

個人情報など、機密性の高い情報を クラウドで扱うための注意事項

虎ノ門南法律事務所

弁護士 上沼 紫野

はじめに

クラウドで扱う情報のうち最も注意を要する情報は？

- **第1 現行個人情報保護法について**
- **第2 改正個人情報保護法について**
- **第3 マイナンバー**

第1 現行個人情報保護法

■ 1 法の定める義務の内容

情報・データの種別			要求される義務の内容	該当条文
個人情報 (個人情報取扱事業者はも 個人データでなく 負っている義務)	個人データ (個人データ等 を構成する 情報)	有個人データ (開示、訂正、 削除、利用停止、 保守等の義務)	利用目的の特定	15条
			利用目的による制限	16条
			適正な取得	17条
			利用目的の通知等	18条
			データ内容の正確性の確保	19条
			安全管理措置	20条
			従業者の監督	21条
			委託先の監督	22条
			第三者提供の制限	23条
			保有個人データ事項の公表	24条
			上記開示	25条
			上記訂正等	26条
			上記利用停止等	27条

第1 現行個人情報保護法

2 クラウド上に個人情報を保管すること

■ 個人情報保護法23条(第三者提供の制限)

原則) 予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。

例外) 個人データの提供を受ける者が第三者とされない場合

- ① 個人データの取扱の委託
- ② 合併・事業譲渡
- ③ 共同利用

第1 現行個人情報保護法

3.1 クラウド事業者に個人情報の取扱を委託する場合

■ ユーザーの義務

個人情報保護法20条 安全管理措置

- ・個人データの安全管理のために必要かつ適切な措置
- 具体的には

組織的安全管理措置(規程・手順書の整備)

人的安全管理措置(従業員の教育、秘密保持)

cf. 21条従業員の監督 22条委託先の監督

物理的安全管理措置(入退室の管理等)

技術的安全管理措置(システムへのアクセス制御等)

第1 現行個人情報保護法

3.2 クラウド事業者に個人情報の取扱を委託する場合

安全管理措置の具体化

22条 委託先の監督(ユーザー自身に要求される義務)

- ① 委託先を適切に選定すること(事前に安全管理措置を確認)
- ② 委託先に安全管理措置を遵守させるために必要な契約を締結すること
- ③ 委託先における委託された個人データの取扱状況を把握すること

第1 現行個人情報保護法

■ 3.3 クラウド事業者に個人情報の取扱を委託する場合(1) 金融庁ガイドライン(平成27年7月9日改正。改正点は下線)

第12条(委託先の監督)

- 1 監督の程度: 本人の権利利益侵害の程度、委託する事業の規模、性質、個人データの取扱状況等に起因するリスクを考慮
- 2 委託先の適正な選定(再委託の場合は、再委託先の監督状況についても監督が必要)

必須	望ましい
・委託先選定基準の <u>定期的見直し</u>	・選定にあたり現地調査その他の合理的な方法による確認を行い、 <u>個人データ管理責任者が適切に評価すること</u>
・契約内容(監督・監査権限、改ざん・目的外利用の禁止、再委託条件、漏えい時の委託先の責任) ・ <u>定期的な見直し(監査等)</u>	・再委託の際、 <u>事前報告・承認手続き、再委託先の定期的な監査など、再委託先の安全管理措置を十分に確認すること</u>

第1 現行個人情報保護法

■ 3.3 クラウド事業者に個人情報の取扱を委託する場合(2)

金融庁安全管理実務指針(平成27年7月9日改正)

・外部委託に係る規程の整備(盛り込むべき内容)

①選定基準 ②委託契約に盛り込むべき安全管理の内容

・ガイドライン12条「委託先の監督」について

➤ 基準として定める内容、基準にそった選定、基準の定期的な見直し

①委託先の安全管理指針・取扱規程の整備

②安全管理の実施体制の整備

③実績等に基づく信用度

④委託先の経営の健全性

第1 現行個人情報保護法

■ 3.3 クラウド事業者に個人情報の取扱を委託する場合 契約に盛り込むべき内容(経産省ガイドライン)

- ・委託元及び委託先の明確化(委託先責任者等)
- ・個人データの安全管理に関する事項
 - 個人データの漏えい、盗用禁止
 - 委託契約範囲外の加工・利用、複写・複製の禁止
 - 委託契約期間
 - 契約終了後の個人データの返還・消去・廃棄に関する事項
- ・再委託に関する事項(事前報告又は承認、再委託先の監査)
- ・個人データの取扱状況に関する報告(内容・頻度)
- ・契約内容遵守の確認(監査など)
- ・契約内容不遵守の場合の措置(損害賠償等)
- ・事故発生時の報告・連絡

第1 現行個人情報保護法

4 安全管理措置の程度

対象たる情報が機微情報

→ 要求される安全管理措置のレベルは高くなる

cf. 経産省ガイドライン

- ・漏えい等の場合に本人が被る権利利益の侵害の程度を考慮
- ・事業の性質及び個人データの取扱状況等に起因するリスクに応じた

→ 必要かつ適切な措置



総合的に考慮(ワン・ゼロの世界ではない)

cf. 金融庁安全管理実務指針

機微(センシティブ情報)の取扱

第1 現行個人情報保護法

5 個人情報保護法違反が問題となる状況

個人情報保護法違反 が 直ちに損害賠償とはならないが..
プライバシー権の侵害として問題になり得る
...「公表」がなくても、不適切な使用が侵害となり得る

裁判例:

Nシステム(公権力によるものではあるが)東京地判平13・2・6
客室乗務員データベース事件 東京地判平22・10・28

第1 現行個人情報保護法

6 プライバシー侵害の裁判例(1)

Nシステム事件

道路上の自動車ナンバー読み取りシステム端末による情報の収集等が、肖像権、情報コントロール権を侵害するとの主張

→ 裁判所の基準

①情報の性質(思想、信条、品行等に関わるか)

②利用の目的が正当なものか

③利用の方法が正当なものか

を総合して判断すべき

第1 現行個人情報保護法

6 プライバシー侵害の裁判例(2)

客室乗務員データベース事件

従業員の詳細なデータベースの作成、保管、使用がプライバシー権を侵害するか

・内容には、宗教、支持政党、病歴等のセンシティブ情報、不適切な表現等が含まれていた

裁判所)

1) 一般人の感受性を基準にして人格的自律ないし私生活上の平穩を害する態様で収集、保管又は使用された場合、プライバシー侵害となる。

→ 原則は同意を必要として、行為態様毎に判断

2) 保管について、情報流失防止に対する措置が十分に整えられておらず、流出の具体的危険がある状態で保管することは、同意の範囲を超える (プライバシー侵害)

第1 現行個人情報保護法

7 安全管理措置とプライバシー侵害

プライバシー侵害 → 不法行為（故意・過失が必要）

（1）流出がなくても安全管理措置なき保管自体がプライバシー侵害とされる可能性

（2）流出があってもただちに損害賠償となるわけではない
情報の性質に応じた安全管理措置が講じられている場合
→ 過失なく、損害賠償責任が認められない可能性あり

第1 現行個人情報保護法

8 個人情報漏洩の場合の損害賠償

機微性の高さによって異なる

- ・講演会名簿提出事件(東京高判平16・3・23): 5000円
- ・ISPサービス加入者の個人情報流出(大阪地判平18・5・19): 5000円
- ・住民基本台帳データ流出(大阪高判平13・12・15):
10000円(+5000円弁護士費用)
- ・エステティックサロンデータ(東京地裁判平19・2・8):
30000円(+5000円弁護士費用)

損害賠償額という点からも

機微性の高い情報は、高い安全管理措置を講じるべき

第2 改正個人情報保護法

改正個人情報保護法

平成27年8月28日成立

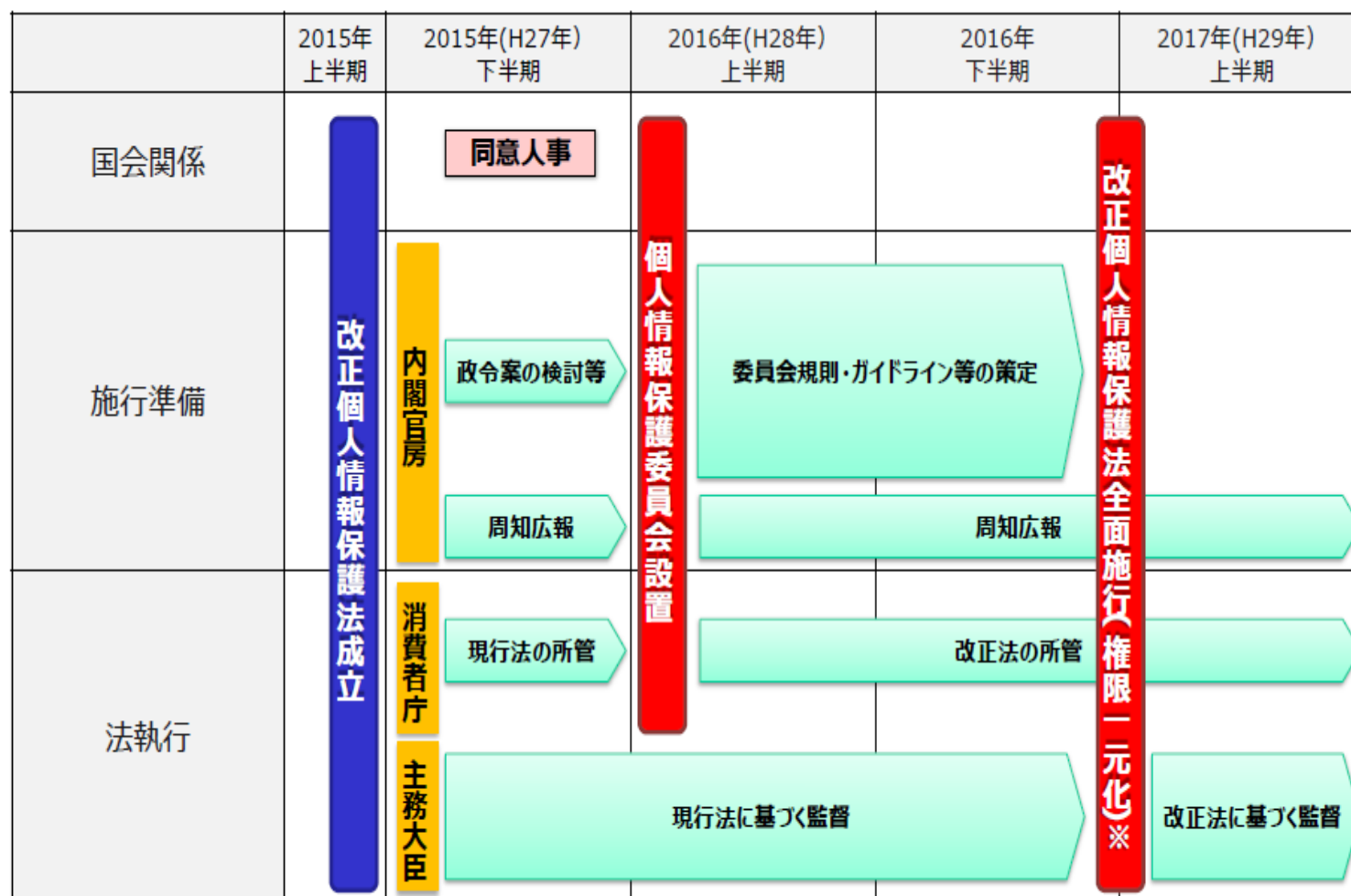
公布) 平成27年9月9日

施行)

公布の日から起算して2年を超えない範囲内において政令で定める日

第2 改正個人情報保護法

2 スケジュール



※「公布の日から起算して二年を超えない範囲内において政令で定める日」から施行。

第2 改正個人情報保護法

3 概要

(1) 個人情報の定義

- ・明確化、要配慮個人情報(原則取得禁止)

(2) 適切な規律の下で個人情報の有用性を確保

- ・匿名加工情報、個人情報保護指針(委員会に届出、公表)

(3) 個人情報保護の強化

- ・トレーサビリティの確保、データベース提供罪

(4) 個人情報の取扱いのグローバル化

- ・外国の事業者への法の適用
- ・外国事業者への第三者提供の禁止

(5) 個人情報保護委員会

第2 改正個人情報保護法

4 クラウドでの取扱いに特に関係する部分

(1) 外国にある第三者への個人データの提供①

新24条

外国にある第三者に個人データを提供する場合には、外国にある第三者への提供を認める旨の本人の同意が必要

例外)

同等性認定:

- ・ 個人の権利利益を保護する上で日本と同等の 保護水準と個人情報保護委員会規則で定めた外国
- ・ 個人情報取扱事業者が講ずべき措置として個人情報保護委員会規則で定める基準に適合する体制を整備している
第三者

第2 改正個人情報保護法

4 クラウドでの取扱いに特に関係する部分

(1) 外国にある第三者への個人データの提供②

新24条

外国にある第三者に個人データを提供する場合には、外国にある第三者への提供を認める旨の本人の同意が必要

以下が例外とされていない

委託、合併、共同利用等

→ 個人情報の取扱いの委託の場合も同条の規制がかかる

■ 外国のデータセンターは？

国会答弁では： 国内と同様の安全管理措置等を契約で定めていればOKという方向になるのではないか

第2 改正個人情報保護法

4 クラウドでの取扱に特に関係する部分

(2)トレーサビリティの確保

新25条

個人データを第三者に提供したときは、提供年月日、第三者の名称その他委員会規則で定める記録を作成しなければならない。

基本) 委託、合併、共同利用は入らないが...

例外) 24条が適用される場合(外国事業者への提供の場合)

委託、合併、共同利用の場合も含まれる

→ データ操作等のログを残す必要がある

(オンラインの場合別途記録は必要ない方向と言われているが)

第2 改正個人情報保護法

5 現状での情報の外国への移転

(1) 個人情報の保管場所の把握

安全管理の一環として必要ではと言われていた

(2) 輸出管理法制 特定の情報については、国外移転を制限

ex 兵器に関連した技術等

以下の契約が締結されている場合には適用を受けない

- ・ 利用者自らが使用するためにデータを保管することのみを目的とする契約
- ・ 犯罪捜査の裁判所命令、サービスを運営するために不可欠等による正当で特別な理由がない限りは、クラウドサービス提供者が利用者のデータを閲覧・取得することはないことが記されている契約

平成25年6月21日経済産業省貿易経済協力局長通達

第2 改正個人情報保護法

5 現状での情報の外国への移転

(3) 経済産業省個人情報ガイドライン

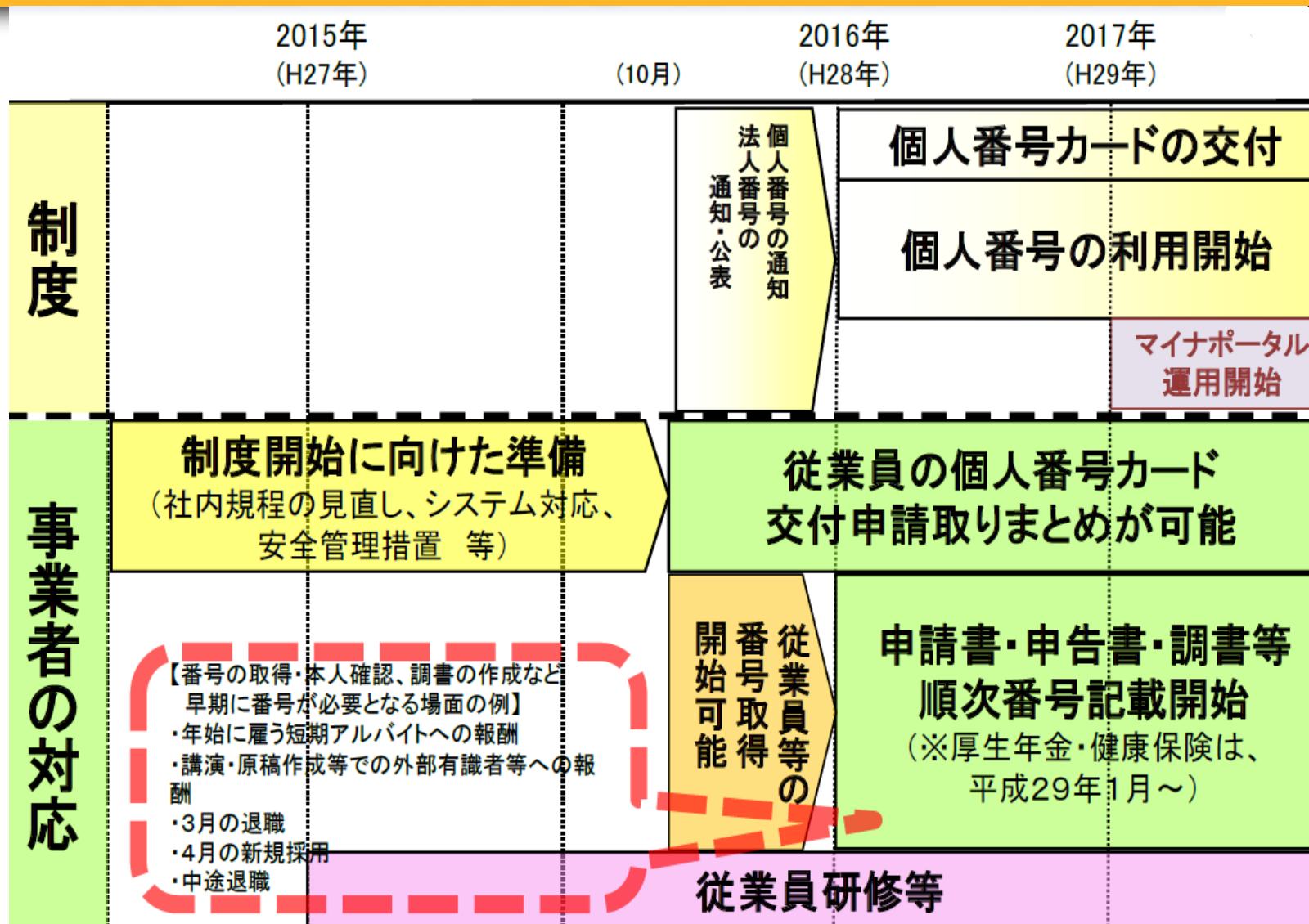
- ・・・個人情報取扱事業者の解釈についてではあるが・・・
(いわゆる5000人を超えるか否かの判定について)

→ 倉庫業、データセンター(ハウジング、ホスティング)の例
「事業の用に供しないため特定の個人の数に算入しない事例」

当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に、その情報中に含まれる個人情報(ただし、委託元の指示等によって個人情報を含む情報と認識できる場合は算入する)

第3 マイナンバー

1 マイナンバーのスケジュール



第3 マイナンバー

1 マイナンバー法

行政手続き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

2 仕組み

マイナンバーの取扱は、個人情報保護法の特則

個人番号(マイナンバー)を含む個人情報 → 特定個人情報

特定個人情報にも個人情報が適用される

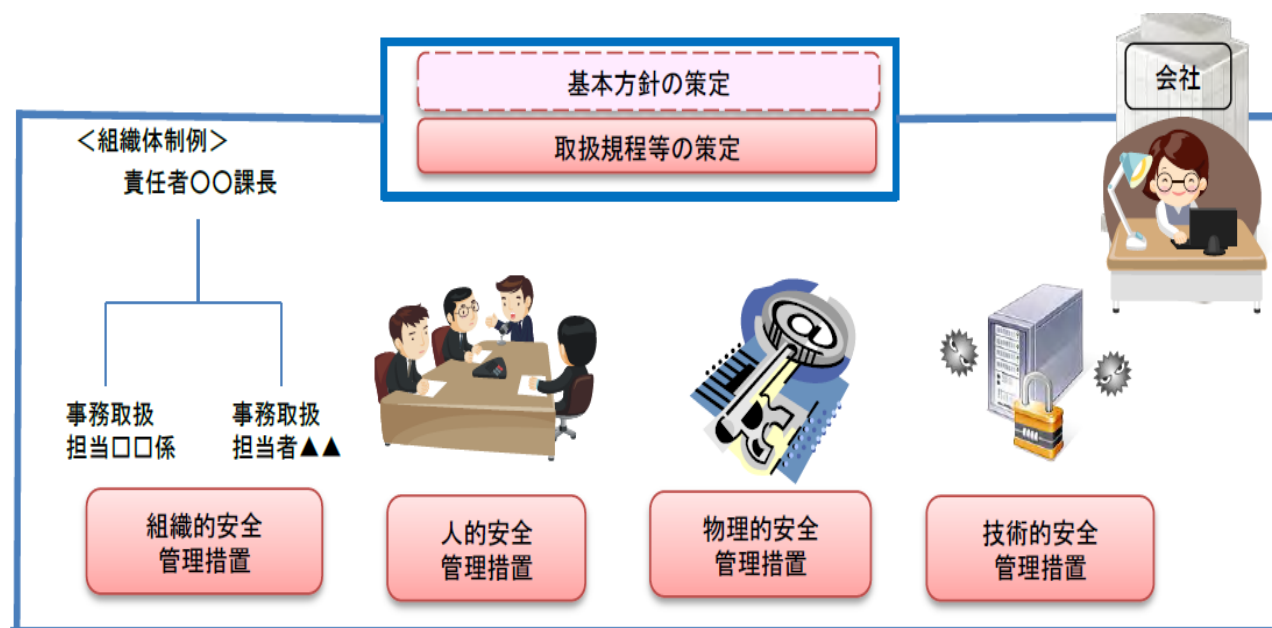
→ さらに、一定の制限が追加される

第3 マイナンバー

2 クラウド上での取扱いに特に関係する部分

安全管理措置

(特定個人情報情報の適正な取扱いに関するガイドライン(事業者編))



第3 マイナンバー

3 個人情報保護法の情報管理体制からの変更必要点

① 書類・データの削除・廃棄

個人番号関係事務を実施する必要がなくなり、法定保管期間が経過すれば

個人番号を削除・廃棄が必要

削除・廃棄についての記録が必要

② システムログ又は利用実績の記録

取扱規程等に基づく運用状況が確認するため

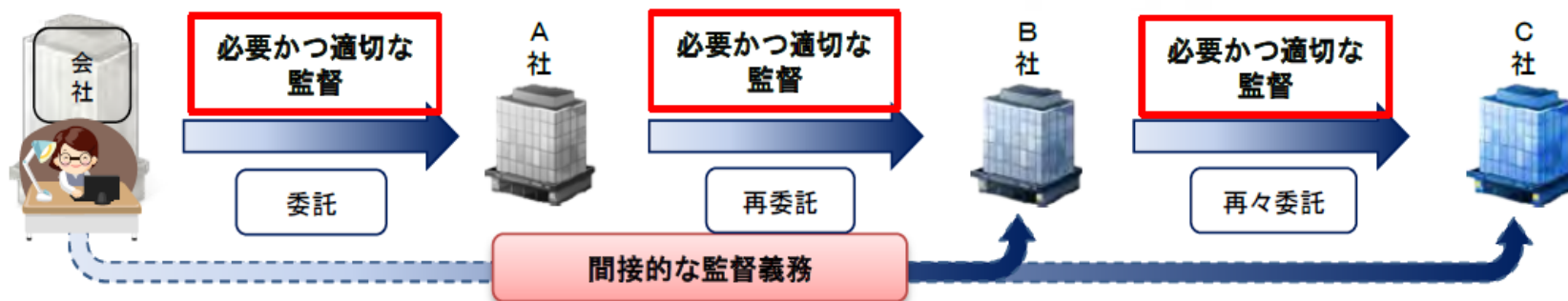
③ 特定個人情報ファイルの取状況を確認するための手段

ex 取扱台帳

④ 取扱区域における物理的安全管理措置

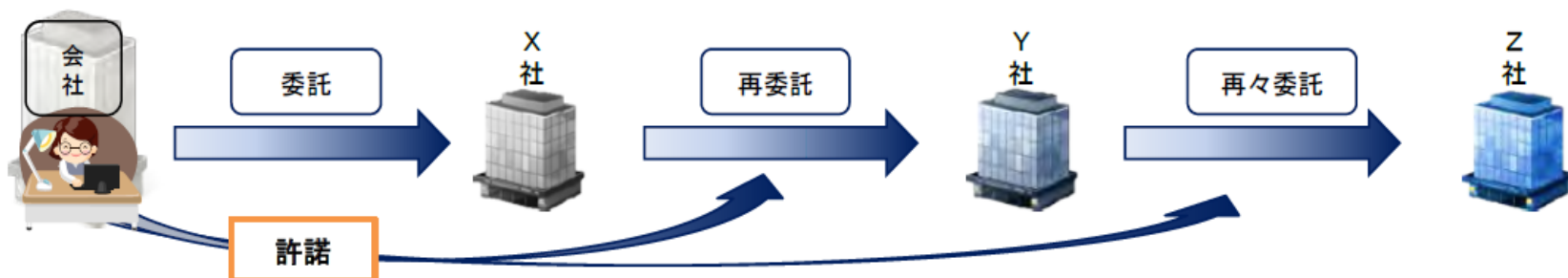
第3 マイナンバー

4 委託の場合



【委託先の監督】

○社会保障及び税に関する書類の作成事務の全部又は一部の委託をする者は、委託先において、法律に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければなりません。



【再委託】

○社会保障及び税に関する書類の作成事務の全部又は一部の委託を受けた者は、委託者の許諾を得た場合に限り、再委託をすることができます。

第3 マイナンバー

4 委託の場合(2)

委託先における安全管理措置

(特定個人情報保護委員会ガイドライン)

→ 必要かつ適切な監督

① 委託先の適切な選定

(自ら果たすべき安全管理措置と同等の措置が講じられていることの確認)

② 委託先に安全管理措置を遵守させるために必要な契約の締結

③ 委託先における特定個人情報の取扱状況の把握
(再委託の場合、再委託先に対しても間接的に監督義務を負う)

第3 マイナンバー

4 委託の場合(3)

契約における注意事項

- ① 委託先の安全管理措置を義務づける
- ② 再委託に関しては、委託元の同意を要する旨を記載
- ③ 委託先の書類・データの削除・廃棄に際し、証明書等の発行を義務づける
- ④ その他盛り込むべき内容(特定個人情報保護委員会ガイドライン)

盛り込むことが
義務

- ①秘密保持
- ②事業所内からの特定個人情報の持出の禁止
- ③特定個人情報の目的外利用の禁止
- ④再委託における条件(同意の要求を含む)
- ⑤漏えい事案等が発生した場合の委託先の責任
- ⑥委託契約終了後の特定個人情報の返却・廃棄
- ⑦従業者に対する監督・教育
- ⑧契約内容の遵守について報告を求める規定

盛り込むことが
望まれる

- ⑨特定個人情報を取り扱う従業者の明確化
- ⑩委託者が委託先に対して実施の調査を行うことができる規定

第3 マイナンバー

4 委託の場合(4)

個人情報保護法上の監督に追加して求められる事項
(特定個人情報保護委員会Q&A3-2)

- ・個人番号を取り扱う事務の範囲の明確化
- ・特定個人情報等の範囲の明確化
- ・事務取扱担当者の明確化
- ・個人番号の削除、機器及び電子媒体等の廃棄

→ 上記は、国外の事業者へ委託する場合も同じ(Q&A3-3)

第3 マイナンバー

5 クラウドに関するガイドライン(1)

特定個人情報保護委員会 ガイドラインQ&A

Q3-12 特定個人情報を取り扱う情報システムにクラウドサービスを利用していたら、委託に該当するか？

A 個人番号をその内容に含む電子データを取り扱うかどうか
が基準(取り扱わない場合は、事務の委託ではない)

取り扱わない場合とは？

- ・契約条項によって当該事業者が個人番号をその内容に含む電子データを取り扱わない旨が定められている
- ・適切にアクセス制御が行われている

第3 マイナンバー

5 クラウドに関するガイドライン(2)

Q3-13 クラウドサービスが番号法上の委託に該当しない場合、クラウドサービスのユーザーがクラウドサービス事業者に対し、監督を行う義務は課せられないか？

A クラウドサービスが番号法上の委託に該当しない場合、委託先の監督義務は課せられないが、クラウドサービスの利用者は、自ら果たすべき安全管理措置の一環として、クラウドサービス事業者内にあるデータについて、適切な安全管理措置を講ずる必要がある。

第3 マイナンバー

5 クラウドに関するガイドライン(3)

Q9-2 個人番号を暗号化等により秘匿化すれば、個人番号に該当しないか？

Q9-3 個人番号をばらばらの数字に分解して保管すれば個人番号に該当しないか？

・・・一定の法則に従って変換したものは個人番号
また、ばらばらにしても復元して利用するのが前提
となっているので、全体として、個人番号

第4 まとめ

- 1 現行個人情報保護法下では
クラウドサービスを用いた保管に同意は不要
ただし、安全管理措置を要する
- 2 改正個人情報保護法では
海外事業者への委託について
- 3 マイナンバー
個人情報保護法の特例
クラウド事業者との契約にも注意