資料2-2：サイバーセキュリティ関係法令Q&Aハンドブック改訂ドラフト論点一覧表

2022年1月26日 ※赤背景：新規　青背景：Ver1.0からのアップデートが必要　黒背景：別トピックへ統合予定

カテゴリー	No	改訂後No（暫定）	タイトル(見出し)	トピックテーマ（Q）	タグ	改訂カテゴリ 1：新規　2:更新(大) 3:微更新or更新なし
1（総論）	0	0	・巻頭言 ・前文 ・サイバーセキュリティと法令 ・主な関係法令			3
2（基本法）	1	1	サイバーセキュリティの定義	法令上「サイバーセキュリティ」はどのように定義されているか。	サイバーセキュリティ基本法、サイバーセキュリティの定義	3
2（基本法）	2	2	サイバーセキュリティ基本法	サイバーセキュリティ基本法にはどのような規定があり、サイバーセキュリティ戦略本部及びその事務局であるNISCはどのような事務を行っているのか。	サイバーセキュリティ基本法、サイバーセキュリティ戦略本部、政府機関等の情報セキュリティ対策のための統一基準群、重要インフラの情報セキュリティ対策に係る第４次行動計画、GSOC、サイバーセキュリティ協議会	3
3-1（内部統制）	3	3	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。	会社法、内部統制システム、リスク管理体制、事業継続計画、グループ・ガバナンス・システム、CSIRT、モニタリング	3
3-1（内部統制）	4	4	サイバーセキュリティと取締役等の責任	会社が保有する情報の漏えい、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。	サイバーセキュリティ、会社法、個人情報保護法、損害賠償責任	3
3-1（内部統制）	5	5	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	会社法、内部監査、情報セキュリティ監査、システム監査、情報開示、内部通報、CSIRT	3
3-2（情報開示）	6	6	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。	会社法、金融商品取引法、有価証券報告書、コーポレート・ガバナンス報告書、情報セキュリティ報告書、CSR報告書、サステナビリティ報告書	3
3-3(インシデント発生時の当局等対応)	50	6の2	企業がサイバーセキュリティインシデントにあった場合の当局等対応①	企業が保有するデータの漏えいをはじめとするサイバーセキュリティインシデントにあった場合に法的義務またはそれに準じるものとして必要な対応は何か。		1
3-3(インシデント発生時の当局等対応)	50	6の3	企業がサイバーセキュリティインシデントにあった場合の当局等対応②	企業が保有するデータの漏えいをはじめとするサイバーセキュリティインシデントにあった場合に対応した方がよい事項としてどのようなものがあるか。		1

4-1（個人情報）	7	7	個人情報保護法の安全管理措置義務とサイバー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、個情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。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。 また、企業におけるサイバーセキュリティ対策と個情法への対応の関係性はどのようなものか。	個情法、個人データ、安全管理措置、保有個人データ、ISO/IEC27001、JIS Q 15001、Pマーク	2
4-1（個人情報）	8	8	個人データの委託と安全管理	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。	委託先,監督,個人データ,個人情報,選定,監査,報告,委託契約	2
4-1（個人情報）	9	9	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、個情法上どのような点に留意すべきか。	個情法、安全管理措置、委託先の監督、クラウドサービス、外国にある第三者	2
4-1（個人情報）	10	10	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。	個情法、行個法、独個法、個人情報保護条例、安全管理措置、安全確保措置、個人情報の定義	2
4-1（個人情報）	11	11	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ついて、近時の個人情報保護法の改正によってどのような変更があるか。	個情法、行個法、独個法、個人情報保護条例、安全管理措置、研究開発、適用除外	2
4-2（個人情報派生）	12	12	個人データの加工と法令上の安全管理	個人データを安全管理のため、又は利活用のために加工する場合に、法令上どのような安全管理が必要となるか。	個情法、安全管理措置義務、統計情報、匿名加工情報	2
4-3（個人情報関連情報の取扱い）	13	13	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。	割賦販売法、クレジットカード情報、重要インフラ、PCI DSS、非保持化	3
4-3（個人情報関連情報の取扱い）	14	14	労働者の心身の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。	労働安全衛生法、個情法、労働契約法、労働者、メンタルヘルス、健康診断	3
4-4（マイナンバー）	15	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。	番号利用法、個情法、マイナンバー、個人番号、安全管理措置	3
4-4（マイナンバー）	16	16	マイナンバーカード	民間企業がマイナンバーカードを活用することは可能か。	番号利用法、マイナンバーカード、本人確認、身分証明証、公的個人認証、通知カード	3

5（不競法・知財法等）	17	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	サイバーセキュリティインシデントが発生し、企業が秘密として取り扱いたい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・開示の停止・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。どのように秘密情報を管理していれば、「営業秘密」として認められるのか。	不正競争防止法、刑事訴訟法、関税法、営業秘密、秘密管理性、有用性、非公知性	3
5（不競法・知財法等）	18	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。	不正競争防止法、営業秘密管理、情報管理、内部統制システム、リスクマネジメント、コンプライアンス	3
5（不競法・知財法等）	19	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。	不正競争防止法、独禁法、雇用、委託、営業秘密、従業員、営業秘密保有者	3
5（不競法・知財法等）	20	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、サイバー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。	不正競争防止法、限定提供データ、限定提供性、相当量蓄積性、電磁的管理性、営業秘密	3
5（不競法・知財法等）	21	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。	不正競争防止法、著作権法、刑法、不正アクセス禁止法、技術的制限手段、技術的保護手段、技術的利用制限手段、技術的手段	3
5（不競法・知財法等）	22	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。	不正競争防止法、著作権法、著作権、特許権、実用新案権、意匠権、営業秘密，限定提供データ	3

6（労務管理）	23	23	セキュリティ上必要となる雇用関係上の措置と誓約書の徴収	企業は、従業員がサイバー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。	労働基準法、労働組合法、労働契約法、従業員、就業規則、秘密保持義務、懲戒処分	3
6（労務管理）	24	23	誓約書の徴収	※23に統合		
6（労務管理）	25	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や端末画面のスクリーンショット等を行うことについて、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。	民法、個情法、プライバシー権	2
6（労務管理）	26	26	私用メールの制限と私物端末の業務利用	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。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。 ＋27 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を認める場合にはどのようなことを考慮すべきか。	労働契約法、私用メール、SNS、労働契約、就業規則、職務専念義務、解雇・懲戒処分	3
6（労務管理）	27	26	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	※27の2：テレワークについて新設。その他の部分については26に統合		
6（労務管理）		27の2	テレワークにおけるセキュリティ	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。		1
6（労務管理）	28	28	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。		3
6（労務管理）	29	29	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、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。 ＋30 企業が営業上の秘密の漏えい等のサイバーセキュリティインシデントを発生させた従業員に対し、企業が解雇、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。	労働基準法、従業員、情報流出事故、調査協力、始末書、セキュリティ啓発教育	3
6（労務管理）	30	29	従業員に対する解雇、懲戒処分、損害賠償請求等	※29に統合		
6（労務管理）	31	32,33	退職後の従業員の競業避止義務、秘密保持義務	※32，33にエッセンスをちりばめる形で統合		
6（労務管理）	32	32	退職後の秘密保持義務の効力	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。	不正競争防止法、労働基準法、秘密保持契約、秘密保持義務	3
6（労務管理）	33	33	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。 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。	民法、不正競争防止法、競業避止義務、競業避止義務契約	3
6（労務管理）	34	34	退職後の海外での秘密保持義務違反行為について	元従業員・元役員による海外における秘密情報の不正使用・不正開示行為については、どのような対策があり得るか。退職後の秘密情報流出防止を目的とした秘密保持義務契約は有効か。また、当該義務違反時にどのような措置を取り得るか。	不正競争防止法、民事訴訟法、産業競争力強化法、法の適用に関する通則法、秘密保持義務、競業避止義務、情報漏えい、人材を通じた技術流出、懸念国	3
6（労務管理）	35	33	競業避止義務違反による退職金の減額不支給	※33に統合		

7（情報通信ネットワーク関係）	36	36	電気通信事業者に該当する場合	どのような事業を行うと電気通信事業者に該当するか。	電気通信事業法、電気通信事業参入マニュアル、電気通信事業法の消費者保護ルールに関するガイドライン、電気通信役務、電気通信設備、重要インフラ、電気通信事業、通信の秘密	2
		36の2	電気通信事業者に関する規律の概要	電気通信事業者はどのような義務を負うか。	電気通信事業法、電気通信事業参入マニュアル、電気通信事業法の消費者保護ルールに関するガイドライン、電気通信役務、電気通信設備、重要インフラ、電気通信事業、通信の秘密	2
7（情報通信ネットワーク関係）	37	37	IoT機器のセキュリティに関する法的対策	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。	電気通信事業法、国立研究開発法人情報通信研究機構法、IoT セキュリティガイドラインver 1.0、IoTセキュリティ総合対策、電気通信事業法に基づく端末機器の基準認証に関するガイドライン、米国カリフォルニア州IoTセキュリティ法、IoT機器、NOTICE	3
7（情報通信ネットワーク関係）	38	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。	民法、製造物責任法、IoT機器、データ漏えい、製造者責任	3
7（情報通信ネットワーク関係）		38の2	５Ｇ・ドローン法	「５Ｇ・ドローン法」は，どのような法律か。また，同法は，誰に対して，どういったレベルのサイバーセキュリティをどのようにして確保するよう求めているのか。		1
7-2（重要インフラ等）		38の3	重要インフラ分野における規定	各々の重要インフラ分野においては、サイバーセキュリティに関してどのような義務が課せられているか。法令上、どのような規定に着目すべきか。		1
7-2（重要インフラ等）		38の4	モビリティ（自動運転、自動車セキュリティ）	移動サービスが多様化しているが，法令上，どのようなサイバーセキュリティ対策が求められているか。		1
7-2（重要インフラ等）		38の5	ドローン（航空法関係）	ドローンの活用が拡大する中で法規制も整備されているが、サイバーセキュリティの関係でどのような点に留意すべきか。		1

8（契約）	39	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。	電子署名法、電子署名法施行規則、民事訴訟法、電子帳簿保存法、電子帳簿保存法施行規則、電子契約、文書の成立の真正	2
8（契約）	40	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。	民法、個情法、不正競争防止法、データ取引、AI・データの利用に関する契約ガイドライン1.1版	3
8（契約）	41	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。	民法、SQLインジェクション、重過失	2
8（契約）	42	42	クラウドサービスの利用にあたっての留意点	クラウドサービスを利用するにあたって、サイバーセキュリティの観点から留意すべき点は何か。	民法、個情法、不正競争防止法、クラウド、定型約款	3
8（契約）	43	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。	独占禁止法、下請代金支払遅延等防止法、サプライチェーン・リスク、委託、優越的地位の濫用	3
9（資格等）	44	44	情報処理安全確保支援士	「情報処理安全確保支援士」とはどのような者か。	情促法、情報処理安全確保支援士、情報セキュリティサービス基準	3
9（資格等）	45	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。	産業競争力強化法、技術等情報の適切な管理に係る認証制度、技術等情報漏えい防止措置、重要技術マネジメント、自己適合宣言確認型認証、現地審査を含む認証	3
9（資格等）		45の2	DX銘柄	DX銘柄、DX認定とは何か。		1

10（その他各論）	46	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。	著作権法、リバースエンジニアリング、マルウェア、柔軟な権利制限、複製権、翻案権、同一性保持権	3
10（その他各論）	47	47	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。	個情法、行個法、独個法、番号利用法、不正競争防止法、著作権法、電波法、電子署名法、暗号、CRYPTREC、危殆化、安全管理措置、技術的制限手段、技術的利用制限手段、技術的保護手段	3
		47の2	認証に関する法令について	認証とはどのような概念か。認証に関する法制度としてどのようなものがあるか。		1
10（その他各論）	48	48	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。	外為法、輸出貿易管理令、外国為替令、貨物等省令、貿易外省令、役務通達、輸出管理、ワッセナー・アレンジメント、侵入プログラム関連品目	3
10（その他各論）		48の2	サイバーセキュリティ事業者への投資	外国投資家が、サイバーセキュリティに関する事業を営む日本の上場会社の議決権を取得することについて何らかの法令上の制限があるのか。		1
10（その他各論）	49	49	サイバーセキュリティと情報共有・公表	サイバーセキュリティに関する情報共有体制へ参画し、情報共有を行おうとする場合に、法令上どのような点に留意すべきか。また、セキュリティインシデント発生時には、何を目的としてどのような情報を共有または公表すべきか	サイバーセキュリティ基本法、個情法、不正競争防止法、金融商品取引法、刑法、情報共有、サイバーセキュリティ協議会、CISTA、J-CSIP、JC3、セプター、サイバーセキュリティ対処調整センター、ISAC	2
10（その他各論）		49の2	脅威インテリジェンスサービス	脅威インテリジェンスサービスを活用するにあたって、どのような点に留意すべきか？	脅威インテリジェンス、個人情報保護法、不正競争防止法、刑法、	1
10（その他各論）		49の3	データの消去	データを消去する場合に、どのような点に留意が必要か。		1

11（インシデント関係）	50	50	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。	個情法、不正競争防止法、刑事訴訟法、金融商品取引法、個人データ、営業秘密、限定提供データ	3
11（インシデント関係）	51	51	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。	不正競争防止法、民法、営業秘密を示された者、電子メール、誤送信	3
		51の2	ランサムウェア対応	ランサムウェア攻撃を受けた場合、どのような法律に留意すべきか。	ランサムウェア、会社法、善管注意義務、経営判断原則、個人情報保護法、適時開示、テロ資金提供処罰法、組織犯罪収益処罰法	1
11（インシデント関係）	52	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。	民法、不正競争防止法、個情法	3
11（インシデント関係）	53	53	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。	民法、消費者契約法、電気通信事業法、情報消失、寄託、免責規定、責任制限規定、過失相殺	3
11（インシデント関係）	54	54	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。	民法、データ、紛失、消失、滅失、損害賠償額	3
		54の2	インシデント対応における費用負担及びサイバー保険	サイバー攻撃を受けた場合、どのような損害や費用が発生するか？また、サイバー保険ではどのような費用がカバーされるか？	ランサムウェア、サイバー保険、保険業法	1
11（インシデント関係）	55	55	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。	刑法、不正競争防止法、著作権法、児童ポルノ禁止法、金融商品取引法、デジタル・フォレンジック、証拠保全	3
11（インシデント関係）	56	56	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。	情促法、脆弱性、脆弱性情報ハンドリング、JVN	3
		56の2	脆弱性修正の時的範囲	脆弱性にいつまで対応しなければならないか。		1
11（インシデント関係）	57	57	ドメイン名の不正使用への対抗措置	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。	不正競争防止法、サイバースクワッティング、統一ドメイン名紛争処理方針（UDRP）、JPドメイン名紛争処理方針(JP-DRP)	3
11（インシデント関係）	58	58	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。	プロバイダ責任制限法、不正競争防止法、発信者情報開示請求、削除請求	2

12（民事訴訟手続）	59	59	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。	民事訴訟法、証拠能力、デジタル・フォレンジック	3
12（民事訴訟手続）	60	60	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。	不正競争防止法、営業秘密、技術上の秘密、営業秘密侵害訴訟	3
12（民事訴訟手続）	61	61	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。	不正競争防止法、民事訴訟法、営業秘密、限定提供データ	3
12（民事訴訟手続）	62	62	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。	民事訴訟法、特許法、著作権法、不正競争防止法、会社法、弁護士法、弁護士会照会、証拠保全	3
12（民事訴訟手続）	63	63	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。	民事訴訟法、特許法、不正競争防止法、著作権法、証言拒絶、文書提出命令、インカメラ手続、閲覧等制限、査証制度、財産開示制度	3
12（民事訴訟手続）	64	64	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。	民事訴訟法、文書提出命令、証明妨害、e-Discovery	3
13（刑事）	65	65	不正プログラムと刑事罰	いわゆるコンピュータ・ウィルスによって企業活動を阻害する行為について、刑法上どのような罰則があるか。	刑法、不正指令電磁的記録に関する罪、電子計算機損壊等業務妨害罪、コンピュータ・ウイルス、不正プログラム、不正指令電磁的記録、マルウェア	3
13（刑事）	66	66	電磁的記録不正作出	Webサイトに登録されたユーザデータを権限なく変更するなど不正にデータを改ざんする行為について、刑法上どのような罰則があるか。	刑法、私電磁的記録不正作出罪、公電磁的記録不正作出罪	3
13（刑事）	67	67	電算機使用詐欺	例えばインターネットバンキングなどにおいて他人になりすまし、別の銀行口座へ送金するような行為について、刑法上どのような罰則があるか 。	刑法、電子計算機使用詐欺罪	3
13（刑事）	68	68	スキミング	スキミングとはどのような手口なのか。刑法上どのような罰則があるか。	刑法、割賦販売法、スキミング、デビットカード、偽造、IC化	3
13（刑事）	69	69	情報の不正入手・漏えい	情報の不正入手及び漏えいに関して、どのような罰則があるか。	刑法、個情法、行個法、独個法、番号利用法、不正競争防止法、国家公務員法、地方公務員法、電気通信事業法、有線電気通信法、電波法、情報の不正入手、漏えい、ダークウェブ	3
13（刑事）	70	70	不正アクセス	いわゆる不正アクセスに関して、不正アクセス禁止法上どのような行為が禁止されているか。	不正アクセス禁止法、アクセス制御機能、識別符号	3
13（刑事）	71	71	フィッシング	フィッシングとはどのような手口か。法令上どのような行為がに禁止されているか。	不正アクセス禁止法、割賦販売法、フィッシング、識別符号、クレジットカード、フィッシング対策協議会	3
13（刑事）		71の2	越境捜査	越境リモートアクセス捜査とは何か。法的な問題点としてどのようなものがあげられるか。	刑事訴訟法、リモートアクセス捜査、サイバー犯罪条約	1

14（海外法令）	72	72	欧州一般データ保護規則（GDPR）	欧州一般データ保護規則（GDPR）について日本企業が留意すべき個人データの安全管理に関するポイントは何か。	個情法、欧州一般データ保護規則、GDPR、域外適用、安全管理、データ侵害通知、データ保護オフィサー（DPO）、データ保護影響評価（DPIA）	3
14（海外法令）	73	73	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。	データローカライゼーション、越境移転、中国サイバーセキュリティ法、重要データ、個人データ、重要情報インフラ運営者、ネットワーク運営者	2
14（海外法令）		73の2	NIS指令・NIS2指令案	NIS指令とはどのような内容の規制なのか。また、NIS指令及びこれに関連する各国法の適用がある場合の法的留意点はいかなるものか。		1
14（海外法令）		73の3	米国における主なデータ保護・セキュリティ関係法令	米国にはどのようなサイバーセキュリティ関係法令があるか。	CCPA、CRPA、SHIELD Act.、HIPAA、GLBA、OFAC、FinCEN	1
14（海外法令）		73の4	NIST SP800シリーズ	米国国立標準技術研究所(NIST)が公開しているSP800シリーズとは何か。サイバーセキュリティ対策に関してどのようなものがあるのか。		1
14（海外法令）		73の5	捜査に関する条約／協定	国際捜査共助にはどのようなものがあるか。	証拠収集、外交ルート、サイバー犯罪条約、刑事共助条約（協定）、MLAT、ICPO、24時間コンタクトポイント	1