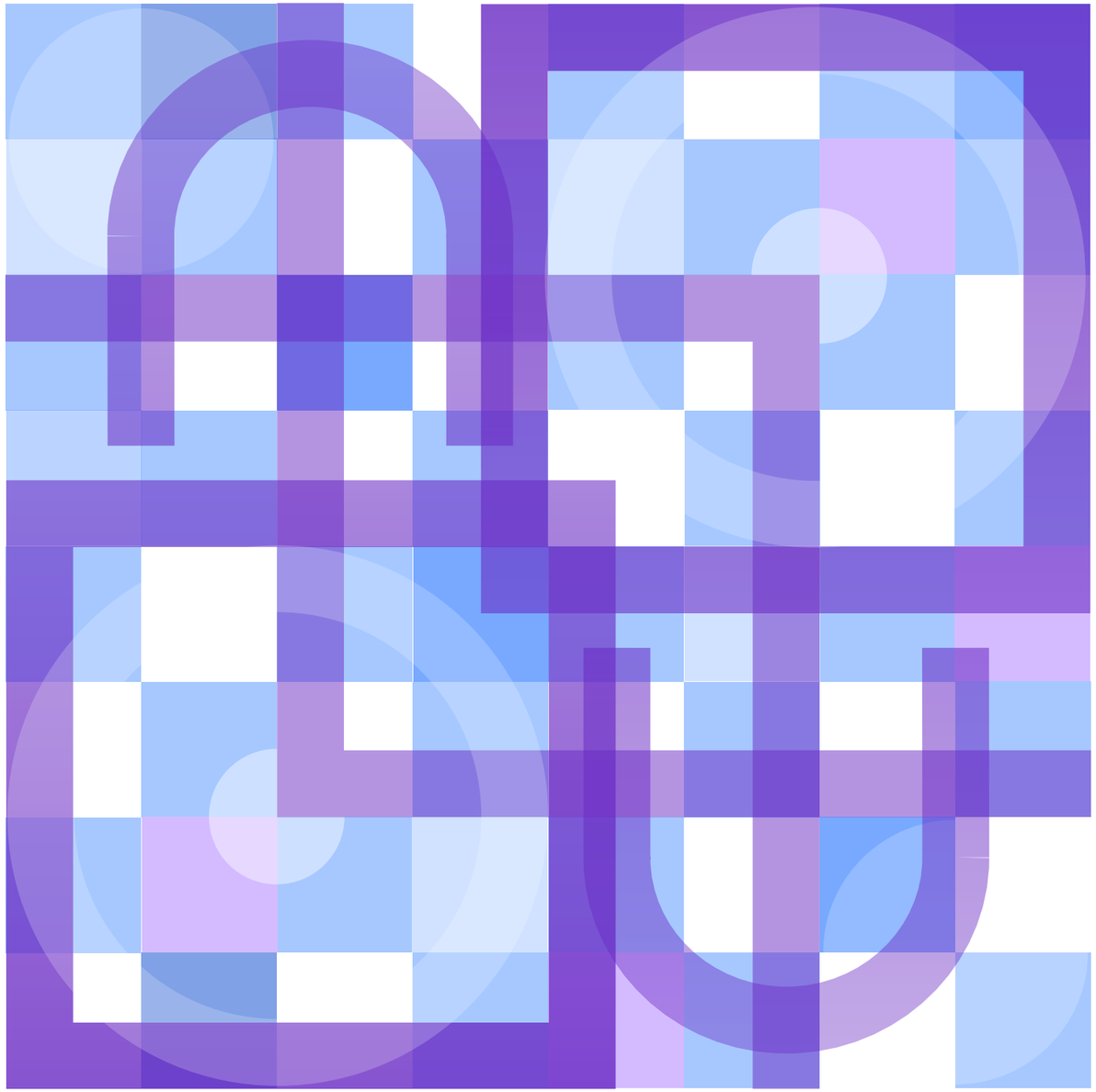
「未来の衝撃」に対する政府の備え

不確実な世界において、サイバー・レジリエンスを確かなものにするためのアクション



共同研究団体

National Academy of Public Administration

IBM Center for The Business of Government

Centro Studi Americani

はじめに

「IBM は、政府のリーダーたちが重要な資産やシステムを認識し、保護することで、不測の事態が発生した場合のレジリエンスを高められるよう支援しています。サイバー攻撃のシナリオをシミュレートし、最悪な事態が実際どのようなものになるかをリーダーたちに示します。」

IBM、グローバル公共セクター担当バイス・プレジデント、**Cristina Caballe Fuguet**

インターネットが登場して以来、犯罪集団、ハクティビスト *、あるいは国家主導などサイバースペースの脅威は、政府機関をサイバー犯罪の標的としてきました。2022 年後半、政府機関を狙ったサイバー攻撃の件数は、2021 年の同時期に比べて世界で 95% も増加しています。[1] 政府公共機関のデータ漏洩の損害額も 2021 年 3 月から翌年 3 月までに 7.25% 増え、1 件当たりの平均損害額は 207 万ドルに上っています。[2]

政府機関が持つデジタル・プラットフォームと機密情報は、攻撃者にとって格好の標的です。経済のグローバル化や、官民のほぼすべての活動が相互にデジタル接続されたことにより、複雑なデジタル・エコシステムが形成されており、サイバースペースの出現によって、新たな国境が生まれ、統治の方法も従来どおりとはいかなくなっています。ネットワークがグローバルに拡大するということは、脅威やインシデントが発生した場合、その影響は、急激に大規模化し広範囲に広がる恐れがあることを示唆しており、迅速かつ効果的な対処が求められます。

米国政府は今日の複雑なサイバー脅威の環境を踏まえ、政府の責務として、安全でセキュアなデジタル・エコシステムを確保するため、2023 年 3 月、包括的な「National Cybersecurity Strategy（国家サイバーセキュリティー戦略）」を発表しています。当戦略は、サイバー攻撃に対する防衛をより簡便で、費用対効果の高いものとするための道筋を示すものです。また、レジリエンスを高め、サイバー・インシデントの影響を軽減し、国の普遍的な価値観に沿った取り組みを行い、デジタル社会の未来を守ることに重点を置いています。

昨年、IBM Institute for Business Value（IBV）と IBM Center for The Business of Government は、2 つのラウンドテーブル会議を、National Academy of Public Administration（全米行政アカデミー）と Center for American Studies（アメリカ研究センター）と共同で開催しています。ワシントン D.C. とイタリアのローマで催された会議では、サイバー・レジリエンスと政府のリーダーシップについて踏み込んだ議論が行われ、そこから得られた知見は、米国やイタリアをはじめとする各国の政府が今後、官民連携でレジリエンスを強化するサイバーセキュリティー戦略を開発・実行する際に役立つものとなるでしょう。

会議で行われた広範な議論は、現在および将来、起こりうるサイバー攻撃に対し、政府を強靭化する実践的なステップとしてまとめられています。

* ハクティビストとは、社会的・政治的な主張を目的としたサイバー攻撃を行うネット犯罪者や集団のこと

著者

Tony Scott
Intrusion 社 社長兼 CEO

セキュリティー・ソフトウェア・ソリューションのプロバイダーである Intrusion 社の CEO に就任する以前は TonyScottGroup を設立し、ワシントン D.C. とシリコンバレーを拠点にサイバーセキュリティーと個人情報保護技術に特化したコンサルティングとベンチャー投資を手がけていた。また複数の企業や政府機関において、経営やマネージメントに携わっている。

オバマ政権時代には、連邦政府の最高情報責任者を務め、政府が IT 関連に投じた年間 850 億ドル以上の予算を監督、確保、管理する立場にあった。

また、Microsoft（マイクロソフト社）の CIO、Walt Disney Company 社（ウォルト・ディズニー・カンパニー）の CIO、および General Motors 社（ゼネラル・モーターズ社）の CTO を歴任している。CIO Magazine の「CIO Hall of Fame（CIO の殿堂）」に選ばれたこともあり、Fed 100 Award（Fed100 賞）を複数回受賞している。業界や政府が催した数多くのイベントにおいて、基調講演を行い、パネリストやアドバイザーを務めてきた。

協賛団体の代表者

Dan Chenok
IBM Center for The Business of Government
エグゼクティブ・ディレクター
chenokd@us.ibm.com
linkedin.com/in/chenokdan/

Dave Zaharchuk
IBM Institute for Business Value
リサーチ・ディレクター
David.zaharchuk@us.ibm.com
linkedin.com/in/david-zaharchuk-59564519/

Terry Gerton
全米行政アカデミー
会長兼 CEO
tgerton@napawash.org
linkedin.com/in/terry-gerton-b43aa73a/

日本語翻訳監修

山中邦裕
日本アイ・ビー・エム株式会社
IBM コンサルティング事業本部
パートナー・官公庁サービス部長

20 年以上にわたり、政府・官公庁、自治体、公益事業者向けのコンサルティングに従事。2011 年に日本アイ・ビー・エム参画以降は、スマートシティー、政府部門の DX、AI ／データ活用など多数のプロジェクトをリード。

ステップ 1

サイバーセキュリティー人材の供給基盤を拡充する

サイバーセキュリティーの分野では、スペシャリストに対する需要と供給のギャップが急速に広がりつつあります。ラウンドテーブル会議の参加者は、実行可能な優先事項のトップにサイバーセキュリティー人材の供給基盤の拡充を挙げています。

主なポイント

- 政府機関がサイバーセキュリティーの人材を確保するには、多角的な取り組みや、幅広い層から人材を採用するといった新しい発想が必要

サイバーセキュリティーの分野では、スペシャリストに対する需要と供給のギャップが急速に広がりつつあります。ラウンドテーブル会議の参加者は、実行可能な優先事項のトップにサイバーセキュリティー人材の供給基盤の拡充を挙げています。サイバーセキュリティーの人材不足は、分析・エンジニアリング、ソフトウェア開発、脅威インテリジェンス *、侵入テスト **、監査・コンサルティング、デジタル・フォレンジック ***、暗号技術などの幅広い分野に影響を及ぼすと、複数の参加者が指摘しています。

ある参加者は、米国における STEM（科学、テクノロジー、工学、数学）教育の制度的問題について、次のように言及しています。「我々は、元々小さな人材プールから、ごく限られた人材を得てきたに過ぎない。米国で STEM 教育を受けた人材から、セキュリティー・クリアランス **** を取得できる能力を持った人物を見つけるということはまさに難題で、まるで伝説の生き物を探すようなもの」

また別の参加者は、世界で不足するサイバーセキュリティー関連の人材は約 350 万人に上ると指摘し、加えて、人材獲得競争が人件費を押し上げ、多くの組織が人員を確保することが難しくなっていると述べています。[3] 多くの民間企業がサイバーセキュリティー職に対して高額な報酬を提示するようになったため、政府がアナリスト、インシデント・レスポンダー、セキュリティー・アーキテクト、研究者、マネージャーなどを採用しようとしても、民間企業の求人と競合してしまい、諦めざるを得なくなってきています。

デジタル化の巨大な波がビジネスの風景を一変させつつある一方で、デジタル技術はサービスの形や提供方法に変革をもたらしつつあります。その結果、サイバー攻撃はより日常的で、広範囲に及ぶものになり、政府に期待されるサイバーセキュリティーには、より一層強いプレッシャーがかかるようになりました。

政府機関にサイバーセキュリティー人材を供給することに関して、参加者たちは以下のようなアイデアを提示しました。

- 一部の専門技能においては、4 年制大学の学位要件を免除する
- 高校以下の教育課程に、サイバー教育を早期に組み入れる
- 現職の人材に対し、再教育を重点的に行う
- サイバー + ビジネス、サイバー + 医療など、学際的なプログラムを開発する
- サイバーセキュリティーの現場での実習プログラムを拡大する
- 現在、サイバーセキュリティー分野の従事者のうち、女性は 24% に過ぎない。[4] この分野を女性にとって魅力的なものにすることで、STEM 教育プログラム、特にサイバー教育への女性の参加者を増やす
- その意思決定が労働力の向上に直接につながる州、地域レベルや、産業界において、職業教育を強化する
- サイバー・スキルを持つ退役軍人の力を活かすため、退役軍人向けサイバーセキュリティー技術の訓練プログラムを増やす
- セキュリティー・クリアランス（適格性審査）や必須基本技術の取得など、現在サイバー職へのハードルを上げている要因について、再検討する
- 多様性、公平性、包摂性、アクセス性を推進し、サイバーセキュリティーの人材プールを強化する
- 職場を包摂的に作り替えることで、従来はセキュリティーの仕事に適さないと思われていた人材を引き付ける

こうした案に加え、National Academy of Public Administration（全米行政アカデミー）は、政府がサイバーセキュリティー向けの人材を育成するのに役立つと思われる報告書を公開しています。
https://napawash.org/academy-studies/dhs-cybersecurity-workforce

* 脅威インテリジェンス（スレット・インテリジェンス）とは、セキュリティーに対する脅威について収集・分析した情報や、それらから得られる知見などを表す用語

** 侵入テスト（ペネトレーション・テスト）とは、ネットワーク、PC・サーバー、システムが、サイバー攻撃にどれほど耐性があるのかを検証するテスト手法

*** デジタル・フォレンジックとは、法科学（フォレンジック・サイエンス）の一分野で、データの改ざんや不正アクセスなど、主にコンピューター犯罪に関して、デジタル・デバイスに記憶された情報の回収と分析を行う科学的調査手法・技術

**** セキュリティー・クリアランスとは、重要な情報を扱う行政機関の職員や研究者などの信頼性を事前に確認するための秘密取扱者適格性確認制度

ステップ 2

スピーディーな対応で、組織間のコラボレーションを改善する

各国や国際機関の間、あるいは官民におけるコラボレーションや情報共有は複雑であり、動きが鈍いという認識で参加者の意見は一致しています。

主なポイント

- 脅威をもたらす攻撃者は新技術に適応することで、ネットワークに侵入し、防御策を突破しようとする。これに対し政府機関はコラボレーションを強化し、情報共有を進めることで、敵の一歩先を行くことが必要

昨今、官民による連携は進んでいるものの、[5] サイバー攻撃者の間の連携も進んでおり、依然として脅威は続いています。脅威をもたらす攻撃者たちは、犯罪に利用するインフラやサービスを開発・拡大しており、敵対する国家や犯罪組織はそれらを不正な目的で使用しています。

脅威をもたらす攻撃者は、新技術を貪欲に取り入れ、攻撃を防ぐ手段を無力化し、ネットワークに侵入します。一方で、それに対抗する側は、標準やミッション、優先順位が異なる組織間のコラボレーションに頼らなければならないため、脅威への対処が難しくなっています。2023 年 3 月に米国政府が発表した「国家サイバーセキュリティー戦略」の主要テーマは、協調とコラボレーションでした。この報告書が強調しているのは、市民社会と産業界のパートナーシップ、協力国とのコラボレーションの深化、責任ある国家の行動規範の強化、無責任な行動に対する国家の責任、そしてサイバー攻撃の背後にある犯罪ネットワークの破壊といったアクションの重要性です。

このような、デジタルでつながれたサービスの多様な相互依存関係、複雑さ、関連するリスクにおける課題として参加者が指摘するのは、サイバー空間における脅威の影響に対する認識共有の不足です。影響認識が十分に共有されていないために、一般の人々にとって、システムの脆弱性やサービスが中断した場合の損害、下流のサプライヤーやパートナーに及ぼす影響などを理解することが困難となっています。

例えば、オープンソース・ソフトウェア、サプライチェーン、重要インフラストラクチャーが、オペレーション、フルフィルメント *、プラットフォーム・セキュリティーなどの技術サービスを外部からの提供に依存する度合いが増していることが、相互依存の例として挙げられます。新興エコシステムがその経済活動において協調を前提とするのであれば、サイバーセキュリティーとレジリエンスについて共有された責務を、もっと自覚すべきであると参加者は指摘しています。

参加者からは、以下のようなコラボレーション改善策が提示されています。

- セキュリティー・ポリシーに基づく幅広いサイバーセキュリティー・イニシアチブに注力することで、重要インフラのベースライン ** を確立し、規制の枠組みの空隙を埋める
- 規制やルール違反の取り締まりを強化する
- サイバーリスク評価の標準フレームワークを最優先で導入することで、より効率的にコラボレーションを進める
- フィードバック・ループを加速させ、検出能力を向上させることで、サイバーリスクの過大評価あるいは過小評価を補正する
- エコシステムにおいて、サイバー・インシデント対応の研修を実施し、パートナー間のオペレーション・サポートを連携させる。また、官民合同の実戦演習を行い、公共部門と民間部門が連携してレジリエンスを強化する
- デジタル運用やサービス提供に関わる組織の間で、サイバー関連の専門知識と費用を共有する。また、そうして生まれた政府または民間のサイバーセキュリティーにおける共同の専門機関を活用して、自前でセキュリティーを確保する能力がない組織を支援する
- US Department of Homeland Security Cyber Safety Review Board（米国国土安全保障省サイバー安全審査委員会）[6] の指針に従い、共有された（オープンソースの）サイバー・サービス、特に安全なクラウド・サービスをより広範囲に活用する
- AI や量子コンピューティング技術の進展がもたらす脅威に備えて、積極的な投資を行う
- AI と自動化技術を活用して、広範にサイバー防衛力を強化し、これらの技術を悪用する敵対者や脅威をもたらす攻撃者に対抗する

* フルフィルメントとは、主に EC 取引において、注文から決済、在庫管理、物流、アフター・フォローに至る一連のプロセスのこと

** ベースラインとは、情報システムの重要性に応じて規定されたセキュリティー・コントロールの最低基準のこと

ステップ 3

サイバーセキュリティーにおける優先課題を、官民の間で共有する

参加者は共通の課題を明確にし、ベストプラクティスを共有することで、協力の道筋を探りました。これにより、官民が連携してサイバーセキュリティーを広範に強化する方法が浮かび上がっています。

連携に当たって優先すべき事項は以下に挙げる通りです。

- サイバー分野の人材を幅広い経歴の持ち主から採用することに力点を置く
- 競争優位となるセキュリティー分野のイノベーションにさらに注力する
- 「ネットワーク・セキュリティーは常に内外からの脅威にさらされている」ことを前提とするゼロトラスト・フレームワークを支援する
- 未就学児から高齢者まで幅広い年齢層を対象に継続的なサイバー教育を制度化する
- 政治家やそのスタッフ、官僚などの間で、サイバーセキュリティーに対する認識を高める
- サイバーセキュリティーに求められる期待、標準、指標、データの向上を図ることで、脅威についての理解を深めるとともに、脅威に対抗し、封じ込めるためには、官民の投資が必要であることを周知する

主なポイント

- 政府と企業は、サイバーセキュリティーの主要な優先課題への取り組みと、互いの利益となるベストプラクティスの徹底を確実に行うべき

ステップ 4

サイバー攻撃から、いかに民主主義国の政府機関を守るべきかを検討する

情報操作や偽情報キャンペーンによって、
民主主義の根幹がサイバー戦争の標的になっていることに、
ラウンドテーブル会議の参加者は懸念を示しています。

こうした攻撃は、選挙や、法律の制定、規制づくりに対する国民の支持や関与に影響を与えるよう仕込まれており、世論の誘導や民主主義の規範を脅かす意図が隠されています。

これらのあからさまな、あるいは隠された攻撃の主な目的は、短期的には社会混乱を招くことであり、長期的には世論を動かすことであると参加者は認識しています。民主的な代議制を採る国に対するサイバー攻撃がもたらす課題は複雑であり、深まる脅威に対し、どう対応すれば効果的であるか、広範な合意は得られておらず、参加者はさらに対策の必要性を感じています。

参加者は以下に示すような懸念事項を挙げています。

- 国家を後ろ盾とする勢力が、インターネットなどから入手できる公開情報を広範に抑圧して世論を操作しようと企図していること。例えばラウンドテーブル会議の参加者が挙げたのは、検索エンジンに対する規制や厳しい検閲政策を行う中国やロシアなどの権威主義国家の事例である。
- TikTok などの人気のモバイル SNS アプリが、消費者行動に関する情報を収集していること。
- 開かれた民主主義国においては、権威主義国のような検閲や情報統制が行えないため、高度に自動化された偽情報の攻撃が効果的に展開された場合、それらを見つけ出し、対策を講じることは極めて難しく、権威主義国のような防御ができない。ラウンドテーブル会議の参加者は、サイバーセキュリティー上のリスク、脅威、レジリエンスの観点から、このトピックへの理解を深めるためには、さらに踏み込んだ研究が必要であると意見を一致させた。

主なポイント

- 情報操作や偽情報キャンペーンは世論を揺さぶり、民主主義を弱体化させる力を秘めており、こうした脅威に対抗する手段について、より一層の研究が必要

結論

将来に備え、サイバー・レジリエンスのリーダーを育成する

かつて情報革命をけん引した技術イノベーションの波が、社会や公共の福祉に影響を与えたように、現在進行中のデジタル化の巨大な波は、広範な分野に影響を及ぼしつつあります。

世界中でテクノロジーのオープンな開発・利用が求められていることから分かるように、社会的つながりやコミュニケーション、コラボレーションは、社会が発展する上で欠かせない要素です。これらは、国家や国際社会のウェルビーイングを高める原動力となっていますが、それと同時にデジタルによるやり取りへの依存は、サイバー犯罪者に付け入る隙を与える結果を生んでいます。

現在の防御対策は、ある程度は機能しているものの、多くのケースで不十分であると言わざるを得ません。政府のリーダーは、リスクを見越した積極的な対策を講じる必要があります。テクノロジーは情報の利用形態や、社会的な意見交換の場としてのプラットフォームの形態を進化させましたが、一方でサイバー攻撃の質も進化させ、世界中で公的部門、民間部門を問わず関係者に大きな影響を与えています。

政府機関は主要な利害関係者と協力して、サイバー上のリスクを特定するという極めて重要な役割を担っています。その第一歩は、リスクに直面したときの対応力とレジリエンスを強化することです。しかし、政府関係者はさらに前進し、リーダーシップを発揮し、よりレジリエンスの高い未来の変革をけん引しなくてはなりません。また同時に防御策は、それぞれの国の有権者の特性や意見を反映させていく必要があり、それを踏まえた目的意識を有した策でなくてはなりません。

ローマで開催されたアメリカ研究センターのラウンドテーブル

ワシントン D.C. で催されたイベントに国際的な視点を加えるため、イタリアのローマにある Center for American Studies（アメリカ研究センター）は、サイバーセキュリティーに関するラウンドテーブル会議を開催しました。そこには欧州各地の専門家が参加し、ワシントンで発表された数々のアクション項目について議論が交わされ、多くの知見がもたらされました。

ローマがウクライナの戦場に近いこともあり、サイバーセキュリティーに関する議論の大半は、防衛と相互安全保障の支援に費やされました。参加者の多くが、サイバーセキュリティーは欧州におけるエコシステムの重要な課題であることを強調しました。サイバーセキュリティーで成果を上げるには、各国の政府や機関が高いレベルで協力し合い、可能な限り障壁を取り除く必要があります。

参加者は、サイバーセキュリティーの強化が技術的主権を支え、基幹インフラ、サプライチェーン、医療データ、宇宙・衛星の防衛、その他のシステムを防護することを確認しています。こうした事項の重要性については、イタリアの National Cybersecurity Agency（国家サイバーセキュリティー庁）が同国の安全を確保し、レジリエンスを高める目的で作成した『国家サイバーセキュリティー戦略』報告書にも記載されています。

ラウンドテーブル（ローマ）の参加者

Luciano Antoci
CIS Division Chief
Italian Army General Staff
（イタリア軍参謀本部CIS部長、少将）

Lorenzo Benigni
Senior Vice President, Governmental and Institutional Relations
Elettronica SpA
（Elettronica社、政府・公共機関関係担当シニア・バイス・プレジデント）

Stefano Bonifazi
Direttore BU Difesa, Spazio e Sicurezza dello Stato
BV-Tech
（BV-Tech社、国防・宇宙・国家安全保障部門、ディレクター）

Cristina Caballe Fuguet
Vice President, Global Public Sector, IBM
（IBM、グローバル公共セクター担当バイス・プレジデント）

Cristiano Cannarsa
Chief Executive Officer, CONSIP
（CONSIP社、CEO）

Marco Carlini
Partner, Public Sector, IBM Italy
（IBMイタリア、公共セクター担当パートナー）

Dan Chenok
Executive Director
IBM Center for The Business of Government
（IBM Center for The Business of Government、エグゼクティブ・ディレクター）

Riccardo Croce
Vice Questore Aggiunto, Responsabile del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
Polizia Postale e delle Comunicazioni
（イタリア・郵政通信警察庁、重要インフラ保護のための国家コンピュータ犯罪センター長、副次官補）

Gennaro Faella
SVP Strategic Innovation & Development
Leonardo Cyber & Security Solutions
（Leonardo Cyber & Security Solutions社、戦略的イノベーション & 開発担当SVP）

Luca Frusone
Presidente della Delegazione parlamentare italiana presso l'Assemblea parlamentare della NATO
（NATO議員連盟イタリア議会、代表部議長）

Ivano Gabrielli
Direttore Servizio Polizia Postale
Polizia di Stato
（イタリア・国家警察、郵政通信警察庁、長官）

Sara Marini
Manager of Government and Regulatory Affairs, IBM Italy
（IBMイタリア、政府・規制関連業務担当マネージャー）

Roberto Menotti
Editor-in-Chief of Aspenia online, Deputy Editor of Aspenia print edition and Senior Advisor - International Activities
Aspen Institute Italia
（NPO法人Aspen Institute Italia、Aspeniaオンライン編集長、Aspenia印刷版副編集長、国際活動担当シニア・アドバイザー）

Julian Meyrick
Senior Partner and Vice President, Security Strategy Risk & Compliance, IBM
（IBM、シニアパートナー兼セキュリティー戦略リスク & コンプライアンス担当バイス・プレジデント）

Karim Mezran
Resident Senior Fellow, Rafik Hariri Center for the Middle East
Atlantic Council
（大西洋評議会、Rafik Hariri Center for Middle East（ラフィク・ハリリ中東研究センター）レジデント・シニア・フェロー）

Alessandro Picardi
Presidente Esecutivo, Olivetti
（オリベッティ社、取締役会長）

Enrico Prati
Professor, Università degli Studi di Milano
（ミラノ大学、教授）

Alessandra Santacroce,
Director, Government and Regulatory Affairs, IBM Italy
（IBMイタリア、政府・規制関連業務担当ディレクター）

Lieutenant General Sergio Antonio Scalese
Commander, Cyberspace Operations Command
Italian Air Force
（イタリア空軍、サイバースペース・オペレーションズ・コマンド司令官）

Daniela Scaramuccia
Lead Client Partner, Public Sector, IBM Italy
（IBMイタリア、公共セクター担当リード・クライアント・パートナー）

Paolo Sironi
Global Research Leader, Banking and Finance
IBM Institute for Business Value
（IBM Institute for Business Value、銀行・金融担当グローバル・リサーチ・リーダー）

Mike Stone
Managing Partner, Global Government, IBM
（IBM、グローバル政府担当マネージングパートナー）

Francesco Stronati
Managing Director, Health & Public, IBM Italy
（IBMイタリア、医療・公共担当マネージング・ディレクター）

Francesco Teodonno
Security Brand Leader, IBM Italy
（IBMイタリア、セキュリティー・ブランド・リーダー）

Shue-Jane Thompson
Managing Partner, Global Deal Leader, Strategic Sales, IBM
（IBM、マネージングパートナー、ストラテジック・セールス担当グローバル・ディール・リーダー）

おわりに

世界を席巻するパンデミック、欧州の大規模な戦争、パキスタンやカリフォルニアそしてオーストラリアで発生した歴史的な大洪水、中国の猛烈な熱波、このように「未来の衝撃」は未来の現象ではなく、現在進行形で起きている現実です。

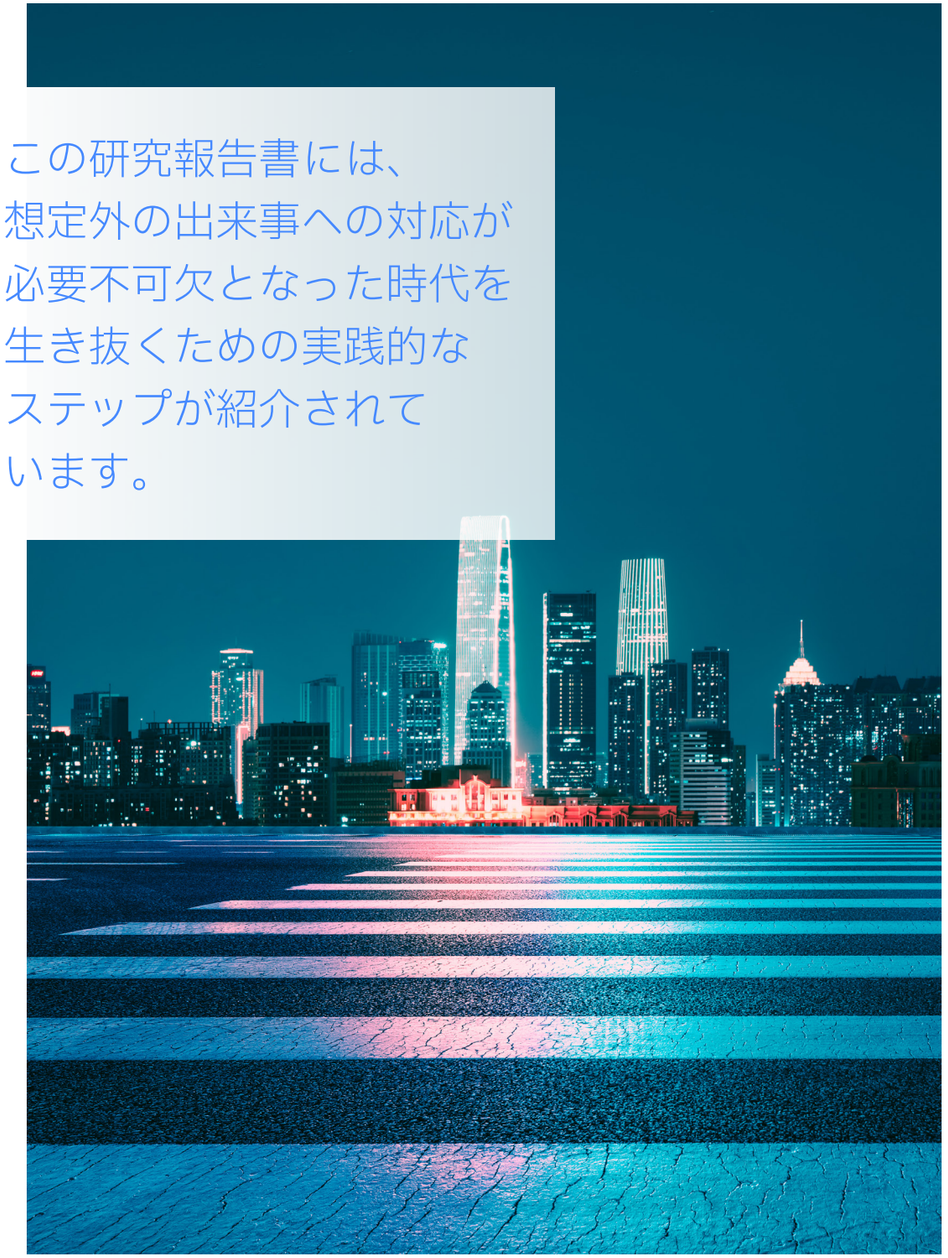
IBM は、政府機関のリーダーが「未来の衝撃」に直面した際、レジリエンスに不可欠なコア能力を把握できるよう、IBM Center for The Business of Government および IBM Institute for Business Value を通じ、National Academy for Public Administration（全米行政アカデミー）と連携し、このイニシアチブを開始しました。

当イニシアチブでは、政府機関のリーダーが「未来の衝撃」に備えて準備すべき 6 つの主要な領域を提示しています。またこの会合外にも、IBM は行動計画を議論し、策定するため、政府、企業、学会、その他のセクターからグローバル･リーダーを招き、国際的なラウンドテーブルの開催を続けています。

このラウンドテーブルのシリーズの初回は、緊急事態への備えと対応策をテーマに、2022 年にワシントン D.C. で開催しています。その内容を研究報告書『Partnering for Resilience: A practical approach to emergency preparedness（レジリエンスのためのパートナーシップ：緊急事態への備えとなる実践的アプローチ）』として公表し、想定外の出来事への対応が必要不可欠となった時代を生き抜くための実際的・実践的なステップを紹介しています。

2022 年の第 2 シリーズとなったワシントン D.C. とローマのラウンドテーブル会議では、同報告書が取り上げたサイバーセキュリティーを主要テーマにしました。2023 年には、さらに 4 回のラウンドテーブル会議が開催され、サプライチェーン、サステナビリティー、労働者のスキル、国際協調がテーマとなる予定です。

それぞれのテーマについてラウンドテーブル会議が提示する知見は、政府機関が今後起こりうる課題を予測し対処するための戦略やソリューションを策定する際に、必ずや役立つはずです。今後、IBM は過去の経験から得た知見をまとめていく予定です（例えば、IBM Center for The Business of Government が 2021 年に発表した、パンデミックから学んだ教訓についての報告書『Covid-19 and its Impact: Seven Essays on Reframing Government Management and Operations（新型コロナウイルスとその影響：政府の管理運営をリフレーミングする 7 つの論考）』など）。さらには、こうした知見を批判的な目で見つめ、短期的には実践に活かし、長期的には準備を進めるために、実践的で具体的な提案を行っていきます。



変化する世界に対応するためのパートナー

IBM はお客様と協力して、業界知識と洞察力、高度な研究成果とテクノロジーの専門知識を組み合わせることにより、急速に変化し続ける今日の環境における卓越した優位性の確立を可能にします。

IBM Institute for Business Value

IBM Institute for Business Value（IBV）は、20 年以上にわたって IBM のソート・リーダーシップ・シンクタンクとしての役割を担い、ビジネス・リーダーの意思決定を支援するため、研究と技術に裏付けられた戦略的洞察を提供しています。

IBV は、ビジネスやテクノロジー、社会が交差する特異な立ち位置にあり、毎年、何千もの経営層、消費者、専門家を対象に調査、インタビューおよび意見交換を行い、そこから信頼性の高い、刺激的で実行可能な知見をまとめています。

IBV が発行するニュースレターは、ibm.com/ibv よりお申し込みいただけます。また、Twitter（@IBMIBV）や、LinkedIn（linkedin.com/showcase/ibm-institute-for-business-value）をフォローいただくと、定期的に情報を入手することができます。

全米行政アカデミー（National Academy of Public Administration）について

全米行政アカデミーは 1967 年に設立された独立の非営利、無党派団体で、1984 年に国会の認可を取得しています。本アカデミーはより効果的、効率的で、責任と透明性を有する組織の構築について、政府のリーダーたちに対して専門家の助言を提供しています。このミッションを遂行するため、本アカデミーは元内閣高官、国会議員、州知事、市長、州議会議員の他、著名な学者、行政官、非営利団体や企業の幹部などを含む、950 人以上のフェローの持つ知識や経験を活用しています。本アカデミーは詳細な調査と分析、アドバイザリー・サービス、技術支援、議会証言、フォーラムやカンファレンス、オンラインでの利害関係者へのエンゲージメントを通じて、公的機関がガバナンスと管理の重要課題に対処できるようサポートしています。本アカデミーとその活動の詳細については https://www.NAPAwash.org をご覧ください。

IBM Center for The Business of Government について

IBM Center for The Business of Government は助成金とイベントを通じて研究を奨励し、連邦、州、地方、国際レベルの政府の効果向上に向けた新たなアプローチに関する話し合いを促進しています。詳細については https://www.businessofgovernment.org をご覧ください。

アメリカ研究センター（Center for American Studies）について

ローマに本部を置くアメリカ研究センターは、米国とその文化を研究する欧州で最も歴史と権威のある研究機関の 1 つです。同センターは大西洋をまたぐ米国と欧州、イタリアとの関係やその対話を促進することを目的に、米国や欧州の有力な組織や専門家と協力し合いながら、国際政治、経済、その他の時事問題を扱うセミナーや会議を数多く開催しています。また、米国の著述家やジャーナリスト、芸術家、音楽家、映画製作者を招いた会議、展示会、上映会、コンサートなどを開催し、来訪する方々が豊かな文化体験を享受できるよう努めています。

ワシントン D.C. ラウンドテーブルの参加者

Zalmai Azmi
President and COO
Innovative Management and Technology Approaches
（イノベーティブ・マネジメント & テクノロジー・アプローチズ社、社長兼COO）

Lisa Barr
Director of Federal Cybersecurity
Office of the National Cyber Director
（国家サイバー長官室、連邦サイバーセキュリティー担当ディレクター）

Florian Breger
Vice President, Civilian Government
IBM
（IBM、民政担当バイス・プレジデント）

Cristina Caballe Fuguet
Vice President, Global Public Sector
IBM
（IBM、グローバル公共セクター担当バイス・プレジデント）

Dan Chenok
Executive Director
IBM Center for The Business of Government
（IBM Center for The Business of Government、エグゼクティブ・ディレクター）

Kelvin Coleman
Partner, Cybersecurity
IBM
（IBM、サイバーセキュリティー担当パートナー）

Paul Dant
Senior Director
Cybersecurity Strategy & Research
Illumio
（Illumio社、サイバーセキュリティー戦略・調査担当シニア・ディレクター）

Curt Dukes
Executive Vice President & General Manager
Center for Internet Security
（Center for Internet Security、エグゼクティブ・バイス・プレジデント兼ゼネラル・マネージャー）

Candice Frost
Commander, Joint Intelligence Operation Center
United States Cyber Command
（米国サイバーコマンド、統合インテリジェンス・オペレーション・センター司令官）

Terry Gerton
President and CEO
National Academy of Public Administration
（全米行政アカデミー、会長兼CEO）

Hope Goins
Majority Staff Director
House Homeland Security Committee
US Congress
（米国連邦議会、下院国土安全保障委員会マジョリティー・スタッフ・ディレクター）

Marilu Goodyear
Interim Director, School of Public Affairs and Administration
University of Kansas
（カンザス大学、パブリック・アフェアーズ & 行政学研究科、暫定ディレクター）

Margie Graves
Senior Fellow
IBM Center for The Business of Government
（IBM Center for The Business of Government、シニア・フェロー）

Terry Halvorsen
General Manager, US Federal
IBM
（IBM、米国連邦政府担当ゼネラル・マネージャー）

Manuel Hepfer, Ph.D.
Cybersecurity Researcher
Head of Knowledge & Insights
ISTARI & Oxford University
（ISTARI & オックスフォード大学、サイバーセキュリティー研究員、ナレッジ & インサイト部門長）

J. Christopher Mihm
Former Managing Director, Strategic Issues
Government Accountability Office
Adjunct Professor, Public Administration & International Affairs Department
Syracuse University
（シラキュース大学・マックスウェル行政大学院、非常勤教授（行政学・国際問題学））

Joe Mitchell
Director of Strategic Initiatives & International Programs
National Academy of Public Administration
（全米行政アカデミー、戦略イニシアチブおよび国際プログラム担当ディレクター）

Tim Paydos
Vice President & General Manager, Government
IBM
（IBM、政府担当バイス・プレジデント兼ゼネラル・マネージャー）

Greg Porpora
Distinguished Engineer and Distinguished Industry Leader
IBM
（IBM、ディスティングイッシュト・エンジニア & ディスティングイッシュト業界リーダー）

Franklin Reeder
Founding Chair
Center for Internet Security
（Center for Internet Security、創設者・会長）

Douglas Robinson
Executive Director
National Association of State Chief Information Officers
（全米国家最高情報責任者協会、エグゼクティブ・ディレクター）

John Roche
Public Governance Directorate,
Governance Reviews and Partnership
Organisation for Economic Co-operation and Development (OECD)
（経済協力開発機構（OECD）、ガバナンス・レビュー & パートナーシップ、パブリック・ガバナンス・ディレクター）

Ronald Sanders
Staff Director, Florida Center for Cybersecurity
University of South Florida
（南フロリダ大学、フロリダ・センター・フォー・サイバーセキュリティー、スタッフ・ディレクター）

Matt Scholl
Chief of Computer Security Division
National Institute of Standards and Technology
（米国国立標準技術研究所、コンピュータセキュリティ部門長）

Tony Scott
Chief Executive Officer
Intrusion Inc.
（Intrusion社、CEO）

Jim Sheire
Branch Chief
Cybersecurity and Infrastructure Security Agency
（サイバーセキュリティー・社会基盤安全保障庁、支部長）

Kee Won Song
Global Research Leader, Government
IBM Institute for Business Value
（IBM Institute for Business Value、政府担当グローバル・リサーチ・リーダー）

Renata Spinks
Cyber Technology Officer
US Marine Corps Cyberspace Command
（米国海兵隊サイバースペース司令部、サイバー・テクノロジー・オフィサー）

Bobbie Stempfley
Business Security Officer
Dell Technologies
（Dell Technologies社、ビジネス・セキュリティー・オフィサー）

Mike Stone
Managing Partner, Global Government
IBM
（IBM、グローバル政府担当マネージングパートナー）

Shue-Jane Thompson
Managing Partner, Global Deal Leader
Strategic Sales
IBM
（IBM、マネージングパートナー、ストラテジック・セールス担当グローバル・ディール・リーダー）

Kiersten Todt
Chief of Staff
Cybersecurity and Infrastructure Security Agency
（サイバーセキュリティー・社会基盤安全保障庁、チーフ・オブ・スタッフ）

Costis Toregas
Director
Cyber Security Policy and Research Institute
George Washington University
（ジョージ・ワシントン大学、サイバーセキュリティー政策研究所、ディレクター）

Daniel Weitzner
3Com Founders Principal Research Scientist,
Computer Science and Artificial Intelligence Laboratory
MIT
（マサチューセッツ工科大学、コンピュータサイエンス・人工知能研究所3Comファウンダーズ主席研究員）

Dave Zaharchuk
Research Director
IBM Institute for Business Value
（IBM Institute for Business Value、リサーチ・ディレクター）

注釈および出典

1 Venkat, Apurva. “Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says.” CSO. January 4, 2023. https://www.csoonline.com/ article/3684668/cyberattacks-against-governments-jumped-95-in- last-half-of-2022-cloudsek-says.html

2 “Cost of a Data Breach Report 2022.” IBM Security. July 2022. https://www.ibm.com/resources/cost-data-breach-report-2022

3 Lake, Sidney. “The cybersecurity industry is short 3.4 million workers–that’s good news for cyber wages.” Fortune.com. October 20, 2022. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

4 “Women make up just 24% of the cyber workforce: CISA wants to fix that.” CBS News. March 19, 2022. https://wtop.com/business-finance/2022/03/women-make-up-just-24-of-the-cyber-workforce-cisa-wants-to-fix-that/

5 “Readout of Cybersecurity Executive Forum on Electric Vehicles and Electric Vehicle Charging Infrastructure Hosted by the Office of the National Cyber Director.” The White House Briefing Room. October 25, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/25/readout-of-cybersecurity-executive-forum- on-electric-vehicles-and-electric-vehicle-charging-infrastructure- hosted-by-the-office-of-the-national-cyber-director

6 “DHS Launches First-Ever Cyber Safety Review Board.” U.S. Department of Homeland Security. February 3, 2022. https://www.dhs.gov/news/2022/02/03/dhs-launches-first-ever-cyber-safety-review-board

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America | March 2023

本書は英語版「Preparing governments for future shocks - An action plan to build cyber resilience in a world of uncertainty -」の日本語訳として提供されるものです。

PJNRBN7E-JPJA-00