Creating New Value by Leveraging Network-AI Technology in Service Operations

Keishiro Watanabe, Yasuhiro Ikeda, Yuusuke Nakano, Keisuke Ishibashi, Ryoichi Kawahara, and Satoshi Suzuki

Abstract

We present in this article an overview of recent research and development done at the NTT laboratories on artificial intelligence technology for networks (Network-AI) that enables proactive maintenance and operations of network services. We also describe some of the key technologies constituting Network-AI and review verification trials of these technologies conducted at an NTT operating company.

Keywords: Network-AI, proactive maintenance and operations, automation

1. Introduction

In order to forge ahead with the development of services while sustaining the services currently available in the face of social changes such as a declining population and ever more diversified communication services, we must have the ability to accurately assess the operational status of services and be able to upgrade and enhance services once they are up and running. The NTT laboratories strive to make service operations more efficient and to enhance service value and are therefore working to implement an autonomous control loop that cycles through the three phases of (1) gathering various types of information, (2) analyzing the collected information, and finally, (3) issuing accurate instructions and controls based on the analytical results in the planning, design, construction, maintenance, and operation of networks. By leveraging artificial intelligence technology for networks (Network-AI)*, we are now making good progress in developing more sophisticated operations and support systems.

Various Network-AI related initiatives are now under consideration. One such initiative is *resources-on-demand*, which automatically suggests and allocates optimal resources required by service providers. Another is *scheduled maintenance*, which eliminates the need for urgent maintenance once a network problem has already occurred. This will give us the ability to autonomously control the entire sequence of service events, from provisioning of services to maintenance and operations, and the entire NTT laboratory community is working toward this objective. This article focuses on key initiatives now underway with the goal of implementing scheduled maintenance.

2. Initiatives enabling scheduled maintenance

Two key capabilities are needed to make scheduled maintenance a practical reality. First, this would require a shift from reactive maintenance and operations that deals with faults and operational problems that have already occurred to proactive maintenance

* Network-AI: The NTT Group has adopted the brand name *corevo* for all its artificial intelligence (AI)-related research and development initiatives. Network-AI is one of the key elements of corevo.

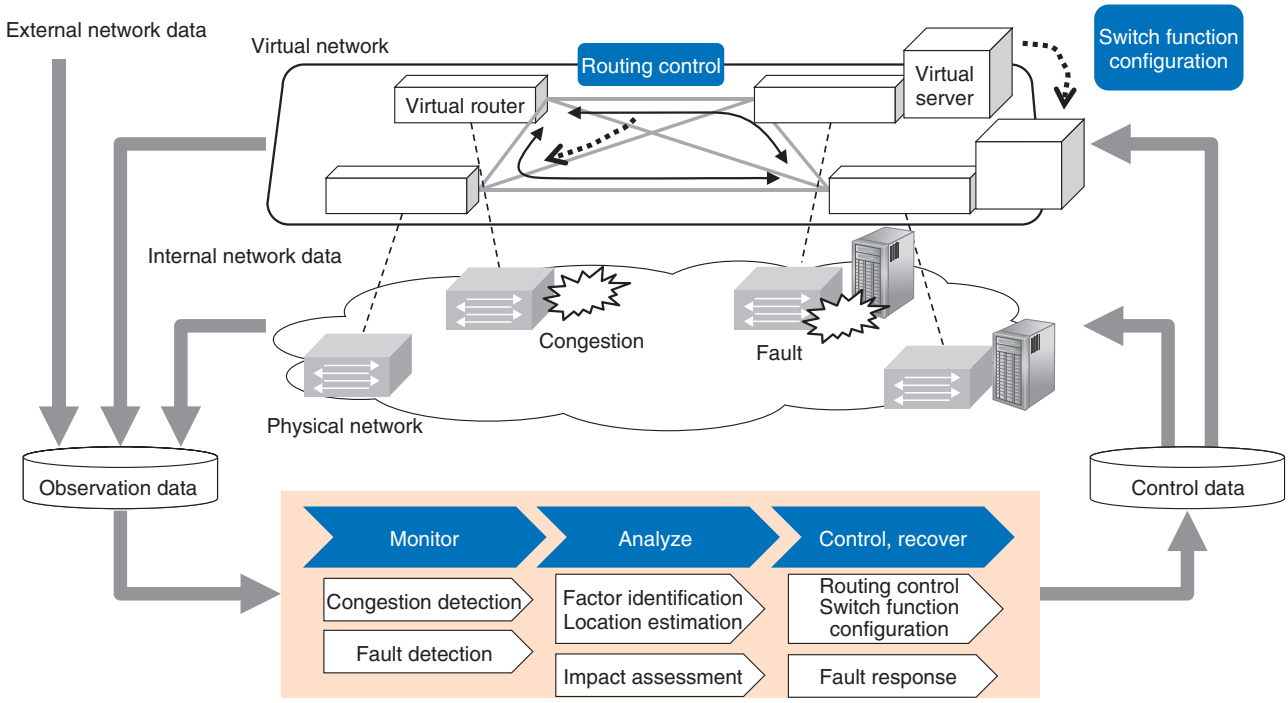


Fig. 1. Proactive controlled network [1].

and operations that focuses on preventing problems before they occur. Second, it requires systematic automated maintenance and operations that fully supports virtualization. The NTT laboratories have come up with the proactive controlled network concept as a way of implementing proactive maintenance and operations combined with automation. The idea behind a proactive controlled network is to anticipate potential performance degradation risks (e.g., outages, failures, and congestion) before they occur, to anticipate foreseeable changes in demand early on, and to achieve proactive control and early automatic recovery.

The proactive controlled network involves a sequence of typical operational phases for dealing with each type of risk: (1) monitor, (2) analyze, and (3) control and recover, as illustrated in **Fig. 1** [1], and we are developing key Network-AI technologies for each phase with the following objectives:

(1) Achieve proactive early detection of changes in network conditions due to degraded performance (congestion, equipment failure, etc.).
(2) Estimate degraded location and likely cause of the changes in network conditions.
(3) Take control to circumvent performance degradation, and implement early recovery.

Some of the core technologies being applied to implement these operational phases are indicated in **Fig. 2**.

We focus here on two of these technologies—*network anomaly detection*, a monitoring technology developed for early detection of anomalous events (e.g., silent failures), and *automatic failure points estimation*, an analysis technology. We also review the status of ongoing verification trials of the network anomaly detection technology that has been deployed and is now being evaluated at an NTT operating company.

3. Network anomaly detection technology

NTT Network Technology Laboratories is making headway in the development of an autoencoder (AE)-based network anomaly detection system designed to achieve early detection of changes in network conditions [2–4]. An AE is a kind of neural network capable of unsupervised learning of the intrinsic complex structure of data and is currently drawing a great deal of interest for anomaly detection applications.

We have utilized AE characteristics such that by setting the number of neurons in the hidden layer of the AE at less than those in the input layer, a data

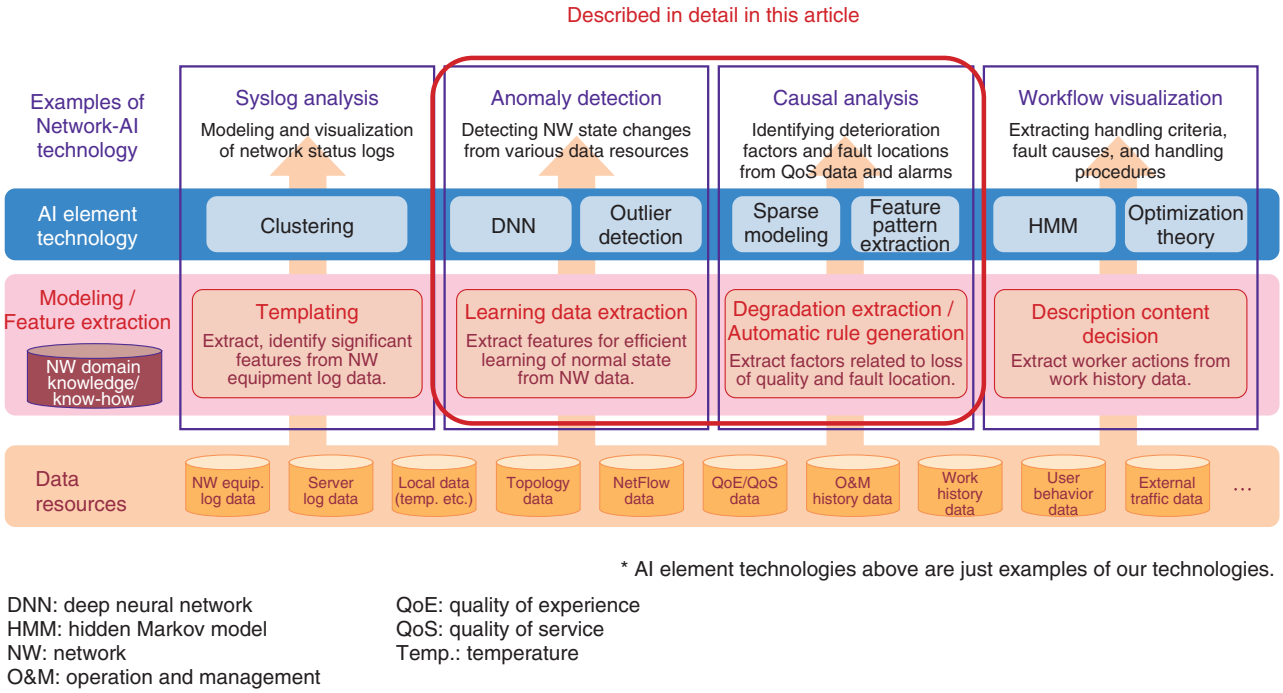


Fig. 2. Core technologies for achieving proactive controlled network.

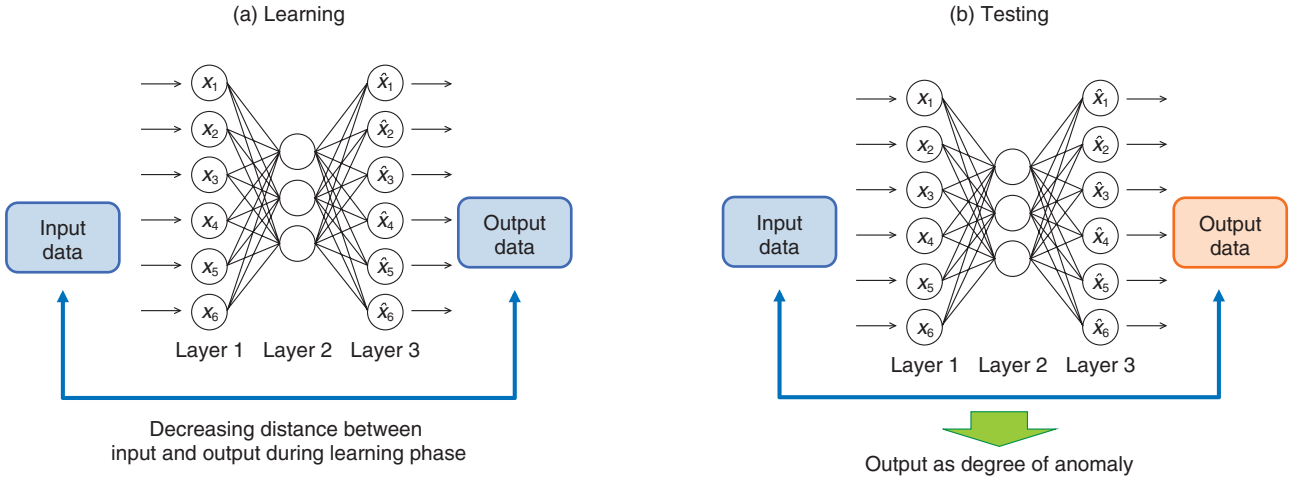


Fig. 3. AE-based anomaly detection.

dimension reduction occurs in the hidden layer by learning parameters to reconstruct the input layer data at the output layer. AE-based anomaly detection is based on the assumption that a normal data distribution is concentrated near a low-dimensional manifold in the input data space. During the learning phase shown in **Fig. 3(a)**, the normal state is learned by observing various types of data during normal operation of the network, while in the test or anomaly detection phase shown in **Fig. 3(b)**, current data are input to the AE learned as described above, and the distance between input and output layer vectors is output as the degree of anomaly. If the degree of anomaly exceeds a certain threshold, it is considered

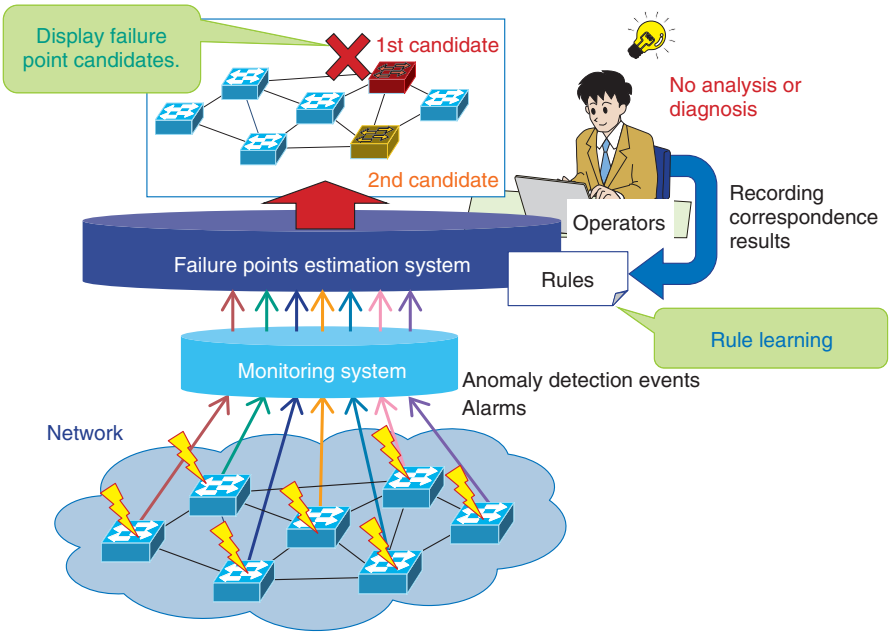


Fig. 4. Automatic failure points estimation system.

anomalous.

For our purposes, the network data that are input include numerical data such as resource/traffic data based on Simple Network Management Protocol and Management Information Base (SNMP/MIB) and flow data based on NetFlow as well as detailed text logs such as syslog data from routers and servers. To input syslog data to AE, we employ syslog analysis [5] to generate identifiers (IDs) from each syslog line, and text data are converted to numerical data based on message ID frequency analysis.

In addition to anomaly detection, efforts are also underway to identify the outlier factor when an anomaly is detected [6]. For example, if an anomaly is detected by AE, we estimate which input dimension is responsible for increasing the degree of anomaly by using a sparse-optimization technique. Calculating the contribution of each input dimension to the anomaly should make it much easier to isolate the problem after an anomaly is detected.

4. Automatic failure points estimation technology

Meanwhile, NTT Access Network Service Systems Laboratories is working on a related analytical scheme for locating network anomalies [7], as illustrated in **Fig. 4**. This system is designed to autonomously derive causal links between failure causes and alarms, or *rules*, from network information and alarms emitted by equipment that approximately locate the point of the failure. When a network anomaly is detected as described in the previous section, a detection event and proximate alarms generate a rule, which accurately predicts the points of the failure. This information is then used to send a command to circumvent the trouble and thus avoid a performance slowdown and/or commence rapid recovery of the service. Moreover, because new rules created to deal with new anomalies and failures are saved, the predictive accuracy of the system should improve over time.

5. Verification trials of network anomaly detection

We are now in the process of evaluating the network anomaly detection technology using real operational data from a testbed and actual services in collaboration with NTT operating companies. This will help us assess the effectiveness of our proposal and identify challenges that still need to be addressed. The trials now being conducted in collaboration with NTT Communications are described in this section.

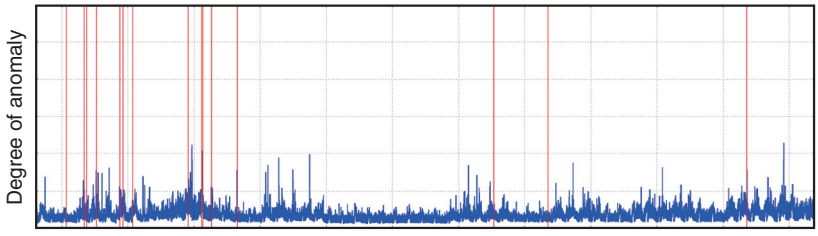


Fig. 5. Results of trial conducted with the Technology Development Department.

5.1 Collaboration with Technology Development Department

The Technology Development Department of NTT Communications operates a testbed that has been made available to NTT Communications for the development of their services. The department is also developing the Data Science Lab (DSL) on the testbed, which is a big-data analysis platform initiative to collect and analyze various types of service and infrastructure data with the idea of exploiting the data to create new service strategies and implement anomaly detection.

For this work, we evaluated the network anomaly detection technology developed by NTT Network Technology Laboratories on a range of typical operational data gathered on the DSL—SNMP/MIB, NetFlow, syslogs, trouble tickets, and the like—to assess the technology's practical performance and problems.

The basic architecture of the DSL is that of a reproducible analysis/research platform, which can reproduce analytical results and infrastructure as code. NTT Network Technology Laboratories' anomaly detection technology is currently containerized, and we are now working to integrate it on the DSL infrastructure.

In **Fig. 5**, we show anomaly data measured over a two-month time frame, with the degree of anomaly (blue line) on the vertical axis versus time on the horizontal axis. The vertical red lines indicate problems identified from trouble tickets issued during the testbed trials. The trouble tickets identify a range of problems—a server breakdown, a bug, a denial-of-service attack, and so on—and they agree remarkably well with the serious anomaly time slots shown on the graph.

However, there were other serious anomaly time slots detected with the anomaly detection technology that were not caught by the trouble tickets, so we are working to verify the effectiveness of the technology while trying to match up the detection results against actual incidents and events that occurred. In addition, there are a number of practical issues that must be resolved if we are to continually operate the anomaly detection technology on a real-time basis, and we are now addressing these issues.

5.2 Collaboration with Network Services Department

The Network Services Department of NTT Communications is currently trying to exploit AI to upgrade the service operations of a whole range of existing network services. For example, the MVNO (mobile virtual network operator) service that has attracted considerable interest and become immensely popular is a case in point, as the department seeks to exploit AI to implement anomaly detection in this service. More specifically, we have been experimenting with applying network anomaly detection to various types of resource data (utilization of central processing unit (CPU), memory, disk input/output, and so on.) on NTT Communications' virtualized service platform to see if we can detect singular events and shifts in the degree of anomaly during normal operation.

As a result, we found that it was possible to detect singular events from the degree of anomaly by AE and from the contribution of the input dimension (various kinds of time series numerical data) to the anomaly. We also observed a tendency for the anomaly degree to persist and to gradually change over longer time spans, and we were able to capture changes in system behavior manifested as changes in the degree of abnormality. In addition, we identified

the specific input dimension causing the change in behavior by calculating to what degree the AE input dimension contributes to the anomaly.

From these analyses, we recognized the need for a mechanism that tracks system configuration changes (switching between act and standby, ID changes of the CPU used, and so on) and system behavior changes (changes in CPU, memory, traffic, and other patterns). Therefore, we are developing a statistical, quantitative, and relearning technology to implement such a mechanism. We also found that the new technology is capable of visualizing a range of before-and-after system state changes by clearly showing monitoring parameter trend changes when the system is upgraded.

We learned a great deal from carrying out this assessment. Work in the months ahead will focus on practically assessing anomaly detection using greater amounts of data, enhancing our interpretive capabilities after an anomaly has been detected, further testing and assessing the technology, and making efforts to build a more user-friendly implementation of the technology suitable for business environments.

6. Future development

We presented a broad overview of some of NTT laboratories' latest initiatives in the area of Network-AI, focusing on two key technologies—network anomaly detection and automatic failure points estimation—and briefly described verification trials of the network anomaly detection technology done in collaboration with an NTT operating company.

Network-AI clearly has enormous potential, and we are committed to following through with more research and development in this area. With regard to network anomaly detection in particular, we will continue to refine and upgrade this technology, conduct further verification trials in cooperation with NTT operating companies, lay the groundwork for prototypes, and eventually implement services using the technology. Network anomaly detection still faces a number of hurdles before it is ready for actual deployment. Most notably, we must improve our ability to interpret the factors involved when an anomaly is detected, and we must adapt the technology for use in different environments. Needless to say, we are hard at work in resolving these issues.

References

[1] S. Harada, K. Watanabe, Y. Nakano, Y. Ikeda, Y. Matsuo, M. Kobayashi, A. Suzuki, and R. Kawahara, "An Introduction of Efforts to Realize Proactive Network Control," Proc. of the 2017 IEICE General Conference, B-7-32, Nagoya, Aichi, Japan, Mar. 2017 (in Japanese).

[2] Y. Nakano, Y. Ikeda, K. Watanabe, K. Ishibashi, and R. Kawahara, "Autoencoder Based Detection Method for Network Anomalies," Proc. of the 2017 IEICE General Conference, B-7-33, Nagoya, Aichi, Japan, Mar. 2017 (in Japanese).

[3] Y. Ikeda, Y. Nakano, K. Watanabe, K. Ishibashi, and R. Kawahara, "A Study of Accuracy Improvement on Network Anomaly Detection with Autoencoder," Proc. of the 2017 IEICE General Conference, B-7-34, Nagoya, Aichi, Japan, Mar. 2017 (in Japanese).

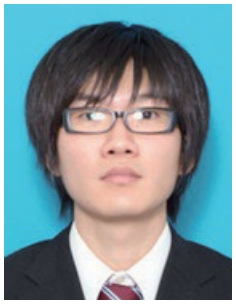
[4] R. Kawahara, "Application of AI/Machine Learning to Enhance Network Operation/Control Technologies," Proc. of the 2017 IEICE Society Conference, BT-2-1, Tokyo, Japan, Sept. 2017 (in Japanese).

[5] T. Kimura, A. Watanabe, T. Toyono, and K. Ishibashi, "Proactive Failure Detection Learning Generation Patterns of Large-scale Network Logs," Proc. of the 11th International Conference on Network and Service Management (CNSM 2015), Barcelona, Spain, Nov. 2015.

[6] Y. Ikeda, K. Ishibashi, Y. Nakano, K. Watanabe, and R. Kawahara, "Inferring Causal Parameters of Anomalies Detected by Autoencoder Using Sparse Optimization," IEICE Technical Report, Vol. 117, No. 89, pp. 61–66, 2017 (in Japanese).

[7] K. Itoi, T. Yakawa, H. Oishi, and K. Okazaki, "Automatic Failure Points Estimation Technology for Generating Knowledge and Rapid Recovering Operations," NTT Technical Journal, Vol. 29, No. 5, pp. 60–64, 2017 (in Japanese).

Keishiro Watanabe
Senior Research Engineer, Traffic Engineering Group, Communication Traffic & Service Quality Project, NTT Network Technology Laboratories.
He received a B.E. and M.E. in satellite communications from Kyushu University in 2002 and 2004. After joining NTT, he conducted research on network management and QoE issues. He was with NTT Communications from 2012 to 2015. He is now working on the development of sophisticated operations of network systems by using AI. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).



Yasuhiro Ikeda
Researcher, Traffic Engineering Group, Communication Traffic & Service Quality Project, NTT Network Technology Laboratories.
He received a B.E. in applied physics and physico-informatics and an M.E. in applied physics from Keio University, Tokyo, in 2008 and 2010. Since joining NTT in 2010, he has been researching traffic analysis techniques for telecommunication networks. He received the IEICE Information Network Research Award in 2012. He is a member of IEICE.

Yuusuke Nakano
Research Engineer, Traffic Engineering Group, Communication Traffic & Service Quality Project, NTT Network Technology Laboratories.
He received an M.E. in system engineering from Wakayama University in 2005 and a Ph.D. in information science and technology from Osaka University in 2011. He joined NTT Network Service Systems Laboratories in 2005. He is currently with NTT Network Technology Laboratories. His research interests include network anomaly detection and web performance measurement and acceleration. He is a member of IEICE and the Information Processing Society of Japan.

Keisuke Ishibashi
Senior Research Engineer, Supervisor, NTT Network Technology Laboratories.
He received a B.S. and M.S. in mathematics from Tohoku University, Miyagi, in 1993 and 1995 and a Ph.D. in information science and technology from the University of Tokyo in 2005. Since joining NTT in 1995, he has been engaged in research on traffic issues in computer communication networks. He received the Information Network Research Award in 2002. Since 2017, he has also been a visiting professor at Osaka University. He is a member of the Institute of Electrical and Electronics Engineers (IEEE), IEICE, and the Operations Research Society of Japan (ORSJ).

Ryoichi Kawahara
Senior Research Engineer, Supervisor, Group Leader, Traffic Engineering Group, Communication Traffic & Service Quality Project, NTT Network Technology Laboratories*.
He received an M.E. in automatic control and a Ph.D. in telecommunication engineering from Waseda University, Tokyo, in 1992 and 2001. Since joining NTT in 1992, he has been conducting research on traffic control for telecommunication networks, traffic measurement and analysis for Internet protocol networks, and network management. He received the Telecom System Technology Award from the Telecommunications Advancement Foundation in 2010, and Best Paper Awards from IEICE in 2003 and 2009. He is a member of IEICE, IEEE, and ORSJ.
*He left NTT at the end of March 2018.

Satoshi Suzuki
Senior Research Engineer, Access Network Operation Project, NTT Access Network Service Systems Laboratories.
He received an M.E. in global environmental engineering from Kyoto University in 1995. Since joining NTT in 1995, he has mainly been researching and developing network operation support systems in access and wide area Ethernet networks. He is a member of IEICE.