■ライブ配信　■アーカイブ配信

【シリコンバレー・AI セキュリティ最前線】

AI の脅威！新世代サイバー攻撃と防衛技術

～AI への攻撃と AI を使った攻撃が米国社会を脅かす、AI で防衛できるか、次の標的は日本～

講　師　　**米国　VentureClef社　代表／アナリスト　宮本　和明**　氏

日　時　**2021 年１０月１３日（水）**　午前９時３０分～１２時３０分

［重点講義内容］

AI の脆弱性と危険性が顕著になった。知的能力を持つ AI であるが、そのアルゴリズムは脆弱で、サイバー攻撃の標的となる。AI へのサイバー攻撃は「Adversarial ML Threat」と呼ばれ、被害が拡大している。その手口は多彩で、教育データを改ざんしたり、アルゴリズムを盗み取るなど、AI は無防備であることが明らかになった。攻撃の対象は、ソフトウェアだけでなく、自動運転車やロボットなどに及び、社会生活が危険にさらされる。

同時に、高度な AI を悪用した攻撃が広がり米国社会が不安定になっている。人間の言語能力に匹敵する AI が開発され、人間と同レベルのフェイクニュースが大量に生成されている。これは「Disinformation Explosion」と呼ばれ Facebook などを介して拡散している。更に、本人と見分けのつかないビデオや音声が生成され、AI 世代の「振り込め詐欺」として被害が広がっている。各国で AI 開発が加速する中、攻撃対象も広がり、次のターゲットは日本とも言われる。

サイバー攻撃を防衛する AI の開発が進んでいるが、防御技術は未熟で、その効果は限定的である。このため、米国はサイバー攻撃を国家安全保障の危機と捉え、IT 大手と共同で技術開発を急いでいる。

このセミナーはビデオや音声などマルチメディアを用い、最新技術を分かりやすくビジュアルに解説する。

＜1＞AI への攻撃：ソフトウェア

1. AI への攻撃手法と分類
2. アルゴリズム教育プロセスへの攻撃
3. アルゴリズム実行プロセスへの攻撃
4. AI システムを防御する技術

＜2＞AI への攻撃：ハードウェア

5. 自動運転車への攻撃
6. ロボットへの攻撃
7. 顔認識 AI カメラへの攻撃

＜3＞AI を使った攻撃ほか

8. 大規模言語モデルを悪用した攻撃
9. シンセティックメディアを悪用した攻撃
10. ケーススタディ：
    AI が社員を解雇することは許されるか
11. ランサムウェアによる大規模な攻撃

＜4＞AI でサイバー攻撃を防御

12. Facebook の偽情報検知技術
13. スパムフィルター
14. フィッシングメール検知技術
15. 米国政府のサイバー攻撃防衛戦略
16. 質疑応答

ＰＲＯＦＩＬＥ　宮本　和明（みやもと　かずあき）氏

広島県出身。大阪大学基礎工学部卒業。1980年　富士通に入社。1985年　富士通関連会社 Amdahl Corp.（カリフォルニア州サニーベール）に出向し、アメリカでスーパーコンピュータ事業の立ち上げに従事。
2003年3月　富士通を退社し、リサーチ会社 VentureClef（カリフォルニア州マウンテンビュー）を設立。アナリストとしてコンピュータ技術の最新動向を追う。シリコンバレーのベンチャー企業にフォーカスし、時代を変える技術の発掘と解析を行う。
25年に及ぶアメリカでのキャリアを背景に技術トレンドをレポート。
【著書等】『機械学習・人工知能　業務活用の手引き（共著）』（情報機構）2017。『人工知能アプリケーション総覧（共著）』（日経BP社）2015。最新技術をブログ「Emerging Technology Review」で発信。
日経新聞に寄稿「宮本和明のシリコンバレー最先端技術報告」
http://itpro.nikkeibp.co.jp/article/COLUMN/20130326/466162/
日経新聞に寄稿「未来の技術の実験場－シリコンバレー最先端を追う」
http://itpro.nikkeibp.co.jp/article/COLUMN/20140603/561130/

●受　講　料　　1名につき　33，660円（税込）
同一のお申込フォームよりお申込の場合、2人目以降　27，500円(税込)

●お申込方法　　お申込フォームにご記入いただきFAXでお申込み下さい。
折り返し、受講証、請求書を郵送致します。
お申込み後、5営業日以内にお手元に届かない場合は必ずご一報下さい。
※お客様のご都合でキャンセルされる場合は、**「開催1週間前まで」**にお申し出下さい。
その後のキャンセルは、お申し受けできませんのでご了承下さい。

●お支払方法　　請求書を発行いたしますので、開催日までに銀行振込でお願いします。（遅れる場合はご相談下さい）

■ライブ配信について
＜1＞Zoom にてライブ配信致します。
＜2＞お申込時にご記入いただいたメールアドレスへ視聴用 URL と ID・PASS を開催前日までにお送り致しますので、開催日時に Zoom へご参加ください。
■アーカイブ配信について
＜1＞開催日より 3 営業日以降（収録動画配信のご用意ができ次第）に Vimeo にて配信致します。
＜2＞お申込時にご記入いただいたメールアドレスへ視聴用 URL をお送り致します。
＜3＞動画の配信期間は公開日より 2 週間ですので、その間にご視聴ください。2 週間、何度でもご都合の良い時間にご視聴可能です。

10月13日（水）　「新世代サイバー攻撃と防衛技術」　申込日　月　日

貴 社 名	
所 在 地	〒

参加希望の受講方法を選び□に✔をお入れ下さい。

□ ライブ配信　□ アーカイブ配信

氏名（フリカナ）		所属部署・役職	
ＴＥＬ	（　　）　－	ＦＡＸ	（　　）　－
E－mail	ブロック体でのご記入をお願いいたします。		

参加希望の受講方法を選び□に✔をお入れ下さい。

□ ライブ配信　□ アーカイブ配信

氏名（フリカナ）		所属部署・役職	
ＴＥＬ	（　　）　－	ＦＡＸ	（　　）　－
E－mail	ブロック体でのご記入をお願いいたします。		

※「受講証」等の送付先が上記と異なる場合は下記にご記入下さい。　K

通信欄	

●E-mail アドレス登録受付＆ご紹介キャンペーン実施中〔図書カード（500円）を進呈いたします〕
□セミナーへのお申込みではなく、メール配信登録のみの方は左記へ✔を入れて下さい。
※携帯アドレス、フリーメールアドレスは登録対象外となっております。
※メール配信登録をご希望の方をご紹介下さい！ご紹介いただいた方には図書カード（500円）を進呈させていただきます。
※上記お申込フォームに、ご郵送先（貴社名・所在地・氏名・所属部署・役職）をご記入下さい。

■主催（お申込み・お問い合せ先）　株式会社　新社会システム総合研究所
お申込み受付　FAX　０３－５５３２－８８５１
〒105-0003　東京都港区西新橋2－6－2　ザイマックス西新橋ビル4階
Tel:03-5532-8850／E-mail：info@ssk21.co.jp／URL：https://www.ssk21.co.jp

※配信停止、宛先変更、個人情報の苦情及び相談・開示は上記までご連絡下さい。　２１３９６－I