各　位

2020 年 12 月 16 日
サイバネットシステム株式会社
（コード番号 4312 東証第一部）

世界で唯一※1、ディープラーニング※2を用いたAIで未知のサイバー攻撃を予測し防御する「Deep Instinct」販売開始のお知らせ

数十億のマルウェアを自ら学習することで、未知の脅威も高い精度で防御し、業務負荷を増やさずセキュリティを強化。

サイバネットシステム株式会社（本社：東京都、代表取締役 社長執行役員：安江 令子、以下「サイバネット」）は、Deep Instinct Ltd.（ディープインスティンクトリミテッド、本社：米国ニューヨーク州、以下「Deep Instinct 社」）の日本法人であるディープインスティンクト株式会社（本社：東京都、カントリーマネージャー　並木 俊宗）と日本における販売代理店契約を締結し、Deep Instinct 社が開発・販売するディープラーニングによるサイバーセキュリティ「Deep Instinct（ディープインスティンクト、以下「Deep Instinct」）」を 12 月より国内販売を開始することをお知らせいたします。

近年のサイバーセキュリティ対策

近年のサイバー攻撃は、マルウェアを利用した従来の攻撃に加えて PowerShell※3など OS 付属ツールを悪用したファイルレス攻撃が増えるなど日々高度化・巧妙化しており、現在主流のシグネチャ※4を利用したアンチウイルスソフトでは攻撃を防ぐことが難しくなっています。

一方で、セキュリティ技術者の不足※5はこれまでも指摘されており、専門の知識に乏しい担当者に兼任させる組織も多いのが現状です。また、昨今のテレワークの増加などの業務環境の変化に伴い、セキュリティ対策が不十分なシステムや端末が用いられることからサイバー攻撃の被害への対応が遅れる事案も報告※6されており、高い精度で攻撃を防御できるセキュリティ対策がこれまで以上に求められています。

ディープラーニングを利用したサイバーセキュリティ「Deep Instinct」とは

画像認識や車の自動運転で大きな成果をあげている AI（人工知能）の一つ、ディープラーニング（深層学習）を世界で初めてセキュリティ対策に取り入れ、攻撃を高い精度で予測し、防御できるのが Deep Instinct です。

これまでも機械学習を利用した製品は存在しましたが、その多くは、マルウェアの特徴を人間が抽出し、その特徴を含むデータを学習させて使う物でした。一方 Deep Instinct は、数十億を超える実際の攻撃データファイルと無害なファイルを繰り返し学習させることで、AI 自らマルウェアの特徴を抽出し「予測モデル」を作成します。

この予測モデルを各端末に配布することで、人間が気付かない僅かな特徴をも見逃さず攻撃を予測できるようになり、機械学習では検出しにくい攻撃までも検知し、防御することができます。また、検知の精度が高く誤検知も非常に少ないため、セキュリティ担当者の負担を増やすことなく、セキュリティ対策を強化できます。

主なアンチウイルスソフトの特長の違い		
従来型	マシンラーニング （機械学習）	ディープラーニング （深層学習）
主に既知のマルウェアおよびその亜種の攻撃に有効で、シグネチャとヒューリスティック※7による対策が一般的。	ゼロデイ攻撃※8やマルウェアは防御可能だが、実行ファイル形式のみ。また特徴抽出を人に依存するため、検知能力に限界があり誤検知も多い。	ゼロデイ攻撃やマルウェアの防御が可能で様々なファイルに対応。特徴抽出自体を AI が行うため、高い精度で検知が可能かつ、誤検知が少ない。

「Deep Instinct」の主な特長

- **未知の脅威への対応**：これまでのシグネチャベースのアンチウイルスソフトは、主に既知のマルウェアの検知と防御のみ可能でした。Deep Instinct は、内部構造を微妙に変えた亜種のマルウェアや未知のマルウェアのほか、PowerShell などを悪用するファイルレス型も高い精度で防御します。
- **高い検出率と低い誤検知数**：情報セキュリティの向上を目的に関連製品やサービスの評価を行う第三者機関「SE Labs」が昨年実施したテスト※9によると、未知・既知のマルウェアに対する Deep Instinct の検知率は 100%、誤検知数は 0（ゼロ）でした。
- **攻撃種別の提示と対策手段の提供**：Deep Instinct がマルウェアを検知した際は、上記「予測モデル」と同時に作成される「分類モデル」により、ランサムウェア、ワーム、ウイルス、ドロッパー、スパイウェア、バックドア、疑わしいアプリの 7 つに分類して管理者に知らせます。これが悪意の度合いとマルウェアタイプの判別と対策を立てる指標となるため、管理者は必要に応じて遠隔地からファイルを削除／復元したり、実行中のプロセスを停止したり、エンドポイントを隔離することが可能となります。
- **ユーザーの利便性を高め、オフラインでも強固な監視を実現**：Deep Instinct の「予測モデル」の更新頻度は数ヶ月に一度程度で済むため、シグネチャベースのアンチウイルスソフトのように頻繁にシグネチャファイルを更新する必要がありません。また、これまでのアンチウイルスソフトの中には、端末がオフラインのときは検知力が低下するものがありますが、Deep Instinct はオンライン・オフラインの区別なく脅威からエンドポイントを保護します。メモリー消費量も少なく、CPU の使用量も 1%未満と軽量なため、業務を妨げないのも特長です。
- **PC だけでなくモバイル OS も一元管理**：Windows、macOS のほか、モバイル OS の Android、iOS、Chrome OS まで、主要な OS を網羅しており、これらを統一したセキュリティポリシーで一元管理できます。

価格

別途お問い合わせください。

オンラインセミナー「Deep Instinct Deep Dive」

Deep Instinct 販売開始に合わせ、オンラインで視聴いただけるセミナーを開催します。世界で唯一セキュリティ対策にディープラーニングを用いた Deep Instinct が他のアンチウイルスソフトとどう違うかなど、デモを交えて詳しくご紹介します。多くの方の参加をお待ちしています。

販売開始記念 Deep Instinct Deep Dive セミナー ～ なぜディープラーニングが高い精度でサイバー攻撃を検知・防御できるのか ～	
日　程	2020 年 12 月 24 日（木）13 時 30 分～14 時 30 分 2021 年　1 月 14 日（木）13 時 30 分～14 時 30 分 2021 年　1 月 27 日（水）13 時 30 分～14 時 30 分
会　場	Zoom を用いた Web セミナー形式
対象者	最新マルウェア対策を実施・強化されたい方
共　催	ディープインスティンクト株式会社、サイバネットシステム株式会社
参加費	無料
定　員	100 名
参加申込および詳細	https://www.cybernet.co.jp/deepinstinct/seminar_event/didd.html

Deep Instinct の詳細については、下記 Web サイトをご覧ください。
https://www.cybernet.co.jp/deepinstinct

PRESS RELEASE

Deep Instinct 社 CEO 兼共同創業者 Guy Caspi(ガイ・カスピ) 氏コメント

Deep Instinct にとって、サイバネットとのパートナーシップを結ぶことはエキサイティングなことです。サイバネットは、当社がアジアへの事業拡大を展開していく中で、新しいビジネスラインの成長に豊富な経験を持ち、鋭い市場知識を提供してくれる貴重な戦略的パートナーとなってくれました。企業は、侵害が問題になる前に即座に対応できるサイバーセキュリティソリューションを必要としています。

注釈

※１： 世界で唯一ディープラーニングをセキュリティ対策に取り入れている：2020 年 12 月現在 Deep Instinct 社調べ。

※２： ディープラーニング（深層学習）：音声認識や画像の特定など、人間が行うようなタスクを実行できるようコンピュータに学習させる機械学習の手法。人間の脳細胞を模倣した多層構造のニューラルネットワークに、大量の画像、テキスト、音声データなどの実データを入力することで、データに含まれる特徴を各層で自動学習させることが可能。人工知能（AI）の開発や発展を支える技術の一つ。

※３： PowerShell：マイクロソフトが開発した拡張可能なコマンドラインインターフェイス（CLI）シェルおよびスクリプト言語。

※４： シグネチャ：コンピュータ セキュリティの用語で、マルウェアや不正アクセスといった攻撃の「特徴的なパターン」を指す。一般にシグネチャを利用した攻撃防御は、既知の攻撃には確実に対応できるものの、未知の攻撃には対応できないという弱点がある。

※５： 【参考】総務省発表資料『我が国のサイバーセキュリティ人材の現状について』１頁 2018 年 12 月
https://www.soumu.go.jp/main_content/000591470.pdf

※６： 【参考】警視庁発表資料『令和２年上半期におけるサイバー空間をめぐる脅威の情勢等について』２頁 2020 年 10 月１日
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf

※７： ヒューリスティック：ウイルスを検出する手法の一つで、マルウェアがもつ特徴的な動きの有無を判断する手法であり、主に既知のマルウェアの亜種などに有効。

※８： ゼロデイ攻撃：OS やアプリケーションの脆弱性をベンダーよりも早く見つけ、修正プログラムが配布される日＝「ワンデイ」より前の「ゼロデイ」に、その脆弱性を突く攻撃のこと。危険が最も高いサイバー攻撃の一つ。

※９： SE Labs 試験結果：SE Labs INTELLIGENCE-LED TESTING February 2019

Deep Instinct 社について

サイバーセキュリティにエンドツーエンドのディープラーニングを適用した初めての企業であり、唯一の企業です。ディープラーニングは脳の学習能力から発想を得ています。脳はある物体を識別することを学習すると、それを元に予測ができるようになります。同様に、Deep Instinct の人工知能はあらゆるタイプのサイバー脅威の検知を学習することによって、これらを本能的に予防できる機能を備えています。その結果、既知・新種、初見のマルウェア、ゼロデイ、ランサムウェア、APT（高度な持続的脅威）など、あらゆる種類のマルウェアをゼロタイムで予測・防御し、ネットワーク、エンドポイント、モバイルなど、企業内のあらゆる場所で、比類のない精度とスピードで、多層的な防御を可能にします。

Deep Instinct 社に関する詳しい情報については、下記 Web サイトをご覧ください。
https://www.deepinstinct.com/

サイバネットについて

サイバネットシステム株式会社は、CAE のリーディングカンパニーとして、30 年以上にわたり製造業の研究開発・設計関係部門、大学・政府の研究機関等へ、ソフトウェア、教育サービス、技術サポート、コンサルティングを提供しています。また ICT 分野では、最新のセキュリティソリューションのみならず、企業のセキュリティ向上に欠かせない IT 資産管理ツールや IT 運用管理ツールを提供しています。近年では、IoT やデジタルツイン、ビッグデータ分析、AI 領域で、当社の得意とする CAE や AR/VR 技術と組み合わせたソリューションを提案しています。

ブランドメッセージは「つくる情熱を、支える情熱」。日々、多様化・複雑化する技術課題に向き合うお客様に、「まずはサイバネットに聞いてみよう」と思っていただける企業を目指しています。

サイバネットシステム株式会社に関する詳しい情報については、下記 Web サイトをご覧ください。
https://www.cybernet.co.jp/

本件に関するお問い合わせ　サイバネットシステム株式会社

- 内容について
  IT ソリューション事業部／松岡
  E-MAIL：itdsales@cybernet.co.jp
- 報道の方は
  コーポレートマーケティング部／新留
  E-MAIL：prdreq@cybernet.co.jp
- 投資家の方は
  IR 室／目黒
  E-MAIL：irquery@cybernet.co.jp