Orchestrating a brighter world NEC

WebSAM Network Flow Analyzer 3.3
WebSAM NetvisorPro V 9.6
強化内容のご紹介

2024年10月

日本電気株式会社

はじめに

- 本書では以下の略称を使用します。
  - NVP･･･WebSAM NetvisorPro V
  - NFA･･･WebSAM Network Flow Analyzer
  - IMS･･･WebSAM Integrated Management Server

強化内容

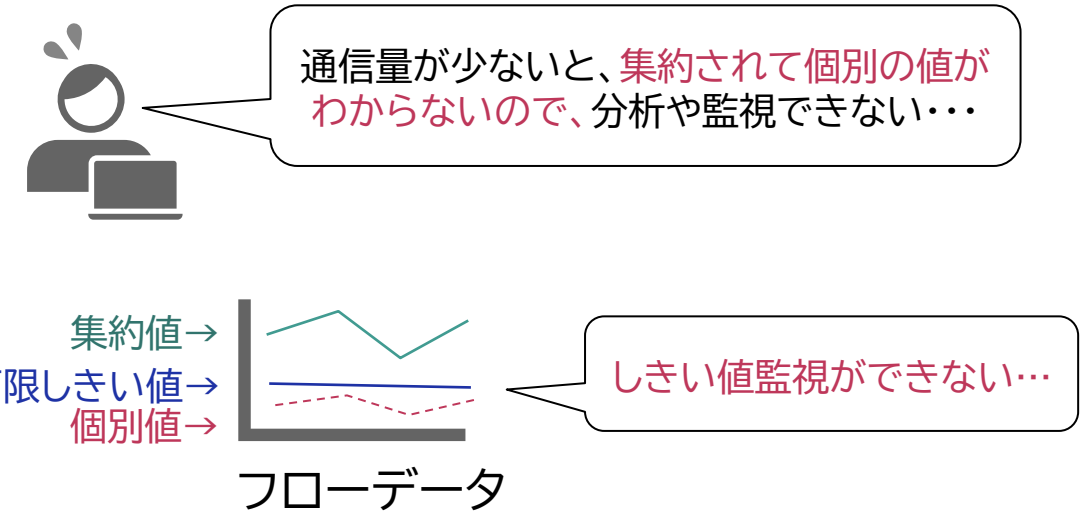
- 少量フローの分析(NFA)
- ホスト名でのフローの検索(NFA)
- セキュリティ監視機能の監視上限数の拡張(NFA)
- MIBファイルの組み込みなしでのMIB監視サポート(NVP)
- ネットワークインターフェイスの詳細情報を表示する機能を追加(NVP)
- ネットワークインターフェイスの管理機能の強化(IMS)
- WebAPIの強化(NVP)
- WebAPIの強化(IMS)

少量フローの分析(NFA)

通信量の少ないフローでも監視・分析が可能になりました。また、しきい値を下回ったことを検知する判定条件を指定できるようになりました。

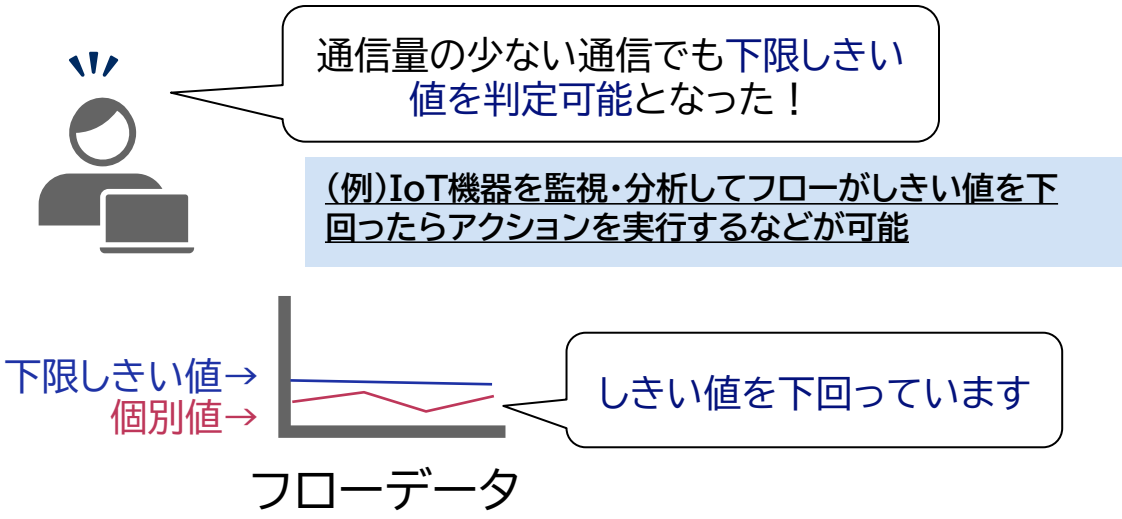
◆ Before

- 通信量の少ないフローデータは、フローデータの丸め処理により1つに集約して保存するので、分析画面で分析することや、しきい値監視によって監視することができませんでした。



◆ After

- 少量フローとして分析するアプリケーションを定義することで、通信量の少ないフローでも分析できるようになりました。
- しきい値監視機能で、しきい値を下回ったことを検知する判定条件を指定できるようになりました。

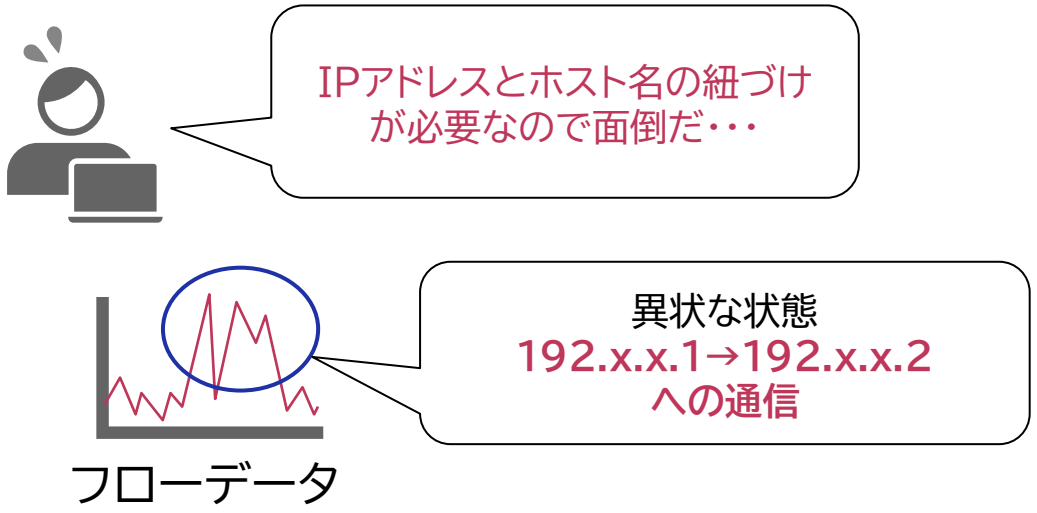


ホスト名でのフローの検索(NFA)

ホスト名によるフローの検索機能を追加。本機能により、セキュリティインシデントの早期発見やボトルネック箇所の特定がより簡単になりました。

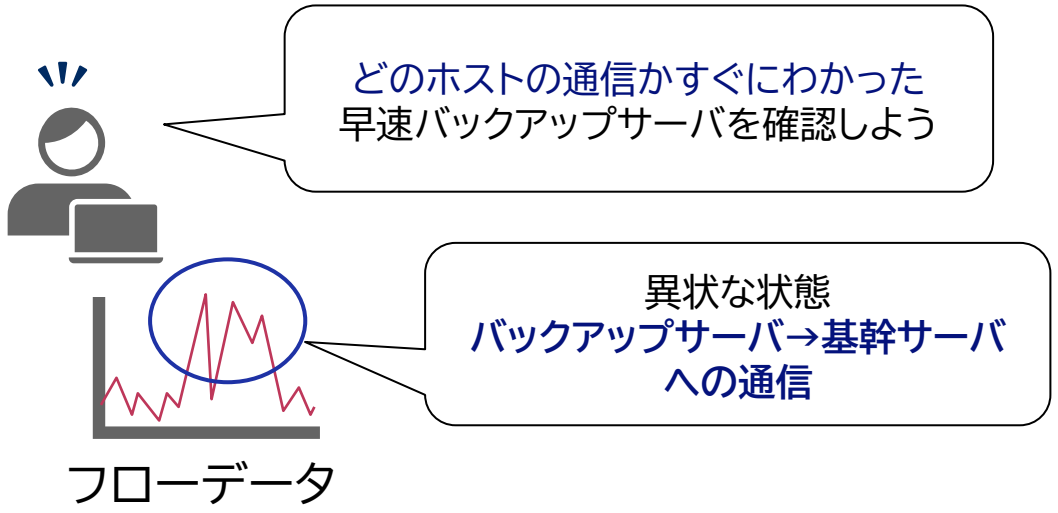
◆ Before

- 異常な箇所をIPアドレスで絞り込むことが可能でしたが、ホスト名で絞り込むことができませんでした。



◆ After

- エクスポーター分析画面のフィルター条件において、送信元ホスト名と宛先ホスト名を指定できるようになりました。
- しきい値監視機能のフロー条件において、送信元ホスト名と宛先ホスト名を指定できるようになりました。



セキュリティ監視機能の監視上限数の拡張（NFA）

Security Monitoring ライセンスを追加しました。これらのライセンスを登録により、従来の5監視を超えるセキュリティ監視設定が実施可能となりました。

◆ 追加されたライセンスは以下の通りです。

ライセンス名
①WebSAM Network Flow Analyzer 3.3 Security Monitoring（25 監視ライセンス版）
②WebSAM Network Flow Analyzer 3.3 Security Monitoring（50 監視ライセンス版）
③WebSAM Network Flow Analyzer 3.3 Security Monitoring アップグレードライセンス（5 to25 監視ライセンス）
④WebSAM Network Flow Analyzer 3.3 Security Monitoring アップグレードライセンス（25 to50 監視ライセンス版）

（注1）監視対象を増やす場合は必ず「アップグレードライセンス」をご購入ください、「WebSAM Network Flow Analyzer Security Monitoring」ライセンスを複数購入しても監視対象数は増えません、例えば上記①を2つ購入しても50監視にはなりません

（注2）「アップグレードライセンス」は、25もしくは50にアップグレードする、というライセンスであり、25もしくは50を追加する、ということではないのでご注意ください。例えば、「5to25監視ライセンス」を適用する場合、5に25を追加して30ライセンスにはなりせん

MIBファイルの組み込みなしでのMIB監視サポート(NVP)

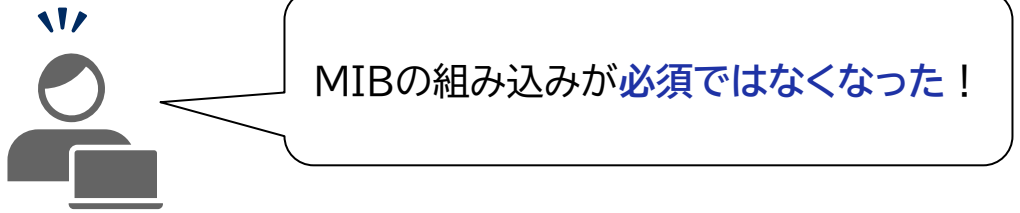
OIDを直接入力することで意図した監視ができるようになり、MIBの組み込みが必須ではなくなりました。

◆ Before

- MIBファイルが組み込まれていない場合、オブジェクト値を正しく判別できず意図した監視が行えない場合があった。
- MIBの設定処理(SNMP Set 処理)では、MIB ファイルから型情報を取得する仕様であり、MIBファイルが組み込まれていない場合、設定処理が行えなかった。

◆ After

- MIBファイルが組み込まれていなくてもNetvisorProがオブジェクト値を正しく判別できるようになった。
- MIBの設定処理(SNMP Set 処理)において、MIBファイルからの型情報取得だけでなく、コマンド引数として型情報(OID)を指定することができるようになり監視可能となった。



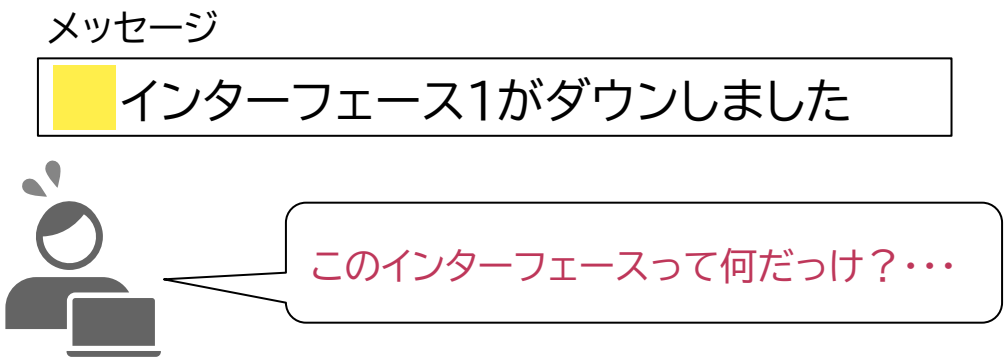
該当機能
状態監視: thresh:しきい値チェック、valchange:値変化 ルール
データ収集: 汎用、MIB 計算式 ルール
その他、SNMP アクセスコマンド

ネットワークインターフェイスの詳細情報を表示する機能を追加(NVP)

ネットワークインターフェイスの詳細情報を表示できるようになりました。障害時の状況把握を即座に実施できます。

◆ Before

- 装置から取得したifAliasやifName(個別に設定可能)の値をインタフェースプロパティダイアログ、およびアラート内に表示できなかった。



◆ After

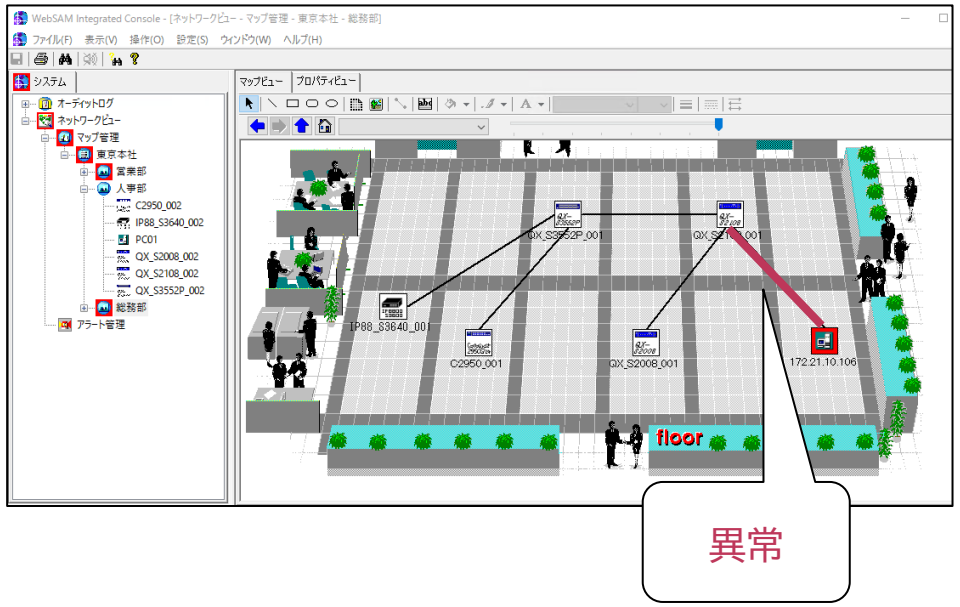
- ネットワークインターフェイスの詳細情報を表示できるようになり、ネットワーク接続を正確に把握。
- SNMPトラップによるアラートでifIndexに対応したifAlias値を表示することで、どのデバイスの状態変化なのか即座に把握。
- データ収集機能のしきい値超過アラートでifAlias、ifName、ifDescrの値をカスタマイズして画面表示し、状況把握が可能。

ネットワークインターフェイスの管理機能の強化(IMS)

WEBブラウザ(IMS)でネットワークインターフェイスの状態を可視化するための機能強化を行いました。

◆ Before

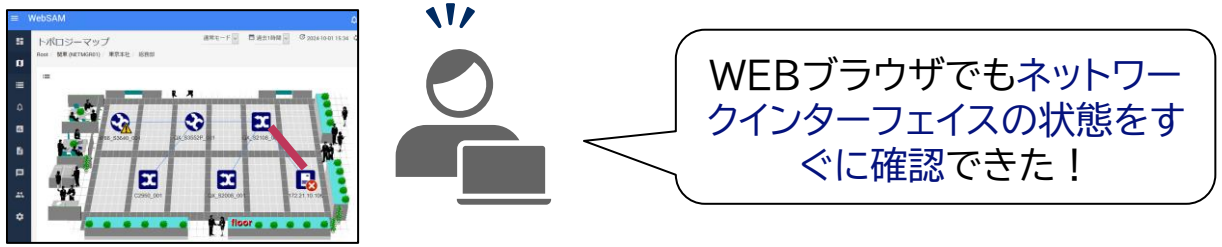
- 専用Viewで特定の監視設定を入れることでネットワークインターフェイスの状態を確認。



◆ After

WEBブラウザで以下を確認できるようになりました

- ネットワークインターフェイス一覧画面にて監視状況に応じた状態を表示。
- 状態が[DOWN]であるネットワークインターフェイスを端点とした接続線を異常を示す赤色で表示。
- ネットワークインターフェイス詳細画面のウィジェットにて、NetvisorProで設定したしきい値をグラフ上に表示。

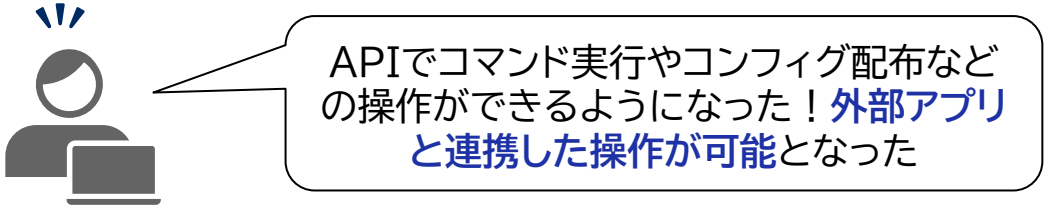


※本強化内容は、WebSAM NetvisorPro V9.6 以上との接続において有効となります

WebAPIの強化(NVP)

管理情報をリモートから取得・操作する、WebAPI を強化しました。

機能名	操作内容	説明
構成情報管理	装置コマンドの実行	装置に対して任意のコマンドを実行することができます。監視端末機能でのコマンド実行機能やnvpdevcmdexe コマンドと同等の操作機能を提供します。
コンフィグ管理 ※コンフィグ管理のWebAPI を利用するためには、ResourceManager 拡張機能ライセンス(RM ライセンス)が必要になります	コンフィグ収集	装置に対するコンフィグの収集・配布を行うことができます。監視端末機能でのrunning-config またはstartupconfigの収集・配布と同等の操作機能を提供します。
	コンフィグ配布	
	コンフィグ一覧取取得	収集したコンフィグの履歴を参照することができます。監視端末機能でのコンフィグの履歴参照と同等の操作機能を提供します。
	コンフィグ詳細取得	



WebAPIの強化(IMS)

管理情報をリモートから取得する、WebAPI を強化しました。

機能名	操作内容	説明
構成情報管理	インターフェイス取得	ネットワークインターフェイスの一覧取得、および詳細取得のAPI において、状態、別名の情報を返却します。
		ネットワークインターフェイスの一覧取得のAPI において、指定可能な検索条件に状態、別名、説明、IPv4 アドレスを追加。
イベント管理	イベント一覧取得	イベント一覧取得、および詳細取得のAPI において、SNMP トラップや Syslog の情報を返却します。
性能管理	データ取得	特定ネットワークインターフェイスのSNMP データ取得のAPI において、NetvisorProで設定されたしきい値の情報を返却します。

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC