

WideAngle マネージド CSPM サービス仕様書

バージョン 3.00

2026年06月22日

NTTドコモビジネス株式会社

マネージド&セキュリティサービス部 セキュリティサービス部門

目次

1. はじめに	3
1.1. 本書の目的.....	3
1.2. 関連文書.....	3
1.3. 用語の定義.....	4
2. サービス概要	5
2.1. CSPM/CWPP/CIEM とは.....	5
2.2. サービス概要.....	5
3. サービス仕様	7
3.1. 提供区分.....	7
3.2. 提供メニュー.....	7
3.3. 提供条件.....	9
3.4. 提供機能一覧.....	16
3.5. 提供機能（基本機能）.....	19
3.6. 提供機能（作業依頼機能）.....	37
3.7. サービスレベル.....	50
3.8. 提供地域.....	50
4. 料金	51
4.1. サービスの価格.....	51
5. お申し込み・ご利用	52
5.1. お申し込み.....	52
5.2. 標準開通日.....	53
5.3. 開通案内・配布同梱物.....	54
5.4. お問い合わせ受付.....	54
5.5. 故障受付.....	56
5.6. お問い合わせ受付・運用受付/通知方法.....	56
5.7. 工事通知（メンテナンス通知）.....	58
5.8. 故障通知.....	59
6. お問い合わせ連絡先	62
7. 重要事項・留意事項	63
7.1. 重要説明事項.....	63
7.2. 留意事項.....	66
改訂履歴	70

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 CSPM 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。機能名や画面、メール文面は、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 CSPM サービス仕様書
B02_【マネージド CSPM】標準提案書
WideAngle マネージド CSPM 利用規約
WideAngle_22_CSPM_新設_L
WideAngle_23_CSPM_変更_L
WideAngle_24_CSPM_変更(更新時)_L
WideAngle_25_CSPM_廃止_L
WideAngle_26_CSPM_簡易変更_L
WideAngle マネージド CSPM カスタマーポータルご利用ガイド
WideAngle マネージド CSPM Prisma Cloud_AWS 連携ガイド(Business Edition)
WideAngle マネージド CSPM Prisma Cloud_AWS 連携ガイド(Enterprise Edition)
WideAngle マネージド CSPM Prisma Cloud_Azure 連携ガイド(Business Edition)
WideAngle マネージド CSPM Prisma Cloud_Azure 連携ガイド(Enterprise Edition)
WideAngle マネージド CSPM Prisma Cloud_Google Cloud 連携ガイド(Business Edition)
WideAngle マネージド CSPM Prisma Cloud_Google Cloud 連携ガイド(Enterprise Edition)
WideAngle マネージド CSPM Cortex Cloud_AWS 連携ガイド
WideAngle マネージド CSPM Cortex Cloud_Azure 連携ガイド
WideAngle マネージド CSPM Cortex Cloud_Google Cloud 連携ガイド
WideAngle マネージド CSPM Prisma Cloud ご利用ガイド
WideAngle マネージド CSPM Cortex Cloud ご利用ガイド
WideAngle マネージド CSPM Prisma Cloud クラウドアカウント削除ガイド
WideAngle マネージド CSPM クラウドアカウント情報記入シート
WideAngle マネージド CSPM Prisma Cloud Defender インストールガイド : App-embedded(Fargate)
WideAngle マネージド CSPM Prisma Cloud Defender インストールガイド : AWS Lambda(Auto-Defend)
WideAngle マネージド CSPM Prisma Cloud Defender インストールガイド : Docker
WideAngle マネージド CSPM Prisma Cloud Defender インストールガイド : Kubernetes
WideAngle マネージド CSPM Cortex Cloud_XDR エージェントインストールガイド
WideAngle マネージド CSPM Prisma Cloud レジストリスキャンガイド : Amazon ECR
WideAngle マネージド CSPM Prisma Cloud レジストリスキャンガイド : Azure Container Registry

WideAngle マネージド CSPM_Prisma Cloud_レジストリスキャンガイド : Docker Hub
WideAngle マネージド CSPM_Prisma Cloud_レジストリスキャンガイド : Google Container Registry
WideAngle マネージド CSPM_Cortex Cloud_レジストリスキャンガイド

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
CSPM	Cloud Security Posture Management の略称。お客様の IaaS がセキュアな状態であるかを可視化し、管理するツール
CWPP	Cloud Workload Protection Platform の略称。クラウド ワークロード（クラウド上の仮想マシン、データベース、コンテナ、アプリケーション等）に対して監視と保護を行うツール
CIEM	Cloud Infrastructure Entitlement Management の略称。クラウド環境内のアクセス権や権限を可視化し、管理するセキュリティプロセス
Prisma Cloud	Palo Alto Networks 社による、複数のクラウド環境から API 経由で設定情報やイベントログ/トラフィック情報などを継続的に収集し、それらを統合/分析した上でリアルタイムに可視化するツール
Cortex Cloud	Palo Alto Networks 社による、マルチクラウドに対応したクラウドセキュリティ（CNAPP）、検知・対応（CDR/SOC）、AI・自動化を一体化した統合型クラウドセキュリティプラットフォーム
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。
IAM セキュリティ	Identity and Access Management の略称。お客様クラウドの ID を可視化し、管理するツール

2. サービス概要

2.1. CSPM/CWPP/CIEM とは

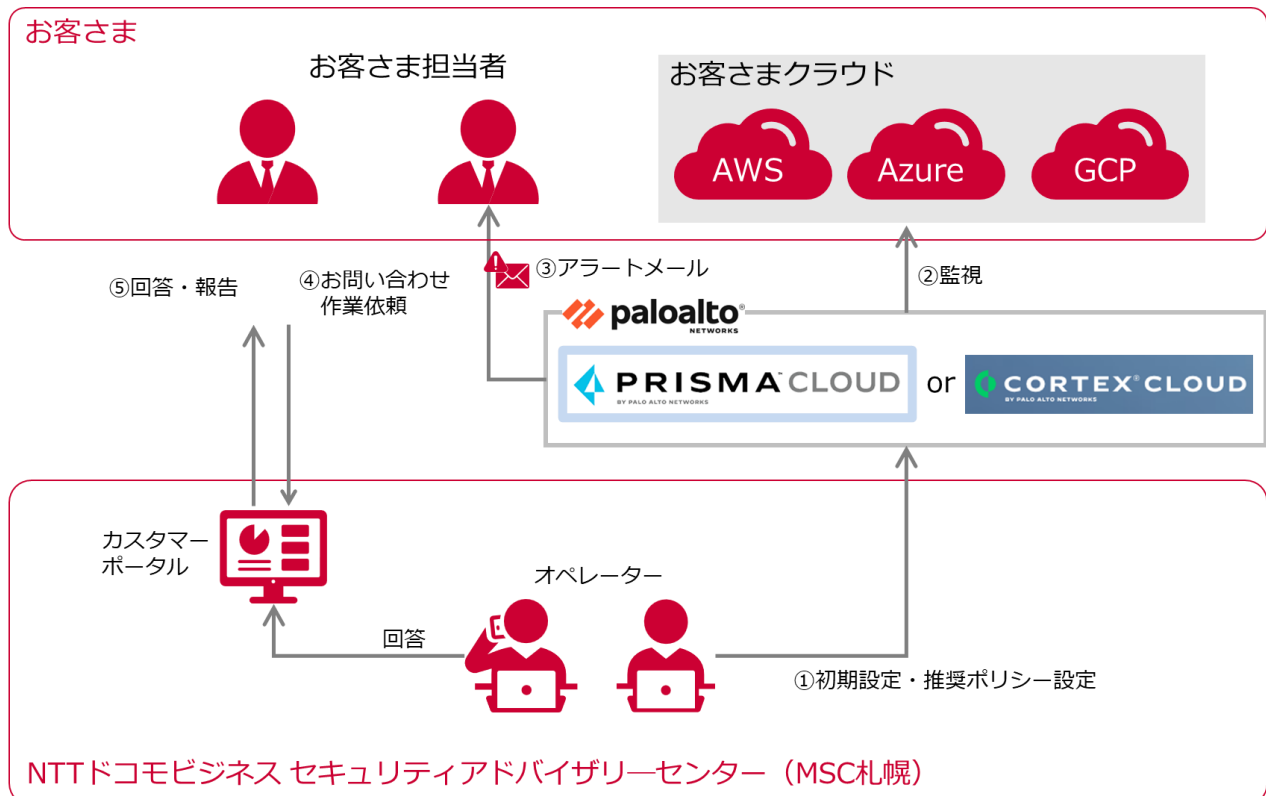
- CSPM（Cloud Security Posture Management）は、お客様の IaaS がセキュアな状態であるかを可視化し、管理するツールです。
- IaaS の設定ミスや、コンプライアンスの準拠状況を可視化し、お客様のクラウド環境のセキュリティ強化を支援します。
- CWPP（Cloud Workload Protection Platform）は、クラウド ワークロード（クラウド上の仮想マシン、データベース、コンテナ、アプリケーション等）に対して監視と保護をするツールです。
- お客様の IaaS に Defender を導入いただくことで、脆弱性やマルウェアの検知、ランタイム保護の機能が利用でき、セキュリティ強化を実施します。
- CIEM（Cloud Infrastructure Entitlement Management）は、お客様の IaaS（AWS、Azure、GCP）の権限の状況を可視化し、管理するツールです。IAM セキュリティとも呼ばれます。
- 管理権限をもつ人が必要以上に多数存在しないか、長期間利用されていないユーザーがないか、権限が過剰に割り当てられていないかなどを確認し是正することで、ゼロトラストの最小権限を実現し、権限侵害による事故を未然に防ぎます。

<p>CSPMの主な監視機能</p> <ol style="list-style-type: none"> 1 クラウドの設定ミス 2 不正通信の管理（アノマリ） 3 コンプライアンス準拠 4 クラウドリソースの可視化 	<p>CSPM管理画面</p>	<p>CIEMの主な監視機能</p> <ol style="list-style-type: none"> 1 権限付与状況の可視化 2 権限ポリシー脱却検知 3 過剰な権限のはく奪
<p>CWPPの主な監視機能</p> <ol style="list-style-type: none"> 1 ランタイム保護 2 脆弱性検査と保護 3 マルウェア対策 	<p>CWPP管理画面</p>	<p>CIEM管理画面</p>

2.2. サービス概要

- Palo Alto Networks 社の Prisma Cloud/Cortex Cloud を用いてお客様のクラウド環境の監視・運用を提供するサービスです。
- 本サービスにて Prisma Cloud/Cortex Cloud をご利用いただくと初期設定や製品問い合わせの日本語代行なども提供します。

- お客様担当者は、カスタマーポータルから各種問い合わせ、CSPM・CWPP・CIEM 機能に関する各種作業依頼、月次レポート取得等を行います。
- 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、CSPM・CWPP・CIEM 機能に関する各種作業依頼回答、月次レポート提供を行います。
- Prisma Cloud/Cortex Cloud のアラートは、お客様担当者へ直接通知されます。



3. サービス仕様

3.1. 提供区分

Prisma Cloud/Cortex Cloud を提供し、お客さまにて Prisma Cloud/Cortex Cloud へのログインができます。Prisma Cloud/Cortex Cloud とお客さま IaaS との連携はお客さまにて実施いただきます。

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等を受け付けます。

お客さまのクラウド環境と Prisma Cloud/Cortex Cloud までの通信回線、およびカスタマーポータルへの通信回線については、お客さまにてご用意いただきます。

3.2. 提供メニュー

マネージド CSPM には次の種類があります。

種類	概要説明
基本メニュー	Palo Alto Networks 社の Prisma Cloud/Cortex Cloud を提供し、本来英語で実施すべき問い合わせを日本語で対応する機能を含むもの、およびご契約のメニューによって CSPM 機能または CSPM 機能 + CWPP + CIEM 機能に関する運用代行を提供するもの
オプションメニュー	各種付帯サービスを提供するもの

マネージド CSPM の提供メニューは以下の通りです。

種類	メニュー名	概要説明
基本メニュー	基本プラン	<ul style="list-style-type: none"> Prisma Cloud Business Edition (CSPM 機能) CSPM 機能の初期設定 CSPM 機能の製品日本語問い合わせ対応、製品故障問い合わせ対応 CSPM 機能に関する運用代行 (作業依頼) (5 ポイント/月まで)、月次レポート提供 カスタマーポータル
	CWPP 込みプラン	<ul style="list-style-type: none"> Prisma Cloud Enterprise Edition (CSPM 機能 + CWPP 機能 + CIEM 機能)

		<ul style="list-style-type: none"> ・ CSPM 機能 + CWPP 機能 + CIEM 機能の初期設定 ・ CSPM 機能 + CWPP 機能 + CIEM 機能の製品日本語問い合わせ対応、製品故障問い合わせ対応 ・ CSPM 機能 + CWPP 機能 + CIEM 機能に関する運用代行（作業依頼）（5 ポイント/月まで）、月次レポート提供 ・ カスタマーポータル
	Cortex Cloud(Posture Security)	<ul style="list-style-type: none"> ・ Cortex Cloud Posture Security (CSPM 機能 + CIEM 機能) ・ CSPM 機能 + CIEM 機能の初期設定・定期的なポリシー等の見直し提供 ・ CSPM 機能 + CIEM 機能の製品日本語問い合わせ対応、製品故障問い合わせ対応 ・ CSPM 機能 + CIEM 機能に関する運用代行（作業依頼）（5 ポイント/月まで）、月次レポート提供 ・ カスタマーポータル
	Cortex Cloud(Runtime Security)	<ul style="list-style-type: none"> ・ Cortex Cloud Runtime Security (CSPM 機能 + CWPP 機能 + CIEM 機能) ・ CSPM 機能 + CWPP 機能 + CIEM 機能の初期設定・定期的なポリシー等の見直し提供 ・ CSPM 機能 + CWPP 機能 + CIEM 機能の製品日本語問い合わせ対応、製品故障問い合わせ対応 ・ CSPM 機能 + CWPP 機能 + CIEM 機能に関する運用代行（作業依頼）（5 ポイント/月まで）、月次レポート提供 ・ カスタマーポータル
オプションメニュー	作業依頼ポイント追加	<ul style="list-style-type: none"> ・ 作業依頼に利用いただけるポイントを追加します。（5 ポイント単位/月）

3.3. 提供条件

3.3.1. 契約期間

- 定期契約期間があります。
- 定期契約期間は、サービスの提供を開始した日を起算日（以下「定期契約期間起算日」）とし、定期契約期間起算日から1年とします。翌年の定期契約期間起算日の前日を「定期契約期間満了日」といいます。
- 定期契約期間は、規定する日（翌年の定期契約期間起算日の20営業日前）までに契約解約またはクレジット/ワークロードの数量の減少の申出がない場合、同一条件で1定期契約期間延長することとし、以後これに準じて取り扱います。定期契約期間満了日に合わせて当社から契約者へ更新の依頼や更新の通知はいたしません。
- Prisma Cloud にて、定期契約期間中にクレジットを追加する際は個別調整が必要となるため事前に連絡をお願いします。
- Cortex Cloud にて、定期契約期間中にワークロードを追加する場合、その追加する契約の契約期間満了日は定期契約期間起算日に定めた定期契約期間満了日と同じとします。
- 定期契約期間内に契約を解約される場合は、解約があった日から定期契約期間満了日までの期間に相当する本サービスの利用料金を一括してお支払いいただきます。
- 契約の解約またはクレジット数/ワークロード数の減少変更を希望される場合は、解約またはクレジット数/ワークロード数の減少変更しようとする定期契約期間満了日の指定する日（翌年の定期契約期間起算日の20営業日前）の前までに契約の解約またはクレジット数/ワークロード数の減少変更についてお申し込みいただきます。
 なお、定期契約期間中は、クレジット/ワークロードの数の減少はできません。クレジット/ワークロードの数の減少は、次の定期契約期間起算日から適用とします。
- 支払い方法は、原則月額払いとなります。初月および解約月は当該月の日数で日割して計算します。

項目	条件
契約期間	<ul style="list-style-type: none"> • 利用開始日を起点に1年間（1年単位の契約） • 複数年契約はできません。
契約期間の延長	<ul style="list-style-type: none"> • 廃止申込がない限り、利用開始日を起点に1年毎に契約を自動延伸
Prisma Cloud にて、契約期間中のクレジット数やオプション追加	<ul style="list-style-type: none"> • クレジット数追加は個別調整が必要となるため事前に連絡をお願いします。 • オプション追加は可能です。契約終了日は現契約の終了日が適用されます。

Cortex Cloud にて、契約期間中のワークロード数やオプション追加	・可能です。契約終了日は現契約の終了日が適用されます。
契約期間中のオプション解除、減数	・可能です。
契約期間中のクレジット数/ワークロード数削減	・不可のため一切受け付けられません。
契約期間中の廃止	・可能ですが、契約期間の残余期間分の違約金がかかります。
契約期間途中でのメニュー変更	・メニュー変更はできません。廃止/新設となります。

3.3.2. 最低利用期間

- 最低利用期間は、定期契約期間とします。
オプションについては最低利用期間はありません。
- 最低利用期間内に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。

3.3.3. 利用クレジット/ワークロード課金

- Prisma Cloud/Cortex Cloud による監視対象数（クレジット/ワークロード）に応じて、利用クレジット/ワークロード課金料が発生します。
 - Prisma Cloud のクレジット数の追加購入は、個別調整が必要となるため事前に連絡をお願いします。
 - Cortex Cloud の購入の最低数量は、200 ワークロードとなります。
 - Prisma Cloud/Cortex Cloud の購入の最小単位は、100 クレジット/ワークロード単位となります。
 - クレジット/ワークロードのカウントは、お客さまがご利用になっているリソースに応じてカウントされます。また、カウント方法はご契約いただいた提供メニューによって異なります。カウント方法は Palo Alto Networks 社により、予告なく変更される場合があります。
- 基本プランは、下表のとおり、VM 数だけでなく、DB や LB などにも課金されることに注意が必要です。

- 利用クレジット数/ワークロード数¹は、クレジット/ワークロードの利用状況を 1 時間ごとに測定し、日次、週次、月次で集計しています。
 クレジット/ワークロードの消費については、実行中のリソースのみが使用量にカウントされますので、その時点でリソースが実行中でなければカウントされません。
- ご契約いただくクレジット数/ワークロード数と実際の利用クレジット数/ワークロード数が異なる場合には、クレジット数/ワークロード数の追加をお申し込みいただきます。
 90 日間の平均利用クレジット数/ワークロード数が契約クレジット数/ワークロード数をオーバーすると、営業担当よりお客さまへ追加依頼のご連絡を行います。

① Prisma Cloud

■モジュールごとのライセンスユニットおよびクレジットカウント（基本プラン）

種別	Prisma Cloud モジュール	キャパシティユニット	クレジット カウント数
CSPM	可視性 コンプライアンス ガバナンス	以下のインスタンスごと ■AWS EC2、RDS、Redshift、DynamoDB、 ALB & ELB (load balancers)、 NAT gateways ■Azure Virtual machines、SQL databases、 Load balancer、Application Gateway、 Gateway ■Google Cloud GCE、Cloud SQL、Cloud Spanner、LB、 Cloud NAT	1

■モジュールごとのライセンスユニットおよびクレジットカウント（CWPP 込みプラン）

種別	Prisma Cloud モジュール	キャパシティユニット	クレジット カウント数
CSPM	可視性 コンプライアンス ガバナンス	VM ごと	1
CIEM	IAM セキュリティ	VM ごと	0.25

¹ 小数点以下のクレジット/ワークロードは切り捨てでカウントされます。

CWPP	ホストセキュリティ	デプロイされたホスト Defender ごと	0.5
	コンテナセキュリティ	デプロイされたホスト Defender ごと	5
	サーバーレスセキュリティ	保護する Function が 6 個ごと	1

② Cortex Cloud

■アセットカテゴリーごとの 1 ワークロードあたりの課金単位

アセットカテゴリー	1 ワークロードあたりの課金単位	備考
VM	1 個の VM (停止中も含む)	
CaaS	10 個のマネージドコンテナ	
サーバーレス関数	25 個のサーバーレス関数	
レジストリ内のコンテナイメージ	無料割り当て：デプロイされたワークロード (VM/CaaS) ごとに 10 個のコンテナイメージ数をスキャン 無料枠を超えた場合：追加スキャン 10 個	※レジストリースキャンをオンにした場合にのみ
クラウドバケット	10 個のクラウドバケット	
マネージドクラウドデータベース (PaaS)	2 個の PaaS データベース	
DBaaS	1TB の保存容量	
SaaS ユーザー	10 人の SaaS ユーザー	
Cloud ASM - 非管理型サービス	4 つの管理対象外アセット	※ Cloud ASM をオンにした場合にのみ

3.3.4. 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、本サービスの各プラン（基本プラン /CWPP 込みプラン/ Cortex Cloud(Posture Security)/Cortex Cloud(Runtime Security)) には、毎月 5 ポイントが含まれます。
- NTT ドコモビジネス セキュリティアドバイザーセンター (SAC) 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。
- お客さまは申請時に残ポイントがないと申請できません。基本メニューに含まれるポイント数で足りない場合には、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。

- 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ーセンター（SAC）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・申請書の不備等により、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。残ポイントはポータル上で確認することができます。

カスタマーポータルイメージ

ポイント管理					
お客様番号	開始日	終了日	作業依頼契約ポイント合計	消化数	残数
N227907775	2022-12-01	2022-12-31	15	0	15

1行中 1～1行

3.3.5. 監視対象 IaaS

- Prisma Cloud/Cortex Cloud が監視可能な対象 IaaS は、AWS、Azure、GCP となります。

3.3.6. Prisma Cloud/Cortex Cloud 管理者

- Prisma Cloud/Cortex Cloud 管理者情報（ご担当者名、メールアドレス）を、お申し込み時に必ず 1 つ指定いただきます。新設開通時は、任意でプラス 2 人まで指定可能です。初期設定では、この Prisma Cloud/Cortex Cloud 管理者情報のメールアドレスがアラート通知先として設定されます。
- 開通後は、作業依頼で追加できます。

3.3.7. Prisma Cloud/Cortex Cloud のログイン/認証/権限

- Prisma Cloud/Cortex Cloud へお客さまはログインすることが可能です。
- ログイン時には 2 要素認証が強制的に適用されます。2 要素認証の解除はできません。
- ユーザー追加時には SuperUser 権限によるカスタマーサポートポータル（CSP）上でのユーザー承認が必要です。※
- Prisma Cloud では、お客さま IaaS と Prisma Cloud の連携に必要な設定変更権限を例外として Read-Only 権限のみの解放となります。権限の詳細については、「[3.6.6 ユーザー追加/削除](#)」を参

照してください。

Cortex Cloud では、System Admin 権限を開放します。

※ Palo Alto Networks Hub ポータル経由でログインする場合に限る。

3.3.8. Prisma Cloud/Cortex Cloud の利用

- 開通後のご利用開始日以降に、本サービスで提供される Prisma Cloud/Cortex Cloud とお客さま IaaS の連携をお客さまにて実施いただきます。お客さまのクラウド IaaS の管理者アカウントを Prisma Cloud/Cortex Cloud に投入することが必要です。管理者権限を要するアカウントのため、お客さま自身で登録を頂きます。
- お客さまの IaaS を監視している Prisma Cloud/Cortex Cloud に、NTT ドコモビジネス、および提携事業者のオペレーターや、エンジニアがアクセスする場合があります。
- Prisma Cloud/Cortex Cloud に対して、その稼働状況の監視は実施いたしません。

3.3.9. サービス提供範囲外

- 以下の Prisma Cloud モジュールについては、本サービスの提供範囲外となります。
 - コードセキュリティ²
 - データセキュリティ
 - Web アプリケーション & API セキュリティ (WAAS)
- 以下の Cortex Cloud モジュールについては、本サービスの提供範囲外となります。
 - Cloud Posture Security/Cloud Runtime Security
 - ◆ Cloud Attack Surface Management (Cloud ASM)
 - ◆ Artificial Intelligence Security Posture Management (AI-SPM)
 - ◆ Application Security Posture Management (ASPM)
 - ◆ CI/CD Posture Management
 - Cloud Runtime Security
 - ◆ Web Application and API Security
 - Application Security
 - ◆ Infrastructure as Code (IaC) Security
 - ◆ Software Composition Analysis (SCA)
 - ◆ Secrets Security

² Policy Subtype: [Build] のポリシーはコードセキュリティで使用されるポリシー
コードセキュリティを有効化していない状態でも表示されるが、ポリシーとしては無効状態

3.3.10. Prisma Cloud/Cortex Cloud のログ保管期間

- Prisma Cloud/Cortex Cloud 上には、契約期間中、お客さまのクラウドで発生したアラートやログが保存されています。
- 保存される日数は以下の通りです。また、Prisma Cloud の契約が満了した後 90 日で、 Palo Alto Networks 社によって、全てのデータが削除されます。Cortex Cloud の契約が満了した後の 31～180 日の間で、 Palo Alto Networks 社によって、すべてのデータが削除されます。³

機能	保持期間			
	Prisma Cloud		Cortex Cloud	
	Business Edition	Enterprise Edition	Cloud Posture Security	Cloud Runtime Security
取り込みデータ ⁴	契約期間中		31 日	
アラート情報	契約期間中		186 日	
フローログ	取得できない	30 日	取得できない	31 日
クラウド監査ログ ⁵	取得できない	30 日またはログの総数が 12 億件を越えた時点まで	31 日	
テナント監査ログ ⁶	30 日		365 日	
クエリデータ ⁷	-		186 日	

³ 2024 年 1 月現在、メーカー側で変更する可能性があります。

⁴ AWS、Azure、GCP などのパブリッククラウド上で稼働する仮想サーバー、ストレージ、ネットワークなどの各資産（リソース）が、現在どのような設定状態にあるかを示す詳細な情報に加え、クラウド環境でアクティブなアセット構成を含むデータを指します。

⁵ 対象クラウド：AWS、Azure、GCP

⁶ Prisma Cloud テナント、Cortex Cloud テナントでのコンソール操作等を記録する監査ログ

⁷ Cortex Cloud に取り込まれた各種データをクエリ言語（XQL）や API で検索・抽出・分析したデータ

3.3.11. Prisma Cloud/Cortex Cloud のデータ保持容量

- 保持される容量は以下の通りです。

機能	保持期間			
	Prisma Cloud		Cortex Cloud	
	Business Edition	Enterprise Edition	Cloud Security	Posture Security Runtime Security
クラウド監査ログ	制限なし		50ワークロードあたり 1日1GBまで	50ワークロードあたり 1日1GBまで 監査ログの他、VPC フ ローログ、DNS ログに も適用されます。

3.4. 提供機能一覧

3.4.1. 基本機能一覧

マネージド CSPM では、以下の機能を標準で提供します。別途申請やポイントの消費は不要です。

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、「[5.4 お問い合わせ受付](#)」を参照してください。

No.	基本機能	概要
1	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、各種お問い合わせ、作業依頼申請、月次レポートのダウンロード、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、各種情報確認などが行えます。
2	月次レポート	運用状況を毎月まとめて、カスタマーポータルにレポートを掲載します。
3	Prisma Cloud/Cortex Cloud 製品の初期設定	基本プランをお申し込みいただいた場合、Prisma Cloud の利用のための CSPM 初期設定（NTT ドコモビジネスの推奨ポリシー設定含む）を行います。

		<p>CWPP 込みプランをお申し込みいただいた場合、Prisma Cloud の利用のための CSPM+CWPP+CIEM 初期設定（NTT ドコモビジネスの推奨ポリシー設定含む）</p> <p>Cortex Cloud(Posture Security)をお申し込みいただいた場合、Cortex Cloud の利用のための CSPM+CIEM 初期設定（NTT ドコモビジネスの推奨ポリシー設定含む）を行います。</p> <p>Cortex Cloud(Runtime Security)をお申し込みいただいた場合、Cortex Cloud の利用のための CSPM+CWPP+CIEM 初期設定（NTT ドコモビジネスの推奨ポリシー設定含む）を行います。</p>
4	Cortex Cloud 製品の定期的なポリシー等の更新提供	推奨ポリシー等は定期的に見直しを行い、開通済のお客さまへも提供されます。
5	アラート通知	CSPM/CWPP アラートプロファイルに該当するアラートについて、Prisma Cloud/Cortex Cloud から直接お客さまへ通知されます。
6	Prisma Cloud/Cortex Cloud 製品お問い合わせ日本語代行	Prisma Cloud/Cortex Cloud に関して、本来英語で実施すべき問い合わせを日本語で受け付け、Palo Alto Networks 社への問い合わせを代行し、日本語で回答します。
7	Prisma Cloud/Cortex Cloud 製品故障お問い合わせ	Prisma Cloud/Cortex Cloud の故障に関して、問い合わせを受け付け、Palo Alto Networks 社への問い合わせを代行し、日本語で回答します。

3.4.2. 作業依頼機能一覧

マネージド CSPM では、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ないため、窓口よりお断りさせていただきます。

No.	分類	作業依頼機能	概要	必要ポイント数
1	Prisma Cloud	CSPM 検知ポリシー変更	CSPM 機能の作業依頼です。脅威検知のためのポリシー変更作業を行います。 検知ポリシーの ON/OFF を実施します。	1
2		CSPM アラート解除	CSPM 機能の作業依頼です。アラートの解除、一時停止（一定期間アラートを抑制）、再オープン（解除取り消し）を実施します。	1
3		CSPM アラート修復	CSPM 機能の作業依頼です。自動で IaaS 側に対して設定変更を行い、設定を修正します。 アラートは消えます。	2
4		CSPM アラートレポート作成	CSPM 機能の作業依頼です。2 種類（Cloud Security Assessment、Business Unit Report）のレポートのうちいずれかを指定していただき、レポートを作成しご提供します。	2
5		CSPM コンプライアンスレポート作成	CSPM 機能の作業依頼です。コンプライアンス標準を指定していただき、レポートを作成しご提供します。	2
6		ユーザー追加/削除	Prisma Cloud へのログインユーザー（Prisma Cloud 管理者）の追加、削除を行います。	1
7		CSPM アラート通知先メールアドレス追加/削除	CSPM 機能の作業依頼です。アカウントグループに対するクラウドアカウントの追加/削除またはアラートルールに対する通知先メールアドレスの追加/削除を行います。	1
8		CSPM アラートルール追加	CSPM 機能の作業依頼です。主にクラウドアカウントごとにアラート通知先を分けることを目的としてアラートルールの追加を実施します。	1
9		CSPM アノマリ設定変更 (しきい値変更)	CSPM 機能の作業依頼です。アノマリ設定のチューニングを実施します。	1
10		CWPP 脆弱性レポート作成	CWPP 機能の作業依頼です。脆弱例検知のレポートを作成し csv ファイルでご提供します。	2

11		CWPP アラート レポート作成	CWPP 機能の作業依頼です。2種類 (Compliance、Runtime) のレポートを作成し csv ファイルでご提供します。	2
12		CWPP アラート 通知先メールアドレス 追加/削除	CWPP 機能の作業依頼です。CWPP アラート ルールに対する通知先メールアドレスの追加/ 削除を行います。	1
13		IAM セキュリティ 有効化/無効化	IAM セキュリティ (CIEM) の有効化/無効化を 行います。	1
14	Prisma Cloud / Cortex Cloud	各種カスタマイズ 支援	お客さまからの各種カスタマイズ支援依頼を対 応します。 依頼いただいた作業内容を元に 1pt~10pt から 選択していただきます。 作業依頼前に、TAM に対応実現可否や作業依頼 の消費ポイント数をご相談ください。	1~10

3.5. 提供機能（基本機能）

3.5.1. 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（SAC）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、月次レポートのダウンロード、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、お客さまのログインアカウント管理（ユーザー追加・変更、連絡先変更等）、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



3.5.2. 月次レポート

- セキュリティアドバイザリーセンター（SAC）から月次レポートを発行します。運用状況を毎月まとめて、カスタマーポータルにレポートを掲載します。お客さまは、カスタマーポータル上で月次レポートをダウンロードして確認いただけます。お客さまは、運用状況を確認いただきアクションすることが可能です。
- 月次レポート提供のタイミングは月末締め翌月 15 日（営業日外の場合は翌営業日）までの提供となります。セキュリティアドバイザリーセンター（SAC）は、翌月 1 日～15 日（営業日外の場合は翌営業日）の間に月次レポートを作成し、カスタマーポータルへ掲載します。月次レポートの作成日と掲載日の指定はできません。月次レポートには、掲載月の前月分の運用状況が記載されます。月次レポートの項目は Prisma Cloud/Cortex Cloud のアップデート等の状況により適宜見直しを図ります。

項目によっては Prisma Cloud/Cortex Cloud の仕様上、作成日から起算して過去 30 日分のデータとなり厳密に前月分の運用状況とならないことがあります。

そのため、月次レポートはご利用開始日の翌月以降からの提供となります。
- 本サービスを廃止される場合は、廃止日のタイミングにより、最終の月次レポートの提供タイミング、記載される運用状況の期間が異なりますので、予めご了承ください。

(1) 月の 1 日～14 日が廃止日となる場合：

廃止月の前月（1 日～15 日）に提供される月次レポート（廃止月の前々月分の運用状況が記載）が最終となります。

廃止月には月次レポートは提供されません。

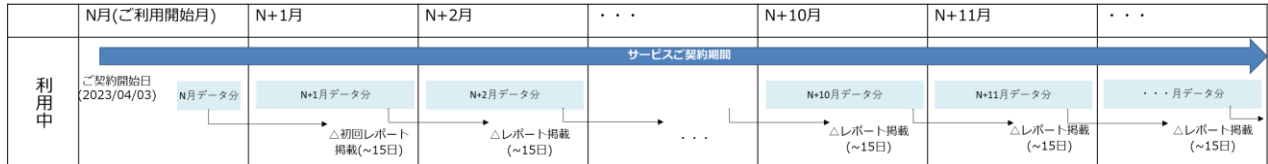
(2) 月の 15 日～月末が廃止日となる場合：

廃止月に提供される月次レポート（廃止月の前月分の運用状況が記載）が最終となります。

※カスタマーポータルでの提供は廃止日までとなりますので、廃止日が 15 日近辺になる場合は、月次レポート提供後、速やかにダウンロードしてください。

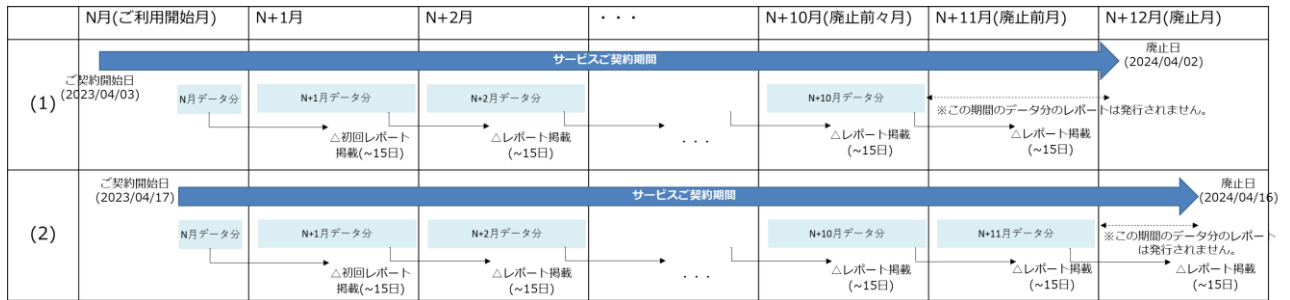
（参考）月次レポートの対象期間と発行/掲載のタイミング

【サービス利用開始～利用中】例：2023 年 4 月 3 日に契約開始し、継続利用中



【サービス廃止時】(1)の例：2023 年 4 月 3 日に契約開始し、2024 年 4 月 2 日にサービス廃止

(2)の例：2023 年 4 月 17 日に契約開始し、2024 年 4 月 16 日にサービス廃止

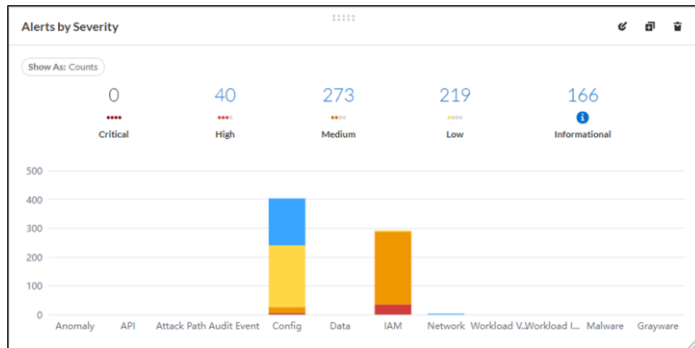


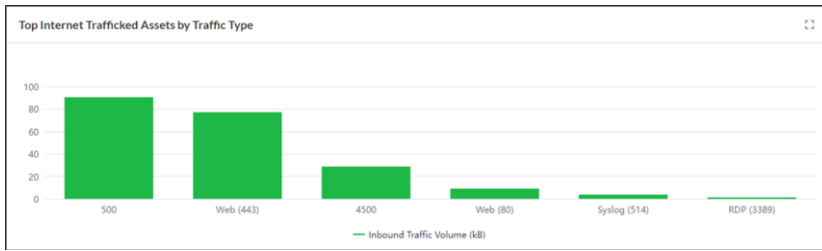
① Prisma Cloud

月次レポートで報告する内容（例）は以下の通りです。また、本内容は予告なく変更される場合があります。

また、ご利用のプラン（基本プラン/CWPP 込みプラン）によって、提供するレポートの内容が異なります。

- ・ CSPM 機能のサマリーグラフ（重大度別アラート、ポリシータイプ別アラート数の推移、サービスごとのトラフィック、インターネットからの接続、前月分のデータを取得）





※ 基本プラン (Business Edition) の場合、以下の 5 つのポリシータイプは月次レポートに表示されません (2025 年 7 月現在)

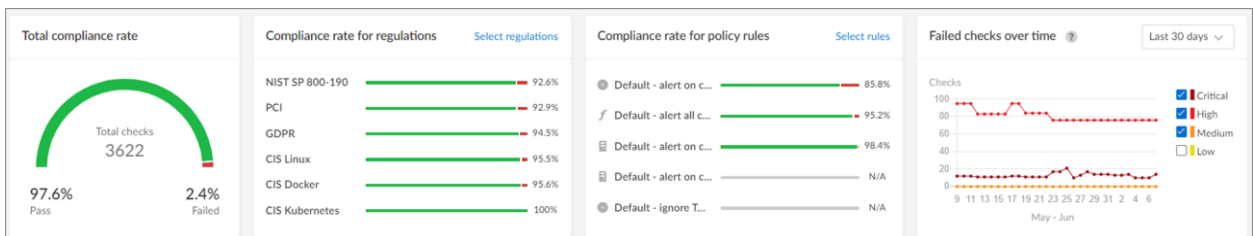
- Workload Incident
- Workload Vulnerability
- API
- Data
- IAM

CWPP 機能をご利用の場合は CWPP 機能に関するサマリーを報告します。

• CWPP 機能のサマリーグラフ (脆弱性アラート数の推移、作成日から起算して過去 30 日分のデータを取得)



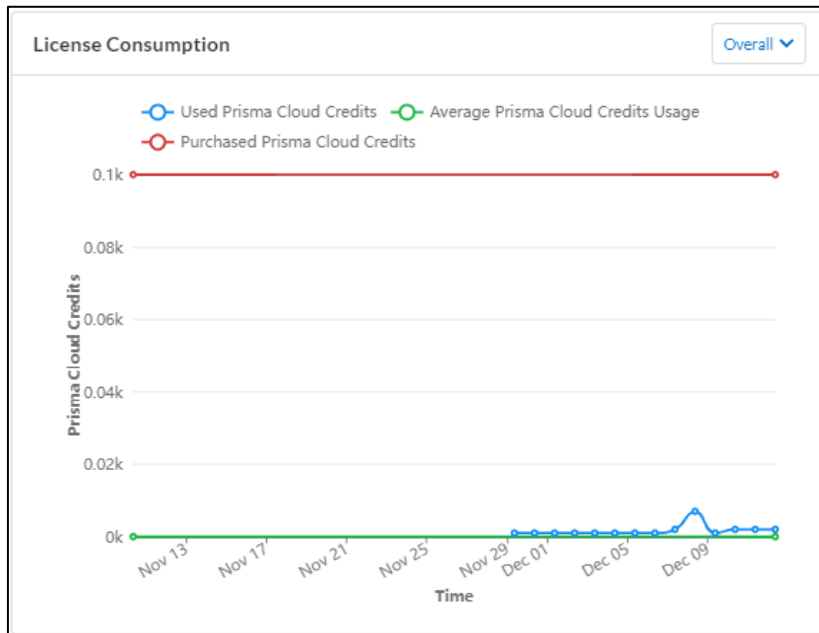
• CWPP 機能のサマリーグラフ (コンプライアンスの統計、Failed checks over time は作成日から起算して過去 30 日分のデータを取得)



• アラート詳細数 (全 Cloud account のアラート一覧を csv ファイルでご提供、前月分のデータを取得)

Alert ID	Policy Name	Policy Type	Description	Policy Lat	Policy Sev	Resource	Cloud Typ	Cloud Acc	Cloud Acc	Region	Recommen	Alert Stati	Alert Time	Event Occ	Dismiss	Dismiss	Dismiss	Resolved	Resolution	Resource ID
P-22905	Instances network	This policy identifies	Policy Sta	medium	instance-gcp	sys60405(Google Cl	GCP	Toky	to the Cloud The	open	Jun 07, 2023 23:57 JST	Asia/Tokyo								6.84E+18
N-22724	GCP VM i network	This polic	Prisma_C	high	instance-gcp	sys60405(Google Cl	GCP	Toky	following steps are Remediat	open	Jun 07, 2023 21:35 JST	Asia/Tokyo								6.84E+18
I-22826	GCP VM i iam	With access to iam.c	high	instance-gcp	sys60405(Google Cl	GCP	Toky	ion	steps:	open	Jun 07, 2023 21:16 JST	Asia/Tokyo								6.84E+18

- ・ライセンス状況（過去3か月間のクレジットご利用状況を時系列で表示）

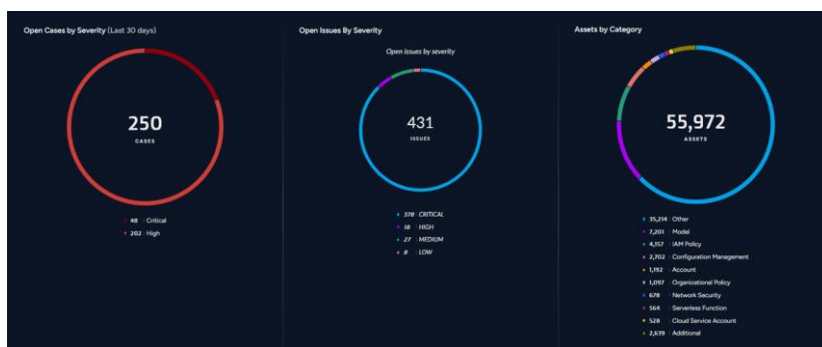


② Cortex Cloud

月次レポートで報告する内容（例）は以下の通りです。また、本内容は予告なく変更される場合があります。

また、ご利用のプラン（Cortex Cloud(Posture Security)/Cortex Cloud(Runtime Security)）によって、提供するレポートの内容が異なります。

- ・CSPM 機能のサマリーグラフ（重大度別アラート、ポリシータイプ別アラート数の推移、インターネットからの接続、前月分のデータを取得）



CWPP 機能をご利用の場合は CWPP 機能に関するサマリーを報告します。

- ・CWPP 機能のサマリーグラフ（脆弱性アラート数の推移、作成日から起算して過去 30 日分のデータを取得）



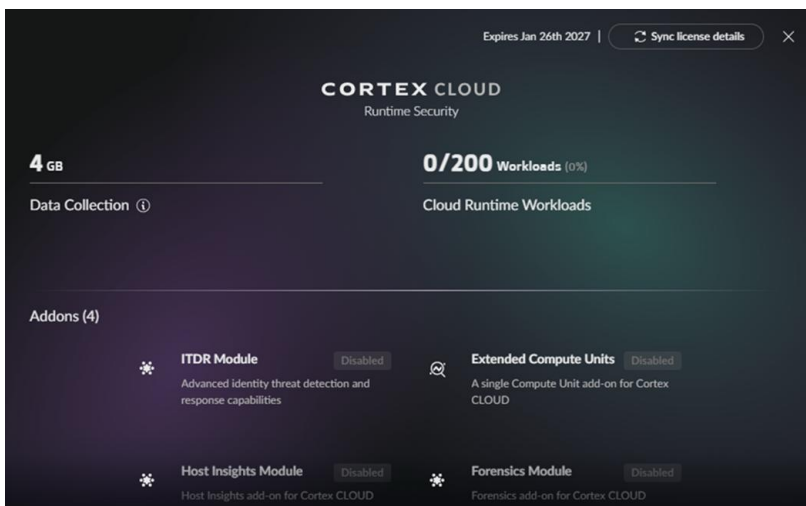
- ・CWPP 機能のサマリーグラフ（コンプライアンスの統計、Failed checks over time は作成日から起算して過去 30 日分のデータを取得）



- ・アラート詳細数（全 Cloud account のアラート一覧を csv ファイルでご提供、前月分のデータを取得）

Last Updated	Severity	Case Name	Status	Case ID	Case Domain	Creation Time	Case Description
Apr 21st 2026 11:26:26	High	Ensure auditing is configured for Docker files and directories - /etc/containerc	Resolved	4709	Posture	Mar 31st 2026 21:33:00	Apart from auditing your regular Linux file system and system calls, audit all D
Apr 21st 2026 11:26:22	Critical	Ensure TLS authentication for Docker daemon is configured	Resolved	4708	Posture	Mar 31st 2026 21:32:58	It is possible to make the Docker daemon available remotely over a TCP port. If
Apr 21st 2026 11:26:00	High	Ensure auditing is configured for Docker files and directories - /run/container	Resolved	4667	Posture	Mar 31st 2026 18:04:43	Apart from auditing your regular Linux file system and system calls, audit all D

- ・ライセンス状況（現在のワークロードご利用状況を時系列で表示）



3.5.3. Prisma Cloud/Cortex Cloud 製品の初期設定

Prisma Cloud/Cortex Cloud 製品をご利用いただくための初期設定を行います。

基本プランの場合は①～②、⑤、CWPP 込みプランの場合は①～⑤を設定します。

Cortex Cloud(Posture Security)、Cortex Cloud(Runtime Security)の場合は①、②、⑤を設定します。

① Prisma Cloud/Cortex Cloud 製品の共通設定 (ライセンス調達・テナント作成)

- Prisma Cloud/Cortex Cloud のライセンス調達、テナント払い出し、開通、ユーザー登録などを行います。お客さまよりお申し込みを受け、NTT ドコモビジネスは提携事業者を通じて、Palo Alto Networks 社に Prisma Cloud/Cortex Cloud の発注を行います。
- Prisma Cloud/Cortex Cloud ライセンスは、NTT ドコモビジネスの資産となり、NTT ドコモビジネスのカスタマーサポートポータル (CSP) に紐付けられます。カスタマーサポートポータル (CSP) はお客さま毎に分けられます。
- 各項目の設定値は、以下となり、「お客様番号」および「カスタマーサポートポータルアカウント (CSP)No」は、新設時に開通案内 (ご利用内容のご案内) にて通知されます。

項目	設定値
カスタマーサポートポータルアカウント(CSP)名	お客様番号
TenantID	お客様番号
カスタマーサポートポータルアカウント(CSP)No	Palo Alto Networks 社から払出し

- テナント作成時に、以下のユーザーを作成します。
※Role については、「[3.6.6 ユーザー追加/削除](#)」を参照してください。

【Prisma Cloud】

アカウント用途	ユーザーアカウント	備考	ROLE	2	3	4	5
Prisma Cloud 管理者①	新設申込書に記載いただくメールアドレス	必須	Cloud Provisioning Admin_NTTCommunications	●	●	●	● 8
Prisma Cloud 管理者②	新設申込書に記載いただくメールアドレス	任意					
Prisma Cloud 管理者③	新設申込書に記載いただくメールアドレス	任意					

⁸ お客さま判断で必要なユーザーに設定をお願いします。

NTT ドコモビジネス 保守用①	sac-cspm-wa@ntt.com	必須	System Admin	●	●	●	×
NTT ドコモビジネス 保守用②	cspm-tech-maintenance@ntt.com	必須		●	●	●	×
提携事業者保守用	prisma-cloud-scsk-support@scsk.jp	必須		●	●	●	×

【Cortex Cloud】

アカウント用途	ユーザーアカウント	備考	ROLE	1	2	3	4	5
Cortex Cloud 管理者①	新設申込書に記載いただくメールアドレス	必須	Instance Administrator	●	●	●	●	● 8
Cortex Cloud 管理者②	新設申込書に記載いただくメールアドレス	任意		●	●	●	●	×
Cortex Cloud 管理者③	新設申込書に記載いただくメールアドレス	任意		●	●	●	●	×
NTT ドコモビジネス 保守用①	sac-cspm-wa@ntt.com	必須	Account Admin	●	●	●	●	×
NTT ドコモビジネス 保守用②	cspm-tech-maintenance@ntt.com	必須		●	●	●	●	×
提携事業者保守用	cortex-cloud-scsk-support@scsk.jp	必須		●	●	●	●	×

1. Cortex User 権限付与
2. SuperUser 権限付与
3. Domain Administrator 権限付与
4. ホワイトリスト登録
5. Emergency Security Contact 権限付与⁹

⁹ Emergency Security Contact : 緊急セキュリティ連絡先 (ESC)。Palo Alto Networks 社からの緊急セキュリティ通知を受け取ることができます。これらの通知では、Palo Alto Networks 製品およびサービスに関連する潜在的な脆弱性、その他のセキュリティ上の懸念事項、お客さまデバイスのセキュリティ侵害の兆候についてお知らせします。

② CSPM 機能の推奨ポリシー設定 Prisma Cloud

- Prisma Cloud に NTT ドコモビジネスの推奨する CSPM 機能のポリシーの設定を行います。AWS/Azure/GCP に対応するポリシーを有効にします。
- NTT ドコモビジネスの推奨ポリシーは原則以下となり、本設定が初期設定として有効化されます。
- なお、NTT ドコモビジネスの判断により、推奨ポリシーは予告なく変更となり、設定が必ずしも以下の通りにならない場合があります。
- 開通後、お客さまが既存ポリシーの ON/OFF の変更を希望される場合は、作業依頼機能の「検知ポリシー変更」にて変更を申請いただけます。
- Prisma Cloud はポリシーが追加される可能性があります。初期設定にて、全てのポリシーは自動的に有効にする設定となっており、ポリシーが追加されたとしても自動で有効化されます。

項目	NTT ドコモビジネスの推奨ポリシー
全ポリシー	自動的に有効にします。
アノマリ設定	機械学習を実施する際の閾値=Aggressive、学習期間=Medium にて設定します。
カスタムポリシー ¹⁰	NTT ドコモビジネス独自のポリシールールを設定します。

③ CWPP 機能の初期設定 Prisma Cloud

- Prisma Cloud に NTT ドコモビジネスの推奨する CWPP 機能のポリシー設定を行います。
- NTT ドコモビジネスの推奨ポリシーは原則以下となり、本設定が初期設定として有効化されます。
- なお、NTT ドコモビジネスの判断により、推奨ポリシーは予告なく変更となり、設定が必ずしも以下の通りにならない場合があります。

項目	NTT ドコモビジネスの推奨ポリシー
Vulnerability	デプロイされたコンテナイメージ、ホスト、関数に対して、Severity が High 以上のアラートを通知します。
Compliance	デプロイされたコンテナイメージ、ホスト、サーバーレスに対して、Severity が High 以上のアラートを通知します。
Runtime	実行中のコンテナ、ホスト、サーバーレスに対して、

¹⁰ 基本プラン（Business Edition）の場合、カスタムポリシーはアノマリ設定に係るポリシーと AWS、Azure、GCP 等の監査ログに係るポリシーについては提供対象外（2025 年 7 月現在）

	ランタイム機能の推奨ポリシーを設定します。
--	-----------------------

④ CIEM 機能の初期設定 Prisma Cloud

項目	NTT ドコモビジネスの推奨ポリシー
IAM セキュリティ	IAM セキュリティを有効化します。

② 推奨ポリシー設定 Cortex Cloud

- Cortex Cloud に NTT ドコモビジネスの推奨するポリシーの設定を行います。AWS/Azure/GCP に対応するポリシーを有効にします。
- NTT ドコモビジネスの推奨ポリシーは原則以下となり、本設定が初期設定として有効化されます。
- なお、NTT ドコモビジネスの判断により、推奨ポリシーは予告なく変更となり、設定が必ずしも以下の通りにならない場合があります。
- Cortex Cloud はルールが追加される可能性があります。初期設定にて、全てのルールは自動的に有効にする設定となっており、ルールが追加されたとしても自動で有効化されます。ただし、一部は自動で有効化されないため定期的な更新を行い対応します。

項目	NTT ドコモビジネスの推奨ポリシー	
Cloud Workload	Misconfigurations (設定ミス)	すべてのワークロードアセットに対して、すべてのルールを対象に設定します。 ¹¹
	Malware (マルウェア)	検知可能なすべてのアセットに対して、すべてのルールを対象に、Severity が High で Issue を作成します。
	Secrets (シークレット)	検知可能なすべてのアセットに対して、すべてのルールを対象に、Severity が High で Issue を作成します。
Cloud Security	すべてのクラウドアセットに対して、すべてのルールを対象に設定します。	
Vulnerability Management	Issue Creation (脆弱性検知)	すべてのアセットに対して、Severity が High 以上を対象に、Issue を作成します。
	Prevention (脆弱性保護)	Cortex CLI を使用して連携した CI/CD パイプラインに対して、Severity が High 以上を対象に設定します。

¹¹ 追加されたルールは自動で有効化されない。

Prevention Policy Rules	エンドポイント、関数に対して、Agent Settings、Malware、Exploit、Restrictions、Exceptions に対して、Issue を作成します。
-------------------------	--

⑤ Prisma Cloud/Cortex Cloud とお客さま IaaS の連携【お客さま作業】

- Prisma Cloud/Cortex Cloud とお客さま IaaS の連携設定はお客さまにて実施いただきます。

ご利用開始日前後のご連絡および設定の流れは以下となります。

日程	実施内容
ご利用開始日の 2 営業日前 ～ご利用開始日	<ul style="list-style-type: none"> Prisma Cloud/Cortex Cloud に設定されたアカウントがお客さまへメールで通知されます。 メールに Prisma Cloud/Cortex Cloud にログインするための URL が記載されています。
ご利用開始日の 1 営業日前	<ul style="list-style-type: none"> 開通案内（ご利用内容のご案内）のダウンロード URL がメールで通知されます。 開通案内には、カスタマーポータル URL が記載されています。
ご利用開始日	<ul style="list-style-type: none"> カスタマーポータルへのログインが可能となります。
ご利用開始日～	<ul style="list-style-type: none"> お客さまにて、カスタマーポータルから各クラウド別の連携ガイドをダウンロードいただき、Prisma Cloud/Cortex Cloud とお客さま IaaS の連携設定（お客さま IaaS の設定および Prisma Cloud/Cortex Cloud へのお客さま IaaS の管理者アカウントの設定等）を実施いただきます。

3.5.4. Cortex Cloud 製品の定期的なポリシー等の更新提供

Cortex Cloud

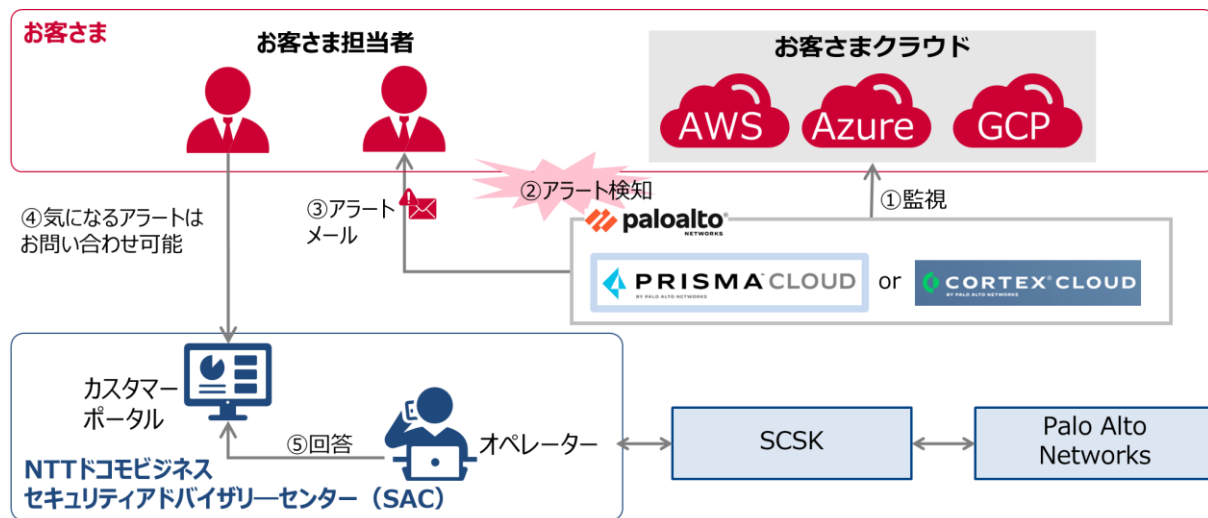
- NTT ドコモビジネスの推奨ポリシー等は定期的に見直しを行い、開通済のお客さまの Cortex Cloud へも更新適応を行います。
- ポリシー等の更新に伴い、新たに対象となったポリシー等に関しては、お客さまのクラウドの状況によってはアラート通知が発生することがありますのでご了承ください。
- お客さまにて作成・変更したポリシーや個別に作業依頼を頂いて作成したポリシーについては、個別の設定を優先し、本ポリシー等の見直しに伴う設定更新の対象からは除外させていただきます。
- なお、Cortex Cloud のルールは、適宜、自動的に増減します。削除されるルールは自動的にポリシーからも削除されますので、定期的なポリシー等の更新のタイミングとは関係なく適応されます。

また、クラウドワークロードのマルウェアやシークレット、クラウドセキュリティのポリシーについても、ルールの増減が自動的に反映されますので、定期的なポリシー等の更新のタイミングとは関係なく適応されます。

3.5.5. アラート通知

■ アラート通知（CSPM 機能・CIEM 機能）

- お客さまへのアラート通知は、Severity が High (高)、または Critical の場合、Prisma Cloud/Cortex Cloud から直接自動的にお客さまに対して通知されます。お客さまは、その通知メールのリンクより Prisma Cloud/Cortex Cloud にログインし、アラートの詳細を確認することができます。
- 本サービスでは、Prisma Cloud/Cortex Cloud のログの分析やアラートの内容の精査はしていませんが、お客さまにてアラートの内容について不明な点がある場合は、カスタマーポータルからお問い合わせをいただくことで、セキュリティアドバイザリーセンター（SAC）がアラートの内容を確認し回答することが可能です。



- NTT ドコモビジネスが推奨しているポリシーにマッチしたものがアラートとして通知されます。お客さまにご確認いただきたいアラートに絞り、通知されるようになっています。
- アラートに対し、お客さまは以下のアクションのうち、いずれかの対応が必要です。

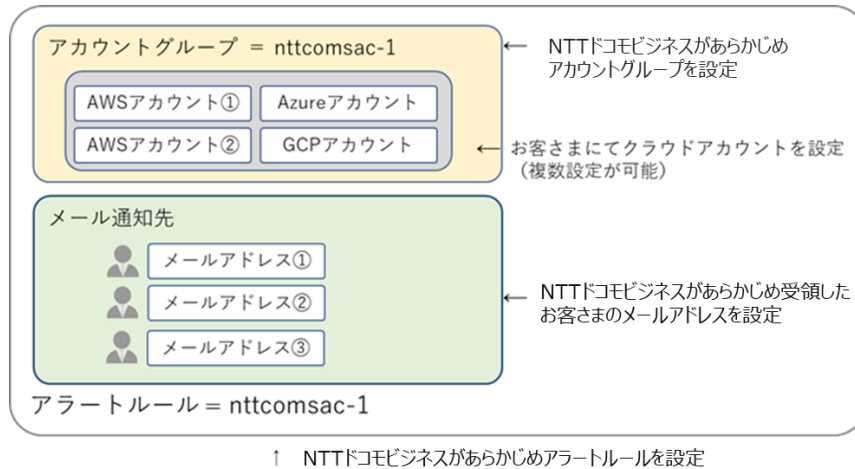
① Prisma Cloud

アラートに対するお客さまのアクション	アクション実施後の動作
お客さまにて、アラートの内容に従い、IaaS (AWS、Azure、GCP) 上で、修正・対応を行う	Prisma Cloud が自動的に対応を確認しアラートが「解決済」となる

<p>セキュリティアドバイザリーセンター（SAC）へ、カスタマーポータルより作業依頼にてアラートの修復依頼を行う</p> <p>※対応しているアラートのみ ※作業依頼申請にポイントが必要です</p>	<p>Prisma Cloud から自動的に、お客様の IaaS に対して修復を実行し、成功すればアラートが「解決済」となる</p>
<p>セキュリティアドバイザリーセンター（SAC）へ、カスタマーポータルより作業依頼にてアラートの解除依頼（解除、または、一時停止）を行う</p> <p>※作業依頼申請にポイントが必要です</p>	<ul style="list-style-type: none"> 「解除」を実行すると、Prisma Cloud 上で「解除済」となり同じアラートは抑制される 「一時停止」を実行すると、「一時停止中」となり、一定期間（ご指定いただいた期間）アラートが抑制される
<p>セキュリティアドバイザリーセンター（SAC）へ、カスタマーポータルより作業依頼にて検知ポリシー変更依頼（検知ポリシーの OFF 設定）依頼を行う</p> <p>※作業依頼申請にポイントが必要です</p>	<p>検知ポリシーを OFF にすることで、アラートが発生しなくなるが、当該ポリシーが今後全く動作しなくなる</p>
<p>無視する（何もしない）</p>	<p>同じアラートは、発生しないが、Prisma Cloud 上で「未解決」としてアラートが残り続ける。月次レポート上も記載され続ける</p>

- アラート通知設定の初期設定は、次の通りです。セキュリティアドバイザリーセンター（SAC）は、「nttcomsac-1」という「アラートルール」を作成します。その「アラートルール」内に「アカウントグループ」と「メール通知先」を登録します。
- アカウントグループに対し、お客様にてお客様 IaaS（AWS、Azure、GCP）のクラウドアカウントを登録いただきます。
- 初期開通時のメール通知先には、お申し込み時に Prisma Cloud 管理者①②③（②③は任意）として記入いただいたお客様のメールアドレスを登録します。
- 本設定により、アラートの通知先の登録が完了されます。

(参考) アラート通知設定のイメージ



- 初期設定では、上記の通り、1つのアラートルールに対し、お申し込み時に Prisma Cloud 管理者①②③ (②③は任意) としていただいたお客様メールアドレスを3つまで登録しています。クラウドアカウントを複数登録した場合でも、メール通知先は同じになります。
 - クラウドアカウント毎にアラートメールの通知先を分けたい場合は、開通後、作業依頼にて「**3.6.8. CSPM アラートルール追加**」依頼を行ってください。
 - アラートメールの通知先のメールアドレスを追加または削除したい場合には、開通後、作業依頼にて「**3.6.7. CSPM アラート通知先メールアドレス追加/削除**」依頼を行ってください。
 - アカウントグループに対するクラウドアカウントを追加または削除したい場合には、開通後、作業依頼にて「**3.6.7. CSPM アラート通知先メールアドレス追加/削除**」依頼を行ってください。

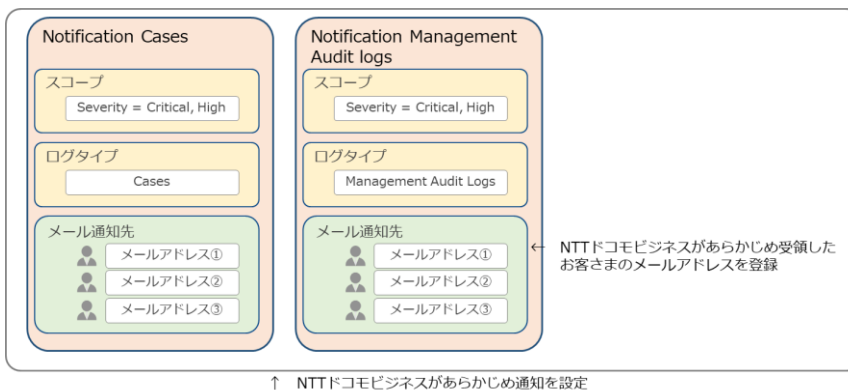
② Cortex Cloud

アラートに対するお客様のアクション	アクション実施後の動作
お客様にて、アラートの内容に従い、IaaS (AWS、Azure、GCP) 上で、修正・対応を行う	Cortex Cloud が自動的に対応を確認し Cases/Issues が「解決済」となる
お客様にて、アラートの修復を行う	Cortex Cloud から自動的に、お客様のIaaSに対して修復を実行し、成功すればアラートが「解決済」となる
お客様にて、アラートの解除を行う	「Resolved - Dismissed」(解除) を実行すると、Cortex Cloud 上で「Resolved - Dismissed」(解除済) となり同じアラートは抑制される

<p>お客さまにて、検知ポリシー変更（検知ポリシーの OFF 設定）を行う ※作業依頼申請にポイントが必要です</p>	<p>検知ポリシーを OFF にすることで、アラートが発生しなくなるが、当該ポリシーが今後全く動作しなくなる</p>
<p>無視する（何もしない）</p>	<p>同じアラートは、発生しないが、Cortex Cloud 上で「未解決」としてアラートが残り続ける。月次レポート上も記載され続ける</p>

- アラート通知設定の初期設定は、次の通りです。セキュリティアドバイザリーセンター（SAC）は、「Notification Cases」、「Notification Management Audit Logs」という「通知」を作成します。その「通知」内に「メール通知先」を登録します。
- 初期開通時のメール通知先には、お申し込み時に Cortex Cloud 管理者①②③（②③は任意）として記入いただいたお客さまのメールアドレスを登録します。
- 本設定により、アラートの通知先の登録が完了されます。

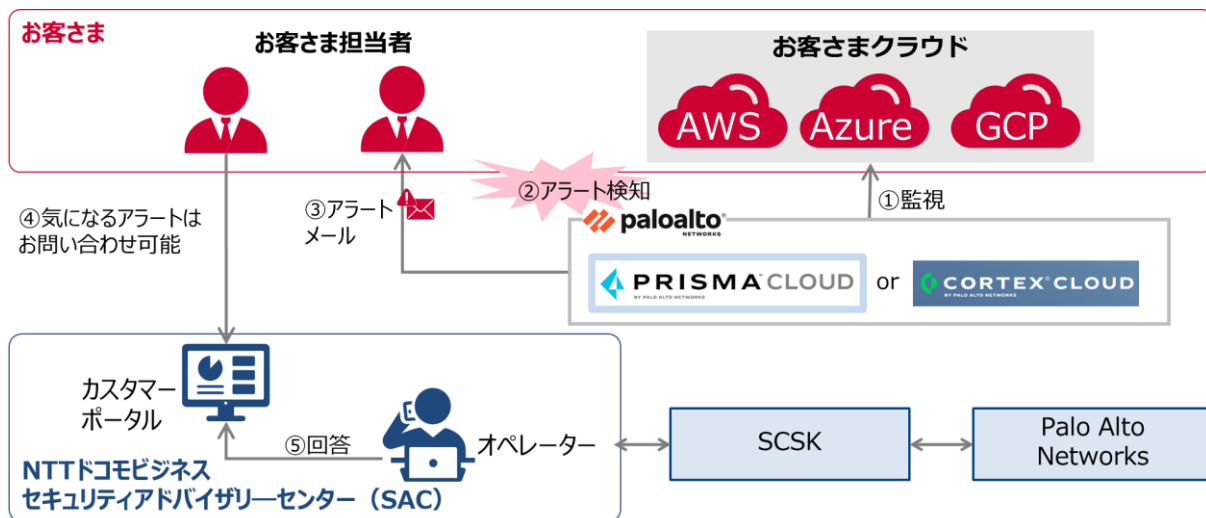
（参考）アラート通知設定のイメージ



- 初期設定では、上記の通り、1つの通知に対し、お申し込み時に Cortex Cloud 管理者①②③（②③は任意）としていただいたお客さまメールアドレスを3つまで登録しています。

■ アラート通知（CWPP 機能）

- お客さまへのアラート通知は、CWPP アラートプロファイルに該当する場合、Prisma Cloud/Cortex Cloud から直接自動的にお客さまに対して通知されます。お客さまは、その通知メールのリンクより Prisma Cloud/Cortex Cloud にログインし、アラートの詳細を確認することができます。
- 本サービスでは、Prisma Cloud/Cortex Cloud のログの分析やアラートの内容の精査はしていませんが、お客さまにてアラートの内容について不明な点がある場合は、カスタマーポータルからお問い合わせをいただくことで、セキュリティアドバイザリーセンター（SAC）がアラートの内容を確認し回答することが可能です。



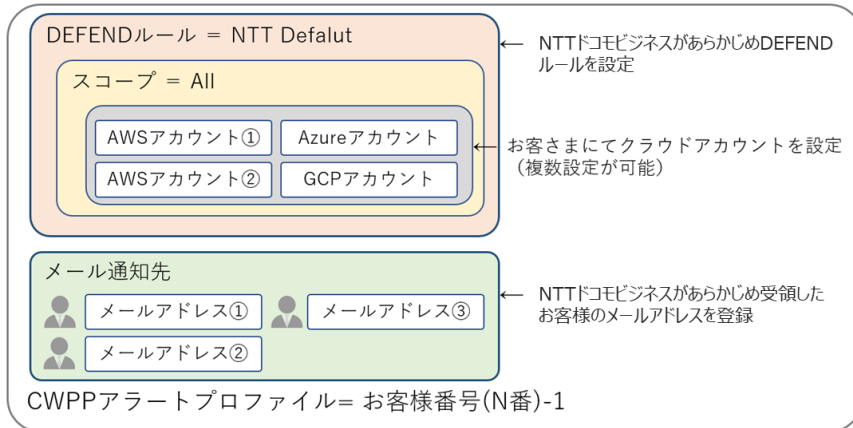
- NTTドコモビジネスが推奨しているポリシーにマッチしたものがアラートとして通知されます。お客様にご確認いただきたいアラートに絞り、通知されるようになっています。
- アラートに対し、お客様は以下のアクションのうち、いずれかの対応が必要です。

アラートの種類	アラートに対するお客様のアクション
脆弱性アラート	Prisma Cloud/Cortex Cloud から、該当する脆弱性の概要と修正バージョンをご確認いただき、対象クラウドアカウントのバージョンアップなどの対策が必要です。
コンプライアンスアラート	Prisma Cloud/Cortex Cloud から、該当するコンプライアンスアラートをご確認いただき、対象クラウドアカウントの設定変更などの対策が必要です。
ランタイムアラート	お客様の方でアラートの内容をご確認いただき、アラート対象のプロセスを停止する、イメージを再デプロイするなどの対処が必要です。

① Prisma Cloud

- アラート通知設定の初期設定は、次の通りです。セキュリティアドバイザリーセンター (SAC) は、「お客様番号(N番)-1」という「CWPP アラートプロファイル」を作成します。その「CWPP アラートプロファイル」内に対象の「DEFEND ルール」と「メール通知先」を登録します。
- お客様にてお客様 IaaS (AWS、Azure、GCP) のクラウドアカウントを登録いただきます。
- 初期開通時のメール通知先には、お申し込み時に Prisma Cloud 管理者①②③ (②③は任意) として記入いただいたお客様のメールアドレスを登録します。
- 本設定により、アラートの通知先の登録が完了されます。

(参考) アラート通知設定のイメージ

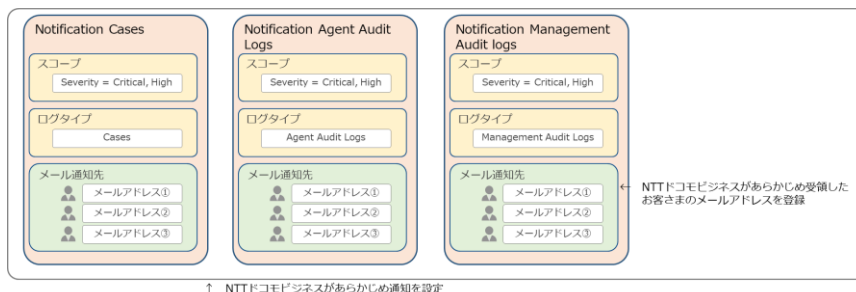


- 初期設定では、上記の通り、1つのアラートプロファイルに対し、お申し込み時に Prisma Cloud 管理者①②③ (②③は任意) としていただいたお客さまメールアドレスを3つまで登録しています。クラウドアカウントを複数登録した場合でも、メール通知先は同じになります。
 - アラートメールの通知先のメールアドレスを追加または削除したい場合には、開通後、作業依頼にて「**3.6.12. CWPP アラート通知先メールアドレス追加/削除**」依頼を行ってください。

② **Cortex Cloud**

- アラート通知設定の初期設定は、次の通りです。セキュリティアドバイザリーセンター (SAC) は、「Notification Cases」、「Notification Agent Audit logs」、「Notification Management Audit Logs」という「通知」を作成します。その「通知」内に対象の「メール通知先」を登録します。
- 初期開通時のメール通知先には、お申し込み時に Cortex Cloud 管理者①②③ (②③は任意) として記入いただいたお客さまのメールアドレスを登録します。
- 本設定により、アラートの通知先の登録が完了されます。

(参考) アラート通知設定のイメージ



- 初期設定では、上記の通り、1つのアラートプロファイルに対し、お申し込み時に Cortex Cloud 管理者①②③ (②③は任意) としていただいたお客さまメールアドレスを3つまで登録しています。

3.5.6. Prisma Cloud/Cortex Cloud 製品お問い合わせ日本語代行

- Prisma Cloud/Cortex Cloud に関して、お客さまが Palo Alto Networks 社へ英語で実施するお問い合わせを日本語で受け付け、Palo Alto Networks 社への問い合わせを代行し、日本語で回答します。
- 基本的には、Prisma Cloud/Cortex Cloud の仕様や操作方法のお問い合わせに回答するものであり、お客さま特有の環境に即した回答は出来かねますので、予めご了承ください。
- 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、次の問い合わせをすることはできません。
- 基本プランについては、CSPM 機能についてのみが対象となります。
- Cortex Cloud(Posture Security)については、CSPM 機能および CIEM 機能についてが対象となります。
- CWPP 込みプラン、Cortex Cloud(Runtime Security)については、CSPM 機能および CWPP 機能、CIEM 機能についてが対象となります。
- お問い合わせ方法については、「[5.4 お問い合わせ受付](#)」および「[5.6 お問い合わせ受付・運用受付/通知方法](#)」を参照ください。

3.5.7. Prisma Cloud/Cortex Cloud 製品故障お問い合わせ

- Prisma Cloud/Cortex Cloud の故障に関して、問い合わせを受け付け、Palo Alto Networks 社への問い合わせを代行し、日本語で回答します。
なお、Prisma Cloud/Cortex Cloud に対して稼働状況の監視を実施するサービスではありません。
- 基本プランについては、CSPM 機能についてのみが対象となります。
- Cortex Cloud(Posture Security)については、CSPM 機能および CIEM 機能についてが対象となります。
- CWPP 込みプラン、Cortex Cloud(Runtime Security)については、CSPM 機能および CWPP 機能、CIEM 機能についてが対象となります。
- お問い合わせ方法については、「[5.5 故障受付](#)」および「[5.6 お問い合わせ受付・運用受付/通知方法](#)」を参照ください。

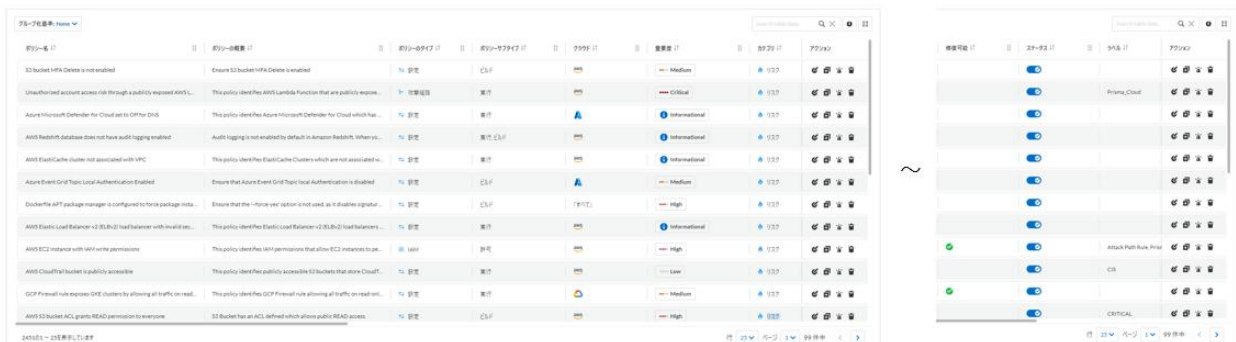
3.6. 提供機能（作業依頼機能）

3.6.1. CSPM 検知ポリシー変更

Prisma Cloud

CSPM 機能の作業依頼です。サービス開始時に推奨設定を NTT ドコモビジネスで実施し運用開始します。しかし、運用開始後、過検知や不要なアラートとお客さまが判断した場合は、お客さまはカスタマーポータルから検知ポリシーの変更申請をすることが可能です。NTT ドコモビジネスのセキュリティアドバイザリーセンター（SAC）は、お客さまからの申告を受け、申告いただいたポリシーを OFF にすることで、お客さまから当該アラートの抑制処理を行います。また、逆に ON にすることも可能です。

（参考）設定のイメージ



セキュリティアドバイザリーセンター（SAC）は、具体的に以下を実施します。

- ・ポリシーのステータスを OFF にする
- ・ポリシーのステータスを ON にする

<お客さまの作業申請項目>

- ・作業概要：検知ポリシーON/検知ポリシーOFF ※いずれか選択していただきます
- ・作業対象ポリシー名 ※1 作業で同時に依頼できるのは 10 ポリシーまでとさせていただきます

3.6.2. CSPM アラート解除

Prisma Cloud

CSPM 機能の作業依頼です。NTT ドコモビジネスからアラートを通知したものの、お客さまにてアラート解除を申請される場合は、セキュリティアドバイザリーセンター（SAC）にて受け付け、Prisma Cloud 上でアラートの解除を行います。アラートの解除を行うと、その同じアラートは、お客さまの環境が変わらない（クラウド側設定変更/Prisma Cloud 側ポリシー変更）限り、抑制されます。また、一時停止の場合は一定期間アラート通知が抑制されます。

さらに、再オープン（アラート解除の取り消し）作業も可能です。

（想定されるケース）

- ・解除 : 検証環境のため無視するようなケース
- ・一時停止 : 開発環境であり、今は一時的にアラートの通知が不要なケース

（参考）設定のイメージ

アラートを解除	アラートをスヌーズ
<div data-bbox="188 689 518 757"> <input type="button" value="解除"/> 1 open alert(s) </div> <div data-bbox="188 772 608 909"> 理由* <input type="text"/> </div>	<div data-bbox="662 678 960 723"> <input type="button" value="一時停止"/> 1 open alert(s) </div> <div data-bbox="662 734 1185 784"> <input type="button" value="停止期間"/> 1 <input type="button" value="週間"/> </div> <div data-bbox="662 795 1212 909"> 理由* <input type="text"/> </div>

<お客さまの作業申請項目>

- ・作業概要 : アラート解除/アラート一時停止/アラート再オープン ※いずれかを選択していただきます
- ・アラート ID ※1 作業で同時に依頼できるのは 10ID までとさせていただきます
- ・アラート一時停止終了日時 ※作業概要にてアラート一時停止を選択いただいたときのみ

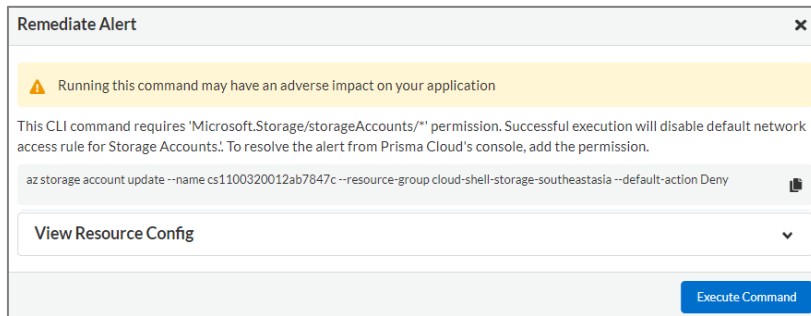
3.6.3. CSPM アラート修復

Prisma Cloud

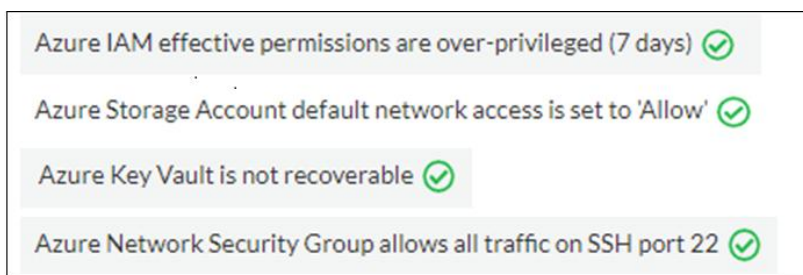
CSPM 機能の作業依頼です。NTT ドコモビジネスからアラートを通知したもののうち、Prisma Cloud からお客さま IaaS（AWS、Azure、GCP）に対して修復が可能なものがあります。セキュリティアドバイザリーセンター（SAC）では、お客さまからの作業依頼に基づき、Prisma Cloud 上からお客さまの IaaS（AWS、Azure、GCP）に対してコマンドを発行します。

コマンド発行後、修復が成功した場合は、Prisma Cloud 上でアラートが「解決済」となり、セキュリティアドバイザリーセンター（SAC）はお客さまに修復完了として報告します。お客さまもご自身で IaaS 側の設定が変更されているか確認してください。また、修復のコマンドが Prisma Cloud 上から実行できない場合は、セキュリティアドバイザリーセンター（SAC）は作業を中止し、お客さまに修復不可として報告します。

(参考) アラート修復の実行イメージ例



(参考) アラート修復可能なものの例



※修復可能なものはアラートの末尾に🟢が付与されています。

<お客さまの作業申請項目>

- ・アラート ID ※1 作業で同時に依頼できるのは 10ID までとさせていただきます

本作業は、お客さまの IaaS (AWS、Azure、GCP) に対して、Prisma Cloud から自動的にコマンドを実行し、IaaS の設定変更を実施するものです。NTT ドコモビジネスは、本作業の実施によりお客さま IaaS 環境の動作を保証するものではなく、事前に検証を行い動作確認が取れたもののみ作業依頼をいただけますようお願いいたします。本作業による、意図しない通信遮断や、クラウドの不具合については、NTT ドコモビジネスは一切の責任を負うことはできません。

3.6.4. CSPM アラートレポート作成

Prisma Cloud

CSPM 機能の作業依頼です。Prisma Cloud で生成可能なアラートレポートは 2 種類あります。セキュリティアドバイザリーセンター (SAC) に作業依頼をいただくことで、NTT ドコモビジネスが Prisma Cloud 上でアラートレポートを作成し、カスタマーポータルへアップロードを行います。お客さまは、カスタマーポータルから、レポートを取得することが可能です。

アラートレポートの種類は次の通りです。

レポートタイプ	Cloud Security Assessment ¹²	Business Unit Report
レポートの内容	アラートのサマリー アラートの一覧	アラートごとの詳細 過去のアラートが全て表示される(解決済み含む)
レポート形式	PDF	CSV
レポートの単位	クラウドタイプ単位 アカウントグループ単位 クラウドアカウント単位	アカウントグループ単位
期間	期間指定可能	期間指定不可(過去分全て表示)
レポート出力内容(例)		

<お客さまの作業申請項目>

- ・ 作業概要 : Cloud Security Assessment 作成/Business Unit Report 作成
※いずれかを選択していただきます
- ・ クラウドタイプ ※作業概要として Cloud Security Assessment 作成を選択した場合のみ
- ・ アカウントグループ名
- ・ クラウドアカウント名 ※作業概要として Cloud Security Assessment 作成を選択した場合のみ
※指定したいクラウドアカウントが 10 アカウントを超える場合には所定のフォーマット (Excel ファイル) に記入しファイル添付してください
- ・ レポート対象の開始日時 ※作業概要として Cloud Security Assessment 作成を選択した場合のみ
- ・ レポート対象の終了日時 ※作業概要として Cloud Security Assessment 作成を選択した場合のみ

¹² 作業依頼申請時点で Prisma Cloud との連携が解除されているクラウドアカウントのレポートは提示できないことがあります。(連携解除後 90 日経過時点でアラートのログは Prisma Cloud 上から削除されます。)

3.6.5. CSPM コンプライアンスレポート作成

Prisma Cloud

CSPM 機能の作業依頼です。Prisma Cloud は、各種コンプライアンス要件と照合したレポートの作成が可能です。このレポートにより、例えば、PCIDSS や CIS の基準に照らし、設定の不備があるか否かが判断できます。セキュリティアドバイザリーセンター（SAC）に作業依頼をいただくことで、NTT ドコモビジネスが Prisma Cloud 上でコンプライアンスレポートを作成¹³し、カスタマーポータルへアップロードを行います。お客さまは、カスタマーポータルから、レポートを取得することが可能です。

(参考) レポート出力内容例



<お客さまの作業申請項目>

- ・コンプライアンス標準
- ・レポート対象日時：最新/カスタム ※いずれかを選択していただきます
- ・レポート対象日時指定 ※レポート対象日時でカスタムを選択した場合のみ
- ・クラウドアカウント

※指定したいクラウドアカウントが 10 アカウントを超える場合には所定のフォーマット（Excel ファイル）に記入しファイル添付してください

- ・クラウドタイプ
- ・アカウントグループ名

¹³ 作業依頼申請時点で Prisma Cloud との連携が解除されているクラウドアカウントのレポートは提示できないことがあります。（連携解除後 90 日経過時点でアラートのログは Prisma Cloud 上から削除されます。）

3.6.6. ユーザー追加/削除

Prisma Cloud

NTT ドコモビジネスが管理する Prisma Cloud の管理画面へ、お客さまもログインすることを可能とします。接続するユーザー情報の変更を行います。なお、払い出しが可能なアカウントの種類は

- ・ Cloud Provisioning Admin_NTTCommunications

であり、申請すると、上記の権限が付与されます。

(参考) 作業イメージ

(参考) Prisma Cloud のアカウント種類 (マネージド CSPM 利用アカウント種類)

アカウント種類	説明
System Admin	サービスを完全に制御（読み取り 書き込み）でき、アカウントグループやクラウドアカウントを作成、編集、削除できます。
Cloud Provisioning Admin_NTTCommunications	Account Group Read Only と Cloud Provisioning Admin を組み合わせ、アカウントグループの作成権限を除いたものに対してカスタマイズを加えたものです。 ※本アカウント種類はカスタムで作成したもの

(参考) Prisma Cloud のアカウント種類 (Prisma Cloud デフォルトアカウント種類)

アカウント種類	説明
Account Group Admin	アクセスが許可されているクラウドアカウントおよびアカウントグループのみへの読み取り書き込み権限を保有しています。
Account Group Read Only	Prisma Cloud の指定されたセクションを表示する、読み取り専用権限を保有しています。このロールは、設定を変更する権限を保有していません。

Cloud Provisioning Admin	Prisma Cloud および API からクラウドアカウントのオンボーディングと管理を行う権限を保有しており、アカウントグループを作成、管理できます。
Account and Cloud Provisioning Admin	Account Group Admin と Cloud Provisioning Admin を組み合わせたものです。
Build and Deploy Security	本ロールは、Prisma Cloud Compute で使用されます。

<お客さまの作業申請項目>

- ・ 作業概要：ユーザー追加/ユーザー削除 ※いずれかを選択していただきます
- ・ メールアドレス
- ・ ユーザー姓 ※作業概要としてユーザー追加を選択した場合のみ
- ・ ユーザー名 ※作業概要としてユーザー追加を選択した場合のみ

※1 作業で同時に依頼できるのは5ユーザーまでとさせていただきます

※ ユーザー追加と合わせて、CSP 上での当該ユーザーの承認、(当該ユーザーのメールアドレスのドメインが CSP 上で未登録の場合には) ホワイトリスト登録を実施します

3.6.7. CSPM アラート通知先メールアドレス追加/削除


Prisma Cloud

CSPM 機能の作業依頼です。アカウントグループに対するクラウドアカウントの追加/削除またはアラートルールに対する通知先メールアドレスの追加/削除を行います。

NTT ドコモビジネスの初期設定状態では、アラートルール（とそれにひもづくアカウントグループ）は1つであり、全てのアラートは、あらかじめ申請いただいた3つのメールアドレスに配信されます。但し、「CSPM アラートルール」でクラウドアカウントごとにアラート通知先を分けた場合は、アラートルールは複数存在する為、作業対象のアラートルールを指定いただきます。本設定により、既存のアラート通知対象の変更（クラウドアカウントとメール通知先の追加/削除）が可能です。



(図) アラート通知設定の初期状態



(図) 既存のアラートルールにメールアドレスを追加する場合

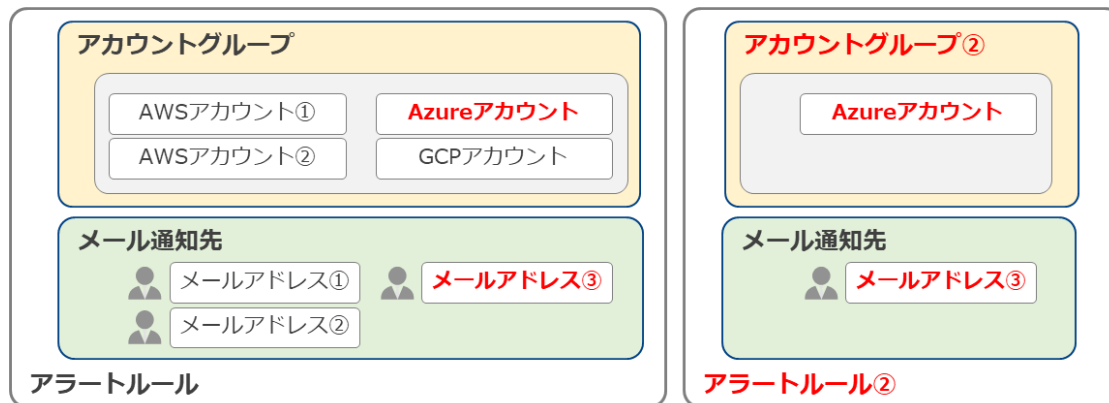
<お客さまの作業申請項目>

- ・作業概要：クラウドアカウント追加/クラウドアカウント削除/メールアドレス追加/メールアドレス削除
※いずれかを選択していただきます
- ・作業対象アカウントグループ
※作業概要としてクラウドアカウント追加またはクラウドアカウント削除を選択した場合のみ
- ・クラウドアカウント名
※作業概要としてクラウドアカウント追加またはクラウドアカウント削除を選択した場合のみ
※指定したいクラウドアカウントが 10 アカウントを超える場合には所定のフォーマット（Excel ファイル）に記入しファイル添付してください
- ・作業対象アラートルール
※作業概要としてメールアドレス追加/メールアドレス削除を選択した場合のみ
- ・メールアドレス ※作業概要としてメールアドレス追加/メールアドレス削除を選択した場合のみ
※1 作業で同時に依頼できるのは 10 メールアドレスまでとさせていただきます

3.6.8. CSPM アラートルール追加

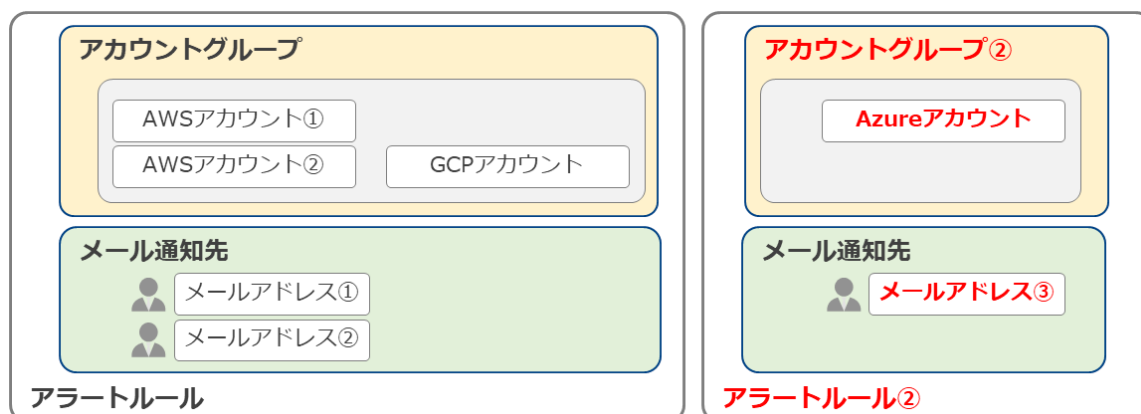
Prisma Cloud

CSPM 機能の作業依頼です。Prisma Cloud からの CSPM 関連アラートの通知先を変更することができます。NTT ドコモビジネスの初期設定状態では、アラートルールは 1 つであり、全てのアラートは、あらかじめ申請いただいた 3 つのメールアドレスに配信されます。しかしながら、クラウドアカウントごとにアラート通知先を分けたい場合は、本設定によりアラートルールを新設することが可能です。また既存のアラートルールの削除も承ります。



(図) 新規のアラートルール②を作成、新規のアカウントグループ②を作成しクラウドアカウントを所属させ、メールアドレスを追加

※単純に追加すると既存アラートルールと、クラウドアカウントおよびメール通知先が一部重複します。



(図) その後既存のアラートルールから、Azureのクラウドアカウントとメールアドレス③を削除（重複がなくなります）

※この作業には、作業依頼「[3.6.7 CSPM アラート通知先メールアドレス追加/削除](#)」の申請をいただく必要があります。

<お客様の作業申請項目>

- ・作業概要：アラートルール追加/アラートルール削除 ※いずれかを選択していただきます
- ・作業対象アラートルール ※作業概要としてアラートルール削除を選択した場合のみ
- ・クラウドアカウント名 ※作業概要としてアラートルール追加を選択した場合のみ
※初期設定時に「nttcomsac-1」という名称で作成しております。アラートルール追加の作業依頼では、「nttcomsac-2」、「nttcomsac-3」というように通番が連番となるように作成します。

※指定したいクラウドアカウントが 10 アカウントを超える場合には所定のフォーマット（Excel ファイル）に記入しファイル添付してください

- ・メールアドレス ※作業概要としてアラートルール追加を選択した場合のみ

※1 作業で同時に依頼できるのは 10 メールアドレスまでとなります

3.6.9. CSPM アノマリ設定変更（しきい値変更）

Prisma Cloud

CSPM 機能の作業依頼です。アノマリ設定のチューニングを実施します。NTT ドコモビジネスの推奨設定では、アラート処理モード=Aggressive、トレーニングモデルしきい値=Medium としています。しかしながら、お客さまの環境において本設定がそぐわない場合は、チューニングを行います。

アノマリの設定は、ネットワーク関連のポリシーが 10 個、UEBA 関連のポリシーが 3 個、DNS 分析関連のポリシーが 2 個、Identity 関連のポリシーが 1 個の合計 16 個のポリシーがあります。（2025 年 4 月現在）

但し、以下は本サービス提供対象外

- ・ DNS 分析
- ・ Identity（IAM セキュリティが無効時）¹⁴

また、基本プラン（Business Edition）の場合、アノマリ設定変更は本サービスの提供対象外となります。（2025 年 4 月現在）

ポリシーにより、アラート処理モード、トレーニングモデルしきい値の両方が設定可能なものと片方のみ設定可能なものがあります。

（参考）アノマリのポリシーごとの設定パラメーター

種別	モード	説明
アラートの処理	Conservative	例) ポートスキャンが 500 ポート以上
	Moderate	例) ポートスキャンが 200 ポート以上
	Aggressive	NTT ドコモビジネス推奨設定。最も敏感に反応する設定。 例) ポートスキャンが 50 ポート以上
トレーニングモデルしきい値	Low	例) 学習期間 7 日

¹⁴ 基本プラン、もしくは CWPP 込みプランだが IAM セキュリティ無効化した場合が該当

	Medium	NTT ドコモビジネス推奨設定。 例) 学習期間 14 日。14 日の間に発生しなかった事象が発生した場合にアラートを上げる。
	High	例) 学習期間 28 日

<お客さまの作業申請項目>

- ・ アノマリポリシー名
- ・ 変更後のアラート処理モード
- ・ 変更後のトレーニングモデルしきい値

※1 作業で同時に依頼できるのは 3 ポリシーまでとさせていただきます

3.6.10. CWPP 脆弱性レポート作成

Prisma Cloud

CWPP 機能の作業依頼です。セキュリティアドバイザリーセンター (SAC) に作業依頼をいただくことで、NTT ドコモビジネスが Prisma Cloud 上で Vulnerability レポートを作成し、カスタマーポータルへアップロードを行います。お客さまは、カスタマーポータルから、レポートを取得することが可能です。

以下のレポートを csv で提供します。

レポートタイプ	Images (Deployed, Registries)	Hosts(Hosts)	Functions(Scanned functions)																																																																																																																																																																		
レポートの内容	Images の脆弱性アラート一覧	Hosts の脆弱性アラート一覧	Serverless Functions で検知した脆弱性アラート一覧																																																																																																																																																																		
レポート形式	CSV	CSV	CSV																																																																																																																																																																		
期間	期間指定不可 (過去分全て表示)	期間指定不可 (過去分全て表示)	期間指定不可 (過去分全て表示)																																																																																																																																																																		
レポート出力内容 (例)	<table border="1"> <thead> <tr> <th>Registry</th> <th>Repository</th> <th>Tag</th> <th>Id</th> <th>Distro</th> <th>Hosts</th> <th>Layer</th> <th>CVE ID</th> <th>Compliance</th> <th>Type</th> <th>Severity</th> <th>Packages</th> <th>Source</th> <th>Package</th> <th>Package</th> <th>CVSS</th> <th>Fix Status</th> <th>Fix Date</th> </tr> </thead> <tbody> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2021</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>15:00.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2020</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>15:00.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2023</td> <td>411</td> <td>binary</td> <td>critical</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>9.8</td> <td>fixed in 1.</td> <td>14:11.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2021</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>15:00.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2021</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>15:00.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2021</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>15:00.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2022</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>15:00.0</td> </tr> <tr> <td>rabbitmq</td> <td>3.9-mana</td> <td>sha256:5f</td> <td>ubuntu-fc</td> <td>LEF-Netskope-sys</td> <td>CVE-2022</td> <td>411</td> <td>binary</td> <td>high</td> <td>go</td> <td>1.13.8</td> <td></td> <td></td> <td></td> <td></td> <td>7.5</td> <td>fixed in 1.</td> <td>12:17.0</td> </tr> </tbody> </table>			Registry	Repository	Tag	Id	Distro	Hosts	Layer	CVE ID	Compliance	Type	Severity	Packages	Source	Package	Package	CVSS	Fix Status	Fix Date	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2020	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2023	411	binary	critical	go	1.13.8					9.8	fixed in 1.	14:11.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2022	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0	rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2022	411	binary	high	go	1.13.8					7.5	fixed in 1.	12:17.0
Registry	Repository	Tag	Id	Distro	Hosts	Layer	CVE ID	Compliance	Type	Severity	Packages	Source	Package	Package	CVSS	Fix Status	Fix Date																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2020	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2023	411	binary	critical	go	1.13.8					9.8	fixed in 1.	14:11.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2021	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2022	411	binary	high	go	1.13.8					7.5	fixed in 1.	15:00.0																																																																																																																																																				
rabbitmq	3.9-mana	sha256:5f	ubuntu-fc	LEF-Netskope-sys	CVE-2022	411	binary	high	go	1.13.8					7.5	fixed in 1.	12:17.0																																																																																																																																																				

3.6.11. CWPP アラートレポート作成

Prisma Cloud

CWPP 機能の作業依頼です。セキュリティアドバイザリーセンター (SAC) に作業依頼をいただくことで、NTT ドコモビジネスが Prisma Cloud 上で Compliance と Runtime レポートを作成し、カスタマーポータルへアップロードを行います。お客さまは、カスタマーポータルから、レポートを取得することが可能です。

以下のレポートを csv で提供します。

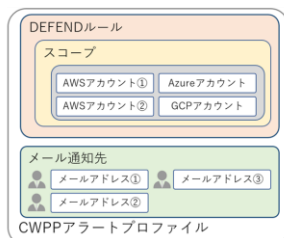
レポートタイプ	Compliance レポート	Runtime レポート																																																															
レポートの内容	Compliance アラート一覧	Runtime の Incident アラート一覧																																																															
レポート形式	CSV	CSV																																																															
期間	期間指定不可 (過去分全て表示)	期間指定不可 (直近 3 ヶ月)																																																															
レポート出力内容 (例)	<table border="1"> <thead> <tr> <th>ID</th> <th>Benchmark ID</th> <th>Regulation</th> <th>Description</th> <th>Severity</th> <th>Category</th> <th>Type</th> <th>Failed res</th> <th>Total resources</th> </tr> </thead> <tbody> <tr> <td>61117</td> <td>CIS_Linux_2.0.0 - 1.1.13</td> <td></td> <td>Ensure separate partition ex</td> <td>medium</td> <td>Linux</td> <td>linux</td> <td>0</td> <td>0</td> </tr> <tr> <td>61613</td> <td>CIS_Linux_2.0.0 - 1.6.2.3</td> <td></td> <td>Ensure SELinux policy is co</td> <td>high</td> <td>Linux</td> <td>linux</td> <td>0</td> <td>16</td> </tr> <tr> <td>6342</td> <td>CIS_Linux_2.0.0 - 3.4.2</td> <td></td> <td>Ensure SCTP is disabled</td> <td>low</td> <td>Linux</td> <td>linux</td> <td>0</td> <td>0</td> </tr> <tr> <td>6616</td> <td>CIS_Linux_2.0.0 - 6.1.6</td> <td></td> <td>Ensure permissions on /etc</td> <td>high</td> <td>Linux</td> <td>linux</td> <td>0</td> <td>16</td> </tr> <tr> <td>215</td> <td>CIS_Docker_v1.5.0 - 7.1</td> <td></td> <td>Do not enable swarm mode</td> <td>high</td> <td>Docker</td> <td>daemon config</td> <td>0</td> <td>16</td> </tr> <tr> <td>216</td> <td>CIS_Docker_v1.5.0 - 7.2</td> <td></td> <td>Control the number of man</td> <td>medium</td> <td>Docker</td> <td>daemon config</td> <td>0</td> <td>0</td> </tr> </tbody> </table>		ID	Benchmark ID	Regulation	Description	Severity	Category	Type	Failed res	Total resources	61117	CIS_Linux_2.0.0 - 1.1.13		Ensure separate partition ex	medium	Linux	linux	0	0	61613	CIS_Linux_2.0.0 - 1.6.2.3		Ensure SELinux policy is co	high	Linux	linux	0	16	6342	CIS_Linux_2.0.0 - 3.4.2		Ensure SCTP is disabled	low	Linux	linux	0	0	6616	CIS_Linux_2.0.0 - 6.1.6		Ensure permissions on /etc	high	Linux	linux	0	16	215	CIS_Docker_v1.5.0 - 7.1		Do not enable swarm mode	high	Docker	daemon config	0	16	216	CIS_Docker_v1.5.0 - 7.2		Control the number of man	medium	Docker	daemon config	0	0
ID	Benchmark ID	Regulation	Description	Severity	Category	Type	Failed res	Total resources																																																									
61117	CIS_Linux_2.0.0 - 1.1.13		Ensure separate partition ex	medium	Linux	linux	0	0																																																									
61613	CIS_Linux_2.0.0 - 1.6.2.3		Ensure SELinux policy is co	high	Linux	linux	0	16																																																									
6342	CIS_Linux_2.0.0 - 3.4.2		Ensure SCTP is disabled	low	Linux	linux	0	0																																																									
6616	CIS_Linux_2.0.0 - 6.1.6		Ensure permissions on /etc	high	Linux	linux	0	16																																																									
215	CIS_Docker_v1.5.0 - 7.1		Do not enable swarm mode	high	Docker	daemon config	0	16																																																									
216	CIS_Docker_v1.5.0 - 7.2		Control the number of man	medium	Docker	daemon config	0	0																																																									

3.6.12. CWPP アラート通知先メールアドレス追加/削除

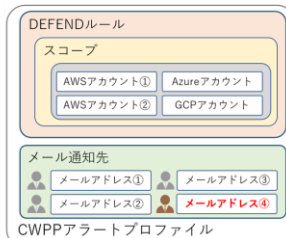
Prisma Cloud

CWPP 機能の作業依頼です。CWPP アラートプロファイルに対する通知先メールアドレスの追加/削除を行います。

NTT ドコモビジネスの初期設定状態では、CWPP アラートプロファイルは 1 つであり、全てのアラートは、あらかじめ申請いただいた 3 つのメールアドレスに配信されます。



(図) アラート通知設定の初期状態



(図) アラートプロファイルにメールアドレスを追加する場合

<お客様の作業申請項目>

- ・作業対象プロファイルネーム：「お客様番号-1」を記載ください。（「お客様番号」は開通案内書に記載しています）
 - ・作業概要：メールアドレス追加/メールアドレス削除 ※いずれかを選択していただきます
 - ・メールアドレス
- ※1 作業で同時に依頼できるのは 10 メールアドレスまでとさせていただきます

3.6.13. IAM セキュリティ 有効化/無効化

Prisma Cloud

IAM セキュリティを有効化/無効化します。

IAM セキュリティは CIEM 機能を提供し、お客様クラウドの ID を可視化し、IAM 監視ポリシーにより権限付与の最小化を行うことで、お客様のクラウドの ID の適切な運用をサポートします。

CWPP 込みプランで申込した場合、NTT ドコモビジネスの初期設定状態では、IAM セキュリティは有効化した状態で提供します。

本機能が不要の場合は作業依頼にて無効化が可能です。

IAM セキュリティを無効化すると、既存の IAM 関連アラートは Resolved にステータス変更されます。

<お客様の作業申請項目>

- ・作業概要：IAM セキュリティ 有効化/無効化 ※いずれかを選択していただきます

3.6.14. 各種カスタマイズ支援

お客様からの各種カスタマイズ支援依頼に対応します。

依頼いただいた作業内容を元に 1pt~10pt から選択していただきます。

作業依頼前に、アドバイザリープラスの TAM に対応実現可否や作業依頼の消費ポイント数をご相談ください。

想定される作業内容は以下

- ・カスタムポリシー検討と作成
- ・ダッシュボードの作成（カスタマイズ）
- ・SSO（シングルサインオン）連携手順書の提供
- ・IaaS 連携

<お客様の作業申請項目>

- 作業概要：1pt～10pt ※作業内容に合わせて、いずれかを選択してください。
- 作業詳細：ご依頼いただいた作業依頼の内容を記載してください。

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。

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。
- リージョンの指定はできず、日本となります。

4. 料金

4.1. サービスの価格

本サービスの料金は、WideAngle マネージド CSPM 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。

本サービスの「利用クレジット/ワークロード課金」の料金は、契約されるクレジット数/ワークロード数 100 クレジット/ワークロード単位に応じて計算します。

5. お申し込み・ご利用

5.1. お申し込み

5.1.1. 申込方法

- 申込内容によって、新設、変更、更新時変更、廃止、簡易変更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/継承等）は、簡易変更申込書で対応します。

申込パターン	備考	申込書
新設	新規で契約する場合 ¹⁵	●
変更	料金変更が発生する以下の契約変更の場合 【ご利用プラン】基本プラン、CWPP 込みプラン： ・クレジット数の追加 ・オプション（作業依頼ポイント追加利用有無）の追加/変更/削除 【ご利用プラン】Cortex Cloud(Posture Security)、Cortex Cloud(Runtime Security)： ・ワークロード数の追加 ・オプション（作業依頼ポイント追加利用有無）の追加/変更/削除	●
更新時変更	契約更新時に契約内容を変更する場合 【ご利用プラン】基本プラン、CWPP 込みプラン： ・クレジット数の追加/削減 ・オプション（作業依頼ポイント追加利用有無）の追加/変更/削除 【ご利用プラン】Cortex Cloud(Posture Security)、Cortex Cloud(Runtime Security)： ・ワークロード数の追加/削減 ・オプション（作業依頼ポイント追加利用有無）の追加/変更/削除	●
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/継承等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	●

¹⁵ 新規の受付はCortex Cloud（Posture Security/ Runtime Security）のみ。（基本プラン、CWPP 込みプランは2026年6月で受付終了）

5.1.2. 申込書

- 申込パターンによって、新設、変更、更新時変更、廃止、簡易変更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
更新時変更	更新時変更申込書
簡易変更	簡易変更申込書
廃止	廃止申込書

5.2. 標準開通日

- 標準開通日は次の日程です。
- 当社が申込を受理し、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	申込項目	標準開通日	備考
新設	「 5.1.1 申込方法 」参照	32 営業日	
廃止	「 5.1.1 申込方法 」参照	15 営業日 ※次回契約更新日の 20 営業日前までの申込にて定期契約満了日に廃止	
変更	「 5.1.1 申込方法 」参照	16 営業日 10 営業日 (オプション (作業依頼ポイント追加利用有無) の追加/変更/削除のみの場合)	翌年の定期契約期間起算日の 36 営業日前から翌年の定期契約期間起算日までは変更申込はできません。更新時変更申込でお申し込みください。
更新時変更	「 5.1.1 申込方法 」参照	次回契約更新日の 20 営業日前までの申込にて翌年の定期契約期間起算日に変更	

簡易変更	「5.1.1 申込方法」参照	15 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。
------	----------------	----------------	---

5.3. 開通案内・配布同梱物

- 新設申し込み、変更申し込み、更新時変更申し込みの場合に開通案内を発行します。
- 自動更新、廃止申し込み、簡易変更申し込みの場合は開通案内等は発行しません。
- 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」	更新時変更 「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	●	-	-

5.4. お問い合わせ受付

- セキュリティアドバイザーセンターにて、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 運用受付	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	<ul style="list-style-type: none"> • 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 • その他次項記載の運用に関するお 問い合わせ • [基本プランのみ]Prisma Cloud Business Edition（CSPM 機能） 製品に関するお問い合わせ • [CWPP 込みプランのみ]Prisma Cloud Enterprise Edition （CSPM 機能+CWPP 機能 +CIEM 機能） 製品に関するお問い合わせ • [Cortex Cloud(Posture Security)のみ]Cortex Cloud Posture Security（CSPM 機能+ CIEM 機能） 製品に関するお問い合わせ • [Cortex Cloud(Runtime Security)のみ]Cortex Cloud Runtime Security（CSPM 機能 +CWPP 機能+CIEM 機能） 製品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あります。

5.5. 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	<ul style="list-style-type: none"> カスタマーポータルの故障に関するお問い合わせ [基本プランのみ]CSPM 機能の製品故障に関するお問い合わせ [CWPP 込みプランのみ]CSPM 機能+CWPP 機能+CIEM 機能の製品故障に関するお問い合わせ [Cortex Cloud(Posture Security)のみ]CSPM 機能+CIEM 機能の製品故障に関するお問い合わせ [Cortex Cloud(Runtime Security)のみ]CSPM 機能+CWPP 機能+CIEM 機能の製品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あります。

5.6. お問い合わせ受付・運用受付/通知方法

- 作業依頼受付、月次レポート送付、お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
作業依頼	<ul style="list-style-type: none"> カスタマーポータルの「作業依頼」から申請いただき、SAC 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。

	<ul style="list-style-type: none"> ・「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。
月次レポート	<ul style="list-style-type: none"> ・毎月 15 日（営業日外の場合は翌営業日）までにカスタマーポータル「ケース」（カテゴリ「月次レポート」）にアップされ、通知されます。
お問い合わせ	<ul style="list-style-type: none"> ・お客さまからのお問い合わせは、カスタマーポータル「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、SAC から回答をします。
アラートに関するお問い合わせ	<ul style="list-style-type: none"> ・お客さまからのアラートに関するお問い合わせは、カスタマーポータル「お問い合わせ」よりお客さまにて「アラートについて」を選択し、ケース起票、お問い合わせ内容を入力いただき、SAC から回答をします。
<p>[基本プランのみ]</p> <p>Prisma Cloud（CSPM 機能）に関するお問い合わせ、製品故障お問い合わせ</p> <p>[CWPP 込みプランのみ]</p> <p>Prisma Cloud（CSPM 機能+CWPP 機能+CIEM 機能）に関するお問い合わせ、製品故障お問い合わせ</p> <p>[Cortex Cloud(Posture Security)]</p> <p>Cortex Cloud（CSPM 機能+CIEM 機能）に関するお問い合わせ、製品故障お問い合わせ</p> <p>[Cortex Cloud(Runtime Security)]</p> <p>Cortex Cloud（CSPM 機能+CWPP 機能+CIEM 機能）に関するお問い合わせ、製品故障お問い合わせ</p>	<ul style="list-style-type: none"> ・ Prisma Cloud（CSPM 機能）または（CSPM 機能+CWPP 機能+CIEM 機能）、Cortex Cloud（CSPM 機能+CIEM 機能）、Cortex Cloud（CSPM 機能+CWPP 機能+CIEM 機能）に関するお問い合わせは、カスタマーポータル「お問い合わせ」よりお客さまにて「製品仕様について」を選択し、ケース起票、お問い合わせ内容を入力いただき、SAC から回答をします。 ・ Prisma Cloud/Cortex Cloud の製品故障に関するお問い合わせは、カスタマーポータル「お問い合わせ」よりお客さまにて「故障について」を選択し、ケース起票、お問い合わせ内容を入力いただき、SAC から回答をします。

5.7. 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) 工事タイミングの分類に関する定義

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。計画された「メンテナンス」は目標信頼性の稼働率を計算するときに除外します。
- 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等の修正を行います。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、パッチ適用等の対処を行います。
- 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 か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/Prisma Cloud/Cortex Cloud）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。

(2) 工事通知（メンテナンス通知）

① Prisma Cloud/Cortex Cloud 工事通知

- Prisma Cloud/Cortex Cloud のメンテナンス情報は、Palo Alto Networks 社の Status サイト (<https://status.paloaltonetworks.com/>) にて周知されます。Prisma Cloud/Cortex Cloud の工事通知・故障通知を受領されたいお客さまは、Palo Alto Networks 社の Status サイトよりメール通知受信をご登録ください。登録すると、メールにて Palo Alto Networks 社からメンテナンス情報・故障情報が通知されます。登録の手順は次項の参考を参照してください。

② ServiceNow（カスタマーポータル）工事通知

- 計画メンテナンスの場合は、通常 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。
- 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。（ServiceNow の脆弱性対応等のカスタマーポータル閉塞を伴う作業については、ポータル故障として NTT ドコモビジネスお客さまサポートで故障通知します。）

5.8. 故障通知

故障の通知は、NTT ドコモビジネスお客さまサポートに掲載します。（お客さまが NTT ドコモビジネスお客さまサポートにてメール通知登録された場合は、掲載時にメール通知されます。）

本故障の通知には、Prisma Cloud/Cortex Cloud の故障の通知は含まれません。Prisma Cloud/Cortex Cloud の故障情報は、Palo Alto Networks 社の Status サイト (<https://status.paloaltonetworks.com/>) にて周知されます。

Prisma Cloud/Cortex Cloud の工事通知・故障通知を受領されたいお客さまは、Palo Alto Networks 社の Status サイトよりメール通知受信をご登録ください。

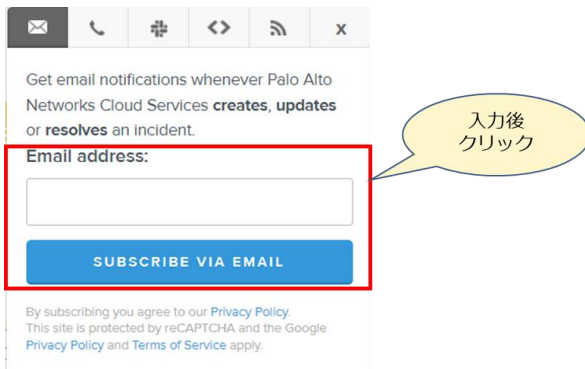
登録すると、メールにて Palo Alto Networks 社からメンテナンス情報・故障情報が通知されます。登録の手順は次項の参考を参照してください。

【参考】 Palo Alto Networks 社の Status サイトからの Prisma Cloud/Cortex Cloud メール通知受信設定方法

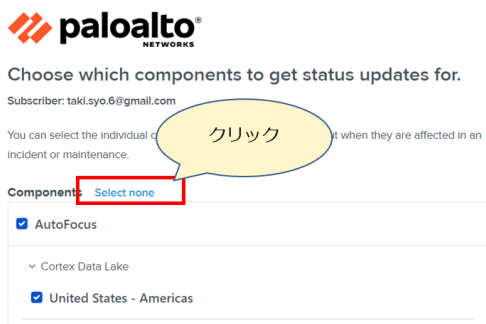
STEP1 : 「<https://status.paloaltonetworks.com/>」へアクセスし、ページ上部の「SUBSCRIBE TO UPDATES」をクリックします。



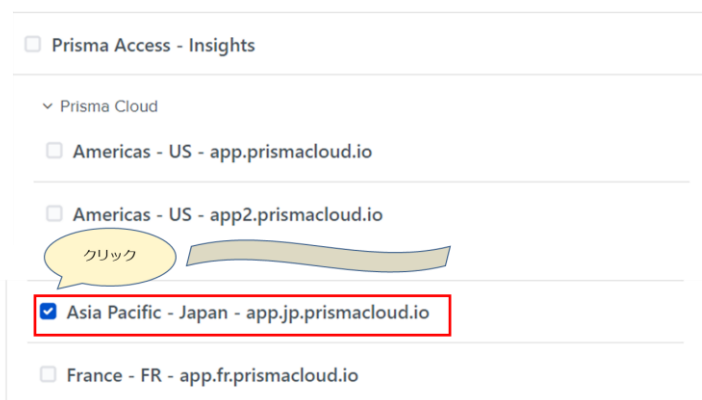
STEP2 : 通知を受け取りたいメールアドレスを入力し、「SUBSCRIBE VIA EMAIL」をクリックします。



STEP3 : 「Select none」 をクリックして、通知対象の Components を全てクリアします。



STEP4 : 「Asia Pacific - Japan - app.jp.prismacloud.io」 にチェックをいれます。



Cortex Cloud の場合は「Cortex Gateway」 > 「Cortex Cloud」
エリアの「Japan」を選択してください。

Components [Select all](#)

<input type="checkbox"/> AutoFocus
<input checked="" type="checkbox"/> Cortex Gateway
▼ Cortex Cloud
<input type="checkbox"/> Australia
<input type="checkbox"/> Canada
<input type="checkbox"/> Germany
<input type="checkbox"/> India
<input checked="" type="checkbox"/> Japan

クリック

STEP5 : ページ下部の「SAVE」 ボタンをクリックします。

<input type="checkbox"/> Threat Vault

Cancel

クリック

6. お問い合わせ連絡先

本サービスのお問い合わせについては、ベストエフォートで対応しており、お問い合わせ内容により、翌営業日対応となることがあります。

内容	受付窓口	連絡先	受付時間
ご利用開始前のサービスのお問い合わせ	営業担当	-	-
ご利用開始後のサービスのお問い合わせ	セキュリティアドバイザー	カスタマーポータル https://nttcomsac.service-now.com/cs	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
料金に関するお問い合わせ	Billingカスタマセンタ	電話：0120-047-128 URL： https://www.ntt.com/b-charge	URL 受付：24時間 365日 対応時間：平日（年末年始除く）9:00～17:00

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

- 「Palo Alto Networks End User Agreement」とは Prisma Cloud/Cortex Cloud で定める End User Agreement のことをいい、契約者は本サービスのうち、Prisma Cloud/Cortex Cloud の利用にあたり、Palo Alto Networks, Inc と直接 End User Agreement に基づき契約を締結するものとしてします。

Prisma Cloud/Cortex Cloud に関して、本規約に定めていない提供条件については、Palo Alto Networks End User Agreement の定めるところによります。

なお、Palo Alto Networks, Inc は、Prisma Cloud/Cortex Cloud の変更ならびに適用される法律の変更に伴い、Palo Alto Networks End User Agreement を適宜変更することができるものとし、Prisma Cloud/Cortex Cloud に関して本規約に特段の定めがない限り、Palo Alto Networks End User Agreement を適用されるものとしてします。

URL:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-end-user-license-agreement-eula.pdf

- 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

- お客さまのクラウド環境と Prisma Cloud/Cortex Cloud 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 料金を含む）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. 定期契約期間について

- 定期契約期間があります。
- 定期契約期間は、サービスの提供を開始した日を起算日（以下「定期契約期間起算日」）とし、定期契約期間起算日から1年とします。翌年の定期契約期間起算日の前日を「定期契約期間満了日」といいます。
- 定期契約期間は、規定する日（翌年の定期契約期間起算日の20営業日前）までに契約解約またはクレジット/ワークロードの数量の減少の申出がない場合、同一条件で1定期契約期間延長することとし、以後これに準じて取り扱います。定期契約期間満了日に合わせて当社から契約者へ更新の依頼や更新の通知はいたしません。
- Prisma Cloudにて、本契約の定期契約期間中にクレジットを追加する場合、個別調整が必要となるため事前に連絡をお願いします。
- Cortex Cloudにて、本契約の定期契約期間中にワークロードを追加する場合、その追加する契約の契約期間満了日は定期契約期間起算日に定めた定期契約期間満了日と同じとします。
- 定期契約期間内に契約を解約される場合は、解約があった日から定期契約期間満了日までの期間に相当する本サービスの利用料金を一括してお支払いいただきます。
- 本契約の解約またはクレジット数/ワークロード数の減少変更を希望される場合は、解約またはクレジット数/ワークロード数の減少変更しようとする定期契約期間満了日の指定する日（翌年の定期契約期間起算日の20営業日前）の前までに本契約の解約またはクレジット数/ワークロード数の減少変更についてお申し込みいただきます。

なお、定期契約期間中は、クレジット/ワークロードの数の減少はできません。クレジット/ワークロードの数の減少は、次の定期契約期間起算日から適用とします。

7.1.5. 最低利用期間

- 最低利用期間は、定期契約期間とします。
オプションについては最低利用期間はありません。
- 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。

7.1.6. 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。
- 当社は契約者からサービスの申し込みがあった時点で Palo Alto Networks 社に定期契約期間中の Prisma Cloud/Cortex Cloud の手配を一括して行うことから、契約者が、契約の取り消しを定期契約期間起算日の前までに行った場合は、料金表に規定する定期契約期間内の料金の支払いを要します。

7.1.7. 提供中止

- 当社は、災害・広域停電・インターネット障害・パンデミック等の事態が発生し、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、Prisma Cloud/Cortex Cloud、またはお客さま IaaS が故障した場合、当社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。

7.1.8. 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等、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。

7.1.9. 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、当社は契約を解除することがあります。

7.1.10. 免責

- 当社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、当社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します。
- 当社は、本規約の変更等により契約者が本サービスを利用するにあたり当社が提供することとなっている設備、端末等以外の設備、端末等の改造または変更（以下、この条において「改造等」といいます。）を要する場合であっても、その改造等に要する費用については負担しません。
- 当社は、本サービスが日本国外の地域の規制（法令、規則、政府ガイドライン等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等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当社は責任を負いません。
- Prisma Cloud/Cortex Cloud に起因する損害については、契約者と Palo Alto Networks 社との間で締結される End User Agreement のみで保障されるものとし、当社は責任を負いません。
- 契約者自身で、Cortex Cloud 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。（当社が初期設定を行ったポリシー定義の削除などを含みますがこれに限りません。）
- 上記の場合、設定等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。また当社側での再設定が必要となった場合には、別途費用を請求させていただく場合があります。

7.1.11. 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します。
- 各種レポート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当社から通知は致しません。
- カスタマーポータルのお知らせは、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。
- 月次レポートはご利用開始日の翌月以降からの提供となります。本サービスを廃止される場合は、廃止日のタイミングにより、最終の月次レポートの提供タイミング、記載される運用状況の期間が異なります。
- 違約金発生期間は、当該契約のご利用開始日から起算し、定期契約期間の更新により更新されます。
- 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。あらかじめご了承ください。
- 弊社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等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。
- お客さまの IaaS、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、および設定等については、お受けできません。
- Prisma Cloud/Cortex Cloud および、NTT ドコモビジネスが提示する、各種レポート、推奨設定等は、お客さまの IT 環境を熟知したものではありません。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。
- Prisma Cloud に対して、お客さまご自身で検知ポリシーの追加や編集は実施できません。
- Prisma Cloud に対して、お客さまからのご要望に基づいた検知ポリシーの追加や編集は実施いたしません。
- Prisma Cloud/Cortex Cloud に対して、その稼働状況の監視は実施いたしません。
- Prisma Cloud/Cortex Cloud に、NTT ドコモビジネス、および提携事業者のオペレーターや、エンジニアがアクセスする場合があります。
- Prisma Cloud/Cortex Cloud 製品についてのお問い合わせ回答内容は、Prisma Cloud/Cortex Cloud 製品仕様上における情報となり、各お客さま IaaS 環境を全て考慮した内容であることを保証するものではありません。
- Prisma Cloud/Cortex Cloud 検知結果に対する推奨修正内容は、お客さま IaaS 環境設定におけるセキュリティ改善・向上の可能性を示唆するものとなり、セキュリティ事故の予防を保証するもので

はありません。また、各お客さま IaaS 環境を全て考慮した内容であることを保証するものではありません。

- Prisma Cloud/Cortex Cloud のご利用については、Palo Alto Networks 社の以下の資料もご確認ください。

- Service Level Agreement (Prisma Cloud)

- <https://www.paloaltonetworks.com/resources/datasheets/prisma-cloud-service-level-agreement>

- Privacy Data Sheet (Prisma Cloud)

- <https://www.paloaltonetworks.com/resources/datasheets/prisma-cloud-privacy>

- Service Level Agreement (Cortex Cloud)

- https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/cortex-service-level-agreement.pdf

- Privacy Data Sheet (Cortex Cloud)

- <https://www.paloaltonetworks.com/resources/datasheets/cortex-cloud-privacy-datasheet>

- 本サービスを廃止される場合には、廃止日以降に Prisma Cloud 上でクラウドアカウントの削除を実施していただくことをお勧めします。Prisma Cloud 上でのクラウドアカウント削除を実施していないと、別の Prisma Cloud との連携が必要になった際に連携が出来ない可能性があります。Prisma Cloud 上からクラウドアカウント削除を実施するための手順については、カスタマーポータルに掲載されている「**WideAngle マネージド CSPM_Prisma Cloud クラウドアカウント削除ガイド**」をご参照ください。

Cortex Cloud は、Cortex Cloud 上でのクラウドアカウント削除を実施していなくとも別の Cortex Cloud との連携が可能であるため、削除いただく必要はありません。

- 管理者ユーザー追加後に、Palo Alto Networks 社から送られる「Welcome to Palo Alto Networks!」メールのアクティベーションリンクの有効期限は 7 日間となります。期限切れによる再有効化は Palo Alto Networks 社のみ対応可能なため、相応の時間を要します。
- 過去作成済ユーザーにおいても、以下ケースのどちらかに該当する場合、非アクティブ状態になり、同様の対応が必要となります。

- ・過去 2 年間ログインの試行が実施されていない。

- ・ユーザー作成から 6 か月間ログインされていない。

また、非アクティブ状態では PW リセットも実施できません。

- Prisma Cloud は、ライセンス期限の 90 日後に全データが自動的に削除されます。

Cortex Cloud は、ライセンス期限後の 31~180 日の間に全データが自動的に削除されます。

- 契約期間中にサービス廃止を行った場合はライセンス期限まで Prisma Cloud/Cortex Cloud を利用可能な状態となりますが、契約終了後に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。
- 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。
- お客さまご自身で、Cortex Cloud の本サービス提供範囲外の機能を有効化または設定を変更することにより、ワークロード数が増加する可能性があります。
- メーカーにより更新されたポリシーは定期的にサービスとして適用されます。

改訂履歴

バージョン	主な変更	日付
1.00	・初版発行	2022年12月23日
1.01	<ul style="list-style-type: none"> ・ Prisma Cloud の Severity 変更対応 ・ Prisma Cloud のメンテナンス関連通知に関するサービス仕様および運用プロセスの変更 ・ Prisma Cloud のお客さま管理者のロール設定 ・ 作業依頼の作業希望日の廃止 	2023年5月31日
1.02	<ul style="list-style-type: none"> ・ Prisma Cloud の Severity 変更対応 ・ Prisma Cloud のメンテナンス関連通知に関するサービス仕様および運用プロセスの変更 	2023年6月7日
1.03	<ul style="list-style-type: none"> ・ 管理者ユーザー追加に伴うアクティベーションリンクの有効期間と期限切れの対応を明記 ・ 誤記修正 	2023年7月19日
1.04	<ul style="list-style-type: none"> ・ Prisma Cloud のライセンス体系変更に伴う修正 ・ クレジットの算出方法を明記 ・ サービス提供範囲外の明記 ・ カスタマーポータル故障時の問い合わせ受付修正 ・ 月次レポートの作成日指定不可、作成データ期間を明記 ・ 検知ポリシーの追加・編集不可を明記 ・ 提携事業者保守用の連絡先変更 	2023年8月30日
2.00	・ CWPP のマネージド提供に伴う修正	2023年10月2日
2.01	<ul style="list-style-type: none"> ・ Prisma Cloud とカスタマーポータルの連携停止 ・ カスタム権限グループの修正 ・ 作業依頼「CSPM コンプライアンスレポート作成」の項目追加 ・ 作業依頼「CSPM アラートルール追加」のアラートルール名の明記 ・ アノマリ設定のポリシー追加 	2023年11月8日
2.02	<ul style="list-style-type: none"> ・ Prisma Cloud のログ保管期間の修正 ・ コードセキュリティに注釈追加 ・ 「NTT Com 指定休業日」の明示化 ・ Prisma Cloud UI 変更 (Darwin) 	2024年1月24日
2.03	<ul style="list-style-type: none"> ・ IAM セキュリティ追加に伴う修正 ・ 開通案内の送信元メールアドレス修正 	2024年3月27日
2.04	<ul style="list-style-type: none"> ・ 関連文書などのドキュメント名の修正 ・ アノマリ設定変更の修正 	2024年5月22日
2.05	・ ドキュメント名の変更	2024年9月18日

	<ul style="list-style-type: none"> ・ Prisma Cloud 製品の初期設定にユーザーを追加 ・ Business Edition ガイドの更新に伴い修正 	
2.06	<ul style="list-style-type: none"> ・ 「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 ・ カテゴリー1 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、カテゴリー2 の標準開通日を修正 ・ 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
2.07	<ul style="list-style-type: none"> ・ Business Edition の制約事項追加 ・ フローログの保持期間の変更 	2025 年 5 月 21 日
2.08	<ul style="list-style-type: none"> ・ Business Edition の制約事項修正 	2025 年 7 月 30 日
2.09	<ul style="list-style-type: none"> ・ NTT コミュニケーションズから NTT ドコモビジネスへの社名・略称・ロゴ・コピーライト変更対応 ・ 正常性確認の廃止に伴う記載の削除 	2025 年 12 月 1 日
2.10	<ul style="list-style-type: none"> ・ ユーザー追加時の CSP 上での承認対応に伴う修正 ・ ESC 通知対応に伴う修正 3.3.7. Prisma Cloud のログイン/認証/権限 3.5.3. Prisma Cloud 製品の初期設定 3.6.6. ユーザー追加/削除 	2025 年 12 月 25 日
2.11	<ul style="list-style-type: none"> ・ PrismaCloud の監査ログ保持期間変更に伴う修正 3.3.12. Prisma Cloud のログ保管期間 	2026 年 4 月 30 日
3.00	<ul style="list-style-type: none"> ・ Cortex Cloud のマネージド提供に伴う修正 1.2. 関連文書 1.3. 用語の定義 2.1. CSPM/CWPP/CIEM とは 2.2. サービス概要 3.1. 提供区分 3.2. 提供メニュー 3.3. 提供条件 3.4. 提供機能一覧 3.5. 提供機能（基本機能） 3.6. 提供機能（作業依頼機能） 3.8. 提供地域 4.1. サービスの価格 5.1. お申し込み 5.2. 標準開通日 5.3. 開通案内・配布同梱物 5.4. お問い合わせ受付 	2026 年 6 月 22 日

	5.5. 故障受付	
	5.6. お問い合わせ受付・運用受付/通知方法	
	5.7. 工事通知（メンテナンス通知）	
	5.8. 故障通知	
	7.1. 重要説明事項	
	7.2. 留意事項	