

SHIELDeXpress オンデマンド  
メールセキュリティ on-Demand  
サービス仕様書兼 SLA

Ver.1.1

2011/09/21

(株) 日立システムズ

SHIELDDeXpress セキュリティオンデマンド  
メールセキュリティ on-Demand サービス仕様書兼 SLA

---

<変更履歴>

#	変更日付	変更箇所	変更内容
1	2010/08/31		新規作成

<目次>

用語の定義 .....	5
<b>1. サービス全体にかかわる事項 .....</b>	<b>6</b>
1. 1 サービス概要 .....	6
1. 2 サービス導入条件 .....	6
1. 3 サービス導入時の同意事項 .....	7
1. 4 サービス利用中の同意事項 .....	8
1. 5 サポート対応 .....	8
1. 6 予定メンテナンス .....	9
1. 7 クライアントネットおよびアナウンス .....	9
1. 8 適用法 .....	9
<b>2. アンチウイルス (AV) サービス .....</b>	<b>10</b>
2. 1 処理対象 .....	10
2. 2 処理方法 .....	10
2. 3 ウイルス検知時の対応 .....	10
2. 3. 1 受信 E メールにおける通知 .....	10
2. 3. 2 送信 E メールにおける通知 .....	10
2. 3. 3 ウイルスに感染した Eメールの措置 .....	10
2. 4 ウイルスに感染した Eメールの確認 .....	10
2. 5 諸注意 .....	10
<b>3. アンチスパム (AS) サービス .....</b>	<b>11</b>
3. 1 処理対象 .....	11
3. 2 処理方法 .....	11
3. 3 スпам検知時の処理 .....	11
3. 4 スпам隔離に関する説明 .....	11
3. 5 確認 .....	12
3. 6 諸注意 .....	12
<b>4. コンテンツ監視 (CC) サービス .....</b>	<b>13</b>
4. 1 処理対象 .....	13
4. 2 処理方法 .....	13
4. 3 監視対象 Eメール検知時の処理 .....	13
4. 4 確認 .....	13
4. 5 諸注意 .....	13
<b>5. イメージ監視 (IC) サービス .....</b>	<b>15</b>

SHIELDExpress セキュリティオンデマンド  
メールセキュリティ on-Demand サービス仕様書兼 SLA

---

5. 1	処理対象 .....	15
5. 2	処理方法 .....	15
5. 3	不適切な画像検知時の処理 .....	15
5. 4	確認 .....	15
5. 5	諸注意 .....	15
<b>6. SLA</b>	.....	<b>17</b>
6. 1	定義 .....	17
6. 2	一般規定 .....	17
6. 3	100%サービス可用性 .....	18
6. 4	100%Eメール配信 .....	19
6. 5	Eメール待ち時間-60 秒 .....	19
6. 6	スパム-偽陽性 0.0003%.....	20
6. 7	95%スパム検知率 .....	21
6. 8	スパムサービスクレジットの要請 .....	21
6. 9	Eメールウイルス保護-100% .....	22
6. 10	Eメールウイルス偽陽性 0.0001% .....	23

## 用語の定義

用語	定義
本サービス	メールセキュリティ on-Demand
対象 E メールシステム	本サービスを利用する対象の E メールシステム (E メールサーバ、DNS サーバ等を含む)
クライアントネット	本サービスにおいてお客様の情報を管理するためのポータルサイト。 サービス導入時、利用時には本サイトを利用して、お客様に各種設定をしていただく必要があります。サービス導入時、お客様単位で 1 アカウントを提供します。
管理マネージャ	本サービスにおいてメールアドレスごとに提供する、 スパムメール到着等の情報を参照するためのポータルサイト。サービス導入時、お客様希望に応じ、メールアドレスごとにアカウントを提供します。
有効メールアドレス	本サービスを利用するために当社のサーバへ登録した、メールアドレスの総称です。 初期登録は、新規サービスを申し込みされた際に当社が行います。 サービス利用開始後は、お客様自身がクライアントネットからアドレスの登録、変更、削除を行います。
クレジットリクエスト	お客様が弊社に、件名に「クレジットリクエスト」と記載した shield-ondemand@hitachijoho.com宛の E メールを送付することにより行わなければならない通知をいう(弊社が別途通知する場合を除く。)
指定タワークラスタ	お客様にサービスを提供するために指定される 2 ヶ以上の場所に配置される二つ以上のタワー群をいう。
E メールサービス可用性	指定タワークラスタのポート 25 上に、メッセージラボ・トラッカーの測定に基づき SMTP セッションを確立する能力をいう。
E メールウイルス偽陽性	誤ってウイルスを含んだものとして識別または検知された正当な E メールをいう。
E メールサービス	E メール AV、E メール AS、E メール IC、および E メール CC サービスをいう。
E メール待ち時間	メッセージラボ・トラッカーが測定する、各 E メールサービスタワー間で 5 分ごとに送信される Eメールの平均往復時間をいう。
メッセージラボ・トラッカー	サービス可用性および待ち時間を測定するツールをいう。
月額料金	本契約に詳細を記載する、影響を受けるサービスに対する月ごとの料金をいう。
サービスレベル	本サービスレベル契約書に定義される各サービスのパラメーターをいう。
スパム偽陰性	スパムと認識されないスパムメールをいう。
スパム偽陽性	誤ってスパムと識別され検知された、正当な E メールをいう。
スパム推奨設定	お客様のアンチスパムサービスの最良のコンフィグレーション実施ガイドラインをいう。
タワー	多数の負荷分散サーバをいう。

## 1. サービス全体にかかわる事項

### 1. 1 サービス概要

- 本サービスは、Eメールに関するさまざまな脅威（スパム、ウイルス、機密情報の漏えいなど）からお客様を守り、システム担当者の運用負担を軽減することを目的としたサービスです。
- 本サービスは、「アンチウイルス(AV)」「アンチスパム(AS)」「コンテンツ監視(CC)」「イメージ監視(IC)」の4サービスからなり、各機能はオンデマンド方式で提供するためお客様が好きなサービスを選択可能です。
- 本サービスは、英国メッセージラボ社のセンタを経由して、お客様メールのフィルタリングを行うことにより実現します。

### 1. 2 サービス導入条件

- 本サービスの導入条件は、お客様所有の対象 Eメールシステムを対象とします。
- 本サービスを導入するお客様および対象 Eメールシステムは下記を満たす必要があります。
  - 対象 Eメールシステムは固定 IP アドレスを有すること。
  - 対象 Eメールシステムの IP アドレス、ネットワーク構成、メールアドレス等の情報をお客様が常に把握・管理していること。
  - 対象 Eメールサーバがオープンリレーとして機能しないこと。
  - 対象 Eメールサーバがバルクメール（1回の操作または一連の関連操作により送信または受信される、実質的に同じ内容の 5,000 通以上の Eメール）を送受信しないこと。
  - スпамメールを送信しないこと。
  - 利用しているドメインの MX レコード設定を変更できること。
  - 対象 Eメールサーバは(ダイナミック IP ではなく)固定 IP を持っていること。
  - 対象 Eメールサーバに対し、25 番ポートを利用した、出張者やリモートユーザからの対象 Eメールサーバへの接続がないこと。
- 本サービスの利用に先立ち、トライアル(最大 30 日間)をご利用いただくことが必要です。
- トライアルの利用はお客様の責任で実施します。トライアル利用中のトラブル等について弊社は一切の責任を負いません。

### 1. 3 サービス導入時の同意事項

- 本サービスの導入(トライアル利用開始)の際は、弊社所定のフォーマットに必要事項を記載の上、申し込みいただくことが必要です。
- 本サービスの導入(トライアル利用開始)は、上記申込書を弊社に提出いただいた後、5営業日以内に開始することが可能です。ただし、申込書に記載不備があった場合、その限りではありません。
- 本サービスの導入(トライアル利用開始)に当たり、利用しているドメインのMXレコード設定の変更をお客様責任で実施いただく必要があります。(弊社から変更依頼を送付するまでMXレコード設定変更はしないで下さい)
- 利用しているドメインのMXレコード設定に誤りがあった場合、メールの送受信が正しくできなくなる可能性があります。
- 本サービスの導入(トライアル利用開始)に当たり、対象メールシステムにおける全ての有効メールアドレス(存在するメールアドレス)を本サービスの管理用ポータルサイトに登録していただく必要があります。
- 登録メールアドレスの情報に誤りがあった場合、メールの送受信が正しくできなくなる可能性があります。
- 本サービスを正しく利用するためには、ファイアウォール若しくは対象Eメールサーバ上でメッセージラボインフラ以外からのメール受信を制限できる必要があります。(最新のIPレンジについては下記をご参照下さい。上記IPレンジについては年に1~2回程度更新される可能性がございますので、その際はFW等の設定変更が必要となります)  
[http://imageserver.messagelabs.com/EmailResources/ImplementationGuides/Subnet\\_IP.pdf](http://imageserver.messagelabs.com/EmailResources/ImplementationGuides/Subnet_IP.pdf)
- 上記ファイアウォール等の設定作業は、お客様責任で実施いただきます。
- その他別途開催する本サービスのトレーニングを受講いただき、導入前にサービス内容をご理解いただく必要があります。
- 本サービスの最低契約期間は12ヶ月となります。
- ユーザー数は利用対象ドメインに存在する全てのメールアドレス数(メーリングリスト、エイリアス等も含みます)とします。
- ユーザー数のカウント方法は下記のとおりとします。
  - 契約当初月は、登録時のユーザー数に基づいてカウントします。
  - 契約次月以降は、前月利用実績に基づいてカウントします。
  - ユーザー数のカウントは25名単位とします(11名の場合は25名扱いとなります)。

#### 1. 4 サービス利用中の同意事項

- 対象 E メールサーバに E メールを配信できない場合、本サービスはお客様の受信メールを最大 7 日間保管した後配信します。
- 本サービスを利用されている対象 E メールサーバに対し、オープンリレー状態にないかどうかの定期的な確認をメッセージラボ社から行います。
- 対象メールシステムにおけるメールアドレスに追加・変更があった場合、都度メールアドレスをクライアントネットにて登録していただく必要があります。
- 登録メールアドレスの情報が誤りがあった場合、メールの送受信が正しくできなくなる可能性があります。
- お客様のドメインを対象とする、あるいはお客様のドメインから開始されるハッキング、サービス妨害攻撃、メール爆弾およびその他の悪意的行為により、お客様へのサービスの提供を継続することでサービスの安全が危殆化される場合には、お客様へのサービスが一時中断される場合があります。かかる場合には、お客様へ速やかに通知するものとし、可能な限り早期にお客様へのサービスを再開するものとしします。
- 弊社およびメッセージラボ社は、適用法に従い、サービスの一部である世界中のどのハードウェアからでもサービスを提供することができ、サービスを提供するハードウェアを、いかなる時点でも別のものに移転することができるものとしします。
- 弊社は、サービス遂行の義務を果たすため、サービスおよびその関連文書を、法律上、安全上、業務上、技術上などその理由の如何を問わず、いかなる時点でも変更することができます。
- SLA(サービスレベルアグリーメント) を締結させていただくものとしします。
- お客様の責任として下記の事項を実施いただくものとしします。
  - ・ インターネットの使用に適用されるすべての関連法に準拠すること。
  - ・ インターネット上で適宜公開され、インターネット利用者の過半数が採用するプロトコルおよび標準に従うこと。

#### 1. 5 サポート対応

- サポート問い合わせの受け付けは、サービス契約時に指定された窓口用メールアドレスへのメールのみとします。
- サポート問い合わせの受け付けは 24 時間行いますが、返答は弊社営業日の 9:00~17:00 となります。
- 当社は問い合わせへの返答が最短となるよう努めますが、問い合わせの内容および調査状況によっては返答までに必要となる時間が変動するため、特定の期日までの返答および解決については保証するものではありません。



#### 1. 6 予定メンテナンス

- 「予定メンテナンス」とは、弊社からお客様に7日前に通知され、タワーが利用できないことによりサービスの中断を生じる可能性のあるメンテナンス期間を意味します。予定メンテナンスは1ヶ月に合計8時間を越えないものとします。
- 予定メンテナンスは、可能な限りサービスに影響を与えないように実施するものとします。具体的には、通常は、トラフィックが少ないと予想される期間中に予定メンテナンスを実施し、また、一度にネットワークの全部ではなく一部で実施します。予定メンテナンス期間中は、サービスの中断を最小にするため、トラフィックがネットワークのメンテナンスを受けていないセクションに迂回する場合があります。
- 緊急メンテナンスが必要で、それがサービスに影響を与えると見込まれる場合には、弊社は影響を受ける当事者に通知するよう努めるものとし、可能な限り速やかにクライアントネットに非常メッセージを掲載するものとします。

#### 1. 7 クライアントネットおよびアナウンス

- インターネットベースの設定・管理・報告ツールであるクライアントネットは、サービスの不可欠な一部です。お客様は、パスワードで保護された安全なログインによりクライアントネットを利用することができ、かかるパスワードは第三者に開示してはいけません。クライアントネットはお客様に対し、お客様のサービス利用に関するデータおよび統計を閲覧する機能を提供し、多数の設定・管理機能を提供します。
- お客様によるクライアントネットのログイン ID、パスワードの管理の不備による影響に対しては、弊社は一切責任を負いません。
- 本サービスにかかわる各種アラートやアナウンス等はクライアントネット上に掲示するものとします。ただし、緊急を要するアナウンスについてはメールもしくは FAX にてご連絡する場合がございます。

#### 1. 8 適用法

- 本サービスの契約は日本法に準拠し、同法に従って解釈するものとします。
- 本サービスにかかわる秘密情報の取り扱いとは別途締結する契約書の第 11 条に準ずるものとします。

## **2. アンチウイルス (AV) サービス**

### **2. 1 処理対象**

有効メールアドレスから発信された、または有効メールアドレス宛に送信された全ての送受信 E メール。(添付ファイル、マクロ、実行ファイルを含む)

### **2. 2 処理方法**

独自技術および有名ベンダの各種アンチウイルス製品を組み合わせ、非常に高精度なウイルススキャンを行います。

### **2. 3 ウイルス検知時の対応**

#### **2. 3. 1 受信 E メールにおける通知**

当該 Eメールの送信者および宛先指定されたユーザが有効メールアドレスの Eメールに対し、警告を自動通知することができます。

#### **2. 3. 2 送信 E メールにおける通知**

当該 Eメールを送信したユーザに対し、警告を自動通知することができます。

#### **2. 3. 3 ウイルスに感染した Eメールの措置**

- 検知後、メール本文および添付ファイルを直ちに安全なサーバに隔離され、30 日後に自動的に削除します。
- 感染した Eメールが大量メール送信業者からの場合には、上記措置を取らず、直ちに削除します。

### **2. 4 ウイルスに感染した Eメールの確認**

- 対象 Eメールシステム管理者はクライアントネットを使用して、監視結果を確認することができます。
- 対象 Eメールシステム管理者はクライアントネットを使用して、隔離したメールを解放できる場合があります。

### **2. 5 諸注意**

- パスワード設定保護や暗号化された添付ファイルについては、ウイルススキャンを正しく行えない場合があります。
- ウイルスが添付されたメールに対し、隔離が行われます。添付ファイルを削除してのメール本文送付などは実施できません。
- 2. 4項に基づき、隔離したメールを顧客側で故意にリリースした結果、日立システムズに損失および費用が発生した場合、その損失および費用についてはお客様が補償するものとします。

### 3. アンチスパム (AS) サービス

#### 3. 1 処理対象

有効メールアドレス宛に送信された、全ての受信 E メール。

#### 3. 2 処理方法

- 公開データベースによる送信元チェックや、2000 件以上の人工知能ルールなど最新技術を駆使し、非常に高精度な能動的スパムスキャンを行います。

[ルールの例]

HTML Obfuscation (リンク先の偽装)、Hash Busters (バルクメール対策破り)、Known Ratware (既知のラットウェア)、Header Forgeries (ヘッダの偽装)、Header Inconsistencies (ヘッダの不整合)、RFC Violations (RFC 非準拠) など

- ユーザは、個人的な承認送信者リストを設定・使用することができます。この場合、当該送信者 (ドメイン) から送信された E メールはアンチスパムの処理対象外となります。ただし、明らかにスパムメールであると技術的に判断される場合はアンチスパムの処理対象となります。
- ユーザは、個人的なブロック送信者リストを設定・使用することができます。この場合、当該送信者 (ドメイン) から送信された E メールは 3. 3 項に記すアンチスパムの処理対象となります。
- 一般的なブロック送信者リストを複数使用することができる。この場合、当該送信者 (ドメイン) から送信された E メールは 3. 3 項に記すアンチスパムの処理対象となります。

#### 3. 3 スパム検知時の処理

検知された疑わしい E メールに対し、以下の何れかの処理を行うことができます。

何れの処理を行うかは、対象 E メールシステム管理者がクライアントネットにて設定できます。

- ① 当該 Eメールのヘッダにタグを付ける。
- ② 当該 Eメールの件名にタグを付ける。
- ③ 当該 Eメールの送信元を予め定めた Eメールアドレス (スキャン対象アドレスであること) に変更する。
- ④ 当該 Eメールを削除する。
- ⑤ 当該 Eメールをスパム隔離する。

#### 3. 4 スパム隔離に関する説明

あるドメインの処理に対し 3. 3 の⑤を選択した場合、以下の処理を行うことができ

す。

- ① 各ユーザが管理マネージャを使うためのアカウントが自動的に設定されます。(疑わしい E メールを隔離した初回のみ)
- ② 疑わしい E メールを隔離すると、当該ユーザに自動通知を行います。通知頻度は、対象 E メールシステム管理者がクライアントネットにて設定することができます。
- ③ 当該ユーザは、管理マネージャを介して隔離された Eメールの件名を確認できます。
- ④ 管理マネージャにより、隔離された E メールに対し、削除、解放、テキストのレビューを行うことができます。
- ⑤ 隔離されたメールは最大 14 日間保管することができ、その後自動的に削除されます。

### 3. 5 確認

対象 E メールシステム管理者はクライアントネットを使用して、監視結果を確認することができます。

### 3. 6 諸注意

- 本サービスは、スパムメールの 100%の検知率を保証することはできません。また、お客様（対象 E メールシステム管理者）の責任において、ルール・処理を設定いただきます。お客様が行う各種設定により、疑わしい E メールを検知できなかった、または疑わしいと検知し処理したことによって生じる一切の責任を当社は負いません。
- 本サービスは、スパムメールに対する 0%の誤検知率を保証することはできません。また、送信者がスパムメールを送信していることを意識していない場合でも、各種理由により技術的にスパムメールと判断される場合があります（例：送信サーバが知らずにスパムを送っている場合。SMTP の正しいプロトコルが利用されていない場合。）。

## 4. コンテンツ監視 (CC) サービス

### 4. 1 処理対象

有効メールアドレスから発信された、または有効メールアドレス宛に送信された全ての送受信 E メール。(添付ファイルを含む)

### 4. 2 処理方法

- 対象 E メールシステム管理者が設定するルールに応じた監視 (フィルタリング) を行います。
- ルールの設定は、管理者用画面から行うことができます。
- ルールの適用は、ドメイン、グループ、個人の何れかの単位で行うことができます。

### 4. 3 監視対象 E メール検知時の処理

予め設定したルールにより検知された疑わしい E メールに対し、以下の何れかの処理を行うことができます。

何れの処理を行うかは、対象 E メールシステム管理者がクライアントネットにて、送信・受信の場合ごとに設定できます。

- ① 当該 E メールをブロックし、削除する。
- ② 当該 E メールにタグを付け、送信先を指定管理者に変更する。(受信の場合)
- ③ 当該 E メールにタグを付け、指定管理者にコピーを送信する。(受信の場合)
- ④ 当該 Eメールのヘッダにタグを付ける。(受信の場合)
- ⑤ Eメールの添付ファイルを圧縮する。
- ⑥ クライアントネットの統計に記録するのみ。
- ⑦ 件名にタグを付ける。

### 4. 4 確認

対象 E メールシステム管理者はクライアントネットを使用して、監視結果を確認することができます。

### 4. 5 諸注意

- アンチスパム (AS) と同時に契約し、アンチスパムの処理において「隔離」を選択している場合、本サービスの監視以前にメールが隔離される場合があります。
- Microsoft Word、Excel、PowerPoint 以外の文書中に埋め込まれたコンテンツは、監視対象外とします。
- 一部の監視ルール (文字列のマッチング等) は英語でのみ指定可能となるため、英語以外の言語で記述された文書については一部の監視ルールが適応不可となります。

SHIELDDeXpress セキュリティオンデマンド  
メールセキュリティ on-Demand サービス仕様書兼 SLA

---

- 本サービスは、お客様（対象 E メールシステム管理者）の責任において、ルール・処理を設定いただきます。お客様が行う各種設定により、疑わしい E メールを検知できなかった、または疑わしいと検知し処理したことによって生じる一切の責任を当社は負いません。
- 予め用意されているルールのテンプレート中に不快とみなされる言葉を含む可能性があります、かかる単語リストによって発生した一切の責任を当社は負いません。

## 5. イメージ監視 (IC) サービス

### 5. 1 処理対象

有効メールアドレス宛に送信された送受信 E メールに添付された全ての画像ファイル。

### 5. 2 処理方法

- 独自の解析技術により、画像が業務上不適切なものでないかスキャンを行います。
- 上記解析技術のスキャン対象はポルノ画像のみとなります。その他の残虐系などの画像は対象となりません。
- スキャンレベルは、対象 E メールシステム管理者がクライアントネットにて、3 段階から選択することができます。
- 予め登録された例外的 E メールアドレス（信頼する E メール送信者および受信者）のメールについては、スキャンの対象外とします。

### 5. 3 不適切な画像検知時の処理

検知された疑わしい画像が添付された E メールに対し、以下の何れかの処理を行うことができます。

何れの処理を行うかは、対象 E メールシステム管理者がクライアントネットにて、送信・受信の場合ごとに設定できます。

- ① 当該 E メールを記録する。(クライアントネットの統計に反映)
- ② 当該 Eメールのヘッダにタグを付ける。(受信の場合)
- ③ 当該 E メールを予め定めた E メールアドレスにコピー送信する。
- ④ 当該 Eメールの送信先を予め定めた E メールアドレスに変更し送信する。
- ⑤ 当該 Eメールを削除する。
- ⑥ 当該 Eメールの件名にタグを付ける。
- ⑦ 上記処理により宛先変更または削除した場合、送信者に対し自動警告メールを送信することができます。また、受信メールの場合、受信予定者に対しても自動警告メールを送信することができます。

### 5. 4 確認

対象 E メールシステム管理者はクライアントネットを使用して、監視結果を確認することができます。

### 5. 5 諸注意

- パスワード設定保護や暗号化された添付ファイルについては、ウイルススキャンを正しく行えない場合があります。

SHIELDDeXpress セキュリティオンデマンド  
メールセキュリティ on-Demand サービス仕様書兼 SLA

---

- Microsoft Word、Excel、PowerPoint 以外の文書中に埋め込まれた画像は、監視対象外とします。
- 本サービスは、お客様（対象 E メールシステム管理者）の責任において、例外的 E メールアドレス・スキャンレベル・処理を設定いただきます。お客様が行う各種設定により、疑わしい E メールを検知できなかった、または疑わしいと検知し処理したことによって生じる一切の責任を当社は負いません。



## **6. SLA**

### **6. 1 定義**

- 本 SLA 条項において、以下の用語は以下の意味を持つものとする。「甲」とは、本サービスを提供する、東京都品川区大崎 1 丁目 2 番 1 号に登記上の事務所を有する会社である株式会社日立システムズをいう。「乙」とは、本サービスの契約者をいう。

### **6. 2 一般規定**

- 6. 2. 1 乙は、本規定により救済を受ける権利を有すると考える場合は、当該適格性が発生した月の末日より 20 日以内に甲にクレジットリクエストを提出するものとする。クレジットへの適格性は、本書中に詳細を記載する、甲の内部ログ記録その他適切な書類に基づく検証により決定される。クレジットへの適格性が甲により確認された場合は、甲は本規定により乙にクレジットを与える。乙は、ログ記録が保管される日数が限定されており、よって規定の時間枠を超えて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認識する。クレジットは発生次月の月額料金減額、もしくは返金によって行われる。
- 6. 2. 2 次の場合には、本サービスレベル契約は効力を生じないものとする。
  - (a) 予定メンテナンスまたは緊急メンテナンスの期間中
  - (b) 不可抗力または乙、第三者のいずれかの作為、不作為により利用不可能な期間中
  - (c) 本契約に従いサービスを停止する期間中
- 6. 2. 3 本サービスレベル契約に規定する救済は、契約、不法行為（過失を含むがこれに限らない）、その他に基づく乙のサービスのレベルに関する唯一かつ排他的な救済である。
- 6. 2. 4 クレジットはすべて、サービスのレベル劣化の影響を受けたユーザ数により比例配分される。
- 6. 2. 5 各顧客についての乙に対する甲の責任の各暦月における最高累計額は、いかなる場合も、影響を受けたサービスに関わる顧客への月額料金の 100%を超えないものとする。

### 6. 3 100%サービス可用性

- 6. 3. 1 本条のサービス可用性サービスレベルは、乙が一つまたは複数のEメールサービスを利用する場合に限り有効とする。
- 6. 3. 2 Eメールサービスに関しては、本サービス可用性サービスレベルは、指定タワークラスタが以下を行うことができる場合にのみ適用される。

(a) 乙の着信Eメールを乙のドメインに代わり 1 日 24 時間週 7 日体制で受信すること

(b) 正しく設定された乙所有のSMTPホストよりの乙の発信Eメールを乙のドメインに代わり 1 日 24 時間週 7 日体制で受け入れること

- 6. 3. 3 1 暦月中のサービス可用性が 100%を下回る場合は、乙は以下の割合のクレジットを受ける権利を有す。

各暦月のサービス可用性割合	月額料金のクレジット比率
99%以上 100%未満	25%
98.0%以上 99%未満	50%
98.0%未満	100%および影響を受けたサービスの解除

- 6. 3. 4 1 暦月のサービス可用性が 98%未満となった場合は、乙は影響を受けたサービスを直ちに解除し、支払済料金の解除後の期間について案分した額の返金を受ける権利を有するものとする。

#### 6. 4 100% Eメール配信

- 6. 4. 1 本条のEメール送信サービスレベルは、乙が一つまたは複数のEメールサービスを利用する場合に限り有効とする。
- 6. 4. 2 甲は以下を条件に、顧客が送信、受信するEメールを100%配信する。
  - (a) Eメールは顧客の指定タワークラスタにより受信されていなければならない。
  - (b) Eメールにウイルスが含まれていたり、アンチスパムサービスでブロックされていてはならない。
- 6. 4. 3 上記6. 4. 1項および6. 4. 2項を条件に、甲が乙よりまたは乙へのEメールを配信できず、乙が本契約の条件に違反していない場合は、乙は、30日前までに事前の書面による通知を行うことにより、影響を受けた顧客へのEメールサービスを解除する権利を有するものとする。

#### 6. 5 Eメール待ち時間-60秒

- 6. 5. 1 本条のEメール待ち時間サービスレベルは、顧客が一つまたは複数のEメールサービスを利用する場合に限り有効とする。
- 6. 5. 2 1暦月における顧客の指定タワークラスタの平均往復時間が、以下の表に定める遅延を超える場合は、乙は以下の表に従いクレジットリクエストを提出することができる。

測定したEメール100%の平均往復時間(単位:分・秒)	月額料金のクレジット比率
1分を超え、1分30秒以下	25%
1分30秒を超え、2分以下	50%
2分を超え、2分30秒以下	75%
2分30秒を超える場合	100%

- 6. 5. 3 本条のEメール待ち時間サービスレベルは以下の期間には効力を生じない。
  - (a) ウイルス対Eメール比率が1:50を超えるウイルス発生期間中
  - (b) 乙がサービス妨害攻撃の被害を受けている期間
  - (c) 乙のシステムを往復するメールループにより遅延が生じている期間

## 6. 6 スпам-偽陽性 0.0003%

- 6. 6. 1 本条のスパム偽陽性サービスレベルは、乙がEメールアンチスパムサービスを利用し甲のスパム推奨設定を行う場合に限り有効とする。
- 6. 6. 2 平均スパム偽陽性検知率が乙の1暦月中の全Eメールトラフィックの0.0003%を超える場合は、乙は以下の表に従ってクレジットを受ける権利を有す。

1 暦月間のスパム偽陽性検知率	月額料金のクレジット比率
0.0003%を超え、0.003%以下	25%
0.003%を超え、0.03%以下	50%
0.03%を超え、0.3%以下	75%
0.3%を超える場合	100%

- 6. 6. 3 本サービスレベルにおいては、次のEメールはスパム偽陽性Eメールとはみなされない。
  - (a) 正当な営業用EメールでないEメール。
  - (b) 受信者が20名以上のEメール。
  - (c) Eメールの送信者が乙のブロック送信者リストに掲載されている場合。  
これには、乙がユーザレベルの設定を許可する場合に個人ユーザが定義するブロック送信者を含むが、これに限らない。
  - (d) 障害が生じたマシンから送信されるEメール。
  - (e) 第三者のブロックリストに掲載されているマシンから送信されるEメール。
  - (f) (一回または一連の操作で) 20名以上の受信者に送信され、内容の80%以上が同じものであるEメール。

#### 6. 7 95%スパム検知率

- 6. 7. 1 本条のスパム検知サービスレベルは、乙がEメールアンチスパムサービスを利用し、スパム推奨設定を行う場合に限り有効とする。本6. 7条の規定は一月月に測定された偽陰性スパム数に相当する。
- 6. 7. 2 乙は、以下の表に従ってクレジットを受ける権利を有す。

1 暦月間のスパム検知率	月額料金のクレジット比率
94%を超え、95%以下	25%
93%を超え、94%以下	50%
92%を超え、93%以下	75%
92%以下	100%

- 6. 7. 3 本条のスパム検知サービスレベルは、Eメールが正当なアドレスに送信されなかった場合には効力を生じないものとする。

#### 6. 8 スпамサービスクレジットの要請

- 6. 8. 1 6. 6項および6. 7項に基づきクレジットを受ける権利を取得するには、偽陰性または偽陽性Eメールと疑われるEメールを、当該Eメール受領後5日以内に shield-ondemand@hitachijoho.com 宛に送付しなければならない。甲は、当該Eメールがスパム偽陰性または偽陽性か否かを調査、確認し、その結果を記録する。乙が受信したスパム偽陽性または偽陰性で確認されたものの数に基づき当該顧客が上記の表に従いクレジットを受ける権利を有すると考える場合は、乙は、本明細の6. 2. 1項に従って、甲にクレジットリクエストを送付するものとする。

## 6. 9 Eメールウイルス保護—100%

- 6. 9. 1 本条のEメールウイルス保護サービスレベルは、乙が一つまたは複数のEメールアンチウイルスサービスを利用する場合に限り有効とする。
- 6. 9. 2 乙のシステムが、1 暦月中に一つ以上のウイルスに感染し、ウイルスがサービスを経由して乙に到達したことが、記録および検証されたサポートコールにより甲に通知された場合、乙は、その時点で存在する月額料金の 100%相当の予定賠償額、または、200,000 円のいずれか低い額を甲に請求することができる。本項に規定する救済は、サービスを経由して乙または第三者に到達したウイルスによる感染に関する、契約、不法行為（過失を含むがこれに限らない）、その他に基づく唯一および排他的救済である。疑義を避けるため言及すると、本項に規定する救済は、故意による自己感染には適用されない。
- 6. 9. 3 EメールAVサービス経由で受信したEメールに含まれるウイルスが、乙のシステム内で自動的または手動の介入により活動を始めた場合に、乙のシステムは感染したものとみなされる。
- 6. 9. 4 甲が、ウイルスに感染したEメールを検出しながらこれを阻止しない場合は、甲は速やかに乙に通知し、ウイルスに感染したEメールを識別し、削除することができるよう十分な情報を提供するものとする。かかる通知の結果感染が阻止された場合は、上記6. 9. 2項に規定する救済は適用されない。乙に係る情報に基づいて速やかに行動しない場合は、上記6. 9. 2項に記載されるサービスレベルは無効となる。
- 6. 9. 5 サービスでは、可能な限り多くのEメールおよびその添付ファイルをスキャンするものとする。送信者が直接その内容を支配する添付ファイル（例えば、パスワードで保護された添付ファイルおよび/または暗号化された添付ファイルなど）は、スキャンすることができない場合がある。かかるEメールおよび/または添付ファイルは、上記6. 9. 2項のサービスレベルから除外される。
- 6. 9. 6 本条のEメールウイルス保護サービスレベルは、乙が意図的にリリースしたウイルスに関しては効力を生じない。

6. 10 Eメールウイルス偽陽性 0.0001%

- 6. 10. 1 本条のEメールウイルス偽陽性サービスレベルは、乙が一つまたは複数のEメールアンチウイルスサービスを利用する場合に限り有効とする。
- 6. 10. 2 Eメールウイルス偽陽性検知率が乙の1暦月中の全Eメールトラフィックの0.0001%を超える場合は、乙は以下の表に従ってクレジットを受ける権利を有す。

1 暦月間のEメールウイルス偽陽性検知率	月額料金のクレジット比率
0.0001%を超え、0.001%以下	25%
0.001%を超え、0.01%以下	50%
0.01%を超え、0.1%以下	75%
0.1%を超える場合	100%