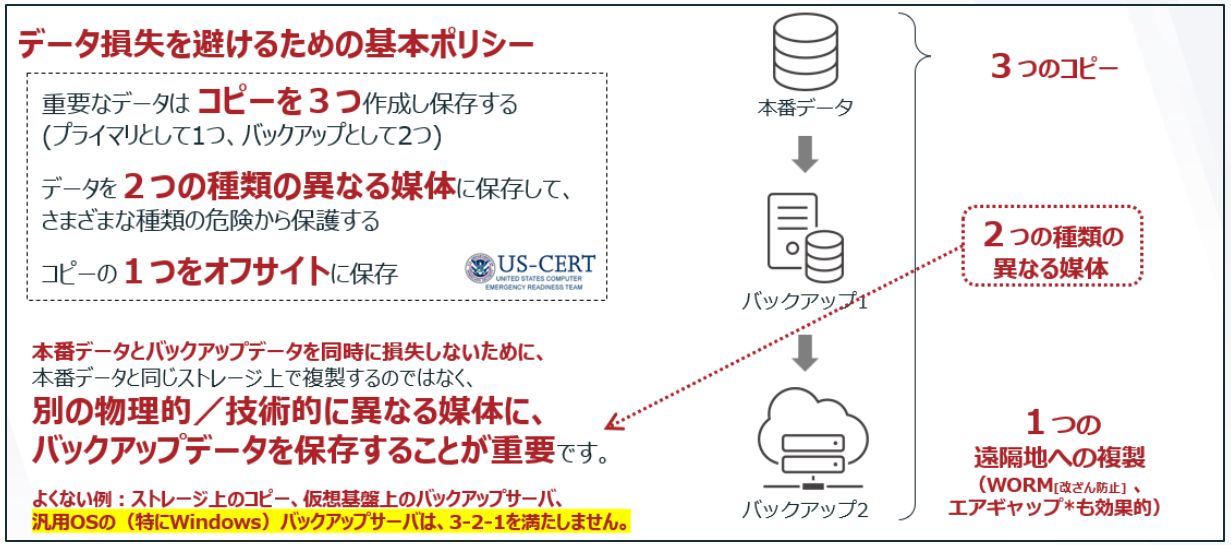
オリジナル　　スナップショット

障害やサイバー攻撃にて、
オリジナルが消失すると・・・



オリジナル　　スナップショット

スナップショットを取得していても、
もとに戻せない・・・

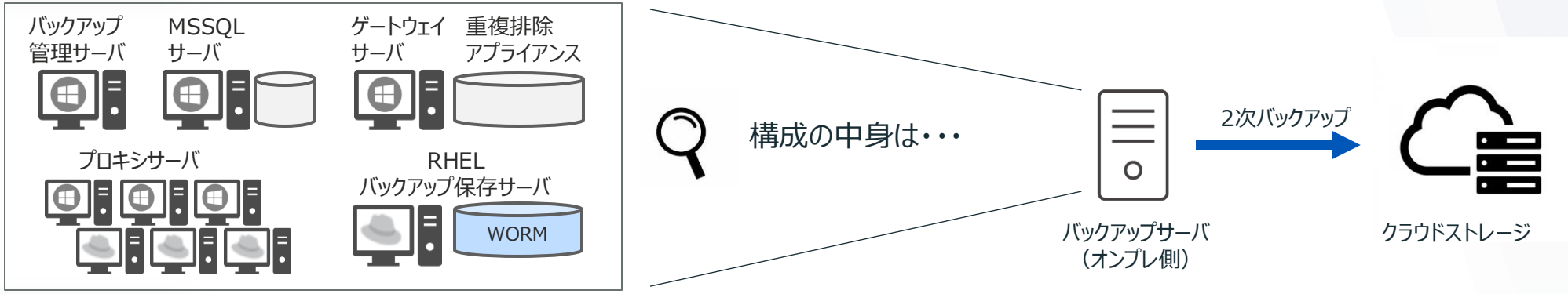


既存バックアップの延長で
ランサムウェア対策をしても、
3-2-1ルールに沿ってバックアップデータを
強固に守り切れる構成にできない・・・

他社との比較

競合A社、B社

3-2-1バックアップルールに沿った構成をする上で、
オンプレ側のバックアップサーバにて、コスト面や要件に未達の部分あり



Veritas

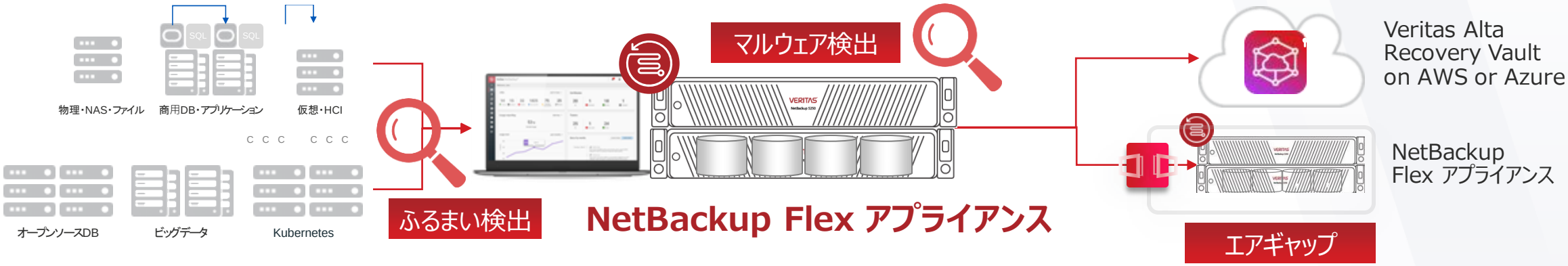
アプライアンスなので構成がシンプル、かつクラウドもVeritasで調達が可能

Agenda

- ランサムウェア攻撃の現状
- 課題解決のための要件とベリタスのソリューション
- ベストプラクティス
- 株式会社mizkan様の事例をご紹介
- まとめ

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



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

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

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

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

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

Q&A

Veritas Vibe Webinar

VERITAS

ありがとうございました