RSA

ホワイト ペーパー

デジタル リスクはミッション リスク

政府機関のミッションに影響を与えるIT モダナイゼーションの動向

連邦機関（民間機関、防衛および諜報機関など）から州政府、地方政府に至るまで、公共部門の組織は、有権者向けサービスを向上させ、国土を保全し、市民をデータに結びつけ、各機関の効率性を高めるためにデジタル トランスフォーメーションを進めています。

デジタル トランスフォーメーションは一夜で成し遂げられるわけではありません。この取り組みは、ITモダナイゼーションを監督および実行する政府機関レベルのCIOを定めた1990年代の法律制定（1996年のクリンガー・コーエン法）[1]で始まり、政府への市民参加を向上させるためにインターネットの使用を促進する2002年の電子政府法[2]を通じて継続されました。また、2002年には連邦情報セキュリティ近代化法（FISMA）が制定され、政府の変革に応じて適切なセキュリティ対策を確実に実施できるようになりました。最近では、Cloud First[3]やCloud Smart[4]などのポリシーと標準により、組織が政府のデジタル トランスフォーメーションを急速に推進するようになっています。さらに、大統領令には、行政機関のサイバー アジェンダの概要が示されています。このような変化によって、政府のITおよびセキュリティの専門家は、システムとデータの安全を確保し、政府と市民の機密データを保護すると同時に、関係者に対してオープンかつ透明であり続けることを求められています。

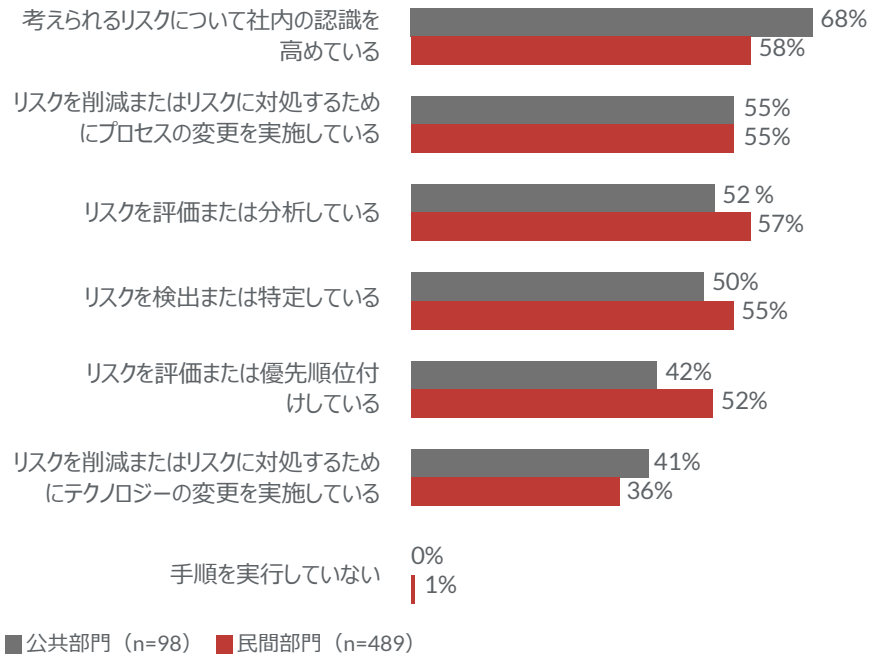
有権者にミッションの成果をもたらすためにデジタル トランスフォーメーションを推進している政府組織は、単独で活動する場合も、他の組織（公共および民間）と連携して活動する場合も、ミッションに影響を及ぼす可能性のあるリスクの増大に直面しています。政府機関とそのパートナーは、オンラインおよびモバイル エクスペリエンスを通じて市民が政府のサービスに簡単にアクセスできるようにする取り組みを進めているため、これらの活動がオペレーションとデータをサイバー攻撃に対してより脆弱にするリスクもあります。この場合、サイバー攻撃は、国家、活動家、不満を抱く国民など、混乱を生み出そうとしている外部の行為者によるものと、政府機関の職員という内部関係者による脅威があります。これらの攻撃は、次のような重大な影響を及ぼす可能性があります。

- 国家安全保障への脅威
- 公共サービス、公益事業、医療の混乱
- プライバシー侵害、データ侵害、何百万人もの市民の個人データと財務データがダークWeb上の犯罪者に公開されること
- 機密情報の漏洩による国外または国内からの反感、経済貿易への影響、軍隊への危害の可能性
- 正当な選挙に対する有権者の信頼を損なう選挙改ざん

政府機関とそのパートナーは、オンラインおよびモバイル エクスペリエンスを通じて市民が政府のサービスに簡単にアクセスできるようにする取り組みを進めているため、これらの活動がオペレーションとデータをサイバー攻撃に対してより脆弱にするリスクもあります。

公共部門の組織は、デジタル リスクの深刻な性質を痛感しており、それを緩和するための措置を講じています。2019年版のRSAデジタル リスク レポートに収録されているRSAデジタル リスク調査の結果によると、公共部門の回答者の68%が、デジタル トランスフォーメーションの潜在的なリスクについて組織内で意識を高めるための措置を講じていると報告しました。それに対し、民間部門の組織の割合はわずか58%にとどまっています。このことは、リスクについての従業員の意識を高め、自分自身および政府のデータとシステムを悪意のある行為者から保護する方法について従業員を教育することにおいて、公共部門の組織が民間部門の組織を上回っていることを示しています。

デジタル リスクを管理するための手順



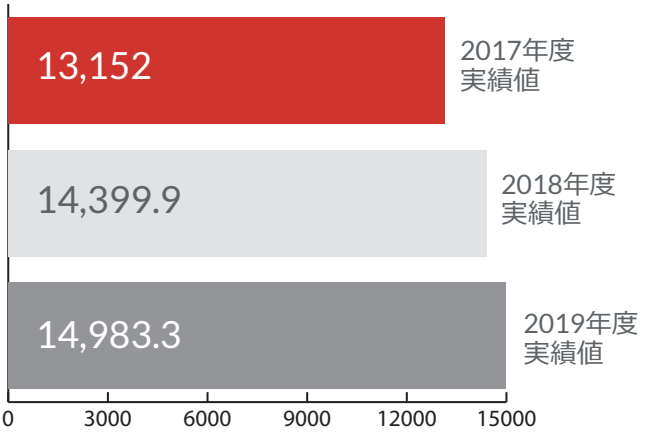
2019年版のRSAデジタル リスク レポートに収録されているRSAデジタル リスク調査の結果によると、公共部門の回答者の68%が、デジタル トランスフォーメーションの潜在的なリスクについて組織内で意識を高めるための措置を講じていると報告しました。それに対し、民間部門の組織の割合はわずか58%にとどまっています。

また、公共部門の回答者は、今後2年間で最も懸念されるデジタル リスクのトップ3領域として、サイバー攻撃のリスク、データ プライバシー リスク、動的ワークフォース リスクを指摘しました。

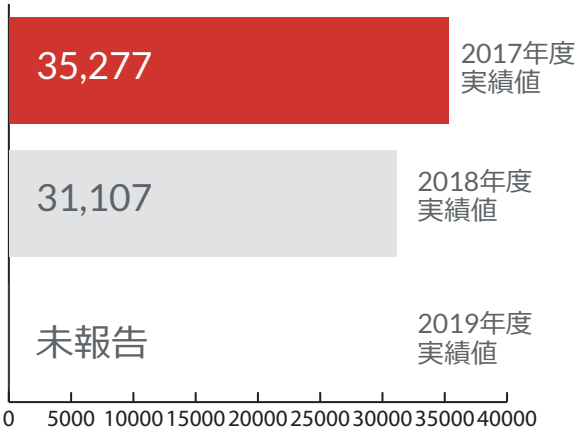
サイバー攻撃のリスク

RSAデジタル リスク調査によると、サイバー攻撃を緩和することは、公共部門が過去2年間に取り組んできた最大のリスク管理目標でした。このリスクを管理することの重要性は、米国会計検査院（GAO）のFISMA 2018年版年次報告書で取り上げられています。この報告書は、サイバー攻撃リスクの管理に向けた大幅な進展を示しています。たとえば、サイバーセキュリティ インシデントは前年度比で12%減少しました（2017年度は35,277件）。その一方で、2018年度にはまだ31,107件を超えるサイバーセキュリティ インシデントが発生したという事実も強調されています[5]。これは、連邦機関が情報やシステムを悪意のある行為者から保護するという大きな課題に直面しており、サイバーセキュリティの課題が連邦政府にとって「ハイリスク問題」となっていることを示しています[6]。さらに最近のGAOの報告では、「国家のサイバーセキュリティを保証すること」が9つのハイリスク領域の1つとして特定され、行政と議会が注力することの必要性が指摘されています[7]。

政府機関のサイバーセキュリティ資金の合計
（百万ドル）



FISMAによって報告されたがサイバーインシデント件数



出典：https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf

今日のサイバーセキュリティの課題に直面している公共機関は、連邦機関だけではありません。今年の初めには、テキサス州で発生したランサムウェア攻撃が22の自治体に影響を与えたのとほぼ同時期に、ボルチモア市のデータ ネットワーク、ジョージア州の裁判所システム、ユタ州の郡政府も標的にされました[8]。これらの政府がランサムウェア攻撃に対して連邦政府よりも脆弱であるのは、攻撃者が小規模な政府ほどサイバーセキュリティに投資できるリソースが少ないと考えているためであると推測されます。このようなタイプの攻撃の多くは増加していますが[9]、州レベルと地方自治体レベルで対策が練られています。たとえば、テキサスをはじめとした州は、セキュリティ ツールや監視および検出機能への費用対効果の高いアクセスを地方自治体や公共機関に提供するため、民間プロバイダーと協力して、サイバーセキュリティ サービスとマネージド セキュリティ サービス（MSS）などのツールやサポートを提供しています[10]。さらに、州や地方自治体はトレーニングを拡大し、サイバー対応のためのベスト プラクティスに関する従業員の教育を支援しています。フィッシング メールに関するユーザーの教育、それらを認識して適切に対応する方法などの簡単なトレーニングを実施することによって、潜在的な脅威にフラグを立て、フィッシング ベースの同様の攻撃を防げる可能性があります。

公共部門の組織は、予算やリソースの制約と戦いながら、サイバーセキュリティに対するアプローチに改善を重ねています。政府機関は、アメリカ国立標準技術研究所（NIST）のCyber Security Framework（CSF）などの一般的なサイバーセキュリティ フレームワークを採用して、サイバー攻撃に対する特定、検出、保護、対応、回復のためのテクノロジー、人員、プロセスに重点的に取り組んでいます。政府組織は、リスクベースのアプローチを採用し、オートメーションと高度な脅威検出を導入して、最も重要な脅威に優先順位を付けられるようにしています。また、政府組織のセキュリティ リーダーは、基本的なセキュリティ保護（多要素認証、アイデンティティー ガバナンス、ライフサイクル管理など）の導入と改善を続け、誰が政府の情報にアクセスしているかを確実に把握できるようにしています。

政府組織のセキュリティ リーダーは、基本的なセキュリティ保護（多要素認証、アイデンティティー ガバナンス、ライフサイクル管理など）の導入と改善を続け、誰が政府の情報にアクセスしているかを確実に把握できるようにしています。

動的ワークフォースのリスク

今日の公共サービスの労働力は劇的な変化を遂げています。より多くのミレニアル世代が公共サービスに参加するようになるに伴い、政府の労働力構成が進化しているだけでなく、ミッションをサポートするために多数の請負業者を利用する傾向も続いています。民間部門と同様に、公共部門の組織は、より多くのデジタル テクノロジーを採用して、ミッションの成果を達成できるよう従業員の生産性と効率性を高めています。ただし、このことは課題も生んでいます。つまり、政府のセキュリティおよびリスク管理リーダーは、多様なワークフォースのためにデバイス、プラットフォーム、およびクラウド間でオープンかつ流動的な情報の流れを確保するとともに、市民と政府のデータを保護する上で必要なリソースのセキュリティを管理し、コントロールする必要もあります。

この課題をさらに複雑にするものとして、政府機関は、公共部門のエコシステム全体でアクセスとアイデンティティーを保証できるよう、政府機関と行政レベルの命令に加え、規制当局の命令による追加の要件も満たす必要があります。このバランスを管理するためのポリシーも変更されています。政府は長年にわたって内部関係者による脅威への対策を講じてきましたが、内部関係者による脅威の概念は進化しています。ますます多くの政府データがモバイル デバイス上とクラウド内に置かれるようになる中、単に不注意な（悪意はない）従業員や請負業者でさえも、脆弱なリンクになる可能性があります。政府発行のノートパソコンをバスに置いたままにしたり、PIVカードをなくしたり、政府発行のデバイスから個人用またはその他の仕事用デバイスに仕事のデータを転送したりすることは、すべて現実のリスクであり、単純なミスでさえデータ損失につながる可能性があります。公共部門の組織は、トレーニングと意識向上を通じて、この問題への取り組みを強化しています。RSAデジタル リスク レポートの発見事項として前述したとおり、デジタル リスクに対する従業員の意識を高める取り組みは、公共部門の組織の方が民間部門の組織よりも優れています。すべての公務員と請負業者が政府のデータとリソースのセキュリティに責任を負うようにするための鍵は、継続的な警戒とトレーニングにあります。

最後に、従業員の生産性を高めるために政府機関のセキュリティ リーダーが導入するツールも進化しています。リーダーは、従来のアクセス制御（CAC/PIV）を補完するとともに、最新の認証アプローチを使用してアクセスをシンプルにする、多要素認証、モバイル プッシュ、バイオメトリクスなどの新しいコントロールを採用することを検討しています。これにより、従業員のアクセスを取得するプロセスが合理化されると同時に、各システム全体のアクセス制御も保証されます。バックエンドでリスクベースの分析を行うと、利用者である従業員にとってフリクション（手間やストレス）を引き起こさない新しい方法で不適切なアクセスを監視し、検出することが可能になります。

政府組織はデータ プライバシー リスクへの対処に絶えず取り組んでいます。その一環として、アクセス制御を向上させて、誰がデータにアクセスでき、そのデータで何をしているのかを可視化するとともに、従業員と市民のプライバシーを確保できるよう、データ管理ポリシーを進化させています。

データ プライバシーのリスク

データ プライバシーは誰にとっても懸念事項です。ビジネスの世界では、注目度の高いデータ侵害が新聞の見出しを飾っていますが、公共部門の組織が影響を受けていないわけではありません。2019年のVerizonデータ侵害調査レポートでは、データ侵害の16%が公共部門で発生しており、医療機関とほぼ同じ割合であることが明らかになりました[11]。National Law Review誌は、公共部門のデータ プライバシー リスクのことを、特に2019年に連邦人事管理局（OPM）が侵害された後で重要性を高めつつある、「あまり議論されてこなかった」リスクとして表現しています。この侵害事例では、何百万もの身元調査記録と人事書類が公開されました[12]。

OPMの侵害の規模は、政府機関のシステムでどれだけの個人データが危険にさらされているかを再認識させるものです。政府機関のシステムには、連邦政府で働いている、または連邦政府の仕事に応募している何百万人もの人以外にも、さらに何百万人分ものデータが保存されています。政府機関のミッションは、有権者にサービスを提供することです。その意味で、市民のデータを保護し、データが意図された目的にのみ使用されることを保証することは、政府が市民からの信頼に応える一つの方法であり、ミッションの成功を確実にする上で非常に重要です。

プラスの側面に目を向けると、政府組織はデータ プライバシー リスクへの対処に絶えず取り組んでいます。その一環として、アクセス制御を向上させて、誰がデータにアクセスでき、そのデータで何をしているのかを可視化するとともに、従業員と市民のプライバシーを確保できるよう、データ管理ポリシーを進化させています。たとえば、内国歳入庁は、納税者を認証するための社会保障番号の使用を最小限に抑えるプログラムを導入しています[13]。また、NISTはまもなく、公共機関だけでなく民間企業のモデルとしても機能するデータ プライバシー フレームワーク（既存のNIST CSFと同様）を導入する予定です[14]。

まとめ

今日の政府組織は、有権者にサービスを提供する方法とテクノロジーでミッションの成果を実現する方法をモダナイズし続けています。RSAデジタル リスク調査が明らかにしているとおり、デジタル トランスフォーメーションに関連するリスクの管理は、政府のセキュリティ リーダーにとって最優先事項です。しかし、今日の政府の仕事がデジタル トランスフォーメーションとともに変化しているように、デジタル リスクも進化を遂げています。また、政府機関のミッションに影響を及ぼすのは、ここで説明した3つのリスクだけでなく、規制リスクや運用リスク、その他のリスクもあります。政府機関にとってのリスクは間違いなく高く、課題もその分重大です。一つ確実なのは、デジタル トランスフォーメーションに関連したリスクを管理する必要があるということです。RSAデジタル リスク調査によると、デジタル トランスフォーメーションを推進している公共部門の組織は、このことを痛感しています。公共部門は、デジタル リスクに対する意識を高める点で民間部門よりもはるかに進んでいますが、ミッションの成功を確実にするために、そのリスクのさまざまな側面を評価し、優先順位を付け、対処することにおいては、まだまだ道半ばです[15]。

公共部門は、デジタル リスクに対する意識を高める点で民間部門よりもはるかに進んでいますが、ミッションの成功を確実にするために、そのリスクのさまざまな側面を評価し、優先順位を付け、対処することにおいては、まだまだ道半ばです。

誰もが持つデジタル リスクの管理をRSAがサポート

RSA® Business-Driven Security™ソリューションは、統合型の可視性、自動化されたインサイト、調整されたアクションに依存する、統一されたデジタル リスク管理アプローチを組織に提供します。RSAのお客様は、迅速な検出と対応、ユーザー アクセス制御、消費者向け詐欺防止、統合型リスク管理のためのソリューションを使用して成長し、革新的な変化に継続的に適応できるようになります。

リスクの高い動的な世界で成功を収める方法については、rsa.com/ja-jpをご覧ください

1 『Information Technology Management Reform Act of 1996』、Wikipedia: The Free Encyclopedia、Wikimedia Foundation, Inc.（2019年2月19日午後7時45分）、https://en.wikipedia.org/wiki/Information_Technology_Management_Reform_Act_of_1996（2019年10月10日にアクセス）

2 『E-Government Act of 2002』、Wikipedia: The Free Encyclopedia、Wikimedia Foundation, Inc.（2019年4月18日午後2時00分）、https://en.wikipedia.org/wiki/E-Government_Act_of_2002（2019年10月10日にアクセス）

3 『OMB announces 'cloud first' policy for agencies』、Federal News Network、https://www.federalnewsnetwork.com/technology-main/2010/11/omb-announces-lsquocloud-firstrsquo-policy-for-agencies/（2010年11月23日）

4 『From Cloud First to Cloud Smart』、Federal Cloud Computing Strategy、https://cloud.cio.gov（2019年10月10日にアクセス）

5 『Federal Information Security Modernization Act of 2014: Annual Report to Congress』、https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf（2018年度）

6 『Key Issues: Cybersecurity Challenges Facing the Nation—High Risk Issue』、米国会計検査院、https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary（2019年10月10日アクセス）

7 『High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas』、米国会計検査院、https://www.gao.gov/products/GAO-19-157sp#summary（2019年3月6日）

8 『22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault』、National Public Radio、https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault（2019年8月20日）

9 Allen Kim、『In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks』、CNN、https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html（2019年10月8日）

10 『Cyberdefense for Texas State Government』（Fiscal Notes: A Review of the Texas Economy from the Office of Glenn Hegar, Texas Comptroller of Public Accounts）、https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php（2019年3月）

11 『2019 Data Breach Investigations Report』、Verizon、https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf（2019年5月）

12 Kristin Ann Shepard、『Data Privacy Exposure Hits the Public Sector』、The National Law Review、https://www.natlawreview.com/article/data-privacy-exposure-hits-public-sector-lessons-opm-data-breach-class-action（2019年8月13日）

13 『What are we doing to protect taxpayer privacy?』IRS、https://www.irs.gov/privacy-disclosure/what-are-we-doing-to-protect-taxpayer-privacy（2019年10月18日）

14 Alex Hickey、『Government takes baby steps in data privacy with NIST framework, bill discussions』、CIO Dive、https://www.ciodive.com/news/government-takes-baby-steps-in-data-privacy-with-nist-framework-bill-discu-1/550084/（2019年3月12日）

15 『RSA Digital Risk Study』（RSA Digital Risk Report, 1st Edition）、https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf（2019年9月）