「ICTサイバーセキュリティ総合対策2022」（案）に対して提出された意見及び その意見に対するサイバーセキュリティタスクフォースの考え方（案）

■意見募集期間　：　令和４年６月17日（金）～同年７月16日（土）

■意見提出件数　：　11件（法人・団体：２件、個人：9件）

■意見提出者

	意見提出者
1	KDDI株式会社
2	楽天モバイル株式会社
ー	個人（9件）

※頂いた御意見につきましては、原文を御意見ごとに分割して記載しております（ただし、本総合対策（案）と無関係と判断されるものは除いております）

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
1	個人Ｄ	Ⅰ-2.	2020年下半期から2021年下半期にかけてのランサムウェア被害の報告件数や2021年７月から 2022 年５月のフィッシング報告件数がそれぞれ約４倍、約 2.5 倍に増加しており ↓ これだと「2020年下半期から2021年下半期にかけてのランサムウェア被害の報告件数」がそれ以前に比べると4倍に増加しているように捉えられてしまう（フィッシング報告件数についても同様）。 ↓ 2020年下半期から2021年下半期にかけて、ランサムウェア被害の報告件数が、2021年７月から 2022 年５月にかけて、フィッシング報告件数が、それぞれ約４倍、約 2.5 倍に増加しており あるいは 2021年下半期のランサムウェア被害の報告件数や2022 年５月のフィッシング報告件数が、それぞれ2020年下半期に比べて約４倍、2021年７月に比べて約 2.5 倍に増加しており とした方がよい	御指摘を踏まえ、「2021年下半期のランサムウェア被害の報告件数は、2020年下半期に比べて約４倍、2022 年５月のフィッシング報告件数は、2021年７月に比べて約 2.5 倍に増加しており」といたします。
2	個人J	Ⅱ-1.	・要旨（1000字を越えるため） 国は、ISPやVNEに協力を求めて、ISPやVNEにおいて、基本としてTCP通信がSPI（ステートフルパケットインスペクション）フィルタにより外部の攻撃から保護が可能になるようにされたい。 ・内容全体 全般的に非常に広範に効果を発揮するので、ほとんど全てに通じる事として「１．情報通信ネットワークの安全性・信頼性の確保」を対象に意見を行うのであるが、国は、例えそれが日本においての独特の対策となるとしても、ISPやVNEに協力を求めて、ISPやVNEにおいて、基本として（利用者通信の）TCP通信がSPI（ステートフルパケットインスペクション）フィルタにより外部の攻撃から保護が可能になるようにされたい。 要するに、電気通信利用者によるインターネットとの通信においてSPIファイアウォールが基本として自動的に有効（利用者による解除は可）になるようにせよ、という事であるが、これは廉価ながら非常に強力に効くと思われるので、是非とも実現を行っていただきたい。 （なお、C&Cサーバ、DRDoS他各種DoS攻撃やPC・スマートフォンへのハッキングなども非常に強力に抑えられる事になるはずである。TELNETもSSHも（利用者が望まなければ）SPIにより外部からの接続がブロックされるとなると、攻撃側によるTCPを利用した攻撃などが、全く、といったレベルで行えなくなるので、これは非常に有効に機能するはずであると考える。） （なお、自宅でサーバを運用したい、といった人間は、多少なりとも技術について知っているのが通常であるし、SPIフィルタが外せる事の案内をしておけばそれらに対しての悪影響は無いはずであろう。（可能であればポート限定でのSPIフィルタの解除機能もあると更に良いが（そうすると素のFTP（今日ではあまり推奨されないが）などを使う場合に便利と思われる。）、それは事業者による努力目標的なもので良いと考える。（なお、設定がある程度の規模までであれば事業者においてそれなりに運用は可能ではないかと思われる。）））） （なお、SPIフィルタのために通信速度が若干低下するかもしれないが、全体の通信レイテンシからすると影響は相対的に低いのが通常と思われるので、特に問題無いと考える。いざとなったらSPIフィルタの解除（処理のバイパス）も行えるとすれば更に問題は少ないと思われる。） （なお、加えて言っておくと、行政等によるDoS攻撃への対応を名目あるいは口実とした通信制限が行われるよりも、SPIフィルタでTCP経由のアタックの多く（おそらくほとんど。）を防いだ方が（又、外部からのTCP経由のアタックを防ぐ事により問題分析対象を大幅に小規模化させて対応を容易にして当該問題の注意喚起及び場合により緊急の強制的な対応を行う方が）、スマートであるし国民・市民・事業者の権利侵害事態（※場合により生活の安全等も関係する事に注意されたい。）が少なくて済むと考える。常識的に考えると恒常的にこちらの方が良い案と思われるので、通信制限を実行していくよりもISPやVNEでSPIフィルタをかけるようにされたい。きっと見違える様な状況になるはずである。）	御指摘の SPI 技術のようにヘッダ以外の情報を利用者の同意なく活用することについては、通信の秘密との関係で慎重な検討が必要であると考えます。
3	KDDI株式会社	Ⅱ-1.-(1)-ア.	サイバー攻撃への予防的対処を可能とするため、C&Cサーバ検知技術における検知精度の向上は、対処の効果をあげるために非常に重要と考えます。22年度の実証の結果を踏まえ、検知技術の高度化のための実証を引き続き継続することに賛同いたします。	賛同の御意見として承ります。
4	個人Ｄ	Ⅱ-1.-(1)-ア.	(1)平時におけるフロー情報の収集・蓄積・分析による C&C サーバである可能性が高い機器の検知については正当業務行為、(2)フロー情報を収集・蓄積・分析して検知した C&C サーバに関する情報の共有については通信の秘密の保護規定に直ちに抵触するとまではいえないとの整理 ↓ 元資料においてもタイトルが同じ問題を抱えているため仕方がないが、係り受けの問題で文意が曖昧・複雑になっている。 ↓ (1)平時にフロー情報を収集・蓄積・分析し、C&C サーバである可能性が高い機器を検知することは正当業務行為である、(2)フロー情報を収集・蓄積・分析して検知した C&C サーバに関する情報を共有することは通信の秘密の保護規定に直ちに抵触するとまではいえない、との整理 とした方がよい	御意見については、参考として承ります。
5	個人I	Ⅱ-1.-(1)-ア.	・１３ページの脚注のリンクが不良です。	御指摘を踏まえて脚注リンクを修正しました。
6	個人I	Ⅱ-1.-(1)-イ.	・１７ページの最下行から上に４行目「あたって」と、２９ページの１８行目「当たって」とは、どちらかに字句を統一したほうがよい。	御指摘を踏まえてp17、ｐ20、ｐ44の「あたって」を「当たって」に修正しました。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
7	KDDI株式会社	Ⅱ-1.-(1)-イ.	ソフトウェア製品の構成管理は、システムのソフトウェア化が進む情報通信分野において、サプライチェーンリスク対策として今後重要になるものと考えています。ソフトウェアの構成部品に関して、問題等が発生した場合でも第三者機関が検証可能であるトレーサビリティの実現を含む、SBOMの活用の検討が実施されることを期待します。	いただいた御意見は今後の施策における参考とさせていただきます。
8	KDDI株式会社	Ⅱ-1.-(1)-ウ.	ISPを通じた注意喚起だけでは、サポート切れIoT機器のソフトウェアの脆弱性に十分に対応できない可能性があり、IoTの機器製造事業者との連携が重要になると考えております。より効果的な注意喚起を行う手法について検討が進められることに賛同いたします。	賛同の御意見として承ります。
9	KDDI株式会社	Ⅱ-1.-(1)-カ.	高度化するサイバー攻撃に対処するため、攻撃に係わる情報の収集・分析およびそのスピードが重要になると考えております。そのための仕組みとして、ICT-ISACの取り組みを活性化し活用することに賛同いたします。	賛同の御意見として承ります。
10	個人Ｄ	Ⅱ-1.-(1)-ク	その一部においては、我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではないと考えられる提案も行われている ↓ この出典、あるいは根拠があると良い。「既存のインターネットの TCP/IP 等のアーキテクチャに内在する脆弱性の存在を強調し、それを解決するための案として主張される場合もある。」ともあるが標準化提案のうち、我が国と整合性のない提案が具体的に示されていないため、議論が曖昧になっている。このままでは、国際標準化の取り組みに水をさすことになるから、具体的に指摘されたい。	御指摘の「整合的ではないと考えられる提案」としては、既存のTCP/IPアーキテクチャのオープンで、分散型・自律的な運用の原則に反するような提案を指しますが、当該記載箇所はこれらの提案を詳細に記載することを目的とする部分ではため、原案のとおりとします。
11	個人Ｄ	Ⅱ-2.-(1)	p.27 我が国のサイバーセキュリティ製品・サービスは、海外製品や海外由来の情報に大きく依存しており、国内のサイバー攻撃情報等の収集・分析等が十分にできていない。そのため、製品・サービスの開発に必要なノウハウや知見の蓄積が困難となっている。また、我が国のサイバーセキュリティ人材は質的にも量的にも不足しており、人材育成を全て国で実施することは困難である ↓ の根拠があれば盛り込むのが望ましい。	御指摘を踏まえ、注釈に追記いたしました。
12	個人Ｄ	Ⅱ-2.-(1)	「総合的にカバーする、オープン型の新たな人材育成プラットフォーム」について、経産省が作成したデジタル人材育成プラットフォーム「マナビDX」について言及すべきである。総務省も含めてこのプラットフォームによる人材育成を進めていくことが政府資料によって明らかになっている。	御意見については、参考として承ります。
13	楽モバイル株式会社	Ⅱ-2.-(2)	「サイバーセキュリティに係る実践的な研究開発の推進が求められる」(P29)とする本報告書に賛同いたします。 諸外国では民間による積極的な先進的研究投資やこれに対する外国政府の資金援助等が進んでおり、我が国としても、国際展開を見越した取組を強化しなければ、開発競争に遅れを取り、グローバル市場での存在感を失いかねません。 他方、これまでの要素技術に関する応用研究や実証等の成果を早期に社会実装し、本格的な国際展開・国際標準化を推進していくことも必要になると考えております。 当社には国際展開に強みがあり、例えば当社が日米連携等をリードすることは、ベンダー等の国内企業の国際競争力の強化にもつながり、ひいては国益の向上に資すると考えているところ、ぜひ補助金等による継続的な支援をお願い致します。	基本的に賛同の御意見として承ります。その他の御意見は今後の施策における参考とさせていただきます。
14	個人Ｄ	Ⅱ-2.-(2)	p.30 NICT における研究開発において、個々の具体的な研究例が挙げられているが、論文として発表されているものがあればその論文へのリンクをつけてほしい。	個別の研究開発成果に係る発表論文については以下を御確認ください。 https://www.nict.go.jp/outcome/papers/index.html
15	個人F	Ⅱ-4.-(1)	プライバシーマーク（Pマーク）のようなセキュリティ版の認定制度を見当してはいかがでしょうか。 普及啓発のみではインセンティブが得られないので、インセンティブを用意してセキュリティ対策導入を促すと同時に、セキュリティに関する研究開発・製品開発の継続性を持たせる事が狙いです。 提案のアウトラインとしては、社内規程等で情報セキュリティ規程が整備されており、それらがガイドラインに沿ったレベルであると同時に、ペネトレーションテスト等を通じて、インターネットに接続されている利用中のサービスが一定レベルのセキュリティを確保できているかをチェックして、基準を満たせれば認定とする。 認定にあたっては認定レベルを設け、認定組織が推奨しているセキュリティ対策機器・ソフトウェア等を使って対策を行っている企業に対しては上位の認定レベルを付与、それ以外で基準を満たせば下位の認定レベルを付与するなど。企業規模等に応じたレベルを容易する。 またこれら認定は一定期間のみ有効であり更新の際には、最新の認定試験を必要とすることで、セキュリティ対策の陳腐化対策とする。 認定組織が推奨するセキュリティ対策機器ソフトウェア等に関しては、自律的な対応能力の向上による成果物等を想定する。 また審査基準を策定し、審査基準を満たすメーカー製品等を指定する。 認定制度は、企業ブランディングとして積極的に採用される事が想定されるため、これらのサイクルを回すことで国全体としてのセキュリティレベルが向上する事を期待します。またこれらの取り組みから組織内1人1人のリテラシーの平均値の押し上げも期待します。	御意見については、参考として承ります。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
16	個人Ｃ	Ⅱ-4.-(1)-ア.	テレワークにおいてセキュリティはかなり重要であるが、会社経営者層の認識が著しく杜撰である。 例えるなら知床で船を沈めた会社の様に船倉に普通に穴を空ける様な安全意識が無い状態を放置し、危険性を訴えた社員を冷遇する様な状態が中小企業を中心にまかり通っている。 主にサポート期限の切れたOS・サードパーティ製品、ハードウエアを平然と使い続ける等が横行している為、IT企業においてもサイバー攻撃に著しく弱く、個々の社員の意識・行動・セキュリティ理解力頼みという現状である。 そのくせサポート期限の切れたOS・サードパーティ製品、ハードウエアの必要かつ必須な更新費用は出し渋る割に、不要不急である社員旅行といった、経営層の自己満足には費用を惜しまないといった矛盾だらけである。 そういった状況も監査があっても指摘・改善すらされない為、より劣悪な環境に落ちる負のスパイラルが続いている。 これは最早まともな働き方ではないと言わざるを得ない。 中小企業も仕事を大企業から下請けする事もある為、大企業も関係ないというわけではない。 頭の弱い会社経営者層の認識を放置したから2020年以降、IT関連の産業で重大なサイバーテロ被害が何度も発生したとも言える。 Emotetの大流行やみずほ銀行のもはや醜聞としか言い表せない状況も杜撰な状態を長年放置した結果である。 これではIT産業の国際競争力を向上させるスタートラインにすら立ってない負け犬のような状態である。 頭の弱い会社経営者層を本格的に駆除しないと日本の産業力は落ちる一方である。	御意見については、参考として承ります。
17	個人Ｅ	Ⅱ-4.-(1)-イ.	デジタル田園都市国家構想との連携がなんら見られない。同じく「地域」(Local,rural)を対象としているのだから確り連携願い度。	御意見については、参考として承ります。
18	個人Ｄ	Ⅱ-4.-(1)-イ.	「先行的に一部地域で開催した若年層のサイバーセキュリティ人材育成に向けた CTF（Capture The Flag）など、地域における先進的な取組み」について、CTFではすでに全国規模にSECCONが開催されており、日本最大級のCTFとして認知されているが、ここではそれについて述べられていない。CTFが地域のみで開催されているという誤解を防ぐために、SECCON等の全国規模のCTFと連携をとる、あるいは注視するなど、全国規模のCTFとの関連を少しでも出してほしい。	ご指摘いただいた箇所は、地域セキュリティコミュニティの強化について、あくまで地域SECUNITYにおけるCTFを記載しているため、原案のとおりとさせていただくとともに、御意見については参考として承ります。
19	個人Ｈ	Ⅱ-4.-(1)-ウ.	ガイダンス策定の必要性についてのコメント ・IPAやExtraHop Networksが行った調査によると、多くの組織はサイバー攻撃の被害に遭ってもあまり公表しない傾向があることが確認されています。こうした結果が社会にとって望ましくない場合、かつ、各組織がどのように公表したら良いかわからないことや知見不足が主な理由であれば、ガイドラインを策定する意義・必要性があると思います。しかし、他に理由があることも想定されるため、そもそも各組織が適切な公表ができているのかどうかの現状把握や、社会をセーフティなものにしていくにあたって各社適切な公表ができていない場合の様々な観点からの原因究明を推進する活動、その原因に対して対策を推進する活動も必要だと思います。 ガイダンス策定にあたってのコメント ・年内に策定を進めるガイダンスの対象範囲が共有だけのように読めるため、インシデント収束後の教訓の公表も含む公表も対象にしてほしいです。 ・既出知見との矛盾がないよう、JPCERTが既に提示するサイバー攻撃被害情報の共有と公表のあり方についてとの著しい方針乖離がないようにしてほしいです。 ・共有のガイダンス策定にあたってはNCA、ISAC、JPCERT、IPA J-CSIPなどの関連組織が複数あるように認識しています。これらの既存組織の目指す取り組みと矛盾がないようにしてほしいです。 ・JPCERTは、公表にあたって、類似事案の再発防止をするため、同業他社や社会に共有が望まれる教訓は、インシデント収束後の公表が望まれる旨の提案もされています。この教訓をどのような観点で整理すべきかという点も盛り込んでほしいです。例えば、徳島県つるぎ町立半田病院のコンピュータウイルス感染事案有識者会議調査報告書は教訓を読み解くのに苦労します。	御意見については、参考として承ります。
20	KDDI株式会社	Ⅱ-4.-(1)-エ.	民間企業によるサイバーセキュリティ対策の情報開示は、企業が社会からの信頼感を得ることが期待できることに加え、企業のプラクティスが公開・共有されることで、個々の企業の対策の改善に参考とする機会を得ることにつながると考えているため、情報開示の推進に賛同いたします。	賛同の御意見として承ります。
21	個人Ｄ	Ⅱ-4.-(2)-ア.	オンライン動画講座と広告について、リンクを貼ることが望ましい。また、2204 名が受講登録を行ったとあるが、実際に修了したのは何名なのか明記されると望ましい。	御指摘を踏まえて、脚注を追記いたしました。なお、本講座は、動画を1つ見るだけでもサイバーセキュリティについて学ぶことができるようなものとなっており、修了証の発行等は行っていないため、原案のとおりとします。

項番	意見提出者	該当箇所	御意見の詳細	御意見に対する考え方
22	個人J	Ⅱ-4.-(2)-ウ.	・要旨（1000字を越えるため） 国は、電子メール利用の安全性向上のために、信事業者へのDKIMの普及振興を行い、また、電子メール役務を扱う電気通信事業者には義務として電子メールの（基本として）TLSでの保護（ICMPoverTLS、STARTTLS）を行わせるようにされたい。 ・内容全体 フィッシングメールについては、（国内においては国内事業者の）DKIMの普及で減少するものと考えるが、そうする事により、他国から発信されたものについて「DKIM対応でない」事でのフィッシング注意警告が行えるようになるので、日本国内においてのDKIMの普及を行われたい。（なお、言っておくが、電子メールについては、末端の、POP・IMAPで電子メールを閲覧するISP等契約者（及びその使用するメーラー）が、電子メールについてのスパム判断を行うものであるので、使用する技術については、（他の、専らISP等しか参照しない様な情報を用いる様な技術ではなく）DKIM（の様な末端の利用者（メール受信者）が閲覧できる情報を用いた技術）である必要が強くある。総務省はかなりDKIMについて振興を行おうとしていたように見えるが、近頃、「どういうわけか」（どこかからの要請であろうか？火種が多い事を好むような）、その勢いがかなり減退しているので少々問題と考える。DKIMの望ましさは、末端のメール受信者に情報が可視である点で目立って高いものであるので（なお、クラウド事業者などがホスティングを行っている場合などは、途中のメールサーバーで仮想サーバから発信されるメールについてDKIMを付すサービスを提供する事なども可能である。）、積極的に推進させていくべきと考える。） また、これはフィッシングメールだけでなく個人情報保護及びサイバーセキュリティに有用であり、また個人情報保護法、サイバーセキュリティ基本法、及びそれらをふまえた電気通信事業法からすると、本来的には推論により自明的となるはずの事であるが、法定の電気通信事業者が電子メール役務を提供する際においては、電子メールについての認証局証明書を用いたTLSによる保護及び認証（SMTPoverTLS、STARTTLS）があれば（日本国内事業者の全てがちゃんとサーバにおいての運用を行っていれば）、そこで「TLSによる認証がある安全と思われる電子メール」と「それ以外」の区別がISPやメール受信者に容易に行えるようになるので（電子メールの信頼性の判断が大いに捗るであろう。）、総務省は、ちゃんと、それらの法律の趣旨に沿った行政を行うために、電気通信事業者が電子メール役務を提供する場合は、ちゃんとインターネット上で他サーバとやり取りされる電子メールについての暗号化（※個人情報保護のため必須である。総務省はその点を誤魔化さないでいただきたい。）及び認証が（SMTPoverTLS、STARTTLSにより）なされるようにされたい（※電子メールの保護がちゃんと行われなければそれらの法律が適切に運用されている事にはならない！総務省はちゃんとその事を認識されたい。それが行えないのであればそれはあまりに国家公務員として官庁として不明である。）。 総務省は、いい加減、無知のふりをやめて、真っ当な電子メールのセキュリティ向上を行うようにされたい。（国民として数年指摘し続けているのであるが、法定の電気通信事業者の電子メール役務におけるTLSでの電子メールの保護の（準）義務化について全然聞く気が無いようであり、（分野の専門のはずの）国家公務員の質の低さに呆れている。そんなんだから防衛省mod.go.jpのMXサーバが依然としてTLSで保護されたメールの受信に対応していないのではないか（同ドメインのMXサーバでは国民や事業者からの重要性ある業務等にも関係するメールの受信を行っているはずであるが。）。総務省の質の低さが国家公安を確実に破綻させている部分がある事についてしかと自覚されたい。）	いただいた御意見は今後の施策における参考とさせていただきます。
23	個人A	全体	内閣サイバーセキュリティセンターの「サイバーセキュリティ戦略」と著しく重複しているため、廃止してはどうか。 「縦割り行政」から一刻も脱却し、サイバーセキュリティ政策は内閣サイバーセキュリティセンターに一元化すべきである。	御意見については、参考として承ります。
24	個人D	全体	・BGP や DNS, 5G SA, OSSの正式名称は載せなくて大丈夫か。略語に対して正式名称を付記する基準を統一した方がよいのではないか。	御意見については、参考として承ります。
25	個人D	全体	・トラフィック　トラヒック　の表記揺れを治した方が良い。	ご指摘を踏まえて、「トラヒック」に統一することといたします。
26	個人D	全体	・5ページ, 48ページが画像になっているようで、テキスト検索が不可能です。	御指摘を踏まえ、5ページの画像を一部修正しました。なお、48ページの画像については、前後の検索可能テキストに記載のある「国民のためのサイバーセキュリティサイト」についての該当WEBページの参考画像であり、当該WEBページのURLも脚注に記載してあることから原案のとおりとします。
27	個人D	全体	・PDFにしおりをつけてください。このPDFではしおりがついていないため、全体の構造把握が面倒でした。視覚などに障害をもつ人達が長いPDF文書で必要な内容に迅速にアクセスできるためにもしおりが重要です。そこで、Webコンテンツ・アクセイシビリティ・ガイドライン（WCAG 2.0）でもPDFにしおりを作ることが重要とされています。しおりのつけかた：　https://www.antenna.co.jp/pdf/reference/pdf-shiori.html	御指摘を踏まえてしおりを付記致しました。
28	個人G	全体	米国のセキュリティ技術等最新技術を駆使して対応しなければならないと考えます。	御意見については、参考として承ります。