その常識、変えてみせる。
SHIFT

Vol.03
March / 2023

知の再分配白書

Industry Trend

～ITがよりよく世界に貢献するために～

特集

露宇戦争のサイバー領域への示唆

～第2報 我が国の国家安全保障戦略への教訓の反映の状況など～

Index

02 ［シリーズ］業界動向解説 SHIFTから世界を読む
「内製化のための従業員採用・教育」について

03 特集 露宇戦争のサイバー領域への示唆
～第2報 我が国の国家安全保障戦略への教訓の反映の状況など～

11 ［シリーズ］技術特集
攻撃者の視点から設計上の弱点を洗い出す脅威モデリング

シリーズ　業界動向解説 SHIFTから世界を読む

「内製化のための従業員採用・教育」について

近年、IT・DX 分野における「リスキリング」が、さまざまなところで取り上げられています。経済産業省では「リスキリング」について、

・デジタル社会においては、全ての国民が、役割に応じた相応のデジタル知識・能力を習得する必要がある。
・若年層は、小・中・高等学校の情報教育を通じて一定レベルの知識を習得する。現役のビジネスパーソンの学び直し（＝リスキリング）が重要。

と定義しています。ここでは、事業会社における「リスキリング」について考察します。

実際に、従業員の「リスキリング」を計画しようとしたとき、「誰に何を学んでもらうか?」は、事業会社のIT体制構築の考え方に密接に関係してくるでしょう。具体的には「内製化」の度合いが大きく影響します。「内製化の度合い」というのは、システム設計・開発を含めた仕事を社内で完結させるのか、アウトソースするのかを決めることです。

「内製化」を行わず、「アウトソース」を中心にIT 体制を組み立てる場合には、IT 予算・IT 発注に関わるスキルが不可欠となります。IT ガバナンス系のスキル、システム化構想・要件定義といった発注側が責任をもつべき上流工程系のスキル、IT をベースにビジネスを組み立てるDX 系のスキルなどが、その例です。

一方で「内製化」を中心に行う際には、システム設計・開発を社内で行うことになるため、システム開発会社に相当するIT 全般のスキルが必要です。クラウド、セキュリティなどの技術分野設計にはじまり、アプリケーション設計・プログラミング、運用まで幅広いIT スキルが求められます。

内製化の場合、別業務を行っていた従業員が、IT 分野の高度なリスキリングを行い、対応していかなくてはなりません。IPA では「ITSS（IT スキル標準）」を定義しており、IT に携わる人が習得すべきスキルが記載されているため、参考にして各企業のスキル体系を整備し、教育していただければと思います。

IT 体制構築の考え方によって、教育すべきスキルの種類は異なってきますが、「リスキリング」によって、IT人材を増やし、社会のデジタル化を進めていくことは変わりません。厳しい道のりではありますが、前に進めていくことが重要だと考えています。

【参考】
経済産業省「経済産業省の取組」
https://www.mhlw.go.jp/content/11801000/000894640.pdf

IPA 情報処理推進機構「IT 人材の育成」
https://www.ipa.go.jp/jinzai/itss/itssplus.html#section1-6

著者

細田 俊明　株式会社 SHIFT　上席執行役員 兼 アカウントビジネス推進本部 本部長

大手SIer、証券会社などでCIO室長、品質管理部長を歴任し、2017年1月、SHIFTに入社。同年10月に執行役員に就任し、その後、品質技術部門、コンサルティング部門を設立。2021年9月より、アカウントビジネス推進本部 本部長として、金融領域からゲーム領域までSHIFT事業全般を管掌。

特集

露宇戦争のサイバー領域への示唆

～第2報 我が国の国家安全保障戦略への教訓の反映の状況など～

はじめに

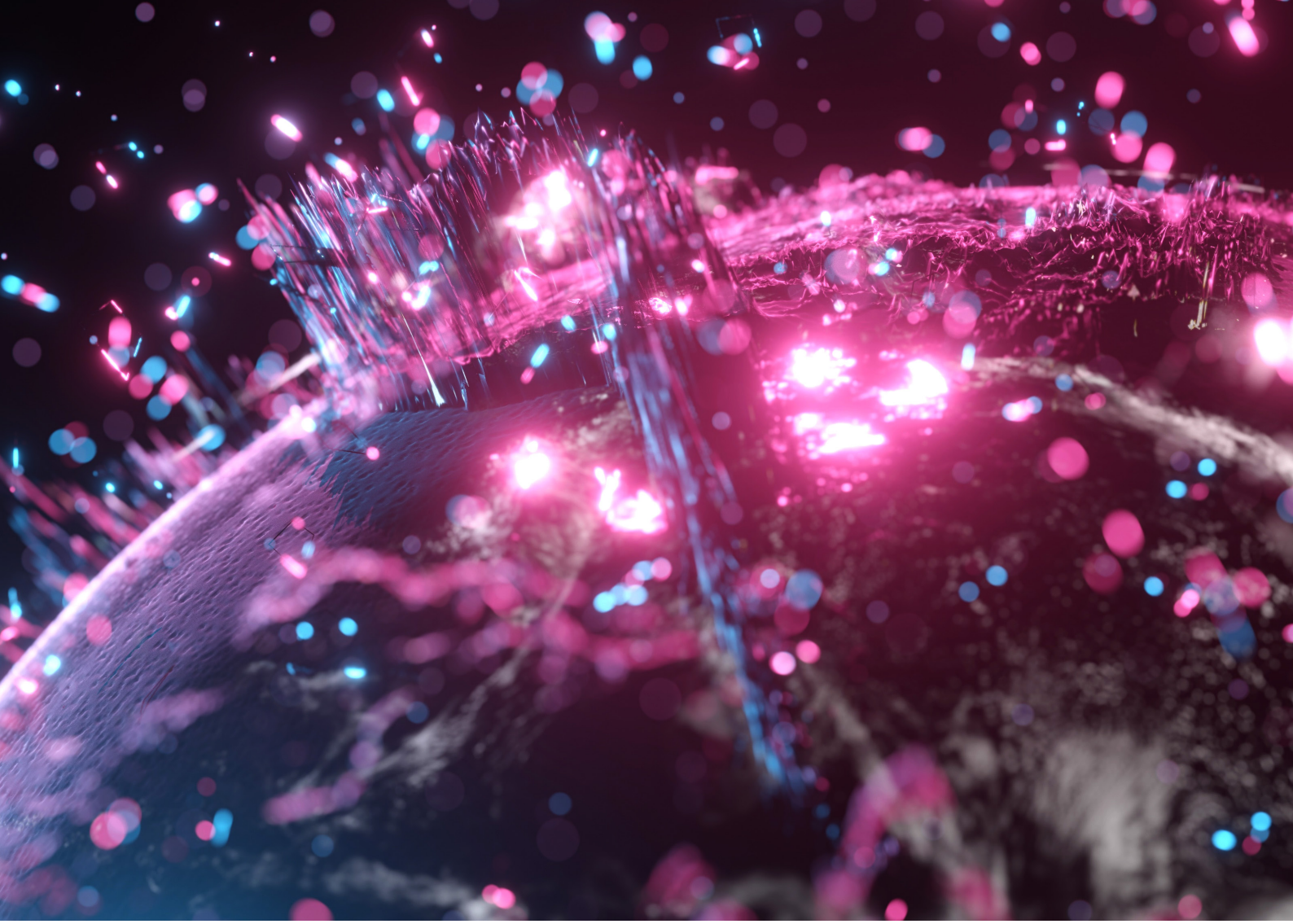
本論考は、露宇戦争のサイバー領域への示唆に関する論考の、続報の位置付けである[1]。まず、露宇戦争の教訓としてサイバー領域に示唆的な論考を紹介、次に、第1報で言及した露宇戦争において重要なサイバー基盤として注目されたスターリンク衛星システムに関してアップデートし考察。最後に、2022年末に閣議決定された国家安全保障戦略以下のいわゆる安保三文書を受け、国家安全保障戦略策定後のサイバー関連の具体的な国の施策に関する報道を概観する。

露宇戦争：オールドメインの戦い

現在、各種メディアで精力的に情報発信を行っている渡部悦和氏*1は「露宇戦争はオールドメインの戦いであり、その視点での分析が必要」と述べている[2]。

今日の戦いは、米陸軍の最新のドクトリン（マルチドメインオペレーションズ）的には、その対象とする領域は、陸、海、空の従来からあるキネティック領域に加え、宇宙、サイバー、電磁波のノンキネティックの領域にまで拡大されており、これら既存の領域に拡大した全体の優勢の争奪戦と見ることができる。

そして、現在の露宇戦争にみられるように、現実の世界においては、情報、認知、心理、経済、外交、エネルギー、法律、歴史、文化、宗教の範囲にまで拡大して考察すべき、つまり、すでに全ての領域を駆使する社会全体を巻き込んだ「オールドメイン」の戦いが常態



化しているとの同氏の指摘は極めて的を射ている。

このことを踏まえると、今日の情報化社会においては、サイバー領域は社会・経済活動のみならず、そのシームレスな延長線上にある防衛組織のC2（Command and Control：指揮・統制）機能をはじめとした防衛力発揮にも共通かつ死活的に重要な基盤であることから、オールドメインを制するためにはサイバー領域優勢を確保することが極めて重要とも言える。

なお、露宇戦争においては、ノンキネティック火力は、キネティック火力の代替手段にはなり得ていない。つまり、主戦場はキネティックな領域、国民の意志と地域の確保が重要であり、そのためにはキネティック火力を発揮する編成・装備が整えられていること、そして地域を確保できる指揮官と兵士の集合体である部隊の存在、つまり陸ドメインの重要性が示されていることも肝銘する必要があろう[3]。

＊1 元陸上自衛隊陸将、東部方面総監、ハーバード大学アジアセンターシニアフェロー

著者

菅野 隆

株式会社 SHIFT
アカウントビジネス推進本部　金融事業統括部 銀行・公共事業部　アカウントマネージャー

防衛大学校卒業後、1989 年陸上自衛隊入隊。陸上幕僚監部防衛部情報通信・研究課総括班長、第35 普通科連隊長、ハイチ派遣国際救援隊長、中央即応集団司令部幕僚副長（国内、国際）などを歴任。2022 年に定年退官し、株式会社SHIFT へ入社。
国際安全保障学会一般会員、偕行社安全保障研究委員会研究員、博士（工学）
著書「アメリカ合衆国陸軍の基本的運用の変遷と背景」NextPublising, 2022.7

サイバー領域を巡るトピック

1 露宇戦争におけるハイブリッド戦に関する論考

ハイブリッド戦とは、ワレリー・ゲラシモフ（Valery Gerasimov）ロシア連邦軍参謀総長が提案した「新たな世代の戦い方」の概念で、2014 年クリミア以降、ウクライナに対して適用してきたものであり、露宇戦争においてロシアが採用した戦い方の一部分と整理できる。

ランド研究所のウェイロン・コン（Weilong Kong）、ティム・マーラー（Tim Marler）の両氏は、論考“Ukraine's Lessons for the Future of Hybrid Warfare[4]”において、露宇戦争を「開かれた社会、閉じた社会の2つの競合するタイプの社会を持つ国家の戦い」との視点で分析している。

NATO は、軍事行動と非軍事行動を1:4の割合としたこの「ハイブリッド戦」を「敵対国の脆弱性を利用し、相乗効果を達成するために、従来型および非従来型の権力手段および転覆手段を同期的に混合した相互作用または融合」と定義している。わかりやすく言い換えると、ウクライナの民間防衛を弱体化させるため、スパイ活動、サイバー攻撃、インターネットをベースとする偽情報の配布などの能動的手段も活用しているのである。そして、その場の一つであるサイバー空間は「急速な技術の変化とグローバルな相互接続性により促進された速度、規模、強度」により、相互の影響が増しているともしており、これらの主要な特性をモデル化して統合する必要があることを主張している。

筆者らは、ロシアが 2014 年以降、ウクライナに対し使用してきたこの「能動的手段」による攻撃は、失敗したと評価している。ロシアの、スパイ活動はソーシャルメディアで圧倒され、ウクライナ侵攻の口実は暴かれ、侵攻は 2 月に延期、彼らのプロパガンダと偽情報も即座に暴露された。一方でウクライナは、ソーシャルメディアキャンペーンで、国内の士気を高め、ロシアの残虐行為を暴露し、国際的な支持・支援を集め、防御兵器のクラウドファウンディングによる支援を得た。

そして露宇戦争は、「開かれた社会」と「閉じた社会」の間での「ハイブリッド戦」の重要な特徴を実証した（している）とも主張する。双方が情報と偽情報を使用してソーシャルメディアで競争したため、いずれも従来の動員の概念を超えた「社会全体での戦争へのアプローチ」となった。つまり、ロシア側は、西側の民主主義の開放性を悪用することを目指しつつ、自らの閉鎖社会の構造に依存して自らを防御した*2。他方、ウクライナ側は、その開放性から力を引き出し、顕在化した脆弱性は技術的手段により緩和した。両タイプの社会が進化すると、将来の競争は二極化したものとなる。ただし、ウクライナに対する国際的な支援は、将来の競争において、自由で開かれた社会のメリットは、その脆弱性を上回ることができる可能性があると主張する。一方で、開放性の低い社会は、社会的動員、イデオロギー的防衛、主要な経済部門での自立により、今後増加する可能性があるともしている。

そして、複雑なシステム、部分的な可観測性、深い不確実性を伴うハイブリッド戦においては、意思決定者には、効果的な戦略を策定するための新しいツールが必要と締めくくっている。

*2 この手法は、ロシアの情報戦の常套手段である「反射統制」の原理を活用したものと考えられる。「反射統制」については次の書籍が詳しい。
参考：アンティ・バサラ, 鬼塚隆志監修,『ロシアの情報兵器としての反射統制の理論』五月書房, 2022.10.28

2 サイバー基盤（宇宙）を巡る動き（スターリンク衛星システム）

■全般

第１報でも報告したが開戦以降、イーロン・マスク（Elon Reeve Musk）氏が提供したスターリンク衛星システムにより[5][6]、ウクライナの情報通信インフラは維持されている。このことは、ウクライナがロシアに優位に立っている大きな要因でもある。スターリンク衛星システムとマスク氏によるサービス提供の判断は、これからの国際社会における不測の事態に、新たな可能性と、官民連携の観点で多くの示唆を与えているともいわれている。

■優れた抗たん性を有するシステム

スターリンク衛星システムは、高度540キロから570キロを周回する低軌道衛星を使い「ブロードバンド通信網」を構築しているもので、衛星が軌道にとどまるための燃料がなくなった場合は、大気圏に突入し、燃えてなくなってしまう仕組みである。いわば使い捨てのような衛星システムであり、消失した衛星と同数の衛星を打ち上げることで、その機能を維持する[7]。

これは、低軌道衛星コンステレーションによるものであり、電波の遅延が少なく、電波の出力が小さいもので通信可能である[8]。スペースＸは、低軌道衛星は今後も増加させる計画であり、衛星の単価も低減していくであろう。ロシアは、電子戦兵器「クラスハ-4」やサイバー攻撃などのノンキネティック火力による攻撃により、スターリンク衛星システムに攻撃を加えてきたようであるが、これまでは無力化には至っていない模様である[9]。キネティック火力による攻撃の効果に関しては伝えられておらず、費用対効果の問題があるかもしれないが細部不明である。

■テクノロジー企業にとってのメリット／デメリット

ウクライナは、共感をえる大義を世界に向けて発信できれば、国際社会が支援する可能性があることを示した。そして、ソーシャルネットワークサービスでの発信は、外交交渉に匹敵する極めて強力で即効性のあるツールであることが明らかになった。ただし、この見方は、あくまでも一つの切り口に過ぎない。

すなわち、ウクライナはサイバー戦の実験場のようでもあり、米国や欧米諸国及びテクノロジー企業は、独立した意思決定により、ウクライナに協力･支援（サイバー防御、監視、偵察）することを通じ、ロシアのサイバー攻撃に関する貴重な情報の収集・共有を受けたことにより、知識やノウハウの蓄積が可能となった。その結果、紛争のイベントの脅威にさらされた自社製品を改善することができた。加えて、これらの企業は、この取り組みを通じて社会からの尊敬と承認を獲得し、企業ブランディングにも良い影響を得ることに成功した。反面、これらは無償で支援が開始され、攻撃を含む事態のエスカレーションリスクによる影響（報復）を受ける可能性を否定することはできない。

■テクノロジー企業の経営者の意志決定への依存

クリスティン･フォックス（Christine H. Fox）氏らは、Foreign Affairsに「Big Tech Goes to War[10]」と題する、ウクライナにおけるテクノロジー企業の振る舞いを俯瞰したきわめて示唆的な論考を投稿している。

ウクライナが、スターリンク衛星システムに依存することは、マスク氏の決定に依存していることに他ならない。マスク氏は、ウクライナの要求に反し、クリミア地域でのスターリンクサービスを提供をしない決定をしているという。また、最近ではロシアが支配する地域での信頼性が低下しているともいわれている[11]。マスク氏は、ペンタゴンに対し、ウクライナにおける資金を支払うよう要請したように見えるが[12]、一方で資金提供を継続する旨を述べている[13]。

このように、スターリンク衛星システムを起動する場所と、起動しない場所に関する彼の決定は、ロシアのエスカレーションリスクに関する彼の判断に基づくものと伝えられている。つまり、スペースX社は、政府の方針や目的とは無関係に、これらを全て自ら決定しているのである。

マイケル・ロジャース(Michael S. Rogers)*3 英ブランズウィック・グループ・シニアアドバイザーは、サイバー防衛体制の教訓として、官民連携の枠組みは既に存在するものの、重要インフラや重要技術の日常的なサイバー上の安全管理が、基本的に企業の経営者に任されている現在の体制に対する不安を指摘しており*4 [14]、マスク氏の対応も、経営者の判断という観点では、その問題認識に類似した一つの大きな課題といえるかもしれない。

スターリンク衛星システムは、ウクライナを支える基盤的インフラとして、必要不可欠な位置づけにあり、これからの国際社会においても、そうであり続けると考えられるが、テクノロジー企業の経営者の判断が戦争に影響を与えることが顕著になった過去にはなかった事例といえるであろう。

*3 元米国海軍大将、米国サイバーコマンド(USCYBERCOM)第2代司令官、国家安全保障局長を兼任

*4 民間企業により所有・管理されている米国の重要インフラについて、平素のサイバーセキュリティに関しては企業が責任を負っているが、問題が発生した場合の意志決定を企業側に単独で負わせた場合、国民の安全や経済活動に重大な影響が及ぶ可能性があるという経験(2021年に発生したコロニアルパイプラインに対する犯罪グループによるサイバー攻撃。米国社会を支える重要インフラがサイバー攻撃により5日間にわたる操業停止に追い込まれた)に基づく問題認識からくる指摘
参考:「ランサムウエア攻撃で石油パイプラインが停止、犯罪組織DarkSideの手口を検証」, 日経クロステックActive, 関原 優
https://active.nikkeibp.co.jp/atcl/act/19/00324/100800001/

3 安保三文書決定以降のサイバー領域関連の報道

■経緯

露宇戦争開始10ヶ月目、奇しくも我が国では2022年12月16日、新たな「国家安全保障戦略」[15]が閣議決定された。同戦略は最新の国際・周辺情勢と今後の情勢予測や技術動向、サイバー、宇宙、電磁波の新しい領域など、安全保障をめぐる幅広い視点を踏まえた今後に向けた国家安全保障の基本的考え方(指針)であり、政府が公表した有識者との17回にわたる意見交換の結果(「新たな国家安全保障戦略等の策定に関する有識者との意見交換」[16]、2022年9月1日)を基礎として2022年9月30日以降、4回の有識者会議を経てとりまとめ、閣議決定する手順で作成されたものである。

今回の決定は、1957(昭和32)年に閣議決定された「国防の基本方針」[17]に代わるものとして2013(平成25)年に制定された「国家安全保障戦略」[18]を、初めて改定した意義がある。また、新たな「国家安全保障戦略」と同時に発出された「国家防衛戦略」[19]「防衛力整備計画」[20](これらを合わせて安保三文書と呼ぶ。)は、従来の「防衛計画の大綱」「中期防衛力整備計画」に代わるものであり、かつて中期(5年)を対象とした防衛力整備の計画が、今後10年を見据えたものに変化した。これは、現在の防衛力の実態を正確に把握し、その課題を明確にした上で、専守防衛に留意しつつ、最も厳しい情勢の地域の一つにある現在の我が国の周辺情勢下、国の平和と安全を維持する上での必要性から、我が国としての意志と態度を明確に表したものといえる。

そして、策定プロセスにおいて内閣府が公にした「新たな国家安全保障戦略等の策定に関する有識者との意見交換(議論の要旨)」には、露宇戦争の教訓に関する議論も含まれていることから、今後明らかに

なる政策や具体的な取り組みは、ウクライナ教訓が反映されていると読み取ることができよう。

■これまでの具体的な報道

新しい「国家安全保障戦略」の閣議決定を受けて、サイバー領域に関係する具体的施策についての報道の一部（抜粋）は、以下の通りである。

[a]ソフトウェアの安全基準

日米の安全保障戦略改定に伴い、日米両国政府間で、サイバー防衛で連携する第一弾として、政府が調達するソフトウェアについて両国で同レベルの安全基準を作る。さらに、クアッド（Quad）にこの取り組みを拡大するよう働きかけることを目指す。

現在の我が国の政府調達のソフトウェアには安全基準はなく、政府が安全基準に関する仕組みを導入すれば、民間にも広がると期待される。一方で、管理コストの増加も見込まれ、基準適用の範囲を絞り込むなどの配慮も検討する。

具体的には、調達する企業のソフトウェア開発工程についての安全管理体制の検証に加え、出荷前に弱点に関する分析、問題があった場合、原因を特定するなど、継続的対策を要請する。そして、安全対策チェックリストを作成し、購入者が確認できるようにする[21]。

[b]サイバー防衛

政府はサイバー攻撃を未然に防ぐための法整備に乗り出す。有事にならなければ対応できない現行法を改め、兆候段階でも攻撃元に監視、侵入などで対処する「能動的サイバー防御」を実現する。

国家安全保障戦略の骨子には、サイバー安保に関し、「新たな取り組み実現のために法制度の整備、運用の強化を図る」と盛り込むとともに、その対応力を「米欧主要国並みに強化」するとも言及。「武力攻撃に至らないものの、国、重要インフラなどに対する安全保障上の懸念を生じさせる攻撃の恐れがある場合」を想定し、被害が発生する前に悪意のあるソフトウェアを停止させることを含む「能動的サイバー防御」の導入を記した。我が国は、電力、金融などの民間インフラの防御にも国が関与できる体制作りを進める。新たな法整備においては、有事以前に、相手側のシステムの監視、侵入を可能にすることを念頭に置き、状況により反撃して攻撃を無力化する。2023年初めから与党で関連法改正や新法の議論を始める。

ロシアによるウクライナ侵攻では、政府機関や民間インフラを狙ったサイバー攻撃が相次ぎ、我が国の現行の法や体制では防げないとの見方が多かった。サイバー防御を指揮する司令塔機能を担う組織の新設に向け、内閣サイバーセキュリティセンター（NISC）を発展的に改組する[22]。

[c]自衛隊による民間企業の防護の取組

政府は、サイバー領域においても「能動的サイバー防御」を活用するため、2024年を目標に法整備を進める模様である。

自衛隊は2022年、サイバー防衛隊を新設したが、その防護対象は防衛省や自衛隊の共通ネットワークに限定され、民間の防護を見送ってきた。今後も、同盟国である米国と幅広く連携していくためには、我が国は官民を挙げての対応が欠かせない。平和・安全を確保する自衛隊の任務遂行に必要な範囲であれば、現行法のままでもサイバー領域での民間防護も許容されると判断

したものである。具体的には、防衛上重要で自衛隊の協力が必要な企業と連携し、サイバー攻撃の兆候を監視。重大な攻撃があると判断した場合は相手システムに接触し、攻撃を無力化するといった仕組みを検討する。

第一段階として2027年度までに防衛産業を守る態勢、第二段階として2028年度以降に電力や交通、通信といった重要インフラ事業者などに支援を拡大する[23]。

[d]人材育成

防衛省は2027年度にも防衛大学校にサイバー学科を新設する検討に入った。学生の受け入れは2028年度から始める見通し。

防衛大の専門課程は情報工学科を中心とする複数の学科にサイバー分野に関連する授業がまたがる。これらの内容を新学科に集約し、サイバーに特化した技術を学べるようにする。防衛大のカリキュラム変更や学科新設は文部科学省が所管する独立行政法人「大学改革支援・学位授与機構」が認めれば可能となる。

政府は2022年末に決めた国家安全保障戦略で、サイバー防衛の強化を打ち出し、重要インフラなどへの攻撃で社会経済活動が停止するリスクを防ぐために「能動的サイバー防御」の導入を明記した。

防衛大の学科設立に先立ち、陸上自衛隊は23年度に通信学校を「陸自システム通信・サイバー学校」に改める。サイバー教育を受ける自衛官をこれまでの100人規模から3割増やす。自衛隊サイバー防衛隊などの専門部隊の人員を27年度までに現在の4倍以上の4,000人程度、サイバーの基礎知識を持つ自衛官をおよそ2万人にする計画を立てる。

一方で、サイバーに精通する人材は民間も不足しており人手の確保が課題となっているが*5、待遇面で自衛隊や政府職員が劣後する事例が目立つ[24]。

4 考察

❶露宇戦争におけるハイブリッド戦に関する論考

論考における「ソーシャルメディアでの競争が、従来の動員の概念を超えた社会全体でのアプローチであること」との分析は、情報化社会が深化しつつある今日、そして将来に向けて、サイバー領域が、社会、国際社会における基本的社会基盤として極めて重要な位置づけに変化していることを示しており、我が国に対しては、自由で開かれた世界側として、ゼロトラストの考え方をベースとしたサイバー領域の安全性の確保、支える基盤の強度・レジリエンスの確保、情報の正確性の担保などについての示唆を与えており、重要な考慮事項である。

❷サイバー基盤(宇宙)を巡る動き(スターリンク衛星システム)

宇宙領域での優勢の保持は、サイバー優勢の観点からも今後死活的に重要である。

露宇戦争においては、マイクロソフトやスペースXのようなテクノロジー企業が、他では代替がきかない公共の国際社会インフラとして、その能力と可能性が明らかになった。裏を返せば、今後、これらの企業の経営者の判断が、作戦に影響を与える可能性がある。

我が国においては、東日本大震災以降、国や自治体のみならず、民間企業においても危機管理に対する意識が高まり、防災計画に加え、災害を含む有事に備

＊5 これに関連し、少子高齢化が進めば、人材の絶対数が不足するため、民間の有識者や技術者の防衛省自衛隊での活用については今後避けて通れない今まさに迫りつつある現実の課題である。手塚悟慶応大学教授は、「民間のデジタル人材の最大限活用の視点が不可欠。しかしながら、民間人材登用にあたっての適格性評価の仕組みがなく、スキルがあってもハイレベル情報を取り扱う部局には配置できない。海外ではIT企業と軍は一緒に動く。ウクライナは米国、英国などが官民一体で支援した。日本は全く貢献していない。機密情報を共有する英語圏5か国の枠組み「ファイブアイズ」」で連携しようとしても、提供できる情報がない国は相手にされない。」との課題を挙げている。
参考:「人材・実戦経験、基盤整備をサイバー戦争インタビュー」手塚悟慶応大学教授日経新聞 2022年12月21日2:00（2022年12月21日17:48更新）
https://www.nikkei.com/article/DGXZQOUA14CNZ0U2A211C2000000/

える対処計画や、事業継続計画の保持などの必要性について、改めて認識されるようになってきている。しかしながら、これらの視点は一般に内向きである。明文化の是非は別として、テクノロジー企業は、国家レベルの緊急事態における公共への寄与について、あらかじめ意識しておくべき時代が到来しているのかもしれない。

❸ 安保三文書決定以降のサイバー領域関連の報道

国家安全保障戦略を受けて報道されてきている一部施策は、安保三文書の提示という「包括的なアプローチ」「協力・連携体制」により、「サプライチェーンリスク対応」のためのソフトウェアの安全基準、「主動性を確保」するためのサイバー防衛、能動的サイバー防御、そして人材育成など多岐にわたり網羅されている。

これらの取り組みは、我が国においても、露宇戦争の状況に直面し、より現実的な危機感から抑止力の必要性が広く認識され、取り組みの考え方や施策の適時性、妥当性が広く受け入れられるものであると評価された結果であろう。

露宇戦争の状況を踏まえると、有事におけるサイバー領域における官民の連携は不可欠と考えられる。今般の国家安全保障戦略は、官民の人材の活用に注目しており、今後の検討が期待される。

おわりに

本論考では、第２報の位置づけで、露宇戦争の教訓としてサイバー領域に示唆的な論考を紹介、第１報で言及した露宇戦争で重要なサイバー基盤として浮上したスターリンク衛星システムに関してアップデートし考察、年末に閣議決定された国家安全保障戦略以下の安保三文書を受け、国家安全保障戦略策定後のサイバー関連の具体的な国の施策に関する報道を概観し考察を行った。

ロシアによるウクライナ侵攻の終わりは見えない。動向を引き続きウォッチしつつ、法治が行き渡り、言論の自由が保証された民主主義世界の一員として平和と繁栄に貢献する我が国において、それを支えるIT企業としての重責を認識しつつ努力を継続していく。

（2023.02.10 執筆）

【参考】

［１］「ロシアによるウクライナ侵攻開始８ヶ月の段階でのサイバー領域への示唆」, 菅野隆 株式会社 SHIFT『知の再配分白書』Vol.01 2022.12 https://service.shiftinc.jp/industry-trend/7890/

［２］ 渡部悦和、井上武、佐々木孝博『プーチンの「超限戦」―その全貌と失敗の本質』株式会社ワニブックス（2022.12.10）9-11頁

［３］［２］）11頁

［４］ Weilong Kong, Tim Marler, “Ukraine’s Lessons for the Future of Hybrid Warfare” https://nationalinterest.org/feature/ukraine%E2%80%99s-lessons-future-hybrid-warfare-205922

［５］「スペースX、ウクライナに衛星ネット接続サービス提供マスク氏表明」CNN, 2022.02.28 Mon posted at 12:42 JST https://www.cnn.co.jp/tech/35184139.html

［６］「ウクライナ政府へ衛星ネットサービスの端末を大量供与、米国」CNN, 2022.04.07 Thu posted at 17:15 JST https://www.cnn.co.jp/usa/35186011.html

［７］「ウクライナ軍を支える通信安保の強力ツール低軌道衛星コンステレーション」山崎文明、エコノミスト Online, 2022.7.4

［８］［２］）135 頁

［９］［２］）136 頁

［10］Christine H. Fox and Emelia S. Probasco, “Big Tech Goes to War”, Foreign Affairs October 19, 2022 https://www.foreignaffairs.com/ukraine/big-tech-goes-war

［11］「ウクライナ軍に通信障害、費用問題からスターリンク端末1300台が接続不能に」CNN, 2022.11.05 Sat posted at 18:15 JST https://www.cnn.co.jp/tech/35195610.html

［12］「ウクライナに提供のスターリンク、米国防総省の拠出なければサービス中止 もスペースXが要請」CNN, 2022.10.14 Fri posted at 11:02 JST https://www.cnn.co.jp/tech/35194623.html

［13］「イーロン・マスク氏、資金提供なくても『スターリンクは継続』」CNN, 2022.10.25 Tue posted at 10:18 JST https://www.cnn.co.jp/tech/35195081.html

［14］“Ukraine’s cyber power shows value of public-private partnership” interview with Adm. Mike Rogers by Mr. Ken Koyanagi. Nikkei Asia, October 30, 2022 16:30 JST https://asia.nikkei.com/Politics/Ukraine-war/Ukraine-s-cyber-power-shows-value-of-public-private-partnership

［15］「国家安全保障戦略について」内閣官房 , 令和４年 12 月 16 日 https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf

［16］「新たな国家安全保障戦略等の策定に関する有識者との意見交換」内閣官房 https://www.cas.go.jp/jp/siryou/pdf/yousi.pdf

［17］「国防の基本方針」内閣官房 https://www.cas.go.jp/jp/gaiyou/jimu/taikou/1_kokubou_kihon.pdf

［18］「国家安全保障戦略について」内閣官房 , 平成 25 年 12 月 17 日

［19］「国家防衛戦略について」内閣官房 , 令和４年 12 月 16 日 https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueisenryaki.pdf

［20］「防衛力整備計画について」内閣官房 , 令和４年 12 月 16 日 https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueiryokuseibi.pdf

［21］「ソフトウエアに安全基準　日米、サイバー防衛で覚書へ　政府調達でインフラなどの対策強化」日本経済新聞 , 2023.01.05 https://www.nikkei.com/article/DGXZQOUA0314J0T00C23A1000000/

［22］「サイバー防衛、法整備へ　重要インフラ、平時から攻撃元監視　防衛３文書に明記」日本経済新聞 , 2022.12.11 https://www.nikkei.com/article/DGKKZO66735200R11C22A2MM8000/

［23］「自衛隊、民間企業をサイバー防護へ　機密情報の流出防止」日本経済新聞, 2022.12.31 https://www.nikkei.com/article/DGXZQOUA21BO90R21C22A2000000/

［24］「防衛大学校にサイバー学科、27 年度にも　幹部候補を養成」日本経済新聞, 2023.1.10 https://www.nikkei.com/article/DGXZQOUA2773Q0X21C22A2000000/

シリーズ

技術特集

Vol.03

攻撃者の視点から設計上の弱点を洗い出す脅威モデリング

はじめに

セキュアなソフトウェアを開発するためにソフトウェアの設計工程で実施する「脅威モデリング（threat-modeling）」という方法論をご存知だろうか。脅威モデリングは、攻撃者の視点で攻撃シナリオを洗い出し、防御策をソフトウェアの設計に反映させる方法論であり、近年、「セキュア・バイ・デザイン（Secure by Design）」、「シフトレフト（Shift Left）」などの概念で提唱されているソフトウェアの上流工程からセキュリティ対策を実践するための活動として、主要な標準やガイドライン（NIST SP800シリーズ、ISO/IEC 27002:2022、FedRAMP、ISMAP など）でも明記されている。

しかしながら、この脅威モデリングについては、具体的な実施方法を解説した文献が少ないことや、セキュアソフトウェア開発を推進できる人材が開発チームに少ないことなどから、実際のソフトウェア開発の現場ではあまり実施されていないのが現状だ。

本稿では、この脅威モデリングの重要性と実施手順の概要を解説するとともに、脅威モデリングの効果的な活用について述べていく。

脅威モデリングとは

「脅威モデリング」と聞くと、ソフトウェア開発のための特別な方法論と思われるかもしれないが、ソフトウェア開発に限らず、攻撃者からのリスクを回避する方法として、古くから無意識的に実践されてきた。

例えば、近世以前に築かれた城の多くには、敵からの攻撃を想定したさまざまな防御の工夫が施されている。城の周囲を何重もの堀で囲んだり、城の中心部に至るまでの経路を壁で迷路状にしたり、城内にいくつもの狭い門を設置したり、隠し通路をつくるなどが、まさにそれである。これらは、築城する場所の地形的特性などを踏まえ、着工する前の設計段階で、あれこれと敵の攻撃シナリオを想定して生み出された工夫だと想像できる。

本稿で解説する「脅威モデリング」は、このような活動をソフトウェア開発の場面で実践するものであり、攻撃者が仕掛けてくるさまざまな悪用ケース[*1]を予め想定し、それらの脅威に対抗するための防御方法を、ソフトウェアアーキテクチャーやソフトウェアの詳細設計に反映させるものである。

著者

増田 佳弘　株式会社 SHIFT　サービス＆テクノロジー本部 技術統括部 セキュリティサービス部

大手事務機器メーカーにて、顧客向けクラウドサービスやソフトウェア商品に関するサイバーセキュリティ対策やCSIRT/PSIRTの構築運用をリーディングし、2022年1月、SHIFTへ入社。
現在は、セキュアソフトウェア開発運用、DevSecOps、CISRT/PSIRT構築運用などのコンサルティング案件に従事している。
日本シーサート協議会 運営委員

図 1　築城における攻撃者対策

セキュアソフトウェア開発ライフサイクルと脅威モデリング

脅威モデリングを実施するメリットは、大きく2 つ。ひとつめのメリットは、設計上の弱点の抽出だ。次ページ図2 はソフトウェアの開発工程（「ソフトウェア開発ライフサイクル」と呼ばれる）を示した、いわゆる「V モデル（vee model）」であるが、セキュリティ上安全なソフトウェアを開発する際に実施すべきセキュリティ対策といえば、何といっても、リリース直前のテスト段階で実施する「脆弱性検査」を思い浮かべる方が多いかもしれない。ソフトウェア開発に携わる人のなかにも、脆弱性検査で発見された問題点をすべて潰しておけばセキュリティ上の安全性は確保されると信じている人をしばしば見かけるが、実は、脆弱性検査だけではセキュリティ上の安全性を確保することは難しい。

脆弱性検査は、あくまでも完成したソフトウェアの「実装上の弱点」を発見することを目的としたものであり、先の城の例でいえば、築城後に、錠前が破られないか、城門や壁の強度は攻撃に耐えられるかなどの点検を実施することに等しく、門番が騙されて敵に侵入される、大軍勢で一斉に攻撃を仕掛けられる、裏口の通用門から侵入される、トンネルが掘られるなど、「設計上の弱点」を悪用される可能性までは確認できない。つまり、ソフトウェアの話に戻すと、なりすましログイン、DoS 攻撃、マルウェア感染させたシステム管理端末からの侵入などの悪用の可能性は、脆弱性検査では発見できないのである。

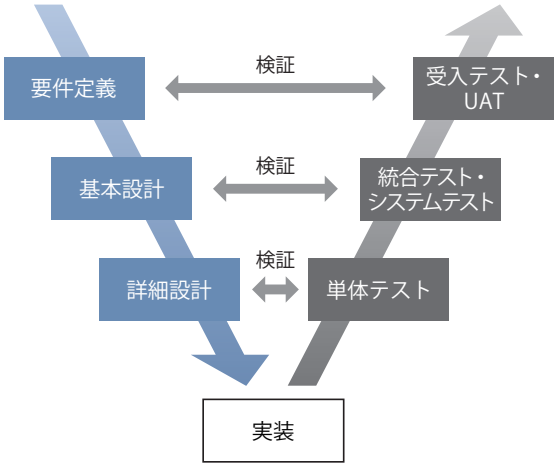
このような理由から、ソフトウェアの設計段階で脅威モデリングを実施し、実装する前に悪用される可能性を洗い出して設計に反映しておくことが重要だ。ちなみに、OWASP が定期的に発行している最新の OWASP Top10:2021*2 [1] でも、「設計上の欠陥と実装上の欠陥は別物であり、設計に起因するセキュリティ上の弱点は実装で補えるものではないため、設計段階で脅威モデリング等を実施して設計上の弱点を排除することが重要である」と記載されている（「A04:Insecure Design（セキュアでない設計）」）。

二つめのメリットは、ソフトウェア開発コストの最適化だ。ここでも、城の例で考えてみよう。例えば、数年かけて築城した後、設計が不十分で敵からの攻撃に対抗できそうにないと気づいたとする。もし、その時点から城の周囲に堀を巡らしたり、城内に迷路状の壁をつくったりというような大規模改修工事をしたら、莫大な時間と費用が必要だ（工事している間に敵が攻めてくるかもしれない）。

＊1 ソフトウェアの設計時に機能仕様として具体化する正常操作としての「ユースケース（use case）」と対比し、攻撃者が悪意を持っておこなう操作は「アブユースケース（abuse case）」と呼ばれる。
＊2 OWASP(Open Web Application Security Project)が定期的に発行している Web アプリケーションに関する 10大リスクのランキング。

このことはソフトウェア開発でも同様であり、設計段階で脅威モデリングを実施しておかないと、実装後に気づいた悪用ケースに対処するための設計変更や修正に多大な時間とコストが必要となり、場合によっては、リリース納期を優先するために対策が不十分なままの状態でリリースしてしまうことにもなりかねない。このように、設計変更に伴う改修コストを最適化するためにも脅威モデリングの実施は、非常に重要だ。ちなみに、リリース後の保守段階で気づいてから修正するコストは、設計段階で修正するコストに比べて約100倍になってしまうという研究報告がある[2]。

図 2 ソフトウェア開発プロセスの V モデル



脅威モデリングの実施手順

さて次に、脅威モデリングの実施手順について述べることにしよう。脅威モデリングの方法論の元祖は、1999 年にマイクロソフトのLoren Kohnfelder と Praerit Garg によって提唱されたSTRIDE である。それ以降、PASTA、Trike、TARA、STRIDE-LM などさまざまな手法が考案されてきているが、ここでは、もっとも標準的なSTRIDE に基づき脅威モデリングの実施方法について概説する。

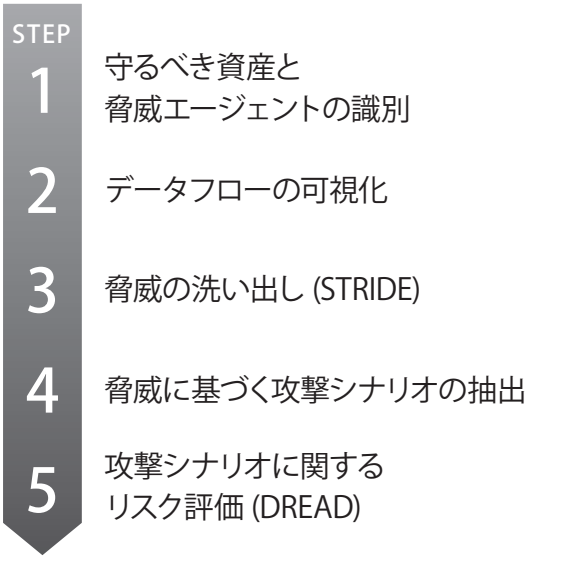
脅威モデリングを実施するタイミング

脅威モデリングを実施するタイミングは、基本設計が終了した段階で実施するのが一般的だ。これは、脅威モデリングを実施するにあたり、システムを構成する要素間でのデータの流れ（データフロー）が決まっていないと効果的な分析ができないことが理由である。なお、後述するが、脅威モデリングは、セキュア設計以外の目的でも実施することがあり、そのような目的で実施する場合は、必ずしも基本設計終了後に実施する必要はない。

脅威モデリングの５つの実施ステップ

脅威モデリングは、図3 に示すような5 つのステップで実施する。以下に、それぞれのステップについて簡単に説明していく。なお、脅威モデリングの実施ステップは、想像力／創造力を要する活動であるため、ひとりで実施するのではなく、ソフトウェアの設計開発や運用に関わるメンバーと共にディスカッションし、さまざまな観点からアイデアを出し合いながら実施していくことが望ましい。

図 3　ソフトウェア開発プロセスの V モデル



STEP1：守るべき資産と脅威エージェントの識別

脅威モデリングの最初のステップは、攻撃者から守るべき資産（データやシステムなど）と、それら守るべき資産に対して、脅威エージェント（攻撃者）がどのような動機で攻撃してくる可能性があるかを列挙することである。公知の情報しか保持しておらず、システム停止しても何ら事業影響を受けないようなWebアプリケーションであれば、脅威はほとんどゼロに等しい。しかし、通常、多くのシステムでは、攻撃者から狙われる情報資産や、停止すると事業上の損失を被るサービスが存在する。まずは、そのような「守るべき資産」を、表1に示すような観点から特定する。

次に、上記で洗い出した「守るべき資産」それぞれに対して、攻撃をしてくる可能性がある「脅威エージェント（攻撃者）」と、「想定される攻撃動機」を以下のような形で列挙する。（表2）

なお、ここでの抽出結果は、STEP4で実施する攻撃シナリオの抽出とSTEP5で実施するリスク評価で利用していく。

STEP2：データフローの可視化

STEP2では、基本設計で作成したシステム構成図やネットワーク構成図などを元に、システムを構成する要素間（対象サービスと外部サービスなどの間）でのデータのやりとりをDFD（Data Flow Diagram）として可視化し、STEP1で抽出した守るべき資産の位置を明確にする。そしてさらに、サイバー攻撃から守る範囲、つまり、開発しているシステムの範囲を信頼境界（Trust Boundary）として点線で囲み、その信頼境界上の、外部要素との接点を攻撃界面（Attack Surface：攻撃を仕掛けられる可能性がある界面）としてマークする。次ページ図4に例を示す。

なお、データフローダイアグラムを作成するための無償ツールとして以下のようなものが公開されており、これらを用いて作図することも可能だ。

・Microsoft Threat Modeling Tool[3]

・OWASP Threat Dragon[4]

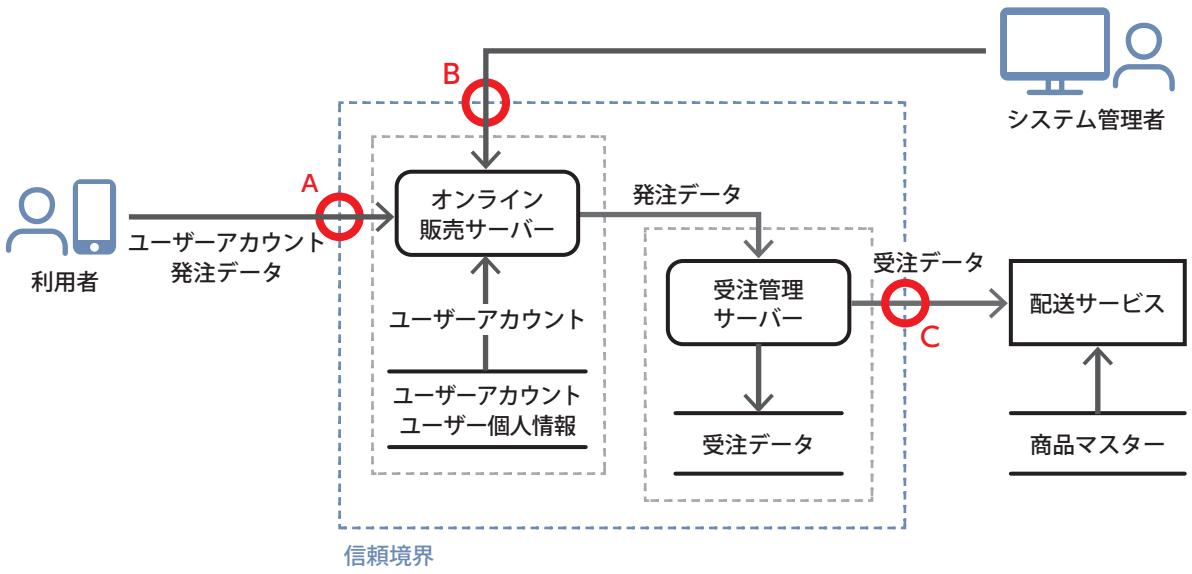
表1　守るべき資産の分析

カテゴリ	説明	守るべき資産（例）
データ	窃取・改ざん・破壊などの被害を受ける可能性がある情報資産	ユーザーアカウント、ユーザー個人情報、クレジットカード情報、銀行口座情報、顔写真、購買履歴など
サービス	システム停止による影響を受ける可能性があるサービス	アプリケーションサービス
基盤環境	上記サービスが稼働するクラウドやデータセンター基盤	クラウド基盤、仮想化基盤、ミドルウェア、コンテナエンジン
物理環境	物理的な攻撃を受ける可能性があるハードウェア	IoTデバイス、専用端末

表2　脅威エージェントと攻撃動機の分析例

守るべき資産（攻撃対象）	脅威エージェント	攻撃の動機
ユーザー個人情報	サイバー犯罪集団	窃取した個人情報をダークウェブ上で販売
ユーザー個人情報	サイバー犯罪集団	窃取データの暴露、データ暗号化などによる身代金要求
アプリケーションサービス	ハクティビスト	政治的主義主張に基づく事業妨害
技術情報	従業員	産業スパイからの働きかけによる情報持ち出し

図4　データフローダイアグラムの例



STEP3：脅威の洗い出し

STEP3では、STEP2で明確にしたすべての攻撃界面に対して、なりすまし（Spoofing）、改ざん（Tampering）、否認（Repudiation）、情報開示（Information Disclosure）、サービス拒否（Denial of Service）、権限昇格（Elevation of Privilege）という6つの視点から想定される攻撃手法を列挙していく。[*3] なお、STRIDEという呼称は、これらの脅威の洗い出し視点の頭文字をとったものである（表3）。

例として、次ページ表4に、図4に示したデータフローダイアグラムの攻撃界面Aに注目した脅威の洗い出し結果を示す。なお、これと同様の脅威洗い出しをすべての攻撃界面（図4の例ではA～C）について実施する。

なお、表4に示す「攻撃手法」として、どのような攻撃手法が存在するか列挙するには、幅広い攻撃手法に関する知識が必要だ。これにはMITRE[*4]が

表3　STRIDE

脅威	侵害されるセキュリティ特性	説明
なりすまし（S）	認証（authenticity）	正規のユーザー（やシステム）を偽装される脅威
改ざん（T）	完全性（integrity）	データを書き換えられる脅威
否認（R）	否認不可（non-repudiation）	攻撃行為を立証できない脅威
情報開示（I）	機密性（confidentiality）	秘匿情報にアクセスできてしまう脅威
サービス拒否（D）	可用性（availability）	正規利用者の利用を妨害する行為
権限昇格（E）	認可（authorization）	正規ユーザーの権限／上位権限が奪取される脅威

＊3 STRIDE法には、攻撃界面に注目して脅威を洗い出すSTRIDE per interactionと、各要素に注目して脅威を洗い出すSTRIDE per elementsの2つの方法があるが、ここでは説明紙面の都合上、前者についてのみ説明する。
＊4 米国政府の支援を受けた非営利団体。サイバーセキュリティ、国土安全保障、ヘルスケアなどの分野での官民連携を促進している。

表 4　攻撃界面 A に関する攻撃手法の洗い出し例

攻撃界面	脅威の分類	脅威	攻撃手法（括弧内は MITRE CAPEC の ID）
A	なりすまし	エンドユーザーになりすます	漏えいアカウントによるログイン（CAPEC-600）
		偽サイトに誘導する	スピアフィッシング（CAPEC-163）
	改ざん	リクエストを改ざんする	中間者攻撃（CAPEC-662）
	否認	攻撃の痕跡が残らない	ログデータの未取得
	情報開示	構成情報の開示	フィンガープリンティング（CAPEC-541）
		セッション情報の開示	セッションハイジャック（CAPEC-593）
	サービス拒否	大量なリクエストの送信	フラッディング攻撃（CAPEC-125）
		大量アカウントロック	アカウントロックアウト（CAPEC-2）
	権限昇格	アカウントハイジャック	パスワードリセットの悪用（CAPEC-50）

作成しているCAPEC™[5]、ATT&CK®[6]、CWE™[7] などの攻撃手法に関する知識ベースを活用するのが効果的である。また、攻撃手法の洗い出しのスキルを開発するのに役立つ、以下のような無料のカードゲームが公開されているので、これらを活用して開発チーム内で楽しみながらスキルを身につけることも有効だ。

・Microsoft Elevation of Privilege (EoP) Thereat Modeling Card Game[8]

・OWASP Cornucopia[9]

STEP 4：攻撃シナリオの抽出

STEP4では、STEP1で特定した守るべき資産と攻撃エージェントの攻撃動機に対応させ、STEP2とSTEP3で抽出した各攻撃界面への攻撃手法を悪用した場合に想定される、具体的な攻撃シナリオをピックアップする。なお、オリジナルのSTRIDEでは、図5に示すような攻撃ツリーとして攻撃手段をブレークダウンしていく方法を用いるが、次ページ図6に示すような攻撃者の典型的な攻撃ステップ（調査、侵入、探索、攻撃実行）に従って攻撃シナリオを抽出することで、攻撃ステップとして攻撃シナリオを表現することが可能だ。

図 5　攻撃ツリーを用いた攻撃手段のブレークダウン

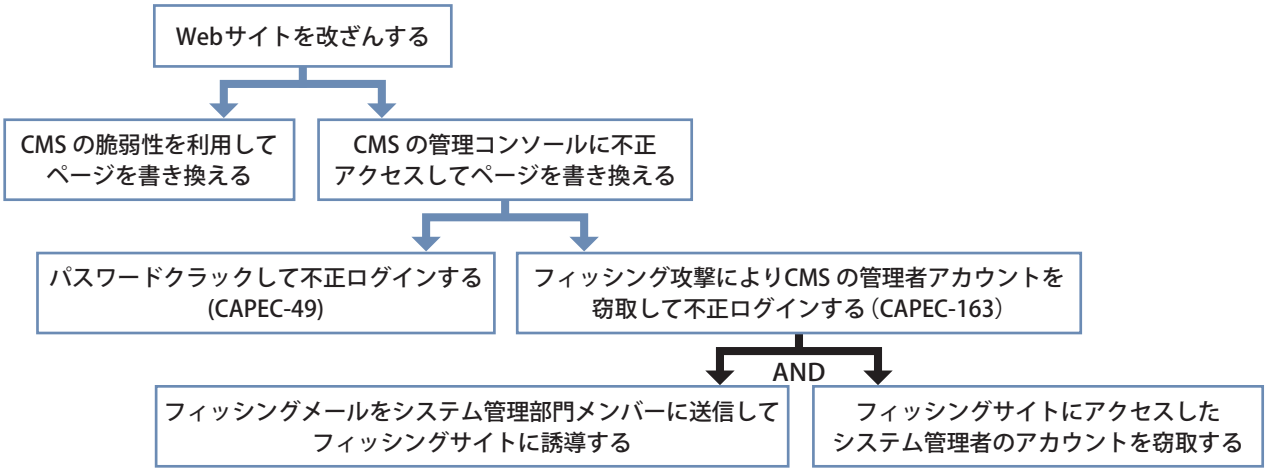
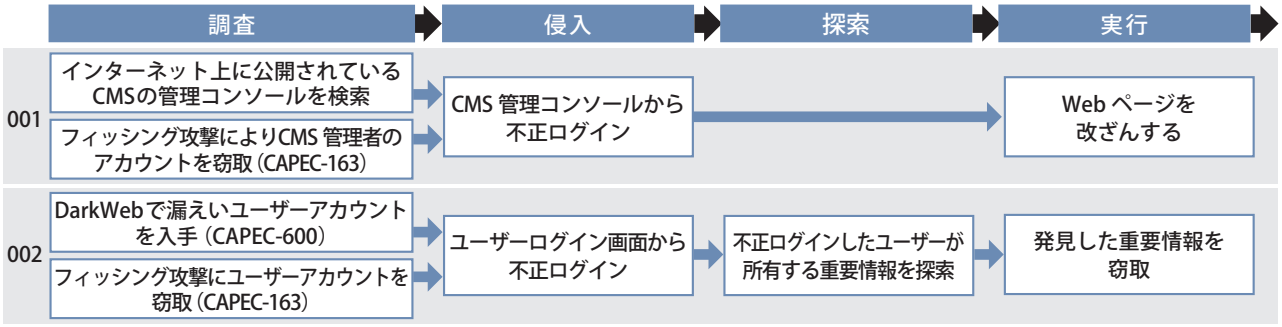


図 6　攻撃ステップに注目した攻撃シナリオの抽出



STEP5：攻撃シナリオに関するリスク評価

STEP5 では、STEP4 で抽出した各攻撃シナリオについて、表6 に示すような、発見容易性（Discoverability）、再現性（Reproducibility）、攻撃容易性（Exploitability）、影響ユーザー数（Affected Users）、被害（Damage）の観点（各項目の頭文字をとってDREAD と呼ばれる）からレベル評価をおこない、リスク値を算出する。なお、リスク値は、以下に示すように、発生可能性の因子と影響の因子の積で計算する。

そして、リスク値の大きい脅威シナリオから優先的にリスク対応方針（軽減、回避、移転、受容）と具体的な対応策を検討していく。表7 にこれら一連のリスク評価の実施例を示す。

リスク値
＝ 発生可能性×影響
＝（発見容易性Di ＋再現性R ＋攻撃容易性E）/3
×（影響ユーザー数A+ 影響D）/2

以上が、脅威モデリングの実施ステップの概要である。

表 6　DREAD の評価指標

項目	説明	レベル	定義
発見容易性 (Di)	どれくらい攻撃対象システムの弱点を発見しやすいか	3	比較的容易に弱点を発見できる
		2	探索やテストなどをすれば弱点を発見することができる
		1	管理者権限や設計情報が無ければ弱点の発見は困難
再現性 (R)	どれくらい複雑な攻撃ステップを踏む必要があるか	3	既知の攻撃手法・ツールを用いて容易に攻撃可能
		2	認証突破など特定の条件が揃えば攻撃が可能
		1	攻撃を成功させることは、ほぼ困難
攻撃容易性 (E)	どれくらいの技術的スキルが必要とされるか	3	スキル・知識はほとんど必要としない
		2	ある程度のスキル・知識があれば実行可能
		1	高度なスキル・知識が必要
影響ユーザー数 (A)	攻撃が成功した場合の影響ユーザー数	3	大多数、もしくはすべてのユーザーが影響を受ける
		2	一部のユーザーが影響を受ける
		1	ごく僅かのユーザーが影響を受ける
被害 (D)	攻撃が成功した場合の影響度合いはどれくらいか	3	数日間以上に渡る業務停止をもたらす被害
		2	1 日程度の業務停止をもたらす被害
		1	数時間程度の業務停止をもたらす被害

表 7　DREAD に基づくリスク評価の実施例

攻撃シナリオ No.	DREAD 評価					リスク値	対応方針	対応策
	Di	R	E	A	D			
シナリオ 001	2	2	2	3	3	**6.0**	軽減	CMS 管理コンソール画面へのアクセスを IP 制限する
シナリオ 002	2	3	2	1	2	**3.5**	軽減	ユーザー認証に 2 段階認証を導入する

脅威モデリングの応用

これまで述べてきたように、脅威モデリングは、セキュリティ上安全なソフトウェアを設計するために有効な手段であるが、ソフトウェアの設計だけにとどまらず、脅威モデリングの結果は、以下に示すような、さまざまな場面にも活用することができる。

❶攻撃検知のための SIEM 構築への利用

サイバー攻撃の兆候の検知やサイバー攻撃による被害が発生した場合、原因究明のために、攻撃者の侵入経路となるサーバーやネットワーク機器でさまざまなログデータを取得し、それらを集約して分析するSIEM（Security Information and Event Management）を構築・運用するケースが多い。しかし、やみくもにログデータを収集しても、攻撃の足跡を追跡するのに十分なログが取得できていない可能性がある。このため、脅威モデリングで抽出した攻撃シナリオに基づいてログデータを選定してSIEM を構築することで、より効果的なログの監視が可能となる。

❷リスクマネジメントへの利用

ISMAP、FedRAMP、NIST Cybersecurity Framework、NIST SP800-171、SP800-53 などのサイバーセキュリティ関連の監査要件や管理基準に準拠するためには、リスクマネジメントを実践することが求められる。リスクマネジメントを実践するうえで、脅威の洗い出しを実施する必要はあるが、脅威モデリングの結果をリスクマネジメントのインプットのひとつとすることによって、リスクマネジメントの効率化を図れるとともに、脅威モデリングで抽出した対応方針・対応策の実施状況をモニタリングできるようになる。

❸サイバー演習への利用

サイバー演習（机上演習）を実施する場合、演習シナリオを作成する必要がある。その際、脅威モデリングで抽出した攻撃シナリオを活用して演習シナリオを作成することにより、より現実的なサイバー演習のシナリオを作成することが可能だ。

❹ペネトレーションテストへの利用

ペネトレーションテストの手法のひとつに、想定される攻撃シナリオを洗い出した上でテストを実施する「シナリオベースのペネトレーションテスト（Scenario-based Penetration Testing）」がある。脅威モデリングで抽出した攻撃シナリオをペネトレーションテストで利用することにより、検査内容の網羅性の向上や、リスクの大きさに応じた検査シナリオの選択が可能となる。

最後に

本論考では、セキュアソフトウェア開発の活動のひとつである脅威モデリングの重要性と、その実施ステップ、応用について述べた。ギリシア神話に、戦士を潜伏させた巨大な木馬を、敵自身の手で敵の城内に運び入れさせる作戦により一気に戦いの形勢を逆転させて勝利したという、有名な「トロイヤ戦争」の話がある。現代のサイバー攻撃においても、攻撃者は、時間と労力をかけ、巧妙な攻撃ステップで攻撃を仕掛けてくる。そのような攻撃に対抗できるシステムを開発するためにも、脅威モデリングを実施されることをお勧めする。

【参考】
[1] OWASP Top10:2021
https://owasp.org/www-project-top-ten/
[2] Maurice Dawson et.al Integrating Software Assurance into the Software Development Life Cycle (SDLC)
https://www.academia.edu/2431006/Integrating_Software_Assurance_into_the_Software_Development_Life_Cycle_SDLC_
[3] Microsoft Threat Modeling Tool
https://learn.microsoft.com/ja-jp/azure/security/develop/threat-modeling-tool
[4] OWASP Threat Dragon
https://owasp.org/www-project-threat-dragon/
[5] MITRE CAPEC™
https://capec.mitre.org/
[6] MITRE ATT&CK®
https://attack.mitre.org/
[7] MITRE CWE™
https://cwe.mitre.org/
[8] Microsoft Elevation of Privilege (EoP) Thereat Modeling Card Game
https://www.microsoft.com/en-us/download/details.aspx?id=20303
[9] OWASP Cornucopia
https://owasp.org/www-project-cornucopia/

知の再分配白書

Vol.03
March/ 2023

その常識、変えてみせる。

SHIFT

※許諾を得ずに無断で複写・複製・二次使用することはご遠慮ください。※掲載の写真はイメージです。※掲載の内容は 2023年2月現在のものです。