## (A) 電子署名付きデジタルはがき、デジタル信書EM 信頼されたはがき用

\*公的・民間の電子証明書による電子署名があり、 防犯の為発信者たどれる。Mは暗号文も搭載可能

ΕM

宛名情報RESU EOAユーザ識別子A、(住所、氏名A)

> メッセージM 平文、暗号文 混合可能

差出人情報TRAU EOAユーザ識別子B、

ユーザ名又はドメイン名"例: Bob@389010X"、 住所〒389010X、 氏名Bob Bar

差出人デジタル署名・電子署名CAS

- (1) EOAの秘密鍵ETHCASKによる署名ETHCAS
  - (2) 公的・民間の電子証明書CAPCAS

トランザクションコスト、切手トークン部 トランザクションID、特定記録追跡ラベル部 差出日・トランザクション送付日時タイムスタンプ

- (B) デジタルはがき、一部メッセージ暗号化
- \*ETHCASが30APPEM-ULのユーザ識別子による署名の場合、信頼の輪により信頼される。
- \*EOAの秘密鍵はランダム生成可能でETHCASが 未認証・匿名状態のとき匿名のはがきになる。

EM

宛名情報 EOAユーザ識別子A

メッセージM 平文、暗号文 混合可能

\*防犯の為、CAPCASの無いEMの 暗号文のメッセージは消去又は 優先して表示しないノード3Aでもよい

差出人情報

EOAユーザ識別子B、ユーザ名又はドメイン名

差出人デジタル署名 (1) EOAユーザ識別子Bの 秘密鍵ETHCASKによる署名ETHCAS

トランザクションコスト、切手トークン部 トランザクションID、特定記録追跡ラベル部

- (C) デジタルはがき
- \*メッセージ公開型
- \*SNSにおける公開型メッセージ・発言

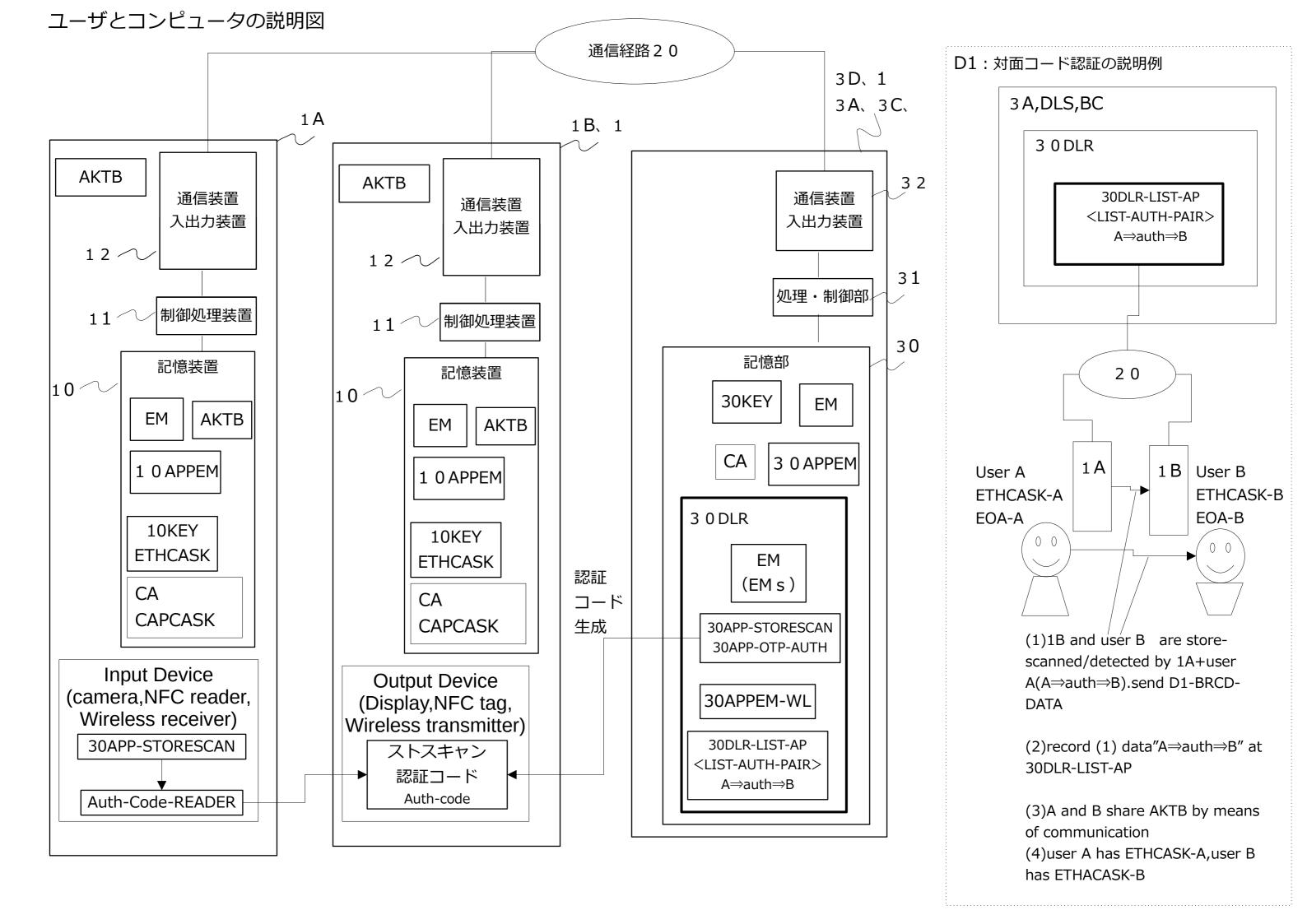
EM 宛名情報 EOAユーザ識別子A

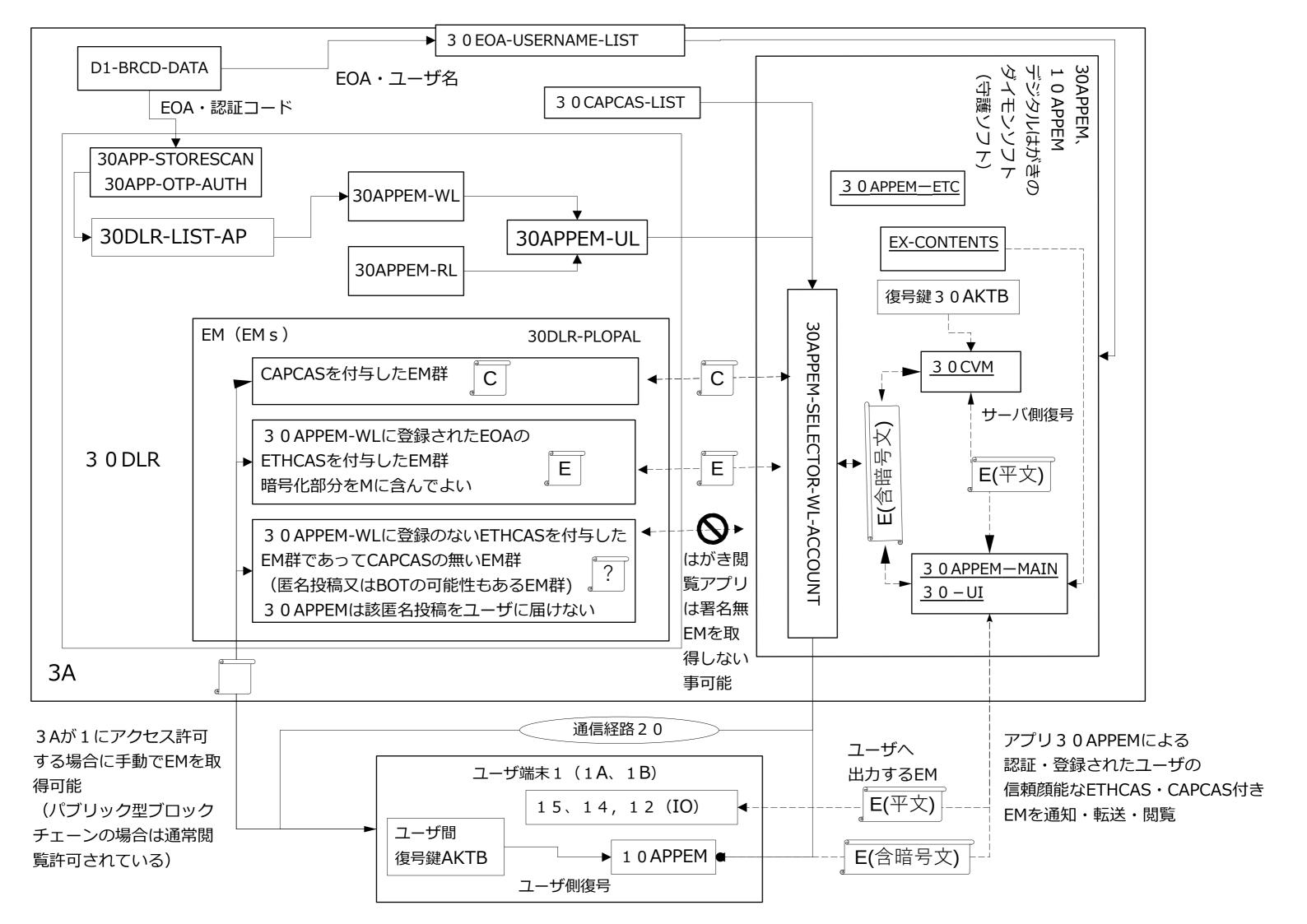
> メッセージ**M** 平文

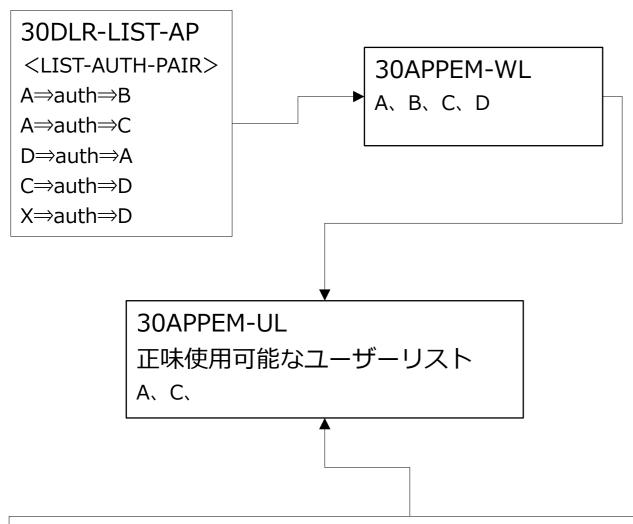
差出人情報 EOAユーザ識別子B、 ユーザ名又はドメイン名

> 差出人 デジタル署名 ETHCAS

トランザクションコスト トランザクションID







## 30DLR-LIST-CA-ET

(CAPCASによる署名が無いと失効指示できないETHCASのリスト)

<CAPCAS-ETHCAS-PAIR>

CAPCAS"AAA"⇒auth⇒ETHACAS"AAA"

CAPCAS"AAA"⇒auth⇒EHACAS "A" (\*AはCAPCAS"AAA"の署名付き失効支持がない

と削除されない。C⇒revoc\_reason:A's key is changed ⇒A の命令は無視される)

## 3 0 APPEM-RL

<LIST-REVOC-PAIR-byCAP>

C⇒revoc\_reason:user B lost B's key(at block number xxx)⇒B

C⇒revoc\_reason:D's key is changed (D changed family name)⇒D

C⇒revoc\_reason:A's key is changed (\*不正な削除)⇒A

SYSTEM⇒revoc\_reason:X's key is timeout and expired⇒X

