資料２

第１３回ＯＤＲ推進検討会資料

（ＯＤＲを実施する際のセキュリティと規律の見直しの要否）

【論点１】ＯＤＲの適正な実施のためのセキュリティのあるべき姿について

※第１・第２フェーズを念頭

- インターネット等の情報通信技術への社会の依存度が高まるにつれ，情報セキュリティ対策はますます重要。
- とりわけ，ＡＤＲは，紛争当事者等の秘密がＡＤＲ事業者に開示されることで，紛争の実情に即した適切で納得感のある解決を図ることが可能。仮にそのような秘密が漏れるようなことがあっては，紛争当事者等に不利益が生じるだけでなく，ＡＤＲの信頼性も損なわれ，利用の促進は期待できない。
- ＯＤＲは，紛争当事者等の秘密が情報通信技術を通じて取り扱われるため，ひとたび情報が漏えいすれば，その拡散の範囲，程度は，従来型の対面手続と比較してより大きく，秘密保持，セキュリティ確保の要請は一層高い。

以上を踏まえ，ＯＤＲの適正な実施のためのセキュリティのあるべき姿をどのように考えるか。

- **セキュリティの在り方を検討する上で，どのような点に留意すべきか。**

  （例）

  ・企業，組織の情報セキュリティ対策として一般的に議論されているものについて，どのように考えるか。

  ・クラウドサービス等の他者のサービスを利用することの当否，留意点
- **ＯＤＲを実施する認証紛争解決事業者には，どのような水準の対策が求められるべきか。**

【論点２】　法・規則の規律の見直しの要否

※関連する規律は別表①，別紙の１参照

- 認証紛争解決事業者は，その業務につき，当事者に対する通知に係る基準（第６条第６号），秘密保持に係る基準（同条第１１号，第１４号），提出資料の保管等に係る基準（同条第１０号）に適合していることが求められるほか，手続実施記録の作成・保存が義務付けられている（第１６条）が，情報通信技術を活用すること自体は禁じられていないものと解される。
- もっとも，論点１の検討の結果次第では，現行の規律では，ＯＤＲの適正な実施を確保するためには必要かつ十分でないと考えられる場面が生じる可能性もある。

➢ 論点１の検討を踏まえ，現行の規律の見直しの要否について，どのように考えるか。

【論点３】　ガイドラインの見直しの要否

※ガイドラインの内容は別紙の２参照

□　法第６条第６号のガイドラインについて

- 現行法上，オンラインによる通知も許容されているものと解される。
- これまでの検討会での議論では，電子メールについては，通信の暗号化の観点からセキュリティレベルが高くない旨の指摘や，標的型攻撃メールによる情報漏えいのリスクからすると，セキュリティの観点からは必ずしも推奨される手法ではないのではないかとの意見。
- 他方，社会経済生活上，電子メールの利用はごく一般的なもので，ＡＤＲ実務上も，オンラインによる通知の方法として電子メールの利用が最も一般的。このような実情を踏まえつつ，適切な情報セキュリティ対策を求めて

いくことも，方法論としては十分にあり得るのではないか。

- **以上を踏まえ，現時点において，ガイドラインの見直しまでは必要がないと考えられるが，どうか。**

□　法第６条第１０号，第１６条のガイドラインについて

- 現行法上，資料の保管等の方法は限定されていないものと解される。
- もっとも，現行のガイドライン上は，例示として紙媒体の保管等を念頭に置いたものしかない。

- **資料，記録の電子化が許容されることを明確にする趣旨で，その旨をガイドライン上に明記することが考えられるが，どうか。**
- **クラウドサービスの利用が許容されるのであれば，その旨をガイドライン上に明記することが考えられるが，どうか。**

□　法第６条第１１号及び第１４号のガイドラインについて

- これまでの検討会での議論では，情報通信技術が日進月歩であることや，どのようなセキュリティ対策等を講じるかは認証紛争解決事業者のポリシーによるべき性質のものであるなどの指摘がされ，具体的基準等をガイドラインに記載すべきではないとの意見が大勢を占めた。
- 他方で，抽象的な文言であれ，セキュリティを適切に確保すべきことをガイドライン上に明記することも検討すべきではないかとの意見もあった。

- **以上を踏まえ，法第６条第１１号及び第１４号のガイドラインに，セキュリティの確保に関する記載をすることの当否，記載する場合の内容について，どのように考えるべきか。**