

情報セキュリティ運用効率化のための VMware仮想基盤構築

背景

企業の情報セキュリティに関する意識は高まる一方です。中でも、さまざまな機密情報や個人情報を取り扱う放送業界では、2016年に外部からの攻撃による大規模な個人情報漏洩事件があったこともあり、今回のお客様も情報保護や事故防止の仕組み作りが大きな課題となっていました。

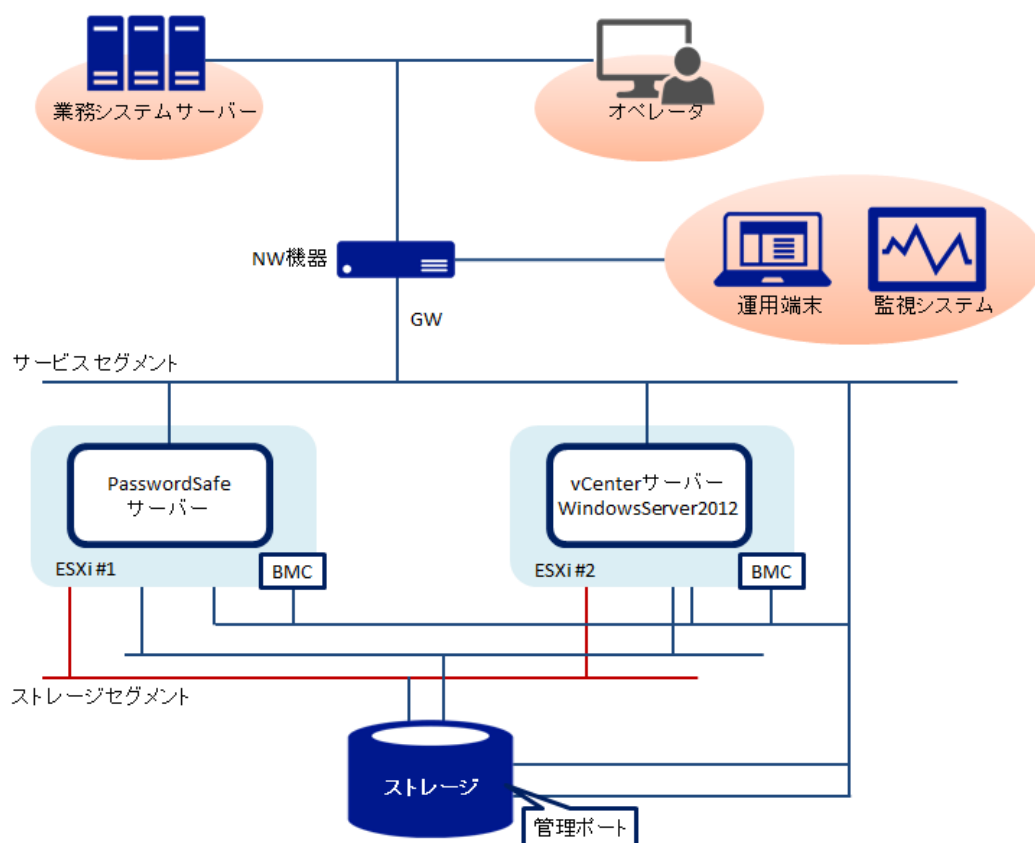
情報セキュリティは、外部からの脅威への対策はもちろん、社内の情報管理の強化が必須です。お客様の環境では、業務サーバへのログイン時に、特権ID及び一般IDを使用して個人の特定ができるログを残せていませんでした。事故や事件が発生した場合、まずログを解析することが基本ですが、情報にアクセスしたりシステムを操作した個人を特定できなければ、原因究明や対策を施すことはできません。また、現行システムの特権IDはパスワードを定期的に変更するシステムになっていませんでした。情報漏洩の事故や事件は、システムそのものよりも、人による操作や運用方法が原因となっている場合が多いと言われています。システムによるパスワードの定期的な変更は、単純なことに見えますが、人による管理のばらつきをなくし、事故の未然防止につながる重要な機能です。

IHSでは、特定アカウントのパスワード自動変更管理サービスを提供するため、Password Safe導入用の仮想基盤の構築させていただきました。また、運用効率を向上させるためにスクリプトを提供し、サービスの自動化を実装しております。

概要

業種	放送業
目的	特定アカウントのパスワード自動化変更管理導入のための仮想基盤の構築
作業規模	[開発環境 - 第一フェーズ] ・物理サーバ 2台 (VMware vSphere ESXi) ・仮想サーバ 2台 (VMware vCenter Server 兼 バックアップサーバ、Password Safeサーバ) ・L2スイッチ 2台 ・共有ストレージ 1台 [本番環境 - 第二フェーズ] ・物理サーバ 2台 (VMware vSphere ESXi) ・仮想サーバ 2台 (VMware vCenter Server 兼 バックアップサーバ、Password Safeサーバ) ・L2スイッチ 2台 ・共有ストレージ 1台
作業ボリューム	第一フェーズ／6人月 第二フェーズ／6人月
作業内容	要件定義/基本設計/詳細設計/インフラ構築/インフラテスト/ドキュメント作成

構成図



作業のポイント

vCenter Serverによる仮想基盤管理機能の冗長化

Password Safeサーバ導入に伴い、仮想基盤導入の管理ソフトウェアであるvCenter Serverの導入によりHAクラスタを組み込んだ構成となるため、vCenter Server自体にも高い冗長性が求められていました。本件では、ESXi2台を用いてアクティブ-アクティブ構成とし、Password SafeサーバとvCenterサーバを別ESXiサーバで稼働させたHAクラスタ上に配置することにより、サーバ障害が原因のダウンタイム軽減を目的とした構成にしました。また、物理サーバのNICに障害が発生した場合でも、残ったポートで通信が行えるように、2つのポートをグループ化するチームング構成にしました。

ARCserve D2Dによるサービス停止時間の短縮

バックアップを実施する際には、vCenterサービスを停止する必要があります。お客様は、バックアップ終了後のサーバ再起動・各種接続等を手動で実施されていたため、人手がかかる上に担当者による技術のばらつきがあり、障害対応に時間がかかり、vCenterサーバに接続不可能な時間がどうしても長くなっていました。そこで、ARCserve D2Dの、特定のコマンドを起動させる機能を用いて、スナップショット取得後にvCenterサービスを起動するバッチを起動させる環境を構築しました。これにより、vCenterのサービス停止期間を短縮し、全体的なダウンタイムを減少させることができました。

スクリプト作成によりPassword Safeの機能を補完

Password Safeには世代管理の機能がありません。Password Safeの標準機能でバックアップを取得すると、バックアップデータが溜まり続けてしまいます。そこで、IHSがスクリプトを作成し、Password Safeバックアップファイルの世代管理を実現、世代管理の自動化をおこない、お客様の運用工数削減に貢献することができました。

作業内容の詳細

要件定義・設計

1. 要件定義

- プロジェクト要件定義
- 機能要件の定義
- 非機能要件の定義

2. 基本設計

- ネットワーク設計
- サーバ設計
- ストレージ設計
- 仮想基盤設計
- インフラ設計
- 信頼性設計
- 運用設計
- バックアップ設計

環境構築

1. 仮想基盤構築

- VMware ESXi 5.5
- VMware HA (High Availability)

2. 仮想基盤管理機能

- vCenter Server 5.5

3. システムバックアップ機能

- CA ARCserve D2D r16.5 for Windows
- 世代管理バッチ作成

4. ストレージ機能

- NEC iStorage M10

5. ネットワーク機能

- DGS-1100-16

納品ドキュメント

- 要件定義書
- 基本設計書
- 詳細設計書
- 動作確認項目表兼結果報告書
- 運用手順書

弊社利用による効果

自動化のノウハウを活かした運用の効率化

IHSには、VBS、bat、PowerShellといったスクリプトをカスタマイズすることによってパッケージによる自動化の効率をさらに向上させるノウハウがあります。

本件でも、

- ・Password Safeバックアップファイルを世代管理するスクリプト
- ・ARCServeD2Dが内包するSQL Serverのバックアップスクリプト

等を作成し、パッケージ製品の標準機能では解決できない機能を提供することによって、お客様のご要望にお応えしました。優れたセキュリティ製品は多数ありますが、お客様の環境や体制にあわせた無理のない運用をおこなわなければ、その効果を最大限に引き出すことができません。情報セキュリティの運用は24時間365日続く業務です。運用を効率化することは、それにかかるコストを削減するだけでなく、セキュリティを強化することにつながるため、地味ながら重要な取り組みです。

IHSには、本件以外にも、System Center Configuration Managerの運用で、PowerShellを使用し自動化をおこなった実績があり、お客様からは、カスタマイズによる運用品質の向上、ならびに運用工数削減が実現できたことをご評価いただいております。

仮想化の強みをプラスαでご提案

当初お客様のご要望では、仮想アプライアンスの実行のための仮想化環境が必要ということでした。これのみを要件とし提案することは、比較的容易におこなうことができます。しかし、それだけでは仮想化の持つさまざまなメリット（クラスタリングやネットワーク高可用性等）が考慮されていません。IHSでは常にお客様のご要望に沿ったものからさらに「プラスα」でご提供可能なサービスや機能をご提案させていただきます。

ハードウェア構成のご提案

IHSでは、サーバの構成だけではなく、ストレージまたはネットワーク機器構成のご提案もおこなっております。今回は、信頼性のため、サービス継続に重点を置いた単一障害点を排除する構成をご提案することを心がけ、ネットワーク機器の多重構成に加えて、データの安全性を確保する設定をさせていただきました。