DARKTRACE

# AIで未知のセキュリティ脅威をリアルタイムに検知・可視化する「Enterprise Immune System」と連携

クラウドベース Cyber AI Eメール・ゲートウェイ

# Antigena Email for Microsoft 365

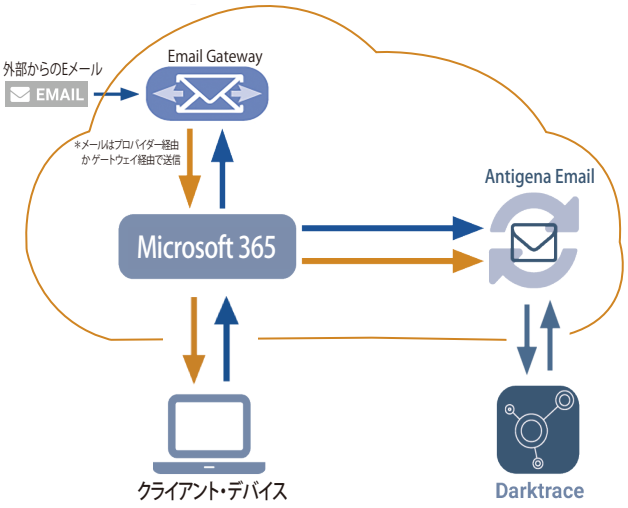
未知の標的型メール攻撃にAIが自動対処できるセキュリティ強化オプション「Antigena Email」Microsoft 365（旧称Office 365）版は、Microsoft 365メール利用において個人のコミュニケーションの定常パターンを機械学習することでアカウントハイジャック、Eメールスプーフィング、および標的型メール攻撃に自動対処することで多種多様な「デジタルフェイク」から顧客を強力に保護し、本物のEメールを自動的に識別します。

## 特徴

- ✓ Enterprise Immune System オプション機能
- ✓ 自己学習：メールアドレスだけでなく、個人の「生活パターン」も理解します。
- ✓ 従来のツールが通過させる悪質なEメールを識別します。
- ✓ ソーシャルエンジニアリングを含むすべての高度な Eメール攻撃に対して有効です。

## Eメールの脅威を Antigena Email が捕捉

- 標的型スピアフィッシング攻撃
- ソーシャルエンジニアリングとなりすまし
- ビジネスメールの侵害
- サプライチェーンアカウントの乗っ取り
- データ漏えい
- 未知のマルウェア




## 進化したEメールの脅威が通過しています。

Eメール攻撃はますます巧妙になっており、攻撃的なAIが近い将来にEメール攻撃キャンペーンを激増させる恐れがあります。標的型のなりすましEメールを本物の通信と区別することはほとんど不可能になりつつあります。進化した攻撃は、従来のEメールセキュリティツールを通過しており、個々の Eメールを個別に監視し、既知の悪意のある攻撃のルールおよびシグネチャと比較します。
サプライチェーンがより複雑になり、従業員の分散とモバイル化が進む中、Eメールセキュリティに対するAIによる自己学習アプローチがますます必要になっています。

## 世界初の自己防衛型受信トレイ

Antigena Emailは、受信トレイ向けの世界初のサイバーAIソリューションです。このテクノロジーは、すべてのユーザと関係する送信者の通常の「生活パターン」を学習することで、メール・コミュニケーションにおける「個人」の理解を構築します。
従来の防御策では、過去の攻撃でEメールの要素が観察されたかどうかを確認しますが、Antigena Emailは、受信者が通常の「生活パターン」の他、仲間や組織全体のコンテキストにおいて、特定のEメールとやり取りすることが異常であるかどうかを確実に確認することができる唯一のソリューションです。
このコンテキストに関する知識により、AIは非常に正確な決定を下し、不正な支払いを仕掛けようとする「クリーンな」なりすましメールから高度なスピアフィッシング攻撃まで、あらゆる範囲のメール攻撃を無力化できます。

## メールから個人を理解する

人間の免疫システムにインスパイアされたAntigena Emailは、Darktraceのコアである人工知能を使用して、すべての内部および外部ユーザの「個人」の挙動を学習し、送受信される両方向の通信を分析します。
Antigena Emailは、受信者を動的な個人およびグループとして扱うことにより、「標準」からの微妙な逸脱を独自に特定し、害のないように見えるEメールが紛れもなく悪意のあるものであることを明らかにします。

## 事例：

### サプライチェーンアカウント乗っ取り

検出が最も難しい攻撃の1つは、外部アカウントの乗っ取りです。この場合、犯罪者は信頼できる連絡先のEメール資格情報を乗っ取り、受信トレイにアクセスします。いったん侵入すると、攻撃者は過去の通信にアクセスし、非常に説得力のあるEメールを作成でき、悪意のあるリンクや添付ファイルを会話に適切なタイミングで埋め込みます。従来の防御策では、これが信頼できるユーザであると想定していますが、Antigena Emailは信頼できないと認識します。学習した生活パターンに照らして各Eメールを分析し、ほんのわずかな逸脱も検出します。
これらには以下が含まれます（ただし、これらに限定されません）。

**異常なログイン場所:**
Antigena Emailは、本物の送信者の地理的に配置可能なIPアドレスを抽出し、信頼できる連絡先が過去の生活パターンから考えると、これが稀であるかどうかを判断できます。稀なログイン場所だけではアラートや自律応答がトリガーされない場合がありますが、システム全体の計算と異常スコアで反映されます

**稀なリンク:**
人々は、信頼するWebサイトへのリンクを共有することがよくあります。これらのリンクを側面からメールで監視することにより、Antigena Emailは、組織のコンテキストでは稀な(珍しい)リンクとドメインを特定できます。
これは、特定の送信者のEメールドメインが共有内部リンクで監視されているかどうかを判断するときに、他の脅威シナリオでも役立ちます。

**異常な受信者:**
Antigena Emailは、内部および外部のユーザとグループの関係をグラフ・ベースでモデル化し、それらの関係を詳細なレベルで理解します。攻撃者が組織内の一定範囲の受信者に複数の Eメールを送信する場合、Antigena Emailはこの特定のグループが同じソースからのEメールを受信する可能性を推定できます。

**行動異常:**
Antigena Emailは、さまざまな送信者がどのようにEメールを構築するかを学び、隠されたEメールのメタデータと本文のパターンの両方を分析します。
ダークトレースは、すべての受信メールにAIを適用することで、Eメールが真のアカウント所有者以外の誰かによって送信されたことを示す可能性がある微妙な変更を識別します。

これらの些細な兆候を相互に関連付けることにより、Antigena Emailは包括的な異常スコアに迅速に到達し、Eメールが悪意のあるものであると確信を持って判断し、影響を与える前に攻撃を無力にします。

製品情報URL: https://www.psi.co.jp/products/list5-2.html
問い合わせ E-Mail: support@psi.co.jp

PSI 株式会社ピーエスアイ
https://www.psi.co.jp

【東京本社】
〒160-0022
東京都新宿区新宿5-5-3 建成新宿ビル4F
Tel: 03-3357-9980

【大阪営業所】
〒532-0011
大阪市淀川区西中島3-21-13 新大阪日新ビル4F
Tel: 06-4805-9601

【福岡営業所】
〒810-0001
福岡県福岡市中央区天神1-15-5 天神明治通りビル3F
Tel: 092-600-4570



2020年5月