# 最先端AI搭載の次世代型セキュリティ「Deep Instinct」

# 1. Deep Instinct 企業情報

- 設立：2015年 、Guy Caspi、Dr. Eli David、Nadav Mamanによって設立。
- 本社：アメリカ（ニューヨーク）
- 業種：サイバーセキュリティ会社

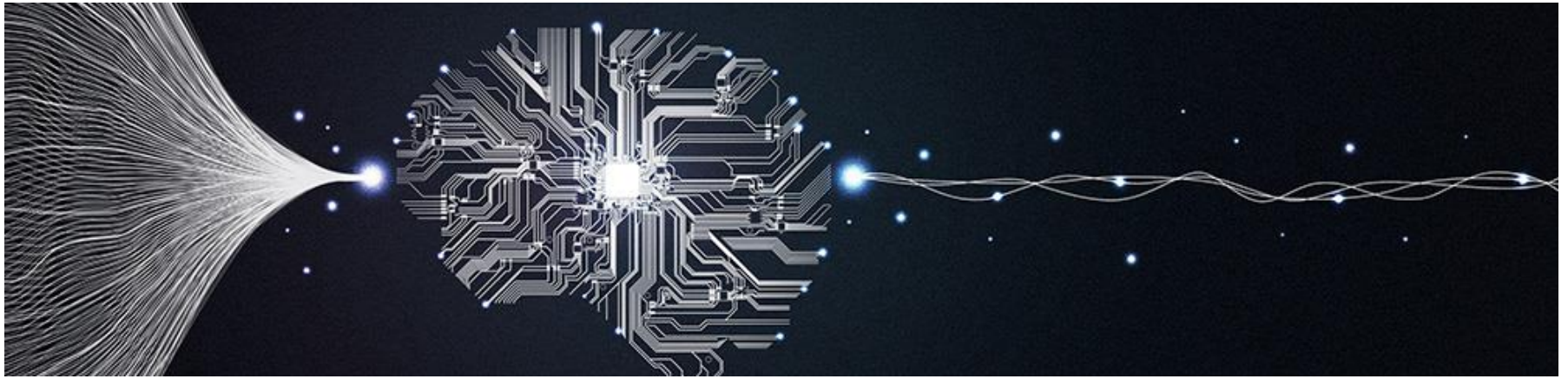
- Deep Instinctは、最も洗練されたセキュリティ技術を見つけるために、世界初のDeep Learning （深層学習）を活用したサイバーセキュリティ会社として設立。
- その先見性は注目を集め、nVIDIA（米国の半導体メーカー）、HP、SAMSUNG、LG など多くの企業から総額92万USドル（約1億円）の投資を受ける。
- 市場参入から約2年が経過した2020年までに約3,000社の顧客を獲得。
- 日本HPが自社の法人向けノート PC に Deep Learning機能を搭載したことからDeep Instinct社の日本での信頼性の高さを証明。
- 2020年9月、日本法人ディープインスティンクト株式会社を設立。

# 2. Deep Instinct とは？

- Deep Instinctは、高度なAI（人工知能）の1つであるDeep Learning を採用した次世代型セキュリティシステムです。

- Deep Learning（深層学習）の採用によって、既知・未知を問わず、あらゆるサイバー攻撃を予測・検知してエンドポイント（末端）を防御します。

- 第三者機関のテストにおいては、未知・既知のマルウェアを100％検知し、誤検知数はゼロと報告されております。

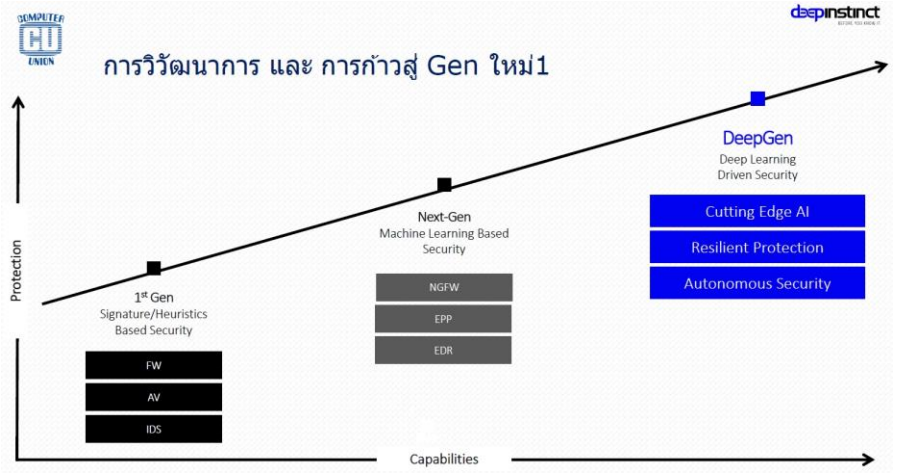


# 3. Deep Learning （深層学習）とは？

- Deep Learning（深層学習）とは、十分なデータ量があれば、人間の力なしに機械が自動的にデータから特徴を抽出する学習機能です。
- Deep Learning自体がAIと言う事ではなく、人工知能の要素技術の１つです。

  AI（人工知能）＞Machine Learning（機械学習）＞Deep Learning（深層学習）

- 第1世代のシグネチャ/ヒューリスティック型のセキュリティから、第2世代のMachine Learning型のセキュリティを経て、次世代のDeep Learningを採用したセキュリティが今後主要となります。



# 4. Machine Learning とDeep Learning の違い

＜Machine Learning（機械学習）＞

- エンジニアや科学者がデータ内の特徴量を**手動で選択し、モデルを学習させるAIの一種です。**
- 主に、出力の予測や傾向の発見を伴うプロジェクトに使用されております。限られたデータを使用して、新しい入力データを正しく判断するために後で使用できるパターンを学習します。

＜Deep Learning（深層学習）＞

- 人間の脳の神経経路を大まかにモデル化したMachine Learningの一種です。アルゴリズムが**自動的に有用な特徴量を学習します。**
- 主に、画像の分類、画像内のオブジェクトの識別、画像や信号の増幅を伴うプロジェクトに使用されております。画像や信号などの空間的および時間的に構成されたデータから特徴を自動的に抽出するように設計されてます。

# 5. Deep Learning でできること

## ● 画像認識

画像や動画を入力とし文字や顔などの特徴を認識・検出する技術。
背景から特徴を分離抽出しマッチングや変換をおこない、目的となる特徴を特定。
※例： Facebookのタグ付け（顔認証）、自動運転、感情分析など

## ● 音声認識

音声を認識させる技術。
人間の声を認識してテキストに出力したり、音声の特徴をとらえて声を出している人を識別する技術。
※例：iPhoneの「Siri」のような音声入力など

## ● 自然言語処理

人間が日常的に使う自然言語（書き言葉・話し言葉）をコンピューターに処理・理解させる技術。
※例：銀行のコールセンターでの問い合わせ対応、文書要約、機械翻訳など

## ● 異常検知

産業機器などに取り付けられたセンサーなどの時系列データから異常の兆候を感知する技術。
※例：工場内の監視（故障や異常動作の検知）など

# 6. Deep Instinct の長所

- ゼロタイムで脅威を予防
- 未知の脅威も予測して防御
- ゼロデイなど高度な攻撃も予防
- 幅広い攻撃面をカバー
- シンプルな運用（専任者要らず）
- 圧倒的に少ない誤検知
- 年に1、2回のアップデートのみ（シグネチャの更新不要）

# 7. Deep Instinct の利用環境


- **どのネットワークでも利用可能**

  ネットワーク境界、エンドポイント、携帯端末、データセンター、クラウド。

- **どの脅威にも有効**

  マルウェア、敵対行為、インサイダー脅威。

- **どの環境でも有効**

  オンライン/オフライン、VDI、クラウド/オンプレミス、マルチテナンス、エアギャップ

- **どのOSにも利用可能**

  Windows、macOS、iOS、Android、Chrome OS

**クラウドサービスのため導入は簡単で、自社サーバーの用意や専任者は不要です。**

# 8. マルウェアの脅威

毎日35万を超える
新しいマルウェアが
生成されている。

組織を危険にさらすゼロデイ攻撃
（ソフトウェアの脆弱性を狙った
攻撃）は、4倍以上増加。

過去12ヶ月で約3分の2の
企業がマルウェア攻撃の
対応に追われている。

1企業あたり4,000万～
3億5,000万ドルの損害を
マルウェア攻撃によって被っている。

マルウェア違反検出まで
平均196日の時間を要して
いる。

**マルウェアの攻撃の頻度と複雑さは日々加速しています。**

**Deep Instinct の利用によりこれらの脅威、損害額、対応時間から回避可能です。**

# 9. Deep Instinct のビジネスモデル

マルウェア対策ソフト「Deep Instinct」を搭載したノートPCを発売。「Deep Instinct」は元々有料製品ですが、日本HPは無償でバンドルしております。


アジア太平洋地域全体で年間9千万人以上の乗客にサービスを提供しているため、「Deep Instinct」の利用によって乗客の個人情報を保護しております。

# 10. Deep Instinct ご利用価格

●弊社では、本「Deep Instinct」システムのご提供を開始致しました。

●システムご利用価格は、1～2,000端末ご利用時、
1台につき1,480THB/年～ご利用頂けます。
月額料金換算では、1台につき123.3THB/月でセキュリティ保護対策が可能となります。

●この便利なシステムをより多くの企業様にご体験頂きたく、サポートさせて頂いておりますので、是非お気軽にお問い合わせください。


**a2network Thailand Co.,Ltd.**

689 Bhiraj Tower at Emquartier 20th Floor Room No. 2003
Sukhumvit Road Klongtonnua Wattana Bangkok 10110
Tel / Fax : +66-2-105-4568
http://www.berrymobile.jp/thailand/
http://www.berrymobile.jp/wizberry/
http://www.a2network.co.th/