RSA CONFERENCE 2014
アジア太平洋地域および日本

Share.
Learn.
Secure.
集約型インテリジェンスの活用

クラウド トラスト 新定義：
強力な防御に不可欠な8つのステップ

セッションID：JPN-T11

Davi Ottenheimer

トラスト担当シニア ディレクター
EMCコーポレーション
@daviottenheimer

クラウドトラスト 新定義

透過性

関連性

回復力

クラウド脆弱性のタイプ例

1. **Iceberg**
   - CardSystems
   - Sony

2. **Evil Maid**
   - Google
   - Shionogi
   - サンフランシスコ市

3. **SLA-urprise**
   - Salesforce
   - Amazon
   - Google

4. **Barn Door**
   - LinkedIn
   - Groupon

教訓

1. （規制された）データの除去
   - World
   - Large
   - Named
2. 境界の定義
   - サービス、ポート、リスナー、インターフェイス
   - 権限、プロセス、パターン
3. アクセス用のセキュアなID
4. 監視の変更、「脆弱性」と人の動作
5. データの保護

不可欠なステップ

1. ターゲット領域の縮小
2. I&Mの管理
3. 監視とアラート
4. 可用性の管理

5. 統合（自動化）
6. セキュリティのテスト
7. インシデントへの対応
8. バックアップとリストア（終了）

1. ターゲット領域の縮小

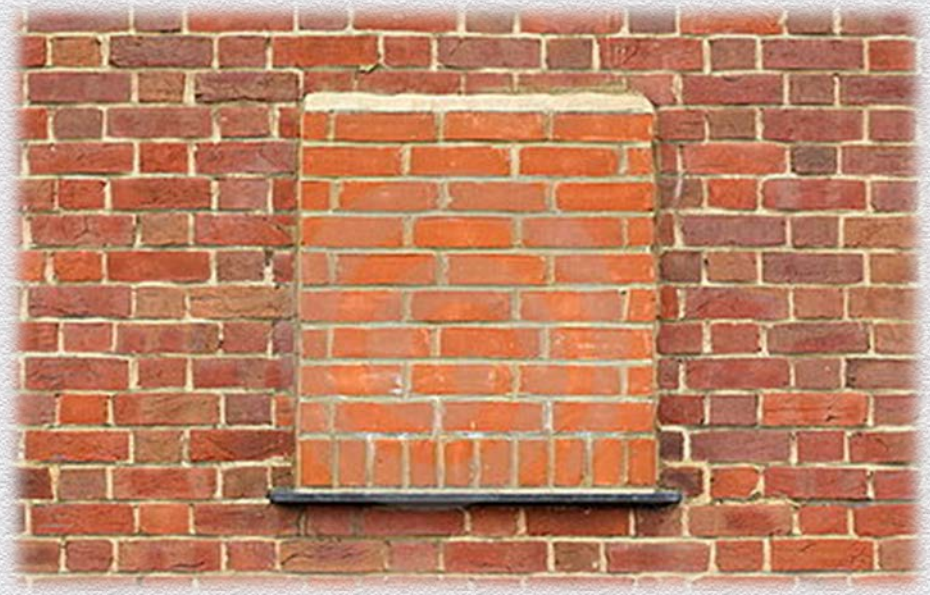
- 強固なイメージ
- 信頼できるソースからのインストールのみ
- パッケージ シグネチャのチェック
- 管理のための多要素認証

  （多要素を使用するAPIは扱いにくい場合がある）

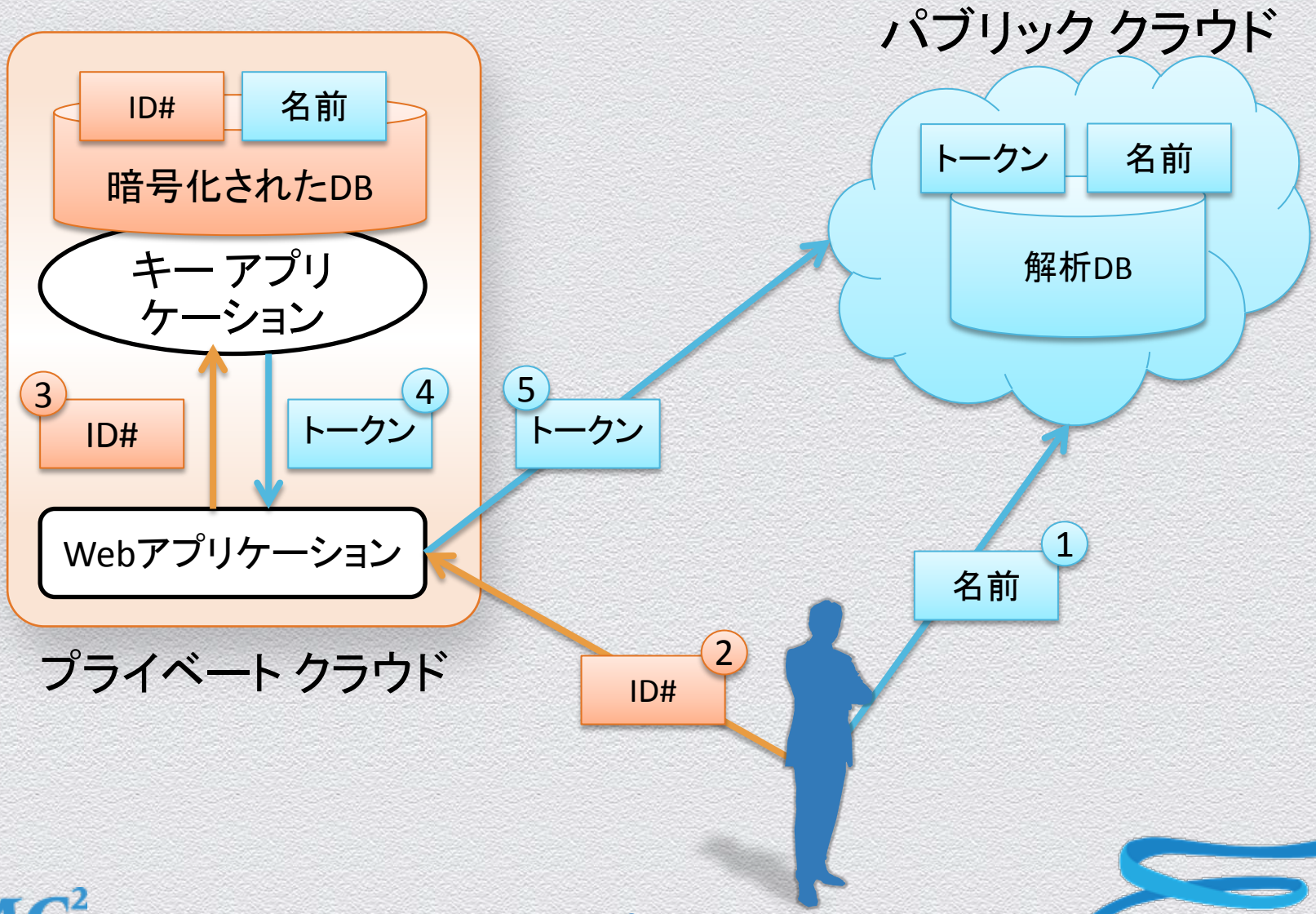
1. ターゲット領域の縮小

- リスクを管理可能にする
- 欠陥調査のトレンド
  - KVM（qemu/PIIX、Nelson Elhageによる功績）
  - VMwareバリアントでのCloudburstビデオドライバーのハッキング
  - 仮想ビデオframebuffer経由のXenハッキング

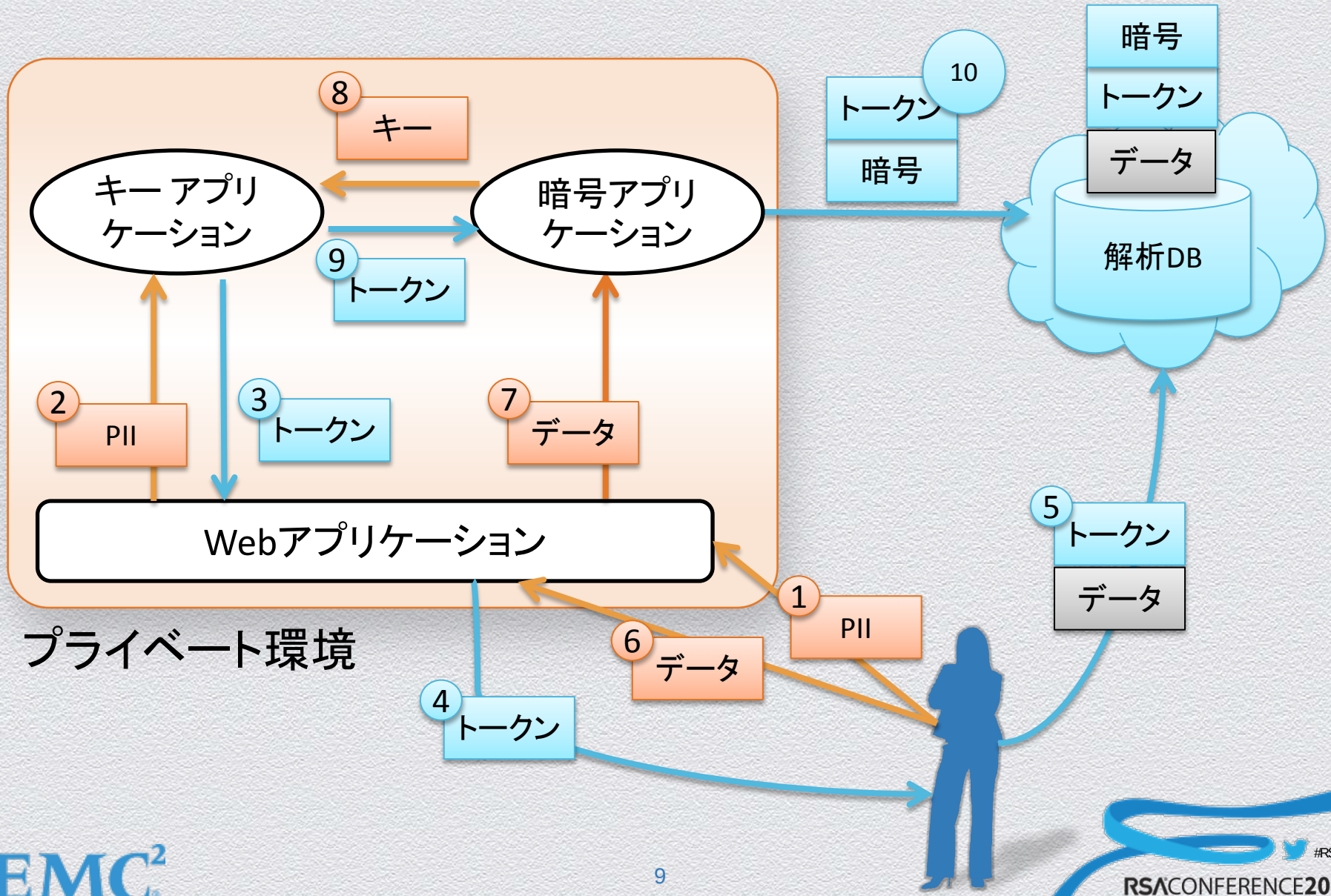
…すべて仮想化 ***デバイス***



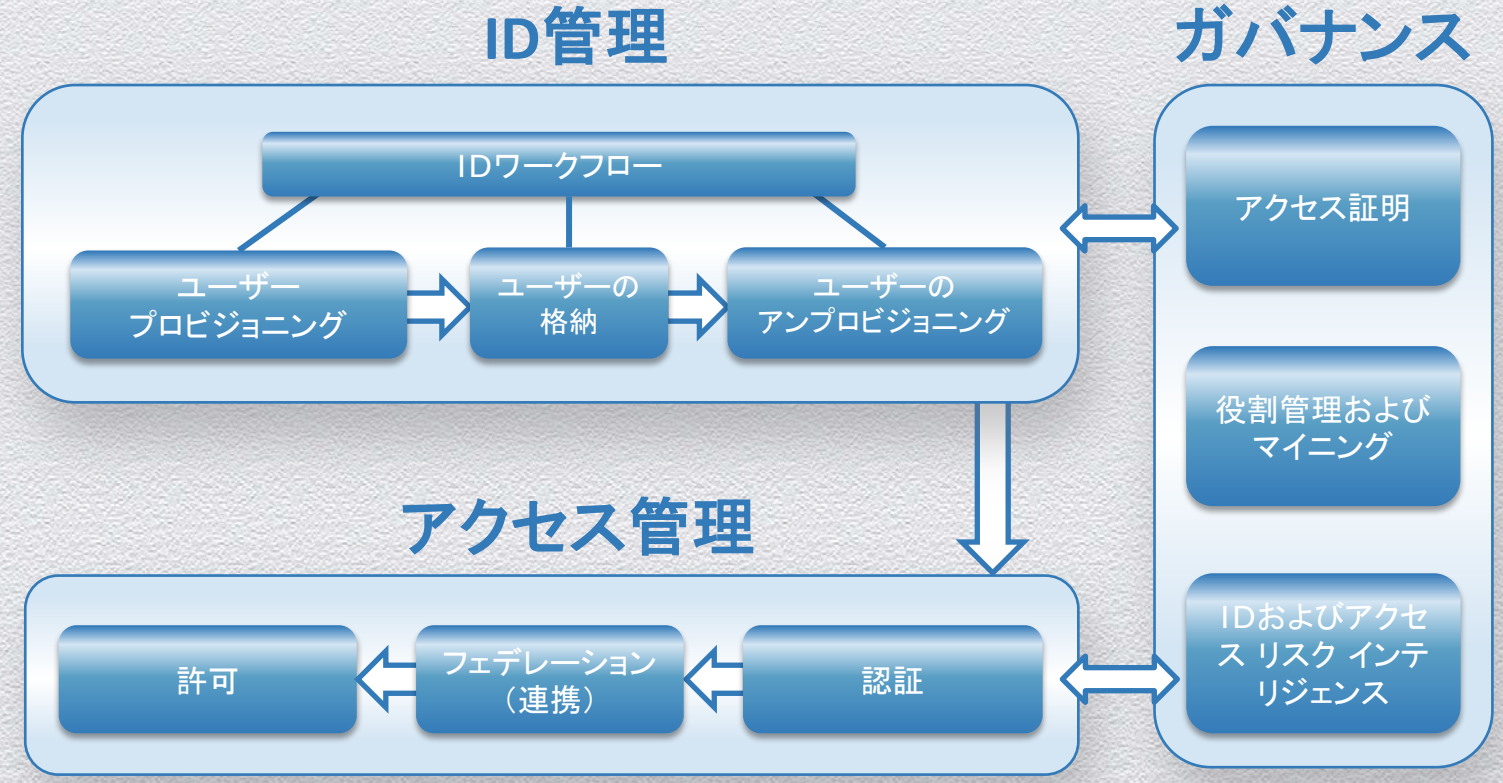
1. ターゲット領域の縮小 – トークン化



1. ターゲット領域の縮小 – 暗号化



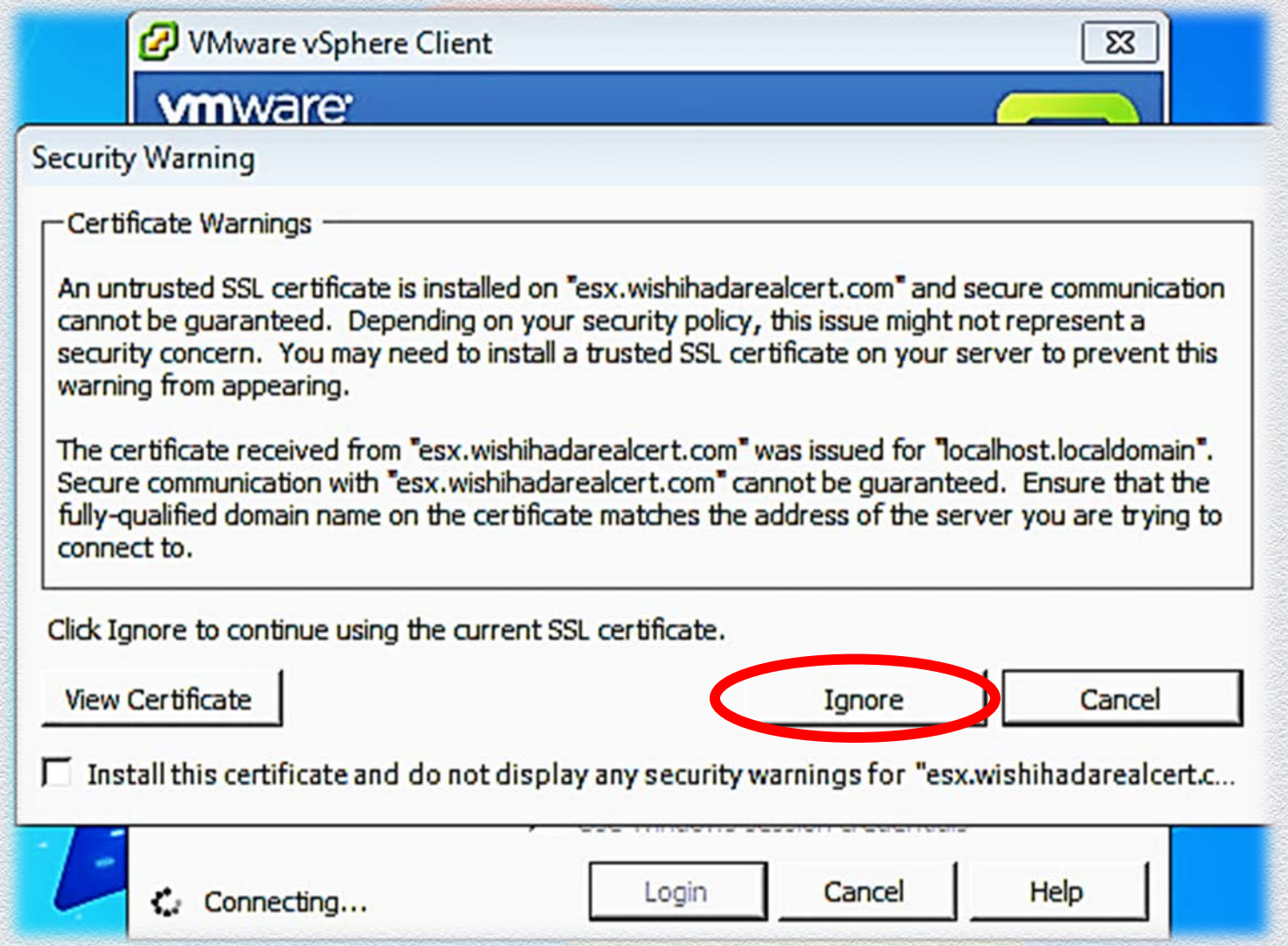
2. IDとアクセスの管理(IAM)

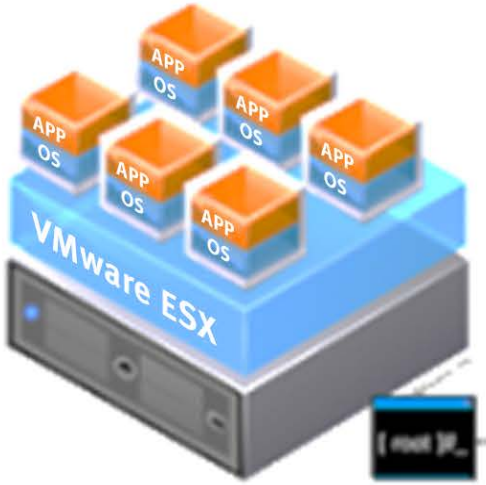


- 共有アカウントを使用しない
- 権限の付与にはグループ(役割)を使用する
- 強力なパスワードを使用する多要素が必要

2. IAM

警告を無視していませんか?

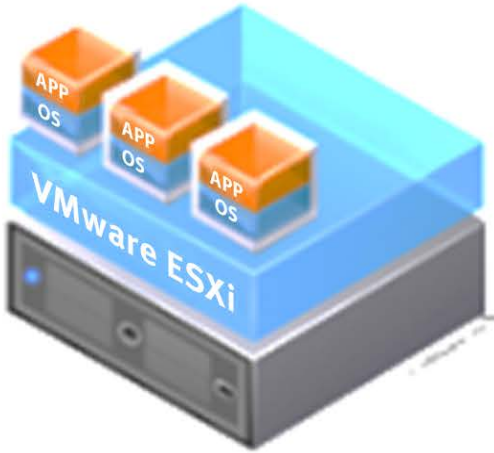




データを分類していますか?

チョーク ポイントはありますか?

マネージャー



ブリッジまたはプロキシ

ディレクトリサービス

ファット

CLI

Web

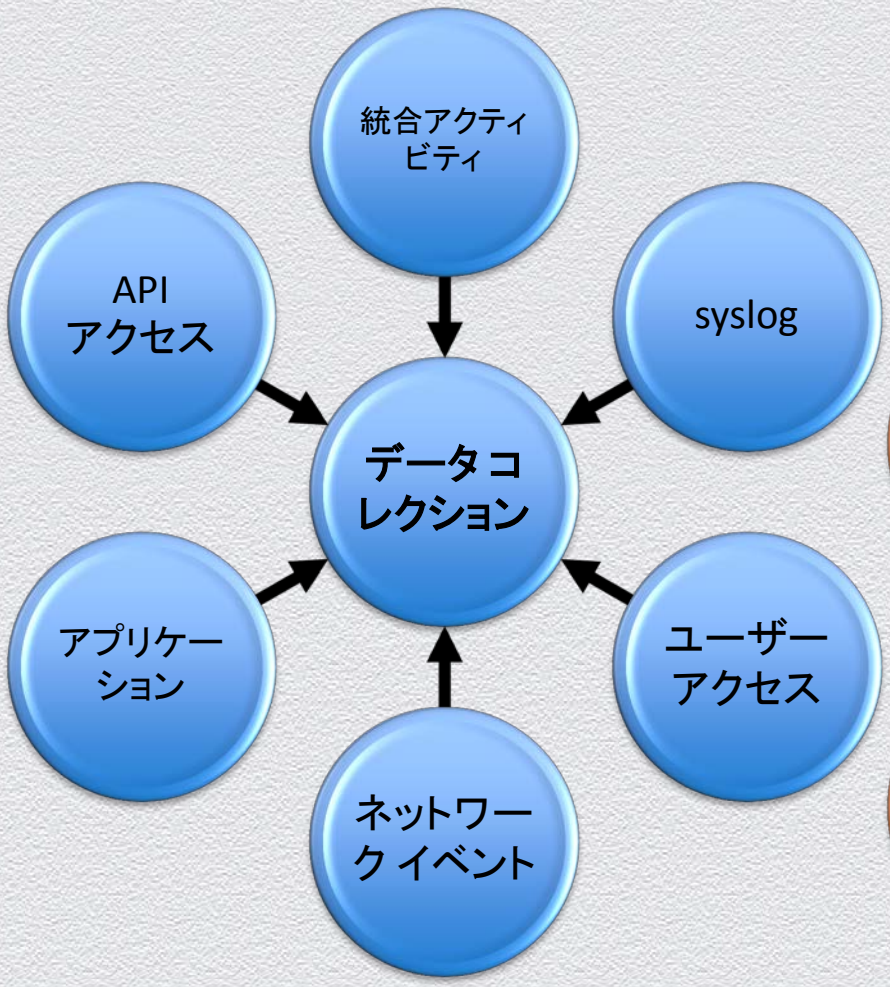
API

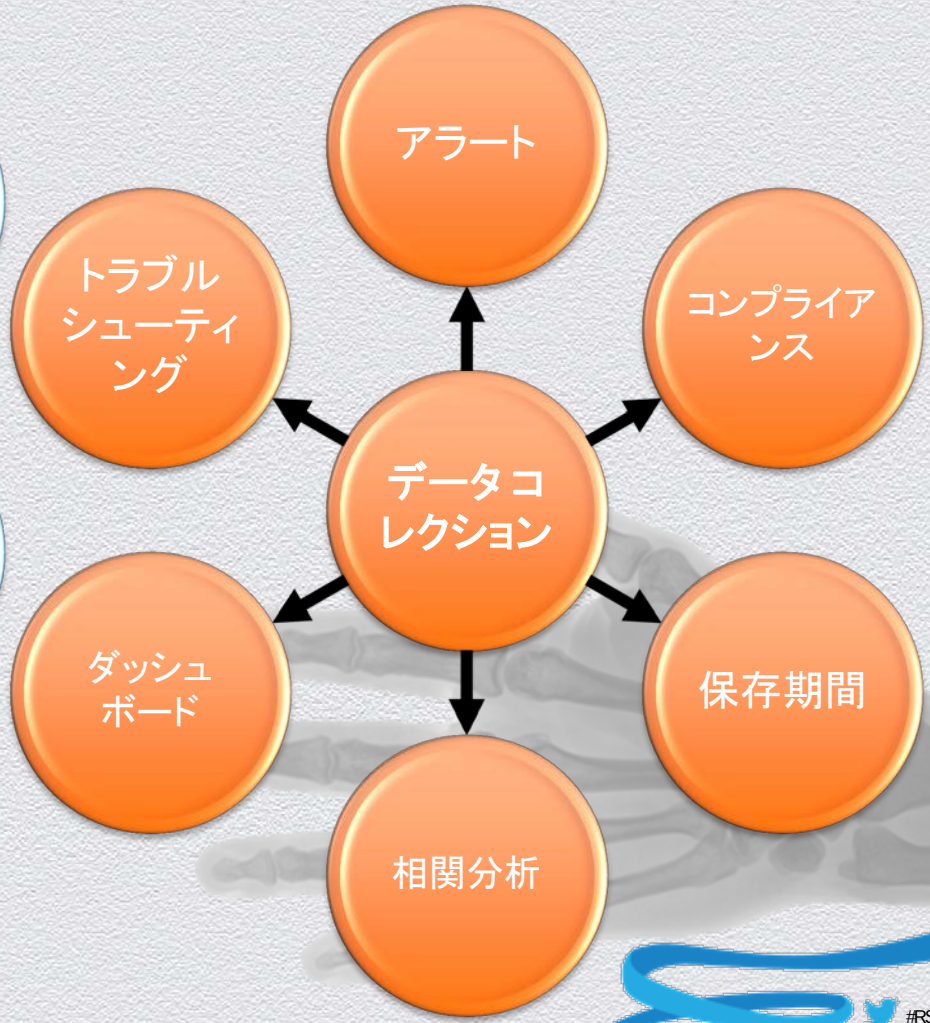
管理インターフェイス

3. 監視とアラート

- 読み取り専用ユーザー/役割
- 可能な限りログに記録（自身へのDoS攻撃にならないように）
- WORMを考慮
- シェルをログに記録（シェルのログインが有効な場合は特にVMware ESXi）
- UNIXのsshd ForceCommandを考慮（不正なトンネルを停止し、ログに記録されないコマンドを停止する）
- すべてのファイアウォールおよびVPNトラフィック、成功と失敗をログに記録、通常のエンド ユーザーVPN = 権限のあるアクセス、弱い制御
- 仮想化ログ = クライアントの保護レイヤー

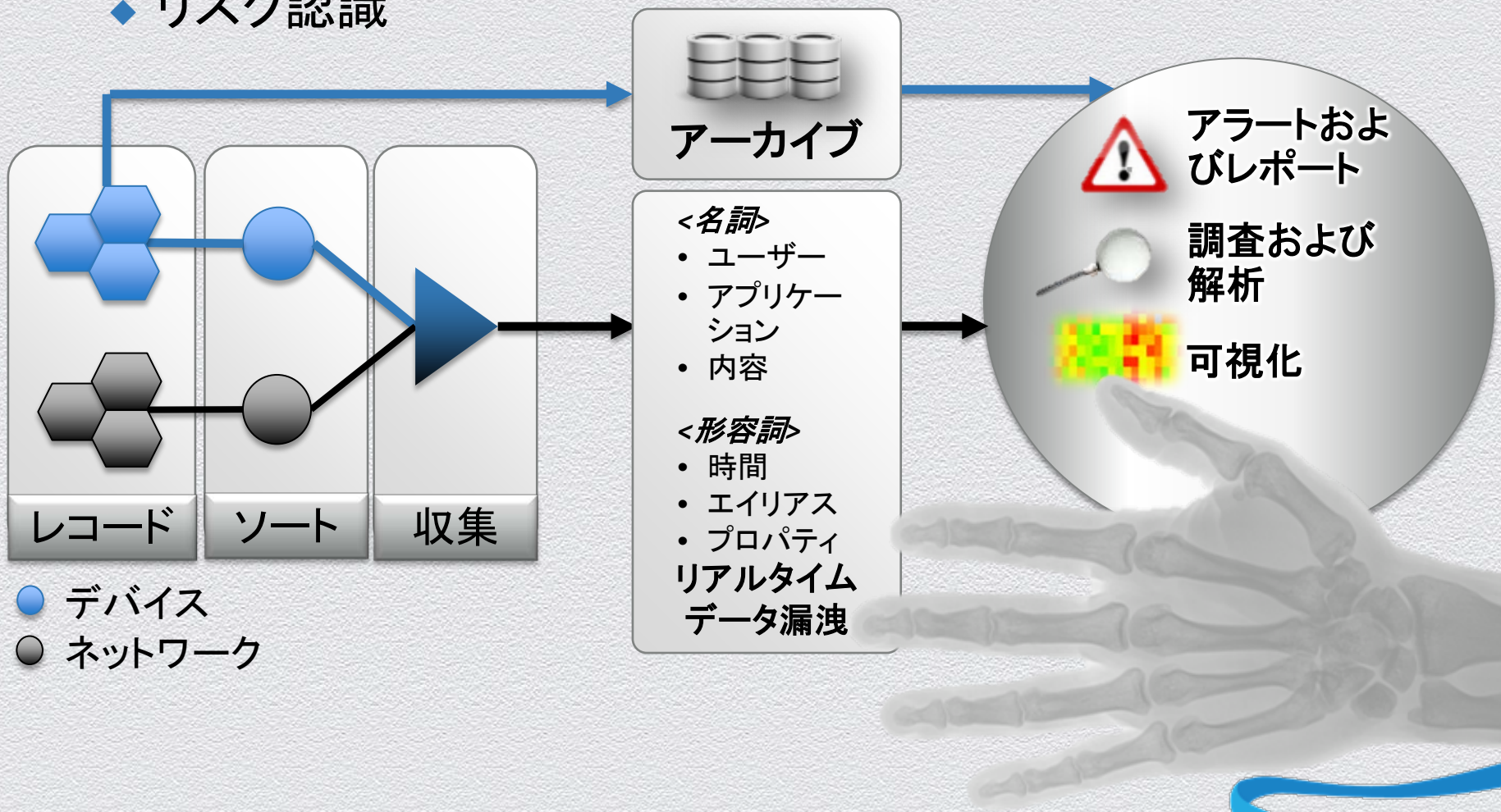
3. 監視とアラート



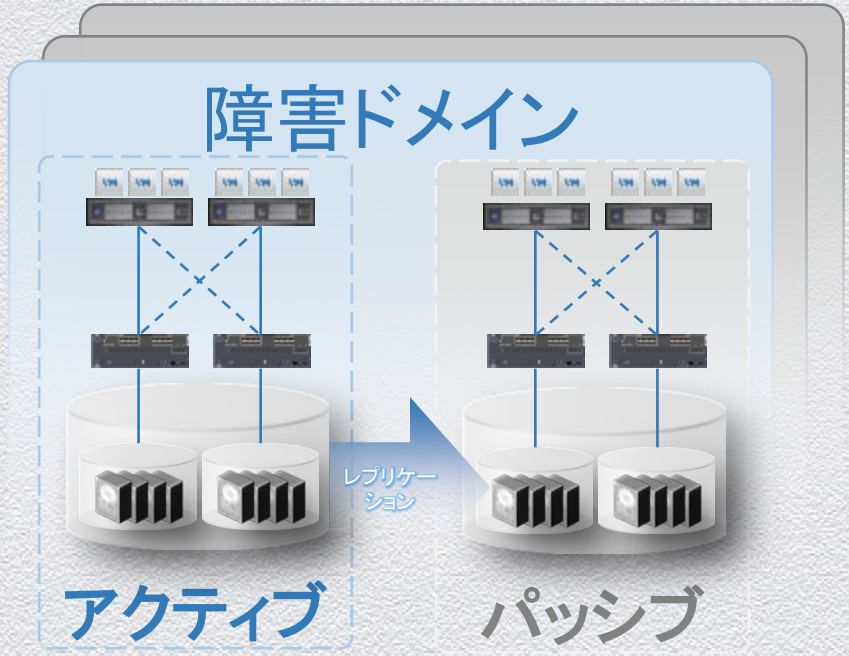


3. 監視とアラート

- インテリジェンス主導型
- リスク認識

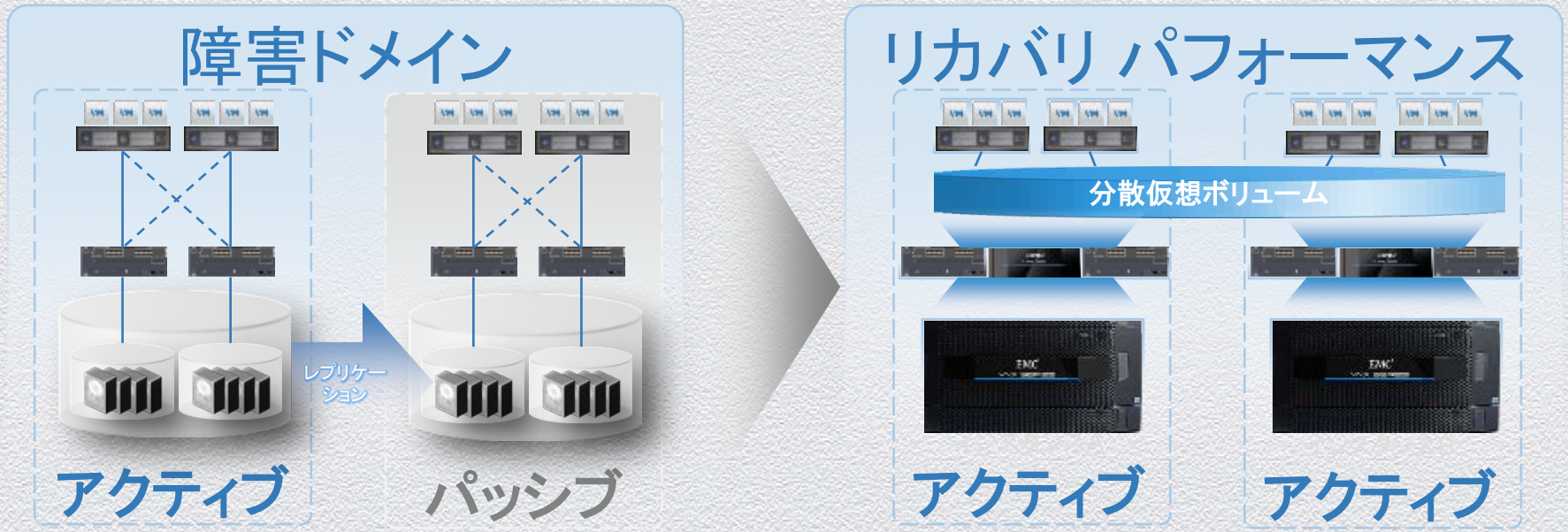


4. 可用性の管理



- アプリケーションの中断
  - 対応予定
  - 計画外
- RTO：数分から数時間
- フェイルオーバーとフェイルバック
- パッシブ、アイドル リソース

4. 可用性の管理

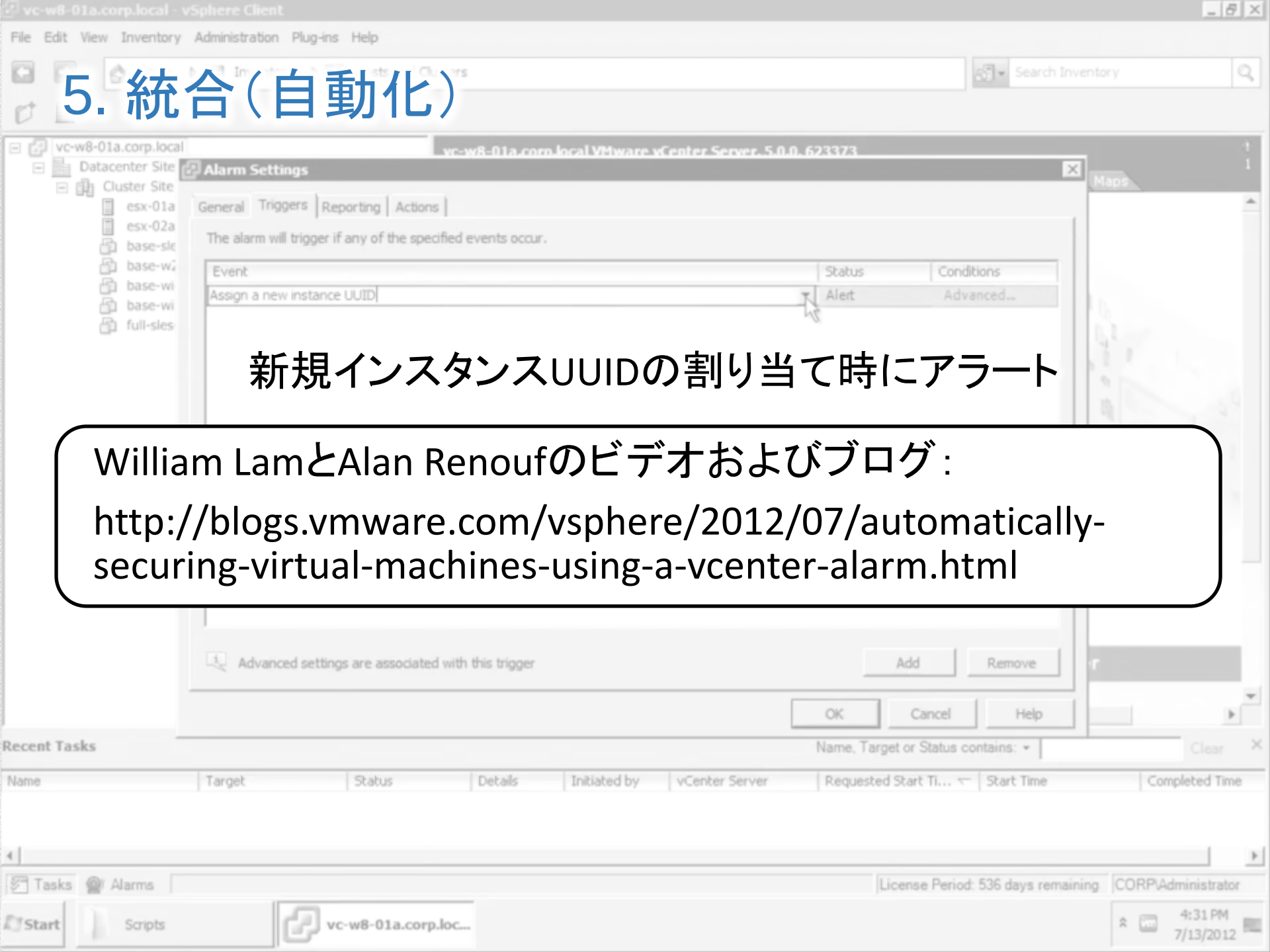


- 中断なし
- RTOがゼロ
- アイドル リソースなし

5. 統合（自動化）

- クラウドのセキュリティ保護は難しい場合がある
- 統合ツールを使用すると簡単になる
  - 統合には認証情報が必要
  - 複雑になり、攻撃面が増える
  - コストと人為的エラーを減らすか、増やすかのどちらか
- 共通インターフェイス
  - 強制チェック
  - 構成の確認
  - 自動化の強化

5. 統合（自動化）



新規インスタンスUUIDの割り当て時にアラート

William LamとAlan Renoufのビデオおよびブログ：

http://blogs.vmware.com/vsphere/2012/07/automatically-securing-virtual-machines-using-a-vcenter-alarm.html

5. 統合（自動化）

SSL証明書の取消し

Michael Websterのビデオおよびブログ：

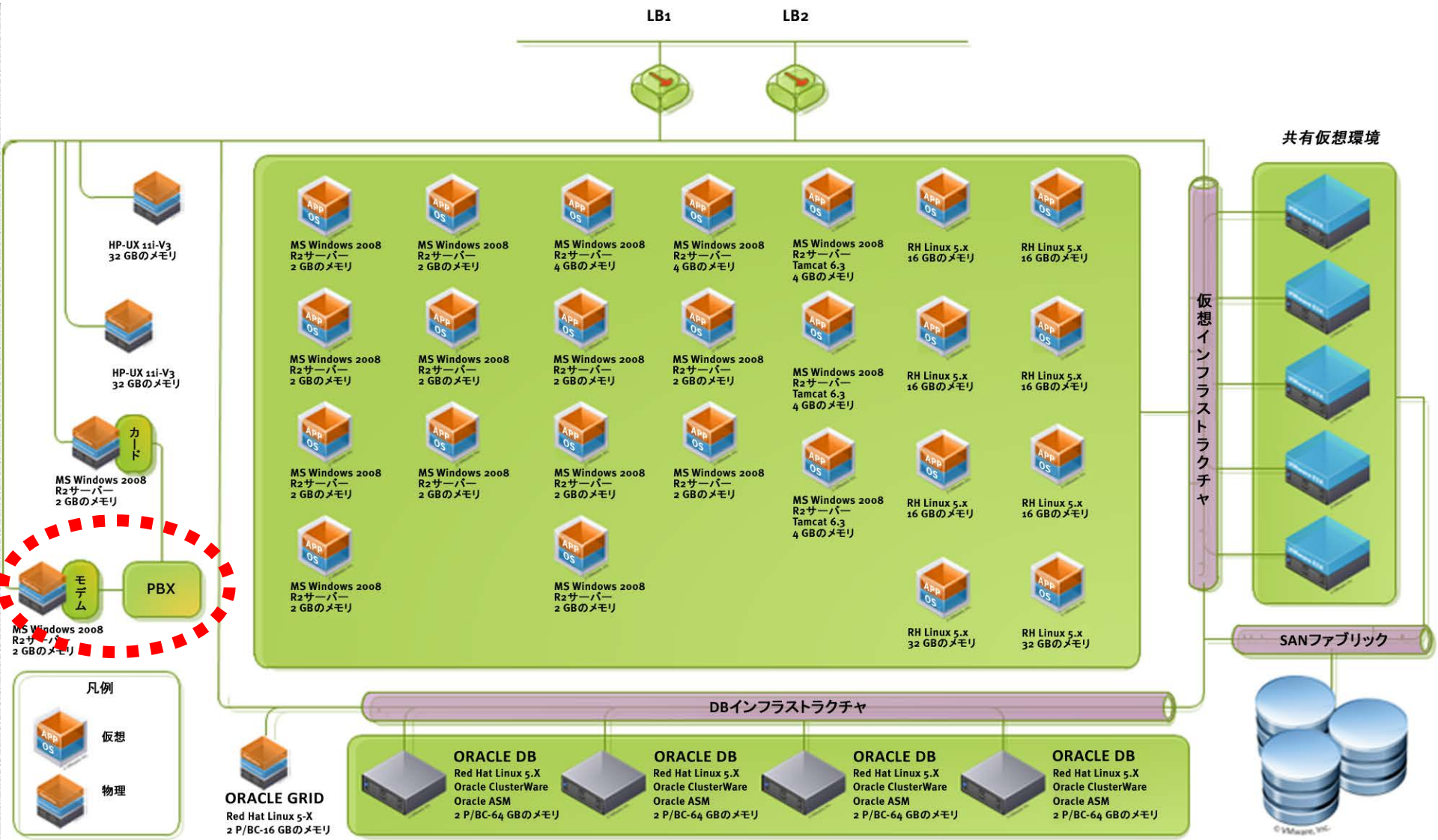
http://longwhiteclouds.com/2013/01/31/automating-vsphere-ssl-cert-management-vcert-manager-beta-demo/

6. セキュリティのテスト

- 脆弱性（Vulnerability）
  - アクセス権は持つ「べきではない」（例：CHAPシークレットが必要）
  - 自身をポート スキャンする
  - ギャップの検出とインベントリ

- 侵入透過性（Penetration）
  - Business-Logicの評価
  - 仮想化OPSEC（「テナント」をロードし、混合を試す）
    - 内部知識を活用
    - iSCSIターゲットまたはNFS共有をマウント
  - アプリケーション アーキテクチャ

6. セキュリティのテスト



6. セキュリティのテスト

- 仮想化OPSEC
  - .vxmf：チーミング構成（ワークステーション グループ）
  - .vmx：マシン構成
  - .vmsd：スナップショット ディスクリプター
  - .vmdk：ディスク ジオメトリ、レイアウト、構造
  - .vmem：バックアップ ページング ファイル
  - .vswp：スワップ ファイル
  - .vmss：中断状態
  - .vmsn：稼働中マシン状態のスナップショット
- 中断（物理ディスク上のメモリ）
  - .vmssが作成される
  - .vswpが削除される

6. セキュリティのテスト

- コラボレーション/変換
  - 認証情報
  - 刑務所釈放カード
- 報告を受けるか、盲目的でいるか
- 「止める」ことから始める
- アプリケーションにデータを*含める*
- エクスプロイト攻撃 = ？
  - **S** poof（なりすまし）
  - **T** amper（改ざん）
  - **R** epudiate（否認）
  - **I** nformation Disclose（情報開示）
  - **D** *eny Service*（*サービス拒否*）
  - **E** levate Privileges（権限の昇格）

…他のカスタマーと共有している可能性のあるリソースのパフォーマンス上の潜在的な悪影響を防ぐ

警告

セキュリティ評価を実施するためのツールやサービスの選択に制限はありません。
…任意の資産や自身の資産などに対してDoS（サービス拒否）攻撃やシミュレーションを行ったり、その他の方法でツールまたはサービスを使用することは禁止されます。

禁止されるアクティビティには次のようなものがありますが、これに限定されません。

- プロトコル フラッディング（例、SYNフラッディング、ICMPフラッディング、UDPフラッディング）
- リソース リクエスト フラッディング（例、HTTPリクエスト フラッディング、ログイン リクエスト フラッディング、APIリクエスト）フラッディング

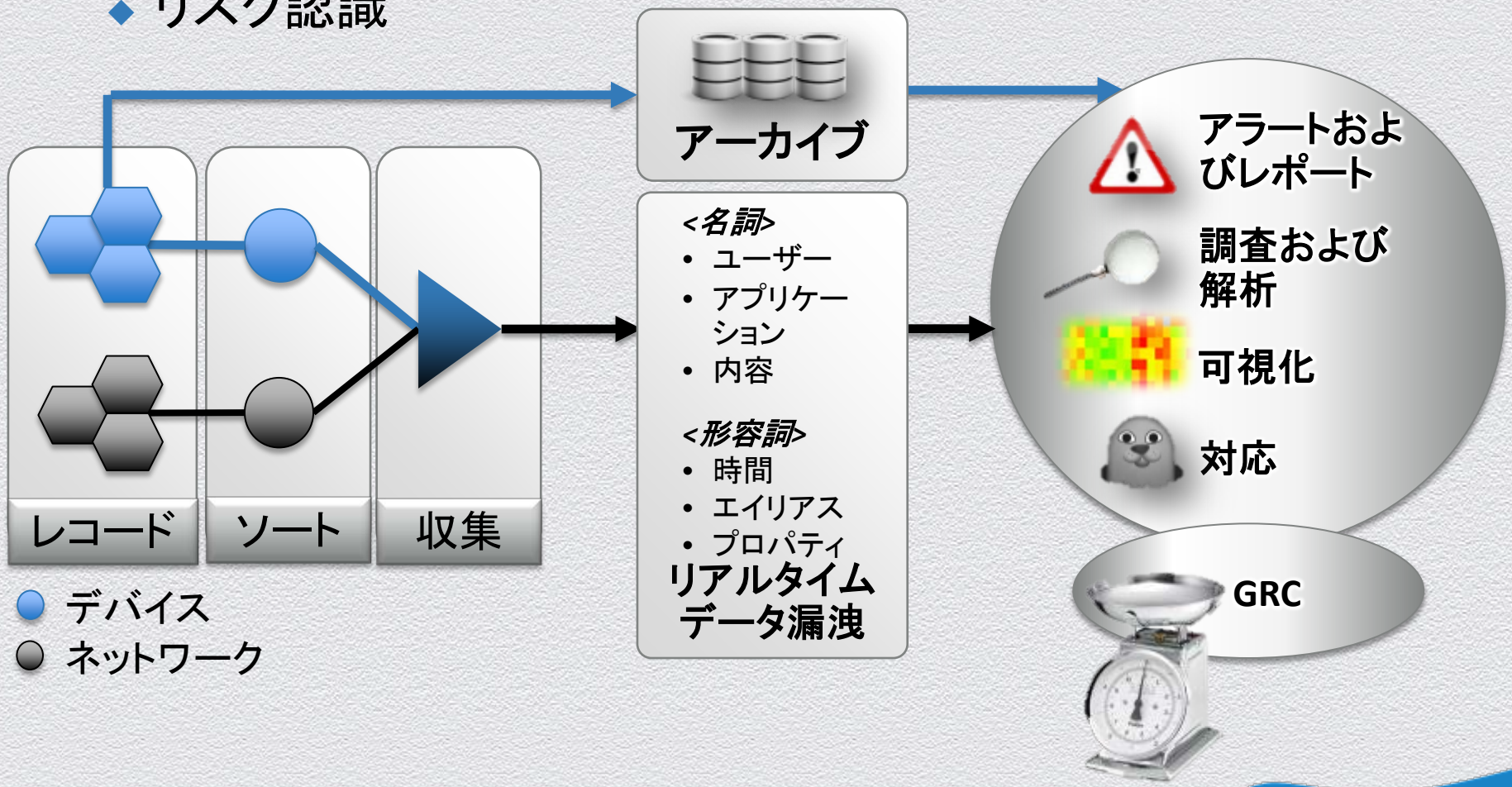
7. インシデントへの対応

- タイプI：アプリケーションまたはプラットフォーム対象
- タイプII：インフラストラクチャ対象
- タイプIII：不正なアプリケーション

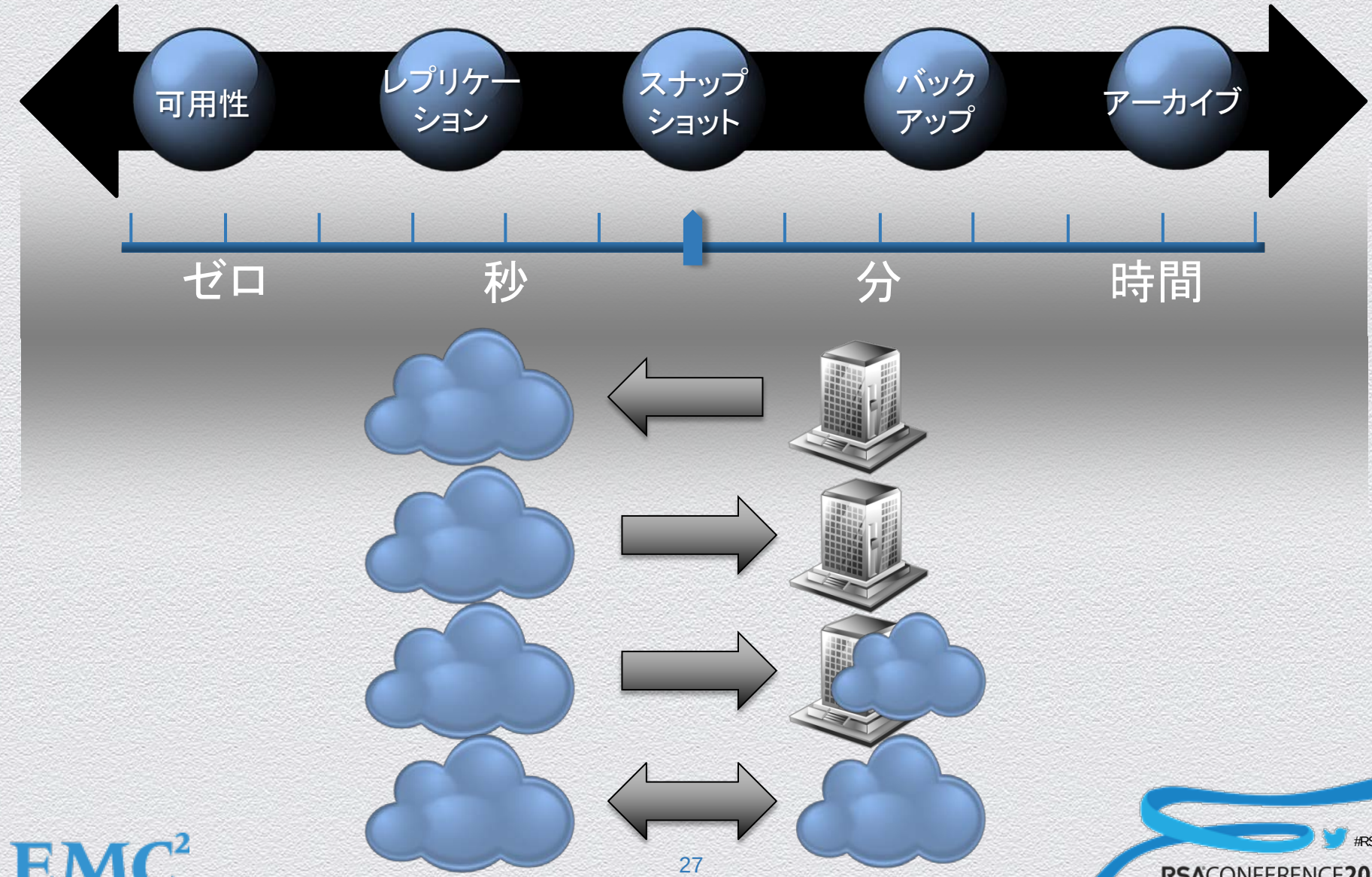
- 保護（SLA）
- 所有（場所、単一/多数、ハイブリッド クラウド?）
- 制御（実践アプリケーション、ネットワーク、システム…）

7. インシデントへの対応

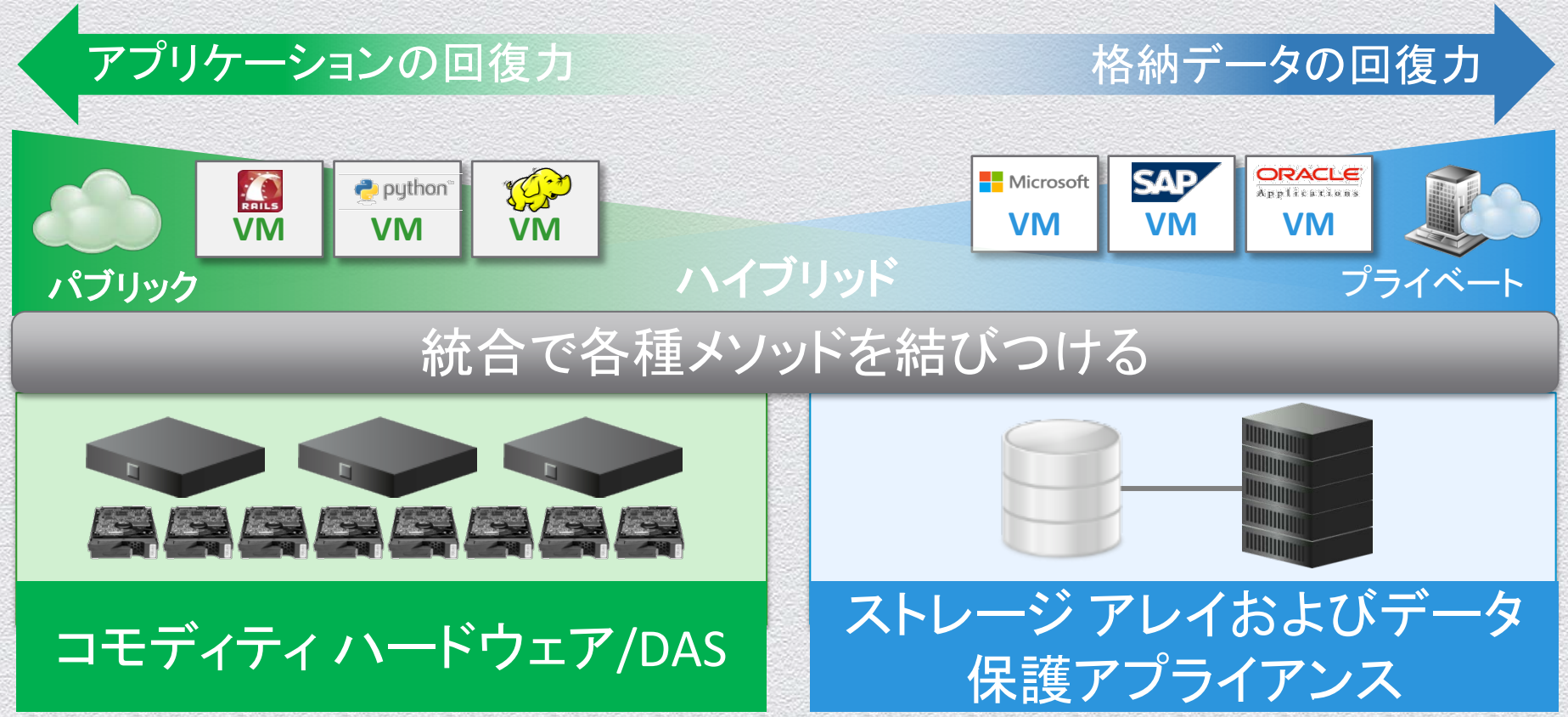
- インテリジェンス主導型
- リスク認識



8. バックアップとリストア



8. バックアップとリストア



不可欠なステップ

1. ターゲット領域の縮小
2. I&Mの管理
3. 監視とアラート
4. 可用性の管理

5. 統合（自動化）
6. セキュリティのテスト
7. インシデントへの対応
8. バックアップとリストア（終了）

クラウドトラスト 新定義

透過性

関連性

回復力

Thank You!

@daviottenheimer