第25回 石油化学工業協会　CEDI/ITフォーラム
情報セキュリティWG活動報告

# 制御システムにおける
# ネットワークトラフィック可視化技術とサービスのご紹介

## ～ネットワーク健全性確認サービス～

**【抜粋版】**

2016年5月24日
横河電機株式会社
ソリューションサービス事業本部
ライフサイクルサービス事業部
畠山敏弘

【抜粋版】

# 目次

【抜粋版】

# 制御システムが狙われる

制御システムが狙われる

# 制御システムの近況と比較

## 課題

- 近年、重要インフラの制御システムもサイバー攻撃の対象となり、セキュリティ確保が大きな課題となっています。

スタックスネット(Stuxnet)
2010年9月イランの核燃料装置のウラン濃縮用遠心分離器を制御しているソフトウェア(OS、製品)をターゲットにしたサイバー攻撃を受けて全て(約8400台)の分離器が稼働不能の陥った。

## 原因

- サイバー攻撃の対象となる原因の一つに、制御システムインフラ(PC等のハードウェア、Windows OS等のソフトウェア)のオープン化があります。(高度情報通信による見える化や価格競争)

## 対策

- セキュリティ確保として、オープン化では標準の対策を導入するには制御システム固有の特徴があり困難になっています。

表　制御システム固有の特徴

| | 制御システム | 情報システム |
|---|---|---|
| セキュリティ優先順位 | A.I.C(可用性重視)※ | C.I.A(機密性重視)※ |
| 可用性 | 24時間365日 | 通常業務時間内 |
| 運用期間 | 20年以上 | 3～5年 |
| データ遅延 | リアルタイム | 遅延許容あり |
| 運用管理 | 現場操業部門 | 情報システム部門 |

※　C：「機密性」(Confidentiality)、I：「完全性」(Integrity)、A：「可用性」(Availability)

「**重要インフラ分野**」(平成26年5月19日 情報セキュリティ政策会議　第３次行動計画)
「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス(地方公共団体を含む)」、「医療」、「水道」、「物流」に加えて「クレジット」、「**化学**」及び「**石油**」の13分野

制御システムが狙われる
# 実現に向けて

専門家でないエンジニアが見ても
直感的に通信状態が把握できる
ネットワーク監視の実現

お客様の制御システム

ネットワークリアルタイム可視化システム
**NIRVANA**
国立研究開発法人　情報通信研究機構（NICT）


＋

制御機器・システム　メーカー

YOKOGAWA
Co-innovating tomorrow™

【抜粋版】

# ネットワークトラフィック可視化の技術

# NIRVANAとYOKOGAWA

## ■国家プロジェクトにおける共同研究からスタート

2007年4月、通信トラフィックのリアルタイムな可視化・分析を実現するシステム（通信の見える化）を国立研究開発法人　情報通信研究機構「NICT」と共同研究を開始
(ネットワークリアルタイム可視化システム：NIRVANAの基礎研究)

## ■研究開発コンセプト

●フローを可視化できること。
従来の流量ではなくPC単位の通信内容を読み取れる。

●可視化により通信状況が直感的に理解できること。
全てのパケットをアニメーションで可視化できる。

●ネットワークの通信状況を判定できること。
管理対象システム内の通信か否かが分かること。

## ■発表

NICTが、2011年6月に“NIRVANA”(ニルヴァーナ：nicter real-network visual analyzer)を発表。

# 機能評価と導入効果

## ■可視化システムに対する要件と評価

| No | 要件 | 評価 | |
|---|---|---|---|
| 1 | 操業に影響が出ないこと | 良 | ネットワーク機器へのミラーリングのみで、各PCへソフトウェア等をインストールしない。 |
| 2 | 理解が容易であること | 良 | 通信の発生を視覚的に直感的に捉えることができる。 |
| 3 | 柔軟性があること | 良 | フィルタリング機能により必要な通信のみに絞り込みできる。 |
| 4 | リアルタイムに可視化できること | 良 | バッファリングせずに描画できる。 |
| 5 | 障害発生時の様子を再現できること | 良 | 保存したデータを読み込んで描画を再現できる。 |

## ■効果

●正常ではない通信の検出
　観測対象ネットワークの外部との通信を発見できる。

●必要な通信の不在
　存在しなければならない通信が不在であることも把握できる。

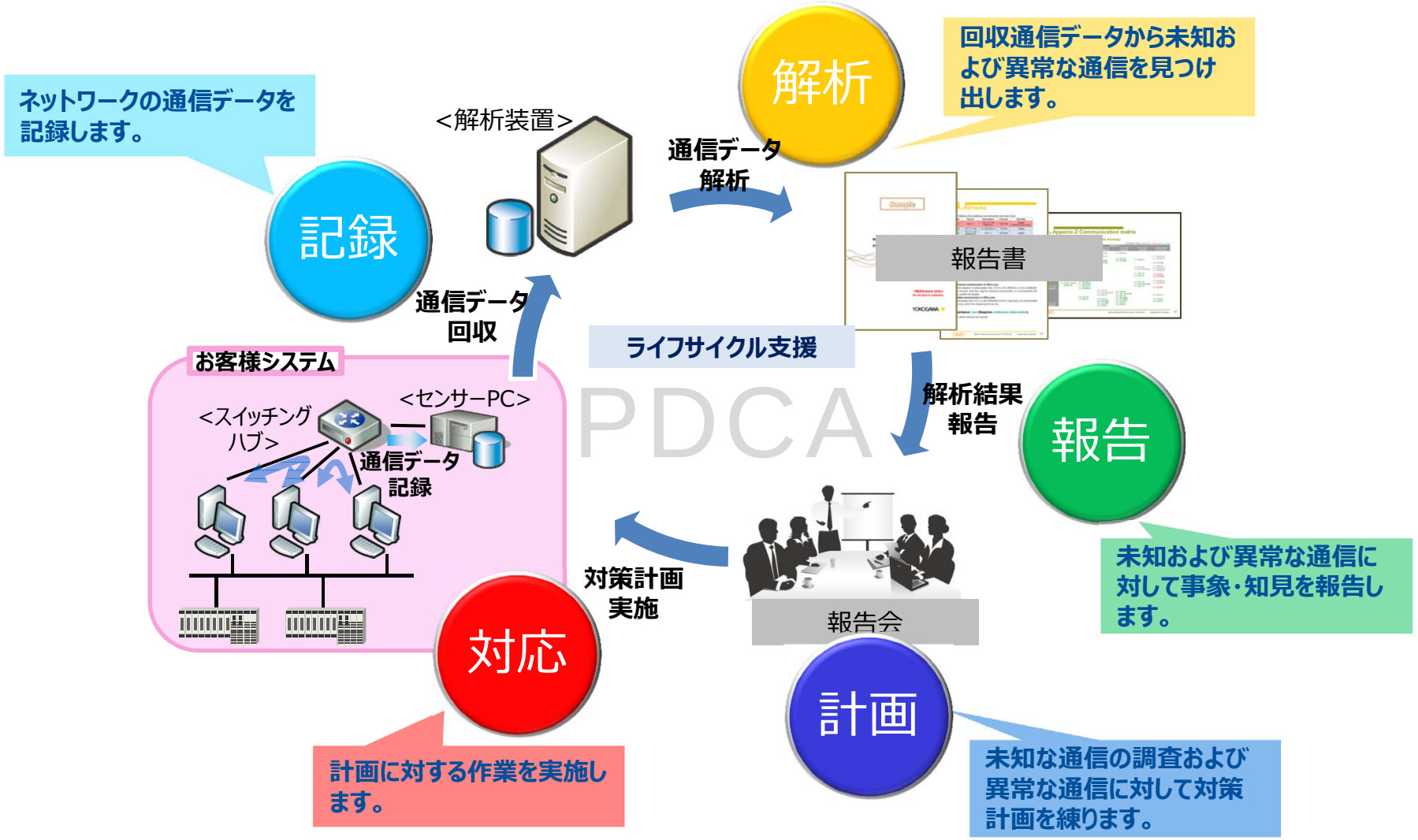
【抜粋版】

# ネットワーク健全性確認サービス

ネットワーク健全性確認サービス

# ライフサイクル支援

## 安定操業をライフサイクルで支援します。



# 適用例

**適用例①：現状把握**

情報系システムとのデータ交換や、他システム間との連携処理のためにネットワーク接続しているが、実際にどのような通信が流れているのかを把握したい。

**適用例②：障害解析**

複数台の操作PCの応答が遅くなることがあり、しばらくすると解消されるがOSやソフトウェアのログには記録がない。ネットワークの通信内容から原因を調査したい。

**適用例③：監査履歴**

システム・セキュリティ監査の対象が制御システムに拡大され、システムの運転状況を記録することが必要になり、ネットワークの通信状況も記録したい。

【抜粋版】

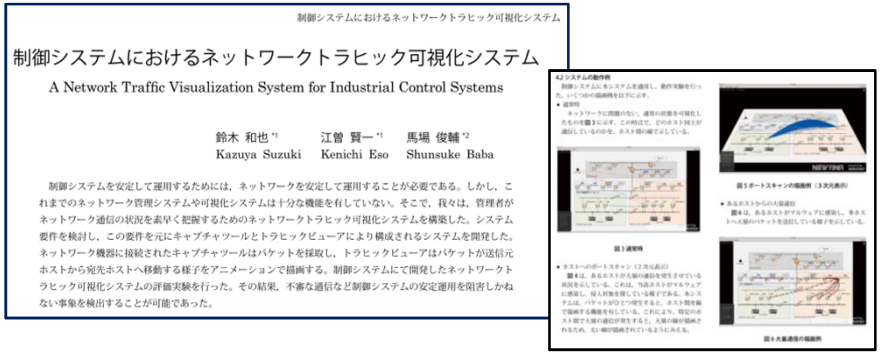
# 詳細について

詳細について

# 横河電機ホームページ

## 2014年　横河技報　［Vol.　57］

### 技術報告 特集／制御システムのセキュリティ 特集
### 制御システムにおけるネットワークトラヒック可視化システム


制御システムにおけるネットワークトラヒック可視化システム

制御システムにおけるネットワークトラヒック可視化システム

A Network Traffic Visualization System for Industrial Control Systems

鈴木 和也 *1　江曽 賢一 *1　馬場 俊輔 *2
Kazuya Suzuki　Kenichi Eso　Shunsuke Baba

制御システムを安定して運用するためには，ネットワークを安定して運用することが必要である。しかし，これまでのネットワーク管理システムや可視化システムは十分な機能を有していない。そこで，我々は，管理者がネットワーク通信の状況を素早く把握するためのネットワークトラヒック可視化システムを構築した。システム要件を検討し，この要件を元にキャプチャツールとトラヒックビューアにより構成されるシステムを開発した。ネットワーク機器に接続されたキャプチャツールはパケットを採取し，トラヒックビューアはパケットが送信元ホストから宛先ホストへ移動する様子をアニメーションで描画する。制御システムにて開発したネットワークトラヒック可視化システムの評価実験を行った。その結果，不審な通信など制御システムの安定運用を阻害しかねない事象を検出することが可能であった。

## プレスリリース　(2015年9月16日発表)

### 国立研究開発法人 情報通信研究機構 / 横河電機株式会社 / 国立大学法人 京都大学
### 制御システムの健全性を確認するトラフィック分析・可視化技術を開発
### ～電力・ガス・水道などの重要インフラを支える制御システムのセキュリティインシデントを検知～

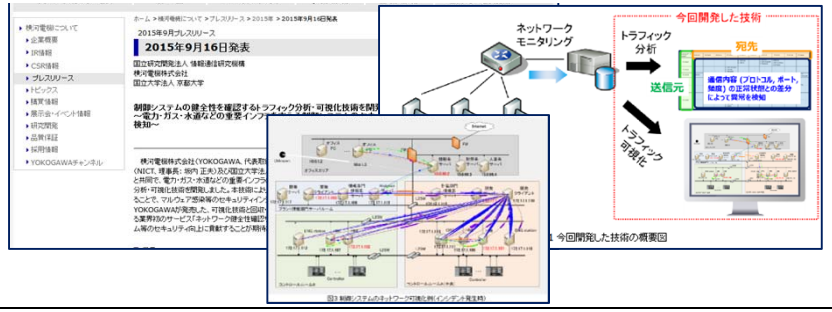


図1 今回開発した技術の概要図

【抜粋版】

Co-innovating tomorrow™

ご清聴　ありがとうございました