PCIDSSセキュリティフォーラム2013

カード会員データへの
アクセス制御・ログ管理を短期・安価に実現

～SecureCube / Access Check のご紹介～

NRIセキュアテクノロジーズ株式会社

2013年 7月 10日（水）

NRIセキュアテクノロジーズ株式会社
セキュリティソフトウェア営業部
齋藤　真理子

目次

NRIセキュアテクノロジーズ株式会社

野村総合研究所グループにおける情報セキュリティ専門の中核企業

- 本社所在地：東京都港区東新橋１-５-２ 汐留シティセンター
- 代表取締役社長：増谷 洋
- 設立　：２０００年８月１日（サービス提供は１９９５年開始）
- 資本金：４．５億円


東京（本社）


横浜（テクニカルセンター）

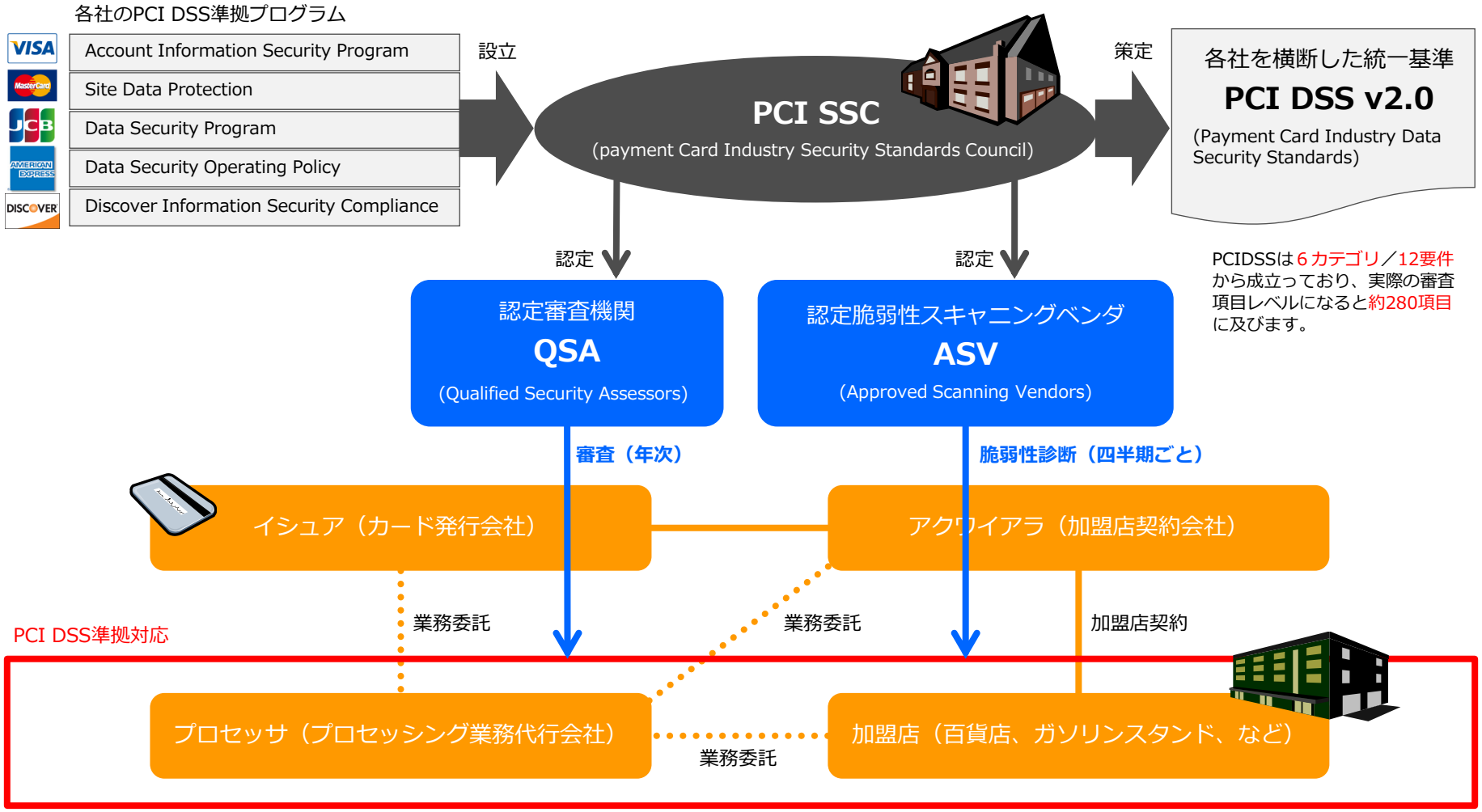
- 拠点：
  - 東京 （本社）
  - 横浜 （テクニカルセンター）
  - Irvine, CA （北米支店）
  - 北京・上海 （NRI北京）
- 社員数（連結）：249名　（単独）：225名
- 資格取得者数
  - 高度情報処理技術者 ： のべ324名
  - GIAC(Global Information Assurance Certification) ： のべ92名
  - CISA(Certified Information System Auditor) ： 56名
  - CISM(Certified Information Security Manager) ： 31名
  - CISSP(Certified Information Systems Security Professionals) ： 32名
- ISO/IEC 27001認証取得

- サービス提供実績
  - 官公庁、金融、流通、製造、製薬、 通信、マスコミ　等500社以上に運用サービスを提供
  - 一次的なスポットサービスを含めると2000社以上にサービス提供

（２０１３年６月１日現在）

（ご確認）PCIDSSとは

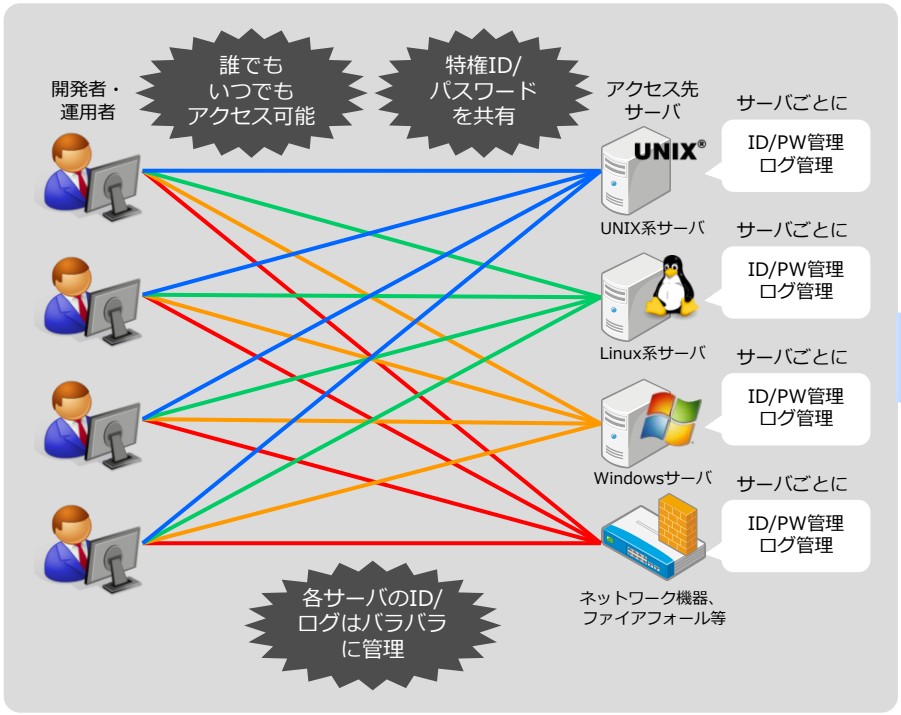
- PCIDSSとは、クレジットカード情報の漏洩を防止するために策定された、クレジットカード業界におけるグローバルなセキュリティ基準です。



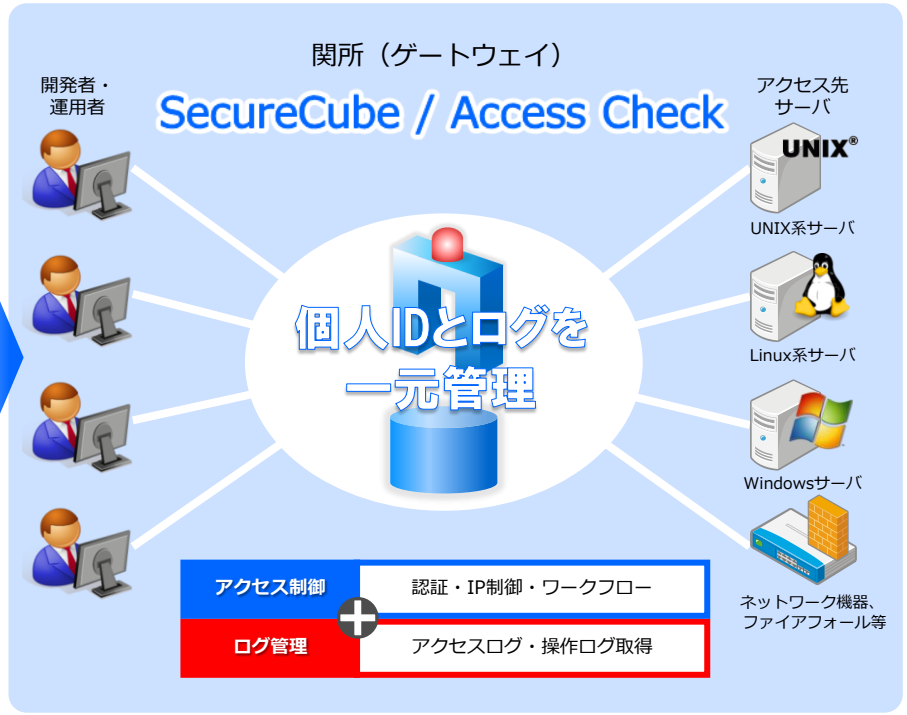
SecureCube / Access Checkの概要

- SecureCube / Access Checkは、既存の本番環境に影響を与えないゲートウェイ型（完全エージェントレス型）のアクセス管理ソリューションです。
- 本番環境の入口に関所（ゲートウェイ）として設置し、個人IDとログを一元管理します。
- 関所（ゲートウェイ）上で、利用者ごとのアクセス制御が可能です。

特権ID管理の現状と課題

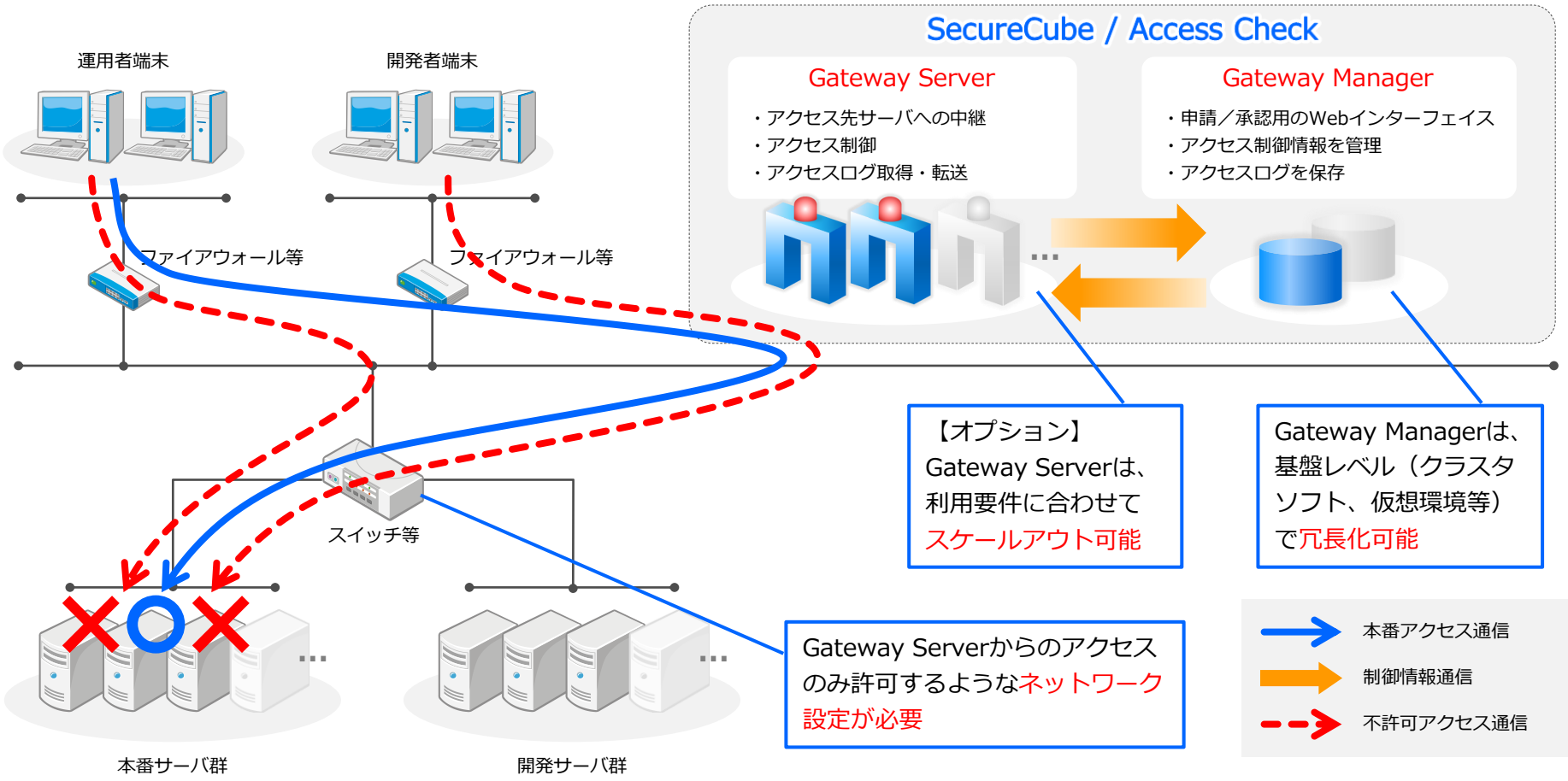


SecureCube / Access Checkで解決!



大規模システムにも対応可能なシステム構成

- SecureCube / Access Checkは、アクセス制御を行うための各種制御情報やアクセスログを管理するGateway Managerと、踏み台として中継機能を担うGateway Server（複数可）から構成されます。
- Gateway Mangerは、アクセス申請・承認や各種設定を行うWebインターフェイスを備えています。



SecureCube / Access Checkの特長

- SecureCube / Access Checkは、システム開発・運用の現場を知り尽くしたNRIグループから生まれた、実績豊富な特権ID管理（アクセス管理）における ベストプラクティスソリューション です。

大手金融機関をはじめとする**１７０社以上の導入実績**！

多くのお客様で J-SOX や PCI DSS といった**法令・基準の監査をクリア**！

エージェントレスのため、**本番サーバに影響を与えずに短期導入が可能**！（最短１ヶ月の実績あり）

アクセス申請からログ監査までを一元管理することで業務効率がアップ！（とくにログ監査業務）

ネットワーク制御、権限最小化、特権パスワード管理による**強固なアクセス制御**を実現！

シンプルなシステム構成で、OS/HW/MWなどの基盤コストも含めた**トータルコストを抑制**！

数台から数千台まで管理対象サーバをカバーできる**システム拡張性の高さ**！

SecureCube / Access Checkの機能

PCIDSS要件に対応する機能

- おもに要件7・8・10の対応として、SecureCube / Access Checkの導入を検討いただいています。

PCI DSS要件			SecureCube /Access Check対応機能	
1. 安全なネットワークの構築と維持	要件1	カード会員データを保護するために、ファイアウォールをインストールして構成を維持する		
	要件2	システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない		
2. カード会員データの保護	要件3	保存されるカード会員データを保護すること	3.4	取得した操作ログの暗号化保存機能を実装。
	要件4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	4.1	主要な暗号化通信（SSH, SCP, SFTP, HTTPS）へ対応。
3. 脆弱性管理プログラムの整備	要件5	アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新する		
	要件6	安全性の高いシステムとアプリケーションを開発し、保守する	6.4.1 6.4.2	開発環境・本番環境それぞれのアクセス制御を設定可能。 責務分掌のための、アクセス申請・承認機能を実装。
4. 強固なアクセス制御手法の導入	要件7	カード会員データへのアクセスを、業務上必要な範囲内に制限する	7.1, 7.2	個人に紐づいた接続元IPアドレスレベルでのアクセス制御、およびアクセス申請・承認機能によるアクセス制御を実装
	要件8	コンピュータにアクセスできる各ユーザに一意のIDを割り当てる	8.1-8.5	Access Check上での一元的なユーザ認証機能、およびユーザ管理機能（パスワードポリシー、有効期限、アカウントロックなど）を実装。
	要件9	カード会員データへの物理アクセスを制限する		
5. ネットワークの定期的な監視およびテスト	要件10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	10.1-10.7	リモートからのサーバアクセス全般に対して、ログ取得、改ざん防止、ログ管理（閲覧範囲の制限）などの機能を実装。
	要件11	セキュリティシステムおよびプロセスを定期的にテストする		
6. 情報セキュリティポリシーの整備	要件12	すべての担当者の情報セキュリティポリシーを整備する		

※ 実際の要件への準拠は各社の環境によるため、QSAによる判断が必要となります。

SecureCube / Access Checkのおもな機能

- SecureCube / Access Checkは、おもに下記の機能を備えています。
- それぞれの機能の詳細について、次頁以降で説明します。

1 SecureCube / Access Checkを対象システムの手前に配置することで特権ID利用者を特定

＞＞要件8

2 特権ID利用者ごとにアクセス可能なサーバ・システムを限定することでアクセス権限の最小化を実現

＞＞要件7

3 特権ID利用者・管理者の職務分掌のためのアクセス申請・承認機能を実装

＞＞要件6

4 SecureCube / Access Check経由でのリモートアクセス全般に対するアクセスログを一元管理

＞＞要件10

5 SecureCube / Access Checkでは主な暗号化通信に対応

＞＞要件4

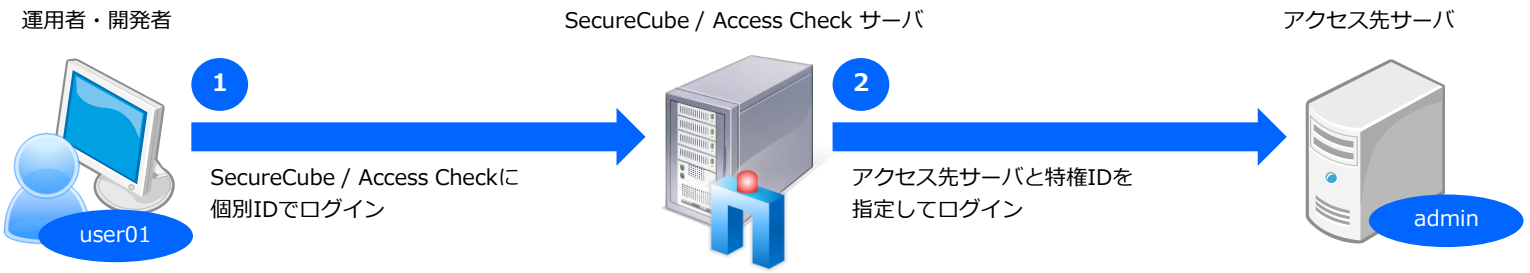
6 取得したログの暗号化保存も可能

＞＞要件3

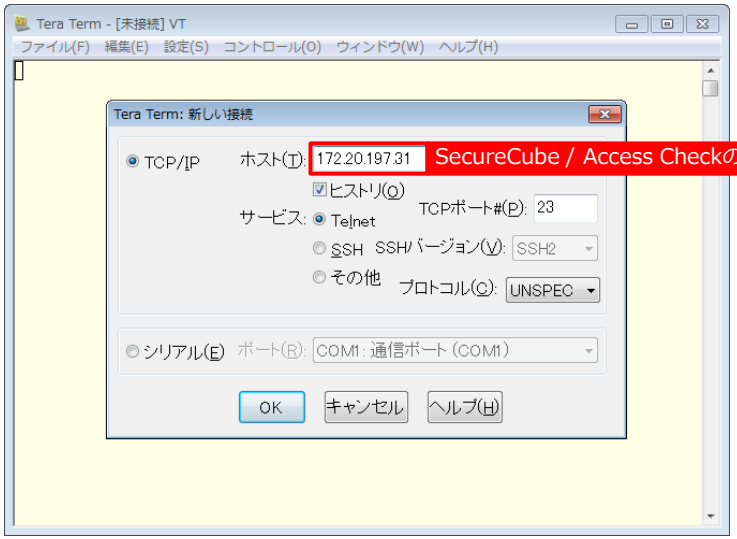
※ 実際の要件への準拠は各社の環境によるため、QSAによる判断が必要となります。

POINT1　特権ID利用者の特定

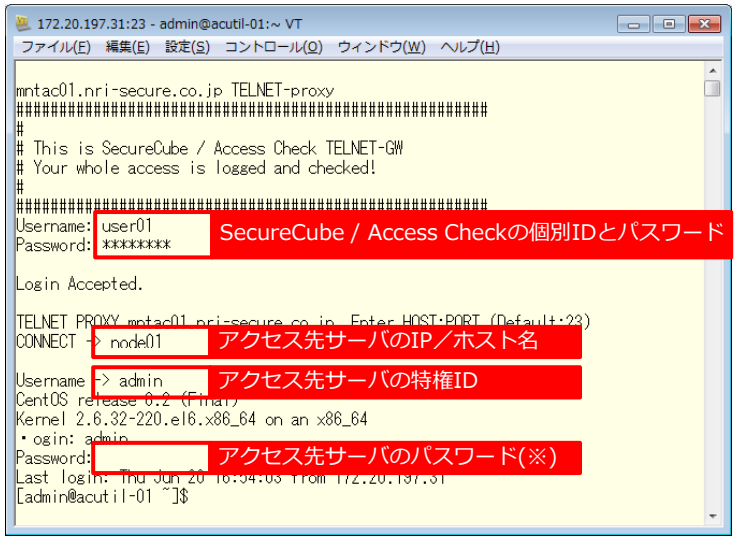
- 特権IDを共有している場合においても、SecureCube / Access Checkに個別IDでログインが成功した後にアクセス先サーバへ接続することで、特権ID利用者の個人が特定可能です。



▼ SecureCube / Access Checkを指定してアクセス（例：Telnet）



▼ 個別IDでログイン成功後、アクセス先サーバへログイン（例：Telnet）

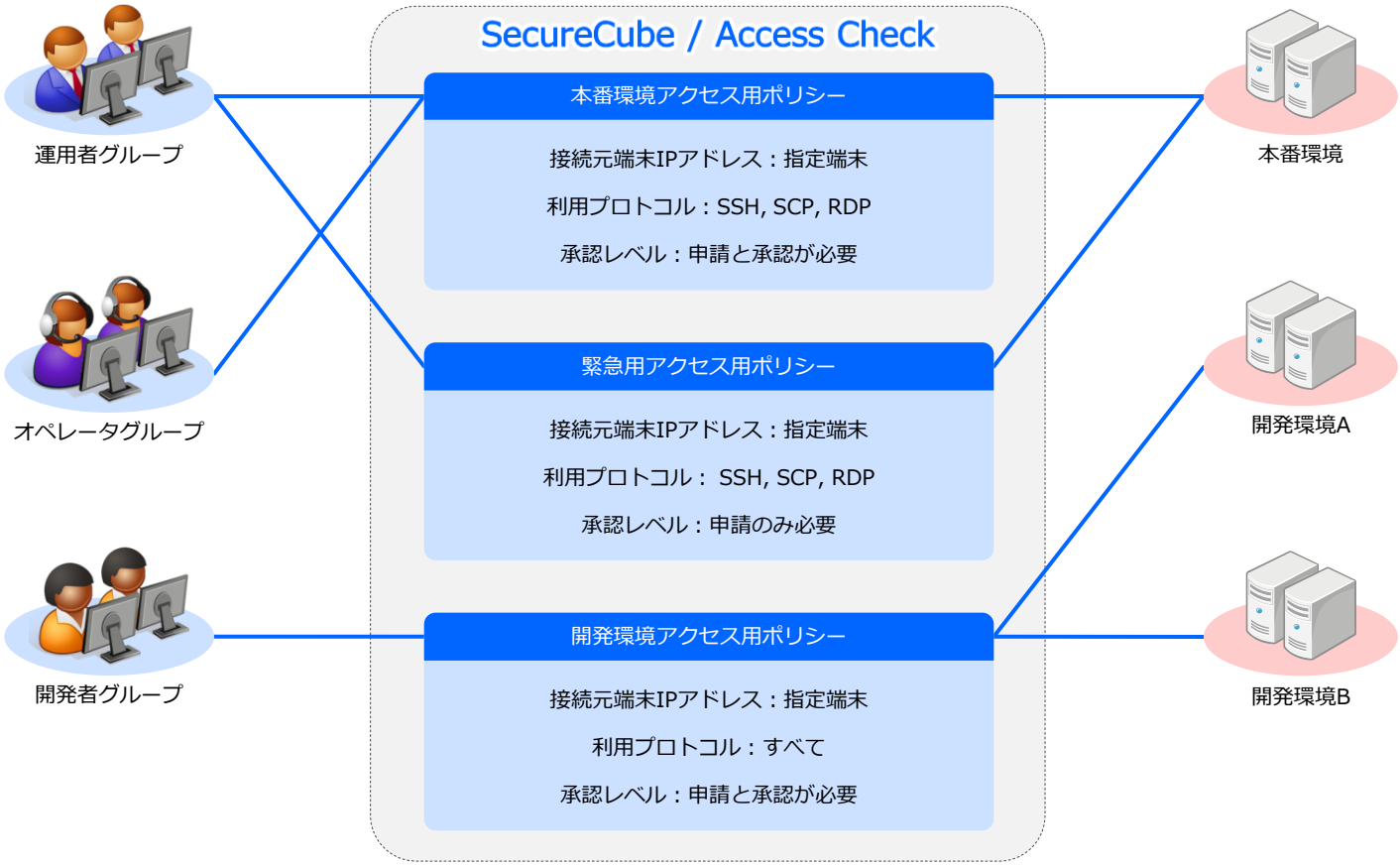


※「特権パスワード管理システム連携」を利用することで、特権ID利用者がパスワードを知ることなく、アクセス先サーバへログインすることも可能です。

POINT2　アクセス権限の最小化

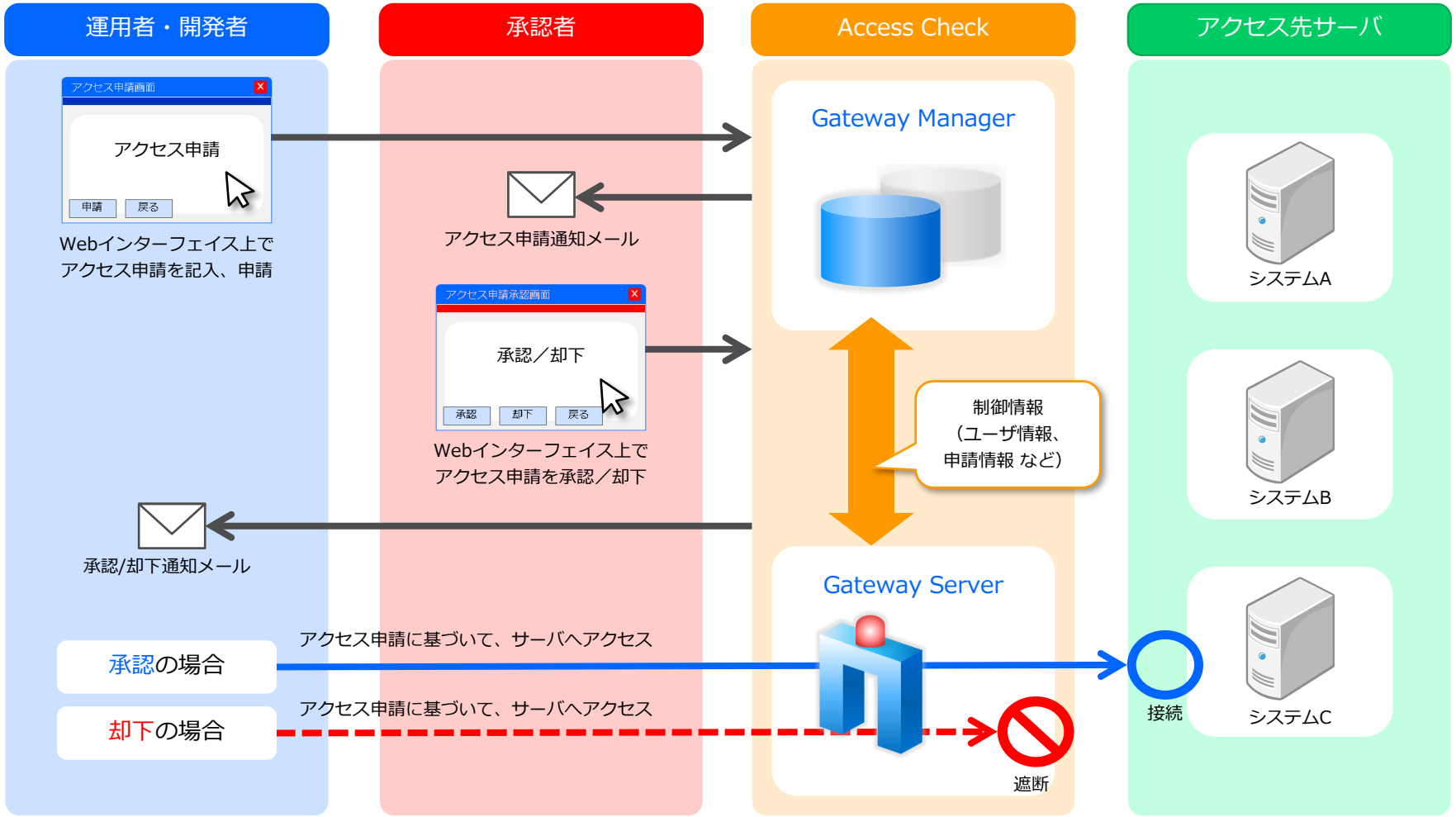
- SecureCube / Access Checkは、あらかじめ設定されたポリシーにしたがってアクセス制御を行います。
- SecureCube / Access Checkのユーザは、決められた端末から、決められたサーバ／システムに対して、決められたプロトコルを利用した接続のみ許可されます。

ユーザは、ポリシーを介して紐づいていないシステムへは接続できません。



POINT3　アクセス申請・承認機能

- アクセス申請・アクセス承認に基づいたアクセス制御を行うことで、「承認されたユーザに対して」、「承認された時間帯で」、「承認されたシステムへ」のアクセスのみを許可します。



POINT4　アクセスログの一元管理

- SecureCube / Access Checkでは、ユーザがアクセス先サーバへ接続した際に、アクセスの概要を記録した「サマリーログ」と実操作を記録した「操作ログ」を取得し、保管します。
- 取得したログは、利用したポリシーに紐づく監査者のみがWeb画面上で検索・閲覧できます。

▼ アクセスログ検索結果一覧（サマリーログ）

アクセスログ検索結果

アクセス開始日時	アクセス終了日時	接続時間（秒）	アクセス可否	申請番号	申請時間超過	利用ポリシーID	操作ログ
2013/04/09 15:35	2013/04/09 15:45	590	アクセス許可	20130409000000		policy_001	
2013/04/09 15:36	2013/04/09 15:46	599	アクセス許可	20130409000000		policy_001	
2013/04/09 15:39	2013/04/09 15:40	71	アクセス許可	20130409000000		policy_001	
2013/04/09 15:43	2013/04/09 15:44	33	アクセス許可	20130409000001		policy_002	
2013/04/09 15:44	2013/04/09 15:46	95	アクセス許可	20130409000001	超過	policy_002	

該当件数：5, 件中 1 - 5

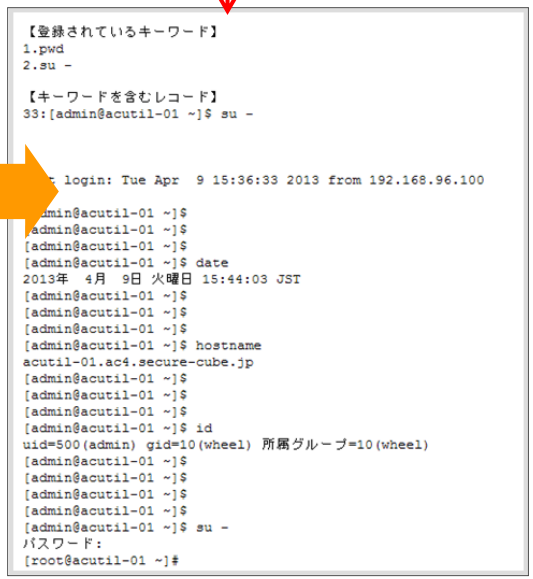
検索結果一覧ダウンロード

検索結果で表示されたサマリーログの一覧をCSV形式でダウンロードすることも可能です。

事前申請と作業ログとの突合せ時間が大幅に削減!

▼ 事前申請の内容を表示

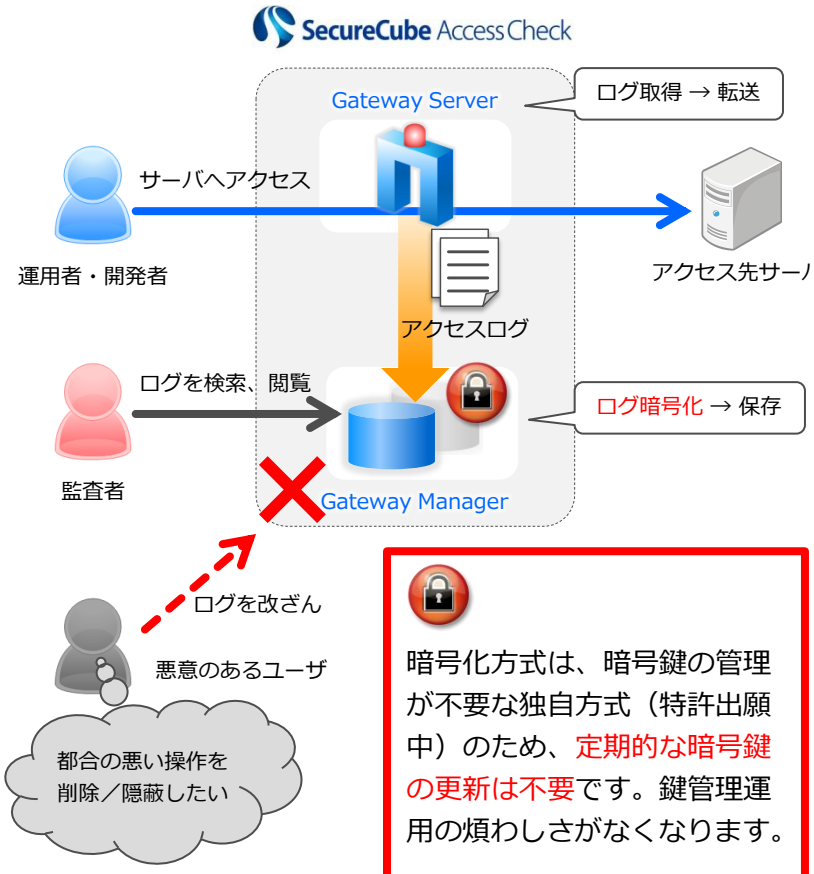
▼ 操作ログの例



POINT5・6　ログの暗号化・暗号化通信対応

- 取得された操作ログは、内容を改ざんされることを防ぐため、暗号化して保存することが可能です。
- 暗号化された通信（SSH, SFTP, SCP）の内容も取得することができます。

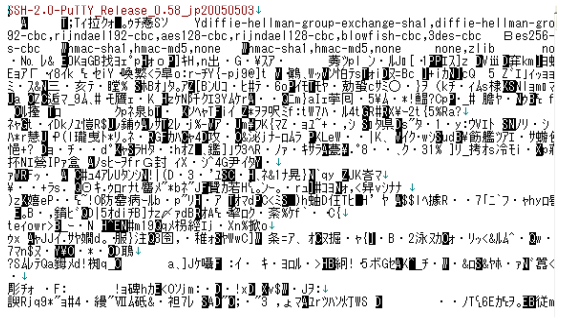
ポリシーのアクセス制御に関する設定



暗号化方式は、暗号鍵の管理が不要な独自方式（特許出願中）のため、定期的な暗号鍵の更新は不要です。鍵管理運用の煩わしさがなくなります。

暗号化通信の対応

▼ 暗号化された通信データ（例：SSH）



▼ 復号して操作ログを取得

```
----------------------------------------------------------------------
WARNING! By accessing and using this system you are consenting
to system monitoring for law enforcement and other purposes.
Unauthorized use of this computer system may subject you
to criminal prosecution and penalties.
----------------------------------------------------------------------
[admin@acback01 ~]$ w
 16:35:33 up 505 days, 21:57,  3 users,  load average: 0.24, 0.05, 0.02
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                 25Oct09  6days  0.39s  0.39s -bash
admin    pts/0    192.168.0.10      16:35    1.00s  0.08s  0.06s w
admin    pts/1    192.168.0.11      22Apr10 132days  0.03s  0.03s -bash
[admin@acback01 ~]$
[admin@acback01 ~]$
[admin@acback01 ~]$
[admin@acback01 ~]$
[admin@acback01 ~]$ exit
logout
Connection to 192.168.0.1 closed.
#in=1333 out=91 duration=260
```

PCIDSSの要件に対する課題と対策事例

- PCI DSSの準拠を目指し、特権ID管理システムツールとしてSecureCube / Access Checkを導入された事例を紹介します。
- 運用の現場からは、「業務負荷が減った」などの歓迎の声をいただいています。

背景・目的

大手百貨店グループのシステム系グループ企業 様

- 大規模な合併に伴い、オンラインショッピングのWebサイトをはじめとする本番環境サーバの数が増大（10→100台以上）
- 本番環境のセキュリティ管理レベルがばらばらで運用負荷が増加すると予想
- セキュリティ管理レベルを見直すなかで、クレジットカード情報を扱う会社に対して適用されるPCIDSSの準拠を目指す

要　　件

本番環境サーバの数が数百台に及んだとしても、特権IDの管理業務が現実的に運用可能であること	本番環境サーバにログインする際に、特権IDのパスワードを知ることなくログインできること	本番環境サーバへのアクセスの際に、上司などの第三者の承認がないとアクセスできないこと

SecureCube / Access Checkの導入を決定

導 入 効 果

SecureCube / Access Checkのユーザ IDを個人の識別が可能なIDにすることで、本番環境サーバ上に個別IDを作成・管理する業務が不要になり、**特権ID管理の業務負荷が軽減!**	SecureCube / Access Checkの特権IDパスワード管理システム連携機能を利用することで、強固なパスワードの設定や定期変更などの**パスワード管理業務の負荷が軽減!**	SecureCube / Access Checkのアクセス申請・承認機能を利用することで、事前申請に基づき承認された時間帯のみ本番アクセス可能になり、**監査業務の負荷が軽減!**

ご清聴いただき、ありがとうございました。

NRIセキュアテクノロジーズ株式会社

〒105-7113　東京都港区東新橋1-5-2　汐留シティセンター
Tel:03-6274-1011 Fax:03-6274-1099
E-mail:info@nri-secure.co.jp
Home Page:http://www.nri-secure.co.jp