高度な配信の設定方法(Microsoft 365のプランによって利用できない場合があります。)

●管理者アカウントにて、Exchange 管理センター: Microsoft Defender (https://security.microsoft.com/homepage) にサインインします。

①「ポリシーとルール」-「脅威ポリシー」をクリックください。

Micros	soft Defender	▶ 桃奈
=		
G #−4		ポリシーとルール
① インシデン	トとアラート ~	デバイスの管理、骨ェリケの保護、組織内のさまざまなアクティビティに関するアラートの受信を行うポリシーを設定します。詳細情報
⑦ アクション	と報告 ~	3 毎のアイラム
合 育成インう	デリジェンス 〜	名前 ~
	137	各成点()/
咨 試用版		75-1-102-
12 x-1123	ラボレーション ヘ	アクティビティのアラート
目 確認		
Exchange	e メッセージの追跡	
毒 ポリシーと	16-16	
ビルホ		
1 型 型 型 型 型 型 型 型 型 型 型 型 型 型 型 型 型 型 型		
♡ 正常性		
③ アクセス計	可	
© RE		

②高度な配信をクリックください。

iii Microsof	t Defender		,○ 検索	<i>\$</i> @ ?
=		テンプレー	ート化されたポリシー	
		A B	既定のセキュリティポリシー	推奨される保護テンプレートを使用してすべてのポリシーを一座に適用することによって、保護を簡単に構成できます
① インシデントと	アラート 〜	bô	構成アナライザー	現在のポリシー構成の問題を特定して、セキュリティを強化します
③ アクションと新	告 ~			
(注) 骨成インテリ:	¹ 177 ~	ボリシー		
😨 🛛 セキュア スコフ	7	3	フィッシング対策	フィッシング攻撃からユーザーを保護し、不要なメッセージの安全性のヒントを構成します。
谷 試用版		2	スパム対策	組織のメールを送越メールから保護します。これには、送越メールが快出された場合の対処法も含まれます
ビコ メールとコラボ	V-937 ^	۲à	マルウェア対策	組織のメールをマルフェアから保護します。これには、マルフェアが検出された場合の対処法と通知先の設定も含まれます
E 確認				
🕼 Exchange 🖇	ッセージの追跡	ルール		
幸 ポリシーとルー	JL	Θ	テナント許可/禁止リスト	組織の許可または狭止 エントリを管理します。
		9	メールの認証の設定	組織内での原証源み受信チェーン (ARC) と DKIM の設定。
		9 1	高度な配信	特殊なシステムのユース ケースによるオーバーライドを管理します。
		2	拡張フィルタリング	ドメインの MX レコードでメールが祭初に Exchange Online Protection (EOP) にルーティングされない場合に、EOP スキャンが正しく機能するように構成しま
♥ 止寒性		51	検疫ポリシー	既定の他疫がリシーを使用するか、独自のポリシーを作成して、機疫済みのメッセージにカスタム ルールを適用します
~ アリセス計可				

③高度な配信画面のフィッシングのシミュレーションを クリックください。



④訓練用ドメインとKIS MailMonのIPアドレスを入力後に保存を クリックください。





