「防犯カメラシステムネットワーク構築ガイドⅡ（別冊）
―防犯カメラシステムにおけるサイバー攻撃の手口と対策―」

公益社団法人　日本防犯設備協会　映像監視分科会

1. はじめに

当協会では、平成22年（2010年）10月にネットワーク防犯カメラやネットワークデジタルレコーダを認定対象に加え、平成24年（2012年）10月に「防犯カメラシステムネットワーク構築ガイド」、平成29年（2017年）4月に「防犯カメラシステムネットワーク構築ガイドⅡ」を発行した。令和4年（2022年）1月に発行した「映像ネットワーク構築手順書」は、上記ガイドにネットワーク構築の当時の最新情報を盛り込み、映像ネットワーク構築手順書としてまとめたものである。

今回発行する「防犯カメラシステムネットワーク構築ガイドⅡ（別冊）―防犯カメラシステムにおけるサイバー攻撃の手口と対策―」は、防犯カメラシステムネットワークの構築について、実際の機器の設定方法、クラウドなどの最新の構築手法に加えて、防犯カメラを攻撃対象としたマルウェアによるサイバー攻撃について重点的に記載している。これはその抜粋版である。

2. サイバー攻撃手法

2.1 サイバー攻撃の動向

インターネットに接続された防犯カメラシステムは、様々なサイバー攻撃にさらされる。攻撃の手法は多岐にわたるが、特に以下のような事例が多く報告されている。

(1) 管理画面に簡単なパスワードを設定していたために、攻撃者に容易に推測されログインされる。
(2) Telnet や SSH といった、機器の操作が可能となる機能が意図せず開放されており、攻撃者に悪用される。
(3) 機器がマルウェアに感染し、様々な攻撃の踏み台として悪用される。

国立研究開発法人情報通信研究機構（NICT）が実施している攻撃パケットの観測調査によると、2021年以降、防犯カメラシステムやネットワークレコーダの Telnet（23/TCP）や SSH（22/TCP）を狙った攻撃パケットが観測数の上位を占めている。また、日本国内の複数のネットワークレコーダが Mirai と呼ばれるマルウェアに感染し、様々な攻撃の踏み台として悪用されている事象が報告されている。

情報通信研究機構（NICT）
NICTER 観測レポート
https://csl.nict.go.jp/nicter-report.html

2.2 Miraiマルウェアについて

Mirai は 2016 年にはじめて確認されたマルウェアの一種であり、インターネットに接続されたルータや IoT 製品を主な標的としている。Mirai は機器から他の機器へと感染を拡大させる性質を持ち、感染した機器は他の感染機器と連携してボットネットと呼ばれる巨大なネットワークを形成する。

ボットネットに組み込まれた機器は、攻撃者が用意したサーバ（C&C サーバと呼ばれる）と通信することによりその制御下に置かれ、攻撃者の命令を受信して様々な攻撃に悪用される。ボットネットにより行われる主な攻撃として、分散型サービス拒否攻撃（DDoS 攻撃）が挙げられる。ボットネットに組み込まれた機器がタイミングを合わせて大量のパケットを攻撃対象に送信することにより、対象の処理能力を失わせ機能不全に陥らせる攻撃手法であり、多くの被害が発生している（図 2.2.1）。

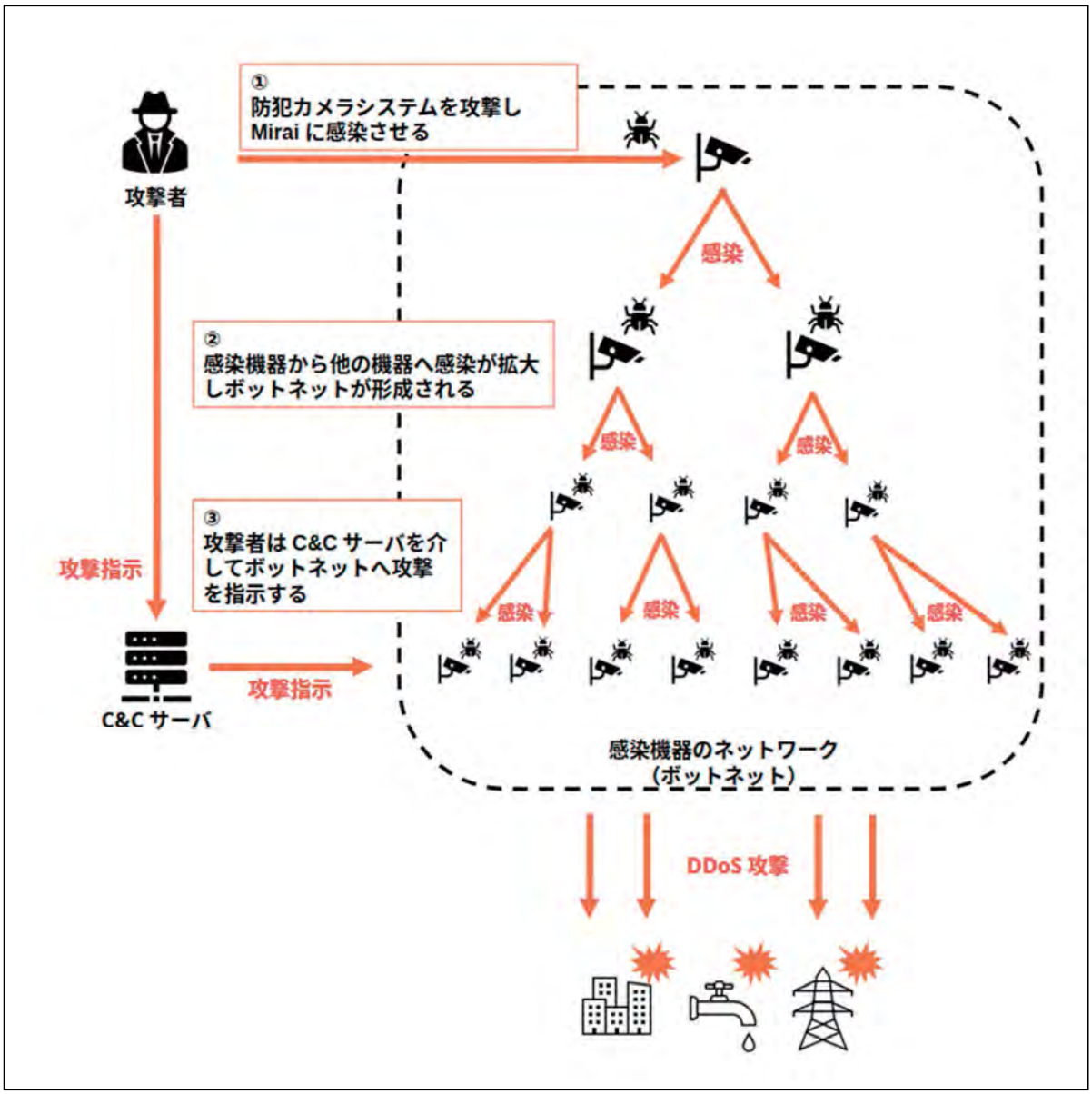


図 2.2.1 Miraiによるボットネット形成と攻撃

Mirai の感染数は近年増加傾向にある。Mirai は、機器の脆弱性を悪用されることにより感染することもあるが、初期設定のままのパスワードあるいは容易に推測できるような弱いパスワードを破られることにより感染する事例も多い。Mirai に感染することにより、自身のカメラシステムが他者への攻撃に転用されないよう、「3 章 サイバー防御手法」を参照して十分な対策を実施することが必要となる。

3. サイバー防御手法

3.1 概要

一般的に、IT システムがサイバー攻撃の被害を受けた場合、システムの機密性（限られたあるいは許可された人だけが情報にアクセスできること)、完全性（情報の改ざんや欠落がなく正確な状態が維持されていること)、可用性（情報を利用する必要があるタイミングで使える状態が維持されていること）のいずれかに影響が発生する。ネットワークカメラやネットワークレコーダに対してサイバー攻撃が行われた場合、防犯カメラネットワークシステムの場合は、国内外での過去の事例から、例えば図 3.1 のようなことが生じ得る。

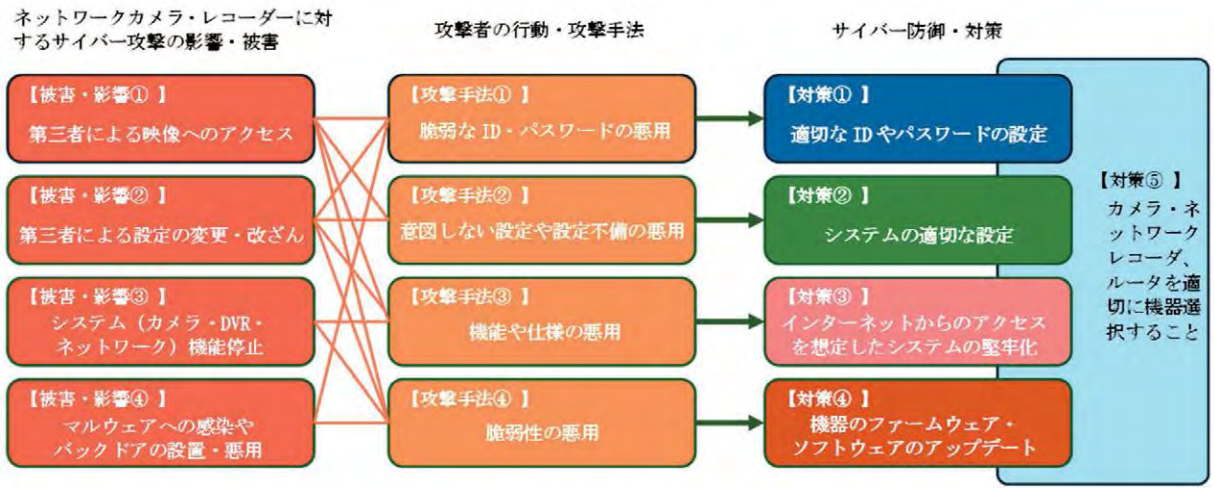


図3.1 ネットワークカメラ・レコーダに対するサイバー攻撃とその対策

3.2 被害と影響

(1) 【被害・影響①】第三者による映像へのアクセス

第三者が防犯カメラネットワークシステムにアクセスし、設置した用途以外の目的で防犯カメラネットワークシステムの映像にアクセスする

(2) 【被害・影響②】第三者による設定の変更・改ざん

第三者が防犯カメラネットワークシステム内の設定やデータを変更・改ざんしたり、意図しないメッセージを表示させたりする

(3) 【被害・影響③】防犯カメラネットワークシステムの機能停止

システムを不正に操作したり、ボットに感染させてネットワーク内の処理をひっ迫させたりすることで予定外の再起動や、ネットワーク全体に通信障害を生じさせる

(4) 【被害・影響④】マルウェアへの感染やバックドアの設置・悪用

ランサムウェアに感染してシステムとして機能の提供が継続できなくなったり、バックドアを設置されて攻撃インフラとして悪用されたりする

3.3 一般的な防御手法

3.2 に記載されている 4 つの影響に対する対策は次の通り。

(1) 【対策①】適切な ID やパスワードを設定すること

(2) 【対策②】適切な設定を行うこと

(3) 【対策③】インターネットからのアクセスを想定したシステムの堅牢化を行うこと

(4) 【対策④】機器のファームウェア・ソフトウェアのアップデートを行うこと

(5) 【対策⑤】カメラ・ネットワークレコーダ、ルータを適切に機器選択すること

それぞれの対策については、機器の設定に関しては各機器によって名称や機能が異なるため、各機器ベンダーより公開されているマニュアルや、サイバーセキュリティ対策のための設定ガイドを参照すること。

No	確認項目	備考
1	販売元、メーカーの連絡先が明記されている （国内 / 海外含めて、保守連絡対応が出来ること）	
2	機器のファームウェアについて、購入後もアップデートの対応が可能である	
3	メーカーHP等で、ソフトウェアのアップデートの連絡などが行われている	
4	メーカーHP等で、サイバーセキュリティに対する方針が明示されている	
5	機器寿命やメーカー保守期日が明確であり、万が一機器に脆弱性が発見された際は、アップデート対応が可能である	
6	VPN接続機能を持つルータである	システム全体のセキュリティ設計による
7	HTTPS通信が可能な機器である	
8	802.1X認証に対応した機器である	

※日本防犯設備協会としては、RBSS（優良防犯機器認定）を取得している製品を推奨する。

表3.3.1 カメラ・ネットワークレコーダ、ルータの選択方法

3.4 具体例：Miraiの対策

2 章の通り、Mirai はネットワークカメラを始めとした IoT 製品が標的とされることが多い。防犯カメラシステムを構築する際は、以下の対策を実施することが望ましい。

(1) 機器の製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施する。

(2) 製品によってはファームウェアの自動アップデート機能が存在する。そのような製品を使用している場合には、同機能を有効にする。

(3) 製造終了から年月が経過した製品は、製造元のサポートが終了し、脆弱性への対応が実施されない場合がある。そのような製品を使っている場合には、サポート中の製品へ切り替える。

(4) 機器をインターネットに接続する場合には、直接インターネットに接続せず、ルータ等を介して接続するようネットワークを構成する。

(5) インターネットからのアクセスを許可する場合は、必要なポートのみ開放する。また、接続元 IP アドレスを限定したり、VPN を用いて接続したりすることも検討する。

(6) パスワードは初期設定のまま使用せず、必ず変更する。また、パスワードを変更する際は、推測されにくいものにする。

3.5 チェック方法

サイバー攻撃はいつ、どこに対して、どのように、何が行われるのかが一概に定まらない。設置しているすべてのカメラや機器などシステムが意図通りに機能しているかに注意を向けておくことが必要である。

3.3 で挙げた 5 つの基本的な対策に対して、サイバー攻撃の影響や被害を受けていないかを確認するためにチェック方法やポイントについて示す。

図3.5.1　取りうる対策とチェック方法とチェックポイント

(1)【チェックポイント①】設定の確認（システムの設計・設置時）

機器の設定について設定シート・パラメーターシートを作成し、初期設定状態、設置時の設定、実際の設定内容を記録し、設定内容の妥当性や正確性を確認すること。なおサービスを提供する前に、提供先とも設定内容や作業記録を基に確認を行うことが望ましい。

(2)【チェックポイント②】変更点の確認（定期的・運用時・被害発生時）

サイバー攻撃により第三者が設定を変更することが考えられる。設置時のパラメーターシートや設定ファイル、設定変更作業記録と比較するなどして、意図しない設定の変更がされていないかを確認すること。過去のサイバー攻撃では、新しいユーザーアカウントの作成や機器名称等の変更、DDNS などのネットワーク設定が変更されていたことがある。

(3)【チェックポイント③】インターネットからのアクセス確認（システムの設計・設置時）

設置時には、インターネットからのアクセスが可能かを確認すること。確認方法として、第三者の視点に立って、インターネット越しにパソコンやスマートフォンからシステムへのアクセスを試みる（たとえば、マイクロソフトエッジなどの Web ブラウザにて、システムに付与されたグローバル IP を入力して表示を確認するなど）などして確認する。なお、システムによってはグローバル IP が固定されていないケースも考えられる。その場合にはルータにてグローバル IP アドレスを確認することができる。

(4)【チェックポイント④】バージョンの確認・アップデートの実施（システムの設計・設置時、定期的・運用時）

システムの設計・設置時にはバージョンを確認し、設定シートなどに記録を控えておくこと。

なお、調達時点で、すでに新しいバージョンのファームウェア・ソフトウェアがリリースされていることもあるため、設置時点で最新のバージョンであるかをメーカーの Web サイトなどで確認すること。不明な場合には問い合わせを行うことが望ましい。新しいファームウェア・ソフトウェアでは、脆弱性以外にも不具合やバグが修正されているケースがあるため、システムの健全性を保つ上で定期的に確認し、新しいバージョンを確認した場合には、適用すること。

なお、Web ブラウザなどの PC ソフトウェアに関しては JVN（Japan Vulnerability Notes）等の情報を確認する方法もある。例えば、独立行政法人情報処理推進機構の提供する MyJVN 脆弱性対策情報フィルタリング収集ツールを利用することで情報が効率的に取得できる。

緊急適用が必要なケースでは、メーカーから情報が提供されることがあるため、連絡経路は適切に整備しておくことが望ましい。

(5)【チェックポイント⑤】侵害有無・被害の確認（定期的・運用時、被害発生時）

サイバー攻撃の被害を認識し、被害発生時の対処を進めるには、システムへの侵害の有無を確認することが不可欠である。運用時、定期的に確認することで、早期に侵害を発見し対処を開始できるため、確認を行うことを推奨する。

具体的なチェック方法として次がある。

ア．各機器におけるシステムログ・アクセスログの確認

機器のシステムログやアクセスログを確認し、認識のない機器の再起動や認識のない不審なアクセスが行われていないかを確認する。なお各機器でログの取得方法が異なるため、具体的な取得方法はマニュアルを参照すること。

イ．ネットワークトラフィック量の確認

ボットネットに感染したり第三者からアクセスされたりすることで、想定していないトラフィックが生じる。ネットワークトラフィック量から侵害の有無を推測することが可能である。特に定期的な確認時にルータを通過したトラフィック量を控えておくことで、正常なケースでの通信量と異常なケースでの通信量を区別できることがある。

防犯カメラネットワークシステムがボット等に感染していないかの外部チェックを行うことも推奨する。具体的には、防犯カメラネットワークシステムのネットワークから（外部 IP を入力して確認するのではないため注意）、横浜国立大学の提供する「Am I Infected?（https://amii.ynu.codes）」を用いて確認することができる。

3.6 被害や問題の発生を確認した後の対応

サイバー攻撃による問題や被害を、自ら気が付くことができることは極めて稀で、多くのケースでは他者（警察、通信事業者、セキュリティ専門家・研究者など）からの通知により気が付くことが大半である。

(1) サイバー攻撃被害を認識する主なフロー

ア . 自分で気が付けるケース：設置者が運用の確認で異常に気が付くケースや、システムの利用者が運用中に気が付くケース

イ . 他者（警察、通信事業者、セキュリティ専門家・研究者など）からの通知により気が付くケース

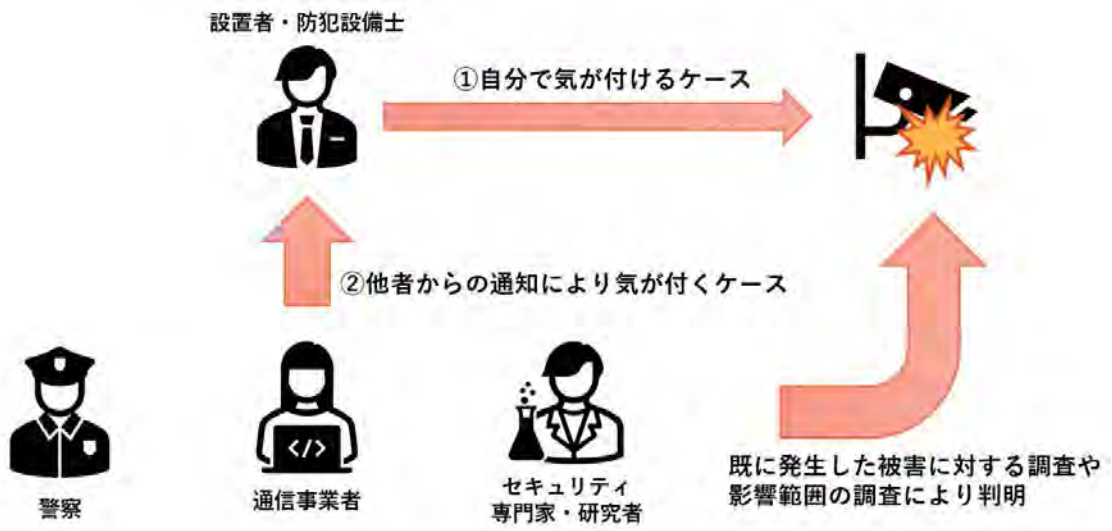


図3.6.1 サイバー攻撃被害を認識する主なフロー

特に他者が認識しているということは、すでにシステムが悪用されており、何らかの被害を及ぼしていると考えられ、早急な対応を進めることが不可欠である。一方で、対応を急ぐあまりに、適切でない対処を進めてしまうと、問題解決ができなかったり、調査に必要な証跡を失ってしまったりすることもあるため、対応手順に沿って進めること。

なお、他者からの通知により認識するケースでは、防犯カメラネットワークシステムをインターネットに接続する際のインターネットサービスプロバイダーとの契約の際に交換される登録情報や、メーカーでの保守・サービス等の登録情報、サーバや機器に設定される電子証明書の登録情報などに基づいて連絡がなされることがある。また、防犯カメラネットワークシステムの場合、稀に「映り込んでいる情報から設置場所が推測」できることで、連絡がなされることもある。そのため、適切に連絡を受け取ることができるよう、それぞれの登録情報を適切に管理することが望ましい。現在、防犯カメラネットワークシステム自体のインシデントについて、通知元を含め報告の義務はないが、インシデントの内容（例えば個人情報に影響があるなど）や設置場所（例えば国が指定する重要インフラ事業者に設置しているなど）によっては報告が必要となるケースがあるため、設置先にあらかじめ確認をしておくことが望ましい。なお、通知元が公的機関ではない国内外の民間企業やサイバーセキュリティ分野の専門家・研究者であることもある。日本語で通知が届けられないケースを想定しておき、適切に応答することが望ましい。

サイバー攻撃への対策を進める上で、次の資料が参考になる。

IPA
中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/guide/sme/about.html

一般社団法人愛媛県防犯設備協会設立

一般社団法人愛媛県防犯設備協会が、2025年11月4日に全国の地域協会の46番目として設立されました。10月31日に行われた設立総会には、愛媛県県民環境部県民生活局長、愛媛県警察本部生活安全部長はじめ多くのご来賓がご臨席されたほか、当協会の代表理事も参加しました。総会では、正会員35社にて無事すべての議案が審議可決され、役員が選任されました。また、今年度および来年度の事業計画案として協会会員の拡充、警察や防犯団体等の各種関係機関との連携、防犯設備士の訴求及び認知度の向上、防犯設備士養成講習等の実施協力、研修会等の開催、防犯優良施設の認定制度の実施、防犯相談・防犯診断の実施等の計画が報告されました。総会閉会の後、祝賀会ではご出席の皆様が親睦を深められました。

竹中エンジニアリング株式会社様 研修会
― 防犯設備士委員会活動報告 ―

防犯設備士テキスト改訂ワーキンググループ(WG) WG長　小林 宜生

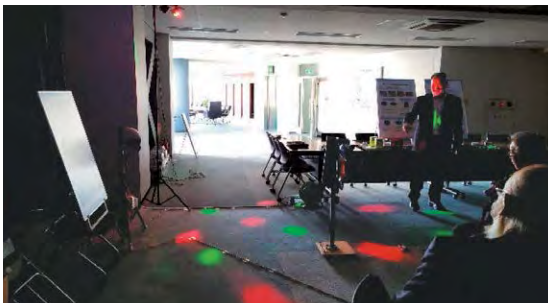
防犯設備士委員会におきまして、去る10月28日竹中エンジニアリング株式会社様本社にお伺いして、侵入警報設備の研修会を行いました。

協会では、常日頃、防犯設備士テキストの改訂を重ねております。その目的は、勉強される方々に正しい知識を“常に”より分かりやすくお伝えすることが使命であるからに他なりません。本テキストを総合的な防犯対策の策定、防犯設備機器の“正しい”選定、配置、施工などにより、様々な犯罪防止に貢献できるものにしていかなければなりません。改訂のWGにおきまして、テキスト改訂作業を行っていますが、折々に疑問点が発見されており、これは防犯設備機器を製造されているお会社様のご指導をいただく必要があると判断するに至りました。2024年には竹中エンジニアリング様東京支店で勉強会の場を設けていただきましたが、講師の皆様から技術的な側面も拝聴したいと本社技術部門にお願いする次第になりました。快くお引き受けいただき、京都に足を運ぶことになりました。メンバーも折角の機会ですので委員会の講師の方々にもお声をかけさせていただき事務局含め11名でお伺いしました。

協会と竹中エンジニアリング様との関係は協会が発足した時からのとても深いものです。防犯設備の歴史の原点は、侵入警報設備です。竹中エンジニアリング様は、1972年に警戒距離200ｍの赤外線ビーム検知器を開発された専業トップメーカーであることは誰にも異論は無いところです。

訪問するにあたっては、赤外線ビーム検知器における干渉と回り込みの違いであるとか、赤外線パッシブ検知器のツイン方式の原理などさらなる知識を深めるため、また侵入窃盗対応の各種無線機器について等、最新の機器の情報を得るためにと、課題をもって行きました。

研修会におきましては、汎用センサー事業部　次長　中田浩幹様と営業技術課　課長代理　加藤学様のお力添えにより並々ならぬご配慮をいただきました。幾多の機器をご用意いただいての機能の実演、また、赤や緑のLEDを装着した赤外線パッシブ検知器でセンシティブゾーンの確認が出来ること等、大変わかり易いご講義をしていただきました。さらにレーザー式検知器、マイクロ波式検知器の作動原理の解説等とても充実した素晴らしい研修の場となりました。



また、中田次長様には竹中エンジニアリング株式会社様の社史と企業の取り組みや実績などを折々開発されました商品を通じてご案内いただきました。社会に必要なものを真摯に且つ地道に一歩一歩開発し続けておられる企業姿勢に感銘を受けました。竹中エンジニアリング様の理念を知る良い機会となりましたことを心よりうれしく思った次第です。そうこうしている内にあっと云う間に17時になってしまい、平野委員長より謝辞を申し上げて終了いたしました。

帰途、京都駅付近にて“反省会”を行い、日頃はパソコンの画面越しでしかお会いしていない面々同士が懇親を深め散会しました。来年度も企業研修会を実施したいと思います。

SECURITY SHOW 2026　セミナーのご案内

自動車盗難防止セミナー

～最新の盗難手口から見えた対策とは!～

当協会からは、「自動車盗難防止に関するセミナー」を開催します。最新の盗難手口から見えた対策等について考察します。是非ご来場ください。

●**会　　場**：SECURITY SHOW 2026　東7ホールステージ【会場（リアル）定員150名】予定
〒135-0063　東京都江東区有明3-10-1　東京ビックサイト東展示棟

●**日　　時**：2026年3月5日（木）10：40 ～ 12：10

セミナーのオンライン配信はございません。リアル会場での参加のみです。是非、展示会場にてご参加下さい。事前申込が必要となります。【申込番号：SS-S5】

●**講演内容**

【概　　要】自動車盗の認知件数は2022年から3年連続で増加しており、犯行グループによって組織的に特定の高額車種が巧妙な手口によって集中的に窃取され、海外へ不正に輸出されるなど非常に厳しい情勢となっております。

こうした情勢を踏まえて、本セミナーでは、最新の手口調査による自動車盗難の防止に関する課題や今後取り組むべき事項について、分かりやすく解説します。

登壇者

石垣 光 氏
（いしがき ひかる）

警察庁生活安全局
生活安全企画課
課長補佐

登壇者

加藤 学 氏
（かとう まなぶ）

加藤電機(株)
代表取締役社長

日本防犯設備協会 正会員
自動車オートバイ委員会
会員企業

一般社団法人 全国自動車
用品工業会（JAAMA）
理事長

登壇者

倉林 亮太 氏
（くらばやし りょうた）

(株)カーメイト
TE・SQグループ
プロダクトマネージャー

一般社団法人 全国自動車
用品工業会（JAAMA）
技術委員会副委員長

★★★日本防犯設備協会のYouTube専用チャンネルのご紹介★★★

ホームページ・会報誌とは異なる広報媒体として、YouTubeに専用チャンネルを作成して動画を使用した広報を強化しています。

いろいろな動画を掲載し、防犯・セキュリティ業界に興味を持っていただくと共に、安全安心まちづくりに役に立つよう頑張っています。チャンネル登録とグッドボタンを押して応援をお願いします。

1. チャンネル名　防犯のプロチャンネル
2. 作成者　広報分科会
3. 収録動画　86本（2025年12月現在）
セキュリティショー関連：47本
その他の紹介等　：39本

「防犯のプロ」チャンネルはこちらから