インターネット接続サービス
安全・安心マークについて

インターネット接続サービス安全・安心マーク推進協議会

https://www.isp-ss.jp/

2023年7月

協議会の構成

構成団体： 一般社団法人日本インターネットプロバイダー協会 （JAIPA）
一般社団法人テレコムサービス協会 （TELESA）
一般社団法人日本ケーブルテレビ連盟 （JCTA）
一般社団法人電気通信事業者協会 （TCA）

会　　長： 一般社団法人日本インターネットプロバイダー協会　久保　真

副会長： 一般社団法人テレコムサービス協会　北岡　隆之

審査委員長： 英知法律事務所　弁護士　森　亮二

事務局： 一般社団法人日本インターネットプロバイダー協会事務局内

オブザーバ： 総務省　総合通信基盤局　電気通信事業部　データ通信課
総務省　総合通信基盤局　電気通信事業部　利用環境課
総務省　総合通信基盤局　電気通信事業部　安全・信頼性対策課
総務省　サイバーセキュリティ統括官室
国民生活センター　相談情報部

安全・安心マークとは

インターネット接続サービス関係４団体では、
利用者が事業者を選択する際の目安として、
安全・安心マーク制度を設けています

↓

セキュリティ対策・ユーザ対応体制等が一定基準を満たしているかサービス毎に審査しマーク付与

審査範囲

・基本的な考え方

消費者が安心してインターネット接続サービスを利用できる環境の整備推進という安全・安心マーク普及促進の主旨に則り、セキュリティ体制、サービス提供条件の透明性、利用者への適切な対応の３点を重視し、ISP版、公衆無線LAN版、それぞれの審査項目で構成しています。

審査項目（ISP版）

Safe Security ISP
安全安心

１　セキュリティポリシーの確立及び監査制度の導入

セキュリティポリシーが策定され、これに基づき社内監査が適切に行われているか

２　システムのセキュリティレベル

システムのセキュリティレベルが一定の基準を満たしているか

３　トラブル発生時の対応体制の確立

障害に関する責任者や指揮系統が確立されているか、障害対応が適切に行われているか

４　利用者向け契約約款等の整備と公表

利用者契約に係る契約約款・重要事項説明が適切に整備・運用されているか

５　ユーザ対応体制の整備

ヘルプデスクその他のユーザ対応体制が適切に整備・運用されているか

６　利用者に対する周知・啓発等の取組み

セキュリティ対策情報等が利用者に対し適切に周知啓発されているか

７　個人情報保護に関する取組み

個人情報保護のための体制・取組みが適切に行われているか

手続・料金（ISP版）

- **手続**

１次審査は随時受付

✓ JAIPA・TELESA・TCAの３団体で受付けて一次審査実施

１次審査合格後、２次審査

✓ 年3回（3月・7月・11月）実施 （審査事務局：TELESA）

２次審査合格後、通知・マーク付与

※資格は1年更新。最初に審査した翌年の同月に更新申請→審査（3・7・11月）

- **料金**

新規審査料金	80,000 円	使用許諾申請書の提出迄にお支払い
更新審査料金	60,000 円	使用許諾更新申請書の提出迄にお支払い
マーク年間使用料	20,000 円	合格通知書を受け取った日から1ヶ月以内にお支払い

ISP版　設問抜粋(1)

安全安心

※　審査点に「必須」がついている項目は、その要件を満たす必要があります。点数は、その要件を満たしている場合に与えられる推奨点数です。必須29項目、推奨119点中92点以上（更新審査の場合、必須30項目、推奨114点中88点以上）で合格となります。ただし、7-1-1と7-1-2と7-1-3が0点の場合は不合格となります。

1　セキュリティポリシーの確立及び監査制度の導入

1－1　セキュリティポリシー及び監査体制が確立されていること。

1-1-1 （必須）

以下の内容が盛り込まれたセキュリティポリシー、又はそれに相当する内部規程がありますか？

- ＊　セキュリティポリシーの基本方針並びに適用範囲
- ＊　組織と体制
- ＊　重要情報と保護対策（情報機器廃棄時の対策を含む）
- ＊　評価と見直し
- ＊　運用と教育
- ＊　法令遵守、違反に対する対応

セキュリティポリシー、又はそれに相当する内部規程となる書類を提出して下さい。

1-1-2 （5点）

過去1年以内に、セキュリティポリシー、又はそれに相当する内部規程による監査が行われましたか？
行われた場合は、直近の監査報告書を提出して下さい。

（ほか　略）

ISP版　設問抜粋(2)

Safe Security ISP
安全安心

2　システムのセキュリティレベル

2－1　必要なセキュリティ対策が施されているか。

2-1-1　（必須）

インターネット接続サービスを提供するために使用されている、主なサーバ（DNS、メール、Web、認証、ルータ）について、別途定めるセキュリティ診断項目に記載の対策を施してありますか？
それを示すCVSS v2の基本評価基準が記載されているセキュリティ診断報告書（本申請書提出日の3ヶ月以内に行われたもの）を提出して下さい。
なお、提出にあたっては、深刻度がCVSS基本値7.0以上（Level III：危険）の脆弱性については、これらが検出されないか、または解消されていること。深刻度がCVSS基本値4.0以上（Level II：警告）の脆弱性については、事業者がそれらの脆弱性を認識し、自社のネットワーク運用環境を鑑みて、検出されたそれぞれの項目について、十分な検討・配慮がなされたことを示す責任者の意見書を提出すること、とします。

注1）　脆弱性診断は、CVSS v2 の基本評価基準（以下CVSS基本値）に対応したソフトウェアもしくはサービスを使用して脆弱性診断を行うこと、また、発見された脆弱性の深刻度の指標としてCVSS基本値が報告書に必ず記載されること
注2）　セキュリティ診断報告書には必ず「対応機器名・対応IPアドレス・FQDNの一覧表」を“鑑”として、ならびにセキュリティホールが検知されていてもバージョン情報等に基づく誤検知やFirewallのセキュリティポリシーによって問題がなければそれらについて記述した「要約レポート」を“鑑”として必ず添付すること

2-1-2　（必須）

施設への立ち入りは、適切な権限を持つものに限定されていますか？
その担当者による署名押印をお願いします。

（ほか　略）

ISP版　設問抜粋(3)･(4)

安全安心

3 トラブル発生時の対応体制の確立

3－1　障害発生時の体制が適切であるか。

3-1-1 （必須）

障害発生時における連絡体制がきちんと決められていますか？その書類を提出して下さい。

3-1-5 （5点）

以下に挙げるシステム･データのバックアップが適切に取られていますか？
取られている場合は、その担当者による署名押印をお願いします。

＊　顧客のアカウント管理情報、及び課金情報
＊　顧客が登録したデータ類

4 利用者向け契約約款等の整備と公表

4－1　契約時における契約約款の提示が適切であるか。

4-1-1 （必須）

約款等（会員になろうとする者に対して提示する契約約款や会員規約等をいう。）がありますか？
Webにて提示している場合は、トップページからそのURLまでの経路を記入して下さい。また、書面のみの提示の場合は、その書類を提出して下さい。

4-1-2 （必須）

会員になろうとする者に対して提供している重要事項説明書がありますか？
Webにて提示している場合は、トップページからそのURLまでの経路を記入して下さい。また、書面のみの提示の場合は、その書類を提出して下さい。

（ほか　略）

ISP版　設問抜粋(5)･(6)

Safe Security ISP
安全安心

5　ユーザ対応体制の整備

5－1　ヘルプデスクの設置は適切に行われているか。

5-1-3　（5点）

ユーザー対応業務のフローとマニュアルが整備されていますか？
整備されている場合は、そのご担当者による署名押印をお願いします。

6　利用者に対する周知･啓発等の取組み

6－1　会員に対して基礎的なセキュリティの啓発を行っているか。

6-1-1　（必須）

会員に対して、以下に例示するようなネット利用時の基礎的なセキュリティ情報を提供していますか？

- ＊　クレジットカード番号や個人情報等を送信する場合の注意事項
- ＊　認証パスワードの保護
- ＊　詐欺、取引上のトラブル例
- ＊　基礎的なウィルス対策方法
- ＊　常時接続時の注意事項

それを示すことができる書類を提出して下さい。または、それがWebにて閲覧可能な場合には、トップページからそのURLまでの経路を記入して下さい。

6－2　会員に対して最新のセキュリティ関連情報を提供しているか。

6-2-1　（必須）

会員に対して、最新のセキュリティ情報を発信していますか？それを示す書類を提出して下さい。

（ほか　略）

ISP版　設問抜粋(7)

Safe Security ISP
安全安心

7　個人情報保護に関する取組み

7－0　主務大臣により改善命令を受けていないか。

7-0-1　（必須）
主務大臣により改善命令を受けましたか？
受けていないことの確認のため、個人情報保護管理者本人の署名・押印をお願いします。

7－1　安全管理に係る取組みを適切に行っているか。

7-1-2　（0～5点、ただし0点の場合は不合格）
個人情報の持ち出し手段の制限について、コンピュータなど、機器から外部記憶媒体への記録の禁止等、具体的な取組みを行っていますか？
それを規定した当該文書を提出してください。

7－6　情報漏えい等が発生した場合の措置を策定しているか。

7-6-1　（必須）
個人情報の漏えいが発生した場合、事実関係を本人に速やかに通知する措置を策定していますか？その内部規程がわかる書類を提出してください。

7-6-2　（必須）
個人情報の漏えい等が発生した場合、二次被害の防止、類似事案の発生回避等の観点から可能な限り事実関係、その他有用な情報を公表する措置を策定していますか？
その内部規程がわかる書類を提出してください。

（ほか　略）

公衆無線LAN版安全・安心マーク

- ユーザが安全に安心して利用できる認定マークを目指す

  最低限の条件を満たした事業者等に付与

  不可視な無線空間を利用する際、安全なWi-Fiを選ぶことを可能に

  運営事業者の技術および運用レベルの底上げが図られる

- 審査対象

  公衆無線LANを運営する主体(自治体・団体等を含む)

  個別契約を持つISPでなくても取得可能

  自治体、レストランホテルなどのエリアオーナー等

審査項目（公衆無線LAN）

1　無線区間の暗号化またはその手法の案内
2.　ユーザー利用規約または契約約款等の整備と公表
3.　ログ情報・利用者情報等の取り扱いについて
4.　本人確認をしていることの確認
5.　ネットワークの制限について
6　ユーザーに対して基礎的なセキュリティの啓発を行っているか
7　セキュリティに関する取組み
8　災害時等の公衆無線LAN活用について
9.　個人情報保護に関する取組み

手続・料金

手続

１次審査は随時受付

✓ JAIPA・TELESA・TCAの３団体で受付けて一次審査実施

１次審査合格後、２次審査

✓ 年３回（3月・7月・11月）実施 （審査事務局：TELESA）

２次審査合格後、通知・マーク付与

※資格は1年更新です。最初に審査した翌年の同月に更新申請→審査（3・7・11月）

料金

取得料金	公衆無線LAN版
新規審査料金	30,000 円
更新審査料金	30,000 円

安全・安心マーク取得メリット

- 業界によって行われる一定基準の確認
  - ✓ 第三者によって社内体制がチェックされる
  - ✓ ISP、Wi-Fi提供事業者として必要な対策が分かる
  - ✓ 業界一体的な取組みへの参画

    法制度上のセーフハーバーでは無いが、一定基準を満たしている事をISP専門の第三者が確認する営み

- 付加特典
  - ✓ セキュリティ注意喚起情報提供　JPCERT/CCの注意喚起情報をメールにてお知らせ（無償）
  - ✓ セミナー優遇　情報セキュリティ政策会議後援「情報セキュリティシンポジウム」無償参加制度あり（数に限りあり）

最後に

皆様、安全・安心マークのご紹介は以上でございます。

協議会の具体的な取組み、詳細事項は、以下の協議会ホームページを参照願います。

https://www.isp-ss.jp/

また、遠方でも、オンライン会議等で、ご説明することは、可能でございます。

各種、お問合せは、以下の安全・安心マーク推進協議会の事務局メーリングリストまで、お気軽にお願い致します。

anan-sec@isp-ss.jp