# Email Security R2 あんしんプラス　デフォルトポリシー
# 【受信保護設定】

**ドメイン毎に生成されるデフォルトポリシールール**

| ポリシー | ウイルスポリシー | スパムメールポリシー |
|---|---|---|
| 名前 | Virus | Spam or Phish |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | 【検出タイプを指定 (最低1つ):】<br>☑駆除可能な不正プログラムまたは不正プログラムコード<br>☑マスメーリング型の駆除不能なウイルスまたは不正プログラムコード<br>☑マスメーリング型ではない駆除不能なウイルスまたは不正プログラムコード<br><br>【機械学習型検索の指定:】<br>[2022年5月以前]<br>なし<br><br>[2022年5月以降]<br>☑機械学習型検索を有効にする<br>☑検出機能向上のため不審ファイルをトレンドマイクロに送信する<br><br>【高度な設定の指定:】<br>☑仮想アナライザに不審ファイルを送信する<br>低 (最も控えめ)<br>☑マクロ、JSEおよびVBE検索を含める | ☑スパムメール<br>レベル: 中低<br>☑ビジネスメール詐欺 (BEC)<br>このルールを次の場合に適用:<br>●スパムメール対策エンジンでBEC攻撃として検出<br>☑フィッシングおよびその他の不審なコンテンツ<br>☑グレーメール<br>グレーメールのカテゴリ<br>☑マーケティングメッセージとニュースレター<br>☑Webレピュテーション<br>☑ソーシャルエンジニアリング攻撃 |
| 処理 | インターセプト：隔離<br>変更：なし<br>監視：なし | インターセプト：隔離<br>変更：なし<br>監視：なし |
| 備考 | | |

| ポリシー | スパムメールポリシー | スパムメールポリシー |
|---|---|---|
| 名前 | Newsletter or spam-like | Probable BEC threat |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | ☑スパムメール<br>レベル: 中高<br>☑グレーメール<br>グレーメールのカテゴリ<br>☑マーケティングメッセージとニュースレター<br>☑Webレピュテーション | ☑ビジネスメール詐欺 (BEC)<br>このルールを次の場合に適用:<br>●スパムメール対策エンジンでBEC攻撃の可能性ありと判定 |
| 処理 | インターセプト：メッセージをインターセプトしない<br>変更：件名にタグを挿入 - "spam>"<br>監視：なし | インターセプト：メッセージをインターセプトしない<br>変更：本文にスタンプを挿入- "Probable BEC threat"<br>監視：なし |
| 備考 | | |

| ポリシー | スパムメールポリシー | コンテンツポリシー |
|---|---|---|
| 名前 | Writing style BEC threat | High-risk attachment |
| ステータス | 無効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | ☑ビジネスメール詐欺 (BEC)<br>このルールを次の場合に適用:<br>●ライティングスタイル分析でBEC攻撃として検出 | 条件: いずれかを満たす<br>☑添付ファイルが次の状態　ファイル名または拡張子<br>☑ブロックが推奨されるファイル拡張子<br>☑添付ファイルが次の状態　MIMEコンテントタイプ<br>☑オーディオ<br>☑ビデオ<br>☑添付ファイルが次の状態　実際のファイルタイプ<br>☑実行可能ファイル<br>☑メディア<br>☑添付ファイルのサイズが次に一致する　> 5 MB<br>☑添付ファイルの数が次に一致する　> 20 |
| 処理 | インターセプト：メッセージをインターセプトしない<br>変更：なし<br>監視：通知送信 - ”Writing Style Analysis Violation” | インターセプト：隔離<br>変更：なし<br>監視：なし |
| 備考 | | 特に添付ファイルのサイズ、添付ファイルの数がお客様の要件を満たすか確認してください。 |

| ポリシー | コンテンツポリシー | コンテンツポリシー |
|---|---|---|
| 名前 | Exceeding msg size or # of recipients | Password protected |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | 条件: いずれかを満たす<br>☑メッセージサイズが次に一致する　> 50 MB<br>☑受信者の数　> 50 | 条件: いずれかを満たす<br>☑添付ファイルが次の状態　パスワードで保護されている |
| 処理 | インターセプト：隔離<br>変更：なし<br>監視：通知送信 - "Notification of Exceeding message size" | インターセプト:メッセージをインターセプトしない<br>変更：本文にスタンプを挿入 - "Unscanned Attachment"<br>監視：なし |
| 備考 | 特にメッセージサイズ、受信者の数がお客様の要件を満たすか確認してください。 | |

| ポリシー | 相関インテリジェンスのポリシー | 相関インテリジェンスのポリシー |
|---|---|---|
| 名前 | Organization: Correlated Intelligence Security Risks | Organization: Correlated Intelligence Anomalies |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | 所属する組織 | 所属する組織 |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | 【セキュリティリスク設定の指定:】<br>☑セキュリティリスク | 【異常設定の指定:】<br>☑事前定義された異常<br>●すべての事前定義のルール<br>事前定義された強力な相関ルールを使用して検出<br>☑不審メール<br>☑不要な可能性があるメール<br><br>事前定義された中程度の相関ルールを使用して検出<br>☑不審メール<br>☑不要な可能性があるメール |
| 処理 | インターセプト:メッセージをインターセプトしない<br>変更：なし<br>監視：なし | インターセプト:メッセージをインターセプトしない<br>変更：なし<br>監視：なし |
| 備考 | | |

| ポリシー | 相関インテリジェンスのポリシー | 相関インテリジェンスのポリシー |
|---|---|---|
| 名前 | Correlated Intelligence Security Risks | Correlated Intelligence Anomalies |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | 【セキュリティリスク設定の指定:】<br>☑セキュリティリスク | 【異常設定の指定:】<br>☑事前定義された異常<br>●すべての事前定義のルール<br>事前定義された強力な相関ルールを使用して検出<br>☑不審メール<br>☑不要な可能性があるメール<br><br>事前定義された中程度の相関ルールを使用して検出<br>☑不審メール<br>☑不要な可能性があるメール |
| 処理 | インターセプト：隔離<br>変更：なし<br>監視：なし | インターセプト:メッセージをインターセプトしない<br>変更：件名にタグを挿入 - "Anomaly:"<br>☑デジタル署名の付いたメッセージにはタグを挿入しない<br>監視：なし |
| 備考 | | |

| | |
|---|---|
| ポリシー | 情報漏えい対策ポリシー |
| 名前 | デフォルトのポリシーはありません |
| ステータス | |
| 受信者と送信者 | |
| 受信者 | |
| 受信者の除外 | |
| 送信者 | |
| 送信者の除外 | |
| 検索条件<br>※有効の設定のみ記載 | |
| 処理 | |
| 備考 | |

**組織レベルのデフォルトポリシールール**

| ポリシー | ウイルスポリシー | スパムメールポリシー |
|---|---|---|
| 名前 | Organization: Virus | Organization: Spam or Phish |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | 所属する組織 | 所属する組織 |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | 【検出タイプを指定 (最低1つ):】<br>☑駆除可能な不正プログラムまたは不正プログラムコード<br>☑マスメーリング型の駆除不能なウイルスまたは不正プログラムコード<br>☑マスメーリング型ではない駆除不能なウイルスまたは不正プログラムコード<br><br>【機械学習型検索の指定:】<br>[2022年5月以前]<br>なし<br><br>[2022年5月以降]<br>☑機械学習型検索を有効にする<br>☑検出機能向上のため不審ファイルをトレンドマイクロに送信する<br><br>【高度な設定の指定:】<br>☑仮想アナライザに不審ファイルを送信する<br>低 (最も控えめ)<br>☑マクロ、JSEおよびVBE検索を含める | ☑スパムメール<br>レベル: 中低<br>☑ビジネスメール詐欺 (BEC)<br>このルールを次の場合に適用:<br>●スパムメール対策エンジンでBEC攻撃として検出<br>☑フィッシングおよびその他の不審なコンテンツ<br>☑グレーメール<br>グレーメールのカテゴリ<br>☑マーケティングメッセージとニュースレター<br>☑Webレピュテーション<br>☑ソーシャルエンジニアリング攻撃 |
| 処理 | インターセプト：隔離<br>変更：なし<br>監視：なし | インターセプト：隔離<br>変更：なし<br>監視：なし |
| 備考 | | |

| ポリシー | スパムメールポリシー | スパムメールポリシー |
|---|---|---|
| 名前 | Organization: Newsletter or spam-like | Organization: Probable BEC threat |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | 所属する組織 | 所属する組織 |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | ☑スパムメール<br>レベル: 中高<br>☑グレーメール<br>グレーメールのカテゴリ<br>☑マーケティングメッセージとニュースレター<br>☑Webレピュテーション | ☑ビジネスメール詐欺 (BEC)<br>このルールを次の場合に適用:<br>●スパムメール対策エンジンでBEC攻撃の可能性ありと判定 |
| 処理 | インターセプト：メッセージをインターセプトしない<br>変更：件名にタグを挿入 - "spam>"<br>監視：なし | インターセプト：メッセージをインターセプトしない<br>変更：本文にスタンプを挿入- "Probable BEC threat"<br>監視：なし |
| 備考 | | |

| ポリシー | スパムメールポリシー | コンテンツポリシー |
|---|---|---|
| 名前 | Organization: Writing style BEC threat | Organization: High-risk attachment |
| ステータス | 無効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | 所属する組織 | 所属する組織 |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | ☑ビジネスメール詐欺 (BEC)<br>このルールを次の場合に適用:<br>●ライティングスタイル分析でBEC攻撃として検出 | 条件: いずれかを満たす<br>☑添付ファイルが次の状態　ファイル名または拡張子<br>☑ブロックが推奨されるファイル拡張子<br>☑添付ファイルが次の状態　MIMEコンテントタイプ<br>☑オーディオ<br>☑ビデオ<br>☑添付ファイルが次の状態　実際のファイルタイプ<br>☑実行可能ファイル<br>☑メディア<br>☑添付ファイルのサイズが次に一致する　> 5 MB<br>☑添付ファイルの数が次に一致する　> 20 |
| 処理 | インターセプト：メッセージをインターセプトしない<br>変更：なし<br>監視：通知送信 - ”Writing Style Analysis Violation” | インターセプト：隔離<br>変更：なし<br>監視：なし |
| 備考 | | |

| ポリシー | コンテンツポリシー | コンテンツポリシー |
|---|---|---|
| 名前 | Organization: Exceeding msg size or # of recipients | Organization: Password protected |
| ステータス | 有効 | 有効 |
| 受信者と送信者 | | |
| 受信者 | 所属する組織 | 所属する組織 |
| 受信者の除外 | なし | なし |
| 送信者 | 任意のアドレス | 任意のアドレス |
| 送信者の除外 | なし | なし |
| 検索条件<br>※有効の設定のみ記載 | 条件: いずれかを満たす<br>☑メッセージサイズが次に一致する　　> 50 MB<br>☑受信者の数　　> 50 | 条件: いずれかを満たす<br>☑添付ファイルが次の状態　　パスワードで保護されている |
| 処理 | インターセプト：隔離<br>変更：なし<br>監視：通知送信 - "Notification of Exceeding message size" | インターセプト:メッセージをインターセプトしない<br>変更：本文にスタンプを挿入 - "Unscanned Attachment"<br>監視：なし |
| 備考 | | |

# Email Security R2 あんしんプラス　デフォルトポリシー
# 【送信保護設定】

**ドメイン毎に生成されるデフォルトポリシールール**

| ポリシー | ウイルスポリシー | スパムメールポリシー |
|---|---|---|
| 名前 | Outbound - Virus | Outbound - Spam or Phish |
| ステータス | 無効 | 無効 |
| 受信者と送信者 | | |
| 受信者 | 任意のアドレス | 任意のアドレス |
| 受信者の除外 | なし | なし |
| 送信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 送信者の除外 | なし | なし |
| 検索条件 | 【検出タイプを指定 (最低1つ):】<br>☑駆除可能な不正プログラムまたは不正プログラムコード<br>☑マスメーリング型の駆除不能なウイルスまたは不正プログラムコード<br>☑マスメーリング型ではない駆除不能なウイルスまたは不正プログラムコード<br><br>【機械学習型検索の指定:】<br>[2022年5月以前]<br>なし<br><br>[2022年5月以降]<br>☑機械学習型検索を有効にする<br>☑検出機能向上のため不審ファイルをトレンドマイクロに送信する | ☑スパムメール<br>レベル：中低<br>☑フィッシングおよびその他の不審なコンテンツ<br>☑Webレピュテーション |
| 処理 | インターセプト：隔離<br>変更：なし<br>監視：なし | インターセプト:隔離<br>変更:なし<br>監視:なし |
| 備考 | デフォルト無効です。使用する | |

| ポリシー | コンテンツポリシー | コンテンツフィルタ |
|---|---|---|
| 名前 | Outbound - High-risk attachment | Outbound - Exceeding msg size or # of recipients |
| ステータス | 無効 | 無効 |
| 受信者と送信者 | | |
| 受信者 | 任意のアドレス | 任意のアドレス |
| 受信者の除外 | なし | なし |
| 送信者 | *@［ドメイン名］ | *@［ドメイン名］ |
| 送信者の除外 | なし | なし |
| 検索条件 | 条件: いずれかを満たす<br>☑添付ファイルが次の状態　ファイル名または拡張子<br>☑ブロックが推奨されるファイル拡張子<br>☑添付ファイルが次の状態　MIMEコンテントタイプ<br>☑オーディオ<br>☑ビデオ<br>☑添付ファイルが次の状態　実際のファイルタイプ<br>☑実行可能ファイル<br>☑メディア<br>☑添付ファイルのサイズが次に一致する　> 5 MB<br>☑添付ファイルの数が次に一致する　> 20 | 条件:いずれかを満たす<br>☑メッセージサイズが次に一致する　> 50 MB<br>☑受信者の数　> 50 |
| 処理 | インターセプト：メッセージ全体を削除<br>変更：なし<br>監視：なし | インターセプト：メッセージ全体を削除<br>変更：なし<br>監視：通知送信 - "Notification of Exceeding message size" |
| 備考 | 特に添付ファイルのサイズ、添付ファイルの数がお客様の要件を満たすか確認してください。 | 特にメッセージサイズ、受信者の数がお客様の要件を満たすか確認してください。 |

| | |
|---|---|
| ポリシー | 情報漏えい対策ポリシー |
| 名前 | デフォルトのポリシーはありません |
| ステータス | |
| 受信者と送信者 | |
| 受信者 | |
| 受信者の除外 | |
| 送信者 | |
| 送信者の除外 | |
| 検索条件 | |
| 処理 | |
| 備考 | |

**組織レベルのデフォルトポリシールール**

| ポリシー | ウイルスポリシー | ウイルスポリシー |
|---|---|---|
| 名前 | Organization: Global Outbound Policy (Virus)　※設定変更できません | Organization: Outbound - Virus |
| ステータス | 有効 | 無効 |
| 受信者と送信者 | | |
| 受信者 | 任意のアドレス | 任意のアドレス |
| 受信者の除外 | なし | なし |
| 送信者 | 所属する組織 | 所属する組織 |
| 送信者の除外 | なし | なし |
| 検索条件 | 【検出タイプを指定 (最低1つ):】<br>☑駆除可能な不正プログラムまたは不正プログラムコード<br>☑マスメーリング型の駆除不能なウイルスまたは不正プログラムコード<br>☑マスメーリング型ではない駆除不能なウイルスまたは不正プログラムコード<br><br>【機械学習型検索の指定:】<br>☑機械学習型検索を有効にする<br>　☑検出機能向上のため不審ファイルをトレンドマイクロに送信する | 【検出タイプを指定 (最低1つ):】<br>☑駆除可能な不正プログラムまたは不正プログラムコード<br>☑マスメーリング型の駆除不能なウイルスまたは不正プログラムコード<br>☑マスメーリング型ではない駆除不能なウイルスまたは不正プログラムコード<br><br>【機械学習型検索の指定:】<br>[2022年5月以前]<br>なし<br><br>[2022年5月以降]<br>☑機械学習型検索を有効にする<br>　☑検出機能向上のため不審ファイルをトレンドマイクロに送信する |
| 処理 | ＜2021/2/28以前からご利用いただいているお客様＞<br>インターセプト：メッセージ全体を削除<br>変更：なし<br>監視：通知送信 - "Global Outbound Virus detection"<br>※インターセプトを「メッセージ全体を削除」から「隔離」へ変更することをご希望の場合は、<br>弊社サポート窓口までご相談下さい。<br><br>＜2021/2/28以降にご利用を開始されたお客様＞<br>インターセプト：隔離<br>変更：なし<br>監視：通知送信 - "Global Outbound Virus detection" | インターセプト：隔離<br>変更：なし<br>監視：なし |
| 備考 | 処理を「メッセージ全体を削除」から「隔離」へ変更することをご希望の場合は、<br>あんしんプラスサポートセンターまでご相談下さい。 | |

| ポリシー | スパムメールポリシー | スパムメールポリシー |
|---|---|---|
| 名前 | Organization: Global Outbound Policy (Spam or Phish)　※設定変更できません | Organization: Outbound - Spam or Phish |
| ステータス | 有効 | 無効 |
| 受信者と送信者 | | |
| 受信者 | 任意のアドレス | 任意のアドレス |
| 受信者の除外 | なし | なし |
| 送信者 | 所属する組織 | 所属する組織 |
| 送信者の除外 | なし | なし |
| 検索条件 | ☑スパムメール<br>　レベル：最高（最も強力）<br>☑フィッシングおよびその他の不審なコンテンツ<br>☑Webレピュテーション | ☑スパムメール<br>　レベル：中低<br>☑フィッシングおよびその他の不審なコンテンツ<br>☑Webレピュテーション |
| 処理 | インターセプト:メッセージをインターセプトしない<br>変更:なし<br>監視:なし | インターセプト:隔離<br>変更:なし<br>監視:なし |
| 備考 | | |

| ポリシー | コンテンツポリシー | コンテンツフィルタ |
|---|---|---|
| 名前 | Organization: Outbound - High-risk attachment | Organization: Outbound - Exceeding msg size or # of recipients |
| ステータス | 無効 | 無効 |
| 受信者と送信者 | | |
| 受信者 | 任意のアドレス | 任意のアドレス |
| 受信者の除外 | なし | なし |
| 送信者 | 所属する組織 | 所属する組織 |
| 送信者の除外 | なし | なし |
| 検索条件 | 条件: いずれかを満たす<br>☑添付ファイルが次の状態　ファイル名または拡張子<br>☑ブロックが推奨されるファイル拡張子<br>☑添付ファイルが次の状態　MIMEコンテントタイプ<br>☑オーディオ<br>☑ビデオ<br>☑添付ファイルが次の状態　実際のファイルタイプ<br>☑実行可能ファイル<br>☑メディア<br>☑添付ファイルのサイズが次に一致する　> 5 MB<br>☑添付ファイルの数が次に一致する　> 20 | 条件:いずれかを満たす<br>☑メッセージサイズが次に一致する　> 50 MB<br>☑受信者の数　> 50 |
| 処理 | インターセプト：メッセージ全体を削除<br>変更：なし<br>監視：なし | インターセプト：メッセージ全体を削除<br>変更：なし<br>監視：通知送信 - "Notification of Exceeding message size" |
| 備考 | 特に添付ファイルのサイズ、添付ファイルの数がお客様の要件を満たすか確認してください。 | 特にメッセージサイズ、受信者の数がお客様の要件を満たすか確認してください。 |