（データ編）

データの利活用とセキュリティに関する意識調査

－調査結果－

2023 年 3 月 26 日

一般財団法人 国際経済連携推進センター

目次

はじめに　調査の背景・目的

コロナ禍と地政学的緊張の 2 つの要素により、サイバーセキュリティの考え方が大きく転換を強いられている。情勢の急速な展開の中で、日本のサイバーセキュリティ政策は各省各部局が個別に各局面を扱っている傾向から脱却しにくく、俯瞰視点において新たな状況に対処する必要がある。

当財団主催のタスクフォース「デジタルニューノーマルへの環境整備」では、これまで国境を超えるデータ流通について、ASEAN とインド地域におけるビジネス界の意識調査などの活動を行ってきた。

2022 年は引き続き DFFT の一要素としての「サイバーセキュリティ」に焦点を当て、まずは立ち遅れた国内の現状を浮き彫りにし、国内関係機関向けの提言を行うのみならず、海外の主要な政策議論の場に提示できるようなエビデンス探索の一環としてセキュリティに関するアンケート調査およびインタビュー調査を実施した。また、サイバーセキュリティは DFFT の一要素であることから、DFFT に関するアンケート調査も同時に実施した。

第1章　アンケート調査

1.調査概要

■調査対象国
日本（JP)、アメリカ（US)、シンガポール（SG)、フィリピン（PH)、インド（IN)、オーストラリア（AU)、中国（CN)、タイ（TH)、インドネシア（ID)、台湾（TW)、マレーシア（MY)、ベトナム（VN)、ベルギー（BE）　（合計 13 か国・地域）

■調査方法
調査会社経由で登録パネルに調査票を展開（Web アンケート）

■調査期間
2022 年 3 月 31 日（木）～4 月 27 日（水）　＊各国期間をずらして順次実施

■回答者数
各国 以下のカテゴリ毎に 100 件（各国合計 400 件、全体で 5,200 件）
【消費者対象】セキュリティの感覚を聞く設問群（セキュリティ編）とデータの自由な流通についての意見を聞く設問群（DFFT 編）を別々に各国 2 つの消費者グループに対して調査
【勤労者対象】セキュリティの感覚を聞く設問群（セキュリティ編）とデータの自由な流通についての意見を聞く設問群（DFFT 編）を別々に各国 2 つの勤労者グループに対して調査

■設問内容
消費者対象,勤労者対象の 2 通りについてセキュリティ,データの自由な流通の 2 通り、合計 4 通りの設問群を用意した。それぞれの設問群は回答者の属性、セキュリティに関する意識、信頼に関する意識、データ越境移転についての状況、データ利用に関する意識等、最大 33 問から構成される（各国調査会社がサンプリングを担当)。

2.調査票

（1） 共通設問

F1. あなたの居住地をお答えください。
日本/アメリカ/中国/台湾/オーストラリア/シンガポール/マレーシア/インドネシア/タイ/ベトナム/ベルギー/インド/フィリピン/その他
F2. あなたの性別をお知らせください。
男性/女性/その他
F3. あなたの年代をお知らせください。
10 代/20 代/30 代/40 代/50 代/60 代/70 代/80 代以上
F4. 現在、あなたと同居されている方をすべてお知らせください。（複数選択可）
配偶者/子ども/自分の親/配偶者の親/兄弟・姉妹/孫/恋人・友人/その他/一人暮らし
F5. あなたの職業をお知らせください。
会社・団体の経営者・役員/大学教授・学校教師・研究者/自営業・自由業/会社員・公務員・団体職員（IT 関係・エンジニア）/会社員・公務員・団体職員（総務系）/会社員・公務員・団体職員（その他）/専業主婦・主夫/パート・アルバイト/学生/無職/その他
F6. 下記について、あてはまるものをお知らせください。
対象：ゲーム機（携帯用含む）/通話、テキスト通信用携帯/スマートフォン（ネットができるもの）/PC（ノート、デスクトップ)、タブレット/他社にサービスを提供するためのサーバー/当てはまるものがない
それぞれに対し：個人で所有している/勤め先で支給され所有、または勤め先で関わっている
SC1. あなたが現在勤めている業種についてお答えください。
ICT（情報通信関連）/製造業/不動産・建築業/インフラ（電気・ガス・空調供給等）/金融・保険業/運輸・卸・小売業/医療福祉・社会保障業/その他サービス業（教育・宿泊・飲食・娯楽・その他専門サービス等）/その他
SC2. 現在の部署におけるあなたの立場として最もあてはまるものをお知らせください。
経営者/管理者/一般職/その他
SC3. あなたが勤めている企業の売上高についてお知らせください。
109 万円（10,000USD）未満/ 109 万円～1090 万円（10,000USD-100,000USD）未満/ 1090 万円～1 億 900 万円（100,000USD-1,000,000USD)未満/ 1 億 900 万円～10 億 9000 万円（1,000,000USD-10,000,000USD)未満/ 10 億 9000 万円～109 億円（10,000,000USD-100,000,000USD)未満/ 109 億円～1090 億円(100,000,000USD-1,000,000,000USD)未満/ 1090 億円（1,000,000,000USD)以上/わからない/該当しない
SC4. あなたが勤めている企業の各拠点を合わせた総従業員数についてお知らせください。
1～10 人/11～50 人/51～100 人/101～500 人/501～1000 人/1001 人以上/わからない/該当しない
SC5. 現在の職務における権限において、該当するものをすべてお選びください。
個人情報保護管理あるいは監査/特許、商標権など知財の管理/輸出入管理/財務管理（海外投資などを含む）/ESG 投資、環境、人権/法令順守（コンプライアンス）/上記以外の権限/権限は特にない/該当しない
SC6. 世帯年収をお知らせください。
10.9 万円(USD1,000)未満/ 10.9 万円～54.5 万円（1,000USD-5,000USD）未満/ 54.5 万円～109 万円（5,000USD-10,000USD）未満/ 109 万円～218 万円（10,000USD-20,000USD）未満/ 218 万円～545 万円（20,000USD-50,000USD)未満/ 545 万円～1090 万円（50,000USD-100,000USD)未満/ 1090 万円～2180 万円（100,000USD-200,000USD)未満/ 2180 万円～5450 万円（200,000USD-500,000USD)未満/ 5450 万円（500,000USD)以上/わからない/答えたくない
※SC1～SC5 については、F5 回答が有職者の場合のみ表示される設定

(2) 消費者対象・セキュリティ編

AQ1. 次の言葉の中であなたが全く聞いたことも気にかけたこともない言葉を全て選んでください。(複数選択可)
サイバーセキュリティ/サイバーアタック/コンピュータウィルス/マルウエア/フィッシング/スパム/プライバシー保護/パスワード/秘密計算/アクセス権限/バックドア/インシデント/DOS 攻撃/証明書/認証局/辞書攻撃/非代替性トークン(NFT)/デジタル署名/トロイの木馬/DMZ(社内ネットの外部公開用ゾーン)/ファイアウォール/パッチ、アップデート/メール爆撃/Zoom 爆撃/炎上/ネット個人攻撃/青少年保護/TVEC(テロ暴力極右極左コンテンツ)/盗聴/不正アクセス/(機器、システムの)乗っ取り/ランサムウェア/有害電子商取引/ディープフェイク/フェイクニュース/アノニマス(あるいはハッカー集団)/すべて聞いたことがある
AQ2. 次の中で、その方法をどの程度知りたいと思うか、選んでください。(それぞれ 1 つずつ選択)
対象：自分や家族の住所・氏名・電話番号を盗まれない/自分や家族の購買履歴を盗まれない/自分のネット上での履歴が他人に見られない/自分のクレジットカード番号・銀行口座情報が盗まれない(実害の有無にかかわらず）/自分の外出・移動の行動履歴が盗まれない/自分の交友関係が不適切に知られない/自分の財産が損なわれない/自分の健康が損なわれたり傷つけられたりしない/不快・不要な情報を見せられない/自分が「いじめ」や誹謗中傷、風評の対象にならない/SNS 等で自分の発言が運営によりブロックされたりしない/誰かが自分になりすますのを防ぐ/その他
それぞれに対し：とても知りたいと思う/やや知りたいと思う/どちらともいえない/あまり知りたいと思わない/全く知りたいと思わない
AQ3. あなたはこれまでスマホや PC を利用していて、データに関する被害に遭ったことがありますか。
ある（攻撃者に悪意があったかどうかを問わない）/ない/わからない
AQ4. 自分または身近な人の個人情報が漏洩した経験はありますか。
ある/ない/わからない
AQ5. あなたはスマートフォン、PC、スマートデバイス（通信機能を持つ家電機器を含む）などを守るためにどんな対策をしていますか。(複数選択可)
ログの確認/定期的なパスワードの変更・管理/すべての機器へのセキュリティツールの導入/一部機器へのセキュリティツールの導入/ルーターの防御機能の利用/セキュリティ向上のための学習/その他/対策をしていない
AQ6. あなたはセキュリティソフト、ツールやサービスなどに関して月にいくらくらい使用していますか。
ほとんど使っていない/月に 109 円(1.00USD)以下/月に 1090 円(10USD)以下/月に 5450 円(50USD)以下/月に 10900 円(100USD)以下/それ以上/わからない
AQ7. あなたはどのようなことを危険と思って避けるようにしていますか。(複数選択可)
見知らぬ人からの SNS/心当たりのないメール/怪しいサイト/街や交通機関で PC やスマホの画面を他人から見られないようにする/簡単なパスワードを避ける/同じパスワードを異なるサービスで使いまわすのを避ける/その他/何も避けているものはない
AQ8. あなたは情報セキュリティに関する情報・知識をどこから入手していますか。(複数選択可)
政府の Web サイト/民間の Web サイト/SNS/書籍/TV/IT に詳しい知人から/その他/何も入手していない
AQ9. 以下に示されるサイバーセキュリティに関する考え方の中で、あなたが「そうだ」と思う項目全てを選んでください。(複数選択可)
セキュリティの問題は実際は大した影響はない、私とは無縁である/災害時や医療の緊急時などはセキュリティなどと言っていられない/セキュリティ対策は私の責任ではなく、国やサービス提供の企業の問題である/過度なセキュリティ上の制約は自由を妨げている/何か起こってから対策を考えたらいい/損害が生じることについて、悪意の有無は関係ない/システムの不具合も悪意があったかどうかで受け止め方が違う/私の周りで被害にあった話は聞かないがなんとなく不安である/損害が発生した場合、保険のよ

うに月額費を支払っていればリカバリーしてくれるサービスがあるといい/今は自分でできる限りの注意はしている/自分は大丈夫だと思う/ランサムウェアなどは自分とは関係ない/怪しいメール、SMS、SNSは見ない/怪しいメール、Web サイト等は詳しい人に相談する/データは手元に持っているよりクラウドサービス上に保管した方が安心だと思う/サイバー犯罪は犯人だけでなくサービス事業者にも責任がある/サイバーセキュリティは利用する自分達の側もある程度意識を高めていかなければいけない/特定の国の製品やサービスはセキュリティ上の問題があり利用がためらわれる/事故が起こるのは仕方がないことで、事故が起こった時の対策をしているかどうかの方が重要である/SNS やネットゲーム、仮想空間（メタバース）サービスを提供する民間企業が利用者に対して利用制限、動画収益の制限などをするのはおかしい/セキュリティ上の懸念を理由に子供に携帯を持たせない学校等のルールは逆にいざという時に連絡が取れず不安である/その他

AQ10. 個人の損失データをリカバリーしてくれる保険のようなサービスについて、月額いくらなら許容できますか。

月 109 円(1.00USD)以下/月 1090 円(10USD)以下/月 5450 円(50USD)以下/月 10900 円(100USD)以下/それ以上でもよい

AQ11. パスワードとその管理について、あなたが「そうだ」と思う項目全てを選んでください。(複数選択可)

ついパスワードを忘れてしまう/パスワードを求められることが多すぎる/パスワードがたくさんあり、管理しきれない/サービスごとにパスワードを変えるのは面倒/パスワードの書式（使える文字や文字数など）がバラバラで面倒/パスワードを使わずに済む方法があればその方がいい/スマホや銀行のトークンなどで毎回変わる暗号キーが安心できる/パスワードを厳重にすることの意味が実感できない/パスワードを紙のメモに書き留めている/パスワードを電子的なメモに書き留めている/あてはまるものはない

AQ12. サイバーセキュリティに関して、あなたの財産、生命と健康を守るために、信頼し助力を期待できる相手はどこでしょうか。信頼できると思う順にお答えください。

1 位 / 2 位 / 3 位

それぞれ対象：政府/政府の認証する機関/職場/セキュリティ民間企業/通信サービス提供事業者/個別サービスの提供事業者（金融・医療等）/友人・知人/家族/テレビや YouTube などネットメディアで有名な人/その他

AQ13. あなた個人の情報を取り扱うサービス・機関について、安心して利用できるというものを全て選んでください。(複数選択可)

SNS/ブログサイト/クラウドサービス(第三者認証を受けている)/その他民間サービス/政府・自治体/その他/どこにも預けてよいと思えない

AQ14. SNS、アプリ、Web サービスなどを利用するにあたり、次の項目はどの程度気になりますか。

対象：運営者の国籍/サーバーの所在地/過去の事件の有無/評判/運営者の国の法整備/利用規約・サービス規約/多要素認証の有無/実装されているセキュリティ機能/その他

それぞれに対し：かなり気になる/少し気になる/どちらともいえない/あまり気にならない/全く気にならない/わからない・その言葉を理解していない

AQ15. セキュリティ確保のためにとられる以下のような仕組みについてどう思いますか。(それぞれ複数選択可)

対象：顔認証/指紋認証/音声認識/虹彩認識/ワンタイムパスワード/二段階認証/銀行などで交付されるワンタイムキー生成器

それぞれに対し：安心できる/便利でつかいやすい/使いづらい/効果があるのか疑わしい/気持ち悪い/その他/わからない

AQ16. その理由として、どのようなことが考えられますか。(それぞれ複数選択可)

対象：顔認証/指紋認証/音声認識/虹彩認識/ワンタイムパスワード/二段階認証

それぞれに対し：恥ずかしい/個人情報が気になる/データを悪用されないか不安/パスワードなど覚えている必要がない/他人に乗っ取られにくい/認証に時間がかかる/その他/わからない

AQ17. 次の事項について、あなたは気になりますか。(それぞれ1つずつ選択)
対象：住所や氏名等の個人情報が流通すること/GPS 情報や閲覧・購買履歴などの個人関連情報が流通すること/その他自分に関する情報が流通すること/直接財産を侵害される恐れ/なりすまし/アクセスしたWebサイトなどで端末情報が取られること
それぞれに対し：かなり気になる/少し気になる/どちらともいえない/あまり気にならない/全く気にならない/わからない・その言葉を理解していない
AQ18. あなたが政府、企業、組織、個人などを信頼する際の考えとして同意できるものを全て選んでください。(複数選択可)
自己の財産や所有物を奪わず、保護してくれる/自己の情報に過度の干渉せず安全に取り扱ってくれる/自分の期待に応えてくれる/騙そうとしない/考え方に共感が持てる/その他/あてはまるものはない
AQ19. 以下に示される考え方の中で、それぞれどの程度「そうだ」と思いますか。(それぞれ1つずつ選択)
対象：DFFTという言葉を知っている、聞いたことがある/データの取り扱いルールが理解しやすく運用も透明でないとならない/データに関連する技術が統一されて使いこなせないとならない/国や事業者が違っても、データの扱いに大きな違いを意識することなく負担が少ないことが大事/いろんなルールが絡み合ってときにどっちを守ればいいかわからなくなるようなことがないことが大事/信頼のおけるデータの具体的な方策を考えてもらいたい
それぞれに対し：非常にそう思う（知っている）/ややそう思う（知っている）/どちらともいえない/あまりそう思わない（知らない）/全くそう思わない（知らない）/わからない・その言葉を理解していない
AQ20-1. 時事問題についての意見をお尋ねします。(それぞれ1つずつ選択)
対象：(消費者の視点でも）民間企業へのサイバー攻撃を脅威と感じる/偏った情報流通により世論が左右されることを脅威と感じる/ネット上でも言論の自由を妨げるべきではない/身代金詐欺、ランサムウェアは社会全体の課題として対応すべきである/企業がビジネスを継続するためにサイバーセキュリティの確保が重要である/民間企業は各国制度の違いを乗り越えて事業拡大の努力をしている/移住したり事業進出する国の法制度が大多数の他国のものと異なっていても黙って従うべきである/多様性を認めつつ法制度を共通化することは世界経済の発展のために必要である/政府が民間企業のサービスに介入・干渉・アクセスする範囲は最小限でなければならない/インターネット上のデータの流れは自由であるべきだ/インターネット上のデータの流れを制御したり止めることはできない/安全を確保するためにある程度データの流通を制限することは必要である
それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない
AQ20-2. 信頼の内容についての意見を聞きます。あなたが最も信頼できると考える人あるいは組織をいくつか思い浮かべてください。その人あるいは組織はどういう理由で信頼できると感じましたか？(それぞれ1つずつ選択)
対象：長い期間安定して歴史があり継続している（実績）/事件があったときにすぐに対応でき回復が速やかである（レジリアンス）/説明が丁寧でわかりやすい（理解）/お金持ち、あるいは財務状況がしっかりしている（財務状況）/マスコミやテレビでよく取り上げられ有名（有名）/ネットで評判が良い（「いいね」）/自分の知っている人がその人・組織と関わっている（関係性）/法律やルールをきちんと守っている（法令順守）/行動に正当な理由がある（比例性）/やりたいことがよくわかり見通せる（透明性）/一方的でなく自分の承認や理解を得ようとしてくれている（承認）/明快な節度と制限を持ち無制限に要求してこない（制限）/公的な機関や第三者が監督監視してくれている（監督）/その人・組織とは何かあったときの保険・救済措置がある（救済）/分け隔てなく差別をせず、公平である（公平）/時と場合によって変わらず一律に一貫性があり対応してくれる（一貫性）/グローバルな基準において差別がなくフェアである（公正）/その人・組織は自分に思いもよらない責任を転嫁しない（責任制限）/その人・組織は他の人・組織と相反せず整合していて敵を作らない（整合）
それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない

(3) 消費者対象・DFFT 編

BQ1. 次の言葉の中であなたが関心があり、より多く知りたいと思う言葉を全て選んでください。(複数選択可)
ガバメントアクセス（政府によるデータ取得と支配）/なりすまし詐欺・フィッシングなどセキュリティの課題/フェイクニュース/サイバー空間炎上・人格攻撃・青少年保護/サプライチェーンの混乱/知的財産・不正コピー・著作権侵害・海賊版/盗聴・盗撮/オンライン上の誹謗中傷/個人情報漏洩・不正利用/オンライン購入に伴うトラブル/オンラインサービス・アプリの不具合/デジタル利用による格差の助長/情報や学習機会の欠如/サービスの不安定・停止/デジタル技術を使った犯罪/人工知能技術の開発・利用倫理/デジタル技術進展による雇用不安/デジタル技術からくる安全保障上の課題/データやサービスの独占や寡占/脱税・不正蓄財・マネーロンダリング/違法薬物取引/暗号通貨による不正送金/格差の助長/ディープフェイク/情報戦・情報操作/アノニマス・ハッカー集団/ディープ WEB/あてはまるものはない
BQ2. あなたはデジタルのサービスをどの程度活用していますか。（それぞれ 1 つずつ選択）
対象：LINE/Facebook/Instagram/Twitter/Viber/WhatsApp/Weibo/WeChat/その他 SNS/YouTube（視聴だけ）/TikTok（視聴だけ）/Netflix/Prime Video/その他動画配信サービス/動画投稿（Youtube, Tiktok など）/音楽配信サービス/Telegram/reddit/Wechatpay/Apple Pay/Alipay/Paypal/その他電子決済/国外コンテンツ/国内コンテンツ/個人輸入サービス/国内ニュースサイト/国外ニュースサイト
それぞれに対し：全く使っていない/無償利用の範囲/月額 109 円（1.00USD）未満の利用/月額 109 円～1090 円（1.00USD～10USD）未満の利用/月額 1090 円～10900 円（10USD～100USD）未満の利用/月額 10900 円（100USD）以上の利用/利用金額はわからないが有償利用している
BQ3. 以下に示されるデータ利用に関する考え方の中で、あなたが「そうだ」と思う項目全てを選んでください。(複数選択可)
データの利用範囲を国内に限定してもらうほうが安心する/自分に関しては何も隠すことはなく、データの利用は最大限に自由であるべきである/データの利用範囲は最小限であるべきである/データを守ることよりも購買ポイントがついたり経済的利益が生じることのほうが重要と思う/デジタル化によって信頼の感覚がだいぶん異なってきていると思う/正直なところ何をどう信頼していいのかはまだよくわかっていない/デジタル化の進展によって、信頼できる企業とそうでない企業の差が鮮明になってきたと思う/正直なところデジタル技術そのものについて信頼をしていない/政府はもっとデジタル課題について力を入れるべきである/特定の国のデジタル政策が自分の生活にも影響を及ぼし始めていると思う/あてはまるものはない
BQ4. データの提供先について、あなたが関心のあることを全て選んでください。(複数選択可)
個人データが安全に処理・管理されているか/自分の個人データの移転先・所在地/自分の個人データ移転先の国の法制度/自分の個人データ移転先の国での取り扱い/自分の個人データが移転先の国の政府により閲覧されるかどうか（ガバメントアクセス制度・状況）/提供後に拒否する権利があるかどうか/その他/あてはまるものはない
BQ5. デジタル技術に関して、あなたの財産、生命と健康を守るために、信頼し助力を期待できる相手はどこでしょうか。信頼できると思う順にお答えください。（それぞれ 1 つずつ選択）
1 位 / 2 位 / 3 位
それぞれ対象：政府/政府の認証する機関/職場/セキュリティ民間企業/通信サービス提供事業者/個別サービスの提供事業者（金融・医療等）/友人・知人/家族/テレビや Youtube などネットメディアで有名な人/その他
BQ6. 政府が令状、裁判所命令、召喚状などの法的要求を利用して、オンラインサービスや製品のプロバイダー（例：電子メールプロバイダー）を通じてお客様のデータにアクセスしようとすることについて、どの程度懸念しますか。
大変懸念がある/やや懸念がある/どちらともいえない/あまり影響はない/全く影響はない

BQ7. 外国政府が自分のデータにアクセスできる可能性があることが、外国にあるオンラインサービスや製品を利用する際の判断に影響しますか。

非常に影響がある/やや影響がある/どちらともいえない/あまり影響はない/全く影響はない

BQ8. サイバー攻撃によって政府や企業、個人があなたのデータにアクセスすることについて懸念がありますか。（複数選択可）

自国政府のアクセスに懸念がある/外国政府のアクセスに懸念がある/自国企業からのアクセスに懸念がある/外国企業からのアクセスに懸念がある/自国の個人からのアクセスに懸念がある/外国の個人からのアクセスに懸念がある/あてはまるものはない

BQ9. 信頼を高め、国境を越えたデータフローの障壁を減らすためには、どのような施策が役立つと思いますか。（複数選択可）

あいまいでなく確実な法律の整備/国の間で共通したプライバシーの保護の枠組み/民間企業が持つデータを政府が利用する時の規律整備と国際的な合意/サイバー攻撃を防止する国際的合意/被害が生じた時の補償制度の国際共通化/データの移転に制限をかける規制の撤廃/その他

BQ10. 国外のサービスを利用する場合、どの国のサービスが多いでしょうか。（複数選択可）

日本/米国/EU 全体/英国/オーストラリア/カナダ/ドイツ/フランス/オランダ/スペイン/イタリア/ベルギー/ルクセンブルグ/アイルランド/ポーランド/チェコ/ハンガリー/ロシア/トルコ/中国/韓国/台湾/香港/シンガポール/インドネシア/マレーシア/タイ/ベトナム/フィリピン/インド/ニュージーランド/その他アジア諸国/アフリカ諸国/南アメリカ諸国/その他ヨーロッパ諸国/外国のサービス利用はしていない・わからない

BQ11. 越境データ流通に関してどの国・地域における規制が最も深刻にビジネスに脅威を与えるでしょうか。（３つまで選択可）

日本/米国/EU 全体/英国/オーストラリア/カナダ/ドイツ/フランス/オランダ/スペイン/イタリア/ベルギー/ルクセンブルグ/アイルランド/ポーランド/チェコ/ハンガリー/ロシア/トルコ/中国/韓国/台湾/香港/シンガポール/インドネシア/マレーシア/タイ/ベトナム/フィリピン/インド/ニュージーランド/その他アジア諸国/アフリカ諸国/南アメリカ諸国/その他ヨーロッパ諸国/データ越境流通はしていない・わからない

BQ12. 以下に示される考え方の中で、それぞれどの程度「そうだ」と思いますか。（それぞれ１つずつ選択）

対象：DFFT という言葉を知っている、聞いたことがある/データの取り扱いルールが理解しやすく運用も透明でないとならない/データに関連する技術が統一されて使いこなせないとならない/国や事業者が違っても、データの扱いに大きな違いを意識することなく負担が少ないことが大事/いろんなルールが絡み合ってときにどっちを守ればいいかわからなくなるようなことがないことが大事/信頼のおけるデータの具体的な方策を考えてもらいたい

それぞれに対し：非常にそう思う（知っている）/ややそう思う（知っている）/どちらともいえない/あまりそう思わない（知らない）/全くそう思わない（知らない）/わからない・その言葉を理解していない

BQ13-1. 時事問題についての意見をお尋ねします。（それぞれ１つずつ選択）

対象：（消費者の視点でも）民間企業へのサイバー攻撃を脅威と感じる/偏った情報流通により世論が左右されることを脅威と感じる/ネット上でも言論の自由を妨げるべきではない/身代金詐欺、ランサムウェアは社会全体の課題として対応すべきである/企業がビジネスを継続するためにサイバーセキュリティの確保が重要である/民間企業は各国制度の違いを乗り越えて事業拡大の努力をしている/移住したり事業進出する国の法制度が大多数の他国のものと異なっていても黙って従うべきである/多様性を認めつつ法制度を共通化することは世界経済の発展のために必要である/政府が民間企業のサービスに介入・干渉・アクセスする範囲は最小限でなければならない/インターネット上のデータの流れは自由であるべきだ/インターネット上のデータの流れを制御したり止めることはできない/安全を確保するためにある程度データの流通を制限することは必要である

それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない

BQ13-2. 信頼の内容についての意見を聞きます。あなたが最も信頼できると考える人あるいは組織をいくつか思い浮かべてください。その人あるいは組織はどういう理由で信頼できると感じましたか？（それぞれ１つずつ選択）

対象：長い期間安定して歴史があり継続している（実績）/事件があったときにすぐに対応でき回復が速やかである（レジリアンス）/説明が丁寧でわかりやすい（理解）/お金持ち、あるいは財務状況がしっかりしている（財務状況）/マスコミやテレビでよく取り上げられ有名（有名）/ネットで評判が良い（「いいね」）/自分の知っている人がその人・組織と関わっている（関係性）/法律やルールをきちんと守っている（法令順守）/行動に正当な理由がある（比例性）/やりたいことがよくわかり見通せる（透明性）/一方的でなく自分の承認や理解を得ようとしてくれている（承認）/明快な節度と制限を持ち無制限に要求してこない（制限）/公的な機関や第三者が監督監視してくれている（監督）/その人・組織とは何かあったときの保険・救済措置がある（救済）/分け隔てなく差別をせず、公平である（公平）/時と場合によって変わらず一律に一貫性があり対応してくれる（一貫性）/グローバルな基準において差別がなくフェアである（公正）/その人・組織は自分に思いもよらない責任を転嫁しない（責任制限）/その人・組織は他の人・組織と相反せず整合していて敵を作らない（整合）

それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない

（4） 勤労者対象・セキュリティ編

CQ1. 次の言葉の中であなたが全く聞いたことも気にかけたこともない言葉を全て選んでください。(複数選択可)

サイバーリスク/サイバーセキュリティ/サイバーアタック/コンピュータウィルス/マルウエア/フィッシング/スパム/プライバシー保護/パスワード/秘密計算/アクセス制限/バックドア/インシデント/DOS攻撃/証明書/認証局/辞書攻撃/非代替性トークン(NFT)/デジタル署名/トロイの木馬/DMZ（社内ネットの外部公開用ゾーン）/ファイアウォール/パッチ、アップデート/メール爆撃/Zoom 爆撃/炎上/ネット個人攻撃/青少年保護/TVEC(テロ暴力極右極左コンテンツ)/盗聴/不正アクセス/(機器、システムの)乗っ取り/ランサムウェア/有害電子商取引/ディープフェイク/フェイクニュース/アノニマス(あるいはハッカー集団)/すべて聞いたことがある

CQ2. 次の中で、その方法をどの程度知りたいと思うか、選んでください。（それぞれ１つずつ選択）

対象：形式主義にとらわれないセキュリティ確保の方法/拠点の場所や電話番号を知られない/営業秘密を盗まれない/取引先関係が不適切に知られない/顧客の情報が盗まれない/支払いのクレジットカード番号・銀行口座情報が盗まれない（実害の有無にかかわらず）/事業所の財産が損なわれない/社員の健康が損なわれたり傷つけられたりしない/自社が運営するサービスに外部からサイバー攻撃を受けない/内部犯行により自社のサービスに支障が起きない/自社が誹謗中傷、風評被害の対象にならない/事業上必要なネットワークやサービスの利用が運営によりブロックされたりしない/誰かが自社を騙ってなりすましを行うを防ぐ/パスワードだけに頼らないデータの安全な共有方法（外部送信を含む）/組織の活性やイノベーション意欲を削がないセキュリティ確保の方法/その他

それぞれに対し：とても知りたいと思う/やや知りたいと思う/どちらともいえない/あまり知りたいと思わない/全く知りたいと思わない

CQ3. あなたの勤め先ではこれまでスマホやPCを利用していて、データに関する被害に遭ったことがありますか？

ある（攻撃者に悪意があったかどうかを問わない）/ない/わからない

CQ4. 自社で扱う個人情報や機密情報が漏洩した経験はありますか。金銭的損害（失った商機、顧客等を含めて）で大まかにお答えください。

ない/あったが損害はない/軽微な損害があった（概ね年間売り上げの 10%未満）/やや損害があった（概ね年間売り上げの 10%-30%に相当/かなり損害があった（概ね年間売り上げの 30%-60%に相当）/大き

な損害を生じた（概ね年間売り上げの 60%以上）
CQ5. あなたの勤め先ではスマートフォン、PC、スマートデバイス（通信機能を持つ機器を含む)、他社にサービスを提供するためのサーバーなどを守るためにどんな対策をしていますか。(複数選択可)
ログの確認/ハイリスクのデータやネットワークセグメントの分割/定期的なパスワードの変更・管理/すべての機器へのセキュリティツールの導入/一部機器へのセキュリティツールの導入/ルーターの防御機能の利用/セキュリティ向上のための学習/その他/対策をしていない
CQ6. セキュリティ意識について、会社(勤め先の)組織としてどのような啓発活動をされていますか。(ユーザーとして受けていますか？)　※自由記述、任意
CQ7. 組織としてのセキュリティ教育・情報提供は十分だと思いますか。
非常に十分だと思う/まあ十分だと思う/どちらともいえない/あまり十分だと思わない/全く十分だと思わない
CQ8. 以下に示されるサイバーセキュリティに関する考え方の中で、あなたが「そうだ」と思う項目全てを選んでください（複数選択可）
組織の過度なセキュリティポリシーによって、業務に支障が生じたことがある/組織から遠隔会議や必要な情報へのアクセスが禁止されていて困ったことがある/セキュリティ対策として求められることは本当に必要なのかどうか納得できていない/形式的なセキュリティ管理は時間の無駄/本来の仕事の時間を削ってまでセキュリティ関連に手間をかけるのは本末転倒である/今の勤め先のセキュリティ対策は意味がない、またはやりすぎではないかと思うことがある/何か問題が生じた時に責任の所在が明確ではないと思う/不正リンクや不正情報を開かないようにするのは社員として当然の注意義務だと思う/私用の機器（スマホ、PC など）と業務用の機器を別々に管理し、持ち歩くのは現実的でない/データは手元に持っているよりクラウドサービス上に保管した方が安心だと思う/何か起こってから対策を考えたらいい/悪意はないシステムの不具合により生じた損害も大きい/適切な負担であれば保険のように損害を補填してくれるサービスがあるといい/パスワードの管理にあまり注意を払っていない/サービス毎にパスワードを色々と考えるのは面倒、逆にきちんと管理できない/今のパスワード管理に頼る方法はおかしいと思う/パスワードを使わずに済む方法があると良い/ランサムウェアなどは自分とは関係ない/サイバー犯罪は犯人だけでなくサービス事業者にも責任がある/サイバーセキュリティは利用する自分達の側もある程度意識を高めていかなければいけない/特定の国の製品やサービスの利用には注意が必要である/事故が起こるのは仕方がないことで、事故が起こった時の対策をしているかどうかの方が重要である/過剰なセキュリティ管理は組織の活性とイノベーションを妨げている/セキュリティの確保は自分の勤め先・組織だけの努力でこれ以上向上させることはできない(顧客や取引先、社会全体の協力が必要だ) /その他
CQ9. セキュリティに関する規制により、勤め先のビジネスモデルを変換せざるを得なくなったケースはありますか。
大きく変換した/多少だが変換した/わからない/多少の変更はあってもそこまで大きな影響はない/全くない
CQ10. 厳格なセキュリティ対策を理由にあなたの勤務先がサプライチェーンから排除されたり、商機を逃がしたことがありますか。どの程度の損失があったかを基準としてお答えください。
経験はない/商機を逃したことはあるが損害はない/年間売り上げの 10%未満の影響/年間売り上げの 10-30%の影響/年間売り上げの 30%-60%の影響/年間売り上げの 60%以上の影響
CQ11. あなたの組織、業務を守るために、信頼し助力を期待できる相手はどこでしょうか。信頼できると思う順にお答えください。
1 位 / 2 位 / 3 位
それぞれ対象：政府/政府の認証する公的機関/職場の情報システム担当部署/職場の所属部署/セキュリティに関するサービスを行う民間企業/通信サービス提供事業者/個別サービスの提供事業者（金融・医療等）/同僚（セキュリティ担当者）/コンサルタント/顧客企業・組織/業務上の取引関係がある企業・組織/その他
CQ12. セキュリティ対策を取ることになったきっかけは何ですか。(複数選択可)

トップダウンでの決定/自社で発生したインシデント/同業他社で発生したインシデント/投資家・取引先からの要請/その他/対策をしていない
CQ13. あなたの勤め先の経営者（CEO）はセキュリティ対策に関与していますか。
経営者は重要性を理解し実践している/経営者は部下からの説得により理解・実践している/経営者は投資家・取引先からの要請があれば対策を実施している/経営者は対策の重要性を理解しているが実施を認めない（予算措置・人的リソースを割り当てない）/経営者は対策の重要性を理解していない/わからない
CQ14. あなたが政府、企業、組織、個人などを信頼する際の考えとして同意できるものを全て選んでください。（複数選択可）
自己の財産や所有物を奪わず、保護してくれる/自己の情報に過度の干渉せず安全に取り扱ってくれる/自分の期待に応えてくれる/騙そうとしない/考え方に共感が持てる/その他/あてはまるものはない
CQ15. 以下に示される考え方の中で、それぞれどの程度「そうだ」と思いますか。（それぞれ１つずつ選択）
対象：DFFT という言葉を知っている、聞いたことがある/データの取り扱いルールが理解しやすく運用も透明でないとならない/データに関連する技術が統一されて使いこなせないとならない/国や事業者が違っても、データの扱いに大きな違いを意識することなく負担が少ないことが大事/いろんなルールが絡み合ってときにどっちを守ればいいかわからなくなるようなことがないことが大事/信頼のおけるデータの具体的な方策を考えてもらいたい
それぞれに対し：非常にそう思う（知っている）/ややそう思う（知っている）/どちらともいえない/あまりそう思わない（知らない）/全くそう思わない（知らない）/わからない・その言葉を理解していない
CQ16-1. 時事問題についての意見をお尋ねします。（それぞれ１つずつ選択）
対象：（消費者の視点でも）民間企業へのサイバー攻撃を脅威と感じる/偏った情報流通により世論が左右されることを脅威と感じる/ネット上でも言論の自由を妨げるべきではない/身代金詐欺、ランサムウェアは社会全体の課題として対応すべきである/企業がビジネスを継続するためにサイバーセキュリティの確保が重要である/民間企業は各国制度の違いを乗り越えて事業拡大の努力をしている/移住したり事業進出する国の法制度が大多数の他国のものと異なっていても黙って従うべきである/多様性を認めつつ法制度を共通化することは世界経済の発展のために必要である/政府が民間企業のサービスに介入・干渉・アクセスする範囲は最小限でなければならない/インターネット上のデータの流れは自由であるべきだ/インターネット上のデータの流れを制御したり止めることはできない/安全を確保するためにある程度データの流通を制限することは必要である
それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない
CQ16-2. 信頼の内容についての意見を聞きます。あなたが最も信頼できると考える人あるいは組織をいくつか思い浮かべてください。その人あるいは組織はどういう理由で信頼できると感じましたか？（それぞれ１つずつ選択）
対象：長い期間安定して歴史があり継続している（実績）/事件があったときにすぐに対応でき回復が速やかである（レジリアンス）/説明が丁寧でわかりやすい（理解）/お金持ち、あるいは財務状況がしっかりしている（財務状況）/マスコミやテレビでよく取り上げられ有名（有名）/ネットで評判が良い（「いいね」）/自分の知っている人がその人・組織と関わっている（関係性）/法律やルールをきちんと守っている（法令順守）/行動に正当な理由がある（比例性）/やりたいことがよくわかり見通せる（透明性）/一方的でなく自分の承認や理解を得ようとしてくれている（承認）/明快な節度と制限を持ち無制限に要求してこない（制限）/公的な機関や第三者が監督監視してくれている（監督）/その人・組織とは何かあったときの保険・救済措置がある（救済）/分け隔てなく差別をせず、公平である（公平）/時と場合によって変わらず一律に一貫性があり対応してくれる（一貫性）/グローバルな基準において差別がなくフェアである（公正）/その人・組織は自分に思いもよらない責任を転嫁しない（責任制限）/その人・組織は他の人・組織と相反せず整合していて敵を作らない（整合）
それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない
CQ17. 信頼性のある自由なデータ流通を実現するための要素として、あなたはそれぞれどの程度同意で

きますか。（それぞれ１つずつ選択）
対象：関連する規制に関する透明性の確保/プライバシー・セキュリティ確保技術の標準化/各国相互の運用性確保/関連する制度との補完性検討/信頼性のある自由なデータ流通枠組みの実装
それぞれに対し：大変同意できる/やや同意できる/どちらともいえない/あまり同意できない/全く同意できない/わからない・その言葉を理解していない

（5） 勤労者対象・DFFT 編

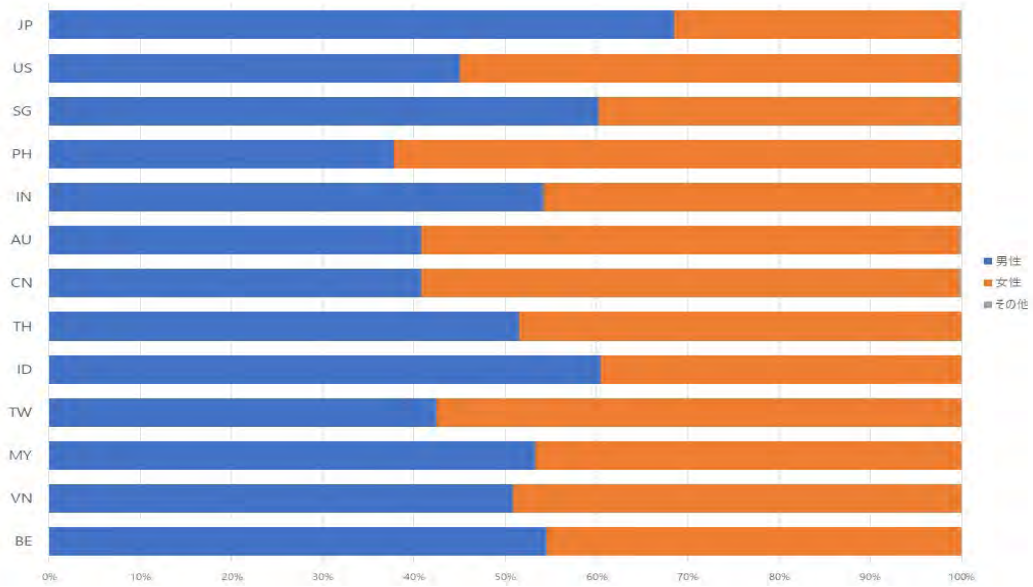
DQ1. 次の言葉の中であなたが関心があり、より多く知りたいと思う言葉を全て選んでください。(複数選択可)
ガバメントアクセス（政府によるデータ取得と支配）/ソースコード開示要求/情報の国内強制保管（データローカライゼーション）/越境データの自由流通の阻害/媒介者責任に関連するルール/サプライチェーンの安全安定/経済安全保障/技術情報の漏洩/なりすまし詐欺・フィッシングなどセキュリティの課題/フェイクニュース/サイバー空間炎上・人格攻撃・青少年保護/商標など知的財産・不正コピー・著作権侵害/データの窃盗・盗聴/オンライン上の誹謗中傷・風評被害/個人情報漏洩・不正利用/オンライン取引に伴うトラブル/オンラインサービス・アプリの不具合/デジタル利用による格差の助長/情報や学習機会の欠如/サービスの不安定・停止/デジタル技術の悪用/人工知能技術の開発・利用倫理/デジタル技術進展による雇用不安/デジタル技術からくる安全保障上の課題/データやサービスの独占や寡占/脱税・不正蓄財・マネーロンダリング/違法薬物取引/暗号通貨による不正送金/イノベーションや起業の阻害/地球環境・温暖化とデジタル変革/人権とデジタル変革/あてはまるものはない
DQ2. あなたが業務上利用するデータは次のうちどれが多いでしょうか。また、それらのうち、自社データと他社データの割合はどの程度でしょうか。（それぞれ１つずつ選択）
業務上利用するデータ：主として国内のデータ/国外データもあるが国内データが多い/国内国外同程度のデータ/国内データもあるが国外データが多い/主として国外のデータ/わからない・データを取り扱わない
自社データと他社データの割合：自社データのみ/数割程度の他社共有データが含まれる/半分程度が他社共有データ/ほとんどが他社共有データ/わからない・データを取り扱わない
DQ3. 海外との間で業務でデータを移転する場合、どの国との間が最も多いでしょうか。該当国のデータを扱う、該当国へデータを移転する双方を含みます。（３つまで選択可）
日本/米国/EU 全体/英国/オーストラリア/カナダ/ドイツ/フランス/オランダ/スペイン/イタリア/ベルギー/ルクセンブルグ/アイルランド/ポーランド/チェコ/ハンガリー/ロシア/トルコ/中国/韓国/台湾/香港/シンガポール/インドネシア/マレーシア/タイ/ベトナム/フィリピン/インド/ニュージーランド/その他アジア諸国/アフリカ諸国/南アメリカ諸国/その他ヨーロッパ諸国
DQ4. 以下に示される越境データ流通に関する考え方の中で、あなたがビジネスユーザーとして「そうだ」と思う項目全てを選んでください。(複数選択可)
データは石油などに替わる新たな資源である/データの利活用により新たな事業機会が生まれる/私の業界ではデータの利用は既存ビジネスを支える副次的なものに過ぎない/データの活用により今までのビジネスを完全に置き換える新しい事業に取り組まないといけない/データの利活用は理解し難く有効化しにくい/データに関する政策や規制はまだ方針が定まっていないので積極的に声を上げてルール作りに参加していかないといけない/政府が示すデータに関するルールを追随していればそれで良い/データの管理は様々な視点から取り組まないとならず難しい/デジタル変革にはコストがかかる/デジタル変革を行うことでより多くのリスクを抱え込むことになる/デジタルに関する「信頼」を顧客・関連企業・政府・社会と構築することでコストとリスクを低減させることができる/信頼を構築した相手とはいくつかの課題をあらかじめ解決し、煩雑な手順を省略しリスクを下げることができる/デジタルにおける信頼はこれまでのビジネスにおける信用とはだいぶ異なる/あてはまるものはない

DQ5. データの越境流通について過度な制限が課せられた場合、あなたのビジネスへの影響はどの程度でしょうか。
ほとんどの取引に深刻な支障が出る/半分程度の取引に深刻な支障が出る/数割の取引に深刻な支障が出る/ほとんど影響はない
DQ6. 所在国の政府、あるいは取引のある国の政府によるデータの開示要求や支配が過度に強まるとあなたのビジネスへの影響はどの程度になるでしょうか。
ほとんどの取引に深刻な支障が出る/半分程度の取引に深刻な支障が出る/数割の取引に深刻な支障が出る/ほとんど影響はない
DQ7. 越境データ流通に関してどの国・地域における規制が最も深刻にビジネスに脅威を与えるでしょうか。（３つまで選択可）
日本/米国/EU 全体/英国/オーストラリア/カナダ/ドイツ/フランス/オランダ/スペイン/イタリア/ベルギー/ルクセンブルグ/アイルランド/ポーランド/チェコ/ハンガリー/ロシア/トルコ/中国/韓国/台湾/香港/シンガポール/インドネシア/マレーシア/タイ/ベトナム/フィリピン/インド/ニュージーランド/その他アジア諸国/アフリカ諸国/南アメリカ諸国/その他ヨーロッパ諸国/データ越境流通はしていない・わからない
DQ8. 政府が令状、裁判所命令、召喚状などの法的要求を利用して、オンラインサービスや製品のプロバイダー（例：電子メールプロバイダー）を通じて顧客のデータにアクセスしようとすることについて、どの程度懸念しますか。
大変懸念がある/やや懸念がある/どちらともいえない/あまり懸念はない/全く懸念はない
DQ9. 政府が自社のデータにアクセスできる可能性があることが、国内外との取引に影響がありますか？
ほとんどの取引に深刻な支障が出る/半分程度の取引に深刻な支障が出る/数割の取引に深刻な支障が出る/ほとんど影響はない
DQ10. サイバー攻撃によって外国政府があなたの勤め先のデータにアクセスすることについて、どの程度影響がありますか。
ほとんどの取引に深刻な支障が出る/半分程度の取引に深刻な支障が出る/数割の取引に深刻な支障が出る/ほとんど影響はない
DQ11. 政府のアクセスからデータを保護するために、データをローカルに保存したり、特定のサービスや製品を避けたり、暗号化を利用するなどの対策を取ったことはありますか。
何度もある/わずかだがある/どちらともいえない/あまりない/全くない
DQ12. 顧客の信頼を高め、国境を越えたデータフローの障壁を減らすためには、どのようなことが重要だと思いますか。（複数選択可）
あいまいでなく確実な法律の整備/国の間で共通したプライバシーの保護の枠組み/民間企業が持つデータを政府が利用する時の規律整備と国際的な合意/サイバー攻撃を防止する国際的合意/被害が生じた時の補償制度の国際共通化/データの移転に制限をかける規制の撤廃/その他/重要だと思うことはない
DQ13. 取引相手を信用するにあたり、第三者認証や国際標準をどの程度信頼しますか。また、自社が信頼を受けるために役に立つと思いますか。（それぞれ１つずつ選択）
取引相手が認証や標準を取得している場合 / 自社が認証や標準を取得する場合（取引相手から見た場合）
それぞれに対し：かなり信頼できる、信頼される/まあ信頼できる、信頼される/どちらともいえない/あまり信頼できない、信頼されない/全く信頼できない、信頼されない/わからない
DQ14.「顧客一件（消費者の場合一人）」に対して、製品やサービスへの信頼を得るための投資はいくらくらいまでかけて行うべきと考えますか。
売上（年収）の 1%以下/売上（年収）の 5%以下/売上（年収）の 10%以下/それ以上でも信頼を得られるのであれば投資する/投資しない
DQ15. 自社の本店・支店がある国でセキュリティ・個人情報保護・知財保護等の過度な規制によりその

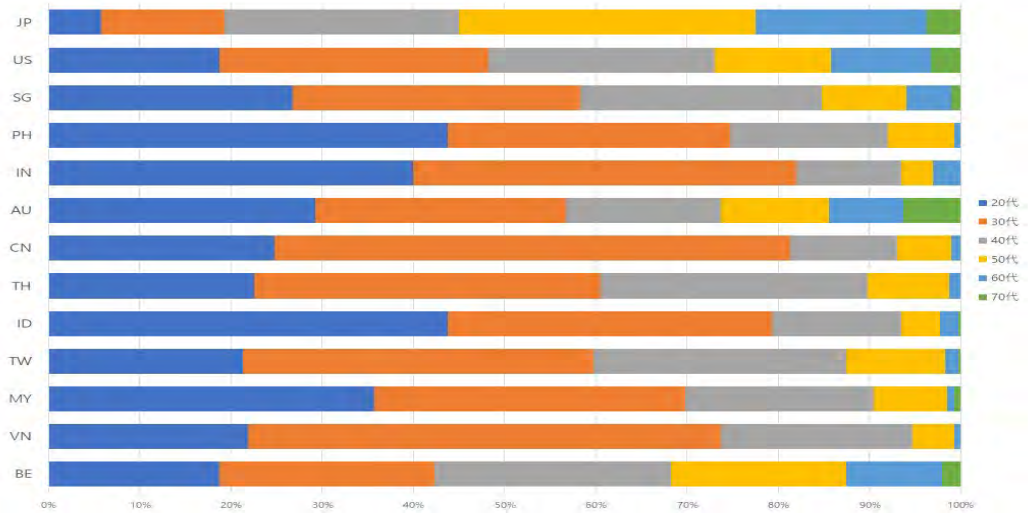
国への投資を引き揚げた（現地法人撤退・本社移転）をした例はありますか。
ある/ない/わからない
DQ16. あなたが政府、企業、組織、個人などを信頼する際の考えとして同意できるものを全て選んでください。（複数選択可）
自己の財産や所有物を奪わず、保護してくれる/自己の情報に過度の干渉せず安全に取り扱ってくれる/自分の期待に応えてくれる/騙そうとしない/考え方に共感が持てる/その他/あてはまるものはない
DQ17. 以下に示される考え方の中で、それぞれどの程度「そうだ」と思いますか。（それぞれ１つずつ選択）
対象：DFFT という言葉を知っている、聞いたことがある/データの取り扱いルールが理解しやすく運用も透明でないとならない/データに関連する技術が統一されて使いこなせないとならない/国や事業者が違っても、データの扱いに大きな違いを意識することなく負担が少ないことが大事/いろんなルールが絡み合ってときにどっちを守ればいいかわからなくなるようなことがないことが大事/信頼のおけるデータの具体的な方策を考えてもらいたい
それぞれに対し：非常にそう思う（知っている）/ややそう思う（知っている）/どちらともいえない/あまりそう思わない（知らない）/全くそう思わない（知らない）/わからない・その言葉を理解していない
DQ18-1. 時事問題についての意見をお尋ねします。（それぞれ１つずつ選択）
対象：（消費者の視点でも）民間企業へのサイバー攻撃を脅威と感じる/偏った情報流通により世論が左右されることを脅威と感じる/ネット上でも言論の自由を妨げるべきではない/身代金詐欺、ランサムウェアは社会全体の課題として対応すべきである/企業がビジネスを継続するためにサイバーセキュリティの確保が重要である/民間企業は各国制度の違いを乗り越えて事業拡大の努力をしている/移住したり事業進出する国の法制度が大多数の他国のものと異なっていても黙って従うべきである/多様性を認めつつ法制度を共通化することは世界経済の発展のために必要である/政府が民間企業のサービスに介入・干渉・アクセスする範囲は最小限でなければならない/インターネット上のデータの流れは自由であるべきだ/インターネット上のデータの流れを制御したり止めることはできない/安全を確保するためにある程度データの流通を制限することは必要である
それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない
DQ18-2. 信頼の内容についての意見を聞きます。あなたが最も信頼できると考える人あるいは組織をいくつか思い浮かべてください。その人あるいは組織はどういう理由で信頼できると感じましたか？（それぞれ１つずつ選択）
対象：長い期間安定して歴史があり継続している（実績）/事件があったときにすぐに対応でき回復が速やかである（レジリアンス）/説明が丁寧でわかりやすい（理解）/お金持ち、あるいは財務状況がしっかりしている（財務状況）/マスコミやテレビでよく取り上げられ有名（有名）/ネットで評判が良い（「いいね」）/自分の知っている人がその人・組織と関わっている（関係性）/法律やルールをきちんと守っている（法令順守）/行動に正当な理由がある（比例性）/やりたいことがよくわかり見通せる（透明性）/一方的でなく自分の承認や理解を得ようとしてくれている（承認）/明快な節度と制限を持ち無制限に要求してこない（制限）/公的な機関や第三者が監督監視してくれている（監督）/その人・組織とは何かあったときの保険・救済措置がある（救済）/分け隔てなく差別をせず、公平である（公平）/時と場合によって変わらず一律に一貫性があり対応してくれる（一貫性）/グローバルな基準において差別がなくフェアである（公正）/その人・組織は自分に思いもよらない責任を転嫁しない（責任制限）/その人・組織は他の人・組織と相反せず整合していて敵を作らない（整合）
それぞれに対し：そう思う/ややそう思う/どちらでもない/あまりそう思わない/全くそう思わない/わからない
DQ19. 信頼性のある自由なデータ流通を実現するための要素として、あなたはそれぞれどの程度同意できますか。（それぞれ１つずつ選択）
対象：関連する規制に関する透明性の確保/プライバシー・セキュリティ確保技術の標準化/各国相互の運用性確保/関連する制度との補完性検討/信頼性のある自由なデータ流通枠組みの実装
それぞれに対し：大変同意できる/やや同意できる/どちらともいえない/あまり同意できない/全く同意できない/わからない・その言葉を理解していない

3.調査結果（単純分析）

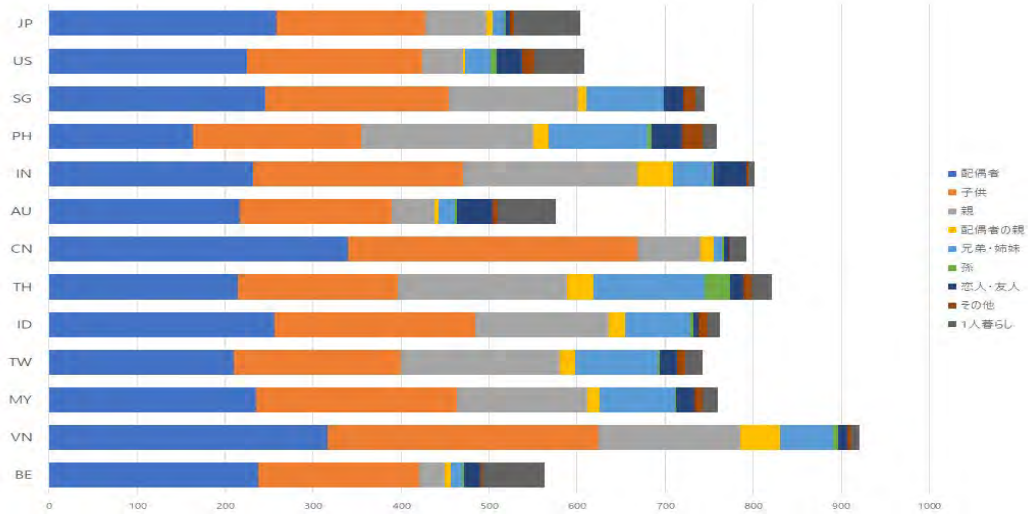
（1）共通設問



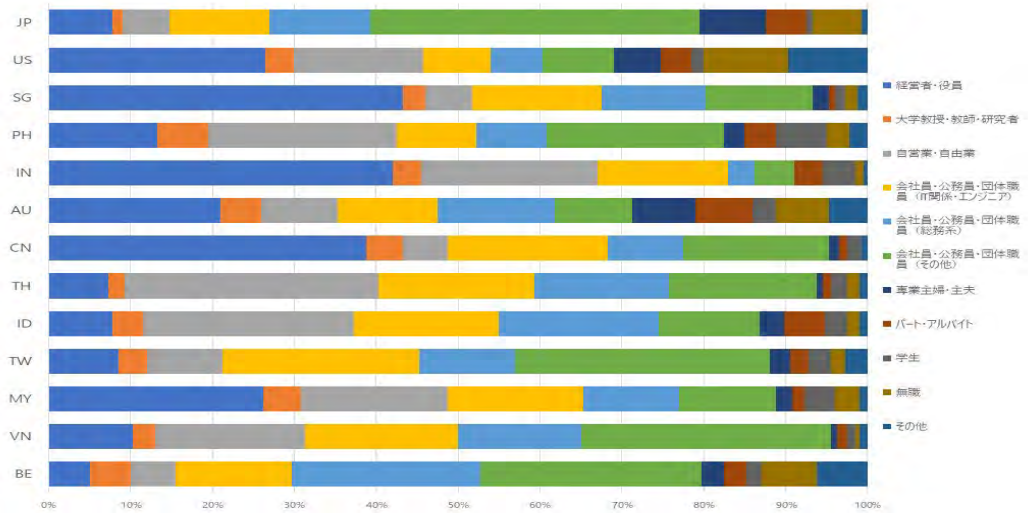
図表 2-3-1 回答者性別



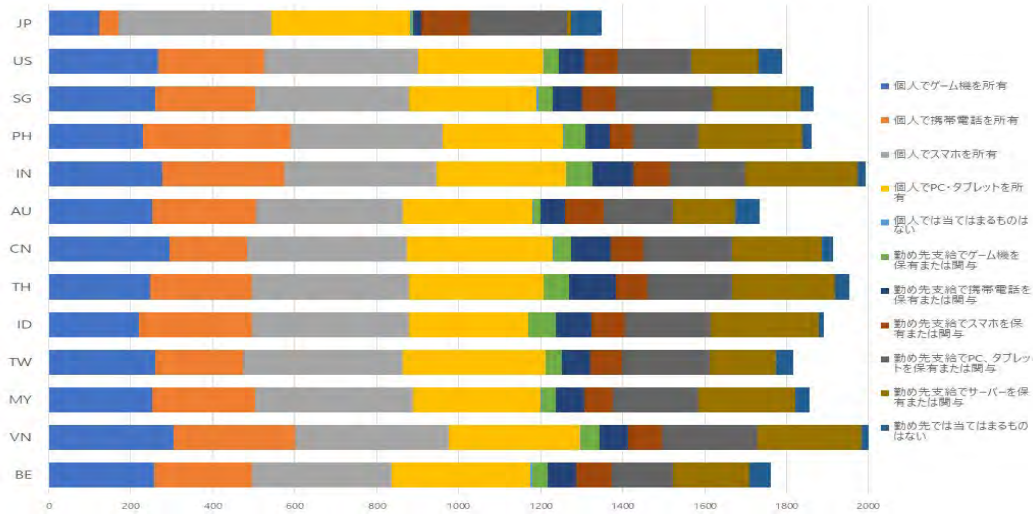
図表 2-3-2 回答者年代



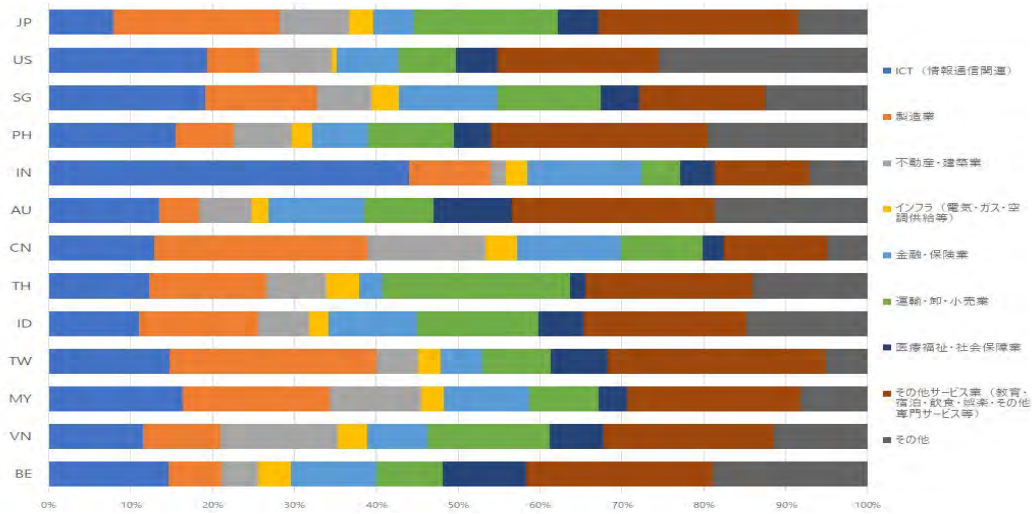
図表 2-3-3 回答者同居家族



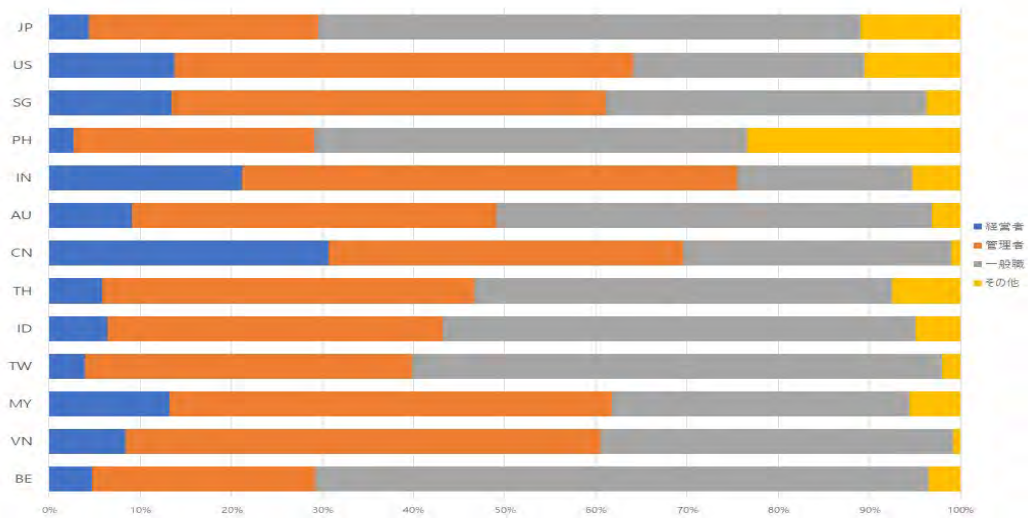
図表 2-3-4 回答者職業



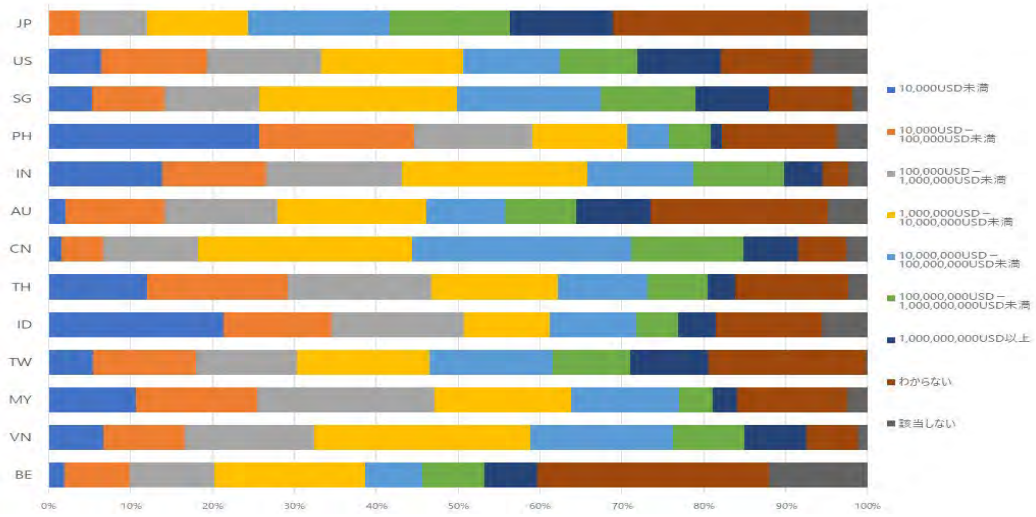
図表 2-3-5 回答者所有機器



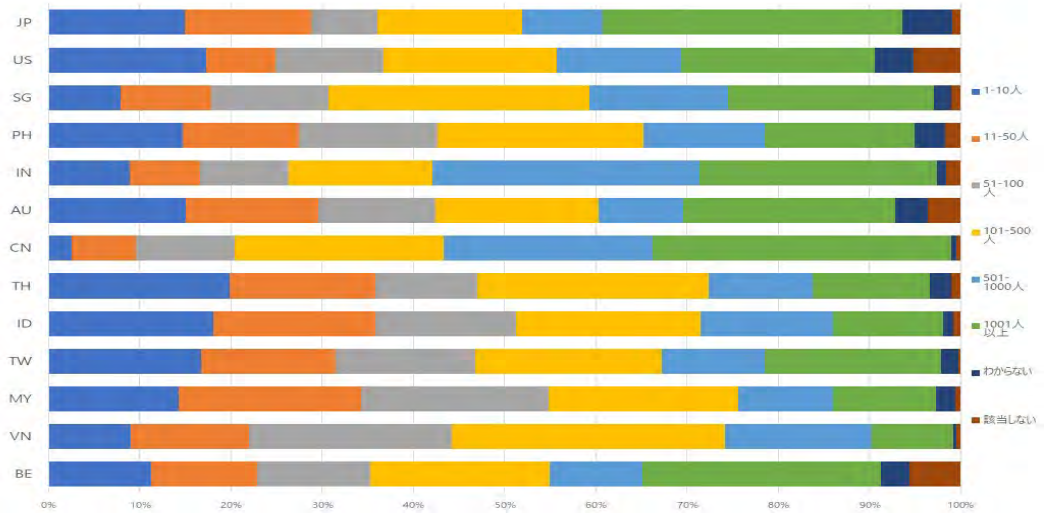
図表 2-3-6 回答者勤務先業種（有職者のみ）



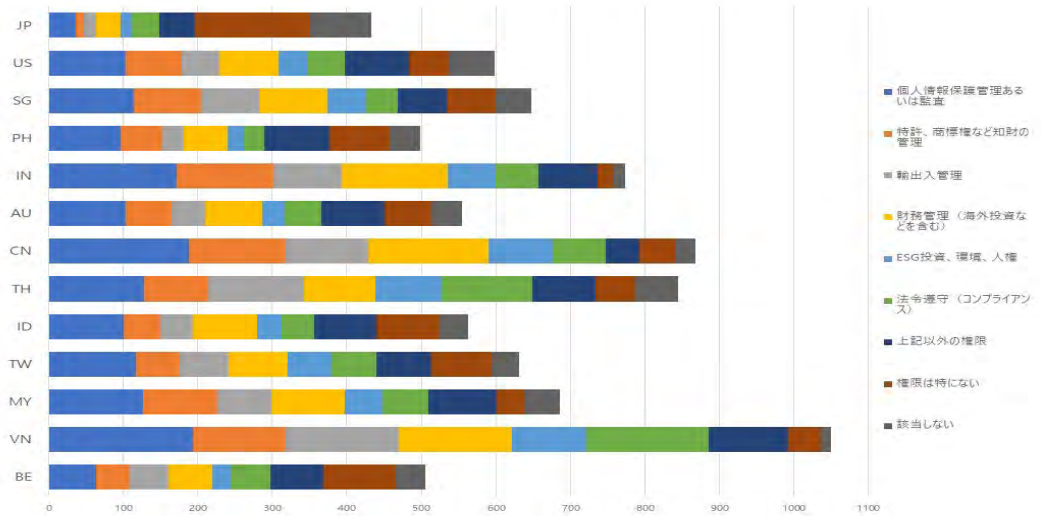
図表 2-3-7 回答者勤務先立場



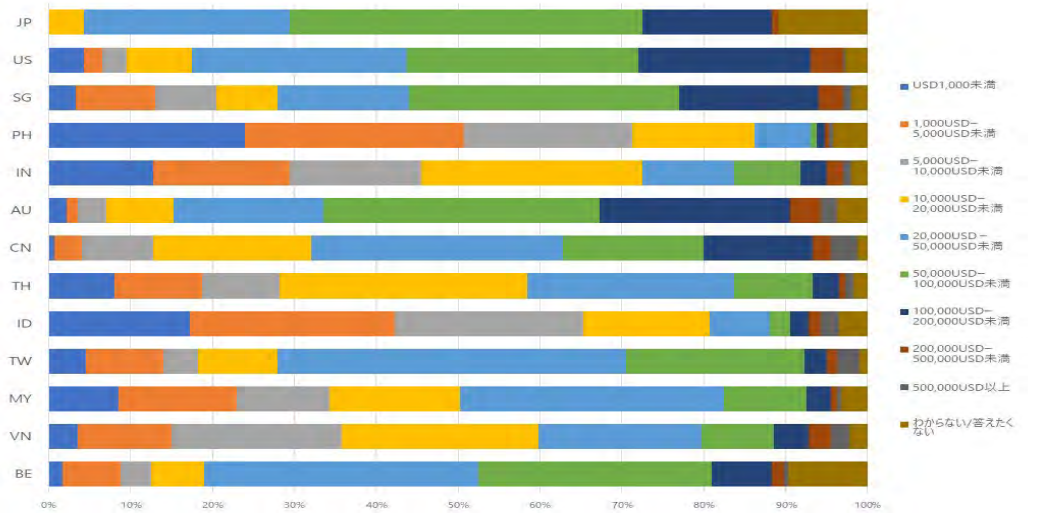
図表 2-3-8 回答者勤務先売上高



図表 2-3-9 回答者勤務先総従業員数

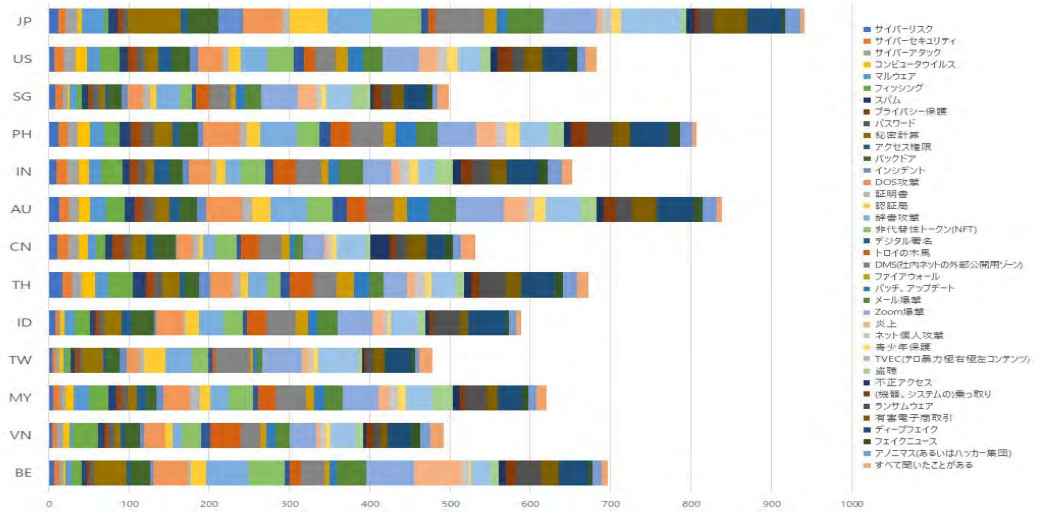


図表 2-3-10 回答者勤務先職務権限

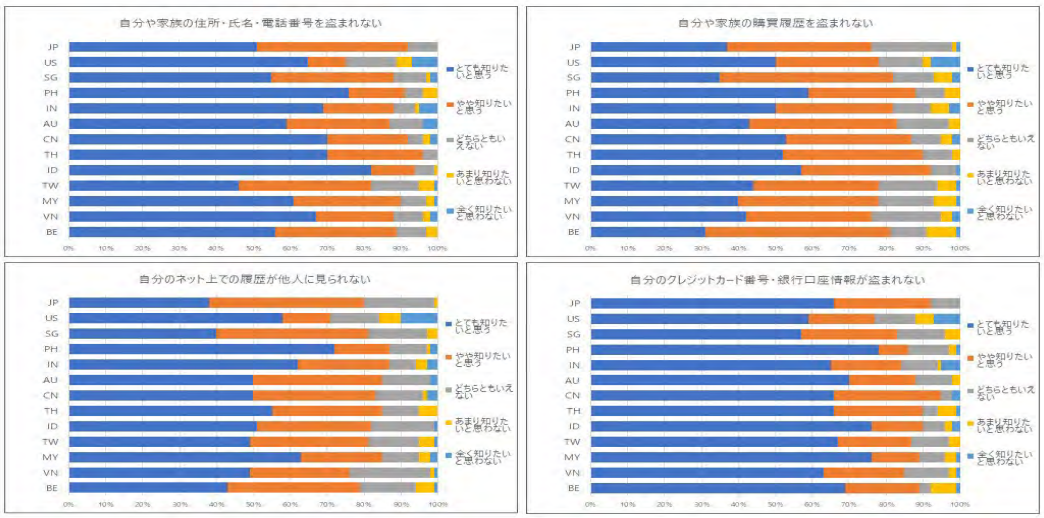


図表 2-3-11 回答者世帯年収

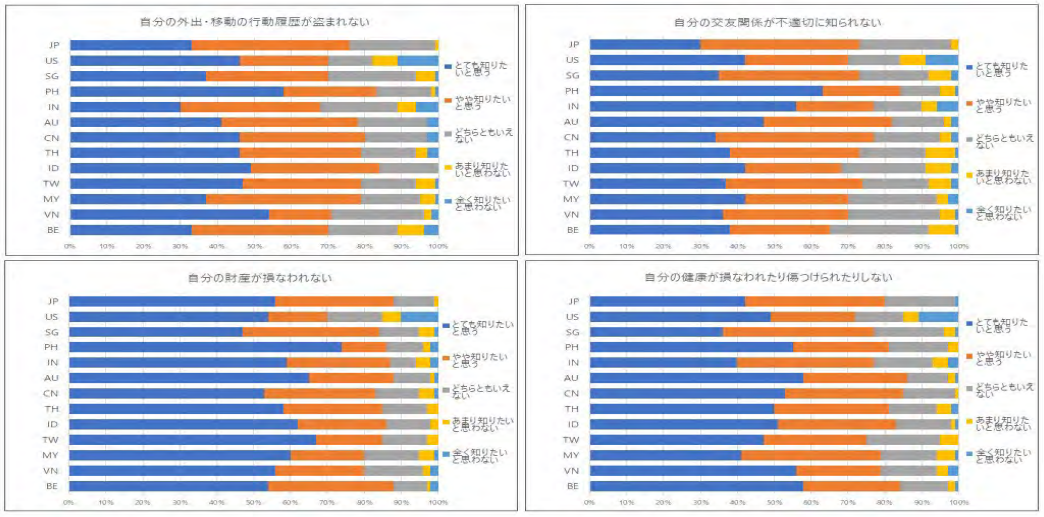
(2) 消費者対象・セキュリティ編



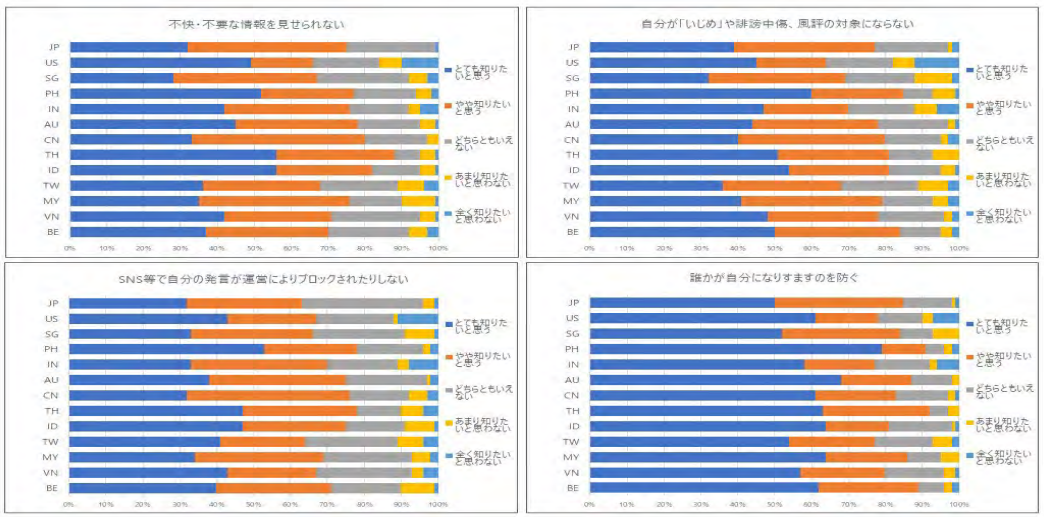
図表 2-3-12 消費者対象・セキュリティ編　聞いたことも気にかけたこともない言葉



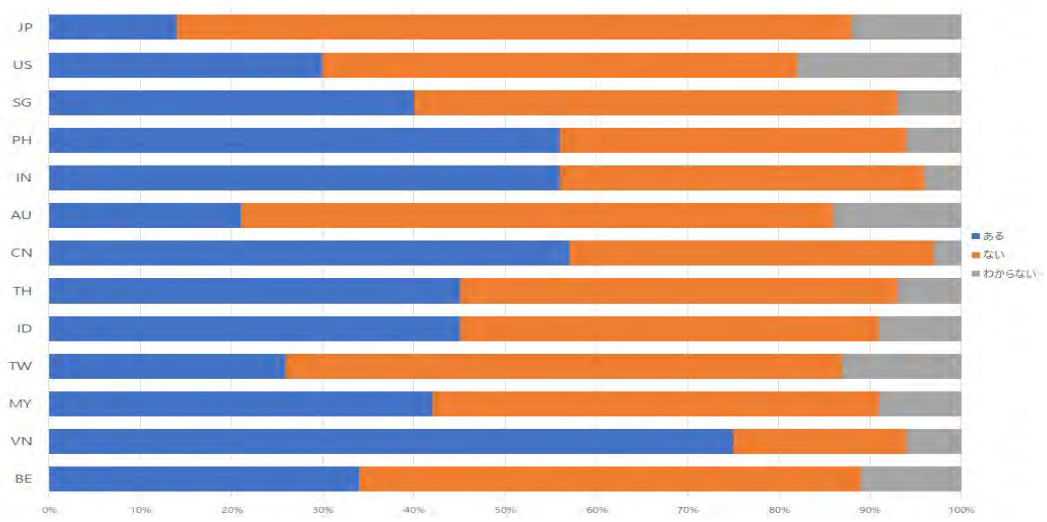
図表 2-3-13 消費者対象・セキュリティ編　セキュリティに対する興味-1



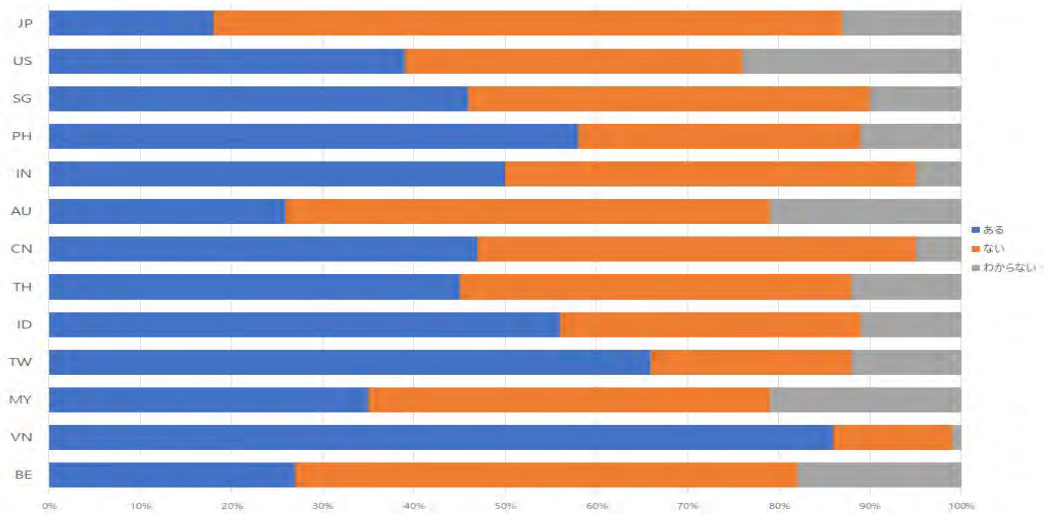
図表 2-3-14 消費者対象・セキュリティ編　セキュリティに対する興味-2



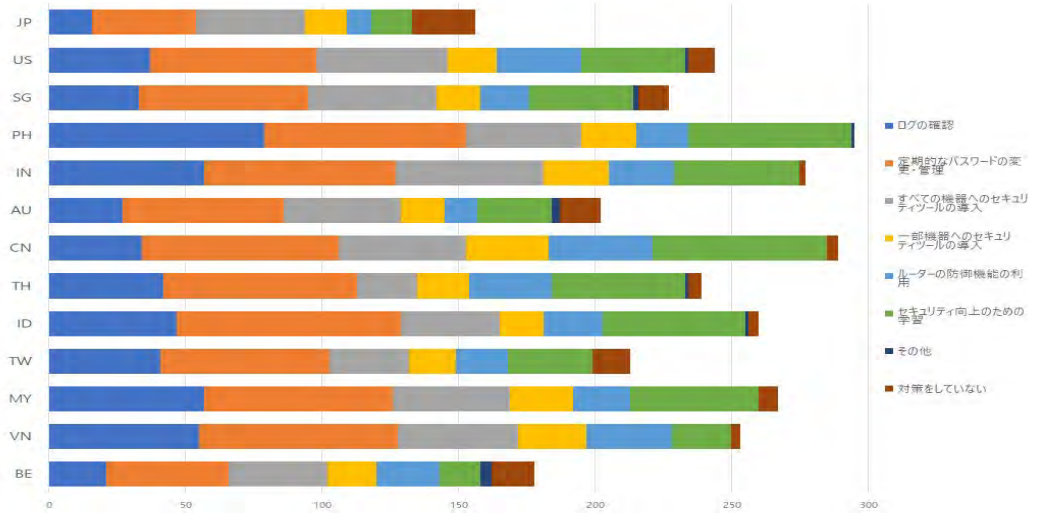
図表 2-3-15 消費者対象・セキュリティ編　セキュリティに対する興味-3



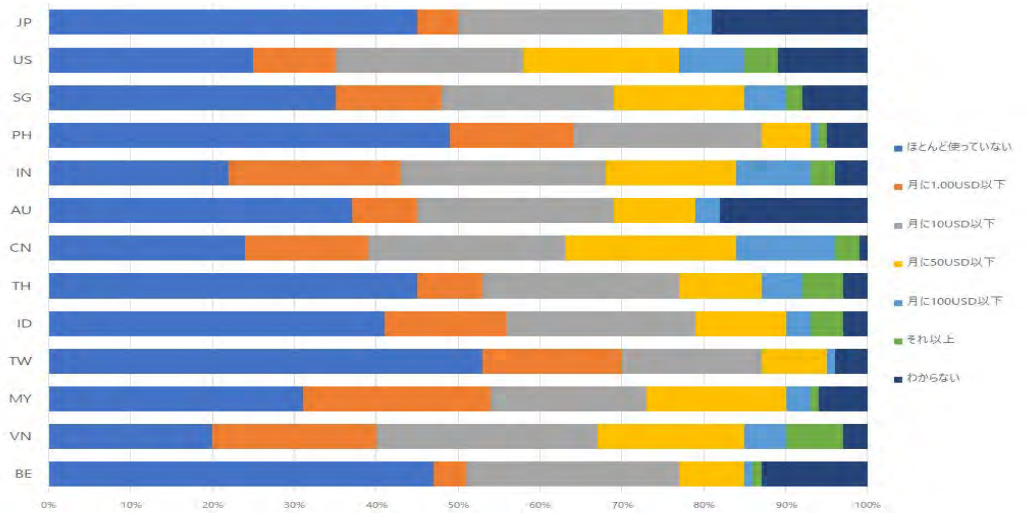
図表 2-3-16 消費者対象・セキュリティ編　スマホ・PC 利用時のデータ被害経験



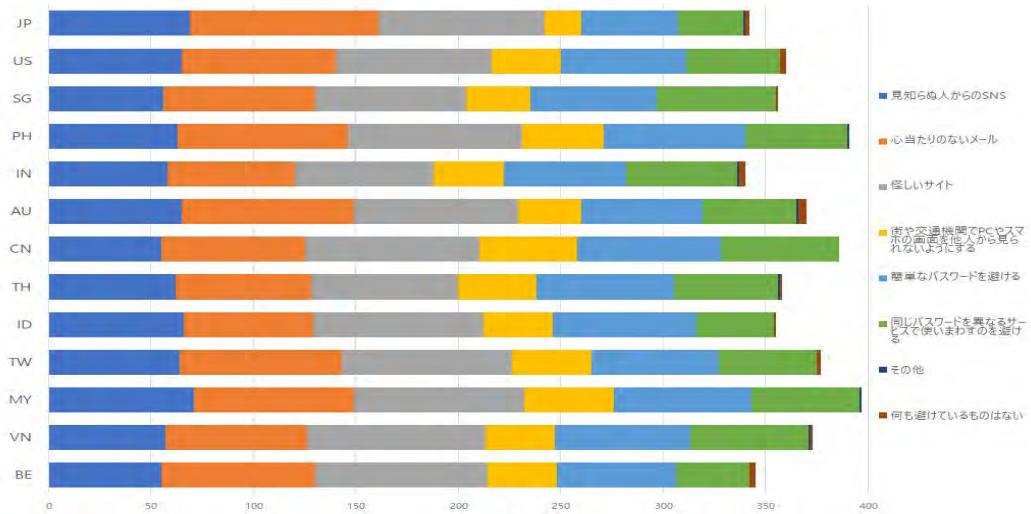
図表 2-3-17 消費者対象・セキュリティ編　自分や身近な人の個人情報漏洩経験



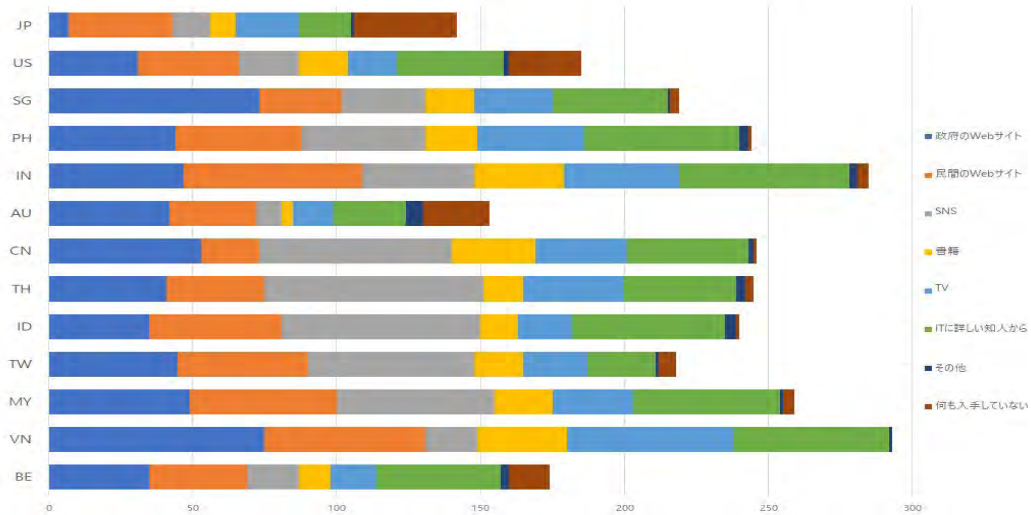
図表 2-3-18 消費者対象・セキュリティ編　実施しているセキュリティ対策



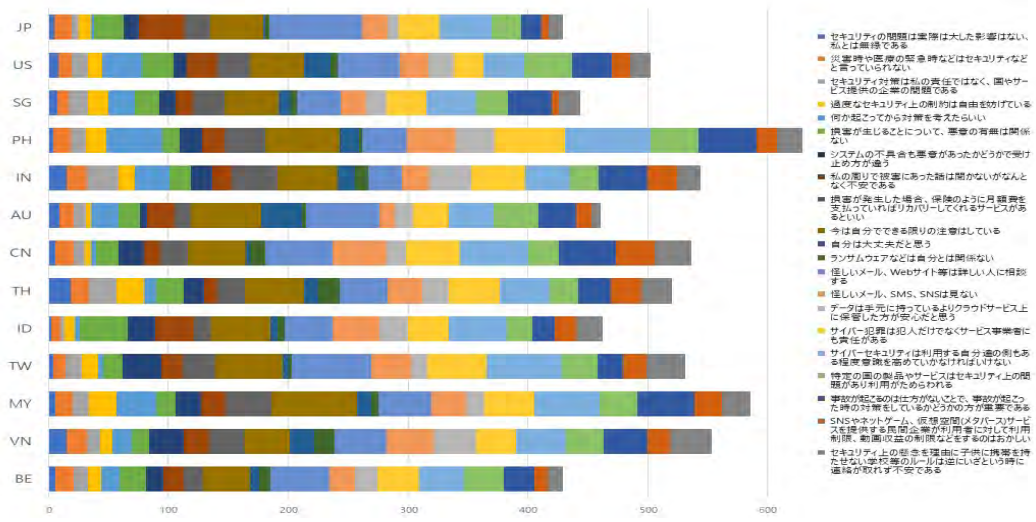
図表 2-3-19 消費者対象・セキュリティ編　セキュリティ対策にかける費用



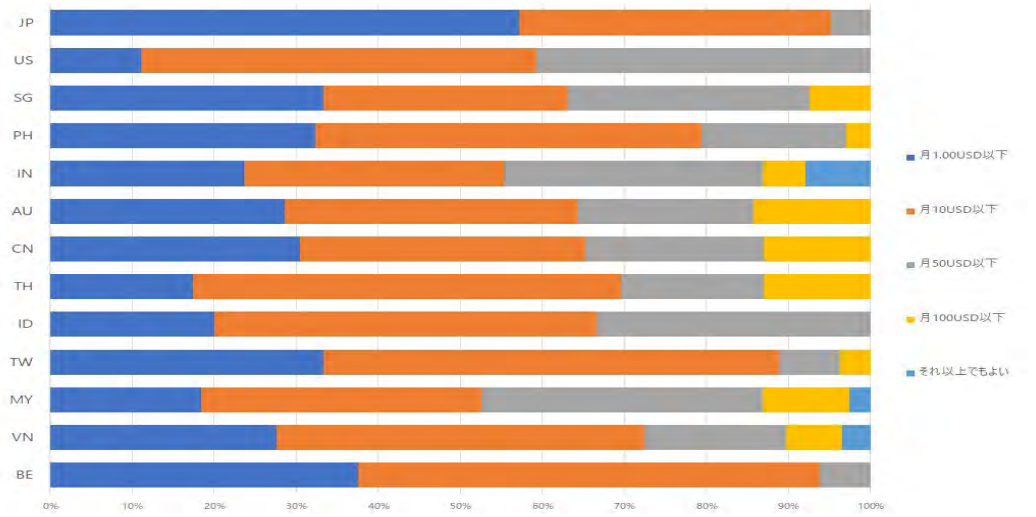
図表 2-3-20 消費者対象・セキュリティ編　危険だと思って避けていること



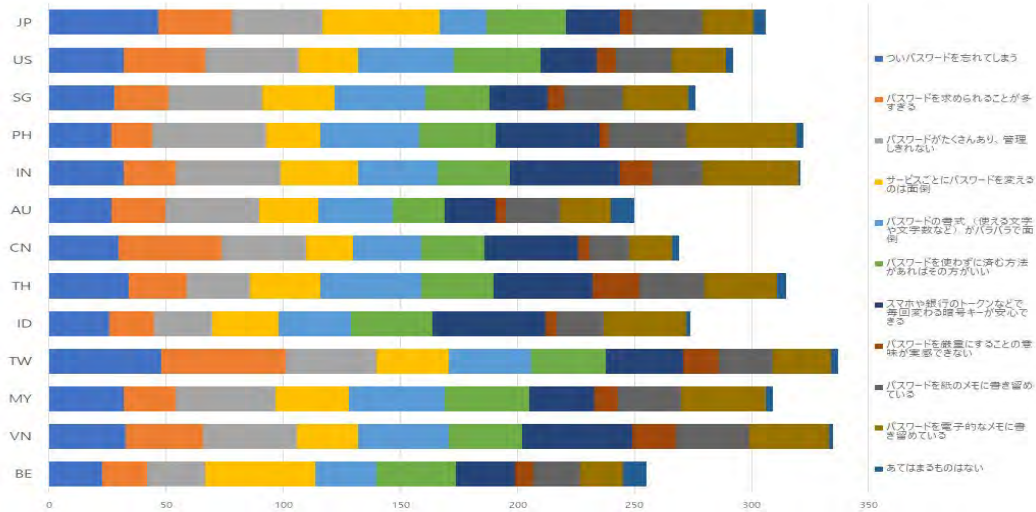
図表 2-3-21 消費者対象・セキュリティ編　情報セキュリティに関する情報入手先



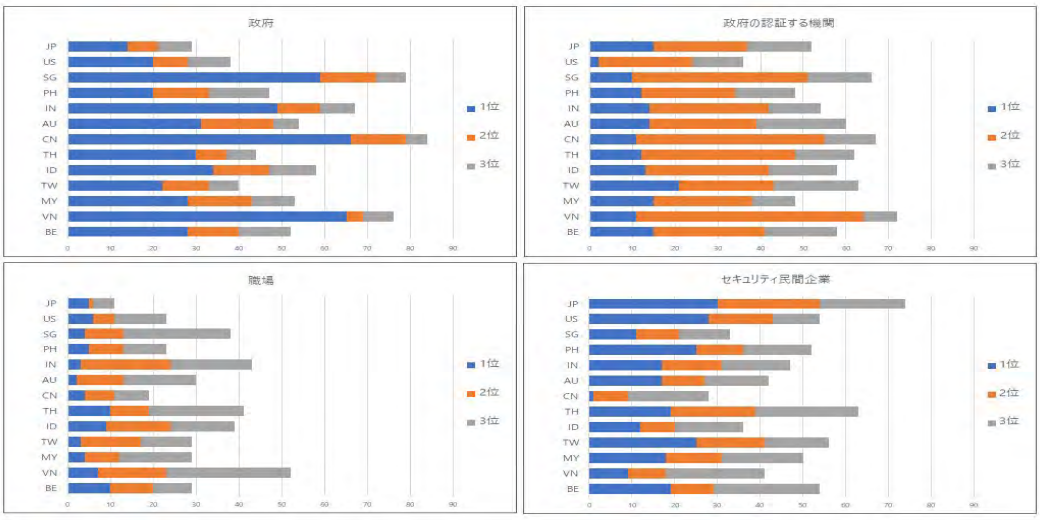
図表 2-3-22 消費者対象・セキュリティ編　サイバーセキュリティに関する考え方



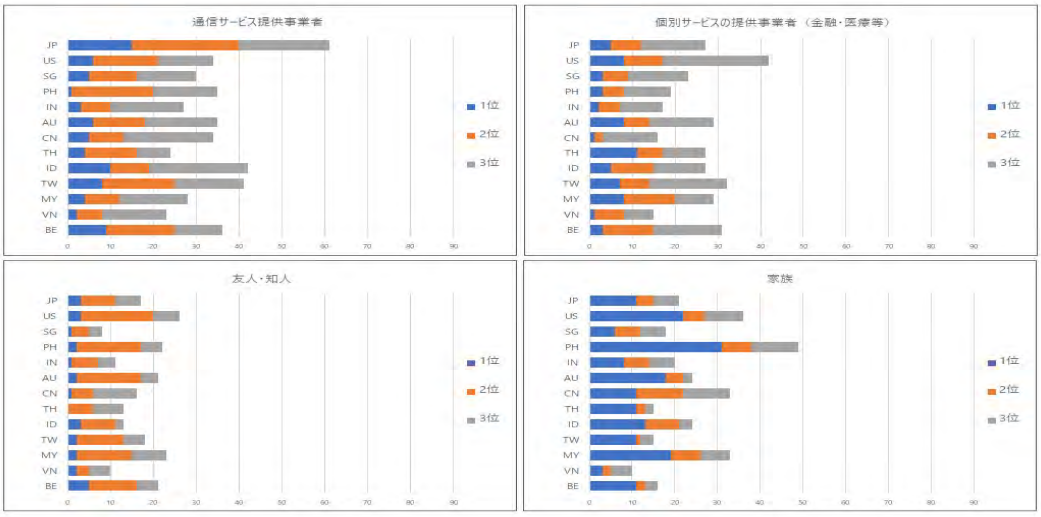
図表 2-3-23 消費者対象・セキュリティ編　データ保険サービスに支払える金額



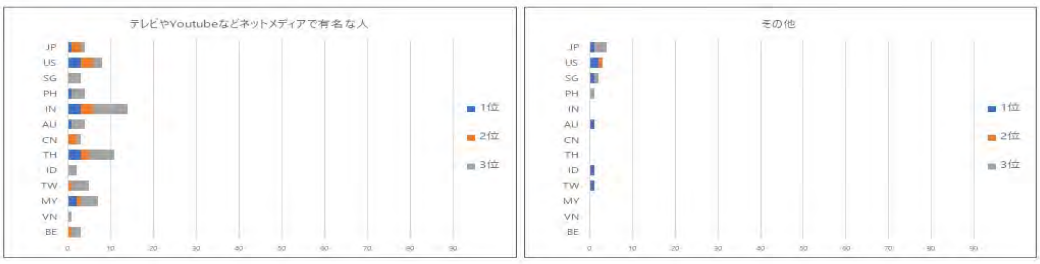
図表 2-3-24 消費者対象・セキュリティ編　パスワード管理に関する考え方



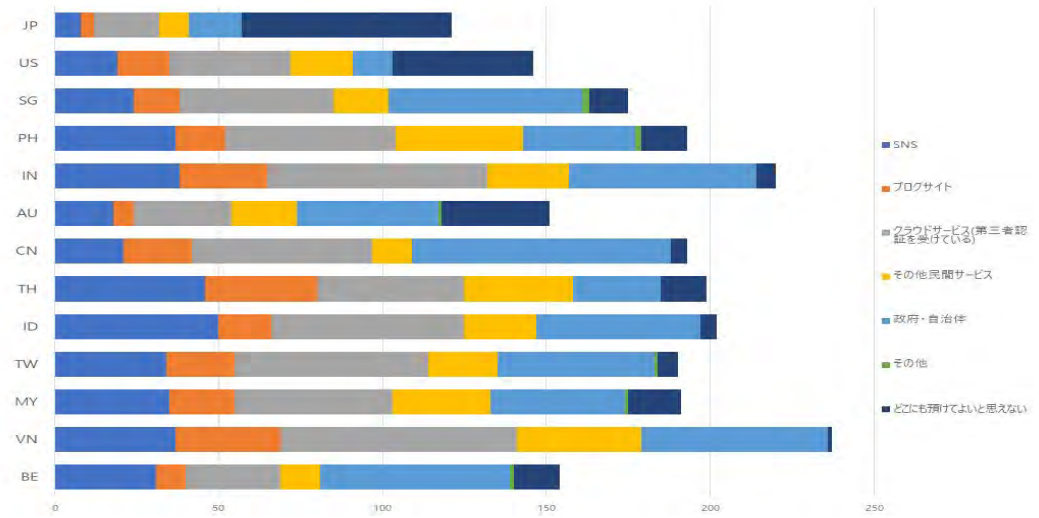
図表 2-3-25 消費者対象・セキュリティ編　サイバーセキュリティについて信頼できる相手-1



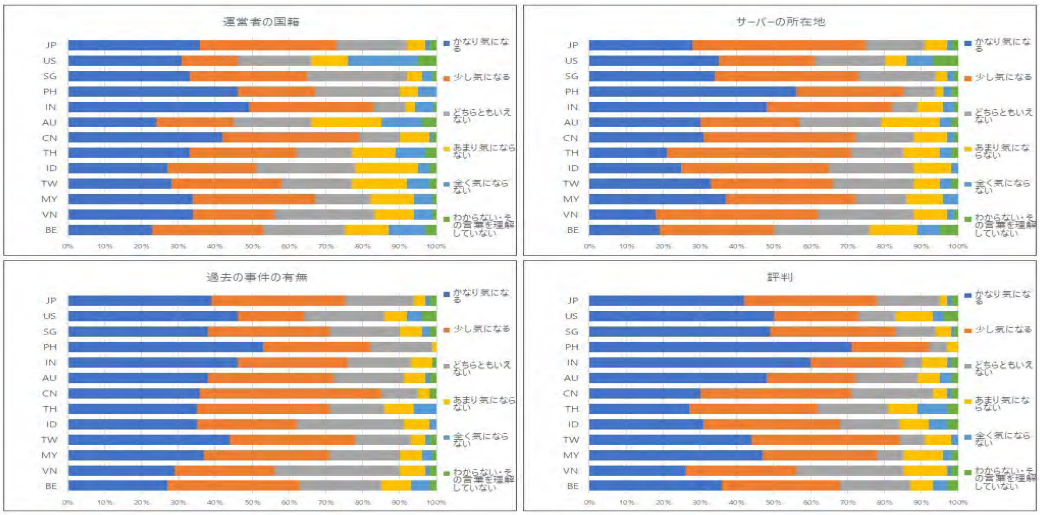
図表 2-3-26 消費者対象・セキュリティ編　サイバーセキュリティについて信頼できる相手-2



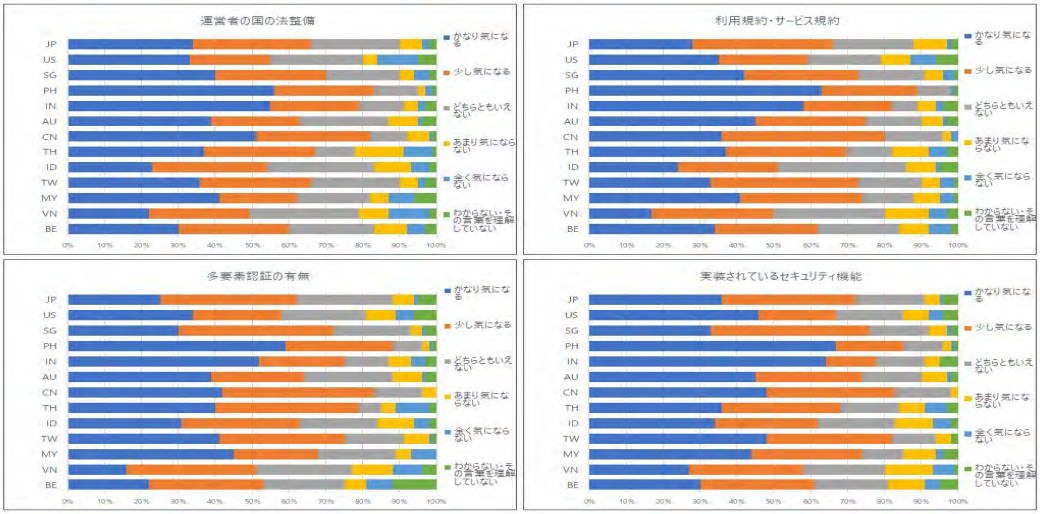
図表 2-3-27 消費者対象・セキュリティ編　サイバーセキュリティについて信頼できる相手-3



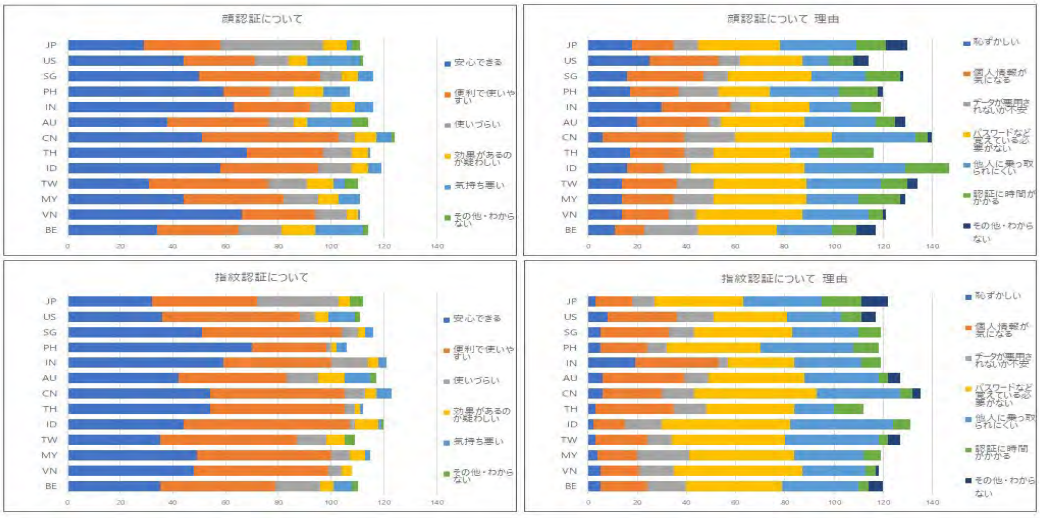
図表 2-3-28 消費者対象・セキュリティ編　個人情報取扱サービス・機関について安心できるもの



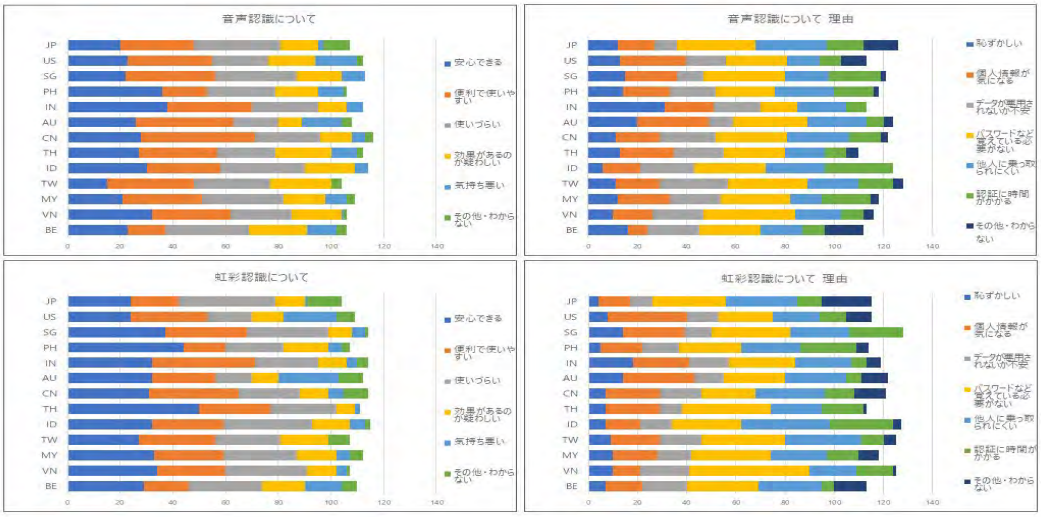
図表 2-3-29 消費者対象・セキュリティ編　サービス利用時に気になること-1



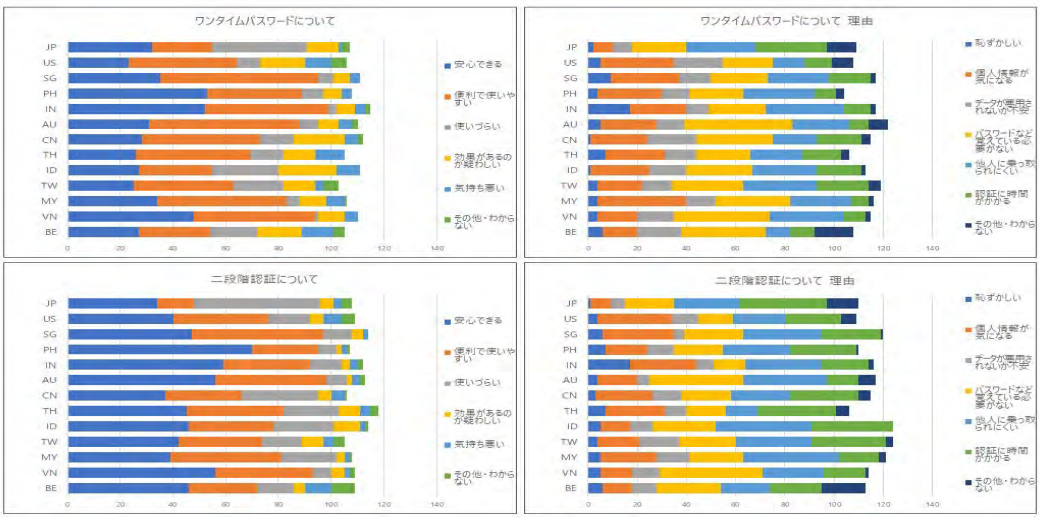
図表 2-3-30 消費者対象・セキュリティ編　サービス利用時に気になること-2



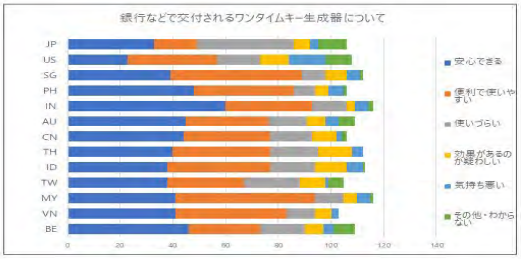
図表 2-3-31 消費者対象・セキュリティ編　セキュリティ確保の仕組みへの印象とその理由-1



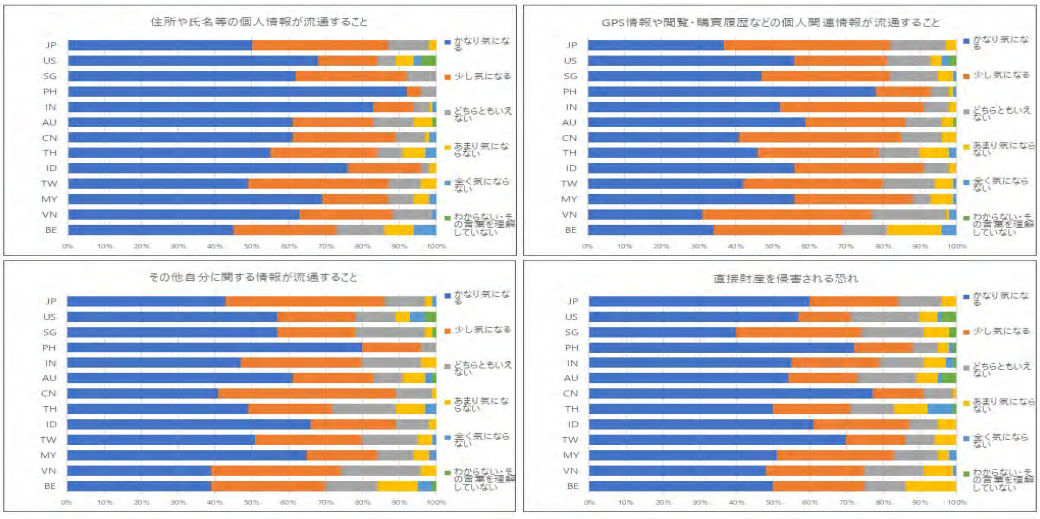
図表 2-3-32 消費者対象・セキュリティ編　セキュリティ確保の仕組みへの印象とその理由-2



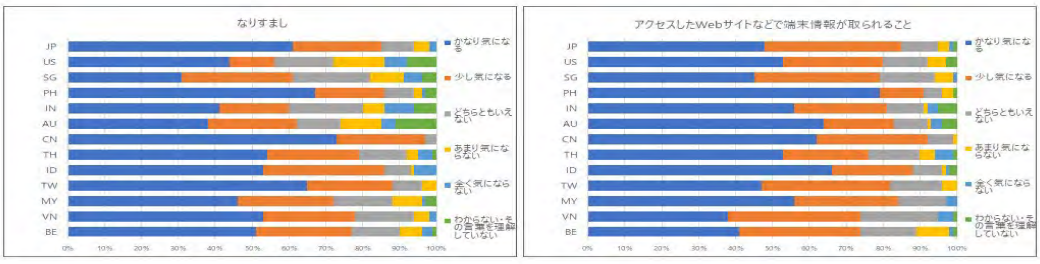
図表 2-3-33 消費者対象・セキュリティ編　セキュリティ確保の仕組みへの印象とその理由-3



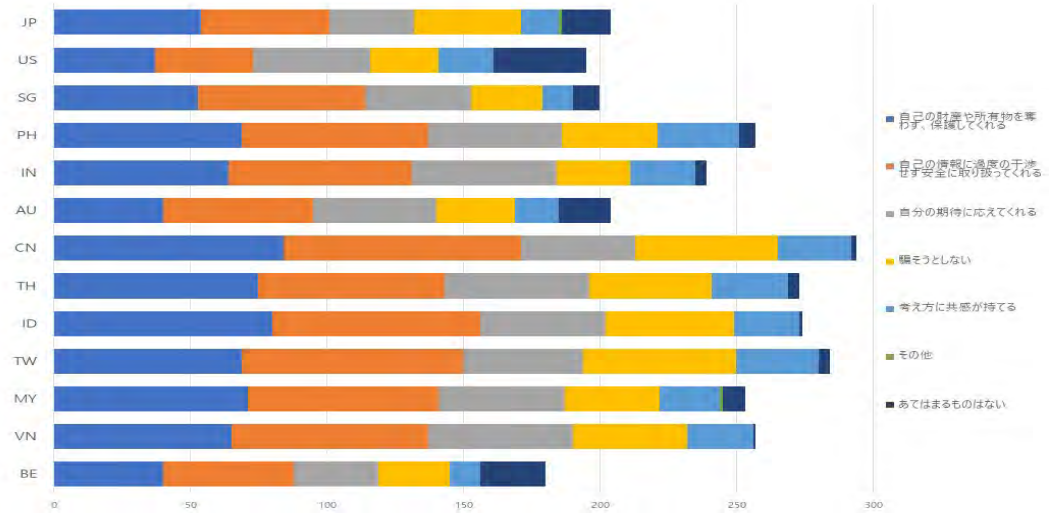
図表 2-3-34 消費者対象・セキュリティ編　セキュリティ確保の仕組みへの印象とその理由-4



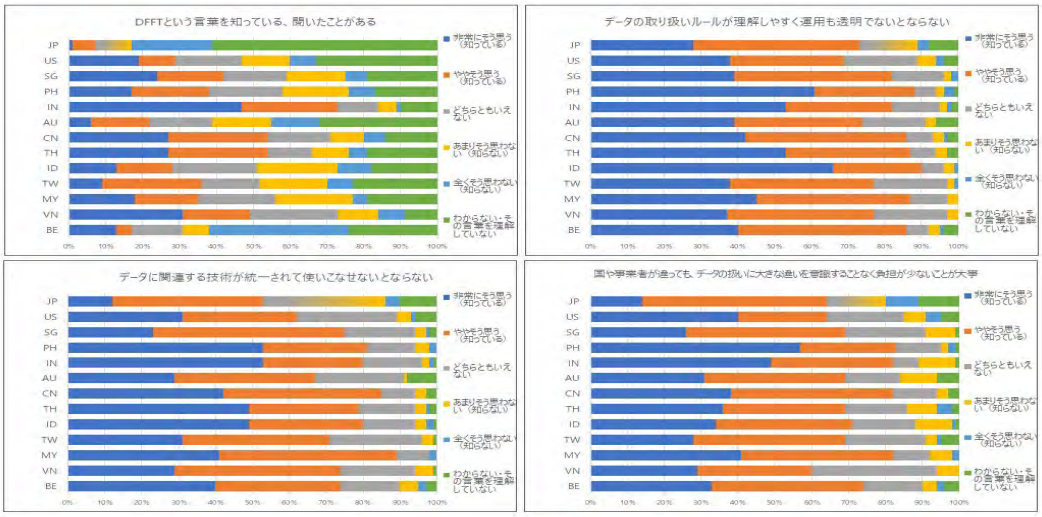
図表 2-3-35 消費者対象・セキュリティ編　個人関連情報の侵害・流通に関する意識-1



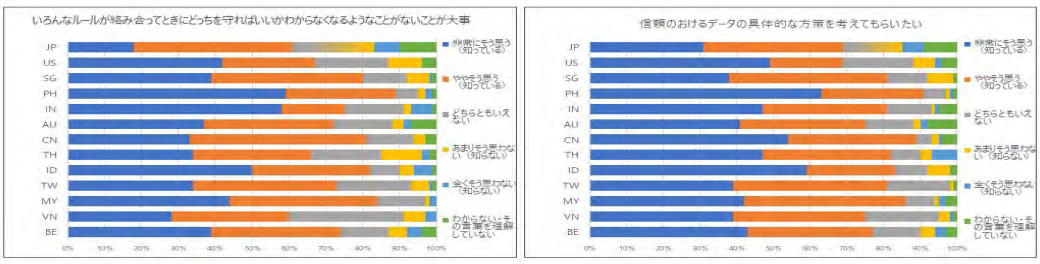
図表 2-3-36 消費者対象・セキュリティ編　個人関連情報の侵害・流通に関する意識-2



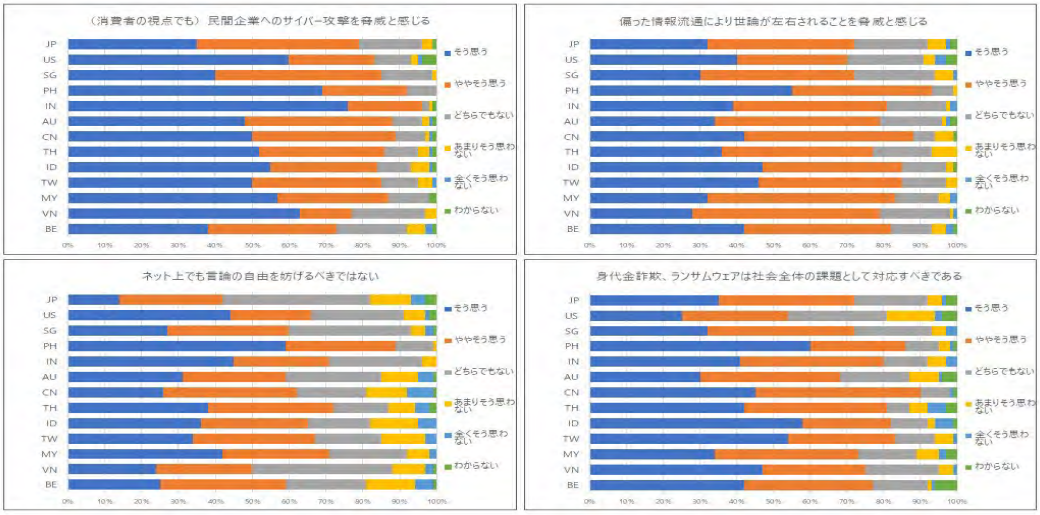
図表 2-3-37 消費者対象・セキュリティ編　政府や企業、組織、個人を信頼するための判断材料



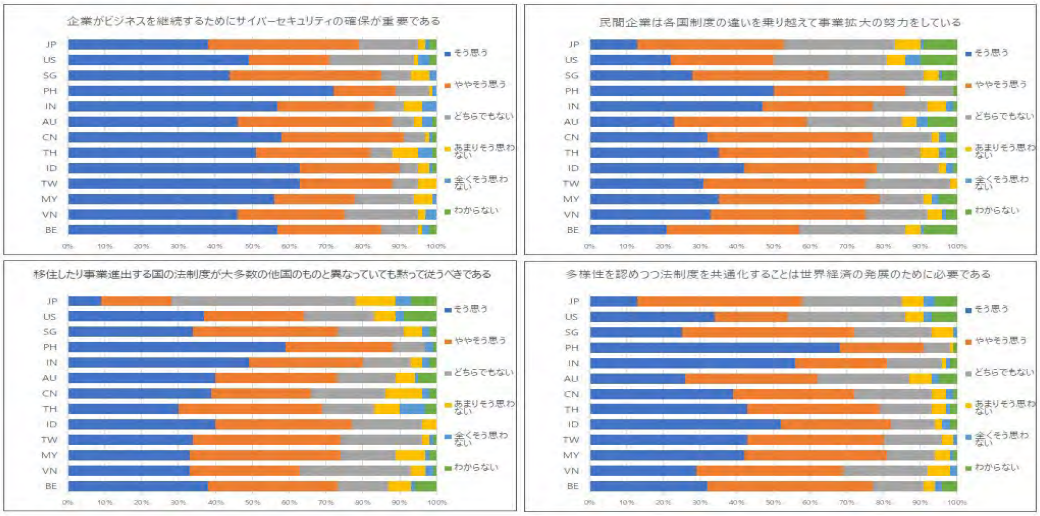
図表 2-3-38 消費者対象・セキュリティ編　データ取扱いに関する考え方-1



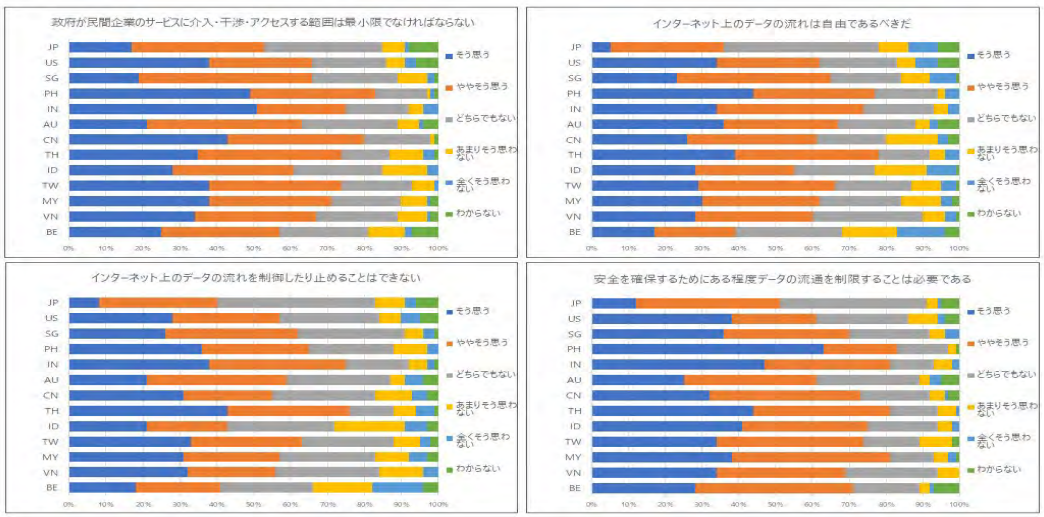
図表 2-3-39 消費者対象・セキュリティ編　データ取扱いに関する考え方-2



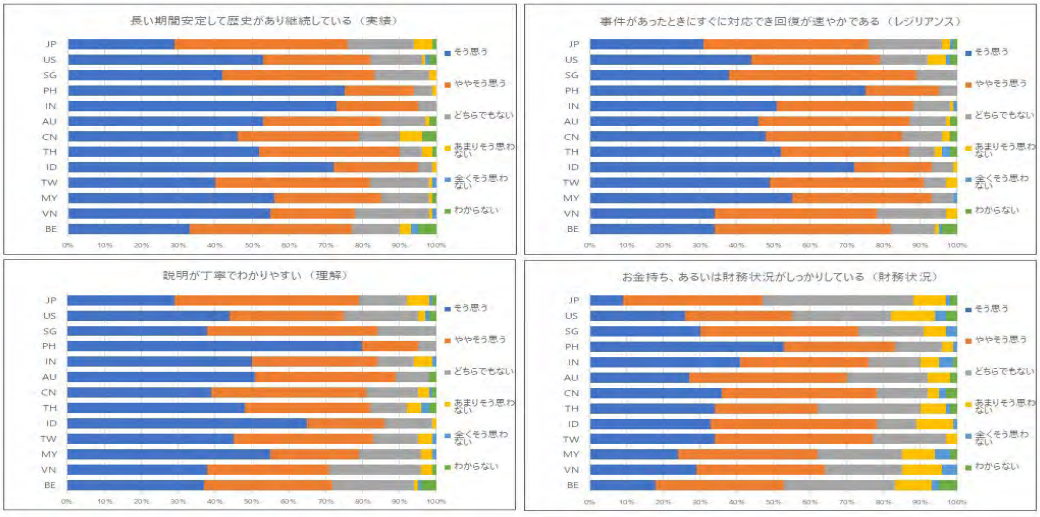
図表 2-3-40 消費者対象・セキュリティ編　時事問題についての意見-1



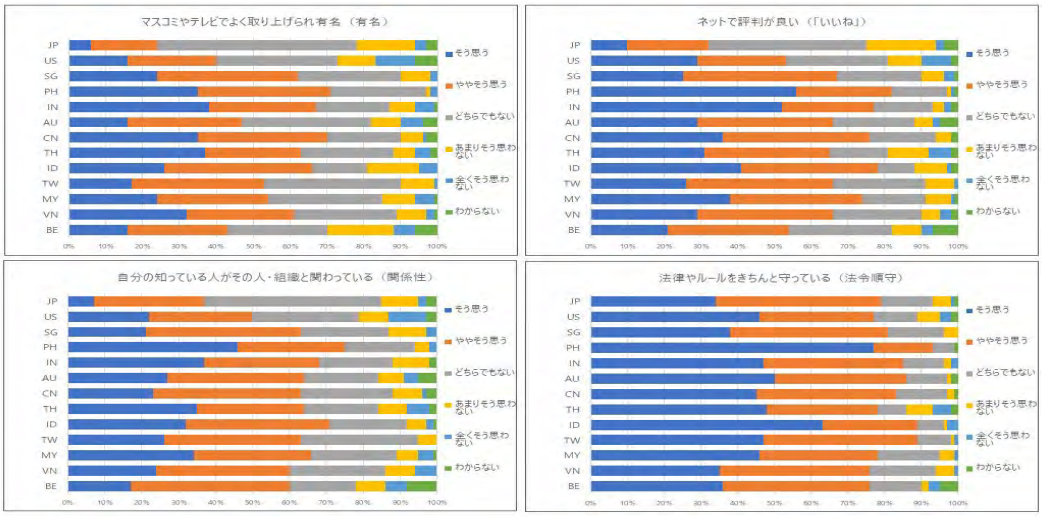
図表 2-3-41 消費者対象・セキュリティ編　時事問題についての意見-2



図表 2-3-42 消費者対象・セキュリティ編　時事問題についての意見-3

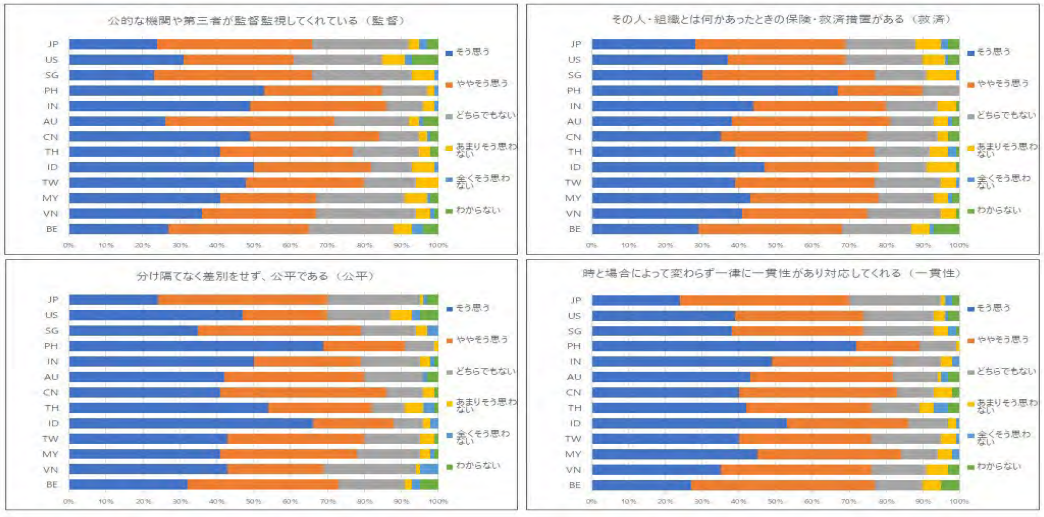


図表 2-3-43 消費者対象・セキュリティ編　相手を信頼できる理由-1



図表 2-3-44 消費者対象・セキュリティ編　相手を信頼できる理由-2

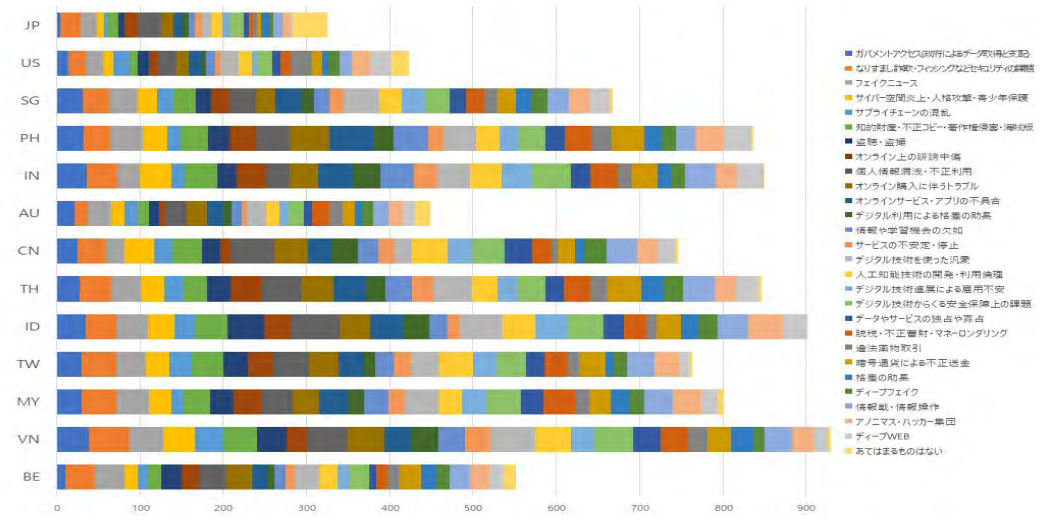
図表 2-3-45 消費者対象・セキュリティ編　相手を信頼できる理由-3



図表 2-3-46 消費者対象・セキュリティ編　相手を信頼できる理由-4

図表 2-3-47 消費者対象・セキュリティ編　相手を信頼できる理由-5

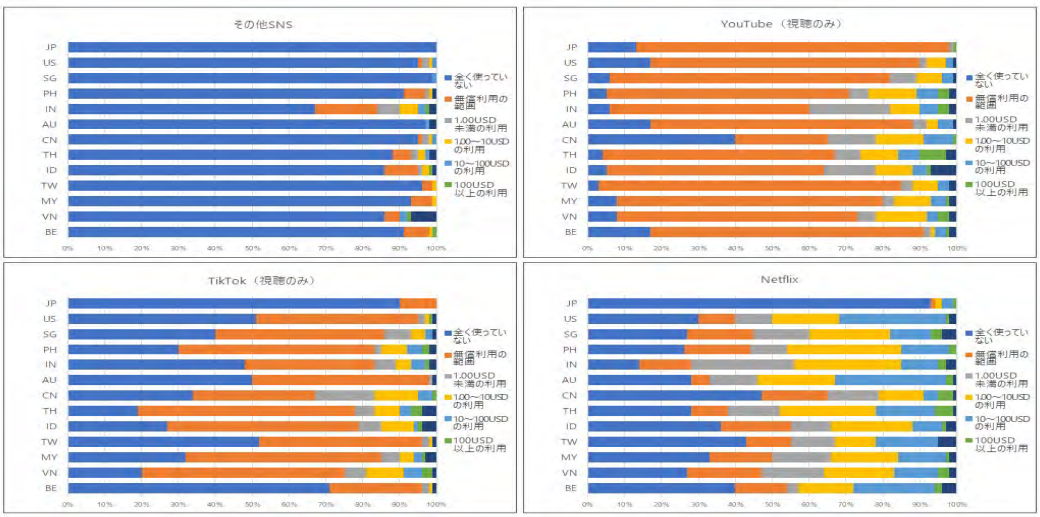
(3) 消費者対象・DFFT 編



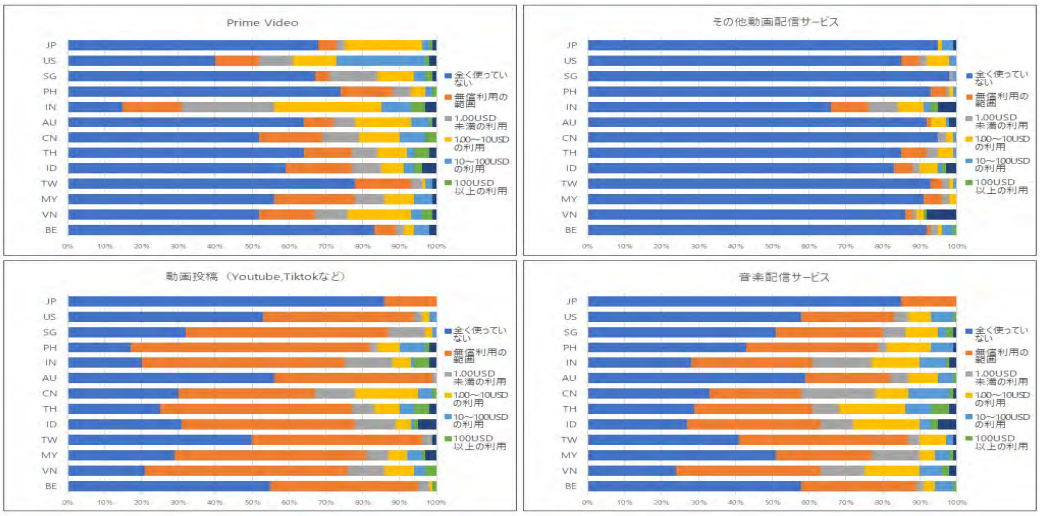
図表 2-3-48 消費者対象・DFFT 編　関心があり、より知りたいと思う言葉

図表 2-3-49 消費者対象・DFFT 編　デジタルサービスの活用状況-1

図表 2-3-50 消費者対象・DFFT 編　デジタルサービスの活用状況-2

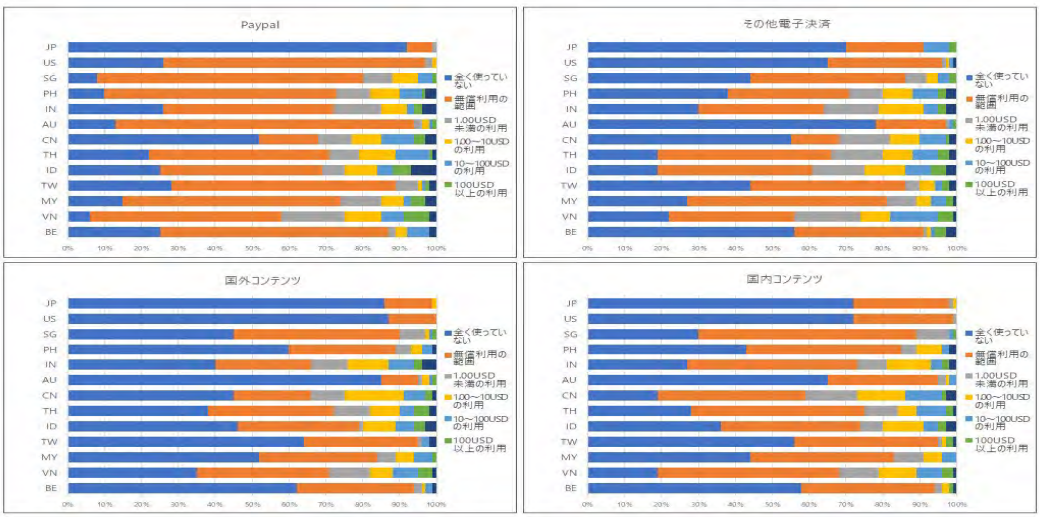


図表 2-3-51 消費者対象・DFFT 編　デジタルサービスの活用状況-3

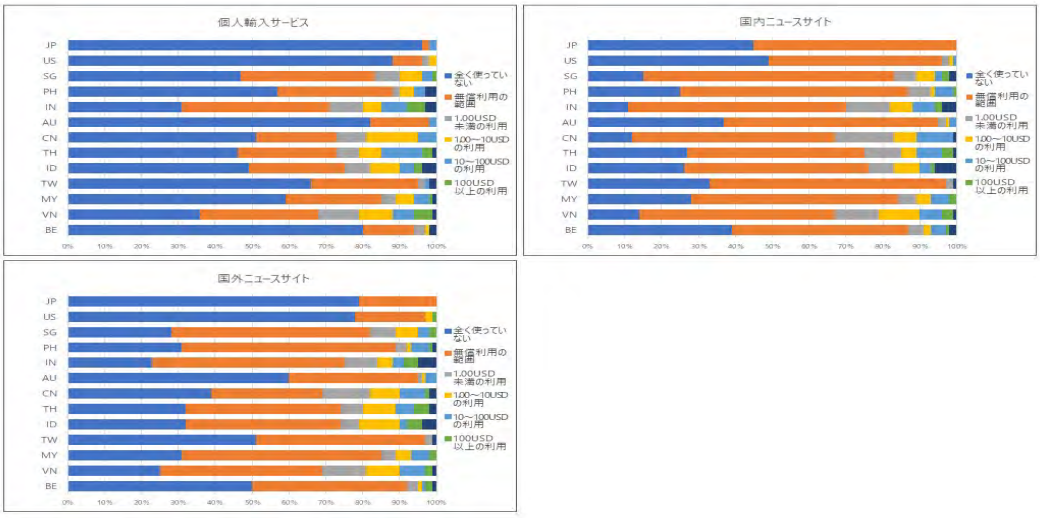


図表 2-3-52 消費者対象・DFFT 編　デジタルサービスの活用状況-4

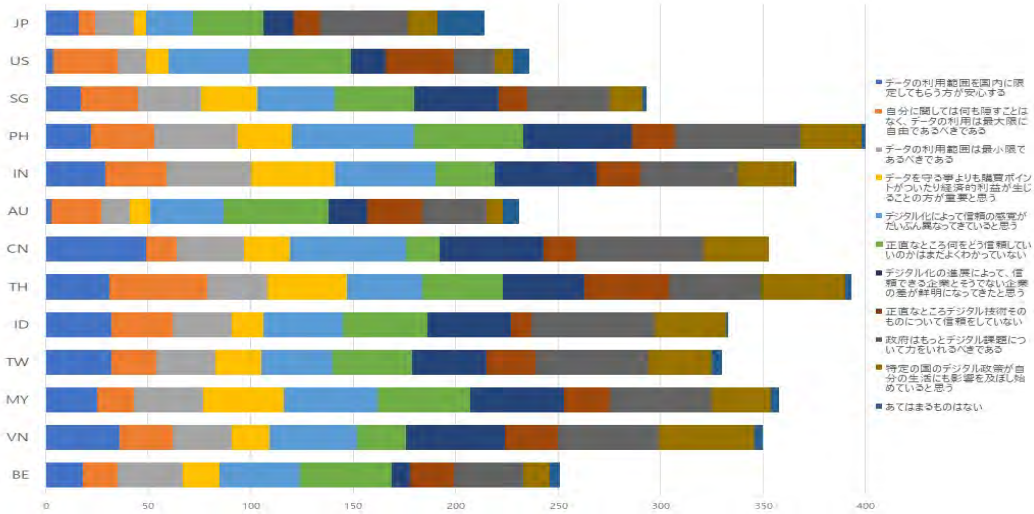
図表 2-3-53 消費者対象・DFFT 編　デジタルサービスの活用状況-5



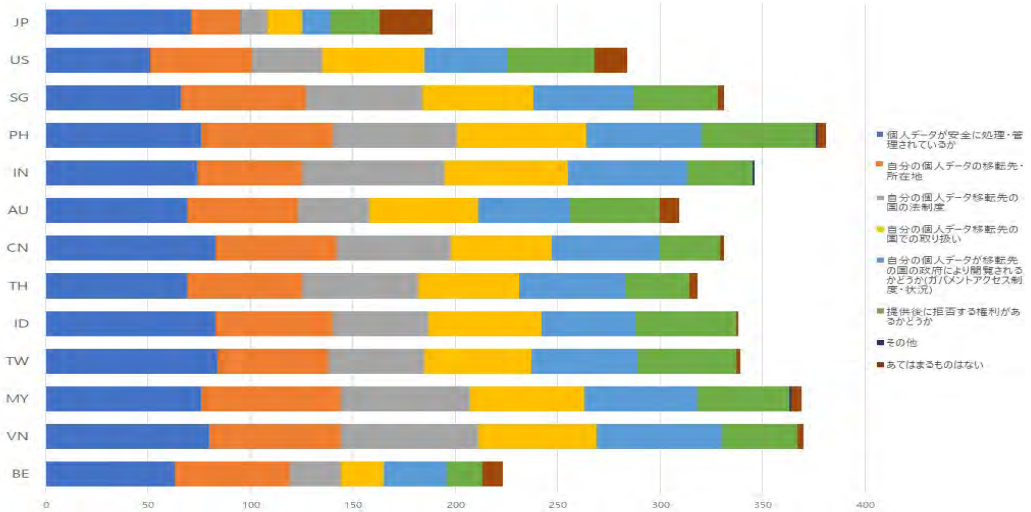
図表 2-3-54 消費者対象・DFFT 編　デジタルサービスの活用状況-6



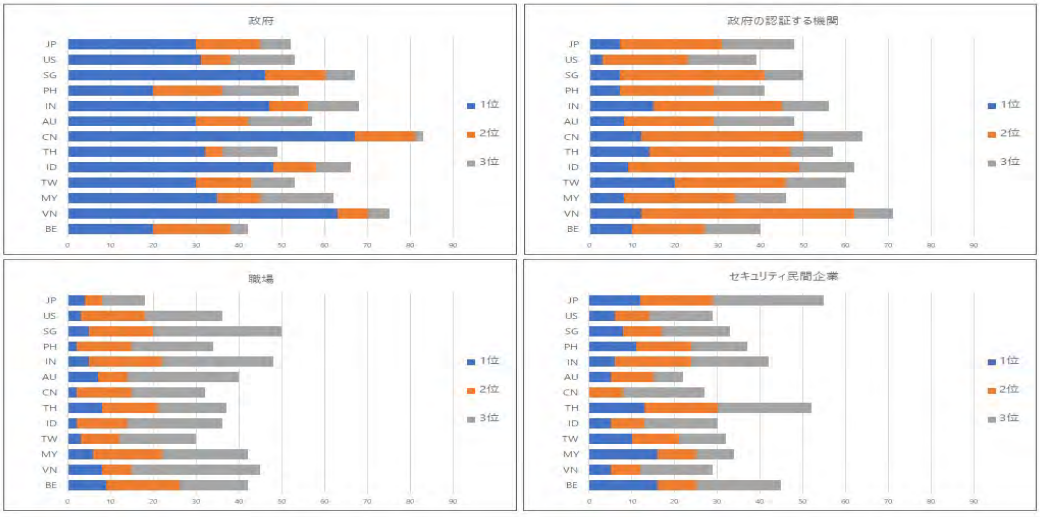
図表 2-3-55 消費者対象・DFFT 編　デジタルサービスの活用状況-7



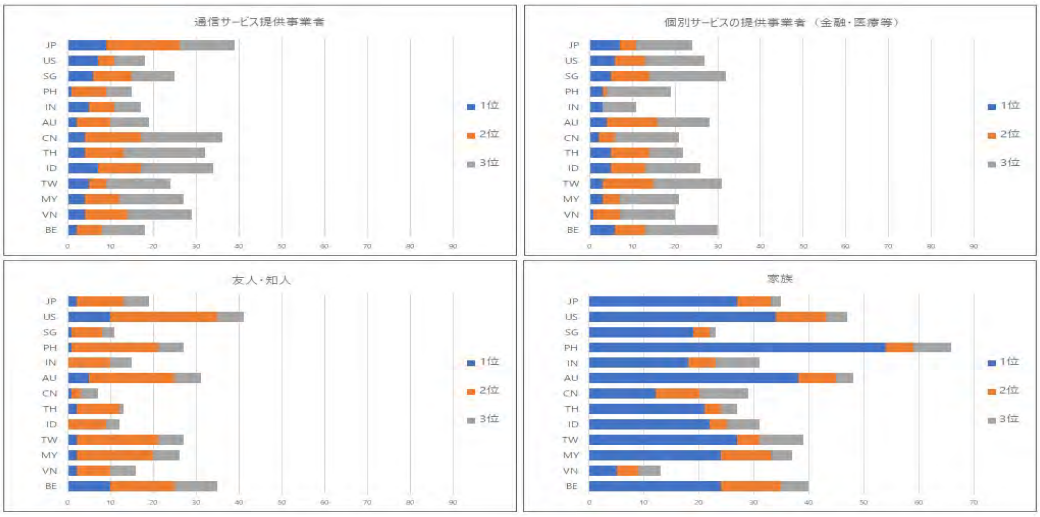
図表 2-3-56 消費者対象・DFFT 編　データ利用に関する考え方



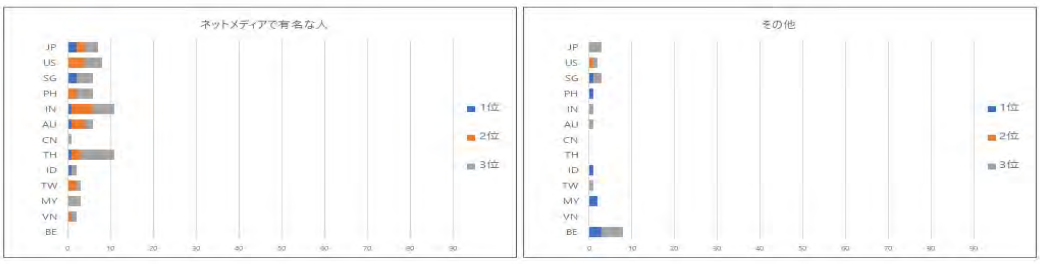
図表 2-3-57 消費者対象・DFFT 編　データ提供先について関心のあること



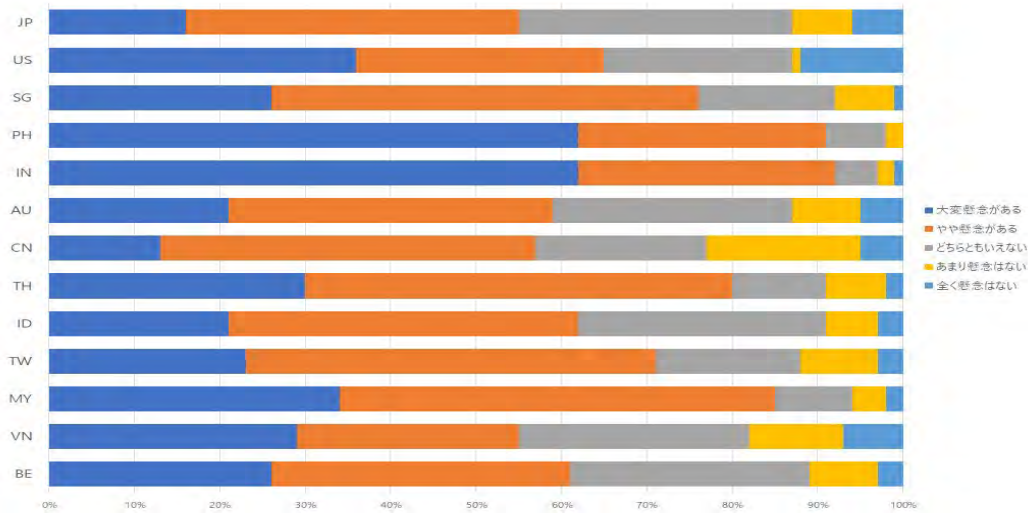
図表 2-3-58 消費者対象・DFFT 編　デジタル技術に関して信頼し助力を期待できる相手-1



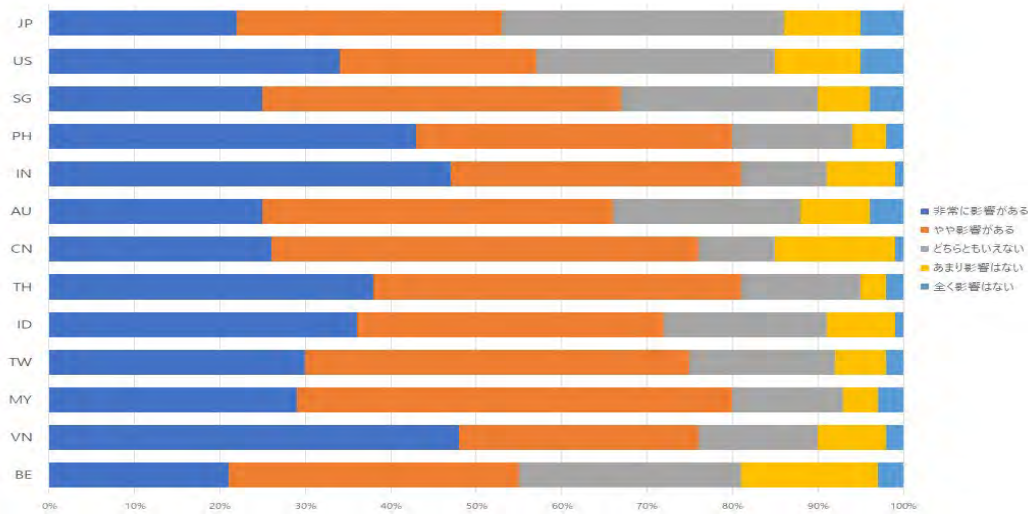
図表 2-3-59 消費者対象・DFFT 編　デジタル技術に関して信頼し助力を期待できる相手-2



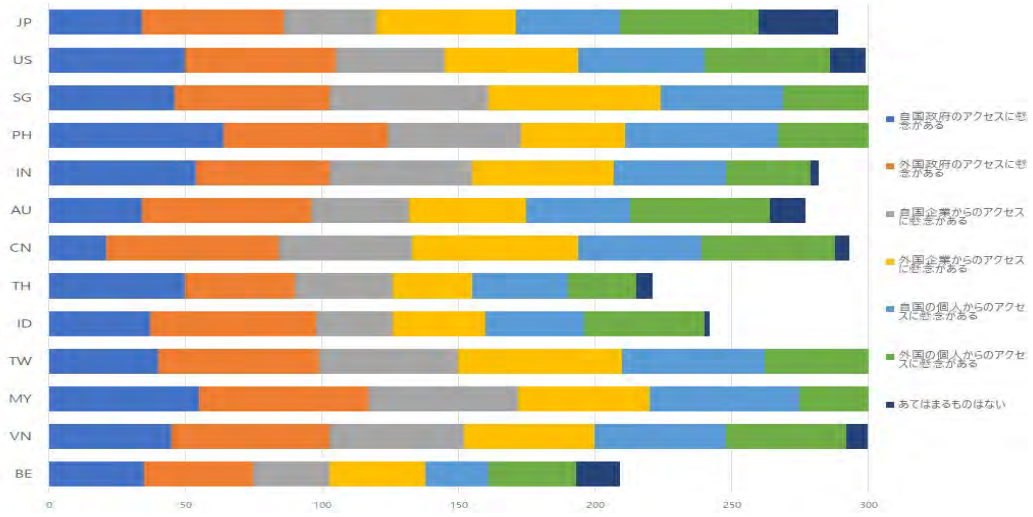
図表 2-3-60 消費者対象・DFFT 編　デジタル技術に関して信頼し助力を期待できる相手-3



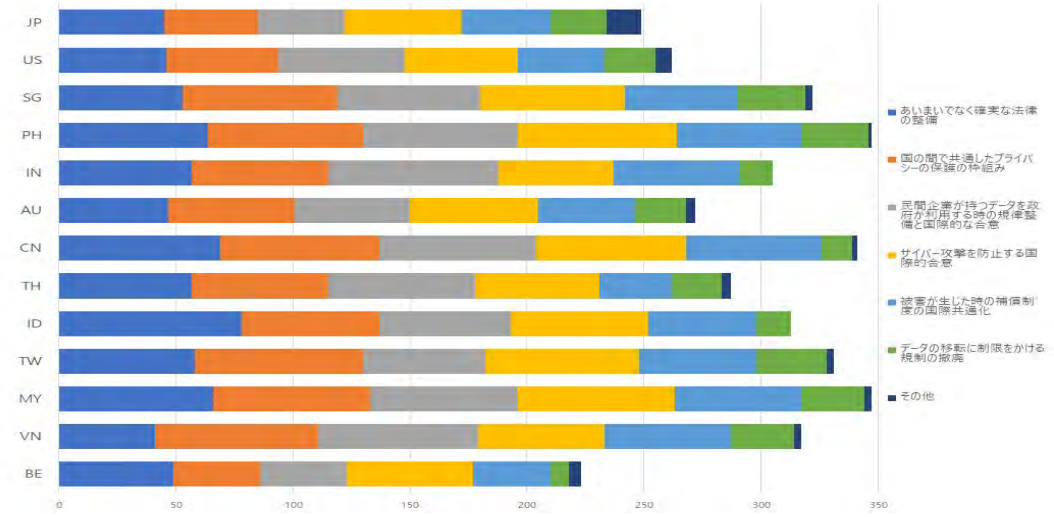
図表 2-3- 61 消費者対象・DFFT 編　法的要求で政府がデータアクセスしてくることへの懸念



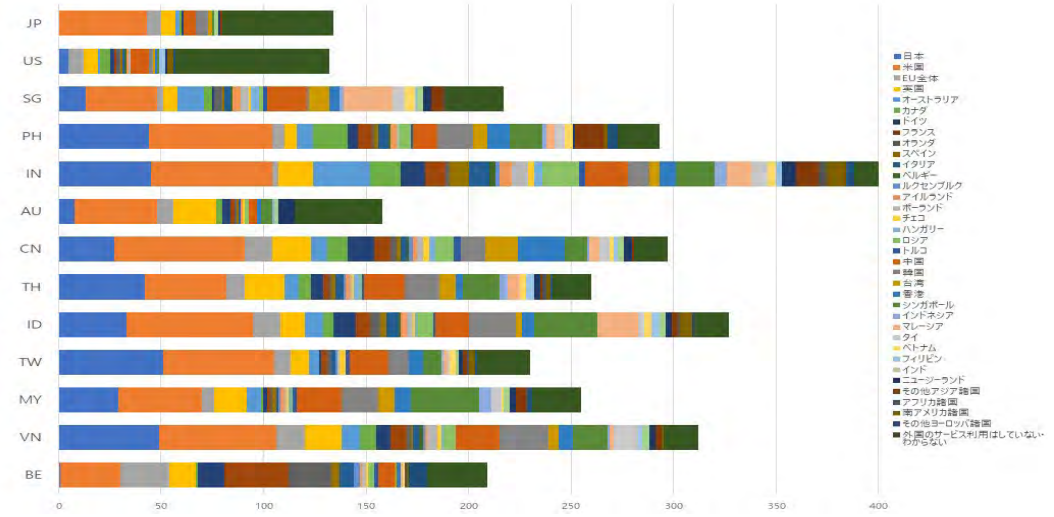
図表 2-3-62 消費者対象・DFFT 編　政府によるアクセス可能性が外国サービス利用の判断に与える影響



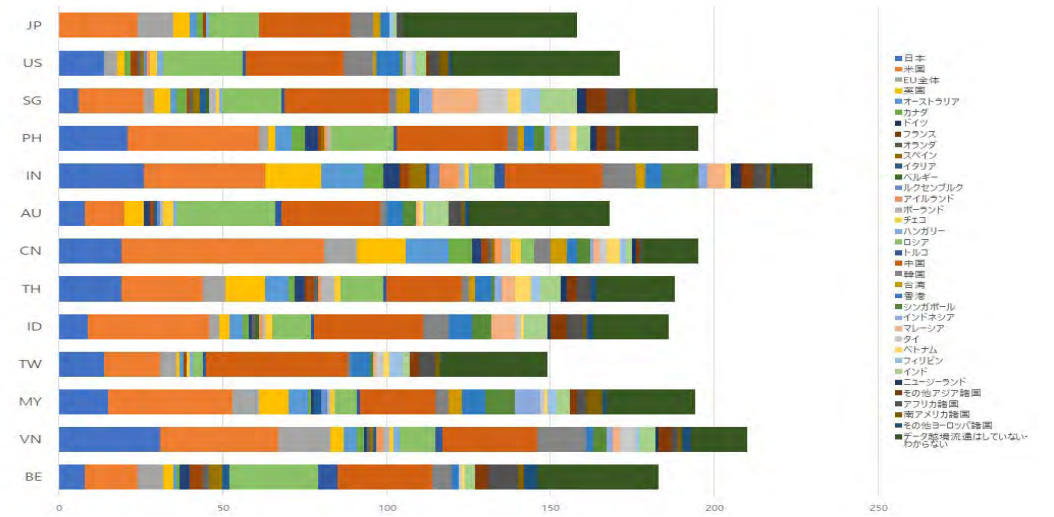
図表 2-3-63 消費者対象・DFFT 編　サイバー攻撃で個人データにアクセスされることへの懸念



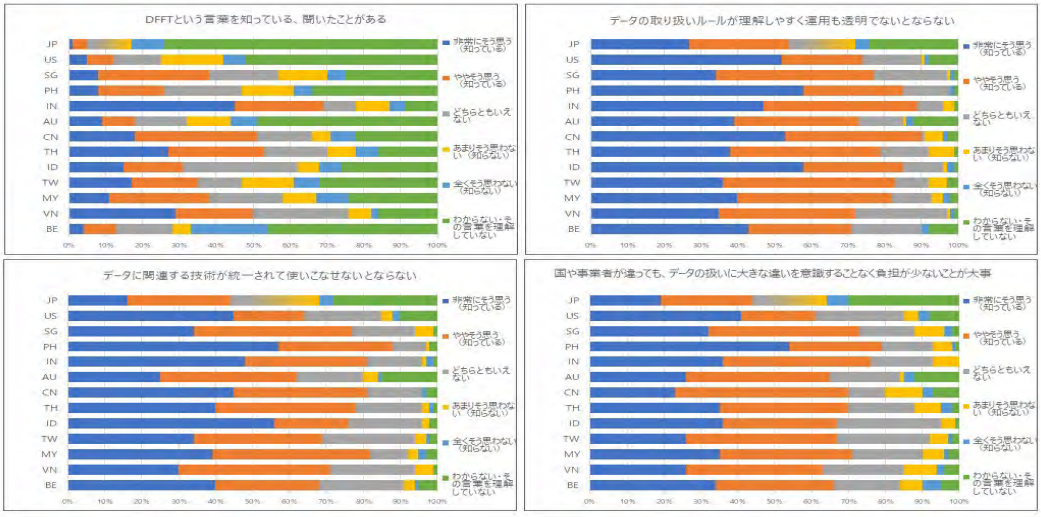
図表 2-3-64 消費者対象・DFFT 編　信頼を高め、越境データ流通の障壁を減らすために役立つ施策



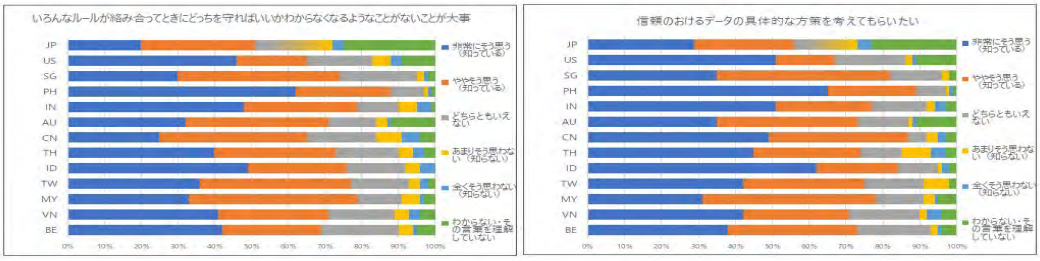
図表 2-3-65 消費者対象・DFFT 編　国外サービスを利用する際、どの国のサービスが多いか



図表 2-3-66 消費者対象・DFFT 編　越境データ流通に影響を与える規制のある国・地域

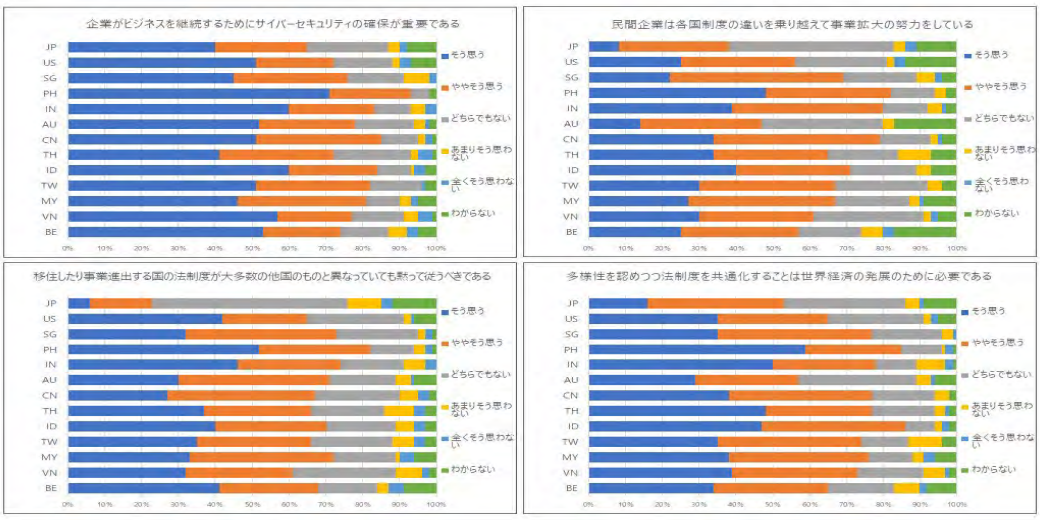


図表 2-3-67 消費者対象・DFFT 編　データ取扱いに関する考え方-1

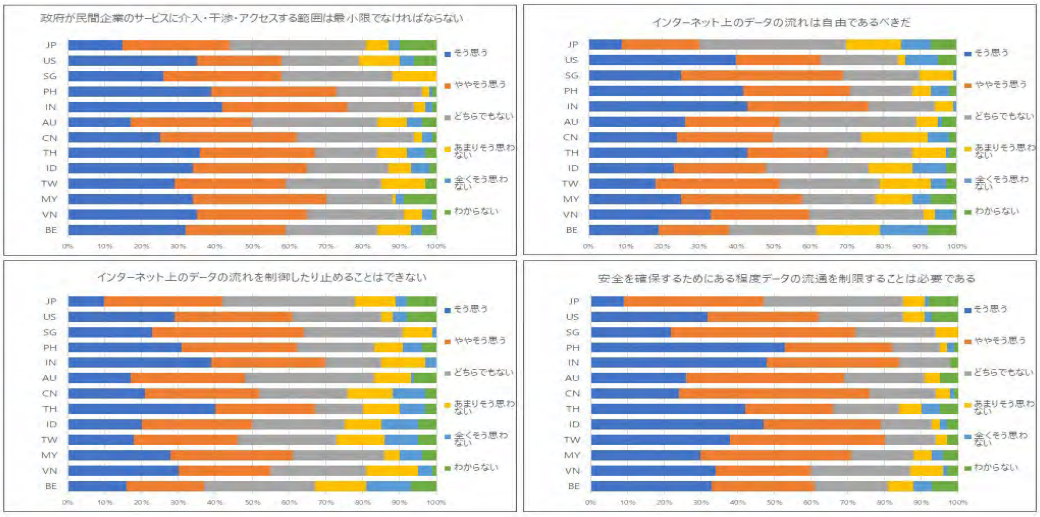


図表 2-3-68 消費者対象・DFFT 編　データ取扱いに関する考え方-2

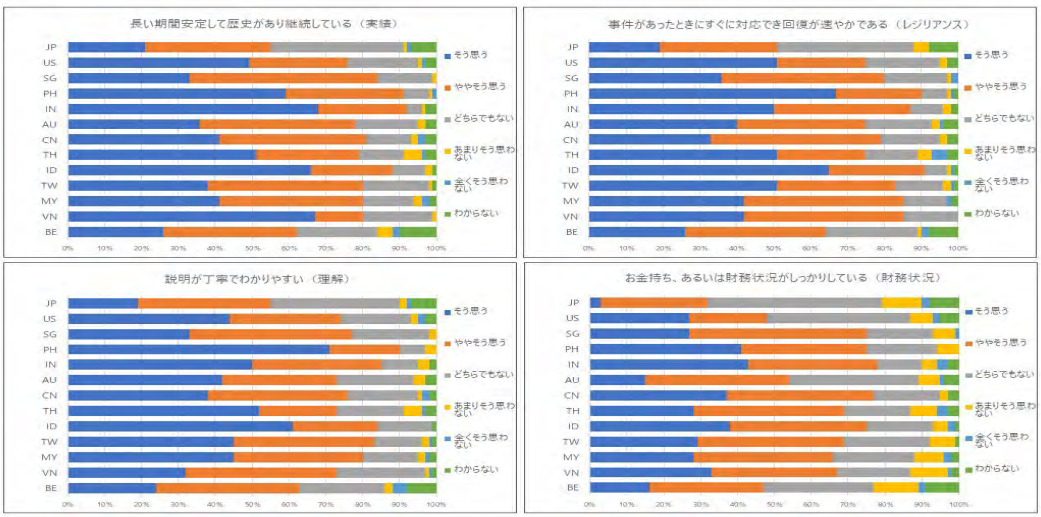
図表 2-3-69 消費者対象・DFFT 編　時事問題についての意見-1



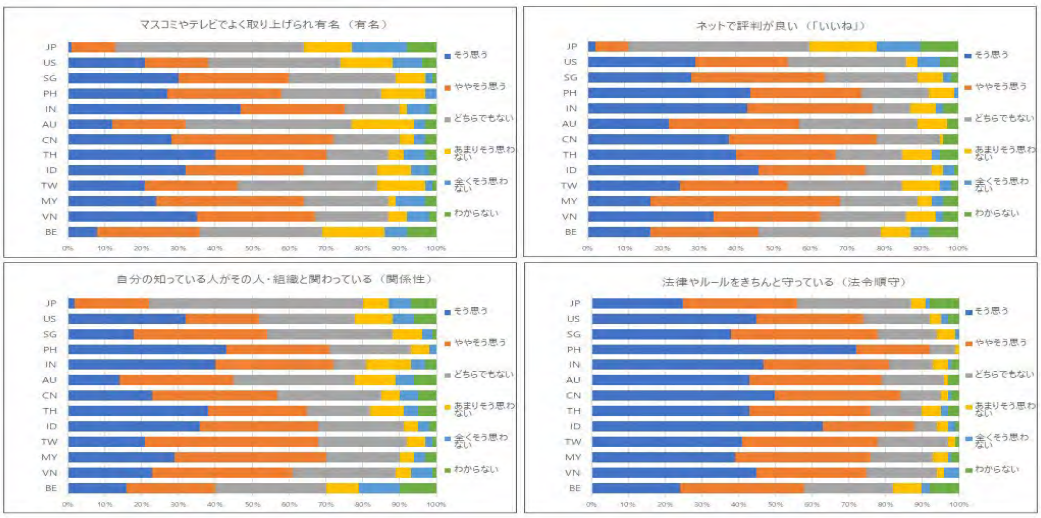
図表 2-3-70 消費者対象・DFFT 編　時事問題についての意見-2



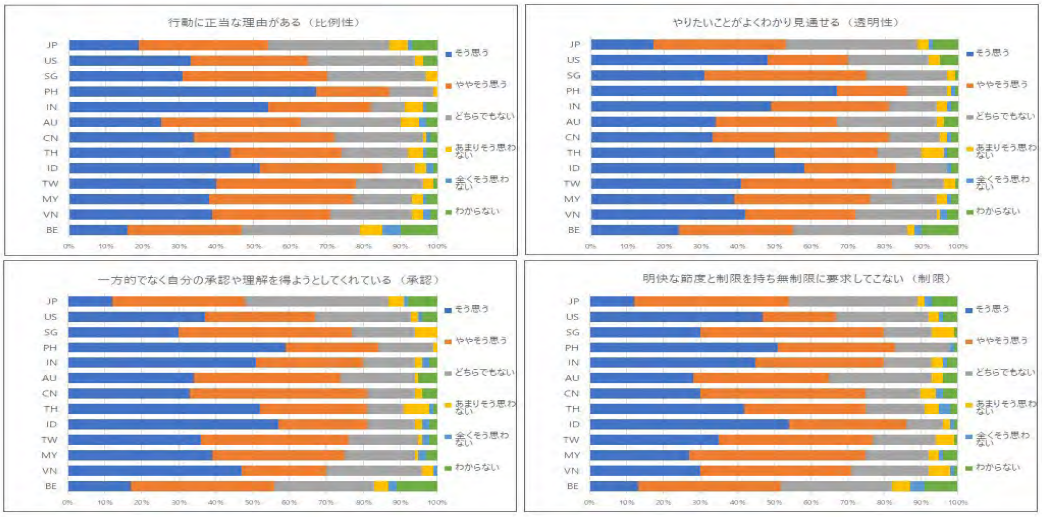
図表 2-3-71 消費者対象・DFFT 編　時事問題についての意見-3



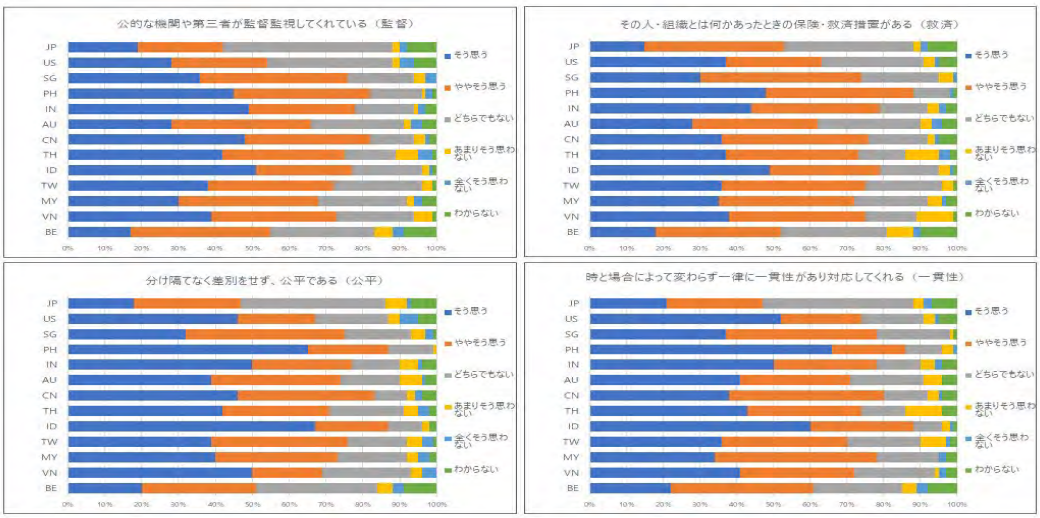
図表 2-3-72 消費者対象・DFFT 編　相手を信頼できる理由-1



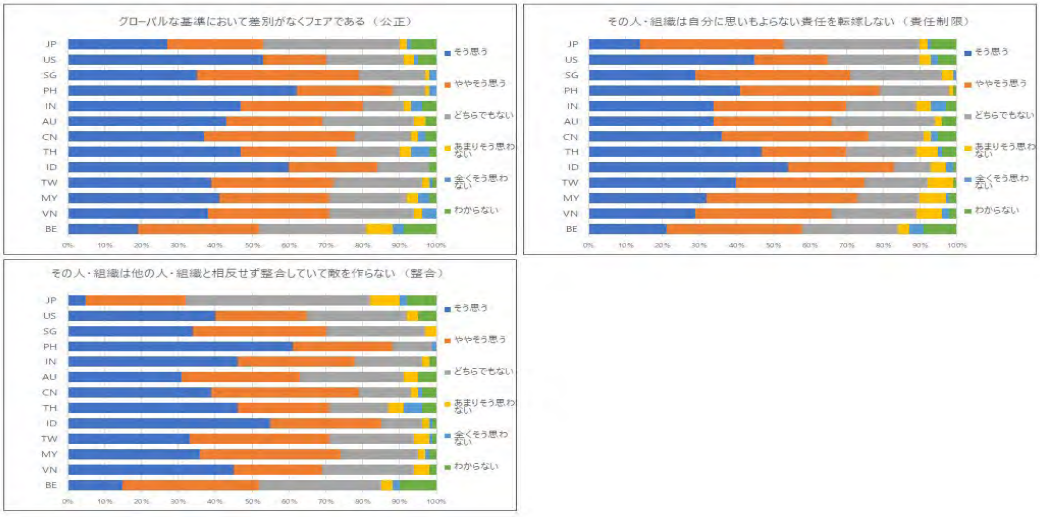
図表 2-3-73 消費者対象・DFFT 編　相手を信頼できる理由-2



図表 2-3-74 消費者対象・DFFT 編　相手を信頼できる理由-3

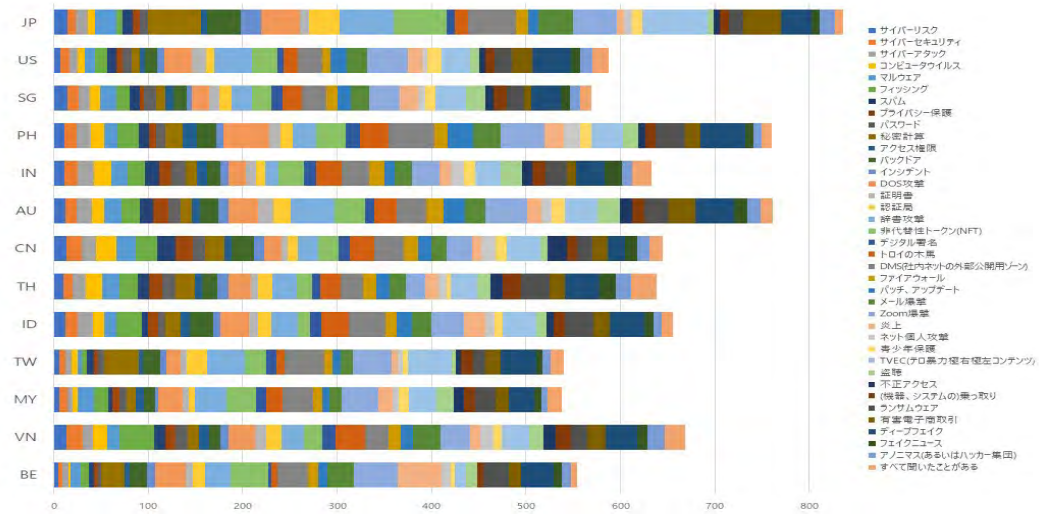


図表 2-3-75 消費者対象・DFFT 編　相手を信頼できる理由-4

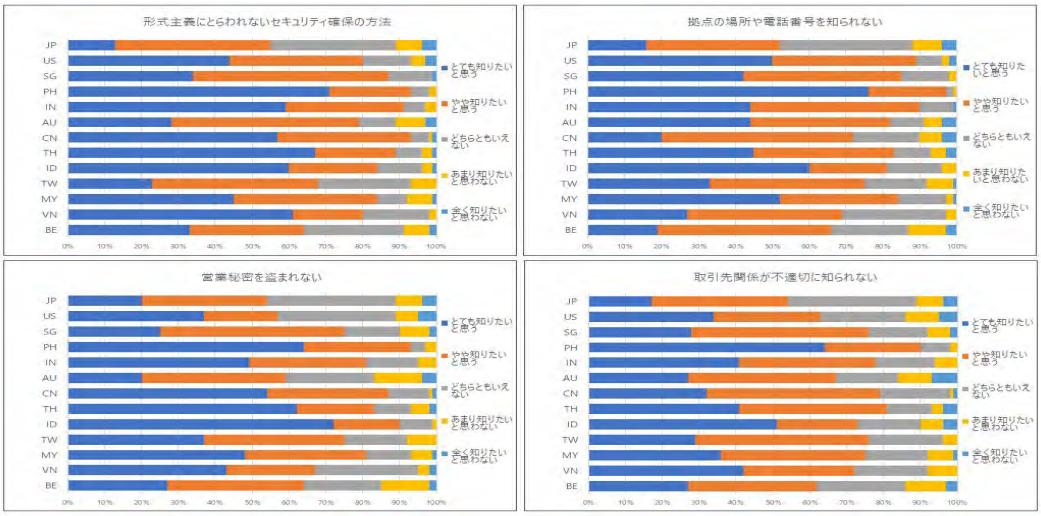


図表 2-3-76 消費者対象・DFFT 編　相手を信頼できる理由-5

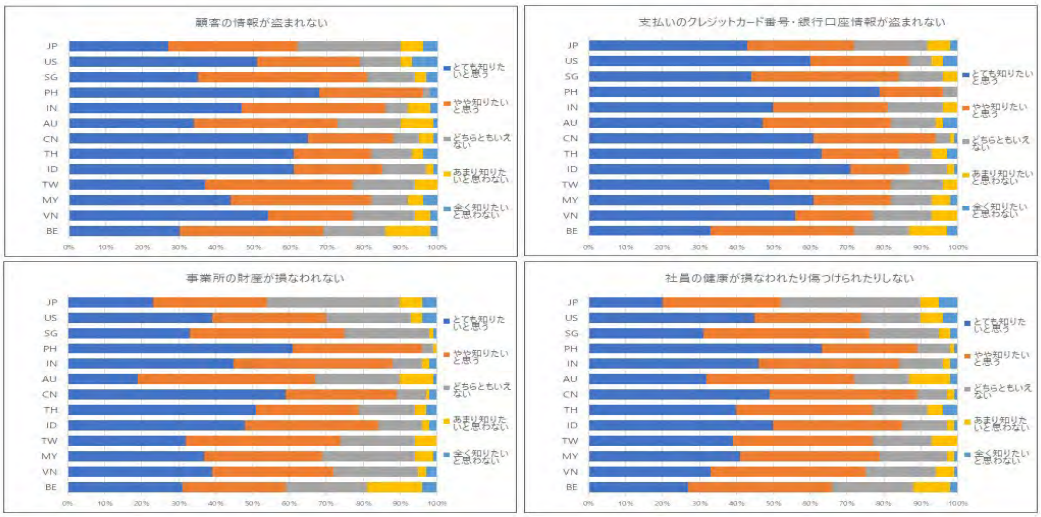
(4) 勤労者対象・セキュリティ編



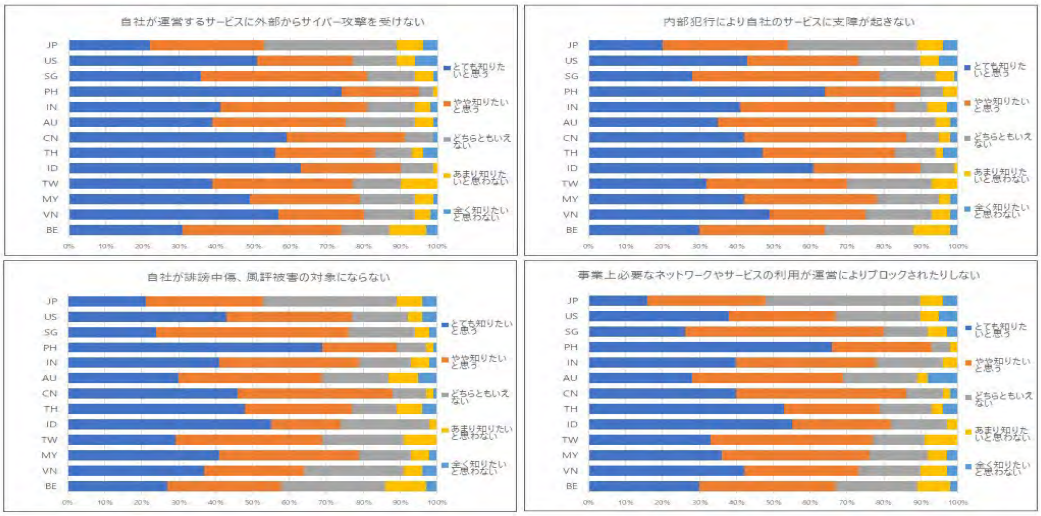
図表 2-3-77 勤労者対象・セキュリティ編　聞いたことも気にかけたこともない言葉



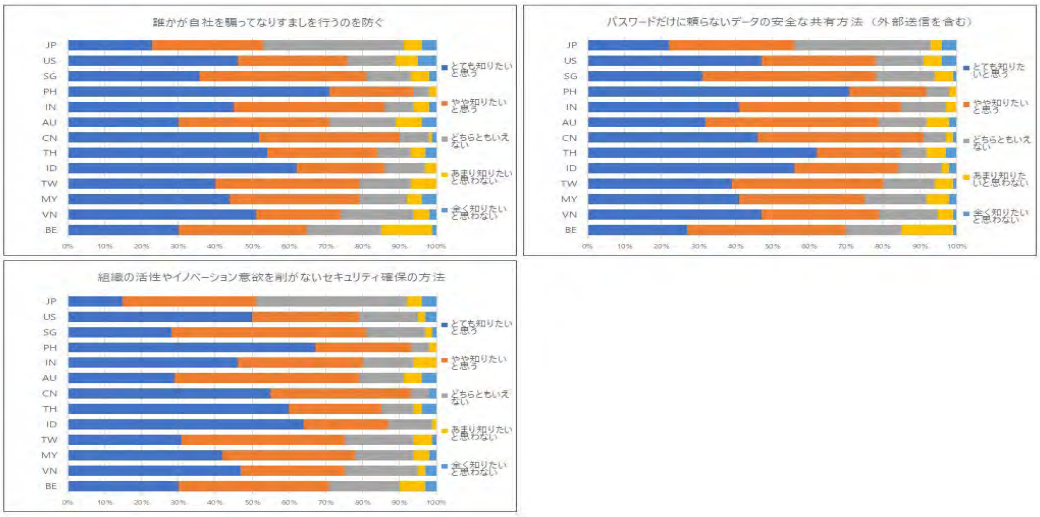
図表 2-3-78 勤労者対象・セキュリティ編　セキュリティに対する興味-1



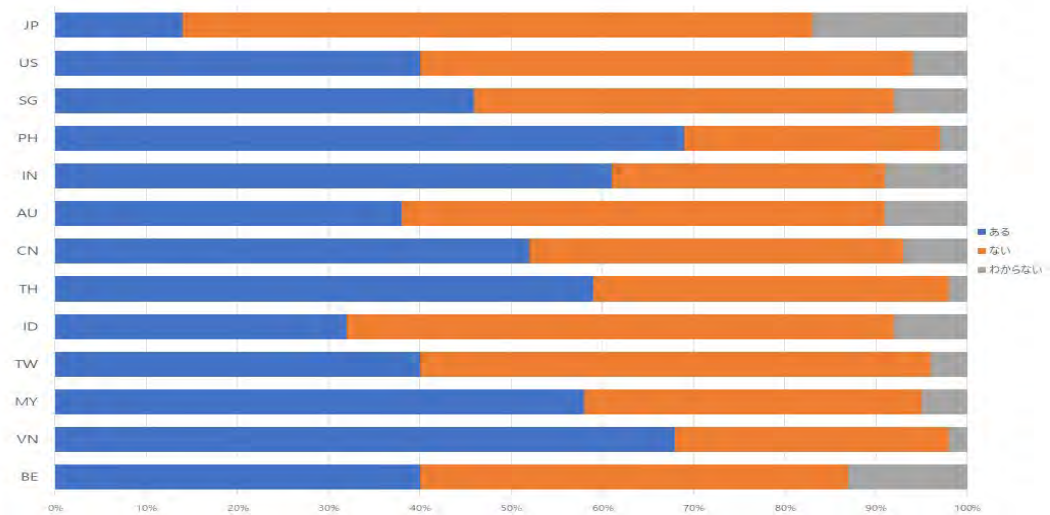
図表 2-3-79 勤労者対象・セキュリティ編　セキュリティに対する興味-2



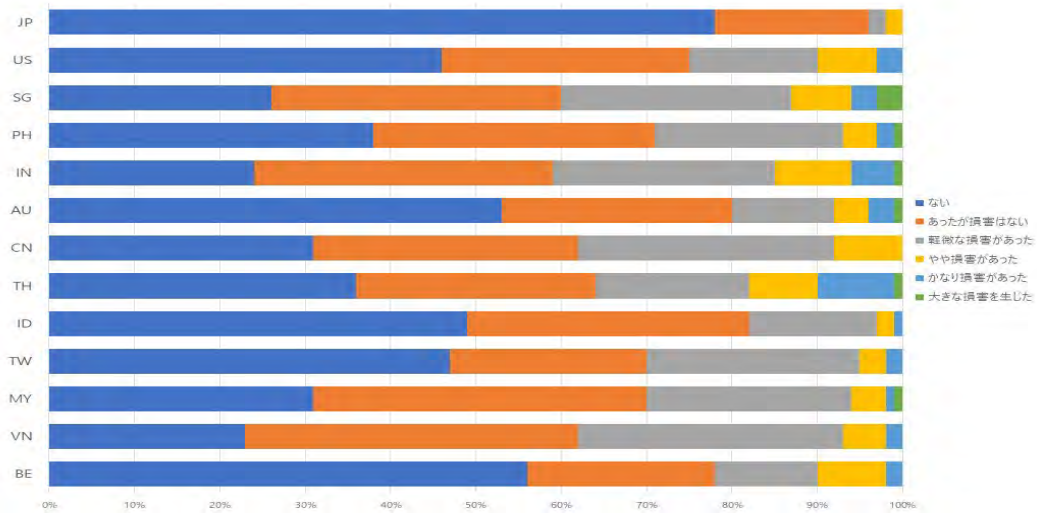
図表 2-3-80 勤労者対象・セキュリティ編　セキュリティに対する興味-3



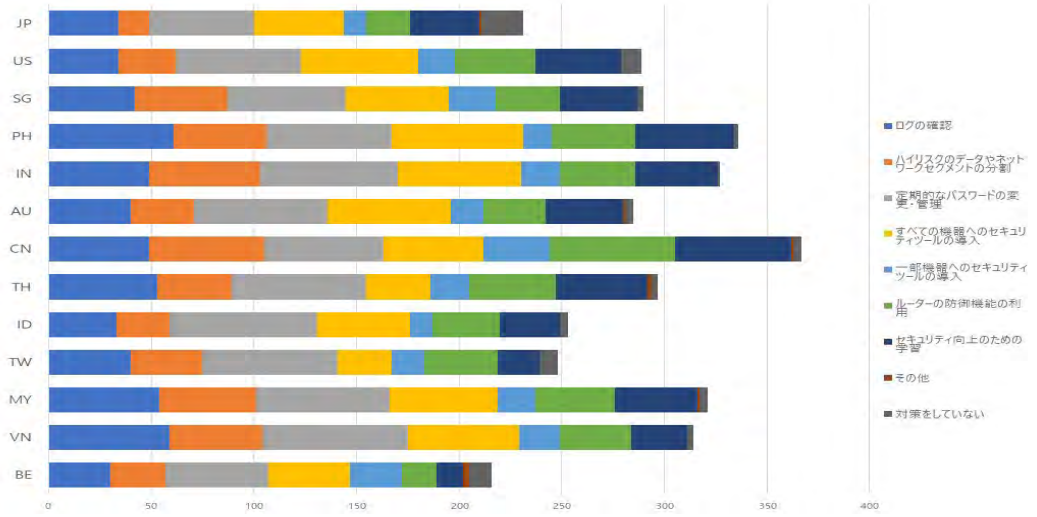
図表 2-3-81 勤労者対象・セキュリティ編　セキュリティに対する興味-4



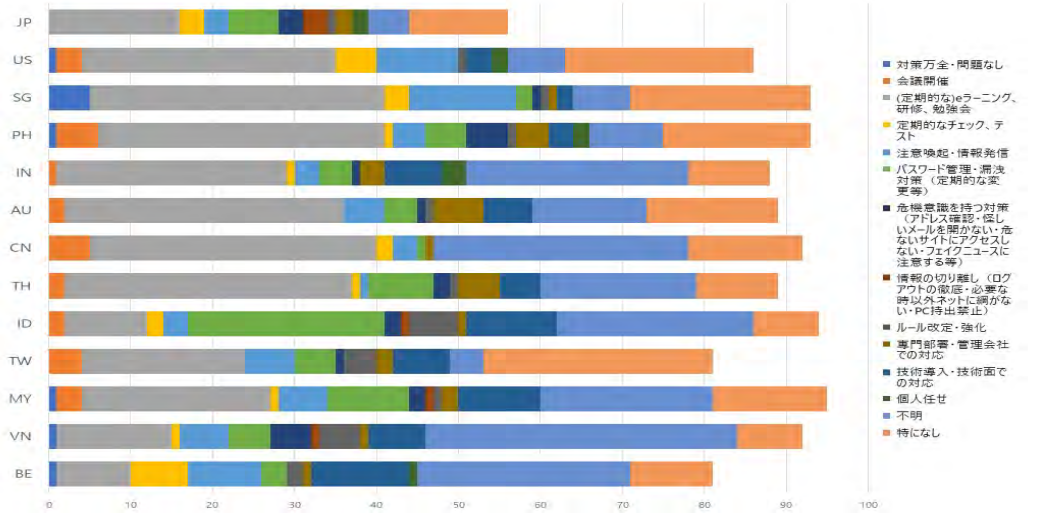
図表 2-3-82 勤労者対象・セキュリティ編　職場におけるスマホ・PC 利用時のデータ被害経験



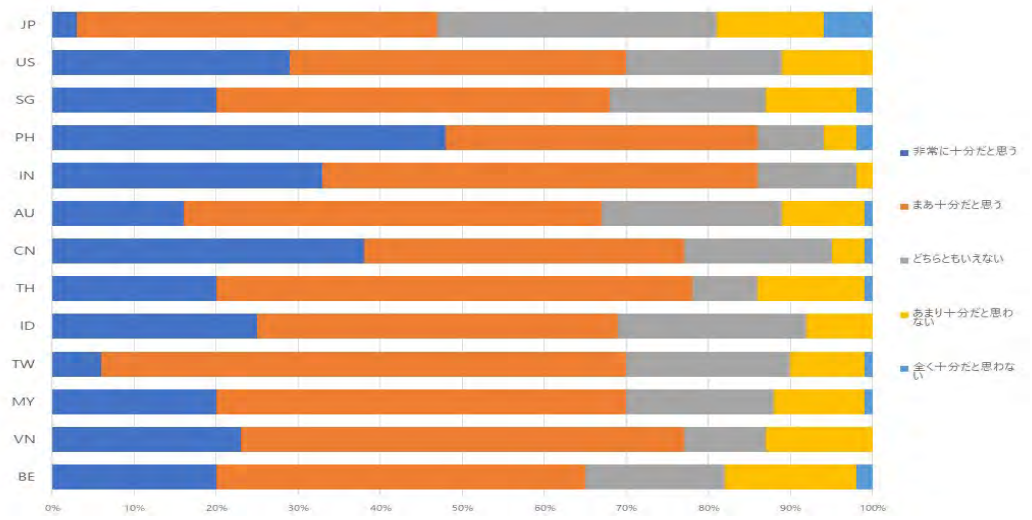
図表 2-3-83 勤労者対象・セキュリティ編　自社の個人情報・機密情報漏洩経験



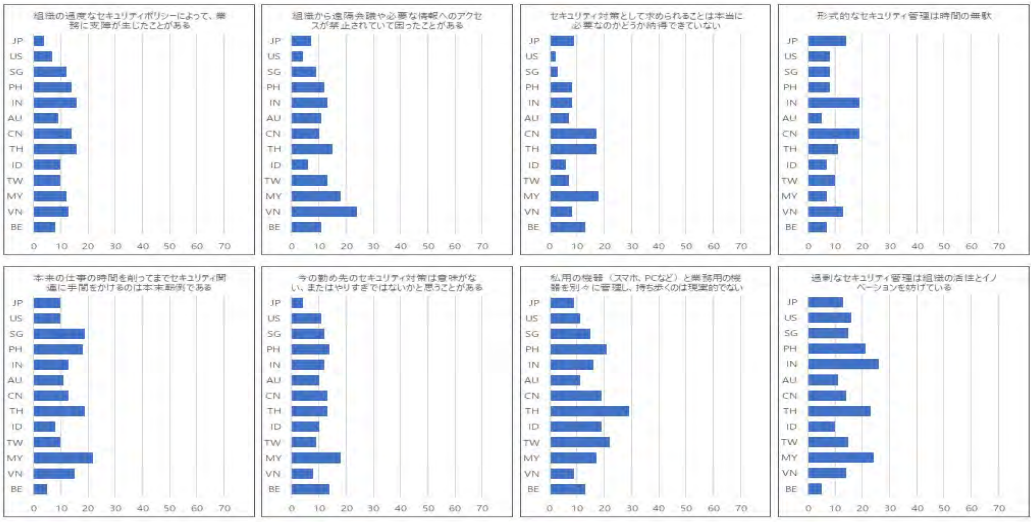
図表 2-3-84 勤労者対象・セキュリティ編　職場で実施しているセキュリティ対策



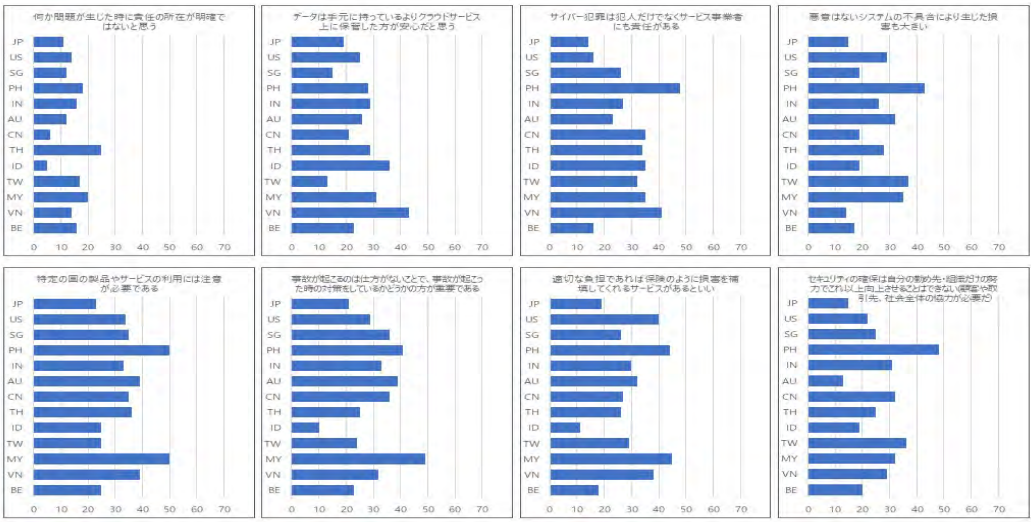
図表 2-3-85 勤労者対象・セキュリティ編　セキュリティ意識に対する啓発活動



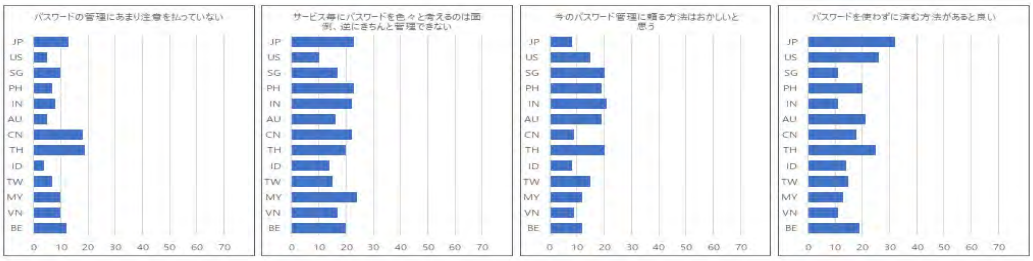
図表 2-3-86 勤労者対象・セキュリティ編　組織としてのセキュリティ教育・情報提供の十分性



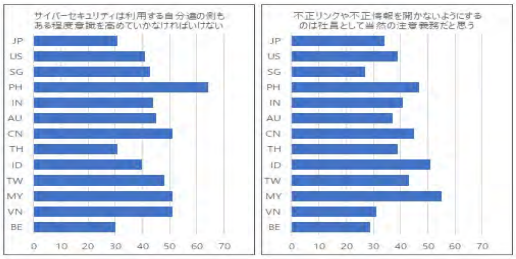
図表 2-3-87 勤労者対象・セキュリティ編　サイバーセキュリティに関する否定的な意見



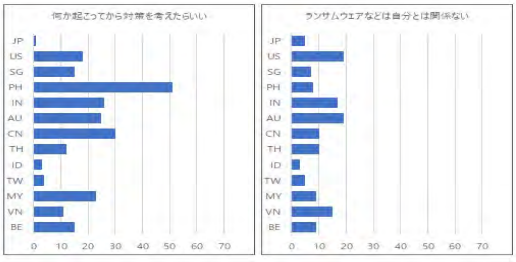
図表 2-3-88 勤労者対象・セキュリティ編　サイバーセキュリティに関する制度的な問題意識



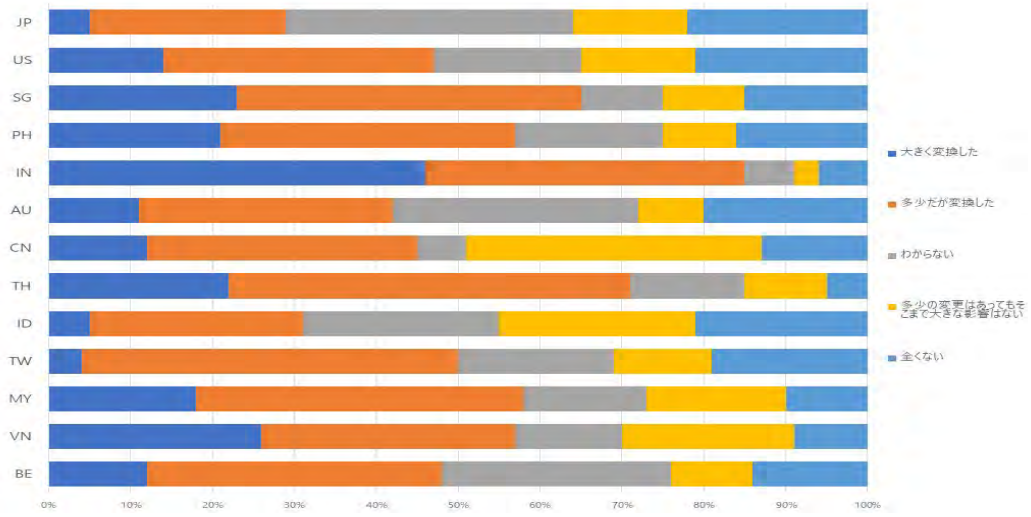
図表 2-3-89 勤労者対象・セキュリティ編　サイバーセキュリティに関するパスワードへの不満



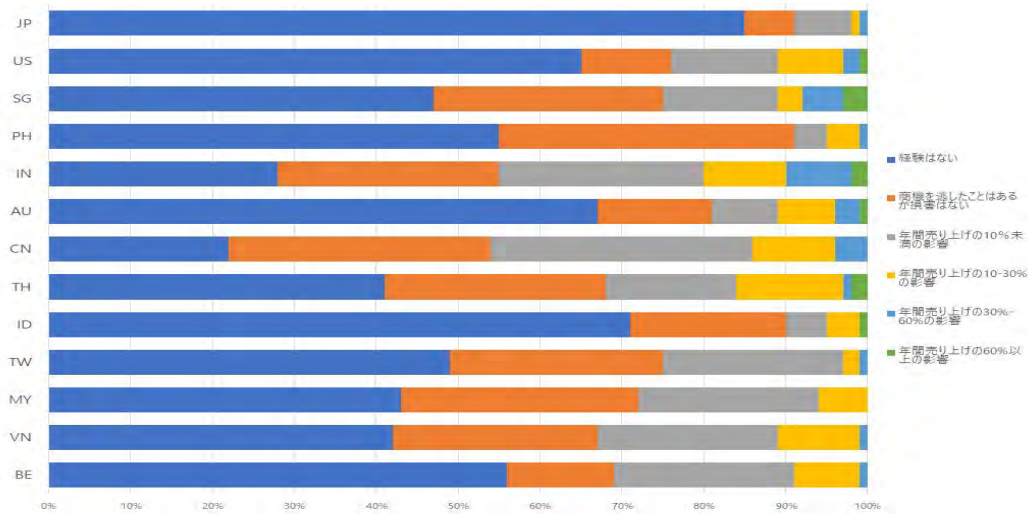
図表 2-3- 90 勤労者対象・セキュリティ編　サイバーセキュリティに関する当事者意識を示す意見



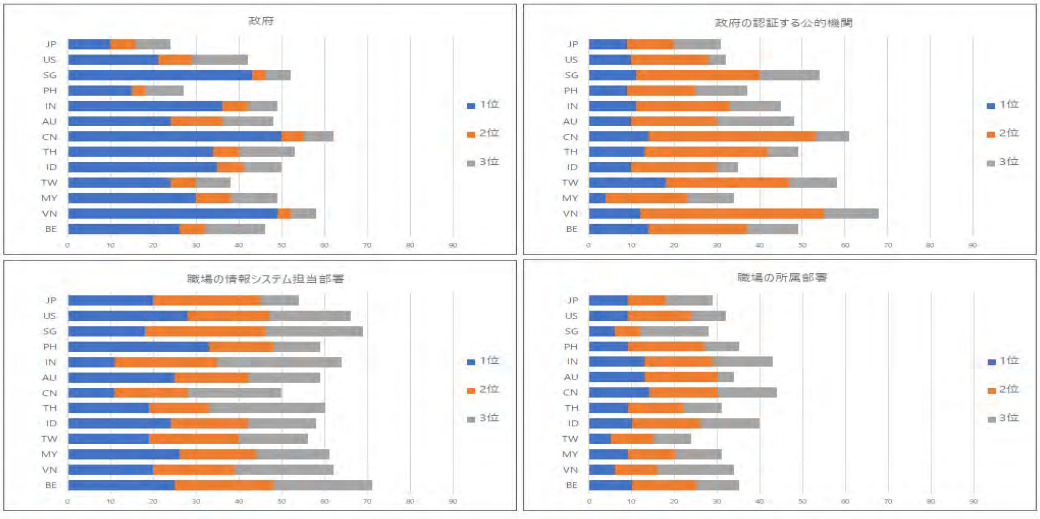
図表 2-3-91 勤労者対象・セキュリティ編　サイバーセキュリティに関する無関心な意見



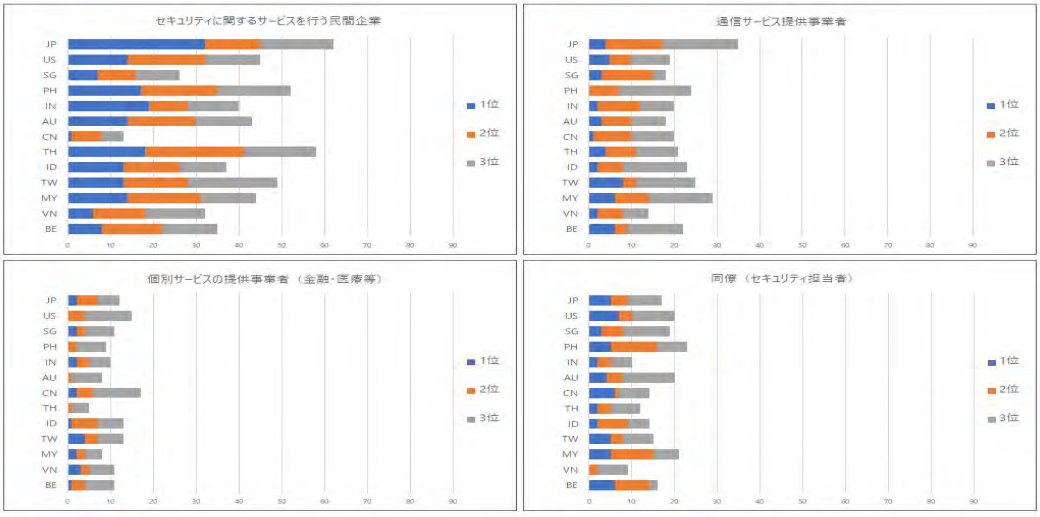
図表 2-3-92 勤労者対象・セキュリティ編　セキュリティ規制でビジネスモデル変換を要した経験



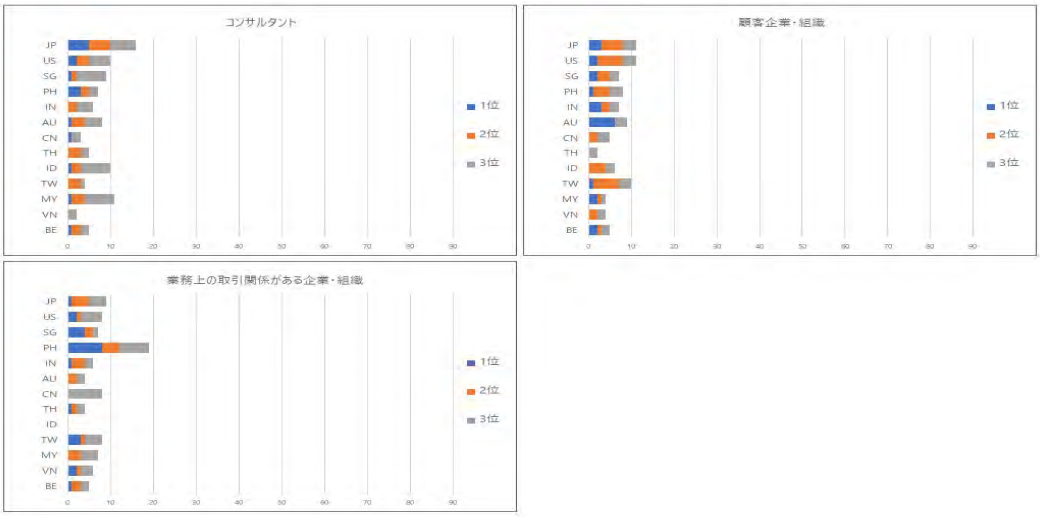
図表 2-3-93 勤労者対象・セキュリティ編　セキュリティ対策でサプライチェーンから排除された経験



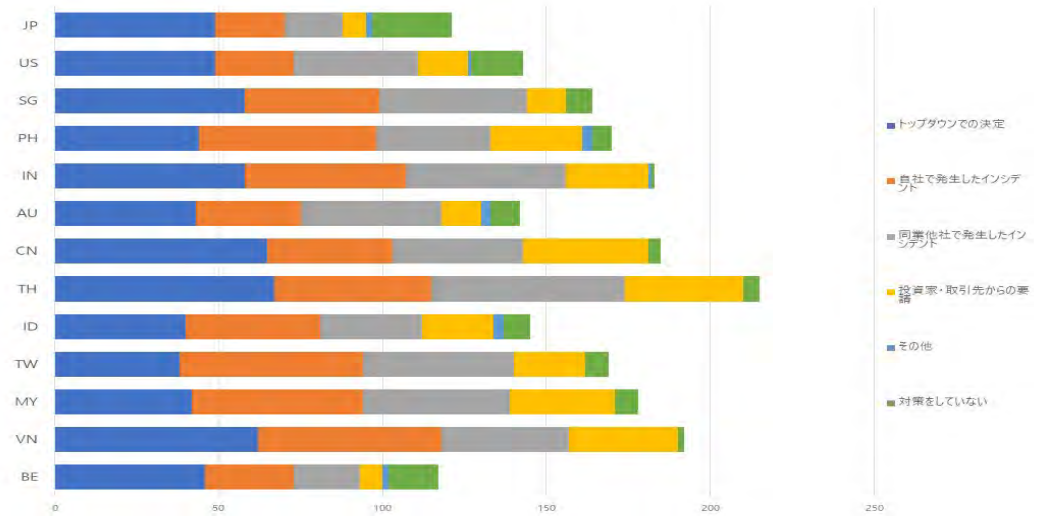
図表 2-3- 94 勤労者対象・セキュリティ編　組織、業務を守るため信頼し助力を期待できる相手-1



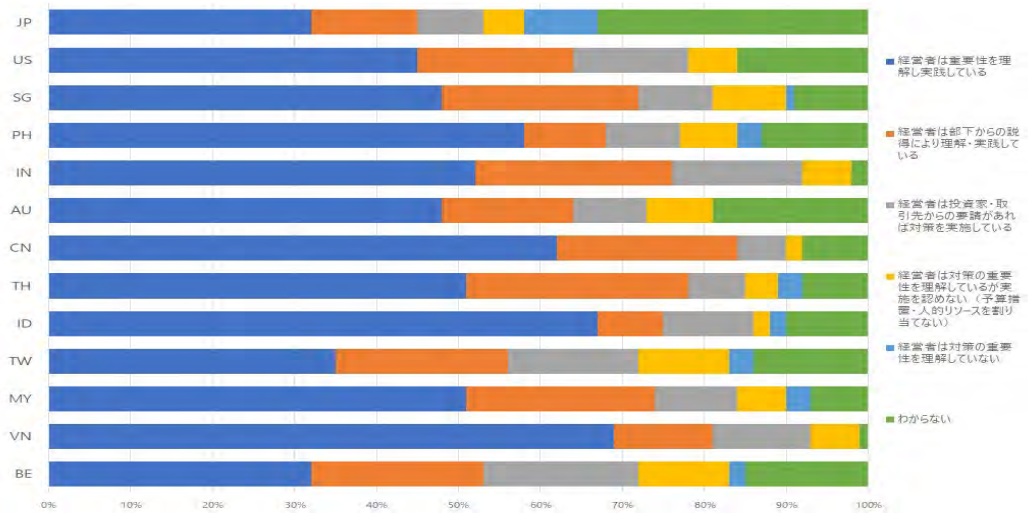
図表 2-3-95 勤労者対象・セキュリティ編　組織、業務を守るため信頼し助力を期待できる相手-2



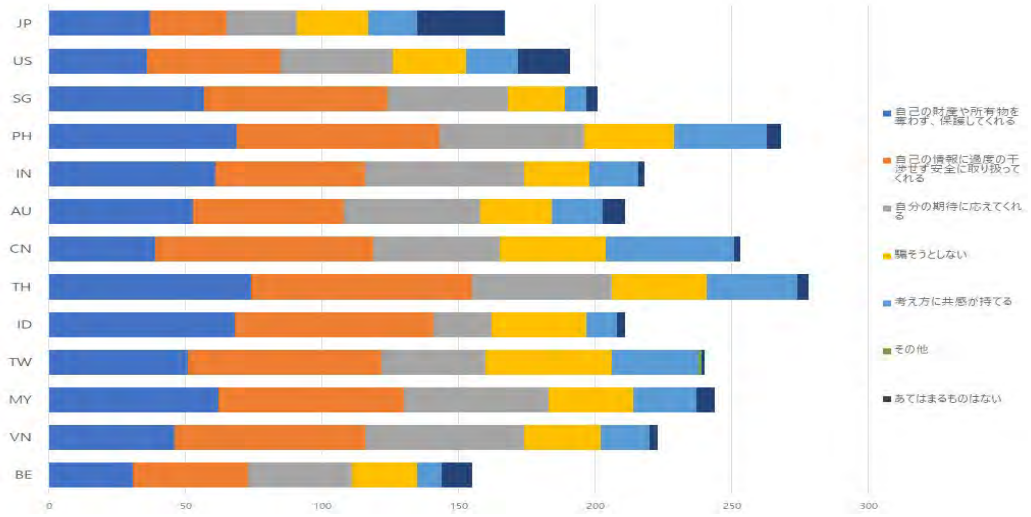
図表 2-3-96 勤労者対象・セキュリティ編　組織、業務を守るため信頼し助力を期待できる相手-3



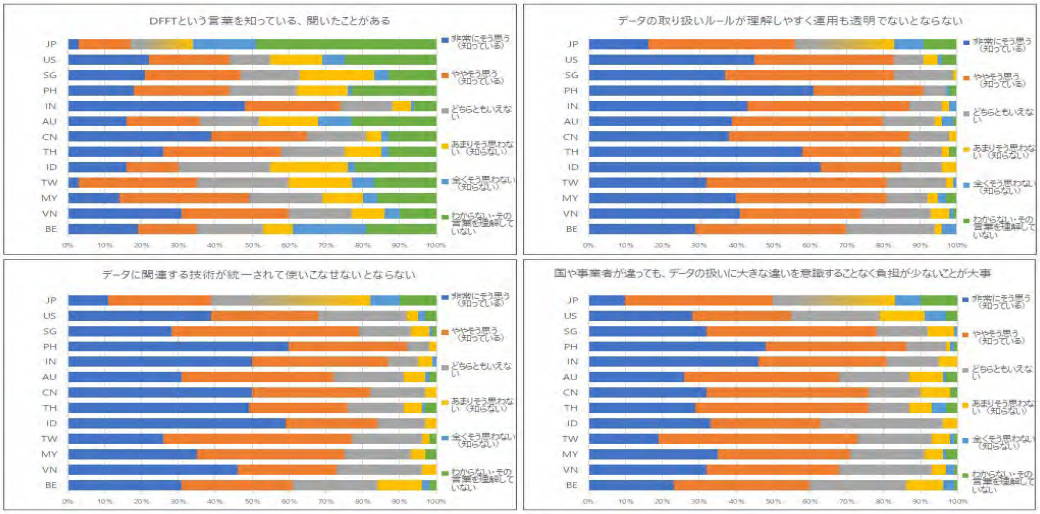
図表 2-3-97 勤労者対象・セキュリティ編　セキュリティ対策を取ることになったきっかけ



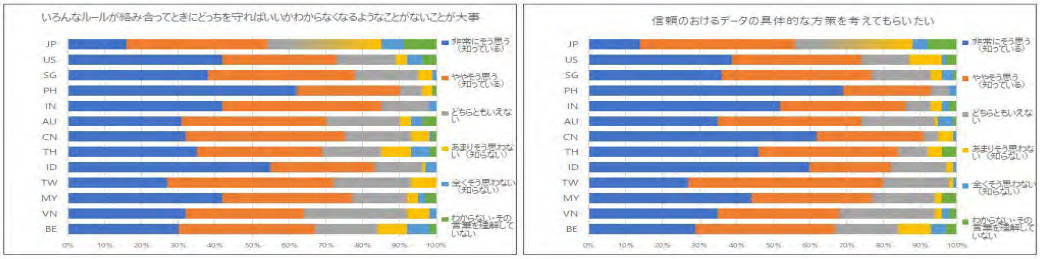
図表 2-3-98 勤労者対象・セキュリティ編　経営者のセキュリティ対策への関与度



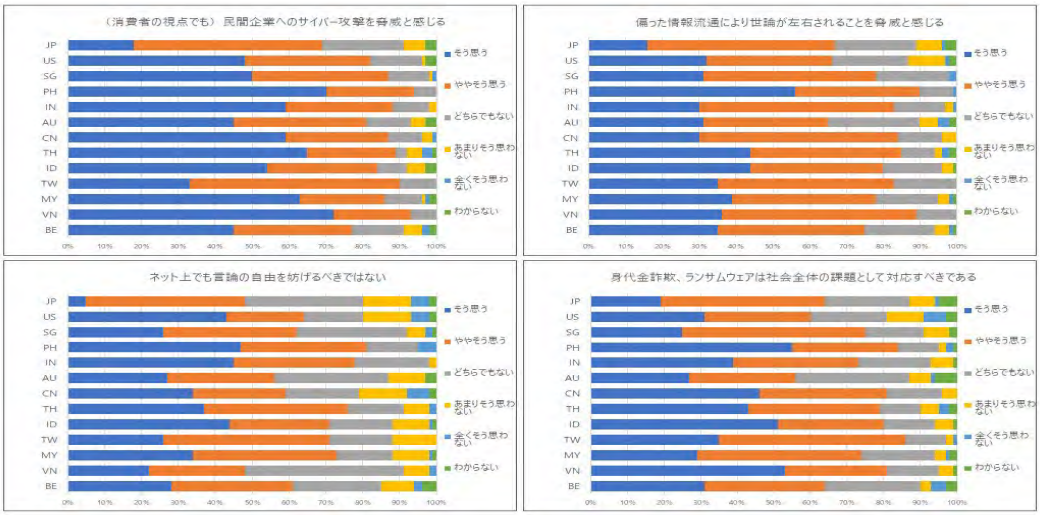
図表 2-3-99 勤労者対象・セキュリティ編　政府や企業、組織、個人を信頼するための判断材料



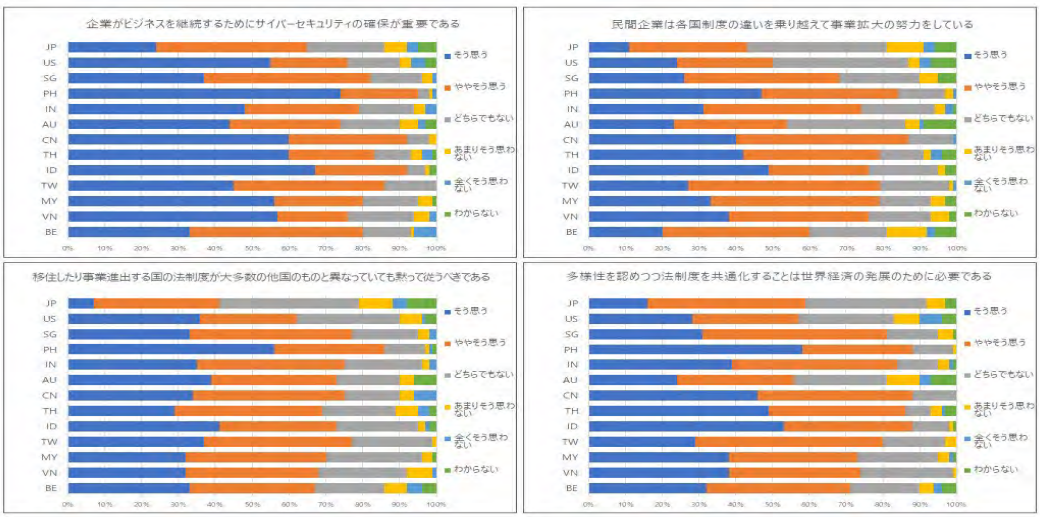
図表 2-3-100 勤労者対象・セキュリティ編　データ取扱いに関する考え方-1



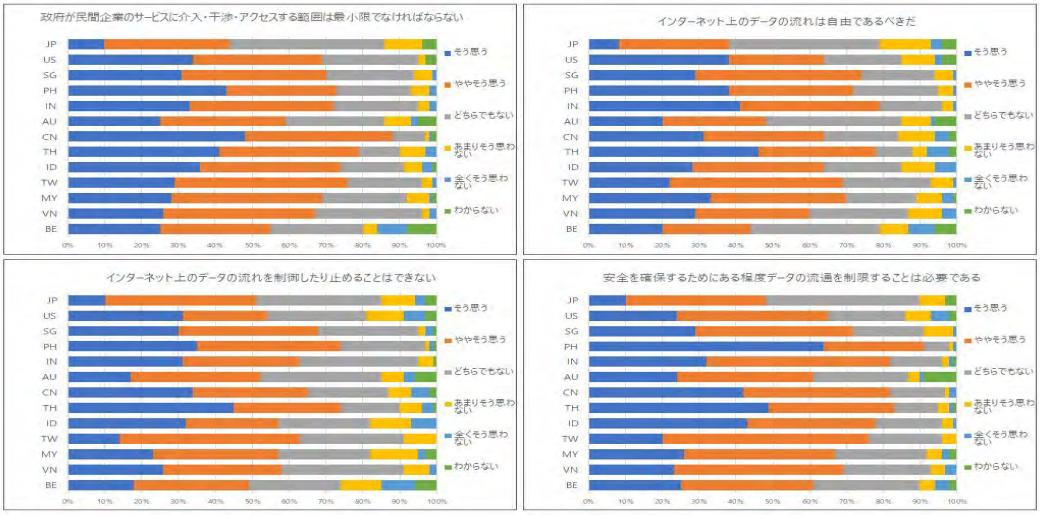
図表 2-3-101 勤労者対象・セキュリティ編　データ取扱いに関する考え方- 2



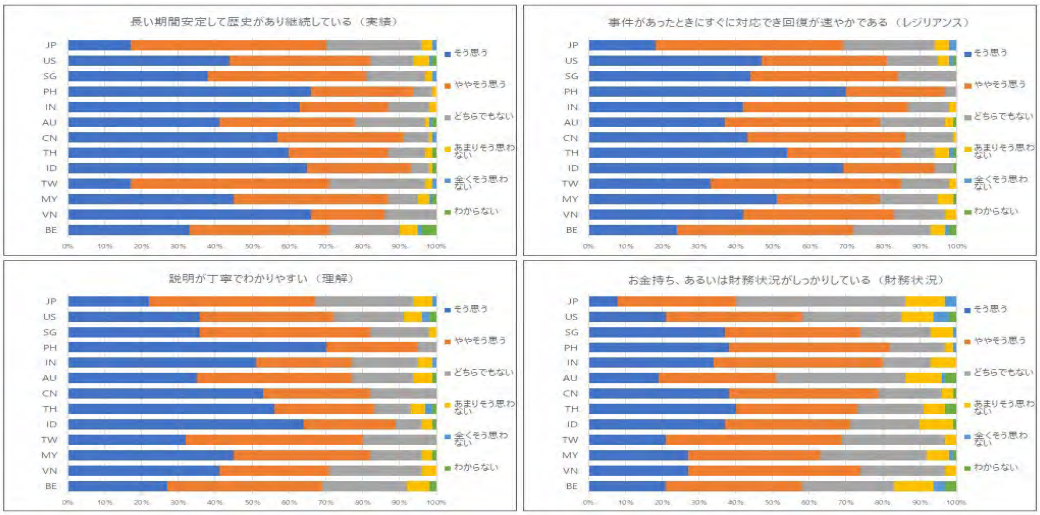
図表 2-3-102 勤労者対象・セキュリティ編　時事問題についての意見-1



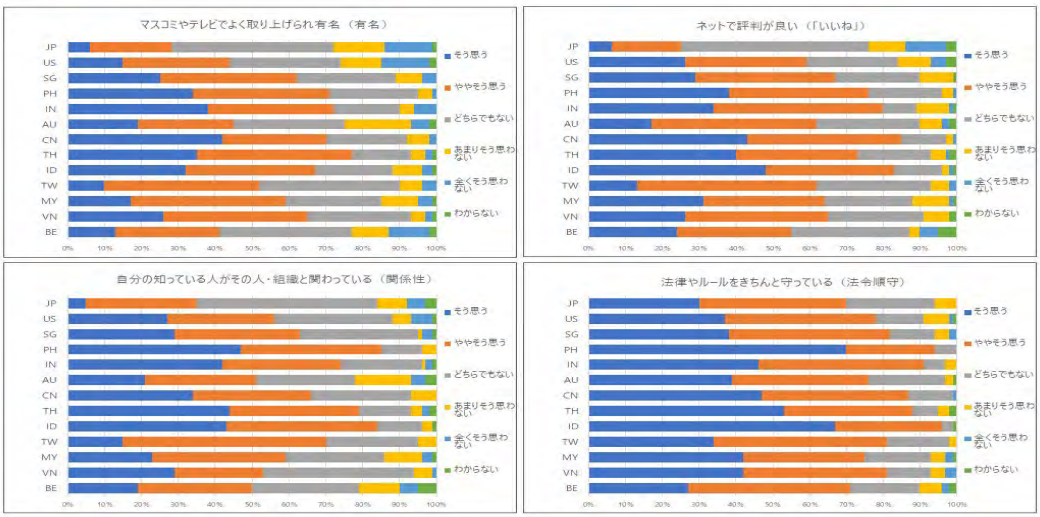
図表 2-3-103 勤労者対象・セキュリティ編　時事問題についての意見-2



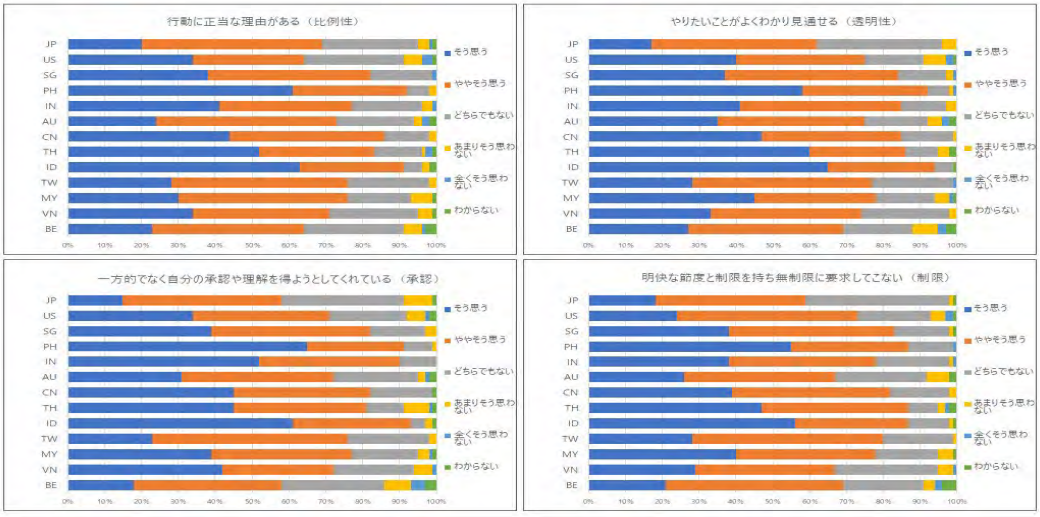
図表 2-3-104 勤労者対象・セキュリティ編　時事問題についての意見-3



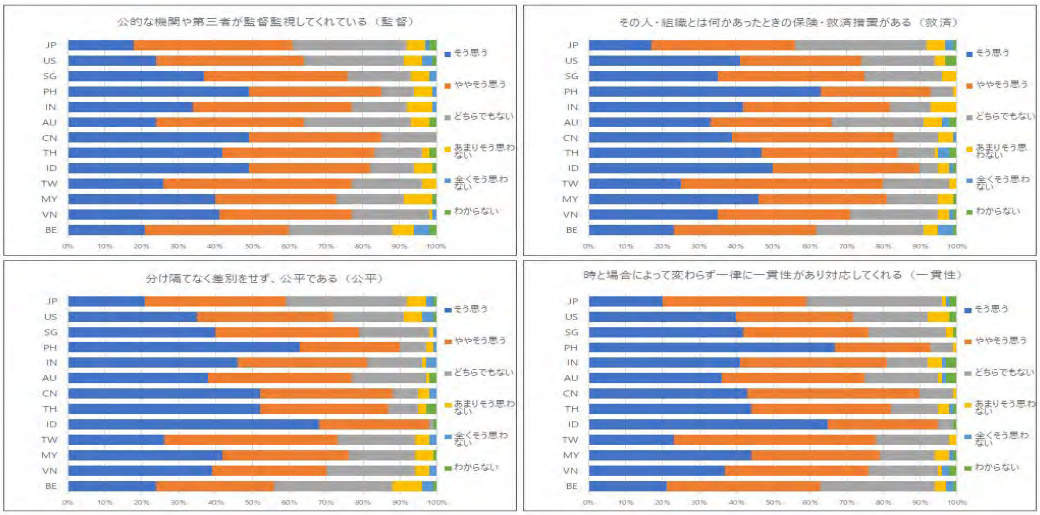
図表 2-3-105 勤労者対象・セキュリティ編　相手を信頼できる理由-1



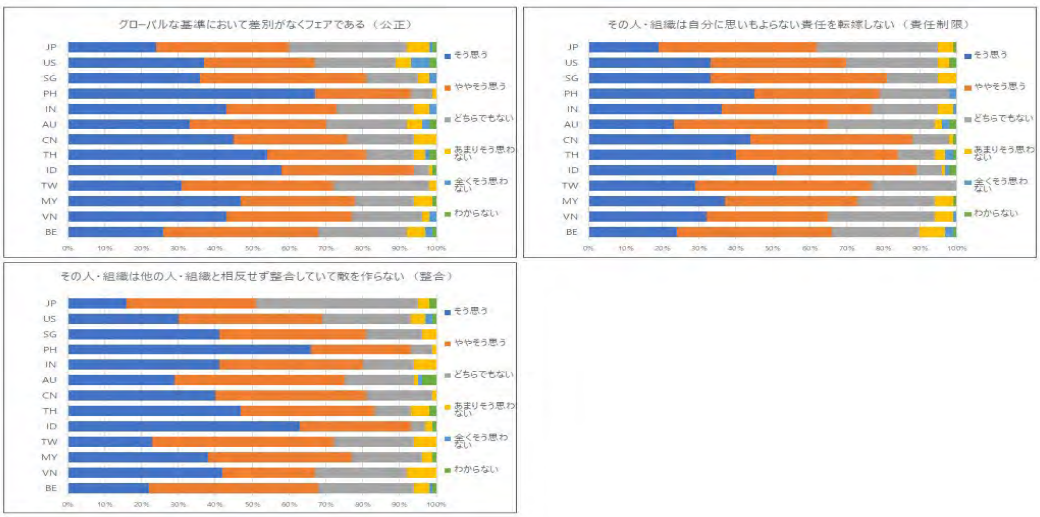
図表 2-3-106 勤労者対象・セキュリティ編　相手を信頼できる理由-2



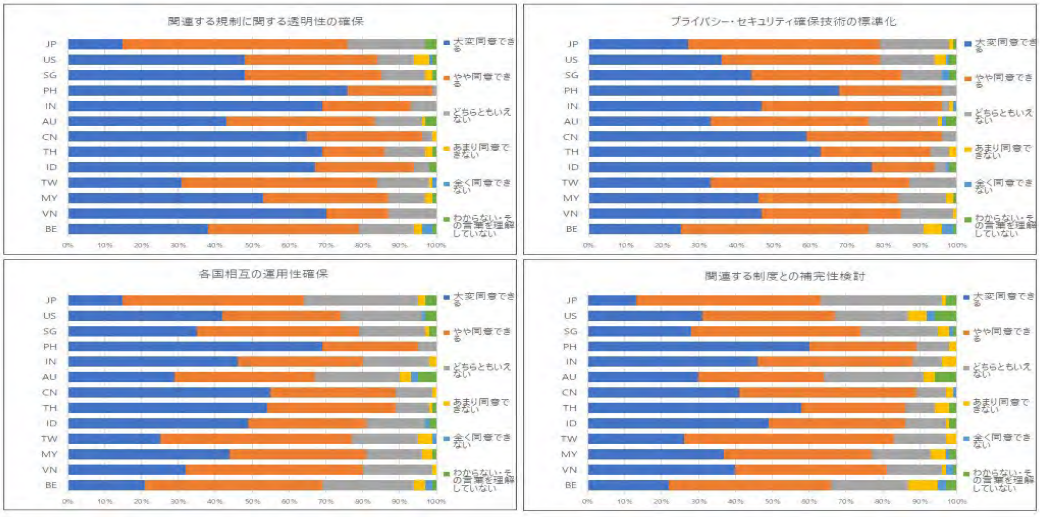
図表 2-3-107 勤労者対象・セキュリティ編　相手を信頼できる理由-3



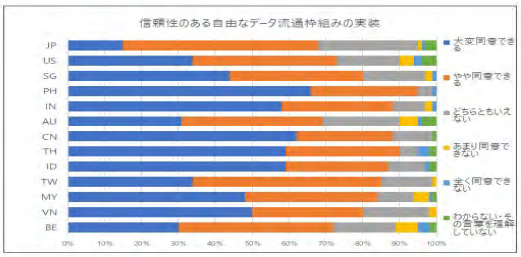
図表 2-3-108 勤労者対象・セキュリティ編　相手を信頼できる理由-4



図表 2-3-109 勤労者対象・セキュリティ編　相手を信頼できる理由-5

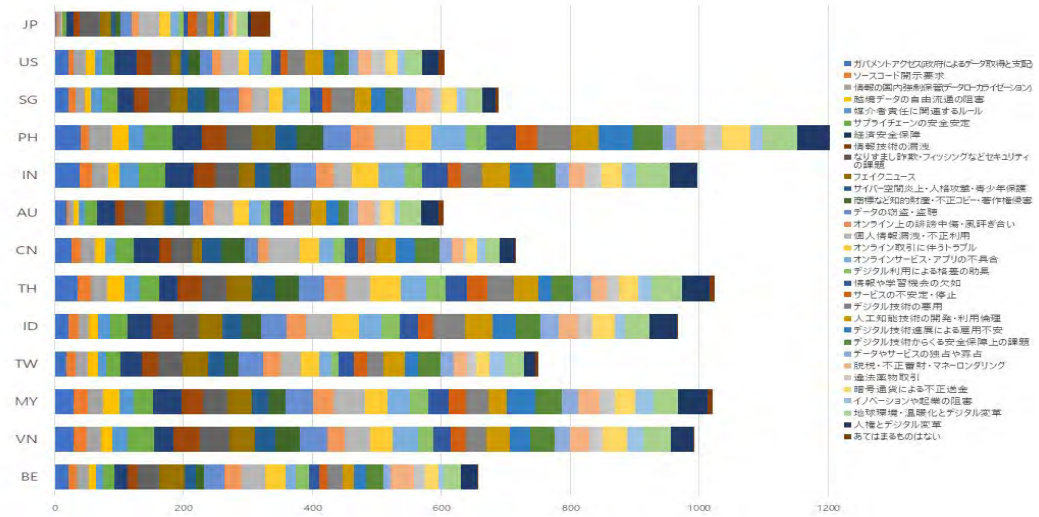


図表 2-3-110 勤労者対象・セキュリティ編　信頼ある自由なデータ流通を実現するための要素-1

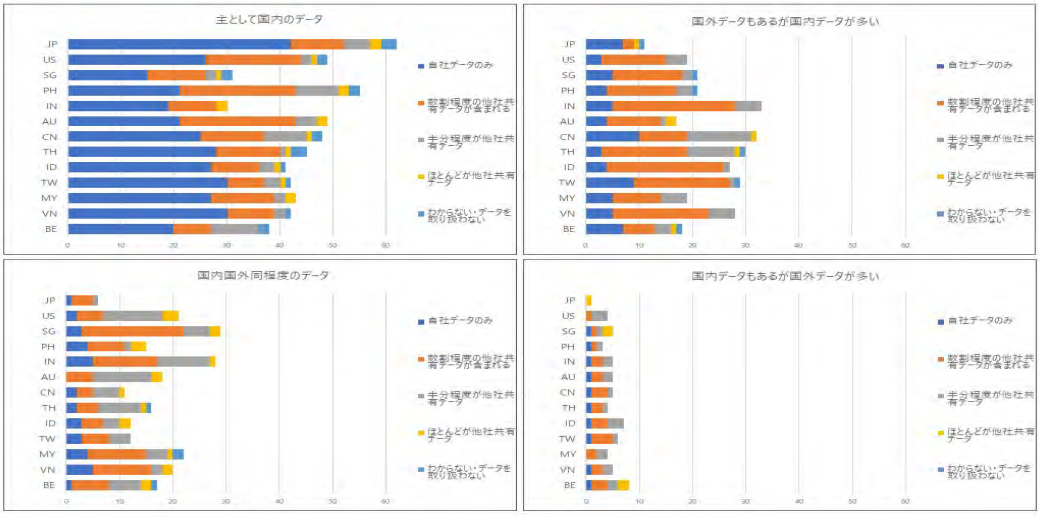


図表 2-3-111 勤労者対象・セキュリティ編　信頼ある自由なデータ流通を実現するための要素-2

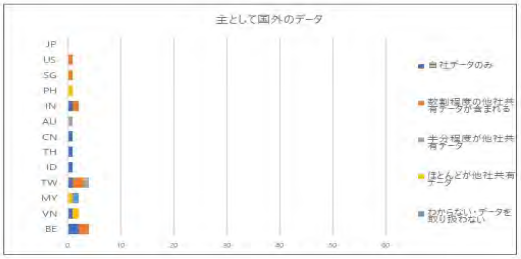
(5) 勤労者対象・DFFT 編



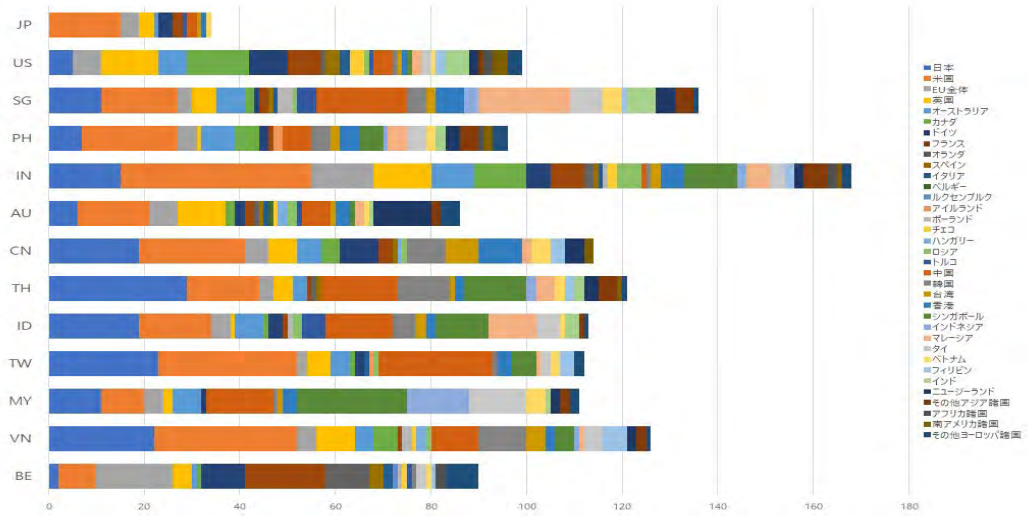
図表 2-3-112 勤労者対象・DFFT 編　関心があり、より知りたいと思う言葉



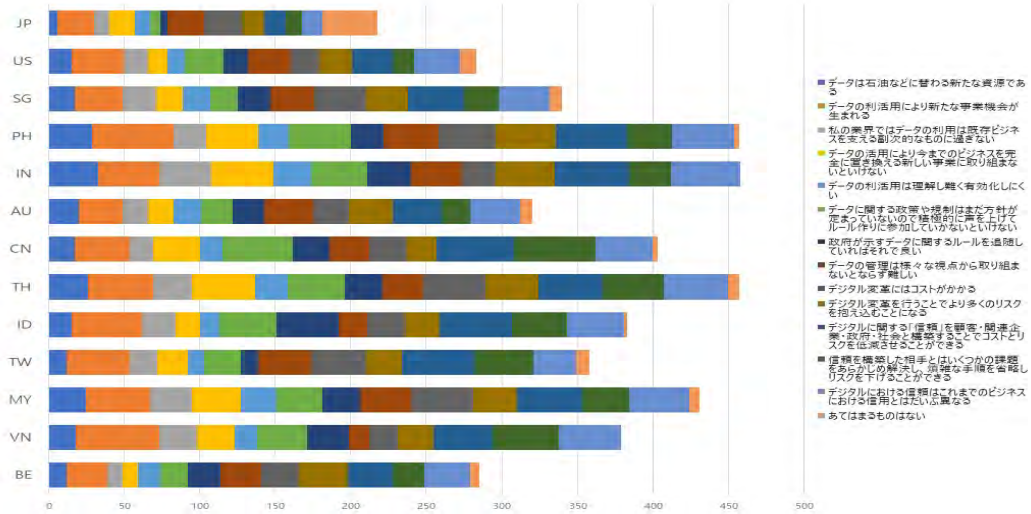
図表 2-3-113 勤労者対象・DFFT 編　業務上利用するデータの内訳（国内/国外、自社/他社）-1



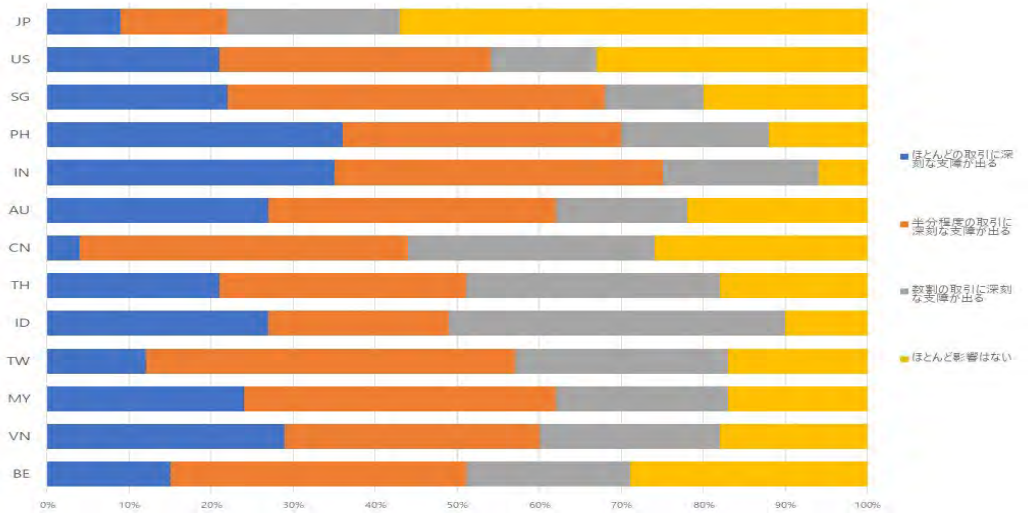
図表 2-3-114 勤労者対象・DFFT 編　業務上利用するデータの内訳（国内/国外、自社/他社）-2



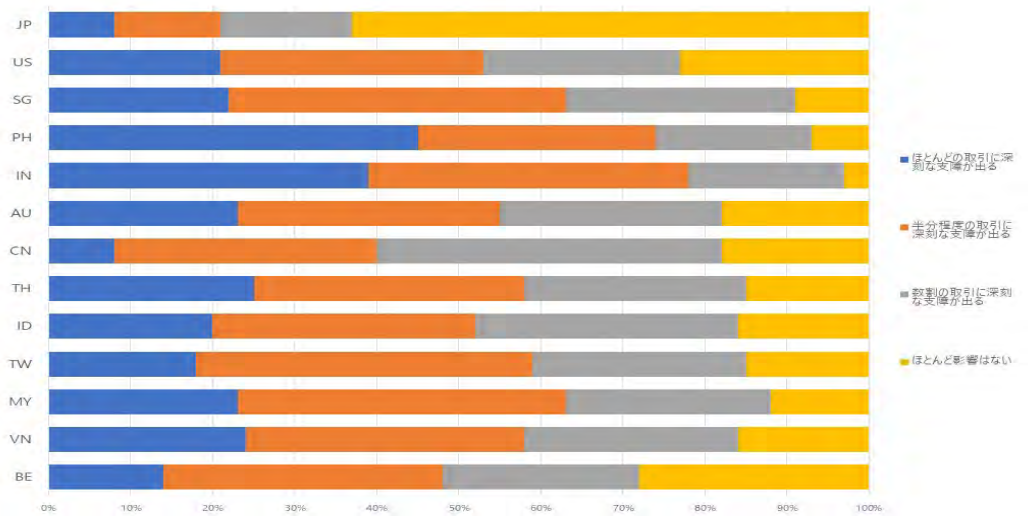
図表 2-3-115 勤労者対象・DFFT 編　業務でよくデータを移転する相手国



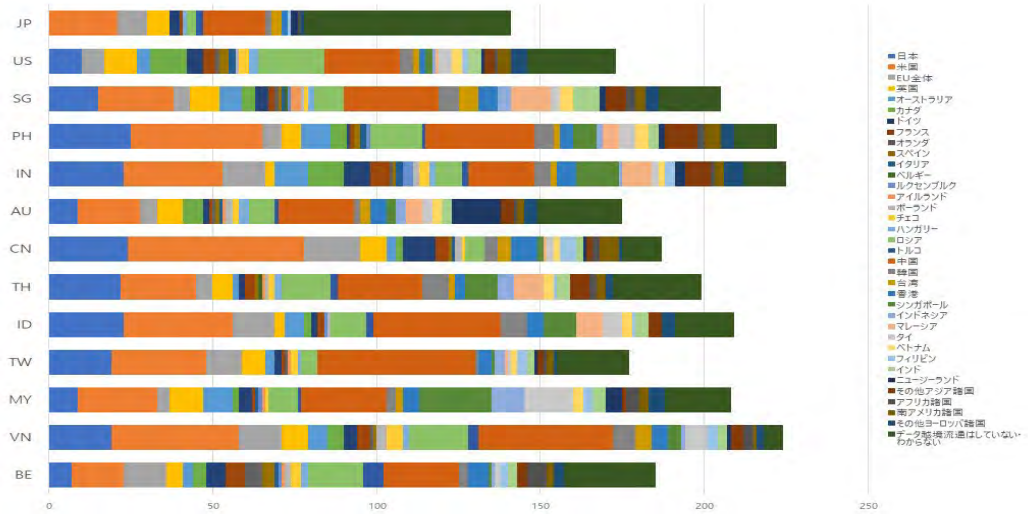
図表 2-3-116 勤労者対象・DFFT 編　越境データ流通に関する考え方



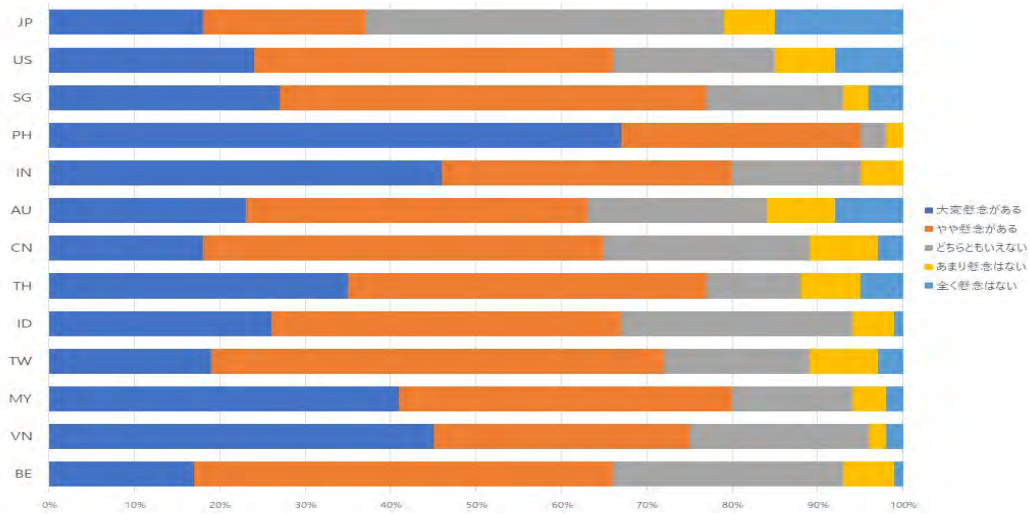
図表 2-3- 117 勤労者対象・DFFT 編　データ越境流通に過度な制限が課せられた場合のビジネスへの影響



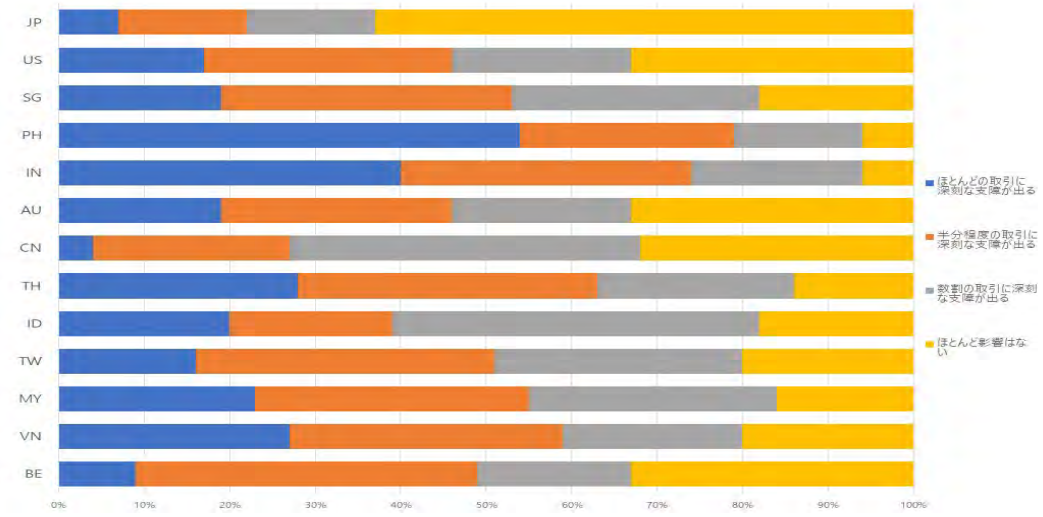
図表 2-3-118 勤労者対象・DFFT 編　取引国政府からのデータ開示要求や支配によるビジネスへの影響



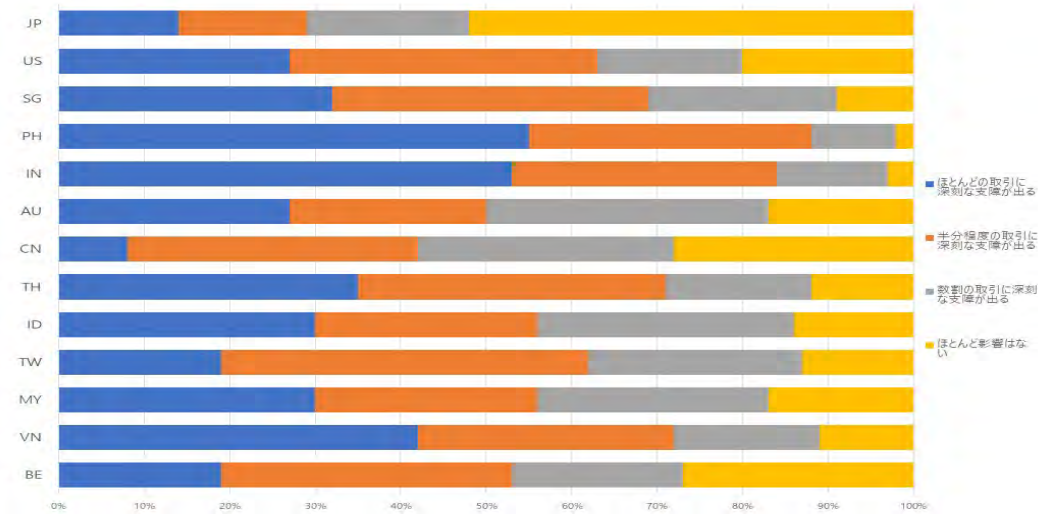
図表 2-3-119 勤労者対象・DFFT 編　越境データ流通に影響を与える規制のある国・地域



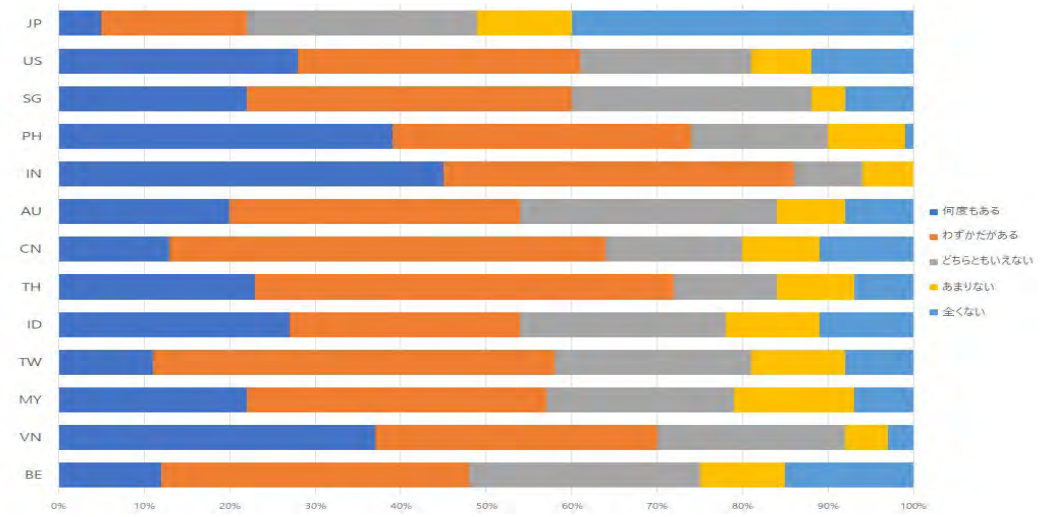
図表 2-3-120 勤労者対象・DFFT 編　法的要求で政府がデータアクセスしてくることへの懸念



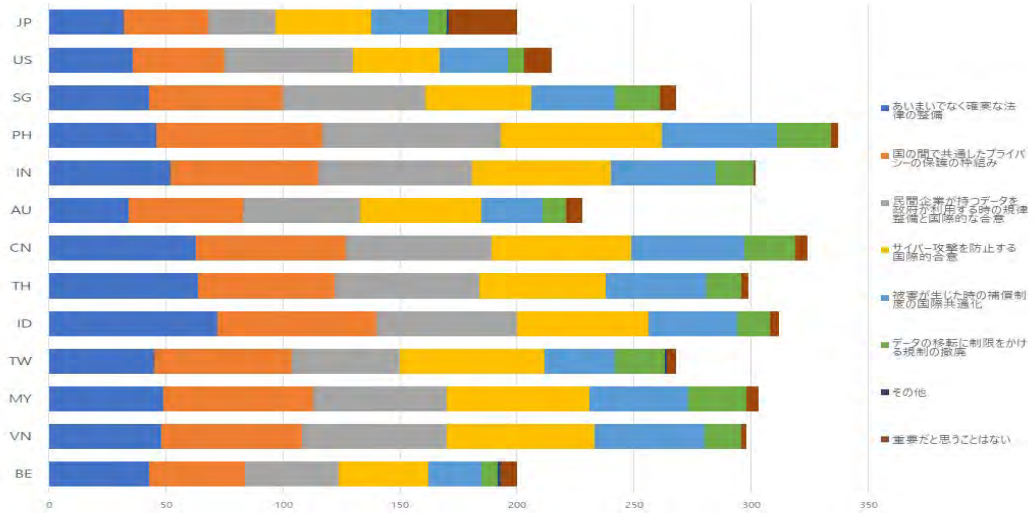
図表 2-3-121 勤労者対象・DFFT 編　政府によるアクセス可能性が国内外取引に与える影響



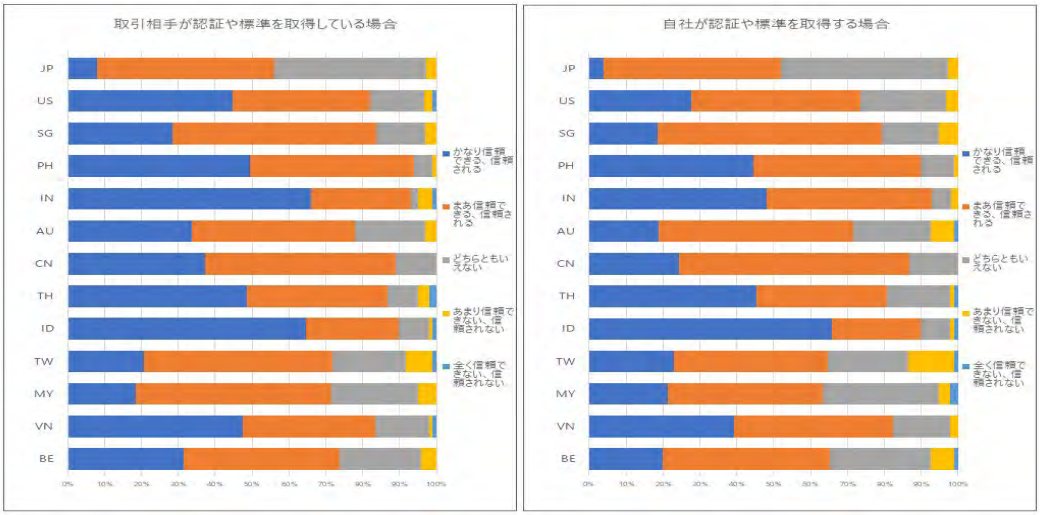
図表 2-3-122 勤労者対象・DFFT 編　サイバー攻撃で外国政府からデータアクセスされることの影響



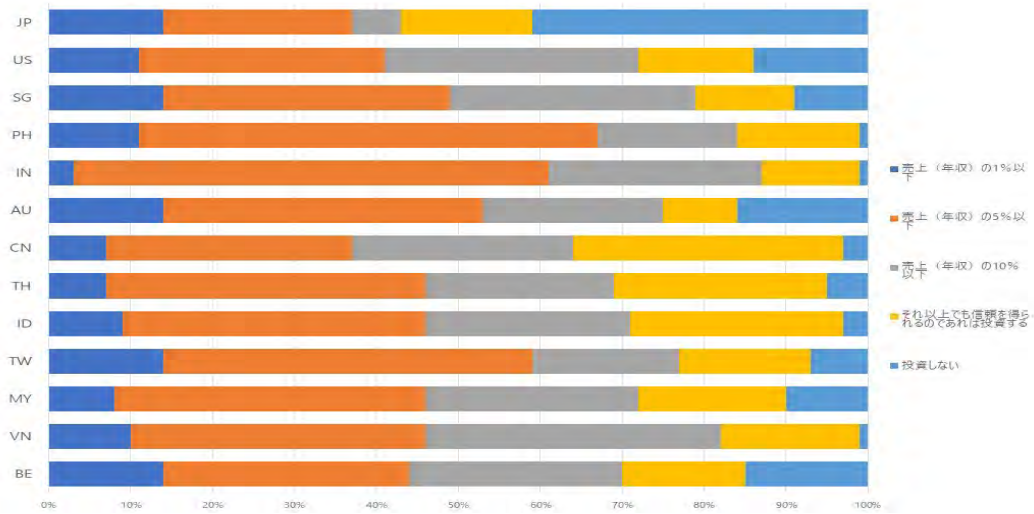
図表 2-3-123 勤労者対象・DFFT 編　政府からデータを保護するために何らか対策をした経験



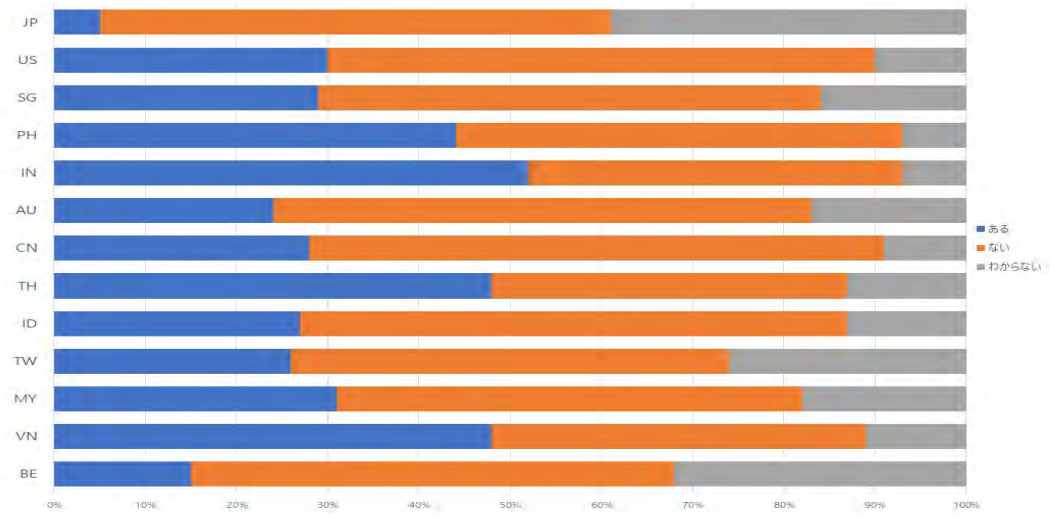
図表 2-3-124 勤労者対象・DFFT 編　信頼を高め、越境データ流通の障壁を減らすために役立つ施策



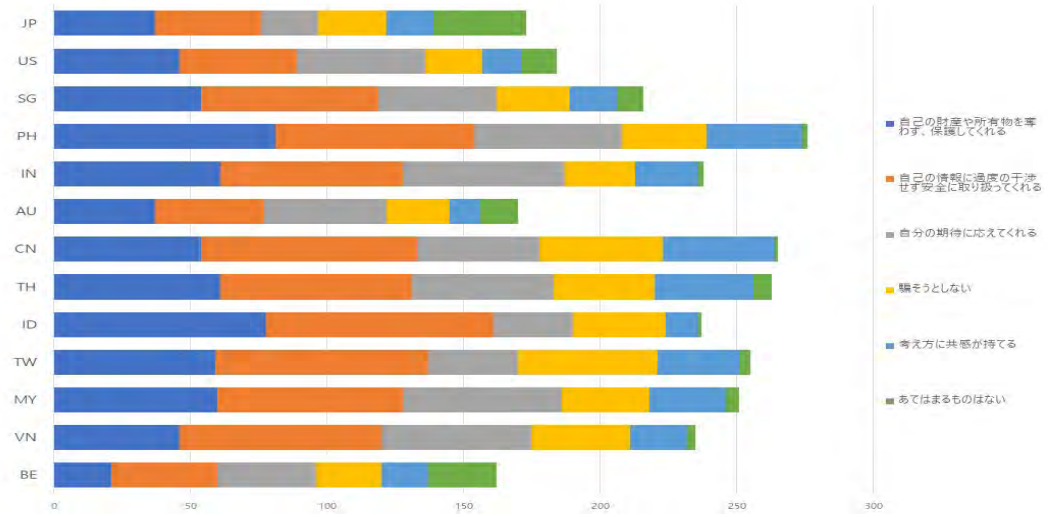
図表 2-3-125 勤労者対象・DFFT 編　取引相手や自社の信頼のため第三者認証や国際標準が役立つか



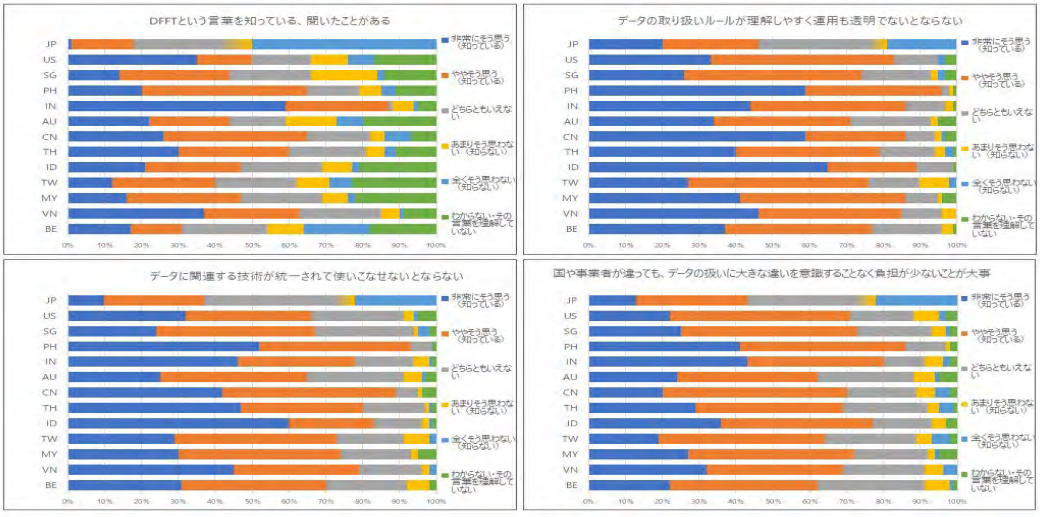
図表 2-3-126 勤労者対象・DFFT 編　顧客 1 件に対し製品やサービスの信頼を得るための投資許容額



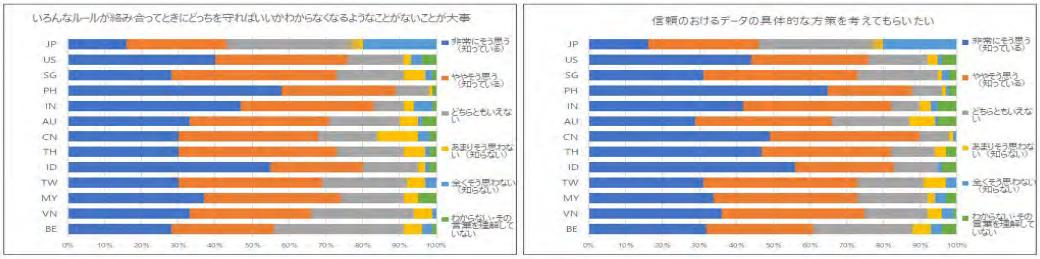
図表 2-3- 127 勤労者対象・DFFT 編　過度な規制によりその国への投資を引き揚げた経験



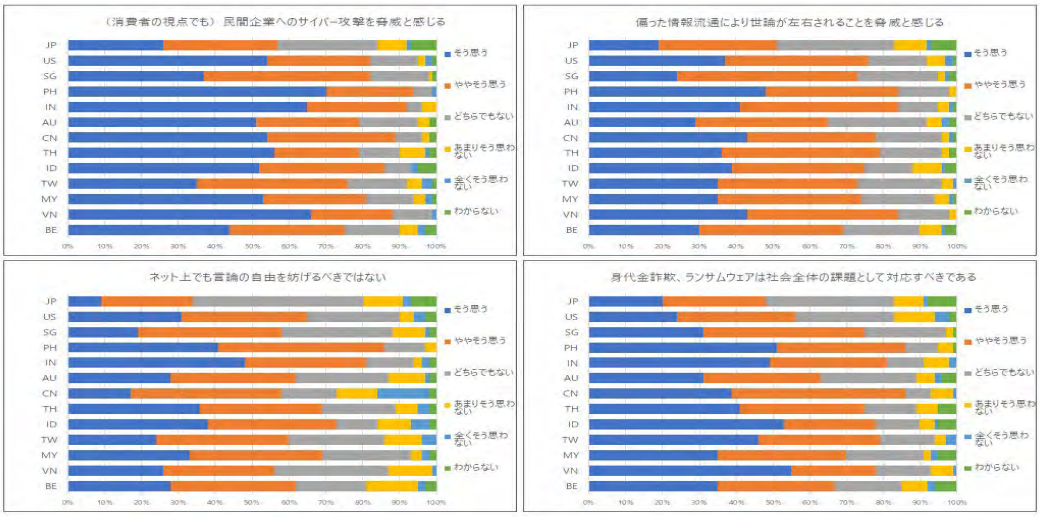
図表 2-3- 128 勤労者対象・DFFT 編　政府や企業、組織、個人を信頼するための判断材料



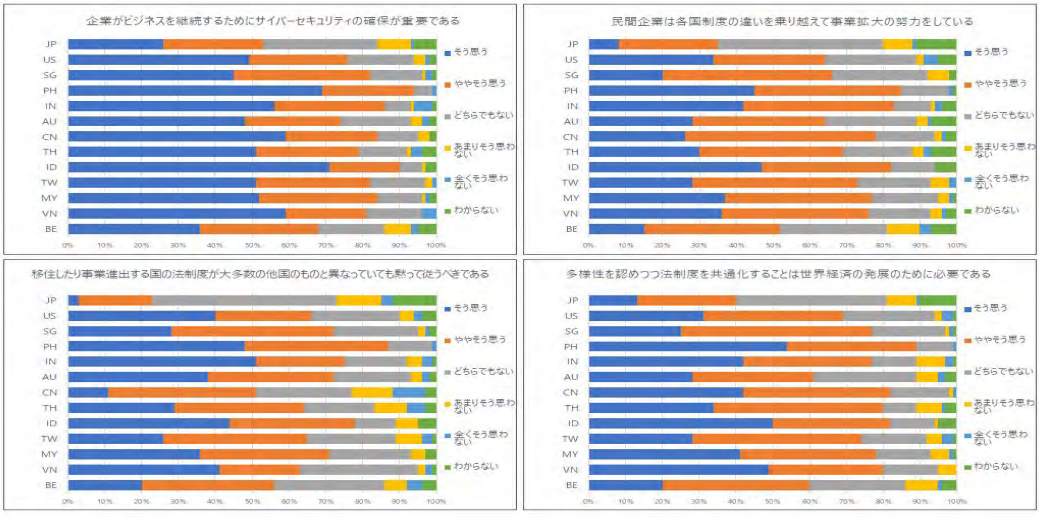
図表 2-3-129 勤労者対象・DFFT 編　データ取扱いに関する考え方-1



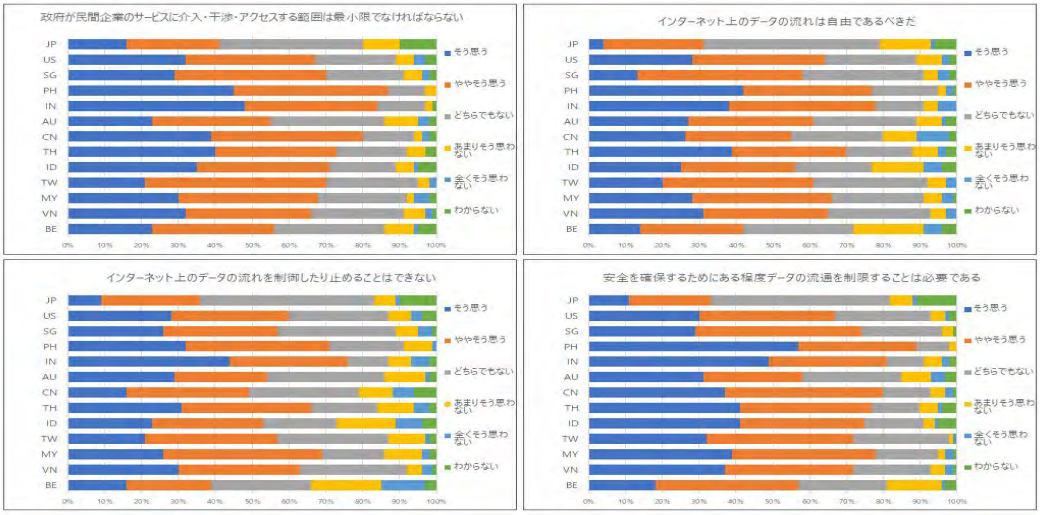
図表 2-3-130 勤労者対象・DFFT 編　データ取扱いに関する考え方-2



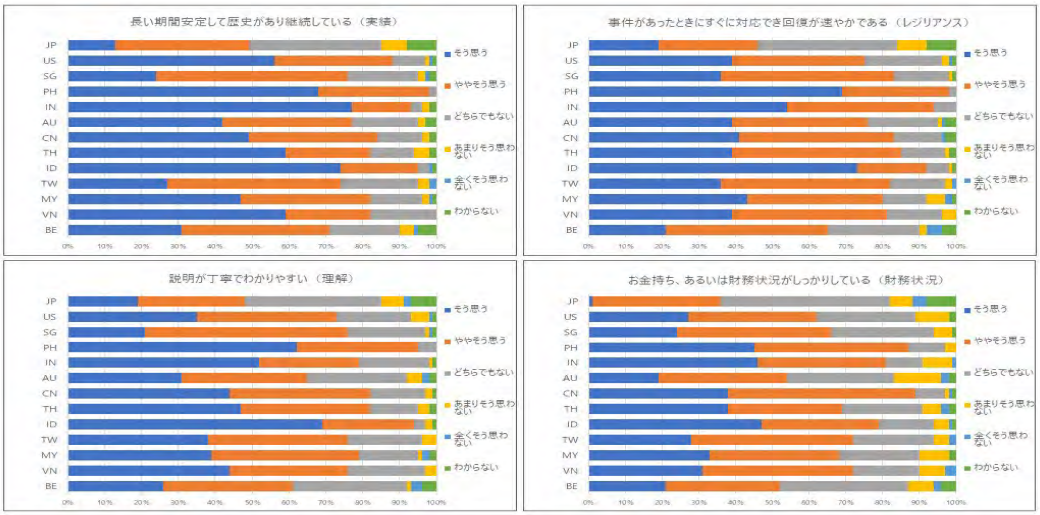
図表 2-3-131 勤労者対象・DFFT 編　時事問題についての意見-1



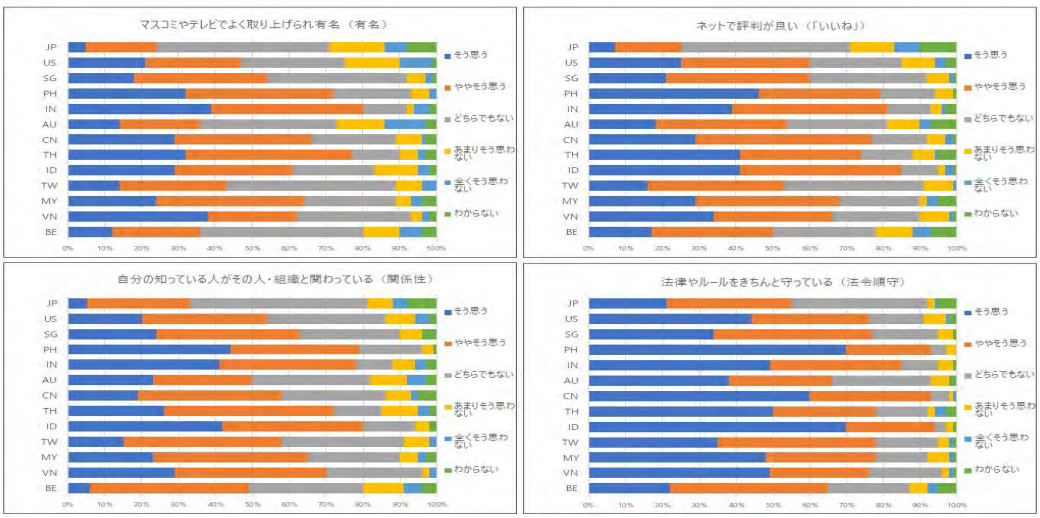
図表 2-3-132 勤労者対象・DFFT 編　時事問題についての意見-2



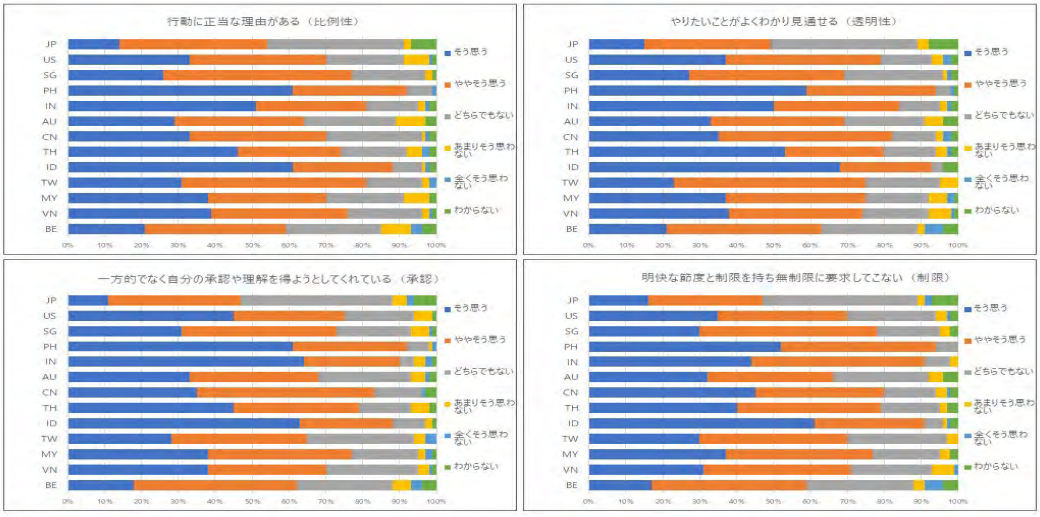
図表 2-3-133 勤労者対象・DFFT 編　時事問題についての意見-3



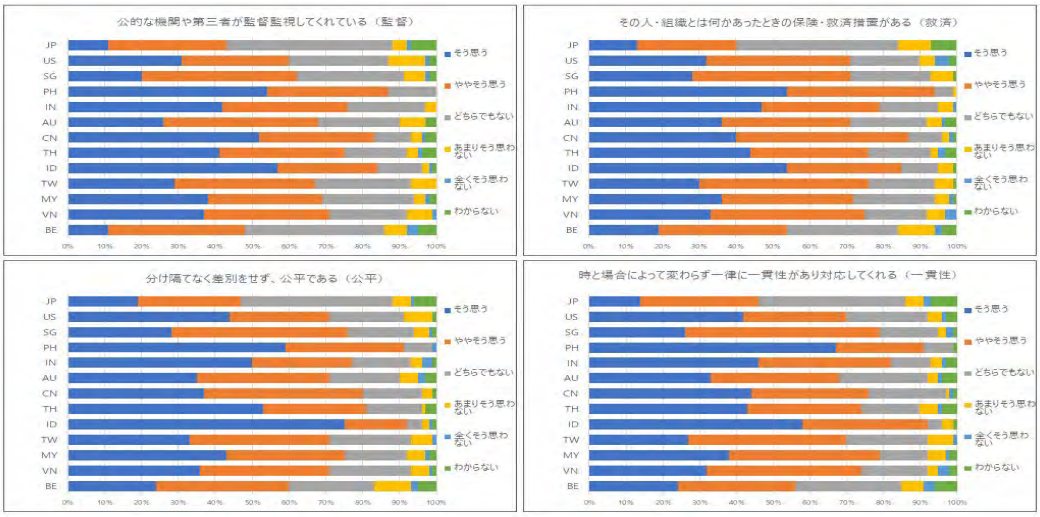
図表 2-3-134 勤労者対象・DFFT 編　相手を信頼できる理由-1



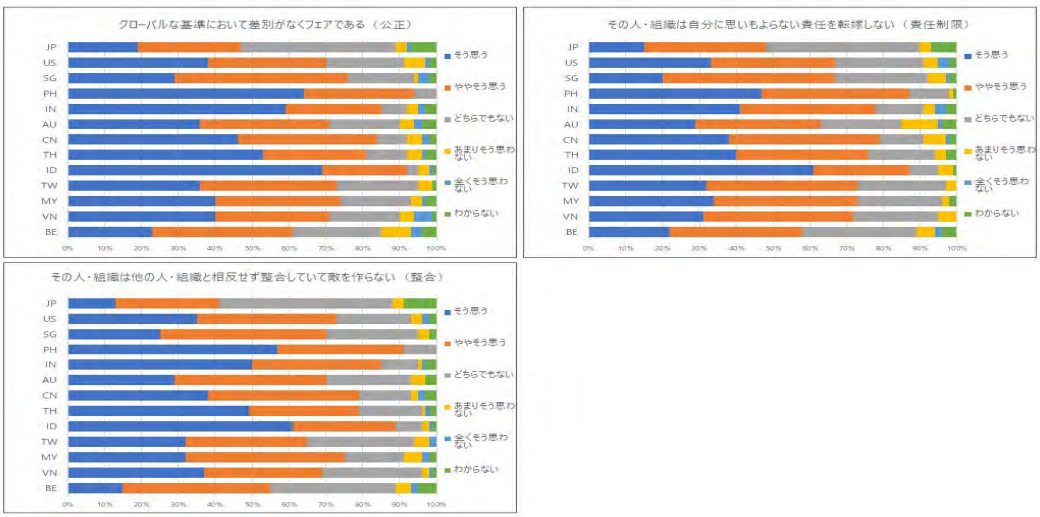
図表 2-3-135 勤労者対象・DFFT 編　相手を信頼できる理由-2



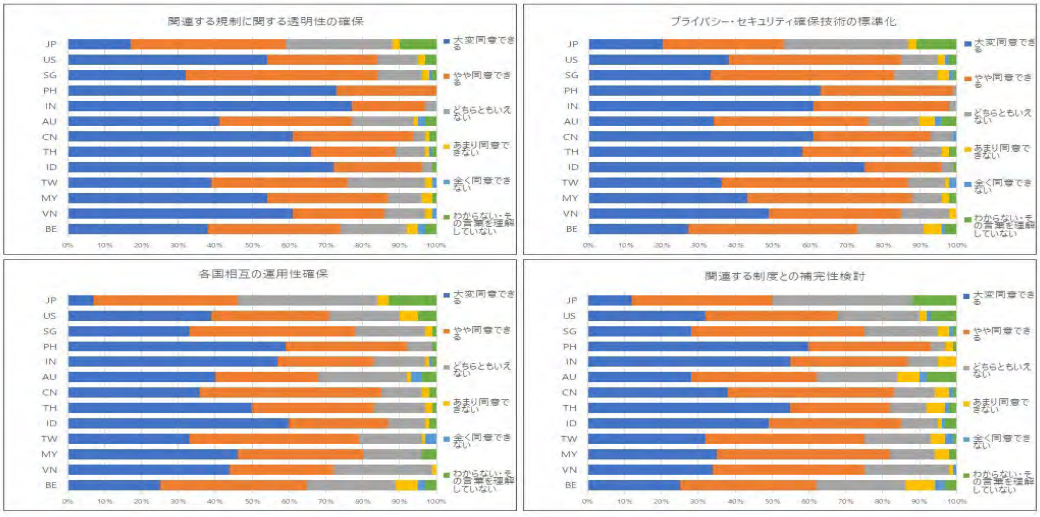
図表 2-3-136 勤労者対象・DFFT 編　相手を信頼できる理由-3



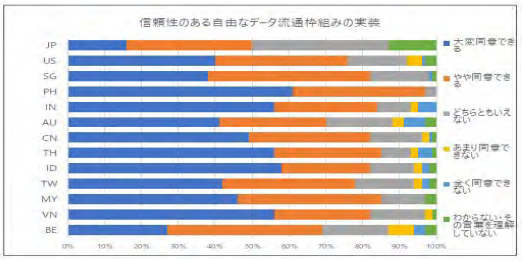
図表 2-3-137 勤労者対象・DFFT 編　相手を信頼できる理由-4



図表 2-3-138 勤労者対象・DFFT 編　相手を信頼できる理由-5

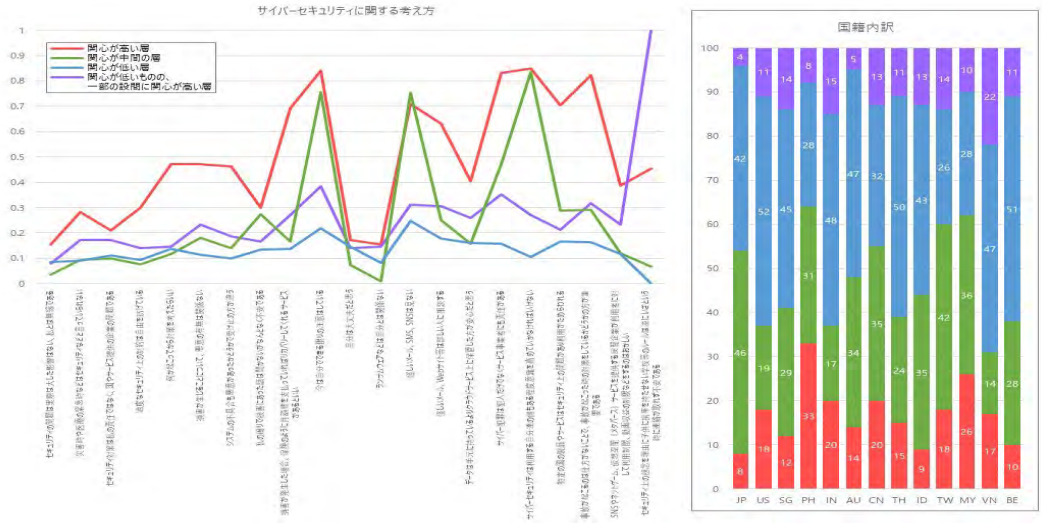


図表 2-3-139 勤労者対象・DFFT 編　信頼ある自由なデータ流通を実現するための要素-1



図表 2-3-140 勤労者対象・DFFT 編　信頼ある自由なデータ流通を実現するための要素-2

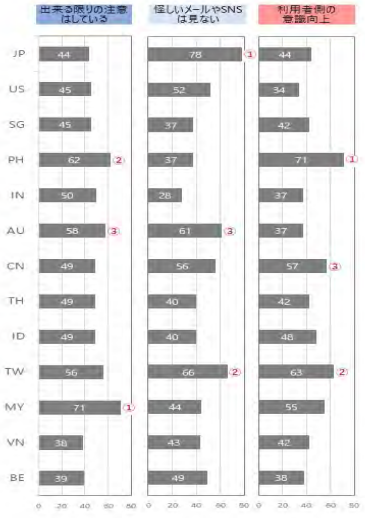
4. 調査結果（詳細分析）



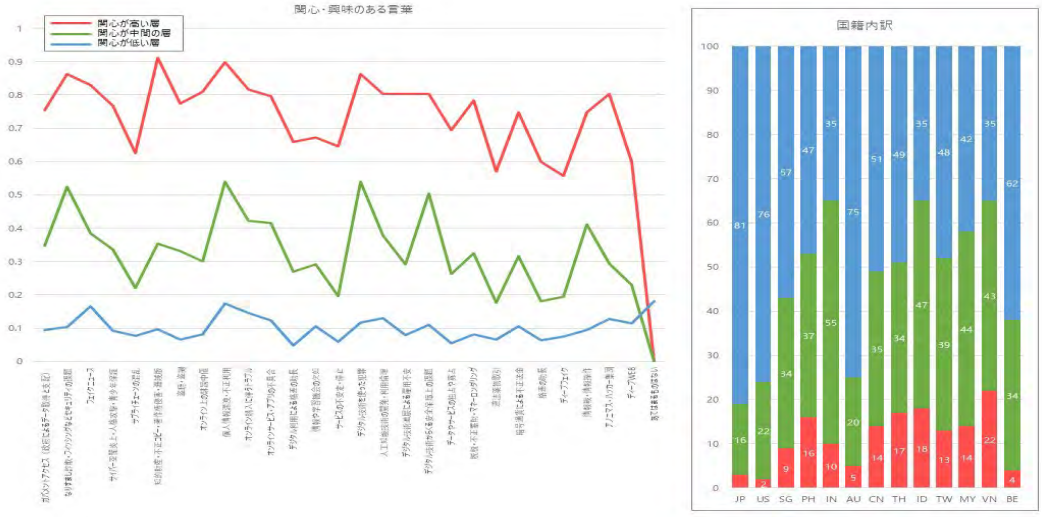
図表 2-4-1 消費者対象・セキュリティ編　サイバーセキュリティに関する考え方-1

	1位	2位	3位
JP	怪しいメールやSNSは見ない	出来る限りの注意はしている	利用者側の意識向上
US	怪しいメールやSNSは見ない	出来る限りの注意はしている	特定国のサービスは利用をため
SG	出来る限りの注意はしている	利用者側の意識向上	怪しいメールやSNSは見ない
			事故が起こるのは仕方ない
PH	利用者側の意識向上	出来る限りの注意はしている	サービス事業者側にも責任があ
IN	出来る限りの注意はしている	サービス事業者側にも責任があ	事故が起こるのは仕方ない
AU	怪しいメールやSNSは見ない	出来る限りの注意はしている	特定国のサービスは利用をため
CN	利用者側の意識向上	怪しいメールやSNSは見ない	出来る限りの注意はしている
TH	出来る限りの注意はしている	サービス事業者側にも責任があ	利用者側の意識向上
ID	出来る限りの注意はしている	利用者側の意識向上	怪しいメールやSNSは見ない
			悪意の有無は関係ない
TW	怪しいメールやSNSは見ない	利用者側の意識向上	出来る限りの注意はしている
MY	出来る限りの注意はしている	利用者側の意識向上	事故が起こるのは仕方ない
VN	怪しいメールやSNSは見ない	利用者側の意識向上	詳しい人に相談する
BE	怪しいメールやSNSは見ない	出来る限りの注意はしている	利用者側の意識向上
ALL	出来る限りの注意はしている	怪しいメールやSNSは見ない	利用者側の意識向上

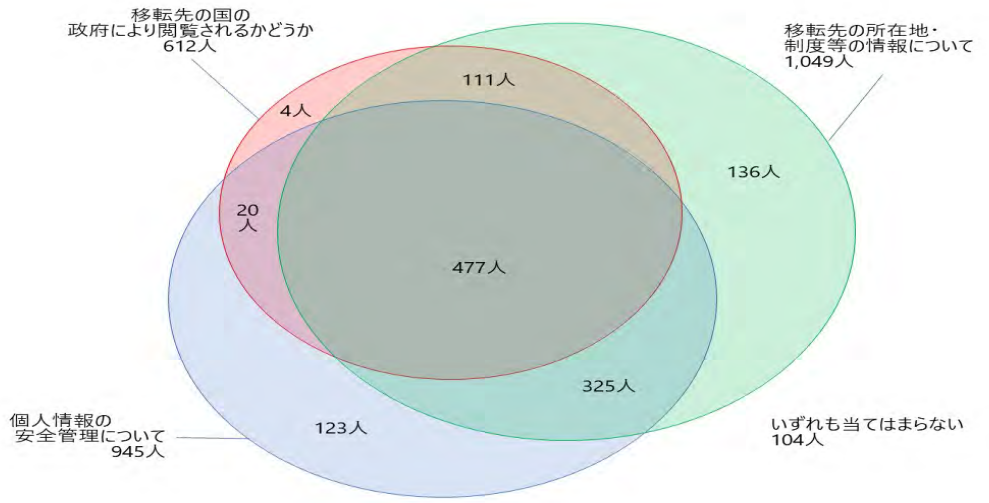
サイバーセキュリティは利用する自分達の側もある程度意識を高めていかなければいけない
事故が起こるのは仕方がないことで、事故が起こった時の対策をしているかどうかの方が重要である
今は自分でできる限りの注意はしている
怪しいメール、SMS、SNSは見ない
怪しいメール、Webサイト等は詳しい人に相談する
損害が生じることについて、悪意の有無は関係ない
サイバー犯罪は犯人だけでなくサービス事業者にも責任がある
特定の国の製品やサービスはセキュリティ上の問題があり利用がためらわれる



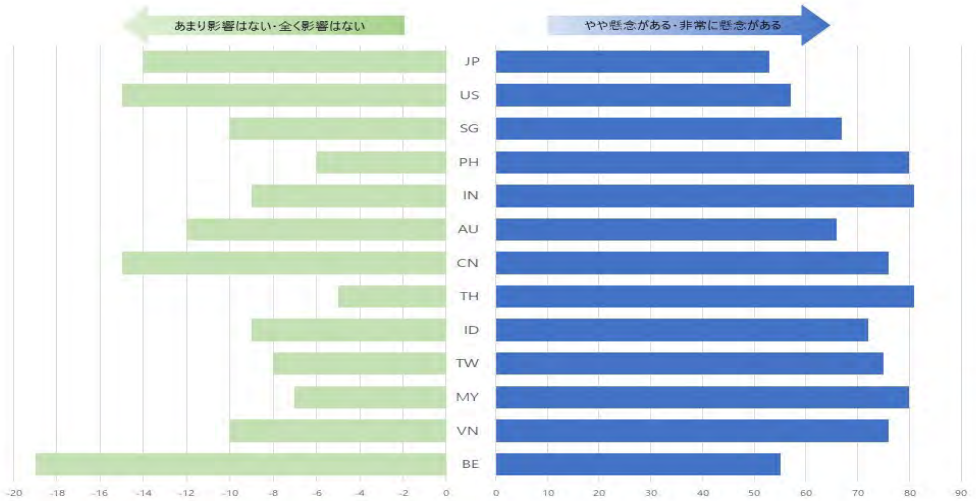
図表 2-4-2 消費者対象・セキュリティ編　サイバーセキュリティに関する考え方-2



図表 2-4-3 消費者対象・DFFT 編　関心があり、より多く知りたいと思う言葉



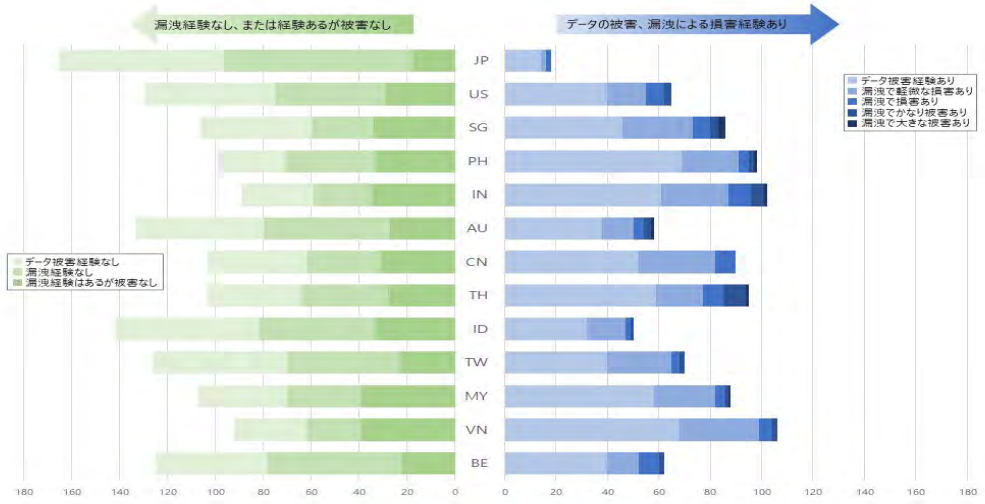
図表 2-4-4 消費者対象・DFFT 編　データの提供先について関心のあること



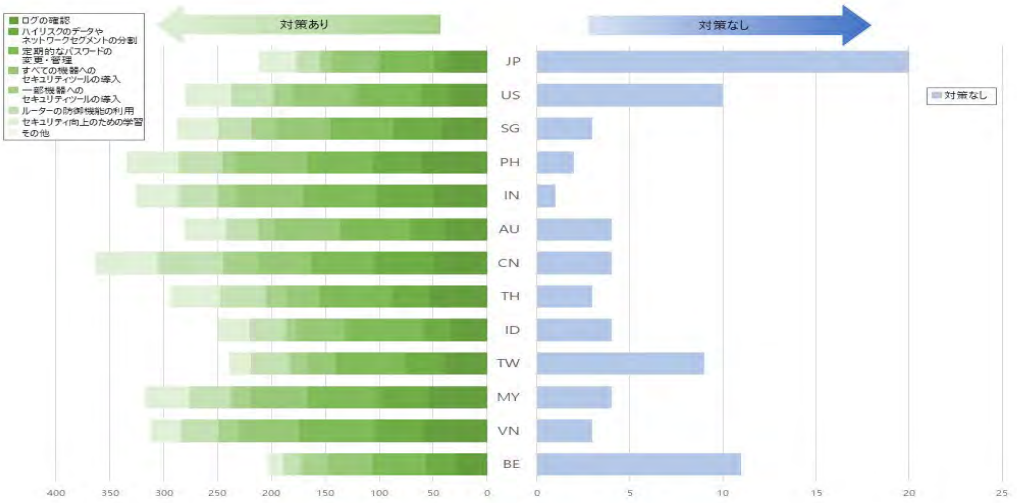
図表 2-4-5 消費者対象・DFFT 編　政府によるデータアクセスの影響

	1位	2位	3位
JP	サイバー攻撃防止に関する合意	あいまいでない法律の整備	共通した枠組み
US	GAに関する規律と合意	共通した枠組み	サイバー攻撃防止に関する合意
SG	共通した枠組み	サイバー攻撃防止に関する合意	GAに関する規律と合意
PH	サイバー攻撃防止に関する合意	共通した枠組み	GAに関する規律と合意
IN	GAに関する規律と合意	共通した枠組み	あいまいでない法律の整備
AU	サイバー攻撃防止に関する合意	共通した枠組み	GAに関する規律と合意
CN	あいまいでない法律の整備	共通した枠組み	GAに関する規律と合意
TH	GAに関する規律と合意	共通した枠組み	あいまいでない法律の整備
ID	あいまいでない法律の整備	共通した枠組み	サイバー攻撃防止に関する合意
TW	共通した枠組み	サイバー攻撃防止に関する合意	あいまいでない法律の整備
MY	共通した枠組み	サイバー攻撃防止に関する合意	あいまいでない法律の整備
VN	共通した枠組み	GAに関する規律と合意	サイバー攻撃防止に関する合意 保証制度の国際共通化
BE	サイバー攻撃防止に関する合意	あいまいでない法律の整備	共通した枠組み GAに関する規律と合意
ALL	共通した枠組み	サイバー攻撃防止に関する合意	GAに関する規律と合意

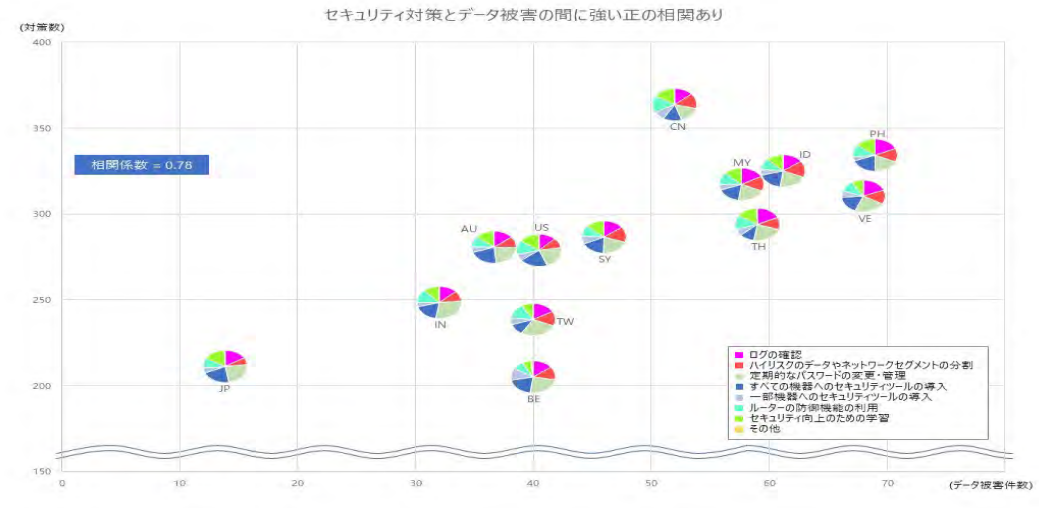
図表 2-4-6 消費者対象・DFFT 編　信頼を高め、越境データ流通の障壁を減らすために役立つ施策



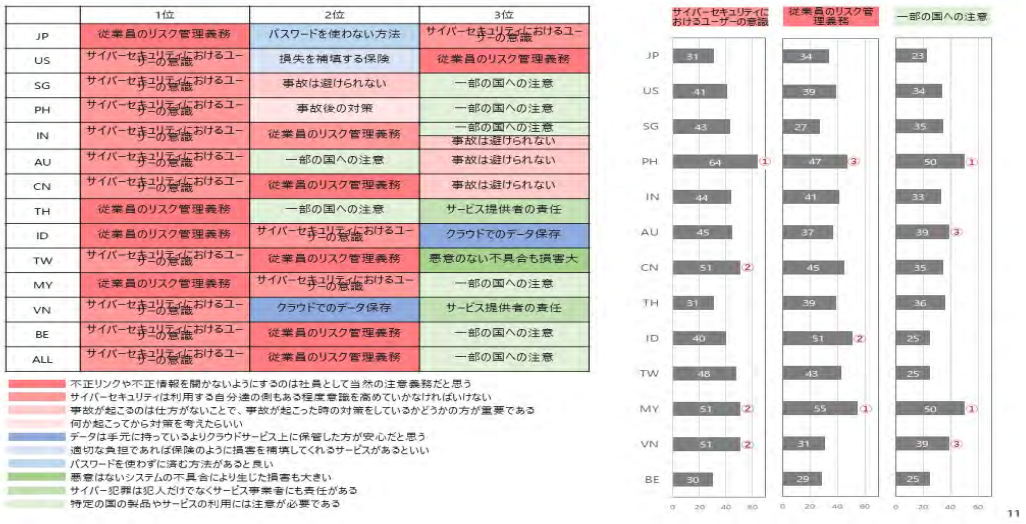
図表 2-4-7 勤労者対象・セキュリティ編　データ被害・個人情報漏洩の経験



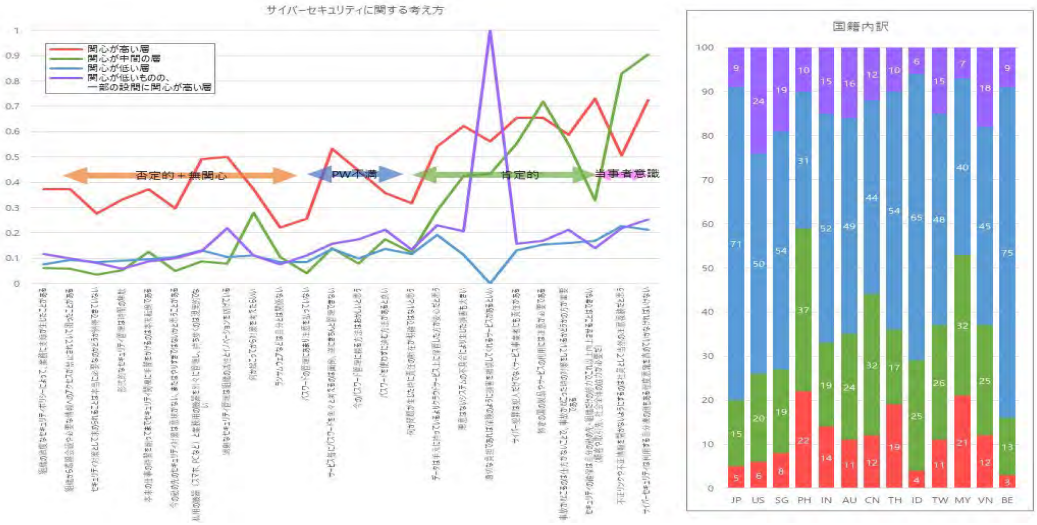
図表 2-4-8 勤労者対象・セキュリティ編　実施しているセキュリティ対策



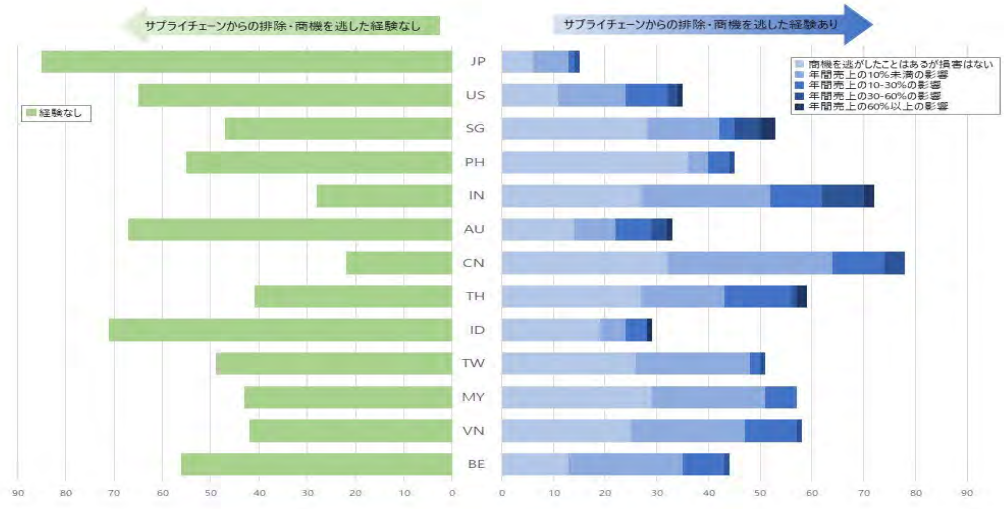
図表 2-4-9 勤労者対象・セキュリティ編　セキュリティ対策とデータ被害の関係性



図表 2-4-10 勤労者対象・セキュリティ編　サイバーセキュリティに関する考え方-1



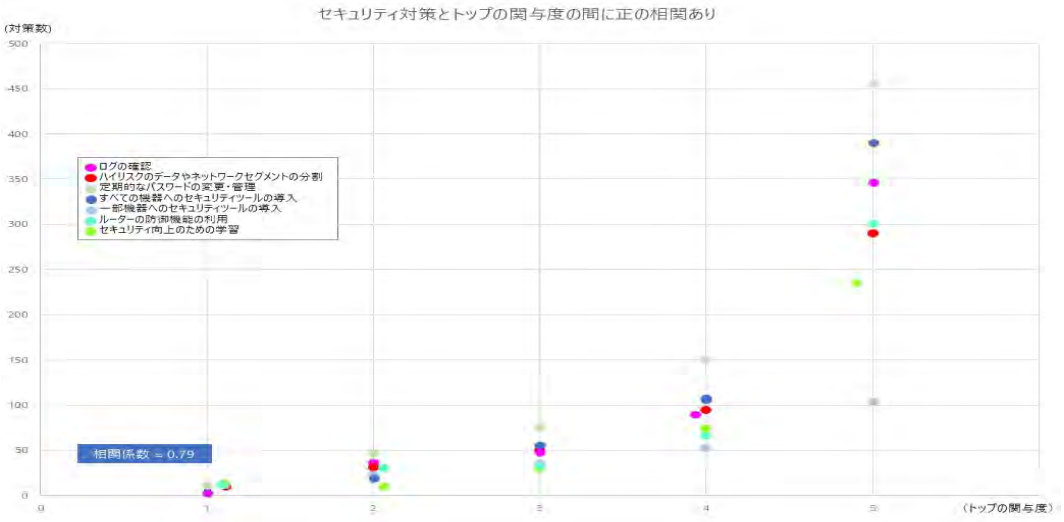
図表 2-4-11 勤労者対象・セキュリティ編　サイバーセキュリティに関する考え方-2



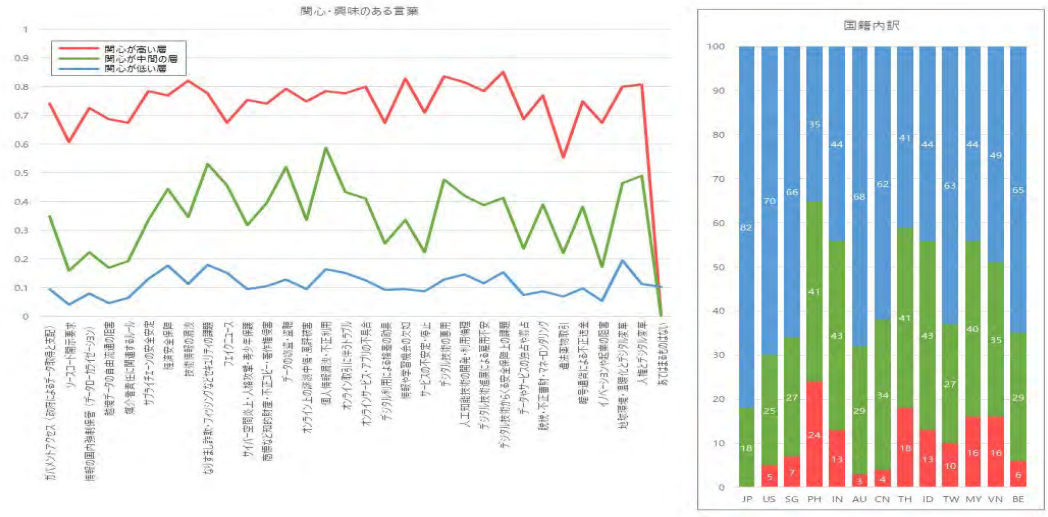
図表 2-4-12 勤労者対象・セキュリティ編　サプライチェーンからの排除経験

	1位	2位	3位
JP	セキュリティ民間企業	職場の情報システム担当部署	通信サービス提供事業者
US	職場の情報システム担当部署	セキュリティ民間企業	政府
SG	職場の情報システム担当部署	政府の認証する公的機関	政府
PH	職場の情報システム担当部署	セキュリティ民間企業	政府の認証する公的機関
IN	職場の情報システム担当部署	政府	政府の認証する公的機関
AU	職場の情報システム担当部署	政府	政府の認証する公的機関
CN	政府	政府の認証する公的機関	職場の情報システム担当部署
TH	職場の情報システム担当部署	セキュリティ民間企業	政府
ID	職場の情報システム担当部署	政府	職場の所属部署
TW	政府の認証する公的機関	職場の情報システム担当部署	セキュリティ民間企業
MY	職場の情報システム担当部署	政府	セキュリティ民間企業
VN	政府の認証する公的機関	職場の情報システム担当部署	政府
BE	職場の情報システム担当部署	政府の認証する公的機関	政府
ALL	職場の情報システム担当部署	政府の認証する公的機関	政府

図表 2-4-13 勤労者対象・セキュリティ編　組織、業務を守るために信頼し助力を期待できる相手



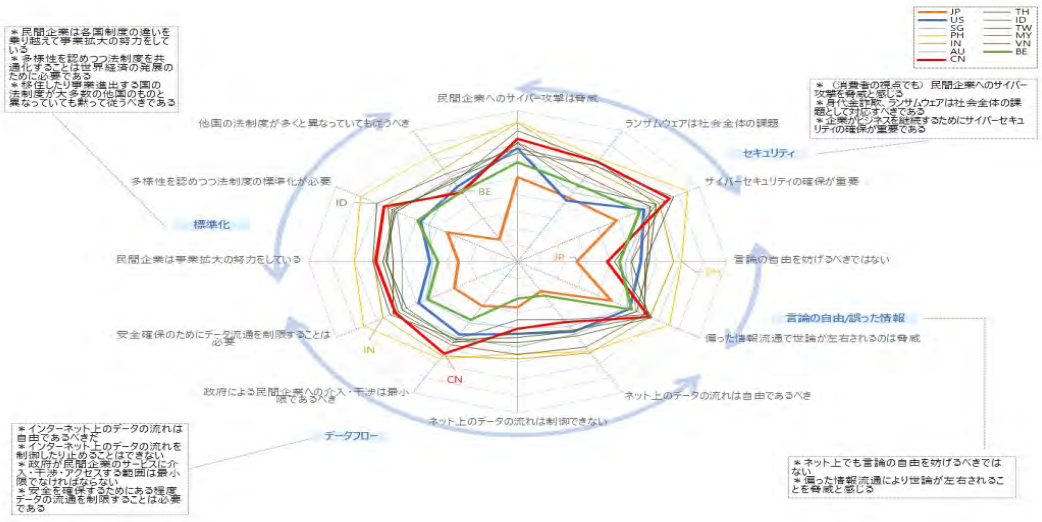
図表 2-4-14 勤労者対象・セキュリティ編　セキュリティ対策とトップの関与度



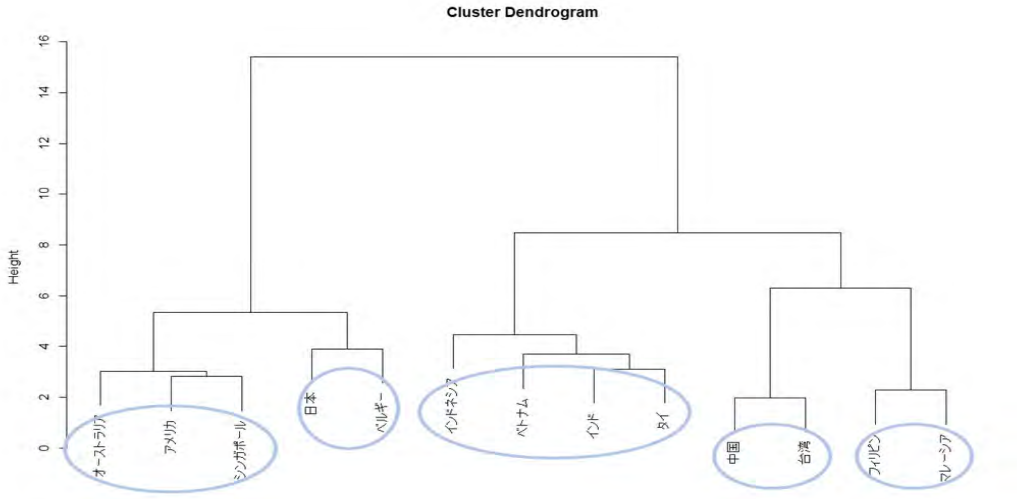
図表 2-4-15 勤労者対象・DFFT 編　関心があり、より多く知りたいと思う言葉

図表 2-4-16 勤労者対象・DFFT 編　越境データ流通に関する考え方

図表 2-4-17 勤労者対象・DFFT 編　信頼を高め、越境データ流通の障壁を減らすために役立つ施策



図表 2-4-18 勤労者対象・DFFT 編　時事問題に対する意見



図表 2-4-19 多変量解析による各国の傾向

第2章　インタビュー調査

1. 調査概要

■調査対象国
日本、アメリカ、インド、オーストラリア、中国、オランダ　（合計 6 か国）

■調査方法
インタビュワーによる個別オンライン実施（zoom を利用）

■調査期間
2022 年 9 月 7 日（水）～11 月 1 日（火）

■回答者数
各国 IT セントリック企業における経営者層（CEO 等）、組織戦略立案者（CIO、CSO 等）を中心に 8 名から回答を得た。回答者の概要は以下の通り。
・日本：金融企業 CDO
・アメリカ：セキュリティコンサル企業 創業者 CEO、国際的コンプライアンス支援企業 創業者オーナー、新興高級バーボンメーカー 創業者 CEO（合計 3 名）
・インド：ネットワークおよびセキュリティサービス企業 創業者 CDO
・オーストラリア：国際協力コンサル企業 シニアシステムアドバイザ（保険分野）
・中国：ソフト開発企業 支社理事長
・オランダ：健康分野デジタルソリューション企業 創業者 CEO

■設問内容
サイバーセキュリティへの取組みや状況、DFFT・ガバメントアクセスの影響等、あらかじめ準備した設問を中心に、回答者の関心に応じて自由に回答いただいた。

2. 質問票

(1) 企業情報

業種/規模（売上、従業員数）/海外子会社・事務所など国際展開の有無/国際ビジネスの有無/回答者の簡単な経歴

(2) サイバーセキュリティについて

Q1. あなたの会社では、サイバーセキュリティや情報セキュリティにどのように取り組んでいますか？

（例）

・なぜ、取り組んでいますか？

・何を脅威・リスクと考えていますか？

・どのような取組みですか？どのような対策ですか？

・セキュリティ対策費用（投資額）はどのくらいですか？（IT 予算の何%？売上の何%？）

・いつ頃から取り組み始めましたか？

Q2. 体制はどうされていますか？

・CISO は設置されていますか？　どのような権限があり、どのような役割を果たしていますか？何を期待していますか？

・CISO は内部から育成しましたか？外部から採用しましたか？

・CISO は何の専門性を持っていますか？

・社内ガバナンスをどうしていますか？

Q3. 取引先からサイバーセキュリティ対策を求められたことはありますか？調達先にサイバーセキュリティ対策を求めたことはありますか？

Q4. 課題は何ですか？

Q5. セキュリティに対する意見をご自由にお話しください。

（例）

・ユーザー企業だけでは防げない

・政策に期待すること

・ベンダーの責任をどう考えるか

(3) DFFT・GA について

Q1. あなたの会社は、デジタル経済、デジタルトランスフォーメーションと言われるビジネスをどのくらいやっていますか。

・インターネットを活用したビジネスなど。

・対象は国内だけか？外国市場もか？

Q2. あなたの会社は国境を越えたデータの利用をどの程度していますか？

（例）

・外国の子会社・関係会社とのやりとり

・外国の外注先、調達先とのやりとり

・外国の販売先、顧客管理とのやりとり

・外国企業との共同開発

・クラウドの利用
・Office365，Google ドライブなどの利用
・ネットを使った情報の提供
・ネットを使った個人情報の収集
・ネットを使ったその他のデータの収集、分析
・ネットを使ったサービスの提供
など
Q3. どの国が多いですか？敬遠、警戒する国はありますか？その理由は？
Q4. 国境を越えたデータ流通で困る（不安がある、注意が必要な、など）ことはありませんか？　それによるビジネスの影響どのくらいですか？（できれば金額換算　、影響を受けるビジネスの規模など）
（例）
・内外の法規制、
・データ保護（個人情報保護)、データローカリゼーション
・セキュリティ
・外国政府による情報の取得、
・外国政府による課税

(4)　その他
別途参考グラフを見て、何かコメントがあれば自由にお話しください。

3. 調査結果（個別回答内容）

（1） 日本　金融企業 CDO、直前までシリコンバレー在住でスタートアップを経営
・当社は CSRIT 設定、P マーク、ISMS 取得等、他社より進んでいる。
・リスクに対して思いがないと、認証は形骸化する。トップの perception gap が問題。
・セキュリティは攻めという意味でも当事者意識をもって取り組む。
・現在のセキュリティルールはテック側により決められていて、全産業が危うい。
・形骸化の原因：日本のトップは IT がわからないので IT 部にやらせておけばよいとなり、IT 部も専門性がないので Sier に丸投げでレガシーなまま。
・入社時、無線 LAN は NG，USB ポートは殺す、Gメールもなかなかアクセスできない、BYOD 不可等。独自ドメインなどをやり始めたら IT 企画部がセキュリティが損なわれると大反対。
・PPAP について、米データ解析企業では軍用をやっていたので、敵方からのメールも多く、暗号化されたファイル添付のメールは受信しない。MS authentication 等にもすべて対応。
・米国 TEC 企業(含む金融)は、セキュリティ含め自社開発。従業員は極端に言うと監視されている。従業員も情報の価値やリスクをよく理解し、ミスによる追求、訴追もあり、真剣。日本は危機感が不足。
・インターネット盗聴の危険について、無法地帯であるというのは正しい。最近は本当に重要なものはメールしなくなっている。

（2） アメリカ　セキュリティコンサル企業 創業者 CEO
・この数年で CEO やコミュニティのセキュリティの必要性の認識が格段に向上（Why から What と How much に）。そのきっかけは、Solar Winds 事件。サプライチェーンのハッキングにより攻撃が大規模に増加し、コミュニティの意識は非常に高まった。人々は何が起きているのか知り、この事件やコロニアルパイプライン事件など、企業の幹部の議会証言で、脅威は完全に変化したことに人々が気づいた。
・CISO の地位は上がったが、他の C 職は本業外なので後回しになる。認識ギャップを埋める必要がある。
・クラウドに任せればよいという誤解があるが、自社での運用管理も重要（認証、モニタリング機能、暗号化）。
・包括的なガバナンスが必要。合理的なセキュリティを示すのが CIS 規格や ISO 規格。
・今後は end to end の可視化が重要に。
・DFFT：多国籍企業にとって法律・体制のフラグメンテーションのため、弁護士費用など非常に負担。総予算の 5 %以上。

（3） アメリカ　国際的コンプライアンス支援企業（従業員数 6 名）創業者オーナー、7 カ国で活動
・セキュリティ対策のポイントは⑴リスク評価、⑵暗号化、⑶優れたソリューション、⑷コンプライアンス・オートメーション（GDPR 等への）。
・しかし、裁量と判断できる人間が必要。内部で作るのは難しく専門家を雇うべき。
・ソフトウェア会社であれば、SOC2 の認証を取得することが期待される。
・欧州企業の方が CCPA に慣れている。米国企業は不慣れ。
・GDPR の下で自分達を知ること。集中型の報告 NW を構築し、セキュリティインシデントと報告を一元管理することで集中監視を。
・ソーラーウィンズ事件は、攻撃者が信頼できるソフトウェアになりすましたことで最悪の事件。

・特権的アクセス者、セキュリティ技術者、CEO などがどれだけ標的になるか、事前に理解されなかった。彼らは常にセキュリティポリシーの例外を求めたり設けたりする人達。他の人と同様、セキュリティを守らせるべき。
・ベンダーの責任は、自分たちがセキュリティサービスについて、自分たちが提供するものとしないものを明確にし、顧客の義務を明確にすること。データ侵害に対するベンダーの責任は強化されるべき。
・インドは欧州に信用されるために導入した高いセキュリティ規制により地位が大きく向上。

（4） アメリカ　新興高級バーボンメーカー（従業員数 15 名）創業者 CEO、過去に大手多国籍企業でセキュリティ・プライバシー要職経験あり
・EC で富裕層個人向け販売をしている。
・個人情報は、GDPR の基本的費用便益分析を適用、米国で一般的に求められているレベル。
・システムは当初からセキュリティ専門家の友人を雇い、GDPR 準拠で洗練されたオーダーメイドソリューションで優れたデータガバナンス。セキュリティ費用は全予算の 0.5%。顧客データは他のデータから分離、分散保管、保存時も転送時も暗号化。
・近いうち、CISO as a service を検討、規模が大きくなったら採用。
・米国の普通の卸業者はプライバシーとセキュリティの重要性を理解していない。
・米国企業は一般的にセキュリティに強く、欧州、アジアではプライバシーに強い。
・高級品の顧客は中国、インド、湾岸諸国などアジアに。それぞれの国にプライバシーやセキュリティのプロトコルがあるので、分けたクラウドにせざるを得ない。
・DFFT について。オプトイン等の考えはもう古い。必要なのは企業や政府の政策が消費者の利益にも合致したデータの流れを促進するように連携するシステム。

（5） インド　ネットワークおよびセキュリティサービス企業 創業者 CDO
・クラウドの課題
・データローカロリゼーションとの両立
・遅延→エッジコンピューティングに。５G など、自動車など。
・データの外部に置くことになるので、セキュリティで多くのイノベーション。
・提供する SAS での経験
・どのようなサービスを利用しているか把握できない→エージェントソフトウエアで可視化し、アプリケーション依存関係マトリックスを作成し問題を解決
・すべての企業に重要なのはセキュリティを中心にインフラを計画すること。最後に付け足すことではない。
・EU 諸国では ISO 規格に準拠して仕事
・2019 年からインドではセキュリティを非常に重要視、新しい制約出現
・CISO への要請は？
①セキュリティガバナンス（政策立案、ポリシー。従業員の権限（ほとんどの漏えいは従業員から））
②インフラ全体の定期的分析、把握
・セキュリティ業界の大きな課題は、オープンソースの脆弱性
（6）オーストラリア　国際協力コンサル企業（4 カ国に拠点）シニアシステムアドバイザ（保険分野）
・顧客の 95%が政府機関。保健省等へのデータ・デジタルプロジェクトでサポート（主に発展途上国か）

・すべてのプロジェクトに CISO が配属。資金提供者のガバナンスを守り、コンプライアンスも確保。
・グローバルに適用可能な最も強力な法律(GDPR)を遵守。ISO の規格も利用。
・顧客(政府や医者）が医療情報なのにセキュリティが強くないツールを利用。最適でないことを教える必要。
・CISO が途上国事情を理解しないことによる問題も。
・セキュリティは継続的に更新し適応させ続ける必要。
・まずは法律。セキュリティシステムの効果測定も必要。
・(グラフを見て)インドの大きな変貌は実感。政府も DX に力を入れる。
・ベトナムも挑戦、タイもデータ活用で変貌
・米国はまだ古いテクノロジーを使用していて新しいウェブベースやクラウドベースのソリューションに移行していないが、アフリカや多くのアジアの国では新しいソリューションが出発点。
・DFFT は良いが、米国企業は無断で個人情報を売却、本人の同意が必要。信頼はデータと共に必要なテクノロジーソリューション化されるべき。

（7）中国　ソフト開発企業 支社理事長、長年日本からの受託業務に従事、東京拠点でも勤務経験あり
・ISO27001 に従って取組む。日本顧客の要請が多いので 2009 年に取得。
・教育意識向上、入退出管理、開発フロア確保、開発用 PC はインターネット接続不可、FW,ウィルス対策ソフト、ログ確認で日常検査
・当時ノウハウはなかったが、取得を契機に体制づくりをしっかりしたことが有益。
・セキュリティ予算は年間売り上げの 1%くらい
・セキュリティは日本からの受注要件だが、中国企業は、金融・通信以外は厳しくない
・課題は、各企業からの要求が違うこと。過度なもの、形式的なところもあり、コストや効率とのバランスが必要と考える。
・PPAP は顧客からの要請でやっている。やめてくれとは言われていない。
・社内で一般的に使用する製品は中国製だが、日本顧客からの仕事は指定あり。
・DFFT について、国の間で共通したプライバシー保護の枠組みがあれば有難い

（8） オランダ　健康分野デジタルソリューション企業（従業員数 13 名）創業者 CEO
・主に発展途上国の健康分野プロジェクトに参加。
・Universal Health Coverage(UHC)をテクノロジーによって実現
・発展途上国では、セキュリティ・プライバシーへの関心低い。EU,US の若者も同様。
・しかし、同社提供のシステムは、セキュリティアーキテクチャーの青写真を持っており、発展フェーズごとに提供（必要性を理解し始めるのは 3 年から 5 年後）
・蘭を拠点とする集中管理型システムを標準にするが、ローカリゼーション要請は国によって違う。
・ケニアは国内保管、ギニアは電力不足なので蘭保管を希望
・セキュリティ面から避けている国はアメリカ。NW 層の上位にいるから。
・(グラフを見て)第 4 次産業革命、ビジネスモデルの変革：中国も多少の変化、タイが UHC 最良。インドがモバイルと 5 G で大きな転換。アフリカや他の発展途上国からある種のリープフロッグが起こり始めている。自社もランサムウェアの被害に。二段階認証などセキュリティ強化。