訪問許可者による玄関入室の安全性を高める、「コンシェルネット」システム

Concierge-net for residential door access control service

室木　勝行*
魚田　勝臣**
*株式会社 SYNCHRO
**専修大学　名誉教授

要旨

少子高齢社会の我が国では自宅で生活支援を受けられる環境整備が遅れており、新型コロナ禍に見舞われる昨今にあっては在宅介護に中っていた身内が感染した際、要介護対象者を施設へ移動させ助成するプログラムが用意される等、遅々として在宅生活支援環境が整っていない実態が明白である。一方、新型コロナ禍で促進された遠隔医療は、初診から受けられる様になる等法整備が進み始めたものの、診断する側とされる側双方の「なりすまし」が課題となっており、フィジカルとサイバー両セキュリティ対策が急務となっている。これら日本の課題に目を向け、IPV4 接続が基本となっているインターネット通信上の脆弱性が明らかな現状に対して、IPV6 暗号化通信方式で IoT の強固なセキュリティを実現し、また本人認証の精度も高めた在宅訪問サービス用のプラットフォーム「コンシェルネット」を紹介する。此れにより、インターネット接続システム全般のセキュリティ課題に対し、解決起案を行う。

1. はじめに

Society5.0 への移行を国あげてプロパガンダを掲げ、SDGs を意識した社会の実現が将来の社会存続の前提であるとの考え方も広く行き渡り始めた昨今、突如新型コロナ禍で社会と生活様式の変化が余儀なくされ、社会システム全般に於いてセキュリティ強化の必要性が顕在化した。

具体的に、職場ではテレワークの普及が加速し、高等教育以降の教育現場では Web を利用しての教育カリキュラムが履修できる中で登校授業がストップし、医療現場では初診から遠隔医療が受けられる様になる等、インターネットを介して遠隔提供される各種のサービスが身近となっている。これらの DX（デジタルトランスフォーメーション）を通じて、社会全般が急速にデジタルツイン社会へと変貌を遂げつつある今、大きな事故をプロアクティブに未然化する次世代型セキュリティ対策が必要である認識を広げる必要性がある。

具体的には、急速に利用が伸長した Zoom に代表される Web 会議ツールでは、許可されていない他者が参加して来たり、学籍が無い他者が不正受講して来たり、保険証を持たない他者が保険証を偽って遠隔医療を受けたりする等、サイバーとリアル空間ともどもセキュリティの脆弱性を突いた「なりすまし」事犯は枚挙に暇がない。

この様に、2020 年は生活基盤の家庭と職場や教育現場や売り場等の遠隔拠点がインターネットで繋がり、製品やサービスを提供し受容する際にアクセスし合う頻度が増し、サイバーとリアルの両世界で認証を強化すべき場面が増加しており、人間中心の安全で安心感を伴ったシステムとして、ネットワークアクセスとフィジカルアクセス両面で防犯耐性を備える事が急務である。

これに対して、セキュリティの備えが無防備な状態の現実下、IoT 機器の普及と利用が加速する現実に対して警鐘を鳴らすと共に、セキュリティの脆弱性に対する有効な解決案と普及促進を図りたいため、小論を執筆した。

本警鐘を鳴らす筆者の経営する株式会社 SYNCHRO は、フィジカルアクセスコントロールとサイバーアクセスコントロールの両面でセキュリティを高めるトータルアクセスコントロールの開発と普及に 20 年間取り組んでおり、現代社会の急務を解決に導く必要十分なソリューションを準備している。

2. デジタルツイン社会の背景にある脅威

昨今、IoT の普及でリアル環境に点在するデバイス群はネットワークを介してビックデータ収集され

ており、そのデータ群は AI（Artificial Intelligence）で目的別に自動解析が行われ、人手を介さず「判断のオートメーション化」が様々な場面で加速している。

この様な社会では、デジタルツインと言う言葉に表現される通り、リアル環境に点在するデバイス群の状態や、ネットワークに直接接続されていない人間像までもが、サイバー空間上に仮想形成されるデータ集積モデルやアバター等と相関関係を持ち始めている。

そして、時間経過と共に相関関係が密接になり、データ集積モデルやアバター等とデバイスや人間像が互いに近似化して来ている。その結果、リアル空間からサイバー空間へ、またサイバー空間からリアル空間へ、相互に影響を及ぼし合う社会へと変貌し始めている。

これ等の変化に対して警鐘を鳴らすべきは、人がリアル空間からサイバー空間に対して危害を加える事が出来る事犯とは逆に、サイバー空間からリアル空間に存在する物や人に対しても危害が加えられる新側面も生まれており、デジタルツイン時代は利便性と危険性が背中合わせとなった点である。

実例として、世界最大手の電機メーカーＧＥ社は、航空機のエンジン稼働状況を IoT データ収集によってリアルタイム監視し、飛行中も逐次実態を把握できる様にしており、データの集積モデルとデバイスのエンジン状態を近似化し、着陸時に合理的な整備を行ってコストダウンの恩恵を享受している。

一方、仮にビルの自動空調システムに上記事例を適用して見ると、仮想空間のデータ集積モデルに対してデータ改竄が行われた場合､設定温度 25 度であるにも関わらず室温が 10 度で認識されたとすると、AI による判断で＋15 度に空調自動制御され、25 度に制御しているつもりが 40 度に制御されオーバーヒートでサーバダウンしたり、熱中症で人が倒れたりする被害等が生じ得る。

この様に、デジタルツイン化する社会では、リアル空間とサイバー空間の両世界から「なりすまし」や「データ改ざん」等の不正アクセスを防ぐ必要性があり、これ迄のセキュリティ概念を超えた総合的な対策手段の登場と普及が急務となっている。

3. トータルアクセスコントロールの必要性

これ迄のセキュリティ概念は、リアル空間での「なりすまし」による不正アクセスと、サイバー空間からの「中間者攻撃」等は別課題として認識され、個別にそれなりの対策が施されて来たものの、「なりすまし」ができる余地が数多く存在している。そして、これ等の課題が融合している現状に対する危機意識が余り根付いていないと筆者は推察しており、此れ迄以上に警鐘を鳴らす必要性を感じている。

例えば、Fintech で現金決済から電子決済へとパラダイムシフトが進む中、「なりすまし」による不正送金や不正引き出し事例は枚挙に暇が無いにも関わらず、多くのユーザーは此れらを使い続けている。ＩＤカードやパスワードもそれなりのセキュリティ対策が講じられながらも、依然としてリアル空間で「なりすまし事犯」は増加の一途を辿っており、またサイバー空間から中間者による「なりすまし攻撃」も増加の一途である事は、日々の報道をみても明らかである。

筆者は 20 年前から此れら様相に鑑み、独自のトータルアクセスコントロール手法を提案して来た。

4. エンドツーエンド暗号化通信方式によるサイバーアクセスコントロール

トータルアクセスコントロール手法の一側面である、インターネット接続される 2 者間の通信方式に大きな共通課題が存在する為、先ずはこの点を指摘したい。

現在、インターネットに接続する機器の大半は IPV4 通信プロトコルで接続されているが、実際に発信者側は繋がろうとする先に対し、正しい相手と接続しているか否かを確認する術を持たない。

例えば、IP カメラが現地画像データを遠隔の画像サーバに発信している最中に、ハッカーがインターネットを介して IP カメラに接続して映像を盗撮する事は可能であり、また画像サーバに蓄積された画像データをハッカーが消去する事も可能である。これらは中間者攻撃と呼ばれ、正規に IP カメラシステムを運用している者にとって、インターネットを介して中間者攻撃してくる相手から通信接続を防御する術を持ち併せていないのが実状である。

そこで、インターネット接続の際、繋がろうとする相手に対し通信制御（アクセスコントロール）を行う為の「エンドツーエンド暗号化通信方式」が防御上有効となるので、以下具体的に説明をする。

一般的に、時速 60 キロで走る車のナンバーを確実に視認できる防犯カメラは秒間 30 フレームの画像データを現地側（IP カメラ）から発信する仕様となっており、これを録画する画像サーバに対して IPV4 通信でインターネット接続しており、監視者もモニター用ＰＣから本画像サーバに IPV4 通信している。

これに対し、オープンソースソフトウェアである Cjdns や Yggdrasil を用いた KATABAMI 暗号化通信で 1 フレームの画像データ毎に鍵と解凍用 Key を発行し、発信側のデバイスから接続許可なデバイスに対するデータ通信できる前提を IP カメラシステムのネットワークレイヤーに組み込んだ。

そして、デバイス間を IPV6 通信プロトコルで接続して、1 フレーム毎のデータ通信接続制御を自動的かつ超短時間に Key ローテーションする仕組みを逐次稼働させる様にした。

かくて、IoT デバイスである IP カメラと画像サーバとモニターPC に、KATABAMI 暗号化通信に必要なサービスソフトウェアを組み込めば、中間者からサイバーアクセスを防御せしめる機能を付与する事が出来る為、2020 年末に日本初の国産 IP カメラに組み込み、市場流通を開始する段階にある。

この他、筆者が経営する SYNCHRO では、KATABAMI 暗号化通信を IoT デバイスに 3 機種に組み込み開発と運用実験を 3 年間に渡り当該技術の応用可能性を実証した為、サイバーアクセスコントロールの有効且つ汎用的な手法として、推奨と普及を企図している。

5. 1:1 型の複数要素（生体）認証によるフィジカルアクセスコントロール

トータルアクセスコントロールのもう一側面として、リアル空間の IoT デバイス群を取り扱う操作者の「アクセス権限」に応じたフィジカルアクセスコントロールがあり、「他人へのなりすまし」を防ぐ為には 1:1 型の複数要素（生体）認証が有効である事を具体的に述べる。

先ず、生体認証は元来、カードやトークンデバイス等による本人認証方式では、なりすましが可能で、また貸しによるセキュリティホールが課題として指摘された為、生体認証が脚光を浴びた経緯がある。それにも関わらず、利便性重視の視点から「顔認証」に代表される通り ID を入力しなくて済む 1:N 型の生体認証が市場に出回っている。この現実から憂慮される点は、他人の空似によるなりすましが偶発してしまうリスクが十分あり、システムに登録された人数が多いほどそのリスクは高い。

1:N 型の生体認証ではセキュリティホールが予め明らかに存在するので、利便性よりもセキュリティ性を重視する上では、ID を入力した上で 1:1 型の生体認証を行うべきである事を力説しておきたい。

また、生体認証は元来、寒暖の差や体のむくみ等、本人であるにも関わらず本人の生体データが変化する性質を持っている為、本人であっても認証出来ないケースも多く、認証を司るセンサー自体の感度を低めて運用する事で日常的な変化を吸収する運用が現実的である。この為、上記の課題同様に、セキュリティ性を重視するには単一生体認証だけでは、なりすましを高次元で防御する事は難しいので最低でも ID 即ち PIN（Personal Identification Number）を打って 1:1 型の認証を行うか、複数要素の認証方式と組み合わせる事が必要である。

SYNCHRO では、19 年間に渡って特許を含めた 1:1 型の複数要素（生体）認証方式を完成させており、高次元のフィジカルアクセスコントロールを実現する認証方式として、推奨と普及に努めている。

6. トータルアクセスコントロールを体現したシステム「コンシェルネット」

サイバー空間からの中間者と、リアル空間での他人による「なりすまし」の両側面を防御すべき重要な環境の代表格として、住環境をターゲットに高次元のセキュリティ機能を具備したトータルアクセスコントロールを設計に盛り取り込んだコンシェルネットシステムが完成している。

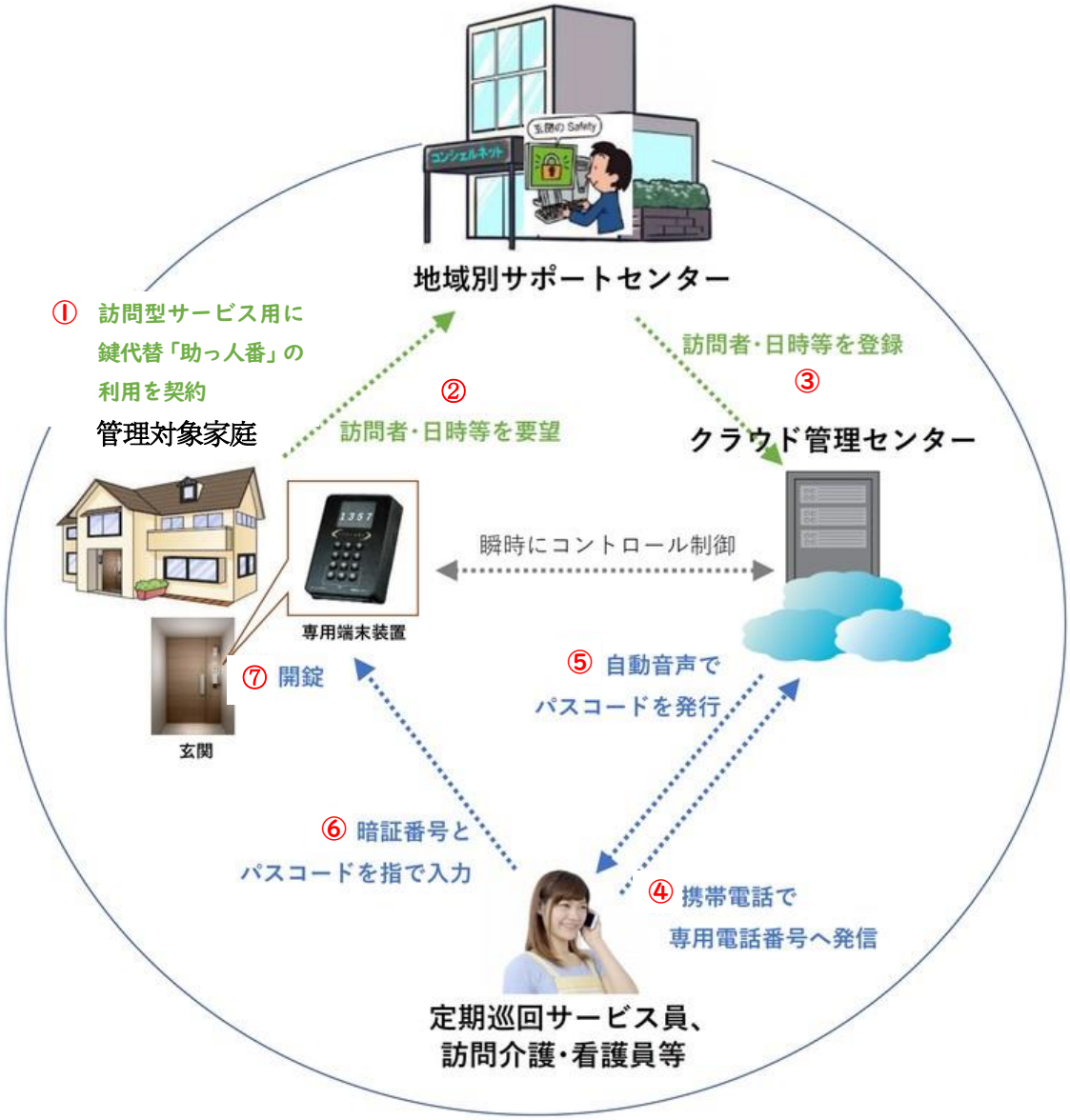

図　コンシェルネットの運営概念

図にコンシェルネットの運営概念を示す。管理対象家庭には、介護・看護等を必要とする寝起きの不自由な人が住んでおり、そこへ定期巡回サービス員が訪問する。正当な訪問者だけが適切にドアを解錠できる様、地域別サポートセンターはクラウド管理センター下の「コンシェルネット」を介して、管理対象家庭の要望に応じた入室管理を行い、利用者に安心感を与える人間中心の情報システムである。

情報の伝達順序を丸で囲った番号で示す。

管理対象家庭は最初に契約を行う。サービスの始動は、管理対象家庭が行う②訪問者・日時等の要望である。その情報は地域管理センターとクラウド管理センターで共有される。一方、定期巡回サービス員等は、クラウド管理センターに携帯電話で発信④、⑤及び⑥の順序で暗証番号とパスコードを入手し、専用端末装置を操作して解錠する。

この過程の重要な点は、音声伝達されたワンタイムパスコードを耳で聞いた定期巡回サービス員が、自らが覚えている暗証番号と共に端末（テンキー）に手打ちすることである。このようにして、契約された日時のみ、物理的ないし電子的な鍵を使わず、携帯電話だけで玄関を開錠し、安全に入室する事が可能となる。利用者である家庭には、キーレスによる利便性と安心感が醸される。

以上に述べた、コンシェルネット開発の背景と経緯を述べておきたい。

もともと、SYNCHRO は、ドア鍵を用いずに入室をアクセスコントロールする静脈認証装置を世界で初めてネットワーク管理する過程でノウハウを研鑽した結果、高次元の安全性をより安く実現する為に BD-Net と言う「フィジカルアクセスコントロール」の独自手法を考案・特許化した。

また、B2B 用途では、誰が・何時・何処のドアを開けられる様にするかを遠隔管理する事は一般的であるが、B2B2C 環境である住宅では、住宅毎に管理サーバを設備投資し、維持管理を行う事自体非現実的である為、クラウド側からアクセス権限を付与できる機能を採択した。

更に、複数要素で 1 : 1 認証を安く実現する必要性から、高価な静脈認証方式から離れて、携帯電話を用いて音声パスコードを認証手段として伝達する方法を採択した。

そして、最終的に認証する環境が雨ざらしである屋外玄関にも対応できる仕様とする為、認証端末は防水型で安く実現できるワンタイムパスを打ち込む為のテンキーを設計し、試作を終えた。

一方、本認証端末ほかシステム構成全般が IoT デバイスである観点に立ち、遠隔から権限を付与する認証用データの通信や、アクセスログを遠隔側にデータ収集して保存管理できる機能が中間者によって脅かされる事を防御する事を絶対条件化し、前述の KATABAMI 暗号化通信機能も組み込んだ。

以上の通り、図に示した構成要素の全てを俯瞰して、セキュリティホールの無い訪問許可者による玄関入室時の安全性を高めた「コンシェルネット」システムの試作を完成し、IEC62443 に準拠した IoT システムである事を国内でいち早く第三者評価を受ける準備と発表を整えている。

2021 年度、量産を見据えた商品化によって普及活動を行い、トータルアクセスコントロールの重要性と実現手法の拡散に臨み、現代の IoT 社会に内在するセキュリティ課題の解決活動に尽力したい。

7. おわりに

インターネットに様々なモノ（製品）が繋がる IoT の普及下では、製品自体が製造される段階から、セキュリティへの耐性を備えた構造にしておかなくては、後から取り繕う事では防ぎきれないとの認識がようやく広がり始めた。

この様な中、筆者が経営する SYNCHRO では、Security by Design のスローガンを掲げ、産業機器全般製品として設計される段階からセキュリティへの耐性を備えさせて製造されるべきであるとの協議会の発起人である辻井先生の理念に賛同し、2017 年 4 月に設立された Secure IoT Platform Organization の発起から加わって活動をしている。

活動 4 年目にあたる今年、自ら開発したコンシェルネットを評価対象に推薦して頂き、制御システムのセキュリティ全レイヤーとクラウドサービスプレーヤー迄をカバーした規格 IEC62443-4 シリーズに準拠したベンダーとなるべく、IoT 製品の安全基準を満たす仕掛けを具備している事を現在、客観評価を受けている。

元来、SYNCHRO が提供する製品が認証装置であると言う性も手伝って、インターネット接続状態でエンドツーエンド暗号化通信方式を採用していなければ中間者なりすましが防げず、フィジカルな認証自体を根本から無効化してしまうリスクに晒らされ、元も子もなくなる事を防御する必要性があった。

この様な着想から、本論文で例示した「コンシェルネット」システムは、日本でも先陣を切って IEC62443-4 の規格に準拠していると言えると考えているが、日本には認証機関がないため、現段階ではお墨付きは得られていない。

しかしながら、今後 IoT が増々普及していく事が明らかな今、フィジカル空間とサイバー空間の双方の側面で認証制御によって高次元のセキュリティ耐性を備える事が出来ている実績として世に示し、IoT デバイスの手本となり、IoT セキュリティの底上げに貢献できると考える。

今後も継続的に、トータルアクセスコントロールの概念を具体的な製品シリーズ拡充によって世に示し、IoT 社会の健全化に努める所存である。

謝辞　2017 年から住宅へのアクセスコントロールサービス創発を掲げて提案を行い、2019 年 1 月から革新的サービス事業化支援を東京都から助成され、2020 年末に製品化試作を終える段階にある今、本予稿論文をもって発表を行える事に応援を頂いた全ての関係者に対し、感謝を申し上げる。