TLP:CLEAR

2023年に大きく変化したサイバー脅威とそれらに適応するための努力方法

2023年 11月

名和 利男

アジェンダ

1. サイバー脅威ランドスケープとは
2. 2023年のサイバー脅威ランドスケープ（企業向け）
3. 2023年のサイバー脅威ランドスケープ（国家機関向け）
4. 2023年のサイバー脅威ランドスケープ（技術者向け）
5. 2023年のサイバー脅威から得るべき教訓

トピック１

サイバー脅威ランドスケープとは

ランドスケープ(Landscape)とは

- 【文学領域】視覚芸術(特に絵画)のように、視覚的なシーンを眼で追う動きを強調したもの。
  - 古風な表現の「ランドスキップ(Landskip)」は、絵画を見るときのような情景を横切る視線の動きを表している。
  - 風景として描写した身体的なイメージの比喩的使用は、西洋思想において基礎的な役割を果たしており、読者(相手)に伝えうる意味の深さと多様性を与えている。
- 【文学理論と記号論に触発された領域】主体(者)、行動、対象を構成要素としたテキストとして読まれるもの。
  - 主観的な人間の経験を通じて媒介された外部世界を示し、地理的な地域よりも個人や社会の感情的反応と結びついている。
  - 社会的プロセスを通じて形成または変化する認識を具現化する視覚的空間とみなされる。

1930 年代の銀座

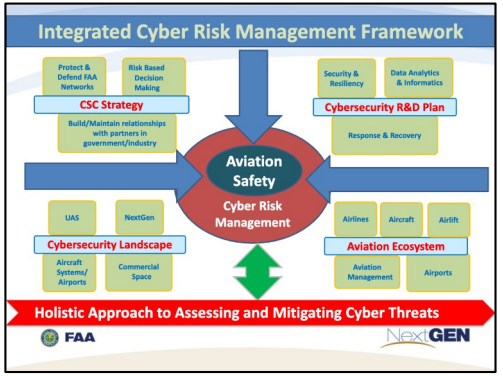
現在の銀座

TLP:CLEAR

サイバー脅威ランドスケープ（Cyber Threat Landscape）

- 【意味】個人、企業、特定の産業、ユーザーグループ、ネットワーク、特定の時間枠内で影響を受け得る潜在的なサイバーセキュリティの脅威全体を指す。
  - 脆弱性やマルウェアなどの（脅威の主体となる）攻撃者の技術など。
  - 日々新たな脅威が出現したり、既存のものが進化したりするなど、常に変化している。
- 【目的】組織のデジタルセキュリティ姿勢を包括的に評価するため。（特に、組織が直面しうる潜在的なサイバー脅威を特定し、分析し、優先順位を付けるため。）
  - サイバー脅威ランドスケープの分析を通じて、情報セキュリティの問題を予見し、組織の情報セキュリティ戦略に積極的な姿勢をとらせる。
  - 組織の情報セキュリティリスクとセキュリティ侵害の潜在的影響を理解するのに不可欠であり、これらの脅威に効果的に対応し、対策を講じるために重要である。

https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030



https://www.faa.gov/sites/faa.gov/files/2022-05/508_AirportsREDACRDPlanBriefing.pdf

TLP:CLEAR

「サイバー脅威ランドスケープ」の利用シーン（1/3）

- 「サイバー脅威ランドスケープ」は、絶えず動的に進化している。そのため、この利用シーンにおいては、継続的なプロセスを前提としている。
  - 組織や個人（意思決定者）が、最新の脅威について情報を得て、セキュリティ対策が最新の状態であることを確認するために、頻繁に参照する。
  - 狙いは、サイバー脅威に対する予防的な防御を可能にし、サイバーインシデントのリスクと影響を最小限に抑えることである。
  - 組織が直面する可能性のあるサイバー脅威を包括的に把握する上で不可欠な要素である。

TLP:CLEAR

「サイバー脅威ランドスケープ」の利用シーン（2/3）

- セキュリティ戦略の開発（策定）
  - 組織は、サイバー脅威ランドスケープを理解することで、サイバーセキュリティ戦略と防御を開発（策定）及び適切に更新する。
- 脅威インテリジェンス
  - サイバーセキュリティ専門家や脅威インテリジェンスチームは、新たに出現する脅威を特定し、潜在的なリスクについて助言するためにランドスケープを評価する。
- セキュリティ運用
  - セキュリティオペレーションセンター（SOC）において、継続するサイバー脅威に備え、それらを監視し、対応するためにランドスケープを使用する。
- 政策立案
  - 政策立案者は、サイバー脅威から市民やインフラをよりよく保護するための規制や政策を策定する際に、サイバー脅威ランドスケープを参照する。

「サイバー脅威ランドスケープ」の利用シーン（3/3）

- 意識向上と教育
  - ビジネスや一般市民にサイバーセキュリティの重要性について認識を高めるために、この文脈で議論する。
- リソース配分
  - 組織（特に企業）は、サイバー脅威ランドスケープからの洞察を用いて、最も緊急なサイバーセキュリティの課題に対してリソースを優先的に配分する。
- リスク管理
  - リスク管理の文脈において、サイバー脅威ランドスケープを理解することで、異なるサイバー脅威の可能性と潜在的影響を評価するのに役立つ。
- インシデント対応計画
  - 組織は、サイバー脅威ランドスケープ内で最も発生可能性の高い、または危険なサイバー脅威に基づいてインシデント対応計画を準備する。

トピック 2

2023 年のサイバー脅威ランドスケープ（企業向け）

2023年のサイバー脅威ランドスケープ（企業向け）

生成 AI の影響

- 生成 AI はサイバーセキュリティ分野に大きな変化をもたらしており、脅威の検出と自動応答の向上を提供する一方で、新たな脆弱性をもたらしている。
- AI システムを標的とした敵対的攻撃、データ汚染、モデル反転などのリスクが増加している。

地政学的要因の影響増大

- 欧州や東アジアの地政学的状況がサイバー脅威環境を形作っている。
- これらの要因は、効果的にサイバーセキュリティ投資を優先するための組織の戦略に影響を与える。

サイバー犯罪の経済規模拡大

- サイバー犯罪の増加は指数関数的であり、2023 年の犯罪コストは 8 兆ドル（1,080 兆円）に達すると予測されている。
- オンラインでの不正活動の増加しているため、金銭的損失から身を守るためのセキュリティ対策の強化が必須となる。

新たな脅威の出現

- 組織が対処しなければならない新しい脅威が絶えず出現（増加）している。
- たとえば、生成 AI ツールの発売や地政学的な脅威の高まりが、サイバーセキュリティの専門家にとって最大の懸念事項の一つとなっている。

サイバー攻撃の洗練化

- 昨年（2022 年）から適応性が高く洗練された脅威が急増し、サイバー攻撃者は容赦なく、より速く、より複雑な攻撃方法を使用している。
- サイバー攻撃の急速な発展により、企業は攻撃に適合した回復力を獲得し、警戒を怠らない努力を増強しなければならない。

TLP:CLEAR

2023年のサイバー脅威ランドスケープ（企業向け）

生成 AI の影響

- 生成 AI はサイバーセキュリティ分野に大きな変化をもたらしており、脅威の検出と自動応答の向上を提供する一方で、新たな脆弱性をもたらしている。
- AI システムを標的とした敵対的攻撃、データ汚染、モデル反転などのリスクが増加している。

https://www.darpa.mil/news-events/2023-08-09

DARPA AI サイバーチャレンジは国家の最も重要なソフトウェアのセキュリティ保護を目指す（2023年8月9日）

- AI とサイバーセキュリティの結びつきでイノベーションを推進することを目的とした 2 年間のコンテスト
- DARPA の専門家は、大規模なシステムを保護できるツールが不足しているため、サイバー攻撃に対して特に脆弱であると述べている。
- 重要なソフトウェアを大規模に自動的に防御することで、国全体、そして世界全体のサイバーセキュリティに最大の影響を与えることができる。

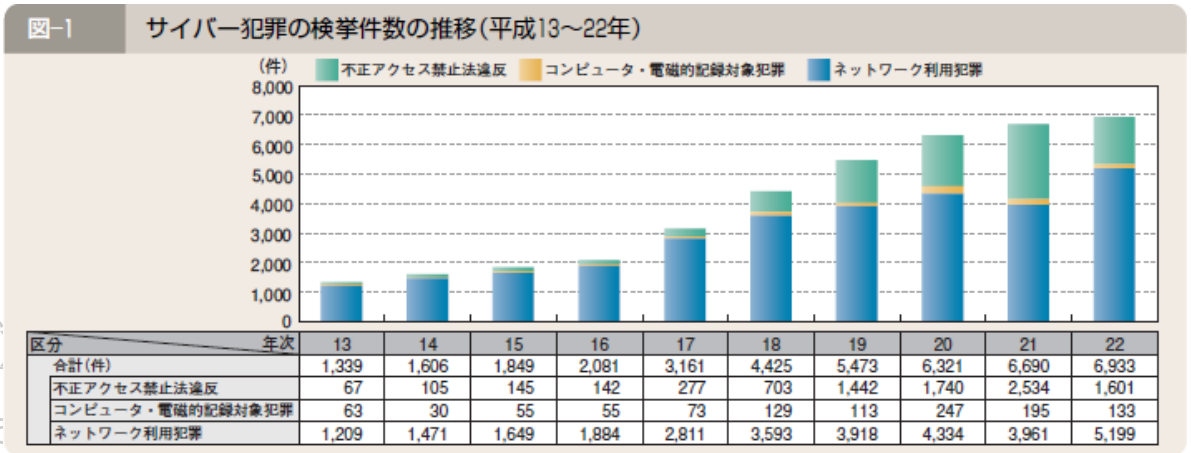
TLP:CLEAR

2023年のサイバー脅威ランドスケープ（企業向け）

サイバー犯罪の経済規模拡大

- サイバー犯罪の増加は指数関数的であり、年の犯罪コストは８兆ドル（1,080 兆円）と予測されている。
- オンラインでの不正活動の増加している的損失から身を守るためのセキュリティ対策の強化が必須となる。

平成 23 年度 警察白書



区分＼年次	13	14	15	16	17	18	19	20	21	22
合計（件）	1,339	1,606	1,849	2,081	3,161	4,425	5,473	6,321	6,690	6,933
不正アクセス禁止法違反	67	105	145	142	277	703	1,442	1,740	2,534	1,601
コンピュータ・電磁的記録対象犯罪	63	30	55	55	73	129	113	247	195	133
ネットワーク利用犯罪	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199

https://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_1_1.html

- インターネットその他の高度情報通信ネットワークは、国民生活の利便性を向上させ、社会・経済の根幹を支えるインフラとして機能している。
- その一方で、サイバー犯罪は年々その深刻さを増している状況にある。

TLP:CLEAR

2023年のサイバー脅威ランドスケープ（企業向け）

サイバーセキュリティの脅威、2030 年に向けて急展開（2023 年 11 月 11 日）

- ENISA 事務局長の ユハン･レパッサール氏の発言：
  「将来のリスクの軽減は延期したり回避したりすることはできません。だからこそ、将来を洞察することが最良の保険プランなのです。格言にあるように、『予防は治療より優れている』のです。2030 年以降のサイバーセキュリティ状況の改善に向けて、長期にわたってレジリエンスを確実に高めるために、可能な限りあらゆる措置を事前に講じる責任があります。」

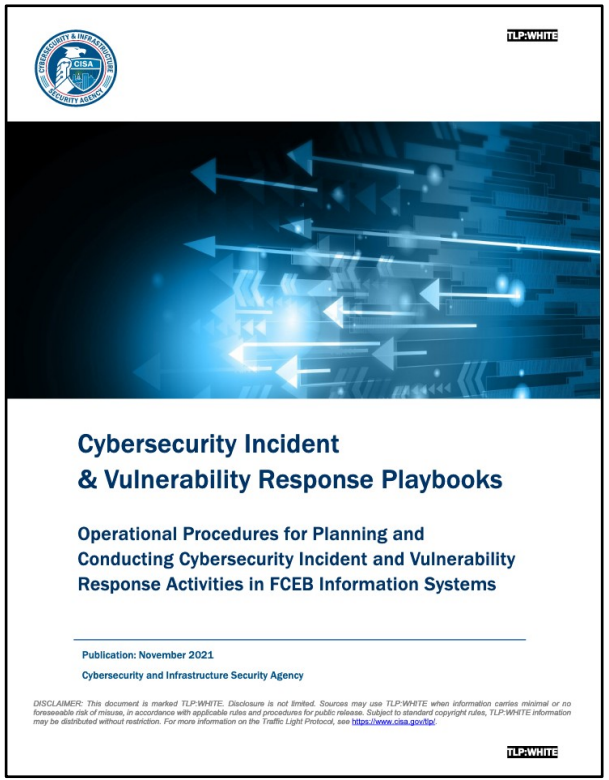
https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

サイバー攻撃の洗練化

- 昨年（2022 年）から適応性が高く洗練された脅威が急増し、サイバー攻撃者は容赦なく、より速く、より複雑な攻撃方法を使用している。
- サイバー攻撃の急速な発展により、企業は攻撃に適合した回復力を獲得し、警戒を怠らない努力を増強しなければならない。

TLP:CLEAR

2023年のサイバー脅威ランドスケープ（企業向け）



https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

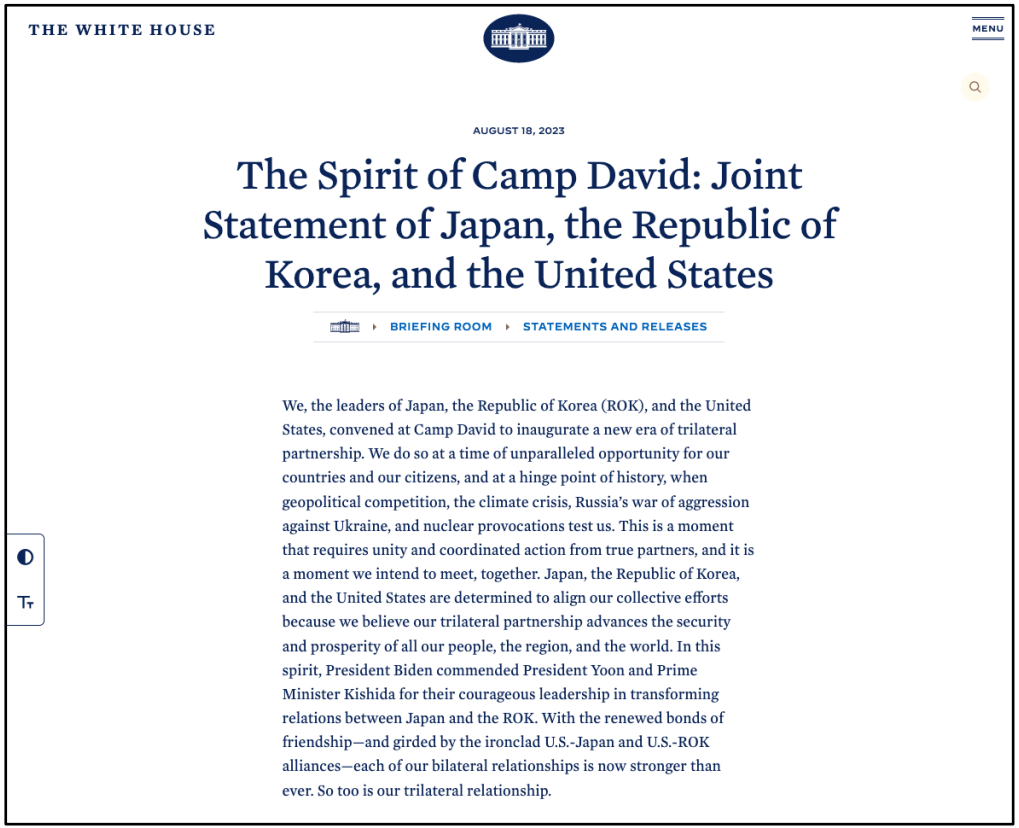
新たな脅威の出現

アクティブ・ディフェンス

- 進んだ防御能力とスタッフ（人材）を有していれば、敵をサンドボックスやハニーネットシステムに誘導する能力のようなアクティブディフェンス能力を確立することができる。
- 敵が機関の正当なインフラストラクチャを発見する能力を遅らせるために、「ダークネット」を利用することもできる。
- ネットワーク防御者は、ハニートークン（架空のデータオブジェクト）や偽アカウントを導入し、悪意ある活動の警告鳥（カナリア）として機能させることができる。
- これらの能力により、防御者は敵の行動や TTP（戦術、技術、手順）を研究し、敵の能力の全体像を構築することができる。

TLP:CLEAR

2023年のサイバー脅威ランドスケープ（企業向け）



THE WHITE HOUSE

MENU

AUGUST 18, 2023

The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States

BRIEFING ROOM › STATEMENTS AND RELEASES

We, the leaders of Japan, the Republic of Korea (ROK), and the United States, convened at Camp David to inaugurate a new era of trilateral partnership. We do so at a time of unparalleled opportunity for our countries and our citizens, and at a hinge point of history, when geopolitical competition, the climate crisis, Russia's war of aggression against Ukraine, and nuclear provocations test us. This is a moment that requires unity and coordinated action from true partners, and it is a moment we intend to meet, together. Japan, the Republic of Korea, and the United States are determined to align our collective efforts because we believe our trilateral partnership advances the security and prosperity of all our people, the region, and the world. In this spirit, President Biden commended President Yoon and Prime Minister Kishida for their courageous leadership in transforming relations between Japan and the ROK. With the renewed bonds of friendship—and girded by the ironclad U.S.-Japan and U.S.-ROK alliances—each of our bilateral relationships is now stronger than ever. So too is our trilateral relationship.

https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/18/the-spirit-of-camp-david-joint-statement-of-japan-the-republic-of-korea-and-the-united-states/

地政学的要因の影響増大

キャンプデービッドの精神：日本、韓国、米国の共同 声明（2023年8月18日）

- 我々は、サイバーセキュリティ及び財務健全性における能力構築の取り組みや新たな三極海洋安全保障協力枠組みを通じたものを含め、ASEAN及び太平洋島嶼国に対する地域的な能力構築の取り組みを調整し、両国が相互に強化し、大切なパートナーにとって最大限の利益をもたらすことを確保することを計画している。
- 我々は、違法な大量破壊兵器及び弾道ミサイル計画に資金を提供する北朝鮮の違法なサイバー活動について懸念を表明する。
- 我々は、北朝鮮のサイバー脅威と闘い、サイバーを利用した制裁回避を阻止するため、国際社会との協力を含む新たな三極作業部会の設立を発表する。日本、韓国、米国は、前提条件なしで北朝鮮との対話を再開することに引き続きコミットする。

TLP:CLEAR

TLP:CLEAR

トピック３

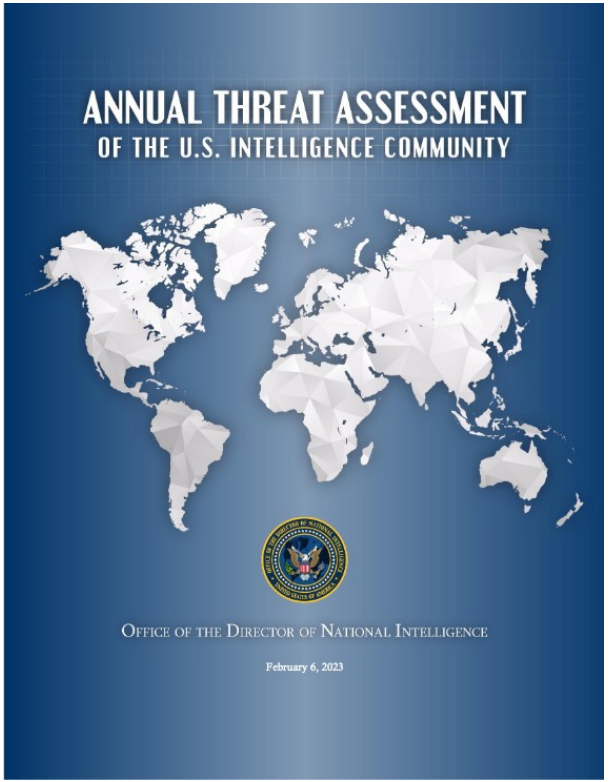
2023 年のサイバー脅威ランドスケープ（国家機関向け）

2023年におけるサイバー脅威ランドスケープ（国家機関向け）

中国

- 中国は、大規模な紛争が予想される場合、米国とその同盟国に対する積極的なサイバー作戦を検討する可能性があり、米国の軍事行動を抑止し、社会的パニックを誘発し、米軍の展開を妨害するために、重要なインフラや軍事資産を標的にする。
- 中国のサイバースパイ活動には、電気通信会社やマネージド・サービス・プロバイダー（MSP）など、情報収集や攻撃、影響力行使のための潜在的に価値のある標的を危険にさらす可能性がある。
  - 中国を拠点とする脅威アクター Storm-0558 は、2023 年 5 月、スパイ活動と推定される目的で、複数の組織の電子メールアカウントに不正アクセスした。

主な引用元：



米国国家情報長官室（ODNI）の年次報告書
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

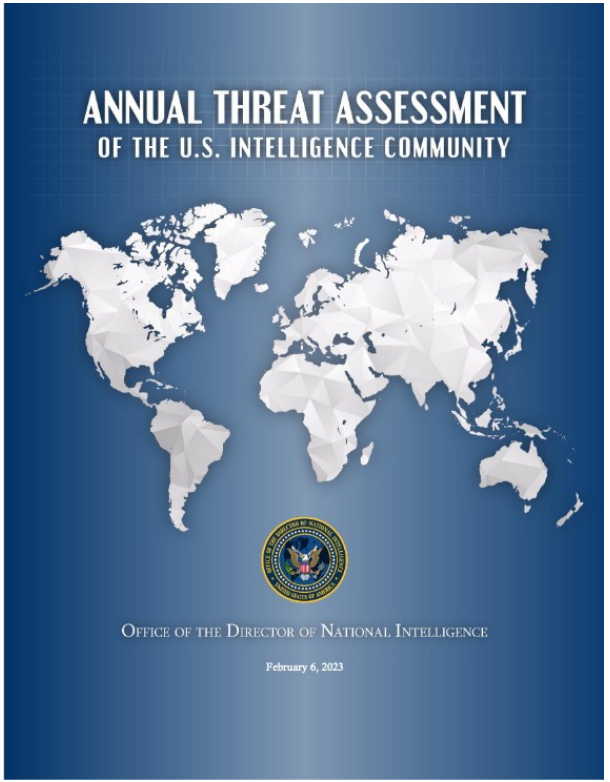
TLP:CLEAR

2023年におけるサイバー脅威ランドスケープ（国家機関向け）

ロシア

- ロシアはサイバー空間におけるスパイ活動、影響力、攻撃能力に磨きをかけ続けており、サイバー破壊を外交政策の手段とみなしている。
- 特に、米国や同盟国の海底ケーブルや産業制御システムなどの重要インフラを標的とし、危機発生時に損害を与える能力を示すことに注力している。

主な引用元：



米国国家情報長官室（ODNI）の年次報告書
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

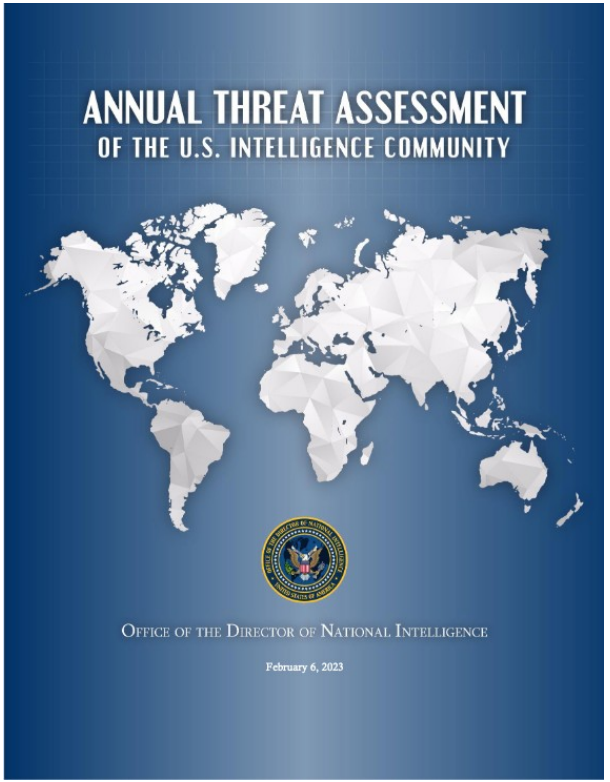
TLP:CLEAR

2023年におけるサイバー脅威ランドスケープ（国家機関向け）

北朝鮮

- 北朝鮮のサイバー能力は、サイバーエスピオナージ（スパイ活動）、金銭獲得のサイバー犯罪などを行うことができる高度で機敏な脅威である。
  - 特に、暗号通貨強奪を行う能力があり、2022 年にはシンガポールを拠点とするブロックチェーン技術企業から記録的な 6 億 2,500 万ドル（約 942 億 2,600 万円）を盗んだ。
- 金銭的な動機に基づくサイバー作戦を多様化・拡大し、高度なソーシャル・エンジニアリング技術を活用し続けている。

主な引用元：



米国国家情報長官室（ODNI）の年次報告書
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

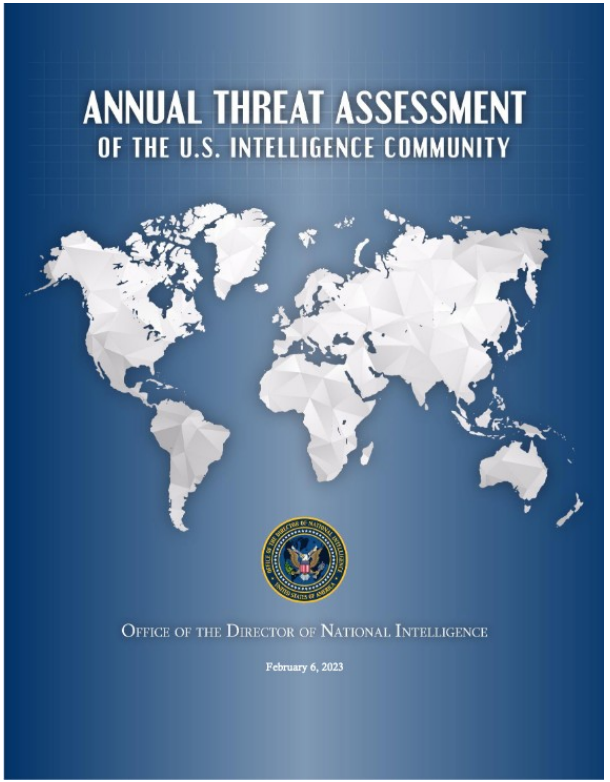
TLP:CLEAR

2023年におけるサイバー脅威ランドスケープ（国家機関向け）

イラン

- 専門知識と積極的なサイバー作戦を実施する意欲を高めており、米国と同盟国のネットワークとデータのセキュリティに重大な脅威をもたらしている。

主な引用元：



米国国家情報長官室（ODNI）の年次報告書
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

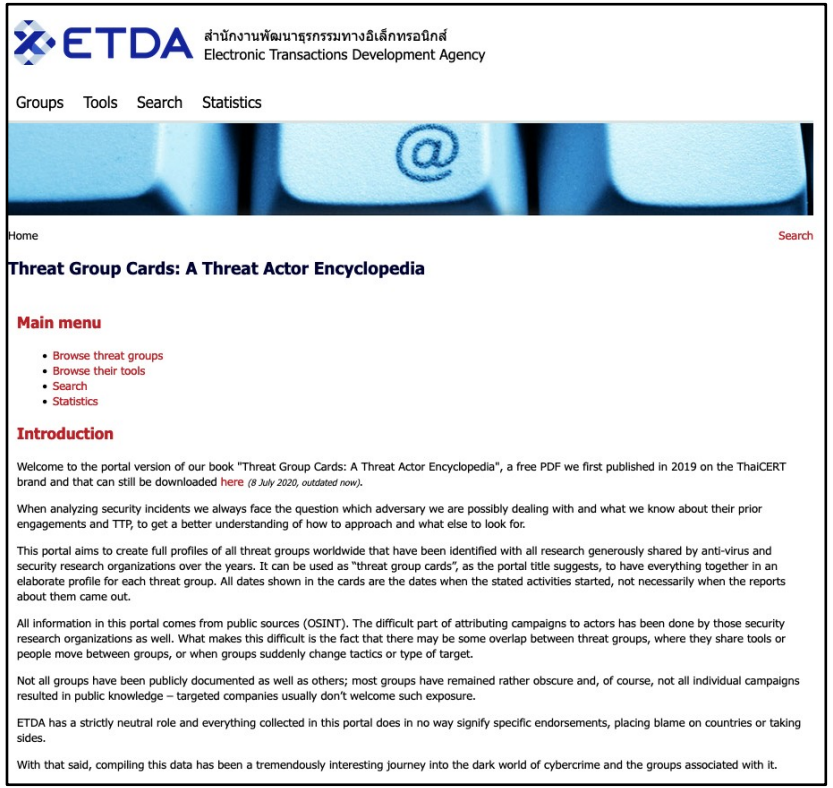
TLP:CLEAR

2023年におけるサイバー脅威ランドスケープ（国家機関向け）

その他

- Malpedia
  https://malpedia.caad.fkie.fraunhofer.de
- Alienvault OTX
  https://otx.alienvault.com
- ETDA Threat Actor Library
  https://apt.etda.or.th
- CyberMonitor
  https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
- APTNotes
  https://github.com/aptnotes
- SecureWorks
  https://www.secureworks.com/research/threat-profiles
- MITRE ATT&CK® Data
  https://github.com/mitre-attack/attack-stix-data

主な引用元：



タイ電子取引開発機構（ETDA）
https://apt.etda.or.th/cgi-bin/aptgroups.cgi

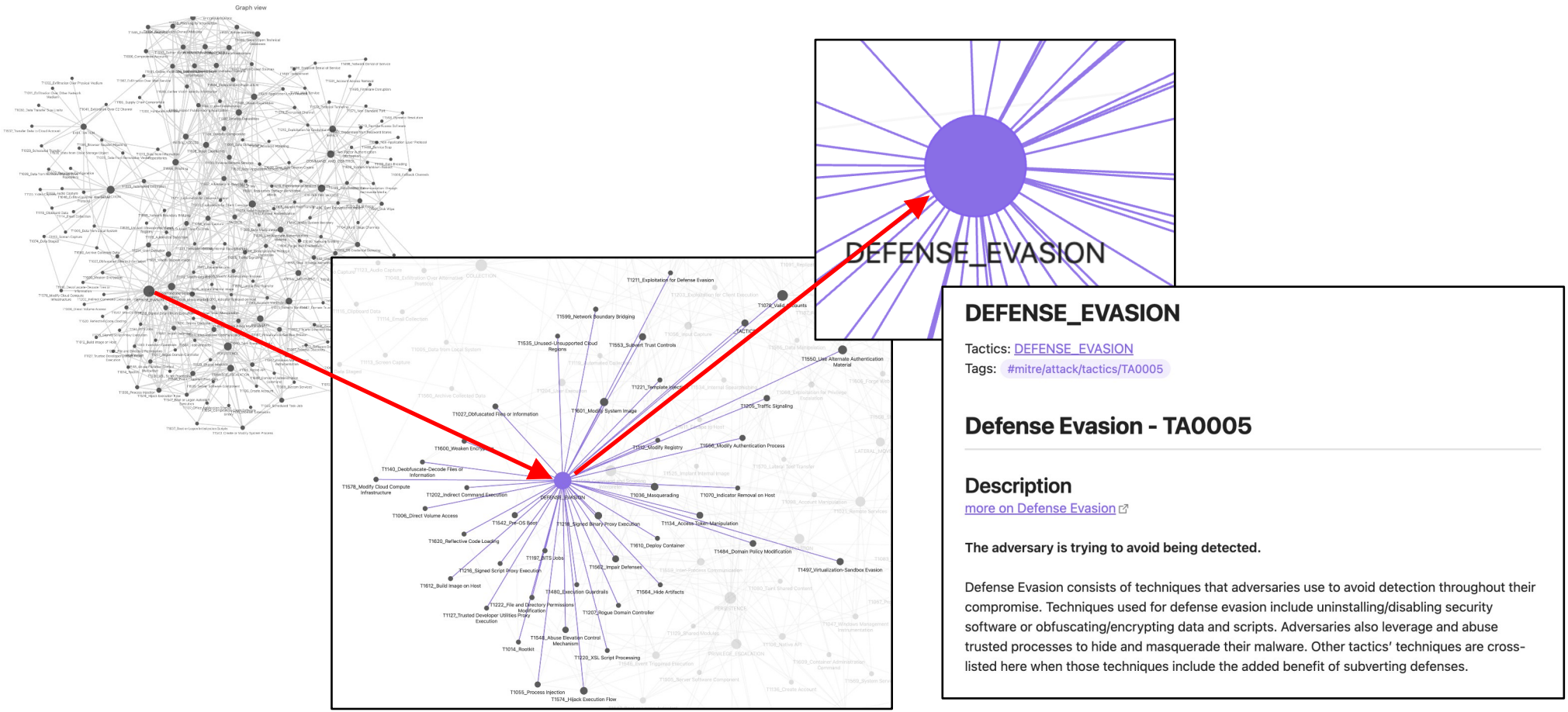
TLP:CLEAR

TLP:CLEAR

トピック 4

2023 年のサイバー脅威ランドスケープ（技術者向け）

2023年におけるサイバー脅威ランドスケープ（技術者向け）



ツール：obsidian
データ：https://github.com/6r3g/ATTACKmd

TLP:CLEAR

TLP:CLEAR

トピック５

サイバー脅威に適応するための努力方法

サイバー脅威に適応するための努力方法

- **増加する脅威**
  サイバー攻撃の頻度と洗練度が増しており、個人から企業、国家まで幅広いターゲットに影響を及ぼしている。
- **多様化する攻撃手法**
  フィッシング、ランサムウェア、ソーシャルエンジニアリング、サプライチェーン攻撃など、攻撃手法は進化し続けている。
- **防御の重要性**
  予防的セキュリティ対策、定期的なセキュリティトレーニング、インシデント対応計画の策定が不可欠である。
- **情報共有の力**
  情報セキュリティコミュニティ間での知見の共有が脅威への対応を強化する。
- **継続的な対策**
  サイバーセキュリティは一度きりの取り組みではなく、継続的な監視、評価、改善が求められる。

TLP:CLEAR

本資料に関する連絡先

名和 利男（ Toshio NAWA ）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

TLP:CLEAR