Symantec™ Email Security.cloud

サービス規定

2019 年 11 月

以下に記載された CA サービス (以下「CA サービス」) は、お客様および CA 事業体 (以下「CA」) が締結し、お客様が CA サービスのサブスクリプションを取得する際に使用した CA の見積またはその他のトランザクション文書で参照される条項に加えて、以下の条項に基づいて提供されます。これらの条項は、当該注文書の有効日から有効になるものとします。

本サービス規定では、CA 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。

目次

Symantec™ Email Security.cloud

サービス規定

2019 年 11 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 (ターゲット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

- お客様は、パスワードで保護された安全なログイン方式を利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、管理コンソールを使用して本サービスの設定と管理、レポートへのアクセス、データと統計情報の表示を実行できます (これらの操作が本サービスで利用できる場合)。
- 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。
- CA 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、CA 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。

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ターゲット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隔離ポータル、API、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
Email Threat Detection and Response	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 Threat Detection and Response (ETDR) 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。さらに、侵害の兆候に基づいて電子メールをブラックリスト化することにより、お客様が電子メール攻撃を修復するのに役立ちます。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。Email Threat Detection and Response では、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されます。Phishing Readiness サービスの使用には、https://www.symantec.com/enterprise-legal 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 CA 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。Email Fraud Protection はスタンドアロンサービスとしても利用できます。Email Fraud Protection のサービス規定については、https://www.symantec.com/enterprise-legal を参照してください。

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、資格情報の盗難、高度な電子メール攻撃に対する保護を強化します。CA は Email Threat Isolation により、高度なスピアフィッシングまたは資格情報の盗難攻撃など、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、Web セッションをリモートで実行してユーザーのブラウザに安全なレンダリング情報のみを送信することにより、ユーザーとユーザーの電子メールリンク、または添付ファイル間の安全な実行環境を提供します結果として、CA は、悪質なリンクと添付ファイルが含まれた脅威がユーザーに到達することを防ぎます。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、ユーザーが企業の資格情報やその他の機密情報を入力できないようにすることで、資格情報を狙ったフィッシング攻撃を阻止します。Email Threat Isolation はスタンドアロンサービスとしても利用できます。Email Threat Isolation のサービス規定については、https://www.symantec.com/enterprise-legal を参照してください。

サービス内容合意書

- CA 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。

サービスソフトウェアのコンポーネント

- 本サービスには次のオプションのコンポーネントが含まれます。**同期ツール**
- いかなるソフトウェアの使用も本契約に従い、該当する場合は、www.symantec.com/enterprise-legal で本サービス規定とともに公開されている追加の利用規約に従います。

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、CA は本サービスを実行できます。それ以外の場合は、CA 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 CA 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、本サービスを提供する際に CA を支援する適切な担当者を指名する必要があります。
- 資格情報の更新: 継続的に本サービスを受けるため、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を維持するため、必要な場合、お客様は該当する注文確認書に記載される新しい資格情報をアカウント管理で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、CA 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。

3: 資格およびライセンス情報

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。

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

CA 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

CA がお客様にテクニカルサポートを提供している場合、テクニカルサポートは以下に示すサービスの一部として含まれます。テクニカルサポートが販売代理店によって提供されている場合、本条項は適用されません。

- 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。
- CA 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、CA の管理の範囲を超えており、このサポート目標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 CA のフォーラムに投稿することを推奨します。

上記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

CA は、適宜メンテナンスを行うものとします。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 https://status.symantec.com/ を参照してください。以下に、当該メンテナンスに当たるメンテナンスを示します。

- **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。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、CA はお客様に 7 日前までに通知します。
- **予定外メンテナンス**「予定外メンテナンス」とは、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。CA はお客様に 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。CA 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。緊急メンテナンスに関しては、できるだけ速やかにお客様に通知します。
- **注意:** 管理コンソールのメンテナンスに関しては、CA はお客様に 14 日前までに通知します。CA は事前の通知なく管理コンソールの軽微な更新や定期メンテナンスを行う場合がありますが、これらの活動ではサービスの中断は発生しません。

5: 追加条項

- CA 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、CA 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。
- スパム隔離 = 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。
- 検疫されたマルウェアやスパム電子メールは上記の検疫の場所にのみ保存されます。たとえばバックアップの目的で別の場所に保存されることはありません。
- 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 = 40 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、CA 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、CA 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、CA が提供するルーティング情報を使用して、CA 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 IP 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、スパム隔離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、CA 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 CA 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 CA 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、CA は責任を負いません。CA 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。CA 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、CA 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)、CA 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、CA 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。CA は、セキュリティ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 CA 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。CA 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、CA 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 CA システム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、CA 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、CA 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、CA 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。

「**指定タワークラスタ**」とは、お客様に本サービスを提供するように指定された 2 つ以上のタワーをいいます。

「**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。

「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。

「**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。

「**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。

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

「**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、「CA のオンラインサービスの利用規約」で規定された意味を持つものとします。

「サービスクレジット」とは、お客様の現在のライセンス期間に追加される日数を意味します。

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

「**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意味します。

「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。

「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 CA 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

第 1.0 条 その他

これらのサービス内容合意書 (以下「SLA」) は、本サービス規定の対象となるオンラインサービスにのみ適用されます。 CA がこれらの SLA を達成しなかった場合、お客様にはサービスクレジットを受け取る資格が与えられます。サービスクレジットは、この SLA の未達成に対する、お客様の唯一かつ排他的な救済、および CA による唯一かつ排他的な責任となります。

第 2.0 条 サービス内容合意書

a. **可用性。**本 SLA は以下に適用されます。Email Protect、Email Safeguard、Email Threat Detection and Response。可用性は、本サービスの分単位の運用時間であり、1 暦月あたりの割合で表されます。ただし、免責対象の停止を除きます。可用性の SLA は、i) インライン (データプレーン) サービス、および ii) 非インライン (コントロールプレーン) サービスがそれぞれ対象になります。

- **インラインサービス可用性**は、お客様とインターネット間で転送中のデータに影響する、本サービスのコア機能へのアクセスを意味します。本サービスのインライン機能は、お客様のメール転送エージェント (MTA) が RFC5321 に準拠し、ポート 25 での SMTP セッションを確立するためのサービスインフラの可用性を意味します。本 SLA は、管理コンソールまたはスパム隔離システムには適用されません。

インラインサービス可用性	**99.999%**

- **非インラインサービス可用性**は、エンドユーザーとインターネット間で転送中のデータに影響しない、本サービスの機能を制御するコントロールへのアクセスを意味します (例: 管理者が使用するレポートツール)。

非インラインサービス可用性	**該当なし**

b. **その他の SLA**: その他の SLA はすべて、本サービスによって受信される電子メールに適用されます。

- **電子メールの遅延**: 本サービスが電子メールを受け取り、サービスインフラから目的の受信者に電子メールが送信されるまでの時間が、シマンテックトラッカーによって測定される以下の平均往復時間を超過した場合、お客様はサービスクレジットを要求できます。遅延 SLA は、以下の場合には適用されません。a) お客様が確認一覧を提供していない、およびお客様がサービス拒否攻撃を受けている、b) 遅延時間がお客様のシステムを宛先または送信元とするメールループに起因している、c) 最初の配信の試行でお客様のプライマリ電子メールサーバーが電子メールを受信できない。

平均往復時間	**60 秒**

- **電子メール配信:** CA が次の条件でお客様との間で電子メールを送受信できなかった場合、お客様はサービスクレジットを要求できます。a) 電子メールが CA によって確実に受信されている、かつ b) マルウェアやスパムなど、本サービスによって阻止される理由となるコンテンツが電子メールに含まれていない。電子メール配信は、本サービスによって処理された、お客様との間で送受信したすべての電子メールの 1 暦月あたりの割合で測定されます。

電子メール配信	**100%**

- **スパム誤検知:** 本 SLA は以下に適用されます。Email Protect、Email Safeguard。オンラインヘルプリソースで提供されている「スパム対策用ベストプラクティス設定」をお客様が実施している状況で、本サービスによってスパムと誤検知された正当なビジネス電子メールの数が以下のスパム誤検知取得率を超過した場合、お客様はサービスクレジットを要求できます。スパム誤検知は、本サービスによって処理された、お客様との間で送受信したすべての電子メール

の 1 暦月あたりの割合で測定されます。以下の電子メールは、本 SLA の目的においてスパム誤検知電子メールに含まれません。a) 正当なビジネス電子メールではない電子メール、b) 受信者数が 20 人を超える電子メール、c) 電子メールの送信者がお客様の送信者遮断リストに登録されている電子メール (お客様がユーザーレベル設定を有効にしている場合、個別のユーザーによって定義された送信者も含むがこれに限定されない)、d) 危殆化したコンピュータから送信された電子メール、e) サードパーティの遮断リストに登録された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って阻止された電子メール。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、CA に報告する必要があります。CA 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。

スパム誤検知取得率	**0.0003% 未満**

- **スパム検知率:** 本 SLA は以下に適用されます。Email Protect、Email Safeguard。オンラインヘルプリソースで提供されている「スパム対策用ベストプラクティス設定」をお客様が実施している状況で、お客様との間で送受信されたスパムを含む電子メールの本サービスによる検知率が以下の最小割合を下回った場合、お客様はサービスクレジットを要求できます。スパム検知率は、本サービスによって処理された、お客様との間で送受信したすべての電子メールの 1 暦月あたりの割合で測定されます。このスパム検知率 SLA 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。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、CA に報告する必要があります。CA 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。

スパム検知率	**99%**
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**スパム検知率 SLA**	**95%**

- **マルウェア対策:** 本 SLA は以下に適用されます。Email Protect、Email Safeguard。本サービスをすり抜けた電子メールによって伝播した既知または未知のマルウェアによってお客様のシステムが感染した場合、お客様はサービスクレジットを要求できます。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見なされます。以下は、マルウェア対策 SLA から除外されます。(a) CA が最新情報の公開またはお客様への通知により、お客様が感染した電子メールを特定して削除できるだけの十分な情報を提供した、CA が検出したが停止しなかった電子メールの添付ファイルのマルウェア、(b) 送信者が直接制御するコンテンツを含む添付ファイル (例: パスワード保護および/または暗号化された添付ファイル、電子メールとは別にパスワードが送信されている)、あるいは (c) お客様によって、またはお客様からの要求により CA によって故意に解放されたマルウェア。本マルウェア対策 SLA 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。お客様は、かかるマルウェアの検出から 5 日以内に CA に通知し、CA はかかる通知を記録、調査、検証するものとします。

マルウェア対策 SLA	**100%**

- **マルウェア誤検知:** 本 SLA は以下に適用されます。Email Protect、Email Safeguard。本サービスによってマルウェアを含むと誤検知された正当なビジネス電子メールの数が以下のマルウェア誤検知取得率を超過した場合、お客様はサービスクレジットを要求できます。マルウェア誤検知取得率は、本サービスによって処理された、お客様との間で送受信したすべての電子メールの 1 暦月あたりの割合で測定されます。

マルウェア誤検知取得率	**0.0001% 未満**

第 3.0 条 可用性の計算

可用性は、分単位の合計時間を 100% として、1 暦月あたりの割合で次のように計算されます。

$$\frac{\text{1 暦月の分単位の合計時間 - 免責対象の停止 - 免責対象外の停止*}}{\text{合計 - 免責対象の停止}} \times 100 > \text{可用性目標}$$

**免責対象外の停止 = 免責対象ではない分単位のサービス停止時間*

注意: 可用性の計算はサービスの開始日にかかわらず、1 暦月全体に基づいて計算されます。

第 4.0 条 サービスクレジット

請求が作成および検証されると、お客様のアカウントにサービスクレジットが適用されます。

可用性 SLA: CA は、24 時間中にサービスを利用できない各 1 時間またはその一部 (集計値) に対して、2 日間の追加サービスに相当するサービスクレジットを提供します。ただし、24 時間中に発生したすべてのインシデントについて 7 暦日を上限とします。

その他すべての SLA の種類: CA は、24 時間中に未達成となった個別の SLA に対して、2 日間の追加サービスに相当するサービスクレジットを提供します。ただし、24 時間中に発生したその SLA に関連したすべてのインシデントについて 7 暦日を上限とします。

お客様は 12 カ月間で最大 4 回、28 日間のサービスクレジットを受け取ることができます。この最大値は、12 カ月間で作成されたすべての請求に対する合計です。

サービスクレジットは、

- 同じアカウント内でも、その他の CA のオンラインサービスに転送または適用することはできません。
- お客様が後続の契約期間を更新しない場合でも利用できる唯一の救済です。サービスクレジットは、お客様の現在のライセンス期間の終わりに追加されます。
- いかなる種類の払い戻しまたはクレジットにも交換できません。
- その他の SLA の違反が本サービスの可用性低下に関連している場合、かかる違反には適用されません。その場合、お客様は可用性 SLA についてのみ請求を送信できます。

第 5.0 条 請求プロセス

お客様は請求の書面を電子メールで CA カスタマーサポート宛てに提出する必要があります。シマンテックが請求を確認するため、各請求は申し立ての対象となる SLA の未達成が発生した歴月末から 10 日内に提出する必要があります。各請求には、以下の情報を含めてください。

(i) 件名に「サービスクレジットの要求」という文言。
(ii) 対象月における請求対象の停止またはその他の SLA の未達成 1 件ごとの日付および期間 (該当する場合)。
(iii) 関連する計算をすべて含む、本サービス規定に基づく請求の説明。

すべての請求は、シマンテックのシステムレコードに照らして検証されます。請求に対して異議がある場合、シマンテックはシステムログ、監視レポート、設定レコードに基づき誠実に判断を下し、問題となる期間のサービス可用性の記録をお客様に提供します。

第 6.0 条 免責対象の停止と請求からの除外

免責対象の停止として定義された分単位の停止時間を以下に示します。

- 本サービス規定で定義された予定メンテナンスおよび予定外メンテナンス。
- 本契約で定義された不可抗力。
- 以下に示す請求の除外に起因する停止時間。

以下のいずれかの除外が適用される場合、請求は受領されません。

- 体験版、評価版、概念実証、非売品、プレリリース、ベータ版を含むがこれに限定されない、臨時的に提供されたサービス。
- お客様が本サービスの料金を支払っていない。
- 本サービスとともに転売された、サードパーティの、シマンテック以外のブランドの製品またはサービス。
- シマンテックの管理下にない、または本サービスの対象外であるハードウェア、ソフトウェア、その他のデータセンターの設備またはサービス。

- 本サービスで使用するために提供されるサービスコンポーネントではないアイテム。
- 本サービスとともに提供されるテクニカルサポート。
- お客様が本サービス規定に従って本サービスを正しく設定していない。
- シマンテックから事前に書面による同意を得ていない、お客様によるハードウェアまたはソフトウェアの設定変更。
- 特定の Web ページまたはサードパーティのクラウドアプリケーションを使用できない。
- 個別のデータセンターの停止。
- 本サービス内のホスティング場所で 1 つ以上の固有の機能または機器を使用できなくなったが、その他の主な機能を使用できる。
- お客様のインターネットアクセス接続の障害。
- お客様の本サービスの使用権の停止または終了。
- シマンテックによる改変または変更ではない (またはシマンテックによる指示または承認なしの)、本サービスの改変または変更。
- シマンテックまたはそのエージェントにより生じた場合を除く、不正使用、またはシマンテックの公開済みドキュメントに従っていない使用による本サービスの欠陥。
- お客様が要求したハードウェアまたはソフトウェアのアップグレード、移動、設備のアップグレードなど。

サービス固有の除外: Email Security.cloud の場合、以下に対して SLA は適用されません: (i) 本サービスを経由していない電子メール (サービス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。

以上、付属書 A