

PPAP問題を解説！

GUARDIANWALLが提案する安全なファイル送付手段とは？

キヤノンマーケティングジャパン株式会社  
橋田 拓弥

Canon

# PPAPとは

メールの添付ファイルをパスワード付きZIPファイルとして宛先に送付するファイル共有の手段

P

assword付き  
ZIPファイルを送付

P

asswordを送付

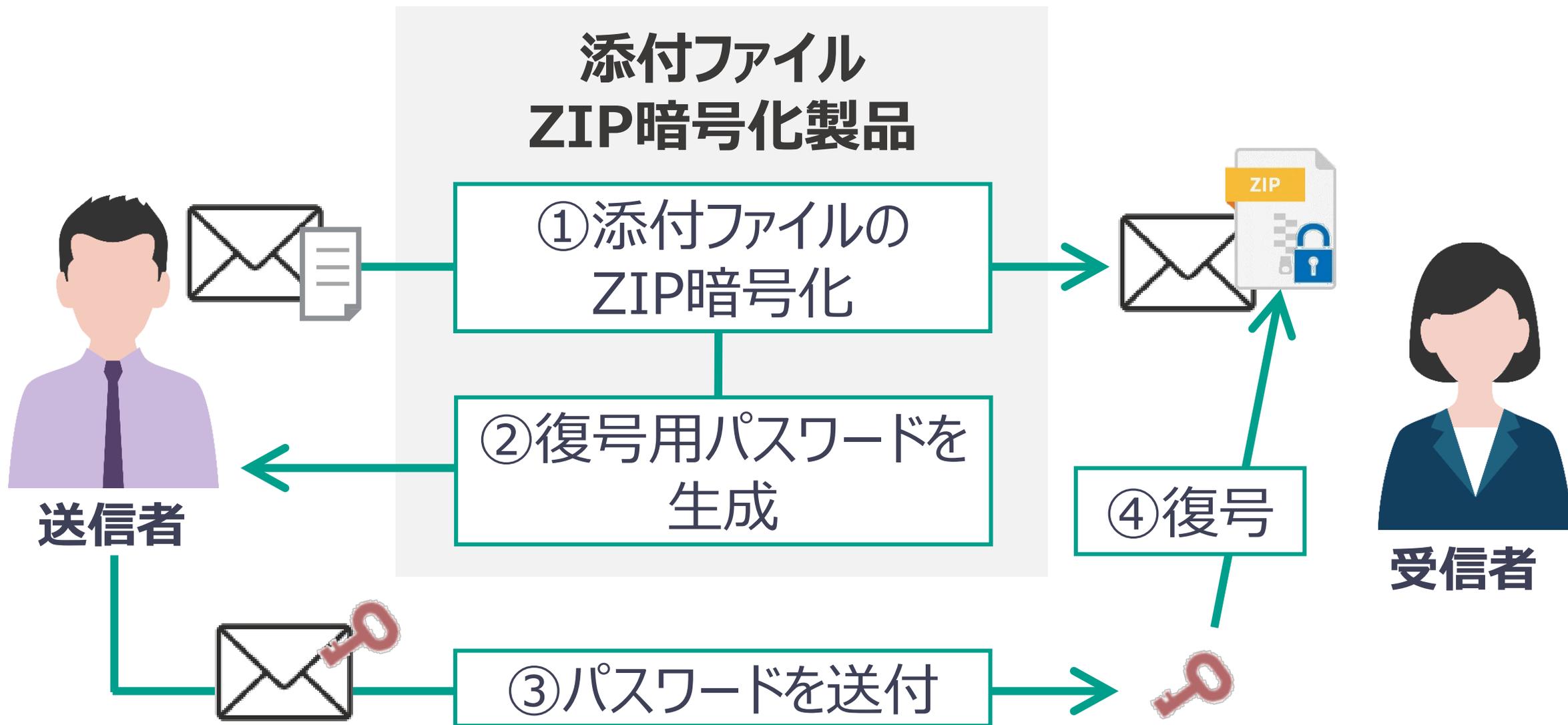
A

ん号化(暗号化)

P

rotocol

# PPAPのよくある運用方法



## ■ パスワード付きZIPファイル（PPAP）の廃止

平井卓也デジタル改革担当相は2020年11月17日の定例会見で、中央省庁の職員が文書などのデータを**メールで送信する際に使うパスワード付きzipファイルを廃止**する方針であると明らかにした

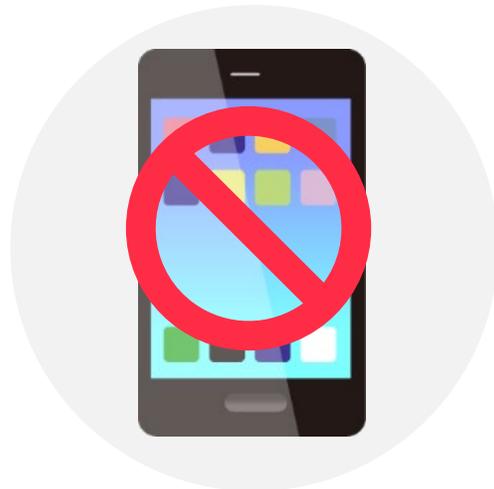
※政府の意見募集サイト「**デジタル改革アイデアボックス**」  
の意見を採用

# PPAPの問題点



ファイルの暗号化・複合化  
パスワードの管理

作業負荷増大



端末によっては  
ZIPファイルの展開が不可

利便性がない



メールを盗聴されると  
パスワードも盗聴される

盗聴のリスク



パスワード付きZIPファイルは  
ウイルスチェックが難しい

マルウェア攻撃への悪用

# PPAPの代替策について

	添付ファイル ZIP暗号化 (PPAP)	添付ファイルの ダウンロード リンク化	ファイル交換 サービス	オンライン ストレージ
特徴	メールの 添付ファイルを 暗号化して送付 パスワードは 別メールにて送付	メールの 添付ファイルを 分離し ダウンロードサーバー へアップロード	ファイルを クラウドストレージに 一時保存し あとからダウンロード	クラウド上の ストレージに 専用IDでログインし ファイルを共有
相性の良い 利用シーン	不特定とのやり取り	不特定とのやり取り	大容量ファイルの やり取り	特定メンバーとの やり取り
ファイルの 受取拒否	△	△	△	△

**企業によってファイル共有のポリシーが異なる**

# PPAPの代替策について

	添付ファイル ZIP暗号化 (PPAP)	添付ファイルの ダウンロード リンク化	ファイル交換 サービス	オンライン ストレージ
大容量 ファイル	△ メーラー側の制限	△ メーラー側の制限	○	○
交換の 容易性	○ メールに添付	○ メールに添付	○ Webでアップロード	△ 権限設定の手間
送信履歴の 確認	○ メールに添付	○ メールに添付	△ メールと別の仕組み	△ メールと別の仕組み
誤送信 対策	○	○	△	△
運用統制	○	○	△ 利用者任せ	△ 利用者任せ



**PPAPのメリットそのまま**

# GUARDIANWALL メールセキュリティ 製品ラインナップ

## 内部脅威対策

GUARDIANWALL

Mailセキュリティ・クラウド

ベーシック

プレミアム

MailFilter

情報漏えい（誤送信）を  
未然に防ぐ

MailConvert

情報漏えい（誤送信）の  
被害を低減する

MailArchive

情報漏えい（誤送信）を  
調べて特定する

## 外部脅威対策

Inbound Security for Microsoft 365

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

# MailConvert on Cloud プレミアム が機能拡張しました！

MailConvert on Cloud **プレミアム**

メールの利便性



安全なファイル共有



# 新機能：添付ファイルのダウンロードリンク化

Step1. 添付ファイル付きメールを送信！



Step2. 添付ファイルを分離！



Step3. 本文にダウンロードリンクを追加！



Step4. リンクからファイルをダウンロード！



## 新機能：5つのポイント



①メールと一緒にファイル共有が可能



②誤送信対策として機能



③ソーシャル認証に対応



④全社レベルでの一括管理



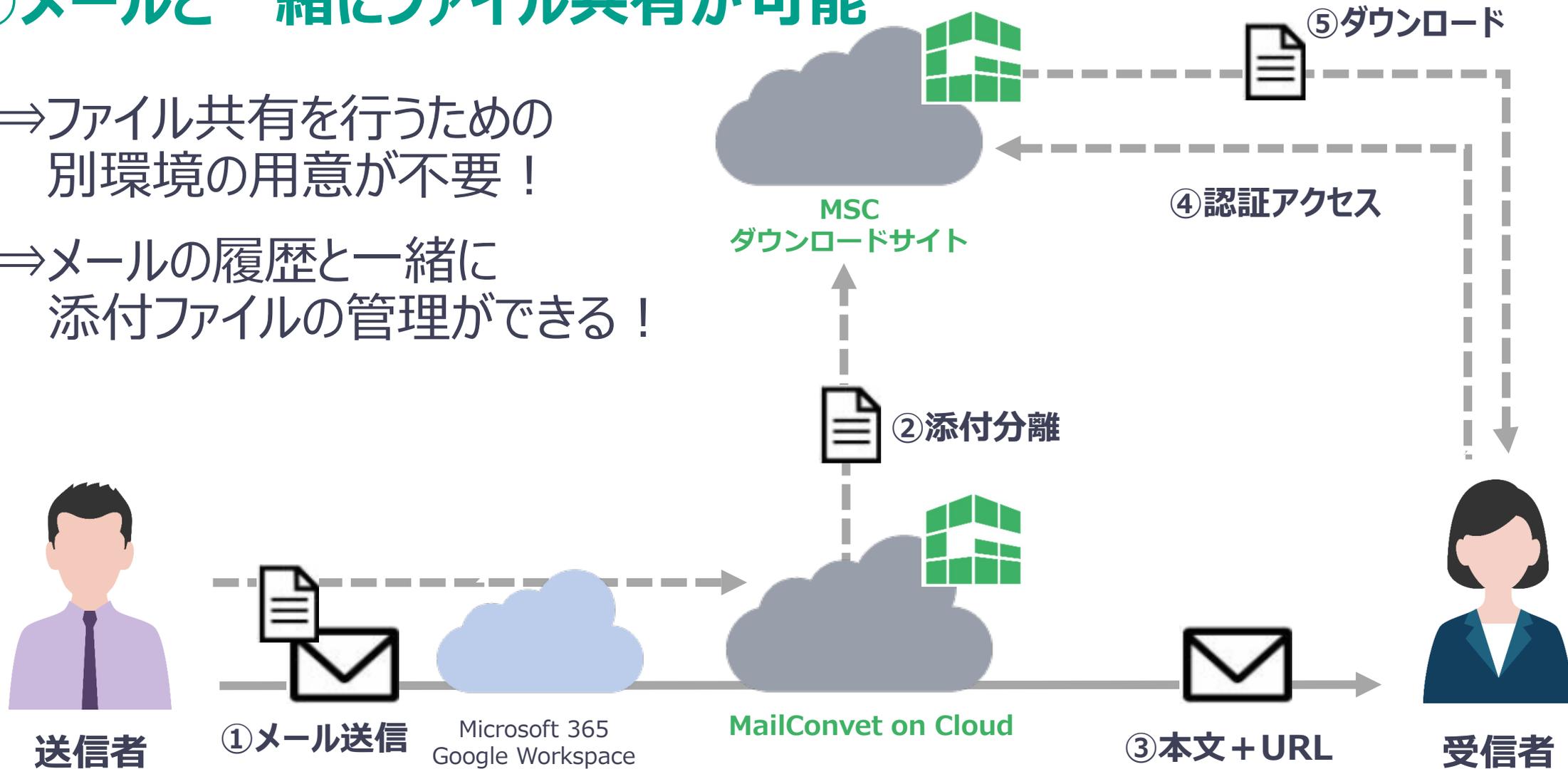
⑤得意先に合わせたファイル共有ポリシー

# 概要図（送信経路）

## 💡 ①メールと一緒にファイル共有が可能

⇒ファイル共有を行うための別環境の用意が不要！

⇒メールの履歴と一緒に添付ファイルの管理ができる！



# 送信者 操作イメージ

あなたが送信したメールの添付ファイルはリンク変換されました。  
ファイル公開設定を以下より確認してください。  
設定を変更する場合は2021/06/26までに実施するようお願い致します。

[http://\[redacted\]/test01/url\\_link\\_convert/publishing\\_settings/sAZd427bfmGxfH7yDDGinD5jfmGmiOuT80uT8BIRgG0pjmfSfYfm0jfm0jfsfjfm0j61ARAW7xrD0](http://[redacted]/test01/url_link_convert/publishing_settings/sAZd427bfmGxfH7yDDGinD5jfmGmiOuT80uT8BIRgG0pjmfSfYfm0jfm0jfsfjfm0j61ARAW7xrD0)

----- URLリンク変換された宛先(RCPT TO:) -----  
(user01@test01.co.jp)



通知メール



送信者

GUARDIANWALL

<input type="checkbox"/>	ファイル名	ダウンロード履歴		
<input checked="" type="checkbox"/>	<a href="#">header_tenant.jpeg</a>	2021-06-03 09:35:14	user02@test01.co.jp	
		2021-06-01 11:21:13	user02@test01.co.jp	
		2021-06-01 11:13:35	user05@test01.co.jp	
		2021-05-26 13:21:50	user02@test01.co.jp	
		2021-05-26 13:21:36	user04@test01.co.jp	
<input type="checkbox"/>	<a href="#">sample.txt</a>	無し		
<input checked="" type="checkbox"/>	<a href="#">てすと.txt</a>	2021-06-01 14:31:42	user02@test01.co.jp	

\* 必須

更新



## ② 誤送信対策として機能

- ⇒メールアドレス単位であとから公開範囲を設定！
- ⇒万一の誤送信時はあとからファイルの削除！

# 受信者 操作イメージ



## ③ ソーシャル認証に対応

※外部サービスのログイン情報を利用して認証を行うこと

⇒受信者のアカウント情報で  
セキュアにファイルダウンロード！

⇒ワンタイムパスワードでの  
ファイルダウンロードにも対応！

本メールの添付ファイルはダウンロードサイトにアップロードされました。  
添付ファイルをダウンロードするには以下のURLをクリックしてください。  
[http://\[redacted\]/mails/844ff92ddb954b869bf77b492287698d/](http://[redacted]/mails/844ff92ddb954b869bf77b492287698d/)  
(ダウンロード期限 2021/06/22)



本文 + URL

GUARDIANWALL



受信者

GUARDIANWALL

添付ファイルダウンロードURLを受信したメールアドレスまたはアカウントでログインしてください。

メールアドレス:

ワンタイムパスワード取得

または

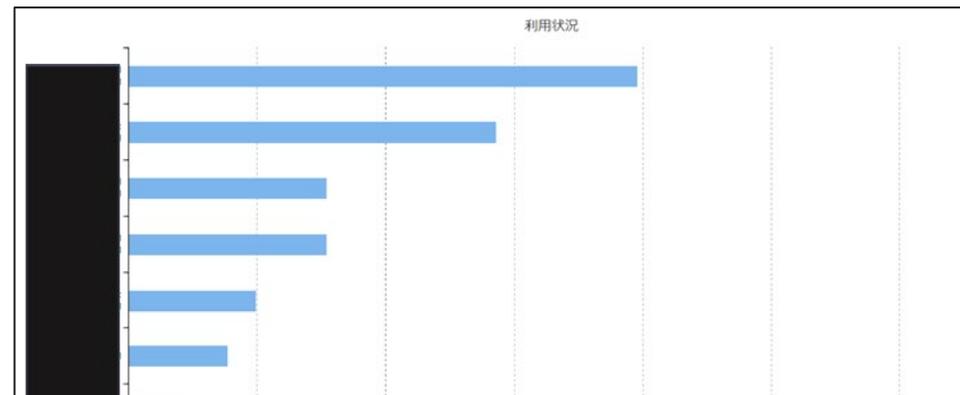
 Microsoft アカウントでログイン

 Google アカウントでログイン

© Canon Marketing Japan Inc. 2020

# 管理者 操作イメージ

添付ファイルダウンロードリンク化  
設定画面



利用状況  
レポート画面



## ④ 全社レベルでの一括管理

⇒クラウド型ゲートウェイ製品のため  
管理者側で一元管理！

⇒社内の組織に合わせて  
運用方法を変更することも！



# 管理者 操作イメージ



管理者

行:3	ID: <input type="text" value="1"/>
<b>ポリシー設定画面</b>	
宛先条件	<input type="text" value="*"/>
数値条件	<input type="text" value="ATTACHMENT(nopasswordlock, all)&gt;=1"/>
暗号化方式: <input type="text" value="ZipCrypto"/>	
適用動作	<input type="checkbox"/> 添付ファイルのダウンロードリンク化
	<input checked="" type="checkbox"/> 添付ファイルのダウンロードリンク化
	<input type="checkbox"/> 添付ファイル暗号化
<input checked="" type="checkbox"/> 更新	

## 💡 ⑤ 得意先に合わせた ファイル共有ポリシー

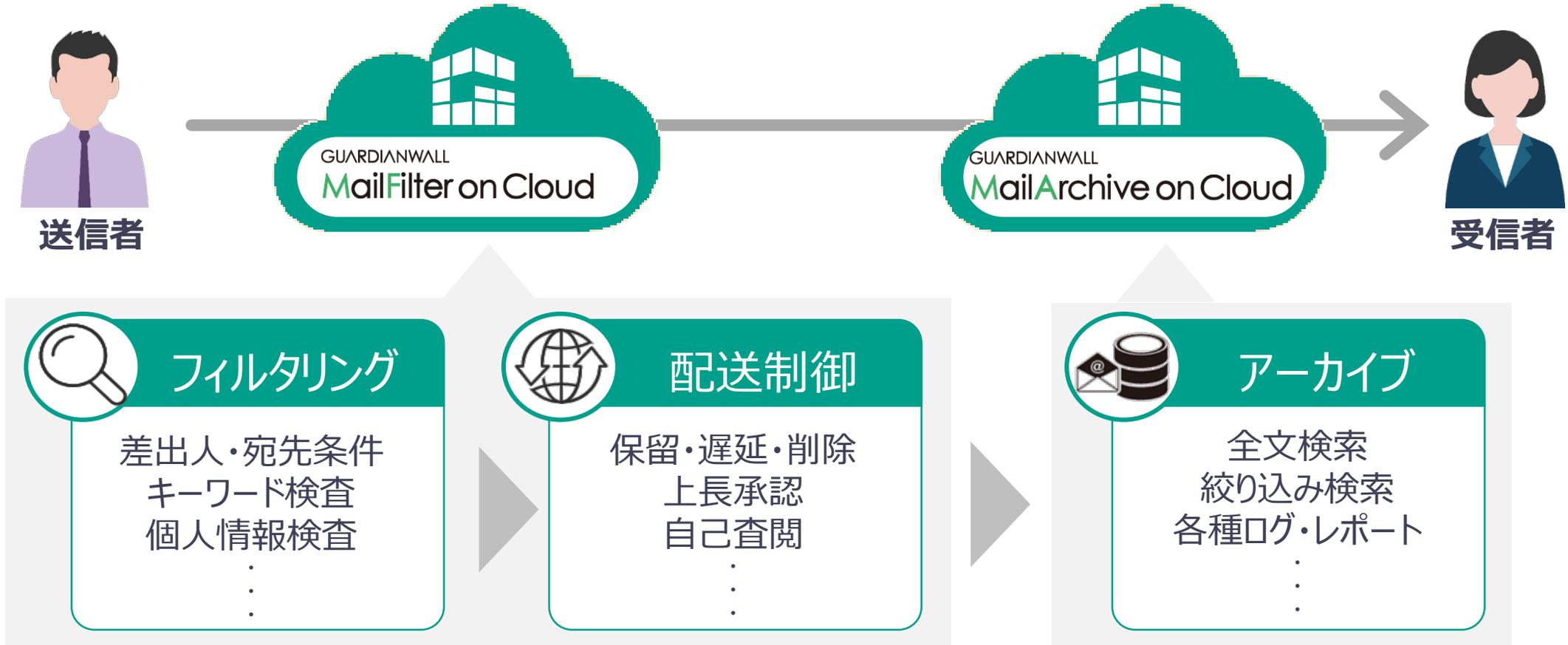
⇒得意先のポリシーに合わせて  
URL化/ZIP暗号化/変換なしの  
選択をすることが可能！



さらに・・・



# 他のMailセキュリティ・クラウドとの組み合わせが可能！



# GWで実現できるメール環境イメージ

GUARDIANWALL

Mailセキュリティ・クラウド

添付ファイル付きメールや  
特定のキーワードが入ったメールは  
送信者が自己監査



送信者



住所/電話番号/  
クレジットカード番号などの  
個人情報が入っているメールは  
上長があとから承認



上長



本文+URL



受信者に合わせて  
添付ファイルを変換



受信者

社内宛・社外宛メールを  
全てアーカイブ保存  
必要に応じて  
メールの検索・事後監査

# Mailセキュリティ・クラウド 製品ラインナップ

GUARDIANWALL

## Mailセキュリティ・クラウド

### MailFilter

情報漏えい（誤送信）を  
**未然に防ぐ**

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

### MailConvert

情報漏えい（誤送信）の  
**被害を低減する**

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

### MailArchive

情報漏えい（誤送信）を  
**調べて特定する**

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

**総合的なメール情報漏えい対策を提供**

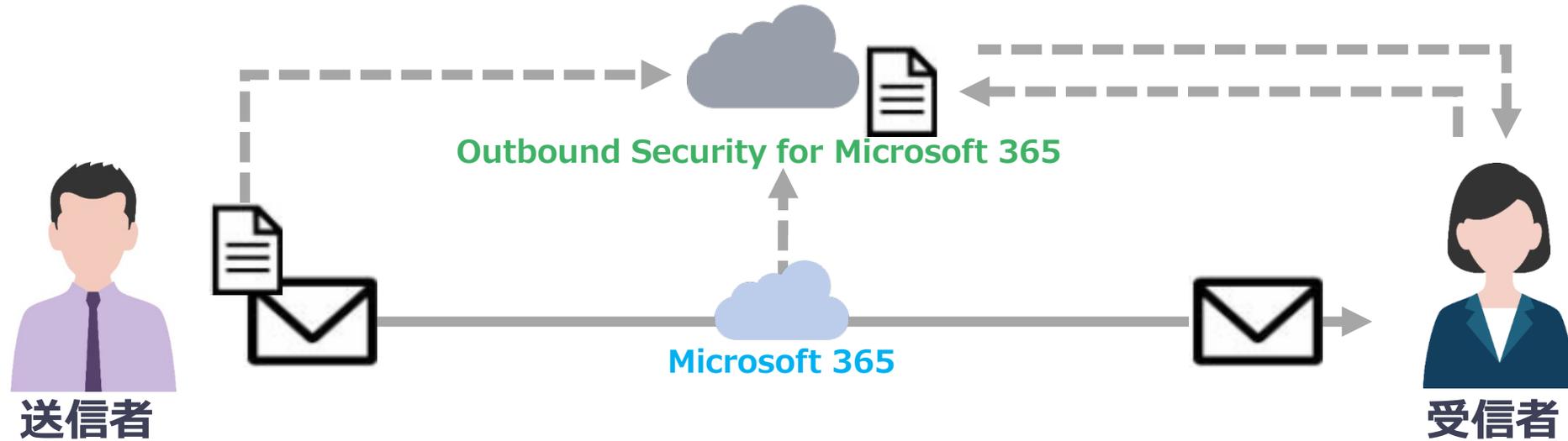
他にも…

10月  
リリース予定

# 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

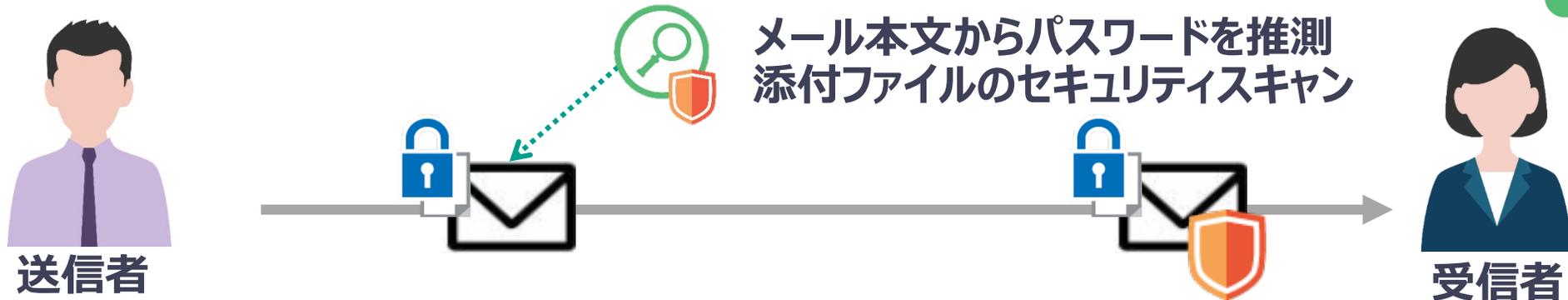
送信後ファイル公開設定  
送信前確認



# 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)



# 本日のまとめ

- PPAP対策としての代替策はいくつか手段があり

それぞれ**特徴や相性の良いシーンが異なる！**

- GUARDIANWALLではMailセキュリティ・クラウドの機能拡張にて

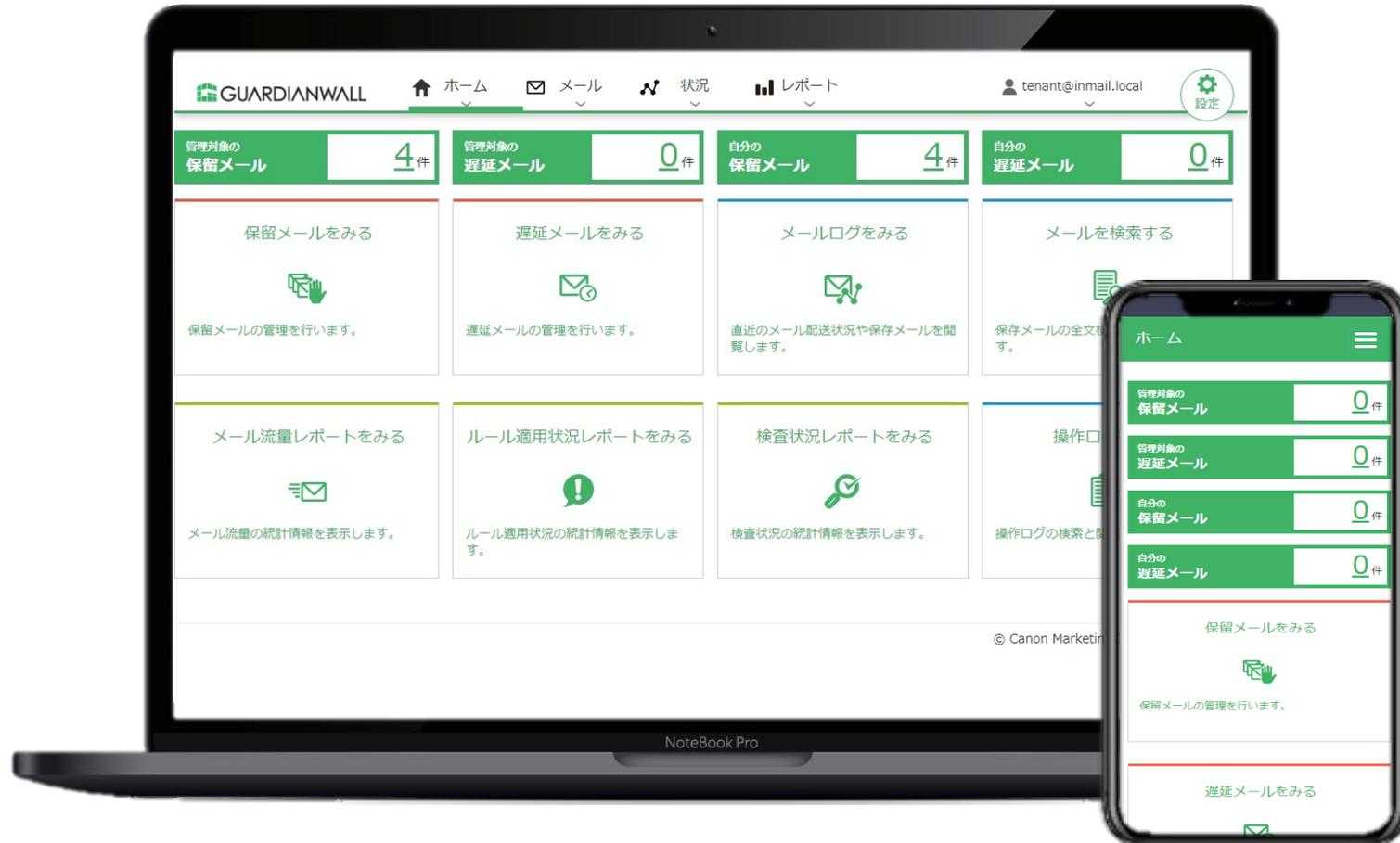
バランスの取れた**添付ファイルの自動URL化を提供！**

- Mailセキュリティ・クラウド シリーズにて

**総合的なメール情報漏えい対策を実現！**



# 最適なソリューションでメールセキュリティの「しんか」を Mailセキュリティ・クラウド



# 無償お試しサービス

## 内部脅威対策

### MSC

「Mailセキュリティクラウド」



GUARDIANWALLの**30日間の無償評価**であなたの会社にあった対策を試してみませんか?

2022年最新のサイバー攻撃による個人情報漏えい等の本人通知が義務化  
よくある誤送信 情報漏えいインシデント発生で迷惑メール再発防止  
働き方改革のセキュリティ対策強化要請

Mailセキュリティクラウドで対策の最適解を見つけませんか!

**1 誤送信の心理抑制**

- 社外メールは自動的に上司にCCする
- 添付ファイルがあるメールは上司に転送する
- アーカイブ・ログをとり、不適切なメールを検知する

**2 社内ポリシーを遵守させる**

- 容量の大きいメールは止める
- フリーメール宛のメールは止める
- 就業時間外のメールにフラグを立てる
- ユーザー自分で添付ファイルの暗号化させない

**3 監査してミスに備える**

- 社外宛メールは上層承認後に送出手続き
- 宛先が複数社ある場合は、メールを止める
- 個人情報の有無を検査し、個人情報を含む場合はメールを止める

利用者の負担を少なく、効果ある対策は? 本来に対策効果があるのか不安な方も...

まずは**30日間の無償評価**をオススメします

## 外部脅威対策

### IS365

「Inbound Security for Microsoft 365」

無償診断  
レポートつき

貴方のMicrosoft Office 365は大丈夫?  
**Office 365 無償健康診断**  
Inbound Security for Office 365

Office 365を狙ったメール侵入

2017年春に公表された某大手電機会社でのデジタルメール群集、2018年9月の大学で個人情報漏えいを取り止めたクレデンシャルフィッシング、また、いまだに悪影響を及ぼしているランサムウェアなど、悪影響を及ぼすメールでOffice 365を狙った事件が後を絶ちません。

ビジネスメール詐欺  
クレデンシャルフィッシング  
標的型メール攻撃  
ランサムウェア

Office 365

昨年1年間で、Office 365をすもりぬけた高質な脅威を約**340万件以上**検知

GuardianWall Mailセキュリティクラウド

アンチウイルス アンチスパム

Office 365

API連携

SaaS

Inbound Security for Office 365

65,009	通知のマルウェア
2,877,522	通知の不正URLリンク
50,030	通知・未知ランサムウェア
260,205	未知のマルウェア
190,480	フィッシングメール
3,040	ビジネスメール詐欺
合計	3,496,316

ご利用中のOffice 365環境にて「お書き込み自身のリスク実態を把握いただくために」  
**「Office 365 無償健康診断」**でチェック!

以下URLより  
お申し込みください

<https://forum1.canon.jp/public/application/add/1575>

# お問合せ窓口

キヤノンマーケティングジャパン

◆GUARDIANWALLシリーズ問合せ窓口  
[guardian-info@canon-mj.co.jp](mailto:guardian-info@canon-mj.co.jp)

デジタルセキュリティで  
お客さまのビジネス変革を支える

**Canon**

[canon.jp/it-sec](https://canon.jp/it-sec)