本資料について

- 本資料は下記論文を基にして作成されたものです。文章の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 題目：A New On-line Certificate Validation Method using LDAP Component Matching Technology

- 著者：Jong Hyuk Choi, Sang Seok Lim, Kurt D. Zeilenga

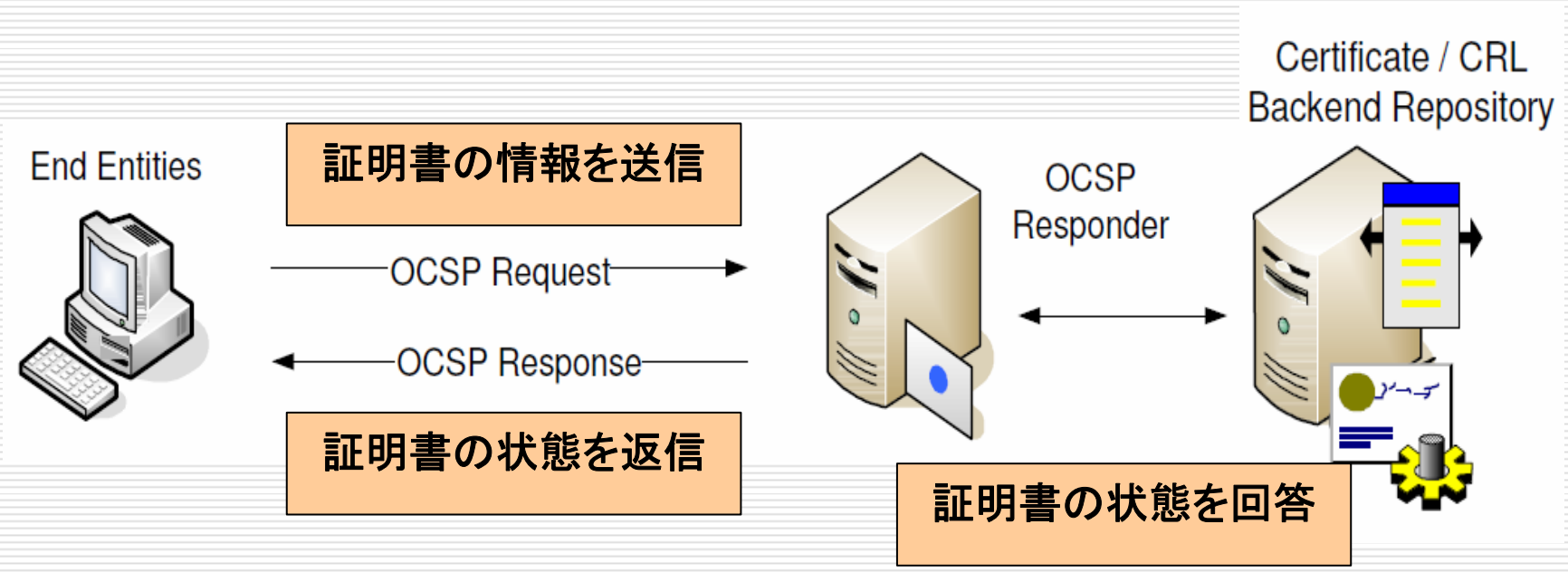
オンライン証明書確認法

名城大学理工学部
渡邊研究室
川島隆太

Online Certificate Status Protocol（OCSP）

- デジタル証明書の有効性をリアルタイムで確認するプロトコル
- クライアントから証明書が失効されているかどうかを調べる処理の負担をなくす

Online Certificate Status Protocol（OCSP）



Online Certificate Status Protocol（OCSP）

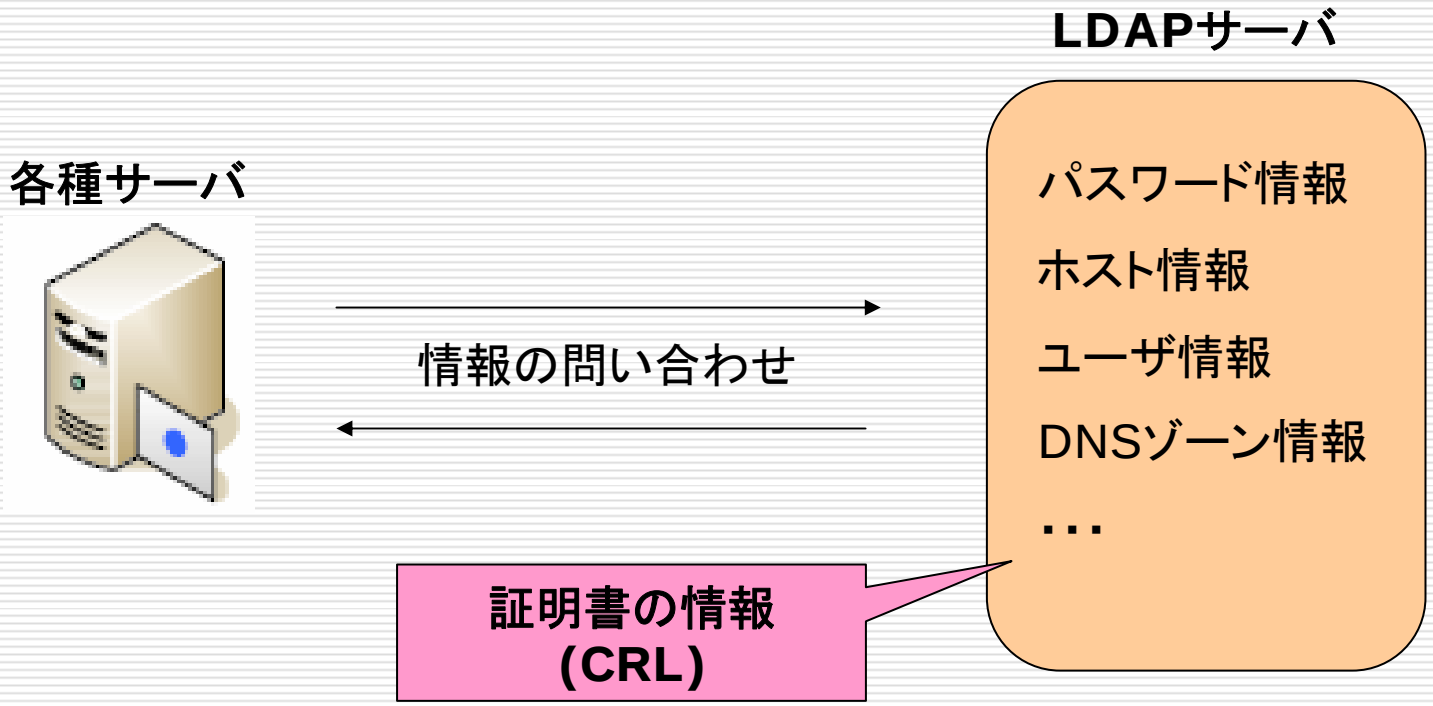
- レスポンスに電子署名を付与するため、パフォーマンス上の問題が発生
  - 待ち時間の増加
  - スループットの減少

Lightweight Directory Access Protocol（LDAP）

- ディレクトリサービスにアクセスするプロトコル
- データの追加や削除よりも検索を重視
- CRLや証明書の配布にも使用されている

Lightweight Directory Access Protocol（LDAP）

- 様々な情報の一元管理が可能



証明書破棄リスト(CRL)の構造

```
CertificateList ::= SIGNED { SEQUENCE {
    version                 Version OPTIONAL,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    thisUpdate              Time,
    nextUpdate              Time OPTIONAL,
    revokedCertificates SEQUENCE OF SEQUENCE {
        serialNumber          CertificateSerialNumber,
        revocationDate        Time,
        crlEntryExtensions Extensions OPTIONAL } OPTIONAL,
    crlExtensions    [0] Extensions OPTIONAL }}
```

(a) Certificate Revocation List.

Version:CRLのバージョン番号

Signature:CRL 発行者の電子署名

Issuer:発行認証局名

thisUpdate:CRLが発行された日時

nextUpdate:次のCRLが発行される期限

revokedCertificates:失効した証明書のリスト

serialNumber:失効した証明書のシリアルナンバー

revokationDate:失効した日時

crlEntryExtensions:CRLエントリ拡張

crlExtensions:CRL拡張

LDAP検索フィルタ

```
( certificateRevocationList:
    componentFilterMatch:=
      item:{ component "toBeSigned.
        revokedCertificates.*.serialNumber",
      rule integerMatch, value 12345 } )
```

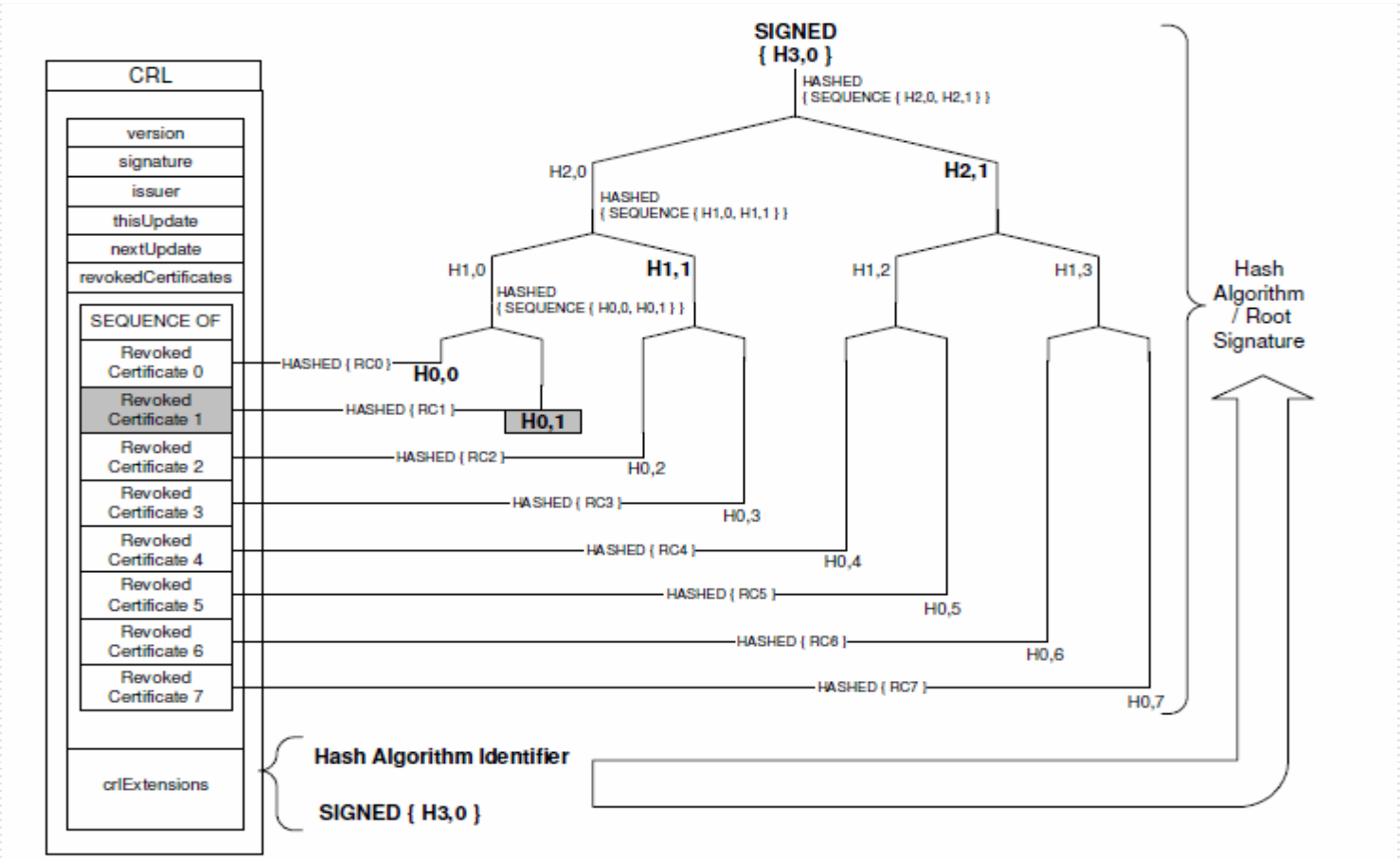
(b) LDAP Filter for CRL Component Matching.

- CRLの失効した証明書のリストの中に、シリアルナンバーが12345の証明書が存在しているかを検索するフィルタ

証明書破棄木(CRT)

- 証明書の破棄情報を効率的に管理および伝達する手法
- 証明書の破棄リストを基にシリアル番号を葉に持った二分木を生成
- 部分木で証明書の有効性を確認

木構造化されたデータ構造



CRLの証明書数に対して必要なハッシュ数