更新事業者向け説明会

一般社団法人　中部産業連盟

Ⅰ.中産連　審査事務局より

①　申請手続き見直し

電子媒体での申請も受付開始予定です。
今回の**「更新事業者向け説明会」にご参加いただきました事業者様に限り、先行で電子媒体での申請も受け付けを開始しました。**
電子媒体での申請をする場合は、下記の注意事項にそってご申請ください。

【電子媒体での申請をする場合】

- 電子媒体はCD-R、DVD-R等を使用してください。（使用した電子媒体の返却はいたしません）
- 格納する形式は、PDF形式、Word形式またはEXCEL形式を用いてください。
- メールの添付ファイル、ストレージサーバ等での提出は不可です。
- 電子ファイルを格納した電子媒体の持参、もしくは配達記録の残る形で郵送してください。

- 今までと変わらず、紙媒体での申請も受け付けています。
- 紙媒体で提出する場合、A4サイズ縦の用紙に、片面印刷・両面印刷のいずれでも問題ありません。

- 申請形式検討の為にアンケートをお願いすることがありましたらご協力をお願いします。
- 一旦受領した申請書類、CD-ROMは原則返却いたしません。記録類は原本ではなく**コピー**を提出してください。

②申請・審査・付与登録料について

消費税法改正に伴う料金変更について、下記URLにて公表しました。

現地審査日と、エントリー審査会の日程で消費税の対応が異なります。

詳しくは下記URLにてご確認ください。
https://www.chusanren.or.jp/pmark/pdf/new-price.pdf

消費税改正前に審査を希望される事業者様は、なるべく早めのご申請をお願いします。

③中産連主催Pマーク関連セミナー

「JISQ:15001規格改定に伴う新審査基準と事例説明会」
https://www.chusanren.or.jp/sc/pdata/4206.html
2019年７月１１日金沢開催【参加費5,000円＋税/2名】

Pマーク登録状況

【中産連】

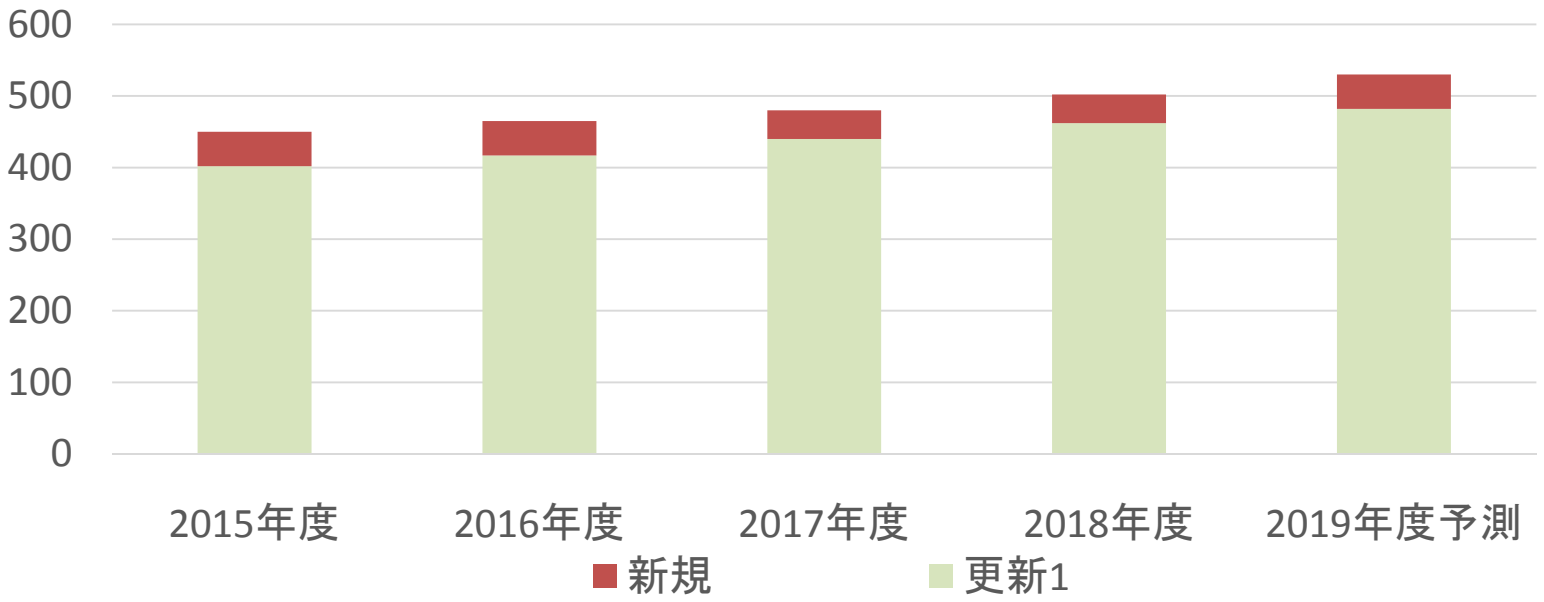
- 登録件数（2018年度実績）
  - 新規：40事業者
  - 更新：470事業者
- 登録件数（2019年度予測）
  - 新規：50事業者
  - 更新：480事業者

【全国（JIPDEC　HPより）】

- 登録件数（2019年5月現在）
  - 16,239事業者

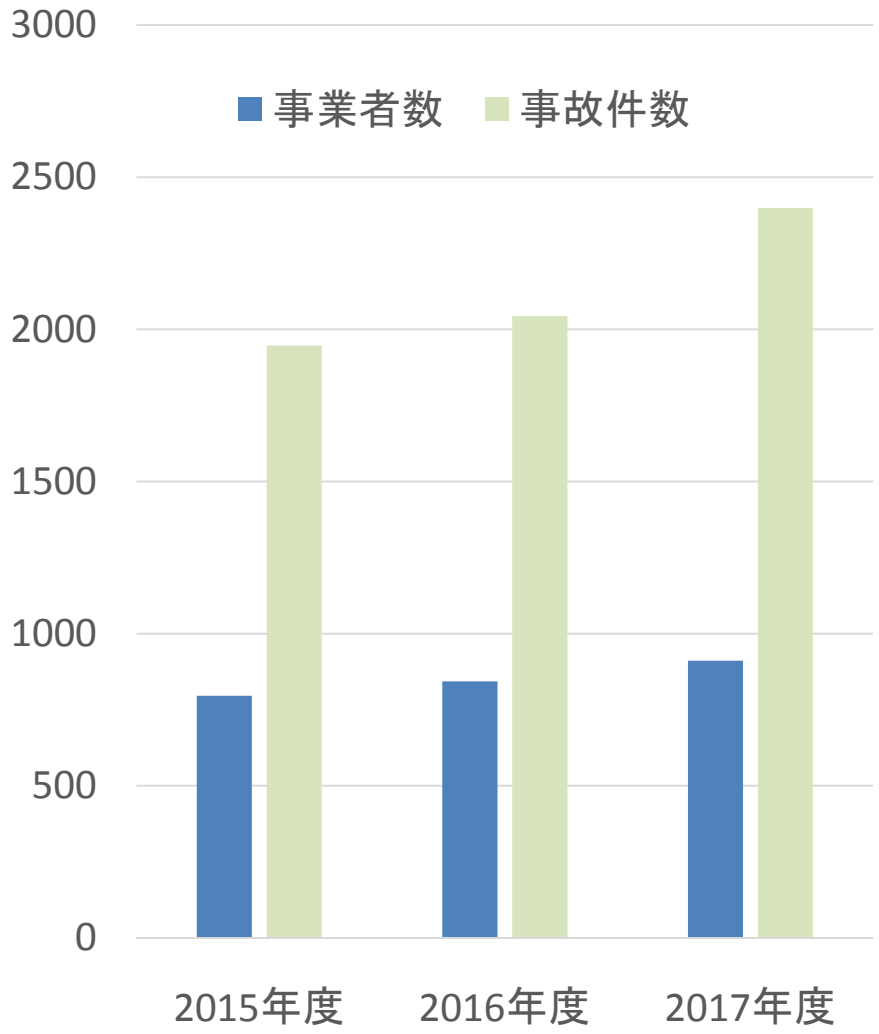
【ご参考】

- ISO9000　約33,000事業者
- ISMS　約5,800事業者



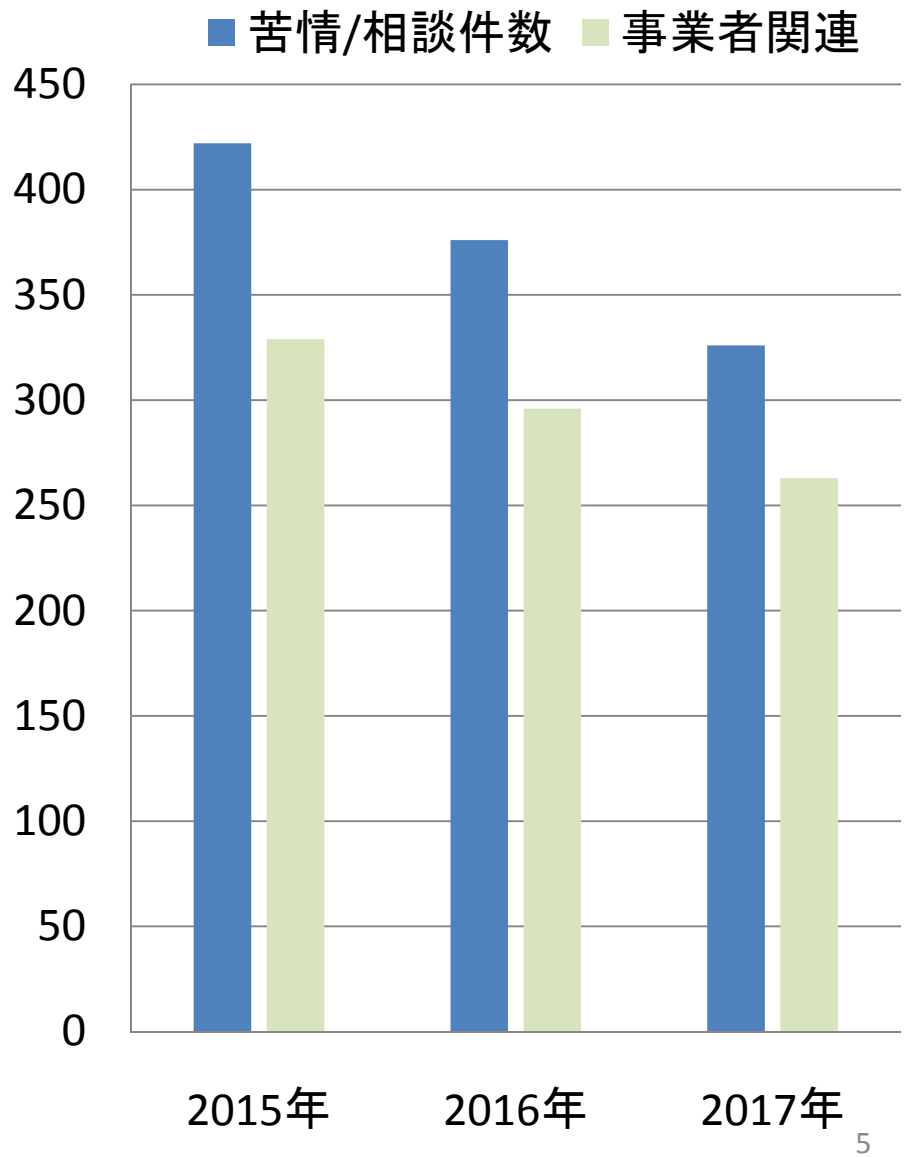
JIPDECへ報告された事故事例：2017年度（2018年8月31日報告より）

- 911付与事業者より2,399件の事故報告があり（前年度、報告事業者数843事業者、事故報告件数2,044件）
- 事故報告事業者/付与事業者数の割合は5.8%
- 事故原因は、「メール誤送信（アドレスや添付ファイル間違え/BCC→CC等で送信）」（26.5%）、次いで「紛失」等の順
- 「事務処理・作業ミス等」による漏えいが2倍強に増加した、「口頭での漏えい」も増加
- 「内部不正行為」が2倍強に増加
- トピック：インターネット上で、公開対象ではない個人情報が外部から閲覧された事故等



JIPDECへ寄せられた苦情/相談事例：2017年度（2018年10月4日公表より）

- 苦情/相談受付件数は、326件（前年度は、376件）
- 受付件数の内、付与事業者に関する件数は263件
- 相談種別の割合では、「個人情報の安全管理関連」（31.4%）、中でも「漏えい・紛失」に係る相談（21.3%）
- 次いで、「個人情報の開示等（開示・訂正、利用停止等）」（18.3%）、「その他」（14.8%）、「プライバシーマーク制度関係（プライバシーマークの不正使用等）」（9.6%）
- 付与事業者への確認調査は、108件（受付件数の30%）



JIPDEC苦情相談事例

【取得/利用等に関する相談】

- 業者が明示した利用目的に同意した覚えはないが、無料サービスを使っただけで個人情報が利用され、会員サービスを勧める電話がかかってきた。
- 本人確認に利用するという理由で運転免許証の写真をスマホのカメラで撮られたが、写真データの拡散の可能性を考えると、個人情報の取得方法として問題があるのではないか。
- 通信関係のサービスを申し込んだときに、別会社が運営するサービスにも申し込んだことにされており、結果として、別会社に個人情報が提供されてしまった。

【安全管理に関する相談】

- 部外者の入館に関するルール（入館の記録、入館証の携帯）があるにもかかわらず、社長が家族・知人を社内に連れてくるときには、ルールが守られていない
- イントラ上の上司のフォルダーに、部下の給与額等が記載されている資料が保管されているが、資料にパスワードはかかっておらず、また、誰もがアクセスできる状況であり、問題がある
- 店舗で苦情を言ったところ、対応した店員から私の知り合いに、そのことが伝わっていた
- 料金未納で契約が強制解除となったことを、義理の家族にまで話されてしまった

主な法令/ガイドラインの制定/改定状況（2018年4月～2019年3月）

法令/ガイドライン名	制定/改定日	主な制定/改定内容
個人情報の保護に関する法律	30/07/27	IR法制定に伴い事業所管大臣（46条）に追記
個人情報の保護に関する法律についてのガイドライン（通則編）	31/01/23	十分性認定により移転を受けた個人データの取扱いに関する「補完的ルール」に関する追記
個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）	31/01/23	十分性認定により移転を受けた個人データの取扱いに関する「補完的ルール」に関する追記
不正競争防止法	30/05/30	限定提供データの不正取得等を不正競争行為として追加、技術的制限手段に係る規律強化
行政手続における特定の個人を識別するための番号の利用等に関する法律	30/06/29	国税分野における番号法に基づく本人確認方法等の追記

マイナンバー関連情報

【個人情報保護委員会情報】

- 2017年度の事故報告件数は、374件（重大な事態：5件含む）→2016年度は165件

- 地方自治体でのマイナンバーを含む書類の誤送付や誤交付が、多い
- 重大な事態（5件）：100件超のマイナンバー記載書類の紛失（4件は事業者、1件は地方自治体で発生）
- 行政機関6件、地方自治体18件、事業者3件を立入検査
- マイナンバー漏洩の報告を受け付けた際、173件の指導/助言

【マイナンバーを取り扱う業務委託に関する留意点：JIPDEC HP　2019/1/9】

- Pマーク付与事業者がマイナンバーを取り扱う業務を受託した際に、関係法令の規定に反し（委託元の許諾を得ずに）、マイナンバーを取り扱う業務の一部を第三者に再委託する事案が複数件発生
- マイナンバー取り扱い業務を受託し再委託する場合は、第三者に再委託することについて委託元の許諾を得ること、再委託先がマイナンバーを保護するための十分な措置を講じているか等を確認する等、組織として責任ある判断ができる仕組みを構築し運用

Windows7のサポート終了

【終了日】

2020年1月14日

【サポートが終了すると】

- Windows 7 の継続使用は可能
- 使用PCのセキュリティリスク（ウイルス被害等）を受ける可能性が高まる
- 技術的サポートが受けられない
- Windows Update からのソフトウェア更新は、利用できない
- Microsoftでは、2020年1月までにWindows10への移行を強く推奨

https://support.microsoft.com/ja-jp/help/4057281/windows-7-support-will-end-on-january-14-2020

【メインストリームサポート期間】

- 発売後5年程度は、セキュリティ更新やセキュリティ関連に関わらず新たな機能の追加、無償サポート
- Windows 8.1は、2018年1月まで
- Windows 10は、2020年10月まで

【延長サポート期間】

- メインストリームサポート期間終了後5年程度は、延長サポート期間
- セキュリティ更新や有償サポート新規の機能追加はない
- Windows 8.1は、2023年1月まで
- Windows 10は、2025年10月まで

新たな情報セキュリティー関連規格（ISO27017/ISO27018とは）

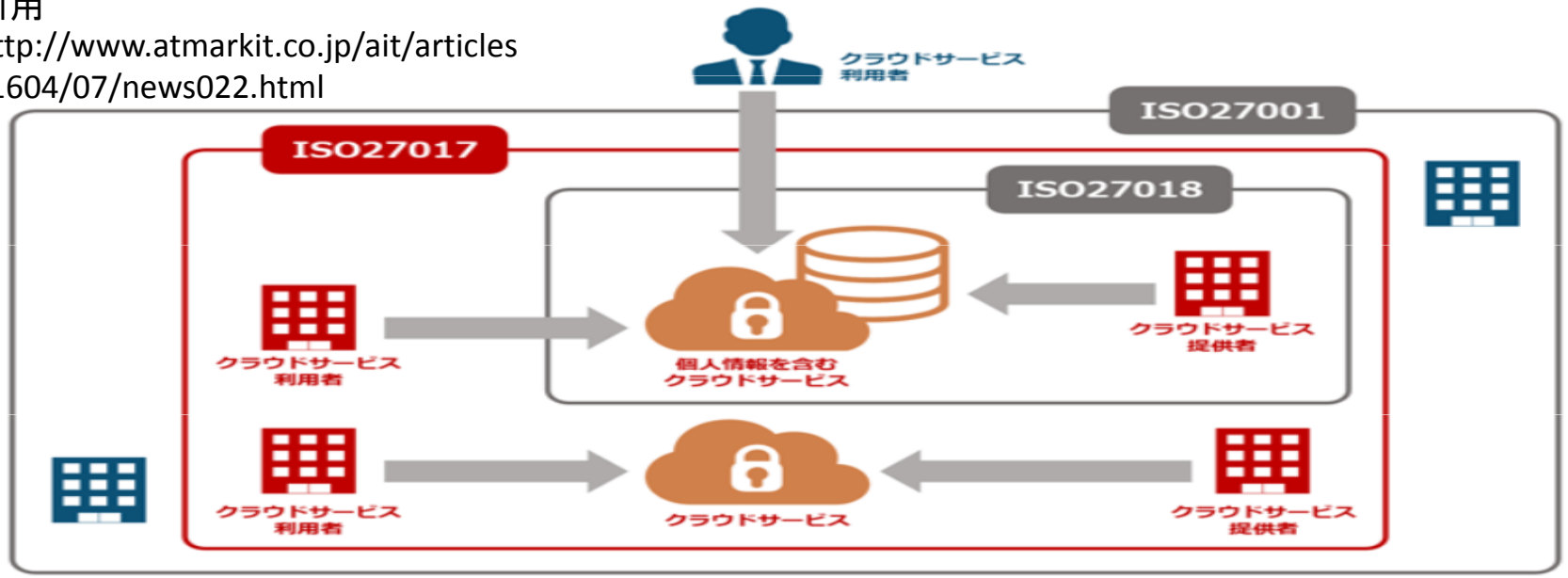
【 ISO27017 】

- クラウドサービスのための情報セキュリティ管理策の実践的規範
- クラウドサービスの提供や利用に対して適用されるISO27001規格を補完するクラウドセキュリティ規格（ガイドライン）
- ISO27001に追加管理策を79追加
  クラウドサービス提供者、又は利用者側の立場で取得することが可能
- 日本国内の認証：約100組織

【 ISO27018 】

- パブリッククラウドでのクラウドサービス事業者個人情報保護の実施基準
- クラウドサービス提供者がパブリッククラウド上で管理する個人情報に焦点を当てたISO27002を補完するガイドライン
- ISO29100のセキュリティ原則を適用
- ISO27001に追加管理策を39追加）
- Microsoft 、AMAZON、Google、ChatWork、TKCも取得

引用
http://www.atmarkit.co.jp/ait/articles/1604/07/news022.html



その他情報

【IPA】

- SECURITY ACTION
  - 「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度

- 中小企業の情報セキュリティ対策ガイドライン
  https://www.ipa.go.jp/files/000055520.pdf

- 新5分でできる情報セキュリティ自社診断
  https://www.ipa.go.jp/files/000055848.pdf

【日本規格協会】

- 個人情報保護マネジメントシステム導入・実践ガイドブック正誤表（2019/4/1）
  https://webdesk.jsa.or.jp/books/W11M0100/index/?syohin_cd=330546

【JIPDEC】

•社内教育用参考資料を作成/公表（2019年5月21日）しました。教育資料作成などにお困りの事業者はご活用ください。

https://privacymark.jp/system/reference/index.html#tools

【個人情報保護委員会】

・「Privacy Awareness Week」制定
2019年度は5月27日から6月3日

https://www.ppc.go.jp/enforcement/cooperation/privacy_awareness_week/

GDPR（General Data Protection Regulation）とは（1/3）

【GDPR】
・個人データ保護に対する権利という基本的人権の保護を目的とした法律（EU基本権憲章）

【適応開始/適応地域】
・2018年5月25日
・EEA＝EU28カ国＋アイスランド、リヒテンシュタイン、ノルウェー
→以下EU域内

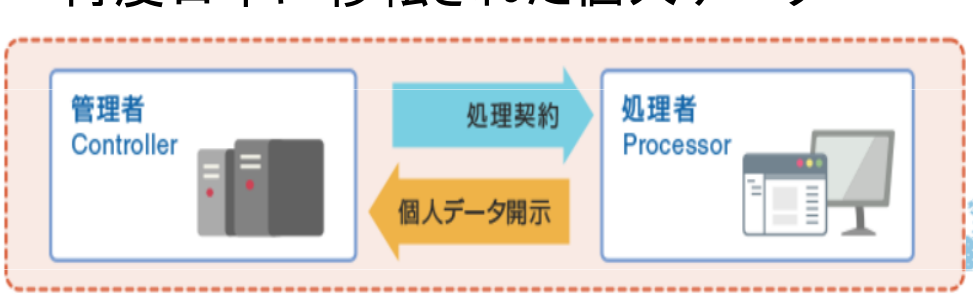
【特徴】
- 適正な管理が必要とされ、違反に対しては厳しい行政罰を適用
- 原則的に組織規模/公的機関/非営利団体等関係なく対象
- 個人データの取扱い状況によっては、EU域内にデータ保護責任者や代理人を選任

【原理原則と十分性認定】
- GDPRでは、EU域内から域外への個人データの移転は、原則禁止
- 以下の条件を満たす場合は、EU域内から域外への個人データの移転が可能
  - SCCによる契約の締結：データ移転元と移転先との間で、欧州委員会が認めた雛形条項による契約を締結
  - BCRの整備：企業グループで1つの規定を策定し、データ移転元の管轄監督機関が承認
  - 十分性認定：欧州委員会からデータ移転先の国が、個人データ保護についての“十分性認定”を受ける

GDPR とは（2/3）

【適用対象個人データ】
- EU域内に所在する個人データ（国籍や居住地などを問わない）
- 短期出張中や短期旅行中、日本へ移転するEU域内の日本人の個人データ
- 日本企業からEU域内に出向した従業員の個人データ
- 日本からEU域内に移転/処理され、再度日本に移転された個人データ

【適用範囲 】
- 管理者又は処理者がEU域内で行う処理に対して適用
- 管理者又は処理者がEU域内に拠点がない場合も、以下の場合には適用
  - EU域内のデータ主体に対し商品又はサービスを提供する場合
  - EU域内のデータ主体の行動を監視する場合



引用：http://www.intellilink.co.jp/article/column/security-gdpr01.html

GDPRとは（3/3）

【個人データ（例）】

- 氏名
- 識別番号
- 所在地データ
- メールアドレス
- オンライン識別子（IPアドレス、クッキー）
- クレジットカード情報
- パスポート情報
- 身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因

【日本の対応】

- 平成30年9月に、個人情報保護委員会は、GDPR対応に関して、「補完的ルール」を公表
- Pマーク審査での対応方針
  - Pマークの審査では、「補完的ルール」対象事業者が個人情報保護法の一部として当該ルールに対応していることを確認する

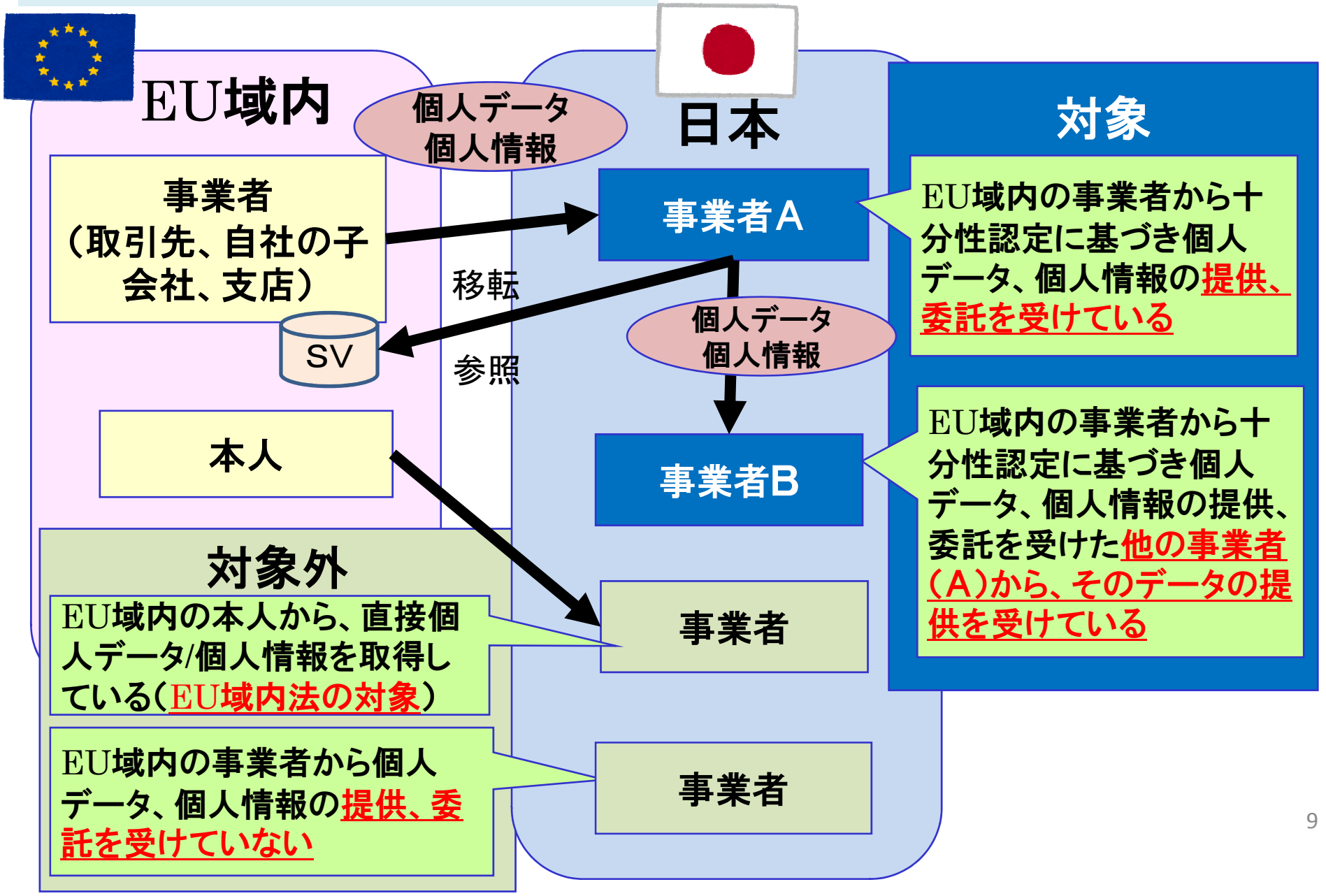
2019.01.24 THU 08:00

グーグルの「GDPR」違反から見えた、個人データ収集を巡るいくつかの課題

フランスのデータ保護当局が、EUの一般データ保護規則（GDPR）への違反があったとしてグーグルに5,000万ユーロ（約62億円）の制裁金を科すことを明らかにした。個人データ収集の同意に“不備”があったというが、そもそもGDPRには不明瞭な部分も多い。今回の一件を通じて、個人データの収集とテック企業のビジネスにまつわる課題が浮き彫りになってきた。

引用https://wired.jp/2019/01/24/eu-privacy-law-snares-google/

補完的ルールの確認対象事業者



補完的ルールの確認対象事Pマーク審査での追加確認項目（1/2）

JISQ15001関連項番	確認項目
補完的ルールの確認対象事業者か否かの確認	対象事業者の有無を確認する
A.3.3.1/3.3.3個人情報の特定及びリスクアセスメント	「当該情報」を特定して、リスクアセスメントしている
A.3.4.2.3要配慮個人情報	「当該情報」に「労働組合」、「性生活」、「性的指向」に関する情報が含まれている場合、要配慮個人情報として取扱う手順があり、運用している あらかじめ書面による本人の同意を得ている
A.3.4.4.1個人情報に関する権利	―

補完的ルールの確認対象事Pマーク審査での追加確認項目（2/2）

JISQ15001関連項番	確認項目
A.3.4.2.1利用目的の特定 A.3.4.2.6利用に関する措置 A.3.4.2.8.3第三者提供を受ける際の確認など	「当該個人情報」の提供を受ける際に、利用目的を含め、その取得の経緯を確認し、記録する手順があり、運用を記録している 「当該個人情報」については、記録確認義務を通じて確認した利用目的の範囲内で当該個人情報を利用している
A.3.4.2.8.1外国にある第三者への提供の制限	「当該個人情報」を外国にある第三者に提供する場合、本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供した上で、外国にある第三者に提供する同意を得る手順があり、情報を提供した上で、同意を得ている
A.3.4.2.9匿名加工情報	「当該個人情報」については、加工方法等情報を削除することにより、匿名化された個人を再識別することを何人にとっても不可能とした場合に限り、匿名加工情報とみなす手順があり、運用している

Tカードの個人情報の取扱い（第三者提供）

【事件概要】

- 「Tカード」を展開する会社が、氏名や電話番号といった会員情報のほか、商品購入によって得たポイント履歴やレンタルビデオのタイトルなどを、裁判所の令状なしに捜査当局へ提供していた。
- Tカード会員数は約6,700万人で、提携先は多業種に広がる。当局は、内部手続きの「捜査関係事項照会」を使い、どの店をどのような頻度で利用するか等の情報を入手していた。
- 運営会社は「捜査機関からの要請や協議の結果、法令やガイドラインにのっとり、開示が適切と判断された場合にのみ、必要な情報を提供すると決定した」と説明していた。

（東京新聞2019年1月21日記事を要約）

【解説】

- 個人情報保護法では、「個人情報取扱事業者は、法令に基づく場合や国の機関等へ協力する場合等を除き、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」旨を規定
- JISQ15001A.3.4.2.8でも、同様に規定

【この記事からわかること】

- 法律やJIS規格と人々の意識感情は異なっている
  →リスクアセスメントが必要

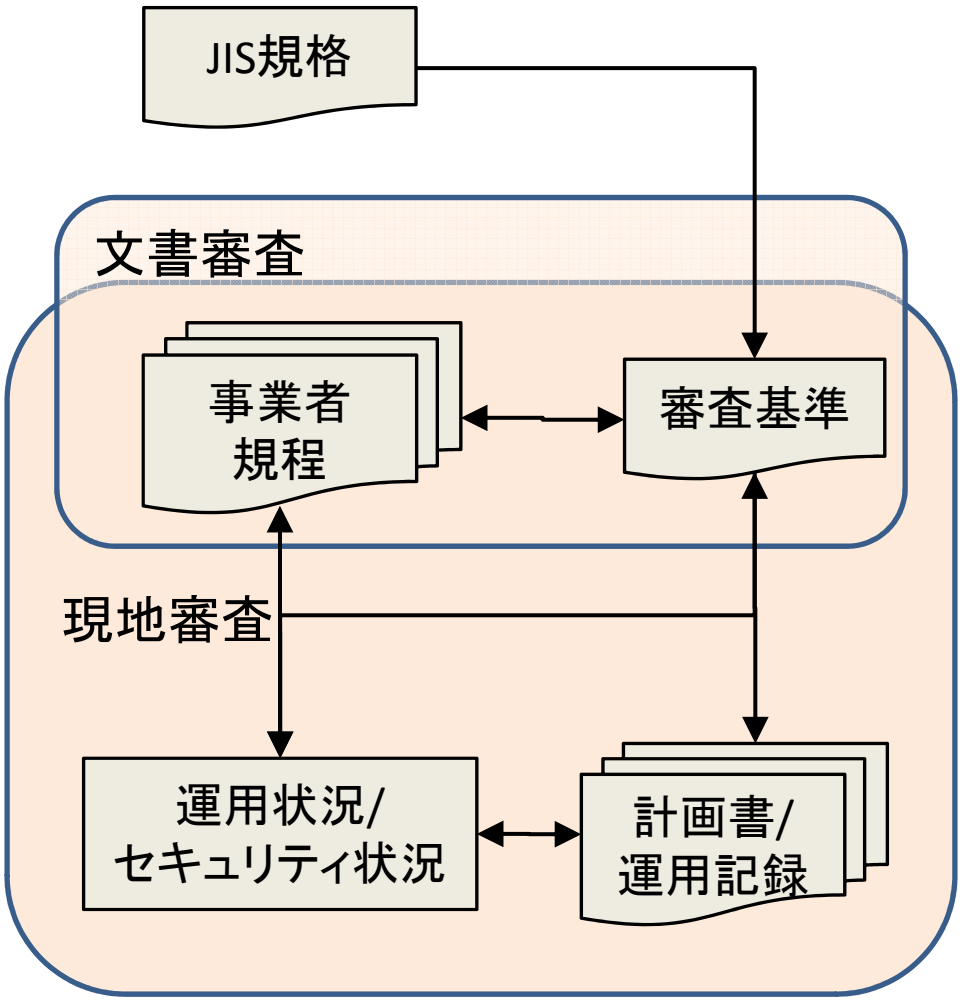
https://www.tokyo-np.co.jp/article/national/list/201901/CK2019012102000110.html

Ⅲ.新審査基準での審査状況(1/3)

【新審査基準について】

- JISQ15001:2017を基に策定された「審査基準」に基づき、審査実施中
- JIPDEC　HPで公開
  https://privacymark.jp/system/guideline/pdf/pm_shinsakijun.pdf

- 新審査基準では審査基準項目が集約/統廃合(362⇒126項目)された→定型的PMS及び定型的審査への反省
- 現地審査では、事業者規程も判定基準の一つとして、規程を順守していなければ、指摘対象となる場合がある。



Ⅲ.新審査基準での審査状況(2/3)

【新審査基準での審査開始】

2018年8月1日の申請受付分より

現在は新審査基準で審査実施中

【新審査基準への対応】

2020年7月31日申請受付分までは、移行に関する特例を適用中

「継続的改善事項に準ずる指摘」

- 指摘事項だが、3か月以内の是正処置でなく、次回の更新審査までの対応で可
- 対応/運用事業者は、指摘事項

【申請様式 7】JIS Q 15001 との対応表

※あてはまるものに☑をしてください。

□申請時点で、JISQ15001：2006 を適用して構築運用している

□申請時点で、JISQ15001：2017 に適合する様に規程類を見直したが運用していない

□申請時点で、JISQ15001：2017 を適用して構築運用している

(申請事業者の内部規程・様式が JIS Q 15001:2017 要求事項 附属書 A の全項目に対応

【参考：更新事業者が審査時に】(原則として)

①JISQ15001：2006で運用構築の場合
・新審査基準項目の指摘
→「継続的改善事項に準ずる指摘」

②JISQ15001：2017に規程類を適用、運用はしていない(これから運用)
・新審査基準項目の指摘
規程について→指摘事項
運用→「継続的改善事項に準ずる指摘」

③JISQ15001：2017に規程類を適用、構築運用している
・新審査基準項目の指摘　→指摘事項

※構築運用している状態とは、PMSの計画から始まり、特定、リスク分析、教育、監査、Mレビュー、是正処置等のPDCAサイクルが全て一回りした状態のこと

Ⅲ.新審査基準での審査状況(3/3)

【新審査基準受審済み事業者の対応状況】
(中産連調べ)

＜対象期間＞
2019年1-3月申請分事業者(約130事業者)

＜見直し・構築・運用状況＞
申請時点で、
・2006年版のまま運用している
→75事業者
・2017年版に規程を見直しているが、運用はこれから →40事業者
・2017年版を適用/運用している
→15事業者(ほぼ新規)

＜適用済み事業者の規程/マニュアル類の状況＞

①従来の2006年版規程を生かした一部改訂が多い(用語の見直し、追加要求項目を付加)
②JISQ15001規格本文も加えた全面改訂もちらほら

現地審査での指摘事項(1/3)
(継続的改善事項に準ずる指摘)

条項	審査項目	指摘事項
A3.1.1 一般	①A.3.2からA.3.8の管理策について,定めた手段に従って承認していること	規定で定めた権限者が、「個人情報管理台帳」/「監査計画書」等を承認していない
A.3.3.1 個人情報の特定	③「(個人情報管理)台帳」には,少なくとも以下の項目が含まれていること 個人情報の項目、利用目的、保管場所、保管方法、アクセス権を有する者、利用期限、保管期限	①「(個人情報管理)台帳」に、左記の項目設定していない。 ②利用目的の範囲内での利用期限とその後の保管期限を一律的に特定している
A.3.3.3 リスクアセスメント及びリスク対策	③特定した個人情報保護リスクに対して、現状で実施し得る対策を内部規程として文書化していること ⑤未対応部分を残留リスクとして把握し,管理していること ⑥個人情報保護リスクの特定,分析及び講じた個人情報保護リスク対策を少なくとも年一回,適宜に見直していること	①実施しているリスク対策を文書化していない ②クラウドサービス特有のリスク(セキュリティ対策が不明等)について、残留リスクとして把握/管理していない

現地審査での指摘事項（2/3）
（継続的改善事項に準ずる指摘）

条項	審査項目	指摘事項
A.3.4.2.8.2 第三者提供に係る記録の作成など （A.3.4.2.8.3 第三者提供を受ける際の確認など）	①個人データを第三者に提供した場合，記録を作成，保管していること。 ②記録を作成しなかったのは，A.3.4.2.3のa)～d) のいずれかに該当する場合，又は左記a)～c)の場合に限定していること。	左記に関する局面があるにも関わらず、その手順がなく運用していない（記録を作成していない、但し書きの適用手順がない）
A.3.4.2.9 匿名加工情報	①匿名加工情報の取扱いを行うか否かの方針が存在すること。 ②匿名加工情報を取り扱う場合，匿名加工情報の取扱いの手順を内部規程として文書化していること。	匿名加工情報を取扱うか否かを決定していない、 及び取り扱う場合はその取り扱い手順を文書化していない

現地審査での指摘事項(3/3)
(継続的改善事項に準ずる指摘)

条項	審査項目	指摘事項
A.3.4.3.1 正確性の確保	②利用する必要がなくなった個人データの消去を含む管理を，規定に基づいて適切に行っていること。	「個人情報管理台帳」で特定した保管期限を超えた個人情報を規定に基づいて処分していない (人事労務関連書類の法定保管期限参照)
A.3.4.3.2 安全管理措置	①取り扱う個人情報の個人情報保護リスクに応じた安全管理措置を講じていること。	規定された安全管理措置を実施していない (安全管理措置の確認手段の変化による)
A.3.4.5 認識	①全ての従業者に対して、少なくとも年一回、適宜に教育を実施する手順が内部規程として文書化されていること。 ④全ての従業者に対して，a)～d)の内容を認識させていること。 a)個人情報保護方針 b)個人情報保護マネジメントシステムに適合することの重要性及び利点	a)個人情報保護方針を教育/認識させる手順を文書化していなくて、実施していない

新審査基準対応へPMSの見直しに向けて（1/2）

【Pマーク認証の目的は何か】
- 顧客のニーズ/期待、要求事項
- 自社のセキュリティルールの確立/運用

【対応ポリシー】
- 要求事項の追加/差分だけ対応する
- 従来よりも事業者の規模/事業内容/リスクに応じて、自社の運用に合わせて、全般的に見直しする（但し書き等の表記や様式類を含めて）

【参考情報】
- JISQ15001：2017対応個人情報保護マネジメントシステム導入・実践ガイドブック https://webdesk.jsa.or.jp/books/W11M0100/index/?syohin_cd=330546

【対応済の規程類の傾向】
- 保護マニュアル目次は、JISQ15001付属書Aをほぼそのまま流用している
- 用語は、JISQ15001：2017規格に合わせて変更している
- 「個人情報管理台帳」/「個人情報取扱申請書」/「計画書」を改訂している
- 新たに「第三提供に係る記録」を作成している、又は従来より活用している「授受記録」を活用している

- JISQ15001：2017をほぼそのまま記述していて、自社規程として理解/活用しにくい

新審査基準対応へPMSの見直しに向けて（2/2）

【運用の傾向】

- 個人情報保護方針は、内部向け/外部向けを分けていない
- 「リスク分析表」や「セキュリティ規程」に記載したリスク対策と実際のリスク対策が大幅に乖離している→指摘の対象になる場合がある
- どの様な場合に但し書きを適用するのか運用に落とし込まれていない（第三者提供に関して記録が不要な場合等）→指摘の対象になる場合がある
- 自社規程の規定事項を運用していない→指摘の対象になる場合がある

【「適宜に」の意図】

- 新審査基準で、「適宜に」の運用を求めている項目は、見直し後に運用がなければ、指摘の対象になる場合がある
  - 個人情報台帳を適宜に確認
  - 個人情報保護リスク対策を適宜に見直し
  - 従業者に対して、適宜に教育
  - 個人情報保護管理者は、適宜にトップマネジメントに運用確認の状況を報告
  - 個人情報保護マネジメントシステムのこの規格への適合状況を適宜に実施
  - 適宜にマネジメントレビューを実施

お問合わせ先：
一般社団法人中部産業連盟
Pマーク審査センター
〒461-8580　名古屋市東区白壁3-12-13
Tel:052-931-7701　Fax:052-931-7702
E-mail : p-mark@chusanren.or.jp