

1月29日 10:00 発表のプレスリリースです



## Press Release

2020年1月29日  
株式会社 TwoFive

# TwoFive、米 Area 1 Security 社のフィッシング対策クラウドサービス 「Area 1 Horizon」を提供開始

AI、機械学習、コンピュータビジョン技術で、100%に近い検出が可能に  
攻撃を先取りし、業界標準の 24 日前にフィッシングサイトやマルウェアを検出

株式会社 TwoFive（本社：東京都中央区、社長 末政 延浩）は、米 Area 1 Security 社（エリア・ワン・セキュリティ、本社：カリフォルニア州）と国内販売代理店契約を締結し、クラウド型のフィッシング対策サービス「Area 1 Horizon（エリア・ワン・ホライズン）」の提供を開始します。

「Area 1 Horizon」は、革新的な予測分析と機械学習のアルゴリズムにより、既存のアンチスパムソリューションでは検知が難しいフィッシングを検出し、すべてのトラフィックベクトル（電子メール、Web、ネットワーク）にわたるフィッシング攻撃を、ユーザーに影響が及ぶ前に無効にします。

サイバー脅威の約 95%がフィッシング攻撃から発生すると言われていますが、フィッシング攻撃はスパムやウイルスなどのメール脅威と比較して巧妙に設計されており、従来のセキュリティ防御（メールセキュリティ、Web セキュリティ、ファイアウォール）をすり抜けて被害が発生します。また、既存のテクノロジーは、フィッシングサイトやマルウェアを積極的に検出することはなく、多くの場合、攻撃がすでに進行中の場合にのみ脅威データを分析するので被害を未然に防ぐことはできません。

これに対して、「Area 1 Horizon」は、高速 Web クローラー「ACTIVESENSORS」を世界中に配備しており、積極的にクロールしており（2 週間で 60 億ページ以上）、フィッシング攻撃サイクルの初期段階におけるフィッシングキャンペーン、攻撃者のインフラストラクチャ、攻撃の配信メカニズムを特定します。また、2,500 億を超える攻撃メタデータ、5 ペタバイト以上の攻撃データウェアハウスを独自のスモールパターン解析エンジン「SPARSE」で包括的に分析し、ACTIVESENSORS ネットワークによって生成されたデータセット内の脅威を発見します。

「Area 1 Horizon」は、これらの革新的なテクノロジーにより、攻撃が開始される前に、新たなフィッシングサイト・キャンペーンを見破り、Virus Total などの業界リソースの 24 日前に悪質なフィッシングサイトやマルウェアを検出しています。

「Area 1 Horizon」は、クラウドサービスのため導入が容易で、セキュアメールゲートウェイ（SEG）、セキュア Web ゲートウェイ（SWG）、ファイアウォール、SIEM など、既存のセキュリティソリューションとスムーズに統合することが可能で、他のソリューションでは見逃してしまう少量の標的型フィッシングからユーザーを保護します。

TwoFive は、「Microsoft Office 365」、「Google G Suite」などのクラウドでメール運用している組織を主なターゲットとして、直販ならびにパートナー経由で販売します。

「Area 1 Horizon」は、年間契約の他に、既存の防御対策をすり抜けたフィッシング攻撃の防御に対してのみ費用が発生する Pay-per-Phish（ペイ・パー・フィッシュ）モデルを選択することも可能です。

尚、TwoFive は、来る 3 月 3 日（火）「フィッシング・なりすましメール対策セキュリティセミナー」を開催し、「Area 1 Horizon」の技術と導入事例などについてご紹介します。

#### ◆「Area 1 Horizon」独自のテクノロジー

##### ◇「ActiveSensors」高速クローラー

緊急のキャンペーンインフラストラクチャを検出し、攻撃者が脅威キャンペーンを開始するために使用している中継ポイントから攻撃データを集約します。Web を大規模にクロールする能力はユニークであり、すべての Web ページ、URL、ドメイン、および IP アドレスを見て明らかになる新しいパターンを見つけます。Google がコマースとコンテンツのために Web のインデックスを作成するように、数週間ごとに 80 億ページ以上と 2 億 2000 万 TLD の Web 全体のインデックスを作成します。これは、これまでに構築された脅威の発見に焦点を合わせた最も包括的な Web クロール機能です。

##### ◇「SPARSE」スモールパターン解析エンジン

フィッシングは組織のトラフィックの約 0.1～1%に過ぎませんが、ほぼ 100%の損害を引き起こします。これらの低ボリューム/高ダメージ攻撃を探し出すために、Web 全体を集約するスモールパターン解析エンジン SPARSE により、フィッシング攻撃を特徴付けるさまざまなモデルを分析します。SPARSE は、複合的な上場解析により、攻撃の形成パターンを理解し、ActiveSensors ネットワークによって生成されたデータセット内の脅威を見つけます。

製品詳細は以下をご参照ください。

<https://www.twofive25.com/service/area1security.html>

#### ◆「Area 1 Horizon」の販売について

◇販売開始：2020 年 2 月 1 日

◇提供形態：SaaS

◇サービスメニュー：

- ・ Cloud-based DNS（フィッシング URL & ドメイン遮断）
- ・ Cloud-based MTA（フィッシングメール検知）
- ・ Edge Device Integration（フィッシングコール遮断）

◇料金体系と価格：

- ・ 年間契約 オープンプライス
- ・ Pay-Per-Phish 1,000 フィッシングあたり 300 万円（税別）

◇販売経路：TwoFive および パートナー経由

#### ◆「Area 1 Horizon」ご紹介セミナー

◇セミナー名称：フィッシング・なりすましメール対策セキュリティセミナー

◇主催：株式会社 TwoFive

◇日時：2020 年 3 月 3 日(火) 13:00～17:00

◇場所：千代田区丸の内 三菱ビル 10F コンファレンススクエアエムプラス  
※詳細プログラム/お申込み方法などは追って TwoFive の Web サイトで公開します。

#### ■株式会社 TwoFive 社について

<https://www.twofive25.com/>

株式会社 TwoFive は、大手 ISP、ASP、携帯事業者の電子メールシステムインフラで長年経験をつんだメールシステムの技術者集団により 2014 年に設立されました。日本の電子メール環境を向上させることを使命としてベンダーニュートラルな立場で最適な技術とサービスを組み合わせ、メールシステムの設計・構築、電子セキュリティなどについてコンサルティング、ならびに各種レピュテーションデータを提供しています。

#### ■報道関係者お問い合わせ

株式会社 TwoFive

Email : [info@twofive25.com](mailto:info@twofive25.com) TEL : 080-2021-8067 (担当：谷口)

※読者お問い合わせ先は以下をご掲載ください。

[info@twofive25.com](mailto:info@twofive25.com) TEL : 03-5704-9948

記載されている会社名、製品名は各社の商標です。

## ◆添付資料◆

### [Area 1 Horizon 導入例]

#### ◇MXレコード書き換え



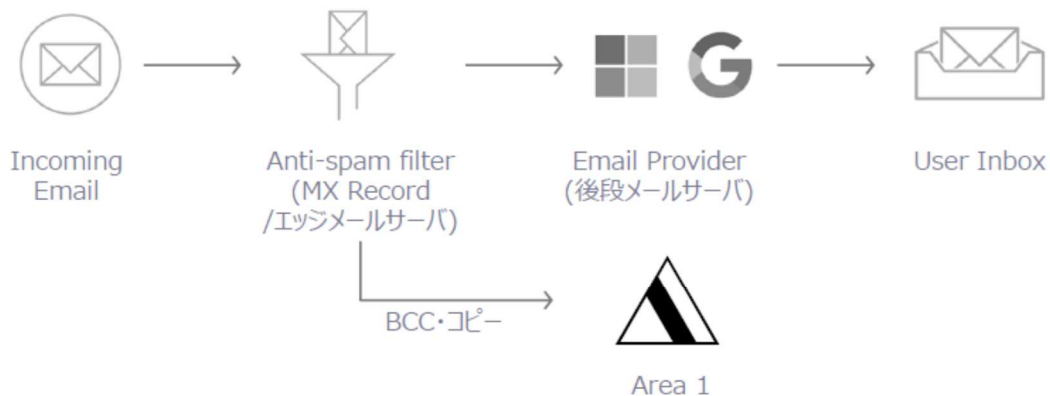
- MXレコードに Area 1 を指定
- X-headerに判定結果記載
- メール書き換えオプション: 件名/本文差し込み、URL書き換え/無効化
- X-headerを元に後段メールサーバで処理(配送、隔離、破棄)

#### ◇既存システム内メール経路変更



- エッジメールサーバからArea 1へメール経路変更
- X-headerに判定結果記載
- メール書き換えオプション: 件名/本文差し込み、URL書き換え/無効化
- X-headerを元に後段メールサーバで処理(配送、隔離、破棄)

#### ◇BCC / コピーによるメール経路分離



- エッジメールサーバからArea 1へBCCまたはコピー
- 管理者がレポート閲覧、アラート受信