積極的なデータ活用を見据えた『攻め』と『守り』のプライバシー

TMI総合法律事務所／PwC

NISTプライバシーフレームワークを日本企業はどう活用するべきか

米国国立標準技術研究所（NIST※1）は、企業・組織のプライバシーリスク管理を促進するため「NISTプライバシーフレームワーク」のバージョン1.0を2020年1月に正式公開しました。

今後、企業・組織がデータを利活用しながらサービス・製品などの拡充を進めるためには、プライバシー保護を考慮することは大前提となります。それゆえ、NISTプライバシーフレームワークをリスク管理のためのツールとして使用することは有用であると言えます。セキュリティ領域におけるデファクトスタンダードとなっている「NIST Cyber Security Framework」の姉妹版ということもあり、日本でも普及が想定されるNISTプライバシーフレームワークの意義や活用例を解説します。

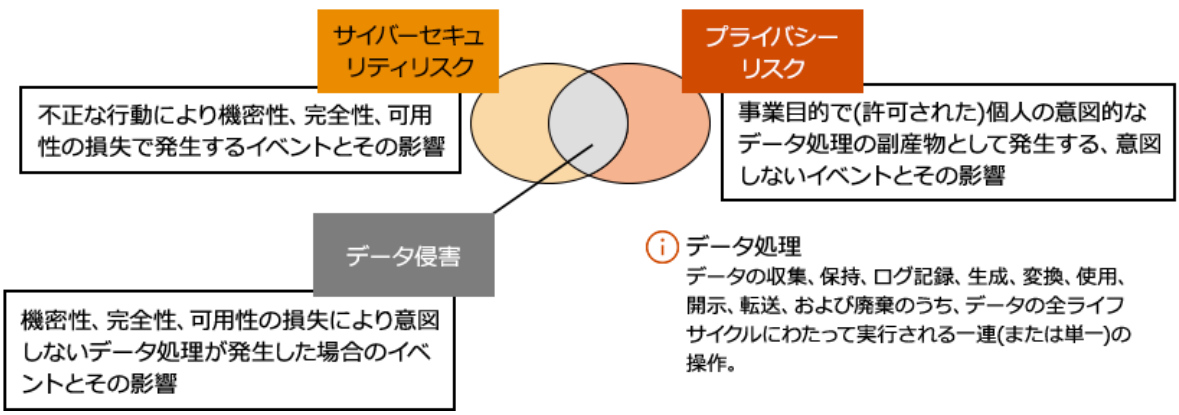
NISTプライバシーフレームワーク公開の背景

日本企業からの注目度が高かったEU一般データ保護規則（GDPR）においては、2019年より、プライバシー保護違反などを理由に数百億円レベルの制裁金が企業に課される事例が増えています。またGDPRの施行に前後して、各国でGDPRに似た規制が次々に法制化、施行されています。日本では、2020年3月に個人情報保護法改正案が閣議決定され、今後、企業の責任が厳格化される見込みです。

また、インターネット上の言論の自由を尊重している米国であっても、ソーシャル・ネットワーキング・サービス（SNS）事業者からの個人情報漏えいを契機にしてプライバシーリスク管理への注目は高まっており、州ごとにプライバシー規制が施行・検討され始めています。現在、連邦政府による米国全土をカバーした連邦法上のプライバシー規制法は無いため、米国でビジネスを展開する企業は州ごとの規制に対応する必要があり、それゆえ、かなり煩雑な運用が求められています。そこで、NISTは2020年1月にプライバシーフレームワークを公開し、個人のプライバシー保護のために各企業・組織が遵守すべきベースラインの設計をしやすくしたのです。

参考URL：「第23回世界CEO意識調査」デジタルトラスト編 ― 日本のCEOに求められるデジタルトラストの姿勢

図表1：プライバシーリスクの位置づけ



※1 NIST:National Institute of Standards and Technology
（米国国立標準技術研究所）

NISTプライバシーフレームワークの概要

NISTプライバシーフレームワークの目的

まず、NISTプライバシーフレームワークの目的から見てみましょう。このフレームワークは、以下の3つを目的に策定されました。

- 製品やサービスなどの設計や開発において、プライバシー保護の合理的な説明責任を果たすこと
- プライバシー保護活動の情報発信やコミュニケーションをしやすくすること
- 評価結果をもとに経営層、法務部門、IT部門などの間で、部門横断的なコラボレーションを実現できること

NISTプライバシーフレームワークの構成

次に、NISTプライバシーフレームワークの構成を見てみましょう。このフレームワークは「(1)Core(コア)」、「(2)Profile(プロファイル)」、「(3)Tier(ティア)」という3つの要素から構成されています。

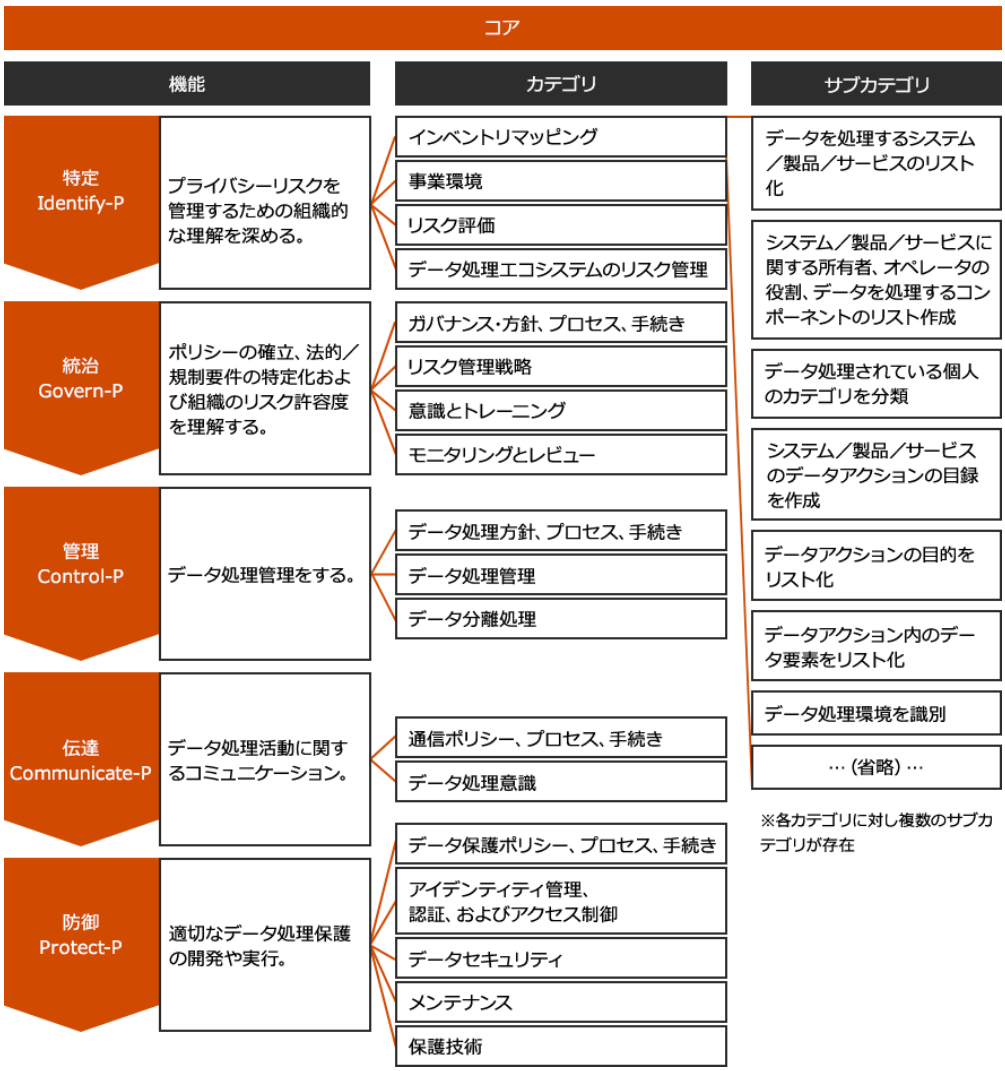
図表2:NISTプライバシーフレームワークを構成する3つの要素

NISTプライバシーフレームワーク	
① Core (コア)	プライバシーリスク管理への要求事項一覧。一連のアクションとして5つの「機能」に分類され、定義される。
② Profile (プロファイル)	プライバシーリスクを優先順位付けして管理するための分析結果(カテゴリ、サブカテゴリに分かれる)。
③ Tier (ティア)	組織のプライバシーリスクへの対策レベルを評価するための指標。(4段階)

（1）Core（コア）

コアはプライバシーリスク管理に係る要求事項一覧です。「機能」、「カテゴリ」、「サブカテゴリ」から構成され、各機能は複数のカテゴリへ、各カテゴリは複数のサブカテゴリへと細分化されます。コアの定義により経営層から実務層までが、プライバシー保護のための対応や優先事項を共通言語で理解・議論し、リスク管理できるようになります。

図表3：Core（コア）の構成要素



【機能】プライバシーリスクを管理するための一連のアクションで、5つに分類されます。

- 「Identify-P（特定-P）」：データ処理により発生する個人のプライバシーリスクを管理するために、組織的な理解を深めます。
- 「Govern-P（統治-P）」：プライバシーリスクの優先順位を理解するために、ガバナンス構造を開発し、実装します。
- 「Control-P（管理-P）」：組織／個人がプライバシーリスクを十分な精度で管理できるように、適切な活動を展開します。
- 「Communicate-P（伝達-P）」：組織／個人がデータの処理方法や関連するプライバシーリスクについて理解し、対話できるように適切な活動を展開します。
- 「Protect-P（防御-P）」：データ処理のセーフガードを開発し、実装します。

【カテゴリ】機能を課題や特定の対応にもとづき細分化・グループ化した成果を示します。

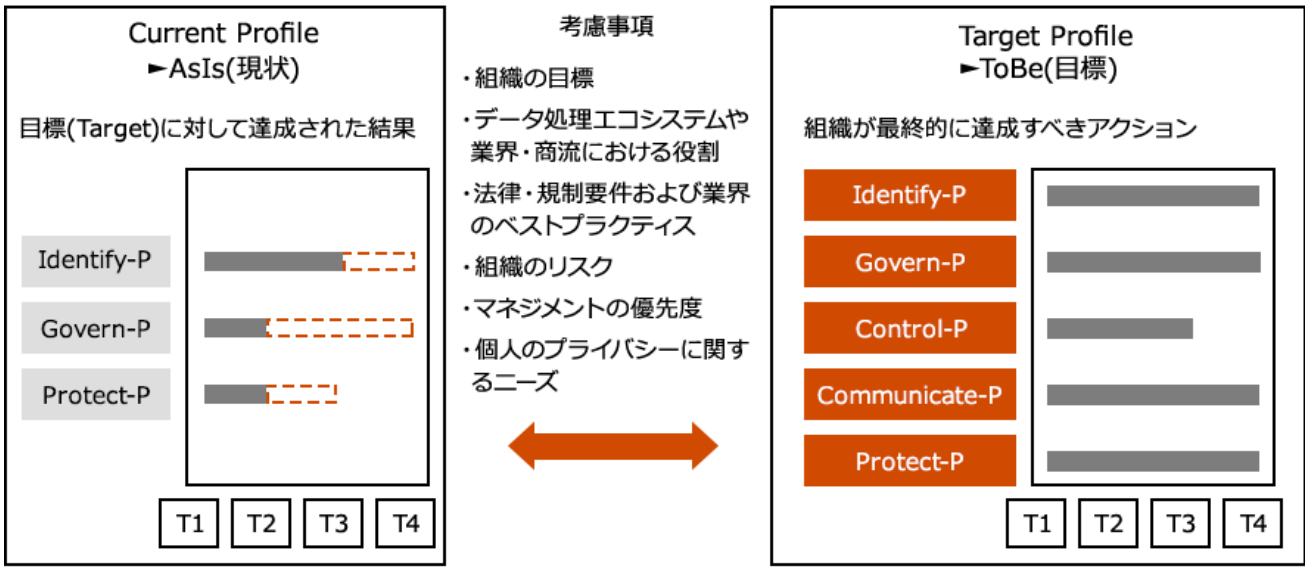
【サブカテゴリ】カテゴリを技術的／管理的対応にもとづき細分化した成果を示します。

(2)Profile(プロファイル)

任意のアクションを企業・組織のニーズに応じてコアから選択し、作成します。テンプレートは用意されておらず、各組織は特定の機能・カテゴリ・サブカテゴリを組み合わせて独自のプロファイルを設定します。組織や役割が個人データのエコシステムのどの領域に属していても、業界・部門・役職などに沿った設定をすることで、適切なプライバシー保護が実現できるように設計されています。

プロファイルは、組織のビジネス要件、リスク許容度。プライバシーバリュー、リソースを総合的に鑑みた上で構築された指標と言え、組織がプライバシーリスクを優先付けして管理するために有効です。

図表4:プロファイルの例



(3)Tier(ティア)

企業・組織のプライバシーリスク管理レベルを定量的に評価する指標。Tier 1(T1)からTier 4(T4)の4段階に定義されており、階層が高くなればなるほど、より多面的なリスク管理が求められます。

- Tier 1:部分的
- Tier 2:リスクを把握済み
- Tier 3:繰り返し適用可能
- Tier 4:適応している

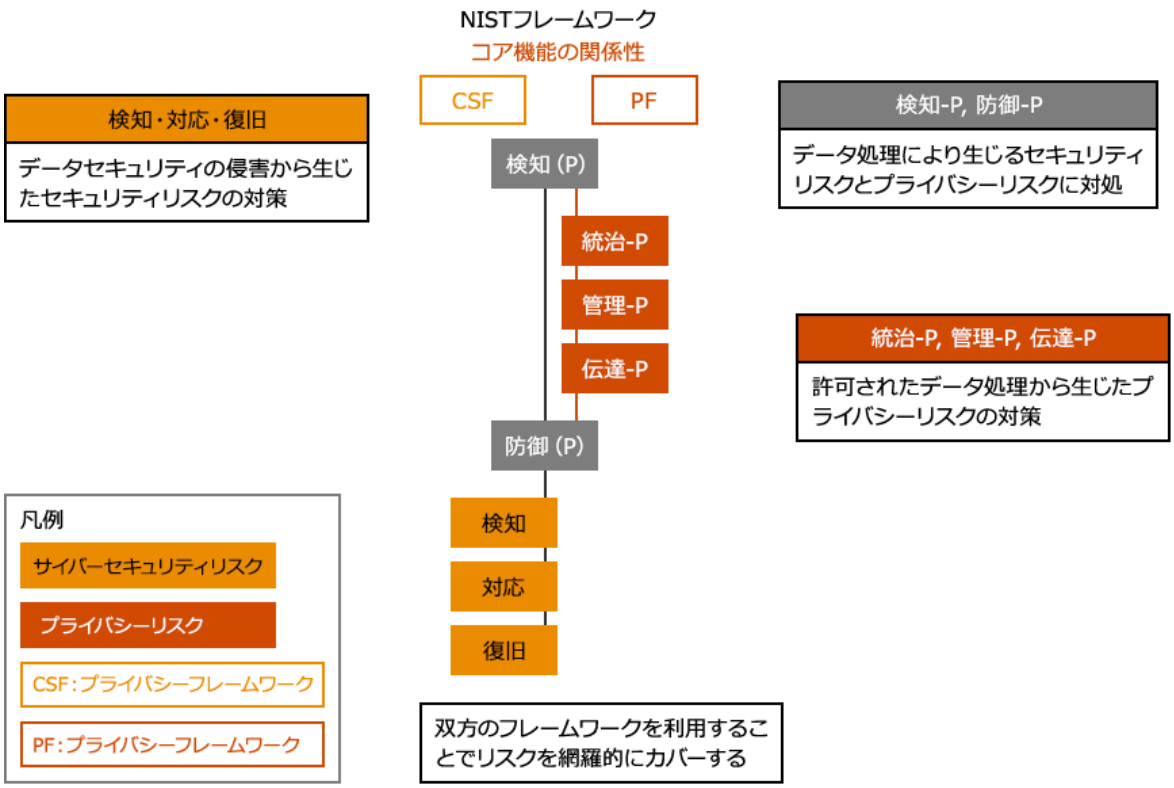
各サブカテゴリについて望ましい状態を達成しているか、達成している場合はどの程度であるのかというアセスメントを行い、また目標とする達成状況を設定することで現状とのギャップが可視化され、今後の改善プラン策定に利用することが可能になります。

図表5:プライバシーリスク管理のフェーズごとに見るTier (ティア) の例

サイバーセキュリティフレームワーク（CSF）との併用が効果的

NISTプライバシーフレームワークの特長として、セキュリティ領域におけるデファクトスタンダードであるNISTサイバーセキュリティフレームワーク（CSF）と併用できる点が挙げられます。同フレームワークは、サイバーセキュリティリスクを管理する上で有用な機能を5つに分類したCSFと互換性のある構成となっています。双方を同時に活用してサイバーセキュリティリスクとプライバシーリスクを網羅的に管理することが望ましいと言えます。

図表6：NISTフレームワークとサイバーセキュリティフレームワークのコア機能の関係性



NISTプライバシーフレームワークの活用例

今後、企業・組織がデータを利活用し、サービス・製品などの拡充をするためには、プライバシーリスクを適切に管理していく必要があることは明白です。以下に、プライバシー保護の目標レベルを達成するためのNISTプライバシーフレームワークの活用例を紹介します（図表7）。例えば、新規にプライバシー保護の仕組みの構築を検討している組織であれば、上記で紹介したようなカテゴリやサブカテゴリが有効でしょう。また、既にプライバシーリスク管理の仕組みがある組織であれば、目標と現状とのギャップ分析に使用することができるでしょう。

図表7：NISTプライバシーフレームワークの活用例

想定企業	大手家電メーカー（従業員3000人規模）
課題	国内外にある多数の個人情報関連法規制への対応

現状（As Is）

既にプライバシー保護に関するガバナンス体制は構築済み

あるべき姿（To Be）

さまざまな法規制で要求される「データ分離処理※」を組織全体で実装すること

※Disassociated Processing (CT.DP-P)

NISTプライバシーフレームワークの導入

NISTプライバシーフレームワーク導入プロセス

- ・初めに、組織のミッション、法的要件、プライバシーリスク、リスク許容度を理解する。
- ・その後、データ収集ポイントの整理、データアクションのリスト化、データマップの作成などを実施する。

NISTプライバシーフレームワークによる効果

- ・顧客への説明責任能力の向上
  プライバシー保護やデータ主体の権利に関する組織の対策について顧客に合理的に示すことが可
- ・スムーズなコンプライアンスの遵守
  フレームワークに従って作成された文書類は、プライバシー監査の有効な証跡として使用可能。

日本企業への示唆

まず多くの日本企業では、プライバシー保護を「法務・コンプライアンス部門」が、サイバーセキュリティを「ITセキュリティ部門」が主管しています。この2つの部門は、同じ企業・組織内であっても業務カルチャーや使用する用語が異なり、部門間の壁が少なからず存在するケースが少なくありません。しかし、デジタルトランスフォーメーション（DX）は世界的に急激なスピードで進んでおり、テクノロジーの活用なしにビジネスを成功させることは、もはや考えづらい状況です。日本企業がデジタル社会で業界をリードしていくためには、プライバシー保護とサイバーセキュリティの部門横断的なコラボレーションが不可欠です。

NISTプライバシーフレームワークは、そうしたコラボレーションを目的の一つとして策定されているため、これを活用することで、法務・コンプライアンス部門やITセキュリティ部門、さらには経営層が共通の言語で議論をしやすくなるでしょう。その結果、ビジネスにおけるリスク認識の共有と対策の優先順位付けを促進することも可能になります。

同フレームワークにはもう一つの目的があります。企業が製品／サービスなどを設計・開発する際にプライバシーを適切に保護していることを、顧客・取引先企業、消費者に対して合理的に説明可能にすることです。例えば、データの削除要求があった場合に実行可能な機能を備えている（「CT.DM-P4」）ことや、データのライフサイクル終了と共にデータを適切に破棄するプロセスが実装されている（「CT.DM-P5」）ことは、NISTプライバシーフレームワークを利用すれば共通言語として説明可能になります。このような理由から、DXを目指す日本の企業・組織は、NISTプライバシーフレームワークの活用を検討するべきだと考えます。

監修・執筆

大井 哲也

TMI総合法律事務所
TMIセキュリティ&プライバシー株式会社
弁護士

執筆

上杉 謙二

PwCコンサルティング
合同会社
シニアマネージャー

監修

平岩 久人

PwCあらた有限責任監査
法人
ディレクター

TMI総合法律事務所
http://www.tmi.gr.jp/

TMIセキュリティ&プライバシー株式会社
https://tmiconsulting.co.jp/

PwC Privacy
https://www.pwc.com/jp/ja/services/digital-trust/privacy.html

TMI PRIVACY AND SECURITY

pwc