

Vario Network Security Suite Ver1.0.0

リリース日: 2020年3月1日

この度は、Vario Network Security Suite をご利用いただきまして誠にありがとうございます。
簡単にではありますが、サービスの紹介をさせていただきます。

Vario Network Security Suite

Vario Network Security Suite とは、昨今懸念される情報システム部門の人材不足、システムインフラに潜むセキュリティ問題等の様々な課題への解決策として、情報システム部門の機能をサービスにより軽減する **情シス as a サービス** 構想に基づいたIT運用・管理サービスです。

以下の3つの主機能により構成されています。

- Vario Network Finder
- Vario Vulnerability Tracker
- Vario System Monitor

お申込みいただきますと、専用の管理画面からサービスをご利用いただけるようになります。
それぞれの機能については下記をご参照ください。
詳しいご利用方法はご利用手引きをご覧ください。

Vario Network & Security Suite Version 1.0.0

- Network Finder →**
社内ネットワークのノードをスキャン・管理する。
- Vulnerability Tracker →**
社内ネットワークのノードに対して脆弱性を診断する。
- System Monitor →**
社内ネットワークのノードを監視する。
- サポート →**
よくある質問やサポート連絡先を確認する。

Vario Network Finder

Vario Network Finder (VNF) では、お客様のネットワーク環境にあるPCやサーバ、ルータやスイッチ等のネットワーク機器を自動スキャンします。

スキャンには、申し込み時にお送りいたします専用機器 **VNSS one** を利用します。
事前にネットワーク情報をいただきすべて設定のうえお送りいたしますので、
お手元に届きましたらお客様ネットワーク内へ機器をお繋ぎいただくとすぐにご利用いただけます。

スキャンで取得した情報をもとに資産管理台帳を作成することもできます。

VNF機能一覧
ネットワークプロトコル：IPv4
最大ノード数：300
対象ノード：Windows PC, Mac, 物理サーバ, クラウドインスタンス, ネットワーク機器 など
取得項目：IPアドレス, MACアドレス, 製品モデル名/製品ベンダ名, OS名/バージョン/シリアル番号 (サーバ), ファームウェア名/バージョン/シリアル番号 (ネットワーク機器), Windows Update (Windowsの場合), BIOS情報 (ベンダ名, バージョン), マザーボード (ベンダ名, モデル番号, バージョン名, シリアル番号), CPU情報 (ソケット数, コア数, プロセッサ数, モデル名, 定格クロック), メモリ, ストレージ情報 (ドライブ数, 総容量), カーネル (名前, バージョン, リリース)
その他：エクスポート, 管理ノード手動登録

Home Network Finder Vulnerability Tracker System Monitor サポート

管理グループ V-SENSOR

現在の管理グループ: [メニュー] 🔍

管理グループの設定 ⚙️ スキャン 📄 🔍

IPアドレス詳細 🔍

システム情報

機種・OS	Microsoft Windows 10 Pro
バージョン	10.0.17763
シリアルNo.	00330-80000-00000-AA173

検出アドレス一覧

IPアドレス	サブネット	ホスト名	MACアドレス	MACアドレスベンダー
192.168.101.191	192.168.101.0/24	DESKTOP-DE4KTQS	24-b6-fd-fa:cf:2e	Dell Inc.

ノード詳細情報

BIOS	ベンダー名	Dell Inc.	
	バージョン番号	DELL - 6222004	
マザーボード	ベンダー名	Dell Inc.	
	モデル番号		
	バージョン番号	A00	
製品	モデル番号		
	モデル名	Latitude E6220	
	シリアル番号	GZH46XP1	
	バージョン番号	01	
	ファームウェアバージョン番号		
	ベンダー名	Dell Inc.	
CPU	ソケット数	1	
	コア数	2	
	プロセッサ数	4	
	cpu0	モデル名	Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz
		定格クロック	2501
メモリ	総容量	8.00GB	
ストレージ	ドライブ数	1	
	総容量	232.88GB	
カーネル	名前	N/A	
	バージョン	N/A	
	リリース	N/A	
Windows	バージョン	1809	
	OSビルド番号	17763.678	

<h4>パッケージ数</h4> <p>78 個</p> <p>詳細 →</p>	<h4>適用済みWindowsアップデート数</h4> <p>8 個</p> <p>詳細 →</p>
---	--

Vario Vulnerability Tracker

Vario Vulnerability Tracker (VVT) では、Microsoft,Apple,Linux など、さまざまなベンダから発表されている脆弱性情報を1つの画面で提供いたします。
※現バージョンではMicrosoftのみ

VNFで取得した適用済みのWindows Update情報をもとに、発表されている脆弱性情報とマッチングしそれぞれの機器の脆弱性を可視化することができます。

VVT機能一覧

ノード/OSによる脆弱性情報確認, 対策ToDoリスト作成

The screenshot shows the VVT interface with the following elements:

- Navigation: Home, Network Finder, **Vulnerability Tracker**, System Monitor, サポート
- Sub-navigation: TOP, **新着情報**, 検知ノード一覧
- Header: 脆弱性情報詳細 - CVE-2020-0824 (公開日: 2020-03-10) 緊急 Microsoft
- Buttons: 新着情報一覧に戻る, 該当ノード: 8件を表示, 原文
- Section: **March 2020 Security Updates**
- Table with columns: CVE ID, Vulnerability Description, Severity, Impact
- Table Content:

CVE ID	Vulnerability Description	Severity	Impact
CVE-2020-	Internet Explorerがメモリ内のオブジェクトに不適切にアクセスする場合に、リモートコード実行の脆弱性が存在します。この脆弱性により、メモリが破損し、攻撃者が現在のユーザーのコンテキストで任意のコードを実行する可能性があります。攻撃者がこの脆弱性を悪用した場合、現在のユーザーと同じユーザー権限を取得する可能性があります。現在のユーザーが管理者ユーザー権限でログオンしている場合、攻撃者が影響を受けるシステムを制御する可能性があります。その後、攻撃者はプログラムをインストールする可能性があります。データの表示、変更、または削除。または、完全なユーザー権限を持つ新しいアカウントを作成します。	Critical	Remote Code
- Buttons: 対象を表示

Vario System Monitor

Vario System Monitor (VSM) では、VNFで取得した機器を監視することができます。

デフォルトの監視設定は **ping監視** となっております。

VSM機能一覧

LAN内ノードの死活監視, Zabbix連携

The screenshot shows the Vario System Monitor interface with the following elements:

- Header: Vario-NSS Your Board: vnf1001 (vNSS)
- Navigation: Home, Managed Security, Network Finder, Vulnerability Tracker, **System Monitor**, Data Analyzer, Data Protect, サポート
- Sub-navigation: 監視データ, インベントリ, レポート, 設定, 管理
- Global view: タッチボード, 障害, 概要, Web, 最新データ, グラフ, スクリーン, マップ, ディスカバリ, サービス
- Dashboard Widgets:
 - データの概要**: Table of host status (VNSS-192.168.101.11 to VNSS-host-192.168.101.144) with columns for ICMP loss, ICMP ping, and ICMP response time.
 - 深刻度ごとの障害数**: Bar chart showing the number of incidents by severity (致命的な障害, 重度の障害, 軽度の障害, 警告).
 - ディスカバリのステータス**: Table showing discovery status for icmp (134 Up, 90 Down), Local network (2 Down), and snmp_agents.
 - 障害**: List of incidents with columns for time, host, severity, duration, status, and action.
 - Web監視**: Section for monitoring web services.