Orchestrating a brighter world NEC

ActSecure クラウドメールセキュリティサービスご紹介資料

日本電気株式会社

目次

1. メールシステムを取り巻く課題

多発する標的型攻撃

標的型攻撃の８～９割は、メールがきっかけ！

後を絶たない情報漏えい

うっかりミス！内部不正！

標的型攻撃や情報漏えいの脅威が増加する中、

標的型攻撃を防ぎたいけど対策製品は高くて買えない！

標的型攻撃だけでなく情報漏えいも合わせて対策したい！

セキュリティ対策を継続的に運用する人材がいない！

2. サービス概要

◆ クラウドメールセキュリティサービスは、スパム／ウィルスチェックをはじめ、標的型攻撃対策から情報漏えい対策まで包括的なサービスをご提供します。

◆ スパム／ウィルスチェック
- 多様な技術でスパム、ウィルスを検知・防御

◆ 標的型攻撃対策
- サンドボックスにより未知のマルウェアを検知・防御

◆ 情報漏えい対策
- メール誤送信対策（一時保留、ZIP暗号化、メール暗号化、宛先BCC化）
- 添付ファイルの自動暗号化

メールシステムのセキュリティ対策を
サービス型でご提供いたします！

3. ここがポイント！

1. 標的型攻撃などの危険なメールを検知し、防御力を向上

- サンドボックスによる挙動解析で、標的型攻撃を検出し、標的型攻撃と判断される添付ファイル付きメールを削除し、利用者には削除の通知を本サービスから行います。
- メール本文中に記載されたURLリンクを検査する機能を有し、メール配信後に危険なWebサイトに変わるケースなど、配信時点には判定できない脅威についても対処可能です。
- お客様で受けた攻撃メールの状況は月次レポートにて確認できます。

2. 送受信メールのオールインワンセキュリティ対策を低価格でご提供

- ウイルス・スパム対策、標的型メール対策などの受信メール対策に加えて、メール誤送信対策などの送信メールのセキュリティ対策も行えます。

3. 簡単導入・運用

- お客様で設備を用意する必要はなく、お申込みから短期間（最短７営業日）で導入可能です。
  お客様環境は、メール配送経路を変更するだけでご利用可能です。

4. クラウド型メールサービス連携

- オンプレミスのメールシステムでのご利用はもちろん、クラウド型メールサービス（Microsoft 365, Gsuite等）環境でもご利用可能です。

3. ここがポイント！ / NECの強み

1. 高精度のスパム検知

- スパム対策は日本語スパムにも精度の高い検知を実現しており、メール利用者のメール管理の負担やフィッシングサイトへの誘導のリスクを軽減します。

2. 導入・運用容易なメール暗号化

- 添付ファイルに加えてメール本文の暗号化にも対応しており機密情報を安全かつ簡単に送付できます。
- 従来のメール暗号化で必要な証明書の運用や、別途クラウドストレージの契約や権限設定・ユーザ管理などの運用は必要ありません。

3. 手厚い運用サポート

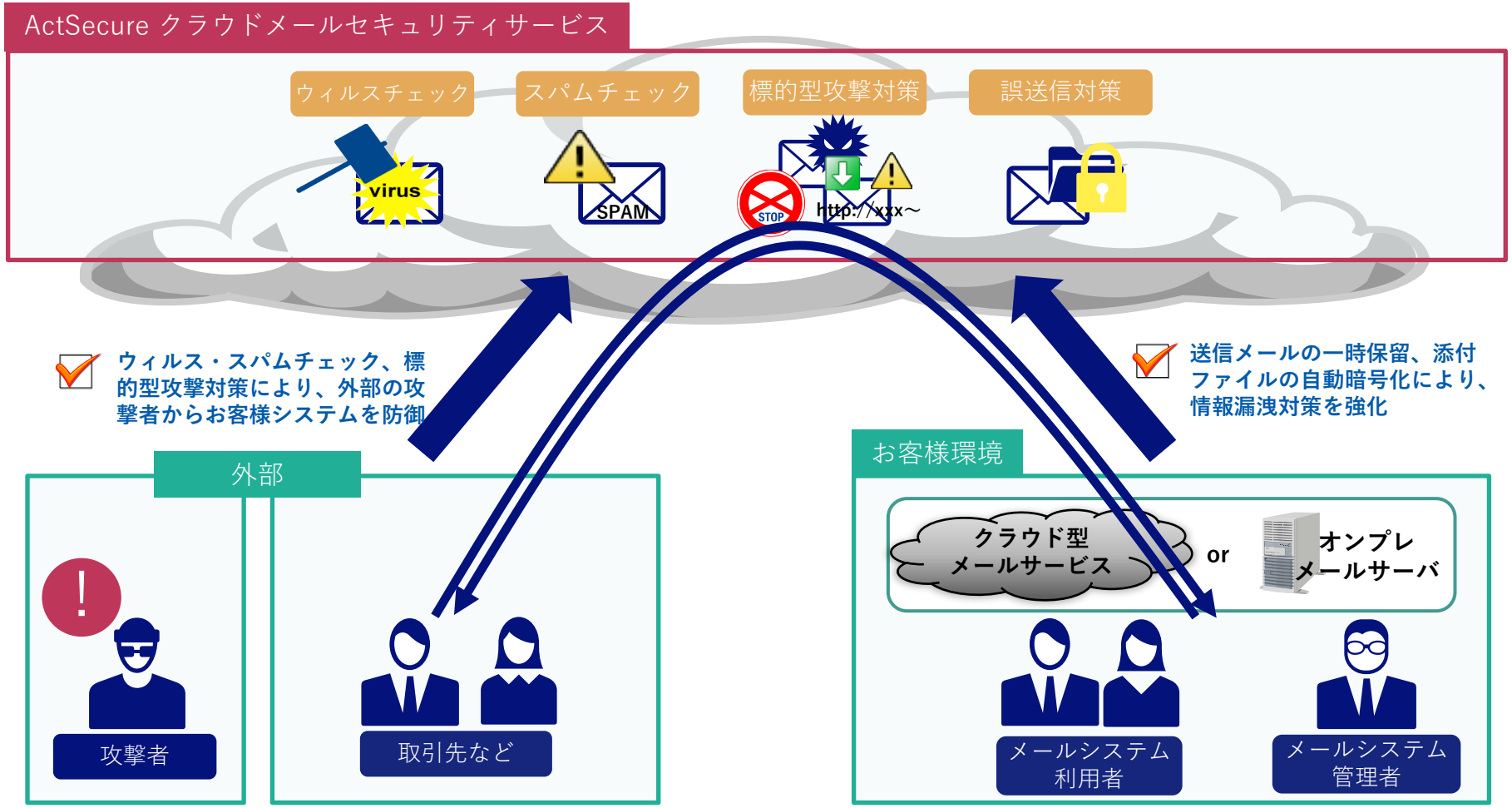
- 検査結果の確認や設定変更作業などの運用サポートが備わっており、メールシステム管理者の負担を抑えて運用できます。

4. 多数の導入実績

- 計100社以上の導入実績、計10万ID以上の導入実績があります。

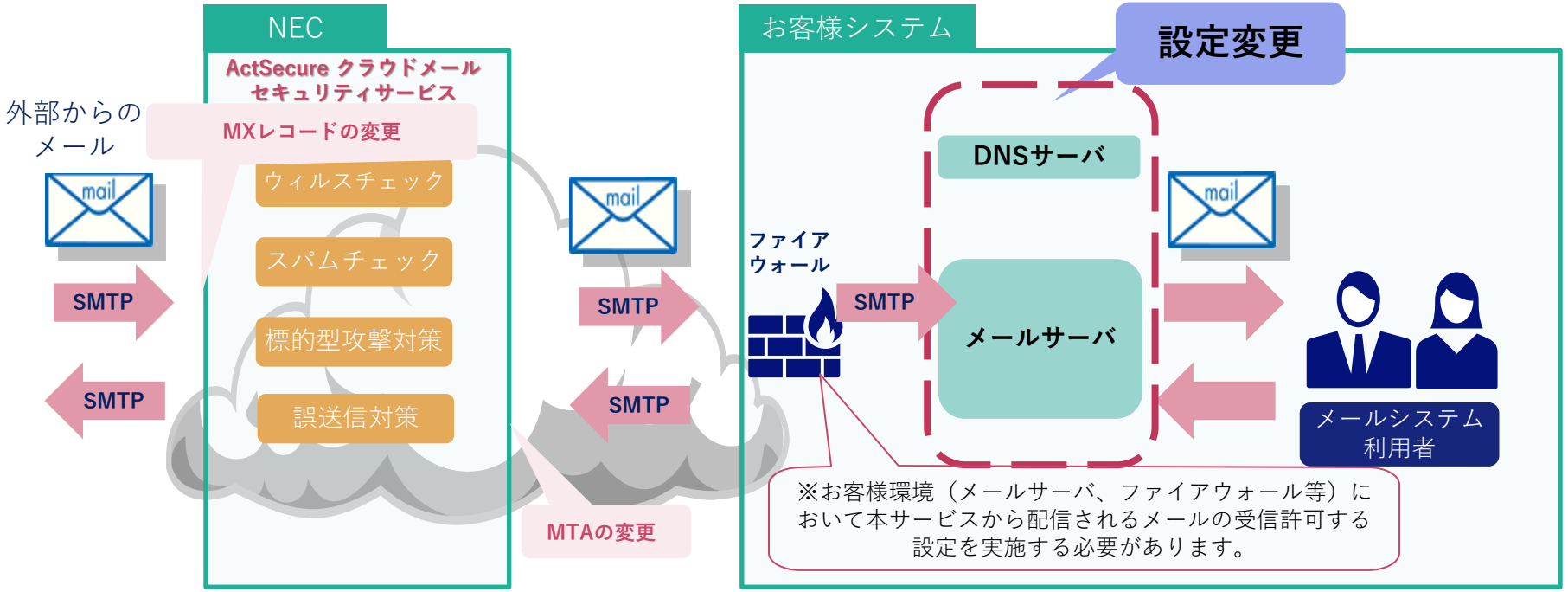
4. サービスご利用イメージ

- メール経路上にActSecure クラウドメールセキュリティサービスを入れていただくことでセキュリティ対策がご利用できます。



4.1. メール配送イメージ（オンプレメールサーバ）

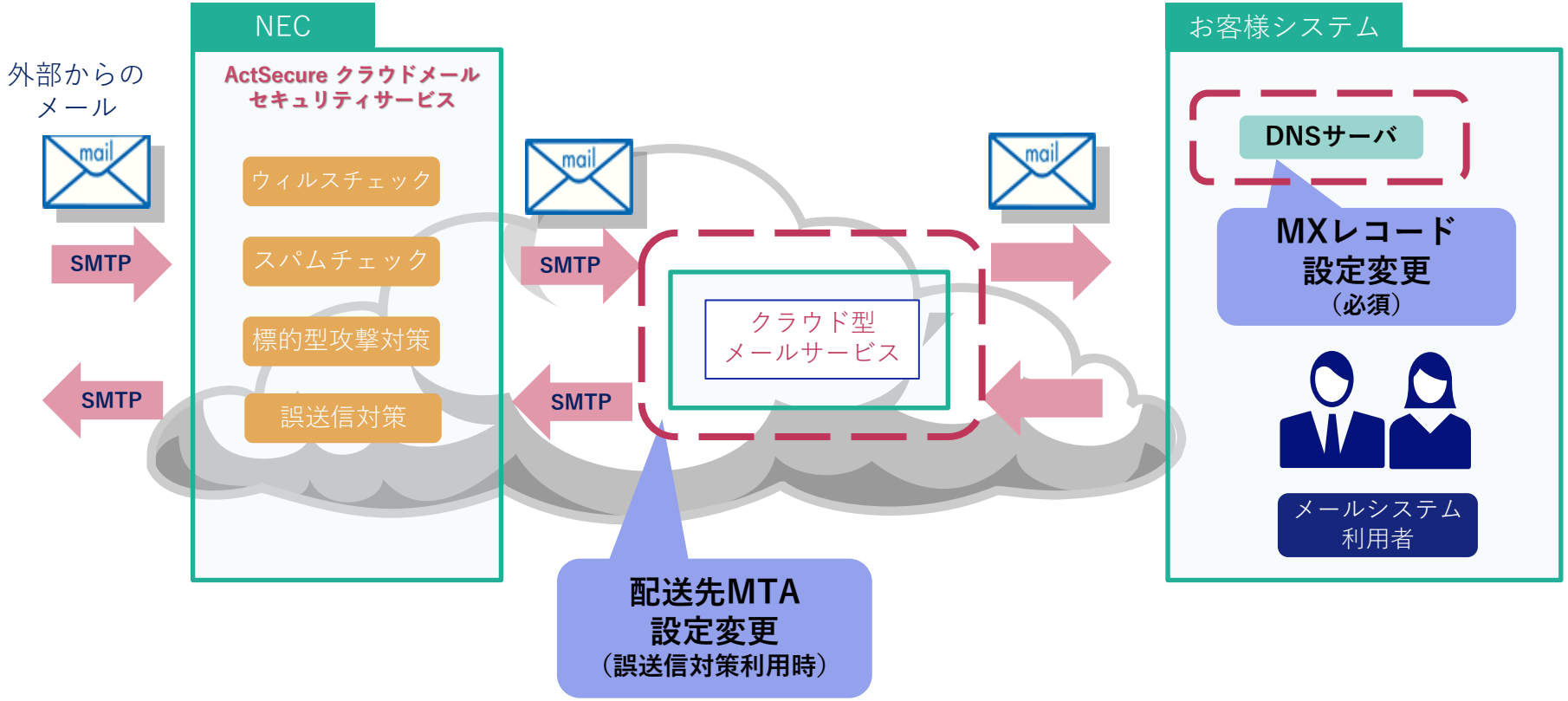
- お客様側のDNSのMXレコードを変更することにより受信メールを本サービス宛とすることでサービスが適用されます。
  送信時（誤送信対策を利用する場合）はメールサーバの配送先MTAの変更で本サービスに向けることで、本サービスで誤送信対策を適用後メール送信を行います。



※お客様システムで外部から受信するすべてのメールの送信元IPアドレスは、本サービスのIPアドレスとなります。
※お客様側のDNSサーバ、メールサーバ、ファイアウォール、NW等の設定変更作業は、お客様にて実施をお願いします。

4.2. メール配送イメージ（クラウド型メールサービス）

- お客様側のDNSサーバの設定変更（MXレコードの移行）と、クラウド型メールサービスからメールコネクタの配送先MTAの設定を変更（誤送信対策を利用する場合のみ）することで、本サービスをご利用頂けます。



※お客様システムで外部から受信するすべてのメールの送信元IPアドレスは、本サービスのIPアドレスとなります。
※ DNSサーバ及び、クラウド型メールサービスの設定変更作業は、お客様にて実施頂きます。

5. サービスメニュー

- NECクラウドのサービス環境をシェア型でご提供する形態で、100IDからご利用いただけるサービスです。
- 必要に応じてサービス組み合わせてご利用頂ける構成となっております。

サービスの組み合わせ

- ①アンチスパム／ウィルス
- ②アンチスパム／ウィルス ＋ 標的型攻撃メール対策
- ③アンチスパム／ウィルス ＋ 誤送信防止（添付ファイルZIP暗号化）
- ④アンチスパム／ウィルス ＋ 標的型攻撃メール対策 ＋ 誤送信防止（添付ファイルZIP暗号化）
- ⑤アンチスパム／ウィルス ＋ 誤送信防止（メール+添付ファイル暗号化）
- ⑥アンチスパム／ウィルス ＋ 標的型攻撃メール対策 ＋ 誤送信防止（メール+添付ファイル暗号化）

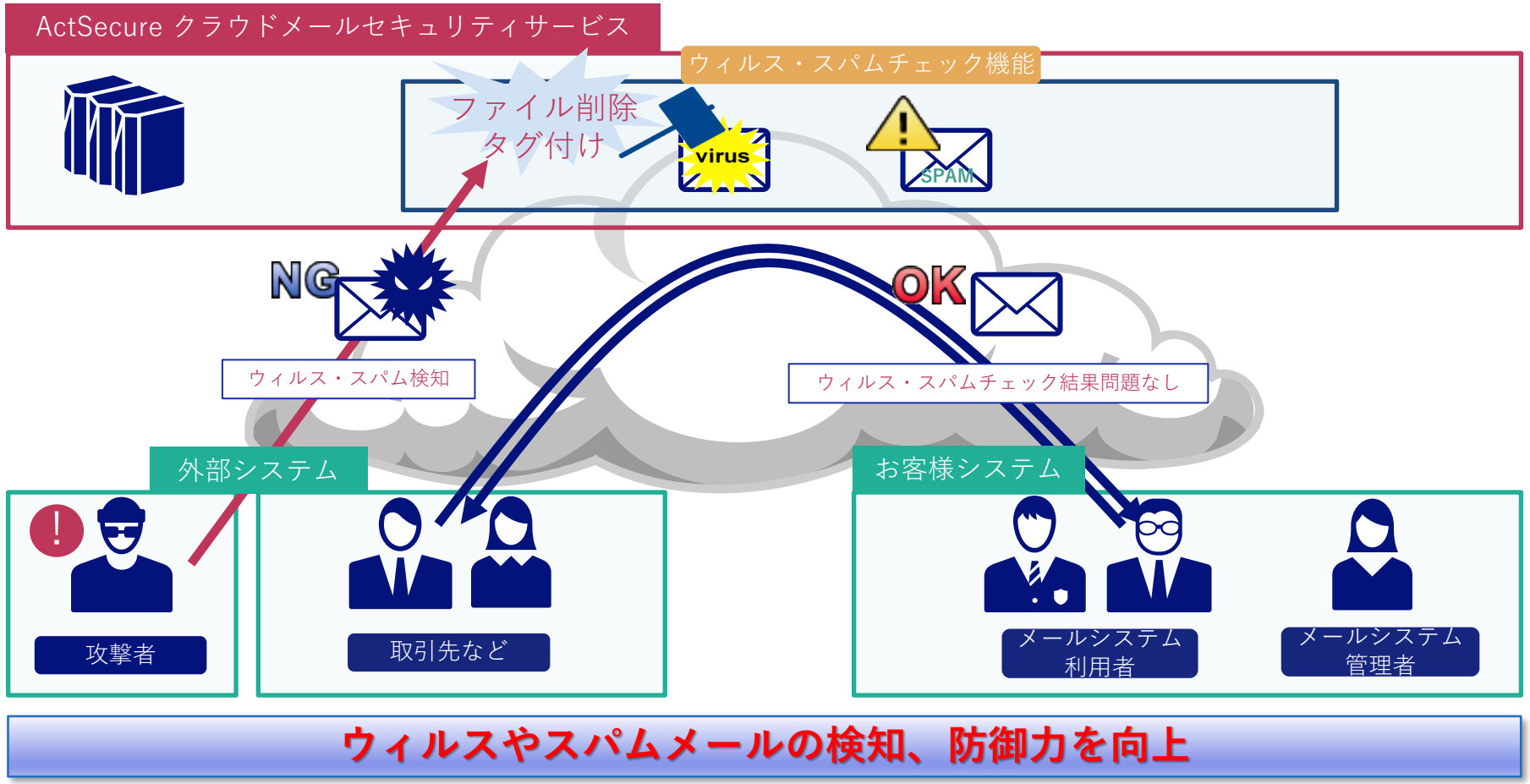
アンチスパム／ウィルス	• メールのウィルス・スパムチェック機能を提供します。 ※送信メールのチェックは、誤送信防止サービスをご契約時に機能提供が可能です。
標的型攻撃メール対策	• サンドボックスにより未知のマルウェアを検知し、標的型攻撃メールを削除します。 • メール受信時には脅威が判断できないURLリンクについては継続的に監視し、危険が確認された場合には当該Webサイトに対するアクセスを遮断します。
誤送信防止（添付ファイルZIP暗号化）	• 「添付ファイルのZIP暗号化」、「送信メール一時保留」、「送信メール宛先強制Bcc化」の機能を提供します。
誤送信防止（メール+添付ファイル暗号化）	• PPAP対策を含む新たな誤送信防止サービスとして、「メール+添付ファイル暗号化」、「送信メール一時保留」、「送信メール強制BCC化」の機能を提供します。

※誤送信防止（添付ファイルZIP暗号化）と誤送信防止（メール＋添付ファイル暗号化）は併用できません

5.1. ウィルス・スパムチェック

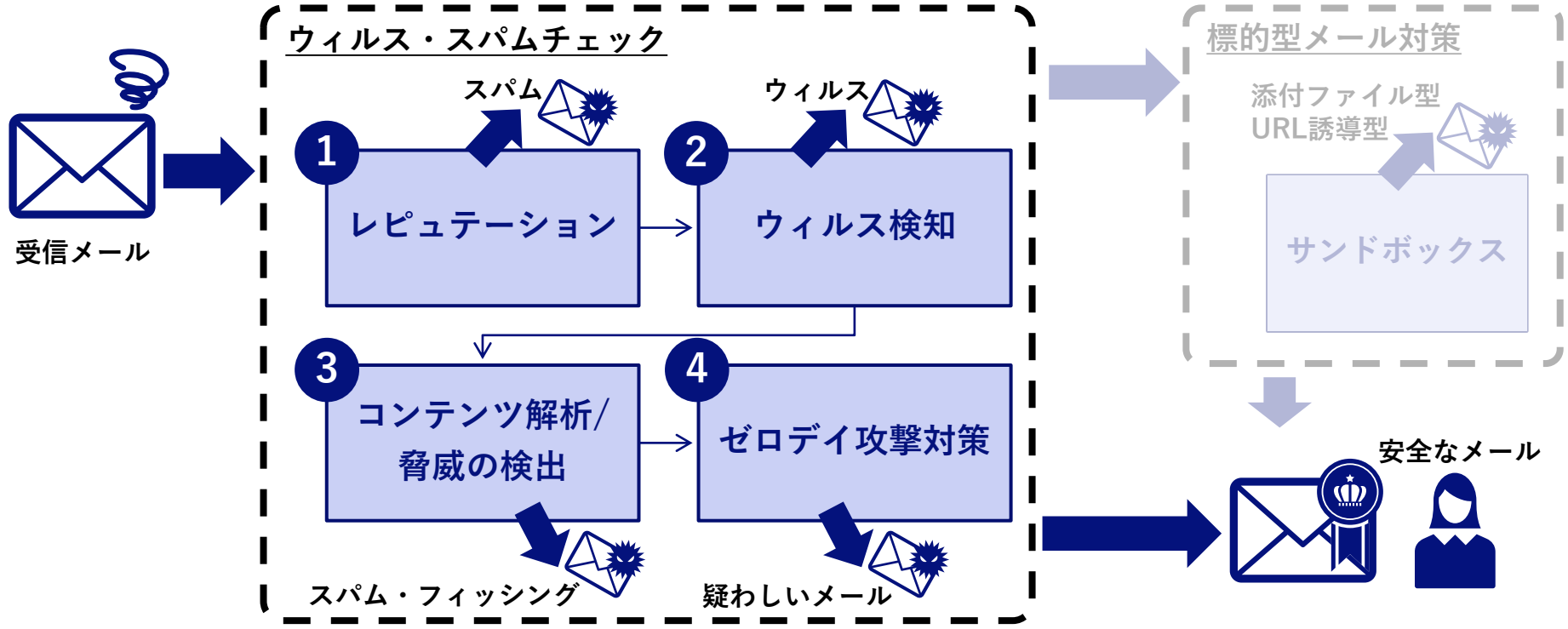
多様な検知技術で外部から受信するスパム・ウィルスの脅威を防御

- 送受信メールのウィルス・スパムチェックが可能です。
- ウィルス感染による情報漏えいや、大量のスパムによる業務効率低下を防ぎます



5.1. ウィルス・スパムチェック / 検知イメージ

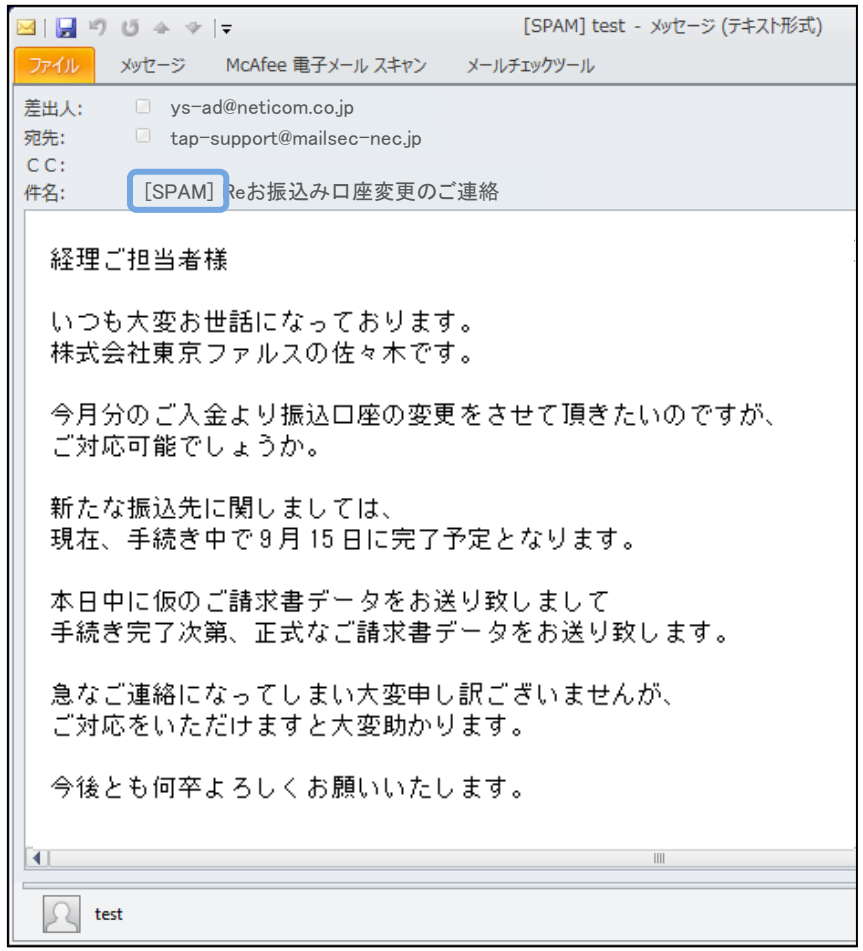
◆ 多様な技術でスパム・ウィルス・フィッシングメールを検知



レピュテーション	ウィルス検知	コンテンツ解析/脅威分類	ゼロディ攻撃検出
メールのIPアドレスやドメインの分析を行い、悪意のあるIPアドレスからのコネクションを拒否し、ウィルス・スパムメールを排除。	受信したメールのスキャンを行い、ウィルスやワームを検知・排除。	自動機械学習技術で、メールの各構成部分から、相関関係を解析し、フィッシング、スパム、なりすまし、悪意隠蔽・偽装、などの疑いのあるメールを検知。	スパム、フィッシング、難読化されたウィルスなど悪意の疑いありと判断したメールは、その旨のメッセージをメール本文に挿入し配送。

5.2. ウィルス・スパム判定時の受信メール

《タグ付けメール（スパム判定）》



《添付ファイル削除メール（ウィルス判定）》

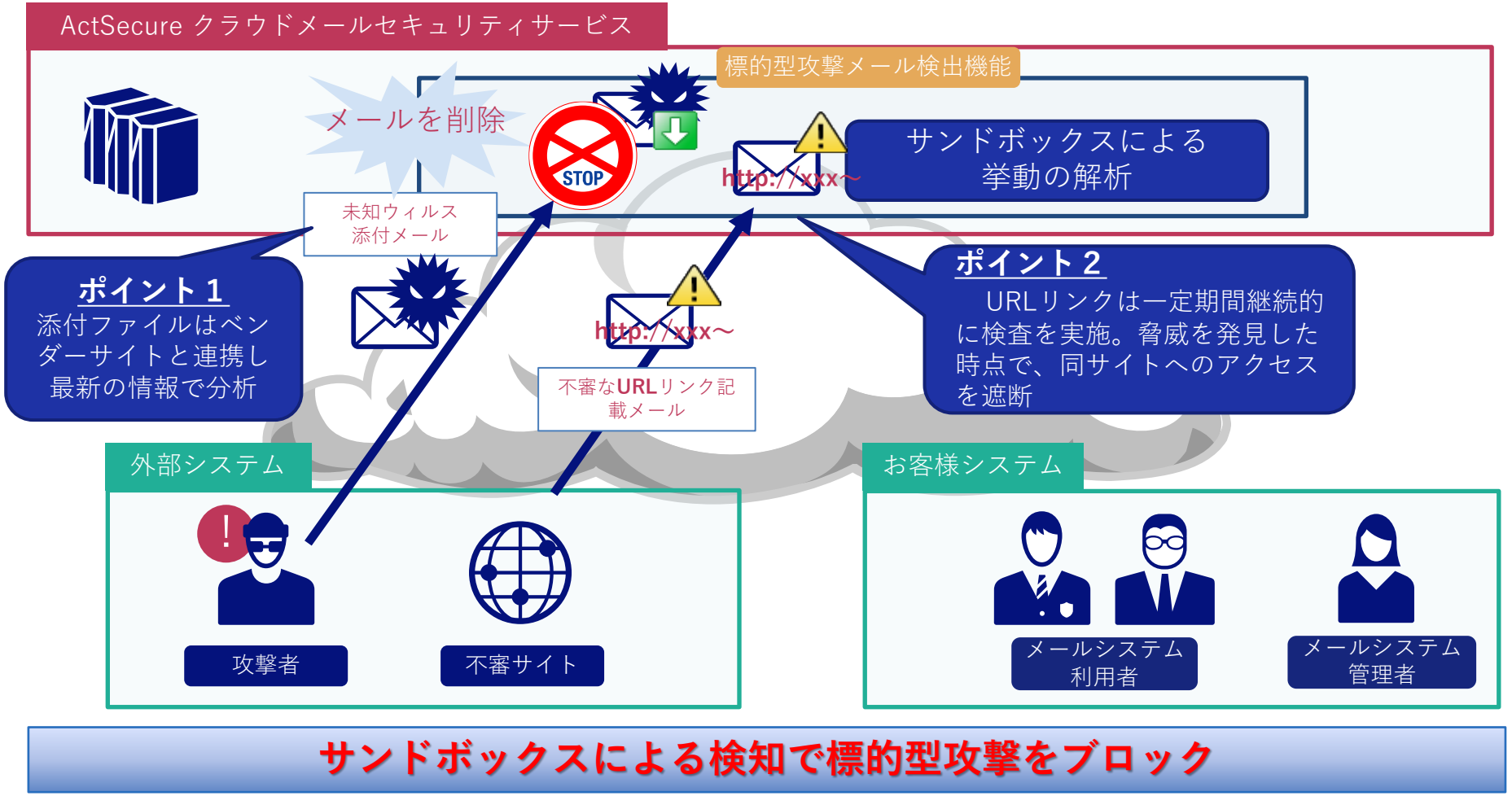
件名に [SPAM] タグを挿入し、受信者に注意喚起

**ウィルスが検出された添付ファイルを削除した
メッセージを本文先頭部に挿入**

5.2. 標的型攻撃メール対策

未知のマルウェアをサンドボックスで検知

◆ サンドボックスによる挙動解析で、標的型攻撃メールを検出し、情報漏えいリスクを低減します。



5.2. 標的型攻撃メール対策 / 機能の特長

クラウドメールセキュリティサービスの標的型対策

標的型攻撃メールに特化した、新しいセキュリティ対策
次世代の検知技術で標的型攻撃を検知・防御します。

【主な機能】

- ✓ 定義ファイルに頼らない方式で、悪意あるメールを検知
- ✓ クラウドベースのサンドボックスでＵＲＬ、及び、添付ファイルを分析
- ✓ メール配信後に仕掛けられる脅威に対応する次世代の検知技術

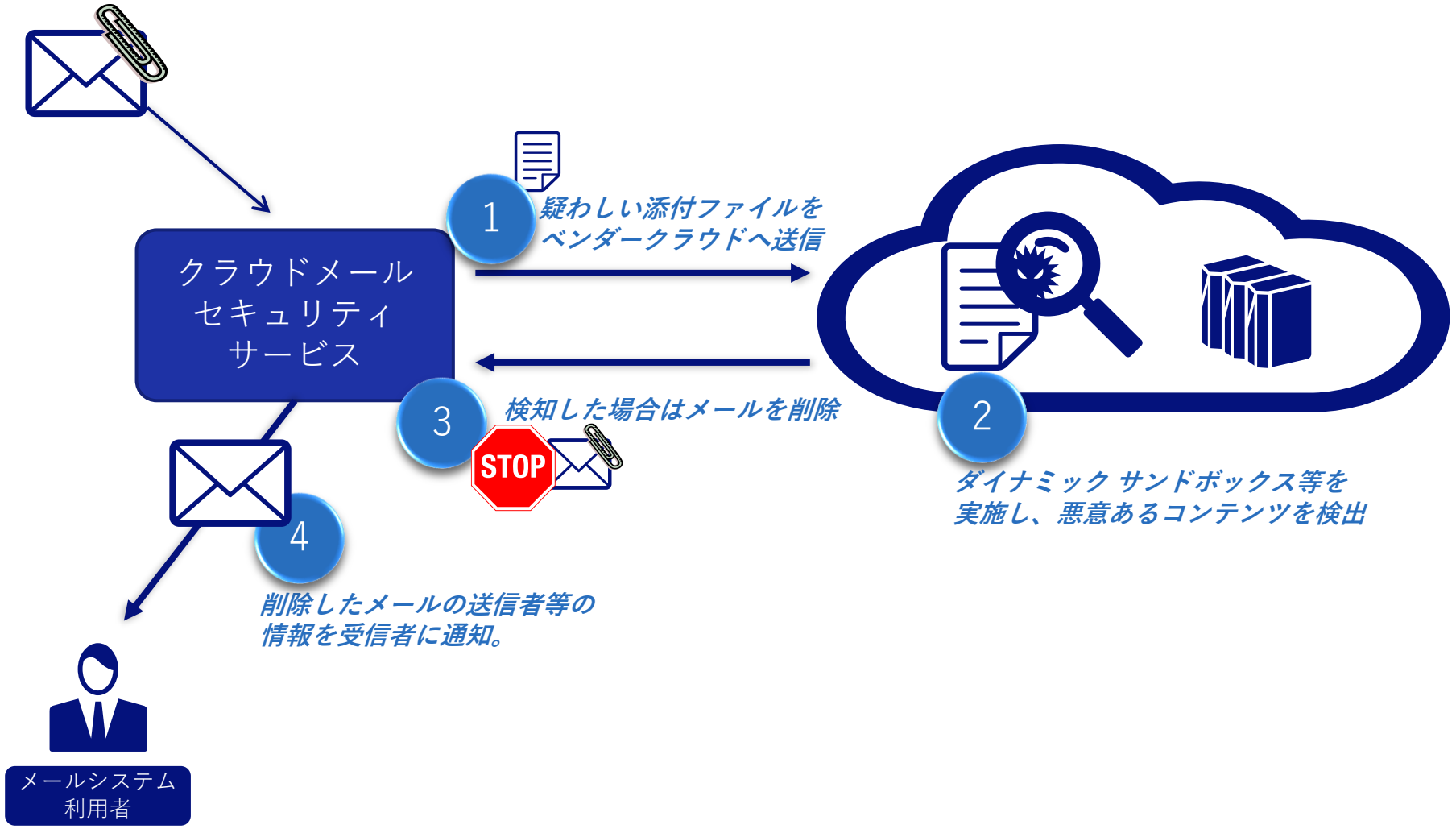
＜サンドボックスとは＞
未知の脆弱性を狙った攻撃やマルウェアの場合は、従来のアンチウィルスゲートウェイでは検出されない為、サンドボックス（振る舞い検知）により、添付ファイルを実際に仮想環境で実行して、その挙動により判断する手法です。

【対応ファイル形式】

・Microsoft Word (doc & docx)
・Microsoft Excel (xls & xlsx)
・Microsoft Powerpoint (ppt & pptx)
・Adobe PDF
・Adobe Flash (swf)
・RTF
・HTML attachments
・以下の圧縮・アーカイブ・エンコード変換・カプセル化ファイル
（※）－ZIP, TAR, RAR, Gzip, UUencode, CAB, TNEF

5.2. 標的型攻撃メール対策 / ポイント１

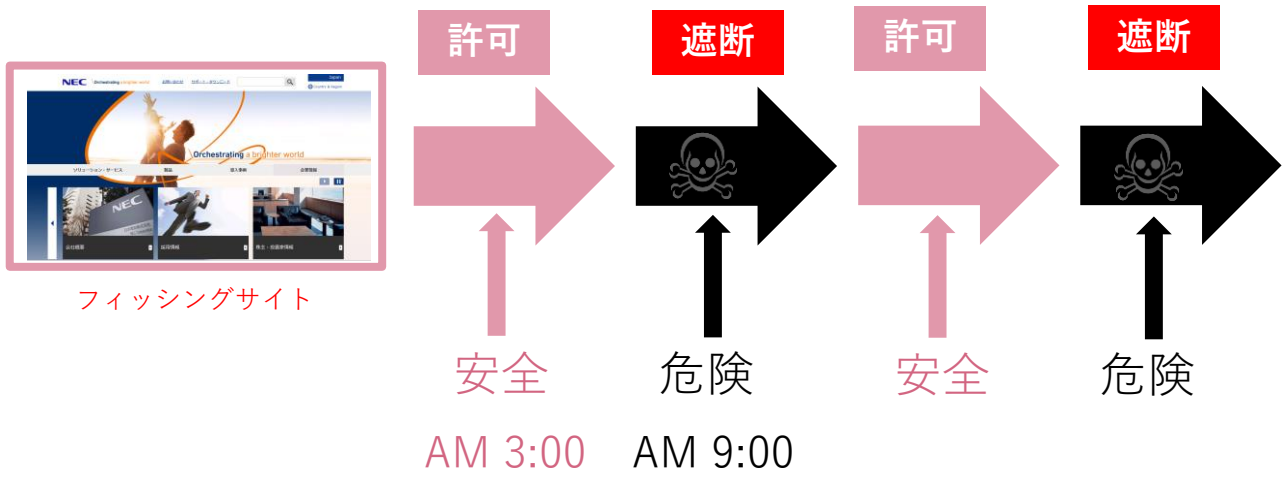
◆ ポイント１：添付ファイル型攻撃に対する動作



5.2. 標的型攻撃メール対策 / ポイント２

◆ ポイント２：特定時間に攻撃サイトに切り替わり、メール配信時の危険性検査を回避するURL誘導型攻撃にも対応

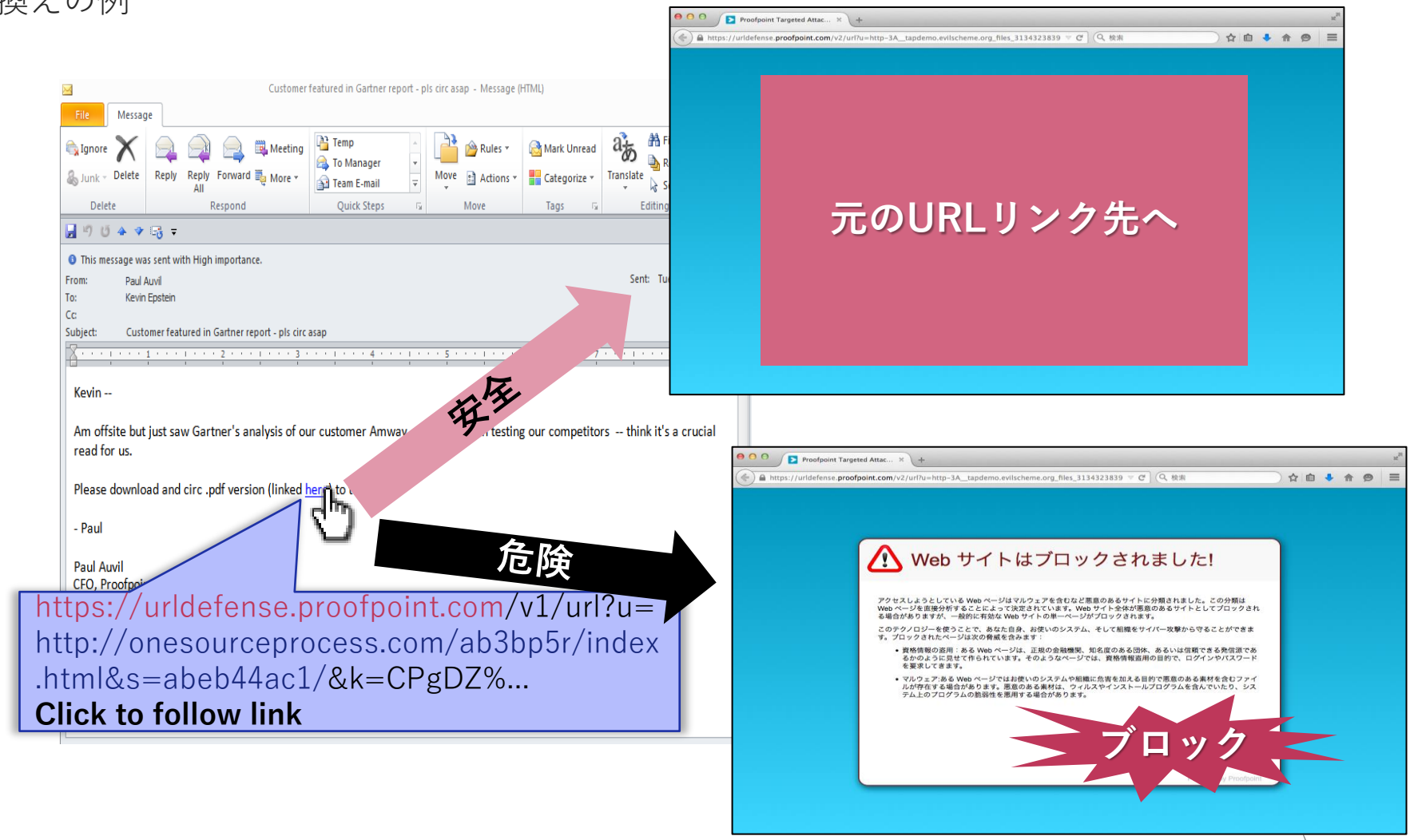
1. メール配送時（例：AM3:00）
   - 誘導先Ｗｅｂサイトは正常
2. 受信者がメールを確認する頃（例：AM9:00）
   - 誘導先Webサイトの挙動を変える
   - アクセスしただけでマルウェアをダウンロード



メール配信後に仕掛けられる脅威にも対応します

5.2. 標的型攻撃メール対策 / ポイント2

- ポイント2：URL誘導型攻撃への対応
  - URL書き換えの例



5.2. 標的型攻撃メール対策 / ポイント 3

◆ パスワード付きZIPファイル検査について

- ■ パスワード付ZIPファイル受信時に、クラウドサンドボックスにて当該メール本文中からパスワードを自動抽出して開封、検査を行います
  - • パスワードはファイルが添付されているメールの本文内に記載されているものが解析対象です
  - • パスワードを別メールで別送している場合は抽出できません
- ■ 検査時は添付ファイルとメール本文をクラウドサンドボックスにて検査します

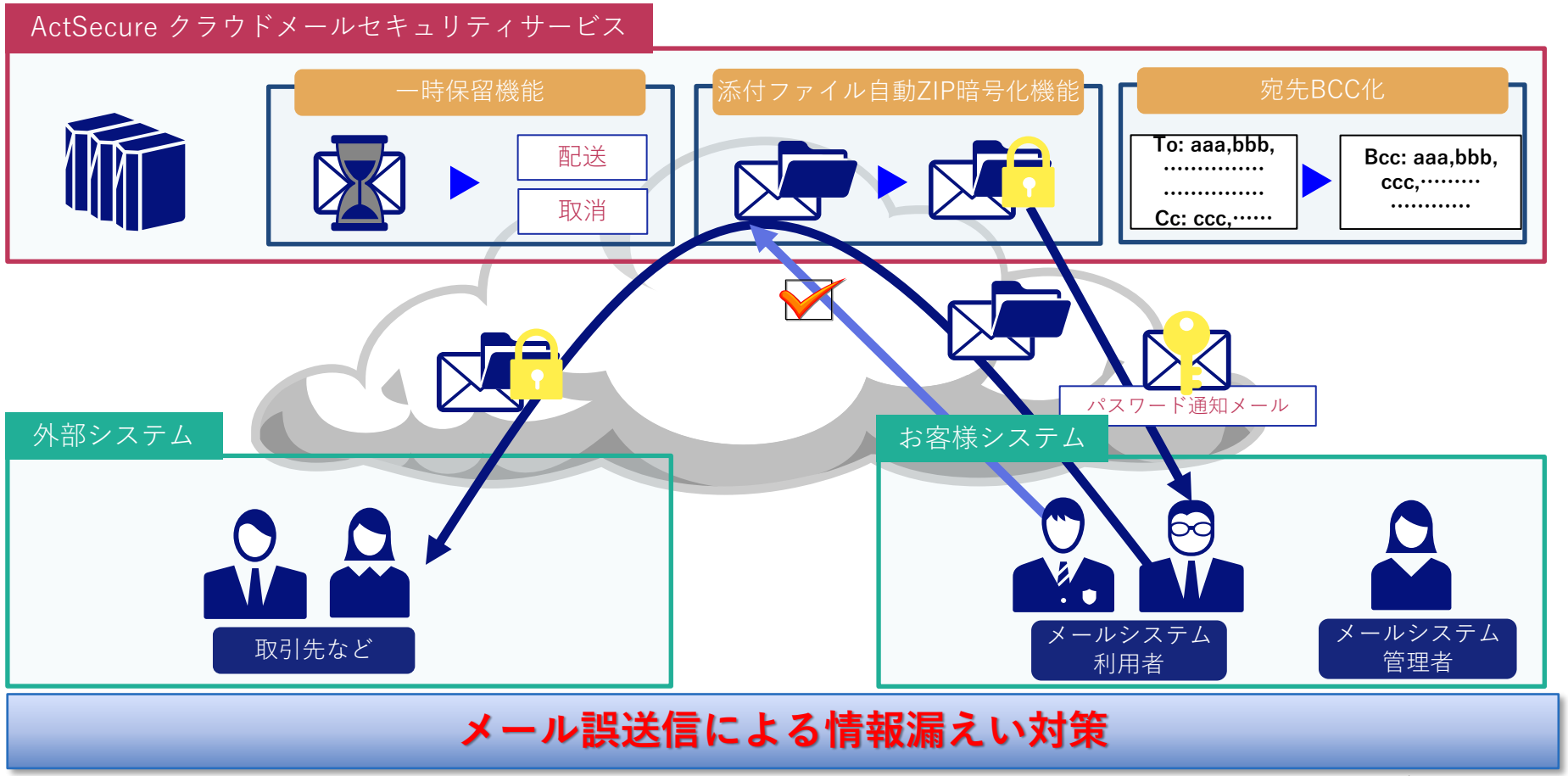
◆ 制限事項

- ■ パスワード抽出精度は100%ではないことをご理解お願いします

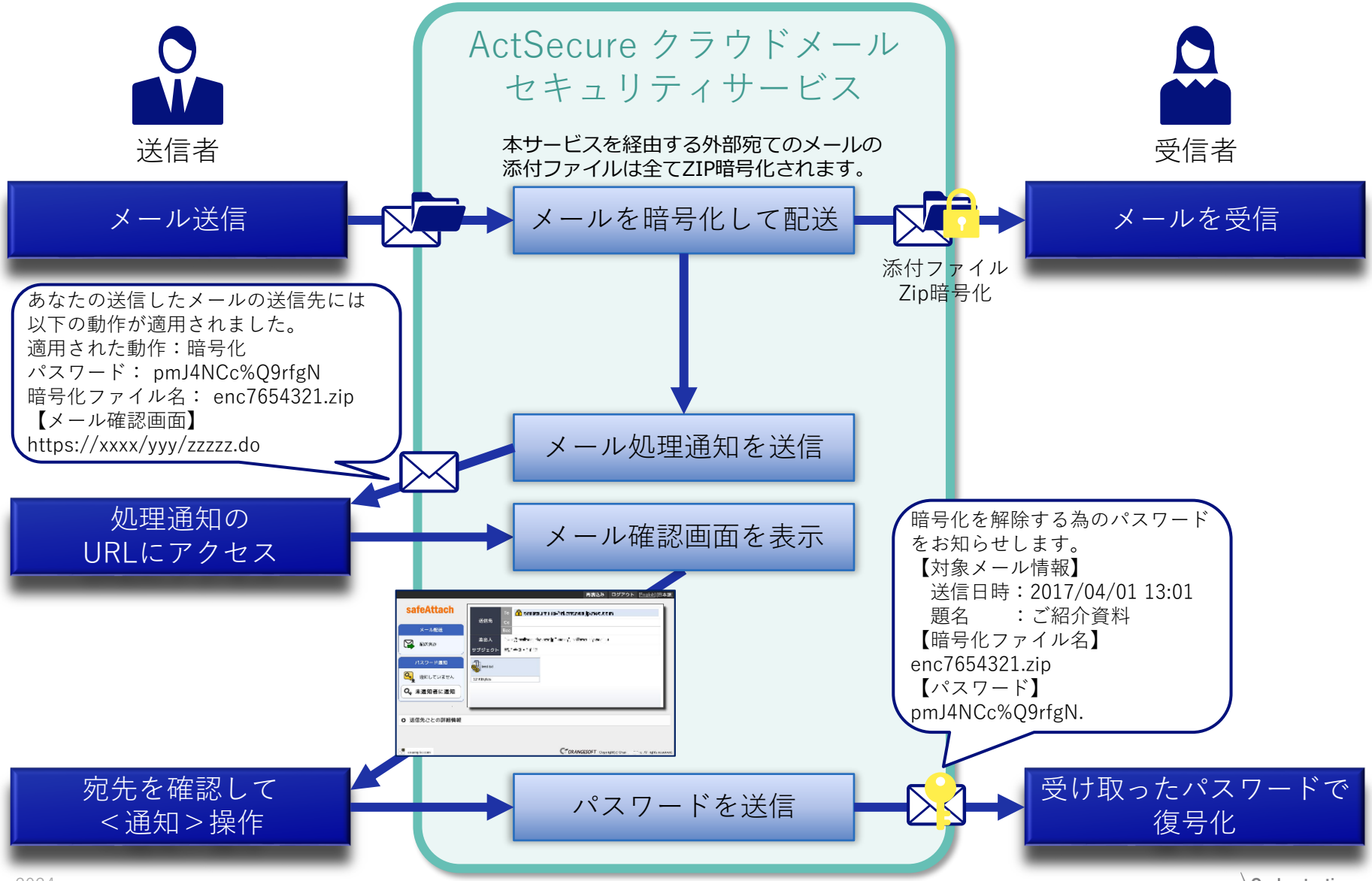
5.3. 誤送信防止（添付ファイルZIP暗号化）

うっかりミスのメール誤送信を防ぐ

- 外部宛てメールを一時保留し、送信者自身がメールの配送を取消すことが可能です。
- 添付ファイルを自動でZIP暗号化し、情報漏えいリスクを低減します。
- 大量のアドレスを宛先に指定した配信によるメールアドレスの流出を防ぎます。



5.3. 誤送信防止（添付ファイルZIP暗号化）運用フロー



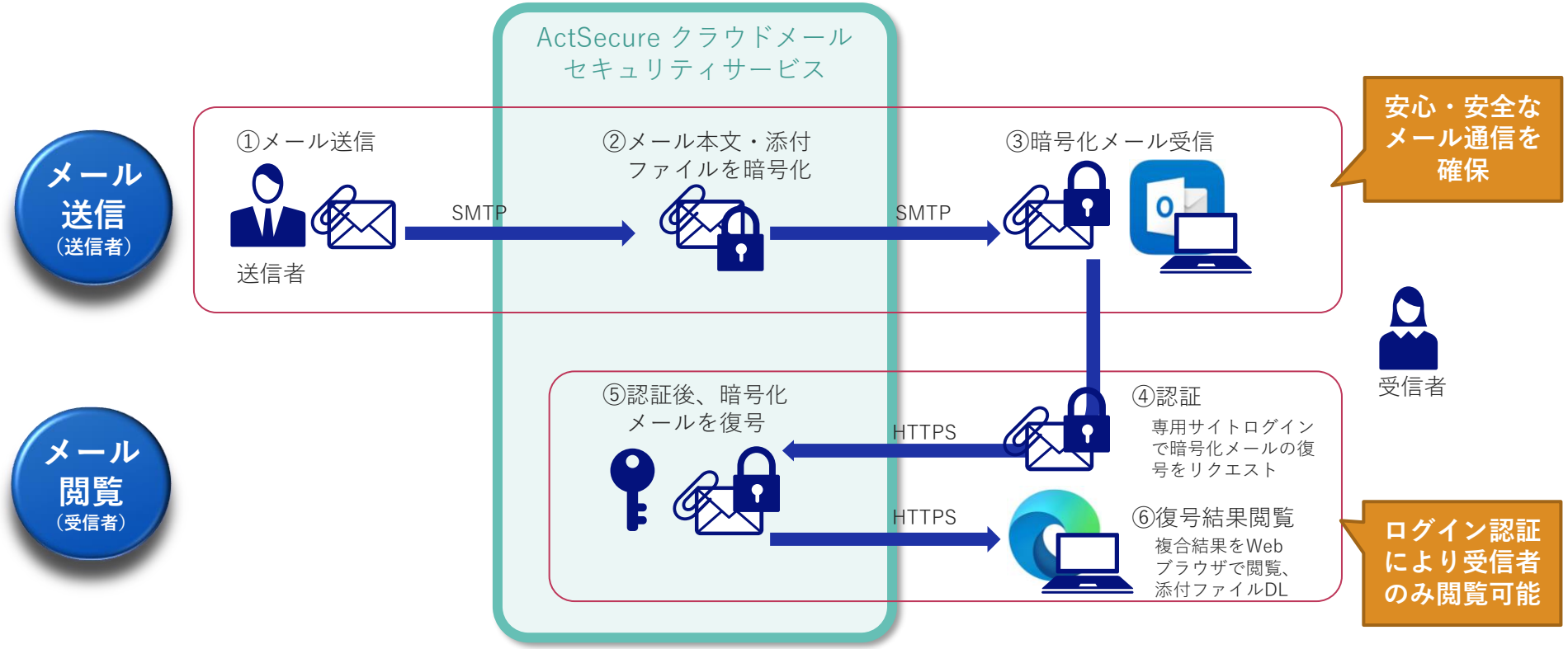
5.3. 誤送信防止（添付ファイルZIP暗号化）メール確認画面

5.3. 誤送信防止（メール+添付ファイル暗号化）

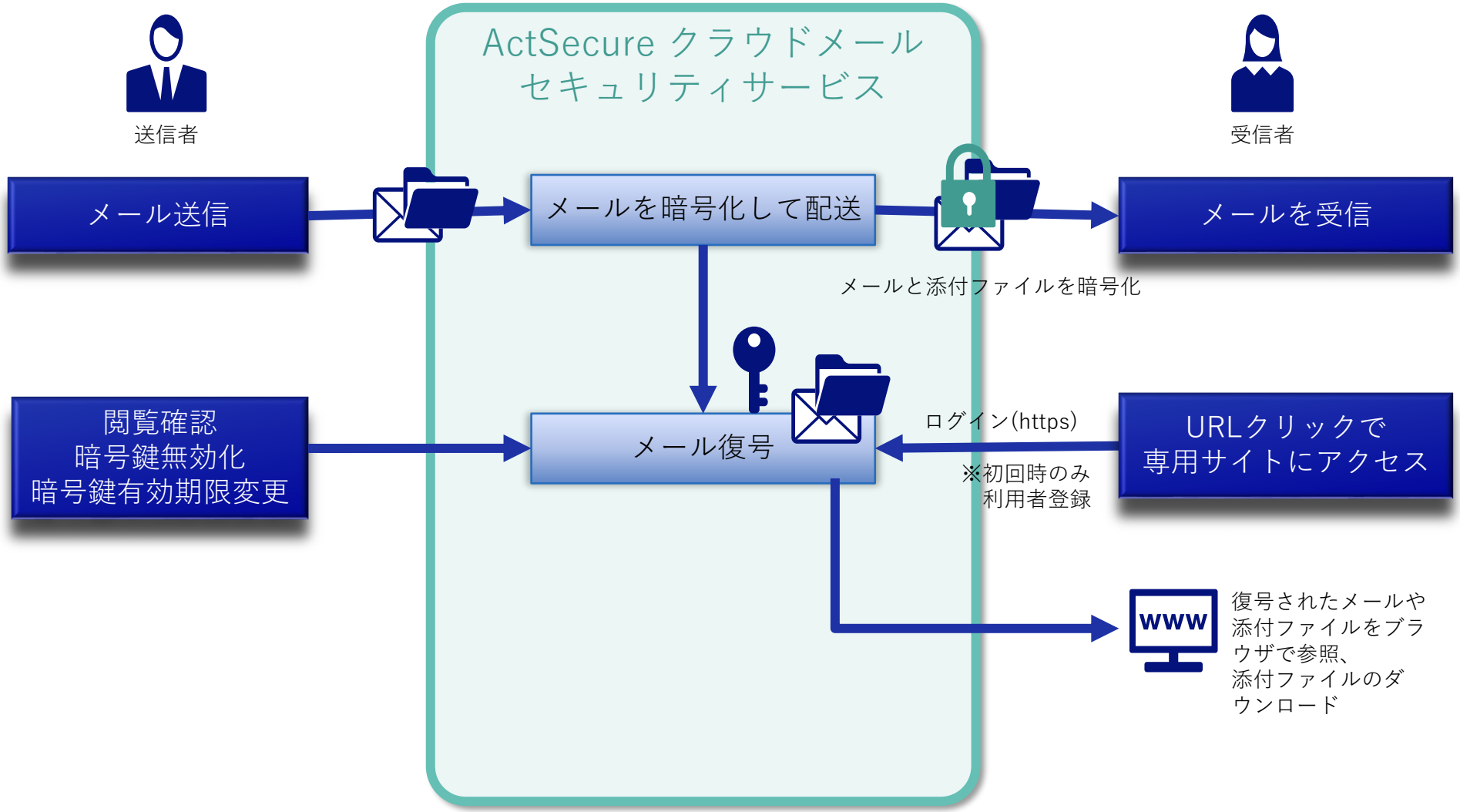
受信者へのパスワード送付が不要で便利＋添付ファイルに加えてメール本文も暗号化が可能

一時保留機能による送信取消に加えて、送ってしまった後でも閲覧不可にする対処が行えるため情報漏えいを水際でも防ぎます。

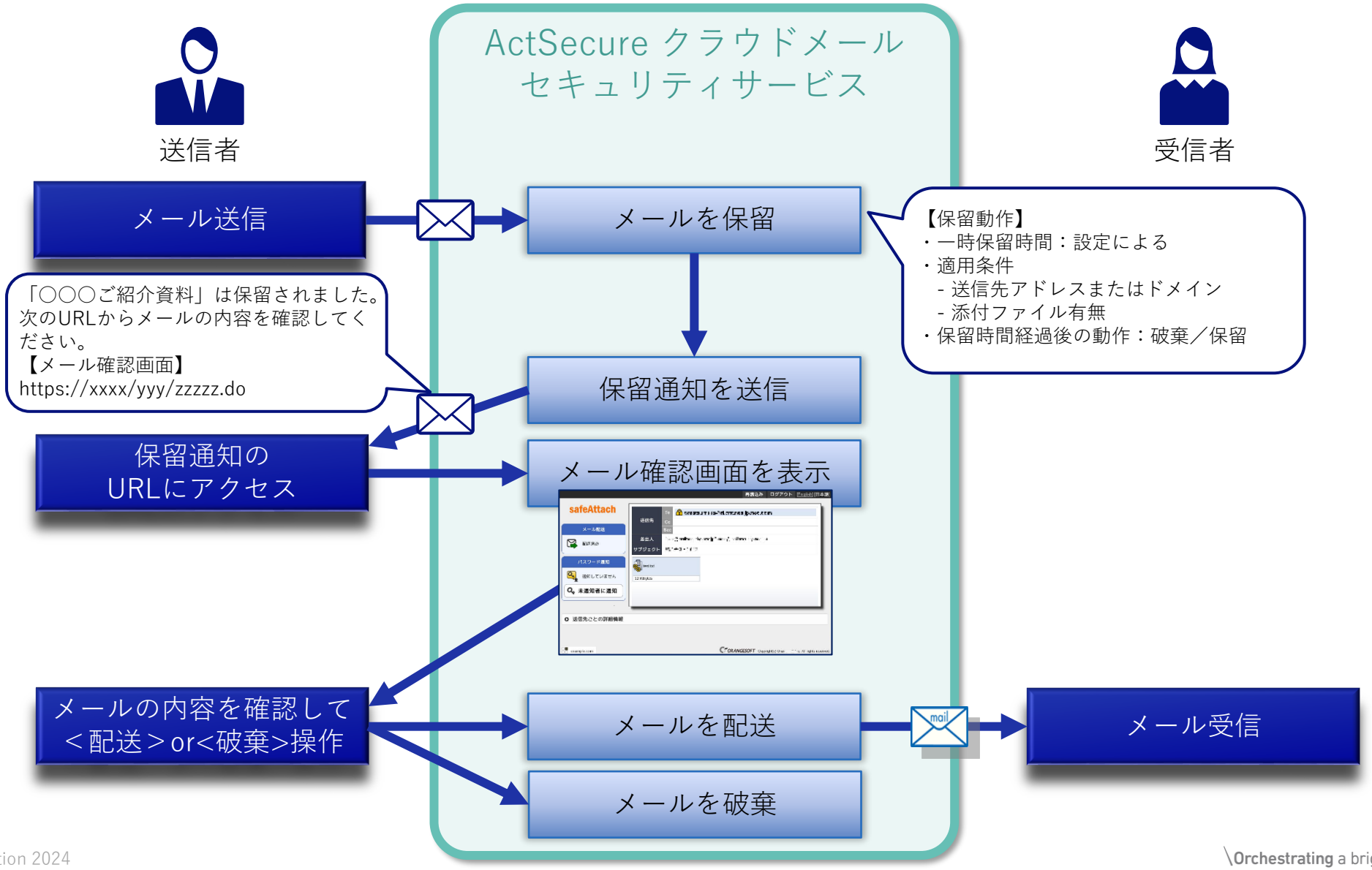
- 従来のPPAP方式で行っていたパスワードの送付が必要無くなり、非暗号化経路でのパスワードのやりとりがありません。
- 添付ファイルの暗号化だけでなくメール本文の暗号化にも対応し、よりセキュアな送付を可能にします。
- S/MIMEの運用で必要な証明書の管理や別途クラウドストレージの用意は必要ありません。



5.3. 誤送信防止（メール+添付ファイル暗号化）運用フロー

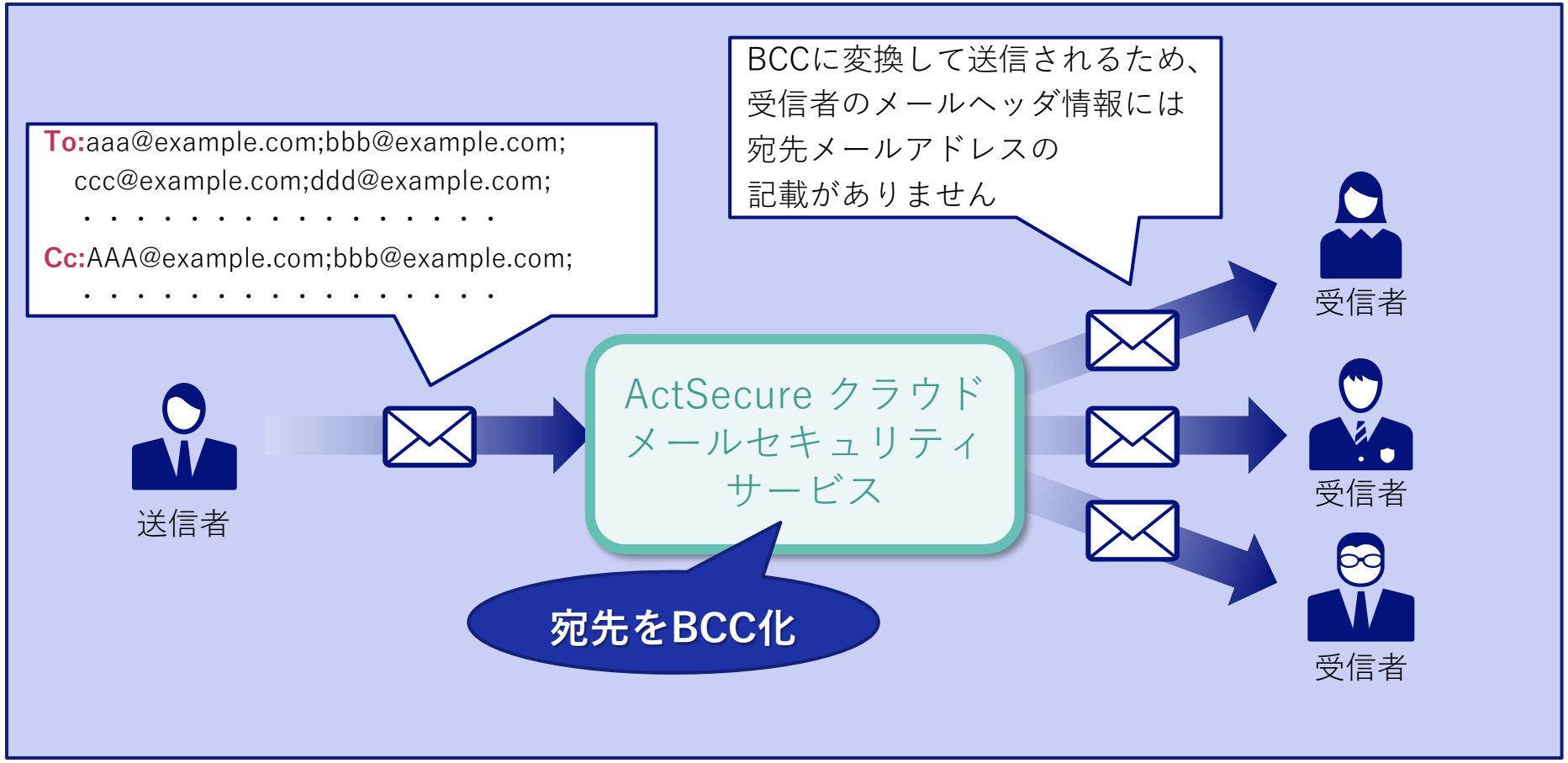


5.3. 誤送信防止 / メール一時保留（共通）運用フロー



5.3. 誤送信防止 / BCC化（共通）イメージ図

- メールのToやCcに指定されたアドレスを自動的にBCCへと変換し、
  メールマガジンなどの情報発信での、個人アドレスの情報漏えいを防止



※BCC化適用件数：10件（規定値）

6．サービスご利用にあたっての注意事項

1. 本サービスのご利用には、DNSの設定変更(MXレコードの変更)と、 誤送信防止機能をご利用の場合オンプレ、クラウド問わずお客様のメールシステムの配送先MTAの設定変更が必要です。
2. 本サービスをご利用された場合、お客様システムで外部から受信するすべてのメールの送信元IPアドレスは、本サービスのIPアドレスとなります。その為、お客様システム側で送信元IPアドレスに基づくチェックを実施されている場合は、影響有無を事前にご確認ください。
3. 本サービスは、お客様のメールサーバー（ドメイン）単位での登録となります。一部のメールアカウントでのみご利用いただくことはできません。
4. 標的型メール対策機能で検査するファイル形式は下記の通りです。
   Microsoft Word (doc & docx)、Microsoft Excel (xls & xlsx)、Microsoft Powerpoint (ppt & pptx)、Adobe PDF
   Adobe Flash (swf)、RTF、HTML attachments、以下の圧縮・アーカイブ・エンコード変換・カプセル化ファイル
   （※）ZIP, TAR, RAR, Gzip, UUencode, CAB, TNEF
5. 弊社が知りえたサービス履行に必要なお客様情報は、本サービスを提供する目的以外では使用しないものとします。
   ①お客様のご連絡先情報、ネットワーク、サーバの設計情報
   ②サービス提供に必要となるＩＤ、パスワード情報
   ③サービス開始後に作成した報告書、障害履歴
6. サービス機器から取得したログデータは、お客様を特定できないようデータを加工した上で、弊社内で下記の用途に二次利用（調査、分析、編集）する事にご了承いただいたものとします。
   ①セキュリティに関する脅威トレンドの調査・分析
   ②分析結果の弊社サービス利用顧客への情報提供
   ③弊社サービスの販売促進データとしての活用
7. 本サービスは、セキュリティインシデントを完全に防止するサービスではありません。万が一損害が生じてもその補償を行いません。損害には以下のようなものが含まれます。
   ①セキュリティインシデントによる情報機器（ハード、ソフト）の損傷
   ②情報機器の障害による売り上げ減少等に伴う収益減少
   ③第三者に対して負担する損害賠償責任による損害
9. 本サービスの最低利用期間は契約日から1年間で、更新契約も1年間単位となります。
10. お客様システム内や外部システム（それぞれのDNSサーバやメールサーバ、社内用端末など）で発生する障害は本サービスの障害対応範囲外となります。
11. ファイルタイプ制限によりexe,com等の形式のファイルは削除されることがあります。また、入力情報を扱うプログラムファイルがウィルスや、標的型攻撃と判定される場合がありますので実行形式のファイルを取り扱う場合はご注意ください。

7. サービス価格表

【再掲】サービスメニュー

- NECクラウドのサービス環境をシェア型でご提供する形態で、最低契約数100ID以上からご契約いただけます。（最低契約数をご契約いただければ、100ID未満でもご利用は可能です。）
- 必要に応じてサービス組み合わせてご利用頂ける構成となっております。

サービスの組み合わせ

- ①アンチスパム／ウィルス
- ②アンチスパム／ウィルス ＋ 標的型攻撃メール対策
- ③アンチスパム／ウィルス ＋ 誤送信防止（添付ファイルZIP暗号化）
- ④アンチスパム／ウィルス ＋ 標的型攻撃メール対策 ＋ 誤送信防止（添付ファイルZIP暗号化）
- ⑤アンチスパム／ウィルス ＋ 誤送信防止（メール+添付ファイル暗号化）
- ⑥アンチスパム／ウィルス ＋ 標的型攻撃メール対策 ＋ 誤送信防止（メール+添付ファイル暗号化）

アンチスパム／ウィルス	• メールのウィルス・スパムチェック機能を提供します。 ※送信メールのチェックは、誤送信防止サービスをご契約時に機能提供が可能です。
標的型攻撃メール対策	• サンドボックスにより未知のマルウェアを検知し、標的型攻撃メールを削除します。 • メール受信時には脅威が判断できないURLリンクについては継続的に監視し、危険が確認された場合には当該Webサイトに対するアクセスを遮断します。
誤送信防止（添付ファイルZIP暗号化）	• 「添付ファイルのZIP暗号化」、「送信メール一時保留」、「送信メール宛先強制Bcc化」の機能を提供します。
誤送信防止（メール+添付ファイル暗号化）	• PPAP対策を含む新たな誤送信防止サービスとして、「メール+添付ファイル暗号化」、「送信メール一時保留」、「送信メール強制BCC化」の機能を提供します。

※誤送信防止（添付ファイルZIP暗号化）と誤送信防止（メール＋添付ファイル暗号化）は併用できません

7.1. サービス初期費用

◆ 初期費用は利用する機能、機能数に関わらず、利用するID数によって変動します。

（単位：円）

サービスカテゴリ	区分	提供価格
初期費用	100～500IDまで	弊社担当営業まで、 お問い合わせください。 （弊社担当営業がご不明の場合は、お手数をおかけし恐縮ですが、以下のお問い合わせフォームより営業アサインご希望の旨、お問い合わせをお願いいたします。 http://www.nec.co.jp/contactus/index.html）
	501～1000IDまで	
	1,001ID～10,000IDまで	
	10,001ID～	

※1 サービス初期費用は、サービス利用開始前の登録費用として申し受けます。
※2 サービス利用途中に区分を超えて利用ID数を追加する場合は、追加前の区分の費用との差額を申し受けます。

7.2. サービス月額費用

◆ 基本サービス、オプションサービスの機能毎の1IDあたりの月額価格は下記の通りです。

（単位：円）

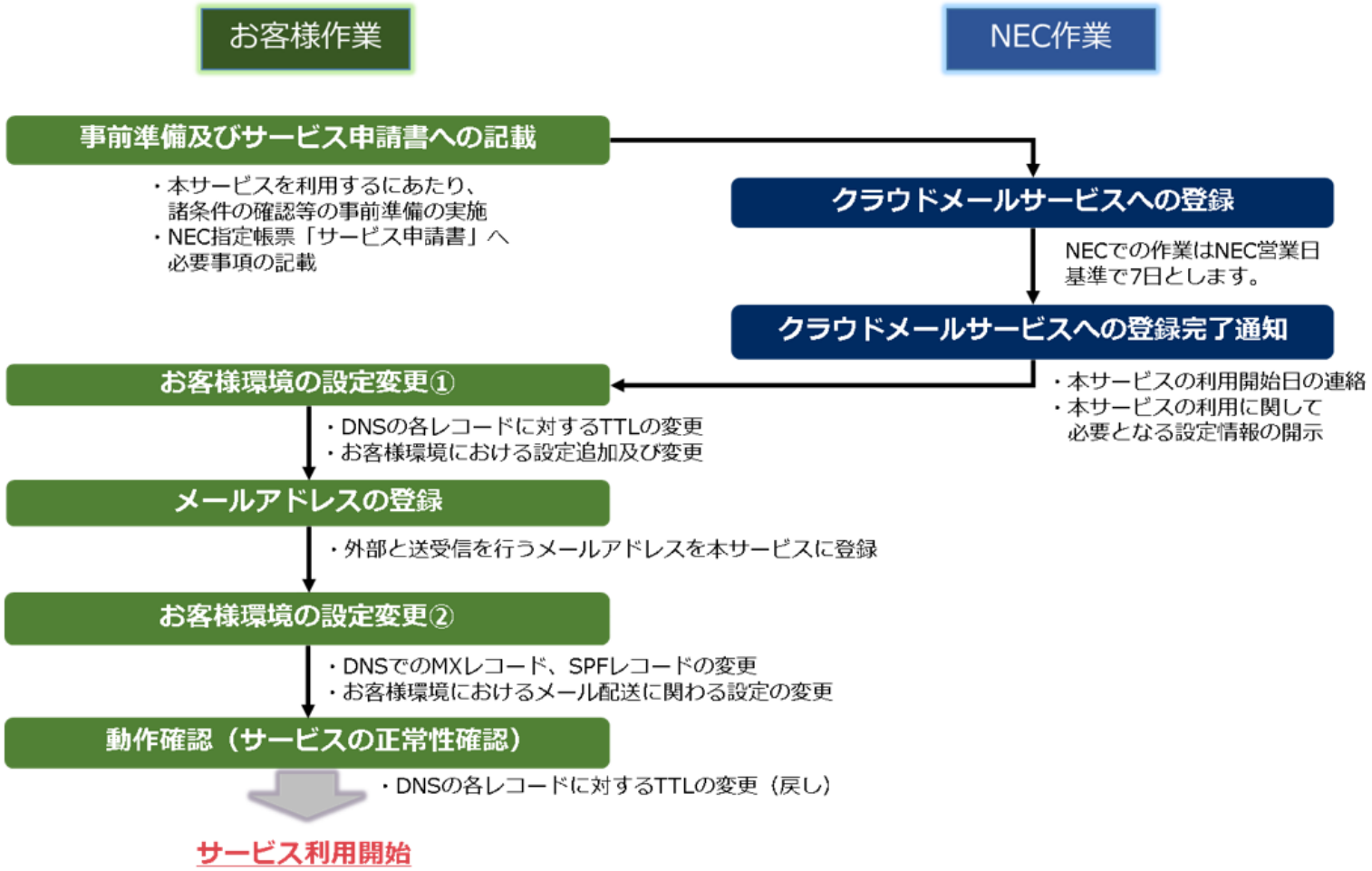
<table>
<tr><th>サービスカテゴリ</th><th>機能</th><th>提供価格</th></tr>
<tr><td>基本サービス</td><td>スパム・ウィルスチェック</td><td rowspan="4">弊社担当営業まで、
お問い合わせください。

（弊社担当営業がご不明の場合は、お手数をおかけし恐縮ですが、以下のお問い合わせフォームより営業アサインご希望の旨、お問い合わせをお願いいたします。
http://www.nec.co.jp/contactus/index.html）</td></tr>
<tr><td rowspan="3">オプションサービス</td><td>標的型メール対策</td></tr>
<tr><td>誤送信防止（メール+添付ファイル暗号化）</td></tr>
<tr><td>誤送信防止（添付ファイルZIP暗号化）</td></tr>
</table>

※1 誤送信防止機能には、送信メールのスパム・ウィルスチェックが含まれます。
※2 誤送信防止（メール+添付ファイル暗号化）と誤送信防止（添付ファイルZIP暗号化）は併用できません。

8. サービス導入までのスケジュール

◆ サービスの利用申請から最短7営業日でサービス環境を提供いたします。



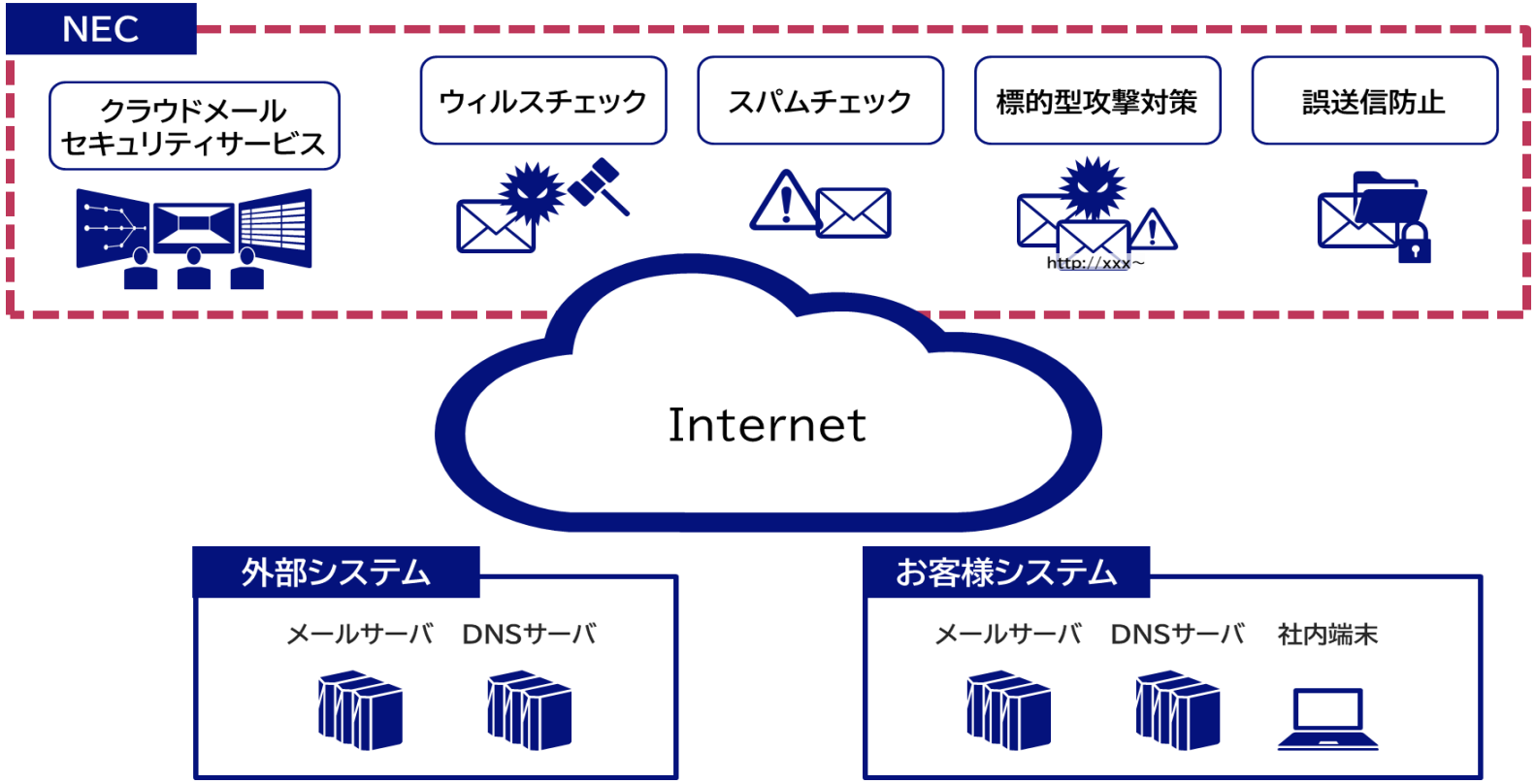
9. SOW

◆ サービス導入におけるSOWは次の通りです

項	作業アクティビティ	詳細	担当	
			お客様	NEC
1	サービス利用申請	サービス申請書に必要事項を記入し、お客様または担当営業がActSecureポータルより利用申請を実施します。 提出物: クラウドメールセキュリティサービス申請書	○	―
2	サービス環境準備	NECがNECCI上にサービス環境の構築（マルチテナントの環境へお客様のアカウント登録、メールの振り分け設定、NW設定など）を実施します。構築は最短で7営業日です。	―	○
3	登録完了通知	サービス環境の構築が完了したことを通知します。 通知内容: 配送設定情報、管理GUIへのアクセス情報	―	○
4	お客様環境の設定①	経路が素早く切り替わるように、お客様のドメインを管理しているDNSのキャッシュ生存時間を一時的に短くします。また、サービス環境へアクセスできるようにお客様環境のファイアウォールの設定を変更します。	○	―
5	メールアドレスの登録	サービスの管理GUIから、お客様が外部と送受信を行うメールアドレスを全て登録します。	○	―
6	お客様環境の設定②	お客様のドメインを管理しているDNSの設定を変更し、お客様環境外からお客様環境へのメールがサービス環境を経由するようにします。 お客様のメール配送サーバの設定を変更し、お客様環境から外部へのメールがサービス環境を経由するようにします。	○	―
7	動作確認	お客様環境外からのメールをお客様環境へ送付し、サービスが正常動作していることを確認します。 お客様環境からお客様環境外へメールを送付し、サービスが正常動作していることを確認します。 正常性を確認後、必要に応じてお客様環境の設定①で実施したDNSのキャッシュ生存時間を元に戻します。 また、必要に応じて従来のメール経路をファイアウォールで遮断します。 ※正常動作を確認できない場合、NECへ問い合わせください。問い合わせ対応にて解決へ向けて支援いたします。	○	△

10.責任分界点

- NECでの責任範囲は点線部で示した、本サービスを提供する部位のみとします。お客様にてご利用されている他のサービスを含めたシステムや外部システム（それぞれのDNSサーバやメールサーバ、社内端末など）で発生した障害やインターネット上のネットワーク障害は本サービスの障害対応範囲外となります。



11. SLA/SLO

- SLA (Service Level Agreement）については定義しないものとします。

- SLO (Service Level Objective) はは稼働率99.9%です。ただし、以下に定めるサービス停止を伴う作業実施時を除きます。
  - OSやソフトウェアのサポート期限等による、システム停止を伴うバージョンアップ
  - OSやソフトウェアのセキュリティパッチ適用（2回/年ほどを予定）
  - OSやソフトウェアの不具合等の修正により停止が必要な作業
  - その他、NECが必要と判断した場合

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC