2018 AUTUMN 情報誌

日防設ジャーナル

●**法令解説**：古物営業の現状と古物営業法改正について
●**総務省のIoT機器を含む端末設備のセキュリティ対策について**
●**技術解説**：特殊詐欺等対策優良迷惑電話防止機器（優良防犯電話）

No.122
爽秋号

公益社団法人 日本防犯設備協会

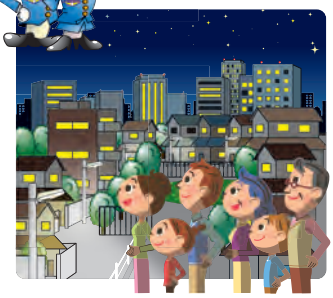
RBSSは防犯機器の安心マーク

RBSS（優良防犯機器認定制度）は公益社団法人 日本防犯設備協会が実施する認定事業です。

RBSSはRecognition of Better Security Systemの英文略称です。

防犯カメラ
デジタルレコーダ

LED防犯灯



優良防犯機器

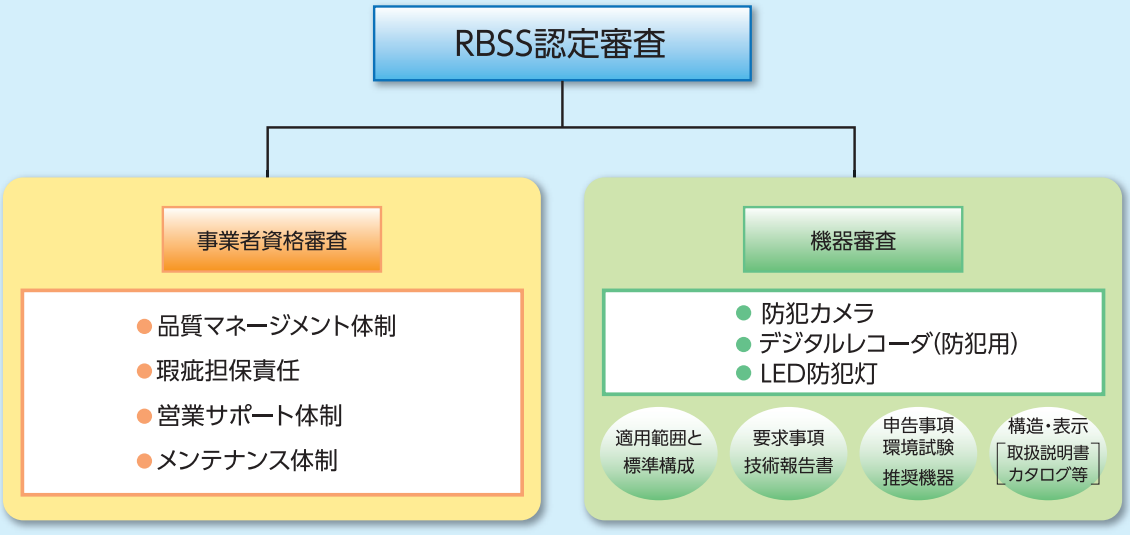
RBSS

公益社団法人
日本防犯設備協会

は、防犯機器の安心マークです。

RBSS（優良防犯機器認定制度）は、公益社団法人 日本防犯設備協会が一般の方々の安全・安心に寄与することを目的に、防犯機器に必要とされる機能と性能の基準を策定し、その基準に適合した機器を「優良防犯機器」と認定することにより、優良な防犯機器の開発及び普及促進を図る自主認定事業です。

- **申請事業者（企業）の資格審査と申請機器審査の2重審査認定ですので安心です。**



- **申請事業者の品質管理や企業姿勢及びサポート力などを審査します。**
- **各機器の防犯上に必要な機能・性能や環境対応及び表示などを審査します。**

日防設ジャーナル

2018 爽秋号 No.122

CONTENTS

巻頭言

「継続は力なり」

NEC プラットフォームズ株式会社　営業事業本部 営業推進本部
スマートアクセスソリューション営業推進部　シニアエキスパート　藤井　慶太

この度、防犯設ジャーナルの巻頭言執筆依頼を受け、不肖ながら筆を執ることとなりました。巻頭言は今回で3回目となり、既にネタが尽きた感がありますが、最後のネタとして今や私のライフワークとなった剣道を通して実感した「継続は力なり」という格言について触れてみたいと思います。

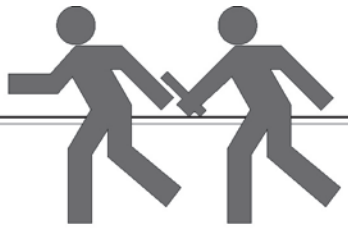
私と剣道の出会いは小学5年生のある日、幼いころから体が弱く病気がちであった私を心配した父が、父の田舎の屋根裏部屋に仕舞い込んであった剣道具を持ってきたことから始まりました。当時通っていた小学校の体育館で週に数回の稽古でしたが、もともと体力も無く、運動神経も悪く、腕前は遅々として上がらず、ただ、両親が言うには、他の習い事は休んだり止めたりしたが、剣道の稽古だけは休むこともなくせっせと通っていたそうです。

中学校に上がり、当時名門で名高い剣道部に迷いながらも入部し、怖い先生や先輩達に睨まれながら稽古に励みました。腕前は相変わらず下手な方から数人目といったところでしたが、私の中ではいつか皆に通用する面打ちを1本でいいから打てるようになりたいという目標を持ち、日々の稽古に励んでいたという記憶があります。そして、中学2年生も終わりの春休みのある日、本当に突然に、これまで全くできなかった面打ちが誰にでもほとんど一振りで当たる技を打てるようになったのです。そして、部内の勝ち抜き試合で十数人を勝ち抜きレギュラークラス入りを果たしました。小学5年生に剣道を始めて約4年、継続して努力してきた成果、続けてきてよかったと実感した最初の体験でした。

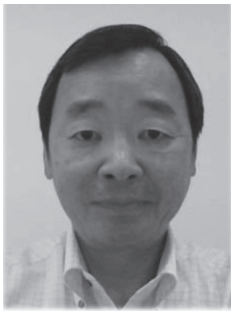
その後、高校、大学とも剣道部に所属し、社会人になるまで剣道を続けましたが、24歳のころアキレス腱を切ったことを機に剣を置き、私の剣道とのかかわりは一旦途切れてしまいました。それから30年が経った5年ほど前、小学生の長男が剣道を習いたいと言い出したため、私も剣道を再開することにしました。まず当たり前ですが直面したのは、すぐに息が切れる、竹刀が重くて振れない、体が思うように動かない、更には、腕や足の筋肉を痛めてしまうなど体力と気力の衰えでした。また、大学時代の剣道部のOB会や稽古会に参加してみると、剣道を続けていた当時の私から見れば大変失礼ながら格下であった同輩や後輩が、腕前もさることながら段位も6段、7段といった大先生になっているという現実でした。私も剣道を続けていればそのようになれたのか?はわかりませんが、この30年の間に継続して努力することを怠っていたことを実感し後悔することになり、今後はライフワークとして継続していくことを決めた次第です。

この剣道に関わる2つの体験を通して、継続して努力を続けることで成し遂げられる成果と喜び、怠ったための結果と後悔の両方、正に「継続は力なり」という格言を私なりに実感することができました。

継続といえば、私が日防設の活動に参加させていただいて10年ほどが経ちました。この間に運営幹事会や各種委員会活動などへの参加を通して協会の設立当初から30年間の活動の歴史を学ばせていただく機会を得ました。協会の活動に参加された多くの方々が、長年に渡り安全安心な社会に向けて弛まぬ努力を継続されてきたことに本当に頭が下がります。残念ながら私は今年度一杯で定年退職を迎え、協会活動への継続参加も終えてしまうことになりますが、今後も協会に参加されていかれる多くの方々により、安全安心な社会に向けた活動が継続されていくことで、大いなる社会貢献が成し遂げられていくことを祈念し私の巻頭言を〆させていただきたいと考えます。



『進化するガードマン（安全・安心のプロフェッショナル）』



セコム株式会社　執行役員
技術開発本部　本部長　　進藤　健輔

私は社会人になった際に、ガードマンを数年間経験しました。なかなか経験することがないと思いまして、今回、私の体験も踏まえ、ガードマンに関連した内容を紹介させていただきます。

都心の大きなビルディングやイベント会場、美術館、空港、重要施設には、凛々しく精悍な警備員を何人も見かけます。彼らは、そのビルディング等、重要施設やイベントの安全・安心を守るために、様々な教育を受け、使命感をもって職務に取り組んでいます。

警備員と言っても幅広く、「交通誘導」「雑踏」「空港保安」「施設」「巡回」と様々な役務によって分類されていますが、一般的に「交通誘導」を除いた警備員をガードマンと呼んでいます。

ガードマン、言葉の由来

このガードマンという言葉は、日本特有の呼び名であることはあまり知られていません。この呼び名の由来は、1965年4月～1971年12月の6年9カ月（全350話）にTBSテレビで放映された「ザ・ガードマン」（放映開始初期は、「東京警備指令　ザ・ガードマン」）からきていると言われています。

このテレビ放送は、当時とても人気があり、様々な個性の人がそれぞれに強くて、頭が切れ、カッコ良く、私も小学生の頃、毎週欠かさず見ていたことを記憶しています。

ガードマンへの期待

こうしたカッコ良い職業であるはずのガードマン職の求人倍率が、他の業種に比べ「きつい」…で敬遠され、非常に高い状況であることをよく報道で耳にします。

しかし、ガードマンは安全・安心のプロフェッショナルですから、庁舎・空港・発電所等多くの施設に配置されていますし、2020年の東京オリンピック等、大規模なイベントを控え、これから経済が発展する中、多くの施設・イベントにガードマンが必要になるのは明らかであり、ガードマンへの期待は非常に高い状況が続いていくと考えます。

ITを利用したガードマン

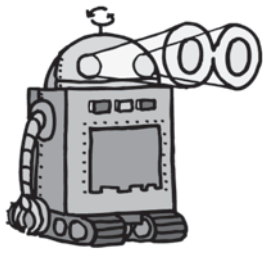
このような状況の中、近年の技術の向上と人員不足を補うために、ガードマンもITを利用した効率の良い警備の実現が進められています。例えば、従来は固定カメラによる周囲の画像監視が主体でしたが、現在では、ガードマンに装備されたウェアラブルカメラによる取得した画像を警備本部に無線送信

する装備が広がってきています。さらにその画像をAIによって処理することで、今までガードマン自身の経験やスキルによって判断されていたものが、その画像を取得することで、自動的に問題の抽出を行い、警備本部と情報を共有した連携対応ができるようになります。こうすることにより、迅速で的確な対応が、全てのガードマンにできるようになることでしょう。

ロボットと連携するガードマン

さらに今後は進化し、ロボットによる警備が現実のものになってきます。近年は、ロボット技術も向上し、ありとあらゆるところにロボットが入り込んでくると言われています。身近なところでは、掃除ロボットがありますが、利用者が増えています。

このように便利なロボットが身近になることと同じように、人員が不足している警備の世界にも広く導入されていくことが予想されています。



各種センサーを利用して、警備する監視場所を自律で走行し、搭載されているカメラやセンサーで侵入者を自動的にとらえるようになりますし、複数台のロボットを使用することで、きめ細やかな監視を行うことができます。

しかし、すべてがロボットでできるようになるにはまだ先になるとしても、現時点でもロボットができる業務もたくさんあることから、人とロボットが連携して警備を行うことが徐々に広がってゆくと感じています。今後は、ガードマンとガードロボ（私が勝手につけた名称）による効率よい警備が実現されていくと思っています。

ロボット警備への期待

最後に、私も入社してから数年間ある施設でガードマンをしていた時の経験をお話します。ある施設では、定期的に各種展示会が行われるエリアがあり、その展示物の警備を行っていました。展示物もさまざまであり、高価な絵画や茶器、宝飾品等が主な展示物でした。その展示物を昼・夜展示場内で警備を行っていましたが、その中でも現在も良く覚えている警備の経験をお話しします。その経験とは、季節が夏ということで幽霊に関する絵画の展示会の警備でした。展示物は、おぞましい顔をした幽霊から、とても幽霊とは思えないほど美しい幽霊（ずっと見つめると顔が変化するとのコメントがありました）まで、様々な幽霊画が展示されていました。昼間帯は、展示会場も明るく、鑑賞しているお客様がいるので、幽霊画も少し気持ちが悪いぐらいの感覚でしたが、夜間の巡回では、幽霊などいないとわかっていても本当に恐怖を感じました。当然仕事ですからしっかり巡回を行いましたが、大人になって通常とは違った怖さを感じたことをよく憶えています。

これからは、先ほど述べたように先進的なロボットが活躍していくことになりますので、人がこのような体験することが少なくなり、代わりにロボットが夜の巡回をこなしていってくれることでしょう。

様々な形で、ガードマンが進化してゆくこれからが大変楽しみです。

法令解説

古物営業の現状と古物営業法改正について

警察庁生活安全局生活安全企画課
課長補佐　石川　博昭

1 はじめに

古物営業法（昭和24年法律第108号）は、制定されてから70年近くが経過し、その営業態様等が大きく変化してきているとともに、規制緩和要望がなされるなど、事業者負担の軽減を図るなどの見直しを行う必要性が生じてきていました。

これらの状況を踏まえ、警察庁において法改正に係る検討を行い、平成30年の第196回国会において、古物営業法の一部を改正する法律案が提出・審議され、同年4月に成立・公布されました。

本稿においては、古物営業の現状や法改正に至る経緯を説明しながら、今回の古物営業法の改正概要についてご紹介します。

なお、文中の意見にわたる部分にあっては、筆者の私見であることを申し添えます。

2　古物営業の現状

（1）中古品取引市場の状況

ア 市場規模

中古品取引に係る市場規模は、環境省の「平成27年度使用済製品等のリユース促進事業研究会報告書」によると、一般消費者の最終需要ベースにおいて、推計で約3兆1,000億円（平成27年）となっています。これは、医療機器市場の約3兆3,700億円（平成27年。厚生労働省「薬事工業生産動態統計年報」）や宿泊産業市場の約3兆2,100億円（平成28年。公益財団法人日本生産性本部「2017 レジャー白書」）と肩を並べる市場規模となっています。

この中古品市場における主な業態としては、多い順に、自動車（57.6%）、バイク・原付バイク（6.6%）、ブランド品（6.0%）となっています。

なお、品目別で平成24年と27年の市場規模の増減率を比較すると、携帯電話・スマートフォンが＋113.1%、カメラ・周辺機器が＋53.2%、テレビ・洗濯機・冷蔵庫・エアコンが＋35.4%と、日常に使用する物の増加が著しくなっています。一方で、書籍が－20.9%、ソフト・メディア類が－18.1%と大きく減少しています。

イ 市場の構成

市場規模について、環境省が実施した消費者アンケート調査（前述の環境省報告書参照）を基にした世代別構成比を見てみると、「10～20歳代」が37%と一番多く、次いで「30歳代」の20%、「60歳代以上」の18%となっている一方で、「40歳代」が15%、「50歳代」が11%と少なくなっています。

これに対し、総務省統計局の人口推計（平成28年2月1日現在）を元に作成した人口の世代別構成比（「10～20歳代」（19%）、「30歳代」（12%）、「40歳代」（15%）、「50歳代」（12%）、「60歳代以上」（33%））と比べると、中古品市場において、「10～20歳代」の若者世代の構成比が突出しているのが分かります。

これは、新品にこだわらず、また、物を所有するのではなくシェアするといった若者の価値観の変化が一因と考えられます。したがって、今後、世代交代が進んでいくにつれ、ますます中古品の売買を行う者が増えていくとともに、中古品市場の規模も拡大していくのではないでしょうか。

(2) 古物営業法の目的

古物営業法の目的は、「盗品等の売買の防止、速やかな発見等を図るため、古物営業に係る業務について必要な規制等を行い、もって窃盗その他の犯罪の防止を図り、及びその被害の迅速な回復に資すること」とされています。これは、古物営業は、盗品等を取り扱う蓋然性が高い業態であるためであり、よって、古物商及び古物市場主は許可制とされ、取引の相手方の本人確認や不正品の疑いを認めた場合の警察への申告等の義務が課されています。また、インターネット・オークションにおいても、盗品等が売却されるおそれが高いことから、インターネット・オークション業者（古物競りあっせん業者）は届出制とされ、古物を売却しようとする者の本人確認の努力義務が課されています。

(3) 許可等の状況

古物商等の許可件数は、平成29年末において78万4,677件（古物商78万3,110件、古物市場主1,567件）となっています。また、インターネット・オークション業者の届出件数は、平成29年末において85件となっています。

(4) 古物商等に対する盗品等の処分状況等

既に述べたとおり、古物営業法の目的は盗品売買の防止等ですが、古物商及びインターネット・オークションにおいて盗品等が処分される事案は依然として把握されており、平成29年においても、盗品等の処分先としてこれらが利用された件数は、合計13,755件に上っています。

このように古物商等が盗品等の処分先として利用されるおそれが高いことから、古物商等に対しては、前述のとおり、不正品の疑いを認めた場合の警察への申告義務が課されていますが、これを端緒として窃盗の被疑者を検挙しているものが、平成29年には246件※となっています。また、警察が行う古物商等への手配、立入り等の捜査を端緒として窃盗の被疑者を検挙しているものが、平成29年には3,275件※となっています。

※窃盗犯検挙件数における主たる被疑者特定の端緒別の件数（解決事件を除く）。ただし、犯罪統計上、古物商等には、古物商及びインターネット・オークションに加え、質屋も含む。

3 古物営業法の改正

(1) 規制改革ホットラインへの要望

内閣府では、「規制改革ホットライン」という窓口を設け、日常生活・仕事や事業活動において不便を感じている、あるいは改善を図るべきと考える規制・制度に関する提案を受け付けているところ、古物営業に関する提案として、

○古物商の許可は、都道府県単位に申請を行うこととされている上に、申請から許可まで1か月半以上かかるため、許可権限を国家公安委員会に格上げをして全国共通の許可とする、または、既に一つの都道府県で許可を取得していれば、新たな都道府県では届出のみとして許可を不要とする措置を講じてほしい。

○古物営業を行うことができる場所として、集合住宅のエントランス等住居人以外が容易に侵入できない場所、居住者以外が容易に利用できないコンシェルジュカウンター、百貨店等におけるイベント会場を追加してほしい。

という規制緩和に係る要望がなされていました。

(2)行政手続部会の取りまとめ

政府の規制改革推進会議の行政手続部会が、規制改革、行政手続の簡素化、IT化を一体的に進めるため、平成29年3月に公表した「行政手続部会取りまとめ～行政手続コストの削減に向けて～」(平成29年3月29日規制改革推進会議行政手続部会)では、事業者の負担感が高い、「営業の許可・認可に係る手続」等の9分野を重点分野と位置付け、削減目標(「時間(事業者の作業時間)」の20%削減)の達成に向けて、各省庁において取組を進めていくこととされました。

(3)有識者会議の開催

前述のとおり、古物営業については、その営業形態が大きく変化し、規制改革ホットラインへの要望がなされるなど、事業者負担の軽減等の見直しを行う必要性が生じてきていましたので、このような現状を踏まえ、各方面の専門家の意見を聞きながら、現在のニーズに即した古物営業の在り方について検討を行う場として、平成29年10月から、「古物営業の在り方に関する有識者会議」(以下「有識者会議」という。)を開催することとしました。

有識者会議は、行政法等の学者、関係業界団体関係者、関係事業者及び消費者団体関係者により構成し、それぞれの経験・知見を元に、古物営業に係る各種課題について議論した結果として、同年12月に「古物営業の在り方に関する有識者会議報告書」が取りまとめられました。

4　古物営業法の改正概要

警察庁では、有識者会議の報告書の内容を踏まえ、古物営業法の一部を改正する法律案を立案し、第196回通常国会に同法案を提出して審議され、成立しました。以下では、主な改正項目について説明します。

(1)許可単位の見直し

これまでは、営業所等が所在する都道府県ごとに古物営業の許可を受けなければなりませんでしたが、今回の改正により、主たる営業所等の所在地を管轄する公安委員会の許可を受けていれば、その他の都道府県に営業所等を設ける場合には届出をすれば足りることとなりました。これにより、主たる営業所等の所在地を管轄する公安委員会の許可を受けていれば、新たな都道府県に営業所等を開設するに当たっての手続的負担が軽減されることとなりました。

(2)営業制限の見直し

これまでは、古物商は、営業所又は取引の相手方の住所若しく居所以外の場所で、買受け等のために古物商以外の者から古物を受け取ることができませんでしたが、今回の改正により、事前に公安委員会に日時・場所の届出をすれば、仮設店舗において古物を受け取ることができることとなりました。これにより、例えば、百貨店の催事場や集合住宅のエントランス等の一時的なイベント会場で古物の買取りを行うことができることとなります。

(3)簡易取消しの新設

これまでは、所在不明となった古物商等の許可を取り消すには、古物商が3か月以上所在不明であることを公安委員会が立証し、聴聞を実施する必要がありましたが、今回の改正により、古物商等の所在を確知できないなどの場合には、公安委員会が公告を行い、30日を経過しても申出がない場合には許可を取り消すことができることとなり、所在不明の古物商等の許可の迅速な取消しが可能となりました。

(4)欠格事由の追加

これまでは、古物営業法の許可の欠格事由に、暴力団排除条項が設けられていませんでしたが、古物営業法の目的は、盗品売買の防止等であることから、古物商等に課せられる各種義務の適切な履行ができない者が古物営業を営むことがないよう、今回新たに、暴力団員であることやその関係者であること、窃盗罪で罰金刑を受けていることを許可の欠格事由に追加し、これらの者を古物営業から排除することが可能となりました。

(5)施行期日

これら改正事項は、上記(2)～(4)の事項については、法の公布の日(平成30年4月25日)から6月を超えない範囲内において政令で定める日(10月24日)から、また、上記(1)の事項については、公布の日から2年を超えない範囲内において政令で定める日から施行することとされています。

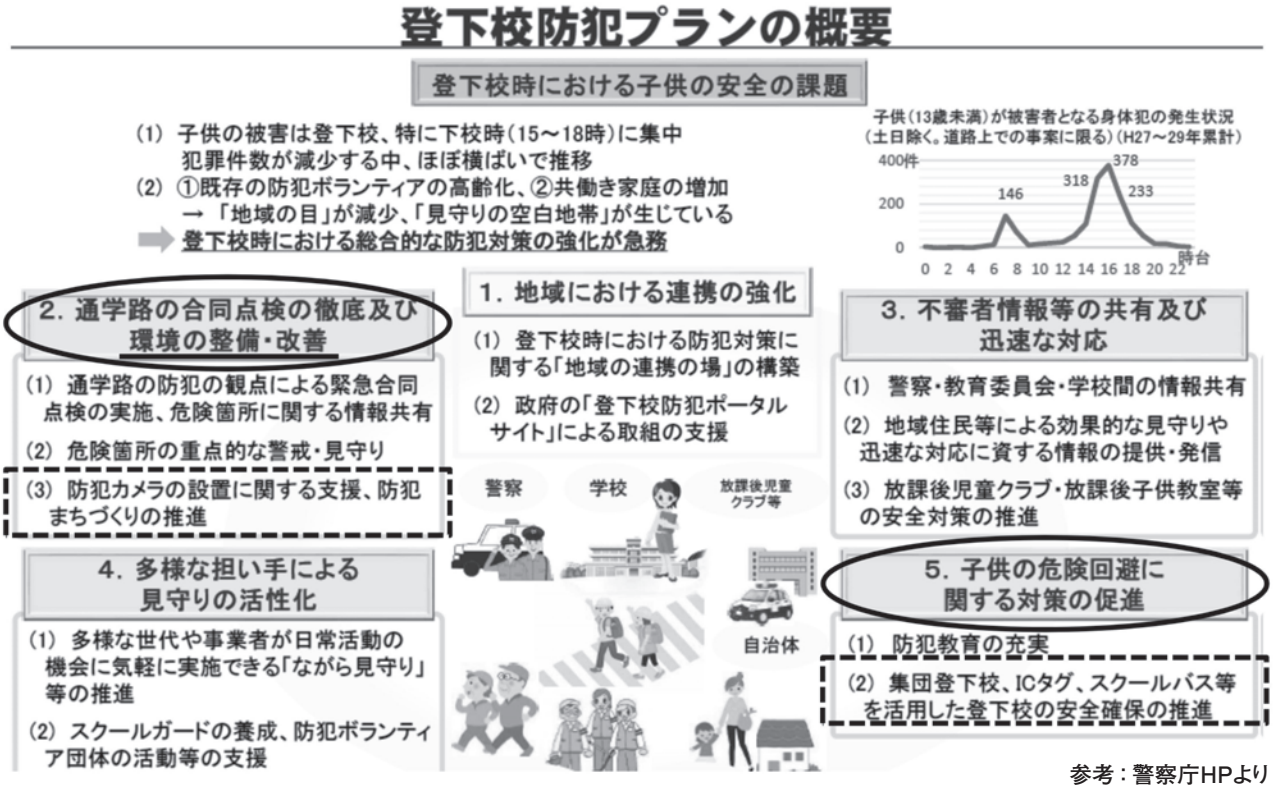
5　おわりに

今回の法改正の内容は、主として事業者負担の軽減となっていますが、一方で、簡易取消し制度の新設や欠格事由の追加なども組み込まれています。中古品の取引については、近年のフリマアプリ等の台頭など、その時代の流れに合わせ、その取引方法の態様に大きな変化が生じてきているところ、盗品等が流通するおそれが常につきまとってしまうことから、警察において中古品取引に関わる事業者としっかり連携を図るとともに、今後も、その時代にあった古物営業の在り方について、検討を行っていく必要があります。また、各事業者においても、自社の利益を追求するのみでなく、盗品売買の防止等に関する意識をしっかりと持って、それぞれの取組を進め、より良い古物市場が形成されていくことが期待されます。

登下校防犯プランの概要

平成30年5月、新潟県新潟市において下校中の女子児童が殺害される事件が発生するなど、依然として、通学路等において子供が被害者となる凶悪犯罪がおきています。政府は、これらの再発防止のため「登下校時の子供の安全確保に関する関係閣僚会議」を開催し、平成30年6月22日に「登下校防犯プラン」を決定し、また、平成30年7月11日には、警察庁生活安全局長より「通学路等における子供の安全確保のための対策推進について」通達が出されました。

今回は、これらの内容から、全国の地域協会で活動されている方や、防犯設備士、総合防犯設備士の方々に必要な情報を抜粋した形でご紹介いたします。



参考：警察庁HPより

①登下校防犯プラン

同プランでは、

「登下校時における子供の安全を確保するための対策については、地域の安全に大きく貢献してきた既存の防犯ボランティアが高齢化し、担い手が不足しているという課題がある。加えて、共働き家庭の増加に伴い、保護者による見守りが困難となっている上、放課後児童クラブ・放課後子供教室等において放課後の時間を過ごす子供が増加し、下校・帰宅の在り方が多様化していると考えられる。したがって、従来の見守り活動に限界が生じ、「地域の目」が減少した結果、子供が1人で歩く「1人区間」等において、「見守りの空白地帯」が生じている。」

とし、登下校時における総合的な防犯対策を強化することが急務であるとして、対策を取りまとめています。

大きくは以下5項目が上げられておりますが、「2.通学路の合同点検の徹底及び環境の整備・改善」及び「5.子供の危険回避に関する対策の促進」について抜粋紹介します。

1.地域における連携の強化
2.通学路の合同点検の徹底及び環境の整備・改善
3.不審者情報等の共有及び迅速な対応
4.多様な担い手による見守りの活性化
5.子供の危険回避に関する対策の促進

2.通学路の合同点検の徹底及び環境の整備・改善

登下校時における子供の安全確保のためには、関係者が連携して通学路の安全点検を緊急かつ確実に行い、「1人区間」等の「見守りの空白地帯」等の危険箇所を把握・共有した上で、下記(2)のソフト面と下記(3)のハード面の両面から、環境の整備・改善を行う必要がある。

このため、以下の対策に取り組む。

(1)通学路の防犯の観点による緊急合同点検の実施、危険箇所に関する情報共有

①教育委員会・学校、子供・保護者、見守りに関わる地域住民、警察、自治体、地方整備局、道路管理者、放課後児童クラブ関係者等は連携して、政府が示す要領を踏まえ、平成30年9月末までに、通学路の防犯の観点から緊急合同点検を実施する。

②関係者が連携して合同点検を実施する際には、例えば地域安全マップの作成等を通じ、危険箇所を「見える化」して情報共有し、環境の整備・改善につなげやすくするとともに、こうした作業過程を通じ、関係者の連携を実質的に深める。

(2)危険箇所の重点的な警戒・見守り

①緊急合同点検により把握された危険箇所について、警察官による警戒・パトロールを重点的に実施する。

②防犯ボランティア団体等、地域住民による見守りについても、危険箇所への重点的な配置にシフトすることにより、その効率的・効果的な実施を図る。

(3)防犯カメラの設置に関する支援、防犯まちづくりの推進

①緊急合同点検により把握された危険箇所に関し、上記(2)のソフト面での対策を補完するハード面での環境整備・改善策として、現場のニーズを踏まえ、通学路における防犯カメラを緊急的に整備するため、政府において必要な支援を講じる。

②地下通路、駐車場、公園等の公共施設の整備に併せ、安全性の確保等の施設管理上の観点から防犯カメラ、防犯灯、見通しの良い植栽・柵等を設置する場合、市街地整備の一環として、政府において、社会資本整備総合交付金等による支援を実施する。

③国土交通省等の小冊子「安全で安心なまちづくり～防犯まちづくりの推進～」を改訂するとともに、各地方整備局等に、防犯まちづくりに関する相談窓口を設置し、自治体における防犯まちづくりの取組を促進する。

④適切に管理されていない空き家の存在は防犯の観点から望ましくないため、政府において、空家等対策の推進に関する特別措置法に基づく取組、立地誘導促進施設協定制度の活用等を推進する。

⑤政府において、子供等を対象とした犯罪・前兆事案の発生状況を踏まえた地理的特性の分析などの調査研究を実施し、防犯環境整備の充実等に向けた取組を推進する。

5.子供の危険回避に関する対策の促進

登下校時における防犯対策については、子供を極力1人にしないという観点から、安全な登下校方策を策定し実施することが重要であり、例えば「見守りの空白地帯」における子供の危険を取り除くためには、様々な方策を組み合わせて対応する必要がある。

また、小学校低学年の子供に多くの役割を期待することは現実的ではないものの、子供自身にも、発達の段階に応じて、危険予測・回避能力を身に付けさせるための防犯教育を行うことは不可欠である。さらに、こうした能力を身に付けた子供が社会人となり、社会全体の防犯意識の向上や安全で安心な地域社会づくりに寄与することも期待される。

このため、以下の対策に取り組む。

(1)防犯教育の充実

①防犯の専門家の知見等も活用しつつ、例えば、地域安全マップ作りや防犯教室等を通じ、子供に危険予測・回避能力を身に付けさせる実践的な防犯教育を推進する。

その際、「子供110番の家」への駆け込み訓練や「子供110番の家」の実施主体との顔の見える関係の構築等により、実践的な防犯教育と地域における防犯意識の向上の両面から、「子供110番の家」の活用を推進する。

また、学校と警察が連携し、学年や理解度に応じ、紙芝居、演劇やロールプレイング方式等により、危険な事案への対応要領等について、子供が考えながら参加・体験できる防犯教室を引き続き開催する。

②防犯教育の担い手である教職員の研修を充実させ、指導力・安全対応能力を向上させるとともに、見守り活動を行うスクールガード等に対し、最新の知見の伝達や意識啓発を行うこと等により、質の向上を図る。

③保護者が、直接的な見守り活動への参加が困難な場合であっても、自宅周辺の「1人区間」の状況や「子供110番の家」の所在地等を子供と確認すること、子供が把握した不審者情報等を聞き出すこと等、家庭においてこそ効果的に果たせる役割を踏まえた防犯の取組を推進する。

(2)集団登下校、ICタグ、スクールバス等を活用した登下校の安全確保の推進

政府において、防犯ブザー等の活用、集団登下校・スクールバス等による安全な登下校方策の実施、ICタグを活用した登下校管理を始めとするICTを活用した防犯対策等、全国の様々な好事例について、実施に当たっての留意点等と併せて、「登下校防犯ポータルサイト」等を通じて周知することにより、地域・学校の実情に応じた、より効果的な安全確保の取組を推進する。

②通学路等における子供の安全確保のための対策の推進について(通達)

平成30年7月11日に警察庁生活安全局長より各都道府県警察の長宛に、政府の「登下校防犯プラン」決定に伴い、関係機関・団体及び地域住民等と連携して、通学路等における子供の安全確保のための対策を推進されたい、とした通達が出されました。

内容は以下4項目ですが、「3.関係機関・団体等との連携」について抜粋紹介いたします。

1.通学路等における警戒活動等の推進
2.不審者情報等の共有及び提供
3.関係機関・団体等との連携
4.防犯教育の推進

3.関係機関・団体等との連携

(1)登下校時における防犯対策に関する「地域の連携の場」の構築

教育委員会・学校、放課後児童クラブ・放課後子供教室、自治体、保護者、PTA、地域のボランティア、自治会等の関係者が集まり、登下校時における防犯対策について意見交換・調整を行う「地域の連携の場」に参画し、必要な助言等を行うこと。

(2)多様な担い手による見守り活動の推進

「持続可能な防犯ボランティア活動に向けた更なる支援の推進について(通達)」(平成28年3月17日付け警察丙生企発第52号)に基づき、見守り活動や青色回転灯装備車(青パト)によるパトロールを行う防犯ボランティア団体等に対し、積極的な表彰、活動の周知・情報発信、関係者との交流の場の提供等の各種支援を実施す

るとともに、日常生活や事業活動を行いながら、防犯の視点を持って見守りを行う「ながら見守り」等を推進すること。その際、通学路等において事業活動を行う自動車運送業者等（タクシー業者、宅配業者等）に対し、見守り等への協力依頼に努めること。

（3）「子供110番の家・車」等への支援等

危険に遭遇した子供の一時的な保護や警察への通報等を行う「子供110番の家・車」等の実施主体や、子供が立ち寄る施設、店舗、学習塾等の管理者等に対し、不審者等を発見した時の対応について、より実践的・具体的な指導・研修を行うとともに、見守りへの協力や不審者情報等の受信を依頼するなど、支援を強化すること。

（4）通学路等における環境面の改善

通学路や不審者事案の発生場所及びこれらの事案が発生する危険性のある場所については、教育委員会・学校、子供・保護者、見守りに関わる地域住民、自治体、地方整備局、道路管理者、放課後児童クラブ等と連携し、随時、防犯の観点による合同点検を実施するなどして、

○人や車の通りが少ない場所や見通しの悪い場所での見守り活動やパトロール等の実施
○防犯カメラの設置
○落書き消去等の環境美化活動
○公共施設の損壊改修や公共掲示板の掲示物等の整理
○歩車道間のガードレール等による分離
○沿道にある草木等の植栽管理
○駐車場や空き家等の侵入規制措置
○街路灯の設置や門灯の点灯促進
○子供110番の拡充
等、環境面の改善に努めること。

以上、政府の「登下校時の子供の安全確保に関する関係閣僚会議」の「登下校防犯プラン」及び警察庁生活安全局長からの「通学路等における子供の安全確保のための対策推進について」の通達について抜粋してご紹介をいたしました。詳細については、以下のURLで確認いただき、皆様の活動にお役立ていただければと思います。

■登下校防犯プランの概要
警察庁HP URL:
https://www.npa.go.jp/bureau/safetylife/bouhan/tougekou/tougekoubouhan.html
ホーム>内部部局から>生活安全局>登下校防犯プランについて

■通学路等における子供の安全確保のための対策の推進について（通達）
警察庁HP URL:
https://www.npa.go.jp/bureau/safetylife/bouhan/tougekou/300711anzenkakuho.pdf
ホーム>法令>通知・通達>生活安全企画課>通学路等における子供の安全確保のための対策の推進について

総務省のIoT機器を含む端末設備のセキュリティ対策について

総務省 総合通信基盤局 電気通信事業部
電気通信技術システム課
中山　貴博

近年、インターネットから操作可能な家電やスマートメータ等の利用が進む中、様々な分野においてIoT（Internet of Things）の普及が進んでおり、IoTサービスが国民生活に深く浸透しつつある一方、IoT機器に感染するマルウェア「Mirai」による大規模DDoS攻撃等により、インターネットに障害を及ぼす事案も増加している。今後普及していく様々なIoTサービスを誰もが安心して安定的に利用できるネットワーク環境を確保するため、総務省では、電気通信事業法上の観点からIoT機器を含む端末設備のセキュリティ対策について検討を行ってきた。本稿では本検討の背景や検討結果について概略を述べる。

1.検討の背景

民間調査会社（HIS Technology）の推定によれば、2015年時点でIoTデバイスの数は約154億個、2020年までには約2倍の約304億個まで増大すると予測されている。IoTの普及に伴い、IoT機器を踏み台とするサイバー攻撃も増加している。このように、近年サイバー攻撃等によりインターネットに重大な支障が発生する事例が増加していることを踏まえて総務省が開催した、「円滑なインターネット利用環境の確保に関する検討会」において、2018年2月、電気通信事業におけるこれらの障害への対処を促進するための「対応の方向性」が取りまとめられた。

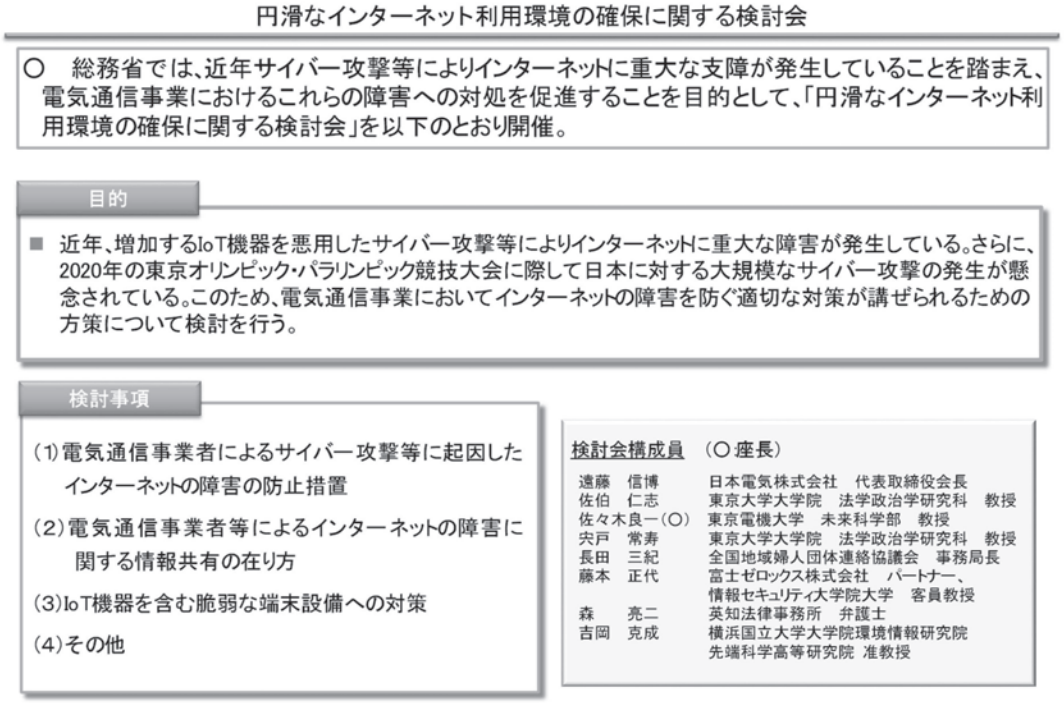


図1　円滑なインターネット利用環境の確保に関する検討会概要

「円滑なインターネット利用環境の確保に関する検討会」により取りまとめられた「対応の方向性」の概要は図2及び図3のとおりである。

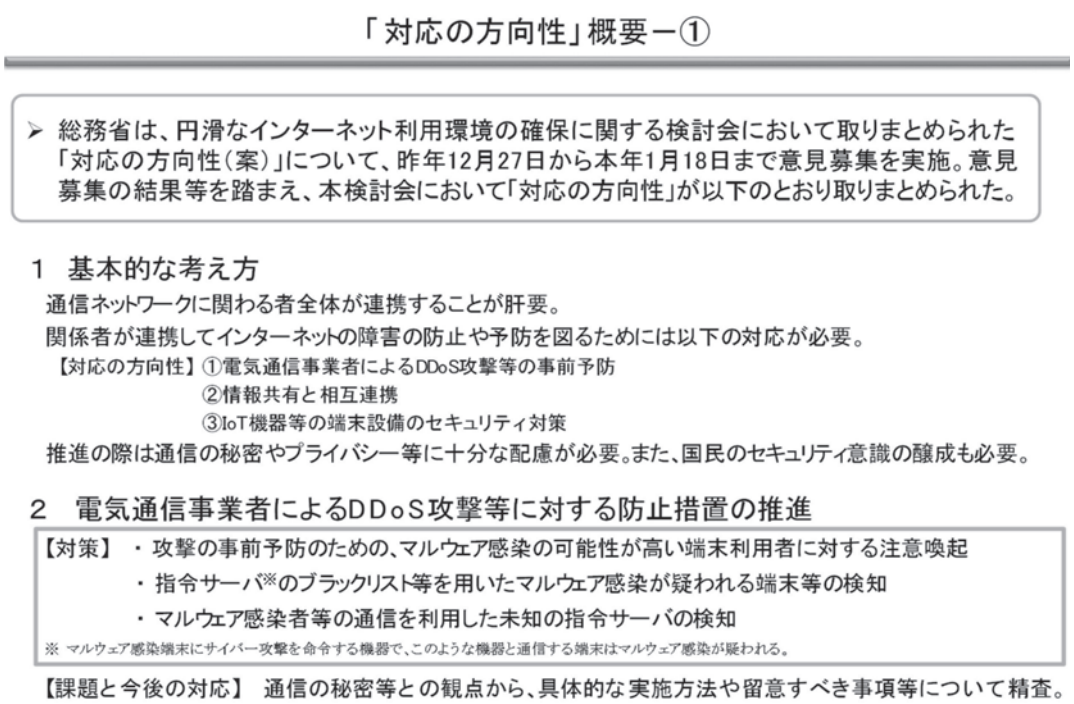


図2　円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要①

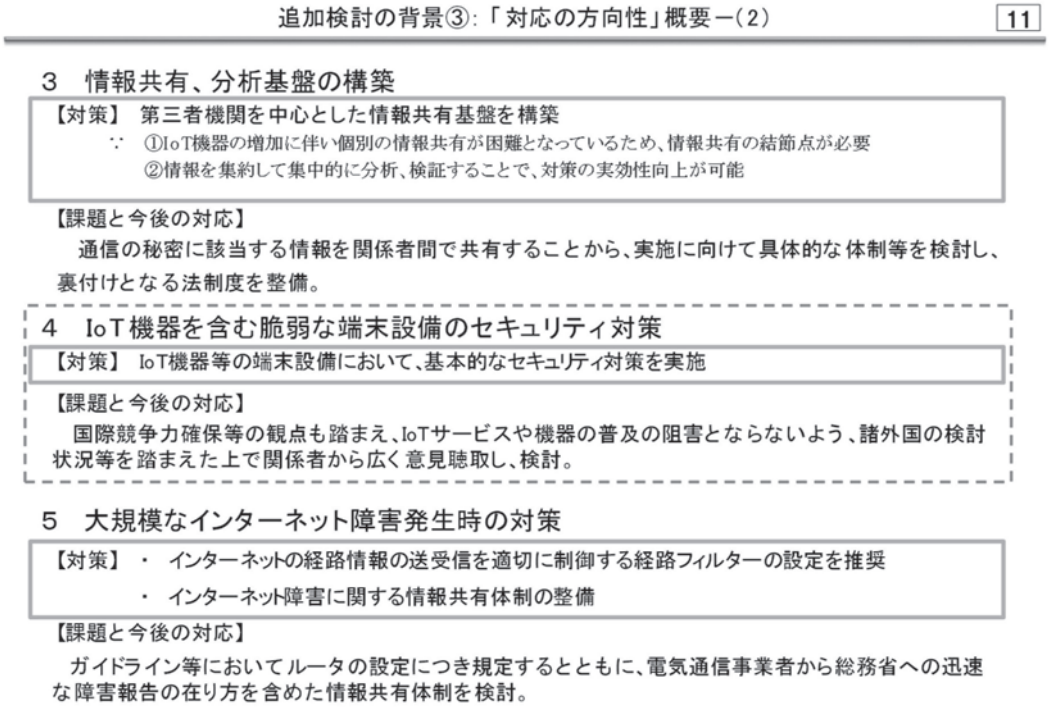


図3　円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要②

このうち、「IoT機器を含む脆弱な端末設備のセキュリティ対策」については、IoT機器等の端末設備において、基本的なセキュリティ対策を実施すべきとして、具体的な検討にあたっては、国際競争力確保等の観点も踏まえ、IoTサービスや機器の普及の阻害とならないよう、諸外国の検討状況等を踏まえた上で関係者から広く意見聴取し、検討することとされた。こうした結論を踏まえ、どのような対策が有効か、技術的な観点から専門的な検討を行うため、情報通信審議会情報通信技術分科会IPネットワーク設備委員会（以下「委員会」という。）において検討を実施した。

2.端末設備の接続の技術基準と端末機器の基準認証制度について

IoT機器に関連する電気通信事業法における制度として、利用者が接続する端末設備の接続の技術基準と、その技術基準に適合していることを認証する端末機器の基準認証制度がある。本節では、これらの制度について概略を説明する。

(ア)端末設備の接続の技術基準の考え方

電気通信事業法における「端末設備」とは、電気通信回線設備(図4のONU)の一端に接続される電気通信設備であって、一の部分の設置の場所が他の部分の設置の場所と同一の構内等であるものをいい、図4の例では、無線LANルータ、電話機、スマートTV、PC、スマートフォンの総体が端末設備となる。

電気通信事業法では、電気通信事業者の電気通信回線設備に接続して使用する端末設備について、次の事項を確保するものとして総務省令に定める技術基準に適合することを求めている。

- 電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること
- 電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること
- 電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界を明確であるようにすること

また、電気通信回線設備を設置する電気通信事業者以外の者が設置する端末設備以外の電気通信設備を「自営電気通信設備」といい、その接続の技術基準として、端末設備に係る技術基準が準用されている。

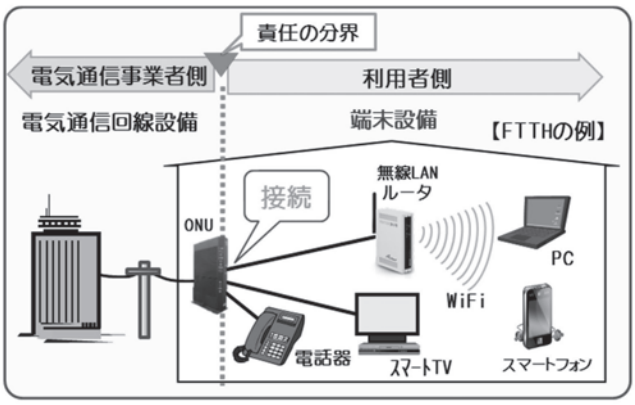


図4　利用者が接続する端末設備

(イ)端末設備の接続と技術基準の確保

電気通信事業者は、利用者から端末設備をその電気通信回線設備に接続すべき旨の請求を受けたとき、その接続が(ア)の技術基準に適合しない場合等を除き、その請求を拒むことができないとされている(電気通信事業法第52条)。

また、利用者は、適合表示端末機器(技術基準に適合している旨の表示(図5、いわゆる技適マーク)が付された機器)を接続する場合等を除き、電気通信事業者による接続の検査を受け、技術基準に適合する端末設備と認められなければ、当該設備を使用できないとされている(電気通信事業法第69条)。

さらに、利用者は、端末設備を電気通信回線設備に接続するとき、適合表示端末機器をプラグジャック方式等により接続する場合を除き、これに係る工事を工事担任者に行わせ、又は実地に監督させる必要がある(電気通信事業法第71条)。

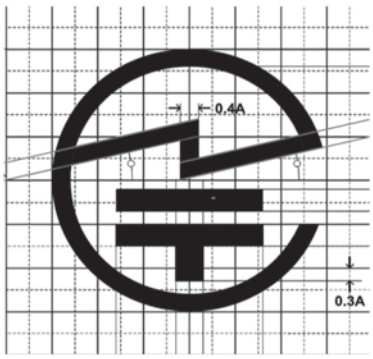


図5　技術基準に適合している旨の表示(電気通信事業法の認証では「A」又は「T」の記号が付される。)

（ウ）端末機器の基準認証制度

端末機器の基準認証制度とは、事業用電気通信設備に接続して使用される端末機器やその設計について、接続の技術基準に適合していることを登録認定機関等が認定する制度であり、

－端末機器を1台毎に認定する技術基準適合認定

－端末機器の設計を認証する設計認証

－製造者等が技術基準に適合していることを自ら確認し、総務省に届け出る技術基準適合自己確認

のいずれかの方法により認定等を取得することができる。認定等を取得した機器は図5の表示を付すことができ、当該表示が付された機器は適合表示端末機器となる。

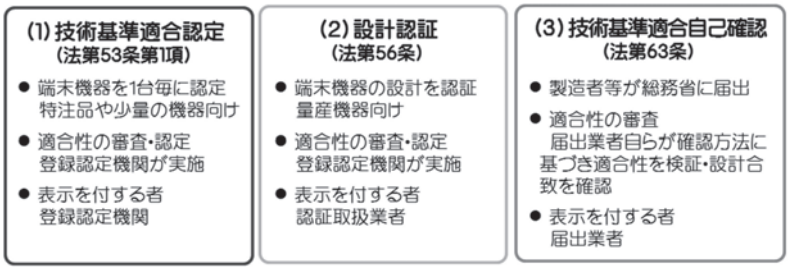


図6　技術基準適合認定等の取得方法

3.IoT機器を含む端末設備のセキュリティ対策について

近年、Webカメラやルータ等のIoT機器が乗っ取られ、インターネットに障害を及ぼすようなDDoS攻撃等のサイバー攻撃に悪用される事案が増加している。

一方、情報通信ネットワークの安全・信頼性を確保するために、電気通信事業法においては、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさない等を原則とする端末設備の接続の技術基準が定められている。

委員会では、そのような制度の枠組みの中で、大規模DDoS攻撃等のサイバー攻撃を抑止するため、IoT機器を含む端末設備がマルウェアに大量感染しないこと等を目的とするセキュリティ対策を技術基準に追加することについて検討を行った。

以下では、これらの検討をとりまとめた情報通信審議会一部答申「IoTの普及に対応した電気通信設備に係る技術的条件」（平成30年9月、以下「一部答申」という。）を基に説明する。

・端末設備の接続の技術基準にセキュリティ要件を追加する必要性について

近年増加しているマルウェア「Mirai」等による大規模DDoS攻撃を抑止するためには、ネットワークを提供する電気通信事業者、ネットワークの利用者、IoT機器のそれぞれで対応を行うことが重要となる。以下にそれぞれの対応の概略を説明する。

○電気通信事業者における対応

大規模DDoS攻撃については、電気通信事業者による対応が期待されることは言うまでもない。しかしながら、電気通信事業者は、電気通信事業法第4条に基づき、その取扱中に係る通信の秘密は侵してはならないとされていることから、原則として、通信内容を確認することは不可能である。このため、仮にIoT機器からの大量通信が発生した場合であっても、通信内容を確認して正常な通信なのか、DDoS攻撃に加担しているものであるか判別することができない。また、マルウェア感染したIoT機器のみの通信を止めることについても、技術面から困難であるため、電気通信事業者が取り得る対応も制約がある状況となっている。

なお、本年5月に成立した「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」により、電気通信事業者によるセキュリティ対策を強化するため、電気通信事業者による情報共有体制などの新たな取組みが導入されることとなっている。

○利用者における対応

大規模DDoS攻撃に対処する上では、IoT機器の利用者における対応も重要である。しかしながら、例えば機器メーカ等がソフトウェアの更新を呼びかけたとしても、技術的に対策が難しい、利用者が更新に気づかない等の理由で全ての利用者に対応を求めることは容易ではない。

更に、DDoS攻撃の踏み台となっている機器は、必ずしもその利用者に直接の被害が及ぶわけではないことから、IoT機器が目的どおり動作している限り、そもそも利用者は攻撃の踏み台となっていることを認知することが難しいという課題も存在する。

実際に過去の事例では、利用者に注意喚起を行った後、脆弱性のある機器の約8割に対処が行き届くのに約3年を要したものもあった。

以上のことから、利用者における対応についても限界がある状況となっている。

○IoT機器における対策

現在のIoT機器に対するサイバー攻撃は、グローバルIPアドレスを有する機器を対象として、セキュリティ上の不適切な設定や利用者に認知されていない脆弱性等を悪用したサイバー攻撃が多い。平成28年10月に、米国を中心に大手インターネットサービスの障害を引き起こしたマルウェア「Mirai」の事例では、本来不要な通信機能のアクセス制御のため、主に工場出荷時のID/パスワードをそのまま使用していたIoT機器が数多く乗っ取られ、大規模DDoS攻撃が行われた。このような事例でも、IoT機器において比較的に簡易なセキュリティ対策を行うことで大半の攻撃を防ぐことが可能である。

また、アクセス制限がない機器、ハードコーディングされたID/パスワードを持っている機器、既知の脆弱性が埋め込まれている機器等が出荷された場合には、その脆弱性を事後に修正することは困難なものとなる。そのため、出荷前に必要な対策を講じることが有効であると考えられる。

以上を踏まえ、一部答申においては、IoT機器を含む端末設備に対するセキュリティ対策として、電気通信事業法の枠組みの中で、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさないといった端末設備の接続の技術基準の原則の範囲内において、その技術基準にセキュリティ要件を追加することが適当とされた。

なお、当該セキュリティ要件は、電気通信事業法の観点からIoT機器のマルウェア大規模感染を防止することを目的としているものであり、IoTセキュリティを確保するためには、これらの対策だけでは不十分であることに留意する必要がある。

・IoTセキュリティ対策に関する国内外の動向

IoTセキュリティ対策については、現在、欧米等においても議論が活発に行われているところである。

米国においては、「ボットネット等の脅威に対するインターネットの強固性と通信のエコシステムの強化」に関する報告書が取りまとめられた。当該報告書では、IoTセキュリティに関し、初期設定及び自動ソフトウェアの更新機能などの重要性を指摘するとともに、機器の大半は国外に存在するため、国際的に認められた標準に基づくセキュリティの向上が重要であるとして、今後、具体的な施策の検討が行われていくことが見込まれる。

一方、欧州においては、ICT機器やサービスに対し、既知の脆弱性を含まないソフトウェアが提供され、安全にソフトウェア更新がおこなわれることを保証すること等を目的として、「ICTサイバーセキュリティ認証に関する規則案」が公表され、引き続き欧州議会で検討が行われているところである。

機器を対象としたセキュリティ認証に係る国際標準については、政府調達機器の一部に関し、国際標準ISO/IEC15408に基づくCC(Common Criteria)認証が行われている。CC認証は、世界28カ国で受け入れられている認証制度であり、複合機の例では、他の利用者による不正な操作や通信データの盗聴・改ざん、管理機能への不正なアクセス等を脅威として想定し、識別・認証・権限付与やアクセス制御、ファームウェアに電子署名を付すといった高信頼な通信等のセキュリティ機能を保証するとともに、セキュリティ機能自体の脆弱性評定も実施している。

IoTセキュリティ対策に関する国際標準は、ISO/IEC JTC1/SC27において検討が開始されたところであり、現時点で確立しているものではない。しかし、IoTのグローバル市場への展開や国際競争力確保といった観点から、CC認証をはじめとした国際標準との整合性を図るとともに、今後も、国際的な動向の把握に努める必要がある。

また、日本からは現在、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」の内容について国際標準の議論の場に提案が行われているところであり、今後も積極的に我が国の取組みを発信していくことが重要である。

・端末設備の接続の技術基準に追加すべきセキュリティ対策の内容

一部答申では、端末設備の接続の技術基準に追加すべきセキュリティ対策として、インターネットプロトコルを使用する端末設備であって、電気通信回線設備を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なものについて、大量感染を防ぐための最低限のセキュリティ要件として、アクセス制御機能、アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能及びファームウェアの更新機能、又はそれらと同等以上の機能を具備することを要件とすることが適当であるとされた。その具体的な機能については、表1のとおりである。

表1　端末設備に最低限必要なセキュリティ要件の具体的な機能

セキュリティ要件	具体的な機能
アクセス制御機能	・電気通信回線設備を介して接続されることにより当該端末が不正に操作されないことを目的として、当該操作の前にアクセス制御を行うことが必要。
アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能	・アクセス制御を識別符号によって行う場合は、当該識別符号が他人から容易に推測できないものとして設定されることを目的として、当該端末の利用者に対し当該識別符号について初期値の変更を促す（二以上の識別符号の組み合わせによるものの場合は少なくとも一つの識別符号が対象。以下同じ。）若しくは識別符号の初期値について機器毎に別のものを付す、又はそれらに準じる措置を行うことが必要。
ファームウェアの更新機能	・端末に記憶されている当該電気通信の送受信の機能に係るソフトウェアの更新が可能であることが必要。当該更新は安全かつ自動で行われることが推奨されるが、IoT機器は多種多様であり、更新の手法は機器の種別毎に異なることから、安全かつ自動の更新までは要件とはしない。 ・端末への電力供給が停止した場合であっても、当該更新されたソフトウェアや変更されたアクセス制御の設定内容を維持することが必要。
同等以上の機能	・CC認証などの国際標準に基づくセキュリティ認証を取得した複合機など、上記の機能と同等以上のセキュリティ機能を有すると認められるものについては、当該セキュリティ要件を満足するものとみなす。

なお、PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能であり、それにより上記セキュリティ要件に関する機能が出荷時とは異なるものになることが想定される機器については、当該セキュリティ要件を適用することが馴染まないことから、本要件の規定の対象外としている。しかしながら、その場合においては、利用者においてアンチウィルスソフトを導入する等の適切な対策を行うことが求められる。

・技術基準適合認定等の対象機器の範囲

セキュリティ要件が追加された技術基準に関し、当該技術基準に係る技術基準適合認定等を求める端末機器の範囲については、インターネットプロトコルを使用する全ての機器に対し、セキュリティ対策を求めることが理想的ではあるが、より効率的かつ効果的な対策とするため、一部答申では、セキュリティ対策を行うことが効果的な機器の範囲を明確にすることが適当としている。

マルウェアに感染しているIoT機器に関する研究では、感染機器の９割以上が不明であるものの、判明している範囲では海外製品のインターネットカメラ、デジタルビデオレコーダ、ルータ等が多い。国内製品においても、ルータ、ゲートウェイ、ネットワークストレージ、太陽光パネル管理システム、電力デマンド監視システムといった機器に感染事例が見つかっているという報告がなされている。

現在のIoT機器に対するサイバー攻撃は、グローバルIPアドレスを有する機器へのインターネット側からの直接的攻撃が主流であり、ルータ等の直接接続される機器に感染した後、更に家庭内の機器にまで感染活動を行うものは5%程度という分析事例がある。そのため、インターネット側からアクセスし操作可能なネットワークサービス（Web管理、telnet等）を使用する機器については、特に脆弱性対策が必要と考えられる。

現状の技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施しているが、上記を踏まえれば、現状においてネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが特に高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、一部答申では、セキュリティ要件が追加された技術基準適合認定等の対象についても、従来と同様に電気通信回線設備に直接接続される端末機器とすることが適当としている。

なお、直接接続される機器とは、電気通信回線設備に物理的かつ技術的に直接接続可能な端末機器を指すが、その中でも恒常的に既認定機器を介して接続する機器（屋外に持ち出す等により電気通信事業者の回線設備に直接接続して使用することを全く想定していない機器(例: 大型白物家電等)）については、今後、技術基準適合認定等の対象外とすることとされた。

ただし、この場合に利用者が認定等を取得していない機器を誤って直接接続しないようにするため、例えば、取扱説明書等において、①当該機器は既認定機器に接続する必要があることや、②電気通信事業者の電気通信回線設備に直接接続する場合には、電気通信事業者による検査が義務付けられていることを記載すること等をガイドライン等により明示することについて検討する必要があるとされている。

また、認定等を取得していない機器については、表1のセキュリティ要件を満たしていないおそれがある。こうした機器の乗っ取りを防ぐためには、IoT機器メーカやIoTシステム/サービス提供者等において、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」等に基づき、直接接続される既認定機器における対策も含む適切なセキュリティ対策を検討・実施していくことが必要となる。

今後、端末機器の接続が多様化することが想定される。認定等が必要な機器の範囲等については、一部答申の記載だけでは判断が難しくなる事例が出てくる可能性があることから、一部答申においては、機器メーカ等が判断できるように、ガイドライン等により明示することについて速やかに検討を開始する必要があるとされている。

・セキュリティ要件の追加に係る経過措置

端末設備の接続の技術基準へのセキュリティ要件の規定の追加が制度化された場合には、IoT機器メーカや登録認定機関等の対応を考慮して、一定の期間を設けて施行することとなるが、本件に関する改正について、その期間は1年から2年程度とすることとされている。

また、従来の制度に基づき、新制度の施行前に取得した技術基準適合認定等については、施行後も引き続き有効であり、当該認定等に基づく機器も引き続き使用することを可能とすることが適当とされている。

・技術基準適合認定等の審査方法等

登録認定機関等による技術基準適合認定については、セキュリティ要件の対象となる機器の審査が円滑に行われるよう、その審査方法や機器の審査単位等について通信事業者、機器メーカ等が参画可能な場で別途議論を行うことが適当であるとされている。

4. 今後の予定

一部答申を踏まえ、総務省では、3.のセキュリティ要件を端末設備の接続の技術基準に追加するための制度整備を行うこととしている。本制度整備による改正法令の施行後は、端末メーカ等において技術基準適合認定等を取得する場合には、セキュリティ要件にも適合する必要があることとなり、大規模DDoS攻撃等の抑止に寄与することが期待される。

また、ガイドライン等において明示することとされた、技術基準適合認定等を要する機器の範囲や端末機器の審査単位等については、今後、総務省において検討を実施し、ガイドライン等を策定・公表する予定である。こうしたガイドラインにより、端末メーカ等による技術基準適合認定等の取得に係る検討や手続が円滑に進むことが期待される。

本稿では、本年9月に取りまとめられた一部答申の内容を基にIoT機器を含む端末設備に関するセキュリティ対策について説明を行った。本文でも触れたとおり、今回検討を行ったIoT機器を含む端末設備のセキュリティ対策は、あくまで電気通信事業法の観点から大規模DDoS攻撃等を抑止するため、IoT機器のマルウェア大規模感染を防止することを目的としているものであり、個人情報の保護などのIoTセキュリティ全体を確保するためには、これらの対策だけではなく、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」等に基づき、適切なセキュリティ対策を検討・実施していくことが必要である。

技術解説

「特殊詐欺等対策 優良迷惑電話防止機器（優良防犯電話）」

公益財団法人全国防犯協会連合会　防犯部　防犯課長　島田　重夫

1.はじめに

急速に高齢化が進む中、特殊詐欺や悪質商法事犯等、高齢者の財産を狙った犯罪が後を絶たない状況にあります。

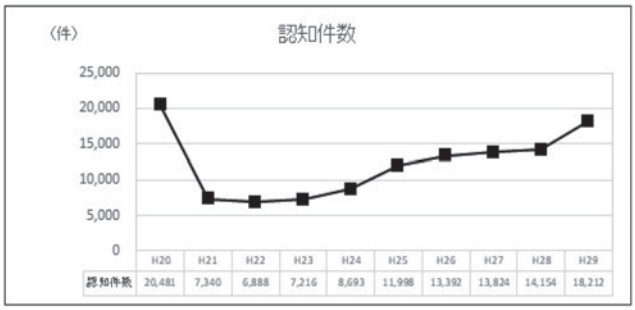
とりわけ特殊詐欺は、65歳以上の高齢者の被害が認知件数の7割を超え、オレオレ詐欺と還付金詐欺にいたっては9割を超えているなど、高齢者が特殊詐欺の標的になっています。

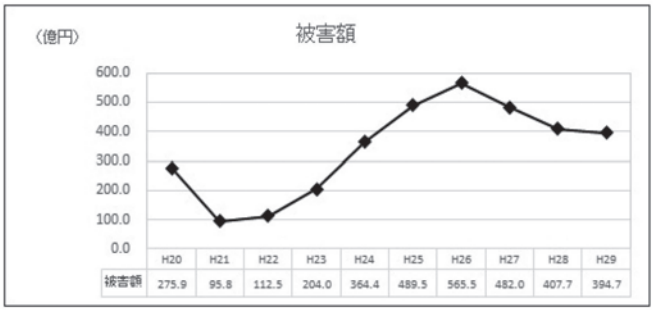
平成29年の特殊詐欺認知件数及び被害額は、18,212件（前年比29%増加）、約394億7000万円（前年比3%減少）となっており、被害の拡大に歯止めがかからない状況にあります。

「特殊詐欺」とは

面識のない不特定の者に対し、電話その他の通信手段を用いて、預貯金口座への振り込みその他の方法により、現金等をだまし取る詐欺をいい、振り込め詐欺（オレオレ詐欺、架空請求詐欺、融資保証金詐欺及び還付金詐欺）及び振り込め詐欺以外の特殊詐欺（金融商品等取引名目の特殊詐欺、ギャンブル必勝情報提供名目の特殊詐欺、異性との交際あっせん名目の特殊詐欺及びその他の特殊詐欺）を総称したものをいいます。

（警察庁より）





2.迷惑電話防止機能を備えた機器の活用

全国防犯協会連合会では、特殊詐欺など被害防止のため、平成29年4月から「優良迷惑電話防止機器（以下「優良防犯電話」という。）推奨事業」を始めました。（表1参照）

ほとんどの方が、特殊詐欺や悪質商法の種類や手口を知っていますが、電話に出ることにより騙されてしまっているのが実態です。

今まで、警察、行政、マスメディア及び防犯協会などのボランティア等が、特殊詐欺撲滅に向けた様々な対策を推進してきましたが、依然として認知件数、被害額とも高い水準で推移してます。

こうした現実を見ますと、特殊詐欺の被害を防止するための防犯広報・啓蒙活動の効果には限界があると言わざるを得ないところです。

特殊詐欺被害を未然に防止し、不要な電話をブロックするには、優良防犯電話の導入が最も効果的です。実際に、優良防犯電話を設置した方からの声では、特殊詐欺の電話はおろか、様々な迷惑電話がかかって来なくなったとのことです。

第4条　優良防犯電話の推奨基準は、次の条件を満たすものとする。

(1) 電話機又は電話機に容易に取り付けることが可能な外付け機器であって、次のいずれかの機能を有するものであること。
　ア 電話の着信時に、電話の相手方に警告音声を発する機能を有し、かつ、通話中に自動的に通話内容を録音する機能
　イ 迷惑電話番号データベース(警察、自治体等から提供された迷惑電話番号のデータベースであって、着信拒否を判別するための電話番号情報が逐次蓄積されるものをいう。)に登録された情報により、迷惑電話番号からの電話を自動判別して着信を拒否又は着信ランプ等で警告表示する機能
(2) 耐久性を有し、正常に作動するものであること。
(3) 高齢者等が使用するに当たって、操作が容易にできるもの。

◆「優良迷惑電話防止機器シール」

◆全国防犯協会連合会のホームページ

http://www.bohan.or.jp/suishou/denwa.html

(表1)全国防犯協会連合会の推奨の基準

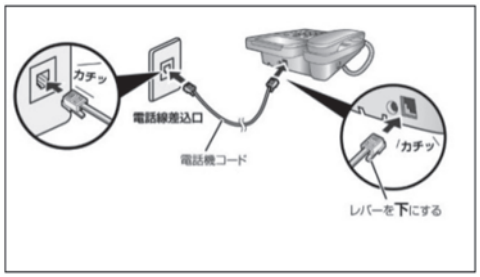
3.優良防犯電話の種類

(1) 警告・通話録音機能を使用するもの

◎動作概要

現在、使用している電話機を迷惑電話防止機能のある電話機に交換するか(ア)、または、外付け機器を接続して使用します(イ)。

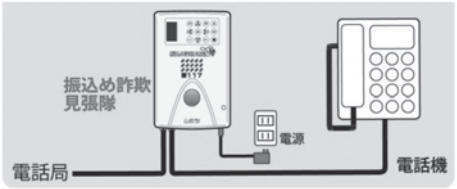
ア　迷惑電話防止機能付き電話機



接続系統図

迷惑電話防止機能付き電話機

イ　迷惑電話防止機器(外付け)



接続系統図

電話がかかってくると本機が応答して、「この通話は迷惑電話防止のために録音されます。ご了承ください。」等の警告音声を流します。警告音声が終わると、電話機を呼出し、通話内容が自動的に録音されます。（機種によっては、「ただ今、お名前確認モードになっております。呼び出しますので、恐れ入りますがあなたのお名前をおっしゃってください」と音声が流れます。）

受けたくない場合は、「拒否する」を選ぶと「この電話はお受けすることができません。」と警告音声が3回流れ、自動的に切断します。

ナンバー・ディスプレイを契約（有料）し、本機に事前登録した電話番号と照合することにより、「この電話は、お受けすることができません。」や「恐れ入りますが、電話番号の前に186を付けてダイヤルするなど、番号を通知しておかけ直してください。」と警告音声を発し、自動的に切断する機能を使うことが可能になります。

本機能により、不要な電話に対応する必要がなくなります。

【ナンバー・ディスプレイとは】

かけてきた相手の電話番号が、電話に出る前に電話機等のディスプレイに表示されるサービスです。誰からかかってきたのか確認してから電話に出ることができるため安心です。

（NTT東日本より）

◆拒否登録した電話番号から着信した場合

「おかけになった電話番号からはお繋ぎできません。」と警告音声を再生します。電話機は鳴りません。

◆許可登録した電話番号以外から着信した場合

「振り込め詐欺等犯罪被害防止のため、会話内容が自動録音されます。」と警告音声を再生し、通話内容が自動的に録音されます。

(2) 迷惑電話番号データベースを使用するもの

◎動作概要

現在、使用している電話機を迷惑電話防止機能のある電話機に交換するか（ア）、または、外付け機器を接続して使用します（イ）。なお、本機能を使用する場合は、ナンバー・ディスプレイ契約（有料）、及び迷惑電話フィルタサービス利用料（有料）、データ通信料（迷惑電話防止機能付き電話機の場合）が必要となります。

本システムを採用した優良防犯電話にかかってきた電話番号と迷惑電話番号データベースを照合することで、振り込め詐欺などの迷惑電話と自動的に判別して着信を拒否します。

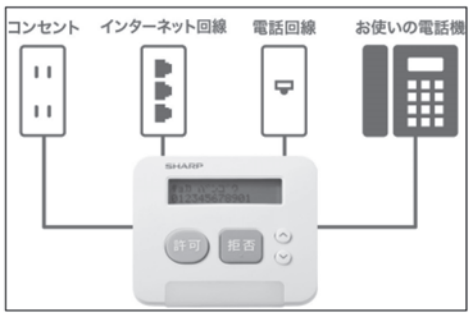
着信すると（LED発光部の色で）着信電話番号の安全度が事前にわかります。

ア 迷惑電話フィルタ機能付き電話機

接続系統図は、迷惑電話防止機能付き電話機と同様です。

対応電話機

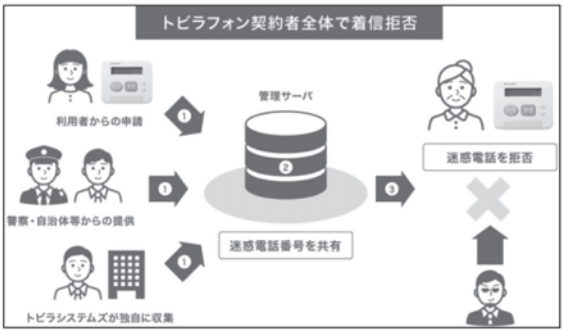
イ 迷惑電話フィルタ機能（外付け）



接続系統図

迷惑電話番号データベース（迷惑電話番号情報）は、特殊詐欺や迷惑電話に使われた電話番号など同じ機器を使用するユーザからの収集、警察、自治体等からの提供、及びトビラシステムが独自に収集したリストをデータベースとして活用するものです。

迷惑電話番号データベース登録件数は、約25,000件で毎日更新されています。



「迷惑電話番号データベース収集概要図」

◆迷惑電話・拒否番号から着信した場合

「この電話はお受けすることができません。」と3回警告音声を発し、自動的に切断します。

【赤色のLEDが点滅】

◆非通知から着信した場合

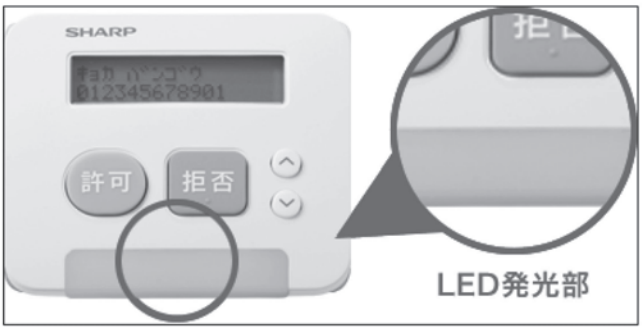
「恐れ入りますが電話番号の前に186を付けてダイヤルするなど、番号を通知しておかけ直しください。」と3回音声を発し、自動的に切断します。

【黄色のLEDが点滅】（内蔵タイプは赤色）

◆許可登録者から着信した場合

安心して電話が受けられる電話番号であることが分かります。

【緑色のLEDが点滅】



迷惑電話フィルターボックス

電話番号の種類	分類	本機		接続している電話機の着信音
		LED	着信動作	
迷惑電話番号リストに登録された電話番号	危険	赤	拒否（メッセージお断り）	×
ご自身で拒否登録した電話番号				
非通知からの着信				
表示圏外			拒否しない	○
公衆電話	注意	黄		
0120／0800から始まる電話番号				
表に記載の項目以外の電話番号				
ご自身で許可登録した電話番号	許可	緑		

迷惑電話フィルタLED発光部の表示

（出所）

（株）オンキヨー&パイオニア、シャープ（株）、ソフトバンク（株）、東芝エルイートレーディング（株）、トビラシステムズ（株）、パナソニック（株）、（株）レッツコーポレーション

4.特殊詐欺事例集

以下に、事例を紹介しますが、このような電話を取らなくてすむようにするのに「優良防犯電話」は大変効果的です。是非活用いただき詐欺被害防止に役立ててください。

◆「キャッシュカードを預かります」は詐欺!

警察官、銀行協会などを名乗る犯人から電話があり、「あなたの口座が事件に悪用されています」「新しいキャッシュカードに作り直した方がいい」「今から自宅に取りに行きます」「手続きに必要なので暗証番号を教えてほしい」などと言ってきます。

電話を受けた被害者は、その言葉を信じてしまい、暗証番号を教え、自宅に訪ねてきた銀行協会の職員などになりすました犯人にキャッシュカードを渡してしまい、だまし取られるのです。

キャッシュカードを受け取った犯人は、コンビニエンスストアや銀行のATMを操作してお金を引き出す手口です。

◆「コンビニで、支払い番号を言ってお金を支払って」は詐欺!

インターネットサイト事業者などを名乗る犯人から、「インターネットの未納料金が発生しています」「本日中に電話連絡がない場合には裁判になります」「○○番まで電話をかけてください」などとメールが送付されてきます。

メールを受け取った被害者は、不安になり、記載された電話番号に電話をかけると、業者を名乗るものが出て「インターネットの未納料金が○円あります」「○日までに支払わないと裁判になります」「コンビニエンスストアで、今からお知らせする『支払番号』を店員に言って支払ってください」などと言ってきます。

被害者は、その言葉を信じて犯人の要求どおりコンビニエンスストアで支払番号を言って支払ってしまいます。

犯人は、あとで換金しやすい商品を購入し、その代金を被害者に支払わせるという手口です。

◆「お金が戻るからATMに行け」は詐欺!

自治体、税務署、年金事務所の職員など名乗る犯人から電話があり、「医療費(保険料)の払戻しがあります」「お知らせの書類はご覧いただけましたか」「手続きが今日までです」などと言ってきます。

さらに「医療費(保険料)を受取る口座を教えてください」「今日中の手続きとなります」「○○駅前のATMに着いたら携帯電話で電話をかけてください」などと言ってきます。

お金が返金されると信じた者は、急いで指示されたATMへ行き、携帯電話で電話をかけると、「こちらで手続します」「説明どおり画面のボタンを押してください」などと言われます。

犯人は、「あなたの受付番号(パスワード)は、○○……番です」などと言って、被害者に振り込みの操作だと気づかれないように送金額を入力させて、犯人が管理する口座に振り込ませる手口です。

注目商品

「NeoFace Access Control」のご紹介

日本電気株式会社　システムデバイス事業部　エキスパート　古橋　隆幸

1 商品開発背景

・新時代を担う!「立ち止まる必要のない高速顔認証」

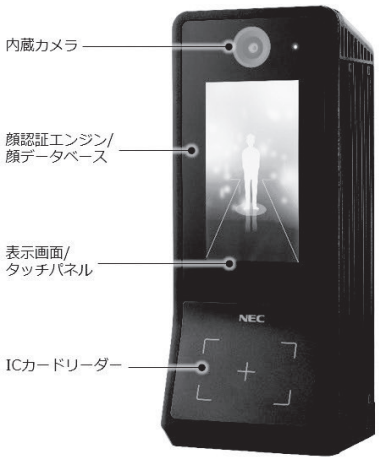
安全・安心な街づくりのニーズが高まる中、指紋や静脈などを使った生体認証が普及しています。NECは約30年前から、顔認証技術の研究開発を進めてきました。今回、NECでは、世界最高レベルの認証精度を有する顔認証エンジン「NeoFace」を活用した「NeoFace Access Control」を開発しました。

従来、ビルの入場ゲートには、IDカードをリーダーにかざすタイプのセキュリティシステムが多く導入されてきました。このようなシステムの場合、IDカードの紛失や、使い回しと言ったリスクが避けられない状況です。NECの「NeoFace Access Control」は、事前に撮影した顔画像と、ゲート通過時に撮影した顔画像を照合して本人確認を実現することができます。

また、従来の顔認証は一旦立ち止まる必要がありましたが、「NeoFace Access Control」は、ゲート通過時にカメラの前で立ち止まることなく歩きながら本人確認が行え、「顔認証を活用してスムーズに入退したい」「顔認証でセキュリティレベルを向上させたい」「顔認証を手軽に導入したい」というお客さま向けに開発した商品です。

2 商品の特長

今回開発した「NeoFace Access Control」は、世界最高レベルの顔認証エンジンをはじめ、データベース、カメラやディスプレイ、カードリーダーなど、顔認証に必要なソフトウェア・ハードウェアをパッケージ化した商品です。あらかじめ端末内のデータベースに登録した顔写真と、内蔵カメラが撮影した動画から検出した顔画像を照合し、瞬時に本人確認を行うことができます。カメラの前で立ち止まることなく、歩きながらスムーズに認証を行うため、通勤時等でも円滑な入場管理が可能です。



顔認証による解錠を行うために必要となるハードウェア（無接点インターフェースの搭載）とソフトウェア（顔認証機能・カメラ・画面表示機能など）をコンパクト筐体に凝縮しました。既存のセキュリティゲートや入退管理システムに本製品を追加で導入するだけで、顔認証によるセキュリティゲートの解錠ができます。さらに顔認証とセキュリティカードの二要素認証により、セキュリティレベルの向上を実現します。

端末内のデータベースには5,000人までの顔情報の登録ができるため、スタンドアローンの顔認証製品として、1台で運用することもできます。

さらに、大規模な施設やビルにおける複数台利用（最大100台）には、顔管理サーバソフトウェア「NeoFace Access Control Manager」の活用により、10,000人の顔情報の一括登録・管理も可能です。顔情報の登録後は電源を入れるだけで使用でき、停電時でも非常用電源さえあれば運用し続けることができます。

立ち止まる必要のない高速顔認証ができる「NeoFace Access Control」は、企業や行政機関をはじめ、工場、イベント会場、会員制施設、スタジアム、会議室、工事現場など、多種多様な入退シーンで活躍できます。

例えば、データセンターや研究開発施設など利用者を限定するエリアに対して、顔認証と社員証などのIDカードと組み合わせる二要素認証を活用することで、より安全・安心な空間を提供しつつ、効率的な入退を可能とします。また、顔認証は非接触で生体認証が行えるため、食品加工工場や医療施設などの衛生施設にも適しています。

さらに、防塵・防滴・気温45度条件下での利用ができる耐環境性（IP54）と、スタンドアローンでの利用が可能である特性を活かし、イベント会場や一時的に作業を行う工事現場など、半屋外のような環境でも利用することが可能です。

3 詳細

・多様な利用シーンにあわせて複数の認証モードを提供

認証モードは端末単位で一つのみ選択可能です。

認証モード		説明	特徴
1	顔・カード連携認証 （ウォークスルー）	ゲート連携用途 ①人が近づくと顔認証し、 ②ICカードをタッチしてGO	●二要素認証によるセキュリティレベルの向上 ●認証エラー表示が可能
2	顔・カード連携認証	ゲート連携以外の用途 ①ICカードをタッチ後に、 ②顔認証してGO	
3	顔のみ認証 （ウォークスルー）	人が近づくと顔認証してGO	●ゲート連携用途「立ち止まる必要のない高速顔認証」 注）認証エラー表示はできません
4	顔のみ認証 （タッチ認証）	本体のタッチパネルに指でタッチしてから顔認証してGO	●認証エラー表示が可能
5	カード認証	ICカードをタッチしてGO	●試験用途 （顔認証導入までの一次的な運用など）

・顔情報登録は端末、パソコン、サーバによる3種類の登録方法を提供

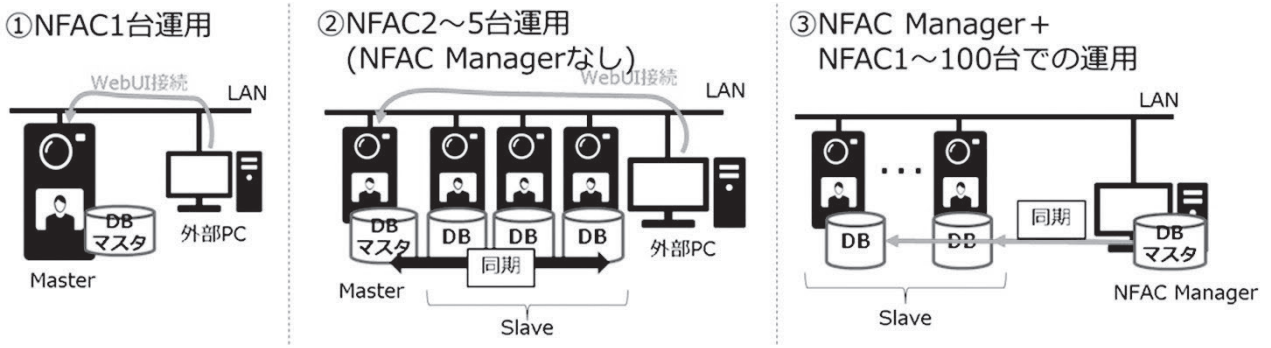
複数台運用でも登録は1台だけで行えます。マスタ端末またはサーバソフトに登録すれば、他のスレーブ端末へ自動的にデータ同期されます。

顔写真JPEGファイルのサイズは、横400pixel×縦500pixel以上で顔登録をします。

登録方法	作業対象	方法
①端末から	本製品のマスター端末 （USBキーボード、マウス利用可）	・マスター端末にログインして登録画面を表示します ・登録者が端末のカメラの前でシャッターボタンを押します ・必須／任意の登録情報を入します（カードIDは内蔵カードリーダーにカードをかざすと登録できます） ・入場制限エリア情報を登録して完了（これを人数分繰り返します）
②管理用PCから	本製品とLAN接続されたパソコン	・PCのブラウザからマスター端末のIPアドレスに接続しログインします ・登録画面で顔写真JPGファイルを指定して登録情報を入力します ・入場制限エリア情報を登録して完了（これを人数分繰り返します）
③サーバから	NeoFace Access Control Manager （サーバソフト）導入済みのサーバ	・登録する全員の顔写真JPGファイルを任意のフォルダに保存します ・登録情報の一覧をCSV形式で作成します ・サーバソフトにログイン後、登録画面でCSVファイルを指定し、一括登録して完了

・運用構成について

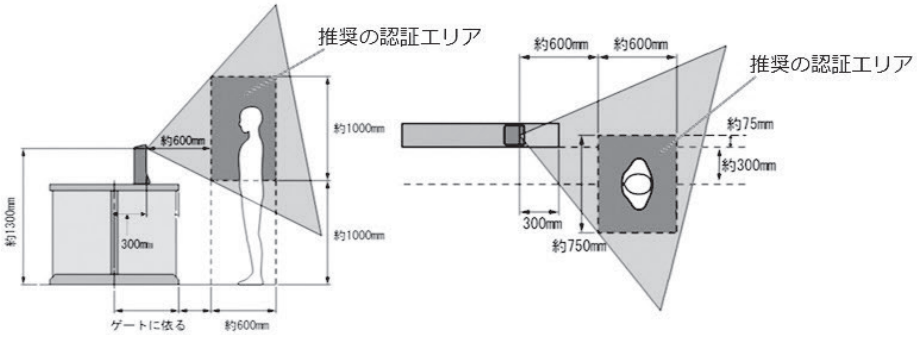
本製品は端末だけで1台から、5台まで運用できます。設定、監視する場合は外部PCからWebUI接続することで操作ができます。6台以上で運用する場合は、サーバにインストールして使用するソフト「NeoFace Access Control Manager」を利用するとサーバがマスタ端末となり運用ができます。



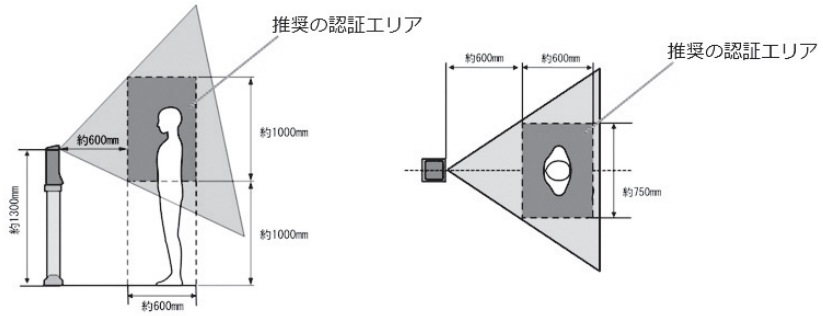
(NeoFace Access Control：NFAC)

・設置について

本製品は入場ゲート設置やスタンド設置が可能です。



入場ゲート設置する場合は、カメラの高さは頭部（顎下から頭頂まで）が接地面から約1000～2000mm、カメラの手前600～1200mm、ゲート端から750mmが認証エリアとなります。



スタンド設置する場合は、カメラの高さは頭部（顎下から頭頂まで）が接地面から約1000～2000mm、カメラの手前600～1200mm、カメラを中心として750mmが認証エリアとなります。

4 技術

・世界最高レベルの性能を誇る顔認証

NECの顔認証技術は、2017年、米国政府機関主催の顔認証技術ベンチマーク（NIST-FIVE※1）において、認証精度99.2%と、他社を大きく引き離す第1位の性能評価を獲得しました。これまでの静止画の顔認証テストに続き、4回連続の世界一を獲得しました。

顔認証は、人間が普段相手を判別する手段をシステムで実現した最も身近な認証方式です。

また、指をかざす等のアクションが不要なため、特別なユーザ操作を強いることなく、利便性に優れた認証が可能です。

・顔認証の仕組み

顔認証は大きく「顔検出」と「顔照合」の2つの処理に分かれます。「顔検出」処理では、画像の中から顔領域を決定し、次に顔特徴点の検出を行って目・鼻・口端などの顔の特徴点位置を求めます。次に特徴点位置を用いて顔領域の位置・大きさを正規化した後、「顔照合」処理を行います。

NECの顔認証は優れた環境耐性と様々な条件に対応し、高精度を実現しています。

顔の特徴の中から個人を識別する最適な特徴を選択することにより、経年変化の影響をうけにくいほか、ディープラーニングにより、顔の向きの変化や低解像度の顔画像にも対応できます。

・立ち止まる必要のない高速顔認証

カメラの前で立ち止まって行う顔認証は、本人の意思で認証をするため照合処理は簡単です。

一方、立ち止まらない顔認証は、本人がカメラを意識しないで行われるため、対象者がカメラから遠い、正面を向いていない、複数人を同時に認証しなければならないなどの条件が加わります。

そのため立ち止まらない顔認証は照合処理が複雑になりますが、顔認証エンジン「NeoFace」を活用することで実現しました。

・NECの顔認証技術開発の歴史

NECは1989年より顔認証技術の研究開発を開始しました。これは50年以上前から行ってきた文字認識の研究で確立したパターン認識技術を応用したものです。

「NeoFace Access Control」の顔認証エンジンは、米国政府機関主催の顔認証技術ベンチマーク（NIST-FIVE※1）にて第1位を獲得しました。

※1 米国国立標準技術研究所 Face In Video Evaluation - 2017
http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

5 最後に

今後も顔認証エンジン「NeoFace」のさらなる精度と速度の追求と、顔認証の利便性向上のため「NeoFace Access Control」の開発を続けてまいります。

【本商品に関するお問い合わせ先】

日本電気株式会社
ファーストコンタクトセンター
電話番号：03-3455-5800
受付時間：9:00～12:00 / 13:00～17:00
月曜日～金曜日（除祝日、弊社休日）

商標について
- **NeoFace は、日本電気株式会社の登録商標です。**
- **顔認証技術はあらゆる条件下での認証を保証するものではありません。**

情報通信と防犯対策のプロを目指して

株式会社 NTT 東日本－東北　営業部　福島営業担当
防犯設備士資格番号　第 16－27063 号
橋本　祐子

NTT東日本－東北では、2016年11月から会社全体として防犯設備士の資格取得を進めてきました。現在、東北エリアで約60名が取得しております。

【通信だけではなく防犯対策の声も】

これまでNTT東日本は通信サービスの提供を中心に活動してきましたが、昨今、防犯カメラなどのインターネットにつながる防犯機器が増えたことや、実際にお客様から「集合住宅の入口で不審者が出た」「夜間、駐車場で車のいたずらや無断駐車があり困っている」「ごみ置き場で不法投棄が散見される」等の防犯対策に関するお困り事の相談が非常に多くなってきたことから、対応策を検討してきました。

その中で、インターネットを経由して遠隔地から監視できるNWカメラは、通信回線と防犯カメラをワンストップで提供することで、上記のような防犯に関するお困り事の解決が可能となるため、力を入れて取り組むこととなりました。

【会社を挙げた防犯設備士資格取得チャレンジ】

日常の営業活動の中で、通信と防犯対策についてお客様からの声にお答えできるよう、まずは防犯設備の知識を習得しお客様に防犯対策のプロとしてコンサルティングができるよう防犯設備士資格試験にチャレンジすることにしました。

宮城県防犯設備士協会様からは、弊社の活動における防犯設備の専門知識や提案活動の助言をいただきました。なお、弊社の資格取得者は2年間で約60名になりました。

また、2017年度から、弊社でプロフェッショナル分野ごとに取得を推奨する社外認定資格に設定されております。

【防犯設備士資格取得後の活動】

防犯設備士試験に合格し資格取得したものの、実際にどうやって防犯設備士のスキルを活かした活動をしたら良いか分からず、模索しながら様々なチャレンジをしました。

防犯設備の専門スキルを活用するため受験で勉強した防犯設備士テキストを参考にし、防犯設備士協会様からのアドバイスを受け、NTT東日本の資格所有者が活用できる簡易なチェックシートを作成しました。

ポイントとしては、建物外周、共用部、各住居部分の防犯設備の有無や照度を防犯設備士がチェック・診断し防犯対策のアドバイスができるようにしています。

NTT東日本

防犯診断チェックポイント

	チェックポイント	診断結果	ひとことアドバイス
建物外周	フェンスの破損状況	△	[illegible]
	外灯等の照明	×	[illegible]
	外部からの見通し	○	
	駐車場・駐輪場・ごみ置き場の明るさ	△	[illegible]
	駐車場・駐輪場・ごみ置き場の防犯カメラ設置状況	×	
共用部	共用廊下の明るさ	○	[illegible]
	共用廊下の防犯カメラ設置状況	×	[illegible]
各住居部分	郵便受けの鍵有無	(郵便受けなし)	
	ドア錠の数（二つ以上）	×	[illegible]
	[illegible]	×	[illegible]
	カメラ付きインターホンの有無	○	[illegible]
	共用廊下側窓の状況	×	[illegible]
	居室窓に雨戸やシャッターの有無	×	
	補助錠設置の有無	×	[illegible]
	ベランダの見通し	○	
	室内の異変を通知する設備の有無	×	[illegible]

NTT東日本-東北 営業部

調査では、NTT東日本の防犯設備士の証として資格証と腕章を着用し活動をしています。

【関係機関との連携強化】

防犯設備士として更なる活動を広げるため、今後は、各県の防犯設備士協会様や関係機関様から助言をいただきながら「防犯の専門家」として活躍できるよう連携して地域の防犯対策や安心・安全なまちづくりのための役割を担う事が必要だと考えております。

【安心・安全な利用環境を提供】

私たちは情報通信に関する社会的な課題に真摯に取り組み、安心・安全な利用環境を提供します。今後においても防犯設備士資格を活用し、防犯設備機器だけではなく、サイバー犯罪対策などにも活動を広げ、これまでの情報通信を通じて安心・安全なまちづくりに貢献できるよう取り組んでまいります。

高知県防犯設備協会の紹介

NPO 法人高知県防犯設備協会　理事長
（元　高知県警察本部刑事部長）　上田　瀧雄

【高知県の概要】

○風土

高知県は、豊かな森林と青い海の国です。北は四国山地で愛媛県、徳島県に接し、南は太平洋に面して扇状に突き出しています。太平洋を臨む海岸線は長く、西部はリアス式海岸、東部は隆起海岸で平坦な砂浜が続いています。

○歴史

「とさ」の呼称は、古くから国産みの神話のなかで、土佐国建依別（とさのくにたけよりわけ）と呼ばれています。戦国時代には七雄が並び立ちましたが、長宗我部氏が土佐を統一、その後、関ヶ原の合戦で西軍に味方して破れた長宗我部氏に代わって、慶長六年（1601年）山内一豊が土佐二十四万石の国主として入国しました。

幕末には、坂本龍馬など多くの志士を輩出、明治維新には板垣退助などが、自由民権運動を起こし、「自由は土佐の山間より」とうたわれるようになりました。

【協会の概要】

当協会は、2011年10月に高知県防犯設備協会として発足、翌2012年1月NPO法人の認証を得て今日に至っています。現在、正会員法人14社（会員企業社員数約200名）。会員企業には防犯設備会社だけでなく、県内大手の建設会社や建築会社が加わっていて、防犯カメラの設置普及活動のほか、社会貢献活動の一環として、年間を通じ通学路の子ども見守り活動や防犯パトロール活動なども実施しています。

【高知県の犯罪情勢】

最近の犯罪情勢は、全国的に犯罪の総量が増加している中で、県内でも県民が不安に感じている住宅や店舗・事業所対象の侵入盗などの犯罪が増加しております。このため、県警においては県民が犯罪被害に遭いにくい「安全・安心まちづくり」対策を重点施策として推進していますので、その実現のためにも当協会と県警との連携が一層重要と考えています。

【主な活動内容】

1　会員研修会の開催

会員のスキル向上を目的に、防犯セキュリティー機器メーカー担当者を招聘して勉強会を開催。

(1) 平成27年1月22日
講演者：アイホン株式会社 様
①戸建て住宅向けテレビドアホン（防犯性能・操作機能の向上等）
②IPネットワーク対応インターホーン（低コスト、ネットワークカメラ連携等）

(2) 平成28年6月27日
講演者：株式会社JVCケンウッド　公共産業システム営業本部　プロダクト営業統括部　西日本営業部　中四国システム支店 様
①セキュリティーカメラシステムの紹介

(3) 平成29年6月6日
講演者：株式会社　日本防犯システム 様
①昨今の防犯カメラ機器性能と設置の状況

2　防犯活動

県内自治体等を訪問して防犯カメラの普及促進を図っているほか、高知市内及び県中東部香南市内において、会員企業が主催する通学路における子ども見守り活動、拍子木防犯パトロールなど実施し犯罪や事故に遭わない安全安心な地域社会の実現に努めています。

【本年度の重点施策】

本年度中に、防犯優良マンション認定制度を実施すべく、京都、福岡の各地域協会担当者のご指導を頂きながら、鋭意取り組んでいます。

【表彰】

平成29年11月、当協会理事長上田瀧雄が、県民生活の向上に貢献した功績が認められ、高知県知事から平成29年度高知県文化環境功労者として表彰されました。

上田理事長（左）と推薦者藤川理事（右）

コラム

RBSS H30 プロジェクトが目指したこれからの防犯水準と活用方法

優良防犯機器 RBSS は防犯機器の安心マークです。
公益社団法人 日本防犯設備協会

公益社団法人　日本防犯設備協会　顧問　RBSS委員会　委員長　三澤　賢洋

10月1日のテレビは、京都大学の本庶佑（ほんじょ・たすく）教授のノーベル医学生理学賞受賞の話題で大変でした。「オプジーボ」に関心がある歳ですので、おめでとうとありがとうの気持ちです。長期間の基礎研究の積み上げの大切さを痛感します。

リュウグウでの「はやぶさ2」にも驚きです。遠隔コントロールの制御伝送技術に加え、「ミネルバ」から送られてくる写真は、漆黒（無反射）の宇宙空間と太陽光線で浮び上るリュウグウの岩山が見事に高解像度でカラー撮影されており感激です。失敗をチャンスにした技術者の取り組みを尊敬します。

●防犯カメラの進化と活躍

防犯カメラではどうでしょうか。

平成12年に発出された「安全安心まちづくり推進要綱」を起点に防犯カメラが各地で整備され、平成16年頃に記録装置がテープ式からHDD使用のデジタルレコーダに切替り画質が良くなり、平成22年頃からIP-IF対応（いわゆるネットワーク）の防犯カメラと同デジタルレコーダ（防犯用）が普及してさらに良くなり、平成30年ではフルハイビジョン解像度が主力になりました。

警察庁から出された犯罪情勢に、防犯カメラ等の画像が検挙の端緒になった分析が掲載されています。

区分＼特定の端緒（警察活動）		本件事件	防犯カメラ等の画像
重要窃盗犯（件）		8,097	813／10.0%
	侵入窃盗	6,192	607／ 9.8%
	自動車盗	913	50／ 5.5%
	ひったくり	411	84／ 20.4%
	すり	581	72／ 12.4%

出典:警察庁　平成28年犯罪情勢より抜粋

●個人情報保護法と防犯カメラ取扱い上の変化

RBSS（優良防犯機器認定制度）は平成20年にNTSC対応（いわゆるアナログ）、平成22年にIP-IF対応（いわゆるネットワーク）の基準を作りました。

RBSS認定機器はIP-IF対応機器が半分以上でフルハイビジョン解像度が多いため、防犯カメラの記録画像は改正個人情報保護法内の取扱が必要です。

皆さん「厄介だなー」と思っていませんか。

幼稚園児は道路を横断するには、横断歩道で手をあげて渡ることを習います。車は左側通行があたり前で、老人の逆走は違法行為で非常に危険です。

防犯カメラも同じで、法で示す使い方を守れば良いだけで、今までよりよっぽど楽だと思いますよ。

防犯カメラとデジタルレコーダ（防犯用）の設置などには、いくつかの注意事項があると思いますし（後述）、各都道府県で整備されている「防犯カメラの設置と管理に関するガイドライン（自治体によって名称が違いますが）」を見直す検討が必要になる場合があると思っています。

●RBSSであること、とは

さて、自治体などの入札条件にRBSSを使っていただく機会が多くなり、大変感謝しています。

その理由は次の3つになると思います。

1.RBSSであれば、機器基準だけでなく、機器に責任を持つ会社と品質マネージメントの優れている生産工場が認定されているので安心。

2.RBSSであれば、防犯に必要な共通機能を、全ての認定機器が満足しているので安心。

3.RBSSであれば、機器ごとにどの高度機能を持つか「見える化」されており、設置対象条件が分かれば、それにあった機器を指定しやすい。

●これからの防犯カメラを検討したRBSS H30

当協会はRBSS発足10年を機に「RBSS H30」プロジェクトを編成、防犯カメラとデジタルレコーダ（防犯用）（以下「DVR」という。）の進化やそれらの機器への期待を検討して、RBSSの共通（必須）機能と、高度（選択）機能を改正しました。

RBSS H30 改正ポイント

簡単に背景や注意点をご説明します。

○4K解像度への進化に対応できるようにしました。フルハイビジョンが普及を始めた頃、周辺画像が中心画像より非常に悪い機器が多々あり問題になりました。原因は「ハイビジョン用」として称した周辺解像度が悪いレンズを安いから買った会社があったのです。RBSSはフルハイビジョン画像の周辺も評価できる評価チャートを開発してそれを防ぎました。今回4Kでも、評価用に5枚組で約1.5m×約2.7mの大きさになる「4K評価チャート」を開発しました。

「なんちゃって4K」の防犯カメラやDVR及びレンズには、くれぐれもご注意ください。

○犯罪が多くかつ不安感が高い夜間の屋外生活道路や駐車場などに、LED防犯灯を設置すれば、RBSS共通機能の水準を上げたので、防犯カメラによるカラー撮影と、人物の動きに記録漏れの無いDVRにより、安全安心が格段に向上します。人物が防犯カメラの縦方向でも横切る方向でもしっかり撮影・記録が可能です。

・防犯カメラ共通機能　最低被写体照度（5.1.10）
　従来基準3ルクス以下⇒新基準0.5ルクス以下
・DVR共通機能　記録コマ数（5.1.3）
　従来基準1コマ/秒⇒新基準5コマ/秒

＊もっと暗い場合はどうするか?

方法1:

新最低被写体照度（高感度タイプ）機能（5.2.1）の新基準「0.05ルクス以下でカラー撮影可能」の機種を使います。ちなみに、星明かりの夜間は0.02ルクス、人間の色に反応する視細胞の動作限界は0.01ルクスなので、大半の場所でカラー撮影が可能です。

さらに方法2:

新基準0ルクス環境撮影機能（5.2.2）の「カメラに搭載した照射機能（近赤外光源または可視光源）により撮影可能」の機種を使います。RBSSでは、中心のスポット光でなく、実用撮影範囲を明らかにしています。これは、不法投棄対策用に威力を発揮できると思います。

＊もっと動きが早い被写体（車やオートバイ、万引きの早い手の動きなど）の場合はどうするか?

DVRの高度機能（5.2.1）の新基準「記録コマ数を10コマ/秒以上」の機種を使います。

○照度への対応だけでなく、逆光への対応能力を強化しました。

防犯カメラの高度機能（5.2.6）でダイナミックレンジ拡大比が40dB以上の機種を認定しており、マンションの出入口などでご利用いただいておりましたが、夜間や西日の場合では難しい場合もありました。今回、ダイナミックレンジ拡大比が60dB以上を測定可能な方法を使い、同基準に新機能を追加しました。雪面反射光や夜間ヘッドライトへの対応など、厳しい場所で使用可能な機種が選べるようになります。

○海外のウェブサービスが防犯カメラとDVRのデフォルト情報を公開しています。それを利用した攻撃を受けて、動作不能やボットネットへ取り込まれる可能性が高いので、2段階の対策機能を設定しました。

・第1段階（共通機能）
　防犯カメラとDVRとも、IDやパスワード認証の管理を義務化しました。
・第2段階（高度機能）
　さらに、防犯カメラとDVRとも、パスワードや画像の暗号化、外部攻撃からの耐性を求める仕組みを持つ基準を新設しました。高度セキュリティ機能を持つ機種を選んでください。

○記録方式や記録媒体を大きく変更して、フレキシブルなシステムが組めるようにしています。

・DVRの適用範囲を改正して、記録メディアをハードディスクだけでなく、SSDやSDカードなども使える様にしました。合わせて、ユーザが指定された記録メディアを入れて使うことができる記録メディアレスデジタルレコーダ（防犯用）も申請対象にしました。
・ネットワークを使った記録装置の増設や、冗長化をハードだけでなくソフトで行う機能が普及する可能性が高いので、それに対応する高度機能を新設しました。

●防犯設備士の腕の見せ所

個人情報保護法の取扱で以下のポイントを注意して取り組んでください。

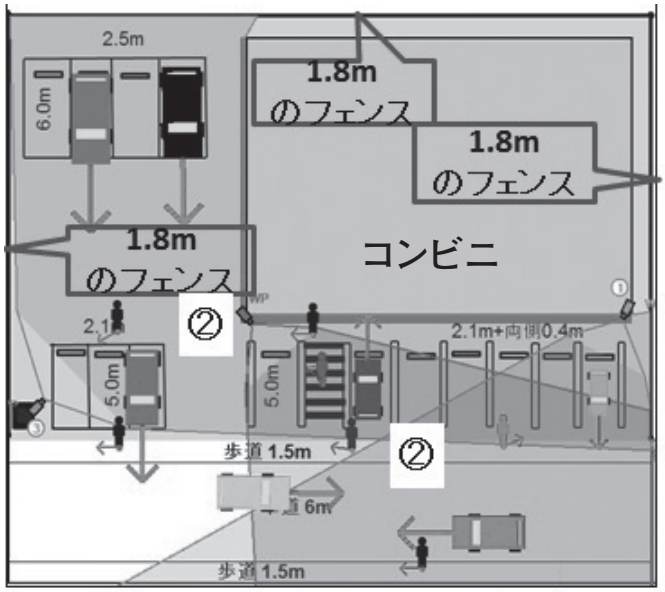
・防犯カメラ設置の目的を明確にして、その実現手段（撮影対象の設定、視野角と画角の設定、記録コマ数の選定など）を決めます。

・管理者名の表示を掲示します。

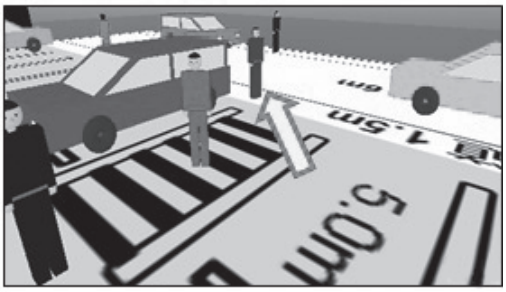
・RBSSを参考に、最適な機器（機能と性能を揃えた）を選びます。

・設置前に、設置後の状況を関係者との共通理解が得られるように、説明資料を準備します。

図は駐車場セキュリティガイドVOL.2作成時のシミュレーションで使用した説明用の参考例です。



カメラ②は、コンビニ右軒下に設置して②の範囲を撮影する。歩道にいる人物（矢印）が画角A25。
主に、コンビニ正面入り口を出入りする人物・荷物及び店舗前駐車場右半分を撮影範囲とする。



『めざせ500人!!』
総合防犯設備士には『数』が必要

総合防犯設備士委員会　委員長
総合防犯設備士資格番号　第01-0018号　永井　健三

2018年4月、期せずして総合防犯設備士委員会委員長を拝命しました。私は、総合防犯設備士のいわゆる1期生。以来、2004年から総合防犯設備士委員会の委員、2005年から総合設備士資格試験セミナー講師、問題作成委員、講習認定講師、など総合防犯設備士制度に携わる末席を汚してきました。自ずとこの制度には愛着があり、大きな期待を寄せる者の一人です。

【めざせ500人!!】

総合防犯設備士に求められる任務には、設備士の育成や教育をすること、防犯監査や防犯コンサルティングができること、などがあります。日本防犯設備協会（以下、協会）は、2016年から防犯設備士の資格更新制度をスタートしておりますが、これを現在のレポート方式から講習方式とし、さらにこの講習方式の講師を総合防犯設備士に委ねることを検討しています。更新時講習の講師派遣は、総合防犯設備士委員会から総合防犯設備士に委ねる。この関係を効率よく回すことにより、設備士の更新時講習制度の体制が早期に確立できると考えます。

2018年4月現在、総合防犯設備士登録数は367人、防犯設備士登録者数は27,848人。総合防犯設備士の適切な数は、何人か。正答は見当たらない。今後、総合防犯設備士が防犯の専門家として、事業として成り立ち、内外にその活躍の場を求めるなら、根拠のない乱暴な言い方ではあるが設備士数の10%は最低限必要と考えます。総合防犯設備士登録者数が「ゼロ」の県は、新潟県、山梨県、長野県、鳥取県、徳島県、愛媛県、佐賀県の7県。将来を見据えた事業は枚挙にいとまないし、内外からその活躍が期待されています。まず、「数」の分母が無いと、活動も事業も成り立たないと考えます。

設備士の更新時講習講師を総合防犯設備士が担う、登録者数「ゼロ」の県を無くす、この2つを目の前の最重要課題として委員会は取組んでまいります。その為には、2020年3月31日までに『500人』の登録を実現すべく委員会を挙げて、否協会を挙げて取り組みます。キャッチフレーズは『**めざせ500人!!**』。

【「総合の試験は難しい」と言う風評を払拭する】

「総合の資格を受験しませんか」、「総合の試験は難しい、もうイイよ」「以前挑戦したが、難しく不合格だった。もう、うけないよ」。受験セミナーの受講や試験の受験を勧める委員会メンバーと受験対象者の会話です。難しいと言う風評を定着させたのは、試験問題作成委員を担ってきた私も「戦犯の一人」と言えるかもしれません。しかし、より高度な理解力・表現力を求めた結果であると理解して頂きたいと思います。

2016年までの合格率は、29.2%に留まります。合格率だけを見ると確かに低いです。総合の試験は、論文形式、全て記述式であり、ただ単に丸暗記するだけでは点は取れなく、総合的な知識や表現力が要求されています。

受験セミナーでは、過去問題（協会HPで過去5年間の過去問題が公開されている）の解読の仕方、解答の書き方を徹底的に講習します。担当する講師陣は、協会から委嘱された認定講師が担っています。過去問を中心にした受験セミナーは、2017年から実行されています。結果、2017年の合格率は、63.9%でした。2018年の結果も期待されています。

講師陣の私心を捨てた熱心な講習に敬意を表し、感謝します。

【2020年に向けて】

2020年は、「めざせ500人!!」プロジェクトの最終年;

①「総合の試験は難しい」と言う風評を払拭するため、合格体験談などで広く「外」へ向けて受験者を「その気にさせる」施策を講じる。「総合の合格率が大幅UP中!!今が旬」などのキャッチで拡散させる。

②チラシを漫画チックな親しみ易いものに一新し、それを一つの手段として、あらゆる機会を通じて拡散する。

③拡散先は、防犯設備士資格取得後3年を経過した防犯設備士有資格者に対し直接DM、e-mailなどで周知する。また協会のHPやメルマガを通じて周知する。これらのアクションを最低年間4回は実行する。

④総会や研修会（地域協会主催も含む）などあらゆる機会を通じてPRする。

⑤セミナー受講生の負担を軽減し、総合防犯設備士を身近に感じてもらうため、東京と大阪の会場以外でも受験セミナー開講を検討する。他の地域での開催などを検討する。経済計算も重要な要素となる。

これらの試みは、地域での様々な活動の布石になるはずである。

500人達成は、安全・安心の伝道師「総合防犯設備士」序奏の第一歩に過ぎない。

平成30年度　防犯設備士養成講習・資格認定試験のご案内

平成30年度防犯設備士養成講習・資格認定試験が下記の要領で開催されます。受講・受験を希望される方は、お申込みください。なお、講習・試験の詳細、会場の住所・地図などは、協会のホームページに掲載いたします。

開催回	開催日		開催地	会場名	募集期間
	講習	試験			
第104回	11月16日(金) 11月17日(土)	11月17日(土)	東京	ベルサール新宿グランド コンファレンスセンター	募集終了
			大阪	天満研修センター	
			仙台	トラストシティカンファレンス・仙台	
第105回	平成31年 2月1日(金) 2月2日(土)	2月2日(土)	東京	ベルサール西新宿	11/1～12/7
			大阪	新梅田研修センター	
			広島	RCC文化センター	

平成30年度　総合防犯設備士資格認定試験のご案内

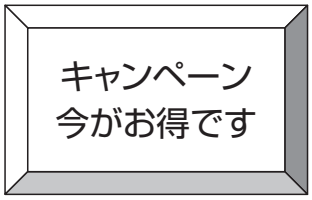
平成30年度総合防犯設備士受験セミナー・資格認定試験の募集は全て終了いたしました。ありがとうございました。また、来年宜しくお願いします。

No	名称	開催日	開催地	会場名
1	一次試験B(講習認定)	12月1日(土)	東京	日本防犯設備協会
2	二次試験B(面接試験)	12月1日(土)	東京	日本防犯設備協会
3	二次試験A(面接試験)	12月8日(土)	大阪	新梅田研修センター
		12月15日(土)	東京	日本防犯設備協会

重要なお知らせ

平成24年度以前に防犯設備士の資格を取得された方へ

大幅に内容を刷新した新防犯設備士テキストを無償で進呈!!
更に、協会発行のガイドブック（1冊）も無償で進呈!!



◆資格更新の必要性

防犯設備士の資格認定制度を開始した1992年当初は、防犯設備の進歩はあまり早くなく、資格更新が無い制度となっていましたが、近年では特に防犯カメラなどの機器の性能向上が著しいだけでなく、運用面では、犯罪手口が巧妙になり、セキュリティ関連等の対策も必須になってきました。そのような情勢の変化に伴い、防犯設備士として常に新しい情報を取り入れる必要性が高まり資格更新制度の立ち上げに至りました。

◆従来の防犯設備士テキストから大幅に刷新した内容（抜粋）

①防犯カメラの最新方式
②サイバー犯罪、振り込め詐欺などの犯罪最新情報
③個人情報とプライバシー
④マイクロ波式やレーザービーム式の最新検知器
⑤出入管理設備の電気錠、フラッパーゲート等

※・資格更新はすぐに受け付けますが、新テキスト、ガイドブックの発送は、2019年3月以降になります。資格更新の手続きや流れはホームページをご覧ください。
・平成24年度以前に防犯設備士資格を取得された方は更新の義務はございません。
・一度資格更新を実施いただいた後は3年毎の資格更新義務が生じます。

●メールマガジン登録のお願い

現在、防犯設備士の方にはメールで協会情報誌「日防設ジャーナル」ダイジェスト版をはじめ、協会主催セミナーや防犯関連情報などを送信しています。メールマガジンの配信を希望される方は、ホームページの「メールマガジン配信申込」からお申込みください。

●連絡先の更新をお願いいたします

今後、資格更新関連情報などお役に立つ情報を確実にお伝えしたいので、防犯設備士資格認定試験申込み時に登録された連絡先（住所、電話番号、メールアドレス、勤務先等）に変更があった場合には、ホームページの「住所・勤務先変更」から変更届のご提出をお願いいたします。 また当時の登録内容が不明な方は、念のため変更届をご提出いただきますようお願いいたします。

防犯カメラとデジタルレコーダ（防犯用）のRBSS認定基準を改正

（公社）日本防犯設備協会　RBSS 事務局

■ 背景

RBSS（優良防犯機器認定制度）は平成20年10月に発足し、平成30年9月末現在、累計で防犯カメラは459型式、デジタルレコーダ（防犯用）は169型式、LED防犯灯は152型式を認定し、認定会社数は防犯カメラとデジタルレコーダ（防犯用）が23社、LED防犯灯が10社になりました。

防犯カメラとデジタルレコーダ（防犯用）のRBSS基準は下表に示すように、新機種の追加と防犯設備として求められる機能性能の充実に取り組んできました。

時期	主な改正内容	現状の効果
平成22年	IP-IF対応の防犯カメラとデジタルレコーダ（防犯用）、いわゆるネットワーク防犯カメラシステムを組入れた。	現在、認定機器の51%がIP-IF対応機器であり、増加傾向である。
平成24年	記録一体型屋外用防犯カメラを認定対象とした。	55型式認定。街頭防犯カメラの主流で、RBSSが入札の特記仕様に記載される事例が増えている。
平成25年	HD-SDI対応防犯カメラとデジタルレコーダ（防犯用）システムを組入れた。	同軸ケーブルを使ってフルHDの撮影と記録ができる。認定機種の10%が対応機器である。
平成27年	全方位型防犯カメラを認定対象とした。	6型式認定。食品工場や金融機関などで使用されている。

RBSS認定会社の努力と関係機関のご協力もいただいた結果、RBSS自体の認知度が高くなっており、RBSS認定機器が全国で広く使われています。

このような状況の中、RBSS発足から10年が経過し、RBSS認定基準で使用しているISOなどの関連規格が改正されたり、最新のカメラやデジタルレコーダ等性能の飛躍的な向上、及びサイバー攻撃などの外部環境の大きな変化がでてきました。この状況に対応すべく、RBSS基準（資格審査基準、防犯カメラ機器認定基準、デジタルレコーダ（防犯用）機器認定基準）を改正しました。

■ 資格審査基準を改正

RBSSは認定機器の品質を確保するため、資格審査では生産工場単位でISO9001の取得を要請しています。

従来はこのISO9001は2000年版を基本にしていましたが、現在のISO9001は2015年版に移行して、項目の大幅な組み換えが行われ、業務委託への細かな対応や項目ごとの取扱いの変更がされました。このため、RBSSでもISO9001の2015年版を使用するように、資格審査基準を改正しました。

■ 防犯カメラとデジタルレコーダ（防犯用）の機器認定基準を改正

（1）共通機能（必須機能）の主な改正内容です。

①最低被写体照度：従来の3ルクス以下を0.5ルクス以下にしました。LED防犯灯を設置した街路では、すべての認定機器は、カラー動画撮影が可能になります。

②記録コマ数：デジタルレコーダ（防犯用）は、記録コマ数を1コマ／秒から5コマ／秒に増やしました。RBSS認定機器では、街路での縦方向や横方向の人物撮影で記録モレが無くなります。

③IP-IF対応の防犯カメラとデジタルレコーダ（防犯用）には、IDやパスワードの対応を必須としました。外部サイトから、まる見えになることはありません。

(2) 高度機能（選択機能）の主な改正内容です。

①4K解像度：防犯カメラとデジタルレコーダ（防犯用）に4K解像度の基準を追加しました。4K評価チャート（約1.5m×約2.7m）を新たに製作し、このチャートを使って画質を判定します。

②ダイナミックレンジ拡大：逆光対応の機能で、従来の40dBに加え、より高レベルの60dB以上の能力の基準を追加しました。雪面反射や非常に暗所でのヘッドライトでも撮影にも対応可能です。

③最低被写体照度（高感度タイプ）：従来の0.5ルクス以下を0.05ルクス以下としました。星明かりが0.02ルクスなので大半の場所でカラー撮影が可能になります。

④0ルクス環境撮影機能：0ルクス環境下でも近赤外光か可視光を照射して撮影する基準を新設しました。スポット光でなく、照射範囲を規定（JEITAの測定方法）します。不法投棄の場所などで利用可能です。

⑤高密度記録レート：デジタルレコーダ（防犯用）では、高密度記録レートを従来の5コマ／秒から10コマ／秒に増やして、生活道路などを走る車をしっかり撮影できるようにしました。

⑥IP-IF対応記録装置増設：ネットワークを使った記録装置増設の対応や、急速に進化する冗長化の新方式に対応できる機能を新設しました。

⑦高度セキュリティ機能：防犯カメラとデジタルレコーダ（防犯用）はネットワークからの攻撃の可能性があります。パスワードや画像の暗号化、外部攻撃からの耐性を求める高度セキュリティ機能を新設しました。

(3) 記録メディアの種類

デジタルレコーダ（防犯用）の記録メディアは、従来はハードディスクであることが必要でしたが、ハードディスク以外のSSD、SDカードなども適用としました。また、記録メディアレスのデジタルレコーダ（防犯用）も認定対象になります。

■今後の予定

新基準による認定は、11月の第42回RBSS認定から行いますので、申請受け付けを開始しました。

なお、従来基準で認定済みの型式についてのRBSS認定に変更はありません。

また、2019年3月のセキュリティショーで、RBSS開始10年を記念したシンポジウムを2テーマ実施予定です。（テーマ1：RBSS新基準について、テーマ2：4K解像度防犯カメラについて　を予定）

問合せ先：公益社団法人日本防犯設備協会　RBSS事務局
担当：関根　晨貴
TEL：03-3431-7301
E-mail：tokitaka.sekine@ssaj.or.jp

協会出版物の販売についてご案内します。

公益社団法人 日本防犯設備協会発行　調査研究報告書　頒布価格一覧

平成30年10月末現在

会　　報

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
428	会報　防犯設備　2018　盛夏号　No.121	運営企画会議	平成 30 年 7 月	―	2,160	
427	情報誌　日防設ジャーナル陽春号　No.120	運営企画会議	平成 30 年 4 月	―	540	
424	情報誌　日防設ジャーナル爽秋号　No.118	運営企画会議	平成 29 年 10 月	―	540	
414	会報　防犯設備　2016 年創立 30 周年特別号 No.115	運営企画会議	平成 28 年 6 月	―	2,160	

防犯ガイドブック　　多部数の場合、別途ご相談ください。

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
421	防犯カメラシステムネットワーク構築ガイドⅡ	RBSS 委員会	平成 29 年 4 月	500	620	
289	防犯カメラシステムネットワーク構築ガイド	RBSS 委員会	平成 24 年 10 月	620	830	
277	地域セキュリティの創出の手法 「あなたのまちの安全対策」	防犯システム委員会	平成 23 年 11 月	310	420	
250	安全・安心なまちづくりをめざして 防犯照明ガイド vol.5.1	防犯照明委員会	平成 27 年 1 月	310	420	
238	防犯カメラと防犯照明による明るいまちづくり 防犯カメラシステムガイド vol.2.1	映像セキュリティ委員会	平成 28 年 3 月	350	450	
198	暗証番号やカード、生体認証による出入りの制限と管理 出入口のセキュリティガイド	出入管理機器委員会	平成 19 年 3 月	310	420	
419	あなたのまちの駐車場はだいじょうぶですか 駐車場セキュリティガイド vol.2	防犯システム委員会	平成 29 年 3 月	480	580	
415	あなたの愛車をまもる オートバイセキュリティガイド vol.2	自動車・オートバイ委員会	平成 28 年 3 月	350	450	
416	あなたの愛車をまもる 自動車セキュリティガイド vol.2	自動車・オートバイ委員会	平成 28 年 3 月	350	450	
171	暮らしの安全のために、知識と対策を ホームセキュリティガイド	防犯システム委員会	平成 24 年 4 月	350	450	

統計調査

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
420	平成 29 年版　防犯設備機器統計調査報告書	統計調査委員会	平成 30 年 3 月	3,600	5,200	

防犯システム

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
277	地域セキュリティー創出の手法（冊子） 「あなたの街の安全対策」	防犯システム委員会	平成 23 年 11 月	310	420	
267	繁華街・歓楽街の安全対策 DVD 「もっと楽しく、快適に！笑顔ひろがるまちづくり」	防犯システム委員会	平成 22 年 11 月	―	―	ご希望の方は協会まで ご連絡ください
252	高齢者の暮らしを守る　DVD 防犯対策「ちょっと待った！泥棒・・・」	防犯システム委員会	平成 21 年 12 月	―	―	ご希望の方は協会まで ご連絡ください
230	学童の安全確保のための 防犯・防災対策 DVD	防犯システム委員会	平成 20 年 11 月	1,600	2,300	

映像セキュリティ

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
130	防犯映像システム評価用チャート（3 枚一式） （チャートご利用の手引き付き）	映像セキュリティ委員会	平成 16 年 3 月	5,200	7,800	

技術関連

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
254	防犯設備の施工要領（一戸建住宅編）第 2 版	施工基準委員会	平成 22 年 3 月	1,900	2,800	
253	防犯警報システム用語集　第 4 版	国際規格委員会	平成 22 年 3 月	2,800	4,200	
161	防犯設備の施工要領（Ver-2）	施工基準委員会	平成 17 年 4 月	4,300	6,500	

制度事業関連

NO.	タイトル	発行委員会	発行年月	会員価格	非会員価格	備　　考
266	RBSS 画質 A3（静止画）評価チャート A2（静止画）評価チャート セット1式	RBSS 委員会	平成 22 年 10 月	10,800	16,200	
410	【CD-R 版】RBSS2013 認定基準（HD-SDI 対応編） ・防犯カメラ、デジタルレコーダの 2 品目含む	RBSS 委員会	平成 27 年 12 月	5,200	7,800	
411	【CD-R 版】RBSS2015 認定基準（IP-IF 対応編） ・防犯カメラ、デジタルレコーダの 2 品目含む	RBSS 委員会	平成 27 年 12 月	5,200	7,800	
423	【CD-R 版】RBSS2013 認定基準（NTSC 対応編） ・防犯カメラ、デジタルレコーダの 2 品目含む	RBSS 委員会	平成 27 年 12 月	5,200	7,800	
240	総合防犯設備士テキスト	総合防犯設備士委員会	平成 26 年 7 月	5,400	5,400	
225	デジタルレコーダ（防犯用）標準画像（DVD 版 Ver1.0）	RBSS 委員会	平成 20 年 10 月	5,200	7,800	

価格は消費税込みの価格です。（送料別途）

申込み先、問合せ先

〒105−0013 東京都港区浜松町1−12−4　（第２長谷川ビル４F）
公益社団法人　日本防犯設備協会　事務局
（TEL：03−3431−7301　　FAX：03−3431−7304　mail：info@ssaj.or.jp）

協会技術標準の販売についてご案内します。

公益社団法人 日本防犯設備協会　技術標準（SES E）一覧［頒布価格表］

平成30年10月現在

	規格名称	規格番号	頁数	会員価格※1		一般価格※1		最終発行日
				日本語	英語	日本語	英語	
共通	防犯に関する用語※2	SES E 0001-6	33	1,160	—	1,730	—	2015/5/19
共通	防犯図記号※2	SES E 0002-4	10	600	—	900	—	2015/5/19
技術基準	防犯警報設備一般基準	SES E 0003-3	3	270	—	410	—	2017/5/16
技術基準	環境試験規格	SES E 0004-4	28	2,020	—	3,030	—	2013/1/10
技術基準	防犯警報音規格	SES E 0005-2	5	390	390	570	570	2012/3/31
技術基準	検知器共通技術基準	SES E 0501-4	4	290	—	440	—	2017/5/16
技術基準	マグネットスイッチ規格	SES E 0502-3	3	270	—	410	—	2017/5/16
技術基準	赤外線ビーム検知器規格	SES E 0503-4	5	290	—	440	—	2017/5/16
技術基準	赤外線パッシブ検知器規格	SES E 0504-4	7	440	—	650	—	2017/11/6
技術基準	超音波式検知器規格	SES E 0505-3	5	380	—	560	—	2017/5/16
技術基準	ガラス破壊検知器規格	SES E 0506-3	4	290	—	440	—	2017/5/16
技術基準	シャッタ検知器規格	SES E 0507-4	5	380	—	560	—	2017/5/16
技術基準	防犯用非常通報スイッチ規格	SES E 0508-3	4	290	—	440	—	2017/5/16
技術基準	キー式入出操作器規格	SES E 0509-3	3	270	—	410	—	2017/5/16
技術基準	警報制御盤規格	SES E 1501-4	8	580	—	870	—	2017/5/16
技術基準	防犯用ベル・サイレン規格	SES E 1502-3	4	290	—	440	—	2017/5/16
技術基準	防犯用直流電源装置規格	SES E 1503-3	5	520	—	780	—	2017/8/1
技術基準	警告灯規格	SES E 1504-3	3	290	—	440	—	2017/8/1
技術基準	電子式物品監視装置規格	SES E 1506-3	6	440	—	650	—	2017/8/1
技術基準	センサーケーブル式警報器規格	SES E 1507-3	5	380	—	560	—	2017/8/1
技術基準	自動通報機規格	SES E 1508-3	7	440	—	650	—	2017/11/6
技術基準	防犯灯の照度基準	SES E 1901-4	9	360	—	540	—	2015/2/3
技術基準	センサー付ライト規格	SES E 1902-2	9	660	—	990	—	2017/8/1
技術基準	センサー付防犯灯規格	SES E 1903-2	9	720	—	1,080	—	2017/11/6
技術基準	出入管理装置一般基準	SES E 2001-3	3	270	—	410	—	2018/2/6
技術基準	出入管理装置共通技術基準	SES E 2002-3	3	270	—	410	—	2018/2/6
技術基準	磁気ストライプカードリーダー規格	SES E 2004-4	4	290	—	440	—	2018/2/6
技術基準	ゲート管理装置規格（ホテル用）	SES E 2005-3	6	440	—	650	—	2018/2/6
技術基準	出入管理コントローラ規格	SES E 2006-3	6	460	—	680	—	2012/3/31
技術基準	鍵管理装置規格	SES E 2007-3	5	380	—	560	—	2018/2/6
技術基準	ICカードリーダー規格	SES E 2008-3	4	290	—	440	—	2018/2/6
技術基準	非接触カードリーダー規格	SES E 2009-4	5	360	—	540	—	2018/2/6
技術基準	キーパッド装置規格	SES E 2010-3	6	440	—	650	—	2018/2/6
技術基準	指紋認証装置規格	SES E 2011-3	7	520	—	780	—	2018/2/6
技術基準	出入管理用記録プリンター規格	SES E 2012-3	5	380	—	560	—	2018/2/6
技術基準	出入管理用電動シャッターインターフェース基準	SES E 2013-3	6	440	—	650	—	2018/2/6
技術基準	出入管理装置シリアルインターフェース(RS-232C)基準	SES E 2014-3	5	380	—	560	—	2018/2/6
技術基準	出入管理用自動ドアインターフェース基準	SES E 2015-3	5	380	—	560	—	2018/2/6
技術基準	出入管理用ソフトウェア規格	SES E 2016-2	8	600	—	900	—	2012/3/31
技術基準	出入管理用ソフトウェア管理データ入出力ファイル様式基準	SES E 2017-2	15	1,030	—	1,550	—	2018/2/6
技術基準	防犯用映像監視装置一般基準	SES E 3001-2	3	270	—	410	—	2010/3/31
技術基準	防犯用映像監視装置共通技術基準	SES E 3002-2	4	290	—	440	—	2010/3/31
技術基準	映像用モニタ規格	SES E 3004-3	9	660	—	990	—	2016/2/9
技術基準	映像用制御機器規格	SES E 3006-2	2	190	—	280	—	2010/3/31
技術基準	映像処理機器規格	SES E 3007-2	3	270	—	410	—	2010/3/31
技術基準	映像用旋回機器規格	SES E 3008-2	3	270	—	410	—	2010/3/31
技術基準	映像用ハウジング規格	SES E 3009-2	3	270	—	410	—	2010/3/31

※1 価格には消費税を含んでおります。（送料別途）
※2 協会ホームページよりダウンロードできます。その他の規格については当協会ホームページで閲覧可能です。

協会技術標準の販売についてご案内します。

公益社団法人 日本防犯設備協会　技術標準（SES E）一覧［頒布価格表］

平成30年10月現在

	規格名称	規格番号	頁数	会員価格※1		一般価格※1		最終発行日
				日本語	英語	日本語	英語	
技術基準	映像伝送装置規格（有線方式）	SES E 3010-2	6	440	—	650	—	2010/3/31
	監視カメラ用レンズ規格	SES E 3011-2	5	380	—	560	—	2010/3/31
	電動ドーム型防犯カメラ規格	SES E 3012-3	9	520	—	780	—	2017/8/1
	防犯カメラシステム評価用チャート規格	SES E 3013-2	3	270	—	410	—	2011/3/31
	IP-IF対応防犯カメラ規格	SES E 3101-2	11	790	—	1,180	—	2013/5/31
	IP-IF対応デジタルレコーダ（防犯用）規格	SES E 3102-1	10	720	—	1,080	—	2013/5/31
	HD-SDI対応防犯カメラ規格	SES E 3151-1	12	860	—	1,290	—	2016/11/7
	HD-SDI対応デジタルレコーダ（防犯用）規格	SES E 3152-1	12	860	—	1,290	—	2016/11/7
	HD-SDI周辺機器取扱い規格	SES E 3153-1	5	380	—	560	—	2016/11/7
	NTSC対応防犯カメラ規格	SES E 3201-1	11	790	—	1,180	—	2013/5/31
	NTSC対応デジタルレコーダ（防犯用）規格	SES E 3202-1	18	1,300	—	1,950	—	2013/5/31
	遠赤外線防犯カメラ規格	SES E 3251-1	9	660	—	990	—	2016/2/9
	画角と評価規格	SES E 3401-1	11	790	—	1,180	—	2016/2/9
	テレビドアホン規格	SES E 3501-1	8	600	—	900	—	2013/5/31
	防犯用共同住宅インターホン規格	SES E 3502-1	11	790	—	1,180	—	2016/11/7
施工基準	侵入阻止の意思表示	SES E 7002-4	4	300	—	450	—	2015/5/19
	基本警戒線の設定	SES E 7003-4	6	460	—	680	—	2015/5/19
	防犯対象物件に対する警戒線の選択	SES E 7004-4	7	540	—	810	—	2015/5/19
	警戒方式における検知・警戒範囲	SES E 7005-4	6	460	—	680	—	2015/5/19
	対象物件の施設等級（重要度・危険性の度合）	SES E 7006-4	4	300	—	450	—	2015/5/19
	対象物件の地域環境等	SES E 7007-3	3	280	—	420	—	2015/5/19
	対象物件の見通し	SES E 7008-3	3	280	—	420	—	2015/5/19
	対象物件への侵入防御	SES E 7009-3	3	300	—	450	—	2015/5/19
	侵入警報設備の設計	SES E 7102-4	5	300	—	450	—	2015/5/19
	警戒線の設計	SES E 7103-4	6	390	—	570	—	2015/5/19
	機器の選定方法	SES E 7104-4	4	280	—	420	—	2015/5/19
	施設される回路の電圧	SES E 7202-4	5	300	—	450	—	2015/5/19
	施設される回路の電流	SES E 7203-4	3	280	—	420	—	2015/5/19
	施設される回路の絶縁抵抗	SES E 7204-4	3	280	—	420	—	2015/5/19
	施設される回路の接地	SES E 7205-4	4	280	—	420	—	2015/5/19
	施設される回路の電線	SES E 7206-4	3	280	—	420	—	2015/5/19
	電線の接続	SES E 7207-4	2	300	—	450	—	2015/5/19
	施設される回路の保護装置	SES E 7208-4	3	280	—	420	—	2015/5/19
	施設される回路の充電部の保護	SES E 7209-4	3	220	—	320	—	2015/5/19
	機器の設置場所	SES E 7210-4	4	280	—	420	—	2015/5/19
	電線の施設方法	SES E 7211-4	5	300	—	450	—	2015/5/19
	機器の取付	SES E 7212-3	2	220	—	320	—	2015/5/19
	検査、試験、取扱説明	SES E 7602-3	3	280	—	420	—	2015/5/19
	維持管理	SES E 7702-3	3	280	—	420	—	2015/5/19
共通	SES E標準化規定	SES E 9901-6	8	600	—	900	—	2012/10/1
	SES E規格票の様式	SES E 9902-4	20	1,440	—	2,160	—	2013/3/10
	SES E規格の処理手順（解説）	SES E 9903-5	14	1,010	—	1,520	—	2012/10/1
	防犯に関する用語の登録運用規定	SES E 9905-3	5	440	—	650	—	2017/8/1
	防犯図記号の登録運用規定	SES E 9906-3	5	440	—	650	—	2017/8/1

申込み先、問合せ先

〒105-0013 東京都港区浜松町1-12-4　（第２長谷川ビル４F）
公益社団法人　日本防犯設備協会　事務局
（TEL：03-3431-7301　　FAX：03-3431-7304　mail：info@ssaj.or.jp）

平成 30 年　警察白書　（抜粋）

平成30年警察白書が発表され、特集として「近年における犯罪情勢の推移と今後の展望」について掲載されております。本誌では、この中より刑法犯認知件数推移と、総合的な犯罪対策、新たな課題への対応と今後の展望（犯罪情勢分析の高度化と効果的な情報発信）について抜粋し紹介いたします。

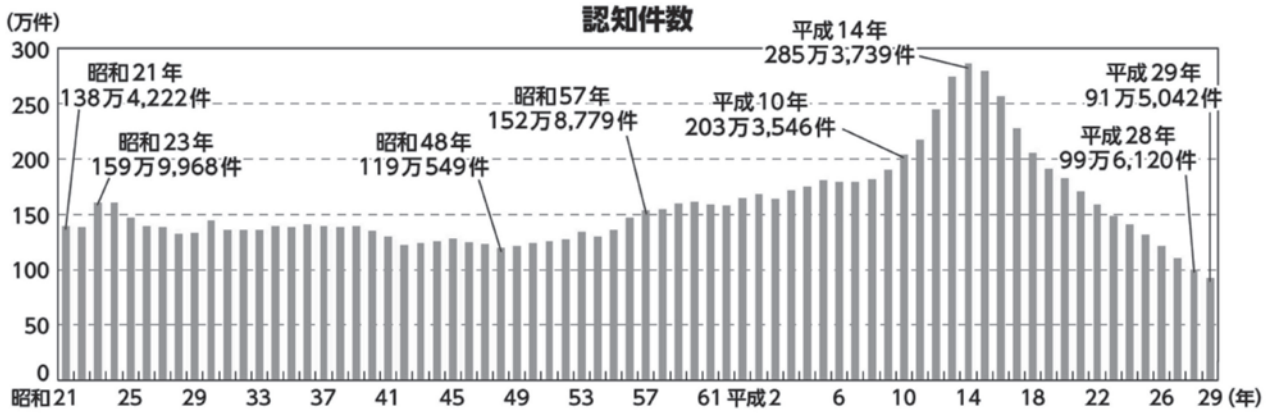
（警察庁HPより）

犯罪情勢

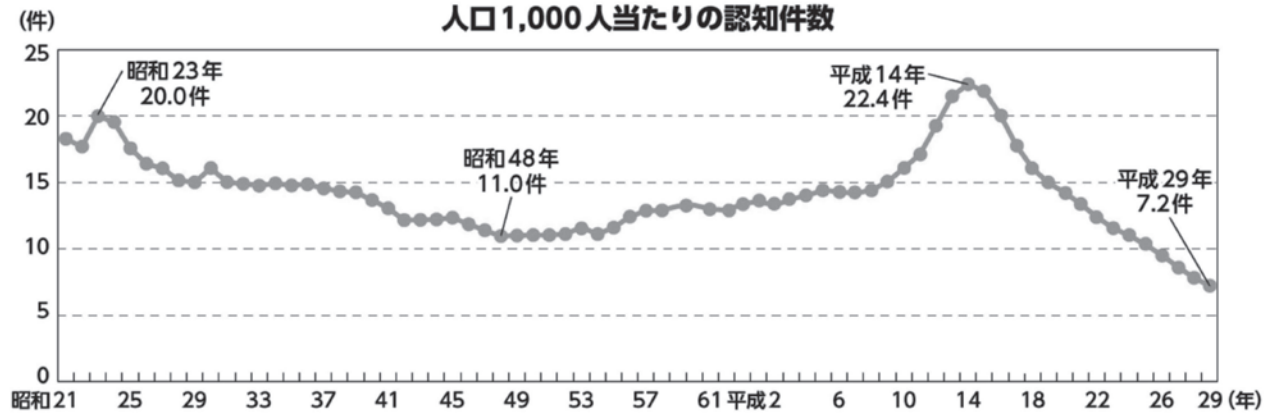
＜概要＞

刑法犯認知件数は、平成29年中は約91万5,000件と、前年より8万件以上減少しており、ピーク時の平成14年と比べ約194万件（67.9%）減少している。また、人口1,000人当たりの刑法犯認知件数は、平成29年は戦後最少の7.2件となった。

刑法犯認知件数及び人口1,000人当たりの刑法犯認知件数の推移（昭和21～平成29年）



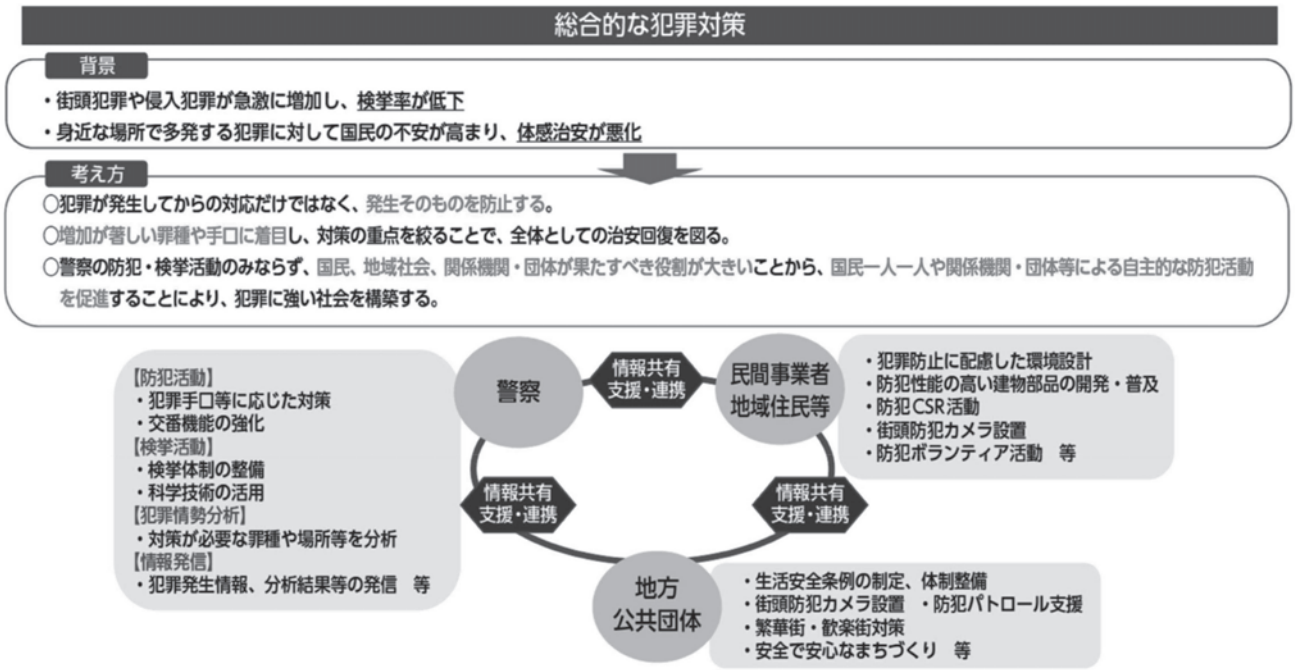
区分＼年次	平成20	21	22	23	24	25	26	27	28	29
認知件数（件）	1,826,500	1,713,832	1,604,019	1,502,951	1,403,167	1,314,140	1,212,163	1,098,969	996,120	915,042
検挙件数（件）	573,392	544,699	497,356	462,535	437,610	394,121	370,568	357,484	337,066	327,081
検挙人員（人）	339,752	332,888	322,620	305,631	287,021	262,486	251,115	239,355	226,376	215,003
検挙率（%）	31.4	31.8	31.0	30.8	31.2	30.0	30.6	32.5	33.8	35.7



注:算出に用いた人口は、総務省統計資料「国勢調査」又は「人口推計」（各年10月1日現在人口（平成12年までは補完補正人口、13年以降は補完補正を行っていいないもの））による。

総合的な犯罪対策の枠組みの構築

警察では、平成15年を治安回復元年とすべく、同年以降、総合的な犯罪対策を推進した。



新たな課題への対応と今後の展望

＜犯罪情勢分析の高度化と効果的な情報発信＞

(1) 犯罪情勢分析の高度化

効果的かつ効率的な犯罪対策を講ずるためには、絶えず変化する犯罪情勢の分析を高度化し、その分析に基づいた取組を推進する必要があり、今後は、専門家や民間事業者の知見、人工知能等の技術を一層活用し、より効果的かつ効率的な警察活動の在り方を検討する必要がある。また、社会情勢、人口動態等の変化が犯罪情勢に与える影響の視点を取り入れた犯罪情勢分析の高度化を進めていく必要がある。

(2) 効果的な情報発信

今後は、国民の権利利益、国の安全等が害されることのないように配慮しつつ、国民がインターネット等を通じてより容易に利用できるよう、既に警察において公開している情報を利用しやすい形に加工し、汎用性を高めるなど、オープンデータ化を一層進める必要がある。

＜今後の展望＞

刑法犯認知件数は平成14年をピークに一貫して減少しており、犯罪情勢には一定の改善がみられる。これは、政府、警察、地方公共団体、民間事業者等が一体となって様々な犯罪対策を推進してきたことなどによるものと考えられる。一方、人身安全関連事案が増加傾向にあることに加え、特殊詐欺の被害が深刻な状況にあり、サイバー空間における脅威も増大しているなど、犯罪情勢は依然として予断を許さない状況にある。これらの治安上の課題は、少子高齢化が進展し、コミュニケーションやビジネスにおける情報通信技術の活用が不可欠となる中で、これまで以上に深刻な問題となることが予想され、警察は、従来とは異なる対策を的確に講じていかなければならない。

こうした新たな課題を含め、今後の様々な治安上の課題に的確に対処するためには、これまでの対策を不断に見直すことに加えて、社会情勢の変化に迅速かつ柔軟に対応し、民間事業者等と連携しながら、犯罪情勢分析の高度化、人工知能等の技術の活用、更なる情報発信等、これまでにない手法や知見を積極的に取り入れながら、より効果的かつ効率的な対策を講じていくべきである。

●「平成30年 警察白書」詳細はこちらをご覧ください。　https://www.npa.go.jp/hakusyo/h30/index.html

編集後記

前回の「防犯設備」盛夏号の編集後記で、協会の1階の駐車場にツバメが巣を作ったと紹介しましたが、その後、ツバメは見かけなくなってしまいました。巣はそのまま残っています。ツバメの巣があるうちは繁栄するとよく言われており、雛を見るのを楽しみにしていましたので残念です。ツバメは古い巣を修復してまた使うこともあるようですので、連年また来てくれることを期待しています。

さて、話はかわりますが、最近のニュースで来年初めに日本にいよいよレジなし自動精算店がオープンするようです。既にアメリカでは今年、コンビニ「アマゾン・ゴー」を開店させ話題となりました。スタンダード・コグニションというアメリカの振興企業で試験店舗として日本企業と組んではじめるようです。客が商品を棚から取ったり戻したりするのをカメラなどで認識。スマートフォンのアプリを通じ、店外に持ち出された商品だけに課金するというものです。

既に、スタンダード・コグニションでは「Standard　Market（スタンダード・マーケット）」をサンフランシスコにオープンしており、185.8㎡（約56.3坪）に27台のカメラを設置し、AIを基盤とし、買い物客がどの商品を持っているか、を正確に把握し、買い物客が商品を棚に戻したのか、ポケットやバッグに入れたのか、まで認識するとのこと、少子高齢化の日本で、人手不足解消となるか、今までの買い物の概念が大きく変わるものと思われます。

（S.H）

ご意見・ご感想をお寄せください　協会事務局　e-mail：s.habu@ssaj.or.jp　FAX：03（3431）7304

「日防設ジャーナル」2018 爽秋号（No.122）　平成30年10月24日発行

編　集　公益社団法人　日本防犯設備協会　運営企画会議

発　行　公益社団法人　日本防犯設備協会

〒105-0013　東京都港区浜松町1-12-4（第２長谷川ビル４階）

TEL 03（3431）7301　FAX 03（3431）7304

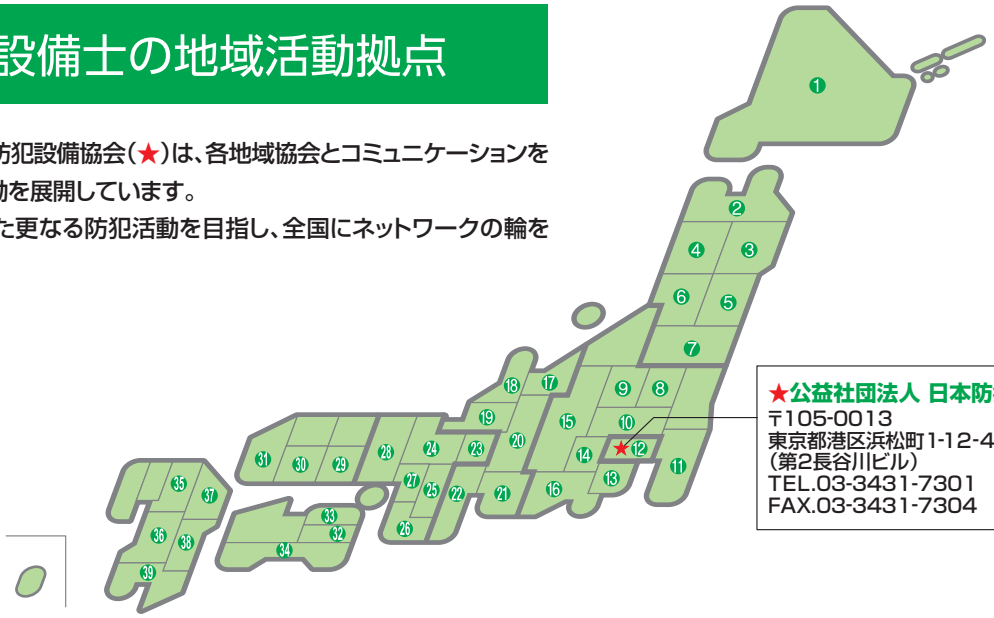
ホームページ　https://www.ssaj.or.jp/

印　刷　真生印刷株式会社　〒101-0041　東京都千代田区神田須田町2-6　TEL 03（5256）7731

本誌掲載記事の複写・転載の際は協会事務局へご連絡ください。

防犯設備士の地域活動拠点

公益社団法人 日本防犯設備協会(★)は、各地域協会とコミュニケーションを図りながら、防犯活動を展開しています。
また、地域に根ざした更なる防犯活動を目指し、全国にネットワークの輪を広げて行きます。



★公益社団法人 日本防犯設備協会
〒105-0013
東京都港区浜松町1-12-4
(第2長谷川ビル)
TEL.03-3431-7301
FAX.03-3431-7304

❶北海道防犯設備士協会
〒065-0017
北海道札幌市東区北17条東7丁目1-15
進栄ロックサービス(株)内
TEL.011-742-3961
FAX.011-742-0473

❷青森県防犯設備協会
〒030-0822
青森県青森市中央2丁目16-15
アシスト青森内
TEL.017-776-6551
FAX.017-776-6551

❸岩手県防犯設備協会
〒024-0023
岩手県北上市里分7-57
南光警備保障(株)内
TEL.0197-65-5110
FAX.0197-65-7215

❹秋田県防犯設備協会
〒011-0904
秋田県秋田市寺内蛭根3丁目24-13
(株)パワーズ内
TEL.018-838-4666
FAX.018-824-8003

❺宮城県防犯設備士協会
〒984-0001
宮城県仙台市若林区鶴代町4番22号
(有)仙台クマックス内
TEL.022-239-8155
FAX.022-239-8154

❻山形県防犯設備協会
〒990-2401
山形県山形市平清水1-1-75
山形パナソニック(株)内
TEL.023-622-5580
FAX.023-623-4370

❼福島県防犯設備協会
〒960-8252
福島県福島市御山字稲荷田83-2
(株)メディアシステム内
TEL.024-534-5810
FAX.024-534-5810

❽栃木県防犯設備協会
〒320-0061
栃木県宇都宮市宝木町1-14-7
(株)宇都宮ロック内
TEL.028-622-1169
FAX.028-622-1125

❾一般社団法人 群馬県防犯設備協会
〒371-0023
群馬県前橋市本町1丁目3-2
橋爪ビル3階
TEL.027-226-0110
FAX.027-226-6400

❿一般社団法人 埼玉県防犯設備士協会
〒338-0002
埼玉県さいたま市中央区下落合6-19-3
(株)ジャロック内
TEL.048-831-3927
FAX.048-825-2812

⓫一般社団法人 千葉県防犯設備協会
〒263-0043
千葉県千葉市稲毛区小仲台2-6-10
木下ビル2階
TEL.043-301-6409
FAX.043-301-6419

⓬NPO法人 東京都セキュリティ促進協力会
〒170-0013
東京都豊島区東池袋1-32-6
河合ビル3階
TEL.03-3985-8676
FAX.03-3985-8678

⓭NPO法人 神奈川県防犯セキュリティ協会
〒220-0011
神奈川県横浜市西区高島2-11-2
スカイメナー横浜312号
TEL.045-451-0232
FAX.045-451-0232

⓮NPO法人 山梨県防犯設備士協会
〒400-0045
山梨県甲府市後屋町363
(株)センティス21内
TEL.055-241-0378
FAX.055-241-4480

⓯長野県防犯設備協会
〒399-0033
長野県松本市笹賀7117-1
アイ・エヌ通信工業(株)内
TEL.0263-86-7788
FAX.0263-85-3311

⓰静岡県防犯設備士生活安全協議会
〒427-0061
静岡県島田市中河原8968-7
(株)日本防災システム内
TEL.0547-35-2001
FAX.0547-35-2023

⓱富山県防犯設備協会
〒939-3541
富山県富山市水橋沖64-1
ライフガード北陸内
TEL.076-479-0801
FAX.076-479-0804

⓲石川県防犯設備促進協力会
〒920-0055
石川県金沢市北町乙63
(株)マスターキー内
TEL.076-262-0110
FAX.076-223-6269

⓳NPO法人 福井県防犯設備協会
〒910-0019
福井県福井市春山1-7-3
染織会館2階
TEL.0776-25-3177
FAX.0776-89-1954

⓴岐阜県防犯設備協会
〒500-8269
岐阜県岐阜市茜部中島3-20
日本ガード(株)内
TEL.058-277-6222
FAX.058-271-4326

㉑愛知県セルフガード協会
〒460-0004
愛知県名古屋市中区新栄町1-1
明治安田生命名古屋ビル10階
アイホン(株)内
TEL.052-961-3501
FAX.052-685-3884

㉒NPO法人 三重県防犯設備協会
〒514-0131
三重県津市あのつ台4丁目7番7
三重電業(株)内
TEL.059-232-0303
FAX.059-232-5586

㉓滋賀県防犯設備士協会
〒520-0101
滋賀県大津市雄琴5-8-12
オプテックス(株)内
TEL.077-579-8999
FAX.077-579-8999

㉔NPO法人 京都府防犯設備士協会
〒602-8027
京都市上京区下立売通新町東入東立売町195
防犯会館1階
TEL.075-411-9111
FAX.075-411-9113

㉕NPO法人 奈良県防犯設備士協会
〒635-0823
奈良県北葛城郡広陵町三吉254-14
アクティブ防犯センター内
TEL.0745-54-5141
FAX.0745-54-5141

㉖和歌山県防犯設備協会
〒640-8301
和歌山県和歌山市岩橋1576-7
近畿システム(株)内
TEL.073-473-9200
FAX.073-473-3024

㉗NPO法人 大阪府防犯設備士協会
〒540-0029
大阪府大阪市中央区本町橋2番23号
第7松屋ビル5階
TEL.06-6585-0061
FAX.06-6585-0062

㉘NPO法人 兵庫県防犯設備協会
〒670-0825
兵庫県姫路市市川橋通2-49-2
セキュリティハウス神姫(株)内
TEL.0792-23-7450
FAX.0792-23-7460

㉙岡山県防犯設備業防犯協力会
〒703-8265
岡山県岡山市中区倉田296-13
(株)セキュリティハウス内
TEL.086-276-0110
FAX.086-276-7478

㉚NPO法人 広島県生活安全防犯協会
〒732-0055
広島県広島市東区東蟹屋町5-10
(株)ロックサービス内
TEL.082-263-5390
FAX.082-262-4169

㉛一般社団法人 山口県防犯設備士協会
〒755-0084
山口県宇部市大字川上528
TEL.0836-38-5224
FAX.0836-33-7613

㉜一般社団法人 徳島県防犯設備協会
〒777-0005
徳島県美馬市穴吹字平ノ内29-1
TEL.0883-52-3280
FAX.0883-53-9775

㉝香川県防犯設備業防犯協力会
〒761-8071
香川県高松市伏石町2157-5
(有)エーワンセキュリティサービス内
TEL.087-815-3917
FAX.087-815-3918

㉞NPO法人 高知県防犯設備協会
〒780-0055
高知県高知市江陽町10-24
土佐通信システム(株)内
TEL.088-882-1891
FAX.088-883-0501

㉟NPO法人 福岡県防犯設備士協会
〒810-0021
福岡県福岡市中央区今泉1-13-28
幸ビル501号
TEL.092-718-3990
FAX.092-718-3995

㊱一般社団法人 熊本県防犯設備協会
〒862-0962
熊本県熊本市南区田迎3-3-23
TEL.096-234-7531
FAX.096-221-8816

㊲大分県防犯設備士協会
〒870-0024
大分県大分市錦町3-4-5
(株)勉強堂内
TEL.097-534-3842
FAX.097-534-0827

㊳NPO法人 宮崎県防犯設備士協会
〒880-0951
宮崎県宮崎市大塚町流合5115-5
(株)九州ガードシステム内
TEL.0985-52-7338
FAX.0985-50-3290

㊴鹿児島県防犯設備協会
〒890-0034
鹿児島県鹿児島市田上5-1-30
(株)セキュリティサービス内
TEL.099-252-3881
FAX.099-252-3841

平成30年10月現在

防犯設備士・総合防犯設備士

受講生・受験生 募集

「防犯設備士」＝「防犯のプロフェッショナル」

今、まさに社会が求めている資格です。

防犯設備士

■防犯設備士とは？

(公社)日本防犯設備協会が行う防犯設備士資格認定試験に合格し、申請により防犯設備士資格者証の交付を受け、同協会の防犯設備士登録簿に登録された方をいいます。また、3年毎の更新義務があり、知識の更新を行います。

■どんなメリットがあるの？

防犯設備機器に関わる職業の方が、自身の社会的地位の証明、製品の知識や施工技術の向上、有資格が条件となる地域協会に加入することが出来ます。有資格者にはメールマガジン配信の申込により協会から各種情報が登録先に発信されます。

■試験概要

養成講習：受講必須（年４回）
認定試験：マークシート式
（養成講習最終日実施）

総合防犯設備士

■総合防犯設備士とは？

(公社)日本防犯設備協会が行う総合防犯設備士資格認定試験に合格し、申請により総合防犯設備士資格者証の交付を受け、同協会の総合防犯設備士登録簿に登録された方をいいます。

総合防犯設備士は、防犯設備士の上位資格として、特に防犯設備の監理および監査並びに防犯設備士の指導、育成を行う者をいいます。総合防犯設備士資格試験は、防犯設備士資格取得後、通算 3年以上の実務経験をもって受験することが出来ます。また、試験は筆記試験および講習認定試験となっており、受験セミナーも開催しています。

■試験概要

筆記試験：1次10月頃、2次(面接)12月頃
講習認定試験：各地域協会からの応募(6月頃)
受験セミナー：年４回(7月～9月頃)

お申し込み・お問い合せ

公益社団法人 日本防犯設備協会

〒105-0013　東京都港区浜松町1-12-4(第2長谷川ビル4F)
TEL 03(3431)7301　FAX 03(3431)7304
メール info@ssaj.or.jp　ホームページ https://www.ssaj.or.jp