

Oracle Database Technology Night

～集え！オラクルの力(チカラ)～

Technical Discussion Night

～今宵のテーマ:「データベースに適した
ストレージの管理・設定手法」を語ろう～

ORACLE[®] 12^c
DATABASE

Plug into the Cloud



日本オラクル株式会社
クラウド・テクノロジー事業統括
Database & Exadata プロダクトマネジメント本部

Safe Harbor Statement

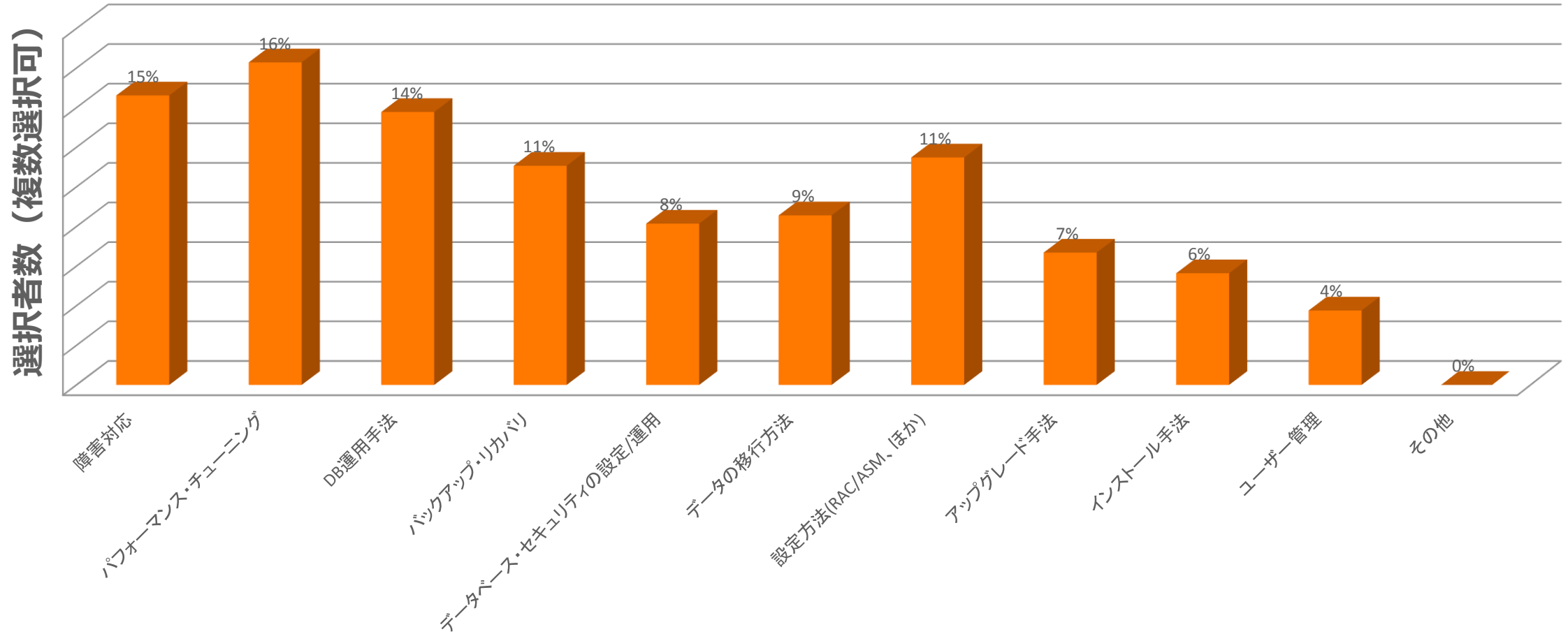
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Technical Discussion Night

～今宵のテーマ:「データベースに適したストレージの管理・設定手法」を語ろう～

- 本当に必要としている技術やTipsについて、熱く語り合いましょう！
 - 今宵のテーマは、技術者の皆様から要望が高かった「ストレージの管理・設定手法」
 - 本当に必要としている「ストレージの管理・設定」の考え方やTips
- ファシリテーター: 田子 得哉
 - 日本オラクル株式会社
クラウド・テクノロジー事業統括
Database & Exadata プロダクトマネジメント本部
本部長

【事前アンケート】データベースを構築、運用する上で、
オラクルの技術情報として必要な情報をお聞かせください。



Topic#1

*Pluggable Database*でASMを
使用する場合の注意点はありますか？

Pluggable Database でASMを使用する場合の注意点は？

ありません！！

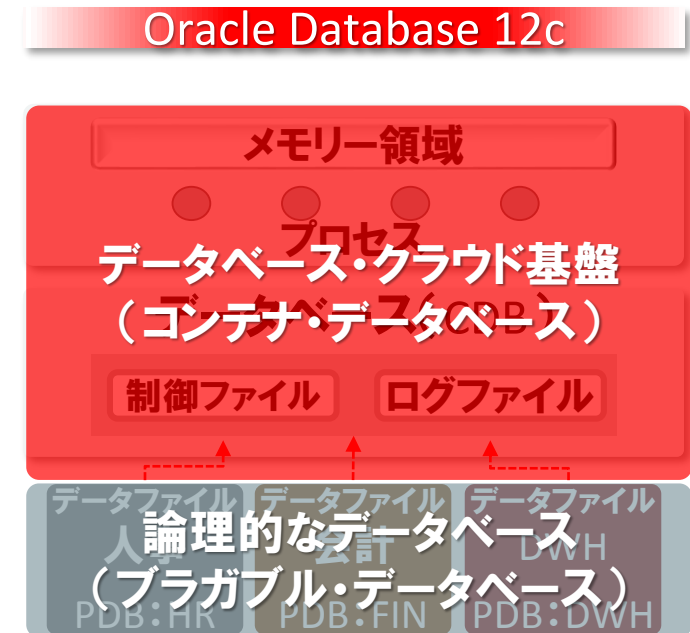
マルチテナント・アーキテクチャ

メモリー、バックグラウンド・プロセスが必要なのは、テナント・データベースのみ

- Non-CDB構成(11gまでと同様の構成)とCDB構成(12c以降で利用可能なMultitenant Architecture構成)の違い



Non-CDB構成



CDB構成

ファイル・システムでもOMFのご利用を推奨します

- Oracle Managed Files(OMF)

- データベースがファイルを自動的に作成、命名および管理するファイル・システム・ディレクトリを指定

- DB_CREATE
ONLINE_LOG_DEST_n
DB_RECOVERY_FILE_DEST

- Oracle 9i から提供開始

- ASMでも利用されている機能

- マニュアル

- Oracle Database 管理者ガイド 12cリリース1 (12.1)
 - 17 Oracle Managed Filesの使用

- Pluggable Databaseの作成およびリモート・クローン

- OMFの場合(ファイルシステム/ASM)

```
SQL> create pluggable database pdb_omf
      admin user admin identified by password;
プラガブル・データベースが作成されました。
```

```
SQL> create pluggable database pdb_test
      from pdb_prodcution@dblink;
プラガブル・データベースが作成されました。
```

- OMFではない場合

```
SQL> create pluggable database pdb_nonomf
      admin user admin identified by password;
*
行1でエラーが発生しました。:
ORA-65016: FILE_NAME_CONVERTを指定する必要があります
```


Topic#2

*Enterprise Manager*でASMを管理、
監視する為に便利な画面があったら
教えてください。

Enterprise ManagerでASMを管理、監視する為に
便利な画面があったら教えてください

あります！！

視覚的・直感的に使用量が確認可能

ディスク・グループ

パフォーマンス ディスク・グループ ユーザー ASMクラスタ・ファイルシステム

作成 すべてマウント すべてディスマウント

マウント ディスマウント リバランス チェック 修正 削除

すべて選択 | 選択解除

選択	名前 ▲	マウント済	ディスマウント済	冗長性	スパース・タイプ	サイズ(GB)	使用量(GB)	使用率(%)	使用可能な空き領域(GB)	メンバー・ディスク
<input type="checkbox"/>	DATA_H2	2	0	HIGH	非スパース	33,576.00	9,641.87	28.72	7,045.38	24
<input type="checkbox"/>	DATA_L2	2	0	HIGH	非スパース	33,573.00	3,007.10	8.96	9,256.05	24
<input type="checkbox"/>	DBFS_DG	2	0	HIGH	非スパース	608.59	14.45	2.37	175.51	20

ヒント 使用可能な空き領域は、データに安全に使用できる領域の大きさを示します。0(ゼロ)より大きい値は、ディスク障害の後、冗長性が適切にリストアされることを示します。
 ヒント 「すべてマウント」および「すべてディスマウント」操作では、「ディスク・グループの自動マウント」パラメータで指定されているディスク・グループのみがマウントおよびディスマウントされます。

グラフィカルに容量監視可能。
閾値もプリセット済みなので、空き容量が枯渇したらアラートが上がる

※使用可能な空き容量とは、冗長性を考慮した上での使用可能な空き領域
(マイナスになっても、物理的に空き領域があれば利用はできますが、障害発生時の冗長性回復が保証されません)

ディスクグループ内のデータベースごとの使用量が把握可能
(ASM コマンドでは出来ないこと)

ディスク・グループ: DATA_H2

一般 パフォーマンス テンプレート ファイル アクセス制御 ボリューム

一般

名前 DATA_H2
状態 MOUNTED
冗長性 HIGH
合計サイズ(GB) 33,576
保留中の操作 0
割当て単位(MB) 4

拡張属性

データベースの互換性 11.2.0.4.0
ASMの互換性 12.1.0.2.0
ASMボリュームの互換性 12.1.0.2.0
ディスク修復時間(時間) 3.6
スマート・スキャン機能 有効
ファイル・アクセス制御 無効
障害グループ修復時間(時間) 24.0
ディスク・グループ・コンテンツ Data
シン・プロビジョニング済 無効
コンテンツ・チェック 無効
スパース・タイプ 非スパース

現在のディスク・グループの使用量(GB)

空き領域(23,934.13)
システム(0.69)
ASM(0.00)
DBM01(9,028.03)
DBM02(613.15)

空き領域の表示

ヒント レポートされた領域は、デバイスではRAWサイズです。実際の使用可能領域は、冗長要件のため、空き領域より少ないことがあります。

視覚的・直感的に使用量が確認可能

ディスク・グループ: DATA_H2

一般 | パフォーマンス | テンプレート | **ファイル** | アクセス制御 | ボリューム

このディスク・グループ内のサービスされたデータベースに関連するディレクトリ、ファイルおよび別名は次のとおりです。

別名の作成 | ディレクトリの作成 | 名前の変更 | ファイル・プロパティの編集 | 修正 | 削除

すべて選択 | 選択解除 | すべて開く | すべて閉じる

選択	名前	物理サイズ(KB)	論理サイズ(KB)	プライマリ・リージョン	ミラー・リージョン	権限			所有	
						所有者	グループ	その他	所有者	グループ
<input type="checkbox"/>	DATA_H2									
<input type="checkbox"/>	▶ ASM									
<input type="checkbox"/>	▶ DBM01									
<input type="checkbox"/>	▶ CHANGETRACKING									
<input type="checkbox"/>	▶ CONTROLFILE									
<input type="checkbox"/>	▶ DATAFILE									
<input type="checkbox"/>	JPET.274.917.289473	7549808640	2516582408	COLD	COLD	Read-write	Read-write	Read-write		
<input type="checkbox"/>	SYS_AUX.261.915658185	50356224	16777224	COLD	COLD	Read-write	Read-write	Read-write		
<input type="checkbox"/>	SYSTEM.260.915658185	50356224	16777224	COLD	COLD	Read-write	Read-write	Read-write		
<input type="checkbox"/>	UNDOTBS1.262.915658187	50356224	16777224	COLD	COLD	Read-write	Read-write	Read-write		

さらに、ASM ディスクグループ内での DB ファイルごとの使用量も確認可能

ASM メンテナンスも画面から直感的に実施が可能

選択	ディスク	障害グループ	パス	ライブラリ	グリッド・ディスク	読み込み/書き込みエラー	状態	モード	サイズ (GB)	使用量 (GB)	使用
<input checked="" type="checkbox"/>	DATA_H2_FD_07_AORICEL06	AORICEL06	0\192.168.208\3:192.168.208\4\DATA_H2_FD_07_aorice106	CELL	DATA_H2_FD_07_aorice106	0	NORMAL	✓	1,399.00	401.66	
<input checked="" type="checkbox"/>	DATA_H2_FD_01_AORICEL04	AORICEL04	0\192.168.207\9:192.168.208\0\DATA_H2_FD_01_aorice104	CELL	DATA_H2_FD_01_aorice104	0	NORMAL	✓	1,399.00	401.70	
<input type="checkbox"/>	DATA_H2_FD_05_AORICEL05	AORICEL05									

ASM のメンテナンスも、2ステップ程度で画面から実施可能。

確認

選択したディスクがオフラインになると、ASMインスタンスは「ディスク修復時間」で指定した期間を待機してから、ディスクを削除します。「ディスク修復時間」の期間中、ディスクを修復してオンラインにすることが可能です。正常にオンラインになった各ディスクについては、保留中の削除操作が取り消され、再同期化の操作が開始されます。

次のディスク DATA_H2_FD_07_AORICEL06, DATA_H2_FD_01_AORICEL04 をオフラインにしますか。

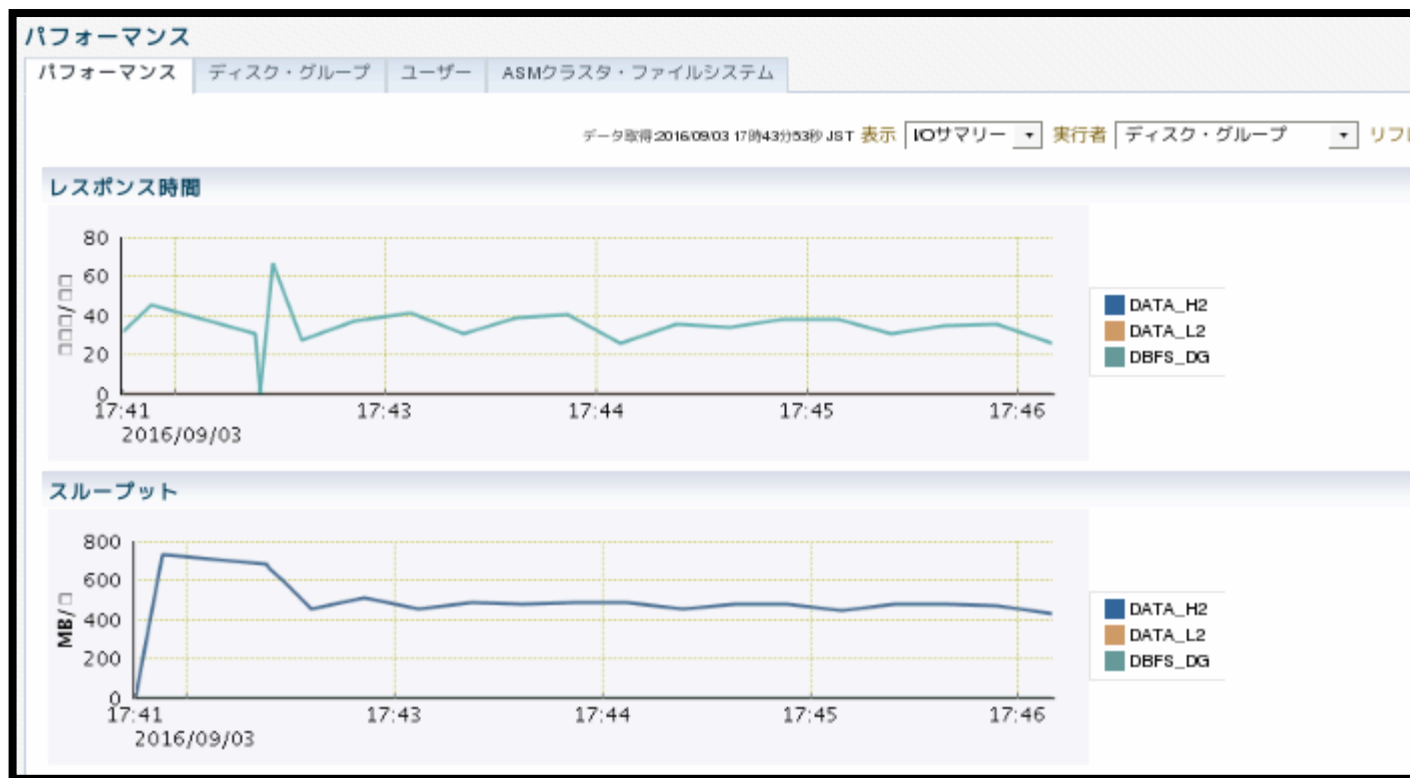
ディスク修復時間 時間

指定した時間が経過した後、ディスクは削除されます。ディスクを修復するのに十分な期間を指定してください。1日を超えるなどの大きい値を指定した場合、データ損失の可能性が高くなることに注意してください。これは、指定の間中はディスク・グループのファイルがより低い冗長性で保護されるためです。

ASM コマンドに慣れていない場合にも「SQL表示」をすることで、コマンドの学習も可能

```
ALTER DISKGROUP DATA_H2 OFFLINE DISK DATA_H2_FD_07_AORICEL06 DISK DATA_H2_FD_01_AORICEL04 DROP AFTER 3.6 h
```


パフォーマンス確認もグラフィカルに確認可能



統計情報から、手動でグラフ化するのは大変な作業だが、EM では、ディスクグループごとの IO パフォーマンスをグラフが用意されている

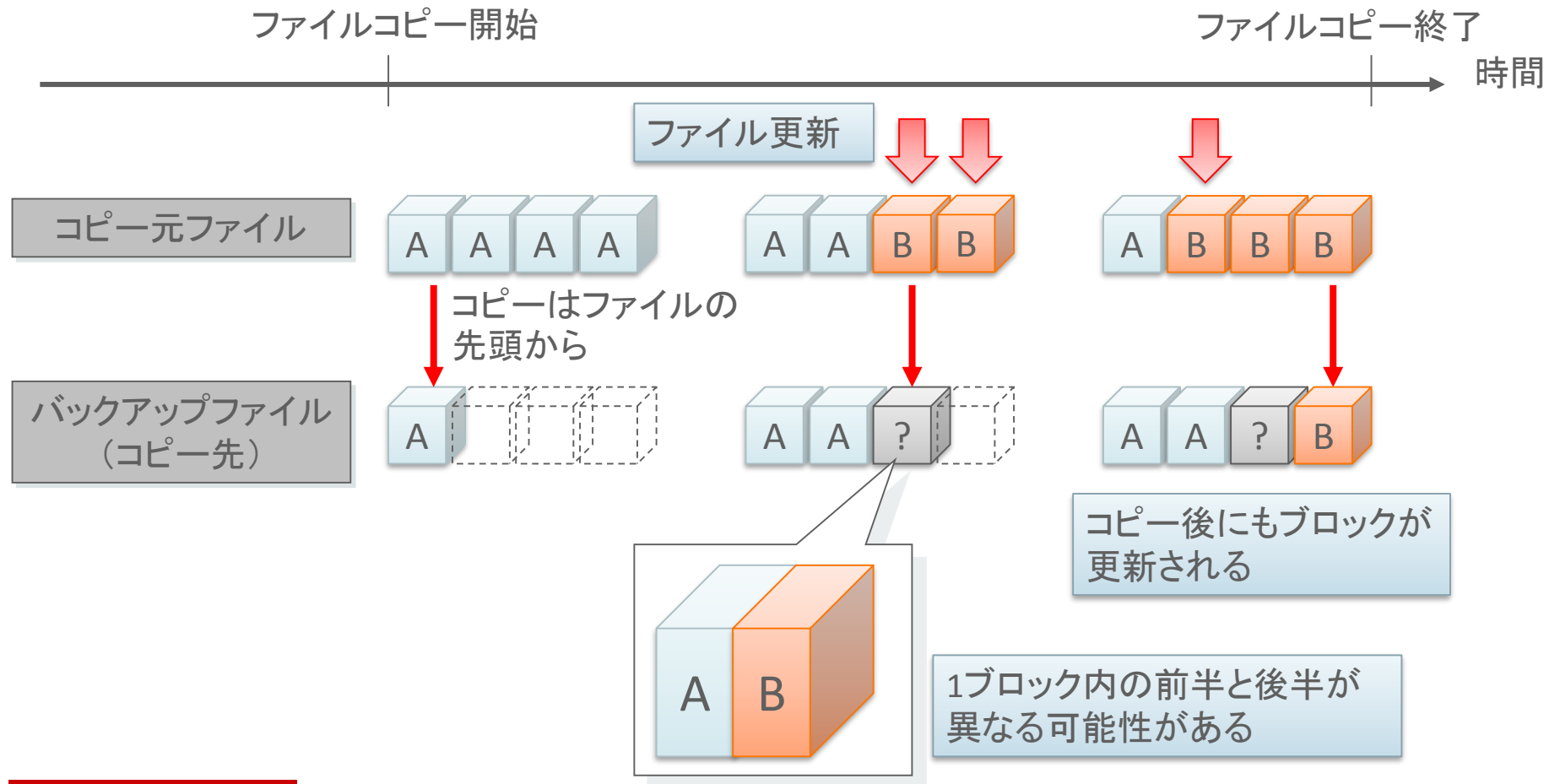
Topic#3

ASM構成におけるストレージ機能を使ったバックアップ方法は？

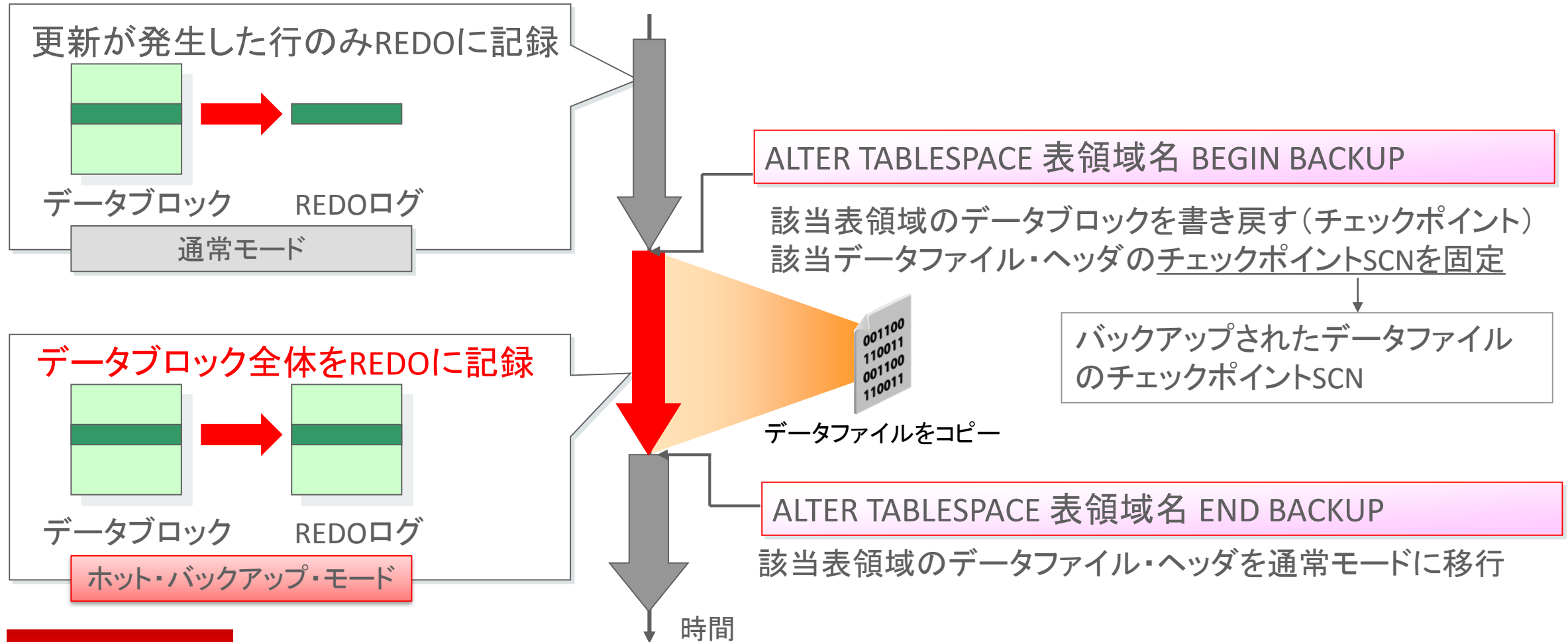
- バックアップ・モード
 - オンライン・バックアップを取る場合
- ASM Disk Group の分け方
 - 最低3つのグループ
 - リストアの要否、タイミングが異なる

更新され続けるファイルのコピー

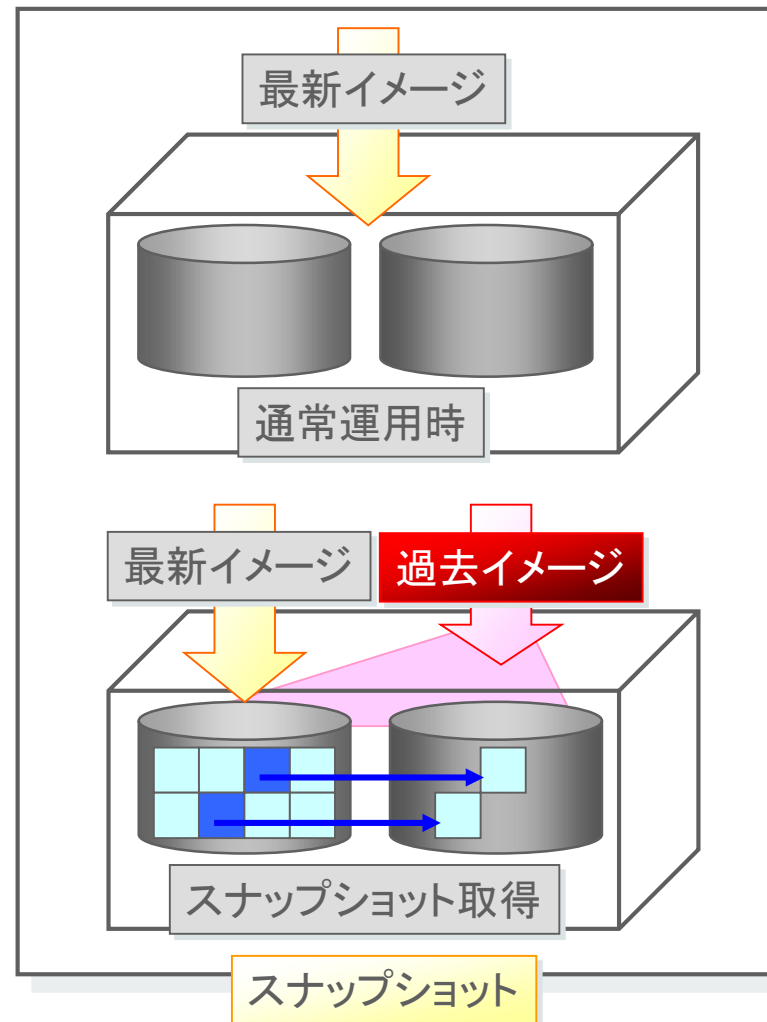
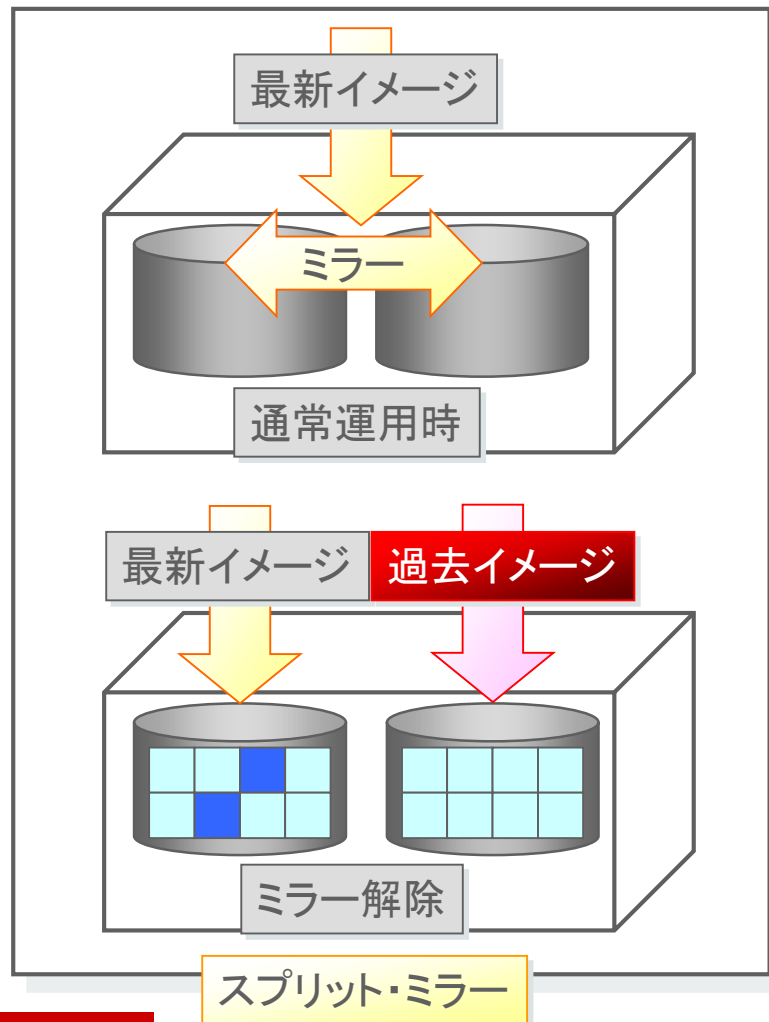
ユーザ管理バックアップでのホット・バックアップ



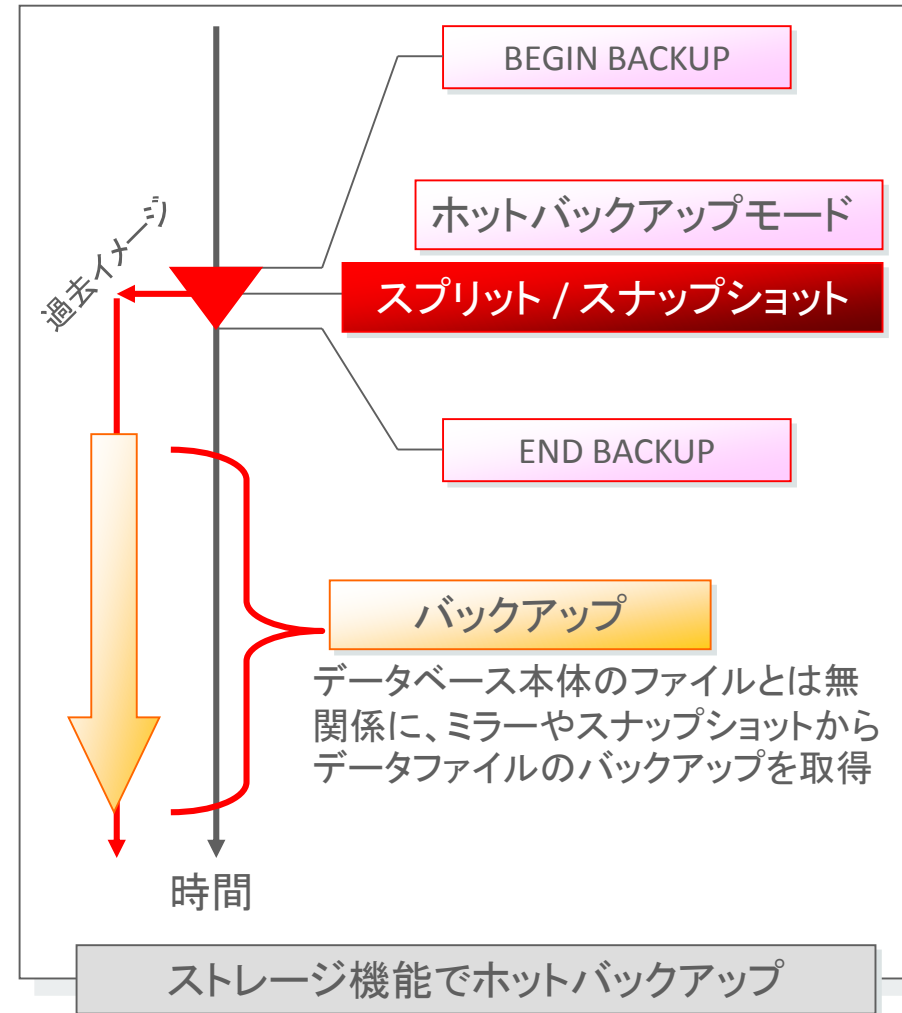
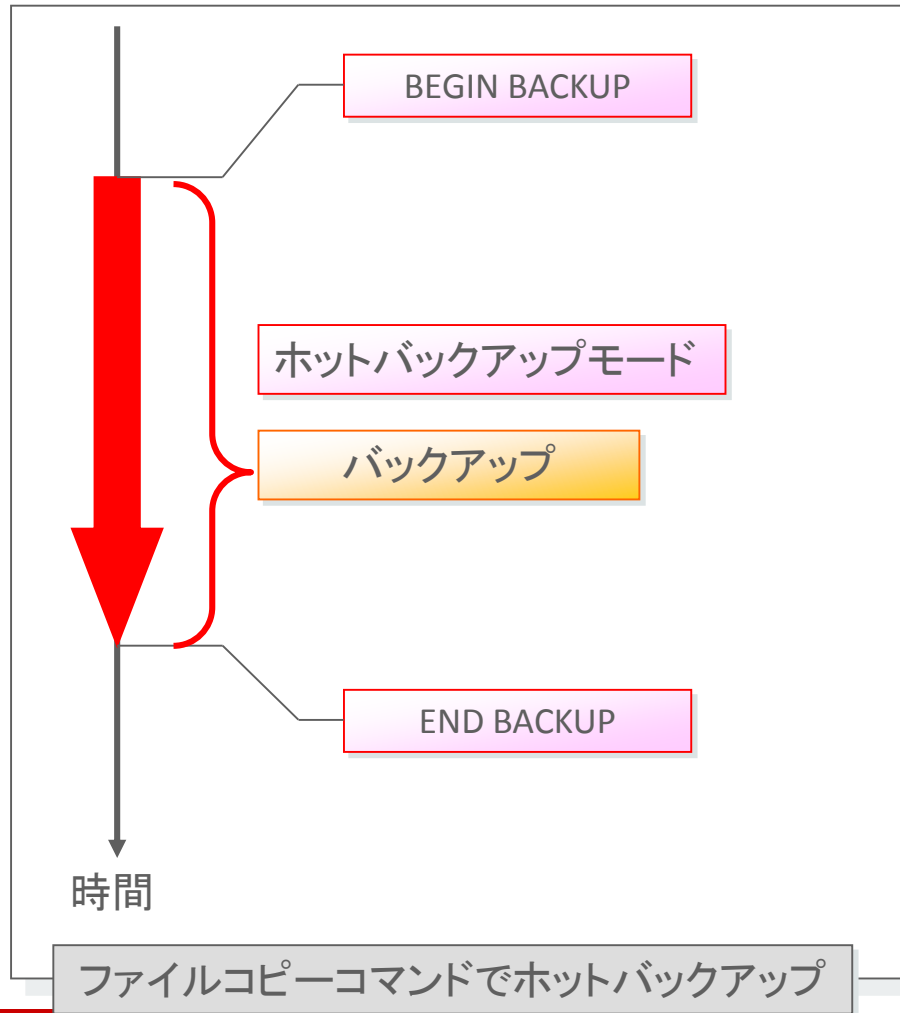
ホット・バックアップモード



スプリット・ミラーとスナップショット



ストレージ機能でホット・バックアップ



ホット・バックアップからのリカバリにはREDOが必要

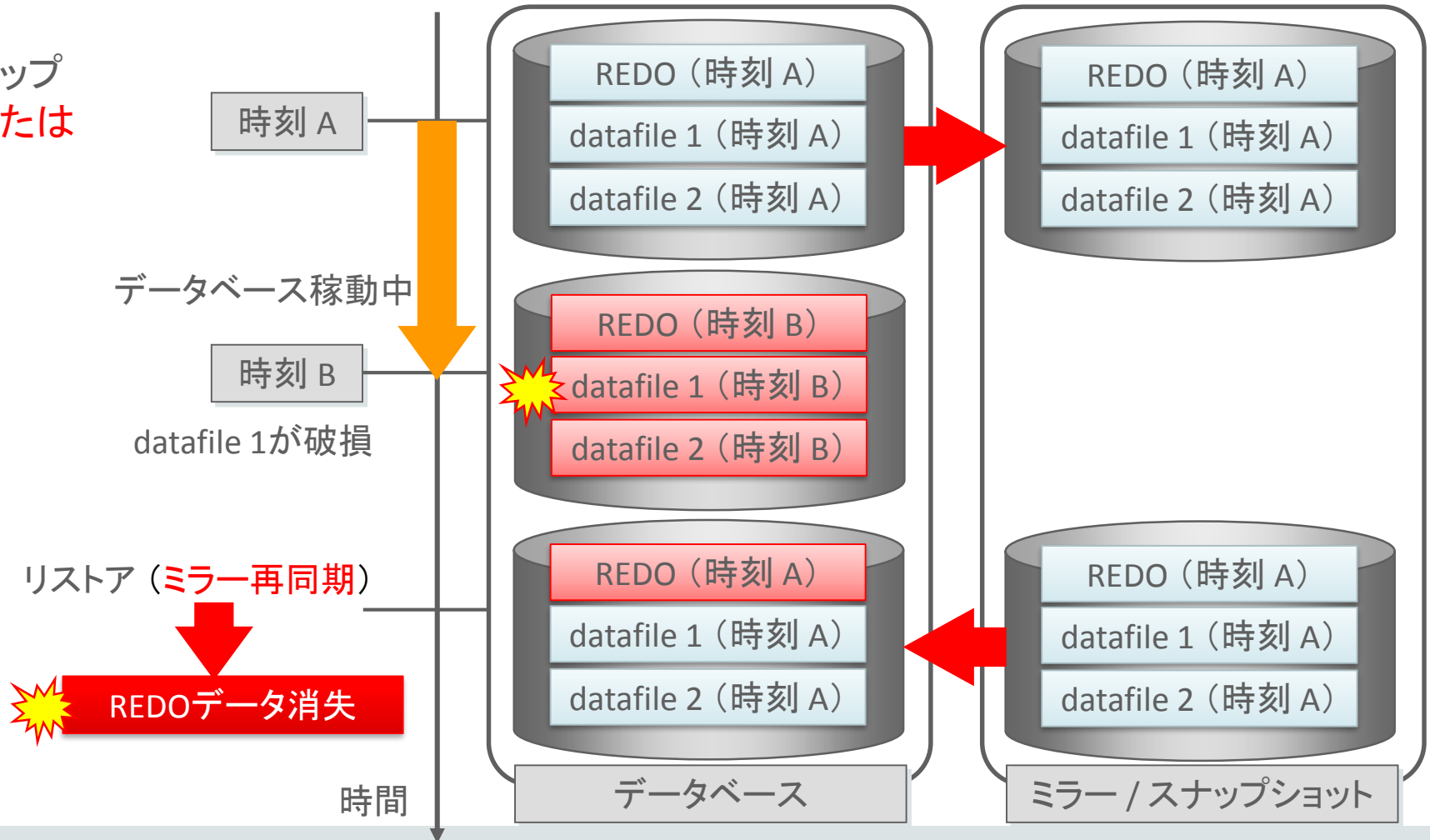
ストレージ機能を使用したバックアップからのリストア・リカバリ

- スプリットしたストレージ・ボリュームは、サーバーの電源をいきなり落としたのと同じ状態になっている
 - REDOを使ったリカバリが必要となる
- リストア / リカバリできるようにバックアップ設計を行うこと
 - なんでもボリューム再同期が使用できるとは限らない
 - 上書きして良いファイル、悪いファイルがあるので、適切にボリュームを切る必要がある

リカバリ不能になるケース

REDOとデータファイルを同じボリュームに格納していると

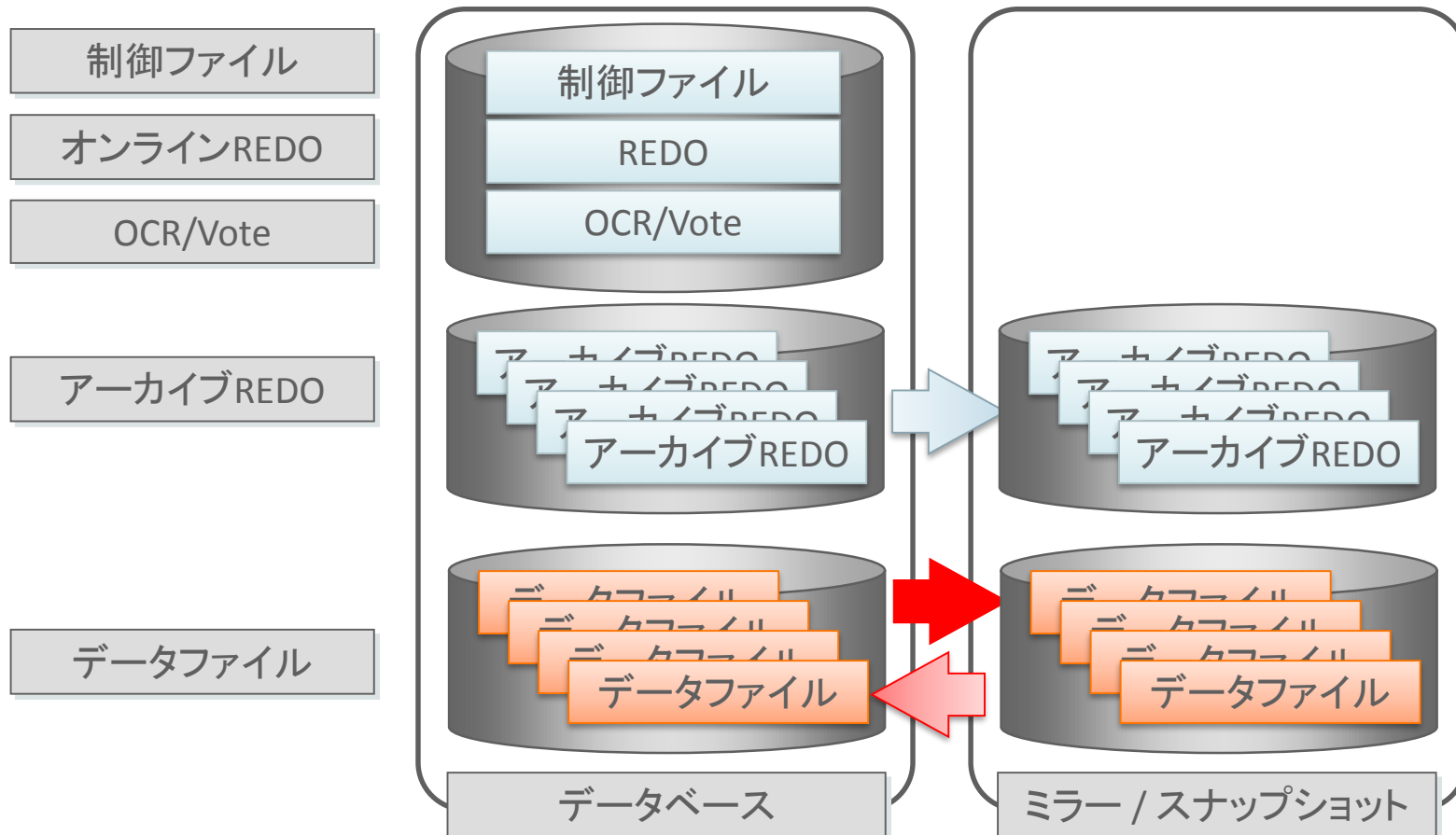
ストレージ機能でバックアップ
(オンラインREDOかつ、または
アーカイブREDO込み)



REDOが格納されている
ボリュームを上書きすると
リカバリ不能に！

スプリット / スナップショットのグループを分ける

REDOを上書きしないように



OCR/Votingはocrconfigを使ってバックアップ・リカバリ

再同期すると、スプリット後のアーカイブREDOを失う



ファイルとして取り出す

再同期すると、正常ファイルも上書きされる ⇒ リカバリが増える



ファイルとして取り出すことも検討する

スプリット・ミラーのガイドライン

- 次の条件を満たす必要がある
 - 全てのLUでPoint-in-Timeスプリット可能、各LUのスプリットが同じ時刻
 - 全LUが書込み完了を守り、アトミックにスプリットされ、書込み順序性が保たれる
 - オンライン・バックアップ・モードでストレージをスプリット
 - データ領域とアーカイブログは別ディスクグループにある
- 多くのストレージベンダーでは、複数のボリュームを「コンシステンシーグループ」に配置すれば、含まれる全てのLUがアトミックに同時刻で分断される

参考情報

- Supported Backup, Restore and Recovery Operations using Third Party Snapshot Technologies (My Oracle Support Doc ID 604683.1)
- 高可用性システムに適した管理性と性能を向上させる ASM と RMAN の魅力
 - http://otndnld.oracle.co.jp/ondemand/ddd/PDF/MA-4_print_c.pdf

Topic#4

Oracle Supportの観点からの ASM使用時の注意点

Oracle Supportの観点からのASM使用時の注意点

- ASMの冗長性は3重化がオススメな理由
- ASM 12.1で追加されたスクラブ機能は重要です！
 - 次の文では、論理データの破損検査中に検出したエラーの修復を試行します。

```
SQL> ALTER DISKGROUP dgroup_01 SCRUB REPAIR WAIT ;
```

- ASMディスク毎の空き容量を確認しよう！
 - 参考)しばちょう先生の試して納得！DBAへの道
 - 第31回 ASMのストライピングとリバランスによるI/O性能の向上

Topic#5

ストレージ(データファイル)を覗いて みよう ~ Database Security

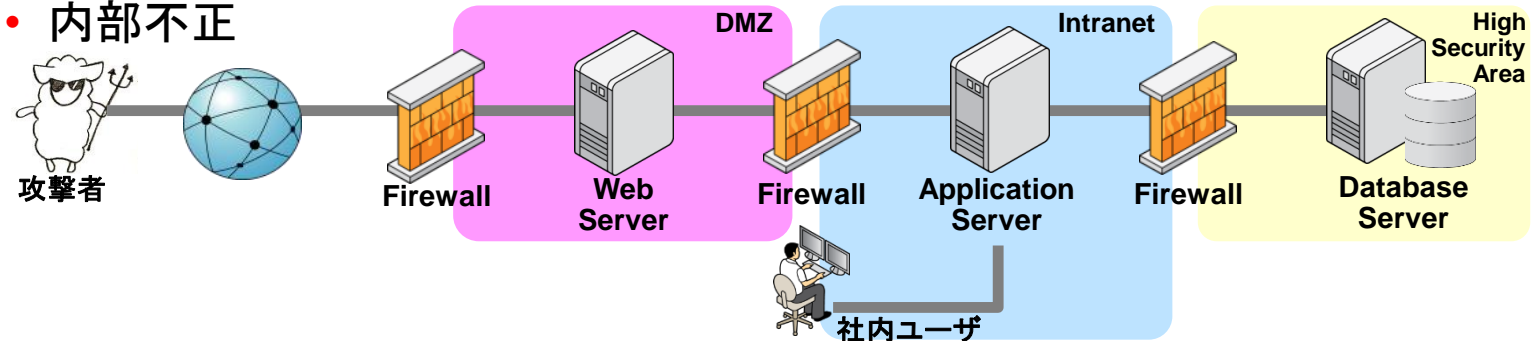
「本来、隔離されているはずのデータベースが どのように攻撃されるのか？」

2013年実施の某セミナー資料より

データベースへの攻撃の例

本来、隔離されているはずのデータベースがどのように攻撃されるのか？

- Webアプリケーションへの攻撃
 - SQLインジェクション
- 標的型攻撃
 - 標的型攻撃メールからの遠隔操作ウイルス
- データベース・ソフトウェアの脆弱性攻撃
- 内部不正



ORACLE

Copyright © 2013, Oracle and/or its affiliates. All right

6

大規模情報漏えい事例

引用: Healthcare Info Security 「Update: Top 5 Health Data Breaches」 (2015年2月5日)
 引用: Reuters, Forbes, USA Today, IT Media, ITPro 等

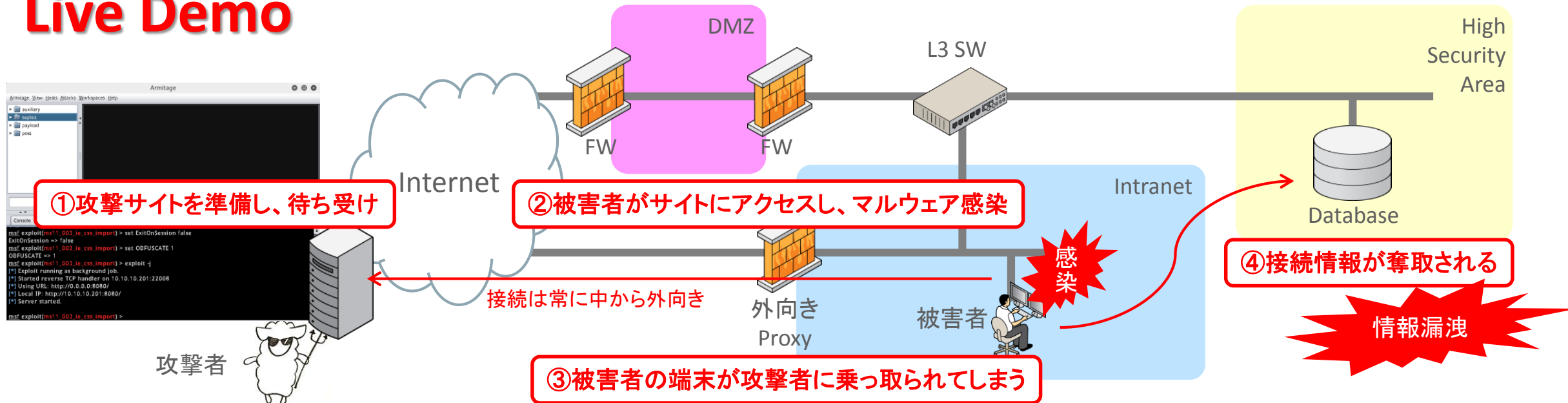
年	企業・団体名	漏洩件数	最終的な漏洩の原因	攻撃手法
2016	国内大手企業	679万件	OSアカウント or DBアカウント	業務端末がマルウェア感染し、サーバー内にデータファイルを作成し、情報を奪取
2015	Anthem (医療保険)	8,000万件	DBアカウント	データベース管理者のログイン情報を活用し、暗号化されていないデータベースの情報を奪取
	Community Health Systems (医療機関)	450万件	OSアカウント	Heartbleedの脆弱性を利用し、N/Wのパケットからログイン情報を奪取し、VPN経由でDBの情報を奪取
2014	eBay (インターネット事業)	12,800万件	DBアカウント	高度サイバー攻撃による従業員のログイン情報入手し、社内ネットワークに侵入しDBの情報を奪取
	国内大手企業	2,300万件	DBアカウント	委託先の職員がDBの管理者権限を使用し奪取
2012	State of South Carolina (州政府)	360万件	OSアカウント	高度サイバー攻撃によるOSアカウントの奪取
2012	Advocate Medical (医療機関)	403万件	PC	泥棒が侵入し、個人情報含む4台のPCが盗難
2011	TRICARE (政府機関)	490万件	バックアップテープ	バックアップテープの紛失

物理盗難

サイバー攻撃では、約50%がユーザーアカウントを奪取して攻撃を行う

実際の攻撃はどのようにおこなわれるのか？

Live Demo



①攻撃サイトを準備し、待ち受け

水飲み場攻撃:

アクセスするだけでマルウェアに感染させるウェブサイト。メールなどで攻撃サイトに誘導したり、被害者がよくアクセスするようなサイトを改ざんしたりする。

②被害者がサイトにアクセスし、マルウェア感染

被害者が攻撃サイトにアクセスすると、アプリ脆弱性をつかれマルウェアをダウンロードしてしまう。

※最新のバージョンのソフトウェアの利用、セキュリティパッチの適用、アンチウイルスソフトの利用などでほぼ対策できる。

③被害者の端末が攻撃者に乗っ取られてしまう(遠隔操作)

ファイルのぞき見/ダウンロード/アップロード、キーロギング、任意のコマンドの実行、近隣端末への感染拡大など。サーバーへの接続情報が狙われる。

※被害者端末側からProxy経由で攻撃者に接続するので、FWがあっても防げないこともある。

④-1. DBサーバーのOS接続情報が奪取される

データファイルがのぞき見られて情報漏洩(ASMでもボリュームが直接参照されると漏洩)!

④-2. DBの接続情報が奪取される

データベースに接続されて、情報漏洩!
特にSYS、SYSTEMなどの管理権限が狙われやすい。

次回予告

Technology Night 第4弾

ORACLE[®] 12^c
DATABASE

会社帰りに参加できる夕方開催セミナー

Oracle Database Technology Night

～集え！オラクルの力（チカラ）～

～えっ、知らなかったでは済まされない。
データベース・セキュリティの勘所～

Oracle Databaseは優れたセキュリティ機能を提供し、セキュアなデータベース環境を構築できます。昨今のサイバー攻撃や内部犯行などの情報漏洩事件からデータを守るために、どのような設計・設定・運用をおこなうべきか、各社にセキュリティ・リスク・アセスメントを提供してきた**データベース・セキュリティに精通したエンジニア**が具体的な**デモ**を交えながら解説させていただきます。

お申し込み・詳細はこちら

11月7日（月）18:45～20:30（受付 18:30より）

<http://www.oracle.com/goto/jpm161107>



Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



Integrated Cloud

Applications & Platform Services

ORACLE®