CYNOTE

構造計画研究所
KOZO KEIKAKU ENGINEERING Inc.

情報セキュリティ担当者様へ

トラフィック可視化・検知・再現ソリューション

ネットワーク内部対策における
トラフィック可視化・検知・再現ソリューション

従来の対策の限界

ウィルス対策ソフトだけでは侵入を 100% 防ぐことは難しくなり、侵入されることを前提とした早期発見、防御を求められるようになった。

管理すべき機器の増加

モバイル機器の普及などにより、守るべき資産が増加。また、複数ベンダーのセキュリティ機器の管理コストも増大する傾向にある。

専門人材の不足

24 時間 365 日の稼働を要求されるネットワークにおいて、トラブル発生時の初動対応にあたる内部スタッフの確保が難しい。

通信トラフィックの **見える化** **検知** **再現** によって、

不正アクセスや異常の兆候の気づきを与え、

非専門家でも迅速な対応を可能にします。

構造計画研究所のサイバーセキュリティ・ソリューション

侵入させない入口対策から
「組織内部での不正通信の早期発見」へ対策をシフト

- サーバセグメントなど通信禁止セグメントへの侵入検知
- ルールベースの検知エンジンでセキュリティポリシ違反検知
- インシデント時の過去の通信を後から再現

可視化

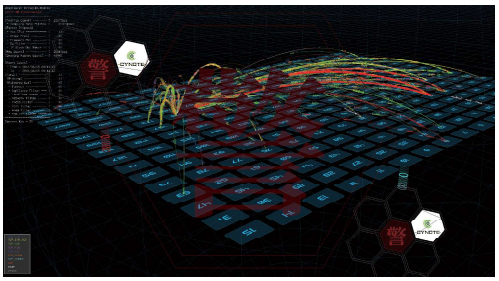
サイバー攻撃統合分析プラットフォーム NIRVANA 改※1

• トラフィックの見える化

通信パケットを 3D アニメーションで描画します。

• セキュリティアラートの見える化

各種セキュリティ機器からのアラートを一元的に表示します。



検知

ライブネットを分析し
不正通信を発見します

CyNote®セグメント侵害検知※2

• 検知エンジン

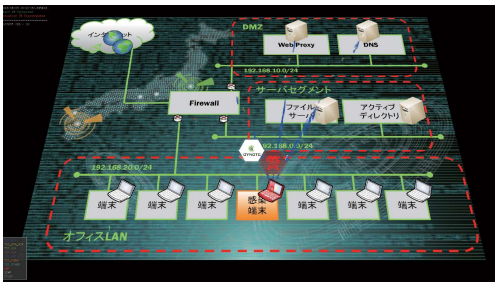
ルールベースの検知エンジンで不正侵入を検知します。

• ルール設定

約 6 万件の検知ルールを設定し動作することを実証しています。

• Web インタフェース

検知結果は Web インタフェースで確認可能です。



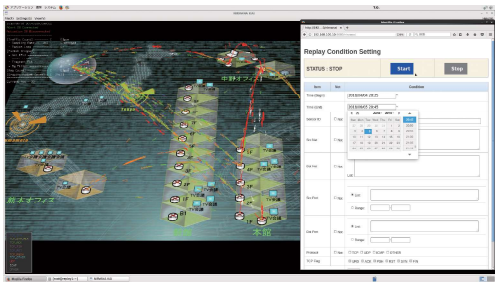
再現

インシデント発生時の
トラフィックを再現します

CyNote®トラフィック再現機構※2

• トラフィック再現

NIRVANA 改と連携し通信の可視化、
過去の通信の再現を行います。
インシデントの分析や確認、報告に活用できます。



CyNote® セグメント侵害検知機能	・分析ルール (セキュリティポリシ設定) : IP アドレス、ポート番号、プロトコルを使用 ・Interop Tokyo 2015 の会場全体のトラフィックを使用し、約 6 万件の検知ルールを設定し動作することを実証済
CyNote® トラフィック再現機構	・設定可能な再現条件 ➤ 開始・終了時刻／送信元・宛先 IP アドレス／送信元・宛先ポート番号／プロトコル／ TCP フラグ ➤ サンプリングレート (1 ～ 100%) ／再生速度 (1/100 ～ 100 倍速)

※1 NIRVANA 改は国立研究開発法人情報通信研究機構 (NICT) が開発したサイバー攻撃統合分析プラットフォームです。
※2 この資料で説明されている機能は、国立研究開発法人情報通信研究機構 (NICT) からライセンス提供を受けて販売しています。

構造計画研究所
KOZO KEIKAKU ENGINEERING Inc.

株式会社構造計画研究所　情報通信営業部

Tel: 03-5342-1121　Mail: cybersecurity@kke.co.jp