2026/4/16

【　機密性の高いメールサーバ運用についてのご提案　】

TINS-NET

昨今、生成 AI の普及により、Microsoft365 メール、Yahoo メール、グーグル gmail、Apple icloud メールなど大手メールサービスにあるユーザのデータが AI 学習に使われているのではないか、という疑念が一時持ち上がりました。
また、Amazon AWS、マイクロソフト Azure といった大手クラウドサービスで運用されている数々のサービスが大元から侵入を受けた場合の責任の所在が不明瞭、という件も指摘されております。この場合にメールデータの流出の可能性もゼロではないと認識されております。

現時点ではその様な事例は無いと確認はされましたが、実際問題として
「インターネットメールのデータそのものは、本来お客様のプライベートに所有されるデータであるにもかかわらず、99%以上は暗号化などの処理はされていない状態でサーバに保存されている」という事実が再認識されて来ております。

仮に暗号化保存されていたとしても、暗号化の責任はサービス提供者側にあり、いつでも解読でき、国によってはデータの無条件提出などの法的処置からも免れない状態にあります。

こういった状況において、弊社つくばインターネットサービスとしましては

１．お客様によりメールの暗号化を行い
２．サーバが侵入を受けてもお客様のメールの内容は漏洩しない

メールサーバをご用意致しました。

試験的にこの暗号化専用メールサーバを構築し、専用ドメイン **xxxx@smail.tins.ne.jp** の
メールアドレスにより運用を致しております。
ご興味がありましたら、info@tins.ad.jp までご希望のメールアドレス(**xxxx@smail.tins.ne.jp**)を
ご連絡下さい。メール ID とパスワードを発行し、お返事致します。

※使用の条件としましては

・使用メールソフトウェアは、Thunderbird 指定　（現状テストでは。今後増える可能性あり）
・暗号に用いる鍵の生成の作業はユーザ様にして頂く（弊社側でも可能ですがそれでは機密と言えない）

という手間が必要とはなります。ご面倒ではありますが機密化の為に必要な要件としてご理解下さい。

設定手順は、以下に提示しておりますのでご参照下さい。
設定についてご質問等がございましたら、info@tins.ad.jp までお問い合わせ下さい。

「tins.ne.jp サービスご利用のお客様向け」パソコン用メールソフト Thunderbird のインストール・設定方法：　https://www.tins.ad.jp/img/SecureThunderBird.pdf

今回、暗号化保存に対応したメールサーバは個人ユーザ様対象サービスですが、ドメイン単位、お客様専用サーバ、または暗号鍵の管理方法をどうするかによって（個人・組織）何通りかの運用方式がございます。サーバ預かり、バーチャル・ドメインサービスご利用のお客様で、このメールサービスにご興味がございましたら、info@tins.ad.jp までご連絡下さい。

よろしくお願いいたします。

以上