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）。

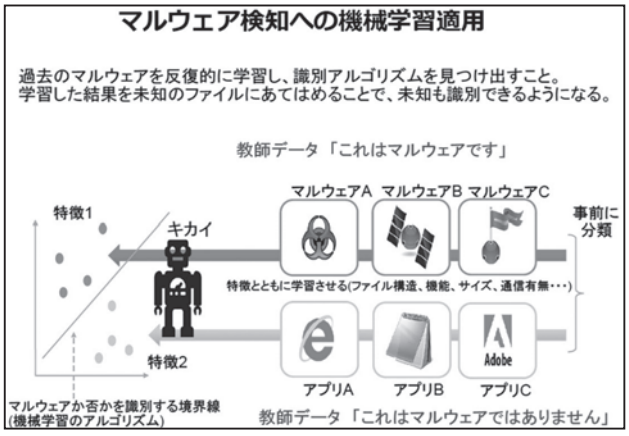

図1　機械学習を応用したマルウェア検知

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）。

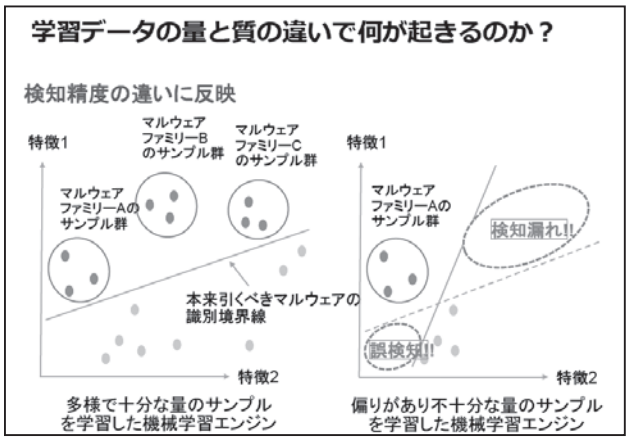

図2　精度向上に必要な学習データ量

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。

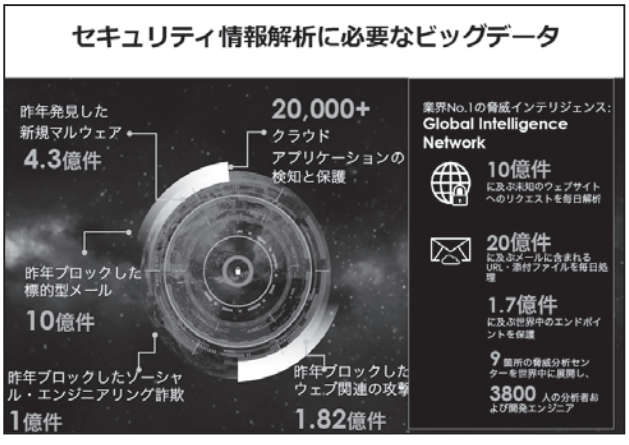

図３　セキュリティ対策に用いられるインテリジェンス

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。

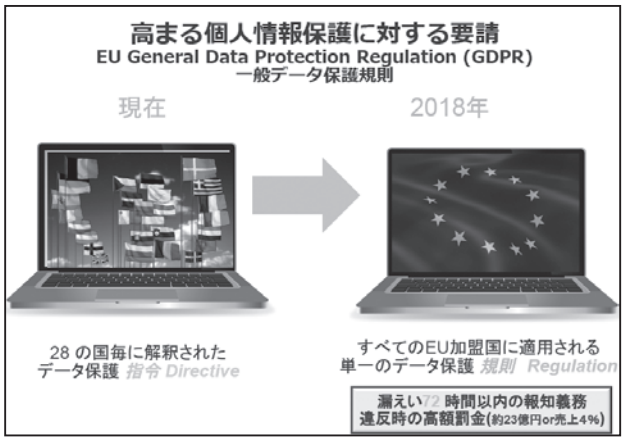

図 5 EU 一般データ保護規則の概要

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。

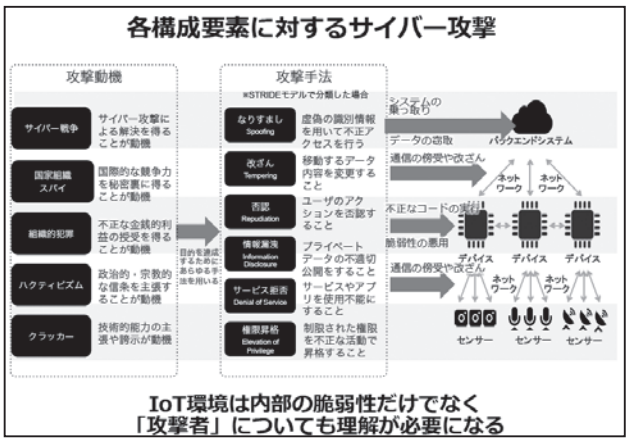

図 6　IoT 構成要素に対する攻撃手法と攻撃動機

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）。

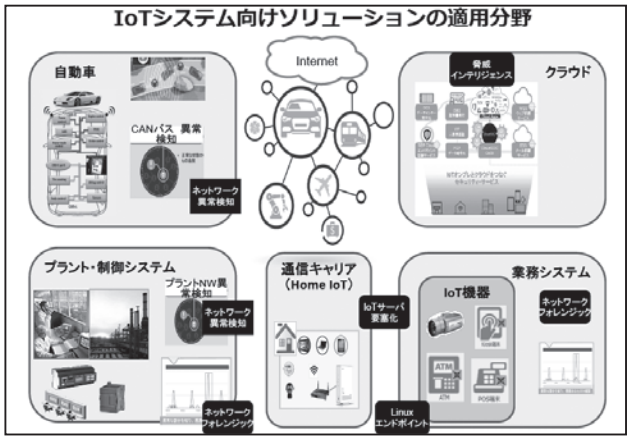

図 8　IoT セキュリティソリューションの適用分野

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）。

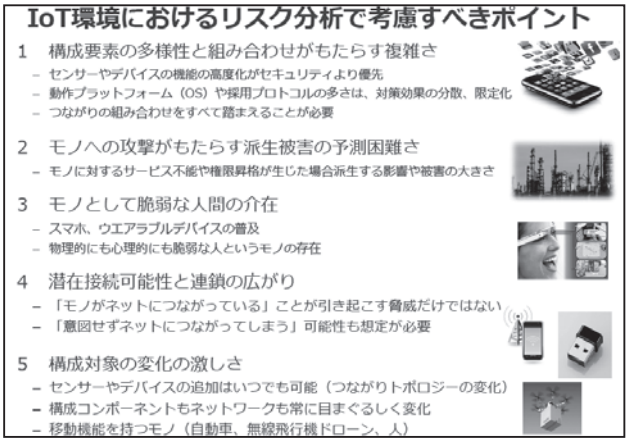

図９　IoT 環境におけるリスク分析の考慮点

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。