# NIST CSFとの併用で効果を最大化するフレームワーク～NIST プライバシーフレームワークの活用方法～

2020年02月18日

コンサルタント

[星野 靖](https://www.newton-consulting.co.jp/company/hoshino.html)



デジタルトランスフォーメーション、略してDXがホットワードになっており、企業はデジタル、データでビジネスを変革する必要に迫られています。既にこれによりデジタルビジネスの成功を収めた企業も出てきており、今後もこの流れがしばらく続きそうです。

一方、近年ではIT技術の急速な成長に法規制が追い付いておらず、プライバシー侵害が問題になるケースも多く見受けられました。



そんな中、エポックメーキングな出来事となったのが、2018年5月のGDPR (EU一般データ保護規則)の施行です。以降、プライバシー侵害に高額な制裁金が科されるようになり、カリフォルニア州消費者プライバシー法(CCPA)発効等、各国もGDPRに追随するようになってきました。ISO27701:2019のような統一規格も出てきています。つまり、データを攻めに活用する際、適切な管理を求められるようになってきたということです。

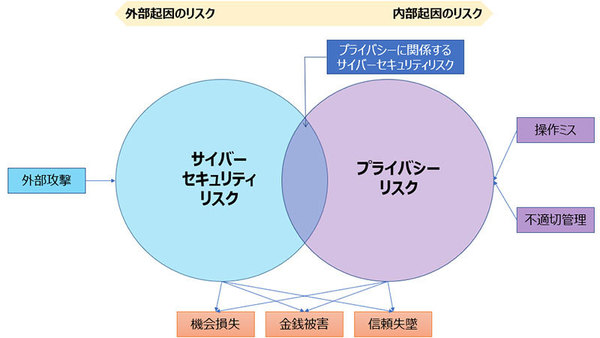
この流れの中、2020年1月16日に米国国立標準技術研究所(NIST)がプライバシーフレームワーク 1.0 (以下、NIST PF)を策定しました。NIST PFは法規制でも認証でもない参考とすべきフレームワークという位置づけであり、必須で遵守すべきものではないのですが、NIST サイバーセキュリティフレームワーク(NIST CSF)のように、世界中で参考にされることが見込まれます。

**NIST PFとは**

では、NIST PFはどんなものか、これはプライバシー保護視点で遵守すべき対応をまとめたものです。NIST CSFではサイバーセキュリティレベル向上に繋がる対応をまとめており、プライバシー保護に貢献している側面はあるものの、サイバー被害が原因ではないプライバシー問題はカバーできていませんでした。そこで、これをカバーするためにNIST PFが策定されました。そのため、どちらか単独で使用しても効果はありますが、両方を組み合わせて使うことがより効果的です。  
また、このフレームワークは特定の業種、組織規模の大小、特定の技術や法規制等は問わない汎用的な内容となっており、以下のような効果が期待されます。

* プライバシーを考慮した設計を行い、それをシステムや製品、サービスに実装することができる
* プライバシー対応について、対外的に取組み状況を発信できる
* プライバシー対応を改善することで、組織を横断した形でデータ活用を促進できる

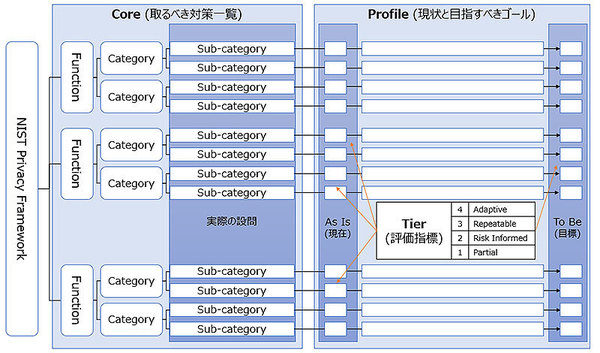
【図表 1: サイバーセキュリティリスクとプライバシーリスクの関係性】



**NIST PFの構成要素**

NIST PFはCSF同様、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)などの要素で構成されています。つまり、取るべき対策を評価して現状把握し、目指すべきレベルを設定、そこに近づくための対策を決定、遂行するという手順で活用します。

【図表 2: Core, Tier, Profileの関係性】



**Coreと機能**

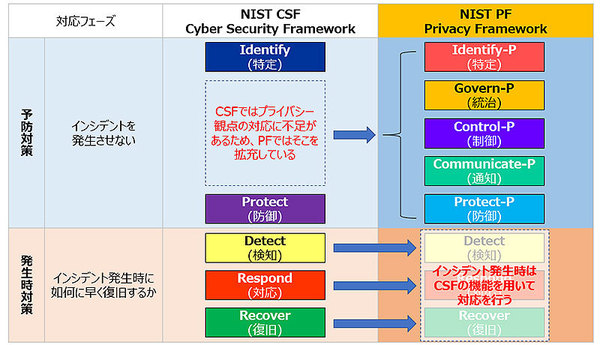
先行するNIST CSFではCoreを特定(Identify)、防御(Protect)、検知(Detect)、対応(Respond)、復旧(Recover)の5つの機能に分けて、予防対策だけでなく、事後対策についても言及しているのが画期的でした。

NIST PFでは、Coreを特定(Identify-P)、統治(Govern-P)、制御(Control-P)、通知(Communicate-P)、防御(Protect-P)の5つに分類しています。

| 【図表 3: フレームワークの機能とリスク種類の関係性】 | | | | | |
| --- | --- | --- | --- | --- | --- |
| **フレームワークと機能** | | | **リスク種類** | | |
| **サイバーセキュリティ リスク** | **サイバーセキュリティリスク であり、かつ プライバシーリスク** | **プライバシーリスク** |
| **CSF** | **Identify** | **特定** | ○ |  |  |
| **Protect** | **防御** | ○ |  |  |
| **Detect** | **検知** | ○ | ○ |  |
| **Respond** | **対応** | ○ | ○ |  |
| **Recover** | **復旧** | ○ | ○ |  |
| **PF** | **Identify-P** | **特定** |  |  | ○ |
| **Govern-P** | **統治** |  |  | ○ |
| **Control-P** | **制御** |  |  | ○ |
| **Communicate-P** | **通知** |  |  | ○ |
| **Protect-P** | **防御** |  | ○ |  |

一見、NIST CSFとPFでは機能が重複しているようにも見えるのですが、実はこの2つを上手く整合して活用できるように考えられています。

【図表 4: 各フレームワーク機能の関係性】

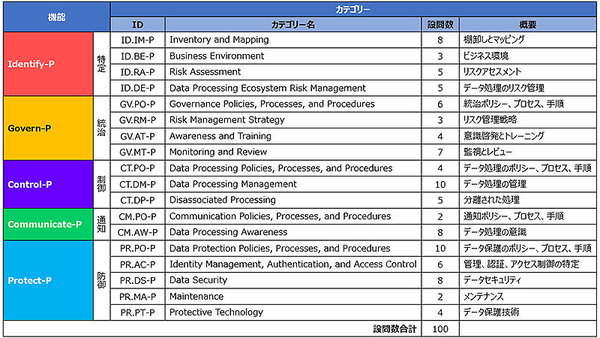


予防対策ではPFはCSFの一部を流用し、CSFに不足しているプライバシー観点の対策を補強しています。また、インシデント発生後の事後対策についてはCSFを流用するように誘導しています。そのため、プライバシー対応のフレームワークとして活用する場合、PFを単独で使うのではなく、CSFとPFを組み合わせて使った方が良いでしょう。

**Core(取るべき対策一覧)の詳細**

Coreでは先に述べた機能5個を大項目と考えた場合、中項目(カテゴリー)が18個、小項目(サブカテゴリー、これが確認すべき設問となる)がちょうど100個(100問)になります。

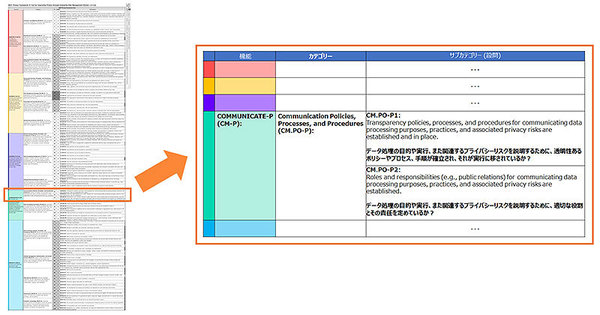
【図表 5: Core機能の詳細】



これら100問に回答していくことでプライバシー対応の現状を把握することが可能となります。設問はそれなりに具体的であり、日本の企業で言うなら、管理職と現場の両方がわかるような立場、課長級の方が回答するのが早そうです。

ただし、Tierが低レベルであれば、現場の対応を改善すればレベルアップが可能ですが、高レベルになるほど、プライバシー対応のポリシー策定や全社で一貫した施策実施等、全社的な対応が必要となるため、全社的な支援、経営層の協力が必要となってきます。

【図表 6: PF Coreの全容と設問例】



**Tier(成熟度評価指標)の詳細**

Coreで細分化された100の設問に回答していくことで評価を進めていくのは先に述べたとおりですが、各設問はTierと呼ばれる成熟度を以って評価していきます。Tierで用意されている成熟度は4段階で、Tier1はPartial(部分的に対応できている)、Tier2はRisk Informed(リスクが認識できている)、Tier3はRepeatable(対応に再現性がある)、Tier4はAdaptive(変化に適応できる)です。つまり、Tier1がもっとも低レベル、Tier4がもっとも高レベルとなります。  
もちろん、評価するにあたってはもう少し判断材料が必要であり、PFでは4つの観点でどのような状態が該当するかを示しています。

* Privacy Risk Management Process (プライバシーリスクの管理プロセス)
* Integrated Privacy Risk Management Program (統合されたプライバシーリスク管理)
* Data Processing Ecosystem Relationships (データ処理システムの関係性)
* Workforce (対応人員)

それぞれの観点で評価した場合、Tier4だったり、Tier2だったりと評価が割れる可能性が考えられますが、設問中の観点で最も厳しい評価を採用するのが良いでしょう。

| 【図表 7: Tierと評価の観点】 | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Tier** | **評価の概要** | **評価の観点** | | | |
| **プライバシーリスクの 管理プロセス** | **統合されたプライバシー リスク管理** | **データ処理システムの 関係性** | **対応要員** |
| **4** | **Adaptive 変化に適応できる** | プライバシーに関わる事例や新たにでてきたリスクを対応手順に反映し、プライバシーに関わる対応を継続的に改善している。 | プライバシーリスクを他の経営リスクと同種と捉え、ポリシー、プロセス、手順におけるリスクを組織レベルで認識し、管理している。 | 大規模なデータ処理システムで自分たちが果たす役割、依存関係等を認識しており、リスクが表面化する際には即座に関係者に通知している。 | 専門性を持った人員がプライバシー対応を担っており、定期的に最新動向を網羅したプライバシートレーニングを提供している。 |
| **3** | **Repeatable 対応に再現性がある** | 対応はマネジメントに承認されており、組織レベルのポリシーにまで昇華されている。 | プライバシーリスクへの意識があり、それが組織レベルとなるまで昇華されている。 | データ処理システムで自分たちが果たす役割、依存関係等を認識しており、その対応に再現性がある。 | 特定の人員が対応要員として、プライバシーリスクの一貫性ある対応を行い、プライバシーに関するトレーニングを受講している。 |
| **2** | **Risk Informed リスクが認識できている** | 対応はマネジメントに承認されているが、組織レベルのポリシーにまで昇華されていない。 | プライバシーリスクへの意識があるが、それが組織レベルとなるまで昇華されていない。 | データ処理システムで自分たちが果たす役割を認識しているが、その対応に一貫性がない。 | 対応要員にプライバシーリスクへの認識があり、役割も与えられているが、対応に一貫性がない。 |
| **1** | **Partial 部分的に対応できている** | 対応が定型化されておらず、発生ベースで対応している。 プライバシー対応の優先度は低い。 | 組織として、プライバシーリスクへの認識は弱い。 データ処理とそのリスクについて情報共有されていない。 | データ処理システムで自分たちが果たす役割を認識していない。ステークホルダーにプライバシーリスクを共有するプロセスがない。 | 対応要員にプライバシーリスクへの認識が薄く、プライバシー保護についての具体的な役割が与えられていない。 |

**Profileの詳細**

Coreの設問をTierで評価した結果、現在のレベルが明らかになり、それを踏まえて、今後どのレベルまで目指すのかを決定します。この自社の現状と目指すべきゴールのギャップを明確化するところがProfileと呼ばれます。Profileでギャップを定義したら、そのギャップを埋めるための改善施策を決定し、以下のような流れで改善施策を決定し、それを実行していきます。

* Ready:プライバシーリスクについて組織が理解を持つよう地ならしをする
* Set: 現状と目指すべきゴールとのギャップを埋める改善施策を決定する
* Go: 改善施策を実行する

また、改善施策を決定する際、データ入手から廃棄に至るまでのライフサイクル(SDLC: System Development Life Cycle)や、プライバシーに関する利害関係者(個人、自社、政府当局、製造者、委託業者…)との関係性も意識する必要があります。  
前述したように、PFは汎用的な内容になっており、組織規模の大小やビジネス展開、リスク状況等を問わず、Tier4 (変化に適応できる)レベルまで目指すのが望ましいです。

その意味で、定期的にPF Profileを更新していくことで、プライバシー対応の継続的改善に繋がります。

**最後に**

データ活用がより重視される世の中で、データの取扱いについて示す法規制や認証、ガイドラインがいろいろ出揃ってきていますが、NISTプライバシーフレームワークはサイバーセキュリティフレームワーク同様、世界の標準になっていく可能性があります。

プライバシーに関する認証取得や法規制遵守は求められていないものの、自社のプライバシー対応レベルを知りたいという場合には最適な選択肢になりそうです。

**参考文献**

* [NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT](https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf)