接続ユーザ向けキャッシュDNS サービスレベル向上の取り組み

ビッグローブ株式会社
システム基盤本部

自己紹介

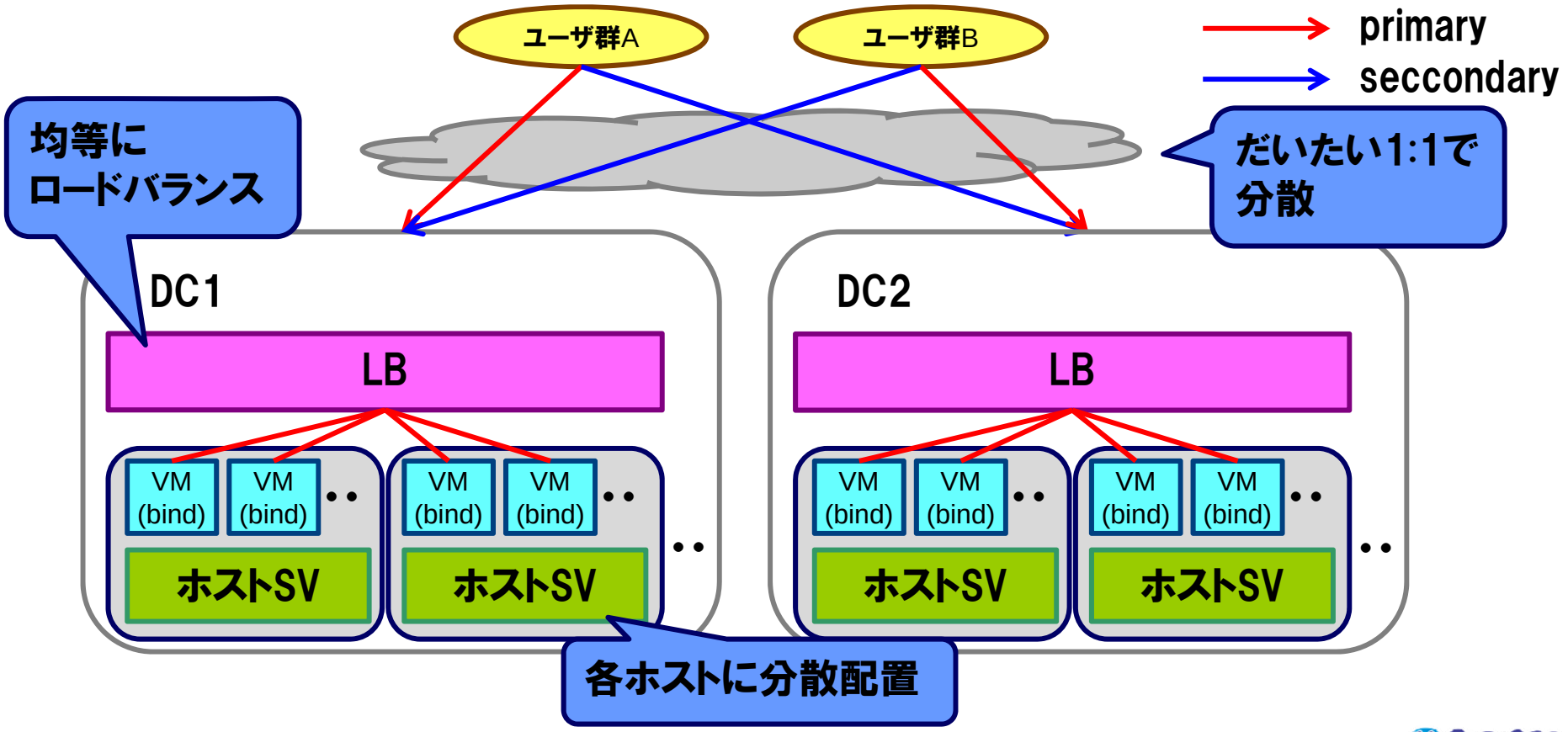
永末　喜己

・2005年入社
・2011年頃からDNS全般を担当し始める
・DNS、ミドルウェア、その他インフラ系の諸々を担当

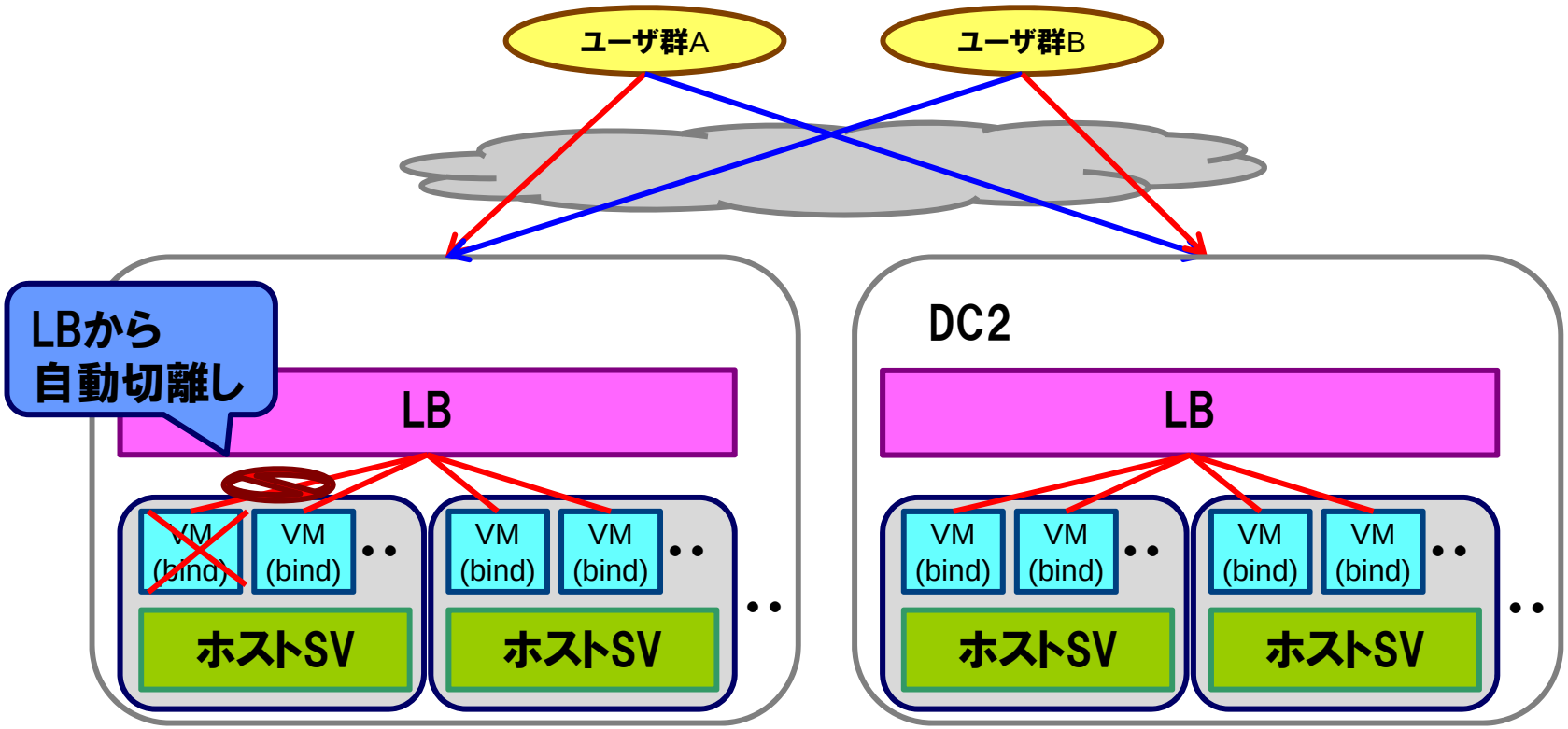
目次

- サービスレベル向上の取り組み
  - システム構成紹介
  - 物理レイヤ
  - 作業ルール
  - 攻撃対策
- こんなことがありました

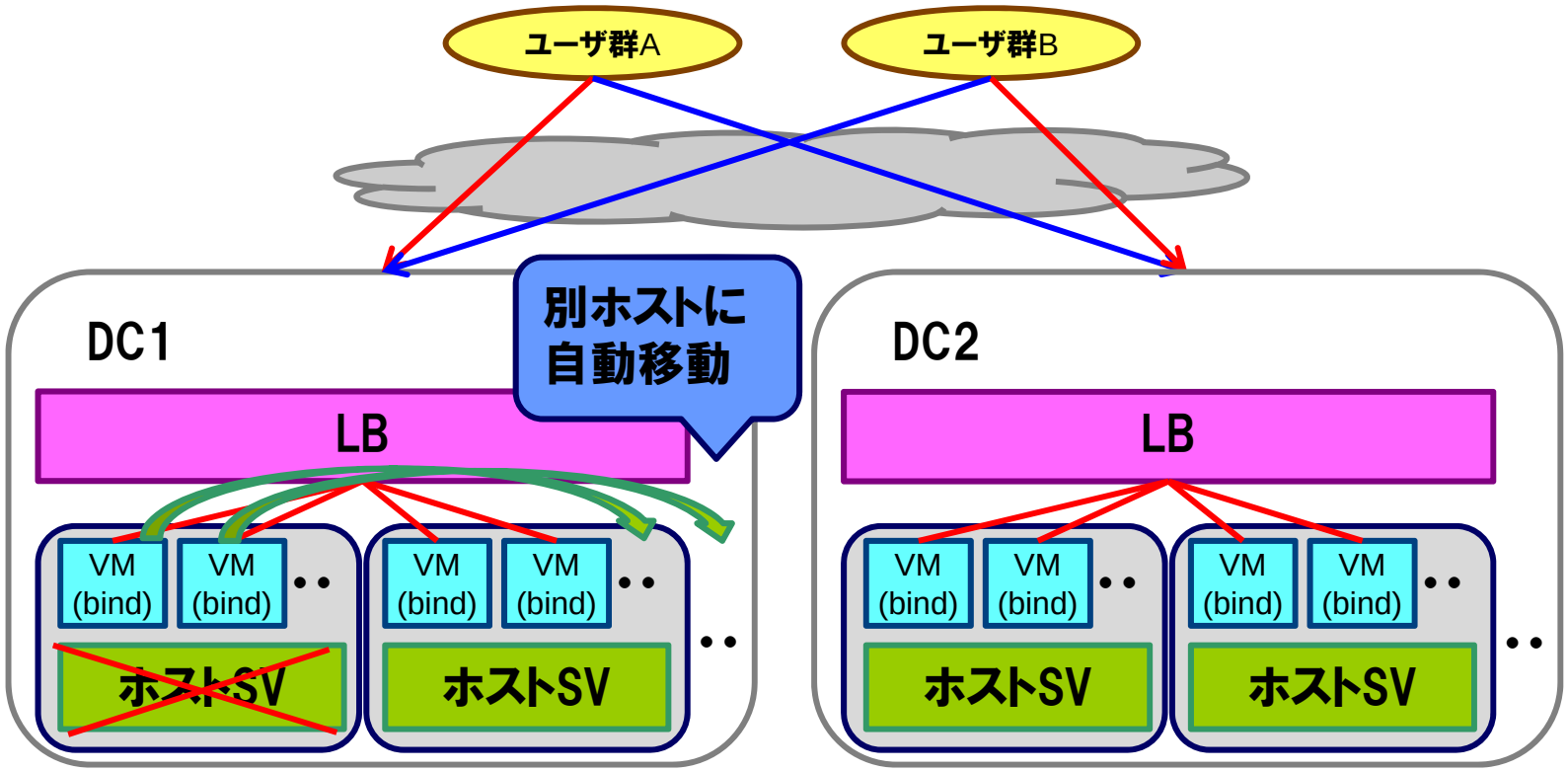
構成概要



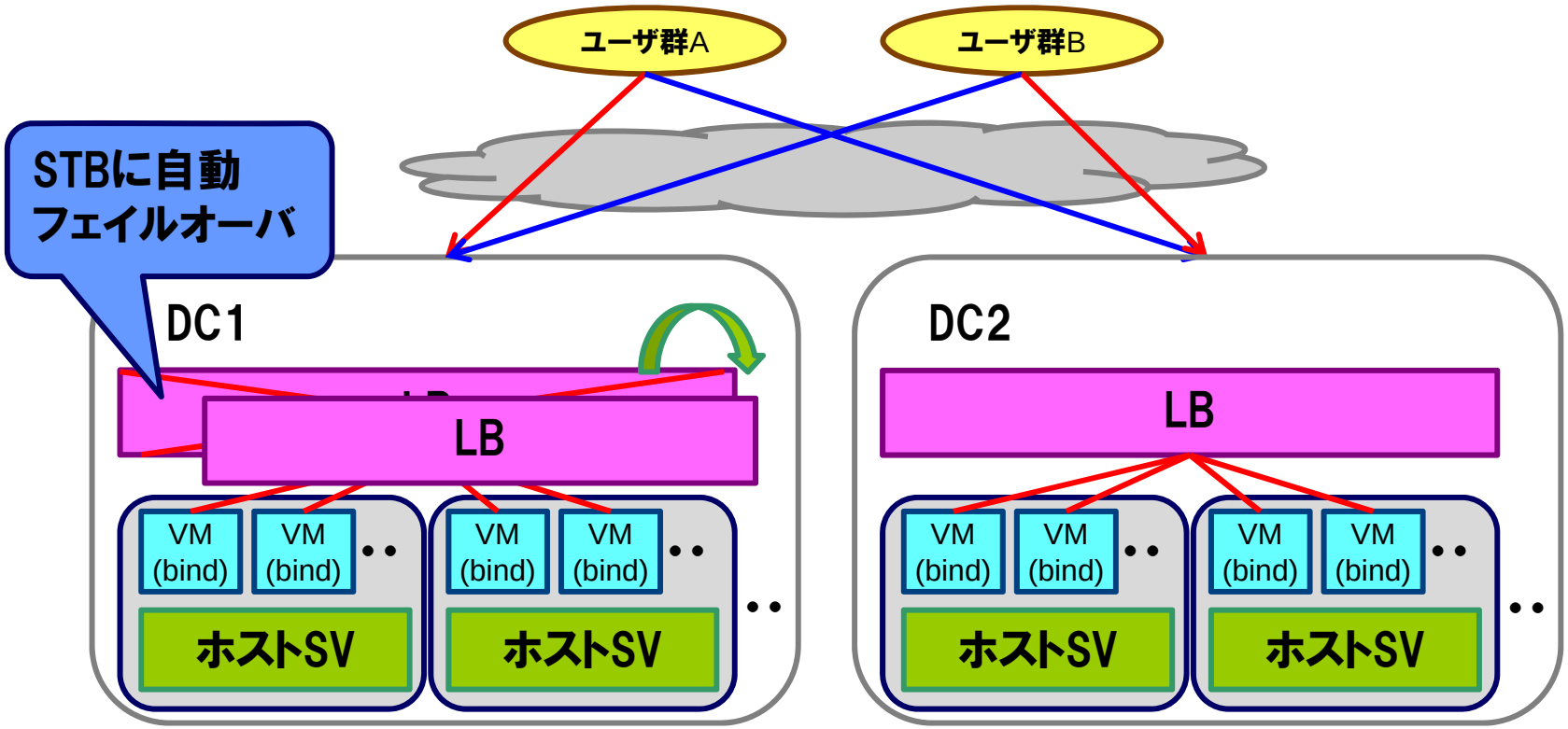
仮想サーバに異常があった場合



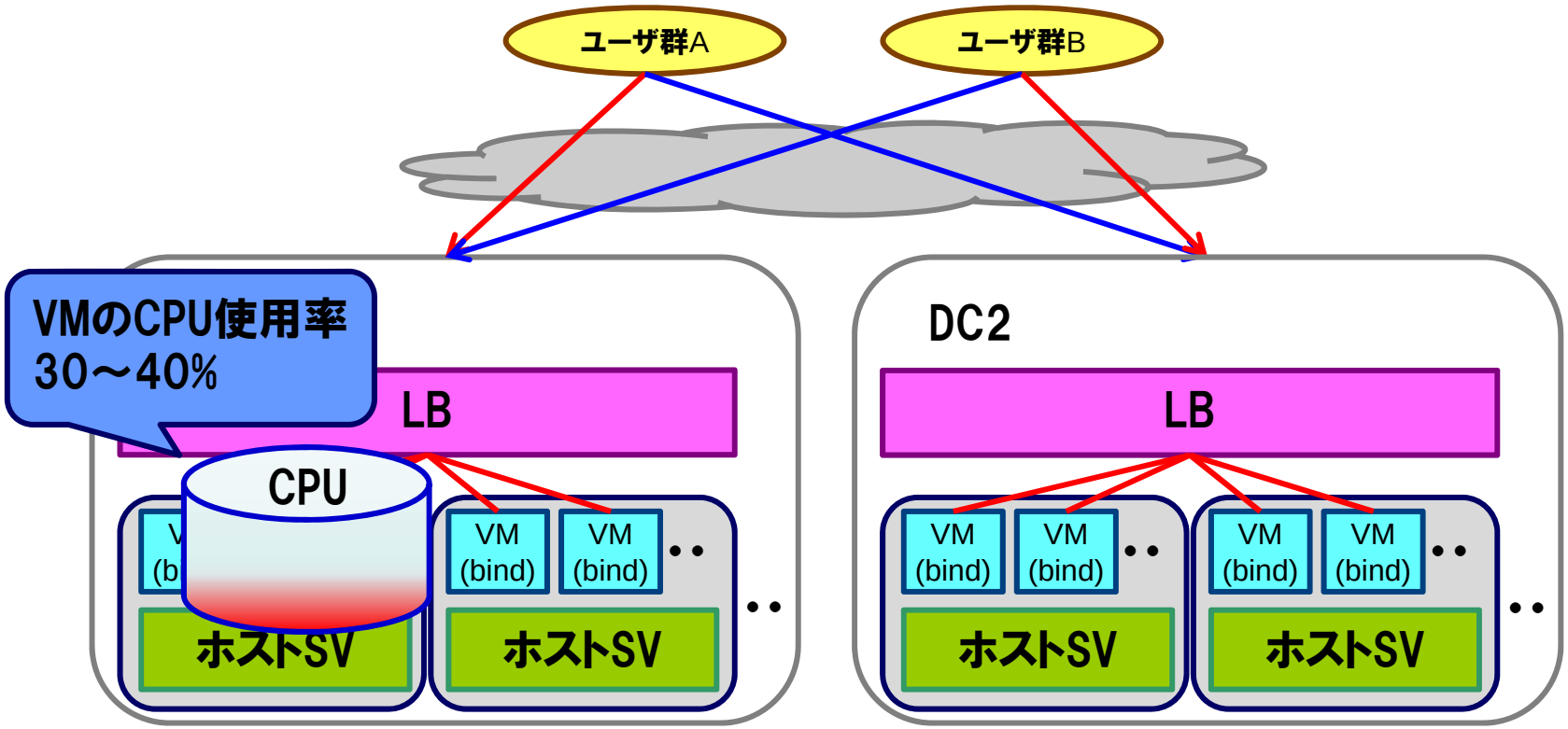
ホストサーバに異常があった場合



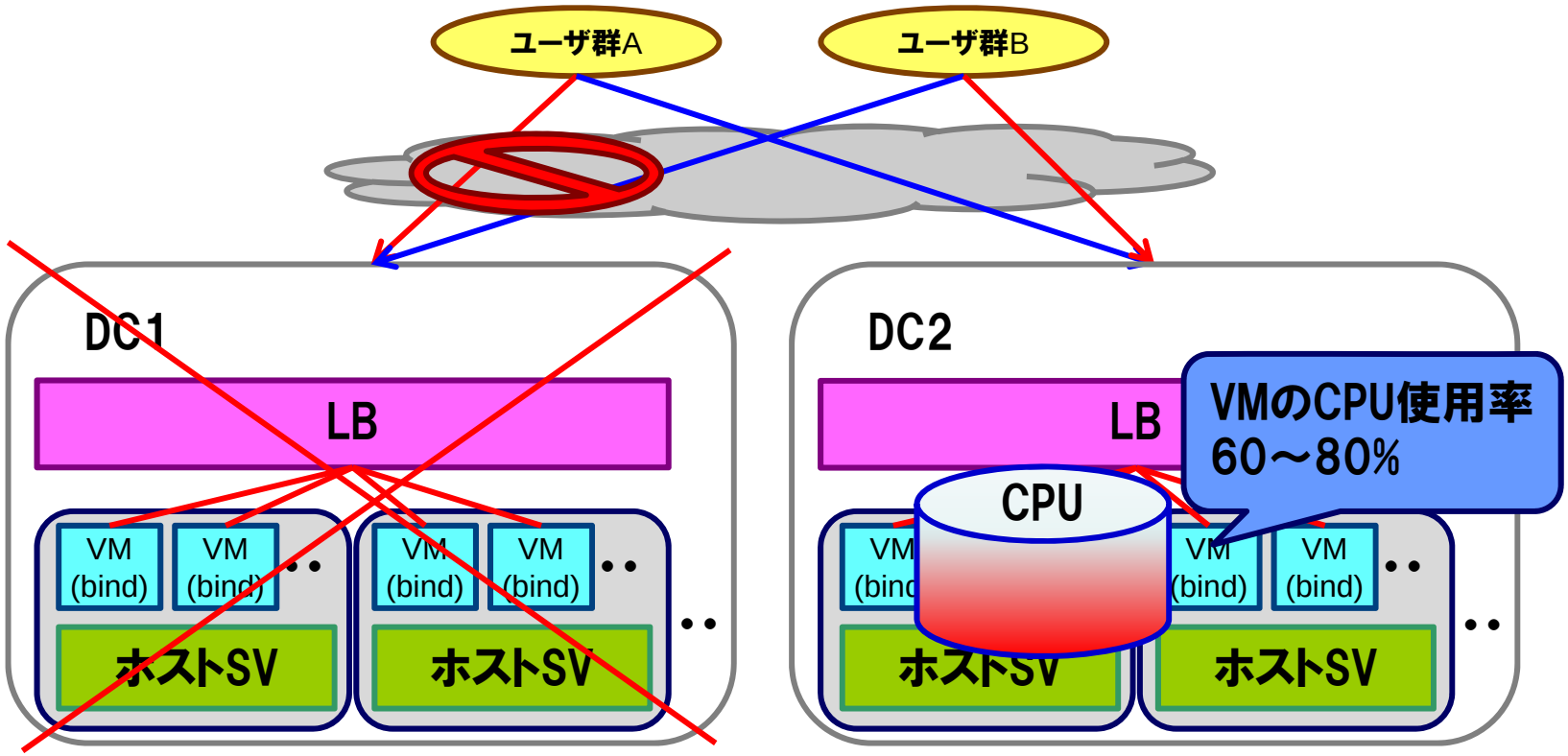
ロードバランサに異常があった場合



データセンタに異常があった場合



データセンタに異常があった場合



物理レイヤ

- 耐震/耐火/防水
- 防犯(入退室管理、監視カメラ等)
- 電源/回線等の冗長化
- 24H365日常駐監視、遠隔監視

システム変更時の作業ミス防止

- システムに変更を加える際は必ず手順書を作成
- 手順書を複数人でレビュー、上司による承認
  - 手順に誤りはないか
  - バックアップの取得/削除は行っているか
  - 作業後に正常性確認は行っているか
  - 切り戻し手順はあるか
- 作業は必ず複数人で実施
- 大きな変更作業は、影響の少ない装置から実施

作業ミスによるサービス断を防止

監視

- サーバリソース監視
  - CPU、メモリ、ロードアベレージなど
- DNS応答監視
- ログ監視
- などなど

サービス異常を迅速に把握・復旧

以上の対策で、通常はサービスに影響がでる障害は
そうそう起こっていない

一番の脅威は**攻撃**

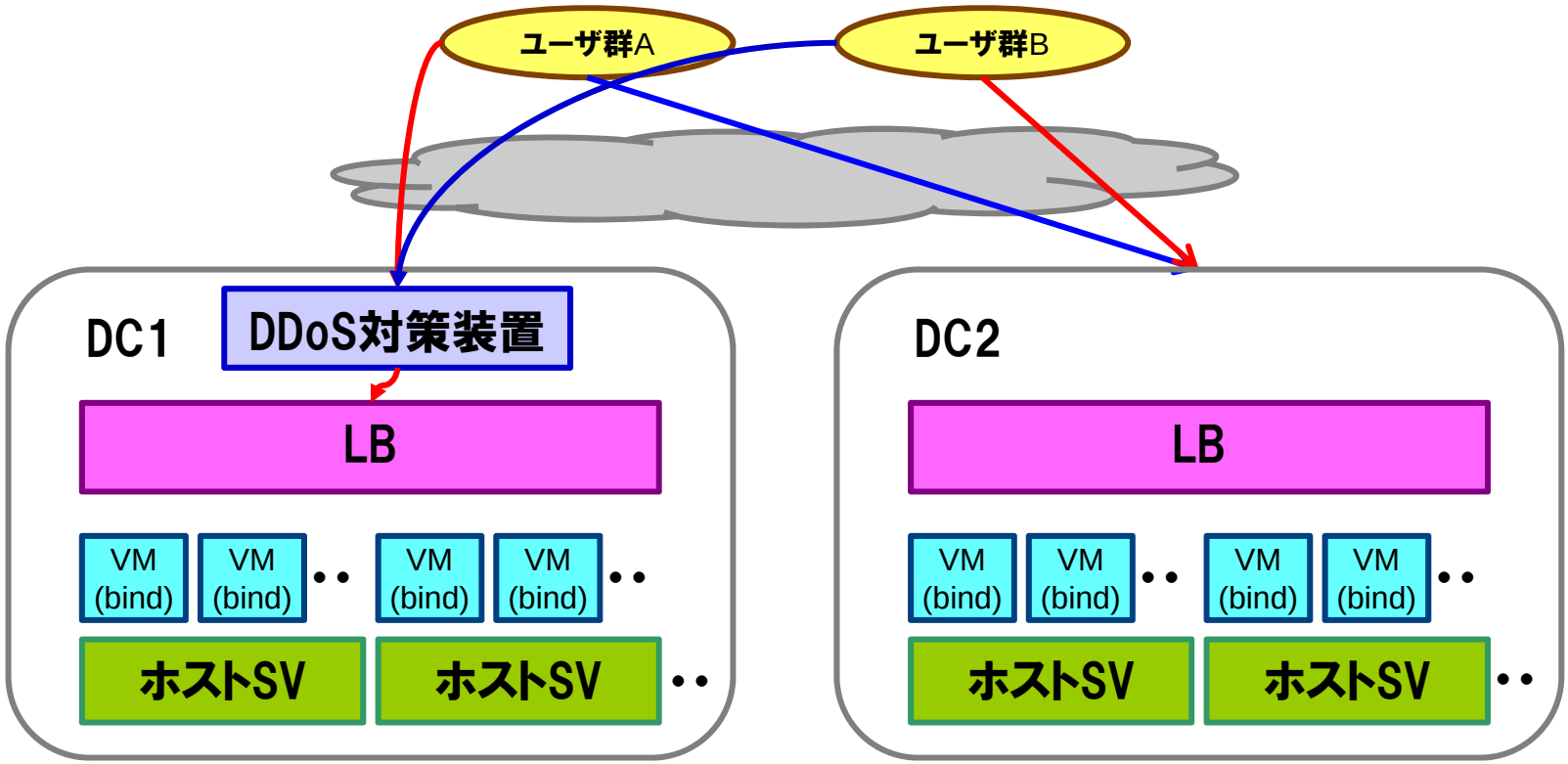
攻撃対策を一部紹介　→

DDoS対策装置

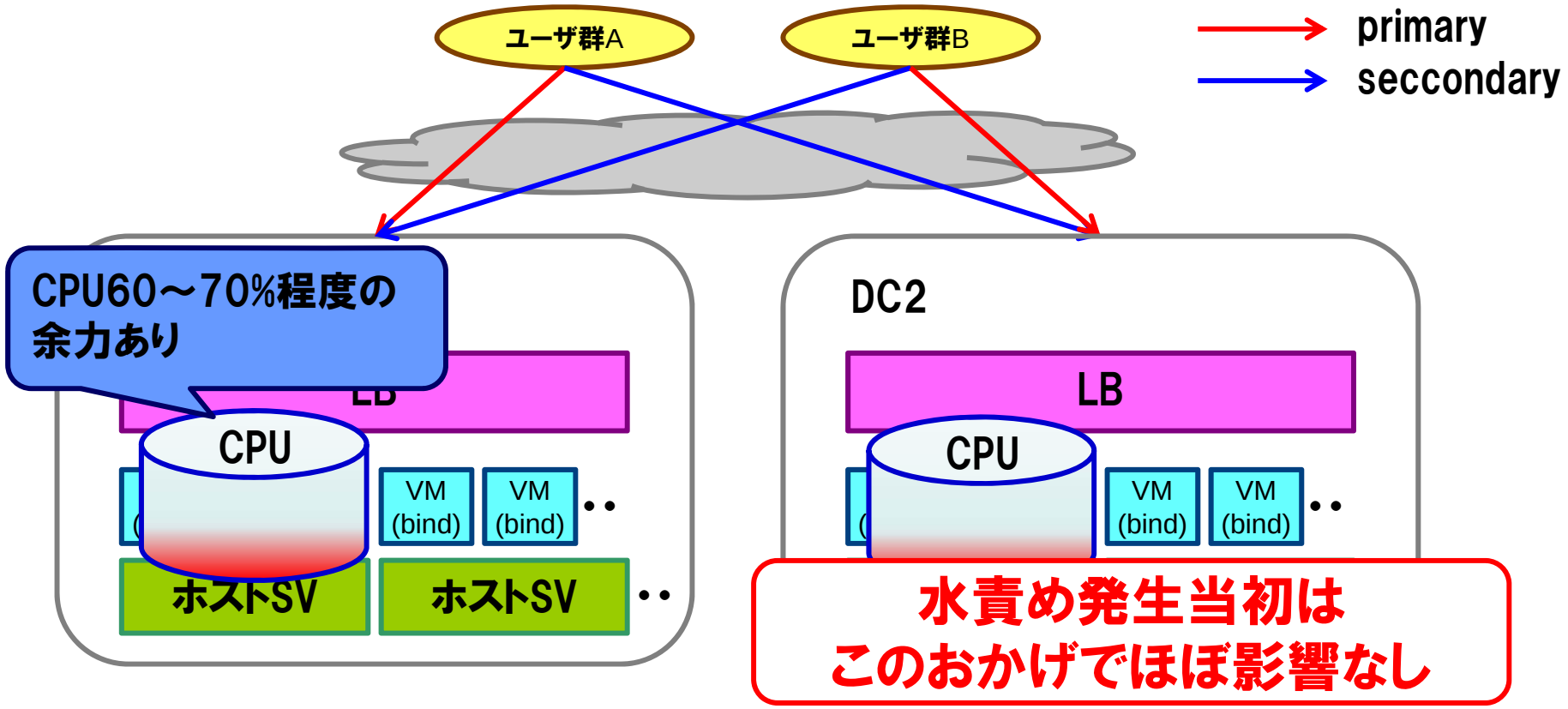
- 緊急時にロードバランサの前段に投入
- Amp対策
  - 特定IPアドレスからの大量クエリをドロップ
- 水責め対策
  - “ランダム”.example.jp で攻撃が来ている場合、「example.jp」をターゲットに設定
  - “ランダム”が10文字以上かつ200QPSを超えた場合、40QPSまで流量を制限

※数値は一例

DDoS対策装置のイメージ



拠点冗長による余剰リソースで防御力アップ



リソース増強(力技)

- CPU、メモリ増強
- サーバ増設

  ※仮想サーバはDNS専用のホストサーバではなく、
  大量に存在するビッグローブサービス共用の
  ホストサーバに収容しているため、比較的容易に
  実施可能

Bind脆弱性対応（7月ですし）

- パッチ（新バージョン）展開の迅速化
  - 脆弱性を攻撃される前にパッチ適用が必要
  - Jenkinsで自動ビルド、自動テスト（計画中）
  - パッチ適用のルーチン化
    - パッチ公開初日には、1拠点の主要なDNSにはパッチを適用（あえて全台にはやらない）
    - 2日目～4日目で残りのサーバに適用
  - ISCとサポート契約（今はできていませんが…）
- 一部サーバでUnboundを運用中
  - Bindでゼロデイが発生したらUnboundに置き換え

こんなことがありました

こんなことがありました

- 海外の某権威DNSからフィルタされた
  - 社内向けの一部DNSで特定ドメインを検索不可に
  - 権威DNSのWhoisの連絡先に連絡してみるも無反応
  - つてをたどって、権威DNSの会社の人に連絡するも
    「私は担当じゃないから」
  - 権威DNSに乗っているドメインの会社（日本）に連絡
    - その会社から権威DNSの会社にクレームが入り、原因が発覚
    - 原因は権威DNS側の設定ミス

**海外の権威DNSにフィルタされたら、DNS自体の運営会社ではなく
その上に乗っている会社に連絡した方が反応がよさそう**

課題

- 攻撃が絶えない
  - 皆様の対策など、教えていただければありがたいです

以上