電子署名の技術的問題点と電子署名法

2010年6月29日

(2010年7月2日改訂版)

ひかり総合法律事務所

宮内　宏

miyauchi@hikari-law.com

目次

- はじめに
- 民事訴訟における証明とは
- 書証の真正な成立
- 電子署名の技術的な論点と電子署名法
  - アルゴリズムの危殆化
  - 証明書の有効期限切れ
- まとめ

はじめに

- 署名アルゴリズムの危殆化問題の発生
  - 近い将来，RSA1024bitや，SHA-1の危殆化する可能性が指摘されており(*)，電子署名法に係るアルゴリズムの移行が必要とされている。
  - 署名アルゴリズムの危殆化について，技術的な検討が進められている一方で，法的効果についての議論は活発とは言えない。
- 電子署名法は，民事訴訟における証拠に関する法律である
  - 技術的論点(アルゴリズム危殆化，証明書の有効期限切れ，相互認証証明書やポリシーマッピングの問題等)と，電子署名の法的効果の関係はどうなるのか。
  - 以下では，民事訴訟における書証の扱いについて，簡単に説明し，アルゴリズム危殆化等の影響につき論じる。

(*) 例えば，暗号技術検討会2006年度報告書
(http://www.meti.go.jp/policy/netsecurity/cryptrec2006.pdf)

法律家は何を判断しているのか

■法的三段論法

小前提	具体的事実	例：太郎は花子を殺した。
大前提	法規	例：人を殺した者は，死刑又は無期若しくは5年以上の懲役に処する。(刑法199条)
結論	法的効果	例：太郎は，死刑又は無期若しくは5年以上の懲役に処せられる。

実体の世界：神様の目からみれば「小前提」の成立・不成立は明白。
訴訟の世界：訴訟では，証拠等により証明されたものだけが，「小前提」として使用できる。
→ 証拠から何が言えるか。どのような効果を得ることができるかを考える。

※ 小前提として必要十分な事実を「構成要件事実」あるは「要件事実」という。殺人罪であれば，殺意(故意)，人に対する殺傷行為・死の結果，因果関係が構成要件事実となる。

民事訴訟における事実の証明
(立証責任)

- 一般に，事実Fから効果Rが法律的に生じる場合(FならばR)，Rを主張する者は，Fを証明する必要がある(例外はある)。
  - 多くの条文は，「FならばRとする」という形をとっている。
- Fについては，訴訟上は，3つの状態がありうる。
  - Fである：Fが「高度な蓋然性」をもって証明された場合
  - Fの存否不明：Fも，not Fも証明されていない場合
  - Fでない：Fでないことが「高度な蓋然性」をもって証明された場合
- Rを主張する者は，「Fであること」を証明しなければならない。
- Rでないと主張する者は，Fが存否不明なら十分であり，「Fでないこと」まで証明する必要はない。

「Rを主張する者は，Fについての立証責任を負う」という

刑事訴訟では，ほとんどすべてのことについて，検察側が立証責任を負う(例えば，「心神喪失でなかったこと」の立証責任を検察側が負う)

高度な蓋然性とは？

- いわゆる「ルンバール・ショック事件」最高裁判決(最判昭和50・10・24民集29-9-1417)は，民事訴訟上の証明について，以下のように判示している。

> 訴訟上の因果関係の立証は，一点の疑義も許されない自然科学的な証明ではなく，経験則に照らして全証拠を総合検討し，特定の事実が特定の結果発生を招来した関係を是認しうる高度の蓋然性を証明することであり，その判定は，通常人が疑を差し挟まない程度に真実性の確信を持ちうるものであることを必要とし，かつ，それで足りるものである。

この事件は，3歳児に施術したルンバール(腰椎穿刺による髄液採取とペニシリンの髄腔内注入)の10~20分後に嘔吐・けいれん発作がおこり，運動障害などが残ったもの。ルンバールが原因との100%の証明はできなかったが，最高裁は，上記の規範を掲げて，因果関係を認めた。

この最高裁の記述は，実は具体的な基準(操作的基準)を示しておらず言語明瞭・意味不明だという指摘がある(*)。つまり，客観的判断ではなく，裁判官が，自分の経験に従って真実だと確信すればよいという意味だという批判である。
上記の判決文は，自然科学に対する誤解も包含しており，色々と問題点があるが，
民事訴訟は，この判決に基づいて，「証明度」(証明を要する程度)が考えられている。

(*) 浜井浩一，「2円で刑務所、5億で執行猶予」(p.158)，光文社新書427, 2009.

書証の証拠能力と証拠力

■ 文書を証拠とするためには，条件がある。

証拠能力

証拠に供する資格のこと。民事訴訟の自由心証主義のもとでは，証拠能力のない文書は存在しない。
(刑事訴訟では伝聞証拠につき，証拠能力の制限がある)

証拠力（要証事実を証明する力）

- **形式的証拠力（真正な成立）**
  文書の記載内容が，挙証者の主張する特定人の思想の表現であると認められること。
  文書に関しては，真正な成立の証明が必要である（民訴法228条1項)
- **実質的証拠力**
  文書の記載内容が，要証事実の証明に役立つ効果

形式的証拠力，実質的証拠力のいずれの認定も自由心証に任される。

(用語の定義は以下の文献を参考にした：新堂，新民事訴訟法第三版，弘文堂，2004.）

形式的証拠力(文書の真正な成立)の認定

- 間接証拠等から自由心証主義で認定する。
- 推定規定＝いわゆる「二段の推定」
  - ① 作成名義者の印鑑の印影があれば，その押印が同人の意思に基づいて行われたと推定する(最判S39.5.12民集18-4-597)
  - ② 作成名義者の署名または押印があれば，文書の真正な成立が推定される。(民訴法228条4項）

注意：二段の推定は，①②ともに「事実上の推定」である。

みなす：前提事実が証明されたら，推定事実を覆すことはできない (例：民31条)

推定：　前提事実が証明されても，推定事実について反証できる

- 法律上の推定：推定事実の不存在を立証しなければ推定を覆せない (例：民186条2項)
- 事実上の推定：推定事実を疑わせる程度の立証で推定を覆せる (例：民訴228条4項)

(事実上の推定は，裁判官が心証を生成する過程で，経験則を利用して，ある事実から他の事実の推認を，事実上行うことを言う）

裁判における真正な成立に関する争い

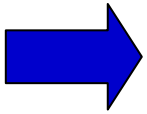
- 真正な成立を否認する場合には，理由が必要である。
  - 例えば，本人以外の者が，本人の印鑑を利用した(冒捺)。あるいは，相手方が印鑑を偽造した。
  - 「最近の技術なら印鑑の偽造は容易」というような主張で十分とは考えにくい。
- 参考
  - 民事訴訟規則145条：文書の成立を否認するときは，その理由を明らかにしなければならない。
  - 民事訴訟法230条1項：当事者またはその代理人が故意又は重大な過失により真実に反して文書の成立を争ったときは，裁判所は，決定で，十万円以下の過料に処する。

電子署名法による真正な成立の推定
(電子署名の推定効)

■電子文書については，一定の条件を満たす電子署名があれば，真正な成立が推定される。

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

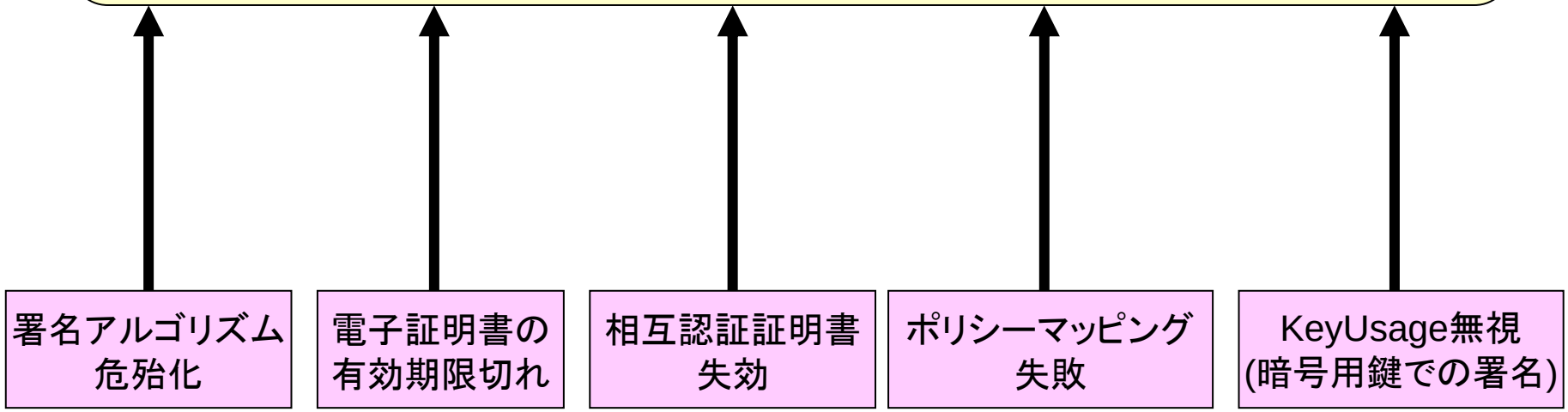
つまり，「秘密鍵等を適正に管理することにより，他人には署名が出来ないようになっている電子署名」がついていれば，電子文書の真正な成立(本人が作成したこと)が推定される。



要するに，「本人だけができる」署名がついていればよい。
これと，相互認証証明書や，ポリシー，KeyUsageなどの技術要素との関係は？

電子署名の技術的な論点と電子署名法

技術的な観点から問題のある電子署名は，民事訴訟では，どのように扱われるのだろうか



アルゴリズム危殆化の問題(1)

- コンピュータの高速化により，公開鍵から秘密鍵を計算することが可能になる。つまり，電子署名で使用している暗号方式が安全でなくなるので，「危殆化」と言っている。
- 現在，もっとも広く使われている方式であるRSA 1024bit(約300桁の数を鍵として使うRSA暗号)は，2014～17年には，世界最高速の計算機を1年使えば解読できる(公開鍵から秘密鍵を計算できる)ようになると言われている。

疑問点

特定認証業務により発行された電子証明書に基づく署名は，危殆化によって，効力を失うのだろうか。
すなわち，世界最高速の計算機を1年間専用利用すれば本人以外が署名を偽造できる場合に，「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」(電子署名法3条括弧書き)の成立はどうなるのだろうか。

アルゴリズム危殆化の問題(2)

- 2014~17年にRSA 1024bitが危殆化するとすれば，それまでに，より強い暗号(例えばRSA 2048bit)に切り替えなければならない。
- そのためには関連のシステムや，ユーザのIC-Card(秘密鍵と電子証明書を保持)などをすべて，新方式対応に切り替えなければならない。
- 電子署名法による電子証明書の有効期限は最長5年(電子署名法施行規則6条4号)なので，有効期限内に切り替えなければならない事態が発生しうる。
  - この場合，RSA1024による証明書を失効させて，RSA2048による別の証明書を発行することになる。
  - 商業的に証明書を発行している認証局に強制するのは難しい

アルゴリズム危殆化の問題(3)

- 考え方1：
  - 「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」という要件が，具体的状況において「高度の蓋然性」を持てばよいという考え方
  - → 普通の状況では「世界最高速のコンピュータの1年分の計算量」を使うことはできないので，「・・・本人だけが行うことができる」が証明され，電子署名の推定効が働く（真正な成立が推定される）
- 考え方2：
  - 「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」は，技術的解読可能性がないことまで要求しているという考え方
  - → たとえ具体的当事者が巨大なコンピュータ資源を使えなくても，技術的に解読可能なら，推定効は否定される。
  - ※ 推定効は働かないにしても，特定認証業務が発行した電子証明書に基づいていること，具体的当事者は巨大なコンピュータ資源を使えないこと，などから，他人に署名が偽造できないことを証明することはできそう。
- どちらにしても，世界最高速のコンピュータ1年分の計算量を使わなければ解読できない程度の状態では，電子署名による真正な成立の証明は可能であると考えてよいのではないだろうか？

アルゴリズム危殆化の問題(4)

■印鑑の場合との対比

- ●印鑑の場合「偽造の技術的可能性がある」というだけでは不十分で，偽造の事実まで主張しないと，真正な成立を否定できそうにない。
- ●同様に考えた時に，「署名偽造の技術的可能性」だけで，真正な成立を否定できるかどうかは，かなり疑問がある。

アルゴリズム危殆化の問題(5)

■ アルゴリズムの危殆化の態様により危険度には違いがある。

- RSA1024bitの素因数分解が，世界最高速の計算機を専有すれば，1年程度できる

  → 電子署名の有効性への影響は限定的

- RSA1024bitの素因数分解が，一般的なPCで短時間でできる

  → すべての電子署名の有効性に疑いが生じる

- SHA-1の衝突攻撃が可能になる（署名の偽造はできない場合）

  → 電子署名の有効性には，ほとんど影響はなさそう

- SHA-1の第二原像攻撃が可能になる（署名を偽造できる）

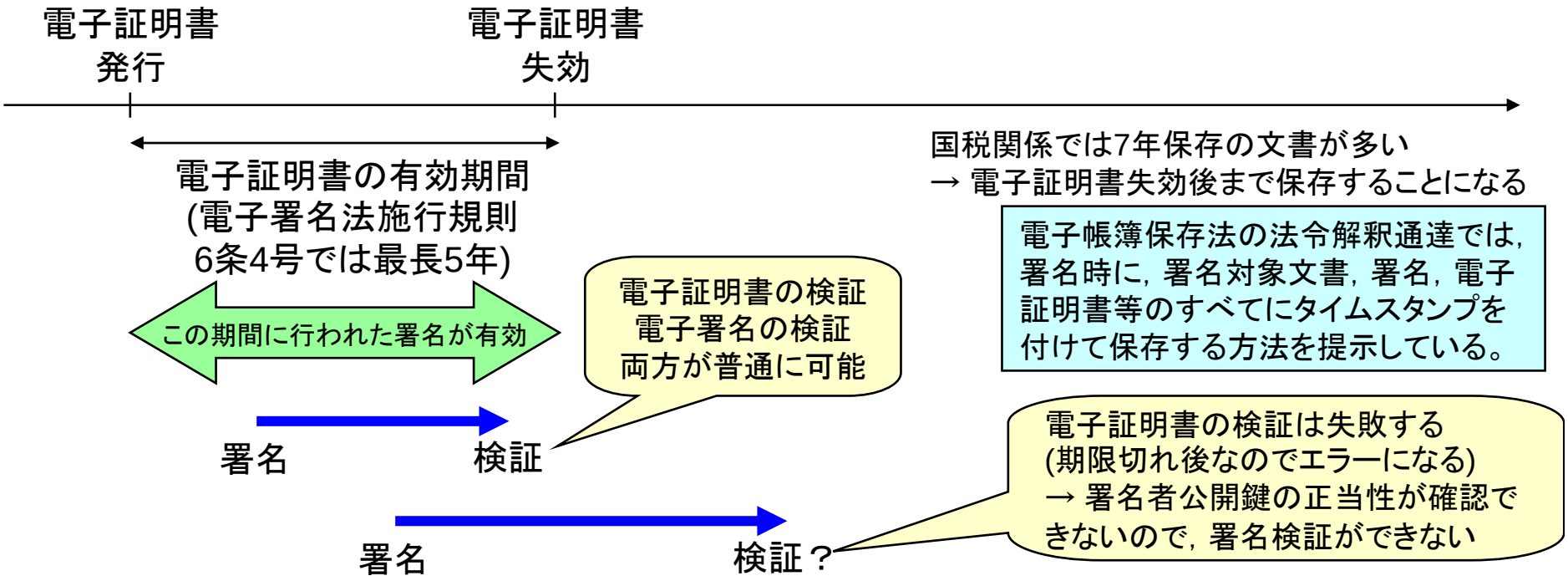
  → (必要な計算量にもよるが)電子署名の有効性に疑いが生じる

※ 危殆化の実情に合わせて，電子署名法にいう「本人だけが行うことができる」という要件が損なわれているかどうかを，検討しなければならない。

電子証明書の有効期限経過後の問題(1)

- 電子証明書には有効期限がある。
- 有効期限は延長されない。更新するとすれば，新しい鍵を作って，それに対応する新しい証明書を作る。(古い鍵は利用できなくなる)
- 期限切れ後の検証や署名の扱いの問題がある。
  - 期限切れ後は，通常の方法では電子証明書の有効性を検証できない。

→ *特定認証業務に基づく電子署名の扱いはどうなるのか*



※ 電子証明書は有効期限内でも，本人の都合等で失効することがあるが，ここでは省略した。

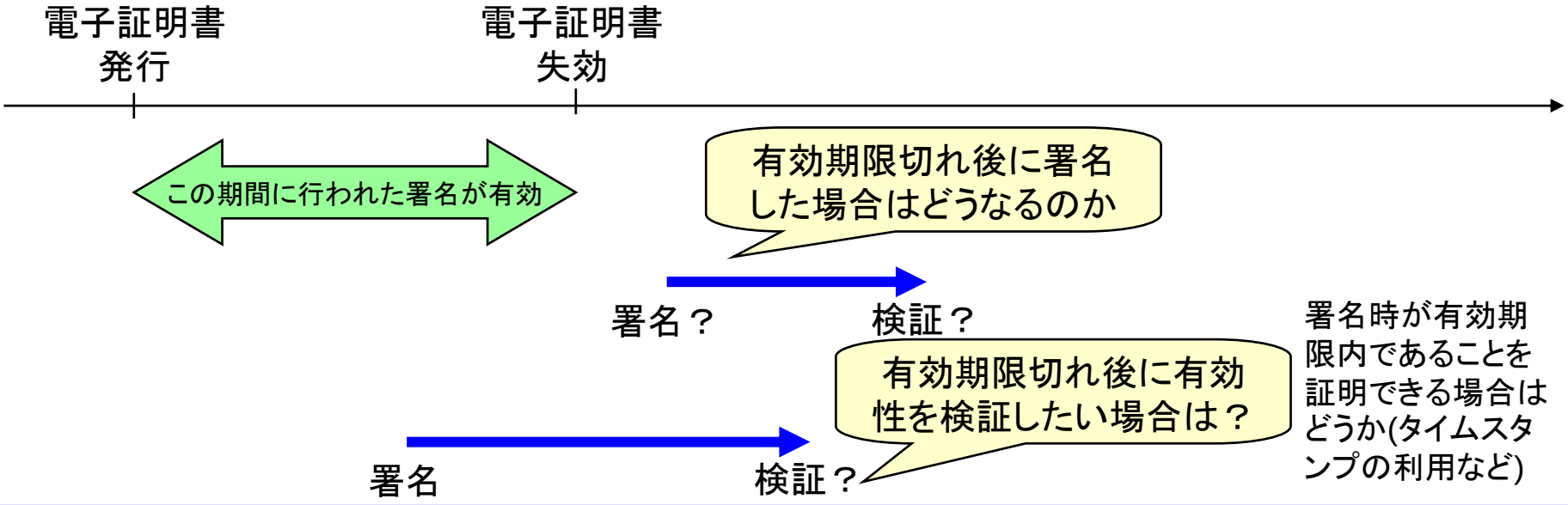
電子証明書の有効期限経過後の問題(2)

- 電子証明書失効後に署名した場合には，民事訴訟では，どう扱われるのだろうか？
- 「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」という要件は成立するのか？

※ 有効期限が切れても，ただちに，他人に署名が偽造できるとはいえない。

→ 電子署名法3条の推定効は成立するか，*そうでなくても真正な成立が認められるのではないか？（有効期限切れだけをもって否定できるのか？）*

※ ただし，失効情報が失われ，本人の管理も有効期間内とは異なってくること，有効期限後の署名は本来の利用方法とは違うことなどから，真正な成立の立証は，有効期限内の場合に比べて難しくなることが考えられる。



電子署名は裁判でどう扱われるか？

■ 本人だけができる署名かどうかが争点となる

問題点(署名の欠陥)	訴訟上の判断の例
証明書有効期限切れ後の電子署名	「認証局は，証明書有効期限切れ後まで，安全性を保証していない」と判断されることもありえるが，電子署名の暗号的な安全性から，他人には署名生成不可能と判断されうる。
暗号方式の危殆化	暗号解読(秘密鍵の解読)により，他人にも署名が可能になれば，推定効は得られない。しかし，現実的には実行できないほどの計算量が必要な場合にまで推定効が否定されるかどうかは微妙。
相互認証証明書の失効，ポリシーマッピングの失敗など	検証者が誰であるかは，本人だけが署名できたかどうかに無関係。したがって，相互認証証明書の有効性は，推定効の成否には無関係となりそう。
KeyUsageを無視した署名生成(暗号用の鍵での署名など)	KeyUsageに合っているかどうかは，本人だけができるかどうかと無関係なので，本人だけができたと認められそう。

まとめ

- 技術屋と法律屋の視点の違い
  - 電子署名の有効性を見てわかるように，同じ現象であっても，技術屋と法律屋の観点は全く違う。
  - 電子署名の技術的内容は実用上重要なものであるが，訴訟においては，そもそも裁判官に理解されない可能性があるし，理解されたとしても，電子文書の真正な成立の推定には影響しないこともありうる。
- アルゴリズム危殆化などの問題が発生した場合について
  - どの程度の危険が実際にあるのか，法的効果はどうか，をも考える必要がある。
  - いたずらに不安をあおらないように，専門家として適切な説明ができるように用意しておく必要がある。