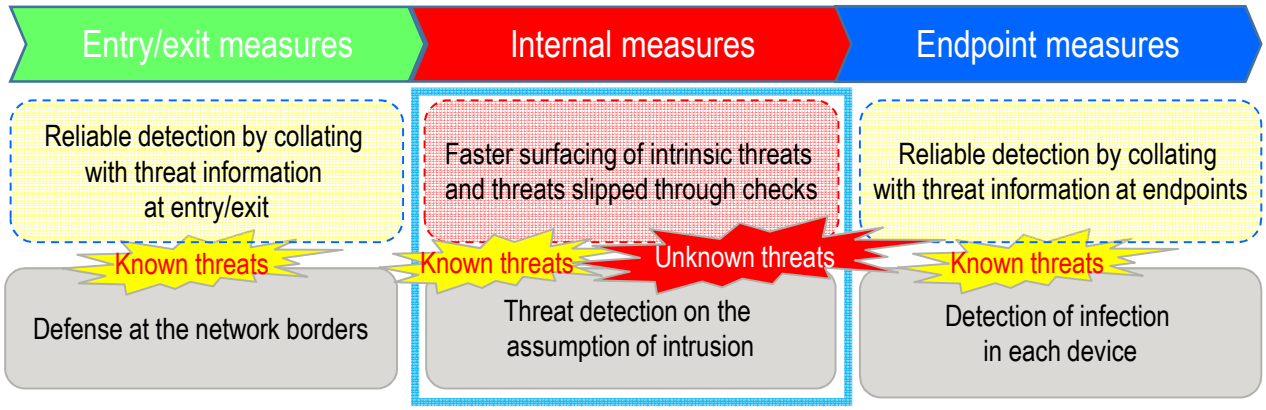
1-2 Minimize Impact on Businesses by Revealing Intrinsic Threats in Early Stages

Operation monitoring and analysis technologies

Support highly skilled operations that reveal, in early stages, intrinsic threats slipped through the existing security measures and monitor and analyze such threats.

Technology used for measures internally taken to complement (defense in depth) the measures against threats at entry and exit points

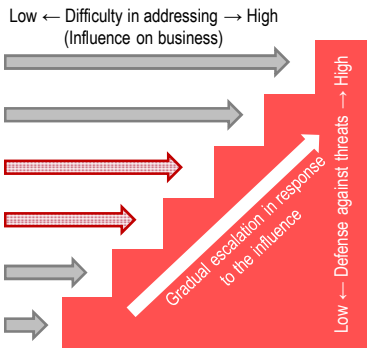
Defense in depth technology used for making intrinsic threats that have slipped through the entry/exit and endpoint measures surface faster in order to capture such threats before the threat level is escalated



Support highly skilled operation that monitors and analyzes threats

Along with the increase in intrinsic unknown threats, highly skilled operation in Level-2/3 has increased. Support is systematically provided for Level-1 engineers to be able to perform Level-2/3 operations.

Threat Detection Level (definition)		Decision-maker for Measures	Perspective of Measures
Level-5	Detection of abnormalities in operation services	Responsible person Manager	Business continuity (BCP)
Level-4	Detection of inhibition of the health of the overall operation system	Risk committee (CISO)	Soundness of the system
Level-3	Detection of abnormal diffusion (deep intrusion) in internal networks (ex. measures of C&C)	CSIRT	Stability of the system
Level-2	Detection of abnormal communication (C&C server communication) with external networks (ex. existence of C&C, information leakage)	Security expert (SOC)	Identification of influence area
Level-1	Detection of changes in communications within internal networks (ex. Possibility and target area of C&C communication)	Network operator (NOC)	Identification/removal of damage
Level-0	Notification of security threats from external networks (ex. occurrence of attacks)	Tools (devices)	Identification/removal of damage



Difference from the existing technologies

Application of mathematical models that do not require prior learning in a large-scale network

Technical Factors	Existing Technologies	Technologies for the Research Theme
Detection method	Difference from past behaviors	Difference from behaviors of other devices
Detection model	Machine learning (prior learning required)	Mathematical models (prior learning not required)
Applicable network	Small to large scale	Large scale
Communications to be monitored	Monitoring for each network	Support for different devices mixed: from old to virtualization devices

Cross-ministerial Strategic Innovation Promotion Program (SIP)

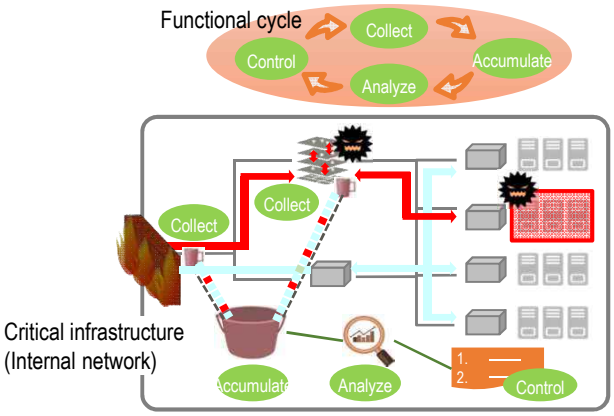
Fujitsu

1-2 Minimize Impact on Businesses by Revealing Intrinsic Threats in Early Stages

Operation monitoring and analysis technologies

Support highly skilled operations that reveal, in the early stages, intrinsic threats that slipped through the existing security measures and monitor and analyze such threats.

Functional Cycle and Deployment of Internal Measures



Technical key pointes

In a large-scale network where physical and virtual devices coexist, a four-function cycle (collection, accumulation, analysis, control) has been achieved.

(i) TAP collection technology of high-speed capturing at 10 Gbps from a virtual network

(ii) Technology of high-speed and large capacity accumulation technology at 100 Gbps

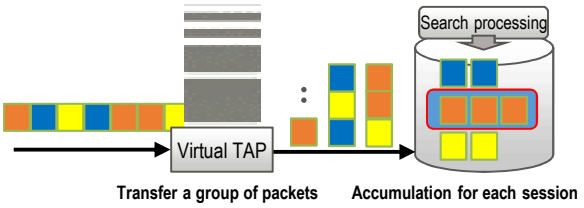
(iii) Analysis technology using mathematical models that do not require prior leaning

(iv) Control technology supporting highly skilled operation for measures against threats

Technology of High-speed Capturing and Accumulation of Communication from Virtual Networks

Collect Accumulate

- Add-on technology to a virtual switch can capture high-speed packets and transfer multiple packets that are grouped together, preventing congestion at virtual switches.
- High-speed access is achieved by reading/writing of disks on a session basis.



Analysis Technology Detecting Suspicious Communication in Normal Communication

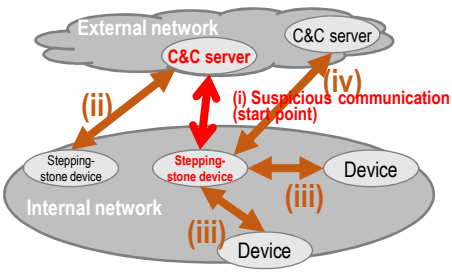
analyze

- By focusing on the regularity of communication (right figure), the types and transfer operations of communication destinations are indexed for more reliably differentiating normal from abnormal communications.
- With a unique threshold adjustment method (patent pending), both increase in immediacy and decrease in accuracy deterioration have been achieved.
- Suspicious communication, which was overlooked by the existing security technologies, has been successfully identified. (Press released on November 29, 2019, by NEDO. Fujitsu, and NII)

Automatic Extraction of Influence Investigation Range by System

Control

- Communications related to suspicious communications are analyzed and made visible by the system to determine the range of investigation of the damage by threats to reduce operators' investigation operation.



i. Detected suspicious communication (primary threat)
ii. Communication with the C&C server (secondary threat)
iii. Communication with the stepping-stone device server (secondary threat)
iv. Communication with the SBY C&C server (secondary threat)

Product Roll Out Plan

Product commercialization: collection/accumulation technology in FY2019; analysis/control technology in FY2020

Contact: Network Solution Division 044-280-9861 fj-ci-procontact@dl.jp.fujitsu.com