WideAngle マネージド SOAR
サービス仕様書

バージョン 4.05

2026 年 6 月 8 日

NTT ドコモビジネス株式会社

目次

記載されている会社名や製品名は、各社の商標または登録商標です。

1. はじめに

1.1. 本書の目的

本書は、マネージド SOAR のサービス提供機能、利用条件、および注意事項などについて記述したものです。本書に記載の内容について、予告なく変更される場合があります。

1.2. 関連文書

文書名
WideAngle マネージド SOAR_サービス仕様書_
B01_【マネージド SOAR】標準提案書
WideAngle マネージド SOAR_利用規約
WideAngle マネージド SOAR_自動対処機能説明書【ご契約者様向け】
WideAngle マネージド SOAR_アラート通知内容補足説明書【ご契約者様向け】
WideAngle_27_マネージド SOAR_新規_L
WideAngle_28_マネージド SOAR_変更_L
WideAngle_29_マネージド SOAR_廃止_L
WideAngle_30_マネージド SOAR_簡易変更_L
WideAngle_31_マネージド SOAR_ヒアリングシート（新設・変更・廃止用）_T
WideAngle_32_マネージド SOAR_ヒアリングシート(Severity 設定用)_T
対処除外設定リスト（Account.csv、Host.csv、Alert.csv）
マネージド SOAR_対処除外設定リスト作成時の留意事項
WideAngle マネージド SOAR_カスタマーポータルご利用ガイド_版数
WideAngle マネージド SOAR_受信メール設定ご利用ガイド_版数
マネージド SOAR_NTT Com 工事用アカウント準備ガイド_WideAnglePS
マネージド SOAR_NTT Com 工事用アカウント削除ガイド_WideAnglePS
WideAngle マネージド SOAR_MicrosoftEntraIDP2 用検知試験ガイド_版数
WideAngle マネージド SOAR_MDE 用検知試験ガイド_版数
WideAngle マネージド SOAR_MDI 用検知試験ガイド_版数
WideAngle マネージド SOAR_MDCA 用検知試験ガイド_版数
WideAngle マネージド SOAR_MicrosoftEntraIDP2 用検知試験チェックシート_版数
WideAngle マネージド SOAR_MDE 用検知試験チェックシート_版数
WideAngle マネージド SOAR_MDI 用検知試験チェックシート_版数
WideAngle マネージド SOAR_MDCA 用検知試験チェックシート_版数

1.3. 用語の定義

本サービスで使用する用語は以下の通りです。

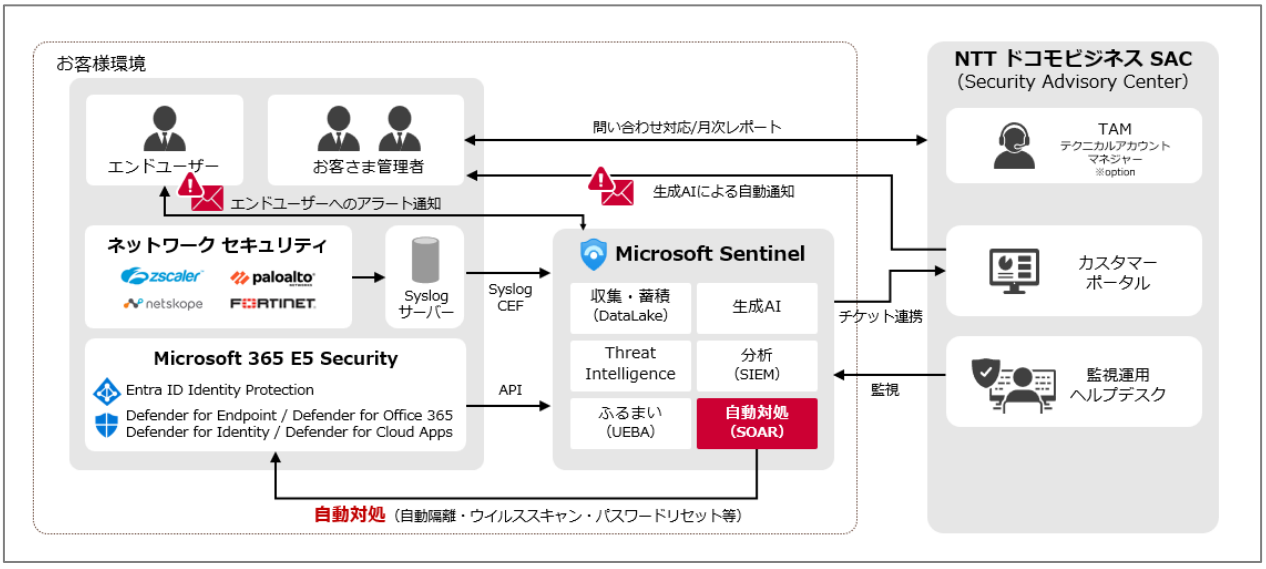
用語	定義
Microsoft Sentinel	Microsoft 社のセキュリティ運用の自動化ソリューション。
SOAR	Security Orchestration, Automation and Response の略称。お客さま環境のインシデント管理やインシデント対応の自動化を支援するためのセキュリティソリューション。
SIEM	Security Information and Event Management の略称。SOAR 同様にさまざまなソースから収集したデータをインシデント検知や分析に活用するソリューション。
Logic Apps	Azure Logic Apps は Microsoft 社のクラウド プラットフォーム。自動化されたワークフローを作成、実行できます。 またこの機能を使用して構築したワークフローのことを指す場合もあります。
Playbook	アラートやインシデントに対する応答として Microsoft Sentinel から実行できる手順のコレクションです。
SAC	セキュリティアドバイザリーセンターの略称。
ServiceNow	ServiceNow 社。ServiceNow 社が提供するプラットフォームを指す場合もあります。
NTT ドコモビジネス	NTT ドコモビジネス株式会社の略称。
Threat Detection	マネージド SOAR のメニュー名。お客さまのセキュリティデバイスからログの転送を Common Event Format（CEF） /Syslog で送っていただき、Microsoft の Threat Intelligence でマッチングし脅威が発見されれば通知される。
Threat Intelligence	脅威情報インテリジェンス。マネージド SOAR では Microsoft の Defender Threat Intelligence を利用しています。
Microsoft Defender for Endpoint 連携	Microsoft Defender for Endpoint（以下 MDE）と他対象デバイス連携を行うことによって、MDE 連携しているデバイスに対して自動対処のホスト対処を実施します。
AIR	Automated Investigation and Response の略称。 Microsoft Defender for Endpoint の機能であり、感染調査から復旧対処までを自動的に行う。

2. サービス概要

2.1. サービス概要

- 本サービスは、お客さまのセキュリティデバイス（M365-Business Premium/E3/E5、その他セキュリティ製品など）に対し、 Microsoft 社のクラウド SIEM/SOAR 製品である Microsoft Sentinel を用いた、セキュリティ監視、自動ログ分析、自動通知、自動対処を提供するサービスです。
- 本サービスでサポートするログを監視対象として、SIEM（Security Information and Event Management）による自動ログ分析、SOAR（Security Orchestration and Automation Response）による自動対処を実現します。
- お客さま担当者は、カスタマーポータルから本サービスに関する各種問い合わせ、各種作業依頼などを行います。
- NTT ドコモビジネスは、カスタマーポータルにて、各種問い合わせ回答、各種作業依頼回答を行います。

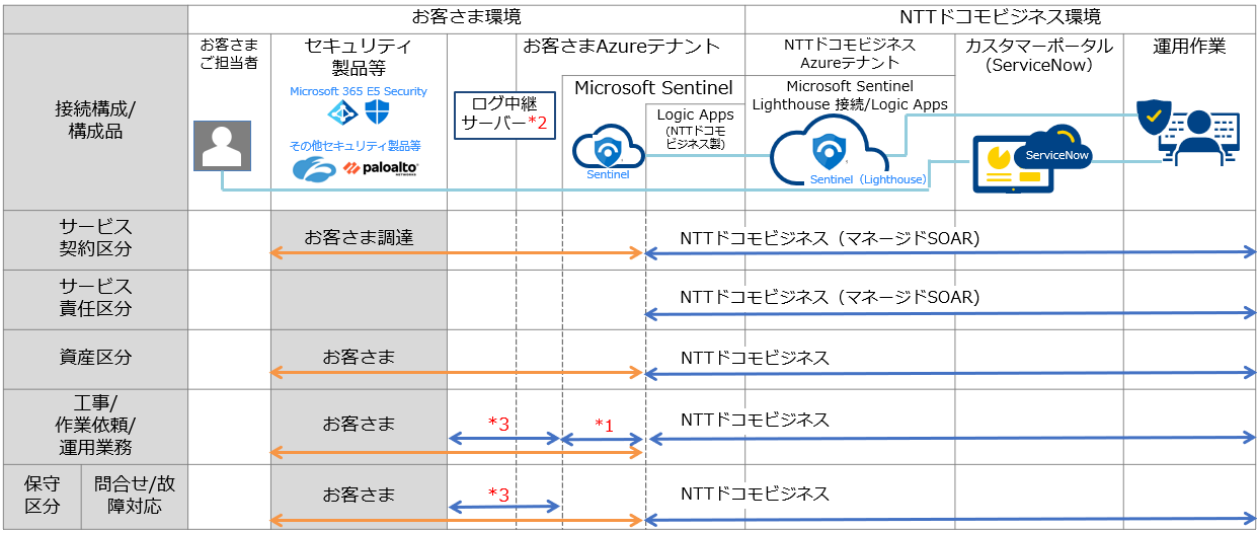
（参考）サービス提供イメージ



3. サービス仕様

3.1. 提供区分

- 本サービスのサービス提供/保守区分は、下図の通りです。
- お客さまにて Microsoft Sentinel のサブスクリプションを調達いただいたうえで、NTT ドコモビジネスにて Microsoft Sentinel の構築を行い、Logic Apps を提供します。
- またカスタマーポータルを提供し、お客さまからのお問い合わせや作業依頼などを受け付けます。



*1 お客さま Azure テナントの Microsoft Sentinel に対し、開通工事時や運用中に NTT ドコモビジネス推奨の設定をさせていただきます。

*2 Threat Detection メニューをご契約の際は、ログ中継サーバーをお客さまにてご用意いただく必要があります。ログ中継サーバーはお客さま宅内/Azure 上のどちらに設置しても構いません。

*3 NTT ドコモビジネスでログ中継サーバーを構築する場合は、ログ連携設定や保守作業をチケットによる作業依頼で申込みいただけます。

3.2. 提供メニュー

- マネージド SOAR の提供メニューは以下の通りです。

サービス区分	メニュー名	概要説明
基本サービス	基本プラン	・ログ収集/自動ログ分析/自動通知/自動対処 ・カスタマーポータル ・作業依頼ポイントは含まれません。（0 ポイント）
オプションサービス	作業依頼ポイント追加	・作業依頼に利用いただけるポイントを、予め申し込みいただき、提供します。（5 ポイント単位/月、上限 50 ポイント）

3.3. 提供機能一覧

3.3.1. 基本サービス機能一覧

- 本サービスでは、お申し込みに応じて以下の機能を提供します。
- カスタマーポータルによる受付は 24 時間 365 日（日本語のみ）、回答は平日 9 時~17 時（※年末年始を除く）となります。詳細は、「**6.4 お問い合わせ・作業依頼受付**」を参照してください。

【基本プラン】

提供機能		概要
標準提供機能	カスタマーポータル	カスタマーポータルを提供します。カスタマーポータルでは、通知アラートの確認、各種お問い合わせ、作業依頼申請、ご契約情報・サービス設定情報の確認、お客さまのログインアカウント管理、受信メール設定、各種情報確認などが行えます。
選択型提供機能	ログ収集	Microsoft Sentinel に標準で実装されているデータコネクタを利用してログを収集します。
	自動ログ分析	Microsoft Sentinel に標準で実装されている分析ロジックを用いて自動分析を行います。

	自動通知/自動対処	NTT ドコモビジネスが自動通知/自動対処の Playbook を作成し、Microsoft Sentinel に適用します。自動通知/自動対処が正常に機能するか監視を行います。

- 選択型提供機能は、「ログ収集」「自動ログ分析/自動通知」「自動ログ分析/自動通知/自動対処」の各セットで提供され、1 つ以上選択いただきます。
- 選択型提供機能のお申し込み時には、サポートデバイスを選択いただきます。

【選択型提供機能 対応デバイス】

サポートデバイス	**選択型提供機能**		
	ログ収集	**自動ログ分析 /自動通知**	**自動ログ分析 /自動通知 /自動対処**
・Microsoft Entra ID P1 ・Microsoft Entra ID P2	●	—	●
・Microsoft Defender for Identity	●	—	●
・Microsoft Defender for Endpoint ・Microsoft Defender for Business	●	—	●
・Microsoft Defender for Cloud Apps	●	—	●
・Microsoft Defender for Office 365	●	●	—
・UEBA	—	●	—
・Threat Detection	—	●	—

- 「自動ログ分析/自動通知」または「自動ログ分析/自動通知/自動対処」を申し込む場合、選択されたデバイスに対応する「ログ収集」を、併せて申し込みいただく必要があります。

提供機能	**サポートデバイス**	**併せて申し込みが必要な ログ収集（対象デバイス）**
自動ログ分析/自動通知	Microsoft Defender for Office 365	Microsoft Defender for Office 365
	UEBA	Microsoft Entra ID P1 or Microsoft Entra ID P2
自動ログ分析/自動通知/自動対処	Microsoft Entra ID P1	Microsoft Entra ID P1
	Microsoft Entra ID P2	Microsoft Entra ID P2
	Microsoft Defender for Identity	Microsoft Defender for Identity
	Microsoft Defender for Endpoint	Microsoft Defender for Endpoint
	Microsoft Defender for Business	Microsoft Defender for Business
	Microsoft Defender for Cloud Apps	Microsoft Defender for Cloud Apps
	Microsoft Defender for Office 365	Microsoft Defender for Office 365

UEBA（自動ログ分析/自動通知）についての注意事項
Microsoft Defender for Identity のログ収集の利用は必須ではありませんが、利用される場合は、オンプレミス AD のログも自動ログ分析/自動通知の対象となります。

上記に加え、「SecurityEvents」および「AzureActivity」の任意ログソースを対象としたい場合は、お客さまにて該当ログの収集設定が必要です。なお、該当ログの収集設定が新規開通以降となる場合は、別途 NTT ドコモビジネス側での変更工事が必要となり、変更申込が必要となります。お客さま側の収集設定だけでは自動ログ分析/自動通知の対象となりません。

Threat Detection（自動ログ分析/自動通知）についての注意事項
Threat Detection を利用される場合は、お客さまにて Threat Detection に対応したログの収集設定が必要です。

3.3.2. 作業依頼機能一覧

- 本サービスでは、オプションサービスの「作業依頼ポイント追加」を契約いただき、このポイントを消費することで、以下の作業依頼機能をお客さまからの作業依頼申請に基づき提供します。
- 作業は、作業依頼の承認日から 3 営業日以内に実施いたします。作業実施は平日 9 時~17 時（※年末年始を除く）となります。
- 同時にご依頼できる作業は 1 件までとし、作業が完了し、ケースが Close となるまでは、次の作業依頼をすることはできません。

【作業依頼機能】

No.	作業依頼機能	概要	必要ポイント数
1	ログ保存期間変更	Log Analytics ワークスペースに保管するログの保存期間は製品としてはデフォルト 30days ですが、本サービスでは 90days を初期設定としています。 作業依頼の申請により、以下の設定値への変更が可能です。 保存期間（30, 31, 60, 90, 120, 180, 270, 365, 550, 730）	1
2	対処除外設定	Microsoft Sentinel 上で対処（端末隔離、アカウントのパスワードリセット）が不要な端末がある場合は、対処対象外に設定します。	1

		「自動ログ分析/自動通知/自動対処」を利用している場合で、自動対処を行わず自動通知のみとしたい際に、申請に基づき設定します。 「自動ログ分析/自動通知/自動対処」を利用している場合で、自動通知のみだったが自動対処も行いたい際に、申請に基づき設定します。	
3	各種設定変更	以下の設定内容の変更が可能です。 ・「自動通知」または「自動対処」の Severity 設定に変更がある場合は、申請に基づき設定します。 ・パスワード変更が必要なエンドユーザに対して実施されるエンドユーザ通知の通知内容について変更がある場合は、申請に基づき設定します。 ・初回 AIR の結果が NG だった場合に実施されるエンドユーザ通知の通知内容について変更がある場合は、申請に基づき設定します。 ・AIR 自動再実行回数を申請に基づき設定します。 ・XDR ポータル統合を解除する場合に必要な設定を、申請に基づき設定します。 ・追加／削除したいデータコネクタを、申請に基づき設定します。 ・自動対処除外アラートの登録／削除を、申請に基づき設定します。 ・NTT ドコモビジネス構築済みログ中継サーバーからのログ連携を、申請に基づき設定します。 ・NTT ドコモビジネス構築のログ中継サーバーの保守を申請に基づき実施します。 ・ブロックリスト利用／利用中止のため、接続元 IP アドレスの登録／削除を申請に基づき実施します。 ・WideAngle AI Advisor 連携の有効化/無効化を、申請に基づき設定します。	2

「対処除外設定」については、サービス開通時に特定の端末について希望がある場合のみ、新設に必要な申込様式（対処除外設定リスト）に記入いただくことで開通時に設定を行います。開通後の依頼は本作業依頼にて申請してください。

「各種設定変更 ＞ Severity 設定」の場合、ヒアリングシートの不備チェック作業依頼内容の確認に伴い、作業依頼の受理・不受理の判定までに、3 営業日かかる場合があります。

3.4. 提供機能（基本サービス機能）

3.4.1. カスタマーポータル

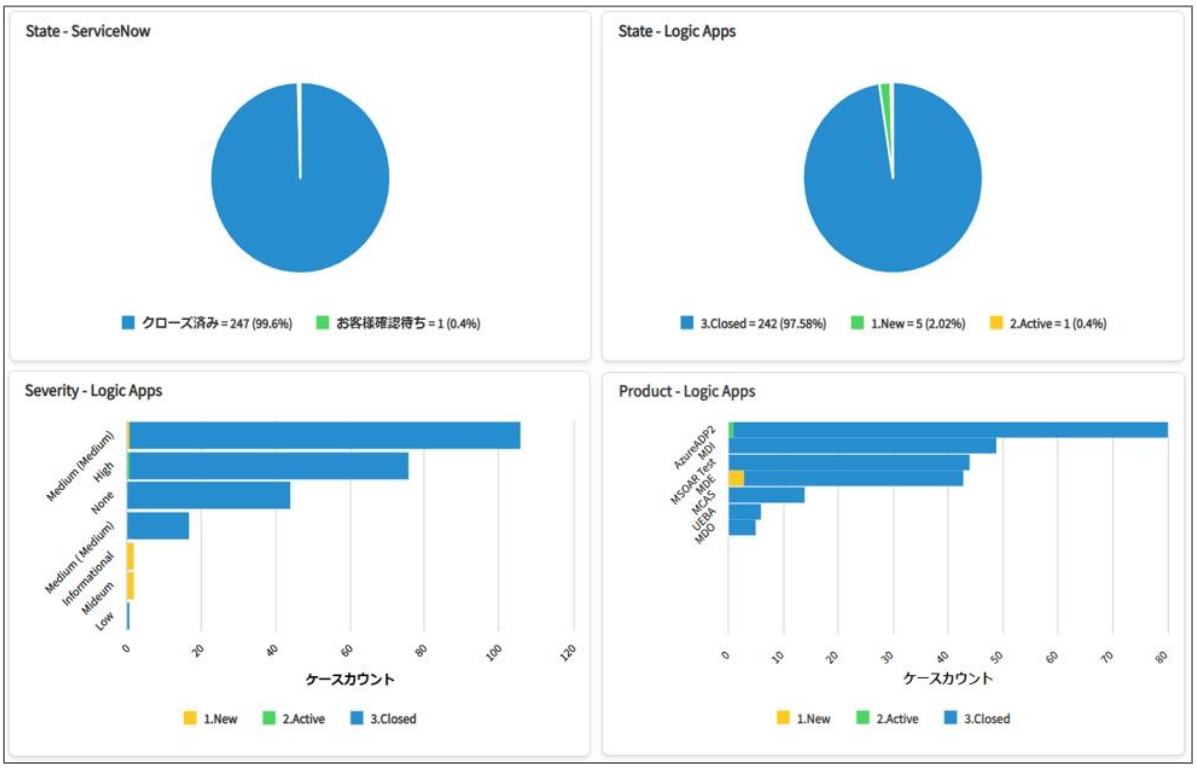
- 本サービスでは、カスタマーポータルを提供し、サービスとして提供されるものは、基本的にカスタマーポータルを通じて提供されます。
- お客さまとセキュリティアドバイザリーセンターとのやり取りは、すべてカスタマーポータルを通じてやり取りされます。
- カスタマーポータルは ServiceNow を利用しており、お客さまはインターネットからアクセスすることが可能です。

- カスタマーポータルへのログインには多要素認証のご利用が可能です。
- カスタマーポータルでは、各種お問い合わせ、作業依頼の申請、お客さまのご契約情報・サービス設定情報のご確認、受信メール設定、お客さまのログインアカウント管理（ユーザー追加・変更、連絡先変更など）、各種情報（工事情報、お知らせ、各種マニュアル）のご確認などが行えます。
- お客さまのログインアカウントは、管理者と担当者と 2 つの権限があります。管理者アカウントは、ユーザーの追加が可能です。担当者アカウントは、自分自身のユーザー情報変更が可能です。

（参考）カスタマーポータルイメージ

- カスタマーポータルには、ダッシュボード機能があり、Microsoft Sentinel 運用状況をグラフで確認することができます。
- アラートが発生すると Logic Apps を通してカスタマーポータルにケースが起票されます。ダッシュボードを参照することで、ケースの傾向を確認することができます。

（参考）ダッシュボードイメージ

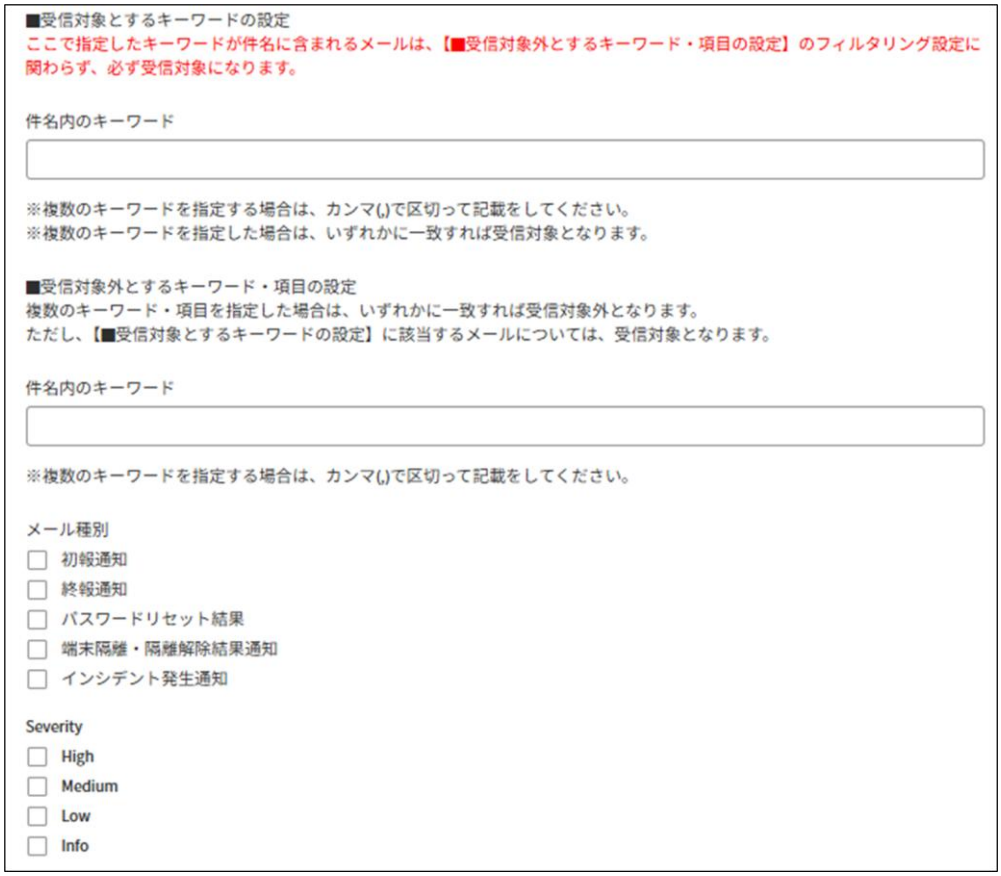


グラフの名前	概要
State - ServiceNow	ケースのステータスの比率
State - Logic Apps	Logic Apps のステータスの比率
Severity - Logic Apps	Logic Apps のステータスと重大度ごとのケース数
Product - Logic Apps	Logic Apps のステータスとサポートデバイスごとのケース数

ケースのステータスはケースそのものの状態を、Logic Apps のステータスは Logic Apps の処理完了時の状態を示します。

- インシデントに関して通知されるメールのフィルタリング設定を実施します。
- ここで設定した内容は、設定者が受信するメールのみに適用されます。
- 受信対象とする件名のキーワード、受信対象外とする件名のキーワード、送信区分や Severity によりフィルタリング設定できます。

（参考）受信メール設定画面イメージ



3.4.2. ログ収集

- 本サービスでは、Microsoft Sentinel に標準で実装されているデータコネクタを利用してログを収集します。 Microsoft Sentinel 上でデータコネクタによって対象デバイスと連携します。
- 本機能のご利用開始時点では、収集するログの保存期間（Azure Monitor のログ保存期間）は、Microsoft Sentinel のデフォルトの 30days から変更し、90days で設定します。
- ご利用開始後に作業依頼を申請いただくと、期間の変更（ 30, 31, 60, 90, 120, 180, 270, 365, 550, 730days より選択）が可能です。なお、ログ保存期間は、Sentinel 全体での設定となり、対象デバイスごとに保存期間を設定することはできません。

「自動ログ分析/自動通知」「自動ログ分析/自動通知/自動対処」をお申し込みの場合、ログ保存期間が短いと十分なログ検証が行えないため、90 日以上に設定することを推奨しております。

【ログ収集】

対象デバイス	利用するデータコネクタ	デフォルト設定ログ（有効化必須）	ログ収集 Configuration 設定変更（選択有効化可能）
・Microsoft Entra ID P1 ・Microsoft Entra ID P2	Microsoft Entra ID	Sign-In Logs Audit Logs	Service Principal Sign-In Logs（Preview） Managed Identity Sign-In Logs（Preview） Provisioning Logs（Preview） ADFS Sign-In Logs（Preview） User Risk Events（Preview） Risky Users（Preview） Network Access Traffic Logs（Preview） Risky Service Principals（Preview） Service Principal Risk Events（Preview）
	Microsoft Entra ID Protection ※Microsoft Entra ID P1 では利用不可	データコネクタから収集されるログ *1	-
・Microsoft Defender for Identity	Microsoft Defender for Identity	データコネクタから収集されるログ *1	-
・Microsoft Defender for Endpoint ・Microsoft Defender for Business	Microsoft Defender for Endpoint	データコネクタから収集されるログ *1	-
・Microsoft Defender for Cloud Apps	Microsoft Defender for Cloud Apps	Alerts	Cloud Discovery Logs（Preview）
・Microsoft Defender for Office 365	Microsoft Defender for Office 365	データコネクタから収集されるログ *1	-

*1 これらのログについては、Microsoft Sentinel 上のデータコネクタ画面でログ名称は表示されませんが、ログの格納先は「SecurityAlert」テーブルです。

- Microsoft Defender XDR 化する場合は以下の通りとなります。

対象デバイス	利用するデータコネクタ	デフォルト設定ログ（有効化必須）	ログ収集 Configuration 設定変更（選択有効化可能）

・Microsoft Entra ID P1	Microsoft Entra ID	SigninLogs(Sign-in Logs) AuditLogs(Audit Logs)	Service Principal Sign-In Logs（Preview） Managed Identity Sign-In Logs（Preview） Provisioning Logs（Preview） ADFS Sign-In Logs（Preview） User Risk Events（Preview） Risky Users（Preview） Network Access Traffic Logs（Preview） Risky Service Principals（Preview） Service Principal Risk Events（Preview）
・Microsoft Entra ID P2			
	Microsoft Defender XDR	SecurityIncident Security Alert	- *1
・Microsoft Defender for Identity			
・Microsoft Defender for Endpoint ・Microsoft Defender for Business			
・Microsoft Defender for Cloud Apps			
・Microsoft Defender for Office 365			
・Threat Detection	Common Event Format(CEF) via AMA	CoomomSecurityLog	-
	Syslog via AMA	Syslog	-

*1 XDR 化すると「Cloud Discovery Logs (Preview)」のデータは収集されているので、変更 SO における「ログ収集　Configuration 設定変更　：　Microsoft Defender for Cloud Apps」は、申し込み不要となります。

（参考）Microsoft Azure Sentinel データコネクタ
https://learn.microsoft.com/ja-jp/azure/sentinel/data-connectors-reference

3.4.3. 自動ログ分析

- 本サービスでは、Microsoft Sentinel に標準で実装されている分析ロジックを用いて自動ログ分析を行います。
- Microsoft Sentinel 上では、各デバイスに対して、NTT ドコモビジネスがカスタムで検知ロジックを投入できるわけではなく、Microsoft 社のロジックを有効にするのみであり、Microsoft 社の検知ロジックに従ってアラートが出力されます。（UEBA を除く）

- 本サービスでは、既定の Severity（重要度）のアラートが検知された場合に、NTT ドコモビジネス独自の Playbook の機能により自動通知・自動対処を実施します。
- デバイス毎に有効化している分析ロジックは以下の通りです。これ以外のロジックは原則利用しません。

【XDR 未導入】

対象デバイス	有効化する分析ロジック
・Microsoft Entra ID P1	・Advanced Multistage Attack Detection（Fusion）*1 ・Anomalous sign-in location by user account and authenticating application ・Attempt to bypass conditional access rule in Microsoft Entra ID ・Brute force attack against a Cloud PC ・Distributed Password cracking attempts in Microsoft Entra ID ・MFA Spamming followed by Successful login ・Microsoft Entra ID PowerShell accessing non-Entra ID resources ・Password spray attack against Microsoft Entra ID application ・TI Map IP Entity to SigninLogs ・MFA Rejected by User ・Privileged Accounts - Sign in Failure Spikes ・Sign-ins from IPs that attempt sign-ins to disabled accounts ・Successful logon from IP and failure from a different IP ・User Accounts - Sign in Failure due to CA Spikes
・Microsoft Entra ID P2	・Advanced Multistage Attack Detection（Fusion）*1 ・Create Incidents based on Microsoft Entra ID Protection alerts
・Microsoft Defender for Identity	・Advanced Multistage Attack Detection（Fusion）*1 ・Create Incidents based on Microsoft Defender for Identity Alerts
・Microsoft Defender for Endpoint ・Microsoft Defender for Business	・Advanced Multistage Attack Detection（Fusion）*1 ・Create Incidents based on Microsoft Defender for Endpoint Alerts
・Microsoft Defender for Cloud Apps	・Advanced Multistage Attack Detection（Fusion）*1 ・Create Incidents based on Microsoft Cloud App Security alerts
・Microsoft Defender for Office 365	・Advanced Multistage Attack Detection（Fusion）*1 ・Create Incidents based on Microsoft Defender for Office 365
・UEBA*2	※判定ロジック・スコアリングは Microsoft の標準機能ですが、お客さまに通知する閾値を NTT ドコモビジネス独自で設定しています。
・Threat Detection *3	（Preview） Microsoft Threat Intelligence Analytics

*1 Microsoft Sentinel に標準で実装されている相関分析ロジックです。

*2 Microsoft Sentinel に標準で実装されているユーザー/エンティティの行動分析ロジックです。

*3 NTT ドコモビジネス マネージド SOAR のメニュー名です。

【XDR 導入】

対象デバイス	有効化する分析ロジック
・Microsoft Entra ID P1	XDR 未導入の場合と同じ
・Microsoft Entra ID P2 ・Microsoft Defender for Identity ・Microsoft Defender for Endpoint ・Microsoft Defender for Business ・Microsoft Defender for Cloud Apps ・Microsoft Defender for Office 365	分析ロジックの有効化は不要
・Threat Detection	XDR 未導入の場合と同じ

＜UEBA（ユーザー/エンティティ行動分析）＞

- UEBA は、Microsoft Sentinel に標準で実装されているユーザー/エンティティの行動分析ロジックです。

  この機能では、ユーザーやその他のエンティティの通常の行動を学習し、異常行動を検知し、その行動にセキュリティ上の影響があるかどうかを自動で分析しアラートを生成します。

  （参考）ユーザー/エンティティ行動分析（UEBA）
  https://docs.Microsoft.com/ja-jp/azure/sentinel/identify-threats-with-entity-behavior-analytics

＜Fusion（相関分析）＞

- Fusion は、Microsoft Sentinel に標準で実装されている相関分析ロジックです。

  この機能では、複数のデバイスからの様々なアラートを分析し、高度なマルチステージ攻撃（ランサムウェアなど）を自動で検出し、Fusion アラートを生成します。

  （参考）Microsoft Sentinel での高度なマルチステージ攻撃の検出
  https://docs.microsoft.com/ja-jp/azure/sentinel/fusion
  なお、XDR 化する場合は、Fusion は不要となり、その機能は、Microsoft Defender XDR 相関エンジンに置き換えられます。

Fusion の有効化に関する注意事項
1）Fusion の有効化については、初期開通時に NTT ドコモビジネスにて有効に設定するためお申し込みは不要です。
2）自動ログ分析・自動対処をご利用の場合に、ご利用のデバイスの「Advanced Multistage Attack Detection（Fusion）」分析ロジックを有効に設定します。
ただし、複数の対象デバイスからのアラートを分析するという Fusion の特性上、1 つのみ対象デバイスのお申し込みを行ったとしても動作せず、2 つ以上の対象デバイスの「自動ログ分析/自動通知」もしくは「自動ログ分析/自動通知/自動対処」をご利用の場合のみ 、その対象間のアラートについて相関分析（Fusion アラート出力）と自動対処が行われます。

※「ログ収集」のみご利用のデバイスは、Fusion の相関分析・自動対処の対象になりません。
（対象デバイス：Microsoft Defender for Endpoint、Microsoft Defender for Business、Microsoft Entra ID P1、Microsoft Entra ID P2、Microsoft Defender for Identity、Microsoft Defender for Cloud Apps、Microsoft Defender for Office 365）
3）Fusion は、Microsoft Defender for Identity と同じ Playbook を使用しているため、お申し込みデバイスの中に Microsoft Defender for Identity がない場合であっても、２つ以上の対象デバイスをお申し込みいただいた場合は、Microsoft Defender for Identity/Fusion の Severity 設定が必要です。
例えば Microsoft Defender for Endpoint のサービスと Microsoft Entra ID P2 のサービスをお申し込みの場合、お申し込みのサービスの Severity 設定と併せて、 Microsoft Defender for Identity/Fusion の Severity 設定が必要です。
4）Microsoft Defender for Identity の Severity 設定を行う場合、同時に Fusion の Severity 設定も行われる（Microsoft Defender for Identity と Fusion の Severity 設定を個別に設定することはできない）点にもご注意いただき、設定をご検討いただくようお願いいたします。

＜Threat Detection＞

- Threat Detection は、Microsoft Sentinel に標準で実装されている（Preview） Microsoft Threat Intelligence Analytics という分析ルールを活用して、お客さまから転送(*1)された CEF/Syslog 形式のログを、Microsoft の保有する脅威インテリジェンスとのマッチングを行い、不審な通信が発見する機能（手法）です。
  また、不正通信を行った端末のホストが特定できた場合で、マネージド SOAR の MDE 自動対処をご契約の場合は、MDE 経由で自動対処がされ脅威を除去することが可能です。

  *1 Microsoft Sentinel 上で使用できるデータコネクタの種類は、Microsoft の Web サイト（ https://learn.microsoft.com/ja-jp/azure/sentinel/data-connectors-reference ）を参照ください。こちらの中で CEF/Syslog 形式が対象のデバイスとなります。

Threat Detection についての注意事項
1）お客さまにて、セキュリティデバイスのログ送信設定、ログ中継サーバーの構築が必要です。
2）「（Preview） Microsoft Threat Intelligence Analytics」の分析ルールが反応するように、ログの送信設定を設定していただく必要があります。サービス仕様書を参照し適切に設定を行ってください。これらがログに含まれない場合は、正常な検知ができません。
3）Threat Detection をご利用になる場合、Sentinel へのログ転送量が増大しますので、Azure の利用条件を確認の上、Azure の利用料金などにご留意ください。

3.4.4. 自動通知/自動対処

NTT ドコモビジネスが自動通知/自動対処の Playbook を作成し、Microsoft Sentinel に適用します。また、自動通知/自動対処が正常に機能するか監視を行います。
機能の詳細については、ご契約者様に提供される「**WideAngle マネージド SOAR_自動対処機能説明書【ご契約者様向け】**」をご参照ください。

【自動通知/自動対処 機能一覧】

対象デバイス	通知	対処	
		ホスト対処	アカウント対処
		端末隔離/端末隔離解除 ウイルススキャン/駆除	パスワードリセットなどの対処
・Microsoft Entra ID P1 ・Microsoft Entra ID P2	●	● *1	●
・Microsoft Defender for Identity / Fusion	●	● *1	●
・Microsoft Defender for Endpoint ・Microsoft Defender for Business	●	●	
・Microsoft Defender for Cloud Apps	●	● *1	●
・Microsoft Defender for Office 365	●	● *2	
・UEBA	●		
・Threat Detection	●	● *2	

*1 Microsoft Defender for Endpoint を併せてご契約かつ、 Microsoft Defender for Endpoint 連携をご希望の場合に実施します。
*2 Microsoft Defender for Endpoint を併せてご契約の場合に実施します。（自動連携のため Microsoft Defender for Endpoint 連携有無の選択はできません。）

- これらの対処は、お客さまが自動対処を要望された Severity に対して、アラートを検知した場合に実施します。

- 自動通知/自動対処は、Microsoft Sentinel に連携されたインシデントに含まれる情報をもとに実施します。そのため、通知または対処に必要な情報が取得できないインシデントについては、自動通知/自動対処の対象外となります。
- UEBA は自動通知のみの機能のため、通知のみを実施します。

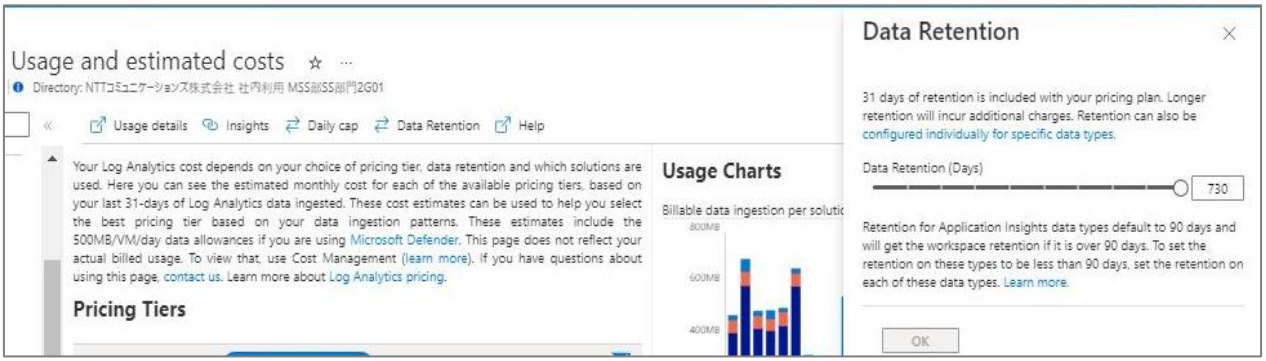
3.5. 提供機能（作業依頼機能）

3.5.1. ログ保存期間変更

- 本サービスでは、Azure Monitor のログ保存期間は、デフォルトの 30days から変更し 90days として設定しておりますが、以下の何れかの期間設定に変更が可能です。
- ■保存期間設定値：30, 31, 60, 90, 120, 180, 270, 365, 550, 730days

⚠ ログ保存期間は、Sentinel 全体での設定となり、対象デバイスごとに保存期間を設定することはできません。

（参考）Log Analytics 設定画面イメージ



3.5.2. 対処除外設定

- 本サービスでは、「自動ログ分析/自動通知/自動対処」機能をご利用の場合、特定の重要度のアラートが検知された端末、アカウントについて、自動的に端末隔離やパスワードリセットを行います。
- 上記の自動対処が不要な端末、アカウントがある場合、作業依頼の申請に基づき、端末やアカウントを個別に対処除外に設定することができます。
- 「自動ログ分析/自動通知/自動対処」を利用している場合で、自動対処を行わず自動通知のみとしたい際に、申請に基づき設定します。
- 「自動ログ分析/自動通知/自動対処」を利用している場合で、自動通知のみだったが自動対処も行いたい際に、申請に基づき設定します。

【作業依頼で設定が可能な除外設定のパターン】

対象	作業項目	概要	対処除外設定リスト
ホスト	全ホスト対処除外	全ての端末を自動対処の対象から除外します	不要 （NTT ドコモビジネスにて準備）
	全ホスト対処（対処除外設定の全解除）	全ての端末を自動対処の対象とします	不要 （NTT ドコモビジネスにて準備）
	指定ホスト対処除外	お客さま指定の端末のみ自動対処の対象から除外します	所定のフォーマットにてご提示が必要*1
アカウント（ユーザー）	全アカウント対処除外	全てのアカウントを自動対処の対象から除外します	不要 （NTT ドコモビジネスにて準備）
	全アカウント対処（対処除外設定の全解除）	全てのアカウントを自動対処の対象とします	不要 （NTT ドコモビジネスにて準備）
	指定アカウント対処除外	お客さま指定のアカウントのみ自動対処の対象から除外します	所定のフォーマットにてご提示が必要*1

*1 フォーマットは新設時と同様。詳細は、「**6.1.4.対処除外設定リスト**」を参照してください。

3.5.3. 各種設定変更

以下の各種設定内容を変更することが可能です。

1. Severity 設定
    - Severity 設定またはエンドユーザ通知内容を変更したい場合、こちらの作業依頼から依頼いただくことで変更・設定いただけます。

＜Severity 毎の自動対処内容変更＞

- 「自動ログ分析/自動通知」または「自動ログ分析/自動通知/自動対処」を利用している場合で「自動通知」または「自動対処」の Severity 設定に変更がある場合は、申請に基づき設定します。
- 作業依頼についてはお客さまで、カスタマーポータルのサービス設定情報画面にある「ヒアリングシート（Severity 設定用）」をダウンロードしていただき、内容を記載いただきカスタマーポータルからファイル添付いただきます。
- 自動通知についてはお客様の要望に合わせて、「ON/OFF」を申請に基づき設定します。
- Severity 毎に対処パターンを選択していただくことでお客さまの要望に沿った自動対処を実施します。
- 変更する Severity 毎の対処パターンは「**WideAngle マネージド SOAR_自動対処機能説明書【ご契約者様向け】**」をご参照ください。

<パスワード変更が必要なエンドユーザに対して実施されるエンドユーザ通知内容変更>

- パスワード変更が必要なエンドユーザに対するエンドユーザ通知の内容について設定に変更がある場合は、申請に基づき設定します。
- 作業依頼についてはお客さまで、カスタマーポータルのサービス設定情報画面にある「ヒアリングシート（Severity 設定用）」をダウンロードしていただき、内容を記載いただきカスタマーポータルからファイル添付いただきます。
- エンドユーザ通知の内容と項目はパスワード変更回数に基づき以下 2 パターンとなります。 *1
- エンドユーザ通知のメールは、カスタマーポータル（ServiceNow）を介することなく、ロジックアプリが「HTTP」コネクタを使用して Graph API の sendMail メソッドでメール送信いたします。

通知パターン / **項目**	**パスワード変更上限回数内** *2	**パスワード変更上限回数超過時**
送信元メールアドレス	お客さまにて指定可能（他パターンと共通）	
送信先メールアドレス	アラートが発生したユーザーのメールアドレス	
件名	お客さまにて指定可能	お客さまにて指定可能
本文	・アラート発生時、システム側でのパスワード変更が実施されますが、変更後のパスワードは固定パスワードになりますので、お客さまご自身でパスワード変更を行うことを推奨いたします。	・パスワード変更上限回数に達した場合、アラート発生時にシステム側でのパスワード変更が実施されませんので、セキュリティ上の観点より、お客さまご自身でパスワード変更を行う必要があります。

	通知内容はお客さまが任意で設定を行うため、以下の内容を盛り込むように通知内容を設定することを推奨いたします。 ①お客さまご自身でパスワード変更を行うことを促すような通知内容。 ②メールとのすれ違いでユーザーがすでにパスワード変更を行っている可能性があるため、そちらを考慮するような通知内容。	通知内容はお客さまが任意で設定を行うため、以下の内容を盛り込むように通知内容を設定することを推奨いたします。 ①お客さまご自身でパスワード変更を行うことを促すような通知内容。

*1 パスワード変更：「0：(パス変無し)」を選択されている、かつエンドユーザ通知：「1：通知有り」を選択している場合についても、通知内容の指定が可能です。指定した場合、「パスワード変更回数」で設定した数値を基準に、アラートの発生回数によって通知内容が切り替わります。

*2 お客さまご自身でのパスワード変更を実施した後に、すれ違いでメールが送信される場合もございますのであらかじめご了承ください。

＜初回 AIR の結果が NG だった場合に実施されるエンドユーザ通知内容変更＞

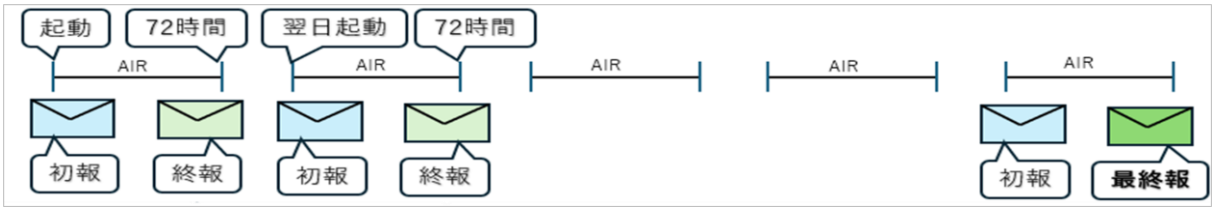
- MDE の AIR 初回 NG 時に、当該時間帯にホストを利用したアカウントを特定し、MFA 登録メールアドレス宛へ定型文で通知を自動送信します。そのエンドユーザ通知の内容について設定に変更がある場合は、申請に基づき設定します。
- 作業依頼についてはお客さまで、カスタマーポータルのサービス設定情報画面にある「ヒアリングシート（Severity 設定用）」をダウンロードしていただき、内容を記載いただきカスタマーポータルからファイル添付いただきます。
- 作業依頼についてはお客さまで、カスタマーポータルのサービス設定情報画面にある「ヒアリングシート（Severity 設定用）」をダウンロードしていただき、内容を記載いただきカスタマーポータルからファイル添付いただきます。
- エンドユーザ通知のメールは、カスタマーポータル（ServiceNow）を介することなく、ロジックアプリが「HTTP」コネクタを使用して Graph API の sendMail メソッドでメール送信いたします。
- Microsoft Defender for Business では、本機能はご利用できませんので、お申込書のヒアリングシートで「初回 AIR 失敗時のエンドユーザ通知」は選択いただけません。（EU 通知が「通知有り」を選択できません。）

項目	通知
送信元メールアドレス	お客さまにて指定可能
送信先メールアドレス	アラートが発生したユーザーのメールアドレス
件名	お客さまにて指定可能
本文	・アラート発生時、システム側でのウイルスキャンが実施されますが、AIRの処理が失敗した際は脅威を取り除けておりませんので、お客さまご自身でウイルススキャンを行うことを推奨いたします。 通知内容はお客さまが任意で設定を行うため、以下の内容を盛り込むように通知内容を設定することを推奨いたします。 ①お客さまご自身でウイルススキャン（フルスキャン）を行うことを促すような通知内容。 ②エンドユーザーより対応状況を報告してもらう通知内容。

＜AIR 自動再実行回数変更＞

- AIR 自動再実行回数を申請に基づき設定します。
- 以下は初期値 5 回の場合の処理イメージです。 1 回から 9 回までの間で設定可能です。
- AIR 再実行対象は AIR 失敗したもののみであり、成功したものは次回再実行対象から除外されます。

また、AIR 失敗理由が端末が既に存在していない等の場合で、再実行しても成功しないと判明している場合も再実行対象から除外されます。



2. XDR ポータル統合の解除
   - XDR ポータル統合を解除する場合は Microsoft Sentinel に設定が必要なため、申請に基づき設定作業を実施します。

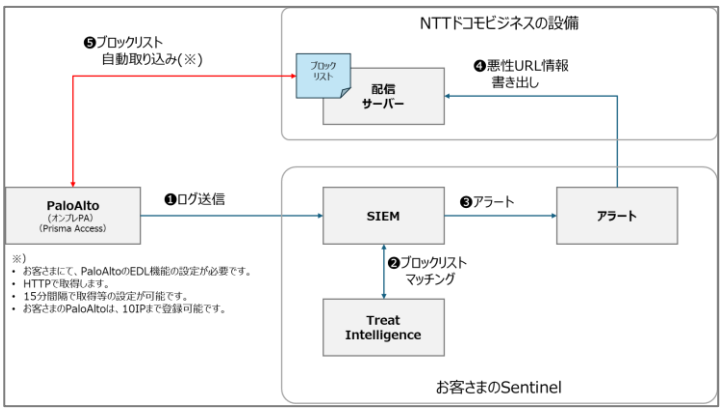
3. データコネクタの有効化／無効化
   - お客さまが追加／削除したいデータコネクタを、申請に基づき設定します。
   - 相関分析に必要なログ収集のため、Zscaler をはじめとするデータコネクタの追加/削除を作業依頼「各種設定変更」にて受け付けます。

- 1 回の作業依頼(2pt)につき、最大 10 個のデータコネクタ追加/削除作業を受け付けます。
- 既存でサービス提供している製品群は、本作業依頼の対象外とします。

4. 自動対処除外アラートの登録／削除
   - 指定されたアラート名の自動対処を除外します。また取り消しも受け付けます。
   - 作業依頼についてはお客さまで、カスタマーポータルのサービス設定情報画面にある csv ファイルをダウンロードしていただき、内容を記載いただきカスタマーポータルからファイル添付いただきます。
   - 「EDR-NCS_」から始まるアラートは、NTT ドコモビジネスが提供する WideAngle の SOC サービスをご利用の場合に提供される検知ルールによって生成されるアラートであり、その特性を考慮し、本サービスの標準仕様として自動対処除外アラートにあらかじめ登録されています。

5. 弊社構築のログ中継サーバーからのログ連携(Log API/DCR の設定)
   - NTT ドコモビジネス構築済みのログ中継サーバーからのログ取り込みに必要な Log Ingestion API／DCR を、申請に基づき設定します。

6. 弊社構築のログ中継サーバーに関する調査(Log API/DCR の設定確認)
   - NTT ドコモビジネス構築のログ中継サーバーの保守（調査・再起動 等）を申請に基づき実施します。
7. ブロックリスト利用(接続元 IP アドレスの登録/修正)／利用中止(接続元 IP アドレスの全削除)
   - Palo Alto に対し、ブロックリスト利用／利用中止のため、接続元 IP アドレスの登録／削除を申請に基づき実施します。
   - Threat Detection の契約が前提となります。
   - 最大 10IP まで登録できます。
   - 作業依頼のみの受付とします。お客さま側にて、Palo Alto 製品が HTTP 経由でブロックリストを自動取得・自動反映する構成とし、取得の為の EDL 機能の設定はお客さまの責任範囲となります。



8. WideAngle AI Advisor 連携の有効化／無効化

- WideAngle AI Advisor 連携を有効化する場合は、 WideAngle AI Advisor をご契約中のお客さまを対象に、契約中のすべてのデバイスに対して WideAngle AI Advisor 連携を有効化※します。本設定はデバイス単位では指定できず、作業依頼のお申し込み時点で契約中のすべてのデバイスに反映されます。
- 有効化の作業依頼では、自動対処を実施する際に参照する SeveritySource を申請いただきます。Microsoft の分析結果に基づいて自動対処を実施する場合は「SeveritySource：Microsoft」、WideAngle AI Advisor の分析結果に基づいて自動対処を実施する場合は「SeveritySource：WideAngle AI Advisor」と記載いただきます。なお、現時点でログ収集のみの契約であっても、将来的に自動対処を利用する可能性を踏まえ、SeveritySource を記載いただきます。
- また、既に WideAngle AI Advisor 連携を有効化済みのお客さまが、AI Advisor 連携自体は継続したまま SeveritySource のみを変更する場合も、「WideAngle AI Advisor 連携の有効化」の作業依頼として受け付けます。
- WideAngle AI Advisor 連携を無効化する場合は、申請に基づき、契約中のすべてのデバイスにおいて、WideAngle AI Advisor 連携を無効化します。無効化の作業依頼時に、お客さまが別途提出する項目はありません。
- WideAngle AI Advisor 連携を有効化の申し込みにあたっては、以下の条件を満たしている必要があります。

  ①WideAngle AI Advisor 連携に対応した Playbook が導入済みであること

  ②WideAngle AI Advisor が利用可能な状態であること
- WideAngle AI Advisor 連携における各サービスの責任範囲は、以下の通りです。

  ①WideAngle マネージド SOAR の責任範囲

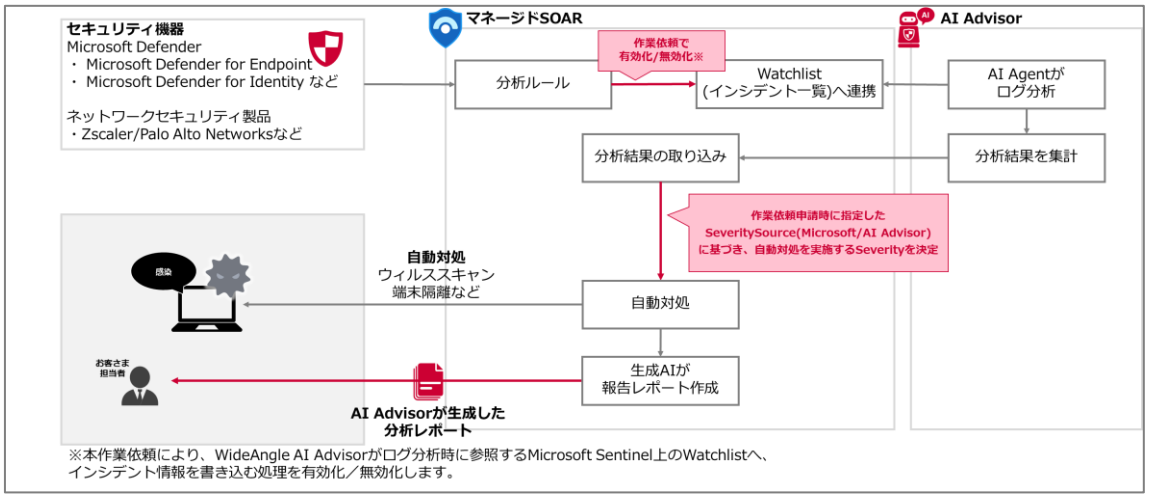
  Microsoft Sentinel 上のインシデントを Watchlist に記載します。AI Advisor 分析結果に基づき自動対処（ウイルススキャン、端末処理等）の実行

  ②WideAngle AI Advisor の責任範囲

  Sentinel 上の Watchlist を参照し、Watchlist に記載のインシデントをもとに

  ログ分析を実施し、その結果を Microsoft Sentinel のコメント欄に記載します。
- WideAngle AI Advisor の詳細な提供区分については、「WideAngle AI Advisor _サービス仕様書」に準ずるものとします。

※本作業依頼により、WideAngle AI Advisor がログ分析時に参照する Microsoft Sentinel 上の Watchlist へ、インシデント情報を書き込む処理を有効化／無効化します。



- 受付タイミング（●：受付あり）

作業依頼で実施する作業のいくつかは SO 工事と同時に、追加費用無く実施可能です。

作業依頼メニュー		受付タイミング		
		新設 SO	変更 SO	作業依頼
ログ保存期間変更		—	—	●
対処除外設定		●	—	●
各種設定変更	Severity 設定	●	●	●
	XDR ポータル統合の解除	—	—	●
	データコネクタの有効化／無効化	—	—	●
	自動対処除外アラートの登録／削除	—	—	●
	弊社構築のログ中継サーバーからのログ連携(Log API/DCR の設定)	—	—	●
	弊社構築のログ中継サーバーに関する調査(Log API/DCR の設定確認)	—	—	●
	ブロックリスト利用(接続元 IP アドレスの登録/修正)／利用中止(接続元 IP アドレスの全削除)	—	—	●
	WideAngle AI Advisor 連携の有効化／無効化	—	—	●

3.6. 提供条件

3.6.1. Microsoft Sentinel について

- お客さまには本サービスの提供に必要となる新規の Azure サブスクリプションをご準備いただきます。ご準備いただいたサブスクリプション上に、NTT ドコモビジネスが Microsoft Sentinel を構築します。
- 上記サブスクリプションは、お客さまが監視を希望される Microsoft 365 と同一テナント（同一の Microsoft Entra ID 管理）でご準備いただく必要があります。
- お客さまのサブスクリプションと NTT ドコモビジネスのサブスクリプションを Azure Lighthouse により連携します。NTT ドコモビジネスに対して権限を委譲していただくことで、本サービスの提供を実現します。
- NTT ドコモビジネスが本サービスで提供する Logic Apps 以外の、お客さま Azure テナントに対するサポート（故障対応を含む）は本サービスでは提供いたしかねます。
- Microsoft Sentinel のワークスペースを Defender ポータルに接続する Microsoft Defender XDR 統合を使用される場合は、NTT ドコモビジネスの Sentinel ワークスペースをプライマリとして構築します。

⚠ NTT ドコモビジネスからお客さまサブスクリプション内のリソース（仮想マシン、ストレージ、データベースなど）が確認可能な状態となるため、上記サブスクリプション上でのリソース作成はお控えください。

⚠ お客さまご自身で、Microsoft Sentinel をはじめとした Azure の設定を変更することにより、本サービスが正常に提供できなくなる可能性があります。（データコネクタの設定を変更する、ログ保存期間を変更する、Logic Apps の設定を変更する など）。

⚠ Microsoft Defender XDR 統合を解除すると分析ルールが再アクティブ化されず Playbook が正常に動作しないため、Microsoft Defender XDR 統合を解除した場合は作業依頼をお申し込みください。

3.6.2. サポートデバイス毎の構成条件・設定条件

- 各サポートデバイスを対象としてお申し込みいただく場合には、前提として、サポートデバイス毎に以下の構成、設定をしていただくことが提供条件となります。
- お客さまが各デバイスを利用中である場合に、Sentinel 標準のデータコネクタを利用して、Azure Monitor にログを取りこみ、Sentinel がログ分析を行います。
- 本サービスでサポートされるデバイスは、以下となります。

サポートデバイス	構成条件/設定条件
・Microsoft Entra ID P1	・Microsoft Entra ID Protection は、Microsoft Entra ID P1 ライセンスでは利用できません。 ・Azure テナント配下に、Microsoft Entra ID P1 と、Azure Monitor、Microsoft Sentinel が存在する構成とします。 ・Microsoft Entra ID P1 としてアラートが発生することを事前にご確認ください。 ・パスワードリセットなどの自動対処を実施するには、MFA（多要素認証）を設定いただいている必要があります。 ・Microsoft Entra ID のパスワードリセットをご希望の場合、SSPR（セルフサービスパスワードリセット）を有効にしていただいている必要があります。 ・オンプレミス AD のパスワードリセットも併せてご希望の場合には、Microsoft Entra ID に writeback を設定いただいている必要があります。 ・Microsoft Defender for Endpoint を契約、かつ、Microsoft Defender for Endpoint 連携をご希望しているお客さまは、Microsoft Entra ID P1 の検知をトリガーに、Microsoft Defender for Endpoint の自動対処が動作します。 *1*4*5 ・Microsoft Entra ID P1 では UEBA の契約がない場合でも UEBA 機能を有効にいたします。
・Microsoft Entra ID P2	・Microsoft Entra ID Protection は、Microsoft Entra ID P2 ライセンスをお持ちのお客さまが利用できる機能です。 ・Azure テナント配下に、Microsoft Entra ID P2 と、Azure Monitor、Microsoft Sentinel が存在する構成とします。 ・Microsoft Entra ID P2 としてアラートが発生することを事前にご確認ください。

	・パスワードリセットなどの自動対処を実施するには、MFA（多要素認証）を設定いただいている必要があります。 ・Microsoft Entra ID のパスワードリセットをご希望の場合、SSPR（セルフパスワードリセット） を有効にしていただいている必要があります。 ・オンプレミス AD のパスワードリセットも併せてご希望の場合には、Microsoft Entra ID に writeback を設定いただいている必要があります。 ・Microsoft Defender for Endpoint を契約、かつ、Microsoft Defender for Endpoint 連携をご希望しているお客さまは、Microsoft Entra ID P2 の検知をトリガーに、Microsoft Defender for Endpoint の自動対処が動作します。 *1*4*5
・Microsoft Defender for Identity	・Microsoft Defender for Identity ライセンスをお持ちである必要があります。 ・Azure テナント配下に、Microsoft Defender for Identity と、Azure Monitor、Microsoft Sentinel が存在する構成とします。 ・Microsoft Defender for Identity で監視対象のオンプレミスの Active Directory サーバーには、お客さまにて Agent（センサー）がインストールされ有効化されている必要があります。Microsoft Defender for Identity としてアラートが発生することを事前にご確認ください。 ・パスワードリセットなどの自動対処を実施するには、MFA（多要素認証）を設定いただいている必要があります。 ・Microsoft Entra ID のパスワードリセットをご希望の場合、SSPR（セルフサービスパスワードリセット）を有効にしていただいている必要があります。 ・オンプレミス AD のパスワードリセットも併せてご希望の場合には、Microsoft Entra ID に writeback を設定いただいている必要があります。 ・Microsoft Defender for Endpoint を契約、かつ、Microsoft Defender for Endpoint 連携をご希望しているお客さまは、Microsoft Defender for Identity の検知をトリガーに、Microsoft Defender for Endpoint の自動対処が動作します。 *1*4*5
・Microsoft Defender for Endpoint ・Microsoft Defender for Business	・Microsoft Defender for Endpoint Plan2 ライセンスをお持ちである必要があります。 ・Azure テナント配下に、Microsoft Defender for Endpoint と、Azure Monitor、Microsoft Sentinel が存在する構成とします。

	・Microsoft Defender for Endpoint で監視対象の Client 端末には、お客さまにて Agent が全て有効化されている必要があります。 Microsoft Defender for Endpoint としてアラートが発生することを事前にご確認ください。 ・Microsoft Defender for Endpoint は、複数の機能がありますが、本サービスでは「アンチウィルス」「EDR」の 2 つの機能に絞って運用を行います。 ※Microsoft Defender for Business については、上記「Endpoint Plan2」または「Endpoint」を「Business」と読み替えて下さい。
・Microsoft Defender for Cloud Apps	・Microsoft Defender for Cloud Apps ライセンスをお持ちである必要があります。 ・Azure テナント配下に、Microsoft Defender for Cloud Apps と、Azure Monitor、Microsoft Sentinel が存在する構成とします。 ・Microsoft Defender for Cloud Apps としてアラートが発生することを事前にご確認ください。 ・パスワードリセットなどの自動対処を実施するには、MFA（多要素認証）を設定いただいている必要があります。 ・Microsoft Entra ID のパスワードリセットをご希望の場合、SSPR（セルフサービスパスワードリセット）を有効にしていただいている必要があります。 ・オンプレミス AD のパスワードリセットも併せてご希望の場合には Microsoft Entra ID に writeback を設定いただいている必要があります。 ・Microsoft Defender for Cloud Apps は、主に脅威検知とシャドーIT 検知の機能がありますが、本サービスでは「脅威検知」の対応を実施します。 ・Microsoft Defender for Endpoint を契約、かつ、Microsoft Defender for Endpoint 連携をご希望しているお客さまは、Microsoft Defender for Cloud Apps の検知をトリガーに、Microsoft Defender for Endpoint の自動対処が動作します。 *1*4*5
・Microsoft Defender for Office 365	・Microsoft Defender for Office 365 Plan2 ライセンスをお持ちである必要があります。 ・Azure テナント配下に、Microsoft Defender for Office 365 と、Azure Monitor、Microsoft Sentinel が存在する構成とします。 ・Microsoft Defender for Office 365 としてアラートが発生することを事前にご確認ください。

	・Microsoft Defender for Endpoint を契約しているお客さまは、Microsoft Defender for Office 365 の検知をトリガーに、Microsoft Defender for Endpoint の自動対処が動作します。 *1*4*5
・UEBA *2	・UEBA の利用には、Microsoft Entra ID P1 or Microsoft Entra ID P2 のログ収集が必須となります。このため、Microsoft Entra ID P1 or Microsoft Entra ID P2 ライセンスをお持ちである必要があります。 ・Azure テナント配下に、Microsoft Entra ID P1 or Microsoft Entra ID P2 と Azure Monitor、Microsoft Sentinel が存在する構成とします。 ・Microsoft Entra ID P1 or Microsoft Entra ID P2 としてアラートが発生することを事前にご確認ください。 ・Microsoft Entra ID P2 のログ収集のうち、本機能の対象となるのは Microsoft Entra ID P2 の AuditLogs、SigninLogs のみで、Microsoft Entra ID Protection は分析対象とはなりません。 ・Microsoft Entra ID P1 のログ収集のうち、本機能の対象となるのは Microsoft Entra ID P1 の Audit Logs、SigninLogs です。
・Threat Detection *3	・お客さまから転送されるログが、CEF 形式か Syslog 形式の場合は、Microsoft が保有する脅威インテリジェンスとのマッチング結果に加えて、詳細な検知方法が通知されます。（どのデバイス、いつ検知したか、セキュリティデバイスでの Action の結果） ・お客さまから転送されるログが、CEF 形式か Syslog 形式の場合、かつ、MDE を契約しているお客さまは、Threat Detection の検知をトリガーに、MDE の自動対処が動作します。 *1 ・お客さまから転送されるログが、CEF 形式/Syslog 形式でない場合は、通知されません。 ・お客さまにて、セキュリティデバイスの適切なログ送信設定、ログ中継サーバーの構築と Sentinel へのログ転送設定が必要です。 ・Threat Detection の契約は 1 つでも、複数のセキュリティデバイスのログを Sentinel に転送し、アラート通知を受け取ることができます。

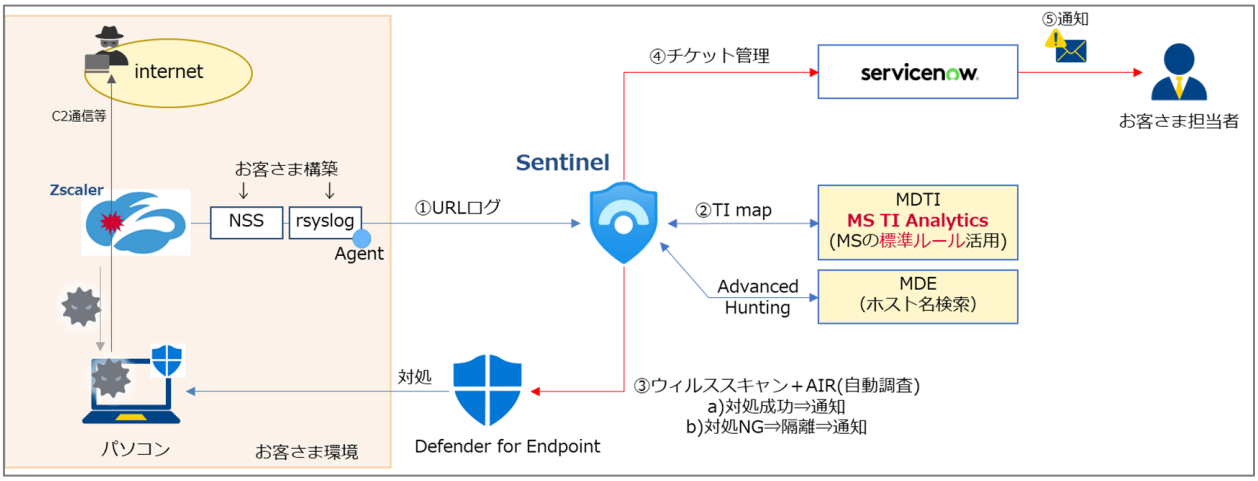
*1 Microsoft Defender for Business 連携は出来ません。

*2 デバイスではなく、Microsoft Sentinel に標準で実装されているユーザー/エンティティの行動分析ロジックです。

*3 デバイスではなく、NTT ドコモビジネス マネージド SOAR のメニュー名です。

*4 Microsoft Defender for Endpoint 連携時、Microsoft Entra ID に登録されているユーザー情報を取得します。このため、ホストへのログオン時に利用している情報が Entra ID に連携されていない場合は利用していたホストを特定できないため、連携機能を呼び出す事が出来ません。
*5 Microsoft Defender for Endpoint 連携については、Microsoft Defender for Endpoint の自動対処を正しく動作させるため、お客さま環境に応じてチューニングが必要となる場合があります。

3.6.3. Threat Detection ご利用時の固有の提供条件



<ログ中継サーバーの要件>

- ログ中継サーバーは、お客さまにて適切に設定、維持管理される必要があります。送信ログは、以下のログ要件を参照してください。
- ログ中継サーバーは、セキュリティデバイス 1 つにつき、1 つのログ中継サーバーを構築することをお勧めします。複数のセキュリティデバイスのログを 1 つのログ中継サーバーに転送してまとめることもできますが、以下の点を留意していただく必要があります。
  ① Microsoft Sentinel から見て、どのセキュリティデバイスから送信されてきたか特定することができません。(Microsoft Sentinel では、どのログ中継サーバーからログが送信されてきたか判断できます。したがって、ログ中継サーバーのホスト名をわかりやすくしておくことを推奨しています)
  ② CEF と Syslog でログが重複して出力される可能性があります。
  これに伴い、同じ内容のアラート通知メールの送付や対処が行われることになります。

<ログ要件>

- 以下のログを、Microsoft Sentinel にログ転送してください。CEF/Syslog 形式のみサポートされます。

ログの種類	転送の有無	ログ項目	備考
CEF の場合	いずれか必須	・RequestURL ・DestinationIP	値に「RequestURL」または「DestinationIP」の少なくとも一方が含まれるように設定してください。 このログが受信できないと、分析ロジック（Microsoft Threat Intelligence Analytics）が反応せず、検知されません。 ＊「RequestURL」の値はドメインのみではなくフルパスの URL となること。
	いずれか推奨	・SourceHostName ・SourceIP ・SourceUserName	ホスト情報特定に使用されるため、お客さまが Threat Detection でホスト対処を望む場合は 「SourceHostName」または「SourceIP」、 「SourceUserName」のいずれかに値が必要です。 但し、このログが受信できない場合でも MDE のログなどにてホスト情報特定処理を試みます。
	自動的に付与	・Computer	ログ中継サーバー名 ＊ Threat Intelligence 分析ルールでは使われないが、メールに載せるために必要です。 メールは以下の 2 種類あります。 ①アラート通知のメール（初報・終報兼用） ②ログ件数通知のメール
		・TimeGenerated	
Syslog の場合	必須	・Facility	値に“cron”が設定されているログに対して、分析ロジック（Microsoft Threat Intelligence Analytics）が反応して、検知が行われます。
		・SyslogMessage	値に、「通信先の URL」または「通信先の IP アドレス」の少なくとも一方が含まれるように設定してください。
	自動的に付与	・Computer	ログ中継サーバー名 ＊ Threat Intelligence 分析ルールでは使われないが、メールに載せるために必要です。 メールは以下の 2 種類あります。 ①アラート通知のメール（初報・終報兼用） ②ログ件数通知のメール

（参考）Microsoft Sentinel の仕様 URL（https://learn.microsoft.com/ja-jp/azure/sentinel/use-matching-analytics-to-detect-threats）

<ログ件数通知>

マネージド SOAR では、CEF/Syslog 形式のログを受信したときに、以下の動作で、ログの受信件数をお客さまにメールで通知します。

- 通知間隔：1 日ごと
- 通知内容：1 日ごとの、ログ受信件数を、ログ中継サーバーごとに表示

このログ件数通知のメールをお客さまにて確認することで、ログが正常に転送され、Microsoft Sentinel に保存されていることが確認できます。また、ログが極端に少ない場合や、ゼロになっている場合は、お客さまのセキュリティデバイスやログ中継サーバーに不具合が発生していることが考えられますので、ご確認ください。

また、半年間（180 日）ログ受信がないログ中継サーバーは自動で対象から削除します。

ただし、ログ保存期間が変更されている場合、期間の上限は 180 日までとなります。

メールイメージ

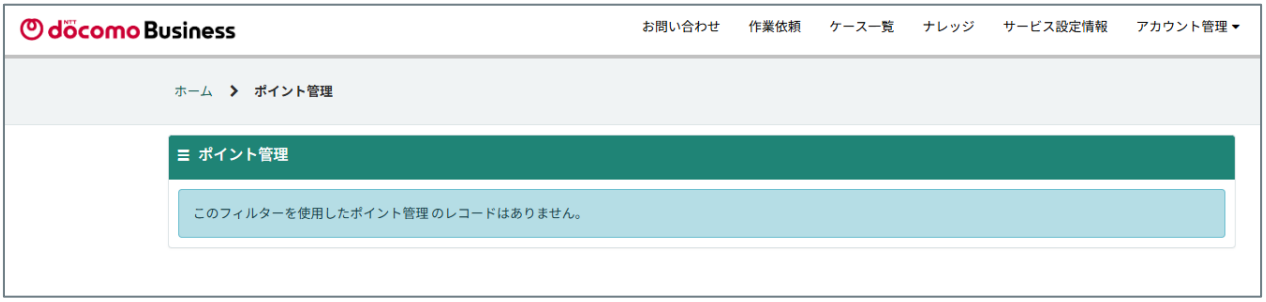
TO：（アラート通知先と同じ）
FROM：（アラート通知の送信元と同じ）
TITLE：ログ件数通知 / Log count notification-[お客様番号]
――――――――――
本文：
お客さまへ
平素はNTTドコモビジネスのサービスをご利用いただき誠にありがとうございます。
直近24時間での各ログ中継サーバーからのログ件数をお知らせいたします。
・ログ中継サーバーのComputer名
Cef：　〇〇件
Syslog:〇〇件
・ログ中継サーバーのComputer名
Cef：　〇〇件
Syslog:〇〇件
・ログ中継サーバーのComputer名
Cef：　〇〇件
Syslog:〇〇件
　　・・・・

3.6.4. ポイント

- ポイントとは、作業依頼の申請および実施に必要となる単位で、本サービスのオプション「作業依頼ポイント」では、5 ポイント単位で契約いただけます。
- NTT ドコモビジネス セキュリティアドバイザリーセンターに作業依頼を実施する際には、作業に応じてポイントを消費します。

- 基本プランにはポイントは含まれませんので、必要なお客さまはオプション（作業依頼ポイント追加）をご契約いただくことにより、毎月発行されるポイント数を追加いただけます。
- 「自動ログ分析/自動通知/自動対処」の機能を 1 デバイスでもご契約いただくお客さまは、合わせてオプション（作業依頼ポイント追加）もご契約いただくことを推奨しております。
- 「自動ログ分析/自動通知/自動対処」をご利用の場合、アラートの発生状況やお客さま環境の運用状況に応じて、自動対処除外アラートの登録、Severity 設定の変更など、各種設定変更が必要となる場合があります。これらの設定変更を行う際には、ポイントを消費する作業依頼を申請いただく必要があります。
- 作業依頼ポイントをご契約いただいていない場合、または申請時に残ポイントがない場合、カスタマーポータルから作業依頼を申請することができません。その場合、特定のアラート通知を抑制したいあるいは自動対処内容を変更したいといったご要望に対して、作業依頼による設定変更を速やかに実施できない可能性があります。
- ポイントは、お客さまが作業依頼の申請を行い、セキュリティアドバイザリーセンターにて作業内容を確認し承認した時点で消費されます。作業内容・申請書の不備などにより、確認作業が行われ、承認が遅れることもあります。
- ポイントは利用開始日または変更日に発行（翌月以降は月単位で毎月 1 日に発行）され、消費されなかったポイントはその月末に失効します。残ポイントはカスタマーポータル上で確認することができます。

（参考）カスタマーポータルイメージ



3.7. サービスレベル

- 本サービスは、SLA/SLO の定めはありません。
- 本サービスでは、自動ログ分析（自動ログ収集 *1）機能の正常性の監視結果の確認を、セキュリティアドバイザリーセンターにて行います。この確認の頻度は、営業日に 1 日 1 回とします。

*1 Threat Detection は、自動ログ収集機能を提供していないため、自動ログ収集機能の正常性の監視は行いません。

　正常性監視の代替手段として、ログ件数通知のメールを 1 日 1 回送付しますが、本サービスによる正常性の監視は行いません。

3.8. 提供地域

- 日本国内の法人、かつ日本国内での契約を対象とします。

※当サービスでは NTT ドコモビジネス側の工事として、お客さま Azure テナントに Microsoft Sentinel を Japan-East リージョンで構築します。

4. 工事・故障対応

4.1. 工事

4.1.1. 各種工事

本サービスの工事の種類は、以下となります。対象のサポートデバイスについては、「**3.4 提供機能一覧**」を参照してください。

【提供工事一覧】

分類	工事	単位	対象	申込形態
基本設定	基本設定工事	契約	Sentinel 基盤	新設
バックアップ	ログバックアップ工事	契約	Sentinel 基盤	変更
利用設定	利用設定工事（ログ収集）	デバイス	「ログ収集」のサポートデバイス	新設/変更
	利用設定工事（自動ログ分析/自動通知）	デバイス	「自動ログ分析/自動通知」のサポートデバイス ※UEBA の任意ログソース追加	新設/変更
	利用設定工事（自動ログ分析/自動通知/自動対処）	デバイス	「自動ログ分析/自動通知/自動対処」のサポートデバイス	新設/変更
設定変更	設定変更工事（ログ収集 Configuration 設定変更）	デバイス	・Microsoft Entra ID P1 ・Microsoft Entra ID P2 ・MDCA	変更
	設定変更工事（自動ログ分析任意ログソース変更）	デバイス ※	・UEBA	変更
利用削除設定	利用削除設定工事（ログ収集）	デバイス	「ログ収集」のサポートデバイス	変更
	利用削除設定工事（自動ログ分析/自動通知）	デバイス	「自動ログ分析/自動通知」のサポートデバイス	変更
	利用削除設定工事（自動ログ分析/自動通知/自動対処）	デバイス	「自動ログ分析/自動通知/自動対処」のサポートデバイス	変更

＜基本設定工事＞

サービス開通にあたり、基本設定を行う工事です。

＜ログバックアップ工事＞

サービス開通後にログのバックアップ設定の変更（バックアップを ON にする、または ON にしたものを OFF にする）を希望される場合に発生する工事です。

ログバックアップ工事によりバックアップ設定を ON とした場合のログ保存期間は「12 年」です。対象デバイス毎に、バックアップ対象のログが異なります。

【バックアップ対象一覧】

バックアップ対象	・Microsoft Entra ID P1 ・Microsoft Entra ID P2	・Microsoft Defender for Identity	・Microsoft Defender for Endpoint ・Microsoft Defender for Business	・Microsoft Defender for Cloud Apps	・Microsoft Defender for Office 365	・UEBA	・Threat Detection
SigninLogs	●						
AuditLogs	●						
AADServicePrincipalSignInLogs	●						
AADManagedIdentitySignInLogs	●						
AADProvisioningLogs	●						
ADFSSignInLogs	●						
AADUserRiskEvents	●						
AADRiskyUsers	●						
NetworkAccessTraffic	●						
AADRiskyServicePrincipals	●						
AADServicePrincipalRiskEvents	●						
SecurityAlert	●	●	●	●	●		
McasShadowItReporting				●			
AzureActivity						●*	
SecurityEvents						●*	
BehaviorAnalytics						●	

SecurityIncident	●	●	●	●	●	●	●
CommonSecurityLog							●
Syslog							●

*UEBA の自動ログ分析/自動通知の対象として、任意ログ「AzureActivity」「SecurityEvents」をお申し込みされた場合のみ対象です。

＜利用設定工事＞

「ログ収集」、「自動ログ分析/自動通知」、「自動ログ分析/自動通知/自動対処」を新設と同時に利用する場合、または、開通後に利用追加する場合に発生する工事です。

UEBA の任意ログソースを「自動ログ分析/自動通知」の対象としたい場合の工事も含みます。

＜設定変更工事（ログ収集 Configuration 設定変更）＞

対象のデバイスについて「ログ収集」を利用している場合で、Configuration 設定の変更を希望される場合に発生する工事です。

XDR 化すると「Cloud Discovery Logs (Preview)」のデータは収集されているので、変更 SO における「ログ収集　Configuration 設定変更　：　Microsoft Defender for Cloud Apps」は、申し込み不要となります。

＜設定変更工事（自動ログ分析 任意ログソース変更＞

「自動ログ分析/自動通知」の UEBA を利用している場合で、UEBA の対象ログソースに変更が必要な場合に発生する工事です。

一度の申し込みで指定いただく、対象または対象外とする任意ログソースの数は問いません、幾つでも 1 デバイスとして扱います。

＜利用削除設定工事＞

「ログ収集」「自動ログ分析/自動通知」「自動ログ分析/自動対処」を利用している場合で、その利用をやめる場合（本サービス自体の契約は継続）に発生する工事です。

4.1.2. 工事に関する留意事項

＜初期開通時（新設工事）＞

NTT ドコモビジネス側では以下の設定（工事）を実施します。

- サブスクリプション名（修正）
- リソースグループ作成
- Log Analytics ワークスペース作成
- Lighthouse 接続設定
- 監視用 Logic Apps のデプロイ

初期開通時（新設工事）に際して、お客さまには事前に以下の作業を実施いただく必要があります。

- 「**マネージド SOAR_NTT Com 工事用アカウント準備ガイド_WideAnglePS**」に基づき、工事用の NTT ドコモビジネス利用アカウントの作成。
- 提供機能「自動ログ分析/自動通知/自動対処」を「Microsoft Entra ID P1」、「Microsoft Entra ID P2」、「Microsoft Defender for Cloud Apps」、「Microsoft Defender for Identity」、「Microsoft Defender for Business」および「Microsoft Defender for Endpoint」のいずれかの対象デバイスについてお申し込みの場合で、「検知試験用端末・ホスト準備」を「お客さま準備」を選択された場合の検知試験用端末・ホスト準備。
- Threat Detection を契約する場合は、お客さまのセキュリティデバイスとログ中継サーバーの設定は、お客さまにて実施頂きます。
- Threat Detection において「ログ保存」の試験を行います。お客さまのセキュリティデバイスでログを発生させ、NTT ドコモビジネスは Sentinel 上で CommonSecurityLog、Syslog を確認しログが保存されていることを確認します。

⚠ 「Microsoft Defender for Identity」をお申し込みされた場合は、「お客さま準備」のみとなります。

⚠ 初期開通工事は、申込書にて指定された開通希望日前に行います。そのため、自動分析/自動通知/自動対処の処理、ログ件数通知*1 の送付が開通希望日前から開始される場合があります。（カスタマーポータルへのアクセスは、開通希望日以降に可能となります。）
*1 ログ件数通知は、Threat Detection を申し込んだ場合に送付されるメールです。

＜変更工事＞

本サービスの変更工事時に、初期開通時と同様、お申し込み内容により検知試験用端末・ホスト準備をお客さま側で実施いただきます。

⚠ 変更工事は、申込書にて指定された変更希望日前に行います。そのため、変更申込にて新たに申し込まれた自動分析/自動通知/自動対処の処理、ログ件数通知*1 の送付が変更希望日前から開始される場合があります。また、変更申込にて廃止した自動分析/自動通知/自動対処の処

理、ログ件数通知*1 の送付についても、申込書にて指定された変更希望日前に行いますので、変更希望日前に停止される場合があります。
*1 ログ件数通知は、Threat Detection を申し込んだ場合に送付されるメールです。

＜廃止工事＞

本サービスの廃止（解約）の場合は、「ログ収集/自動ログ分析/自動通知/自動対処の設定は全削除」または「ログ収集設定のみ残し、自動ログ分析/自動通知/自動対処の設定は全削除」から選択いただきます。

本サービスの廃止工事時に、初期開通時に設定いただいた工事用の NTT ドコモビジネス利用アカウントの削除を、お客さま側にて実施いただきます。

⚠ ログバックアップの設定（ON/OFF）は削除されずそのままとなります。本サービスの廃止に伴いログバックアップ設定も OFF にしたい場合は、事前に変更申込が必要です。

⚠ Log Analytics ワークスペースは、Sentinel 以外で利用している可能性があるため廃止工事では削除いたしません。

⚠ 廃止工事は、廃止申込書にて指定された廃止希望日の翌日以降に行います。そのため、カスタマーポータルへのアクセスは不可となりますが、自動分析/自動通知/自動対処が廃止希望日の翌日以降も処理される場合があります。

また、廃止希望日の翌日以降から NTT ドコモビジネス利用アカウント削除依頼までに、NTT ドコモビジネス側で実施する廃止工事のため、お客さまテナントにログインし作業を実施いたします。

4.2. 故障対応

本サービスでは、本サービスで提供する Playbook 機能の正常性確認のための監視ロジック*から異常を検知した場合や、作業依頼などの対応中に故障が疑われる挙動を検知した場合、またお客さまより故障のお問い合わせをいただいた場合に、調査を行い以下の対応を行います。

- 必要に応じて NTT ドコモビジネスにて原因の調査を実施し、故障と判断された場合はセキュリティアドバイザリーセンターよりお客さま通知を行います。
- また、NTT ドコモビジネスにて復旧対応を実施する必要がある場合については、NTT ドコモビジネスにて復旧対応を行います。

*Microsoft 社の提供する基盤を監視しているわけではありません。お客さま Azure テナントの故障については、お客さまにて対応をお願いいたします。

【調査結果と通知・対応】

故障箇所	原因	通知・対応
Playbook の故障 NTT ドコモビジネス Azure テナントの故障	NTT ドコモビジネスの設定または Playbook が原因と判断された場合	カスタマーポータルを通じてお客さまに通知し、NTT ドコモビジネスにて復旧対応を行います
	お客さま側の設定が原因と判断された場合	カスタマーポータルを通じてお客さまに通知し、お客さまにて復旧対応を行っていただきます
	Microsoft 側の故障が原因と判断された場合、または Microsoft 社から故障情報がアナウンスされた場合	カスタマーポータルを通じてお客さまに通知する（Microsoft 社が提供するクラウドサービスのため、NTT ドコモビジネスによる復旧対応は行いません）
カスタマーポータルの故障	ServiceNow の故障が原因と判断された場合、または ServiceNow 社から故障情報がアナウンスされた場合	カスタマーポータルが利用できない場合、NTT ドコモビジネスお客さまサポートに故障情報を掲載します（他社が提供するクラウドサービスのため、NTT ドコモビジネスによる復旧対応は行いません）
お客さま Azure テナントの異常	お客さまが調達し、他社が提供するクラウドサービスのため、NTT ドコモビジネスによる調査、復旧対応は行いません	

サポートサイト

本サービス情報サイトとして、NTT ドコモビジネス サポートサイトを公開しています。
https://support.ntt.com/wideangle-soar

5. 料金

5.1. サービスの価格

- 本サービスの料金は、**WideAngle マネージド SOAR_利用規約**の料金表に定めます。
- 本サービスに係るオプション「作業依頼ポイント追加」の料金は、本オプションサービスで追加される追加ポイント数 5 ポイント単位に応じて計算します。

6. お申し込み・ご利用

6.1. お申し込み

6.1.1. 申込方法

- 申し込み内容によって、新設、変更、簡易変更、廃止の申込パターンがあります。
- ご契約者情報の変更（譲渡/改称/継承など）は、簡易変更申込書で対応します。

申込パターン	説明	申込書	ヒアリングシート	Severity 設定用ヒアリングシート	対処除外設定リスト
新設	新規で契約する場合	●	●	●	●*1
変更	料金変更が発生する以下の契約変更の場合 ・利用機能（ログ収集/自動ログ分析/自動通知/自動対処）の追加/変更/削除 ・オプション（作業依頼ポイント追加）の追加/変更/削除 料金変更が発生しない以下の契約変更および設定変更の場合 ・利用機能（ログ収集のみ）の追加/削除 ・ログ収集（Configuration 設定変更）の設定変更 ・自動ログ分析（UEBA の任意ログソース変更）の設定変更 ・ログバックアップ（ON/OFF）の設定変更	●	●*3	●*4	-*2
簡易変更	料金変更が発生しない以下の契約変更の場合 ・譲渡/改称/継承などによる契約者情報の変更 ・契約者住所の変更 ・契約に関する連絡先の変更	●	-	-	-
廃止	契約を解約する場合	●	●	-	-

*1. 新設時に自動対処の除外設定をリスト指定で申し込む場合に必要です。

*2. 自動対処除外対象を設定する場合や、対処除外対象の設定内容を変更する場合は、カスタマーポータルからの作業依頼となります。

*3. 変更時、オプション（作業依頼ポイント追加）の追加/変更/削除のみの申し込みの場合は、新設・変

更・廃止用ヒアリングシートは不要です。

*4. Severity 設定またはエンドユーザ通知内容を変更する場合は、カスタマーポータルからの作業依頼となります。

ただし、利用機能（ログ収集/自動ログ分析/自動通知/自動対処）の追加/変更を行う際は、Severity 設定やエンドユーザ通知内容を指定していただく必要がありますので、変更申し込みで受け付けます。

また、Severity 設定用ヒアリングシートは契約情報も管理している関係上、利用機能（ログ収集/自動ログ分析/自動通知/自動対処）の削除を行う際にも送付が必要となります。

6.1.2. 申込書

- サービスを新規で契約する際、契約内容を変更する際、解約する際の申込書式です。
- 申込パターンによって、新設、変更、簡易変更、廃止の申込書があります。

申込パターン	申込書
新設	新設申込書
変更	変更申込書
簡易変更	簡易変更申込書
廃止	廃止申込書

6.1.3. ヒアリングシート

- サービス提供に必要な詳細ヒアリング情報をお客さまに記入いただくシートです。
- 新設、変更（*1)、廃止をお申し込みの際に、申込書と合わせてヒアリングシートを添付いただきます。ここで記載いただく初期ポータル管理者のメールアドレスの末尾に「.so」を付加したもの（例：taro@ntt.com.so）をユーザーID として設定（*2）し、そのユーザーID を初回カスタマーポータルログイン時にご利用いただきます。

  *1 変更のお申し込み時、オプション（作業依頼ポイント追加）の追加/変更/削除のみのお申し込みの場合は、ヒアリングシートの添付は不要です。

  *2 メールアドレスが 38 文字以上の場合は、原則 38 文字以降を削除して末尾に「.so」を付加したもので設定します。

  （カスタマーポータルのユーザーID の仕様上、最大文字数が 40 文字であるため）

6.1.4. 対処除外設定リスト

- サービスを新規で契約する際、また新設時以降に対処除外を設定する場合や、設定内容を変更する場合、自動対処の除外対象（ホスト、アカウント、アラート情報のリスト指定）を記入いただくリストです。
- 対処除外設定が不要な場合や、リスト指定以外の設定（全ホスト、全アカウント指定）の場合は、お客さまでの提示は不要です。
- 対処除外設定リストは「ホスト指定用（Host.csv）」と「アカウント指定用（Account.csv）」、「アラート指定用（Alert.csv）」の 3 種類あります。新設時のヒアリングシートの「サービス開通時の自動対処除外設定条件」の指定内容に合わせて、対処除外設定リストを添付いただきます。
- 対処除外設定リストの種別に応じて、以下の作業依頼を選択してください。

リスト種別(ファイル名)	申請いただく作業依頼種別
ホスト指定用(Host.csv)	2. 対処除外設定
アカウント指定用(Account.csv)	
アラート指定用(Alert.csv)	3. 各種設定変更 ＞ ⑤自動対処除外アラートの登録 3. 各種設定変更 ＞ ⑥自動対処除外アラートの削除

⚠ 新設時以降に対処除外対象を設定する場合や、対処除外対象の設定内容を変更する場合は、お客さまのカスタマーポータル画面より、作業依頼にてお申し込みください。

なお、カスタマーポータル上では、以下の名称で登録されております。

ホスト指定用：No-Action-Host_N 番_yyyymmdd.csv（ 旧 Host.csv ）

アカウント指定用：No-Action-Account_N 番_yyyymmdd.csv（ 旧 Account.csv ）

アラート指定用：Exclusion-Alert_N 番_yyyymmdd.csv（ 旧 Alert.csv ）

⚠ アラートのリスト指定につきましては、作業依頼のみでの受付となります。

6.1.5. 開通試験

＜開通までの流れ＞

- 下記 4 点の作業・確認をもって、開通 OK 判断を実施します。

① 保守情報シート一括登録：カスタマーポータルを利用するために必要なお客さま情報を登録

② Microsoft Sentinel 設定：お客さまの Azure、Microsoft Sentinel などへのサービス提供に必要な設定を実施

③ ローカル試験：お客さま環境にデプロイした Playbook の動作確認

④ 検知試験：お客さまのご協力のもとアラートを発生させ、ログ収集/自動ログ分析/自動通知/自動対処が想定通り動作するかどうか確認

検知試験は、お客さま環境などに依存してイベントが発生できない場合があります。
この場合は、設定状態チェックなどの代替手段により確認を行うことになります。

＜検知試験概要＞

- Microsoft Entra ID P1、Microsoft Entra ID P2、Microsoft Defender for Identity、Microsoft Defender for Endpoint、Microsoft Defender for Business、Microsoft Defender for Cloud Apps において「自動ログ分析/自動通知/自動対処」をお申し込みの場合に実施します。
- また、試験実施にあたっては NTT ドコモビジネス 工事統制担当より検知試験用のガイドおよびチェックシートをお客さまに送付します。
- 試験用の端末については、サービスお申し込み時にお客さま準備/ NTT ドコモビジネス準備を選択いただきます。ただし Microsoft Defender for Identity を申し込まれた場合はお客さまにご準備いただきます。また、試験用のアカウントについても別途ご準備いただきます。
- 検知試験に必要な端末・アカウントの準備にご協力いただけない場合や、下記の試験内容の実施に同意いただけない場合には、検知試験は実施いたしませんのでご了承ください。
- お客さまのお申し込み内容に合わせて検知試験を実施します。（たとえば、パスワードリセットや端末隔離をご要望いただいていない場合は、その検知試験はスキップとなります）

【サポートデバイス毎の試験内容】

サポートデバイス	**内容**
・Microsoft Entra ID P1 ・Microsoft Entra ID P2	• 試験用端末に Tor Browser をインストール • Tor Browser を立ち上げ、匿名 IP アドレスから Microsoft 365 ポータルにサインイン • Sentinel にてインシデントの生成がされていること、Logic Apps にて該当 Playbook の実行成功を確認 • 試験用アカウントのパスワードリセット動作を確認

	• MDE 連携を行っている場合は MDE 単体での検知試験で確認をさせていただくため、ホスト対処を実施するための Playbook 起動されるまでを試験とします。 • 試験用アカウントにエンドユーザ通知が送信されていることを確認
・Microsoft Defender for Identity	• 試験用端末にて擬似攻撃ツール（JoeWare の NetSess ツール）をダウンロード • 試験用端末にて擬似攻撃ツールを実行（ユーザーと IP アドレスの偵察を実行） • Sentinel にてインシデントの生成がされていること、Logic Apps にて該当 Playbook の実行成功を確認 • 試験用アカウントのパスワードリセット動作を確認 • MDE 連携を行っている場合は MDE 単体での検知試験で確認をさせていただくため、ホスト対処を実施するための Playbook 起動されるまでを試験とします。 • 試験用アカウントにエンドユーザ通知が送信されていることを確認
・Microsoft Defender for Cloud Apps	• Microsoft Defender for Cloud Apps 管理者センターにてポリシー（試験用端末の IP アドレスを「危険な IP アドレス」として設定）の準備 • 試験用端末にて Microsoft Defender for Cloud Apps 管理者センターへサインイン • Sentinel にてインシデントの生成がされていること、Logic Apps にて該当 Playbook の実行成功を確認 • 試験用アカウントのパスワードリセット動作を確認 • MDE 連携を行っている場合は MDE 単体での検知試験で確認をさせていただくため、ホスト対処を実施するための Playbook 起動されるまでを試験とします。 • 試験用アカウントにエンドユーザ通知が送信されていることを確認 • 事前準備したポリシーの無効化・削除
・Microsoft Defender for Endpoint ・Microsoft Defender for Business	• 試験用端末にて検知試験（PowerShell ISE によるファイル作成・編集）を実施 • Sentinel にてインシデントの生成がされていること、Logic Apps にて該当 Playbook の実行成功を確認 • 試験用端末が隔離（通信がブロック）されていることを確認 • 試験用端末が隔離から自動復帰し、通信が正常に実施できることを確認 • 試験用アカウントにエンドユーザ通知が送信されていることを確認（Microsoft Defender for Endpoint のみ）

6.2. 標準開通日

- 標準開通日は次の日程です。
- NTT ドコモビジネスが申し込みを受理し、不備が無いことを確認した時点から起算した日数となります。尚、当日 15 時を過ぎた場合は翌営業日受付の扱いとなります。

申込種別	標準開通日	備考
新設	14 営業日	左記の標準開通日は、お客さまの条件が満たされている場合の目安です。お客さま側の条件が満たされていない場合は、例外となります。
廃止	11 営業日	
変更	18 営業日 7 営業日（オプション（作業依頼ポイント追加）の追加/変更/削除のみの場合）	左記の標準開通日は、お客さまの条件が満たされている場合の目安です。お客さま側の条件が満たされていない場合は、例外となります。
簡易変更	5 営業日 （目安）	申込書に希望開通日はなく、また開通案内も送付しません。左記の標準開通日は目安です。

6.3. 開通案内・配布同梱物

- 新設申し込み、変更申し込みの場合に開通案内を発行します。
- 廃止申し込み、簡易変更申し込みの場合、開通案内などは発行しません。送付物は、NTT ドコモビジネスの BOX サービスを利用して送付します。次の手順でファイルを受領していただきます。

① お客さまへ、送信元が”<wa-sac-customer@ntt.com>”からメールが届きます
② お客さまはメール本文の URL をクリックして、BOX の Web サイトへアクセスします
③ ファイルダウンロードには、申込書に記載のパスワードを入力します

- 各申し込みで送付するものは次のものです。

申込 / 送付物	新設 「サービス利用開始のお知らせ」	変更 「サービス利用内容変更のお知らせ」
開通案内（ご利用内容のご案内）	●	●

サービス利用に必要な情報の通知 -カスタマーポータル URL/ユーザーID	●	-

6.4. お問い合わせ・作業依頼受付

- セキュリティアドバイザリーセンターにて、お客さまからのお問い合わせおよび作業依頼を受け付けます。
- お問い合わせは、同時にお問い合わせできるのは 1 件までとし、回答が完了し、ケースが Close となるまでは、次のお問い合わせをすることはできないため、窓口よりお断りさせていただきます。ただし、故障に関するお問い合わせはこの限りではありません。
- 作業依頼は、同時にご依頼できる作業は 1 件までとし、作業が完了し、ケースが Close となるまでは、次の作業依頼をすることはできないため、窓口よりお断りさせていただきます。

窓口業務	受付時間	手段	主な内容
お問い合わせ受付 作業依頼受付	カスタマーポータル受付： 24 時間 365 日 対応時間：平日（年末年始除く）9:00～17:00	カスタマーポータル	• サービスの内容に関するお問い合わせ • 作業依頼に関する受付、対応 • カスタマーポータルの操作方法に関するお問い合わせ

※カスタマーポータルの故障などによりご利用できない場合、一時的にお問い合わせをお受けできない場合がございます。

6.5. 故障受付

- セキュリティアドバイザリーセンターにて、お客さまからの故障のお問い合わせを受け付けます。

窓口業務	受付時間	手段	主な内容
故障お問い合わせ受付	カスタマーポータル受付： 24 時間 365 日 対応時間：平日（年末年始除く）9:00～17:00	カスタマーポータル	• 故障に関するお問い合わせ

※カスタマーポータルの故障などによりご利用できない場合、一時的にお問い合わせをお受けできない場合がございます。

6.6. お問い合わせ受付・運用受付/通知方法

- 作業依頼受付、問い合わせ受付の対応方法は以下となります。
- お客さまとのやり取りはカスタマーポータルを介して行われます。

項目	対応方法
お問い合わせ	・お客さまからのお問い合わせは、カスタマーポータルの「お問い合わせ」よりお客さまにてケース起票、お問い合わせ内容を入力いただき、セキュリティアドバイザリ―センターから回答をします。
作業依頼	・カスタマーポータルの「作業依頼」から申請いただき、セキュリティアドバイザリ―センターで内容を確認します。 ・「作業依頼」が受付された場合は「ケース」として起票されクローズまで管理されます。ケースとして起票された時点でポイントが消費されます。 ・「作業依頼」に不備がある場合は受付受理できない旨、理由が通知されます。

作業依頼の中でも、各種設定変更（Severity 設定）の場合、ヒアリングシートの不備チェック作業依頼内容の確認に伴い、作業依頼の受理・不受理の判定までに、3 営業日かかる場合があります。

＜お問い合わせについて＞

- マネージド SOAR のサービス仕様に関する問い合わせにご回答いたします。
- マネージド SOAR の技術仕様に関する問い合わせにご回答いたします。
- Microsoft 製品/Sentinel 製品に関する問い合わせはご回答できません。お客さまにて調達先にお問い合わせください。
- お客さま Azure テナントのログに関するお問い合わせにはご回答できません。また、お客さま Azure テナントのログの調査が必要なお問い合わせにはご回答できません。
- Threat Detection ご利用時におけるログ中継サーバーのログ取り込み設定、NTT ドコモビジネスが構築したログ中継サーバーの調査はカスタマーポータルの「作業依頼」で受け付けます。
- Threat Detection ご利用時におけるログ収集元セキュリティデバイスに関する問い合わせに対する回答および、ログの調査は行えません。
- マネージド SOAR で検知もしくは対処した結果の通知をトリガーとしたイベントの詳細については回答できません。

6.7. 工事通知（メンテナンス通知）

工事（メンテナンス）の通知は、カスタマーポータルに掲載します。

（1） 計画メンテナンス

- お客さま影響のある作業は「メンテナンス」として、サービス仕様として定義されたとおり事前の案内など必要な条件を満たした上で実施します。
- NTT ドコモビジネスが提供するカスタマーポータルは、毎月最終日曜日 22:00~翌月曜日 6:00（8 時間）までをメンテナンスウィンドウとしています。当該時間に監視が中断され、お客さまがカスタマーポータルにアクセスできない場合があります。当該時間に発生したイベント通知は、メンテナンスウィンドウが完了後に通知されます。
- 本メンテナンスウィンドウを利用して、NTT ドコモビジネスは、基盤設備のバージョンアップや不具合などの修正を行います。バグや脆弱性の対応については、NTT ドコモビジネスの判断基準において、月に 1 回の本メンテナンスウィンドウで、パッチ適用などの対処を行います。
- メンテナンスウィンドウにて NTT ドコモビジネスが作業を行う場合は、3 営業日前までにカスタマーポータル上で事前にアナウンスされます。
- カスタマーポータルは ServiceNow を利用しているため、ServiceNow のメンテナンスや障害によりアクセスできない場合があります。ServiceNow は通常年に 2 回アップデートがあり、1 カ月ごとにセキュリティパッチがリリースされます。

（2） 緊急メンテナンス

- サービスで利用するクラウドサービス（ServiceNow）のメンテナンスは、NTT ドコモビジネスにて実施時間帯をコントロールできない場合があります。その場合はメンテナンスウィンドウ以外の時間帯でメンテナンスが実施される可能性があります。
- 緊急を要するメンテナンスについては、可能な限り早くカスタマーポータル上でアナウンスします。

（3） お客さま Azure 環境に対するメンテナンス

- サービスで提供する Playbook 機能のバージョンアップとして、1 年に 1 回のメンテナンスウィンドウを設けます。
- メンテナンス作業におけるお客さま影響は有りません。サービスに影響が出る事無く実施されます。また、Playbook 機能のバージョンアップについては年 1 回必ず実施されるわけではありません。
- サービス影響は発生しませんが、メンテナンスを実施する場合には、メンテナンス実施の 1 週間前までにカスタマーポータル上でアナウンスします。

- Playbook 以外のお客さま Azure テナントのメンテナンスについては、NTT ドコモビジネスでは実施しません。Microsoft 社によるメンテナンスが実施される可能性はありますが、NTT コ NTT ドコモビジネスからメンテナンス通知を行うことはありません。

6.8. 故障通知

- 本サービスでは、本サービスで提供する Playbook 機能の正常性確認のための監視ロジックから異常を検知した場合や、作業依頼などの対応中に故障が疑われる挙動を検知した場合に、故障の通知を、カスタマーポータルに掲載します。
- また ServiceNow（カスタマーポータル）の故障情報を把握した場合には、カスタマーポータルの故障の通知をサポートサイトに掲載します。

6.9. サポートサイト

- 本サービス情報サイトとして、NTT ドコモビジネス サポートサイトを公開しています。
https://support.ntt.com/wideangle-soar

7. 重要事項・留意事項

7.1. 重要説明事項

7.1.1. ライセンスについて

- 本サービスのカスタマーポータルは、ServiceNow 社のサービスを利用していますが、ServiceNow 社とお客さまとの間に契約関係は生じません。

7.1.2. 品質について

- 本サービスは、SLA（Service Level Agreement）を規定しません。

7.1.3. アクセス回線について

- Microsoft Sentinel までの通信回線、および本サービスで提供されるカスタマーポータルへの通信回線については、お客さまにてご準備ください。回線にかかる費用（ISP 料金を含みます）は、本サービスとは別に発生し、ご利用になった通信会社から利用料金が請求されます。

7.1.4. 最低利用期間

- 最低利用期間は 1 カ月とします。
- 最低利用期間内に本サービスにかかる契約の解約があった場合は、当該解約があった日から最低利用期間末日までの期間に相当する本サービス利用料金を一括してお支払いいただきます。
- オプションについては、最低利用期間はありません。

7.1.5. 料金

- 本サービスの料金は利用規約 別紙 料金表に記載します。
- 初期費用は利用開始月に一括料金の請求とし、変更費用は変更月に一括料金の請求とします。
- 月額料金は、契約開始日もしくは契約変更日が毎月 2 日以降となる場合、契約開始日もしくは契約変更日を含む月の料金は日割り計算します。また、契約解除日が毎月末日前日以前となる場合、契約解除日を含む月の料金は日割り計算します。
- サービスの数量の変更があった場合、当該月の月額料を日割りします。
- 契約の解除およびサービスの廃止があった月の月額料は、契約解除および廃止した時点の数量をもとに当該月の利用料を計算します。

- お客さま都合により本サービス開通日までにご利用のご案内をお受取になれなかった場合は、本サービスの料金の返還はいたしません。
- 初期設定作業または工事の着手後完了前に契約の解約があった場合は、契約者はその作業に関して解約などがあったときまでに着手した作業の部分についてそれに要した費用の支払を要します。
- Microsoft Azure（この中には Sentinel や Logic Apps を含みます）の利用に対する課金は、本サービスの料金には含まれません。別途お客さまにてお支払いいただく必要があります。

7.1.6. 提供中止

- NTT ドコモビジネスは、災害・広域停電・インターネット障害・パンデミックなどの事態が発生し、本サービスを提供することが困難な場合は本サービスの一部または全部の提供を中止することがあります。
- ServiceNow、Azure Lighthouse、Microsoft Sentinel またはお客さま Azure テナント、ログ中継サーバーが故障した場合、NTT ドコモビジネスは本サービスの一部または全部の提供ができない場合があります。

7.1.7. 契約の成立

- 契約の成立は、お客さまからお申し込みを頂いた日をもって成立するものとさせていただきます。ただし、そのお申し込みに不備がある場合など、お承りできない事があります。また、お承りのご連絡は、ご利用開始時に通知する『ご案内』をもって代えさせていただきます。

7.1.8. 契約の解除

- お客さまが本サービスの利用規約に記載のお客さまの義務の規定に違反したとき、NTT ドコモビジネスは契約を解除することがあります。

7.1.9. 免責

- NTT ドコモビジネスは本サービスを現状有姿で提供するものであり、契約者は、NTT ドコモビジネスが本サービスについて正確性、実現性、有用性、有効性を保証するものではないことを了承し、契約者の責において本サービスを利用するものとします。
- NTT ドコモビジネスは、本規約の変更などにより契約者が本サービスを利用するにあたり NTT ドコモビジネスが提供することとなっている設備、端末など以外の設備、端末などの改造または変更（以下、この条において「改造など」といいます）を要する場合であっても、その改造などに要する費用については負担しません。

- NTT ドコモビジネスは、本サービスが日本国外の地域の規制（法令、規則、政府ガイドラインなどを含みますがこれに限りません）に適合していること、および日本国外の地域で利用可能であることについて何ら保証を行わず、契約者もしくは契約者のエンドユーザーによる日本国外の地域での本サービスの利用または契約者もしくは契約者のエンドユーザーの保存データおよび生成などデータの日本国外から日本国内への移転によって発生したいかなる損害についても NTT ドコモビジネスは責任を負いません。
- Microsoft Sentinel、Microsoft Azure および、NTT ドコモビジネスが提示する、アラート通知、自動対処、レポート、調査報告、各種設定などは、お客さまの IT 環境を熟知したものではなく、お客さま IT 環境での動作を完全に保証するものではありません。お客さまの判断により実施決定いただいた設定変更に伴い発生した如何なる事象においても、NTT ドコモビジネスは責任を負いません。
- NTT ドコモビジネスは、本サービスがすべてのセキュリティ上の脅威や攻撃を検知、乃至は対処することについて何ら保証を行わず、これらに関連して契約者に損害が発生したとしても責任を負いません。
- Azure Lighthouse または Microsoft Sentinel が動作しないこと（Microsoft に起因する Azure Lighthouse または Microsoft Sentinel の不具合、使用不可を含みますがこれに限りません）に起因して本サービスが提供できない場合、NTT ドコモビジネスは責任を負いません。
- お客さまご自身で、Microsoft Sentinel をはじめとした Azure の設定を変更することにより、本サービスが正常に提供できなくなる可能性があります。ご了承ください。（データコネクタの設定を変更する、ログ保存期間を変更する、Logic Apps の設定を変更するなどを含みますがこれに限りません）
- 上記の場合、設定などの切り戻しはお客さま責任で実施いただく必要があります。また NTT ドコモビジネス側での再工事が必要となった場合には、別途工事費が発生いたします。

7.1.10. サービスの廃止

- 本サービスは、お客さまからの廃止申込により本契約は終了し廃止されます。

7.2. 留意事項

7.2.1. ご利用について

- 提供する各種推奨事項の実行はお客さまの判断・責任において行われるものとします。
- ダッシュボードの情報はその状況に関して保証や意見表明などを行うものではありません。

- 本業務の中で発生した著作物に関する著作権は NTT ドコモビジネスに帰属します。お客さまの内部使用に限って利用は可能ですが、関連会社以外の第三者に配布・公開はできません。

7.2.2. サービス全般の注意事項について

- ご利用開始時および変更時に通知する『ご案内』は、送信元が<wa-sac-customer@ntt.com>からメール通知が届きますので、このドメインからのメールが受信できるようにしてください。また、送付物をダウンロードする際のパスワードは、お申し込み時にお客さまに記載いただいたものを使用し NTT ドコモビジネスから通知は致しません。
- カスタマーポータルの通知は、送信元が<nttcomsac@service-now.com>のメールアドレスから、通知が送られます。本メールが受信できるように設定される必要があります。
- 違約金発生期間は、当該契約のご利用開始日から起算します。
- 違約金は、当該契約の解約があった時点の月額料金を元に違約金発生期間末日までの未払い期間で計算します。
- 同業者様からのお申し込みはお断りすることがあります。予めご了承ください。
- NTT ドコモビジネス セキュリティアドバイザリーセンター被災により運用業務の継続に支障をきたす場合でも、お客さまの業務が停止するなどのリスクは最小限のため、DR/BCP 対策をとらない運用体制となっています。
- Microsoft Azure（お客さまテナント）、Microsoft 365 E5 Security、Microsoft 365 Business Premium、Microsoft 365 E3、セキュリティ製品など、ログ中継サーバー、端末、パソコン、サーバー、OS、アプリケーション自体の仕様に関する問い合わせ、および設定などについては、お受けできません。
- （アカウントの権限について）工事や保守作業のため、お客さまテナントのアカウントを貸与いただく必要があります。
- サービスの提供終了時にはアカウント返却のご連絡をしますので、確実にアクセスできないように対応をお願いします。
- 故障などで再構築が必要な場合には権限を再付与いただく必要があります。
- Threat Detection を利用する場合には、お客さまのセキュリティデバイス・ログ中継サーバーの設定が適切に設定されている必要があります。適切に設定されていない場合は、Threat Detection の機能が正常に動作しない場合があります。
- Threat Detection を利用する場合には、アラートの重複を防ぐため NTT ドコモビジネスにて分析ロジック（Microsoft Threat Intelligence Analytics）を ON にするため、同じイベントログを持つ脅威インテリジェンスインジケーターやカスタム アラートルールをオフにすることをお勧めします。

- 分析ロジック（Microsoft Threat Intelligence Analytics）での検知は Microsoft Sentinel の動作仕様上、数時間程度を要します。また、Microsoft Sentinel へのログ転送量によっては、ログ検索などの処理に時間がかかり、通知にさらに時間を要する場合があります。
- カスタマーポータルは、MFA（多要素認証）の有無をお客さまにて選択できますが、以下の点を考慮して選択してください。
  MFA（多要素認証）を利用いただくことにより、アカウントのセキュリティを強化し、第三者による不正侵入からの防御をより高めることができます。
  MFA（多要素認証）を利用いただかない場合、アカウントのセキュリティを脆弱にするおそれがあるため、MFA（多要素認証）を利用されることを強く推奨します。
- Microsoft Defender XDR 統合を解除すると分析ルールが再アクティブ化されず Playbook が正常に動作しないため、Microsoft Defender XDR 統合を解除した場合は作業依頼をお申し込みください。
- 自動対処時、終報通知が遅れるリスクを避けるために端末を 5 台またはアカウントを 5 つまで自動対処を実行します。端末を 6 台またはアカウントを 6 つ以上存在する場合は自動対処を一切実施せず、メール通知にて初報で最初の端末を 5 台またはアカウントを 5 つまで、終報で全端末・アカウント名を通知いたします。
  （対象デバイス：Microsoft Defender for Endpoint、Microsoft Defender for Business、Microsoft Entra ID P1、Microsoft Entra ID P2、Microsoft Defender for Identity、Microsoft Defender for Cloud Apps、Microsoft Defender for Endpoint 連携を行うデバイス）
- 自動対処を実施する対象を増やす（例：Low のアラートが発生した場合にも自動対処を行う）設定変更を行う場合、特に Microsoft Defender for Endpoint の場合に、自動対処（フルスキャンなど）の頻度が多くなることから、クライアント側のパフォーマンスが落ちる場合があります。
- アラート通知メール文章内のアラートの和訳および解説文については、生成 AI によって作成されたものであり、情報の正確性や完全性について保障するものではありません。当社はこちらの内容について一切の責任を負いません。また、内容に関するお問い合わせは受け付けておりませんので、ご了承ください。
- アラート通知メールを作成する際、以下の情報を生成 AI 基盤(Azure OpenAI)に送信いたします。
  - インシデント ID
  - インシデントタイトル
  - インシデント Severity
  - 端末隔離・ウイルススキャン・AIR の処理結果
  - 処理開始時刻
  - マネージド SOAR の動作設定値

- アラート名
- アラートディスクリプション
- アラート ID
- 検知サービス名（MSOAR としての）
- エンティティ情報(ホスト情報、アカウント情報、ファイルハッシュ、ファイル名など)※

  ※Microsoft Sentinel のエンティティ情報の詳細については以下の Microsoft 公式ドキュメントを参照してください。

  https://learn.microsoft.com/ja-jp/azure/sentinel/entities

- 本サービスで利用する 生成 AI 基盤(Azure OpenAI) に送信されたデータは、Microsoft 社のデータプライバシーポリシーに従って、以下のように取り扱われます。
  - 生成 AI に入力されたデータは、本サービスのアラート通知メールの作成にのみ利用されます。
  - 生成 AI に入力されたデータは、OpenAI の学習やモデル改善には利用されません。
  - 生成 AI に入力されたデータは、本サービスの提供のみを目的として構築・運用している NTT ドコモビジネスの Azure テナント内でのみ取り扱われ、当該テナント以外の OpenAI ユーザーには利用されません。
  - 生成 AI に入力されたデータは、 Microsoft 社や第三者の製品改善には利用されません。

  その他、データ取り扱いに関する詳細は、以下の Azure OpenAI の公式ドキュメントを参照してください。

  https://learn.microsoft.com/ja-jp/azure/ai-foundry/responsible-ai/openai/data-privacy?view=foundry-classic&tabs=azure-portal

  なお、Microsoft 社における仕様変更その他の要因により、データの取り扱い方法が変更となる場合があります。これに起因して生じたいかなる損害についても、弊社は責任を負いません。

- 弊社へ申告なく以下のデバイスの切り替えを行った場合、Playbook が動作しません。

  以下のデバイスの切り替えを行う場合は、NTT ドコモビジネスの作業が発生するため、お問い合わせください。
  - Microsoft Defender for Endpoint ⇔ Microsoft Defender for Business
  - Microsoft Entra ID P2 ⇔ Microsoft Entra ID P1

改訂履歴

バージョン	主な変更	日付
1.00	初版発行	2023 年 3 月 31 日
1.01	・「Microsoft Defender for Identity」→「Microsoft Defender for Identity / Fusion」	2023 年 7 月 12 日
1.02	・MDI に関する提供条件の記載漏れ対応 ・カスタマーポータル故障時の問い合わせ受付修正	2023 年 11 月 22 日
1.03	・「Playbook 用アカウントに MFA をかけることができない」旨を明記 ・「NTT Com 指定休業日」の明示化	2024 年 1 月 17 日
1.04	・名称変更「Azure AD」→「Microsoft Entra ID」 ・開通案内の送信元メールアドレス修正 ・関連文書などのドキュメント名を実際のドキュメント名に変更	2024 年 5 月 22 日
2.00	・メニュー追加（Threat Detection）に伴う修正	2024 年 9 月 3 日
2.01	・ドキュメント名の変更	2024 年 9 月 18 日
2.02	・バックアップ対象から「AADNonInteractiveUserSignInLogs」「Non-Interactive User Sign-In Logs（Preview）」を削除。 ・作業依頼「アラートレポート作成」を廃止に伴い、削除。	2024 年 11 月 29 日
2.03	・Logic Apps の実行結果の保存期間の明記削除 ・Microsoft Entra ID Protection から収集するログの種類に「Security Alert」の記載漏れ ・「同時に問合せできる件数は 1 件」という制約から故障問合せを除外 ・プロフェッショナルサービス、PS の表記を削除 ・お客さまガイド新規作成に伴う修正 ・変更申込のオプション追加/変更/削除のみの標準開通日を追記 ・メンテナンスに関して、実運用に則していなかったため修正	2025 年 3 月 19 日
3.00	・Severity 設定の柔軟化に伴う修正 ・Entra ID/MDO/MDCA からの MDE 自動対処実行機能に伴う修正	2025 年 5 月 14 日
3.01	・生成 AI アラート解説についての免責記載を追加	2025 年 6 月 11 日
3.02	・ライセンス追記「M365 Business Premium」、「M365 E3」 2.1. サービス概要 3.1. 提供区分 7.2.2. サービス全般の注意事項について ・対象デバイス追加「Microsoft Defender for Business」、「Microsoft Entra ID P1」 3.3.2. サポートデバイス毎の構成条件・設定条件 3.4.1. 基本サービス機能一覧 3.5.2. ログ収集	2025 年 8 月 27 日

	3.5.3. 自動ログ分析 3.5.4. 自動通知/自動対処 4.1.1. 各種工事 4.1.2. 工事に関する留意事項 6.1.5. 開通試験 7.2.2. サービス全般の注意事項について ・マネージド ID 化に伴う修正 （Playbook 用アカウントは不要、Client Secret 更新は不要） 3.3.1. Microsoft Sentinel について 4.1.2. 工事に関する留意事項 6.7. 工事通知（メンテナンス通知） 7.1.9. 免責 ・メンテナンスのアナウンスに関して実運用に則して修正（2.03 版の修正漏れの反映） 6.7. 工事通知（メンテナンス通知）	
4.00	Day4 リリースに伴う対応 ・Microsoft Defender XDR 対応 ・アラートメールの報告形式の改善 ・AIR 再実行方式の改善 ・インシデントへの AIR 結果タグ付与 ・MDE デバイスタグによるホスト単位の自動対処制御 ・作業依頼申し込み内容の追加・変更 ・ポータル機能拡充 1.2. 関連文書 3.1. 提供区分 3.3.1. 基本サービス機能一覧 3.3.2. 作業依頼機能一覧 3.4.1. カスタマーポータル 3.4.2. ログ収集 3.4.3. 自動ログ分析 3.5.3. 各種設定変更 3.6.1. Microsoft Sentinel について 3.6.2. サポートデバイス毎の構成条件・設定条件 3.6.3. Threat Detection ご利用時の固有の提供条件 4.1.1. 各種工事 6.1.4. 対処除外設定リスト 6.1.5. 開通試験 6.6. お問い合わせ受付・運用受付/通知方法 7.2.1. ご利用について 7.2.2. サービス全般の注意事項について	2025 年 11 月 19 日

4.01	・社名変更に伴う修正 ヘッダー フッター 表紙 1.3. 用語の定義 2.1. サービス概要 3.1. 提供区分 3.3.1. 基本サービス機能一覧 3.4.1. カスタマーポータル 3.4.3. 自動ログ分析 3.4.4. 自動通知/自動対処 3.5.2. 対処除外設定 3.6.1. Microsoft Sentinel について 3.6.2. サポートデバイス毎の構成条件・設定条件 3.6.3. Threat Detection ご利用時の固有の提供条件 3.6.4. ポイント 3.8. 提供地域 4.1.2. 工事に関する留意事項 4.2. 故障対応 6.1.5. 開通試験 6.2. 標準開通日 6.3. 開通案内・配布同梱物 6.7. 工事通知（メンテナンス通知） 6.9. サポートサイト 7.1.6. 提供中止 7.1.8. 契約の解除 7.1.9. 免責 7.2.1. ご利用について 7.2.2. サービス全般の注意事項について ・生成 AI アラート解説についての免責記載を追加	2025 年 12 月 1 日
4.02	・Microsoft Entra ID P1 に関する制限事項の削除 3.4.3. 自動ログ分析 ・<ブロックリスト利用(接続元 IP アドレスの登録/修正)／利用中止(接続元 IP アドレスの全削除)> の構成図の最新化 3.5.3. 各種設定変更 ・軽微文言修正	2026 年 1 月 22 日
4.03	・Microsoft Defender for Endpoint 連携に関する留意事項の追記 3.6.2. サポートデバイス毎の構成条件・設定条件 ・対処除外設定リストにおけるリスト種別と作業依頼の対応関係の明記 8.1.4. 対処除外設定リスト ・自動対処除外アラートに関するサービス仕様見直しに伴う修正 3.5.3. 各種設定変更 ・軽微文言修正	2026 年 4 月 27 日

4.04	・自動通知/自動対処の対象条件に関する注意事項を追記 3.4.4. 自動通知/自動対処 ・作業依頼ポイント未契約時の留意事項について追記 3.6.4. ポイント	2026 年 5 月 20 日
4.05	・WideAngle AI Advisor 連携に関する作業依頼項目及び関連仕様を追記 3.3.2. 作業依頼機能一覧 3.5.3. 各種設定変更 ・軽微文言修正	2026 年 6 月 8 日