ORACLE

あらためて考えるデータベースのバックアップとリカバリ Oracle Databaseの場合

2023年3月7日

日本オラクル株式会社
日下部明

Safe harbor statement

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することを確約するものではないため、購買決定を行う際の判断材料になさらないで下さい。
オラクル製品に関して記載されている機能の開発、リリース、時期及び価格については、弊社の裁量により決定され、変更される可能性があります。

データベースのデータにアクセスできなくなる

情報セキュリティ3要素

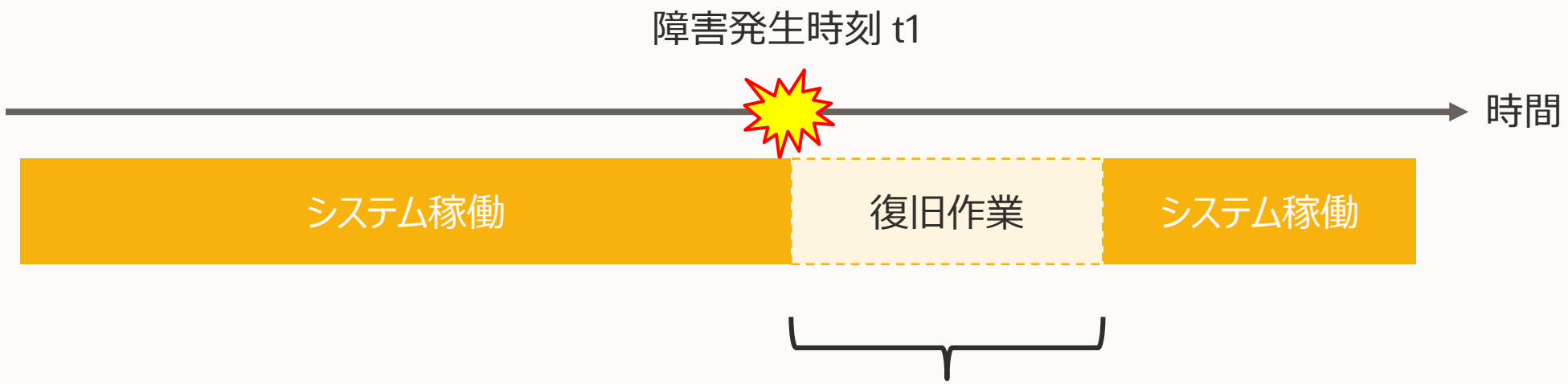
- Confidentiality (機密性)
- Integrity (完全性)
- Availability (可用性)

この時間は「(正しい)データにアクセスできなくなる」というIntegrityとAvailabilityの観点からの話

データへのアクセスに障害が発生したデータベースを復旧させるには？

いつ復旧できるか/いつまでのデータを復旧できるか

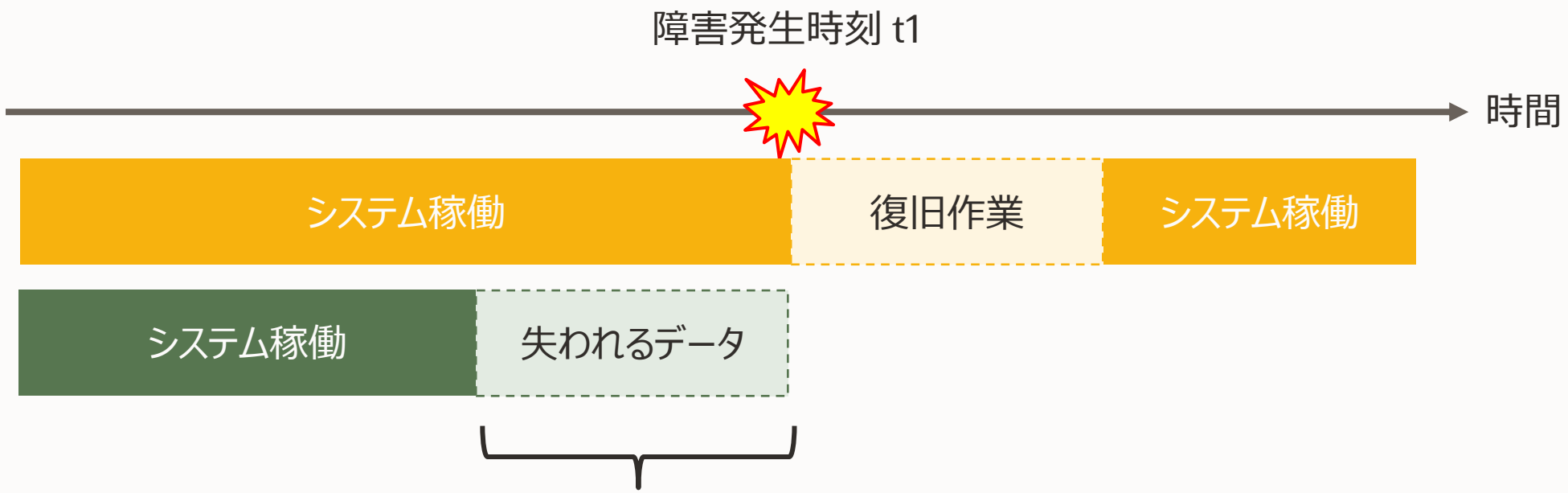
目標復旧時間/目標復旧時点



目標復旧時間 (Recovery Time Objective: RTO)
障害が発生してからどれくらいの時間でシステム稼働を再開できるか

いつ復旧できるか/いつまでのデータを復旧できるか

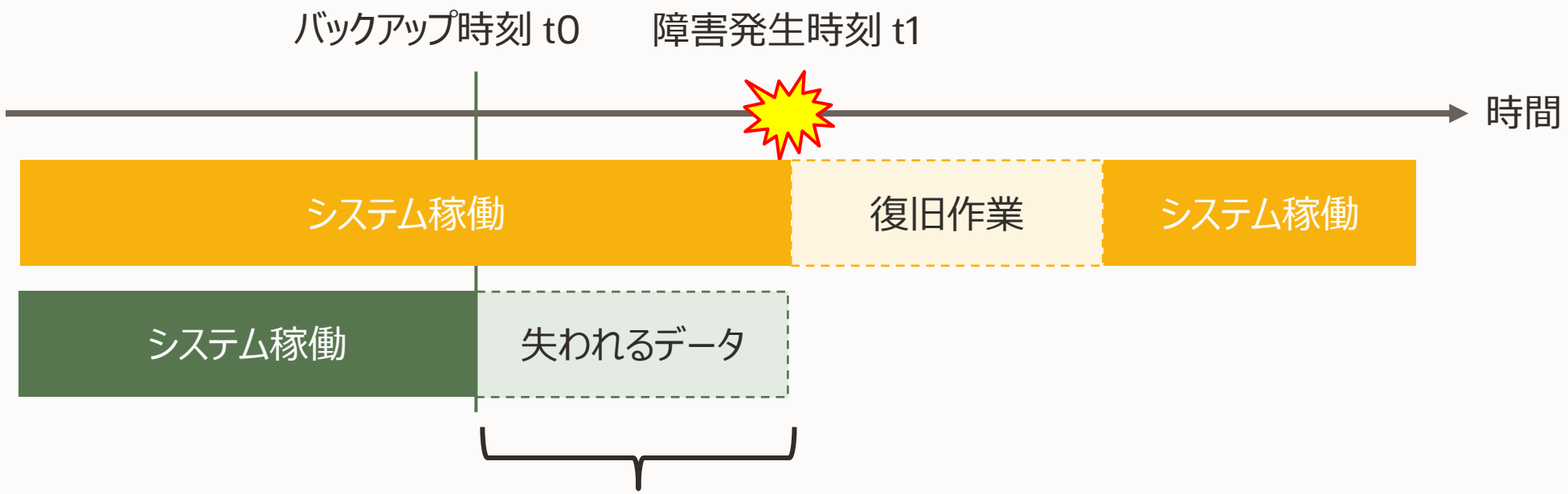
目標復旧時間/目標復旧時点



目標復旧時点 (Recovery Point Objective: RPO)
復旧させたとき障害が発生するまでのどれくらいの時間のデータが失われるか

なぜ失われるデータが発生するか

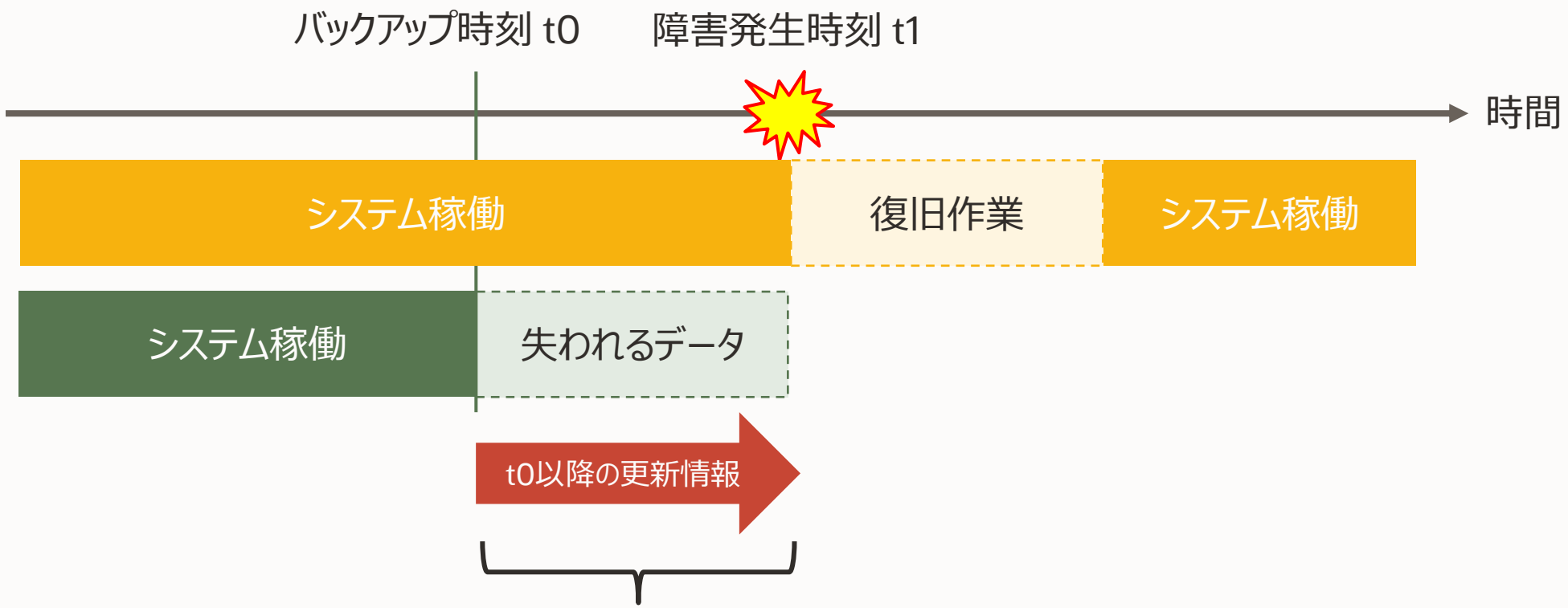
バックアップ操作と目標復旧時点の関係



データの複製が時刻t0までのものしかなければ、時刻t0とt1の間のデータがどこにも存在しない

データベースはストレージに障害が発生することを想定している

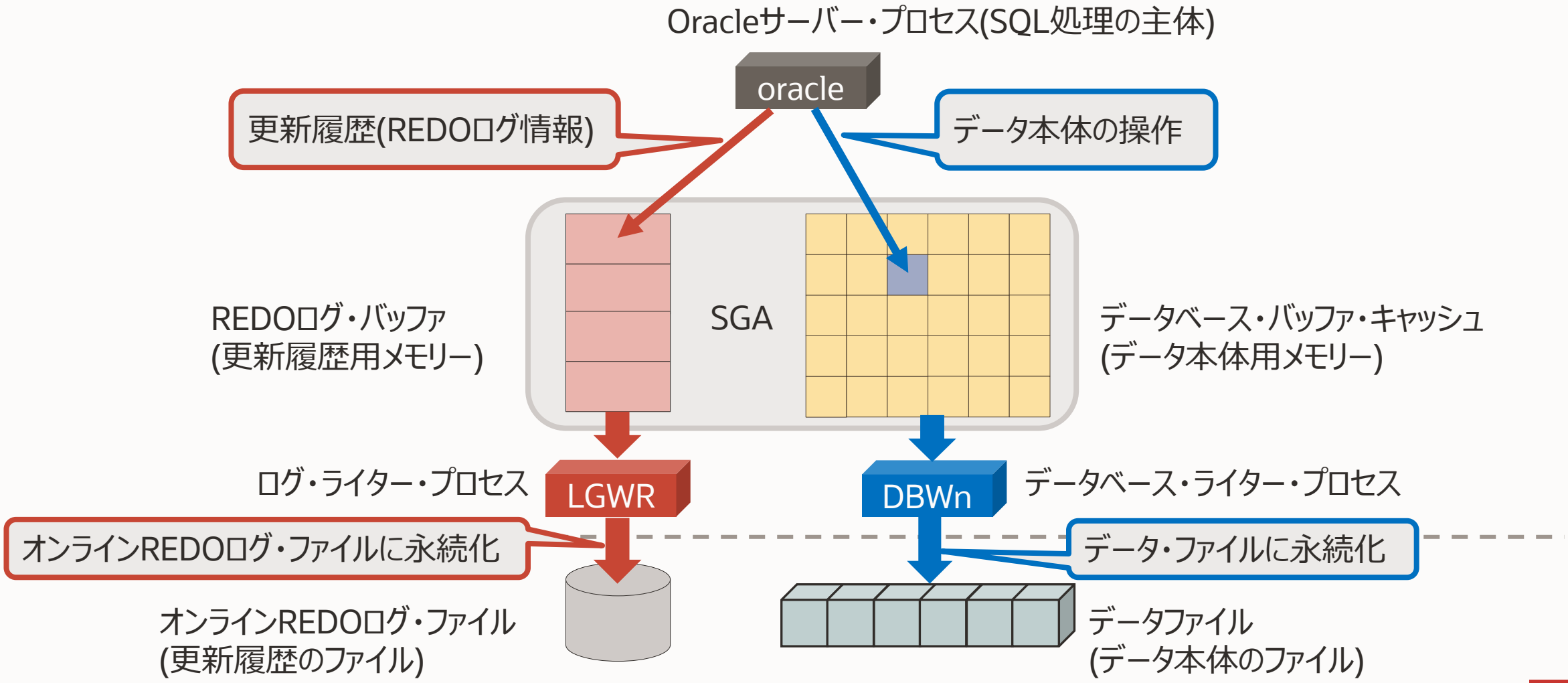
障害発生直前の状態(RPO=0)まで復旧する方法が存在する



データ本体の複製が時刻t0まで + 時刻t0以降の更新履歴情報

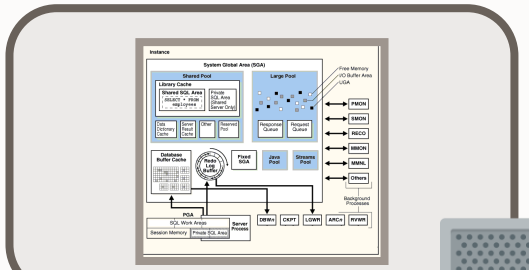
データベースでのデータの更新

データ本体の更新と更新履歴情報の追記



「Oracleインスタンス」と「データベース」

「データベース」はストレージ上のファイルの集合



Oracleインスタンス

データベース・サーバー上の
プロセスとメモリーの集合

データベース

ストレージ上のファイルの集合

オンラインREDOログ・ファイル

- 更新の履歴
- 1本書き込み完了したら複製

アーカイブREDOログ・ファイル

- オンラインREDOログ・ファイルの
  バックアップ

データファイル

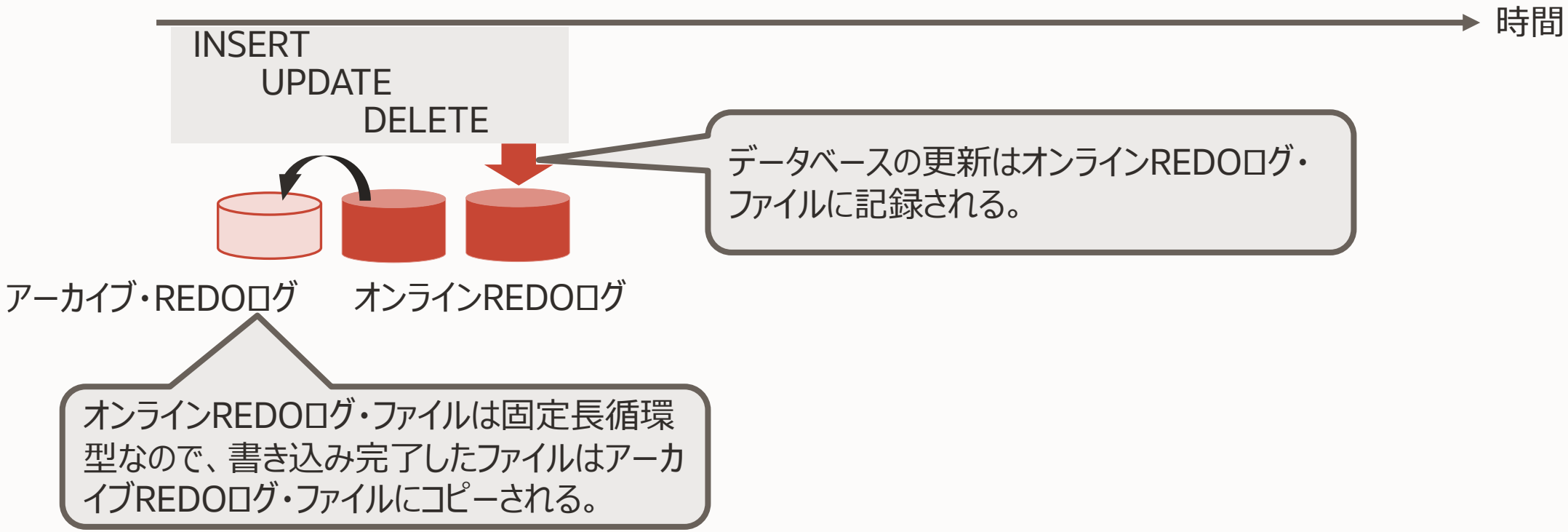
- 表データの本体

ORACLE

データの更新とバックアップ/リストア/リカバリ

データの更新

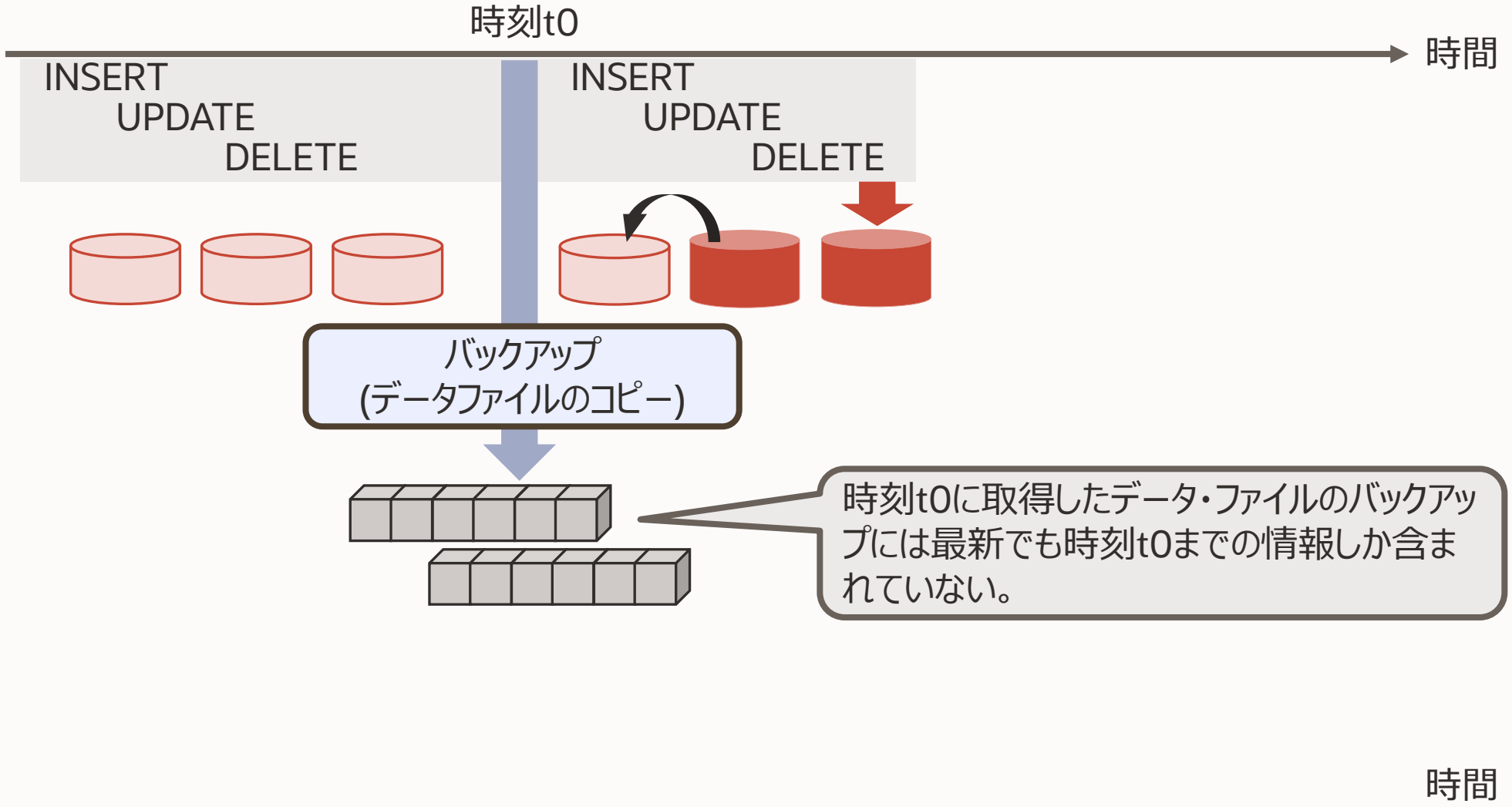
更新履歴のREDOログとデータ本体のデータブロックを更新



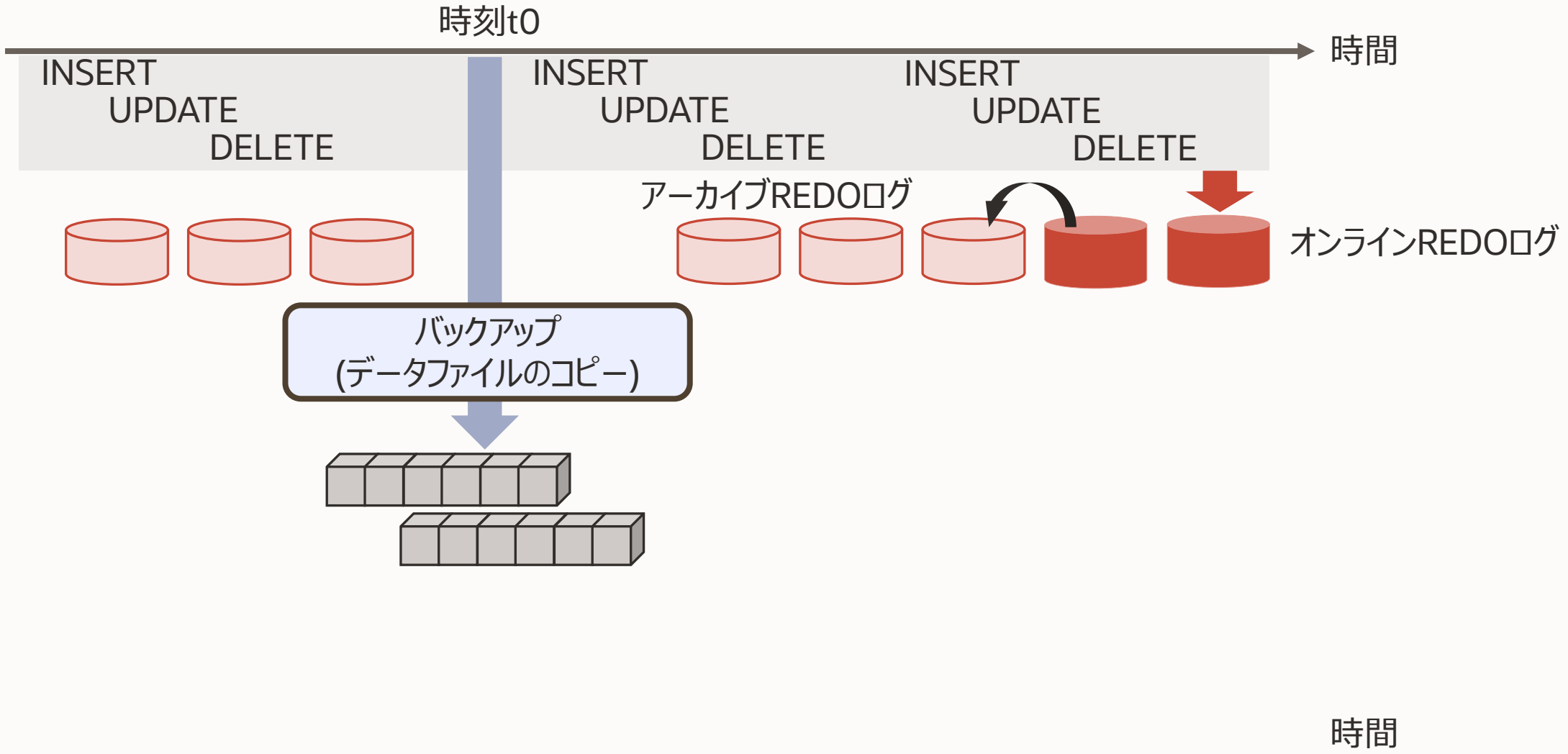
時間

バックアップ

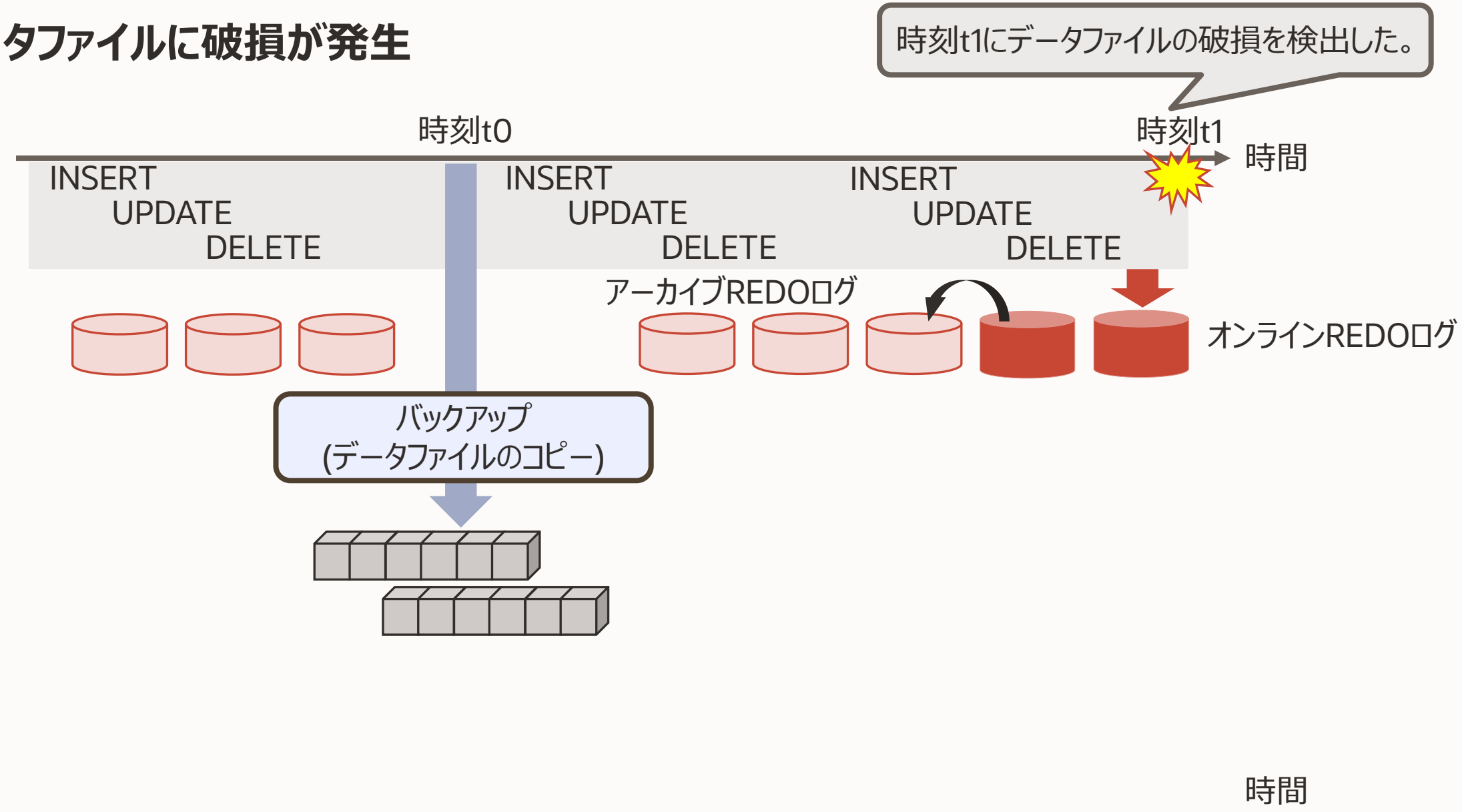
バックアップ操作をした時点のファイルの複製を作る



バックアップ操作以後もデータは更新され続ける

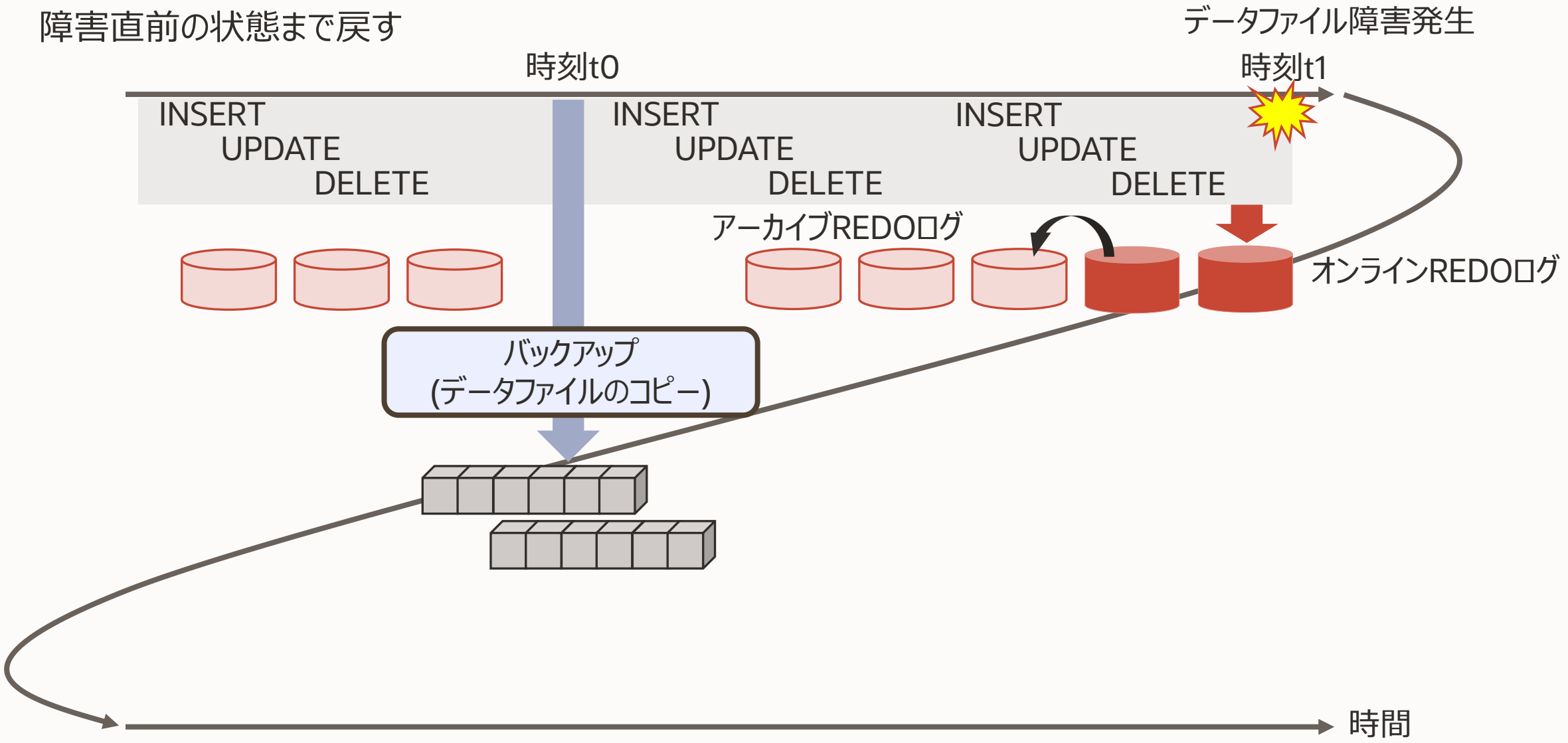


データファイルに破損が発生



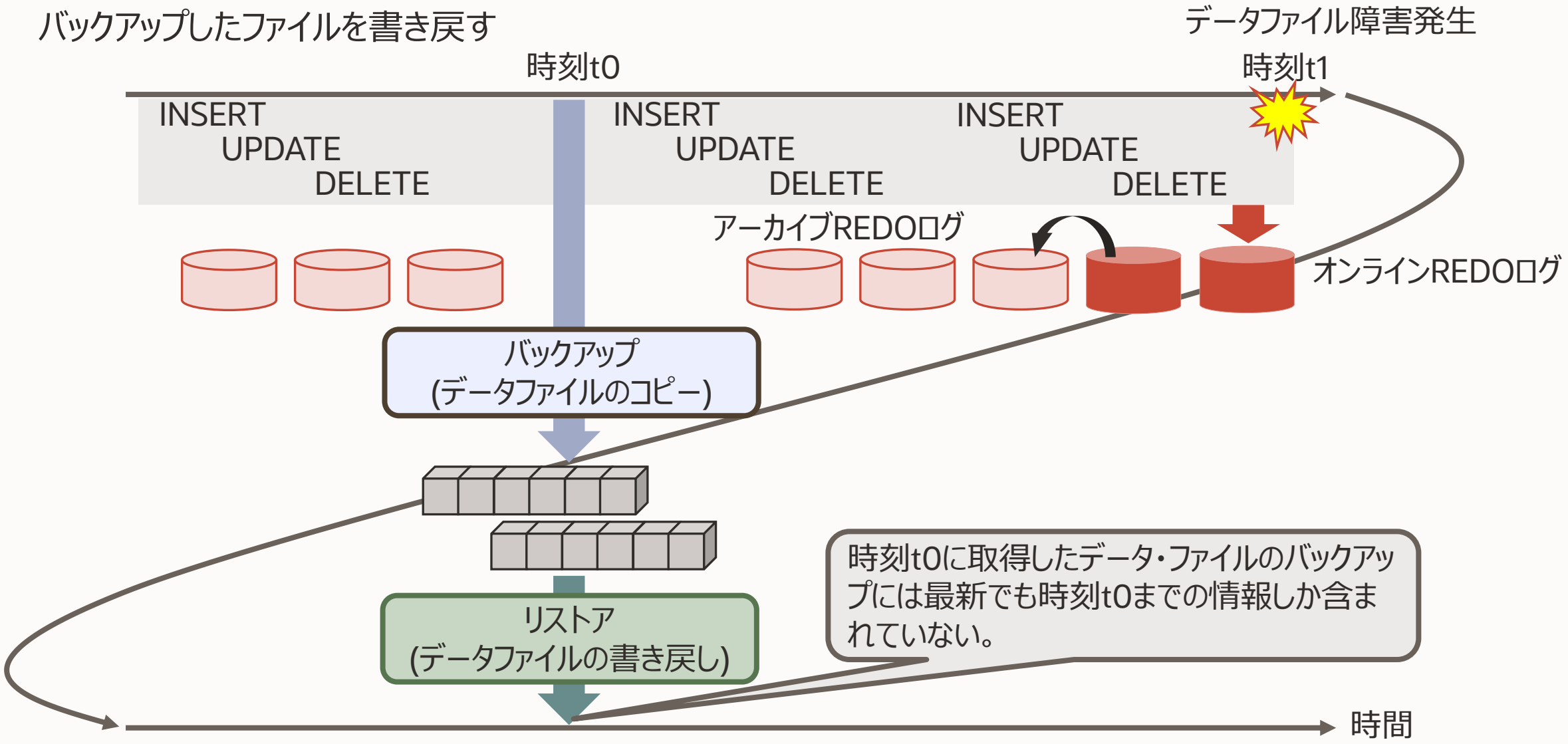
リストア・リカバリ

障害直前の状態まで戻す



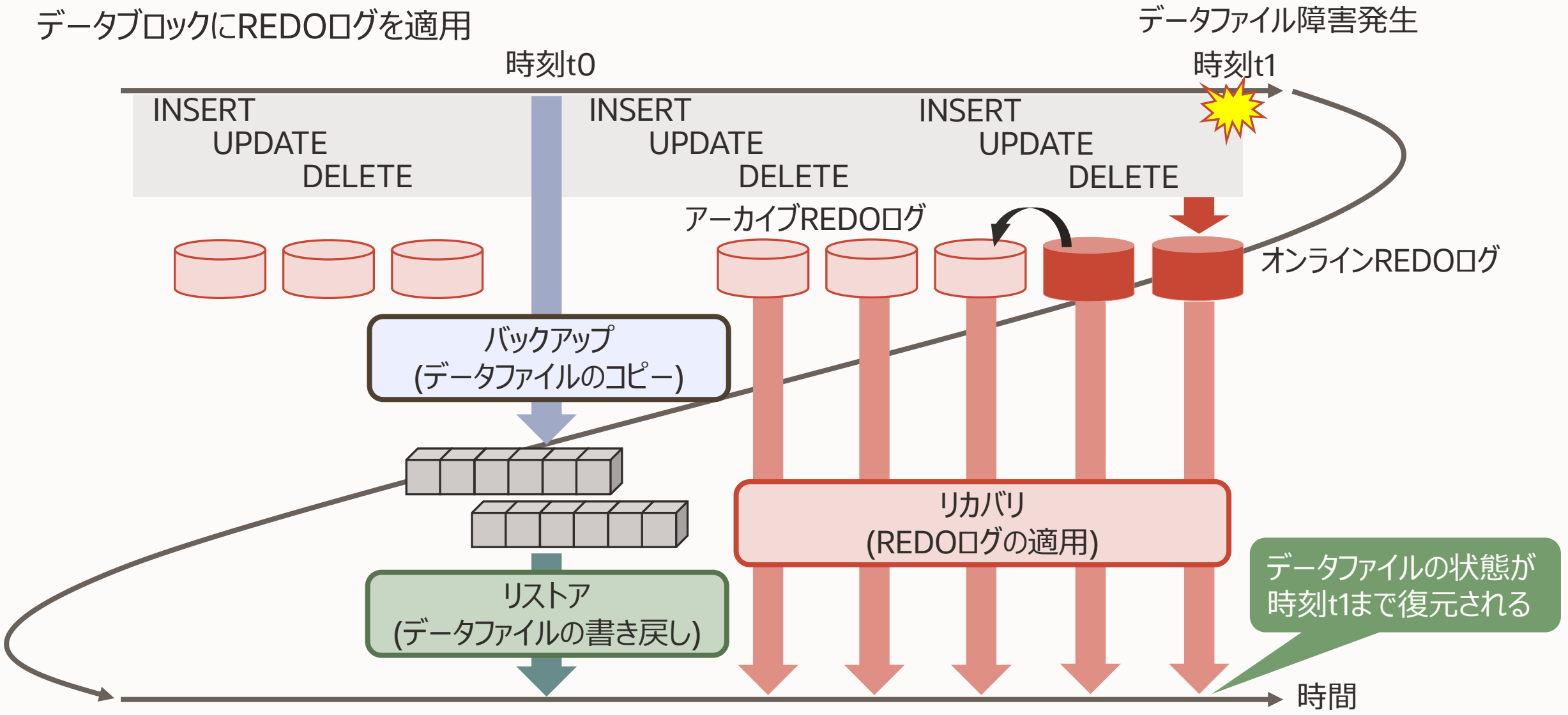
リストア

バックアップしたファイルを書き戻す

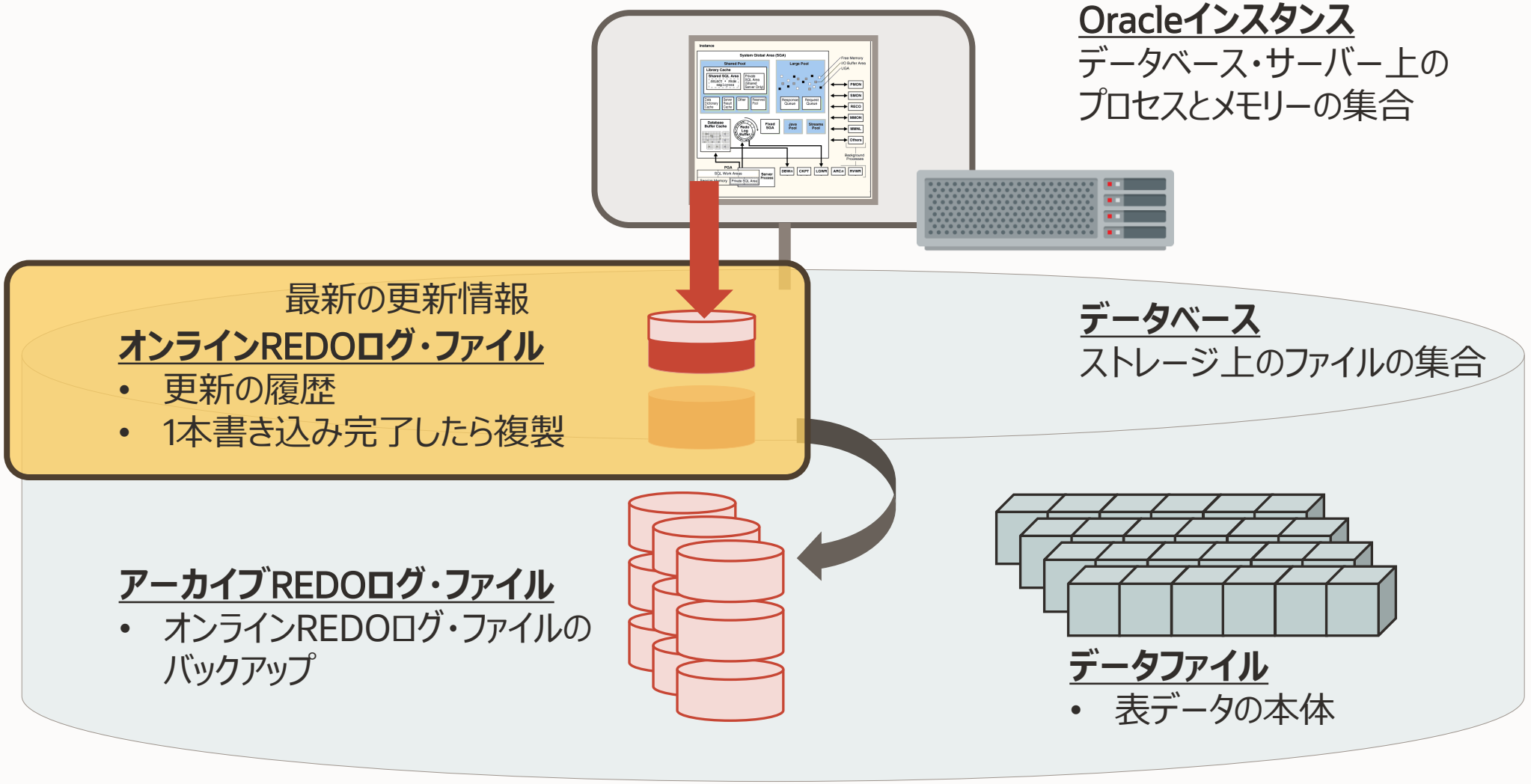


リカバリ

データブロックにREDOログを適用

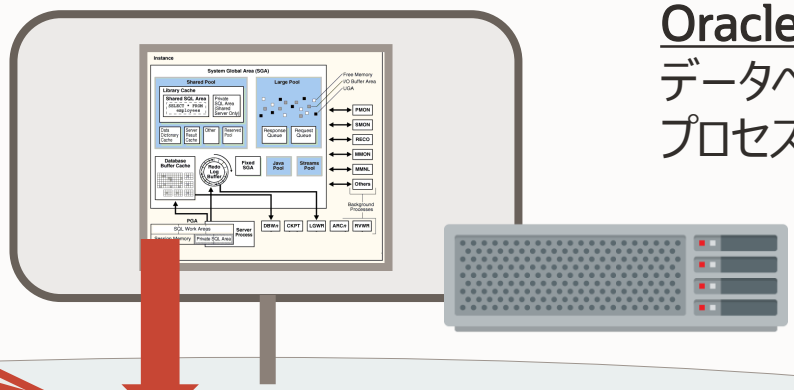


最新の更新情報はオンラインREDOログ・ファイルにしかない



「バックアップ」操作で複製できる範囲

書き込み真っ最中のオンラインREDOログ・ファイルは複製できない



Oracleインスタンス
データベース・サーバー上の
プロセスとメモリーの集合

追記中のオンラインREDOログ・
ファイルは複製できない

オンラインREDOログ・ファイル
- 更新の履歴
- 1本分書き込み完了したら複製

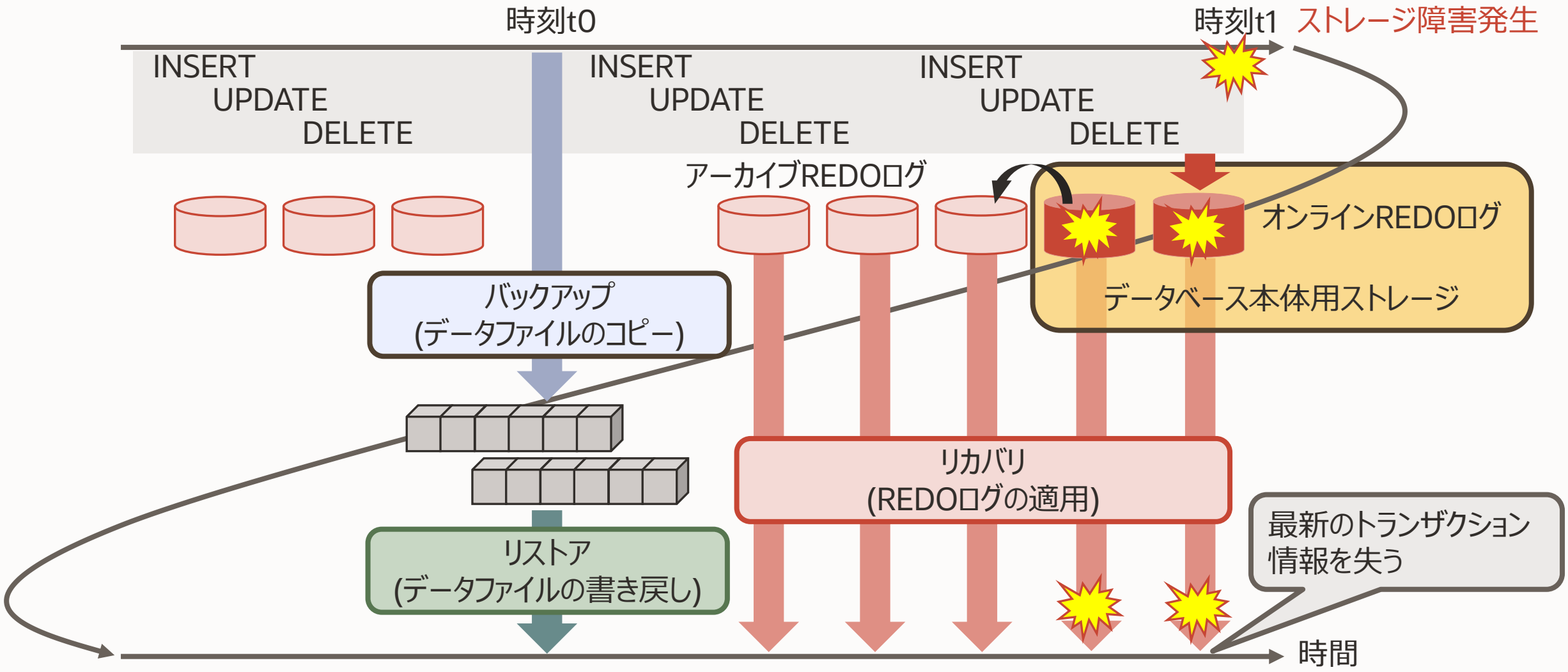
データベース
ストレージ上のファイルの集合

アーカイブREDOログ・ファイル
- オンラインREDOログ・ファイルの
  バックアップ

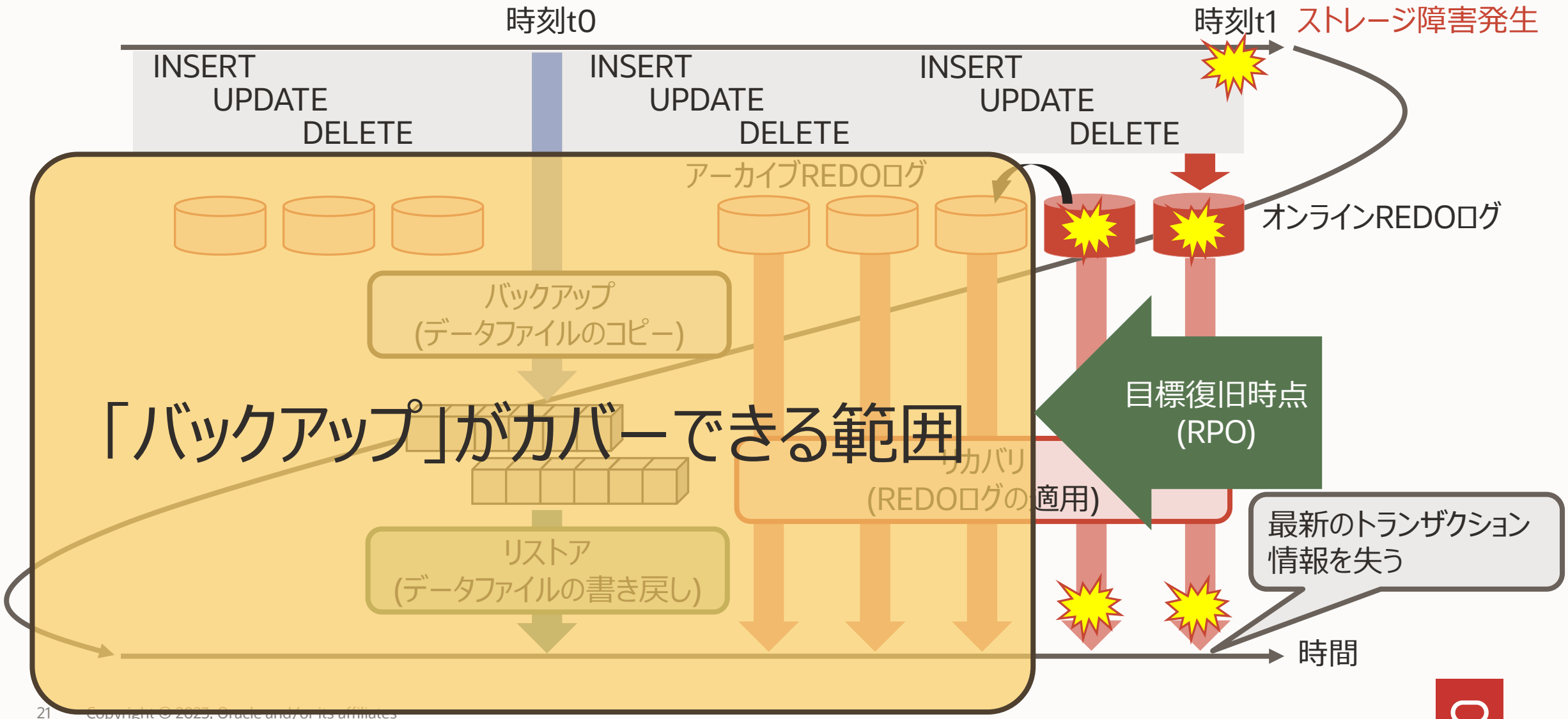
データファイル
- 表データの本体

「バックアップ」操作で複製できる範囲

オンラインREDOログ・ファイルが格納されているストレージが全損すると



「バックアップ」で復旧できるのはバックアップ操作時に存在していたデータまで



データの複製手段

「バックアップ」という言葉はあいまいに使われている

- 「複製されたデータ」を指す
- 「データの複製を作る操作」を指す

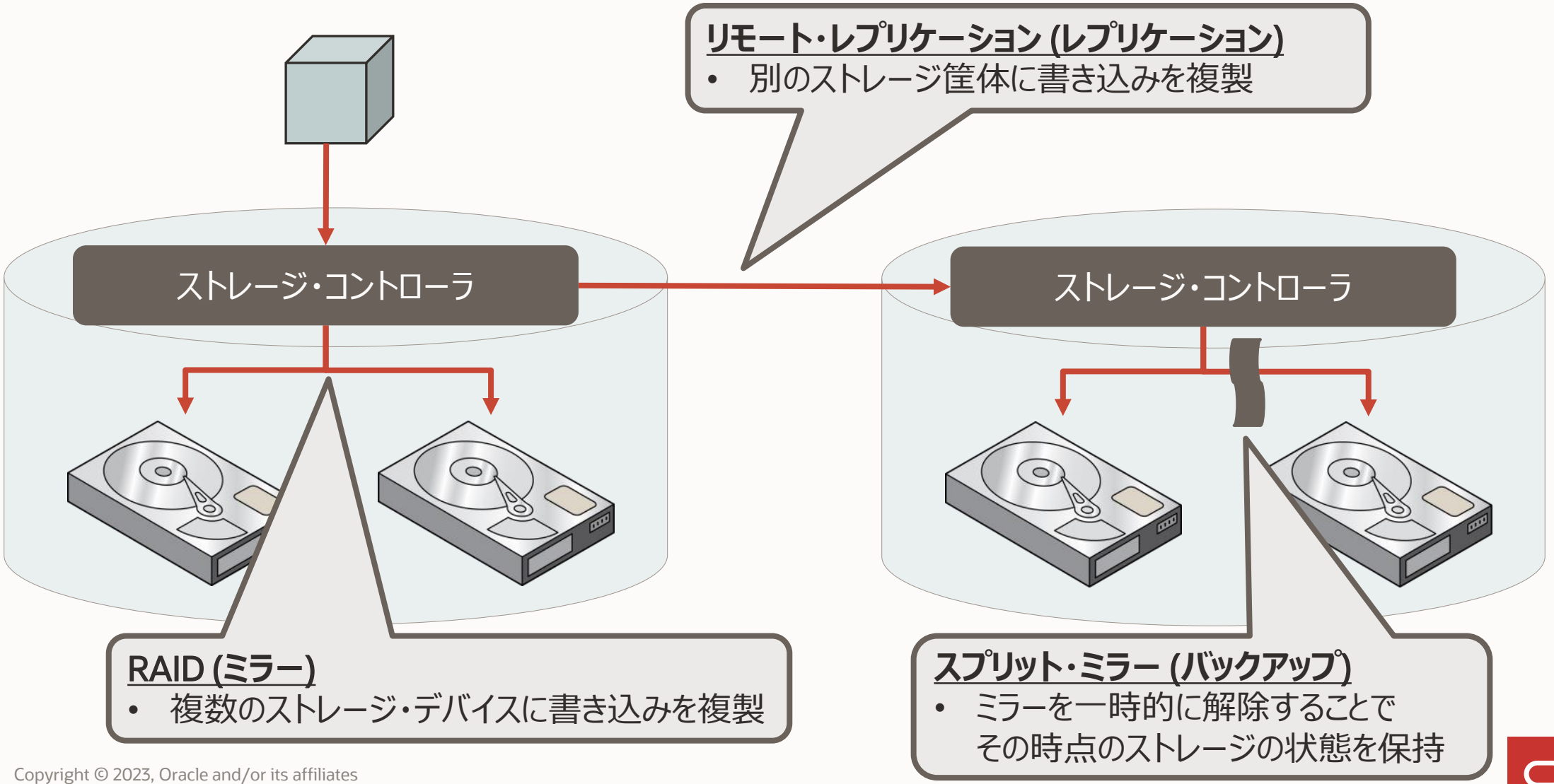
ここではバックアップとは「データの複製を作る操作」を指す

データを複製する手段

- バックアップ: バックアップ操作をした時点のデータの複製
- ミラー: 継続的なデータの複製 (ローカル・ストレージ)
- レプリケーション: 継続的なデータの複製 (リモート・ストレージ)
- (スナップショット)

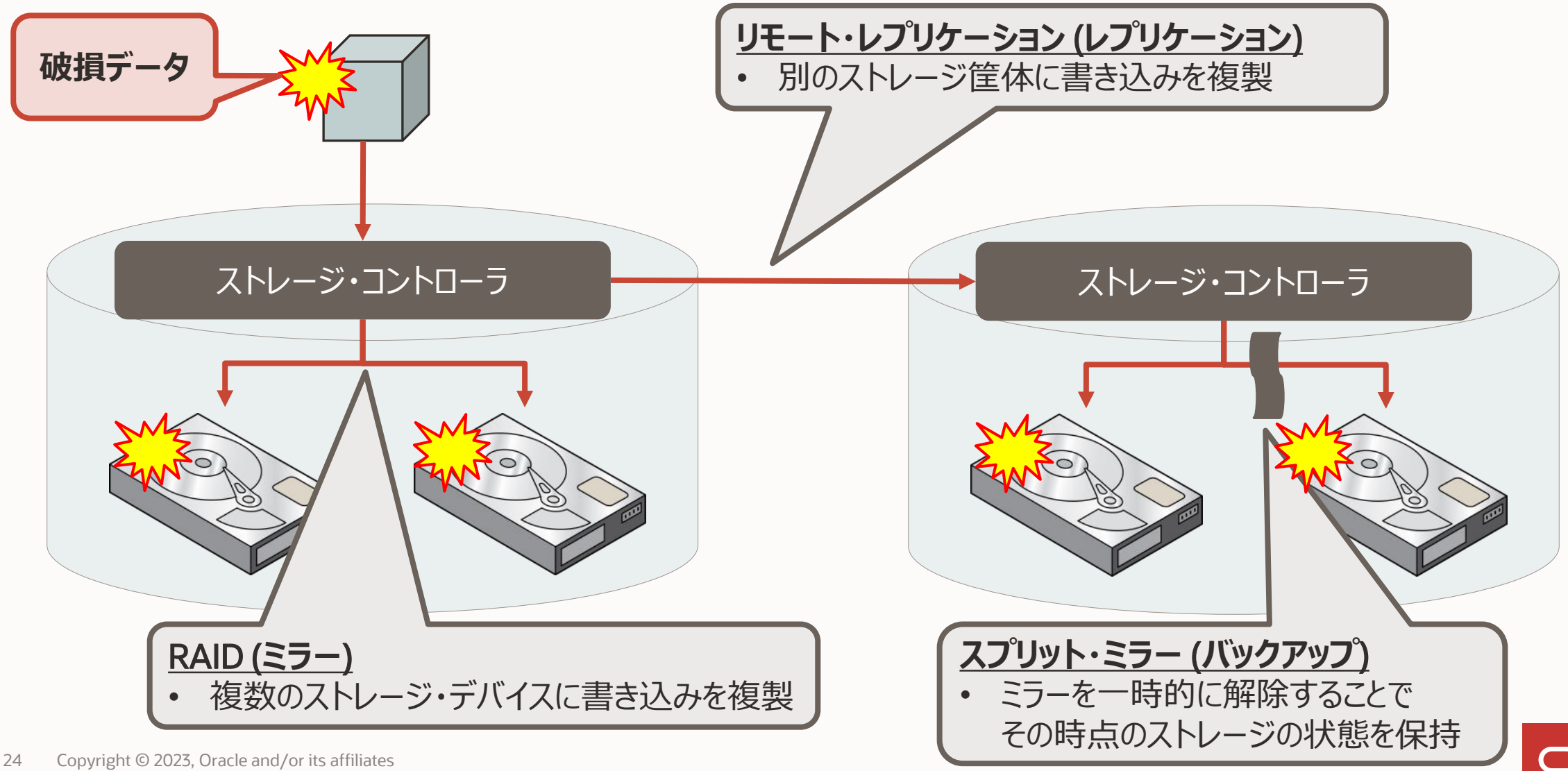
ストレージ機能でのデータの複製

ミラー/レプリケーション/バックアップ

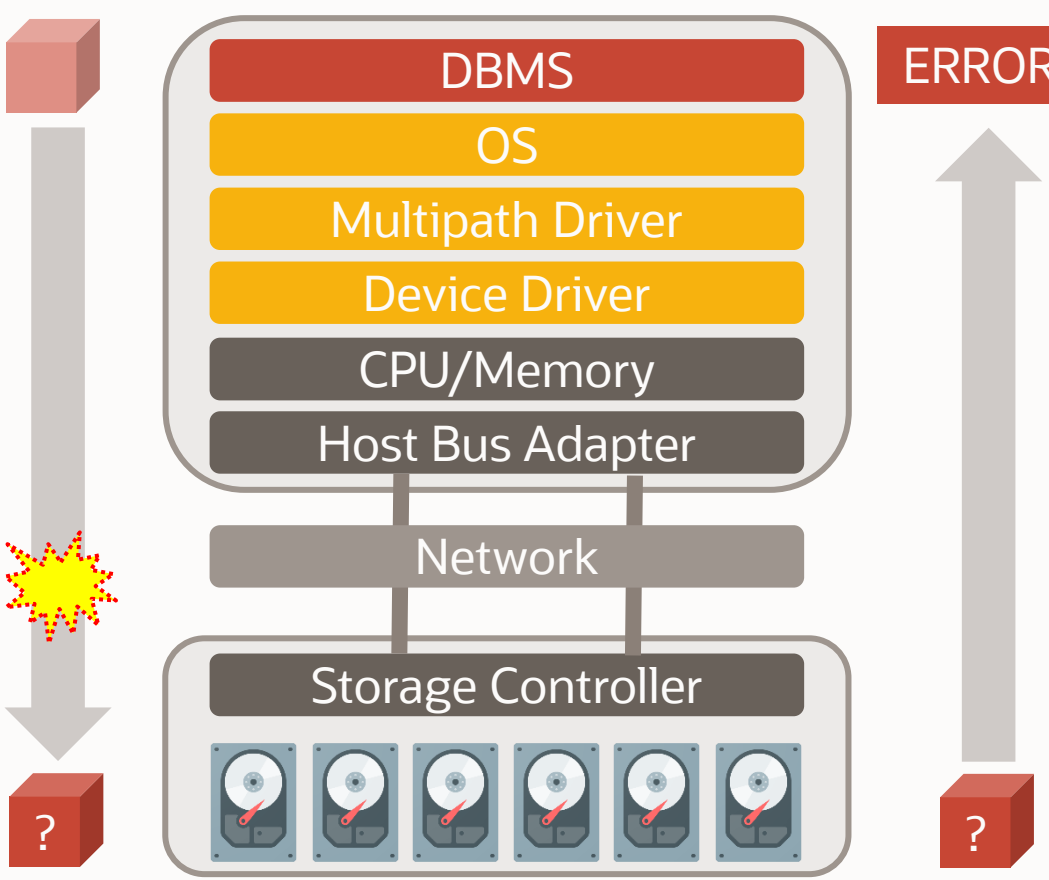


ストレージ機能でのデータの複製

書き込むデータが意味的に正常なのかはストレージは判別できないのでデータ破損が伝搬する



データを失う要因はストレージ・デバイスの故障以外にもある



ストレージ・デバイスが故障していなくても、格納されているファイルのデータが破損している場合がある。

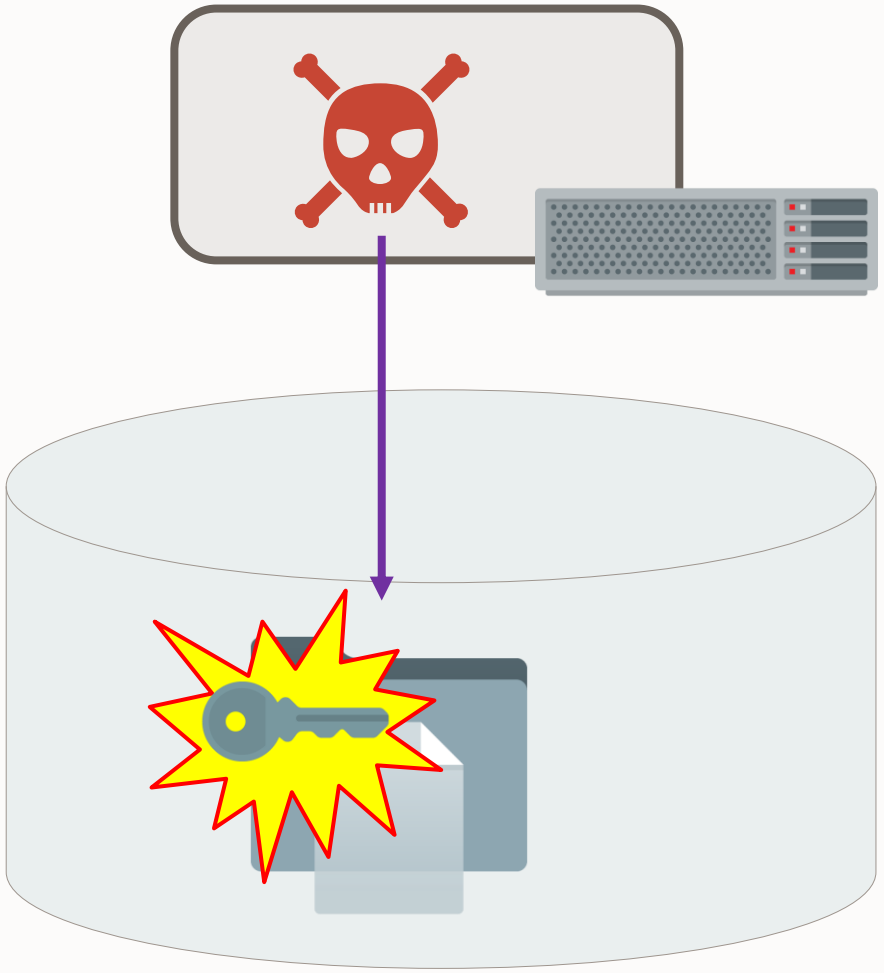
エラー・ログを出力するのは、その異常を検出した階層。
異常検出能力のない階層はエラー・ログを出力できない。
⇒ 破損データを次の階層に伝搬させる。
データを破損させた階層を特定することは困難。

ストレージのデータを破損させる要因

- CPU/メモリー故障
- レーザー出力不安定
- 電源障害
- ランサムウェア
- …

ランサムウェア： ソフトウェア的なデータの破損

ソフトウェアからデータの内容にアクセスできなくなる



ランサムウェア

- OSに侵入してファイルを暗号化
- アプリケーションからファイルの内容にアクセス不能になる

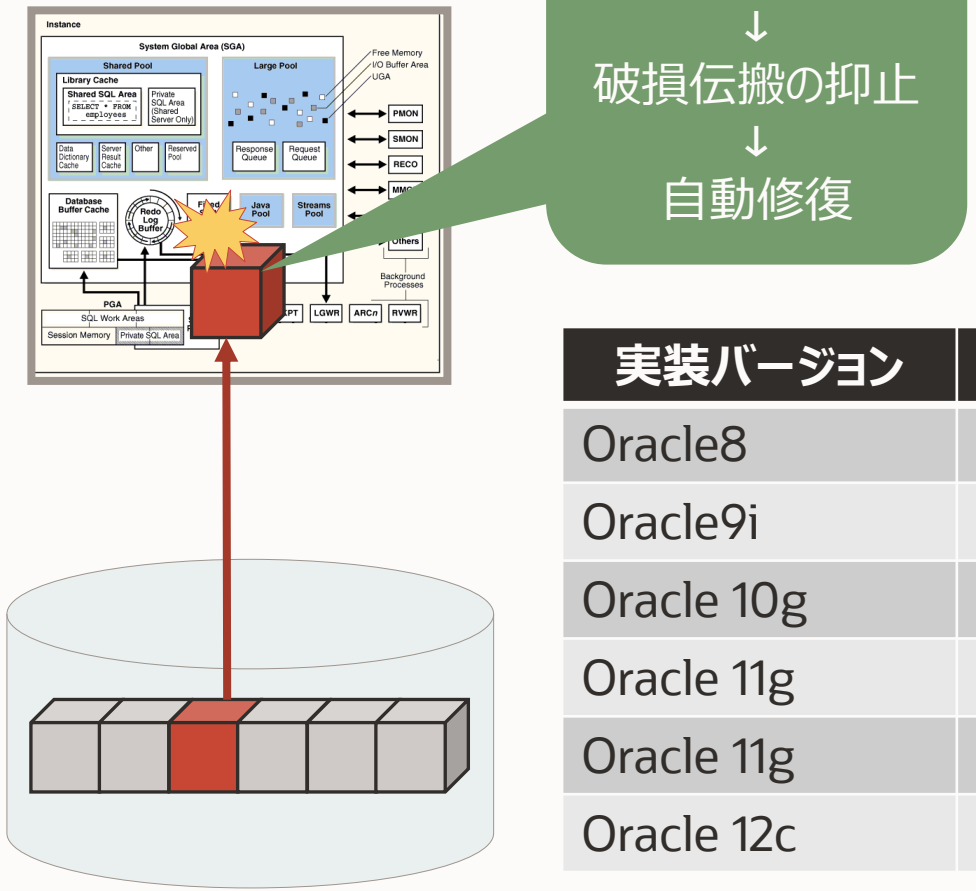
- ハードウェアが故障したわけではない
- **ソフトウェア的なデータの破損**

Oracle Databaseのデータ保護機能は
「ソフトウェア的なデータの破損」も想定している

Oracle Databaseはなぜデータの複製をOracleソフトウェアでやろうとするのか

Oracle Databaseの歴史はデータ破損との闘い

Oracleインスタンス



破損検査
↓
破損伝搬の抑止
↓
自動修復

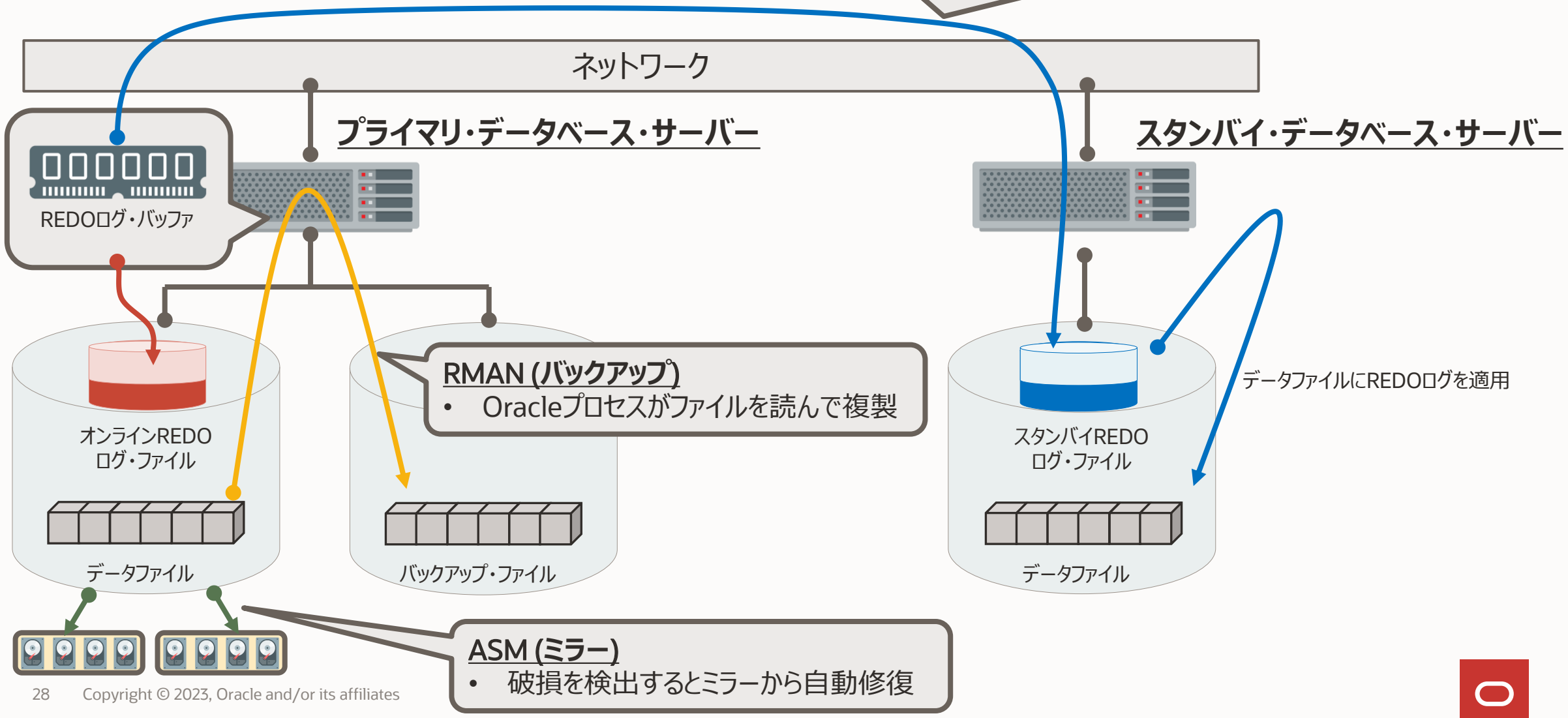
- データ構造がOracle Databaseとして正しいかを検査できるのはOracle自身しかない
- ある階層から別の階層に移動させるとき検査される
- 破損が次の階層に伝搬しない
- データの複製がある場合は自動修復を試みる

実装バージョン	機能名	機能
Oracle8	RMAN	バックアップ/リストア
Oracle9i	Data Guard	REDO情報を別サーバーに転送
Oracle 10g	ASM	ストレージの冗長化と自動修復
Oracle 11g	Exadata	Oracle専用ストレージがデータ構造を検査
Oracle 11g	Active Data Guard	Data Guard+自動修復
Oracle 12c	ZDLRA	RMANバックアップ+REDO転送

Oracle Databaseのデータ複製機能

データを移動させるときに破損検査が行われる

Active Data Guard (レプリケーション)
- REDO情報を別のデータベース・サーバーに転送
- リカバリを継続することで最新のデータベース状態を維持
- 破損を検出すると対向サーバーから該当データを取り寄せ自動修復



RMAN (バックアップ)
- Oracleプロセスがファイルを読んで複製

ASM (ミラー)
- 破損を検出するとミラーから自動修復

ORACLE

Automatic Storage Management (ASM)

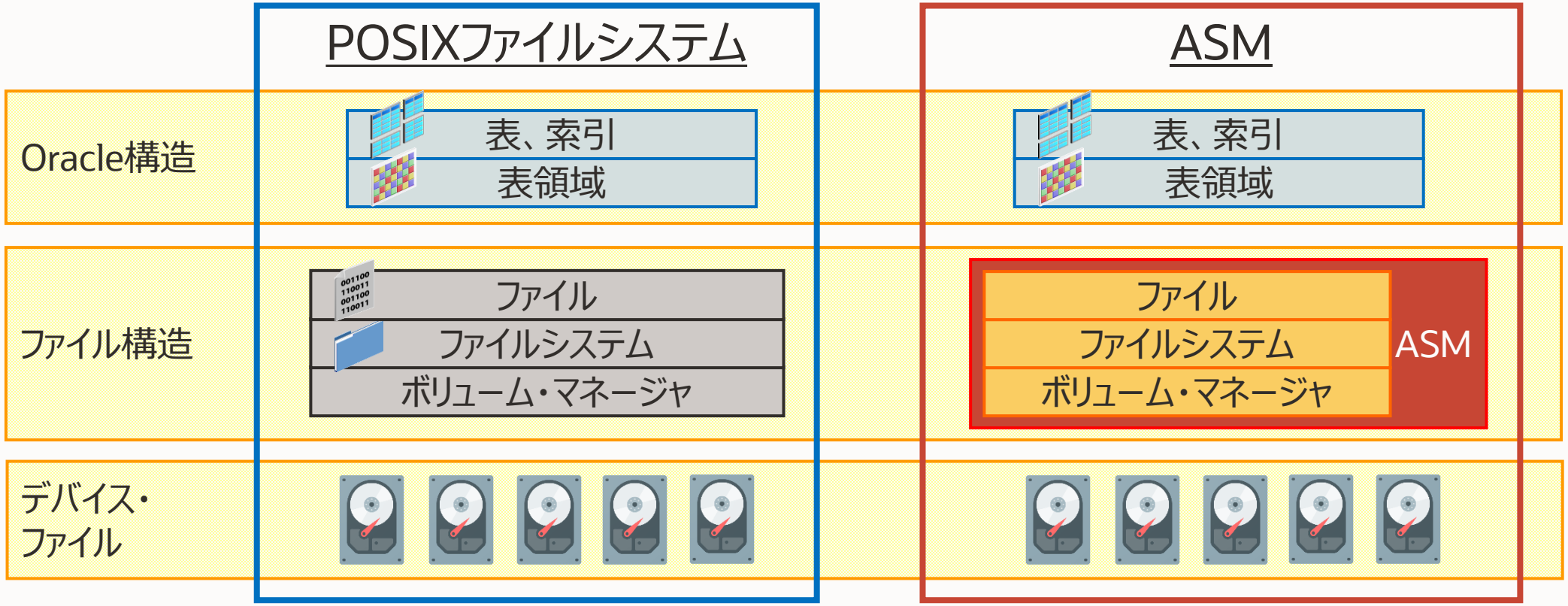
データのストライプ＆ミラー

データ破損検出からの自動修復

Oracle Automatic Storage Management

Oracle Database専用のクラスタ・ボリューム・マネージャ兼クラスタ・ファイルシステム

管理者から見た操作の階層はどちらもディレクトリ・ツリーとファイルで同じ



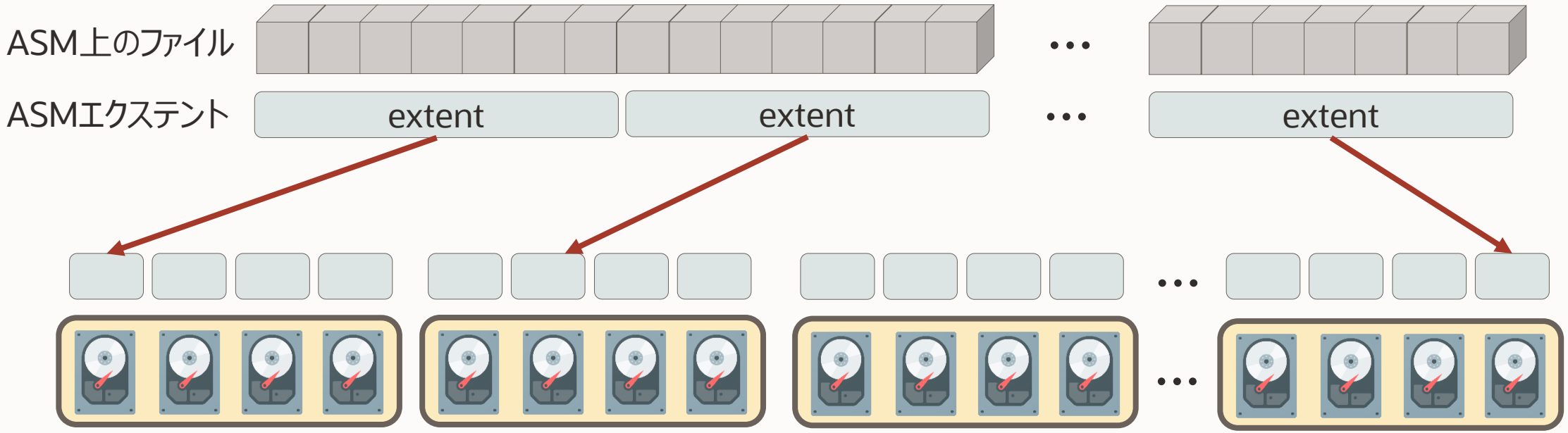
RAIDとは異なる実装で

- ストレージ・デバイスの障害に対処可能
- データ破損を検出すると自動修復

ASMのファイル配置コンセプト1

どのファイルへのアクセスもストレージの性能を最大限引き出す

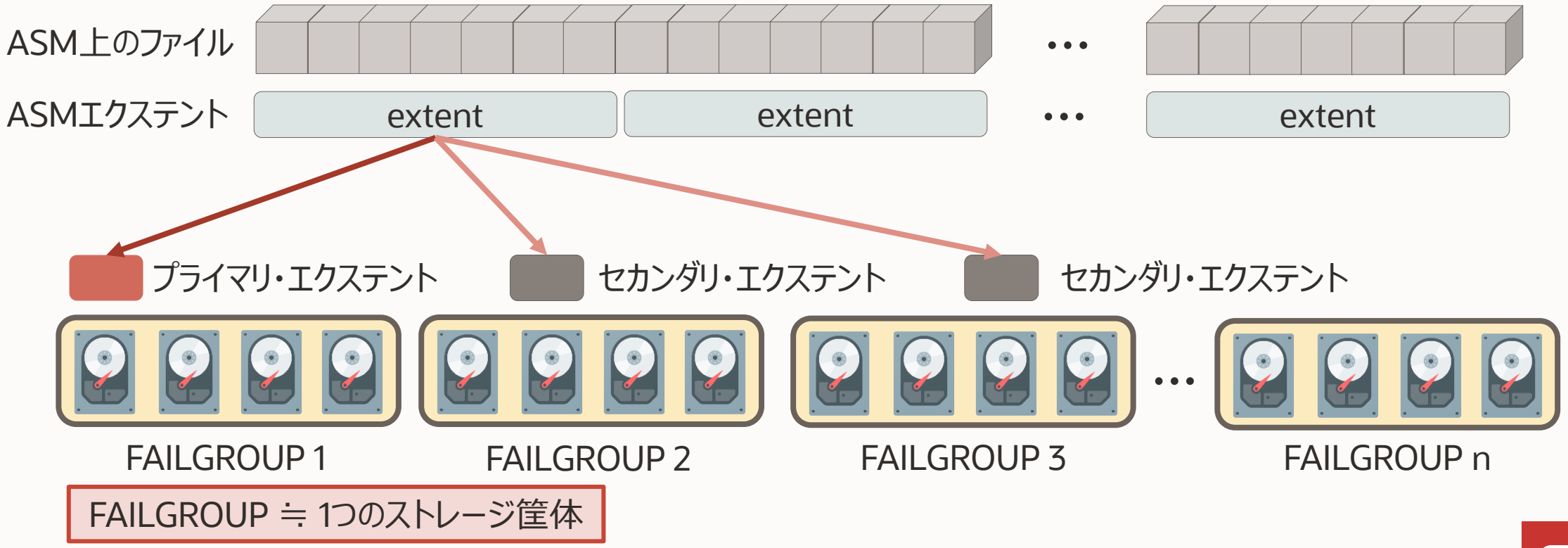
ファイルを分割し、すべてのストレージ・デバイスに均等に分散する。
ストレージ・デバイスが増減しても、再配置して均等を維持する。



ASMのファイル配置コンセプト2

どのファイルも冗長化して障害に対処する

ファイルを分割しミラーを用意する。
ミラーは異なる障害グループ(FAILGROUP)のストレージ・デバイスに配置する。
ストレージ・デバイスが増減しても、再配置して冗長構成を維持する。



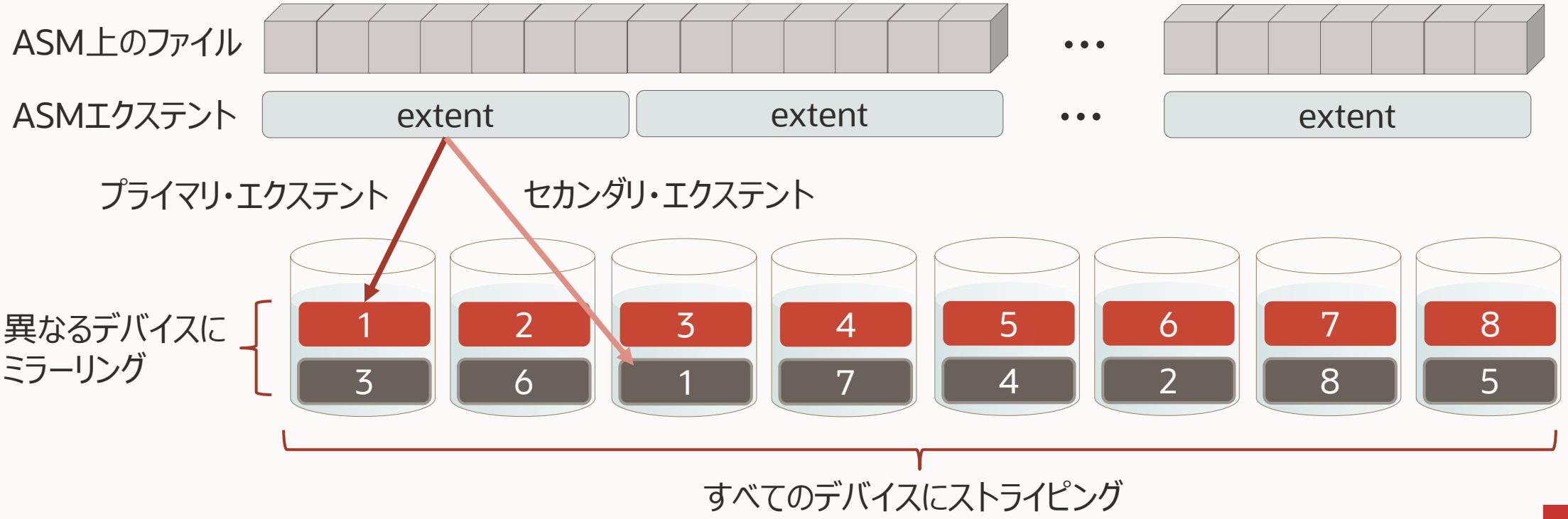
FAILGROUP ≒ 1つのストレージ筐体

ASMのファイル配置コンセプト
Stripe And Mirror Everything (S.A.M.E.)

ファイルを分割し、

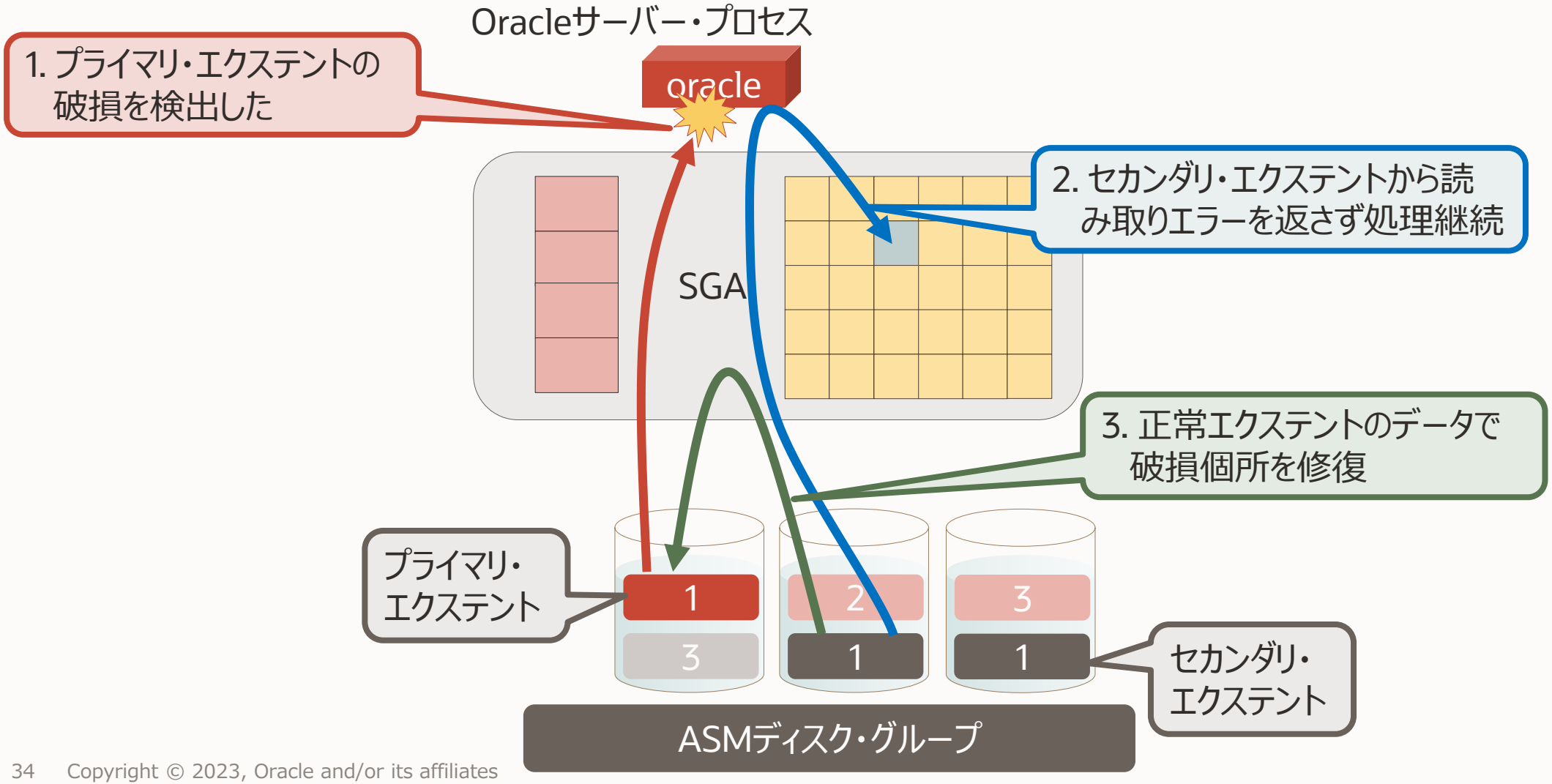
- すべてのストレージ・デバイスに均等に分散する ⇒**Stripe**
- ミラーは異なる障害グループ(FAILGROUP)のストレージ・デバイスに配置する ⇒**Mirror**

そして**ストレージ・デバイスが増減してもリバランスすることでStripeとMirrorを維持する**



ファイルの破損検出と自動修復

ASMファイルの破損が検出されるとセカンダリ・エクステントから読み取って処理継続および自動修復

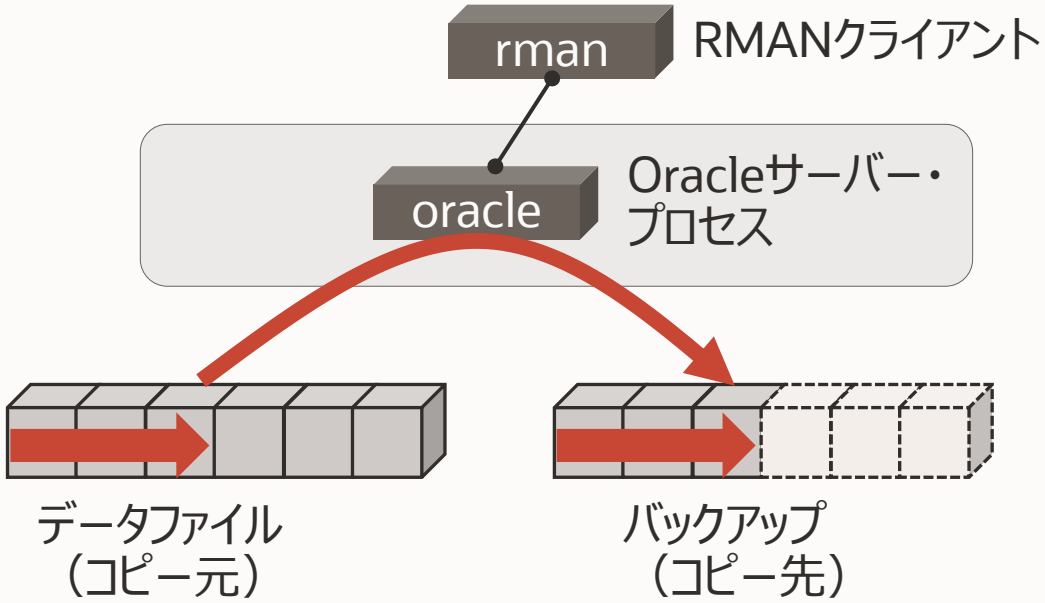


ORACLE

Recovery Manager (RMAN)

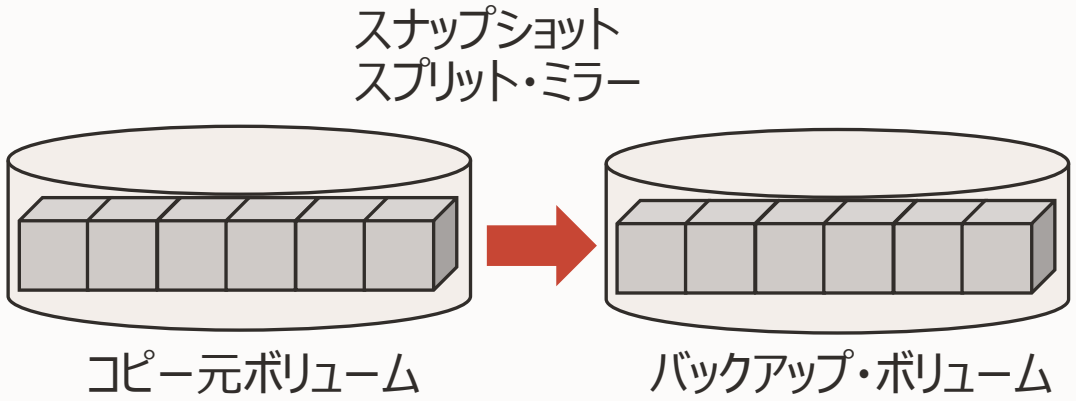
破損検査付きバックアップおよびリストア・リカバリ

Oracle Databaseの2種類の物理バックアップ手法
推奨はRMAN



Recovery Manager (RMAN)

- Oracle付属のバックアップ・ツール
- Oracleサーバー・プロセスがデータベースのファイルにアクセスする仕組みを使ってファイルをコピー
- Oracleインスタンス管理下で行われる操作

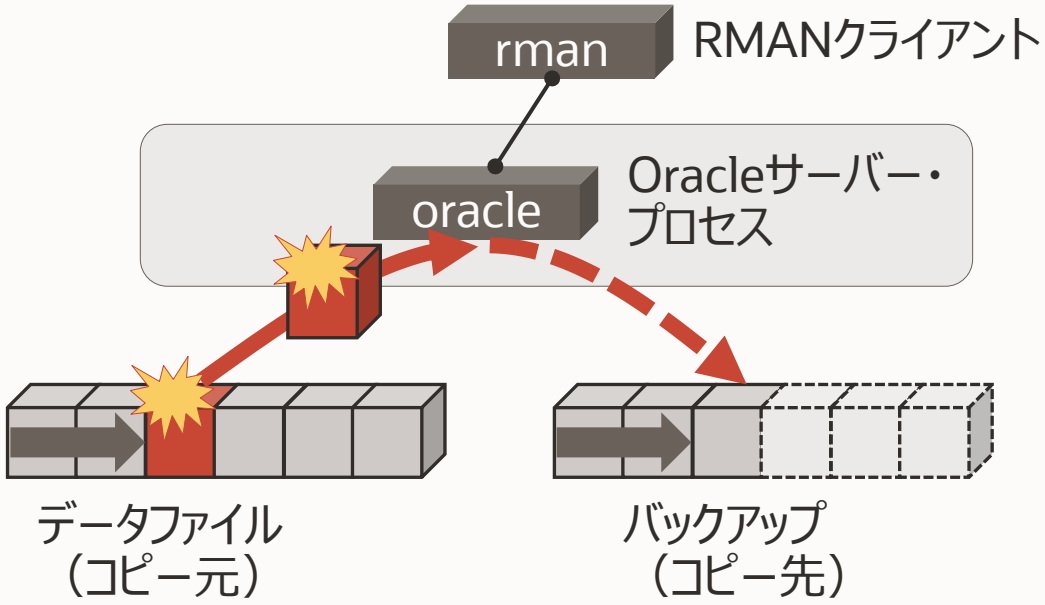


ユーザー管理バックアップ

- RMAN以外の方法でコピーするすべての手法
- Oracleインスタンスがコピーを関知しない
  - OSのファイル・コピー・コマンド
  - ストレージ機能のスナップショットやスプリット・ミラー

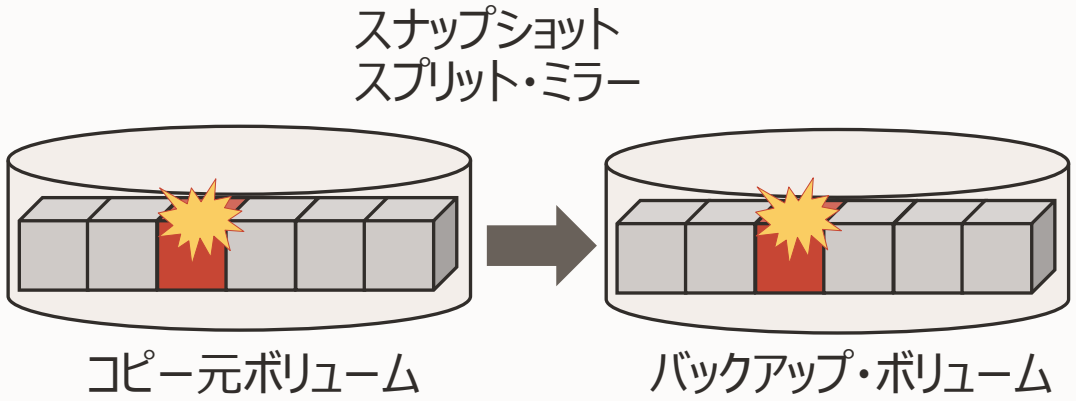
ファイル・コピー中のブロック破損検査

確実にリカバリするための"Recovery" Manager



Recovery Manager (RMAN)

- コピー時に破損検査が行われる
- 破損が伝搬しない
- バックアップしたファイルの破損検査も可能



ユーザー管理バックアップ

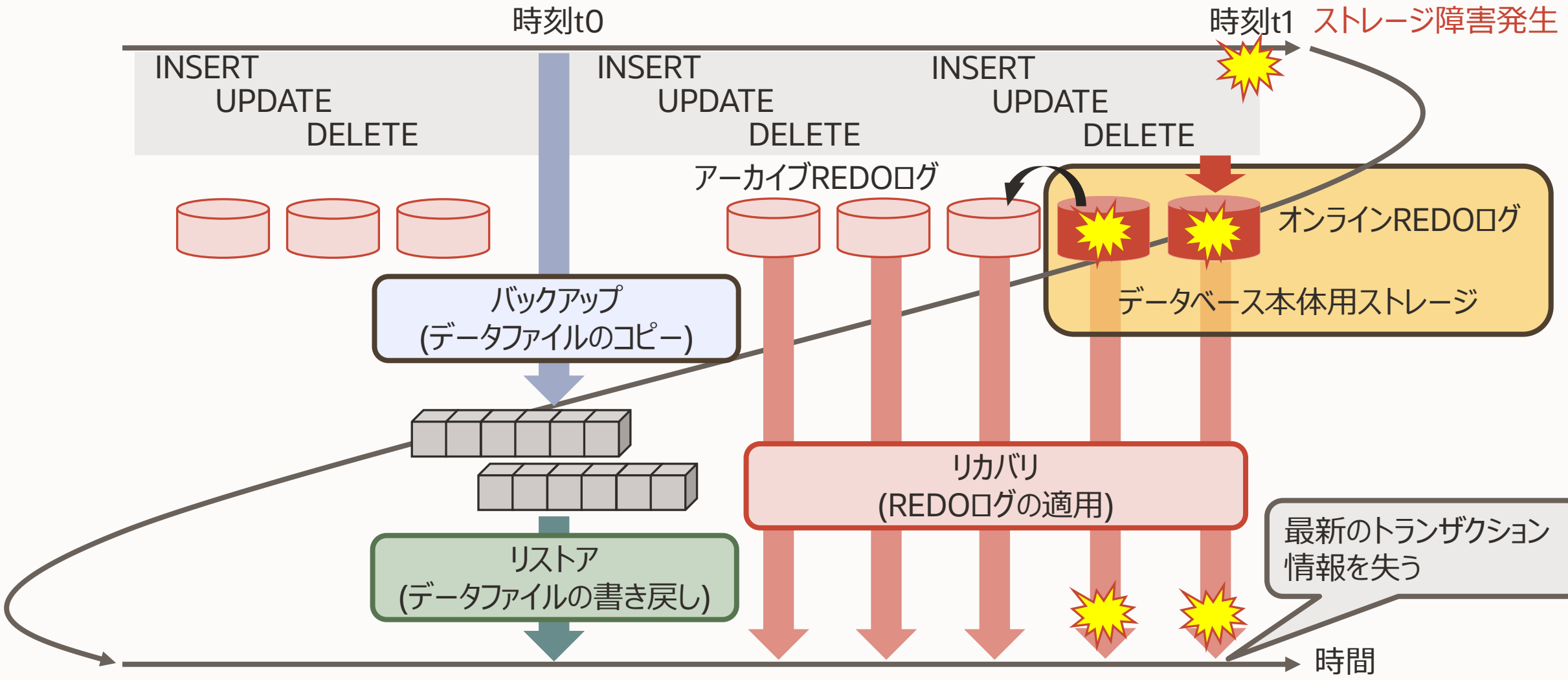
- 破損領域がそのままコピーされる
- バックアップも破損している場合がある
- 誤った単位でボリュームをコピーしているとリカバリ時になってはじめてリカバリ不能に気付く

ORACLE

(Active) Data Guard

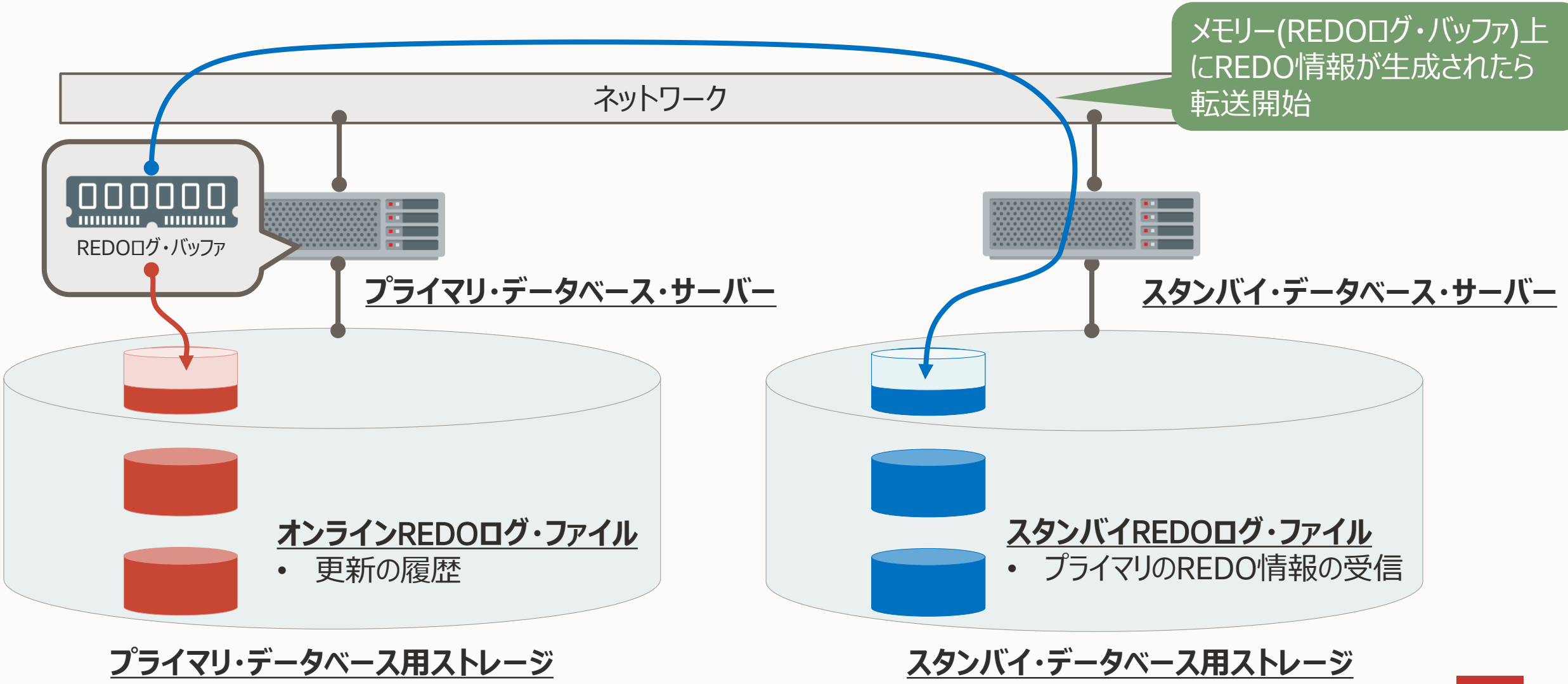
最新のREDO情報をリモート・データベースに転送してリカバリ継続

オンラインREDOログ・ファイルが格納されているストレージが全損すると (再掲)



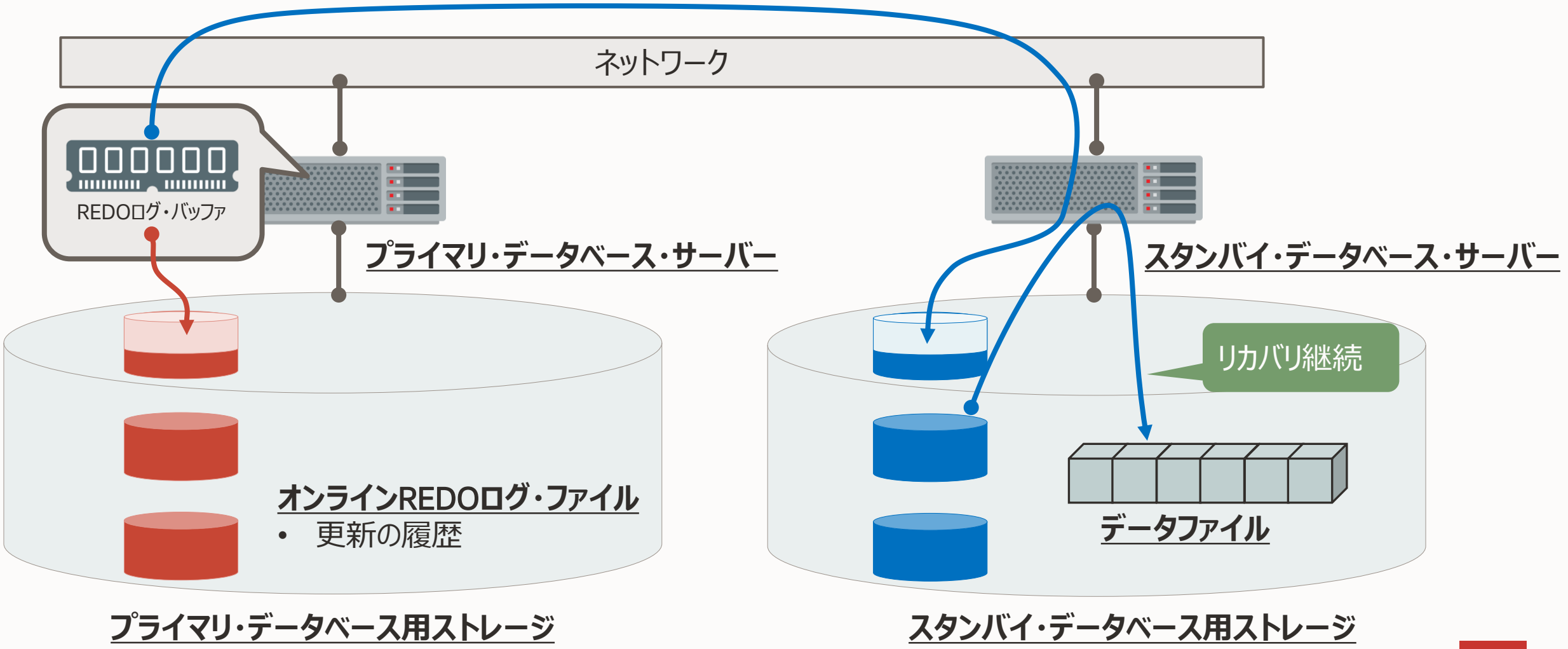
REDO情報が生成されたら即時に別のサーバーに転送：(Active) Data Guard

プライマリ・データベース用ストレージが全損しても最新のREDO情報が別の場所にある

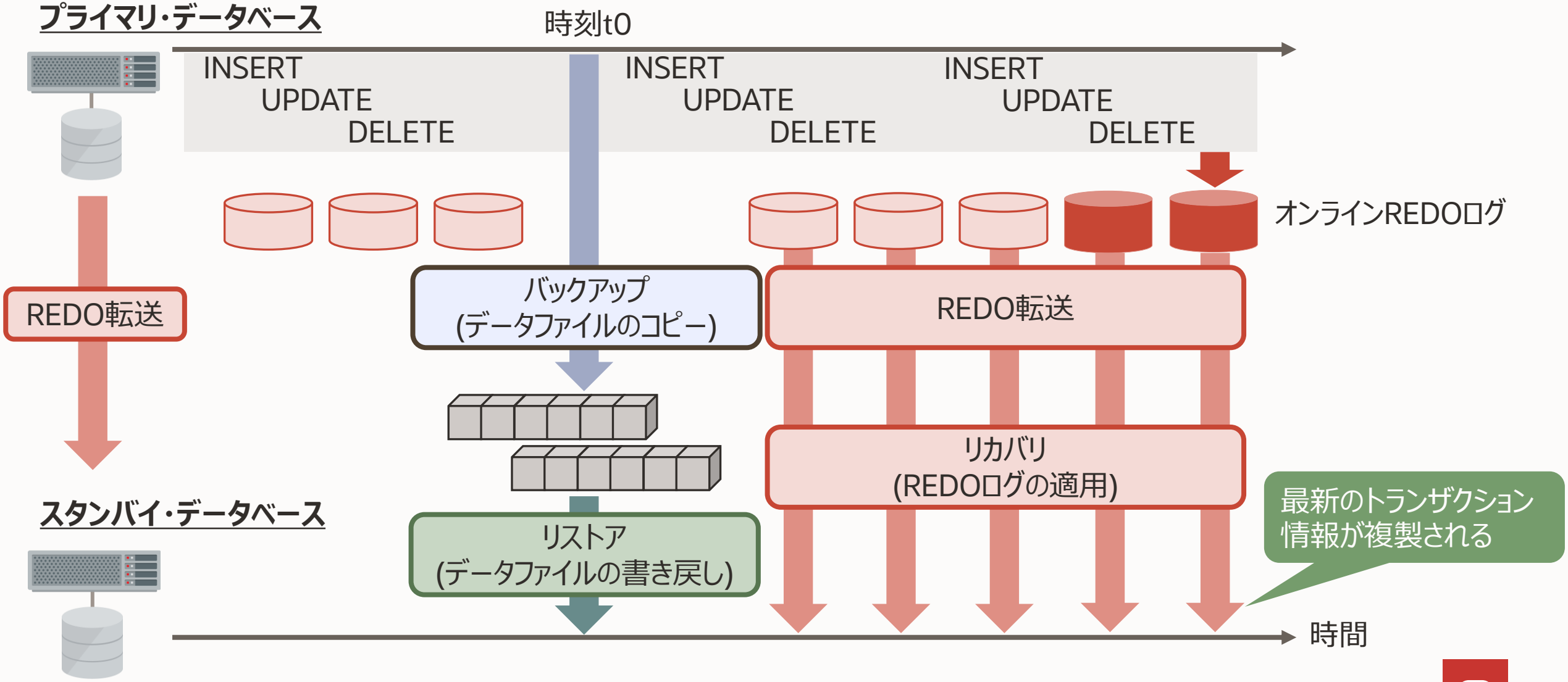


(Active) Data Guard：プライマリ・データベースと全く同じ内容になる

プライマリ・データベースのREDO情報でデータファイルをリカバリし続ける



(Active) Data Guard：リモートでリストア＆リカバリを継続



ORACLE

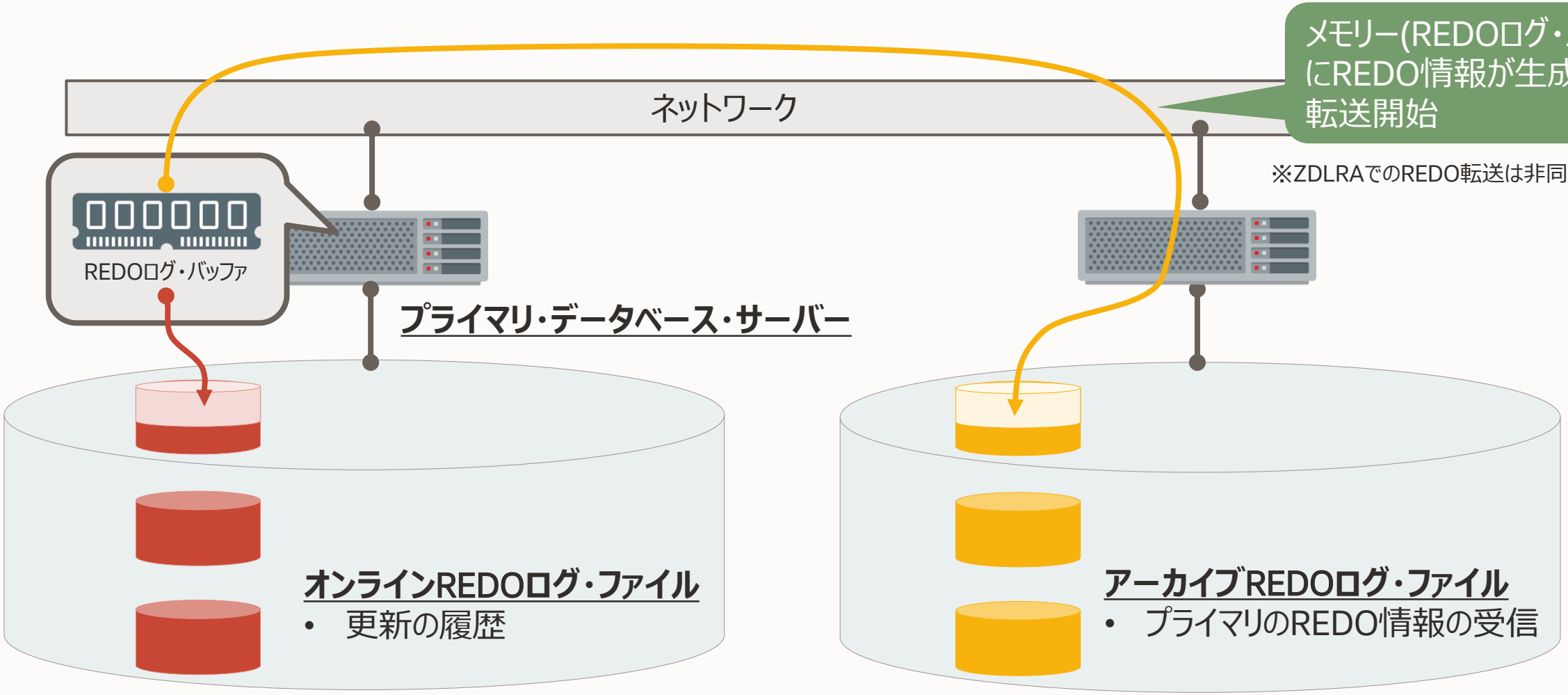
Zero Data Loss Recovery Appliance (ZDLRA)

Oracle Database専用のバックアップ・アプライアンス

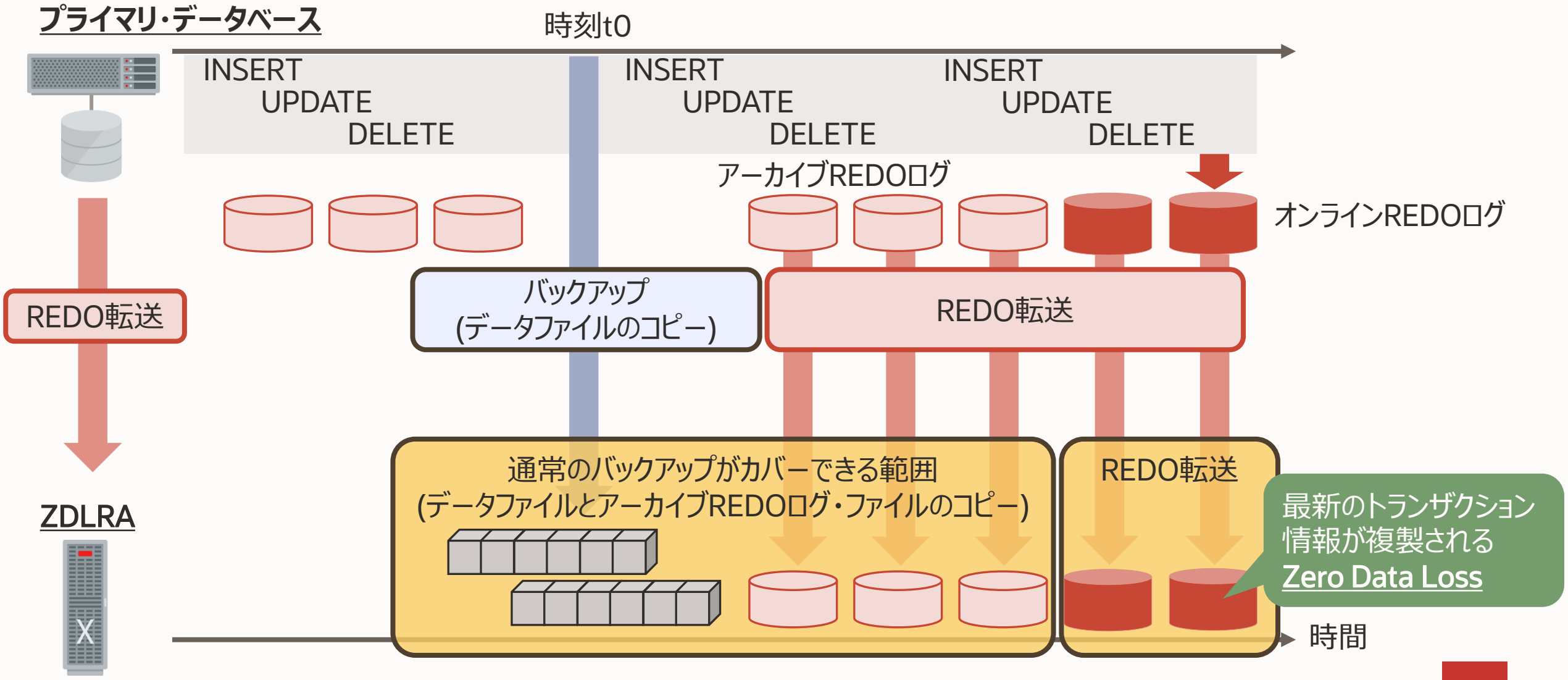
RMANバックアップ+最新のREDO情報の複製

Data Guard REDO転送の仕組みをバックアップ用サーバーにも実装：ZDLRA

プライマリ・データベース用ストレージが全損しても最新のREDO情報が別の場所にある



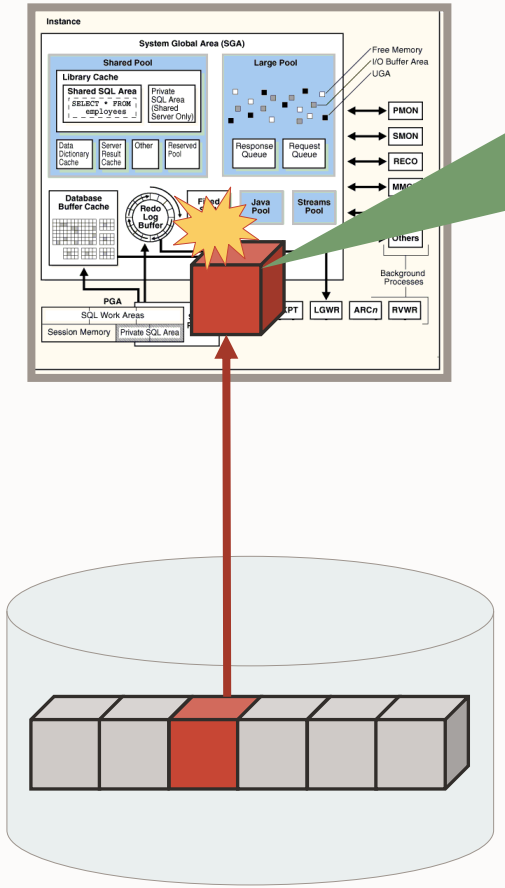
Zero Data Loss Recovery Appliance：データファイルのバックアップ+REDO転送



Oracle Databaseはなぜデータの複製をOracleソフトウェアでやろうとするのか

Oracle Databaseの歴史はデータ破損との闘い

Oracleインスタンス



破損検査
↓
破損伝搬の抑止
↓
自動修復

- データ構造がOracle Databaseとして正しいかを検査できるのはOracle自身しかない
- ある階層から別の階層に移動させるとき検査される
- 破損が次の階層に伝搬しない
- データの複製がある場合は自動修復を試みる

実装バージョン	機能名	機能
Oracle8	RMAN	バックアップ/リストア
Oracle9i	Data Guard	REDO情報を別サーバーに転送
Oracle 10g	ASM	ストレージの冗長化と自動修復
Oracle 11g	Exadata	Oracle専用ストレージがデータ構造を検査
Oracle 11g	Active Data Guard	Data Guard+自動修復
Oracle 12c	ZDLRA	RMANバックアップ+REDO転送

データベースのバックアップ・リカバリ

Database Management System

- ストレージに障害が発生することを想定している
- データ本体のバックアップ + バックアップ以後の更新履歴の組み合わせで目標復旧時点(RTO)を0にできる

データがソフトウェア的に破損することがある

- ストレージ・ハードウェアが故障していなくとも
- データ破損を検出できない階層は破損を次の階層に伝搬させる

Oracle Databaseのデータ構造として正しいかを検査できるのはOracleソフトウェアのみ

- Oracle Databaseがデータの複製機能をストレージ機能ではなくソフトウェアで持つ理由
- 破損伝搬の抑止と自動修復
  - バックアップ: Recovery Manager (RMAN)
  - ミラー: Automatic Storage Management (ASM)
  - レプリケーション: Active Data Guard


ORACLE