

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。

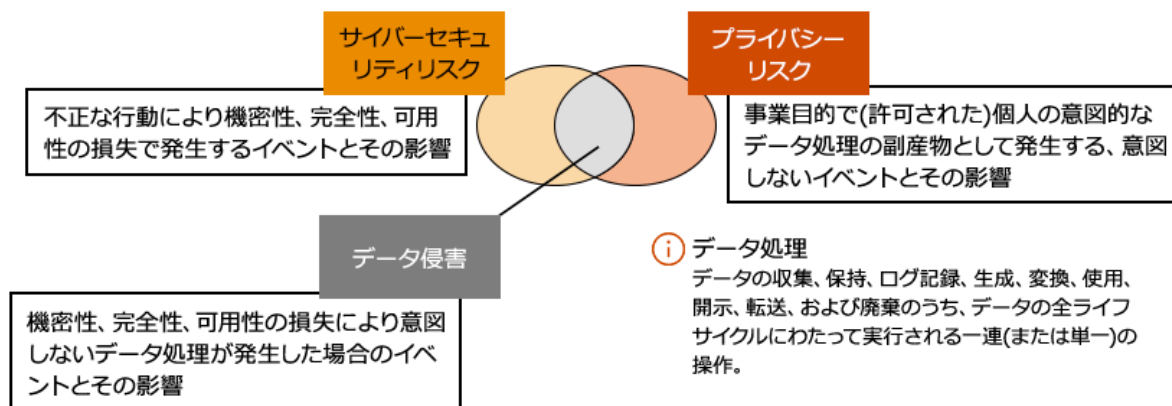
NISTプライバシーフレームワーク公開の背景

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



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

コア				
機能		カテゴリ		サブカテゴリ
特定 Identify-P	プライバシーリスクを管理するための組織的な理解を深める。	インベントリマッピング		データを処理するシステム／製品／サービスのリスト化
		事業環境		システム／製品／サービスに関する所有者、オペレータの役割、データを処理するコンポーネントのリスト作成
		リスク評価		データ処理されている個人のカテゴリを分類
		データ処理エコシステムのリスク管理		システム／製品／サービスのデータアクションの目録を作成
統治 Govern-P	ポリシーの確立、法的／規制要件の特定化および組織のリスク許容度を理解する。	ガバナンス・方針、プロセス、手続き		データ処理されている個人のカテゴリを分類
		リスク管理戦略		システム／製品／サービスのデータアクションの目録を作成
		意識とトレーニング		データ処理されている個人のカテゴリを分類
		モニタリングとレビュー		システム／製品／サービスのデータアクションの目録を作成
管理 Control-P	データ処理管理をする。	データ処理方針、プロセス、手続き		データアクションの目的をリスト化
		データ処理管理		データアクション内のデータ要素をリスト化
		データ分離処理		データ処理環境を識別
伝達 Communicate-P	データ処理活動に関するコミュニケーション。	通信ポリシー、プロセス、手続き		データ処理環境を識別
		データ処理意識		… (省略) …
防御 Protect-P	適切なデータ処理保護の開発や実行。	データ保護ポリシー、プロセス、手続き		※各カテゴリに対し複数のサブカテゴリが存在
		アイデンティティ管理、認証、およびアクセス制御		
		データセキュリティ		
		メンテナンス		
		保護技術		

※各カテゴリに対し複数のサブカテゴリが存在

【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。

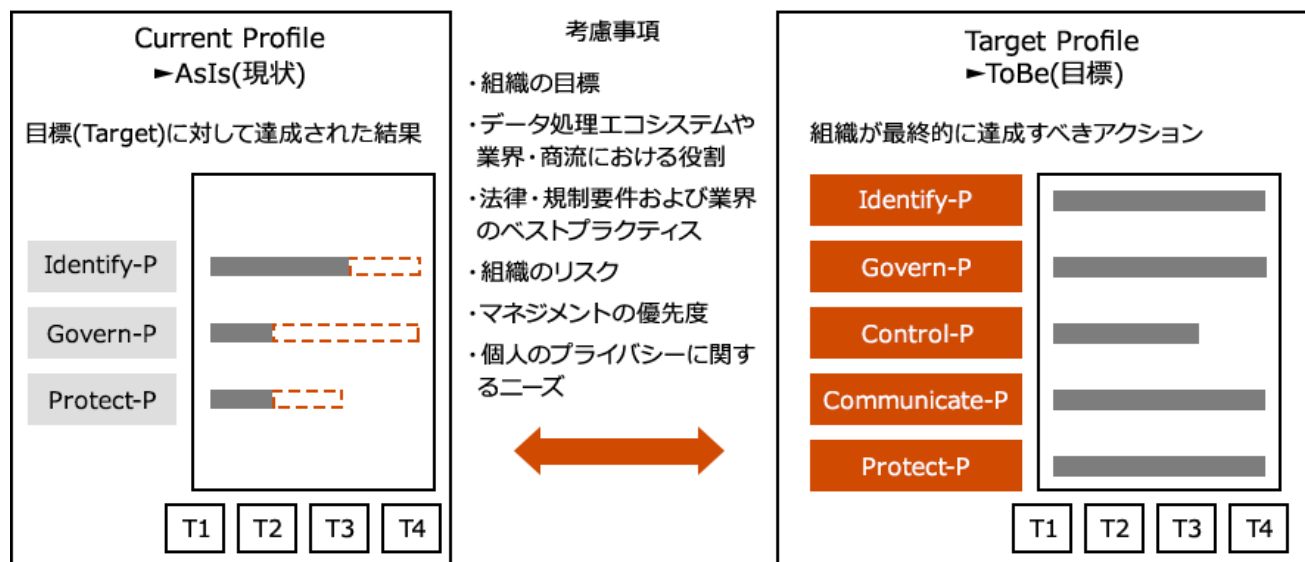


(2) Profile(プロフィール)

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ることで独自のプロフィールを設定します。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。

プロフィールは、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ます、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。

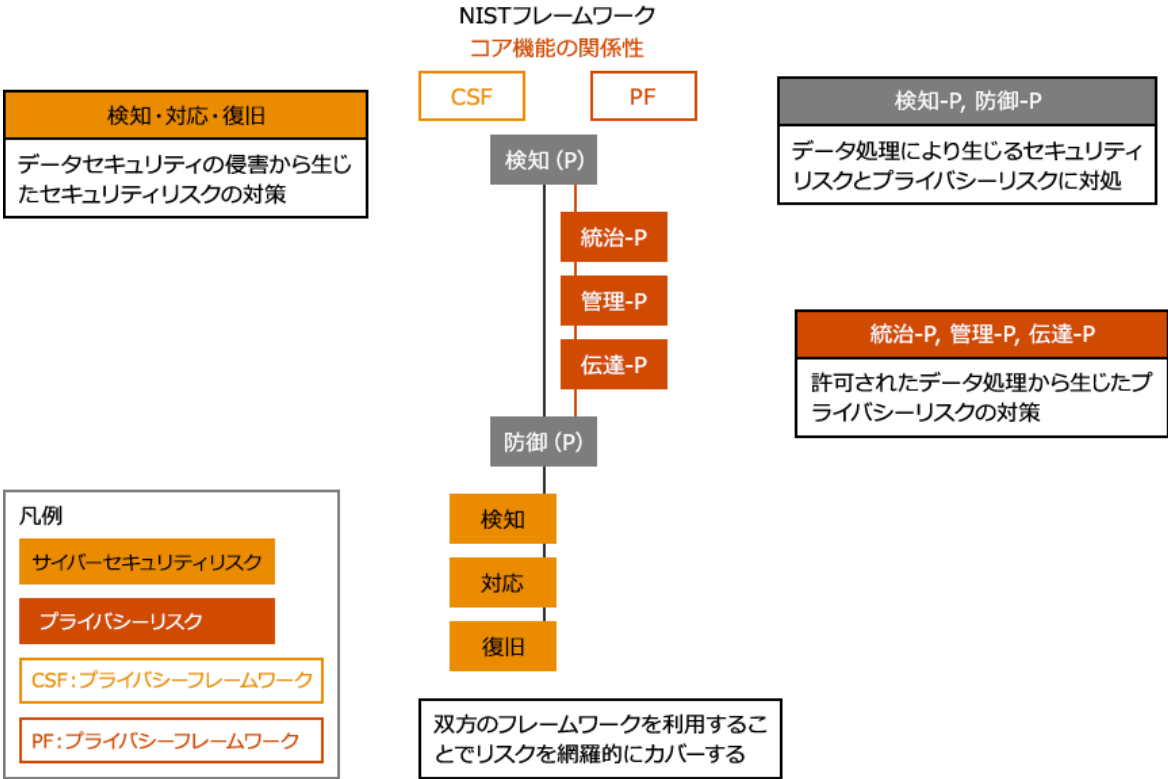
図表5: プライバシーリスク管理のフェーズごとに見るTier (ティア) の例

Tier4 適応している	経営の意向を 即時反映	経営視点から ブレイク、 発展・改善	最新情報を 反映して対応	全社員へ浸透& 高いスキルの人 材配置
Tier3 繰り返し適用可能	経営の意向に 従って運用	網羅的に整備、 運用	書面合意に もとづき対応	全社員への 教育&網羅的 に人材配置
Tier2 リスクを把握済み	経営意向が 確立	リスクを把握 し部分運用	契約外で部分 的に対応	特定業務に対 して教育、人材 配置
Tier1 部分的	統制が取れて いない	現場判断での アドホック	ほぼ未対応	教育・人材 が実践レベル にない
	<u>経営プロセス</u>	<u>リスク管理</u>	<u>ステークホルダー 管理</u>	<u>ヒューマンスキル</u>

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。

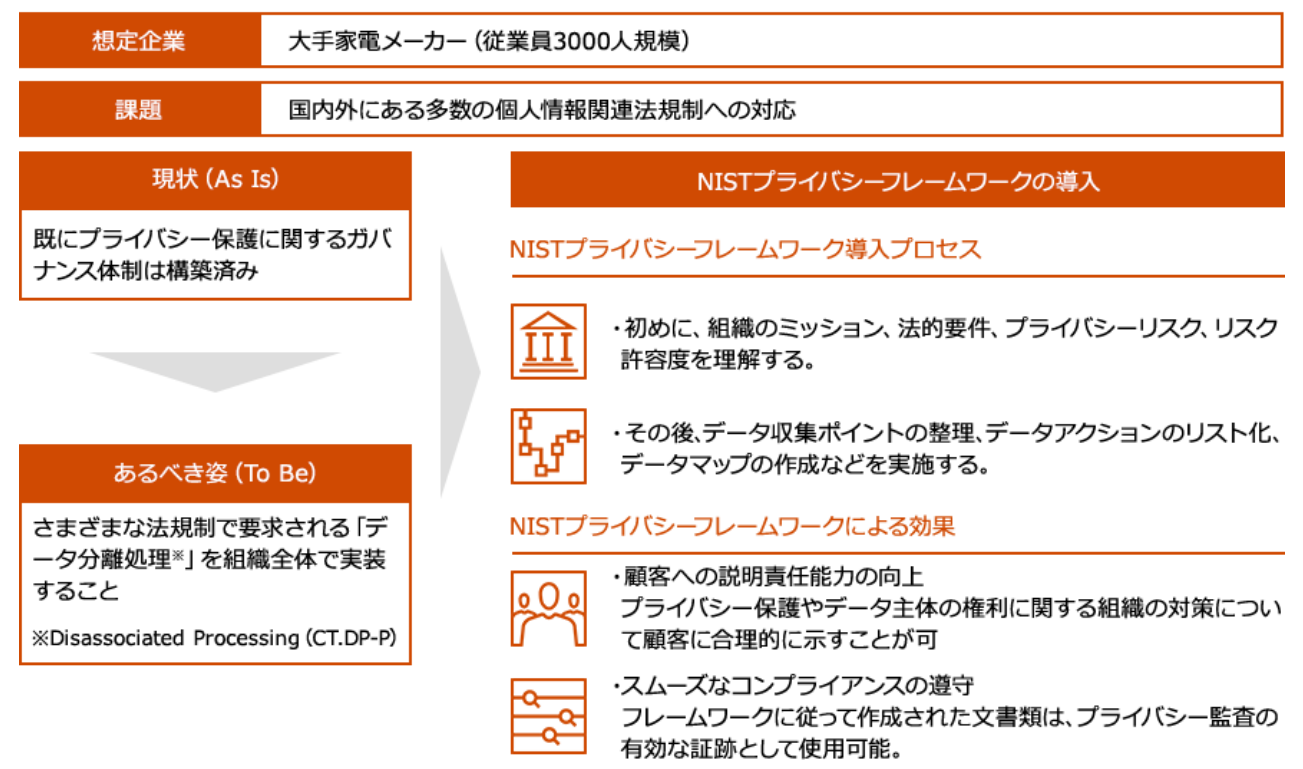
図表6：NISTフレームワークとサイバーセキュリティフレームワークのコア機能の関係性



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



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

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



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>



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8,100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築き、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157カ国に及ぶグローバルネットワークに276,000人以上のスタッフを有し、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。

© 2020 PwC. All rights reserved. PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.