NAD Monthly Report.

Market Flash

ハイブリッド戦争
～サイバー空間での攻防～

2022.7&8

日本アルプス電子株式会社
NIHON ALPS ELECTRONICS CO.,LTD.

暑中お見舞い申し上げます

平素は格別のお引き立てにあずかり、誠にありがとうございます。

新型コロナウイルス感染が再び拡大しつつあります。
くれぐれもご自愛のほどお祈り申し上げます。

今後共なお一層ご愛顧のほどよろしくお願い申し上げます。

～ハイブリッド戦争～

最近、ロシアのウクライナ侵攻についてのニュース報道が少なくなった。戦況が落ち着いているわけでも、和平交渉が進んでいるわけでもない。今なおロシアの蛮行は続いている。
一方で、フィンランドとスウェーデンのNATO加盟が進み、各国の安全保障に対する議論が盛んにおこなわれている。日本も例外ではなくGDP２％の軍事費の議論が始まっている。
日本の弱みは「核」だけではない、ロシア・ウクライナ戦争でもわかるように、今の戦争は「ハイブリッド戦争」といわれているサイバー攻撃への備えである。ウクライナ侵攻前から始まっているロシアのサイバー攻撃は、それに乗じた他の国（中国、米国、北朝鮮など）からのサイバー攻撃も急増し、民間企業にまで拡大している。
そこで、今月はその「ハイブリッド戦争」の中身をのぞいてみたい。
日本におけるハイブリッド戦争研究の第一人者の廣瀬陽子女史（慶應義塾大学教授）の著書「ハイブリッド戦争――ロシアの新しい国家戦略」から少しだけご紹介したい。
現代のハイブリッド戦争の概要やロシアのサイバー攻撃部隊などについて詳しく書かれているので是非ご一読いただきたい。

１．ハイブリッド戦争とは

ハイブリッド戦争とは、政治的目的を達成するために軍事的脅迫とそれ以外のさまざまな手段、つまり、正規戦・非正規戦が組み合わされた戦争の手法である。いわゆる軍事的な戦闘に加え、政治、経済、外交、プロパガンダを含む情報、心理戦などのツールの他、テロや犯罪行為なども公式・非公式に組み合わされて展開される。　ハイブリッド戦争は、2013年11月の抗議行動に端を発するウクライナ危機でロシアが行使したものとして注目されるようになった。ウクライナ危機においてハイブリッド戦争という言葉が使われるようになったのは、2014年4月26日に、ＮＡＴＯの前安全保障アドバイザーであったオランダ少将フランク・ヴァン・カッペンが「プーチンはウクライナでハイブリッド戦争をおこなっている」と述べたことが契機となっている。　ウクライナ危機を例にとれば、ロシアはかなり前から政治技術者などをクリミアやウクライナ東部に送り込んでいた。さまざまな政治的なプロパガンダを浸透させたり、親露的な人物がより政治の中枢を占めるように工作した状態で、標識をつけない特殊部隊（Little Green Men）や民間軍事会社（PMC: Private Military Company）などの民兵をクリミアやウクライナ東部に送り込んで展開させた。そして、官庁など要所を占拠し、大規模な正規軍を国境付近に集積して圧力をかけながら、フェイクニュースの多用などの宣伝戦やサイバー攻撃、経済的脅迫、時に融和的な外交などありとあらゆる手段を組み合わせ、住民投票や一方的独立をバックアップし、それにより領土併合や地域の不安定化を実現したのである。　フェイクニュースを用いた宣伝戦・情報戦やインフルエンス・オペレーション、サイバー攻撃などは、2016年の米国大統領選挙はじめ、欧米の多くの選挙への介入や政治の揺さぶりの手段としても多用されてきた。・・・

ハイブリッド戦争はロシアだけが用いてきたものではない。近年、さまざまな兵器が新たに開発され、世界中で展開される一方、ハイブリッド戦争に代表される新たな戦闘の仕方が世界を震撼させるようになった。戦い方は近年、明らかに変化しているのである。そして、最近の戦争のあり方は、「現代型戦争」、「新しい戦争」、「現代戦」、「21世紀型の戦争」、「新世代戦争」などと呼ばれるようになった。

～ハイブリッド戦争～

2．ロシアのハイブリッド戦争

ロシアの亡命白軍軍人で戦略家であったエフゲニー・メスネルは、ロシアの「新世代戦争」の目的が五段階のヒエラルキーで構成されていると主張していた。

第一段階は、敵対国のモラルをくじき、連帯を打ち砕くことである。モラルをくじくことの意義はきわめて大きく、それにより、相手国の対抗力を著しく低下させることができる。

第二段階は、武力戦争に寄与しうるもの、すなわち軍、ゲリラ、国家組織などを掌握することである。武力戦争に寄与するものを掌握することにより、相手の戦力を削ぎ、戦闘を優位に展開できる。

第三段階は、心理的な観点から価値あるものを掌握するか破壊することである。それにより敵国や敵陣営に心理的なダメージを与えることができ、混乱や戦意喪失などを引き起こすことができるため、戦争遂行のうえでは好条件を生み出すことができる。

第四段階は、物質的に価値あるものを掌握するか破壊することである。心理的にダメージを受けているところに、さらに物質的に価値があるものを掌握されたり破壊されたりすると、心理的ダメージも倍増するだけでなく、物理的な損失も大きく、相手に大きな打撃を与えることができる。

第五段階は、「外部性の達成」である。外部性の達成とは、新たな同盟における勝利、すなわち、自身の同盟を生み出したり、メンバー国を増やしたり、同盟を増強したりというような自身の同盟の強化、および敵の同盟を弱体化する、すなわち、敵の同盟の連帯を弱めたり、メンバー国を脱退させたり、武装力を弱めたりするようなことを意味する。

一方、自国への対応として、
① 自国の連携強化
② 自国軍の保護
③ 中立国におけるネガティブな反応を避ける
という努力が行われているという。

ロシアにおけるハイブリッド戦争ないし「新世代戦争」として認識されているものは、ウクライナ危機でロシアが用いた手法であることにはまず異論はないだろう。ロシアは前述のような手段を用い、第一に、ウクライナと欧米の関係をパニックに陥れて機が熟すのを待ち、第二に、ウクライナが欧米から距離を置くように誘導し、第三に、ウクライナと欧米の関係がバランスを失ったときに侵攻するという三つのプロセスをくりかえして徐々にウクライナを手中に収めようとしたという。

このようなロシアのハイブリッド戦争は、2014年のクリミア侵攻・支配においては見事に成功したといえる。ウクライナ国内では新ロシア大統領の退陣を求め国内は混乱し、米国もそれを支援しているすきにロシアはクリミアを併合しいたのである。また、2016年の米国大統領選挙においても見事にプーチンを敵視するヒラリー・クリントンを引きずり落としトランプ氏を大統領にすることに成功した。
この意味で成功したといえる。しかし、今年のウクライナ侵攻においては苦戦を強いられ、欧米を完全に敵に回してしまったことや世界中からサイバー攻撃を受けていることなど、決してハイブリッド戦争が成功しているという状況ではない。

～ハイブリッド戦争～

３．シャープ戦略

ハイブリッド戦争と切り離せない「シャープパワー」とは、米国の「全米民主主義基金（ＮＥＤ）」が2017年12月に公表したリポートではじめて使った造語であるが、テレビやＳＮＳなどさまざまな方法で偽情報の流布をおこない、調略、恫喝、嫌がらせなどの手段を組み合わせて、自分たちに都合の良い方向に転向させる手段であり、主に、中国、ロシアがそれを近年多用しているという。そして、それは諸外国の政治への介入や妨害の際に効果的に用いられている。　シャープパワーは、ソフトパワーの「悪質版」とでも考えるとイメージが湧きやすいだろう。中国については、孔子学院の展開（＊１）などが顕著な事例とされるが、ロシアは資金もないため、中国のような大規模なシャープパワー戦略は取れない。だが、ロシアは偽ニュースの拡散や宣伝キャンペーンを自国メディア（例えばＲＴ〔ロシア・トゥデイ〕など）やＳＮＳを利用し、世界各地で展開してきた。ＳＮＳによる拡散には既述の「トロール部隊」（＊２）が特に暗躍してきた。また、対スペイン語圏での作戦ではスペイン語が使用されているベネズエラなどの協力が、また最近の英語による作戦では英語を公用語とするアフリカ諸国の協力も確認されるなど、より安価でより効果的な作戦がとられてきた。
他方、シャープパワー的な手法は判定されづらい傾向があり、実際の攻撃からかなり時間が経ってから認定されることが多く、実際にロシアからの攻撃があったとしても認定されていないケースも多々あるとされる。また、シャープパワーの実施においては、さまざまな手段が複合的に展開され、またサイバー攻撃が中心的役割を果たすケースが多いため、サイバー攻撃の成果とみなされることも多いのが実情であり、実際のところ、厳密に区別することは難しい。

（＊１）孔子学院

中国政府が世界各国の大学等と提携してその地に設立する中国語および中国文化に関する教育機関である。一方、中華人民共和国が諸外国の大学などで「外交関係」を名目にした「統一戦線工作」によって、教育の名を借りて中国共産党の主張を基づいた世論戦宣伝（プロパガンダ）を行う機関だという主張も存在している。欧米やオーストラリアなどでは閉鎖の動きが広がっている。日本では早稲田大学や立命館大学など14の大学に設置されている。

（＊２）トロール部隊

ネットスラングとしての「トロール（troll）」は、炎上を狙ったネタを投稿する人あるいはその投稿を指す。1日24時間365日、ネット上で情報工作をする民間会社の存在も確認されている。300～400人の従業員が業務ごとに部署に分かれ、メディアにコメント投稿、フェイスブックなど交流サイト（SNS）には偽情報を拡散し、架空の人物になりすましてブログも展開する。政治風刺画を手掛けるデザイン部や映像制作部もあるという。

シャープ戦略の主な事例

2016年1月	ドイツにおける難民によるロシア人少女への暴行という偽ニュース拡散により、ロシア系住民が抗議行動を起こし、対ロ制裁を主導するメルケル首相を揺さぶる（リサ事件）
2016年6月	英国のBREXITをめぐる国民投票
2016年10月	NATO加盟を妨害するためにモンテネグロでロシアの情報機関が関与する当時のジュカノビッチ首相を暗殺し政府転覆を狙ったクーデター未遂
2016年11月	米国大統領選挙。ヒラリー・クリントンに対してネガティブな、ドナルド・トランプに対してポジティブなキャンペーンを行う「プロジェクト・ラフタ」もコンコルドが出資
2016年11月	モルドヴァ大統領選挙（2014年4月の同国ガガウズ首長選挙も）
2017年	フランス大統領選の際のマクロン候補（当時）へのサイバー攻撃・偽ニュース攻撃
2017年10月	スペイン・カタルーニャ州の独立問題をめぐる住民投票

表1－2　ロシアのシャープパワー戦略（主な事例）

（筆者作成）

４．ロシアのサイバー攻撃部隊の実態

米国の戦略国際問題研究所（ＣＳＩＳ）によれば、近年、ロシアは中国につぐサイバー攻撃の発信地とされている。ロシアの場合には圧倒的に国家レベルの関与がある攻撃が多く、
また、サイバー攻撃のさまざまな類型をほぼ網羅した複雑なタイプのものが多く、与える打撃も相当なものとなっている。

2019年２月に、セキュリティ企業CrowdStrikeは、３万件以上に及ぶハッキング事件を分析した調査データを発表したが、ハッカーの１位に選ばれたのはロシアのハッカーだった。同社の発表によれば、ロシアのハッカーらは、ネットワークへの侵入からコンピュータやデバイスの乗っ取り、システムダウンに至るまでの作業をわずか18分で完了させており、その能力は圧倒的に世界最速とされた。
ちなみに２位は、北朝鮮のハッカーだとされたが、その、作業時間は平均２時間20分（ハッカー集団はスターダストチョリマ〈ＡＰＴ38〉）で、ロシアと比して、8倍近い時間がかかっていた。ついで、3位は中国（作業時間は平均四時間で、主たるハッカー集団はアンカーパンダ〈ＡＰＴ14〉、ディープパンダ〈ＡＰＴ19〉、ゴブリンパンダ〈ＡＰＴ27〉、ムスタングパンダ、サムライパンダ〈ＡＰＴ４〉）、4位はイラン（同、5時間強で主たるハッカー集団は、賢い子猫、らせん子猫〈ＡＰＴ34〉、洗練された子猫〈ＡＰＴ33〉）、5位はその他の組織的サイバー犯罪者（同、9時間42分）であった。　このように、侵入時間だけ見れば、世界最強のサイバー攻撃能力を持つとされる一方、ロシアのサイバー攻撃は脆弱だとされる側面もある。

～ハイブリッド戦争～

＜ロシアの主なハッカー集団＞

「ＡＰＴ28」

同グループは「Fancy Bear」「Sednit」「Pawn Storm」などの名前で呼ばれることもある。

フィッシングメッセージとなりすましウェブサイト 「ＡＰＴ28」は、防衛・地政学的な問題に関する情報、すなわち政府機関のみが必要とする情報の収集に取り組む、開発者および攻撃実行者のグループで、その技術力はきわめて高度である。ＡＰＴ28は、ロシア語設定の開発環境でマルウェアを変換しており、その時間は、モスクワやサンクトペテルブルクなどのロシアの主要都市の標準的な業務時間帯（午前8時から午後6時）に合致する。それらの事実から、ＡＰＴ28が、強固な基盤を持つ組織、最も可能性が高いのはＧＲＵの指揮下にあり、資金を含むさまざまなサポートを直接的かつ継続的に受けていると考えられている。

ＡＰＴ28の攻撃範囲はロシアが敵対視する欧米のみならず、世界中の複数のセクターを標的にしてきたが、ロシア政府の戦略的利益を体現するために、ロシアの軍事情報機関とも提携してきたと見られる。

東京五輪は訴追内容に含まれていなかったが、2015ー6年にウクライナの電力会社のシステムを攻撃し、たびたび停電を引き起こしたことや17年の仏大統領選挙ではマクロン候補（当時）陣営のメールなどをハッキングし、情報流出をさせたことなども罪に問われている。彼らがウクライナで使用したマルウェア「ノットペーチャ」は、米国内の病院システムなどにも用いられ、復旧費用などで10億ドルの損害を与えたという。ノットペーチャは史上最強の破壊力を持つとされ、これまで世界が被った損害額は100億ドルとみなされているが、ＧＲＵはこれを多用する傾向がある。

「ＡＰＴ29」

セキュリティを巧妙にすり抜ける「ＡＰＴ29」は、コージー・ベアなどとしても知られるサイバー攻撃集団で、2014年に最初に国際的に存在が認識された。この母体は、ＦＳＢ（連邦保安庁）とＳＶＲ（連邦対外情報庁）で、高度な訓練を受け、高い能力を持つ攻撃集団だとみなされており、適応性が高く、最も進化を遂げていると評価されている。ＦＳＢとＳＶＲはともに、ＫＧＢが母体になっているので、ソ連解体後に異なった組織になっても連携が可能

コージー・ベアは、幅広い対象に攻撃をおこなうのが特徴で、何千ものフィッシングメールを幅広いターゲットに送信する方法を好むとされるが、その行動様式は注目されている。なぜなら、ほとんどの国家基盤のハッカーは、より小さな攻撃対象に対し、より集中的な操作をおこなう傾向があるからだ。

ＡＰＴ28とＡＰＴ29の違いとして知られているのが、入手した情報の扱い方である。ＡＰＴ29はクレムリンの政策立案者に役立つ情報を収集するが、それをばらまくことは基本的にはせず、情報を外に流す際にもダークウェブや秘匿性の高い限定的な手段で実施するという。しかし、ＡＰＴ28は、ハッキングして情報を盗み出すだけでなく、それをかなり広い対象に公開することが多いとされている

だがロシアの攻撃集団はＡＰＴ28やＡＰＴ29にとどまらない。「Bear（熊）」の総称でも呼ばれるロシア系ハッカーグループは無数に存在しているのである。

グループ名	別名	想定される上位・関連組織	主要な標的・活動
APT28	ファンシー・ベア、セドニット、ポーンストーム、ソファシー、26165部隊、29155部隊、74455部隊、サンドウォーム、ストロンチウム、ツアー・チーム、NotPetya、アイアン・トワイライト（Iron twilight）など多数	GRU	・米国民主党全国委員会（2020年にトップ） ・米国・米国政府（2020年に2位） ・米大統領選挙への介入（2016年） ・欧州諸国・国際機関に対する侵入 ・ジョージアを中心としたコーカサス地域に対する侵入 ・ウクライナ、ドイツなど欧州諸国の政府および軍隊に対する侵入 ・NATOをはじめとする欧州の安全保障機関、防衛業界の企業への侵入 ・世界アンチ・ドーピング機関（WADA） ・韓国・平昌冬季五輪（2018年） ・その他多数
APT29	コージー・ベア、コージー・デューク（ス）、デュークス、Cozer, Monkey, CozyCar, Euro APT, Office Monkeys, RUS2, YTTRIUMなど多数	FSB・SVR	・米国民主党全国委員会（2020年にトップ） ・米国・米国政府（2020年に2位） ・米大統領選挙への介入（2016年） ・ロシア（国家としては2020年に2位） ・世界の国際機関に対する侵入 ・ノルウェー、オランダ、ウクライナなど欧米諸国の政府、外交政策担当グループ、およびその類似組織への介入 ・英国などの医療機関（2020年） ・その他多数
ブードゥー・ベア	Sandworm, Black Energy, Electrum	不明（GRUか？）	・ジョージアへのDDoS攻撃（2008年）。 ・ウクライナの電力網に対するマルウェア攻撃（2015年）
ベノモウス・ベア	Snake, Turla, Uroboros, Group 88, Waterbug	FSB	・スイス国防省・軍需企業に対する侵入 ・東欧諸国の領事館に対する侵入 ・韓国政府機関に対する侵入
Koala	Energetic Bear, Dragonfly 2.0, Group 24, Crouching Yeti	不明（ロシア政府が関与）	・エネルギー、原発、水、航空、重要製造業などに対する侵入（2014年～）
TEMP. Armaggedon	—	不明（ロシア政府が関与）	・ウクライナの保安・法執行機関に対する攻撃
TEMP. Isotope	Dragonfly 2.0, Energetic Bear	不明（ロシア政府が関与）	・米国の電力網に対する侵入
TEMP.Veles	—	中央化学機械研究所（TsNJKhM）	・産業用制御システム（ICM）に対する侵入

表2－2　ロシアの主要なハッカー集団と政府機関との関係

出所：小泉悠「ロシアのサイバー戦略」『海外事情』2019年7・8月に、報道などを利用して筆者が加筆・一部改変。

５．ウクライナの逆襲

ロシアは2014年クリミア半島併合以来、ウクライナに対して何度を大掛かりなサイバー攻撃を行ってきた。2015年と2016年には、2年続けてウクライナ国内の電力会社をサイバー攻撃して大規模停電を起こしている。2017年には、「NotPetya」という名の感染力の強いランサムウエアでウクライナの政府機関や民間企業の動きを止めるような広範囲なサイバー攻撃を行った。

しかし、今回の侵攻においては、侵攻の1か月前から大規模なサイバー攻撃は見られたが、深刻なサイバー攻撃は報告されていない。通信施設などへの攻撃を受け通信網が一時遮断されたが、ウクライナのミハイロ・フョードロフ副首相兼デジタル転換相がツイッター上で、米スペースX社のイーロン・マスク最高経営責任者（CEO）にスターリンク通信衛星サービスの提供を要請した。そのわずか10時間後、マスク氏は「スターリンクのサービスが既にウクライナで始まっており、更なる端末が向かっている」とツイート。世界を驚かせた。ウクライナのデジタル転換省は戦争開始の数カ月前には地方におけるインターネット接続性を向上させるため、スターリンクの提供を打診していたとのことである。

このようにウクライナではロシアによるこれまでのサイバー攻撃により準備を進めてきた。何年も前からウクライナ軍にさまざまな訓練を施してきた米国特殊作戦軍（ＳＯＣＯＭ）に加えて、２０２１年１０月までには米国のサイバー攻撃をＮＳＡとともに主導的に組み立てている米サイバー軍もウクライナに部隊を送り込んでいる。また、米マイクロソフト社などのエンジニアらも同じくウクライナに入り、ロシアから侵攻があった場合のサイバー攻撃に備えて、国内の鉄道や電力などのインフラをはじめとする重要な拠点の保守を行っている。ロシアが平時にウクライナ国内のコンピューターなどに埋め込んでいたとされるマルウエア（ウイルスなど悪意のある不正なプログラム）の駆除も実施したという。

また、NATOでは、何年も前からロシアがどんなハイブリッド戦を仕掛けてくるか研究をしており、ウクライナ側もそうした知識を踏まえて、政府と事業者の間で、何十回も重要インフラへの攻撃を想定して研修を行ってきた。

さらに、ウクライナは、ウクライナを支持する世界中にいるエンジニアなどの「民兵」を募集した。現在、無料登録できるそのチャンネルは会員数が３０万人近くになっている。チャンネルでは毎日何度も、ロシア国内の攻撃ターゲットをリストアップし、会員にサイバー攻撃を実施するよう指示している。

さらにウクライナを支持するハッキング集団は、確認されているだけで５０組織近くが活動している。日本でもニュースになった活動家集合体のアノニマスもその一つだ。アノニマスのハッカーらは、ＤＤｏＳ攻撃だけでなく、ロシア国内の政府組織などから情報を奪って暴露もしている。

こうした攻撃に加えて、ウクライナ側には、ロシアへのＤＤｏＳ攻撃を行うためのウェブサイトがいくつも設置されている。そこのサイトに行けば、ターゲットの情報とともに「攻撃」というボタンが用意されており、誰でもロシアを攻撃するＤＤｏＳ攻撃に参加できるというものもある。

要するに、日本のどこかのカフェにでもいながら、クリック一つでロシアとのサイバー戦争に日本人でも参加できてしまうのである。（実際に日本人のハッカーも参加している）

ロシア国内の政府機関や民間企業をサイバー攻撃することによって、政府機関や民間企業のサーバーが一時的に使えなくなるなど被害も出ているようだ。

一方で、政府機関へのハッキングなどを行う高い技術を持つとされるベラルーシを拠点とする「サイバーパルチザン」は、今回、ウクライナ支持を表明した。そして、実際にロシアの輸送路へのサイバー攻撃を実施した。鉄道の最適化システムを狙い、2日間完全に停止させた。また、信号や分電盤の破壊工作も展開したとされる。これによりロシアは首都キーウ掌握をあきらめざるを得なくなったと思われる。

6．日本にも及ぶサイバー攻撃

ロシアのウクライナ侵攻が始まった2022年2月以降、国内企業へのサイバー攻撃が急増している。各省庁やサイバーセキュリティーに関わる組織は続々とセキュリティー対策に関する注意喚起を出した。

情報処理推進機構（IPA）はセキュリティーに関する相談窓口を用意している。2022年4月19日に発表した「情報セキュリティ安心相談窓口の相談状況」によれば、その窓口への相談件数は2022年第1四半期（1～3月）で2716件と、前期（2021年10～12月）より約800件増えた。このうち、Emotetウイルスに関する相談は656件で、前期から約54.7倍に急増している。

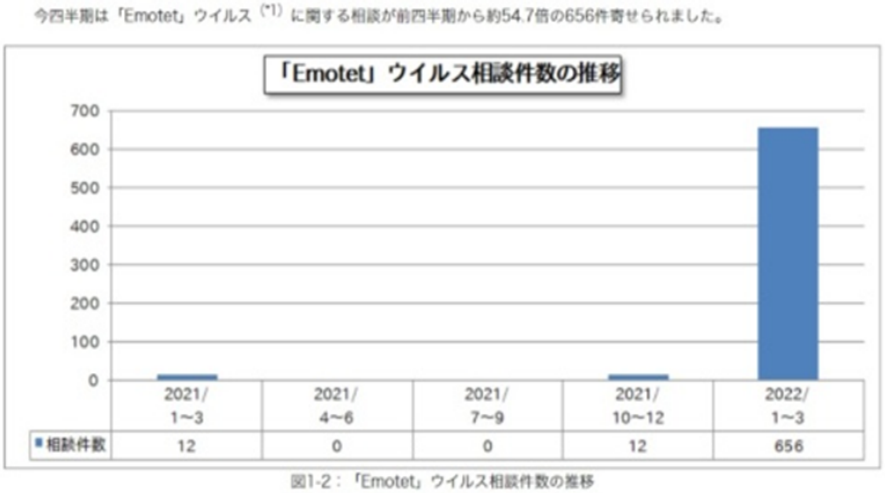

図1-2：「Emotet」ウイルス相談件数の推移

こうした状況を受けて、IPAやJPCERTコーディネーションセンター（JPCERT／CC）などはEmotetに関する最新情報を提供し、注意を呼びかけている。JPCERT／CCはEmotetの感染確認を行うツール「EmoCheck」を無償で提供している。

経済産業省と金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター（NISC）が2022年3月1日に、セキュリティー対策強化に関する注意喚起を出した。さらに経産省と総務省、警察庁、NISCは3月24日にも同様の注意喚起を出した。この中で、「サプライチェーン全体を俯瞰（ふかん）し、発生するリスクを自身でコントロールできるよう、適切なセキュリティー対策を実施する」「国外拠点などについても、国内の重要システム等へのサイバー攻撃の足掛かりになることがあります」としている。


サイバーセキュリティ対策の強化について注意喚起を行います

2022年3月1日 同時発表：金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター

▶安全・安心

本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところ、昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。
このため、サイバーセキュリティ対策の強化について、関係7省庁から改めて注意喚起を行います。

1．概要

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。
政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、別添に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。
また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。
さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。
実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にも御相談ください。

サプライチェーンにおけるセキュリティー対策強化を呼びかける要因は国内大手自動車メーカーの関連会社がサイバー攻撃の被害を受けて、製造が一時停止する状況になった背景があるからだ。
国内で猛威を振るうEmotetウイルスに感染すると、第三者が感染した端末を制御し、機密情報にアクセスしたりランサムウエアに感染させたりする被害を引き起こす可能性がある。その影響は当該の企業だけでなく、取引先企業にも影響を及ぼす。
サプライチェーンを含めたセキュリティー対策については、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が3月31日、企業が実施した具体的な事例を公開した。具体的には、国内外の関連企業に対してチェックリストを使ってセキュリティー対策の取り組み状況を把握することや、取引企業間のネットワーク、アプリケーションのマクロの自動実行機能、データのバックアップ、インシデント発生時のCSIRTなどの社内プロセスの確認をポイントとしている。

７．日本政府の安全保障への対策

日本政府は、2018年12月に、「防衛計画の大綱（防衛大綱）」と「中期防衛力整備計画（中期防）」を改定した。それは、筆者が国家安全保障局顧問を拝命していた時期と重なる。新たな防衛大綱では、従来の陸・海・空に加え宇宙・サイバー領域での対応強化が明記された他、政府与党内にも異論のあった護衛艦「いずも」の事実上の空母化や、空母に垂直着陸できる戦闘機「F35B」の導入も事実上明記した。

本改定は、前回の改定から５年での改定となったが、中期防は５年毎の改定が通例である一方、防衛大綱は通常は10年に一度、改定がなされてきたが、世界の安全保障状況が短期間で顕著に変化したことから5年前倒しでの改革となった。
新防衛大綱は「中国等のさらなる国力の伸長等によるパワーバランスの変化が加速化・複雑化し、既存の秩序をめぐる不確実性が増している」と強調しており、中国の軍備増強や米国の相対的地位低下という地政学的変化が懸念されていることがわかる。
また、技術面で特に危惧する変化として、ハイブリッド戦争が指摘され、宇宙やサイバー、電磁波への対応、戦術面では戦時・平時とも判別の難しい状況での防衛を確実にする「ハイブリッド戦」への対応を重視することが示された。
改定に着手した小野寺五典元防衛大臣も改定の背景として、北朝鮮が核ミサイルの能力を顕著に増強させたこと、またロシアのクリミア併合以後、戦い方が変わったことを挙げている。戦い方が変わった、ということは、つまり「ハイブリッド戦争」の脅威が高まったことを意味する。

サイバー攻撃は普段私たちの目では見ることができない。サイバー攻撃を受けて初めてその破壊力のすさまじさを知ることになる。今の日本の民間企業、政府、公共機関すべてサイバー攻撃に対する脆弱性は日本の将来を決定する最も重要な課題であろう。（しかし、皮肉なことに紙社会の日本はそのサイバー攻撃の脅威をある意味防御しているのかもしれない。ただし、こんな冗談は全く通用しないが・・・）
目に見えないだけに、サイバー攻撃の実態は常に注視する必要があるであろう。それはデータを取り扱う一般の社会人にも必要不可欠な知識である。

こちらでサイバー攻撃に関するいろいろな情報が見れます（ご参考までに）
https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/