



NetStare®

ネットワーク・セキュリティ運用監視

## 紹介資料





# NetStare(セキュリティ/システム運用監視サービス)とは

NetStareでは、3つのサービスコンポーネントを組み合わせて、お客様のシステム仕様に合わせたベストな運用監視サービスを24時間365日ご提供します。

- インフラマネージドサービス** : 全てのシステム構成機器を対象とした統合的なサービス
- セキュリティマネージドサービス** : セキュリティ機器を中心とした標準化された運用サービス
- カスタムマネージドサービス** : 運用設計に基づくお客様独自アプリの運用サービス

## 2 標準対応アプリケーション

セキュリティ機器を中心としたアプリケーションは当社で標準化された運用サービスを提供

ファイア  
ウォール

IDS  
IPS

コンテンツ  
セキュリティ

ロード  
バランサ

L2/L3  
スイッチ

## 3 運用設計

ユーザアプリケーションや標準対応していないアプリケーションは運用設計に基づき対応

ユーザ  
アプリA

ユーザ  
アプリB

ユーザ  
アプリC

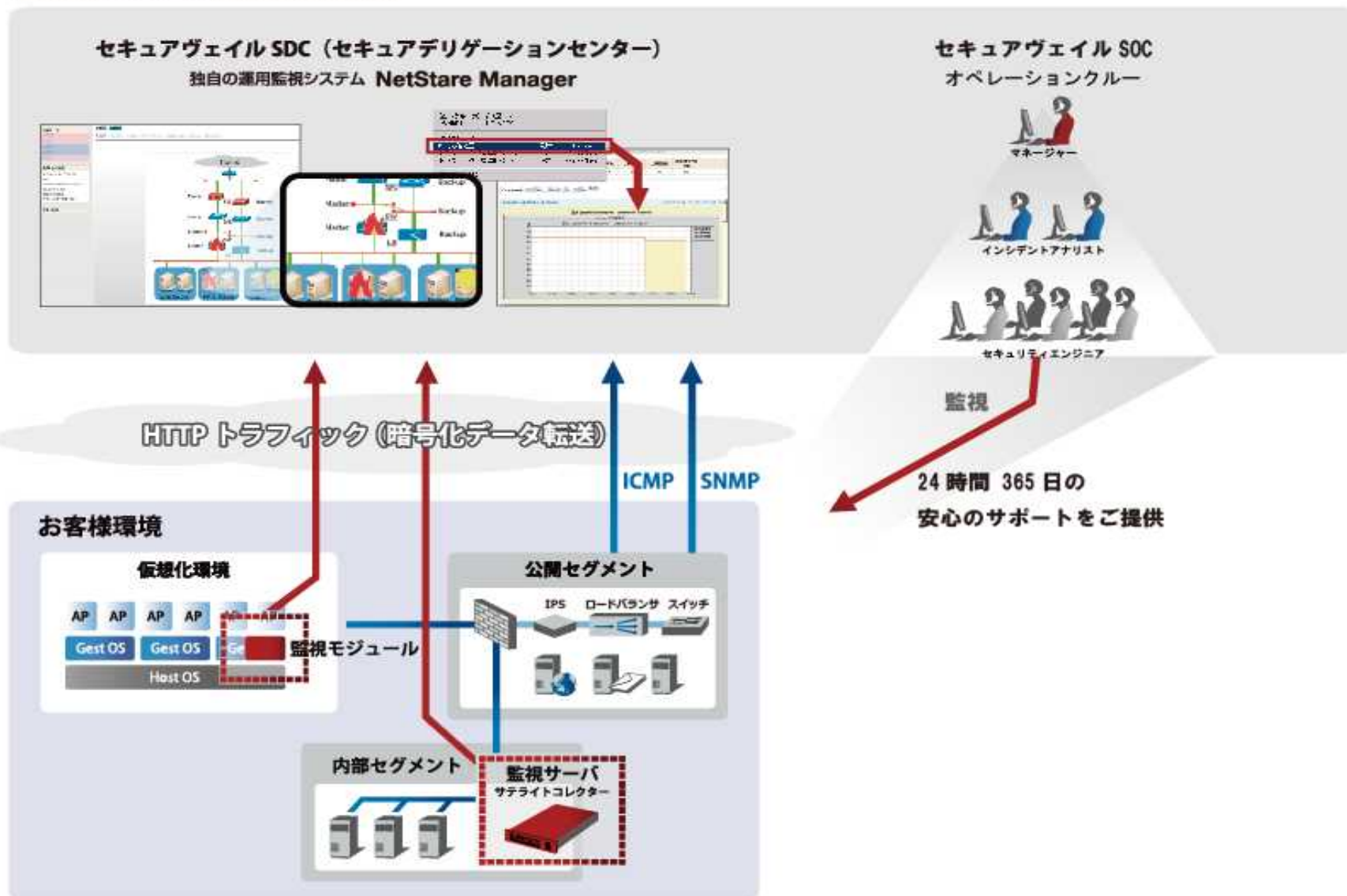
## 1 インフラ監視サービス

対象機器のインフラレベル（稼動状況やリソース使用状況等）監視は標準プラグインで実装



# NetStareサービスの適用構成例

## NetStare サービスの適用構成例





# NetStareサービスの特性

NetStareサービスでは、弊社のSecurity Operation Center(SOC)が、お客様のシステムをリモートでサポートいたします。近年、ますます複雑化が進む情報システムに対し、SOCでは独自のシステムと専門のエンジニアから、柔軟で高品質なサポートサービスを提供しています。

品質と効率を高めた独自開発の**運用監視システム「NetStare Manager」**  
インシデントアナリストを中心とした24時間365日**オペレーションクルー**





## 運用監視システム NetStare Manager



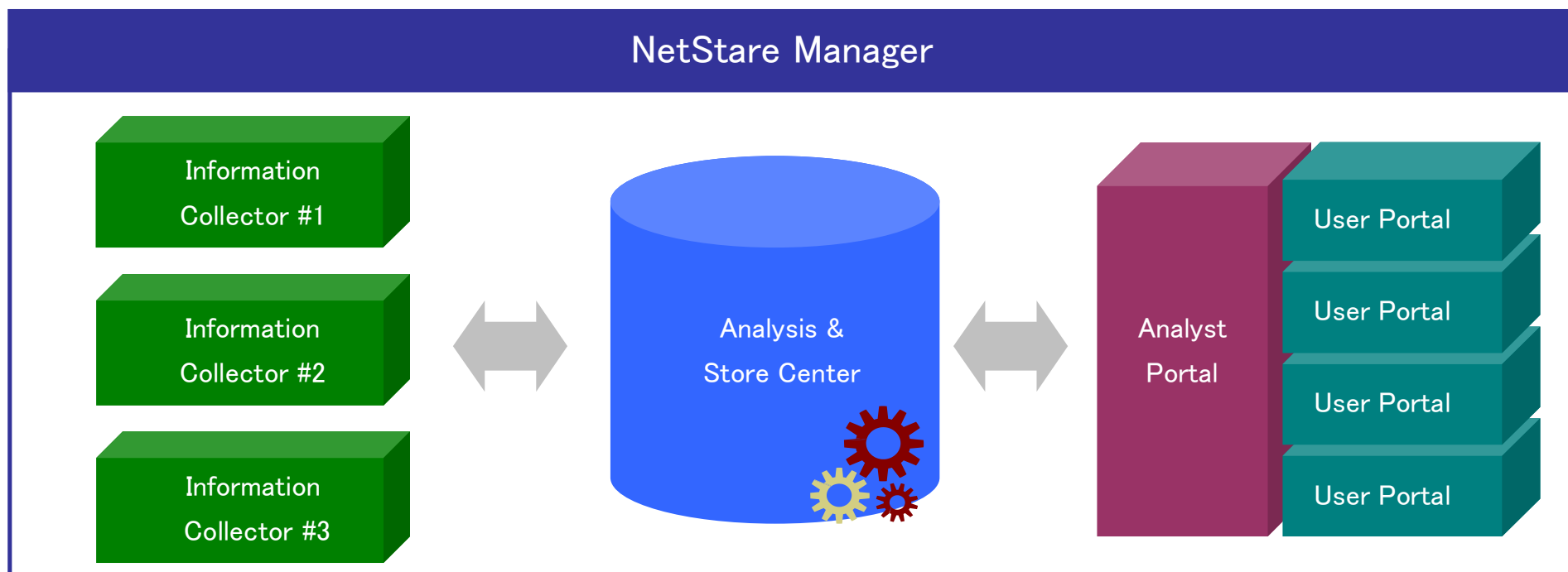


NetStareManagerでは、3つのサービスモジュールが連携し、対象システムの稼働状態をダイナミックに監視&レポートする総合運用監視システムです。

Information Collector : サービス対象機器をリアルタイムに監視するモジュール

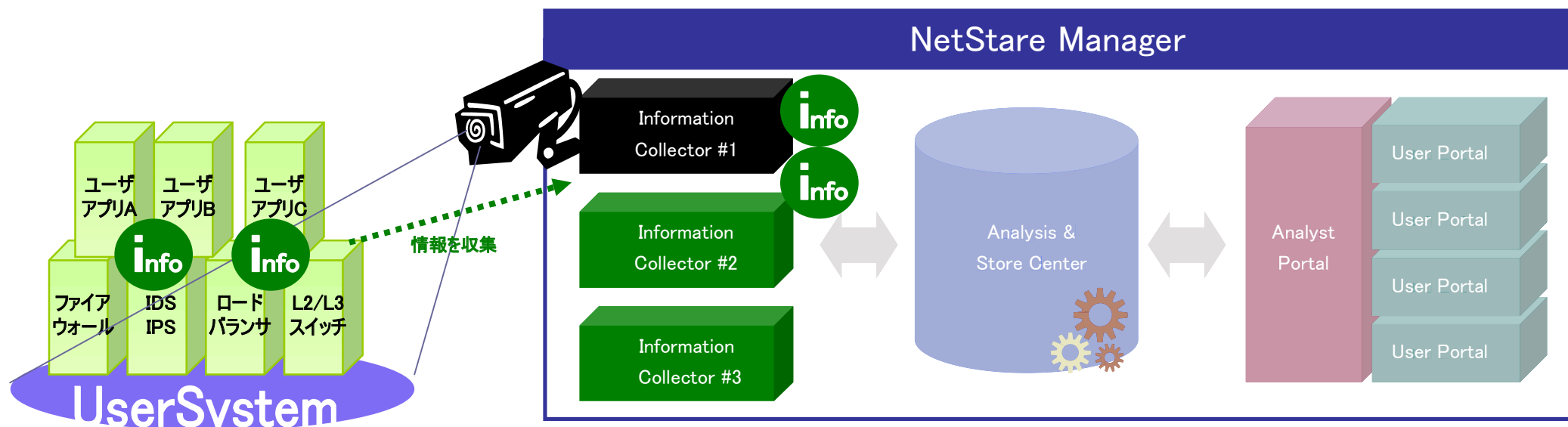
Analysis & Store Center: Information Collectorで取得した値とカスタマ情報を対照し、優先すべきタスクを分析するモジュール

Analyst Portal : Information Collectorで取得した値をダイナミックにレポートするモジュール





# NetStare Managerの概要 (Information Collector)

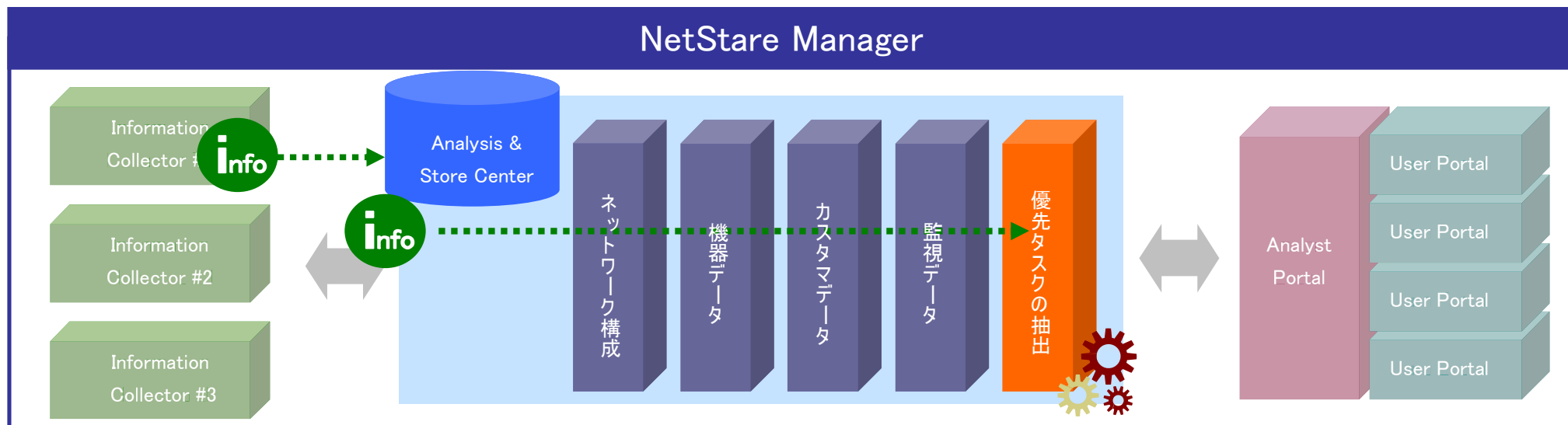


## Information Collectorの特徴

- ・インフラレベルの監視テンプレートを標準装備
- ・定常的に分析を必要とするポイントには、Information Collectorが能動的に情報を収集
- ・突発的に発生するアノマリイベントには、検知用のインターフェースを搭載
- ・アプリケーションレベルの監視には、キーワード分析機能と個別スクリプトで対応
- ・静的または動的な閾値設定から、障害の未然予防を実現
- ・1台のInformation Collectorで、数万ポイントの情報収集が可能

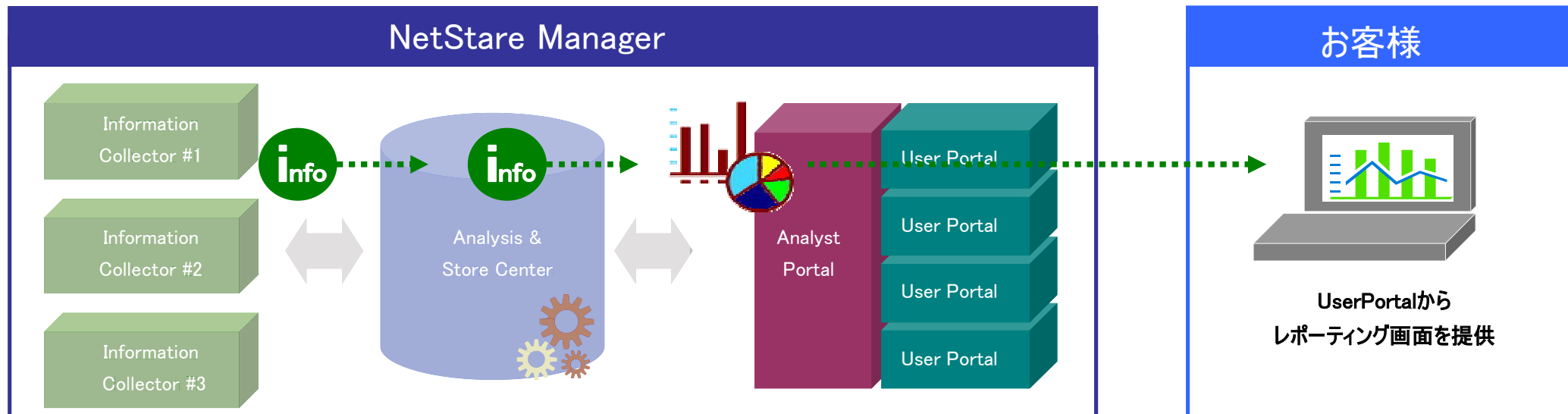


# NetStare Managerの概要( Analysis & Store Center)



## Analysis & Store Centerの特徴

- ・カスタマ情報の管理テンプレートを標準装備
- ・機器単位の監視ポリシー(閾値など)を柔軟に定義可能
- ・お客様と弊社間のISP情報を含むネットワークポロジを定期的に収集管理
- ・Information Collectorが収集した情報を分析し、インシデントを自動判別
- ・抽出された優先タスクは、分析結果を可視化して「人」へ配信
- ・監視データとインシデント分析結果(障害履歴)を、データベースに自動保存



## Analyst Portalの特徴(弊社オペレーションクルー向け)

- ・全ての監視対象機器を一括表示
- ・Analysis & Store Centerへの管理用インターフェースを提供
- ・障害に対し、様々な単位で(お客様、機種、障害特性)ナレッジ検索

## User Portalの特徴(お客様向け)

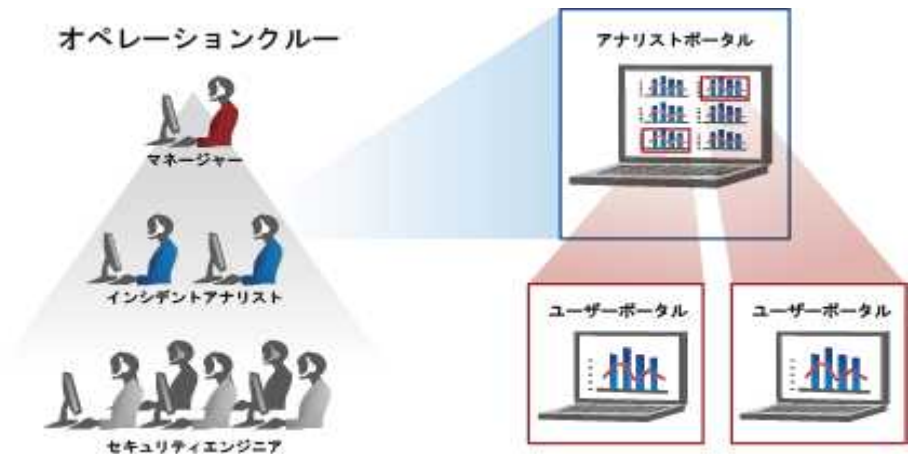
- ・トポロジ情報から、ダイナミックにステータスを閲覧
- ・日次、週次、月次の詳細なレポート画面
- ・ワンクリックで監視レポートをpdf形式でダウンロード



# ユーザポータル構成

お客様にご提供するNetStare ManagerのWebポータルは、弊社オペレーションクルーとの共通言語として利用します。

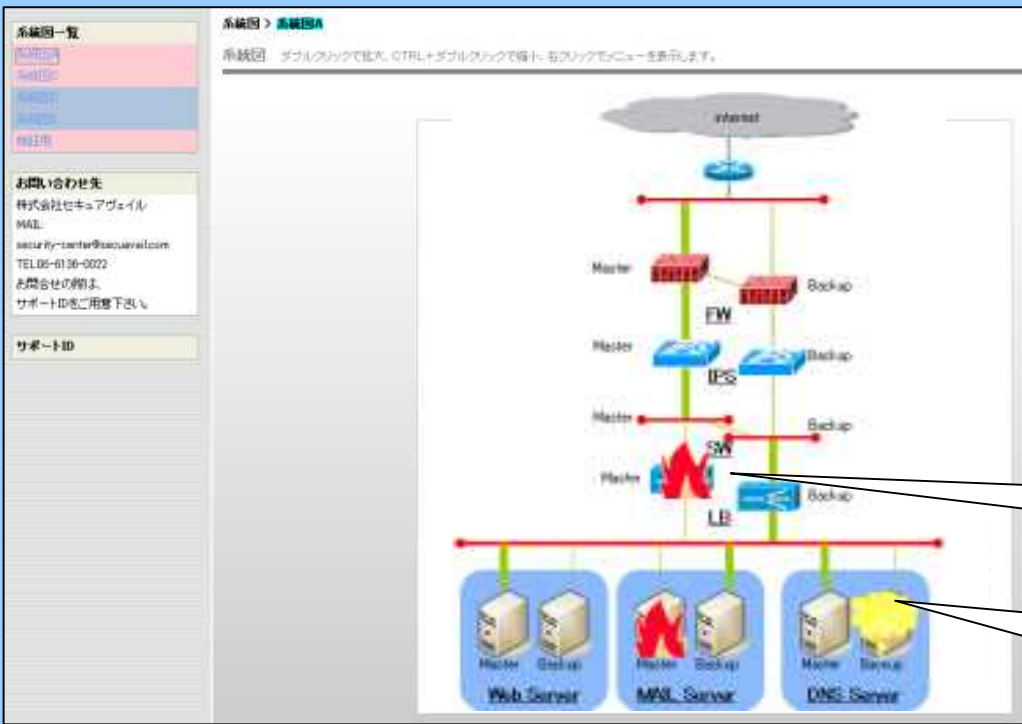
Webポータルでは、お客様が一目でシステムの状態を把握できるように、稼働状態をビジュアル的に表現し、画面遷移は概要から詳細へと障害箇所をクローズアップできるよう設計しています。



DSV (Dynamic Status Viewer)とは、サービス対象のシステムと監視情報をリアルタイムに表現した系統図です。DSVには、大きく3つの機能があります。

- ハザード機能 : 全体俯瞰と障害ポイントの明確化
- ドリルダウン機能 : 障害事象のドリルダウン調査
- トラフィックリンク機能 : 障害による影響範囲の特定

ハザード機能
ドリルダウン機能
トラフィックリンク機能



< 全体俯瞰と障害ポイントの明確化 >

DSVでは、監視対象のシステム構成をWeb上に表現し、障害の発生状態(注意/警告)にある機器にハザードマークを表示します。これにより、全体の構成を把握しつつ、個々の障害ポイントを一目で把握することができます。

【炎マーク】  
3回応答ナシまたは警告閾値のオーバー

【煙マーク】  
1回応答ナシまたは注意閾値のオーバー

ハザード機能

ドリルダウン機能

トラフィックリンク機能

PC3

[基本グループ] 系統図Grp  
[機器名] 山田太郎PC

[監視項目一覧] クリック

Ping応答確認	<b>異常</b>	0.20msec
トラフィック (標準MIB) (in)	正常	462,778bps
トラフィック (標準MIB) (out)	正常	475,484bps

縮小(現在80%)

< 障害事象のドリルダウン調査 >

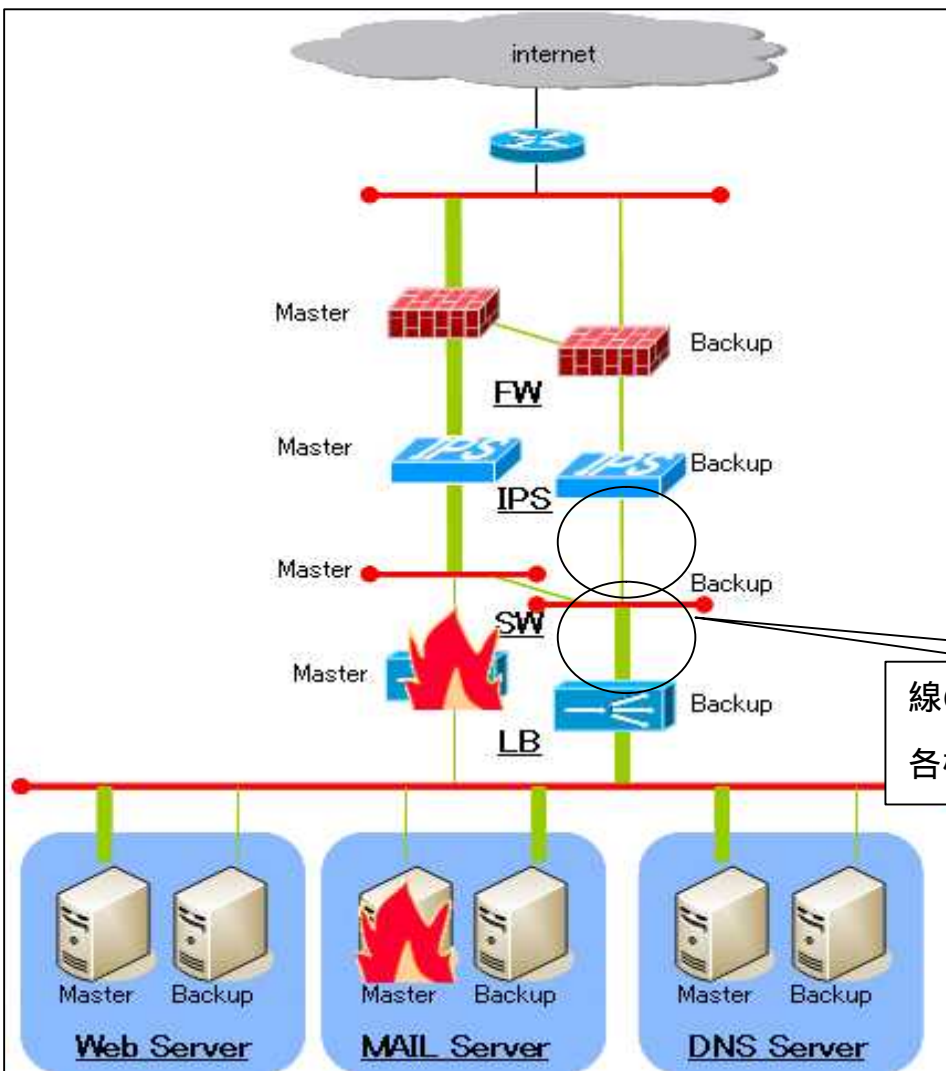
ハザード機能で、「炎」マークが点灯した障害発生機器は、より詳細な障害の箇所をドリルダウン機能から特定することができます。  
これにより、一連の障害調査プロセスをシームレスに実現することができます。



ハザード機能

ドリルダウン機能

トラフィックリンク機能



< 障害による影響範囲の特定 >

DSVにおける配線オブジェクトは、単に機器同士の接続を示しているだけではありません。  
線の太さは流通するトラフィック量に応じてダイナミックに変化します。  
機器の障害がシステム全体のトラフィックにどのような影響を及ぼすのか、または、トラフィックの迂回経路の状態が一目で判断できます。

線の太さの違いに注目

各機器を結ぶラインは、3段階の太さで表現



## Layer1 モニタリング状況一覧



「モニタリング状況一覧」では、サービス対象となる機器ごとに監視項目を一覧で表示します。

障害が発生している場合は、監視項目をステータスに応じて「赤(警告)」または「黄色(注意)」で表示します。

## Layer2 監視項目別状態表示



DSV、またはモニタリング状況一覧から、ドリルダウンによって、詳細な状態表示画面へ移ります。

障害が発生時には、リアルタイムのデータと、過去データを突き合わせることで、状態推移や値比較などのチェックを行なうことが可能です。

## Layer3 監視項目別レポートिंग



監視項目ごとに、基点日を指定した日次、週次、月次レポートをPDFまたはCSVでダウンロードすることが可能です。

バージョンや機種に依存せず、全ての機器を同一フォーマットのレポートとして管理することが可能です。



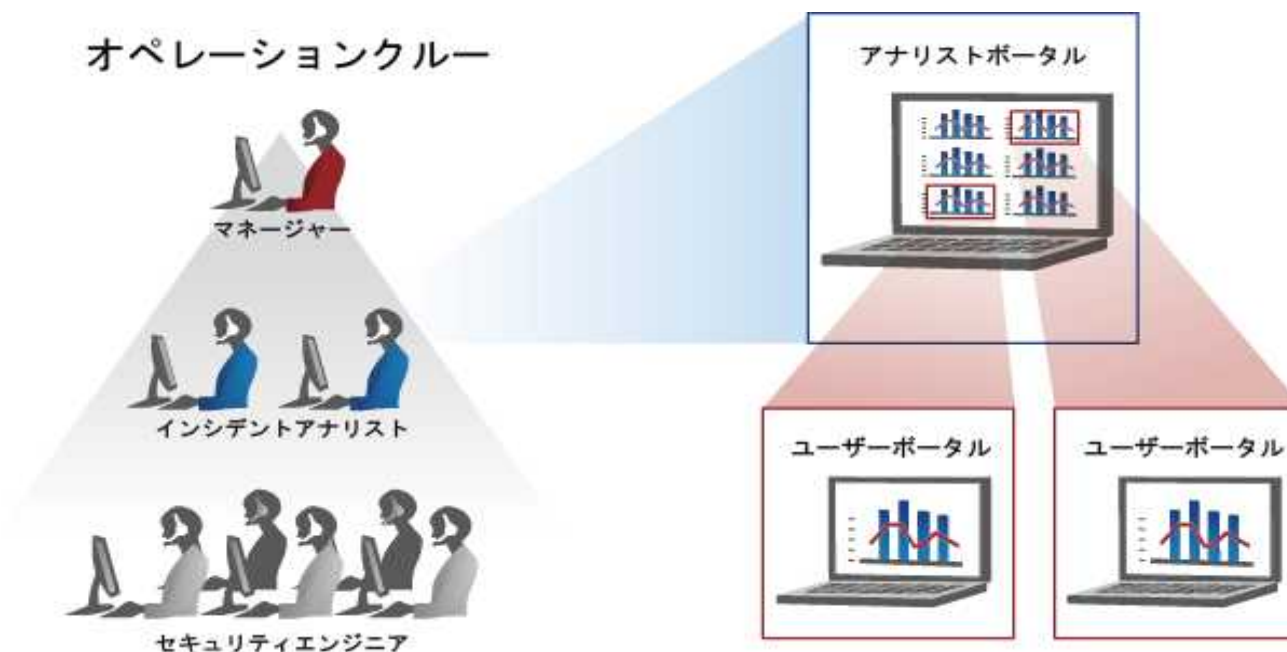
## 運用監視体制 オペレーションクルー





# オペレーションクルーとアナリストポータル

オペレーションクルーは、当社の正社員のみで24時間のサービス実施体制を築いています。  
経験とスキルに応じて3つの役割を設け、重要なインシデントには専門のアナリストが対応いたします。  
オペレーションクルーが使用する「アナリストポータル」は、ユーザ向けポータルと同じインターフェースをもちつつ、複数の顧客を同時にコントロールできるよう設計されています。





# オペレーションセンターの物理環境

当社のSOCは、最新の通信技術や建築技術を終結して建設したコンピュータビルに入居しており、「自家発電、耐震、漏水防止、防火性能」を強化した万全の物理的セキュリティ対策が施されています。また、最新の入退管理システムでは不正侵入者を許しません。NetStareサービス用機材は、ISP回線を含むすべてを二重化し、サービス停止の排除に努めています。



最新鋭のコンピュータビル



自家発電装置



厳重な入退管理システム

- A. ビル専用 ICカード ( 写真)
- B. 当社専用 ICカード + 暗証番号
- C. オペレータ専用ICカード
- D. オペレータ専用ICカード(システム)

