米国のプライバシー保護に関する動向

目次

1. 概要 2
2. NIST におけるプライバシー保護の体系 4
3. NIST Privacy Framework 6
4. NIST SP 800-53 Rev5 7
5. NIST OSCAL 10
6. グローバルにおける米国のポジションと将来展望 12

1. 概要

米国における最近のプライバシー保護に関する動向としては、2020 年 1 月に施行されたカリフォルニア州消費者プライバシー法（California Consumer Privacy Act：CCPA[1]）が、日本企業への影響も大きく話題となった。その後も多くの州でプライバシー保護関連法の制定を目指した動きが続いている。米国にはプライバシーの保護を国家（連邦）として規定した法律は存在せず、これまでは主に業種などのセクターごとに必要に応じて策定されてきた。ここに州ごとの規制や、州ごとのセクター規制が加わり、複雑化する様相を見せている。

また、プライバシー侵害には、これまで消費者保護の観点から、主として連邦取引委員会（Federal Trade Commission：FTC）が、FTC 法第 5 条を根拠に取締りを執行している。FTC 法第 5 条は「商取引における又は商取引に影響を及ぼす不公正若しくは欺瞞的な行為又は慣行は、本法により違法と宣言する。」というもので、消費者を騙す実務は「欺瞞的」、データ漏えいの場合は「不公正」としている。つまりプライバシーを定義して保護するのではなく、消費者にとって欺瞞的、不公正なものとなる行為の中にプライバシー侵害が含まれているとする考え方である。今後、州ごとにプライバシーを定義した法律が成立することで、FTC 以外の規制当局が増えることになり、取締りについても複雑化するおそれが高まっている。

一方で、連邦レベルでの議論も活発化しており、Microsoft、Google、Apple、Facebook 等の米国グローバル企業は、これまでの慎重意見から積極的に法制度化を求める姿勢に転じている。これは、ケンブリッジ・アナリティカ事件[2]をはじめとするプライバシー侵害の続発による消費者意識の変化に対応するという側面もあるが、セクターごと州ごとに分断された法制度を統一化することで、手間やコストの増大を回避したいという側面も強い。

グローバル企業の制度統一化に対する思惑は、国内だけではなく世界へも向かっており、EU の一般データ保護規則（General Data Protection Regulation：GDPR[3]）におけるプライ

---

[1] https://oag.ca.gov/privacy/ccpa
個人情報保護委員会による日本語訳：
https://www.ppc.go.jp/files/pdf/ccpa-provisions-ja.pdf

[2] 英国のケンブリッジ・アナリティカ社が Facebook のユーザー情報を不正に取得して、米国大統領選や英国のブレクジットに関する投票に影響を与えたとする事件

[3] https://eur-lex.europa.eu/eli/reg/2016/679/oj
個人情報保護委員会による日本語訳：
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

バシーシールド[4]、アジア太平洋経済協力（Asia Pacific Economic Cooperation：APEC）における越境プライバシールール（Cross Border Privacy Rules；CBPR[5]）といった国家・地域間の越境データ保護の相互協定への積極的な関与に見て取ることができる。

以上のように、米国では現時点で EU や日本を始めとする多くの国のような、プライバシーや個人情報の保護に関する包括的な法律を制定し、これを根拠としてさまざまな施策を展開するという構造にはなっていない。そのため、セクターごとや州ごとに規制が乱立することとなってきたが、近年、その弊害である負担の増大への対応だけではなく、グローバル企業による国境を越えた個人情報の流通等への対応が必要になってきていることから、連邦法の制定による制度の統一化の議論が活発化している。しかしながら、極めて多くのステークホルダーの利害が絡むこともあり、早期の成立は困難であるとみられている。

一方で明確な法的根拠がない中であっても、消費者のリテラシーの向上に伴い、消費者や取引企業、さらには公的機関からもプライバシーの保護について実務的、技術的な対策を行い、これを証明することを求める声が高まっている。この潮流を受けて、米国標準技術研究所（National Institute of Standards and Technology：NIST）は 2020 年 1 月にプライバシーフレームワーク（Privacy Framework：PF[6]）をリリースした。また、2020 年中の発行を目指した情報セキュリティ対策とプライバシー保護の要求仕様を統合した Special Publications 800-53 Revision5[7]（以下 SP 800-53 Rev5）の開発を進めている。併せて、これらのガイドラインや仕様書等への準拠の検証について、正確性を高めると同時に労力を低減するために、構造化され機械可読可能な言語、Open Security Controls Assessment Language[8]（以下、 OSCAL）の開発が進められている。

NIST は米国商務省（Department of Commerce：DoC）の傘下にあり、米国の国家機関が採用する情報機器やシステムは、NIST が発行したガイドライン等に準拠することが求められている。また、民間企業へも波及していることから、事実上、米国における国家標準と見なされており、さらにはサイバー・セキュリティ・フレームワーク（Cyber Security Framework：CSF[9]）のようにグローバルでデファクトとなっているものもある。したがっ

---

[4] プライバシーシールドは EU から米国企業への個人情報の移転を当該企業が個人情報保護ルールと保護条項に則っていることを条件に認めるもので、米国商務省に登録し、プライバシー原則（Privacy Principles）にある義務を遵守しなければならない。
https://www.privacyshield.gov/welcome

[5] 個人情報保護委員会による解説：https://www.ppc.go.jp/files/pdf/CBPR_ppc.pdf

[6] https://www.nist.gov/privacy-framework

[7] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[8] https://pages.nist.gov/OSCAL/

[9] https://www.nist.gov/cyberframework

て、現在 NIST が進めているプライバシー保護に関する前述の取り組みは、米国における標準となる可能性が高く、また、米国と取引する企業への影響、その結果としてグローバルへの影響も大きいものと考えられる。以下、NIST におけるプライバシー保護に関する取り組みについて概観する。

2. NIST におけるプライバシー保護の体系

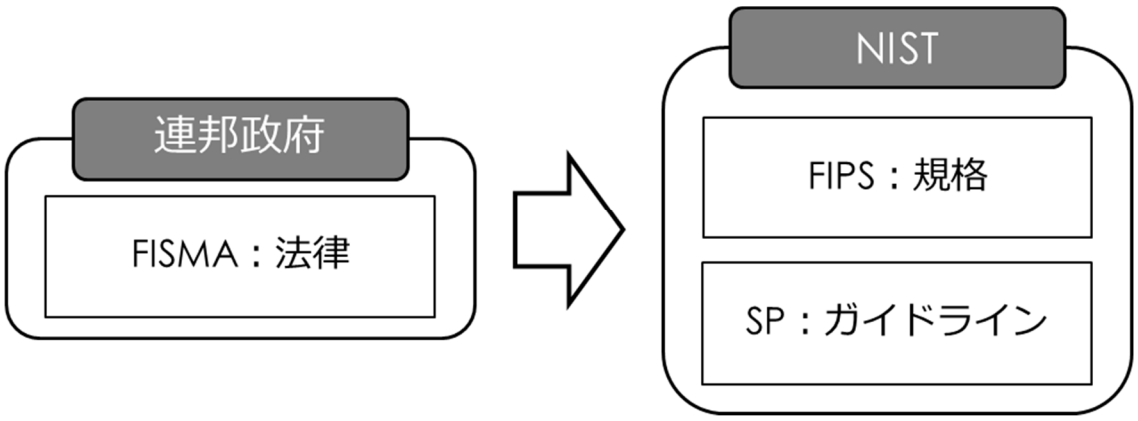
米国では国家レベルでの法的な体系が無いこともあり、プライバシーの保護に関する包括的な基準、規格、ガイドライン等も存在しない状態であった。唯一、連邦政府機関が IT 機器やシステムを導入する際の要求仕様である NIST SP800-53 に記載されているが、扱いとしては情報セキュリティ対策における追加的なものである。また、対象は政府機関であり、民間に対しても推奨されてはいるが、強制力としては中途半端な位置づけであることは否めない。そこで、重要な保護対象と位置づけるプライバシーに関する情報を拡大し、情報セキュリティ対策として包括的な対応を図る動きが急速に進み始めた。

情報セキュリティ対策については、2001 年の 9.11 同時多発テロ事件を機に法的な体系化が行われたが、行き過ぎた市民監視への反動から、プライバシー保護に関しても考慮されるようになってきている。そのため、この体系の中であらためて情報セキュリティ対策とプライバシー保護を両立させて整備することは、理にかなった流れと言えるだろう。

情報セキュリティ対策における法的根拠となるのは、2002 年に制定された連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002：FISMA[10]）である。これは連邦政府機関及びその委託先に情報セキュリティ対策を義務付けたものである。この中で、NIST に対しては情報セキュリティ対策のための規格やガイドラインの開発を義務付けている。

[10] 2002 年 12 月に大統領により署名された電子政府法（公法 107-347）のタイトル III
https://csrc.nist.gov/Projects/risk-management/detailed-overview

図表 1　米国の情報セキュリティ対策の体系



これを受けて、NIST は連邦政府機関が軍事以外の用途で購買・利用する情報・通信機器が満たすべき技術標準を定めた規格である連邦情報処理標準（Federal Information Processing Standards：FIPS）を策定し、さらにガイドラインとして Special Publications 800（SP800）のシリーズを発行している。

プライバシー保護に関連するものとしては、最低限のセキュリティ要求事項について、17 のセキュリティ関連分野にわたり規定した FIPS Publication 200[11]（連邦政府の情報、および連邦政府の情報システムに対する最低限のセキュリティ要求事項）がある。これに準拠するための具体的な指針を示す文書として発行されたのが、NIST SP 800-53 である。FIPS Publication 200 の公布にあたって、NIST SP 800-53 の最新版に記載されたセキュリティ管理策を導入することによって、本規格で規定された最低限のセキュリティ要求事項を満たさなければならないと明記されている。現在、最新のものは 2013 年 4 月に発行された NIST SP 800-53 Revision4[12]で、この中でプライバシー保護に関する管理策が示されている。

この体系とは別に、NIST ではサイバーセキュリティとプライバシーに関してフレームワークを策定している。2013 年 2 月、オバマ大統領が、重要インフラのサイバーセキュリティの強化に向けた大統領令（Executive Order）を発令し、これに則り NIST が 2014 年に公開したのが、重要インフラのサイバーセキュリティを向上させるためのフレームワーク（Cyber Security Framework：CSF）である。2018 年 4 月に発行された最新版 Version 1.1[13]

---

[11] 独立行政法人情報処理推進機構（IPA）による日本語訳：
https://www.ipa.go.jp/files/000025322.pdf

[12] 独立行政法人情報処理推進機構（IPA）による日本語訳：
https://www.ipa.go.jp/files/000056415.pdf

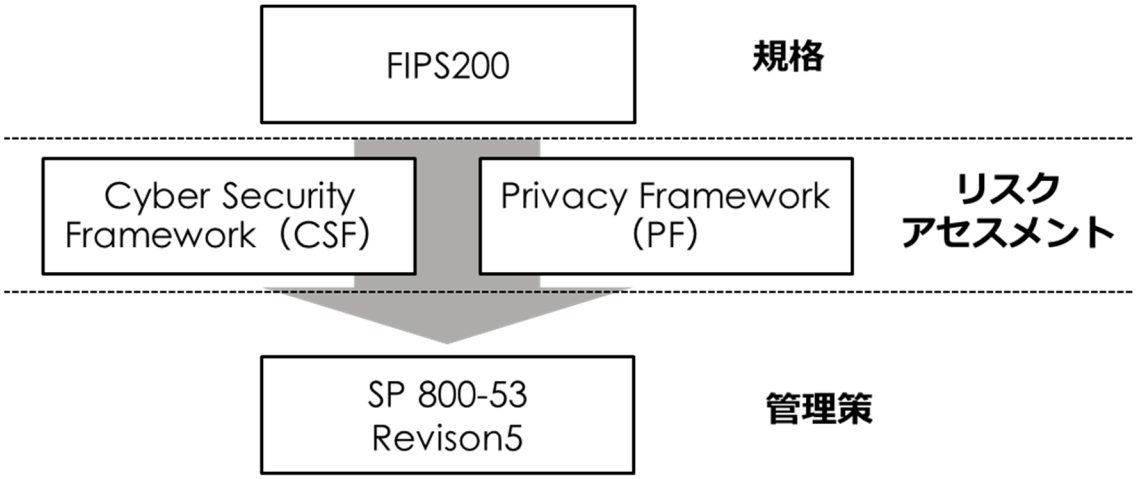
[13] 独立行政法人情報処理推進機構（IPA）による日本語訳：
https://www.ipa.go.jp/files/000071204.pdf

では、対象を重要インフラのみに限らず、業種や企業規模などに依存しない汎用的なものへと進化している。

NIST CSF はサイバーセキュリティに関するリスクアセスメント・ツールとしての位置づけであるが、プライバシーに特化したリスクアセスメント・ツールとして開発されたのが、2020 年 1 月に発行された Privacy Framework（PF）である。NIST PF は、CSF と対をなすものとして策定されており、それぞれの関係性や相違点についても記載されている。

この二つのフレームワークに対応し、管理策を統合すべく改訂が進められているのが SP 800-53 の最新版となる Revision5 であり、最終ドラフトのパブリックコメントが 2020 年 5 月に締め切られたところである。Revision5 では、プライバシーに関する管理策が本編に組み込まれており、また前述した FISMA や大統領令に端を発する法的体系から見ても、事実上、米国におけるプライバシー保護のリスク管理における標準としての位置づけになると考えられる。

図表 2　NIST の情報セキュリティ対策とプライバシー保護に関する統合の体系

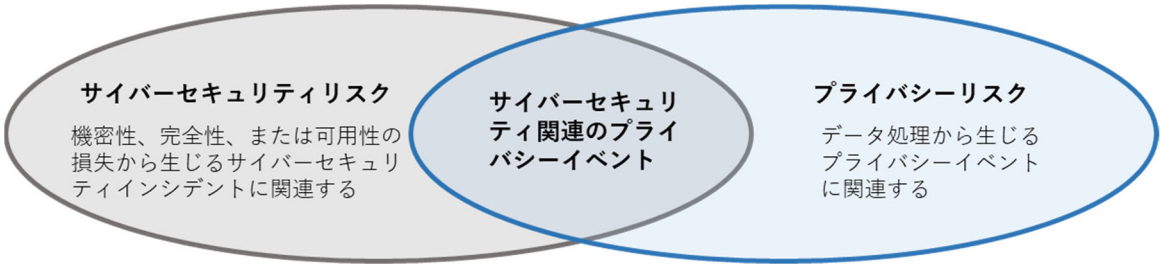


3.　NIST Privacy Framework

NIST CSF においても、プライバシーに関連する情報を保護すべき情報として位置付ける場合には、遵守すべき対応がまとめられている。しかしながら、あくまでもサイバー被害に対するものであって、それ以外のプライバシーについてのリスクは対象としていない。そのため、プライバシー保護の視点でリスクへの対応をまとめたものが NIST PF である。両方のフレームワークを参照することで、サイバーセキュリティだけではなく、プライバシーを含めたインシデント全般のリスクアセスメントが完成する。

いずれのフレームワークもリスクを特定しマネジメントすることを基本としていることから、それぞれのリスクの違いについて NIST PF で下記のように明確化している。

図表３　サイバーセキュリティリスクとプライバシーリスク



また、NIST PF においても NIST CSF と同様に Core(取るべき対策一覧)、Tier(成熟度評価指標)、Profile (現在のレベルと目指すべきレベル)という構造を取っており、フレームワークの親和性を高めている。

図表４　３つの要素

要素	機能	詳細
コア	特定	組織のプライバシーリスクの把握
	統制	組織のガバナンス構造の開発
	管理	適切なデータ管理の手法の開発
	通知	データ処理に関するコミュニケーション活動
	対応	プライバシー侵害の対応策
プロファイル	組織の現在のプライバシー活動または望ましい結果	コアの５つの機能にそれぞれ定義されたカテゴリ及びサブカテゴリに従い自己評価し、現状と目標を比較して改善策を特定する
ティア	組織のプライバシー対応の効果を評価する基準	ティア１：部分的な ティア２：リスク情報を生かした ティア３：反復可能な ティア４：適応性のある

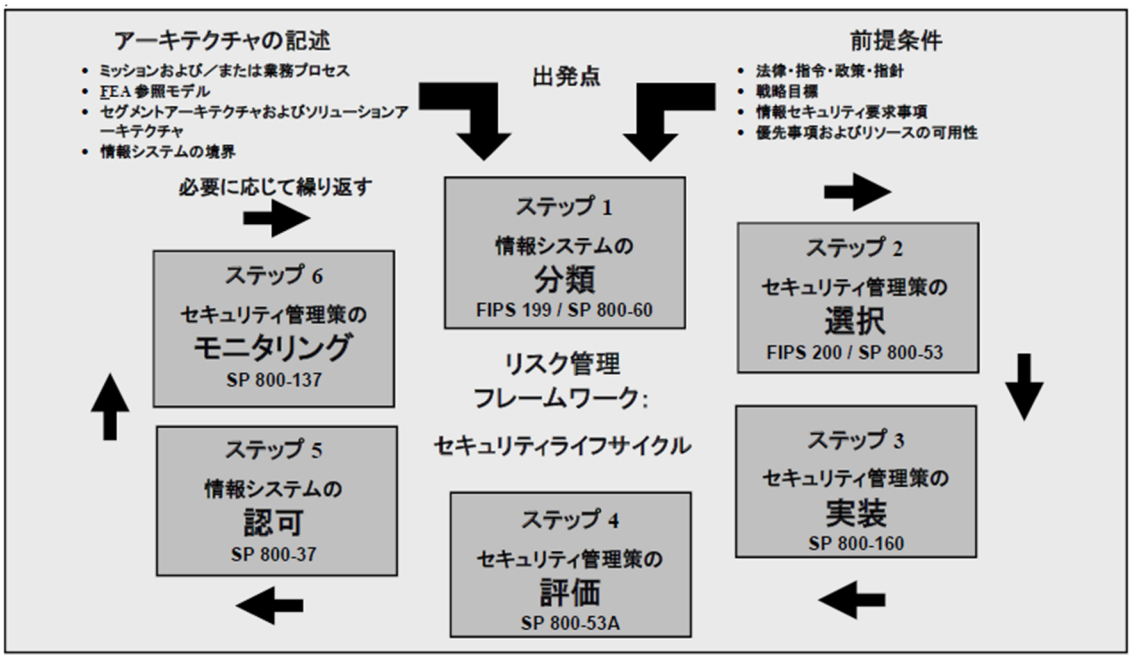
さらに、各フレームワークは補完し合うように構成されており、予防対策では NSIT PF は NIST CSF の一部を流用しつつ不足しているプライバシー保護観点の対策を大幅に補強、インシデント発生後の事後対策については NIST CSF を流用するようになっている。

4.　NIST SP 800-53 Rev5

現行の SP 800-53 Rev4 は 2013 年 4 月に発行されており、規格名は連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策 (Security and Privacy

Controls for Federal Information Systems and Organizations）である。情報システムの設計・開発・実装・運用・廃棄までの一連のライフサイクルの中におけるリスクマネジメントのフレームワークを規定した NIST SP800-37[14]（Risk Management Framework for Information Systems and Organizations）において、リスクマネジメントフレームワークの「ステップ 2 セキュリティ管理策の選択」に位置づけられている。

図表 54　リスクマネジメントフレームワークにおける SP 800-53 の位置づけ[15]



出典：連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策（IPA）

現在、改訂が進められており、最終ドラフト版のパブリックコメントが 5 月に締め切られ、年内には Revision 5 として発行される予定である。今回の改訂のインパクトは大きく、発行後 1 年以内の対応が望まれるとされていることから、米国では対応に向けた活発な動きがみられる。

---

[14] 独立行政法人情報処理推進機構（IPA）による日本語訳：
https://www.ipa.go.jp/files/000025329.pdf
2018 年 12 月に Revision2 に改訂
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[15] 連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策（IPA）

Rev5 における主要な変更点は以下となっている。

（対象）

・タイトルから「連邦（Federal)」という文言が削除され、公共部門と民間部門の両方の使用に適していることを明確にする。

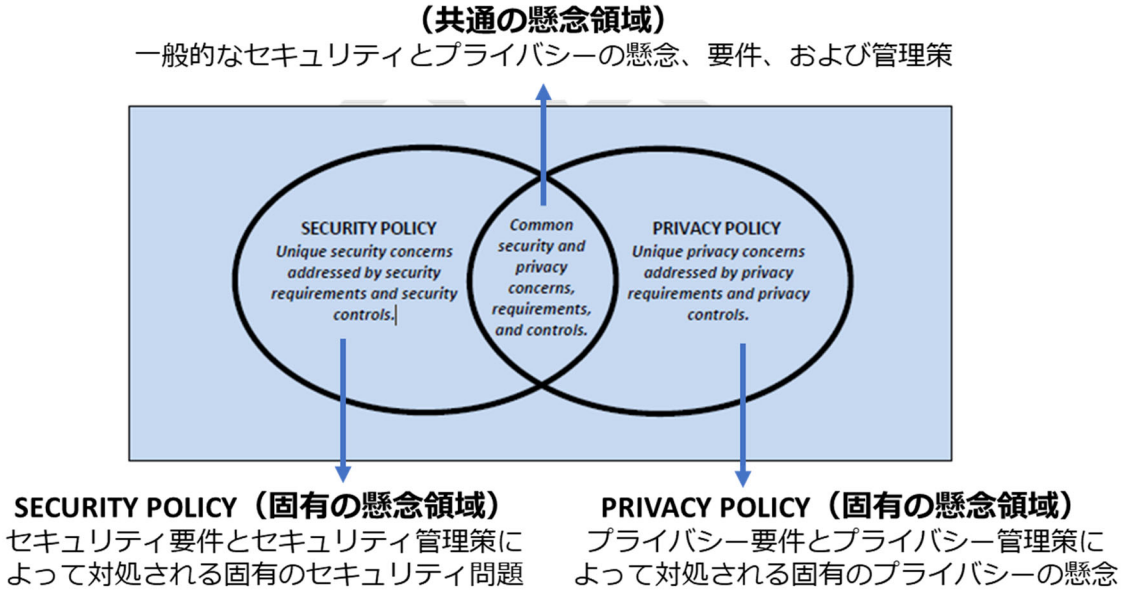
・情報システムという用語をシステムという用語に置き換え、汎用システム、サイバーフィジカルシステム、産業/プロセス制御システム、IoT デバイスなど、あらゆるタイプのシステムに適用できるようにする。

（管理策の統合）

・個別にまとめられていたプライバシー管理策とセキュリティ管理策を完全に統合し、システムと組織のための統一された管理策セットを作成する。

・セキュリティ管理策とプライバシー管理策の間を関連付ける共同管理策（joint control）という考え方を導入し、付録 E に関連付けを示す。

図表 6　管理策におけるセキュリティとプライバシーの関係



（構造の変更）

・管理策の選択プロセスを分離（SP 800-37 Rev2 へ移動)、また管理策ベースラインから管理策カタログを分離することで、関心のある様々な関係者（システムエンジニア、ソフトウェア開発者、エンタープライズアーキテクト、事業主等）が管理策を使用できるようにする。

・管理策の構造を変更することにより、セキュリティとプライバシーの管理策をより成果ベース（outcome base）にする。

（その他）

・NIST Cyber Security Framework および Privacy Framework を含む、さまざまなリスク管理およびサイバーセキュリティアプローチと辞書の連携を促進する。

また、我が国でも、年内に申請受付が始まる予定の政府のクラウドサービス調達の認証制度における「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：ISMAP）[16]」において、参考とする 8 つの国内外の基準等に SP 800-53 Rev4 が記載されている。ISMAP は日本版 FedRAMP[17]（Federal Risk and Authorization Management Program）とも言われており、米国の政府調達プログラムを強く意識したものである。その FedRAMP の認証基準が SP 800-53 であることから、今回の改定による日本への影響も小さくはないと考えられる。

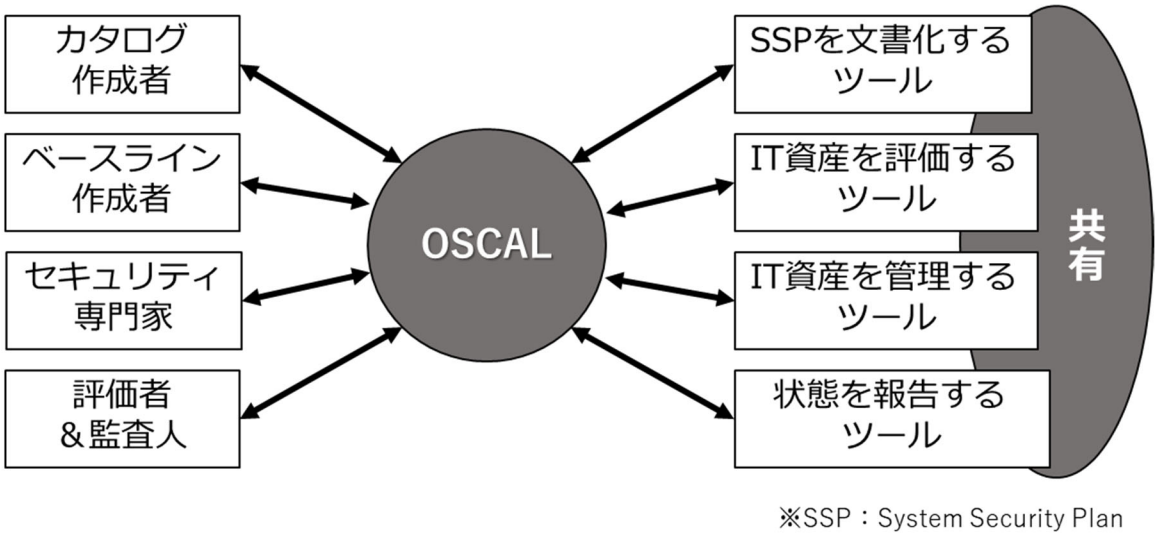
5. NIST OSCAL

セキュリティやプライバシーの管理について、文書化および評価するための標準化されたデータ中心のフレームワークとして開発が進められているのが OSCAL（Open Security Controls Assessment Language）で、XML および JSON で記述される共通、単一の機械可読言語である。そのゴールは、増加し複雑化し続ける多種多様なセキュリティやプライバシーの管理策について、これまでの個別のテキストやスプレッドシートによる手作業での選択、実装、評価を自動化することにある。また、それらのノウハウやレポートの共有を図り、評価に関する省力化、継続的な評価と複数の要件セットの同時評価の機能やシステムのタイプに影響を受けない一貫したパフォーマンスの実現を目指すとしている。

[16] https://www.ipa.go.jp/security/ismap/summary.html

[17] https://www.fedramp.gov/

図表 75　OSCAL のゴールとターゲット

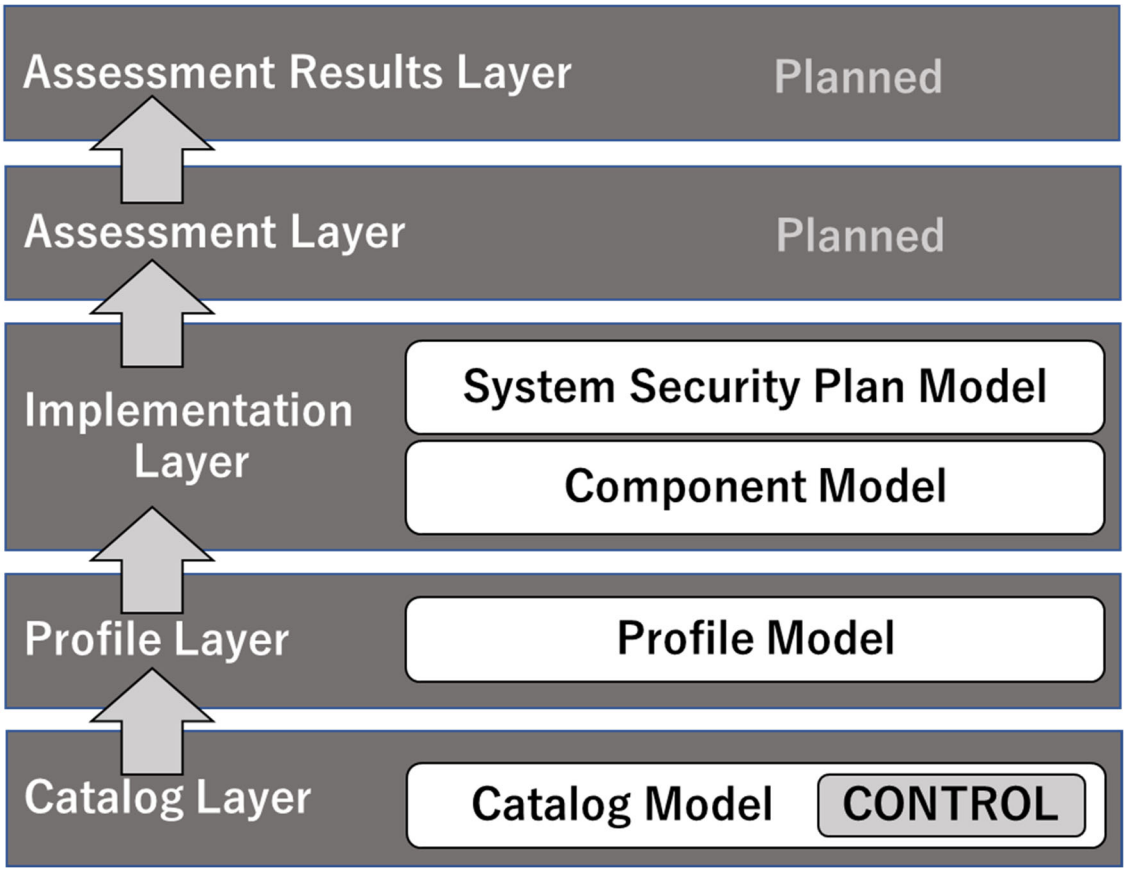


※SSP：System Security Plan

OSCAL の構造は、管理策のカタログレイヤーをベースに、プロファイル、実装のレイヤーが積み上げられ、開発も下位層から上位層へと順に進められている。まず、多種ある管理策のカタログを整備することで、すぐにでも OSCAL を導入できるようにし、上位層が開発されるに従い高機能になっていくという実戦的な開発手法になっている。

Version1.0 は、2020 年 7 月発行予定となっているが、この時点で含まれている管理策は、NIST SP 800-53、ISO/IEC 27001&27002、COBIT 5 が例示されている。この時点では評価や評価ルールレイヤーは含まれていない。しかしながら、管理策の選択から実装までが統一的な機械可読可能な方法で記録されていることから、上位層が開発されると同時に自動化された評価、監査が可能になると期待されている。

図表 8　OSCAL Layers and Models



6.　グローバルにおける米国のポジションと将来展望

米国に限らず、情報セキュリティ対策とプライバシー保護の統合は世界的な潮流となっており、国際標準化機構（International Organization for Standardization：ISO）においても、2019 年 8 月に ISO/IEC 27701 が発行されている。これは、情報セキュリティマネジメントの国際標準として普及している ISMS（Information Security Management System）の認証基準である ISO/IEC 27001 及び情報セキュリティ管理策の実践のための規範である ISO/IEC 27002 を拡張したものである。ISMS に加えて、個人情報の処理によって影響を受ける可能性のあるプライバシーを保護するための要求事項とガイドラインを規定したものである。つまり、ISMS と ISO/IEC 27701 の管理策をセットにすると SP 800-53 Rev5 と似たような構成になる。[18]

EU は一般データ保護規則（General Data Protection Regulation：GDPR）の制定により、データプライバシーに関する法制度の整備で世界を牽引しており、これに基づく認定・認証

[18] https://www.iso.org/standard/71670.html
（参考）https://isms.jp/topics/news/20200408.html

のシステムを開発することも表明しているが、具体的なプランはまだ発表されていない。規格の開発を主導するのは欧州ネットワーク・情報セキュリティ機関（European Network and Information Security Agency：ENISA）とみられており、2018 年 1 月にはデータプライバシーの保護の方法を情報セキュリティ対策の観点からまとめた Handbook on Security of Personal Data Processing[19]が発表しているが、具体的な管理策は含まれていない。ENISA だけではなく欧州データ保護会議（European Data Protection Board：EDPB）を始め様々な関係者は、新たな規格を開発するというよりも国際標準との親和性に重点を置いた規格の採用に言及している。先の ISO/IEC 27701 の開発に関しても EU の関与が大きかったことから ISO/IEC 27001、27002、27701 との関係性が強いものとなることが予想されている。

一方、NIST によって開発される規格は、世界をリードする米国の技術がビジネス化された際に起こる様々な新たな課題を反映していることから、最先端の規格と見なされる場合が多い。NIST CSF や NIST PF も ISO/27001 では規定されていないインシデントの検知や回復なども含まれており、よりカバー範囲が大きく、また最新の対策が含まれている。経済規模の大きさからくる対外的な影響も重なって、多くの国や企業が米国の規格を参考にしており、NIST CSF や SP 800-53 はグローバル・デファクト・スタンダードとなっている。さらに最近は、経済的な影響力が大きくなってきた新興国への対抗ともみられる国際標準化にも積極的で、ISO での提案が増えているが、その多くは NIST の規格をベースとしたものとなっている。

これらの動向を総合的に俯瞰すると、以下の潮流が認められる。

①プライバシー保護対策とサイバーセキュリティ対策の統合

②欧米においては国際標準規格に収斂する方向性が主流

③具体的な管理策等で先行する NIST の規格が国際標準を牽引する可能性

④認証システムの確立

さらに、④認証システムを確立させるためには、省力化や評価の均一化が重要になるが、NIST の OSCAL はこれを解決する有力な方法であり、完成度次第では今後のプライバシー保護対策とサイバーセキュリティ対策におけるソリューションの基盤となる可能性を秘めている。また、米国の精力的な活動は、これまでの EU 主導のプライバシー保護のフレームワーク構築に対するカウンターでもあり、EU による rule making から execute は米国主導へと移行していく兆候のようにも見える。

いずれにしろ、前述の 4 つの潮流は急速に顕在化している。例えば、ISMS プラス ISO/IEC 27701 の認証は、ISO による認証機関を定める認定基準の成立を待たずに、米国も含めて各国で始まっており、①②④が事実上始まっていると言える。さらに NIST では SP 800-53

[19] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Rev5 で国際標準以上の範囲をカバーし、OSCAL によって各規格を統一的に扱う機械可読化を進めることで、認証システムのビジネス化までが視野に入ってきている。

日本はプライバシー保護については、これまで EU の動向、特に GDPR やその派生ルールの動向に重きを置いて対応してきたが、ビジネスの関係性の大きさを考慮にいれると、今後は米国の動向にも注視する必要があるだろう。世界的に圧倒的なシェアを持つプラットフォーム事業者が、本国である米国において本格的なプライバシー保護を求められたことから、各国・地域別ではなくグローバルでの標準化を指向し始めた影響は大きい。最大規模の事業者と国家が協同して同一のゴールを目指すことになれば、メインストリームとなりうる可能性があるからだ。特に、各国・地域が拠り所としてさらに重視し始めた ISO における米国の動向を把握することは、極めて重要になる。

GDPR における十分性認定や APEC における CBPR に見られるように、プライバシー保護の政策は、すでに国内政策から国際的な土俵での重要課題へと移行している。プライバシーに関する理念が希薄な日本は、逆にこれを長所ととらえて各国の調整役として関与することで、公正・中立的に主導することが可能となるだろう。