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”

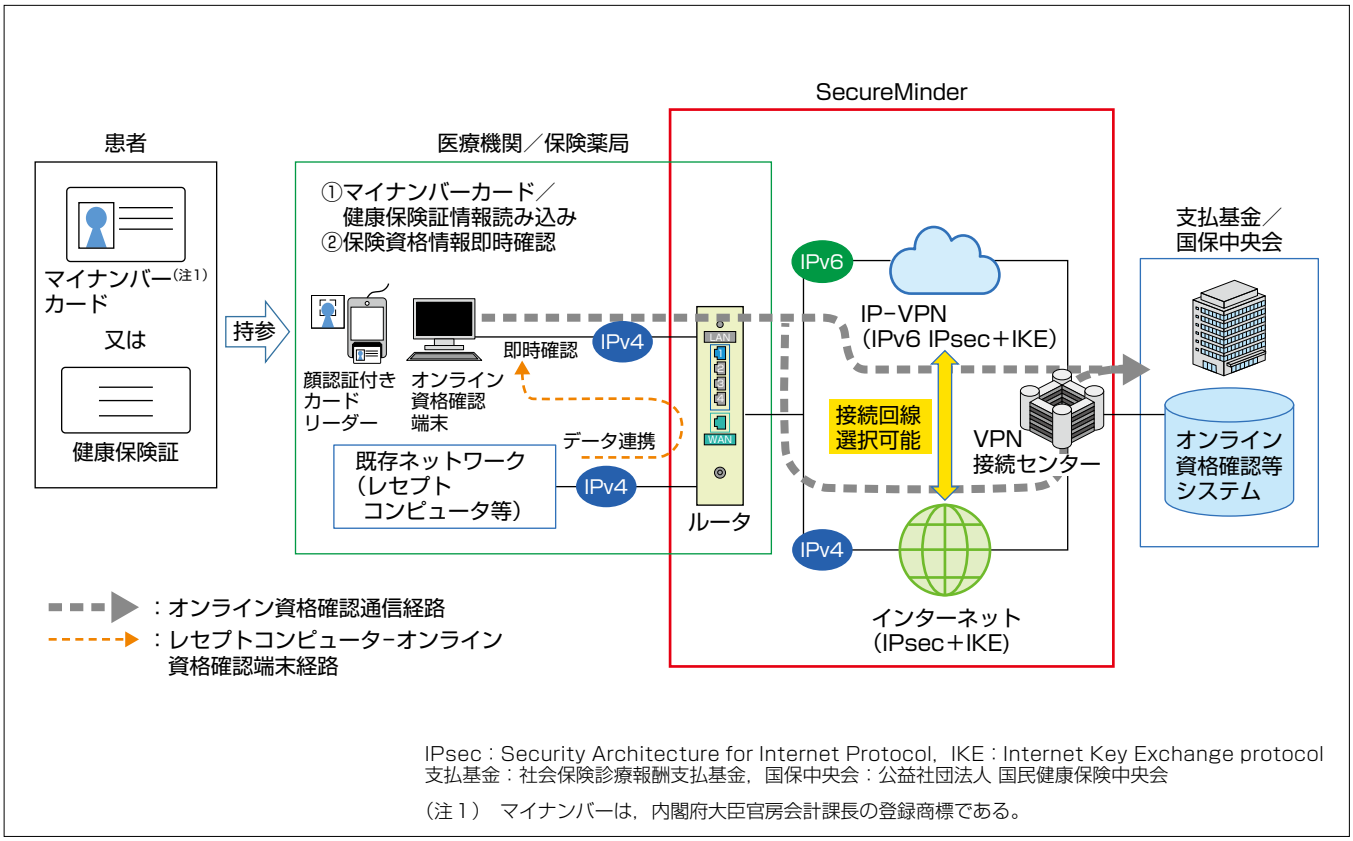
武田　哲*
Satoshi Takeda
仲村渠　剛*
Takeshi Nakandakare
北井孝生*
Kosei Kitai
松坂孝一郎†
Koichiro Matsuzaka
濱口雄人†
Yuto Hamaguchi

MIND Secure Network Service "SecureMinder" Corresponding to Medical Insurance Online Confirmation

要　旨

2021年３月からプレ運用が開始された医療保険のオンライン資格確認（以下“オンライン資格確認”という。）で，保険資格の有効性を即時に確認できるようになった。

三菱電機インフォメーションネットワーク㈱（MIND）ではオンライン資格確認の開始に合わせて，2021年１月から医療機関や保険薬局向け新VPN（Virtual Private Network）サービスMINDセキュアネットワークサービス“SecureMinder”の提供を開始した。SecureMinderは厚生労働省が定める各種ガイドラインに準拠し，オンライン資格確認に求められるセキュリティ要件を満たしている。また医療機関や保険薬局では資格確認端末用ネットワークと既存ネットワークをルータ１台に集約し，接続回線がIPv6（Internet Protocol version 6）ネットワークのIP（Internet Protocol）－VPNの場合であっても，施設内をIPv4ネットワークで構成することが可能であり，既存ネットワークとの円滑な連携を実現する。さらにインターネットとIP－VPNの２種類の接続回線をサポートすることで，多種多様な環境に合わせて導入することが可能である。これによって，顧客の設備環境を活用したオンライン資格確認のいち早い導入を支援する。MINDは今後もセキュリティ要件を満たしたネットワークサービスを提供することで，医療情報の迅速かつ効率的な利活用を下支えし，社会に貢献していく。



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

（注１）　マイナンバーは，内閣府大臣官房会計課長の登録商標である。

マイナンバーカード／健康保険証を用いた医療保険のオンライン資格確認のイメージ

医療機関や保険薬局から医療保険のオンライン資格確認を利用するため，SecureMinderは支払基金や国保中央会にあるオンライン資格確認等システムに接続するVPNサービスを提供する。

*三菱電機インフォメーションネットワーク㈱
†三菱電機㈱ コミュニケーション・ネットワーク製作所

1. ま え が き

オンライン資格確認はマイナンバーカードの普及と利活用の促進策の一つで，マイナンバーカードを健康保険証として利用できるようになった。政府が医療機関や保険薬局での導入を支援しており，急速な普及が予想される。

MINDではこれまで，2007年に開始された診療(調剤)報酬明細書のオンライン請求(以下“オンライン請求”という。)向けにインターネットVPNサービス“MINDセキュアネットワークサービス”を提供してきた実績があり，オンライン資格確認についてもオンライン請求用ネットワークを利用する厚生労働省の方針を受けて新サービスを企画・開発し，オンライン資格確認の開始に合わせて新サービス“SecureMinder”の提供を開始した。

2. SecureMinderの三つの特長

⑴ 高度なセキュリティ要件を最小構成で実現

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”の準拠に加えて，“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”[1](以下“セキュリティ対策例”という。)で示されているアセスメント結果に基づいた推奨構成を三菱電機製の１台のルータで構築することを実現した。これによって，医療機関や保険薬局(以下“医療機関等”という。)では複数のルータを準備する必要がなくなり，オンライン資格確認対応へのコスト削減が可能になる。

⑵ ２種類の接続回線から選択可能

医療機関等の多くはオンライン請求を利用中で，既にインターネット回線やIP-VPN回線を契約しているのでSecureMinderではインターネットとIP-VPNの２種類の接続回線に対応し，契約中の回線を継続利用できるようにした。

⑶ 施設内ネットワークとの円滑な連携を実現

オンライン資格確認では，健康保険証の資格確認ができるだけでなく，特定健診情報，薬剤情報，医療費情報等をオンライン資格確認端末(以下“資格確認端末”という。)に取り込むことが可能になる。取り込んだ情報は医療機関等の施設内の既存ネットワークにあるレセプトコンピュータ(診療(調剤)報酬明細書を作成するコンピュータ)等と連携することで，データの利活用が可能になる。医療機関等の施設内はIPv4ネットワークで構成されている場合が多く，一方で資格確認端末の接続回線がIP-VPNの場合，IPv6ネットワークのフレッツ・キャスト(注2)であることから，施設内では既存のIPv4と接続回線のIPv6のネットワークが混在した環境になり，これに対応する機器構成が複雑になることが課題となる。この課題を解決するため，SecureMinderでは接続回線がIPv6のネットワークであっても施設内にある端末やシステムをIPv4ネットワーク構成のルータ１台に集約し，施設内の既存ネットワークと資格確認端末との円滑な連携を可能にした。また以前から行われているオンライン請求も利用可能である。

(注２) フレッツ・キャストは，東日本電信電話㈱及び西日本電信電話㈱の登録商標である。

3. システム機能

3.1 システム要件

オンライン資格確認の導入に当たっては，厚生労働省でオンライン資格確認等システムが提供する機能，及び医療機関等のシステムベンダーが実装すべき要件及び対策例が，**２章**に述べたセキュリティ対策例に提示されている(**図１**)。

セキュリティ対策例でのシステム要件(接続事業者向け要旨)は次のとおりである。

⑴ T11：IPsec＋IKEの利用や閉域網の利用等，ネットワーク経由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。

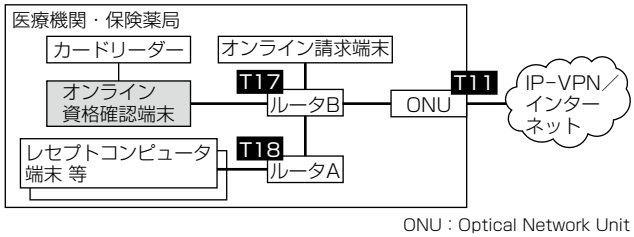
⑵ T17：ファイアウォールやルータのステートフルパケットインスペクション機能を用いて，外部ネットワークからのアクセスを制限すること。

⑶ T18：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。

3.2 システム構成

従来のオンライン請求向けのシステム(以下“インターネットVPN用システム”という。)では，VPN接続センター内に設置されたVPNゲートウェイに対して，医療機関等に導入されたルータでインターネットを介してVPN接続を行い，オンライン請求用ネットワークへ安全にアクセスできる(**図２**)。

一方，オンライン資格確認の開始に合わせて構築した新システム(以下“IP-VPN用システム”という。)はフレッ



ONU：Optical Network Unit

図１．システム要件を満たす構成例

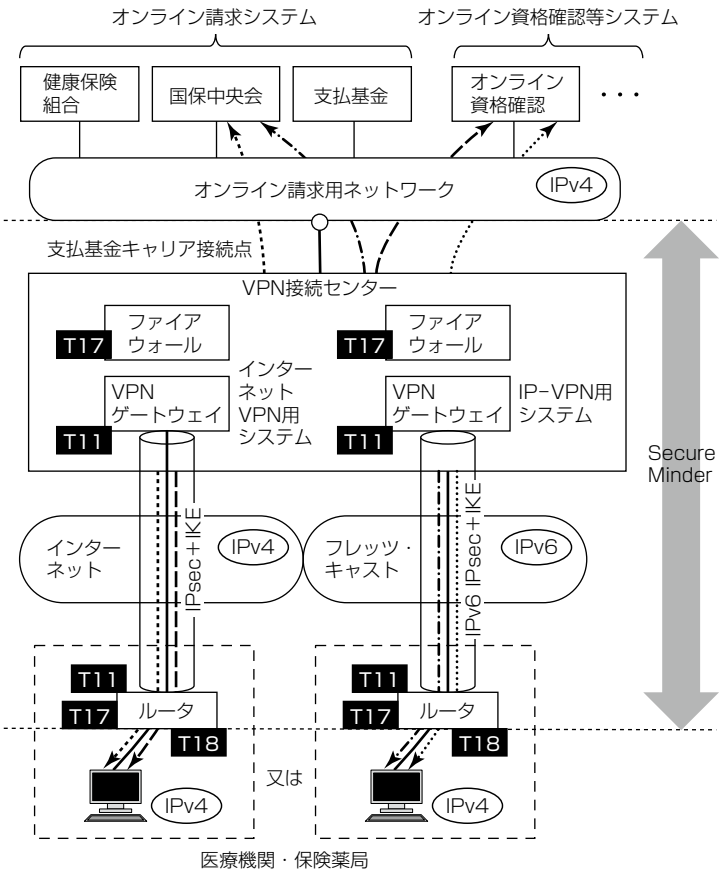


図2．システム構成

ツ・キャストのIP-VPN網を利用する。ルータでIPv6ネットワークのフレッツ・キャストを介してVPNゲートウェイへVPN接続を行い，オンライン資格確認のネットワークへ安全にアクセスできる。医療機関等は，自身の接続回線環境に合わせて，VPNシステムを選択可能になる。

3.3　VPN接続センター

システム要件を満たすために，VPN接続センターでは，主に次の二つの機能を実装している。

3.3.1　VPN機能

IP-VPN用システムでは，医療機関等からVPN接続センターへのアクセスはIP-VPN網を介して行われる。そこで，医療機関等からVPN接続センター間をIPv6 IPsecで暗号化と認証を行い，医療機関等の施設内ネットワークからオンライン請求用ネットワークへのIPv4通信をIPv6 IPsec＋IKEトンネル上に通すことで，医療機関等の構成を変更することなく，オンライン資格確認等システムへの安全なアクセスを実現している(T11要件)。

3.3.2　アクセス制御機能

医療機関等からのオンライン資格確認等システムへの通信については，アクセス制御等を行うためにVPN接続センター内にファイアウォールを導入している。ファイアウォールのステートフルパケットインスペクション機能によって，送信元／宛先IPアドレスと通信プロトコルのルールセットに基づいて，特定通信だけを通過させる制御を行っている。

また，オンライン資格確認等システムへのアクセスは機関ごとにユニークなIPアドレスによるアクセスが必要になるが，機関ごとに独自のネットワークを構成していることから，IPアドレスの重複が想定される。そこで，ファイアウォールのアドレス変換機能を使用し，各機関へユニークなIPアドレスを割り当てる変換を行う。変換用のIPアドレス数が限られている中で多くのアクセスが可能になるよう，NAPT(Network Address Port Translation)機能で必要なIPアドレス数を節約して実現している。

またオプション機能として特定のインターネットサイトへのアクセスを可能にし，医療機関等でVPN接続中の端末のセキュリティソフトウェア更新などを行うことができる(T17要件)。

3.4　ルータ

オンライン資格確認等システムの利用に当たって，医療機関等は，**3.1節**に述べた厚生労働省のガイドラインに要求されるセキュリティ対策への対応が必要になる。ルータを設置することで，医療機関等は，このセキュリティ対策要求に適合したSecureMinderの安全かつ安定した接続環境を利用できる。ルータには，三菱通信ゲートウェイ“smartstar(XS-5N-01)”を採用している。

3.4.1　IPsecルータ機能

smartstarではL2L(LAN-to-LAN)でのIPレイヤのセキュリティとして，IPsec＋IKEによる暗号通信を行い，第三者による盗聴と改ざん防止を図っている。暗号通信ではIPsec SA(Security Association)，IKE SA単位でPFS(Perfect Forward Secrecy)を有効化しており，鍵更新での鍵の再利用は行わず，安全性の高い鍵生成を実現している。また，鍵交換では，DH(Diffie-Hellman)グループ14まで対応しており，セキュリティ強度向上を実現している。さらに，複数拠点(L2L)とのIPsec＋IKEの通信路構築は，同時並行かつオンデマンドで実現しており，常時接続で構築する場合に比べて，外部ネットワーク上でのIPsec＋IKEのトラフィックを抑制している。さらに，クライアント証明書と認証局証明書には強度の高いSecureMinder用のSHA-256(Secure Hash Algorithm 256bit)電子証明書を搭載しており，ルータのなりすまし(偽装)防止を図っている(T11要件)。

3.4.2　IPv4／IPv6デュアルスタック機能

医療機関等での接続回線がインターネット(IPv4)か，IP-VPN網(IPv6)のどちらかにかかわらず，IPsec＋IKEの通信路がIPプロトコルのバージョンの差異を吸収することで，E2E(end-to-end)の通信，すなわち，資格確認端末とオンライン資格確認等システム間の通信は，IPv4通信だけにすることを可能にしている(**図2**)。IPsec＋IKEの通信路構築では一つのIPsec SAに異なる宛先ネットワークへの通信を収容することでVPN接続センター内に設置されたVPNゲートウェイのIPsec利用リソースを最適化するとともに，支払基金ネットワークでの既存設備を維持しながらルータを導入できる。

3.4.3　マルチポートルータ機能

LAN側には4ポート，WAN(Wide Area Network)側には1ポートを具備しており，LAN側にはポートごとに独立したサブネットを割り当てできる。WAN側とLAN側のネットワーク設備と端末に対するアクセス制御を柔軟に設定できるため，医療機関等の既存ネットワーク設備へ必要になる設定変更を少なくできる(T18要件)。

3.4.4　ステートフルパケットインスペクション機能

LAN間，LAN-WAN間のパケット転送では，ステートフルパケットインスペクションを利用し，上り通信が生じた場合に対応する下り通信のポート開放を制御する。下り通信のポート開放は上り通信中に限定できるため，高度なアクセス制御が可能になるとともに，上り通信条件(通信方向，プロトコル，セッション情報)の設定に注力できる。これに基づいて，医療機関等の施設内にあるオンライン請求端末から外部ネットワークへの通信と，医療情報システムから資格確認端末へのアクセスを1台のルータだけで実現している(**図3**)(T17，T18要件)。

3.4.5　リモートメンテナンス機能

電子証明書の更新，ファームウェアの更新，コンフィグレーションの変更を，ユーザーによる操作なしに，Secure-Minderのリモートサーバからオンラインで実施可能である。リモートサーバとの通信でも，IPsec＋IKEの暗号通信を用いて自動的に行う仕組みを設けることで，運用の効率化やトラブルへの迅速な対応を可能にしている。

3.5　運用支援機能

運用支援機能は，申込み情報，顧客情報，ルータであるsmartstarの構成・設定情報などを一元的に管理し，運用開始時・運用中の顧客への安定したサービス提供を実現する。運用開始時では，smartstarへの設定を自動化するとともに，機器ごとの作業内容や作業ログを残すなどによって作業漏れ防止策を講じることで，顧客が円滑にサービスを利用できるよう工夫した。また，運用段階では，障害発生等によってルータ交換が必要になった場合，現地交換機器に対して遠隔で設定を送り込み，障害発生時のスムーズな復旧処理を支援できる機能も実現した。

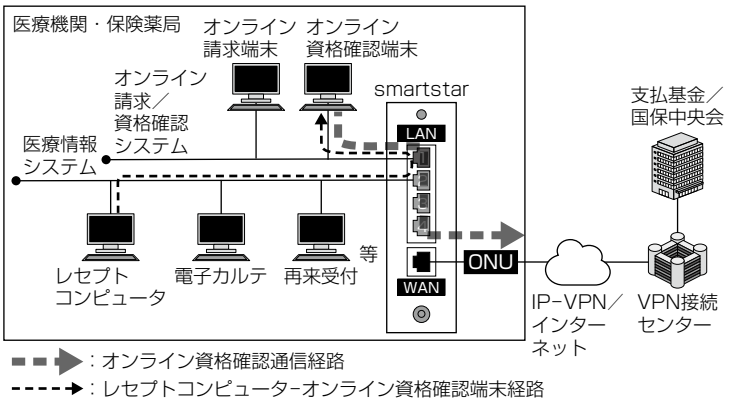


図3．smartstarの設置例

今後24時間365日対応できるサービスメニューを増やし，更なる顧客の利便性向上を目指す。

4．今後の取組み

現在，厚生労働省では“新たな日常にも対応したデータヘルスの集中改革プラン”で，2020年7月から2年間で三つのACTIONを集中的に実行するプランを掲げている。この中で“ACTION2：電子処方箋の仕組みの構築”については，オンライン資格確認等システムを基盤として計画されており，ネットワークへの新たな要件や，ルータへの要件が出てくる可能性が考えられる。MINDではこれらの要件にいち早く対応し，電子処方箋への対応をスムーズに展開する。更に継続して医療DX(デジタルトランスフォーメーション)への対応を推進する。

5．む　す　び

今後ますます医療DXが進むことで，システム連携や情報共有が更に可能になり，医療機関等での業務効率化や患者の待ち時間軽減，診察や治療の円滑化の実現が期待される。

MINDは今後もセキュリティ要件を満たしたネットワークサービスを提供することで，医療情報の迅速かつ効率的な利活用を下支えし，社会に貢献していく。

参 考 文 献

(1)　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