



## 産業制御ネットワーク向け リアルタイムサイバーセキュリティの可視化!

今までは、ICSネットワーク、デバイスおよびプロセスのステータスに対する包括的でリアルタイムの可視性を得ることが困難でした。Nozomi Networksの既に特許を有する最新のAIおよび機械学習を駆使した革新的な技術は、ICSネットワークおよびSCADAネットワークに対して完全に非侵襲的で安全な方法で、この難題を解決します。

これらの他に類を見ない最新技術は、産業ネットワークを、そのコンポーネント、接続およびトポロジを含めて、リアルタイムで自動的に発見します。その高度な学習能力により、ICSに固有のプロセスプロファイルとセキュリティプロファイルを作成し、挙動分析を使用してプロファイルを常に監視することにより、サイバー攻撃と深刻なプロセス異常を迅速に検出します。

### ● 産業制御ネットワーク向けのリアルタイムのサイバーセキュリティと可視性

**Guardian™** を用いて、サイバー攻撃や運用の中断から制御ネットワークを保護し、サイバー攻撃やプロセス異常を迅速に検出することで、これまでになく運用の可視性を提供します。**Guardian™** が誇る最新の見識は、サイバー・レジリエンシー、信頼性および安全性を改善するのに役立ちます。

### ● 特許を有する「サイバーセキュリティとプロセス異常の迅速な特定」

#### - 侵入を検出

スキャンおよびMITM攻撃・複雑な攻撃またはゼロデイ攻撃。

#### - 不正な挙動を検出

リモートアクセス・設定・ダウンロード・コントローラ論理の変更・PLCプロジェクトの編集・インターネットまたはエンタープライズネットワークへの接続・PLC認証など。

#### - 脆弱性を検出

脆弱性を有する資産を自動的に特定・深刻度毎にすべての脆弱性を検索可能な専用表示。

#### - インシデントまたは懸念すべき状態を検出

誤設定・弱いパスワードまたは設定・パッチの欠如・既知の脆弱性・開いているポート・新規の資産または対策を講じていない資産・クロスレベルまたはゾーン通信・デバイスが生成したトラフィックストーム・動作不良・セキュアでないインターネット通信・暗号化されていない通信・通信障害。

#### - 自動学習

- ・製品を学習モードから保護モードに切り替えるための手動による入力不要。
- ・異常検出とサイバーセキュリティ監視を迅速に開始。

### ● ICSやプロセスおよび資産の自動リアルタイム・モデリング

- ・ダウンタイムまたはネットワークの中断なしにインストール可能。
- ・SPANポートまたはミラーポートを介してネットワークデバイスに接続。
- ・大規模な異種ICSを自動的に学習・モデル化し、ベースラインのセキュリティプロファイルとプロセスプロファイルを作成。
- ・あらゆるベンダのあらゆるシステム資産を特定・把握。
- ・各資産およびその通信に関する詳細な情報を提供。
- ・並べ替えや検索が容易な専用ビューで資産を提示。
- ・設定、ファイアウォール、デバイスの変更など、資産の変化があったときに警報をトリガ。

### ● 信頼性の保護と時間の節約を実現する運用の可視性

- ・トポロジを含むリアルタイムのネットワーク可視化を提供。
- ・資産、通信、基礎となる産業プロセスを監視。
- ・警報をコンテキストウェア・インシデントに一元化することを含め、すぐに使用可能な情報をカスタマイズ可能なダッシュボードに提示。
- ・ネットワークまたはICSのパフォーマンスの任意の側面に関するリアルタイム照会を可能にし、スプレッドシート作業や工場現場でのデータ収集を大幅に低減。
- ・障害がある機器に関する事前通知。
- ・トラブルシューティングや修復作業を低減し、ICSインシデントの再現とアーカイブにより、フォレンジック調査を支援。



コーネットソリューションズ株式会社



(TEL) 03-5817-3655 (代)  
www.cornet-solutions.co.jp

## ● マルチサイト、多国籍の事業者に提供される価値

### - 企業の要件を満たす

- ・数百のサイトまで拡大し、アグリゲートされた情報にGuardian中央管理コンソールを使用してアクセス可能です。
- ・アドバンス・バージョン、アップグレード・バージョン、ロールバック・バージョンの制御機能を提供します。
- ・ユーザおよびマネージド・サービス・プロバイダ用の役割ベースのアクセス制御を含みます。
- ・複雑な照会に対する素早い応答と絶え間ないコンプライアンスチェックの迅速な処理によって、最適なパフォーマンスを提供します。

### - セキュリティ・インフラと統合

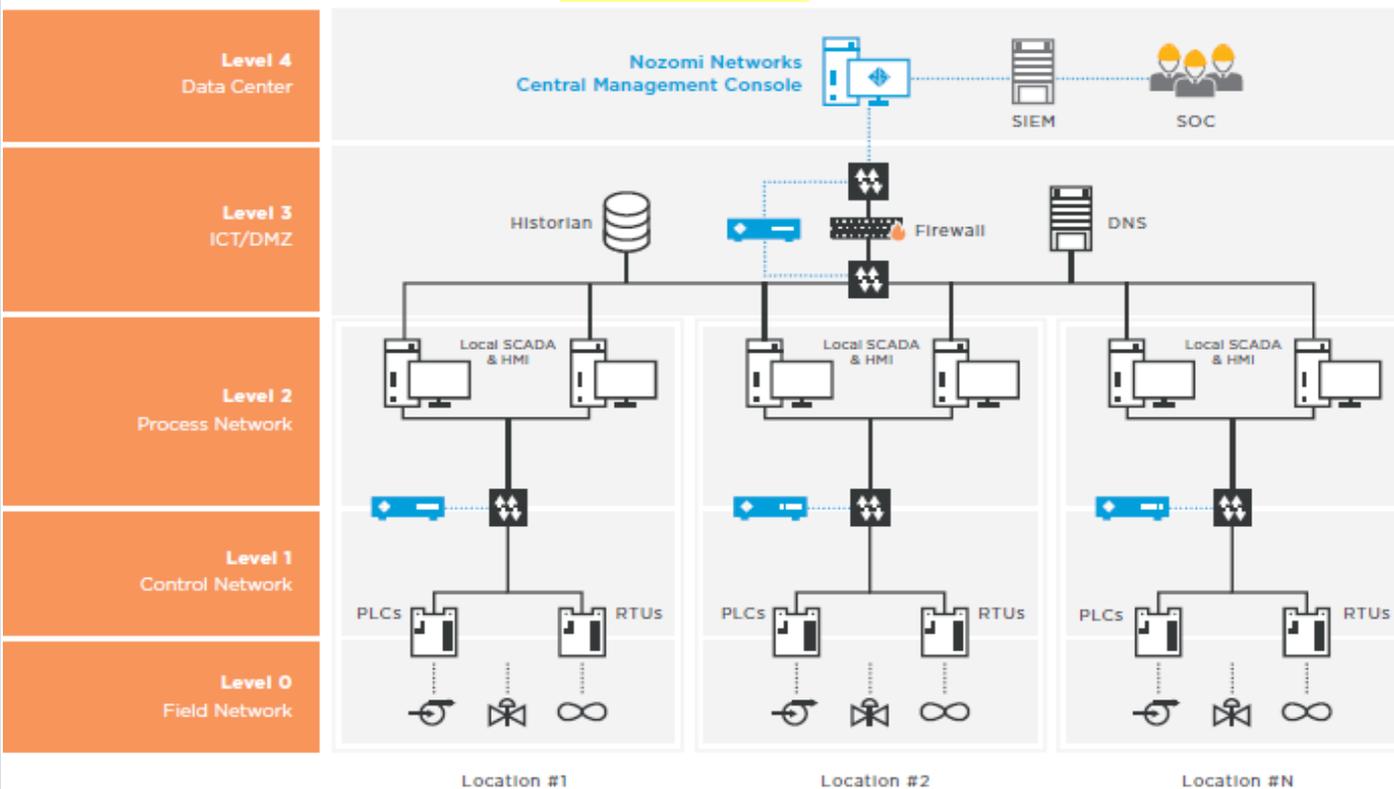
- ・SIEM: HP ArcSight, Splunk, IBM QRadar, AtosCodex, LogRhythm, FireEye
- ・ユーザ認証: Active Directory, LDAP
- ・ファイアウォール: Fortinet, Check Point, Cisco, Paloalto

### - 迅速なROIを提供

既に、多数の顧客サイトに導入され、石油&ガス、電力公益事業、製造および輸送の分野にわたる数万の産業デバイスを監視しています。

## アーキテクチャの例

## “Guardian”シリーズ



## 産業制御システムおよびICS/ITプロトコルの広範なサポート

### ● ICSベンダ

ABB, Allen-Bradley/Rockwell, Bristol Babcock, Beckhoff, Emerson, General Electrics, Honeywell, IBM, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa, Omron

### ● 産業プロトコル

ABB PGP2PGP, Aspentech Cim/IO, BACnet, Beckhoff ADS, BSAP IP, CC-LINK IE, CEI 79-5/2-3, COTP, DNP3, Emerson DeltaV, Enron Modbus, EtherCAT, EtherNet/IP - CIP, Foundation Fieldbus, Foxboro IA, Generic MMS, GE EGD, GE iFix2iFix, GE SRTP, GOOSE, Honeywell Experion Protocols, Kongsberg Net/IO, IEC 60870-5-7(IEC 62351-3 + IEC 62351-5), IEC-60870-5-104, IEC-61850 (MMS, GOOSE, SV), IEC DLMS/COSEM, ICCP, Modbus/RTU, Modbus/TCP - Schneider Unity Extensions, MQTT, OPC, PCCC, PI-Connect, Profnet/DCP, Profnet/I-O CM, Profnet/RT, ROC, Sercos III, OPC, PI-Connect, Profnet, Siemens S7, S7 Plus, Telvent OASyS DNA, Triconex TSAA, Vnet/IP, Melsec (Melsoft), SLMP, Omron FINS

### ● ITプロトコル

ARP, BitTorrent, BROWSER, CDP, DCE-RPC, DHCP, DNS, DRDA ( IBM DB2 ) Dropbox, eDonkey (eMule), FTP, FTPS, GVCP, HTTP, HTTPS, ICMP/PING, IGMP, IKE, Indigo Vision, IMAP, IMAPS, ISO-TSAP/COTP, Kerberos, KMS, LDAP, LDAPS, LLDP, LLMNR, MDNS, MS SQL Server, MySQL, NetBIOS, NTP, OSPF, POP3, PTPv2, RDP, STP, SIP, RTCP, RTP, SSH, SNMP, SMB, SMTP, SSDP, Symantec Endpoint Manager, Syslog, Team Viewer, Telnet, TNS, VNC



- ・追加のシステムおよびプロトコルのサポートは常に拡大されています
- ・最新のリストについては、Nozomi Networksの営業担当者またはパートナーにお問い合わせください。
- ・他の産業プロトコルの追加も可能です。

## “Guardian™” の主な機能

### ● 産業制御ネットワークの自動リアルタイム・モデリング

- ・非侵襲的な設置は、ネットワークの変更、ダウンタイム、中断を必要としません。
- ・ICSネットワークトラフィックを使用して、物理プロセス/ネットワーク展開のベースラインとなるICS仮想イメージを構築します。
- ・高度な産業ネットワーク挙動分析と継続的なリアルタイム評価による、深刻な状態の迅速な特定。

### ● サイバーセキュリティとプロセスの異常の迅速な特定

- ・内部からのものか外部からのものか、悪意のあるものか偶発的なものかにかかわらず、サイバーセキュリティ・インシデントを検出・軽減します。
- ・警報と一目でわかるダッシュボードにより、最新のサイバーセキュリティ・ステータスを維持します。
- ・リアルタイムの照会、再現、フォレンジック・ツールを使用してインシデントを把握します。

### ● これまででない運用の可視性

- ・常に最新のネットワーク・マッピングと仮想化により、ネットワークとプロセスに対する認識を改善します。
- ・不正確なアクティビティ、誤設定、動作不良などのリアルタイムのICSプロセス異常を直ちに検出します。
- ・主要な問題をハイライト表示する直観的でカスタマイズ可能なダッシュボードにより、プロセスに対する見識を強化します。ドリルダウン・ツールにより、問題の分析が容易になります。

### ● エネルギー、公益事業および製造業のリーダーに価値を提供

- ・大規模なグローバル展開で実証済みのソリューションです。
- ・多くのICSプロトコルおよび多種多様な産業/自動化ベンダのデバイスのサポートに対する広範な適用可能性。
- ・VAR、SI、デバイスメーカーをはじめとする顧客、アナリスト、パートナーによる支持。



## “Guardian™” 導入の主なメリット

### ● サイバーセキュリティ脅威とインシデントを迅速に検出

非侵襲的な設置は、ネットワークの変更、ダウンタイム、中断を必要としません。ICSネットワークトラフィックを使用して、物理プロセス/ネットワーク展開の論理的で包括的なモデルである、運用のベースラインとなるICS仮想イメージを構築します。高度な産業ネットワーク挙動分析と継続的なリアルタイム評価による、深刻な状態の迅速な特定。

### ● 運用の異常の素早い特定と修復

Nozomi Networksのソリューションは、ネットワーク上のデバイスや、それらのデバイスがプロセス挙動にどのように影響を及ぼすかをベースライン化することによって、動作不良、誤設定および異常を迅速に特定します。レポートと警報は、サービスの中断、費用のかかる修理、収益の損失を回避するのに役立ちます。

### ● 時間を節約し、規制コンプライアンスの罰金を回避

Guardianは、自動化された詳細なビジネスレポートを提供するので、時間のかかる手作業でのデータ収集を行う必要がなくなり、規制違反の罰金を回避します。

### ● トラブルシューティングおよび修復作業の低減

ネットワークデータを復号したり様々なソースから手作業で情報を収集したりするのに何日も費やす代わりに、Guardianの詳細な集中型の分析を使用することで、産業上の問題やインシデント調査に対するリアルタイムの回答を出します。時間の節約とコストの削減を実現します。

### ● 産業資産とそれに対応するサイバーセキュリティリスクを追跡する

リアルタイムの資産管理と脆弱性評価により、ICSのシステムとデバイスを、そのハードウェア構成とソフトウェア構成を含めて把握します。脆弱性評価と組み合わせることで、サイバーセキュリティリスク体制に対する完全な可視性が得られ、迅速な修復を実施することができます。

### ● 中央拠点から遠隔サイトを容易に監視

Nozomi Networksの中央管理コンソールを使用して、複数の施設や広い地理的領域にわたる可視性を利用します。遠隔からトラブルシューティングを行い、インシデントに素早く対応して、オンサイトサポート費用を削減します。

### Nozomi Networksについて

Nozomi Networksは、2013年からICSサイバーセキュリティに大改革をもたらし、産業制御システム(ICS)に対する運用の可視性を可能にしています。Nozomi Networksのソリューションはいくつかの世界最大級の産業施設に導入されており、産業ネットワークの可視性、資産管理、脆弱性管理、プロセス異常と侵入の両方の検出を提供しています。他に類を見ないサイバーセキュリティの強化、アップタイムの最大化、真のROIを実現します。

\* Nozomi Networksはカリフォルニア州メンローパークとスイスのメンドリシオに本社があります。

# ニーズに合う“Guardian™”アプライアンスシリーズ

## 大規模システム向け “HS” “H” シリーズ

	NSG-HS 3500	NSG-HS 3000	NSG-H 2500	NSG-H 2000
Max. Protected Nodes	500,000	300,000	200,000	100,000
Max. Throughput	6 Gbps		3 Gbps	
Max. Remote Collectors*	50		50	
Monitoring Ports	Modular up to 16*2		Modular up to 12*2	
Expansion Slots	4 slots available: 4x1000Base-T   4xSFP   4xSFP+		2 slots available: 4x1000Base-T   4xSFP   4xSFP+	
Storage	512 Cb		512 Cb	
Form Factor	1 rack unit		1 rack unit	
Max. Power Consumption	750 W		750 W	
Power Supply Type	100-240V AC - 50/60Hz		100-240V AC - 50/60Hz	
Temperature Range	0 / +40° C		0 / +40° C	
HxWxL (mm/in)	44 x 438 x 600 173 x 17.24 x 23.60		44 x 438 x 600 173 x 17.24 x 23.60	
Weight	18 Kg		17 Kg	



## 耐環境向け “R” ポータブルタイプ “H” シリーズ

	NSG-R 150	NSG-R 50	P550
Max. Protected Nodes	1,000	500	2,500
Max. Throughput	250 Mbps	100 Mbps	200 Mbps
Max. Remote Collectors*	20	10	Not available
Monitoring Ports	7x1000BASE-T	4x1000BASE-T	5x1000BASE-T
Expansion Slots	Not available		Not available
Storage	64 Cb		256 Cb
Form Factor	2 rack unit	DIN mountable	Desktop with wall mount kit
Max. Power Consumption	250W	60W	38W
Power Supply Type	100-240V AC 100-240V DC	100-240V AC 12-36V DC	90-240V AC 12-30V DC
Temperature Range	-40 / +70° C	-40 / +75° C	0 / +60° C
HxWxL (mm/in)	88 x 440 x 301 3.46 x 17.32 x 11.86	80 x 130 x 146 3.15 x 5.11 x 5.74	70 x 190 x 240 2.75 x 7.08 x 9.44
Weight	6 Kg	3 Kg	2.5 Kg

## 中小規模システム向け “M” “L” シリーズ

	NSG-M 1000	NSG-M 750	NSG-L 250	NSG-L 100
Max. Protected Nodes	40,000	10,000	5,000	1,000
Max. Throughput	1 Gbps		500 Mbps	
Max. Remote Collectors*	50		20	
Monitoring Ports	7x1000BASE-T + 4xSFP		5x1000BASE-T	
Expansion Slots	1 slot available: 4x1000Base-T   4xSFP   4xSFP+		1 slot available: 4x1000Base-T   4xSFP	
Storage	256 Cb		64 Cb	
Form Factor	1 rack unit		1 rack unit	
Max. Power Consumption	360W		250W	
Power Supply Type	100-240V AC - 50/60 Hz		100-240V AC - 50/60 Hz	
Temperature Range	0 / +45° C		0 / +45° C	
HxWxL (mm/in)	44 x 429 x 438 173 x 16.89 x 17.24		44 x 438 x 300 17 x 17.2 x 11.8	
Weight	14 Kg		8 Kg	



## 仮想アプライアンス “V” シリーズ

	V1000	V750	V250	V100
Max. Protected Nodes	40,000	10,000	5,000	1,000
Max. Throughput*	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Scenarios	Enterprise	Large	Medium	Small
Deployment Options	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+			
Max. Remote Collectors**	50	50	20	20

\* Performance is dependent upon hardware configuration and resource allocation. \*\* See Remote Collector tech specs for details.

### Container Edition Dockerコンテナ

Embedded container appliance for switches, routers and other security infrastructure. Fast, flexible deployment option that leverage your existing devices.

## オプション機能 ① Threat Intelligence

脅威を検出するための最新のThreat Intelligenceを提供！

- Yara rules
- Packet rules
- STIX indicators
- Threat definitions
- Threat knowledgebase
- Vulnerability signatures

## オプション機能②CMC ( Central Management Console : 中央管理コンソール)

複数のGuardianを一元管理！ 階層化された管理ネットワークの構築に最適！

### Cloud or Virtual Central Management Console

Deployment Options - Cloud	Amazon AWS and Microsoft Azure
Deployment Options - Virtual	Hyper-V 2012+, KVM 1.2+, VMware ESX 5.x+, XEN 4.4+
Max. Managed Appliances	Unlimited*
Storage	100+ Gb

CMCをインストールするために必要な仮想環境要求仕様

## オプション機能 ③ Remote Collectors

リモート拠点を可視化するための超小型パケットキャプチャ装置！

## オプション機能 ④ Smart Polling

より精度の高い脆弱性情報を得るために監視対象ノードへアクティブなポーリングを送信！



コーネットソリューションズ株式会社



(TEL) 03-5817-3655 (代)  
www.cornet-solutions.co.jp