2018 SPRING 情報誌

日防設ジャーナル

- **最新の犯罪情勢**：平成29年の犯罪情勢について
- **法令解説**：茨城県ヤード条例の制定とヤード対策
- **技術解説**：ピョンチャン五輪のICT戦略とセキュリティ

No.120
陽春号

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

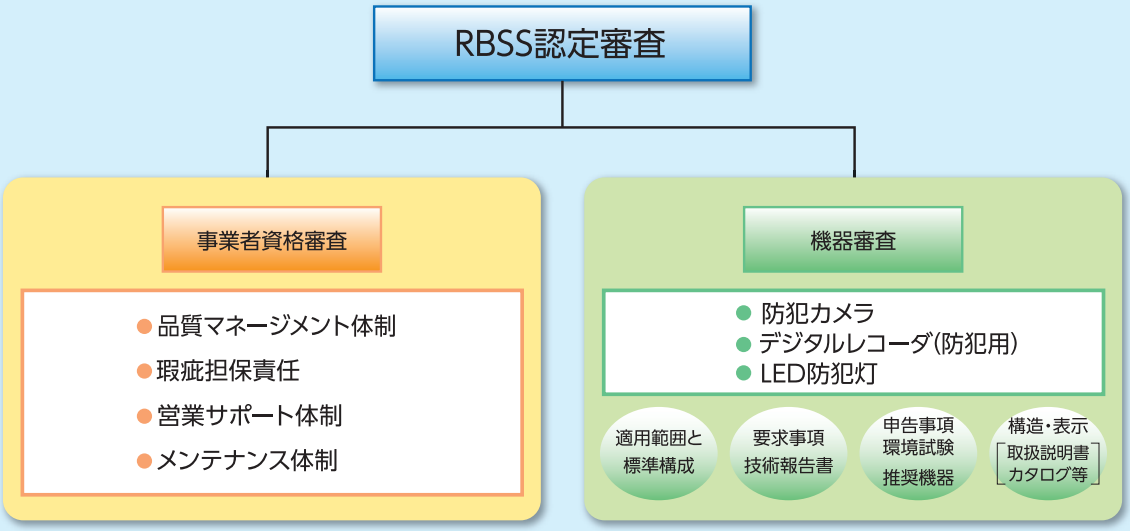
RBSS

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 陽春号 No.120

CONTENTS

巻頭言

「大型施設のセキュリティシステムの変遷」

公益社団法人　日本防犯設備協会　常任理事　横田　光司
（オーテック電子株式会社　代表取締役社長）

早いものでセキュリティの仕事に携わり30有余年、そのほとんどが大型施設のセキュリティシステムの構築に係わるものであった。

当時（1980年代半ば）、都心の大型ビルのセキュリティは未だ常駐警備(人的警備)と部分的な機械警備が中心であったが、一方で徐々にビル全体としての総合的なシステムも導入され始めていた。

その中心はキーボックスシステム（事務室の鍵を保管箱から取り出すと同時に扉のセンサーの警戒がOFFとなり、鍵を保管すると同時にセンサーの警戒がONとなる）であったが、このシステムにはセキュリティ上の大きな問題点が2つ存在していた。

1つは鍵で運用している為、容易に鍵の複製が可能となることであり、もう1つは、事務室の該当フロアーからキーボックスの設置されている1階通用口までの移動時間が無警戒状態となることであった。

そこで、事務室の各扉に電気錠とカードリーダーを設置しセンサーの警戒をOFFにすると同時に電気錠が解錠となり、センサーの警戒をONにすると同時に電気錠が自動施錠されるキーレスシステムも導入されるようになった。

しかし、当時は磁気カード方式であった為、昼間時間帯は電気錠が解錠状態つまりフリーのままとする運用が一般的であった。

その後2000年代に入ると、非接触ICカードの普及と共に扉を常時施錠し、入室の度にカードを翳して電気錠を解錠する運用が一般化される事となった。また、現在では事務室フロアーの共用部のセキュリティグレードを高める為、1階のエントランスにセキュリティゲートを設けカードを所持しない人はエレベーターホールに入場できなかったり、エレベーターシステムと連動し、カードが無いと該当の事務室フロアーにエレベーターが着床しない等のシステムも一般化されている。

ICカード以外にも重要な部屋の出入りには、カードの貸し借りによる本人への「なりすまし」を防ぐ目的でバイオメトリクス（生体認証）装置が利用されている。当時、国内では指紋認証装置が開発・導入され始めた頃であった。その後、掌形・静脈・虹彩等のシステムが開発または輸入され、入退室のみならず、例えば金融機関のATMの本人確認にも利用されるようになっている。また、現在では画像認識技術の進歩により、顔画像で認証するシステムも普及している。

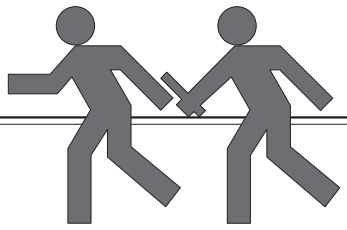
監視カメラシステムについても当時はモノクロが主流であり、撮像管のカメラも存在していた。その後CCD化されカラーが当たり前の時代となり、更にデジタル化・ネットワーク化されたことにより、当時では考えられないほど沢山の高画質カメラが現在では至る所に設置されている。

まさにこの30年は他の分野における製造技術と同様、セキュリティシステムの進歩・技術革新が目覚しい時代であった。

しかし、いくら技術が進歩したとしてもそのハードを有効に活用する為には、リスクを想定してセキュリティポリシーを決定し、十分な運用想定に基づいた計画を立案しなければならない。更に稼動後はシステムと運用との整合性の監査を継続的に行なう事も必要となる。

高価なセキュリティ機器を導入したが、当初からシステムと運用が完全に合致しなかったり、導入後の運用の変化により徐々に有効利用されなくなったりするケースを数多く見てきた。

長年セキュリティシステムの構築に携わった人間の責務として、セキュリティとは、ハードとソフト（計画・運用・維持）の両輪が完全に融合することが不可欠であることを今後も語り続けていきたい。



『プロ野球選手の眼からみたお客様の姿』

株式会社ゴール　代表取締役社長　岸本　俊仁

私には、40数年たった今でも脳裏に鮮明に焼き付いている光景がある。それは、昭和49年10月14日に後楽園球場で行なわれた、長嶋茂雄さんの引退試合の模様である。

その当時、私は大学生で朝のニュースでその事を知り、居ても立ってもいられなくなり、ゼミの友人4～5人と授業を自主休校にして、後楽園球場に駆け付けた。その年は、中日ドラゴンズの優勝が決まっており、巨人にとっては消化試合であったが、スタンドは超満員で、球場に入りきれない人達が周りを取り囲んでいる様な状況だった。

また、その時の引退セレモニーの挨拶は、伝説となっている「我が巨人軍は永久に不滅です」ですが、球場を包む雰囲気は異常なもので、例え様のない熱気を帯びていた。そして、第一試合終了後に長嶋さんが外野を一周した時には、興奮が最高潮に達して、絶叫が球場を包み込んでしまった様な感覚に落ち入った事を覚えている。

そのような状況の中、面白かったのは携帯電話が無い時代だった為、会社員の人達が攻守交替の度に公衆電話の前に長い列を作り、会社や得意先に遅くなっている嘘の言い訳をしている姿が滑稽だった。そう云う私も、長嶋さんがデビューした頃からのファンで、あの躍動感あふれるプレーから不可能を可能に変えてくれそうなワクワク感に堪らない魅力を感じていた一人だった。だからこそ、引退試合を眼に焼き付けておきたい心理は良く理解出来たものである。しかし一方で、大勢の人達を惹きつける源泉はいったいなんなんだろうかと、その時漠然と考えていたもう一人の自分もいた。

後年（40年位経って）、プロ野球の解説者の講演を聞く機会があり、その題目はかつてプレーした球団の三人の監督論であった。

まず一人目は、球団や多くの選手を再生させ野村再生工場と言われた、野村克也氏である。野村さんは、ID野球と云われた様に、体の仕組みから機能迄説明し、どの機能を鍛えれば筋肉が強化され、打球が早く遠く迄飛ぶようになるかを理論的に説明し、それを具体的に指導されたとの事。それ迄は、深く考えたこともなかったが、言われた通りにすると、飛距離も伸び、ホームラン数も打率もアップしたと話された。野村さんは、『理論の人』であったとの事。

二人目は、闘将と言われ鉄拳制裁も辞さない指導の星野仙一氏である。星野さんは、一見強面で直線的に突き進むように見えているが、実は計算された行動であり、相手を考えてその人に合った話し方で指導をするタイプであったらしい。繊細な選手には、ミスをしてもあまり怒らず、逆に精神的なフォローをしていたとの事。また、解説者の様に叱りやすいタイプの選手には、鉄拳制裁も辞さなかったらしい。これは、星野さんが監督として尊敬していた元巨人軍監督の川上哲治氏より学んだ管理術である。川上さんは、ミスをした負け試合の反省会では、まず長嶋さんを故意に叱責したらしい。そうする事によって、他の選手にはあの長嶋さんが叱られているのだからと、何も言わなくても十分に効き目があったとの事。但し、完全主義者の王さんには、一言も

言わなかったと聞いた事がある。人の性格も考慮して、誉めたり、叱ったりして選手を上手く乗せながら使う。星野さんは、『言葉の人』であったとの事。

三人目は、ミスター・プロ野球と言われた長嶋茂雄氏である。長嶋さんは、一般的には天才・感性の人と言われている。しかし、彼の頭の中には、プロである以上、技術が有るのは当然である。だからこそ、その技術を如何に見せ、ファンの方々に満足してもらえるかが大事であると考え、常々選手にも言っていたらしい。具体的には、無様な試合をして負けた時には必ず選手全員が監督室に集合させられ、お客様に申し訳ないとコンコンと説教されたとの事。この根底には、プロ野球は入場券を買って球場に観戦に来てくださるファンやテレビの向こうで、応援してくれているファンあってのもので、給料を払ってくれる球団や親会社のものではない。また、君達選手は日によっては調子の悪い時や体調の思わしくない時があるかもしれない。君達にとっては、130分の1の試合かもしれないが、球場に足を運んでくださる方々にとっては、1年に1回、もしくは一生に1回の試合かもしれないではないか。そのファンの方々に失礼な試合をするとは何事かと言われたらしい。それ故にプレイヤー時代の長嶋さんは、出場した全ての試合には全力で臨んだし、監督になってからも選手全員にその事を望んだらしい。長嶋さんは常にプロ野球ファンを大事にした『ファン第一の人』であったとの事。

これらのエピソードには有名な三人の監督の物の見方・考え方がでていて面白い。この講演を聞いていて、冒頭に書きました様に、長嶋さんが野球界だけでなく、一般の人々に何故好かれているのかの一端を垣間見たような気がした。

三人の監督の考えに鑑みて、同時代の日本の産業界も躍動感が有り、組織も制度も機能しており人々の要望に合った商品やワクワク感を感じさせる奇想天外な物が出てくる予感があった。事実、戦後の日本経済を牽引した多くの業界でこの様な現象が見受けられたと思う。いつの時代にも、人々から支持されるヒット商品と云うのは、長嶋さんのプレーに感じたワクワク感に似ていて、ニーズを的確に掴んで、使ってみたいと云う気にさせるものだと思う。

それでは、私が属する業界はどうだろうかと考えてみた。私どもの業界は、一般錠前や電気錠システム等を製造販売しているロックメーカーであり、玄関や勝手口をメインに外部に面する扉に付いていて、人の生命や資産を守るセキュリティー産業である。ただ、今まで玄関錠にワクワク感を持っていたのは泥棒が多かったでしょうが、これからは一般の方々も、安全・安心に基づく商品選びが大事になってくるはずである。また、企業サイドからすれば、錠前の種類は多岐にわたり、年間に何十万・何百万セット出荷されている。

しかし、長嶋さんの様な観点に立てば、企業にとっては何百万分の1かもしれないが、殆んどのお客様にとっては、1年に1回どころか一生に1回か2回位しか購入しない商品も多いはずである。お客様にすれば、購入した1セットが全てなのである事を企業は認識する必要があると思う。

今、コンプライアンスの重要性が叫ばれているが、これはどの組織にもあてはまる事と当然思われる。今一度お客様に信頼してもらい、ワクワク感を感じさせるような製品作りに、真摯に取り組まなくてはいけないと教えられた気がした。

「平成29年の犯罪情勢について」

警察庁生活安全局生活安全企画課　課長補佐　深見　幸治

1 はじめに

「犯罪情勢」というものを正確に把握するには、警察が犯罪の発生を認知した件数等の指標である「犯罪統計」、国民が治安に関して感じている「体感治安」、「サイバー空間の脅威」、「国際テロ情勢」等の犯罪リスクの増大に関するもの等を複合的に勘案する必要があると考えています。

そうした検討は、他稿に譲るとして、本稿においては、「犯罪統計」のうちでも刑法犯認知件数を中心に、平成29年の情勢をみていくこととします。なお、本稿中の意見に係る部分については、小職の私見であることを申し添えます。

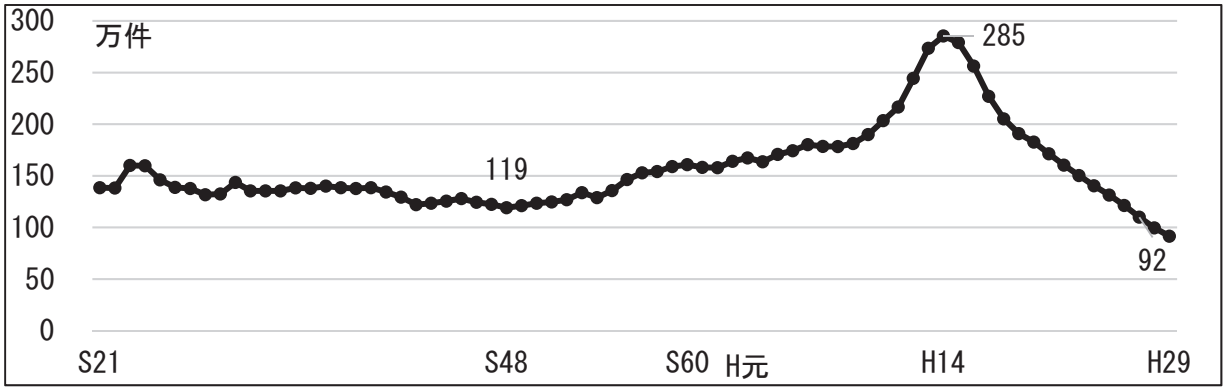
2 刑法犯認知件数の推移

我が国における昭和21年以降の刑法犯認知件数の推移は、昭和48年を底として、平成に入り顕著な増加基調になり、平成8年以降は戦後最多を毎年更新し続け、平成14年に約285万件を記録しました。

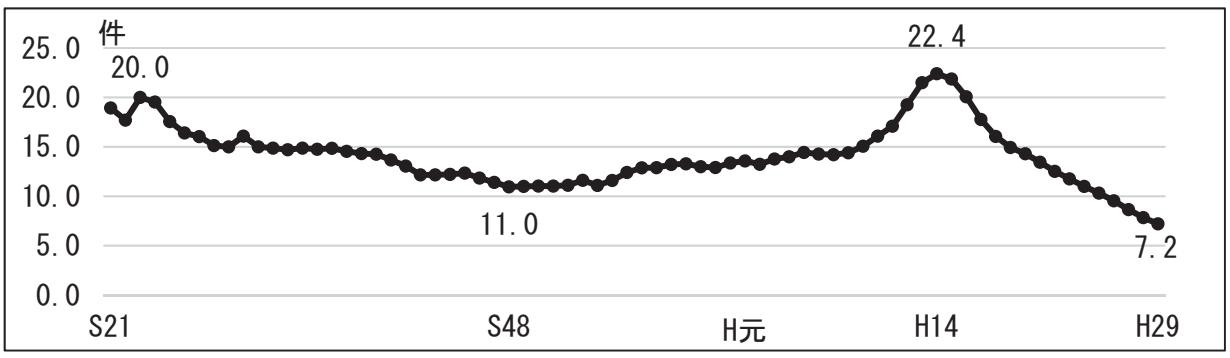
その後は、15年連続して減少を続け、平成29年には91万5,042件と3年連続で戦後最少を更新しました。

また、人口千人当たりの刑法犯認知件数においても、平成14年のピークから減少を続け、平成29年は7.2件と戦後最少の数値を更新したところです。

刑法犯認知件数の推移（S21 ～）



人口千人当たりの刑法犯認知件数の推移（S21 ～）



3 重要犯罪の刑法犯認知件数の推移

警察においては、刑法犯のうち殺人、強盗などの個人の生命、身体及び財産を侵害する度合いが高く、国民の脅威となっている犯罪を重要犯罪として重点的な対処を行っています。

過去10年の重要犯罪の発生状況をみると、31.6%減少しており、特に強盗は過去10年で56.9%減少するなど、顕著な減少をみています。

なお、平成29年の重要犯罪の検挙率は80.4%ですが、重要犯罪の検挙率が80%を超えるのは19年ぶりとなりました。

重要犯罪の刑法犯認知件数等の推移（H20～）

	H 20	H 21	H 22	H 23	H 24	H 25	H 26	H 27	H 28	H 29
重要犯罪	15,922	15,271	14,878	14,144	14,581	14,596	14,051	12,565	11,546	10,888
殺人	1,301	1,095	1,068	1,052	1,032	938	1,054	933	895	920
強盗	4,298	4,535	4,051	3,695	3,691	3,324	3,056	2,426	2,332	1,852
放火	1,441	1,347	1,212	1,122	1,081	1,086	1,093	1,092	914	959
強制性交等	1,590	1,415	1,293	1,193	1,266	1,409	1,250	1,167	989	1,109
略取誘拐・人身売買	155	156	186	153	190	185	198	192	228	239
検挙率(%)	62.3	64.0	62.4	63.4	65.1	63.4	68.2	72.3	76.6	80.4

4 重要窃盗犯の刑法犯認知件数の推移

重要窃盗犯（窃盗犯のうち侵入窃盗、自動車盗、すり、ひったくりをいう。）の過去10年の発生状況をみると、57.4%減少しており、全ての手口で50%以上の減少をしているなか、特にひったくりは過去10年で84.9%減少するなど、顕著な減少をみています。

なお、検挙率は、過去10年間は50%前後で推移していますが、平成29年は過去10年では最高の55.3%でした。

重要窃盗犯の刑法犯認知件数等の推移（H20～）

	H20	H21	H22	H23	H24	H25	H26	H27	H28	H29
重要窃盗犯	210,530	201,037	181,567	169,653	152,219	142,259	120,488	108,558	95,302	89,753
侵入窃盗	155,270	148,771	136,749	126,382	115,328	107,313	93,566	86,373	76,477	73,122
自動車盗	27,668	25,960	23,970	25,238	21,319	21,529	16,104	13,821	11,655	10,213
ひったくり	19,165	19,053	14,587	12,493	10,097	7,909	6,201	4,142	3,493	2,894
すり	8,427	7,253	6,261	5,540	5,475	5,508	4,617	4,222	3,677	3,524
検挙率(%)	53.5	50.8	47.7	48.0	49.8	47.5	51.5	52.6	54.6	55.3

5 住宅を発生場所とする侵入窃盗の発生状況

日本防犯設備協会に関係の深い罪種として、侵入窃盗のうち特に住宅を発生場所とする空き巣、忍込み及び居空き（以下「空き巣等」という。）の情勢をみると以下のとおりです。

(1) 住宅形態別発生状況

過去5年間における空き巣等の発生について住宅の形態別にみてみますと、一戸建住宅が発生の約7割を占める傾向で推移しています。

住宅1万戸当たりの発生件数をみてみますと、平成29年は、一戸建住宅が4階建以上共同住宅の約4倍発生しました。

住宅で発生した空き巣等の侵入窃盗認知件数の推移（H25-H29）

	H25	H26	H27	H28	H29
合計	57,574	47,944	45,924	39,090	36,881
空き巣	40,619	34,116	31,374	27,058	25,511
一戸建住宅	26,305	21,398	19,875	17,576	16,418
４階建以上共同住宅	3,866	3,306	3,048	2,612	2,427
３階建以下共同住宅	10,448	9,412	8,451	6,870	6,666
忍込み	13,683	11,098	12,169	9,828	9,470
一戸建住宅	11,212	9,226	10,515	8,296	8,179
４階建以上共同住宅	792	499	443	452	389
３階建以下共同住宅	1,679	1,373	1,211	1,080	902
居空き	3,272	2,730	2,381	2,204	1,900
一戸建住宅	2,512	2,079	1,770	1,728	1,485
４階建以上共同住宅	254	228	199	153	136
３階建以下共同住宅	506	423	412	323	279

（注）空き巣……家人等が不在の住宅の屋内に侵入し、金品を窃取するもの。
忍込み……夜間家人等の就寝時に住宅の屋内に侵入し、金品を窃取するもの。
居空き……家人等が在宅し、昼寝、食事等しているすきに住宅の屋内に侵入し、金品を窃取するもの。

住宅１万戸当たり空き巣等の侵入窃盗認知件数の推移（H25-H29）

	H25	H26	H27	H28	H29
空き巣等侵入窃盗	11.1	9.2	8.8	7.5	7.1
一戸建住宅	14.0	11.4	11.2	9.7	9.1
４階建以上共同住宅	3.8	3.1	2.8	2.5	2.3
３階建以下共同住宅	12.0	10.7	9.6	7.9	7.5

（注）住宅数は、国土交通省住宅経済関連データ中平成 25 年統計の居住住宅数を計上した。

(2) 侵入手段別発生状況

過去5年間における空き巣等の発生について侵入手段別についてみてみますと、無締りとガラス破りが、発生の8割以上を占める傾向で推移しています。

ガラス破りは、平成29年の発生件数中34.5%を占めていますが、特に空き巣では、無締りを上回る最多の件数であるなど、主要な侵入手段となっています。

いわゆるピッキング用具等の特殊開錠用具については、過去5年間も減少を続けておりますが、平成20年と比較すると1,294件減少し、減少率では89.7%となっています。

空き巣等侵入手段別認知件数の推移（H25-H29）

	H25	H26	H27	H28	H29
認知件数（件）	57,574	47,944	45,924	39,090	36,881
無締り	25,995	22,265	21,591	18,996	17,302
ガラス破り	21,399	16,840	16,080	12,894	12,740
施錠開け	3,029	2,422	2,539	2,207	2,218
合かぎ	1,811	1,542	1,600	1,475	1,479
特殊開錠用具関係	260	212	212	161	148
その他の施錠開け	958	668	727	571	591
ドア錠破り	1,267	1,153	1,009	932	814
戸外し	302	254	225	221	174
その他	2,304	1,934	1,769	1,511	1,445
不明	3,278	3,076	2,711	2,329	2,188

6 治安に関する世論調査

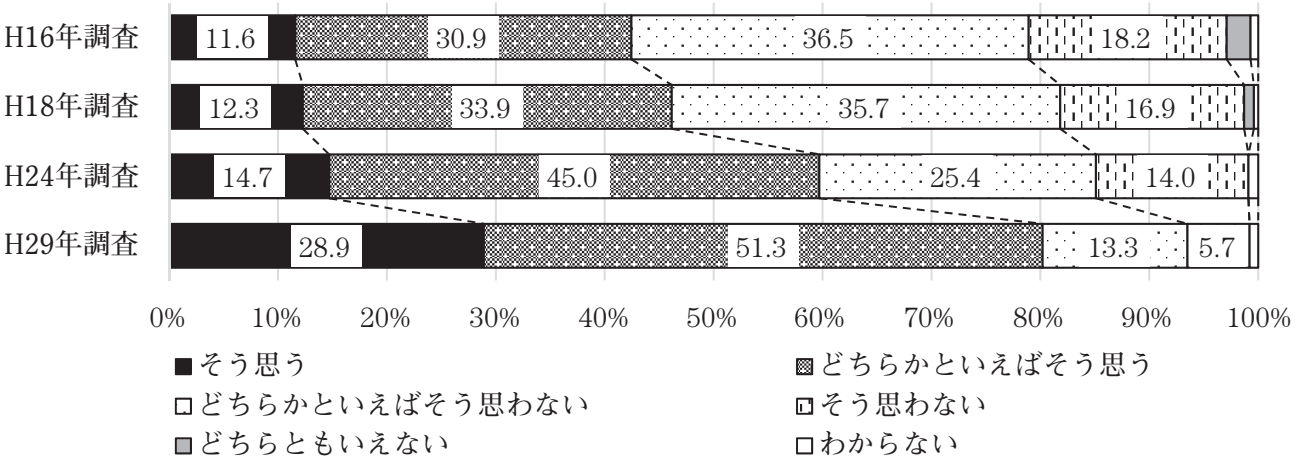
これまで、犯罪統計をみてきましたが、昨年、内閣府において5年ぶりに「治安に関する世論調査」を実施したところ、過去3回の調査と比較すると下記の表のとおりの結果となりました。

まず、「現在の日本が、治安がよく、安全で安心して暮らせる国だと思いますか。」という設問では、80.2%が「そう思う」又は「どちらかといえばそう思う」と答え、前回調査からは約20ポイント、平成16年調査からは約40ポイントも国民の意識は改善しました。一方で、「ここ10年間で日本の治安はよくなったと思いますか。それとも、悪くなったと思いますか。」という設問では、過去の調査と比較して「よくなったと思う」又は「どちらかといえばよくなったと思う」という回答が増加しているものの、依然として約6割の人が「悪くなったと思う」又は「どちらかといえば悪くなったと思う」と回答しました。

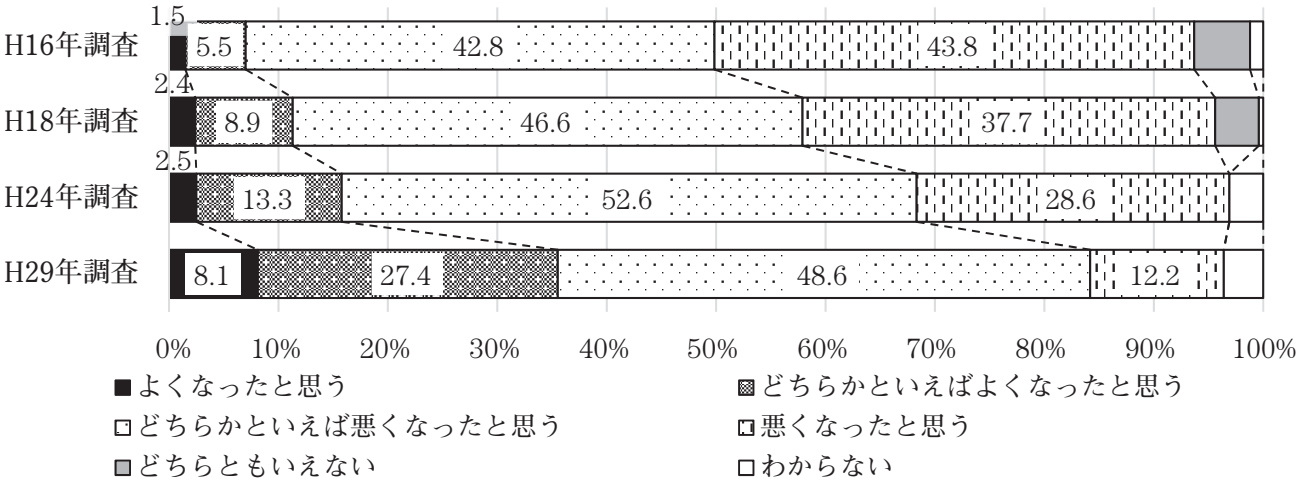
このように、昨年の世論調査においては、国民の体感治安の改善は一定程度みてとれましたが、その他の設問の回答から、インターネット利用犯罪や、振り込め詐欺など、新たな形態や非対面の犯罪に対する不安が増大していると推察されるところです。

治安に関する世論調査の結果

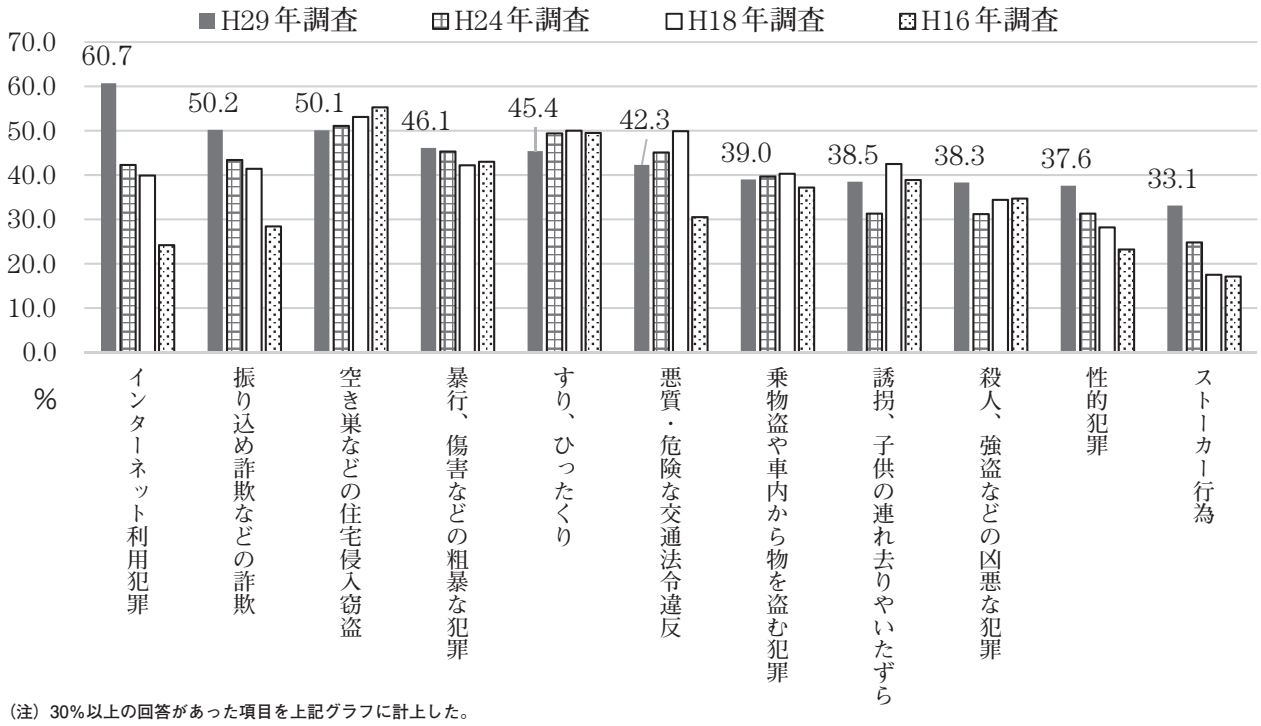
日本は安全・安心な国か



ここ10年の治安に関する認識



不安を感じる犯罪



（注）30%以上の回答があった項目を上記グラフに計上した。

7 さいごに

我が国の犯罪情勢については、刑法犯認知件数がピーク時より大幅に減少するとともに、国民の体感治安も改善基調で推移するなどしているところです。

これは、平成14年以降、防犯カメラや防犯性能の高い建物物品等の普及促進、地域住民等による自主防犯活動の活性化等の官民一体となった的確な犯罪対策を推進してきた成果によるものと認識しているところです。

しかし、他方でサイバー犯罪、特殊詐欺、子ども・女性等の社会的弱者に対する犯罪等の発生が、国民の安全安心に対する脅威や不安を与えているなど、予断を許さない犯罪情勢にあります。

警察としては、今後とも、日本防犯設備協会の皆様をはじめ、官民一体となった幅広い犯罪抑止対策を推進し、我が国の治安水準の一層の向上に努めてまいります。

犯罪防止と企業の役割

積水化学工業株式会社　顧問　国士舘大学非常勤講師
元警察庁生活安全局審議官
荒木　二郎

日防設様に初めて接したのは、筆者が警察庁防犯企画課の理事官当時で、日防設創設から6年目位、防犯設備士の第一回の認定試験のときでした。

貴協会にあっては、犯罪防止についての関心が、警察部内でも、また社会全体でも今日ほど高くなかった時代から30年余の間、孜々営々として防犯機器の性能向上、防犯設備士制度の運用等を通じて、犯罪の防止、社会の安全安心確保のためにご尽力をいただいており、改めて敬意を表する次第です。

当時と比べると、組織も格段に充実され、優良機器認定制度、防犯優良マンション認定事業等、時代の要請に応じて新たな事業も加わり、隔世の感があります。

ご案内のように、日本の犯罪件数は、平成14年の約285万件をピークに減少を続けており、昨年は約91万件とピーク時の1/3以下となりました。昨年の内閣府の調査では、日本は治安がいいと思う人が8割を超えており、調査開始以来最高を記録しています。この犯罪の減少には、私見ですが、以下のような要因があると考えております。

一つには、警察が本腰を入れて犯罪の減少に取り組んだ事です。言うまでもなく、警察の目的は、「個人の権利と自由を守り、公共の安全と秩序を維持すること」（警察法1条）です。犯罪、事故等を防止し、国民の生命、身体、財産の安全を守ることこそ、警察の任務ということができます。

戦後の混乱期以来、犯罪が多発し、警察の体制も弱く、警察は起きた犯罪を検挙することで手一杯でした。警察は、「泥棒など悪い人を捕まえるところ」というイメージを持つ人が多く、また、戦前の保安処分等、犯罪が起きる前の警察介入が人権侵害につながったとする考えもあって、社会一般の風潮も警察が事前に犯罪を予防するよりも、犯罪が起こった後で犯人を検挙することを警察に期待していたという歴史的経緯があったと考えられます。

しかしながら、犯罪が起きてから検挙するだけでは、国民の生命、身体、財産はすでに侵害されてしまっており、警察の目的である個人の権利と自由を守ることは、達成されません。性犯罪被害者、殺人被害遺族等から、より積極的に犯罪の未然防止を求める声が上がり、ストーカー、ＤＶ、児童虐待等について、事件にならないから相手にしないという警察の相談や被害申告に対する消極的対応が大きな問題となりました。

このようなことから、警察は犯罪検挙だけでなく、犯罪抑止を目指す方向へ大きく舵を切り、15年前の平成15年以降、「街頭犯罪、侵入犯罪抑止総合対策」を強力に推進しています。

二つは、「自助」、「共助」、「公助」による犯罪防止活動の推進です。犯罪の検挙は、警察にしかできないことであり、「悪いことをしたら捕まる」ということで犯罪の抑止効果（「一般予防」）があります。また、犯人を一定期間刑務所に収容し、社会から隔離できるとともに、再犯防止の教育も可能となります（「特別予防」）。

したがって、警察が、国民の望む犯罪をより的確に検挙することは、依然重要なことであることに変わりはありませんが、警察の検挙のみでは犯罪は減少しない、というのも経験の示すところです。

犯罪の防止、社会の安全安心の確保は誰の役割でしょうか。

以前の日本は、いわゆる「お上意識」が強く、犯罪のことは警察にまかせておく、警察も自分たちが治安を維持するので、余計な注文をつけられるのを好まない傾向も見られたところです。

しかし、現在でも25万人余しかいない警察官だけで、1億1千万人余の国民が犯罪にあわないようにすること、社会の安全安心を確保することはできません。そこで、一人ひとり、地域住民、警察をはじめとする公的機関が意識改革をし、それぞれの役割を果たして犯罪を防止する「自助」、「共助」、「公助」による犯罪予防が推進されています。

「自助」とは、自分の身は自分で守ることです。家に鍵をかける、ホームセキュリティーをつける、自転車に鍵をかける、防犯登録をする、自動車に警報装置をつける、ひったくりにあわないようバッグを道路側に持たない、危険な場所に立ち入らない、夜間女性の一人歩きをしない等ちょっとしたことで、犯罪被害にあうことを防止できます。

「共助」は、地域住民で皆で協力しあって、地域の安全を守ることです。防犯ボランティアによる通学路等のパトロール活動、少年ボランティアによる非行防止、補導活動等を活性化し、地域の安全は地域で協力しあって守ることが、重要です。コンビニも、昔は、非行少年のたまり場になっているところもありましたが、今は「地域の安全安心ステーション」として、あるいは「こども110番の家」として機能しています。都市部は、犯罪が多発しているのに、地域のコミュニティーが崩壊しているところも多くあります。地域の犯罪防止ボランティア活動を通じて逆に地域の絆やコミュニティーが復活した団地等も増えてきました。

「公助」とは、警察はもちろん、警察だけでなく、文部科学省や税関、出入国管理等の各省庁、保健所、地方自治体等がそれぞれ犯罪の予防に資する活動を行うことです。警察だけでは、少年非行を減らすことはできません。外国人犯罪、精神障害者による犯罪対策等も同様です。

このようなことから、平成15年、総理をヘッドとし、全閣僚からなる「犯罪対策閣僚会議」が発足し、毎年、随時、犯罪情勢に応じた犯罪抑止対策が策定されています。「公助」として警察が行うべきことは、犯人の検挙はもちろんですが、犯罪の形態、場所、時間帯など犯罪発生の的確な分析とこれに応じた対策をとること、さらにその犯罪発生情報を「自助」、「共助」のために、国民、地域住民に対し、情報発信することです。どこで、どのような犯罪が発生しているかを知らずして、自分の身を守ることも、地域ボランティア活動を的確に行うこともできません。情報を有する警察がより積極的に犯罪情報を発信することが、「自助」、「共助」にとって不可欠です。

従来、「捜査にあたっては秘密を厳守する」との犯罪捜査規範の規定もあり、捜査に関することは、全部秘密のように扱われていたこともありますが、よく読むと秘密にしなければならないのは、「被害者等のプライバシー」と、「犯人を利することになる捜査の手の内」です。性犯罪の場合は当然ですが、窃盗や暴行であっても被害者であることを隠したい場合が多々あります。また、すでに逮捕状をとった等、捜査がここまで来ているといった情報も犯人を利するために、秘密にするのが当たり前です。この地域では、このような手口の犯罪がこのような時間帯に起きている、というような統計的な情報を、よりわかりやすく、タイムリーに地域住民に提供、発信することが警察に求められています。

このような、国民を挙げての「自助」、「共助」、「公助」の努力が、今日の安全安心をもたらした基礎であると考えています。

これからの、ポスト平成時代の犯罪予防をより強化するためには、この3つに加えて、「商助」が重要になると考えております。「商助」は、聞きなれない言葉で、広義には「共助」の中に入れてもいいと思いますが、商売、企業による犯罪防止のサポートのことです。

近年、経営学等で強調されているのは、CSR経営、ESG投資です。ご案内のように、CSR経営は、C（企業）がS（社会的）R（責任）を果たすべきということで、ESG投資は、E（環境）、S（社会貢献）、G（ガバナンス）に優れた企業に投資すべき、とする考え方です。目新しい概念のようですが、実はわが国には、昔から、同じような考え方が根付いているようにも感じられます。

一つは、近江商人の「三方良し」すなわち「売り手良し、買い手良し、世間良し」とする考え方です。近江商人は、中世から江戸時代、今の滋賀県から全国各地へ、てんびん棒を担いで、行商を行いました。質実で刻苦精励することで知られており、高島屋や西武、伊藤忠等が有名ですが、多くの一流企業のルーツになっています。「三方良し」は、売り手と買い手が満足するだけでなく、世間良し、すなわち世の中も満足するのが、良い商売である、という意味で、社会貢献CSRの重要性を早くも認識していたものと考えられます。

現在もいわゆるステークホルダーということで、企業を取り巻く、お客様、株主、従業員、取引先、環境、地域などの関係者の利益を尊重する考え方がありますが、近江商人の考えも似ているところがあったと思います。

二つは、日本資本主義の父と言われる渋沢栄一です。明治期に、電力、ガス、鉄道、銀行等500近い会社を創設し、現在の日本の産業のほとんどを立ち上げ、日本発展の基礎を築いた渋沢栄一は、自ら財閥を率いることなく、日米親善や社会福祉事業に、力を入れました。彼の『論語と算盤（そろばん）』には、「士魂商才」を説き、世の中を渡っていくには、武士の魂と商売の才能がともに必要であるとしています。論語の道徳と利潤の追求は全く矛盾するものではなく、孔子は、利潤の追求は否定しておらず、正当な手段によらない商売等を戒めているとし、自分の利益のために他人はどうでもいい、という考えを退けています。自分で苦労した富も、国家社会の助けがあって初めて得られたものであるということを肝に銘じて、国家社会に恩返しをすべきである、旨述べられています。

また、ESGも、これまで特にアメリカで採られてきた、目先のROE（自己資本利益率）ROA（総資本利益率）等の財務指標にのみ捕らわれて投資や経営をするのでなく、環境にどれだけ配慮しているか、社会、地域にどれだけ貢献しているか、ガバナンスすなわちコンプライアンス等にどれだけ配慮しているかについて見極めて、投資、経営すべきであるという考え方で、CSRを含めた企業の社会的信頼性を重視するものです。

このように、現在の経営学で、CSR、ESGが強調されるのも、経営の重点をより分析的に明確にしたという意義は十分ありますが、わが国では、必ずしも目新しいものではないのではないか、と思料します。

缶コーヒーのCMで、「世界は誰かの仕事でできている」とガードマンの方がつぶやくシーンがありますが、ことさらに、「社会貢献」といわなくとも、商売自体、仕事をすること自体が、自分の生活を支えるとともに、世の中の需要に応じて国民に必要な価値を提供し、国民のために役に立っています。

商品の品質をより向上させて、より国民の役に立つ製品にすること、その上でさらに、現在の経営学、日本の近江商人の哲学、渋沢栄一の教え等に基づいて、利潤を社会のために還元することを積極的に行うことで、その会社、企業の社会的信頼が増加し、さらに仕事に好循環が生まれることにもなるわけであり、社会貢献を考えない仕事、経営は、いずれは行き詰まりかねない、と考えられます。

皆様の防犯機器の製造、システムの設計等は、それ自体が大きくわが国の安全安心に寄与するものであり、より一層安価かつ先進的な製品を提供いただくとともに、本協会を通じてより一層公益的な活動を行われることを期待いたしております。

当然のことですが、会社によって、CSR、ESGの取組みには、かなりの格差が見られます。この格差をなくし、できるだけ多くの企業が犯罪防止という社会貢献活動に参画して「商助」を推進することが、新たな時代の安全安心構築のため、効果的な施策ではないか、と愚考しております。

最後に、弊社積水化学工業の取組みについて、ご参考までに申し上げます。

積水化学工業では、従来からCSR推進部署を設けて、環境問題の解決、環境教育の推進や地域の安全安心に対する貢献を中心にCSR経営を経営の最大の柱として参りました。人事や人材育成はすべてCSR推進のためにあるとする強固な信念の下に、一時期、人事部を廃止し、CSR推進部署の下に置いたこともあります。

また、最後に弊社の組織図の簡略版を掲載しましたが、一番上部に、お客様、株主、地域等のステークホルダーの方を置いて、この方々のために仕事をしていることを常に認識できるようにしております。

現場で現実にお客様等と接する部門こそが重要であり、会社の管理部門、役員等はその活動を支えるためにある、ということで、社長等は、一番下位に位置しており、会社のＣＳＲ、ＥＳＧ経営にかける意欲を示しているものであります。

さらに、特に、弊社の住宅部門であるセキスイハイムにおいては、犯罪や災害時に安全に居住できる住まいを提供すべく、太陽光、蓄電池の設置、防犯性能をアップした防犯優良住宅、セキュリティー・アパート認定の集合住宅製造に取り組むとともに、住宅周辺地域の安全安心に貢献すべく、防犯や交通安全に関する警察活動に関して、各県警と協定書を結ぶなどして、地域安全運動等のイベントへの積極的な参加、振り込め詐欺防止グッズの提供、犯罪被害者支援センターへの寄付等の警察支援活動を展開しております。

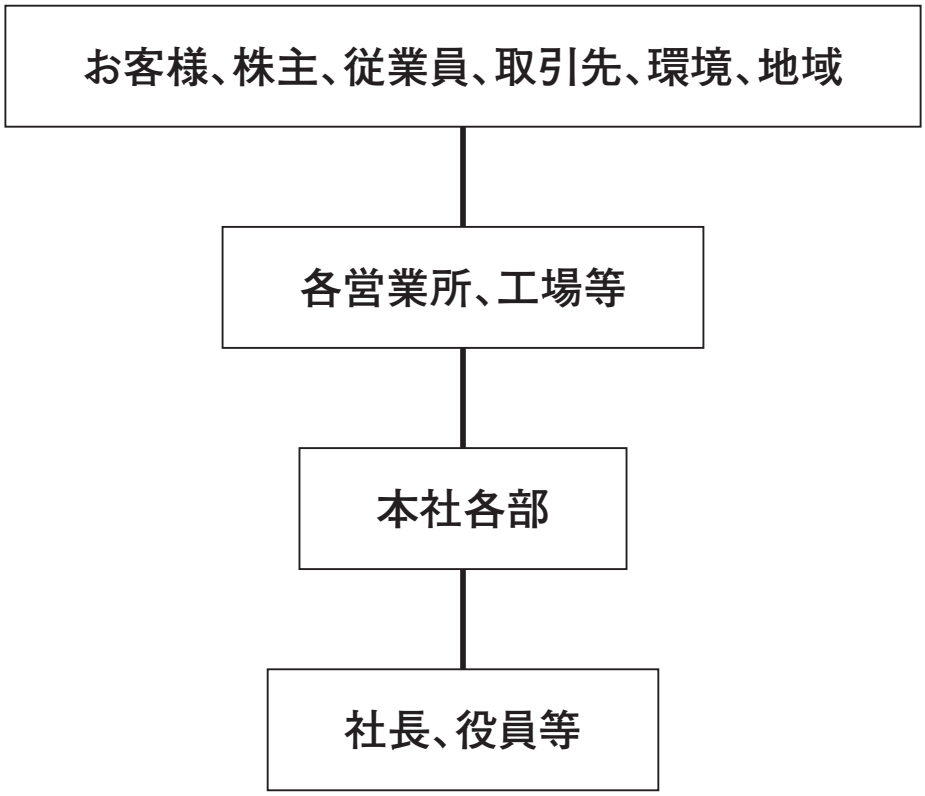
また、東日本大震災のときには、福島、宮城、岩手の三県警に放射線下作業用のゴーグルや長手袋等を提供し、三県の警察本部長から感謝状をいただきました。

警察庁生活安全局においても、犯罪防止面において、企業のＣＳＲ活動を支援するということが、年間活動の重点推進項目に取り上げられております。

弊社としては、今後も、犯罪情勢、時代の動きに応じた、より効果的な施策を質的、量的にさらに充実させて、国民生活の安全安心の強化に微力ながら尽くして参る所存であります。

ご指導、ご鞭撻のほど、よろしくお願いいたします。

積水化学工業組織図 簡略版



法令解説

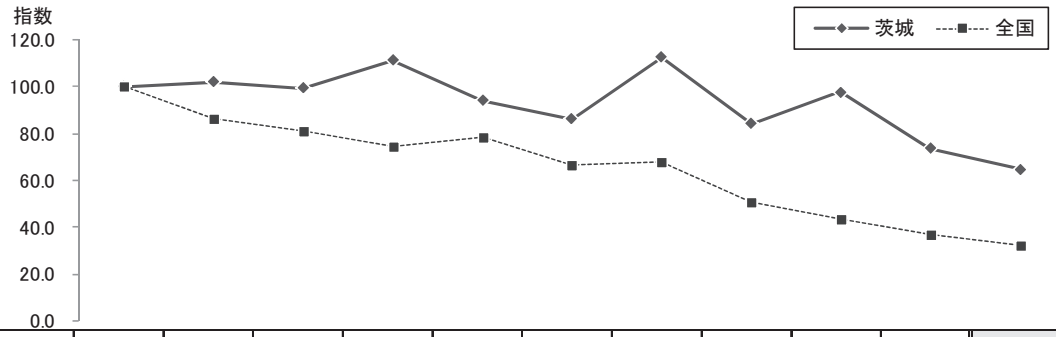
茨城県ヤード条例の制定とヤード対策

茨城県警察本部生活安全部参事官兼生活安全総務課長　岡崎　孝平

1 はじめに～自動車盗の現状

茨城県は、全国的にみて自動車盗の多発県であり、平成28年以降の認知件数は減少に転じているものの、平成29年の認知件数は全国ワーストとなっています。このような情勢を踏まえ、県警では自動車盗の検挙・抑止対策に取り組んでいます。

自動車盗認知件数の推移



	H19	H20	H21	H22	H23	H24	H25	H26	H27	H28	H29	増減（率）
茨　城	2,155	2,194	2,144	2,393	2,025	1,857	2,425	1,814	2,107	1,590	1,397	−193
指　数	100.0	101.8	99.5	111.0	94.0	86.2	112.5	84.2	97.8	73.8	64.8	(−12.1%)
全　国	31,790	27,515	25,815	23,775	24,928	21,070	21,595	16,104	13,821	11,655	10,213	−1,442
指　数	100.0	86.6	81.2	74.8	78.4	66.3	67.9	50.7	43.5	36.7	32.1	(−12.4%)

認知件数上位5府県

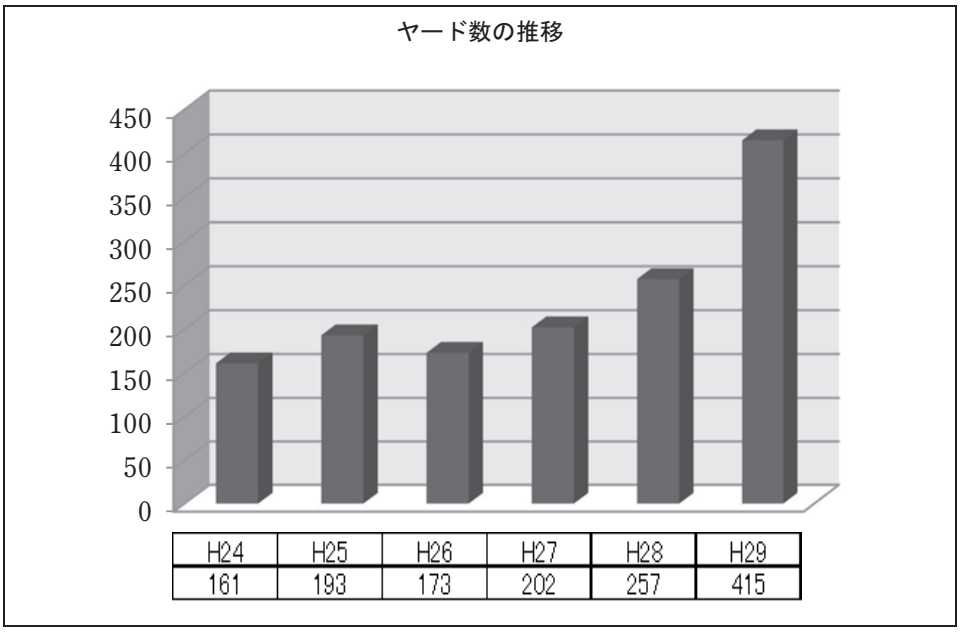
	H25		H26		H27		H28		H29	
1位	千葉	3,295	愛知	2,724	愛知	2,205	茨城	1,590	茨城	1,397
2位	愛知	2,712	大阪	2,184	茨城	2,107	大阪	1,577	大阪	1,393
3位	大阪	2,466	千葉	1,846	大阪	1,747	千葉	1,538	千葉	1,178
4位	茨城	2,425	茨城	1,814	千葉	1,277	愛知	1,349	愛知	1,127
5位	神奈川	1,757	神奈川	945	埼玉	919	埼玉	914	埼玉	758

2 ヤードの現状

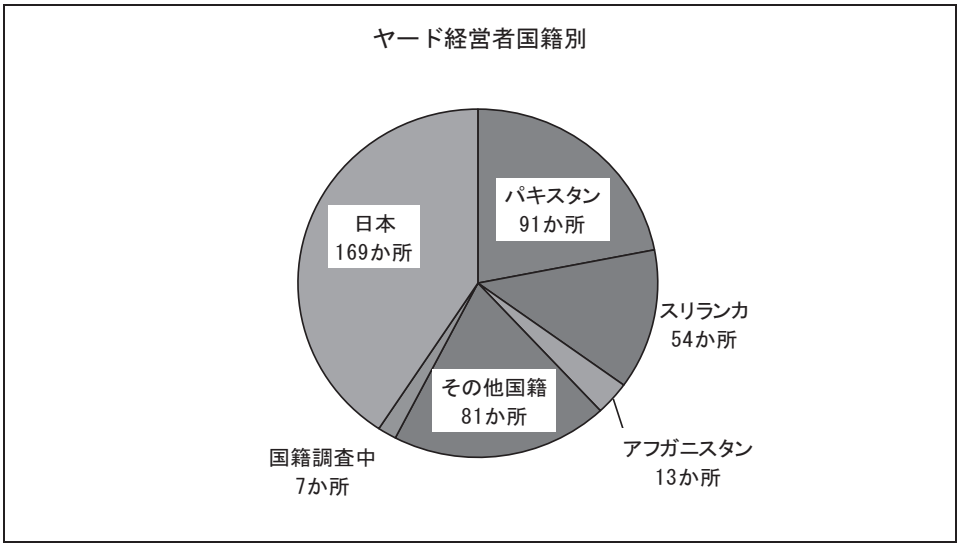
自動車盗と密接な関係にあると認められるのが通称ヤードと呼ばれている施設の存在です。ヤードは周囲が鉄壁等で囲われており内部の状況を視認できないようにしていることから、一部のヤードでは盗難自動車の保管・解体先として利用されているほか、不法滞在外国人の潜伏先にもなるなど各種犯罪の温床となっている実態が見受けられます。

県警では、自動車盗抑止対策の一環として、既存のヤードや新たに設置されるヤードの実態把握を強化しています。

平成29年末で把握しているヤードは415か所に及び、5年前の平成24年に比べ2.5倍の把握数となっています。



ヤードの経営者を国籍別に見ると、外国籍経営者が約6割を占めており、その中でもパキスタン、スリランカといった南アジア圏の経営者が3割強を占めています。



本県にヤードが多数存在していることについては、次のような理由が考えられます。

①土地の価格が安く、広い敷地が手に入ること

②道路網が発達しており、輸出するためのアクセスが良いこと

③オークション会場に近いこと

④成田空港、茨城空港があり、外国人の就労等に便利であること

3 ヤード条例の制定

自動車盗の多発及び一部のヤードで盗難自動車の保管、解体等が行われている実態、さらに、茨城県議会に設置された安全・安心を実感できる地域づくりに関する調査特別委員会から、平成26年11月に「県独自の条例を制定し、ヤードに対する規制を強化すべき」との提言を受け、ヤードを規制する条例を制定することになりました。

条例の制定に当たっては、警察が主体となって自動車盗の防止に関与できる条例の制定を目指して検討を重ねた結果、「茨城県ヤードにおける自動車の適正な取扱いの確保に関する条例」が、平成28年12月の茨城県議会において全会一致で可決、平成29年4月1日施行となりました。

県議会で条例可決後、県域テレビ、ラジオ等を活用した広報活動のほか、県廃棄物対策課との合同による条例説明会の開催、条例の概要を5カ国語に翻訳したパンフレットの作成・配布等により、県民及びヤード関係者に対して条例施行に向けた周知活動を行いました。

4 条例の概要

条例では警察職員によるヤードへの立入検査のほか、ヤード内で自動車を解体する者の各種義務を定めており、違反した場合には罰則もあります。主なものは以下のとおりです。

(1) 届出(第3条)

ヤード内で自動車の解体を行おうとする者に対する県公安委員会への届出義務

(2) 相手方の確認(第4条)

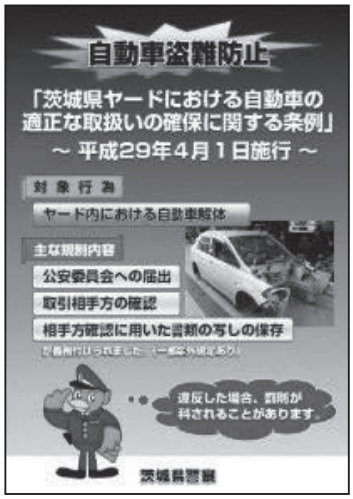
解体しようとする自動車を引き取る際に、運転免許証等により取引相手の身分を確認するとともに自動車検査証等の書類の提示を受けなければならない確認義務

(3) 相手方確認書類の写しの保存(第5条)

相手方を確認するために提示を受けた運転免許証や自動車検査証等の写しの保存義務

(4) 立入検査等(第7条)

警察職員によるヤードへの立入り、書類等の検査、関係者への質問



5 ヤード対策(平成29年中)

(1) 立入り・指導

昨年はヤード条例の施行に伴い、警察本部内にヤードへの立入り、指導及び検挙を専門に取扱うヤード対策係を新設するなど体制を強化し、県内のヤードに対し659回(前年比+267回)の立入りを実施しました。

この立入りにより古物営業法に基づく帳簿記載義務違反や標識掲示義務違反等で93件、ヤード条例に基づく届出義務違反や相手方確認義務違反等で36件の違反を認め、経営者等の責任者に対する行政指導を実施しています。また、県廃棄物対策課や労働基準監督署との合同立入りも多数実施するなど関係機関との連携も図った結果、自動車リサイクル法や労働安全衛生法に基づく行政指導も実施しています。

(2) 検挙

行政指導に従わないヤード経営者については、軽微な違反であっても看過しない強い姿勢で臨み、古物営業法やヤード条例を始めとした各種法令違反を適用して検挙しています。

特に、ヤード条例違反の検挙については、テレビ・新聞等で報じられるなど大きな反響があったことから、県内のヤード経営者に警鐘を与えているものと考えています。

6 おわりに

県警では、「安全・安心を実感できるいばらきの確立」のため、今後も自動車盗の検挙・抑止対策に取り組んでまいります。

第20回　特別セミナー講演

昨年10月6日（金）に開催された特別セミナーの講演について紹介いたします。

講演1については既に、「日防設ジャーナル」2017年爽秋号に掲載いたしましたので、今回は以下の講演2及び講演3について紹介いたします。

◆講演1

「防犯カメラの高機能化と法的規制の新たな動向」　　「日防設ジャーナル」2017年爽秋号（掲載済）

◆講演2

「AI／ビッグデータ／IoT時代のセキュリティ対策」

◆講演3

「IoTのセキュリティとAIの考え方」

※ 著作権の関係で、写真等を割愛しているページがありますが、URL を入れてありますので確認してください。

特別セミナー講演２

「AI ／ビッグデータ／ IoT 時代」のセキュリティ対策

株式会社シマンテック　**山内　正**

1.はじめに

AI（Artificial Intelligence：人工知能）やIoT（Internet of Things：モノのインターネット）に象徴される革新的な情報技術が、身の回りの生活の利便性や産業の生産性を飛躍的に向上させようとしている。多くのセンサーやデバイスがインターネットに繋がるIoT環境で収集された膨大なデータは、いわゆるビッグデータとなり、「教材」として機械が学習することでAIの「知的能力」を高め、問題解決能力が向上する。

防犯設備を取り巻く環境でも、こうした新しい技術の導入により顔認証機能を持つインターネット接続カメラなど機能の高度化が進みつつある。

その一方で、人間の安全性を脅かす「AIの暴走」や今までインターネットに繋がれていなかったモノが常時接続されることによる新たなセキュリティ脅威の影響が懸念されている。すでにセキュリティを強化するために設置されたカメラがサイバー攻撃の片棒を担ぐといった事態も生じている。

本講演では、こうしたAI／ビッグデータ／IoTといった革新的な技術がもたらすセキュリティ上のリスクを明らかにするとともに、こうしたリスクへの対処への考え方や対策例を紹介する。

2.攻めるAIと守るAI

従来のコンピュータでは、問題解決の具体的な手順（アルゴリズム）は、コンピュータが理解できるプログラムとして作成され、それを実行させることで問題解決を行ってきた。一方AIは、多くの情報をもとに問題解決に必要なしくみを継続的に内部で自律的に改良・精緻化して問題解決を行う。「知能」という言葉が使われる背景には、人間が行う認識、判断、問題解決といった高度な情報処理を機械上で実現しようとする動機がある。その適用分野は広がっており、音声や画像を認識したり、将棋や囲碁のプロ棋士と対戦するAIや大学入試問題を解くAIも登場している。

AIが注目を浴びるのは歴史的に今回が初めてではなく、現在のブームは第三世代のAIブームと言われている。1960年代の第一世代のAIブームでは、「探索・推論」技術を用いた数学の定理証明やチェスゲームへの適用が、1980年代の第二世代では、「知識表現」技術を用いたエキスパートシステムが構築された。第三世代の現在は、「深層学習（Deep Learning）」に象徴される「機械学習[1]（Machine Learning）」を用いた本格実用化[2]の時代とも言われている。過去の蹉跌[3]を知る人の中にはブームに懐疑的な人もいるが、第三世代では「深層学習」を中心に適用範囲の広がりが期待されている。

「深層学習」は、人間の脳における神経回路をモデ

ル化したニューラルネットワークを複数層用いて、問題解決に必要な知識が学習される。この多層ニューラルネットワークには、大量のデータから高度な概念を段階的に抽出する機能[4]があり、画像認識や音声認識の分野で人間の認識力を上回る結果を出している。

AI技術がもたらす影響を考える際には、「AIを用いた攻撃の高度化（攻めるAI）」といった影の部分と「AIを用いたセキュリティ対策の高度化（守るAI）」といった光の部分の両面を考える必要がある。

「AIを用いた攻撃」に対する懸念の背景として、「機械」は人と異なり疲れや飽きを知らずに学習を続ける点がある。AIの加速度的な能力向上により、AIが全人類の知的能力を超えてしまう時期「シンギュラリティ（技術的特異点）[5]」が来るという未来予測がある。シンギュラリティ以後は、人類からの制御が不能になったAIにより人類が滅亡するという視点から「人類最悪にして最後の発明[6]」という警告も出ている。ポリモーフィック型[7]ウィルスやイランの核濃縮工場を狙ったスタックスネット[8]は、その振る舞いから「AIを用いた攻撃」のさきがけとも言われている。

少々抽象的であるが、サイバー攻撃が実行されるためには、何らかのIT基盤が必要である。当初は、パソコン（コンピュータウィルス）が主な基盤であったが、昨今はスマートフォン（悪性アプリ）やIoT機器を含むシステムが攻撃IT基盤として用いられている。近い将来、AIがサイバー攻撃基盤として使用された場合、その対応が極めて難しくなる懸念が高まっている。

一方、AI技術をセキュリティ対策に積極的に活用することが進められている。サイバー攻撃対策の中心は、メールや通信先の「白黒」[9]判定。事前にマルウェア（被害をもたらす悪性なもの）の特徴を機械学習[10]させておくことで新たに送付されてきたデータがマルウェアであるか否かを識別できる（図1）。

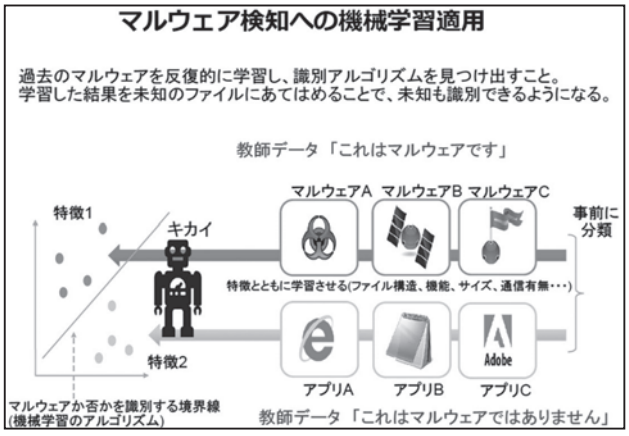


図1　機械学習を応用したマルウェア検知

防御側は、膨大な関連情報の中から「黒」のものを識別する必要がある。攻撃側は、防御側の「黒」判断基準を見越して判断基準に引っかからない攻撃を新たに引き起こす。このいわば「白黒識別」における「イタチごっこ」的な状況がセキュリティ対策の長年の課題となっていた。AI技術はこの白黒の識別を得意としており、機械学習の採用による問題解決力の向上が期待されている。

昨今は、AIを活用した事例が数多く提案されているが採用にあたって考慮すべきは、「AIの知能レベル」である。いうまでもなく識別力レベルの低い知能では、対策はおぼつかない。知能レベルは、用いられている「機械学習の方式（アルゴリズム）」と「学習環境」（教材データの量と質）に左右される。

機械学習の方式は数多くあり、適用に際しては各アルゴリズムの特徴と問題解決に対する有攻性の見極めや複数の方式を組み合わせによる解決力補完が必要である。選択に際しては、深層学習のような新方式を問題特性にかかわらず闇雲に採用せず、適用しようとしているアルゴリズムの対象問題への有効性が事前に確認されていることが重要となる。

学習データが不足していたり、質の悪い誤った学習データを用いた機械学習は正しい識別結果をもたらさない。正常なファイルをマルウェアと判定（誤検知）したり、マルウェアの検知漏れを引き起こす（図2）。

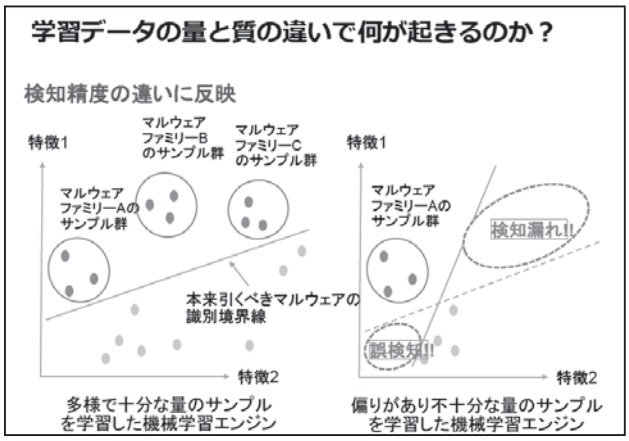


図2　精度向上に必要な学習データ量

有効な結果を出すためには、学習に必要となる十分なデータ量（サイバー空間から広く攻撃情報）と誤った学習をさせない質の良いお手本（詳細な解析結果）となる教師データが必要なのである。

セキュリティ分野では教材の鮮度も重要だ。「白黒」の判定基準は、その時点までの学習データ（攻撃者の攻撃手法）であり、攻撃者が攻撃挙動を変更した新しいマルウェアに対する正しい判定ができない可能性がある。攻撃者は、攻撃を阻止されないために攻撃機能の進化を進めるため、学習を怠ってしまうと、防御力の

低下に繋がってしまう。リアルタイムで学習データを取り込み、弛まず学習を行う仕組みが必要となる。

1 多くの情報をもとに自身で、「問題解決に必要なしくみ（学習結果）を構築し、継続的に改良・精緻化して問題解決を行う。

2 第2次ブームにおいては、人工知能の実現がルールベースに頼っていたため、最終的な問題解決能力に限界があった。

3 第二世代の人工知能においては、画像や音声認識、エキスパートシステムなどが実用化されたが、知能の実現がルールベースに頼っていたため、最終能力に限界があった。

4 入力情報と正解教師データとの関係を最適に表現するモデルを、統計力学モデルに基づきニューラルネットワーク上の素子間の重みを段階的に調整していく。

5 過去の経験が通用しない異次元のレベル。米国の研究者レイ・カーツワイルらが広めた考え。2045年に逆転の時期を迎えると予測されている。

6 AIが人類を滅亡させてしまうことを示唆。ジェイムズ・バラット「人工知能　人類最悪にして最後の発明」（ダイヤモンド社）

7 新しいファイルに感染する毎に自身の構造を変える（多形態）マルウェア。

8 https://www.symantec.com/connect/nl/blogs/stuxnet-plc?page=1

9 マルウェア対策ソフトで配布されるパターンファイルは、黒の判断基準の典型。

10「選別器（Classifiers）」を構築する。例えば、正規のソフトウェアファイルと悪質なソフトウェアファイルを大量に収集し、機械学習により、悪質なソフトウェアファイルを選別する機能を実現する。

3.ビッグデータ環境で重要なセキュリティインテリジェンス

ビッグデータ環境は、単にデータの量が多いだけではない。日々刻々生じるデータ系列をインフォメーション（情報）として、時間軸や同じ属性、特定の種類といった視点で整理し、それらを統計解析などの手法を駆使して分析、再整理することで新たな関係や背景にある意味といった価値ある情報を見つけ出す。この新たな情報は、インテリジェンス(情報)と呼ばれ、問題解決を効果的、効率的に進めるために極めて有効な役割を果たす。

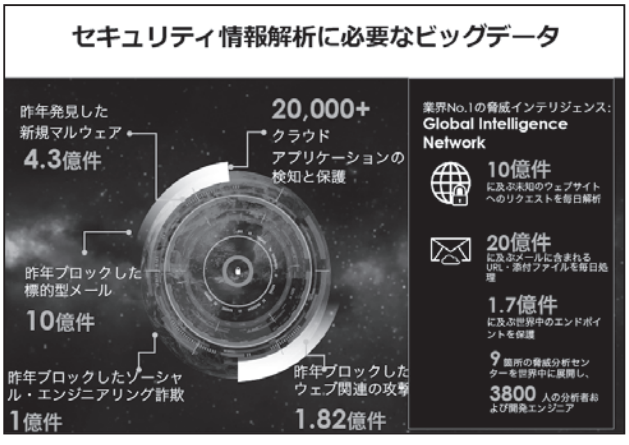


図３　セキュリティ対策に用いられるインテリジェンス

セキュリティ対策でもこのインテリジェンス（情報）は重要な役割を果たす。シマンテックでは、長年の観測を通じて蓄積したマルウェアや悪意のあるWebサイト関連のインテリジェンス（情報）をクラウド基盤上に構築している。このGIN「グローバルインテリジェンスネットワーク」[11]と呼ばれるセキュリティ対策基盤は、日々のセキュリティ対策に活用されている（図3）。

GINの中には、不正な活動が確認されているIPアドレスやURLの評価情報（レピュテーション）、様々なOSやアプリケーションの脆弱性[12]情報、マルウェアの情報やサイバー空間で飛び交うファイルごとの評価情報が集められている。これらのインテリジェンス（情報）を活用することで、迅速な攻撃防御や検知、事後対処の作業負荷軽減が可能となる。

サイバー攻撃の背後には組織や人が存在するが、攻撃を行う主体という切り口でのインテリジェンス（情報）として、「攻撃者元情報MATI[13]」がある（図4）。

図４　セキュリティ対策に必要な攻撃者に関する情報

MATIでは、いつ、どの国・組織に対して何を標的に何の目的でどのような攻撃が行われたのか（TTP[14]）や過去に用いられた攻撃手法に関する情報が利用できる。データフィード（Datafeeds）と呼ばれる他の防御システムに直接取り込めるXML形式[15]での情報共有も可能である。自組織を狙っている攻撃者に焦点をあてたインテリジェンス（情報）により、受け身ではなくプロアクティブな対策が可能となる。

ビッグデータを活用する際に留意すべき点として、「個人情報の取扱い」がある。スマートフォンに限らず多種多様なウエアラブルデバイスが普及し、それを装着している人の身体に関する情報や行動に関するデータがネットを通じて集約されている。防犯カメラで撮影された画像も個人識別可能であれば、個人情報として法的規制の対象になる。一度の個人情報漏洩で与える影響は従来とは比較にならない。

この分野で早急な対応が必要となっているのが、GDPR[16]である（図5）。GDPRは、EU域内の個人データを域外に持ち出すことを厳格に制限する法律であり、EU加盟国全てに一律に適用される。この「規則」は、2018年5月に施行される予定であり、EU域内の個人データを扱うあらゆる企業や組織[17]は、施行開始までに対応を完了させなければならない。

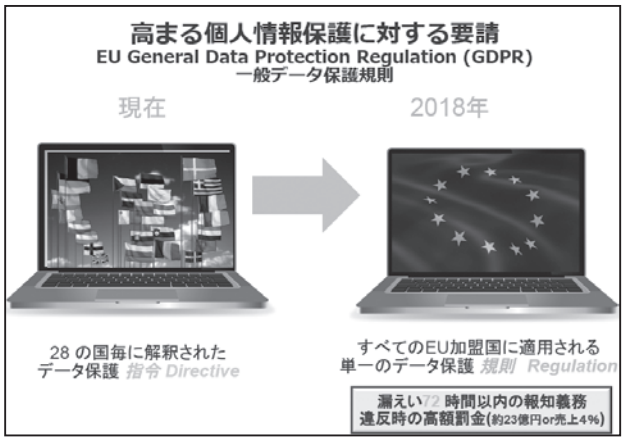


図 5 EU 一般データ保護規則の概要

取り扱う個人データの漏えい等のインシデントが発生した場合、それが判明してから72時間以内に監督当局に届けることが求められている。通常情報漏えい事故の原因調査には数週間から数ヶ月といった時間を要するが、72時間で迅速な初期報告を行うためには、既存のインシデント対応や報告手順の見直しが急務である。違反時の制裁金もかなり高額[18]に設定されている。

11 総レコード数3.7兆件からなる世界最大規模の「ビックデータ基盤」。日々のセキュリティ攻撃の解析から得られた情報に基づき、時々刻々データが更新されている。約24万個のハニーポットをサイバー空間上に設置し、インターネットを流れる全メールの約3割をモニタリングしている。集められたデータは、脆弱性、マルウェア分析情報、スパム発信源のIPアドレスに関する情報が含まれる。

12 コンピュータまたはネットワーク全体のセキュリティに弱点を作り出すソフトウェアの欠陥や仕様上の問題点。

13 Managed Adversary and Threat Intelligence：攻撃者元情報提供サービス https://www.symantec.com/services/cyber-security-services/deepsight-intelligence/adversary

14 Tactics,Techniques and Procedures：攻撃の戦術、技術及び手順。

15 Extensible Markup Language：拡張可能な言語。自組織のログ情報と直接相関をとる等、容易に防御システム高度化が可能。

16 General Data Protection Regulation「EU一般データ保護規則」

17 EU域内に物理的な施設を持つ企業・組織だけでなく、EUの個人データを取り扱う域外の企業や組織も対象。EU域内の個人に向けて商品やサービスを提供する日本企業は、域内に拠点やシステムがなくても、GDPRの適用対象となる。

18 違反を犯した企業のグローバルでの年間総売上金額の4%または2000万ユーロ（約23億円）のいずれか高い金額。

4.IoT環境におけるセキュリティ対策

適用範囲が広まるIoTは、攻撃者にとっては格好の攻撃のターゲットとなり、すでに社会インフラ全体にサイバー攻撃の影響が及ぶ事態が生じている。2016年10月に、DNSプロバイダのDyn社[19]がIoTのボットネットを悪用したDDoS攻撃[20]を受け、Twitter、PayPalといった大手Webサイトが軒並みサービス停止[21]に追い込まれた。ドイツでは、通信業者が攻撃を受け、90万人以上のインターネットユーザが利用できなくなる[22]という国家レベルの被害に至った。

この攻撃では、ネットワークカメラなど約50万台の機器が、Mirai（Linux.Gafgyt.B）と呼ばれるマルウェアに感染し、ボットネット[23]と呼ばれる攻撃基盤が構築された。ボットネットから特定の送付先に大量の通信が行われたことで、送付先のサービスが機能不全となった。防犯カメラなどインターネットに接続されている脆弱なIoT機器を検索するサービスも公開されており、接続した瞬間にサイバー攻撃の脅威に直面する。

セキュリティ対策担当者は、自組織がIoTによるサイバー攻撃を受けた場合の対策だけでなく、「保有・管理対象のIoTデバイスが踏み台となって悪用され、自組織が攻撃に加担してしまわないための対策」も必要となっている。

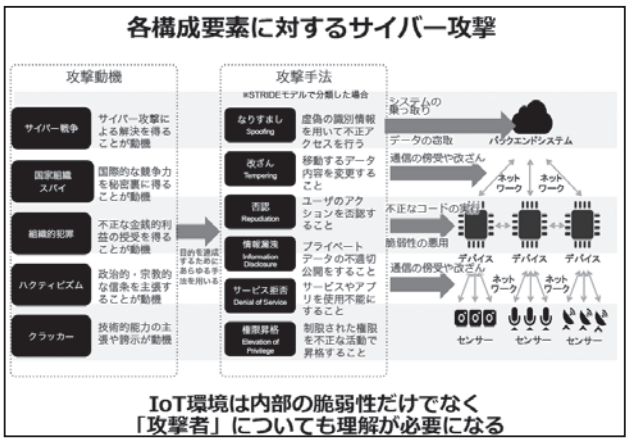


図 6　IoT 構成要素に対する攻撃手法と攻撃動機

数多くのセンサー[24]やデバイス[25]がバックエンドシステム[26]とネットワークで接続されたIoTシステムに対する攻撃には、ネットワーク上の「通信の傍受や改ざん」、デバイス上での「不正なコードの実行」、バックエンドシステム上の「システム乗っ取り」や「データ窃取」がある（図6）。

こうしたサイバー攻撃を仕掛ける主体は、「技術的能力の主張や誇示」が主な動機のクラッカーや「政治的・宗教的な信条を主張」が動機のハクティビズムだ

けではない。金銭目的の犯罪集団や機密情報を狙う産業スパイ組織などの攻撃集団がある。最近では、サイバー空間を第五の戦場[27]と捉え、サイバー戦争を行う部隊を保有する国も増えている。彼らにとっては少ない労力で大きなダメージを与えられるという点でIoT環境への攻撃は魅力的なものとなっている。

特に交通、エネルギー、医療、金融といった重要社会インフラの中核をなすサーバにサービス拒否攻撃が行われた場合の影響力は計り知れない。IT環境におけるサービス拒否攻撃は、大量のメールでパソコンが使えなくなるなど影響は対象機器周辺に留まる。一方、制御システムの中核サーバがサービス拒否攻撃を受けた場合は、制御対象の暴走による二次被害が引き起こされる。現実にサイバー攻撃によるダムの放水異常や発電システムのダウンが発生している。

IoT における問題対処の困難さ

IT		IoT
“Open” 容易なインストール	オープン性	“Closed” デバイス出荷後のソフトウェア更新は困難
“3” (大半は UDP, TCP, IP)	プロトコル	Thousands of Protocols (個々の業種ごとに数百)
“5” (大半は Windows, Linux, OSX, iOS, Android)	オペレーティングシステム (OS)	Dozens (多様な種類)
20k seat enterprise (Typical Enterprise)	スケール	100M “things” (Typical Car Maker)
同じハード、OS,サプライチェーン	分散・断片度合い	個々の業界ごとに異なったハード、OS,サプライチェーン
“2” X86 to x64 by Intel and AMD	チップアーキテクチャ	多数 8 bit AVR, 32/64 bit ARM, x86/x64 and 16 bit MCU; dozens of vendors

図 7　IoT 環境の特徴

IoTのセキュリティ対策を考えていく上で、ITとIoTにおける特性の差異を考慮する必要がある（図7）。IoT環境は、IT環境と比べてオープン性に欠け、ソフトウェアのインストールや削除は簡単に行えない。一度出荷されたデバイスに組み込まれたソフトウェアに問題があったからといって、インターネット経由で簡単にソフトウェアや修正パッチを更新できる場合は限られている。セキュリティ機能を後付けできないケースが多いため、当初より「組み込んでおく」ことが求められる。

またIoTデバイスで採用されているOSや通信プロトコルの種類は、ITと比べて桁違いに多い。従来のITに対するセキュリティ対策の多くは、特定のOSや通信プロトコルを前提としているが、IoTの場合は異なったアプローチが必要となる。

加えてシステムを構成している要素の数が異なる（スケール）などITとIoTでは様々な点で違いがあり、ITシステムに適用されるセキュリティ対策をそのまま適用できない場合も多い。

IoTシステム全体のセキュリティ対策[28]を行うためには、自動車やプラント・制御システムといったIoTシステム固有のアーキテクチャ[29]を踏まえたセキュリティ対策が重要である（図8）。

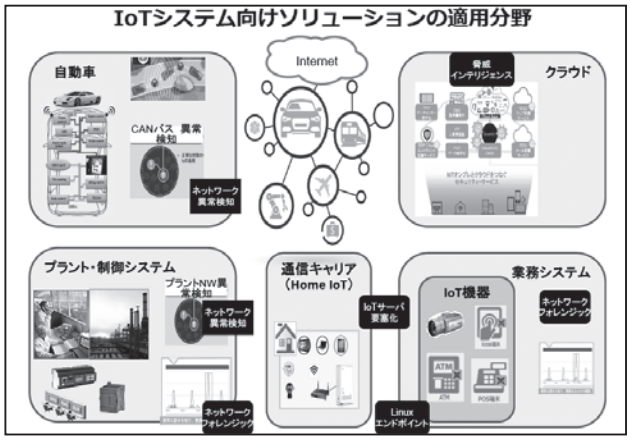


図 8　IoT セキュリティソリューションの適用分野

ネットワーク上の「通信の傍受や改ざん」に対する対策を実施するためには、「通信の暗号化」や「電子署名」が有用である。暗号化通信が確立されれば、盗聴されることなく端末間で通信できる。電子署名は、通信相手先（デバイス）の真正性確認に有用である。不正な送信元からの通信を受信することで、悪意ある指示内容を実行するなどのリスクがあるからだ。IoTデバイスに組み込まれた電子証明書を用いることにより、アクセス権限を持たない攻撃者の不正利用を防ぐだけでなく、不正チップの置き換えやプログラムのダウンロードなどによる改ざん有無の検知が可能となる。

図7に示したように、ITでは限られた通信プロトコル（UDP、TCP、IP）で情報をやり取りしているが、IoTでは多様なプロトコルが用いられている。機械学習を活用した「ネットワーク異常検知」は、サイバー攻撃により想定されていない異常通信がもたらす新たな脅威に対する適応力が高く、プラント・制御システムだけでなく、自動車のCANバス[30]における攻撃検知にも適用可能である。

IoTの重要構成要素であるデバイスはCPUを持ち、何らかのプログラムが動作する。従来のIT環境で使

われていたCPUやOSがそのまま使われる場合もあるが、多くは個々の目的別に異なったCPUやOSが搭載される場合がある。脆弱性の悪用やプログラムの書き換えでデバイスに意図しない不正なコードを実行させ、デバイスの誤作動や蓄積データの搾取などが起こる脅威がある。不正コードの実行を防ぐため、公開鍵と秘密鍵、一方向性コードハッシュを利用してプログラムの改ざん有無を確認する仕組である「コードサイニング」や、OS、パターンファイル更新ができないという運用上の制約を克服するため、ホワイトリストにより特定の挙動だけを許可するサーバ要塞化[31]が有効とされている。

IoT環境におけるバックエンドシステム上では、「システム乗っ取り」や「データ窃取」の脅威がある。バックエンドは、IoTデバイスやセンサーを管理・操作可能な支配的立場にある。そのため、一度バックエンドサービスが攻撃者に乗っ取られると、その配下に存在するあらゆるIoTデバイスが悪意ある第三者に乗っ取られるリスクがある。従来のIT環境におけるクラウドセキュリティよりもさらに厳密なセキュリティ管理が必要になる。また、「データ窃取」に対しては、情報漏えい防止（DLP）が有効である。

IoTシステムに対する抜け漏れがなく投資効果の高いセキュリティ対策を考えるためには、IoT環境のリスク分析が極めて重要である。構成するシステムやIoT環境特有の状況を十分考慮したリスク分析[32]を行うことが最も重要である（図9）。

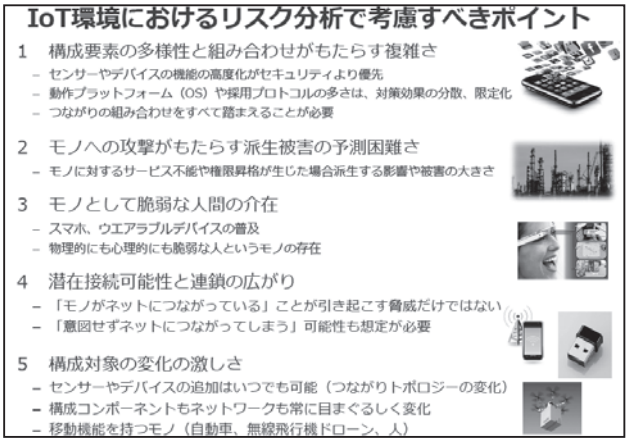


図９　IoT 環境におけるリスク分析の考慮点

実際にIoTシステムの構築段階でセキュリティ対策を具体的に進めていくためには、関連するガイドラインの活用が有用である。日本防犯設備協会が作成した「防犯カメラシステムネットワーク構築ガイドⅡ」は、インターネット接続カメラに対する脅威として、画像盗み見、画像の改ざん、画像の閲覧不能、Dos攻撃加担の4つを想定し、取るべき対策が具体的に示されている。防犯カメラ以外の対策に対しては、独立行政法人情報処理推進機構（IPA）が作成した「IoT開発におけるセキュリティ設計の手引」[33]の記載内容が参考になる。

19 ダイナミック・ネットワーク・サービシズ社。DNS（Domain Name System）は、ドメイン名をIPアドレスに変換するサービス。

20 DDoS（Distributed Denial of Service）分散サービス拒否攻撃
https://www.symantec.com/connect/ru/blogs/ddos-1

21 Mirai：先週の大規模なDDoS攻撃に使われたボットネットについての心得
https://www.symantec.com/connect/nl/blogs/mirai-ddos-0

22 Mirai：IoTボットネットによる攻撃の新しい波、ドイツのユーザーを直撃
https://www.symantec.com/connect/ja/blogs/mirai-iot

23 悪質なコードを含み外部からの指示で連携して動作する複数コンピュータからなるネットワーク。

24 明るさや温度、速度、動きといった様々な物理量を計測して、その結果をデバイスへ送るもの。

25 CPUを持ったコンピュータであり、何らかのプログラムが動作する。多くは個々の目的別に異なったCPUやOS、ソフトウェアが搭載される。

26 センサーやデバイスから生成された多くのデータを主にクラウド上に保存し、データ分析やその結果を用いた様々な処理を行う。

27 サイバースペースは、陸、海、空、宇宙空間に続く5番目の戦場。

28 IoTデバイスおよびシステムの保護：https://www.symantec.com/ja/jp/iot/

29 IoTの参照アーキテクチャ：
https://www.symantec.com/content/ja/jp/enterprise/white_papers/iot-brochure-final-sr-101515-jp-w.pdf

30 Control Area Networkと呼ばれる車載LAN。

31 デバイス上のアプリケーションが実行できる内容を、システムコールレベルで制御し、不必要な権限設定やネットワーク設定、メモリーへの書き込みなどを最初から許容しない。

32 すべてわかるIoT大全2016　日経コンピュータ

33 https://www.ipa.go.jp/files/000052459.pdf

5.おわりに

今後もAI／ビッグデータ／IoTといった革新技術は、お互いの成果を取り入れてさらなる高度化を図り、防犯設備関連のサービスや製品の高度化にも貢献すると見られる。守る技術の高度化は、攻める技術の高度化も伴い、いままで想定していなかった脅威を生じさせる。セキュリティ対策の歴史は、「想定する脅威やリスクに基づく対策」と「その裏をかく想定外の攻撃・事故発生に基づく対策の見直し」の繰り返しであった。この「AI／ビッグデータ／IoT」時代で起こりうる従来とは異なった脅威を受け止めた上で、これら技術の長所を積極的に活かしていく知恵と工夫が求められている。

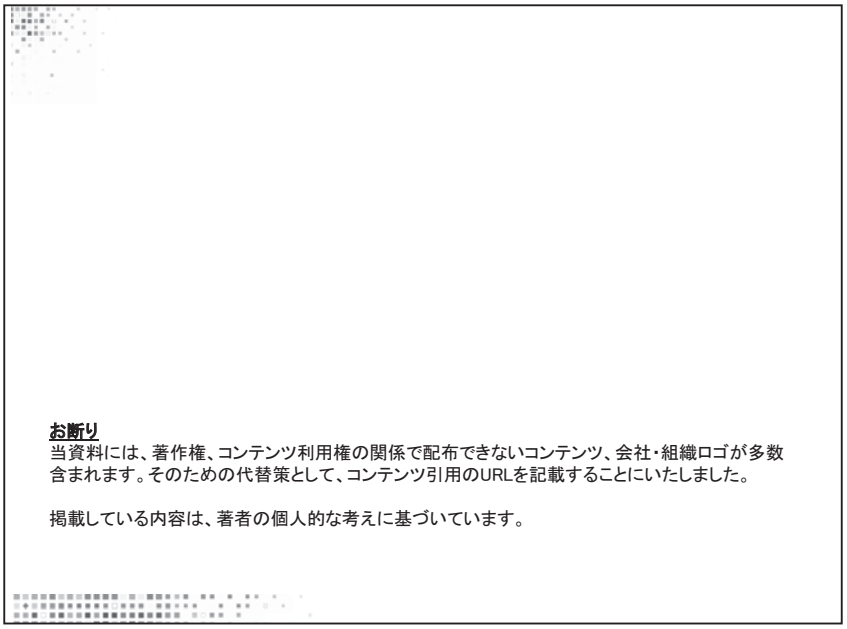
特別セミナー講演３

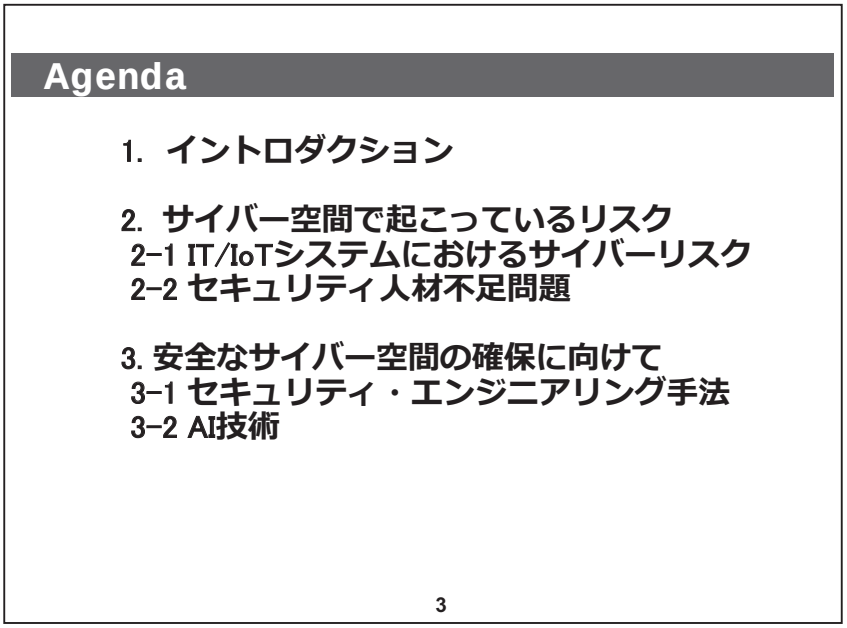
IoT のセキュリティと AI の考え方

セキュリティ・アーキテクト　**大西　克美**

IoTシステム対するサイバー攻撃の事例が増加し、火急な対応が必要な時代になっています。

このセッションでは、実際のお客様事例を元に、安全なIoTシステムの設計方法、AI技術の適用方法をご紹介します。





Agenda

1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

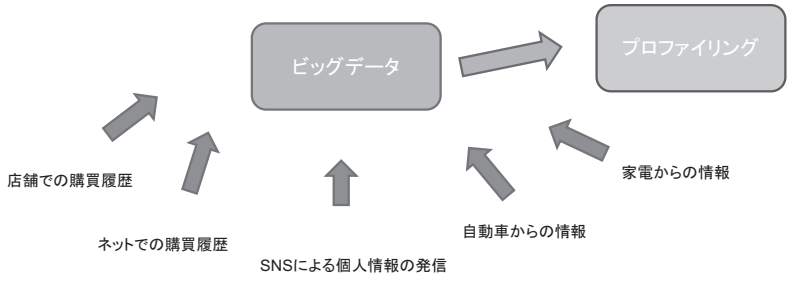
3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

4

なぜ、つなげたい/つながりたい??

企業目線：マーケティング分析、顧客囲い込み
消費者目線：特典、新しいユーザー体験

AI技術により
洞察/ 助言/ 提言/ 指示/ ・・・



5

AI技術とビッグデータがもたらす新しい価値

重要インフラ

重要サービスを支える機器群

つながる機器、システムは安全なのか？（セキュリティの観点）

私たちの個人情報は安全に管理されているのか？（プライバシーの観点）

6

Agenda

1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

7

Agenda

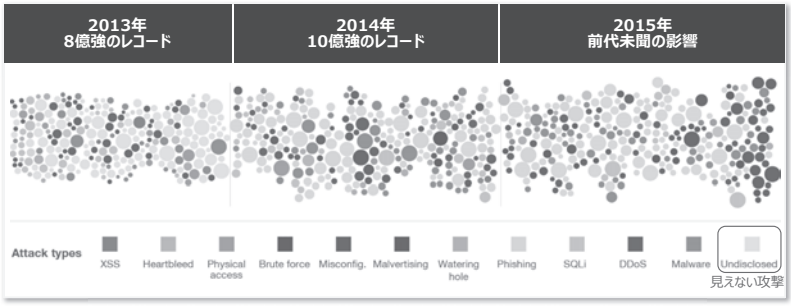
1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

8

2-1. IT/IoTシステムにおけるサイバーリスク



資料出典： IBM X-Force レポート

なぜ、「見えない攻撃」が多いのか？
 →監視するログが少なすぎる
 →攻撃を判断する要員の経験値が不十分である

現時点では、IOTデバイスはモニタリングされる準備ができていない

9

IoT機器がサイバー攻撃の対象に

セキュリティ対策が十分でないIoT機器に対して、カンファレンス、論文などでハッキング事例が数多く紹介されています

防犯カメラ/ 監視カメラ
自動車
医療機器

資料出典：
http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/
https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf
http://www.popsci.com/technology/article/2012-10/hacker-attackers-could-reverse-pacemakers-distance-delivering-deadly-shocks

10

IoT・制御システムもサイバー攻撃の対象に

重要インフラもターゲットになることで、サイバーリスクはITを超えた社会問題になりつつある
IoTシステムに対する攻撃、IoTを利用した攻撃も増加中

- 2013年　NYダム制御システムに対するイランのサイバー・ハッキング
- 2015年　ウクライナ西部でサイバー攻撃による大規模停電(6時間、70万人に影響)
- 2015年　走行中のクルマ乗っ取りに成功（140万台のリコール）
- 2016年　監視カメラを経由した覗き見サイト公開（http://www.insecam.org/）
- 2016年　Miraiマルウェア：IoTデバイスを踏み台にした世界最大規模（数千万アドレス）のDDoS攻撃
- 2016年　経済産業省「今後のサイバーセキュリティ政策」を発表
  - 「国民の生命や社会システム全体に甚大な被害が発生する可能性があり、国家として対応を強化すべき課題」と認識
- 2017年　日本の大手製造業でランサムウェアに感染、甚大な被害をもたらす

パンドラの箱を空けたら、SF映画の世界に迷い込んでしまった！

11

参考）IoTシステムに対する攻撃手法

- Plain old software bugs (buffer overflows, SQLi, XSS, …)
- No transmission encryption (e.g., plain HTTP)
- Weak encryption (home brewed?)
- Key storage on device (symmetric encryption)
- Simple username/password
- Backdoor accounts
- Too many exposed services / lack of hardening
- No firmware integrity checks

=> ITでは有名な攻撃／脆弱性の利用であり、特段の違いがあるわけではない

安全な製品を作る手法を確立する

ITで培った知見・技術をIoTに適用する

12

Miari IoTボットネット

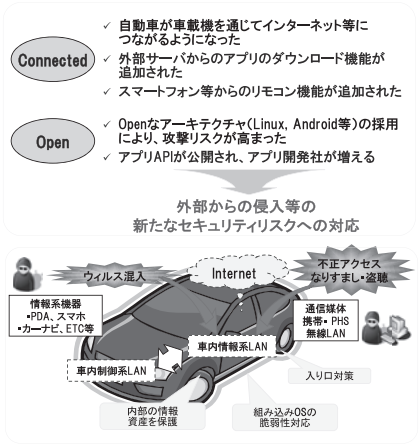
セキュリティ対策が十分でないIoT機器を利用したサイバー攻撃が話題になりました

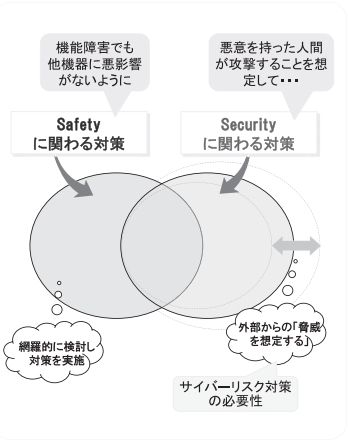
資料引用：IBM Security Intelligence
https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins /

13

何故IoTデバイスが狙われる？（自動車の例）

・自動車が何かとつながることで、外部からの脅威が発生します
・その脅威は、Safety対策でカバーできない想定外の攻撃を仕掛けてきます





14

自動車に対するサイバー攻撃発生！

ホワイトハッカーが走行中の自動車に対するハッキングデモを実施。
日本でも大きな話題となり、経産省などのガイドなどでも引用される有名なハッキング事例となっています

米国におけるハッキング事例

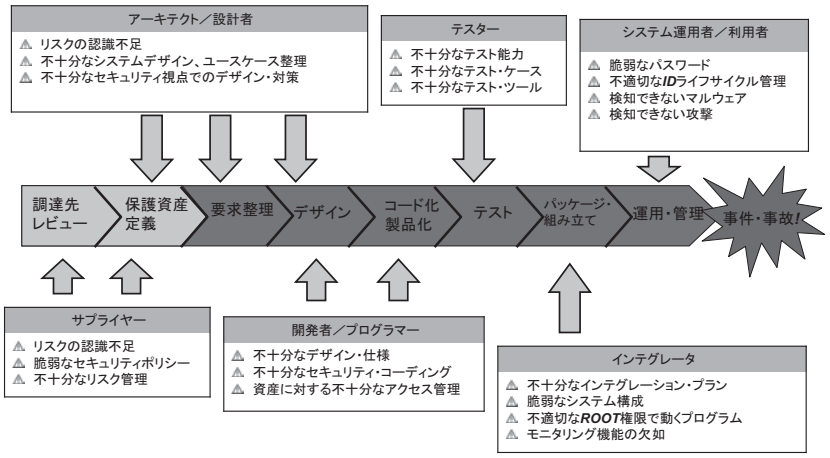
考察：ロボット、制御機器、IoTデバイスなどを遠隔操作して、人類を攻撃できないか？
→ 遠隔操作で走行に影響を与えるハッキングには成功済み
→ 製造業に根付いている"Fail Safe"という概念の限界

資料引用
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

15

セキュリティ事件・事故が発生する理由

各専門分野におけるセキュリティ視点の欠落



16

2-2. セキュリティ人材不足問題

セキュリティ対策が進まない理由の一つに、セキュリティの人材不足の問題があります。
2020年では、約20万人のセキュリティ技術者が不足していると報告されています

人材不足の統計資料

資料出典：**経産省「IT人材の需給に関する推計」**
http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

17

Agenda

1. イントロダクション

2. サイバー空間で起こっているリスク
 2-1 IT/IoTシステムにおけるサイバーリスク
 2-2 セキュリティ人材不足問題

3. 安全なサイバー空間の確保に向けて
 3-1 セキュリティ・エンジニアリング手法
 3-2 AI技術

18

セキュリティの設計、実装は難しいでしょう？

→ 匠の技・経験にだけ頼るのは危険です

セキュリティだけでも大変なのに、プライバシー対策なんて・・・

製造社と利用者の責任範囲は？

周囲にセキュリティを知っている人がいないのですが・・・

→ セキュリティもシステム・エンジニアリングしましょう

19

3-1 セキュリティ・エンジニアリング手法

計画、設計段階からセキュリティ対策、プライバシー対策の実施が必要です。
それを実践するためには、過去の経験だけではなく、「エンジニアリング」を実施することです。

セキュリティ対策の範囲、高度はリスクの大きさ、ビジネス用途で決定されます。
例えば、家庭でペットを眺めるためのWebカメラと空港などのテロ対策向けの防犯カメラでは、サイバー攻撃に対するセキュリティレベルが違うことになります。

プライバシーに関しても、冒頭に紹介したように、個人情報を積極的に発信する世代が台頭しています。よって、昔ながらの一律的な規制ではなく、用途や時代のニーズにマッチした設計が必要になっています。

「Secure by Design」／「Privacy by Design」を実践するにはエンジニアリングが必要
- →想定される脅威を網羅的に整理する手法
- →整理したリスクを評価し、対策の必要性を検討する手法
- →体系化したセキュリティテストの手順、方法
- →PDCAサイクルを適用した脆弱性管理

20

各局面で実施すべきセキュリティ対策

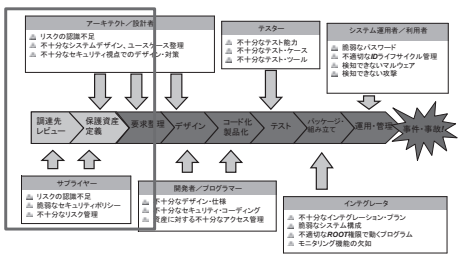
1.計画局面

・守るべき資産の定義・確認
- 製品の商品性、安全性
- 各社のブランド
- 製品に含まれる個人情報　など

・利用用途に応じたリスクの定義
- サービス停止
- 情報漏えい　など

・製品に整備すべきセキュリティ技術の洗い出し
- 侵入検知システム
- フィリタリング技術
- データ暗号化・匿名化　など

・サプライヤーへの調達要求
- サイバー観点からの脆弱性に対する保証範囲
- 責任範囲の明確化（ソフトウェア脆弱性＝欠陥とは言えないケース）



21

各局面で実施すべきセキュリティ対策

2.設計・開発・製造局面

・セキュリティ設計

　セキュリティ要件の整理と設計

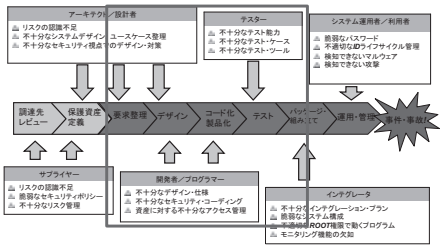
　プライバシー要件の整理と設計

・セキュリティ・テスト

　コード検証

　仕様確認テスト

　攻撃者目線でのハッキングテスト



　エンドツーエンドでのセキュリティテスト（特に、ITシステムとの連携時）　など

　　例）監視カメラで録画された自宅映像をスマホのアプリケーションを利用して閲覧する

　　　監視カメラの録画データが改ざんされる？

　　　アプリケーションを提供するサーバーが攻撃を受けてサービスが停止する？

　　　スマホがハッキングされて、第三者に自宅映像を盗聴される？　など

各局面で実施すべきセキュリティ対策

3.利用・運用局面

・セキュリティ知識を有しない利用者対応

　初期値：利便性＜セキュリティ

　遠隔保守の可否

・脆弱性対応

　脆弱性情報の入手

　リスクの評価

　社外に対する公表

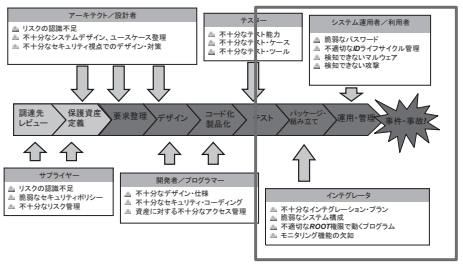
　修正ソフトウェアの配布・適用

　品質不具合対応（リコール？）

・保証範囲

　ソフトウェアに対する保証期間

　有料vs無償の分岐点



3-2 AI（Artificial Intelligence）技術

サイバー攻撃に対するAI技術の適用事例を、IBMの事例をもとに紹介します

アナリストを支援：

外部データの迅速な使用

パワフルな洞察の入手

新しい傾向とパターンの発見

脅威の正確な分析

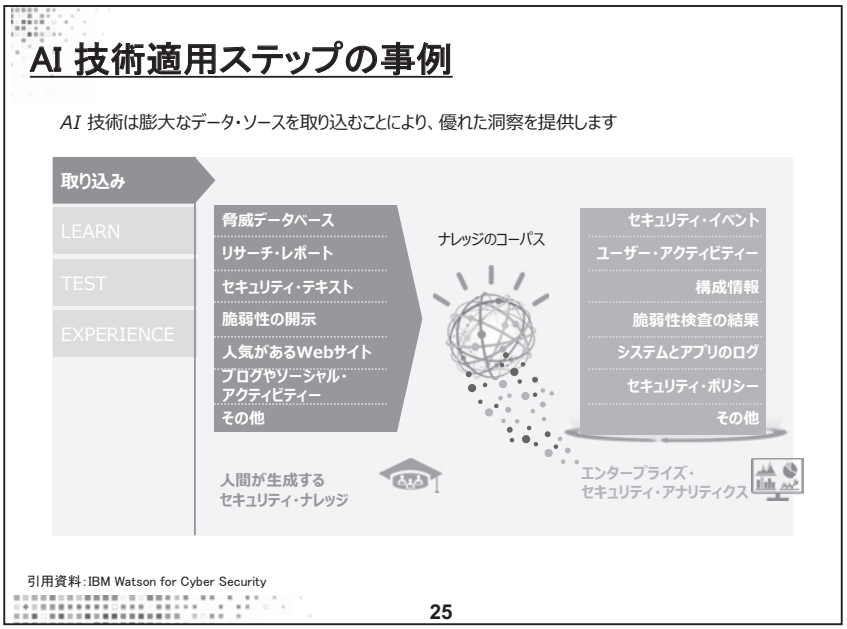
時間と資源の節約

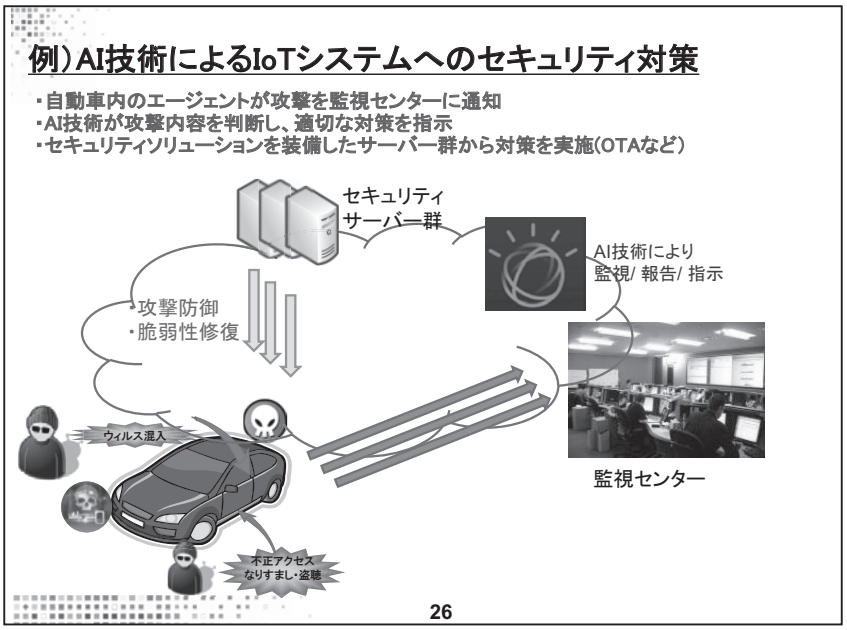
セキュリティ・アナリストの経験不足を補填

セキュリティ技術者の学習時間を節約

　→「見えない攻撃」の解決の糸口

引用資料：IBM Watson for Cyber Security





■当資料のコンテンツ引用URL

資料10（出典）

・http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/
・https://media.blackhat.com/us-13/US-13-Heffner-Exploiting-Network-Surveillance-Cameras-Like-A-Hollywood-Hacker-Slides.pdf
・http://www.popsci.com/technology/article/2012-10/hacker-attackers-could-reverse-pacemakers-distance-delivering-deadly-shocks

資料11

・http://www.insecam.org/

資料13（引用：「IBM Security Intelligence」）

・https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/

資料15（引用）

・http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

資料17（出典：経産省「IT人材の需要に関する推計」）

・http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

技術解説

「ピョンチャン五輪のICT戦略とセキュリティ」

一般財団法人マルチメディア振興センター
情報通信研究部　主席研究員
三澤　かおり

1.はじめに

2月9日から3月18日にかけて開催されたピョンチャン（平昌）冬季オリンピック・パラリンピック大会（以下、ピョンチャン五輪）では、連日の日本選手の活躍で、大会閉幕後もまだ興奮さめやらぬ日々が続いている。各競技の醍醐味はさておき、2020年東京五輪を目前に控える日本では特に、ピョンチャン五輪の運営面への注目度も大変高かった。韓国はICT（情報通信）分野に強みを持つため、ピョンチャン五輪をICT五輪と位置づけ、大会期間中に最先端のICTサービスを世界に向けてアピールした。セキュリティ面においてもICT活用の新たな取り組みが見られた。そこで、ピョンチャン五輪ではどのようなICTサービスが活用されたのか、そして、セキュリティ面ではどのようにICTを活用したのかを振り返りたい。

2.短期間でICT先進国化した韓国

まず、今回の五輪開催地の韓国がなぜ短期間でICT先進国となったのか、その背景から触れておきたい。1960年代半ばの朝鮮戦争もあり、韓国は経済成長面で長らく日本と差があった。軍事政権時代が終わり、文民政権が誕生した1990年代後半以降、政権主導で世界で最も早く国家インフラとして全国にブロードバンド網を構築し、これを活用した電子政府サービスもトップダウンで整備した。21世紀初めに整備された韓国の電子政府サービスは日本のサービスよりも格段に便利である。韓国大統領の権限は強力であり、トップダウンで決まった政策は日本では考えられないほど展開が速い。21世紀初頭の金大中・盧武鉉の2代の政権にわたり、ICT分野促進に力を注いだことが、韓国のICT分野成長に奏功した。

韓国では現在に至るまで世界初のタイトルをねらっていち早くICT新サービスを取り入れ、独自技術の開発にも大変積極的である。人口約5,000万人と市場規模が小さな韓国では企業の成長には限界があるため、企業は初めから海外展開を視野に入れる。代表例として、サムスン電子は世界の携帯端末市場シェアで出荷台数第一位となっている。

また、せっかちともいえるほどのスピード感と新規性、高品質を顕著に求める国民性も相俟って、いったん新サービスが導入されると普及速度は世界最速である。最近の例を挙げると、スマートフォンや4G（LTE）方式携帯電話サービス、モバイルチャットのカカオトークなどの普及も日本より格段に速かった。現在、韓国のICTサービスは総じて日本よりも1年先を進んでいると言えよう。

3.ピョンチャン五輪でアピールするICTサービス

今回の五輪に向けて韓国が戦略的に開発を進めてきたICTサービスは、5G、IoT、UHD（4K/8K）放送、AI、VRの5分野である。今回提供された主なサービスは次ページの表のとおり。

五輪のICT分野の計画と進捗管理は、科学技術とICT分野行政担当省の科学技術情報通信部（部は日本の省に相当）が2014年7月に立ち上げたICT専門タスクフォースを中心に進められた。タスクフォースは関連の政府機関、クリエイティブプランナー、ピョンチャン五輪組織委員会、開催地自治体の江原道（カンウォン道：道は都道府県に相当）、関連企業、スポーツマーケティング及びICT分野有識者で構成される。今回の五輪ICTサービス戦略はタスクフォースが2015年5月にまとめた計画が土台となっている。当初計画では5G、IoT、UHD放送の3分野が対象とされていたが、2016年5月にまとめられた修正版計画で、AIとVRの2分野が追加された。

分野	サービス	内容
5G	選手視点映像 （SyncView）	ボブスレーの先端に設置した超小型カメラからの映像で選手視点での臨場感を リアルタイムで体験。
	自由視点映像 （オムニビュー）	視点を切り替えながら観戦。 クロスカントリー中継時に地図上で見たい視点を選択。
	タイムスライス	競技場に設置した100 台のカメラで撮影した映像をつなぎ、見たい角度で フィギュアスケートのジャンプやショートトラックをリアルタイム視聴。
IoT	IoTストリート	カンヌン駅前通り地区で様々なIoTサービスを体験。
	AR道案内	空港到着時から五輪会場までAR活用で道案内をするモバイルアプリ。
	選手トレーニング	脈波や脳波センサーでのストレス測定結果をビッグデータ化して選手の健康管理に活 用。アイスホッケー選手の動きを分析する精密測位システム等。
UHD （4K/8K） 放送	地上4K放送	2017年5月開始の世界初の地上4K本放送による五輪中継。
	Ultra Wide Vision （UWV）放送	連続した曲面スクリーン（15m×4m）を駅・空港・五輪広報館等に設置。
	8K試験放送	衛星による8K試験放送実施。
AI	自動翻訳・通訳	自動翻訳アプリの提供。
	AIコールセンター	競技・観光情報等五輪関連の電話による問い合わせ対応。
	ロボット VS 人間 カーリング大会	五輪とパラリンピックの間にAI カーリングロボットと高校チームが対決。 人間チームが勝利。
VR	VR中継、 五輪競技VR体験	放送局が五輪競技映像等を高画質VRカメラで撮影して中継、 VRローラーコースター等のテーマパーク型アトラクション。

ピョンチャン五輪で提供された ICT 戦略サービス

大会開催期間中、これらの最先端サービスをまとめて体験できるICT体験館が、会場地域や空港に開設された。大会会場まで行けない人のために、ソウル市内でも冬季五輪を実感できるように5G体験施設やVRのアトラクションが設置された。

また、AI活用の取り組みとして、今回の五輪向けに開発された自動翻訳・通訳モバイルアプリは、警察官による外国人観光客の案内でも活用された。警察官の利用を想定して、各種シーンに応じた警察との会話例文があらかじめ多く盛り込まれていることが特徴でもある。

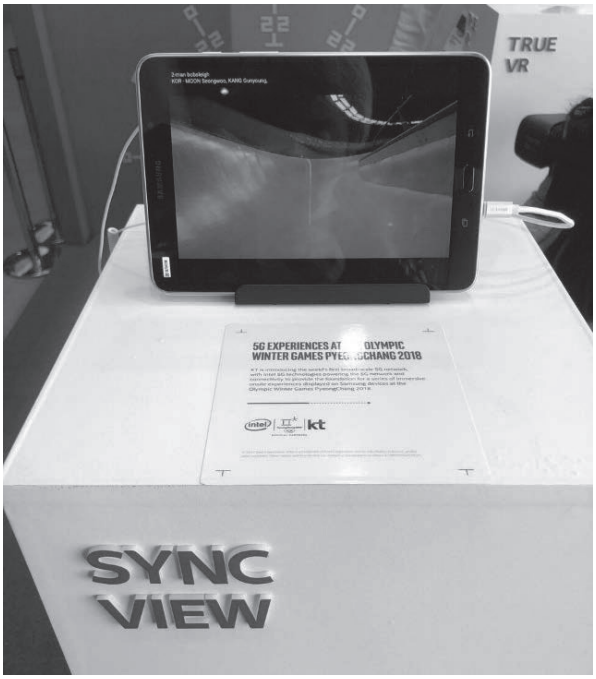
VR で冬季五輪競技体験
写真提供：神部様（NHK エンタープライズ）

韓国技術による
ピョンチャン五輪向け自動翻訳アプリ画面

4.世界初の5G五輪

ピョンチャン五輪では、5Gの試験サービスが一般の人も体験できる形で初めて提供されることから「初の5G五輪」とも呼ばれ、海外からの注目度も高かった。移動通信の次世代規格として現在標準化が進められている5Gは、「超高速・大容量」、「低遅延」、「多数端末接続」の三つを特徴とする。5Gの商用化時期は当初は2020年が見込まれていたが、現在、商用化目標を2019年に前倒しする国が次々と出てきている。このような状況から、世界的な動きに乗り遅れないために日本でも5Gの商用化時期の前倒しが検討されている。

韓国ではもともと移動通信分野の世界的主導権をとるために、ピョンチャン五輪での世界初の5G試験サービスに続き、2019年3月に世界初の5G商用化をねらう。今回の五輪では、通信分野公式パートナー企業の総合通信最大手KTが5G試験サービスをはじめ、通信インフラの運営を担当した。



5G 活用で臨場感あふれる
選手視点のボブスレー競技中継
写真提供：神部様（NHK エンタープライズ）

5Gの早期商用化をねらう各国では、実用度の高い「5Gならでは」のサービス開発で現在悩んでいる。このようなタイミングで今回韓国が披露した5G試験サービスは、商用化前段階とは言え、どのような実用的サービスが提供されるのか、海外から大きな注目を集めていた。

ICT体験館ではサムスン電子製の専用タブレットで5Gの映像系サービスの視聴体験を提供した。なお、競技映像以外で実際に5Gが活用されたシーンとして、聖火リレーと開会式が挙げられる。聖火リレーでは、ソウル市内の5G試験ネットワーク設置区間で5Gパフォーマンスが実施された。この区間では人間の走者から5Gで制御されるドローンに聖火がバトンタッチされ、ドローンが聖火リレー走者となった。ちなみに、人ではなくドローンが聖火リレー走者を務めたのは五輪史上初めてという。

開会式では、ジョン・レノンの「イマジン」を歌う歌手の周りをLED蝋燭を持った1,000人が取り囲んで「平和の鳩」模様を作った。この時に、立っている人の位置によるLED蝋燭の点火や明るさの調節を、5Gで制御した。ここでは、5Gの特性である低遅延と多数端末接続が活かされている。なお、開会式のハイライトとして夜空を彩った、インテルの1,218台のドローンによる光の演出では、特に5Gを使う必要はなかったということで、ここでは5Gは活用されていない。

5.五輪テロ対策の体制

国家セキュリティ対策を担う国家情報院がテロ対策の中心組織である。国家情報院は大統領直属機関として、国内・対外の安全保障に関する情報収集や捜査を実施する。韓国ではスパイ通報番号として、国家情報院につながる緊急電話番号111番が設けられている。ピョンチャン五輪大会期間中は国家情報院を中心に警察、軍などの政府17機関で構成する対テロ安全対策本部が設けられ、一日最大6万人がテロ・安全対策の任務についた。国家情報院は大会の1年前から米国CIA等海外の情報機関との協力体制を通じ、大会直前までにテロとの関係が疑われる外国人3万6,000人の入国禁止措置をとっている。

6.バイオ情報活用システム

ピョンチャン五輪では、歴代の五輪史上初めてテロ防止対策として顔認証システムが主要競技場に設置された。海外協力機関から共有された情報を国家情報院でデータベース化して顔認識システムを活用する。登録されている危険人物の顔認識情報は数万名に達する。

危険人物の入国を阻止するため、空港と港湾では入国審査を担当する法務部と協力して、五輪大会期間中、顔と指紋を比較・分析するバイオ情報分析システム（BASE:Biometrics Analysis System for Experts）を活用した。BASEは、あらかじめ収集した海外のテロリスト等危険人物のバイオ情報を入国審査時に申請象者と比較して一致するかを判断するシステムである。BASEの活用で2015～2017年に偽造パスポートでビザや国籍を申請した外国人合計4,790人を

摘発している。麻薬や暴力犯罪の外国人被疑者についても、BASEに登録されていた写真のみで本人を特定したケースも3,301件とされている。

ピョンチャン五輪大会組織委員会によると、競技場周辺に設置された高機能監視カメラは800台以上。監視カメラ映像でとらえた人物は世界の危険人物データベースと照合される。ピョンチャンの組織委員会メイン事務所に設置されたセキュリティ管制センターで24時間体制の監視をする。今回の大会期間中、会場のセキュリティ検査を受けずにフェンスの下から侵入しようとした人物を監視カメラでとらえ、現場で検挙している。

スケート競技場地区のカンヌン五輪パーク
写真：筆者撮影

アイスアリーナ前に設置された監視カメラ
写真：筆者撮影

7.空からの監視体制

今回の五輪会場地域は、スキーやそり系競技は山岳地域のピョンチャン、スケート競技は少々離れた海沿いのカンヌンという二地域に分けて開催された。上空からの警備体制として、スケート競技会場地域となったカンヌン市では24時間体制の軍用飛行船（上空150～200m）が投入された。軍用飛行船はケーブルで10トン級特殊車両とつながれており、運用は軍の専門家が行う。軍用飛行船が国内開催の国際イベントに投入されるのは今回が初めてという。各競技場での競技時間帯には無人飛行機3機が交替で出動した。軍用飛行船と無人飛行機に搭載された高機能監視カメラで異常が発見された際はセキュリティ管制センターに映像が送られ、現場要員が即時出動する体制がとられた。

警察では、映像伝送システムを搭載した国産の新型警察ヘリコプター「チャムスリ（KUH-1P:大鷲の意味）」2台を運用し、大会期間中毎日競技場上空を巡察した。警察の20機以上のヘリコプターのうち、最新システムを備えたチャムスリは現在4機。警察は2020年までに最新型チャムスリを8機に増やす方針である。

8.ドローン活用のテロ対応策
ードローンを捕まえるドローンー

今回はドローンを活用した新型テロへの対策が図られるとともに、ドローンが初めて本格的な警備に活用されたことで、開会式のパフォーマンスのみならず、セキュリティ面でもドローンが注目を集めた。大会開催地域は飛行機やドローンの飛行禁止区域である。飛行許可を受けていないドローン取り締まりのため、国家情報院と科学技術専門大学の韓国科学技術院（KAIST）が開発を進めたドローン探知レーダーシステムが初めて導入された。飛行許可を受けていないドローンをレーダーで捉えた場合、まず、電波遮断技術でドローンを無力化する。そして、専門要員がヘリコプターで接近して散弾銃でドローンを撃墜する。同時に、網を投げて未確認ドローンを捕獲する、いわゆるドローンを捕まえるドローンも出動するという二段構えの体制である。このシステムは海外セキュリティ機関からも関心を集めた。

また、今回、国内開催のイベント会場での要人警護にドローンを初めて活用した。大統領臨席のイベント会場周辺の森林地域等の警備で活用するドローンにはHD-Fullの高画質カメラと熱画像カメラを搭載している。ドローンの活用で、大会期間中の山岳地捜索要員を半分に減らして効率化したという。

9.サイバーセキュリティ

大会期間中、政府の関連機関の合計700名で組織するサイバーテロ対応チーム（CERT）が立ち上げられた。CERTの構成は次の図のとおり。

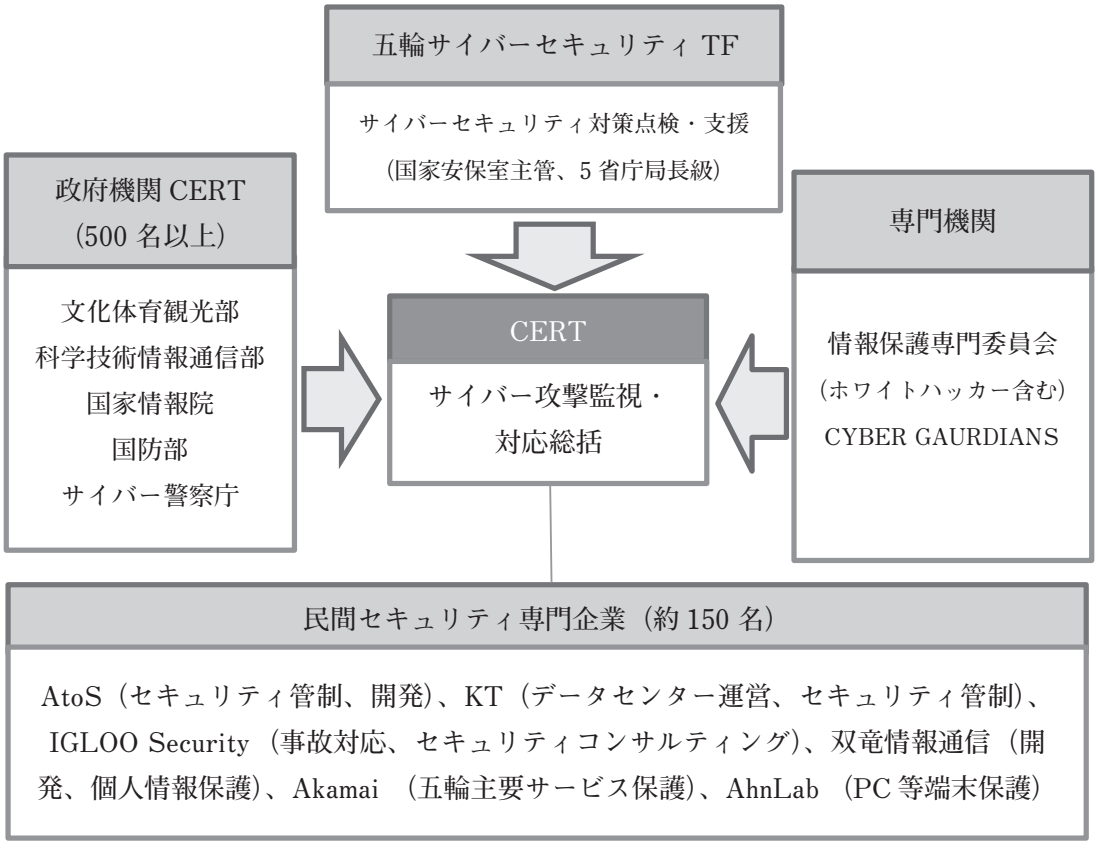
海外との協力体制により、今回は、五輪開会式動画を装ったウィルスやハッキングメール等11件のサイバー攻撃が探知・遮断された。しかしながら、2月9日の五輪開幕式に合わせたサイバー攻撃が発生した。この影響により、ピョンチャン五輪組織委員会ホームページが翌日朝までダウンし、競技会場メインプレスセンターの通信ネットワーク障害を引き起こして会場TVの映像が数分間途切れた。五輪組織委員会は国際五輪委員会（IOC）との協議で、五輪セキュリティ維持を重視するため、今回のサイバー攻撃の経路や詳細は明かさない方針としている。サイバーテロをとりたてて広報することは得策ではないという判断である。

10.終わりに

今回の五輪は開会式直前に北朝鮮に話題を持っていかれた感が強かったものの、特段の事故も起こらずに全日程を終了し、韓国政府や主要メディアは、ピョンチャン五輪は大成功としている。ICTやセキュリティの面についても大成功とされている。

今回の五輪で披露された5Gは標準化前の試験サービス段階であり、サービスの種類は限定的である。今後5Gは、2020年の東京五輪では商用化段階、北京冬季五輪が開催される2022年は応用段階を迎えるため、五輪ごとに段階的に発展する5G活用サービスの姿を実感できることであろう。

今回の五輪のセキュリティ面では顔認識システムやドローンの活用が新たな取り組みとして注目された。一方、五輪開会式のステージで歌う歌手の隣に、乱入した不審者が堂々と立ち並ぶという珍事件も発生した。



ピョンチャン五輪サイバーテロ対応チーム（CERT）構成図
出所：科学技術情報通信部

世界に向けて放送された開会式のこの場面では、不審者があまりにも堂々としていたため、演出の一部と思った人も多いであろう。ちなみに、この不審者は二度もステージに乱入した挙句、取り押さえた直後に逃走し、翌日他の競技場に現れたところをようやく抑えられたという。このような状況も考慮すると、セキュリティの抜け穴もあったと見るべきであろう。開会式中にサイバー攻撃による影響もあり、サイバー攻撃も完全に防ぐことは難しいことが判明した。

最後に、東京五輪の参考とするため、様々な業界が今回の大会期間中現地を訪れたが、韓国での五輪準備のスケジュール感の違いでとまどった人も多いであろう。ICT分野については、前述の5分野のサービスを世界にアピールするための準備がほぼスケジュール通りに進められた。しかしながら、大会期間中にこれらのサービスをいつどこでどのような形で体験できるのかという情報は直前まで広報されず、ICT五輪の英語版案内パンフレットの配布が開始されたのも開会式前日であった。そのため、ICT分野視察目的で訪韓する人のほとんどが、現地に行ってみなければわからないという状況であったと思われる。事前広報の段取りのスケジュール感覚がもともと日本と大きく違うのであろうが、世界からの訪問客向けの情報提供の段取りについては大いに改善の余地がある。

ピョンチャン五輪でのICT活用戦略についてこの1年間調査をしてきたが、現地では前年の政治混乱の影響もあり開催直前まで五輪が盛り上がらずどうなることかと思ったが、大会が始まると一斉に関心が高まった。2年後の東京五輪を考える上で、ピョンチャンの事例がいろいろな面で参考になるであろう。

注目商品

A to M - EG 開発物語

株式会社ゴール
取締役　営業本部長　兼　商品企画開発室　統括マネージャー　葛西　明生

【当社の創世記】

「歴史と伝統」。1914年に創業し、錠前および鍵の製造を生業とし、今年104年目を迎えます。ここまで本業に精進できたのも、当社の技術力がお客様の“安全”と“安心”を守るに値すると評価いただいた賜で、非常にありがたい事と存じます。

大阪白玉錠製作所として創業の後、1928年谷山製作所に改称、1932年我が国初のシリンダー錠の製造を開始、1959年には初の国産円筒錠「ユニロック」の製造販売を開始しました。

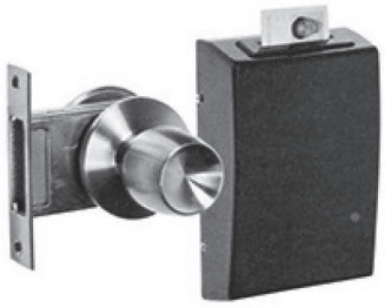
初の国産ユニロック USPシリーズ

1964年（前回の東京オリンピック開催）には社名を現在の「株式会社ゴール」に変更。

1972年日本で最初の電気錠、カードロック及び各種防災システム機器を開発しました。

しかしながら、その開発は困難を極め、カード情報の読み込みが不安定、カードの排出がスムーズでない…。

すべてが初めての経験のため次々と現れる課題を一つひとつ解決した後の誕生でした。



日本初のカードロックシステム

【セキュリティ市場の改革】

当社の電気錠、カードロックの開発から約半世紀、電気を用いたセキュリティシステム関連機器は目覚ましい進歩を遂げました。リモコン操作によるもの、非接触認証によるものなど、自動車におけるセキュリティ認証方法はその都度、住宅玄関錠にも波及していきました。

「スマートエントリー」、「スマートキー」と、呼び方は様々だが、それまでの鍵の概念を超え、ノーアクション、ハンズフリーで解錠できる画期的なキーセキュリティシステム。

現在では、自動車に当然のように搭載され、その利便性は周知のところ。もともと自動車から派生したこのシステムが、我々の商材である扉錠にも採用され始めたのが2005年頃のこと。当社も錠前メーカーである以上当然、商品ラインナップとして持ち合わせなければならないという使命のもと、取り組むこととなりました。

【第一ステージ】

それまでも、電波認証システムの技術はありましたが、あくまでもボタン操作が伴うリモコン認証によるのもので、自動的に認証するものがどのような原理であるかを知ることから開発は始まりました。捻り出した結果①電波法を伴う周波数と強度②バッテリーの消耗③セキュリティエリアに関する課題が残りました。

しかしながら、何れも支援を得てクリアし、共用玄関用ハンズフリーシステム「SRS-200/スマートリーダーパスカル」が完成しました。2015年3月、他社に遅れること10年でした。

意気込みよろしく販売を開始しましたが、懸念された電波干渉による認証不備や、認証用の携帯機の強度など、既に他社が市場投入後に検証してきたことの後追いでの改善を余儀なくされました。

一方市場は、おのずと個別の住宅玄関へもハンズフリーシステムの要求が増し、当社も開発に取りかからなければいけない状況となり、またしても後塵を拝すること

となりました。本来であれば既存システムから派生する開発に取り組むべきであるが、当社は別のチャレンジを試みることを決意しました。

エントランスリーダー SRSチラシ

【第二ステージ】

再度新たな一歩からのスタートであり、セキュリティ及び差別化の側面から、先行する錠前メーカー各社が採用していないモノを模索しました。当然の如く、当初から開発は困難を極め、ゴールは遥かに遠い状況でした。

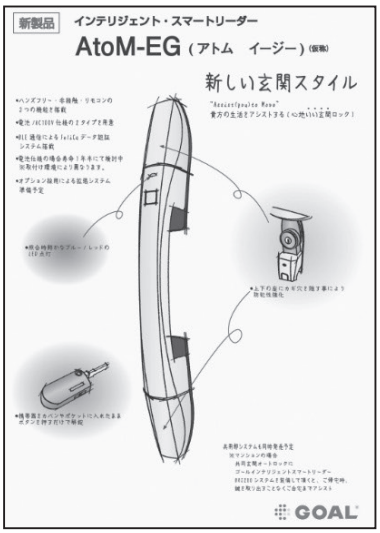
結局、様々な業者との検討と、拡張性を考慮した結果、高周波（2.4Ghz）帯による開発を選択しました。すでに市場には、扉の錠前に関し今まで全く取り組みの無かったベンチャー企業が、スマートフォンを利用したスマートロックを開発、製品化していました。それらに採用されている周波帯が普及し、各社の検証を行った結果、認証セキュリティが脆弱では?と思われるものも存在するということや、認証のバラつきの問題などが聞こえる中、錠前メーカーとして積み上げてきたセキュリティの重要性を最大限に加味した開発検証に踏み出しました。

実際に、PC関連のガジェットや、スマートフォンなど、今日身近に存在し将来的な拡張性を視野に入れ開発は進みます。試作レベルでの検証を終え、参考出品として展示会へも出展し、日を追い順調に進んだが、ユーザビリティの観点から様々な条件を精査する必要を余儀なくされます。

パーソナルセキュリティエリアをより厳密にする必要があること、ユーザー目線での更なる利便性を追求した結果、改善が必要との判断のもと、発売延期を決めました。

どれが正解か分からないまま、認証試験を延々と繰り返し模索し続けた結果、ようやくベストな選択にたどり着くことが出来ました。

現在、最終のブラッシュアップに取り掛かっています。



2016 年 参考出品展示会用チラシ

【新製品　AtoM-EG】

開発からの一貫した製品コンセプトは“Assist you to Move”＝「暮らしをアシストする良い玄関錠」であり、ネーミングは「AtoM-EG（アトムイージー）」と名付けました。

特徴としましては

・ワングリップタイプの洗練されたデザイン
・ハンズフリー、非接触キー、リモコン認証が可能
・電池式と外部電源式の2タイプあり
・バッテリー寿命は一日10回の施解錠で1年半
・携帯機（AtoM-Pocket）、カード、キータグに対応
・室内操作盤との連動可能（外部電源式オプション）
・シルバー、ブラック、ゴールドの3色
・エントランス用BRS-200等との連動可能

玄関錠 AtoM-EG パンフレット

【今後の課題】

私たちは玄関のセキュリティに関し今後、利便性と反する脆弱さやリスクを更に検討する必要があると考えます。以下にその一例を記します。

①ホテルに於いては自動施錠機能が当然であるが、住宅に於いては、入居者の脳内で「扉を閉めると鍵がかかる」という日常動作がルーチン化されない限り、締め出しになる可能性がある。容易に自動施錠を選択することに関して利便性が高いと提唱はすることは難しい。

②電池式のツールを用いる限り、バッテリーが消耗した場合作動しなくなる。また、定期的にバッテリー交換が必要となる。メンテナンスフリーが快適さに繋がるのであれば、玄関錠は外部電源式、手に持つ認証用装置は非接触による無電池のものも選択肢として準備する必要が有る。

③認証機器の追加時や、紛失等に伴い新たに認証用装置を購入する際に高額になる。

④セキュリティの重要度に応じた適正な認証が必要である。例えば、マンションエントランスは、共連れ防止（住人以外の入館を完全にシャットアウト）等が十分に考慮された入館システムでない場合、ハンズフリーシステムは有効。然しながら、各住人に限定される個別玄関は、ハンズフリー機能を活かすにしても、パーソナルセキュリティエリア内でのワンアクションは必須。

これらの理由を加味し、当社がセキュリティ商品を提供するにあたり、十分な打合せのもとにお客様へ提案することを徹底し、また玄関錠は、電気系のトラブルなどの非常時のためのメカニカルなキーが使えるシリンダーは搭載すべきと考えています。

この先も私たちは、“安全”と“安心”をご提供させていただくに値する技術力の研鑽に励んでまいります。

注目商品

電気錠からスマートロックへの展開

美和ロック株式会社　システム機器開発部　部長　宮本　敦

【はじめに】

日本で電気錠が導入され始めたのは1975年頃、ビルの防犯・防災システムへ対応することがきっかけとなり、電気錠の開発と生産がスタートしました。

その後、設置場所・運用方法・認証方法・電源の取り方・取手のタイプなど使用用途によって様々な電気錠が生まれました。IoT時代を迎え、電気錠はスマート化・ネットワーク接続により更なる進化を遂げようとしています。

1.電気錠の基本機能

電気錠は手動で操作する一般的な錠前（メカ錠）に対して、電気的に施解錠の制御が行えること、また施解錠や扉開閉の状態信号を取ることができる錠前であり、電気錠本体とは別に制御部・操作部と組み合わせて使用することが一般的です。

電気錠のタイプは、大きく分けて4タイプあります。

①通電時施錠型

通電している間は施錠状態となるタイプで、通電が切れると解錠となります。主に非常口や避難口に使用されます。

②通電時解錠型

通電している間は解錠状態となるタイプで、通電が切れると施錠となります。防犯性を考慮したオフィスや事務所の入り口などに使用されます。

③瞬時通電施解錠型

短いパルス通電の度に施解錠を繰り返すタイプであり、停電等に影響されることを好まない住宅などの玄関に使用されます。

④モーター施解錠型

モーターにより、デットボルト（かんぬき）を出し入れします。これは電動でデットボルトの出し入れが可能であるため、空錠がない場所に適しています。また、錠ケースの奥行が比較的小さいため、扉の掘り込み深さを小さくする必要のある狭框扉にも有効です。

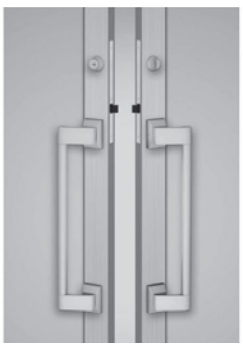
電気錠を採用する際には、使用目的や用途によって最適なタイプを選択することが重要です。

2.ビルの電気錠

近年、企業における個人情報の保護・機密情報の管理など、オフィスに関わるセキュリティへのニーズが更に高まっており、安全性と利便性を向上させるために、出入管理システムも変化しています。テナントオフィスビルで使用される電気錠は、確実に人の出入りを把握し管理するために、自動施錠タイプの電気錠が使われ、目的に応じて『通電時解錠型』、『通電時施錠型』が多く選択されています。これらの機能は電気錠に内蔵されたメカニカルスイッチで切り替えができ、取り付けた後に電気錠を交換することなくニーズや状況に応じて機能を変更することができるようになっています。

また、多くの人が集まるオフィスやテナントの出入口では、1つの扉での入退が多く、さらに扉が閉まるたびに施錠が行われるため、電気錠の施解錠動作回数が非常に多くなります。このような出入りの激しい場所に使用される電気錠は特に耐久性のあるものが適しています。

外観においては、ビル用の電気錠は、レバーハンドルタイプのものが主流となっていますが、最近ではデザインや操作性に優れたプッシュプルタイプのものも市場に出始めています。



プッシュプルタイプ電気錠

3.集合住宅の電気錠

集合住宅では、共用エントランスのオートロックシステムが普及していますが、専用部住戸玄関への電気錠の普及も進みつつあります。

・共用エントランス

共用エントランスではオートロックが多く採用されてお

り、RFIDキー等を使用した入館システムの普及率は非常に高くなってきています。

共用エントランスに設置されているリーダに、鍵と一体になったRFIDキーをかざして入館する「ノンタッチキー」が一般的ですが、バッグやポケットから鍵を取り出すことなくリーダの前を通過するだけで入館できるハンズフリーIDキー「Raccessキー」も近年では増加傾向にあります。

ノンタッチキー（RFID 式）　　Raccess キー（ハンズフリー式）

これらは共用エントランスを統合管理する制御システムとなっており、同一の ID キーで共用エントランス周辺機器や他システムとの連動が可能となります。

宅配ボックスシステムとの連携により、Raccess キーを所持した住人が共用エントランス入館時に着荷の通知を受け、さらに宅配ボックスの前でセンサーに近づくだけで、本人宛に届いた荷物を取り出すことができます。また、Raccess キーを持ったままエレベーターの前に立つことで、自動的にエレベーターを呼び出すことも可能となります。（こういった連動には、接続に必要な配線や通信インターフェイスの仕様について関連機器メーカーと事前にすり合わせを行っておく必要があります。）

共用エントランスの各種連動

さらに、この共用エントランス制御システムは、インターネットを通じて居住者向けのポータルサイトサービスと連携し、パーティールームなどの共用施設の予約情報に基づき居住者用の ID キーで施設を利用したり、子供の帰宅通知メールの送信なども可能となっています。

このように、近年の集合住宅共用エントランスは、安全性と利便性の向上が進んでいます。

・住戸玄関

住戸玄関は家族の命と財産を守るためのもっともセキュリティを重視した出入り口の一つで、高い防犯性が求められます。

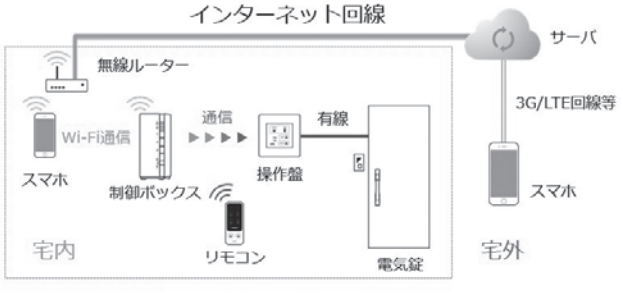
住戸玄関用電気錠はその防犯性を重視しつつ、利便性・デザイン・施工性・低コスト化においても進歩し続けており、年々普及率も高まってきています。

一例として、最新のインテリジェント電気錠「iELZero」について説明します。

インテリジェント電気錠「iEL Zero」

この電気錠は共用エントランスと同じ Raccess キーをバッグやポケットに入れたまま、錠前取手部上部にあるボタンを押すことにより施錠・解錠させることができるものです。この電気錠の最大の特徴は、電気錠制御に必要な回路基板部分を電気錠と別々に取り付けるのではなく、強固な電気錠本体の中に収納している点です。従来のシステムは電気錠と制御盤が別ユニットになっておりその間が配線で結ばれていましたが、iELZero ではこの構造により配線を攻撃する不正解錠を困難としました。さらに認証リーダユニットを取手に内蔵することで、デザイン性・施工性も改善しています。

iELZero には、電源として単三電池を使用するものと AC100V 電源を使用するものの 2 タイプがあります。AC100V 電源を使用するタイプでは専用の操作盤に繋ぎ、さらに機能拡張を図ることができます。操作盤は無線通信により専用のファイヤーウォール装置となる制御ボックスを経由してインターネット上のサーバーとつながり、スマートフォンでの各種操作が可能な「wiremo」システムと連携できます。



wiremo システム構成図

「wiremo」では、スマートフォンにより外出先からでも玄関の施錠・解錠の状態を確認することができます。

また、もしも解錠状態であった場合はスマートフォンで施錠操作を行うこともできます。さらに、子供の外出・帰宅の通知を受ける、家事代行サービスなどの事業者にキーを預けて限られた日時だけ有効な時限キーとして使う、といった多彩な機能を持っています。

4. 電動サムターン

今日までアパートや集合住宅では通常のメカニカルなロック（メカ錠）が取り付けられてきました。最近ではそのメカ錠に対し、電池で駆動し施解錠させることができる後付け可能なロック（電動サムターン）の需要が増加傾向にあります。

テンキー・NFC 対応電動サムターン

電動サムターンは扉外からの配線や電気工事を行うことなく、施工が簡単かつ短時間で取り付けることができます。既設物件に対応する際には導入コストを抑え、また取り付け後に即日運用が可能です。

電気錠と同様に暗証番号・非接触 IC カードなどで認証が可能なさまざまな電動サムターンがあり、集合住宅であれば共用エントランスと ID キーを統一することも可能です。今後は、インターネットにつなげることで、室内外よりアプリを使用しスマートフォンによる施解錠状態確認や施解錠操作、鍵の受け渡しなどを行うことが可能になっていきます。

電動サムターンのデメリットとしては、駆動部と電池を扉面に有することでユニットのサイズが大きくなり、意匠的には不利であることが挙げられます。また、すべてのメカ錠に対し、電動サムターンが取り付け可能というわけではなく、長期間安定して使っていただくにはしっかりとした取り付けが基本となる為、施工においては当社サービス代行店等のプロに相談することをお勧めします。

5. ホテルの電気錠（ホテルカードロック）

ホテルの客室で使用される電気錠は、最近ではカードで認証を行うタイプが主流となっています。初期の製品は磁気カードから始まり、その後接触式 IC カード、非接触 IC カードへと使うカードの種類も時代に応じて進歩してきました。

ホテルカードロックは、ホテルの多数の客室に設置する上での設置性や施工コストを考慮し、電池式となっています。扉外への配線はなく、制御回路・リーダ部などすべての電子機器部分が電気錠とハンドル台座に内蔵されており、ホテルカードロック一式で電気錠としてのシステムが完結するスタンドアロンタイプが一般的です。

ロックの機構的な機能は自動施錠となっており、室内から退出するときにはレバー（ノブ）操作のみで解錠・開扉できるアンチパニック機構が付いています。

使われるカードに関しては、磁気カード時代には摩耗や汚れなどの影響で読取が悪くなる場合もありましたが、近年非接触 IC カードが主流になってからは、操作性・信頼性も大幅に向上しています。

さらに最近では、スマートフォンに搭載されている Bluetooth Low Energy（BLE）を利用した認証を行うことができるホテルカードロックが注目されています。スマートフォンでチェックイン操作をすると、予約情報に基づく鍵データがスマートフォンに配信され、そのまま入室できるシステムも今後可能になっていきます

また、現状は先述のようにスタンドアロンタイプが主流ですが、今後はネットワークにつながるオンライン化も進んでいきます。また、デザインにおいても、スリムタイプなどスタイリッシュさを追求したタイプの展開が広がっています。

ホテルカードロック（イメージ）

6. おわりに

もはやなくてはならない産業インフラ・生活インフラとしてインターネットが普及し、人とネットをつなぐスマートフォンが普及し、物とネットがつながる IoT が本格的な発展期を迎えています。

これまで、先進的なセキュリティシステムはオフィスビル向けや業務用のシステムでしたが、その機能がスマートロックに集約され住宅にも普及していく時代となりました。

遠隔で戸締りが確認でき施錠操作まで可能となり侵入盗の第一因である無締まりを防止できることは住宅のセキュリティの大きな進歩をもたらします。こういった機能は新たな利便性・快適さ・安心をもたらしてくれるものですが、ネットワークを通じて情報が行き交うことはセキュリティ上のリスクでもあります。

今後も我々は人々の生活を守る要である鍵にセキュリティと利便性を兼ね備えた電気錠を作り続けて行かなければならないと考えています。

静岡県防犯設備士生活安全協議会の紹介

防犯設備士　第 92-0587 号
静岡県防犯設備士生活安全協議会　会長　大島　至了

静岡県は日本のほぼ中央に位置し、太平洋に面しており東西155㎞、南北118㎞の距離があり、海や山、湖等の様々な自然に富んだ県といえます。南側は遠州灘、駿河湾、相模灘に沿った海岸線と北側は富士山等の山岳地帯が東西に長い地形を囲んでいます。

【協会の概要】

静岡県防犯設備士生活安全協議会は防犯機器及び防犯システムの普及啓発・研究、その他会員相互の緊密な連携を図ると共に安全産業としての特性を生かした活動を推進し、もって安全で住みよい住環境づくりに寄与することを目的として、平成11年8月20日に設立し今年で18年になります。

現在の正会員事業所数は20社で、役員体制として会長1名、副会長2名、監事1名は会員の互選により選任されます。更に静岡県警察本部より顧問に生活安全部長、参与に生活安全企画課長と同課の防犯対策推進室管理官の3名のご協力を頂いております。原則として役員の任期は2年とし、事務局は会長の所属する事業所としております。

【静岡県下の犯罪発生状況】

静岡県警察本部における平成28年度の全刑法犯の認知件数は20,869件であり、15年連続で減少しています。罪種別で増加したものは知能犯＋60件であり、減少したのは凶悪犯、粗暴犯、窃盗犯、風俗犯、その他全てに見られます。窃盗犯の認知件数は減少傾向にあるものの検挙率は低下傾向にあります。増加した主な手口としては出店荒らし、忍び込み、空き巣で減少した主な手口は自転車盗、万引き、オートバイ盗です。

【主な活動】

1.「くらしの防犯伝導士」の派遣事業

「くらしの防犯伝導士」は平成19年に設けられ、静岡県警察本部長より当協議会に所属する会員の防犯設備士に委嘱されています。


委　嘱　状

大　島　至　了　様

くらしの防犯伝導士として委嘱します

委嘱期間　平成29年　4月　1日から
平成30年　3月31日まで

平成29年　4月　1日

静岡県警察本部長

防犯伝導士 委嘱状

各地域で開催される防犯に関する講習会等への派遣依頼により講師として派遣され、各種の防犯のハード、ソフト面でのニーズに対応した適切な情報提供や防犯についての啓蒙活動を行っています。前年度の主な内容は「防犯協会会員を対象とした企業の防犯対策」をはじめ、「保育園に対する防犯対策」や「小学校の生徒・職員・保護者を対象にスマートホンを使用する場合の犯罪の防止策」、「看護専門学校での女性の防犯」、「車両ねらいに関する防犯対策」、等々他種多様な依頼内容でした。

防犯伝導士講演（小学校）

特に最近では子供や女性対象の防犯対策やパソコン･スマートホンに関する犯罪防止対策等の講演依頼が多くなっております。やはりその時代による犯罪の傾向の多い分野への講演依頼が多くなっています。平成28年度の派遣依頼は13件でした。

防犯伝導士講演（事業所）

2.「防犯環境改善プラン提案制度」の活動

官庁及び民間を問わず静岡県警察本部より防犯対策について依頼又は要請があった場合、静岡県民の安全安心を確保するための提案活動を行っています。

防犯設備の設置に関する相談や設置調査及び工事見積等の依頼があった場合の対応策として、「防犯環境改善プラン提案制度」を設けています。それらの案件に対応可能な会員企業から防犯設備士を派遣し対応を行っています。尚、会員が現地調査等に訪問し成約に至らなくても、当協議会より対応費用の一部として補助金をお支払いしております。年に数件あります。

3.「防犯ホットライン」の運用

防犯に関する無料相談窓口としてダイヤル直通の専用電話を設け、県民の防犯に対する悩み事や防犯対策の相談等のなんでも相談窓口の「防犯ホットライン」を設けています。

それらの対応については電話相談だけで解決できない場合は現地を訪問し、「防犯環境改善プラン提案制度」と同様の対応をしております。年に数件あります。

4.「各種展示会」へ参加、出品

地区職場防犯管理協会や（公社）静岡県防犯協会連合会等からの要請又は各種展示会に参加し、防犯機器や警備サービス、カーセキュリティ、錠前、防犯フイルム等を普及推進する為、当協議会の会員を派遣すると共に当協議会のＰＲ活動にも努めております。

5.「公益社団法人日本防犯設備協会」との連携

地域活動の支援、防犯設備士のスキルアップを図る等の活動を行っています。

6.ホームページによるPR広報活動

静岡県警察本部のＨＰとリンクしており、双方からＨＰを閲覧することができます。

【平成29年度の新規事業計画】

1.静岡県防犯設備士生活安全協議会の法人化について

下記の「防犯モデルアパート認定制度」を設ける計画に合わせ「一般社団法人」を取得する為の調査、研究を進めたいと考えております。

2.「防犯モデルアパート認定制度」について

「防犯モデルアパート」として認定することにより、集合住宅での犯罪抑止に貢献します。静岡県警本部や住宅メーカーと連携して制度の普及促進を図りたいと思います。既に実施されている他県の協会様を参考にさせて頂き、実現できるように努力したいと考えております。

【感謝状の授与】

平成29年の定期総会において、静岡県防犯設備士生活安全協議会の「くらしの防犯伝導士」として10年の功労者に対し、静岡県警察本部生活安全部長より感謝状が贈られました。


感謝状

くらしの防犯伝導士
大島至了 殿

貴殿は長年にわたり
くらしの防犯伝導士として
県民の防犯意識の高揚に
貢献されました
ここに感謝の意を表します

平成二十九年六月二十日
静岡県警察本部生活安全部長
警視正 石津裕士

防犯伝導士 感謝状

【課題と今後の取り組み】

1.会員数の減少と会員拡大について

現在の会員数は20社ですが、設立当初よりも減少しております。最大の原因は事業所が新規に入会する場合、又は現在入会してのメリットは何かを求めます。それも当然かも知れませんが、協議会のホットラインのＰＲチラシの裏面に会員名簿を載せ、講演会やイベントの時に配布し企業のＰＲをしています。又、年一回の総会後の懇親会では県警察本部の顧問、参

与を交えた会員同士の情報交換の場を設けていますが更に工夫する必要があるかも知れません。

2.新規事業の一般社団法人化と「防犯アパート認定制度」の認定

現在のところ三役のみで進めていますが、既に実施されている他県の協会の資料を参考にしながら、又、関係機関との調整も図りながら原案の作成等事務的なことから進めております。

3.財政面の問題

現在の収入はすべて会員の会費のみで運営されており、今後一般社団法人化への方向と「防犯アパート認定制度」の制定により今後も現在の会費のままでの運営が可能かどうかの懸念材料もあります。ある程度時間をかけて進める必要があります。

【関係機関との連携強化】

新規事業である一般社団法人化と「防犯アパート認定制度」等の推進があります。

今後益々、公益財団法人日本防犯設備協会及び各地域協会並びに関係各機関等と綿密に連携し情報交換し皆様のご指導を仰ぎながら実現することを願っております。今後共、よろしくお願い申し上げます。

実践型防犯教室の開催

北海道防犯設備士協会　会長
進栄ロックサービス株式会社　代表取締役　高橋　進

我が国の刑法犯認知件数の推移は平成15年より過去15年間減少と言われ続けられておりますが、北海道においても、北海道警察本部資料からも10年前の平成20年刑法犯認知件数全体で59,733件でしたが、平成29年では28,160件と約半数の認知件数と報告されておりますが、反面、国民意識の中で何処かで何かの犯罪に巻き込まれるのではと、いわゆる体感治安はまだまだ改善されていないような気がします。

【安心・安全どさんこ運動・実践型防犯教室】

北海道では、平成17年4月1日施行された「北海道犯罪のない安全で安心な地域づくり条例」。この、条例の関連事業として同年より、北海道警察本部生活安全企画課部外委託講師として地域住民による自主防犯意識を向上させることを目的に、全道69警察署において地域安全推進委員・自主防犯ボランティア団体構成をはじめ広く地域住民を対象にさまざまな犯罪の被害対策カリキュラムで実践型防犯教室を開催しております。そのカリキュラムの内容は下記のとおり実施しております。

①一般住宅の侵入手口と防犯対策の解説
例えば道内における4大侵入手口の解説
第1位…無施錠
※北海道は開放的な土地柄で、施錠する習慣欠如しがち、カギのかけ忘れや無施錠は犯罪者の恰好な餌食となるなど…しっかり施錠習慣＜玄関・窓・上階窓＞
第2位…ガラス破り
※犯行の大半は人目につきにくい窓ガラスを割って侵入される…＜窓の防犯を見直す。ガラス破壊センサー・防犯ガラスやフイルム・補助錠＞など
第3位…こじ破り
第4位…特殊工具等など
と、同上に手口の内容とその対策を分かりやすく解説し、理解していただいています。

②ガラス破りの手口と防犯対策の解説

教室の出席者に参加協力していただき、一般的な板ガラス、網入りガラス、防犯ガラス等の特徴や強度の違いなど比較する「ガラス破壊試験の実演と体験」を行いその知識を持ち帰って地域の方へ伝えていただいております。

③街頭路上犯罪の手口と防犯対策の解説

誰もが路上での犯罪に巻き込まれたり、バック等などのひったくりに遭わないような心構えを踏まえた実演と体験をしており、町内や自治体などには防犯カメラの設置の推進を促しております。

【防犯ボランティアリーダ養成講座】

平成17年4月1日の条例に同じく関連事業として、地域における自主防犯活動のコーディネーターの役割を果たすとともに住民の先頭に立って防犯活動を推進するリーダとなるべき人材の養成講座を開催しており、特にこの講座では侵入犯罪と防犯性能の高い建物部品について解説を行っております。

建物への侵入犯罪の防止を図るため、平成14年11月に「防犯性能の高い建物部品の開発・普及に関する官民合同会議」が開催設置され従来の建物部品、ドアー・窓（サッシ）・ガラス、フイルム・シャッター・玄関錠等などは平成15年10月には建物部品の試験基準が決定され、11月から試験が実施され平成16年4月1日に試験合格品の目録が公表され、このことから共通のCP（防犯）マークを表示する旨などの周知説明など行っており、より防犯意識を高めていただいております。

また、近年の侵入犯罪などの事例やそれらの対策等などでは従来の建物部品から防犯性能の高い建物部品の違いの壊れにくい開けにくい時間が掛かるなどのデモ機を用いて説明を行い続けた結果賃貸マンション等で採用実績が生まれました。

【防犯カメラ】

・防犯カメラの抑止効果…犯罪を企てる者は周囲の「人の目」を伺います。防犯カメラは「人の目」に代わり文句も言わず24時間撮影監視し、犯罪の捜査に重要に貢献し、犯罪の早期解決に欠かせません。

・街頭カメラの設置事例（北海道犯罪のない安全で安心な地域づくり…ハンドブックより抜粋）

1）函館では、北海道新幹線の開業による利用客の安全を確保するため、駅舎外を撮影する防犯カメラを設置し、平成28年3月から運用しております。

2）北海道警察では、札幌ススキノの地区において、犯罪の予防と被害の未然防止を図るため、公共空間に街頭防犯カメラを設置し、平成24年1月から運用しています。

犯罪は環境によって変化して行きます。
今後も今迄同様に安全・安心に寄与してまいります。

総合防犯設備士 合格体験談

総合防犯設備士の昨年度合格者の中から3名の方に、合格体験談をお寄せいただきました。これから総合防犯設備士を目指す方々には大変参考になる良きアドバイスとなっております。皆様のチャレンジをお待ちしております。

体験談 1

総合防犯設備士　第 17-355 号
株式会社グッドライフ　代表取締役
宮本　昇幸

ー これから総合防犯設備士を目指す、皆様へ ー

警察人生のうち、長年、刑事警察に身を置いて、悪質、巧妙化する犯罪を目の当たりにするたび、警察力だけでは、立ちいかなくなってきていると感じておりました。防犯カメラや侵入警報システム等について調べていたとき、防犯対策や防犯機器についてハード・ソフトの両面から学べる、防犯設備士資格のことを知りました。

防犯設備士の資格を取ってからは、被害者への防犯指導や警戒場所を選定することにも役立ちました。また、DIYで行った自宅の防犯カメラの施工にも参考になりました。その後、危機管理や犯罪機会論などに興味を持ち、新たに総合防犯設備士を目指そうと思いました。

受験勉強について、自己流で参考になるか分かりませんが、ご紹介します。

まず、日防設のホームページの「過去問サイト」過去5年分の問題解答を手書きノートにしました。手軽にダウンロードできないことが、逆に、学習効果を高めたと思います。次に、過去問と「総合防犯設備士テキスト」を突き合わせ、テキストの該当部分に付箋・マーカーをしました。出題傾向の分析になる他、テキストを読み込むことで、解答部分が導き出された背景を知ることが出来きて記憶の助けとなり、何より、実務に役立ちました。セミナーは2回受け、講師の方から重要と言われた部分を、資料と自分のテキストにチェックし、自分なりの想定問題を作りました。ポイントの絞り込みに非常に役立ちました。最後は、想定問題を、ひたすら手書きして覚えました。また、スマホのメモ帳機能や録音機能を使って記録した文字や音声を覚えるのも、スキマ時間学習には、良いと思います。

今春、早期退職して起業しましたので、培った知識、経験、取得した色々な資格を生かし、「安全・安心・快適・幸せ」な社会を、ワンストップで実現できるような仕事をしたいと考えております。安全・安心面だけでなく、少子高齢化や労働人口減少等、社会の様々な問題解決にAIやIOTの活用が叫ばれていますが、それらの情報発信と活用ができる総合防犯設備士は、今後、益々、重要になってくるのではないかと思います。

スティーブ・ジョブズも、挑戦し続け、経験を積むことの重要性についてこの様に語っています。「今は先を読めなくとも、大切なのは、点と点はいずれ繋がると信じることだ。」と。

体験談 2

総合防犯設備士　第 17-370 号
大阪ガスセキュリティサービス株式会社
営業第二部　業務用チーム　第 1 グループ
川邊　英雄

私は、大阪ガスセキュリティサービス株式会社という警備会社に勤めております。入社13年目になります。入社時に防犯設備士の資格を取得いたしましたが、当時の所属部署が機械警備とは縁の薄い福祉関係の部署であったこともあり総合防犯設備士という防犯設備士の上位資格があることは知っておりましたが受験することまでは考えておりませんでした。しかし4年前に部署異動があり、業務用機械警備の営業担当としてお客様や関連企業の各施設に対し、機械警備や入退管理システム、防犯カメラ等を提案していくこととなり、警備の勉強を一からやり直す機会を得ました。今回の総合防犯設備士の資格取得挑戦は、部署異動して積んだ経験を試す自分自身の力試しということと、まだ知識の不足している点を振り返る非常に良い機会となりました。

今回、私が総合防犯設備士資格に合格できた大きな要因は、総合防犯設備士受験セミナーを受講したからです。講師の方の親身な指導により過去問から推測する出題傾向を知ることができたのは大きな収穫でした。総合防犯設備士の試験は全て記述式の問題です。設問もセキュリティ概論の知識、警備業法の説明、警備機器の知識、警備システムのプロット、総合防犯監査等、非常に多岐にわたった知識を求めてくるものですので、受験セミナーの受講は絶対におすすめです。

今回、会社のメンバー複数名で受験したのですが、試験日が差し迫ってくるとお互いに勉強の進み具合や覚えた箇所の問題の出し合いをするなど受験に向け意気込みを高められたことも要因の一つとなったかもしれません。

今後は、「総合防犯設備士」の資格取得者ということを念頭に知識を深め、多様化する社会に適した警備提案をお客さまの気づかれていない視点からもおこなっていければと思います。

体験談 3

総合防犯設備士　第 17-375 号
医療法人　静心会　桶狭間病院　藤田こころケアセンター
医療福祉相談室
仁科　満紀子

防犯設備士取得について

私が防犯設備士を取得しましたのが平成21年12月です。翌年の平成22年4月に愛知県セルフガード協会に個人会員として入会致しました。当時（今も）、私の職業は医療・福祉の分野なので、なぜ防犯設備士に?とよく聞かれます。そこで私は【犯罪を少しでも減らすこと】とよく言います。そのような私の動機の背景には、私の父は自衛官、叔父は警察官でした。祖父は騎馬警官だったと聞いておりますので、やはり血筋なのかな、と考えたりします。

総合防犯設備士取得までの経緯

防犯設備士になり愛知県セルフガード協会においていろいろな研修会に参加させて頂いている中、最も勉強になりましたのが、平野富義先生、瀬澤外茂幸先生にご指導いただきました「防犯優良マンション認定審査」の講義でした。

平野先生はわざわざ実際の建築図面までご用意いただきまして丸一日訓練をしていただきました。もちろん私は自身の知識の低さを痛感させられたのですが、同時に両先生方の総合防犯設備士としての高い使命感と倫理観に感銘を受け、それが総合防犯設備士を目指すきっかけとなりました。

受験勉強について

今回の勉強でやはり一番効果的だったのは受験セミナーだと思います。お勧めは各分野の担当講師の違うバージョンでの二回以上の受講です。講師の先生方は、各分野に精通されていらっしゃるので、教え方、伝え方の引き出しも多く、同じ分野の講義を受けていても講師が変わるとその都度学びがあり、大変勉強になり、また、合格に向けても大変参考になりました。

お勧めの書籍としては、小宮信夫先生の著作【写真でわかる世界の犯罪ー遺跡・デザイン・まちづくり】（2017年4月30日初版）です。写真を見ながらなので、小宮先生のコメントが大変分かりやすく頭に入ってきました。そして同先生著作【犯罪は予測できる】（2013年9月20日発行）です。私が【犯罪機会論】という言葉に初めて出会った本で、受験対策はもとより、今後の私に大変大きな影響を与えた本です。

今後の抱負について

総合防犯設備士として専門的な知識を得ながら、地域住民の方に【防犯啓発活動】を行っていきたいと思います。特に、【犯罪機会論】について、もっと勉強し、【犯罪を少しでも減らすこと】に邁進していきたいと思います。

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、順次当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102回	6月1日(金) 6月2日(土)	6月2日(土)	東京	ベルサール西新宿	3/1～4/6 先着順
			大阪	新梅田研修センター	
第103回	9月7日(金) 9月8日(土)	9月8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	6/11～7/13 先着順
			大阪	新梅田研修センター	
			名古屋	ウィンクあいち	
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	8/20～9/21 先着順
			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 先着順
			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　総合防犯設備士受験セミナー･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。また、講習・試験の詳細、会場の住所・地図などは、順次当協会のホームページに掲載いたします。

No	名称	開催日	開催地	会場名	募集人員	募集期間
1	受験セミナーNo.1	7月21日(土)	東京	未定	30名	6/1～7/13
2	受験セミナーNo.2	7月28日(土)	大阪	吹田商工会議所	50名	6/1～7/13
3	受験セミナーNo.3	8月25日(土)	東京	未定	30名	7/2～8/20
4	受験セミナーNo.4	9月15日(土)	大阪	未定	30名	7/2～8/20
5	一次試験A(筆記試験)	10月13日(土)	東京	飯田橋レインボービル	30名	7/2～8/24
6			大阪	新梅田研修センター	30名	
7	一次試験B(講習認定)	12月1日(土)	東京	公益社団法人 日本防犯設備協会	若干名	6/1～6/29
8	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	一次試験 合格者	―
9		12月15日(土)	東京	公益社団法人 日本防犯設備協会		
10	二次試験B(面接試験)	12月1日(土)	東京	公益社団法人 日本防犯設備協会	講習 修了者	―

※セミナーの会場は、決まり次第当協会のホームページに掲載いたします。

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3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
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	
422	会報　防犯設備　2018 年新年号　No.119	運営企画会議	平成 30 年 1 月	―	2,160	
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	
238	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	
250	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	
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
426	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3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 2001-2	3	270	—	410	—	2009/3/31
技術基準	出入管理装置共通技術基準	SES E 2002-2	3	270	—	410	—	2009/3/31
技術基準	磁気ストライプカードリーダ規格	SES E 2004-3	4	290	—	440	—	2010/3/31
技術基準	ゲート管理装置規格（ホテル用）	SES E 2005-2	6	440	—	650	—	2009/3/31
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 2007-2	5	380	—	560	—	2009/3/31
技術基準	ICカードリーダ規格	SES E 2008-2	4	290	—	440	—	2009/3/31
技術基準	非接触カードリーダ規格	SES E 2009-3	5	360	—	540	—	2011/3/31
技術基準	キーパッド装置規格	SES E 2010-2	6	440	—	650	—	2009/3/31
技術基準	指紋認証装置規格	SES E 2011-2	7	520	—	780	—	2009/3/31
技術基準	出入管理用記録プリンタ規格	SES E 2012-2	5	380	—	560	—	2009/3/31
技術基準	出入管理用電動シャッタインタフェース基準	SES E 2013-2	6	440	—	650	—	2009/3/31
技術基準	出入管理装置シリアルインタフェース(RS-232C)基準	SES E 2014-2	5	380	—	560	—	2009/3/31
技術基準	出入管理用自動ドアインタフェース基準	SES E 2015-2	5	380	—	560	—	2009/3/31
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 2017-1	15	1,030	—	1,550	—	2010/3/31
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3月現在

	規格名称	規格番号	頁数	会員価格		一般価格		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）

コラム

便利さの裏に潜む怖さ

公益社団法人　日本防犯設備協会　特別講師　富田　俊彦

1 急速に進化する防犯機器

物がインターネットにつながるIoTの時代が到来して、ビックデータとAI（人工知能）が連動する新たな防犯機器が次々と開発されています。監視カメラが他のAI技術と融合することによって多様化・高機能化が急速に進み、防犯だけでは無く、防災や雑踏警備、社会インフラなど国民に質の高い機器が提供されています。更に、2020年に開催される東京オリンピック・パラリンピックに向けて、防犯機器の研究と開発が加速されている今、私達は防犯のプロとして進化する防犯機器の現状を正しく理解して適切に対応することを求められています。

2 便利さの裏に潜む怖さ

「防犯の要」と言われるカギも進化しており、ノンタッチキー、カードキーをはじめ、指紋、静脈等のバイオメトリックスを利用した電気錠システムが普及しています。

一方では、インターネットで合い鍵を複製した犯人が女性の部屋に不法侵入する事件や、電子キーの制御設定を変更して不正解錠し自動車を多量に窃取する事件など新たな手口の犯罪が発生しています。カメラの高機能化・高解像度化によって人の目では見えない遠方から気付かない間に撮影され鮮明画像で瞬時に何処でも見ることが出来ます。使い易さ、格好良さを優先するあまり、安全性が疎かになって、映りすぎのリスクを抱え、予想もしなかった新たな手口の犯罪を誘発し、流出した画像で誹謗中傷されるなど国民生活に悪影響を及ぼす危険性があります。

3 見えすぎる怖さ

錠前はスマートフォンを使い遠隔操作してドア錠を施解錠するAIの時代を迎えています。指紋は「万人不動、終生不変」と言われますが、スマートフォンで撮影したピース画像から指紋を盗み取って、3Dで偽の指を作り、偽造した指の指紋から、本人になりすましてパソコン等に不正侵入することが可能になっています。

最近の新聞報道によると、パソコンの位置情報（ストリートビュー）を使用して、犯行対象の住宅を検索して空き巣を繰り返していた4人組の窃盗グループが検挙されました。見ず知らずの他人に我が家をいつも見られていることに不安を感じます。

4 見られている怖さ

「顔認証システム」は、ここ数年で急速に普及し、スマホのロック解除、業務用パソコンにログインする際の本人確認、スーパー・書店・ドラックストアーでの万引き防止、空港ビルやスタジアムでの不審者の検索やテロ対策、会社やテーマパークの入退場ゲートのチェック、会員制飲食店の入店チェックなど様々な分野で使用されています。高精度の防犯カメラが各所に設置されて、日常生活で知らない間に、群衆の中の自分の顔が常時撮影され続け、解像度の高い映像で瞬時に個人識別され、事前登録した指名手配犯人などと照合されています。マスクやサングラスを掛けていても顔の一部からAIが推測して本人確認することが可能となり、顔認証システムの精度は99.2%に上っています。

更にカメラは、「群衆の中で不自然な人の行動を読み取る動体検知。人の心理状態から身体の揺れの変化や

体温で興奮状態を読み取る感情検知。人の歩き方から特徴をつかんで個人を特定する歩容認証」など夢の様なシステムが次々と開発されています。

5 場所を特定される怖さ

平成29年3月15日「全地球測位システム（GPS）端末を使用した捜査は違法である」と最高裁判決が出され、本年3月22日、東京高裁では「令状をとらずにGPSシステムを使用して行われた捜査は違法である」と連続空き巣事件で無罪判決が出ました。

一方では、同様のGPSシステムの機器を一般人がネットで簡単にリースして浮気調査や行動確認などで使われているのが現状です。スマートフォンのSNSを使い書き込みや写真投稿する際に、GPS機能をONの状態にすると投稿場所や写真の撮影場所などが閲覧者に分かってしまう恐れがあります。

6 画像を活用した新技術の取り組み

画像の鮮明度と解析技術が急速に進み「防犯カメラ映像は警察の武器」と言われるほど事件・事故の捜査資料で有効に活用されています。更に情報技術が進み設置されたカメラや車載カメラから収集した画像と地図情報や統計データをAIで融合させ、不審者の行動を自動検出し、犯罪の発生を予測して、画像解析や顔認証システムによる指名手配容疑者の特定やドローンによる容疑者の追跡など新たな技術研究と開発が期待されます。

7 問題点と対策

私達は、進化し続ける技術の恩恵を受け、便利さを共有していますが、その裏に潜むリスクや現状の問題点を把握して、機器のシステムや性能・品質を十分理解すると共に、新たに開発された防犯機器の使用目的を明確にして、許容範囲を検討するなど、一定の線引きや必要な法規制を行い、プライバシー保護や個人情報保護法を遵守しなければなりません。防犯リーダーである総合防犯設備士と防犯設備士は、次々と開発される防犯機器に精通し、専門知識と経験に裏付けられた技術を効果的に使い、犯罪の抑止と国民生活の安全に貢献することを求められています。

編集後記

この季節になると花粉症に悩まされる方が多いと思いますが、私は住んでいるところが東京の西、多摩地区のせいか、花粉症がひどくマスクと目薬が手放せません。家族はみんな医者に処方してもらった薬を飲んでいる状況です。

毎年この時期は花粉情報が出されますが、今年は特にヒノキの花粉が例年の10倍との報道もあり、国民病ともいえるのではないでしょうか。

そんなことで、花粉のことがチョット気になり調べると、環境省のホームページに、「はなこさん」なる環境省花粉観測システムというものがありました。

全国120ヶ所に観測所があり、私の近所にも日本医科大学付属多摩永山病院が観測拠点としてありました。データを見ると多い日（3月29日19時）に1m^{3}当たり930個という数字が出ていました。このシステムでは1時間毎にデータ収集されており時間毎のデータが出ています。

しかし、花粉をどうやって数えているのでしょうか。この辺も詳しく説明されていました。

従来は、固定式の採取器で1日1回花粉を採取し、顕微鏡を用いて花粉数を数えるダーラム法が用いられてきたとのことですが、このシステムでは、花粉自動測定器により、内蔵された吸引ポンプで大気を吸引してレーザー光を照射すると花粉などの粒子で光が散乱するので、その散乱光の量から粒子の大きさを判別し、散乱光の数から粒子の数を求めると説明がありました。チョット難しいですが、レーザー光を使うことは確かなようです。

皆さんも良かったら、環境省のホームページを一度見てください。

URL：http://kafun.taiki.go.jp/index.aspx

（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 陽春号（No.120）　平成30年4月25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）

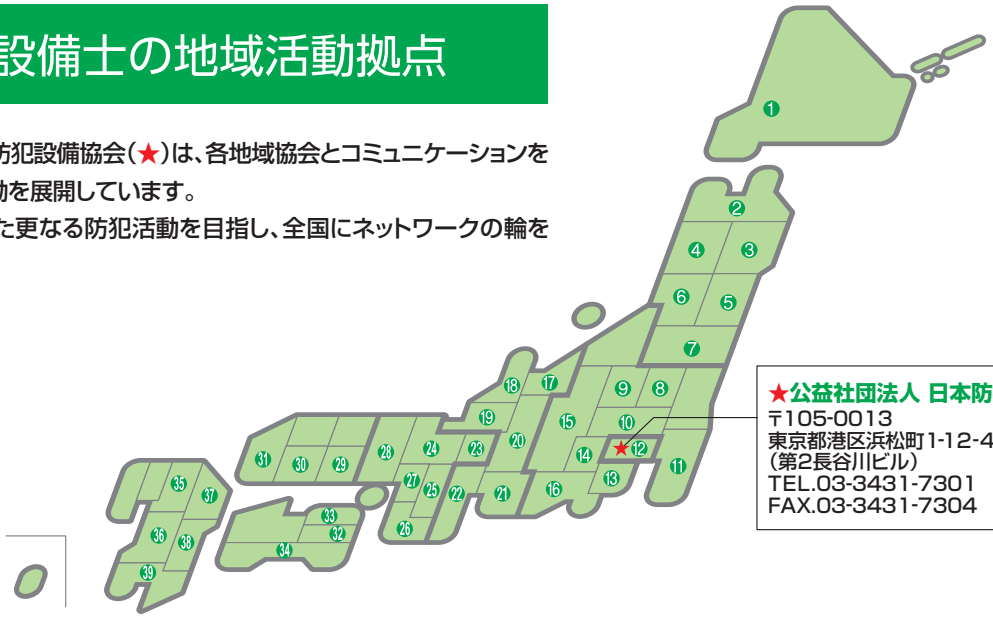
TEL 03（3431）7301　FAX 03（3431）7304

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

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

㉕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
〒812-0021
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3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