ITセキュリティからサイバー領域へ

脅威を持続的に研究するWGリーダー
甲斐根　功

ご挨拶

甲斐根　功(カイネ　イサオ)
JNSA 脅威を持続的に研究するWGリーダ

株式会社日立システムズ

セキュリティリスクマネジメント本部
サイバーセキュリティテクニカルR&Tセンタ所属
(兼)日本サイバー犯罪対策センター(JC3)職員等

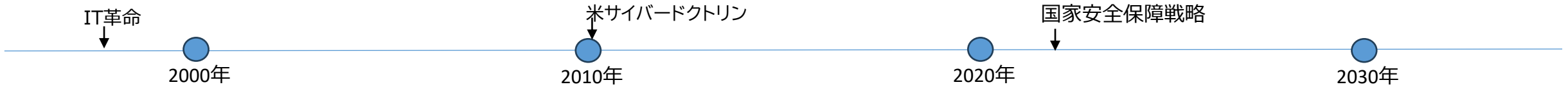
■ 略歴

2005年　日立情報システム(現日立システムズ)入社
2015年　官民人事交流法に則り、霞ヶ関に出向
2018年　日立システムズ帰任
2018年　JNSA 脅威を持続的に研究するWGリーダー
　　日本サイバー犯罪対策センター(JC3)職員兼務
2020年　JC3暗号資産PJ主査
2022年　近畿管区警察局サイバーセキュリティテクニカルアドバイザー

サイバー攻撃とセキュリティ

サイバー攻撃とセキュリティの変遷

サイバー攻撃の動向



	いたずら	功名な犯罪	実世界への影響/テロ
目的	愉快犯	金銭・情報窃取、事業妨害	世間誘導/偽情報
攻撃者	技術者	国家レベルの作成、プロの犯罪組織化、分業化	
対象	不特定多数	標的国家、企業、社会インフラ、グローバル化	
攻撃内容	マルウェアばら撒き、WEB改ざん	標的型諜報攻撃	ランサムウェア SNS/AI悪用

セキュリティの動向

日本	ＩＴセキュリティ時代	サイバー領域時代？
世界	ＩＴセキュリティ時代	サイバー領域時代

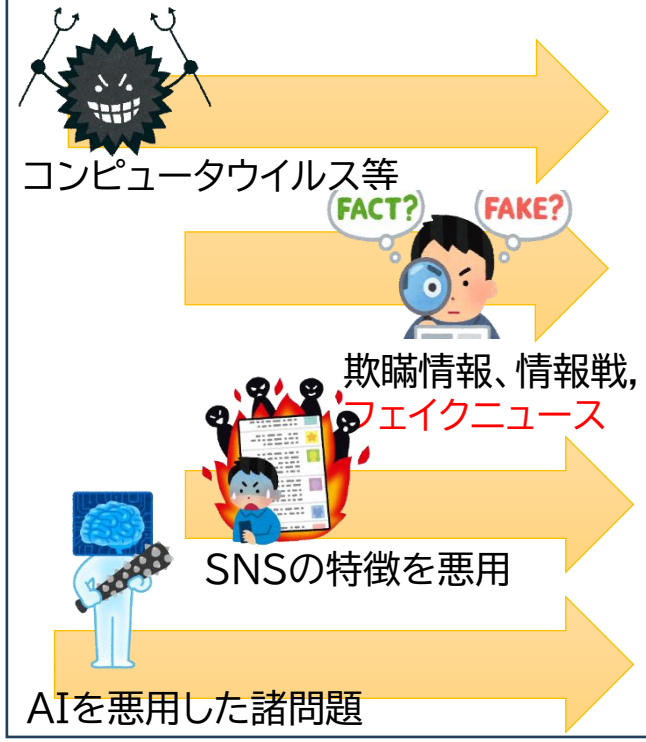
サイバー領域とは

セキュリティ＋サイバー領域

従来のセキュリティ対策のみでなく、サイバー領域（空間）全体の問題（戦術・影響等）への対応が必用な時代

従来

現在

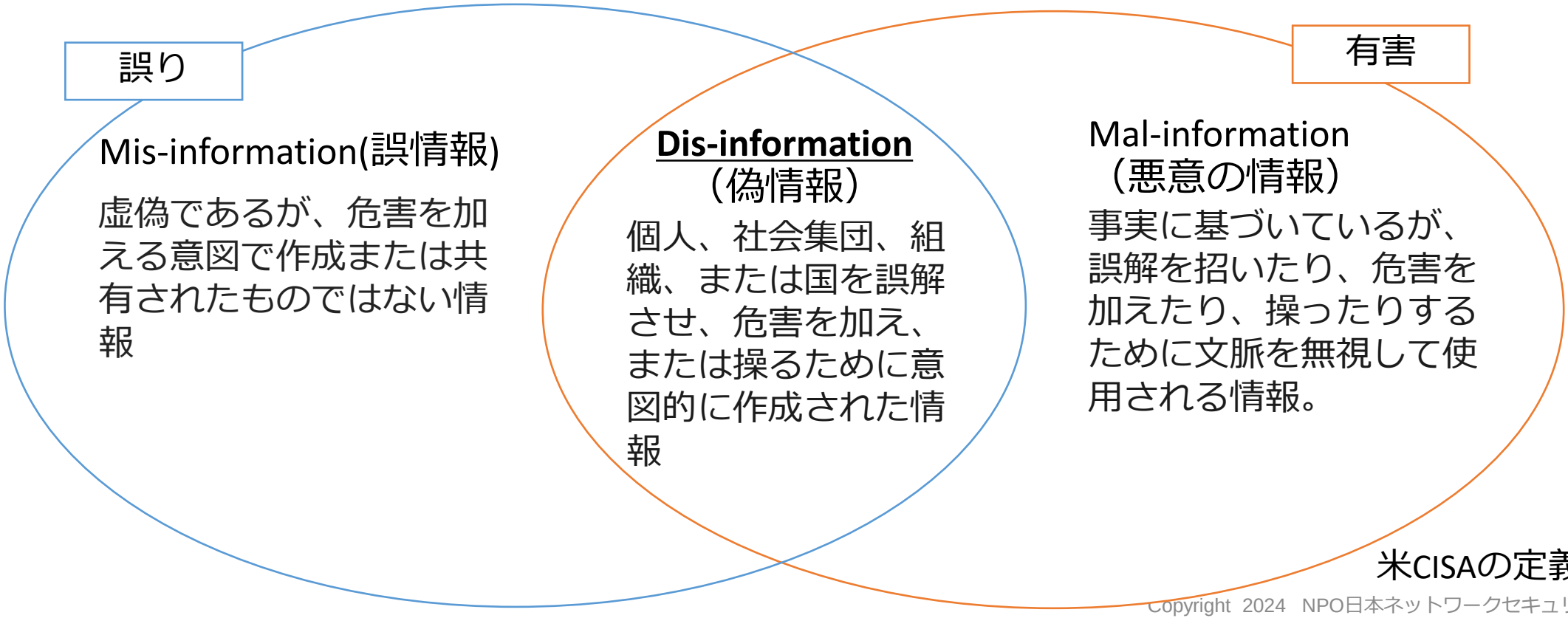


- 従来のセキュリティ対策
- 法執行機関・国際連携
- 改訂安保戦略の理解と対応
- BCP・BCMの整備

フェイクニュースと偽情報

- 「フェイクニュース」という言葉の定義に関して は世界的に議論があり、一般的な定義は難しい
- 政策文書ではdisinformation（偽情報）、misinformation（誤情報）という表現が用いられるようになっている。

https://www.soumu.go.jp/main_content/000668595.pdf



米CISAの定義による

ロシアによるものとされる偽情報

ゼレンスキー大統領の信用を失墜させることを目的としたロシアによる偽情報

“ゼレンスキーは西側から金を吸い取るブラックホール”だという俗説を広げ

- EU および各国からの財政援助の提供を損なう。
- SpaceX 社からの援助の提供を弱体化させる。
- 西側諸国からの軍事的および技術的援助の提供を弱体化させる。
- ウクライナ復興のための西側プログラムの信用を傷つける

スペイン

ドイツ

米国

ウクライナのCenter for Countering Disinformation(偽情報対策センター)は、外務省の支援を得て、国際パートナー間での偽情報キャンペーンへの対応実施
情報プラットフォーム(SNS等)上で積極的に削除、初期段階で対応が完了したため、影響は少なかったものと考えられる

https://cpd.gov.ua/en/report/analytical/

ロシアによるものとされる偽情報

ゼレンスキー大統領の信用を失墜させることを目的としたロシアによる偽情報

ディープフェイク

偽の契約書画像

パリのブガッティ販売店の実在しない従業員が登場し、オレーナ・ゼレンスカが6月7日に新型モデル「ブガッティ・トゥールビヨン」を450万ユーロ（約480万ドル）で購入したと主張

また、親ロシア派でドナルド・トランプ支持の活動家によってSNSを介して拡散するなど、合計1200万人が閲覧した。

ロシアによるものとされる偽情報

国際社会から見限られた、とのウクライナ国民への誤解を与える事を狙った

ロシアによる偽情報

「日本はもうウクライナ支援に疲れている」というメッセージをウクライナ国内に向けて、送る狙いがあると考えられる。(ロシア下院議員とされる者が、Telegramに投稿されたものがTwitterでも拡散)

SNS上で数十万回以上、閲覧されていたと報告されている

偽情報とAI、SNSの課題は密生に絡み合う

偽情報(**Dis-information)**

密接に絡み合う問題

AIを悪用した諸問題

SNSの特徴を悪用

サイバー領域時代では、様々な問題が密接に絡みあう
多角的な視点で、問題に対処していく必要がある

米国選挙におけるディープフェイクの位置づけ

米国選挙においては、ディープフェイク等の規制が始まっている

■州法による規制

カリフォルニア州	**2019年**	**AB730法案**
テキサス州	**2019年**	**SB751法案**
ワシントン州	**2021年**	**SB5152法案**
ミネソタ州	**2023年**	**HF1370法案**

■ 審議中の州(2024年3月時点)

フロリダ州	**SB850**
イリノイ州	**SB1742**
ケンタッキー州	**HB45**
ニューハンプシャー州	**HB1596**
ニュージャージー州	**A5510**
ニューヨーク州	**A7106A**
オハイオ州	**HB367**
サウスカロライナ州	**H4660**
ウィスコンシン州	**SB644**

■連邦法

2020年　「敵対的生成ネットワークの出力の識別に関する法律」
IOGAN法: Identifying Outputs of Generative Adversarial Networks Act

米国における偽情報（Dis-information）の位置づけ

米国における選挙システムは重要インフラ指定

選挙に関する偽情報（Dis-information）
　サイバー攻撃を通じた選挙に対する介入は、
　　広義の国家・政府に対するサイバー攻撃

　米国ではとっくに、ITセキュリティだけの時代ではない

日本における偽情報（Dis-information）への対応

偽情報に関する検討が始まっている

資料1－1

広島AIプロセスについて

総務省
2023年12月

広島AIプロセスの本年の成果とりまとめに向けた G7デジタル・技術大臣会合の結果 3

3．高度なAIシステムを開発する組織向けの広島プロセス国際行動規範
- 10月30日に公表した国際行動規範を支持する声明を発出している組織をG7として歓迎。
- 幅広い支持を得るために、より多くの組織への働きかけを継続することを確認。

4．偽情報対策に資する研究の促進等のプロジェクトベースの協力
- OECD,GPAI及びUNESCO等が実施する「生成AI時代の信頼に関するグローバルチャレンジ」の取組を歓迎。生成AIを用いて作成される偽情報の拡散への対策に資する技術等の実証を実施。
- 設立予定のGPAI東京センターを含め各国政府や民間企業等による広島AIプロセス国際指針及び行動規範の実践をサポートするための生成AIに関するGPAIプロジェクトの実施を歓迎。（例：コンテンツの発信元の識別を可能とするコンテンツ認証・来歴管理メカニズム）

広島AIプロセス G7デジタル・技術閣僚声明における主な成果② - 広島AIプロセス推進作業計画

◆ G7として、以下の項目の「**広島AIプロセスを前進させるための作業計画**」についても合意。

1．広島プロセス国際指針及び行動規範への**賛同国増加に向けたアウトリーチ**
2．企業等による**国際行動規範への支持拡大**及び**企業等による国際行動規範履行確保のための モニタリングツールの導入に向けた取組**の実施
3．グローバル・チャレンジやその他の潜在的な機会を通じた、**OECD、GPAI、UNESCOとのプロジェクトベースの協力の継続**

これらの他、以下の取組を推進。

- 関連国の政策動向及び国際行動規範にコミットする組織のリストに関する最新情報等を提供する **広島AIプロセス専用ウェブサイトの立ち上げ**
- マルチステークホルダーコミュニティとの対話促進を通じた、広島AIプロセスの成果の推進
- **OECDに対して**既存のAIの取組みにおいて**広島AIプロセスの成果を考慮するよう奨励**
- **OECD、GPAI及び国連等の多国間の場**における協調と協力の強化による**広島AIプロセスの更なる前進**

https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/11hiroshimaaipurosesu.pdf

日本も既に、ITセキュリティだけの時代ではない

まとめ

まとめ

偽情報（Dis-information）を例に、拡大サイバー領域分野をご説明

日本においても、IT(情報)セキュリティの時代は終わり

従来のセキュリティ対策のみでなく、サイバー領域(空間)全体の問題(戦術・影響等)への対応が必用な時代となている

ご清聴ありがとうございました