ＣＳＰサイバーガード
サービス仕様書

第 1.2 版
発行年月日　2022 年 01 月 12 日

ＣＳＰ

セントラル警備保障株式会社

目次

1.　本サービス仕様書について

「ＣＳＰサイバーガードサービス仕様書」（以下「本サービス仕様書」といいます）の目的および用語の定義について記述します。

1.1.　本サービス仕様書の目的

本サービス仕様書は、セントラル警備保障株式会社（以下「ＣＳＰ」といいます）が、ＣＳＰサイバーガード（以下「本サービス」といいます）をお客様に提供するにあたり、ＣＳＰのホームページに掲出してサービス内容を周知するものであり、契約申し込み前、並びに契約期間中にその内容を確認できるよう定めたものです。

1.2.　本サービス仕様書の変更

本サービス仕様書は、「ＣＳＰサイバーガード契約約款」（以下「本約款」といいます）第３条第２項の定めにより、適宜、改定されるものとし、改定時には最新の内容が適用されます。改定にあたり、ＣＳＰは、お客様にＣＳＰのホームページへの掲出によりその変更内容を通知することとします。その変更された本サービス仕様書の効力は、ＣＳＰのホームページに変更後の本サービス仕様書を掲載後 14 日経過した日から有効になるものとします。お客様は、本サービスを利用する際、ＣＳＰから提供またはＣＳＰのホームページに掲載されている最新の本サービス仕様書をご確認いただくものとします。お客様が、本サービス仕様書の変更の効力が生じた後に本サービスを利用した場合には、本サービス仕様書変更後のすべての記載内容に同意したものとみなされます。

1.3.　用語・略語の定義

本サービス仕様書で使用する用語・略語の意味は、以下に定めるとおりとします。なお、本サービス仕様書において明示的に定めのない、その他の用語は本約款の定めに従うものとします。

表 1-1　本仕様書にて定義する本サービス固有の用語

用語・略語	説明
ＣＳＰ	セントラル警備保障株式会社および同社の指定する会社
ＮＥＣ	日本電気株式会社および同社の指定する会社
お客様	ＣＳＰと契約して本サービスを利用する法人もしくは個人事業主またはその管理者
サービス利用者	お客様がネットワークへの接続により本サービスの利用を認めた個人
本サービス	ＣＳＰが提供する「ＣＳＰサイバーガード」
本システム	ＮＥＣが提供するクラウド上のサイバーセキュリティ監視システム
ＵＴＭ装置	お客様のネットワーク環境に設置するＮＥＣプラットフォームズ製造の統合脅威管理（Unified Threat Management）装置
セキュリティサービスポータル	お客様が、本サービスの監視状況の確認や、各種手続きを行う Web サイト
アラート	ＵＴＭ装置が検知したセキュリティ上の脅威
重要アラート	お客様に通知する必要があるとＮＥＣが判断したアラート
★★★アラート	重要度が「 ★★★(高)」の重要アラート。簡易サイバー保険の発動対象となる。
通知先メールアドレス	重要アラート検知やＵＴＭ装置の停止、ファームウエアの更新等の通知先として登録されたメールアドレス
相談窓口	ＵＴＭ装置の設置・撤去やセキュリティサービスポータル、重要アラート、簡易サイバー保険についてのお客様の問い合わせを受け付ける窓口
営業日	土曜日、日曜日、国民の祝日に関する法律に定める休日、およびＣＳＰ並びにＮＥＣ所定の休日を除く日。
相談窓口営業日	土曜日、日曜日、国民の祝日に関する法律に定める休日および年末年始の休日を除く日。
本契約	本サービスの提供のため、お客様とＣＳＰがＵＴＭ装置ごとに締結する契約
契約申請日	ＣＳＰがＮＥＣに利用を申請した日（お客様の申込の翌日以降となる場合がある）
契約開始日	契約申請日の翌月１日（契約申請日が各月１日から５日までの場合に限り、契約申請日とすることができる）。
有償期間開始日	契約開始日の翌月１日

2.　サービス概要

2.1.　本サービスの概要

本サービスは、お客様のイントラネットとインターネットの境界点にＵＴＭ装置を設置して、通信に含まれる脅威を監視します。サイバー攻撃の脅威を検知した際には、不正通信の遮断や有害ファイルの無害化を行います。また、フィッシングサイトや閲覧によってマルウェア感染を起こす有害な Web サイトへのアクセスも遮断します（すべての脅威や有害ファイル、有害な Web サイトへのアクセスの検知を保証するものではありません。）。アラート検知情報はセキュリティサービスポータルでご確認いただけるとともに、重要アラートについてはメールで通知します。※１※２

脅威の監視や通信の遮断などの処理はＵＴＭ装置内部で行われ、サービス利用者所有のファイル、メール本文といったサービス利用者所有のデータは送信されませんが、ＵＴＭ装置でアラートを検知した通信の通信元/通信先の端末 IP アドレス、MAC アドレス、サービス利用者がアクセスした URL およびウイルスファイル名といったアラート検知の判断根拠となった情報が検知結果としてサイバーセキュリティ見守りシステムに送信されます。

本サービスは、ご利用環境におけるアラート検知の実態をご確認いただき、セキュリティ意識の強化、施策の追加などお客様ごとの取り組みにお役立ていただくことを目的とした多数のお客様向けのクラウドサービスです。　※３

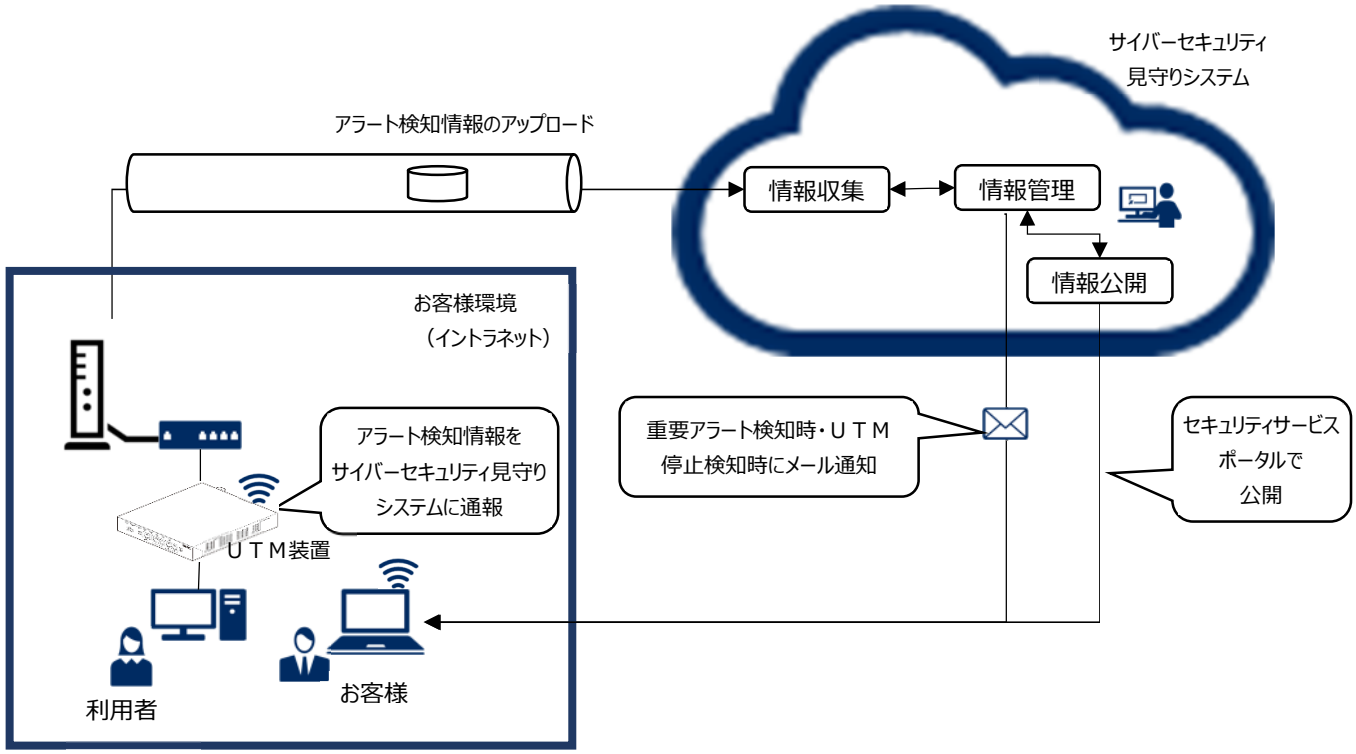


図 2-1　サービス提供イメージ

ご利用前にご確認ください。

※１　本サービスではお客様のネットワーク環境にＵＴＭ装置を適切に設置いただくことが前提のサービスです。このため事前に、「６．ご利用に必要な環境」で設置可能かどうかをお客様にてご判断の上、ご利用を申請いただく必要があります。

※２　一部重要アラートと判断したものをお客様利便性の改善のためにメールで通知いたしますが、いかなる場合にもＣＳＰは、重要性の判断の適確性の保証を行いません。

※３　本サービス仕様書に実質的に適う範囲でＣＳＰ都合により細部の仕様を予告なく変更する場合があります。本サービスは多数のお客様向けに共通的に提供することを想定しており、個別のお客様の目的達成を保証するものではありません。

2.2. 本サービスを構成するシステム

本サービスは、ＮＥＣからお客様に貸し出されるＵＴＭ装置と、ＮＥＣのサイバーセキュリティ見守りシステムから構成されます。本サービスの稼働はこれら要素の稼働の影響を受けるほか、お客様にて用意される接続回線の影響を受けます。

2.2.1. ＵＴＭ装置

ＵＴＭ装置はお客様ネットワーク環境に設置してお客様ネットワーク上の機器を脅威から守るための装置で、各お客様に占有・管理していただきます。ＵＴＭ装置の使用上の注意は「ＵＴＭ取扱説明書」をご参照ください。

2.2.2. サイバーセキュリティ見守りシステム

本システムは他のお客様と共用のサーバー・ネットワーク機器を組み合わせてサービス環境を構築し、提供しております。本システムは、特に重要となる箇所については冗長化を行っているほか、主にサーバー等における OS、および各種ソフトウェアの不具合修正を目的とした修正パッチは必要性を判断の上、適宜適用し、サービスの提供を行う上で健全な状態を維持します。なお、本システムは日本国内外のデータセンタ内に構築等をしておりますが、ディザスタリカバリ（Disaster Recovery）として、遠隔地かつ複数のデータセンタを用いたサービス環境での提供は行っておりません。

2.3. 本サービスに付帯する「駆けつけサービス」

本サービスには、お客様の実施するウイルス除去などの作業をサポートする「駆けつけサービス」が付帯されています。詳細は「3.5 駆けつけサービス」と「別紙１：駆けつけサービス」をご参照ください。

2.4. 本サービスに付帯する「簡易サイバー保険」

本サービスには専用の「簡易サイバー保険」（以下「簡易サイバー保険」または「保険」といいます）が付帯されています。保険の詳細、補償内容、保険請求に関する手続きは、「3.6 簡易サイバー保険」と別紙の「別紙２：簡易サイバー保険規約」をご参照ください。

3. サービス内容

本サービスは、ＵＴＭ装置に接続される端末、モバイルデバイス等の機器とインターネットとの通信を監視し、重要アラートを検知した場合は通知先メールアドレスに通知します。重要アラート以外のアラートについてはセキュリティサービスポータルからご確認いただくことが可能です。

3.1. 見守りサービス（脅威検知・防御機能）

Web ブラウザやアプリケーション等が行う通信を監視し、サイバー攻撃の脅威を検知した際には通信の遮断や有害ファイルの無害化を行います。フィッシングサイトや閲覧によってマルウェア感染を起こす有害な Web サイトへのアクセスも遮断します。また重要アラートと判断した場合は通知先メールアドレスに通知します。なお、すべての脅威や有害ファイル、有害な Web サイトへのアクセスの検知、防御を保証するものではありません。

3.2. 見守りサービス（インターネットアクセスやアプリケーション通信の記録機能）

Web ブラウザやアプリケーション等が行う通信を監視し、あらかじめ用意されている Web カテゴリやアプリケーション種別に該当するものをセキュリティサービスポータルで表示します。

3.3. お知らせサービス

(1) 重要アラート通知

・本サービスは、お客様環境のパソコン、モバイルデバイス等の機器について「3.1 見守りサービス（見守りサービス（脅威検知・防御機能）」に記載のように通信データをチェックし、特に重要性が高いと判断したケースについて重要アラートとして通知先メールアドレスに通知メールを送信します。

・通知メールのタイトルおよび本文には重要度を表す★が記載されます。★の定義は以下となります。

重要度: ★★★(高)・・・マルウェアに感染している可能性が高く、ウイルス対策ソフトでフルスキャンを強く推奨するもの（★★★アラート）

重要度: ★★☆(中)・・・マルウェアに感染している可能性があり、ウイルス対策ソフトでフルスキャンを推奨するもの

重要度: ★☆☆(低)・・・マルウェアに感染している可能性は低いが、セキュリティ上の注意を促すもの

調査中または記載なし・・・マルウェアに感染しているか調査中のもの。通知メールの本文に「※調査中※」と表示される。。

※複数の重要アラートを検知した場合は、1 つの通知メールでまとめて送信します。その際のタイトルには最も重要度が高いものの重要度（★）が設定されます。

・通知メールの本文に必要な作業が記載されている場合は、記載内容に従って作業を実施してください。

・通知メールの本文に「※調査中※」が含まれる場合があります。この場合、調査完了後に調査結果報告を通知先メールアドレスに送信します。

・通知先メールアドレスは３つまで指定可能です。

(2) ＵＴＭ装置稼働停止通知

・本サービスでは、お客様環境に設置されたＵＴＭ装置の稼働状況を監視し、停止状態と判断した場合は、通知先メールアドレスに通知します。

・初回の停止検知以降は日次で定時に確認し、停止状態から復旧していないと判断された場合は、再度通知します。

・初回の停止検知によるメール通知が、日次の定時確認時刻に近い場合は、メールが続けて複数届く場合があります。

(3) 制限事項

・メールでの通知は、24 時間自動的に送信されます。このため、メールを携帯、スマートフォンに転送設定されている場合、夜間であってもメール受信されますのでご注意ください。

・メールでの通知は、その性格上、到着の保証はできかねます。

・重要アラートの通知については、いかなる場合にもＣＳＰは、重要性の判断の適確性の保証を行いません。

3.4. セキュリティサービスポータルでの情報提供

ＵＴＭが収集した情報は、セキュリティサービスポータルから確認することができます。詳細は「セキュリティサービスポータル利用マニュアル」をご参照ください。

3.5. 駆けつけサービス

重要アラートが発生した際には、お客様の要請によりＣＳＰが駆けつけてサポートすることができます。この駆けつけサービスは有償となりますが、「簡易サイバー保険」により費用を賄われる場合があります。なお、駆けつけサービスは、お客様の実施するウイルス除去などの作業をサポートするものであって、作業結果を保証するものではありません。詳細は「別紙１：駆けつけサービス」をご参照ください。

3.6. 簡易サイバー保険

★★★アラートを検知した場合、原則としてお客様がウイルス対策ソフトでフルスキャンを実施することを条件に、本サービスに付帯する保険により駆けつけサービス費用が賄われる場合があります。具体的な補償発動条件や保険金請求/支払いフローなどは、「別紙 2：簡易サイバー保険規約」をご参照ください。なお、保険金は、駆けつけサービスを行ったＣＳＰに直接支払われ、お客様に支払われることはありません。

保険の補償発動には★★★アラートの通知メールの受信が必要です。通知メールをお客様が受信するためには、ＵＴＭ装置の設置が完了し、セキュリティサービスポータルで該当のＵＴＭ装置の状態がオンライン状態で、ログが表示される状況である必要があります。

なお、重要度が「★★☆（中）」の場合でも、ウイルス対策ソフトによるフルスキャンの実行結果により、補償発動の対象となる場合があります。実行結果を相談窓口宛にお送りいただき、★★★アラート相当と判断できた場合は、あらためて★★★アラートの通知メールをお送りします。

4. お客様サポート

4.1. 相談受付サービス

「別紙３：相談窓口」 をご参照ください。

4.2. サービスのメンテナンス通知

・計画的なサービスのメンテナンス

計画的なサービスの停止を行う場合は、原則１か月以上前にセキュリティサービスポータルに案内を掲載いたします。

・緊急メンテナンス

本サービスの品質を維持するため、緊急メンテナンスを行う場合は、通知が直前になることがあります。ただし、緊急でやむを得ないと判断した場合は通知なしでメンテナンスを実施する場合があります。

5.　本サービスのご利用について

5.1.　サービス利用対象

・本サービスを契約した法人や個人事業主は、本サービスを利用できる権利を有します。
・上記以外の法人や個人事業主が利用する場合は、別途契約する必要があります。
・本サービスは、消費者が契約して利用することはできません。
・本サービスの利用権利を、他の企業・団体や個人に譲渡することはできません。

5.2.　サービスの利用開始

サービスの利用開始までの手続きは、「9.1 サービスご利用開始」をご参照ください。

5.3.　サービス申請内容の変更

サービス申請内容のうち変更が可能な項目は以下のとおりです。

会社情報：会社名
お客様氏名、部署名、役職、メールアドレス
住所
電話番号

5.4.　お客様による利用休止

お客様の都合による本サービスの一時的な利用の休止、停止はできません。

5.5.　メンテナンス等によるサービスの一時停止

本サービスは、本システムに対するメンテナンス等のために一時停止する場合があります。この場合には、以下のような条件のもとにサービス停止時間を設けます。

5.5.1. 計画停止

システム停止を伴わずメンテナンス作業ができない場合には、事前に通知の上、計画的にサービスを停止します。

5.5.2. 緊急メンテナンス

お客様がサービスを利用する上で重要な問題が発生した場合、サービス提供時間中にメンテナンスを実施する場合があります。緊急度の高い問題に対しては、通知を行わずに実施する場合もあります。

5.5.3. その他

天災、事変、その他の非常事態が発生し、もしくは発生するおそれがあるときには、お客様への事前通知を行わず、ＣＳＰまたはＮＥＣの判断にて本サービスを一時的に停止します。

6.　ご利用に必要な環境

6.1.　ＵＴＭ装置の設置

- ＵＴＭ装置は、お客様のネット環境のインターネット接続機器（ルータ等）と監視対象の機器の間に設置します。監視対象の機器がＵＴＭ装置を経由してインターネットと通信できるようにネットワークを設計してください。
- 図 3-1 のお客様環境イメージの場合は、インターネットに接続されるルータの LAN ポートとＵＴＭ装置の WAN ポートを接続し、ＵＴＭ装置の LAN ポートに機器を接続する構成となります。
- LAN ケーブルはお客様でご手配ください。なお、ＵＴＭ装置に LAN ケーブル（２ｍ　程度）が１本同梱されております。
- ＵＴＭ装置到着後は、いつでも設置できますが、作業中はインターネットとの通信ができなくなりますので、ご留意ください。
- ＵＴＭ装置設置後、初期設定としてアクティベーションを実施してください。
- アクティベーション実施後、必ずパソコン、タブレットなど、利用するすべての機器からインターネットに接続できることをご確認ください。
- ＵＴＭ装置の設置作業は本サービスに含まれません。ただし、お客様から特段の要望があった際にはＣＳＰは有償（税別 15,000 円）で設置作業を代行いたします。詳細は「別紙１：駆けつけサービス」をご参照ください。

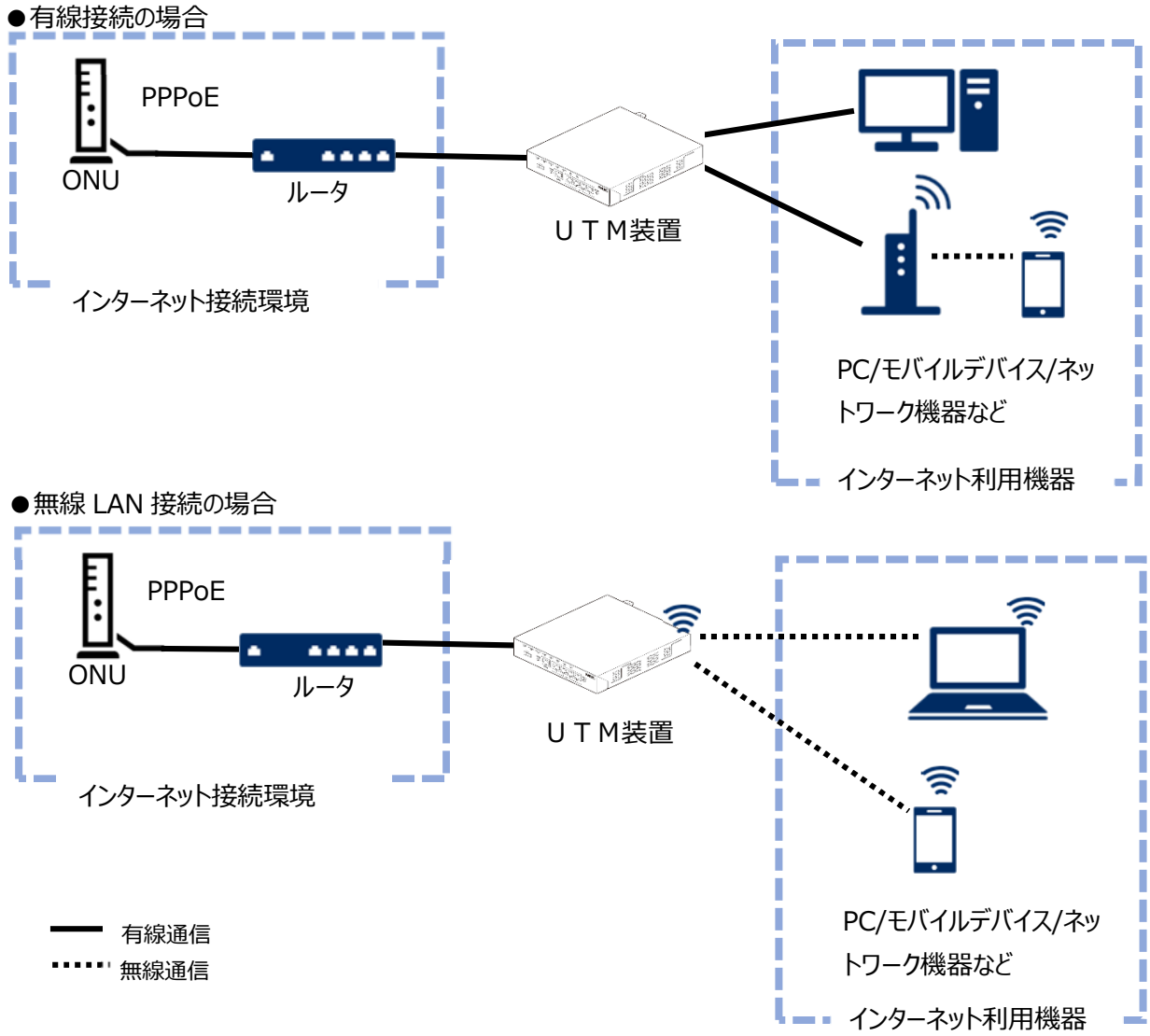


図 3-1 お客様環境イメージ

6.2.　ＵＴＭ装置の設置環境等

6.2.1. ＵＴＭ装置について

・サービス利用申し込み後にＵＴＭ装置をお客様に送付いたしますので、ＵＴＭ取扱説明書の以下の章について同意の上、ＵＴＭ装置の設置をお願いいたします。

はじめに(制限事項、免責事項、注意事項)
ソフトウェア使用許諾契約書
セキュリティ・スキャン機能　利用規約

・上記については、本サービス仕様書とともにＣＳＰのホームページに掲出されるＵＴＭ取扱説明書の記載が、ＵＴＭ装置に同梱されるものより優先されます。

・本サービスにてお客様環境に設置するＵＴＭ装置はＮＥＣの保有資産です。故意に破損した場合、賠償責任が発生します。また、ＵＴＭ装置は本サービスの目的にのみ使用が認められたものであり、別用途に使用しないでください。

6.2.2. ＵＴＭ装置の設置場所

・お客様はＵＴＭ取扱説明書などに記載されている適正な場所にＵＴＭ装置を設置し常に環境を整備、維持するものとします。

・ＵＴＭ装置は外寸突起部/スタンドを含めず約 174(W) x 195(D) x 40(H)mm で、スタンド取り付けにより縦置きも可能です。設置場所については事前に電源（100V）コンセント含めて手配してください。

6.2.3. インターネット環境、機器との接続

・ＵＴＭ装置とインターネット接続環境との間は、LAN ケーブルにて有線接続となります。ＵＴＭ装置に付帯する LAN ケーブルは約 2m です。ケーブルの長さが不足する場合は、お客様にて手配してください。

・ＵＴＭ装置 1 台に接続する機器数は、約 100 台以下を目安にしてください。なお、ここでいう機器とは、IP アドレスを持ち、ＵＴＭを経由した通信を行う機器を指しており、モバイル端末や複合機などを含みます。接続する機器の数が多い場合、通信がしづらくなったり、通信速度が遅くなったりすることがあります。接続する機器が 100 台以下でも、機器の使用状況によっては、同様の事象が発生することがあります。この場合はＵＴＭ装置を追加し、接続する機器を分散させてください。

6.2.4. その他

・ＵＴＭ装置は、ファームウェアの更新、最新の定義情報の取得の際に直接インターネットにアクセスするため、ＵＴＭ装置自体が IP アドレスをもつ必要があります。このためＵＴＭ装置は常に起動し、インターネットに接続できる状態にしてください。

・ファームウェアの更新を行う場合は、通知先メールアドレスに通知します。ファームウェアの更新はＵＴＭ装置の電源を一旦 OFF にして、再度 ON にする必要があります（電源 OFF・ON）。お客様の都合の良い時間にＵＴＭ装置の電源 OFF・ON の実施をお願いします。なお、ファームウェアの更新のため、ＮＥＣがインターネットを経由してリモートでＵＴＭ装置の再起動を行う場合があります。

・故障時はインターネットとの接続ができなくなることがあります。この場合は、お客様自身でＵＴＭ装置を一旦取り外して設置前の状態に戻していただくことでインターネット接続できるようになります。この間は、脅威の監視、不正通信の遮断や有害ファイルの無害化などのセキュリティ監視はできません。

・故障の際は代替機を手配いたします。詳細は「9.3. 故障時の問い合わせ」をご参照ください。

・ＵＴＭ装置の脅威検知機能は、メール、Web サイトでのファイルアップロード/ダウンロードなど、通信経路で送受信されるデータについて脅威の有無をチェックする機能です。このため通信路に流れるデータ量、ファイルの数、ファイルの種別等によって処理性能が低下する場合があります。

・耐用年数の制約で製造から 7 年経過するとＵＴＭ装置の交換が必要になります（代替機を手配いたします）。

6.3. 必要なネットワーク環境

(1) インターネット環境との接続

・ＵＴＭ装置を接続するため、インターネット接続機器（ルータ等）の LAN ポートを１つ占有する必要があります。

・ＵＴＭ装置は、本サービスのために、以下のプロトコル・ポートを宛先とした通信を行います。ＵＴＭ装置と通信先の間にファイアウォールを設置されている場合は、ファイアウォールでＵＴＭ装置と各通信先の通信を許可してください。

表 6-1 宛先ポート/プロトコルと通信先

宛先ポート/プロトコル	通信先
80/TCP	インターネット
443/TCP(*1)	インターネット
8443/TCP(*1)	インターネット
53/UDP	DNS サーバ
67/UDP	DHCP サーバ
123/UDP	インターネット
ICMP	ゲートウェイ

*1：ＵＴＭ装置とクラウド上のサーバの通信では SSL 通信を使用します。

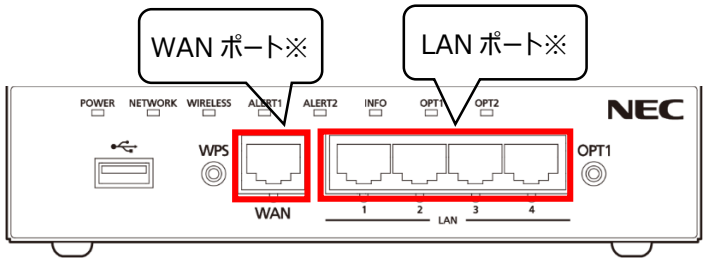
(2) 監視対象機器の接続

・通信を監視したい機器は、ＵＴＭ装置の LAN ポートまたは無線 LAN 機能に接続し、ＵＴＭ装置を経由して通信を行うように設定してください。

・監視対象となる通信パケットは、以下の通信経路によりＵＴＭ装置を通過する IPv4 のパケットおよび IPv6 のパケットです。ＵＴＭ装置を通過しない通信は検知の対象となりません。

- WAN ポートと LAN ポート間を通過する通信
- WAN ポートと無線 LAN 接続先(SSID)間を通過する通信
- 本体装置の異なる無線 LAN 接続先(SSID)間を通過する通信

●ポートの説明



※ポートの詳細はＵＴＭ取扱説明書をご参照ください

		受信側			
		WAN ポート	LAN ポート	プライマリ SSID	セカンダリ SSID
送信側	WAN ポート	対象外	対象	対象	対象
	LAN ポート	対象	対象外	対象	対象
	プライマリ SSID	対象	対象	対象外	対象
	セカンダリ SSID	対象	対象	対象	対象外

(3) 無線 LAN 接続の利用

・既存の無線 LAN 装置に接続された機器を監視対象にする場合、無線 LAN 装置をＵＴＭ装置の LAN ポートに接続してください。

・ＵＴＭ装置の無線 LAN 機能を使用する場合、ＵＴＭ装置に SSID を設定し、監視対象の機器の接続先をＵＴＭ装置に切り替えてください。

・無線 LAN 機能を使用した通信は、環境によって十分な通信速度が出ない場合や接続が不安定になる場合がありますが、無線 LAN 通信の品質について本サービスは保証しません。

・ＵＴＭ装置が対応している無線規格、暗号化方式は以下の表のとおりです。これら以外の機能が必要な場合、別途、無線 LAN 装置をご用意ください。

表 6-2 ＵＴＭ装置が提供する無線 LAN 機能

分類	機能
無線規格	IEEE802.11b/g/n(※) ※ 周波数は 2.4GHz のみサポートし、5GHz はサポートしません。
暗号化方式	WPA-PSK（TKIP） WPA-PSK（AES） WPA2-PSK（TKIP） WPA2-PSK（AES） WPA/WPA2-PSK（TKIP） WPA/WPA2-PSK（AES） 802.1x（EAP）

6.4. セキュリティサービスポータルのご利用に必要な環境

(1) アカウントの発行

・お客様のアラート検知情報は、セキュリティサービスポータルよりご確認いただくことが可能です。セキュリティサービスポータルにログインいただくためにはサービス契約時に通知する ID とパスワードが必要です。追加の ID が必要な場合は別途、相談窓口にお問い合わせください。

・ID、パスワードはお客様にて大切に保管いただくものとし、これらをお問い合わせいただいてもＣＳＰからは開示いたしません。

(2) 対応ブラウザ

・Google Chrome

・Internet Explorer 11

・Microsoft Edge

・FirefoxSafari

上記、対応ブラウザは 2021 年 7 月時点のもので、サービスの改善や強化により断りなく変更されることがあります。

(3) ログイン時の認証

・セキュリティサービスポータルの利用開始時には、仮ユーザ ID と仮パスワードをメールで通知します。このメールを受信するための環境が必要です。

・セキュリティサービスポータルへのログインには多要素認証を使用することができます。認証アプリケーションを使用する場合、認証アプリケーションをインストールするためのスマートフォンなどが必要です。SMS 認証を使用する場合、国際 SMS が受信可能な携帯電話が必要です。

はじめにご確認ください。

・本サービスをご利用いただくためのソフトウェア、2 段階認証は、お客様の責任にて準備いただく必要があります。スマートフォンアプリ、PC にインストールするフリーソフトの利用条件を事前にご理解いただいた上でご利用ください

・重要アラートの通知メールの受信には、ＵＴＭ装置の設置が完了していて、セキュリティサービスポータルでオンライン状態とログの表示を確認できる状態である必要があります。保険の利用には、重要アラートの通知メールが必要です。

7. ご利用にあたってご承諾いただく事柄

7.1. 脅威検知の基準

「脅威検知」の基準となるＵＴＭ装置の定義ファイルは、同装置製造者（ＮＥＣプラットフォームズ）の裁量により定期的に更新されます。お客様は、本サービスご利用の前提として、同装置の最新の定義ファイルに基づく基準に抵触したことをもって「脅威」とみなし、通信遮断等の「検知」の対象とされることに予め同意いただけるものとします。

7.2. セキュリティインシデントへの対応

本サービスは、セキュリティインシデントを完全に防止するサービスではありません。また、万が一損害を被った場合にＣＳＰはその補償を行わないものとします。損害には以下のようなものが含まれます。

・セキュリティインシデントによる情報機器（ハード、ソフト）やファイルの破損
・情報メディアの損壊による再作成
・本サービスの主たる機能の停止により発生する、お客様の売り上げ減少等に伴う収益減少
・第三者に対して負担する損害賠償責任による損害

7.3. お客様環境における情報取得作業

本サービスが意図した機能、性能を提供することができない状態となった場合、ＣＳＰまたはＮＥＣにて調査を行うことがあります。その場合、お客様はＣＳＰまたはＮＥＣの依頼に応じてお客様環境における各種情報をご提供いただくものとします。

7.4. お客様情報の取り扱い

本サービスの提供に必要な以下のお客様情報をＣＳＰおよびＮＥＣにて取り扱うことをご了承いただいたものとします。なお、本サービスにて取り扱うお客様情報は、本サービスをご提供する目的においてのみ使用するものとします。

- サービス申請情報（会社名、氏名・部署名・役職・メールアドレス、住所、電話番号など）
- 設置機器情報（IP アドレス、MAC アドレス、その他ＵＴＭ装置設定情報）

7.5. 契約終了時のお客様情報の破棄

契約の終了時には、本サービスにてお預かりしているお客様情報は指示により破棄します。また、設置したＵＴＭ装置は回収し、ＵＴＭ装置で収集した情報および設定した情報はすべて削除します。

7.6. データの取り扱いについて

本サービスによりＵＴＭ装置が検知した通信内容などのログ情報は、お客様を特定できないようデータを加工したうえで、以下の用途に二次利用（調査、分析、編集）することを承諾したものとします。

(1) 製品、サービス利用者への分析結果の情報提供
(2) 製品、サービスの販売促進データとしての活用
(3) 製品、サービスの品質向上のための活用
(4) セキュリティに関する脅威トレンドの調査・分析
(5) 新たなサイバー攻撃等の被害未然防止に資する目的での第三者（報道関係者含む）への提供

7.7. 通信回線について

お客様は、ネット接続に利用する回線を通じ、ＵＴＭ装置が検知した通信内容について本システムに送信されることをあらかじめ承諾するものとします。お客様は本サービス利用期間中、接続回線を適切に管理するものとします。

7.8. サイバーセキュリティ見守りシステムのサービス稼働率目標（SLO: Service Level Objective）

本サービスにて、ＮＥＣが責任をもつサイバーセキュリティ見守りシステムについて、サービス稼働率目標（SLO: Service Level Objective）は 99%以上とします。ただし、以下に定めるサービス停止を伴う作業実施時を除きます。

・OS やソフトウェアのサポート期限等による、システム停止を伴うバージョンアップ
・OS やソフトウェアのセキュリティパッチ適用(2 回/年ほどを予定)
・OS やソフトウェアの機能的制限により停止が必要な作業
・その他、ＮＥＣが必要と判断した場合

これらの作業実施を行う場合に、サービス停止を伴う作業を実施する場合、事前にお客様に告知の上、実施します

7.9. 禁止事項について

お客様は、本サービスの利用に際して以下の禁止事項に抵触しないことを承諾するものとします。

(1) 本サービスのシステムに対して、過重な負荷をかけて、ＣＳＰまたはＮＥＣの本サービスの提供に関する業務に悪影響を与えたり、第三者の利用を妨げたりすること。
(2) 本サービスに関連するサービス、アカウント、コンピューターシステムおよびネットワークに対して不正なアクセスを試みること。
(3) 本サービスにて設置したＵＴＭ装置を故意に破損もしくは売却することおよび別用途に転用すること。
(4) ＵＴＭ装置を不法投棄すること。
(5) ＵＴＭ装置を本来の用途以外に使用すること。
(6) ＵＴＭ装置を第三者への譲渡、質入れ、転貸その他の処分をすること。
(7) ＵＴＭ装置の分解、解析、改造、改変等を行うこと。
(8) ＵＴＭ装置の損壊、破棄等を行うこと。
(9) ＵＴＭ装置の著しい汚損を行うこと。
(10) ＵＴＭ装置を契約外の不正使用を行うこと。
(11) ＵＴＭ取扱説明書に記載されている禁止事項に該当する行為を行うこと。
(12) ＵＴＭ装置を日本国外に持ち出すこと。

7.10. その他

・本サービス仕様書にて定めのない事項について、お客様とＣＳＰとの間で別途協議の上、判断させていただきます。
・本サービス仕様書に記載された社名、商品名は各社の商標または登録商標です。
・本サービスは、日本国内の企業、団体に提供します。
・本サービス仕様書に記載する条項は、日本国法に準拠するものとします。
・お客様とＣＳＰとの間で利用される言語は日本語とします。
・本サービスのセキュリティサービスポータルは日本語にて提供されます。英語等には未対応です。

8. ドキュメント一覧

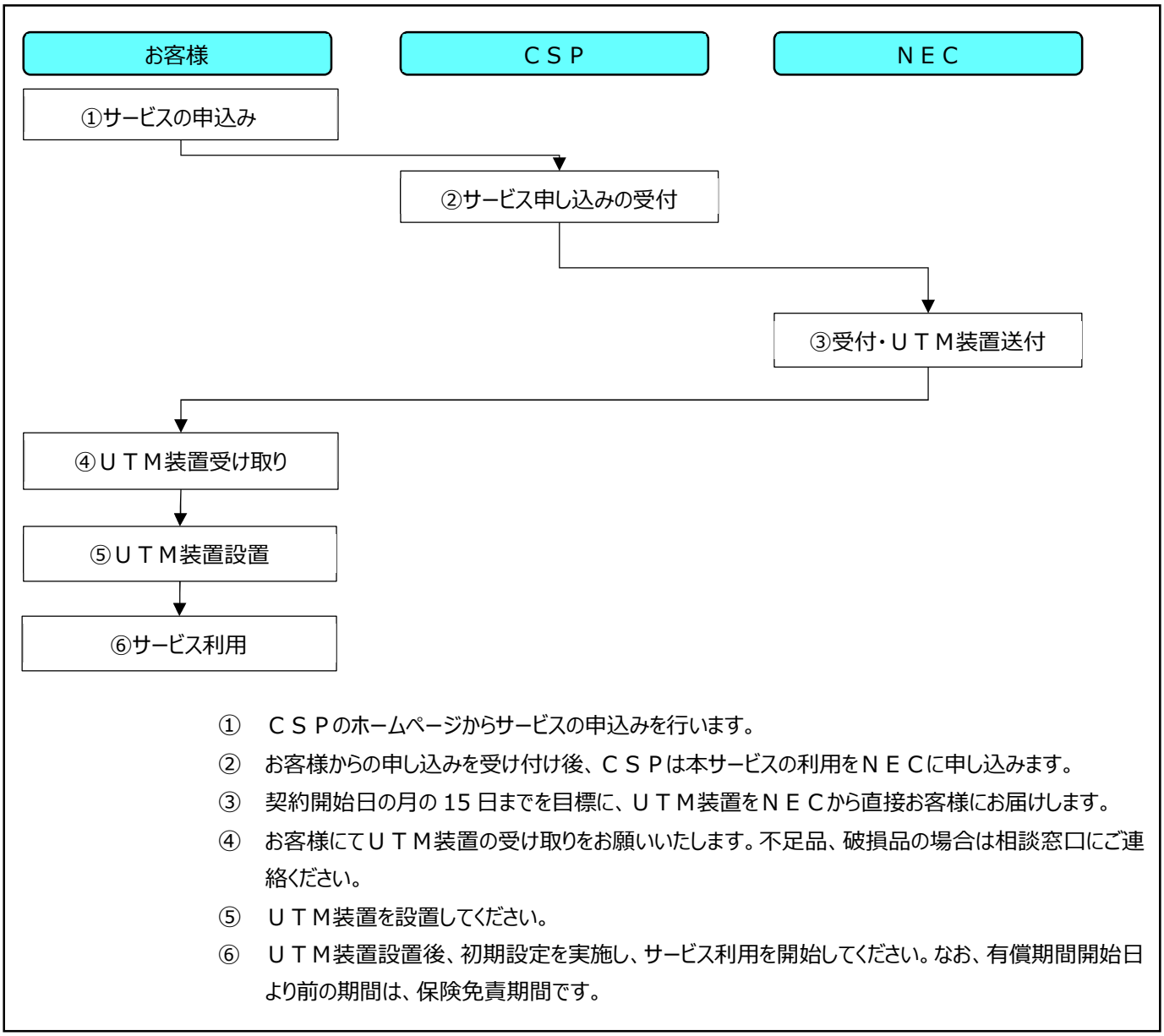
表 7-1 本サービスで利用するドキュメント一覧

No	ドキュメント名	マニュアルの主な記載内容
1	ＣＳＰサイバーガードサービス仕様書	お客様に提供するサービス内容を記載。
2	クイックスタートガイド	ＵＴＭ装置の設置方法を記載。ＵＴＭ装置に同梱されます。お客様がＵＴＭ装置受け取り時に入手します。
3	ＵＴＭ取扱説明書	ＵＴＭ装置の設置方法、動作状態の確認および故障時の復旧操作が記載されています。本サービス仕様書に付録されるほか、ＵＴＭ装置に同梱されます。
4	セキュリティサービスポータル利用マニュアル	お客様向けのセキュリティサービスポータルの使用方法を記載。

9.　サービスご利用の流れ（概要）

9.1.　サービスご利用開始

本サービスの開始までの手順の概要を以下に示します。



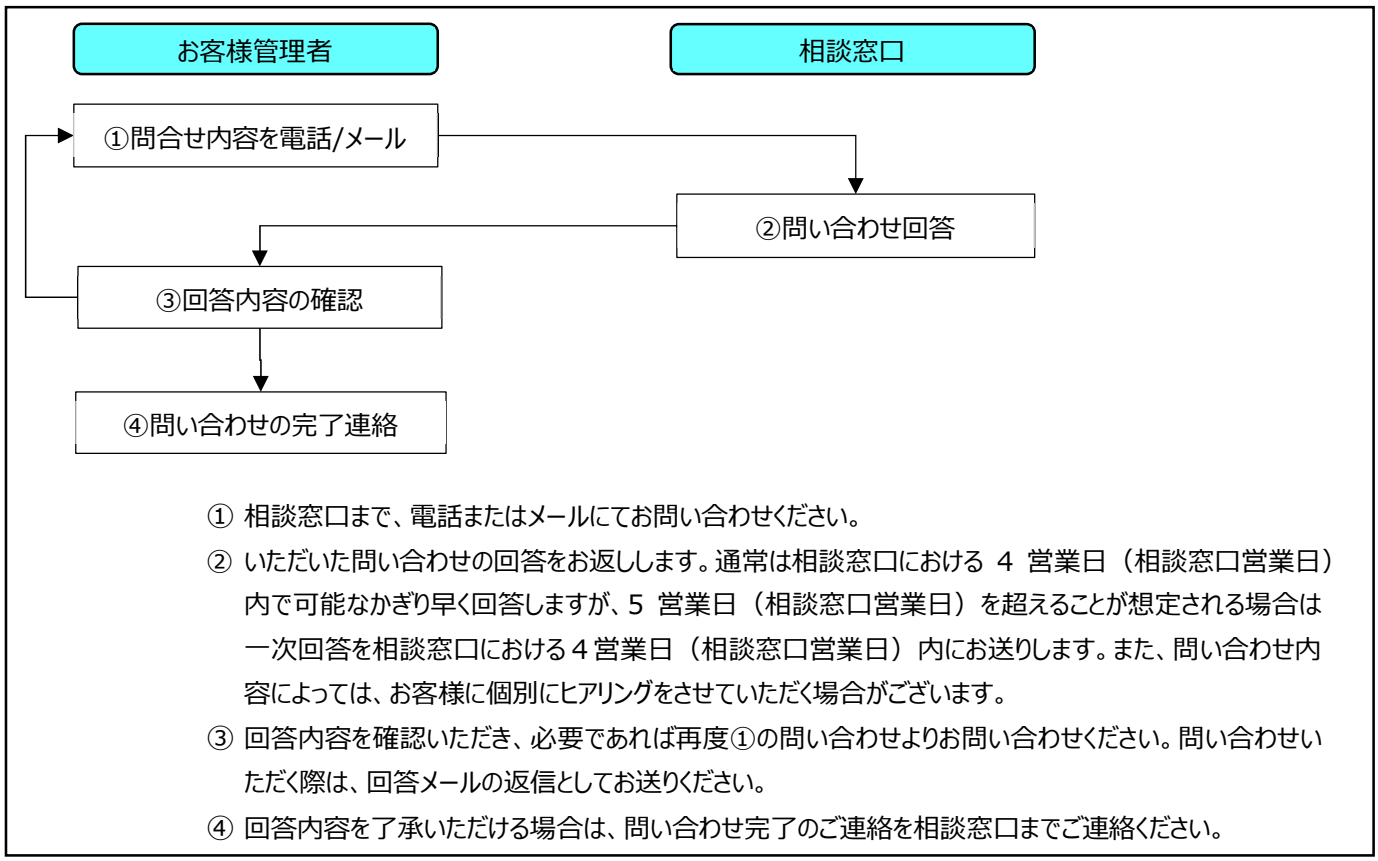
① ＣＳＰのホームページからサービスの申込みを行います。
② お客様からの申し込みを受け付け後、ＣＳＰは本サービスの利用をＮＥＣに申し込みます。
③ 契約開始日の月の 15 日までを目標に、ＵＴＭ装置をＮＥＣから直接お客様にお届けします。
④ お客様にてＵＴＭ装置の受け取りをお願いいたします。不足品、破損品の場合は相談窓口にご連絡ください。
⑤ ＵＴＭ装置を設置してください。
⑥ ＵＴＭ装置設置後、初期設定を実施し、サービス利用を開始してください。なお、有償期間開始日より前の期間は、保険免責期間です。

図 9-1 サービス利用の流れ(概要)

表 9-1　契約申請日と契約開始日、有償期間開始日の関係

契約申請日	契約開始日	有償期間開始日
各月 5 日以前の場合	契約申請日の当日	契約申請日の翌月 1 日
	または　契約申請日の翌月 1 日	契約申請日の翌々月 1 日
各月 6 日以降の場合	契約申請日の翌月 1 日	契約申請日の翌々月 1 日

9.2. 問い合わせ



① 相談窓口まで、電話またはメールにてお問い合わせください。

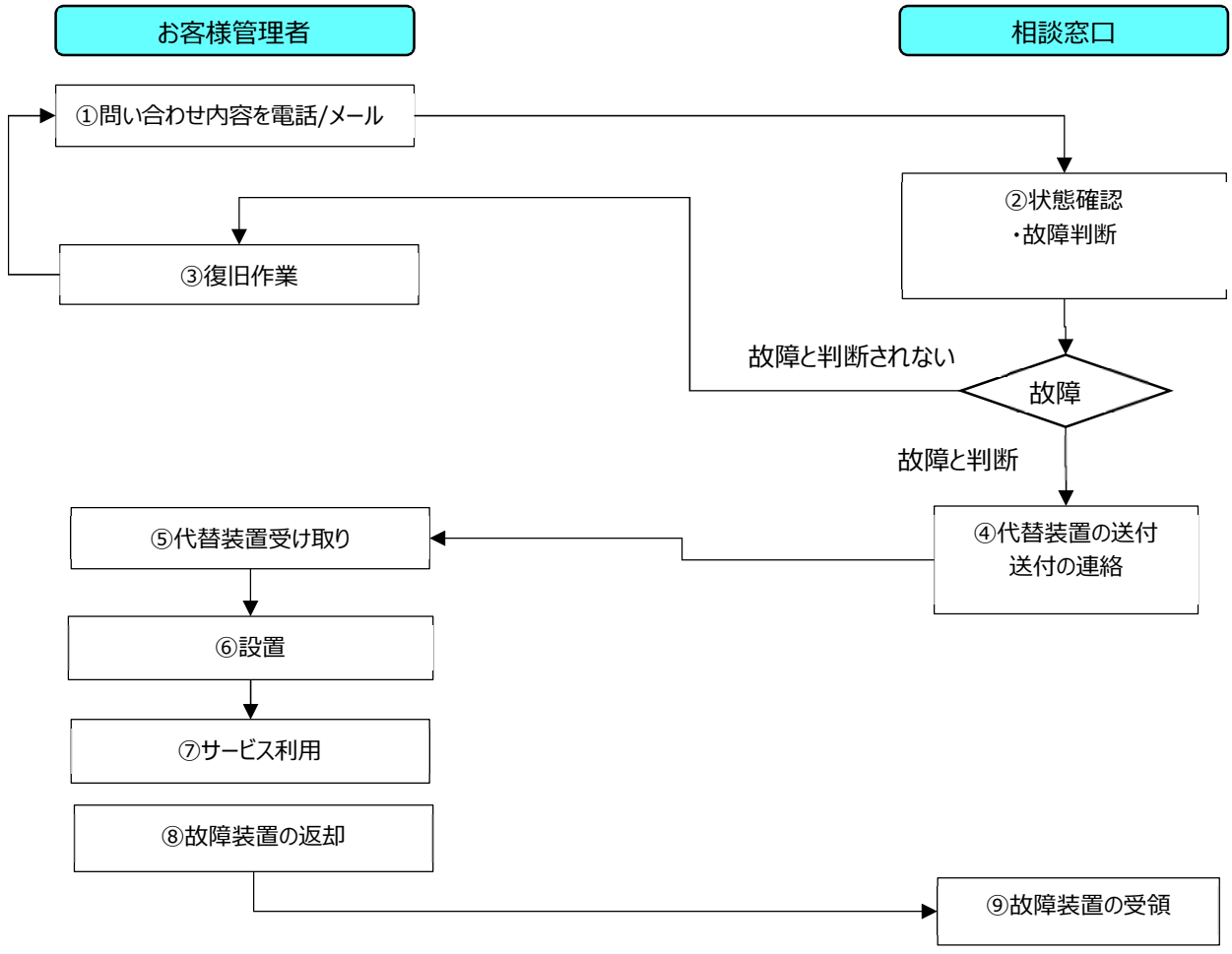
② いただいた問い合わせの回答をお返しします。通常は相談窓口における 4 営業日（相談窓口営業日）内で可能なかぎり早く回答しますが、5 営業日（相談窓口営業日）を超えることが想定される場合は一次回答を相談窓口における 4 営業日（相談窓口営業日）内にお送りします。また、問い合わせ内容によっては、お客様に個別にヒアリングをさせていただく場合がございます。

③ 回答内容を確認いただき、必要であれば再度①の問い合わせよりお問い合わせください。問い合わせいただく際は、回答メールの返信としてお送りください。

④ 回答内容を了承いただける場合は、問い合わせ完了のご連絡を相談窓口までご連絡ください。

図 9-3 問い合わせ時の流れ

9.3.　故障時の問い合わせ



① 相談窓口まで、電話またはメールにてお問い合わせください。
② ＵＴＭ装置の状態を確認させていただきます。
③ 窓口の指示や「ＵＴＭ取扱説明書」をご参照いただき、復旧作業をしてください。
④ 故障と判断された場合は、代替装置送付のご連絡をし、代替装置を発送します。
⑤ 代替機器をお受け取りいただきます。
⑥ お客様にて代替装置を設置してください。
⑦ サービスをご利用ください。
⑧ お客様は代替機器に同梱された案内に従い、故障したＵＴＭ装置を返却してください。
⑨ 故障装置を受領します。

図 9-4 故障時の問い合わせの流れ

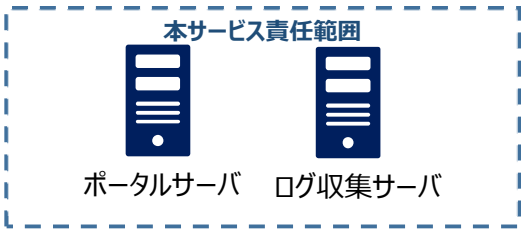
10. 障害対応

本サービスにおいて障害が発生した場合、以下の基準に従い、障害の対応を実施します。

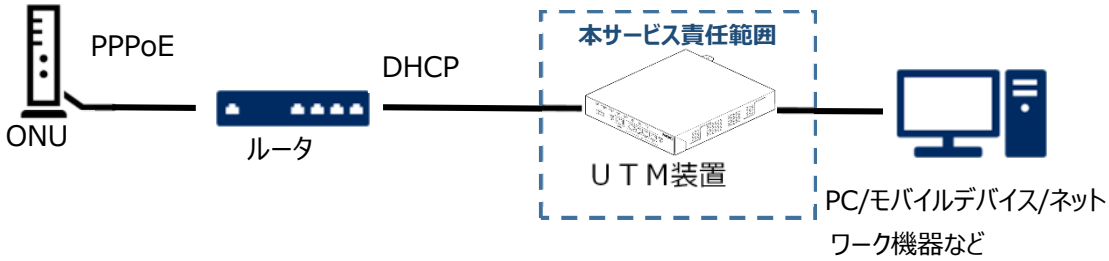
10.1. 責任分界点

本サービスの責任分界点を以下に示します。

●サイバーセキュリティ見守りシステム



●有線接続の場合



●無線 LAN 接続の場合

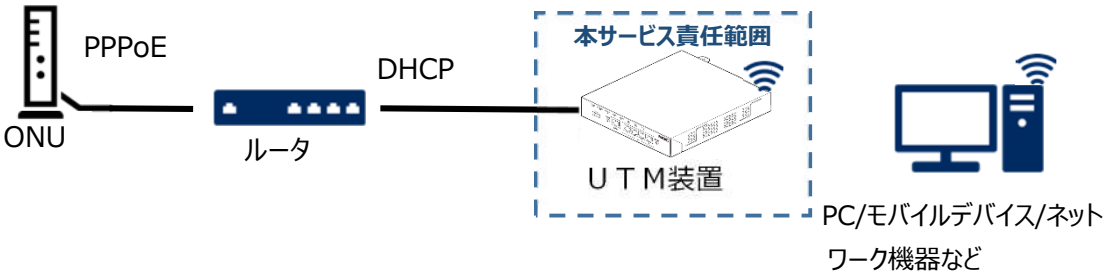


図 10-1 サービスの責任分界点

本サービスの責任範囲は、表 10 1 の「本サービスの責任範囲」で○とした箇所のみとします。これ以外でお客様にて準備されるものについては、お客様の責任とします。

表 10-1 障害箇所と責任範囲について

障害箇所	本サービスによる責任範囲	備考
ポータルサーバ	○	
ログ収集サーバ	○	
ONU	×	
ルータ	×	
ＵＴＭ装置	○	
PC/モバイルデバイス/ネットワーク機器など	×	
LAN ケーブル	×	
ポータルサーバ/ログ収集サーバとインターネットの間の通信	○	
インターネットと ONU の間の通信	×	
ONU とルータの間の通信	×	
ルータとＵＴＭ装置の間の通信	○(※)	※ 通信障害がＵＴＭ装置の障害に起因するものである場合のみ、責任範囲とします。
ＵＴＭと PC/モバイルデバイス/ネットワーク機器などの間の通信	○(※)	※ 通信障害がＵＴＭ装置の障害に起因するものである場合のみ、責任範囲とします。
ルータと PC/モバイルデバイス/ネットワーク機器などの間の通信	○(※)	※ 通信障害がＵＴＭ装置の障害に起因するものである場合のみ、責任範囲とします。

別紙 1:駆けつけサービス

１． 駆けつけサービスの概要

重要アラートが発生した際には、お客様の要請によりＣＳＰが駆けつけてサポートします。この駆けつけサービスは有償となりますが、保険により費用を賄うことができます（1 回／年まで）。なお、駆けつけサービスは、お客様の実施するウイルス除去などの作業をサポートするものであって、作業結果を保証するものではありません。

２． 駆けつけサービスの要請

駆けつけサービスの要請手順は以下のとおりです。

(1) 保険適用の確認

重要アラートの通知メールを受信したら、記載されている重要度をご確認ください。重要度が「★★★（高）」の場合（★★★アラートの場合）は、駆けつけサービスの費用を保険で賄うことができます（重要度が「★★☆（中）」で、ウイルス対策ソフトによるフルスキャンの結果、★★★アラート相当と判断された場合も同様です。）。

(2) 要請の前に実施していただくこと

★★★アラートを発生したパソコン等を特定できた場合は、以下の作業を実施してください。なお特定できない場合や通知メールの内容が不明な場合は、相談窓口（別紙３）にご連絡ください。

・LAN ケーブルを抜く、Wi-Fi を無効にするなどにより、ネットワークから切り離す。
・通知メールに必要な作業が記載されている場合は、記載内容に従って作業する。
・ウイルス対策ソフトでフルスキャンを実施し（定義情報が最新ではない場合は、ネットワークから切り離す前に、情報を更新する）、結果を保存しておく。

(3) 相談窓口への連絡

・相談窓口には、重要アラートの内容確認や、パソコン等の特定、必要な処置について問い合わせることができます。
・問い合わせの際、相談窓口からＵＴＭの設置状況等について確認する場合があります。
・相談窓口がリモート調査を行う際に、パソコン等の設定についてお伺いする場合があります。
・問い合わせへの回答に従って、必要な作業を実施してください。
・駆けつけサービスを要請する場合は、相談窓口にお伝えください。訪問を希望する日時があれば、併せてお伝えください。

(4) 訪問日時の決定

・ＣＳＰの担当者から電話でご連絡しますので、訪問日時を調整いたします。

３． 駆けつけサービスの内容

（１） サポート内容

・★★★アラートが発生したパソコン等を特定するサポート
・特定されたパソコン等をネットワークから切り離すサポート
・特定されたパソコン等のウイルス対策ソフトによるフルスキャンのサポート

（２） サポートにあたって、ご承諾いただくこと

・お客様のネットワークと電源に、持参したパソコンやモバイル端末等を接続することがあります。

・必要により、パソコン等の使用者に対し、ヒアリングやパソコン等の操作依頼をすることがあります。

・サイバーインシデントが発生する「パソコン等」には、パソコンやモバイル端末やネットワーク機器のほか、複合機や空調機、ＴＶなどのネットワークに接続されたあらゆる機器が含まれます。

・駆けつけサービスは、発生したサイバーインシデントへのお客様の対応をサポートしますが、端末の特定やウイルス除去の結果については保証できません。

・また、作業に関連して発生した電子情報の消失等の損害についても、一切の責任を負いません。

（３） サポートできない作業

・パソコン等に保存されていたプログラム、データの保全

・サイバーインシデントによって発生した損害の復旧

・サポート対象外のＯＳ、ウイルス対策ソフトに関する対応

・複合機や空調機、ＴＶなどウイルス対策ソフトでのフルスキャンができない機器への対応

４．駆けつけサービスの対応日時と対応エリア

(1)対応日時

平日（土日祝日とＣＳＰの定める休日を除いた日） ０９：００～１８：００

(2)対応エリア

東京都（島しょ部を除く）、神奈川県、埼玉県、千葉県

５．駆けつけ費用

・駆けつけ費用 50,000 円（交通費、消費税含）

なお、対応が長時間にわたる場合や、専門的な知識や技能が必要な対処は別途申し受けます。また、対応する機器や被害状況により、十分対応できない場合があります。

６．保険の発動条件

・「別紙２：保険契約」によります。

７．ＵＴＭの設置、撤去サービス

ＵＴＭの設置、撤去の作業が必要な場合は、有料でお受けいたします。

・出張費 15,000 円（消費税別） （ＵＴＭ1 台の場合）

・追加作業費 5,000 円（消費税別）／台 （ＵＴＭ2 台目以降。1 台目と同時作業に限る）

※設置、撤去に必要な電源、ＬＡＮケーブル等は事前にご準備ください。

別紙２：簡易サイバー保険規約

■保険の概要

補償発動要件を満たした場合にご提供する駆けつけサービスにかかった費用ついて、本サービスの 1 契約あたり 1 年間の保険責任期間において 1 回のみ 5 万円（税その他一式全て含む）を限度に駆けつけサービスの提供を受けることが可能です。保険金は、駆けつけサービスを行ったＣＳＰに直接支払われ、お客様の手元に支払われることはありません。

■補償発動要件

補償発動要件は以下のとおりとなります。

★★★アラートの検知に起因して、被保険者が使用、所有または管理するネットワーク（ただし、専ら他人に使用される目的のものを除きます。）に対する不正アクセス等の発生またはそのおそれの発生が明らかになること。

■補償する費用

以下の費用を補償致します。

不正アクセス等の有無を判断するために支出する調査依頼費用および不正アクセス等の原因調査ならびに初動対処のために支出する駆けつけサービス費用。ＣＳＰ（またはＣＳＰが指名する代理人）が駆けつけサービスをした場合に限ります。

■保険責任期間

本サービスの有償期間開始日 00:00 から 1 年間です。

本サービス加入期間中であれば保険責任期間満了時に、さらに 1 年間自動更新されます。

本サービスの有償期間開始日より前の期間においては、駆けつけサービスに関する費用はお客様負担となります。

保険責任期間中であっても、本サービスの利用期間満了後または本サービス解約後に生じた原因に基づく駆けつけサービスに関する費用に関しては保険金の支払いはなされず、お客様負担となります。

■支払限度額

5 万円（本サービスの 1 契約あたり 1 年間の保険責任期間で 1 回の駆けつけサービスのみ保険金支払いの対象となる。金額には税その他一式全て含みます。）

■保険が支払われない主な場合

・保険責任期間の開始時より前に発生した事由により事故が発生するおそれがあることを保険契約者または被保険者が保険責任期間の開始時に認識していた場合（認識していたと判断できる合理的な理由がある場合を含みます。）
・被保険者による窃盗、強盗、詐欺、横領または背任行為その他の犯罪行為。ただし、過失犯を除きます。
・被保険者が法令に違反することまたは他人に損害を与えるべきことを認識していた行為（認識していたと判断できる合理的な理由がある場合を含みます。）

■注意制限事項

・保険金請求に関する保険会社との手続きは相談窓口が行います。
・保険金の支払先は駆けつけサービスを行ったＣＳＰとなります。
・★★★アラート発生後、駆けつけ対応前に被保険者にて、原則ウイルス対策ソフトでフルスキャンを行っていただいた後に問題に応じて保険を使った駆けつけ対応となります。
・保険を使った駆けつけサービスが利用できる期間は、★★★アラート発生後、30 日以内とします。

■保険についての相談窓口

★★★アラートの通知メールが着信されましたら相談窓口（別紙 3）にご連絡ください。

■保険金請求／支払いフロー

① 保険発動条件適合

② お客様から相談窓口へ駆けつけサービス依頼

③ 相談窓口からお客様へアンチウイルス対策ソフトでのフルスキャンの実施をご案内

④ フルスキャン後も駆けつけが必要な場合、相談窓口からお客様へＣＳＰによる駆けつけサービスのご案内

⑤ お客様がＣＳＰと駆けつけサービスの日程および作業調整

⑥ ＣＳＰが駆けつけサービス実施

⑦ ＣＳＰから相談窓口に実施報告書兼請求書を提出

⑧ 相談窓口から保険会社に保険金請求

⑨ 保険会社からＣＳＰに保険金支払い

別紙３：相談窓口

１．連絡先
　フリーダイヤル：０１２０－５１９－９８８
　E-mail　　：cyberguard_cc@we-are-csp.co.jp
２．サポート実施方法
　・電話/メール
３．受付時間
　・相談窓口営業日の 09:00-18:00
４．サービス提供方法
　お客様から相談窓口への電話、またはメールに対する受付・回答を行う。
5．サービス利用対象
　・本サービスを契約したお客様に限り、相談窓口を利用できます。
　・本サービスの利用権利を、他の企業・団体や個人に譲渡することはできません。
6．受付対応範囲
　・ＵＴＭ設置・移設および撤去に関する問い合わせ
　・セキュリティサービスポータルに関する問い合わせ
　・重要アラートに関する問い合わせ
　・保険に関する問い合わせ
7．受付対応範囲外
　・他社サービス（製品）等に関する問い合わせ
　・インターネット回線が起因とする不具合やトラブル問い合わせ
　・周辺機器の相性問題、ＵＴＭ装置以外のハードウェア故障と断定できる状態でのお問い合わせ
　・ハードウェアの改造、またはそれを助長すると思われるお問い合わせ
　・デュアルブート状態のパソコンならびにその設定に関するお問い合わせ
　・OS 復旧作業および支援作業
　・OS 付属以外のゲームソフトに関するお問い合わせ
　・OS 以外のアドオンプログラム（プラグイン含）の導入、操作方法に関するお問い合わせ
　・雑誌の付録 CD・DVD に関するお問い合わせ
　・体験版、β版ソフトウェアに関するお問い合わせ
　・プログラミング開発支援（HTML、マクロ、VBA、Access など）に関するお問い合わせ
　・スクリプティング、プログラミング、データベース、Web などの設計や開発に関するお問い合わせ
　・マクロ、財務関数、統計関数、検索/行列関数およびデータベース関数のお問い合わせ
　・各種ソフトウェアのアップデートで提供される修正プログラムの詳細に関するお問い合わせ
　・ファイル交換ソフトウェアに関するお問い合わせ
　・ソフトウェアの設計または製造に関するお問い合わせおよび起因する障害に関するお問い合わせ
　・ソースコードの解析やシステムのパフォーマンス劣化による解析などのお問い合わせ
　・フリーウェア・シェアウェアに関するお問い合わせ
　・PC 本体以外へのソフトウェアのダウンロードならびにインストールのお問い合わせ
　・企業向けソフトウェア、専用会計ソフトウェアに関するお問い合わせ
　・日本語版以外の OS、アプリケーションおよびマニュアルに関するお問い合わせ
　・付属マニュアルに記載のない応用的操作・設定、メーカーがサポートしていないお問い合わせ
　・メーカー起因のお問い合わせ、メーカー独自仕様のアプリケーションのお問い合わせ
　・違法行為（不正コピーなど）、またはそれを助長すると思われるお問い合わせ
　・データバックアップ支援および消失データの復旧に関するお問い合わせ
　・ウイルス、スパイウェア感染時におけるインストール済セキュリティソフトウェア以外での駆除操作
　・パソコンでのファイル共有、プリンタ共有設定
　・IP アドレスを固定で使用されている環境でのネットワーク全般に関するお問い合わせ
　・事業用ネットワーク環境の再設定作業、インストール作業、インプリメント作業などのお問い合わせ

・大型複合機など固定 IP アドレスを使用する機器が導入された環境でのネットワーク共有のお問い合わせ
・TCP/IP 以外のネットワーク接続方法に関するお問い合わせ
・ドメイン参加しているパソコンに関するお問い合わせ
・海外からのお問い合わせ
・オンライングループ作業に関するお問い合わせ
・文書や書類などの代行作成に関するお問い合わせ
・紛争や訴訟等の対応および報道機関への対応
・その他、ＣＳＰまたはＮＥＣがサポート範囲外と判断するお問い合わせ

【改定履歴】

第 1.1 版　2021 年 10 月 01 日

第 1.2 版　2022 年 01 月 12 日　P.25 別紙 3 ：相談窓口　1．連絡先
フリーダイヤル番号及び E-mail アドレスを追記