


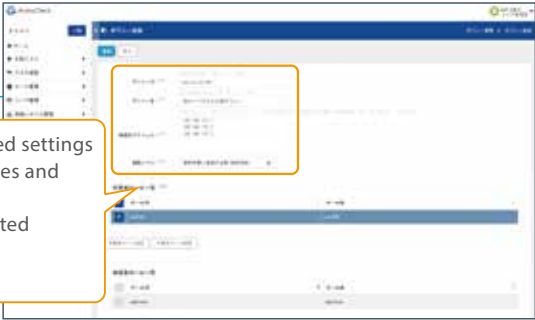
Image of how SecureCube / Access Check is used

Work request screen



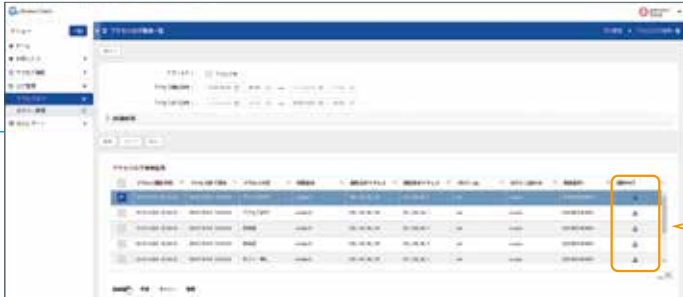
Setting regular access and planned access periods

Policy setting and editing screen



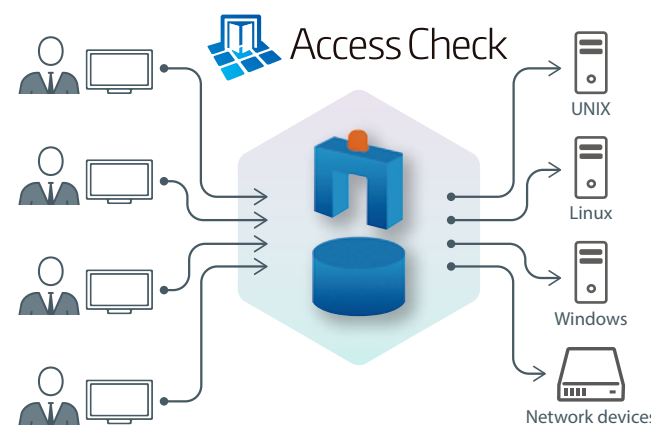
Configuring detailed settings such as policy names and contents, connection-permitted IP addresses, and approval level

Acquired log list and search screen



Operation logs can be downloaded from here

SecureCube / Access Check product configuration and operating environment



Access Check

Supported OS	Red Hat Enterprise Linux Server 7 (7.5 or later) • Installation and configuration of the middleware included in the package (MariaDB, OpenLDAP, etc.) is required.
Hardware Minimum configuration	Hardware or virtual environment infrastructure that can run the above OS CPU: 2.5 GHz × 8 cores or more (x86_64) Memory: Minimum 16 GB HDD: Minimum 500 GB Network: Minimum 1 network interfaces * Depending on the log saving requirements, larger device capacity may be necessary.
Supported languages	Japanese, English
Managed protocols	TELNET, SSH, FTP, SFTP, SCP, RDP, HTTP(S), CIFS, Oracle SQL *Plus, other TCP

Links with external systems are possible.

SecureCube / Access Check can be easily linked with external systems by using API. It can operate in combination with an active directory, a workflow system, advanced authentication system, integrated log management system, or other system from another company. This prevents the tools that are currently installed and operating from going to waste, and allows the construction of an environment that suits actual needs. It also offers multi-tenant support that provides multiple services using a single control infrastructure.

Contact regarding products and services


+81-3-6706-0500
info@nri-secure.co.jp

Available hours: 9:00 – 17:00 (JST) Mon – Fri
(excepting Japanese holidays and days when the company is closed)

NRI SecureTechnologies, Ltd.

Tokyo Sankei Building, 1-7-2 Ote-machi, Chiyoda-ku, Tokyo 100-0004, Japan
www.nri-secure.co.jp

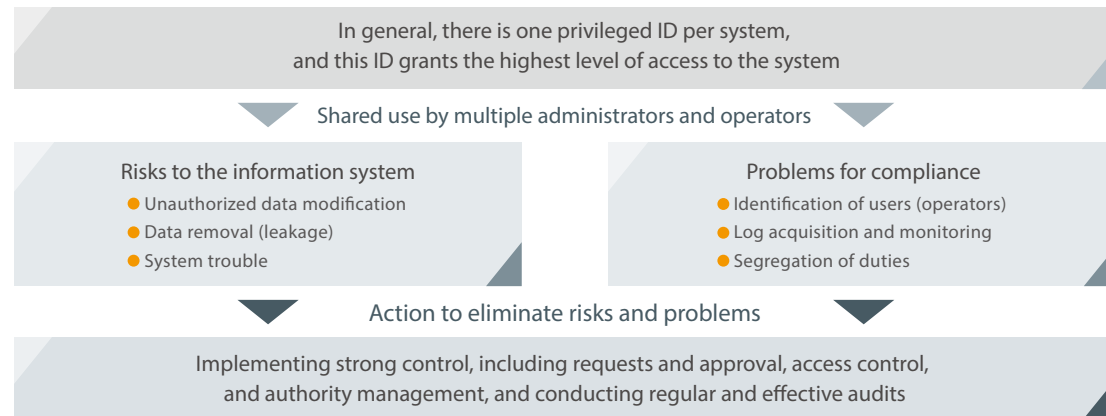
* NRI, NRI SecureTechnologies, and SecureCube are trademarks or registered trademarks of Nomura Research Institute, Ltd.
 * Company names, product names, logo marks, and other items printed in the catalog are trademarks or registered trademarks of the corresponding companies in Japan and other countries.
 * The information in this catalog is subject to change without notice.
 © 2018 NRI SecureTechnologies, Ltd. All rights reserved.

An all-in-one solution for privileged ID access control, delivering robust access control that protects information systems

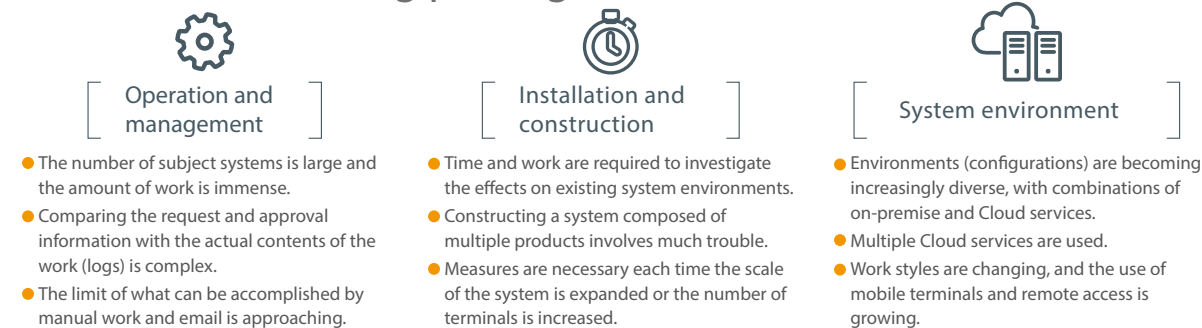


What is privileged ID control?

Correctly controlling and operating the privileged IDs that have the highest authority in an information system is essential for maintaining and strengthening compliance, as well as for reducing risk to the information system. It is necessary to construct a process flow for privileged ID management and operation, and to establish a strong audit system, not only in order to comply with various audits and standards (J-SOX, SAS70, PCIDSS, FISC, etc.), but also to prevent accidental or deliberate data leakage, unauthorized data modification, and other illicit acts.



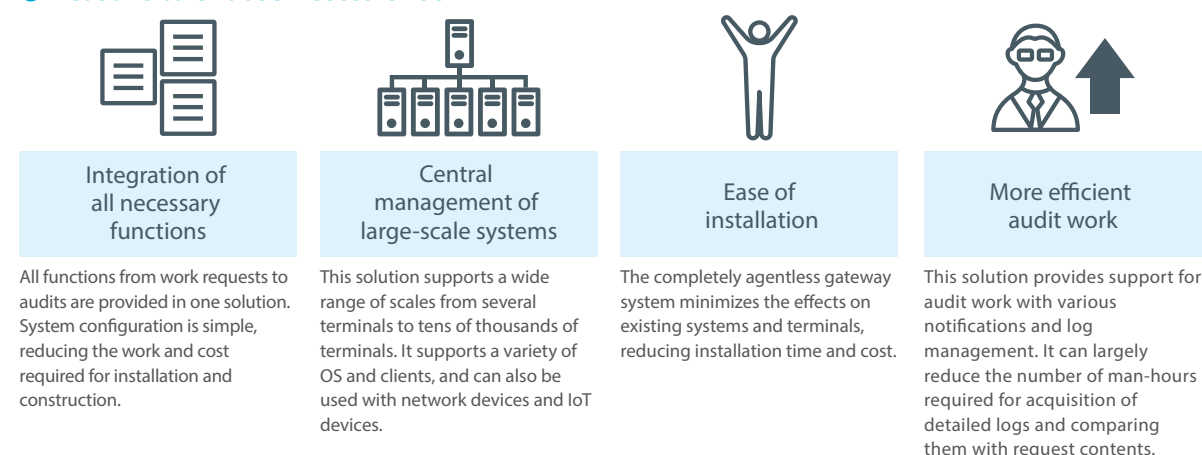
Issues with achieving privileged ID control



Resolving privileged ID control issues with Access Check

SecureCube / Access Check is a gateway-type privileged ID access control solution provided by NRI Secure, a company with in-depth frontline knowledge of IT management and system operations. This solution has been adopted by customers in a wide range of fields including financial institutions, the retail industry, and the manufacturing industry. It has been highly rated both for the fine-tuned maintenance and support system that is only possible with in-house development, and for the functional expansions that incorporate specific customer needs.

Reasons to choose Access Check

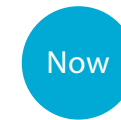


Best Solution for Privileged ID Access Control SecureCube / Access Check

Privileged ID access control market share in Japan **No.1***



- Procedures and tools for requests and approval varied widely.
- An immense amount of time and work was required for issuing work IDs.
- Regular password changes were a large burden and troublesome.



Unnecessary work is eliminated, reducing workloads.

With SecureCube / Access Check, the process from request to approval is systemized, allowing anybody to complete the procedures by using the designated documents and processes. The system supports post-fact approval, multi-stage approval, and regular password changes, greatly reducing the workload on the responsible staff.

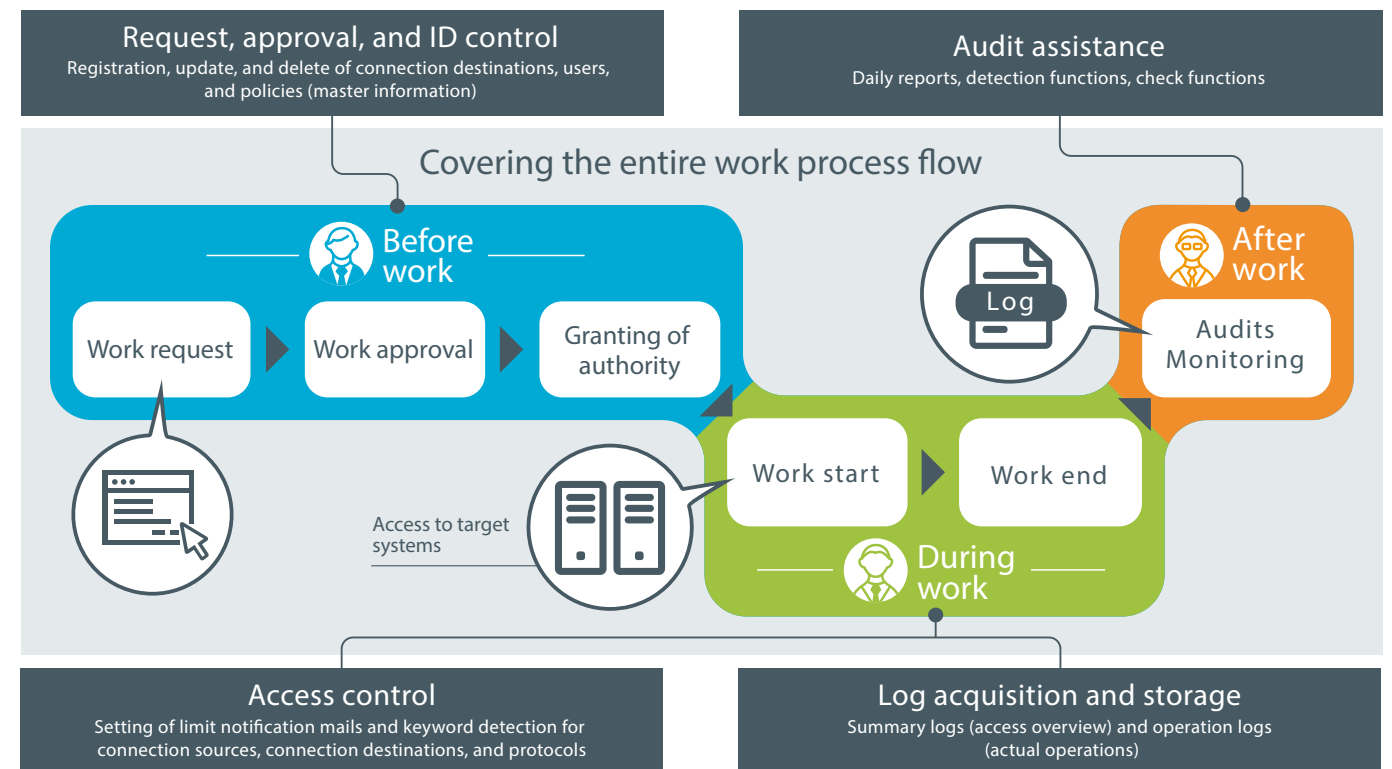


- Request information and operations logs were stored separately.
- It was not possible to immediately find the necessary logs.
- An immense amount of time and work was required for comparing the requests and logs.

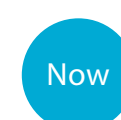


More efficient and labor-saving audit work

Because SecureCube / Access Check centrally manages work request information and access/operation logs, it is possible to easily compare them to one another, and to find the necessary logs immediately. Functions that support audit work, such as tabulating numbers from daily reports, are also available.



- It was possible to connect to systems from disallowed network systems.
- There was no way to know if prohibited commands were used.

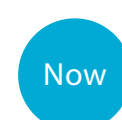


Eliminate unauthorized acts in information systems.

SecureCube / Access Check acts as a gateway and authenticates users, providing robust access control in accordance with the request contents and policy. Communications can be cut off in real time when a command (keyword) which was designated in advance is detected during work.



- It was not possible to acquire detailed logs that could be used in audits.
- There were limits to acquisition of OS and protocol logs.



Recording every operation in all kinds of environments

SecureCube / Access Check can acquire logs of all operations regardless of the OS or protocol. The acquired logs can be viewed only by the administrators identified by the policy, making them effective for monitoring of internal audits and verifying internal controls.

* Sources:
ITR : ITR Market View: Identity/Access Control Market 2018, Privileged ID control market: Sales share by vendor (FY 2017)
MIC Research Institute : Current State and Future Prospects of the Identity Authentication and Access Control Security Solutions Market FY 2018 Edition, Privileged ID control