TLP:CLEAR

ウクライナ情勢で発生した「重要インフラサービス」へのサイバー攻撃のレビューと得るべき教訓

2022年 10月

名和 利男

本資料は、第 86 回運輸政策セミナーにおける講演資料(TLP:AMBER)を一般公開向けに加工したものです。

講演概要

- ロシアによるウクライナ侵攻「以前」、「直前と直後」、「以降」において、ウクライナとロシアの重要インフ ラ事業者およびそのサプライヤー等に**さまざまな種類のサイバー攻撃**の発生が観測されました。
- その中で、日本の重要インフラ事業者に理解いただきたい「**脅威アクター（攻撃者）がとった戦略・戦術・手順**」を簡潔にレビューします。
- そして、それらから得られた教訓等を示した上で、経営者自らが**従来のセキュテリィ対策のあり方を大きく変革**させていかなければならない現状（特に必要性と重要性）を考えます。

TLP:CLEAR

アジェンダ

1. ウクライナ情勢で発生した「重要インフラサービス」への
   サイバーオペレーション

2. 親ロシアのハクティビストの背景の理解と対策

3. サイバーセキュティの当事者意識が薄れる日本企業の環境

4. 重要インフラ事業者に理解していただきたいこと

TLP:CLEAR

TLP:CLEAR

トピック 1

ウクライナ情勢で発生した「重要インフラサービス」へのサイバー攻撃

ウクライナ情勢で発生したサイバー攻撃

2021 年 4 月～：「国家の利益」や「次のサイバー攻撃」に繋がる**情報窃取**

2022 年 1 月～ 2 月：ロシア軍の優位性を高める**影響工作**

侵攻開始前後：ウクライナの反撃遅延を狙った情報通信能力の**破壊攻撃**

2022 年 2 月～現在：ウクライナの重要施設内 IT システムへの**侵害攻撃**

TLP:CLEAR

ウクライナ情勢で発生したサイバー攻撃

2021 年 4 月～：「国家の利益」や「次のサイバー攻撃」に繋がる**情報窃取**

2022 年 1 月～ 2 月：ロシア軍の優位性を高める**影響工作**

侵攻開始前後：ウクライナの反撃遅延を狙った情報通信能力の**破壊攻撃**

2022 年 2 月～現在：ウクライナの重要施設内 IT システムへの**侵害攻撃**

TLP:CLEAR

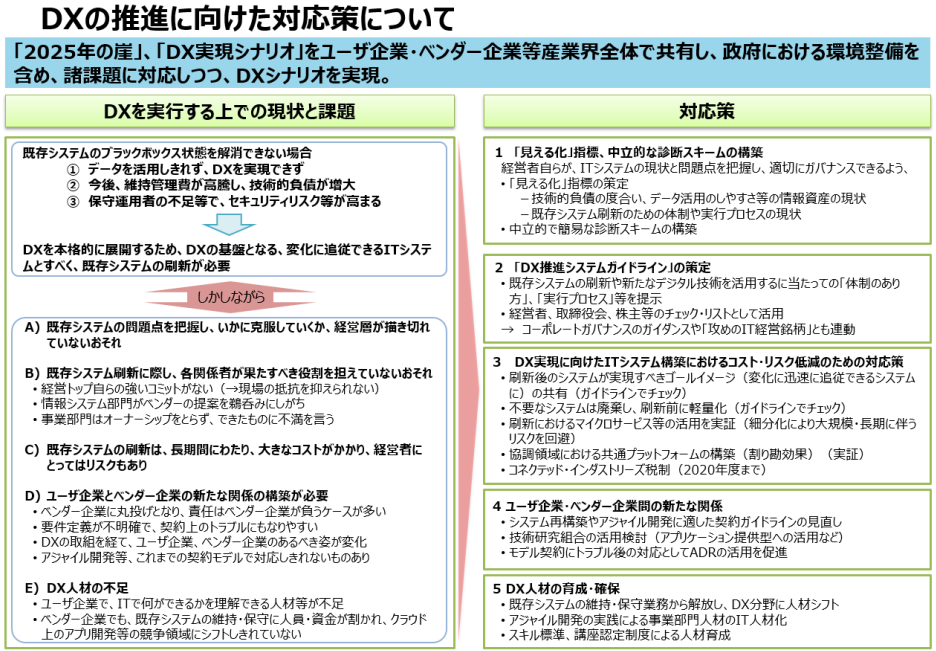
「国家の利益」や「次のサイバー攻撃」に繋がる情報窃取

- 2021 年 4 月頃から、「 Nobelium (ノベリウム)」と関連した脅威グループが、世界中の企業や政府機関を標的に、サービスプロバイダーの経由や特権アカウントの悪用などで侵害し、ロシアの利益に関連するデータを窃取していた。
  - 出典：Suspected Russian Activity Targeting Government and Business Entities Around the Globe（2021年12月6日、Mindiant）https://www.mandiant.com/resources/russian-targeting-gov-business

- 2021 年 10 月頃から、脅威グループ「 ACTINIUM (アクチウム)」が、緊急対応や領土の安全確保に重要なウクライナの組織(政府、軍隊、NGO 、司法、法執行機関)、危機的状況にあるウクライナへの国際支援・人道支援の分配調整等に関わる可能性のある組織のアカウントを標的または侵害していた。
  - 出典：ACTINIUM targets Ukrainian organizations（2022年2月4日、Microsoftの専任部門）https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

注目すべきサイバー活動のベクトルとレベル(情報窃取)

- 攻撃標的にサービスプロバイダー(クラウドサービス事業者、MSP 、再販業者等)が増加
  - IT化とDX化により、攻撃標的におけるサービスプロバイダーの利用が増加している。
  - ダウンストリームにある複数の顧客(企業)を効率よく侵害することが期待できる。



出典:産業界におけるデジタルトランスフォーメーション(DX)推進施策について(経産省)
https://www.meti.go.jp/policy/it_policy/dx/dx.html

TLP:CLEAR

注目すべきサイバー活動のベクトルとレベル(情報窃取)

- 特権アカウントや資格情報を積極的に利用したサイバー侵害が増加
  - 闇サイト(ディープ・ウェブ・マーケット等)において、ランサムウェアギャングのニーズの高い資格情報の売買が活性化しているため、以前より資格情報が調達しやすい。
  - 法人向けクラウド型メールサービスへの特権アカウントで侵害して、機密性の高いデータを取得するために、「アプリケーション偽装権限」アカウントを作成する。

注目すべきサイバー活動のベクトルとレベル(情報窃取)

- 2022 年 6 月、Digital Shadows Photon Research チームが、約 246 億の完全なユーザー名とパスワードのセットが、サイバー犯罪市場で流通している状況についてレポートした。
  - 前の調査が実施された2020年から65%増加した。
- Digital Shadows のシニア サイバー脅威インテリジェンス アナリストである Chris Morgan 氏は、「現時点で認証情報の漏洩の問題は制御不能」と見ている。

出典: 24 billion usernames and passwords available on the dark web – an increase of 65% in just two years（digital shadows_）
https://www.digitalshadows.com/press-releases/24-billion-usernames-and-passwords-available-on-the-dark-web-an-increase-of-65-in-just-two

注目すべきサイバー活動のベクトルとレベル(情報窃取)

- 侵害後に C2 通信の持続的に確立するために、住宅用 IP プロキシサービスを悪用
  - データスクレイピング(コンピュータープログラムが別のプログラムから生成された出力からデータを抽出する)等を目的とした膨大なアクセスを行うユーザや自国内のネットワークの利用が制約されているユーザが、アクセス制限を回避する(データ収集のリクエストが実際の住宅からのリクエストとしてみなされる)ために、他の地域にある住宅用ネットワークにあるホストをプロキシとしてアクセスに利用するサービスを悪用する。

ウクライナ情勢で発生したサイバー攻撃

2021 年 4 月～：「国家の利益」や「次のサイバー攻撃」に繋がる**情報窃取**

2022 年 1 月～ 2 月：ロシア軍の優位性を高める**影響工作**

侵攻開始前後：ウクライナの反撃遅延を狙った情報通信能力の**破壊攻撃**

2022 年 2 月～現在：ウクライナの重要施設内 IT システムへの**侵害攻撃**

TLP:CLEAR

ロシア軍の優位性を高める影響工作

- 2022 年 1 月 13 日、ウクライナに拠点を置く複数の政府、非営利、情報技術組織を標的に展開された WhisperGate マルウェアは、ランサムウェアのように見えるが身代金回収メカニズムがなく、身代金を要求せず、対象のデバイスを動作不能にする破壊目的のものであった。
  - 出典：Destructive malware targeting Ukrainian organizations（2022年1月15日、Mindiant）
    https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

- 2022 年 2 月 23 日、ウクライナ国内の数百台のマシンに展開された HermeticWipe マルウェアは、ランサムウェアを偽装して PC を起動できない状況にしていたことが明らかになった。2021 年 12 月にコンパイルされたものが多かった。
  - 出典：ESET research のツイート（2022年2月24日、ESET）
    https://twitter.com/ESETresearch/status/1496581904916754435
  - HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine（2022年2月23日、SentinalLab）
    https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
  - Ukraine: Disk-wiping Attacks Precede Russian Invasion（2022年2月24日、Symantec）
    https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

注目すべきサイバー活動のベクトルとレベル(影響工作)

- 「破壊的なマルウェア」と「偽のランサムウェアメッセージ」を組み合わせた攻撃は、ウクライナの組織の日常業務に直接的な脅威をもたらし、重要な資産とデータの可用性に影響を与える可能性がある。
  - 「破壊的なマルウェア」の手法は、2015年から2017年にかけて、Sandworm(ロシア軍事諜報機関GRUの一部)が、ウクライナのメディア、電気事業者、鉄道システム、財務・年金基金等の政府機関のシステムに対して発生したデータ破壊目的のTeleBotsと類似している。
  - 「偽のランサムウェアメッセージ」の手法は、2017年6月に Sandwormが、ウクライナの銀行、キエフの病院、チェルノブイリの監視やクリーンアップの設備まで、数百以上組織に機能障害を発生させ、合計100億ドルの被害をもたらしたNotPetyaに類似している。

TLP:CLEAR

ロシア軍の優位性を高める影響工作

- 2022 年 1 月 13 日から 14 日の夜にかけて、ウクライナ外務省、文部科学省、国防省、国防省、内閣府等の政府機関のウェブサイトが改ざんされた。
  - この改ざんにより、すべてのWebサイトコンテンツが消去され、ロシア語、ウクライナ語、ポーランド語で、ウクライナ人に対するメッセージに置き換えられた。
  - このメッセージにおけるポーランド語は、ロシアで有名なプラットフォーム yandex.ru の翻訳機能を使用したロシア語のメッセージの翻訳であることが判明している。

注目すべきサイバー活動のベクトルとレベル(影響工作)

- この改ざん後に表示されたメッセージは、異なる民族グループ間、特にウクライナ人と少数派のポーランド人の間に反対意見を生じさせることを目的としている。特に、最後の文は、ヴォルヒニアとガリシアのポーランド人の民族浄化の地域の人々に思い出させることを狙っている。
  - 出典:Gary Warner's Post(ゲイリーワーナー)
    https://www.linkedin.com/posts/garwarner_cyber-attacks-against-several-prominent-ukrainian-activity-6887753187915309056-CCKI/

【改ざん後に表示されたメッセージ】

ウクライナ人よ! あなたの個人情報がすべて公衆ネットワークに送信された。あなたのコンピュータのデータはすべて破壊され、回復することはできない。あなたに関するすべての情報は公開され、おとぎ話の伝わり、最悪の事態になるだろう。それはあなたの過去、未来、将来のためである。
ヴォルヒィニア、OUN UPA 、ガリシア、ポーランド、歴史的地域のために。

- 「**ヴォルヒィニア(Volhynia)**」とは、ポーランド南東部、ベラルーシ南西部、ウクライナ西部の間の中央および東ヨーロッパの歴史的地域のこと。1945年、この地域に住んでいたポーランド民族のほとんどがポーランドに追放された歴史を持つ。
- 「**OUN**」とは、1919年に優れたポーランド軍によって打ち負かされたガリツィア東部が1923年にポーランドに編入されたことに対して、不満を抱いたウクライナの退役軍人が設立したウクライナ軍事組織と、1929年に学生グループが合併したウクライナ民族主義者組織(Organization of Ukrainian Nationalists)のこと。
- 「**UPA**」とは、1941年、ドイツがソビエト連邦に侵攻した際、ドイツ軍の退役軍人である一部のOUN-B指導者が、主に元警官を集めて独自に創設したウクライナ蜂起軍(Ukrainian Insurgent Army)のこと。このUPAはウクライナ人をドイツの弾圧から守り、ソビエトのパルチザンと戦い、1943年と1944年に、ウクライナ西部の先住民族のポーランド人を民族浄化した。
- 「**ガリシア(Galicia)**」とは、現在のウクライナ南西部を中心とした地域のこと。18世紀末からポーランド最南部も含まれることもある。住民は主にウクライナ人で、西部にはポーランド人も住んでいる。1945年2月のヤルタ会談では、1919年にポーランドとソ連との国境線として定められていたカーゾン線をポーランド東部国境とすることが決定され、東部ガリツィアはウクライナ領、西部ガリツィアはポーランド領となった。

ウクライナ情勢で発生したサイバー攻撃

2021 年 4 月～：「国家の利益」や「次のサイバー攻撃」に繋がる**情報窃取**

2022 年 1 月～ 2 月：ロシア軍の優位性を高める**影響工作**

侵攻開始前後：ウクライナの反撃遅延を狙った情報通信能力の**破壊攻撃**

2022 年 2 月～現在：ウクライナの重要施設内 IT システムへの**侵害攻撃**

TLP:CLEAR

ウクライナの反撃遅延を狙った情報通信能力の破壊攻撃

- 2022 月 2 月 24 日(ロシア侵攻当日)、欧州をカバーする通信衛星ネットワークプロバイダー Viasat がサイバー攻撃を受け、欧州中央から東欧のセグメントの商業顧客の約 30,000 端末が妨害を受け、インターネットアクセスが不能となった
  - この影響により、2月24日午前5時から6時の間、ドイツのEnercon社の風力タービン設備において、衛星接続を介してインターネットに接続された5,800台を超えるシステムが影響を受け、リモートで制御および調整することができなくなった。ただし、ケーブルを介してインターネット接続する風力タービン設備への影響はなかった。
  - 出典：Viasat Investigating KA-SAT Outage Due to Potential Cyber Event（2022年2月28日、Access Intelligence）
    https://www.satellitetoday.com/cybersecurity/2022/02/28/viasat-investigating-ka-sat-outage-due-to-potential-cyber-event/

注目すべきサイバー活動のベクトルとレベル(破壊攻撃)

- Viasatへのサイバー攻撃は、設定ミスが残っていたVPNアプライアンスを悪用してKA-SATネットワークの信頼管理セグメントに不正アクセスし、多数のモデムに対して、「管理コマンド」を悪用した。
  - 使用されたマルウェアは、以前、ロシアがスパイ活動に利用したVPNFilterのステージ3の破壊的なプラグインと類似性が見られた。

ウクライナ情勢で発生したサイバー攻撃

2021 年 4 月～：「国家の利益」や「次のサイバー攻撃」に繋がる**情報窃取**

2022 年 1 月～ 2 月：ロシア軍の優位性を高める**影響工作**

侵攻開始前後：ウクライナの反撃遅延を狙った情報通信能力の**破壊攻撃**

2022 年 2 月～現在：ウクライナの重要施設内 IT システムへの**侵害攻撃**

ウクライナの重要施設内ITシステムへの侵害攻撃

- 2022 年 4 月 12 日、ウクライナの政府コンピュータ緊急対応チーム CERT-UA は、ウクライナのエネルギー施設への標的型攻撃に関連する情報セキュリティインシデントに対応するための緊急措置を行なった。
  - この攻撃者は、高電圧変電所のインフラ機能を無効にすること企てていた。
  - 被害を受けた高電圧変電所は、2回の攻撃を受けた。最初の侵害は2022年2月までに行われていた。
  - 特に、データを消去して電力をオンラインに戻す試みを遅延させる設計がされていた。
  - 出典：Кібератака групи Sandworm (UAC-0082) на об’єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)（2022年4月10日、CERT-UA）https://cert.gov.ua/article/39518

注目すべきサイバー活動のベクトルとレベル(侵害攻撃)

- 高電圧変電所の機能操作と事業会社のITインフラのデータ破壊は、2022年4月8日(金)夜に実行されるスケジュールが設定されていた。
  - スロバキアEsetと米国Microsoftの研究者の協力を受けたウクライナは、これらが実行される前に実行を防ぐことができた。
  - サイバーセキュリティ研究者らは、この攻撃は、ロシア軍の支援を受けたグループであるサンドワーム(Sandworm)により仕掛けられたと推定している。
  - ロシアの侵略以来、ウクライナに対するサイバー攻撃の中で、最も深刻なものであった。

“報奨金！ロシア GRU ハッカー 6 名(サンドワーム)の情報提供で最高 1000 万ドル。彼らは悪意のあるサイバー操作で米国の重要インフラをターゲットにしていた。”
https://twitter.com/RFJ_USA/status/1518983587697147906

TLP:CLEAR

トピック 2

親ロシアのハクティビストの背景の理解と対策

ハクティビストとは

- ハックティビスト(hacktivist)とは、**政治的な意思表示や政治目的の実現**のためにハッキングを手段として利用する行為もしくはそのような行動主義を持つ個人やグループのこと。
  - hack(ハッキング行為)とactivist(積極行動主義家)を組み合わせた造語

- ウクライナ侵攻(ロシア国内では特殊作戦)以前から、主要な親ロシアのハクティビストであるJokerDNRやBeregin は、ウクライナ軍メンバーの**個人情報を含むリーク文書の公開**などを通じて、ウクライナを標的に積極的に活動している。

- ロシア国内のプロパガンダによる影響を受ける形で、ロシア国家との関係が不明なハックティビスト**Killnet**、Xaknetiii、RahDitiv が設立され、**分散型サービス妨害(DDoS)攻撃**、**ハッキング**、**情報リーク**、**改ざん**など、ロシアを支持・支援するのためのハックティビスト型脅威活動を行っている。

Killnetとは

- 2022 年 1 月 23 日、「**DDoS 攻撃を仕掛けることができる加入者限定のツールの名称**」である Killnet が利用可能になったと、Telegram チャネルで宣伝された。
  - 宣伝メッセージ：「ユーザーは15台のコンピューターを備えた500 GbpsのボットネットをKillnetから月額1,350米ドルでレンタルでき、Killnet を使用してレイヤー3、4またはレイヤー7のDDoS 攻撃を即座に開始できる。」

- 2022年2月24日、ロシアによるウクライナ全面侵攻の影響を受けて、Killnetは**突然ハクティビストグループに変容**した。
  - Killnetの作成者は、このツールの名前を使用して、ウクライナを支持する国やロシアに反対する国に対してDDoS 攻撃を開始した。
  - Killnet は、その攻撃の唯一の目的は「ロシアに対する攻撃を阻止すること」であると主張した。

Killnetとは

- 2022 年 2 月 24 日以降、Killnet の Telegram チャネルにおいて、「**レギオン（軍団兵）- ロシア連邦のサイバー特殊部隊**」と称して、多数のグループを形成するために、プログラマー、DDoSer 、ペネトレーションテスター等を中心に、新しいメンバーを募集し始めた。
  - それぞれのグループは、スクワッド（分隊）と呼び、Killnetの司令塔によって割り当てられた標的型 DDoS 攻撃を実行する。
  - 主なスクワッドは、Mirai、Jacky、Zapя（Zarya）、Rayd、Sakurajima、DDOSGUNGで、最も活発で攻撃成果をあげているのはMiraiである。

2022年8月 モルドバ　Killnet等からサイバー攻撃を受けた背景

- モルドバは、**親ロシア派が支配している「トランスニストリア地域（沿ドニエストル共和国）」**がある。
  - この地域は、1990年代前半に「独立」を宣言し、ロシア軍の支援を受けてモルドバ共和国から離れたが、現時点で、国際的な国家承認は受けていない。

ウクライナと国境を接するモルドバと
トランスニストリア地域（赤い部分）

TLP:CLEAR

2022年8月 モルドバ　Killnet等からサイバー攻撃を受けた背景

- 2022 年 2 月 25 日 ･･･ ロシアによるウクライナ侵攻の際、当時黒海を航行していたモルドバのケミカルタンカー MV Millennial Spirit が、**ロシア軍によって砲撃**された。

- 2022 年 4 月 7 日 ･･･ モルドバ政府は、ウクライナに侵略したロシア非難し、**ロシア軍のシンボル V と Z を禁止**した。モルドバの親ロシア政党は強く抗議し、モルドバ政府が彼らの歴史を消し去ったと非難した。また、モルドバのロシア系民族が、この決定により、キシナウの第二次世界大戦の英雄墓地を破壊した。

- 2022 年 4 月 21 日 ･･･ ロシア外務省のスポークスウーマン、マリア・ザハロワとロシア上院議員のアレクセイ・プシュコフは、モルドバ政府がナショナリストのシンボルを禁止したことを**非難**した。

- 2022 年 4 月 22 日 ･･･ ロシアのルスタム・ミネカエフ少将は、ロシアによるウクライナ侵攻の目的の 1 つは、占領された沿ドニエストルとの陸路を確立することであると述べ、「**ロシア語を話す人々が抑圧されている証拠**」があると主張した。これに続いて、沿ドニエストルで実行犯不明の一連の爆発が発生した。これらは、ロシアまたは沿ドニエストル共和国による**偽旗作戦**だった可能性がある。

2022年8月 モルドバ　Killnet等からサイバー攻撃を受けた背景

- 2022 年 5 月 1 日 ･･･ 親ロシアのハクティビスト Killnet が、**モルドバの公的機関の複数の ウェブサイトを DDoS 攻撃**した。

- 2022 年 7 月 5 日 ･･･ モルドバ当局に、キシナウ国際空港、首都の市議会、国会、各省庁など 50 以上の国家機関に**爆弾を仕掛けたとする偽メール**が送信された。治安当局によると、2022 年初め以来、885 の国家機関に対する 148 件の爆予告を記録し、同年 7 月と 8 月だけで 124 件が報告された。いずれも本物ではなく、爆発物は発見されず、誰もまだ起訴されていない。しかし、空港の警備は強化され、法執行機関は警備体制を敷いている。

- 2022 年 8 月 15 日 ･･･ ロシアは「危険な検疫対象物」が含まれていると主張した後、**モルドバからのほとんどの農産物の輸入を禁止**した。しかし、禁止の本当の理由は、モルドバがロシアからの 8 月の天然ガス供給の支払いの延長を要求したためであると推定されている。ロシアには、エネルギーとエネルギーの支払いをめぐる論争において、貿易を武器として使用してきた歴史がある。

2022年8月 モルドバ　Killnet等からサイバー攻撃を受けた背景

- 2022 年 8 月 24 日 ･･･ 親ロシア派のハクティビスト Killnet の Telegram アカウントのメッセージで、**モルドバ国家財政局(FISC)のウェブサイトに問題を発生**させた。
  - Killnetは、「モルドバの心臓部を攻撃せよ！モルドバで今日何が起きた？答え: ポータル www.servicii.fisc.md に深刻な技術的問題が発生した」とロシア語で主張し、「税金請求書、税金に関する報告書、統計情報」の発行を妨害し、FISC のウェブサイトとデータベースを意図的に攻撃したと伝えた。

- 2020 年 8 月後半 ･･･ **国家情報システムに対する約 80 件の攻撃未遂(主に DDoS 攻撃)**を記録した。モルドバの情報技術・サイバーセキュリティサービス(STICS)は、「サイバー攻撃について公表された情報は、悪意を持った潜在的なハッカーに有利に働く」とコメントした。

2022年9月 日本　Killnetからサイバー攻撃を受けた背景

- 2022 年 8 月 12 日 ･･･ **モルドバ工科大学 (TUM) のチームによって開発**された TUMnanoSAT と名付けられた CubeSat が、国際宇宙ステーション（ISS）の日本実験モジュール「きぼう」から正常に展開された。

- 2022 年 8 月 18 日 ･･･ 日本政府は、大量のウクライナ難民が流入しているモルドバを支援するため、**モルドバに 10 億円（約 740 万ドル）を寄付**することを決定した。

- 2022 年 9 月 6 日 ･･･ モルドバ共和国と日本は、温室効果ガスの排出を削減し、気候変動と闘い、環境を保護するために協力するため、共同信用メカニズムに関する**協力覚書に調印**した。

2022年8月 Killnetによるサイバー攻撃の特性

- 主にレイヤー 4（トランスポート層／ SYN フラッド等）とレイヤー 7（アプリケーション層／ボリューメトリック攻撃等）の DDoS 攻撃であり、**ターゲットを混乱させるだけで、特に巧妙なものではない**。
- よく見られる **DDoS 攻撃プロセス**は、次のとおり。
  - フェーズ1：ACKフラッド、DNS増幅、IPフラグメンテーション攻撃
  - フェーズ2：IPフラグメンテーション攻撃
  - フェーズ3：ボリューメトリック攻撃とステート枯渇攻撃
- DDoS攻撃と並行して行われる**SSHハイジャック攻撃**を試行する。
  - 初期設定のまま運用されている状態にあるデバイスを標的として、ポート22（SSH）に対して10を超えるIPアドレスから「初期設定の認証情報」を使用した辞書攻撃を仕掛ける。
  - もっとも多く試行された文字列は「Root」である。一部に、「mcserver」（3D創作ゲームMinecraftサーバーの初期値の管理者ID）、「 ts3」（ゲーマー向けボイスチャットTeamSpeak3サーバーの初期値の管理者ID）が見られる。

KillnetによるDDoS攻撃への対策

- ルーマニア国家サイバーセキュリティ総局(DNSC)が、Killnet 等の親ロシアのハクティビストによる **DDoS 攻撃で利用される IP アドレス**や**セキュリティガイド**を公表している。

Document	Data	Dimensiune	
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (15.09.2022)	2022/09/15	4.67 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (detalii)	2022/06/30	3.49 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware	2022/06/30	9.43 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (02.06.2022)	2022/06/02	2.82 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (17 mai 2022)	2022/05/17	1.31 MB	Afișează
Phishing-ul bancar	2022/05/03	0.62 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (03.05.2022)	2022/05/03	8.54 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (02.05.2022)	2022/05/02	0.29 MB	Afișează
Situație site-uri cu activitate în contextul crizei Ucraina – Rusia, plus adrese IP specifice utilizate în atacuri malware (29.04.2022)	2022/04/29	0.99 MB	Afișează

https://dnsc.ro/doc/ghid

https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021

TLP:CLEAR

KillnetによるDDoS攻撃への対策

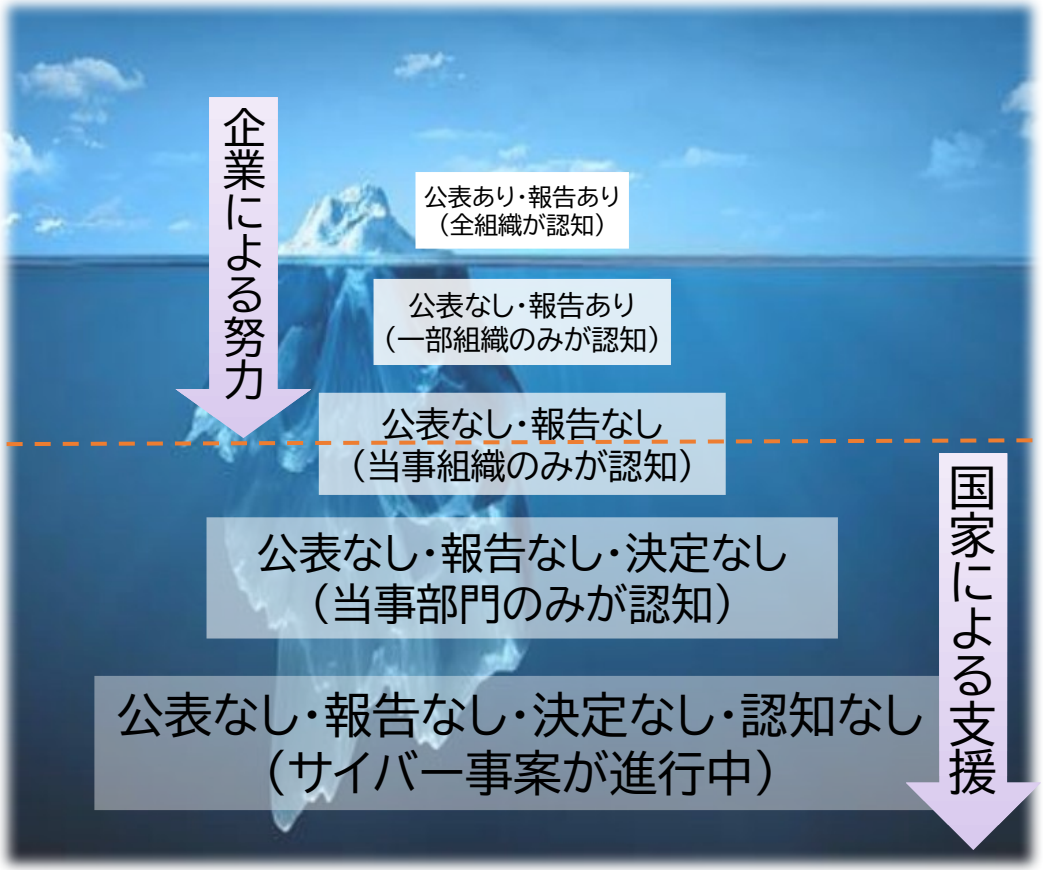
- 主要国における「国家サイバーセキュリティ機関」が公表している**サービス拒否攻撃（DDoS 攻撃）対策に関するガイド**に従う。
  - このようなガイドには、サービスの弱点の理解、サービスプロバイダーによるリソース枯渇への対応、同時セッションに対応するサービスの拡張、対応策の準備、システムの定期的なストレステストといった事前準備の努力が含まれている。
- Telegram や Twitter など、攻撃が準備や計画されている**ハクティビストグループの活動を監視**する。
- **脆弱な IoT デバイスを特定**し、SSH トンネルや DDoS ボットネットの一部として使用されないようパッチを適用する。
- IoT デバイスのデフォルトのパスワードや推測しやすい**パスワードを変更**する。
- IoT デバイスのトラフィックを監視し、分散型攻撃の一部として使用されている**デバイスを特定**する。

トピック３

サイバーセキュティの当事者意識が薄れる日本企業の環境

サイバー脅威の状況認識の獲得が難しい

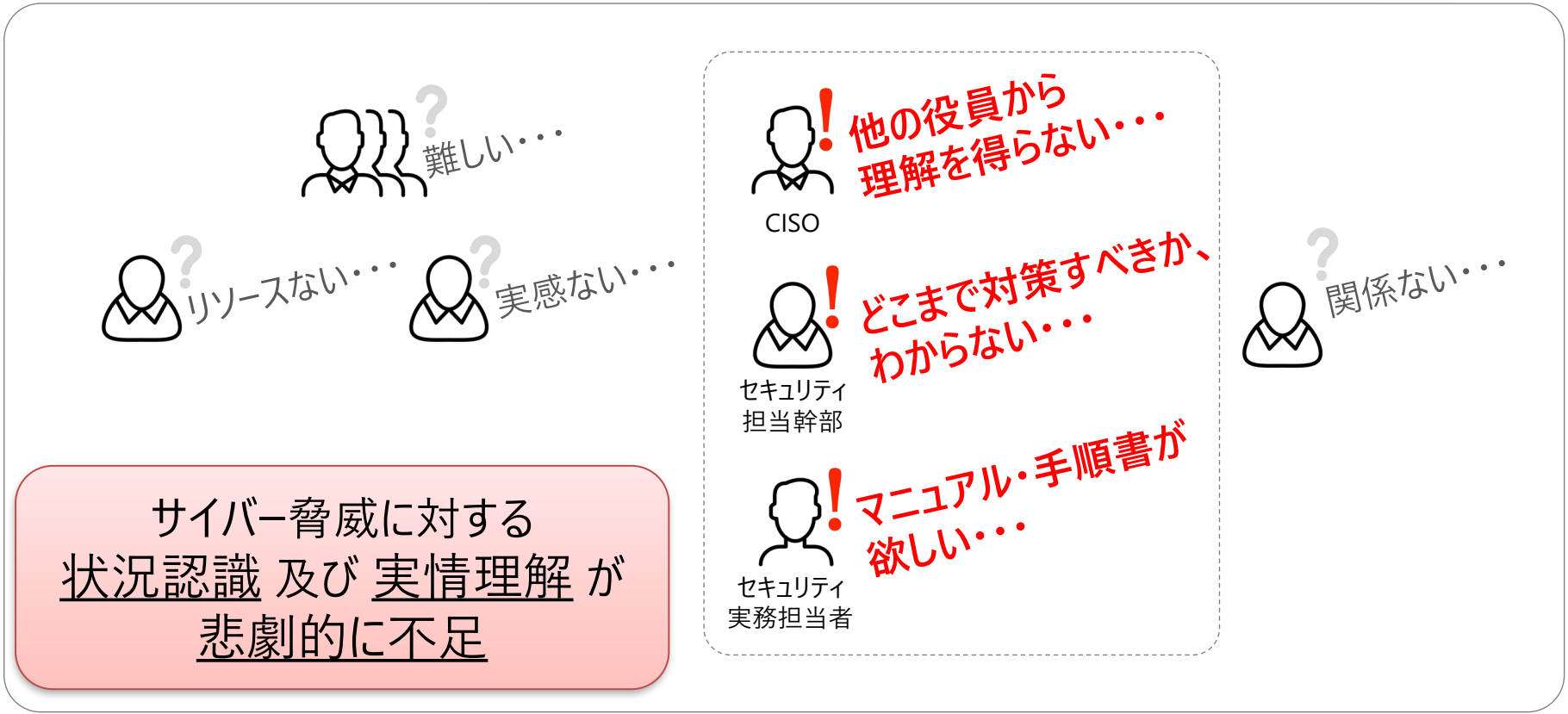
- 不特定多数に公表される「企業におけるサイバー攻撃事例」が少ない。



TLP:CLEAR

担当者への**丸投げ**

- サイバーセキュテリィ担当を決めて、**（ほぼ）丸投げ**している。



TLP:CLEAR

方向性の異なる対処

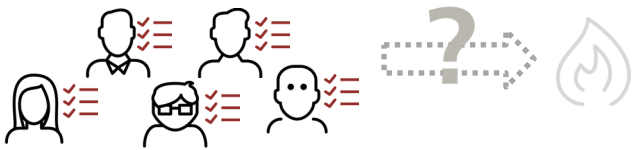
- 情報セキュリティの管理策（英語では Security Control）の影響により、セキュリティ対策における実行主体の性質が「体制」をベースにしている。
- サイバー攻撃対処の観点においては、「態勢」でなければならない。
- それぞれにおいて**取るべき行動の準備姿勢が大きく異なる**。

– **態勢**: 事態に対処するための準備ができている状態のこと。（**前もっての身構え**）

本当に事態対処できるかどうかが重要

– **体制**: 基本原理・方針によって秩序づけられている組織のこと。（**政治支配の様式**）

組織内の役割分担（責任所在）が重要



TLP:CLEAR

情報(資産の)保証に偏重したセキュリティ対策

- サイバー攻撃の重点事項は、CND（Computer Network Defense）概念に基づく「システムによる多層的な防御」である。
- IT（Information Assurance）概念に基づいたセキュテリィ対策は、「情報資産の単層的な防御」になりがちである。

（IAを重点事項にした場合、システム管理者に対し「適切に・・・せよ」という現場任せの指示になりやすい。）

- 「外部漏洩させない」ためのセキュリティ対策
- 「IA的なインシデント ＝ **情報漏えい**」
- 攻撃プロセスの後半で認識
- システム所有者（発注者）が対応

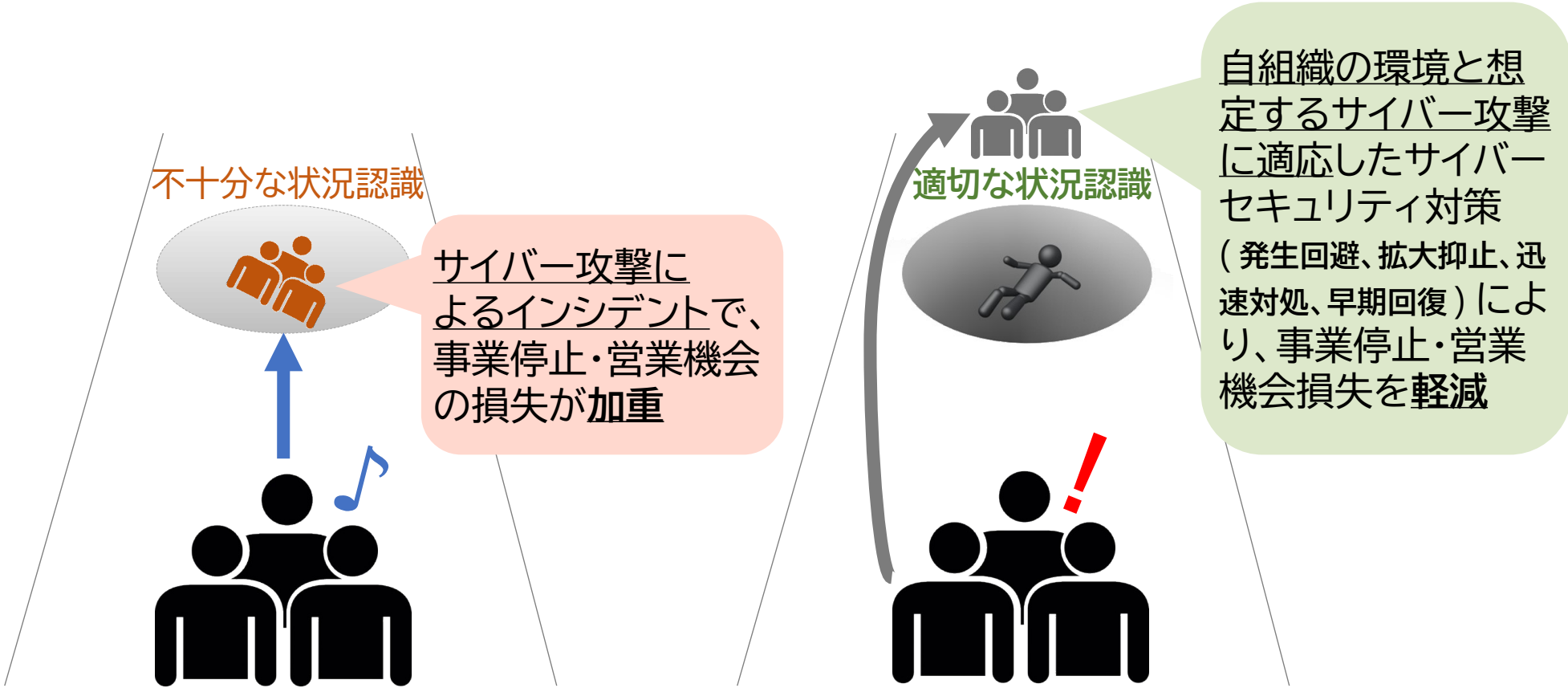
「**情報資産**」をベースにしたセキュリティ対策

- 「侵入させない」ためのセキュリティ対策
- 「CND的なインシデント ＝ **侵入**」
- 攻撃プロセスの前半で認識
- システム保守管理者（委託者）が対応

「**システム防護**」をベースにしたセキュリティ対策

TLP:CLEAR

状況認識の不足による**想像力の欠如**



TLP:CLEAR

ほぼすべてにおいて**意思決定プロセスが遅い**

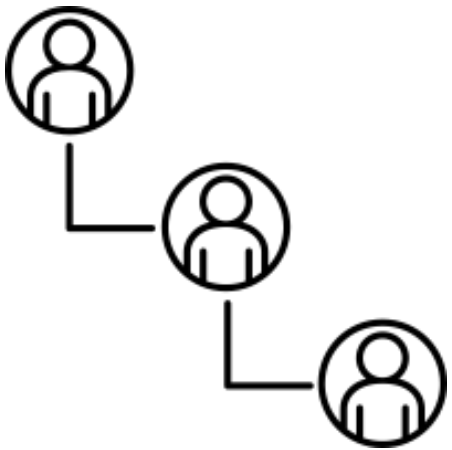
日本型組織は、依然として**「表面的な組織構造」と「内面的な組織構造」の2つが共存**している。

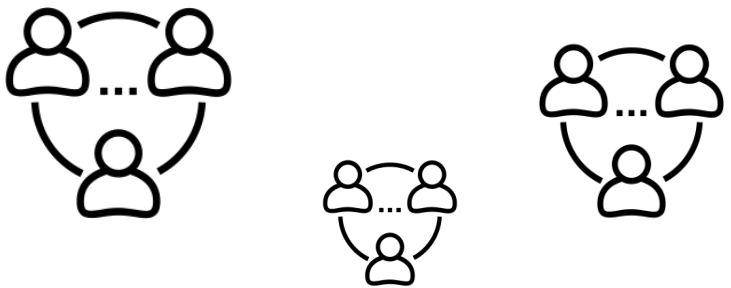
表面的な組織構造

- ピラミッド型の階層化された権限
- トップダウン型の上意下達
- 規律やルールによるガバナンス（統制）

内面的な組織構造

- 同じ階層における社員間の**非公式なやり取り**
- **横並び意識**と**同調圧力**の場の空気
- 上位階層への**忖度**と隣接領域への**根回し**





TLP:CLEAR

TLP:CLEAR

トピック４

重要インフラ事業者に経営層に（是非とも）理解していただきたいこと

重要インフラ事業者の経営層に理解していただきたいこと

- すでに主要組織において**極めて高度なサイバースパイ**が活性化しているとみなす。
  - 「システムの脆弱性や設定不備の悪用」に加えて、「組織の内部者（人間）の認知（考え方）に影響を与える巧妙な影響工作（認知戦）」に加えて**持続的に行われている**。
- 有事前後において、敵対国におけるプロパガンダに強く影響を受けた「**ハクティビストによる露出の激しいサイバー攻撃**」と、敵対国の実力攻撃を有利にするような「サイバーオペレーションによる**高度に検知回避する機能破壊攻撃**と**識別困難な情報戦**」が同時多発的に発生する。
  - 日本は、国家を防衛するためのサイバーオペレーションや情報戦の能力が**整備されていない**ため、最後の砦は存在しない。
  - 平時において認知戦の影響を強く受けた**内部者による（内側からの）破壊攻撃**も発生する。
- 同盟国や友好国のチームからサイバー支援を迅速かつ適切に受けために必要な言語能力や信頼関係が不足しているため、**被害が甚大化かつ広域化**する。
  - 上層部における旧態依然（伝統的な）のリーダーシップ（上意下達）により、**現場が混乱**する。

本資料に関する連絡先

名和 利男（ Toshio NAWA ）

SITE: https://www.nawa.to

PGP: 0xE38B4E01