一般論文

# オンライン資格確認向け三菱通信ゲートウェイ“smartstar”

横里純一* Junichi Yokosato
名取英男* Hideo Natori
松坂孝一郎* Koichiro Matsuzaka
泉　裕作* Yusaku Izumi
佐藤浩司* Koji Sato

*Mitsubishi Communication Gateway "smartstar" for Health Insurance Online Confirmation*

**要　旨**

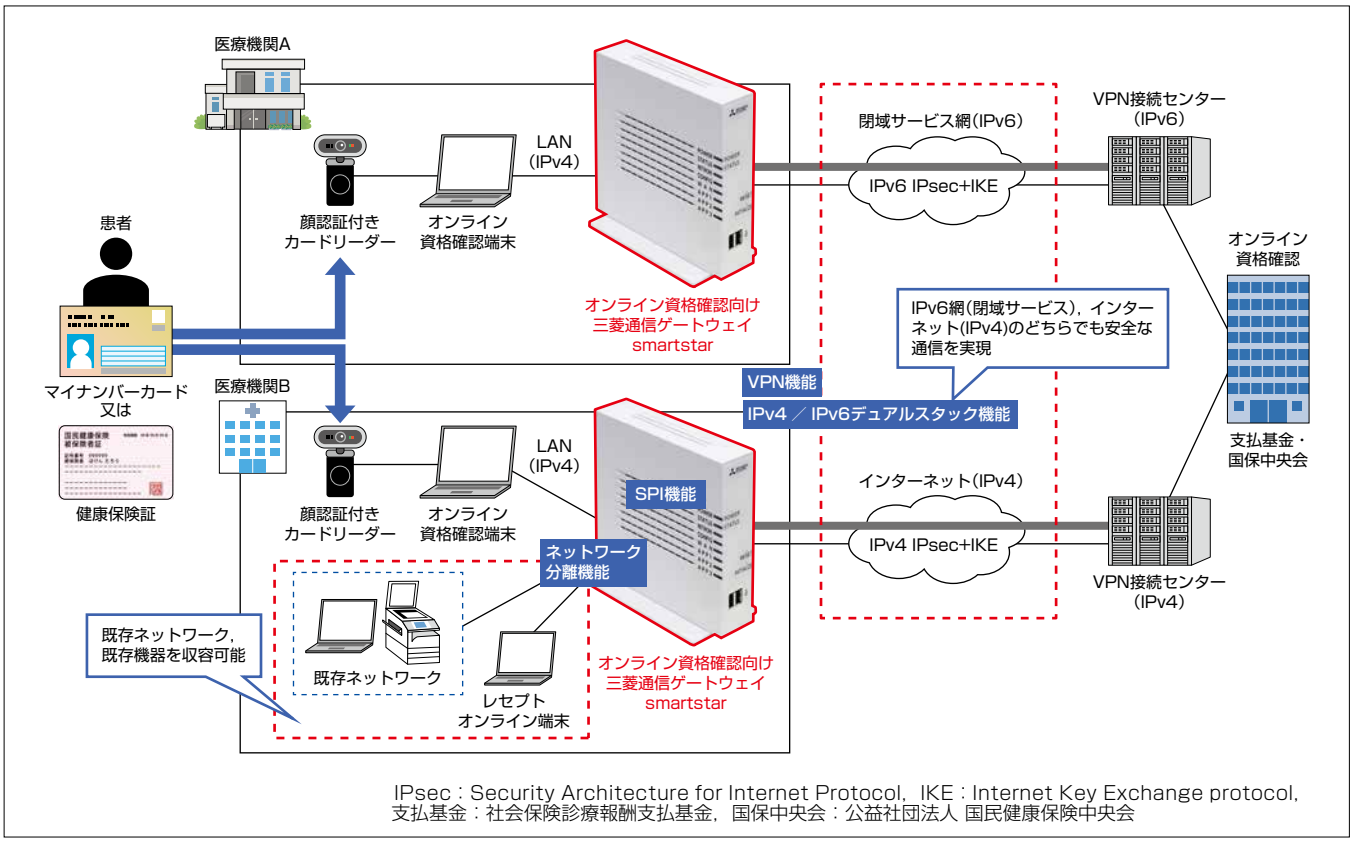
厚生労働省が主導するオンライン資格確認に対して，安全なネットワーク接続環境を提供するオンライン資格確認向け三菱通信ゲートウェイ“smartstar”を開発した。オンライン資格確認は，マイナンバー(注1)カード等を利用し，医療機関・保険薬局が患者の健康保険資格情報をオンラインで確認できるサービスで，2021年10月から本格運用を開始している。この装置は，2017年に開発したIoT(Internet of Things)システム対応三菱通信ゲートウェイsmartstarをベースに，オンライン資格確認向け機能を追加することで，厚生労働省の定める各種ガイドラインのセキュリティ要件を満足した上で，既存ネットワークとの共存を実現させた。この装置の主要な機能を次に示す。

(1)　VPN(Virtual Private Network)機能
(2)　IPv(Internet Protocol version)4／IPv6デュアルスタック機能
(3)　SPI(Stateful Packet Inspection)機能
(4)　ネットワーク分離機能

(1)と(2)で，閉域サービス網(IPv6)，インターネット(IPv4)のどちらのネットワーク経由でも医療機関・保険薬局を安全にオンライン資格確認に接続する。(3)で，LAN-WAN(Wide Area Network)間，LAN-LAN間の不正アクセスを防止する。(4)で，LAN側はポートごとに独立したサブネットを割り当てて，既存ネットワークを一つのサブネットに収容可能にする。

三菱電機は，今後も通信機器に対するセキュリティ高度化を推進し，介護向けサービス等に事業を拡大していく。

(注1)　マイナンバーは，デジタル庁会計担当参事官の登録商標である。




IPsec：Security Architecture for Internet Protocol，IKE：Internet Key Exchange protocol，
支払基金：社会保険診療報酬支払基金，国保中央会：公益社団法人 国民健康保険中央会

**オンライン資格確認向け三菱通信ゲートウェイsmartstarを用いたシステムイメージ**

オンライン資格確認向け三菱通信ゲートウェイsmartstarは，VPN接続センターとの間に閉域サービス網(IPv6)経由又はインターネット(IPv4)経由のIPsec接続を行い，医療機関と支払基金・国保中央会間での安全なオンライン資格確認を実現する。

*コミュニケーション・ネットワーク製作所

## 1. ま え が き

2021年10月から本格運用が開始されたオンライン資格確認によって，マイナンバーカードを利用し，医療機関・保険薬局(以下“医療機関等”という。)が患者の健康保険資格情報をオンラインで確認できるようになった。

オンライン資格確認では，厚生労働省の定める“医療情報システムの安全管理に関するガイドライン”(1)，“オンライン資格確認等システムの導入・運用に係るセキュリティアセスメントに基づいたセキュリティ対策例”(2)に準拠した通信制御が必要である。

当社は，2017年に開発を完了したIoTシステム対応三菱通信ゲートウェイsmartstar(3)(以下“IoT向けsmartstar”という。)をベースに，オンライン資格確認向け機能を追加開発することで，先に述べたガイドラインに準拠した通信制御が可能なオンライン資格確認向け三菱通信ゲートウェイsmartstar(以下“この装置”という。)を開発した。

三菱電機インフォメーションネットワーク㈱は，この装置を採用したVPNサービス“MINDセキュアネットワークサービスSecureMinderオンライン資格確認”(4)をプレ運用として2021年１月から医療機関等向けに提供開始している。このサービスによって，必要とされる高度なセキュリティを確保の上，オンライン資格確認への接続が可能である。

本稿では，**２章**でオンライン資格確認向けのシステム要件を述べて，**３章**ではこの装置の主要諸元，**４章**ではオンライン資格確認向け主要機能について述べる。

## 2. オンライン資格確認向けのシステム要件

オンライン資格確認向けのシステムに求められるガイドラインに記載の主要なセキュリティ要件を**表１**の要件１～３に示す。

医療機関等の多くは，診療報酬(レセプト)のオンライン請求を利用しているため，既にインターネット回線や閉域サービス網(IPv6)回線を契約中であり，施設内にIPv4の既存ネットワークを敷設済みであることが多い。これらの施設でも既存設備を変更することなく，オンライン資格確認に接続可能にするため，セキュリティ要件に加えて，**表１**の要件４～５をシステム要件として追加した。

この装置を適用したオンライン資格確認への接続サービスのシステム構成例を**図１**に示す。

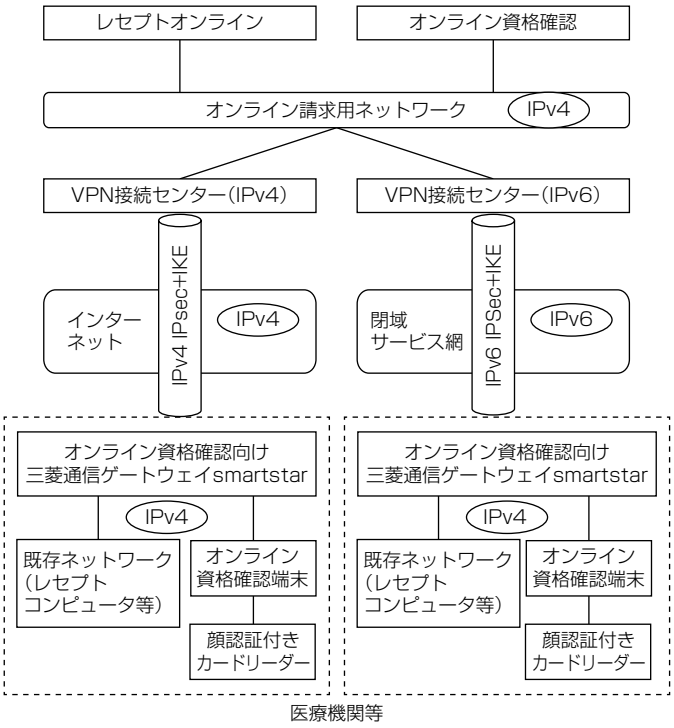



**図１．システム構成例**

## 3. この装置の主要諸元

**２章**で述べたシステム要件１を満たすため，IPsecの高速転送機能を持つ必要がある。このため，パケット転送処理と暗号化処理をCPUからオフロードするネットワークプロセッサを搭載した当社IoT向けsmartstarをベースにこの装置を開発した。これによってこの装置のIPsec転送能力は１Gbpsを実現する。

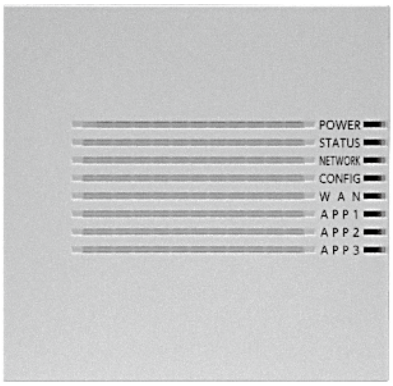
この装置の主要諸元を**表２**に，外観を**図２**(a)(b)(c)に示す。

**表１．この装置の要件**

| 要件No. | 内容 |
|---|---|
| 要件１ | IPsec＋IKEの利用や閉域網の利用等，ネットワーク経路でのメッセージ挿入，ウイルス混入等の改ざんを防止する対策を行うこと。 |
| 要件２ | ファイアウォールやルータのSPI機能を用いて，外部ネットワークからのアクセスを制限すること。 |
| 要件３ | セキュリティ要件の異なるシステム間や安全管理上の重要部分との境界にはファイアウォール等を設置し，ネットワークを物理的又は論理的に分割すること。 |
| 要件４ | 医療機関等が既契約中のインターネット(IPv4)や閉域サービス網(IPv6)を継続利用可能なこと。 |
| 要件５ | 医療機関等内の既存IPv4ネットワークを収容し，レセプトオンライン請求を利用可能なこと。 |

**表２．この装置の主要諸元**

| 項目 | 内容 |
|---|---|
| WAN端子 | 1000BASE-T／100BASE-TX　１ポート |
| LAN端子 | 1000BASE-T／100BASE-TX　４ポート |
| LED(装置状態表示用) | LED ８個(うち１個がVPN状態表示用) |
| 電源<br>(付属の<br>AC-DC変換アダプタ) | 入力電圧／周波数：AC100V±10V，<br>50Hz／60Hz±1Hz<br>出力電圧 DC12V±5%<br>定格電流 1.5A |
| 消費電力 | 15W以下 |
| 外形寸法(mm) | 40(W)×168(H)×172.9(D) |
| 質量 | 0.5kg以下 |
| IPsec同時接続数 | 最大16対地 |




(a) 側面


(b) 前面


(c) 背面

**図2．この装置の外観**

## 4．オンライン資格確認向け主要機能

IoT向けsmartstarをベースに，**2章**で述べた五つの要件を実現した。**表3**に**2章**で述べたシステム要件と実現機能との相関を示す。各機能は○印の要件を実現している。

### 4.1 VPN機能

この装置は高いセキュリティ性を確保するためにVPN機能として次の機能を持っており，**2章**で述べた要件1，4，5を実現している。

(1) IPsec＋IKEによる暗号通信
(2) PFS(Perfect Forward Secrecy)による安全性の高い暗号鍵生成

**表3．システム要件と実現機能との相関**

| 要件 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| ①VPN機能 | ○ | | | ○ | ○ |
| ②IPv4／IPv6デュアルスタック機能 | | | | ○ | ○ |
| ③SPI機能 | | ○ | ○ | | |
| ④ネットワーク分離機能 | | | ○ | | ○ |

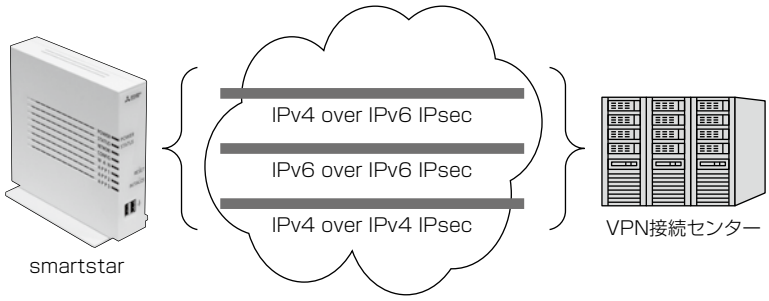



**図3．この装置が対応可能なIPsecのパターン**

(3) DH(Diffie-Hellman)グループ14による安全な鍵交換
(4) クライアント証明書とCA(Certificate Authorities)証明書のSHA-256(Secure Hash Algorithm 256bit)対応によるセキュリティ強化
(5) 通信発生時だけVPN接続を行うオンデマンド接続によるセキュリティ強化

### 4.2 IPv4／IPv6デュアルスタック機能

この装置はIPv4／IPv6デュアルスタックによって，接続回線のIPプロトコルのバージョンに合致したIPsec＋IKE通信路を構築し，end-to-endの通信を実現している。

**図3**にデュアルスタック機能によってこの装置が対応可能な3種類のIPsecのパターンを示す。この機能によって**2章**の要件4，5を実現している。

### 4.3 SPI機能

この装置は，LAN-WAN間だけでなく，LAN-LAN間のパケット転送に対してもSPI機能を提供し，各ポート間の不正アクセスを防止する。これによってLAN-WAN間及びLAN-LAN間で，通信が禁止されている方向からの通信の場合でも，通信が許可されている方向へのリクエストに対するレスポンスは，送信可能になる。通信可否のフィルタ設定は，リクエスト方向の通信条件(通信方向，プロトコル，ポート番号)だけを設定すればよい。この機能によって**2章**で述べた要件2，3を実現している。

### 4.4 ネットワーク分離機能

この装置は，LAN側4ポート，WAN側1ポートを持っている。LAN側はポートごとに独立したサブネットを割当て可能であり，これによって医療機関等の既存ネットワークを一つのサブネットに収容可能にする。

**表4**にLAN側に四つのサブネットを設定した例を示す。ここで，LAN1～LAN4／WANはポートV(Virtual)LANで分離し，トラフィックに対するフィルタ設定によって，ポート間のアクセス制限を実現している。

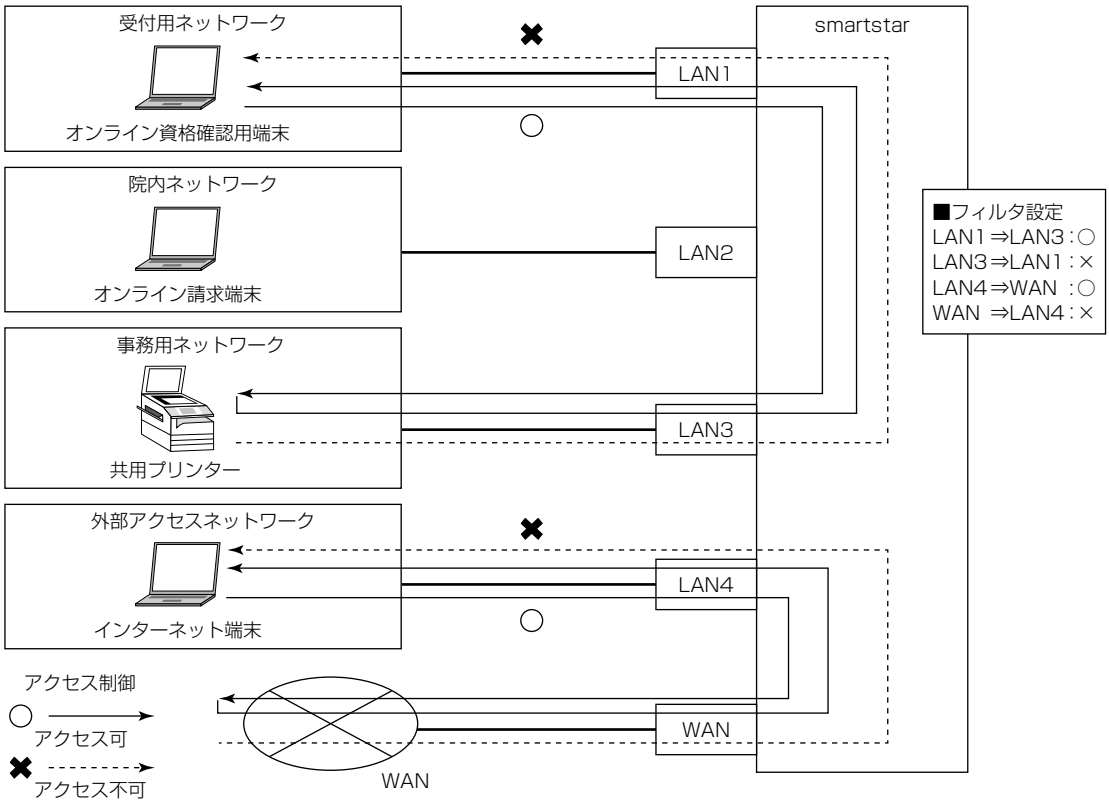



**図４．SPI機能によるアクセス制御及びネットワーク分離**

**表４．サブネット構成例**

| サブネット | 接続ネットワーク |
|---|---|
| LAN１ | 受付用ネットワーク<br>（オンライン資格確認端末を含む） |
| LAN２ | 院内ネットワーク<br>（オンライン請求端末を含む） |
| LAN３ | 事務用ネットワーク<br>（共用プリンター等のOA機器を含む） |
| LAN４ | 外部アクセスネットワーク<br>（インターネット端末を含む） |

**図４**に，**表４**のサブネット構成での，SPI機能によるアクセス制御の例を示す。**図４**では，LAN１からLAN３方向はアクセス可，LAN３からLAN１方向はアクセス不可に設定している。そのため，オンライン資格確認端末から共用プリンターへの印刷処理通信を行った場合，共用プリンターからオンライン資格確認端末への応答通信は可能である。一方，直接，共用プリンターからオンライン資格端末への通信は抑止される。なお，プロトコル(TCP(Transmission Control Protocol)／UDP(User Datagram Protocol))とport番号を指定することによって，共用プリンターでスキャンしたドキュメントを直接オンライン資格確認端末に送信することを，限定的に許可することが可能である。

このように，WAN側，LAN側のネットワーク設備，端末に対するアクセス制御を柔軟に設定可能になり，**２章**で述べた要件３，５を実現している。

## ５．む　す　び

厚生労働省は，オンライン資格確認に加えて，処方箋の電子化についても2023年の運用開始に向けて準備を進めており，医療データのオンライン化は加速していく。さらに，健康，介護の各分野のデータとの連携も検討されている。

当社は，今後も通信機器に対するセキュリティ高度化を推進し，事業を拡大することでデータヘルス改革に貢献していく。

### 参　考　文　献

(1) 厚生労働省：医療情報システムの安全管理に関するガイドライン第5.1版（2021）
https://www.mhlw.go.jp/content/10808000/000730541.pdf
(2) 厚生労働省保険局：オンライン資格確認等システムの導入・運用に係るセキュリティアセスメントに基づいたセキュリティ対策例（2021）
https://www.mhlw.go.jp/content/10200000/000738078.pdf
(3) 大野聖信，ほか：IoTシステム対応三菱通信ゲートウェイ，三菱電機技報，**91**，No.6，325～328（2017）
(4) 武田　哲，ほか：医療保険のオンライン資格確認に対応したMINDセキュアネットワークサービス“SecureMinder”，三菱電機技報，**95**，No.8，518～521（2021）