4

Analyzing network failure/cyber attacks and their root causes

ビッグデータ分析によるネットワーク異常対策

～ ネットワーク故障、サイバー攻撃などのNW異常を早期に検出～

どんな研究

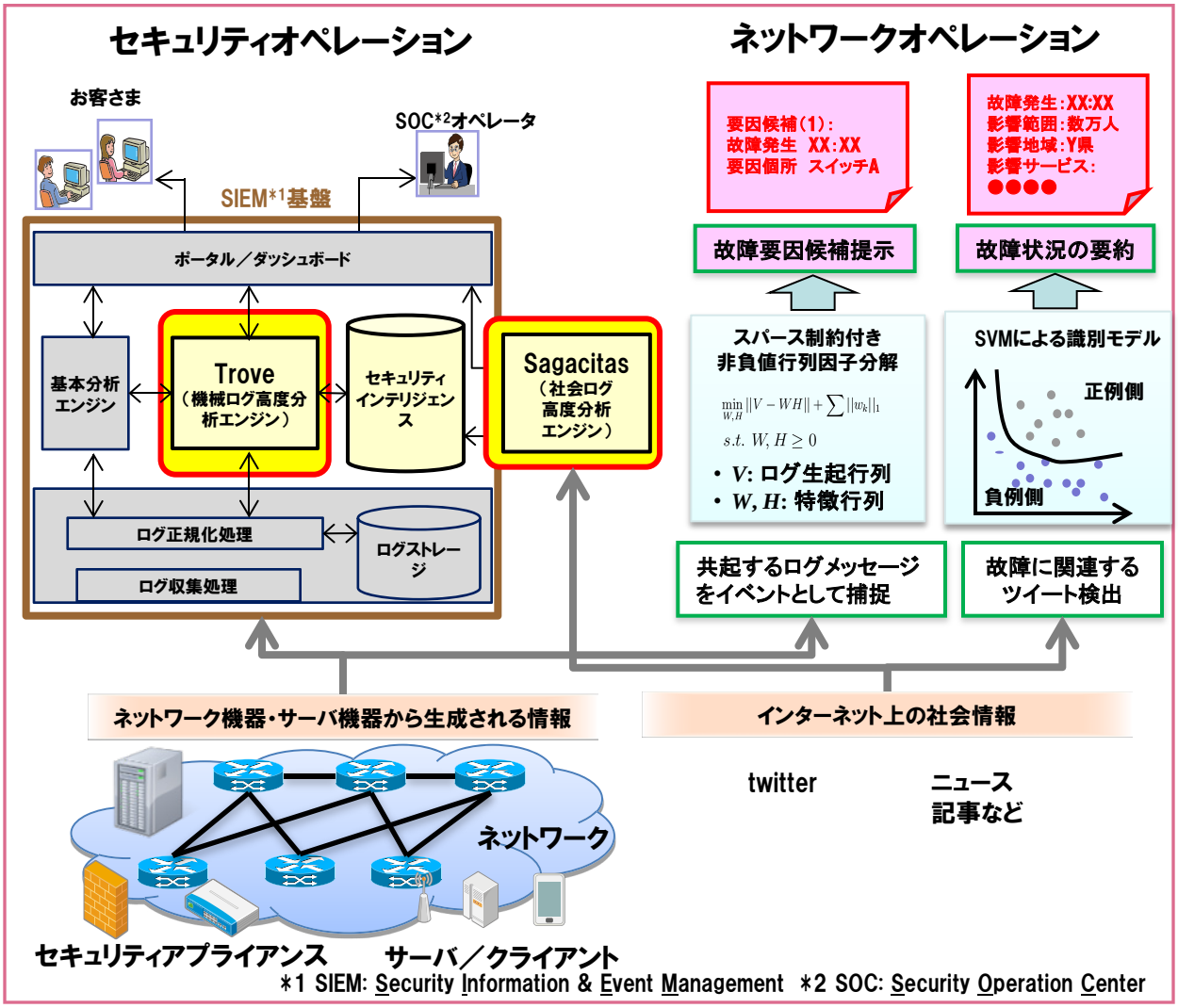
ネットワーク機器やサーバ機器からのログ情報や、SNSやニュース記事などの社会情報といった膨大、不統一、かつ非定型なデータから、機械学習等の高度分析技術を用いて、**従来検出できなかったネットワーク故障やセキュリティインシデント(サイバー攻撃等)**を早期に検出します。

どこが凄い

ネットワーク情報を**時間共起性や通信先共起性を**用いてグルーピング化し、故障イベントの可視化や未知の悪性ホスト検出を行います。また社会情報から、セキュリティや故障に関連する情報を抽出し、リアルタイムに分析し、攻撃予兆や故障発生を早期に検出します。

めざす未来

ネットワーク故障、サイバー攻撃検出技術により、それぞれNTTグループの**ネットワークオペレーション、セキュリティオペレーション**を高度化し、今までより一歩進んだ安心・安全なネットワーク環境の実現に寄与します。



関連文献

[1] K. Sato, K. Ishibashi, H. Hasegawa, and H. Yoshino, “Extending Black Domain Name List by Using Co-occurrence Relation between DNS Queries,” *IEICE Trans. Commun.*, 2012.

[2] 針生剛男，秋山満昭，青木一史，八木毅，岩村誠，倉上弘，“進化するマルウェア等によるサイバー攻撃の検知・解析・対策技術，” NTT技術ジャーナル，2012.

[3] 木村達明，森達哉，石橋圭介，塩本公平，“大規模ネットワーク監視情報における重要イベント抽出法，” 信学技報 NS2011-225, 2012.

連絡先

石橋 圭介 (Keisuke Ishibashi)
NTT ネットワーク基盤技術研究所
通信トラヒック品質プロジェクト
E-mail： ishibashi.keisuke{at}lab.ntt.co.jp

綱川 光明 (Mitsuoka Tsunakawa)
NTT セキュアプラットフォーム研究所
セキュリティマネジメント推進プロジェクト
E-mail： tsunakawa.mitsuaki{at}lab.ntt.co.jp

({at}の部分を@に置き換えてください)