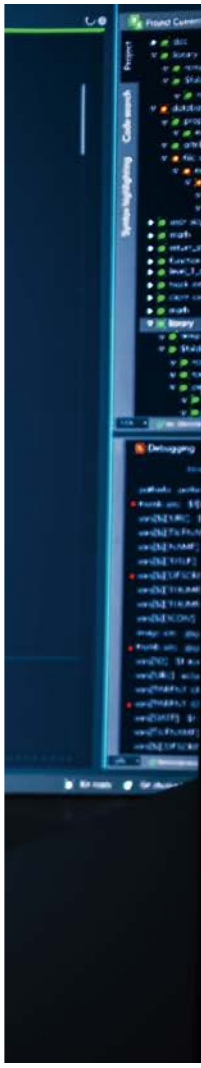


ISMAPから考える
デジタルサプライチェーン管理

pwc

www.pwc.com/jp

目次

はじめに　～サプライチェーン管理の重要性の高まり～

昨今、グローバル化の進展とデジタル技術の急速な発展により、組織のサプライチェーンはますます複雑化しています。そのため、サプライチェーンに起因する情報漏洩や事業停止によってブランド・信用を毀損するケースが増加しており、その影響は組織の存続にまで及ぶケースもあります。特に、サプライチェーンの脆弱性を狙った攻撃による深刻な被害が急増しています。情報処理推進機構（IPA）が発表する「情報セキュリティ10大脅威（組織）」においても、2019年以降、常に上位に位置づけられており、近年ではさらに重要度が増しています（図表1）。

サプライヤーは自組織と異なりコントロールが難しいため、サプライチェーンに対してガバナンスを効かせるのは難易度が高いのが実情です。加えて、サプライチェーン全体の透明性が低いことから、どの部分にリスクが潜んでいるのかを把握すること自体が難しい場合もあります。

このため、サプライチェーンにおけるインシデントは社会問題化しており、自組織だけでなく、消費者や取引先、さらには国全体の経済にも影響をもたらしかねません。

これからの組織運営においては、サプライチェーンを健全に維持し、適切にリスクマネジメントするための包括的な戦略が必要です。組織が上述の課題に対処するためには、サプライチェーン全体を可視化し、リスクを特定してコントロールすることが求められます。

また、近年では、クラウドサービス、IoT、AIといった先進技術を利用したサービスが社会に浸透してきています。これらの技術は、業務効率の向上や新たなビジネスモデルの創出に大いに寄与する一方で、新たなリスクも生み出しています。特に重要なのが、これらの技術がデジタルサプライチェーンとして成り立っていることに伴うセキュリティ対策です。デジタルサプライチェーンとは、複数の事業者が提供するデジタルサービスが連携し、1つのシステムとして機能する構造を指します。この連携により、企業は高度なサービスを提供できる一方で、各事業者のセキュリティ対策が十分に実施されていないと、その影響が連鎖して広がるリスクが高まります。

このレポートでは、デジタルサプライチェーンのリスクに焦点を当て、その特徴や制度の活用方法について、ISMAP（政府情報システムのためのセキュリティ評価制度）を例に取りながら解説します。デジタルサプライチェーン管理の現状と今後の方向性を探ることで、組織が直面するリスクをコントロールし、持続可能な成長を実現するための手助けとなれば幸いです。

図表1：情報セキュリティ10大脅威（組織）の変遷

情報セキュリティ10大脅威 2021（組織）	
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	テレワーク等のニューノーマルな働き方を狙った攻撃
4	サプライチェーンの弱点を悪用した攻撃
5	ビジネスメール詐欺による金銭被害
6	内部不正による情報漏えい
7	予期せぬIT基盤の障害に伴う業務停止
8	インターネット上のサービスへの不正ログイン
9	不注意による情報漏えい等の被害
10	脆弱性対策情報の公開に伴う悪用増加

情報セキュリティ10大脅威 2022（組織）	
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	サプライチェーンの弱点を悪用した攻撃
4	テレワーク等のニューノーマルな働き方を狙った攻撃
5	内部不正による情報漏えい
6	脆弱性対策情報の公開に伴う悪用増加
7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8	ビジネスメール詐欺による金銭被害
9	予期せぬIT基盤の障害に伴う業務停止
10	不注意による情報漏えい等の被害

情報セキュリティ10大脅威 2023（組織）	
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等のニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化（アンダーグラウンドサービス）

情報セキュリティ10大脅威 2024（組織）	
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

出所：IPA発表資料を基にPwC作成

1 デジタルサプライチェーンとセキュリティ対策

デジタルサプライチェーンをセキュリティの観点から考えた場合、以下のような特徴を有しています。

(1) 複雑なエコシステムと相互依存性

デジタルサプライチェーンは、複数の異なる事業者やサービスプロバイダーが連携して成り立っています。各事業者が提供するサービスやデータが一体となってシステム全体を構成しているため、1つの事業者のセキュリティ対策が不十分だと、その脆弱性が全体に影響を及ぼす可能性があります。この相互依存性の高さが、セキュリティ対策を複雑化させ、全体のリスク管理を難しくしています。

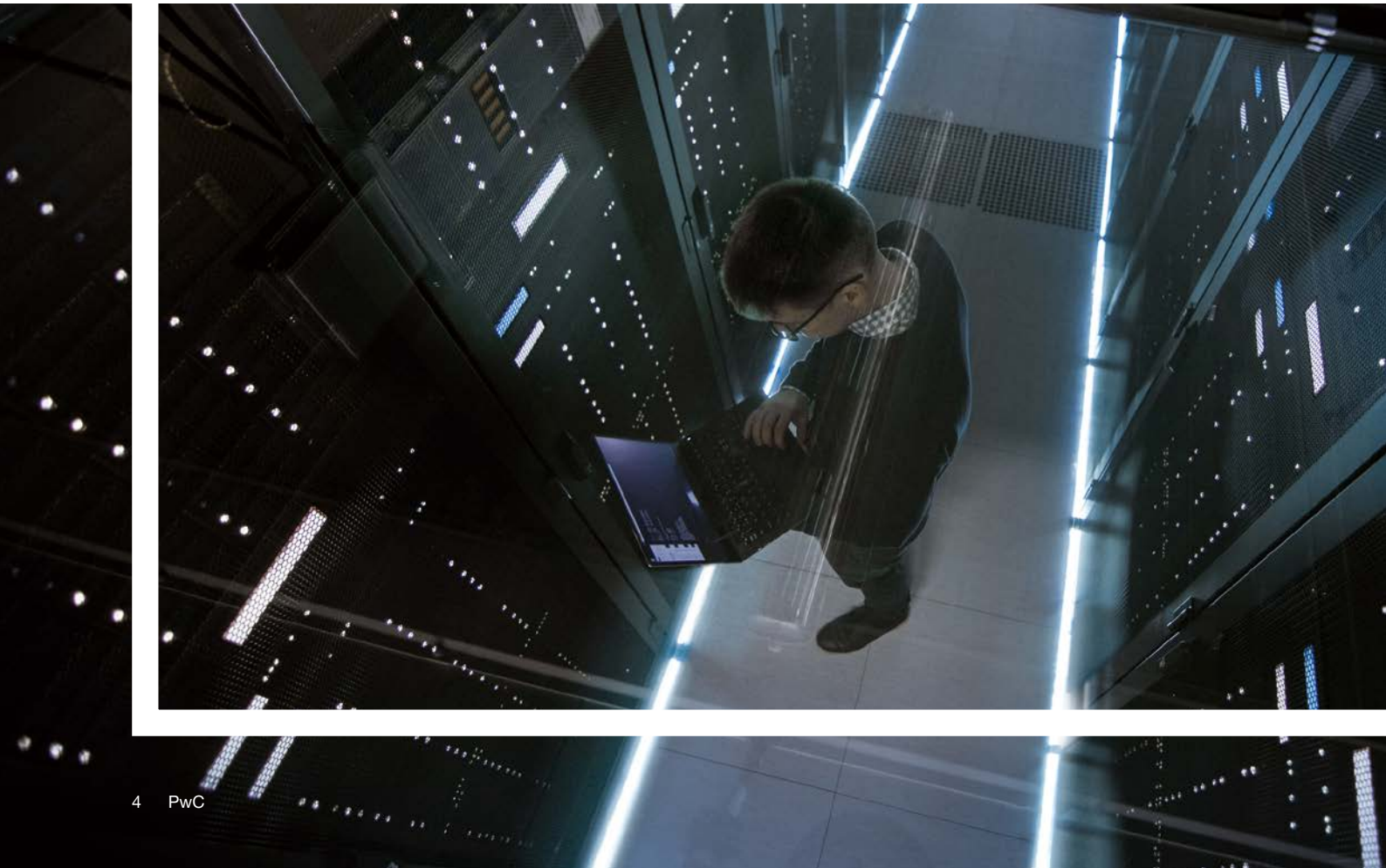
(2) 境界の曖昧さと広範な侵入ポイント

従来のサプライチェーンでは、物理的な境界やネットワークの境界が比較的明確でした。しかし、デジタルサプライチェーンでは、クラウドサービスやIoTデバイスが広範に接続されるため、境界が非常に曖昧になりがちです。このため、攻撃者が侵入できるポイント（攻撃面）が広がり、セキュリティ対策が一層困難になります。各ノードや接続点での強固なセキュリティが求められます。

(3) データのリアルタイム性と可視性の必要性

デジタルサプライチェーンでは、個人情報・機密情報について、リアルタイムでのデータ交換が行われることが多く、迅速な意思決定が求められます。このため、データの可視性とトレーサビリティ（追跡可能性）がより重要となります。適切なアクセス制御や監視体制を整えることで、不正アクセスやデータ漏洩のリスクを最小限に抑える必要があります。リアルタイムで異常を検知し対応できる柔軟なセキュリティ対策が不可欠です。

組織はこれらの特徴を有するサービスのリスクに対処するために、統合的なリスクマネジメント戦略を策定し、実行に移さなければなりません。例えば、クラウドサービスのセキュリティ評価を効率化するためには、サプライチェーン全体を通した定期的なリスクアセスメントを実施し、各事業者の責任分界点を明確にした上で、共通のセキュリティ基準を設け、それに基づいて評価を行うことが有効です。また、APIやIoTデバイスのセキュリティ強化に向けたガイドラインの策定や、それらを遵守するための監査体制の整備も欠かせません。



2 日本の政府機関における デジタルサプライチェーン管理の課題とISMAP制度

日本の政府機関においても、デジタルサプライチェーン管理の重要性が増大しています。従来、各府省庁は個別にセキュリティチェックリストを作成し、サプライヤーに記入させることでセキュリティ評価を行っていました。しかし、この方法には多くの課題がありました。まず、各府省庁が作成するチェックリストには重複が多く、サプライヤーの負担が大きかったことです。さらに、府省庁内にはセキュリティ評価を適切に行える専門人材が不足しており、その結果、評価が形骸化するケースも少なくありませんでした。

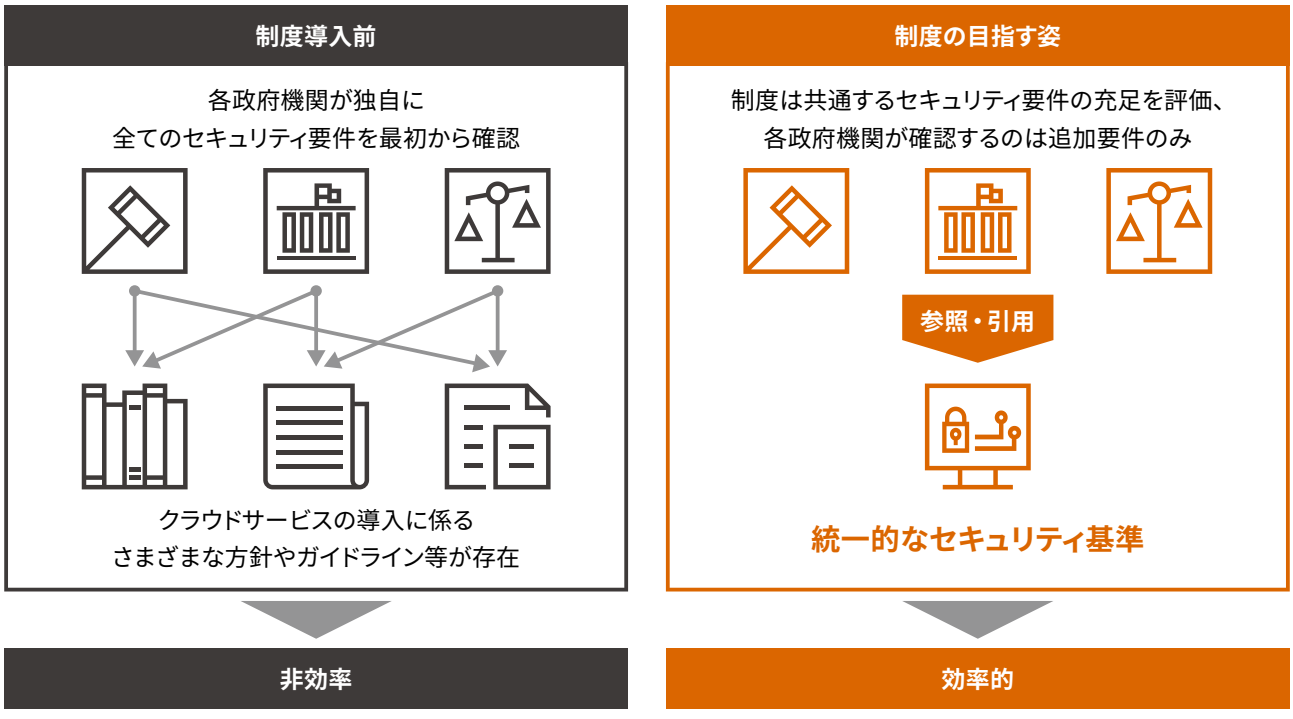
これらの課題に対処するために、日本政府は諸外国の事例を参考にしました。例えば、米国のFedRAMP（Federal Risk and Authorization Management Program）は、クラウドサービスのセキュリティリスクを統一された基準で評価・管理する仕組みを提供しています。この制度では、従来省庁ごとに実施していたセキュリティ評価を統一化し、セキュリティ評価の効率化と透明性の向上、リスク管理の強化、そしてコスト削減を実現することを目的としています。これにより、連邦政府機関が安全かつ効率的にクラウドサービスを利用できる環境が整備されています。

これに倣い、日本ではISMAP（政府情報システムのためのセキュリティ評価制度）が導入され、政府機関が共通の基準でクラウドセキュリティを評価できる仕組みを構築しました。ISMAPは、政府機関が求めるセキュリティ水準を標準化し、共通の評価の仕組みを導入することにより、政府機関におけるクラウドサービスの円滑な利用を可能にしています（図表2）。

ISMAPの導入により、各府省庁はセキュリティ対策の大部分をISMAPで担保できるため、個別にセキュリティをチェックする領域が大幅に削減され、セキュリティ評価の効率化が図られました。また、共通の基準に基づく評価により、サプライヤーも一度の評価で複数の府省庁に対応できるため、サプライヤー側の評価・チェック負担が軽減されました。さらに、ISMAPはクラウドセキュリティの知見を持つ制度運営機関による審査を行うため、セキュリティ評価の信頼性も向上しています。

図表2：ISMAPの仕組みと目的

ISMAPは、従来各政府機関等が個別に評価していたクラウドサービスのセキュリティ要件について統一的な評価を可能にし、政府機関等のクラウドサービス調達における**セキュリティ水準の確保**と**円滑な導入**を**目的**としています。



出所：総務省発表資料「はじめてのISMAP」を基にPwC作成

3 デジタルサプライチェーンのセキュリティリスクの特徴から考えたISMAPの適合性

前述したデジタルサプライチェーンのセキュリティリスクに、ISMAPは以下のように対応しています。

図表3：デジタルサプライチェーンのセキュリティリスクに対するISMAPの対応

デジタルサプライチェーンにおけるセキュリティリスクの特徴	ISMAPの対応状況
1. 複雑なエコシステムと相互依存性	• ISMAPでは、クラウドサービス事業者が「言明書」を作成し、自社の管理範囲を明確化した上で、監査が実施されている。 • SaaS事業者が別の事業者のIaaSサービスを利用するなど、申請中のクラウドサービスに必要不可欠な別事業者のサービスを利用している場合には、当該サービスがISMAPに登録されているかを審査によってチェックしている。
2. 境界の曖昧さと広範な侵入ポイント	
3. データのリアルタイム性と可視性の必要性	• クラウドサービス事業者の管理策（セキュリティ上の要求事項）として、ログモニタリングやインシデント対応の管理策が存在する。 • リアルタイムに監視するという具体的な要求事項は存在しない。

出所：PwC作成

ISMAPでは、複数の事業者が関係するクラウドサービスのセキュリティ評価の問題について、責任分界点をクラウド事業者に明示させ、他の事業者のクラウドサービスを利用している場合、その重要性を審査過程で考慮し、ISMAP対応の必要性を検討するという形で対応を実施しています。一方、リアルタイム監視という観点では、具体的な管理策の内容として明示されていない状況です。また、サプライチェーン管理全般で考えると、米国立標準技術研究所（NIST：National Institute of Standards and Technology）のSpecial Publication 800-161（Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations）もリリースされていることから、これらの内容を考慮・参考にした上で継続的に管理策の内容を改善・検討していくことが重要になると考えられます。

4 ISMAPの継続的改善

前述したように、デジタルサプライチェーンのセキュリティ対策においては、リアルタイムにデータを監視することが重要です。また、単に特定の時点で想定されるリスクへの対応を確認するだけではなく、環境の変化や技術の進化に応じてセキュリティ上必要な項目を定期的に更新し、その遵守状況を継続的にモニタリングすることも必要不可欠です。これは、デジタルサプライチェーンが新しい技術を取り入れ絶えず進化し続けており、新たなリスクや脅威が発生するためです。

ISMAPにおいても、このような観点を踏まえて、管理策内容の定期的な見直しが実施されています。例えば、NISC（内閣サイバーセキュリティセンター）が発行している「政府機関等のサイバーセキュリティ対策のための統一基準群」の更新を受けて、2024年8月にISMAPの管理基準が改定されました。また、JIS Q 27001およびJIS Q 27002の改定を受けて、ISMAPの管理基準の見直しも検討されています。これにより、ISMAPの管理基準が最新のセキュリティ要件に準拠し、クラウドサービスの安全性がより確保できるよう目指しています。

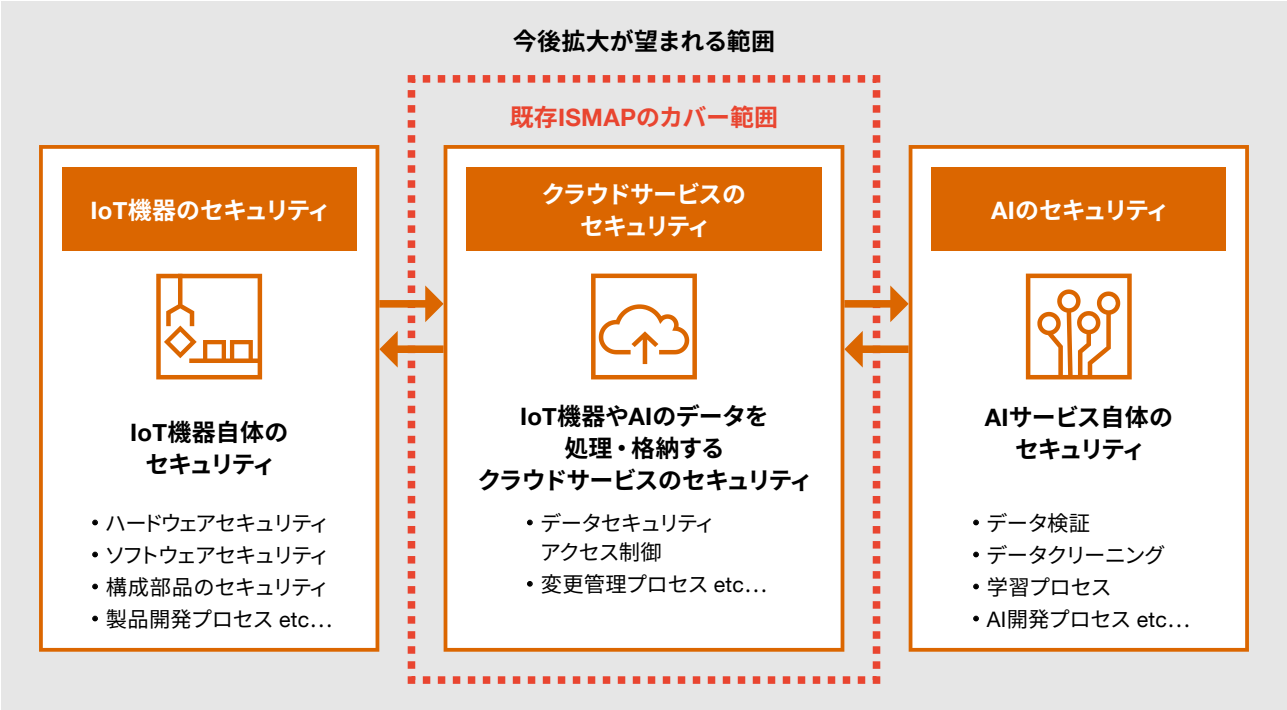
5 ISMAPが日本のデジタルサプライチェーンに与える影響・ポテンシャル

2024年9月17日時点で、ISMAPクラウドサービスリストには73のサービスが登録されています。10年以上の運用実績がある米国のFedRAMP（346サービス）と比較しても順調に登録サービス数を増やすことができており、ISMAPは4年程度の運用期間であることを考えるとまだ伸びしろのある制度と考えられます。

ISMAPは、クラウドサービスの一般的なセキュリティ要求事項への遵守・対応状況を確認し、クラウドサービスリストへの登録を行うものです。したがってAIやIoTなどの個別のトピックに特化して対応できているわけではありません。しかし、AIやIoTなどは、データ処理にクラウドサービスを利用しているケースが多く、デジタルサプライチェーン全体で見れば、クラウドサービスが1つの構成要素として存在します。

したがって、以下の図表4のように、既にクラウドサービスのセキュリティ評価で成功しているISMAPをベースに、IoTやAI特有のセキュリティ上の論点をカバーすることにより、デジタルサプライチェーン全体でのセキュリティを担保する仕組みを検討することが、迅速な新技術の導入とリスク対応を実現する上で重要な役割を果たします。

図表4：ISMAPを活用したAI・IoTセキュリティ対応



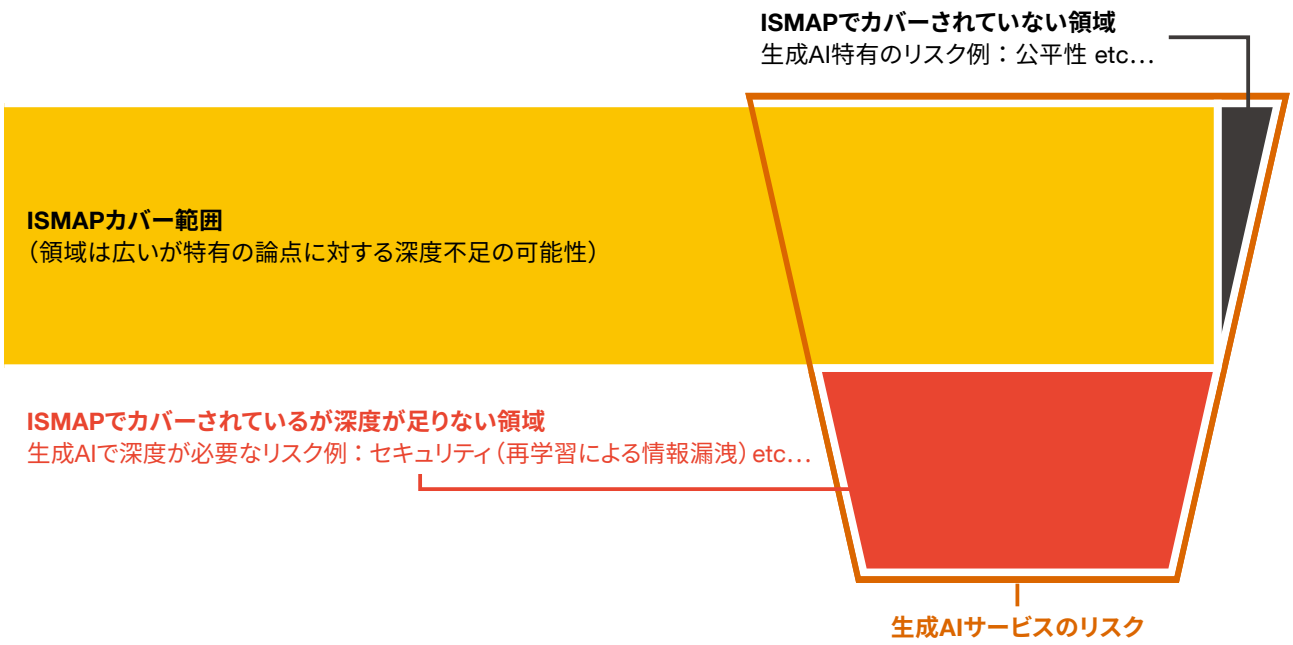
出所：PwC作成

なお、米国では、NISTのSpecial Publication 800-183（Networks of ‘Things’）が、IoTデバイスのネットワークアーキテクチャとセキュリティに関するガイドラインを提供しており、データ管理にクラウドサービスを利用している場合のセキュリティ評価にFedRAMPを活用することが推奨されています。このように、セキュリティ評価の制度を相互利用することで、評価の効率化と信頼性の向上が図られています。

日本でも、クラウド・バイ・デフォルト原則やガバメントクラウドの導入が進んでおり、デジタル行政システムのクラウド化が加速しています。ISMAPに登録されているサービスも増加しており、今後ますますその重要性が高まると予想されます。ただし、ISMAPはあくまでもクラウドサービスの一般的な安全性評価の仕組みであるため、前述のとおり特定の論点やリスクに対しては、追加の評価が必要です。したがって、図表5の生成AIの例のように、個別のトピックに対してもISMAPを適切に活用・参照することで、デジタルサプライチェーン管理の効率化を図り、限られたリソースを本当に必要な領域に集中させることも可能であると考えられます。

ISMAPは、政府機関だけでなく、地方公共団体の調達時にISMAPの登録簿を参照することが推奨され、基幹インフラ分野での活用も検討されています。今後デジタルサプライチェーン全体のセキュリティ向上を目的に、さらに活用が広がることが期待されます。

図表5：生成AIへのISMAPの活用例



出所：PwC作成

おわりに

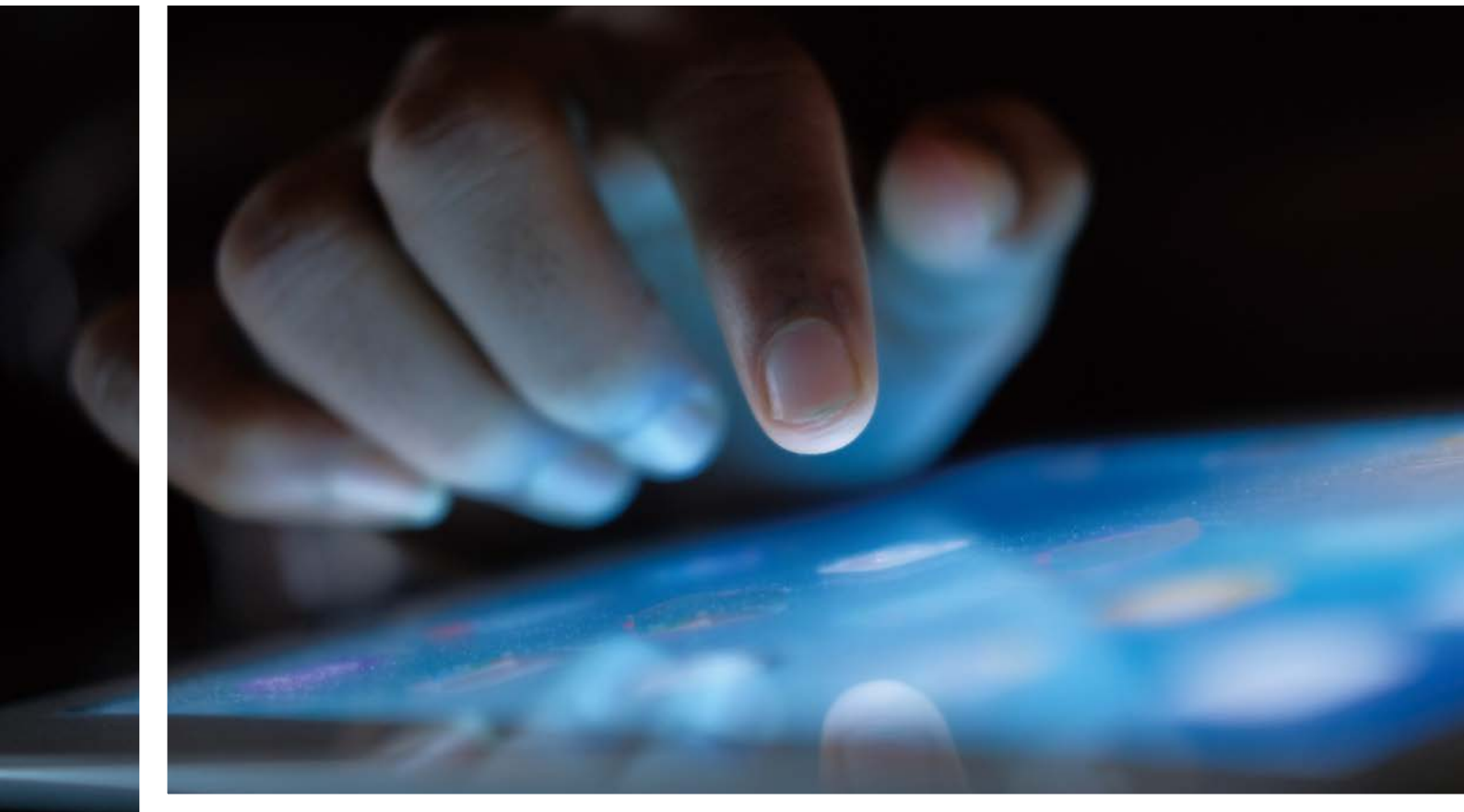
デジタルサプライチェーンのセキュリティリスクを担保するプログラムとして、ISMAPを例に取り、その重要性と具体的な取り組みについて解説しました。デジタルサプライチェーンのリスクマネジメントは、従来の物理的なサプライチェーンとは異なり、より複雑で高度な管理が求められます。また、セキュリティやプライバシーの保護はもちろんのこと、サステナビリティやESG（環境・社会・ガバナンス）、Responsible AI（責任あるAI）といった新しい領域への対応や、ソフトウェアサプライチェーンを対象にSBOM（Software Bill of Materials: ソフトウェア部品表）などを利用して管理するなど、高度な対応も必要となります。

ISMAPは、クラウドサービスのセキュリティ評価を標準化し、政府機関だけでなく、将来的には重要産業分野や民間企業にも広く活用されることが期待されています。これにより、デジタルサプライチェーン全体の安全性と信頼性が向上し、組織が持続可能な成長を実現するための基盤が整備されると考えられています。

デジタルサプライチェーンの重要性が高まる一方で、そのリスクも日々高まっています。したがって、組織においてはデジタルサプライチェーン管理プログラムの早期導入が求められています。適切なリスクマネジメントを行うことで、情報漏洩や事業停止といった重大なインシデントを未然に防ぎ、ブランドや信用を守ることができます。

組織が直面するサプライチェーンリスクに対処するためには、単に制度や基準を遵守するだけでなく、常に最新のリスク情報や技術動向を把握し、柔軟に対応することが求められます。今後も継続的な改善を図りながら、強固なデジタルサプライチェーンを構築していくことが重要です。

デジタルサプライチェーンの管理は、企業の持続可能な成長と競争力強化に不可欠な要素です。ISMAPをはじめとする既存の制度を活用し、総合的なリスクマネジメントを行うことで、組織は安心してデジタル時代のビジネスを展開することが可能となります。



お問い合わせ先

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

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約12,700人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界149カ国に及ぶグローバルネットワークに370,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2024年12月　　管理番号：I202409-01