IBM **Storage**

ランサムウェア攻撃への最後の砦

バックアップでデータを守る

対策ソリューション
IBM Spectrum Protect
IBM Spectrum Protect Plus

目次

© 2020 IBM Corporation

データ保護に求められる課題と脅威
Data Protection & Cyber Security challenges

10x

2016~2025 の間の
データ量の増加

68%

バックアップデータの
コピーをリストア以外
にも活用している企業

73%

バックアップや災対先
としてパブリック・
クラウドの利用を
計画している企業

NotPetya による
1 企業あたりの
平均被害金額

$310+ M

206日

ハッカーによる侵入が
発見されるまでに
かかる平均日数

既に問題はサイバー攻撃
被害に遭うか否かではな
い、いつ被害に遭うかだ

Risk

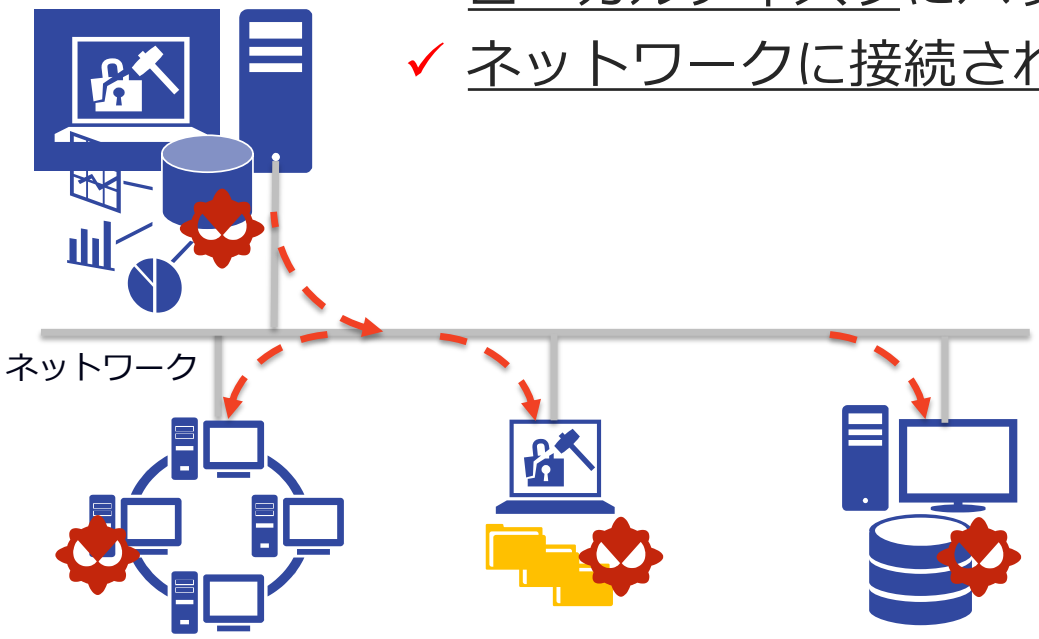
被害に遭う可能性 **#5位**

被害のインパクト **#7位**

World Economic Forum
Global Risks Report 2019

そのバックアップではランサムウェア攻撃でピンチ！

IBM Storage



- ✓ ローカルディスクにバックアップしている
- ✓ ネットワークに接続されたディスクにバックアップしている

この運用でランサムウェアに感染すると

- × 本番ディスクがロックされる
- × バックアップサーバやデータもロックされる

バックアップしていても
リカバリできない

- ✖ サーバー接続のディスク装置
- ✖ CIFS/NAS など、サーバーで認識されているファイルシステム
- ✖ バックアップ管理サーバーやディスク上のバックアップデータ

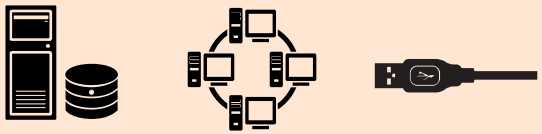
ビジネスに必須のデータを失い、業務再開ができない

ランサムウェア対策の観点で保管先を再点検

IBM **Storage**

高リスク

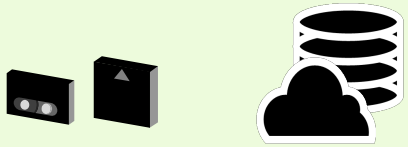
- ネットワーク・ドライブ、ファイル・サーバー
- オンライン状態の DVD、USB HDD、USBメモリ
- オンラインアクセス可能な状態にあるオブジェクトストレージ



低リスク

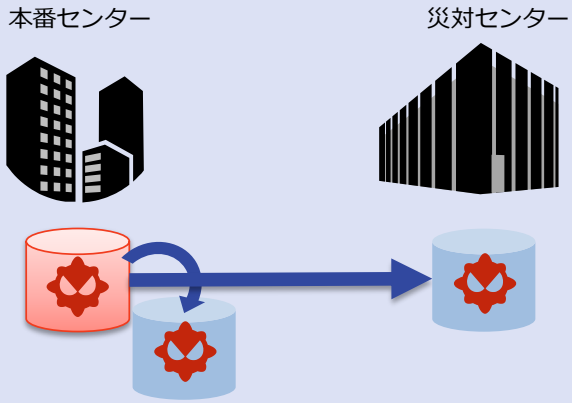
アプリケーションを介してのみアクセス可能な

- テープ装置
- オブジェクト・ストレージ



災対目的のディスク・コピーは安全か？

○	ハードウェア障害（物理破壊）や災害への対策としては有効
×	サーバーからアクセス可能なディスクは感染のリスクがある
×	感染したデータがコピーされる運用は論理障害やウィルス感染のようなデータ破壊に対して有効ではない



破壊されたデータがコピーされるため、論理破壊やウィルス感染には対応できない

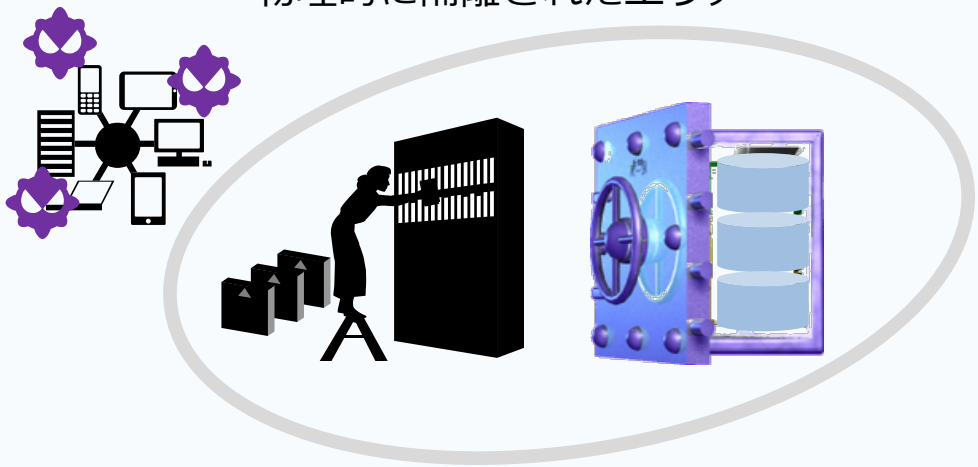
© 2020 IBM Corporation

安全な保管先は「エアギャップ」と「イミュータブル」

IBM **Storage**

エアギャップ (Air Gap)

物理的に隔離されたエリア



- オフラインのテープ
- サーバー・アクセスから完全分離された隔離エリア（DS8000 セーフガードコピー）

Immutable Storage

改変不能（Immutable）な保管先

- Immutable オブジェクト・ストレージ
- Immutable ファイル・システム
- WORM テープ

  WORM: Write Once Read Many

© 2020 IBM Corporation

IBMテープ製品ポートフォリオ

IBM **Storage**

LTO

容量

1PB

500TB

100TB

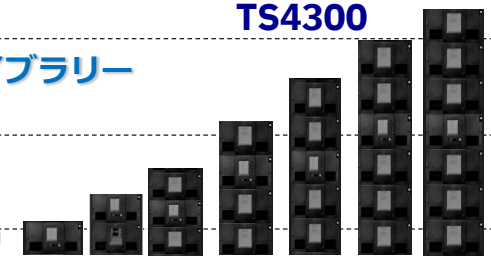
TS4300

LTOドライブ搭載ライブラリー

TS2280
12TB

TS2900

～108 TB



～3.2PB

LTOコンソーシアムで仕様とライセンスが管理されるオープンテクノロジー

転送レート

400 MB/s

300 MB/s

200 MB/s

100 MB/s

LTOドライブ

LTO-5

～1.5 TB/巻
～140 MB/Sec

LTO-6

～2.5 TB/巻
～160 MB/Sec

LTO-7

～6.0TB/巻
～300MB/Sec

LTO-8(*)

～12TB/巻
～360MB/Sec

*LTO-8(HH)は300MB/Sec

Enterprise

TS4500

～351PB

エンタープライズテープ・ドライブ搭載ライブラリー

IBM独自規格。高性能を追求したテープドライブ

エンタープライズテープ・ドライブ

TS1140

～4TB/巻
～250 MB/Sec

TS1150

～10TB/巻
～360 MB/Sec

TS1155

～15TB/巻
～360 MB/Sec

TS1160

～20TB/巻
～400 MB/Sec

※エンタープライズ・ライブラリーはLTOドライブも搭載が可能です。

© 2020 IBM Corporation

IBM Cloud のイミュータブルなオブジェクト・ストレージ

IBM Storage

WORM (Write-Once-Read-Many)

書き込んだデータは
変更/削除不可

IBM Cloud **Object Storage**
Lockable Object Buckets

Validated with

IBM **Spectrum Protect Plus**

COMMVAULT

actifio

NICE

IBM FileNet Content Manager

各種記録保持規制に対応

- 米国証券取引委員会 (SEC) Rule 17a-4(f)
- 米国金融取引業規制機構（FINRA）Rule 4511(c)
- 米国商品先物取引委員会（CFTC）Rule 1.31(c)-(d)

高セキュリティなデータ保護 – 規制対応やランサムウェア対策に

© 2020 IBM Corporation

IBM バックアップソフトのサイバーリジリエンシー機能 IBM Storage

IBM Spectrum Protect（ISP）

- WORM TAPE への保管
- ICOS への保管
- ランサムウェア検知機能

IBM Spectrum Protect Plus（SPP）

- ICOS WORM への保管
- ICOS への保管

バックアップ・データを守る IBM ソリューション

IBM Storage

IBM Spectrum Protect Plus ＋ IBM Cloud Object Storage（WORM）

Lockable Object Buckets

IBM Spectrum Protect ＋ IBM Cloud Object Storage

または

IBM Tape (WORM)

IBM Spectrum Protect ウィルス検知機能

※ウィルス自体の検知、侵入検知機能ではありません

© 2020 IBM Corporation

IBM **Storage**

Spectrum Protect Plus による対策

ICOS WORM へのデータ保管

© 2020 IBM Corporation

仮想環境とクラウドのバックアップは「Spectrum Protect Plus」 IBM Storage

Spectrum Protect Plus の特長

1

簡単導入・管理者負担の軽減

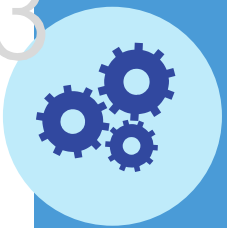
- 15分で導入、 1 時間で運用開始
- 日本語GUI、操作ナビゲーション
- エージェントレス・バックアップ

2

高速バックアップ／リストア

- 永久増分、重複排除、圧縮
- インスタント・リストア
- テスト・モード

3



アプリケーション対応

- Oracle
- SQL Server
- MongoDB
- Db2
- Exchange
- Office 365

4

クラウド

- VMware on IBM Cloud
- VMware Cloud on AWS
- AWS EC2 バックアップ
- コンテナデータのバックアップ

5

災対・サイバーリジリエンシー

- オブジェクトストレージのアーカイブティア対応 (ICOS Archive 他)
- ICOS WORM Verified

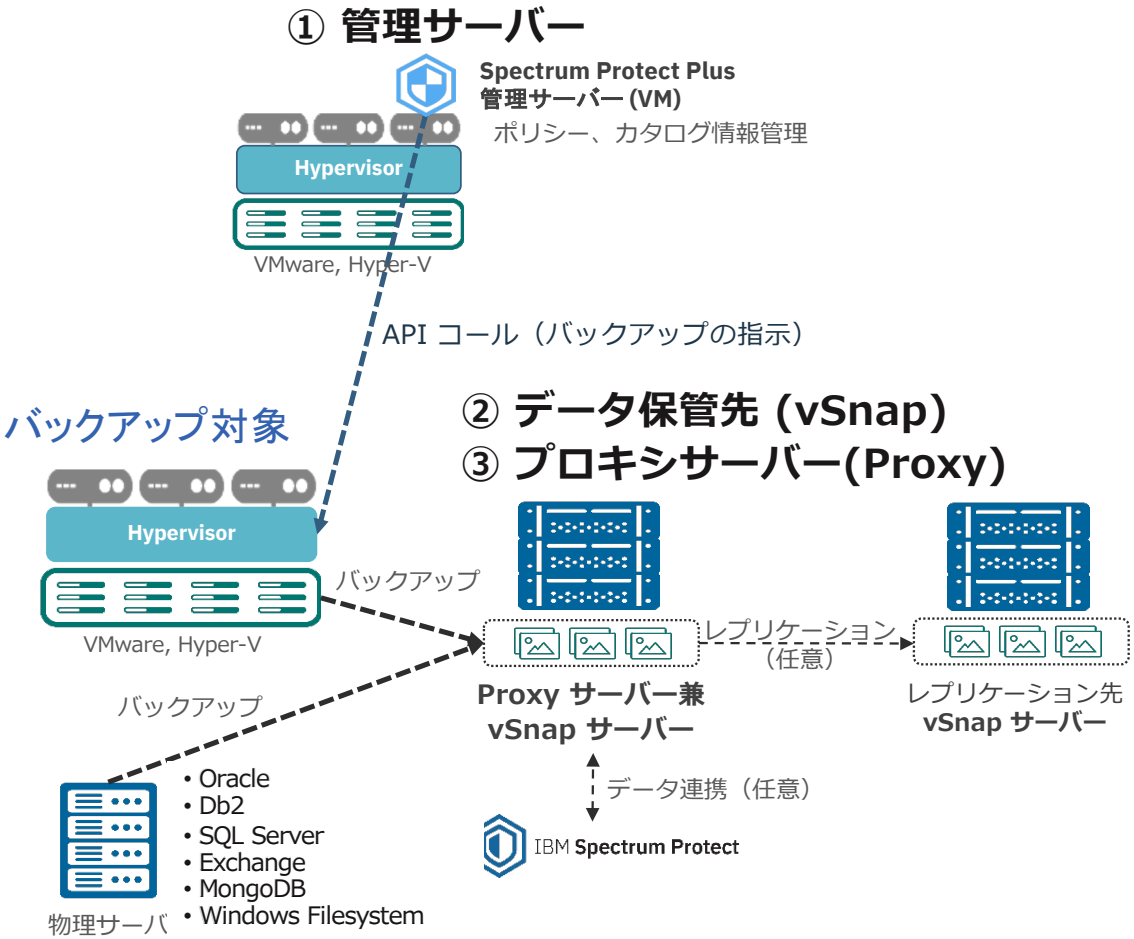
6

データ活用

- クローン機能による容易なVM複製
- ロールベース・アクセス制御（RBAC）による他部門のデータ利用

© 2020 IBM Corporation

Spectrum Protect Plus の構成



① 管理サーバー（必須構成）

- 管理インターフェース
- ポリシーやカタログ情報（メタデータ）を保管
- １環境に１台
- 仮想サーバーのみ

② vSnap サーバー（任意構成）

- バックアップデータの保管先
- vSnap 間のレプリケーションの実行
- 複数台可
- 仮想・物理サーバーいずれも可

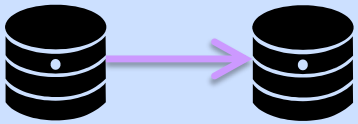
③ プロキシ・サーバー（任意構成）

- バックアップ／リストア処理の実行
- vSnap サーバーもしくは管理サーバーと同居可能
- 複数台可
- 仮想・物理サーバーいずれも可

© 2020 IBM Corporation

3つの複製方式：レプリケーション、コピー、アーカイブ

IBM Storage

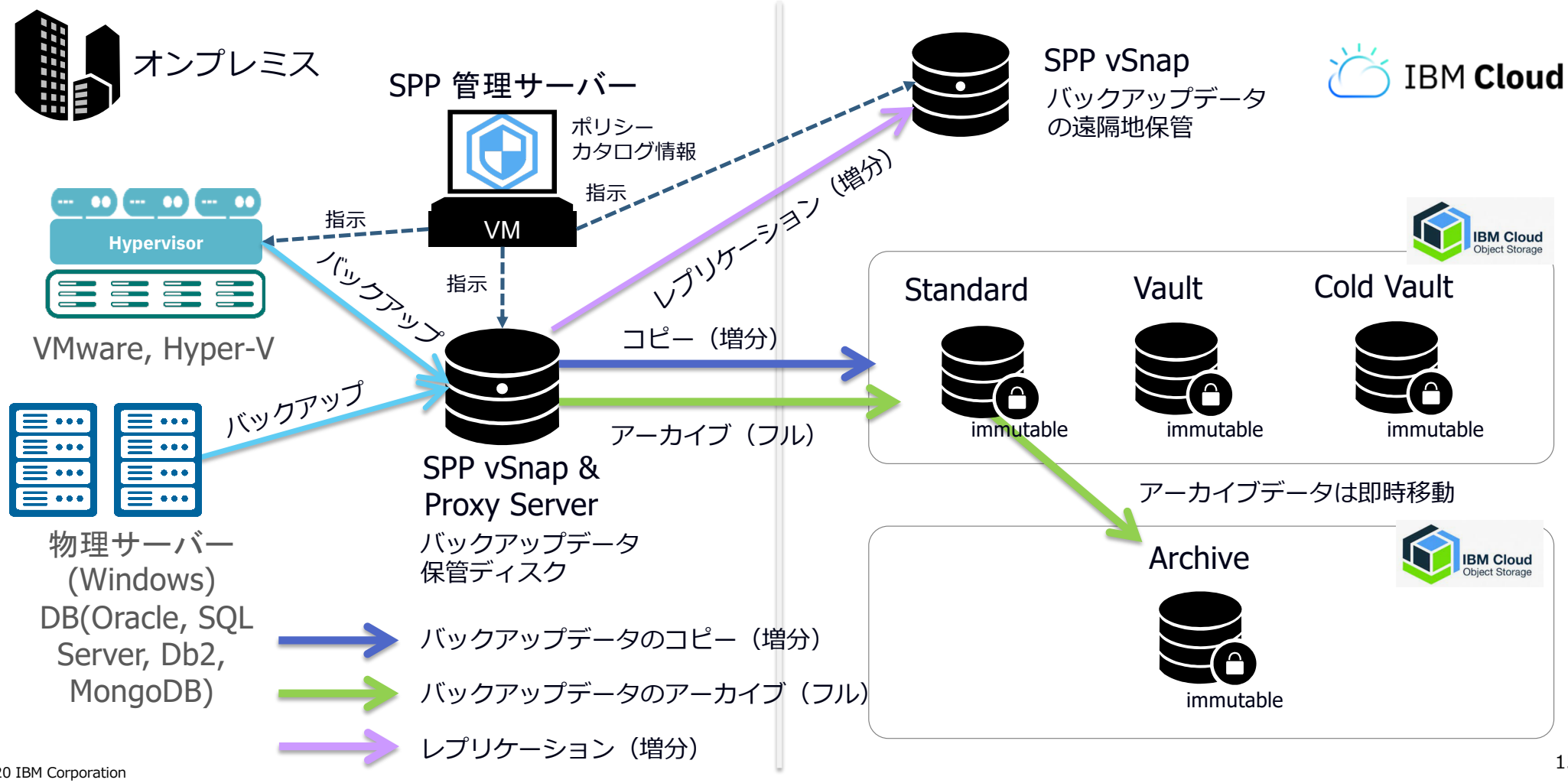
	レプリケーション	コピー	アーカイブ
			
転送先	転送先はDRサイトやクラウド上の SPP vSnap（ディスク）	転送先はオブジェクト・ストレージの標準ストレージ (Standard, Vault, Cold Vault)	転送先はオブジェクトストレージのアーカイブ・ティア (ICOS Archive, AWS Glacier, Microsoft Azure Archive Storage)
転送量	初回はフル、以降は変更データのみ転送	初回はフル、 以降は変更データのみ転送 圧縮データは圧縮のまま転送	毎回フルデータを転送 圧縮データは圧縮しなおして転送
リストア	転送先 vSnap から直接リストア	オブジェクトストレージから直接リストア（vSnap経由）	オブジェクトストレージから一旦 vSnap にリストア（遅い）
適用先	災害対策	RPO = 日次～週次、**RPO重視**	RPO = 週次～月次、**コスト重視**

© 2020 IBM Corporation

IBM Cloud COS へのコピーとアーカイブ

IBM **Storage**

ローカルのバックアップ・データを災対サイトやクラウドに複製し、ランサムウェア被害に備える

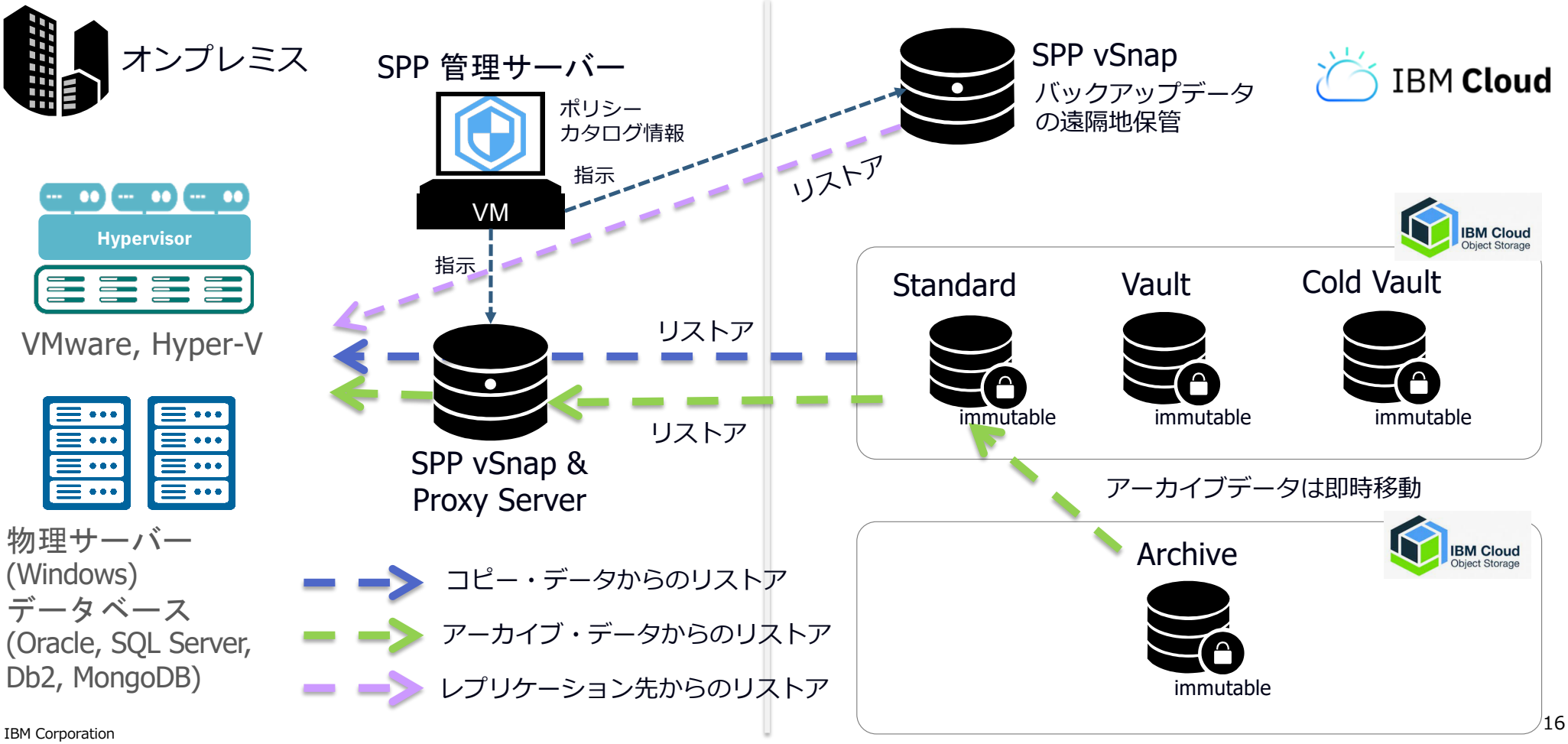


© 2020 IBM Corporation

IBM Cloud COS からのリストア

IBM Storage

ICOS に保管されたデータは vSnap を介してリストア。コピー・データはインスタントマウントで即アクセスも可能。バックアップ時の vSnap を失った場合は別（新規）の vSnap でもリストア可能

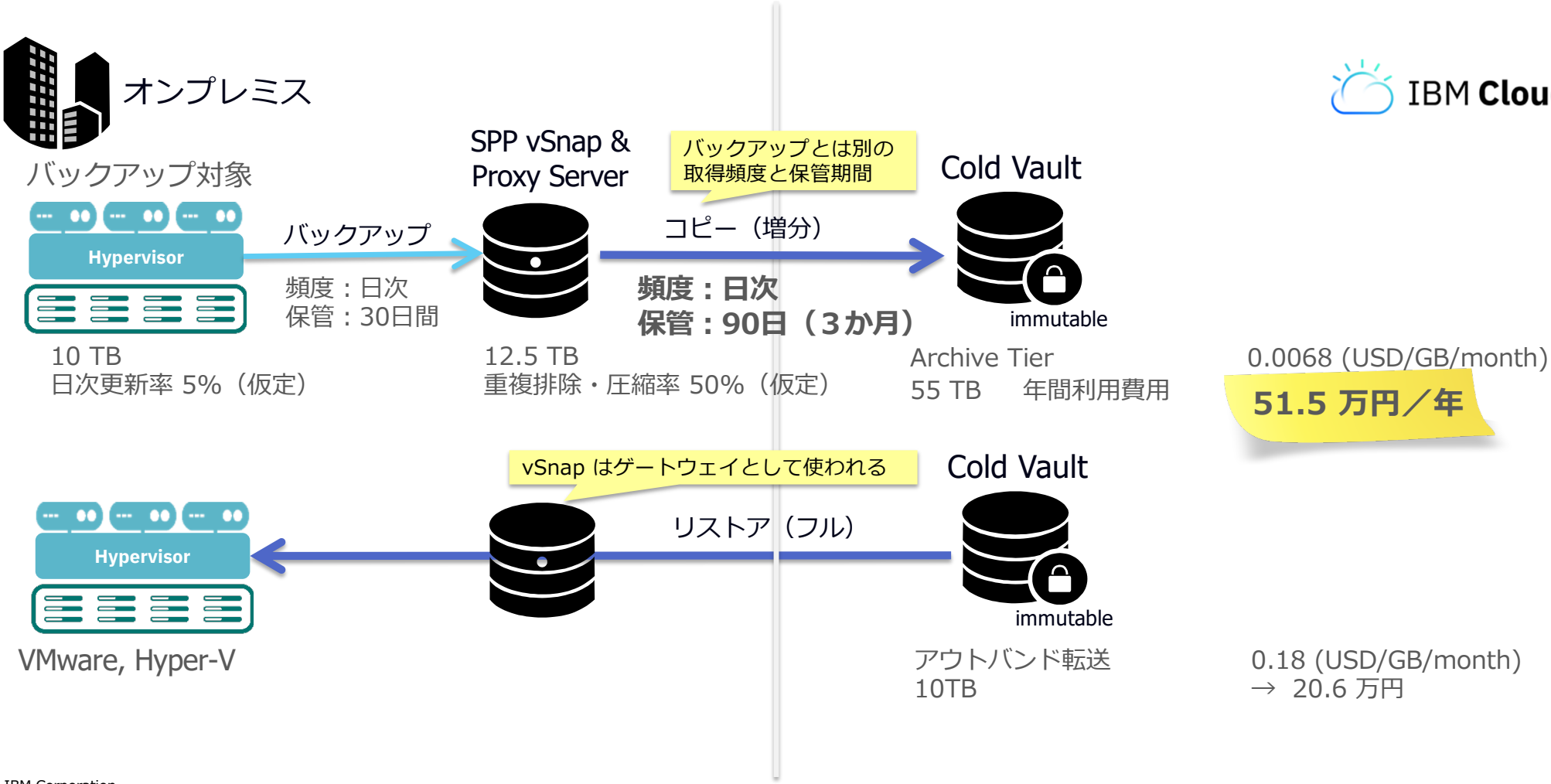


© 2020 IBM Corporation

SPP+ICOS コピー運用（例）

IBM **Storage**

増分データのみを転送するコピーは短めのRPO向き　（例）頻度：日次　90日保管

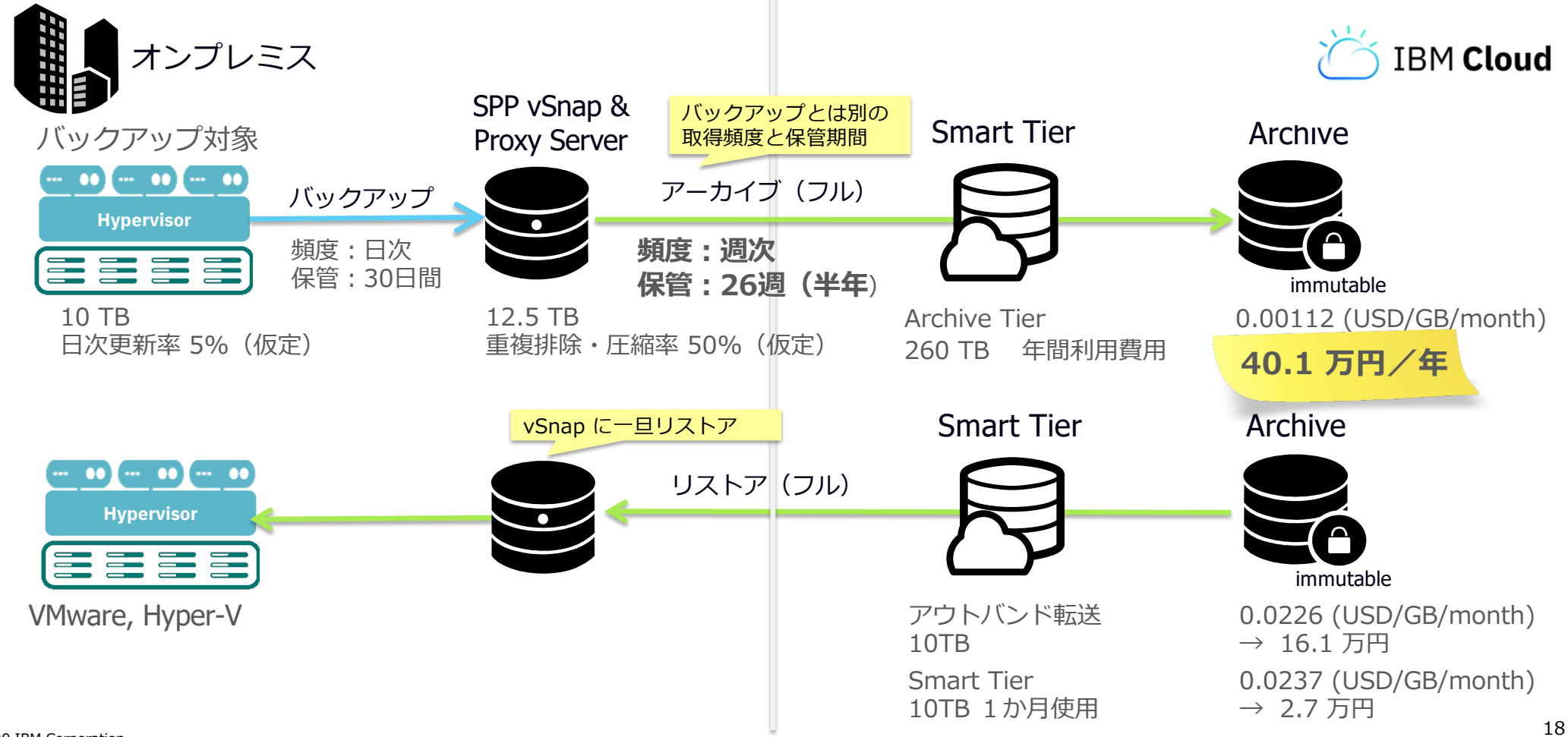


© 2020 IBM Corporation

SPP+ICOS アーカイブ運用（例）

IBM **Storage**

低コストの ICOS Archive に保管するアーカイブは長期保管向き　（例）頻度：週次　半年保管



© 2020 IBM Corporation

IBM **Storage**

Spectrum Protect による対策

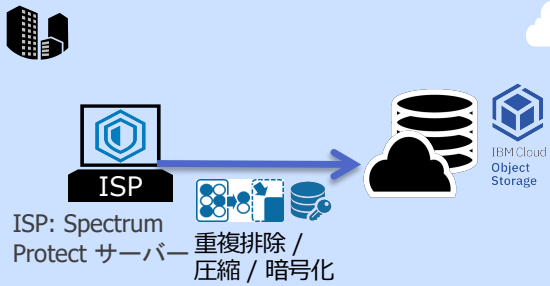
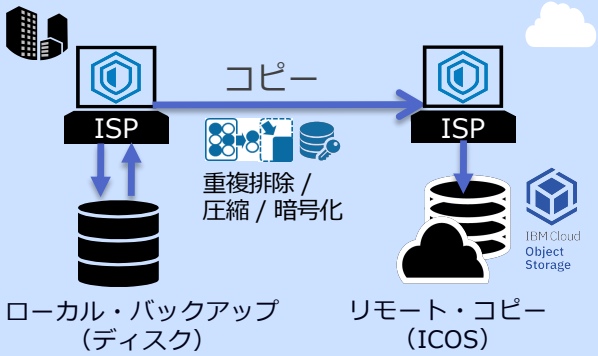
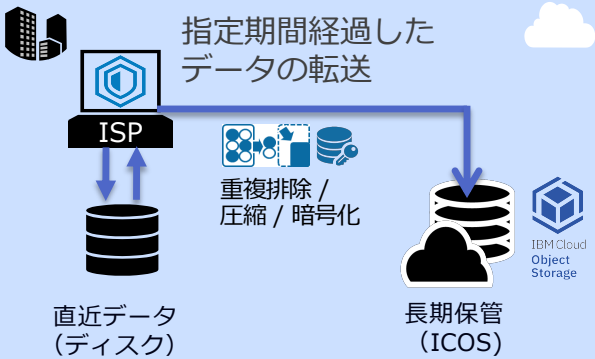
ICOS/テープ保管とランサムウェア検知機能

© 2020 IBM Corporation

バックアップデータの ICOS、テープへの保管方法

IBM **Storage**

図はICOSですが、保管先がテープの場合も構成は同じ

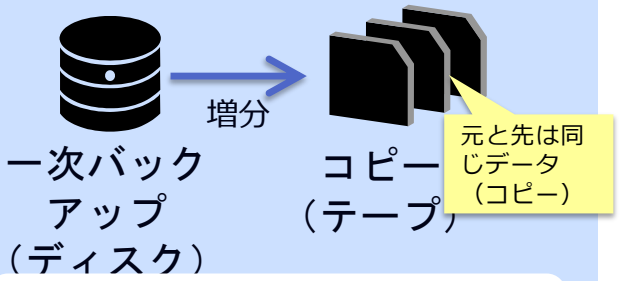
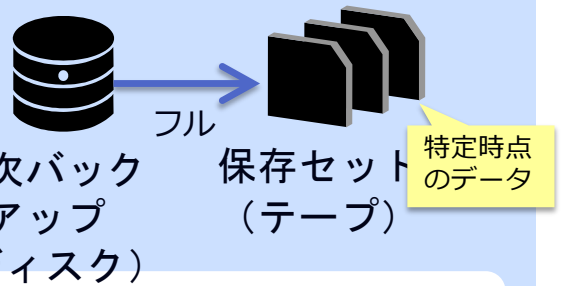
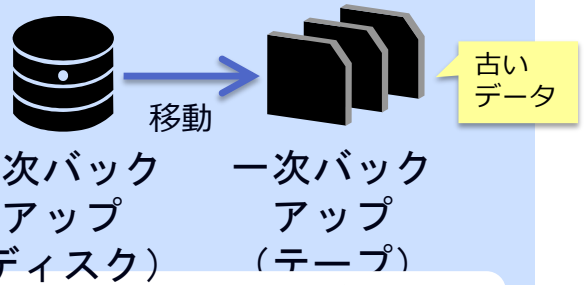
	直接保管	レプリケーション	階層保管
			
データ保管先	ICOS：バックアップデータ	ディスク：ローカル・バックアップ ICOS：バックアップのコピー	ディスク：直近データのみ ICOS：指定した期間経過後のデータ
所要時間	バックアップ、リストアともにネットワーク速度に依存	バックアップ、リストアともにローカル・ディスクからのため速い	バックアップ、リストアともに直近データはローカル・ディスクからのため速い
利用目的	クラウド活用や**ランサムウェア対策**	**災害対策**や**ランサムウェア対策**	**長期保管のコスト削減**
考慮点	• リストア時間は回線依存のため、リカバリ目標時間（RTO）が厳しくないケース向き。	• リモート側のバックアップサーバーの構築・管理コスト	• オンプレ被災時に直近データが失われる

© 2020 IBM Corporation

ディスク・バックアップをテープにコピーする

IBM **Storage**

ディスク・バックアップにテープ・バックアップを追加すれば両者のメリットを享受できる

	コピー（多重化）	保存セット	アーカイブ（階層化）
			
コピー単位	バックアップ・データをストレージプール※単位でコピー	バックアップ・データから指定した特定時点のデータをコピー	指定した期間経過後にバックアップ・データをテープに移動
コピー容量	初回以降は変更データのみ（増分）をコピー	フル・バックアップのコピー	直近のデータはディスクから素早くリストア
リストア	バックアップを取得したどの時点からもリストア可能	保存セット取得時に指定した特定時点でのリストア可能	データ移動を意識することなくどの時点からもリストア可能
効果	災害やランサムウェアなどからの**データ保護**	災害やランサムウェアなどからの**データ保護や長期保存**	低コストのテープによるデータ保管**コストの削減**

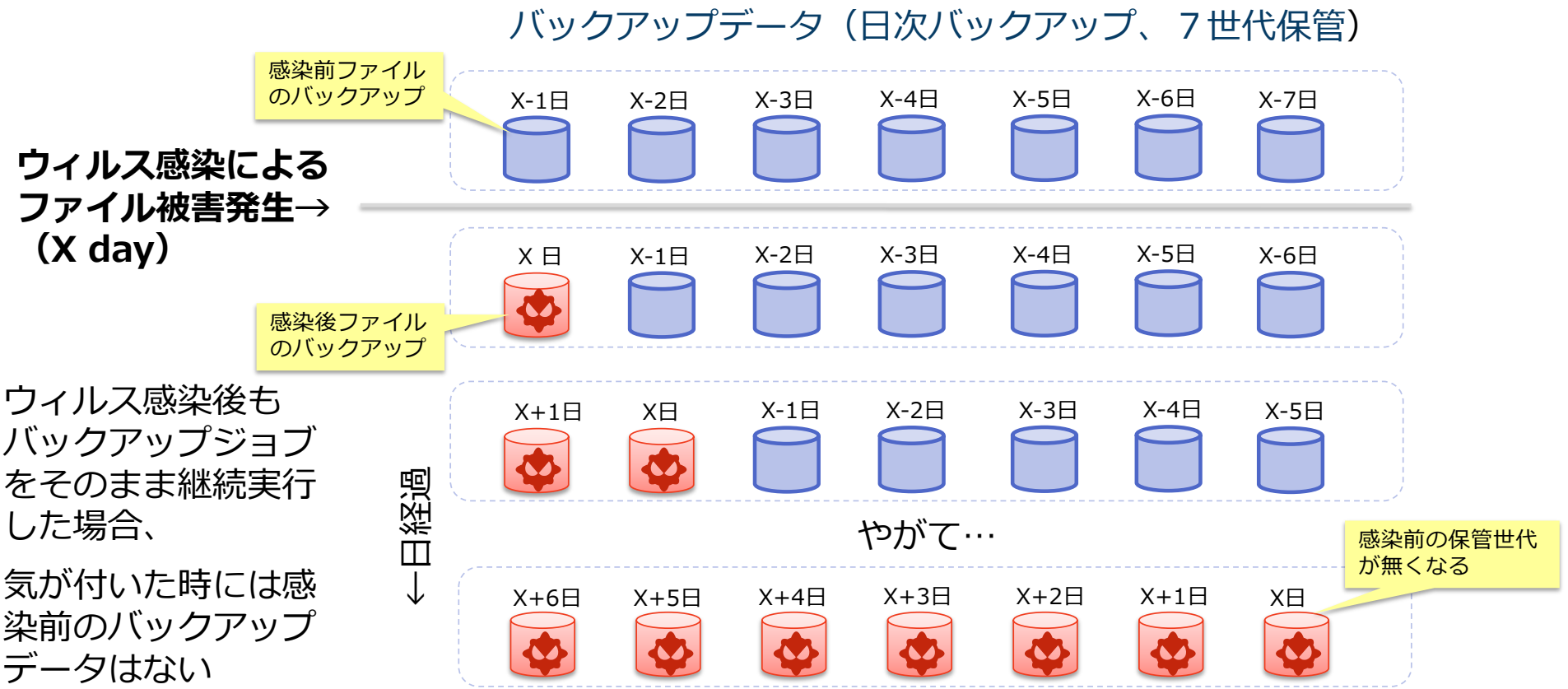
© 2020 IBM Corporation

※ストレージプール：ISP保管データの論理グループ

早期検知の重要性

IBM **Storage**

ウィルスが広がるだけでなく、感染前のバックアップを失うリスクも



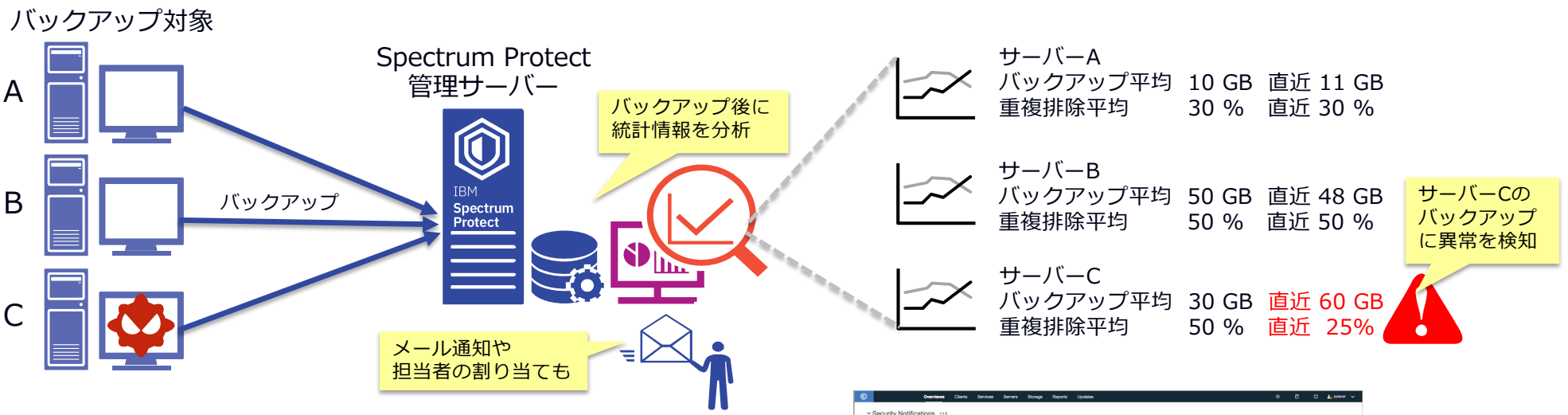
早期に検知することでいち早くデータ保全のアクションが可能

© 2020 IBM Corporation

Spectrum Protect の検知機能

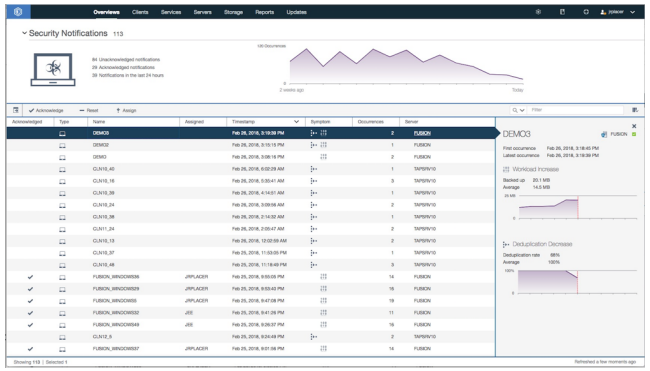
IBM Spectrum Protect　IBM Storage

バックアップ状況をモニターし、統計情報をもとに感染時の異常を検知



ランサムウェアの活動により起こされる対象データの変化を、Spectrum Protect のもつ統計情報をもとに異常として検知します

- ✓ バックアップしたファイル数の急増
- ✓ バックアップしたデータ量の急増
- ✓ 重複排除率の大幅な減少

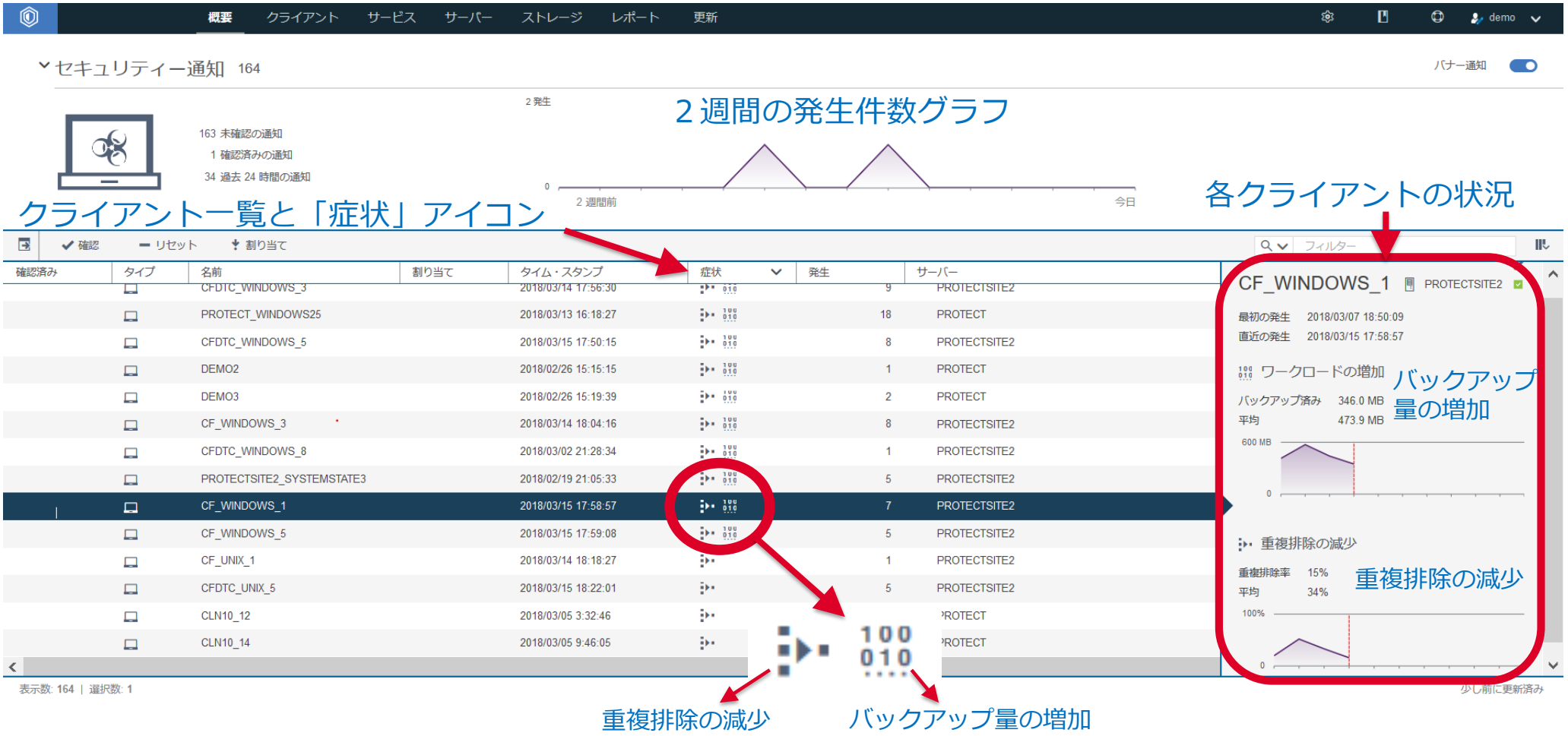


Spectrum Protect のセキュリティ通知画面

© 2020 IBM Corporation

Spectrum Protect 管理 GUI 「セキュリティ通知画面」

IBM Storage



© 2020 IBM Corporation

ランサムウェア感染の検知とアラート

IBM **Storage**

ランサムウェアに感染した可能性があることを検知し、アラート通知

- ランサムウェア感染に伴う事象がないか、
  バックアップ実行後に毎回統計情報を分析
  - 直近 5 回のバックアップの平均より 25% 以上の
    バックアップ・データ量の増加
  - 直近 5 回のバックアップの平均より 25% 以上の
    重複排除率の減少

- 条件に合致した場合、
  - セキュリティ通知画面に警告メッセージを表示
  - 管理 GUI オペレーションズセンター画面に通知ポップアップを表示
  - ログ（actlog）に「ANR3692W」を記録
  - 予め設定した宛先にアラートのメール通知（任意）

統計データを持つ Spectrum Protect だからできる分析と検知

© 2020 IBM Corporation

検知後のアクション

Spectrum Protect 管理者の対応

- 管理GUIの通知と２週間のグラフ表示を確認
- 「確認」で確認済に変更
- 「割り当て」で担当者をアサイン
- 「リセット」でバックアップと重複排除のベースラインをリセット
- オペレーションズセンターの「アラート」画面でアラートを管理

（詳細）セキュリティー通知のモニター

https://demo.tsm.ibmserviceengage.com:11090/help/SSGSG7_OP_CNTR/com.ibm.tsm.ui.doc/ic/t_secnote.html

© 2020 IBM Corporation

まとめ

IBM Spectrum Protect Plus ＋ IBM Cloud **Object Storage**（WORM）

Lockable Object Buckets

IBM Spectrum Protect ＋ IBM Cloud **Object Storage**

または

IBM Tape (WORM)

IBM Spectrum Protect ウィルス検知機能

※ウィルス自体の検知、侵入検知機能ではありません

© 2020 IBM Corporation

IBM®

© 2019 IBM Corporation