

富士通UNIXサーバー「SPARC M12」に対する 特権ID管理ソリューション「SecureCube Access Check」 の動作検証

2024年03月28日

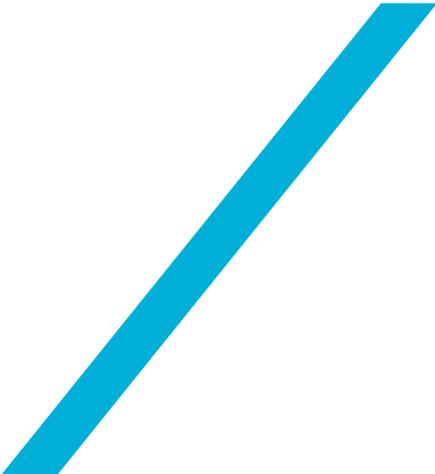
NRIセキュアテクノロジーズ株式会社

検証目的と結果

検証環境と検証内容

検証結果詳細

お問い合わせ先



検証目的と結果

検証目的

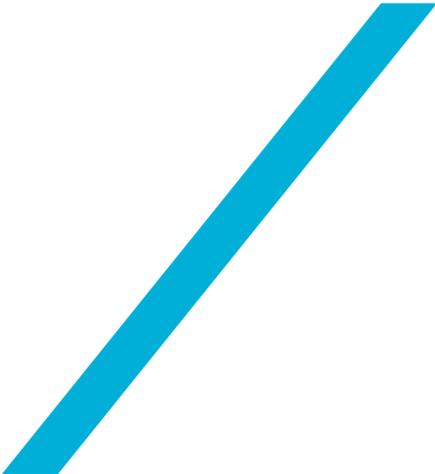
PRIMERGY機にインストールした「SecureCube Access Check」（以下Access Check）を利用し、SPARC M12機にインストールされたOracle Solaris OSへSSH接続の中継が行えることを検証する。

検証はFUJITSU Platform Solution Labにて富士通株式会社より貸与いただいた環境を用いて実施した。

検証結果

Access Checkを利用したSolaris 10 / Solaris 11へのSSH接続は問題なく行える

- Access Checkを利用したSSH接続で以下のバージョンのSolaris OSを操作することが可能
 - Solaris 10 1/13
 - Solaris 11.3
- 事前に認証情報をAccess Checkに登録することで、Solarisへの自動ログインが可能
- 操作内容に関して、崩れることなく正確に記録することが出来ている

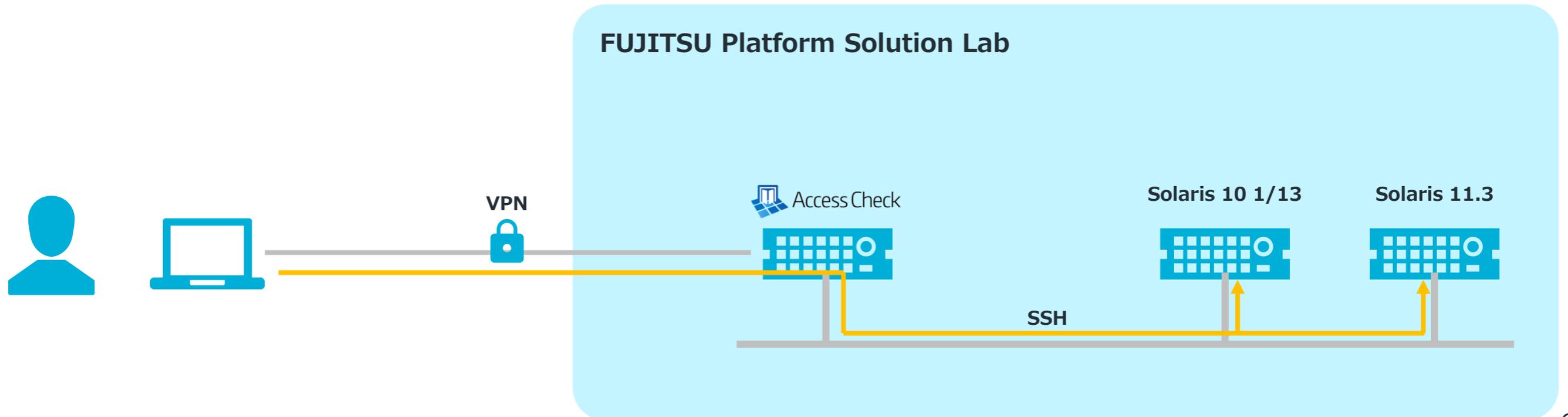


検証環境と検証内容

検証環境（概要）

環境

- ／ FUJITSU Platform Solution Lab上に環境を構築
 - ／ PRIMERGY機 1台（RHEL 8.6）
 - ／ SPARC機 2台（Solaris 10 1/13, Solaris 11.3）
- ／ 操作端末はVPN経由でFUJITSU Platform Solution Labへアクセスを行う



検証環境構成

Access Check用サーバ		Solaris 10用サーバ		Solaris 11用サーバ	
PRIMERGY RX2540 M6		SPARC M12-1		SPARC M12-1	
CPU	Xeon Gold 6346 3.1Ghz x 2	CPU	SPARC64 XII 3.2Ghz	CPU	SPARC64 XII 3.2Ghz
メモリ	64GB	メモリ	128GB	メモリ	128GB
ストレージ	HDD 900GB x 2	ストレージ	HDD 600GB x 2	ストレージ	HDD 600GB x 2
OS	Red Hat Enterprise Linux 8.6	OS	Solaris 10 1/13	OS	Solaris 11.3

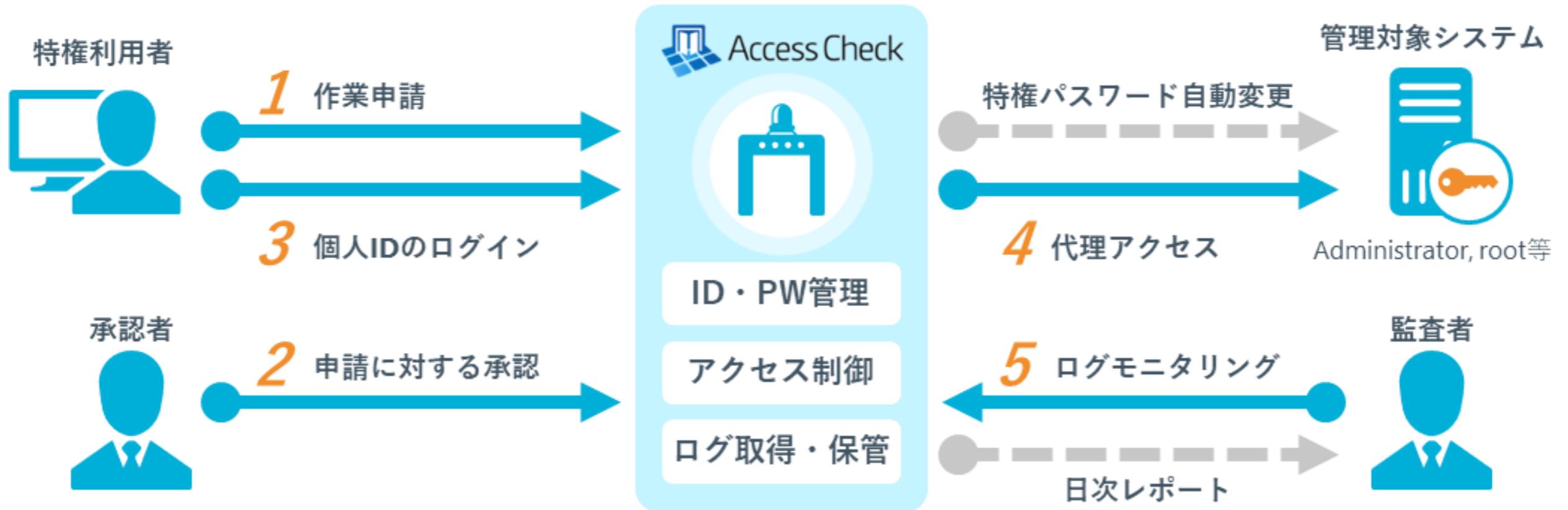
検証内容

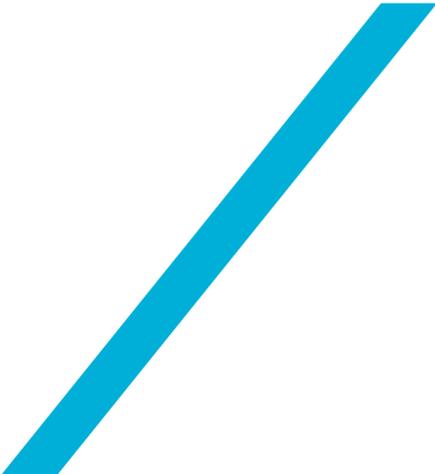
Access Checkを経由したSSH接続を行い、以下観点で正常動作することを確認

- SSHを利用した中継の疎通
- 接続先Solarisへの認証
- パスワード秘匿機能を利用した自動ログイン
- 中継時にSolaris上での任意コマンドの実行
- キーワード検知機能の利用
- アクセスログ、操作ログの取得
- アクセスログのダウンロード
- 操作ログのダウンロード

SecureCube Access Checkとは

- ／ NRIセキュアが提供するゲートウェイ型の特権ID管理ソリューション
- ／ 特権ID管理に必要な機能をオールインワンで提供





検証結果詳細

Access Checkを経由したSolaris 10へのログイン

```
10.40.6.13 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
rx2540m6-013 SSH-GW
#####
#
# This is SecureCube Access Check SSH-GW
# Your whole access is logged and checked!
#
#####
SSHGW PROXY rx2540m6-013. Enter HOST:PORT (Default:22)
CONNECT -> 10.40.6.12

Username: guest
This access will not login automatically. please enter the password.
guest@10.40.6.12's password:
Last login: Thu Jan 25 11:18:29 2024 from 10.40.6.13
Oracle Corporation      SunOS 5.10      Generic Patch   January 2005
m12-1-04% cat /etc/release
                Oracle Solaris 10 1/13 s10s_u11wos_24a SPARC
    Copyright (c) 1983, 2013, Oracle and/or its affiliates. All rights reserved.
                Assembled 17 January 2013
m12-1-04%
```

Access Checkを経由したSolaris 11へのログイン

```
10.40.6.13 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
rx2540m6-013 SSH-GW
#####
#
# This is SecureCube Access Check SSH-GW
# Your whole access is logged and checked!
#
#####
SSHGW PROXY rx2540m6-013. Enter HOST:PORT (Default:22)
CONNECT -> 10.40.6.11

Username: guest
This access will not login automatically. please enter the password.
guest@10.40.6.11's password:
Last login: Thu Jan 25 11:05:28 2024 from 172.21.10.48
Oracle Corporation      SunOS 5.11      11.3    February 2019
guest@m12-1-03:~$ cat /etc/release
                                Oracle Solaris 11.3 SPARC
                                Copyright (c) 1983, 2018, Oracle and/or its affiliates. All rights reserved.
                                Assembled 09 May 2018
guest@m12-1-03:~$
```


キーワード検知機能

```
Tera Term - [未接続] VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
CONNECT -> 10.40.6.12
Username: guest
guest@10.40.6.12's password:
Last login: Thu Jan 25 11:35:05 2024 from 172.21.10.48
Oracle Corporation      SunOS 5.10      Generic Patch   January 2005
m12-1-04% su -
パスワード:
Oracle Corporation      SunOS 5.10      Generic Patch   January 2005
You have new mail.
# cat test.txt
cat: test.txt をオープンできません。
# cat /export/home/guest/test.txt
test
# cat test.txt
cat: test.txt をオープンできません。
# cat /export/home/guest/test.txt
070-2482-8160
test
# exit
m12-1-04% exit
m12-1-04% ログアウト
Connection to 10.40.6.12 closed.
```

```
ssh.acui001.s001.2024.01.25.035223004.74535.22.in.txt - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

【登録されているキーワード】 (いずれかのキーワードを含む)
1. su -

【キーワードを含むレコード】
13:m12-1-04% su -

Last login: Thu Jan 25 11:35:05 2024 from 172.21.10.48
Oracle Corporation      SunOS 5.10      Generic Patch   January 2005
m12-1-04% su -
パスワード:
Oracle Corporation      SunOS 5.10      Generic Patch   January 2005
You have new mail.
# cat test.txt
cat: test.txt をオープンできません。
# cat /export/home/guest/test.txt
070-2482-8160
test
# exit
m12-1-04% exit
m12-1-04% ログアウト
Connection to 10.40.6.12 closed.

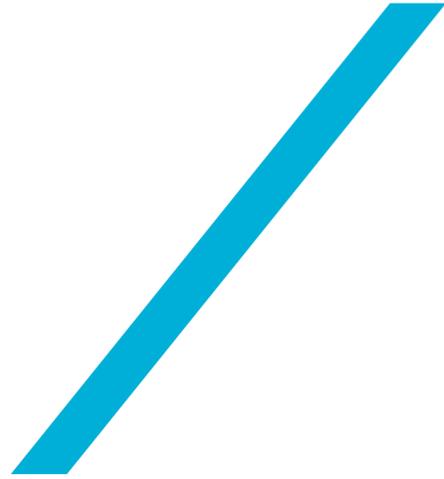
22行、5列 120% Windows (CRLF) UTF-8
```

アクセスログの確認

The screenshot displays the 'Access Check' web application interface. The top navigation bar includes the title 'Access Check' and a user profile dropdown for '監査者1[監査者]'. The left sidebar contains a menu with options: 'ホーム', 'お気に入り', 'アクセス確認', '一覧・検索', 'パスワード払出確認', 'ログ管理', and '日報レポート'. The main content area is titled 'アクセス申請検索一覧' and features a search bar with '操作' and '検索' buttons. Below the search bar is a 'フィルタ' dropdown menu. The primary data table lists access requests with columns for '申請番号', 'ポリシー名', '申請状態', '件名', '申請者名', and '利用者ID'. Two rows are visible: one with status '承認待ち' and another with status '作業完了' (highlighted with a blue selection bar). Below this table, there are tabs for '詳細', 'ポリシー', '関連ログ', and '履歴'. The '関連ログ' tab is active, showing a table titled 'アクセスログ検索結果'. This table has columns for 'アクセス開始日時', 'アクセス終了日時', 'アクセス可否', '利用者ID', '接続元IPアドレス', '接続先アドレス', 'プロトコル', 'ログイン試行ID', '申請番号1', and '操作ログ'. Four rows of access logs are listed, all with 'アクセス許可' status, and each row includes a download icon for the '操作ログ'.

申請番号	ポリシー名	申請状態	件名	申請者名	利用者ID
20240125A00001	ポリシー-1	承認待ち	Solaris接続検証	作業者1	
20240125A00000	ポリシー-1	作業完了	Solaris接続検証	作業者1	

アクセス開始日時	アクセス終了日時	アクセス可否	利用者ID	接続元IPアドレス	接続先アドレス	プロトコル	ログイン試行ID	申請番号1	操作ログ
2024/01/25 10:46:38	2024/01/25 10:47:04	アクセス許可	worker001	172.21.10.48	10.40.6.12	ssh	guest	20240125A00000	📄
2024/01/25 10:48:17	2024/01/25 11:11:00	アクセス許可	worker001	172.21.10.48	10.40.6.12	ssh	guest	20240125A00000	📄
2024/01/25 10:50:31	2024/01/25 11:11:12	アクセス許可	worker001	172.21.10.48	10.40.6.11	ssh	guest	20240125A00000	📄
2024/01/25 11:16:55	2024/01/25 11:17:10	アクセス許可	worker001	172.21.10.48	10.40.6.12	ssh	guest000	20240125A00000	📄



お問い合わせ先

お問い合わせはこちらから

お問い合わせ先

info@nri-secure.co.jp

NRIセキュアテクノロジーズ
Access Check営業担当

弊社Webサイトでも情報を公開しております

URL : <https://www.nri-secure.co.jp/service/solution/accesscheck>