わたしの構想

2021. 12
no. 57

MY VISION

日常化するサイバー攻撃、問われる官民の責務

**コロナ禍でテレワークやオンラインサービスなど IT シフトが急速に進む一方で、
サイバー空間を巡る脅威は深刻さを増している。
いま、何が起きているのか。**

企画に当たって
About this Issue

柳川範之
NIRA総研 理事／東京大学大学院経済学研究科 教授

識者に問う
Expert Opinions

村島正浩
株式会社イエラエセキュリティ ペンテスター

西尾素己
多摩大学ルール形成戦略研究所 客員教授

松原実穂子
NTT チーフ・サイバーセキュリティ・ストラテジスト

坂 明
デジタル庁 Chief Information Security Officer（CISO）

神保 謙
慶應義塾大学総合政策学部 教授

日常化する サイバー攻撃、 問われる官民の責務

コロナ禍でテレワークやオンラインサービスなどIT シフトが急速に進む中で、サイバー空間を巡る脅威が極めて深刻なものとなってきた。官民を問わずサイバー攻撃に晒されているだけでなく、その脅威の次元がこれまでとは異なるものになってきたとされる。

サイバー空間でどのような脅威が起きているのか。

検討すべき対策は何か。

サイバーセキュリティの最前線で活躍する専門家に聞いた。

企画に当たって

DX下のサイバー攻撃、対策急務

――経済や社会に致命的な影響の恐れ

NIRA総合研究開発機構　理事／東京大学大学院経済学研究科　教授
柳川範之

サイバー空間のセキュリティについて、その重要性はかなり以前から指摘されてきた。しかし、ここへきて、今までとはかなり違う次元で、さまざまな問題が生じるようになってきている。にもかかわらず、それらについての意識が、まだ社会全体に十分には広まっていないように思われる。そこで今回の「わたしの構想」においては、今、サイバーセキュリティが抱える課題と重要ポイントについて、専門の識者の方々に語っていただいた。

急速なデジタル化を前に、無防備なＩｏＴ機器

官民の別なくデジタル化の重要性が叫ばれ、デジタル・トランスフォーメーション（ＤＸ）という言葉が頻繁に聞かれるようになったいま、デジタルデータが安全に管理されることの重要性は言うまでもないだろう。特に、業務に不可欠なデータや、生命の安全性に関わるようなデータのセキュリティ向上は、喫緊の課題だ。例えば、医療データがサイバー攻撃によって盗まれたり、改ざんされたりすれば、それが原因で人の命に関わる重大な事態になりかねない。今後、ＩｏＴで多くのモノのネットワーク化がより現実的になると、データの改ざんが、企業ひいては社会に致命的な問題を引き起こす可能性も容易に想像できる。

株式会社イエラエセキュリティ　ペンテスターの村島正浩氏は、ＩｏＴ機器が生活の利便性や企業の新しいサービスにとって重要であることを指摘する半面、サイバー攻撃の侵入の起点にもなり得ると警告を鳴らす。村島氏によれば、ＩｏＴ機器の問題点は、そもそも、基本的な対策すら行えていないケースが多々あることであり、それに対するセキュリティ対策の重要性が指摘されている。

国の安全保障や経済を揺るがしかねない

すべての識者が強調するのが、サイバー攻撃は、いまや、一個人や一組織の被害にとどまらない脅威となっているということだ。

デジタル庁ＣＩＳＯの坂明氏は、組織や個人、またインフラなどへの直接的なサイバー攻撃に加え、人びとや国の意思決定に影響を与える攻撃が深刻化しているとして、米国政府が、連邦機関、州や地方政府、さらには軍までが連携して、選挙を守る体制を築いている例を挙げている。また、東京オリンピックにおいても、大会運営システムや大会サイトへの攻撃、偽チケットなどの脅威があり、運営システムの強じん化など、さまざまな対応が取られていたことを明らかにし、デジタル庁は今後も、ＤＸとサイバーセキュリティの両立を目指した政策運営をしていくと決意を述べている。

NTTチーフ・サイバーセキュリティ・ストラテジストの松原実穂子氏は、＊「ランサムウェア」の脅威が、日本企業にとってまったく人ごとではなく、現実的な課題であると強調する。また、たとえ一社への攻撃でも、国の経済や安全保障への大きな打撃にもつながり得ることが示されたとして、国家安全保障のためにも、日本の政府や企業にとって、今こそ、サイバーセキュリティ対策強化に取り組む絶好のチャンスであるとしている。

日本も、より踏み込んだ対策を検討する時期に

急速に深刻化するサイバー攻撃の脅威に対し、われわれはどのような対策を検討すべきなのか。

多摩大学ルール形成戦略研究所客員教授の西尾素己氏は、さらに踏み込んで、これまで日本では、攻撃を受けた側を一律に被害者として扱ってきたが、それを改め、サイバー攻撃への対策をしなかったことに対する責任を問うべきだと主張している。そして、抑止力として攻撃能力を保有する世界の潮流に触れ、日本がいかに合法的に、実践的なサイバー攻撃を学べるかは、国益にもかかわる深刻な課題だとして、より実践的な対策の重要性を指摘している。

慶應義塾大学総合政策学部教授の神保謙氏は、サイバー攻撃で人命に危害が及べば、武力を伴う戦争に発展する可能性が強まるとして、日本もサイバー攻撃に対して、法的な制裁や自衛隊による物理的な制裁をかける「アクティブ・ディフェンス」体制の整備が必要と強調している。そして、少なくとも、サイバー攻撃に関する自衛権行使の要件については、政府の統一見解をまとめる作業を行っておくべきだと踏み込んでいる。

サイバー空間でのテロや攻撃の可能性は、経済全体あるいは国家全体を大きな危機に陥れる可能性があるという専門家の危機感は、多くの国民にとっては、なじみのない専門分野だということもあり、あまり共有されてこなかった傾向がある。しかし、今後は、サイバーセキュリティ分野の重要性を、もっと広く国民が認識する必要性があり、そのための対策を考える必要があるだろう。

人材育成に力を注げ

さらに、これらの指摘は、危機感だけではなく、人材育成の方向性を示しているようにみえる。現在では、AIやプログラミングに関する専門人材育成の必要性が強く主張されている。もちろん、これらの人材も不可欠だが、それに加えて、サイバーセキュリティを担う人材もこれからは一層重要になってくるはずだ。人材がいなければ、識者が述べているような課題に応えることはできない。そして、サイバーセキュリティの分野は、どちらかといえば、課題を緻密に解決していくという意味で、日本人にとって決して不得意な分野ではないはずで、世界的にも活躍できる可能性も十分にある。もっとサイバーセキュリティ人材の育成に、今後は、力を注いでいくべきではないだろうか。

＊巻末の用語集参照

柳川範之（やながわ・のりゆき）……NIRA総合研究開発機構理事。東京大学大学院経済学研究科教授。博士（経済学）（東京大学）。専門は契約理論、金融契約。経済財政諮問会議議員。

KEY WORDS

デジタル・トランスフォーメーション（DX）、実践的な対策、専門人材の育成

識 者 に 問 う

サイバー空間でどのような脅威が起きているのか。検討すべき対策は何か。

インタビュー実施：2021 年 10 月
聞き手：鈴木壮介（NIRA 総研研究コーディネーター・研究員）

村島正浩　株式会社イエラエセキュリティ ペンテスター

攻撃の起点になり得るIoT機器、備えを怠るな

KEY WORDS　侵入起点、基本的なセキュリティ対策、認証用証明書

西尾素己　多摩大学ルール形成戦略研究所 客員教授

組織犯罪・国家間紛争を見据えた、実効性のある対応が急務

KEY WORDS　マフィアビジネス化、エコノミック・ステイトクラフト、ネーションバック、善管注意義務

松原実穂子　NTT チーフ・サイバーセキュリティ・ストラテジスト

ランサムウェアの脅威を直視せよ

KEY WORDS　ランサムウェア、米コロニアル・パイプライン、米 JBS、CISO

坂 明　デジタル庁 Chief Information Security Officer（CISO）

DX とサイバーセキュリティを両立させていく

KEY WORDS　コロナ禍のオンライン利用、意思決定に影響、政府間の連携

神保 謙　慶應義塾大学総合政策学部 教授

サイバー攻撃は激化、アクティブ・ディフェンスを検討せよ

KEY WORDS　安全保障領域、人的被害、タリン・マニュアル、アクティブ・ディフェンス

識者に問う

サイバー空間でどのような脅威が起きているのか。検討すべき対策は何か。

攻撃の起点になり得るIoT機器、備えを怠るな

村島正浩
株式会社イエラエセキュリティ
ペンテスター

急速に増加するIoT機器は、生活の利便性を高める一方、サイバー攻撃の侵入起点にもなる。攻撃によって製品のリコールが起きれば、株価が下落し、企業はダメージを負う。ランサムウェアによる攻撃で大量のデータが暗号化され、決算を出せずに決算発表を延期した事例もある。端末やファイルサーバーを目的にWindowsの脆弱性を突くだけでなく、今後はIoT機器のデータ保存場所である＊NAS（Network Attached Storage）がランサムウェアの標的となり、企業が攻撃者との取引に応じてしまう事例が出てくる可能性がある。

攻撃者は攻撃に膨大な時間を掛けており、攻撃者優位といわれる現状を崩すのは難しい。しかし、攻撃者が有利であるから対策をしなくてよいという話ではない。狙われるリスクを事前に想定して、メーカーは対策を実装していく必要がある。IoT機器のセキュリティの観点からまず確認するポイントは、ハードウェアの実装、ファームウェア、機器やクラウドと通信するプロトコルなどだが、一台のIoT機器に投資できる開発予算やセキュリティ予算には限りがあり、全て防御するのは不可能である。サイバー攻撃では、特定の会社の知的財産を狙うケースが多い。家電など家庭用のIoT機器は、機器単体に攻撃するメリットはボットネット化を除いて少ないが、今後、IoT機器を通じて収集されたセンシングデータが市場での価値を高めると、そのデータが狙われる可能性がある。

IoT機器の問題は、そもそも、基本的な対策すら行えていないケースが多々あることだ。例えば、私が過去に見つけた脆弱性で、複数のIoT機器に、クラウドに接続する認証の際に同一の証明書（クライアント証明書や「秘密鍵」）を使っているケースがよく見られた。一つの製品を複数社のブランド名で生産しているOEM製品でも、ブランドをまたいで同一の証明書を使っていることがある。犯罪者がそのうちの一台の証明書を取得してしまえば、IoT機器の実装次第で他の全ての機器を攻撃することが可能になり、深刻な被害を招く。例えば自動車の制御に関連する箇所にこのような脆弱性が存在すれば、運転中の全車両のシステムを停止することもできてしまう。

しかし、読者はお気づきかもしれないが、攻撃を受けても阻止することは可能だ。証明書を機器ごとに変えれば、他の機器への攻撃という最も重大な脅威を防ぐことができる。セキュリティ対策において、攻撃者がどこから攻撃を行うのか想定して投資する必要がある。

＊巻末の用語集参照

村島正浩（むらしま・まさひろ）

神戸デジタル・ラボでセキュリティエンジニアとして勤務後、イエラエセキュリティでペンテスターとして活躍中。クライアントの要望に合わせ、ハッカー目線で限りなくリアルな疑似攻撃を行っている。IoTセキュリティの知見を共有するコミュニティ「IoTSecJP」の中心メンバーも過去に務める。著書に『ハッカーの教科書』（データハウス）シリーズがあり、エンジニアや初心者に向けてハッキングアプローチ方法を解説。セキュリティ啓発団体の各種イベントで講演多数。

RECOMMENDED

識者が読者に推薦する1冊

F. Chantzis, I. Stais, P. Calderon, E. Deirmentzoglou, B. Woods〔2021〕

Practical IoT Hacking

The Definitive Guide to Attacking the Internet of Things

No Starch Press

識者に問う

サイバー空間でどのような脅威が起きているのか。検討すべき対策は何か。

組織犯罪・国家間紛争を見据えた、実効性のある対応が急務

西尾素己
多摩大学
ルール形成戦略研究所
客員教授

サイバー空間の脅威について、注視すべき最近の変化を三点指摘したい。一つ目は、サイバー攻撃の「マフィアビジネス化」である。かつての政治的主張や自己顕示欲による攻撃から、今では、資金目当てに、組織化された犯罪グループが攻撃を仕掛けるものに変わっている。技術力がなくてもランサムウェア攻撃ができるプラットフォームサービスが広く使われており、元手資金も要らない。稼いだ資金を洗浄する闇の換金所も存在する。金銭を取れさえすれば、企業規模に拘わらず攻撃の対象となる。

二つ目は、大国の経済安全保障―エコノミック・ステイトクラフト―との絡みだ。トランプ政権は中国ファーウェイの製品を米国から締め出した。こうした間接的な経済制裁を行うだけでなく、米国はサイバーセキュリティを自国の経済圏を拡大する戦略にしている。すなわち、米国企業とビジネスをする外国企業にも、安全保障に関わる製品や設備、情報を扱う場合は、米国が策定したサイバーセキュリティ基準に準拠することを義務付けた。この基準に対応できない企業は、米国と取引ができなくなってしまう。

三つ目は、サイバー攻撃の背後に国家が控える「ネーションバック」といわれるものだ。相手国の国力を削ぐ目的で、国家が攻撃を仕掛ける。サイバー攻撃は攻撃元の特定と証明が難しいため、国家による他国への攻撃が、実はやりたい放題で行われている。米国、中国、ロシア政府などは、自国攻撃しない限りはサイバー空間のマフィアビジネスを黙認し、また、サイバー犯罪者と司法取引をして、そこからサイバー活動に投入する人材を獲得している。世界の潮流は、抑止力として攻撃能力を保持しており、日本がいかに合法的に、実践的なサイバー攻撃を学べるかは、国益にもかかわる深刻な課題に発展している。

危険性が増すサイバー攻撃への対応を、企業や社会に義務付けなければ、やがては日本全体の国力が削がれる。これまで日本では、攻撃を受けた側を一律に被害者として扱ってきたが、それを改め、サイバー攻撃への対策をしなかったことへの責任を問うべきだ。そのためには、責任の基準を「善管注意義務」として定義し、その範囲を明確にする必要がある。まずは政府が各省庁向けに制定し、その後、民間に波及させるのがよい。範囲が明確になれば、それがサイバーセキュリティへの投資額の目安ともなる。

西尾素己（にしお・もとき）
世界各国の著名なホワイトハットとの「模擬戦」を通じてサイバーセキュリティ技術を独学。世界トップクラスの専門家による情報セキュリティ国際会議「CODE BLUE二〇一五」に、学生枠を除く最年少として登壇。二〇一六年より、多摩大学ルール形成戦略研究所にサイバーセキュリティ領域における国際標準化研究担当の客員研究員として着任。サイバーセキュリティの視点から、国際動向の分析や安全保障起点でのルール形成活動と、それに基づく産業力強化を推進している。

識者が読者に推薦する1冊

國分俊史〔2021〕
経営戦略と経済安保リスク
日本経済新聞出版

識者に問う

サイバー空間でどのような脅威が起きているのか。検討すべき対策は何か。

ランサムウェアの脅威を直視せよ

松原実穂子
NTTチーフ・サイバーセキュリティ・ストラテジスト

ランサムウェアの被害が急拡大してきた。五月上旬、米東海岸の燃料供給の四五％を担うコロニアル・パイプラインが攻撃を受け、ガソリン不足を巡る暴力沙汰やアメリカン航空の航路変更など、東海岸を中心に大混乱に陥った。同月末には食肉大手のJBSが攻撃され、北米とオーストラリアの食肉処理工場が一時操業停止した。ランサムウェアはこれまで金銭目的の犯罪と思われてきたが、たとえ一社への攻撃でも、国の経済や安全保障に大打撃を与え得ることが示された。

そのため、米国政府は、ランサムウェア攻撃への対応を根本的に見直している。六月初め、国家安全保障担当副補佐官から企業の経営層に、サイバーセキュリティ対策の強化を要請する異例の書簡が送られた。コロニアル社が怠っていた*「多要素認証」の利用や、サイバー攻撃を受けた際の対応要領の作成など、取るべきアクションが具体的に列挙されている。驚いた企業の経営層は、自社のCISO（最高情報セキュリティ責任者）に必要な補完策を至急確認し、サイバーセキュリティ強化に取り組んだ。米国企業から取引先の他国の企業にも対策の確認が今後あれば、サプライチェーン全体のセキュリティ向上につながるであろう。

さらに一〇月には、ランサムウェア攻撃への対処策と国際協力について話し合う国際会議が、米ホワイトハウス主催で二日間、オンラインで行われた。日本を含む三〇もの国から閣僚クラスが招かれ、この種の会議では前代未聞の陣容だ。米国政府の強い意気込みが窺える。

「サイバー攻撃に屈しない」という米国の断固たる決意は「人」と「予算」の数にも示されている。七月、マヨルカス国土安全保障長官は、短期雇用の五〇〇人を含む計八〇〇人ものサイバーセキュリティに特化した人材を雇用すると宣言した。また、二〇二二年度の米国政府のサイバーセキュリティ予算は、国防部門を除いても一兆円を超える。日本政府の同年度概算要求額の九一九億円とは桁違いだ。

日本企業も、北米など海外拠点を含め、さまざまな業種でランサムウェア攻撃の被害に遭っている。米国などの各国の官民と、攻撃の手口や対策などについて緊密な情報共有を行い、被害の最小化を目指していかなければならない。国家安全保障のためにも、日本の政府や企業にとって、今こそサイバーセキュリティ対策強化の絶好のチャンスである。

＊巻末の用語集参照

識者が読者に推薦する1冊

松原実穂子〔2019〕

サイバーセキュリティ

組織を脅威から守る戦略・人材・インテリジェンス

新潮社

松原実穂子（まつばら・みほこ）
早稲田大学卒業後、防衛省にて勤務。米ジョンズ・ホプキンス大学高等国際問題研究大学院卒業後、日立システムズでサイバーセキュリティのアナリスト、インテルでサイバーセキュリティ政策部長、パロアルトネットワークスのアジア太平洋地域拠点における公共担当の最高セキュリティ責任者兼副社長などサイバーセキュリティにおける重役を歴任。現在はNTTのチーフ・サイバーセキュリティ・ストラテジストとして、情報発信と提言に努める。著書『サイバーセキュリティ　組織を脅威から守る戦略・人材・インテリジェンス』（新潮社、二〇一九年）は、第二九回二〇二〇年度大川出版賞受賞。同書は、攻撃者及び守る側それぞれの人材育成についても解説。

＊巻末の用語集参照

識者に問う

サイバー空間でどのような脅威が起きているのか。検討すべき対策は何か。

DXとサイバーセキュリティを両立させていく

坂 明
デジタル庁
Chief Information Security Officer（CISO）

社会のデジタル化の進展に加え、コロナ禍でオンラインの利用が一気に高まる中、サイバー攻撃の脅威が増大していることが、あらためて浮き彫りになった。社会の情報セキュリティの強化に取り組む「情報処理推進機構（ＩＰＡ）」は、脅威のトップに、組織に対するランサムウェア攻撃と、個人に対するスマホ決済の不正利用を挙げた。現実世界で、刑法犯などの犯罪数が減少してきている一方で、サイバー犯罪は増えており、脅威が現実世界からサイバー空間へと移ってきた。攻撃者はあらゆるレベル、分野、ターゲットに対して、常に攻撃を仕掛けており、攻める側と守る側の力がぶつかり合っているのが現状だ。

私が非常に大きな問題と認識しているのが、組織や個人、またインフラなどへの直接的なサイバー攻撃に加え、人びとや国の意思決定に影響を与える攻撃が深刻化していることだ。例えば、米国の大統領選挙では、選挙システムに対する攻撃のほか、フェイクニュースやフェイク動画といったサイバーツールを用いて世論操作を行う動きが見られた。米国政府は国土安全保障省、財務省などの連邦機関、州や地方政府、さらには軍までが連携して、選挙を守る体制を築いている。日本においても、政府機関間の連携は、今後の課題となるだろう。

二〇二一年の東京オリンピックは、大会運営システムや大会サイトへの攻撃、偽チケットなどの脅威がある中で、運営システムの強じん化、政府の対応体制・関係者との情報共有基盤の構築、国際的な協力などによって、大会運営に影響を出すことなく、大会を終えることができた。課題として、国内外の多くの企業・組織と共にシステムを構築・運用するため、それら関係者のセキュリティを確保すること、また、開催会場について、組織委員会が設置するシステムのみならず、既存施設のレガシーシステムも守る必要があったことなどが挙げられる。こうした経験はオリンピック・レガシーとして、今後の参考になるだろう。

サイバーセキュリティの前線にいる担当者は、常に相手が攻めてきている状況におかれ、戦場にいるような気持ちで戦っている。二〇二一年九月に発足したデジタル庁は、「誰一人取り残さない」というミッションを掲げ、多くの方々が安心してデジタルを利用できる社会を目指している。また、九月に閣議決定した新たな「サイバーセキュリティ戦略」では、安全保障的な観点と、一人ひとりの国民を守る「公共空間化したサイバー空間の安全安心の確保」という考えのもと、国全体のＤＸ化とサイバーセキュリティの両立を目指している。

坂 明（さか・あきら）
一九八一年、警察庁に入庁し、生活安全局セキュリティシステム対策室長、情報技術犯罪対策課長として、サイバー犯罪対策に従事。二〇〇二年にはハーバード大学国際問題研究所（ＷＣＦＩＡ）客員研究員としてサイバーテロの研究を行う。二〇〇八年から二年間、慶應義塾大学大学院政策・メディア研究科教授。二〇二一年に開催された東京オリンピック・パラリンピック競技大会では、同組織委員会ＣＩＳＯを務めた。現在、日本サイバー犯罪対策センター（ＪＣ３）理事、公益財団法人公共政策調査会（ＣＰＰ）専務理事を兼務。

識者が読者に推薦する1冊

わが国の「サイバーセキュリティ戦略」

https://www.nisc.go.jp/materials/index.html

識者に問う

サイバー空間でどのような脅威が起きているのか。検討すべき対策は何か。

サイバー攻撃は激化、アクティブ・ディフェンスを検討せよ

神保 謙
慶應義塾大学総合政策学部 教授

サイバー攻撃が人的被害を引き起こす可能性が高まっており、安全保障の領域に拡大している。DX化が進み、工場やインフラなどさまざまな施設を、ネットワークを介してリモートで制御できるようになると、システムの乗っ取りや重要インフラへの攻撃、さらに軍のオペレーションへの妨害などが可能になる。実際に、米国のガスパイプライン会社や水道局、ウクライナの電力会社の制御システムが、サイバー攻撃で被害を受けた。水道に薬品を混入されたり、大停電が引き起こされたりすれば、多数の犠牲者が出る恐れもある。サイバー攻撃で武力行使に等しい被害が出る可能性が、現実のものとなってきた。

サイバー攻撃で人命に危害が及べば、武力を伴う戦争に発展する可能性が強まる。したがって、各国が個々のサイバー攻撃を安全保障上のどのような危険度に位置付けるかという判断が、重要な局面となりつつある。これ以上の攻撃は軍事的対処を可能にするという「越えてはならない一線」を、国際的に合意することが重要だ。それが、攻撃の激化を抑止することにもつながる。基準となる「一線」について、＊「タリン・マニュアル」という国際規範では、原発の溶融やダムの破壊といった大規模な被害を想定しているが、もっと昨今のサイバー攻撃の事例に沿って基準を見直す必要がある。

日本も、サイバー攻撃に対して、法的な制裁や、自衛隊による物理的な制裁をかける「アクティブ・ディフェンス」体制の整備が必要と考える。アクティブ・ディフェンスは、まず、攻撃者・攻撃内容を把握していると相手に示す活動を行い、それにより、さらなる攻撃を防御、抑止する。ここまでは、日本政府もオリンピック開催などで実績を積んだ。次の段階では、攻撃で奪われた財産、資産を取り戻し、敵の攻撃手段を奪い取るといったアクションをとる。これは、米国などが行っているが、現在の日本には難しい。少なくとも、サイバー攻撃に対し自衛権を行使する要件について、政府の統一見解をまとめる作業は行っておくべきだ。

日本では現在、内閣サイバーセキュリティセンター（ＮＩＳＣ）、警察庁、総務省、経済産業省のサイバー部門が個別に対応しているが、これらの各省庁の部署に、横串を刺す必要がある。また、サイバー攻撃に対し世界各国との協力的枠組みを作るため、各国代表との協議のカウンターパートとなる、閣僚級のサイバーセキュリティ専門の責任者が必要だ。

＊巻末の用語集参照 NIRA

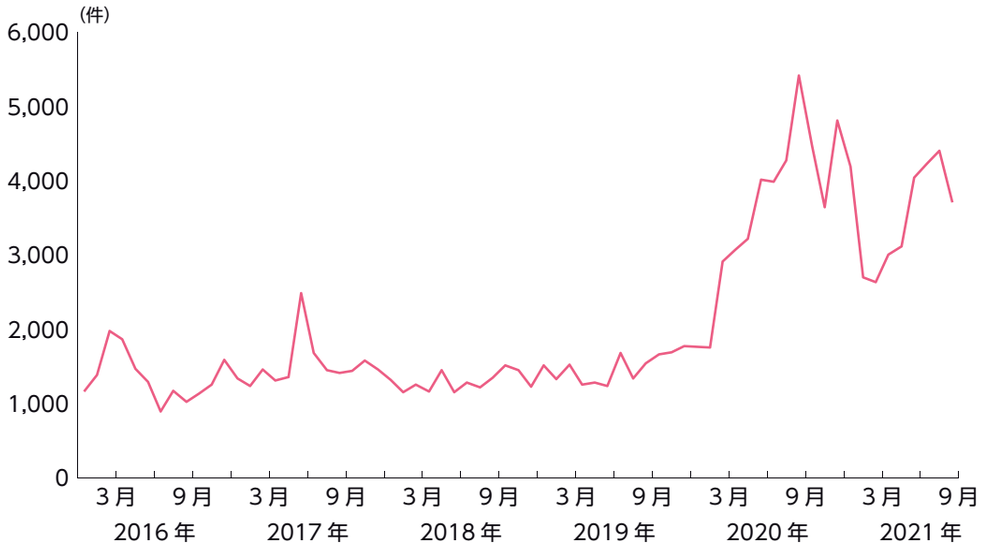
識者が読者に推薦する1冊

松原実穂子〔2019〕
サイバーセキュリティ
組織を脅威から守る戦略・人材・インテリジェンス
新潮社

神保 謙（じんぼ・けん）
専門は国際政治学、安全保障論、アジア太平洋の安全保障、日本の外交・防衛政策。防衛省、サイバーディフェンス連携協議会（ＣＤＣ）研究会委員、内閣サイバーセキュリティセンター（ＮＩＳＣ）重要インフラ専門委員会委員などを歴任。飛躍的に発展していくサイバーテクノロジーの陰に潜むリスクを、国際政治学の見地から警鐘を鳴らしている。著書に『アジア太平洋の安全保障アーキテクチャー地域安全保障の三層構造』（編著、日本評論社、二〇一一年）、『人口学に聞け！二〇五〇年の世界地図』（共著、中央公論、二〇二〇年）。

データで見る 日常化するサイバー攻撃、問われる官民の責務

セキュリティインシデントの報告件数の推移



注）国内外で発生したインシデントで、JPCERT/CC 日本窓口に報告された件数の推移。インシデントとは、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピューターのセキュリティに関わる事件、できごとの全般を示す。
出所）一般社団法人 JPCERT コーディネーションセンター「JPCERT/CC　インシデント報告対応レポート」より作成。

ランサムウェア：各国の「身代金支払い率」と支払い後の状況（2020 年）

	米国	イギリス	日本
身代金　支払い率	87%	59%	33%
支払い後の状況			
初回の支払後にデータ／システムへのアクセスが回復	78%	60%	51%
追加的な身代金の要求を受けたため、再度支払い、最終的にデータへのアクセスを回復	20%	40%	49%
身代金を支払った後もデータを回復できず	2%	0%	0%

注）「支払い後の状況」は、下記の出所データを元に NIRA で算出した。
出所）日本プルーフポイント株式会社（2021 年）「身代金を支払うのは正解か？―ランサムウェア支払い結果７か国比較から考えるサイバー犯罪エコシステムへの対処」より作成。

米国のランサムウェア二大事件

▶ **Colonial Pipeline（米国の石油パイプライン最大手）**

2021 年 5 月 7 日、ランサムウェア攻撃を確認。約 100 ギガのデータが暗号化され、操業を停止。8 日に身代金 440 万ドル相当を支払う。VPN への侵入が原因。12 日稼働再開。一部地域でガソリンが不足し、原油先物価格が一時的に高騰。DarkSide（露）による攻撃とされる。

▶ **JBS（食肉世界最大手のブラジル企業）**

5 月下旬、データが暗号化される。米国等にある食肉工場が一時停止。身代金 1,100 万ドル相当を支払い、6 月 3 日操業再開。その間、食肉価格が上昇し、畜産先物は下落した。REvil（露）からの攻撃とされ、11 月に犯人が検挙。

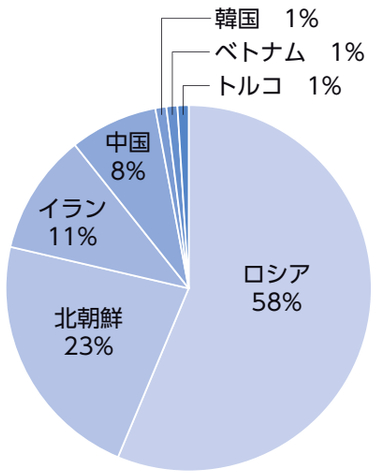
〈政府の対応〉

5 月　8 日　ホワイトハウス、FBI 他 2 機関が、ハッカー使用のサーバーを停止。
　　10 日　連邦エネルギー規制委員会委員長が、パイプライン業界に電力業界同様の基準義務付けを迫る声明発出。
6 月　2 日　米国家安全保障担当副補佐官（サイバー・先端技術担当）が企業経営者に公開書簡送付。
　　7 日　司法省が Colonial Pipeline の身代金のうち、230 万ドル相当を回収したと発表。

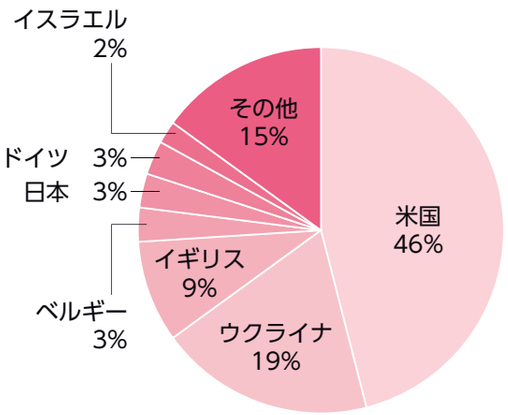
出所）報道資料等により作成。

サイバー攻撃の拠点国と標的国

サイバー攻撃の拠点国（攻撃元）



サイバー攻撃の標的国



注）2020 年 7 月から 2021 年 6 月までの集計結果。
出所）Microsoft（2021）“Digital defense Report” より作成。

日常化するサイバー攻撃、問われる官民の責務

用語集

クライアント証明書	個人や組織を認証し発行される電子証明書。クライアントがシステムやサービス、メールなどを利用する際、サーバーに対してクライアントが正規の利用者であることを証明する。
センシングデータ	感知機器（センサー）などを使用して集められたデータ。センサーを搭載した IoT 機器により、温度、湿度、光、動き、音、臭い、味などのさまざまな情報が収集される。
多要素認証	利用者本人であることを認証する際に、記憶、所有物、生体情報の 3 要素のうち、2 つ以上の認証情報を組み合わせる方法。セキュリティがより強化される。
タリン・マニュアル	サイバー空間における国際法の適用に関する手引。国際法上、サイバー戦における「武力攻撃」は定説がないため、その解釈例を示そうしたもの。2013 年、NATO のサイバー防衛協力センターが公表。
NAS（ナス）, Network Attached Storage	ネットワーク経由で利用できる外部記憶装置のこと。
秘密鍵	公開鍵暗号方式による暗号化や電子署名を利用する場合に、他人に見せることなく所有する鍵のこと。暗号化された通信を受け取った者は、秘密鍵を用いてデータを解読する。
ファームウェア	ハードウェアの基本的な制御のために、コンピュータなど機器に組み込まれたソフトウェアのこと。
プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順などの国際標準規則のこと。
ボットネット	「ボット」は、コンピュータを外部から遠隔操作するためのコンピュータウイルス。「ボットネット」は、ボットに感染したコンピュータのネットワーク。インターネット上から攻撃者が指示を出すと、ボットネットに接続されたコンピュータは、迷惑メールの配信や他のコンピュータへの攻撃、情報の窃取などを行う。
ランサムウェア	感染すると、端末等に保存されているデータを暗号化して使用できない状態にする不正プログラム。犯罪者は、そのデータを復号する対価として金銭（身代金）を要求する。

出所）警察庁、総務省、外務省、首相官邸、イミダス、NTTIT トレンド用語、GMO グローバルサイン、デジサートの資料等を元に作成。

～5 人の識者の意見～

サイバー空間でどのような脅威が起きているのか

脅威

ランサムウェア攻撃の激化
国の安全保障を揺るがす

- コロナ禍で、企業への攻撃急増
- プラットフォームを使った
  マフィアビジネス化
- IoT 機器が侵入起点に
- ガソリンや食肉の供給に影響

米国の対応

- 閣僚から企業に書簡
- セキュリティ基準→日本
  も対応せねば取引不可に
- 人と予算の盤石な体制

検討すべき課題

人材育成

- 合法的・実践的なサイバー
  攻撃の学び
- 企業の CISO の手腕

アクティブ・ディフェンス

- 攻撃能力保持が世界潮流
- 自衛権の要件
  抑止のための国際合意

官民 / 組織の大小の別なく、
国全体での対応

- IoT 機器の基本的対策
- 「善管注意義務」で責任を明確に
- 政府間で連携
- 人と予算の確保

PDF はこちらから

NIRA

わたしの構想　No.57
2021 年 12 月 10 日発行

編集：神田玲子、榊麻衣子、山路達也

本誌に関するご感想・ご意見をお寄せください。
E-mail：info@nira.or.jp

［NIRA 総研ホームページ］
https://www.nira.or.jp
諸活動を紹介するホームページをご利用ください。

［NIRA 総研公式 Facebook］
https://www.facebook.com/nira.japan
研究成果や活動状況を紹介していますので、ご利用下さい。

（公財）NIRA 総合研究開発機構
〒150-6034 東京都渋谷区恵比寿 4-20-3　恵比寿ガーデンプレイスタワー 34 階
Tel. 03-5448-1710　Fax. 03-5448-1744　E-mail. info@nira.or.jp