IoT へのサイバー攻撃仮想ストーリー集

Vol. 1　2017 年 8 月 1 日

一般社団法人　日本クラウドセキュリティアライアンス（CSA ジャパン）
IoT ワーキンググループ

内容

はじめに

IoT （Internet of Things）という言葉は、毎日のように新聞に紙面をにぎわすようになりました。あらゆるモノをネットワーク化し、さらに、それ単独では実現できなかった付加価値の創出や、まったく違った発想からの利用を可能にする IoT は、ビッグデータの応用や AI（人工知能）の発展にも支えられて、様々な分野で開発や応用が進められています。

その一方で、ネットワーク機能を持った機器が標的となるサイバー攻撃が近年激増するなど、新たなリスクも生じています。CSA ジャパン IoT ワーキンググループ（IoT WG）では、こうした IoT のリスクに対応するセキュリティ対策について、CSA グローバルの IoT WG とも連携しつつ、CSA 英文ガイダンス文書の日本語訳の提供や、日本独自の検討とその成果の発表等の活動を行っています。

このドキュメントは、IoT のカテゴリーに属するシステムに対する仮想の攻撃シナリオ集です。日々、新たな技術が生み出されている IoT の領域では、脅威も日々変化します。新たな脅威に対して後手にまわりがちなセキュリティ対策を、脅威を予測することで、少しでも先回りできるようにしようというのが、このシナリオ集の目的です。

各シナリオには、IoT に関するセキュリティインシデント発生のストーリーと、その影響、原因と推奨される対策が含まれます。読者は、このシナリオを読む中で、自らが開発している、もしくは開発しようとするシステムを念頭に、類似のインシデントが発生する可能性を考え、必要な対策を知ることができます。

今回、リリースしたシナリオには、リスクの高い用途に使われるシステムだけでなく、コンシューマ向けのシステムのような一見無害と思われるものも含まれています。一方、脅威については高いレベルのものを想定しており、一見無害に見えるシステムが、想定外の使われ方をする可能性も示唆するものとなっています。

一見、荒唐無稽に思われる内容も多いですが、現実には、そうした「ありえない」事態が生じた例も過去にはあり、実際に対策を行うかどうかは別にしても、可能性を知っておくことは意味のあることだと考えます。CSA ジャパン IoT WG では、今後、さらに多くのシナリオを追加していく予定です。

CSA ジャパン IoT ワーキンググループ　リーダー
二木　真明

シナリオ集執筆メンバー

阿賀 誠
小野寺　正
勝見 勉
上村 竜也
新宮 貢
鶴田 浩司
二木 真明
山崎 英人
山下 亮一
（50 音順）

編集　二木真明

レビュー：CSA ジャパン IoT WG 有志

A1. 家電製品の乗っ取りによる DDoS 攻撃

ある国際的なスポーツイベント当日、イベントの Web 情報サイトや、メディアセンターのインターネット回線が使えなくなる障害が発生した。調べてみると、日本国内の非常に多数の IP アドレスから、DDoS 攻撃が発生し、ISP の回線すら飽和させる量のトラフィックが発生していた。また、攻撃の一部は DNS を標的としており、DNS 障害のため、広範な Web 上のサービスのアクセス不能、メールの不達などの影響も出た。攻撃元 IP アドレスの多くは、国内の主要な ISP の加入者に対し動的に割り当てられたもので、広い地域に分散しているため、個別対処が困難となった。発生から数時間の後、ISP は、監督官庁の指示でやむなく家庭向けを中心に加入者の利用を一時的に停止させたが、これによる社会的影響は多大で、復旧のメドもたたず、インターネットが生命線の ISP とビジネスユーザに多大な経済的被害をもたらすことになった。後日、調査の結果、家庭内にある複数のインターネット家電製品が DDoS 攻撃の発信元と判明した。

【影響】

大量のコンシューマ機器が乗っ取られ、攻撃に悪用されることで、ネットワークインフラに対して重大な被害を与える。これにより、インターネットを使用したあらゆるサービスが影響を受け、大きな社会的混乱につながる。また、一旦乗っ取られた機器の復旧は容易ではなく、メーカーにとっては大きなダメージとなる可能性が高い。

【原因】

調査の結果、家電製品へのマルウエア感染、ファームウエア改ざんなど複数の原因が判明した。

攻撃者は家電製品の解析により、ファームウエアの動作とメーカーサービスサイトへの通信経路を把握し、その脆弱性を把握。脆弱性を利用してメーカーサイトに侵入し、改ざんしたファームウエアを一斉配布した。この方法で改ざんされたデバイスは、以降、メーカーサイトからのソフトウエア更新などは一切できなくなってしまった。

一部の製品は、UPnP を使用したサービスに脆弱性があり、家庭用ルータを経由して外部から攻撃可能な状態にあった。これらの製品は、外部から攻撃を受け、不正コードをリモート実行させられてしまった。

一部の家庭では、スパムメールに添付されたマルウエアに PC が感染。この PC が、ネットワーク内の家電製品を探して、脆弱性を攻撃した。不要なサービスが起動していて、なおかつそのサービスに脆弱性があった機器は、かなりの部分が侵入を許し、不正なプログラムを埋め込まれた。スパムメールは家電メーカーを騙った物で、複数のメーカーのものが確認された。それぞれに、そのメーカーの家電製品攻撃に特化したマルウエアが添付されていた。

問題点としては、以下のような点が挙げられる。

①機器を統括するメーカーのサービスサイトに攻撃者が侵入できる脆弱性が存在した。また、侵入可能なサーバに、機器に配布するファームエアが容易に発見できる形で置かれていたこと。

②攻撃者は機器のファームウエアを機器内のメモリーから読み出すことができ、それは容易に解析が可能だったこと。またファームウエアとサービスサイトの間の通信の大半が暗号化されておらず、モニタリングすることで様々な情報を得られたこと。

③機器が改ざんされたファームウエアや、マルウエアを受け入れてしまったこと

④機器のファームウエアが Linux 等の汎用 OS を基盤としており、脆弱性や不要なサービスが残っていたこと

⑤家庭内 LAN を過信し、PC 等を経由した攻撃を想定していなかったこと

【対策】

①製品とサービスの安全対策

・家電製品におけるファームウエアのリバースエンジニアリング抑止。たとえば、ファームウエアの難読化などによる解析作業の困難化。
・ファームウエア改ざんの防止。たとえば、パッケージへの電子署名と製品内のチップに保存された公開鍵による検証など。
・サービスサイトのセキュリティ強化。多数の製品を統括、管理するサイトは、高度な攻撃を受ける可能性が高く、リスクレベルは非常に高いという認識が必要。防御しきれない前提で、侵害の発見と対応を念頭においた対策が重要。

②UPnP を含む外部接続のセキュリティ強化

・UPnP 実装の脆弱性対策。発見された脆弱性が早期に修正されるような更新方法の実装。
・サービスポート開放の是非の再検討。安易に外部からのアクセスを受け付けるのではなく、内部側からのアクセスでサービスを行う方法を検討すること。

③PC 等のマルウエアからの攻撃対策

・DLNA 機能へのアクセス制御の強化。PC などネットワーク上のコンピュータからのアクセスは利用者が明示的に許可するまで禁止すること
・機器のシステムに汎用 OS を使用する場合、必要なサービス以外を確実に停止させ、かつファイアウォール機能を有効にして、外部からの不要なアクセスを、すべて遮断すること
・機器のファームウエアの脆弱性、とりわけ汎用ソフトウエアに含まれる脆弱性を確実に修正できるようなアップデート手段を実装すること

A2. 病院システムへのマルウエア感染

ある病院で、長時間の手術中に、手術室の室温が異常に上昇するという現象が発生した。幸いにも、手術は無事に終了したが、患者を集中治療室に運んだ直後、今度は重要な医療機器が接続されたネットワークに障害が発生し、患者のバイタル等の監視ができなくなった。調査したところ、モニタリングや機器の管理を遠隔で行うための PC やサーバにマルウエアが感染し、それらから大量のポートスキャンがネットワーク内に発生していた。これにより、ネットワークに接続された一部の医療機器がダウンしたり、異常動作を起こしたりしていたことが判明した。さらに、空調システムで、環境センサーの情報を集中管理するための機器にもマルウエア感染が発見され、温度や湿度を正常に計測できなくなっていた。これらのネットワークはインターネットから隔離されていて、PC やサーバに対する USB メモリーなどの接続はできなくなっていたため、マルウエアの侵入原因は不明だった。

【影響】

病院の重要な医療システムや環境システムに障害をもたらすことで、最悪の場合、患者の生命を危険にさらす可能性がある。また、病院の事務系システムがマヒすれば、その運営に大きな支障を生じる。

【原因】

実は、この日入院患者の一人が、持ち込んだ PC を病室の隅にあった LAN コネクタに接続した。当人は、インターネットへのアクセス手段を持ち合わせておらず、接続すればインターネットに出られるのではないかと考えたらしい。このネットワークはインターネットには接続できなかったが、DHCP により自動的にアドレスが付与される。たまたま、その患者の PC にはマルウエアが感染しており、それが、LAN 内の PC やサーバの脆弱性を利用して感染を広げていった。

問題点としては以下のようなことが挙げられる。

①LAN コネクタがむき出しになっており、接続制限も行われていなかった。
②LAN 内の PC、サーバに対してセキュリティパッチが適用されていなかった。また、医療機器メーカーが提供したサーバの中には、Windows の Administrator アカウントのパスワードがデフォルトのままだったものがあった。
③一部の医療機器はポートスキャンなど、想定外のネットワークアクセスにより異常をきたした

④の空調センサー管理ユニットは Linux ベースのシステムで、不用意に telnet サービスが起動しており、root ログインが可能だった。root パスワードはデフォルトのままで、admin だった

【対策】

①LAN コネクタに対する不正接続防止
・鍵付きカバーの設置などの物理的な保護を行うこと。
・認証スイッチなどによる機器認証、DHCP の MAC アドレスによる制限、その他、不必要な接続を防止する措置の実装。

②確実な脆弱性対策とアクセス管理
・インターネットに直接接続されないネットワークであっても、アップデート用サーバなど脆弱性がタイムリーにアップデートされるような仕組みやその運用手順を導入すること。
・サーバ特権アカウントへのリモートアクセスを制限し、デフォルト（ビルトイン）特権アカウントは可能な限り無効化しておくこと。

③誤動作の防止
・ネットワーク接続される機器は、その設計段階で想定外の着信に対する誤動作を防止する措置を組み込むこと

④不要なサービスの停止
・特にシステムに汎用 OS を使用する場合、必要ないサービスはすべて停止させること。
・ファイアウォール機能を有効にし、外部からの不必要な接続をすべて遮断すること。
・外部からの接続が不可欠な場合は、可能な限り接続元を IP アドレス等で制限し、与える権限は必要最小限のものに制限すること。

A3. 監視カメラシステムの画像流出

ある重要施設内に設置されている複数の監視カメラの画像とみられる動画がインターネット上に流出していることが判明した。鮮明な動画は施設内の人員やその活動内容の特定も可能で、施設の安全を確保する上で秘匿されるべき多くの情報が含まれていた。

監視カメラのネットワークはインターネットから完全に分離されており、当初は内部犯行や管理サーバへのマルウエア感染等が疑われたが、いずれも確認することはできなかった。施設の管理組織は疑心暗鬼の状態となり、警備員を増員したり、セキュリティルールを厳しくしたりするなど従業者にも多くのストレスがかかったため、中期的に業務にも悪影響が出ることになった。

【原因】

施設内の監視カメラの多くに、マルウエアが感染していた。一部の監視カメラには他のカメラから転送されたとみられる動画が複数確認された。動画が発見された監視カメラはすべて無線 LAN 接続であり、電波の到達範囲には、一般の無線 LAN アクセスポイントが存在した。マルウエアによって接続先の無線 LAN を変更され、インターネットへの通信が可能になったと考えられた。また、メンテナンスに使用するため、一般の LAN にも接続されることがあるノート PC にマルウエア感染が見つかった。マルウエアが収集したとみられる情報の痕跡もあり、この情報は PC が一般の LAN に接続された段階で送信された形跡があった。監視カメラメーカーのダウンロードサイトの一部ページに改ざんの痕跡が見られ、メンテナンス用 PC はこの改ざんによりマルウエアに感染したと考えられる。

①監視カメラの脆弱性。telnet サービスや VNC サービスが動作しており、root アカウントの直接ログインが可能な上、そのパスワードは password であった。

②無線 LAN 接続の監視カメラ。一部の監視カメラは設置場所の都合で無線 LAN 接続となっていた。アクセスポイント側は十分なセキュリティ対策を行っていたが、カメラ側は接続先のアクセスポイントが正当なアクセスポイントかどうかの確認手段を持っていなかったため、偽のアクセスポイントに誤って接続してしまう可能性があった

③管理サーバは Windows の古いバージョンで、セキュリティ更新も行われていなかった。

④メンテナンス用 PC に感染したマルウエアは、監視カメラネットワークに接続された際、

そのネットワークを探索し、脆弱なサーバにマルウエアを感染させた。サーバに感染したマルウエアは、ネットワーク内にあるカメラのアドレス、ファームエアバージョン、通信方式などの情報を収集し、無線 LAN 接続のカメラに対して、telnet サービスから侵入し、制御用のマルウエアに感染させた。その後、メンテナンス PC が再度接続された際に、収集した情報を転送し、サーバ内のマルウエアは痕跡も含めて自己消滅した。この過程は何度か繰り返された。

⑤カメラに感染したマルウエアは、他のカメラを攻撃して感染を広げると同時に、無線 LAN の電波状況を調べ、一部のカメラの周辺で外部へ接続が可能なネットワークが存在することを確認した。

⑥監視カメラシステムは警備室で監視されていたが、少数のモニタでカメラを切り替えて表示するようになっていたため、このシーケンスが改ざんされて一部のカメラが表示対象外になっていたことに監視員は気づかなかった。データはその間に外部の無線 LAN を経由して送信された可能性が高い。

⑦メンテナンス用 PC,無線 LAN など複数の外部通信手段を攻撃者は確保して、適宜使い分けていた。放置すれば、さらに内部無線 LAN のアクセスポイント機器等が乗っとられ、永続的な外部接続を構築されてしまうといったシナリオも考えられる。

【対策】

①不要なサービスの停止とアクセスの管理
・特にシステムに汎用 OS を使用する場合、必要ないサービスはすべて停止させること。
・ファイアウォール機能を有効にし、外部からの不必要な接続をすべて遮断すること。
・外部からの接続が不可欠な場合は、可能な限り接続元を IP アドレス等で制限し、与える権限は必要最小限のものに制限すること。
・外部アクセス可能なアカウントに与える権限は最小化し、パスワード認証を行う場合、パスワードは適切な強度のものを設定すること。

②無線 LAN 利用時の安全管理
・重要機器のネットワーク接続にあたっては、通信障害の防止なども念頭に、有線方式の利用を検討すること
・無線 LAN を重要機器に使用する場合、WPA2/IEEE802.11i など脆弱性がない方式を使用すると同時に、AP、機器相互の認証を確実に行うこと。

③確実な脆弱性対策とアクセス管理
・インターネットに直接接続されないネットワークであっても、アップデート用サーバなど脆弱性がタイムリーにアップデートされるような仕組みやその運用手順を導入すること。
・サーバ特権アカウントへのリモートアクセスを制限し、デフォルト（ビルトイン）特権アカウントは可能な限り無効化しておくこと。

④保守用 PC,機器によるマルウエア持ち込み防止
・重要なネットワークに対し、保守用 PC や外部記憶装置など、外部のネットワークへの接続履歴がある機器を接続する際は、マルウエア持ち込みなどのリスクを考慮し、事前のチェックを徹底すること
・特に重要なサーバ等には、セキュリティソフト等を導入すると同時に、不正なアクセスを監視、発見する仕組みの導入などを検討すること

⑤機器間のセパレーションと電波漏洩防止策の実施
・マルウエア感染や不正アクセスのリスクがある機器は、他機器との不要な通信ができないような措置（無線 LAN のプライバシーセパレータ機能や、スイッチのポート間通信禁止など）を検討すること
・重要な機器に無線ネットワークを利用する場合、構外への電波漏洩や構外からの電波混入などを防止する措置を検討すること

⑥重要機器の接続監視
・重要な機器については、ネットワーク監視システムによる稼働監視など、動作異常を検出するしくみの導入を検討すること

⑦定期的なチェック
・重要なネットワークに設置されたネットワーク機器などについては、コンフィグレーションの不正変更などがないことを定期的に確認すること
・重要なシステムの保守用 PC 等はできる限り専用のものを使用し、定期的に不審なソフトウエアやファイルがないかどうかを確認すること

A4. ビル・エネルギーマネジメントシステム（BEMS）への攻撃

国際的なスポーツイベントを契機に東京はスマートシティを構築、政府の掲げるリソースアグリゲーションの先駆けとして、スマートグリッドによる電力需給バランスの制御を開始していた。大都市におけるスマートグリッドは、一つの街とも言えるビルの電力マネジメントと不可分である。主要なビルには、蓄電装置や屋上、壁面の太陽光発電、コージェネレーションシステムなどが配置され、ビルの電力制御システムを介して地域の配送電網とリンクし、地域全体の電力需給を調整している。当然ながら、新たにに建設されたスポーツ施設や選手村、メディアセンターなどの関連施設も、こうした枠組みの中に組み込まれていた。

真夏のある日、イベントの中盤、競技場、選手村施設や都内の大規模商業ビル複数で、原因不明の停電が断続的に発生。選手村や競技施設ではエレベーターが動かない、建物の扉が顔認証システムの停止により入館出来ない、入場ゲートや空調設備が動かないなどといったトラブルに発展した。

【影響】

競技では選手村から競技場への移動に遅れる選手が続出、競技場の停電などにより大会のスケジュールが大きく狂った。また競技場では、その影響でトラブルが頻発し、観客や選手の混乱は長時間続くこととなった。国際競技団体はこの事態を問題視して、日本に対し、ただちに原因の究明と報告を要求する声明を発表、日本の大会運営が問われる問題に発展した。影響は競技関連施設のみならず、複数の大規模ビルにも広がって、ビジネス活動にも大きな影響が出た。この件では国際的な批判を受けて大会組織委員長が開催期間中に辞任、都知事は責任を取って自ら減俸処分を課した。大会組織委員会も社会的な批判にさらされ、障害を発生したシステム導入の監督責任を国会で追及される事態となった。

【原因】

調査の結果、これらの施設やビルの集中管理を請け負っているビル管理会社の制御ネットワークで用いられている機器やコンピュータの一部が定期メンテナンス直後から、マルウエアに感染していたことが判明。これらは保守を担当する委託先による作業時に混入したものと考えられた。これらの機器の多くは導入から数年間、ソフトウエアが更新されておらず、多くの脆弱性や不必要なサービスが起動されているといった問題を抱えていた。このため、そうした切り口で攻撃されマルウエアの侵入を許したと考えられる。

対応に手間取った原因は、各機器がマルウエアによって異常動作を起こしたことを認識できず、電力会社との間でのやりとりに時間をとったことだろう。実際、ビル管理会社の管理用ネットワークと社内ネットワークの接点にあるファイアウォールで、管理ネットワーク側からの異常な通信を IT 部門が委託している SOC 事業者が検知したが、現場と IT 部門間の連絡体制の問題から、現場が問題を認知するまでに多くの時間を要した。専門機関の調査によれば、マルウエアは新種のものであり、大きなシェアを持つ同社のビルマネジメントシステムに特化して妨害する機能を持っていた。電力需給が逼迫した状態を検知して制御に介入し、停電に至るような状況を作り出す目的で作られたことが判明している。

後日、感染元を確認するため、ビル管理会社が感染原因となった作業を行った保守委託先に事情聴取をした所、当日作業用をした担当者は関連会社の外国人契約社員であり、既に退職済みのため連絡が取れないことがわかった。意図的な犯罪行為が疑われたが、捜査機関が聴取しようとしたところ、本人は既に出国済みであった。

問題点として、以下の点が挙げられる。

①管理用ネットワークが非公開かつインターネット等に直接アクセスできないため、当初からマルウエア感染の可能性が考慮されていなかった。

②①と同様の理由で、ネットワーク内のコンピュータのソフトウエアに関してのセキュリティアップデートが行われていなかった。

③コンピュータの OS だけでなく、オープンソースを基盤として作られた機器のファームウエアにおいても、本来不要なサービスが数多く動作していた。

④メンテナンス作業時のネットワークへのアクセス（PC 接続等）についてのポリシーがなく、また、作業は委託先任せになっていた。

⑤重要な施設であるにもかかわらず、こうした事態を想定したインシデント対応訓練が行われておらず、マニュアルも用意されていなかったため、初動が遅れ、被害が拡大した。

【対策】

①適切なリスク評価と設計段階での対応

システムの重要度に応じて、独立したシステムやネットワークにおいても、マルウエアの感染やサイバー攻撃の可能性を評価し、必要に応じて適切な対策（検知や防御の手段）を設計段階から織り込んでおく必要がある。このような場合、少なくともサーバや PC 等に対してマルウエア対策を導入し、その更新やソフトウエアのセキュリティ更新が確実に行えるような仕組み（たとえば、更新ソフトウエアを配信するためのサーバなど）を用意すると同時に、監視体制や対応手順なども検討しておくべきである。

②適切なソフトウエア更新の実施

設計段階での仕組み作りに加え、運用においては、セキュリティ更新に関するポリシーを定め、必要なタイミングで更新が行えるように作業手順を確立しておく必要がある。対象となる脆弱性等について、CVSS 評価値などをもとに、対処の緊急度などを定めておくことが望ましい。

③機器のセキュア化

専用のネットワークとはいえ、特に重要な機器に関しては侵害を受けることを前提に、インターネット等に接続された機器同様に必要な対策を講じておくべきである。不要なサービスを停止させるなどの措置はもちろんのこと、オープンソースソフトウエア等を利用している場合は、それらに脆弱性が発見された場合に、速やかに修正できるよう、開発元における体制整備や機器のファームウエア更新の手順などを考慮すべきである。誤動作や停止が深刻な影響をもたらす可能性がある機器については、必要に応じて不正な操作や攻撃を検知する機構の組み込みも検討されるべきだろう。

④ネットワーク管理ポリシーの確立

重要なネットワークへのアクセスが厳重に管理される必要がある。とりわけ、メンテナンス等の際に、外部から持ち込んだ機器を接続する場合のリスクについては、あらかじめ十分に検討しておくことが重要である。ファームウエアやソフトウエアの更新などの際に、不正なプログラムが紛れ込んだり、マルウエアが持ち込まれることを防止するため、接続前に適切な検疫チェックの実施を義務づけたり、作業者のミスや不正行為を監視、発見するためのしくみなどの導入も検討されるべきである。

⑤高度脅威を前提とした従業者や委託先管理の徹底

重要インフラ等の場合、高度な脅威の対象となる可能性を考慮し、システムにアクセスする業務への従事者が買収、脅迫等の対象となることや、悪意を持っての潜入などの可能性も評価されるべきである。こうした問題への対策は、人事的、法的な対応を含めて検討され、こうした行為の実行を牽制するような施策の導入がなされるべきである。

A5. 介護支援用ロボット端末の悪用

特殊詐欺の被害者が特定の企業が運営する複数の介護・福祉施設の入居者やサービス利用者に集中していることが明らかになった。被害者が利用していた企業系列の介護・福祉施設では、入居者・利用者に対してロボット AI 端末の廉価でのレンタル提供を行っており、後に逮捕された犯行グループのメンバーの供述から、このロボット AI 端末がハッキングされ、詐欺のターゲット選定や掛け子（電話にてだます役割）への誘導等に悪用されていたことが明らかになった。

ロボット AI 端末はカスタム追加アプリケーションによる機能強化にも対応しており、管理用サイトを経由して不正なプログラムを導入させることで、中間者攻撃により通信内容の傍受を行ったり、家族に電話したつもりが掛け子に電話転送されてしまうような仕掛けが施されていた。また、複数の銀行のインターネットバンキングにも接続でき、被害者の多くは、指示に従って操作することで、送金させられていたとみられる。

ロボット AI 端末は利用者の日常の話し相手になったり、コンシェルジュサービスを提供したり、家族とのコミュニケーション支援機能を有しており、クラウドサービスにより高度な AI による介護支援を行うもの。家族側に対してもスマホアプリによる見守りサービス等が提供されており、同施設利用者にて幅広く利用されていた。

【影響】
一連の被害総額は数十億円に及んだ。被害者により詐欺に用いられる題材が異なっており、被害発生地域も分散していたことから、被害者に共通性があることが判明するまでに期間を要し被害が拡大したと見られる。また、職員の目が届かないところで、インターネットバンキングが悪用されたことで、抑止もまったく働かなかった。

【原因】

介護・福祉施設向けに提供されていたロボット管理用サイトを経由してクラウドサービスのシステムが不正にアクセスされており、管理情報やロボット AI 端末とクラウドサービス間の通信内容からプライバシー情報（資産状況、趣味・嗜好、家族構成認知機能状態等）を得ることで、ターゲット選別が行われていた。

管理用サイトのアプリケーションには脆弱性が確認され、これを経由して SQL や OS コマンドのインジェクションが可能になっていた。サイトアクセスには電子証明書による認証

が必要で、これをインストールしたPCからしか接続できないようになっていたが、この企業のほぼすべての施設の管理用PCからマルウエア感染が発見され、このマルウエアによってPCが遠隔操作され、証明書と秘密鍵が盗まれたと考えられる。マルウエアは、その企業から各施設への連絡を装ったメールに添付されており、担当者は疑問を持たずに開いて感染してしまった。

問題点としては、

①認証用の秘密鍵が、暗号化されない状態でPCに保存されていたため、マルウエアによって簡単に盗まれてしまったこと。また、管理サイトに対してIPアドレス等による接続元制限が行われていなかったこと。

②管理サイトのアプリケーションにインジェクション脆弱性があったこと。これにより、攻撃者が管理サーバのデータやOS機能へアクセスできたこと。

③ロボット端末は一般的なモバイル用のOSを基盤として構築されていたが、その上で動作するアプリケーションに関する制限は行われていなかったこと。このため、攻撃者は独自に製作したアプリケーションを管理サイトに仕掛けることでダウンロードさせ、端末上で実行させることができた。また、これらのアプリケーションを介してインターネット上の任意のサイトにアクセスできたこと。

④各施設の管理用端末が、担当者のPCであり、その上で担当者がメールの送受信を含めて様々な作業を行っていたこと。

などが挙げられる。

【対策】

①PCや機器内に秘密鍵を置く場合は、それを適切なパスワード等で暗号化するか、TPMなどのハードウエアに格納する等して保護すること。

②クラウド上の管理サイトに対しての接続は可能であれば、特定のIPアドレスからのみに制限すること。

③機器を統括する管理サーバは、それが侵害された場合のリスク（たとえば、全機器の制御や情報を奪われるなど）を考慮し、脆弱性の排除や攻撃の検知・防御、適切な機能の分離など、必要な対策を講じること

④機器のプラットフォームとして汎用の OS を使用する場合は、可能な限りその機能を必要最小限に制限すること。また、インストールされるアプリケーションについては署名確認等、不正なコードの導入を防ぐ手段を講じること。

⑤機器がインターネットにアクセス可能である場合は、接続先や利用できるプロトコル（ポート）を必要最小限に制限しておくこと

⑥特定の重要サービスに接続する PC 等（特に、そのためのクレデンシャル等が格納されているもの）については、可能な限り通常の作業用 PC 等とは分離すること

A6. 農業工場の生産妨害

野菜をはじめとする作物は、これまでの地面やハウス栽培ではなく工場内に設置された栽培棚の上で生育し収穫されるようになった。また、工場に限らず、そういう設備をもった小型コンテナサイズのものもあり、平坦で膨大な敷地を必要とせず、展開が可能となる。また、従来日本国内では栽培が困難だった作物も大量生産が可能になった。農業の自由化に伴い、多くの企業がこうした方式での生産を全国規模で展開し始めた。

それら作物の生育にあたっては、室温、湿度、光量、水量、薬剤の投入調整などを工場内や栽培棚に設置されたセンサーの値やタイマーで制御する。制御は各地の工場単独でも可能だが、通常は企業の管理センターで集中管理される。これにより、各地での作物の栽培状況や収穫時期を管理し、物流を含む適切な出荷管理が行われる。

この工場では、多品種の作物を栽培しており、そのため、複数種類の飼料や薬品を栽培する品種ごとに、それぞれの状況に応じて配合している。配合データは中央制御システムから最適な値が各工場に送られる仕組みだ。

この企業で、全国の工場内の特定の作物が枯れてしまう事故が発生した。

調べたところ、光量センサーから中央制御システムに送られるデータが異常な値を示し、室内の光源となるライトの輝度制御が異常となっていた。さらに、栽培棚に設置された室温センサーや湿度センサーから中央制御システムに送られる室温情報や湿度情報も異常で、室温や湿度の制御も不安定になっていた。

原因を調査すると施設内の光量センサー、室温センサーを含めたセンサー情報を集約し、中央制御システムに送る役目のゲートウエイシステムが侵入を受け、プログラムが改ざんされ、不正なロジックが組み込まれていた。

中央制御システムから末端の制御機器への制御データも、ＧＷシステムのプログラムにより改ざんされ、配合内容（配合種類や分量）が変更されたデータが制御機器に渡されていた。これにより、人体への健康被害に及ばない許容量を超えて、薬品などが作物に与えられ、それらが出荷された可能性もあることがわかった。

【影響】

作物が枯れるだけであれば、影響は企業のビジネスに対するものが主となるが、飼料や薬品が過剰投与されるなど、健康被害を与える可能性がある場合、出荷済み商品の回収が必要になるだけでなく、社会的な責任を問われ、消費者への被害に対する補償や賠償金支払い、信頼失墜により、以降のビジネスへの影響が深刻となる可能性が高い。

さらに、こうした農業生産の IT 化が進んだ社会では、広範囲な攻撃によって、その作物が生産できなくなることで、サプライチェーン全体にも大きな影響を生じることになる。こうしたことを念頭に、社会混乱やそれによる利益などを目的にした高度脅威による攻撃も考えられる。

【原因】

GW のプログラム改ざんは専門知識が必要である。その開発は外注されており、外注先の技術者が常駐して保守作業にあたっていた。警察が捜査にのりだしたが、システム上に不正操作の痕跡はみあたらなかった。しかし身辺調査の結果、この技術者は高額の借金をかかえており、返済に困っていたが、最近完済したことが判明。そうした事実をもとに聴取を行ったところ、何者かに買収されて犯行に及んだことを自供した。技術者は何者かにプログラムのソースコードを提供し、さらに改ざんされたプログラムを受け取って、それを導入した。作業の痕跡を消す方法も細かく指示されたという。こうしたやりとりは、すべてネット上で行われており、相手が何者かは技術者自身も知らないという。警察では、企業への業務妨害や流通混乱による価格の変動などを意図した犯行を念頭に操作を進めている。

問題点としては、以下のようなものが挙げられる。

①外注先の担当者が、保守作業を自由に行える状況が存在し、それを管理するプロセスが存在しなかった。

②制御の明らかな異常を各工場で検知するしくみが機能していなかった。一部の工場では、アラームが発生したが、すべて誤報として処理されていた。

③こうした農業工場の発達で、特定の作物について寡占状態が発生し、特定の企業にリスクが集中する状況が生じていた。（こうした問題は、将来的な農業だけでなく、現状でも工業や流通における様々なサプライチェーンにおいて存在する）

【対策】

①システム運用のガバナンス強化
・社員、外注要員を問わず、重要なシステムの運用においては、定められた運用手順を遵守し、それが組織的にチェックされるような枠組みを確立する必要がある
・重要な作業については単独での作業を避け、必ず複数の人員によるダブルチェックを行うこと
・監視システムや監査ログの検査を通じて不正行為を発見する手段を確保すると同時に、それを周知し、心理的な抑止力にすること

②現場での異常対応の強化
・制御が異常となった場合の物理的な検知、抑止策も検討しておくこと。
・緊急度が高い異常を確認した場合の対応手順や代替手段を整備すること。

③社会的リスクの認知
・企業は、自社の生産が停止することによる社会的な影響を正しく評価し、その対策を講じる必要がある。また調達側も、調達先の複数化など、リスク分散を行う必要がある。
・社会的な影響が大きい事業については、行政として一定の規制をかけることが必要な場合もある

A7. 自動車システムからの情報混乱

ある夏の日の午後、都内の空は次第に黒雲に覆われ始めていた。202x 年、地球温暖化の影響で、気象の極端化、不安定化はますます進行し、この夏、東京都内は何度か局地的な豪雨に見舞われ、地下街の浸水などの被害が発生していた。気象庁は、数年前から民間企業と協力して局地的な降雨データの収集、分析による、細かいメッシュでの降雨警戒システムを構築し、1Km 四方の範囲で、極端な降雨が予想される場合に警報を出す仕組みを整えている。この仕組みは一定の成功を収め、豪雨の増加にもかかわらず被害は今年に入って減少傾向になっている。このシステムでは、屋外にある様々な機器、たとえば自動販売機につけられたカメラなどから副次的に得られる情報をもとに降雨を検知する。この情報収集に最も力を発揮しているのが自動車からの情報である。近年の自動車は降雨センサーによるワイパー自動制御の機能を持つものが少なくない。また、降雨があれば、運転者はワイパーを作動させる。この情報をメーカー経由でリアルタイムに収集し、気象情報に活かす試みは民間では早い時期から行われてきた。今では、気象庁がこうした民間の気象情報会社や自動車メーカーと契約を結んで情報の提供を受け、スーパーコンピュータを使ったリアルタイムな解析で、正確な短時間降雨予測を行っているのである。実は、風向や風速などの情報を間接的に自動車から得る実験も行われている。最近の高級車では、運転者のハンドリングをアシストして車線を外さないようにする制御を行う車がほとんどである。もちろん、高速道路に限って言えば、完全な自動運転車も次第に増加しつつある。こうした車の動きに対して風が与える影響は無視できず、少なからずその制御に影響を与える。こうした微妙な制御の変化から車が受けている風圧を計算し、その時点の風向と風速を求めるような試みである。自動車のハンドル角、車線の曲率、タイヤとステアリング装置への抗力、駆動力とそれに対する抵抗力など、様々なパラメータから風圧を計算するモデルが検証されており、これらは車種ごとに大量のデータからその特徴を学習した AI によって補正されている。これらの情報を総合すれば、降雨と大気の状態が非常に細かいメッシュで得られるため、ゲリラ豪雨の数分から数十分前に警報を出すことが可能となる。

この日も、システムは、ゲリラ豪雨の兆候をとらえていた。まだ、警報を出すには至っていないものの、かなり強烈な雨が降る可能性が次第に高まっている。そんなときに、気象庁にある警報センターのコンソールに異常が表示された。ある大手自動車メーカーから受け取っているデータの異常値が急増しているという AI からのアラームである。AI は、これまでのデータをもとに、現在のデータの信頼性や異常な動きを検証している。異常値の急増は気象の異常を示す可能性もある。担当者は、システムに対して、この異常値をもとにしたシミュレーションを指示する。結果は、ある地域で数十年に一度あるかないかの豪雨が発生するというものだった。担当者は、ただちに警報を発令する手続きに入った。

その頃、首都高速道路の至る所で、大渋滞が発生していた。渋滞の列にいる車の半数ほどが雨も降っていないのにワイパーを動かしている。いくつかの渋滞の先頭では、事故車両が止まっている。この事故車両の多くがワイパーを動かしていた。

その頃、気象庁から一部の地域に対して局地的な豪雨警報が発令された。警報が発令されると、交通機関は徐行や運転見合わせを実施する。地下街や地下鉄の駅では、浸水に備えて、避難指示が出され、入り口の階段等には遮水盤が設置されることになっている。しかし、この日の警報は珍しく空振りに終わった。一方、全く違う地域で激しい豪雨が発生し、道路の冠水や地下街に浸水するなどの被害が発生した。これにより、冠水したガード下で逃げ遅れた車の運転手が溺死したのをはじめ、避難時の混乱などで多くの負傷者も出てしまった。

この状況が発生した際、走行中の車のワイパーが突然動き出すという現象が、都内を走行している多くの車に発生した。これらはすべて、ある大手自動車メーカーの車種で、ドライバーはこれに慌てて、減速したり、ハンドル操作を誤って事故を起こしたりしたのだという。それが原因で、至る所で大渋滞が発生することとなった。事故による負傷者も少なからず発生している。

【影響】

自動車では、運転を妨げる可能性があるいかなる動きも、事故や渋滞を引き起こす可能性が有り、非常に重大な結果に至る可能性がある。（ワイパーに限らず、たとえば、カーオーディオが突然大音響で鳴り出した・・・など）また、今後、IoT においては、様々な機器から、その目的以外で副次的に得られる情報を活用する動きが拡大していくと思われ、これまで想定していなかった影響をもたらす可能性にも注意が必要となる。

【原因】

気象情報が混乱した原因は、ワイパーの異常動作による降雨検知情報の混乱と、渋滞が発生したことで、正確な風速、風向の情報が得られなくなったことである。気象庁の担当者は、AI が異常と判定した理由をよく確認せず、そのデータをシミュレーションに使用してしまった。実際、AI はその現象が特定のメーカーのみで発生していることを認識しており、それがアラームの主な要因となっていたのである。

後日の調査で、ワイパーの異常動作は、自動車の情報系システムに感染したマルウエアが引き起こしていたことが判明した。マルウエアの本体は純正のカーナビゲーションシステムに存在していて、5G 通信網を経由して、外部の不正な指令サーバに接続していた。カーナ

ビは GPS 情報を取り扱えるほか、CPU の処理能力も高く、通信機能や CAN を経由して自動車のいくつかのシステムにもアクセスできるため、このメーカーでは、先に述べた気象情報収集用のプログラムをカーナビの中で動作させていたのである。こうした関係から、ワイパー制御のＥＣＵも、カーナビからアクセスが可能になっていた。マルウエアは、こうした機能を逆手にとってワイパーを誤動作させたものと思われる。何者が、こうした攻撃を仕掛けたのか、また、交通の混乱と気象情報の混乱のいずれを意図したものかは、まだ不明である。

問題点としては以下のような点が挙げられる。

①カーナビゲーションシステムは、スマートフォンなどに使われる汎用 OS を使用しており、利用者が様々なアプリをダウンロードして使用できるようになっていた。こうしたアプリを介してマルウエア感染が広がったと考えられる。

②カーナビゲーションシステムから、ワイパー制御用 ECU に対して情報取得だけでなく、制御用のコマンド発行が可能になっていた。これにより、マルウエアはワイパーを制御することができた。また、この事実はカーナビにインストールされた情報収集用アプリケーションを解析することで把握できた。

③気象情報を処理するシステムの運用において、異常値がサイバー攻撃や特定メーカーのシステム異常が原因で発生する可能性を考慮していなかった。

【対策】

①アプリを介したマルウエア感染防止
・汎用 OS を重要なシステムに利用する場合、利用者によるアプリケーション導入の制限を検討すること。一般のアプリストアからではなく、メーカー自身が提供する検証済みアプリのストアに限定するなどの方法がマルウエア混入対策としては有効

②ECU へのアクセス制御の強化
・ECU が他の ECU や外部機器からの不要なコマンドを受け付けないようにする。情報取得のみが必要な場合は、制御に関するコマンドは ECU で受け付けないようにするか、ゲートウエイで排除する

③データ検証の強化
・ビッグデータや AI を活用した情報処理において、入力される情報について、意図的な加

工や特定の状況が作り出す異常などの影響を十分考慮すること。
・特に利用者への影響が大きな情報を処理する場合は、こうした異常が発生した場合の対処について、事前に十分な検討を行っておくこと。

④システムにおける異常検知、アラーム発生時の手順の確立
・システムが異常を検知した場合に、確実に対処するため、あらかじめ様々な原因を想定した対処手順を定めておく必要がある

A8. デジタルサイネージ乗っ取り

ネットワークに接続され、集中制御とタイムリーな広告表示が可能なデジタルサイネージは、市街や大規模な商業施設、駅、空港などに設置され、その数は増え続けている。近年、4K、8K といった高解像度のディスプレイを使ったものや、インタラクティブに表示内容を変えられ、案内板としても使用できるものも増加しており、利用シーンも拡大を続けている。

某年某月、首都圏のとある空港では、A 国元首の特別機到着を控え、厳戒態勢がとられていた。A 国は、この数年、地域紛争に介入しており、かねてより複数のテロリスト集団が報復を示唆している。このため空港は通常の国賓受け入れよりも数段ハイレベルの警戒態勢となっている。今回の元首訪日は、経済対話が中心ということもあり、同国の経済界からも、代表団として多くの VIP が民間機で到着することになっていたため、空港全体に警備が増強されていた。

空港のあちこちに配置されたデジタルサイネージには、歓迎ムードを演出するためのコンテンツが流されている。ちょうど日本の夏休みシーズンであることもあって、空港は多くの旅行客で混雑していた。旅行客は、ものものしい警戒に戸惑いながらも、旅への期待を膨らませている。そんな中、事件が起こった。

突然、空港内のすべてのデジタルサイネージに、テロリストとおぼしき映像が表示され、英語と日本語でA国を非難するメッセージに続いて空港の爆破宣言が行われたのである。空港内の複数箇所に仕掛けられた爆発物を間もなく爆破するという。これを見た旅行客がパニックを起こし、出口に殺到したため、空港ロビーは大混乱となった。警備にあたっていた警察官が制止、誘導しようとするも多勢に無勢で収拾がつかない。搭乗ゲートがあるコンコースでも同じ状況で、逃げ場を失った旅行客が入出国審査場などに殺到して制止を振り切って外へ出ようとしたため、こちらも大混乱となった。一部の旅行客はゲートから空港の敷地内に逃げ出した。こうして、空港のセキュリティは崩壊したのである。

旅行客、空港職員、警察官などに多くの負傷者が出た上に、混乱によって施設の一部も破壊されてしまった。結果的に爆発物は発見されなかったが、この影響で空港は閉鎖され、多くの旅客に影響が出ると共に、A 国元首の特別機は別の空港に向かわざるをえなくなってしまった。

【影響】

大衆がパニックを起こすことで混乱が生じると、様々な事態が発生する。これにより、多くの死傷者や、施設、設備の破壊が生じる可能性があり、また、それが特定の施設等で発生した場合は、その施設の機能やセキュリティが大きく損なわれる可能性が高い。こうした事態は、空港のみならず、鉄道の主要駅や大規模商業施設、イベント会場等でも発生する可能性がある。

【原因】

デジタルサイネージのコンテンツがテロリストによって改ざんされたことが直接の原因。このコンテンツは、サイネージの専用ネットワークを経由して配信サーバから配信される。空港内のネットワークは場所ごとに分かれていて、各配信用サーバは、クラウド上のサービスからコンテンツを取得するようになっていた。当初、原因として配信サーバ内のコンテント改ざんもしくは、クラウド上のコンテンツサービスが侵害された可能性が疑われ、調査が行われた。サービスへの攻撃の痕跡がいくつか発見されたが、いずれも失敗していた。また、配信サーバには攻撃の痕跡は見られず、ログによればコンテンツは正常に正式なサービス URL から TLS でダウンロードされていた。

ここにきて原因究明は暗礁に乗り上げたかに思えたが、配信サーバからの通信が経由するインターネットとのファイアウォールのログを確認したところ、配信サーバが不正な IP アドレスに対して接続していることが判明した。DNS サーバを調べたところ、設定が改ざんされ、本来のサービスドメインが別の IP アドレスに誘導されていた。配信サーバは、この IP アドレスを本来のサービスとみなして不正なコンテンツを受け取ってしまったものと思われる。通信自体は TLS で行われていたが、互いに証明書の確認などは行われておらず、単純なパスワード認証が行われていただけだった。配信サーバとサービス間の通信手順は公開されていないが、攻撃者は、通信を一旦復号して本来のサーバに中継する（いわゆる MiTM を行う）ことで、内容を解析できた可能性がある。

問題としては、以下の点が挙げられる。

① DNS サーバに脆弱性があり、外部からの侵害を許してしまったこと。（直接の侵害でなく、キャッシュポイズニングのような攻撃方法も考えられる）

②配信サーバとクラウド上のサービスとの間で TLS の証明書ベースでの認証が相互に行われていなかったこと。（機器と配信サーバ間でも同じ問題があることが考えられる）

③ダウンロードされたコンテンツについては、同じ通信で受け渡された SHA1 ハッシュを検証するだけで、電子署名などは行われていなかった。

【対策】

①TLS による機器、サーバ間、クラウド上のサービス間などの通信は、互いに電子証明書による正当性確認を必ず行うこと。

②コンテンツの改ざん防止策を講じること。コンテンツには、サービス側で電子署名を付与して、配信サーバや機器側で検証を行うこと。

③DNS 等の周辺サーバを含め、脆弱性をタイムリーに修正できるようにしておくこと。

A9. 自動販売機への Man in The Middle（MiTM）攻撃ツール拡散

自動販売機メーカー大手某社は、スマートフォン等を無線接続して、クレジットカードやポイントを使用して商品を購入できるような仕組みを入れた新製品をリリースした。周辺で使用できるよう、パワーを抑えた WiFi アクセスポイントの機能を自販機にもたせ、スマートフォンに専用アプリをインストールすれば、自販機の近くで自動的に接続が行われる。専用アプリは、この接続を介してサーバと通信し、利用者のアカウントのポイントを管理する。AP 接続中の利便性を考えて、アプリで認証すればメールや通常の Web へのアクセスも可能だが、連続使用は 5 分以内で、再接続には 30 分のインターバルを必要とするようになっている。購入の際は、周辺のスマホとの競合を避けるため、スマホをタッチして NFC を使って購入者が自販機をロックするようになっている。利用するたびにポイントがたまることもあって、数年の間に同社の自販機の大半が、こうしたものに置き換わった。

しかし、ある時期から同社のサービス拠点には、この機能が不安定でうまく使えないという苦情が多く寄せられるようになった。しかし、いずれも点検の結果、自販機自体に異常はみあたらず、同社の担当者は首をかしげた。この現象は、いくつかの地域に設置された自販機に集中して発生していた。また、こうした不調を訴えた利用者の多くが、その後、スマホの動作がおかしくなったという話が SNS を通じて広がっていた。

その地域の電波状況を疑った担当者は、専門の業者に依頼して、自販機周辺の WiFi 電波状況調査を行った。その結果、問題が発生した自販機の周辺で、自販機と同じ SSID を持ったアクセスポイントが複数存在することが判明した。業者によれば、信号は自販機のものよりも、ずっと強く、複数のスマホで試したところ、10 台中 7 台が自販機ではなく、別のアクセスポイントに接続してしまったという。妨害行為を疑った担当者は、別の専門業者に依頼して、これらの偽アクセスポイントの所在や、接続した際の挙動などを調査した。その結果、あるアクセスポイントは、近隣のアパートの一室に設置されていると見られ、スマホから通信を受けて、それを自販機に中継していることが判明した。調査した業者からは、通信の盗聴や改ざんが行われている疑いが強いとの指摘もあった。実際、追加の調査で、自販機の操作に失敗したケースを調べると、明らかに通信が改ざんされていることがわかった。スマホから送られたトークンが正しく中継されていなかったのである。このトークンは、利用者が商品を購入するためにスマホでクレジットカード決済やポイント利用の手続きを行った結果として、サーバ側から入手するもので、サーバが発行したシリアル番号、金額、有効期限などの情報に自販機メーカーの電子署名がかけられている。自販機は電子署名を検証し、シリアル番号をサーバに確認した上で記載された金額に応じた商品を購入可能にする仕組みだ。一度使用したシリア

ル番号はサーバ側で無効化され、重複使用を防いでいる。だが、一度得たシリアル番号はそれが使用されるまで、最大一ヶ月間有効であった。問題のケースでは、スマホから偽 AP に送ったトークンは、そのまま中継されず、異なるデータが送られていた。このため、自販機側で電子署名の検証に失敗して無効になっていたのである。

その後、数日たった時点で、その時中継されなかったシリアル番号のトークンが使用されたことをサーバ側で確認した担当者は、警察に相談した。警察がアパートを捜索した結果、指向性アンテナを含む WiFi アクセスポイント機器とコンピュータが押収された。警察が解析したところ、コンピュータ内には、複数の有効なトークンが保存されていた。その部屋に住んでいた 20 代の男は、盗聴で得たトークンを自分が商品を買うのに使用していたという。

さらに捜査の結果、ネット上のサイトに、こうした盗聴のためのマニュアルと不正接続用のソフトウエアが存在することが確認された。同様の事態が発生した他の地域でも、こうした情報を元に盗聴を行っていた複数の容疑者が逮捕された。警察は不正接続ソフトウエアの解析を試みたが、高度な方法で難読化されており、困難を極めた。しかし、そのソフトウエアがスマホや自販機だけでなく、インターネット上の特定のサイトと通信をしようとすることも判明した。このため、このソフトウエアには、自販機の悪用以外の機能があることも推定できたが、既にそのサイトは応答せず、通信の内容は不明である。誰がこのソフトウエアやマニュアルを作って公開したのかも、まだ判明していない。その後、不調を訴えた利用者のスマホからある種のマルウエアが検出された。このため、ツールを公開した者の本当の意図は、マルウエアの拡散にあったのではないかと推測されている。メーカーは自販機とシステムを改良するまでの間、すべての自販機でその機能を停止させ、トークンを奪われたと考えられる利用者に 2 倍のポイントを還元した。

【影響】

正当な利用者が、クレジットカードで支払った代金やポイントを横取りされてしまう。こうした行為を特定の場所においてでなく、毎回異なる場所に移動して行うことで、追跡も困難となり、発覚もしにくくなる可能性がある。また、こうした情報がアンダーグラウンドで流れることで、利用者だけでなく、メーカー自身にも様々な被害が予想される。

さらに、こうした不正を行うためのツールに、何者かが悪意を持って別の機能を組み込んで拡散させることで、別の攻撃の足場に利用することも考えられる。こうした一見単純な不正ツールが、実は別の目的を持って拡散される可能性も、場合によっては考慮が必要だろう。たとえば、自販機を介してメーカーサイトからスマホアプリになんらかの情報がプッシュされ、それが Web ブラウザなどで表示されるような仕組みに介入し、マルウエアなどの不正なコンテンツを送り込むことができる可能性も考慮したい。自販機の不正利用は自販機の利用者が多い場所ほど効率が良いから、この点でも、ツールの提供者と使用者の利害が一致する。

【原因】

①アプリケーションが正当な AP と偽の AP を識別する手段を持たず、容易に偽の AP に誘導されてしまったこと。

②トークンが端末もしくは利用者のアカウントと紐付けられておらず、一旦入手できれば、どの端末からでも使用できるようになっていたこと。これは、利用者が複数の端末を持っていることや、利用者同士でトークンを受け渡せるように配慮した結果だった。

③WiFi を経由して行われる通信は WPA2 で暗号化されていたが、その上で行われる通信そのものは暗号化されておらず、Man in The Middle 攻撃で、通信の内容を取得、解析できてしまったこと。

【対策】

①アプリが自販機の正当性を確認できる手段を用意すること。たとえば、AP の認証において電子証明書を検証するなどの方法を検討すること。

②トークンを端末固有の情報や認証済みユーザの情報に紐付けて管理すること。端末間でのトークンの移動や利用者間での受渡は、一旦発行済みトークンを無効化した上で、実際に利用する端末もしくは利用者側で再発行すること。また、トークンの有効期限は必要最小限にすること。

③アプリとデバイスの間で行われる通信を、TLS 等で暗号化すること。また、①が困難であれば、この通信のレベルで相手方の正当性を電子証明書等で確認すること。

④通信内容を解析する手段を封じること。③は有効な手段だが、スマホアプリのリバースエンジニアリングなども想定して対策を検討することが望ましい。

Man in The Middle 攻撃や盗聴は、WiFi に限らず、他の形態の無線通信や、物理的な保護のない有線ネットワークでも発生する可能性がある。機器間の通信は、常にこうした事態を想定して行う必要がある。特に、不特定多数が利用するサービスは、まったく別の目的への悪用を念頭に攻撃される場合もある点に留意が必要である。

A10. 遠隔医療機器へのマルウエア攻撃と脅迫

Y 県の X 地方は医療改革特区として遠隔医療に関しての導入が進んでいた。過疎地域の高齢者を中心に、遠隔によるモニタリングと、地域の診療所、高度医療を行う中核病院の連携によるテレケア実証プロジェクトである。医師と患者間の遠隔対応（DtoP）だけでなく、家庭医と専門医の間の遠隔連携（DtoD）も含む総合的なシステムが実現されている。

県中央病院のテレケアセンターに設置された遠隔患者診断治療ルームには、各科の専門医に加え医療用の AI が遠隔地の在宅医療患者(主にペースメーカーやインスリンポンプを装着した慢性疾患患者)を２４時間体制でモニターし、異常を検知した際は必要に応じてドクターヘリや遠隔手術室のある地域中核病院への救急車による搬送などを行う体制も整えられていた。このシステムでは、患者が装着した小型のモニタリング端末が家庭内の専用 WiFi ゲートウエイや外出時には５G 通信を使用して情報をテレケアセンターに送信するようになっている。モニタリング端末は常時患者の心電図波形や体温をモニターできるほか、ペースメーカーやインスリンポンプの稼働状況とそれに付属する血糖値センサーなどの情報を統合し、センターの開始システムに定期的に送信する。また、ある種の異常を検知した場合は即座にアラームを発生するため、患者に発生した緊急事態にも即応できるのである。こうした患者の状況はシステムを介して、患者の「かかりつけ医」とも共有され、必要に応じて専門医の助言も得ることができるようになっている。

このシステムで最初の障害が発生したのは、ある秋の日だった。一部の患者から送られてくるデータの受信間隔が不安定になったのである。最初、ある患者のデータが 3 回連続で欠落したというアラームが発生し、それが復旧すると今度は別の患者、というように順次現象が発生し、最終的にすべての患者にアラームが上がる事態となった。担当者はシステムのサプライヤーの保守窓口に連絡し、調査を依頼したが、その後現象は発生せず、原因も不明との回答だった。

数日後、ある患者が体調不良をきたし、救急搬送された。血糖値が異常に低下したことと心電図、心拍の異常がシステムで検知されたのである。病院での治療に結果、患者は回復したが、インスリンポンプの異常も疑われたために、この機器は交換され、点検のためメーカーに送られた。さらにその直後、別の患者が心臓の異常で搬送された。この患者には慢性的な不整脈の症状があり、除細動機能を持つペースメーカーが装着されていた。患者が心臓に強い痛みを感じると訴えたため、ペースメーカーの異常が疑われ、緊急手術で交換されることになった。

テレケアセンターの窓口に脅迫メールが届いたのはその翌日だった。メールには、前日に搬送された患者の氏名が記載されており、インスリンポンプやペースメーカーの誤動作は自分がハッキングした結果であったことと、一億円相当のビットコインを支払わなければ、複数の患者に対し、致死量のインスリン投与やペースメーカーの誤作動で心停止を起こさせると書かれていた。

中央病院は直ちに県に報告すると同時に警察に相談。ビットコインを支払うべきかどうかの協議と並行して、回収されていたインスリンポンプとペースメーカーの解析が行われ、インスリンポンプについてはファームウエアの改ざんが確認された。ペースメーカーについては改ざんの兆候はなかったが、専門家とメーカーによる解析の結果、外部から不正操作が可能な脆弱性が発見された。

これらから、犯人はモニタリング装置を経由して操作を行っていることが推定されたため、全患者に連絡を取って医療機関に行くよう指示すると共に、それが困難な患者に対しては、かかりつけ医や救急隊が対応、モニタリング装置を停止させ、各機器をオフライン状態においた。

【影響】

① これにより、多くの患者の生命が危険にさらされた。場合によっては多くの死傷者が出た可能性がある。
② 対応のため、多くの医療機関、救急隊の人員が動かざるを得ず、医療、救急の業務に支障が出た。
③ 以後、このプロジェクトは中断し、再開の目途はたっていない。この事件以降、国内の同種のプロジェクトの延期や見直しが頻発した。

【原因】

その後の調査で、テレケアセンターにある複数の PC からマルウエアが発見された。また、管理用サーバ内に置かれたモニタリング装置やインスリンポンプ遠隔更新用のファームウエアに改ざんが発見された。この改ざんによって、モニタリング装置やインスリンポンプはセンターからの指示以外に、犯人のサーバからの指示によって動作することが確認された。インスリンポンプは本来、モニタリング装置に情報を送るだけで、指示を受けることは無いが、改ざんによってモニタリング装置で中継された犯人からの指示を受けて動作することも確認された。

テレケアセンターの管理ネットワークからは、特定の情報検索用の PC を除いてインターネットには接続できないようになっていたが、情報検索用 PC と管理用のシステムは同じネットワーク内にあり、検索用 PC に感染したマルウエアが脆弱性を攻撃することで、ネットワーク内に広がったと考えられる。また、検索用 PC に感染したマルウエアが、他の PC からインターネットへの通信を中継する機能を持っていたため、各マルウエアは、外部からの指示を受け、また情報を外部に送る事ができた。犯人は、こうした仕組みで内部のネットワークを調査し、ファームウエアを発見、取得してリバースエンジニアリングを行ったものと考えられる。これらのファームウエアには難読化などのリバースエンジニアリング回避のための措置はまったく行われておらず、犯人が相応のスキルを持っていれば比較的容易に解析ができたと考えられる。犯人はそれを利用して改ざんしたファームウエアをサーバに送り込み、遠隔更新機能を利用して一台ずつファームウエアを改ざんしていった。

ペースメーカーのファームウエアに関しては、サーバには置かれていなかったが、研究者によって同種の製品に関する近接無線を経由した外部からのハッキングの可能性が指摘されていた。また、この機器は近接無線により、機器のモニタリングの他に様々な保守操作が追加認証なしで行えるようになっていた。犯人が具体的な攻撃方法をどのように入手したかについては不明だが、モニタリング装置から、この近接無線を使用して脆弱性を攻撃していたことが確認されている。

細部の原因と考えられるものを列挙してみると、

① システムの管理用ネットワーク内にインターネット接続可能な PC が存在していたこと。マルウエアがネットワークを経由して感染する可能性が考慮されていなかった。
② 管理システムの PC やサーバのセキュリティ修正が行われておらず、多くの脆弱性が残っていたことがマルウエア拡散の一因。また、サーバの管理者アカウントのパスワードには非常に単純なものが使用されていた。
③ 機器のファームウエアについて、機器側で正当性を確認する手段が用意されていなかった。また、ファームウエアが容易に解析、変更できたこと。
④ 機器について攻撃可能性の指摘に対して対応が行われていなかった。これは、こうした攻撃の可能性を過小評価したことと、機器交換のコストが膨大になることが原因と考えられる。
⑤ 機器の保守操作に対して追加の認証が不要であった。これにより、攻撃者はモニタリング機器に設定されていたパスワードを使用することで、保守機能にもアクセス出来てしまった。

【対策】

① インターネットと機器が直接通信できない環境にあっても、同一ネットワークに通信可能な機器やコンピュータが存在すれば、それが抜け穴になる可能性がある。また、こうした機器が常設されていなくても、外部から持ち込んだ機器や USB メディアやコンピュータを介してマルウエア感染が生じる可能性を考慮する必要がある。従って、システムの管理用ネットワークや重要な機器が配置されるネットワークはすべての機器からインターネットへの通信経路をなくすと同時に、外部との間の機器やデータ、ソフトウエア等の移動に関してポリシーを確立し、必要な移動制限と検疫措置を講じておく必要がある。また、誤接続等を防止するため、こうしたネットワークの近くに一般のネットワークの接続口や WiFi アクセスポイントなどを配置しないことも重要となる。

② 閉鎖されたネットワーク内でも、マルウエア感染や悪意による脆弱性への攻撃が発生する可能性があることを念頭に、適切な脆弱性管理ポリシーを確立し、特にリスクの高い脆弱性については、修正プログラムを早期に適用するための作業手順を確立しておくことが必要である。なお、外部から修正プログラムを持ち込む際、その正当性を必ず確認すること。（ベンダ提供のハッシュ値などを利用）また、コンピュータや機器がネットワーク経由のアクセスを許す場合、その接続には必ず認証を行い、使用するクレデンシャル（パスワード等）を適切な強度に設定し、保護すること。（OS のデフォルトアカウント、デフォルトパスワードは必ず変更すること）

③ 機器のファームウエアについては、メーカーによるコード署名などを付与し、改ざんを防止すること。また、特に重要な機器では、ファームウエアの難読化など、リバースエンジニアリングへの対策も検討すること。

④ 外部からの脆弱性や攻撃可能性への指摘については真摯に対応すると同時に、対応が困難な場合は専門機関、専門家等に相談すること。また、設計段階から脆弱性の修正を安全に行う手段（たとえば、機器を止めずに更新する方法等）について検討し、あらかじめ組み込んでおくこと。

⑤ 機器の接続に無線（WiFi, Bluetooth, その他近接無線、携帯通信網等）を使用する場合は、それらを経由した攻撃や通信傍受、通信不能な事態発生の可能性に留意すること。また、無線による操作は必要最小限のものに限定すること。

⑥ ネットワークを使用した保守機能の利用には追加の認証（もしくは一般のアクセスとは異なる認証）を行うこと。