別紙

放送システム委員会報告（案）に対する意見とそれに対する考え方

（意見募集期間：令和元年 11 月 9 日から同年 12 月 9 日まで）

提出された全意見 139 件

（**本報告（案）に対する意見 10 件（個人 8 件、法人 2 件）**

日本放送協会に関する意見 111 件

その他無関係と思われる意見 18 件）

No.	頂いた意見	頂いた意見に対する考え方	提出意見を踏まえた案の修正
1	今回の地上デジタルテレビジョン放送等の安全・信頼性に関する技術的条件に賛同します。 ケーブルテレビ事業者は放送サービスだけでなく、多くの事業者は電気通信サービスの提供を行っています。この電気通信サービスの提供にあたっては、昨今の状況から電気通信設備に対するセキュリティ対策の強化に取り組んでおり、この取り組みを通じて放送設備のセキュリティ対策を行っているころです。 ケーブルテレビにおける放送設備ならびに電気通信設備は地域における重要なインフラ設備です。地域の皆様に安全・安心なサービスを持続的に提供していくため、これら設備の情報セキュリティの確保、向上に引き続き取り組んでまいります 【一般社団法人日本ケーブルテレビ連盟】	本報告（案）について賛同のご意見として承ります。	無
2	まず根本的な話として、現状の放送システムはラジオ放送、テレビジョン放送を行っている限りにおいては、サイバー対策としてはかなり優秀なシステムではある。 なぜなら、放送波を受信するだけの一方通行のシステムだからである。 ただ、現実問題として、放送までに至るまでの様々なところでインターネット技術が使われているだけでなく、インターネットの同時配信も行われていることで、そちらも憂慮する必要がある。	本報告（案）では、放送設備（番組送出設備、中継回線設備、放送局の送信設備）を対象としており、番組送出設備とオンラインで繋がる外部ネットワークから隔離することによって対処することとしております。 また、本報告（案）の 40 ページに記載のとおり、報告（案）におけるサイバーセキュリティ対策の措置内容は、現在の放送ネットワーク	無

	これについては、多くの IT 企業と同様のレベルのものが必要と考える。 【個人】	を想定したものであり、今後新たな放送サービス、技術革新等の環境変化が生じ放送ネットワークの設備形態等が変更された場合には、措置とその対象となる放送設備の対応について、セキュリティ対策を不断に見直しすることが必要と考えています。なお、インターネットの同時配信は法令上、通信との扱いになります。	
3	＞3-3-2 サイバーセキュリティ確保に係る主な対策技術 各方式における弱点なども記述しておくべきではないかと思われた。（例えば、ホワイトリスト方式については偽装された場合に効果が無いという弱点があるが、その様な事は一応注意として書いておくのが良いのではないかと思われる。） セキュリティについては他にも、通信方式で同軸方式の場合は電磁的な盗聴が容易であるという様な事についての記述が抜けている等が気になった。どうもセキュリティについての記述が疎かである様に思われたが、放送といってもデジタル放送の時代にあっては多少の双方向性があると思われるので（それがうたい文句でもあったのであるし）、セキュリティに関係する記述については多少意識して行っていただきたく思われた。 ＞25 頁目図 完全性の扱いが可用性より低い様な図であるが、完全性が確保されないと可用性は無用のものとなるので（機密性もであるが）、完全性について大きい扱いとしていただきたく思われた。 もちろん、末端利用者への映像伝達の部分のみであれば、多少完全性が壊れていても大きな問題とはならないケースが多いであろうが、しかしその様な場合を除けば、完全性こそが通信（あるいは情報処理）を行う場合の最重要事項であるので、完全性については、映像伝達以外について大きく取り扱う場合は、最重要となる様な扱いを行っていただきたく思われた。 【個人】	各方式の弱点等については、セキュリティの観点から、明記すべきではないと考えます。 放送設備及び有線放送設備については、「いかなる状況下でも安定的に継続運用できること」が求められ、可用性の確保を最優先するとの考えから、図 3-1-1 中、「可用性」の図を大きくしておりましたが、ご指摘の通り、内容の改ざんを防ぐ観点から「完全性」についても重要であることを踏まえ、図 3-1-1 の図を修正します。	有
4	当該技術要件を拝読したが不十分な点があるため指摘したい。 ・NISC が発行する「重要インフラにおける情報セキュリティ確保に係る安全基準等	本報告（案）では、放送設備（番組送出設備、中継回線設備、放送局の送信設備）を対象としており、番組送出設備とオンラインで	無

	策定指針」についての参照を追加し、内容に沿った技術的条件とするべきである。 以下「NISC 指針」と称する ・NISC 指針の 4.1.4(2)「人材育成及び意識啓発」が求められているが、当該技術要件では具体性に欠けている。NISC 指針に『「情報処理安全確保支援士」等の資格取得等も期待される。これらの取組は 人材育成の達成状況を客観的に評価・確認する際にも有効となる。』と記載ある通り、当該資格の必置化など重要インフラにおいては具体的取組が求められる。 ・NISC 指針 4.2.2 の通り『サイバー攻撃に備えたコンティンジェンシープラン及び事業継続計画の策定』およびインシデント対応時に必須である『CSIRT 等の整備、関連部門との役割分担等の合意』も実施するべきである。 ・NISC 指針 4.3.1『モニタリング及び監査』にある通り対策が継続的に取り組まれていることを客観的に検証するためにも情報セキュリティ監査を定期的に実施するべきである。 次に本技術的条件に記載の内容について指摘したい。 ・各所に「番組送出設備」と記載があるが、現代において「番組送出設備」は IT により動作している。具体的には IT のサーバ・ストレージであり、保管している番組もファイル化されている。またオンラインで番組編集システムと結合している局も多数あるにも関わらず、まったく想定されていない。これは現状に即していないため想定を追記するべきである。 さらにはクラウドを放送設備にて運用している基幹局（フジテレビ：クラウド活用の送出マスター）も存在する。これに対する想定も追記するべきである。 ・民放においてはコマーシャルが収益源であるが、コマーシャル（CM）を送出する CM 送出設備に関する記載が抜けている。特に CM に関しては広告代理店等からインターネット回線を利用して CM の配信を受けている局が多数存在しているが、言及されていない。CM 送出設備と放送設備のアクセスコントロール、安全対策についても記載する事。 ・P29「3－3－2－1 VPN（Virtual Private Network）構築」について、VPN を構成	繋がる外部ネットワークから隔離することによって対処することとしております。 ご指摘の VPN の脆弱性の認識も含めて、報告書（案）P35 に「一般的に、情報システム等では、その脆弱性を完全に除去するのは難しく、意図しない脆弱性が残るものであり、また、悪意のある攻撃者が脆弱性を組み込む場合があり得ることから、放送設備で使用する機器についても、脆弱性があることを認識し、セキュリティ対策が継続的に行われることが必要となる。」旨を記載しております。このことを踏まえ、各放送事業者等においては、VPN にも脆弱性があるとの認識を持ち、運用にあたっては、脆弱性対策を確認するなどの対応が期待されます。 基幹放送の認定を受けようとする者は、放送法に従って、当該業務を維持するに足りる技術的能力が求められ、具体的には組織体制、管理規程、業務に従事する者の実務経験等を審査することとしております。「情報処理安全確保支援士」の資格については、各放送事業者の自主的な取組が期待されます。 本報告（案）の 40 ページに記載のとおり、報告（案）におけるサイバーセキュリティ対策の措置内容は、現在の放送ネットワークを想定したものであり、今後新たな放送サービス、技術革新等の環境変化が生じ放送ネットワークの設備形態等が変更された場合には、措置とその対象となる放送設備の対応について、セキュリティ対策を不断に見直しすることが必要と考えています。	

	する VPN 装置の管理、バージョンアップの必要性が認識されていない。VPN 装置においても脆弱性が発見され遠隔から管理者権限を奪取される脆弱性なども過去に発見され実際に被害が出ている。よって VPN 装置や UTM 等セキュリティアプライアンスにおいてもソフトウェアを搭載している以上、脆弱性が発見される前提にて対策を講じるべきである。具体的には脆弱性情報の監視および定期的なログ監査とバージョンアップを行うべきである。本修正を P36にも反映する事。 ・p37「5. 放送設備の運用・保守に際して、業務を確実に実施遂行するための組織体制の構築及びその実施に係る規程やマニュアルを整備するための措置 」 前述の通り、実際に対策をおこなう放送局の職員のスキルレベル向上が必要である。陸上無線技術士資格と同様、国家資格である情報処理安全確保支援士資格を人員育成の客観的指標として採用し、必置化を推奨する。 上記指摘の通り本技術的条件はまだまま内容が薄いため今後一層の研究と改訂を期待する。 【個人】		
5	2020 東京五輪を迎えるにあたり、地上デジタルテレビジョン放送等の映像・音声情報の公共性は増加すると考えます。 令和元年 10 月 28 日付け資料「情報通信審議会 情報通信技術分科会 放送システム委員会 放送設備安全信頼性検討作業班1及び2 報告」を拝読した上でサイバーセキュリティーの観点から技術的要件について意見を提出します。 同資料の対策として番組送出設備においては VPN(インターネット VPN)を利用するとの記述がございます。対応の機密性から具体的な方法についての記述が無いのかもしれませんが、この点についてリスクを感じます。 VPN であっても過去にはある企業の VPN に出張中の社員が社用パソコンを民間宿泊施設にて利用した際に社用外のウェブサイトに接続したことによりマルウェアに感染、企業情報漏洩インシデントが発生したと認識をしております。 インターネット接続を前提としたネットワーク環境において上記の様なリスクは必ずあるとの前提でサイバーセキュリティをご検討頂きたいと考えております。利便性(コス	ご指摘の VPN の脆弱性の認識も含めて、報告書(案)P35 に「一般的に、情報システム等では、その脆弱性を完全に除去するのは難しく、意図しない脆弱性が残るものであり、また、悪意のある攻撃者が脆弱性を組み込む場合があり得ることから、放送設備で使用する機器についても、脆弱性があることを認識し、セキュリティ対策が継続的に行われることが必要となる。」旨を記載しております。このことを踏まえ、各放送事業者等においては、VPN にも脆弱性があるとの認識を持ち、運用にあたっては、脆弱性対策を確認するなどの対応が期待されます。 また、検知した際の対応組織に関するご意見については、今後の政策の検討において参考とさせていただきます。	無

	ト抑制)とのバランスが重要だと考えますが、特に東京五輪の様な世界最大のイベントの際には当該インターネット VPN を利用する関係者(海外の方含める)の方々の人数も増加する事が考えられるため、インターネット接続する外部ネットワークの制限、接続した際の可能な範囲での早期の検出が必要ではと考えます。 上記は予備的防御の案の一つですが、実際に検知した際の対応組織も必要だと認識しております。具体的には ISAC の元に産官学連携 CSIRT 組織を有し、さらにその下に SOC 組織を有すべきだと考えます。当該組織には強いガバナンスが必要です。地上デジタルテレビジョン放送には重要インフラとしての放送・通信事業者以外にも電力、交通、流通事業等のサプライチェーンが存在すると考えております。サイバーインシデント発生時にサプライチェーンへの影響を最小化するために、強いガバナンスの元での重要インフラ間の CSIRT が有機的に構築される事を希望致します。 【ブリッジシップ株式会社】		
6	この「地上デジタルテレビジョン放送等の安全・信頼性に関する技術的条件」(以下、本条件)では、主にサイバーセキュリティの確保手段につき書かれているようです。一方、物理的なセキュリティについては、「4－2 サイバーセキュリティ確保のための措置の解説と具体例」の【具体策の例】の「4. 放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための措置 」に「 ID カードの使用をした入退室管理、テンキー錠、有人による入退室管理などの措置を講じること」とあります。 しかし、例えば外国の軍隊・テロ組織などが、上記入退室管理を破り、主要な放送設備を占拠したらどうなるでしょうか。政府は必要な情報を国民に発信できなくなり、代わりに占拠した者が偽の情報を国民に発信することになります。こう考えると、入退室管理だけでは十分でないと思われます。万一放送設備が占拠された場合、リモートでその放送設備を働かなくする仕組み、予備サイトに準備した放送設備から正しい情報を発信するための仕組みなどが必要と思います。	本報告(案)は、放送設備のサイバーセキュリティの確保に関する技術的条件について、検討を行ったものです。 ご意見については、今後の政策の検討において参考とさせていただきます。	無

	本条件によれば、有線放送を除き、番組送出設備と送信設備が別の場所にあり、両者が回線で接続されため、上記の仕組みは実現可能であり、既に本条件に組み込まれているかもしれませんが、念のため、意見として提出しておきます。 【個人】		
7	反対です 【個人】	本件報告（案）の内容に対する具体的な反対の理由は明らかではありませんが、本報告（案）は、放送設備のサイバーセキュリティの確保に関する技術的条件について、検討を行ったものです。 取りまとめにあたっては、地上、衛星及び有線放送事業者、メーカ、放送関係団体、学識経験者等放送設備の安全信頼性に係る専門家から知見を踏まえたものであり、放送設備の安全性信頼性の確保が可能となると考えます。	無
8	「サイバーセキュリティー対策」における「人材（ヒューマンリソース）」を「育成（ヒュマンリソースデボロップメント）」するべき構造と、私し個人は思います。例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」における ISP サーバーから成る「DNS サーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」等の構造。具体的には、「方式規格（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第 3 世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP 方式（GSM 方式及び W-CDMA 方式）」の構造。（イ）「4G（第 4 世代）」における「LTE 方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第 5 世代）」における「MCA 方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデーター（BD）」から成る「データ	本報告（案）は、放送設備のサイバーセキュリティの確保に関する技術的条件について、検討を行ったものです。 取りまとめにあたっては、地上、衛星及び有線放送事業者、メーカ、放送関係団体、学識経験者等放送設備の安全信頼性に係る専門家から知見を踏まえたものであり、放送設備の安全性信頼性の確保が可能となると考えます。	無

	ーベース(DB)」の融合により、IT ネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側(プロバイダー側)←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側(ユーザー側)」等を融合する事で、ハードウェアーの強化の構造。(イ)エッジコンピューティングでは、Web 上における「URL(ユニフォームリソースロケーター)」での「HTML(ハイパーテキストマークアップラングエッジ)」から成る「API(アプリケーションプログラミングインターーフェイス)」の導入により、「HTTP 通信(ハイパーテキストトランスファープロトコル)」における暗号化によるソフトウェアーでの「HTTPS(HTTP over SSL/TLS)」の融合により、AI ネットワークの構造。具体的には、「サイバー空間(情報空間)」及び「フィジカル空間(物理空間)」での「回線(サーキット)」の事例が有ります。(ア)「サイバー空間(情報空間)」では、「SDN/NFV」における仮想化サーバー(メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー)」から成る「リレーポイント(中継点)」での「VPN(バーチャルプライベートネットワーク)」の構造が主流と、私は考えます。(イ)「フィジカル空間(物理空間)」では、「AP(アクセスポイント)」の構造が主流と、私は考えます。要約すると、「垂直統合(ベイティカル)」における破壊的イノベーションでの「量子コンピューター(クアンタム)、AI(人工知能)、全能アーキテクチャー(脳科学)」等での「サイバーセキュリティー対策」を教えられる教師がい無いと言う事が「ネック(壁)」の構造と、私は考えます。「平行統合(ホライゾンテル)」における持続的イノベーションでの「IT(情報技術)、IoT 機器(インターネットオブシィングス)」等での「サイバーセキュリティー対策」を教えられる教師がいると言う構造と、私は考えます。 【個人】		
9	放送システム委員会 報告(令和元年11月7日)は国家としてのサイバーセキュリテイ(SS)としては実効がないと思われるため、これを破棄すべし。テレビ放送会社をコンテンツ制作会社(発信者)とテレビ通信会社(通信会社)に分離して、その上でやるべきことを行うべしとの趣旨です。 仮想敵 SS での攻撃者は北朝鮮、中国、ロシアのサイバー攻撃部隊や現在暗躍しているテロリストなどを含む団体(以下テロリスト)などを想定するのが妥当である。テロリストは高度に組織化されており基本戦略のもと、悪意を持って攻撃して来る。明らかに日本のテレビ業界より技術力が高く、その技術は日進月歩している。 問題点 テロリストは、平時には放送局内に協力者を作り、また工作員を忍び込ませて、不法アクセスを行い、システムの弱点を探り仲間を増やす。その弱点を利用し情報を	本報告(案)は、放送設備のサイバーセキュリティの確保に関する技術的条件について、検討を行ったものです。 取りまとめにあたっては、地上、衛星及び有線放送事業者、メーカ、放送関係団体、学識経験者等放送設備の安全信頼性に係る専門家から知見を踏まえたものであり、放送設備の安全性信頼性の確保が可能となると考えます。	無

	得て外部に流し、放送局を攻撃する(デマやプロパガンダ)、政府や国民が困る番組を流し、相互不信を増大させ、社会不安をあおる。戦時には虚偽情報を流し、また通信網の遮断などを行い、混乱を拡大させる。まだ自衛隊への不信を煽り、虚偽情報を流して、暴動を起こし自衛隊の作戦を阻止し、作戦遂行を困難にする。 もう一つの側面はテロリスト同士の情報通信です。例えば東京のテロリスト支部から国内や外国で隠れているテロリストに情報を伝える。IN で通信を行えばアドレスが特定され逮捕できる。しかしテレビは受信者管理が不十分なためにテロリストは安全に情報伝達ができる。 明らかな様にテロ対策と SS は表裏一体であり、日本の国内にいるテロリストやその協力者を取り除くことが最重要課題になる。 国家の役割 国家としてのテロ対策及び SS の目的は以下の様である。 1. 日本において不正アクセスを困難にして、不正アクセスを減らすとともにそれが監視できる体制を作る。 2. 公的機関が常時監視するシステムを機能させ、テロリストを摘発する体制を整える。 3. 国際連携を図り、グローバルなテロ撲滅に寄与する。 総務省、審議会の役目はテロ対策と SS を考慮した上で、テレビ放送業界で SS の実効的なスキームを作ることです。 SS 防御スキームの類似例 武器の密輸入の場合、武器は以下の様に移動する。 武器密輸グループ⇒外国の運送会社⇒外国の輸出検査⇒成田空港⇒入国検査⇒運送会社⇒活動家 外国の輸出検査、入国検査で公的機関がレントゲン調査を行い、事件が発覚しインボイスから武器密輸グループと活動家が判明します。 テロメイルの場合のメイル情報の流れは以下の様になる。 テロメイル発信者⇒プロバイダー⇒IN の公衆網⇒プロバイダー⇒活動家 IN 公衆網は常時監視されていて、怪しいメイルを見つければその通信ログからプロ		

	バイダー、発信者、受信者が判明し、活動家が判明します。 これと同じスキームをテレビ放送に適用することが基本となる。 IN の場合をもう少し詳しく見ると ○ テロリストは公的機関の目を逃れてメイルを発信する。 ○ PC の OS はメイルに発信者と受信者のアドレスを追加し暗号化して発信する。 ○ プロバイダーは通過ログを追加して IN 公衆網のポイントに渡す。 ○ 公衆網のポイントでは通過ログを追加して受信者にたどり着く。受信者以外は受け取れない。 ○ 受信者の PC の OS が暗号を解読して表示する。 ○ プロバイダーや IN 公衆網を、公的機関が常時検査を行い、ログからテロリストを特定する。 今 IN の世界では誰もが自由に情報を発信することができ、他人に漏れることなく受信でき、SS のための常時検査が国際的に可能です。一方テレビ放送は特定の特権的な人のみが発信を行い、受信者は不定で通信の秘匿性が保たれません。SS のための常時検査ができず、信頼に足る通信になっていません。IN 業界の技術力を導入し、抜本的な対策が望まれます。 技術的には発信者、受信者、通信会社、暗号化会社、公的検査組織がそれぞれ独立していて、各自が職務を完全に遂行できること、職務に必要な技術情報、特に暗号化技術が外部に漏れないことが重要です。注意すべきは通信会社が複数あり、悪意のある通信会社を排除しても全体の通信は保たれることです。テレビ業界をこの様なスキームに変えるべきです。 以下具体的な対策ですが 現在のテレビ業界は発信者と通信会社が分離されていないので、経営的、技術的に完全分離する必要があります。発信者（コンテンツ制作会社）、通信会社（テレビ通信会社）、受信者の間は公衆網（IN とテレビ電波）で接続します。これらは公的な検査可能エリアです。 発信者はコンテンツ制作の全権を持ち、コンテンツを製作します。また出荷品にコンピュータウイルス、デマやプロパガンダなどがないことは発信者の責任になり、違反した場合は通信会社から受け取りを拒否されるなどのペナルテイを受ける。発信者と通信会社は LAN で接続し、発信直前に暗号化が行われ、受信者を指定し、通信会社に情報を受け渡します。		

	発信者と通信会社が使用する公衆網のLANでは暗号化が行われているため通常の人が傍受することはできない。公的機関は検査を行うことができる。 通信会社は指定された受信者に情報を届ける。発信者から LAN を通して、コンテンツを受け、通過ログを追加して、テレビ電波で放送する。コンテンツは全て暗号化されているので通信会社での改ざんは不可能です。 テレビ電波は LAN と同様に公衆網であり、発信者、通過ログ、受信者情報が添付されており、暗号化が行われている。通常の人が傍受することはできないが、公的機関は検査を行うことができます。 受信者は有料無料を問わず、通信会社に登録し、受信機 ID を登録しておく。登録された ID の受信器では暗号を解読して視聴できるが、非登録の受信器では暗号解読ができず視聴できない。受信者と受信機を対応付けるために、2 段階登録や、リアルタイムまたはエベントごとに（例えば番組ごとに）再確認する手段も必要です。 NHK の国際放送は受信可能者が 2.8 億人もいるそうです。そのほとんどは受信者が特定できないのが実態と思います。外国ではテロリストの危険が高く、注意深い受信者管理の必要があります。受信者を特定できない場合は国際放送を取りやめるべきです。 公的検査機関が公衆網である LAN やテレビ電波を監視し、関係会社から受信者情報やアクセス情報などを入手すればテロリスト割り出しは難しくない。 災害時には国または地方自治体が通信会社の通信権を優先的に取得することができ、テロ、戦争の場合には自衛隊も優先権を取得できます。発信者にアクセスしないのでコンテンツ制作権を侵害しません。 災害発生時に地方自治体の長がツイッタなどで情報発信をしています。今のテレビの災害放送はテレビ局が地方自治体に取材してコンテンツを作り放送しているが、2 つの問題点があります。一つは時間がかかり放送が遅れることです。もう一つは情報責任者が地方自治体であるのにテレビ局の製作になっていて、責任者が明確でないことです。地方自治体が直接通信会社にコンテンツを流し込む様にすれば時間も短縮でき、きめの細かい情報が発信できます。このことは有事の際に必要な迅		

	速性とプロパガンダ防止に役立ちます。 以上のことは既に IN で実現されているので技術的な問題はほとんどない。受信者確認に 2 段階認証を行う場合はテレビ受像機に LAN や Wifi を付けるか、スマホの付属機器にしてリンクすれば良い。いずれにしても CAS よりは各段に確実な受信者認証ができる。 最後に 国は国民の財産である電波をテレビ放送会社に貸与しているが、国民の生命財産を危険にさらしてまで貸与する理由はないのです。従ってサイバーセキュリテイ、テロ対策に協力する団体にのみ電波を貸与することは当然です。国民の生命財産を守ることが最重要です。 【個人】		
10	現在の NHK の地上デジタル放送に安全性と信頼性を認めることはできない。抜本的な改革が必要である。 【個人】	本報告(案)は、政府のサイバーセキュリティ戦略等を踏まえるとともに、多様化するサイバー攻撃や 2020 年東京オリンピック・パラリンピック競技大会を見据え、放送設備に関するサイバーセキュリティ確保が急務となっていることから、その技術的条件について検討を行ったものです。	無
	日本放送協会のインターネット活用業務に関する御意見(111 件)	本報告(案)に対する御意見ではありませんが、担当部署に情報提供いたしました。	無

その他、本報告(案)と無関係と思われるものが 18 件ありました。