

# System Centerのコレクション適正化

## 背景

2017 年に起きたランサムウェア攻撃によって、Microsoft の古いファイル共有プロトコルの脆弱性が露呈しました。

Microsoft はこの脆弱性を確認し、セキュリティパッチをリリースしましたが、非常に多くの企業がランサムウェアの被害を受けました。これは、Microsoft のパッチサイクルを意図的に遅らせていたか、システムへのパッチ適用頻度が低かったことに原因があります。

セキュリティパッチの適用にあたっては、クライアント端末や企業の重要なシステムを考慮し、信頼性の高い方法で適用後の影響を検証する必要があります。また、セキュリティパッチの配信においても、配信対象を正確に把握すること、ネットワーク負荷を考慮した配信計画を検討することが大切です。

当該事例のお客様は、Microsoft の System Center Configuration Manager のコレクションを使用することで、クライアント、およびその他のリソースをグループ化し、そのコレクションに対してセキュリティパッチを適用しようと検討しておりました。しかし、コレクションのメンテナンス不足により配信対象を正確にグループ化することができなかったため、セキュリティパッチの配信が正常に行えない状態であることがわかり、弊社にて今後の運用も考慮した改善のご支援をさせていただきました。

## 概要

業種	サービス業
目的	セキュリティパッチ配信の適正化
作業規模	<ul style="list-style-type: none"><li>利用ユーザー数: 約 3,000 名</li><li>総クライアント台数: 約 4,000 台</li></ul>
作業ボリューム	1 人月
作業内容	<ul style="list-style-type: none"><li>現配信コレクション(グループ)内容の調査</li><li>管理端末の調査</li><li>全国各地の拠点情報調査</li><li>ネットワーク帯域の調査</li><li>配信計画</li><li>配信</li></ul>

## 作業効果

### セキュリティパッチ配信

#### <課題>

コレクションのメンテナンス不足により、配信対象となるリソースのグループ化ができない状況であった。

#### <改善内容>

- 現在の配信コレクション(グループ)内容の確認
- 全拠点の情報および配信対象となる全リソースの調査
- 配信コレクション(グループ)の作成(配布ポイントを考慮)

#### <効果>

- 再作成したコレクションを用い、これまで配信できていなかった端末へのセキュリティパッチ適用が完了した。

### ネットワーク不可分散

#### <課題>

セキュリティパッチにはファイルサイズが大きいものもあり、また配信対象となるリソースも多いことから、業務に支障をきたすことがないようにネットワーク負荷を考慮しなければならなかった。

#### <作業内容>

- 各拠点への配信スケジュール見直し
- 配布ポイントの設置箇所や、端末の設置台数を考慮し、配信スケジュールの見直し

#### <効果>

ネットワーク負荷を考慮したセキュリティパッチの配信が行えた。

### 継続的な配信コレクションの適正化

#### <課題>

今後も配信対象となる拠点やリソースが増加した際においても、今回のように正確に配信できるようコレクションのメンテナンス方法をどのようにすべきか検討する必要がある。

#### <作業内容>

- System Center のレポート機能やコレクション情報より、コレクションに含まれない端末のリストアップと調査を月次にて実施する態勢作り。

#### <効果>

月次のフローに組み込むことにより常に最新の状態へメンテナンスされていることを確認できた。

## 弊社利用による効果

当該お客様へは弊社にて運用・保守のご支援をさせていただいております。

### 管理ドキュメントの作成

これまでの運用ではネットワーク構成や管理対象端末等がわかるドキュメントが存在していなかった。そのため、新たにドキュメントを作成し、月次にて更新する運用へと態勢を強化したことにより、管理対象等の最新情報がいつでもすぐにわかるようになった。

### 継続的なコレクション見直し

- 上記の通り、新たに増えた拠点、配信端末がわかる仕組みを構築したため、常に配信対象へセキュリティパッチの配信が行えるようになった。
- 管理端末が増えた際、コレクションの所属する端末数、それに紐づく配信ポイント(配信データー時保管ポイント)を考慮し、配信時間をずらす、コレクションを分ける等を行うことで、ネットワーク負荷を考慮した配信を実現することができた。

## 作業内容の詳細

### 設計

#### 1. 設計

- 既存コレクション状態の調査
- 配布対象端末の設置個所の調査
- 新コレクション用、クエリの作成
- 新コレクション作成
- 各拠点への配信スケジュール作成
- 配信