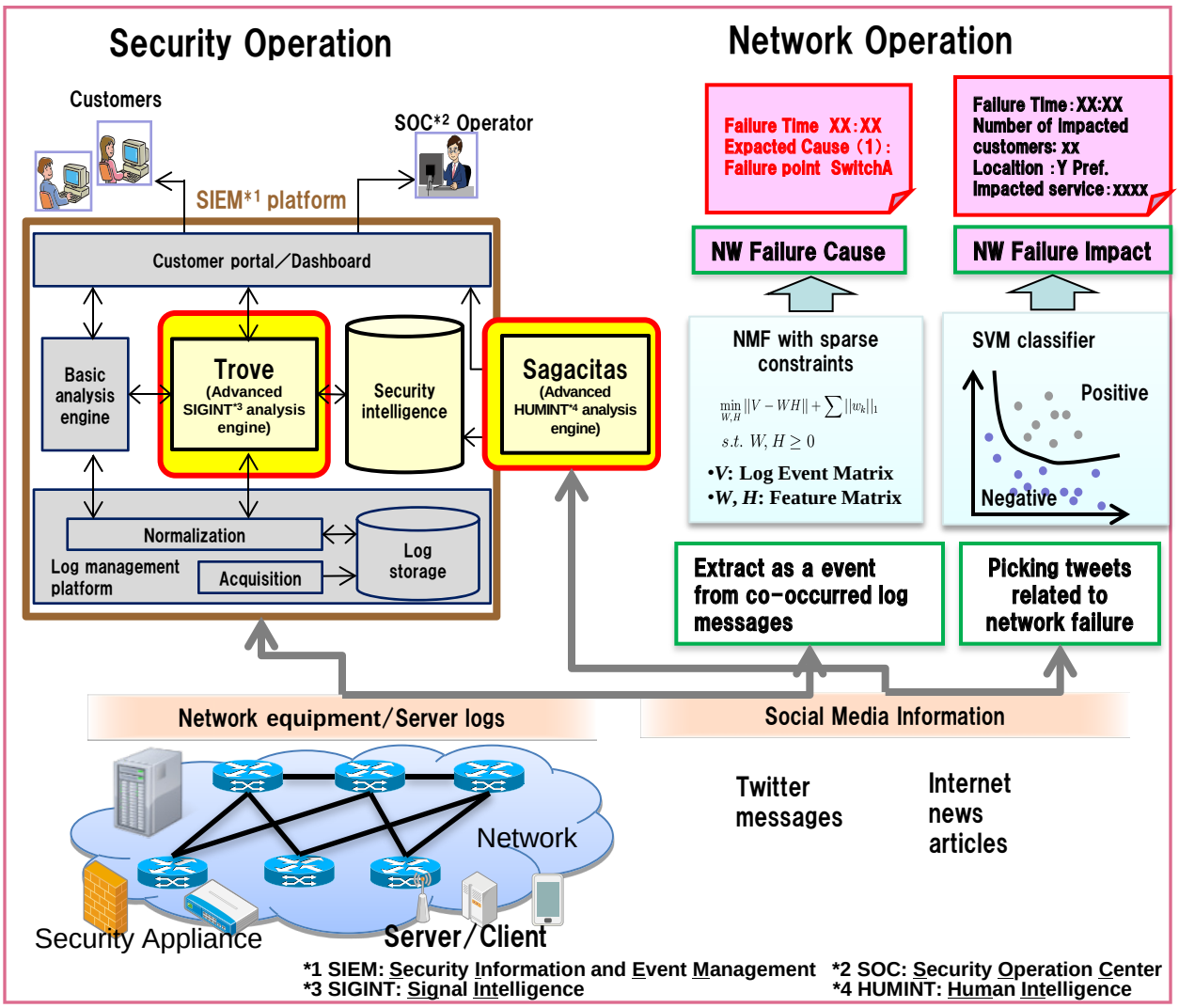
4 Network anomaly detection using big data analysis

Analyzing network failure/cyber attacks and their root causes

***Abstract*— Network anomalies including network failures and cyber attacks are major concerns for both network and security operators, and their rapid detection is crucial to the provision of safe and reliable services. We are developing technologies for the rapid detection of such events via log messages from security appliances, network equipment, and servers or social media information such as Twitter messages. Since such information is atypical and its volume can be huge, we adopt machine learning methods, for example, mining temporal/host correlations in logs to detect network failure events or malicious hosts. By employing these technologies, we will help to provide safe and reliable communication services for our customers.**



Related works

[1] K. Sato, K. Ishibashi, H. Hasegawa, H. Yoshino, "Extending Black Domain Name List by Using Co-occurrence Relation between DNS Queries," *IEICE Trans. Commun.*, 2012.
[2] T. Hariu, M. Akiyama, K. Aoki, T. Yagi, M. Iwamura, H. Kurakami, "Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware," *NTT Technical Review*, Vol. 10, No. 10, 2012.

Contact

Keisuke Ishiabshi
Communication Traffic & Service Quality Project
NTT Network Technology Laboratories
E-mail : ishibashi.keisuke{at}lab.ntt.co.jp

Mitsuaki Tsunakawa
Security Management & Operations Project
NTT Secure Platform Laboratories
E-mail : tsunakawa.mitsuaki{at}lab.ntt.co.jp

(Please replace {at} with @)