サイバーインテリジェンス

ジオテクノロジー（技術の地政学）とサイバーセキュリティ

デカップリングがもたらすセキュリティリスクに日本はどう対峙すべきか

pwc

www.pwc.com/jp

目次

1 米中技術覇権におけるデカップリング 4

2 デカップリングがもたらすセキュリティリスク 5

3 知的財産を狙うサイバー攻撃の増加、攻撃者の狙いとその実態 6

4 サイバー諜報活動への対峙、日本の課題はインテリジェンス 7

5 日本企業に求められるサイバーインテリジェンス強化 12

はじめに

2020年12月に開催されたユーラシア・グループ主催の「GZERO SUMMIT 2020」。このイベントの中で、PwC Japanグループ代表 木村浩一郎は、テクノロジー分野における米中のデカップリングが進む中、企業が経営課題にどう取り組んでいくべきか、米中対立の間で日本企業が直面するサイバーセキュリティリスクについて議論しました。

米中両国の市場とサプライチェーンが交わる場所にある日本は、双方からのサイバー攻撃やサイバースパイ活動の対象になり得ます。このようなリスクに直面しながらも、諜報機関を持たない日本はインテリジェンス機能に課題を抱えています。日本企業にとってサイバーインテリジェンスの強化は、喫緊の課題といえるでしょう。

このレポートでは、米中覇権争いがもたらすデカップリングやセキュリティリスクについて、詳細を解説するとともに、サイバー攻撃の裏側にある攻撃者の狙いについてひも解きます。

本レポートが、皆さまのサイバーセキュリティ対応の一助になれば幸いです。

1

米中技術覇権における デカップリング

米国国務省は2020年8月に「クリーン・パス構想」の拡大を公表した[1]。この構想は、米国の最も機密性の高い情報を保護する「クリーン・ネットワーク」の概念を5Gネットワークだけでなく、通信キャリア、モバイルアプリストア、アプリ、クラウド、海底ケーブルにまで拡大したものである。そして5Gによる通信が米国関連施設を通過する際に、主に中国企業を中心とした信頼できないベンダーからの機器・サービスが一切介されないことを、同盟・友好国に迫ることを目的としている。そしてバイデン政権は、より広範で包括的な中国対策の一環として、「クリーン・パス構想」を再評価している。

中国は「一帯一路（その一環としてのデジタル・シルクロード戦略）」および「中国標準2035」[2]などの政策を進めており、米国のハイテク技術の輸入依存から脱する「自力更生」というスローガンのもとで、想像以上に米国とのデカップリング（切り離し）が実現しつつある。「デジタル・シルクロード戦略」においては、欧州・アジア・中南米・中東などの国とも共同で進める動きを見せている。

また、冷戦時の米国とソ連の関係とは異なり、現在の米国と中国の間には経済的な依存、軍事的な依存があるため、これまでとは違う形での「安定した緊張関係」を保って共存していくことになる。米国を中心とした経済圏と中国を中心とした経済圏が表向き平和を保ちながら、水面下では見えない争いを続けることになるであろう。

2

デカップリングがもたらす セキュリティリスク

米国と中国それぞれのサプライチェーン二極化の可能性がみられる中で、日本はその両方が交錯する領域に位置している。そのため、双方のサプライチェーンから、相手を牽制するためのサイバー活動を受けることが考えられる。そのサイバー活動の種類としては、双方のサプライチェーンが併存するところにはサイバースパイ活動、どちらか一方のサプライチェーンのみ存在するところにはサイバー破壊活動が想定できる。

次に、サイバー攻撃の対象となる領域について考察をする。

中国は経済構想である「一帯一路（その一環としてのデジタル・シルクロード戦略）」、製造強国への政策「中国製造2025」、人材確保の政策「千人計画」を推し進めている。中でも自立した製造と知的財産を重要視している。製造に関しては「中国製造2025」はすでに目標をほぼ達成し、現在は「中国標準2035」の準備段階へと移行した。「中国標準2035」は、中国政府と大手ハイテク企業がグローバルな標準設定に参加するためのブループリントを確立することを目的として、策定が進められている。

中国は「軍民両用技術（デュアルユース）」を前提に、主要技術の知財情報の収集、自国生産を進めている。また、「中国標準2035」に向けて、デジタル主権を通じた世界標準を目指す取り組みを加速させることが想定される。「中国標準2035」における主な注力分野は、「新インフラ」と「新エネルギー」に位置付けられている宇宙・海洋におけるデュアルユースを想定した技術である。その中には、ブロックチェーン、IoT、新クラウドコンピューティング、ビッグデータ、5G、新世代のAI、新しいスマートシティ、地理情報などが含まれる。サイバー攻撃で狙われる可能性の高い知的財産としては、衛星関連、ソナー、センサー、リモートセンシング、ロボット技術、充電技術、新材料、そして自給率70%以上を目指している半導体関連技術が考えられている。

3

知的財産を狙うサイバー攻撃の増加、攻撃者の狙いとその実態

本節では、現在報告されているサイバー攻撃の動向を解説する。

米国司法省は2018年11月に、中国の知財窃取や投資活動などをターゲットとして対処するための対策チーム「チャイナ・イニシアチブ」を設置した[3]。その結果、1,000を超える知財窃取が暴かれた。窃取の方法はハッキングから米国企業内部のインサイダーの利用や、事業提携を通じて行われるものなど多岐におよび、これらを組み合わせて実行されていた[4]。

特に、航空宇宙分野等の軍民両用技術に関する先端技術分野においては、以前より注目されている。2018年10月に米司法省が国家安全部の江蘇省当局のメンバーを含む10名を、経済スパイの容疑で起訴している。また、2021年4月には警視庁が、航空宇宙分野のハッキングに関与したとして、元留学生を私電磁的記録不正作出・同供用の容疑で書類送検したことは記憶に新しいものだ。

これらの事案では、インサイダーの関与も見逃せない。前者の2018年10月の事案に関しては、米司法省の起訴状によれば、経済スパイ行為はハッキングだけでなく、標的組織の従業員の協力を得て行われていたことが明らかになっている。インサイダーに関する脅威の増大は、その特性から具体的数値で示すことができるものではないが、2020年に米FBIとNCSC（国家防諜安全保障センター）は海外の諜報機関によるスパイ行為に対する啓発映画を作成し、米国および同盟国に対して注意を呼びかけていることは注目に値する。

こうした状況からインサイダーが関与する事件は今後も増加する可能性があり、知財窃取はその中でももっとも危惧されるところである。さらに、2021年1月初旬には、地域社会や公民権団体などの連合体が、人種的な偏見の問題を理由に、バイデン大統領にチャイナ・イニシアチブの廃止を求めた。しかし、中国に対する強硬姿勢は超党派で支持されているため、これらの取り組みが短期的に支持を得られるかどうかは不明である。

もちろん狙われているのは米国だけではない。2020年7月21日に米国司法省が公開した資料によると、中華人民共和国国家安全部（MSS）広東省国家安全局（GSSD）と連携する中国ハッカー 2名がおよそ10年間にわたり、11カ国のハイテク製造業から知財を窃取する攻撃キャンペーンを行っており、日本企業もターゲットになっていた[5]。

また、日本を標的にしたAPTグループ（APT10、Cicada、Stone Panda、Cloud Hopper）の存在も分かっている。このグループは以前から日本をターゲットにしていることが分かっており、世界17の地域の日本企業（特に自動車産業）およびその子会社を狙い撃ちしている[6]。

これらは氷山の一角にすぎない。米国のシンクタンクである外交問題評議会は、世界のサイバー攻撃の状況を紹介するサイトCyber Operations Trackerを運営しており[7]、攻撃国と被害国を入力すると、過去の攻撃の一覧を確認できる。攻撃国を中国、被害国を日本にすると毎年さまざまな事件が起きていることが分かる。

現在進行形で知的財産窃取は行われているが、問題なのは窃取されている事実に被害企業が気づいていないケースがあることと、窃取が分かっても盗まれた内容とボリュームを知ることはできないことである。そのため被害の実態を知ることは困難である。

これらは、早急に対処しければならない課題であり、先ほどあげた中国の注力分野の技術を持っている日本企業は、これらの知的財産を対象としたセキュリティリスクが増大するという前提で、サイバー攻撃の可能性に備える必要がある。

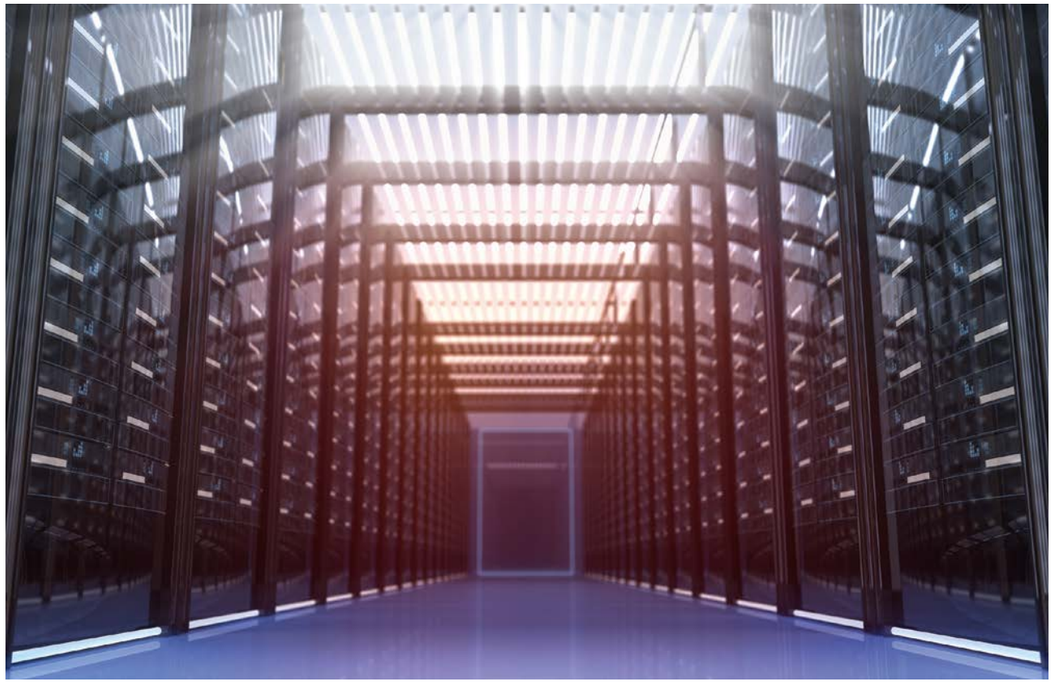
4

サイバー諜報活動への対峙、日本の課題はインテリジェンス

これまで述べてきたようなサイバー攻撃リスクの増加が見込まれる中、日本はサプライチェーン、テクノロジーの両面において中国とのデカップリングが不可能という前提で対策を考える必要がある。

ハーバード大学ベルファーセンターが2020年9月に発表した国家のサイバーセキュリティ能力に関する調査「National Cyber Power Index 2020」（NCPI2020）で、日本は初めて9位にランクインした[8]。この調査によれば、日本は防御の管理的対策は進んでいるものの、インテリジェンス（脅威情報の分析能力）が弱いという結果になっている。

サイバーセキュリティの産業分野は軍事産業に入るため、米中は高度化が進んでいるが、日本は米CIA、英SIS、独BNDなどのような専属の対外情報機関を持たないため、インテリジェンス機能に課題があると考えられる。サイバーセキュリティ能力は、実際の攻撃や防御の経験を通じて向上するため、調査対象30カ国のうち21カ国でサイバー諜報活動を行っており、15カ国では諜報能力向上のためにサイバー攻撃を行っていると推定される。



解説

「National Cyber Power Index 2020[8]」（NCPI2020）2020年9月

NCPI2020で9位にランクインした日本、しかし弱点も鮮明に

NCPI2020は、国家としての総合的なサイバーセキュリティ能力を、7つのカテゴリーと、2つの尺度で指標化したものである。（調査対象は30カ国）

2つの尺度（以下の表は、インテリジェンス機能を2つの尺度で比較したもの）

- **意思（Intent）：**計画やイニシアチブなどから数値化されるもの、インプット
- **能力（Capability）：**実際に保有している能力、アウトプット

7つのカテゴリー

- **国内監視：**国内の脅威（テロリストなど）に対処するための監視や情報収集などを行える法制度および体制の整備状況。
- **サイバー防衛：**国家、資産、システムならびに民間産業の防御と復元能力。民間企業および国民のサイバー防衛能力と意識の向上も含まれる。
- **情報操作：**国内外に対してネット世論操作を行い、自国に都合のよい情報を流布したり、相手国に混乱を起こしたりする。他国からの同種の緩衝に対する防御も含まれる。
- **インテリジェンス：**他国の外交、軍事などの機密情報の窃取および、人事情報や政府関係者の通信盗聴も含まれる。
- **商業および産業成長：**サイバー技術による産業成長。IP窃取によるものも含まれる。関連する投資や法制度の整備。
- **サイバー攻撃：**いわゆるサイバー戦能力。
- **国際規範および標準化：**サイバー空間の規範に関する国際的な議論や条約への参加。アライアンスやパートナーシップへの参加も含まれる。

出所：Julia Voo, et al., 2020. National Cyber Power Index 2020, p.65.「intelligence」の図を基にPwC作成

結果から以下のような各国の傾向を読み解くことができる。評価項目はサイバー攻撃や適法外の手段も含めた総合的なものになっており、国家資本主義あるいは超限戦やハイブリッド脅威を駆使している方が高いスコアになる傾向がある。

- **日本：**日本は全体的に中より上のパワーを持っているが、Capabilityに比べてIntentが低い項目が多くなっている。例えばCapabilityの総合指標が8位なのに対してIntentは14位、中でも国内監視はCapabilityが世界5位なのに対してIntentは21位と差が大きくなっている。これは民主主義的価値観を重視する国で起こりがちな現象である。全体の総合指標では国内監視（20位）、インテリジェンス（18位）、サイバー攻撃（16位）が目立って低くなっている。国内監視についてはIntentの向上によって改善される可能性があるが、サイバー攻撃とインテリジェンスについてはIntentとCapabilityのいずれも順位が低く、根本的な対策が必要と考えられる。
- **米国：**米国は7つのカテゴリーの指標のうち4つで世界第1位となっており、総合指標で世界1位である。国内監視では中国とロシア、商業および産業成長では中国、サイバー防衛では中国とフランスとオランダの後塵を拝している。国内監視と商業および産業成長のCapabilityは1位であるが、Intentが4位と9位のため総合順位が下がっている、民主主義的規範を守るために保有する能力を十分に活用できない可能性を示している。なお、商業および産業成長ではそのためのサイバー攻撃や国家としての戦略（国家資本主義的傾向が強いほどスコアがあがる）も評価に含まれている。また、サイバー防衛の順位が低いことは、以前から指摘されていた米国社会のネット依存度の高いことによる防衛が弱いことが確認されたことになる。
- **中国：**中国は米国に次いで総合で2位となっている。米国が1位ではない3つの指標で1位となっており、他の指標でも上位に位置している。民主主義規範を重んじていない国は国内監視や商業および産業成長のIntentが高くなっている。例えばIntentの国内監視指標では中国に加えてロシア、ベトナム、サウジアラビア、イランなど非民主主義国が上位に入っている。その一方でCapabilityが追いついていない国が多く総合的な順位は必ずしも高くない。中国はその中では高いCapabilityを持っていることから全体総合指標で2位となっている。

インテリジェンスに対する能力の評価が著しく低い日本

国家の軍事計画や戦略面における評価の意味合いもあるが、国内産業や国際市場に対してのシェアなども考慮しての評価であると推察されるため、大きく外れた結果ではないと判断できる。わが国の能力における課題はサイバー攻撃とインテリジェンスである。調査データにさかのぼってその要因を確認すると、Cyber Military Doctrine（サイバー戦略）、Cyber Military Staffing（サイバー部隊の人的リソース）が他国と比較して低いことが分かる。このレポートでは国家の持つあらゆる手段を講じているほどスコアは高くなるため、国家戦略として官民含めた総合的なサイバー戦略を策定することが施策の1つとして考えられる。

解説

THE DIPLOMAT「A Missing Piece in Japan's Cyber Defense[9]」2020年11月

中国、北朝鮮、ロシアからの脅威にさらされている日本はサイバー空間でも専守防衛だけで乗り切るのは難しいと指摘している。

その対処方法として「ゼロデイ脆弱性」を日本政府が管理することをあげている。世界でも政府がゼロデイ脆弱性情報を管理している例は少なく、その代表例は米国である。日本でも政府機関から独立した組織がゼロデイ脆弱性の公開などの管理を行っている。

ゼロデイ脆弱性情報は攻撃そのものではないものの、国内発見あるいはなんらかの方法で入手したゼロデイ脆弱性の公開あるいは秘匿する決定を日本政府が行い、情報を管理することによってサイバー防衛で取れる選択肢が増えるのである。また、いくつかの国では防衛の一環として相手国のシステムに侵入し情報を収集しているという説明が紹介されている。

現在日本がもっとも遅れているインテリジェンスを強化することによって、他国からの脅威をやわらげることは急務である。

上述のように日本のサイバーセキュリティのインテリジェンスに関する取り組みは抜本的な見直しが必要であり、こうした状況をNATO Cooperative Cyber Defence Centre of Excellence（NATO CCDCOE）が2020年12月の資料[10]で分析している。この資料は2016年のいわゆるWarsaw communiquéをベースに今後10年間に想定される脅威とその対応をまとめたもので、日本の体制などにおける課題について次の3点を指摘している。以下、NATO CCDCOEの内容を引用・要約する。

（1）CTI（Cyber Threat Intelligence:サイバースレットインテリジェンス）共有のための日本の能力とやる気（the capacity and willingness to share threat intelligence）

日本は米国や他の国とサイバーセキュリティに関する協定を結んでいるが、以下のような理由から実際には日々の技術的な協力関係を築けていない。

- **迅速で自動的な情報共有：**米国のUS-CERT Automated Indicator Sharing (AIS)で標準となっているStructured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)を一部の組織しか利用していない。
- **CTIを含む機密情報の全体像の把握：**CTIの共有そのものは解決にはならず、国家の戦略などの文脈にそって人間が解釈しなければならない。
- 異なる情報源からCTI情報を統合するための必要なスキルや洞察力。
- セキュリティクリアランス（特別管理秘密を扱う行政機関の職員を対象とする適格性審査）と管理プログラム。

（2）日本側の担当と責任の所在の曖昧さ（fuzzy boundaries of responsibility and accountability）

政府が脅威に対抗する方法は2つある。1つは権限を委任して階層的に対処する方法、もう1つはリスク低減のために仲介組織を通じて調整を行う方法である。日本は仲介モデル、英国は権限委任モデル、米国はハイブリッド型を取っている。重要インフラとサプライチェーンの脆弱性を使用した脅威アクターの活動にはCTIの共有と関係者全てが責任を持って対応する必要がある。

日本では民間セクターとの協力関係が不十分である。例えば日本では被害にあった企業が政府の専門家を招き入れることに抵抗があるため、民間セクターのCTIの共有における透明性や信頼に限界がある。

日本の民間セクターはほぼ半数しかCTIの共有と活用ができておらず、米国の80%、欧州の65%に比べると遅れている。インセンティブをつけて民間部門に参加させるよう仕向ける必要がある。

（3）米国の意図や戦略文化の不完全あるいは不正確な理解（incomplete or inaccurate understanding of partners' expectations and strategic culture）

CTIの共有で各国が同じような体制、法律で対応することはなく、またその必要性もない。必要となるのは方法論と基準が最小限一致していることであり、これによって当面の危機に対処することができる。

方法論と基準は戦略的文化によって形作られ、戦略文化は過去の経験から醸成される。米国、英国、日本、そして中国はそれぞれ異なる戦略文化を持っており、日本は平和憲法に縛られ、攻撃的な行動が制限されている。

NATO加盟国の間で標準化されたIndications and Warning (I&W)を確立するためには、戦略文化が一致する部分を把握し、CTIの共有のための共通言語を確立することが必要となる。日本は他の国（特に米国）の戦略文化と共通言語を理解しなければならない。

以上、NATO CCDCOEで指摘された、日本のサイバーセキュリティに関する課題について紹介した。特に（3）の内容は前述の「National Cyber Power Index 2020」と重なる部分もあり、日本のサイバーセキュリティに関するインテリジェンスについて大きな見直しを迫られていると言える。

5

日本企業に求められるサイバーインテリジェンス強化

最後に、企業として取りうる2つの対策を考察する。

まず、国家が支援するサイバー活動に対して、一企業が太刀打ちできるものではないという認識を持ち、官民での連携が必要不可欠であると認識する必要がある。そこで考えられるのが米国のサプライチェーンへ参画することで期待できる、米国当局からのサイバーセキュリティに関するインテリジェンスサービスを積極的に活用することである。具体的には、米国当局や米国の有力企業からの上級幹部を外部アドバイザーとして活用することで、米国当局を中心としたインテリジェンスコミュニティへのアクセスが容易になる。

もう1つの対策として、企業としての脅威情報の収集・分析・報告の実務能力の向上が挙げられる。上述のようにサイバーセキュリティに関するインテリジェンスサービスの活用を通して自組織におけるサイバーインテリジェンスの概念を浸透させ、実効性のある運用を検討・構築していく必要がある。現在、多くの日本企業では、標準やガイドラインに基づいたセキュリティコントロールを適切に実装・運用してリスクを低減する、日々発見される脆弱性・インシデントを予防・検知・対処するといった取り組みがセキュリティ対策の主軸となっている。一方でサイバーインテリジェンスの本質は、「自組織に発生し得る脅威を予測し、脅威が発生した際に対応できるように備える」ことである。これは、網羅的なリスクアセスメントによる自組織の弱みの洗い出し、単一のセキュリティ情報の分析だけでは実現することができない。自組織の弱みに加えて、日々発生するサイバー攻撃の背景・目的、サイバー攻撃者の能力を踏まえた分析を行い、意思決定に利用可能なインテリジェンスを導出する必要がある。そのため、提供された情報（インフォメーション）をただ利用するという姿勢から、自組織での活用に根差した目的を設定し、分析、意思決定を行うというプロセスに改めていくことが求められる。

これら2つの対策により、サイバーインテリジェンスが強化でき、企業に求められるサイバー攻撃への能動的な対応力を醸成することが可能となるであろう。

参考資料

1 US Department of State, “Announcing the Expansion of the Clean Network to Safeguard America’s Assets”, 5 August. 2020, https://mr.usembassy.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/
2 中华人民共和国人民政府「中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议」2020年11月3日 http://www.gov.cn/zhengce/2020-11/03/content_5556991.htm
3 David H. Laufman, Joseph M. Casino, Michael J. Kasdan,. “The Department of Justice’s National Security Division Chief Addresses China’s Campaign to Steal U.S. Intellectual Property”, The National Law Review, August 24, 2020. https://www.natlawreview.com/article/department-justice-s-national-security-division-chief-addresses-china-s-campaign-to
4 The United States Department of Justice, “The China Initiative: Year-in-Review (2019-20)”, November 16, 2020. https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20
5 The United States Department of Justice, “Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research”, July 21, 2020. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
6 Symantec, “Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign”, November 17, 2020. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
7 Council on Foreign Relations, “Cyber Operations Tracker” https://www.cfr.org/cyber-operations
8 Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, Anina Schwarzenbach, “National Cyber Power Index 2020”, 2020. https://www.belfercenter.org/publication/national-cyber-power-index-2020
9 Eugenio Benincasa, “A Missing Piece in Japan’s Cyber Defense”, The Diplomat, November 20, 2020. https://thediplomat.com/2020/11/a-missing-piece-in-japans-cyber-defense/
10 Abraham, Chon., Daultrey, Sally. “Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK”, Cyber Threats and NATO 2030: Horizon Scanning and Analysis, NATO Cooperative Cyber Defence Centre of Excellence, pp.194-214. December 2020. https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

名和 利男
PwC Japanグループ
サイバーセキュリティ最高技術顧問

岩井 博樹
PwC Japanグループ
スレットインテリジェンスアドバイザー

林 和洋
PwCコンサルティング合同会社
パートナー

村上 純一
PwCコンサルティング合同会社
ディレクター

www.pwc.com/jp

発刊年月：2021年5月　　管理番号：I202103-03