1　本書の位置づけ

本書は株式会社エヌ・ティ・ティピー・シーコミュニケーションズ(以下「当社」といいます)が Security BOSS シリーズのゲートウェイ・セキュリティ運用監視サービス及びオプションサービス(以下「本サービス」といいます)の機能や提供条件についてご説明するものです。提供条件の詳細は利用規約のとおりといたします。

2　用語説明

本書に記載している用語は以下の通りに定義します。

障害:障害とは、今までできていた通信ができなくなった場合、通るべき通信が通らなくなった場合を指します。
平日:祝日、年末年始(12 月 29 日～1 月 4 日)、9 月 4 日を含む週の金曜日をのぞく月曜日～金曜日となります。
お客さま:本サービスのお客さまを指します。
ルーターモード:ブリッジインターフェースを作らない構成を指し、機器の全てのインターフェースがそれぞれ異なるネットワークに属するような構成となります。
ブリッジモード:ブリッジインターフェースを利用する構成を指し、DMZ なしの場合は WAN インターフェースと LAN インターフェースが、DMZ ありの場合は WAN インターフェースと DMZ インターフェースが、ブリッジインターフェースとして共通の IP アドレスを持つ構成です。
Up2date サイト:ゲートウェイ装置がウイルスパターンやシグネチャのアップデートを行うためのサーバです。

3　サービス概要

本サービスは当社が提供するゲートウェイ・セキュリティの運用監視サービス及びオプションサービスです。本サービスでは、お客さまネットワークとインターネットの境界、もしくはお客さまネットワーク内にゲートウェイ装置を設置し、そのゲートウェイ装置を当社内セキュリティ・オペレーション・センタ(以下「SOC」といいます)から遠隔監視・運用することにより提供いたします。

サービス構成、概要図は以下のとおりとなります。

【サービス構成】

(1) 基本機能	(2) セキュリティ機能	(3) オプション機能
・24 時間 365 日死活監視 　-監視不具合検知時の SOC からの電話連絡及び受付 　-監視不具合検知時の SOC からのメール連絡 　-お客さまからの障害申告受付・対応 　-技術問い合わせ対応 ・24 時間 365 日駆け付け交換保守 ・先出しセンドバック保守 ・月次レポート ・対応レポート	・ファイアウォール ・侵入検知・防御(IPS) ・アプリケーションコントロール ・Web アンチウイルス ・アンチスパイウェア ・URL フィルタリング ・メールアンチウイルス ・メールアンチスパム・アンチフィッシング ・出口対策	・オンライン・ストレージ

基本機能:機器の運用や保守に関連して提供するサービス機能です。
セキュリティ機能:機器が本来具備している機能を用いて提供するサービス機能です。
オプション機能:オプションとして、別途契約可能なサービス機能です。

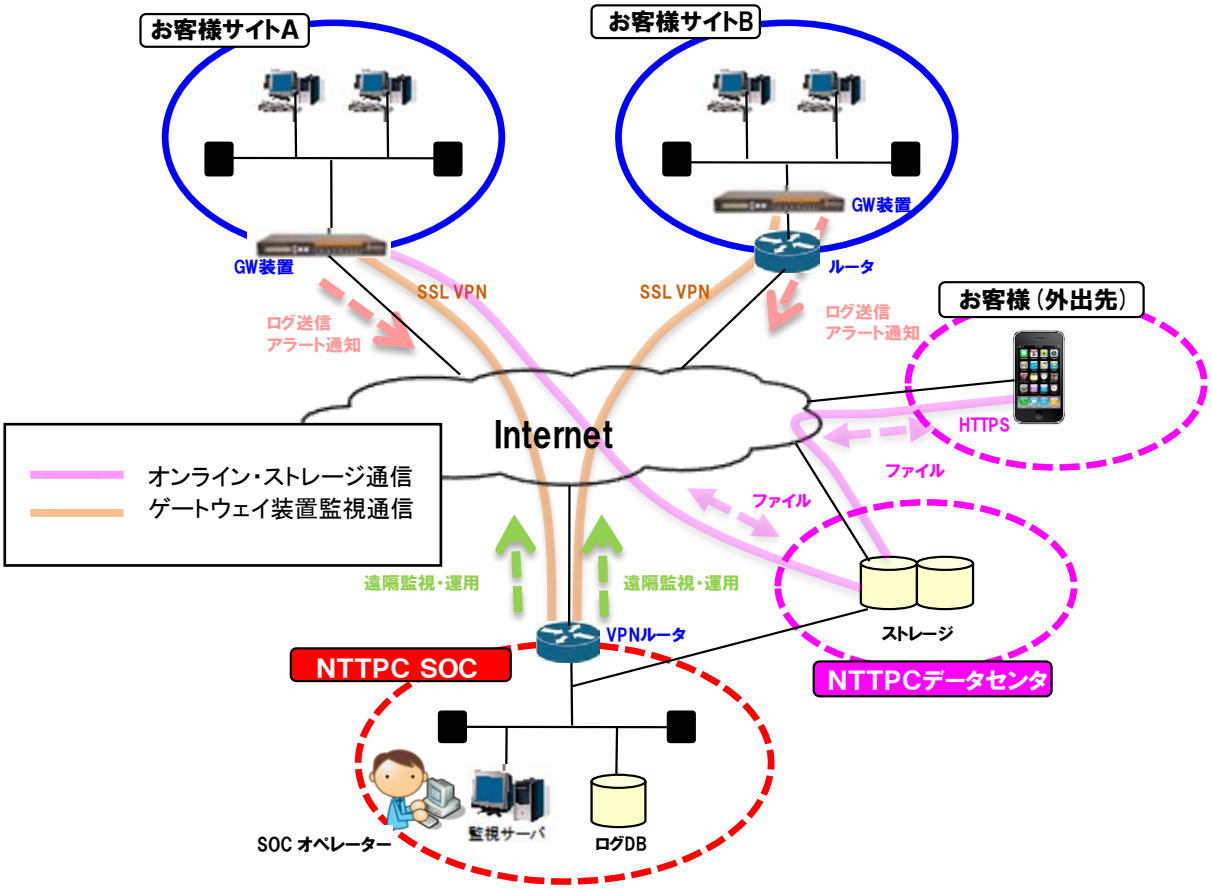

図 3-1　サービス概要図

3.1　サービスプラン

3.1.1　提供形態

本サービスのプラン別提供形態は表 3-1 のとおりです。提供プランにより利用する機種、提供形態、提供機能が異なります。
サービスプラン：想定収容クライアント数や提供機能によって変わります。
サービスコース：ゲートウェイ装置の機器本体をご購入されるか、レンタルにてご利用されるかを選べます。
提供形態：ゲートウェイ装置がルータまたはブリッジとして動作するかと、ゲートウェイ装置で DMZ を作るかによって 4 つの形態に分かれます。詳細は「3.3.4 ゲートウェイ装置の提供形態」をご覧ください。
提供構成：サービスプランによっては二重化を選択できます。詳細は「3.3.4.5 二重化構成」をご覧ください。

表 3-1 サービス提供形態表

サービス プラン	サービスコース		提供形態				提供構成		想定収容 クライアント数 （※注意 1）
	レンタル	買取	パターン 1	パターン 2	パターン 3	パターン 4	シングル	二重化	
ライト・オンデマンド・ネクスト	●	●	―	―	●	―	●	―	ゲートウェイ装置 によります
ライト・オンデマンド 10	―	●	―	―	●	―	●	―	10 端末まで
ライト・オンデマンド 30	―	●	―	―	●	―	●	―	50 端末まで
ライト 10	●	●	―	―	●	―	●	―	10 端末まで
ライト 30	●	●	―	―	●	―	●	―	50 端末まで
ベーシック	●	●	●	○	●	○	●	●	200 端末まで[旧] 500 端末まで[新]
スタンダード	●	●	●	●	●	●	●	●	500 端末まで
ハイエンド	●	●	●	●	●	●	●	●	1,000 端末まで

●：提供　　○：別途オプションの契約にて提供　　―：未提供
※　注意 1：トラヒックの状況によって想定収容クライアント数が少なくなる場合がございます。

3.1.2 提供機能

本サービスのプラン別提供機能は表 3-2 のとおりです。
提供機能はサービスプラン別に以下の組み合わせになります。

- ♦ レンタルコースの場合、本サービスとして基本機能、セキュリティ機能、オプション機能を合わせて提供いたします。
- ♦ 買取コースの場合、本サービスでは基本機能のみを提供し、セキュリティ機能はお客さまにご購入いただいたゲートウェイ装置の持っている機能をご使用いただくことが可能となります。

表 3-2 プラン別提供機能表

機能		ライト・オンデマンド・ネクスト	ライト・オンデマンド	ライト		ベーシック	スタンダード	ハイエンド
			10/30	10	30			
基本機能	24 時間 365 日死活監視	●	●	●	●	●	●	●
	監視不具合検知時の SOC からの電話連絡および受付 ※	平日 9 時～17 時		24 時間 365 日				
	監視不具合検知時の SOC からのメール連絡	24 時間 365 日						
	お客さまからの障害申告受付・対応	平日 9 時～17 時		24 時間 365 日				
	技術問合せ受付	平日 9 時～17 時		24 時間 365 日				
	24 時間 365 日駆け付け交換保守	ー	ー	ー	○	○	●	●
	先出しセンドバック保守	●	●	●	△	△	ー	ー
	月次レポート	●	●	●	●	●	●	●
	対応レポート	ー	ー	ー	ー	●	●	●
セキュリティ機能	ファイアウォール	●	●	●	●	●	●	●
	侵入検知・防御(IPS)	ー	ー	ー	ー	○	●	●
	アプリケーションコントロール・ファイル転送アプリケーション検知	●	●	●	●	●	●	●
	WEB アンチウイルス	●	●	●	●	●	●	●
	アンチスパイウェア	●	●	●	●	●	●	●
	URL フィルタリング	●	▲	▲	▲	○	●	●
	メールアンチウイルス	●※1	●	●	●	●	●	●
	メールアンチスパム・アンチフィッシング(注)	●※1	●	●	●	●	●	●
	出口対策	●	ー	ー	ー	ー	ー	ー
オプション機能	オンライン・ストレージ	ー	●	●	●	ー	ー	ー

●:提供　○:別途オプション契約にて提供　△:別途オプション契約がない場合に提供　▲一部機能のみ提供　ー:未提供
※大規模な範囲で障害が発生した場合は、伝達速度を重視し、メールにて連絡することもございます。あらかじめご了承ください。
※1　一部機種（SSB5/10/20/30/80）、POP3s セキュリティ機能を提供する。ただし、SSB5 においてはメールアンチウイルスのみを POP3s セキュリティ機能を提供する。利用規約やマニュアルに特別な記載ががない限り、POP3s セキュリティ機能は POP3 と同等程度に動作するものとする

注:ライト・オンデマンド・ネクストプランの場合、当社が別に定める一部のゲートウェイ装置では「メールアンチスパム」はご利用できません。

3.2 サービス内容

3.2.1 基本機能

基本機能はサービスに付随し、提供いたします。
※ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30、ベーシックプランでは一部基本機能の提供に制限がございます。

提供される基本機能は表 3-3 のとおりです。

表 3-3 基本機能一覧表

機能	内容
24 時間 365 日死活監視	ゲートウェイ装置が動作しているかの死活監視を IP レベルで実施しております。設定された死活監視の閾値を超えた場合、監視サーバはアラートを通知します。SOC 担当者はアラート内容を確認し、お客さまへの連絡対応を行います。
監視不具合検知時の SOC からの電話連絡および受付 ※注意 2	機器の監視に不具合を検知した時、SOC からお客さまへ電話連絡し、通信が可能かどうかの確認をいたします。その上でお客さまの通信に障害が発生していた場合には、障害の切り分けや技術的対処を行います。電話連絡の有無は弊社指定の時間枠の中で選択する事ができます。
監視不具合検知時の SOC からのメール連絡	機器の監視に不具合を検知した際、SOC からお客さまへシステムを利用して自動的にメールで連絡をいたします。24 時間 365 日問わず監視不具合を検知した際に、頂いた連絡先宛てに通知されます。
お客さまからの障害申告受付・対応 ※注意 2	お客さまから障害の申告をいただいた場合、ご申告の障害に関して切り分けや技術的対処を行います。
技術問合せ受付 ※注意 2	機器仕様や提供機能等、サービスに関連する技術的な問合せを受付いたします。お問合わせの内容によっては、翌営業日での対応となる場合がございます。
24 時間 365 日駆け付け交換保守	障害発生時、障害の切り分けを行い、ゲートウェイ装置に問題があると判断された場合、保守要員がお客さまのゲートウェイ装置の交換対応を行います。
先出しセンドバック保守 ※注意 3	SOC より交換用のゲートウェイ装置をお客さまに送付いたします。装置到着後、お客さまにて交換対応を実施していただき、交換後の故障機は弊社宛てに送っていただきます。
月次レポート ※注意 4	ゲートウェイ装置が、機器に到達したトラフィックを処理した結果を 1 ヶ月毎に集計し、NTTPC 独自のレポートの形でお客さま担当者へ提供いたします。
対応レポート ※注意 4	SOC のお客さま対応履歴を 1 ヶ月毎にレポートの形で報告いたします。ベーシックプラン、スタンダードプラン、ハイエンドプランで提供いたします。

※注意 2:
ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30 プランの場合、対応時間は平日 9 時～17 時に限らせていただきます。それ以外の時間で発生した監視不具合検知や各種ご申告などに対しては、翌営業日の 9 時～17 時での対応とさせていただきます。

※注意 3:
機器の送付は平日 9 時-15 時での対応(正午までの受付は当日発送、以降は翌営業日発送)となります。送料に関しては、送り元負担とさせていただきます。(交換用の機器をお客さま先へ送付するのは弊社負担、故障品を弊社宛てに送り返すのはお客さま負担となります。)

※注意 4:
提供形式は、弊社ダウンロードサイトからお客さま自身でダウンロードしていただく形となります。

3.2.2 基本機能での監視・運用・保守

お客さまネットワーク内に設置したゲートウェイ装置の監視・運用を 24 時間 365 日、当社内 SOC が提供いたします。ゲートウェイ装置を遠隔にて監視・運用を行うため、ゲートウェイ装置と弊社監視設備との間で VPN を構築します。詳細は「3.3.5.1 VPN 接続」をご覧ください。

(1) 監視
基本機能である「24 時間 365 日死活監視」にて対応いたします。表 3-3 をご参照ください。

(2) 障害対応
SOC にて監視不具合を検知した場合、およびお客さまからの障害申告を受けて、ゲートウェイ装置に障害が発生しているかの切り分けを SOC 担当者が行います。なお、切り分けの際にはお客さまにご協力をいただく事もございます。

(3) 保守対応
障害対応によりゲートウェイ装置に問題があると判断された場合、提供している保守サービスにより以下のいずれかの対応を実施いたします。

-24 時間 365 日駆け付け交換保守
-先出しセンドバック保守

(4) 問い合わせ
基本機能である「技術問合せ受付」にて対応いたします。表 3-3 をご参照ください。

3.2.3 セキュリティ機能

ゲートウェイ装置が持つセキュリティ機能を使用し提供いたします。

♦ 表 3-4 の 8 つのセキュリティ機能の中から、お客さまが最低 1 つ以上の機能を選択されることとなります。
※ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30、ベーシックプランでは提供するセキュリティ機能に一部制限がございます

- 選択したセキュリティ機能の設定は当社にてあらかじめ決められた初期値に基づきますが(初期値は参考資料参照)、お客さまから提出される変更オーダシートに基づき変更可能といたします。
- セキュリティ機能の変更を行う場合はお客さまからヒアリングシートを再提出いただくことで変更可能といたします。なお、ライト・オンデマンド・ネクストプランの場合、一部機能はお客さまにて変更可能となっております。

ゲートウェイ装置の持つセキュリティ機能は表 3-4 のとおりです。

表 3-4 セキュリティ機能一覧表

機能		内容
ファイアウォール		ゲートウェイ装置の内側と外側を流れるパケットを監視し、ルールに従ってパケットを制御します。 ➢ 不要なパケットの侵入を防ぎ、お客さまネットワークを保護いたします。 ※ 注意 5 ※ 注意 6 ※ 注意 7
侵入検知・防御(IPS)		ファイアウォールを通過したトラヒックを監視し、攻撃や異常行動を検知、制御を行います。 ➢ ファイアウォールを通過したパケットから、攻撃や異常行動を検知し、警告を行うとともに、サーバやネットワークへの不正侵入を防ぎます。 ※ 注意 8 ※ 注意 9 ※ 注意 10
アプリケーションコントロール・ファイル転送アプリケーション検知		ゲートウェイ装置を通過したトラヒックをモニターし、 • Instant Message (IM)系アプリケーション • Peer-to-Peer (P2P)系アプリケーション • Web メール系アプリケーション • クラウドストレージ系アプリケーション • SNS 系アプリケーション • ストリーミング系アプリケーション • リモートアクセス系アプリケーション を検知、制御を行います。 ➢ ゲートウェイ装置を通過したパケットから、該当アプリケーションの使用行動を検知し、警告を行うとともに、不特定多数との相互アクセスを検知し、アクセスの濫用を防ぎます。 ※ 注意 11
WEB アンチウイルス	HTTP HTTPS	クライアントが WEB アクセス実行時、アップロード/ダウンロードコンテンツをチェック • ウイルス を検知し、ゲートウェイ装置が WEB アクセスの遮断、クライアントへ警告を行います。 ➢ ダウンロードコンテンツ内にウイルスやワームその他悪意あるソフトが潜んでいないかをチェックし、クライアントが感染するのを防ぎます。 ※ 注意 12 ※ 注意 13 ※ 注意 14 ※ 注意 15 ※ 注意 16
	FTP	クライアントが FTP アクセス実行時、ダウンロードコンテンツをチェック • ウイルス を検知し、ゲートウェイ装置が FTP アクセスの遮断を行います。 ➢ ダウンロードコンテンツ内にウイルスが潜んでいないかをチェックし、クライアントが感染するのを防ぎます。 ※ 注意 12 ※ 注意 15 ※ 注意 17

表 3-4 セキュリティ機能一覧表(続き)

機能	内容	
アンチスパイウェア	HTTP HTTPS	クライアントが WEB アクセス実行時、ダウンロードコンテンツをチェック • スパイウェア を検知し、ゲートウェイ装置が WEB アクセスを遮断、クライアントへ警告を行います。 ➢ ダウンロードコンテンツ内にワームその他悪意あるソフトが潜んでいないかをチェックし、クライアントが感染するのを防ぎます。 ※ 注意 12 ※ 注意 13 ※ 注意 15 ※ 注意 16 ※ 注意 18
URL フィルタリング	HTTP HTTPS	クライアントが WEB アクセス実行時、URL をチェック • プロテクションカテゴリ(契約者がブロック指定したカテゴリ) に分類されている URL とマッチした場合、アクセスを遮断、クライアントへ警告を行います。 • ブラックリスト に指定されている URL とマッチした場合アクセスを遮断、クライアントへ警告を行います。 • ホワイトリスト に指定されている URL とマッチした場合、上記の条件を無視し、アクセスを許可します。 ➢ サイトへのアクセスを制御(許可・不許可)し、WEB アクセスの濫用を防ぎます。 ※ 注意 15 ※ 注意 16 ※ 注意 19
メールアンチウイルス	POP3 POP3s	あらかじめ定期的にゲートウェイ装置がメールを受信し、メールをチェック • ウイルス を検知、ゲートウェイ装置内に隔離を行います。 クライアントは 1 日 1 回(デフォルト)、または 2 回送付されるレポートを受信し、隔離されたメールの確認を行います。 ➢ メール本文、添付ファイル内にウイルスやワームその他悪意あるソフトが潜んでいないかをチェックし、クライアントがウイルスに感染するのを防ぎます。 ※ 注意 15 ※ 注意 20 ※ 注意 21 ※ 注意 25 ※ 注意 29
	SMTP	クライアントがメール送信実行時、またゲートウェイ装置の内側に配置されたメールサーバへメールリレー時、メールをチェック • ウイルス を検知、ゲートウェイ装置内に隔離を行います。 クライアントは 1 日 1 回(デフォルト)、または 2 回送付されるレポートを受信し、隔離されたメールの確認を行います。 ➢ メール本文、添付ファイル内にウイルスやワームその他悪意あるソフトが潜んでいないかをチェックし、ウイルスに汚染しているメールの着信を防ぎます。 （クライアントがウイルスに感染している場合、外部へウイルスメールが送信されるのを防ぎます） ※ 注意 15 ※ 注意 22 ※ 注意 23 ※ 注意 24 ※ 注意 25

表 3-4 セキュリティ機能一覧表(続き)

機能	内容	
メールアンチスパム･アンチフィッシング	POP3 POP3s	あらかじめ定期的にゲートウェイ装置がメールを受信し、メールをチェック • スパム • フィッシング を検知、設定値に基づきゲートウェイ装置が警告、または隔離を行います。 クライアントは 1 日 1 回(デフォルト)、または 2 回送付されるレポートを受信し、隔離されたメールの確認を行い、必要に応じてメールをゲートウェイ装置から受信します。 ➢ 不要なメールの受信を防ぎます。 ➢ クライアントが気づかずに重要な情報を奪われるのを防ぎます。 ※ 注意 15 ※ 注意 21 ※ 注意 25 ※ 注意 26 ※ 注意 29
	SMTP	ゲートウェイ装置の内側に配置されたメールサーバのメールリレー時、メールをチェック • スパム • フィッシング を検知、設定値に基づきゲートウェイ装置が警告、または隔離を行います。 クライアントは 1 日 1 回(デフォルト)、または 2 回送付されるレポートを受信し、隔離されたメールの確認を行い、必要に応じてメールをゲートウェイ装置から再送信します。 ➢ 不要なメールの送信、メールサーバへの着信を防ぎます。 ※ 注意 15 ※ 注意 23 ※ 注意 24 ※ 注意 25 ※ 注意 26 ※ 注意 27
出口対策		ゲートウェイ装置を通過するトラフィックをモニターし、異常なトラフィックを検知/ブロック ➢ ゲートウェイ装置を通過したパケットから、異常トラフィックを検知/遮断することにより、お客さまネットワーク外部への情報流出を防止します。 ※ 注意 28

※ 注意 5 : ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30 プランでのファイアウォールは 2 つのルールどちらかのみに対応しております。また、ライト・オンデマンド・ネクストプランの場合、当社が別に定めるゲートウェイ装置では、ルール 2 に外部から許可するトラフィックを指定することができます。
- ルール 1:全てのトラヒックを通過する
- ルール 2:LAN ネットワークからのトラヒックを通過する

※ 注意 6 : ライト・オンデマンド・ネクストプランの場合、当社が別に定めるゲートウェイ装置では IPv6 通信に対応します。
※ 注意 7 : ゲートウェイ装置に対する Ping、Traceroute はデフォルトで応答する設定になっており、パケットフィルタで応答を制御することや応答を無効にすることはできません。
※ 注意 8 :侵入検知・防御(IPS)による監視におきましては、ゲートウェイ装置の持つ初期設定にて『防御』(トラヒックの遮断)を行います。
※ 注意 9 : ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30 プランでは対応しておりません。ベーシックプランの場合、別途「フル機能オプション」をご契約いただくことで対応可能となります。
※ 注意 10 :侵入検知・防御(IPS)の設定変更を実施する際には最大 30 秒程度の通信断が発生する場合がございます。
※ 注意 11 : サービスプランにより対応するアプリケーションが異なります。(詳細は参考資料参考)
※ 注意 12 : ファイルをダウンロードする際、ファイルサイズ・転送速度によりダウンロード時間が 5 秒を超える場合、ブラウザにゲートウェイ装置のダウンロード画面が表示されます。
※ 注意 13 : スキャンを行うコンテンツサイズは 30M までとなります。それを超えるコンテンツについてはウイルススキャンを行いません。またトラヒックの状況によってゲートウェイ装置が高負荷となり、ダウンロードに失敗する場合がございます。
※ 注意 14 : デフォルト設定に当社が指定した一部のサイト(ウイルスパターンダウンロードサイトなど)がホワイトリストに登録されております。
※ 注意 15 : プロキシを利用してセキュリティ機能を実現するため、各種サーバへのアクセスはゲートウェイ装置の IP アドレスに書き代わって行われます。
※ 注意 16 : ライト・オンデマンド・ネクストプランの場合、当社が別に定めるゲートウェイ装置では HTTPS 通信および IPv6 通信に対応します。
※ 注意 17 : WEB アンチウイルスを選択すると FTP のスキャンが有効となります。スキャンを行うコンテンツサイズは 50M までとなります。それを超えるコンテンツについてはウイルススキャンを行いません。またトラヒックの状況によってゲートウェイ装置が高負荷となり、ダウンロードに失敗する場合がございます。
※ 注意 18 : スパイウェア検知はアンチスパイウェア以外にも WEB アンチウイルスでも行われております。アンチスパイウェ

ア設定を「無効」とした場合でも、WEB アンチウイルス機能に含まれて動作しているスパイウェア検知につきましては「無効」にできません。

※ 注意 19 : ライト・オンデマンド 10/30、ライト 10/30、ベーシックプランの場合、URL カテゴリによるフィルタリングは当社が指定した有害サイト(ウイルスサイト、フィッシングサイト)についてアクセスを遮断いたします。お客さまからの設定変更の運用には対応しておりません。
ライト・オンデマンド・ネクストの場合、お客さまがゲートウェイ装置の管理画面を利用して、当社が指定したサイトカテゴリ区分の範囲内でのカテゴリの選択・変更、およびブラックリスト・ホワイトリストの登録をすることができます。
ベーシックプランの場合、別途「フル機能オプション」をご契約いただくことで対応可能となります。
尚、ブラックリストによる個別サイトのブロックや、ホワイトリストによる個別サイトの許可などはすべてのプランにおいて共通してご利用いただけます。

※ 注意 20 : スキャンを行うメールサイズは、ライト・オンデマンド 10/30、ライト 10/30、ベーシック、スタンダード、ハイエンドプランの場合 2M(ヘッダ、本文、添付を含む)までとなります。また、ライト・オンデマンド・ネクストプランの場合も 2M ですが、当社が別に定めるゲートウェイ装置では 10M(ヘッダ、本文、添付を含む)までとなります。それを超えるメールについてはウイルススキャンを行いません。

※ 注意 21 : ゲートウェイ装置の POP3 プロキシ機能には以下のような制限がございます。また、ライト・オンデマンド・ネクストプランの場合、当社が別に定めるゲートウェイ装置では定期的なメール受信機能が提供されません。

- メールクライアントの設定に「サーバにメールを残す」を設定されている場合、下記のタイミングで既に受信したメールをゲートウェイ装置がメールサーバから再度受信を行います。そのため、ゲートウェイ装置及び、メールサーバで一時的に負荷の高い状態になる可能性がございます。
  1) ゲートウェイ装置導入時
  2) ゲートウェイ装置の交換保守時
  3) メール受信動作を 30 日以上行わない時
- ※ 上記によりメーラにすでに受信したメールが二重に取り込まれることはございません。
- ゲートウェイ装置は保存されているメールアカウント情報を基に 5 分間隔で定期的にメールを受信後、ウイルスチェックやスパムチェックを行います。クライアントはゲートウェイ装置が問題ないと判断したメールを受信します。
- メールサーバの「パスワード」を変更した場合、ゲートウェイ装置に保存されているパスワード情報はクライアントのメーラに設定されているパスワードが変更されるまで更新されません。そのため、メールサーバに新着したメールを受信できない場合がございます。
- スパムメールを検出時、「隔離」を選択した場合、ゲートウェイ装置はスパムメールと判定した当該メールを POP3 サーバから削除いたします。

※ 注意 22 : スキャンを行うメールサイズは 10M(ヘッダ、本文、添付を含む)までとなります。それを超えるメールについてはウイルススキャンを行いません。

※ 注意 23 : ゲートウェイ装置の SMTP プロキシ機能には以下のような制限がございます。

- 送信可能なメールサイズは 10M(ヘッダ、本文、添付を含む)までとなります。それを超えるメールサイズについては送信を行いません。
- お客さまのクライアントから他ドメイン宛てにメールを送信する場合、ゲートウェイ装置が設定値に基づき送信内容のチェックを行い、メールを配送します。このためお客さまドメインのメールサーバへログが残らなくなります。

※ 注意 24 : ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30 プランでのメールアンチウイルス、メールアンチスパムはメール受信時のみに対応しております。(メール送信時での検出には対応しておりません。)また、ライト・オンデマンド・ネクストプランの場合、当社が別に定めるゲートウェイ装置ではメールアンチスパム機能は提供されません。

※ 注意 25 : スパムのチェックを行うメールサイズは各プランのアンチウイルススキャン上限と同じとなります。それを超えるメールサイズについてはスパムのチェックを行いません。

※ 注意 26 : ゲートウェイ装置内に隔離したメールコンテンツの保管には以下のような制限がございます。詳細内容については「3.3.5.4 ゲートウェイ装置に隔離されたメールについて」に記述しております。

- 保管期間を経過したメールはゲートウェイ装置及びメールサーバ内から削除されます。
- メールコンテンツを保管するための容量には上限がございます。それを超える場合、保管期間経過前でもゲートウェイ装置及びメールサーバ内から削除されます。

※ 注意 27 : 他ドメイン宛にメールを送信することができるお客さまクライアントからのメール送信時は、スパムのチェックを行いません。

※ 注意 28 : 当社が指定した異常トラフィックの定義および適用ルールに基づき処理を行いますが、異常トラフィックの検知/ブロックや情報流出の防止を完全に保証するものではありません。

※ 注意 29 : POP3s のセキュリティ機能提供について、対象となる POP3s サーバは 1FQDN に限られます

3.2.4 セキュリティ機能の監視・運用

「3.2.2 セキュリティ機能」よりお客さまが選択された機能に対して、監視・運用を 24 時間 365 日、当社内 SOC が提供いたします。ゲートウェイ装置を遠隔にて監視・運用を行うため、ゲートウェイ装置と弊社監視設備との間で VPN を構築します。詳細は「3.3.5.1 VPN 接続」をご覧ください。

(1) 監視

1)24 時間 365 日 侵入監視

ゲートウェイ装置にて通信が IPS ルールとパターンマッチした場合、ゲートウェイ装置からアラートが通知されます。SOC 担当者はアラートの内容を確認し、検知したトラフィックの当日分を、翌営業日に契約担当者へメールにて連絡します。

2)アプリケーションコントロール・ファイル転送アプリケーション検知

ゲートウェイ装置にてトラヒックが検知可能なアプリケーションのルールとパターンマッチした場合、ゲートウェイ装置からアラートが SOC 宛に通知されます。SOC にてアラートの内容を集計し、1 日最大 2 回契約担当者へメールにて連絡します。

(2) 設定値の変更運用

ゲートウェイ装置に対し、変更オーダシートに基づいて SOC より遠隔にて設定変更対応を行います。
設定変更後、対応の完了をお客さま担当者へメールにて連絡します。

(3) ログの管理

ゲートウェイ装置から送付されるログを SOC 内の監視サーバが受信し、ログ DB に保管します。
ログは設定値に基づいて管理を行います。詳細な内容については「表 4-1 ゲートウェイ装置のログ一覧」に記述しております。

(4) 対応レポート、月次レポートの提供

サービス開通後、1 ヵ月毎に、以下のとおりレポートをお客さまへ提供いたします。こちらは、弊社のダウンロードサイトからお客さまにてダウンロードしていただく形となります。

1)対応レポート

1 ヶ月間 SOC が行ったお客さま対応の一覧を提供します。

2)月次レポート

ゲートウェイ装置毎に「表 3-4 セキュリティ機能一覧表」からお客さまが選択した機能について、1 ヶ月間の活動結果の一覧を提供します。

月次レポートの例を図 3-2 に記述します。当月分が翌月 10 営業日にダウンロード可能となります。

(5) 設定一覧表の提供

ゲートウェイ装置の設定一覧を提供いたします。対応レポート、月次レポート同様、弊社のダウンロードサイトからお客さまにてダウンロードしていただく形での提供となります。
変更オーダが発生した場合、設定変更対応後に最新の設定一覧がダウンロード可能となります。

セキュリティ機能別、監視・運用内容の一覧は以下の表 3-5 のとおりです。

表 3-5 監視・運用内容及び報告方法一覧表

機能	内容		報告形式
ファイアウォール	監視	ー	ー
	運用	• パケットフィルタルールの設定変更 • 通過、遮断パケットのログ管理	• 月次レポート • 設定一覧表
侵入検知・防御(IPS)	監視	• アラートの監視 • シグネチャルールのアップデートの監視	• 侵入検知・防御(IPS)のご連絡
	運用	• ルールの設定変更 • 攻撃検知時、連絡の対応 • 攻撃検知のログ管理	• 設定変更完了のご連絡 • 月次レポート • 設定一覧表
メールアンチウイルス WEB アンチウイルス アンチスパイウェア	監視	• ウイルスパターンのアップデートの監視	ー
	運用	• ウイルス、スパイウェア検知のログ管理 • 隔離レポートの送信	• 月次レポート
メールアンチスパム アンチフィッシング	監視	シグニチャルールのアップデートの監視	ー
	運用	• ホワイトリスト送信者の設定変更 • スパム検知時の動作設定変更 • スパム検知のログ管理 • 隔離レポートの送信	• 設定変更完了のご連絡 • 月次レポート • 設定一覧表
URL フィルタリング	監視	ー	ー
	運用	• プロテクションカテゴリの設定変更 • ホワイトリストの設定変更 • ブラックリストの設定変更 • URL フィルタ活動のログ管理	• 設定変更完了のご連絡 • 月次レポート • 設定一覧表
アプリケーションコントロール・ファイル転送アプリケーション検知	監視	• アプリケーション検知の監視 • ルールのアップデートの監視	• アプリケーションコントロール・ファイル転送アプリケーション検知のご連絡
	運用	• 対応アプリケーションの追加・変更 • アプリケーション検知時の動作設定変更 • アプリケーション検知時、連絡の対応 • ファイル転送アプリケーション検知のログ管理	• 月次レポート • 設定一覧表
出口対策	監視	• 該当通信の検知/ブロック	• 通信ブロックのご連絡(メール)
	運用	• 出口対策の動作設定変更(利用有無)	ー

図 3-2 月次レポートの例

3.2.5 オプション機能

(1) オンライン・ストレージ

当社データセンタ内にあるストレージを提供いたします。

- 1 申込に付き、管理者用アカウント 1ID、一般ユーザ用アカウントを最大 10ID まで払い出します。
- ストレージ申込容量は 100GByte 単位で増設することが可能で、100GByte～1000GByte の範囲でお申込み可能です。
- ストレージ申込容量を変更する場合は、別途変更申込書を提出いただくこととなります。
- ライト・オンデマンド・ネクストプランではご利用頂けません。

3.2.6 オプション機能機能の監視・運用

(1) 監視

1) オンライン・ストレージの監視

・オンライン・ストレージ用 VPN の監視

ゲートウェイ装置および当社データセンタ間でオンライン・ストレージ用 VPN を構築します。この VPN を 24 時間 365 日、当社内 SOC が監視します。※

・ストレージ容量の監視

実際にご利用いただいている容量を定期的に監視し、ストレージ申込容量に対しある一定以上となった場合にお客さまへ通知します。

・当社データセンタ内ストレージの監視

当社データセンタ内ストレージの正常性を監視し、異常を検知した場合、予備系への切替等、復旧作業を行います。

※「3.3.5.1 VPN 接続」に準じます。

(2) 設定値の変更運用

1)オンライン・ストレージの変更運用

・ストレージ申込容量の変更

ストレージ申込容量の変更は、お客さまから提出いただいた変更申込書に基づき行います。変更工事は SOC より遠隔にて行います。設定変更後、対応の完了をお客さま担当者へメールにて連絡します。

監視・運用内容の一覧は以下の表 3-6 のとおりです。

表 3-6 監視・運用内容一覧表

機能	内容		報告形式
オンライン・ストレージ	監視	• オンライン・ストレージ用 VPN の監視 • ストレージ使用容量の監視 • 当社データセンタ内ストレージの監視	• 対応報告メール • 容量制限警告のご連絡
	運用	• ストレージ申込容量の変更	• 設定一覧表

3.3 サービス提供条件

3.3.1 提供エリア

日本全国(一部離島を除く)で、インターネット常時接続が可能なお客さま。
※ISDN およびダイヤルアップでインターネット接続されているお客さまはご利用なれません。

3.3.2 責任範囲

本サービスの責任範囲の概要を図 3-3 に示します。

図に示す当社区分にあたる
・お客さまサイトゲートウェイ装置
・SOC 内のシステム構成(当社内データセンタのストレージを含む)
・SOC 管理用プライベート IP アドレス
について当社が正常動作に留意する責任を持ちます。

異常検知時、もしくはお客さまによる障害申告時に、当社にて障害の切り分けを行います。
当社責任範囲に問題があると判明した場合、速やかに障害の回復を行います。

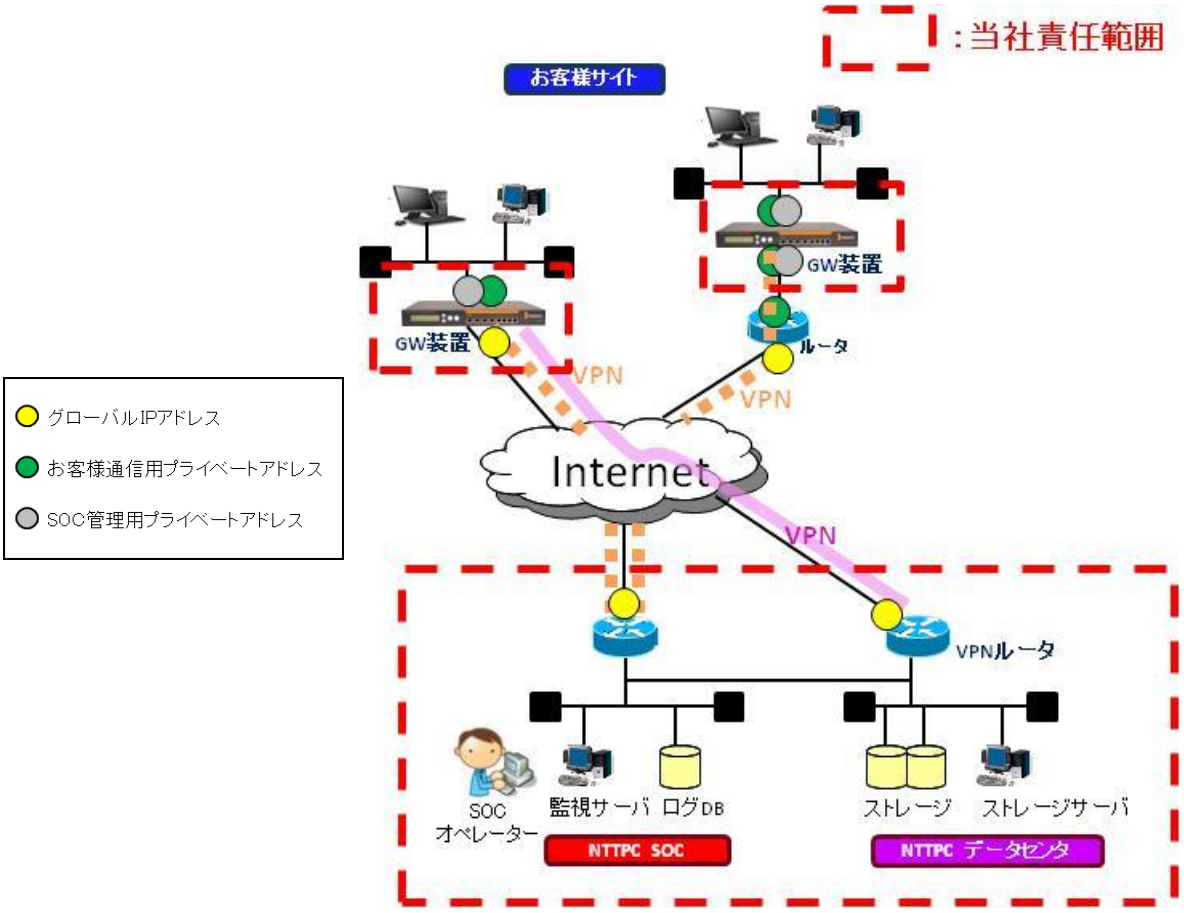

図 3-3 責任範囲概要

3.3.3 ゲートウェイ装置の設置条件

3.3.3.1 物理要件

サービスをご契約いただきますと当社よりゲートウェイ装置を設置提供いたします。
サービスの提供プラン別の物理要件は、以下表 3-7、表 3-8、表 3-9、表 3-10、表 3-11 のとおりです。
なおハードウェア要件は予告なく変更される場合がございます。

表 3-7 ライト・オンデマンド・ネクストプラン ハードウェア要件表

サイズ	電源	実用温度	相対湿度	重量
297(W)×44(H)×218(D) mm	100V 1.6A	0° C – 40° C	5% – 95%	2 kg
225(W)×44(H)×150(D) mm	100V 1.3A	0° C – 40° C	10% – 90%	1.19 kg
288(W)×44(H)×186.8(D) mm	100V 1.2A	0° C – 40° C	10% – 90%	1.7kg

ラックに設置される場合は、契約者より棚板の提供が必要です。

表 3-8 ライト・オンデマンド 10/30、ライト 10/30 プラン ハードウェア要件表

サイズ	電源	実用温度	相対湿度	重量
270(W)×40(H)×190(D) mm	100V 1.8A	0° C – 40° C	5% – 95%	2 kg
210(W)×44(H)×145(D) mm	100V 1.6A	5° C – 35° C	5% – 95%	2 kg

ラックに設置される場合は、お客さまより棚板の提供が必要です。

表 3-9 ベーシックプラン ハードウェア要件表

サイズ	電源	実用温度	相対湿度	重量
426(W)×43.5(H)×379.8(D) mm または 426(W)×44(H)×365(D) mm	80 W 100–240V	0° C – 40° C	10% – 90%	6 kg
438(W)×44(H)×292(D) mm	34W 110–240V	0° C – 40° C	10% – 90%	5.1Kg

その他:(付属品)ラックマウントキット

表 3-10 スタンダードプラン ハードウェア要件表

サイズ	電源	実用温度	相対湿度	重量
426(W)×43.5(H)×379.8(D) mm または 426(W)×44(H)×365(D) mm	80 W 100–240V	0° C – 40° C	10% – 90%	6 kg

その他:(付属品)ラックマウントキット

表 3-11 ハイエンドプラン ハードウェア要件表

サイズ	電源	実用温度	相対湿度	重量
426(W)×88(H)×600(D) mm	230 W 100–240V ×2	0° C – 40° C	10% – 90%	15 kg

その他:(付属品)ラッキング用レール、電源、ハードディスク冗長

3.3.3.2 物理インターフェースについて

ゲートウェイ装置には提供するゲートウェイ装置のグレードにより用意されていますポート数が異なります。
本サービスでは、管理上各ポートを下記のように割り当てております。

表 3-11 物理インターフェース一覧表

	ライト・オンデマンド・ネクストライト・オンデマンド 10/30 ライト 10/30	ベーシック	スタンダード	ハイエンド
eth0	LAN セグメント用	LAN セグメント用	LAN セグメント用	LAN セグメント用
eth1	WAN セグメント用	WAN セグメント用	WAN セグメント用	WAN セグメント用
eth2	保守要員用	DMZ セグメント用	DMZ セグメント用	DMZ セグメント用
eth3	（使用不可）	二重化構成用	二重化構成用	（使用不可）
eth4	－/ LAN セグメント用 ※	（使用不可）	（使用不可）	（使用不可）
eth5	－/LAN セグメント用 ※	（使用不可）	（使用不可）	（使用不可）
eth6	－/LAN セグメント用 ※	保守要員用［新機種］ （使用不可）［旧機種］	（使用不可）	（使用不可）
eth7	－/LAN セグメント用 ※	保守要員用［旧機種］ （使用不可）［新機種］	保守要員用	保守要員用
eth8	―	―	―	（使用不可）
eth9	―	―	―	（使用不可）
eth10	―	―	―	（使用不可）
eth11	―	―	―	（使用不可）
eth12	―	―	―	（使用不可）
eth13	―	―	―	（使用不可）

未使用となっておりますポート、または提供形態より使用しないポートについては、本サービスでは使用いたしません。
そのため、お客さまから提出していただいたヒアリングシートに記入された WAN、LAN、DMZ 以外のネットワークセグメントを使用されたい場合にはお客さまにて以下の対応を実施していただく必要がございます。

・ ルータを用意していただき、ルータ配下に増やしたいネットワークセグメントを追加していただく。

※当社が別に定めるゲートウェイ装置では eth4～eth7 を LAN セグメント用ポートとして使用可能です。

3.3.3.3 WiFi インターフェースについて

ライト・オンデマンド・ネクストプラン対応ゲートウェイ装置のうち、当社が別に定めるゲートウェイ装置では WiFi インターフェースが提供されます。WiFi インターフェースの仕様は以下の通りです。

表 3-12 WiFi インターフェース

項目	仕様	備考
規格	IEEE802.11a/b/g/n または IEEE802.11a/b/g/n/ac	
周波数帯	2.4GHz または 5GHz	同時利用不可
機能	無線アクセスポイント機能	
モード	ブリッジモード	

3.3.4 ゲートウェイ装置の提供形態

3.3.4.1 パターン 1(ルーターモード・DMZ なし)

パターン 1 では、ゲートウェイ装置をインターネットとの接続点または、お客さまネットワーク内にルータとして設置いたします。設置対応パターンを図 3-4 に示します。
ゲートウェイ装置に対してインターフェース毎に固定のアドレスを 1IP お客さまに指定していただく必要がございます。

WAN インターフェースについて・・・PPPoE の終端に対応しております。
Static、Dynamic 共に対応可能です。
IP Unnumbered には対応しておりません。

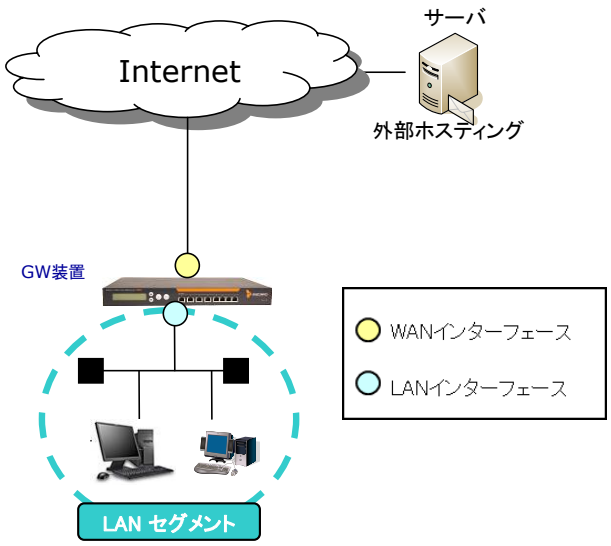

図 3-4 パターン 1 設置概要

3.3.4.2 パターン 2(ルーターモード・DMZ あり)

パターン 2 では、ゲートウェイ装置をインターネットとの接続点または、お客さまネットワーク内にルータとして設置いたします。対応パターンを図 3-5 に示します。
ゲートウェイ装置に対してインターフェース毎に固定のアドレスを 1IP お客さまに指定していただく必要がございます。

WAN インターフェースについて・・・PPPoE の終端に対応しております。
Static の場合対応可能です。(Dynamic には対応しておりません。)
IP Unnumbered には対応しておりません。
DMZ インターフェースについて・・・プライベート、グローバル共に対応可能です。
(構成上対応ができない場合もございます。)

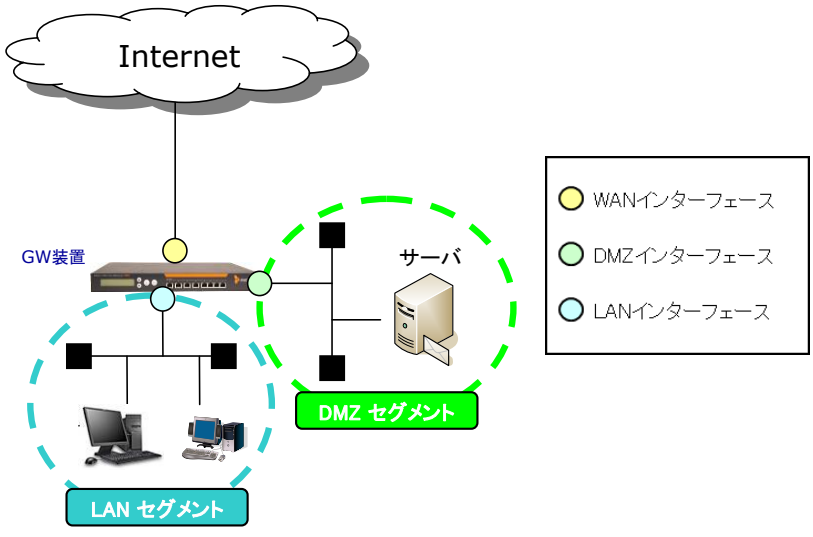

図 3-5 パターン 2 設置概要

3.3.4.3 パターン 3(ブリッジモード・DMZ なし)

パターン 3 では、ゲートウェイ装置を既存のお客さまネットワーク内にブリッジとして設置いたします。設置対応パターンを図 3-6 に示します。
ゲートウェイ装置に対してお客さまネットワークアドレスより、固定のアドレスを 1 装置につき 1 IP 提供していただく必要がございま

WAN インターフェースについて・・・プライベート、グローバルアドレス共に対応可能です。
PPPoE の終端に対応しておりません。
LAN インターフェースについて・・・WAN インターフェースとブリッジインターフェースを構成することで、WAN セグメントと同ネットワークアドレスを使用することが可能となります。

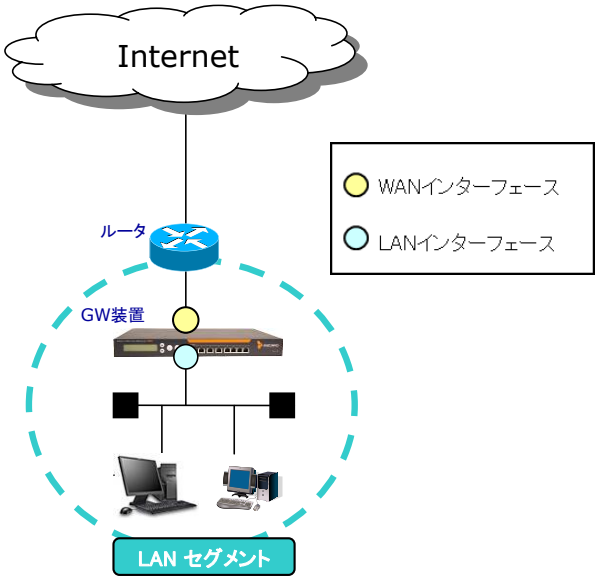

図 3-6 パターン 3 設置概要

3.3.4.4 パターン 4(ブリッジモード・DMZ あり)

パターン 4 では、パターン 1 同様ゲートウェイ装置をインターネットとの接続点または、お客さまネットワーク内にルータとして設置いたします。設置対応パターンを図 3-7 に示します。
ゲートウェイ装置に対してインターフェース毎に固定のアドレスを 1IP お客さまに指定していただく必要がございます。

WAN インターフェースについて・・・PPPoE の終端には対応しておりません。
DMZ インターフェースについて・・・WAN インターフェースとブリッジインターフェースを構成することで、WAN セグメントと同ネットワークアドレスを使用することが可能となります。

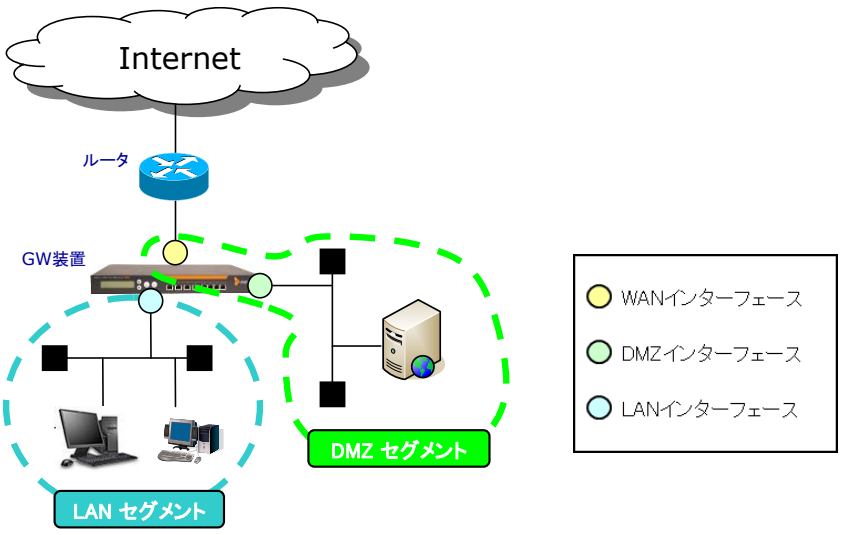

図 3-7 パターン 4 設置概要

3.3.4.5 二重化構成

ゲートウェイ装置を Master・Slave の二重化構成とすることで障害時のダウンタイムを最小限に抑えることができます。
設置概要を図 3-8 に示します。
※シングル構成で障害が発生した場合は、SOC で監視不具合を検知するか、お客さまからの申告をいただいてからの対応となります。

- お客さまが「3.2 サービス提供形態」より選択したプランから提供されるゲートウェイ装置を 2 台設置し、構成します。
  構成は Master/Slave 形式となります。（※通信は Master 側にのみ流れます。）
- 各ゲートウェイ装置に HA 構成用のインターフェースを設定し、ストレートケーブル(Cat5e 以上)で接続します。
  構成用のインターフェースにはゲートウェイ装置より自動的にアドレスが付与されます。
  構成用のインターフェースの間で障害の検知、データの同期が行われます。
- Master/Slave の同期に時間がかかる場合がございます。
- ゲートウェイ装置の上位にお客さま所有のネットワーク機器または、スイッチが存在する場合、機器の切り替わりの際にゲートウェイ装置から送信する Gratuitous ARP が受信可能な状態にしていただく必要がございます。
- ルータモード(パターン 1 かパターン 2)のみでのご提供となります。

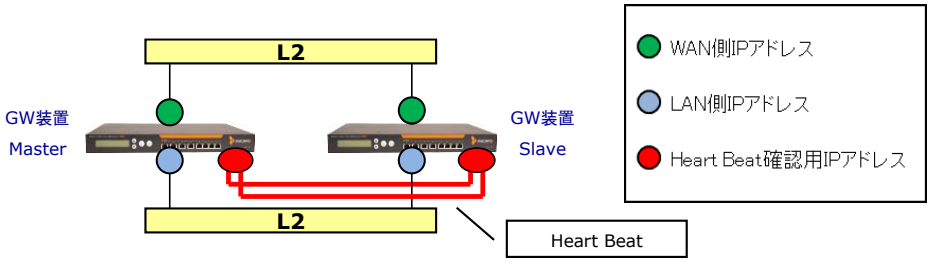

図 3-8 二重化構成 設置概要

3.3.5 遠隔監視・運用形態

3.3.5.1 VPN 接続

SOC から遠隔監視・運用を実施するため、お客さまサイトと当社 SOC サイトとの間で VPN を構築します。またオンライン・ストレージオプションをご利用の場合、お客さまサイトと当社データセンタ間で VPN を構築します。VPN 概要を図 3-9 に示します。

- ゲートウェイ装置に対して、「3.1.1 提供形態」の別なく、お客さまプライベートネットワークのインターフェースに SOC 管理用アドレスを付与いたします。
- SOC 管理用アドレスは、サービス申込時に SOC より払い出され、解約まで同じアドレスを利用いたします。また SOC 管理用アドレスはお客さまネットワーク内のアドレスと重複しないよう事前に確認を行います。
- ゲートウェイ装置の上位ネットワークにお客さま所有のファイアウォールやルータ等のネットワーク機器が存在する場合、そのネットワーク機器に対してゲートウェイ装置がインターネット上に存在する管理サーバと通信するための設定の変更をお願いいたします。詳細な通信内容については「表 3-12 インターネットへの通信一覧」に記述いたします。

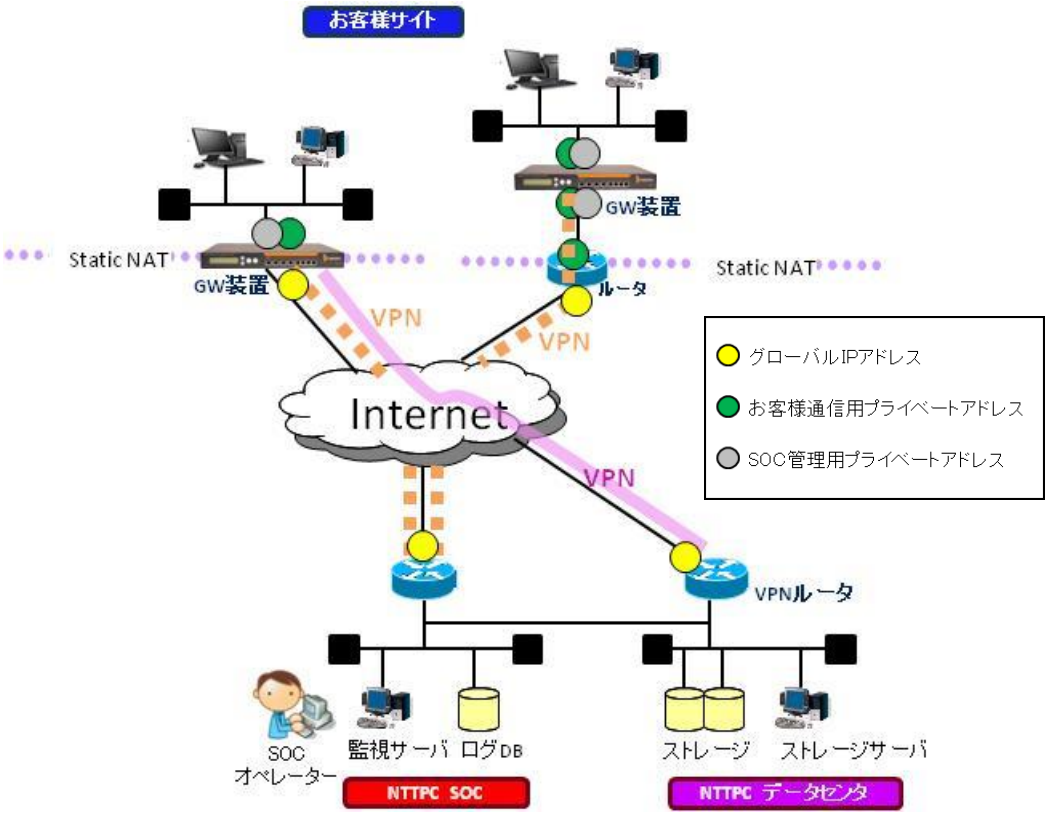

図 3-9 VPN 接続概要

3.3.5.2 ゲートウェイ装置が使用するアドレス帯

お客さまネットワーク内にゲートウェイ装置を設置する際、お客さま通信を行うために必要な、機器に設定する IP アドレスはお客さまにてご用意ください。また、保守などのため、お客さま通信とは別に監視用に IP アドレスを使用します。使用するアドレス帯は下記の通りで、お客さまは本サービス提供開始後、お客さまネットワークの拡張等で下記のアドレス帯を使用することはできません。

- 保守用　：172.30.0.0/24
- VPN 接続用　：172.26.0.0/16
  172.27.0.0/16
  172.28.0.0/16
  172.29.0.0/16

※ベーシック、スタンダード、ハイエンドプランについてはサービス申込時のヒアリングシートから、すでにお客さまが上記のアドレス帯を使用している場合、他のアドレス帯を使用いたします。ライト・オンデマンド・ネクストプランについては上記のアドレス帯を使用することはできません。

3.3.5.3 ゲートウェイ装置からのインターネットへの通信について

本サービスを提供するにあたり当社より提供するゲートウェイ装置が Up2date サイトまたは外部 DB へ接続するため、インターネットへの接続が必要となります。表 3-13 に定める接続が維持されない場合、お客さまへのセキュリティ機能およびリモートによる監視・運用、レポートの提供等が停止する場合があります。

- 事前にお客さまが契約する ISP から提供される DNS サーバアドレスの確認をいただき、ヒアリングシートに記入いただく必要がございます。
- ゲートウェイ装置の上位ネットワークにお客さま所有のファイアウォールやルータ等のネットワーク機器が存在する場合、そのネットワーク機器に対して、ゲートウェイ装置がインターネット上に存在する管理サーバと通信するための設定変更をお願いする場合がございます。

詳細な通信内容の一覧は以下表 3-13 のとおりです。

表 3-13 インターネットへの通信一覧

提供機能		通信内容	通信ポート
基本機能	監視・運用	お客さまーSOC 間の VPN 接続	TCP 443
セキュリティ機能	侵入検知・防御(IPS)	Up2date サイトへのシグネチャ ルールファイルの更新	UDP 53 UDP 33000-34000 TCP 443
	出口対策		
	アプリケーションコントロール・ファイル転送アプリケーション検知		
	メールアンチウイルス	Up2date サイトへのウイルス パターンファイルの更新	UDP 53 UDP 33000-34000 TCP 443
	WEB アンチウイルス		
	アンチスパイウェア		
	メールアンチスパム	外部 DB へスパムスコアの問い合わせ	UDP 53 TCP 80
	アンチフィッシング	外部 DB へ URL カテゴリの問い合わせ	UDP 53 TCP 80
	URL フィルタリング		
オプション機能	オンライン・ストレージ	お客さまー当社データセンタ間の VPN 接続	TCP 443 UDP 500 UDP 4500(NAT-T)

3.3.5.4 ゲートウェイ装置に隔離されたメールについて

ゲートウェイ装置内に隔離されたメールは、隔離されたメールをメールアドレス毎に集計し、隔離レポートを作成します。

(1) 隔離レポートの作成
- SMTP 通信で隔離されたメールの情報は初期値の場合、午前 1 時以降最初に集計し、隔離レポートを作成後設定されたメールサーバ宛てに送付します。
- POP3 通信で隔離されたメールの情報は初期値の場合、午前 1 時または午後 15 時以降のクライアント初回受信時に集計し、隔離レポートを作成後クライアント宛てに送付します。

※ゲートウェイ装置は 1 度集計した隔離メールを再度集計しません。隔離レポートをクライアントが削除した場合はメールのリリースが行えなくなります。

(2) 隔離レポートが提供する情報

隔離レポートは、件名「Quarantine Report for(メールアドレス)」で送付され、ゲートウェイ装置内に隔離したメールの一覧を提供します。
- アンチスパムにより隔離されたメールについて、メールの情報を確認できます。受信したいメールをゲートウェイ装置に対して、リリース要求を行うことが可能です。
- アンチウイルスにより隔離されたメールについて、メールの情報を確認できます。

「メールの情報(詳細)」
- 時間
- 添付ファイルの有無
- 差出人アドレス
- 宛先アドレス
- 件名
- 隔離された理由
- サイズ
- アクション

※ゲートウェイ装置とリリース要求を行うクライアントの間にお客さま所有のファイアウォールやルータ等のネットワーク機器が存在する場合、そのネットワーク機器に対してクライアントがゲートウェイ装置へリリース要求の通信をするための設定変更をお願いする場合がございます。詳細な通信内容については以下表 3-14 のとおりです。

(1) 隔離レポートのメール形式
- 隔離レポートは HTML 形式で文字コードに UTF-8 を使用し作成されます。ご使用のメールソフトが表示対応可能かご確認をお願いいたします。
  受信のエンコード設定が UTF-8 以外の設定の場合、文字が化けて表示されます。
  (エンコード設定を設定しなおすことで、正しく参照が可能となります。)

(2) ゲートウェイ装置内のメールの保管
- ゲートウェイ装置に隔離されたメールの保管期間は 16 日間となります。保管期間を経過したメールは自動的に削除されます。
- ゲートウェイ装置に隔離されたメールを保管する容量には上限があります。上限に達した場合保管期間経過前でも古いメールから自動的に削除されます。プラン別の容量については「参考資料」に記載しています。

※上記の条件に伴いゲートウェイ装置から削除されたメールは、クライアントからリリース要求を行ってもエラーとなり受信することができません。

表 3-14 ゲートウェイ装置への通信一覧

提供機能		通信内容	通信ポート
セキュリティ機能	メールアンチスパム	ユーザからのメールのリリース要求	TCP 3840

3.4 サービス対応

本サービスのオペレーションは当社 SOC 内で行われ、故障対応等のお客さまからの連絡(電話、またはメール)に対して対応を実施します。SOC の受付・対応時間、リードタイムについてまとめます。

(1)ゲートウェイ・セキュリティ運用監視サービス

表 3-15 サービス対応表

対応内容			受付時間	標準リードタイム	対応時間
工事	初期工事		・平日 9 時-17 時 (当日分の受付は 16 時まで)	ヒアリングシート受領後 10 営業日	・平日 9 時-17 時 ・平日 17 時-22 時 ・平日 22 時-翌日 9 時 ・土日祝日 9 時-17 時 ・土日祝日 17 時-翌日 9 時
	再工事/移設工事		・平日 9 時-17 時 (当日分の受付は 16 時まで)	ヒアリングシート受領後 10 営業日	・平日 9 時-17 時 ・平日 17 時-22 時 ・平日 22 時-翌日 9 時 ・土日祝日 9 時-17 時 ・土日祝日 17 時-翌日 9 時
運用	サービス変更オーダ処理 (変更オーダシート内の変更オーダ)		・平日 9 時-17 時 (当日分の受付は 16 時まで)	変更オーダシート受領後 5 営業日	・平日 9 時-17 時
	解約オーダ処理		・平日 9 時-17 時 (当日分の受付は 16 時まで)	解約申請書受領後 30 営業日	・平日 9 時-17 時
交換保守	24 時間 365 日駆け付け交換保守		・24 時間 365 日	ー	・24 時間 365 日
	先出センドバック保守		・24 時間 365 日	ー	・平日 9 時-15 時 (正午までの受付は当日発送、以降は翌営業日発送)
監視	通知	24 時間 365 日死活監視	ー	ー	・24 時間 365 日
		侵入検知・防御(IPS)	ー	ー	・監視:24 時間 365 日 ・レポート:平日 9 時-17 時
		アプリケーションコントロール・ファイル転送アプリケーション検知	ー	ー	・監視:24 時間 365 日 ・レポート:1 日 2 回、365 日
		出口対策	ー	ー	・監視:24 時間 365 日 ・レポート:1 日 1 回、365 日
その他	監視不具合検知時の SOC からの電話連絡および受付		・24 時間 365 日 (ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30 は平日 9 時-17 時)	ー	・24 時間 365 日 (ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30 は平日 9 時-17 時)
	監視不具合検知時の SOC からのメール連絡		ー	ー	・24 時間 365 日
	お客さまからの障害申告受付・対応		・24 時間 365 日 (ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30 は平日 9 時-17 時)	ー	・24 時間 365 日 (ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30 は平日 9 時-17 時)
	問い合わせ受付		・24 時間 365 日 (ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30 は平日 9 時-17 時)	ー	・平日 9 時-17 時

※工事対応については、対応時間により提供料金が異なります。詳細内容については「別紙 2: ゲートウェイ・セキュリティ運用監視サービス 料金表」に記載しています。

(2) オンライン・ストレージオプションサービス

表 3-16 サービス対応表

対応内容			受付時間	標準リードタイム	対応時間
工事	初期工事		・平日 9 時-17 時 （当日分の受付は 16 時まで）	申込書受領後 5 営業日	・平日 9 時-17 時
運用	サービス変更オーダ処理		・平日 9 時-17 時 （当日分の受付は 16 時まで）	変更申込書受領後 5 営業日	・平日 9 時-17 時
	解約オーダ処理		・平日 9 時-17 時 （当日分の受付は 16 時まで）	解約申請書受領後 30 営業日	・平日 9 時-17 時
監視	通知	24 時間 365 日死活監視	ー	ー	・24 時間 365 日
その他	問い合わせ対応		・24 時間 365 日 （ライト・オンデマンド 10/30 は平日 9 時-17 時）	ー	・平日 9 時-17 時

※工事対応については、ゲートウェイ・セキュリティ運用監視サービスとセットで申込みされた場合、提供料金が異なります。詳細内容については「別紙 2: ゲートウェイ・セキュリティ運用監視サービス 料金表」に記載しています。

4 品質

4.1 サービス対応

本サービスでゲートウェイ装置から取得される情報についてISMSの情報資産運用規定に基づき適切に管理され、原則として 1 年間保持されます。(ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30 に関してはログの 1 年間保持は行いません)

- 本サービスで提供する各種セキュリティ機能は、ゲートウェイ装置上で動作するプログラムにより提供されますが、ゲートウェイ装置が二重化されていない(二重化についてはオプションにて提供されます)場合、装置の障害発生の間又は、ゲートウェイ装置上で動作するプログラムの特性上、お客さまネットワークに問題を引き起こす場合がございます。
- 問題が発生した場合の免責については本規約第 6 条、第 32 条に記載しております。

当社で保持するゲートウェイ装置のログ内容の一覧は以下表 4-1 のとおりです。

表 4-1 ゲートウェイ装置のログ一覧

	ログ名	packetfilter	ips	afc	http	ftp	pop3	smtp
セキュリティ機能	ファイアウォール	●	―	―	―	―	―	―
	侵入検知・防御(IPS)	―	●	―	―	―	―	―
	メールアンチウイルス	―	―	―	―	―	●	●
	WEB アンチウイルス	―	―	―	●	●	―	―
	アンチスパイウェア	―	―	―	●	―	―	―
	メールアンチスパム アンチフィッシング	―	―	―	―	―	●	●
	URL フィルタリング	―	―	―	●	―	―	―
	アプリケーションコントロール・ファイル転送アプリケーション検知	―	―	●	―	―	―	―

※ライト・オンデマンド・ネクスト、ライト・オンデマンド 10/30、ライト 10/30 プランに関してはログの 1 年間保持は行いません。

4.2 当社データセンタ設備

当社のセンタ側のサービスで使用するサーバ及び、ネットワークは、二重化するなどしてシステムの可用性を考慮しております。

4.3 SOC

サービスを提供するために使用するサーバ・ゲートウェイ装置の取り扱いについて情報セキュリティマネジメントシステムの規格「ISO/IEC27001:2005」(2005 年 2 月 10 日取得)「に基づき SOC 担当者が下記に記述するとおり運用しており、お客さまよりお預かりした情報のセキュリティを確保しております。

- アカウント
  SOC 作業用のアカウントを払い出し、作業者(アカウント名)の履歴を残しております。
- データ
  アクセス権が設定されたサーバにお客さま毎に保存し、アクセス権を所有しているユーザのみのデータの閲覧、変更が可能となっております。

4.4 メンテナンスによるサービス停止

障害によるサービス停止の他、ゲートウェイ装置のメンテナンスのためサービスの一部停止が発生いたします。
停止が発生する際は事前にお客さま連絡先へメールにて連絡いたします。

4.5 ゲートウェイ装置の保守対応

故障等によりゲートウェイ装置の交換が発生した場合、交換前のゲートウェイ装置の設定情報を元に原状回復を行いますが、以下の設定情報については回復できない場合があります。

- お客さま自身がゲートウェイ装置の管理画面から選択・変更した情報
  - -WEB アンチウイルス
    プロキシスキップ設定
  - -URL フィルタリング
    URL カテゴリ選択設定、URL カテゴリカスタマイズ、ホワイトリスト設定、ブラックリスト設定
  - -アプリケーションコントロール
    対象アプリケーションの選択、詳細設定
  - -メールアンチウイルス・アンチスパム
    POP3 ホワイトリスト設定
    POP3 サーバ設定
  - -WiFi アクセスポイント
    WiFi 設定

※お客さま自身が変更できる情報は、ご利用されるゲートウェイ装置により異なります。