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. 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、インターネットと本サービスの契約者（以下「契約者」といいます）のネットワーク（以下「契約者ネットワーク」といいます）との接続点もしくは、契約者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 － 障害時のSOCからの連絡 - 技術問合せ対応	ファイアウォール運用	オンライン・ストレージ
24時間365日駆け付け交換保守	24時間365日侵入監視	
月次レポート	ファイル転送 アプリケーション検知	
対応レポート	WEBアンチウィルス運用	
	アンチスパイウェア運用	
	URLフィルタリング運用	
	メールアンチウィルス運用	
	メールアンチスパム・ アンチフィッシング運用	

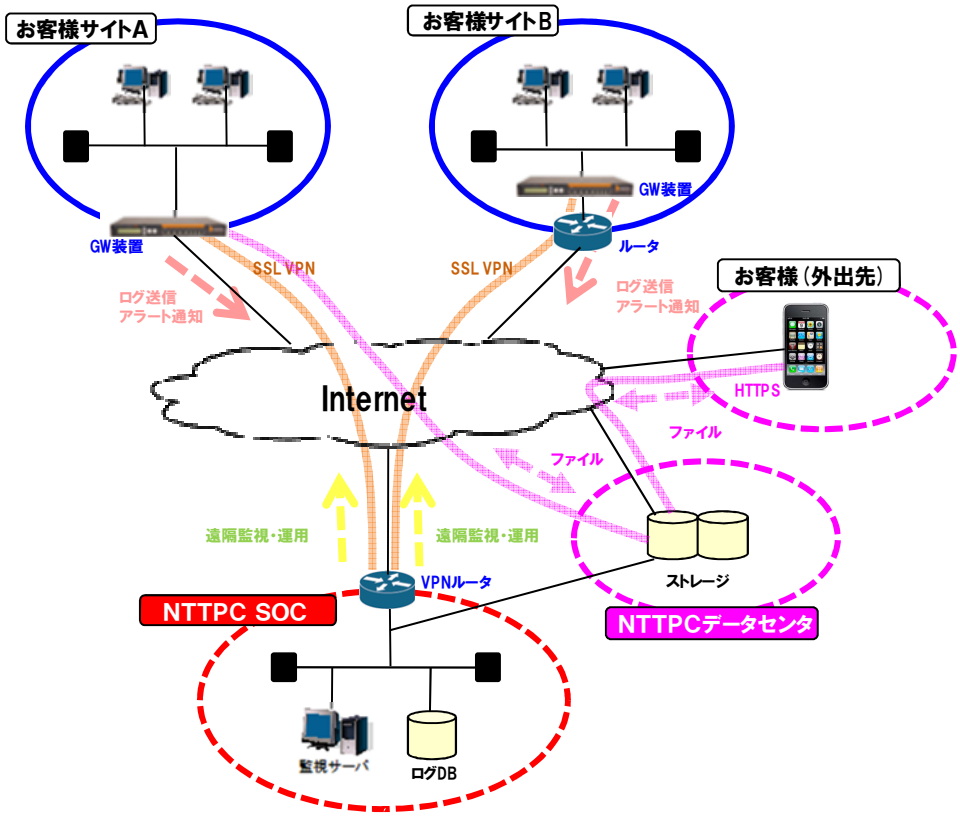


図 2-1　サービス概要図

2.1 サービスプラン

2.1.1 提供形態

本サービスのプラン別提供形態は表 2-1 のとおりです。
契約者サイトに設置するゲートウェイ装置のグレードにより、提供形態、提供機能が分かれます。

表 2-1 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 10	ー	●	ー	ー	●	ー	●	ー	10 端末まで
ライト オンデマンド 30	ー	●	ー	ー	●	ー	●	ー	50 端末まで
ライト 10	●	●	ー	ー	●	ー	●	ー	10 端末まで
ライト 30	●	●	ー	ー	●	ー	●	ー	50 端末まで
ベーシック	●	●	●	○	●	○	●	●	200 端末まで
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　ー：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。

2.1.2 提供機能

本サービスのプラン別提供機能は表 2-2 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 2-2 プラン別提供機能表

機能		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	●	●	●	●	●	●	●
	障害時の SOC からの連絡	平日 9 時～17 時※		24 時間 365 日				
	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	○	○	●	●
	月次レポート	●	●	●	●	●	●	●
	対応レポート	ー	ー	ー	ー	●	●	●
セキュリティ機能	ファイアウォール運用	●	●	●	●	●	●	●
	24 時間 365 日侵入監視	ー	ー	ー	ー	○	●	●
	ファイル転送アプリケーション検知運用	●	●	●	●	●	●	●
	WEB アンチウィルス運用	●	●	●	●	●	●	●
	アンチスパイウェア運用	●	●	●	●	●	●	●
	URL フィルタリング運用	ー	ー	ー	ー	○	●	●
	メールアンチウィルス運用	●	●	●	●	●	●	●
	メールアンチスパム・アンチフィッシング運用	●	●	●	●	●	●	●
オプション機能	オンライン・ストレージ	●	●	●	●	ー	ー	ー

●：提供　○：別途オプション契約にて提供　ー：未提供　※ 土日祝日・年末年始は除きます。

2.2 サービス内容

2.2.1 基本機能

基本機能はサービスに付随し、提供いたします。

- 表 2-4 の 8 つのセキュリティ機能の中から、契約者が最低 1 つ以上の機能を選択されることにより提供いたします。

※ 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 2-3 のとおりです。

表 2-3 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死活監視を行います。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、契約者への連絡対応を行います。
障害時の SOC からの連絡 ※注意 2	監視が出来なくなった際に SOC からお客様へ連絡し、通信が可能かどうかの確認を致します。 お客様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。
技術問合せ対応 ※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に対応いたします。
24 時間 365 日駆け付け交換保守 ※注意 3	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、保守要員が契約者のゲートウェイ装置の交換対応を行います。
月次レポート	1 ヶ月毎に、契約者担当者へ提供いたします。
対応レポート	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 10/30 の場合、障害時の連絡や技術問合せへの対応は平日 9 時～17 時に限らせていただきます。上記時間外で発生した障害や技術問合せへの対応は、翌営業日の 9 時～17 時とさせていただきます。

※ 注意 3: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、SOC より交換用のゲートウェイ装置を契約者に送付いたします。装置到着後、契約者にて交換対応をお願いいたします。(先出しセンドバック)
ライト 30、ベーシックプランの場合、別途「アドバンスドサポート」をご契約いただくことで本機能が提供可能となります。

2.2.2 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 2-4 の 8 つのセキュリティ機能の中から、契約者が最低 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 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デフォルト値に基づきますが(デフォルト値は参考資料参照)、契約者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契約者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。

ゲートウェイ装置の持つセキュリティ機能は表 2-4 のとおりです。

表 2-4 セキュリティ機能一覧表

機能	内容
ファイアウォール運用	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。 ※ 注意 4 ※ 注意 5 ➢ 不要なパケットの侵入を防ぎ、契約者ネットワークを保護いたします。
24 時間 365 日侵入監視	ファイアウォールを通過したトラヒックをモニターし、攻撃や異常行動を検知、制御を行います。 ※ 注意 6 ※ 注意 7 ※ 注意 8 ➢ 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。

表 2-4 セキュリティ機能一覧表（続き）

<table>
<tr><td>ファイル転送
アプリケーション検知</td><td colspan="2">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)
• Peer-to-Peer (P2P)
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、ファイル転送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。</td></tr>
<tr><td rowspan="2">WEB アンチウィルス
運用</td><td>HTTP</td><td>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
• ウィルス
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ィ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 9
※ 注意 10
※ 注意 11
※ 注意 12</td></tr>
<tr><td>FTP</td><td>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
• ウィルス
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ィ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 13</td></tr>
<tr><td>アンチスパイウェア
運用</td><td>HTTP</td><td>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
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 10
※ 注意 12
※ 注意 14</td></tr>
<tr><td>URL フィルタリング
運用</td><td>HTTP</td><td>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。
クライアントが WEB アクセス実行時、URL をチェック
• 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。
クライアントが WEB アクセス実行時、URL をチェック
• 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 12
※ 注意 15</td></tr>
<tr><td>メールアンチウィルス
運用</td><td>POP3</td><td>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
• ウィルス
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ィ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、クライアントがウィルスに感染するのを防ぎます。
※ 注意 12
※ 注意 16
※ 注意 17
※ 注意 21</td></tr>
</table>

表 2-4 セキュリティ機能一覧表（続き）

機能	内容	
メールアンチウィルス運用	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 • ウィルス 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ィ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、ウィルスに汚染しているメールの着信を防ぎます。 （クライアントがウィルスに感染している場合、外部へウィルスメールが送信されるのを防ぎます） ※ 注意 12 ※ 注意 18 ※ 注意 19 ※ 注意 20 ※ 注意 21
メールアンチスパム・アンチフィッシング運用	POP3	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 12 ※ 注意 17 ※ 注意 21 ※ 注意 22
	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 12 ※ 注意 19 ※ 注意 20 ※ 注意 21 ※ 注意 22 ※ 注意 23

※ 注意 4 ： 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運用は 2 つのルールどちらかのみに対応しております。
- 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 5 ： 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出来ません。

※ 注意 6 ： IPS による監視におきましては、ゲートウェイ装置のもつデフォルト設定にてルールの危険度により『防御』(トラヒックの遮断)、『警告』(トラヒックの通過)を行います。検知した攻撃によりましては、『警告』のみを行い、『防御』を行わないものがございます。(『防御』を行うのは、危険度が非常に高い攻撃に対してのみです。)

※ 注意 7 ： 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 8 ： 侵入監視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 9 ： 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 10 ： 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ィ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 11 ： デフォルト設定に当社が指定した一部のサイト(ウィ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 12 ： 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 13 ： WEB アンチウィルス運用を選択すると 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ィ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 ： スパイウェア検知はアンチスパイウェア以外にも WEB アンチウィ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 アンチウィ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 15 ： 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、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。契約者からの設定変更の運用に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 16 ： スキャンを行うメールサイズは 2M（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ィルススキャンを行いません。

※　注意 17 ： 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。

- 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、ウィ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 18 ： 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ィルススキャンを行いません。

※　注意 19 ： 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。
- お客様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。このためお客様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 20 ： 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ィルス、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。）

※　注意 21 ： スパムのチェックを行うメールサイズは 128Kbyte までとなります。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 22 ： 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「2.3.5.4 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 23 ： 他ドメイン宛にメールを送信することができるお客様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。

2.2.3　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～500GByte 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。

2.2.3　基本機能の監視・運用

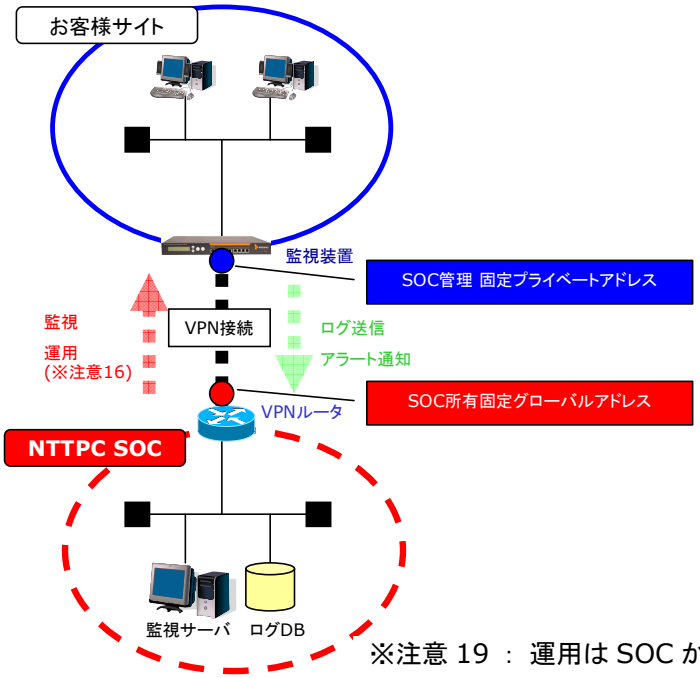
契約者ネットワーク内に設置したゲートウェイ装置の監視・運用を 24 時間 365 日、当社内 SOC が提供いたします。ゲートウェイ装置を遠隔にて監視・運用を行うため、図 2-2 が示すように契約者所有のネットワークアドレスと SOC のネットワークアドレスとの間で VPN を構築します。

(1) 監視
監視サーバに設定された監視の閾値を超えて応答がなかった場合、監視サーバは SOC 担当者へアラートを送信します。SOC 担当者はアラートの内容を確認し、契約者対応を行います。
(2) 障害対応
監視により通知されたアラート内容確認後、ゲートウェイ装置に障害が発生しているか SOC 担当者が切り分けを行います。
(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、契約者ネットワーク内に設置したゲートウェイ装置を保守要員が交換作業を行います。
(4) 問い合わせ
契約者からのサービス内容や技術質問などメールにて問い合わせ対応を行います。

監視・運用内容の一覧は以下の表 2-5 のとおりです。

表 2-5 監視・運用内容一覧表

	内容		
保守	監視	• 死活監視	• 対応報告メール
	運用	• 契約者問い合わせ （故障申告、技術質問など） • 障害発生後の障害切り分け • 機器交換対応	• 対応報告メール



※注意 19 ： 運用は SOC からのみアクセス可能とする

図 2-2 SOC～契約者サイト間通信イメージ

2.2.4　セキュリティ機能の監視・運用

「2.2.1 セキュリティ機能」より契約者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、図 2-2 が示すように契約者所有のネットワークアドレスと SOC のネットワークアドレスとの間で VPN を構築します。

(1)　監視

1)侵入監視

ゲートウェイ装置にてトラヒックが 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、以下のとおり契約者対応を行います。

- 遮断の場合・・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。
- 通過の場合・・SOC にて対応が必要と判断した場合、ファイアウォールルールの設定変更を行い、送信元アドレスからの通信を遮断します。
  変更内容は契約担当者へメールにて連絡します。

2)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ファイル転送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通知されます。SOC 担当者はアラートの内容を確認し、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、対応の完了を契約者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 3-1 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契約者へ提供いたします。

1)対応レポート

1 ヶ月間 SOC が行った契約者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 2-4 セキュリティ機能一覧表」から契約者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 2-3 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。
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 2-6 のとおりです。

表 2-6 監視・運用内容一覧表

機能	内容		
ファイアウォール運用	監視	―	―
	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
24 時間 365 日 侵入監視	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	• IPS 検知のご連絡
	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
メールアンチウィルス運用 WEB アンチウィルス運用 アンチスパイウェア運用	監視	• ウィルスパターンのアップデートの監視	―
	運用	• ウィルス、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運用 アンチフィッシング運用	監視	―	―
	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 フィルタリング運用	監視	―	―
	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
ファイル転送アプリケーション検知	監視	• ファイル転送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	• ファイル転送アプリケーション検知のご連絡
	運用	• 対応プロトコルの追加・変更 • アプリケーション検知時の動作設定変更 • ファイル転送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

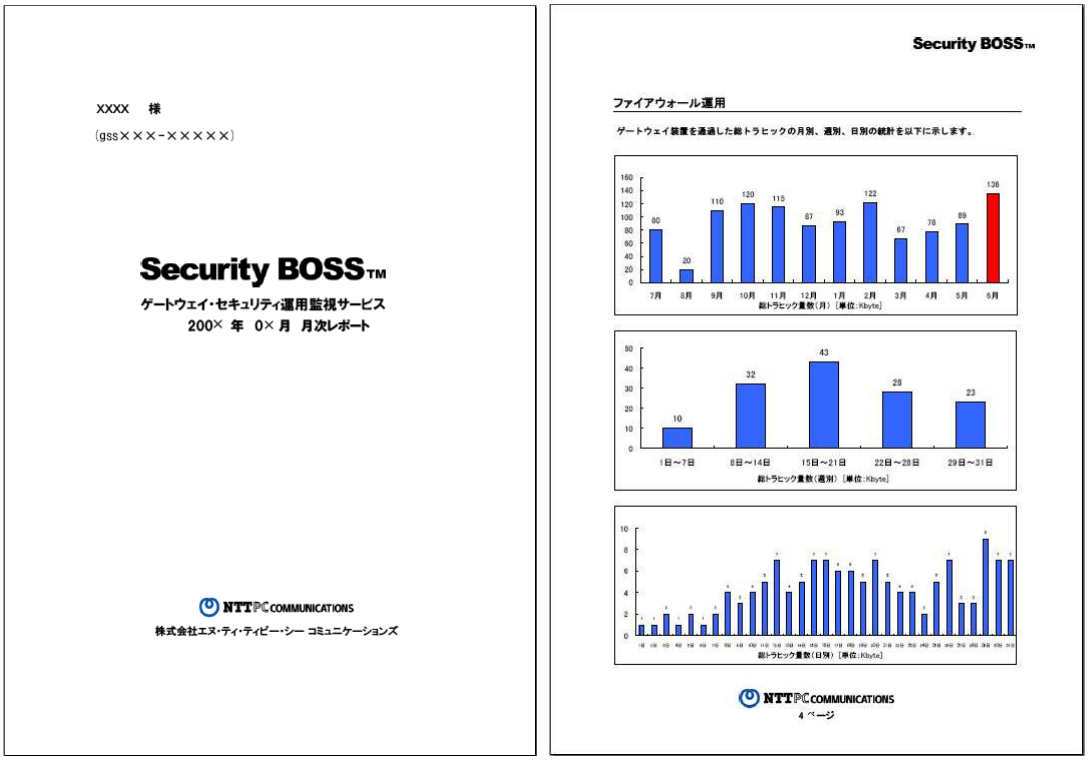


図 2-3 月次レポートの例

2.2.4 オプション機能の監視・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様へ通知します。

・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。

※「2.2.3 基本機能の監視・運用 (1)監視」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、お客様から提出頂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、対応の完了を契約者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 2-7 のとおりです。

表 2-7 監視・運用内容一覧表

機能	内容		
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

2.3 サービス提供条件

2.3.1 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契約者。
※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様はご利用なれません。

2.3.2 責任範囲

本サービスの責任範囲の概要を図 2-4 に示します。

図に示す当社区分にあたる
・契約者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)
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、もしくは契約者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。

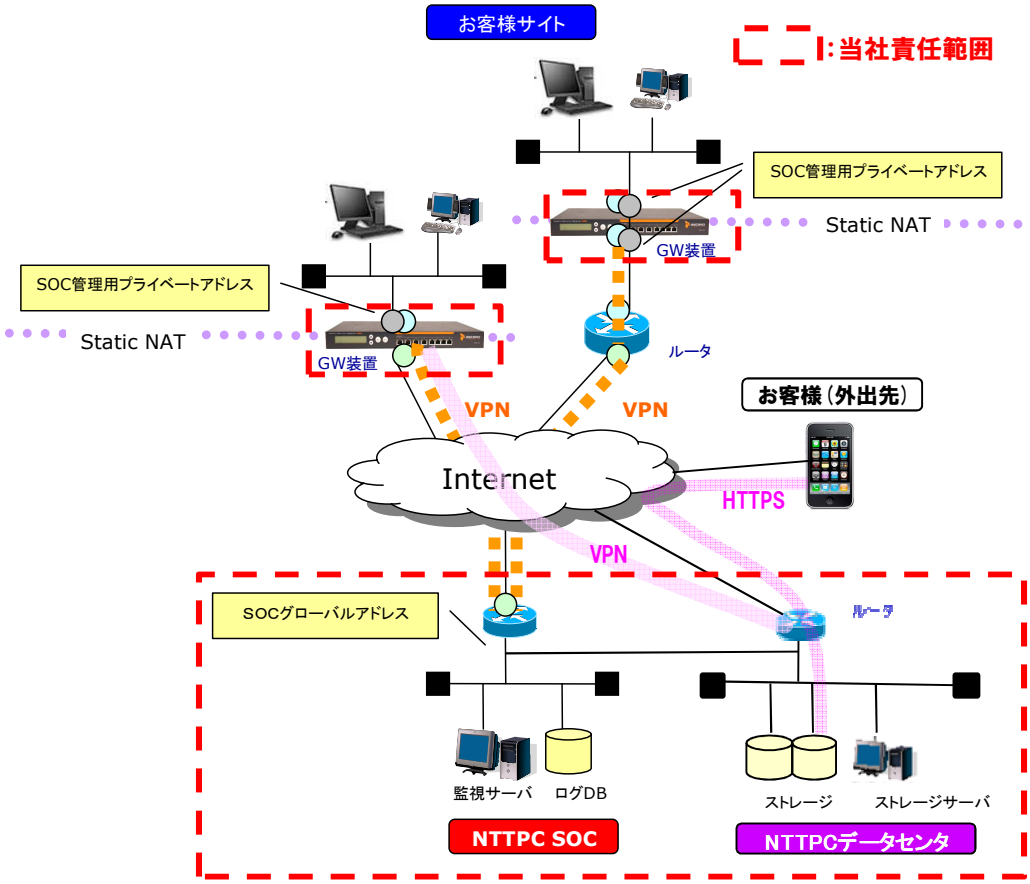


図 2-4 責任範囲概要

2.3.3 ゲートウェイ装置の設置条件

2.3.3.1 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 2-8、表 2-9、表 2-10、表 2-11 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 2-8 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	重さ
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、契約者より棚板の提供が必要です。

表 2-9 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	重さ
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 2-10 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	重さ
426(W)×43.5(H)×379.8(D) mm または 426(W)×44(H)×365(D) mm	80 W 100240V	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 2-11 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	重さ
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

2.3.3.2 物理インタフェースについて

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 2-12 物理インタフェース一覧表

	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	LAN 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	ー	二重化構成用	二重化構成用	二重化構成用
eth4	ー	(未使用)	(未使用)	(未使用)

表 2-12 物理インタフェース一覧表（続き）

	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
eth5	ー	（未使用）	（未使用）	（未使用）
eth6	ー	（未使用）	（未使用）	（未使用）
eth7	ー	保守要員用	保守要員用	保守要員用
eth8	ー	ー	ー	（未使用）
eth9	ー	ー	ー	（未使用）
eth10	ー	ー	ー	（未使用）
eth11	ー	ー	ー	（未使用）
eth12	ー	ー	ー	（未使用）
eth13	ー	ー	ー	（未使用）

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、契約者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契約者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。

2.3.4　ゲートウェイ装置の提供形態

2.3.4.1　パターン 1

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、契約者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 2-5 に示します。
ゲートウェイ装置に対してインタフェース毎に固定のアドレスを 1IP 契約者に指定していただく必要がございます。

WAN インタフェースについて・・・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。

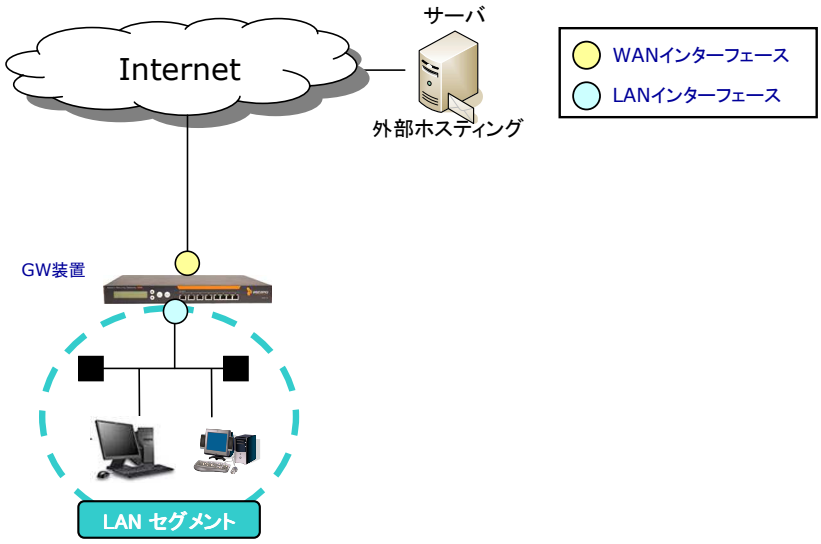


図 2-5 パターン 1 設置概要

2.3.4.2　パターン 2

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、契約者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 2-6 に示します。
ゲートウェイ装置に対してインタフェース毎に固定のアドレスを 1IP 契約者に指定していただく必要がございます。

WAN インタフェースについて・・・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。)

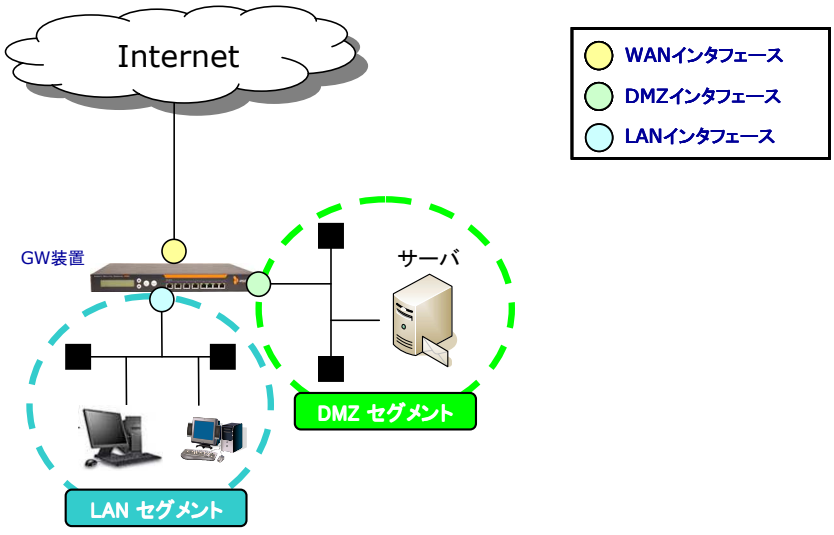


図 2-6 パターン 2 設置概要

2.3.4.3　パターン 3

パターン 3 では、ゲートウェイ装置を既存の契約者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 2-7 に示します。
ゲートウェイ装置に対して契約者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す。

LAN インタフェースについて・・・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。

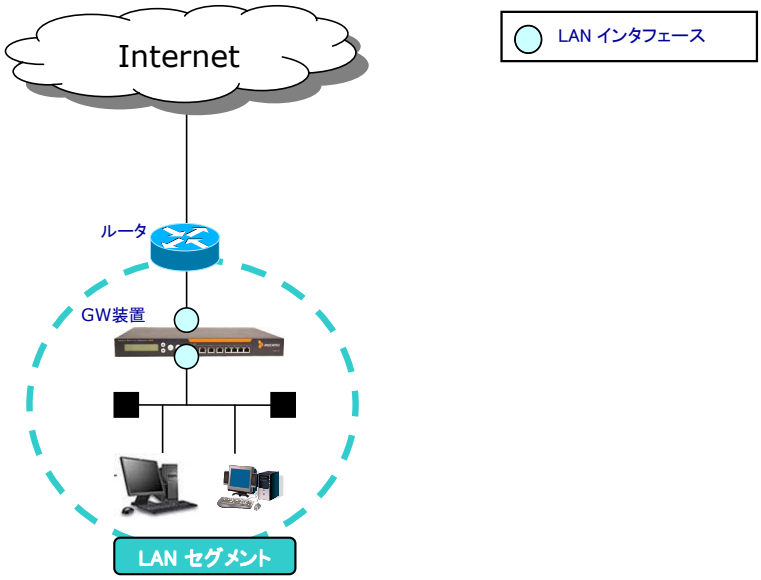


図 2-7 パターン 3 設置概要

2.3.4.4　パターン 4

パターン 4 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、契約者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 2-8 に示します。
ゲートウェイ装置に対してインタフェース毎に固定のアドレスを 1IP 契約者に指定していただく必要がございます。

WAN インタフェースについて・・・PPPoE の終端には対応しておりません。
DMZ インタフェースについて・・・WAN インタ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。

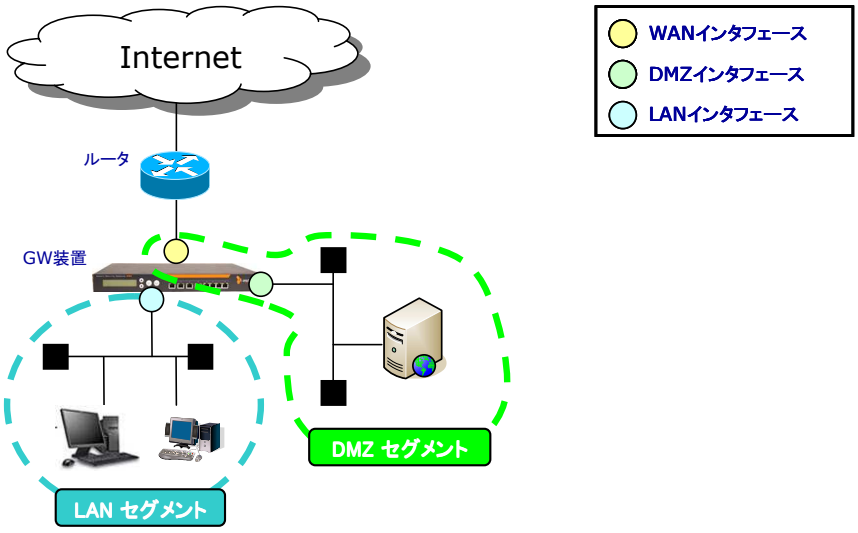


図 2-8 パターン 4 設置概要

2.3.4.5　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出来ます。設置概要を図 2-9 に示します。

- 契約者が「2.2 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。
- Master/Slave 構成されます。
- 各ゲートウェイ装置に HA 構成用のインタフェースを設定し、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契約者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。

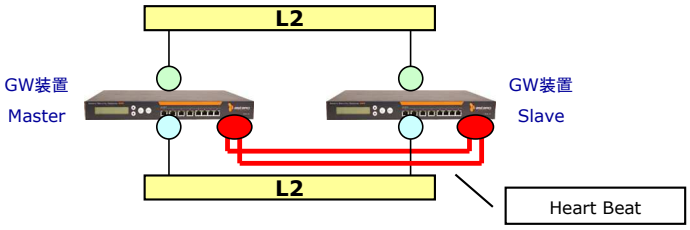


図 2-9 二重化構成 設置概要

2.3.5　遠隔監視・運用形態

2.3.5.1　VPN 接続

SOC から遠隔監視・運用を実施するため、契約者サイトと当社 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、契約者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 2-10 に示します。

- ゲートウェイ装置に対して、「2.1.1 提供形態」の別なく、契約者プライベートネットワークのインタフェースに 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 管理用アドレスは契約者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契約者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 2-13 インターネットへの通信一覧」に記述いたします。

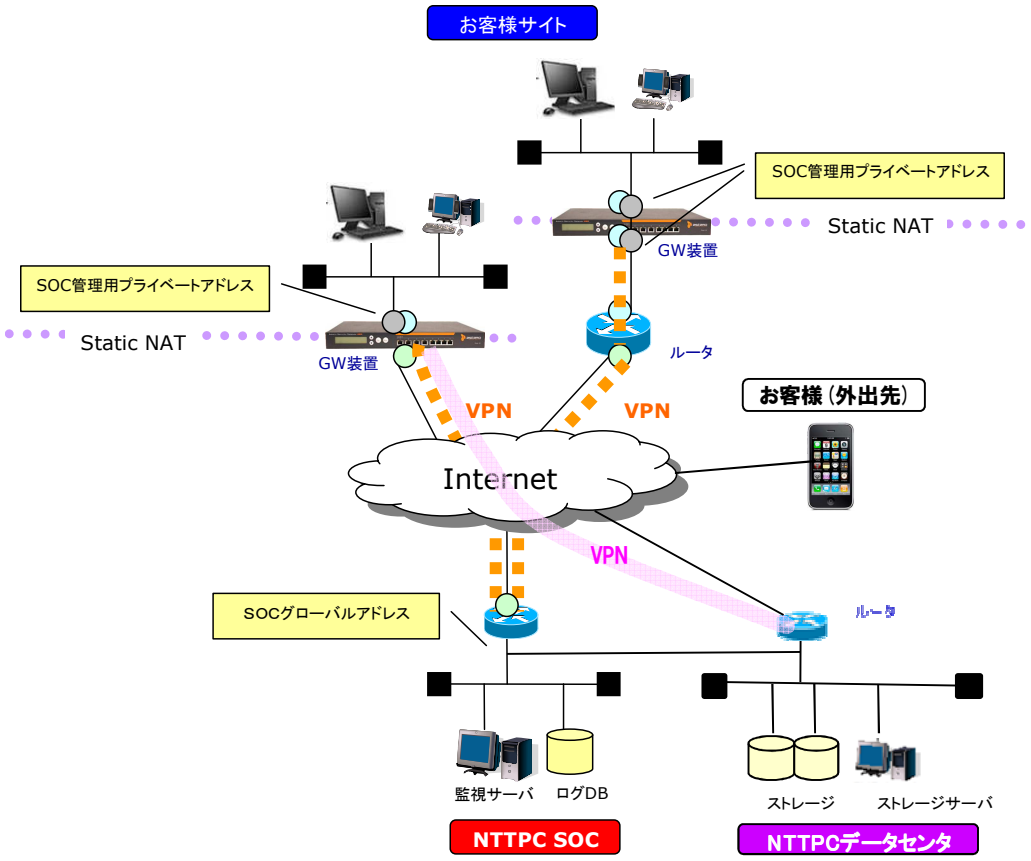


図 2-10 VPN 接続概要

2.3.5.2　ゲートウェイ装置が使用するアドレス帯

ゲートウェイ装置には保守等のため、下記のアドレス帯を使用しております。そのため、契約者は本サービス提供開始後、契約者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出来ません。

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

※　サービス申込時のヒアリングシートから、すでに契約者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。

2.3.5.3 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。

- ♦ 事前に契約者が契約する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契約者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 2-13 のとおりです。

表 2-13 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	契約者－SOC 間の VPN 接続	TCP 443
セキュリティ機能	侵入監視	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
	ファイル転送アプリケーション検知		
	メールアンチウィルス運用	Up2date サイトへのウィルスパターンファイルの更新	UDP 53 UDP 33000-34000 TCP 443
	WEB アンチウィルス運用		
	アンチスパイウェア運用		
	メールアンチスパム運用	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運用	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	契約者－当社データセンタ間の VPN 接続	TCP 443 UDP 500 UDP 4500（NAT-T）

2.3.5.4 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ゲートウェイ装置が 1 日 1 回（デフォルト）、又は 2 回設定された時間より前に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デフォルト設定の場合、午前 1 時に集計し、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デフォルト設定の場合、午前 1 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。
- アンチウィ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契約者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 2-14 のとおりです。

(3) 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。）

(4) 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 2-14 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運用	ユーザからのメールのリリース要求	TCP 3840

2.4 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、故障対応等の契約者からの連絡（電話、又はメール）に対して対応を実施します。

(1)ゲートウェイ・セキュリティ運用監視サービス

表 2-15 サービス対応表

対応内容			受付時間	リードタイム	対応時間
工事	初期工事		・24 時間 365 日 （当日分の受付は 16 時まで）	ヒアリングシート受領後 30 営業日以内	・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		・24 時間 365 日 （当日分の受付は 16 時まで）	ヒアリングシート受領後 15 営業日以内	・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）		・24 時間 365 日 （当日分の受付は 16 時まで）	変更オーダシート受領後 5 営業日以内	・平日 9 時-17 時
	解約オーダ処理		・24 時間 365 日 （当日分の受付は 16 時まで）	解約申請書受領後 30 営業日以内	・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		・24 時間 365 日 （当日分の受付は 15 時まで）	ー	・平日 9 時-15 時
監視	通知	24 時間 365 日死活監視	ー	ー	・24 時間 365 日
		24 時間 365 日侵入監視	ー	ー	・24 時間 365 日
		ファイル転送アプリケーション	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

※ 平日の定義は祝日、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。

※ 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 2-16 サービス対応表

対応内容			受付時間	リードタイム	対応時間
工事	初期工事		・24 時間 365 日 （当日分の受付は 16 時まで）	申込書受領後 5 営業日以内	・平日 9 時-17 時
運用	サービス変更オーダ処理		・24 時間 365 日 （当日分の受付は 16 時まで）	変更申込書受領後 5 営業日以内	・平日 9 時-17 時
	解約オーダ処理		・24 時間 365 日 （当日分の受付は 16 時まで）	解約申請書受領後 30 営業日以内	・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

※ 平日の定義は祝日、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。

※ 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。

3. 品質

3.1 ゲートウェイ装置

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 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、契約者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 3-1 のとおりです。

表 3-1 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	ファイアウォール運用	●	―	―	―	―	―	―
	24 時間 365 日侵入監視	―	●	―	―	―	―	―
	メールアンチウィルス運用	―	―	―	―	―	●	●
	WEB アンチウィルス運用	―	―	―	●	●	―	―
	アンチスパイウェア運用	―	―	―	●	―	―	―
	メールアンチスパムアンチフィッシング運用	―	―	―	―	―	●	●
	URL フィルタリング運用	―	―	―	●	―	―	―
	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 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。

3.2 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。

3.3 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、契約者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契約者毎に保存し、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。

3.4 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契約者連絡先へメールにて連絡いたします。