Azure Active Directory
監視サービス

Azure Active Directory監視サービス 概要

サービス概要

認証基盤としてAzure Active Directory（以降Azure ADと呼称）を利用する企業様を狙う不審な動きを監視し、不正アクセスの兆候が見られた場合はご担当者様へお知らせするサービスです。

特長

本サービスの特長は、以下になります。

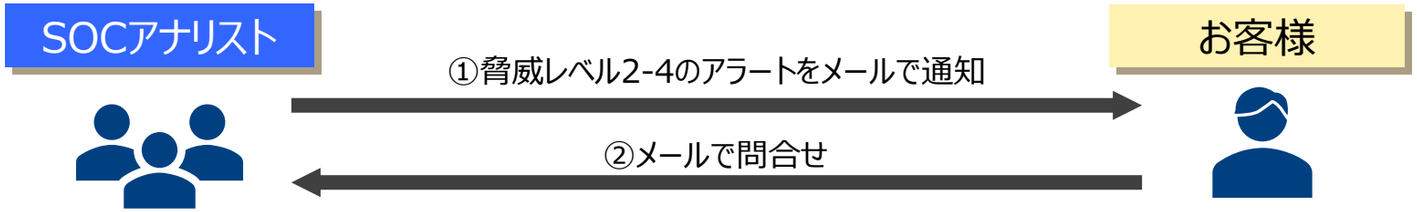
・Identity Protectionにて検出された内容を分析し、4段階の脅威レベルに分類します。

・24時間365日体制で監視を行います。

・24時間365日体制で不審なアカウントをアナリストがセッション切断および無効化します。(オプション)

セキュリティインシデント発生時のエスカレーションフロー／脅威判断基準

監視デバイスのセキュリティアラートを監視し、SOCアナリストが判断した脅威レベル2～4のアラートに対して、
メールにてエスカレーション通知を行います。お客様は、必要に応じてポータルサイトにてお問い合わせが可能です。



「セキュリティアラート脅威判定基準」

SOC 脅威レベル	判断基準	監視内容	通知手段
レベル4	複数のアカウントで不正なログインが強く疑われるイベント	・アラート分析 ・アカウント隔離(※)	メールおよび電話
レベル3	1つのアカウントで不正なログインが強く疑われるイベント		メール
レベル2	安全であるか判断できないイベント	・アラート分析	メール
レベル1	検知されたアラートの内、アナリストの分析で問題なしと判断できたイベント	・アラート分析	なし

(※) アカウント隔離の実施は別途「遠隔操作オプション」をご契約いただく必要がございます。
※ セキュリティ製品の脅威判定を使用せずに、当社独自の4段階の脅威レベルで判断します。
※ アラート分析の結果、レベル1と判断した場合は、製品での脅威レベルにかかわらず、ご連絡（エスカレーション）はございません。

Azure Active Directory監視サービス 監視内容

- **対応製品：**
  Azure Active Directory Identity Protection

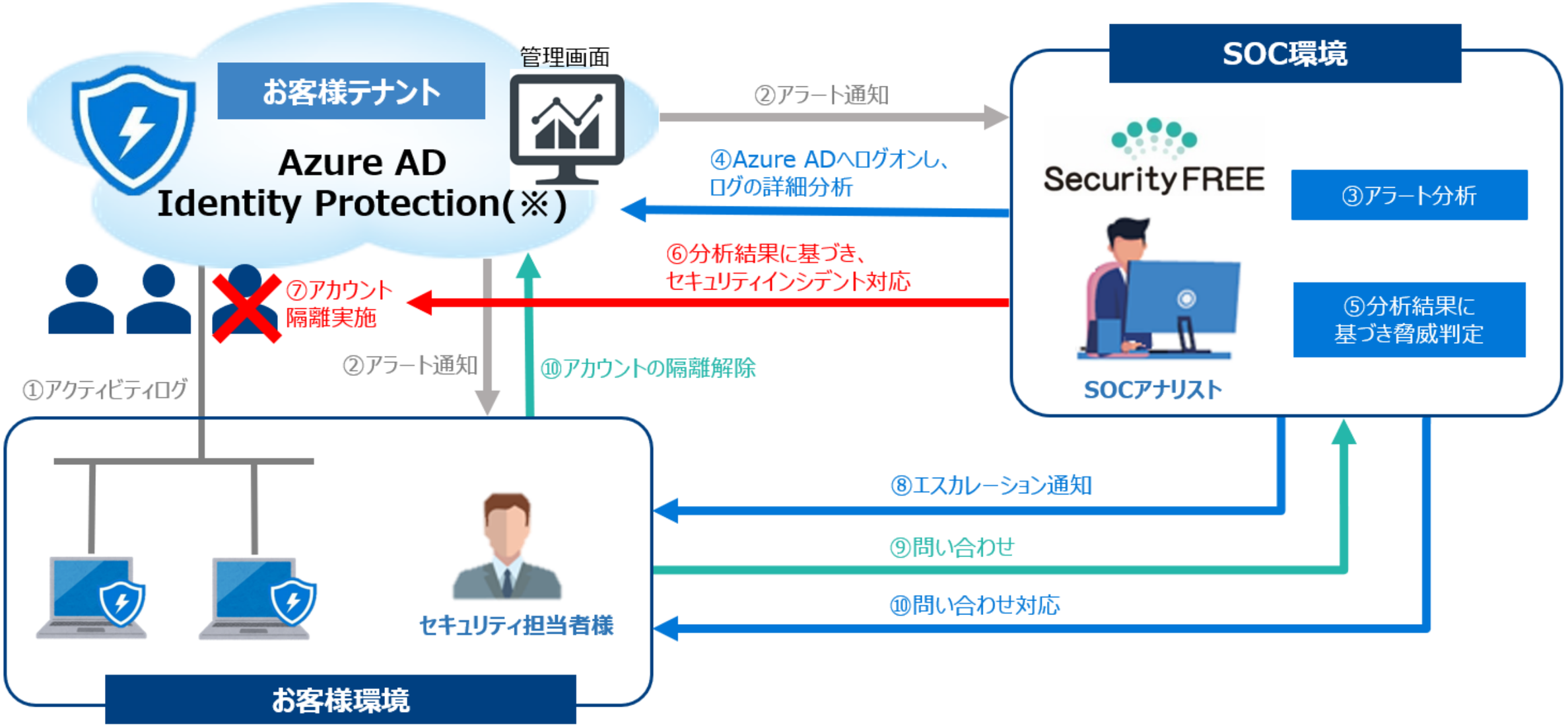
- **分析対象：**
  Identity Protection ＞ レポートより、以下の項目で検知されたアラートが対象
  ① **危険なユーザー**
  ② **危険なサインイン**
  ③ **リスク検出**

- **エスカレーション対象：**
  分析対象の調査の結果、アナリストが**リスク有り(脅威判断基準にてレベル2～4)**と判定したアラート

Azure Active Directory監視サービス サービス提供条件

- **サービス提供条件：**
  - ① **Azure AD Premium P2ライセンスが、利用者の数だけ導入されていること**
  - ② アナリストがお客様テナントのAzure ADにゲストユーザーとして参加可能であること
  - ③ アナリストに「**セキュリティオペレーター**」ロールが設定されていること
    (アラート分析に使用します)
  - ④ アナリストに「**特権認証管理者**」ロールが設定されていること
    (遠隔操作対応に使用します)
  - ⑤ SC管理者に「**特権ロール管理者**」ロールが設定されていること
    (運用開始後のSOCアナリスト追加対応で使用します)
  - ⑥ Identity Protectionにてアナリスト宛のメール通知設定が実施されていること
    (メールアドレスはご契約後に別途ご案内します)
  - ⑦ アナリスト追加時の承認フローが設定されていること

Azure Active Directory監視サービス 構成イメージ



(※) ⑩アカウントの隔離解除はお客様にて復旧作業を実施いただきます。

Azure Active Directory監視サービス 提供内容(1/2)

SOFT CREATE

大分類	中分類	内容	提供機能 エントリー	通知手段	対応時間
セキュリティ監視	セキュリティアラート分析	対象製品のセキュリティログを監視し、設定されたルールに伴いアラートを検知。 検知したアラートに対してアナリストが詳細分析を行います。	○	－	24時間 365日
	エスカレーション通知	分析結果に基づき、当社基準にて脅威レベル2以上と判断したアラートについて、 ポータルサイトを通じてエスカレーション（検知内容/分析結果/対処依頼事項）を実施します。 また、弊社分析基準のレベル 4(アカウント詐取、侵害、侵入の疑いがある)と判断された場合、利用申込書に記載いただいたお電話番号にご連絡いたします。 ※記載いただいたお電話番号のいずれも連絡がつかなかった場合は、それ以降のご連絡は行いません。	○	ポータル (レベル4のみ電話)	
インシデント対応	インシデント対応 (※オプション)	分析結果に基づき、当社基準にて脅威レベル3以上と判断したアラートについて、お客様への確認を行わず、アナリストにて対象アカウントのセッション切断および無効化を実施いたします。 ※オプション機能(チケット制)となります。 ※アカウントの再有効化はお客様にてご対応をお願いいたします。	○	ポータル	
問合せ対応	セキュリティアラート	当社よりエスカレーションしたアラートに起因するお問い合わせに対して回答をします。 ※場合により、二次回答以降は、翌営業日のご案内となる可能性がございます。	○	ポータル	24時間 365日
	セキュリティアラート以外	エスカレーション通知以外のセキュリティに関連したお問い合わせに対して回答をします。 ※月5件まで ※製品の仕様・不具合についてはサポート対象外となります。	○	ポータル	当社営業日 9時~18時

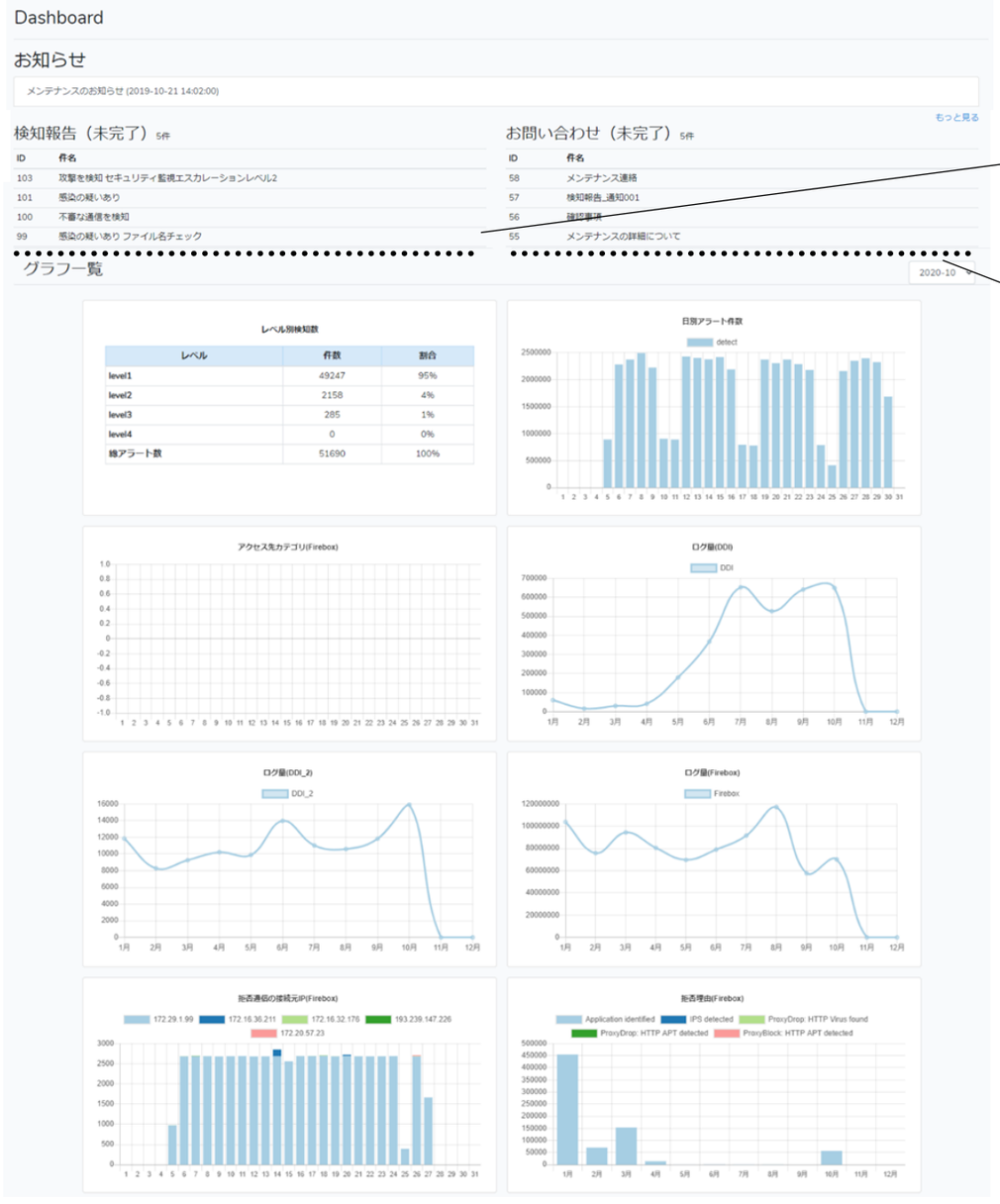
Azure Active Directory監視サービス 提供内容(2/2)

SOFT CREATE

大分類	中分類	内容	提供機能 エントリー	通知手段	対応時間
ポータルサイト	ポータルサイト閲覧	アラートの閲覧、問い合わせ、月次報告書のダウンロードを実施いただけるポータルサイトをご提供します。	○	ポータル	24時間 365日
	アラート集計結果	検知したアラートの集計を行います。 集計した結果は、ポータルサイトでご確認いただけます。 ※脅威レベル1(エスカレーション対象外)のアラートは集計対象外となります。	○	ポータル	
	月次報告書	検知したアラートの集計、分析結果をまとめた月次報告書をご提供します。 月次報告書はポータルサイトよりダウンロードいただけます。	○	ポータル	
複数契約時 (ベーシック契約時)	セキュリティアラート分析 (相関分析)	複数の監視製品間による相関分析を実施し、分析結果に基づき、エスカレーション通知を実施いたします。	－	－	
	月次報告書の作成 (pptx形式)	上記月次報告書に対して、相関分析結果やセキュリティのトピックスも加えた月次報告書を作成いたします。 ※月次報告書は、ポータルサイトからダウンロードいただけます。	－	ポータル	当社営業日 9時～18時
	月次報告会	アナリストが訪問（またはWeb会議）の上、報告会を実施いたします。 報告会では、エスカレーション状況のご確認、アラートに対するアドバイス、セキュリティトピックスをご報告いたします。 ※月1回実施想定となります。	－	－	

Azure Active Directory監視サービス お客様専用ポータルサイト

監視対象製品のログ件数の推移や内容を時系列でグラフ表示します。



ダッシュボード

監視対象製品のログ件数の推移や内容を時系列でグラフ表示します。

検知報告ステータス

検知アラートについて未完了ステータスを表示します。
クローズされた内容についても履歴一覧として閲覧可能です。

問い合わせ（Q&A）ステータス

お客様からのお問い合わせについて未完了ステータスを表示します。
クローズされた内容についても履歴一覧として閲覧可能です。

検知報告内容

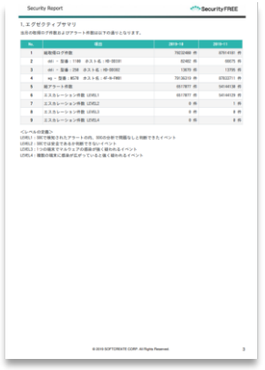
次ページにて詳細を確認ください。

問い合わせ

検知報告内容への問い合わせ、及びQ＆Aは、ポータル画面上よりお問い合わせをいただき対応履歴管理をさせていただきます。

レポート機能

ポータル画面上より、検知内容、対応状況をレポートとしてダウンロードできます。



エスカレーション内容について

【（例）攻撃の可能性が高い場合】

■件名
【ABC-E202211-00**】不審な通信を検知 エスカレーションLv3_Azure AD（11/**）

脅威度が一目で分かる

■本文
株式会社ABC　ご担当者様
お世話になっております。S&Jアナリストチームです。

Identity Protectionのアラートを1件検知しました。
下記にて分析結果をご報告いたします。

〇検知イベント概要
・検知時間　：　2022/11/16 19:00
・検知件数　：　1件
・ユーザー　：　Aiueo Kakikukeko
・ユーザー名　：　kakikukeko@sandj.co.jp
・アプリケーション　：　Azure Portal
・接続元IP　：　192.168.0[.]10
・場所　：　アメリカ
・検出の種類　：　匿名IPアドレス
・ブラウザー　：　Firefox 91.0
・OS　：　Windows 10

何が起こったか、
専門家でなくても把握できる

〇分析結果
匿名のIPアドレスからのサインインを検知しました。
ユーザーのログ情報を確認したところ、これまで日本からのアクセスしかございませんでした。
しかし、匿名のIPアドレスで他国からのアクセスをされていることから、
不審なログインであると判断しております。

該当のサインインが意図したものであるかご確認いただき、
意図したものでない場合は、早急にユーザーアカウントのパスワード変更を推奨いたします。

対処方法まで案内されるため
専門家でなくても安心

〇対処依頼事項
１）上記の検知イベント概要の項目をご確認いただき該当のサインインが意図したものであるかご確認ください。
２）該当のサインインが意図したものでない場合は、早急にユーザーアカウントのパスワード変更を推奨いたします。

検出される脅威

SOFT CREATE

No.	主な検出脅威	ADサーバ		ファイルサーバ		AD管理端末 (Advのみ)	Azure AD (IdP)	備考
		Standard	Advanced	Standard	Advenced			
1	PrintNightmare	-	○	-	○	○	-	別途ログ出力設定が必要
2	パスワードスプレー攻撃	○	○	-	-	-	○	サインインリスク
3	BloodHound	○	○	○	○	-	-	別途アカウント追加設定が必要
4	アカウントロック	○(※1)	○	○(※1)	○	-	-	別途ログ出力設定が必要
5	不審なPowerShell実行	○	○	○	○	○	-	PowerShell5.0以上が必要
6	不審なタスク登録	-	○	-	○	-	-	別途ログ出力設定が必要
7	RDPログオン/ログオフ	○	○	○	○	○	-	
8	不審なレジストリ操作	-	-	-	-	○	-	
9	PSEXECの実行	○	○	○	○	-	-	
10	不審なコマンドの実行	-	○	-	○	○	-	別途ログ出力設定が必要（※2）
11	不審な管理共有	-	○	-	○	○	-	別途ログ出力設定が必要
12	Pass The Hash	○	○	○	○	○	-	
13	Golden Ticketの利用	-	○	-	○	-	-	別途ログ出力設定が必要
14	DCShadow	-	○	-	-	-	-	別途ログ出力設定が必要
15	DCSync	-	○	-	○	-	-	別途ログ出力設定が必要
16	Skeleton Key	-	○	-	○	-	-	別途ログ出力設定が必要
17	メモリからのクレデンシャル情報流出	-	-	-	-	○	-	別途ログ出力設定が必要
18	イベントログ消去	○	○	○	○	○	-	
19	意図しない管理者登録	○	○	-	-	-	-	
20	Kerberoasting攻撃	-	○	-	-	-	-	別途ログ出力設定が必要
21	Zelologon	○	○	-	-	-	-	
22	登録管理者以外の管理者権限ログオン	-	○	-	-	-	-	
23	登録外のIPと管理者の組み合わせによるログオン	-	○	-	-	-	-	
24	不審なグループポリシー操作	○	○	-	-	-	-	
25	監査ログ設定が不十分	○	○	○	○	-	-	
26	重要なセキュリティパッチが未適用	○	○	○	○	-	-	一部のパッチ適用状況を確認

Azure AD監視で検出可能な脅威

検出される脅威

No.	主な検出脅威	ADサーバ		ファイルサーバ		AD管理端末（Advのみ）	Azure AD（IdP）	備考
		Standard	Advanced	Standard	Advenced			
27	特殊な移動	-	-	-	-	-	○	サインインリスク
28	異常なトークン	-	-	-	-	-	○	サインインリスク
29	トークン発行者の異常	-	-	-	-	-	○	サインインリスク
30	悪意のある IP アドレス	-	-	-	-	-	○	サインインリスク
31	マルウェアにリンクした IP アドレス	-	-	-	-	-	○	サインインリスク
32	匿名 IP アドレス	-	-	-	-	-	○	サインインリスク
33	疑わしいブラウザー	-	-	-	-	-	○	サインインリスク
34	通常とは異なるサインイン プロパティ	-	-	-	-	-	○	サインインリスク
35	ユーザーに対するセキュリティ侵害を管理者が確認しま	-	-	-	-	-	○	サインインリスク
36	プライマリ更新トークン (PRT) へのアクセス試行の可能	-	-	-	-	-	○	ユーザーリスク
37	漏洩した資格情報	-	-	-	-	-	○	ユーザーリスク
38	検出された追加のリスク	-	-	-	-	-	○	サインインリスク/ユーザーリスク
39	Azure AD 脅威インテリジェンス	-	-	-	-	-	○	サインインリスク/ユーザーリスク
40	あり得ない移動	-	-	-	-	-	-	サインインリスク、要MCAS
41	匿名 IP アドレスからのアクティビティ	-	-	-	-	-	-	サインインリスク、要MCAS
42	初めての国	-	-	-	-	-	-	サインインリスク、要MCAS
43	受信トレイからの疑わしい転送	-	-	-	-	-	-	サインインリスク、要MCAS
44	受信トレイに対する疑わしい操作ルール	-	-	-	-	-	-	サインインリスク、要MCAS
45	機密ファイルへの大量アクセス	-	-	-	-	-	-	サインインリスク、要MCAS

Azure AD監視で検出可能な脅威

・赤枠以外の監視にはAD監視(オンプレミス版)またはMicrosoft Defender for Cloud Appsが必要です。
・AD監視(オンプレミス版)とは**役割が異なるため、同様の脅威検知はできません。**
・ADとAzure ADの両方を監視することで、**ハイブリッド構成の監視**にも対応します。

Azure Active Directory監視サービス 導入時の役割分担

作業内容		お客様	SC	補足
準備	Azure AD Premium P2ライセンスの手配/割り当て	○	-	ユーザー数分のライセンス契約が必要となります。
	Identity Protection ポリシー適用	○	-	Identity Protectionの設定が完了している必要がございます。
	利用申込書のご提供	-	○	
	お客様情報の記入・返送	○	-	
導入 (初期作業)	Azure AD ゲストアカウント招待/グループ作成	○	★	
	各アカウントへの権限付与	○	★	
	Identity Protection メール設定	○	★	
	Azure AD アナリスト承認フロー設定	○	★	
	セキュリティアナリスト対応準備	-	○	
	ポータルサイト開設	-	○	
動作確認	アラート検知確認	-	○	・Torブラウザからのアクセステストを想定
	エスカレーションテスト	○	○	・当社よりテストエスカレーションの実施 ・お客様による受領確認

★・・・当社作業可(有償)
※具体的なスケジュールおよび体制については、別途ご調整の上、確定となります。

Security FREE サービス運用時の役割分担

大項目	中項目	小項目	お客様	SC	備考
セキュリティ監視	インシデント発生	エスカレーション	–	○	日本語対応のみ
	インシデント対応	強制サインアウト・無効化	–	○	オプション
		アカウント復旧	○	–	お客様にて行う想定
	月次報告書	月次報告書提供	–	○（◇）	同上(◇ベーシックプランはPPT提供)
	月次報告会	月次報告会実施	–	○（◇）	◇ベーシックプランのみ実施
	問合せ対応	ポータルサイト問合せ	–	○	日本語対応のみ
	セキュリティポリシー変更対応	Identity Protection ポリシーチューニング	○	–	指定の保守ベンダが行う想定

※製品運用および保守につきましてはお客様想定となります。

Azure Active Directory監視サービス 納品ドキュメント

内容	補足
ヒアリングシート送付時の納品ドキュメント	
├**Azure Active Directory初期設定手順書**	・Azure Active Directory監視導入作業の手順書
├**Azure Active Directory監視サービス仕様書**	・セキュリティ監視サービスの提供機能や条件を定めた仕様書
└**Azure Active Directory監視サービス利用規約**	・セキュリティ監視サービスの提供にあたる利用条件を定めた約款
サービス導入時の納品ドキュメント	
├ **Security FREEサービス通知書**	・お客様情報および専用ポータルサイトへのログイン情報を記載
├ **Security FREEポータル操作マニュアル**	・専用ポータルの簡易操作マニュアル
├ **Security FREE運用フロー**	・本サービス
└ **作業報告書**	・Azure Active Directory監視導入作業の報告書

最後に

今後も『Security FREE』は拡張を続け、
ITアウトソーシングとSOCサービスを組み合わせた
総合監視モデルの拡充を目指し、
企業のサイバーセキュリティリスクの耐性向上へ貢献して参ります。

Security FREE