

“大震災が怖い”バックアップシステムの状況と優れたもの紹介

TSC障害・災害対策(DR: Disaster Recovery)ソリューション
-ストレージ・セントレック・サービス-

トライアングル・スピリット株式会社

取締役 宮腰 寿之

miya@t-spirit.co.jp

コンピュータの変化と新たな課題

時代	1970年～	1980年～	1990年～	2000年～
	電算機・電卓時代	大型コンピュータ時代	ナローバンド時代	ブロードバンド時代
組織名前	電算室 (事務)	情報システム (業務)	IT×× (会社インフラ)	××? (事業インフラ)
ネットワーク	郵便 電話	モデムネットワーク FAXネットワーク	LAN/WAN ・専用線 ・フレームリレー ・IP-VPN ・広域イーサ	インターネットVPN
ネットワーク スピード		2400bps ↓ 4800bps ↓ 9600bps	64Kbps ↓ 512Kbps ↓ 1Mbps	100Mbps
関心課題	事務処理の機械化	MIS、CIM、SIS	PC1人1台体制の構築 (情報資産の増大)	ITは事業インフラ

1990年代にIT化が進んだ結果、ITシステムが止まると仕事ができない時代が到来

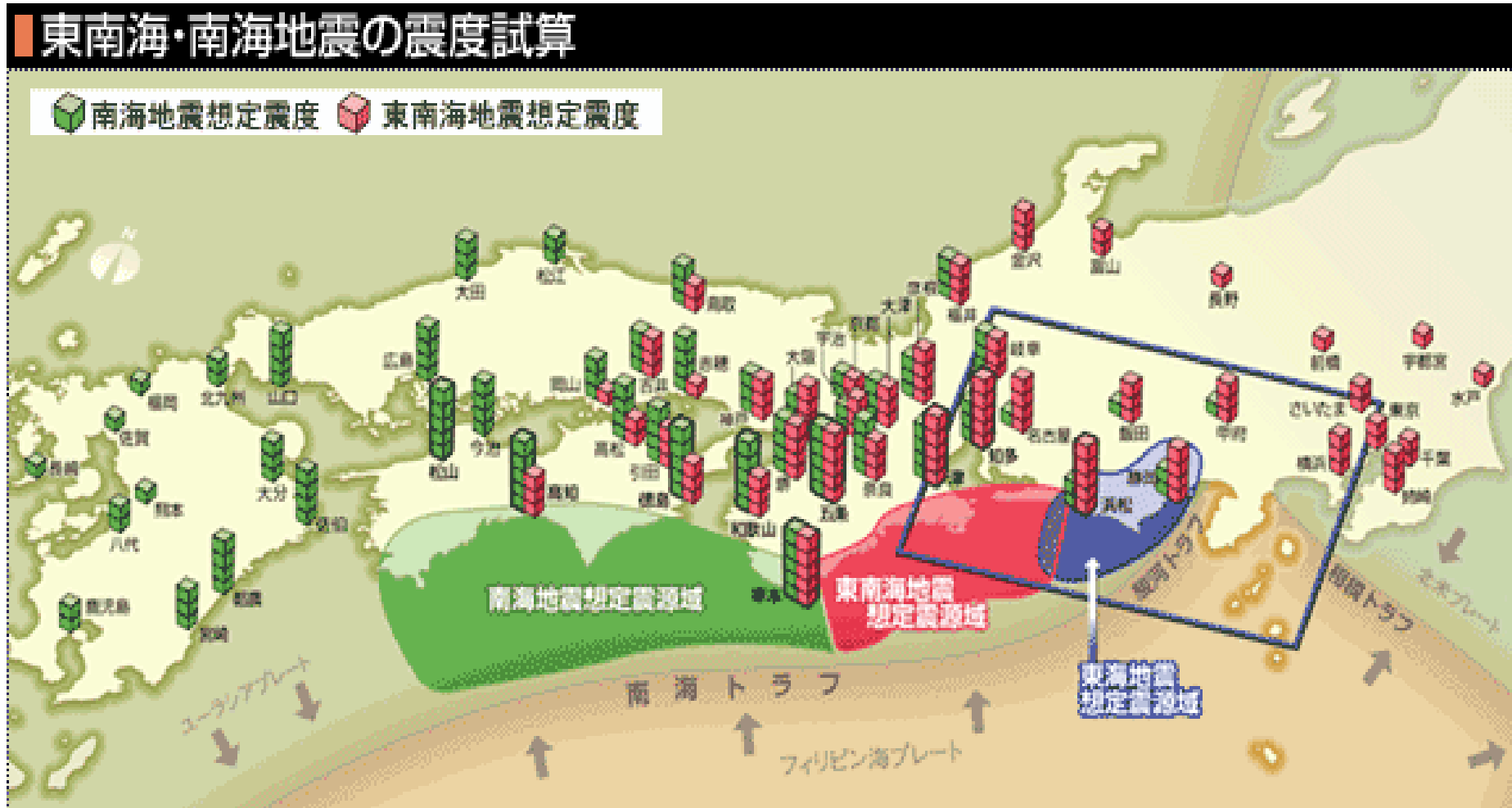


お客様の新たな関心事

- 2008年3月までに施行予定の「日本版SOX法」
 - 不正会計の防止を狙った「日本版SOX法」は顧客情報に限定していた個人情報保護法から、業務プロセスで発生するほぼすべての情報が管理対象
 - 社内に分散する情報をすべて集約し情報管理の徹底を実現する必要性の発生
- 情報の集約化ニーズ
 - コスト削減のためのサーバの集約化ニーズ
 - 情報管理面からの情報集約化ニーズ
 - データ集中化に伴うリスク分散の必要性
- IT資産の地震対策の重要性増大
 - 東海、南海・東南海地震への不安
 - ミュンヘン再保険の災害リスク及び耐震強度偽造事件の発生
 - 首都圏直下型地震対策大綱、事業継続ガイドラインの発表

ソリューション開発の背景(1)

文部科学省 地震調査研究推進本部資料より



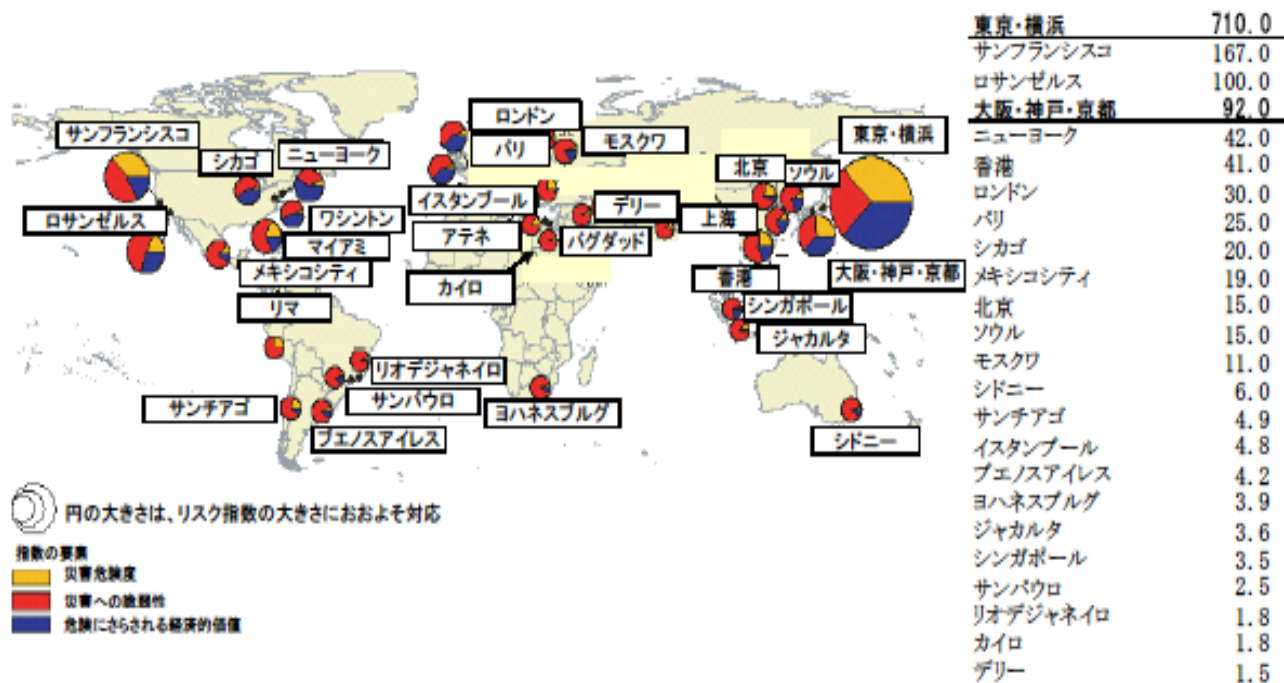
出展: Chunichi WEB Press 大図解シリーズ http://www.tokyo-np.co.jp/daizukai/quake/eq_8.html

東海沖地震から、東海地震へ！ 東海地震想定震源域は、首都直下型地震も含まれる？

ソリューション開発の背景(2)

ビジネスの継続性を維持するためにはデータの喪失は避けなければならない。
 しかし日本は世界の主要都市の中で圧倒的に災害危険度指数が高いにもかかわらず、政府でも十分な対策がとられているとはとてもいえない状況。

ミュンヘン再保険会社によれば、東京・横浜の災害リスク指数は、他国に比して格段に大



出典) 総務省消防庁資料より

(出典) ミュンヘン再保険会社アニュアル・レポートより作成

日本政府の 災害対策の現状

2004年11月に内閣府が中央省庁の情報処理システムのうち救助や救援物資の輸送、交通・通信など地震発生後のインフラ確保に直結する重要なものや、国民の生命・財産・身体にかかわる335システムを対象に調査した結果

- ・バックアップ機能なし : 133システム
- ・データ保管を実施 : 269システム
 (内、保存データが同じ建物 : 190システム)

★満足なものは79システム

東京・横浜の危険性はロンドンの24倍にもかかわらず、日本政府の対策も遅れ気味
 政府は2005年9月27日に行政・金融機能維持を目指した『首都圏直下型地震対策大綱』を発表

ソリューション開発の背景(3)

政府は『首都圏直下型地震対策大綱』に先立ち、2005年8月1日に、

「**事業継続ガイドライン 第一版**」を公表 <http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf>

本ガイドラインは、大企業、中堅、中小企業を対象に、災害に係る事前対応(事業継続計画の策定)と事業継続の対策を進めるために必要な共通かつ基本的な項目をあげることをめざしたものである。

しかし、強制的な規格として定める意図ではもちろんなく、各項目の実施は任意である。

本ガイドラインにより政府として望ましいとして考えている対策とは、多額の投資が不可欠なものを必須としているのではなく、むしろ、企業が自らの事業を点検し、工夫し、計画を立て、資源を有効に活用するような対策を中心に想定していることである。(抜粋)

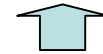
【事業継続計画の項目】

- ① 指揮命令系統の明確化
- ② 本社等重要拠点の機能の点検
- ③ 対外的な情報発信および情報共有
- ④ 情報システムのバックアップ
- ⑤ 製品・サービスの供給

情報システムのバックアップ

- 守るべき重要業務と情報システムの関係の明確化
- バックアップ稼動・切替え計画、復帰計画の策定

各社が行う事



- 自家発電装置、電源や回線など各種設備の二重化対策の実施



- 遠隔地への文書・電子データ保存サービスの活用

外部サービス



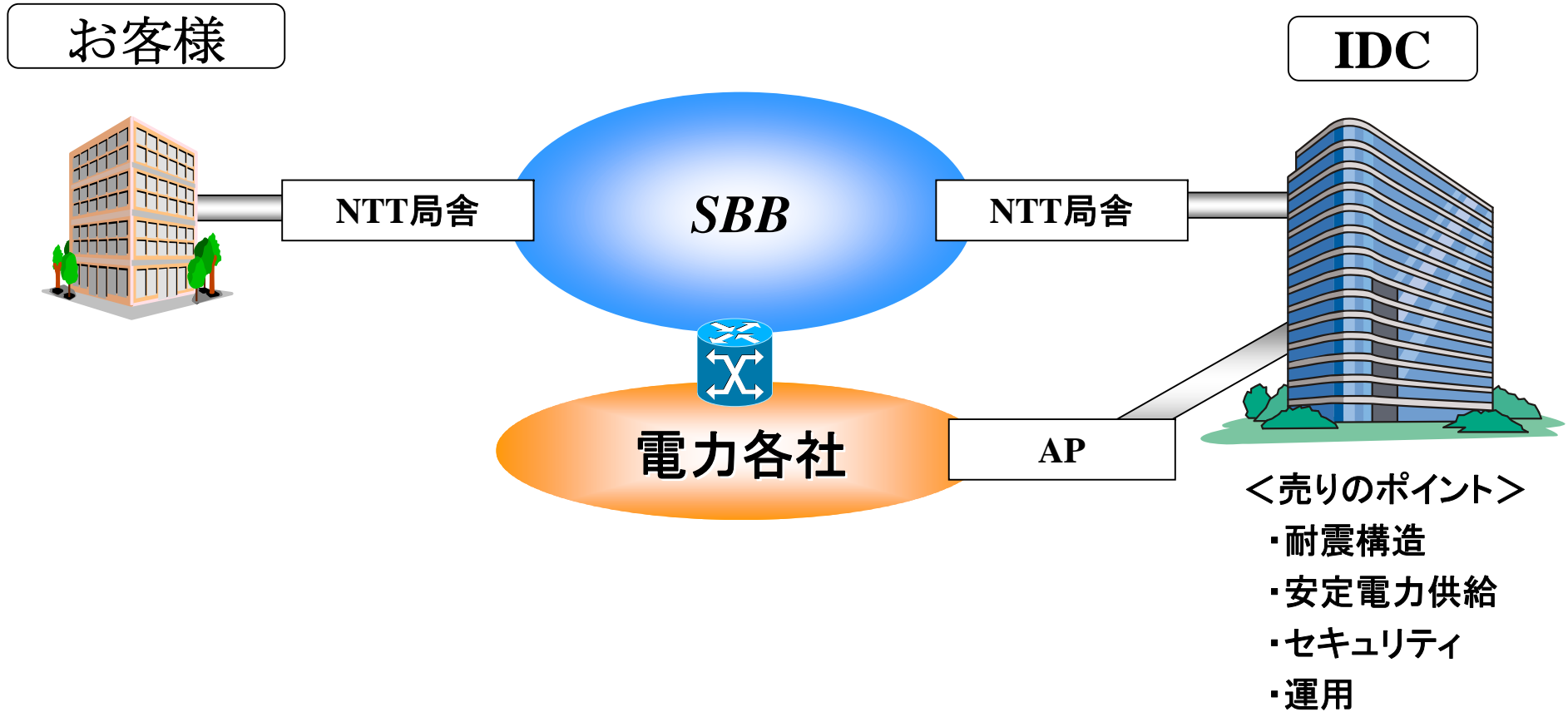
過去の災害事例から見ると、災害発生で事業継続不可に陥るのは中小や中堅企業が多い。これを回避するためにはこれらの企業が利用可能なDRコストでなければならない。



お客様のバックアップに対する関心事

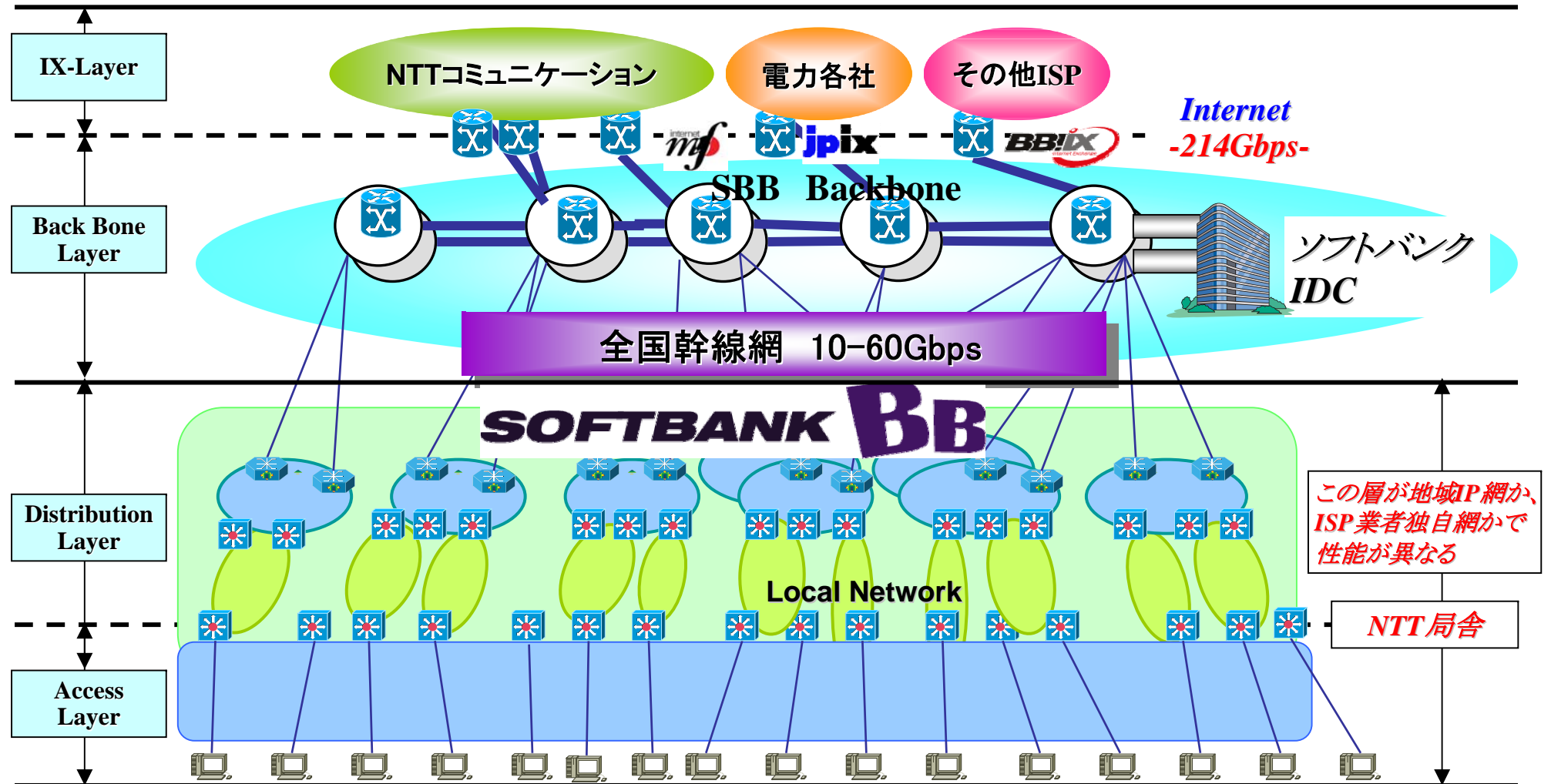
- バックアップの理想は？
 - 最新版を常にバックアップしたい。
 - 一瞬でバックアップを済ませたい。
 - 瞬時にリストアしたい。
- バックアップはまだテープ？
 - 時間がかかる。
 - テープの入れ替えが面倒。
 - 保管が大変。
- 誤消去や災害時に簡単に戻せるの？
 - 機器の管理は。どこに設置。
 - データセンターの利用はコスト大。
 - 災害よりもファイル誤消去時のリストアが大変。

従来のデータセンタ



従来のデータセンターは、お客様毎にラックや回線を用意するビジネス。よって回線はお客様責任で引くもので、データセンターは引込用件を要求するだけ。
しかしデータセンター利用は高速回線が必須で、高速になれば成る程、回線コスト比率は高くなる。

今回使うブロードバンドIDC



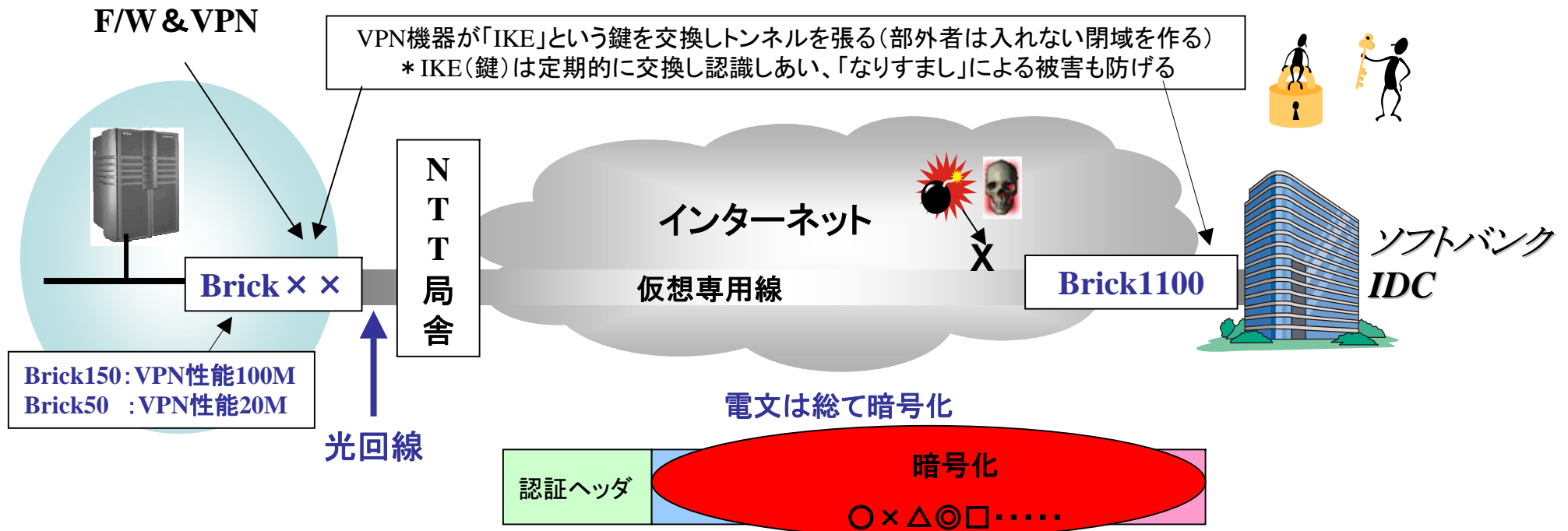
ブロードバンドデータセンタとはインターネットバックボーンの中にあるデータセンタ。
今回のサービスは、この部分にソフトバンクIDC社の設備を利用している。

お客様ブロードバンド回線とVPN装置

インターネットVPN (Virtual Private Network)

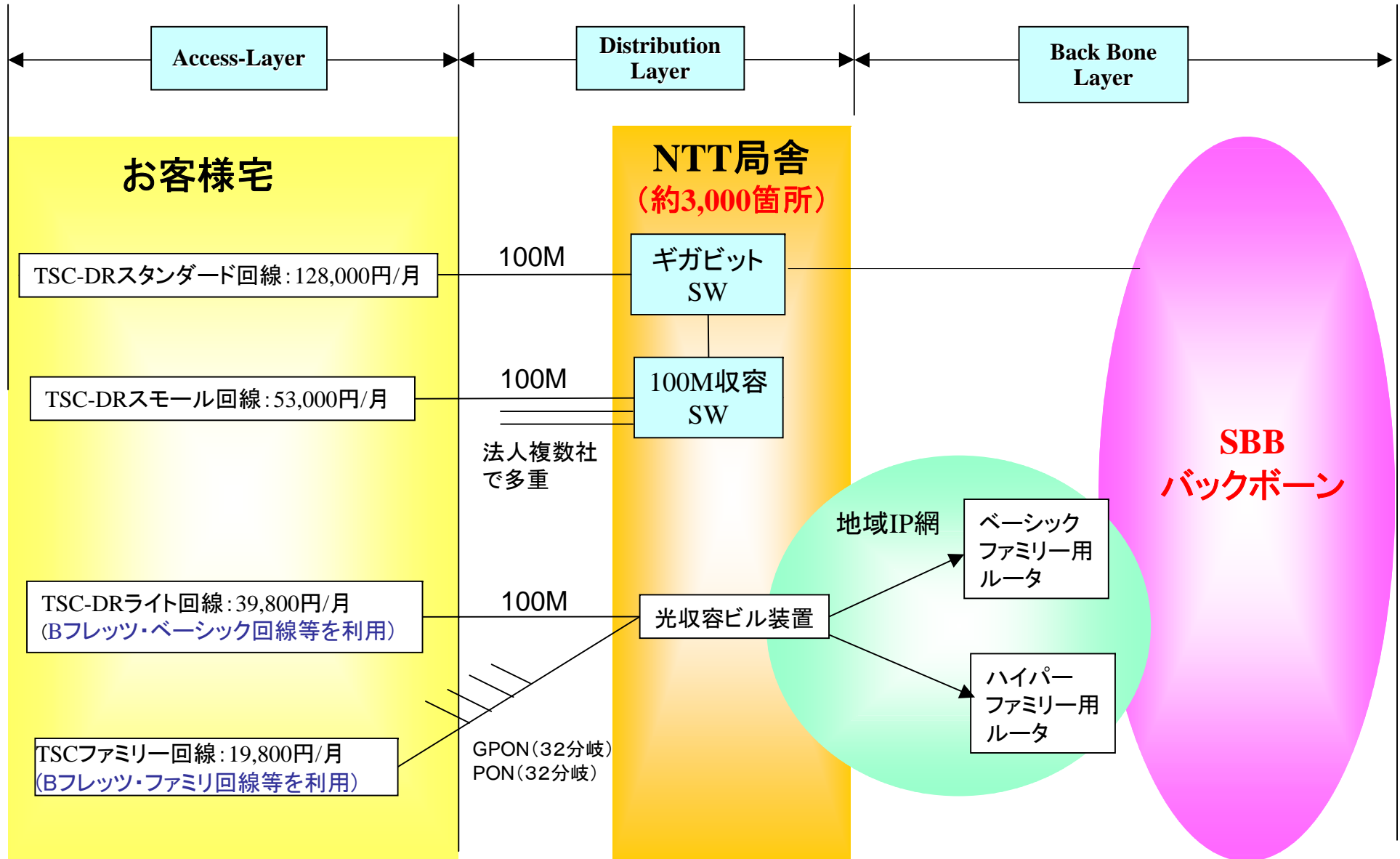
出典：ASCIIデジタル用語辞典

インターネットを経由するにもかかわらず、拠点間を専用線のように相互に接続し、安全な通信を可能にするセキュリティ技術。「仮想専用線」「仮想私設網」と呼ばれる。コストのかかる専用線の代替になる新しいインフラとして、企業を中心に浸透



インターネットは核攻撃に強いネットワークとして登場し、VPNの登場で災害対策用回線として十二分に使える領域に達した。Brickは、米国のベル研究所が開発したF/W、VPN装置で、監視はネットワークサービスアンドテクノロジー(NSAT)社が担当

今回のサービスで利用する光回線の種類



＜VPN通信試験データ＞

	スループット(Mbps)			
	拠点側より		IDC側より	
	httpによるダウンロード測定	Maxスループット	httpによるダウンロード測定	Maxスループット
1回目	56.600	88.020	76.552	88.910
2回目	72.049	85.990	84.541	87.390
3回目	68.533	88.120	65.317	88.200
4回目	73.643	86.470	60.491	88.110
5回目	63.240	87.840	81.007	87.630
6回目	99.032	87.930	69.498	88.150
7回目	75.383	88.040	75.420	88.380
8回目	79.041	85.780	57.299	87.500
9回目	67.595	82.490	73.115	86.200
10回目	85.247	88.450	69.561	85.090
平均	74.036	86.913	71.280	87.556

★上記計測データは、弊社本社と東京IDC間でVPN装置Brick150、回線はTSCスタンダード回線で計測

「httpによるダウンロード」は、2種類のファイルを5回ずつダウンロードしたときの値より計算された回線速度。

「Maxスループット」は、同処理最大転送量。

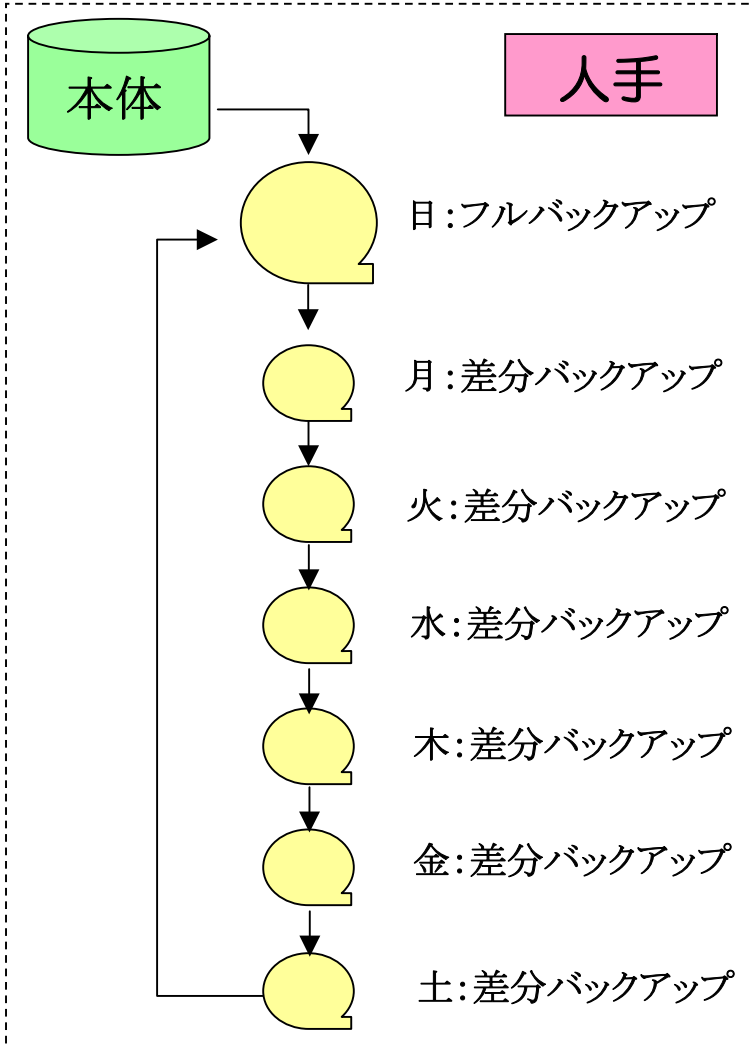
「Maxスループット」より「httpによるダウンロード」が大きい物は、ツール上の特性の為。

「httpによるダウンロード」にて使用したツール: LineSpeedTester 2.0.1, Web Server: anhttpd

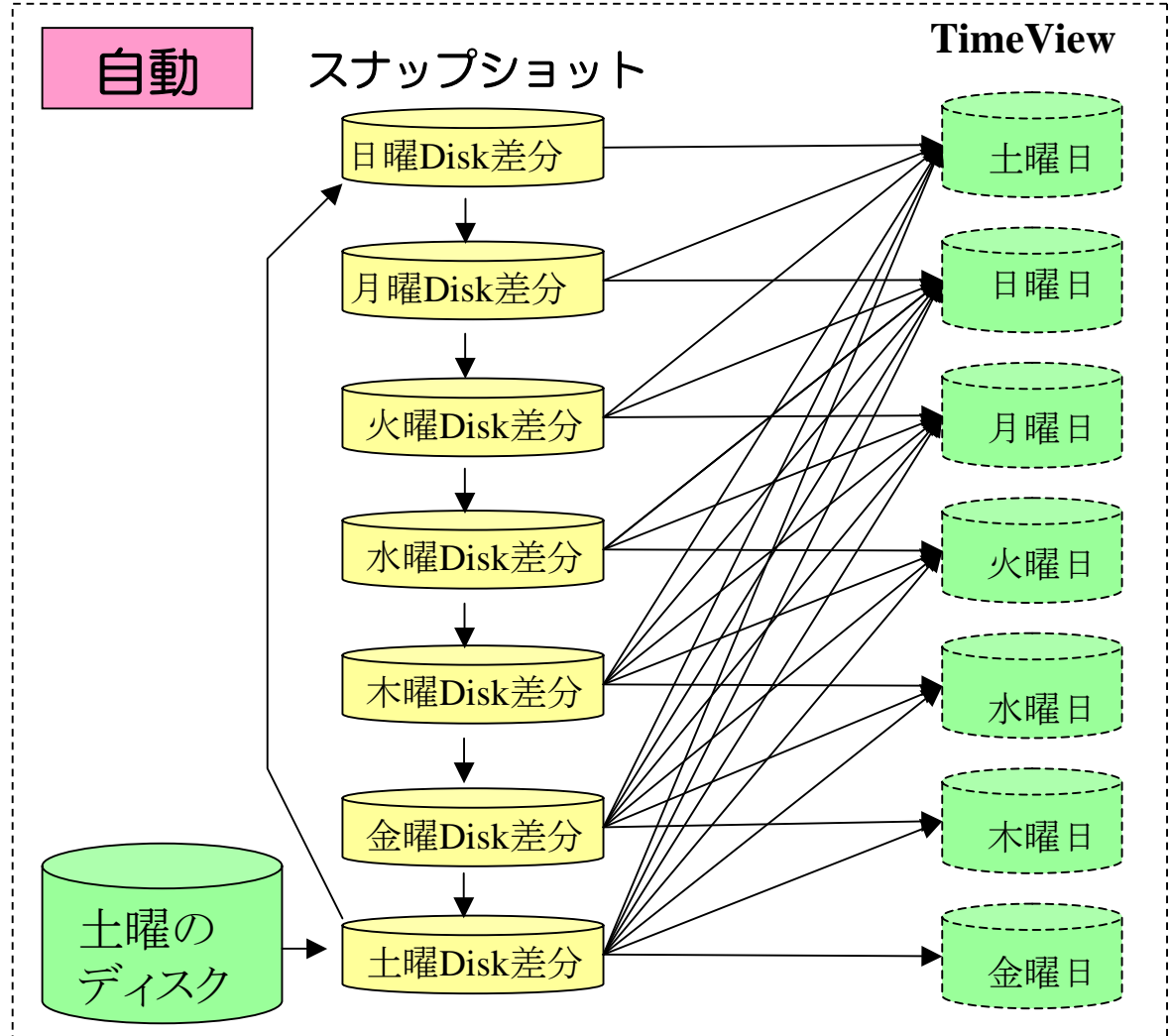
「Maxスループット」の測定に使用したツール: Net Activity Diagram

テープバックアップとディスク差分の考え方の違い

＜テープ時代の考え方＞

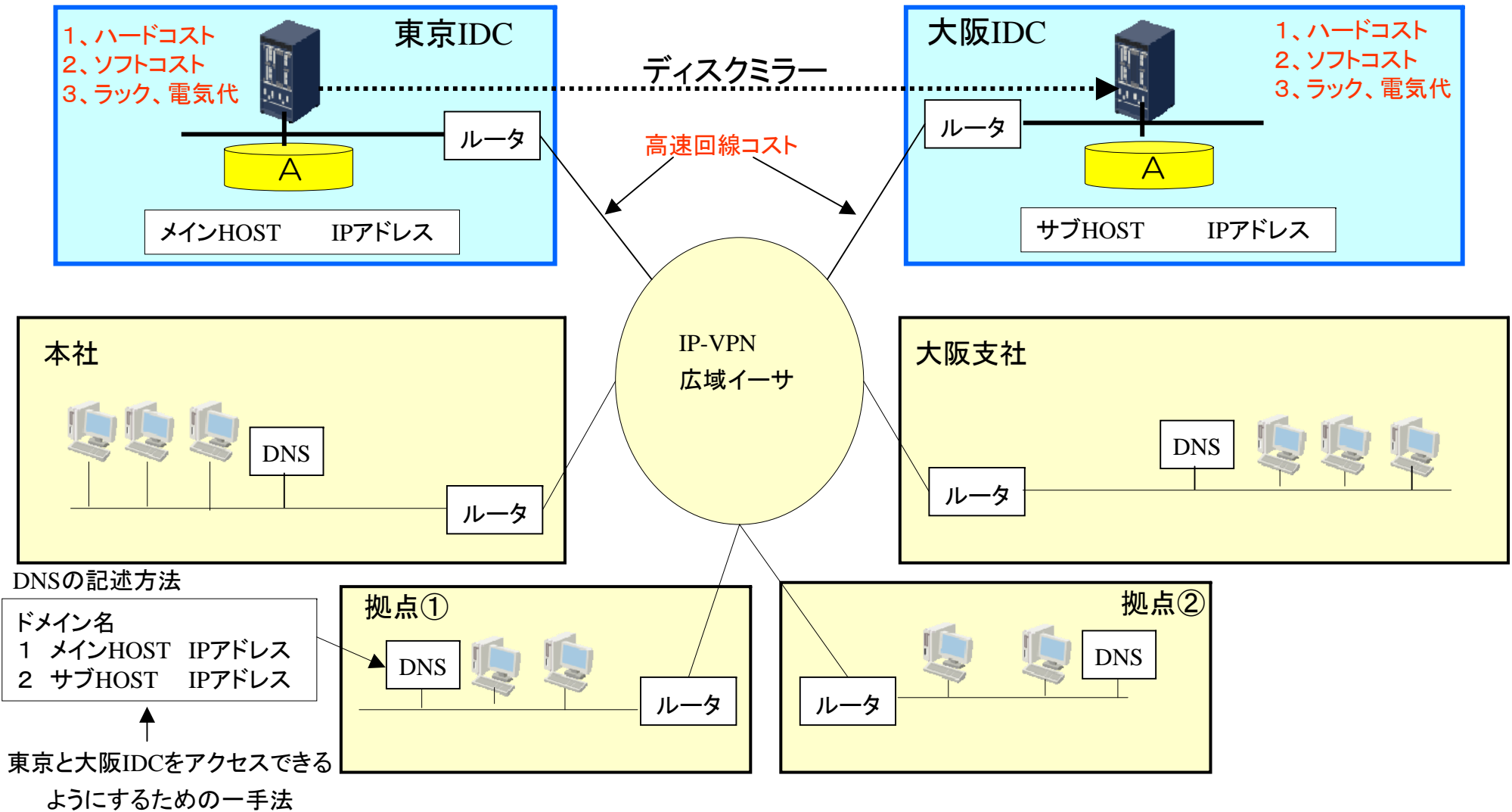


＜スナップショットの考え方＞



仮想ディスクのスナップショットは、十二分にテープバックアップの代用となる

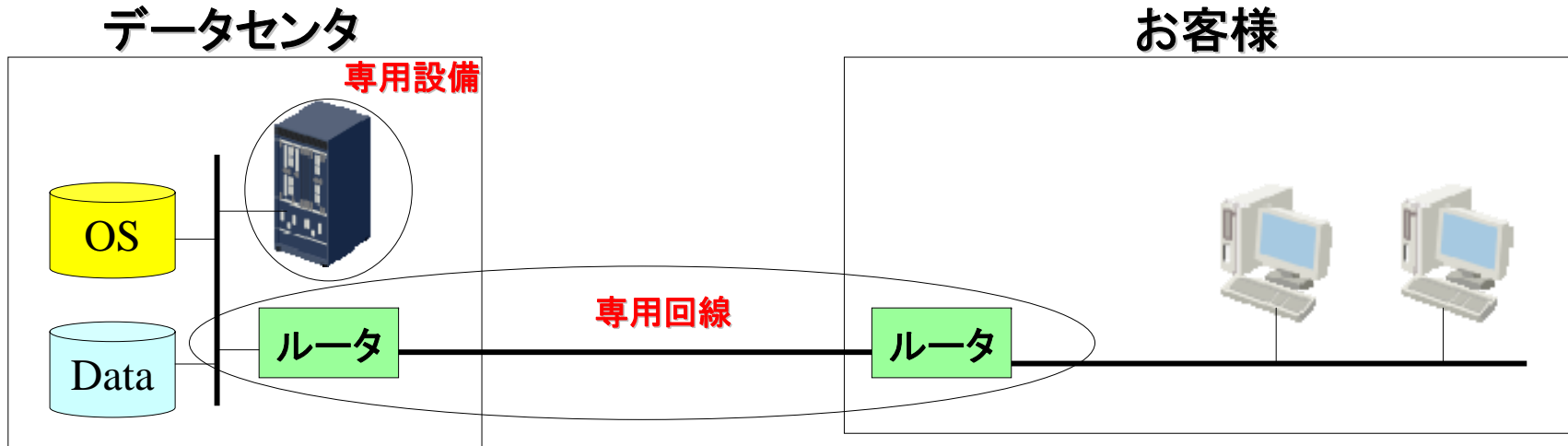
従来手法: システム2重化によるDR



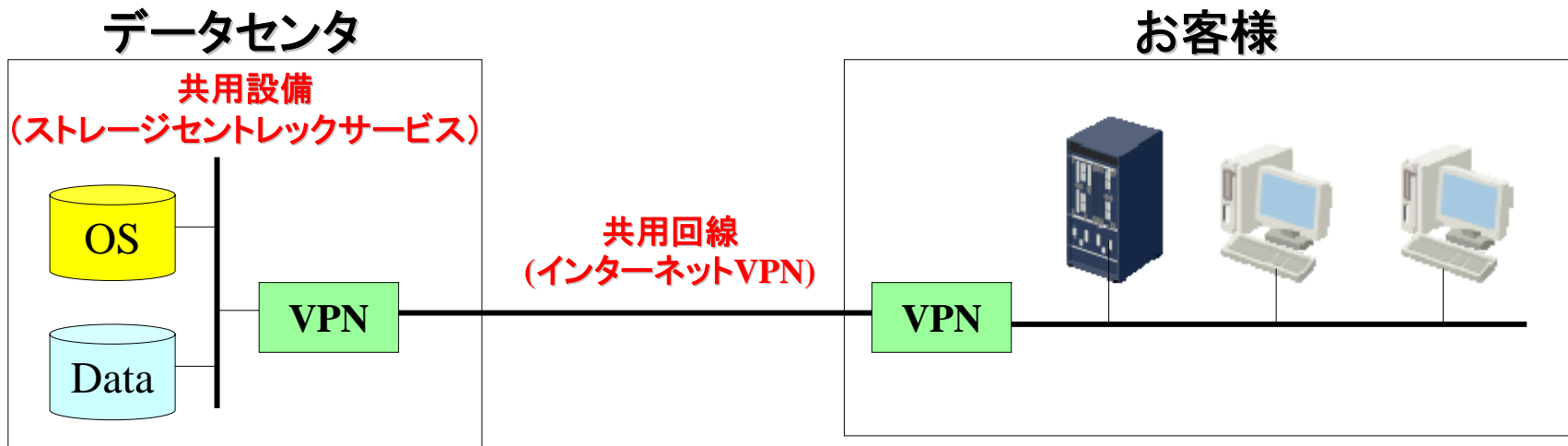
お客様拠点でのシステム2重化で数億、両方をデータセンタに持ち込むと数十億の話になる。
お客様先のデータを安価に遠隔地に保存・保管するためには新たな概念の登場が必要

コスト低減の為の新コンセプト

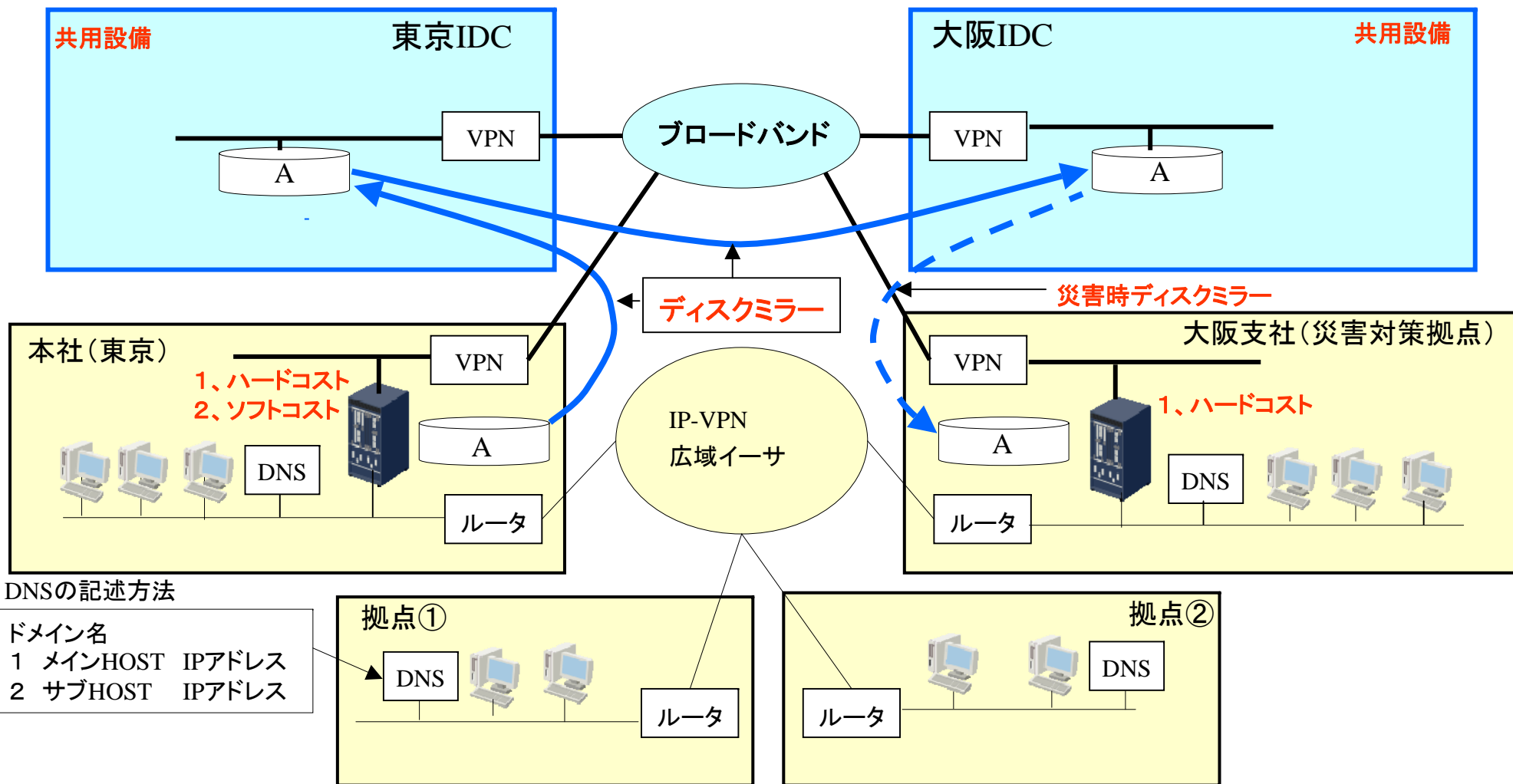
【従来の考え方】



【新コンセプト】

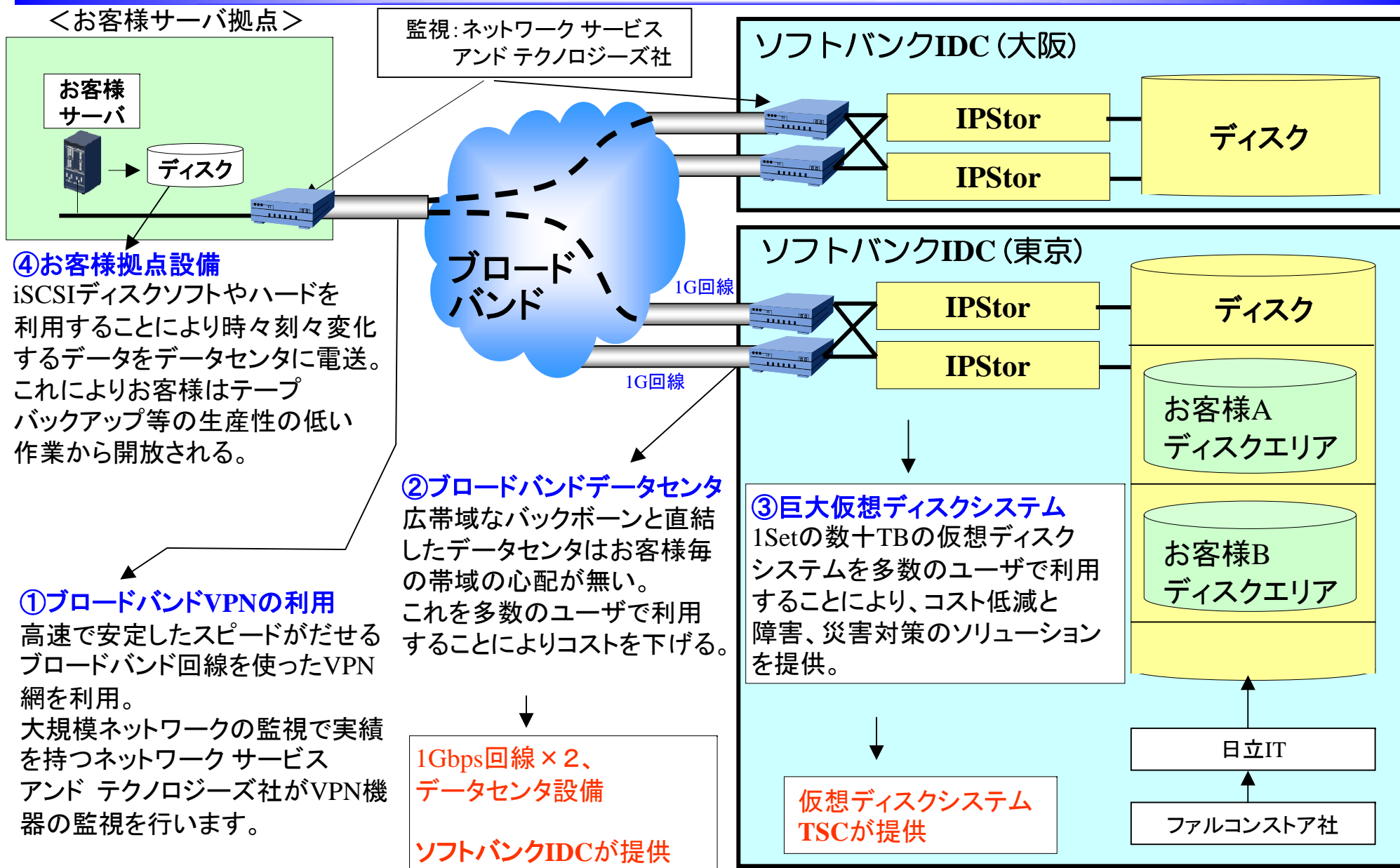


今回提案したいiSCSIディスクによるDR

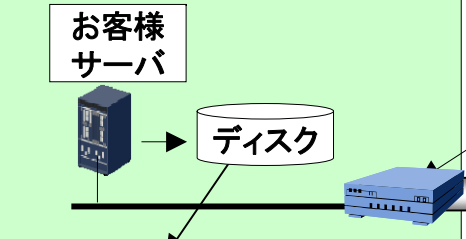


今回のソリューションは、データセンタの利用方法を根本から変えたソリューション。これはローカルディスクを遠隔ディスクにミラーリングする仮想ディスクテクノロジーを採用することにより可能となる。
 従来: お客様個別にデータセンタと契約 今回: 弊社が契約したデータセンタをサービスとして利用

今回のソリューションのポイント



＜お客様サーバ拠点＞



④お客様拠点設備
iSCSIディスクソフトやハードを利用することにより時々刻々変化するデータをデータセンタに電送。これによりお客様はテープバックアップ等の生産性の低い作業から開放される。

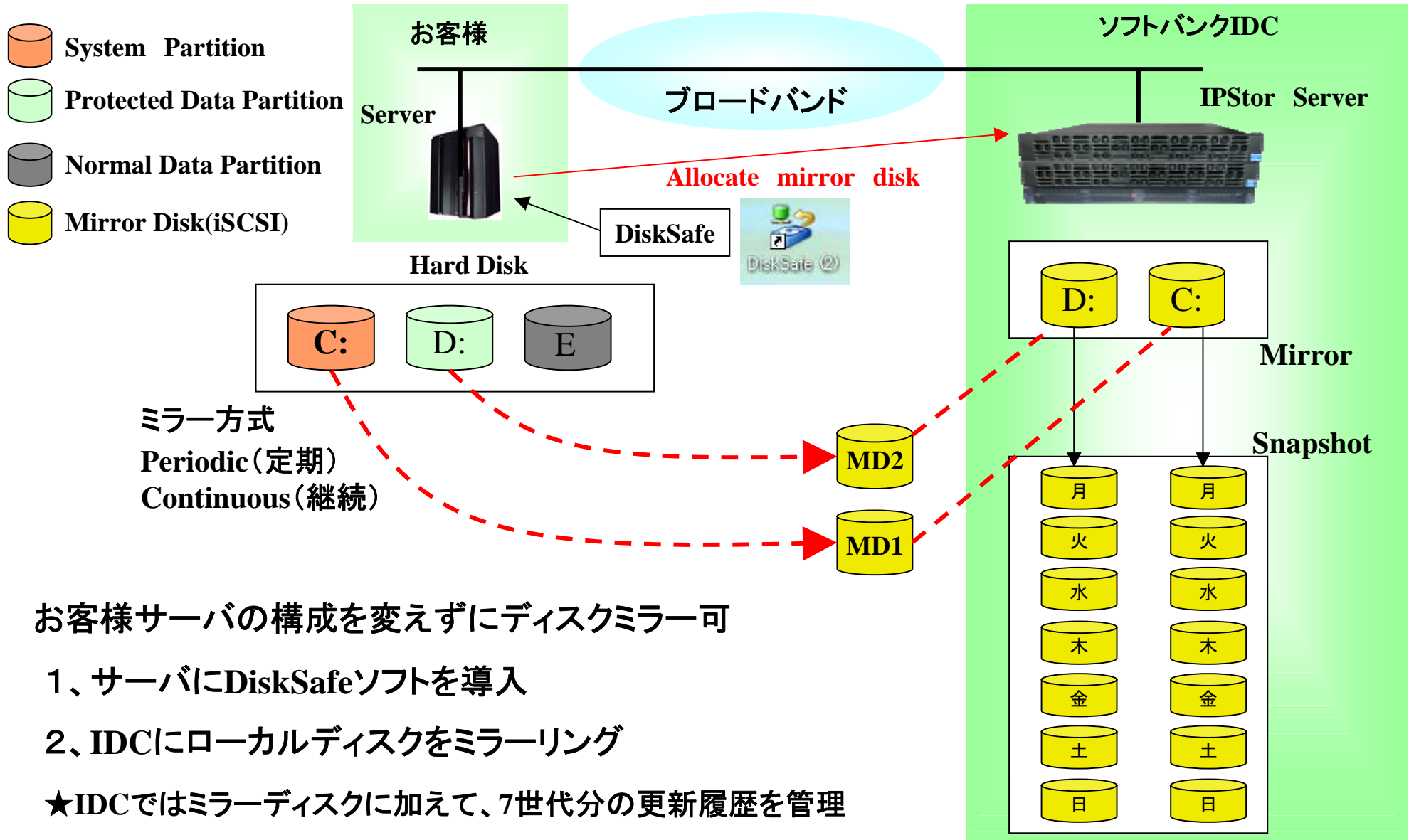
①ブロードバンドVPNの利用
高速で安定したスピードがだせるブロードバンド回線を使ったVPN網を利用。大規模ネットワークの監視で実績を持つネットワーク サービス アンド テクノロジーズ社がVPN機器の監視を行います。

②ブロードバンドデータセンタ
広帯域なバックボーンと直結したデータセンタはお客様毎の帯域の心配が無い。これを多数のユーザで利用することによりコストを下げる。

③巨大仮想ディスクシステム
1Setの数十TBの仮想ディスクシステムを多数のユーザで利用することにより、コスト低減と障害、災害対策のソリューションを提供。

Diskミラー型のご紹介

Diskミラー型のご紹介



お客様サーバの構成を変えずにディスクミラー可

1、サーバにDiskSafeソフトを導入

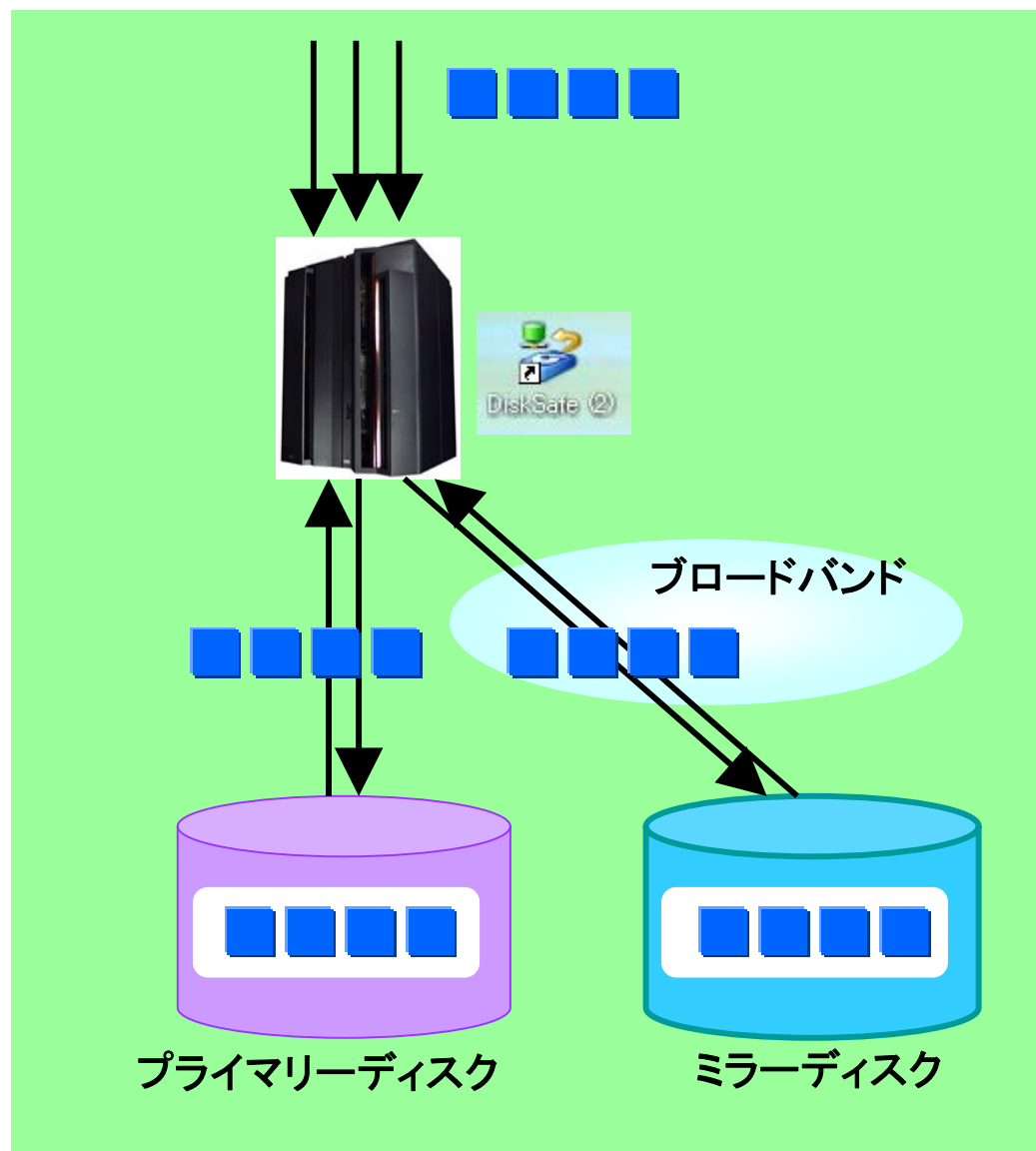
2、IDCにローカルディスクをミラーリング

★IDCではミラーディスクに加えて、7世代分の更新履歴を管理

同期方式: Continuous (継続) モード

継続モードの特性

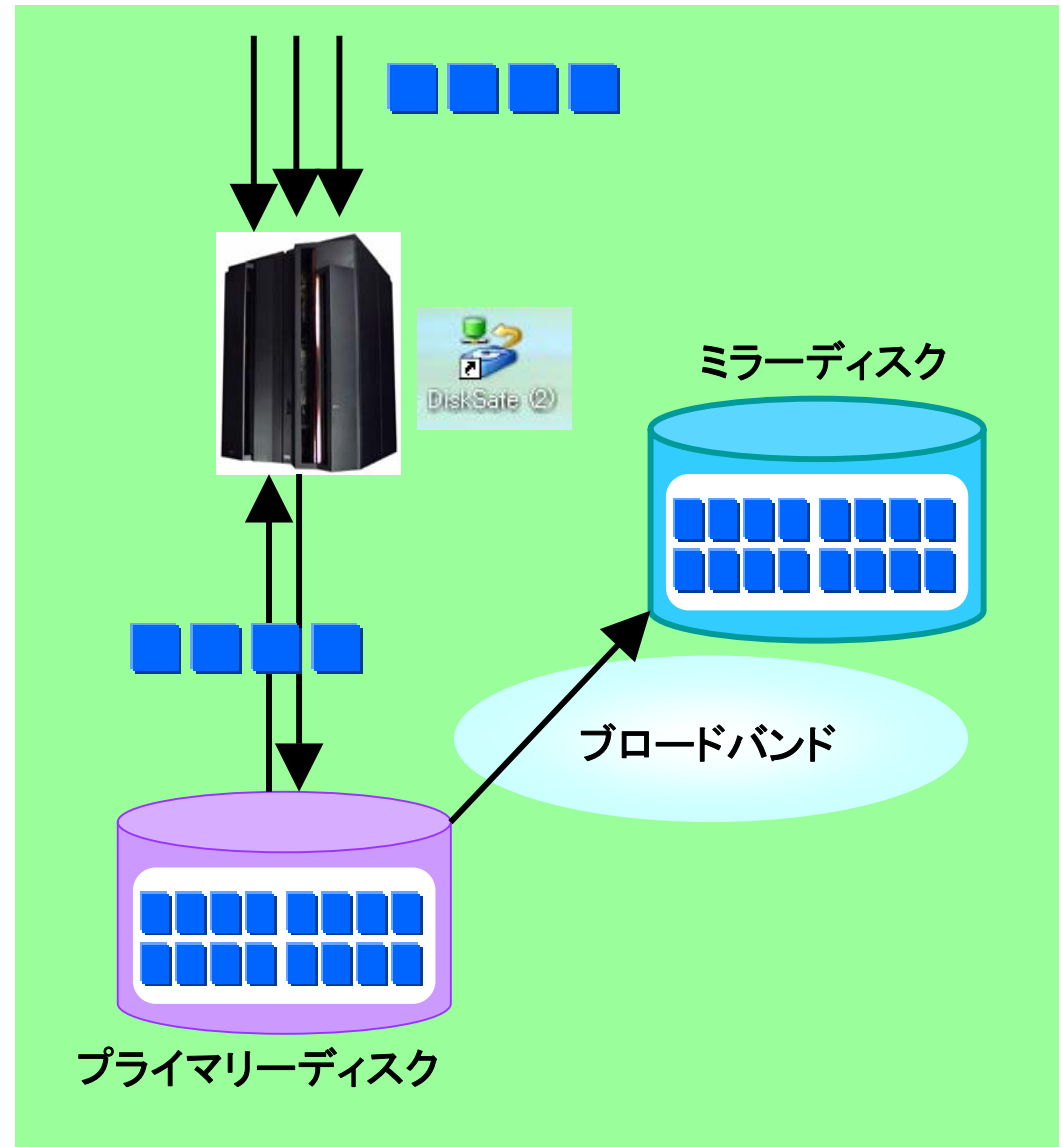
- ミラーディスクは常に最新の情報を保持
- プライマリディスクにブロックの更新があるたびにリモートディスクと同期
- ミラーディスクへの書込み速度が、著しく遅い場合、DiskSafeはミラーディスクからの応答を待たず、プライマリディスクへの書込みを継続
 - この場合、一時的に継続同期を中止



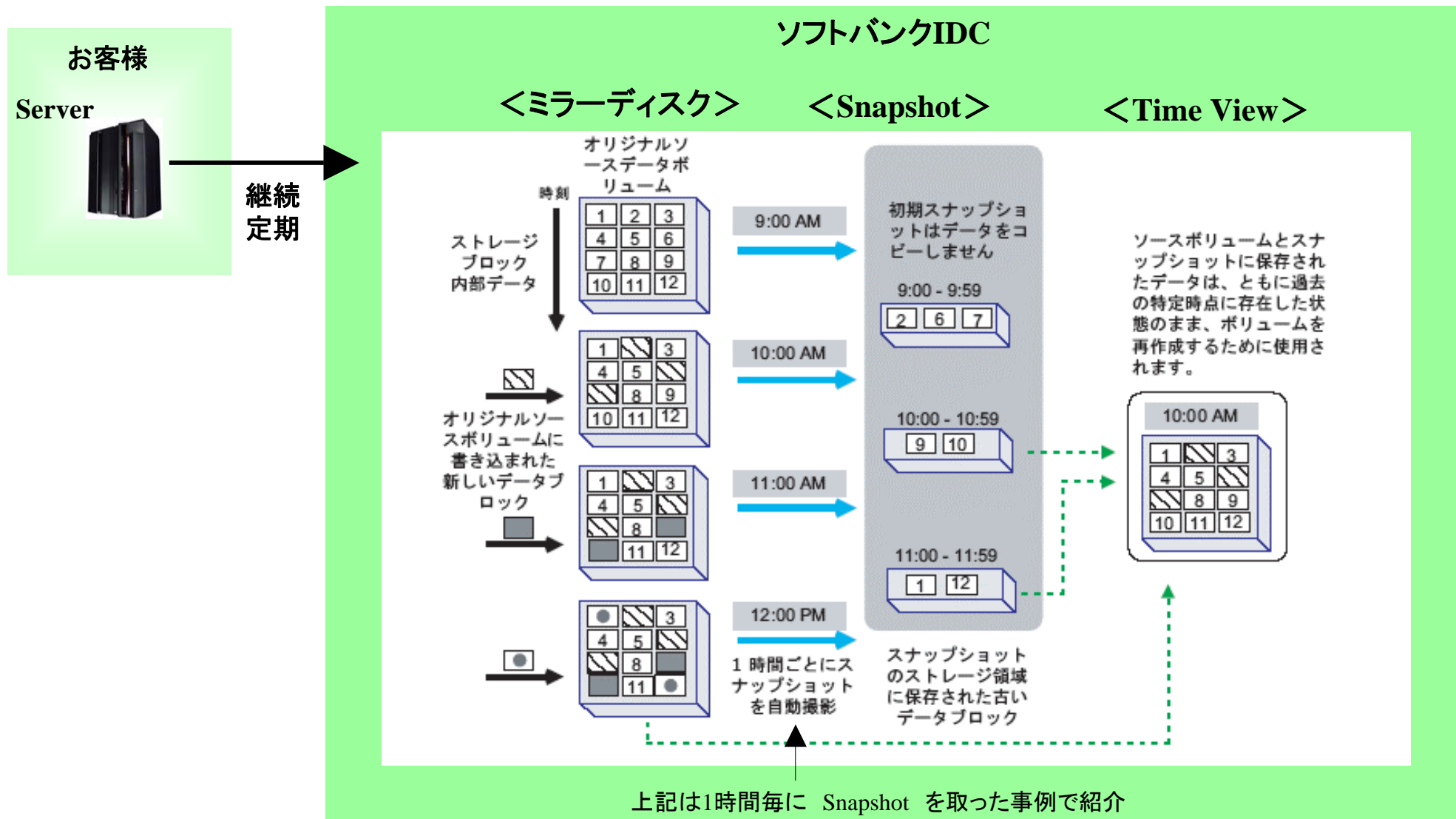
同期方式: Periodic(定期)モード

定期モードの特性

- ネットワークに対して最も負荷の少ない方式で更新データをミラーディスクにコピー
- ネットワーク障害を考慮した同期方式
- 更新されたブロックのみをミラーディスクに電送
- 同期タイミング
デフォルト: 1回/1日
任意時点での手動同期も可

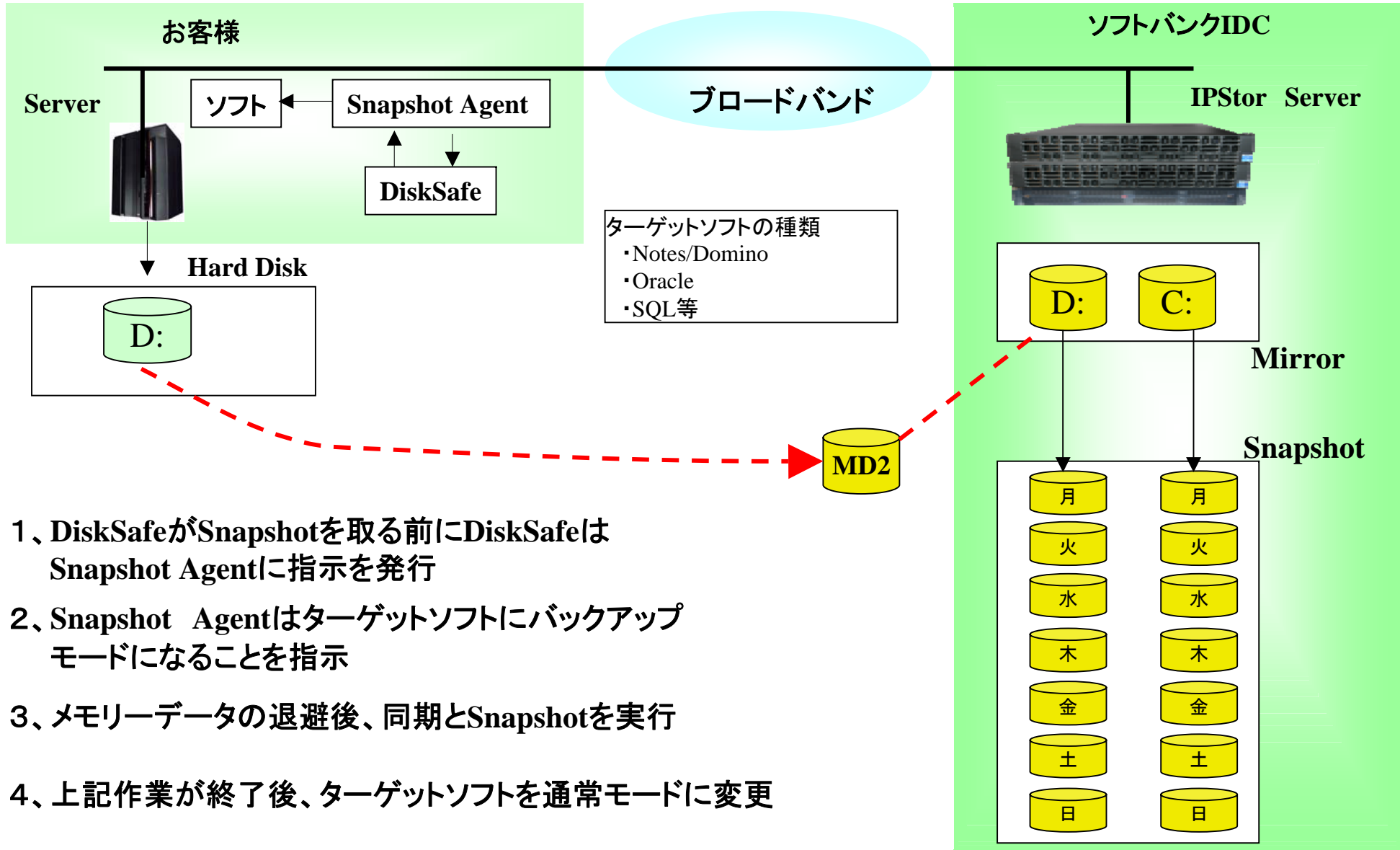


Snapshotの仕組







■ 弊社データセンターでは7世代のSnapShotを管理します。

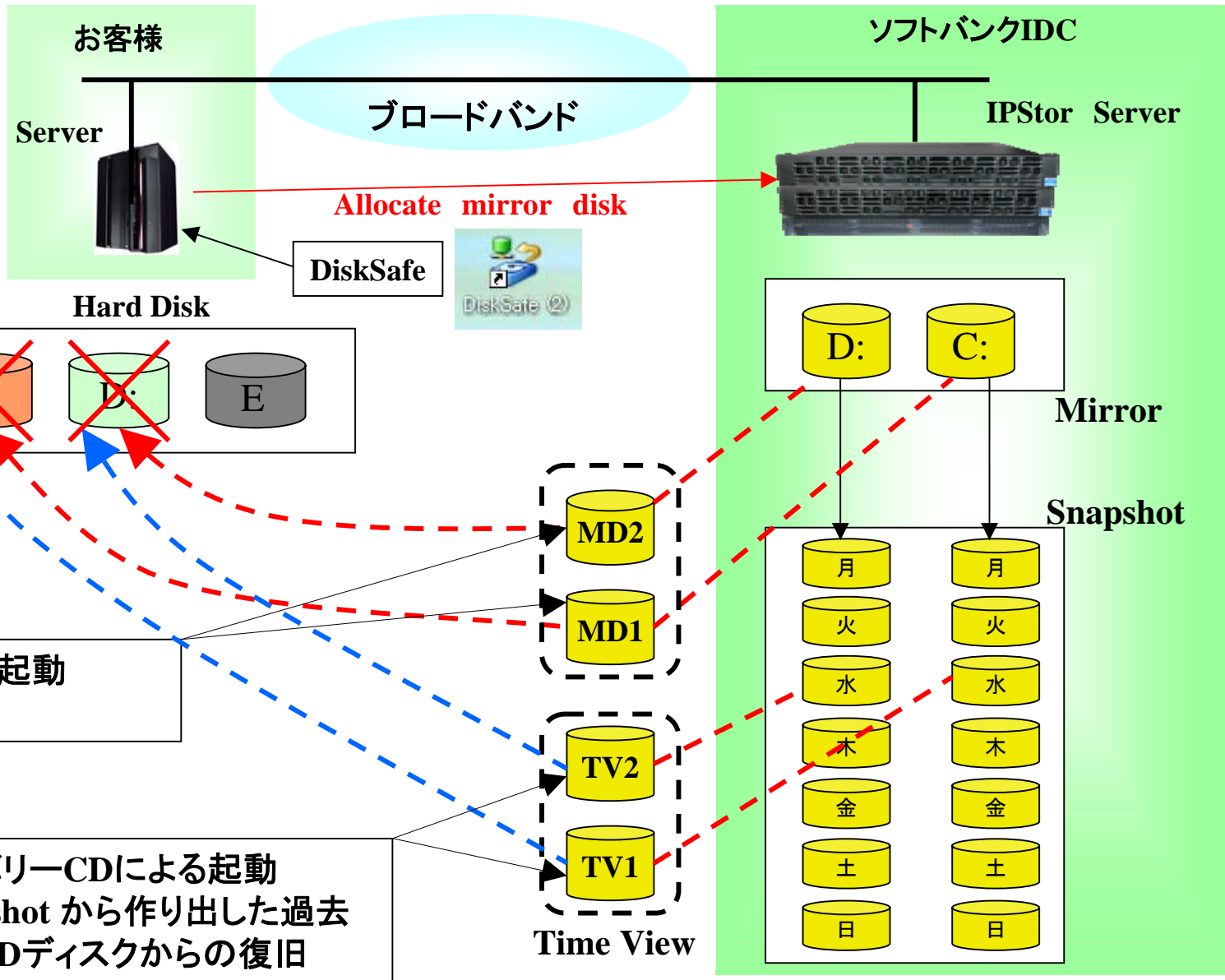
Snapshot Agent







- 1、DiskSafeがSnapshotを取る前にDiskSafeはSnapshot Agentに指示を発行
- 2、Snapshot Agentはターゲットソフトにバックアップモードになることを指示
- 3、メモリーデータの退避後、同期とSnapshotを実行
- 4、上記作業が終了後、ターゲットソフトを通常モードに変更

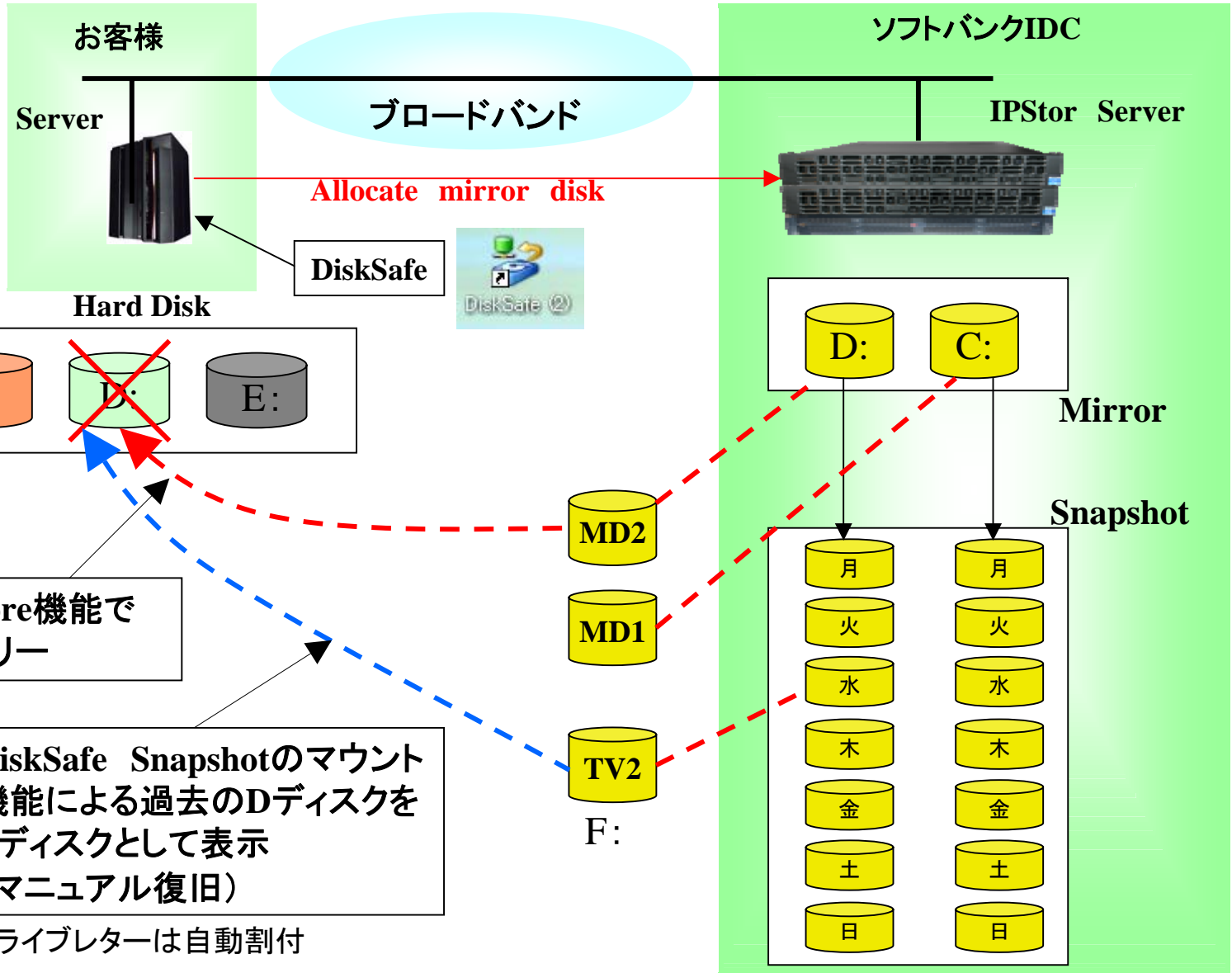
リカバリーシナリオ (リカバリーCD)

-  System Partition
-  Protected Data Partition
-  Normal Data Partition
-  Mirror Disk(iSCSI)

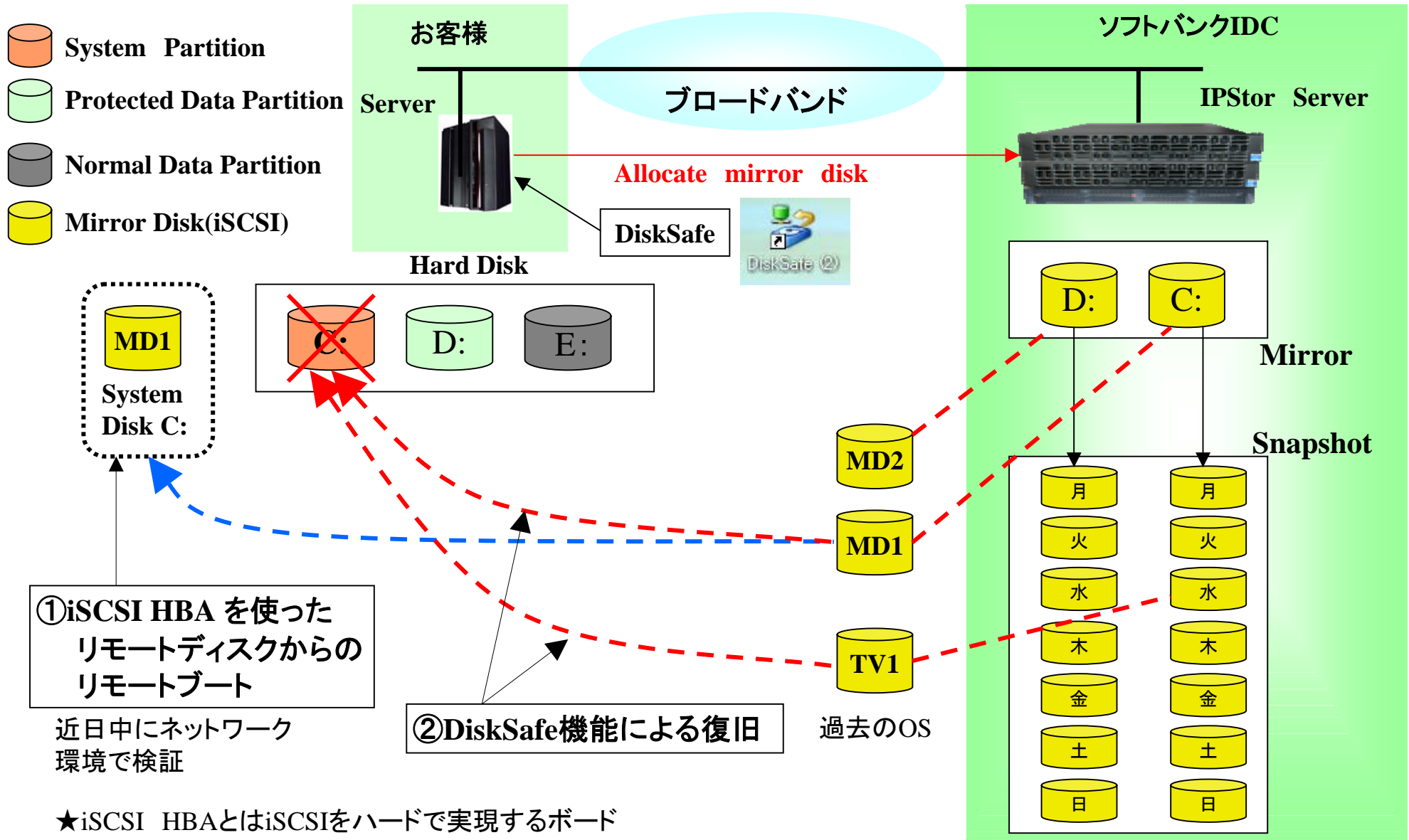


リカバリーシナリオ (DiskSafe機能)

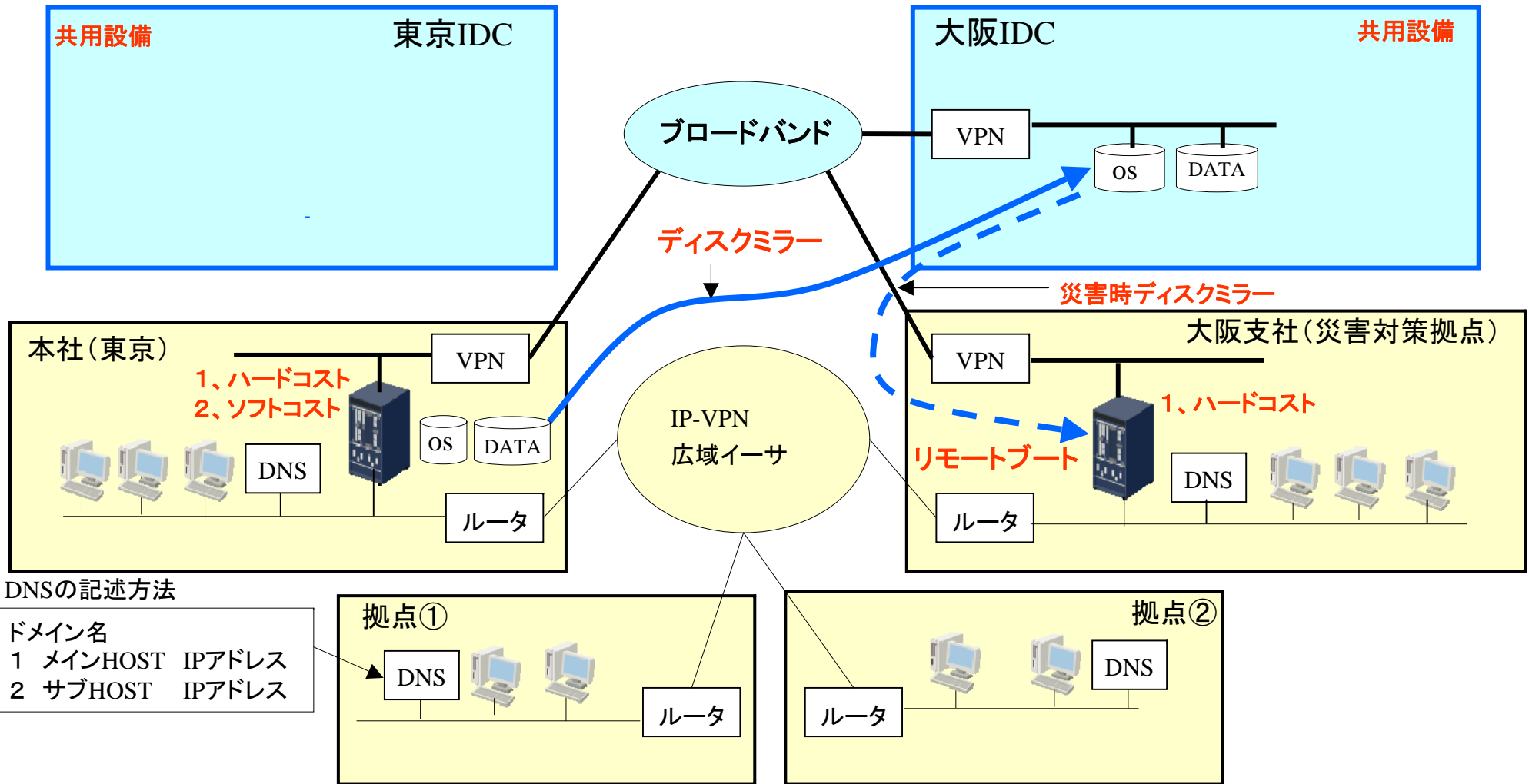
-  System Partition
-  Protected Data Partition
-  Normal Data Partition
-  Mirror Disk(iSCSI)



リカバリーシナリオ (iSCSI HBA) 近日提供予定



iSCSI HBAによるリカバリーシナリオ






DNSの記述方法

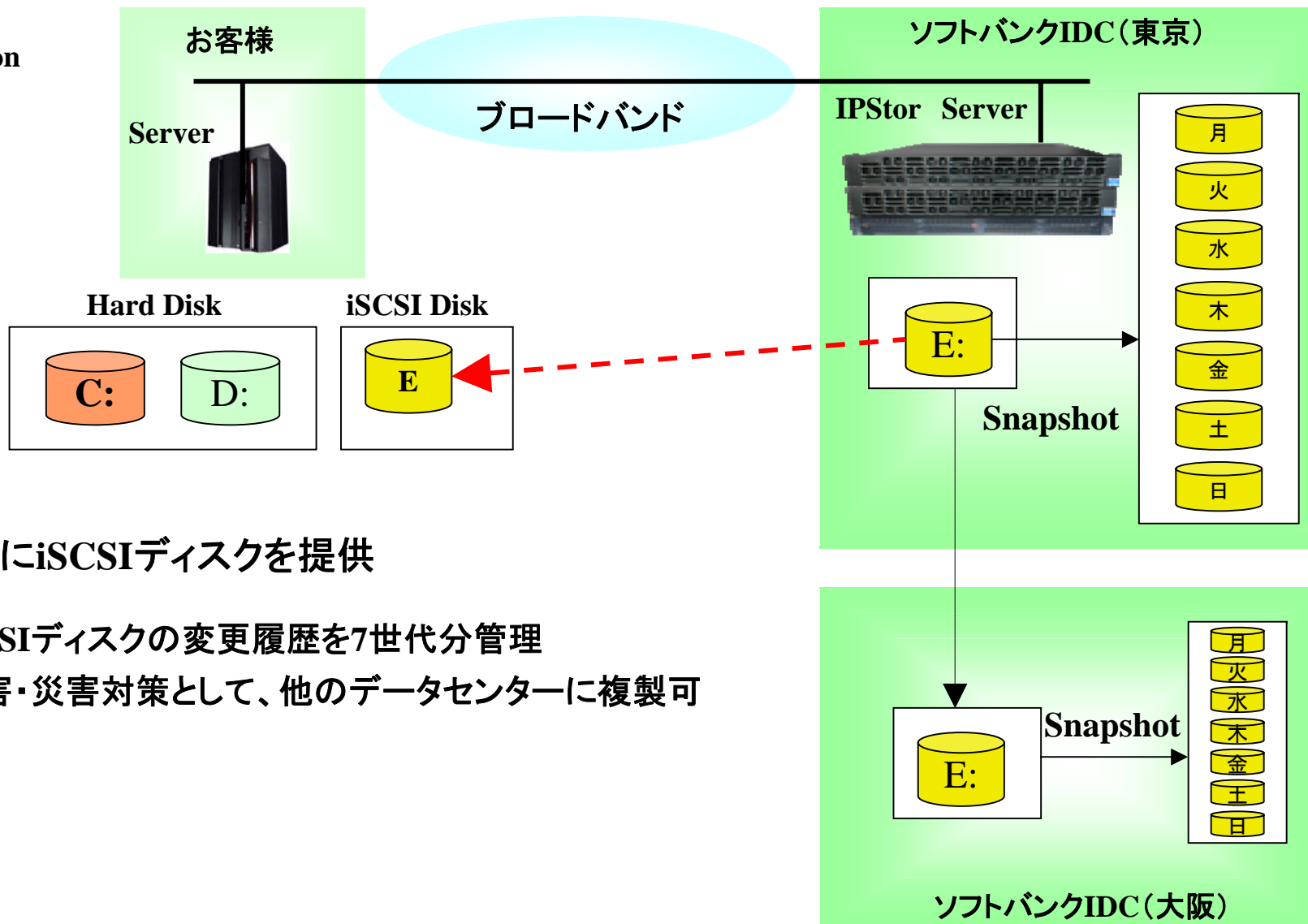
ドメイン名
 1 メインHOST IPアドレス
 2 サブHOST IPアドレス

東京のサーバのOSとDATAを大阪IDCにミラーリングする。災害時は大阪支社のサーバを大阪IDCのOSでリモートブートする。
 これにより、システムのダウン時間を最小にする事が可能になる。

Fileサーバ型のご紹介

Fileサーバ型のご紹介




-  System Partition
-  Data Partition
-  iSCSI Disk

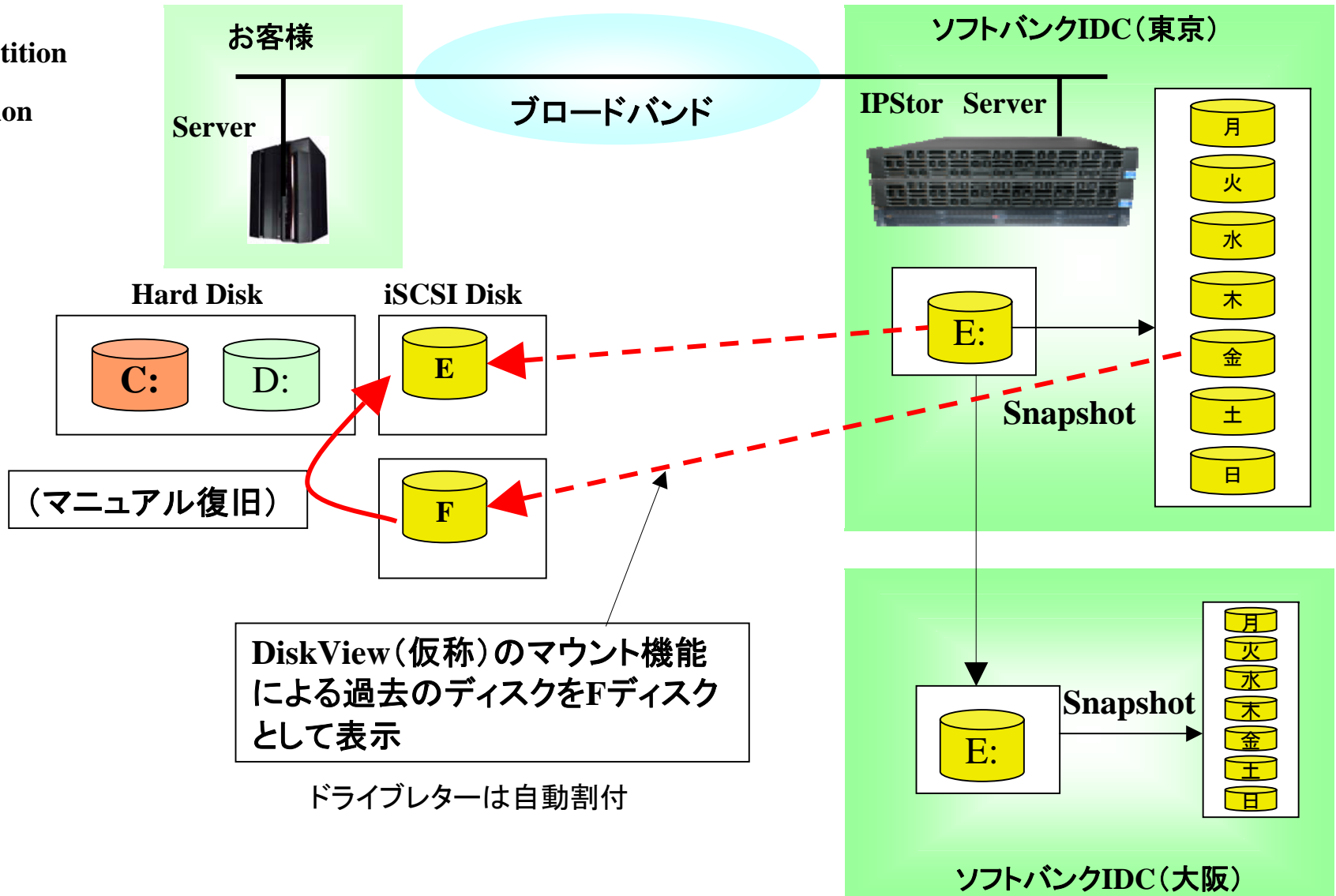


お客様サーバにiSCSIディスクを提供

- 1、IDCではiSCSIディスクの変更履歴を7世代分管理
- 2、データの障害・災害対策として、他のデータセンターに複製可

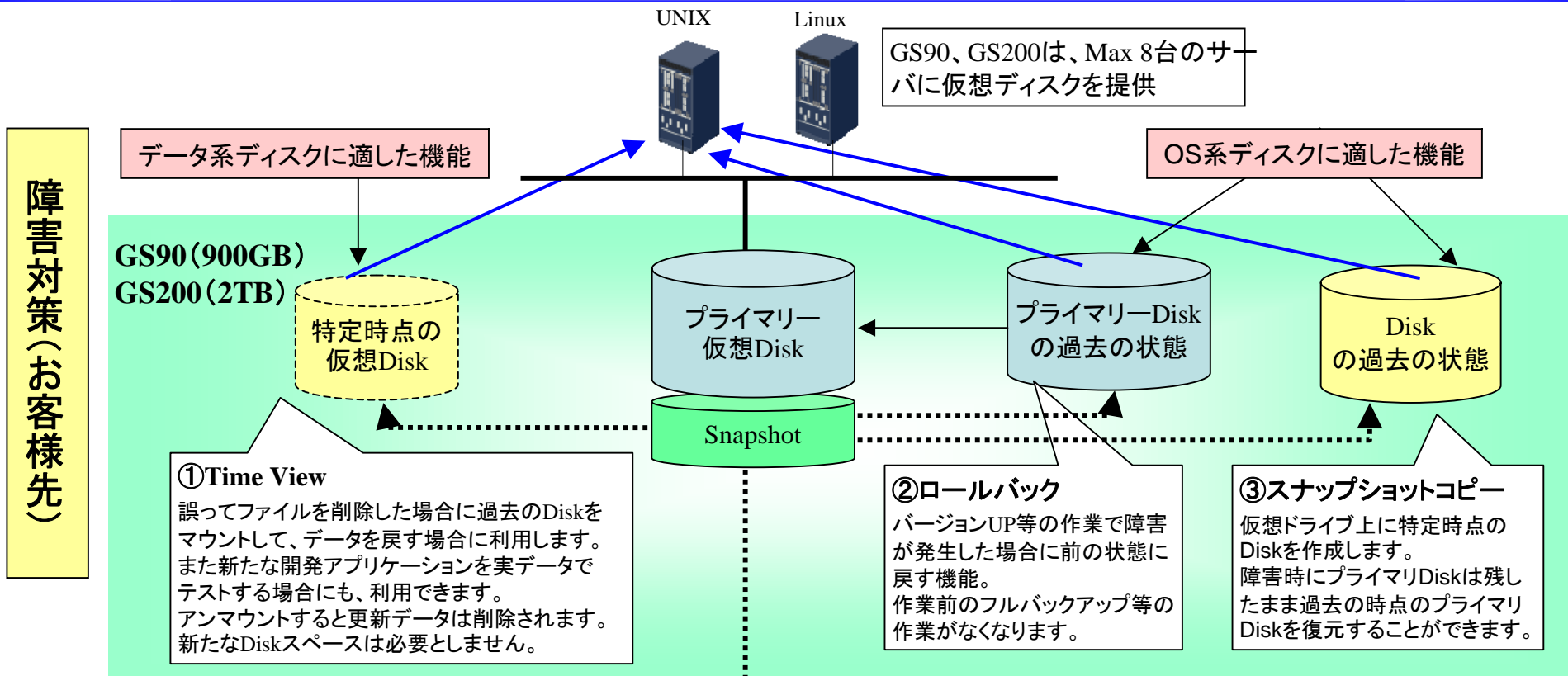
リカバリーシナリオ (DiskView: 仮称)

-  System Partition
-  Data Partition
-  iSCSI Disk

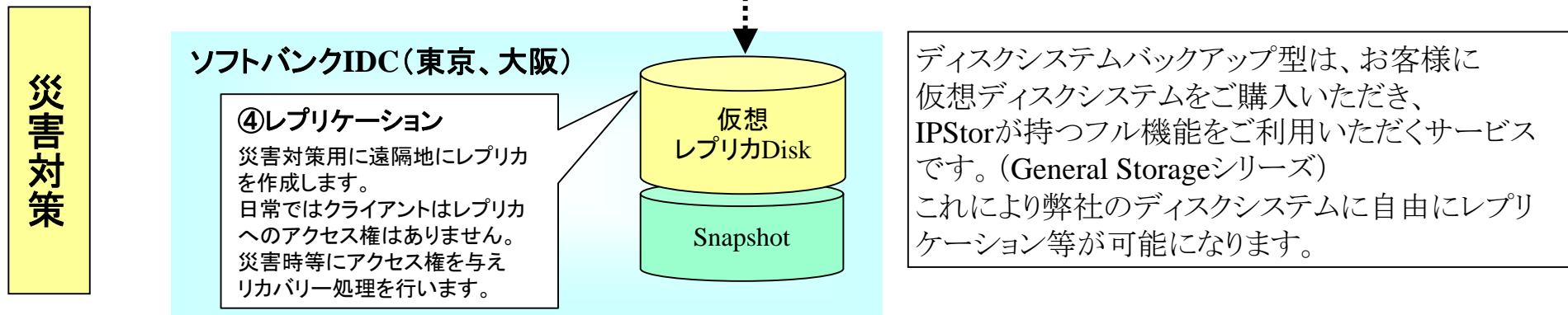


Diskシステムバックアップ型のご紹介

Diskシステムバックアップ型の特徴



障害対策(お客様先)



災害対策