［サイバー・ウォーズ］

①攻撃対象領域の増大に伴い高度化する攻撃戦略

名和利男 | サイバーディフェンス研究所

サイバーリスク・ランドスケープの限界

我が国における国家としてのサイバーセキュリティは，2018 年 7 月 27 日閣議決定により変更された「サイバーセキュリティ戦略」にある．この中で，戦略策定の前提として，サイバー空間がもたらす「恩恵」とこの空間における「脅威」の状況を的確に認識する必要があると言及している．一般に，サイバー空間における脅威は，大規模自然災害と異なり，人為的要素の占める割合が非常に大きい．そして，サイバー空間を利活用または実空間と一体化する領域は，拡大の一途をたどっており，それぞれの相互依存も増大している．そのため，リスクが複合的に重なり，多岐にわたる深刻なリスクを発生させており，時間の経過とともに大きく変動している．

このようなリスクを的確に認識する努力として，世界経済フォーラムにおけるグローバル・リスク・ネットワーク作業部会が，複合的なリスクを風景（ランドスケープ）として見渡そうとする試みをしており，2017 年に公表した「グローバルリスク報告書」において，サイバーリスクを組み込んだリスク・ランドスケープを示した．

しかし，サイバー空間と実空間の一体化が進展する中で，なぜサイバー脅威が発生するのか，どのようにしてサイバー脅威が深刻化していくのかなどを説明した見識は，技術的な観点で個別に分散しており，網羅的かつ客観的に示したものが少ない．政府機関から責任ある情報として公開された文書においても，かなり抽象的な表現にとどまっている．また，一般的なインターネット利用者は，漠然とした事例やサイバーリスクに関する情報を得られるようになってきているが，昨今のサイバー脅威に適合したセキュリティ意識と行動（対策）を変容させるような見識を十分に得られているとは言いがたい．

そこで，本稿において，一般的なインターネット利用者に昨今のサイバー脅威に適合したセキュリティ意識と行動（対策）に変容を与えることをねらい，筆者のサイバー脅威主体へのモニタ活動の経験から得られた「攻撃戦略（Attack Strategy）」と「攻撃対象領域（Attack Surface）」という 2 つの概念に基づいた状況認識を共有させていただく．まず，昨今の防衛企業に対する攻撃戦略を理解する上で象徴的な事例をいくつか紹介する．その上で，攻撃を増大させる大きな要因を IT 利活用の進展と照らし合わせて説明する．

攻撃戦略 (Attack Strategy)

実際の攻撃戦略の変化は，防衛関連組織に対するサイバー攻撃事例をレビューすることで，その一端を垣間見ることができる．

2016 年 オーストラリア

2016 年 11 月，オーストラリア国防省と契約する同国の Tier4（四次サプライヤ）レベルの防衛企業が不正アクセスに遭い，F-35 戦闘機，P-8 哨戒機，

C-130 輸送機，JDAM 誘導装置およびオーストラリア海軍の艦艇に関する技術情報が漏洩した．これらに「極秘」に該当する情報は含まれていなかったが，商業上重要な情報であり，国防や軍事に関する米国技術の輸出を管理する「ITAR（International Traffic in Arms Regulations)」によって「取扱注意」に指定されたものだった．不正アクセスを受けた防衛企業は，従業員は 50 名程度で，すべての IT システムを経験年数 9 カ月の担当者が一人で管理していた．また，同社のネットワークに緩衝領域（DMZ）が設けられておらず，定期的にセキュリティパッチを適用する保守体制も未整備であった．さらに，すべてのサーバにおいて共通の管理者 ID ／パスワードが使われ，多くのホストサーバがインターネットに接続した状態であった．オーストラリア国防省は，直接的なシステム被害はなかったが，サプライヤーである防衛企業に預けていた軍事関連情報が漏洩したことによる二次的被害が発生した．

2016 年 韓国

同年 10 月，韓国軍の Web サイトやイントラネットなどすべての IT サービスを統合管理する「国防統合データセンター（DIDC)」のネットワークに接続する 3,200 台の PC が不正アクセスを受けたことが発覚し，A4 用紙 1,500 万枚相当分の機密情報を盗まれた．この機密情報は，金正恩（キム・ジョンウン）朝鮮労働党委員長を殺害する「斬首作戦」とも言われる「作戦計画 5015」など，2 ～ 3 級の軍事機密が数多く含まれており，米軍から提供された機密資料や写真もすべて流出したと推定された．この主たる原因は，インターネット接続網と内部閉鎖網上の PC にワクチン（ウイルス対策ソフト）の検知パターンを配信する中継サーバが第三者に乗っ取られたことと，インターネット接続網と内部閉鎖網の両方に接続するファイル共有サーバ等が設置されていたことであった．つまり，攻撃ベクタは，ワクチン提供事業者というサプライヤを経由したものであった．

2016 年は，これら 2 つの防衛関連企業へのサイバー攻撃だけでなく，諸外国において多数発生した．その大半において「防衛関連組織に対するサプライチェーン攻撃」という共通性が見られた．

2017 年以降 日本

2016 年 12 月以降，防衛関連企業の NEC が不正アクセスを受けた侵入を受け，2017 年 7 月の外部との暗号通信の解読に成功するまで，内部サーバに保存されていたファイル 27,445 件への不正アクセスがされていたことが判明した．これらの情報には秘密情報は含まれていなかったが，潜水艦用センサの情報（海上自衛隊）など自衛隊装備に関連する資料が含まれていた．また，この侵入は，2014 年頃の地方の北陸地方の子会社の PC がマルウェア感染し，そこを起点に NEC 本社ネットワークに広がった可能性がある．

2019 年 3 月，同じく防衛関連企業の三菱電機の中国拠点において，ルータの脆弱性を通じて侵入され，ウイルス対策システムの管理サーバが侵害を受けて，そのアップデート機能を悪用したラテラルムーブメントが発生した．その後，この拠点で乗っ取られた海外アカウントが悪用され，国内拠点に侵入された上で，同様な手口でラテラルムーブメントが発生し，攻撃者の目的に合わせたように中間管理職の PC を標的にした攻撃が仕掛けられた．これにより，厳重な管理が求められる注意情報が外部に流出した可能性がある．

これら国内の 2 つの防衛関連企業に対するサイバー攻撃は，2016 年における韓国やオーストラリアをはじめとした諸外国の防衛関連企業に対する攻撃戦略から大幅に進展しており，「防衛関連組織グループ内の脆弱な外部拠点に対するサプライチェーン攻撃」になったと見ることができる．

攻撃戦略の進展

諸外国における防衛関連組織は，IT の利活用や

導入を進めており，そのグループの各拠点でも同様である．防衛企業の本社は，顧客（防衛省等）から直接的に影響を受ける形で，相応のコストとリソースをかけて，セキュリティ確保のための取り組みや新しい技術の導入が図られている．しかし，各拠点は，コストやリソースの制約があるため，喪失したセキュリティを取り戻すことが困難となるケースが目立っている．つまり，防衛関連組織グループ全体で，攻撃対象領域が増大しているのである．このため，攻撃戦略が進展したと考えられる．

攻撃対象領域（Attack Surface）

攻撃対象領域が増大している状況を，企業の情報ネットワークの変遷で説明する（図 -1）．

有線 LAN ベースのネットワーク

無線 LAN が一般に普及する前，企業における情報ネットワークは有線 LAN が主流だった．この有線 LAN は，物理的な配線が必要であるため，オフィスレイアウトに影響を受けていた．当時の日本企業の多くは，事務作業の能率的遂行のために最適化された配置として島型のレイアウトを採用し，1 つの課（事務機構の小区分）内での情報が行き渡りやすくさせる反面，複雑な階層構造の組織の中で課をまたぐ情報共有の必要性を少なくさせていた．そのため，有線 LAN のネットワークトポロジは，そのような島型レイアウトに影響を受ける形で，課単位でセグメント（ブロードキャストが届くネットワークの範囲）を分けていることが多かった．

このような情報ネットワークの環境にある PC がコンピュータ・ウイルスに感染した場合，課単位のセグメントというネットワークの壁を超えることが困難であるため，ラテラルムーブメント（偵察，認証情報の盗用，隣接 PC への侵入の攻撃プロセス）による被害拡大は限定的になる．つまり，ネットワーク構成の仕組みに，事実上のファイアウォール（ネットワークとネットワークの間に位置して不正アクセスをブロックするためのシステム）の機能が内在していたといえる．

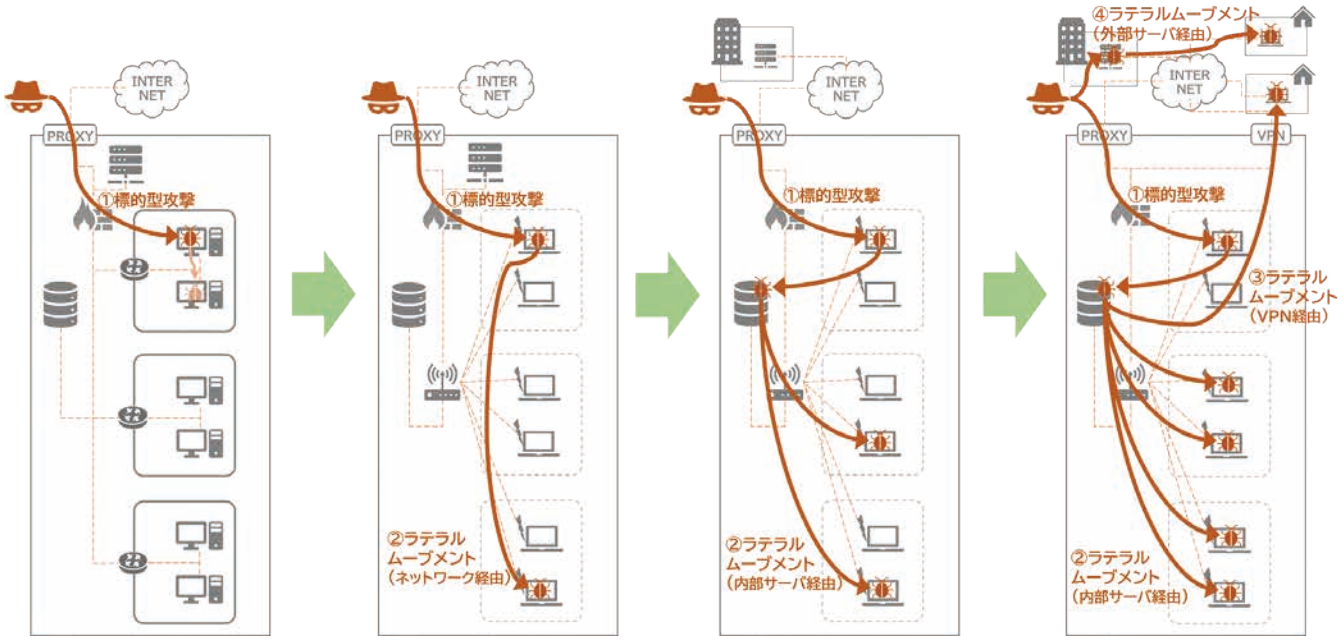

図 -1　企業ネットワークにおける利用形態の移り変わり

無線 LAN ベースのネットワーク

2000 年代中頃から，フリーアドレス（オフィスに社員の固定席を作らずに自由な席で仕事を行える仕組み）を導入する企業が増加したと同時に，一気に無線 LAN の普及が一気に進んだ．このフリーアドレスは，スペースコスト削減や社内コミュニケーションの活性化，自由な行動スタイルによる生産性の向上を期待したものとされてきたが，近年は，働き方の改革の一環として採用される一面もある．また，無線 LAN は，物理的な配線が必要なく，オフィスレイアウトに影響を受けないため，フリーアドレスとの親和性が高い．

ところが，有線 LAN の環境で得られたセキュリティ対策の機能は，無線 LAN を導入することでその一部を喪失した．最も大きなものが，オフィスレイアウトの物理的構成に影響を受けて実現していたセグメントである．これを無線 LAN で実現するには，ユーザのアクセス管理による論理的なセグメントを設けることになる．特に，フリーアドレス環境では，ユーザ権限を管理するための認証用のサーバを構築し，安定かつ厳格な運用を継続していかなければならないため，大きなコスト負担と労力が発生する．一部の企業は，フリーアドレスへの環境移行をコスト削減の一環で実施したため，新たに発生するセキュリティ対策のためのコストや労力をできるだけ避ける姿勢を持つ．現実的には，無線 LAN のセキュリティをパスフレーズによる単純なアクセス制御で運用するケースが少なくない．そのため，企業内の情報ネットワークのセグメントが複数の課をまたぐ，あるいは事実上消失してしまった．

このように，無線 LAN が急速に普及した過程の中で，セグメントの範囲を大幅に広げてしまった情報ネットワークの環境にある PC がコンピュータ・ウイルスに感染して，課をまたいでラテラルムーブメントを発生させた事例が散見されている．

Active Directory 中心のネットワーク

その後，企業の事業や人員の拡大，IT 依存の業務形態の定着，インターネットを通じたクラウドサービスの普及などにより，管理すべき PC の数が増加した．これにより，企業の IT 管理者の業務は膨大になり，IT に不慣れなユーザへのヘルプ業務が積み重なったため，IT 管理コストが大幅に増加した．これを解消する 1 つの手段として，Active Directory と呼ばれる「情報ネットワーク内の PC やユーザアカウントをまとめて管理できる機能」の利用をはじめた．この Active Directory が提供する主な機能は，情報ネットワーク内で使用する「ID・パスワードの管理」，「アクセス権限の設定・管理」，「ソフトウェアの設定・管理」，「USB メモリ等のメディア利用の設定・管理」，「プリンタなどの接続機器の設定･管理」，「Active Directory に関連したサーバに対する操作ログの取得」などである．これにより，企業，IT 管理者，ユーザに大きなメリットやコスト削減をもたらす一方，Active Directory に対する不正アクセスが発生すると，企業内のすべての PC が乗っ取られる，あるいはラテラルムーブメントによる甚大な感染拡大が発生するリスクを受け入れることになった．

さらにここ数年，企業は，オンプレミス（自社施設の構内に機器を設置してシステムを導入・運用する IT 情報基盤）あるいはホスティング（通信事業者などの専用の施設内に設置されたサーバにインターネットを通じて利用する IT 情報基盤）に要にかかわる運用・保守のコストやセキュリティにかかわる対策・管理・運用のコストを削減するために，IT 情報基盤そのものを MSP（マネージド･サービス・プロバイダ）と呼ばれる「顧客の利用する PC・サーバやネットワークなどの IT 情報基盤の運用・監視・保守などを行い，利用可能な状態を維持するサービスを提供する事業者」に委託する傾向が見られる．

このような企業の IT 管理の変化により，自社内

のIT情報基盤の管理におけるソフトウェアへの依存度が急激に高まり，さらに自社の指揮命令関係にない第三者にIT情報基盤の管理を委託するという形態が作られた．つまり，自社の責任で直接的にセキュリティコントロール可能な領域を大幅に喪失したことになる．特に，使用しているソフトウェアに脆弱性が発見され，侵害可能な状況が発生した場合，それを解決するためのセキュリティパッチの作成は，そのソフトウェアの開発元が行う．つまり，使用しているソフトウェアに脆弱性が発見された場合，企業は回避策を講じながら，セキュリティパッチが適用されるまで，待つことしかできないのである．

2018年12月，外務省が「中国を拠点とするAPT10といわれるグループによるサイバー攻撃について」というタイトルの報道官談話を発表した．このAPT10の攻撃ベクターは，MSPのネットワークに侵入し，顧客である企業のデータ窃取やネットワークに侵入することである．つまり，攻撃者は，企業に直接攻撃をせず，委託先（MSP等）を経由して攻撃を仕掛けることができるようになってきたのである．

VPNネットワーク

2020年2月頃から，国内において新型コロナウイルス感染症対策の1つとして，テレワーク（リモートワーク）を緊急導入する企業が急増した．テレワークは，自宅利用型テレワーク（在宅勤務），モバイルワーク，施設利用型テレワーク（サテライトオフィス勤務等）といった種類があり，社内の情報ネットワーク上のサーバに安全に接続するためには，VPN（インタネット上の仮想的な専用線）の利用が必要となる．VPNは基本的に一度ユーザがIDとパスワードで認証が成功すると，通信接続が継続する．つまり，つなぎっぱなしの状態になる．そのため，テレワークでマルウェアに感染したPCがVPNを通じて社内の情報ネットワークに接続すると，他のPCに対するラテラルムーブメントによるマルウェア感染の被害を発生させる可能性がある．これは，社内の情報ネットワークとインターネット間の境界防衛により実現していたセキュリティの一部を喪失したことを意味する．

実際に，VPNに関連したセキュリティインシデントが増加してことを受けて，2020年3月，米国国土安全保障省のCISA（サイバーセキュリティ・インフラストラクチャセキュリティ庁）が，新型コロナウイルス対策に伴うテレワークのVPN利用について，企業にセキュリティ上の注意喚起を行った．

攻撃対象領域の増大

近年，日本は，少子高齢化による労働人口の減少という社会環境の要因に加え，経済のいっそうのグローバル化の進展に伴う国際競争力の激化により，企業の生産性向上が重要課題となっている．これを受けて，多くの企業は，生産性向上とともに，コスト削減も期待できるITの利活用や導入が加速度的に進んでいる状況である．しかし，この過程において，企業の情報ネットワークや仕組みで得られていたセキュリティの一部が喪失していることの認識は十分ではない．それ故，喪失したセキュリティを取り戻すための取り組みや新たな技術の導入の必要性に対する理解が十分に得られない．一部ではいまだに，意思決定層がコストや人的リソースを増やすことに対する費用対効果を求めるという不条理を作り出しているため，レベルの低くなったセキュリティ状態が継続する．新たなITの利活用や導入を積み重ねていくたびに，セキュリティレベルをさらに押し下げているのである（図-2）．

このような状況を観察している攻撃側は，標的となり得る企業が攻撃対象領域を自ら増大させていると見ている．この攻撃対象領域とは，主にソフトウェア環境を攻撃対象として許可されていない第三者（攻撃者）が当該環境にデータを入力する，あるいはデータを抽出することを可能とするさまざまな

ポイント（攻撃ベクタ）の総計のことである．企業における攻撃ベクタは，多くなればなるほど組合せの数が指数関数的に増えるため，その組合せにより作られる攻撃戦略は複雑化かつ多様化する．結果として，攻撃側は，標的とした企業に対する攻撃目標の達成を容易にすることができるようになり，その規模を拡大させている．

企業が，このような悪循環が発生していることを自ら認識し，喪失しているセキュリティを確実に取り戻すための取り組みや新しい技術の導入を図り，その効果測定を徹底していかなければ，今後のサイバー攻撃による被害は，ますます甚大化していくことになる．

意思決定層の正常性バイアス

現在，企業の事業活動の推進において，サイバーセキュリティの戦略が必須となってきている．その戦略策定の前提として，意思決定層が「リスクを的確に認識」することが必要不可欠である．ところが，意思決定層の一部に，認識すらできていない，あるいはそれを避けようとする姿勢を持つ者が存在する．また，意思決定層を補佐する周辺の幹部社員が，意思決定層の認識レベルを向上させようと，多大な労力とコストをかけて努力しているが，彼らにとっての上位者にあたる意思決定層の認識や行動を変容させることは容易なことではない．特に，「現場」のサイバーセキュリティ対策に従事する者にとっては，サイバー攻撃への対処そのものより，意思決定層の低い認識による悪影響のほうが厄介で難儀なものとなってきている．

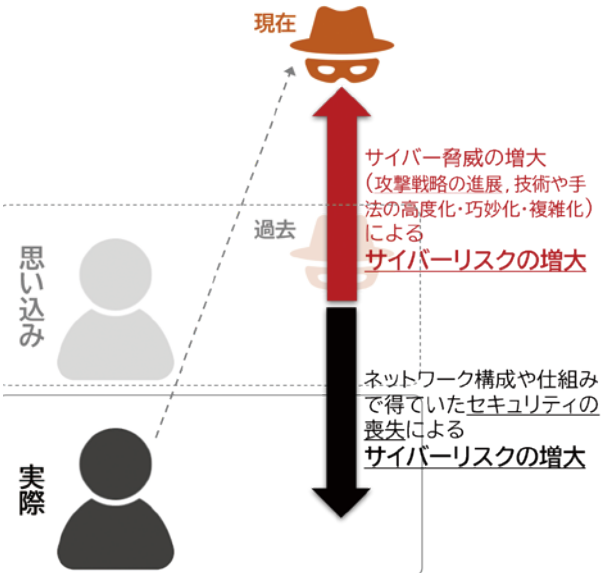

図 -2　思い込みに起因するサイバーリスクの増大

数年前から，国内のさまざまな領域でサイバーセキュリティ人材の育成事業が活発に行われているが，素晴らしい技術や知見を習得した彼らを活躍させる職場環境の整備やキャリアパスはいまだ十分とは言えない．さらに，意思決定層は，コストやリソースを必要とする取り組みや新しい技術の導入の重要性を訴える「現場」に寄り添う姿勢は，皆無に近い．

つまり，実際のサイバーセキュリティのレベルを押し下げているのは，「攻撃者の悪意のある行為」に加え，「意思決定層における正常性バイアス」と言える．正常性バイアスとは，自分にとって都合の悪い情報を無視したり，過小評価したりしてしまう人の特性である．

本稿では，主に「攻撃戦略（Attack Strategy）」と「攻撃対象領域（Attack Surface）」という 2 つの概念に基づいた状況認識を共有した．私たちは，サイバーリスクを増大させている要因の 1 つに，防御側の意思決定層によるリスク認識の不足に起因するセキュリティ低下があることを明らかにする必要がある．そして，意思決定層は，自らのリスク認識の不足が技術以上の喫緊の課題となっていることを受け入れ，今すぐに喪失し続けているセキュリティを取り戻す行動に着手しなければならない．

（2020 年 3 月 29 日受付）

名和利男　nawa@cyberdefense.jp
1971 年，北海道生まれ．航空自衛隊等を経て，2009 年にサイバーディフェンス研究所に参加．現在，宇宙システムや核物質防護を含めた重要インフラ領域におけるサイバー脅威対処や能力構築のためのサイバー演習に専念．