サイバーセキュリティ戦略本部
普及啓発・人材育成専門調査会
サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ
第１回会合　議事概要

１　日時
平成 31 年２月８日（金）　10:00～12:00

２　場所
フレンドビルディング７階大会議室

３　出席者（敬称略）

（主査）	林　紘一郎	情報セキュリティ大学院大学　教授
（副主査）	岡村　久道	英知法律事務所　弁護士
		京都大学大学院　医学研究科　講師
（委員）	大杉　謙一	中央大学大学院　法務研究科　教授
	大谷　和子	株式会社日本総合研究所　執行役員　法務部長
	奥邨　弘司	慶應義塾大学大学院　法務研究科　教授
	小向　太郎	日本大学　危機管理学部　教授
	星　周一郎	首都大学東京　法学部　教授
	丸山　満彦	デロイトトーマツリスクサービス株式会社
		代表取締役社長
	宮川　美津子	ＴＭＩ総合法律事務所　弁護士
	湯淺　墾道	情報セキュリティ大学院大学　教授

（事務局）	山内　智生	内閣審議官
	吉川　徹志	内閣参事官
	吉田　恭子	内閣参事官
	神谷　英亮	参事官補佐
	蔦　　大輔	上席サイバーセキュリティ分析官

（オブザーバー）
警察庁、個人情報保護委員会事務局、総務省、法務省、経済産業省

4　議事概要

（1）山内内閣審議官挨拶

（2）サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループについて

事務局から、資料１－１、１－２に沿って説明。

林委員を主査に互選。

事務局から、資料１－３に沿って説明。

林主査が岡村委員を副主査に指名。

（3）サイバーセキュリティ関係法令集の調査検討に関する方向性について

事務局から、資料２－１、２－２に沿って説明。

その後、委員による自由討議が行われた。

委員からの発言の概要は以下のとおり。

（大杉委員）

・　最近の法令改正として、平成 26 年の会社法改正を受けて平成 27 年に会社法施行規則が改正され、内部統制システム構築義務について、企業グループとして、つまり大企業、上場会社等であれば子会社などにもある程度目配りをした総合的なグループ全体の内部統制システムを構築することとされたため、その点留意して欲しい。

・　ソフトローをどこまで盛り込むかについては、現在どのようなソフトローが存在するかを示して頂いた上で、盛り込むことの是非を判断すべきと考える。

・　成果物を作成する際には、作成時点で未施行のものがあればその旨を注記しつつ、５～10 年前の改正であれば、改正年月を入れておくと読者に親切ではないか。

・　成果物が紙であれば目次という一方向的に流れるものが想定されるが、デジタルであれば色もタグも自由に使えるのではないか。

・　対象とする読み手については、実際には監査役がいるのではないか。

・　経営層は長いもの、条文は読まないので、エグゼクティブサマリーが必要。昨年 9 月に経産省が出した CGS ガイドライン改訂版も、社長向けのエグゼクティブサマリー＋本文＋別紙という構成で作成したので参考になるのではないか。

（大谷委員）

・　まず、経産省で公開している情報セキュリティ関係の要求事項集をアップデートするだけでも価値があるものになるのではないか。

・　グローバルでのデータ交換に際して諸外国の規制を日本国内でどの程度意識すべきかが気になっている。昨今の事例だと、比較的人件費が小さい国に開発拠点を置き、そことデータ交換をするような場合に、各国の規制、セキュリティに関する規

制がどのように関わってくるかという問題。
・　日本の法人経営者が GDPR について留意すべき事項がどのようなものかということも、余裕があれば触れる必要があると考えている。
・　セキュリティ関係の事案としては、仮想通貨の窃取など、直接的に金銭的な被害が発生する事案が増え、QR コード決済といったキャッシュレス化もさらに進んでいる。これまでは一般企業の観点でまとめられていたが、こういった要素も追加する必要があるのではないか。
・　情報信託機能や、医療と金融の融合、地公体の事業とその他の事業の融合など、業種の垣根を越えてさまざまな情報に接するケースが増加しているため、それをカバーできるものをゆくゆくは検討したい。
・　改正民法が来年 4 月から施行され、契約上の不適合責任といったことが大幅に変わる。システム構築を行う事業者のセキュリティの確保も含めた責任のあり方というものも大きく変わるのではないかと注目している。それらについても、ソフトロー的な部分も、あるいは裁判例のようなものも意識しながら解説を加えられれば、と考えている。
・　以上様々なことを述べてきたが、議論するなかで取捨選択を進めたい。

（奥邨委員）
・　経産省の要求事項集は平成 21 年時点のものということだが、不正競争防止法については複数回の改正を経て、不正競争の範囲も広がり、営業秘密が刑事罰の対象となり、刑事罰の対象も広がっている。また、限定提供データも不競法に入ったため、それも視野に入れておくべき。
・　資料に記載された技術的保護手段の回避について、もともと著作権法はコピープロテクション、不正競争防止法はコピープロテクション＋アクセスコントロールだったが、数次の改正を経て、現在、著作権法でも、コンテンツに対するアクセスコントロールに対応している。また、不正競争防止法の平成 30 年改正時に、従来はコンテンツ＋プログラムに対するアクセスコントロールという扱いだったところに、ビッグデータ等を念頭に置いて「情報の処理」というものが入った。情報の処理の定義としては、電磁的な情報の処理ということでかなり広いため、ここにサイバーセキュリティの分野も含まれてくると考える。
・　刑事法に関連して申し上げると、B-CAS カードの改造問題が挙げられる。これを行うことで私電磁的記録不正作出・同供用という罪で逮捕されている事例があるが、B-CAS の問題が出てくるまでは、この罪がこのように運用されることはあまり意識されていなかった。
・　著作権法については、平成 30 年の改正で、サイバーセキュリティの関係で AI を使って何かをするというような場合に活用するものとして柔軟な権利制限規定が措置されたが、運用が固まっているものではないため、セキュリティ関連に対応可

能か否かは議論が必要と考えている。
・　ソフトローに関しては、営業秘密管理指針と限定提供データについての指針は、役所が出しているガイドラインとして実務の上ではかなり重要視されており、特に営業秘密管理指針は裁判例にも影響を与えているため、言及が必要であると考えている。
・　訴訟法と実体法という話があった。分類については、最終的には何らかの形で分類する必要があるが、一方で、検討していく上では必ずしも分類にこだわらないということも必要ではないか。基本的には実体法が前提になるが、訴訟法も考えなければならず、両方を見る必要がある。例えば、営業秘密で関しては、極端に言うと秘密裁判にしないと、営業秘密の訴訟を行うことで営業秘密でなくなるという自己矛盾が解決できないため、営業秘密は、訴訟法と実体法がセットになって初めて営業秘密の実態的な保護ができるという構造と言える。

（小向委員）
・　大学で 10 年ほど情報セキュリティと法という講義を担当しているが、そこで説明を行う際にも、サイバーセキュリティの CIA と、対象とする法益をマトリックスにして説明している。機密性、完全性、可用性というのはセキュリティにとって大変重要である。また、情報を管理する事業者に対して管理責任を課す類型と、不正行為者に対して法的責任を課す類型、こういう分類は大変重要だと考える。ただし、CIA は情報セキュリティの目的としては非常に良いのだが、これを軸に法律を整理したものは一般の人には直感的にわかりにくいところがありそうにも思う。
・　インシデント発生時の対応、訴訟手続、フォレンジック等がすでに挙げられている。論点として、実体法的なものに目が向けられがちであるが、むしろ手続法的なものが多いと感じている。これをどのように入れ込んでいくかも課題だと思っている。例えば事務局からプロバイダ責任制限法が例示されたが、これも手続の問題に近いと考えられ、また、刑事訴訟法の手続がどのようにサイバーセキュリティの確保に関わるかも重要ではないか。
・　例えばサイバー犯罪条約など、条約をどう扱うかも重要ではないか。
・　GDPR への言及があったが、注目すべきものとして e プライバシー規則も挙げられる。こういったものも入れていく必要があるのではないか。
・　ソフトロー関係については、分野によってメリハリをつけざるをえない。例えば個人情報保護関係だとガイドラインは大変重要だが、膨大に出ているため、全部引き写すと大変なことになる。物によっては解説として触れるとか、そういうことも必要ではないか。
・　林主査から話があった、人に注目するか、データに注目するかは、どちらもあり得て、アプリオリにどちらがいいという話ではないのではないか。

（星委員）

・　平成 23 年の刑訴法改正であるとか、不正アクセス禁止法関係とか、刑罰法令についても一定の整備がされてきているものの、刑事法の領域の中でも様々な法令の中に散在しているため、それを横串にした法令集を作成するだけでも非常に便宜であると思う。

・　刑事法関連は、他の分野、例えば民事関係では横のつながりが色々ある中、刑法だけが比較的独自の領域となっているというイメージを個人的に持っていたが、実社会においては、そうはいかなくなってきている。たとえば、様々な情報をビジネスの必要上持っている企業や組織が、刑事手続の一環としてその提供を求められた場合に、どこまでどのように出せば良いのか、ということは、提供を求める側も提供に応じる側もよくわかっていないところがあり、それが今後大きな問題になるのではないか。

・小向委員からもあったが、手続的な問題の重要性が増している。NISC が出す法令集としてどこまで書き込めるかは難しい問題もあると感じる。関係省庁も含めて慎重な検討をしていく必要があるだろう。

・ それに関連して、刑事法の領域では、ガイドラインや指針というものはあまりないのだが、一方で、判例が条文の意味を認識する上でやはり必要。最高裁判例であれば確定したものとして盛り込むこともできるが、高裁とか地裁レベルの裁判例をどう扱うかについては慎重な検討が必要となることもあろう。

（丸山委員）

・　法令集作成にあたって、事典的なものを作るか、ユーザーフレンドリーなものを作るか、最終のイメージがどちらになるかによって、資料２－１の６ページの①、②の類型を示すパターンにするのか、CIA の類型にするのか、事業者の立場からの類型にするのかというのは変わってくるのではないか。ユーザーフレンドリー的なもしユーザーガイドラインのようなもので見やすいものであれば、②の類型ということになるのではないか。

・　次に掲載するものの範囲だが、日本法は当然含むとして、判例やソフトローに関する議論もあったが、事業者側の立場からは、外国法令を取り上げる必要性を感じている。特に最近は、アジアのセキュリティ関連法令が厳格化しており、法令遵守のためにどうするかという仕事が多い。ただ、外国法令の解釈について日本だけで議論することも難しいと考えており、今回どこまでそれを整理するかが課題になるのではないかと思っている。

・　個人的には、まずは事典的なものを作成し、その解説という観点から、事業者の立場からできるだけわかりやすいもの、例えば法令名を挙げるとか、ソフトローの名前を挙げるとか、そういったものを作成するのがよいのではないか。

・　サイバーセキュリティ基本法の「サイバーセキュリティの定義」を切り口として、

情報の安全管理のために必要な措置に関連するような法令、情報システム、情報通信ネットワークの安全、信頼性の確保に必要な措置に関連するような法令というように整理するとわかりやすいのではないか。

・　最近は、データの整理の方法として、タグ型データベース、XML や MarkLogic 等がある。情報にタグを付けていき、どういう切り口で最終的に整理するかを考えていくのもよいのでは。

（宮川委員）

・　資料２－２の３頁に記載された平成 21 年６月以降に行われた法改正が非常に多いことに今さらながら愕然としているが、どれも重要な法令と思うのが、どのようにまとめていくかを検討していきたい。

・　法令集のターゲットということで、資料２－１の３頁目に、（１）経営層、（２）戦略マネジメント層、（３）法務部門という３つが挙げられているが、かなりレベルが違うと考えられる。経営者層は、細かい条文などに踏み込んで検討するより、全体的な大きな流れに関心がある、一方で法務部門は、実務に対応した非常に詳細な部分で重要なところに関心がある。対象をどのように考慮して内容を整理していくかということも意外と難しいのではないか。

（湯淺委員）

・　単なる六法集にするより、平易な解説をつけることには賛成である。

・　中小企業の経営者の方からの声として、ガイドラインの中にも、ある程度拘束性が強いものと、純粋な単なるガイドラインに過ぎないものとがあってわかりにくいというものがある。何かしらの整理ができればと考えている。

・　近年、特に子供、未成年者を対象とするサービスが非常に増加しており、かつ、その法規制もかなり充実してきている。未成年者を対象としたビジネスをする際のサイバーセキュリティ上の留意点という切り口もあってよいのではないか。

・　情報セキュリティの時代からサイバーセキュリティの時代になって、インターネットでつながることで各段に領域が増えている。特に今、一番話題になっておる IoT セキュリティに関する部分は、IoT 機器を普通の会社が普通に導入する時代になっているため、取り扱うべき範囲として検討する必要があるのではないか。

・　刑事法関係については、大手企業を中心に CSIRT などのセキュリティ部門を持つところが増加したが、それに伴い、CSIRT 業務でここまでやっていいのか、あるいはここから先はまずいのかの判断に困るという話ををよく聞く。例えば、マルウェアに感染した、ということで、セキュリティ会社に依頼し、そのマルウェアを出そうとしたら、法務部門がマルウェア提供罪に該当する恐れがあるからダメだと言っているがどうなのだろうか、といったようなもの。要するに、刑事法上、「正当」と認められる範囲の例示的列挙をビジネスあるいは学界も求めているのではない

か。

・　海外のビジネス、または海外の顧客のデータを扱う際に日本企業が守るべき事項が増加している。GDPR その他の個人データの関係のほか、データローカリゼーションの要求が各国で厳格化しているので、その点に触れれば企業の経営者には参考になるのではないか。

（岡村副主査）

・　要求事項集の作成以降、すごいスピードで法令の中にセキュリティに関する条項が続々できている。一例を挙げると、厚労省所管の労働安全衛生法の改正で労働者の健康情報についての適正な取り扱いとともに、セキュリティを図る旨の規定が措置されているような状態であり、まとめておかないと誰も全体像がわからない状態になってしまうということは危惧している。

・　平成 21 年に要求事項集を作成した際には、経済産業省がベースというフレームワークがあったため、取り扱える範囲に限界があったが、今回は内閣官房で扱うという形になったことで、フレームワーク的には広げることができるのではないか。

・　法律の構造をピラミッドに見立てると、基本法、一般法、個別法がある。平成 21 年当時は基本法に位置付けるべきものに IT 基本法ぐらいしかなかったが、現在はサイバーセキュリティ基本法がある。その意味でピラミッド構造が変わったことは反映すべきであろう。

・　平成 21 年に要求事項集を作成した際には、技術の専門家の方に法制度をわかっていただくために分かりやすい切り口は何か、ということから、CIA を活用したという経緯がある。よりよいものがあればお知恵をお借りしたい。

・　分野としては、クレジットカード関係では、割賦販売法で保護規制を強化し、例えば PCI-DSS を入れることになった。これを特定の業界に閉じたものと考えるか、または、クレジットカードの普及状況を踏まえて法令集で取り上げるべきか、ということは色々な意見があると考えられる。この辺りをどうするかで取り扱う法令の範囲も変わるのではないか。

・　法律があり、政令があり、省令があり…、とキリがない面がある。ソフトローと判例の取扱いを含め、分野によって、触れざるを得ない形のものは触れるという弾力的な形が良いのではないか。

・　PDCA の C の部分が制度論的に 1 項目あった方が良いのではないか。大杉委員、丸山委員もいらっしゃるので、是非、監査について簡単でよいので触れてもらいたい。内部統制に関する監査もあれば、システム監査もある。

・　手続法の関係で言うと、特許法の改正で措置されたものとしては、営業秘密に関するものについて、セキュリティに配慮した訴訟手続の規定も措置されたということができるのではないか。

・　今回の議論ではっきりしたのは、議論すべきことが多過ぎる、かつ、複雑である

ということ。このメンバーだけでやり切るというのは非常に大変になるため、NISCから、主に関係する省庁に、できれば自主的に、どのような法令を所管していて、当該法令でセキュリティを目的としていなくても、セキュリティを保護する役割を担っているかについて、思いつく法令をNISCへ集約していただきたい。

・　その他進め方として、必要であればオブザーバー以外の省庁へも照会をかけるということも弾力的にやっていくような形で行っていただきたい。

（林主査）

・　サイバーセキュリティ基本法ができ、戦略における一番重要なプリンシプルとして自由公正かつ安全なサイバー環境を維持するということを言っているので、その辺りはまず明確にした方が良いのではないか。

・　人に注目して、人に責任がどう及ぶかという分類と、データに注目して、データをどう扱われることが期待されているかという分類がマトリックスのようになるのではないか。データに関する契約などにはある種面白い要素がある。CIAはもともとデータのレベルでセキュリティを担保するための機能分類であるが、人に注目したときには、データを扱う人が何らかの責任を負わなければいけないという類型と、それ以外の類型となっているものもあるが、私としては、人がデータに対して権限を持つという類型の法律体系と、権限はないが、何か不都合が起きたときは不法行為で救済するという救済中心の法制と２つがあって、それをどう組み合わせるのかという問題ではないかと考えている。あまり議論されていないところだが、分類学を行う際に少し触れた方が良いのではないか。

・　実体法と手続法というのが、有体物についてはかなり明確に分けられるが、データ系も同じだろうかと印象を持っている。例えば、ウイルス作成罪においては、事後的には共通の見解としてウイルスか否かの判別が可能であるが、実体法的にウイルスを定義するとなるとなかなか難しい。ウイルス作成罪というものを条文上措置したからといって実効性があるという担保にはならないので、実体と手続は密接な関連を持ったものにならざるを得ないのではないか。それが有体物と違うある種の特徴ではないかと考えている。

以　上