IoT 機器のライフサイクル全体をカバーする包括的セキュリティ対策

Comprehensive Security Measures Covering the Entire Life Cycle of IoT Devices

半 田　富 己 男

要　約　サイバー攻撃のターゲットが IT 機器から IoT 機器へと変容し，その攻撃の件数は増加の一途をたどっている．IoT 機器のサイバー攻撃対策は，IoT 機器のライフサイクル全体をカバーする包括的なソリューションであること，多層防御を提供すること，費用と時間のかかるプロセスを避けるために全自動のソリューションであること，が望ましい．この考え方を具現化するソリューションとして，大日本印刷は，IoT 機器の設計・開発段階から導入後まで，ライフサイクル全体を通じてセキュリティと信頼を提供するイスラエルの VDOO（ヴイドゥー）社の「IoT 機器の脆弱性対策ソリューション」に着目し，2019 年 4 月から VDOO 社と提携し，同社のソリューションを提供している．VDOO 社ソリューションは，開発段階で IoT 機器のファームウェアを分析し，その機器の構成に特化した脆弱性を視覚化，また製品リリース後の機器へのサイバー攻撃のモニタリングや保護までを一貫して行うものである．

Abstract　The target of cyber attacks has changed from IT devices to IoT devices, and the number of attacks has been continuing to increase. Cyber attack countermeasures for IoT devices should be 1) a comprehensive solution covering the entire life cycle of IoT devices, 2) providing multi-layered defense, and 3) fully automated to avoid costly and time-consuming processes. As a solution that embodies this concept, DNP focuses on Israeli VDOO's "IoT device vulnerability countermeasure solution", which provides security and trust throughout the life cycle from the design and development stage of the IoT device until after its deployment. In April 2019, DNP partnered with VDOO to provide VDOO solutions. VDOO solutions analyze the firmware of IoT devices at the development stage, visualize vulnerabilities specific to the device configuration, and consistently monitor and protect cyber attacks on devices after product release.

1. は　じ　め　に

あらゆるものがインターネットに接続される IoT（Internet of Things）時代が到来し，センサーネットワークと IoT を通じて集積されたビッグデータを AI が解析してフィジカル空間にフィードバックする Society 5.0 の実現に向かっている．他方，IoT 機器のセキュリティ対策が不十分な場合，IoT 機器へのサイバー攻撃が連鎖的に広範囲のフィジカル空間に及ぶリスクが増大している．こうした状況を受け，総務省と経済産業省は「IoT 推進コンソーシアム IoT セキュリティワーキンググループ」にて 2016 年 7 月に「IoT セキュリティガイドライン Ver1.0」を取りまとめて，IoT 機器メーカーやサービス提供者へのセキュリティ対策の五つの指針と一般利用者のためのルールを提示した[1]．その後も，2016 年 10 月にはボットネットマルウェア「Mirai」に感染してボットネット化した IoT 機器群を踏み台とした大規模な DDoS 攻撃が発生するなど，IoT 機器を悪用したサイバー攻撃の勢いは増すばかりである．総務省は

2019 年 2 月から，サイバー攻撃を受ける恐れのある IoT 機器を特定し，その利用者に注意喚起する取り組み「NOTICE（ノーティス）」を実施しており[2]，2020 年 4 月には IoT 機器の技術基準を改正し，①アクセス制御機能，② ID/パスワードの適切な設定を促す機能，③ファームウェアの更新機能，を具備することを義務付けることを計画している．しかし，IoT 機器は CPU やメモリ容量などリソースの制約が存在するため汎用的なセキュリティ対策の適用は難しく，機器メーカー自社内に専門セキュリティ人材を確保することも容易ではない状況である．

そこで，大日本印刷株式会社（以降，DNP）は，IoT 機器の設計・開発段階から導入後まで，IoT 機器のライフサイクル全体を通じてセキュリティと信頼を提供するイスラエルの VDOO（ヴイドゥー）社の「IoT 機器の脆弱性対策ソリューション」に注目し，VDOO 社と提携して同社ソリューションの日本市場への提供を開始した．本稿では，まず 2 章で IoT 機器の普及とセキュリティ上の課題について述べ，次に 3 章でサイバー攻撃のターゲットが IT 機器から IoT 機器へ変化してきたことと，実際に発生した IoT 機器をターゲットとしたサイバー攻撃事例を紹介する．4 章では，IoT 機器を狙ったサイバー攻撃による影響を軽減するための考え方を考察し，5 章で VDOO 社の「IoT 機器の脆弱性対策ソリューション」が提供するエンドツーエンドの IoT セキュリティプラットフォームを紹介する．

2. IoT 機器の普及とセキュリティ上の課題

本章では，まず IoT 機器の普及動向とそれがもたらす恩恵について述べる．次に IoT セキュリティの課題について整理する．

2. 1 IoT 機器の普及動向

本稿では，固有の IP アドレスを持ちインターネットに接続可能な機器（ただし，パソコンやスマートフォン等の IT 機器を除く）を IoT 機器と呼ぶことにする．従来はスタンドアロン環境で利用されていた機器が，ネットワーク接続されたスマートデバイス，すなわち IoT 機器へと変化してきている．これによって，機器製造者は自社製品の機能をネットワーク経由で容易に拡張することが可能となった．さらに，機器の保守メンテナンスも保守員を現地に派遣

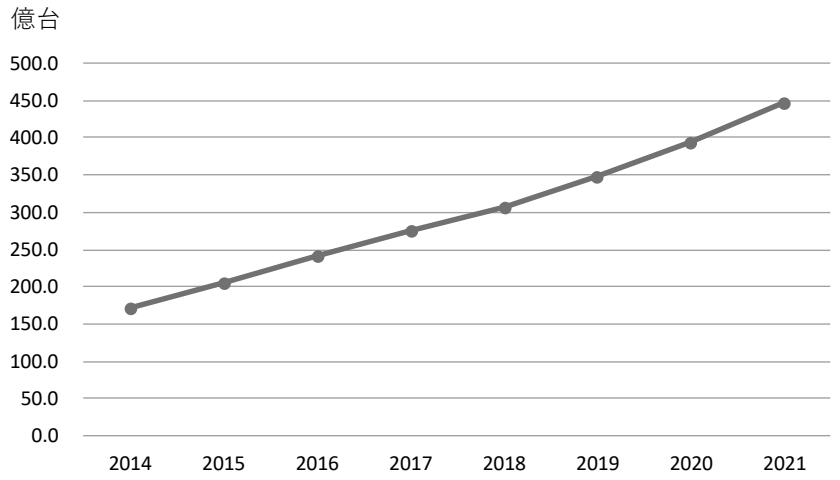

図 1　世界の IoT 機器台数の推移及び予測[*1]

することなく，リモートメンテナンスすることにより保守作業にかかるコストが削減された．IoT 機器によって集積されたビッグデータは，人工知能（AI）によって解析され，これまでにない新たな付加価値が生み出され，サイバー空間とフィジカル空間が高度に融合した Society 5.0 の実現に向けて IoT 化がさらに加速する好循環を迎えている．図 1 に世界の IoT 機器台数の推移及び予測[3]を示す．

2. 2　IoT セキュリティの課題

IoT 化の進展は，サイバー攻撃を仕掛ける攻撃者にとってもチャンスが拡がることになる．なぜならば，サイバー空間とフィジカル空間の融合が進み，フィジカル空間の物理的機器がスマートデバイス化することにより，これらの IoT 機器へのサイバー攻撃が現実社会へ直接的に大きなダメージをもたらすことになるからである．サイバー攻撃に備えて IoT 機器をセキュアに保つためには，いくつかの課題がある．

2. 2. 1　IoT 機器の多様性

一点目は IoT 機器の多様性である．一口に IoT 機器と言っても，末端のセンサーネットワークをクラウドに中継するためのゲートウェイや，監視カメラ，空調機器，医療機器，スマートファクトリーで動くロボット，コネクテッドカーなど，多種多様な機器がある．このため，これらの IoT 機器を構成する CPU やハードウェア・コンポーネント，OS やソフトウェア・コンポーネントは膨大な種類になり，包括的なセキュリティ対策は困難である．

2. 2. 2　IoT 機器の組み込みソフトウェアにおけるサプライチェーンの複雑化

二点目は IoT 機器の組み込みソフトウェアにおけるサプライチェーンの複雑化である．IoT 機器に組み込まれるソフトウェア・コンポーネントは，機器メーカーが自社開発したコンポーネントだけでなく，OSS（Open Source Software）や商用ソフトウェア・パッケージなどのサードパーティ製ソフトウェア・コンポーネントの利用が拡大している．サプライチェーンの複雑化・分業化が進む組み込みソフトウェア開発工程を経て，IoT 機器の最終製品に含まれているサードパーティ製ソフトウェア・コンポーネントの比率や脆弱性対策が確実になされているか，を正確に把握することは困難になっている．

2. 2. 3　既存の IT セキュリティソリューションを IoT 機器に適用する場合の課題

三点目は既存の IT セキュリティソリューションを IoT 機器に適用する場合の課題である．既存のエンドポイントセキュリティ対策製品の多くはパソコンやスマートフォンなどの IT 機器を指向しており，多くの場合 IoT 機器には対応していない．IoT 機器にも多く採用されている Linux OS を対象とした EDR（Endpoint Detection and Response）製品もあるが，リソースが限られている IoT 機器に IT 機器向け EDR 製品を搭載すると，IoT 機器の本来機能の動作が阻害される等の課題がある．

3.　IoT 機器へのサイバー攻撃事例

本章では，まずサイバー攻撃のターゲットが IT 機器から IoT 機器へ変化してきていることを述べ，次に，実際に発生した IoT 機器をターゲットとしたサイバー攻撃事例を紹介する．

3. 1　サイバー攻撃の進化，IT から IoT へ

従来のサイバー攻撃では，攻撃者は Windows OS を実行しているパソコンやサーバーに対して既知の脆弱性や未知の脆弱性（ゼロデイ）を悪用してサイバー攻撃を実行していた．

これに対して，マイクロソフトは Windows OS のセキュリティ対策を強化し，さまざまなセキュリティ・ソリューション・ベンダーも高機能のセキュリティ対策ソリューションを提供するようになった．このため，パソコンやサーバーといった IT 機器を狙ったサイバー攻撃を実行するためには，新たな未知脆弱性（ゼロデイ）を探索する等，攻撃者にとって難易度が上がり，攻撃に要する時間と費用が高くなった．

そこで，サイバー攻撃者はサイバー攻撃によって金銭を取得するという目的を達成するために，新たな方向を模索しなければならなくなった．その結果，サイバー攻撃の傾向として次の二つの方向性が顕著になっている．一つ目は，人間の弱点を突くソーシャル・エンジニアリングを駆使した攻撃で，ビジネスメール詐欺（BEC：Business E-mail Compromise）[4]に代表される．ビジネスメール詐欺（BEC）による被害は急増しており[5]，国際刑事警察機構（インターポール）も BEC に対する注意喚起キャンペーン #BECareful を展開している[6]．二つ目は本稿の主題である IoT 機器を狙ったサイバー攻撃である．IoT 機器は，管理が行き届きにくく，デフォルトの ID・パスワード設定のまま利用されているなど，セキュリティ設定に不備があるケースも多く，サイバー攻撃に狙われやすい特徴を持っている[7]．セキュリティ対策に不備がある IoT 機器は，マルウェアに感染しサイバー攻撃に悪用される恐れがあるため，総務省，国立研究開発法人情報通信研究機構（NICT）及び一般社団法人 ICT-ISAC は，インターネット・サービス・プロバイダ（ISP）と連携し，サイバー攻撃に悪用される恐れのある IoT 機器を調査し，利用者への注意喚起を行う取り組み「NOTICE（National Operation Towards IoT Clean Environment）」を 2019 年 2 月 20 日から実施している．2019 年度第 2 四半期までの実施状況[8]によると，これまでに約 1.0 億個の IP アドレスを調査し，そのうち ID・パスワードが入力可能であったものが約 98,000 件，実際にログインでき，注意喚起の対象となったものが延べ 505 件に達したとのことである．

3. 2　IoT 機器をターゲットとしたサイバー攻撃事例

これまでに実際に発生した IoT 機器へのサイバー攻撃の中で，現実社会に大きなインパクトを与えた事例を二件紹介する．

3. 2. 1　大規模 DDoS 攻撃を惹き起こした Mirai

一件目は感染させた IoT 機器群を攻撃者のリモート指令でコントロールできるようにボットネット化するボットネットマルウェア「Mirai」である．Mirai は，Linux ベースの IoT 機器であれば，ARM，MIPS，intel x86，PowerPC など様々な CPU アーキテクチャの IoT 機器に感染する能力を持つ．VDOO 社のリサーチャーによると，Mirai 及びその亜種は 100 万台以上の機器に感染し，さらに感染を拡大中という．

Mirai の名を有名にしたのは，2016 年 10 月 21 日に発生した DDoS 攻撃で米国の DNS サービス事業者 Dyn 社の DNS サービスが 2 回にわたって数時間ダウンし，Twitter や Netflix にアクセス障害が断続的に発生した事件である．これは Mirai に感染した IoT 機器のボットネットからの DDoS 攻撃とされており，最大で 1.2 テラ bps に達したとの報告もある[9]．

Mirai に感染した IoT 機器は周辺をスキャンして，新たに感染可能な IoT 機器を見つけると攻撃者サーバーにターゲット情報を連携し，感染を拡大していく．Mirai のソースコードはオープンソース化しており，GitHub から誰でもダウンロードできる状態になっているため，2017 年以降も現在に至るまで Mirai の亜種によるサイバー攻撃は進行中である．Mirai 亜種は 2017 年後半からは IoT 機器の脆弱性を悪用するようになり，より広範囲のボットネットを構築して DDoS 攻撃能力の向上を図っているとみられ，警戒が必要である．

3. 2. 2　産業制御システムをターゲットとする VPNFilter

二件目はウクライナで大規模感染が報告されたマルウェア「VPNFilter」である[10]．50 万台以上の機器（おもにルーターと NAS）に感染し，産業制御システム機器にも波及した．プログラムコードの特徴からロシアを拠点とする国家主導のサイバー攻撃者グループ Fancy Bear（別名 APT28）の関与が疑われている．産業制御システム機器固有のプロトコルである Modbus プロトコルを扱うためのプログラムコードを含んでいる．

ウクライナ政府の情報機関 SBU は，ウクライナの塩素蒸留プラントの制御システムと異常検知システムを標的とした VPNFilter によるサイバー攻撃を検知し阻止したと 2018 年 7 月 11 日に発表した[11]．文献[10]によると，法執行機関が攻撃者の C2 インフラストラクチャをダウンさせたことにより，攻撃は回避された．

VPNFilter は，一般的なユーザー名とパスワードで機器へのログインを試みるほか，既知の脆弱性を悪用して機器へ侵入しようとする．VPNFilter に感染した機器は，再起動しても VPNFilter を駆除できず，工場出荷状態へリセットしなければ除去できないほど持続性が強いマルウェアである．VPNFilter に感染した機器は，自機器の周辺ネットワークを偵察し，ネットワーク情報を攻撃者の Command & Control（C2）サーバーに伝えて次のコマンドを待つ．さらに，感染した機器群で Tor ネットワークを構築し，最終的な攻撃元を偽装する機能も備えているなど，重要インフラの産業制御システムをターゲットとした高度な機能を備えたマルウェアである．

4.　IoT 機器のセキュリティ対策の考え方

本章では，IoT 機器を狙ったサイバー攻撃による影響を軽減するための考え方を考察する．

4. 1　IoT 機器へのサイバー攻撃の軽減策：何に対して？

IoT 機器へのサイバー攻撃の軽減策を検討するため，まず攻撃者の動機について考察する．攻撃者の動機には，金銭目的，業務妨害，知的財産の侵害等の産業スパイ，政治的主張を発信するためのハクティビストと呼ばれる集団，国家レベルのサイバー戦争など様々な目的・動機が考えられる．最も一般的なサイバー攻撃者の動機は金銭目的である．

IoT 機器へのサイバー攻撃に使われるマルウェアは，Mirai の例に見られるようにソースコードが公開されていて亜種が次々に登場し続けている状況である．

次に IoT 機器利用者側の状況を見てみると，IoT 機器の多くは脆弱性が公表され機器メーカーがパッチを公開しても，運用上の理由等からパッチが適用されずに脆弱性を有したまま運用され続けている．IoT 機器の管理者インタフェースへのログイン認証においても，ID/パスワードがメーカー出荷時のデフォルト設定のままで使われていたり，ブルートフォース攻撃で

容易に破られるパスワードのまま使われていたりするケースも多い．IoT 機器の利用者は，まず第一に利用者認証の強度設定を確実に実施することから始めなければならない．

4. 2　IoT 機器へのサイバー攻撃の軽減策：どのように対抗するか？

IoT 機器へのサイバー攻撃対策を検討する際に機器開発者は，

1）自分が作製した機器に対して最もよくある攻撃を防ぐにはどうすればよいか？
2）自分が作製した機器に対する将来の攻撃を防ぐにはどうすればよいか？
3）未知の攻撃を防ぐための安全弁は何か？
4）セキュリティ対策が全て失敗した場合，どうすればネットワークを保護できるか？

などの課題を感じるであろう．これらの課題に対する主な防御ソリューションは，

1）セキュリティ対策のベストプラクティス，標準や規制，を参照する
2）機器を堅牢化する
3）ランタイムにおける防御策を講じる
4）ネットワークベースのソリューションを導入する

などが考えられる．

4. 3　IoT 機器へのサイバー攻撃の軽減策：何が必要か？

前節での検討結果から，IoT 機器へのサイバー攻撃対策に必要なソリューションの特性は次のようになる．まず，IoT 機器のライフサイクル全体をカバーする包括的なソリューションであること．次に，多層防御を提供し，SPOF（単一障害点）が残らないこと．また，費用と時間のかかるプロセスを避けるために，全自動のソリューションであることが望ましい．そして，IoT 機器開発者にとって，現在の開発体制のまま増員を要せずに導入できる実用的なソリューションであることが理想的である．

5.　エンドツーエンドの IoT セキュリティプラットフォーム VDOO（ヴイドゥー）について

DNP は，4 章で考察した IoT 機器のセキュリティ対策の考え方を具現化するソリューションとして，イスラエルの VDOO（ヴイドゥー）社の「IoT 機器の脆弱性対策ソリューション」に着目し，2019 年 4 月から VDOO 社と提携し，同社のソリューションを提供している．具体

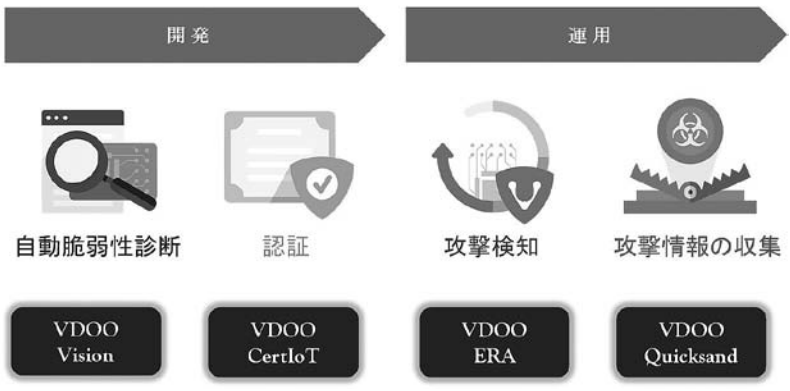

図 2　IoT 機器のライフサイクル全体をカバーする VDOO ソリューション

的には，開発段階で IoT 機器のファームウェアを分析し，その機器の構成に特化した脆弱性を視覚化，また製品リリース後の機器へのサイバー攻撃のモニタリングや保護までを一貫して行うソリューションである．本章では，VDOO 社のソリューションについて紹介する．VDOO 社ソリューションは，図 2 に示すように IoT 機器の設計・開発段階から導入後まで，IoT 機器のライフサイクル全体を通じてセキュリティと信頼を提供する．2019 年 12 月時点で，VDOO 社ソリューションが対応している OS は，Linux と Android と FreeRTOS である．VxWorks 等のリアルタイム OS についても順次サポートしていく予定である．CPU のアーキテクチャは，MIPS，ARM，Intel x86_64 に対応している．

5. 1　IoT 機器のセキュリティ解析自動化プラットフォーム VDOO Vision

IoT 機器や組み込みシステムは，設計・開発時にネットワーク接続やサイバーセキュリティを考慮して開発されていないケースではサイバー攻撃者が容易に侵入できる．しかし，さまざまな IoT 機器は，その特性（メモリ，ストレージ，CPU など限られたリソース）が機器によって異なるため，個々の IoT 機器に必要なセキュリティ要件を特定し，セキュリティ対策を実装することは容易ではない．

VDOO Vision は，IoT 機器のセキュリティ対策状況を分析し，セキュリティ上の欠陥を修正するためのガイダンスを提供してくれるセキュリティ解析自動化プラットフォームである．VDOO Vision は，ソフトウェア部品解析（SCA：Software Component Analysis）ツールや静的アプリケーション・セキュリティ・テスト（SAST：Static Application Security Test）ツールが持つ機能に加え，分析対象機器に必要なセキュリティ要件とその要件への対応状況，組み込まれているソフトウェア・コンポーネントの脆弱性に関する詳細なレポートを提供する．VDOO Vision の分析レポートには，セキュリティ要件とソフトウェア・コンポーネントの脆弱性について，影響度に応じた優先順位をつけたうえ，修正案も示される．

5. 1. 1　VDOO Vision の分析プロセス

IoT 機器のセキュリティ分析を行うには，分析対象機器のファームウェア・バイナリファイルを，クラウド上の VDOO プラットフォームへアップロードすればよい．ソースコードの提供は不要である．分析対象機器のファームウェア・バイナリファイルをアップロードすると，VDOO プラットフォームのファームウェア・ハンドラーがアップロードされたバイナリを分析し，ハードウェア・コンポーネントとソフトウェア・コンポーネントを分類および抽出する（図 3）．

図 3　VDOO Vision の分析プロセス

次に，VDOO プラットフォームの Taxonomy Engine が，分析対象機器のハードウェア・

コンポーネントとソフトウェア・コンポーネントに応じて，分析対象機器に必要なセキュリティ要件を導出し，セキュリティアウトラインを作成する（図 4）．そして，具体的なセキュリティギャップを特定するためにバイナリコード・スキャナーが詳細な分析を行い（図 5），それらを修正する方法についてステップバイステップで示したガイダンスをユーザーに提供する．

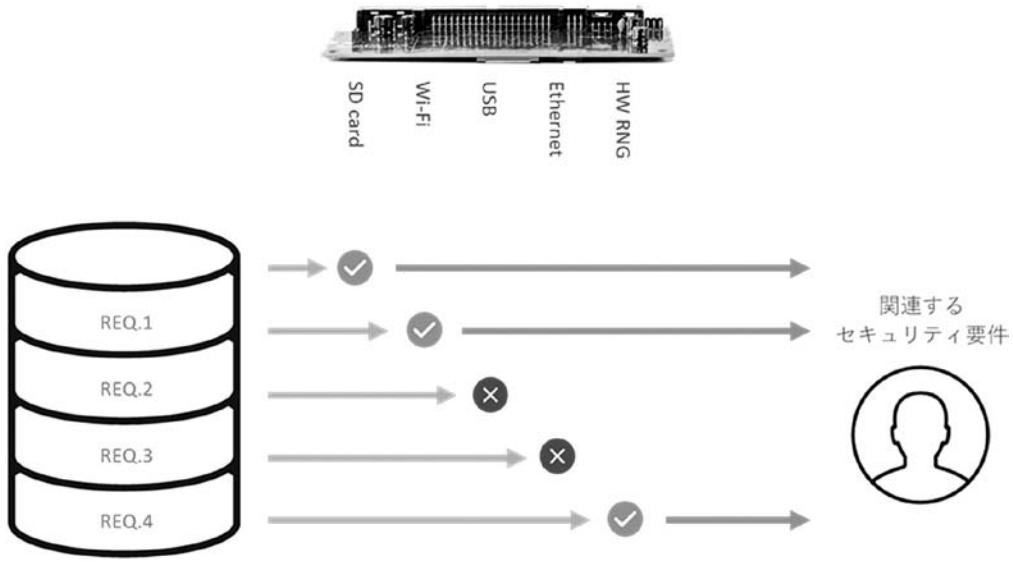

図 4　Taxonomy Engine が必要なセキュリティ要件をフィルタリング

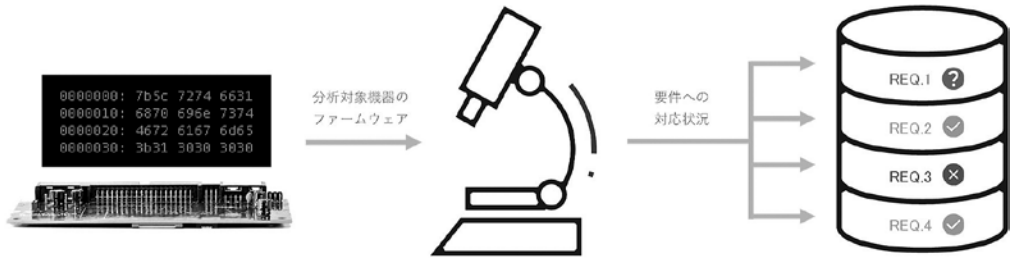

図 5　セキュリティ要件への対応状況をスキャン

VDOO Vision は，VDOO 社が蓄積した 1,000 個以上のセキュリティ要件の中から，分析対象機器のハードウェア構成とソフトウェア・コンポーネント構成に応じて，必要なセキュリティ要件を導出し，要件への対応状況をスキャンする．各セキュリティ要件には，NIST，ENISA，CCDS，IEC 62443 等のセキュリティ規格・ガイドラインの該当項目へのリンクがつけられているため，これらのガイドラインへの準拠を目指した製品開発にも有効である．

5. 1. 2　VDOO Vision の分析レポート

分析対象機器のファームウェア・バイナリファイルを，クラウド上の VDOO プラットフォームへアップロードしてから数十分から 1 時間程度で，VDOO Vision レポートが作成され，ユーザーは WEB ブラウザーから VDOO プラットフォームにアクセスしてレポートを見ることが

できる．

VDOO Vision 分析レポートには，分析対象機器のハードウェア・コンポーネント部品表（BOM：Bill of Material）とソフトウェア・コンポーネント部品表（Software BOM），必要なセキュリティ要件とその対応状況，ソフトウェア・コンポーネントについて既知の脆弱性（CVE 情報）などが示される．ソフトウェア・コンポーネントについては，OSS のライセンス情報も提供される．

セキュリティ要件とソフトウェア・コンポーネントの脆弱性については，影響度に応じた優先順位をつけたうえ，修正方法ガイダンスも示される．セキュリティ要件は，欠陥のあるアーキテクチャ，誤った構成，バックドア，セキュリティ基礎要素の欠落，等の観点で分析され，問題が発見された箇所の具体的な場所や，修正方法に関する詳細なガイダンスがレポートに示される．さらに，コマンドインジェクションに悪用される可能性がある脆弱性と疑われる箇所も指摘されるので，開発者にとって，さまざまなセキュリティ上のギャップを埋めるための手助けになる．

5. 2　オンデバイス・セキュリティ・エージェント VDOO ERA

製品として出荷後の IoT 機器に組み込んで，リアルタイムにモニタリングし，サイバー攻撃への多層防御を提供するエージェントが VDOO ERA である．VDOO ERA のエージェントは，VDOO Vision でファームウェアを分析する過程で，その機器に合わせて自動的に誂えられる専用エージェントである．このため，多層防御機能を備えながらもフットプリントは小さく，CPU のオーバーヘッドは 1% 未満，ストレージのオーバーヘッドは 1MB 未満であり，対象機器の本来の機能を阻害しないことが特徴である．なお，VDOO Vision と VDOO ERA は独立したサービスなので，VDOO ERA だけを利用することも可能である．

5. 2. 1　VDOO ERA の機能

図 6 に VDOO ERA の機能を示す．まず，攻撃者が脆弱性を悪用するエクスプロイトで初期侵入を試みるリモートコード実行，いわゆるファイルレス攻撃から防御する．次に，ホワイトリスト方式による防御である．対象機器を構成するファイルシステム，実行プログラム，構成ファイルの一覧は VDOO Vision でファームウェアを分析する過程で得られているので，ホワイトリストが自動的に生成されている．ファイル，プロセス，構成ファイルについて，ホワイトリストに無いものが導入されたり，ホワイトリストに保護対象として登録されているファイルに対する改変・削除の試みは阻止される．さらに，暗号資産（仮想通貨）をマイニングするマルウェアに感染すると，CPU やメモリのリソースが異常に消費されるので，リソース消費をモニタリングしている．ネットワーク面の防御機能も備えており，マルウェアに感染して攻撃者の C2 サーバーとの通信路が開設されたり，ファイアウォール設定が改変されたりするとこれを検知・防御する．

VDOO ERA は，VDOO Vision によるファームウェア分析の過程で自動的に生成されるが，図 6 に示す上述の諸機能について GUI 画面からパラメータをカスタマイズして生成することができる．各種防御機能について，攻撃イベントを検知したときに攻撃を阻止するか，アラート警告のみにとどめるか，といったポリシーも自由に設定できる．イベントを検知したアラートは，機器内ローカルのログファイルに記録されるが，Syslog 機能を搭載した機器であれば

外部のログ管理サーバーにアラートログを送信することも可能である．

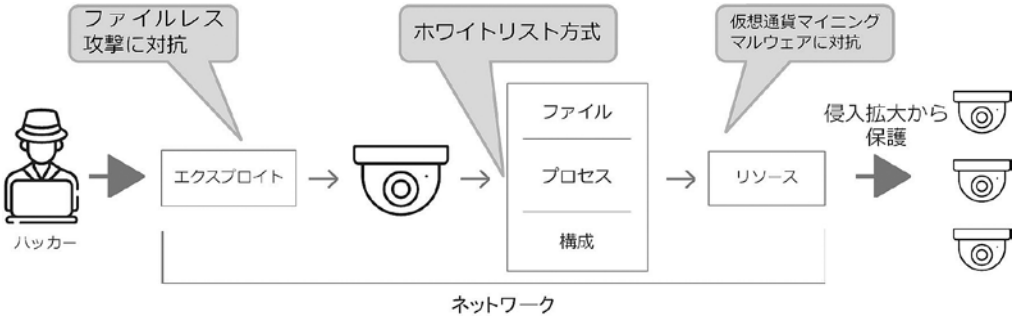

図 6　VDOO ERA の機能

6. お わ り に

サイバー攻撃のターゲットが IT 機器から IoT 機器へと変容してきたことを踏まえ，IoT 機器のサイバー攻撃対策の在り方を考察した．IoT 機器の設計・開発段階から導入後まで，IoT 機器のライフサイクル全体を通じてセキュリティと信頼を提供するイスラエルの VDOO（ヴイドゥー）社の「IoT 機器の脆弱性対策ソリューション」が提供するエンドツーエンドの IoT セキュリティプラットフォームを紹介した．IoT 機器のセキュリティ対策ソリューションを検討している読者に対し，本稿が有益なものとなれば幸いである．

最後に，本稿執筆にあたりご協力・ご指導いただいた全ての皆様に深く感謝し，御礼申し上げます．

＊ 1　出典：参考文献[3]，令和元年版 情報通信白書　図表 1-2-1-3「世界の IoT デバイス数の推移及び予測」を基に筆者が作成．

参考文献
［1］ IoT セキュリティガイドラインを策定しました，経済産業省，2016 年 7 月 5 日，https://www.meti.go.jp/press/2016/07/20160705002/20160705002.html
［2］ IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施，総務省，2019 年 2 月 1 日，https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html
［3］ IoT デバイスの急速な普及，情報通信白書　令和元年版，総務省，2019 年 7 月，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd112120.html
［4］IPA セキュリティセンター，【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口，最終更新日 2018 年 8 月 27 日，https://www.ipa.go.jp/security/announce/20170403-bec.html
［5］ Lee Mathews,「ビジネスメール詐欺」の被害額は年間 1.4 兆円，FBI が警告，Forbes Japan，2019 年 5 月 8 日，https://forbesjapan.com/articles/detail/27057
［6］ INTERPOL，“INTERPOL urges public to #BECareful of BEC fraud”，2019 年 10 月 9 日，https://www.interpol.int/News-and-Events/News/2019/INTERPOL-urges-public-to-BECareful-of-BEC-fraud
［7］ 高橋睦美，攻撃ターゲットは IT から IoT へ―― NICTER，13 年の観測の歴史に見る変化とは，@IT，2018 年 12 月 11 日，https://www.atmarkit.co.jp/ait/articles/1812/11/news014.html
［8］ 脆弱な IoT 機器及びマルウェアに感染している IoT 機器の利用者への注意喚起の実施状況（2019 年度第 2 四半期），総務省，国立研究開発法人情報通信研究機構，一般

社団法人 ICT-ISAC，2019 年 10 月 25 日
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00043.html
［9］ Scott Hilton, “Dyn Analysis Summary Of Friday October 21 Attack”, Dyn Company News，2016 年 10 月 26 日
https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
［10］“VPNFilter の大惨事回避から 1 年”，TALOS Japan，Cisco Japan Blog，2019 年 6 月 13 日
https://gblogs.cisco.com/jp/2019/06/talos-one-year-later-vpnfilter-catastrophe/
［11］“サイバーセキュリティ アニュアルレポート 2019”，NTT-CERT，NTT セキュアプラットフォーム研究所，2019 年 6 月，p.46
https://www.ntt.co.jp/sc/media/NTTannual2019_j_web_lock.pdf

※上記参考文献に記載の URL のリンク先は，2020 年 1 月 7 日時点での存在を確認

執筆者紹介　半 田　富 己 男（Fukio Handa）

1988 年大日本印刷(株)入社．情報システム部門を経て，研究開発部門で IC カード OS への公開鍵暗号アルゴリズム実装の研究に従事．その後，IT セキュリティ評価及び認証制度（JISEC）認定評価機関に出向し，CC 評価業務に従事．認証技術及び PKI 関連技術の研究業務を経て，2015 年からサイバーセキュリティ事業に取り組んでいる．CISSP.