スマートコネクト マネージドサーバ
ファイアウォール/UTM オプション

サービス仕様書

（第 4.0 版　2020 年 3 月 31 日版）

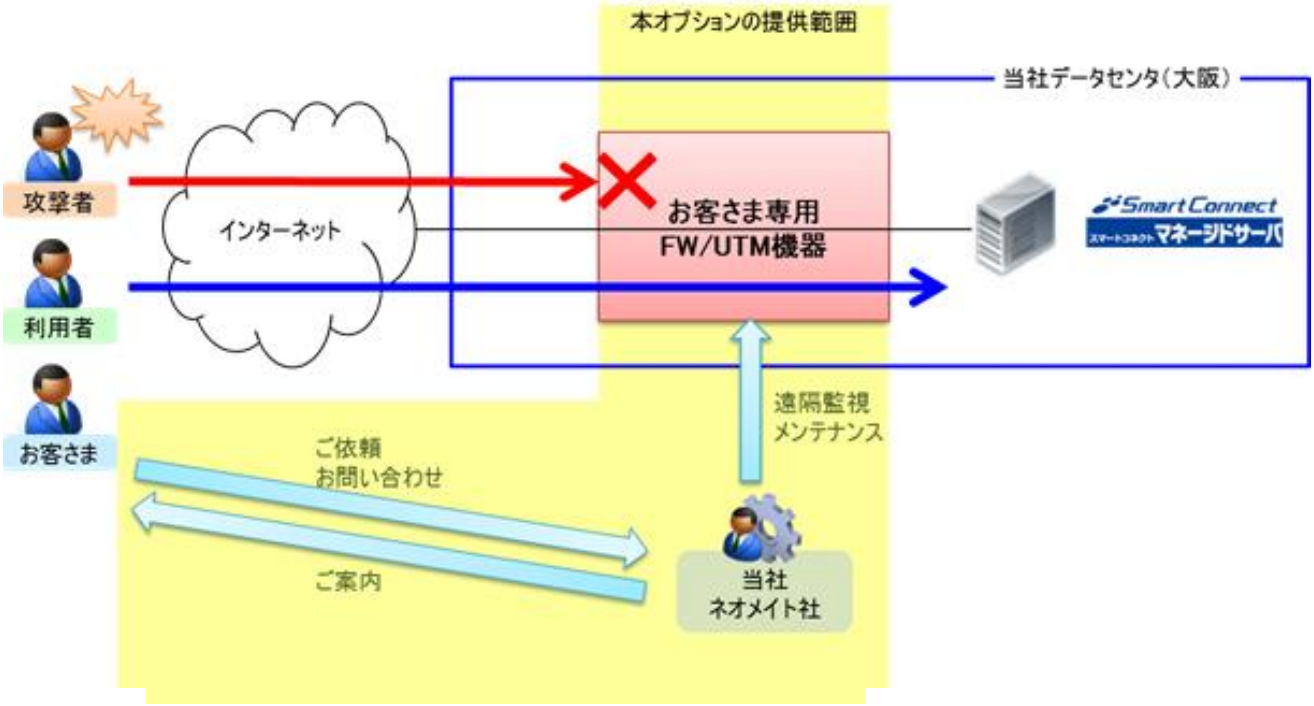
We are the future.

＜目次＞

1. サービス概要

スマートコネクト マネージドサーバ ファイアウォール/UTM オプションは、お客さま専用のファイアウォール/UTM 機器（以下、FW/UTM 機器）をご用意し、FW/UTM 機器の設定情報変更、24 時間 365 日の稼動状態監視といった運用保守サービスをご提供します。

本オプションは 2018 年 12 月 21 日をもって、新規販売を終了しております。
2018 年 12 月 21 日以前に本オプションをご契約されたお客様については、設定情報変更は受付しております。



※　本オプションは、株式会社エヌ・ティ・ティ ネオメイト（以下、ネオメイト社）の「AQStage UTM マネージドパック」をもとに、当社およびネオメイト社がお客さまに提供いたします。したがって、ネオメイト社より直接ご案内をさせていただく場合があります。

2. サービス体系

2.1. サービス仕様

本オプションは、ご契約いただくことで以下のサービスを提供します。

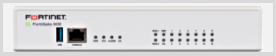
項目	内容
FW/UTM 機器提供	お客さま専用の FW/UTM 機器を、ご契約のスマートコネクト マネージドサーバと接続の上、ご提供します。
セキュリティ機能	FW/UTM 機器が備えたファイアウォール、UTM セキュリティ（アンチウイルス、侵入検知）、ロギング等をご提供します。
運用保守サービス	FW/UTM 機器に対する監視・故障対応等の他、設定変更対応、各種ログ・レポートをご提供します。

2.2. FW/UTM 機器提供

2.2.1. 提供モデル

提供する FW/UTM 機器のモデルを以下に示します。

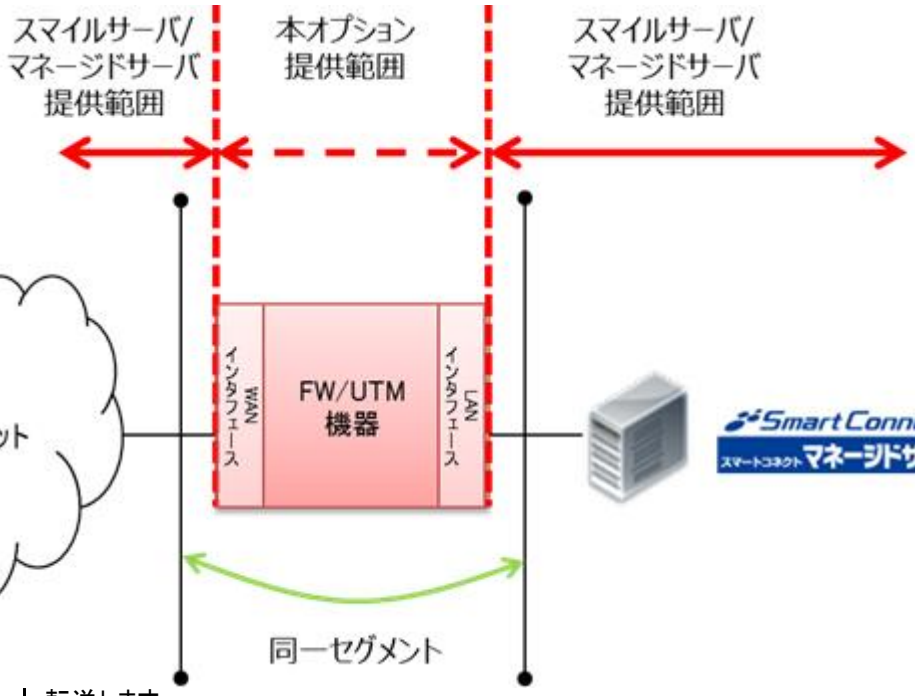
なお、表内の記載値はパフォーマンスをお約束するものではなく、ご利用環境によっては下回ることもございます。

	FortiGate-90E 
システム性能	
ファイアウォールスループット	4.0 (Gbps) 375 Kpps
ファイアウォールレイテンシ	64 バイト(UDP) 182 (μs)
ファイアウォール同時セッション(TCP)	1,200,000
ファイアウォール新規セッション(TCP)	27,500 /s
ファイアウォールポリシー	5,000
IPS スループット	440 Mbps
NGFW スループット	350 Mbps
脅威保護スループット	210 Mbps

2.2.2. 接続構成

提供する FW/UTM 機器の接続構成を以下に示します。

項目	内容
ブリッジ型	通過するイーサネット・フレームを精査するレイヤ2の FW/UTM 機器として動作します。



2.3. セ

FW/UTM

項目	
ファイ	ットワ
UTM	
ア	入およ
侵	御を保
ロギン	ターへ
	転送します。
FW/UTM 機器の 閲覧権限	FW/UTM 機器に閲覧専用のユーザーアカウントを作成し、提供いたします。

2.3.1. ファイアウォール

ファイアウォールの機能について、以下に示します。

項目	仕様
基本動作	FW/UTM 機器を経由する各通信に対し、一致するポリシーに基づき動作します。 なお、本機能はステートフル・インスペクションを実装し、通過する通信データの状態を監視し、戻りの通信データに必要なポリシーを動的に許可します。
ポリシーと通信が一致した際の動作	○アクションとして「 許可 」と「 拒否 」を選択できます。 ●「 許可 」は通信を通過させます。 通過された通信はステートフル・インスペクションにより、戻りの通信は動的に許可されます。 （ 戻りの通信をポリシーで設定いただく必要はございません。 ） ●「 拒否 」は通信を遮断します。
ポリシー走査の動作	○ポリシーは上段より下段に対し比較走査され、最初に合致したポリシーが通信との一致として適用されます。 ○いずれのポリシーにも一致しない場合は、「 拒否 」されます。

項目	仕様
ポリシー定義	ファイアウォール機能を動作させたい通信を定義し、動作させる内容を定義します。 FW/UTM 機器の異なるインタフェースを介す通信（WAN インタフェースから LAN インタフェースへの通信、LAN インタフェースから WAN インタフェースの通信など）に対して記載する必要があります。
定義可能項目	＜ 動作対象の定義 ＞ 通信方向、送信元アドレス、宛先アドレス、サービス ＜ 動作内容の定義 ＞ アクション : 「 許可 」または、「 拒否 」を指定します。 アンチウイルス機能 : 「 有効 」または「 無効 」を指定します。 アクションとして「 有効 」を指定いただいた場合、有効となります。 詳細は 2.3.2.アンチウイルスを参照ください。 侵入検知機能 : 「 有効 」または「 無効 」を指定します。 アクションとして「 有効 」を指定いただいた場合、有効となります。 詳細は 2.3.3.侵入検知を参照ください。 ロギング機能 : 「 有効 」または「 無効 」を指定します。 アクションとして「 有効 」を指定いただいた場合、有効となります。 詳細は 2.3.4.ロギングを参照ください。
定義可能項目(解説)	○通信方向 : 通信の方向を指定します。 ○送信元アドレス : 送信元アドレスを指定します。 アドレス・オブジェクトが指定可能です。 ○宛先アドレス : 宛先アドレスを指定します。 アドレス・オブジェクトが指定可能です。 ○サービス : サービスを指定します。

項目	仕様
アドレス・オブジェクトの定義	ポリシー定義の< 動作対象の定義 >における送信元アドレス、宛先アドレスを適用するためのオブジェクトを定義します。 また、判別を容易とするためのアドレスオブジェクト・グループを定義します。
定義可能項目	
	< アドレス・オブジェクト > オブジェクト名、タイプ、アドレス、インタフェース、コメント < アドレスオブジェクト・グループ > グループ名、メンバー、コメント
定義可能項目(解説)	
	○オブジェクト名 : 英数字にて記載します。 ○タイプ : アドレスの記載方法を選択できます。 ● サブネット : ネットワークアドレスで記載できます。 ● IP 範囲 : IP アドレスの始まりと終わりを範囲指定して記載できます。 ● FQDN : ホスト名で記載できます。 (DNS で正引きできることが必須となります。) ● 国 : 国名で選択できます。 (IP アドレス範囲は FortiNet 社指定のものに準じます。) ○アドレス : 選択タイプに準じた記載方法で、アドレスを記載できます。 ○インタフェース : 該当のオブジェクトを定義するインタフェースを指定します。 ○コメント : 任意入力項目であり、英数字にて記載できます。 備考、備忘用途で用いられる項目であり、基本動作には影響ありません。 ○グループ名 : 英数字にて記載します。 ○メンバー : アドレスオブジェクト・グループに属すアドレス・オブジェクトを複数指定できます。 ※留意点 任意入力可能なパラメータにおいて、以下の『 』内の 7 文字はご利用いただけません。 『 < 』、『 > 』、『 (』、『) 』、『 # 』、『 ‘ 』、『 “ 』

2.3.2. アンチウイルス

アンチウイルスの機能について、以下に示します。

項目	仕様
基本動作	FW/UTM 機器の通過を許可された通信に適用されたポリシーに対し、アンチウイルスを有効とした際、動作します。
アンチウイルスの動作	○アクションとして「 有効 」と「 無効 」を選択できます。 ●「 有効 」は通信をアンチウイルス機能で精査し、検出時は該当通信をブロック(破棄)し、未検出時は通信を通過させます。 ※ STARTTLS 利用時、アンチウイルス・侵入検知でのデータ精査は不可となります。 ●「 無効 」は通信を通過させます。
留意点	
ウイルス検出時	ウイルス検出時は全て、「 破棄(ブロック) 」とし、設定変更することはできません。
対応プロトコル	対応プロトコルは以下のとおりです。適用範囲は設定変更できません。 HTTP(TCP: 80 ・ TCP:11180) SMTP(TCP: 25 ・ TCP: 587) POP3(TCP:110) IMAP(TCP:143) FTP (TCP: 21)
最大検知ファイルサイズ	検出可能なファイルサイズは「非圧縮時 10 MB ※」です。設定変更はできません。 ※ 10MB を超過する際、アンチウイルスは適用(精査)されずに通過されます。
圧縮ファイルへの対応	FortiNet 社の仕様に基づき、全ての主要圧縮ファイルを検知可能です。

2.3.3. 侵入検知

侵入検知の機能について、以下に示します。

項目	仕様
基本動作	FW/UTM 機器の通過を許可された通信に適用されたポリシーに対し、侵入検知を有効とした際、動作します。
侵入検知の動作	○アクションとして「 有効 」と「 無効 」を選択できます。 ●「 有効 」は通信を侵入検知機能で精査し、検知時はシグネチャに定義されたアクションに従い、未検知時は通信を通過させます。 ※ STARTTLS 利用時、アンチウイルス・侵入検知でのデータ精査は不可となります。 ●「 無効 」は通信を通過させます。
留意点	
検知レベル ※ 凡例 ☑:検知する ☐:検知しない	対応レベルは以下のとおりです。適用範囲は設定変更できません。 ☑ 極高(Critical) ☑ 高 （ High ）　検知レベルは侵入時の危険性を示し、全てを検知対象とすると ☑ 中 （ Middle ）　リソースを大幅に使用するため、低レベル以下の攻撃は ☐ 低 （ Low ）　対象外としています。 ☐ 情報(Information)
ターゲット/OS	対応ネットワークデバイスは「 全て 」です。設定変更できません。
検出時のアクション	FortiNet 社の「 デフォルト設定 」を継承し、設定変更はできません。 不正な通信挙動毎に 4 種のアクション(「 モニタ(検知のみ) 」・「 ブロック(破棄) 」・「 リセット(破棄しリセットパケット送出) 」・「 隔離(デフォルト設定では該当無し) 」)を継承します。
検出時のアクション (補足)	上記 4 種のアクションは、不正通信を検知した際にその危険性に応じて変わります。 危険性が基本低い通信には「 モニタ 」、危険性を含む通信には「 ブロック 」もしくは、「 リセット 」が適用され、それぞれ以下のシステム処理が行われます。 モニタ : 不正な通信挙動を検知した際、該当ログを残し、通信を許可します。 ブロック : 不正な通信挙動を検知した際、該当ログを残すと共に、通信をブロック(破棄)します。 リセット : 不正な通信挙動を検知した際、該当ログを残すと共に、通信をブロック(破棄)しかつ、通信先のホストに対し、リセットパケットを送出します。 隔離 : 不正な通信挙動を検知した際、該当通信を隔離(取出し)しますが、デフォルト設定には本適用はございません。
レートベースシグネチャ※	レートベースシグネチャは「 適用しない 」です。設定変更はできません。 (※ DoS/DDoS のように通信の絶対量が問題となる攻撃に対し、通信量に閾値を設けて防御する機能)

2.3.4. ロギング

ロギングの機能について、以下に示します。

項目	仕様
基本動作	FW/UTM 機器を介して通過、遮断された通信履歴を適用されたポリシーで明示することで動作します。
ファイアウォールで通信拒否された際の動作	○アクションとして「 有効 」と「 無効 」を選択できます。 ●「 有効 」はファイアウォール機能としてログ情報を取得します。 （ 本ログが違反トラフィックログになります。 ） ※ 暗黙の deny（いずれのポリシーにも一致しない場合の「 拒否 」）はログ出力対象です。 ●「 無効 」はログ情報を取得しません。
UTM セキュリティ機能が有効のポリシーが適用された際の動作	○アクションとして「 有効」と「 無効 」を選択できます。 ●「 有効」は UTM セキュリティ機能が検出/検知した際にログ情報を取得します。 （ 本ログが UTM セキュリティログになります。 ） ●「 無効 」はログ情報を取得しません。

2.3.5. FW/UTM 機器の閲覧権限

FW/UTM 機器の閲覧権限の機能について、以下に示します。

項目	内容
FW/UTM 機器の閲覧権限	FW/UTM 機器に閲覧専用のユーザーアカウントを作成し、提供いたします。 本権限により、お客さまからも FW/UTM 機器で発生したインシデントおよび、ログ情報もしくは、機器の設定内容を閲覧いただけます。 但し、ログ情報は FW/UTM 機器の内蔵メモリーに保存できる限りとなるため、一定量に達した後は新たに取得されたログ情報が過去取得分を上書きいたしますことご注意願います。

2.4. 運用保守サービス

運用保守サービスの概要を以下に示します。

項目	内容
監視・故障対応	FW/UTM 機器の監視や、故障対応を実施します。
技術サポート・設定変更対応	FW/UTM 機器に関する技術的な問合せや、設定変更対応を実施します。
ファームウェア・ライセンス管理	FW/UTM 機器のファームウェアの動作確認やバージョンアップ、ライセンスの管理を実施します。
ログ・レポート提供	FW/UTM 機器に関するログやレポートをお客さまに提供します。

2.4.1. 監視・故障対応

監視・故障対応について、以下に示します。

項目	内容
リモート監視	FW/UTM 機器とネオメイト社センター間の接続を常時監視します。 最大 10 分間継続して、センターと FW/UTM 間の通信ができない場合、不具合として検知します。
故障対応	FW/UTM 機器のハードウェア故障と判断される際、ハードウェアの交換から設定情報の復元、基本動作の確認作業まで実施します。 また、故障発生時に備え、共用の予備機をデータセンタ内に準備します。 提供機器にてハードウェア故障を確認した場合は速やかに予備機への設定投入と、機器取替えを行います。 機器交換時の設定復旧は、当社にて保管している最新世代の設定情報にて実施します。 ※複数の故障が同時に発生した場合、上記共用予備機で対応できず、復旧に時間がかかる場合があります。
インシデント通知	アンチウイルスおよび、侵入検知機能において、以下のインシデントが検知された際、ネオメイト社よりインシデント通知として、お客さまへお知らせします。 〇インシデント通知の発生条件 ● アンチウイルス機能でウイルスおよび、マルウェアを検出し、危険性が高いと判断される場合。 ● 侵入検知機能でウイルスおよび、マルウェアを検知および、活動を検出し、危険性が高いと判断される場合。 ※ お知らせはあらかじめ、登録いただいたメールアドレスに対し、送信します。 ※ インシデント通知のお知らせは、平日 9 時 00 分～17 時 30 分にて実施いたします。

2.4.2. 技術サポート・設定変更対応

問合せ・設定変更対応について、以下に示します。

項目	内容
技術サポート	FW/UTM 機器の操作方法などの問い合わせに対応します。 受付は、電話もしくはメールで行います。
設定情報変更・管理	設定情報変更
	FW/UTM 機器に何らかの設定変更が必要となった場合、ネオメイト社センターよりリモートで設定変更を実施します。 設定変更はお客さまからの申し込みに基づき実施します。 申し込みは、メールで申込書を送付いただきます。 ネオメイト社より受付番号(SR 番号)のメール送信を実施しかつ、設定変更内容に関してお客さまとネオメイト社にて合意した日を 0 営業日目とし、2 営業日目以内で設定変更を実施します。 ※変更可能な内容については、[2.4.2.1 設定情報変更・管理の詳細]を参照願います。 ※当社およびネオメイト社による運用監視に必要な設定を対象とした設定変更は、お申込みできません。
	設定情報管理
	FW/UTM 機器の設定情報をネオメイト社センターで管理します。 設定情報の保存は、ネオメイト社よりリモートによる設定変更の都度、実施し、最大 2 世代を保管します。 ※設定変更は、お客様の申込に基づく設定変更の他に、その他運用保守サービスによる変更を含みます。

2.4.2.1 設定情報変更・管理の詳細

設定情報変更・管理にて、実施内容や変更が可能な内容を以下に示します。

項目		内容
セキュリティ管理		
	ファイアウォール の設定変更	ファイアウォールポリシーの設定変更として、追加・修正・削除を行います。 設定項目は下記内容が可能です。 ・ 通信方向 ・ 送信元アドレス ・ 宛先アドレス ・ サービス ・ アクション（許可もしくは、拒否） ・ アドレス オブジェクト
	アンチウイルス の設定変更	ファイアウォール内の追加動作として、アンチウイルスの設定変更を行います。 設定項目は下記内容が可能です。 ・ アクション（ 有効もしくは、無効 ）
	侵入検知 の設定変更	ファイアウォール内の追加動作として、侵入検知の設定変更を行います。 設定項目は下記内容が可能です。 ・ アクション（ 有効もしくは、無効 ）
	ロギング の設定変更	ファイアウォール内の追加動作として、ロギングの設定変更を行います。 設定項目は下記内容が可能です。 ・ アクション（ 有効もしくは、無効 ）
	FW/UTM 機器閲覧権限 の設定変更	FW/UTM 機器に閲覧するためのアカウント情報の設定変更を行います。 設定項目は下記内容が可能です。 ・ ログイン用のパスワード ・ ログイン可能な IP アドレス帯
運用保守		
	通知/連絡先 の設定変更	技術サポートとして、問合せされる FW/UTM 運用担当者様情報の登録変更を行います。 設定項目は下記内容が可能です。 ・ FW/UTM 運用担当者様情報
		月次レポートを送信する指定メールアドレスの設定変更を行います。 設定項目は下記内容が可能です。 ・ 月次レポートの送信先メールアドレス
		アンチウイルスおよび、侵入検知機能におけるインシデント検知時に送信する指定メールアドレスの設定変更を行います。 ・ インシデント通知メールの送信先アドレス

2.4.3. ファームウェア・ライセンス管理

ファームウェア・ライセンス管理について、以下に示します。

項目	内容	
ファームウェア管理	メーカである FortiNet 社のサポート方針に準じリリースされたファームウェアに対して、独自に動作確認を行ったファームウェアを提供します。 また、FW/UTM 機器のファームウェアのバージョンアップをお客さまに代わって実施します。 バージョンアップの要否については、ネオメイト社が判断を行います。 なお、ファームウェアのバージョンアップ時には FW/UTM 機器が再起動し、その間、通信ができなくなるためお客さまに事前に連絡を行った後に、作業を実施します。	
ライセンス管理	FW/UTM 機器でセキュリティ機能を利用するためのライセンスを提供及び FW/UTM 機器への適用を行います。	
	提供ライセンス	
	AntiVirus	アンチウイルス機能を有効とするライセンスを提供します。 本ライセンス適用により、最新エンジン、シグネチャが利用可能となります。
	NextGenerationFireWall	侵入検知機能を有効とするライセンスを提供します。 本ライセンス適用により、最新エンジン、シグネチャが利用可能となります。

2.4.4. ログ・レポート提供

ログ・レポート提供について、以下に示します。

項目	内容
ログ情報管理	FW/UTM 機器よりログを収集し、ネオメイト社センター側のログ管理サーバに保管すると共に、お客さまからのご要望に基づき、ログファイルの提供を行います。 ※ 受付は、電話もしくはメールで行います。 ※ ログ保存期間は2ヶ月間、ネオメイト社にて保管します。 ※ ログファイルは、テキスト形式で圧縮して提供します。 ※ お客さま毎に FW/UTM 機器に設定したポリシーに基づいたログ出力とします。 【御提供ログの種類】 (1) イベントログ　(e.log) ・ FW/UTM 機器のシステムイベントログ ・ エンジン、シグネチャのアップデートログ 等 (2) トラフィックログ　(t.log) ・ 違反トラフィックログ ・ ファイアウォール機能による取得ログの一覧 通信拒否におけるブロック(破棄)　: deny ・ セキュリティイベントログ ・ アンチウイルス機能によるログ 検出時におけるブロック(破棄)　: blocked 検出時における通信許可　: passthrough ※1 ・ 侵入検知によるログ 検知時におけるブロック(破棄)　: dropped ※2 検知時における通信リセット　: reset ※3 検知時における通信確立　: detected ※4 ※1 pasthrough　: ファイルサイズ 10MB 超過時における出力ログとなり、アンチウイルス機能は非検査となります。 ※2 dropped　: 不正通信のブロック(破棄)時における出力ログとなります。 ※3 reset　: 不正通信のブロック(破棄)かつ、通信先のホストに対しリセット・パケット送出時における出力ログとなります。 ※4 detected　: 不正通信の検知時における出力ログとなり、通信そのものは正常に行われます。(検知のみで防御措置は取りません。)
月次レポート	FW/UTM 機器の稼動状況について、月単位でその内容を集計し、レポートとしてお客さまに提供いたします。 レポートはロギング機能で取得した情報を元に生成いたします。 月次レポートの送信は以下内容で実施します。 送信時期 ： 毎月、中旬までのメール送信を目途とします。 送信方法 ： 申し込み時に記載いただいている担当者様にメールで送信します。 ※ 詳細は、[2.4.4.1.月次レポートの詳細]を参照願います。

2.4.4.1. 月次レポートの詳細

月次レポート内容について、以下に示します。

項目	内容
(1) 通信帯域使用量と利用アプリケーション	
総通信量の推移	時間単位での通信の送受信量を表示します
総セッション数の推移	時間単位での総セッション数を表示します
使用帯域が多い上位アプリケーション	期間内の通信量が多いアプリケーションのトップ 10 を表示します
セッション数が多い上位アプリケーション	期間内のセッション数が多いアプリケーションのトップ 10 を表示します
使用帯域が多い上位ユーザー	期間内の通信量が多いユーザーのトップ 10 を表示します
セッション数が多い上位ユーザー	期間内のセッション数が多いユーザーのトップ 10 を表示します
使用帯域が多い上位宛先	期間内の通信量が多い通信先のトップ 10 を表示します
セッション数が多い上位宛先	期間内のセッション数が多い通信先のトップ 10 を表示します
利用ユーザー数の推移	時間単位での通信ユーザー数を表示します
(2) Web 利用状況	
Web 利用の多いユーザ(上位 20)	期間内の Web 通信のリクエスト数が多いユーザーを表示します
Web 利用の多いカテゴリー(上位 20)	期間内の Web 通信のリクエスト数が多いカテゴリーを表示します
Web 利用の多いサイト(上位 50)	期間内の Web 通信のリクエスト数が多いサイトを表示します
Web 利用時間の多いユーザー(上位 10)	期間内の Web 通信の利用時間が多いユーザーを表示します
Web 利用時間の多いカテゴリー(上位 10)	期間内の Web 通信の利用時間が多いカテゴリーを表示します
Web 利用時間の多いサイト(上位 50)	期間内の Web 通信の利用時間が多いサイトを表示します
Web 通信量の多いユーザー(上位 20)	期間内の Web 通信の通信量が多いユーザーを表示します
Web 通信量の多いカテゴリー(上位 20)	期間内の Web 通信の通信量が多いカテゴリーを表示します
Web 通信量の多いサイト(上位 50)	期間内の Web 通信の通信量が多いユーザーを表示します
ブロック回数の多いユーザー(上位 20)	期間内の Web 通信のブロック数が多いユーザーを表示します
ブロック回数の多い Web カテゴリー(上位 20)	期間内の Web 通信のブロック数が多いカテゴリーを表示します
ブロック回数の多い Web サイト(上位 50)	期間内の Web 通信のブロック数が多いサイトを表示します
(3) Emails 利用状況	
Email 送信数が多い上位ユーザー	期間内のメール送信数が多いユーザーを表示します
Email 受信数が多い上位ユーザー	期間内のメール受信数が多いユーザーを表示します
Email 総送信サイズが大きい上位ユーザー	期間内のメール送信の通信量が多いユーザーを表示します
Email 総受信サイズが大きい上位ユーザー	期間内のメール受信の通信量が多いユーザーを表示します
(4) 検出/検知された脅威	
検知したマルウェア	検知したマルウェアとその送信元を表示します
マルウェアのターゲットとなったユーザー	マルウェアのターゲットとなったユーザーを表示します
マルウェアの送信元とターゲット	マルウェアのターゲットと送信元を表示します
検知したボットネット	検知したボットネットを表示します
ボットネットの被害者	ボットネットの被害者を表示します
検知された C&C(指令)サーバ	ボットネットの C&C サーバのアドレスを表示します
検知した侵入行為	攻撃の内容を表示します
侵入行為のターゲットとなったユーザー	攻撃の対象となったユーザーを表示します
侵入行為の送信元	攻撃の送信元のアドレスを表示します

項目	内容
（5）ログイン履歴とシステムイベント	
ログイン履歴	機器にログインした情報の履歴を表示します
ログイン回数の推移	期間内のログイン回数の推移を表示します
ログインの失敗履歴	期間内のログイン失敗回数の推移を表示します
重要度別イベントの割合	期間内に発生したイベントについて、重要度別にグラフ表示します
イベント数の推移	期間内に発生したイベントについて、その数の推移を表示します
重要なイベント一覧（重要度 = Critical）	期間内に発生した重要度の極めて高いイベントの一覧を表示します （Crtical： UTM が認識する 5 段階中、5 となる最も高いレベル ）
重要なイベント一覧（重要度 = High）	期間内に発生した重要度の高いイベントの一覧を表示します （High： UTM が認識する 5 段階中、4 となる高いレベル ）
重要なイベント一覧（重要度 = Medium）	期間内に発生した重要度のあるイベントの一覧を表示します （Medium： UTM が認識する 5 段階中、3 となる中間レベル ）

※ 取得対象ログが 0 件の際は、「 適合するログデータが指定期間内に存在しません 」にてレポート上に出力いたします。

3. 主な設定パラメーター覧

主要な設定パラメータについて、以下に示します。

機能	設定パラメータ	備 考
システム		
ホスト名	[当社指定文字列となります]	お客さまにてご指定いただくことができません。
管理者権限	[お客さまはログインできません]	管理権限はお客さまへ委譲できませんことご了承願います。
言語設定	日本語	お客さまにてご指定いただくことができません。
自動アップデート	60 分間隔	お客さまにてご指定いただくことができません。 (UTM セキュリティの最新版を自動適用する間隔になります。)
ファイアウォール		
ポリシー	通信方向 送信元アドレス 宛先アドレス サービス アクション (アンチウイルス 機能の適用 ※) (侵入検知 機能の適用 ※) (ロギング 機能の適用 ※)	お客さま指定可能パラメータ(設定シートに基づき、設定いたします。) ※ アンチウイルスおよび、侵入検知、ロギング機能はポリシー内の 1 行単位で適用(有効/無効)をご指定いただけます。
	スケジュール ポリシー適用可否(有効/無効) コメント	お客さまにてご指定いただくことができません。
アドレス・オブジェクト	名前(以下、オブジェクト名) タイプ アドレス ※ インタフェース コメント	お客さま指定可能パラメータ(設定シートに基づき、設定いたします。) ※ アドレスは、選択したタイプに応じて以下 3 種類が投入可能です。 ・ サブネット/IP 範囲:IP/ネットマスク・IP 範囲タイプ選定時 ・ FQDN : FQDN タイプ選定時 ・ 国 : 地域 タイプ選定時
	アドレスリストへの表示	お客さまにてご指定いただくことができません。 表示する(チェックあり)にて設定いたします。
アドレス・グループオブジェクト	名前(以下、グループ名) メンバー コメント	
	アドレスリストへの表示	お客さまにてご指定いただくことができません。 表示する(チェックあり)にて設定いたします。
アンチウイルス		
適用モード	高精査モード (プロキシモード)	お客さまにてご指定いただくことができません。 プロキシモードは、FW/UTM 機器を通過するファイルを再構築したのちに検査する高検出精度のモードになります。

機能		設定パラメータ	備 考
	ウイルス検出時	破棄(ブロック)	お客さまにてご指定いただくことができません。
	対応プロトコル	HTTP(TCP: 80 ・ TCP:11180) SMTP(TCP: 25 ・ TCP: 587) POP3(TCP:110) IMAP(TCP:143) FTP (TCP: 21)	お客さまにてご指定いただくことができません。
	最大検知ファイルサイズ	10 MB	お客さまにてご指定いただくことができません。 サイズ超過時は検知対象外となります。 ファイルサイズは非圧縮時のものとなります。
	圧縮ファイルへの対応	全ての主要圧縮ファイルを検知可能	お客さまにてご指定いただくことができません。
侵入検知			
	検知レベル ※ 凡例 ☑:検知する ☐:検知しない	☑ 極高(Critical) ☑ 高 (High) ☑ 中 (Middle) ☐ 低 (Low) ☐ 情報(Information)	お客さまにてご指定いただくことができません。 (検知レベルは侵入時の危険性を示し、全てを検知対象とするとリソースを大幅に使用するため、低レベル以下の攻撃は対象外としております。)
	ターゲット	すべて	お客さまにてご指定いただくことができません。 FortiNet 社指定のホスト、アプリケーション、プロトコル定義に準じます。
	OS	すべて	お客さまにてご指定いただくことができません。 FortiNet 社指定の OS 定義に準じます。
	アクション	[デフォルト設定]	お客さまにてご指定いただくことができません。 シグネチャ毎のデフォルトのアクション(「 モニタ(検知のみ) 」・「 ブロック(破棄) 」・「 リセット(破棄しリセットパケット送出) 」「 隔離(デフォルト設定では該当無し) 」)を継承します。
	パケットロギング	無効	お客さまにてご指定いただくことができません。 FW/UTM 機器の冗長構成時における重複ログを発生させないためのオプションであり、ロギング機能との依存関係はございません。
	レートベースシグネチャ	適用なし	お客さまにてご指定いただくことができません。 DoS/DDoS のように通信の絶対量が問題となる攻撃に対し、通信量に閾値を設けて防御する機能。
ロギング機能			
	保存先	ネオメイト社センターへ配信	指定値につき、お客さまにてご指定いただくことができません。 万一の紛失に備え、ネオメイト社センターで保存しております。

機能		設定パラメータ	備 考
	取得ログ ※ 凡例 ☑:取得する ☐:取得しない	☑ 違反トラフィックログ ※1 ☑ セキュリティイベントログ ※2 ☑ イベントログ ※3 ☐ ローカルトラフィックログ ※4	指定値につき、お客さまにてご指定いただくことができません。 ※1 違反トラフィックログは拒否(Deny)対象となったポリシーにおいて、ロギング対象としたもののみ取得します。 ※2 セキュリティイベントログはポリシーで UTM セキュリティのロギング対象としたもののみ取得します。 ※3 イベントログはシステムの稼動状況を記したものになります。 ※4 ローカルトラフィックログは、FW/UTM 機器自身が受発信した通信状況を記すものであるため、取得対象外とします。
ご利用者様向け ログイン権限			
	ログイン・アカウント	アカウント	お客さまにてご指定いただくことができません。 [user-admin]の文字列固定となります。
		パスワード	お客さま指定可能パラメータ(設定シートに基づき、設定いたします。)
	閲覧制限	閲覧可能な IP アドレス帯	お客さま指定可能パラメータ(設定シートに基づき、設定いたします。)
	接続可能プロトコル	HTTPS のアクセス許可	お客さまにてご指定いただくことができません。
	制約事項	読取り権限	お客さまにてご指定いただくことができません。

4. 注意事項

- 本サービスで提供する機能は本仕様書に明記したものに限らせていただきます。FortiGate、FortiWiFi シリーズは各種機能を実装していますが、本サービスにおいては、ご利用できない機能がありますことご了承ください。
- FortiGate および FortiWifi は FortiNet社の登録商標です。
- 各種セキュリティ対策を FW/UTM 機器で実施するため、ご利用状況により通信速度が低下する場合があります。

（例：2.2.1.提供モデルに記載のスループットが出ない場合）

【設定が要因となる場合】

・IPS およびアンチウイルスの両方を有効にした場合

・ポリシーの数が多い場合　　等

【利用用途が要因となる場合】

・複数の宛先を指定することによりメール送信が大量になる場合（メーリングリストにメールを送る場合）

・メールにファイルを添付した場合

・web アクセスが集中した場合　　等

- 各種セキュリティ対策により、正常な通信を遮断する場合があります。
- 全ての攻撃に対する防御を保証するものではありません。
- 新種のウイルスなど FW/UTM 機器で対応できないウイルスや攻撃により、お客さまの環境に影響が発生した場合、当社およびネオメイト社は責任を負いません。
- 設定情報シート、設定変更シートへの記述誤りなどの不備により、お客さま環境に影響を及ぼした場合、当社およびネオメイト社は責任を負いません。
- 回線障害や機器故障、システムメンテナンスなどにより、ログ情報が欠損する場合があり、ログ収集の全てを保証するものではありません。
- システムの更新、メンテナンス等により、お客さまのサービスに影響が発生する場合は事前にご案内をいたします。 但し、緊急の場合には、事前に通知することなく、メンテナンス作業を行うことがあります。
- 平日は祝祭日および、当社指定休日の年末年始 3 日を除く、月曜日から金曜日になります。

5. お申込み（新規・解約・変更）

5.1. 開始までの所要期間

開通までの所要期間は以下のとおりとなります。

所要期間は、0 営業日目（必要事項が全て記載された申込を当社で受け付けた営業日）からの日数となります。

サービス	ご提供までの所要期間	備考
ファイアウォール/UTM	25 営業日目以降の指定日 ※土日祝日、年末年始を除く	・お申込み前に、FW/UTM 機器に収容する物理専用タイプのサーバが開通している必要があります。 ・在庫状況によって 25 営業日以上必要となることがあります

5.2. 変更までの所要期間

変更までの所要期間は以下のとおりとなります。

所要期間は、0 営業日目（ネオメイト社が受付番号（SR 番号）のメール送信を実施し、かつ設定変更内容に関してお客さまとネオメイト社にて合意した営業日）からの日数となります。

サービス		ご提供までの所要期間	備考
ファイアウォール/UTM	設定情報変更	2 営業日以内 ※土日祝日、年末年始を除く	―

5.3. 解約までの所要期間

解約までの所要期間は以下のとおりとなります。

所要期間は、0 営業日目（必要事項が全て記載された申込を当社で受け付けた営業日）からの日数となります。

サービス	ご提供までの所要期間	備考
ファイアウォール/UTM	20 営業日目以降の指定日 ※土日祝日、年末年始可	・ファイアウォール/UTM 解約時、FW/UTM 機器に収容している物理専用タイプのサーバは、すべて解約となります。

5.4. 開始までの流れ

サービス開始までの流れは以下のとおりとなります。

1. オプションサービスの確認　　お客さま

ファイアウォール/UTM のサービス内容について、あらかじめサービス仕様書、
ファイアウォール/UTM オプション仕様書、利用規約、料金表をご確認ください。

2. 設定情報シートの記入　　お客さま

設定情報シートをコントロールパネルよりダウンロードし、ご記入の上、当社まで送付ください。
当社にて、設定情報シートの記入漏れ等、不備がないか確認させていただきます。

3. お申込み可能ご連絡　　当社

設定情報シートについて、記入漏れ等の不備がないことが確認できましたら、
ご連絡させていただきます。

4. ファイアウォール/UTM お申込み（0 営業日目）　　お客さま

コントロールパネルより、表示されるフォームに必要事項をご記入の上、お申込みください。
本受付にてお申込み受理となり、受理後のキャンセル/変更はできませんのでご注意ください。
当社より受け付けた内容の確認メール送付いたします。
※開通日に、10:00～15:00 の時間帯で、ファイアウォール/UTM に収容するサーバの停止（30 分程度）が伴いますので、開通日はご利用に支障のない日時をご指定ください。

5. ファイアウォール/UTM の設置・設定　　当社

ファイアウォール/UTM をご利用いただけるように設置・設定作業を行います。

6. ファイアウォール/UTM の開通（最短で 25 営業日目）　　当社

お申込み時にご指定いただいた開通日に、ご指定いただいた物理専用タイプのサーバを
ファイアウォール/UTM に収容する工事を実施します。
工事完了後、当社からお客さまに通知いたします。

5..5. 変更までの流れ

変更までの流れは以下のとおりとなります。

1. 現状の設定、FW/UTM お客様 ID の確認　お客さま

ファイアウォール/UTM 管理画面より、現状の設定をご確認ください。
また、受付時にお客さま確認として、[FW/UTM 運用担当者様情報]と
[FW/UTM お客様 ID]を確認させていただいております。あらかじめ、ご確認をお願いいたします。

2. 設定変更シートの記入　お客さま

設定変更シートをコントロールパネルよりダウンロードし、ご記入の上、
ネオメイト社（CC：当社）まで送付ください。
ネオメイト社にて、設定変更シートの記入漏れ等、不備がないか確認させていただきます。

3. SR 番号、設定変更予定日の通知（0 営業日目）　ネオメイト社

設定変更シートについて、記入漏れ等の不備がないことが確認できましたら、
SR 番号および設定変更予定日をご連絡させていただきます。

4. ファイアウォール/UTM の設定変更（0～2 営業日目）　ネオメイト社

設定変更シートに基づき、ファイアウォール/UTM の設定変更を実施します。
工事完了後、ネオメイト社からお客さまに通知いたします。

5..6. 解約までの流れ

サービス解約までの流れは以下のとおりとなります。

1. オプションサービスの確認　お客さま

ファイアウォール/UTM のサービス内容について、あらかじめサービス仕様書、
ファイアウォール/UTM オプション仕様書、利用規約、料金表をご確認ください。

2. 解約申込書の記入　お客さま

解約申込書を、ご記入の上、当社まで送付ください。

3. 解約のお申込み（0 営業日目）　当社

解約申込書について、記入漏れ等の不備がないことが確認できましたら、
解約のお申込みを受理いたします。

4. ご解約（最短で 20 営業日目）　お客さま

ご解約以降、ファイアウォール/UTM がご利用できなくなります。
※ご解約日の翌日以降に停止処理をするため、一時的にご利用可能な場合があります。

6. サポート ／ お問い合わせ

本オプションに関するお問い合わせ先を、以下に示します。

<table>
<tr><th>お問い合わせ内容</th><th colspan="3">お問い合わせ先</th></tr>
<tr><td rowspan="6">・サービス内容
・お申込み（新規・解約）
・故障</td><td colspan="3">NTT スマートコネクト</td></tr>
<tr><td rowspan="3">受付時間</td><td>電話</td><td rowspan="4">「スマートコネクト マネージドサーバ サービス仕様書」をご確認ください。</td></tr>
<tr><td>メール</td></tr>
<tr><td>FAX</td></tr>
<tr><td colspan="2">電話番号</td></tr>
<tr><td colspan="2">メールアドレス</td></tr>
<tr><td colspan="2">補足</td><td>ー</td></tr>
<tr><td rowspan="7">・インシデント通知
・技術サポート
・設定情報変更・管理
（お申込み（変更））
・ログ情報管理
・月次レポート</td><td colspan="3">NTT ネオメイト IT ビジネス本部 サービス推進部 BC-SOC</td></tr>
<tr><td rowspan="3">受付時間</td><td>電話</td><td>平日 9:00～17:30</td></tr>
<tr><td>メール</td><td>24 時間 365 日
※回答はネオメイト社営業時間に限ります</td></tr>
<tr><td>FAX</td><td>ー</td></tr>
<tr><td colspan="2">電話番号</td><td rowspan="2">ご契約後にご連絡いたします。</td></tr>
<tr><td colspan="2">メールアドレス</td></tr>
<tr><td colspan="2">補足</td><td>・受付時にお客さま確認として、[FW/UTM 運用担当者様情報]と[FW/UTM お客様 ID]を確認させていただいております。あらかじめ、ご確認をお願いいたします。

・設定変更について(再掲)
ネオメイト社より受付番号(SR 番号)のメール送信を実施しかつ、設定変更内容に関してお客さまとネオメイト社にて合意した日を 0 営業日目とし、2 営業日目以内で設定変更を実施します。</td></tr>
</table>

変更履歴

版数・日付	変更理由	変更内容
1.0 版（2015.09.14）		
1.1 版（2016.6.23）	サービス内容の詳細化 対応サービス（マネージドサーバ）の追加	
2.0 版（2018.4.20）	提供機種の変更により改版	提供機種を「FortiWiFi 90D」から「FortiGate90E」に変更
3.0 版（2018.12.21）	新規販売停止	FW/UTM オプションサービスの新規販売停止を明確化
4.0 版（2020.3.31）	スマイルサーバ（専用サーバ）サービス終了	スマイルサーバ（専用サーバ）のサービス終了に伴い、スマイルに関連する項目を全て削除