開会のごあいさつ Opening

CSA Japan Congress 2023

202311月12日

吉田 眞

日本クラウドセキュリティアライアンス 会長

工学博士　東京大学名誉教授

YOSHIDA Makoto PhD

Executive Advisor, CSA Japan Chapter

Emeritus Professor, the University of Tokyo

Summit and Congress

	CSA Japan Summit 春開催　ー　発信、交流	CSA Japan Congress 秋開催　ー　議論、交流
	クラウドセキュリティの最新動向、諸課題を提示し、CSAの活動成果を伝え共有	クラウドセキュリティについて多面的に取り上げて最新情報を提供し、ステークホルダが一堂に会し、クラウドを取り巻くセキュリティの課題を議論
2014	CSA-JC 発足記念 （グローバルサミット シリーズの一環）	クラウドの要素とセキュリティ
2015	あらゆるものの情報インフラとしてのクラウド	クラウドセキュリティの認証、技術の最新動向
2016	CPSを支えるクラウドセキュリティ	変貌するクラウドとクラウドセキュリティ
2017	新しい地平に突入したクラウドとセキュリティの脅威	クラウド環境におけるプライバシー、その課題と対策
2018	クラウドFIRST・セキュリティMUST	デジタルトランスフォーメーションを支えるクラウド技術の今
2019	Cloud as THE Platform ー待ったなしのビジネス変革 (Disruption)ー	トラスト！
2020	データドリブン社会を展望する ー5G,IoT,AIがもたらす価値とリスクとはー ＊	クラウドセキュリティ 2020 ＊
2021	2025年大阪・関西万博とクラウド ＊	ISMAPの現状と展望 ー動き出したISMAPの今とこれから ＊
2022	SDGs クラウド セキュリティ ~プラットフォームとしてのクラウドとそのセキュリティを考える~ ＊	雲の中から、あらゆる場所、ユーザの近くへ～CSAジャパンが語るCloud Securityの課題と対策～ ＊
2023	2023年トレンド深掘り ～クラウドの進化と真価～ ＊	***ChatGPTが問いかける、クラウドセキュリティの新たなヴィジョン***

＊ オンライン

テーマ *Theme*

テーマ： ChatGPTが問いかける、クラウドセキュリティの新たなヴィジョン

- 人工知能の進化とクラウド技術の融合が、新たな時代を開きつつある、
- ChatGPTなど生成AIのクラウドセキュリティへの影響、脅威、可能性を広く深く見渡し、
- ソフトウェア開発や運用の変化を予測。さらに、AIを取り入れたシステムの品質保証や運用のベストプラクティスも議論。
- COVID-19対策で、2020年からJapan Summit/CongressはWEBで実施し、今回はハイブリッド。

本日の講演ー1　*Lectures-1*

CSA本部講演		
Sean Heide氏	Technical Research Director, CSA	AI initiatives across CSA, Security Implications of ChatGPT, use cases
Introduction of the contents of "Security Implications of ChatGPT”		
基調講演		
石川冬樹 氏	国立情報学研究所　アーキテクチャ科学研究系　准教授 先端ソフトウェア工学・国際研究センター副センター長	対話型生成AIのエンジニアリングへの活用，対話型生成AIに対するエンジニアリング 今後の展望、あり方
対話型生成AIにより大きく変わるエンジニアリングの世界		
WG1		
山崎万丈 氏	クラウドプライバシーポリシー WG リーダー	収集される大量データに個人情報が含まれる恐れと、プライバシー侵害
生成系AIにおけるプライバシー		

本日の講演ー2　*Lectures-2*

WG講演2		
諸角昌宏 氏	AI WG リーダー	CSA本部「Security Implications of ChatGPT」（日本語版：ChatGPTのセキュリティへの影響）解説、CSA Japanの取り組み
CSAが取り組む生成AIのセキュリティ		
主催者講演		
大和俊彦 氏	日本クラウドセキュリティアライアンス副会長、 株式会社アイティアイ 代表取締役、 日本ネットワークセキュリティ協会副会長	ChatGPTのインパクトと、今後の可能性と活用
ChatGPTが加速するAI活用		

Long Social Distancing

[CSA Japan Summit 2023 の開会挨拶より]

❗ Covid-19終息後ソーシャルディスタンスはどうなるか：
「完全に元に戻る」という回答は41%　※

➡ 全体：　情報（とその伝搬）力は、増々強大化
さらに、ChatGPTの急拡大…（判りにくい）うそもつく、

➡ 個人：　サービス経済からモノ経済への回帰
需要不足ではなく、供給（力）の不足、

➡ 企業：　脱グローバル化
供給網の安全化と安定化。

※ https://bfi.uchicago.edu/insight/finding/long-social-distancing/

課題　*Issues to consider*

ChatGPTを含めた大規模生成AIモデル（Large Generative AI Models、LGAIMs）の課題

- データの保護とプライバシー対策：　大量データに含まれる恐れと、その個人情報がどの程度、どのような形で出力されるのかが不明、
- 学習データそのもののバイアスが出力に反映される可能性
- 内部動作や仕組みの説明可能性や透明性の確保が困難：　規制、監視も難しい、
- 有害なデータやコンテンツが含まれる可能性：　コンテンツモデレーション（不適切なものの監視・削除）は誰がどのように、どの段階で行われるべきか。

一旦拡散した汚染情報は、回収不可能。さらに汚染の基に、、

※　例えば，*https://xtech.nikkei.com/atcl/nxt/column/18/02560/082300002/?n_cid=nbpnxt_mled_itmh*

感謝　Thanks to

特別協賛：　CSA本部、
CSAアジアパシフィック本部

スポンサー：　株式会社JSOL

https://www.cloudsecurityalliance.jp

是非、積極的なご参加を！

Join us and let's work together!