デジタル国家ウクライナの強靱性（レジリエンス）
――サイバー・セキュリティ欧州最前線からの報告

揺るがないウクライナの「情報戦」における優位。それを支える強靱な分散型システムを作った先進IT国家エストニアは、EUのDX化の中心で、NATOサイバー防衛協力センターも配置される。最新の動きは、懸念は何か。現地から報告する。

NATO CCDCOEのサイバー演習に集まった「国際法トラック」の面々

防衛研究所主任研究官
河野桂子
こうの　けいこ　上智大学博士後期課程修了（法学博士）。同大学助手、米国海軍大学客員研究員、NATOサイバー防衛協力センター（CCDCOE）国際法研究員を経て現在防衛研究所勤務。近著論文「サイバー・サプライチェーン各国法制の比較」（NATO CCDCOE website）。

ロシアによるウクライナ侵攻が始まって以降、ウクライナのデジタル戦線における奮闘が熱い注目を集めている。

IT軍やインターネット軍の創設、ロシア軍の動きを通報するプログラムや空襲警報アプリの開発運用などは、デジ

タル・トランスフォーメーション省が主導して進める策のほんの一例である。本稿では、筆者がエストニア滞在で見聞きした経験から、その強靭性の秘密に迫ってみたい。

エストニアは電子政府のロールモデルとしてよく知られているが、実はウクライナ政府によるデジタル化推進の中核的支援者としても非常に重要な役割を果たしている。現在進行中の複数のプロジェクトの中でも、eガバナンス・アカデミー（e-Governance Academy：eGA）という組織（エストニア政府、オープン社会基金、および国連開発計画〔UNDP〕が共同で設立した非営利団体）が手がける二つのプロジェクトについて、筆者はウクライナチーム長を務めるマリ・ペダックさん（エストニア人）および同チームのサイバーセキュリティ・サブチーム長を務めるユーリ・カプウーティンさん（ウクライナ人、現在キーウ在住）に、五月二〇日、お話を伺う機会を得た。

分散処理が攻撃への強み、国家情報システム

ITの知識や技術は一朝一夕に身につくものではない。当然のことながら、この分野の教育はエストニア同様、ウクライナでも一九九一年の独立後しばらくして始まっており、そのことは、現在ウクライナ政府の内外で活躍するIT専門家の多くが三〇代であることからも推測できる。しかしウクライナ政府としてのデジタル化の推進はユーロマイダン革命（二〇一四年）での新政府成立を待たねばならなかった。ロシアによるウクライナへのサイバー／デジタル攻撃が、一四年以降恒常化していたことも、このデジタル化（いわば「DX化」）の推進力となっている。

eGAがウクライナで手がけた、国家情報プラットフォームのシステム化プロジェクトは主に二つある。第一はEGOV4UKRAINE（一六～二一年）、第二は現在進行中の後継版EUDigital4UA（二〇～二四年）である。EGOV4UKRAINEは、そのスローガンを「人ではなくデータを走らせる（Make the data run, not people）」としており、エストニアの「X-Road」を手本にして設計した「トレンビータ」などの各種システムの開発・運用によって、エコシステムの構築を目指してきた。

「トレンビータ」（Trembita）とはデータ交換プラットフォームシステムのことであり、この呼び名は、かつてウクライナで通信手段としても使用された、長さ四メートルにおよぶ伝統管楽器に由来している。筆者はエストニア滞在中、同政府が提供する数々の電子サービスの恩恵を享受したが（コロナ禍もあって、医療ポータルを最も活用した。

PCR検査結果証明、ワクチン接種証明、薬の処方箋など全ての医療履歴が閲覧可能である）、データ交換プラットフォームは、具体的な個別の電子サービスの運用を支える基幹システムの役割を果たしている。エストニア国民・在住者がふだん、X-Roadを目にする機会はほとんどないが、これがなければ個別の電子サービスが機能しないと言っても過言ではない。ウクライナのカプウーティンさんは、トレンビータの設計維持運用者の一人であり、現在「トレンビータ2・0」の立ち上げを進めているほか、侵攻に対応して政府のデータサーバをより安全な場所に移すなど、ますます増える業務に日々奔走している。

トレンビータの特徴は、常に中枢の中継地点を経由しなければならない中央集約型ではなく、地方分散型であるため、仮にある地域のインフラが破壊されたとしても、全体としての運用が影響を受けることはない。現在、一六〇以上の政府機関と州政府との間がこのプラットフォームにより連結されており、その結果、ウクライナ国民は首都から遠く離れた過疎地域に住んでいても首都にいると同様の電子サービスを活用することが可能である。また、詳細は不明だが、個人情報がロシア側に漏れることのないような仕組みも採用されている。

「スマホの中に国家」が

ウクライナ国民等が電子サービスを活用する上で日々接するのは、実際にはトレンビータではなく、スマートフォン上のアプリDiiaである。これは、ゼレンスキー大統領が打ち出した「スマートフォンの中の国家（the state in a smartphone）」構想の下でデジタル・トランスフォーメーション省が主導して進めた政策の一つである。現在、ウクライナでは、世界初の電子パスポートをはじめとして各種の電子証明書類（ワクチン接種、運転免許、出生、保険、納税証明書や電子署名が運用中。教育歴の追加についても準備中）が扱われている。侵攻が始まってからは、ロシア軍の動きを各地の住民が当局に通報するプログラムもこのアプリに追加された。

もちろん、電子政府の成否は、ウクライナに限らず普及率の向上にかかる。筆者もエストニアで、ウクライナ政府発行の紙パスポートを手にする方々をしばしば目にした。スマートフォンをまだ十分に使いこなせず、アプリ経由の電子サービス活用が困難である住民向けには、eGAのプロジェクトとして別途「ビュリック（Vulyk）」というシステムが開発運用されている。これは、各州の行政サービ

スセンターにおいて設置された情報システムであり、トレンビータと接続されている。そこでアプリを使いこなせない住民は、このセンターに出向いて地方行政職員の助けを得ながら、各種の公共サービスを利用することが可能である。

ウクライナ国外への避難を余儀なくされる中、必要な証明書類や財産を携行できない場合も多い。そうだとしても、政府が各国民の個人情報を安全に維持管理し、必要に応じて海外から各種手続きの申請や証明書を入手することができれば、また各個人が財産を仮想通貨など電子的手段で保有することができれば、いくぶんかは戦時下の不自由さを軽減できるに違いない。ウクライナ政府は、暗号資産に関する法令の制定によって、国民などの暗号資産口座開設を容易にしただけでなく、海外からの多額の寄付の獲得にも成功しており、侵攻開始後の三週間で、その額は仮想通貨約五四〇〇万米ドルに達したと伝えられている。

電子政府化の自助努力と協働

話をeGAに戻すと、プロジェクト名（特にEUDigital 4UAの〝EU〟）が示す通り、二つのプロジェクトは欧州連合（EU）の財政的支援を基盤にしている。eGAはプロジェクトの運営を任されており、ウクライナチームは現在約五〇名弱の専門家が個別の課題に取り組んでいる。国籍は多岐にわたり、カプーティンさんをはじめ一〇名弱のウクライナ人メンバーが、現在もウクライナ国内にとどまり業務に従事している。カプーティンさんは黒海沿岸都市オデーサの出身で、現在もご家族が居住しているとのことである。他のウクライナ人スタッフも同様の状況に置かれていることが推測され、ご本人およびご家族の安全は、決して保障されていない状況である。

そんな中、eGAは、ウクライナ政府のデジタル・トランスフォーメーション省や国家特別通信情報保護局（SSSCIP）など二〇以上の政府機関と協同連携して、ウクライナ政府のデジタル化を、より推進させることを支援している。個別のウクライナ政府機関や人物を戦時下で一層の危険にさらすことのないよう、具体的な言及は差し控えるが、エストニア人関係者はみな口を揃えて、「EUや個別の欧州諸国がウクライナに対して一方的に知見や技術を施したのではなく、ウクライナは自助努力でデジタル・トランスフォーメーションを実現した」という見方を示していたのが印象的であった。

エストニア国内の議論としてよく聞かれるのは、「デジ

タル化の成否の鍵は、国家の規模ではない」という意見だ。つまり、エストニアが小さい国だから成功したのではなく、四〇〇〇万人以上の人口を抱えるウクライナであってもそれは十分に実現可能だというのである。では何が決定的な要素なのか。ペダックさんは「政府の側の意識変革、この問題に取り組む意欲」だと答えた。ウクライナではこのほか、国内外の人の移動（適材適所）や交流が活発である事情も寄与していると思われる。さらにウクライナでは、各省庁に「最高デジタル・トランスフォーメーション・オフィサー」（Chief Digital Transformation Officer〔CDTO〕）というデジタル・トランスフォーメーションを職務とする序列第二位の幹部を置き、CDTOのネットワークが構築されている。官位が高いのは、序列が低いと、その意見が組織で反映されない恐れがあるからという理由であり、ウクライナ政府の「本気度」が伝わってくる。エストニアにおいても、人材の流動性を実感する。これはEU圏内では日常の風景だが、EU非加盟国であるウクライナのこの例は、日本にも大いに示唆を与えるのではないだろうか。

ちなみに、eGAはウクライナのみならず世界一三〇か国以上のデジタル・トランスフォーメーションの支援プロジェクトに関与しており、対象国の中には自然災害の災禍に見舞われている国も含まれる。こうしたさまざまな危機的状況において、デジタル化された政府の機能はより強靭性を発揮するという議論が、本年五月中旬に開催されたeGA年次会合で披露された。もちろん、デジタル・トランスフォーメーションは単に利便性を追求するだけで終わらない。例えば、EUDigital4UAプロジェクトには、その構成要素として、カプーティンさんが担当するサイバーセキュリティおよびデータ保護が含まれている。またウクライナ政府は、サイバー攻撃に対する抗堪性（survivability）の向上という観点から刑法を改正し、民間のIT専門家が政府のソフトウェアやシステムの脆弱性を自由に探索することが可能となっている。

重要性増す「サイバー・セキュリティ演習」

カプーティンさんの重要な任務のひとつに「サイバー演習」がある。ウクライナは人口が多いので、eGAが研修対象としているのは政府機関職員や重要インフラ事業者の担当者であり、eGAの研修を受けた人間が今度は研修を指導する立場として、よりすそ野を広げていくことが期待されている。演習の形態は、机上演習ではなく、いわば実弾演習（live-fire）によるサイバー攻撃を想定した演習

であり、これは筆者が属したＮＡＴＯサイバー防衛協力センター（ＣＣＤＣＯＥ）の演習形態と同じである。

サイバー演習とはどのようなものか。ＣＣＤＣＯＥでは旗艦サイバー演習を二つ行っているが、その一つが毎年四月のロックドシールズである。これは、武力攻撃事態を必ずしも扱っているものではなく、また他のＮＡＴＯ演習とは異なり、特定の国家を仮想敵として名指ししているわけでもなく、登場人物（国）はすべて空想上のものとして行われる。

今年、ウクライナは米国と組んでブルーチーム（被研修者）として参加を登録していたものの、侵攻によって本番への参加はかなわなかった。ただしウクライナの、侵攻に対する目を見張るべき強靭性に鑑みると、今後同演習への参加が実現した暁には、優秀な成績を収めることができるのではないだろうか。

ウクライナ、ＣＣＤＣＯＥに加盟申請

三月、ＮＡＴＯ ＣＣＤＣＯＥ運営委員会は、ウクライナの加盟手続き開始を承認すると発表した。ＣＣＤＣＯＥはＮＡＴＯの一関連機関だが、侵攻で問題にされている北大西洋条約機構（ＮＡＴＯ）本体へのウクライナの加盟とは全く関係のない事象である。

ＣＣＤＣＯＥにおけるＮＡＴＯ加盟国（ＣＣＤＣＯＥスポンサー国）の数が増えれば増えるほど、加盟手続きは長引くことになり、手続きは最短でも数年はかかることが予想されるが、加盟手続き完了前でもＣＣＤＣＯＥの各種プロジェクトへの参加は可能であり、侵攻が終息した暁には、ウクライナ政府専門家の派遣も実現するであろう。

一口にサイバー防衛といっても、さまざまな角度からの対応が試される。先般行われたロックドシールズ演習では、技術トラックにおいては、ある欧州の国の重要インフラ等がサイバー攻撃にさらされたという想定で、その被害国を支援するために派遣された各国サイバー要員（ブルーチーム）に明らかにされない攻撃のタイムラインが進行する中、リアルタイムでの防御やブルーチーム間での協力の能力が試された。一方、筆者が属する「国際法トラック」では、ディスインフォメーションに関する出題も行われた。限られた時間の中で、自国ブルーチームの作戦司令官の法的諮問に対してどのように回答すべきか、答案を作成し採点される。

日本もブルーチームとして二度目の参加を果たし、ＣＣＤＣＯＥ側からの要望をもとに、民間企業から三名のＩＴ技術者に、本部要員としてご参加いただいた。

日本のサイバー・レジリエンス強化は急務

サイバー／デジタル脅威に対する抗堪性、強靭性は、日本にとって喫緊の課題である。

例えば、自然災害が多く発生する日本にとって、これらの他国の例は決して他人事ではない。二〇一六年には熊本県で地震が発生した後、動物園から放たれたライオンが路上を徘徊しているという合成写真がツイッターに投稿され、一八年の北海道胆振東部地震の際は、断水、火事場泥棒、余震などの誤情報が流された。国家の規模やデジタル化の設計思想や進捗状況など、日本に固有の事情もあるに違いないが、日本におけるデジタル社会の強靭性は、他国に後れを取っている印象を受ける。しかし自身を顧みても、非常事態時に適切に行動し、ディスインフォメーションに惑わされないでいられるか、自信は必ずしもない。

ただし、筆者は三年間の欧州出向で痛感したのだが、外からは一見一枚岩に見える欧州諸国においても、いまださまざまな問題への各国の取り組みには開きがあり、また各国固有の言語や文化的背景を理由に、必ずしも相互理解が十分に進んではいない。であるからこそ、各国のベスト・プラクティスの共有の重要性が叫ばれているという点である。サイバーセキュリティの分野で例えれば、EUの「ネットワークおよび情報システムセキュリティ指令（NIS指令）」の改正手続き（NIS指令2）は、各国間に統一的運用を確保できなかった初版の反省を契機としていると説明されている。

また、これほど体制が整備されたように見える欧州圏内においてすら、常に法的拘束力のある規則の制定が約束されているわけではない（例としては、5Gセキュリティに関するEUツールボックス）。具体的な文脈で何がサイバー／デジタル脅威なのかの評価は、確かに各国で異なる場合もありうる。しかし、日本の現状を見ると、よりデジタルインフラの抗堪性を高めるために他国に学ぶところが多くあり、逆に日本が各国に提供できるベスト・プラクティスもあるだろう。コロナ禍が収束に向かう中、今にも増して各国との知的交流が前進し、この課題に対する日本社会の強靭性がより向上することを願ってやまない。

最後に、業務多忙の中、また自らの安全すら決して万全と言えないまさに危機的な状況において、快く時間を割いてウクライナにおける取り組みについて説明をして下さったペダックさんとカプウーティンさんには心から感謝の意を表したい。●