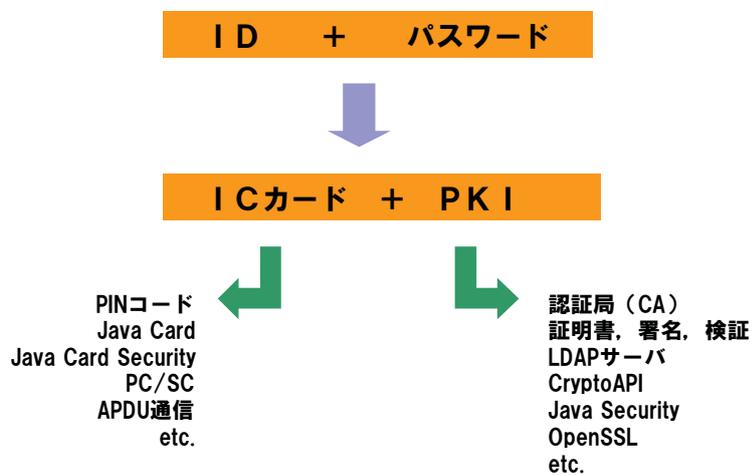


ICカードによる共有端末認証システムの構築について

名古屋大学情報連携基盤センター
葛生和人

第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター

強固なセキュリティを持ったログオン認証



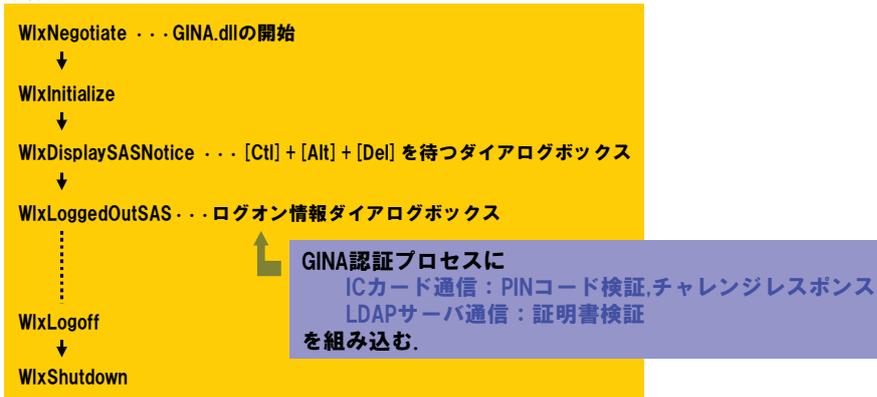
第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター

Windows系パソコンのログオン認証

GINA : Graphical Identification aNd Authentication

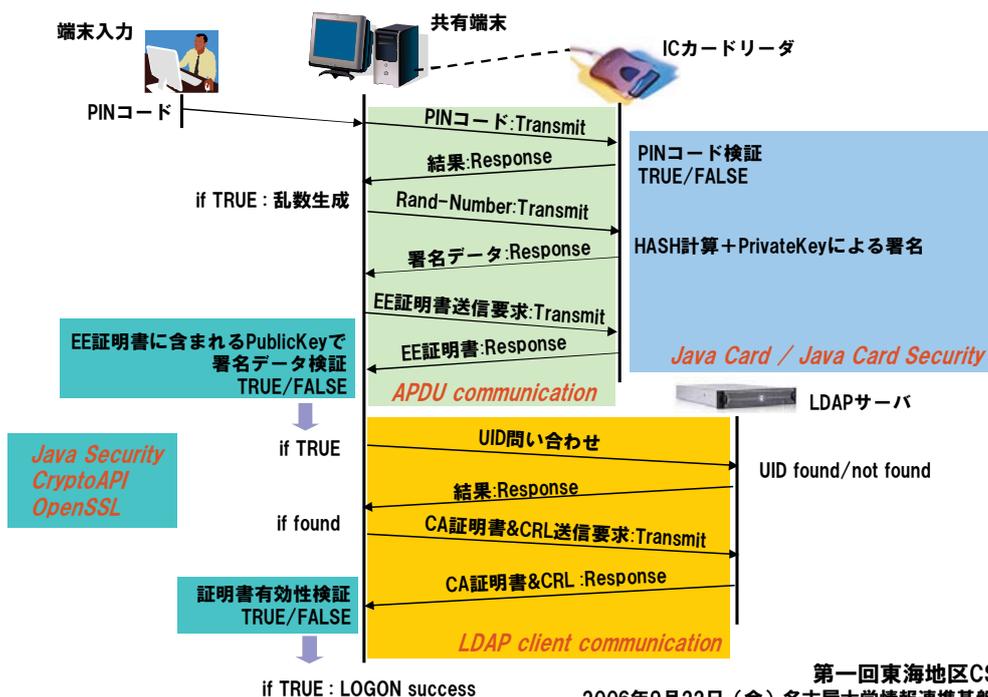
- WINLOGON.exeが持つログオン管理機能を拡張
- Windows起動時にユーザIDとパスワードを得て認証

GINA実行シーケンス



第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター

ICカードを使ったログオン時の認証手続きの流れ



第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター

ICカードを使ったログオン時の認証手続きの流れ

認証を通過するためのステップ

PINコード検証：ICカードがカード所有者のものであることの検証



乱数署名検証（CR）：PrivateKeyと証明書の整合性の検証



UID検証：UIDの実在性の検証

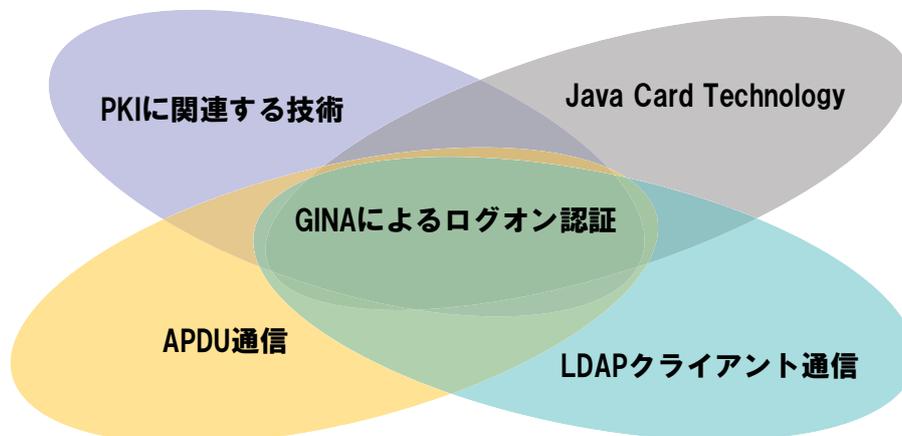


証明書検証：証明書有効性検証

(CAからの署名発行, 改竄の有無, 有効期限, 失効の有無など)

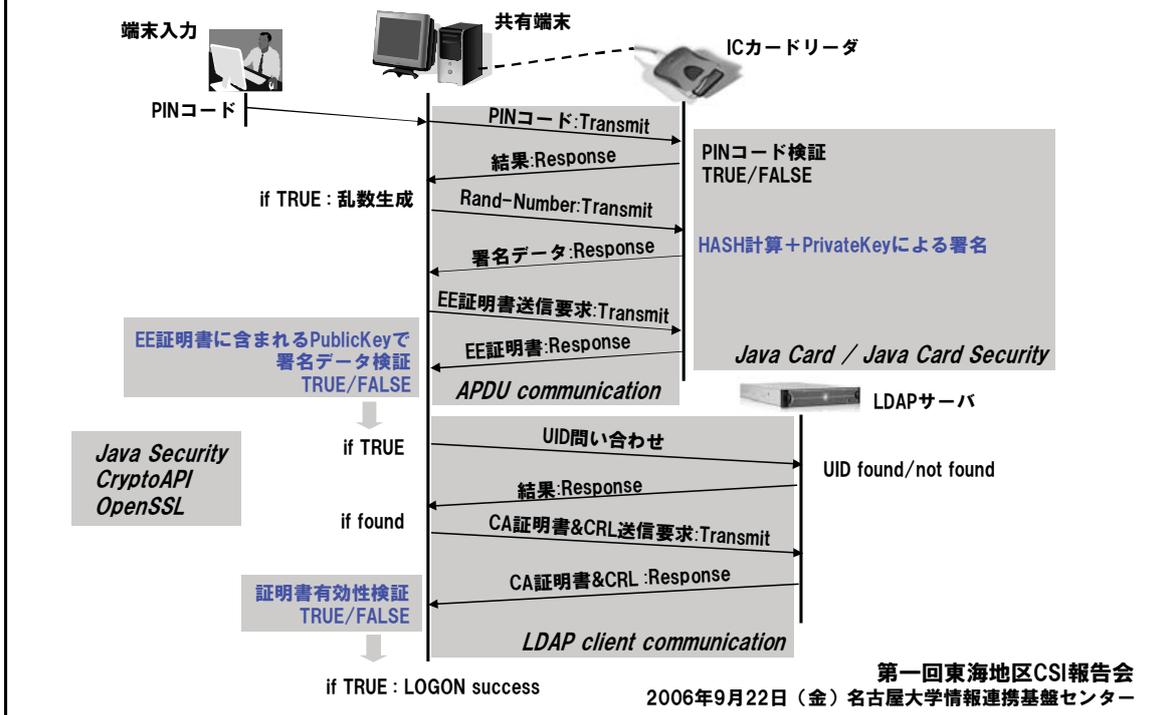
第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター

要素技術



第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター

PKIに関連する技術



PKIに関連する技術

生成したメッセージへの署名およびその検証

署名プロセス (Java Card Security)

```
//RSA PrivateKeyの実装
m_priv1024_rsakey=
(RSAPrivateKey) KeyBuilder.buildKey (KeyBuilder.TYPE_RSA_PRIVATE,KeyBuilder.LENGTH_RSA_1024, false );
//署名アルゴリズムの指定, 署名プロセスの初期化, 署名
m_signature= Signature.getInstance ( Signature.ALG_RSA_SHA_PKCS1,false );
.....
m_signature.init ( m_priv1024_rsakey, Signature.MODE_SIGN );
.....
Licc= m_signature.sign ( buffer, dO, Lc, buffer, (short) 0 );
```

検証プロセス (Java Security)

```
//X.509証明書実装
CertificateFactory cf = CertificateFactory.getInstance ("X.509");
X509Certificate cert = (X509Certificate) cf.generateCertificate (inStream);
.....
//署名アルゴリズムの指定
String alg = "SHA1withRSA";
Signature signAlg = Signature.getInstance (alg);
.....
signAlg.initVerify (cert.getPublicKey ());
signAlg.update (message.getBytes ());
boolean result = signAlg.verify (sign);
```

PKIに関連する技術

証明書の発行者による署名の検証, 有効性およびCRLの検証

ホストコンピュータ上 (Windows) のCSPを利用
各証明書, CRLをメモリ上にストアし署名検証を行う

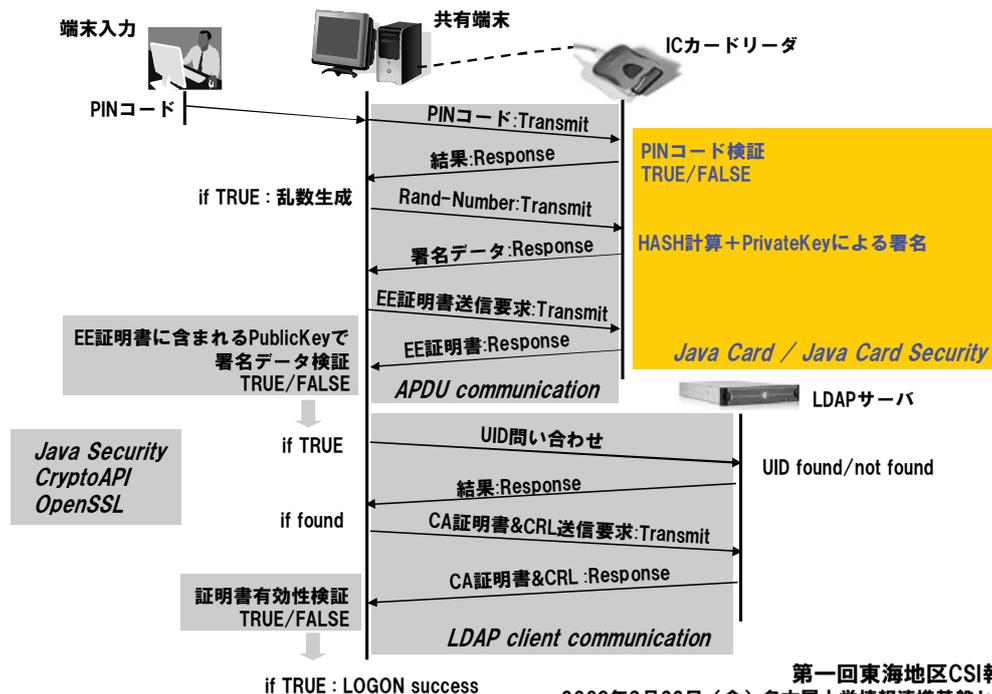
証明書検証 (Crypto API)

```
//証明書コンテキスト構築
pCertContext = CertCreateCertificateContext (X509_ASN_ENCODING, pszBuf, CertFile_Size);
//証明書ストア
CertAddCertificateContextToStore (hCertStore, pSubjectContext, CERT_STORE_ADD_REPLACE_EXISTING, 0);
.....
do {
    dwFlags = CERT_STORE_REVOCATION_FLAG |
              CERT_STORE_SIGNATURE_FLAG |
              CERT_STORE_TIME_VALIDITY_FLAG;

//証明書発行者検索
pIssuerContext = CertGetIssuerCertificateFromStore (hCertStore, pSubjectContext, 0, &dwFlags);
CertFreeCertificateContext (pSubjectContext);
if (pIssuerContext) {
    pSubjectContext = pIssuerContext;
    if (dwFlags & CERT_STORE_NO_CRL_FLAG)
        dwFlags &= ~(CERT_STORE_NO_CRL_FLAG | CERT_STORE_REVOCATION_FLAG);
    if (dwFlags) break;
} else if (GetLastError () == CRYPT_E_SELF_SIGNED) return TRUE; //自己署名検証
} while (pIssuerContext);
```

第一回東海地区CSI報告会
2006年9月22日 (金) 名古屋大学情報連携基盤センター

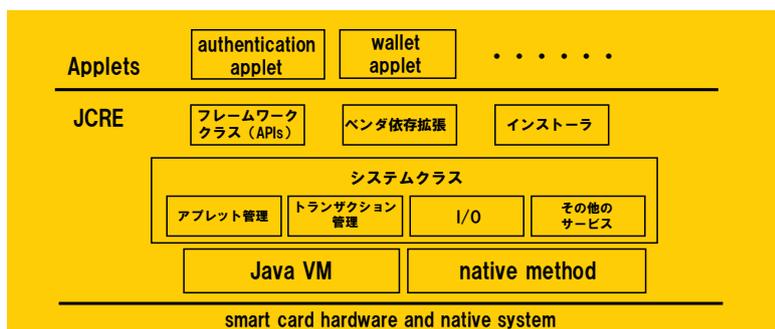
Java Card Technology



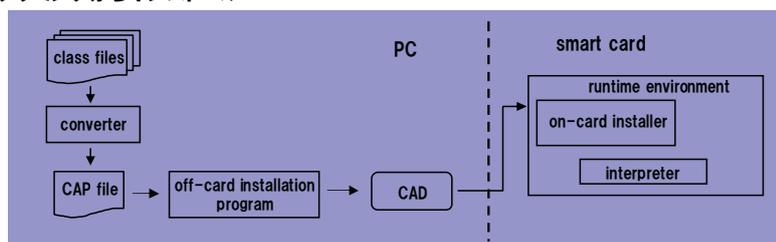
第一回東海地区CSI報告会
2006年9月22日 (金) 名古屋大学情報連携基盤センター

Java Card Technology

Java Card 実行環境



プログラミングからインストール



第一回東海地区CSI報告会
2006年9月22日(金)名古屋大学情報連携基盤センター

Java Card Technology

PINコード、Private Keyに関わるICカード内部処理

—カードから外部へ情報を出さない—

PINコード検証

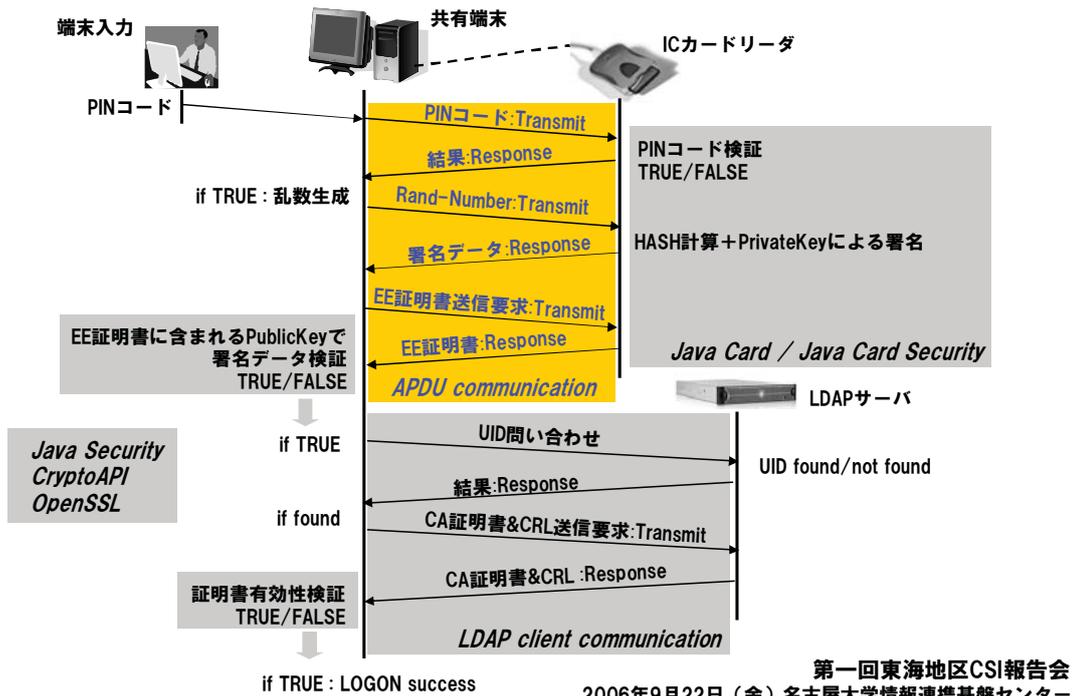
```
//PINコードの登録 (PINコードコンストラクタ)  
pin = new OwnerPIN (PIN_TRY_LIMIT, MAX_PIN_SIZE);  
pin.update (bArray, bOffset, bLength);  
register ();  
//PINコードチェック  
if ( pin.check (buffer, ISO7816.OFFSET_CDATA.byteRead) == false )  
    ISOException.throwIt (SW_VERIFICATION_FAILED);
```

Private Keyを使った受信データへの署名

```
//署名アルゴリズムの指定, 署名プロセスの初期化, 署名  
m_signature= Signature.getInstance ( Signature.ALG_RSA_SHA_PKCS1,false );  
.....  
m_signature.init ( m_priv1024_rsakey, Signature.MODE_SIGN );  
.....  
Licc= m_signature.sign ( buffer, d0, Lc, buffer, (short)0 );
```

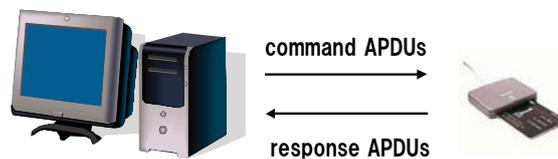
第一回東海地区CSI報告会
2006年9月22日(金)名古屋大学情報連携基盤センター

APDU通信



APDU通信

CADを通してホストコンピュータとICカード間でコマンド送信，結果受信



ISO7816-4 に基づく通信プロトコル

Command APDU structure

Mandatory header				Optional body		
CLA	INS	P1	P2	Lc	Data field	Le

Response APDU structure

Optional body		Mandatory trailer	
Data field	SW1	SW2	

APDU通信

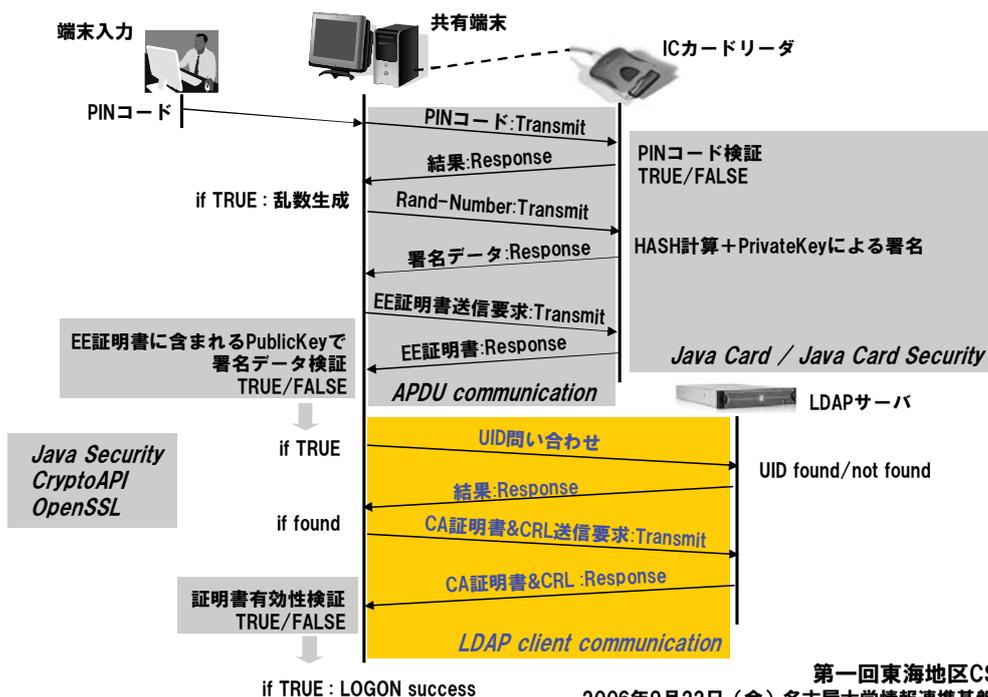
SCardTransmit関連プログラミング

```
//スマートカードコンテキストの構築
SCardEstablishContext (SCARD_SCOPE_USER, NULL, NULL, &hContext);
. . . . .
//CADとの接続
SCardConnect (hContext, rsReaders [0].szReader, SCARD_SHARE_SHARED,
              SCARD_PROTOCOL_T0 | SCARD_PROTOCOL_T1,
              &hCard,
              &dwActiveProtocol);
. . . . .
DWORD dwRecvLength_rtrv_cert_size = 4;
BYTE btRecvBuffer_rtrv_cert_size [4];
BYTE apdu_rtrv_cert_size [5] = {0x90, 0x20, 0x10, 0x00, 0x02};
. . . . .
//Command APDU送信
SCardTransmit (hCard, SCARD_PCT1, apdu_rtrv_cert_size, sizeof (apdu_rtrv_cert_size), NULL,
              btRecvBuffer_rtrv_cert_size,
              &dwRecvLength_rtrv_cert_size);

//Response APDU解析
LengCertificate = (DWORD) ((btRecvBuffer_rtrv_cert_size [0] << 8) + btRecvBuffer_rtrv_cert_size [1]);
```

第一回東海地区CSI報告会
2006年9月22日 (金) 名古屋大学情報連携基盤センター

LDAPクライアント通信



第一回東海地区CSI報告会
2006年9月22日 (金) 名古屋大学情報連携基盤センター

LDAPクライアント通信

UID問い合わせ

```
//LDAPクライアント通信の確立
version = LDAP_VERSION3;
ld = ldap_init ("〇.〇.〇.〇",LDAP_PORT);
ldap_set_option (ld, LDAP_OPT_PROTOCOL_VERSION, &version);
ldap_simple_bind_s (ld,"cn=Directory Manager,dc=sample,dc=net","aaaa");
.....
//ユーザIDの問い合わせ
ldap_search_ext_s (ld,"ou=People,dc=sample,dc=net",LDAP_SCOPE_SUBTREE, uid, NULL,0,NULL,NULL,0, &result);
.....
//ユーザIDのカウンター
counter = 0;
for (e=ldap_first_entry (ld,result); e!=NULL; e=ldap_next_entry (ld,e)) counter++;
```

第一回東海地区CSI報告会
2006年9月22日(金)名古屋大学情報連携基盤センター

LDAPクライアント通信

CA証明書, CRL送受信

```
//PrivateCAエントリへの問い合わせ
ldap_search_ext_s (ld,"ou=PrivateCa,dc=sample,dc=net", LDAP_SCOPE_SUBTREE, "(cn=Admin)",
NULL,0,NULL,NULL,NULL,0, &result);

//CA証明書, CRLの検索取得
for (e=ldap_first_entry (ld,result); e!=NULL; e=ldap_next_entry (ld,e)) {
for (a=ldap_first_attribute (ld,e,&ber); a!=NULL; a=ldap_next_attribute (ld,e,ber)) {

if ( ( strcmp (a,"cACertificate:binary")==0) || ( strcmp (a,"certificateRevocationList:binary")==0) ) {
bvals = ldap_get_values_len (ld, e, a);
if (bvals != NULL) {
for (i = 0; bvals [i] != NULL; i++) {
if ( strcmp (a,"cACertificate:binary")==0) {
pszBuf_CAcert_size = bvals [i] ->bv_len;
pszBuf_CAcert = (BYTE *) malloc (pszBuf_CAcert_size);
for (j = 0; (unsigned long) j < bvals [i] ->bv_len; ++j) pszBuf_CAcert [j] = bvals [i] ->bv_val [j];
} //if CACertificate
.....
} }
else { ..... }
.....
} //CA証明書から証明書コンテキストの構築
pCertContext_CAcert = CertCreateCertificateContext (X509_ASN_ENCODING, pszBuf_CAcert, pszBuf_CAcert_size);
..... } }
```

第一回東海地区CSI報告会
2006年9月22日(金)名古屋大学情報連携基盤センター



今後

非接触仕様対応

正規版アプリケーション開発

第一回東海地区CSI報告会
2006年9月22日（金）名古屋大学情報連携基盤センター