特権ID管理ツール「SecureCube Access Check」紹介セミナー

特権ID管理ツール
「SecureCube Access Check」のご紹介

NRIセキュアテクノロジーズ株式会社
セキュリティソリューション事業本部
統制ソリューション事業部

「特権ID管理ツール「SecureCube Access Check」のご紹介

SecureCube Access Checkのご紹介と導入効果

SecureCube Access Check 提供形態と導入の流れ

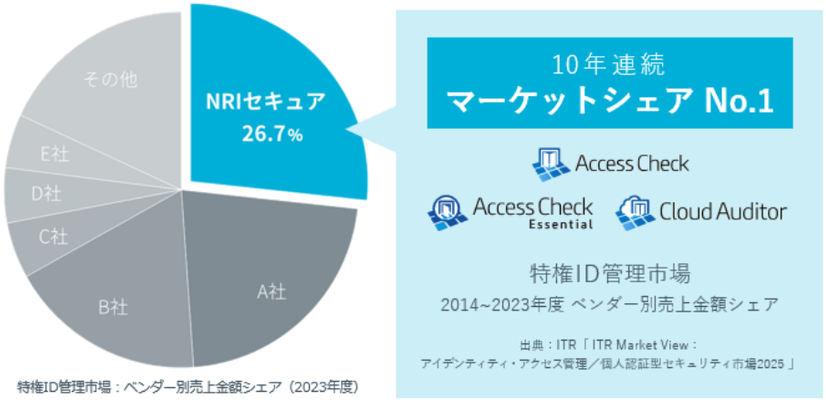
まとめ

SecureCube Access Checkの
ご紹介と導入効果

SecureCube Access Checkの概要

※ 出典：ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2025」特権ID管理市場：ベンダー別売上金額シェア（2023年度）
SecureCube Access Check, Cloud Auditor by Access Check, Access Check Essential が対象

特権ID管理に必要な機能をすべて備えた オールインワンソリューション



特権ID管理市場：ベンダー別売上金額シェア（2023年度）

様々な業種のお客様の課題を解決

出光 / ONE COMPATH / KDDI / TOWER RECORDS
IIJ / CTC / TOKYU CARD / JEOL
東計電算 / ベネッセコーポレーション / SoftBank

一部抜粋・順不同

販売代理店

CTC / TIS INTEC Group / Marubeni IT Solutions / Hewlett Packard Enterprise
IIJ / Computer Science Corporation / GRCS

一部抜粋・順不同

特権ID管理ソリューション SecureCube Access Check の3つの特長

- SecureCube Access Checkは、NRIセキュアが金融機関のシステム保守業務のために開発した、安全性の高いゲートウェイ型の特権ID管理ソリューション
- 下記の3つの特長があるほか、専門エンジニアによるきめ細やかな保守サポートも好評

ゲートウェイ型だから
導入・運用が容易

制約条件が少なく
多様な環境での利用が可能

多くの企業・組織に支持され
市場シェアNo.1※の導入実績

※ 出典：ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2025」特権ID管理市場：ベンダー別売上金額シェア（2023年度）
SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象

ゲートウェイ型だから導入・運用が容易

- 端末や管理対象機器へ専用ソフトを入れることがないため、導入の影響を最小限にして導入可能
- 厳密な運用設計を行わず、まずはログ取得のみで配置するなど、スモールスタートも用意

完全エージェントレスで
既存システムへの
影響を最小に

ゲートウェイを介さない直接ログインに対しては
ID・パスワード管理（PPM）機能で制御可能。

制約条件が少なく多様な環境での利用が可能

- エージェントレスのため、いつも利用している作業クライアントツールをそのまま利用可能
- 管理対象はサーバだけでなく、ネットワーク機器やクラウドサービスなど幅広く対応
- 10種類のプロトコルをサポートし、ファイル転送プロトコルにも対応

作業クライアントに縛られない

ツールなどに縛られず
すべての作業を対象可能に

クラウドにも対応

ネットワーク環境の変化に応じた
柔軟な対応が可能

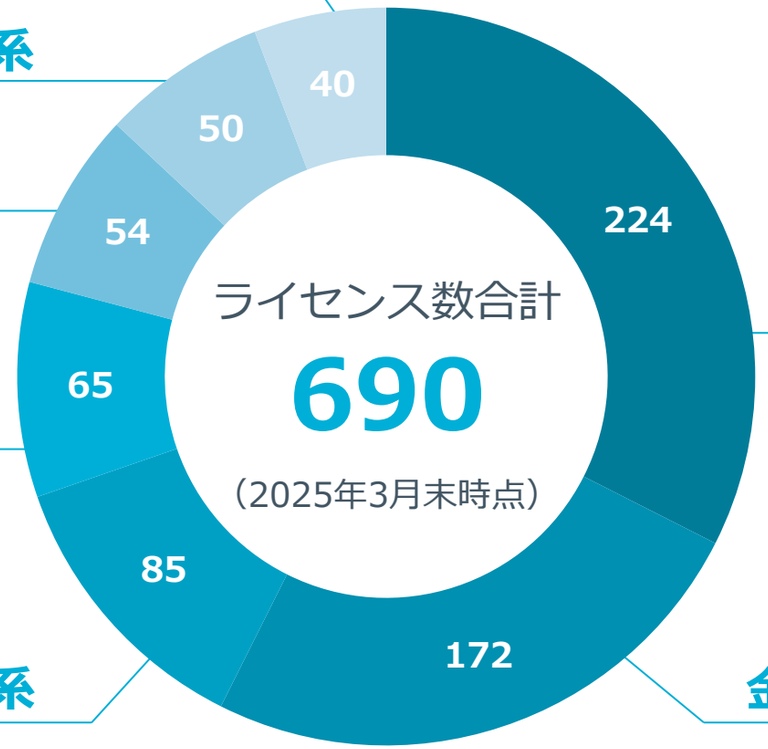
✔RDP ✔Telnet ✔SSH
✔FTP ✔SFTP ✔SCP ✔CIFS
✔HTTP(S) ✔TNS ✔TCP

多くのプロトコルに対応

ファイル転送プロトコルを含む
10種類のプロトコルに対応

多くの企業・組織に支持され市場シェアNo.1※の導入実績

- 上場企業を中心に、業種を問わず、全国690ライセンスの導入実績を誇る
- 特に高いセキュリティを求められる金融の大手証券・保険・銀行などでも採用



情報・IT系
情報処理サービス、
ITコンサル、通信事業　等

金融系
生命保険、損害保険、銀行、
信用金庫、証券、クレジットカード業　等

流通系
運輸、卸売業、百貨店、専門店、
小売スーパー、コンビニエンスストア　等

製造系
石油化学製品製造、製薬、機器製造、
食品製造、ガス・エネルギー　等

公共機関
協会、団体、
特殊法人、官公庁　等

サービス系
航空業、旅行業、
教育関連事業　等

その他
放送、広告、新聞、印刷、
出版、不動産、病院　等

※ 出典：ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2025」
特権ID管理市場：ベンダー別売上金額シェア（2023年度）
SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象

特権ID管理の業務フロー全体をカバーする5つの機能

特権ID管理のすべての課題を解決するオールインワンソリューション

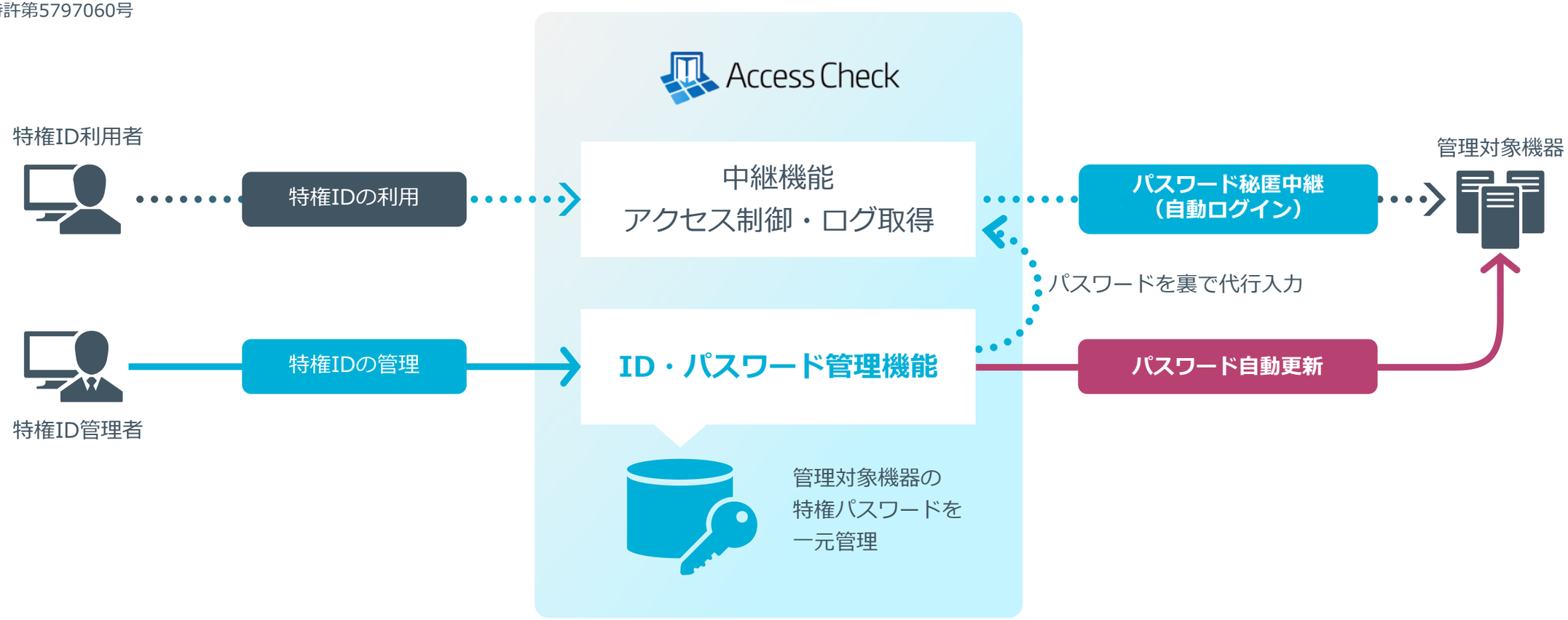
特権利用前		特権利用時	特権利用後	
				
ID・パスワード管理	**ワークフロー**	**アクセス制御**	**ログ管理**	**監査補助**
特権IDのパスワード自動更新や有効期限設定ができるほか、ID情報を収集しCSV出力することが可能です。	申請・承認フローを電子化。事後承認や多段階承認にも対応。既存のワークフローシステムとの連携APIも提供。	予めアクセスできるサーバやプロトコル等をポリシーとして登録。申請時に選択したポリシーや作業時間に従って制御を実行します。	作業の操作内容は記録され、申請と自動的に突合せされます。閲覧権限のある監査者のみ検索・閲覧できます。	定期レポート出力の他、危険コマンドの発行通知や、申請外持ち出しファイルの検出機能などを提供。

ID・パスワード管理

- 特権IDのパスワード自動更新や有効期限設定などのPPM機能※1やパスワード払い出し機能を搭載
- NRIセキュア独自の特許技術※2で特権パスワードを開示せずに、許可された接続先へ自動ログイン可能

※1　PPM（Privileged Password Management）機能：特権IDのパスワードを変更するなどの管理機能

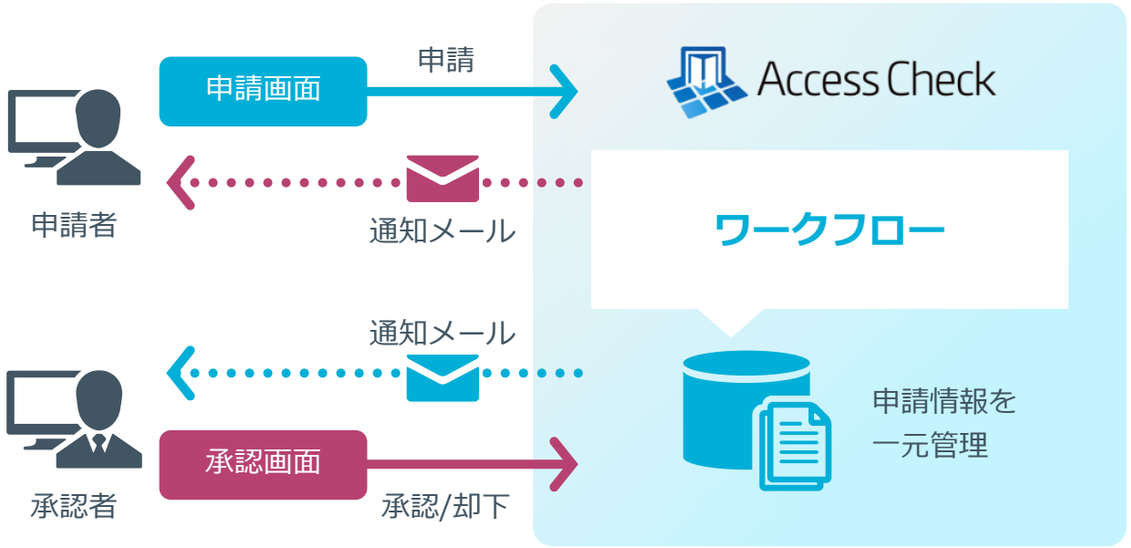
※2　特許第5797060号



ワークフロー

- **特権ID利用における申請から承認までのプロセスをシステム化することで、管理負荷を大幅削減**
- **多段承認や多段グループ承認、事後承認など、自社のルールに合わせた設定が可能※**

※　ServiceNowと申請情報を連携することで、申請内容をさらに細かく設定することも可能です。（Access Check Integrationオプションが必要）



多段承認

指定された承認者が順に承認を行い、承認者全員が承認して初めて「承認済み」となります。

多段グループ承認

指定された各段階の承認者グループの中で一人が順番に承認を行い、すべての段階で承認されて「承認済み」となります。

事後承認

緊急時など、事前に承認者による承認が難しい場合、承認前に作業が可能です。その場合「事後承認」となります。

パスワード払出申請

申請と承認を行うことで、作業者が、作業時に利用する特権IDのパスワードを一時的に参照することが可能です。

テンプレート

よく実施する作業は、申請内容をテンプレートとして保存することが可能です。

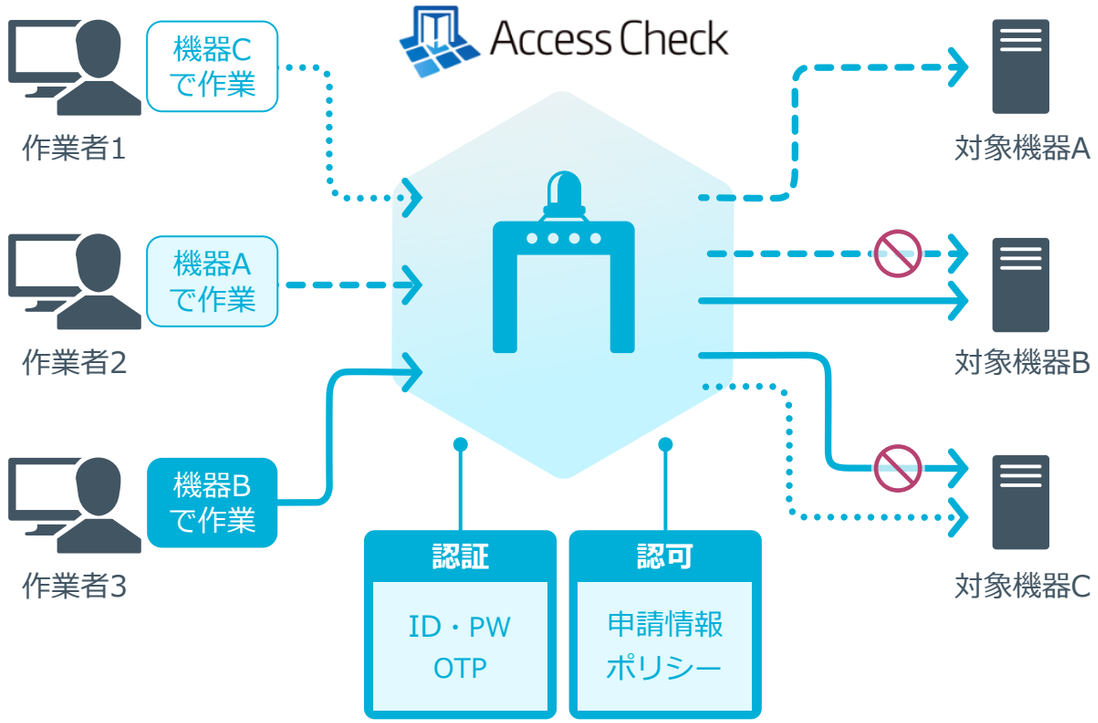
完了報告

作業後、申請内容に対して完了報告（テキスト）を入力することが可能です。

アクセス制御

ID・パスワードとワンタイムパスワード※などによる「認証」と、申請情報あるいはポリシー設定に基づく「認可」によって、管理対象機器へのアクセス可否を判断

※　ワンタイムパスワードを利用した多要素認証には、「高度認証オプション」が必要です。



多要素認証

高度認証オプションを用いることで、SecureCube Access Checkにおける個人認証にワンタイムパスワード（OTP）が必須となります。

New 中継接続許可

中継開始時に、作業者単独では接続できず、別の担当者（再鑑者）による接続許可をもって接続可能になります。

パスワード秘匿中継

中継時に特権パスワードを裏で代行入力して自動ログインさせることで、作業者に特権パスワードを伝える必要がありません。

New 自動特権昇格

SSH中継を利用する際、管理対象機器へ一般ユーザでのログイン後、パスワード入力なしに自動的に特権昇格することが可能です。

アクセス通知

アクセスの開始時、および終了時に、しかるべき承認者へアクセス通知のメールが送信されます。

申請時間超過による強制切断

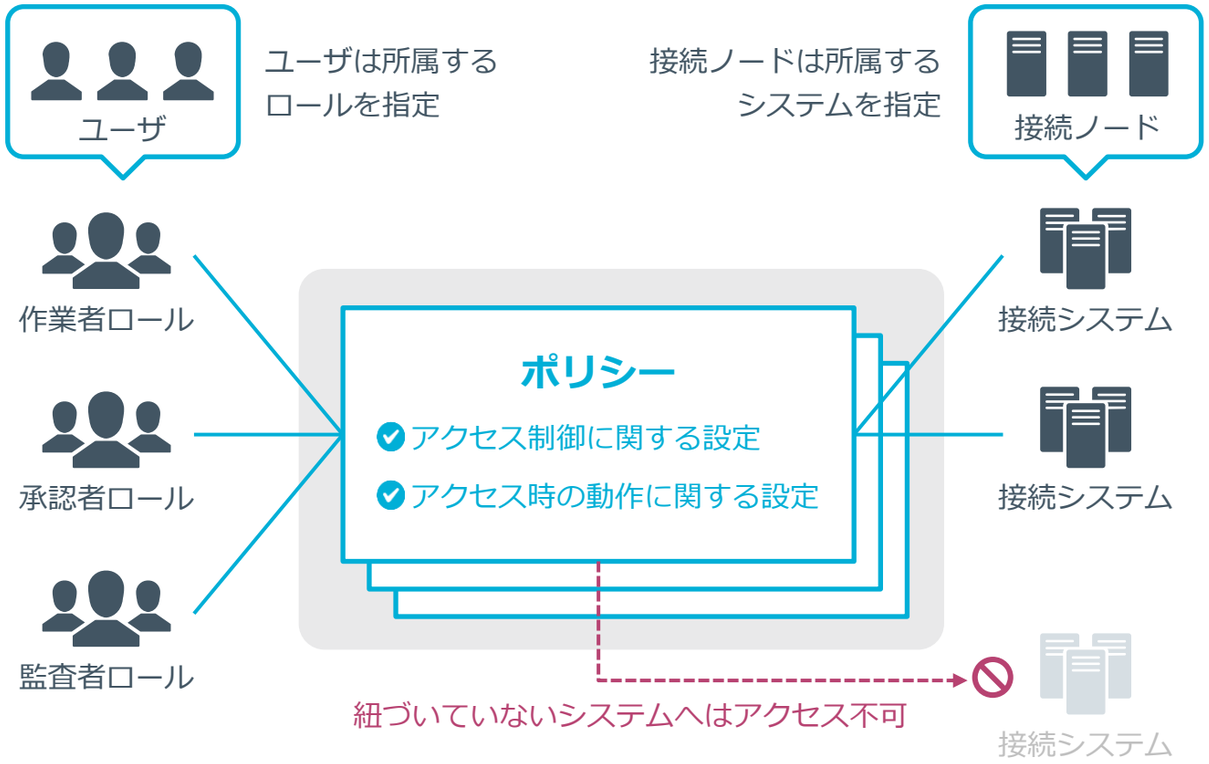
申請時に指定した終了予定時刻を超えると、中継の通信を強制的に切断します。切断しない設定にすることも可能です。

リアルタイムキーワード検知

あらかじめ指定したコマンド（キーワード）が作業中に確認された場合、リアルタイムに通信を遮断することが可能です。

アクセス制御｜ポリシー

- **ユーザの役職や所属に応じて、アクセスできる管理対象機器や、利用できるプロトコル、接続端末の限定、事前承認の有無などを「ポリシー」として設定**
- **ユーザは「ロール」、接続ノードは「システム」にグルーピングされ、「ポリシー」によって紐づけされる**



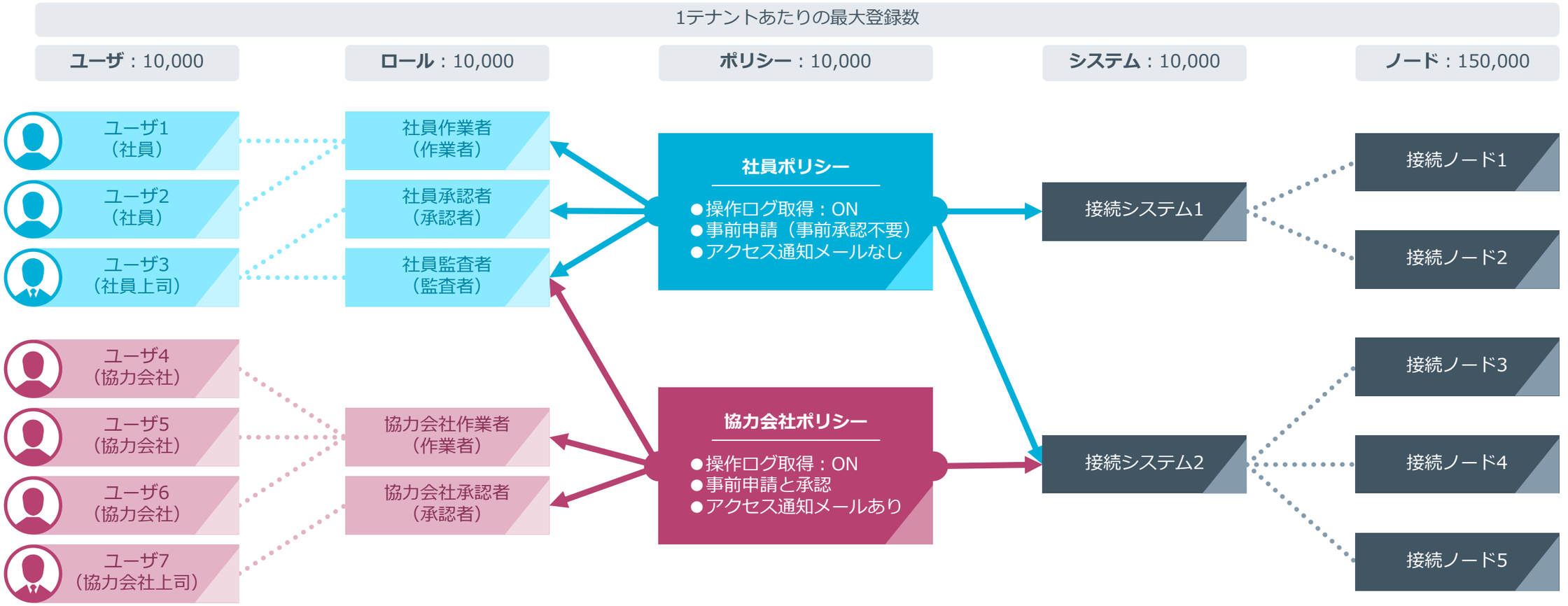
アクセス制御に関する設定

- 接続可能なユーザグループ（ロール）を限定
- 承認者グループ（ロール）、および承認経路を指定
- 中継時の接続元端末のIPアドレスを限定
- 接続可能なサーバ／システムを限定
- 申請時に接続するノードやアカウントの限定有無
- 利用可能なプロトコルを限定
- アクセス申請利用時の事前承認の要否の指定
- アクセス申請利用時の最大申請日数（作業日数）を指定
- 中継接続許可の利用有無（Telnet/SSH/FTP/SCP/SFTP/RDP/TNS）

アクセス時の動作に関する設定

- アクセスを開始または終了した際の通知メール送信の有無
- RDP接続時のクリップボード機能の利用有無
- 検知したいキーワード（Telnet/SSH/TNS利用時）
- リアルタイム切断したいキーワード（Telnet/SSH利用時）
- 重要情報検知の有無（Telnet/SSH/FTP/SCP/SFTP/CIFS/RDP利用時）
- 操作ログの取得有無
- 自動特権昇格の利用有無（SSH利用時）

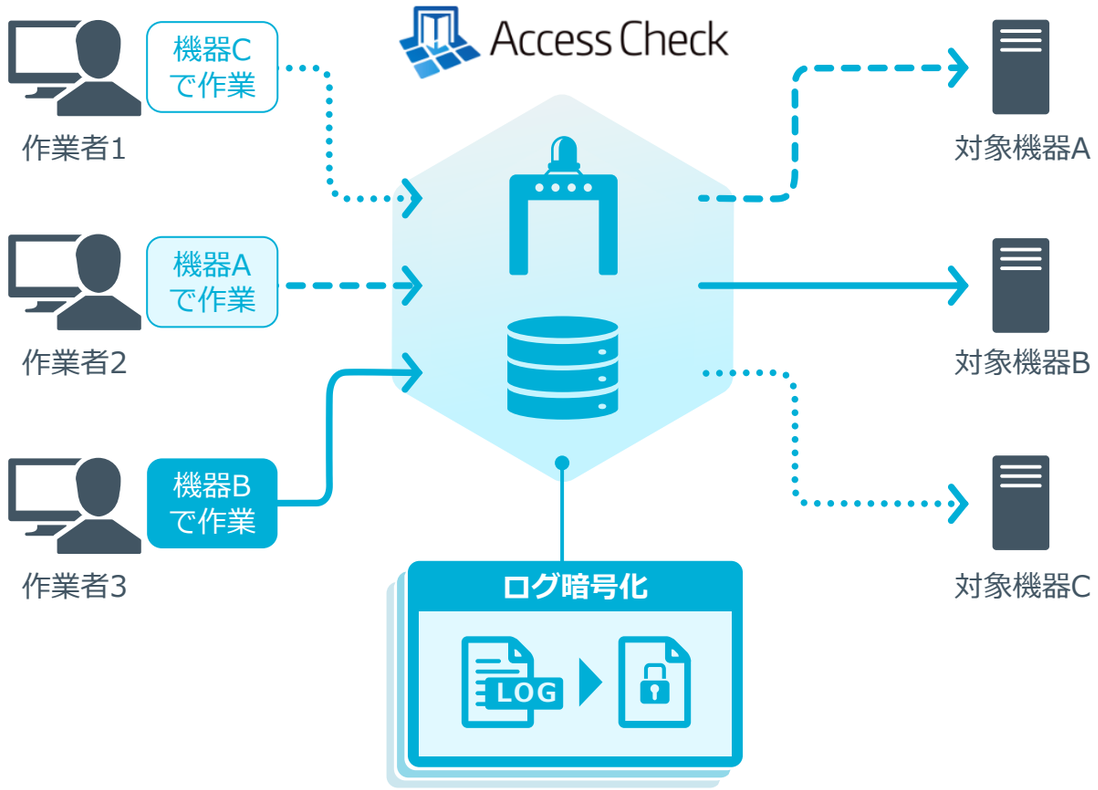
アクセス制御｜ポリシーの設定例



- 「社員作業者」ロールにあてはまる　ユーザ1　と　ユーザ2　は、事前申請のみですべてのシステムにアクセス可能
- 「社員承認者」ロールにあてはまる　ユーザ3　は、社員ポリシーに関わる申請の承認/却下が可能（事前承認・事後承認どちらも可能）
- 「協力会社作業者」ロールにあてはまる　ユーザ4～6　は、接続システム2　へアクセスする際に、協力会社上司である　ユーザ7　の事前承認が必要
- 「協力会社作業者」ロールに当てはまる　ユーザ4～6　が　接続システム2　へアクセスを開始/終了すると　協力会社上司である　ユーザ7へ通知される
- 社員上司である　ユーザ3　は、社員ポリシー、および、協力会社ポリシーに関わるログの監査が可能
- 社員上司である　ユーザ3、および協力会社上司である　ユーザ7　は、作業者ロールにあてはまらないため、いずれのシステムにもアクセス不可

ログ管理

- SecureCube Access Checkを経由したすべての操作が、アクセスログ、操作ログとして取得される
- 取得されたログは暗号化され、ポリシーに紐づく監査者のみが参照できるため内部統制の証明として有効



アクセスログの内容

いつ、誰が、どの端末から、どのサーバへ、どのプロトコルで、どの申請に基づいてアクセスしたか、などのアクセス概要を記録。設定に関わらず、すべての接続で取得される。

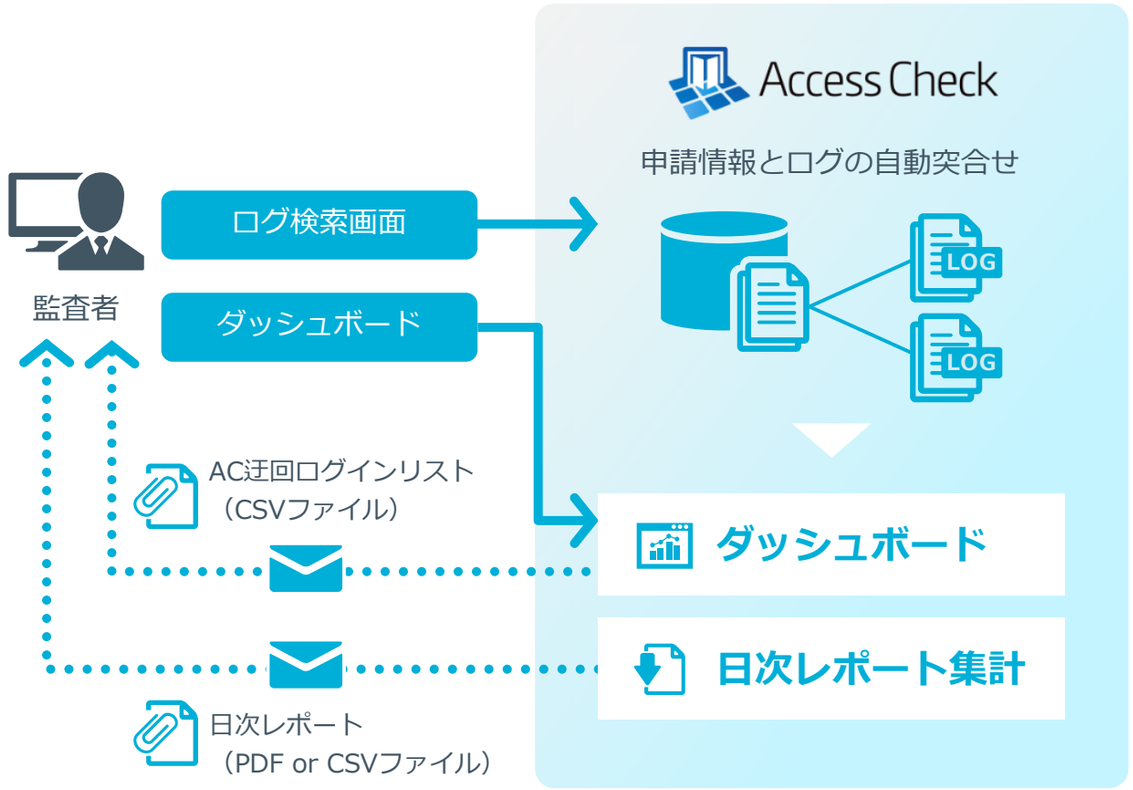
操作ログの内容

アクセス先サーバ／システムでどのような操作を行ったのか、またはどのようなファイルを転送したのか、などの実操作を記録したもの。操作ログの取得有無はポリシーごとに設定する。

プロトコル	操作ログ形式
RDP	リモートデスクトップ上で操作した動画ファイル、クリップボードの転送データ、およびキーボード情報（テキスト）
Telnet / SSH	ターミナルに表示された文字列を記録したテキスト
FTP / SFTP / SCP / CIFS	実際に転送したファイルデータ、およびコマンド（テキスト）
TNS	リクエスト情報（テキスト）
HTTP / HTTPS	リクエスト情報、およびレスポンス情報（テキスト）

監査補助

- 申請情報と実際のアクセスログ、操作ログが紐づけられた状態で記録されているため監査が容易
- 日次レポートやダッシュボードによる集計で、監査業務を支援する機能も標準搭載



日次レポート

- アクセスログ一覧
- アクセス申請一覧
- パスワード払出ログ一覧
- アクセス申請機能による規制履歴
- アクセス申請時間超過アクセス履歴

ダッシュボード

- 接続ノードへのAC迂回ログインリスト
- ログイン失敗総数の推移
- 普段とは異なるIPアドレスからの中継リスト
- 夜間・休日などの利用ユーザリスト　他

各種検知機能

不正操作の早期発見や、ログモニタリングの観点として活用いただけます。

- Access Check迂回ログイン検知
- 要注意キーワード検知
- 不正持ち出しファイル検出
- 重要情報検知（オプション）

確認機能

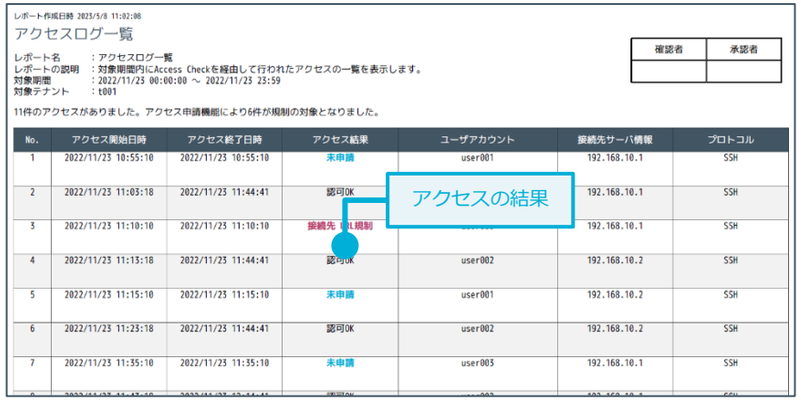
申請内容と関連するアクセスログを照らし合わせて、申請通りの操作であることが確認された場合に、参照している申請を「確認済み」の状態にします。目視で確認したことを明示的に記録できるため、監査状況を管理することができます。

監査補助｜日次レポートの種類とイメージ

アクセスログ一覧（概要）※PDFのみ

対象日にアクセスが終了したアクセスログの一覧

PDF



アクセスログ一覧（詳細）

対象日にアクセスが終了したアクセスログの一覧

PDF CSV

アクセス申請一覧

対象日に利用可能なアクセス申請の一覧

PDF CSV

アクセス申請機能による規制履歴一覧

対象日に、接続ノードへの中継接続がアクセス申請機能による「未申請」や「未承認」等の理由で拒否された履歴

PDF CSV

アクセス申請時間超過アクセス履歴一覧

対象日にアクセス申請を利用した中継接続のうち、アクセス終了予定日を超過して接続していた履歴

PDF CSV

パスワード払出ログ一覧

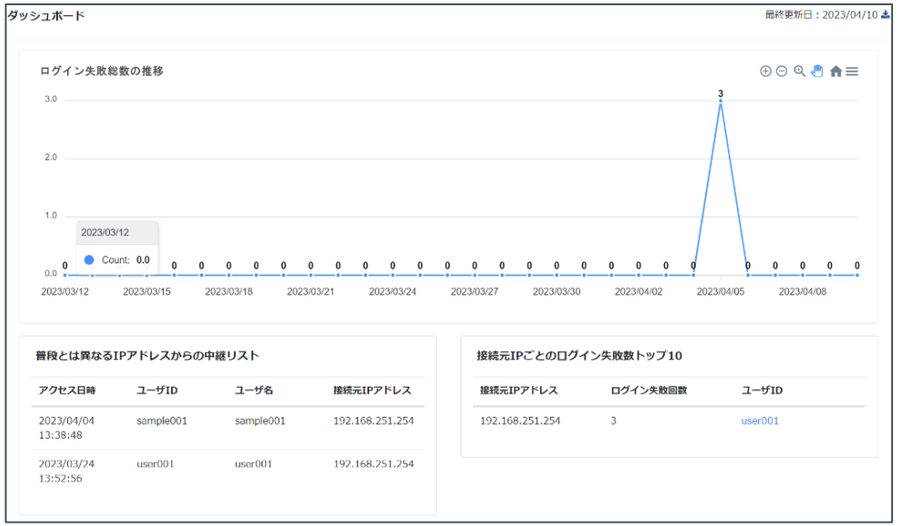
対象日にSecureCube Access Checkからパスワードを払い出しされたログの一覧

PDF CSV

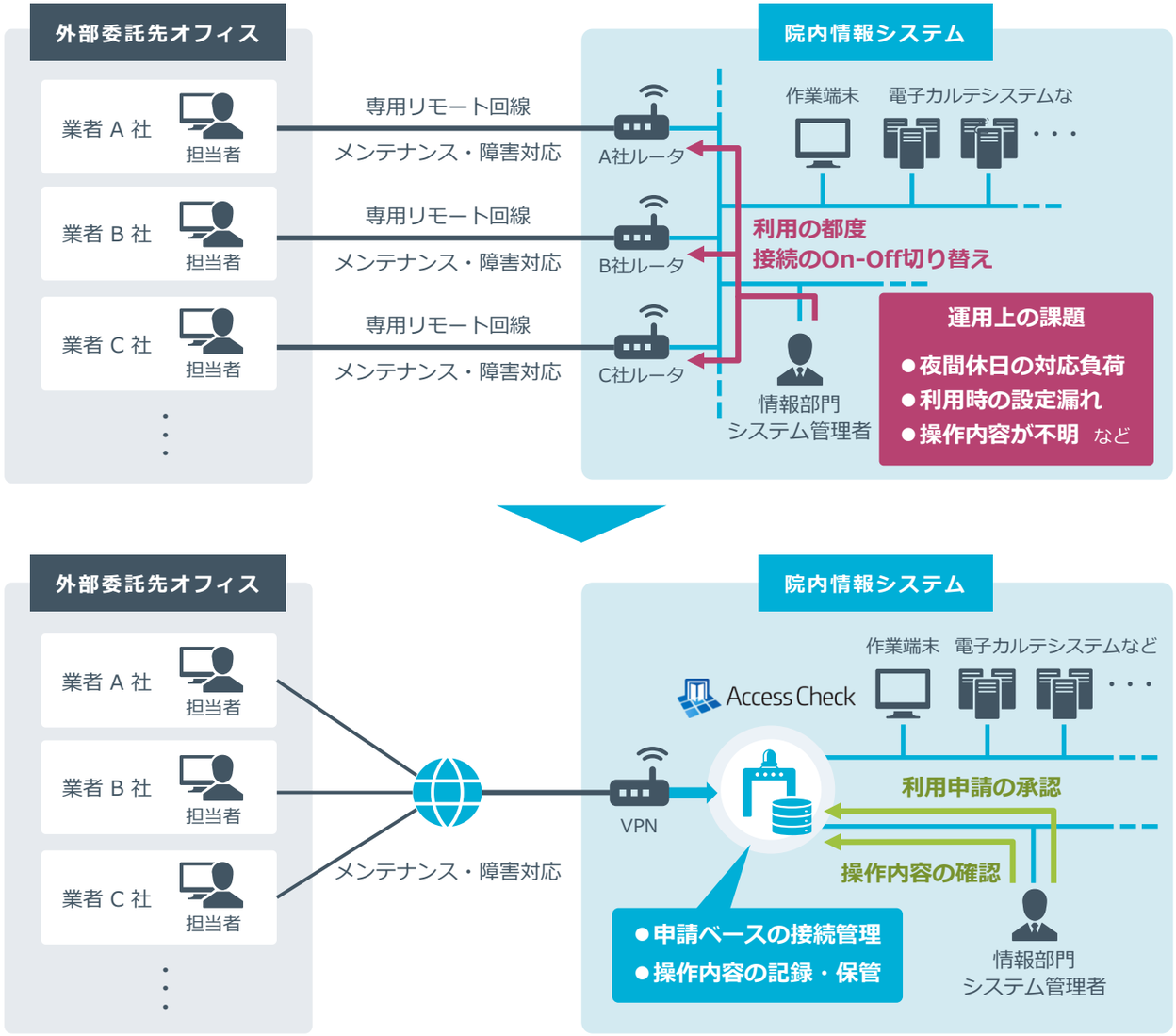
監査補助｜ダッシュボードの項目とイメージ

グローバル管理者向け	
プロトコルごとのディスク利用率の推移	全テナントでのプロトコルごとの中継ログ、およびmysqldumpで使用されているディスクの使用率を日別に表示します。
マスタ管理者向け	
一定期間接続されていないユーザリスト	指定した集計期間中にログイン履歴が1件もないユーザを一覧で表示します。
一定期間接続されていない接続ノードリスト	指定した集計期間中にアクセスログ、またはパスワード払出ログが1件もない接続ノードを一覧で表示します。
監査者向け	
ログイン失敗総数の推移	全ユーザのSecureCube Access Checkへのログインに失敗した総数を日別に表示します。
普段とは異なるIPアドレスからの中継リスト	過去のアクセスログに記録されていないIPアドレスからの中継概要、およびその中継を行ったユーザIDを一覧で表示します。
接続元IPアドレスごとのログイン失敗数トップ10	ログインに失敗した件数を接続元IPアドレスごとに集計し、上位10件を表示します。また、ログインを試行したユーザIDも一覧で表示します。
累計ファイル持込サイズトップ10	集計対象のポリシーを利用した中継接続での持ち込みファイルサイズ（持込量）をユーザごとに集計し、上位10件を表示します。
累計ファイル持出サイズトップ10	集計対象のポリシーを利用した中継接続での持ち出しファイルサイズ（持出量）をユーザごとに集計し、上位10件を表示します。
夜間・休日などの利用ユーザリスト	アクセス開始日時が夜間、または休日であるアクセスログの件数をユーザごとに集計し、一覧で表示します。
接続ノードへのAC迂回ログインリスト	SecureCube Access Checkを経由せずに接続ノードにログインした場合、その接続ノード、およびログインした接続元IPアドレスなどを一覧で表します。

監査者向けのダッシュボードイメージ



ケース1｜病院における活用例



導入目的

外部ベンダーによるリモート作業のアクセス制御

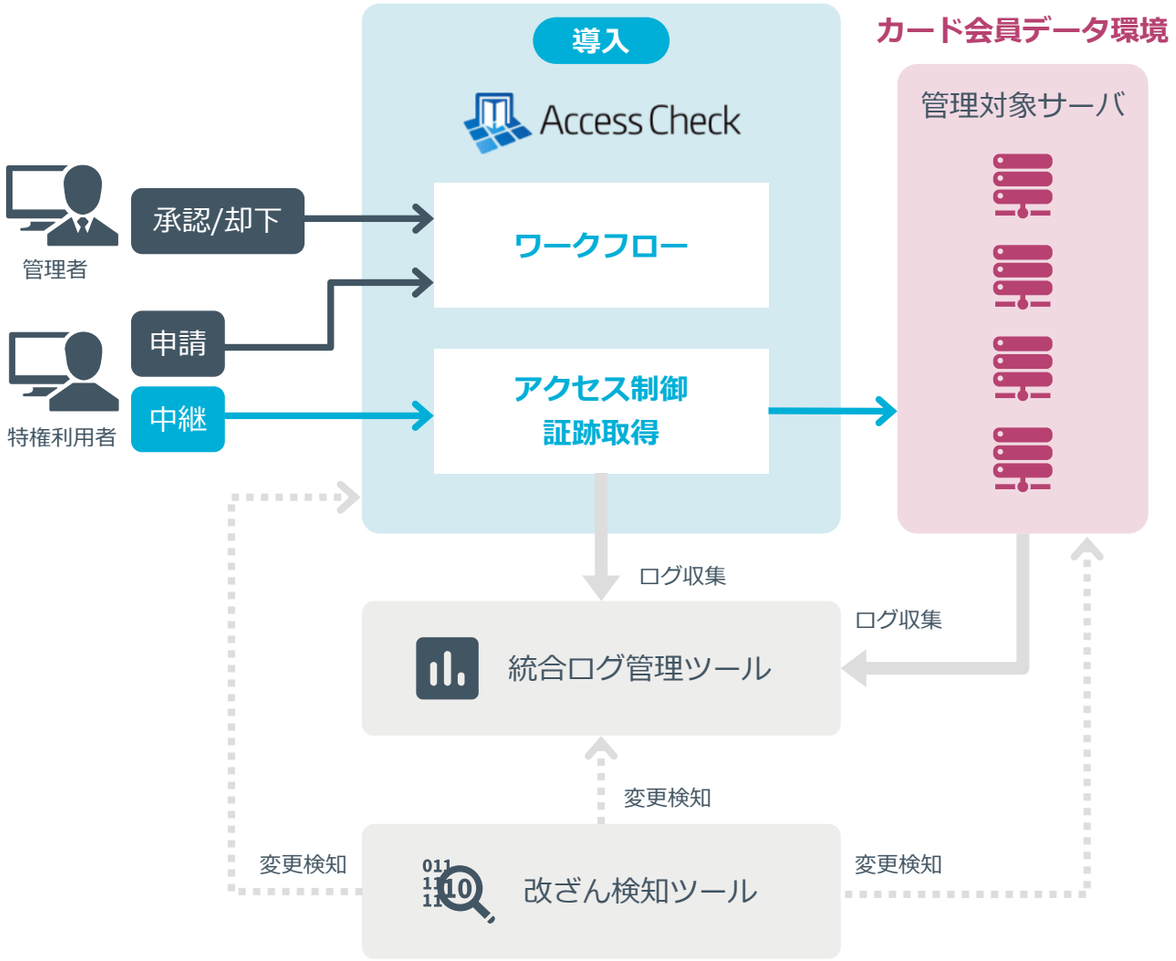
課　題

- ✓ 委託ベンダー専用のルータを、作業の都度、手動でOn-Off対応する管理負荷
- ✓ 緊急メンテナンス作業への対応が困難
- ✓ 作業の証跡は委託ベンダー依存

Point

- ベンダーごとのきめ細やかなアクセス制御を実現
- リモートメンテナンス回線の集約
- システム化による工数削減
- 作業証跡と申請内容の照合の効率化
- 個人情報持ち出しの検知

ケース2｜PCIDSSの求める強力なアクセス制御を実現



導入目的

業界に先駆けたPCIDSS準拠のための「強力なアクセス制御手法」の導入

対応要件

- ✓ 要件7：最小権限・職務分掌、アクセス制御
- ✓ 要件8：個人認証（多要素認証）、ID棚卸
- ✓ 要件10：証跡取得・暗号化保存

Point

- カード決済セキュリティ全般に精通したNRIセキュアが開発提供する製品
- 他システムへの影響がないため、短期間で導入
- 厳格なアクセス制御の仕組みを確立し、組織全体のセキュリティ意識も大きく向上

SecureCube Access Check
提供形態と導入の流れ

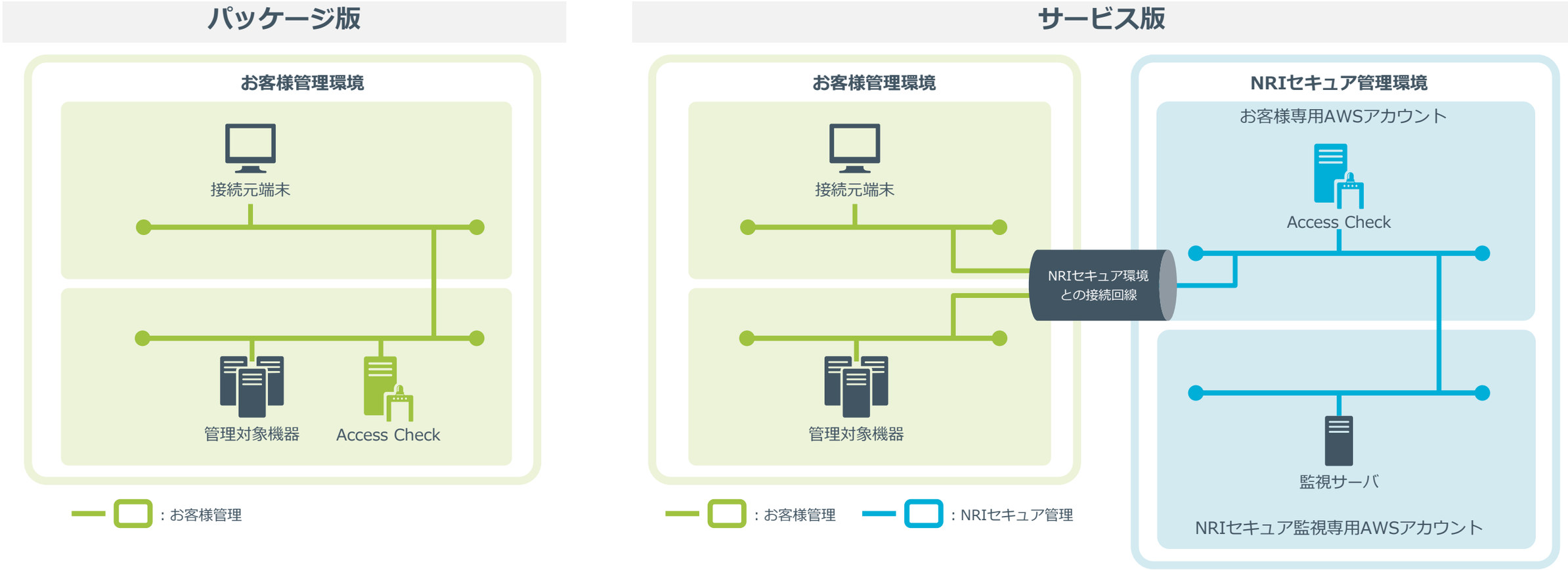
Access Checkシリーズのラインナップ

SecureCube Access Checkは、パッケージ版とサービス版の提供形態を用意

	ハイエンドモデル Access Check SecureCube Access Check		機能限定モデル Access Check Essential Access Check Essential	SaaS型モデル Cloud Auditor Cloud Auditor by Access Check
	パッケージ版	サービス版		
提供方式	ソフトウェア提供	マネージドサービス	ソフトウェア提供	SaaS型
ターゲット規模	中～大規模		小～中規模	
主な要件	● ワークフローや特権パスワード管理など、特権ID管理にかかわる一連の機能が必要 ● 事業部やプロジェクトごとにアクセスポリシーを細かく分けたい	● ワークフローや特権パスワード管理など、特権ID管理にかかわる一連の機能が必要 ● 資産を持たず運用管理負荷を低減したい	● ワークフロー機能は不要でログ取得がメイン ● 最低限のアクセス範囲の制限 ● 低価格で短期間に導入	● AWS上に管理対象機器が存在 ● 特権ID管理サーバの運用アウトソース
課金モデル	買い切りライセンス ＋ 年間保守	年額利用料	サブスクリプション	月額利用料

パッケージ版とサービス版の違い

- **パッケージ版はSecureCube Access Checkをお客様で維持管理する必要があるが、**
  サービス版はNRIセキュアテクノロジーズにてSecureCube Access Checkの維持管理を実施



SecureCube Access Checkサービス版の基本サービス

問い合わせ窓口

サポートサイト上でナレッジを提供するほか、問い合わせを受け付け、専門エンジニアによる対応を行います。

サーバ運用

SecureCube Access Checkを構成するサーバ群の維持・管理のため、OS・ミドルウェアに対するセキュリティパッチ適用などのメンテナンスを行います。

サーバ設定変更

初期設定後、必要に応じて、SecureCube Access Checkを構成するサーバ群に対して、設定変更を実施します。（月2回まで）

稼働監視・障害対応

サービスの稼働監視を24時間365日実施します。障害を検知した場合、一時切り分けを行い、対応・報告を行います。

バージョンアップ・パッチ適用

SecureCube Access Checkのマイナーバージョンアップ、およびSecureCube Access Checkのセキュリティパッチ適用作業を実施します。

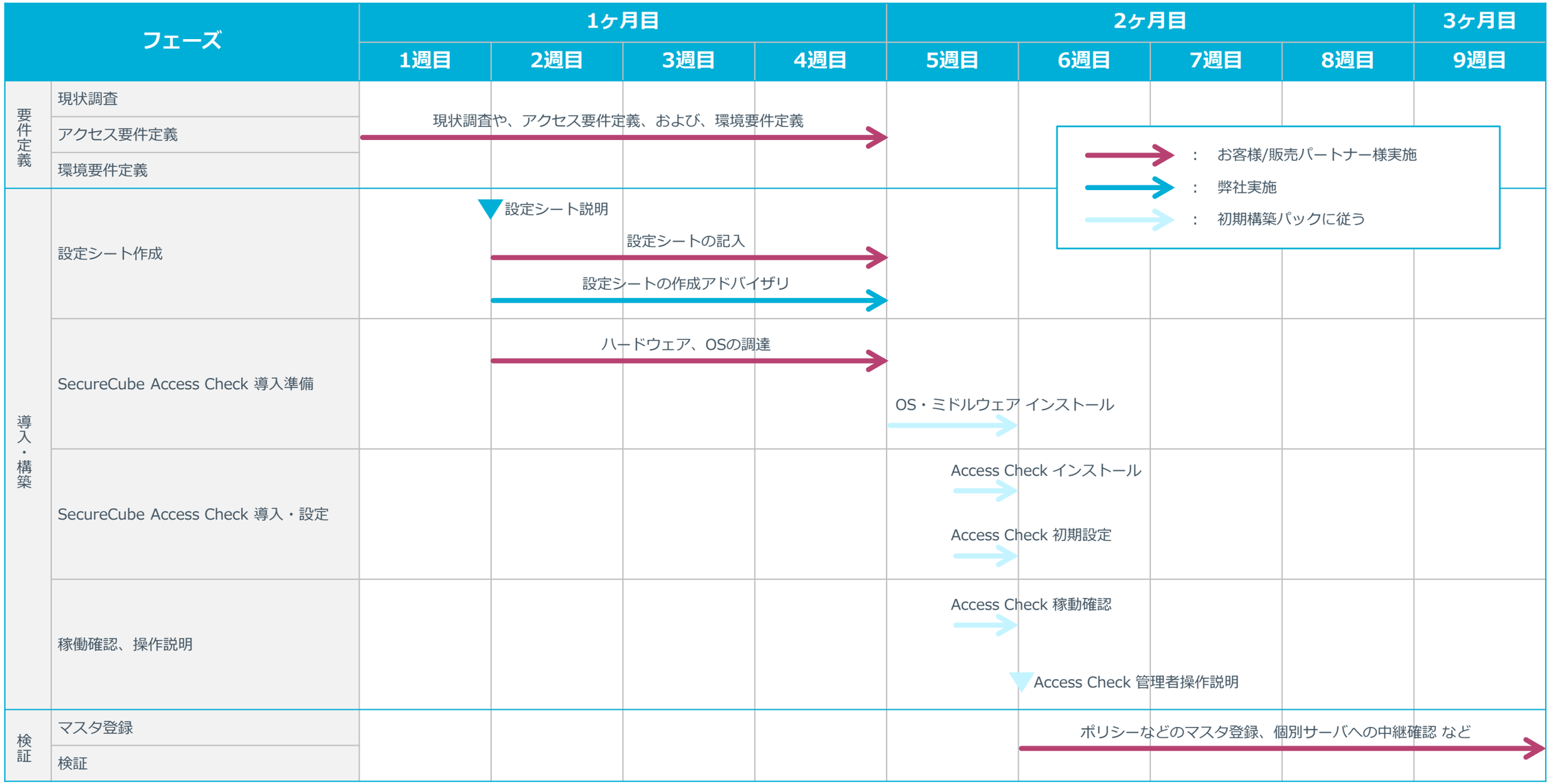
ログ保存

ログは東京リージョンのEBSに、上限500GBまで保存します。ログ容量が上限を超える場合には、オプションが必要です。

SecureCube Access Check 構築支援メニュー

提供形態	構築支援種別	設定シート説明 (2時間×1回)	OS・ミドル 構築	Access Check 構築	稼動確認	操作説明 (2時間×1回)	QA対応	当社環境との つなぎ込み
パッケージ版	構築支援パック **Platinum**	○	○	○	○	○	○	-
	構築支援パック **Gold**	○	お客様対応	○	○	○	○	-
	構築支援パック **Silver**	○	お客様対応	お客様対応	お客様対応	お客様対応	○	-
	構築支援パック **Bronze**	お客様対応	お客様対応	お客様対応	お客様対応	お客様対応	○ (上限10件)	-
サービス版	初期構築サービス	○	○	○	○	○	○	当社/お客様対応

【参考】Access Checkパッケージ版における構築スケジュールのイメージ



まとめ

まとめ

SecureCube Access Checkのご紹介と導入効果

SecureCube Access Check 3つの強み

1．ゲートウェイ方式ならではの、**短期間・低リスク導入**

2．**制約条件が少なく**、多様な環境で利用が可能

3．幅広い業種で採用され、10年連続**国内トップシェア**

SecureCube Access Check 提供形態と導入の流れ

1．ニーズに合わせてパッケージ版、サービス版より選択が可能

2．手厚い構築支援メニューにより導入工数を削減できる

無料デモ体験や**試用版**は弊社HPからお気軽にお申込みください！

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

不定期に関連セミナーも実施しています。ご興味のある方は、アンケートにて「**今後も情報を収集したい**」にチェックをお願いします。

NRI SECURE