



VERITAS

これで失敗しない！
ランサムウェア対策のための
“正しい”バックアップ

ベリタステクノロジーズ合同会社



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。

本日の内容

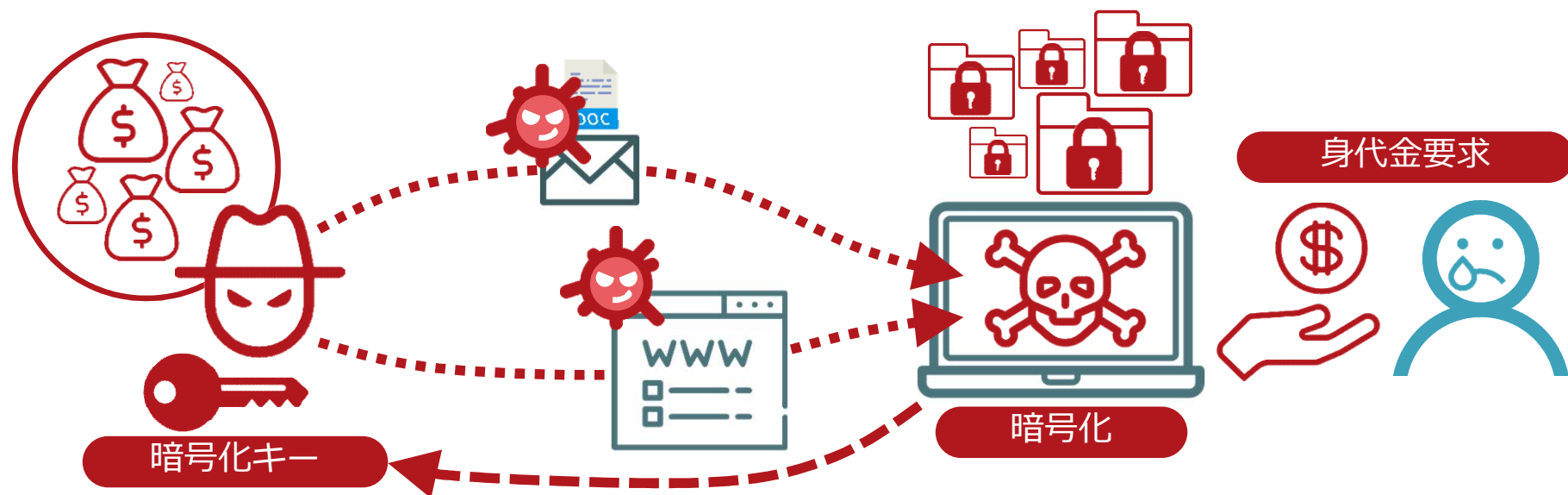
- | | |
|---|---------------------|
| 1 | ランサムウェアは何か怖いのか？ |
| 2 | ランサムウェア対策としてのバックアップ |
| 2 | サーバーのバックアップ棚卸し |
| 3 | 実は難しいクライアントのバックアップ |
| 4 | 本日のまとめ |



ランサムウェア

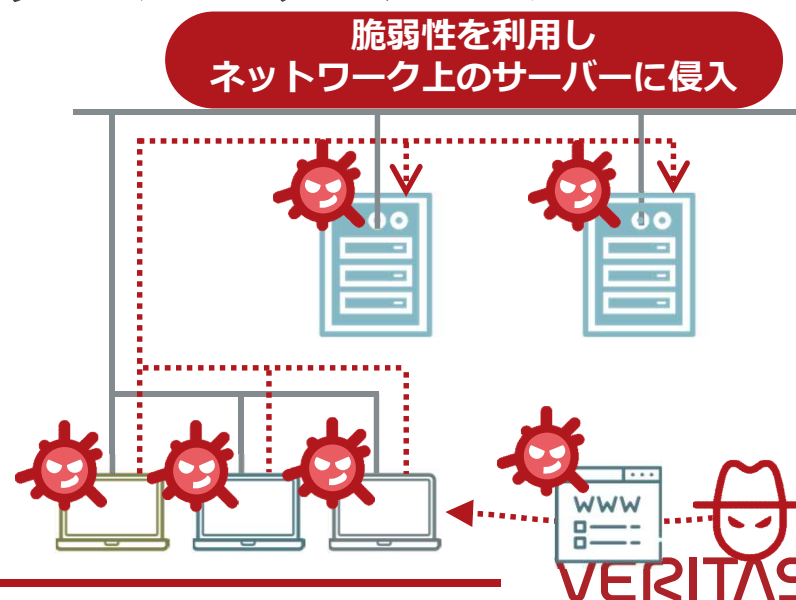
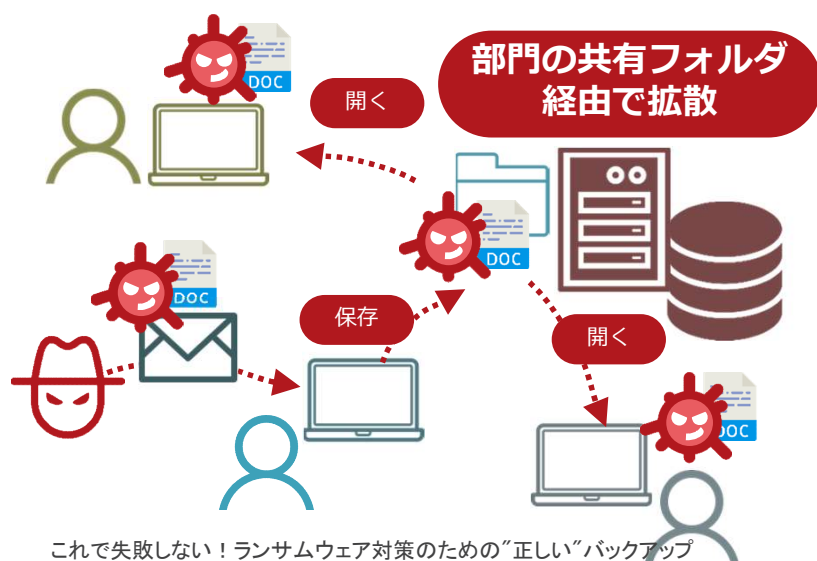
ランサムウェアとは？

- 感染したPCをロック、またはファイルを暗号化し利用不能にした後元に戻す事と引き換えに「身代金」を要求する不正プログラム。
- 主にウェブブラウジングやメールの添付ファイルなどを通じて感染。



ランサムウェアの影響範囲

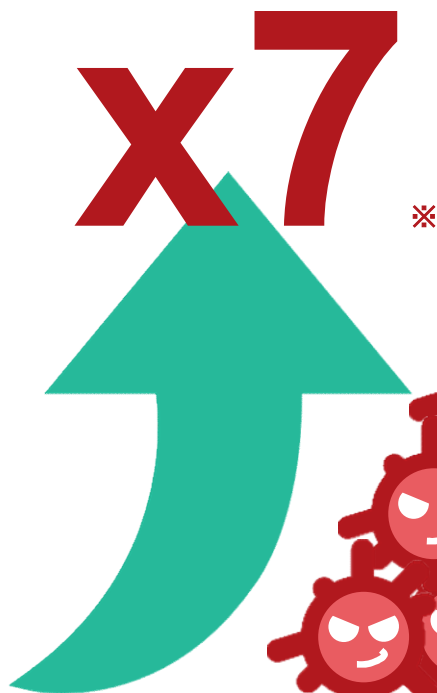
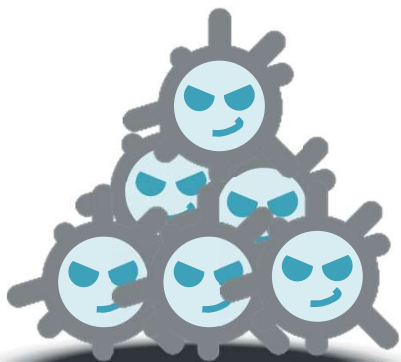
- ❑ 直接感染した**クライアント**はもちろん、悪意あるスクリプトを含むファイルが**ファイルサーバーを通じて拡散**する場合や、社内から向けのサイトをホストする**Webサーバーを通じての拡散**など**被害が広範囲にわたる恐れ**もあり。
- ❑ クライアントだけではなく**サーバーを狙ったランサムウェア**も登場。



x7

感染件数も大幅に増加！

2015年



2016年

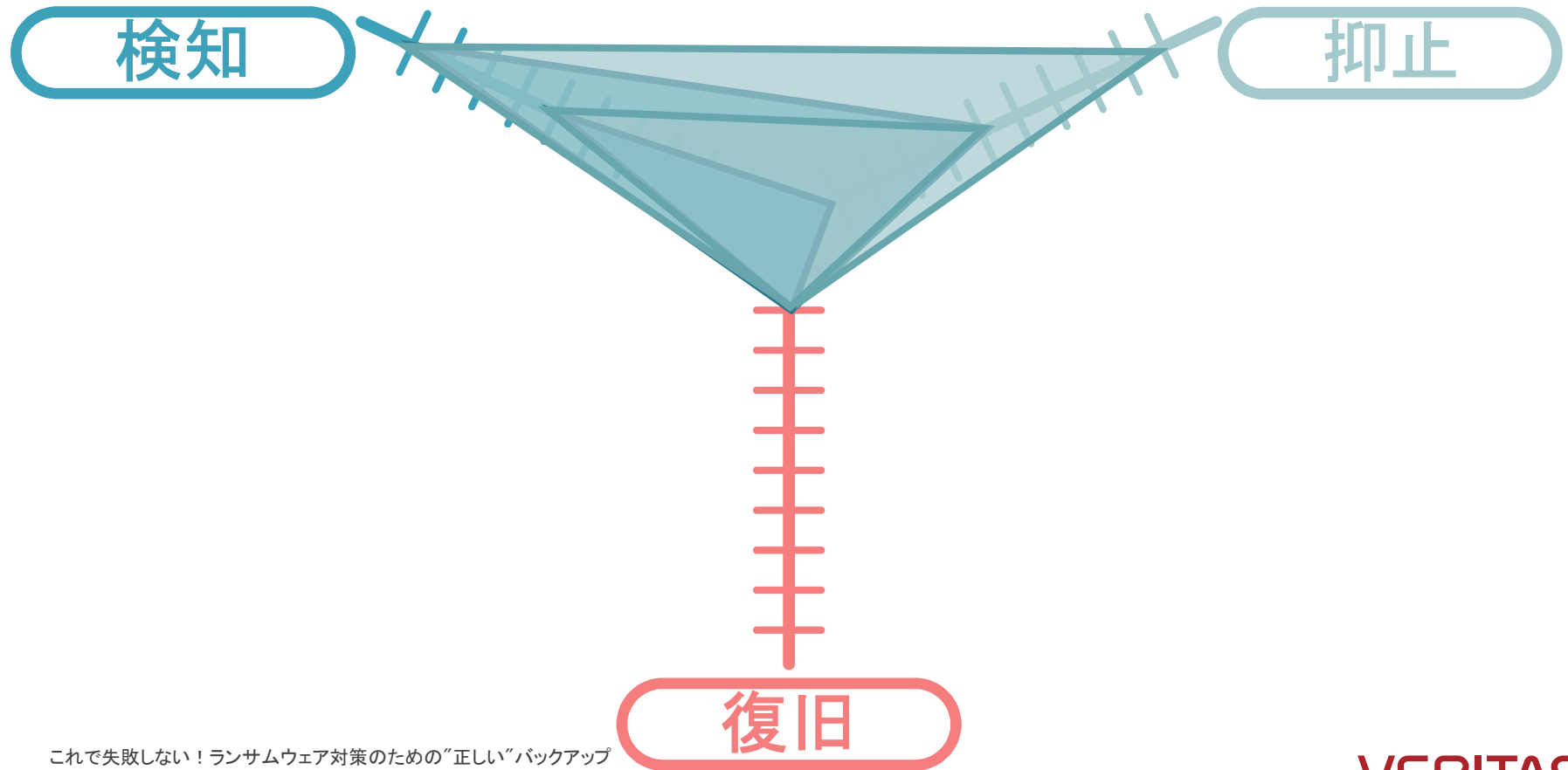


しかし、
ランサムウェアだって
所詮マルウェアの一種
ですよね？

何故そんなに
話題になっているのですか？

従来までのセキュリティアプローチ

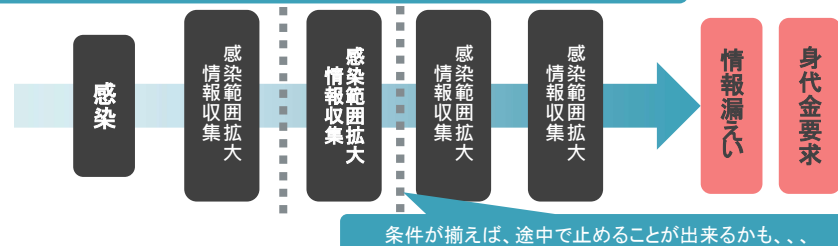
検知と抑止が中心



ランサムウェアの何か他のマルウェアと違うのか？

- 感染から**実被害が出るまでが早い**。また、**止める猶予が無い**。
- ランサムウェアの最大の脅威は、攻撃側の意図に乗る / 乗らないに関わらずそのコンピューターの**全データロストが発生すること**。
そして、**バックアップが無ければデータが戻らない**可能性があること。

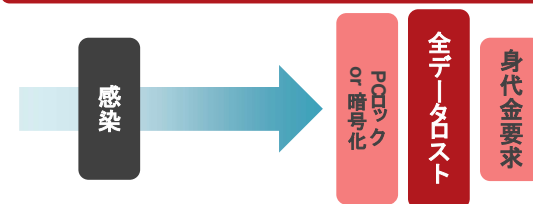
従来からの脅威 ～大器晩成型



実被害

- ・ 企業の**信用**
- ・ **長期**にわたる**ビジネス機会**
- ・ 莫大な**補償金**

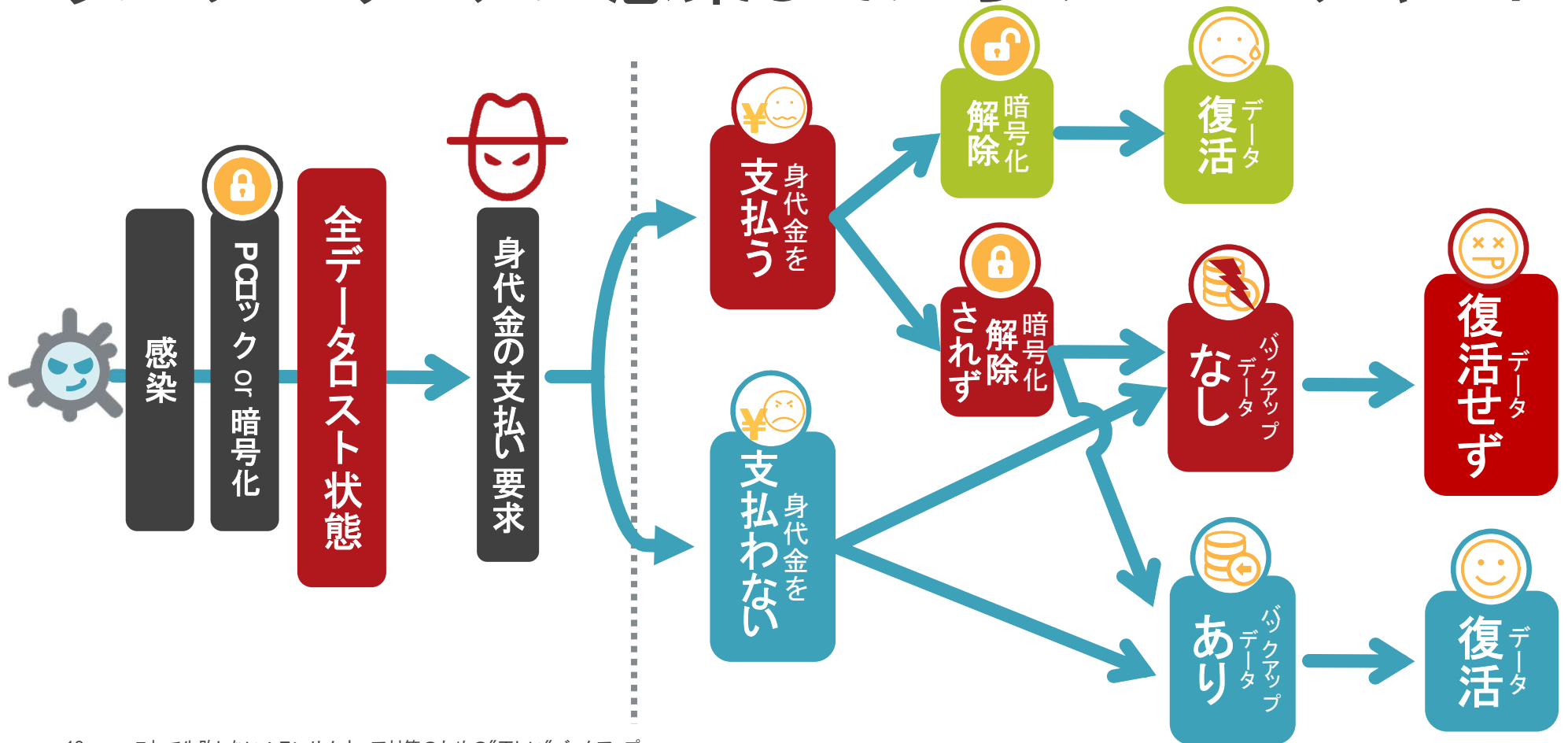
ランサムウェア ～早期熟成型



実被害

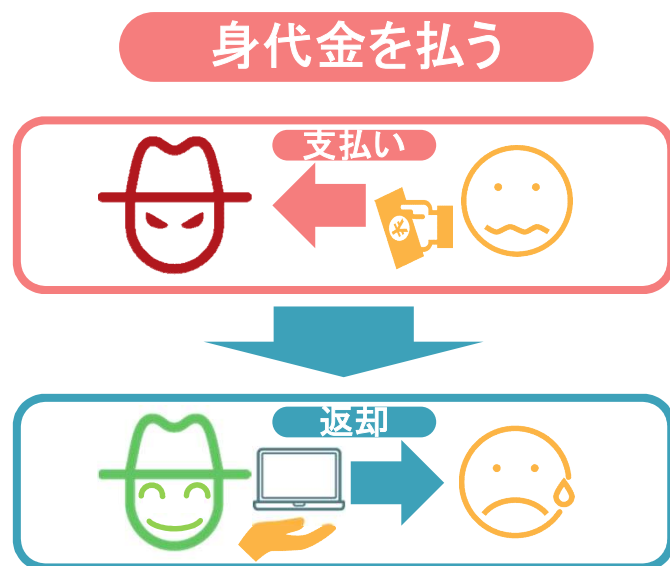
- ・ 感染端末の**全業務データ**
- ・ **直近**のビジネス機会
- ・ (感染した事が表面化した場合の)**信用低下**

ランサムウェアに感染してからのフローチャート

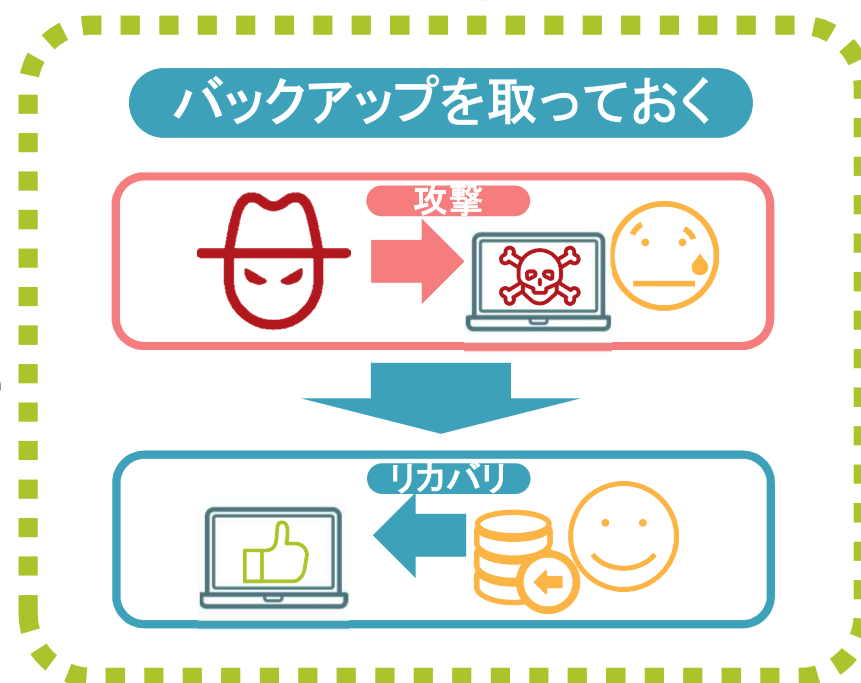


ランサムウェアに感染してもデータを復活させるには？

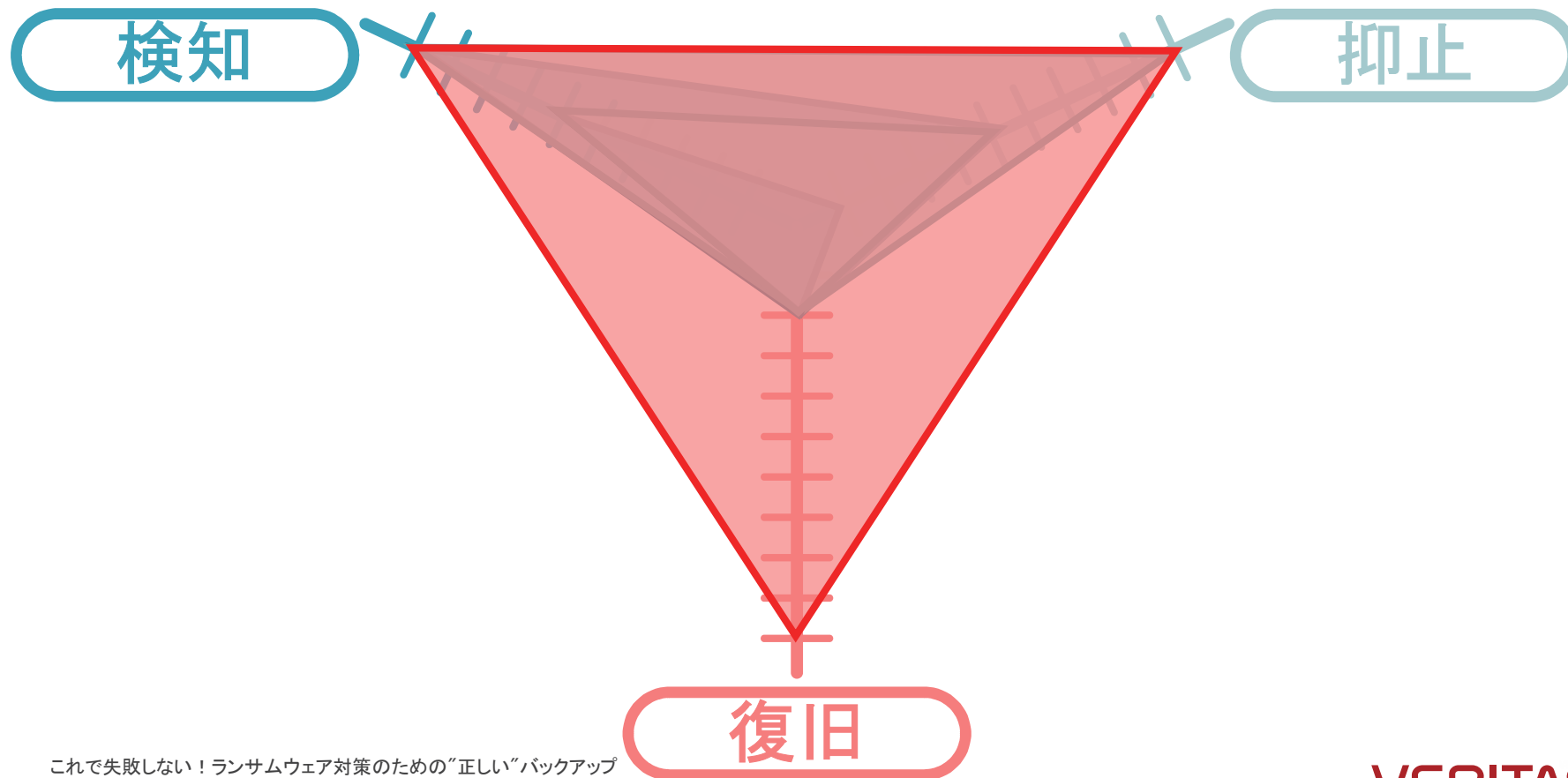
- ❑ 指示通り**身代金を払う**。攻撃者がいい人であれば、ロックが解除されてデータが通常の状態に戻る。
- ❑ 日頃から**バックアップ**を取得し、復旧が必要なときに備える。



or



これからのセキュリティアプローチ 検知と抑止に加え、復旧が重要に



つまり、
セキュリティ
ソリューションとしての
バックアップ
が必要とされています。

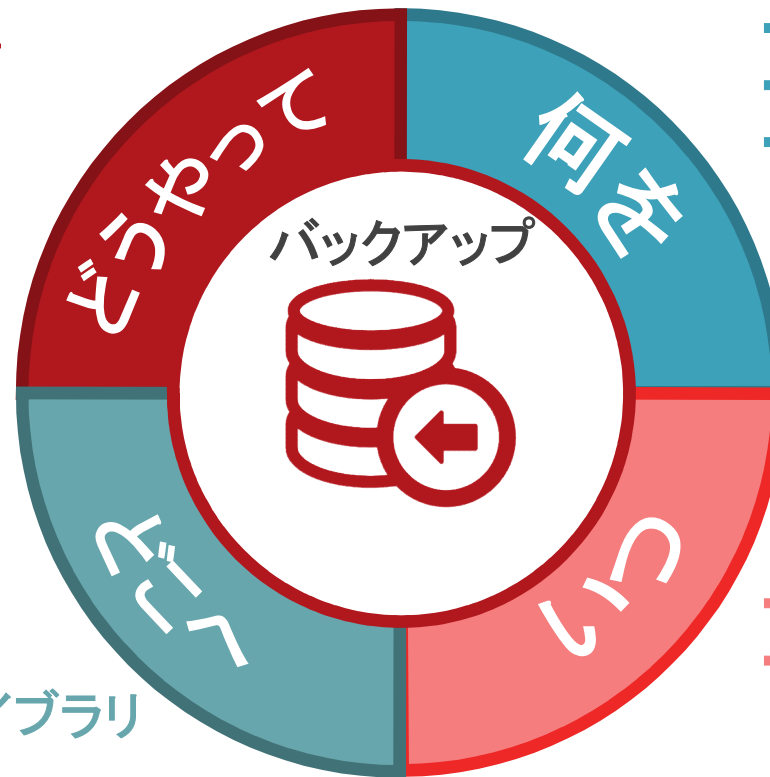


バックアップ

一般的なバックアップの考えかた

- ・ ファイル / フォルダ単位
- ・ イメージバックアップ
- ・ 重複排除

etc...



- ・ ファイル・フォルダ
- ・ Oracle / SQL / Exchange
- ・ 仮想マシン

etc...

- ・ ローカルディスク
- ・ 外付けHDD
- ・ テープ装置 / テープライブラリ

etc...

- ・ 週末フルバックアップ
- ・ 平日増分バックアップ

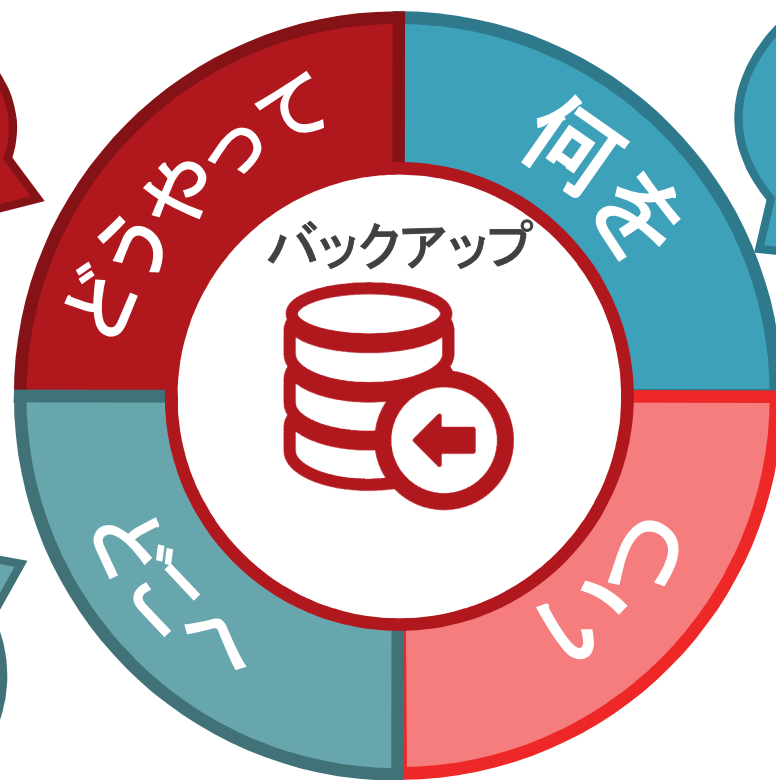
etc...

ランサムウェアを意識したバックアップとは？

生産性への
影響を最小限
に抑える

データの暗号化に加え
システムのロックに備え
システムの
バックアップも
検討する

必要に応じて
バックアップ先を
リスクの低い
場所へ変える



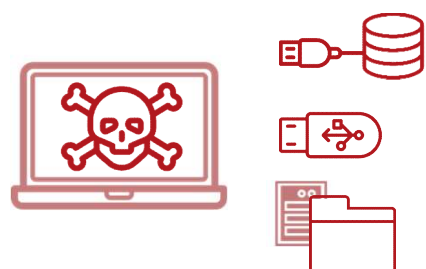
基本的な運用設計は
そのままに
確実性と
利便性を
高める

リスクの少ないバックアップ先を選ぶ



❑ ランサムウェアに暗号化されない場所にバックアップを取得する。

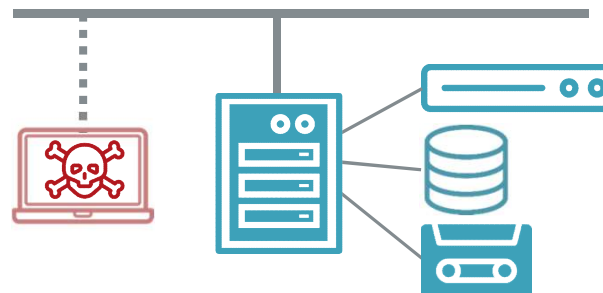
悪い例



感染コンピューターから
直接アクセス可能な場所

例)
・USBメモリ
・外付けHDD
・ネットワークドライブ
・クラウドストレージとの
同期フォルダ

良い例



感染コンピューターから
直接アクセス不能な場所

例)
・バックアップサーバー
越しのデバイス
・テープ装置
・隠し共有

リスクの高いデバイス

外付けディスク

USBHDD

内蔵ディスク

USBメモリ

リムーバブル
ディスク

VSSスナップショット

ネットワークドライブ

ファイルサーバー共有

リスクの低いデバイス

テープ装置

クラウドストレージ

OSTストレージ

バックアップサーバーに
接続したディスク装置

バックアップサーバーに
接続したテープ装置

余裕のあるスケジュールとリソースを持つ

- 取っていたつもり、にならないように**確実にバックアップを管理する。**
感染時のリストア作業などを想定し、**スケジュールに余裕を持たせる。**



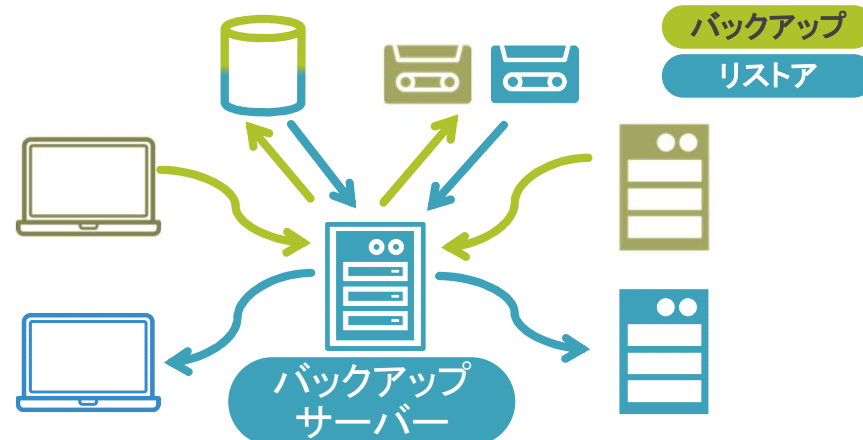
確実にバックアップ

バックアップが失敗した場合の予備があることが好ましい

無理の無いバックアップ計画が必要

	日	月	火	水	木	金	土
1 週目	予備	増		増		増	完
2 週目	予備	増		増		増	完
3 週目	予備	増		増		増	完
4 週目	予備	増		増		増	完

リストアに要するコストを考慮する



- ・バックアップしながらでもリストアを行えるようになっているか？
- ・リストア手順は整備されているか？
- ・リストアを行うのはだれか？

生産性とバックアップのバランスを取る



- サーバー / クライアントそれぞれに求められるニーズを意識し
それぞれに**適した製品選定 / 運用を行う。**

運用の最適化

クライアント



- ・ 外出アリ
- ・ オフィスデータ / メール
- ・ データ量(小)
- ・ ユーザー / 管理者がリストア
- ・ 夜間電源オフ

- ・ 職種によっては、外出等でまとまったバックアップ時間が**確保出来ない**可能性がある。
- ・ 業務中でも**ユーザーに負担の少ないバックアップ**が求められる。
- ・ クライアント数の増加や、外出先での対応など環境が変化してもバックアップ運用を継続出来るだけの**対応力**を求められる。

サーバー



- ・ 24 x 365稼動
- ・ アプリケーションデータ
- ・ 各種データファイル
- ・ 管理者がリストア
- ・ データ量(大)

- ・ バックアップは**夜間に定期的**に行う。
- ・ 限られた時間内で、大容量のバックアップであっても完了出来る**高速なバックアップ**が求められる。
- ・ アプリケーションへの**負荷を最小限**に抑えつつバックアップを可能とすることを求められる。

ニーズに適したバックアップ対象を検討する



- 想定されるランサムウェアの脅威に即し
システムのバックアップ / データのバックアップ
もしくは両方を検討する

クライアント



システム

- ・ マスターイメージからの復元を行う
- ・ ドライブ全体をイメージバックアップ



データ

- ・ デスクトップやマイドキュメントなど特定のフォルダのバックアップ
- ・ ドライブ全体をイメージバックアップ

サーバー



システム

- ・ 構築初期の状態をバックアップ
- ・ システムバックアップを定期的に行う



データ

- ・ アプリケーションやファイルサーバーのデータをバックアップ
- ・ ドライブ全体のバックアップを行う

ランサムウェア対策の バックアップを考えるにあたっては、

サーバー、クライアントそれぞれ
バックアップの棚卸し
を行ったうえで
欠けている部分を埋める
ことが大切

では、

サーバーの場合...

サーバーのバックアップに求められるポイント

□ 高速なバックアップ



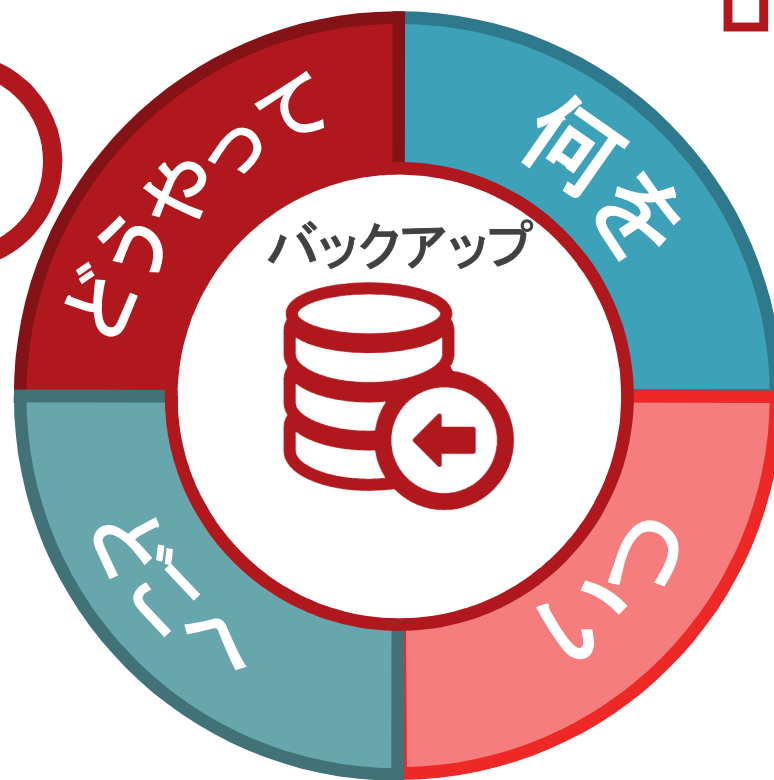
□ 多様なニーズへの対応



□ 安全な構成



□ レポーティング



Veritasが提供するサーバー向けバックアップソリューション

製品	対象	テーマ
 System Recovery	小規模向け  システム  データ	• 高速イメージバックアップ
 Backup Exec	中規模向け  システム  データ	• スタンダード
 NetBackup	大規模向け  システム  データ	• エンタープライズ



NEW

Veritas System Recovery 16

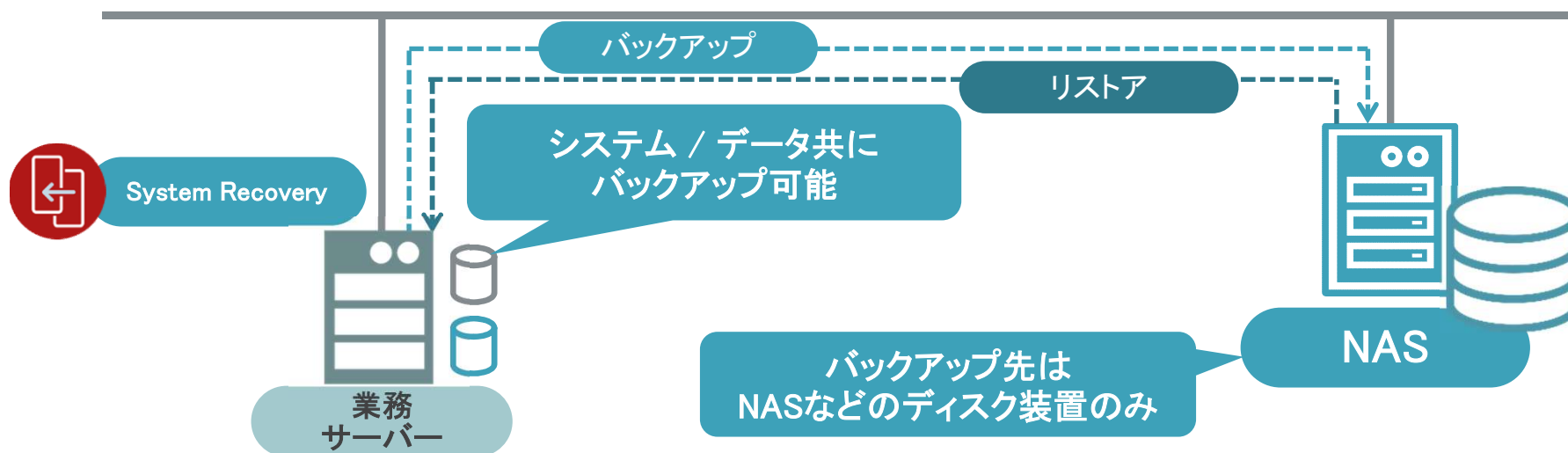
小規模な環境にシンプルなバックアップソリューションを

- 小規模サーバーバックアップにおける課題
 - バックアップ運用に手間はかけない
 - 難しい操作は避けたい



簡単な操作
設定・管理のしやすさ

Veritas System Recovery 16



Veritas System Recoveryの主な機能



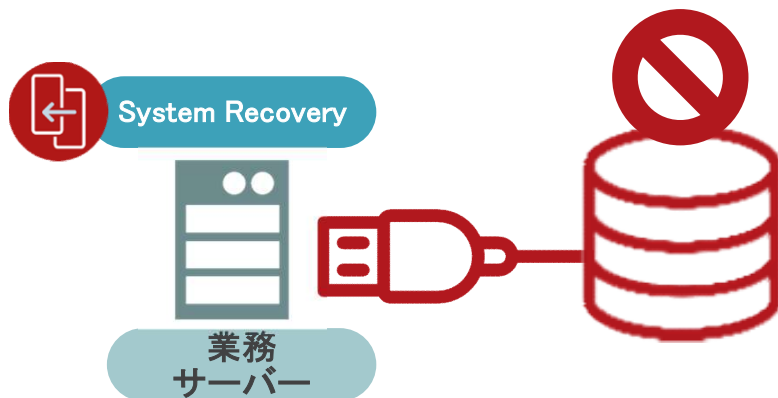
System Recovery

- ✓ドライブ全体を高速にイメージバックアップ
- ✓vTrackによるさらに高速な増分バックアップ
- ✓簡単操作で楽々バックアップ
- ✓Windows 2016 / VMware 6.5対応

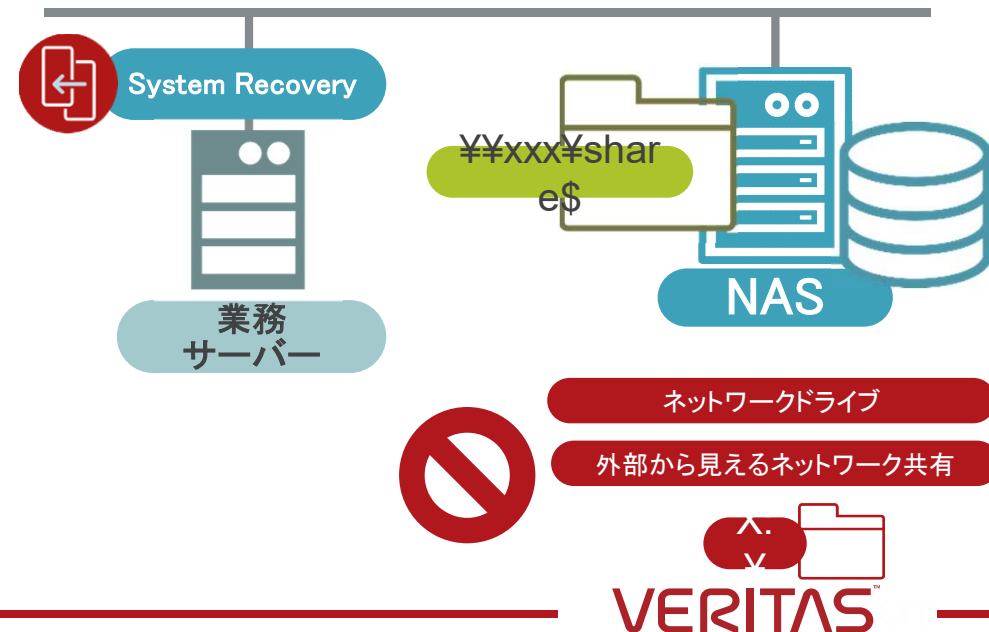
ランサムウェア対策に

Veritas System Recoveryを使う場合のポイント

- ❑ 外付けHDDへの直接バックアップは避ける



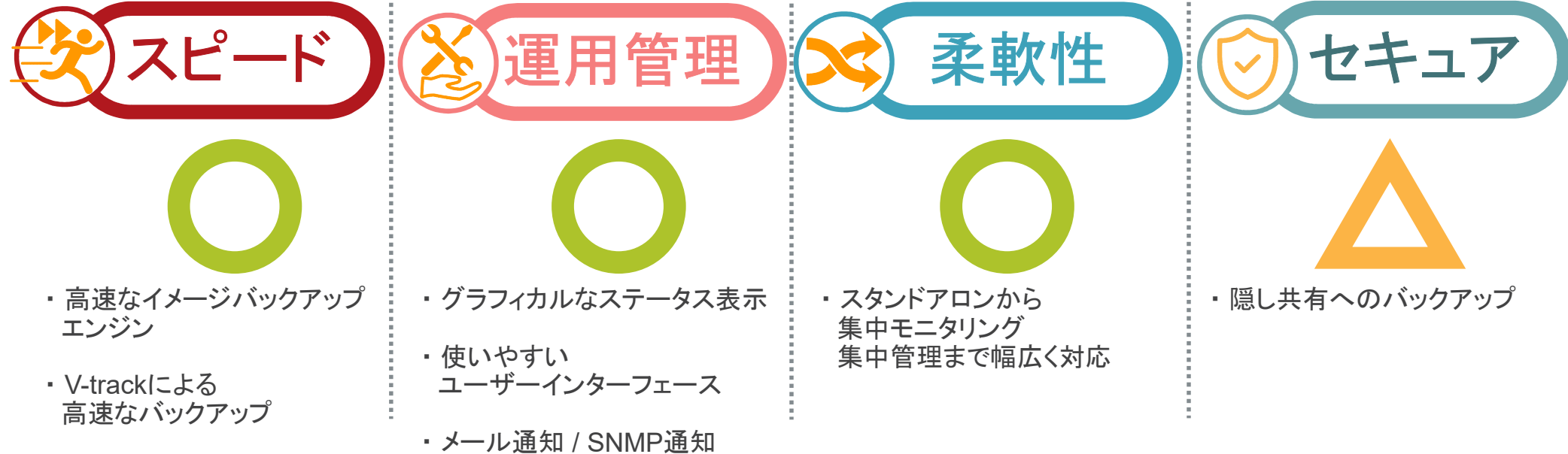
- ❑ NASへバックアップするときはネットワークドライブではなく隠し共有を使う



Veritas System Recovery



System Recovery





NEW

Veritas Backup Exec 16

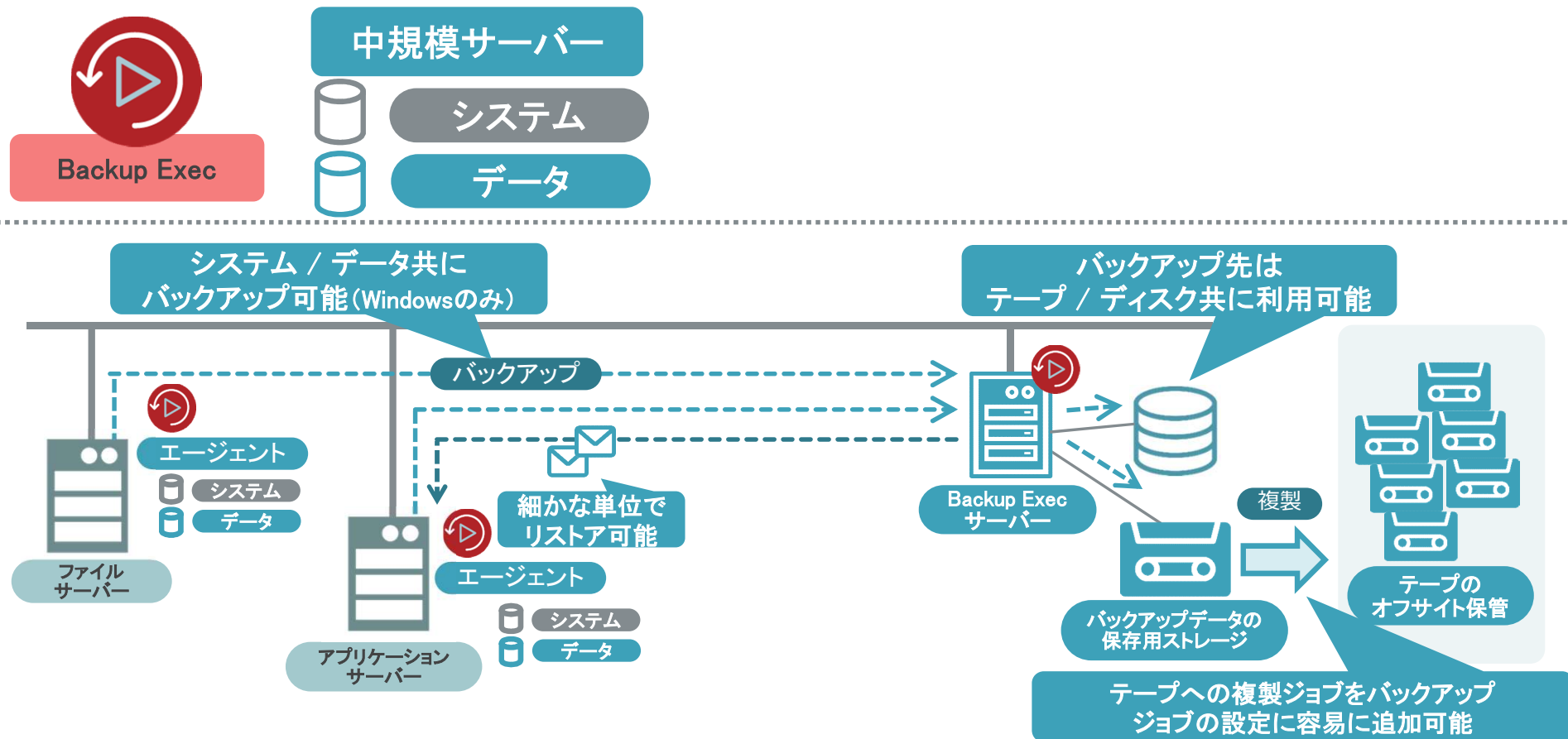
中規模な環境にマルチな機能を持つスタンダードを

- 中規模サーバーバックアップにおける課題
 - 様々なアプリケーション
 - 仮想 / 物理への対応
 - 効率の良い管理
 - 多少複雑なニーズ



多様なニーズへの対応
効率の良い設定・管理
複雑な構成にも対応出来る柔軟さ

Veritas Backup Exec 16



Veritas Backup Execの主な機能



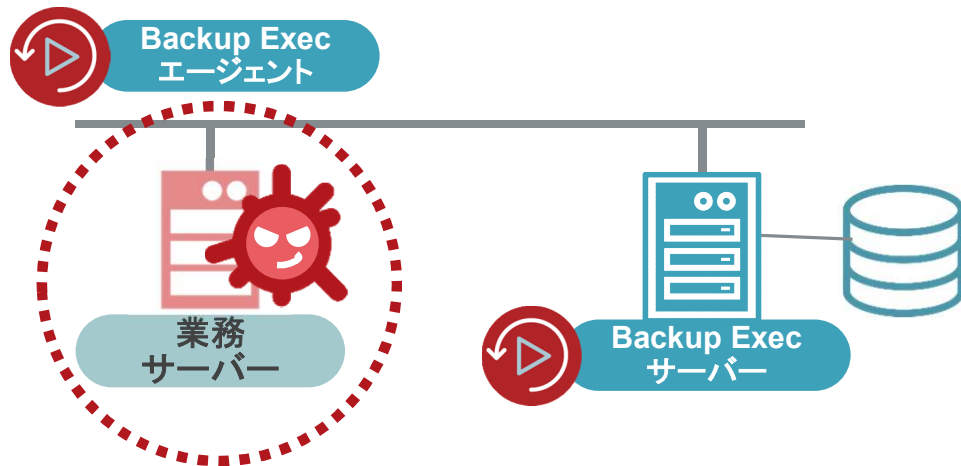
Backup Exec

-
- ✓ データ / システムいずれもバックアップ可能
 - ✓ Windowsを中心に各種アプリケーション、仮想化環境に対応
 - ✓ 重複排除による高いバックアップパフォーマンスと効率の良いストレージ利用
 - ✓ GRTにより細かい単位でのリストアが可能

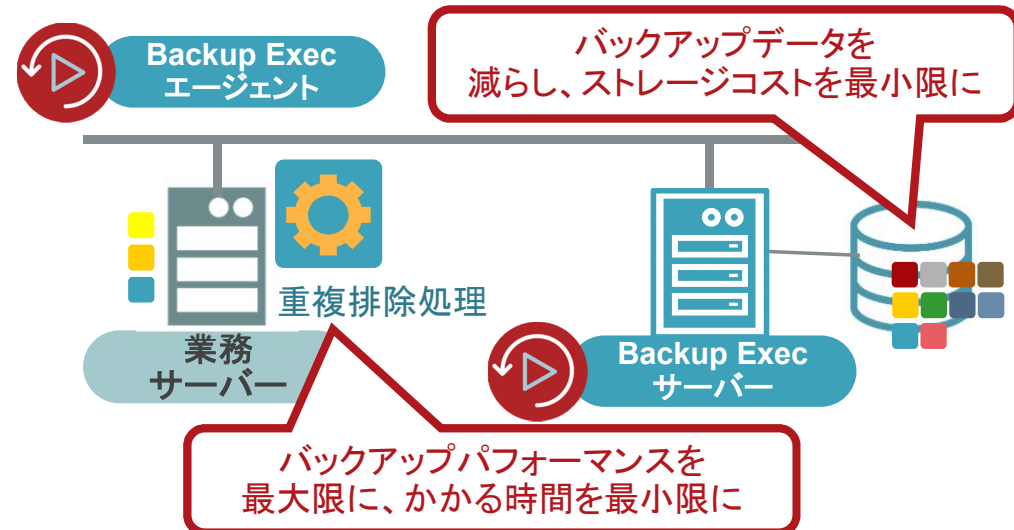
ランサムウェア対策に

Veritas Backup Execを使う場合のポイント

- クライアント – サーバー型の構成で
万が一の時も安心



- 重複排除を利用して
業務への影響とコストを
最小限に抑える



Veritas Backup Exec



Backup Exec

スピード



- ・重複排除による高速なパフォーマンス
- ・仮想マシンのインスタントリカバリ機能

運用管理



- ・バックアップサーバーにてわかりやすいGUIによる一括管理
- ・メール通知、レポートニングによる効率の良い運用管理

柔軟性



- ・クライアントのプッシュ配信
- ・自動リソース検出

セキュア



- ・クライアント - サーバー型
- ・遠隔地 / クラウドでのバックアップデータの保管



NEW

Veritas NetBackup 8.0

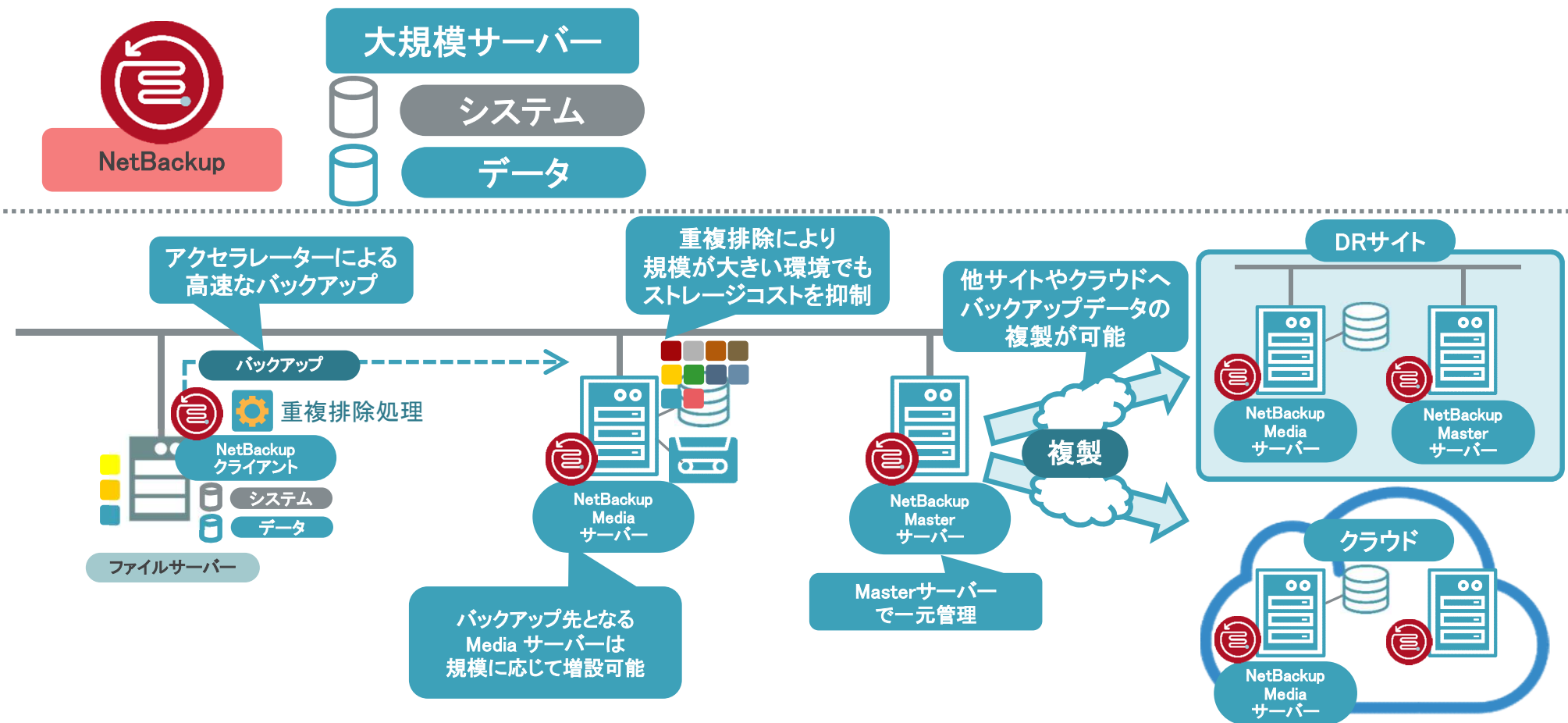
大規模な環境に圧倒的なパフォーマンスと機能を

- 大規模サーバーバックアップにおける課題
 - 大容量データのバックアップが出来ない
 - 膨大なバックアップデータ量
 - 大規模であっても効率的な管理が可能
 - 災害対策など環境のシームレスな拡張



圧倒的なバックアップ速度
ストレージコストの抑制
効率的な管理と柔軟な拡張性

Veritas NetBackup 8.0



Veritas NetBackupの主な機能



NetBackup

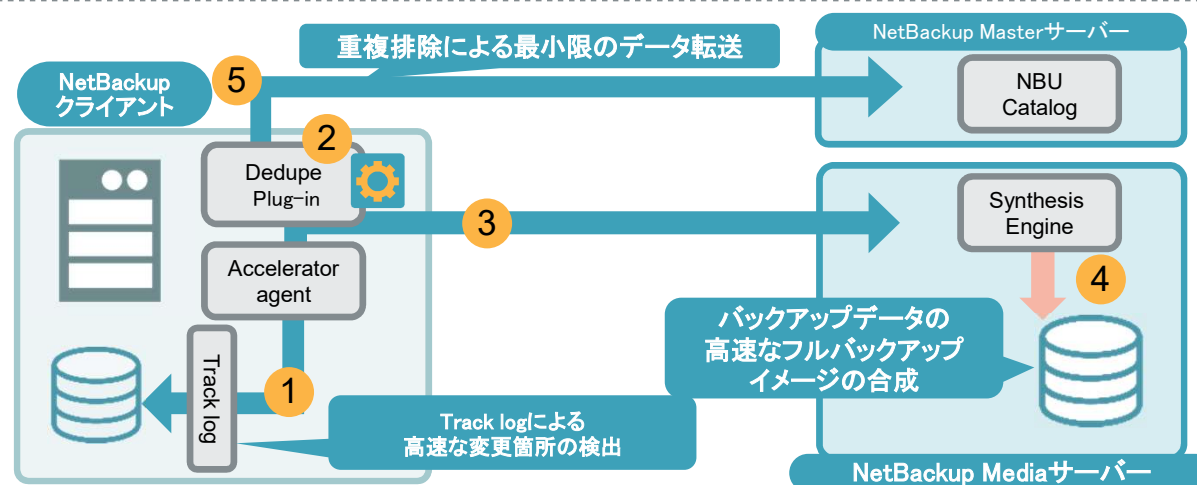
- ✓ 様々な環境を有する大規模環境において効率的な運用を提供
- ✓ アクセラレーターによる高速なバックアップを実現
- ✓ 重複排除によりストレージコストを大幅に削減
- ✓ ニーズに応じて環境を拡大し、クラウドやDCを活用した構成へ柔軟に拡張が可能

Veritas NetBackupの特長



NetBackup

NetBackup アクセラレーター ～100倍速いバックアップ



- 1 変更ファイルのみのリード
- 2 重複排除処理の実行
- 3 ユニークデータのみ転送
- 4 合成バックアップの内部作成
- 5 クライアントからは変更されたメタデータのみ転送

短時間でフルバックアップ
イメージを作成

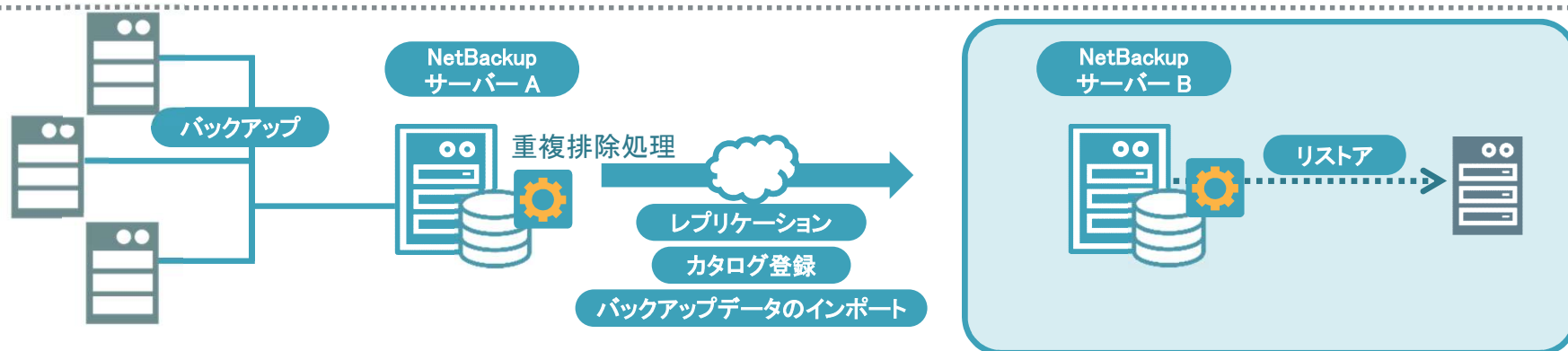
- フルバックアップを数十倍の速さで実行可能
- 重複排除により転送データ量やバックアップデータ量を大幅に削減

Veritas NetBackupの特長



NetBackup

Auto Image Replication (AIR) ～遠隔地を活用した災害対策

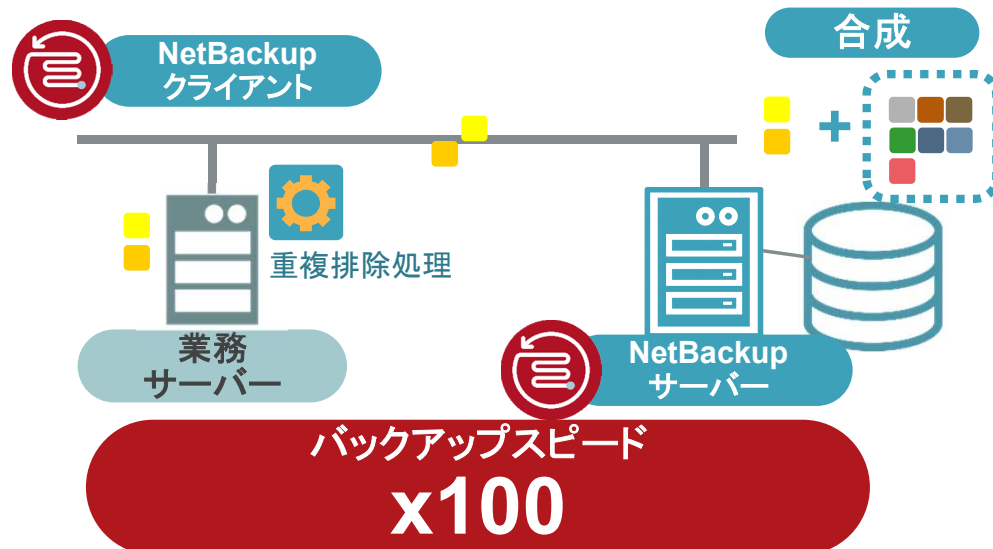


- 遠隔地にリストアレディな災害対策環境を構築
- 重複排除を活用し、ネットワーク負荷を最小限に抑えたデータ転送を実現
- 転送先には距離の離れたDRサイト上やサーバーやIaaS環境を利用可能

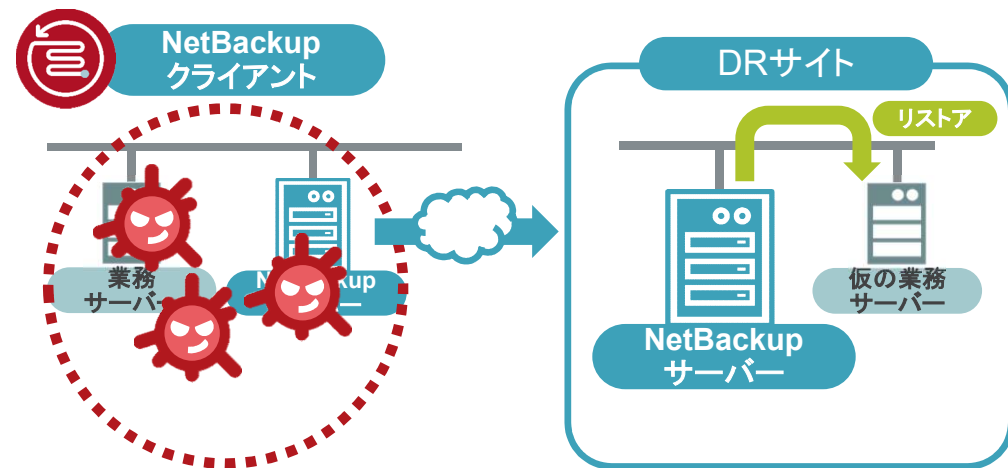
ランサムウェア対策に

Veritas NetBackupを使う場合のポイント

- アクセラレータバックアップによって
バックアップ対象の
増加にも余裕の対応



- 遠隔地へのレプリケーションにより
被害の拡大時にも
さらなる安心を



Veritas NetBackup



NetBackup

スピード



- ・アクセラレーターによる圧倒的なパフォーマンス
- ・仮想マシンのインスタントリカバリ

運用管理



- ・マスターサーバーによる効率のより一括運用管理
- ・OpsCenterと連携しマルチサイトの一括運用も可能

柔軟性



- ・メディアサーバーの追加からクラウドの利用、複数サイトへの拡大まで、ニーズに合わせた幅広い選択肢を提供

セキュア



- ・クライアント – サーバー型
- ・複数のサイトへ拡張し構成の冗長化が可能

その他、全体的なポイント

- バックアップデータの保持期間は多少長めにする。
※潜伏期間が10日間などのケースもあります。
- バックデータは細かくリストア出来ることが好ましい。
※被害にあったユーザーのみのメールデータなど。
- クラウドを利用する場合はパフォーマンスに気をつける。
※バックアップ / リストア共に重要。

サーバー向け各製品の特長まとめ



スピード



運用管理



柔軟性



セキュア



System
Recovery



Backup Exec



NetBackup





さて、クライアントは？

クライアントのバックアップの特長と求められる要件

- 外出や電源OFFなど一定の状態ではないため、
応答性の良いバックアップの仕組みが必要。
- 企業 / 従業員によって**バックアップ / リストアの主体が異なる。**
- 企業規模の拡大やクライアント数の増加に対応出来る**拡張性**や
生産性を低下させないための**利便性**そしてその運用管理の**容易さ**が求められる。



クライアントのバックアップは実はかなり難しい

クライアントのバックアップに求められるポイント

- 場所を選ばない
環境に優しいバックアップ

 機能性

- 管理者 / ユーザーによる
様々なニーズへの対応

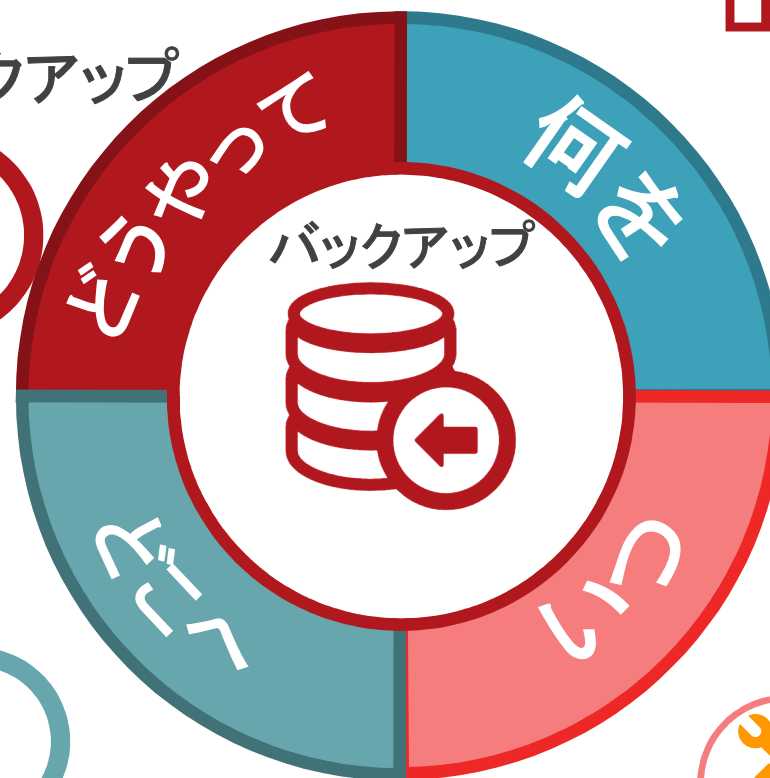
 応答性

- 安全な構成

 セキュア

- 規模を問わず様々な
要件に対応出来る
小回りの利く運用

 運用管理



Veritasが提供するクライアント向けバックアップソリューション

製品	対象	テーマ
 System Recovery	小規模向け  システム  データ	• 高速イメージバックアップ ※機能はサーバー版と同じです
 Desktop and Laptop Option	中～大規模向け  データ	• リアルタイムデータバックアップ



NEW

Veritas System Recovery 16

小規模な環境向けに誰でも扱えるソリューションを

- 小規模クライアントバックアップにおける課題
 - 管理者が不在
 - 難しい操作にはついていけない



簡単な操作
設定・管理のしやすさ

Veritas System Recovery



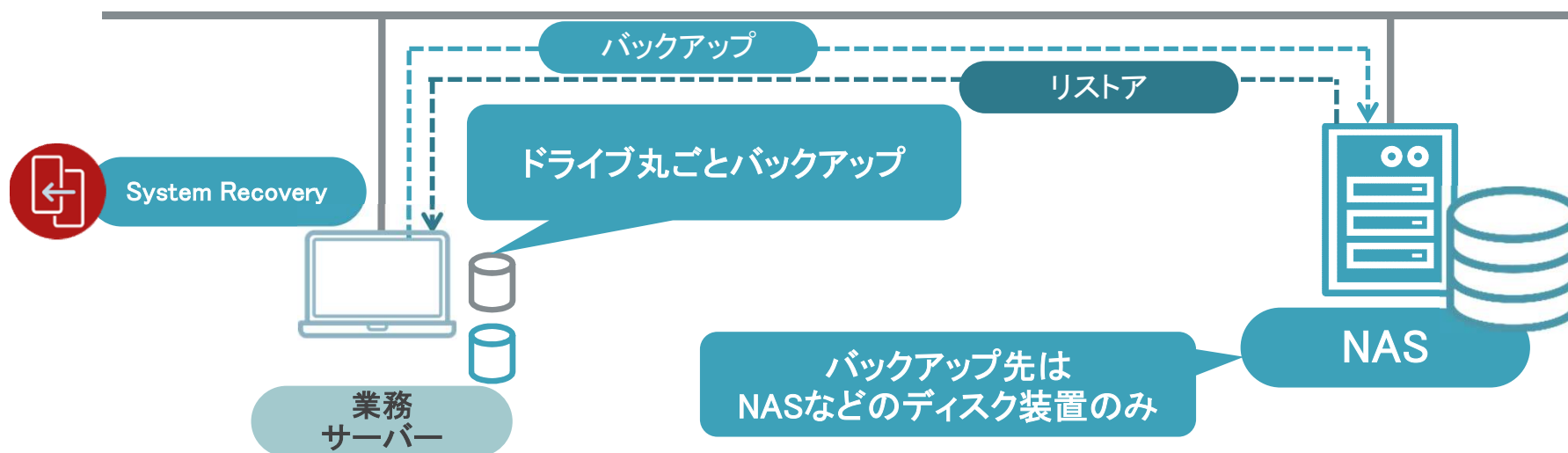
小規模クライアント



システム



データ



Veritas System Recoveryの主な機能

※サーバー向けと機能は同じです。



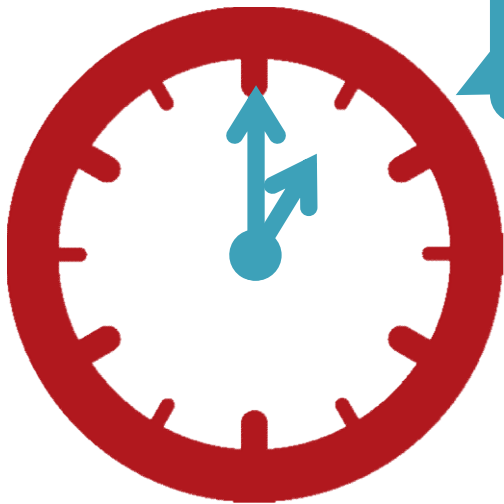
System Recovery

- ✓ドライブ全体を高速にイメージバックアップ
- ✓vTrackによるさらに高速な増分バックアップ
- ✓簡単操作で楽々バックアップ
- ✓Windows 10対応

ランサムウェア対策に

Veritas System Recoveryを使う場合のポイント

- 一定のルールを基に
バックアップ時間を確保する



例)
毎日12時~13時に
バックアップする

- 管理者だけではなく
**ユーザー自身に
管理を任せる**事も視野に入れる



Veritas System Recovery



System Recovery



機能性



- ・ 高速なイメージバックアップエンジン
- ・ V-trackによる高速なバックアップ



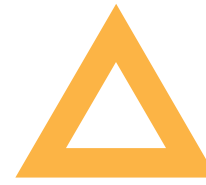
運用管理



- ・ グラフィカルなステータス表示
- ・ 使いやすいユーザーインターフェース
- ・ メール通知 / SNMP通知



応答性



- ・ 管理者による設定が基本
- ・ バックアップはユーザー側で手動でも実行可能



セキュア



- ・ 隠し共有へのバックアップ
- ・ 外付けUSBHDDへのバックアップはリスクが高い



NEW

Veritas Desktop and Laptop Option 9.0

クライアントの数に左右されない専用ソリューションを

- 中～大規模クライアントバックアップにおける課題
 - 管理が煩雑になりやすい
 - 膨大な数のクライアントに対する設定が困難
 - 外出先でのバックアップ
 - 生産性を維持しつつ、確実にバックアップ



あらゆる環境、ニーズに対応する
拡張性と機能性を併せ持った
専用ソリューション

Veritas Desktop and Laptop Option (DLO) 9.0

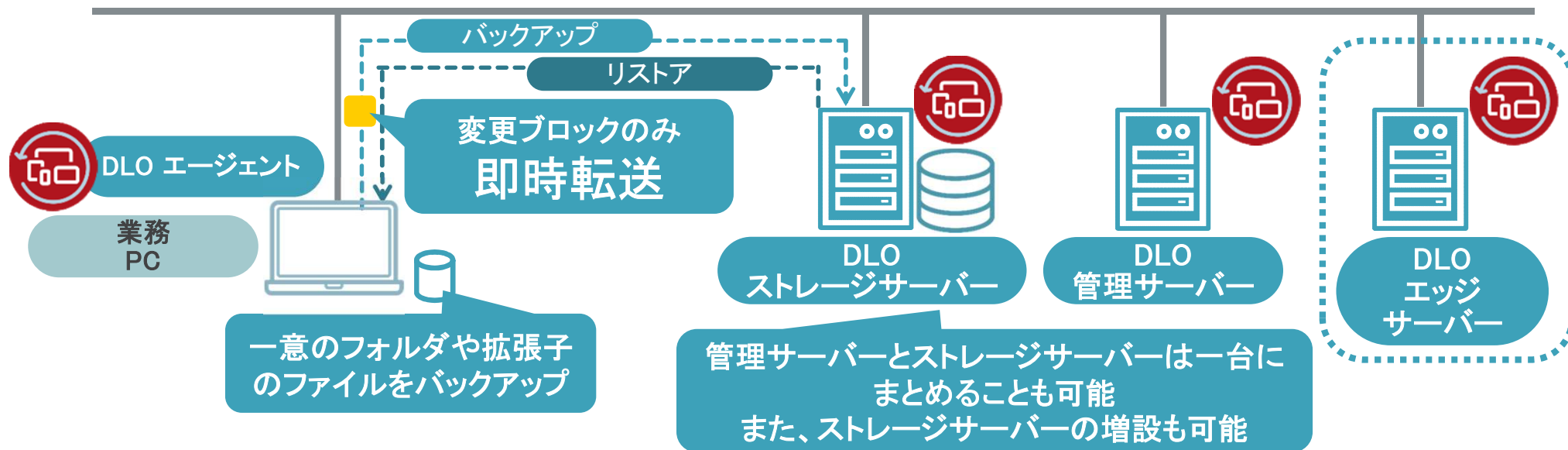


Desktop and
Laptop Option

中～大規模クライアント



データ



Veritas DLOの主な機能



Desktop and
Laptop Option

- ✓ 一台の管理サーバーで100,000台まで対応可能
- ✓ 設定はActive Directoryと連携
- ✓ 機密情報向を有するクライアントに有効なVIPプロファイル
- ✓ ファイルの保存時に即座にバックアップ
- ✓ バックアップは差分ブロック転送/保持により回線負荷とストレージコストを低減
- ✓ Outlookを利用している場合、.pstファイルの増分バックアップ
- ✓ 必要に応じてユーザー自身によるバックアップ / リストアの実行が可能
- ✓ 緊急時にはモバイルデバイスからバックアップデータの参照が可能

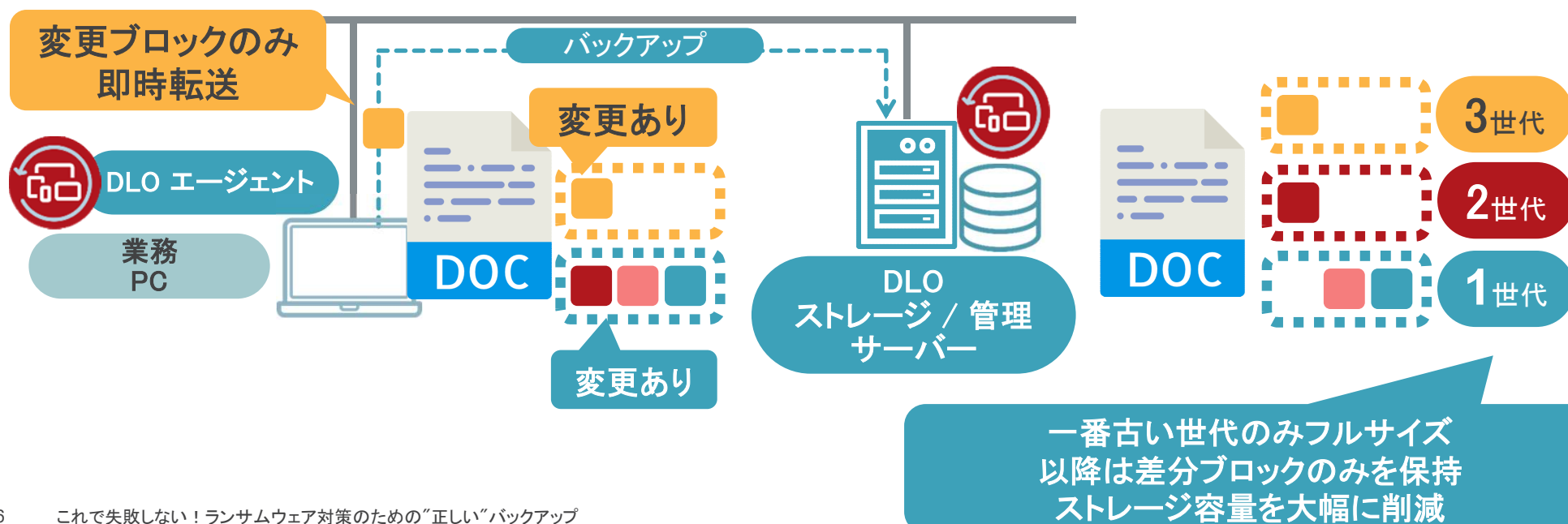
Veritas DLOの特長



Desktop and
Laptop Option

差分ブロック転送 / 保持

～ネットワーク負荷とストレージコストを最小限に

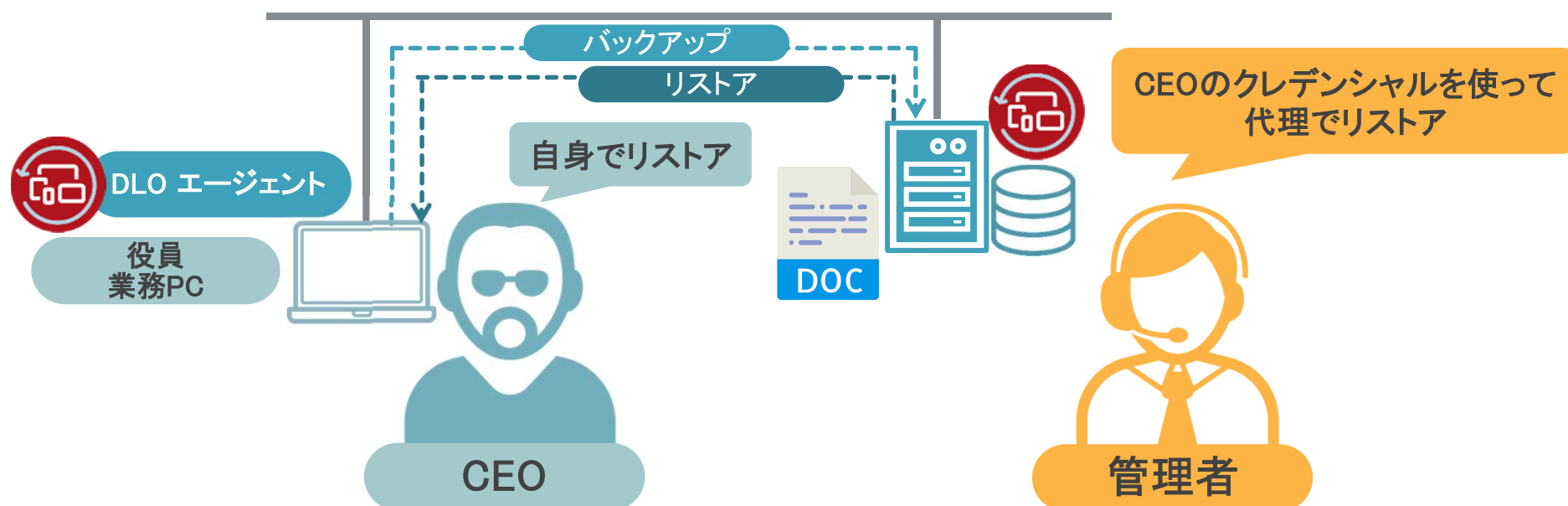


Veritas DLOの特長



Desktop and
Laptop Option

VIPプロフィール機能 ～機密情報の不用意な拡散を防止



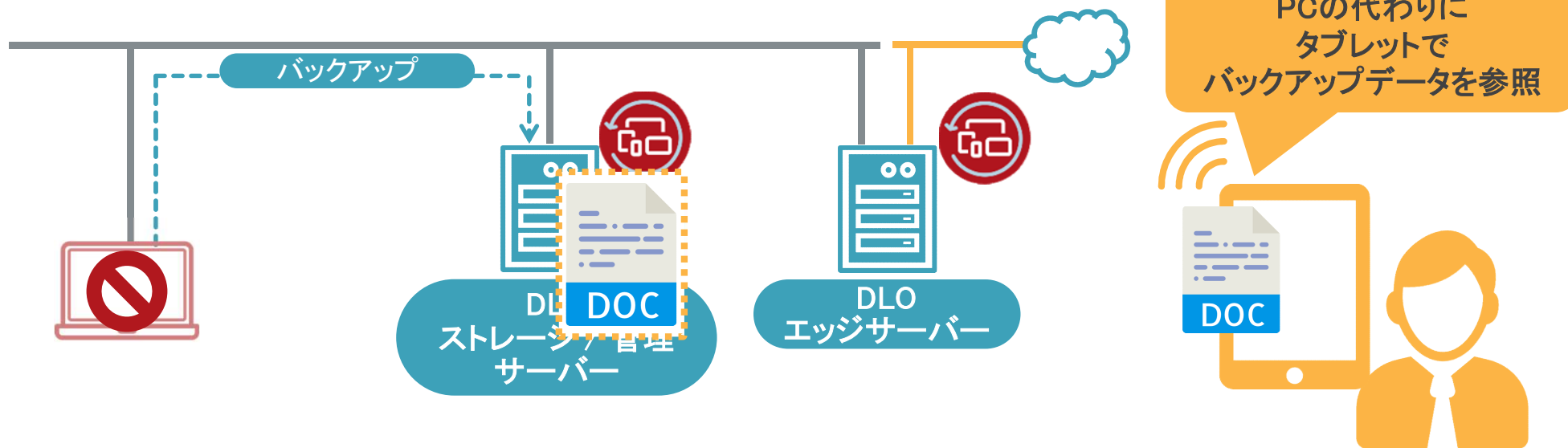
Veritas DLOの特長



Desktop and
Laptop Option

モバイルデバイス活用

～緊急時の対応から生産性の向上まで

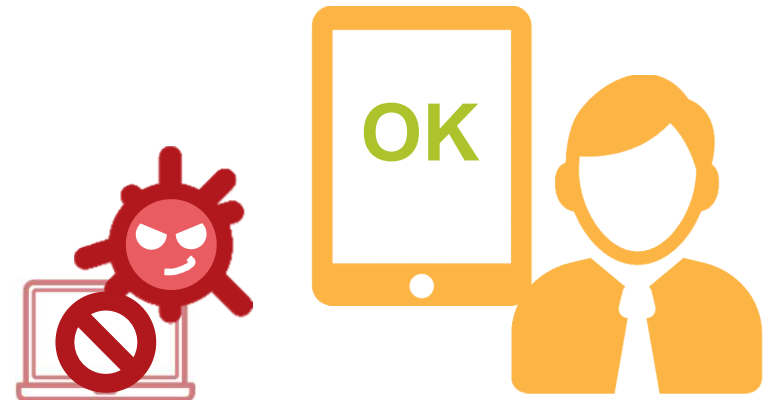


ランサムウェア対策に Veritas DLOを使う場合のポイント

- クライアント上の機密情報は
VIPプロフィールを適用し
コンプライアンスを遵守



- 急な障害に対応するため、代替機か
モバイルデバイスの活用
を検討する



Veritas DLO



Desktop and
Laptop Option



機能性



- ・ 変更即時バックアップ
- ・ ブロック転送 / 保持
- ・ モバイルデバイスでの代替運用



運用管理



- ・ Active Directoryと連携して一括管理
- ・ 大規模環境にも耐えうる拡張性能



応答性



- ・ ユーザー / 管理者共に設定が可能
- ・ 機密情報はVIPポリシーで保護



セキュア



- ・ クライアント - サーバー型で安心の構成

クライアント向け各製品の特長まとめ



機能性



運用管理



応答性



セキュア



Desktop and
Laptop Option



System
Recovery



まとめ

□ランサムウェア対策には
“復旧”のためのセキュリティソリューションとして
バックアップ

□まずは
バックアップの棚卸し
をして
欠けている部分が無いのか
洗い出す

□サーバーは
より高速で堅実、セキュアな
運用を

□クライアントは
ユーザーと管理者双方の細かなニーズに対応出来る
多機能で小回りの利く
確実な運用を

各製品の詳細は 是非展示ブースへどうぞ！

サーバー



NetBackup



Backup Exec



System
Recovery

クライアント



Desktop and
Laptop Option



System
Recovery

VERITASTM

各種製品を利用して
安心して仕事ができる環境の構築を！

サーバー



NetBackup



Backup Exec



System
Recovery

クライアント



Desktop and
Laptop Option



System
Recovery



Information is EVERYTHING

ありがとうございました!

© 2017 Veritas Technologies LLC. All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.