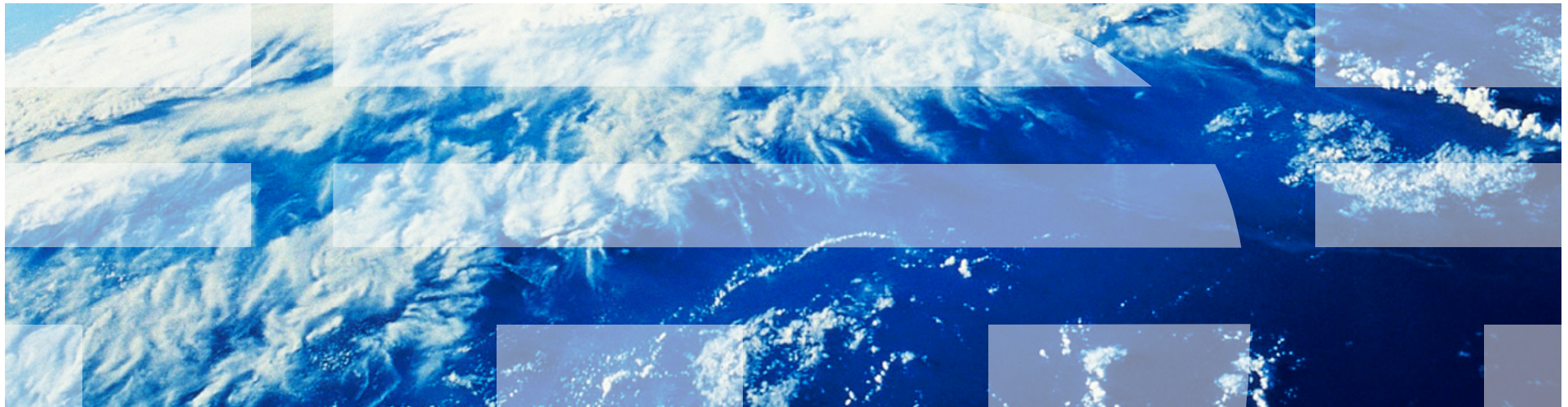


警察庁情報管理システムの合理化・高度化に関する調査研究

報告書（抜粋版）



平成31年 3月 15日
日本アイ・ビー・エム株式会社

-
- I. 認証方式統合方策案の作成**
 - II. データベースの統合方策案の作成**
 - III. バックアップセンター構築の提案**

I. 認証方式統合方策案の作成

1. 認証方式統合方策案の検討方針について
2. 現状の認証方式
3. 現状の課題とその解決方針
4. 認証方式統合方策案①～③
5. 統合方策案の比較

1. 認証方式統合方策案の検討方針について

10システムにおけるID管理、認証、認可の現状を調査し、課題を整理した上で最適な認証統合方策案を検討しました。

2. 現状の認証方式 3. 現状の課題とその解決方針

現状の認証方式を踏まえ、ID管理、認証、認可に加えて、端末も追加要素として課題・問題点を調査しました。また、特にID管理についての課題解決を中心に認証統合方策案を整理しました。

4. 認証方式統合方策案①～③

認証統合方策案を3つ（利用者情報を警察庁へ集約、利用者情報管理を都道府県警察で実施、国費端末VDI化及び端末側での生体情報管理）選定しました。

5. モデルシステム案の比較

3つの案について、集約度、運用性及びコストなどの観点を比較し、最適な認証統合方策案をご提案します。

1. 認証方式統合方策案の検討方針について



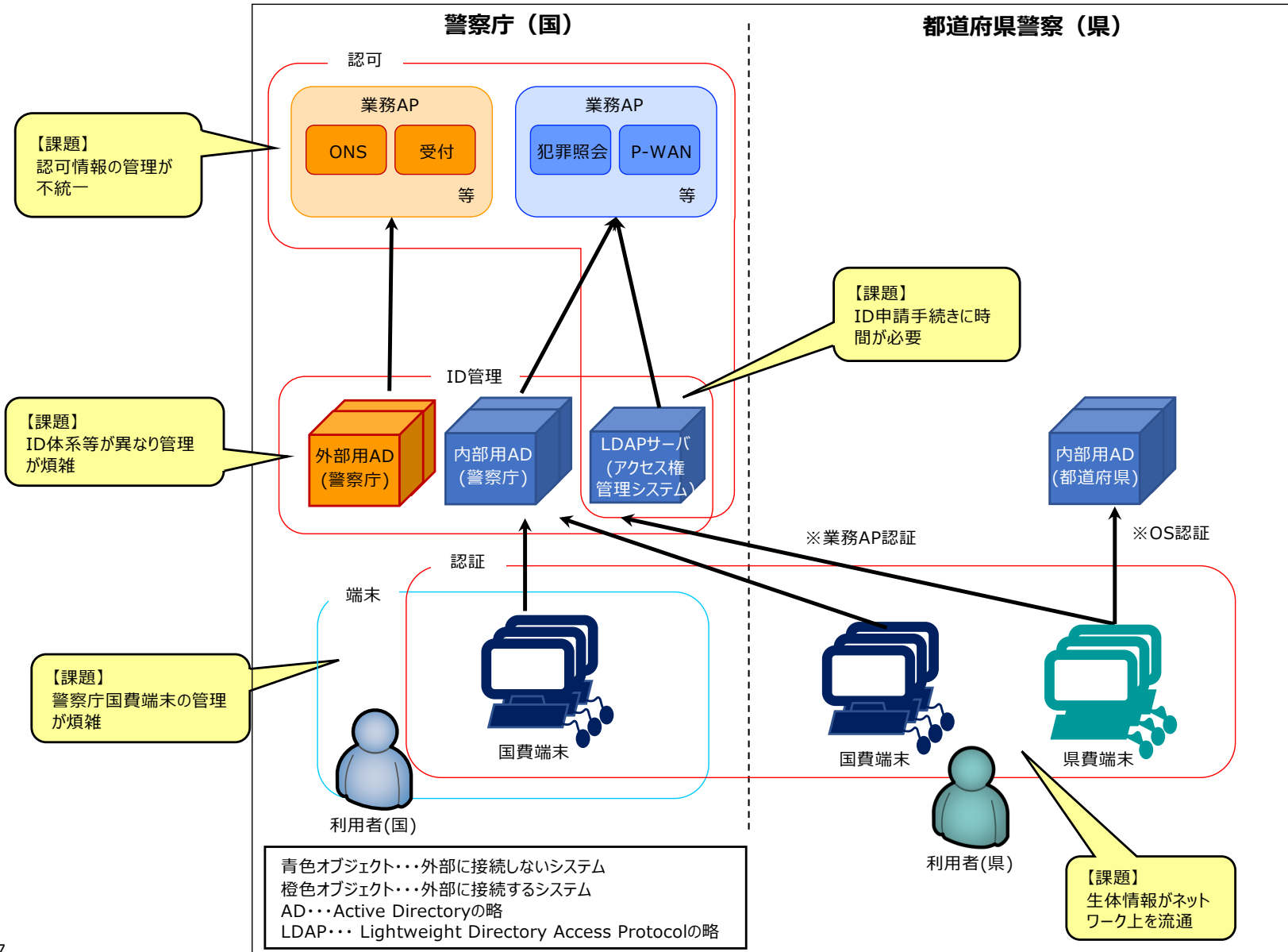
認証方式の統合を実現するためには、「ID管理」、「認証」、「認可」を適切に行うことが必要となります。それぞれの項目は以下のとおりです。

用語	説明
ID管理	利用者を電子的に表現する情報（ID）を組織内のポリシーに基づくプロセスに沿って適切に管理すること
認証	利用者を識別し、本人であることの正当性を確認すること
認可	認証された利用者のシステムの利用可否、利用可能な機能、利用可能な情報の範囲等を定めること

本調査研究では、警察庁様における情報管理システムについて、「ID管理」、「認証」、「認可」の現状を調査し、課題を整理した上で認証統合方策案を検討します。

2. 現状の認証方式

統合対象となる各システムに対して調査シートによる現況調査や対面でのヒアリングを行い、現在の認証方式について整理しました。



3. 現状の課題とその解決方針

現在の認証方式が抱える課題に対し、以下の解決方針を検討しております。

分類	課題の内容	課題の解決方針	解決可能な方策案		
			案①	案②	案③
ID管理	<ul style="list-style-type: none"> ID体系等が異なり管理が煩雑 複数ID所持による利用者負担 ID申請手続きに時間が必要 	(a-1)ID体系の統合	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		(a-2)ID管理を県側で実施		<input type="radio"/>	<input type="radio"/>
認証	<ul style="list-style-type: none"> 認証方式が異なり、管理が煩雑 IDが異なりシステム毎に認証が必要 生体情報がネットワーク上を流通 	(b-1)シングル・サインオンの導入	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		(b-2)生体情報のNW流通防止			<input type="radio"/>
認可	<ul style="list-style-type: none"> 認可情報の管理が不統一 	(c)ID管理基盤へ集約	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
端末	<ul style="list-style-type: none"> 警察庁国費端末管理が煩雑 	(d)国費端末VDI化による管理台数の削減			<input type="radio"/>

 必須検討範囲 追加検討範囲

- 案①：利用者情報を警察庁へ集約（必須検討範囲の解決案）
- 案②：利用者情報管理を都道府県警察で実施（必須検討範囲の解決案）
- 案③：国費端末VDI化及び端末側での生体情報管理（追加検討範囲も含めた解決案）

4. 認証方式統合方策案①



案①：利用者情報を警察庁へ集約

緑色の吹き出し・・・本案で解決される箇所

(a-1) ID体系の統合

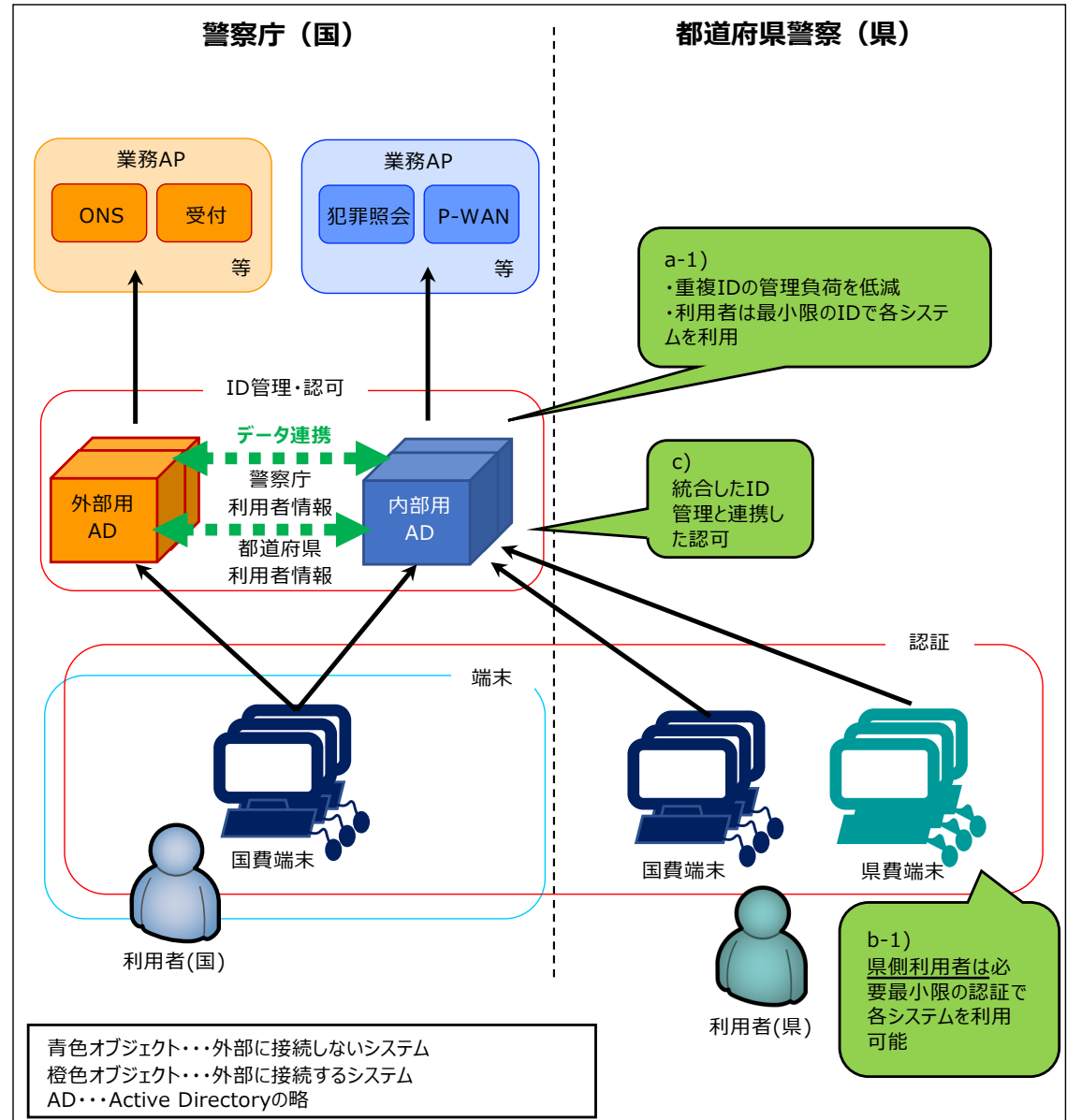
- ・警察庁職員/都道府県警察職員のID体系を統合し集約管理。
- ・内部用/外部用の各ADサーバ間のデータ連携により、重複する利用者情報の変更の同期を自動化、管理負荷を低減。
- ・利用者は最小限のIDで各システムを利用。

(b-1) シングル・サインオンの導入

- ・各システムの業務APの利用において、警察情報システム全体に適用可能なシングル・サインオンを導入。

(c) ID管理基盤へ集約

- ・認可情報の管理をID管理と統合し、各システム個別の認可をID管理と連携した認可機能として実現。



4. 認証方式統合方策案②



案②：利用者情報管理を都道府県警察で実施

…本案で解決される箇所

(a-1) ID体系の統合

・案①と同じ。

(a-2) ID管理を県側で実施

・都道府県警察職員の利用者情報を都道府県警察が管理し、県側におけるID申請手続きに要する時間を短縮。

・各システムとは認証連携を行う。認証連携方式には、事前の連携承認(トラストサークル設定)が必須であるSAMLを採用。

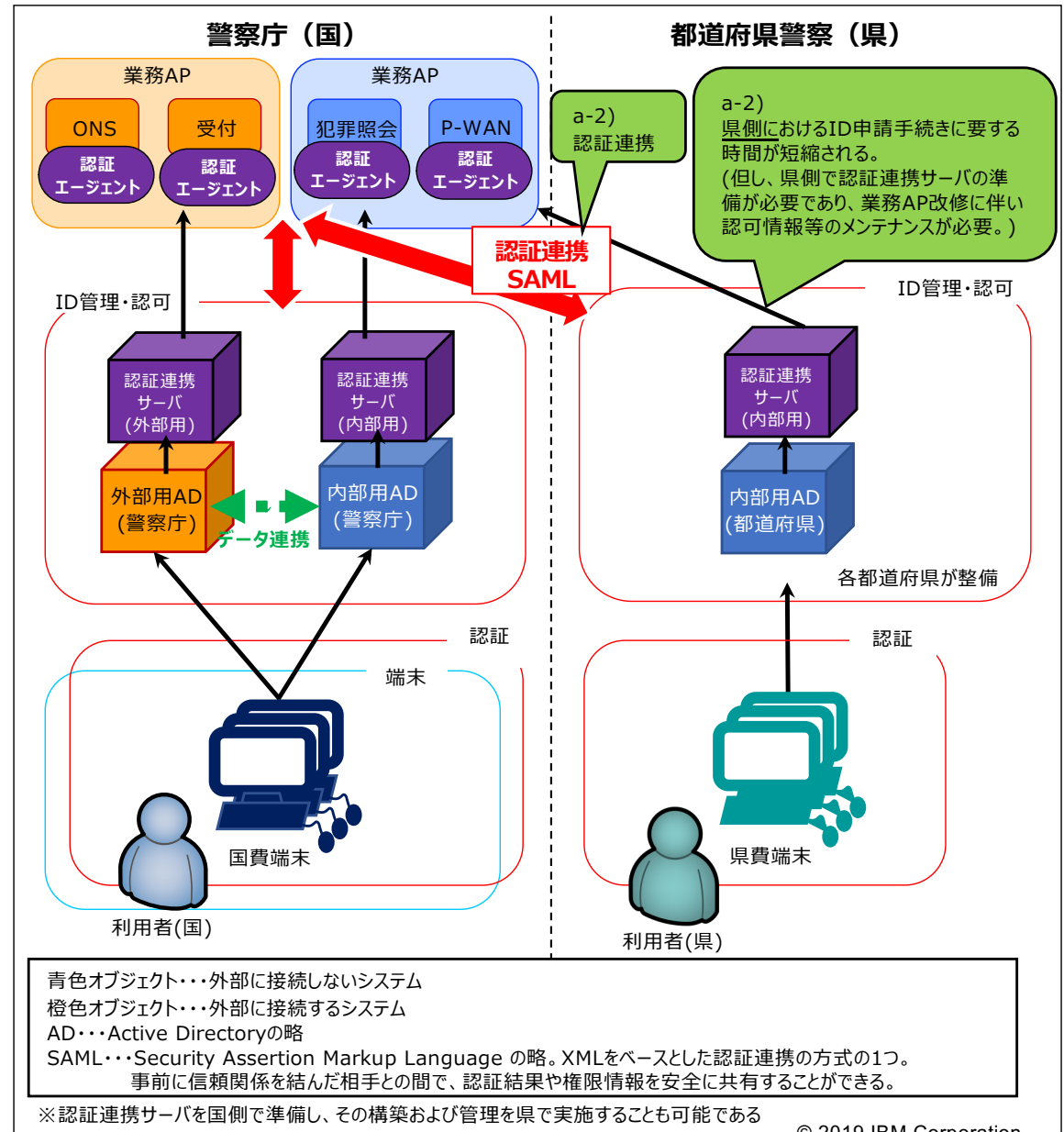
・認証連携サーバ、認証連携エージェントの導入により実現（県側の状況に合わせて段階的な導入も可能）。

(b-1) シングル・サインオンの導入

案①と同じ。

(c) ID管理基盤へ集約

案①と同じ。



案③：国費端末VDI化及び端末側での生体情報管理

…本案で解決される箇所

(a-1) ID体系の統合

案①、②と同じ。

(a-2) ID管理を県側で実施

案②と同じ。

(b-1) シングル・サインオンの導入

案①、②と同じ。

(b-2) 生体情報のNW流通防止

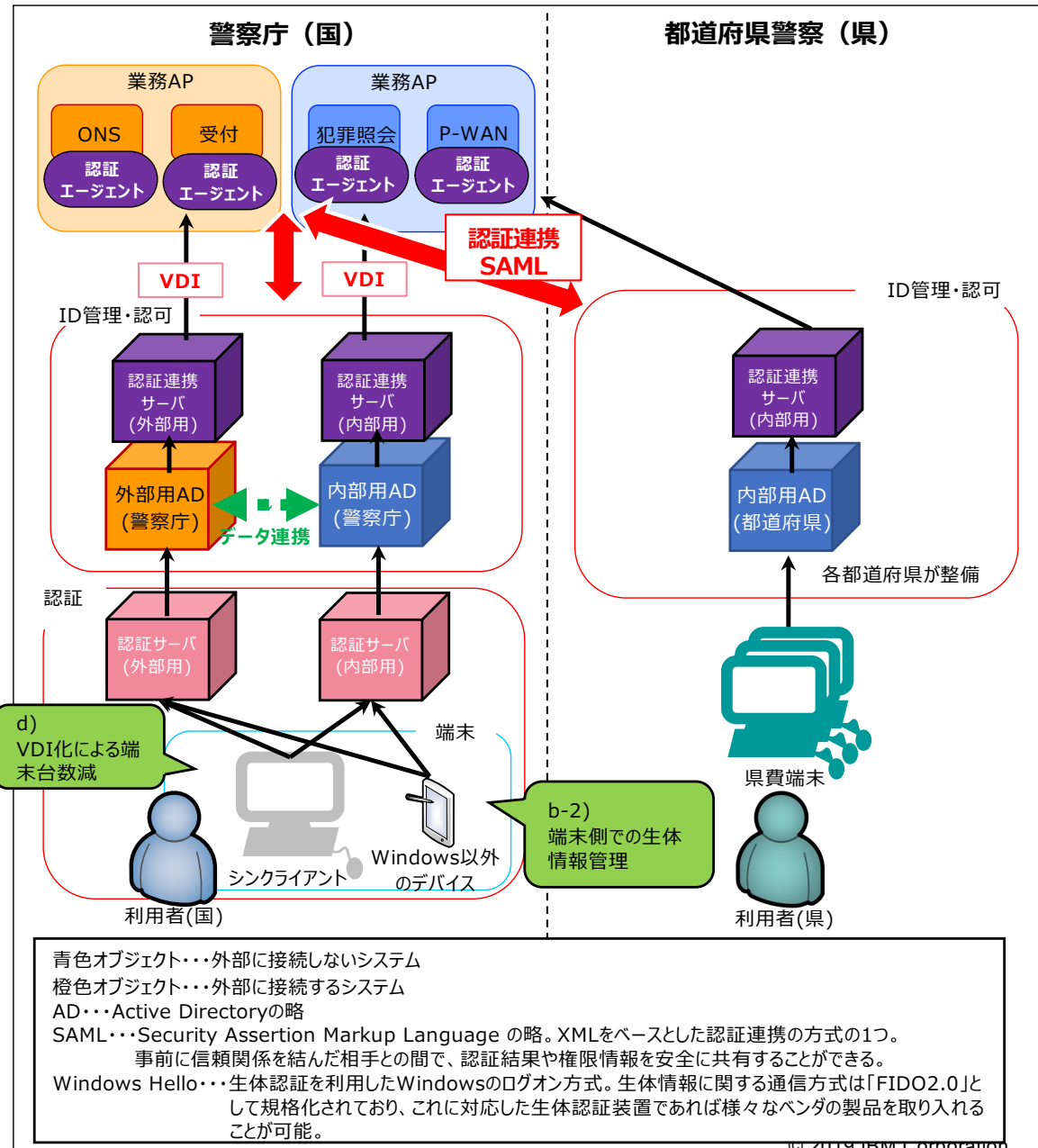
シンクライアントの認証をWindows Helloに統一し、生体情報を端末内に保持することで生体情報をネットワーク上に流通させない。

(c) ID管理基盤へ集約

案①、②と同じ。

(d) 国費端末VDI化による管理台数の削減

国費端末をVDI化。また、Windows以外のデバイスにも対応可能。



5. 統合方策案の比較



項目	案①	案②	案③
集約度	△ ・利用者情報管理サーバがADのみになる。警察庁では、国用AD(内・外)と県用AD(内・外)の4種類を管理。	◎ ・利用者情報管理サーバがADのみになる。警察庁では国用AD(内・外)の2種類を管理。	◎ ・利用者情報管理サーバがADのみになる。警察庁では国用AD(内・外)の2種類を管理。
運用性	△ ・データ連携により利用者情報管理が効率化。 ・但し、ID申請手続きに要する時間は未改善。	○ ・案1に加え、県職員が利用者情報管理を実施することにより、ID申請手続きに要する時間が短縮。	◎ ・案2に加え、警察庁職員の生体情報管理が不要となる。 ※端末毎に生体情報の登録が必要。
拡張性	○ ・利用者が増加してもライセンス等の追加により100万ユーザ程度は十分に対応可能。	○ ・利用者が増加してもライセンス等の追加により100万ユーザ程度は十分に対応可能。	◎ ・利用者が増加してもライセンス等の追加により100万ユーザ程度は十分に対応可能。 ・共通基盤の仕組みを用いることで各システムが他OSのデバイスに対応可能。
コスト	○ ・認証連携サーバの構築、認証連携エージェントの導入が不要。 ・但し、AD台数が他案の2倍必要。	○ ・AD台数が案1の半数。 ・認証連携サーバの構築、認証連携エージェントの導入が必要。	△ ・AD台数が案1の半数。 ・認証連携サーバの構築、認証連携エージェントの導入が必要。 ・端末のVDI化対応が必要。
セキュリティ	○ ・SSO化、生体認証の利用によりパスワード漏えいによる事故を防止。	○ ・SSO化、生体認証の利用によりパスワード漏えいによる事故を防止。	◎ ・生体情報がネットワーク上を流通せず、端末内で安全に管理可能。 ・情報が端末に保存されないため、場所を問わず安全に利用可能。
総評	<p>・案②を認証統合方策案として推奨致します。</p> <p>案①：集約度および運用性に関する改善が不十分 案②：集約度および運用性に関する改善が可能 案③：案②と同様であるが、端末のVDI化によるコストおよびセキュリティ・ポリシーの検討（内部ネットワークと外部ネットワークの論理的接続）が必要 上記から、案②を推奨しますが、長期的な観点（将来構想）として案③は有用と考えます。</p>		

Ⅱ. データベースの統合方策案の作成

1. データベース統合に向けた現状分析および最適化論理データ構造の検討
 - A) 現行データベース論理構造の調査・分析
 - B) 最適化論理データ構造の検討

2. データベース統合方策案の検討
 - A) データベース統合方策案の検討方針
 - B) データベース統合パターン案検討の流れ
 - C) データベース統合パターン案
 - D) 実現性評価
 - E) コスト比較
 - F) データベース統合方策案の比較

1. データベース統合に向けた現状分析および最適化論理データ構造の検討

現行10システムに対するヒアリング調査実施して現行データベースの論理構造を整理し、データベース統合に向けた最適な論理データ構造を検討しました。

2. データベース統合方策案の検討

□ データベース統合方策案の検討方針

データベース統合方策案の検討にあたり、データベース統合の種類について整理し、検討方針を決定しました。（方針：データベースを1つに統合することを検討の開始点とする）

□ データベース統合パターン案検討

データベースを1つに統合した場合の課題・問題点を洗い出し、解決方法としてデータベースを分割して構成しなければならない観点を整理しました。
それぞれの観点への対応方法に応じてデータベース統合パターン案を3つ選定しました。

□ データベース統合方策案の比較

3案について、実現性、リスク、コストなど観点を比較し、最適なデータベース統合方策案をご提案しました。

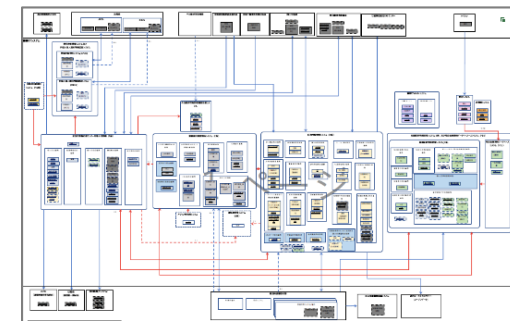
1. データベース統合に向けた現状分析および最適化論理データ構造の検討

A) 現行データベース論理構造の調査・分析

システム間の業務的な共通要素を抽出してデータベースの統合可否を検討するため、現行10システムに対するヒアリング調査結果を整理・分析し、現行データベースの論理構造をモデル図に整理しました。

■ヒアリング内容

1. 業務領域ごとに保持しているデータ
2. 他システムへ連携するデータ



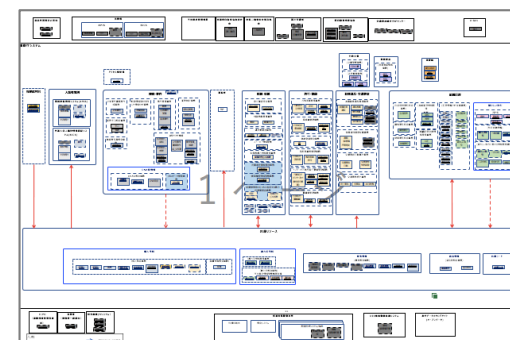
「別紙1）現状データ論理構造モデル図」

B) 最適化論理データ構造の検討

データベース統合に向けて、現行データベースの論理構造を分析し、最適化論理データ構造を検討しました。

■最適化論理データ構造検討の観点

1. システム共通/個別データの識別
2. 業務構造（業務領域）とデータの管理責任
3. 本質的な概念データの類似性による業務領域の統合



「別紙3）最適化論理データ構造モデル図」

2. データベース統合方策案の検討



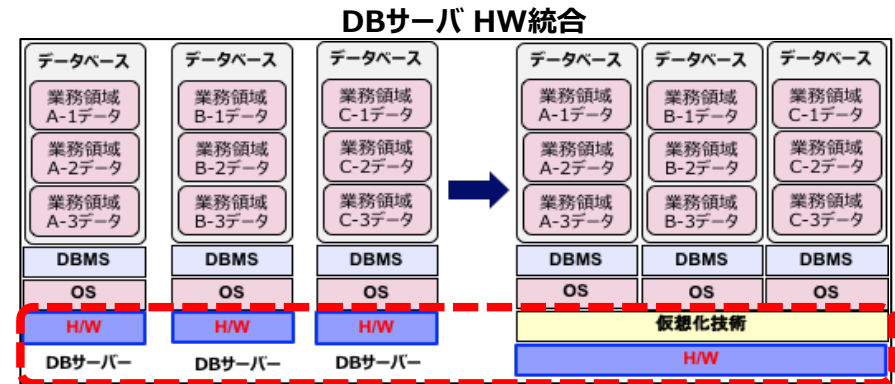
A) データベース統合方策案の検討方針

■ データベース統合方式の種類

a. DBサーバ HW統合

複数DBサーバを1台のHWに統合

→DBサーバ上のOS環境をそのまま1つのHWに統合。

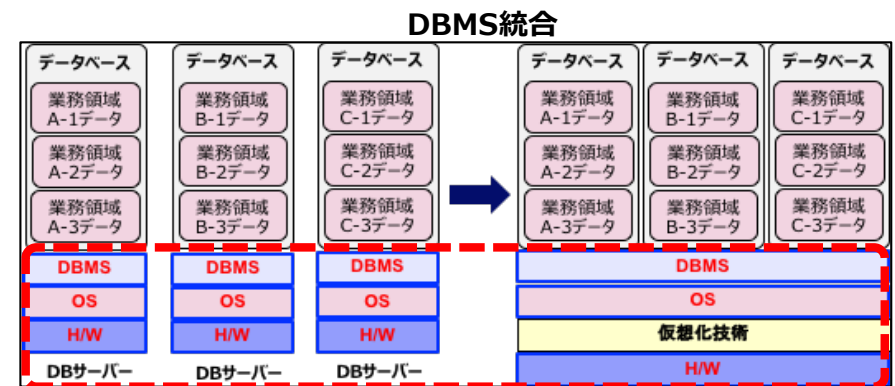


b. DBMS統合

複数データベースを1つのDBMS上へ統合

→データベース単位にDBMSに統合。

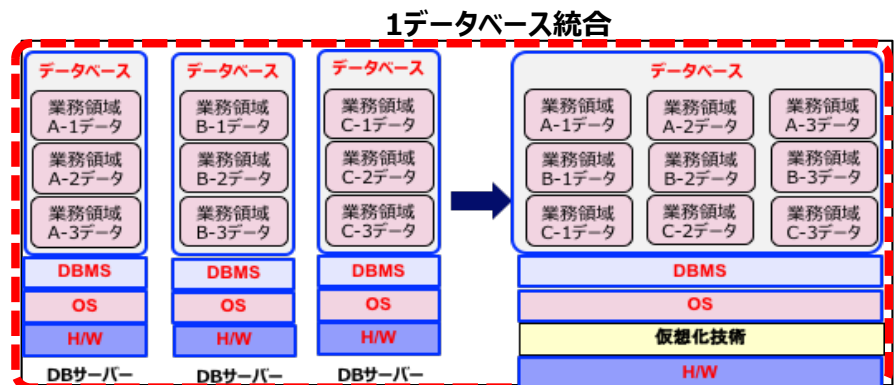
→データベース内部のデータ管理構造はそのまま。



c. 1データベース統合

複数データベースを1つのデータベースへ統合

→各データベース内のデータ管理構造を整理して1つのデータベースへ統合。



2. データベース統合方策案の検討

A) データベース統合方策案の検討方針

■ データベース統合方式の比較

	DBサーバ HW統合	DBMS統合	1データベース統合
特徴	<ul style="list-style-type: none">・複数DBサーバを1台のHWにそのままのOS環境構成で統合	<ul style="list-style-type: none">・複数データベースを1つのDBMS上へデータベース単位に統合・データベース内部のデータ管理構造はそのまま	<ul style="list-style-type: none">・データベース内部のデータ管理構造整理して複数データベースを1つに統合
メリット	<ul style="list-style-type: none">・OS上に構築されているDBMS環境をそのまま移行でき、HW台数を削減可能	<ul style="list-style-type: none">・DBMS上のデータベースをそのまま移行でき、DBMS数を削減可能・HW統合よりOSのリソース効率が良い	<ul style="list-style-type: none">・OSやDBMSのリソース効率が良い・システム間の共通データ集約可能 (データ量削減、データ保守性高い)・システム間のデータ連携削減可能
デメリット	<ul style="list-style-type: none">・OSやDBMSの数が変わらないので、リソース効率や、運用効率が低い	<ul style="list-style-type: none">・既存データベースがそのまま移行されるので、データ集約できない	<ul style="list-style-type: none">・データベース内部のデータ管理構造を統一することで、移行時にアプリケーション側での対応が必要になる可能性あり

2. データベース統合方策案の検討

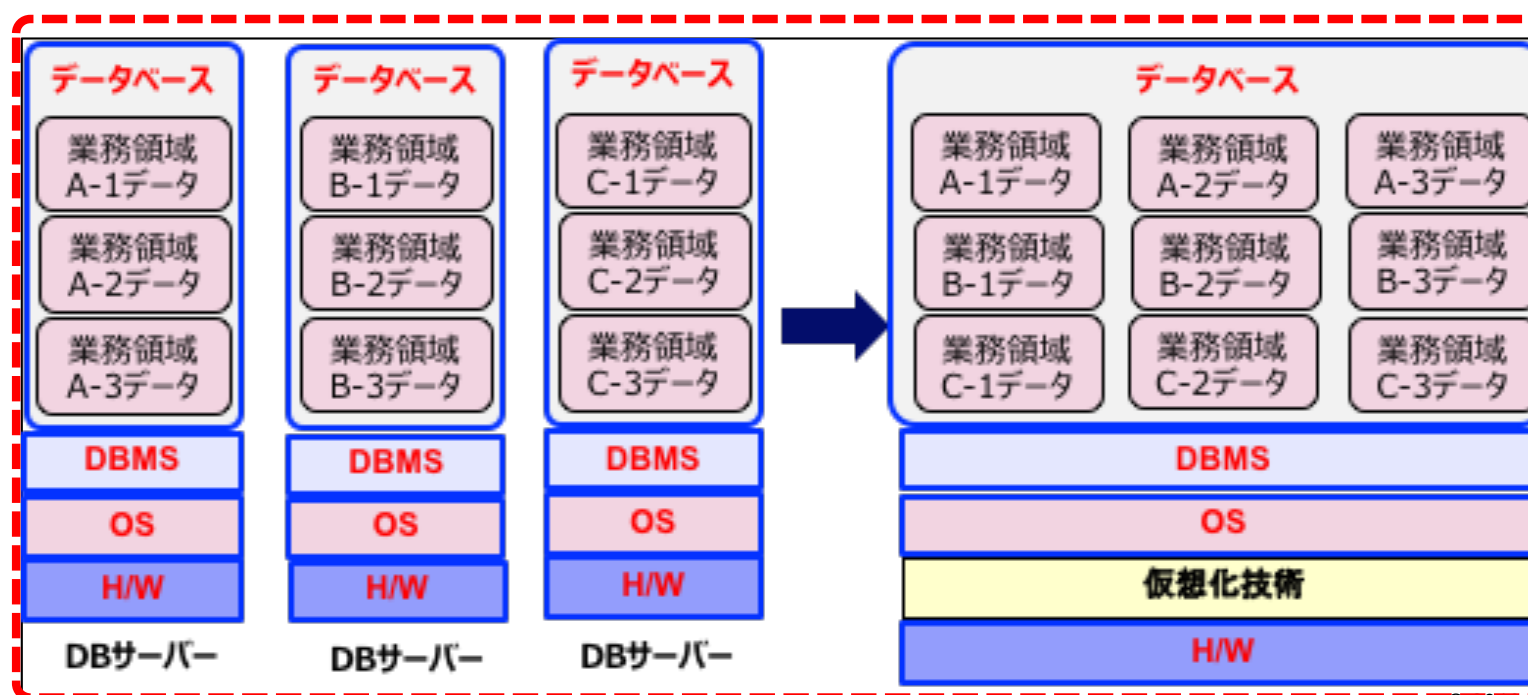
A) データベース統合方策案の検討方針

■データベース統合方策案の検討方針

現行データベースでは、システム間のデータ連携が多数あり、システム間で同様のデータを冗長に保持しているため、「1データベース統合」はリソース効率やシステム間のデータ連携削減の観点で得られるメリットが多いと考えられます。

よって、「1データベース統合」をデータベース統合方策案検討の開始点として検討を行う方針とします。

1 データベース統合



B) データベース統合パターン案検討の流れ

以下の流れでデータベース統合パターン案を検討しました。

(1) データベース統合の課題、解決策検討

データベースを1つに統合した場合の課題の洗い出し

非機能 : 可用性、性能・拡張性、運用・保守性、移行性、セキュリティ

アプリケーション : アプリケーション改修、制約

調達 : 調達スケジュール、調達単位



(2) データベース分割観点の整理

課題を解決するために、データベースをOSから分割しなければならない観点を整理

ネットワーク : セキュリティの観点でアクセスを制限するため、警察庁のみに接続するシステムのネットワーク(内部NW) とインターネットや他省庁、外部機関と連携するシステムのネットワーク(外部NW)でデータベースを分ける

可用性 : システムメンテナンス時などのデータベース起動・停止や災害時のデータベース復旧がデータベース単位で行われるので、可用性が同等のシステムでデータベースを分ける

リスクを回避するために、データベースをOSから分割しなければならない観点を整理

データ量 : 性能の観点で、処理負荷を分散させるため、データ量の閾値でデータベース分ける

B) データベース統合パターン案検討の流れ

以下の流れでデータベース統合パターン案を検討しました。

(3) データベース分割観点による各システムの分割グループ分け

各システムの非機能要件の違いに応じて、複数のデータベース分割観点ごとに各システムをグループ分けする

- 「ネットワーク」 : 内部NW（警察庁内のみで接続するシステムのネットワーク）
 外部NW（インターネットや他省庁、外部機関と連携するシステムのネットワーク）
- 「可用性」 : 最高、高、中、低
- 「データ量」 : 閾値（例えば10TBなど）を超える場合は、サイズで分割



(4) データベース統合パターン案の洗い出し

データベースを分割観点への対応レベルごとにデータベース統合パターン案を選定

データベース統合パターン① : ネットワークの違いでデータベースを分割

データベース統合パターン② : ネットワークの違い、可用性の違いでデータベースを分割

データベース統合パターン③ : ネットワークの違い、可用性の違い、データ量の閾値でデータベースを分割

2. データベース統合方策案の検討

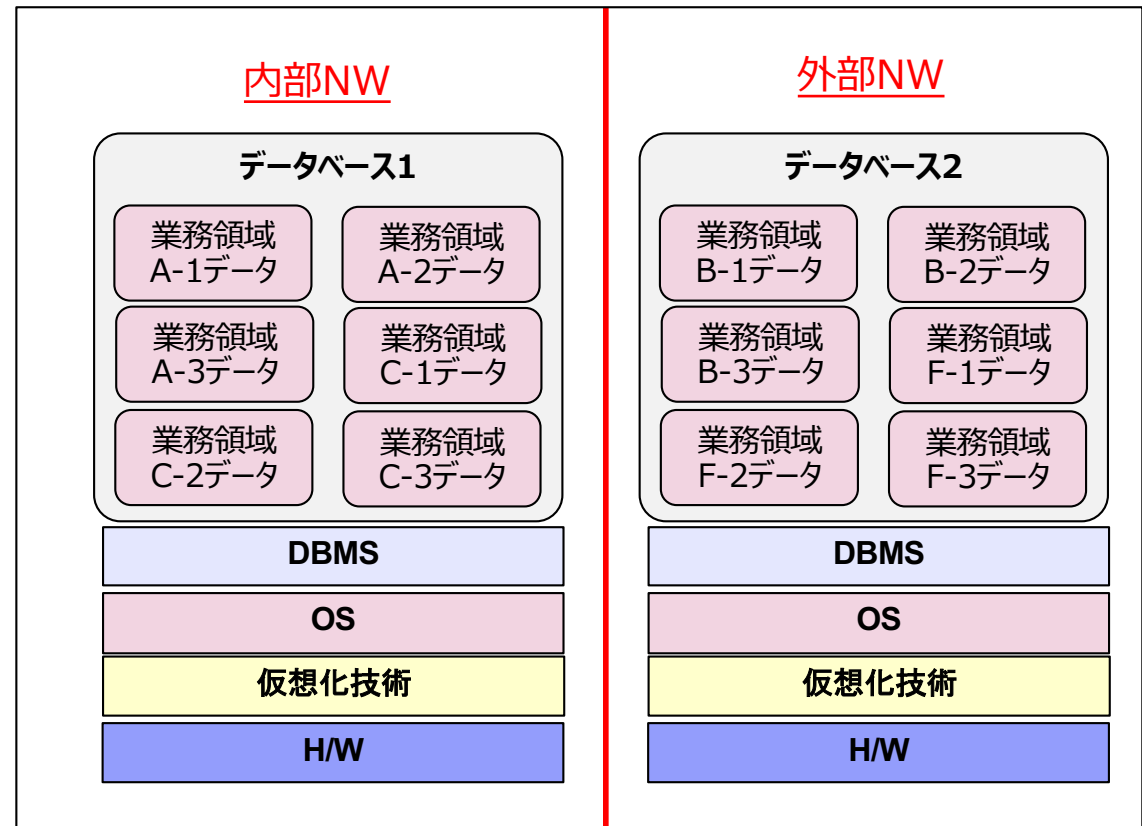
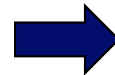
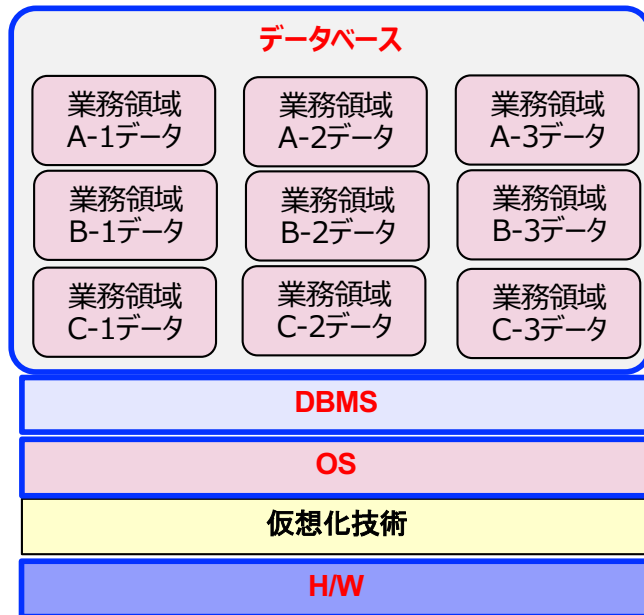
C) データベース統合パターン案

■ データベース統合パターン①イメージ

データベース統合パターン①

(ネットワークの違いでデータベースを分割)

検討開始イメージ (1データベース統合)



2. データベース統合方策案の検討

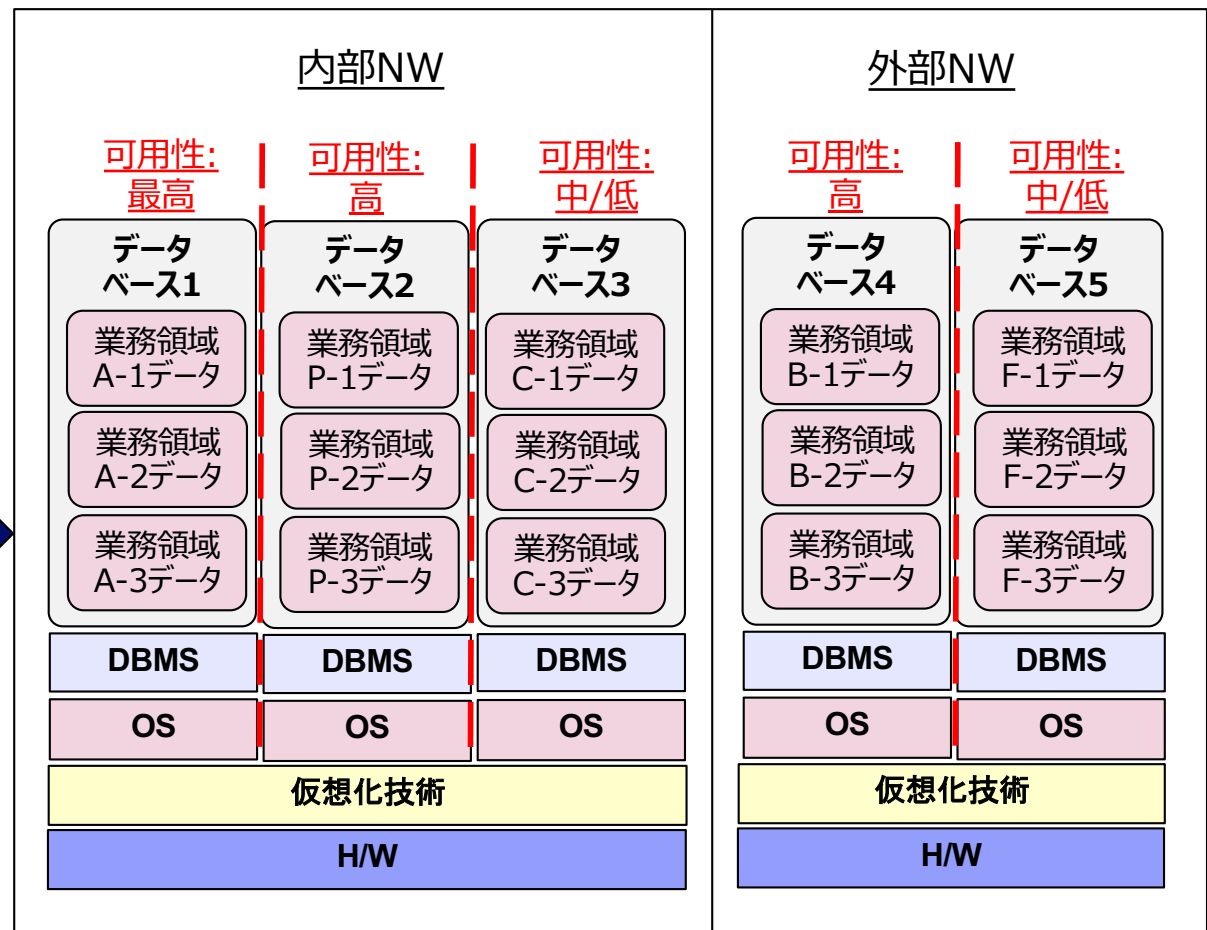
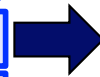
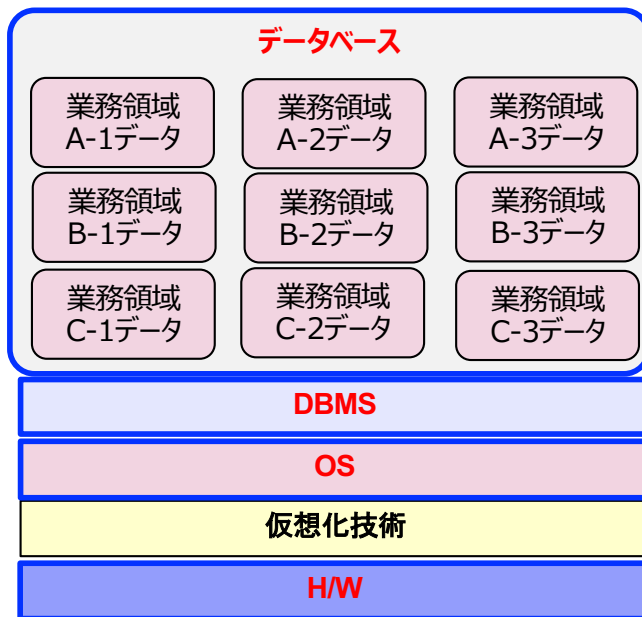
C) データベース統合パターン案

■ データベース統合パターン②イメージ

データベース統合パターン②

(ネットワークの違い、可用性の違いでデータベースを分割)

検討開始イメージ (1データベース統合)



2. データベース統合方策案の検討

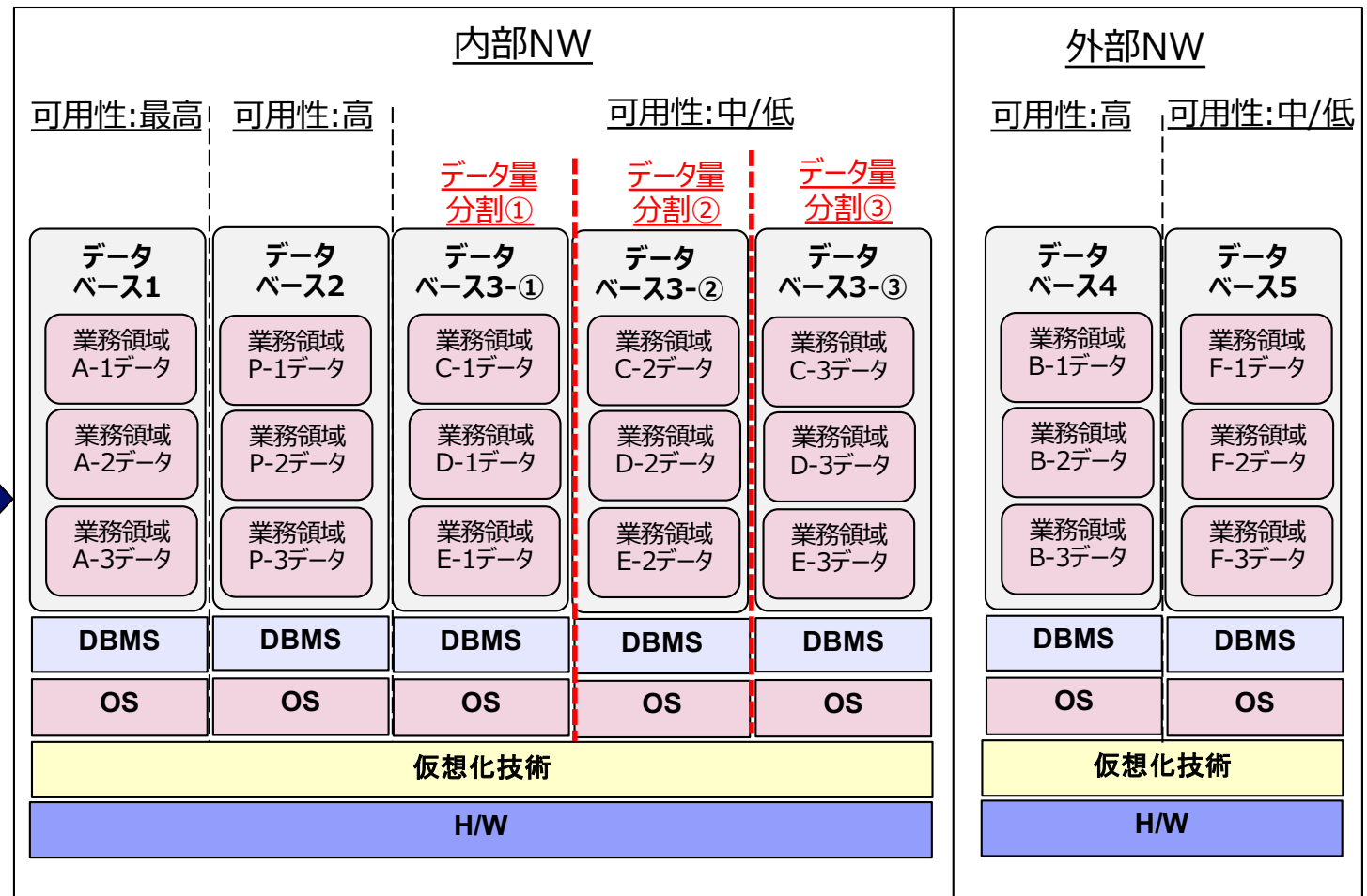
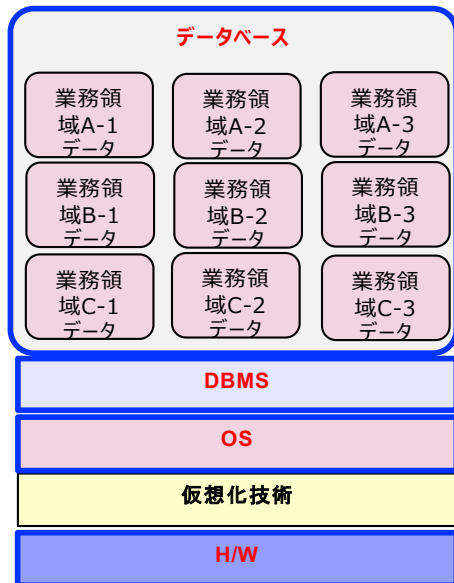
C) データベース統合パターン案

■ データベース統合パターン③イメージ

データベース統合パターン③

(ネットワークの違い、可用性の違い、データ量の閾値でデータベースを分割)

検討開始イメージ (1データベース統合)



2. データベース統合方策案の検討



C) データベース統合パターン案

■ パターン案と各システムとの対応

	犯罪照会 全国的情報 処理センター 用電子計算 機	P-WAN 警察庁WAN システム	総合捜査 警察総合捜 査情報シス テム	相対捜査 組織犯罪情 報管理シス テム及び特 定金融情報 データベース システム	行政情報 行政管理シ ステム	旅客情報 事前旅客情報 システム及び外 国人個別識別 情報認証シ ステム	受付シ ステム	不当要求 情報管理 機関支援 システム	図書 館シス テム	オープ ンネッ トワー クシス テム	
統合パターン① (ネットワークで分割)	データベース1 (内部NW)					データベース2 (外部NW)				-	
統合パターン② (ネットワーク、可用 性で分割)	データベース1 (内部NW, 最高)	データベース2 (内部NW, 高)	データベース3 (内部NW, 中or低)			データベース4 (外部NW,高)	データベース5 (外部NW, 中or低)				-
統合パターン③ (ネットワーク、可用 性、データ量で分割)	データベース1 (内部NW, 最高)	データベース2 (内部NW, 高)	データベース3-①、②・・・ (内部NW, 中or低, データ量)			データベース4 (外部NW,高)	データベース5 (外部NW, 中or低)				-
			3-①	3-②	3-③						
冗長化構成(想定) <統合パターン①>	Active - Active					Active - Standby				-	
冗長化構成(想定) <統合パターン②> <統合パターン③>	最高	高	中			高	中				-

統合パターン①は、一番可用性の高いシステムに合わせた冗長化構成が必要となる。

Active - Active : 両系を同時稼働して並行して処理し、障害時には残りの稼働系で処理を継続する

Active - Standby : 片系を待機状態にしており、稼働系に障害が発生した時に切り替え、引き継いで処理を行う

D) 実現性・リスク評価

データベース統合パターン案の実現性やリスクを評価するため、データベースを1つに統合した場合の非機能・アプリケーション・調達の観点での課題・リスクがどの程度解決されるかを検討しました。

■ 実現性・リスク評価結果

統合パターン①は実現性が低い。

統合パターン②③は実現性が高い。

統合パターン②③はデータ量に起因するリスクが一部残る。

	統合パターン①	統合パターン②	統合パターン③
実現性評価	× 未解決な課題が残るので 実現性が低い	○ 課題ほぼ全て解決可能であるため 実現性は高い	○ 課題は全て対処可能である ため 実現性は高い
リスク評価	× リスクはほとんど軽減せず残る	△ データ量に起因する リスクが一部残る	△ データ量に起因する リスクが一部残る

E) コスト比較

■ コスト比較の想定構成

コスト比較は以下の構成を想定して実施しました。

(統合パターン①は実現性は低いですが、検討としてコストを確認したので含めています)

想定	統合パターン①	統合パターン②	統合パターン③
DB数	2 (内部1/外部1)	5 (内部-最高1,高1,中低1 / 外部-高1,中低1)	9 (内部-最高1,高1,中低5 / 外部-高1,中低1) 内部-中低のデータベース3は 10TBごとに5分割)
冗長化構成	データベース1(Active-Active) データベース2(Active-Standby)	データベース1 (最高) データベース2、4 (高) データベース3、5 (中)	

(高い可用性が必要な冗長化構成を取るシステムは、高い安定性や信頼性が求められるため、採用実績の多い商用DBMSを使用することを想定)

E) コスト比較

■ データベース統合パターンごとのコスト要因の差異

データベース統合パターンの違いによるコスト要因の差異は以下と想定します。

差異要因	統合パターン①	統合パターン②	統合パターン③
① 共通リソースデータのデータ連携本数	少 (5) 5本 : 内部-外部	中 (16) 5本 : 内部-外部 0本 : データベース1 - 2 11本 : データベース1 - 3	多 (21) 5本 : 内部-外部 0本 : データベース1 - 2 16本 : データベース1 - 3
② 移行難易度	高 (段階移行による本番サービス中のDBに対するデータ移行有)	中 (段階移行による本番サービス中のDBに対するデータ移行有。ただし、可用性の違いでDB分割されているため影響範囲は限定される)	
③ データ処理量 (アクセス数、データ量)	差異は少ない (データ連携データ量が大きくないので処理量増加分もあまり大きくならない想定)		
④ 冗長化構成の差異	統合パターン①と統合パターン②③で必要となるサーバー処理能力 (コア数) に差異あり		
⑤ 業務データ量の差異	複製する共通データのサイズがあまり大きくないので差異は少ない 犯罪照会 : 個人、車両、盗品、共通コード 合計 10GB以下 相対捜査 : 暴力団 10GB以下		

E) コスト比較

■ コスト比較結果

データベース統合パターンごとのコスト比較結果（相対比較）です。

	統合パターン①	統合パターン②	パターン③
コスト比較結果	×	○	△

パターン①は、全システム冗長化構成のため、必要となるとサーバー台数(コア数)が増加するため、パターン②、③と比べて**DBサーバーのハードウェアコスト、商用DBMSのライセンスコストが増加する**ため相対的にコストが一番高くなる可能性があると考えられます。

パターン②とパターン③のコスト差は、DBの分割数の違いによりパターン③の方がパターン②よりも**データベース間の共通リソースデータの連携バッチ本数が増える**ため、相対的にコストが高くなると考えられます。

2. データベース統合方策案の検討



F) データベース統合方策案の比較

各方策案の比較結果は以下となります。

項目	統合パターン①	統合パターン②	統合パターン③
実現性評価	× 未解決な課題が残るので実現性は低い	○ 課題ほぼ全て解決可能であるため実現性は高い	○ 課題はほぼ対処可能であるため実現性は高い
リスク評価	× リスクはほとんど軽減せず残る	△ データ量に起因するリスクが一部残る	△ データ量に起因するリスクが一部残る
コスト	× DBサーバーのHWコスト、商用DBMSライセンスコストが一番高くなる	○ コストが一番抑えられる	△ データ連携バッチ数が一番多い
リソース効率	◎ OS分割数が少ないため、リソース効率は一番良い	○ 5つにOS分割するが、複数システムのDBが統合されリソース効率は比較的良い	△ OS分割数が多いため、リソース効率は一番悪い
保守性	◎ 管理対象のOS環境数が一番少なく、保守性は一番高い	○ 管理対象のOS環境数がパターン③より少なく、保守性は比較的高い	△ 管理対象のOS環境数が一番多く、保守性は一番低い
総評	実現性が高く、コストが一番抑えられ、リソース効率、保守性も良いため、 <u>パターン②を推奨します。</u>		

Ⅲ. バックアップセンター構築の提案

1. バックアップセンターの検討方針について
2. システムの切り替え操作等の自動化について
3. データ同期の技術的な方式について
4. バックアップセンターのモデルシステム案
5. モデルシステム案の比較

1. バックアップセンターの検討方針について

被災時等に速やかな業務継続を実現するために、センター切替操作の自動化及びセンター間のデータ同期方式を調査し、RTO (※) とRPO (※) の短縮を検討しました。

※RTO…目標復旧時間。業務停止から定められたレベルに回復するまでに必要となる時間。
RPO…目標復旧時点。どの時点までさかのぼってデータを回復させるかを示した値。

2. システム切り替え操作等の自動化について

バックアップセンターへのシステムの切り替えは、仮想化共通基盤の機能等を用いて操作を自動化することにより、RTOの短縮を図る方針を検討しました。

3. データ同期の技術的な方式について

RPOの短縮にはデータ同期方式の検討が重要なため、被災直前の状態により近いデータに復旧することを念頭に3つの方式（一括同期方式・遅延同期方式・リアルタイム同期方式）を整理しました。

4. バックアップセンターのモデルシステム案

17システムのRPO等を踏まえ、データ同期方式の最適な組み合わせを検討し、バックアップセンターのモデル案を3つ選定しました。

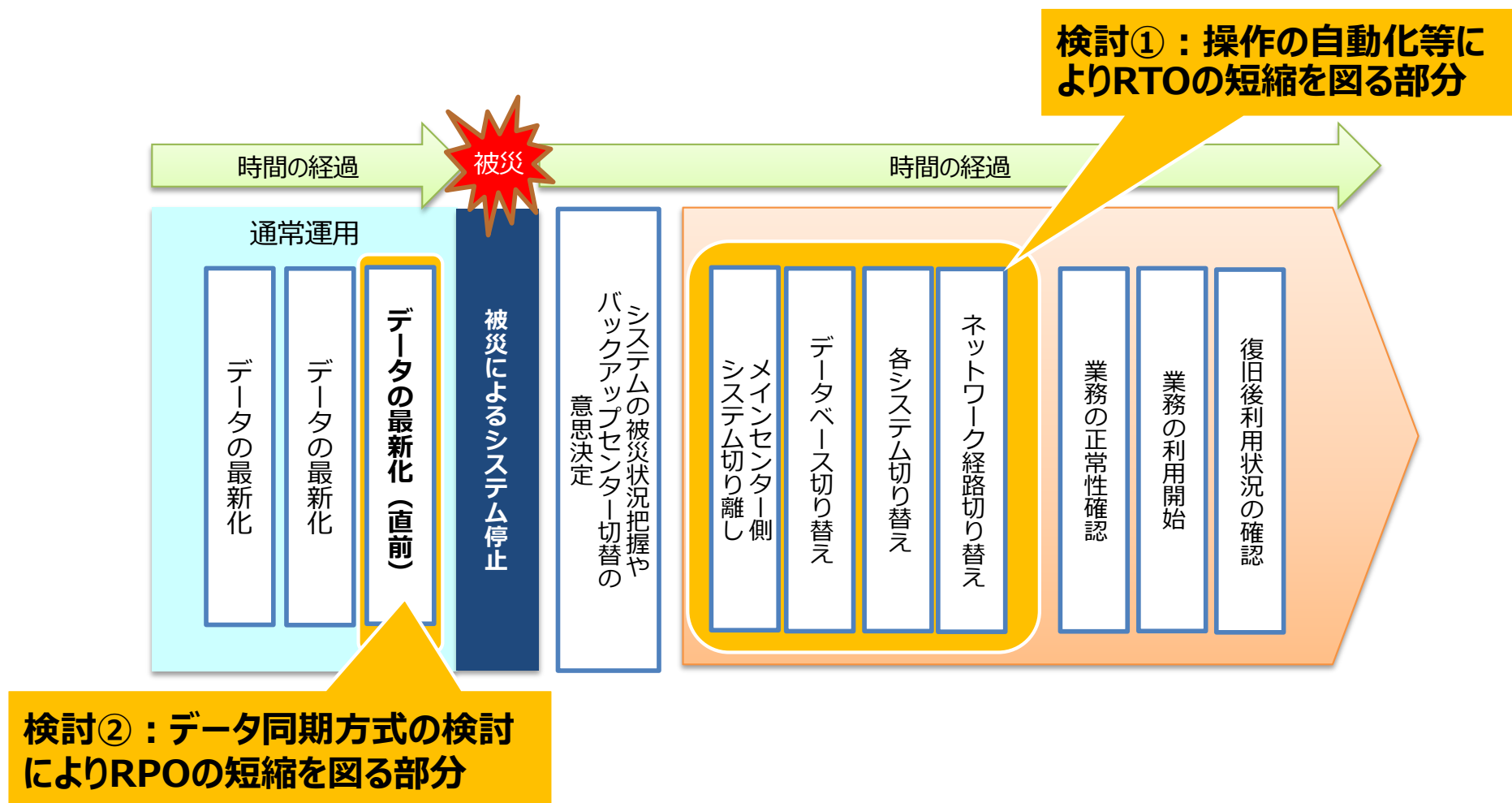
5. モデルシステム案の比較

3つのモデル案について、運用やコスト、移行性などの観点を比較し、最適なバックアップセンター構築案をご提案します。

1. バックアップセンターの検討方針について

情報処理センターが被災した際に、速やかな業務継続を実現するためには、RTOとRPOの短縮が必要です。このため、以下の観点について検討を実施しました。

- 検討①「RTOの短縮」：システムの切り替え操作等の仕組みの自動化
- 検討②「RPOの短縮」：システム単位で最適となるデータの同期の技術的な方式



2. システムの切り替え操作等の自動化について

バックアップセンターへのシステムの切り替えは、仮想化共通基盤の機能等を用いて操作を自動化することにより、RTOの短縮を図る方針を検討しました。

システム切替方式	概要	RTO	
手動切替方式	復旧における切替手順（メインセンターの切り離し、データベースの切り替え、各システムのサーバ群の切り替え、ネットワークの経路情報切り替え）をセンター側もしくはシステム側で手動で実施する。		数時間～ 1日程度
自動切替方式	復旧における切替手順をセンター側で自動的に実施する。		1時間程度

被災時のバックアップセンター側への切り替えを自動化することにより、RTOの短縮を実現可能です。これ以降のどのモデルシステム案においても「自動切替方式」を採用します。

3. データ同期の技術的な方式について

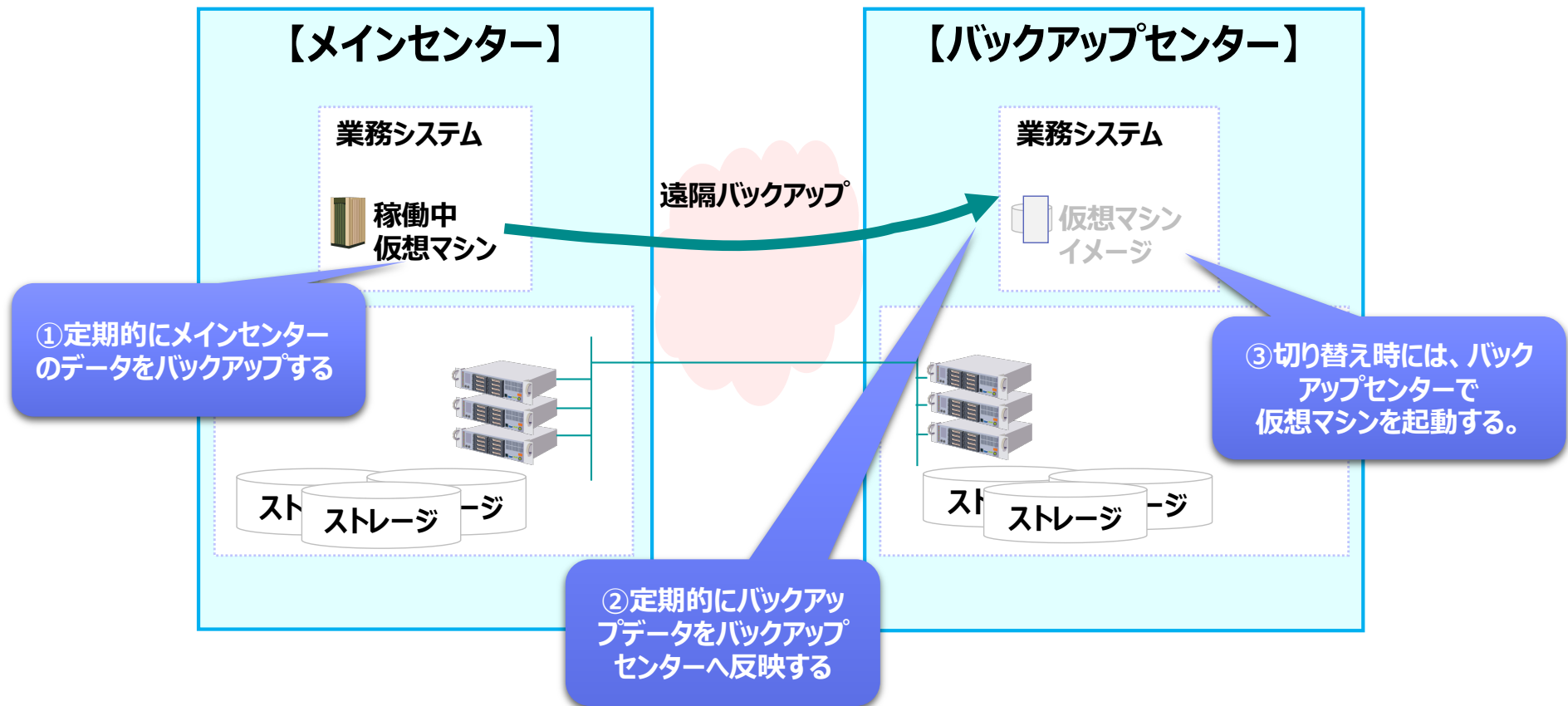
メインセンターとバックアップセンター間の技術的なデータの同期方式として、一括同期方式、遅延同期方式、リアルタイム方式があります。また、同期方式により、RPOが異なるため、システム単位で最適となるデータ同期方式を検討しました。

同期方式	概要	RPO	
一括同期方式	バックアップソフトにより取得したバックアップデータを代替サイトでリストアすることによりシステムを複製し、災害時にバックアップサイトへ切り替え可能とする。		1日程度 ※バックアップ 間隔による
遅延同期方式	各システムはセンター間で非同期（遅延あり）にデータを複製し、最新化する。		10分程度
リアルタイム同期方式	センター間を高速低遅延回線で接続し、データ更新毎に両サイトのストレージをリアルタイムに更新する。		0分程度

3. データ同期の技術的な方式について

データ同期方式A：一括同期方式（バックアップソフトを利用）

バックアップソフトを用いて定期的にメインセンターのデータをバックアップセンターに遠隔バックアップする方式です。

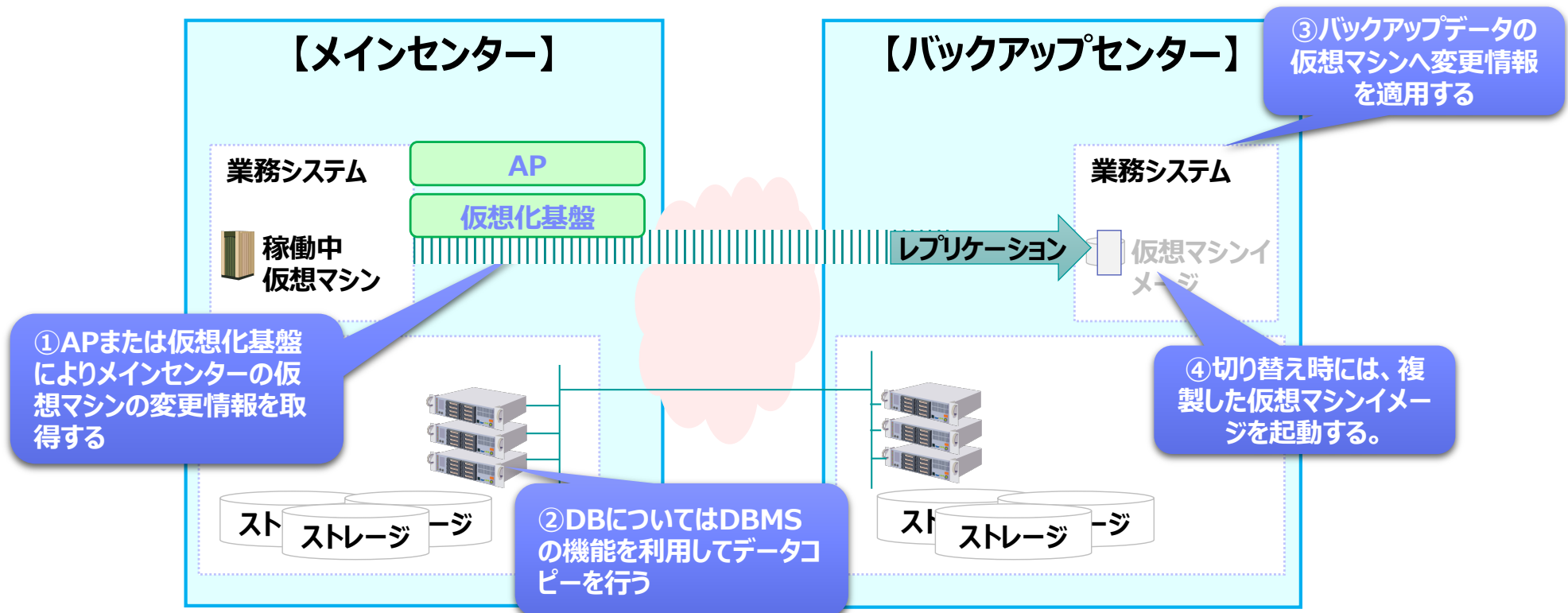


3. データ同期の技術的な方式について

データ同期方式B：遅延同期方式(DBMS/AP/仮想化基盤を利用)

DBMS、AP(作り込みした業務プログラム)あるいは仮想化基盤が備えるレプリケーション機能を利用して、メインセンターの仮想マシンをバックアップセンターへ複製する方式です。

- DB内のデータ：DBMSの機能を用いてデータ複製
- ファイル等（DB外のデータ）：APまたは、仮想化基盤の機能を用いてデータ複製

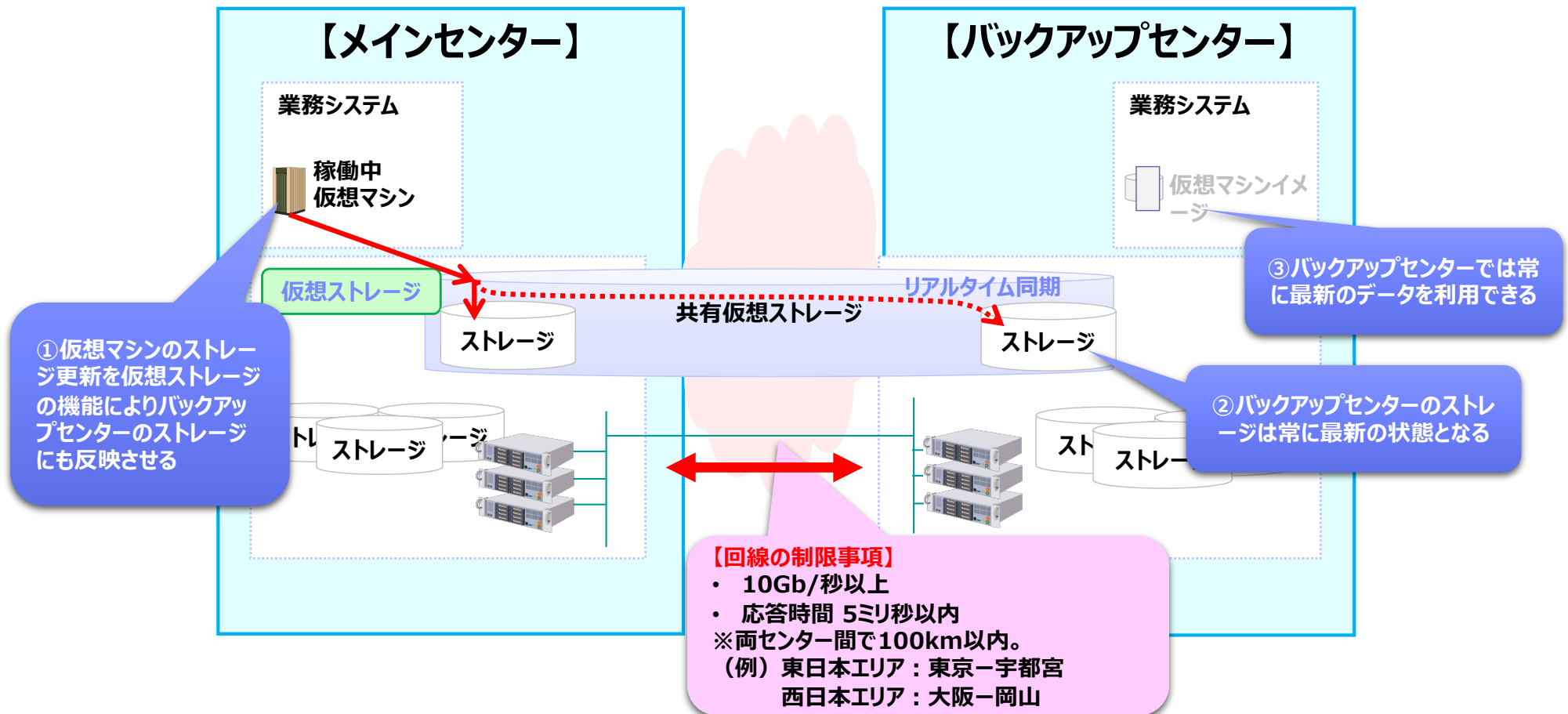


※OSSのDBMS(PostgreSQL等)においてもレプリケーション機能は実装されているものの実績が少なく検証が必要。検証の結果不採用の場合は、OSSのDBMSに対応したバックアップソフトを用い、遅延同期方式相当の間隔で同期を行う方式となる。

※ストレージによる同期はDBMSで行う場合に比べて、追加開発（DBMSと整合を取るための作り込み等）やNWコスト（ストレージの場合は変更の反映に不要な一時ファイルや管理ファイルも転送する）が高く採用していない。

データ同期方式C：リアルタイム同期方式(ストレッチクラスタを利用)

共有仮想ストレージ(ストレッチクラスタ)機能を利用して、メインセンターのストレージをバックアップセンターのストレージとリアルタイムに同期する方式です。



39 ※ストレッチクラスタ以外に、ハードウェアストレージやDBMSの同期型レプリケーション機能によりリアルタイム同期を実現することも可能。
※ストレッチクラスタは拡張性、運用性に優れ、データベース以外のデータも扱えることから本方式を採用している。
(ハードウェアストレージの場合は高機能・高コストな機器が必要となる。また、DBMSの場合はデータベース以外のデータの同期が対応不可となる。)

4. バックアップセンターのモデルシステム案



バックアップセンターのモデル案としてデータ同期方式案のどれを採用すべきかについては、各システムに求められるRPOを元に3案を検討しました。

求められるRPO	システム名 (略称)	データ同期方式A 一括同期方式	データ同期方式B 遅延同期方式			データ同期方式C リアルタイム同期方式
			DBMS	AP	仮想	
直前の状態	<ul style="list-style-type: none"> 犯罪照会 旅客情報 運転者管理 総合捜査 (アクセス権管理システム含む) 行政情報 相対捜査 P-WAN 人事・給与システム 	<p>×</p> <p>求められるRPOが実現できない</p> <p>案①～③共に方式Aを採用</p>	<p>○</p> <p>採用可能</p> <p>案①・② 共通</p>	<p>○</p> <p>採用可能</p> <p>案①</p>	<p>○</p> <p>採用可能</p> <p>案②</p>	<p>○</p> <p>採用可能</p> <p>案③</p>
バックアップ取得時点	<ul style="list-style-type: none"> 不当システム オープンネット 受付システム 図書館システム データ伝送用端末装置 画像処理分析用端末 	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>
指定なし	<ul style="list-style-type: none"> 警察庁ウェブサイト データ送受信端末装置 	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>	<p>○</p> <p>採用可能</p>

「バックアップ取得時点に復元」及び「指定なし」：求められるRPOの要求は高くない。このため、求められるRPOを踏まえて、センター側のコスト影響やシステム側の負担を考慮し、必要な同期方式として方式Aを選択（対象の各システムで方式Bや方式Cを採用する場合、レプリケーションライセンスやセンターリソースの追加が発生。また、システム側では方式Bや方式Cに対する設計要件が追加となる）。なお、「直前の状態」とするシステムと同期方式を合わせることも可能である。

「直前の状態」：求められるRPOの要求は高い。最適なRPOを実現するために施設や共通基盤を考慮し、複数案を選択。

4. バックアップセンターのモデルシステム案

検討したモデルシステム3案の特徴は以下のとおりです。

モデル案	採用するデータ同期方式	モデル案の特徴
案①	<p>RPO「直前の状態」のシステム 遅延同期方式 (DBMS/AP利用)</p> <p>+</p> <p>RPO「バックアップ取得時点」「指定なし」のシステム 一括同期方式</p>	<ul style="list-style-type: none"> データベース：DBMSの機能を利用 データベース以外：AP改修、または、OSやPPの機能を利用してデータを遅延同期 バックアップソフトを利用
案②	<p>RPO「直前の状態」のシステム 遅延同期方式 (DBMS/仮想化基盤利用)</p> <p>+</p> <p>RPO「バックアップ取得時点」「指定なし」のシステム 一括同期方式</p>	<ul style="list-style-type: none"> データベース：DBMSの機能を利用 データベース以外：共通基盤（仮想化機能）を利用してデータを遅延同期 バックアップソフトを利用
案③	<p>RPO「直前の状態」のシステム リアルタイム同期方式</p> <p>+</p> <p>RPO「バックアップ取得時点」「指定なし」のシステム 一括同期方式</p>	<ul style="list-style-type: none"> 共通基盤（ストレッチクラスタ(HCI))を利用してデータをリアルタイム同期 バックアップソフトを利用
共通	-	・切り替え操作の自動化によるRTO短縮

5. モデルシステム案の比較



項目		案① 遅延同期方式(DBMS/AP) +一括同期方式	案② 遅延同期方式(DBMS/仮想) +一括同期方式	案③ リアルタイム同期方式 +一括同期方式			
センター数	2	メインセンター及びバックアップセンター（稼働系を分散運用）	2	メインセンター及びバックアップセンター（稼働系を分散運用）	4	東西で各2センター（稼働系を分散運用）	
RTO	○	50分	○	60分	◎	20分	
RPO	○	DB:10分/DB以外:60分	○	DB:10分/DB以外:60分	◎	DB:0分/DB以外:0分	
効率性	○	両センターが稼働状態	○	両センターが稼働状態	×	余剰リソースが多い	
運用性	△	システム個別の切替・起動	○	仮想化管理ソフトから一元実施	△	システム全体が複雑化する	
運用体制	○	2センター分の体制 ※センター毎の体制は現行より縮小	○	2センター分の体制 ※センター毎の体制は現行より縮小	△	東西で各2センター（4センター分の体制）	
コスト	建物・設備	○	2センター分必要	○	2センター分必要	×	4センター分必要 (100km圏内に2センター設置)
	HW/SW	○	必要となるHW、SWが少ない	○	必要となるHW、SWが少ない	×	必要となるHW、SWが多い
	AP	△	AP個別の改修が必要	○	製品機能で一律実現可能	○	製品機能で一律実現可能
	NW	○	2センター間の回線 (推奨帯域:0.5~1Gb/秒程度、応答時間:制約なし)	○	2センター間の回線 (推奨帯域:0.5~1Gb/秒程度、応答時間:制約なし)	×	東西の各2センター間回線は高帯域低遅延のNW（帯域:10Gb/秒以上、応答時間:5ミリ秒以内）
拡張性	○	HCI構成にした場合は、段階的な運用開始が可能	○	HCI構成にした場合は、段階的な運用開始が可能	◎	HCI構成であり段階的な運用開始やシステムの拡大が可能	
移行性	△	APの改修がシステム毎に発生	○	仮想化ソフト、DBMSの標準機能が利用可能	△	ホットスタンバイ等の信頼性対策の整理が必要	
総評	<ul style="list-style-type: none"> 案②をバックアップセンターの構築案として推奨致します。 案①：各システム側の改修が大きい 案③：RTO及びRPOの観点では最適であるが、施設面、NW、コスト面での要求レベルが極めて高く実現が困難 						

IBM