Symantec™ Email Security.cloud

サービス規定

2018 年 9 月

本サービス規定では、シマンテックの Email Security.cloud (以下「本サービス」) について説明します。本規定で使用されるすべての用語は、本契約 (以下で定義される) または「定義」の条項に記載される意味を持つものとします。

本サービス規定は、参照により組み込まれる添付書類とともに、本サービスの使用を管理するために締結されるお客様の手書き署名もしくはデジタル署名入りのシマンテックとの契約書、またはかかる署名入りの契約書が存在しない場合は、シマンテック社のオンラインサービスの使用条件 (以下、「本契約」) の一部となり、かつ組み込まれるものとします。

目次

1: 技術的/ビジネス的な機能と特性

- サービスの概要
- サービスオプションおよび機能
- サービス内容合意書
- サポート対象のプラットフォームと技術的要件
- ホステッドサービスソフトウェアのコンポーネント

2: お客様の責任

- 利用規約

3: 資格およびサブスクリプション情報

- 課金算出基準
- サブスクリプションへの変更

4: アシスタントおよびテクニカルサポート

- お客様に対するサポート
- テクニカルサポート
- 本サービスやサポートサービスインフラのメンテナンス

5: 追加条項

6: 定義

付属書 A サービス内容合意書

Symantec™ Email Security.cloud

サービス規定

2018 年 9 月

1: 技術的/ビジネス的な機能と特性

サービスの概要

Symantec™ Email Security.cloud は、電子メールメッセージをフィルタリングし、マルウェア (標的型攻撃とフィッシングを含む)、スパム、大量に送信される不要な電子メールから企業を保護するホステッドサービスです。本サービスには暗号化およびデータ保護オプションがあり、電子メールで送信する重要な情報の管理をサポートします。本サービスは、複数のベンダーの複数のメールボックスタイプをサポートします。

サービスの機能

- お客様側の管理者は、パスワード保護した安全なログイン方式を使用してサービス管理コンソールにアクセスできます。お客様は、本サービスの一環として管理コンソールで本サービスの設定と管理、レポートへのアクセス、利用できるデータと統計情報の表示を行うことができます。
- 本サービスは、365 日 24 時間体制で管理されており、ハードウェアの可用性、サービス容量およびネットワークリソースの使用率が監視されています。本サービスはサービスレベルを遵守しているかどうかが定期的に監視され、必要に応じて調整されます。
- 本サービスのレポート機能は、管理コンソールから利用できます。レポートには、アクティビティログや統計情報を含めることができます。お客様は、管理コンソールを使用してレポートの生成を指定し、定期的に電子メールで送信されるように設定するか、または管理コンソールからダウンロードできます。
- 本サービスは、お客様が有効で強制力のあるコンピュータ使用ポリシー、またはそれと同等のものを実施できるようにすることを目的としています。
- シマンテックが提供する推奨単語リストとルールまたはポリシーのテンプレートには、攻撃的と見なされる可能性のある言葉が含まれています。
- 理由の如何を問わず本サービスが中断または停止された場合、シマンテックは、本サービスのプロビジョニングで行われたすべての設定変更を元に戻すことがあります。本サービスを再開する場合、お客様はその他すべての必要な設定変更を行う責任を負うものとします。

サービスオプションおよび機能

本サービスには、メールプロテクトとメールセーフガードの 2 つのオプションがあります。本サービスを利用するには、各ユーザーは (本サービス規定に記載された制限に従い) オプションまたはアドオンとして購入する必要があります。

サービスオプション別機能

	メールプロテクト	メールセーフガード
電子メールのマルウェア対策: フィッシング攻撃や標的型攻撃からの保護を含むマルウェア対策	✓	✓
電子メールスパム対策: スパムやフィッシングからの保護 (リアルタイムリンク追跡を含む)、迷惑メールからの保護	✓	✓
電子メールデータ保護: カスタマイズ可能なコンテンツフィルタポリシー制御		✓

電子メールイメージ制御: 不快感を与える画像の検出		✓
送信フィルタリング	✓	✓
強制的な TLS 暗号化		✓
便宜的な TLS 暗号化	✓	✓
アドレス登録: 無効な受信者の処理	✓	✓
ユーザーおよびグループ LDAP 同期ツール	✓	✓
メッセージ追跡	✓	✓
レポートダッシュボード	✓	✓
概略版（PDF）および詳細版（CSV）のレポート機能	✓	✓
エンドユーザースパム検疫ポータルおよび通知機能	✓	✓
免責事項管理	✓	✓
Policy Based Encryption Essentials		✓
電子メール偽装制御		✓

個別のサービス機能について詳しくは、http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=JA_JP のヘルプを参照してください。

サービスアドオン

	メールプロテクト	メールセーフガード
Advanced Threat Protection: Email	利用可	利用可
Policy Based Encryption Advanced	–	利用可
Email Fraud Protection	利用可	利用可
Email Threat Isolation	利用可	利用可

個別のサービスアドオンについて詳しくは、http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=JA_JP のヘルプを参照してください。Email Fraud Protection のサービス規定については、次の場所を参照してください。https://www.symantec.com/about/legal/repository

Advanced Threat Protection: Email は、電子メール経由で侵入する高度な攻撃を Symantec Cynic™ サンドボックスを使用して検出し、企業またはユーザーを受信者とする標的型電子メール攻撃を識別し、電子メールの配信後に悪質なものに変化する URL を Symantec Click-time™ URL Protection で特定します。O365 ユーザーは、配信後に Cynic™ サンドボックスにより悪質と判断された電子メールを回収する

機能を利用できます。URL 情報、マルウェアカテゴリ、検出方法、ファイルハッシュを含む、マルウェアに関する詳細レポートを作成できます。データフィード API が組み込まれ、ファイルのインポートまたは電子メール送信データなしに認証済み URL を経由してマルウェアレポートを取得できます。Advanced Threat Protection: Email は、担当者のフィッシング攻撃への脆弱性を判定するためにフィッシング攻撃のシミュレーションを実行できる Phishing Readiness サービスへのアクセスも提供します。Phishing Readiness サービスの使用には、https://www.symantec.com/about/legal/repository の利用規約が適用されるものとします。

Policy Based Encryption Advanced では、次のものを利用できます。(i) プル型 Web 取得ポータル。(ii) PGP と S/MIME 配信のサポート。(iii) 透過性の低い暗号化技術に戻る前に TLS 暗号化を試みる機能。(iv) 暗号化 .pdf のプッシュ型配信 (メールセーフガードプランによる Policy Based Encryption Essentials 機能の一環として提供される唯一の暗号化方法)。Policy Based Encryption Advanced のライセンスは、送信ユーザーごとに付与されます。このユーザーはメールセーフガードオプションのユーザー総数に含まれる場合があります。お客様が、電子メールの配信で安全を確保するために Policy Based Encryption Advanced オプションを使用する必要がある場合、配信する電子メール数に基づいて追加のユーザーライセンスをご購入いただけます。その計算方法はシマンテックが定めるものとします。

Symantec™ Email Fraud Protection は、DMARC (ドメインベースのメッセージ認証、レポート、適合) を自動で適用するクラウドサービスです。Symantec Email Fraud Protection を導入すると、DMARC エンフォースメントのあらゆるステップを手動よりもシンプルかつシームレスに完了できます。エンフォースメントによって、認証されていない送信元から生成された電子メールは検疫または拒否されるため、インバウンドの偽装攻撃のリスクが軽減されます。エンフォースメントによって、電子メールの受信者またはメール転送エージェントは、お客様のドメインを信頼できることがわかります。その結果、電子メールの配信可能率が向上します。

Symantec™ Email Threat Isolation は、悪質なリンクを隔離したりリスクを伴う Web ページを安全に表示することで、スピアフィッシング、クレデンシャルの盗難、高度な電子メール攻撃に対する保護を強化します。シマンテックは Email Threat Isolation により、高度なスピアフィッシングまたはクレデンシャルの盗難攻撃など、悪質なリンクを利用する複雑な電子メール攻撃に対して強力な保護を提供します。

Email Threat Isolation は疑わしいリンクをリモートでレンダリングし、予防処置を施した Web コンテンツのみをユーザーに表示してユーザーが電子メールリンクを安全に実行できる環境を提供します。受信するすべてのリンクを悪質なものとして扱い、ユーザーとそのデバイスから離れたリモートの場所で実行するため、シマンテックは悪質なリンクを含むすべての脅威がユーザーに到達することを阻止できます。また、Email Threat Isolation はフィッシング Web サイトを読み取り専用モードで表示し、ユーザーが企業のクレデンシャルやその他の機密情報を入力できないようにすることで、クレデンシャルを狙ったフィッシング攻撃を阻止します。

サービス内容合意書

- シマンテックは、付属書 A に記載のとおり、本サービスに適用されるサービス内容合意書 (以下、「SLA」) を用意しています。

サポート対象のプラットフォームと技術的要件

- 本サービスのサポート対象プラットフォームと技術的要件については、http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=JA_JP をご覧ください。

ホステッドサービスソフトウェアのコンポーネント

- 本サービスには、管理コンソールで利用可能なサービスコンポーネントが含まれており、該当する料金を支払うことで使用できます。

2: お客様の責任

お客様が必要な情報を提供するか、必要な処理を実行する場合にのみ、シマンテックは本サービスを実行できます。それ以外の場合は、次に記載するようにシマンテックの本サービスのパフォーマンスが遅延、低下、抑止されたり、サービス内容合意書に記載された特典の資格が無効になることがあります。

- セットアップの有効化: 本サービスの提供を開始するには、お客様がシマンテックに対して、必要な情報を提供する必要があります。

- お客様の適切な担当者: お客様は、シマンテックからの妥当な要求に応じて本サービスを提供する際にシマンテックを支援する適切な担当者を指名する必要があります。
- お客様は、自分のアカウント情報、パスワード、またはその他のログイン資格情報に責任を負います。
- お客様は、合理的な手段を利用して資格情報を保護することに同意し、お客様のアカウントの不正な使用が判明した場合、速やかにシマンテックに通知するものとします。
- 資格情報の更新: 本サービスを継続的に利用するため、または本サービス期間中に利用可能なアカウント情報とお客様のデータ維持のため、お客様は必要に応じてアカウント管理で該当の「サブスクリプション証書」または「注文確認書」に記載されている新しい資格情報を適用する必要があります。
- お客様の設定とデフォルト設定: お客様は、管理コンソールを使用して本サービスの機能を設定する必要があります (該当する場合)。設定しない場合は、デフォルト設定が適用されます。デフォルト設定が存在しないことがありますが、その場合は、お客様が設定を選択するまでサービスは提供されません。本サービスの設定および使用はお客様によってすべて管理されるため、シマンテックは、お客様による本サービスの使用に対して責任を負いません。また、サービスの運用の結果としてお客様が被る可能性のある民事または刑事責任に対しても責任を負いません。

利用規約

- お客様は、シマンテック社のオンラインサービスの利用規約を遵守する責任を負います。

3: 資格およびサブスクリプション情報

課金算出基準

本サービスは、注文確認書に指定された以下の算出基準でご利用いただけます。

- 「**ユーザー**」とは、本サービスを使用する権限がある、および/または本サービスの使用で恩恵を受ける、もしくは本サービスを一部でも実際に使用する個人やデバイスをいいます。

サブスクリプションへの変更

お客様が直接シマンテックからお客様のサブスクリプションまたは資格を付与されている場合は、お客様とシマンテックとの契約で特に記載がない限り、お客様のサブスクリプションまたは資格に関して承認されている変更通知を CLD_cancellations_MLABS@symantec.com (またはシマンテックが公開している代替アドレス) に送信する必要があります。この手続きに従って送信される通知はすべて、受信された時点で了承されたとみなされます。お客様がシマンテックの販売代理店を経由してお客様のサブスクリプションまたは資格を受け取っている場合は、その販売代理店にお問い合わせください。

4: アシスタントおよびテクニカルサポート

注意: この章は、シマンテックから直接カスタマーアシスタントとサポート (以下「サポート」) を受ける権利を付与されているお客様にのみ該当します。お客様がシマンテックの販売代理店からアシスタントとサポートを受ける権利を付与されている場合、かかるサポートに関して詳しくは、その代理店とお客様が締結した合意書を参照してください。本章に記載されるサポートは、お客様には適用されません。

お客様に対するサポート

シマンテックは、その地域の営業時間に、サービスの一部として次のサポートを提供します。

- 本サービスの実装に関する注文の受付と処理
- サービス機能に対する許可された変更要求の受付と処理
- 請求に関する問い合わせへの対応

テクニカルサポート

本サービスでは、以下に示す初心者レベルのサポートも提供します。

- サポートは、本サービス機能の設定に関してお客様をサポートし、本サービスに関して報告された問題を解決するため、24 時間 365 日利用可能です。サービスのサポートは、https://support.symantec.com/en_US/article.TECH236428.html に公開されている利用規約とテクニカルサポートポリシーに従って履行されます。
- シマンテックはお客様がサポートに送信した問題に重大度レベルを割り当て、次の表に記載されている回答目標時間内に回答するためあらゆる合理的な努力を払うものとします。お客様の行動により障害が発生した場合、または他のサービスプロバイダの対応が必要な場合は、シマンテックの管理の範囲を超えており、このサポート契約の対象とならないことを明記します。

問題の重大度	**サポート (24 時間 365 日体制) 回答目標***
重大度 1: 次のいずれかの状況で、すぐに回避できる方策がない問題が発生した場合: (i) お客様の実稼働サーバーまたはその他のミッションクリティカルなシステムがダウンするか、サービスが大幅に失われている場合、または (ii) お客様のミッションクリティカルなデータのかなりの部分が喪失または破損する重大なリスクにさらされている場合。	30 分以内
重大度 2: 重要な機能が著しい障害を被る問題が発生した場合。お客様は操作方法を制限されますが操作を続行できます。ただし、長期的には生産性に悪影響を及ぼす恐れがあります。	2 時間以内
重大度 3: お客様の業務に限定的に悪影響を及ぼす問題が発生した場合。	翌営業日の同時刻まで**
重大度 4: お客様の業務には悪影響を及ぼさない問題が発生した場合。	翌営業日中。さらに、新機能または機能拡張に関するお客様の提案をシマンテックのフォーラムに投稿することを推奨します。

前のサポート回答目標は通常のサービス業務時の目標であり、次のメンテナンスセクションで説明する本サービスやサポートインフラのメンテナンス時には当てはまりません。

** 回答目標時間は要求に回答するまでの時間であり、問題の解決までの時間 (要求への対応を終了するまでの時間) ではありません。*

*** 「営業日」とは、お客様のローカルタイムゾーンにおけるお住まいの地域の標準的な営業日と営業時間を指し、週末や現地の公休日は除かれます。多くの場合、「営業時間」はお客様のローカルタイムゾーンの午前 9 時から午後 5 時です。*

本サービスやサポートサービスインフラのメンテナンス

シマンテックは、適宜メンテナンスを行うものとします。シマンテックは、可用性の中断を最小限に抑えるため、お客様のアクティビティが少ない時間帯に定期メンテナンスを行うように、商業上合理的な努力を行うものとします。お客様が、これらの定期メンテナンス作業についての事前通知を受け取ることはありません。その他あらゆる種類のメンテナンスおよび以下に示す状況については、［シマンテック製品の状態］ページ (https://status.symantec.com/) に警告を提示することで、影響を受けるお客様に事前に通知するように努めます。サービスの状態、予定メンテナンス、既知の問題について詳しくは［シマンテック製品の状態］ページをご覧になり、Symantec Email Security.cloud ページに登録して最新情報をお受け取りください。**セキュリティスキャンや電子メール配信などのコアサービス機能は、いかなるメンテナンス作業時も中断することはありません。**

- ***予定メンテナンス:*** 「予定メンテナンス」とは、サービスインフラが使用できないため、本サービスが中断または停止される可能性があるスケジュールに基づくメンテナンス期間を意味します。シマンテックは、影響のあるインフラが配置されているタイムゾーンで、お客様の全般的なアクティビティが少ない時間帯に、ネットワーク全体ではなく一部のみに関して予定メンテナンスを実行するように、努力を払うものとします。予定メンテナンス中、本サービスの中断を回避するため、メンテナンスを行っていないインフラにサービスを移動することがあります。予定メンテナンスに関しては、シマンテックは商業的に妥

当な努力を払い、［シマンテック製品の状態］ページへの提示を以てお客様に 7 日前までに通知します。お客様は SMS、電子メール、Twitter でも通知を受信できます。

- ***予定外メンテナンス***「予定外メンテナンス」とは、標準の 7 日前の通知ができず、サービスインフラを使用できないことによりサービスが中断または阻止される可能性がある、スケジュールされたメンテナンス期間をいいます。シマンテックは商業的に妥当な努力を払い、［シマンテック製品の状態］ページへの提示を以てお客様に 1 日前までに通知します。予定外メンテナンス中、本サービスの中断を回避するため、メンテナンスを行っていないインフラにサービスを移動することがあります。シマンテックは緊急メンテナンスを行うことがあります。緊急メンテナンスは、*重大なインシデントを解決または阻止するために可及的速やかに実施する必要があるメンテナンス*と定義されています。シマンテックは緊急メンテナンス開始の 1 時間以上前に［シマンテック製品の状態］ページに警告を提示することで、影響を受ける当事者に通知するように努めます。
- ***管理コンソールメンテナンス:*** 管理コンソールメンテナンスに関しては、シマンテックは商業的に妥当な努力を払い、［シマンテック製品の状態］ページへの提示を以てお客様に 14 日前までに通知します。シマンテックは、管理コンソールの利用の中断期間を最小限に抑えるため、利用者全体の活動が少ない時間帯に管理コンソールのメンテナンスを行うように努力を払うものとします。シマンテックは管理コンソールの軽微な更新を行うことがありますが、お客様が、これらの定期メンテナンス作業についての事前通知を受け取ることはありません。

5: 追加条項

- 本サービスは、適用を受ける輸出コンプライアンスおよび技術上の制限を条件として、その時点で最新のシマンテックの基準に従って世界中でアクセスおよび使用できるものとします。
- シマンテックは、本サービスの主要な機能を大幅に削減しない限り、同等または強化したサービスを提供するために、本サービスの機能を変更したり更新する権利を有します。お客様は、シマンテックが、提供されている本サービスを正確に反映するために、サブスクリプション期間中、随時本サービス規定を更新する権利を留保し、その更新されたサービス規定が投稿時に有効となることを認め、同意します。
- ソフトウェア形式によるすべてのサービスコンポーネントの使用には、当該ソフトウェアに付随する使用許諾契約が適用されるものとします。サービスコンポーネントに付随する EULA（エンドユーザー使用許諾契約）がない場合、http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf に定める条件が適用されます。当該サービスコンポーネントの使用に関する追加の権利と義務は、本サービス規約の規定に従うものとします。
- 本サービス規約に別途指定されている場合を除き、本サービス（付随して提供されるホスト型サービスのすべてのソフトウェアコンポーネントを含む）は、オープンソースやその他のサードパーティの素材を使用する場合があり、その場合、別のライセンスの対象となります。
- シマンテックは、本サービスの有効性を維持するために、いつでも本サービスを更新することができます。
- シマンテックが提供するテンプレートは、お客様が独自にカスタマイズするポリシーや他のテンプレートを作成するために参考として使用されることのみを目的としています。
- 本サービスには以下の制限が適用されます。
    - 1 暦月あたりのユーザーごとのインバウンドとアウトバウンドのメッセージ = 10,000 件。この制限には、お客様を標的としたスパムおよびマルウェアは含まれません。
    - メッセージ制限を超えて使用された場合、シマンテックは、本サービスの契約上残っている月に、通知を以て追加のユーザー分としてお客様に請求する権利を留保します。
    - インバウンドとアウトバウンドのメール再試行スケジュール = 7 日間。
    - デフォルトの最大メールサイズ = 50 MB。お客様は、最大 1,000 MB のメールサイズを指定できます。定められた制限を超えて本サービスが受領したすべての電子メールはブロックおよび削除され、送信者、本来の受信者、管理者に対して警告通知メールが送られます。
    - メッセージ追跡 = データは、トラブルシューティングの検索用に 30 日間利用できます。1 回の調査で返された結果の数に対して追加制限が適用されます。
    - マルウェア検疫 = 電子メールは 30 日後に自動的に削除されます。
    - スパム検疫 = 別途設定されていない限り、電子メールは 14 日後に自動的に削除されます。
    - ダッシュボードのレポートデータの利用可能期間 = 詳細情報は 40 日間、概略情報は 12 カ月。

- 概略版 (PDF) レポートデータの利用可能期間 = 12 カ月。
- 詳細版（CSV）レポートデータの可用性 = 14 日。

- Policy Based Encryption には以下の制限が適用されます。
  - 1 カ月あたりのユーザーごとの Policy Based Encryption (Z) アウトバウンド電子メール = 300 件。
  - Policy Based Encryption Essentials/Advanced の 1 カ月あたりのユーザーごとのアウトバウンド電子メール = 480 件。
  - 複数の受信者に送信する場合は、一意の各アドレスが 1 つの安全な電子メールとして数えられます。任意の月に認められている安全な電子メールの数を超えた場合は、シマンテックは実際の使用分についてお客様に請求する権利を留保します。
  - Policy Based Encryption サービスを経由する電子メールの最大サイズは、50 MB に制限されています。
  - Policy Based Encryption (Z) サービスでプル型暗号化を使用する場合、デフォルトでは、電子メールは安全な取得ポータルに 90 日保管された後、失効します。
  - Policy Based Encryption Advanced サービスでプル型暗号化を使用する場合、デフォルトでは、電子メールは安全な取得ポータルに 30 日保管された後、失効します。
  - 本サービスには可用性および遅延サービスレベルは適用されません。

- 送信中のあらゆる時点でメッセージを確実に保護するために、シマンテックは、お客様が Policy Based Encryption に使用されるドメインを、サービスインフラに送信および受信されるすべてのメッセージに対して TLS 暗号化が適用されるように構成することを推奨します。
- お客様は、シマンテックが提供するルーティング情報を使用して、シマンテックを通じた受信メールの配送を行うものとします。またお客様が、特定のタワーまたは IP アドレスに電子メールを配送することを禁止します。
- 本サービスは、独自のメールドメイン名を持ち、そのドメイン名の MX レコードおよび/または DNS を設定できるお客様のみ利用できます。
- お客様は、すべての必要な IP 範囲からの受信メールを受領し、インフラの一部が利用不可となった場合のサービスの継続性を確保するものとします。
- お客様は、企業への受信メールの配信用メールサーバーアドレスまたはホスト名を指定するものとします。
- お客様は、本サービスを要するすべてのドメイン (サブドメインを含む) がプロビジョニングされていることを保証するものとします。お客様は、プロビジョニングされていないドメインで本サービス機能が正常に動作せず、メール配信が利用できない可能性について承諾するものとします。お客様は、本サービスを受ける有効な電子メールアドレスの一覧 (「確認一覧」) の提供と維持に同意するものとします。本サービスが利用可能になる前および契約期間中に、お客様は確認一覧を検証する責任を負います。確認一覧にない電子メールアドレスに送信された電子メール、または不正確に入力された電子メールは本サービスにより拒否されます。お客様は、SLA が無効なアドレスに送信された電子メールに適用されないことを承諾するものとします。誤解を避けるために、スパム検疫システムを使用するお客様は、確認一覧を維持し、アドレス登録機能を有効にするものとします。お客様がかかる確認一覧を提供できず、アドレス登録機能の無効化を求める場合、シマンテックは単独および絶対の裁量に基づいて、それぞれのかかる要請を状況に応じて見直し、要請を却下する権利を留保します。
- お客様は、お客様のドメイン内で、マルウェアまたはスパムを含むものとして分類された電子メールを解放するか、このような電子メールを解放するようにシマンテックに要請することができます。　　お客様は、お客様の要請によるこのような電子メールの解放に対してシマンテックが責任を負わないことに同意するものとします。
- 本サービスがスパムを識別しなかったこと、または電子メールを誤ってマルウェアまたはスパムとして識別したことに直接的または間接的に起因する損害または損失に対して、シマンテックは責任を負いません。シマンテックは、すべてのアウトバウンドの電子メールをスキャンする権利を留保します。
- デフォルトの免責メッセージは、本サービスがプロビジョニングされた時点から、本サービスがスキャンした電子メールに適用され、お客様はそのテキストを管理コンソールから編集できます。シマンテックは、デフォルトの免責メッセージをいつでも更新できる権利を留保します。
- お客様は、本サービスの使用に関して適用されるすべての法律を遵守する必要があります。国によっては、個々の担当者の同意を得ることが必要な場合があります。本サービスの設定や使用はお客様が完全に管理するため、シマンテックはお客様の本

サービスの使用に対して責任を負いません。また、本サービスの運用の結果としてお客様が被る可能性のある民事または刑事責任に対しても責任を負いません。

- 本サービスをお客様に提供し続けることで、本サービスのセキュリティが損なわれるような場合 (お客様のドメインを狙った、またはお客様のドメインから発生する、ハッキング、サービス拒否攻撃、メール爆弾、その他の悪質な活動を含むがこれに限定されない)、シマンテックがお客様への本サービスを一時的に中断することにお客様は同意するものとします。この場合、シマンテックは速やかにお客様に通知し、お客様と協力して問題を解決します。シマンテックは、セキュリティ上の脅威が取り除かれた時点で、サービスを再開します。
- 理由の如何を問わず本サービスが中断した場合、本サービスはお客様の電子メールに適用されず、電子メールはシマンテックのインフラを使用して配送されません。お客様は、中断中の電子メールをリダイレクトし、サービスが再開したときにすべての設定が正確であることを確認する責任を負います。
- 理由の如何を問わず本サービスが終了した場合、お客様のアカウントは削除され、お客様はサービスを使用できなくなります。
- お客様は、システムで次のことを許可することはできません。(i) オープンリレーまたはオープンプロキシとして稼働する、(ii) スパムを送信する。シマンテックは、お客様が本条に従っていることをいつでも確認できる権利を留保します。誤解を避けるために、本条の違反は本契約の重大な違反となるものであり、シマンテックは本サービスのすべてまたは一部を直ちに中断し、違反が是正されるまでの間停止する権利、もしくは影響を受けたサービスに応じて本契約を終了させる権利を留保するものとします。
- いかなる時点においても、（i）お客様の電子メールシステムがブラックリストに挙がった場合、（ii）お客様がスパムを送信することによりシマンテックがブラックリストに挙がった場合、または（iii）本サービス規定が定める義務をお客様が履行しない場合、シマンテックはお客様に通知を行い、その単独の裁量に基づいて、直ちに本サービスの一部または全部におけるプロビジョニングの保留、サービスの中断または終了を行う権利を留保するものとします。

- お客様は、お客様独自のビジネス目的のみで本サービスの使用を許可されています。お客様は、本サービスおよび関連文書をサードパーティが利用できるようにする再販、再使用許諾、リース、その他を行わないことに同意するものとします。お客様は、シマンテックに事前に書面で同意を得ることなく、競合製品またはサービスの開発、機能またはユーザーインターフェースの模倣、お客様の企業の外部に公表するための本サービスの評価、ベンチマーク、その他の比較分析の目的で、本サービスを使用しないことに同意するものとします。

6: 定義

「**アドレス登録**」とは、本サービスの必須機能を指し、お客様の有効な電子メールアドレスの一覧 (「確認一覧」) に含まれていない電子メールアドレスへのインバウンド電子メールを拒否します。

「**管理者**」とは、お客様の代表として本サービスを管理する権限を持つお客様のユーザーを意味します。管理者は、お客様が指定したサービスの全部または一部を管理できます。

「**スパム対策用ベストプラクティス設定**」とは、シマンテックの推奨する本サービス用の設定ガイドラインを指し、プロビジョニングプロセス時にお客様に提供されるか、オンラインヘルプ資料で公開されます。

「**接続マネージャ**」とは、SMTP ハンドシェイクステージに位置する検出方法をいいます。

「**クレジットリクエスト**」とは、(シマンテックから別途指定されない限り) 件名を「クレジットリクエスト」とし、お客様がシマンテックに対して support.cloud@symantec.com 宛てに電子メールで提出する必要がある通知をいいます。

「**指定タワークラスタ**」とは、お客様に電子メールセキュリティサービスを提供するように指定された 2 つ以上のタワーを指します。

「ドメインレベル設定」とは、管理コンソールで特定のドメイン用にカスタマイズ可能な、電子メールセキュリティサービス向けのドメイン設定を指します。

「**電子メール**」とは、本サービスを経由するすべての受信または送信 SMTP メッセージをいいます。

「電子**メールセキュリティサービス**」とは、メールセーフガードならびにメールプロテクトオプション、およびすべての利用可能なアドオンサービスをいいます。

「電子**メールマルウェア誤検知**」とは、マルウェアを含むと誤って識別された正当な電子メールを指します。

「**エンドユーザー使用許諾契約 (EULA)**」とは、ソフトウェア (以下に定義する) に付随する利用条件を指します。

「**グローバル設定**」とは、本サービスのすべてのドメインとグループレベルに適用される管理コンソールの動作を指します。

「**グループレベル設定**」とは、管理コンソールで特定のグループ用にカスタマイズ可能な、本サービスの当該機能向けのグループ設定を指します。

「**インフラ**」とは、本サービスを提供するために使用する、すべてのシマンテックまたはライセンサーの技術と知的財産を意味します。

「**既知のマルウェア**」とは、シマンテックがコンテンツを受信した時点で、シマンテックが配備したウイルス対策技術により、すでに 1 時間以上シグネチャが利用可能になっていたマルウェアを指します。

「**マルウェア**」または「**悪質なソフトウェア**」とは、コンピュータまたはモバイルの運用を中断するために使用する、または適切な承認を得ることなく重要な情報の収集やプライベートコンピュータシステムへのアクセス取得のために使用するソフトウェアを指します。

「**マルウェア誤検知**」とは、マルウェアを含むと誤って識別された正当な電子メールを指します。

「**メンバー**」とは、お客様、およびお客様とともにレガシーのメールバウンダリエンクリプションアドオンサービスを利用して暗号化されたネットワークを作成するサードパーティを指します。

「**月額料金**」とは、本合意書に定義されている対象サービスの月額料金を意味します。

「**ヘルプ**」とは、http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=JA_JP で入手できる追加情報を指します。

「**オープンプロキシ**」とは、本サービス用の DNS、Web ページ、その他のデータに、匿名のサードパーティまたは認証されていないサードパーティがアクセス、保存、転送できるように設定されたプロキシサーバーを指します。

「**オープンリレー**」とは、匿名のサードパーティまたは認証されていないサードパーティからの電子メールを受信し、電子メールサーバーが接続している電子メールシステムのユーザー以外の 1 人以上の受信者に電子メールを転送するように設定された電子メールサーバーを指します。「スパムリレー」または「パブリックリレー」ともいわれます。

「**注文確認書**」は、「Symantec Online Service の条項」で規定された意味を持つものとします (該当する場合)。本サービスに適用可能な条項が存在しない場合、「注文確認書」は (本項で定義されているとおり) 「サブスクリプション証書」を意味するものとします。

「**本サービス**」とは、お客様が購入した Symantec Email Security.cloud のプロテクトオプションまたはセーフガードオプションを指します。

「**サービスコンポーネント**」とは、本サービスに付随してシマンテックが別途提供する、特定の有効化ソフトウェア、ハードウェア周辺機器および関連文書をいいます。

「**サービスクレジット**」とは、クレジットリクエストが提出され、お客様にクレジットを支払うべきであるとシマンテックが確認した後、お客様の次回請求書で相殺される金額をいいます。

「**サービスソフトウェア**」とは、サービスに必要なことがあり、本サービスを受けるためにお客様の各コンピュータにインストールされている必要がある（以下に定義する）ソフトウェアを意味します。サービスソフトウェアには、本サービスの一環としてシマンテックから別途提供されることがあるソフトウェアと関連文書が含まれます。

「**ソフトウェア**」とは、シマンテックによりお客様に使用許諾され、付随する EULA の条件（本契約に規定された新リリースまたは更新の条件を含むがこれらに限定されない）の対象となる、シマンテックまたはライセンサーのオブジェクトコード形式による各ソフトウェアプログラムをいいます。

「**スパム**」とは、送信者より一方的に送信される商用電子メールをいいます。

「スパム見逃し」とは、本サービスによりスパムとして識別されなかったスパムメールを指します。

「スパム誤検知」とは、本サービスにより誤ってスパムと識別された電子メールを指します。

「**スパム用推奨設定**」とは、シマンテックの推奨する本サービス用の設定ガイドラインを指し、プロビジョニングプロセス時にお客様に提供されるか、ヘルプ資料で公開されます。

「**サブスクリプション契約書**」とは、本サービスに関連するお客様の権利と義務をより詳細に定義する、シマンテックの証明書もしくはシマンテックが発行した類似の文書、または本サービスに付属、先行、もしくは追随するお客様とシマンテック間の書面による合意のうち、該当する 1 つ以上の文書を指します。

「**Symantec Hosted Service の条項**」は、https://www.symantec.com/about/legal/service-agreements.jsp で参照できる条項を指します。

「**Symantec Online Service の条項**」は、https://www.symantec.com/about/legal/service-agreements.jsp で参照できる条項を指します。

「**シマンテックトラッカー**」とは、サービス可用性および遅延を測定するシマンテックのツールをいいます。

「**タワー**」とは、負荷分散されたメールサーバーのクラスタをいいます。

「**ユーザー**」とは、電子メールを送受信する個人を指し、本サービスのすべての条項で保護されます。

付属書 A

サービス内容合意書

その他

- シマンテックが定められたサービスレベルを満たさなかった場合、お客様はサービスクレジットを受ける資格を得られます。お客様がサービスクレジットを受ける権利があると考える場合、お客様はサービスレベル違反が疑われた月の最終日から 10 営業日以内に、クレジットリクエストを提出するものとします。お客様は、ログ記録は限られた日数しか保存されず、規定された期間外に提出されたクレジットリクエストは無効とみなされることを了承するものとします。
- Symantec Technical Support にご連絡いただくと、クレジットリクエストを行うことができます。手順について詳しくは、https://support.symantec.com/en_US/email-security-cloud..html.
- すべてのクレジットリクエストは、本サービス内容合意書の適用条項に従ってシマンテックが検証する対象となります。シマンテックは、クレジットリクエストの検証のためお客様に追加情報を求めることができます。
- 本サービス内容合意書は、次の場合無効となります。(i) 予定メンテナンスまたは緊急メンテナンスの期間、もしくは不可抗力、またはお客様かサードパーティの活動、不作為により使用できない期間、(ii) 本合意書の条件に基づいたシマンテックのサービス中断期間、(iii) お客様が本合意書に違反 (請求未払いを含むがこれに限定されない) した場合、(iv) お客様が本合意書に従って本サービスを設定しなかった場合、(v) 体験版使用期間中。
- 本サービス内容合意書に規定する救済は、本サービス内容合意書に関する、契約違反、不法行為 (過失を含むがこれに限定されない)、その他に基づく、お客様の唯一かつ排他的な救済であるものとします。
- 本サービス内容合意書に基づく任意の月のシマンテックの月額最大累積負担は、月額料金の 100% もしくは $10,000、£5,000、€10,000 (お客様が請求する通貨による) のうちで金額が低い方と同等のクレジットとします。
- 購入したサービスバンドルに含まれるサービスが影響を受けた場合、サービスクレジットはサービスバンドル全体ではなく影響を受けたサービスに基づいて計算されます。

電子メールセキュリティサービスのサービス内容合意書の例外事項

本サービス内容合意書は、次の場合無効となります。(i) 本サービスを経由していない電子メール (シマンテックインフラからのインバウンド電子メールのみを受領する適切なステップをお客様が踏まなかった場合を含むがこれに限定されない)、(ii) 最初にシマンテックに送信されたときに 1 つの SMTP セッションあたり 500 人を超える受信者を含むインバウンドまたはアウトバウンド電子メール、(iii) バルククラスタタワーとして指定されたタワーにプロビジョニングされたお客様、(iv) 本サービス用にプロビジョニングされていないお客様のドメインを対象としたインバウンドまたはアウトバウンド電子メール。

サービス可用性

サービス可用性のサービスレベルは、お客様の MTA とシマンテックインフラ間のポート 25 の SMTP セッションを RFC5321 に準拠して確立する機能によって定義されます。サービス可用性のサービスレベルは、管理ポータルまたはスパム検疫システムには適用されません。本サービスレベルは、お客様が本サービスを誤って設定している場合、またはシマンテックの合理的な制御を超えた予想不能の事情または原因 (自然災害、戦争、テロ、暴動、行政措置、シマンテックのデータセンター外部 (お客様のサイト内またはお客様のサイトとシマンテックのデータセンター間を含む) でのネットワークまたはデバイス障害を含むがこれに限定されない) による場合には適用されません。

サービス可用性が任意の月で 100% を下回る場合、お客様はクレジットリクエストを提出し、以下に示すクレジットの割合に対して、月額料金の 100%、もしくは $10,000、£5,000、€10,000 (お客様の請求通貨による) の低い方の金額と同等のサービスクレジットを受け取ることができます。

1 暦月あたりの可用性の割合	月額料金に対するクレジットの割合

99% 以上 100% 未満	25%
98% 以上 99% 未満	50%
98% 未満	100%

サービス可用性が任意の月で 98% を下回る場合、シマンテックの承認により、お客様は影響を受けたサービスを終了し、終了後に期間の一部に対して前支払いした料金の解除後の期間に相当する按分額の払い戻しを受ける権利を有します。

電子メール配信

電子メール配信のサービスレベルは、以下の条件の両方にあてはまる、お客様が送受信するすべての電子メールを 100% 配信するシマンテックの機能によって定義されます。

a) 電子メールはシマンテックが受信している

b) マルウェア、スパム、本サービスが傍受する対象となるその他のコンテンツが電子メールに含まれない

前述の条件に従って、お客様が送受信する電子メールをシマンテックが配信できず、お客様が本合意書の条件に違反していない場合、お客様は 30 日前の書面による事前通知にて本サービスを終了する権利があるものとします。

電子メール配信遅延

電子メール配信遅延のサービスレベルは、お客様の指定タワークラスタの各タワーで 5 分ごとに送受信される電子メールの 1 暦月の平均往復時間 (シマンテックトラッカーにより計測) が、以下の表に記載された遅延を超えているかどうかにより定義されます。メール配信遅延のサービスレベルが満たされていないとお客様が判断する場合、クレジットリクエストを提出し、以下の表に従ってサービスクレジットを受け取れます。

平均往復時間（秒）	月額料金に対するクレジットの割合
60 より長く 90 以下	25%
90 より長く 120 以下	50%
120 より長く 180 以下	75%
180 より長い	100%

この遅延サービスレベルは、以下には適用されません。

a) お客様がシマンテックに確認一覧を提供せず、サービス拒否攻撃を受けた場合

b) お客様のシステムからのメールループおよびお客様のシステムへのメールループによる遅延期間

c) お客様のプライマリ電子メールサーバーが最初の配信時に電子メールを受信できなかった場合

スパム誤検知

スパム誤検知サービスレベルでは、最大スパム誤検知取得率を定義します。スパム誤検知サービスレベルは、お客様がヘルプ資料に定められたスパム対策用ベストプラクティス設定を実装する場合にのみ適用されます。任意の月の平均スパム誤検知取得率がお客様のインバウンド電子メールトラフィックの 0.0003% を超えた場合、お客様はクレジットリクエストを提出し、以下の表に従ってサービスクレジットを受け取れます。

スパム誤検知取得率（%）	月額料金に対するクレジットの割合
0.0003 より大きく 0.003 以下	25%
0.003 より大きく 0.03 以下	50%
0.03 より大きく 0.3 以下	75%
0.3 より大きい	100%

以下にあてはまる電子メールは、このサービスレベルにおいて、スパム誤検知メールに含まれません。
a) 正当なビジネス電子メールでない電子メール
b) 受信者が 20 人以上の電子メール
c) お客様の遮断送信者リストに含まれる送信者からの電子メール (お客様がユーザーレベル設定を有効にしていた場合に個人ユーザーが指定したものを含むがこれに限定されない)
d）危害を受けたコンピュータから送信された電子メール、
e）サードパーティのブロックリストに挙げられているコンピュータから送信された電子メール、
f) アウトバウンドスパムスキャンにより傍受された電子メール

サービスクレジットの対象となるには、スパム誤検知の疑いのある電子メール受領の 5 日以内に、Symantec Technical Support に報告する必要があります。シマンテックは、電子メールがスパム誤検知かどうかを調査、確認し、結果を記録します。

スパム検知率

スパム検知率サービスレベルでは、最小スパム検知率を定義します。このサービスレベルは、お客様がヘルプ資料に定められたスパム対策用ベストプラクティス設定を実装する場合にのみ適用されます。このサービスレベルは、1 暦月に計測されたスパム見逃しの数に対応します。お客様は、クレジットリクエストを提出し、以下の表に従ってサービスクレジットを受け取れます。

スパム検知率（%）	月額料金に対するクレジットの割合
98 より大きく 99 以下	25%
97 より大きく 98 以下	50%
96 より大きく 97 以下	75%
96 以下	100%

このスパム検知率サービスレベルは、有効な電子メールアドレスに送信されていない電子メールには適用されません。95% を下回るスパム検知率は、50% を超える全角文字セットを含む電子メールに適用されるものとします。かかるスパム検知率が 95% を下回る場合、お客様は月額料金の 25% のサービスクレジットを受ける資格があるものとします。かかるスパム検知率が 90% を下回る場合、お客様は月額料金の 100% と同じサービスクレジットを受ける資格があるものとします。

サービスクレジットの対象となるには、スパム見逃しの疑いのある電子メール受領の 5 日以内に、Symantec Technical Support に報告する必要があります。シマンテックは、電子メールがスパム見逃しかどうかを調査、確認し、結果を記録します。

マルウェア対策

お客様のシステムが、クラウドスキャンサービスを経由した電子メールを介して拡散する既知または未知のマルウェアによって感染した場合、お客様は、以下に定める金額のサービスクレジットを受け取れる場合があります。お客様は、かかるマルウェアの検出から 5 日以内にシマンテックに通知し、シマンテックはかかる通知を記録、調査、検証するものとします。お客様はクレジットリクエストを提出するものとし、該当すると確認された場合、月額料金の 100%、もしくは $10,000、£5,000、€10,000 (お客様の請求通貨による) の低いほうの金額と同等のサービスクレジットを受け取れます。本条に規定する救済は、本サービスを通じてお客様またはサードパーティに渡ったマルウェアによる感染における、契約、不法行為 (過失を含むがこれに限定されない)、その他における唯一かつ排他的な救済であるものとします。誤解を避けるために、本条に定める救済は意図的な自己感染の場合には適用されないものとします。

電子メールに添付されたマルウェアが本サービスをすり抜けて受信され、そのマルウェアが自動的または手作業のいずれかによってお客様のシステム内でアクティブ化された場合に、お客様のシステムは感染したとみなされます。マルウェアが添付された電子メールをシマンテックが検出したが阻止できなかった場合でも、［シマンテック製品の状態］ページに更新情報を公開するか、その他の方法でお客様に通知し、お客様が感染した電子メールを特定して削除できる十分な情報を提供した場合、上記に定める救済は適用されないものとします。

本サービスは、可能な限り多くの電子メールと添付ファイルをスキャンします。送信者によって直接制御されているコンテンツを含む添付ファイルはスキャンできない場合があります(パスワード保護または暗号化された添付ファイルやパスワードが電子メールとは別に送信される場合など)。かかる電子メールまたは添付ファイルについては、サービスレベルの対象とならず、前述の定められた救済は適用されません。

本マルウェア対策サービスレベルは、お客様またはお客様のリクエストに応じてシマンテックが意図的にリリースしたマルウェアに関連する場合は無効となります。

本マルウェア対策サービスレベルは、本サービス規定で定めるとおりマルウェアにのみ適用されるものであり、スパイウェア、アドウェア、悪質なコンテンツを提供する Web サイトの URL リンク、未知のトロイの木馬には適用されません。

マルウェア誤検知

マルウェア誤検知サービスレベルは、最大マルウェア誤検知率を定めます。任意の月の電子メールマルウェア誤検知取得率がお客様の電子メールトラフィックの 0.0001% を超えた場合、お客様はクレジットリクエストを提出し、以下の表に従ってサービスクレジットを受け取れます。

マルウェア誤検知取得率（%）	月額料金に対するクレジットの割合
0.0001 より大きく 0.001 以下	25%
0.001 より大きく 0.01 以下	50%
0.01 より大きく 0.1 以下	75%
0.1 より大きい	100%

365 日 24 時間体制のテクニカルサポートとエラー応答

テクニカルサポートは、以下について 365 日 24 時間体制で利用可能です。

a）本サービスにおける問題について、お客様にテクニカルサポートを提供、

b）かかる問題解決のためのお客様との通信。