閾値署名を適用したリモート署名システムの安全性評価

山中 忠和[1,*] 松田 規[1] 宮崎 一哉[1]

概要：政府が推進しているテレワークの障害の一つとして契約書等への押印が挙げられているが，契約書等への押印は必ずしも必要ではなく，その代替となる，文書の成立の真正を証明する手段を確保するための方法として，電子署名サービスの活用が提言されている．EU では eIDAS 規則が発効され，特定の条件を満たす場合は署名者の署名鍵をサーバで管理するリモート署名に関しても法的効力が認められ，これら流れを受けて，国内ではリモート署名事業者に求めるセキュリティ対策やセキュリティ機能要件を定義したリモート署名ガイドラインが JT2A から公開された．今回，署名鍵を分割した分割鍵をクライアント，サーバのそれぞれが保有する閾値署名を適用したリモート署名システムにおいて，リモート署名ガイドラインが HSM 利用を前提に定義しているレベル 2,3 のセキュリティ要件に対し，安全性を評価した．その結果，HSM 適用が必須となる要件について，リモート署名ガイドラインの準拠性を認めることができず，平文の秘密鍵の漏洩リスクが少なからず残存すること．また，他者の署名鍵を利用するリスクについては，リモート署名ガイドラインのレベル 2 に準拠したシステムと比べ，提案システムの安全性が高いことを示した．

キーワード：閾値暗号，閾値署名，リモート署名，リモート署名システム，安全性評価

Security Evaluation of Trustworthy System Supporting Server Signing with Threshold Signature Scheme

Tadakazu Yamanaka[1,*] Nori Matsuda[1] Kazuya Miyazaki[1]

Abstract: One of the obstacles to telework promoted by the Japanese government is the imprinting of contracts, but the imprinting of contracts is not always necessary, and as an alternative, it is recommended to use an electronic signature service as a method for proving the authenticity of the document . In the EU, eIDAS regulations have come into effect, and if certain conditions are met, the legal effect of remote signatures that manage the signing key of the signer on the server is also recognized. JT2A has released a remote signature guideline that defines security requirements. In this paper, the results of the security evaluation of the remote signature system to which the threshold signature method is applied are shown for the level 2 and 3 security requirements defined by the remote signature guideline on the premise of using HSM.

Keywords: Threshold cryptography, Threshold signature scheme, Remote signature, Trustworthy system supporting server signing, Security evaluation

1. はじめに

政府が推進している働き方改革の一つであるテレワークにより，少子高齢化対策の推進や，ワーク・ライフ・バランスの実現の効果を見込んでいる．テレワークの障害の一つとして契約書等への押印が挙げられているが，2020 年に内閣府・法務省・経済産業省が「押印についての Q&A」[1]を公表し，契約書等への押印は必ずしも必要ではなく，その代替となる，文書の成立の真正を証明する手段を確保するための方法として，電子署名サービスや電子認証サービスの活用が提言されている．

一方 EU では，電子商取引のための電子識別及びトラストサービスに関する規則である eIDAS 規則が発効され，条件を満たす電子署名や e シール，タイムスタンプ等に法的効力が認められることとなった．更に，サービス事業者の電子署名環境が信頼でき，署名者の単独管理の下で使用されることを保証できる等の条件を満たす場合は，署名者の署名鍵をサーバで管理するリモート署名に関しても法的効力が認められている．

近年，国内でもこれらの流れを受けて，業界団体である JT2A（日本トラストテクノロジー協議会）がリモート署名事業者や関係事業者及びリモート署名の利用者がリモート署名の理解を深め，一定の指標として参照可能なリモート署名サービスのガイドラインである「リモート署名ガイドライン」[2]を公開した．リモート署名ガイドラインは，リモート署名事業者に求めるセキュリティ対策やセキュリティ機能要件が 3 段階のレベルに対応付けて記載されている．

本論文では，署名鍵を分割した分割鍵をクライアント，サーバのそれぞれが保有する閾値署名を適用したリモート署名システムにおいて，リモート署名ガイドラインが HSM 利用を前提に定義しているレベル 2,3 のセキュリティ対策やセキュリティ機能要件を比較し，安全性を評価した結果を示す．

1 三菱電機株式会社
Mitsubishi Electric Corporation
* Yamanaka.Tadakazu@ab.MitsubishiElectric.co.jp

2. 閾値署名

閾値署名とは閾値暗号の一種であり，メッセージと複数の秘密鍵から，1 つの署名値を生成する署名方式である．1 つの秘密鍵を n 個に分割し，その内の k 個を使い，1 つの署名値を生成する閾値署名を k-out-of-n 閾値署名と呼ぶ．本論文では，リモート署名システムへ適用する閾値署名の方式として，RSA 署名の閾値署名方式である Boyd の方式[3]を採用する．なお，Boyd の方式は n-out-of-n 閾値署名の方式である．

以下，Boyd の方式を 2 種類示す．Mを平文，dを秘密鍵，eを公開鍵，$Sig(M)$を M の署名値，$n = pq$，$\varphi(n) = (p-1)(q-1)$，$Sig^{TH1}(M)$，$Sig^{TH2}(M)$を中間生成値とする．

2.1 Boyd の方式（その 1）

本方式は，RSA の秘密鍵を乗除算にて分割した方式である．署名値の生成はメッセージに対し，分割した秘密鍵を使い署名処理を行った中間生成値を生成する．その中間生成値に対し，もう一方の分割した秘密鍵を使い，署名処理を行い，署名値を生成する．

$$ed \equiv 1 \bmod \varphi(n) \quad \cdots(1)$$

$$d \equiv d_1 d_2 \cdots d_N \bmod \varphi(n) \quad \cdots(2)$$

$$Sig^{TH1}(M) = M^{d_1 d_2 \cdots d_{N-1}} \bmod n \quad \cdots(3)$$

$$Sig^{TH1}(M)^{d_N} \equiv M^{d_1 d_2 \cdots d_N} \bmod n \equiv M^d = Sig(M) \quad \cdots(4)$$

2.2 Boyd の方式（その 2）

本方式は，RSA の秘密鍵を加減算にて分割した方式である．署名値の生成はメッセージに対し，分割した秘密鍵を使い署名処理を行った中間生成値を生成する．もう一方の分割した秘密鍵を使い，メッセージに対し署名処理を行い，中間生成値を生成，全ての中間生成値を乗算処理し，署名値を生成する．

$$ed \equiv 1 \bmod \varphi(n) \quad \cdots(5)$$

$$d \equiv d_1 + d_2 + \cdots + d_N \bmod \varphi(n) \quad \cdots(6)$$

$$Sig^{TH2}(M) = M^{d_1 + d_2 + \cdots + d_{N-1}} \bmod n \quad \cdots(7)$$

$$Sig^{TH2}(M) \cdot M^{d_N} \equiv M^{d_1 + d_2 + \cdots + d_N} \bmod n \equiv M^d = Sig(M) \quad \cdots(8)$$

3. リモート署名システム

3.1 一般的なリモート署名システム

リモート署名ガイドラインでは一般的なリモート署名システム（以降，既存システムと表す.）の基本モデルとして図 1 が例示されている．以下，鍵生成登録及び署名利用のフローについて説明する．

鍵生成登録フェーズではクレデンシャル発行者（CSP）がリモート署名事業者（RSSP）の提供するサービスを利用するための認証/認可クレデンシャルを署名者に発行（0.1）．登録局（RA）が署名者の本人確認（0.2）を行い，RSSP が署名者の署名鍵を生成（オプションでは発行局（IA）が生成し，RSSP が鍵インポート）（0.3），署名者の証明書発行要求を IA へ送付（0.4）し，RSSP への証明書発行（0.5）を行う．

署名利用フェーズでは，署名者は署名アプリを使い，RSSP にログイン（1.4-1.6）する．署名対象文書を含む署名要求を RSSP へ送る（1.7）と，RSSP は鍵認可要求を署名者に求め（1.8），署名者は認証/認可クレデンシャルを用い，鍵認可を実行（1.9）し，RSSP から署名値生成モジュール（CM : Cryptographic Module）が生成した署名値が署名アプリに返送(1.10)される．

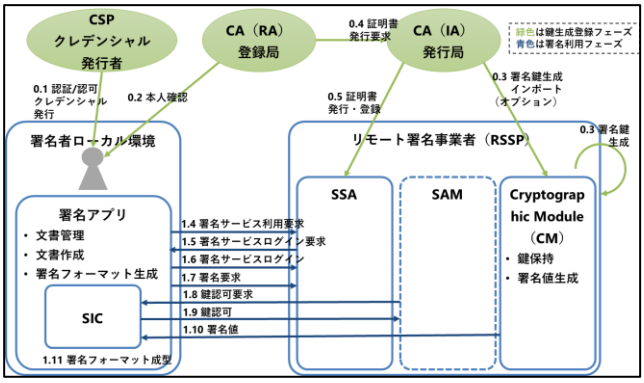

図 1 一般的なリモート署名システム（[2]内の図から筆者が作成）

3.2 閾値署名を適用したリモート署名システム

本節では 2.1 節の方式を適用したリモート署名システム（以降，提案システムと表す.）のモデル（図 2）について説明する．本モデルでは 2-out-of-2 閾値署名とし，秘密鍵を 2 つに分割した分割鍵を署名者と RSSP にインポートするシステムとする．以下，3.1 節の既存システムと異なるフローについて説明する．

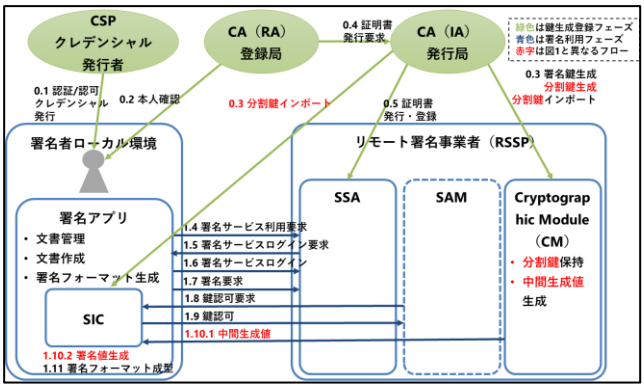

図 2 閾値署名を適用したリモート署名システム

鍵生成登録フェーズで異なるのは，図 2 の 0.3 分割鍵生成と分割鍵インポートのフローである．分割鍵生成は秘密鍵dから分割鍵d_1, d_2を生成し，分割鍵インポートは RSSP へd_1を，署名者へd_2を安全に送付し，署名アプリ内の SIC（Signer's Interaction Component），CM に分割鍵をインポートする．RSSP の CM は秘密鍵の代わりに分割鍵を保持する．この分割鍵生成と分割鍵インポートのフローは図 1 の

0.3 に代わる処理となる．

署名利用フェーズは，図 2 の 1.10.1 中間生成値と 1.10.2 署名値生成が図 1 の 1.10 に代わる処理となる．中間生成値は RSSP の分割鍵d_1を使い，式(3)にて$M^{d_1} \ mod \ n$の値を生成，署名値は署名者の分割鍵d_2を使い，式(4)にて$M^{d_1 d_2} \ mod \ n = M^d = Sig(M)$の値の生成処理で得られる．

4. リモート署名ガイドライン

JT2A が公開しているリモート署名ガイドラインは，リモート署名サービスを開発及び提供する事業者，その利用者を想定読者とし，リモート署名の概要や，リモート署名で必要となるセキュリティ対策事項，セキュリティ機能要件等がまとめられている．リモート署名ガイドラインは，表 1 の 3 部で構成されている．

表 1 リモート署名ガイドラインの構成

Part	概要
I	リモート署名の概要とセキュリティ対策事項
II	署名活性化モジュールとセキュリティ機能要件
III	署名値生成モジュールのセキュリティ機能要件

4.1 リモート署名の重要項目

リモート署名の重要項目として，鍵生成（署名鍵の生成），鍵インポート，鍵保持，鍵認可（署名鍵の活性化）の 4 つの項目が定義され，これら項目の実現手段の違いにより，レベルが定義されている．各レベルの概要を表 2，リモート署名の重要項目のレベル 2,3 の実現手段を表 3 に示す．

表 2 レベル分類

レベル	概要
レベル 1	電子署名に利用する署名者の署名鍵を安全に管理するために最低限必要な対策を施したレベル
レベル 2	電子署名法における認定認証業務において発行する電子証明書に基づいたリモート署名サービスを提供するにあたり，リモート署名サービスが認定認証業務の信頼性と同等の信頼性を達成するために必要なレベル
レベル 3	リモート署名サービスが欧州 eIDAS 規則における適格電子署名と同等の信頼性を達成するために必要なレベル

表 3 リモート署名の重要項目（レベル 2,3 抜粋）

項目	レベル 2	レベル 3
鍵生成	・第三者の評価や認証を受けた HSM でのみ署名鍵の生成が可能.	・国際的に承認されうる評価や認証を受けた HSM でのみ署名鍵の生成が可能.
鍵インポート	・電子署名法に基づく認定認証事業者など信頼できる CA からのみ署名鍵のインポートが可能.	・外部からのインポート不可．HSM 内で生成した署名鍵のみを利用する.
鍵保持	・HSM のセキュアな境界内で署名鍵を保持し，HSM 内でのみ署名生成処理を実行する. ・HSM のセキュアな境界を越えた，署名鍵のエクスポートは不可	
鍵認可	・鍵認可は複数要素認証. ・利用認証と別に鍵認可を行わなければいけない.	・レベル 2 に追加して，評価・認証取得し，耐タンパ領域に実装した署名活性化モジュールでの鍵認可が必要.

4.2 セキュリティ対策を検討すべき事項

リモート署名はサービス側が署名鍵を保管し，署名者からの要求の下に電子署名を行う．署名者自らが署名鍵を保管し，電子署名を行うローカル署名と異なり，サービス側への署名鍵のインポートにおける脅威や，内部不正者による脅威等のローカル署名では起こりえない脅威が考えられる．リモート署名ガイドラインでは，リモート署名にて起こりえる脅威が整理されている．表 4 にそれら脅威を示す．

表 4 リモート署名にて起こりえる脅威の分類

A. 登録フェーズにおける脅威	
A-1	署名者登録等における脅威
A-2	署名者管理における脅威
A-3	証明書署名要求における脅威
A-4	署名鍵のインポートにおける脅威
B. 署名利用フェーズにおける脅威	
B-1	利用フェーズにおける脅威
B-2	鍵利用・管理における脅威
B-3	内部不正者による脅威
C. 利用停止（破棄）フェーズにおける脅威	
C-1	利用停止における脅威

表 4 の脅威へのセキュリティ対策事項として，セキュリティ機能要件が定義されている．表 5 にそれらセキュリティ機能要件を示す．

表 5 セキュリティ機能要件の分類

No.	セキュリティ機能要件
1. 一般的なセキュリティ要件	
1-1	役割・組織の管理
1-2	識別及び認証
1-3	システムへのアクセスコントロール
1-4	監査及びログ

1-5	アーカイブ
1-6	内部不正対策
1-7	バックアップ・リカバリ
2. 組織・運営	
2-1	職務の分離
2-2	事業継続管理
2-3	コンプライアンス
3. 登録時	
3-1	署名者登録等における機能要件
3-2	署名者管理における機能要件
3-3	証明書署名要求における機能要件
3-4	署名鍵活性化（鍵認可）における機能要件
4. 署名利用時	
4-1	署名利用（一般）の機能要件
4-2	共通（システム）における機能要件
5. 利用停止時	
5-1	利用停止における機能要件
6. 署名値生成モジュール	
6-1	CM に関する機能要件

5. 閾値署名を適用したリモート署名システムの安全性評価

3.2 節で示した提案システムについて,リモート署名ガイドラインに定義されたレベル 2,3 のセキュリティ対策やセキュリティ機能要件を比較し，安全性を評価する.

5.1 評価対象

リモート署名ガイドラインが想定している既存システムが 4 章のセキュリティ機能要件を満たしており，提案システムは閾値署名適用と HSM 利用の差異以外は既存システムと同等の機能を持つという前提の下，安全性評価を行う.

そのため，本論文での安全性の評価対象は，既存システムと提案システムの差異である図 2 の 0.3 分割鍵生成と分割鍵インポートと，1.10.1 中間生成値と 1.10.2 署名値生成に関係するセキュリティ上の脅威とする．評価対象とする具体的な脅威（表 4）は以下の通りである.

- 分割鍵生成と分割鍵インポート
  - 鍵利用・管理における脅威
  - 署名鍵のインポートにおける脅威
- 中間生成値と署名値生成
  - 利用フェーズにおける脅威
  - 鍵利用・管理における脅威
  - 内部不正者による脅威

5.2 セキュリティ機能要件整理

5.2.1 分割鍵生成と分割鍵インポート

5.1 節の評価対象とする具体的な脅威に対し,関係するセキュリティ機能要件をまとめたものを表 6 に示す．なお,セキュリティ機能要件の概要は 5.3 節に説明する.

表 6 脅威とセキュリティ機能要件の対応（5.2.1 節）

具体的な脅威	セキュリティ機能要件
A-4. 署名鍵のインポートにおける脅威	
署名鍵と署名鍵情報があり，攻撃者はこれらを扱い不正にインポートする.	1-1 役割・組織の管理 1-2 識別及び認証 1-3 システムへのアクセスコントロール 1-4 監査及びログ 1-6 内部不正対策 3-1 署名者登録等における機能要件 6-1 CM に関する機能要件
攻撃者が他人の署名鍵を自らの鍵情報でインポートする.	
攻撃者が自分の鍵を他人の鍵情報でインポートする.	
攻撃者が同じ鍵を複数回インポートする.	
B-2. 鍵利用・管理における脅威	
攻撃者は平文の共通鍵/秘密鍵（本論文では，署名鍵のことを言う.）に不正にアクセスし開示する.	1-1 役割・組織の管理 1-2 識別及び認証 1-3 システムへのアクセスコントロール 1-4 監査及びログ 1-6 内部不正対策 3-1 署名者登録等における機能要件 3-2 署名者管理における機能要件 3-4 署名鍵活性化（鍵認可）における機能要件 6-1 CM に関する機能要件
攻撃者は共通鍵/秘密鍵を導出する.	
攻撃者は CM 格納時に，鍵及び鍵の属性を不正に変更する.	
攻撃者は CM 管理時に，鍵を誤用する.	
攻撃者は鍵を乱用する.	
攻撃者はクライアントアプリケーションデータから送信中の機密データを不正に開示する.	
攻撃者はクライアントアプリケーションデータから送信中の機密データを不正に変更する.	
攻撃者は CM に対してハードウェアまたはソフトウェアの機能不全を発生させる.	

5.2.2 中間生成値と署名値生成

5.1 節の評価対象とする具体的な脅威に対し，関係するセキュリティ機能要件をまとめたものを表 7 に示す．

表 7 脅威とセキュリティ機能要件の対応（0 節）

具体的な脅威	セキュリティ機能要件
B-1. 利用フェーズにおける脅威	
攻撃者は認証情報を変更する．	1-1 役割・組織の管理 1-2 識別及び認証 1-3 システムへのアクセスコントロール 1-4 監査及びログ 1-6 内部不正対策 3-4 署名鍵活性化（鍵認可）における機能要件 4-1 署名利用（一般）の機能要件 4-2 共通（システム）における機能要件
攻撃者はステップをバイパスし，署名する．	
攻撃者は再生し，署名する．	
攻撃者は偽造された認証情報を使用して署名者に偽造し，署名する．	
攻撃者は SAM（Signature Activation Module：署名活性化モジュール）への転送中に署名対象データまたは SAD（Signature Activation Data：署名活性化データ）の情報を得る．	
攻撃者は SAM への転送中に DTBS/R（署名対象データ）を偽造し，署名する．	
攻撃者は SAM への転送中に SAD を偽造し，署名する．	
攻撃者は，作成中または作成後または転送中に，署名を SAM 外で修正する．	
B-2. 鍵利用・管理における脅威	
攻撃者は平文の共通鍵/秘密鍵に不正にアクセスし開示する．	1-1 役割・組織の管理 1-2 識別及び認証 1-3 システムへのアクセスコントロール 1-4 監査及びログ 1-6 内部不正対策 3-1 署名者登録等における機能要件 3-4 署名鍵活性化（鍵認可）における機能要件 4-1 署名利用（一般）の機能要件 4-2 共通（システム）における機能要件 6-1 CM に関する機能要件
攻撃者は共通鍵/秘密鍵を導出する．	
攻撃者は CM 格納時に，鍵及び鍵の属性を不正に変更する．	
攻撃者は CM 管理時に，鍵を誤用する．	
攻撃者は鍵を乱用する．	
攻撃者はクライアントアプリケーションデータから送信中の機密データを不正に開示する．	
攻撃者はクライアントアプリケーションデータから送信中の機密データを不正に変更する．	
攻撃者は CM に対してハードウェアまたはソフトウェアの機能不全を発生させる．	
B-3. 内部不正者による脅威	
攻撃者（内部者）が運用管理者に詐称し，署名鍵を利用する．	1-1 役割・組織の管理 1-2 識別及び認証 1-3 システムへのアクセスコントロール 1-4 監査及びログ 1-6 内部不正対策 3-4 署名鍵活性化（鍵認可）における機能要件 4-1 署名利用（一般）の機能要件 4-2 共通（システム）における機能要件
攻撃者（内部者）が監査者に詐称し，ログを得る．	
攻撃者（内部者）が署名鍵の活性化情報を得る．	

5.3 リモート署名ガイドラインの準拠性評価

本評価では，提案システムの SAM（Signature Activation Module：署名活性化モジュール）及び SAD（Signature Activation Data：署名活性化データ）を以下のように定義する．

- SAM
  署名者情報の管理及び，鍵認可等を行うソフトウェア
- SAD
  CEN EN 419241-1:2018 [4]では，SAD の要件を以下のように定義している．
  - 署名者の SIC の制御下で SAD を生成すること
  - SAD には，必須パラメータとして以下の情報を含むこと．
    1. 署名対象データ
    2. 署名者の ID
    3. 署名鍵情報

  上記の必須パラメータは以下のリスクへの対策のためだと考えられる．
    1. 異なる署名対象への署名リスク
    2. 署名意思の確認
    3. 異なる鍵での署名リスク

  提案システムでは，ユーザが分割した鍵で最終的に署名生成を行うため，適用した閾値署名が，以下の通り，リスクへの対策となる．そのため，提案システムでは SAD を使わず，リスクへの対策ができるため，SAD は

利用しない.

1. 署名生成の最終実施者はユーザのため，署名生成後の検証で署名対象の確認可能.
2. 署名生成の最終実施者はユーザのため，署名意思の確認可能.
3. 署名生成の最終実施者はユーザのため，サービス側で異なる鍵で処理された場合でも，正しい署名は作成できない.

上記と，「既存システムはリモート署名ガイドラインの要件を満たしており，提案システムは閾値署名適用と HSM 利用の差異以外は既存システムと同等の機能を持つ」という前提の下，5.2 節で抽出したセキュリティ機能要件ごとに，提案システムのリモート署名ガイドラインの準拠性を評価した結果を以降に示す.

5.3.1 役割・組織の管理 (1-1)

本要件は，リモート署名システムがサポートする権限（特権）や，特権ユーザの条件，システム運用で必要となるマニュアルの提供，時刻の同期等の要件を定めている．これら要件は，提案システムと既存システムの差異である閾値署名適用と HSM 利用には関係しない要件である．そのため，リモート署名ガイドラインの要件を満たすことは可能である.

5.3.2 識別及び認証 (1-2)

本要件は，ユーザがリモート署名サービスに対してアクションを認める際に，識別と認証を実施することや，ログアウト後の再認証を必須とすること，認証失敗時の制限等の要件を定めている．これら要件は，提案システムにおいても既存システムと同様に適用可能であることから，リモート署名ガイドラインの要件を満たすことは可能である.

5.3.3 システムへのアクセスコントロール (1-3)

本要件は，システムやユーザオブジェクト，機密性の高い残存情報へのアクセスコントロールの実施を要件として定めている．これら要件は，提案システムにおいても既存システムと同様に適用可能であることから，リモート署名ガイドラインの要件を満たすことは可能である.

5.3.4 監査及びログ (1-4)

本要件は，記録するイベントの種類や，監査データのパラメータ，保管条件（可用性，完全性）等を定めている．これら要件は，提案システムにおいても既存システムと同様に適用可能であることから，リモート署名ガイドラインの要件を満たすことは可能である.

5.3.5 内部不正対策 (1-6)

本要件は，5.3.1 節の役割・組織の管理 (1-1)と 5.3.4 節の監査及びログ (1-4)を満たすことと，定めている．5.3.1 節と 5.3.4 節の評価結果の通り，リモート署名ガイドラインの要件を満たすことは可能である.

5.3.6 署名者登録等における機能要件 (3-1)

本要件は，4 つの要件を定めており，そのうちの 3 要件が公開鍵を含む署名者情報の登録，保管に関する SAM の要件である．提案システムでは SAM をソフトウェアに限定している以外は既存システムと同様，残り 1 要件の安全性評価は表 8 の通りであるため，リモート署名ガイドラインの要件を満たすことは可能である.

表 8 署名者登録等における機能要件に対する安全性評価

要件	評価結果
SAMは，署名者情報の一部として SAD をセキュアに扱うことができなければならない.	提案システムでは SAD を利用せずリスクへの対策は可能なため，本要件への対応は不要.

5.3.7 署名者管理における機能要件 (3-2)

本要件は，公開鍵を含む署名者情報の更新に関する SAM の要件である．提案システムでは SAM をソフトウェアに限定している以外は既存システムと同様に適用可能であることから，リモート署名ガイドラインの要件を満たすことは可能である.

5.3.8 署名鍵活性化（鍵認可）における機能要件 (3-4)

本要件は，鍵認可に関する SAM の要件で，レベルにより要件が異なる．表 9 の通り，レベル 2 はソフトウェアでの実現は可能であるが，レベル 3 では耐タンパ領域が求められているため，HSM の適用が必須である．以上から，リモート署名ガイドラインのレベル 2 の要件は満たすことが可能であるが，レベル 3 の要件は満たすことができない.

表 9 署名鍵活性化（鍵認可）における機能要件

レベル	要件
レベル 2	● 鍵認可は複数要素認証 ● 利用認証と別に鍵認可を行わなければいけない.
レベル 3	● レベル 2 に追加して，評価・認証取得し，耐タンパ領域に実装した SAM での鍵認可が必要

5.3.9 署名利用（一般）の機能要件 (4-1)

本要件は，SAD 検証や SAD の保護，署名対象データの完全性，署名改変不可の保証，特権ユーザ保護に関する SAM の要件である．提案システムでは SAM をソフトウェアに限定している以外は既存システムと同様，SAD に関連する要件は表 10 の通りであるため，リモート署名ガイド

ラインの要件を満たすことは可能である．

表 10 署名利用（一般）の機能要件に対する安全性評価

要件	評価結果
SAM は，SAD を検証しなければならない．	提案システムでは SAD を利用せずリスクへの対策は可能なため，本要件への対応は不要．
SAM は以下を提供するプロトコルのサーバ側エンドポイントを実装しなければならない． 1. 署名者認証 2. 送信された SAD の整合性 3. 少なくとも機密情報を含む SAD 要素の機密性 4. リプレイ，バイパス，偽造からの保護	1,4 については，既存システムと同様であるため，リモート署名ガイドラインの要件を満たすことは可能． 2,3 については，提案システムは SAD を利用せずリスクへの対策は可能なため，本要件への対応は不要．
SAM は，SAM への送信時に，SAD の使用を危うくする攻撃に対して SAD が確実に保護されることを保証しなければならない．	提案システムでは SAD を利用せずリスクへの対策は可能なため，本要件への対応は不要．

5.3.10 共通（システム）における機能要件 (4-2)

本要件は，特権ユーザの認証や，鍵として使用する乱数生成等に関する SAM の要件である．提案システムでは SAM をソフトウェアに限定している以外は既存システムと同様に適用可能であることから，リモート署名ガイドラインの要件を満たすことは可能である．

5.3.11 CM に関する機能要件 (6-1)

本要件は，17 個の要件を定めており，平文の秘密鍵の外部持出不可や，承認された暗号アルゴリズムの使用，鍵及び重要な属性の保護，物理的操作の検出等に関する CM の要件である．署名鍵のインポート，署名鍵生成，署名鍵保持についてはレベルにより要件が異なる．表 12，表 13 を含む物理的な対策を必要とする 3 要件は，HSM の適用が必須である．

以上より，リモート署名ガイドラインの要件は満たすことができない．なお，提案システムは分割鍵をインポートする前提のシステムのため，表 11，表 12 のレベル 2 の要件を満たすことが可能である．

表 11 署名鍵のインポートにおける機能要件

レベル	要件
レベル 2	● 署名者を確認した署名鍵をインポートしなければならない． ● 電子署名法に基づく認定認証事業者など信頼できる CA からのみに限定しなければならない．
レベル 3	● 署名鍵をインポートしてはならない．

表 12 署名鍵生成における機能要件

レベル	要件
レベル 2	● 署名鍵ペアの生成は第三者機関によって使用が適していると認められた暗号アルゴリズム，鍵長，パラメータで生成しなければならない． ● 第三者の評価や認証を受けた HSM で生成しなければならない．
レベル 3	● 署名鍵ペアの生成は国際的に承認されうる評価や認証を受けた HSM 及び本節の要件に適合したデバイスで生成しなければならない．

表 13 署名鍵保持における機能要件

レベル	要件
レベル 2	● HSM のセキュアな境界内で署名鍵を保持し，HSM 内でのみ署名生成処理を実行しなければならない． ● HSM のセキュアな境界を越えた，署名鍵のエクスポートをしてはならない．
レベル 3	● レベル 2 と同じ．

5.4 安全性評価

5.3 節の準拠性評価の結果，提案システムでは，HSM の適用が必須の 4 要件について，リモート署名ガイドラインの準拠性を認められなかった．本節では，前述の要件に関する提案システムの安全性評価を行う．

署名鍵活性化（鍵認可）

レベル 3 の要件である「耐タンパ領域に実装した SAM での鍵認可が必要」は，攻撃者が鍵認可の認証クレデンシャルを持たない状態で，他者の署名鍵を利用（署名値を生成）するリスクに対する要件である．提案システムでは，ユーザの分割鍵を使い，署名生成を行うため，攻撃者が分割鍵を持たない状態では，ユーザの署名を生成することができない．以上より，提案システムはレベル 3 と同等の安全性を持つ．

物理的操作の検出

本要件の「CM への物理的操作の検出」は，CM への直接

的なアクセスによる鍵の盗難や，サイドチャネル攻撃等の物理的な攻撃のリスクに対する要件である．

提案システムでは，CM はソフトウェアによる実装のため，本リスクへの対策は，CM をインストールした装置を厳密なデータセンターで運用する等が必要となるが，署名鍵への攻撃はユーザ及び CM への攻撃が必要となるため，通常の物理的な攻撃と比べ耐性がある．

署名鍵のインポート＆署名鍵生成

レベル 3 の要件「署名鍵のインポート不可」かつ「認証を受けた HSM にて署名鍵ペアを生成」は，登録時に平文の秘密鍵の漏洩リスクを 0 にする要件である．提案システムでは，ユーザ及び CM 内の分割鍵の漏洩により，平文の秘密鍵が漏洩するため，レベル 3 と同等の安全性を持つとは言えない．

署名鍵保持

本要件の「HSM 内でのみ署名生成処理が可能」かつ「HSM のセキュアな境界を越えた署名鍵のエクスポート不可」は署名利用時に平文の秘密鍵の漏洩リスクを 0 にする要件である．提案システムでは，ユーザ及び CM 内の分割鍵の漏洩により，平文の秘密鍵が漏洩するため，レベル 2，3 共にと同等の安全性を持つとは言えない．

5.5 考察

安全性評価の結果（表 14），提案システムは物理的な攻撃と平文の秘密鍵の漏洩についてリスクがあることが分かった．リモート署名ガイドラインの既存システムと比較すると，レベル 3 については，これらリスクに対する安全性について満足することができない．ただし，レベル 2 は署名鍵活性化（鍵認可）について，内部不正者の HSM 利用による，他者の署名鍵を利用するリスクを持つため，提案システムの方が安全性の高いことが分かった．

表 14 安全性評価結果

	既存 Lv3[a]	既存 Lv2[b]	提案[c]
署名鍵活性化	○	×	○
物理的操作の検出	○	○	△
署名鍵のインポート＆署名生成	○	○	×
署名鍵保持	○	○	×

○：セキュリティ機能要件を満たす

×：セキュリティ機能要件を満たすとは言えない

a：リモート署名ガイドラインのレベル 3 に準拠した既存システム

b：リモート署名ガイドラインのレベル 2 に準拠した既存システム

c：提案システム

5.3 節の通り，提案システムは閾値署名の方式自体で SAD の要件を満たすことができる．そのため，既存システムでは必要となる SAD 検証の処理や，SAD の保護が不要となり，実装コストを削減することができる．更に HSM も必要としないため，更にコスト削減が可能となる．

6. おわりに

本論文では，署名鍵を分割した分割鍵をクライアント，サーバのそれぞれが保有する閾値署名を適用したリモート署名システムにおいて，リモート署名ガイドラインの準拠性を評価し，準拠性を認められなかった要件について，安全性評価を行った．

評価した結果，HSM の適用が必須となる 4 要件について，リモート署名ガイドラインの準拠性を認めることができず，平文の秘密鍵の漏洩リスクが少なからず残存することを示した．また，リモート署名ガイドラインのレベル 2 に準拠したシステムと比べると，他者の署名鍵を利用するリスクについては，提案システムの方が安全性の高いことを示した．

リモート署名システムを構築する際には，適用システムの平文の秘密鍵の漏洩リスク，他者の署名鍵を利用するリスク，コストを検討した上，既存システム，提案システムを選定した方がよい．

参考文献

[1] “押印についての Q&A“. http://www.moj.go.jp/content/001322410.pdf, (参照 2021-07-20).

[2] “リモート署名ガイドライン“. https://www.jnsa.org/result/jt2a/2020/index.html, (参照 2021-07-20).

[3] C. Boyd. Digital Multisignatures. Cryptography and Coding 1989. Institute of Mathematics and its application, IMA. 241–246, Clarendon Press, 1989.

[4] CEN EN 419241-1:2018, Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements