その常識、変えてみせる。
SHIFT
Vol.01

知の再分配白書

～ITがよりよく世界に貢献するために～

特集

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

2022/12

「知の再分配白書」発刊にあたって

知識や知見は、個人のものではなく、みんなのものである。もし、多くそれらを有しているのなら、世の中のために役立てるべき。そんな想いがSHIFTにはあります。そこで、私たちが培ってきた知識や知見を少しでも多くの皆さまと共有し、日々のプロジェクトにお役立ていただきたく、「知の再分配白書」と題した冊子を発刊することとなりました。

SHIFTはソフトウェアの品質保証を軸とし、コンサルティング、システム開発など、さまざまな事業を行っています。これらの事業のなかで、日々ノウハウを磨き、独自のデータを蓄積してきました。また、近年では、各業界に精通する優秀なIT人材が集まってきています。SHIFTそして従業員それぞれが有する学びを余すことなくお届けすることは、必ずや皆さまのお力になれると信じています。

今後、IT業界のトレンドや多くの方たちが興味をもつ事柄など、多種多様な記事をそれぞれの分野に長けたプロフェッショナル達が執筆していく予定です。ぜひ、ご期待ください。この「知の再分配白書」が、皆さまの製品やサービスの創造、そしてビジネスの成功に貢献できれば幸いです。

細田 俊明　**上席執行役員 兼 デジタルビジネス事業本部 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、デジタルビジネス事業本部長として、金融領域からゲーム領域までSHIFTの事業全般を管掌。

業界動向解説

SHIFTから世界を読む

上席執行役員 兼 デジタルビジネス事業本部 本部長
細田 俊明

サイバーセキュリティについて

～攻撃のタイプを見極めて、どう守るか決める～

サイバー攻撃の話題が毎日のようにメディアに取り上げられる昨今の状況を受け、記念すべき「知の再分配白書」最初の本コラムでは「セキュリティ」に関する考察をお届けいたします。

サイバー攻撃は「直接的攻撃」「間接的攻撃」の2つに大きくわけられます。

①直接的攻撃：
DDos攻撃など、大量データ送信による
サーバーなどへの直接攻撃

②間接的攻撃：
標的型メールなどによりシステムに侵入。
その後、何かを盗むなどの間接攻撃

「直接的攻撃」は、いわゆる「業務システム・基幹システム」に対する攻撃が多く、多層防御といったセキュアなネットワークの構築・監視をセキュリティの専門部隊に依頼するしか、システムを守る方法がありません。そのため、各企業でネットワーク・セキュリティの専門家を自社採用するのか、または専門企業へアウトソースするのかが、その対策のポイントとなります。

「間接的攻撃」の特徴は、いわゆる「情報システム」に対する攻撃の多さでしょう。この攻撃は業務で利用するメールやインターネットなどを経由してウィルスが侵入するため、従業員のリテラシーを上げる対策が不可欠となってきます。

数年前に発生した日本年金機構のセキュリティ事故は、「間接型攻撃」によるものでした。当時、職員のパソコンからアクセス可能な共用ファイルサーバー上に、基幹システムからもってきた個人情報入りファイルが置かれていました。そして、職員が標的型メールによってウィルス感染したことで個人情報ファイルが漏洩してしまったのです。

この例を見ても「怪しいメールを開かない」「個人情報の入ったファイルはインターネット経由でアクセスできるサーバーに置かない」といった対策を従業員各々が理解し実行することの重要性がわかるのではないでしょうか。

最近、感染したパソコンから盗んだ実アドレス、実メールを加工して、標的型攻撃を仕掛ける例も多く、手口は以前にも増して巧妙です。ランサムウェアによる身代金要求型の攻撃も増えてきています。対策は、やはり従業員教育などを通じて、各自のセキュリティリテラシーを高めていくことが必要不可欠です。ぜひ、みなさまもサイバー攻撃に備え、いまからどう守るのか対策を進めてみてください。

(参考)「日本年金機構における不正アクセスによる情報流出事案について」
https://www.nenkin.go.jp/oshirase/topics/2016/0104.html

特集

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　デジタルビジネス事業本部 金融事業統括部 銀行・公共事業部

1965年生、愛媛県出身、防大卒。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）などを経て2022年定年退官、株式会社SHIFT入社

博士（工学）、国際安全保障学会一般会員

はじめに

ロシアのウクライナ侵攻の開始は2022年2月24日とされているが、それはキネティック領域に限った話であり、「ノンキネティック」領域、とりわけサイバー攻撃は、2014年以降、継続的に実施されてきている状況であることはよく知られている。このことは、サイバー領域には、平時と有事の区分は曖昧、あるいは存在しないことの証左とも捉えることができ、周辺に専制国家が存在する我が国としても、サイバー攻撃に対処し得る「備え」と「構え」を強化し、常態化させることが極めて重要であることを示唆している。

本論考は、インターネットで公表されているいくつかのメディア発表、公刊文書、論考などを参考に、これまでのウクライナ戦争を巡るサイバー領域でのイベントを軍事（作戦レベル）の視点で概観・分析する。そして、今後の国の取り組みに資するために、これらの状況に備えるうえでの、一般的なIT基盤の整備と維持へ向けた考慮事項を教訓として列挙することを試みている。

これまでの戦況全般の概観

陸上領域におけるロシアの戦い方に関していえば*1、当初の3ヶ月の間に、大きく変化した。メディア報道を要約すると、開戦当初、ロシア軍は戦車を主体とする「機動戦」を採用したものの、それに対抗するために米国により提供された対戦車誘導弾ジャベリンなどにより消耗し、2022年5月以降、野戦砲を主体とした「火力戦」に軸足を転移した。そして、狭正面に大量の砲兵火力を集中させる旧来の「消耗戦」により、局地的な攻撃前進を成功させた。

一方、そこに至って劣勢となったウクライナは、専制国家の不正な意図から自由と民主主義を守るといった大義のもと、ロシアとの圧倒的な火力差を埋める必要性を世界に向けて発信し、国際社会（欧米諸国）はそれに呼応して火力装備を提供するなどして支援した。ウクライナは、米国から供与されたM142装輪式自走多連装ロケットシステム（HIMARS）などの火力を用いて、ロシア軍の弾薬庫などの軍事重要施設をピンポイントで地道に攻撃する「非対称戦」を採用することで、彼らの継戦能力を漸減して潮目を変え、2022年9月、大規模な反撃に成功するに至った*2。他方、「消耗戦」を志向したロシア軍は自らが大きく損耗し、人員の補充に加え、装備品や弾薬の補給に大きな問題を抱え、2022年10月の時点で厳しい状況に至っている模様である。

ロシアによるサイバー攻撃

（１）2014年（クリミア危機）以降

我が国の公安調査庁の「サイバー空間における脅威の現況2022」によると、2014年のクリミア危機以降に発生した、ロシアが疑われている国際的イベントとして、ウクライナにおける大規模停電事案（2015年）（Black Energyサイバー攻撃*3）、米国大統領選におけるハッキングによるメール搾取と公開・拡散や偽情報の流布（2016年）、ジョージアでの破壊・混乱を引き起こした大規模サイバー攻撃（2019年10月）、新型コロナウィルス感染症ワクチンの開発組織に対する情報窃取を狙ったとみられるサイバー攻撃（2020年）、平昌冬季五輪の妨害（2020年）などが指摘されている*4。また、ウクライナ国内においては、2014年の選挙に干渉することを皮切りに、それ以降についても、破壊的なマルウェアで

政府機関と民間企業を標的に、サイバー攻撃を実行したなどの活動が疑われている*5。この中には、2017年6月の世界的なランサムウェア攻撃（Not Petyaサイバー攻撃）も含まれており、同攻撃では政府施設、地下鉄に加え、チェルノブイリ原発も標的とされた*6。そして、2018年2月、英国政府が、“同攻撃の責任はロシア政府にある”と断定するに至っている*7。

（２）侵攻前

侵攻の数日前、ウクライナ史上最大といわれるサイバー攻撃が、軍や銀行を含む政府のウェブサイトへのアクセスを妨害、並行してコンピュータウィルス「Hermetic Wipe」が、感染端末のデータを削除するといった大きな被害をもたらした*8。

（３）侵攻当日（D-day）

侵攻に同期させた衛星モデム数万台に対するハッキングは、米国の通信会社Viasatが所有する衛星ネットワークに対して行われたものであり、侵攻の約１時間前にウクライナ国内の通信を遮断、また、衛星ネットワークに頼っていたドイツの風力タービン数千基も停止させた*9。しかしながら、SpaceX社によるStarlinkシステム端末の提供により、インターネット接続は間もなく復旧した*3。

サイバー攻撃 侵攻前の予想と侵攻後の評価

（１）侵攻前の予想

侵攻に至らない段階の一般的な予想では、仮に侵攻する場合、キネティック／ノンキネティックの全ての領域で、ロシアは双方を連携させた攻撃（ハイブリッド戦）を実施する可能性が高いと考えられていた*10。ノンキネティックな領域について言えば、キネティックな軍事行動を支援するため、サイバー空間で３種類のキャンペーン（情報収集作戦、ウクライナ軍の妨害または欺瞞を目的とした作戦、ウクライナ国民に対する心理作戦）も実施する可能性を指摘する向きもあった。

（２）侵攻後の状況

侵攻の段階において、現実には、ロシアのサイバー領域における活動が、ウクライナ軍の戦闘能力に影響を与えてはおらず、緒戦におけるサイバー攻撃以降は、陸、海、空、宇宙といったキネティック領域における作戦、戦闘に影響を及ぼすことはなかったと言われている*11。

（３）評価

サイバー領域における活動が、現実の（キネティックな領域での）作戦及び戦闘に影響を及ぼさなかった理由については、米軍のサイバーコマンドや同国ハイテク企業が役割を果たし、ロシアのサイバー攻撃の防御に成功した可能性があると指摘されている。他方、ロシアの活動のほとんどは、そもそも情報システムを不能にする、あるいはキネティックな活動に影響を与えるものではなかった可能性がある。これは、サイバー領域は同戦争において重要な役割を担っていなかったのではないかという見解である。さらには、ロシアの能力を過大評価していたのではないかと疑問を呈する見方もある*12。

いずれにしても、ロシアのサイバー攻撃はキネティックな部隊行動には連携せず、ウクライナや同国を支援する国々に対しては、ロシアの「ハイブリッド戦」に対応する段階での幅広い議論や行動により、広くサイバー領域の重要性を認識させ、または備える貴重な機会となったことに疑いはない。欧米諸国の政

府やハイテク企業の支援を得るなどして、開戦前からウクライナが努力を重ねたサイバー領域での取り組みは、(西側の)国際社会としても適切であったと評価することは可能であろう。

次章において、これらのことも含めて、今後に資する教訓を整理したい。

教訓

(1)レジリエンス重視

大部隊による軍事作戦においては、攻撃(侵攻)に先立ち火力で打撃を加えることが定石である。この際、精密誘導火力により重要施設を標的にする可能性が高い。この打撃によりデータセンターや、そこにあるオンプレミスのサーバーは物理的に破壊され、デジタル資産はダメージを受けることになる。平素からクラウド化されていること、あるいは、非常時にクラウドに速やかに退避させる運用上の柔軟性を保持することは極めて重要である。ウクライナはクラウドにデジタル資産を退避させることにより、復旧に成功し、軍事・民事活動を継続することができたとされている*13。

今後はレジリエンスに着目し、デジタル資産に対する影響を最小限に抑制することに加え、仮に障害が発生した場合でも、イベントから迅速に回復することを重視する必要がある*14。この際のキーワードとして「予備」「冗長性」「柔軟性」などが挙げられよう。

さらに、レジリエンスを超え、抑止力を裏付ける積極的サイバー防御態勢を採用するための議論の必要性も示唆しており、欧州ではその点に関心が集まりつつあるようである*7。

(2)協力・連携体制

ウクライナは、ロシアの侵攻時に行われた大規模なサイバー攻撃にも関わらず、そのネットワークは機能を維持している。これは、2014年の危機以降、ロシアの侵攻に地道に備えてきた成果であるとの見解がある。

ウクライナは、2015年のロシアによる電力網ハッキング後、サイバーコマンドを設立したことに加え、米国及びその同盟国から技術支援を受けた可能性がある。また、米サイバー軍は2021年10月に「ハントフォワード」作戦の一環として、ウクライナにチームを派遣し、ワイパーマルウェアの検出とクリーンアップを支援した。

そして、侵攻以降は、米国をはじめとする関係国に加え、ハクティビストグループを含む組織から、サイバー攻撃を防御、緩和、回復するための支援を受けたと言われている。多くの場合「ハクティビスト」として特徴付けられる「IT アーミー」は、戦争遂行に貢献する意志を持つIT専門家の間でも大きく形成されたと言われており、防御のみならず、彼らの「標的」は公式サイト、特にプロパガンダサイトにおいて共有された。そして「IT アーミー」は、ウクライナの「攻撃的なサイバー能力」のギャップを補完したと言われている*3,*15。

これらの実績は、当事国と同盟国、民・軍パートナーとのシームレスな協力と連携が、重要であることを示している*8,*12。

(3)包括的なアプローチ

ロシア軍の軍事的行動に加え、ロシアの諜報機関は、ネットワーク侵入と、ウクライナ国内外の同盟政府を標的にするスパイ活動を実施している。彼らの活動は、軍事及び人道支援のロジスティクスの拠点である隣国ポーランドも優先しており、さらにバルト諸国に加え、他のNATO諸国の外務省を標的にする

活動も活発化しているとしている。また、これらサイバー攻撃と連携し、戦争努力を支援するために世界的なサイバー影響力作戦も実施している。

これらのサイバー活動、スパイ活動及び影響力作戦の活動は、ロシアの視点では別々の取り組みではなく、一つの戦略あるいはドクトリンのもと、一貫性のあるものであり、これらに対処するためには、調整された包括的な戦略を必要としている。

サイバー対応は、官民の協力に大きく依存しており、開かれた民主的な社会を保護するために、政府間の密接な多国間協力と包括的なアプローチが必要となる*13。

（4）サプライチェーンリスクへの対応

戦前の予想では、ウクライナのIT基盤は、従来からロシア製のソフトウェアとハードウェアで構築されていたため、ウクライナの重要なインフラサービスを麻痺させることは容易であり、ロシア側が圧倒するであろうとの見方が有力であった。しかしながら、現実には、ウクライナの重要なIT基盤に対する大規模な分散型サービス妨害（DDoS）とワイパー攻撃は成功せず、ロシアのサイバー攻撃は、ウクライナの自衛能力を抑制することに失敗した。これはウクライナ側が長年準備してきた成果と考えられており、サプライチェーンリスクに適切に対応した事例と言えるであろう*3。

一方、ロシアについて言えば、精密誘導兵器のカメラに我が国の民生品をそのまま使用、第一線への故障した携帯無線機の支給、2世代以上前の旧式装備をここに来て前線に投入する状況などがメディアで報じられている。侵攻初期に登場したロシア軍の最新装備は戦闘を通じて損耗、その整備・修理に必要な半導体等の電子部品などは枯渇し、現在入手が困難である可能性があり、これらは、ロシア側のサプライチェーンリスクが顕在化した事例と言えよう。

今日、各国では、戦いの「反対側」にあると見なされた国から調達されたソフト・ハードウェアへの依存に既に疑問を呈し、主要なソフトウェアとハードウェアのサプライチェーンに関する規制と透明性に対する要求が高まっている。さらに、重要なシステムのセキュリティを侵害する信頼されていないコンポーネントの潜在的なリスクを軽減するセキュリティアーキテクチャ（ゼロトラストなど）に移行する可能性も高まっているとされる。これらの趨勢を踏まえると、信頼性が低いと見なされた国に依存したサプライチェーンをめぐる議論が拡大する可能性があり、各国が早急に取り組むべき重要な課題である*13。

（5）情報戦 主動の確保

ウクライナは、士気を高め、国内の結束を維持し、国際的な支援を受けるため、ソーシャルメディアチャネルなどを通じてメディア空間を捉える積極的な取り組みを実施、戦略的なナラティブをコントロールすることに成功している。これは、ロシアの伝統的な情報戦に精通していることに加え、2014年のクリミア併合以来、同国がハイブリッド戦と偽情報キャンペーンに苦しめられてきたという事実に起因している可能性がある*3,*16。

国民は、公刊情報に注目することに留意し、不確かな情報に惑わされることのないよう情報の確からしさを峻別する視点が求められる。

（6）宇宙領域
（サイバー領域の基盤としての観点から）

イーロン・マスク氏から緒戦の段階で無償提供されたStarlinkは、彼のSpaceX事業の一

部である。また、2,000個以上の商用衛星を協調させる「衛星コンステレーション」の仕組みにより提供される、地上インフラに依存しない宇宙領域を活用するインターネット接続サービスであり、2015年に運用が開始されている*17。

ロシアは侵攻前の予想に反し、宇宙領域での物理的戦闘（破壊）を行っていない。この理由として、①多量のデブリ発生に伴う自国の宇宙活動への影響を懸念と②国際社会からの非難を考慮した可能性などが挙げられている。Starlinkのような冗長システムは、物理的な攻撃による機能停止が困難といった側面もある*2。

マスク氏は、緒戦の段階で端末400台をウクライナに提供し、現在は2万台規模まで増加しているとされる。ロシアの攻撃により携帯電話の通信網が破壊されるなか、ウクライナはStarlinkを軍事作戦などに利用し、情報通信や世界に向けた情報発信に活用してきた。ただし、ロシア側からのサイバー攻撃や通信妨害が激化するなか、支援所要が増加しており、今後の経費負担に関しては、米国政府と現在調整中であると報道されている*18。

宇宙領域は、以上のことを踏まえると、サイバー活動を行う上においても重要な基盤としての側面があり、通信サービスを提供する衛星及び同システムのサイバーセキュリティ、物理的防護、その法的裏付けなどについて万全を期する必要があろう。

おわりに

本論考では、ウクライナ戦争を巡るこれまでのサイバー領域でのイベントを概観するとともに、サイバー領域における今後の「備え」と「構え」のための一般的な考慮事項を列挙した。

サイバー領域は、国境のみならず、平時と有事の境界も存在しないシームレスな世界であり、現在を、平時とも有事とも捉えることが可能であろう。我が国周辺の専制国家は、国家目標を達成するために、一貫性のある戦略のもと、着実に取り組みを進捗させていると考えられる。ウクライナ戦争で得られた気づきを基礎として、この点に留意した「備え」と「構え」に万全を期するため、国家としての柔軟な取り組みが求められる。

これに関連した具体的な動きとして、米国においては、既に国防調達においては、保全が必要な情報を取り扱う全ての調達先企業に対し、NIST SP800-171の要求を満たすことを義務化する方針を打ち出し、2017年以降、米国の国防産業に適用している。これは、サイバー攻撃が発生することを前提とした「レジリエンス」を重視した取り組みの強化にほかならない。我が国においても、防衛省は今年4月に米国並みの情報セキュリティを確保するための制度を整備し、令和5年度の契約から適用することを明らかにしており、弊社においても、この取り組みに対応し得る態勢を確保していく。

ウクライナ戦争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平和と繁栄を支える我が国の、責任あるIT企業として、努力を継続していく。

（執筆 2022年11月）

(参考)

＊1 キネティックな領域として、陸、海、空、宇宙が存在するものの、本稿においては、典型的な戦況の推移を要約するため、陸上領域に限定する。

＊2 高木耕一郎「領域横断作戦の観点からのロシア・ウクライナ戦争の教訓」
https://www.mod.go.jp/gsdf/tercom/research.html#ron08

＊3 Omree Wechsler, “The War in Ukraine: Important lessons to be learnt from Ukraine’s cyber defence success”,29 Jun 2022
https://www.geektime.com/the-war-in-ukraine-important-lessons-to-be-learnt-from-ukraines-cyber-defence-success/

＊4 公安調査庁パンフレット「サイバー空間における脅威の概況2022」公安調査庁
https://www.moj.go.jp/content/001343410.pdf

＊5 Dmitri Alperovitch, “How Russia Has Turned Ukraine Into a Cyber-Battlefield-The Kremlin’s Hackers Are Already Targeting Kyiv”, January 28, 2022.
https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield

＊6 Alanna Petroff and Selena Larson, “Another big malware attack ripples across the world“,June 28, 2017
https://money.cnn.com/2017/06/27/technology/hacking-petya-europe-ukraine-wpp-rosneft/index.html

＊7 Foreign & Commonwealth Office, National Cyber Security Centre, and Lord Ahmad of Wimbledon ,“Foreign Office Minister condemns Russia for NotPetya attacks”,15 February 2018.
https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

＊8 Andrea G. Rodríguez,“Lessons from the Ukrainian cyber front”, 28/03/2022
https://www.epc.eu/EN/PUBLICATIONS/LESSONS-FROM-THE-UKRAINIAN-CYBER-FRONT~476F1C

＊9 CNN「EUと英、ロシアのサイバー攻撃を非難　ウクライナ侵攻時に衛星通信が標的に」2022.05.11
https://cnn.co.jp/tech/35187311.html

＊10 「現代の軍隊が関与する紛争では、サイバー攻撃は電子戦（EW）、偽情報キャンペーン、対衛星攻撃、および精密誘導弾と組み合わせて最もよく使用される。その目的は、情報上の優位性と無形資産（データなど）、通信、諜報資産、武器システムを劣化させ、運用上の優位性を生み出すことである。最も有害な行動は、精密誘導弾とサイバー攻撃を組み合わせて、重要な標的を無効化または破壊することである。サイバー作戦は、金融、エネルギー、輸送、政府サービスを混乱させ、防衛者の意思決定を圧倒し、社会的混乱を引き起こすことにより政治的影響を与えるためにも使用できる。ロシアは、これらの目標のいずれも意味のある規模で達成することができなかった。」
James A. Lewis, “Cyber war and Ukraine”, 2022.6.16., https://www.csis.org/analysis/cyber-war-and-ukraine

＊11 大規模なサイバー攻撃が実施された事例はあるが、軍事行動に影響を及ぼすに至っていない。例えば、「ウクライナ国営通信に対し大規模サイバー攻撃　軍優先に復旧中」ITmediaNEWS, 2022.3.29
https://www.itmedia.co.jp/news/articles/2203/29/news070.html

＊12 Daryna Antoniuk, “Report: Lessons learned from Russia’s cyberattacks targeting Ukraine”, July 8, 2022.
https://therecord.media/report-lessons-learned-from-russias-cyberattacks-targeting-ukraine/

＊13 Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War”, 2022.6.22.
https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

＊14 David Ferbrache,“Cyber resilience –lessons from Ukraine“, 27 May 2022
https://home.kpmg/xx/en/blogs/home/posts/2022/05/cyber-resilience-lessons-from-ukraine.html

＊15 “Ukraine at D+197:Lessons from the hybrid war.”, 2022.9.9.
https://thecyberwire.com/stories/d7a434583af04b1a84ab9d16bd966308/ukraine-at-d197-lessons-from-the-hybrid-war

＊16 中国やイランなどの一部の国は、ロシアの情報戦を学び取り入れている。一例として、中国は、2019年10月のソーシャルメディアでの偽情報キャンペーンを通じ、香港での民主化を求めるデモの転覆を企図し、イランのハッカーは、2020年のアメリカ大統領選挙前に有権者の個人情報を搾取し、それを使用して有権者を威嚇し、不正選挙に関する誤った情報を拡散した実績がある

＊17 「ウクライナ侵攻の裏で何が？イーロン・マスクの“技術”が生命線に」ITmediaビジネスonline, 2022.3.24.
https://www.itmedia.co.jp/business/articles/2203/24/news033_2.html

＊18 日本経済新聞「マスク氏、ネット接続費を米政府に要求　ウクライナ向け」2022.10.15.
https://www.nikkei.com/article/DGXZQOGN150BX0V11C22A0000000/

技術特集

Azure IaaS利用時における ネットワークセキュリティグループ（NSG）設定の 注意点について

上野 徹

NSGとは

今回の特集では、Azure IaaSを利用する際、NSG設定で特に注意していただきたいことをご紹介していきたいと思います。

まず、ここでとり上げるのはNSGです。NSGとは、Azure仮想マシン、仮想ネットワークサブネット間の通信制御を行うサービスとなります。「Azure仮想ネットワーク上のファイアウォールのようなもの」とお伝えしたらわかりやすいかもしれません。Azure上に作成した仮想マシンなどは、インターネットからのアクセスができる状態でデプロイされてしまうため、NSGを使用し通信制御を行います。

Microsoft参考ページ
https://docs.microsoft.com/ja-jp/azure/virtual-network/network-security-groups-overview

NSGでは、下記のフィルタリングが可能です。

- IP Address
- Port
- Application security group
- Service Tag

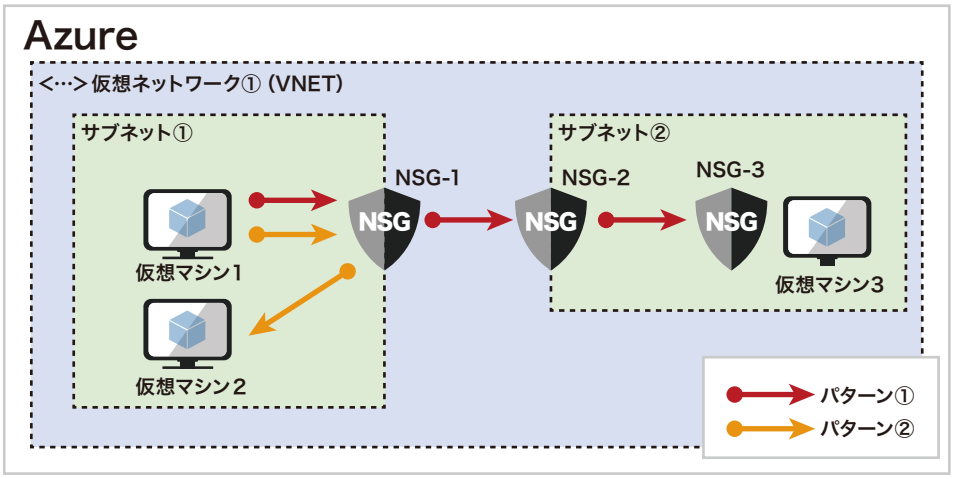
※PaaS系のサービスなどIP Addressで固定できないものがあるため、その際にService Tagを用いてアクセス制限を行います。

ポイント

- ネットワークインターフェース（以下、NIC）、サブネットに適用できる
- 1つのNSGを複数のNICあるいはサブネットに割り当てることができる
- NSGを設置できるのは1ヶ所につき1つ
- NSGはサブネットに適用できるため、仮想マシン以外のサービスにも適用可能
  （サブネットと紐づくサービス）

NSGの通信ルール適用について

つづいて、NSGを設定した際に、ルール適用される状態を見ていきましょう。今回は、仮想マシンを例として確認していきます。



上記の構成図を元に各パターンの通信ルール適用について確認していきます。

パターン①：
1. NSG-1：送信規則
2. NSG-1：受信規則

の順で評価され通信許可・拒否されます。同じサブネット内の仮想マシンであっても送信受信規則が適用されてしまうため、注意して設定しましょう。

パターン②：
1. NSG-1：送信規則
2. NSG-2：受信規則
3. NSG-3：受信規則

の順で評価され通信許可・拒否されます。サブネットおよび仮想マシンに接続されているNICにNSGを設定することにより、仮想マシン1より受信する通信を2ヶ所設定する必要が出てきます。

NSGの作成方法について

NSGの作成方法をご紹介しましょう。NSGは、Azure Portalで作成することが可能です。 リソース作成―検索窓より「NSG」を検索し、作成していきます。

Microsoft参考ページ
https://docs.microsoft.com/ja-jp/azure/virtual-network/manage-network-security-group#create-a-network-security-group

NSG作成時に作成される既定ルールについて

NSG作成時に既定でルールが作成されます。NSGのデフォルト値としておさえておきましょう。

【受信規則】

優先度	名前	ポート	プロトコル	ソース	宛先	アクション
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	任意	任意	AzureLoadBalancer	任意	Allow
65500	DenyAllInBound	任意	任意	任意	任意	Deny

※仮想ネットワーク間の通信、ロードバランサーからの通信は受信許可（Allow）され、それ以外の受信通信はブロック（Deny）される

【送信規則】

優先度	名前	ポート	プロトコル	ソース	宛先	アクション
65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	任意	任意	任意	Internet	Allow
65500	DenyAllOutBound	任意	任意	任意	任意	Deny

※仮想ネットワーク間の通信、インターネットへ通信は送信許可（Allow）され、それ以外の送信通信はブロック（Deny）される

ポイント

- 既定ルールは削除不可
- 優先度が低いルールが優先で適用される
- 既定ルールより優先させる場合は、65000より前の数値で設定する必要がある

NSG追加ルールについて

上記の通り、NSGを作成した際に、既定ルールが作成されます。もちろんそのままで利用いただくことは可能ですが、規則を追加することにより、よりセキュアな環境にすることが可能です。

例①

受信規則：既定ルールでは、仮想ネットワーク間であれば受信通信が許可されています。

仮想マシン（Windows）にて特定のIPアドレスからのみリモートデスクトップ（3389）許可したい場合は、下記の通り規則を追加します。

既定ルールにて仮想ネットワーク間の許可がされているため、「4096：DenyAllInBound」を入れて優先度1000以外の通信を拒否します。

優先度	名前	ポート	プロトコル	ソース	宛先	アクション
1000	AllowRDPInBound	3389	TCP	※IPアドレス	任意	Allow
4096	DenyAllInBound	任意	任意	任意	任意	Deny
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	任意	任意	AzureLoadBalancer	任意	Allow
65500	DenyAllInBound	任意	任意	任意	任意	Deny

例②

送信規則：既定ルールでは、「Internet」への送信通信が許可されています。

HTTPS：443のみの通信を許可する場合は、下記の通り規則を追加します。

既定ルールにて仮想ネットワーク間の許可がされているため、「4096：DenyAllOutBound」を入れて優先度1000以外の通信を拒否します。

優先度	名前	ポート	プロトコル	ソース	宛先	アクション
1000	AllowHTTPOutBound	443	TCP	任意	任意	Allow
4096	DenyAllOutBount	任意	任意	任意	任意	Deny
65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	任意	任意	任意	Internet	Allow
65500	DenyAllOutBound	任意	任意	任意	任意	Deny

※宛先を絞る場合は、「宛先」のところにIPアドレス、サブネット、Service Tagなどを入れてください。

まとめ

NSGについてお話をしてきました。NSGは便利なセキュリティ対策です。しかし、仕組みや設定内容を把握していないと脆弱なまま利用しかねないため、注意が必要となります。利用する際は、まず仕組みをしっかりおさえるようにしましょう。

上野 徹　サービス＆テクノロジー本部 技術統括部 ITソリューション部
システム運用管理サービス事業者にて、金融機関・公共インフラ・製造業などのエンドユーザーが保有する業務システムの運用管理・システム基盤設計構築案件の提案・構築に従事し、2020年8月、SHIFTへ入社。
SHIFT参画後、主にAzure案件に参画し、Azure基盤提案・構築を担当している。