資料2

法令集ＱＡ一覧（案）　　update: 2019.12.3

※青背景：H21要求事項集からのアップデート ※赤背景：新規追加問

カテゴライズ（案）	No（案）	タイトル	トピック（Q）
A（総論）	0		第一部：各関係法令の紹介
A（総論）	0		サイバーセキュリティと法令全般
B1（内部統制）	1	内部統制とサイバーセキュリティとの関係	内部統制とサイバーセキュリティの関係はどのようなものか。
B1（内部統制）	2	サイバーセキュリティと取締役の責任	サイバーセキュリティ情報の漏えい、改ざん又は滅失（消失）若しくは毀損（破壊）によって会社又は第三者に損害が生じた場合、会社の役員（取締役・監査役等）は、どのような責任を問われ得るか。
B1（内部統制）	3	サイバーセキュリティ体制の適切性を担保するための監査等	社内の情報セキュリティ体制が適切であることを担保するためにどのような方策を実施することが考えられるか
B2（情報開示）	4	サイバーセキュリティと情報開示	企業は、サイバーセキュリティに関してどのような情報開示を行うことが望ましいか。
C1（個人情報）	5	「個人データ」の安全管理措置義務	個人情報保護法上、安全管理措置が義務付けられるのはどの範囲か。「個人データ」とは何か。
C1（個人情報）	6	個人情報保護法の安全管理措置義務と情報セキュリティの関係	企業が個人情報を取り扱うに当たって、個人情報保護法が要求する安全管理措置を講ずるための具体的な対応はどのようなものか。また、企業における「情報セキュリティ対策」と個人情報保護法への対応の関係性はどのようなものか。 企業が取り扱う個人情報について、保存・消去、本人からの訂正・消去等請求への対応における注意点は何か。
C1（個人情報）	7	個人データの委託	委託先に個人データを取り扱わせる場合、委託元にどのような監督責任が生じるのか。
C1（個人情報）	8	クラウドサービスの活用と個人情報保護法	クラウドサービスを活用している場合に、個人情報保護法上どのような点に留意すべきか。

C1（個人情報）	9	個人情報保護法制	個人情報の保護に関して法令上求められる安全管理の措置は、個人情報を取り扱う主体に関わらず同じなのか。同じではないとしてどのように異なるのか。
C1（個人情報）	10	国立大学、私立大学及び企業の共同研究と個人情報保護	国立大学と企業、私立大学と企業がそれぞれ共同研究を行う場合のように、様々な主体が共同で個人情報を取り扱う場合に、法令上どのような点に留意すべきか。
C2（個人情報派生）	11	匿名加工情報制度と安全管理	個人データを匿名加工情報や統計的な情報へ加工して利活用する場合にはどのような安全管理が必要となるか。
C3（個人情報関連の管理）	12	クレジットカード情報の取扱い	クレジットカード情報を取扱うにあたって、留意すべき点は何か。
C3（個人情報関連の管理）	13	労働者の心身状態に関する情報の取扱い	労働者の心身の状態に関する情報を扱う際の留意点は何か。
C3（個人情報関連の管理）	14	暗号の利用と情報管理等	暗号の利用は情報の管理を求める法令等に関してどのような役割を果たすか。また、関連する法制度としてどのようなものがあるか。
C4（マイナンバー）	15	マイナンバー管理	企業がマイナンバーを管理する上で留意しなければならない点は何か。
C4（マイナンバー）	16	マイナンバーカード	マイナンバーカードを企業が利用できるのか
D（不競法・知財法等）	17	どのように情報を管理していれば、「営業秘密」として認められるのか	セキュリティインシデントが発生し情報が漏えいした場合に、民事裁判において当該情報の使用・開示の中止を求める、もしくは損害賠償を請求する、または刑事告訴して厳正に対処するためには、当該情報が不正競争防止法上の「営業秘密」に該当する必要がある。どのように情報を管理していれば、「営業秘密」として認められるのか。
D（不競法・知財法等）	18	営業秘密管理とサイバーセキュリティ対策との異同	不正競争防止法に基づく営業秘密としての法的保護を受けるための情報管理とサイバーセキュリティ対策としての情報管理は、どのような点で異なり、どのような点で共通するか。
D（不競法・知財法等）	19	委託元と営業秘密	従業員や委託先企業が作成や取得に関与した顧客リストや技術情報などの秘密情報について、雇用会社や委託元会社は、営業秘密としての保護を受けることができるのか。

D（不競法・知財法等）	20	限定提供データとサイバーセキュリティ	平成30年不正競争防止法改正により新たに導入された「限定提供データ」は、どのような制度であり、セキュリティインシデントにどのように対応できるのか。
D（不競法・知財法等）	21	技術的手段の回避行為・無効化行為の法的責任	企業内の秘密情報や従業員情報、顧客情報等のコピーや改変の禁止のために、もしくは当該情報が格納されたサーバやクラウドへのアクセスの禁止のために、またはアプリやソフトウェアの認証（アクティベーション方式）のために、技術的な手段が施されている場合に、そのような技術的手段を回避したり無効化したりする行為について、法律上、どのような責任が発生するのか。
D（不競法・知財法等）	22	データの知的財産権法規定による保護方法	企業や組織において保有する秘密情報やビッグデータなどの価値ある重要なデータについて、情報漏えい等が生じた場合に、不正競争防止法に基づく営業秘密または限定提供データとしての保護以外に、他の知的財産権法規定による保護方法として有用なものはあるか。
E（労務管理）	23	セキュリティ上必要となる雇用関係上の措置	企業は、従業員が情報セキュリティ上の事故を発生させる事態を未然に防止し、また、こうした事態が発生した場合に適切な対応をとるために、雇用関係上どのような措置を講じておくべきか。
E（労務管理）	24	誓約書の徴収	情報資産の守秘に関する誓約書を従業員から取る意義とは何か、また、取る際にどのようなことを考慮すべきか。
E（労務管理）	25	従業員のモニタリングと個人情報・プライバシー保護	企業が従業員に提供する業務用のPCやスマートホン等の端末について、従業員による個人データや営業秘密の流出・漏えいの未然防止、早期発見のために、企業が、従業員の電子メールのモニタリング、端末画面のスクリーンショット等、又はGPSを用いて従業員の位置を管理すること等について、法律上問題点になる点、留意すべき点は何か。また、従業員の私物であるPCやスマートホン等の端末の場合はどうか。
E（労務管理）	26	私用メール等を禁止・制限する規定と解雇・懲戒処分	企業が従業員の私用メール（企業の電子メールアカウント等を私的なやり取りに利用すること）を禁止し、一定の場合にSNSの利用を禁止または制限する規程を設けることはできるか。また、これに違反したことを理由として、解雇・懲戒を行うことはできるか。
E（労務管理）	27	私物ＰＣの社内利用、業務用データの社外持ち出し、テレワーク時の注意事項	私物PC 等の社内持込及び利用禁止を実施する際に、労働法上、どのようなことを考慮すべきか。また、業務用データの社外持ち出し、テレワークなど社外における業務を認める場合にはどのようなことを考慮すべきか。
E（労務管理）	28	退職後の従業員の競業避止義務、秘密保持義務	企業が、従業員が退職後に他社に転職するなどして会社の秘密情報を流出させることを防止しようとする場合、雇用関係上の対策としては、どのようなものを講じることが考えられるか。

E（労務管理）	29	退職後の情報漏えい防止のためのNDA	退職者が在職中に知り得た秘密情報を使用又は第三者に開示することを防ぐためには、いつどのような方法で秘密保持義務を負わせることが有効であるか。
E（労務管理）	30	退職後の競業避止義務の効力	秘密情報の流出を防止する目的で、従業員に退職後の競業避止義務を課すことを定める就業規則規定や個別合意の効力について、従業員の職業選択の自由との関係でどのような問題が生じるか。
E（労務管理）	31	海外での競業行為について	元従業員・元役員による海外における競業行為については、どのような対策があり得るか。秘密情報流出防止を目的とした競業避止義務契約は有効か。また、当該義務違反時にどのような措置を取り得るか。
E（労務管理）	32	派遣労働者に対する誓約書の要請・教育訓練の実施	派遣先企業は秘密情報流出防止の目的で派遣社員の秘密漏えい防止の誓約書提出を義務付けることができるか。また、セキュリティ対策のための教育訓練を行うことができるか。
E（労務管理）	33	従業員の調査協力、始末書の徴収、教育訓練の実施	情報流出事故を発生させた従業員に対し、調査に協力させたり、始末書を徴収したり、情報セキュリティ啓発教育を受けさせたりする等の措置をとる際に労働法上考慮すべき事項としてはどのようなものがあるか。
E（労務管理）	34	従業員に対する解雇、懲戒処分、損害賠償請求等	企業が秘密性侵害行為などの情報セキュリティインシデントを発生させた従業員に対し、解雇、懲戒処分、損害賠償請求等を行うことができるのはどのような場合か。
E（労務管理）	35	競業避止義務違反による退職金の減額不支給	秘密情報流出防止を目的として競業避止義務を従業員に課した場合、これに違反したことを理由とする退職金の減額・不支給は認められるか。
F（ネットワーク関係）	36	電気通信事業者に関する規律の概要	どのような事業を行うと電気通信事業者に該当するか。電気通信事業者はどのような義務を負うか。
F（ネットワーク関係）	37	ＩｏＴ機器のセキュリティに関する方策	IoT機器のセキュリティに関する法的対策として、どのような取組みがあるか。
F（ネットワーク関係）	38	IoT機器からデータが漏えいした場合、同機器の製造者はデータ漏えいの被害者に対して、どのような責任を負う恐れがあるか。	IoT機器からデータが漏えいした場合、同機器の製造者はデータ漏えいの被害者に対して、どのような責任を負う恐れがあるか。
G（契約）	39	電子契約実務と電子署名法	近年、契約業務の電子化が進んでいるが、電子契約は可能か。また電子契約を行うにあたり関連する法令はどのようなものであり、また、企業はどのような点に留意すべきか。

G（契約）	40	データ取引に関する契約におけるサイバーセキュリティ関連法令上のポイント	AI技術を利用したソフトウェアの開発・利用など、データの流通・利用を目的とする取引（データ取引）において、どのようなサイバーセキュリティ関連法令上のポイントに留意して、データの流通・利用に関する契約（データ契約）を取り決めるべきか。
G（契約）	41	情報流出に関するシステム開発ベンダの責任	システム開発ベンダは、個人情報等を取り扱うウェブシステムの開発に際して、開発当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供する義務を負うか。契約内容に記載されていない場合についてはどうか。
G（契約）	42	クラウド利用に当たっての留意点	クラウドサービスを利用するにあたって、情報セキュリティの観点から留意すべき点は何か。
G（契約）	43	サプライチェーンリスク対策	サプライチェーンリスク対策を実施・推進するにあたり、ビジネスパートナーや委託先等との関係において、どのような法律上の事項に留意すべきか。
H（資格等）	44	情報処理安全確保支援士を企業に置くことの意義	「情報処理安全確保支援士」とはどのような者か。企業内に置くことによってどのようなメリットが生じるか。
H（資格等）	45	技術等情報の適切な管理に係る認証制度	平成30年9月25日からスタートした技術等情報の適切な管理に係る認証制度は、どのような制度か。
I（その他各論）	46	リバースエンジニアリング	マルウェア対策のために当該マルウェアを解析する場合やサイバーセキュリティ対策として不正行為に用いられるソフトウェアの構造等を解析する場合に、当該マルウェアや当該ソフトウェアの複製や一部改変を行うことは、著作権法上、問題ないのか。マルウェアに感染等したソフトウェア、又はマルウェアの感染等から守られるべきソフトウェアについて、サイバーセキュリティ対策の目的で当該ソフトウェアを解析する際にこれを複製することは、著作権法上、問題ないのか。
I（その他各論）	47	サイバーセキュリティと輸出管理	輸出管理上、サイバーセキュリティに関する物の輸出や技術提供を行う場合において、法令上どのような点に留意すべきか。
I（その他各論）	48	サイバーセキュリティと情報共有	サイバーセキュリティに関する情報共有を行う場合には、法令上どのような点に留意すべきか。
J（インシデント関係）	49	企業が保有する情報が漏えいした場合の対応	企業が保有する情報が流出した場合、企業はどのような対応をとるべきか。
J（インシデント関係）	50	電子メールの誤送信	電子メールの誤送信や郵送送付先の誤り等、送信者側の過失により情報漏えいした場合、漏えい対策として、受信者に対して一定の要請（返却要請、削除要請、削除確認、現物確認等）を行うが、このような要請を受信者が拒否したため漏えい対策がとれずに二次被害が出た場合又はそのおそれがある場合、受信者に対して取り得る法的措置はあるか。

J（インシデント関係）	51	サイバー攻撃による情報喪失	受託して管理していた情報がサイバー攻撃等により消失した場合、受託事業者はどのような法的責任を負うか。同様に、受託事業者が故意又は重過失による操作ミスにより消失した場合はどうか。
J（インシデント関係）	52	データ漏えい時の損害賠償額の算定	重要なデータ等の漏えいが起こった場合の損害賠償額はどのように算出されるのか。
J（インシデント関係）	53	データを紛失・消失した場合における損害額	他者のデータを紛失・消失した場合、損害賠償額は、どのように算出されるのか。
J（インシデント関係）	54	デジタル・フォレンジック	デジタル・フォレンジックとは何か。どのような場面で使われるのか。また、デジタル・フォレンジックを活用する上で留意すべき法的な問題点としてどのようなものがあげられるか。
J（インシデント関係）	55	脆弱性情報の取り扱いについて	利用しているソフトウェア製品等に脆弱性が発見された場合、どのような対応を行う必要があるか。
J（インシデント関係）	56	ドメイン名の不正使用に対する対抗措置	第三者に、自社の商標やブランド名を含むドメイン名を勝手に使用されている場合などにおいて、企業が取り得る措置はあるか。
J（インシデント関係）	57	発信者情報開示	営業秘密などの企業が保有する情報がインターネット上で公開されてしまった場合にどのような対処を行うことができるか。
K（訴訟法）	58	デジタルデータの証拠利用について	IT 関連の損害賠償等に関する民事訴訟において証拠を保全・提出するために留意すべき点にはどのようなものがあるか。
K（訴訟法）	59	営業秘密の不正使用行為の立証	被疑侵害者（被告）が特定でき、営業秘密侵害訴訟を提起しようとする場合、原告は、被疑侵害者が営業秘密を使用した事実をどのように立証すればよいのか。特に、技術上の情報の場合はどうか。
K（訴訟法）	60	営業秘密等の漏えい事実の立証と情報管理体制	情報漏えいが営業秘密侵害や限定提供データ侵害に該当すると裁判で認められるためには、営業秘密や限定提供データを不正に取得されたことや、情報の取得者が当該情報を使用したこと、第三者へ開示したことなどを立証する必要がある。しかし、取得対象が情報という無体物であるがゆえに、その証拠を確保することは容易ではない。そこで、情報漏えいが発生した場合に、事後的に、営業秘密や限定提供データの漏えいの事実を立証することを容易にするために、どのような方法により情報を管理しておくべきか。
K（訴訟法）	61	民事訴訟における情報提供	民事訴訟において、訴訟の当事者から、自社が保有する情報の提供を求められることはあるか。
K（訴訟法）	62	民事訴訟における営業秘密、プライバシー情報の非公開の可否	民事訴訟においては、営業秘密やプライバシー情報を公開しないことができるか。
K（訴訟法）	63	自社に不利な証拠となり得る社内文書の破棄について	自社に不利な証拠となり得る情報が記載された社内文書を破棄した場合、破棄したことで訴訟上の不都合を招くことはあるか。

L（刑事）	64	不正プログラムと刑事罰	コンピュータウィルスによって企業活動を阻害した場合に、刑法上処罰されうるか。
L（刑事）	65	電磁的記録不正作出	電磁的記録不正作出罪（刑法第161条の２）における「権利、義務又は事実証明に関する電磁的記録」とはどのようなものか。
L（刑事）	66	電算機使用詐欺	電子計算機使用詐欺罪（刑法第246条の２）はどのような行為を問題としているのか。
L（刑事）	67	スキミング	スキミングとはどのような手口なのか。どのような行為が刑法により処罰され得るのか。
L（刑事）	68	情報の不正入手・漏えい	情報の不正入手及び漏えいには、どのような罰則があるか。
L（刑事）	69	不正アクセス	不正アクセス禁止法の保護を受けるためには　、どうすればよいのか。
L（刑事）	70	フィッシング	フィッシングとはどのような手口か。法令上どのように禁止されているか。
M（海外法令）	71	欧州一般データ保護規則	欧州一般データ保護規則について日本企業が留意すべきポイントは何か。
M（海外法令）	72	データローカライゼーション規制の概要	データローカライゼーションとはどのような内容の規制なのか。また、データローカライゼーション規制の適用がある場合の法的留意点はいかなるものか。