わが国の法制度に基づくプライバシー保護技術に関する調査

調査報告書

平成１７年３月

財団法人ニューメディア開発協会

この事業は、競輪の補助金を受けて実施したものです。

目　次

１．背景と目的

財団法人ニューメディア開発協会では、平成 11 年度に通商産業省からの出資を受けて情報処理振興事業協会が実施する「先進的情報システム開発実証事業」の一環として、国際的 Web 技術標準化団体の W3C（World Wide Web Consortium）の P3P（Platform for Privacy Preference）ワーキングドラフトに基づく「プライバシー情報管理システム」の開発と提供を行っている。また、平成 13 年度および平成 14 年度には、W3C の P3P1.0 勧告候補版および勧告版に基づく「P3P ポリシーウィザード」の開発と提供を行っている。

財団法人ニューメディア開発協会ではこのように継続的に、P3P に基づく実証システムの開発と普及活動を行っている。P3P は企業や組織が Web 上で公開するプライバシーポリシーに基づいて、消費者がその企業や組織の信頼性を自動的に判断するための技術標準であるが、米欧が中心に策定した仕様であるため、日本の法制度や商慣習に合わせたローカライゼーションが必要となってきている。

本調査では平成 15 年 5 月の個人情報保護法の成立及び平成 17 年 4 月からの全面施行、またプライバシーマーク制度の普及等を踏まえ、我が国における個人情報保護法やプライバシーマーク制度等に整合した形で P3P のローカライゼーションおよび応用に関する調査を行う。

２．個人情報保護法等の要求事項に関する調査

個人情報保護法、プライバシーマーク、その他国内の個人情報保護に関する各種ガイドラインにおける要求事項に関する調査を行った。

調査にあたっては、P3P がプライバシーポリシーの掲載項目を XML 言語で記述するための技術使用であることに鑑み、事業者がプライバシーポリシーに掲載すべき項目という観点から法律等における要求事項の調査を行った。また、P3P の技術仕様を踏まえた上で、その項目が P3P を用いて表現できる項目であるかどうかも吟味した。

２．１ 個人情報の保護に関する法律

まず、「個人情報の保護に関する法律（以下、個人情報保護法)」および「個人情報保護に関する法律施行令（以下、政令)」において、関連すると考えられる条項を可能な限りピックアップすると、以下の通りとなる。（下線は本調査報告書の執筆者が付加したもの。）

○第 16 条（利用目的による制限）

第 1 項　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

第 2 項　個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

→あらかじめ特定しておいた利用目的の範囲を超えて個人情報を取扱う場合（目的外利用の場合)、本人の事前の同意が必要となる。通常のヒューマンリーダブルなプライバシーポリシーでは、「お客様から頂いた個人情報をお客様にお伝えした利用目的以外で利用する場合は、お客様から同意を頂いた上で、利用させていただきます」などと、簡単に表現することができる。ただし、この事柄は、P3P を用いたマシンリーダブルなプライバシーポリシーでは表現することが難しい。

→また、他社を合併すること等によって他の個人情報取扱事業者から個人情報を取得した際に、事業承継前の利用目的の範囲を超えて個人情報を取扱う場合も、本人の事前の同意が必要となる。これについても、第 1 項と同様である。

○第 18 条（取得に際しての利用目的の通知等）

第 1 項　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

第 2 項　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

第 3 項　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

→個人情報を取得した場合は、利用目的を本人に通知するか、公表しなければならない。とりわけ、書面（電磁的方式を含む）で個人情報を取得する場合は、利用目的をあらかじめ本人に明示しなければならない。これは、P3P を用いたマシンリーダブルなプライバシーポリシーの最も得意とするところである。方法としては、サイト全体のプライバシーポリシーに利用目的をすべて列挙する方法と、その個人情報を収集したり利用するサイト内特定サービスページのプライバシーポリシーにおいて当該利用目的を明記する方法とがある。

→利用目的を変更した際は、変更後の利用目的を、P3P を用いたプライバシーポリシーで表現することができるが、ただし利用目的の変更履歴や、プライバシーポリシーの変更日時などは表現することができない。

○第 23 条（第三者提供の制限）

第 1 項　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

第 2 項　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

第 3 項　個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

第 4 項　次に掲げる場合において、当該個人データの提供を受ける者は、前三項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

第 5 項　個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

→収集した個人データの第三者提供を行わない場合は利用者への通知等は必要ないが、第三者提供を行う場合は、以下のいずれかの方法をとらなければならない。①第三者提供を行う旨について、本人から同意を得る、②必要事項をあらかじめ本人に通知するか、本人が容易に知り得る状態に置く（オプトアウト）。①は P3P を用いたプライバシーポリシーによって表現できる内容であるが、本人から同意を得るという工程を P3P 上で実現しようとすると、クライアント側に専用のツールを準備する必要がある。②は P3P を用いたプライバシーポリシーによって十分に表現可能な内容であるが、「第三者への提供の手段又は方法」という項目については、P3P の既定のボキャブラリでは定義されていないため、P3P で表現することができない。

→収集した個人データを他の事業者と共同利用する場合は、必要事項をあらかじめ本人に通知するか、本人が容易に知り得る状態に置けばよい。この必要項目自体は P3P を用いたプライバシーポリシーにおいてほぼ表現可能だが、「共同利用」であるということを表現する方法が P3P には含まれていない。また、「当該個人データの管理について責任を有する者の氏名又は名称」も P3P では表現することができない。

○第 24 条（保有個人データに関する事項の公表等）

第 1 項　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

一　当該個人情報取扱事業者の氏名又は名称

二　すべての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く。）

三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

●政令第 5 条（保有個人データの適正な取扱いの確保に関し必要な事項）

法第 24 条第 1 項第 4 号の政令で定めるものは、次に掲げるものとする。

一　当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先

二　当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

→個人情報取扱事業者が公表すべき事項が規定されている。ほぼ全ての項目を、P3P を用いたプライバシーポリシーで表現することができるが、「手数料の額」については P3P で表現することができない。

○第 29 条（開示等の求めに応じる手続き）

第 1 項　個人情報取扱事業者は、第二十四条第二項、第二十五条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求め（以下この条において「開示等の求め」という。）に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。

●政令第 7 条（開示等の求めを受け付ける方法）

法第 29 条第 1 項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる次項は、次に掲げるとおりとする。

一　開示等の求めの申出先

二　開示等の求めに際して提出すべき書面（電子的方法、磁気的方法その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

三　開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

四　法第 30 条第 1 項の手数料の徴収方法

→開示等の求めを受け付ける方法が規定されている。個人情報保護法第 24 条第 1 項第 3 号に

も関連するものと考えられるが、これらの項目を公表するところまでは義務ではないかもしれない。「開示等の求めの申出先」は P3P を用いたプライバシーポリシーで表現できるが、それ以外については P3P で表現することはできない。

以上の結果から、個人情報保護法の要求事項のうち、P3P を用いたプライバシーポリシーによって表現できるものは、以下の項目である。

- 取得する個人情報の利用目的
- （第三者提供を行う場合）
  - 第三者提供を行う旨（本人の同意が必要）　または
  - 第三者への提供を利用目的とすること
  - 第三者に提供される個人データの項目
  - 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること
- 当該個人情報取扱事業者の氏名又は名称
- すべての保有個人データの利用目的
- 利用目的の通知、開示、訂正・追加・削除、利用停止、第三者提供停止の求めに応じる手続
- 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
- 認定個人情報保護団体の名称及び苦情の解決の申出先

ここで、「取得する個人情報の利用目的」と「すべての保有個人データの利用目的」とが重複しているが、「個人情報」と「保有個人データ」を比べると個人情報保護法の定義では前者が後者を包含する広い概念であるため、以降、「取得する個人情報の利用目的」のみを取扱う。

２．２ 省庁のガイドライン

次に、我が国の個人情報保護法制に関連した省庁のガイドラインのうち、一般企業向けの経済産業省のガイドライン「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」、電気通信事業者向けの総務省のガイドライン「電気通信事業における個人情報保護に関するガイドライン」において、関連すると考えられる条項を可能な限りピックアップすると、以下の通りとなる。（下線は本調査報告書の執筆者が付加したもの。）

(a)「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」

経済産業省のガイドラインでは、個人情報保護法以上の要求事項は提示されていないが、第 V 節 p.56～57 において、「個人情報取扱事業者は、以下の事項を参考として『個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等)』を策定し、ウェブ画面への掲載等により公表することが望ましい」とされている。その「個人情報保護に関する考え方や方針に関する宣言」に含めるべき項目として挙げられているのが、以下の項目である。

「また、個人情報取扱事業者は、以下の事項を参考として「個人情報保護に関する考え方や方針に関する宣言（いわゆる、プライバシーポリシー、プライバシーステートメント等)」を策定し、ウェブ画面への掲載等により公表することが望ましい。

① 事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。

ⅰ．取得する個人情報の利用目的（法第１８条関係）

ⅱ．＜本人の同意なく第三者提供する場合＞（法第２３条第２項及び第３項関係）

- 利用目的に第三者提供が含まれていること。
- 第三者に提供される個人データの項目
- 第三者への提供の手段又は方法
- 本人の求めに応じて第三者への提供を停止すること。

ⅲ．＜共同利用する場合＞（法第２３条第４項及び第５項）

- 特定の者との間で共同利用すること。
- 共同して利用される個人データの項目
- 共同利用者の範囲
- 共同して利用する者の利用目的
- 共同して利用する者のうち、個人データの管理について責任を有する者の氏名又は名称

ⅳ．以下の保有個人データに関すること（法第２４条関係)。

- 自己の氏名又は名称

・すべての保有個人データの利用目的
・「開示等の求め」に応じる手続（定めた場合に限る。）
・保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る。）
・苦情の申出先（認定個人情報保護団体の対象事業者である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先を含む。）

ｖ．開示等の求めに応じる手続に関すること（法第２９条関係）。
・申請書の様式（定めた場合に限る。）
・受け付ける方法（定めた場合に限る。）
・保有個人データの特定に役立つ情報の提供

ⅵ．問い合わせ及び苦情の受付窓口に関すること（法第２３条第５項、第２４条第１項、第２９条第１項及び第３１条関係）。

② 個人情報の保護に関する法律を遵守すること。

③ 個人情報の安全管理措置に関すること。

④ コンプライアンス・プログラムの継続的改善に関すること。」

①に挙げられていることは、個人情報保護法における要求事項そのものであるが、②～④に挙げられている項目は、JIS15001 を参考として、経済産業省ガイドラインで追加された項目である。

②～④に挙げられている項目については、P3P を用いたプライバシーポリシーで表現することはできない。

(b)「電気通信事業における個人情報保護に関するガイドライン」

総務省のガイドラインにおいても、基本的には個人情報保護法と同じ要求事項が提示されている。プラスアルファの部分としては、第 14 条にて「電気通信事業者は、プライバシーポリシー（当該電気通信事業者の個人情報の取扱いに関する方針についての宣言をいう。）を公表し、これを遵守するものとする」という規定がされている。

さらに、同ガイドラインの「解説」では、第 14 条について以下のような説明が加えられている。

「プライバシーポリシーは、それぞれの電気通信事業者が、自らの個人情報の取扱いに関する方針を分かりやすい表現で記載すべきものであるが、プライバシーポリシーに記載すべき事項としては、次のようなものが考えられる。

1) 個人情報保護法及び通信の秘密に係る電気通信事業法の規定その他の関係法令の遵守
2）本ガイドラインの遵守
3）（本ガイドライン）第 16 条第 1 項各号に定める公表すべき事項
（ｉ） 電気通信事業者の名称

（ⅱ） 個人情報の利用目的

（ⅲ） 利用目的の通知又は開示若しくは訂正等の本人からの求めに応じる手続

（ⅳ） 苦情の申出先

（ⅴ） 認定個人情報保護団体の名称及び苦情の解決の申出先

4）（本ガイドライン）第 11 条の安全管理措置に関する方針　」

3）については、個人情報保護法の項目と同じである。1)、2)、4）が総務省ガイドラインとして追加されている項目である。

この 1)、2)、4）の項目については、経済産業省ガイドラインと同様、P3P を用いたプライバシーポリシーで表現することはできない。

２．３ JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」

次に、JIS 規格である JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」における、関連する要求事項をピックアップしてみた。これは、JIPDEC が管理している第三者認証制度であるプライバシーマーク制度が拠り所としている規格である。

○4.2 項（個人情報保護方針）

事業者の代表者は、次の事項を含む個人情報保護方針を定めるとともに、これを実行し維持しなくてはならない。事業者の代表者は、この方針を文書化し、役員及び従業員に周知させるとともに一般の人が入手可能な措置を講じなくてはならない。

a) 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること。
b) 個人情報への不正サクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること。
c) 個人情報に関する法令及びその他の規範を遵守すること。
d) コンプライアンス・プログラムの継続的改善に関すること。

→上記の項目を含むプライバシーポリシーを公表しなければならないが、経済産業省ガイドラインの際と同様に、b)～d)については P3P を用いたプライバシーポリシーでは表現することができない。a)については、個人情報保護法でピックアップした項目の総体がこれに該当すると考えることができる（従って、個人情報保護法の要求事項を満たすプライバシーポリシーであれば、自動的に上記の a）も満たすことができる)。

○4.4.2.4 項（情報主体から直接収集する場合の措置）

情報主体から直接に個人情報を収集する場合には、情報主体に対して、少なくとも、次に示す事項又はそれと同等以上の内容の事項を書面若しくはこれに代わる方法によって通知し、情報主体の同意を得なければならない。

a) 事業者の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先。
b) 収集目的。
c) 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無。
d) 個人情報の預託を行うことが予定される場合には、その旨。
e) 情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果。
f) 個人情報の開示を求める権利、及び開示の権利、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法。

→情報収集時に本人に対して上記の項目を通知し、同意を得なければならないとされる。b)～d)については P3P を用いたプライバシーポリシーで表現することが可能である。a)、e)、f)については、P3P では表現することができない。また、本人から同意を得るという工程を P3P 上で実現しようとすると、クライアント側に専用のツールを準備する必要がある。

以上の結果から、JISQ15001 の要求事項のうち、P3P を用いたプライバシーポリシーによって表現できるものは、以下の項目である。

- 情報主体から収集する個人情報の収集目的（本人の同意が必要）
- 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無（本人の同意が必要）
- 個人情報の預託を行うことが予定される場合には、その旨（本人の同意が必要）

２．４ 法律・ガイドラインの要求事項に基づく掲載項目の整理

上記の調査をまとめると、法律・ガイドラインの要求事項に基づき、事業者がプライバシーポリシーに掲載すべき項目は以下の項目である。それらのうち、P3P を用いて表現できるのは下線を引いた項目である。

○個人情報保護法

- 取得する個人情報の利用目的
- 当該個人情報取扱事業者の氏名又は名称
- 利用目的の通知、開示、訂正・追加・削除、利用停止、第三者提供停止の求めに応じる手続
- 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
- （認定個人情報保護団体の対象事業者である場合）
  - 認定個人情報保護団体の名称及び苦情の解決の申出先
- （第三者提供を行う場合）
  - 第三者提供を行う旨（本人の同意が必要）
- （第三者提供を行い、かつオプトアウトを行う場合）
  - 第三者への提供を利用目的とすること
  - 第三者に提供される個人データの項目
  - 第三者への提供の手段又は方法
  - 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること
- （共同利用を行う場合）
  - 個人データを共同利用する旨
  - 共同して利用される個人データの項目
  - 共同して利用する者の範囲
  - 利用する者の利用目的
  - 当該個人データの管理について責任を有する者の氏名又は名称
- （手数料の額を定めた場合）
  - 手数料の額

○JISQ15001

- 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること
- 個人情報への不正サクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること
- 個人情報に関する法令及びその他の規範を遵守すること

・ コンプライアンス・プログラムの継続的改善に関すること
・ 事業者の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先（本人の同意が必要）
・ 情報主体から収集する個人情報の収集目的（本人の同意が必要）
・ 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無（本人の同意が必要）
・ 個人情報の預託を行うことが予定される場合には、その旨（本人の同意が必要）
・ 情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果（本人の同意が必要）
・ 個人情報の開示を求める権利、及び開示の権利、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法（本人の同意が必要）

JISQ15001 の項目のうち、個人情報保護法の項目に統合できるものは、「本人の同意が必要」という条件が付いていることは度外視すると、以下のとおりである。

JISQ15001 の「収集目的」　⇒　個人情報保護法の「利用目的」

３．個人情報保護法等の要求事項に即した P3P 技術の応用に関する調査

２．で調査した個人情報保護法等における要求事項に基づき、P3P を用いたプライバシーポリシーを作成するためには、どの掲載項目をどの P3P 仕様上の項目に当てはめればよいのか、P3P 技術の応用に関する調査を行った。

３．１ W3C の P3P

P3P1.0 の仕様書（The Platform for Privacy Preferences 1.0 (P3P1.0) Specification W3C Recommendation 16 April 2002）において P3P ポリシーに必ず掲載しなければならない（mandatory または MUST）と規定されている「必須エレメント」は以下のものである（図１参照)。

※P3P ポリシーとは、P3P 仕様に則り XML 言語で書かれたプライバシーポリシーのことである。

○ポリシーに関する情報
- ポリシーの名称
- 自然言語で書かれたプライバシーポリシーの URL
- Opt-in または Opt-out の URI(利用目的で Opt-in、Opt-out が指定されている場合のみ)

○事業者・組織に関する情報
- 事業者・組織の名称
- 連絡先情報（住所、電話番号、メールアドレス、URI のうち１つ以上が必須）

○アクセスに関する情報

○苦情処理に関する情報（推奨 SHOULD）・・・(複数重ね書き可能)
- 苦情処理のタイプ
- 上記のサービスに関する URI

○苦情処理の方法（推奨 SHOULD）

○ステートメントに関する情報・・・(複数重ね書き可能)
- 利用目的に関する情報（複数選択）
- 受領者に関する情報（複数選択）
- 保有期間に関する情報（単数選択）
- 収集する個人情報に関する情報（複数選択）
- (収集する個人情報に関する情報の一部として）クッキー利用の有無

P3Pポリシーの必須掲載項目		掲載形式
ポリシーに関する情報 ＜POLICY＞	ポリシーの名称	自由記述
	自然言語で書かれたプライバシーポリシーのURL	自由記述
	Opt-inまたはOpt-outのURI(利用目的でOpt-in、Opt-outが指定されている場合のみ)	自由記述
事業者・組織に関する情報 ＜ENTITY＞	事業者・組織の名称	自由記述
	連絡先情報（住所、電話番号、メールアドレス、URIのうち1つ以上が必須）	自由記述
アクセスに関する情報 ＜ACCESS＞		単数選択
苦情処理に関する情報 ＜DISPUTES＞ [MustではなくShould] （複数重ね書き可能）	苦情処理のタイプ	単数選択
	苦情処理のURI	自由記述
苦情処理の方法に関する情報 ＜REMEDIES＞　[MustではなくShould]		複数選択
ステートメントに関する情報 ＜STATEMENT＞ （複数重ね書き可能）	利用目的に関する情報 ＜PURPOSE＞	複数選択
	受領者に関する情報 ＜RECIPIENT＞	複数選択
	保有期間に関する情報 ＜RETENTION＞	単数選択
	収集する個人情報に関する情報 ＜DATA＞	複数選択

図１　P3P ポリシーの必須掲載項目

それぞれのエレメントについて以下に説明していく。

３．１．１ ポリシーに関する情報

このエレメントについては、「ポリシーの名称」と「自然言語で書かれたプライバシーポリシーの URL」と「Opt-in または Opt-out の URI(利用目的で Opt-in、Opt-out が指定されている場合のみ)」の 3 項目が必須である。これらの項目については事業者側で自由に文字記述を行うことができる。

「Opt-in または Opt-out の URI(利用目的で Opt-in、Opt-out が指定されている場合のみ)」が複雑であるが、これは後に出てくる「利用目的に関する情報」において、或る利用目的に Opt-in または Opt-out の属性が付加されている場合には、利用者がその特定目的について個人情報の利用を申し出たり（オプトイン）、その特定目的について個人情報の利用停止を要求したり（オプトアウト）できることが必要であり、利用者がそうした手続きをするための Web ページの URI がこの「Opt-in または Opt-out の URI」である。

３．１．２ 事業者・組織に関する情報

このエレメントについては、「事業者・組織の名称」と「連絡先情報（住所、電話番号、メールアドレス、URI のうち１つ以上が必須)」の 2 項目が必須である。これらの項目については事業者側で自由に文字記述を行うことができる。

３．１．３ アクセスに関する情報

このエレメントについては、以下の選択肢のいずれか一つを選択することになっている。

a)Web サイトは個人情報を収集していない
b)すべての個人情報へのアクセスを提供
c)オンライン連絡先情報及び物理的連絡先情報と、その他の何らかの個人情報へのアクセスを提供
d)オンライン連絡先情報及び物理的連絡先情報へのアクセスを提供
e)その他の何らかの個人情報へのアクセスを提供
f)個人情報へのアクセスは提供していない

我が国では個人情報保護法によって、個人情報取扱事業者は本人からの個人情報の開示の求めに対して、原則として（「当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合」などは例外）開示しなければならないと定められている。したがって、事業者は本人に「すべての個人情報（本人情報）へのアクセスを提供」するものと考えられるが、人事考量情報などについては開示の求めに応えられない場合があると考えられるので少しレベルを下げて、事業者は「オンライン連絡先情報及び物理的連絡先情報と、その他の何らかの個人情報へのアクセスを提供」するという辺りが妥当な選択肢と考えられる。

３．１．４ 苦情処理に関する情報

このエレメントについては、複数重ね書きが可能である。１つの苦情処理エレメントの中には、「苦情処理のタイプ」（単数選択)、「上記のサービスに関する URI」（自由記述）の項目が必須で含まれなければならない。「苦情処理のタイプ」の選択肢は下記の通りである。

a)カスタマーサービス
b)第三者機関

c)裁判所
d)適用可能な法律

その他、必須ではないが「苦情処理の名称（short-description)」という項目もあり、この中で第三者機関の名称や法律の名称等を記載することができる。

３．１．５ 苦情処理の方法に関する情報

このエレメントについては、以下の選択肢のうち当てはまるものを全て選択することになっている。

a)訂正
プライバシーポリシーに関連して生じた過失や不適切な取扱いについては、当該事業者が是正措置を行う。

b)賠償
当該事業者がプライバシーポリシーに違反した場合は、ヒューマンリーダブルなプライバシーポリシーに明示されている額か、または損害に応じた額を個人に賠償する。

c)法律
プライバシーポリシーの違反行為に対する是正措置は、法律に基づき、決定される。

３．１．６ ステートメントに関する情報

このエレメントは、事業者の具体的な個人情報取扱いについて記述するためのものであり、複数重ね書きが可能である。このエレメントは、さらに、「利用目的に関する情報」「受領者に関する情報」「保有期間に関する情報」「収集する個人情報に関する情報」というエレメントを必須で含まなければならない。

１つのステートメントごとに、事業者の提供するサービス単位での個人情報取扱いを記述することが可能である。例えば、サイト内の「オンラインショッピングページ」や「メルマガ登録ページ」「利用者ごとのページのカスタマイズ」など、異なる個人情報取扱いをそれぞれ別セットにして、別々のステートメントとして記述して、重ね書きすることが可能である。

３．１．７ 利用目的に関する情報

このエレメントについては、以下の選択肢のうち当てはまるもの全てを選択することになっている。

a)データが提供されている活動の遂行とサポート　<current/>

情報は、情報提供や通信、双方向サービスなど、利用者が そのために情報を与えたところの活動を遂行するために、サービス提供者によって利用されるかもしれない。例えば、ウェブ検索の結果の返信、電子メールの送信、商品の注文、または、会員サービスの提供など繰り返し行う活動や、オンラインのアドレスブックや電子ウォレットにアクセスを許可することなど。

b)Web サイトとシステムの管理　<admin/>

情報は Web サイトとそのコンピュータ・システムの技術的サポートのために利用されるかもしれない。 この中には、コンピュータ・アカウント情報の処理や、サイトの一連の保守管理で利用される情報、およびサイトやエージェントによる Web サイト活動の確認などが含まれる。

c)調査と開発　<develop/>

情報は、サイトやサービス、製品、マーケットを改善したり、評価したり、検討したりするために利用されるかもしれない。 この中には、特定個人に合わせてコンテンツを調整したり変更したりするために個人情報を利用することや、特定個人を評価したり、ターゲットとしたり、プロファイルしたり、 また特定個人と連絡をとったりするために個人情報を利用することは含まれない。

d)一回限りのカスタマイズ　<tailoring/>

情報は、コンテンツを調整したり変更したりするために利用されることがある。情報はサイトへの 1 回の訪問のみで利用され、その後のいかなるカスタマイズにも利用されない。例えば、訪問者が買い物かごに入れた商品にもとづいて、彼がその他に購入したいであろう商品を提案するオンラインショップなど。

e)偽名を用いた分析　<pseudo-analysis/>

情報は、個人が特定可能なデータ（氏名、住所、電話番号、メールアドレス等）を記録と結び付けることなく、偽名の識別子と結び付けられた特定個人またはコンピュータの記録を作成するために利用されるかもしれない。このプロファイルは調査や分析、報告を目的として、個人の習慣や関心、その他の特徴を決定のために利用されるが、特定個人を識別するためには利用されないものとする。例えば、マーケッターは Web サイトの異なる部分へアクセスする訪問者のそれぞれの関心を理解したいと考えるかもしれない。

f)偽名を用いた決定　<pseudo-decision/>

情報は、個人が特定可能なデータ（氏名、住所、電話番号、メールアドレス等）を記録と結び付けることなく、偽名の識別子と結び付けられた特定個人またはコンピュータの記録を作成するために利用されるかもしれない。このプロファイルは個人に直接的に影響を及ぼすような決定を行うことを目的として、個人の習慣や関心、その他の特徴を決定のために利用されるが、特定個人を識別するためには利用されないものとする。例えば、マーケッターは、以前アクセスした人が見たページに基づき、ブラウザに表示するコンテンツを調整したり、変更したりするかもしれない。

g)個々人の分析　<individual-analysis/>

情報は、調査や分析、報告を目的として、個人の習慣や関心、その他の特徴を決定し、個人特定可能なデータと結びつけるために利用される。例えば、物理的な店のオンライン Web サイトは、オンライン購入者がどのようにオフライン購入を行うかを分析したいと考えるかもしれない。

h)個々人に対する決定　<individual-decision/>

情報は、個人に直接的に影響を及ぼすような決定を行うことを目的として、個人の習慣や関心、その他の特徴を決定し、個人特定可能なデータと結びつけるために利用される。例えば、オンラインショップが訪問者が以前 Web サイトに訪れた時に購入した物に基づき、商品を提案する場合。

i)サービスや製品のマーケティングのために訪問者と連絡を取る　<contact/>

情報は、商品やサービスの販売促進のために電話以外の連絡方法で個人と連絡をとる目的で利用されるかもしれない。この中には、Web サイトの更新を訪問者に通知することも含まれる。質問やコメントへの直接的回答や、1 回のやり取りのためのカスタマーサービスはこの中には含まない。そういったケースでは、<current/> が利用される。さらに、カスタマイズされた Web コンテンツまたは、ユーザが訪れているサイトに埋め込まれたバナー広告を通じてのマーケティングも含まれない。こういう場合は <tailoring/>, <pseudo-analysis/> と <pseudo-decision/>, または <individual-analysis/> と <individual-decision/> でカバーされるだろう。

j)履歴の保存　<historical/>

情報は、既存の法律や政策の規定に基づき、社会の履歴を保存するために格納したり保存されるかもしれない。この法律や政策は<DISPUTES>要素において参照されなければならないし、この情報（どこにこの情報が保存されるのか、特にどのようにしてこの情報収集が履歴の保存を向上させるのか）にアクセスできる資格のあるリサーチャーの特別な定義を含まなければな

らない。

k)サービスや製品のマーケティングのために電話で訪問者と連絡を取る　<telemarketing/>

情報は、商品やサービスの販売促進のために電話で個人に連絡をとる目的で利用されることがある。この中には、Web サイトの更新を訪問者に通知することも含まれる。質問やコメントへの直接的回答や、1 回のやり取りのためのカスタマーサービスはこの中には含まない。この場合、<current/>が利用される。

l)その他の利用　<other-purpose/>

情報は、上記の定義には当てはまらない方法で利用されるかもしれない。（この場合、人間が読むことのできる説明を与えなければならない。）

それぞれの利用目的は、追加の属性として「always」「opt-in」「opt-out」を持つことができる。「opt-in」とは、利用者がその利用目的を積極的に要求したときのみ、事業者はその利用目的で個人情報を利用できるという意味である。「opt-out」とは、利用者がその利用目的での利用の停止を要求しない限り、事業者はその利用目的で個人情報を利用できるという意味である。「always」は、事業者はその利用目的で常に個人情報を利用でき、利用者はオプトインしたり、オプトアウトすることができないという意味である。

３．１．８ 受領者に関する情報

このエレメントについては、以下の選択肢のうち当てはまるもの全てを選択することになっている。

a)当社内および／または業務委託先

この場合、業務委託先（agent）とは、言明された目的の達成のためだけにサービス提供者に代わってデータを処理する第三者として定義される。（例えば、サービス提供者とその印刷事務所。ただし、印刷事務所は住所ラベルを印刷し、それ以上は情報に関わりを持たない。）

b)当社とは異なる個人情報取扱い方針に従う可能性のある配送業者

言明された目的の遂行以外の目的でデータを利用するかもしれない、配送サービスを行う法人。また、これは個人情報取扱い方針が知られていない配送サービスにも使用される。

c)当社の個人情報取扱い方針に従う法人

サービス提供者と同等な個人情報取扱い方針の下で、自らのためにデータを利用する法人。

（例えば、収集した個人情報へのアクセスを利用者に提供し、かつ、提供された個人情報を一度利用するが保有せずに廃棄してしまうパートナー企業に個人情報を提供するサービス提供者を考えてみる。サービス提供者と同じ個人情報取扱い方針に従う受領者は、個人情報を廃棄するがために個人情報へのアクセスを利用者に提供することはできないので、受領者はサービス提供者と「同等な」プラクティスに従っているとみなされる。）

d)当社とは異なる個人情報取扱い方針に従う法人

サービス提供者の制約を受け、サービス提供者に対して責任を負うが、サービス提供者の個人情報取扱い方針においては特定されない方法でデータを利用するかもしれない法人。（例えば、サービス提供者が収集したデータを、その他の目的で利用するかもしれないパートナー企業に提供する場合。しかし、利用者の利益とサービス提供者の利益への侵害と考えられるような方法でデータが利用されないことを保証することが、サービス提供者の利益となるような場合。）

e)当社とは無関係な第三者

サービス提供者がそのデータ利用取扱い方針について関知しないような法人。

f)公のフォーラム（「公開」）

公のフォーラム。掲示版、公のディレクトリ、または商用 CD-ROM の ディレクトリなど。

「当社内および／または業務委託先」以外のそれぞれの受領者は、追加の属性として「always」「opt-in」「opt-out」を持つことができる。「opt-in」とは、利用者がその受領者への提供を積極的に要求したときのみ、事業者はその受領者へ個人情報を提供できるという意味である。「opt-out」とは、利用者がその受領者への提供の停止を要求しない限り、事業者はその受領者へ個人情報を提供できると言う意味である。「always」は、事業者はその受領者へ常に個人情報を提供でき、利用者はオプトインしたり、オプトアウトすることができないという意味である。

３．１．９ 保有期間に関する情報

このエレメントについては、以下の選択肢のいずれか一つを選択することになっている。

a)保有しない

情報は、オンラインでの１回のインタラクションにおいてその情報を利用するのに必要最低限の時間以上は保有されない。情報はこのインタラクションの後は消去されなければならず、ログとして記録されたり、履歴として残されたり、その他の方法で保存されたりしてはならない。このタイプの保有ポリシーは、例えば、Web サーバのログを取らないサービスや、1 回の

セッションで使用するためだけにクッキーを設定するサービス、Web 検索を行うために情報を収集するが検索に関するログは取らないサービスなどに当てはまるだろう。

b)言明された目的のための保有

情報は言明された目的をかなえるために保有される。これは、情報ができるだけ早期に廃棄されることを要求するものである。サイトは、データ消去のタイムテーブルを設定した保有ポリシーを持たなければならない。保有ポリシーは、サイトの人間が読むことのできるプライバシーポリシーに含まれるか、またはそこからリンクが張られていなければならない。

c)法律による要求事項または適用可能な法律に基づく責務を果たすための保有

情報は、言明された目的をかなえるために保有されるが、その保有期間は、法律上の要求または責務によってそれよりも長い場合がある。例えば、消費者が一定期間の間、取引に対して異議申立てを行うことが法律によって認められているため、企業は責務上の理由によりその取引記録を保持しようとするかもしれない。また、企業が監査上の目的あるいは健全性の目的で記録を保持することが、法律によって肯定的に要求されているかもしれない。サイトはデータ消去のタイムテーブルを設定した保有ポリシーを持たなければならない。保有ポリシーは、サイトの人間が読むことのできるプライバシーポリシーに含まれるか、またはそこからリンクが張られていなければならない。

d)サービス提供者の業務方針による保有期間

情報は、サービス提供者の言明した業務方針に従って保有される。サイトはデータ消去のタイムテーブルを設定した 保有ポリシーを持たなければならない。保有ポリシーは、サイトの人間が読むことのできるプライバシーポリシーに含まれるか、またはそこからリンクが張られていなければならない。

e)無期限に保有

情報は、無期限に保有される。これは、保有ポリシーがない場合に起こるかもしれない。 受領者が公のフォーラムである場合は、これが適切な保有ポリシーである。

３．１．１０ 収集する個人情報に関する情報

このエレメントについては、P3P1.0 であらかじめ定義されたデータエレメントを使って個人情報を列挙することも可能であるし、自ら新たにデータエレメントを定義して掲載することも可能である。

３．１．１１ 結果に関する情報

P3P には、必須でないエレメントもいくつか定義されている。このエレメントはそうした必須でないエレメントの一つである。このエレメントは、ステートメントに関する情報の一つの要素であり、利用者にとって、そのステートメントで表現される個人情報取扱いがなぜ価値があるかを説明するもの、すなわち、利用者が事業者に個人情報を与えた場合にどのような結果になるか（効果・メリットを得られるか）を説明するためのものである。このエレメントについては、事業者が自由に文章で記述することができる。例えば、「お客様のために厳選した商品の販促メールをお送りします」など。

３．２ プライバシーポリシーの掲載項目と P3P のエレメントとの対応表

２．４において抽出した、個人情報保護法および JISQ15001 における要求事項に基づくプライバシーポリシーの掲載項目について、それぞれ対応する P3P のエレメントを表１、表２にまとめてみた。

プライバシーポリシーに掲載すべき項目		対応するP3Pのエレメント	備考
個人情報保護法	取得する個人情報の利用目的	利用目的に関する情報 〈PURPOSE〉	
	第三者提供を行う旨（本人の同意が必要）	受領者に関する情報 〈RECIPIENT〉	第三者提供を行う場合に必要。
	第三者への提供を利用目的とすること	受領者に関する情報 〈RECIPIENT〉	第三者提供かつオプトアウトを行う場合に必要。
	第三者に提供される個人データの項目	収集する個人情報に関する情報 〈DATA〉	第三者提供かつオプトアウトを行う場合に必要。
	第三者への提供の手段又は方法	（対応するP3Pエレメントなし）	第三者提供かつオプトアウトを行う場合に必要。
	本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること	受領者に関する情報 〈RECIPIENT〉〈**** required="opt-out"/〉	第三者提供かつオプトアウトを行う場合に必要。 受領者の属性にopt-outを追加する。
	当該個人情報取扱事業者の氏名又は名称	事業者・組織に関する情報 〈ENTITY〉	
	利用目的の通知、開示、訂正・追加・削除、利用停止、第三者提供停止の求めに応じる手続	Opt-inまたはOpt-outのURI 〈POLOCY opturi〉	P3Pの仕様上は「利用停止の求め先」であるが、開示、訂正等の求め先も同じ窓口であるとみなして適用する。
	当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先	苦情処理のタイプ 〈DISPUTES resplution-type〉 苦情処理のURI 〈DISPUTES service〉	苦情処理のタイプで「カスタマーサービス」を選択し、苦情処理のURIに窓口のURIを記載する。
	認定個人情報保護団体の名称及び苦情の解決の申出先	苦情処理のタイプ 〈DISPUTES resplution-type〉 苦情処理のURI 〈DISPUTES service〉 苦情処理の名称 〈DISPUTES short-description〉	苦情処理のタイプで「第三者機関」を選択し、苦情処理のURIに認定個人情報保護団体の苦情処理窓口のURIを記載する。苦情処理の名称に、認定個人情報保護団体の名称を記載する。
	個人データを共同利用する旨	（対応するP3Pエレメントなし）	共同利用を行う場合に必要。
	共同して利用される個人データの項目	収集する個人情報に関する情報 〈DATA〉	共同利用を行う場合に必要。
	共同して利用する者の範囲	受領者に関する情報 〈RECIPIENT〉	共同利用を行う場合に必要。
	利用する者の利用目的	利用目的に関する情報 〈PURPOSE〉	共同利用を行う場合に必要。
	当該個人データの管理について責任を有する者の氏名又は名称	（対応するP3Pエレメントなし）	共同利用を行う場合に必要。
	手数料の額	（対応するP3Pエレメントなし）	手数料の額を定めた場合に必要。

表１　プライバシーポリシーの掲載項目と P3P のエレメントとの対応表（１）

プライバシーポリシーに掲載すべき項目		対応するP3Pのエレメント	備考
JISQ15001	事業者の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先(本人の同意が必要)	(対応するP3Pエレメントなし)	
	情報主体から収集する個人情報の収集目的(本人の同意が必要)	利用目的に関する情報 <PURPOSE>	
	個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無(本人の同意が必要)	受領者に関する情報 <RECIPIENT> 利用目的に関する情報 <PURPOSE>	
	個人情報の預託を行うことが予定される場合には、その旨(本人の同意が必要)	受領者に関する情報 <RECIPIENT>	
	情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果(本人の同意が必要)	(対応するP3Pエレメントなし)	P3Pの「結果に関する情報」エレメント(<CONSEQUENCE>)を使う方法も考えられる。
	個人情報の開示を求める権利、及び開示の権利、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法(本人の同意が必要)	(対応するP3Pエレメントなし)	Opt-inまたはOpt-outのURIを使う方法も考えられる。

表２　プライバシーポリシーの掲載項目と P3P のエレメントとの対応表（２）

上記の掲載項目以外で、P3P の仕様の上で必須掲載項目とされているもの（すなわち必須エレメント）には、以下のものがある。事業者が P3P ポリシーを公表する場合は、表３の項目もあわせて掲載しなければならない。

その他の P3P 必須エレメント	XML 表記
プライバシーポリシーに関する情報	<POLICY>
アクセスに関する情報	<ACCESS>
苦情処理の方法に関する情報	<REMEDIES>
保有期間に関する情報	<RETENTION>
収集する個人情報に関する情報	<DATA>

表３　その他の P3P 必須エレメント

４．P3P 導入ガイドの作成

Web サイトが個人情報保護法等に即して P3P を導入するためのガイドの作成を行った。ガイドは以下の通りである。

（1）はじめに

個人情報保護法の要求事項では、個人情報取扱事業者は個人情報の利用目的など、様々な事項を「本人へ通知または公表」したり、「本人の知り得る状態に置」いたりすることが求められている。このための手段は、ホームページやパンフレット、店頭ポスターでのプライバシーポリシーの掲示など様々な手段が考えられる。P3P を用いたプライバシーポリシー（P3P ポリシー）は、サイトを訪問した利用者に対して、そのサイトのメタデータとして、サイトの個人情報取扱いを通知するものである。ブラウザのインターネットエクスプローラ（6 以上）を使っている利用者であれば、サイトの P3P ポリシーを「表示」メニューの「プライバシーレポート」にて簡単に確認することができる。したがって、個人情報保護法でいう「通知」や「公表」の一手段として活用することが可能である。ただし、P3P は未だ十分に普及・浸透しないので、メインの「通知・公表」手段として用いるのではなく、あくまで補助的手段に留めるべきである。

（2）プライバシーポリシーの作成

はじめに、サイトのプライバシーポリシーを作成する。プライバシーポリシーは個人情報保護法の要求事項に基づき、下記の項目を掲載する必要がある。

【標準で必要な項目】

- 取得する個人情報の利用目的
- 当該個人情報取扱事業者の氏名又は名称
- 利用目的の通知、開示、訂正・追加・削除、利用停止、第三者提供停止の求めに応じる手続
- 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先

【認定個人情報保護団体の対象事業者である場合に必要な項目】

- 認定個人情報保護団体の名称及び苦情の解決の申出先

【第三者提供を行う場合に必要な項目】

- 第三者提供を行う旨（本人の同意が必要）

【第三者提供を行い、かつオプトアウトを行う場合に必要な項目】

- ・ 第三者への提供を利用目的とすること
- ・ 第三者に提供される個人データの項目
- × 第三者への提供の手段又は方法
- ・ 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること

【共同利用を行う場合に必要な項目】

- × 個人データを共同利用する旨
- ・ 共同して利用される個人データの項目
- ・ 共同して利用する者の範囲
- ・ 利用する者の利用目的
- × 当該個人データの管理について責任を有する者の氏名又は名称

【手数料の額を定めた場合に必要な項目】

- × 手数料の額

また、JISQ15001 の要求事項に基づいて、下記の項目を掲載してもよい。

【JISQ15001 に準拠する場合に必要な項目】

- × 個人情報への不正サクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること
- × 個人情報に関する法令及びその他の規範を遵守すること
- × コンプライアンス・プログラムの継続的改善に関すること
- × 事業者の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先（本人の同意が必要）
- ・ 情報主体から収集する個人情報の収集目的（本人の同意が必要）
- ・ 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無（本人の同意が必要）
- ・ 個人情報の預託を行うことが予定される場合には、その旨（本人の同意が必要）
- × 情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果（本人の同意が必要）
- × 個人情報の開示を求める権利、及び開示の権利、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法（本人の同意が必要）

ここで×となっているのは、P3P ポリシーでは表現できない（対応する P3P エレメントがない）項

目のことである。

通常、一つのサイトにプライバシーポリシーは一つであるが、サイト内のサービスごとに別々のプライバシーポリシーを作成することも可能である。また、第三者提供を行い、オプトアウトは行わない場合は、本人の同意を得ないといけないので、個人情報を収集するページで必ず利用者にプライバシーポリシーを提示し、第三者提供に同意してもらった上で、個人情報を収集する必要がある。

（3）P3P ポリシーの作成

作成したプライバシーポリシーに基づき、P3P ポリシーを作成します。個人情報保護法で要求される掲載項目に対応する P3P エレメントは、３．２節の対応表（表１、表２）の通りである。なお、３．２節の表３で示したように、個人情報保護法で要求された掲載項目以外にも、P3P 仕様書の上で必須掲載項目とされているものがあるので、それらも合わせて掲載する必要がある。

P3P ポリシーを XML 言語で一から作成することは不可能ではないが、日本では財団法人ニューメディア開発協会が「P3P ポリシーウィザード」というツールを Web サイト上（http://www.nmda.or.jp/enc/privacy/index.html）で公開している。（２）で作成したプライバシーポリシーを見ながら、このツールを用いて対応する P3P ポリシーを作成することが可能である。作成した P3P ポリシーは p3ppolicy.xml 等の名称でファイルとして保存しておく。

P3P ポリシーウィザードを用いるとまた、ポリシー参照ファイルを作成することができる。これは、サイトの well-known な場所に置かれたファイルであり、サイト内のどのページに対する P3P ポリシーがどこにあるかを指し示すものである。作成したポリシー参照ファイルは p3p.xml 等の名称でファイルとして保存しておく。

（4）P3P ポリシーとポリシー参照ファイルのアップロード

ポリシー参照ファイルは、P3P の仕様により、(サイトの URI)/w3c/p3p.xml の場所に置くことが強く推奨されている。例えば、www.example.com というサイトのポリシー参照ファイルは www.example.com/w3c/p3p に置くことが強く推奨されている。

また P3P ポリシーは、ポリシー参照ファイルにおいて指定した場所に置くことになる。

（5）エラーチェック

W3C の P3P Validator のページ（http://www.w3.org/P3P/validator.html）にアクセスし、サイトの URL またはサイト内の P3P ポリシーの URL を入力すると、P3P ポリシーに関連して文法的なエラーがないかどうかを確認することができる。