特集論文

ヘルスケアセキュリティSaaSへの取組み

茗原秀幸*
長浜隆次**
田口拓也***

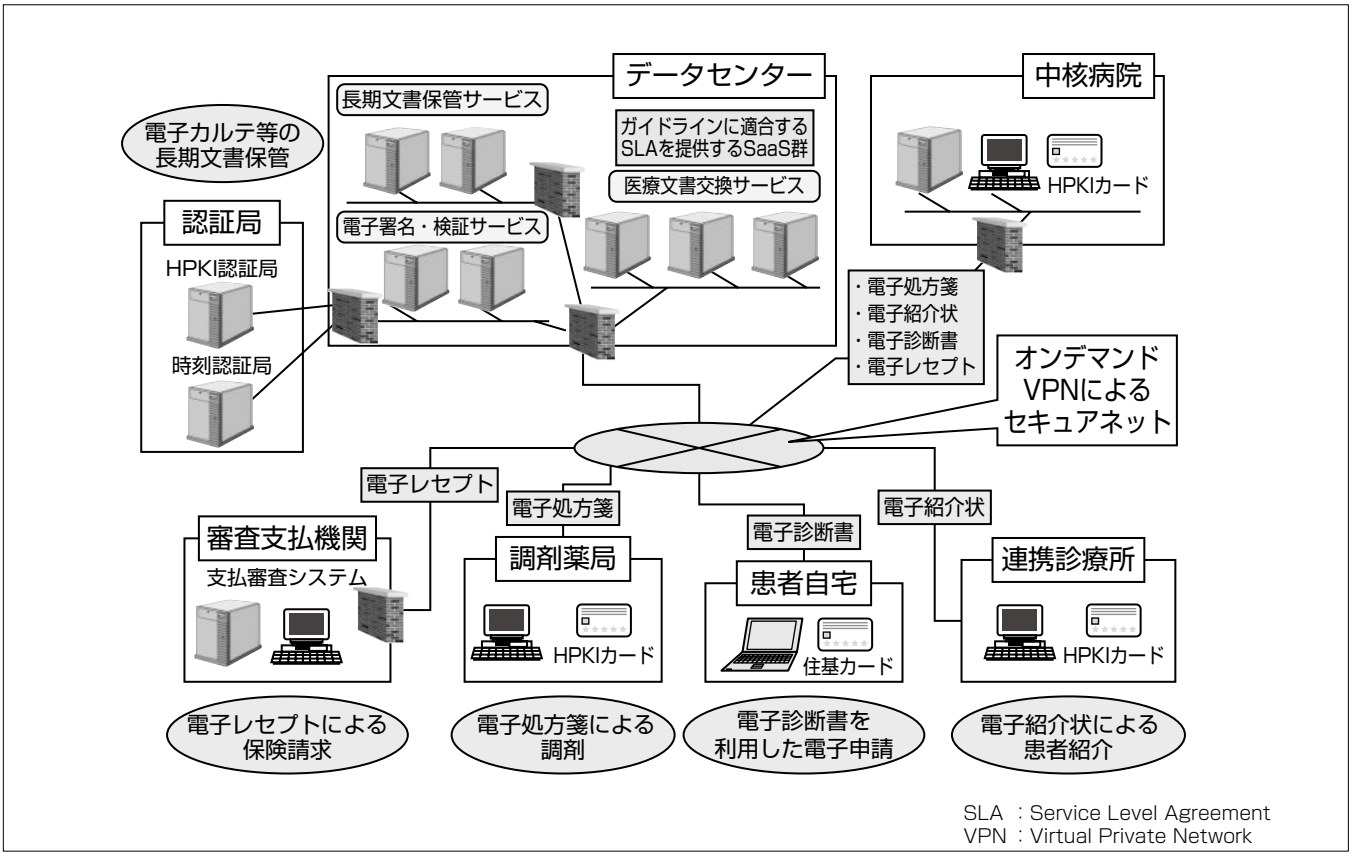
Our Activity on Healthcare Security SaaS

Hideyuki Miyohara, Ryuji Nagahama, Takuya Taguchi

要　旨

ヘルスケア分野では，機微な情報を取り扱うため，情報システムの管理・運用でも特段の配慮が求められる。医療機関等が遵守すべきガイドラインとして，厚生労働省が医療情報システムの安全管理に関するガイドラインを制定し，その遵守を求めている。これに対応し，医療機関などへのサービス提供を行う事業者に対しても，経済産業省及び総務省のガイドラインが制定された。三菱電機グループでは，これらの要求事項を遵守できる低コストのハイレベルセキュリティサービスを医療機関などに提供することを目指して，ヘルスケアセキュリティSaaS(Software as a Service)システムの構築と評価を実施した。構築に当たっては，職能団体の要求事項をヒアリングし，小規模な医療機関などでも簡単に利用可能なサービスとしての要件を明確化した。また，クラウド技術を適用し，①ハイレベルセキュリティを確保したIaaS(Infrastructure as a Service)，②PKI(Public Key Infrastructure)認証による成りすまし防止やID管理を適切に行うPaaS(Platform as a Service)，③これらの基盤上で，医療分野向けのガイドラインに適合した電子署名，検証サービスを提供するSaaSを構築した。

このシステムでは，厚生労働省が推進する署名用HPKI(Healthcare PKI)証明書や認証用HPKI証明書も利用可能な設計となっており，保健医療福祉情報システム工業会(JAHIS)策定のガイドラインに準拠したHPKI電子署名，HPKI認証基盤を提供することができる。今後は自社サービスのみならず，他社の提供するSaaSに対するIaaS，PaaSの提供や，SaaS間連携を実施し，医療情報分野に対するハイレベルセキュリティサービスを提供していく。



ヘルスケアセキュリティSaaSの概念図

医療情報における安心・安全を確保しつつ，円滑な医療情報交換や保存が義務付けられた医療情報の外部保存を行える環境を提供する。真正性を担保するための電子署名・タイムスタンプ付与をSaaSサービスとして提供した上で，電子署名付き文書の文書交換や外部保存に対応したサービスと連携し，ワンストップで地域医療連携のニーズにこたえることができる。認証や署名のフレームワークでは，HPKI環境が利用可能である。また，将来は住民基本台帳カードに格納された公的個人認証基盤との連携も視野に入れている。

*三菱電機㈱ 本社　**三菱電機インフォメーションシステムズ㈱　***ジャパンネット㈱

1. まえがき

ヘルスケア分野では，機微な情報を取り扱うため，情報システムの管理・運用でも特段の配慮が求められる。医療機関等が遵守すべきガイドラインとして，厚生労働省が医療情報システムの安全管理に関するガイドラインを制定し，その遵守を求めている。これに対応し，医療機関等へのサービス提供を行う事業者に対しても，経済産業省の“医療情報を受託管理する情報処理事業者向けガイドライン”，及び総務省の“ASP（Application Service Provider）・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン”が制定された。三菱電機グループでは，これらの要求事項を遵守できる低コストのハイレベルセキュリティサービスを医療機関等に提供すること目指して，ヘルスケアセキュリティSaaSシステムの構築と評価を実施した。

本稿では，ヘルスケア分野における要求事項とそれに対応したヘルスケアセキュリティSaaSの実装方式について述べる。

2. ヘルスケア分野の情報システムにおける要求機能

2.1 ガイドライン

厚生労働省の“医療情報システムの安全管理に関するガイドライン”（以下“ガイドライン”という。）では，インターネット経由での医療情報の送受信に対して，盗聴，セッション乗っ取りなどを防止する対策をとることが必要とされており，その中で次の例が明記されている。

①IPSec（Security Architecture for Internet Protocol）とIKE（Internet Key Exchange）の適用によるセキュアな通信路を確保すること

また，署名又は記名・押印が義務付けられた文書等で，記名・押印を電子署名に代える場合，次の②～④の条件を満たす電子署名を行う必要があると明記されている。

②厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

③電子署名を含む文書全体にタイムスタンプを付与すること

④上記タイムスタンプを付与する時点で有効な電子証明書を用いること

2.2 要求機能の整理

医療分野の情報システムにおける要求機能の検討に当たっては，**2.1節**のガイドラインをベースとし，職能団体の要求事項（次の(4)，(5)）も含め，次のように整理した。

(1) ガイドラインに準拠したセキュアなネットワーク上でのサービス（ガイドライン①に対応）

(2) 電子医療文書等への電子署名並びにタイムスタンプ付与サービス（ガイドライン②，③に対応）

(3) タイムスタンプ付き電子署名文書の検証サービス（ガイドライン④に対応）

(4) 医療機関（組織）並びに医療機関に所属する個人が識別可能な認証サービス

(5) 従量課金が可能な課金方式

3. SaaSサービスとしての要求機能

ヘルスケアセキュリティSaaSでは，小規模な医療機関等でも簡単に利用可能なサービスをねらいとし，ガイドラインに準拠したセキュアなネットワーク上で，高いセキュリティとアプリケーション基盤サービスを安価な料金で提供することを目標としている。

(1) ガイドラインに準拠したセキュアなネットワーク上でのサービス

ガイドラインで要求されるセキュリティ基準をクリアしているセキュアネットワークサービス（三菱電機情報ネットワーク㈱（MIND）が提供）をSaaSサービスのネットワーク基盤とし，セキュアネットワーク上にヘルスケアセキュリティSaaSポータルサイトを作成する。

(2) 電子医療文書等への電子署名並びにタイムスタンプ付与サービス

電子医療文書はPDFを想定し，PDF（Portable Document Format）への電子署名並びにタイムスタンプ付与サービスとし，電子署名機能及びタイムスタンプ付与機能を**表1**のように整理した。なお，性能については，クライアントレスポンスとして8秒以内とした。

(3) タイムスタンプ付き電子署名文書の検証サービス

タイムスタンプ付き電子署名PDFファイルをSaaSサービス上にアップロードして，電子署名並びにタイムスタン

表1．SaaSサービスとしての要求機能(1)

要求機能	内容
電子署名機能	・クライアントパソコン上のPDFファイルに対し，ICカード内の証明書（署名アルゴリズム：SHA1withRSA，鍵長：1,024ビット）を使用して電子署名（ES形式（CMS署名に証明書を特定する属性が付いたもの））が付与できること ・署名行為はクライアントパソコン上で実施し，PDFファイルへの署名付与はSaaSサービス側で実施できること ・クライアントパソコン上にはICカード及びブラウザのみ必要とし，PDFファイルは一度，SaaSサービス上にアップロードすることで署名を付与できること ・電子署名付きPDFはクライアント側にダウンロードされ，ダウンロード後はSaaSサービス上から削除すること
タイムスタンプ付与機能	・電子署名付きPDFへRFC3161に準拠したタイムスタンプ（署名アルゴリズム：SHA1withRSA，鍵長：2,048ビット）が付与できること ・PDFファイルは一度，SaaSサービス上にアップロードすることでタイムスタンプを付与できること ・タイムスタンプ付きPDFはクライアント側にダウンロードされ，ダウンロード後はSaaSサービス上から削除すること

CMS：Cryptgraphic Message Syntax　RSA：Rivest Shamir Adleman
ES：Electronic Signature　SHA：Set Hash Algorithm
RFC：Request for Comments

プを検証し，ブラウザ上に検証結果を表示し，アップロードされたPDFファイルは検証結果表示後，SaaSサービス上から削除する。

⑷ 医療機関(組織)並びに医療機関に所属する個人が識別可能な認証サービス

SaaSサービスのアクセス認証としては，SSL(Secure Socket Layer)クライアント認証又はID／Password認証とし，ユーザー管理機能及び認証／認可機能を**表2**のように整理した。

⑸ 従量課金が可能な課金方式の検討

課金方式については，従量制，固定性，不定期課金があり，SaaSサービスとして必要な課金方式を検討した。また，認証情報によって，医療機関(組織)と医療機関に所属する個人を特定し，だれが，いつ，何のサービスを使用したかを特定できるようにする必要がある。

4. ヘルスケアセキュリティSaaSの実装方式

先に述べたガイドラインに準拠したヘルスケアセキュリティSaaSを実現するために，**図1**に示すようなIaaS，PaaS，SaaSの概念定義を実施し，国内のデータセンターで提供されるIaaSを利用して，電子署名・電子署名検証サービス，PaaS上のSSO(Single Sign-On)，ユーザー管理，課金管理機能の開発を行った。

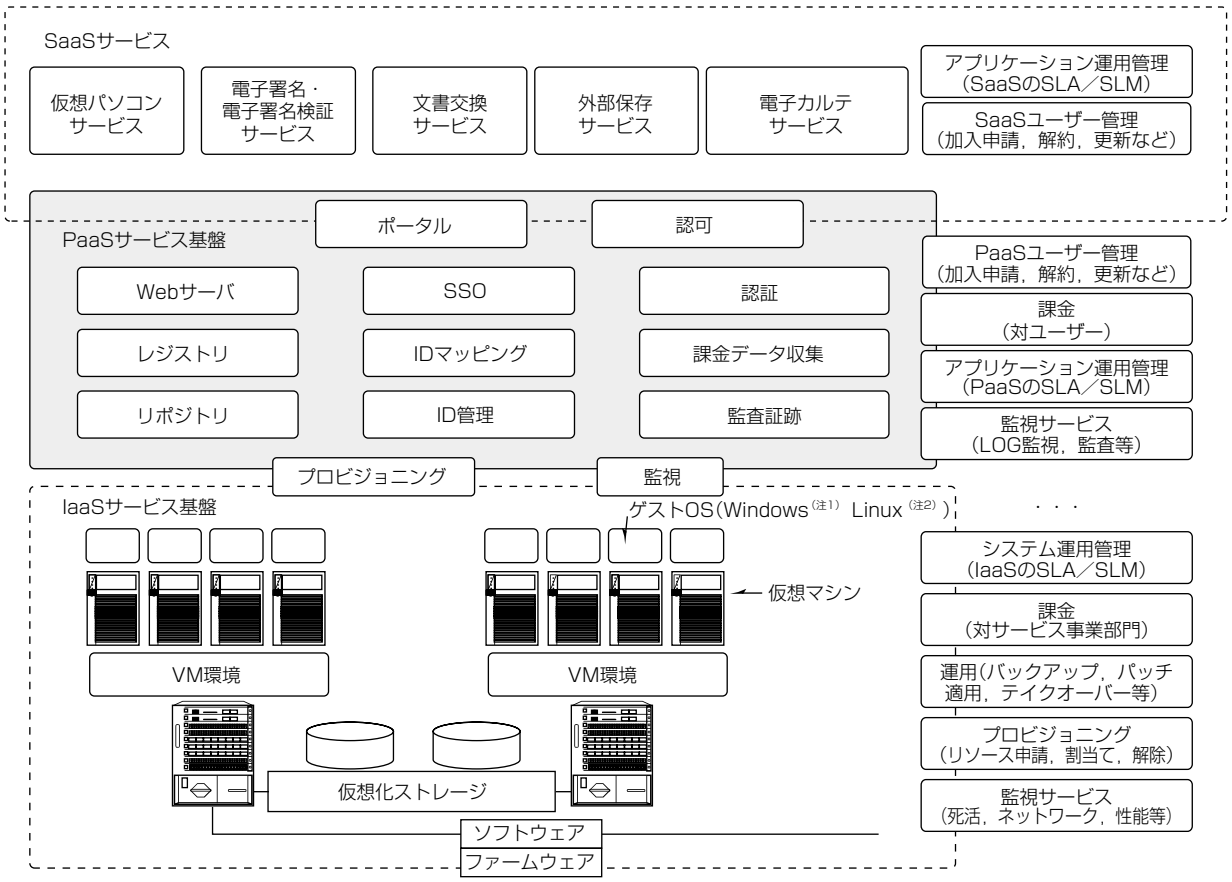
4.1 電子署名・電子署名検証サービス

“電子医療文書等への電子署名並びにタイムスタンプ付与サービス”及び“タイムスタンプ付き電子署名文書の検証サービス”のSaaS化を実現するため，PDFデータへの電子署名及び電子署名検証については，三菱電機インフォメーションシステムズ㈱(MDIS)製SignedPDFシリーズを利用

表2．SaaSサービスとしての要求機能(2)

要求機能	内容
ユーザー管理機能	・SaaSサービス加入者として，医療機関(組織)並びに医療機関に所属する個人を管理できること ・ユーザ管理機能としてGUIを用意し，SaaSサービス加入者情報(認証情報含む)の登録，変更，削除等をCSVファイルで実施できること ・GUIからはSaaSサービス加入者の検索や，認可／認証機能への認証データ反映を実施できること
認証／認可機能	・SSLクライアント認証に加え電子証明書のSubject属性を認証情報とし，認証情報による認証並びにSaaSサービス加入者を特定できること ・ID／Password認証ではID／Passwordを認証情報とし，認証情報による認証並びにSaaSサービス加入者を特定できること ・認証情報からヘルスケアセキュリティSaaSポータルサイトへの認可を実施し，認可されたサービスのみをポータルサイトに表示すること ・認可されて，ヘルスケアセキュリティSaaSポータルサイトに表示されたサービスは，再度認証することなく利用できること(SSO機能)

GUI ：Graphical User Interface
CSV ：Comma Separated Value



(注1) Windowsは，Microsoft Corp. の登録商標である。
(注2) Linuxは，Linus Torvalds氏の登録商標である。

SLA ：Service Level Agreement
SLM ：Service Level Management

図1．ヘルスケア分野向けサービスの概念図

した。ただし，既存製品ではガイドラインの要求事項であるタイムスタンプ機能は未実装なため，今回の，CAdES(Cryptographic Message Syntax Advanced Electric Signatures)対応のタイムスタンプ機能を新たに追加した。電子署名に使用する電子証明書は，厚生労働省が推進する署名用HPKI電子証明書を利用可能とした。また，署名検証サービスでは，クライアントへのCRL(失効リスト)のダウンロードを不要とし，将来のCRL肥大化に対応できる設計となっている。

4.2 ヘルスケアセキュリティ用PaaS

“医療機関(組織)並びに医療機関に所属する個人が識別可能な認証サービス”を実現するため，ユーザー管理機能及び従量課金機能を実装した上で，次の特長を持つヘルスケアセキュリティ用PaaSの開発を行った。

4.2.1 ICカードを用いたSSLクライアント認証

ガイドラインに準拠した電子証明書を利用可能としたSSL(Secure Socket Layer)クライアント認証を実装した。これによって，認証局で本人確認を行った電子証明書の保有者のみがSaaSを利用できることになる。IPSec＋IKEによるネットワークセキュリティの確保とあいまって，成りすましや不正アクセスを防止でき，ハイレベルなセキュリティを確保できる。このPaaSでは，厚生労働省が推進する認証用HPKI証明書も利用可能な設計となっており，保健医療福祉情報システム工業会(JAHIS)策定のガイドラインに準拠したHPKI認証基盤を提供することができる。

4.2.2 SSO

医療機関のデータ保管やデータ交換など，将来的に新たなSaaSサービスを提供することを前提として，医療機関での利便性を考慮し，**4.2.1項**で述べたSSLクライアント認証を行ったあとには，複数のSaaS間で再認証が不要なSSO機能を実現した。SSO機能のコアシステムには，オープンソースソフトウェア(OSS)を採用した。OpenSSOをベースに，リバースプロキシとSAML(Security Assertion Markup Language)2.0の両方をサポートする形で実現されており，SaaSサービスごとにいずれかの形態でSSO機能を利用できる。

システム構築に当たってはOSSを活用したため，導入及び維持管理費用が抑えられる。また，ユーザー管理機能によって，SaaS側で独自に割り振ったIDとPaaSのIDをマッピングし変換することが可能となり，異なるIDを持つSaaSサービス間のSSOも可能になっている。この際，各SaaSは他のSaaSのIDを知る必要がなく，PaaSのIDと連携することでSaaS間の独立性と機密性を担保している。また，課金管理機能とSaaSが連携することで，PaaS運営者が課金代行をすることが可能となり，利用サービスをまとめた一括請求なども利用可能となる(**図2**)。

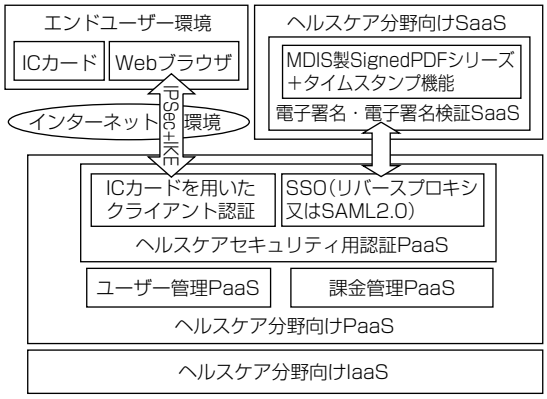


図2．ヘルスケア分野向けサービス構成

4.3 ヘルスケアセキュリティ用IaaS

医療情報を取り扱うこのサービスでは，データの保存場所は国内法の影響が及ぶ範囲であることが不可欠であるため，IaaSは国内に設置し，海外へのデータ流出がないことを担保する必要がある。また，可用性や信頼性の確保が大前提であるため，SaaS，PaaS事業者からのIaaSのSLA(Service Level Agreement)に対する要求レベルは非常に高いものになる。三菱電機グループでは，IaaS，PaaS，SaaSのトータルサービスを提供するため，ハイレベルセキュリティを担保するSLAに対応したIaaSを構築し，機微な情報を扱う分野にも適応できるようにした。仮想化技術を採用し，仮想化サーバ，仮想化ストレージ，仮想化ネットワークを提供するとともに，統合管制センターによる稼働監視，運用自動化が可能である。

5. むすび

今回の構築によって，医療分野の各種ガイドラインに準拠したSaaSサービスの提供に目処(めど)が立った。今後は署名対象ファイルの多様化(XML(eXtensible Markup Language)，ODF(Open Document Format)など)を行うとともに，外部保存サービス，電子カルテサービス，地域連携サービスなどSaaSサービスの多様化を図り，医療分野のユーザーニーズにこたえていく。また，自社サービスのみならず，他社の提供するSaaSに対するIaaS，PaaSの提供や，SaaS間連携を実施し，医療情報分野に対するハイレベルセキュリティサービスを提供していく。

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4.1版（2010）
(2) 保健医療福祉情報システム工業会：JAHISヘルスケアPKIを利用した医療文書に対する電子署名規格（2008）
(3) 保健医療福祉情報システム工業会：HPKI対応 ICカードガイドライン第2版（2010）