メールやWebからの情報漏えいや監査対応を総合的に支援します

GUARDIANWALL

GUARDIANWALLシリーズ　製品総合カタログ

GUARDIANWALL シリーズは

お客さまの情報を守る（GUARD）壁（WALL）として、

「メール環境」と「Web環境」をトータルに守ります。

必要な対策をオールインワンで実現します。
ご利用いただく規模や環境も選びません。

GUARDIANWALL
Mailセキュリティ・クラウド
ベーシック
プレミアム

GUARDIANWALL
Mailセキュリティ・オンプレミス

- 情報漏えい対策
- メール誤送信対策
- 監査対応強化

MailFilter　MailConvert　MailArchive

- Microsoft 365向けメール誤送信対策

Outbound Security for Microsoft 365

- 標的型攻撃対策
- ウイルスメール、スパムメール対策

Inbound Security for Microsoft 365

GUARDIANWALL
Webセキュリティ・オンプレミス
WebFilter

- 不正アクセス・フィッシングサイト対策
- 不正データ送信対策（情報漏えい対策）

進化し続ける統合セキュリティソリューションです。

国内開発・一貫したサポート対応で
皆さまのビジネス環境を支えます。

日本企業の働き方・文化・ニーズを踏まえて開発を続け、
積み上げてきた「実績」と「信頼」があります。

多種多様な企業への導入実績

大手銀行、グローバル企業、ISP事業者などで多数導入いただいています。

導入実績
3,600社以上※1

ユーザー数
530万ユーザー※1

※1 2021年6月現在

多様化への対応

IT環境の変化や、次々に登場する新たなセキュリティ脅威など、多様化する状況に速やかに対応しています。

利用環境

クラウド　仮想環境　オンプレミス

保護対象

メール　クラウド　Web

「独創」と「共創」

外部製品との積極的な連携で、守る領域を今後も拡大していきます。

GUARDIANWALL
Mailセキュリティ・クラウド

GUARDIANWALL
Mailセキュリティ・オンプレミス

GUARDIANWALL Mailセキュリティは「MailFilter」「MailConvert」「MailArchive」と、これら3つを統合した「MailSuite※1」、さらにMicrosoft 365のセキュリティ対策を強化する「Inbound Security for Microsoft 365※2」「Outbound Security for Microsoft 365※2」の各製品・サービスで構成されています。

MailFilter
クラウド　オンプレミス

情報漏えい(誤送信)を
未然に防ぐ

- フィルタリング
- 配送制御

P.6 ▶

MailConvert
クラウド　オンプレミス

情報漏えい(誤送信)の
被害を低減する

- ファイルのダウンロードリンク化※2
- 宛先Bcc変換

P.7 ▶

MailArchive
クラウド　オンプレミス

情報漏えい(誤送信)を
調べて特定する

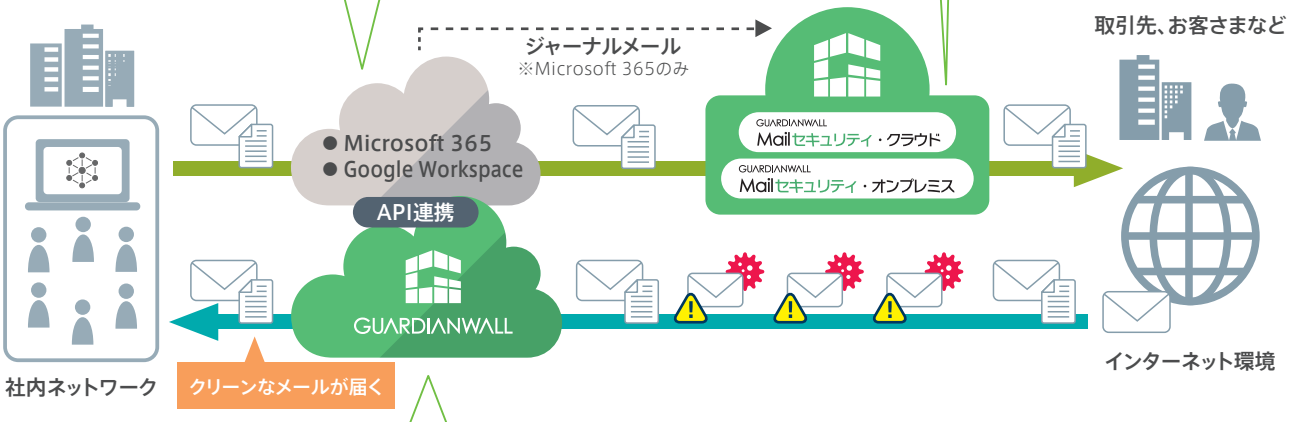
- アーカイブ

P.8 ▶

Outbound Security for Microsoft 365
クラウド　「PPAP問題」の解決や誤送信対策の強化など
安全なファイル送信を実現する

- 添付ファイルの自動分離・ダウンロードリンク化
- 送信後ファイル公開
- 送信前確認

P.9 ▶



Inbound Security for Microsoft 365
クラウド　標的型攻撃や詐欺メールなど
社外からのセキュリティ脅威を防ぐ

- アンチウイルス
- アンチスパム
- Webレピュテーション
- サンドボックス

P.9 ▶

※1 オンプレミスのみ　※2 クラウドサービスのみ

利用形態・メニュー比較

クラウドサービスは、プレミアムとベーシックの契約形態をご用意しております。
ベーシックでは利用を推奨する機能に厳選して提供しています。

		クラウドサービス		オンプレミス
		ベーシック	プレミアム	
		簡単UI・厳選機能	高度な設定が可能	
フィルタリング GUARDIANWALL MailFilter	メール送信遅延	●	●	●
	メール送信監査（自己／上長／第三者）	–	●	●
	検査機能（宛先・差出人／キーワード／個人情報）	–	●	●
	標的型攻撃検知	–	●	●
	配送制御（保留・転送・削除・中継）	–	●	●
ファイルダウンロードリンク化 宛先Bcc変換 GUARDIANWALL MailConvert	添付ファイルのダウンロードリンク化	●	●	–
	添付ファイル暗号化	●（社内間メールは不可）	●（社内間メールは不可）	●
	固定パスワード対応	–	●	●
	AES-256bit方式	●	●	●
	宛先Bcc変換	●（社内間メールは不可）	●（社内間メールは不可）	●
	パスワード通知文編集	–	●	●
	フィルタリング（細かな条件設定）	–	●	●
アーカイブ GUARDIANWALL MailArchive	保存対象	送信／受信／ジャーナル（Microsoft 365のみ）		
	保存期間	1年間（2～5年分保管は別サービス利用）		制限なし（お客さまにてHDD用意）
	全文検索	●	●	●
	メール一括ダウンロード	●	●	●
	レポート	メール分析レポートのみ	●	●
	メール取り込みツール	–	–	●
その他	コスト	経費		資産
	準備期間	数日で使用開始		機器調達の期間が必要
	障害対応／メンテナンス	弊社にて実施		お客さま作業
	価格（月額一人換算）	150円/人～	200円/人～	893円/人～（ライセンス費用のみ）

※クラウドサービスの仕様については、予告なく変更になる可能性があります。あらかじめご了承ください。

GUARDIANWALL MailFilter

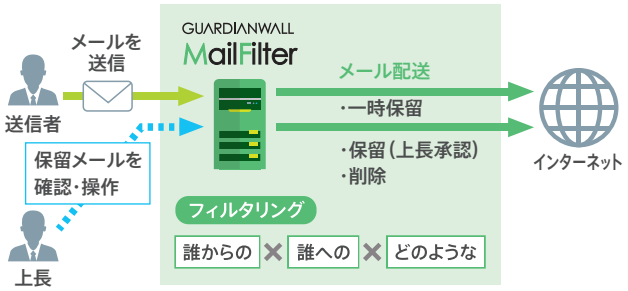
クラウド　オンプレミス

配送処理
（保留、遅延配送、削除）
個人情報検査
自己査閲
上長承認・他者査閲

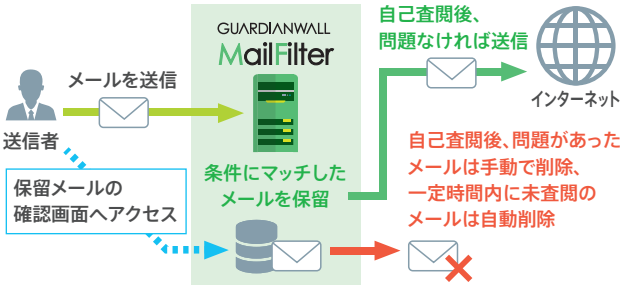
柔軟なフィルタリング設定と豊富な配送処理機能に加え、
強化された標的型メール対策機能により、誤送信対策、情報漏えい対策を実現します。

事前チェックによる誤送信の抑止

上長承認：上長による承認の後、メールを送信します。



自己査閲：送信者自身によるチェックを徹底化します。



個人情報も独自技術で検知 ― 特許取得済

個人情報が含まれていると思われる添付ファイルや
本文を検知します。

個人情報判定項目

- 氏名（漢字、ひらがな、カタカナ）
- 住所
- 電話番号
- メールアドレス
- 生年月日・年齢
- 組織名
- クレジットカード番号
- マイナンバー
（個人番号・法人番号）

個人情報の判定基準

- 検出した個人情報件数
- 検出した属性情報の項目数
・氏名だけ、氏名と電話番号、…
- 属性情報の揃い方
・**指数アップ**：氏名、電話番号などが続いている
・**指数ダウン**：氏名、文章、氏名など、属性に距離がある

これらを統計的に処理し個人情報判定指数として数値化

標的型メールへの対策

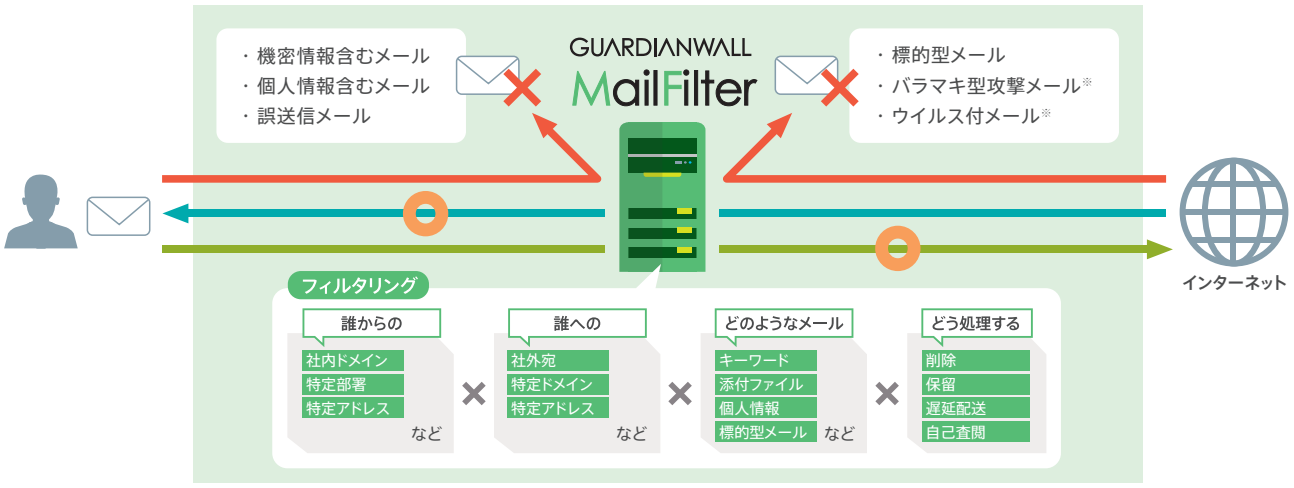
メールの形式を検査して標的型メールを検知する
ことで外部からの攻撃を防ぎます。

ビジネスメール詐欺（BEC）対策

SPF/DKIMなどの送信者ドメイン認証をすり抜けた標的型メールを検知
（類似ドメイン判定機能）

「未知の脅威」への対策

検知・収集した未知の脅威情報をGUARDIANWALL Webセキュリティへ連携し、標的型攻撃の出口対策を実現
（脅威情報連携機能）



※スパム・ウイルス検知には「アンチウイルス・アンチスパムオプション」のご契約が必要です。

GUARDIANWALL

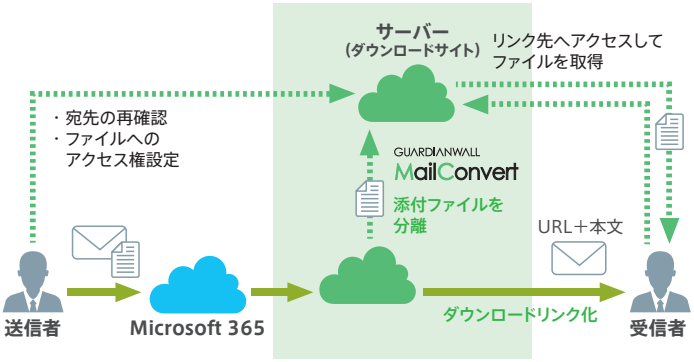
MailConvert

クラウド　オンプレミス

添付ファイル
ダウンロードリンク化
（クラウドのみ）
宛先Bcc変換
パスワード自動通知
AES256対応
リッチテキスト対応

万一の誤送信時にもその被害を無効化・大幅に低減します。
変換を適用する条件は「誰からの」「誰への」「どのようなメールを」と柔軟に
設定でき、業務にマッチしたポリシーの運用を実現します。

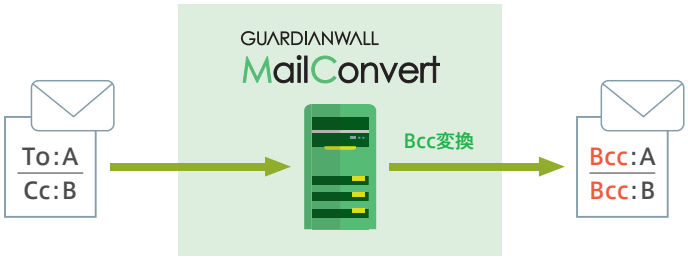
添付ファイルをダウンロードリンク化



ダウンロードリンク化機能で添付ファイルを自動的にメールから分離して、サーバーへアップロードします。
受信者はメールに記載されたURLにアクセスしてファイルをダウンロードできます。
送信者はメール送信後に宛先の再度確認とファイルへのアクセス権変更が行えるので、うっかり誤送信のリスクを低減します。
また、送信先に応じて添付ファイルダウンロードリンク化／添付ファイル暗号化を選択可能。お客さまのセキュリティポリシーに合わせて柔軟に対応します。

※クラウドのみ

宛先アドレスをBccに強制変換



誤送信事故原因の上位に挙げられる『メール一斉送信時に宛先をToやCcで送ってしまった！』というミスを防ぎます。
宛先数や特定の差出人など柔軟に条件設定も可能です。

PPAP（パスワード付きZIPファイル）対策のベストプラクティスとは？

2020年11月に「霞が関での利用を廃止する」と会見されたことで注目を集めた「パスワード付きZIPファイル」（いわゆる“PPAP”問題）。この会見を受けて、多くの企業や団体などでも「廃止か？　継続するか？」の検討が始まっています。

対策検討の視点

1 誤送信対策をどうするか？
- 送信前チェック
- 遅延配送
- 自己保留
- 第三者ダブルチェック

×

2 ファイル送信をどうするか？
- ファイル交換サービス
- オンラインストレージ
- URL変換ダウンロード
- ZIP暗号化
- S/MIME

お客さまの環境・ビジネスシーンに合わせた3つの答え

Outbound Security for Microsoft 365 で対策！ P.9 ▶
- 送信前確認と添付ファイルダウンロードリンク化　2つの機能で誤送信抑制
- 管理者負担が少ないOutlookアドイン型でセキュリティ統制を実現

MailConvert on Cloud で対策！ P.7 ▶
- 宛先により、ZIP暗号化かダウンロードリンク化の選択が可能
- フィルタリングやアーカイブと組み合わせてさらに強固なセキュリティ対策

MailFilter／MailArchive で対策！ P.6、P.8 ▶
- 上長承認/自己査閲/遅延配送など送信制御で誤送信、情報持ち出し防止
- アーカイブによる有事対応や事後監査で漏えい抑制

GUARDIANWALL

MailArchive

クラウド　オンプレミス

- メールデータの保管
- アーカイブデータの検索
- 統計情報などのレポート
- メール一括ダウンロード
- ジャーナル形式対応

Microsoft 365などさまざまな環境のメール保管に対応します。
手軽に導入し、柔軟な監査機能でしっかりとメール利用を管理できます。

わかりやすい検索画面

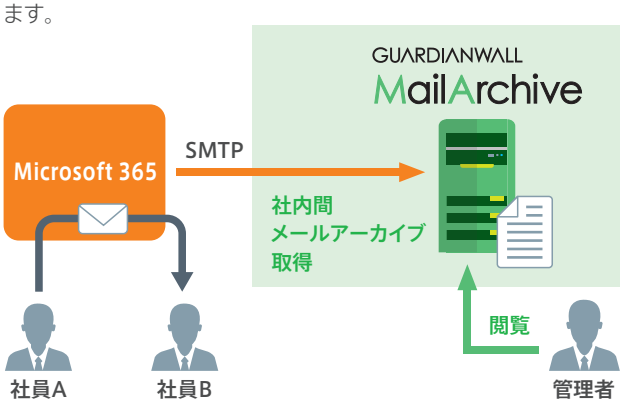
添付も含めて保存し、わかりやすい画面で簡単に検索できます。

検索条件

- 期間（任意期間、時間）
- ヘッダーアドレス
- エンベロープアドレス
- 件名
- 本文／添付ファイル内テキスト
- メールサイズ
- 添付ファイルの有無

Microsoft 365との連携

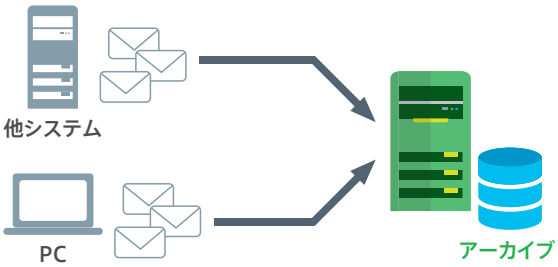
ジャーナル形式に対応し、配送経路上でなくても手軽に導入できます。



※POP3とSMTPに対応

過去のメールデータも一元管理

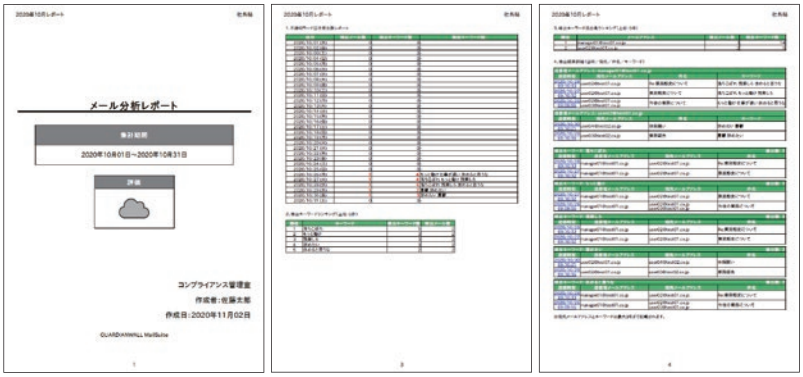
他のアーカイブ製品からの乗り換え時も安心なemlファイルの取り込みツールを標準搭載しています。※オンプレミスのみ



スレッド表示で監査業務を効率化

監査しているメールの、前後にやり取りされた関連メールをワンクリックでスレッド表示が可能です。また同一件名のメールも表示でき、効率的に内容を把握することができます。

メール分析レポートで新しい働き方を支援



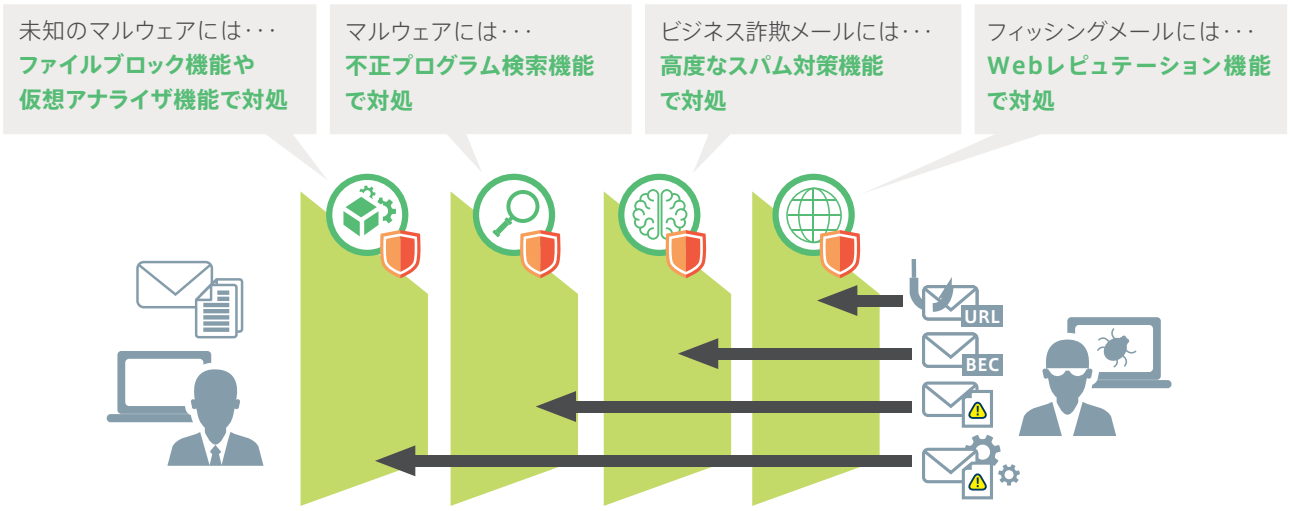
メールのやり取りから、ある特定のキーワードが含まれるメールを業務上不適切なメールとして検出し、レポート形式で自動出力します。
この機能により、「誰が」「誰宛に」「いつ」「どんな」メールのやり取りをしているのかを見える化できるので、故意の情報漏えい、流出や各種ハラスメントの発生を抑制します。
また、コミュニケーション機会の減少や手段の変化により発生する「困りごと」を把握し、業務効率化を支援します。

Inbound Security for Microsoft 365

高度なスパムメール対策
不正プログラム検索
Webレピュテーション
サンドボックス
（仮想アナライザ）

クラウド

Microsoft 365のセキュリティ機能を強化するクラウドサービスです。
メールだけでなくストレージも保護が可能で、オンラインストレージへ危険なファイルを
アップロードしてしまった場合でも、隔離や削除などで感染の拡大を防ぎます。



Inbound Security for Microsoft 365は以下のサービスに対応しています。

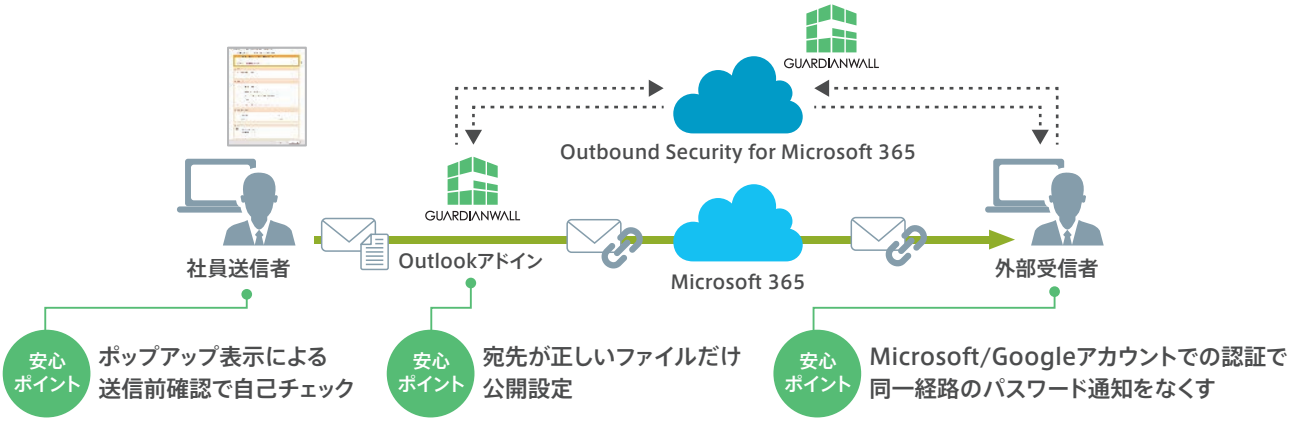
●Microsoft Exchange Online／Microsoft SharePoint Online／Microsoft OneDrive for Business／Microsoft Teams
●Box　●Dropbox　●Google Workspace（Googleドライブ／Gmail）

Outbound Security for Microsoft 365

添付ファイル自動分離・
ダウンロードリンク化
送信後ファイル公開設定
送信前確認

クラウド

Microsoft 365のメール機能をご利用の方向けの誤送信対策サービスです。
Microsoft 365のアドイン配布（Outlookアドイン）の仕組みでご提供し、PPAP（パスワード付きZIP暗号化
ファイルの添付・送信）問題を解決する「添付ファイルのダウンロードリンク化」機能を手軽かつ簡単に実現できます。

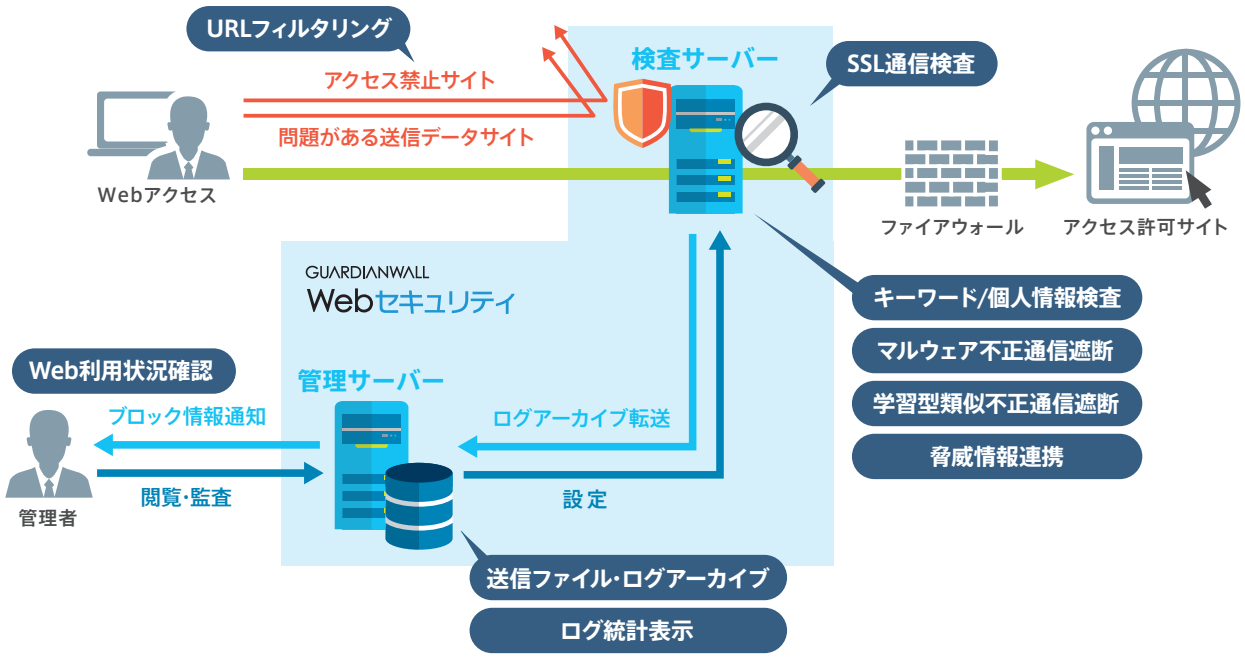


3つの安心ポイントでメールや添付ファイルの誤送信・情報漏えいを防止！
「Outlookアドイン型」でメール経路に影響しない対策を実現！

GUARDIANWALL

Webセキュリティ・オンプレミス WebFilter

URLフィルタリングや外部送信データの検査に加え、
多層型の外部攻撃対策機能により、Web利用からの情報漏えいを防ぎます。



業務に支障を来さない柔軟なポリシー設定

規制をかけたいWebアクセスだけを柔軟なポリシー設定により制御可能です。

誰が	いつ	どこに対する	どのような通信を	どう処理する
ユーザー認証名 IPアドレス User-Agent	時間 曜日	Webカテゴリー URL／IPアドレス	メソッド（POST／GET／HEAD／WebDAV） ファイル形式 キーワード パスワード有無 など	中継 警告 禁止 リダイレクト など

● 豊富なフィルタリングアクション

指定条件に合致したWebアクセスをどう処理するか、豊富な処理パターンから選択できます。

中継	通信をそのまま流します。
試行	通信はそのまま流しますが、ルールにマッチするアクセスがあったことをログに記録します。
	警告メッセージを表示し、ユーザーに注意を促した後、通信を中継します。
禁止	禁止メッセージを表示し、Web閲覧や情報送信をブロックします。
リダイレクト	通信を中継せずに、設定したURLへリダイレクトします。
オーバーライド	オーバーライドコードを入力すると、通信を一時的に中継します。

● 仮想アプライアンス版にも対応

手軽に導入が可能な仮想アプライアンス版もラインアップ。
お客さまの環境に合わせて選択できます。

Linux　仮想アプライアンス

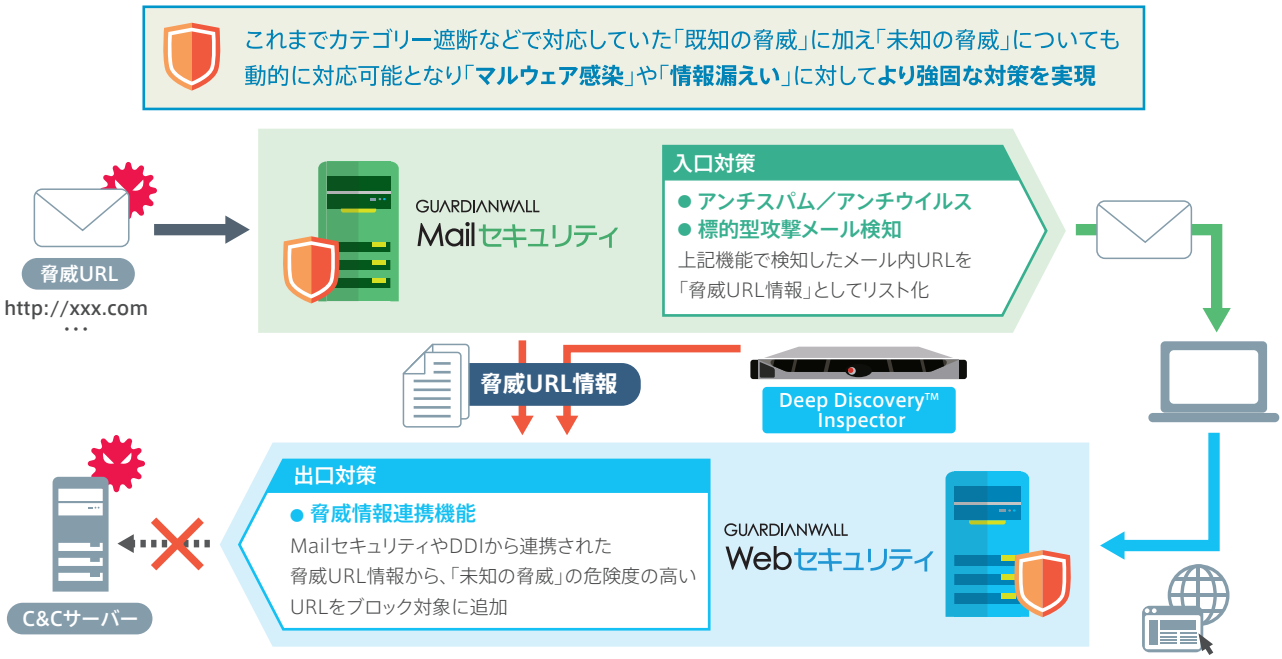
● 個人情報検査 特許取得済
（マイナンバー対応・改正個人情報保護法に対応）

通常のキーワード検査では発見が難しい個人情報も当社独自技術で検知しブロックできます。
マイナンバーもチェックデジットを検査することで正確な検出が可能です。

標的型攻撃への対応

● 脅威情報連携

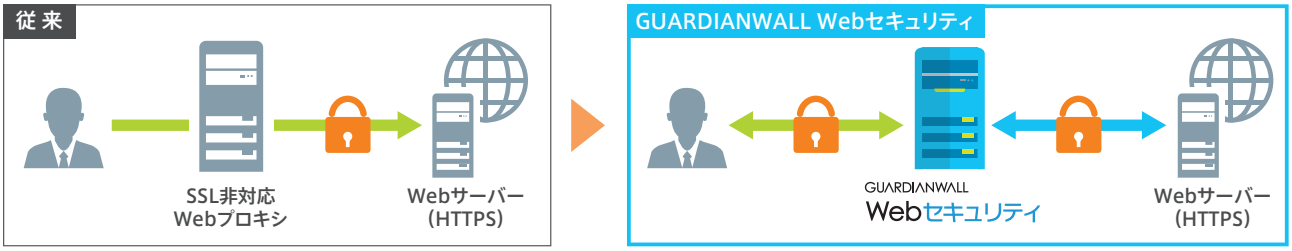
GUARDIANWALL Mailセキュリティおよび、トレンドマイクロ株式会社のDeep Discovery Inspector(DDI)と連携し、標的型攻撃メールなどに含まれる「脅威URL情報」を受け取ります。
受け取った「脅威URL情報」から「未知の脅威」の可能性が高いURLをブロック対象のリストに登録し、接続を禁止します。



※本連携機能は、GUARDIANWALL MailFilter／MailSuite、もしくはトレンドマイクロ社Deep Discovery Inspectorとの併用が必要です。

● SSL通信の検査に対応

通信内容が暗号化されるHTTPSサイトが急速に増えてきています。GUARDIANWALL WebセキュリティはSSLデコード機能を標準搭載し、すべてのWeb通信の内容を検査することが可能です。



● マルウェアの不正通信をブロック

標的型攻撃では、侵入したマルウェアとC&Cサーバーとの間で、プログラムの拡張や入手した顧客情報の送信など断続的な通信が発生します。「コネクトバック通信検知機能」は、長時間にわたる特定サーバーとの通信の検知と自動遮断が可能です。
また、独自解析技術によりマルウェア感染端末特有の不正通信を検知し、自動遮断することができます。さらに、不正通信履歴から自動学習して類似する通信も検知し、新たに感染した別端末からの不正通信を遮断して被害の拡大を阻止します。

ご利用環境

Mailセキュリティ・クラウド

MailFilter on Cloud ／ MailConvert on Cloud ／ MailArchive on Cloud

メール環境	Microsoft 365またはGoogle Workspaceでのメール環境で、独自ドメインご利用が前提となります。
メール経路	メール経路に弊社サーバーを経由することが前提となります。
DNS	ご利用サービスにより、送信系はSPFレコード、受信系はMXレコードなどのDNS設定が必要な場合があります。
メール送受信のサイズ	25MB/通　※メール送信、受信ともに
管理画面対応ブラウザ	PC：Internet Explorer 11／Google Chrome／Microsoft Edge スマートデバイス：Safari(iOS)／Chrome(Android)　※スマートデバイスでは、保留メールおよび遅延配送メールの操作画面を表示できます。

※その他、ご利用における制限事項および注意事項につきましては、各サービスの説明資料をご確認ください。

Mailセキュリティ・オンプレミス

Linux版

OS	Red Hat Enterprise Linux※1　6.6／6.7／6.8／6.9／6.10／7.3／7.4／7.5／7.6／7.7／7.8／7.9／8.3※2／8.4※2 CentOS※1　6.6／6.7／6.8／6.9／6.10／7.3／7.4／7.5／7.6／7.7／7.8／7.9／8.3※2 Kernel　2.6.32-504／2.6.32-573／2.6.32-642／2.6.32-696／2.6.32-754／3.10.0-514／3.10.0-693／3.10.0-862／3.10.0.957／3.10.0-1062／3.10.0-1127／3.10.0-1160／4.18.0-240※2／4.18.0-305※2 ※1 64bit版のみ対応 ※2 GUARDIANWALL Mailセキュリティ製品の冗長化機能は利用できません。
CPU	インテル64bit・マイクロプロセッサー(Itanium 2は非対応) 1.0GHz／2コア以上(推奨：2.0GHz　4コア以上)
メモリー	8GB以上(推奨：12GB以上)
仮想環境	VMwareやMicrosoft Hyper-Vなどで、上記OSをサポートしている環境
IaaS環境	Amazon Web Services(AWS)／Microsoft Azure ※ GUARDIANWALL Mailセキュリティ製品の冗長化機能は利用できません。

※推奨は1台あたりメール流量約20万通／日で、アーカイブやフィルタリング、メール変換すべての機能の利用を想定した場合のシステム要件です。保留メール操作や全文検索などの管理画面操作も考慮しています。
※マシンスペックは実際のメール流量や管理画面へのアクセス頻度などにより変更してください。

仮想アプライアンス版

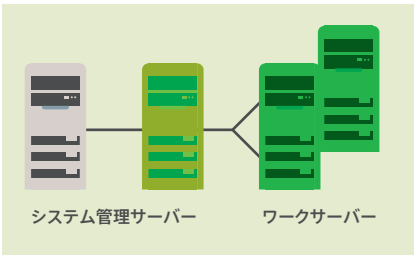
OS	VMware ESXi 6.0／6.5／6.7 Microsoft Hyper-V(Microsoft Windows Server 2012 R2／2016)
リソース	仮想CPU数：2コア以上、メモリー12GB以上

※上記スペックは、仮想マシンのリソースになります。　※ディスク容量はデプロイ後の設定で拡張することができます。
※仮想アプライアンス版は、シングル構成のみのサポートとなっております。

1台構成例

●メール流量(平均100KB)：20万/日、程度
●冗長性なし

4台構成例（冗長構成）



●メール流量(平均100KB)：40万/日、程度
●冗長性あり(サービス、データ)

ユーザー数	CPU	メモリー	ハードディスク
500名以下	クワッドコア2.0GHz×1以上	8GB	200GB/アーカイブ1ヵ月想定
1,000名以下		12GB	400GB/アーカイブ1ヵ月想定
1,500名以下		16GB	600GB/アーカイブ1ヵ月想定

※CPUおよびメモリーは、メール流量 20万通(平均サイズ100KB/通)を想定。
※ハードディスクサイズは、500名で、1日に2万5千通(平均サイズ100KB/通)を想定。
※1,500名を超える規模のサイジングにつきましてはお問い合わせください。

Webセキュリティ・オンプレミス

Linux版

OS	Red Hat Enterprise Linux 7 / 8(64bit) CentOS 7 / 8(64bit)
IaaS環境	Amazon Web Services(AWS)／Microsoft Azure

仮想アプライアンス版

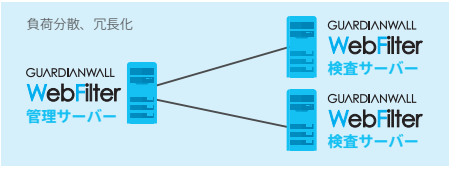
OS	VMware ESXi 6.0／6.5／6.7 Microsoft Hyper-V(Microsoft Windows Server 2012R2／2016)
リソース	仮想CPU数：2コア以上、メモリー4GB以上

※上記スペックは、仮想マシンのリソースになります。
※ディスク容量はデプロイ後の設定で拡張することができます。
※仮想アプライアンス版は、シングル構成のみのサポートとなっております。

オンプレミス構成例(Linux版)※仮想アプライアンス版はシングル構成のみ

1台構成

検査サーバー複数台構成



ユーザー数	CPU	メモリー	ハードディスク
500名以下	クワッドコア2.0GHz×1以上	5GB以上	400GB以上
1,000名以下			700GB以上
1,500名以下			1.0TB以上

※1,500名を超える規模のサイジングにつきましてはお問い合わせください。
● ログの保存期間は180日を想定しております。　● 1名あたりのWebアクセスは1日あたり1,000件を想定しています。
● SSL通信の比率は2割を想定しています。　● アクセスログの検索に関する注意点として、Webアクセスが集中している、もしくは、検索対象のアクセスログのデータ量が多い状況では、タイムアウトが発生し検索結果が閲覧できない場合があります。その場合、検索範囲の絞り込みや、ハードウェアスペックの強化を行ってください。

製品に関する情報はこちらでご確認いただけます。

セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南 2-16-6 CANON S TOWER

2022年4月現在
GW22040500HOK-663