Slackプランの比較

Audit logs

Enterprise Selectプランであれば、全ての会話ログに加え監査ログの取得も可能です。

	プラン	Free	Pro	Business +	Enterprise Select	Enterprise Grid
会話データ	パブリックチャンネル	✅	✅	✅	✅	✅
	プライベートチャンネル	ー	ー	✅	✅	✅
	ダイレクトメッセージ	ー	ー	✅	✅	✅
	編集・削除証跡ログ	ー	✅	✅	✅	✅
	指定したスケジュールでのエクスポート	ー	ー	✅	✅	ー
	単一ユーザーを対象にしたエクスポート※	ー	ー	ー	✅	✅
監査ログ	各種操作ログ等	ー	ー	ー	✅	✅
	ワークスペースへのアクセスログ	ワークスペース管理機能で取得可能				

※ .txt形式、その他の会話データはJSON形式でエクスポートされます

（参考）監査ログ 取得可能なイベントとその内容 1

以下は、Audit Log APIで取得可能なイベントの一覧（一部抜粋）になります。

	アクション	詳細内容
ワークスペース	workspace_created	対象OrG環境にて新規にワークスペースが作成された
	emoji_removed	対象OrG環境からリアクション絵文字が削除された（名称含む）
	pref.dm_retention_changed	ダイレクトメッセージ保存期限が設定（または更新）された
	pref.sso_setting_changed	SSO（シングルサインオン）設定が変更（更新）された
チャンネル	user_channel_join	ユーザーがチャンネルに参加した（共有チャンネル内の情報含む）
	private_channel_created	プライベートチャンネルが作成された
	guest_created	ゲストがチャンネルに招待された
	public_channel_deleted	パブリックチャンネルが削除された

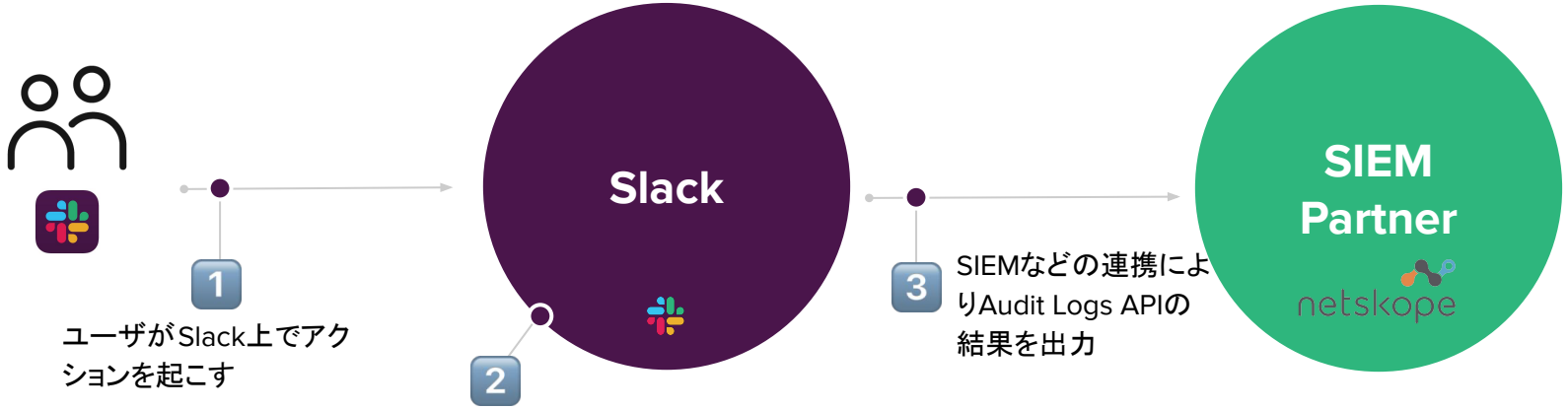
（参考）監査ログ 取得可能なイベントとその内容 2

以下は、Audit Log APIで取得可能なイベントの一覧（一部抜粋）になります。

	アクション	詳細内容
ユーザ	user_login	ワークスペースにユーザがログイン（サインオン）した
	role_change_to_admin	ユーザ権限が〇〇〇から管理者へ変更された
	guest_expiration_set	ゲストユーザの有効期限が設定（更新）された
	custom_tos_accepted	ユーザによってカスタムのサービス利用規約がAcceptされた
ファイル	file_downloaded	ファイルがダウンロードされた
	file_uploaded	ファイルがアップロードされた
	file_public_link_created	該当ファイルに外部共有用のリンクが設定された
	file_shared	ファイルが異なるチャンネルに共有された

Audit logs

Slack Audit Logs



SIEM連携による価値 *(SIEMの機能に依存)*

- JSONフォーマットの出力により、一般的なSIEMやデータベースとの連携が容易
- 契約が有効な限りは全イベントを保持
- Orgレベル、あるいはワークスペースレベルでの出力に対応

技術的な詳細

- Org Ownerのみ利用できるAPIトークンが必要で一般ユーザは活用できない
- イベントの種類、タイムスタンプ、誰がいつ何を行ったか、何が影響を受けたのかなどの詳細を提供
- Audit Logs APIのrate limitは50コール/分

監査ログの例

監査ログの例 APIによりJSON形式で取得：ユーザーがログインした時のログエントリーの例

エントリーのIDと作成日

action:実施したアクションの種類

actor:アクションを行なったユーザーに関する情報

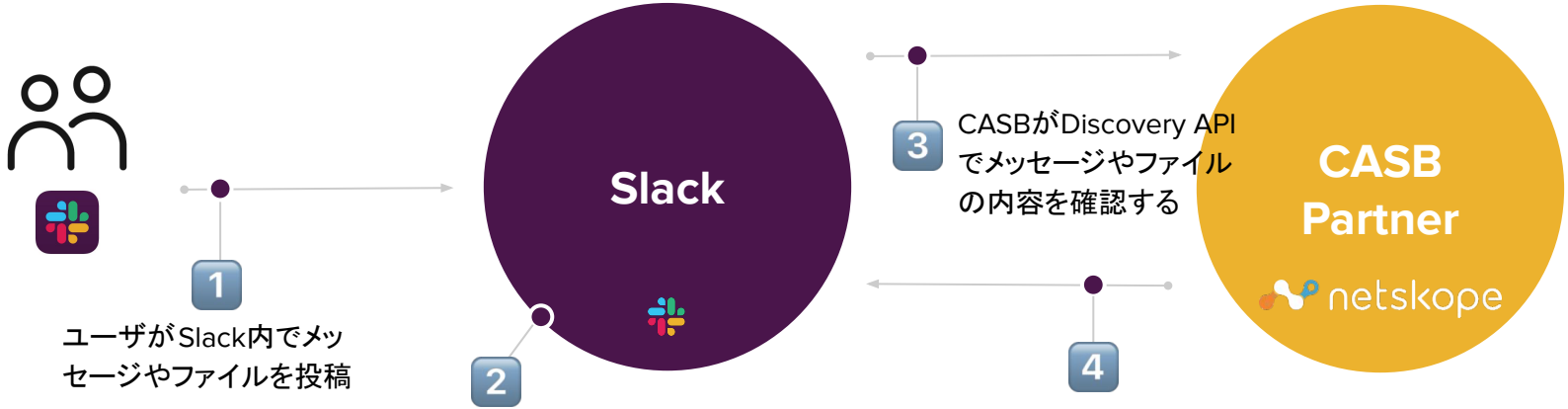
entity:アクションの対象の情報(例：loginの場合はユーザー、filedownloadの場はファイル、channel_jonの場合はチャンネル）

context:entityに対してactionを行なったロケーション情報（typeは、enterpriseかworkspaceの2種類で、enterpriseの場合は組織情報、workspaceの場合はワークスペース情報)

ua/ip:クライアントのUgerAgent情報とIPアドレス

詳細はヘルプ参照：https://bit.ly/2VLSnmH

Discovery API による Data Loss Prevention (DLP)



CASB連携による価値 *(CASB側の機能に依存)*

- Slackの利用状況をほぼリアルタイムに監視
- コンプライアンス違反など行動への自動的な対処
- コンテンツの削除や管理者の承認が得られるまでの隔離など柔軟なポリシーを適用可能
- CASBのBotで違反行動が検知された旨を通知

技術的な詳細

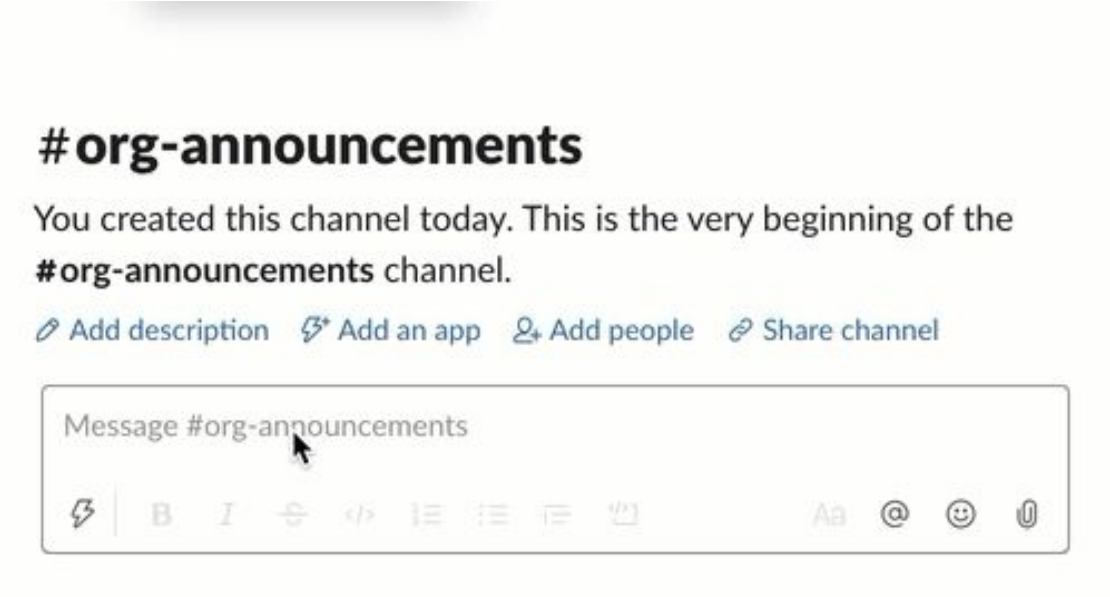
- APIの利用はプライマリーオーナー権限が必須
- Org内の全てのメッセージやファイルへのRead/Write/Delete アクセス
- 編集や削除の履歴も把握が可能
- Discovery APIのrate limitは30コール/秒

Discovery API

Data Loss Prevention(DLP)

機能紹介：
主要なクラウドアクセスセキュリティブローカー(CASB)を使用して、事前定義されたポリシーに違反するSlackメッセージおよびファイル内のコンテンツをスキャンします。

DLPがないリスク：
DLPがないと、従業員は内部または外部の公開チャネルで機密情報を誤って(投稿またはファイルのアップロードを介して)共有するリスクがあります。



効果：上記のように個人情報または事前定義されたポリシーに違反したメッセージやファイルが投稿された場合、システムが検知し自動的に投稿を削除し、警告メッセージに置き換えることができる。

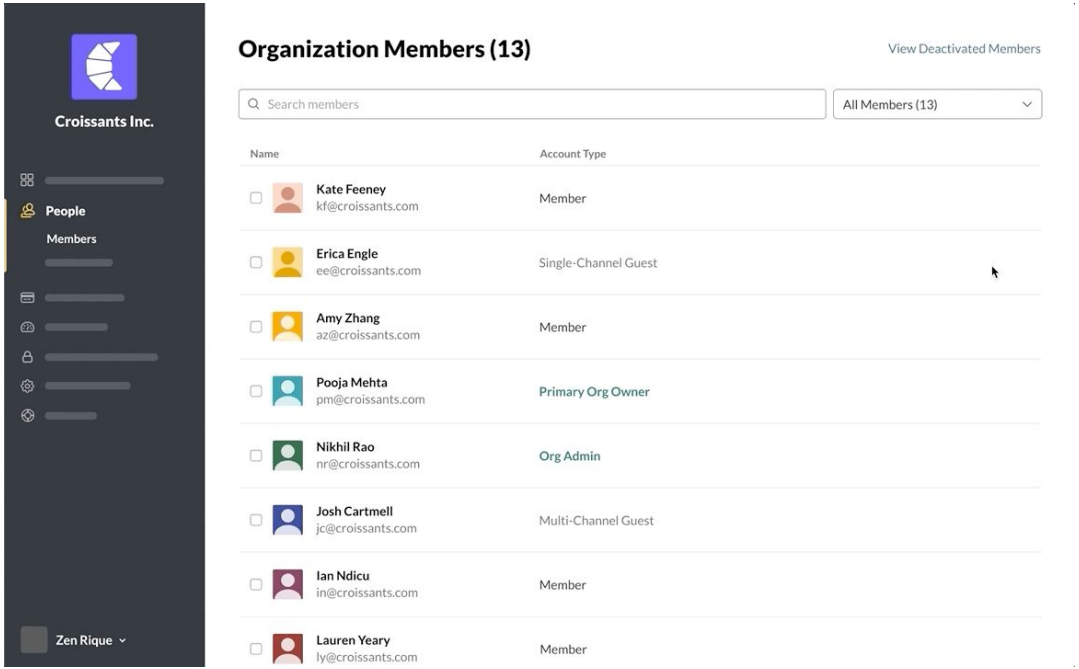
1: DLP ROI Study

Enterprise Selectプランにおける特殊なセキュリティ機能

強制サインアウト機能

機能紹介:

特定のユーザーに紐付いた
モバイルセッション
デスクトップセッション
をリモートで解除します。



強制サインアウト

貴社へのメリット：

ユーザーが端末を紛失したり盗難に遭った場合、管理者が遠隔操作で Slack から強制的にサインアウトさせ、自社の情報を安全に保てます。

強制
サインアウト

参考ヘルプ記事

オーガナイゼーションからメンバーをサインアウトさせる

https://slack.com/intl/ja-jp/help/articles/360041717053


slack