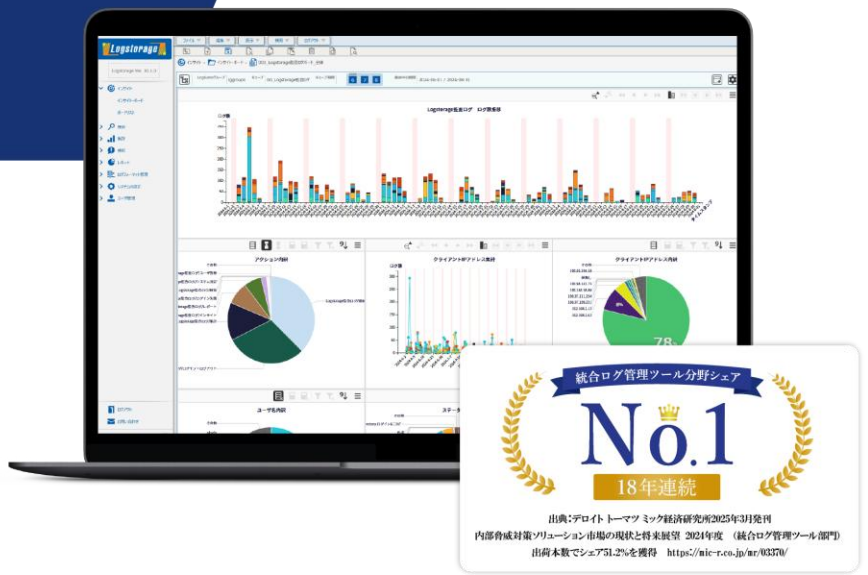
Logstorage

Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage
Access Check 連携パック
参考資料



Infoscience

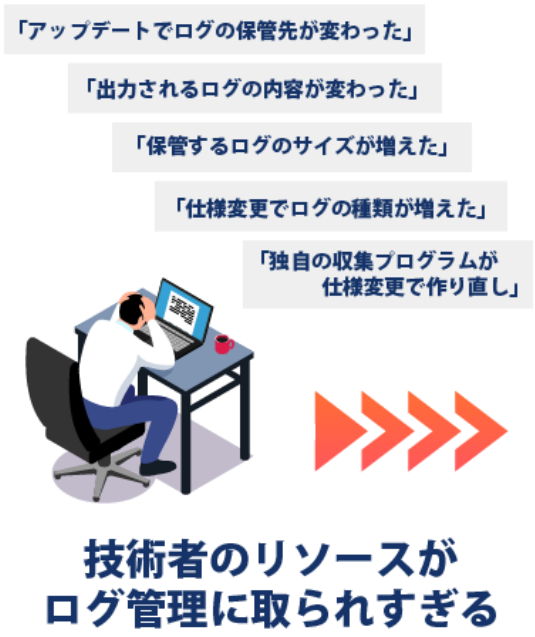
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

Logstorage 連携パックとは

連携パックは、各分野で人気の製品と連携して開発した「ログの収集・分析がすぐにスタートできる」Logstorageのオプション製品です。

連携パックを導入することで、各連携製品のログ管理のセットアップを簡略化できるほか、運用中に、収集対象のログの

フォーマット(並び順や表示の仕方)や出力方法に変更があっても、各連携パックのバージョンアップで、変更を反映できます。



パッケージ内容

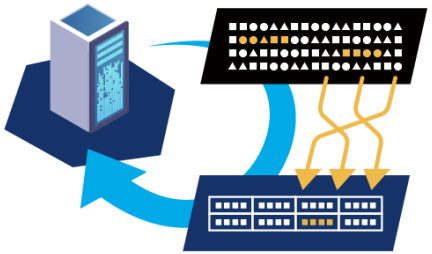
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

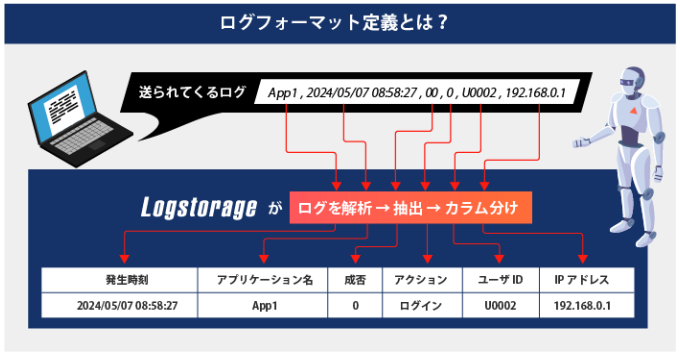
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※製品によっては収集モジュールが不要の場合もございます。
その場合、パッケージに含まれませんので、ご了承ください。

ログフォーマット定義ファイル



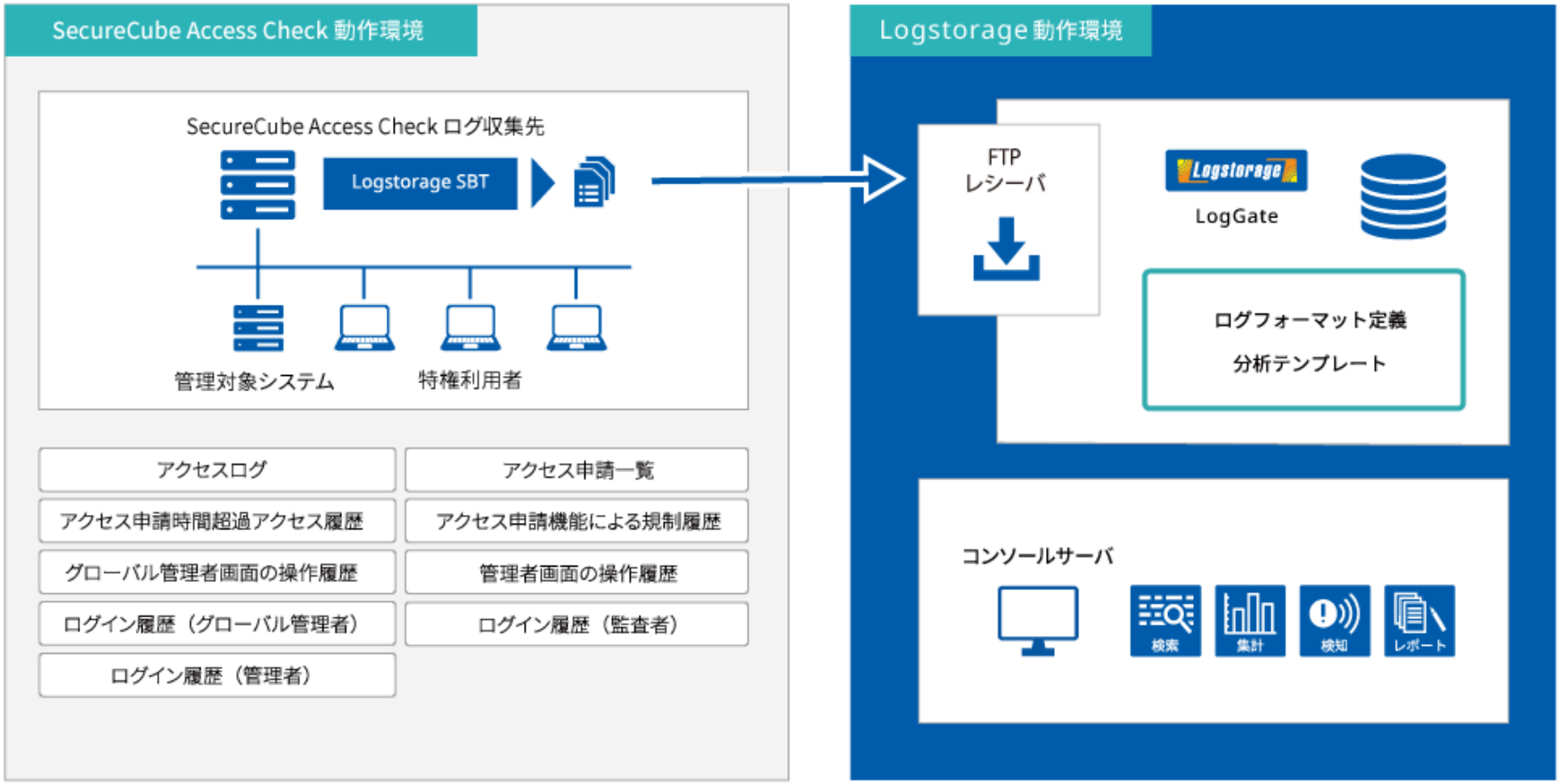
連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。



分析テンプレート

各製品から出力される多数のログの中から、どのログを検索すればよいのか・何を集計したらよいのか・どんなレポートを出力すればよいのか、ログ分析をサポートする分析テンプレートをご提供いたします。

システム構成



検索テンプレート一覧

検索-1

Logstorage Access Check 連携パック の検索テンプレートは以下の通りです。

フォルダ名	検索条件テンプレート名
プロトコル毎	CIFSサマリーログ
プロトコル毎	FTPサマリーログ
プロトコル毎	OTHERサマリーログ
プロトコル毎	ROPサマリーログ
プロトコル毎	SCPサマリーログ
プロトコル毎	SFTPサマリーログ
プロトコル毎	SSHサマリーログ
プロトコル毎	TELNETサマリーログ
プロトコル毎	TNSサマリーログ

検索テンプレート一覧

検索-2

検索条件テンプレート名	概要
AccessCheckのメンテナンスログイン・ログオフ	ELC利用時の検索
AccessCheckを経由しないリモートログイン	ELC利用時の検索
Windowsイベントログ	AC標準レポート
アクセス一覧	AC標準レポート
アクセス申請一覧	AC標準レポート
アクセス申請時間超過アクセス一覧	AC標準レポート
アクセス申請機能によるアクセス拒否一覧	AC標準レポート
グローバル管理者画面操作履歴	管理画面操作履歴ログ
マスタ管理者画面操作履歴	管理画面操作履歴ログ
ログイン履歴（グローバル管理者）	グローバル管理者権限で閲覧できるログイン履歴ログ
ログイン履歴（監査者）	監査者権限で閲覧できるログイン履歴ログ
ログイン履歴（管理者）	管理者権限で閲覧できるログイン履歴ログ
ログ収集対象機器のローカルログイン	ELC利用時の検索
特定キーワードが含まれる申請書リスト	日次レポートにある申請情報のうち、件名、内容、備考の中に、特定文字列がある場合にリストアップ
特定ファイルサイズ以上の流入流出	日次レポートにある流出データ量、流入データ量が、特定量以上のものをリストアップ
管理者画面操作履歴	管理画面操作履歴ログ
長時間アクセスログ	日次レポートにあるアクセス開始、終了から接続時間を計算し、特定時間以上のログをリストアップ（初期値:21600秒/6時間）

集計テンプレート一覧

集計

Logstorage Access Check 連携パック の集計テンプレートは以下の通りです。

集計条件テンプレート名	概要
アクセス数が多いノードトップ10	-
アクセス数が多いユーザトップ10	-
アクセス数が少ないノードトップ10	-
アクセス数が少ないユーザトップ10	-
エラー出力が多いユーザトップ10	-
エラー出力が多い原因トップ10	-
データ流出・流出量の推移	-
利用アカウントリスト	-
利用数が多いプロトコルトップ10	-
単位時間当たりのアクセス失敗が多いユーザとその接続試行先	日別／ユーザ毎の集計値が10件以上の場合に表示します。
単位時間当たりのアクセス失敗が多い接続試行先とそのユーザ	日別／接続先サーバ毎の集計値が10件以上の場合に表示します。
承認者ごとの承認数	-
接続時間が長いユーザトップ10	-

レポートテンプレート一覧

レポート

Logstorage Access Check 連携パック のレポートテンプレートは以下の通りです。

レポート条件テンプレート名
AccessCheckのメンテナンスログイン・ログオフ
AccessCheckを経由しないリモートログイン
Windowsイベントログ
アクセス一覧
アクセス数が多いノードトップ10
アクセス数が多いユーザトップ10
アクセス数が少ないノードトップ10
アクセス数が少ないユーザトップ10
アクセス申請一覧
アクセス申請時間超過アクセス一覧
アクセス申請機能によるアクセス拒否一覧
エラー出力が多いユーザトップ10
エラー出力が多い原因トップ10
データ流入・流出量の推移
ログ収集対象機器のローカルログイン
利用アカウントリスト
利用数が多いプロトコルトップ10
単位時間当たりのアクセス失敗が多いユーザとその接続試行先
単位時間当たりのアクセス失敗が多い接続試行先とそのユーザ
承認者ごとの承認数
接続時間が長いユーザトップ10
特定キーワードが含まれる申請書リスト
特定ファイルサイズ以上の流入流出
長時間アクセスログ

レポート例 1

[AccessCheck5]アクセス一覧

概要
作成日　2019-01-10 14:23:43
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

検索条件名　[AccessCheck5]アクセス一覧
概要　AC標準レポート
件数　166件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	アクセス開始日時	アクセス終了日時	接続時間	アクセス結果	AccessUI	ユーザアカウント	接続元クライアントアドレス	接続先サーバ情報	プロトコル	ポート番号	流出データ量(byte)	流入データ量(byte)	アクセス申請No	アクセス申請No1	アクセス申請
2018-05-23 10:13:24	AccessCheck5	アクセスログ	2018-05-23 10:13:24	2018-05-23 10:14:09	45	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	1708	23000			
2018-05-23 10:13:24	AccessCheck5	アクセスログ	2018-05-23 10:13:24	2018-05-23 10:13:24	0	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	312	318			
2018-05-23 10:13:24	AccessCheck5	アクセスログ			45												
2018-05-23 10:13:24	AccessCheck5	アクセスログ			0												
2018-05-23 10:13:57	AccessCheck5	アクセスログ	2018-05-23 10:13:57	2018-05-23 10:13:57	0	ポリシー無し	gatewayserver_001	user1277	192.168.50.23	192.168.50.175	http	81					
2018-05-23 10:13:57	AccessCheck5	アクセスログ			0												
2018-05-23 10:22:37	AccessCheck5	アクセスログ	2018-05-23 10:22:37	2018-05-23 10:22:49	12	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2270	1381			
2018-05-23 10:22:37	AccessCheck5	アクセスログ	2018-05-23 10:22:37	2018-05-23 10:22:37	0	ポリシー無し	gatewayserver_001	user1277	192.168.50.23	192.168.50.175	http	81					
2018-05-23 10:22:37	AccessCheck5	アクセスログ			12												
2018-05-23 10:22:37	AccessCheck5	アクセスログ			0												
2018-05-23 10:22:45	AccessCheck5	アクセスログ	2018-05-23 10:22:45	2018-05-23 10:22:45	0	ポリシー無し	gatewayserver_001	user1277	192.168.50.23	192.168.50.175	http	81					
2018-05-23 10:22:45	AccessCheck5	アクセスログ			0												
2018-05-23 10:22:49	AccessCheck5	アクセスログ	2018-05-23 10:22:49	2018-05-23 10:22:49	0	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	261	318			
2018-05-23 10:22:49	AccessCheck5	アクセスログ			0												
2018-05-23 10:25:46	AccessCheck5	アクセスログ	2018-05-23 10:25:46	2018-05-23 10:26:12	26	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2529	23244			
2018-05-23 10:25:46	AccessCheck5	アクセスログ	2018-05-23 10:25:46	2018-05-23 10:25:46	0	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	312	318			
2018-05-23 10:25:46	AccessCheck5	アクセスログ			26												
2018-05-23 10:25:46	AccessCheck5	アクセスログ			0												
2018-05-23 10:25:58	AccessCheck5	アクセスログ	2018-05-23 10:25:58	2018-05-23 10:25:58	0	ポリシー無し	gatewayserver_001	user1277	192.168.50.23	192.168.50.175	http	81					
2018-05-23 10:25:58	AccessCheck5	アクセスログ			0												
2018-05-23 11:25:23	AccessCheck5	アクセスログ	2018-05-23 11:25:23	2018-05-23 11:25:43	20	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2529	23244			
2018-05-23 11:25:23	AccessCheck5	アクセスログ	2018-05-23 11:25:23	2018-05-23 11:25:23	0	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	312	318			
2018-05-23 11:25:23	AccessCheck5	アクセスログ			20												
2018-05-23 11:25:23	AccessCheck5	アクセスログ			0												
2018-05-23 11:25:31	AccessCheck5	アクセスログ	2018-05-23 11:25:31	2018-05-23 11:25:31	0	ポリシー無し	gatewayserver_001	user1277	192.168.50.23	192.168.50.175	http	81					
2018-05-23 11:25:31	AccessCheck5	アクセスログ			0												
2018-05-23 11:27:28	AccessCheck5	アクセスログ	2018-05-23 11:27:28	2018-05-23 11:28:23	55	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	5068	23976			
2018-05-23 11:27:28	AccessCheck5	アクセスログ	2018-05-23 11:27:28	2018-05-23 11:28:13	45	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	2000	918			
2018-05-23 11:27:28	AccessCheck5	アクセスログ			55												
2018-05-23 11:27:28	AccessCheck5	アクセスログ			45												
2018-05-23 11:28:19	AccessCheck5	アクセスログ	2018-05-23 11:28:19	2018-05-23 11:28:19	0	ポリシー無し	gatewayserver_001	user1277	192.168.50.23	192.168.50.175	http	81					

SecureCube Access Check が作成する「日次レポート」に含まれる「アクセスログ」を一覧表示します

レポート例 2

[AccessCheck5]アクセス申請一覧

概要
作成日　2019-01-10 14:23:48
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

検索条件名　[AccessCheck5]アクセス申請一覧
概要　AC標準レポート
件数　18件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	アクセス申請No	件名	内容	備考	アクセス開始日時	アクセス終了日時	アクセス予定曜日	ポリシーID	操作ログ取得フラグ	承認レベル	アクセス通知メールフラグ	申請・承認通知処理種別	申請状態最終更新	申請状態	申請者
2018-09-05 09:45:00	AccessCheck5	アクセス申請の一覧	20180905A00013	定期アクセステスト001	定期アクセスのテストを行います。(1回目)		2018-09-05 09:45:00	2018-09-09 09:45:00	Wed,Fri,Sun	policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-06 00:30:06	取消	user00
2018-09-05 10:40:00	AccessCheck5	アクセス申請の一覧	20180905A00016	定期アクセステスト_user001_01	aaaaaa		2018-09-05 10:40:00	2018-09-07 10:38:00	Wed,Fri,Sun	policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-05 10:46:36	確認済み	user00
2018-09-05 10:50:00	AccessCheck5	アクセス申請の一覧	20180905A00017	定期アクセステスト	定期アクセスのテスト		2018-09-05 10:50:00	2018-09-07 10:48:00	Wed,Fri	policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 06:45:52	作業完了	user00
2018-09-06 00:32:00	AccessCheck5	アクセス申請の一覧	20180906A00000	種のテスト	種のテスト		2018-09-06 00:32:00	2018-09-07 00:30:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 01:59:21	却下	user00
2018-09-07 02:05:00	AccessCheck5	アクセス申請の一覧	20180907A00000	アクセス申請	acuiテスト		2018-09-07 02:05:00	2018-09-08 02:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 02:09:57	取消	user00
2018-09-07 02:12:00	AccessCheck5	アクセス申請の一覧	20180907A00001	アクセス申請	テスト		2018-09-07 02:12:00	2018-09-08 02:10:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 08:35:48	作業完了	user00
2018-09-07 04:43:00	AccessCheck5	アクセス申請の一覧	20180907A00002	タイムゾーンテスト	タイムゾーンの違いによるテストを行う		2018-09-07 04:43:00	2018-09-07 04:50:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 07:22:57	作業完了	user00
2018-09-07 05:41:00	AccessCheck5	アクセス申請の一覧	20180907A00003	アクセス申請テスト	タイムゾーンテスト		2018-09-07 05:41:00	2018-09-07 05:45:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 07:23:06	作業完了	user00
2018-09-07 06:48:00	AccessCheck5	アクセス申請の一覧	20180907A00004	中継テスト	各中継を行う		2018-09-07 06:48:00	2018-09-09 06:46:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 06:57:16	作業完了	user00
2018-09-07 07:02:00	AccessCheck5	アクセス申請の一覧	20180907A00005	あ	あ		2018-09-07 07:02:00	2018-09-07 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 08:27:52	作業完了	user00
2018-09-07 07:25:00	AccessCheck5	アクセス申請の一覧	20180907A00006	中継テスト	テスト		2018-09-07 07:25:00	2018-09-07 09:23:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 08:35:57	作業完了	user00
2018-09-07 07:55:00	AccessCheck5	アクセス申請の一覧	20180907A00007	test	tns,cifs		2018-09-07 07:55:00	2018-09-07 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 08:28:01	却下	user00
2018-09-07 08:30:00	AccessCheck5	アクセス申請の一覧	20180907A00008	再起動後の中継テスト	再起動後の中継テスト		2018-09-07 08:30:00	2018-09-08 08:28:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 09:49:13	作業完了	user00
2018-09-07 08:50:00	AccessCheck5	アクセス申請の一覧	20180907A00009	中継テストRDP	中継テストRDP		2018-09-07 08:50:00	2018-09-08 08:49:00		policy_005	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 09:47:59	事後承認済み	user00
2018-09-07 09:29:00	AccessCheck5	アクセス申請の一覧	20180907A00010	test	tns		2018-09-07 09:29:00	2018-09-07 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 09:50:16	取消	user00
2018-09-07 09:53:00	AccessCheck5	アクセス申請の一覧	20180907A00011	test	tns		2018-09-07 09:53:00	2018-09-09 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 10:31:16	作業完了	user00
2018-09-07 10:47:00	AccessCheck5	アクセス申請の一覧	20180907A00012	test	ノード指定込		2018-09-07 10:47:00	2018-09-08 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 10:56:39	取消	user00
2018-09-07 10:59:00	AccessCheck5	アクセス申請の一覧	20180907A00013	test	ノード指定無し		2018-09-07 10:59:00	2018-09-09 00:00:00		policy_005	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 10:57:38	承認待ち	user00

SecureCube Access Check が作成する「日次レポート」に含まれる「アクセス申請の一覧」を一覧表示します

レポート例 3

[AccessCheck5]アクセス申請機能によるアクセス拒否一覧

概要
作成日　2019-01-10 14:23:58
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

検索条件名　[AccessCheck5]アクセス申請機能によるアクセス拒否一覧
概要　AC標準レポート
件数　37件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	ユーザアカウント	アクセス開始日時	接続元クライアントアドレス	ポート番号	アクセス拒否理由	アクセス申請No
2018-05-23 10:13:57	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 10:13:57	192.168.50.23	81	ポリシー無し	
2018-05-23 10:22:37	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 10:22:37	192.168.50.23	81	ポリシー無し	
2018-05-23 10:22:45	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 10:22:45	192.168.50.23	81	ポリシー無し	
2018-05-23 10:25:58	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 10:25:58	192.168.50.23	81	ポリシー無し	
2018-05-23 11:25:31	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:25:31	192.168.50.23	81	ポリシー無し	
2018-05-23 11:28:19	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:28:19	192.168.50.23	81	ポリシー無し	
2018-05-23 11:46:14	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:46:14	192.168.50.23	81	ポリシー無し	
2018-05-23 11:50:35	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:50:35	192.168.50.23	81	ポリシー無し	
2018-05-23 11:50:59	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:50:59	192.168.50.23	81	ポリシー無し	
2018-05-23 11:51:06	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:51:06	192.168.50.23	81	ポリシー無し	
2018-05-23 11:56:27	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 11:56:27	192.168.50.23	81	ポリシー無し	
2018-05-23 13:17:21	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 13:17:21	192.168.50.23	81	ポリシー無し	
2018-05-23 13:25:12	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 13:25:12	192.168.50.23	81	ポリシー無し	
2018-05-23 13:26:40	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 13:26:40	192.168.50.23	81	ポリシー無し	
2018-05-23 14:49:53	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 14:49:53	192.168.50.23	81	ポリシー無し	
2018-05-23 15:06:41	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 15:06:41	192.168.50.23	81	ポリシー無し	
2018-05-23 15:56:35	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 15:56:35	192.168.50.23	81	ポリシー無し	
2018-05-23 16:12:09	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 16:12:09	192.168.50.23	81	ポリシー無し	
2018-05-23 16:28:21	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 16:28:21	192.168.50.23	81	ポリシー無し	
2018-05-23 16:34:57	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 16:34:57	192.168.50.23	81	ポリシー無し	
2018-05-23 16:40:04	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 16:40:04	192.168.50.23	81	ポリシー無し	
2018-05-23 16:43:38	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 16:43:38	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:31	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:31	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:34	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:34	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:35	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:35	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:40	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:40	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:43	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:43	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:46	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:46	192.168.50.23	81	ポリシー無し	
2018-05-23 17:01:49	AccessCheck5	アクセス申請機能による規制履歴	user1277	2018-05-23 17:01:49	192.168.50.23	81	ポリシー無し	

SecureCube Access Check が作成する「日次レポート」に含まれる
「アクセス申請機能によって接続ノードへの中継接続が拒否されたログ」を一覧表示します

レポート例 4

[AccessCheck5]アクセス申請時間超過アクセス一覧

概要
作成日　2019-01-10 14:23:53
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

検索条件名　[AccessCheck5]アクセス申請時間超過アクセス一覧
概要　AC標準レポート
件数　3件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	ユーザアカウント	アクセス開始日時	アクセス終了日時	接続元クライアントアドレス	ポート番号	申請時間超過結果	アクセス申請No
2018-05-23 17:01:31	AccessCheck5	アクセス申請時間超過アクセス履歴	user1277	2018-05-23 17:01:31	2018-05-23 17:02:12	192.168.50.23	81	超過	
2018-09-07 04:48:07	AccessCheck5	アクセス申請時間超過アクセス履歴	user003	2018-09-07 04:48:07	2018-09-07 04:48:52	192.168.50.46	22	超過	20180907A00002
2018-09-07 05:41:05	AccessCheck5	アクセス申請時間超過アクセス履歴	user003	2018-09-07 05:41:05	2018-09-07 05:41:12	192.168.50.46	22	超過	20180907A00003

SecureCube Access Check が作成する「日次レポート」に含まれる
「アクセス申請を利用した中継接続でアクセス予定時間より超過したログ」を一覧表示します

レポート例 5

[AccessCheck5]長時間アクセスログ

概要
作成日　2019-01-10 14:35:03
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

検索条件名　[AccessCheck5]長時間アクセスログ
概要　日次レポートにあるアクセス開始、終了から接続時間を計算し、特定時間以上のログをリストアップ (初期値:21600秒/6時間)
件数　3件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	アクセス開始日時	アクセス終了日時	接続時間	アクセス結果	AccessUI	ユーザアカウント	接続元クライアントアドレス	接続先サーバ情報	プロトコル	ポート番号	流出データ量(byte)	流入データ量(byte)	アクセス申請No	アクセス申請No1	アクセス申請No2
2018-05-23 10:13:24	AccessCheck5	アクセスログ	2018-05-23 10:13:24	2018-05-23 10:14:09	21611	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	1708	23000			
2018-05-23 10:13:24	AccessCheck5	アクセスログ	2018-05-23 10:13:24	2018-05-23 10:13:24	32544	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	312	318			
2018-05-23 10:22:37	AccessCheck5	アクセスログ	2018-05-23 10:22:37	2018-05-23 10:22:49	88135	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2270	1381			

アクセス開始から終了までの時間が、指定時間以上のログをリストアップして表示します

※指定時間はデフォルトで21,600秒（6時間）です。ユーザー様のニーズに合わせて変更可能です

レポート例 6

[AccessCheck5]特定キーワードが含まれる申請書リスト

概要
作成日　2019-01-10 14:24:08
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

検索条件名　[AccessCheck5]特定キーワードが含まれる申請書リスト
概要　日次レポートにある申請情報のうち、件名、内容、備考の中に、特定文字列がある場合にリストアップ
件数　5件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	アクセス申請No	件名	内容	備考	アクセス開始日時	アクセス終了日時	アクセス予定曜日	ポリシーID	操作ログ取得フラグ	承認レベル	アクセス通知メールフラグ	申請・承認通知処理種別	申請状態最終更新	申請状態	申請者アカウント	申請者名	ユーザアカウント	承認者
2018-09-07 07:55:00	AccessCheck5	アクセス申請の一覧	20180907A00007	test	tns,cifs		2018-09-07 07:55:00	2018-09-07 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 08:28:01	却下	user001	ユーザ001	user001	
2018-09-07 09:29:00	AccessCheck5	アクセス申請の一覧	20180907A00010	test	tns		2018-09-07 09:29:00	2018-09-07 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 09:50:16	取消	user001	ユーザ001	user001	app_us
2018-09-07 09:53:00	AccessCheck5	アクセス申請の一覧	20180907A00011	test	tns		2018-09-07 09:53:00	2018-09-09 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 10:31:16	作業完了	user001	ユーザ001	user001	
2018-09-07 10:47:00	AccessCheck5	アクセス申請の一覧	20180907A00012	test	ノード指定込		2018-09-07 10:47:00	2018-09-08 15:00:00		policy_001	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 10:56:39	取消	user001	ユーザ001	user001	
2018-09-07 10:59:00	AccessCheck5	アクセス申請の一覧	20180907A00013	test	ノード指定無し		2018-09-07 10:59:00	2018-09-09 00:00:00		policy_005	全文ログ取得有り	事前申請が必要	送信有り	送信する	2018-09-07 10:57:38	承認待ち	user001	ユーザ001	user001	

申請情報のうち、件名、内容、備考の中に特定文字列があるログをリストアップして表示します

※デフォルトでは「test」の文字列が含まれるものをリストアップします。ユーザー様のニーズに合わせて変更可能です

レポート例 7

[AccessCheck5]特定ファイルサイズ以上の流入流出

概要
作成日　2019-01-10 14:24:13
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

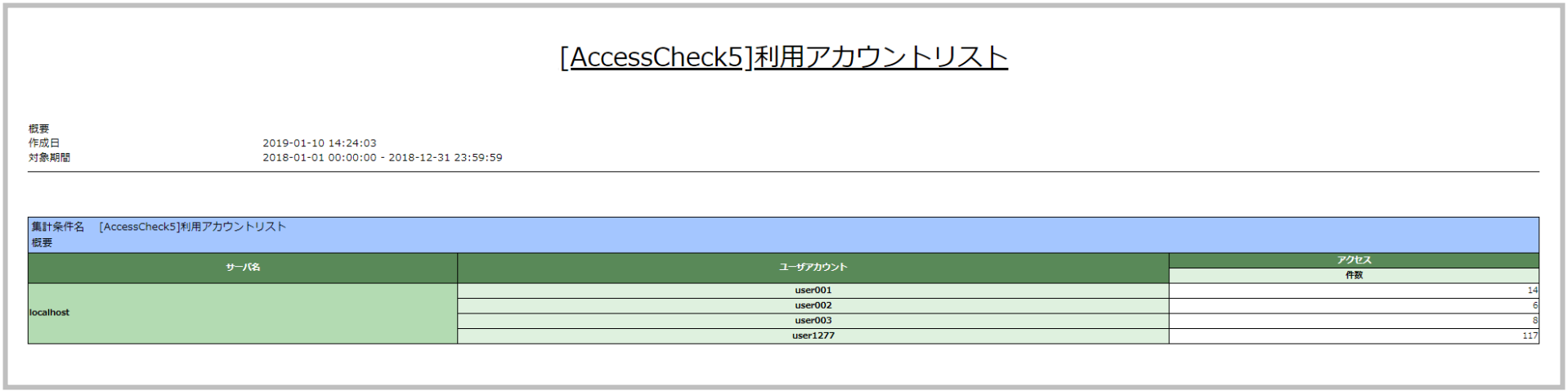
検索条件名　[AccessCheck5]特定ファイルサイズ以上の流入流出
概要　日次レポートにある流出データ量、流入データ量が、特定量以上のものをリストアップ
件数　39件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	アクセス開始日時	アクセス終了日時	接続時間	アクセス結果	AccessUI	ユーザアカウント	接続元クライアントアドレス	接続先サーバ情報	プロトコル	ポート番号	流出データ量(byte)	流入データ量(byte)	アクセス申請No	アクセス申請No1	アクセス申請
2018-05-23 10:13:24	AccessCheck5	アクセスログ	2018-05-23 10:13:24	2018-05-23 10:14:09	45	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	1708	23000			
2018-05-23 10:22:37	AccessCheck5	アクセスログ	2018-05-23 10:22:37	2018-05-23 10:22:49	12	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2270	1381			
2018-05-23 10:25:46	AccessCheck5	アクセスログ	2018-05-23 10:25:46	2018-05-23 10:26:12	26	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2529	23244			
2018-05-23 11:25:23	AccessCheck5	アクセスログ	2018-05-23 11:25:23	2018-05-23 11:25:43	20	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2529	23244			
2018-05-23 11:27:28	AccessCheck5	アクセスログ	2018-05-23 11:27:28	2018-05-23 11:28:23	55	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	5068	23976			
2018-05-23 11:27:28	AccessCheck5	アクセスログ	2018-05-23 11:27:28	2018-05-23 11:28:13	45	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	2000	918			
2018-05-23 11:45:47	AccessCheck5	アクセスログ	2018-05-23 11:45:47	2018-05-23 11:46:17	30	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	4228	23732			
2018-05-23 11:45:47	AccessCheck5	アクセスログ	2018-05-23 11:45:47	2018-05-23 11:46:05	18	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	1578	768			
2018-05-23 11:50:27	AccessCheck5	アクセスログ	2018-05-23 11:50:27	2018-05-23 11:51:16	49	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	5639	24869			
2018-05-23 11:50:27	AccessCheck5	アクセスログ	2018-05-23 11:50:27	2018-05-23 11:51:10	43	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	573	636			
2018-05-23 11:56:21	AccessCheck5	アクセスログ	2018-05-23 11:56:21	2018-05-23 11:56:41	20	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	2529	23244			
2018-05-23 13:17:21	AccessCheck5	アクセスログ	2018-05-23 13:17:21	2018-05-23 13:17:29	8	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	1449	1137			
2018-05-23 13:25:03	AccessCheck5	アクセスログ	2018-05-23 13:25:03	2018-05-23 13:26:46	103	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	7597	47220			
2018-05-23 13:26:17	AccessCheck5	アクセスログ	2018-05-23 13:26:17	2018-05-23 13:26:35	18	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	2000	918			
2018-05-23 14:49:30	AccessCheck5	アクセスログ	2018-05-23 14:49:30	2018-05-23 14:50:00	30	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	5889	24220			
2018-05-23 14:49:30	AccessCheck5	アクセスログ	2018-05-23 14:49:30	2018-05-23 14:49:49	19	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	2000	918			
2018-05-23 15:06:10	AccessCheck5	アクセスログ	2018-05-23 15:06:10	2018-05-23 15:06:43	33	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	3388	23488			
2018-05-23 15:06:10	AccessCheck5	アクセスログ	2018-05-23 15:06:10	2018-05-23 15:06:34	24	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	1156	618			
2018-05-23 15:56:15	AccessCheck5	アクセスログ	2018-05-23 15:56:15	2018-05-23 15:56:39	24	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	4228	23732			
2018-05-23 15:56:15	AccessCheck5	アクセスログ	2018-05-23 15:56:15	2018-05-23 15:56:30	15	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	1578	768			
2018-05-23 16:11:26	AccessCheck5	アクセスログ	2018-05-23 16:11:26	2018-05-23 16:12:12	46	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	9268	25196			
2018-05-23 16:11:26	AccessCheck5	アクセスログ	2018-05-23 16:11:26	2018-05-23 16:12:01	35	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	4110	1668			
2018-05-23 16:28:08	AccessCheck5	アクセスログ	2018-05-23 16:28:08	2018-05-23 16:28:28	20	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	5049	23976			
2018-05-23 16:28:08	AccessCheck5	アクセスログ	2018-05-23 16:28:08	2018-05-23 16:28:18	10	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	1578	768			
2018-05-23 16:34:31	AccessCheck5	アクセスログ	2018-05-23 16:34:31	2018-05-23 16:35:02	31	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	8409	24952			
2018-05-23 16:34:31	AccessCheck5	アクセスログ	2018-05-23 16:34:31	2018-05-23 16:34:54	23	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	3266	1368			
2018-05-23 16:39:53	AccessCheck5	アクセスログ	2018-05-23 16:39:53	2018-05-23 16:40:53	60	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	7474	24708			
2018-05-23 16:39:53	AccessCheck5	アクセスログ	2018-05-23 16:39:53	2018-05-23 16:39:58	5	認可OK	gatewayserver_001	user1277	192.168.50.23	GET /	http	81	734	468			
2018-05-23 16:43:21	AccessCheck5	アクセスログ	2018-05-23 16:43:21	2018-05-23 16:43:46	25	認可OK	gatewayserver_001	user1277	192.168.50.23	GET http://192.168.50.1/IT_test/http/31.html	http	81	4209	23732			

流出データ量、流入データ量が、特定量以上のものをリストアップして表示します

※デフォルトでは「500byte」以上のデータ量が含まれるログをリストアップします。ユーザー様のニーズに合わせて変更可能です

レポート例 8



[AccessCheck5]利用アカウントリスト

概要
作成日　2019-01-10 14:24:03
対象期間　2018-01-01 00:00:00 - 2018-12-31 23:59:59

集計条件名　[AccessCheck5]利用アカウントリスト
概要

サーバ名	ユーザアカウント	アクセス 件数
localhost	user001	14
	user002	6
	user003	8
	user1277	117

アクセスの際に利用されたユーザアカウント情報とアクセス件数を表示します

お問い合わせ

ご不明点、ご相談につきましては、下記お問い合わせ先からご連絡ください。

電話でのお問い合わせ

03-5427-3503

【受付】平日 9:00～17:30

メールでのお問い合わせ

info@logstorage.com

会社名・氏名・メールアドレス・電話番号を
ご記入の上、お問い合わせください

当社のホームページでも資料請求・お問い合わせができます。
https://logstorage.com