サルオフ＃１“署名ブタ野郎は認証先輩の夢を見ない”

リモート署名は電子署名法の夢を見るか?

Do Remote Signatures Dream of the Electronic Signature Law ?

2019年6月19日

宮内・水町IT法律事務所

弁護士 宮内 宏

概要

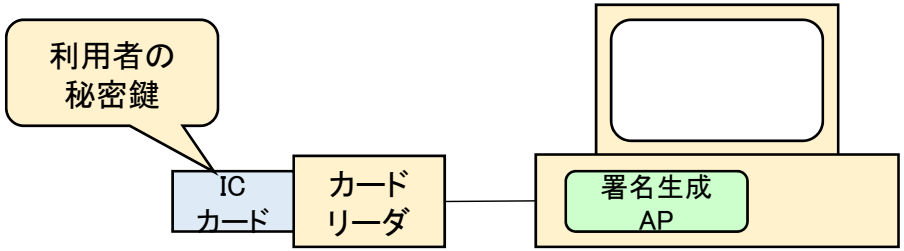
- 民事訴訟での証拠力
  - 真正な成立と，その推定
- 電子署名(ローカル署名の場合)
  - 本人による電子署名（本人性は電子証明書で証明）
- 認証＋DB管理の場合
  - 登録時，ログイン時の本人確認とその記録
  - DB管理の正当性の証明
- リモート署名の場合
  - 認証の正当性，リモート署名サーバの正当性
  - 電子署名はどう役立つ？
  - リモート署名サーバの正当性があらかじめ認められていれば，署名検証だけでよい。

民事訴訟での証拠力

- 民事訴訟で，書証(電子文書を含む)が証拠力を持つためには，「真正な成立」(文書の名義人が，実際にその文書を作成したこと)を証明する必要がある(民事訴訟法228条1項)。
- 推定規定：以下の条件が満たされれば，真正な成立が推定される。
  - 紙文書については，本人又は代理人の署名又は押印があるとき(民事訴訟法228条4項)
  - 電子文書については，本人による電子署名(他人に偽造できない等の制限あり)があるとき(電子署名法3条)
- 推定規定によらずに，他の方法で真正な成立を証明してもよい。

ローカル署名

- 従来型の（本来の）署名方式
- リモート署名と対比して「ローカル署名」と呼ばれる。
- 利用者が秘密鍵を管理するのは大変だし，安全性にも疑問がある。



利用者側で管理する
コンピュータで署名を生成

電子署名(ローカル署名)の場合

電子署名法3条
電磁的記録であって情報を表すために作成されたもの(公務員が職務上作成したものを除く。)は、当該電磁的記録に記録された情報について本人による電子署名(これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。)が行われているときは、真正に成立したものと推定する

■本人による電子署名

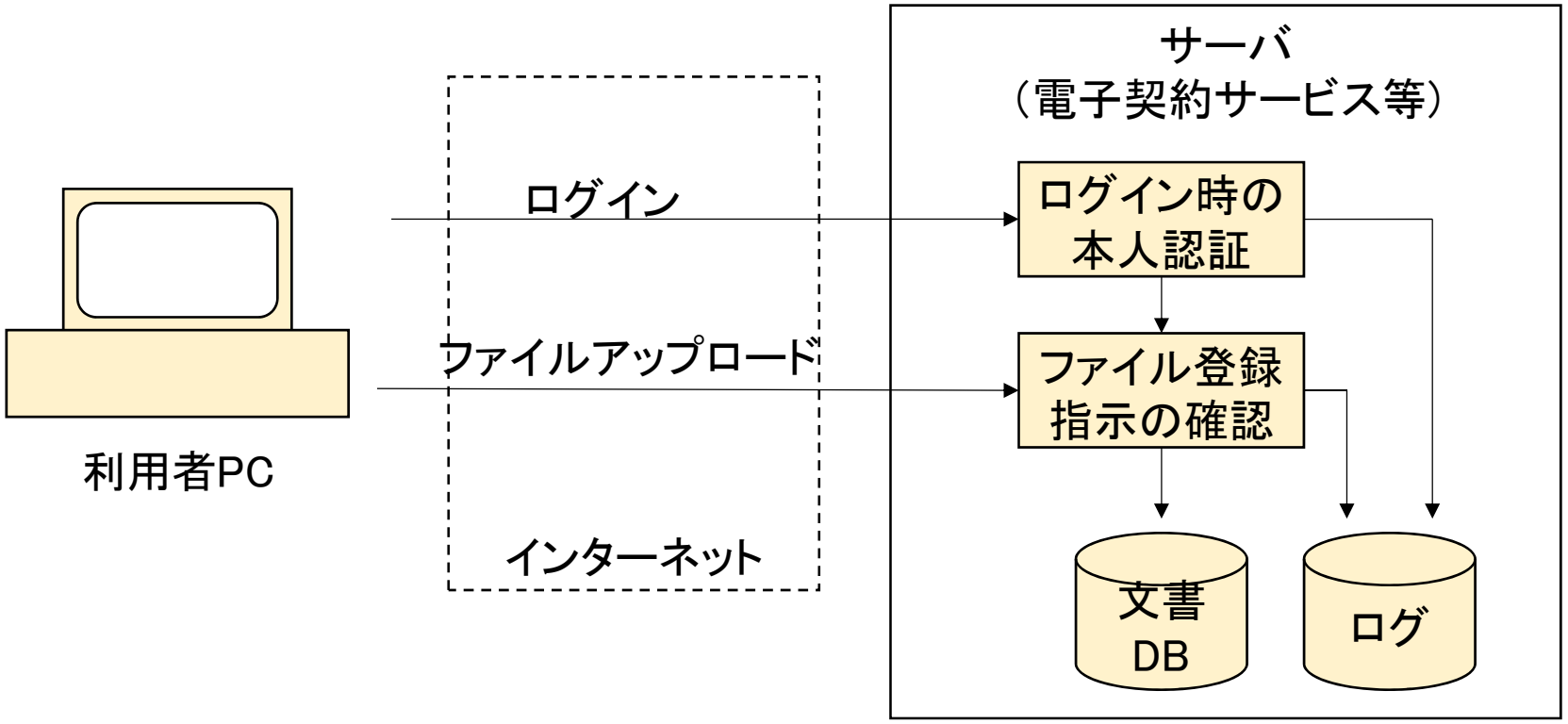
- ●本人の電子署名であることは，電子証明書で証明(発行機関により，信頼性は異なる)
- ●本人「による」は，印鑑に関する最高裁判例(最判S39・5・12。本人の印鑑による印影があれば，本人による押印を推定する)の類推適用が可能ではないか，と考えられている。カードやパスワードは，印鑑と同様に，本人がきちんと管理するはずなので，類推できそうである。

■電子署名(これを……に限る)は，電子証明書にもとづくデジタル署名なら問題はない。

認証＋DB管理における証明

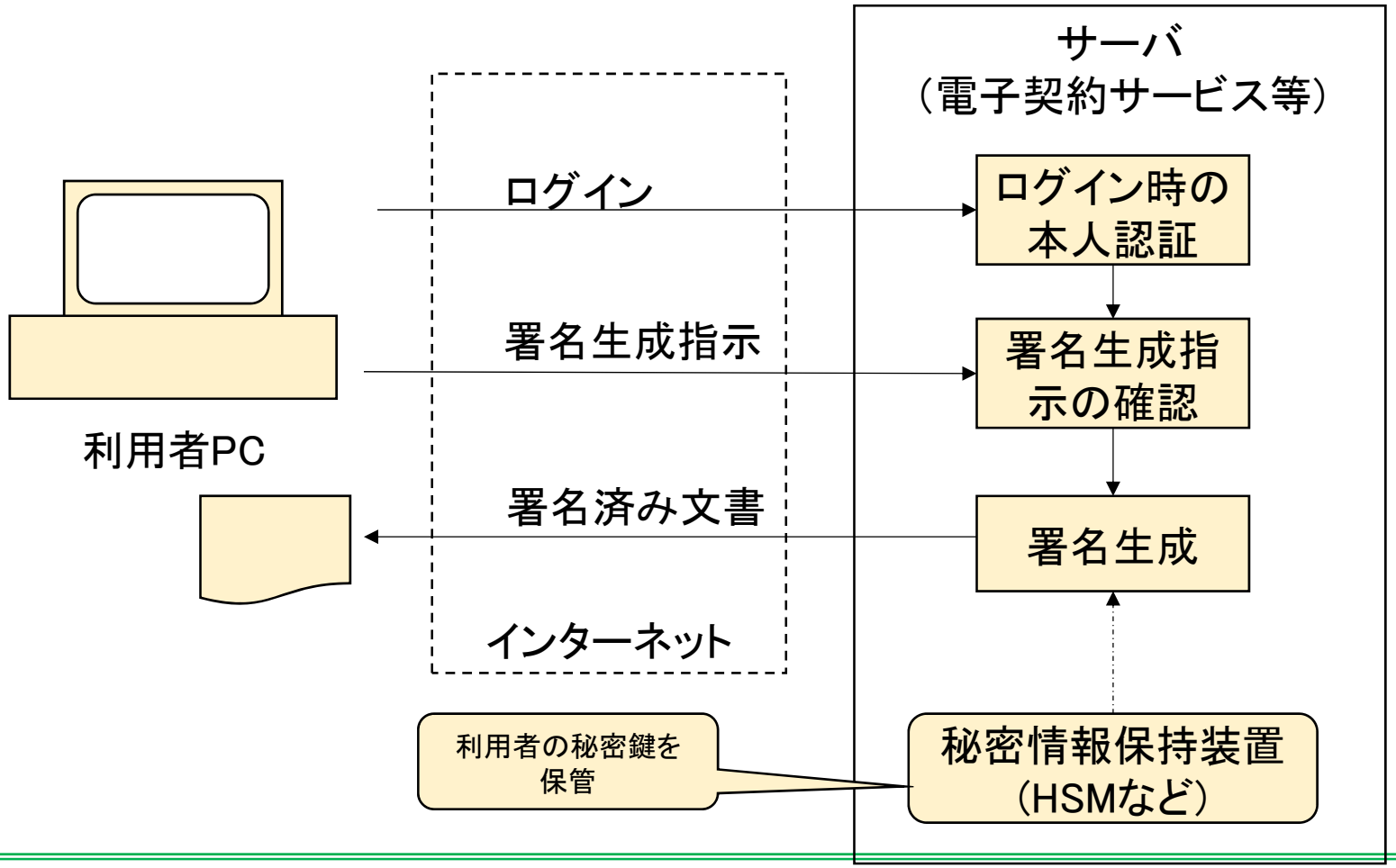
■システムにより作成者情報が管理されており，システム管理者等の証言により，真正な成立を証明する。

- ●ログイン時の本人確認，システム運営の正当性などを，証言又は文書で示す。
- ●登録時の本人確認の資料により，本人性を確保



リモート署名のモデル

■ログインの認証
→ サーバが保管している秘密鍵で署名生成



リモート署名における真正な成立の証明

- 本人による電子署名（→電子署名法3条による推定）
  - 本人の電子署名であることは，電子証明書で証明（発行機関により，信頼性は異なる）。これはローカル署名と同じ。
  - 本人「による」は，少し怪しい。明らかにサーバで署名生成しているのだから。
  - 「本人によるものと同視できる」と言えればよさそう。そのためには，以下が必要。
    - ログイン時の本人確認，システム運営の正当性などを，証言又は文書で示す。
    - 登録時の本人確認の資料により，本人性を確保
- 赤字部分は，認証＋DB管理と同じ。
- だったら，リモート署名は必要なのか？
  - 電子署名法3条なんて，使わないんじゃないの？
  - リモート署名は，電子署名法の夢を見ないのでは？

電子署名法の夢を見ようよ

- リモート署名サーバが，（わざわざ証明しなくても）信頼できるものと認められていれば，ローカル署名と同じように，電子署名＋電子証明書で，電子証明法3条の要件を満たすといえそう。
- そうすると，リモート署名サーバが信頼できるといえるための制度が望まれる。たとえば，公的機関や業界団体による認定制度が考えられる。

※ DB＋認証 についてもサーバの電子署名をつけることにより，そのサーバが処理した文書であると示すことが考えられる。このような方式についても認定制度を検討可能。

まとめ

- PKIベースのデジタル署名をローカル署名でつけていれば，真正な成立の推定を受けられる（電子証明書発行時の本人確認は必要）
- 認証＋DB管理，リモート署名については，サーバの運営の正当性を証明する必要がある。
- サーバの運営について，認定制度等があれば，運営の正当性証明は省ける
  - リモート署名は，ローカル署名と同様に扱える
  - 認証＋DBは，当該電子文書の成立についてのサーバ発行の証明書が必要。なお，このような証明文を電子ファイルにつけてサーバの署名をつける方法も考えられる。