資料３－２－３

情報通信ネットワークにおけるサイバーセキュリティ対策分科会第3回

地域ISPのサイバーセキュリティ対策の現状と課題

2023年3月16日

一般社団法人日本インターネットプロバイダー協会（JAIPA)

http://www.jaipa.or.jp/

一般社団法人日本インターネットプロバイダー協会（以下『JAIPA』）とは

主にインターネットプロバイダーからなる日本で唯一の業界団体です。
JAIPA会員は、

- **インターネット接続サービス(ISP）事業者**
- **クラウド、ホスティング事業者**
- **上記に対してセキュリティや情報通信インフラ構築等の各種サービスを提供する事業者**

など、インターネット関連事業者で構成されています。

JAIPAにおけるサイバーセキュリティ対策への取組

- JAIPAは「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」を策定している業界団体、「インターネットの安定的な運用に関する協議会」の一員として、2007年の発足当初から2018年まで協議会の事務局を務めてきました。
- また「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」の一員としても、設立当初から事務局を務めています。
- JAIPAにおいては、JPCERT/CCやNISCから定期的／不定期随時に提供されるサイバーセキュリティに関する情報を団体内で展開し共有しています。
- ICT-ISAC JAPANにはオブザーバーとして参加し、主に中小ISPのNOTICEへの参加などを促す活動を行ってきました。
- 毎年12月に開催されるICT業界における情報セキュリティのイベントSecurityDay主催団体の一員として、プログラムの策定や運営に関わっています。

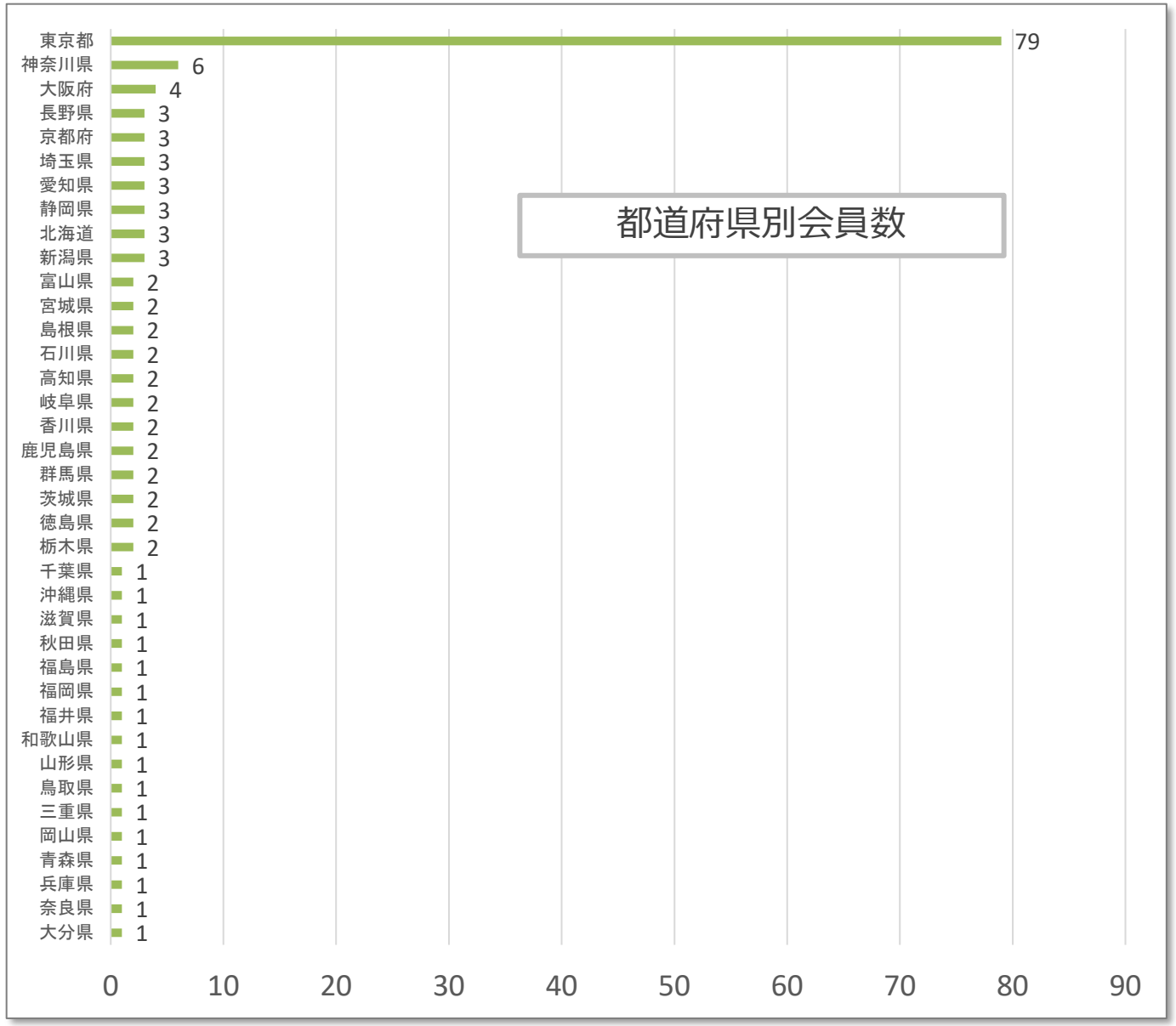
JAIPA概要

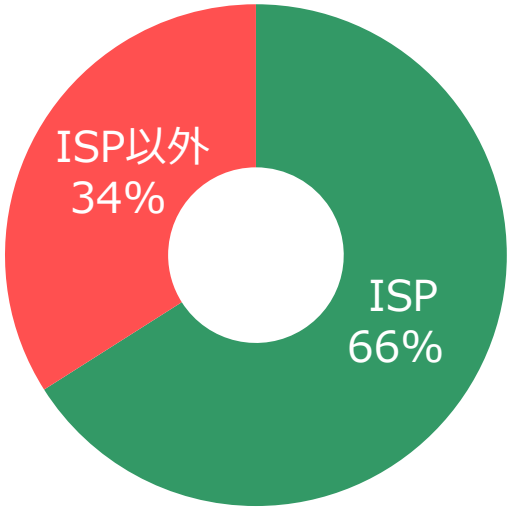
設　　立	1999年12月
会　員　数	147社（正会員 143社　賛助会員 4社）
ホームページ	https://www.jaipa.or.jp/
住　　所	〒151-0053 東京都渋谷区代々木1-36-1 オダカビル6F
連　絡　先	TEL：03-5304-7511 FAX：03-3379-5530
E-mail	info@jaipa.or.jp

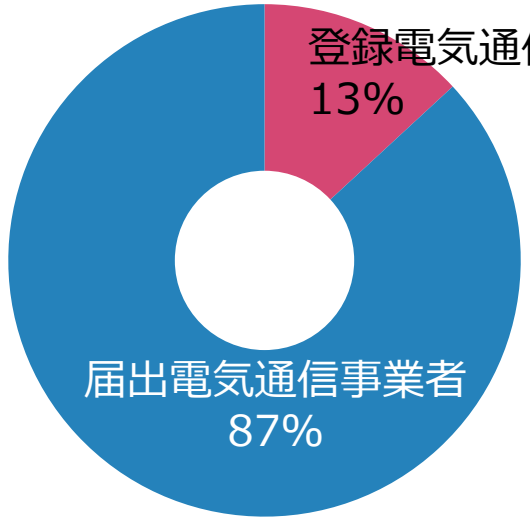
活動内容

- 年次総会、理事会
- 運営委員会
- 部会、ワーキンググループ
- 総務省研究会参画（意見書、プレゼンテーション）
- 業界統計情報の収集、分析、会員企業への情報提供
- 各種イベントを通じた会員同士の交流・情報交換機会の提供

JAIPA 会員数・会員種別　2020年8月現在







中小ISPにおいても最近多発のランサムウェア攻撃は他人事ではない状況

実際このような例も起きています。

WEBサーバーで発生しているサイバー攻撃による被害および状況についてお知らせいたします。

X月Y日未明、○○ネットのWEBサーバーが不正アクセスを受け、ホームページの更新や閲覧等に影響が発生いたしました。
同日、対策チームを立ち上げ、状況の把握や対策の検討を開始したところ、身代金要求型ウィルス「ランサムウェア」によるものと判明し、現在復旧に取り組んでおります。
X月Y+2日には、〇〇県警に被害の届出をしております。

なお、今回の「ランサムウェア」による被害に関して、情報漏えいは確認されておらず、メールサービス等にも影響はございません。

会員の皆様にご迷惑、ご心配をおかけしていることをお

早急な復旧を目指し、チームで尽力しておりますので、

数日後

WEBサーバーで発生しているランサムウェアによる被害の復旧状況についてお知らせいたします。

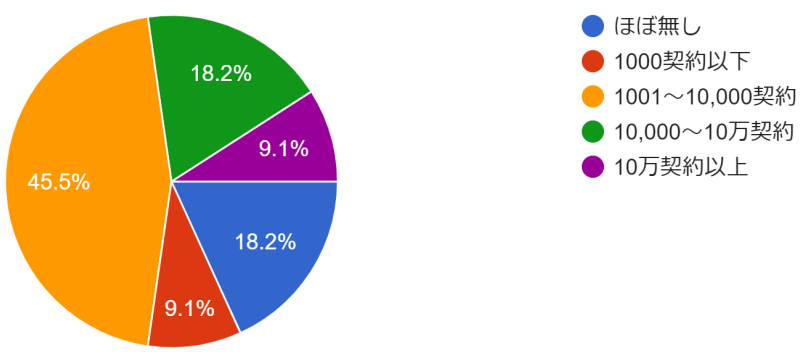
X月Z日午前1時頃より、WEBサーバーの一部が復旧し、順次回復作業を行っております。

会員の皆様にご迷惑、ご不便をおかけしていることを重ねてお詫び申し上げます。
全面復旧へ向けてチームで尽力しておりますので、ご理解のほどよろしくお願いいたします。

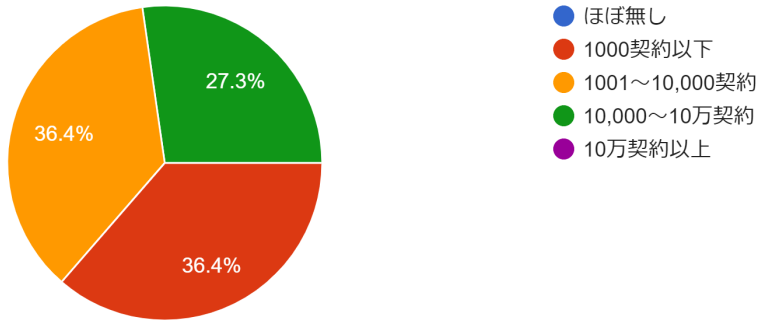
今回のプレゼンに際し、2月に会員に対しアンケートを実施しました。

主に地方で事業を展開する中堅、中小規模の事業者から回答をいただきました。
地域はほぼ全国に散らばっています。

個人利用者契約数



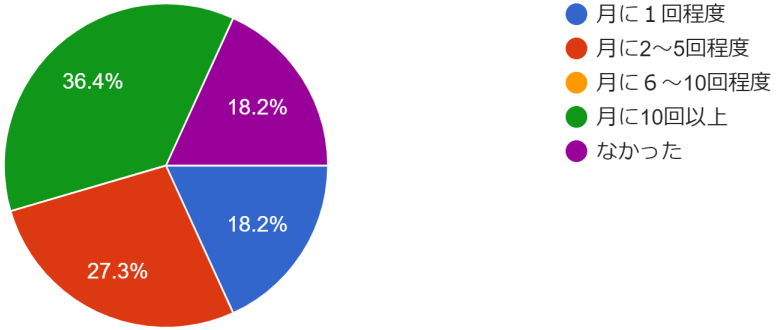
法人利用者契約数



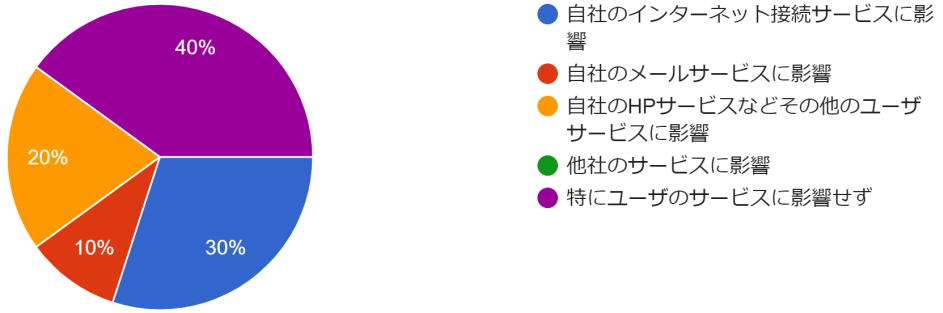
直近3年間のサイバー攻撃の有無

中小ISPに対しても想像以上に、かなりの頻度でサイバー攻撃が行われています。

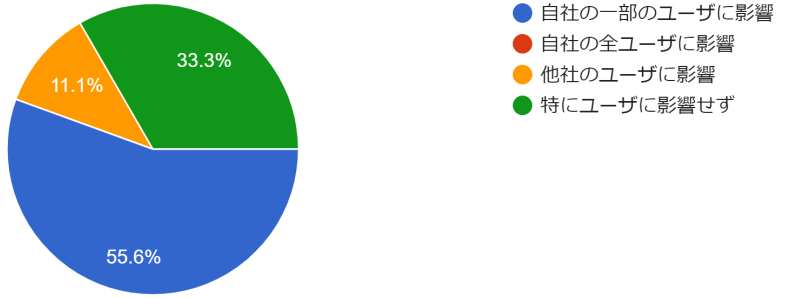
直近３年間に通信サービスに対するサイバー攻撃の有無



攻撃があったところのうち、攻撃の影響範囲



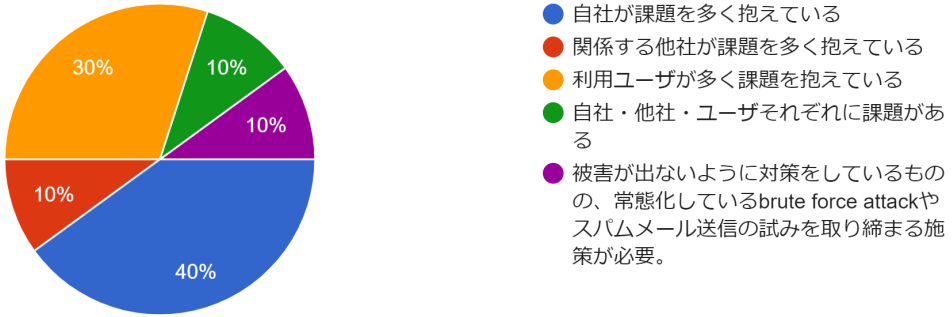
攻撃があったところのうち、攻撃の影響規模



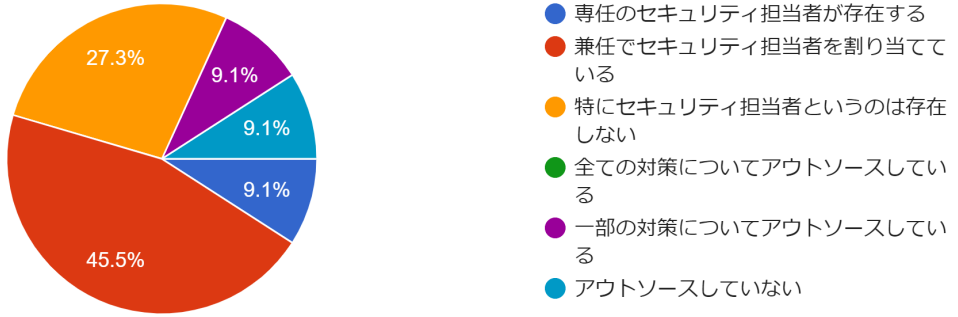
サイバーセキュリティ体制

中小ISPにおけるセキュリティ担当者は兼任か、担当者不在が多いのが現状で、課題感があります。

現在のサイバーセキュリティ環境について、どのように捉えているか。



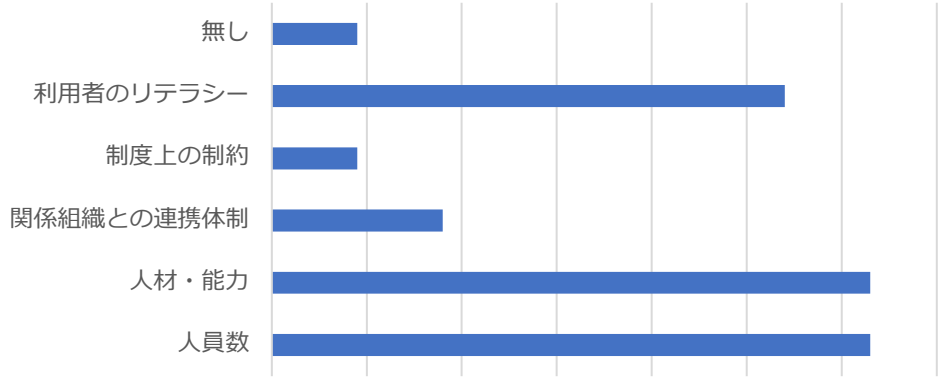
社内のサイバーセキュリティ体制



アウトソースについて

中小ISPでサイバーセキュリティ対策をアウトソースしているところはあまりありませんが、不正通信の検知とDDoS攻撃軽減装置の運用でアウトソースしているという回答がありました。

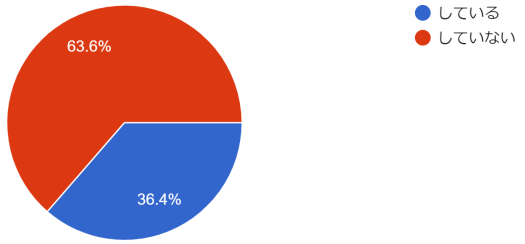
現在のサイバーセキュリティ体制の課題（%）



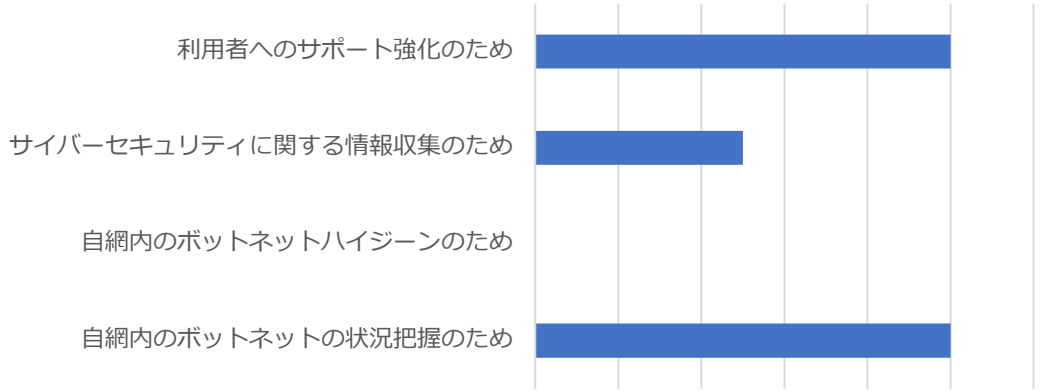
端末（利用者）側のサイバー攻撃対策の実施状況

中小ISPにおけるNOTICEへの参加状況はあまり高くありません。参加しているところでは年間数通から数十程度の通知を認定協会から受け、利用者に対して注意喚起しているとのことです。

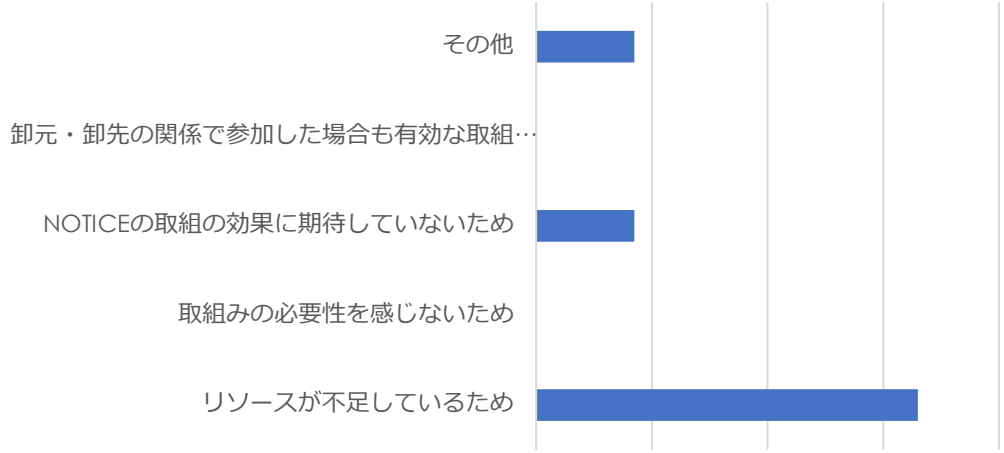
NOTICEに参加しているか？



NOTICEに参加する目的



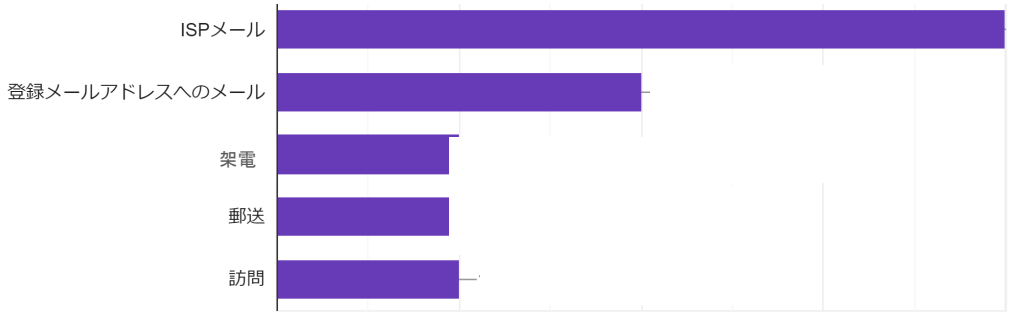
NOTICEに参加していない場合の理由や課題



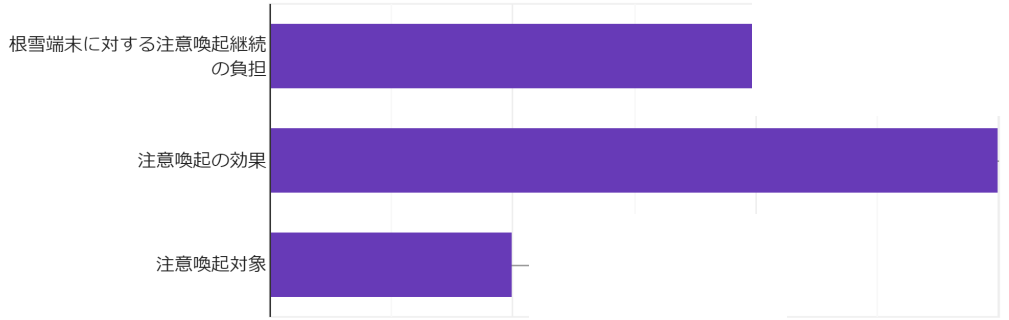
NOTICEの通知への連絡方法や課題感

ICT-ISACから通知を受けた場合は、主に利用者に対しメールで注意喚起していますが、負担や注意喚起の効果について課題としているところが多くみられました。

ICT-ISACから受ける通知があった場合に利用者に対して注意喚起する方法



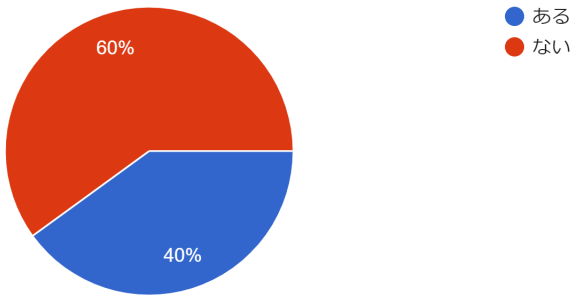
注意喚起にあたっての課題やその実効性を上げていくための方策やNOTICEに関する課題



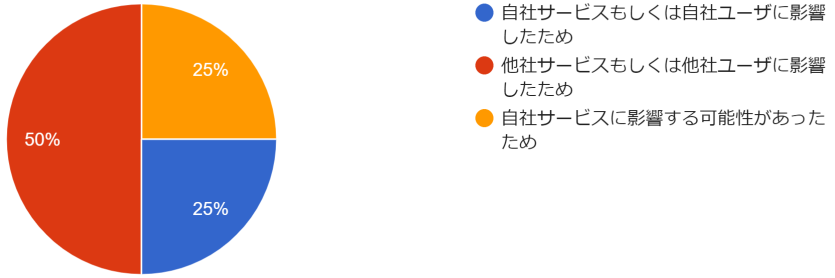
サイバー攻撃による接続の遮断や拒否

中小ISPで攻撃による接続の遮断や拒否を行ったところは少数ですが、行ったところではインターネット接続について、他社サービスもしくは他社ユーザーに影響があったため接続の遮断や拒否を行った状況であったことが分かりました。

サイバー攻撃による接続の遮断や拒否の有無



接続の遮断や拒否を行った理由

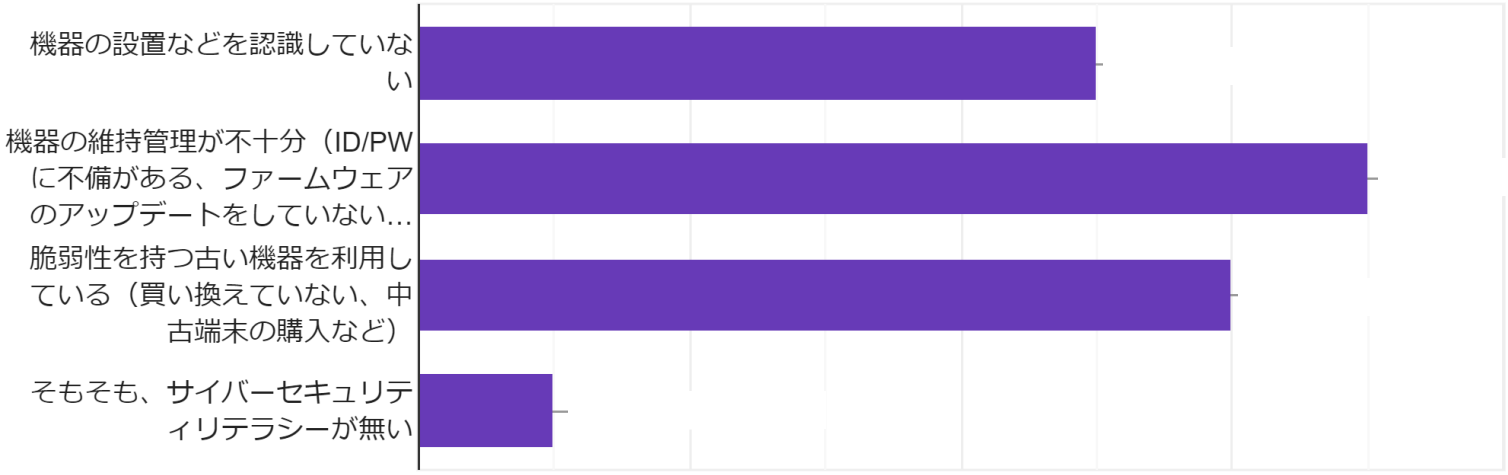


接続の遮断または拒否の内容

利用者端末のセキュリティ対策上の課題

利用者端末側のサイバーセキュリティ対策としては、機器の管理に関する課題が上がっています。

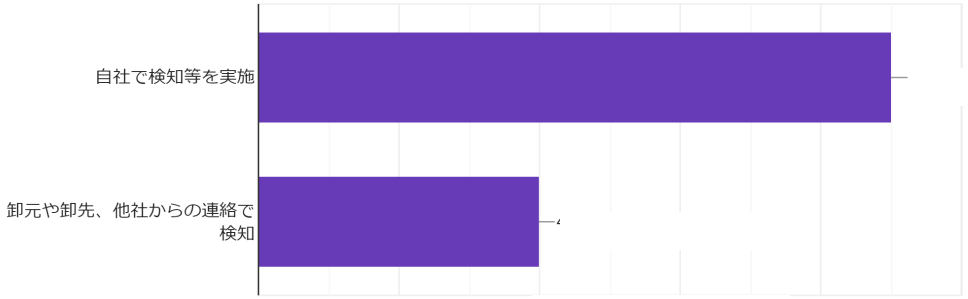
端末（利用者）側のサイバーセキュリティ対策上の課題には、他にどのようなものがありますか？



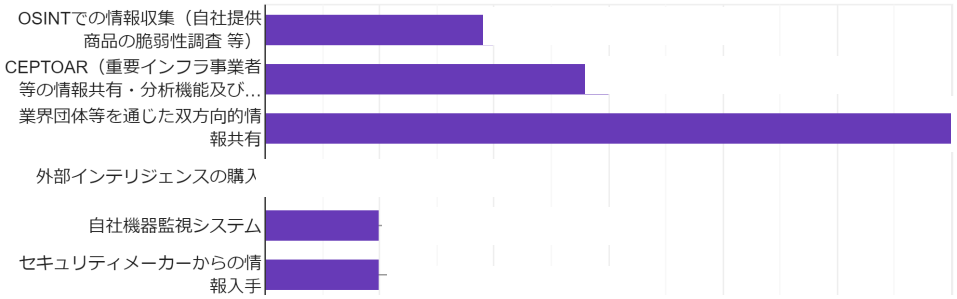
サイバー攻撃の検知、情報収集手法

サイバー攻撃の検知は自社で実施する一方、情報収集は業界団体を通じた取得を挙げるところが最多でした。

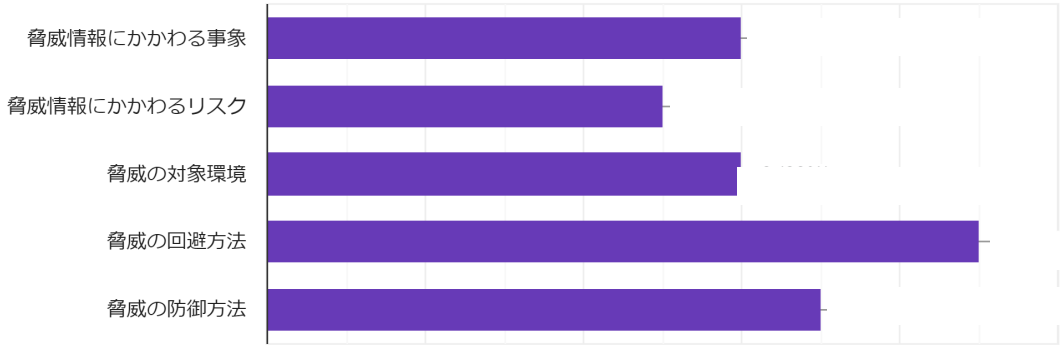
（平時）DDOS攻撃のような通信サービスの提供に支障を生じさせる可能性のあるサイバー攻撃をどのように検知しているか



現在貴社でサイバー攻撃に関する情報をどのような手段で収集していますか。



現在貴社でサイバー攻撃に関する情報が不足している場合、どのような情報が欲しいでしょうか。

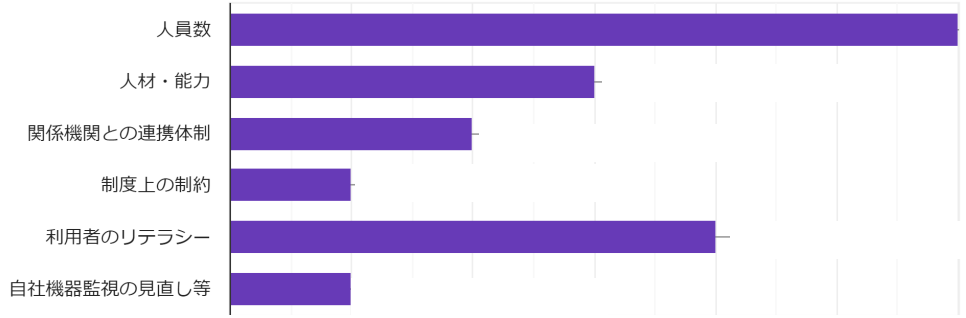


サイバー攻撃への対処能力向上に向けた課題、現在行っている対策

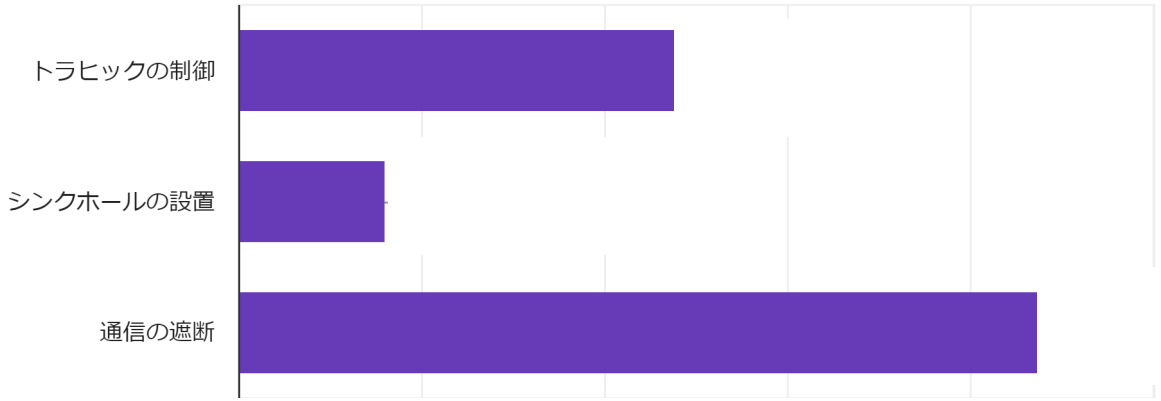
サイバー攻撃への対処能力向上対策としては人員数と利用者のリテラシーが最も多く上がりました。

自社の通信サービス提供に支障が生じる場合は、通信の遮断を行っているところも多くみられました。

サイバー攻撃の検知能力の向上、ネットワーク設備の増強や人材育成など、平時からサイバー攻撃対処能力の向上に向けてどのような対策を講じているか。その場合の課題は何か。



自社の通信サービスの提供に支障を生じさせる可能性のあるサイバー攻撃が発生した場合、トラフィックの制御、シンクホールの設置や通信の遮断など、どのような対策を講じているか。



サイバー攻撃対策を目的とした他のISPとの情報共有や連携

サイバー攻撃対策を目的とした他のISPの情報共有を実施しているところはほとんどありませんでした。

その他我が国のサイバー攻撃対処能力の向上に向けた課題や取り組むべき対策としては、以下のような感想、意見がありました。

- JPCERT/CCなどの機関が主導先導してISPからの情報収集や状況報告などを行ってもらえると良いと思います。 現在も個別に連携しているISPがあるようですが、グループのみに偏っており、日本としての動きが出来ていないと感じています。
- スパムメール送信、DDoS、brute force attack等の取り締まり強化と罰則強化。ISP間のセキュリティ事案情報のプロトコルやインターフェースの標準化が求められると思います。
- 外部からの異常通信へのアクセス遮断は正当防衛として対処できるものの、内部から外部へのアウトバウンド通信で問題らしいものを発見した際には、送信先からの求めがない場合は自社の緊急避難としては対処できないことに課題感があると思います。

最後に

地域ISPは、ユーザーに近いところに立地していいることから、ユーザーよりサイバー攻撃の場合を含め、各種相談が寄せられた場合に直接ユーザー宅等に出向いて対処を行う場合が良くあります。
そのため、エンドユーザーにおきる事象を直接把握、分析することができます。

法人顧客では、病院や病院に限らず企業で構内ネットワークの構築、管理を外部の会社に委託しているから大丈夫という認識しているところもみられ、危険性を感じています。

IoT機器の脆弱性を悪用した重要インフラへの攻撃が懸念されます。例えば、インターネットに接続されたHEMSの機器への攻撃で、家庭内の機器を操作し火事を起こしたり、こうした機器がターゲットになり太陽光発電の出力を制御し、ピーク時に発電能力全体の1%を操作できるとすれば日常生活に大きな影響があり、社会基盤インフラである発電網に対する大きな脅威となると考えています。端末側の対策をしっかりと行う必要性があると思われます。


JAIPA
JAPAN INTERNET PROVIDERS
ASSOCIATION