「サイバー対処能力強化法の施行等に関する有識者会議」（第２回）議事要旨

1. 日時：令和７年 10 月３日（金）16 時 00 分から 17 時 10 分までの間

2. 場所：中央合同庁舎４号館

3. 構成員

岩村 有広	一般社団法人日本経済団体連合会 常務理事
上沼　紫野	LM 虎ノ門南法律事務所弁護士
上原　哲太郎	立命館大学情報理工学部教授
大谷　和子	日本総合研究所 執行役員 法務部長
小栗　泉	日本テレビ放送網株式会社 スペシャリスト・オフィサー 特別解説委員
川口　貴久	東京海上ディーアール株式会社 主席研究員
小柴　満信	公益社団法人経済同友会 幹事
酒井　啓亘	早稲田大学法学学術院教授【座長代理】
宍戸　常寿	東京大学大学院法学政治学研究科教授
高見澤　將林	公益財団法人笹川平和財団 上席フェロー【座長】
野口　貴公美	一橋大学副学長、法学研究科教授
平井　淳生	一般社団法人電子情報技術産業協会 業務執行理事／常務理事
星　周一郎	東京都立大学法学部教授
星野　理彰	NTT 株式会社代表取締役副社長 副社長執行役員 一般社団法人 ICT-ISAC 理事

（政府側）

飯田　陽一	内閣サイバー官
木村　公彦	内閣府政策統括官（サイバー安全保障担当）
泉　恒有	内閣府政策統括官（経済安全保障担当）
佐野 朋毅	内閣府大臣官房審議官（サイバー安全保障担当）
小柳 誠二	内閣官房内閣審議官／内閣府

4.　議事概要

（1）日本労働組合総連合会からのヒアリング

冨田　珠代　日本労働組合総連合会　総合政策推進局長から、別紙１に基づき説明があった後、座長から、関係団体による説明について、各委員に対して質問や意見を求めた。

主な発言は以下のとおり。

○　説明にありました現場の負担をできるだけ軽減するためにはどうしたらよいかという点についての示唆は重要である。

○　２点質問したい。まず、生活者・労働者の立場から、基本方針について重要だと思う点、あるいはこのようにしたらよいのではないかという点をお聞きしたい。また、本日指摘いただいた意見について、生活者・労働者の立場から留意すべき点があればお聞きしたい。

日本労働組合総連合会

○　強化法の必要性については、よほどの注意喚起がなされなければ、一般の国民や働く者が考えることがないと思う。情報を保全することは、自分を守る事につながることも含めて、この法律がなぜ我が国に必要なのか、その背景や必要性について丁寧に説明や周知していただきたい。その上で、この法律は通信の秘密保障されている情報についても必要に応じて一定程度収集を可能とするものなので、なぜそれが許されるのか、どのような目的で収集するのか、万一その情報が外部に漏れるようなことがあった場合に、国民に対してどのような方法で情報公開されるのかといった点について、あらかじめルール等を定めていただけると、国民の安心につながると思われる。

○　基幹インフラ事業者がサイバーセキュリティの対応も含めてインフラを安全に安定的に動かすためには、日々の現場の力がないと成り立たない。外部からの脅威に対して守りを固めることは必要だが、結果として現場で作業している従業員・労働者に対し、今以上に過度な負担とならない制度としていただきたい。

○　国民に丁寧に説明していただきたいとのことだが、これを効果的に行うことは難しい。その方法として具体的な提案があれば教えていただきたい。

日本労働組合総連合会

○　非常に難しい点であると思っている。連合も、700 万人の組合員に連合の考えを効果的に届けるのには、どういったツールを用いればよいのか日々模索している。

○　国民に対する情報提供は、全ての世代の国民が日常的に手にしている情報ツールに届けていただくのがよいのではないか。新聞、テレビに加え、若者向けであれば

YouTube 等の動画配信を活用するなど、行政機関には、様々な方法を検討していただきたい。

○　役割分担については様々なところで議論されることになると思うが、人材育成やスキルの役割分担についてはなかなか難しいと思うところ、国、自治体、事業者、労働者の理想的な役割分担のイメージはあるか。

日本労働組合総連合会

○　実際に対応にあたる方が、迷う事なく対処できるようにすることが大事であり、そのためには、それぞれの立場で研修、教育等を行うことが重要。

○　特に、強化法は守秘義務等の違反に罰則が科されることなっており、何をしたら違反となるのかを理解していないと、労働者は自らを守れないので、その点を明確にした上で、わかりやすい研修や教育を行っていただきたい。

○　政府側の情報共有の仕方も大きな観点であり、受け取られやすいような形で共有していただく必要があるのだろう。

○　企業側は情報が流出することについて危機感を持っていると理解したが、万が一、情報が流出した場合に企業側の責任が問われないような仕組みを明記することまで希望されているか。

日本労働組合総連合会

○　罰則が規定されているため、何をしたらいけないのか、何をしなければならないのかを明確にしていただくことが重要。

○　守秘義務の範囲や守秘義務として何を求めるのかを明確にすることが従事する者を守ることにつながるので、ご検討いただきたい。

（２）　地方自治体からのヒアリング

鈴木　厚 北海道 総務部 イノベーション推進局 情報政策課　情報基盤担当課長
大野　晃 宮崎県都城市 総務部 情報政策課長
鳴川　雅彦 広島県坂町 政策監 兼 デジタル改革推進室 室長
の３名から、それぞれ資料２から資料４に基づいて説明があった後、座長から、関係団体による説明について、各委員に対して質問や意見を求めた。主な発言は以下のとおり。

○　３点質問したい。１点目は、システムを長年利用していて老朽化が課題とのことだが、どの程度古いシステムを利用しているか代表的な例を説明頂きたい。

○　２点目は、セキュリティ部門についてベンダー委託に依存しているとのことだが、今の運用保守等の契約でサイバー対処能力強化法が求める情報共有や届出を阻害する契約条項がないか、また、情報共有や届出対応について料金の追加なく今の契約で対応できる目算があるか説明頂きたい。
○　３点目は、自治体の本庁などのセキュリティ対策について詳細に説明頂いたが、例えば市営病院や学校などの公立の組織に係るセキュリティの課題と協議会への期待があれば説明頂きたい。

北海道

○　１点目は、市町村の場合 1700 の自治体があるので、共通のシステムやパッケージ化されていることが多いと思うが、都道府県の場合は 47 しかないのでパッケージが提供されておらず、フルスクラッチでシステム開発していることが多い。文書管理システムなど市町村と同じものが使える場合はパッケージを使っているが、フルスクラッチを使い続けているものも多い。北海道の知事部局では約 200 のシステムがあるが、フルスクラッチだと、15~20 年、5 年 1 サイクルで保守して 3~4 サイクルを目途に見直しして再開発しているものが多い。
○　２点目は、費用が上がるかどうかも明確になっていない。
○　３点目は、対策基準が病院などは別になっており、それぞれの部局で検討しているところ。

宮崎県都城市

○　１点目は、システムは５年目途に更新している。
○　２点目は、現在調整中。
○　３点目は、市の情報ネットワークに接続している機関については、市の情報セキュリティポリシーが適用されている。それ以外の機関については適用されない。基準や対策があれば国の方で出してほしいと考えている。

広島県坂町

○　１点目は、基幹情報システム系は基本的にはパッケージ化されたシステムをクラウド経由で利用することが多い。
○　２点目は、インシデントが発生すると、本町のネットワーク構成上、ひろしま情報セキュリティクラウドを経由しているので、まずは広島県から連絡がくる。それを踏まえ、具体的な対処については、保守ベンダーと協議の上、実施している。
○　３点目は、国、地方公共団体、重要インフラ事業者等から情報がスムーズに届き、スピーディに情報が共有されることが必要な対処を講じる上で望ましい。

○　北海道に質問させていただく。
○　いただいた説明で情報共有に対するニーズがよく分かった。サイバーセキュリティの確保に当たって注意すべき事項や対処マニュアルは、非常に重要であり、広く周知されるべき情報と思う。
○　他方で、脆弱性に関する情報については、広く周知されるべきとの考え方もあれば、ゼロデイアタックで使用される懸念もあることから、広く知られてはならず、知るべき人がピンポイントで知るべき情報だという考え方もあるが、どのように考えるか教えていただきたい。

○　都城市に質問させていただく。
○　委託についての説明があったが、都城市が委託した事業者から、再委託された事業者について把握されているか。

○　坂町に質問させていただく。
○　システムの保守について、県からの DX 人材派遣制度が有効とのことであったが、ベンダーに委託するよりも派遣された DX 人材の方が信頼おけるというポイントを教えてほしい。
○　官民連携については、事業者の協力を強く要請するとしても、民間がついてこられるような形のインセンティブ設計をすることが重要である。また、業界団体の組織率が業界によってまちまちであることを踏まえれば、網羅性という観点から、関係事業者を全部把握して、連絡のパスをつくるのかといった点も含めて、建付けが重要である。

○　3 自治体へ共通の質問をしたい。迅速な官民連携、情報共有は、3 自治体の共通する期待だと思う。現状、様々な情報ソースがある中で、形式面と内容面でどういう点で過不足があるか伺いたい。形式面としては、発信のタイミング、情報収集の媒体、手段で改善すべき点があれば伺いたい。内容面としては、外部から収集している情報で具体的にどのようなものが不足しており、またどのようなものがあればサイバーセキュリティ対策に役に立つのか教えていただきたい。

○　都城市から、人材が外部化することによって知識が失われるという問題意識があると説明があった。一方で内部で人材を抱えるのが難しいと思うが、どちらの方向が適切なのか。内部の人材であって専門性を高めた人のためのキャリアパスを作るのが望ましいのか、外部人材に委託していかないと回していくと考えていくのか教えてほしい。
○　坂町には、派遣される人材のキャリアパスの構築の方法について教えてほしい。

北海道

○　脆弱性についての情報は必要な者に必要な情報が届くことが重要。

○　情報共有についてお答えする。形式面、内容面について具体的に申し上げられないが、対策のために迅速な情報共有が重要。

宮崎県都城市

○　再委託については、二次までとしており、届け出てもらうようにしている。

○　情報共有の形式については、メールだと他の情報に紛れてしまう可能性があるので、専用サイト等で共有いただきたい。内容については対策の手順を示していただけるとありがたい。

○　人材については、ネットワークが大きくなりすぎて、職員が調整するのが難しく、外部人材を活用することになっていくと思う。

広島県坂町

○　広島県の人材派遣制度について質問があったが、坂町にはセキュリティ専門の人材がいない。県内の市町が個別に人材確保の調整作業を行うのは効率が悪いので、県が一括して人材をプールし、各市町の要請に応じて外部人材を派遣いただいている。ベンダーを定年になった方、システムベンダー、コンサルを経験された方等、様々な方がいる。

○　情報共有については、広島県など、身近なところからいただけるとありがたい。

○　外部人材は必要だが、頼りすぎるのもよくないので、その方と職員がともに学びながら、最終的には自治体で内製化するのが理想。他方で、人員も限られており、直近では外部から専門人材を登用するのが現実的。

（6）次回会合等について

意見交換の後、事務局より以下の通り発言があった。

ヒアリングに対応いただいた日本労働組合総連合会、北海道、宮崎県都城市、広島県坂町に感謝申し上げる。また、構成員から、基本方針を検討する上で重要なご示唆、全体を運用するうえで重要なご示唆をいただき感謝申し上げる。

次回会合でパブリックコメント原案について議論する予定であり、日程は別途連絡する。

以上