

逗子市 様

「Jip-Base」障害原因および再発防止策について

2021年1月20日
日本電子計算株式会社

「Jip-Base」障害原因および再発防止策について

1. 障害の概要
2. 障害分析
3. 再発防止策
(補足)

1. 障害の概要

1. 障害の概要

(1) 障害発生日時

2019年12月4日（水） 10:56

(2) 障害発生個所

Jip-Baseを構成する複数のストレージのうち 1 台（DellEMC社製 Unity500）

(3) 影響団体数

53団体（うち、一部事務組合は5団体）

(4) 影響を受けた仮想OS数

1,318 仮想OS

(5) 障害概況

ストレージに搭載されているコントローラのファームウェアバグによりストレージが全面閉塞したことに伴い、該当ストレージ内に配置されていたデータに対して仮想OSからの参照・更新が不能となりました。

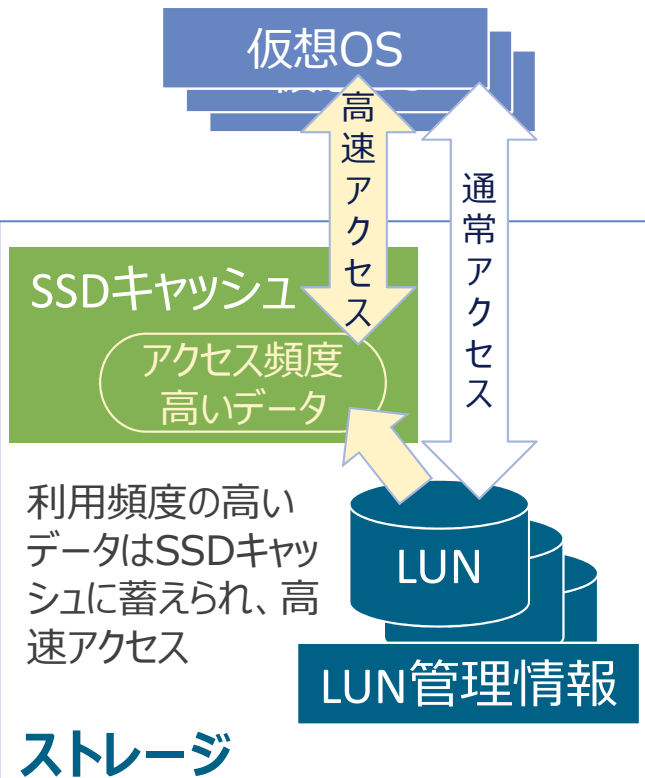
該当ストレージのファームウェアをバグ修正版に更新して、ストレージを機能的に復旧したものの、仮想OSからストレージ内データへのアクセスが正常化しない場合があり仮想OS及び搭載されている業務アプリケーションが利用できない状態となりました。

2. 障害分析

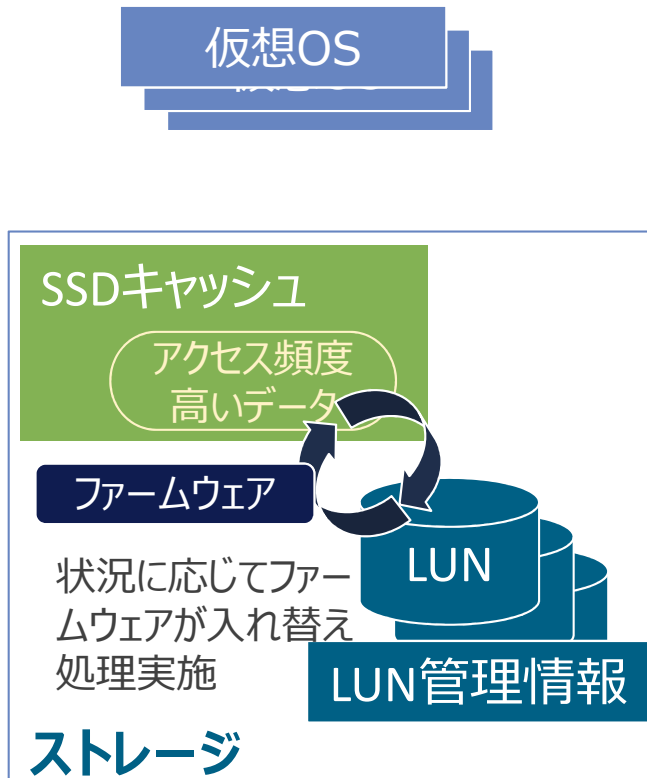
2. 障害分析 (1) 原因 <ファームウェア>

通常処理

1. データアクセス

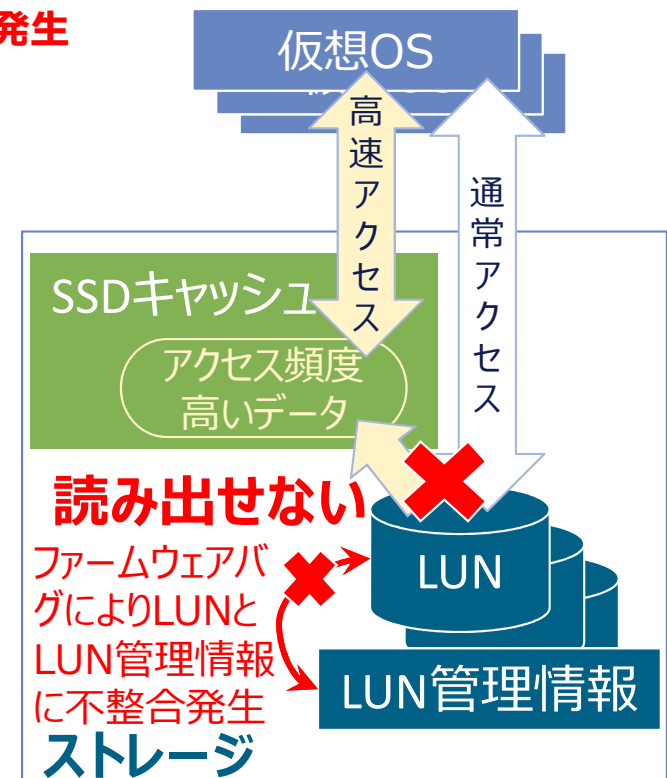


2. SSDキャッシュ入替え処理



障害発生

左記2.SSDキャッシュ入替え処理（ファームウェアの処理）の不具合により下記事象が発生



- ※ 1 SSDキャッシュ：Solid State Drive キャッシュの略。従来のHDDよりも高速に動作するディスク装置であるSSDをストレージキャッシュとして追加することで、高価なメモリキャッシュ増強と類似の効果が得られストレージを高速化できる。
- ※ 2 LUN：Logical Unit Numberの略で、ストレージの中を論理的に分割したものである。LUNでストレージ内を分割することで、大容量ストレージから必要な容量だけ切り出して利用するなど、きめ細やかな管理が可能となる。

問題点

ストレージコントローラのファームウェアバグによるストレージ論理障害

ストレージのファームウェアを更新し、LUNのリカバリ作業を実施後も、一部の仮想OSで正常にログインできないものがあることが確認され、仮想OSの復旧作業が必要となった。

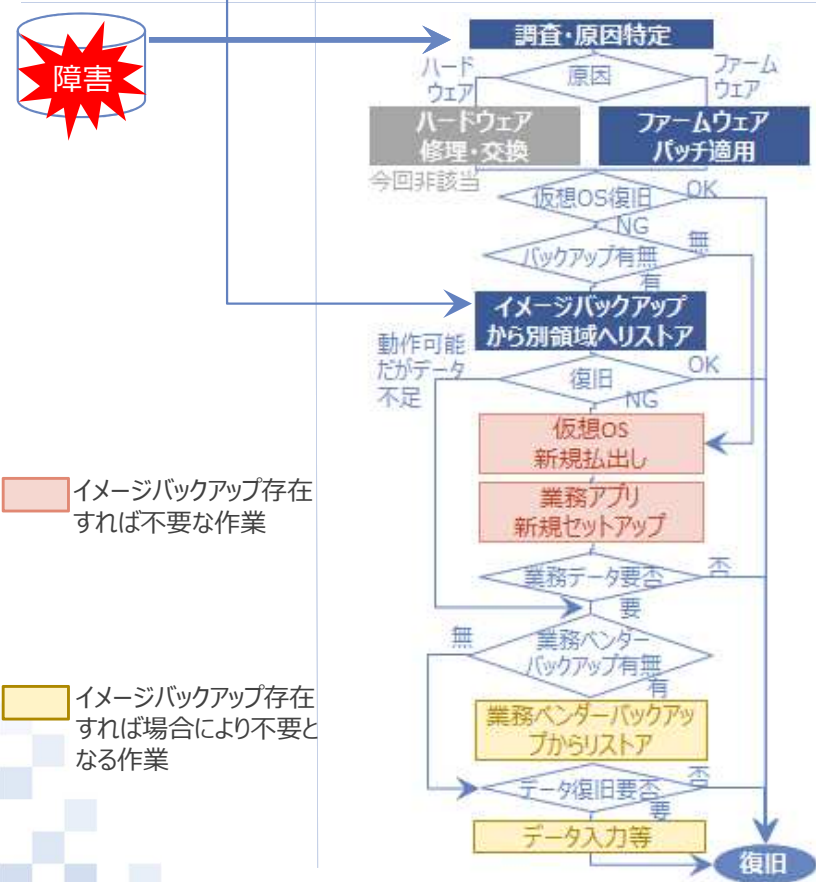
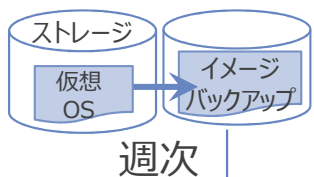
2. 障害分析 (2) 復旧作業

通常運用

復旧作業

説明

問題点



週次でイメージバックアップ取得

※ 一部システムではお客様との契約・要件定義時の合意内容によりバックアップ有無・周期が異なる場合があります。

障害発生後、復旧を最優先に、JIP全社・NTTデータ・ハードベンダー有識者で協議し、復旧方針を決定しながら復旧作業を確実に実施した。

※ 経緯等の詳細については、『(補足)復旧作業詳細』参照

① 一部イメージバックアップが取得できていなかった。

※バックアップ処理の成否に関する検知の運用上の仕組みに問題があり、運用担当者が見逃し

② 多数仮想OS環境の大規模同時論理障害に対する復旧手順が事前に十分検証できていなかった。

当初はストレージ復旧のみで復旧可能と考えていたが、ストレージ内の大規模な論理障害が判明し、膨大なサイズのデータリストアの実施、一部のバックアップデータの取得不備から復旧に多大な時間を要することとなった。

このため、お客様への状況報告・復旧予定報告が迅速にできなかった事態を招いた。

3. 再発防止策

3. 再発防止策（1）ファームウェア①

障害の直接原因であるストレージコントローラのファームウェアバグについては、12/5修正版に更新して解決済であり、再発することはありません。

また、他のストレージ機器についてもファームウェアの横並び点検を行い、重要度・緊急度の高いHP社製ストレージのファームウェアのバージョンアップ版適用を2020/1に実施済です。

問題点	緊急対応策／再発防止策	実施時期
ストレージコントローラのファームウェアバグによるストレージ論理障害	対応策 ・バグの特定と修正版ファームウェア適用 DellEMC本社と連携し、極めて稀なケース（※）であるが、本障害を起因させたバグであることを特定。更新版をインストールして、同事象の再発を抑止	2019/12/5 済
	横並び点検 ・他のストレージ製品ファームウェアの横並び点検 ベンダーへのヒアリングするなど点検を実施。点検の結果、HP社のストレージMSAのファームウェアの適用を実施	2020/1 済

※ グローバルで本件が4件目の発生事例。他の3件は、大規模障害に至らなかった軽微な事象である（DellEMCからの説明）。

3. 再発防止策（1）ファームウェア②

今回の問題で、定期的なファームウェアバグの確認が不十分であったことを認識いたしました。これを解決するため、メーカーとの連携を強化しパッチ適用ルールの見直しを行います。
2020年度からの開始とし、2020年3月中に計画策定を行います。

問題点	緊急対応策／再発防止策	実施時期
<p>ストレージコントローラのファームウェアバグによるストレージ論理障害</p>	<p>2. ファームウェアバグ重要度低い情報のため、ベンダーから更新版適用の情報が提示がなかった</p> <p>3. 他のストレージ製品について、重要度・緊急度の高いバージョンアップがないか、定期的なファームウェアバグの確認頻度が不足</p> <p>4. ファームウェアバージョンアップ版の適用ルールが曖昧</p>	<p>2020年度開始 ↓ <保守・運用> ①2020/4 ②2020/4 ③2020/6</p> <p><方式変更> 2021/2(予定) 2020/10</p>

済
済
済

済

3. 再発防止策（2）復旧作業①

バックアップシステムの点検・改善を実施し、バックアップは取得できていることを確認しています。今後は、新バックアップシステムの構築に向け計画策定を行います。

問題点	緊急対応策／再発防止策	実施時期
一部イメージバックアップが取得できていなかった。	1. バックアップ点検 必要なバックアップを取得し、確実に迅速な復旧作業	
	1.バックアップシステム点検・改善	2020/1 済
	2.バックアップ等監視システム点検・改善	2020/1 済
	3.バックアップ実施状況点検	2020/1 済
	<※詳細 チェック運用方式の改良> ①OSイメージバックアップの取得成否については、バックアップツールのログ管理を自動化し、日次で全件の確認を実施するように強化	
	4.バックアップシステムの構成変更	2020/2 済
	<※詳細 構成変更> ①バックアップサーバを複数のESXサーバとストレージに分散配置し、障害時には別のバックアップサーバからも復元（リストア）作業が可能な構成へ変更	
	5.新バックアップシステム構築 <※詳細 構成変更> ①バックアップ運用再設計・設定変更（管理系サーバの完全独立化） バックアップ管理サーバ、認証系管理サーバ、保守用サーバの完全独立を行い障害時の復旧の障壁とならないように配置します。 ②優先度高いアラートを仕分ける仕組み構築	2020/6 済

3. 再発防止策（2）復旧作業②

管理ルールの再点検、管理者・管理組織増強により管理の強化を図りました。
 今後は、新たな構成管理(※1)・変更管理(※2)方法の整備を進めてまいります。

問題点

緊急対応策／再発防止策

実施時期

- ① 構成管理情報が不足し、影響範囲が特定できない事例があった。
- ② バックアップについて取得対象と対象外を一元的に見える化した資料がなかった。
- ③ 仮想OS環境の大規模同時論理障害に対する復旧手順が事前に十分検証できていなかった。

問題点	緊急対応策／再発防止策	実施時期
<p><注記> ※1 構成管理とは、①Jip-Baseを構成する機器・ファームウェアの型番・保守情報・設定情報の管理および②仮想OSの設定情報管理を指します。</p> <p>※2 変更管理とは、構成管理の情報の変更および更新履歴を管理することを指します。</p>	2. 管理強化 管理ルールの再点検、管理者・管理組織増強により管理強化	
	1. 構成管理・変更管理・見直し メンテナンス作業・障害復旧時確認作業の迅速化・確実性向上	
	1. 構成管理情報再点検	2020/1 済
	2. 構成管理・変更管理ルール再周知	2020/1 済
	2. 新構成管理・変更管理方法の適用	2021/2(予定)
	<※詳細 保守・運用> ① 構成管理・変更管理・リリース管理における一元化の強化 ② ツール見直しによる効率化、管理品質向上	
	3. 組織力強化 管理徹底によるJip-Base安定稼働・障害復旧迅速化	
	1. 管理者増強	2020/1 済
	2. 組織改編・要員追加 構成管理等専任組織新設	2020/1 済
	<※詳細> 「3. 再発防止策（4）再発防止実施体制」に記載	
3. 復旧計画・訓練 事前計画・訓練により障害復旧迅速化		
1. 復旧計画	復旧プロセス・手順を定義、訓練計画策定	2020/3 済
2. 復旧訓練		2021/2(予定)

3. 再発防止策（3）その他＜SLAの見直しについて＞

サービスレベル（障害の内容に応じた障害からの復旧時間、バックアップの取得サイクル、障害の検知までの時間等）について、お客様がご利用の業務システムの重要度に応じたサービス内容説明、SLA締結が出来ておらず、お客様・業務ベンダー様・弊社含めた責任分界点にあいまいさがあり、復旧で必要な作業内容の確認・合意に時間を要するケースがございました。

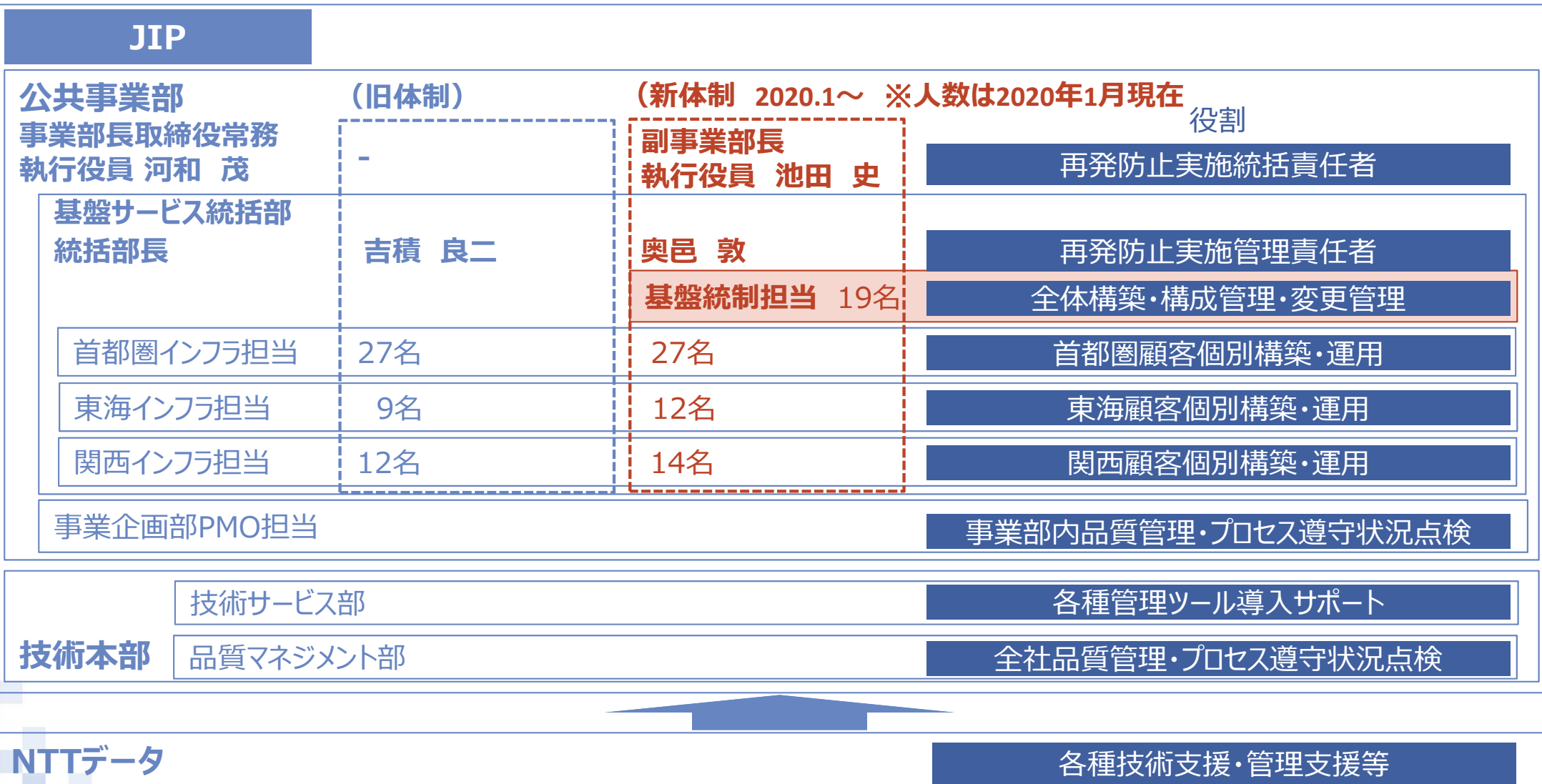
Jip-Base標準のサービスレベルを見直しお客様説明の上、必要に応じてSLA変更・締結を実施します。

緊急対応策／再発防止策		実施時期
1. 要求事項管理	お客様要求事項の再点検・明確化で確実な要求実現	
1. 契約・SLA再点検		2020/1 済
2. SLA締結済お客様の内容確認・再説明		2020/3 済
2. サービスレベル・オプションサービス整理	事前計画・訓練により障害復旧迅速化	
1. 標準SLO・SLAの見直し		2021/1 済
2. SLA未締結のお客様への説明・締結		2021/2(予定)
3. BCP対策オプションメニュー整備	外部データセンターを利用した更なる可用性向上サービス(※)	
1. 計画		2020/3 済
2. 構築		2020/10 済
3. サービス提供開始		2020/10 済

※ 後述の『（補足）BCP対策』参照

3. 再発防止策（４）再発防止実施体制①

Jip-Baseのサービス管理機能ならびに運用体制を強化し、NTTデータグループ一体となって再発防止ならびにシステム・運用改善を図っていきます。



3. 再発防止策（４）再発防止実施体制②

Jip-Baseのサービス管理機能ならびに運用体制を強化し、NTTデータグループ一体となって再発防止ならびにシステム・運用改善を図っていきます。

JIP

公共事業部

再発防止実施統括責任者

副事業部長執行役員 池田 史

公共事業部に新規で1名追加（基盤サービス事業専任）、経営方針・基盤サービス事業方針（再発防止策の履行）に基づき業務を遂行する統括責任者

基盤サービス統括部

再発防止実施管理責任者

基盤サービス統括部長 奥邑 敦

2020.1に統括部長交替、経営方針・基盤サービス事業方針（再発防止策の履行）に基づき業務を遂行する管理責任者

基盤統制担当

基盤共通グループ

全体構築

機器・ミドルウェア等構成の設計・構築、機器・ファームウェア等点検・メンテナンス実施、変更・リリース実施の情報更新

構成管理グループ

構成管理・変更管理

機器・ファームウェア等構成の管理（保守期限情報含む）、稼働状況点検、インシデント記録・管理の全体集約、変更・リリース実施の管理

首都圏インフラ担当

首都圏顧客個別構築・運用

インシデント記録・管理の実施、お客様対応（要件確認、資料作成、報告等）

(補足)

(補足) 復旧作業詳細 (1)

(1) ストレージの復旧作業

ストレージの完全閉塞についてはストレージ内部の障害が疑われたため、障害発生後にDellEMC社に確認したところ、ストレージコントローラのファームウェアのバグが原因であることが判明し、同社と協力して復旧手順を策定、ファームウェアの更新作業、LUNのリカバリ作業を実施しました。

ストレージ障害のメカニズムの詳細が判明していない段階においては、ストレージコントローラのファームウェアの更新後にLUNリカバリツールを実行することで正常な状態に復旧できるものと考えていました。

<復旧方針 12/5時点>



しかしながら、2019年12月7日に全てのLUNのリカバリ作業が完了した後、仮想OSに対するログインを行ったところ、正常にログインできない仮想OSがあることが確認されました。

ストレージの復旧のみではサービスの正常化ができないことが判明したため、次に仮想OSの復旧に取りかかりました。

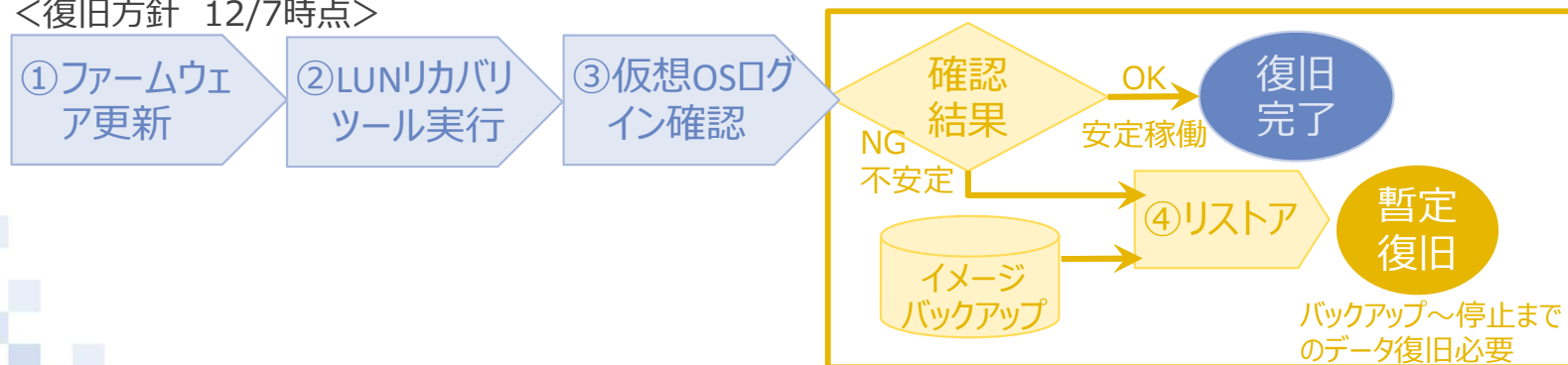
(2) 仮想OSの復旧作業

仮想OSに対して正常にログインできない現象を調査したところ、仮想OSから参照できない領域がストレージ上に複数存在していたことが判明しました。そのため、全仮想OSに対するログイン確認を実施しアクセス可能・不可能の切り分けを実施しました。

アクセス可能な仮想OSの中には動作が不安定と判定されるものも複数存在したことから、これらの仮想OSについては被害拡大を抑止するために、安定稼働している別ストレージへの環境移行作業も行っています。この作業は相応の時間を要しました。

アクセス不可能な仮想OSについては、複数の修復ツールを用いた結果、短期間での修復は困難と判断し、イメージバックアップからのリストアを行う方針としました。

<復旧方針 12/7時点>



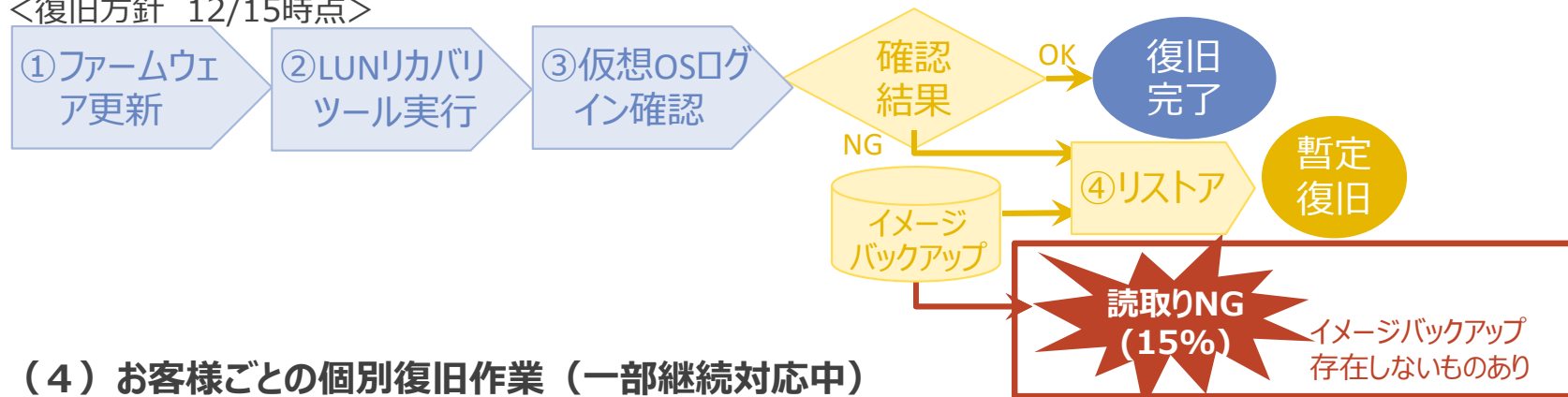
(補足) 復旧作業詳細 (2)

(3) イメージバックアップからのリストア作業

前述の復旧方針に基づき、バックアップストレージ上に保存しているイメージバックアップからリストア作業を実施しました。リストアの対象数が膨大であったこと、対象仮想OSによってはデータ量が数テラバイトに及ぶものがあったこと等の条件もあり24時間体制で対応しましたが、相応の復旧時間を要しました。なお、リストアが完了したものの順次、お客様の確認のもと、サービスを再開させていただきました。

しかし、2019年12月15日時点でイメージバックアップが読み取れないものが仮想OSイメージ全体の15%存在することが明らかになり、その中にはイメージバックアップ自体が存在していないものがあることが判明しました。これらについては仮想OSリストアができないため、復旧方針を見直す必要が生じました。

<復旧方針 12/15時点>

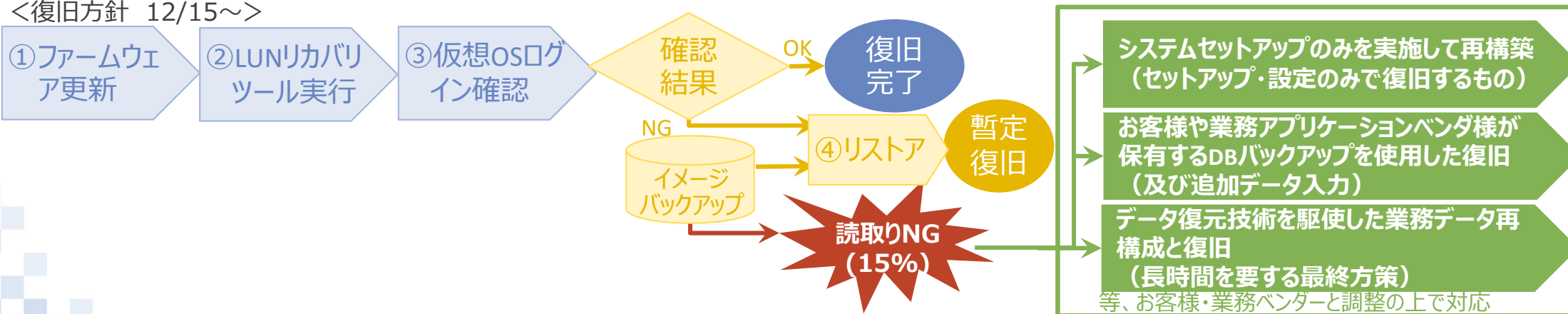


(4) お客様ごとの個別復旧作業 (一部継続対応中)

イメージバックアップが存在しない仮想OSについては、弊社から新規に仮想OSを払い出すことを前提として、個別にお客様、業務アプリケーションベンダ様も含めて復旧水準や復旧手順を協議・策定し、様々な方法で業務システムの復旧作業を実施しています。

なお、本対応にあたっては、弊社が12/19に新規導入したストレージを用いて新規仮想OSの提供を行っています。個別復旧作業の主なケースは以下のとおりです。

<復旧方針 12/15～>



(補足) BCP対策

今回の障害では弊社WizLIFEご利用団体、Jip-Base上に他社が構築された業務システムの一部で、オンプレミス環境等に独自に構築されたバックアップ環境を有する団体がございました。

該当団体では、障害後の一部の業務作業継続、あるいはバックアップ環境の無いシステムと比較し早期の業務作業再開が可能であったことから、下記についてJip-Baseの有償追加オプションサービスとしての構築を計画・実施します。

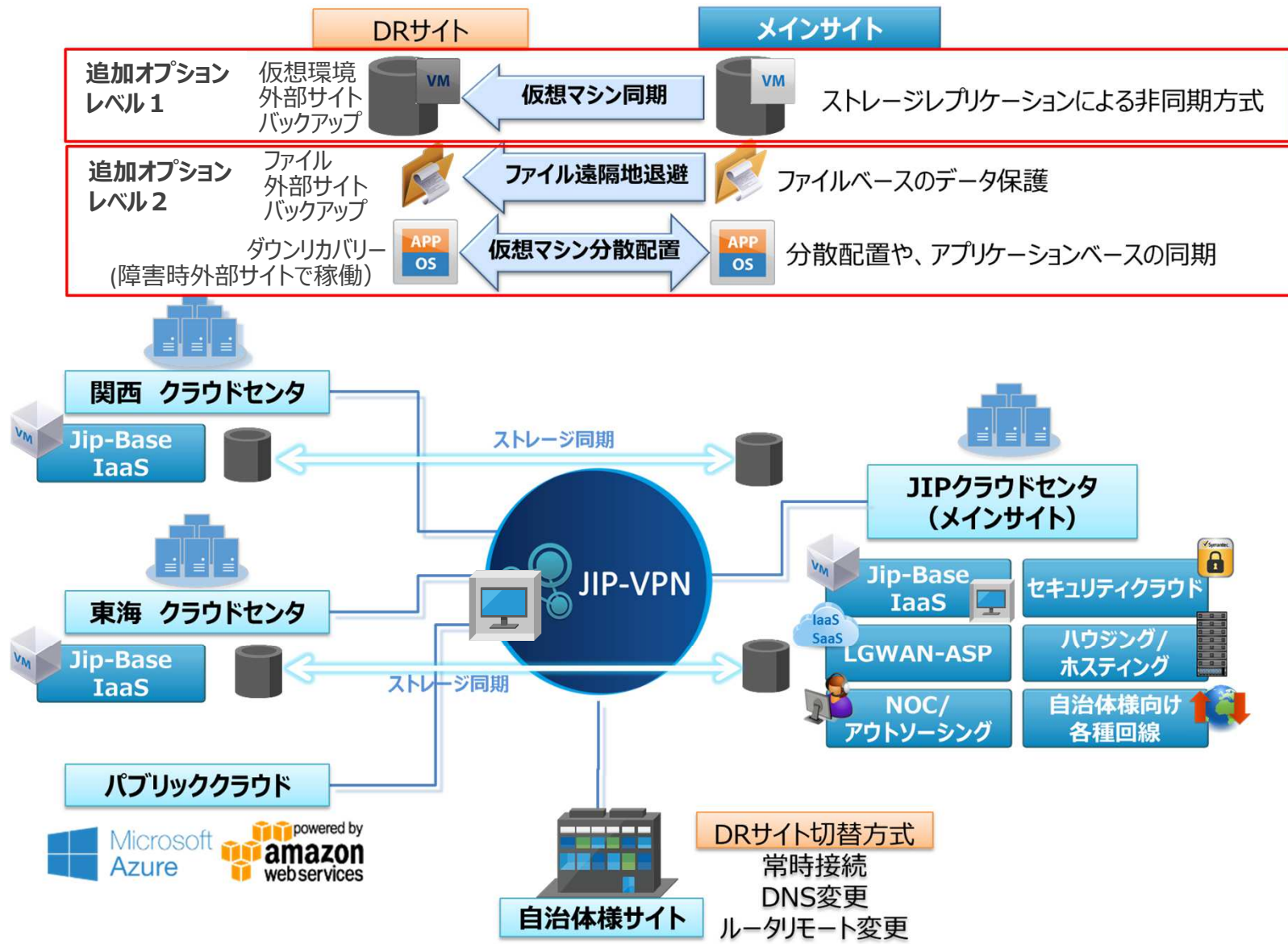
施策	詳細・期待される効果等
追加オプションとして、外部データセンターを利用した可用性向上サービス提供	多重障害・論理障害に備えた、外部データセンターを活用した提案メニューを準備し、上位レベルの非機能要求に対応した可用性を実現する。 仮想環境バックアップの外部保管等を実施。 (また、IaaSサービスJip-Base + 総合行政システムWizLIFE提供のお客様向けには、JLISのBCP対策(※)の活用も検討していきます。)


※ 総務省／自治体システム等標準化検討会第1回検討会資料


『自治体システム等標準化検討会（第1回）事務局提出資料（標準化についてのこれまでの議論等）令和元年（2019年）8月 総務省自治行政局』
P.11～12 J-LIS「小規模市町村向けコンビニ交付サービス・被災者支援システムのクラウド化の試行」

https://www.soumu.go.jp/main_sosiki/kenkyu/jichitaishisutemu_hyojunka/daikai01.html

(補足) BCP対策<概要 (案)>





 Create Values with Clients by IT
お客様とともに、ITで新たな価値を創造する
日本電子計算株式会社

Trusted Global Innovator

NTT DATA Group