GUARDIANWALL MailFilter 機能詳細、製品画面サンプル

フィルタリングルール

柔軟性の高いフィルタリング機能と、豊富な配送制御機能で、業務にマッチしたポリシーを設定でき、メール誤送信や情報漏えい事故を未然に防ぐことが可能です。
またルールの編集画面は、プルダウンやチェックボックスで容易な入力が可能なモードと、関数を用いてより高度な定義が可能なモードの2種類をご用意。

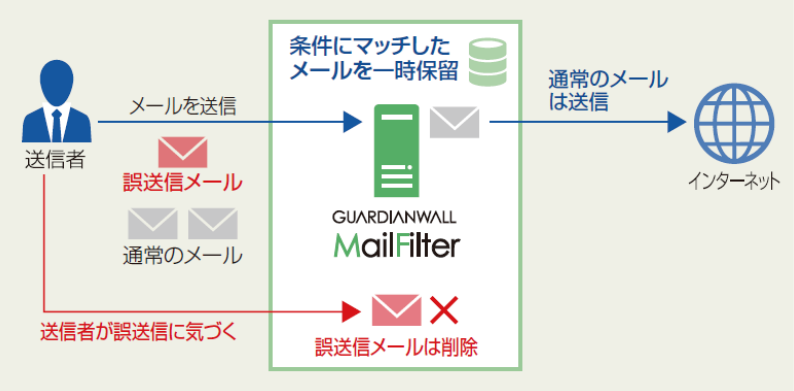
保留機能のスマートデバイス対応

スマートフォンやタブレットなど、スマートデバイス用に最適化した保留メール管理画面から、メールの本文や添付ファイル、ヘッダー情報などを閲覧し、送出／削除／転送、一括送信、一括削除といった操作が可能です。また、保留メールを閲覧や監査した記録を残すことも可能です。

※スマートデバイスからGUARDIANWALL MailFilterへアクセスするためには、別途お客さまネットワーク環境のご対応が必要となります。

遅延配送

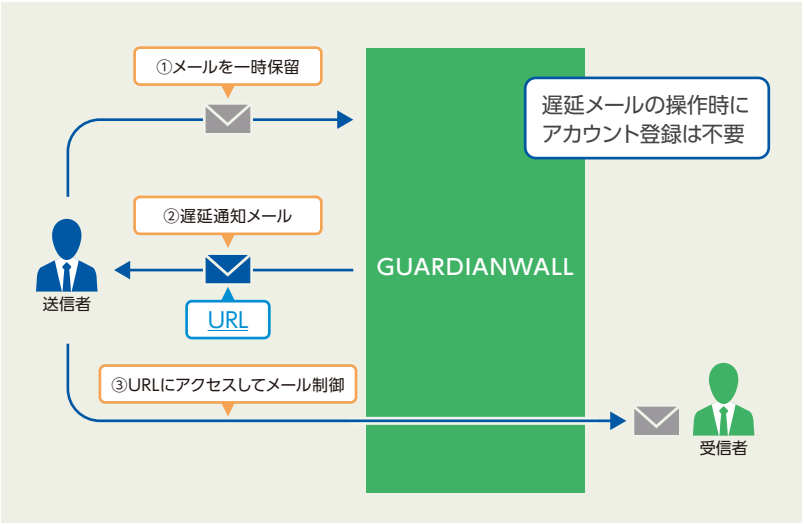
送信メールを一定時間保留することができます。一時保留されたメールは、メール送信者自身で削除することが可能です。
メール誤送信時の多くは送信直後にその送信者自身が気づくケースが多く、送信者自らが誤送信に気づき削除が可能となることで、誤送信を未然に防ぐことができます。

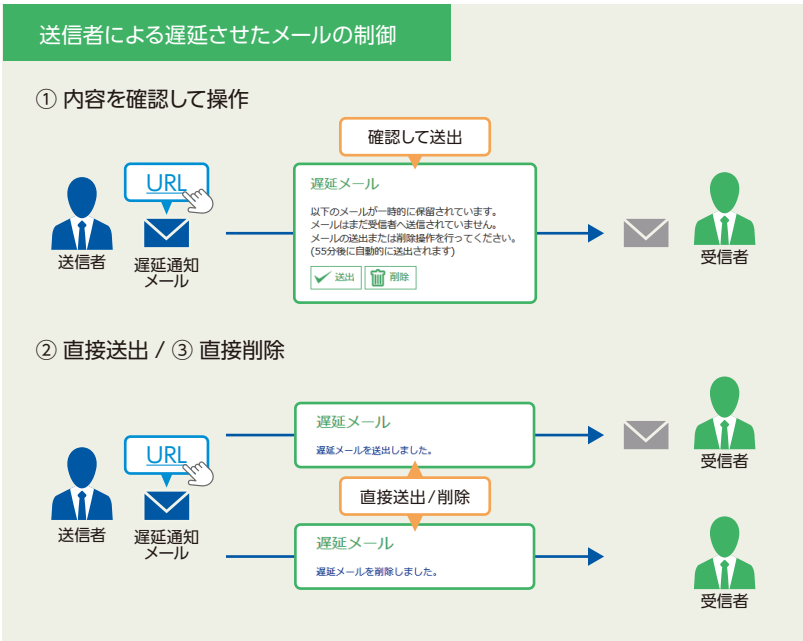


New

遅延配送機能が強化され、アカウント登録なしで遅延メールが操作できるようになりました。
遅延配送機能によってメールが一時保留されると「遅延通知メール」が送出されます。
「遅延通知メール」に記載されているURLにアクセスすることで、遅延されているメールの送出や削除といった操作が可能です。
送信後の誤りに気づいた場合などには、メールをすぐに停止するといった制御ができます。

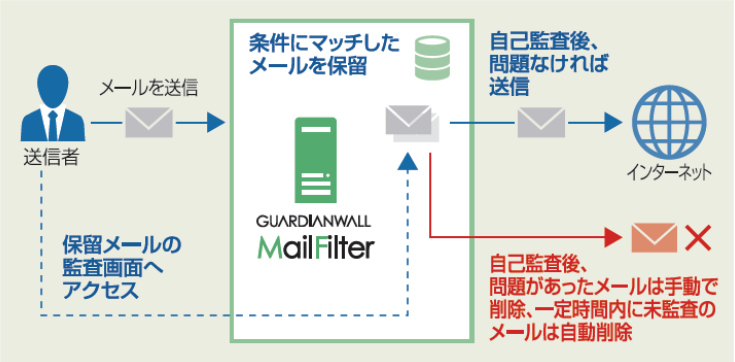
【遅延配送メールの3つの制御】　送信者宛「遅延通知メール」に下記の3つのURLが記載されます。
①送出/削除URL　：　送信後に再度、内容確認を行い、間違いなければメール送出、間違いがあれば、メール削除ができます。
②直接送出するURL　：　送信時に確実に確認し、遅延設定時間を待たずにメールを送出できます。
③直接削除するURL　：　送信後に誤送信に気づいた場合、メールをすぐに削除できます。





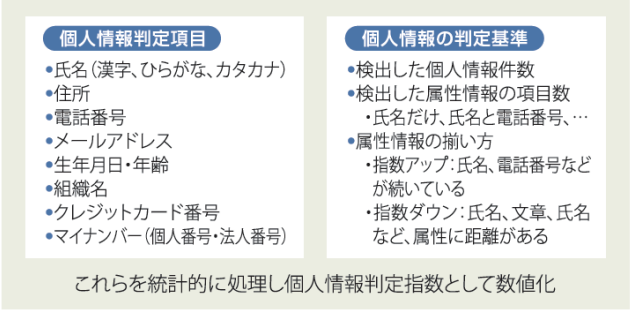
自己監査

送信者が一定時間内に監査を行わないメールを自動で削除することが可能です。
例えば、重要なメールは送信時に上司承認を行い、一般のメールは送信者自身のチェックのみとするなど、メール承認者に負荷のかからない誤送信対策を実現します。



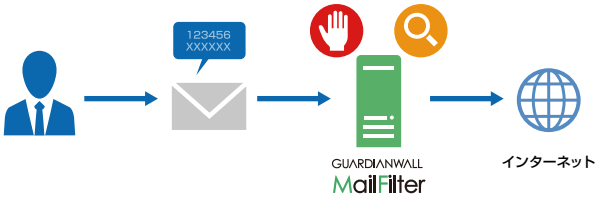
個人情報検査　- 特許取得済 -

情報漏えいで一番注意すべき個人情報も、通常のキーワード検査では発見が難しい個人情報を弊社独自技術によりスコア付け(0～100)を行い、設定したスコア以上のメールを保留や削除することが可能です。
氏名、住所、組織名は約7万語の辞書※を使用し検出、電話番号、メールアドレス、クレジットカード番号はパターンマッチングで検出、個人情報と思われる言葉をあらかじめ登録する必要がありません。
※辞書は追加・編集できません



マイナンバー検出（チェックデジット検査対応）

メール本文や添付ファイル内を検査し、マイナンバー情報を検出したメールを保留や削除できるようになりました。個人番号、法人番号のどちらも検出可能です。メールログ閲覧からマイナンバーを含む過去メールの検索も可能です。



マイナンバーは数字だけで構成される情報ですが、
GUARDIANWALL MailFilterならチェックデジットの検査も行うのでより正確な検知が可能です！

標的型攻撃対策

■ 脅威情報連携機能

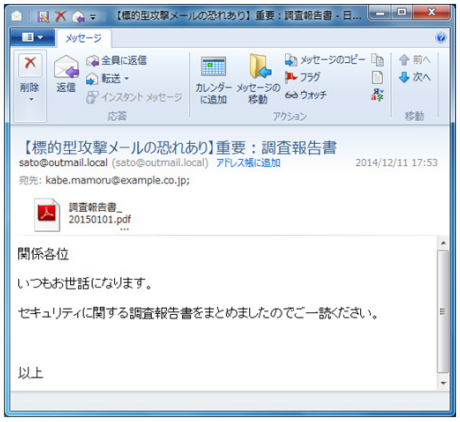
脅威となり得るURL情報を、GUARDIANWALL Mailセキュリティにてメール本文や添付ファイルから収集、またはトレンドマイクロ社の「Deep DiscoveryTM Inspector（DDI）」にて収集し、GUARDIANWALL WebFilter に「未知の脅威」として自動登録します。
標的型攻撃の出口対策として、現状のフィルタリングに加え、登録された脅威URLへのアクセスをGUARDIANWALL Webセキュリティで遮断することで、「マルウェア感染」や「情報漏えい」を防ぎます。

※本連携機能は、GUARDIANWALL MailセキュリティのMailFilterもしくはMailSuite製品と、GUARDIANWALL WebFilterの併用が必要です。

■ 標的型攻撃メール検知機能

近年増加し情報漏えいの脅威となっている標的型攻撃の疑いがあるメールの検知が可能です。
標的型攻撃と判定された場合、件名に警告文を挿入しユーザーが安易に開封しないよう促すことや、メールの強制削除、管理者への通知などが設定できます。

〈標的型攻撃と判定されるメール例〉
- ヘッダーfromとエンベロープfromのドメインが異なるメール
- 二重拡張子の添付ファイルが付いたメール
  （例：ファイル名.pdf.exe）
- 不正プログラムが埋め込まれたOfficeファイルが添付された
- メール（※Office2003以降）
- 偽装されたリンク先URLが本文に記載されたメール
- フリーメールアドレスから送信されたメール
- 類似ドメインから送信されたメール



■ アンチウイルス／アンチスパム機能（オプション）

標的型攻撃の入口対策として、「既知の脅威」に対し効率的かつ有効なシグネチャベースのアンチウイルス・アンチスパム機能をオプションとしてラインアップ。標的型攻撃メール検知機能との併用により、メールからの脅威の侵入を防ぐとともに、脅威情報連携機能においてGUARDIANWALL WebFilterへ自動登録することで、より多くの脅威情報の検知・収集を実現します。さらに、社内から社外へ送信するメールに対しても本検査を実施し、自らが加害者となることを防ぎます。

添付ファイル検査

メール本文だけでなく多くの情報が含まれる添付ファイルに対してもきめ細かな検査が可能です。

キーワード検査 (検査対象拡張子)	添付ファイル内の文字列についてもキーワード検査が可能 ・Word 98～2016 (.doc、.docx) ・Excel 98～2016 (.xlsx、.xls) ・PowerPoint 98～2016 (.pptx、.ppt) ・Visio 2002～2016　(.vsdx) ・PDF 1.2～1.7 (Acrobat 4.0～DC)　(.pdf) ・一太郎 V5～V13/2004～2016 (.jtd) ※Microsoft Office 2003以降に搭載されたIRM(Information Rights Management)機能にて制限をかけたファイルについては検査対象外
パスワード検査	ファイルにパスワードが設定されているか判定が可能 ・Word、Excel、PowerPoint、PDF、一太郎、ZIP、RAR、7ZIP、PKZIP、ARJ圧縮ファイル
圧縮ファイルの展開	圧縮ファイル形式の添付ファイルを展開して中身を検査が可能 ・ZIP、LHA、RAR、CAB、GZIP、BZIP2、Z、TAR、7ZIP、ARJ、RPM、DEB、ISO、MSI、HQX、AppleSingle、TNEF、SZDD、PACK
個人情報検査	添付ファイル内の文字列に対して個人情報の検査が可能

ルールテスト

ルールの動作を本番適用前にテストできるようになりました。emlファイルを管理画面からアップロードし、メールの配送に影響を与えることなく、より安全に、より確実にルールの確認ができます。