オープンソース署名＆認証ラボ

Open-source Signature and Authentication Laboratory

https://www.OsSAL.org/

サルオフ #1

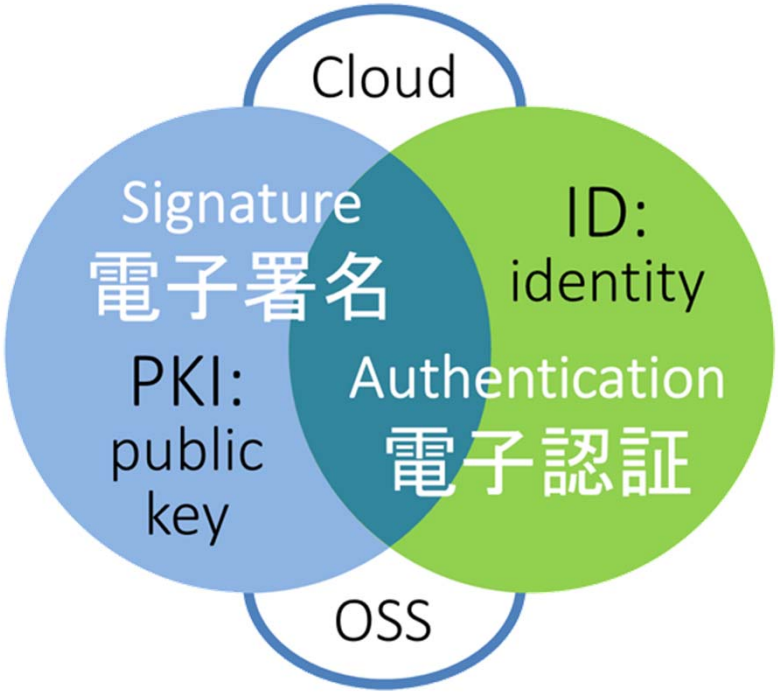
2019年6月19日

署名ブタ野郎は
認証先輩の夢を見ない

SAL No.0001 miyachi@langedge.jp

主催 OsSAL.org（オッサル）とは？

オープンソースを開発＆活用して、電子署名と電子認証について、研究しつつ学んで行く為の主にオンライン上のオープンなグループです。



https://www.OsSAL.org/

参加自由！退会自由！会費無し！
個人ベースでの参加と活動が可能。
運営は主メンバーのサルメンが担当。
サーバ維持費等はメインスポンサーが負担。
他スポンサーはイベント毎に設定。

サルオフとは？

オッサル（OsSAL.org）のオフラインの**勉強会**。
会場費や珈琲代等はスポンサーが支出。
運営はボランティアベースのサルメンが担当。
発表者も無償のボランティアでの発表です。
つまり企業や個人の善意で運営されています。
以下がお願いとなりますのでご注意ください。

※ 資料は出来るだけ公開しますが特に営利目的の再利用や、発表内容の記事やメディアへの転載等はご遠慮頂くか、最低でも発表者本人へ確認して下さい。基本的にプライベートな勉強目的での発表と資料公開です。

責任者はだれ？

メインスポンサー：

有限会社ラング・エッジ

サルメンNo.0001：**@le_miyachi**（miyachi@langedge.jp）

属性：プログラマ（PKI/ドキュメント系、ID系も少し…）

兼 ラング・エッジ（ぼっち有限会社）取締役

何故オッサルを始めたの？

- 基本的には**趣味**です！（巻き込みごめんなさいw）
- PKI/IDプログラマを世の中に増やしたい！
- ついでに新たな市場も作り育てたい！

署名(Certification)と認証(Authentication)

署名：否認防止、改ざん防止

- 本人確認は証明書発行時に行われる。
- 署名における認証がCertificationである。
- PKIとデジタル署名を使った技術が一般的。
- デジタル署名は検証情報をパッキングできる。

だから認証局は Certification Authority (CA)

認証：本人性の保証と確認

- 正確には本人確認はID発行時に行われる。
- ID発行時に認証クレデンシャルが提供される。
- 認証クレデンシャルによりID確認を行なっている。
- OpenID/OAuth系やSAML等の技術が一般的。
- 認証と証拠を使った否認防止もあり得る。

認証局ではIdP (ID Provider) の仕事

個人的な主観

署名も認証も技術（手段）に過ぎない。

開発するサービスやプロダクト**（目的）**に応じて
両方を使いこなす技術者が求められている？

特にPKIや電子署名は歴史がある為かオープンな
情報やソフトウェアが少ない気がするので増やす！

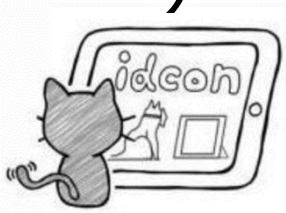
オッサルの目的は誰でも参加可能かつ忖度無しで、
今使えるID/PKIの技術によって実装できる技術や
仕様を学ぶ場を作る事です。

ID厨とPKI厨（独断と偏見による）

ID厨（ID/認証系技術者）が参加するイベント

#idcon (Identity Conference) - **OIDF-J**

https://idcon.connpass.com/



PKI厨（PKI/署名系技術者）が参加するイベント

PKI Day – ***JNSA***（PKI相互運用WG/電子署名WG）

https://www.jnsa.org/seminar/pki-day/2019/

※ サルオフはこの間をゆる～く結びたい。
一般の実装技術者向けに浅く広く！

サルオフ#1のサブタイトル解説

署名ブタ野郎とは、電子署名PKI技術者のこと。
現在のオッサルのメインメンバーがこの分野の技術者です。
PKIは古い技術なので最新のクラウド等へ対応できないブタ野郎です。

署名ブタ野郎は
認証先輩の夢を見ない

クラウドと言えばやはり認証技術は必須なので電子認証ID技術者、
つまり認証先輩の力を借りて勉強したいのです。
これからの電子署名にも電子認証技術は必須なのです。

※ ついでに言うと、ええ…某ラノベ・アニメのタイトルもじりですw

署名と認証の関係（その一部）

1．認証を使った署名

- リモート署名（クラウド署名）
  - クラウド署名の仕様書はOAuth2.0の理解が必要。
- 認証と管理ログによる署名の考え方
  - この辺りは宮内先生から説明があるはず。

宮地

宮内先生

2．署名を使った認証

- ICカード（秘密鍵）によるクライアント認証
  - マイナンバーカードが使えると協力なインフラになる？
- FIDOによる秘密鍵/公開鍵の仕組み
  - 認証系でもPKIの知識はあった方が良いですよね？
- JWTのような署名トークン
  - 認証系でも暗号の知識はあった方が良いですよね？

濱野さん

いとうさん

3．共通項

- 本人確認（そもそも本人確認とは？）

本日のメニュー

【趣旨説明】OsSAL概要とサルオフ#1の趣旨説明

SAL No.0001　宮地 直人（プログラマ）　有限会社ラング・エッジ

【発表1】リモート署名は電子署名法の夢を見るか

SAL No.0002　宮内 宏（弁護士）　宮内・水町IT法律事務所

【ＬＴ】測定機器データの長期保存・施設間での移行の課題

上原 小百合　JIIMA R&Dデータ保存研究会・製薬会社社員

ユーザの立場での課題提起

【休憩】珈琲ブレイク（珈琲スポンサーのプレゼン）

【発表2】ICチップによる本人確認

濱野 司　オープンソース・ソリューション・テクノロジ株式会社

【発表3】コンシューマ向けサービスで使われている認証認可仕様とデジタル署名

いとう りょう (@ritou)　株式会社ミクシィ

【ミニ討論】マイナンバーカードの認証用証明書は使えるか？

サルオフ#1の後援とスポンサー

■後援（5団体）

- 一般社団法人OpenIDファウンデーション・ジャパン（OpenID Foundation Japan）
- NPO日本ネットワークセキュリティ協会（JNSA）
- 公益社団法人 日本文書情報マネジメント協会（JIIMA）
- 先端IT活用推進コンソーシアム（AITC）
- 一般財団法人日本情報経済社会推進協会（JIPDEC）

■珈琲スポンサー（3社）

- オープンソース・ソリューション・テクノロジ株式会社
- アンテナハウス株式会社
- 株式会社テクリエ

ありがとうございました！

オッサル（OsSAL.org）活動概要

サルメン（サルメンバー）

- オッサルの活動に協力してくれる主メンバー。
  - **いつも協力ありがとう！感謝しています！**
- 特に資格は無く**手を挙げれば誰でもなれる**。
- サルメンには4桁サルナンバーが発行される。
  - 4桁縛りは無く更に言えば好きな番号を自己申告制。
- **恥ずかしくなければ**オッサルのトップに記載。
  - 恥ずかしければ情報公開無しでサルメンも可能！
- オッサルの活動に**参加するだけなら**Slack登録。
  - 質問もあれば可能な範囲で対応。Slackは後述。
- ご興味があれば連絡か声をかけてください！
  - なお**いつでも辞めることができます**w お気軽に。

サルオフ (オフライン活動)

勉強会の開催

署名/認証ラボ
OsSAL サルオフ
Open-src Sign & Auth Labo

Connpassグループ

https://ossal.connpass.com/

次回は**サルオフ#2**、不定期に開催を予定。
年に1回以上は開催したいとは考えています。

机と珈琲は最低用意したい！可能なら電源やWiFiも！

聞きたい発表者やネタは常に募集中です！
是非アンケートに書いてください！

サルオン (オンライン活動)

オッサルの活動は出来る限りオンラインで行う。
（オフラインで会うのは勉強会や飲み会だけにしたいw）

Slack：議論・情報共有
https://OsSAL.slack.com/

招待リンクは
OsSAL.org で
公開中です

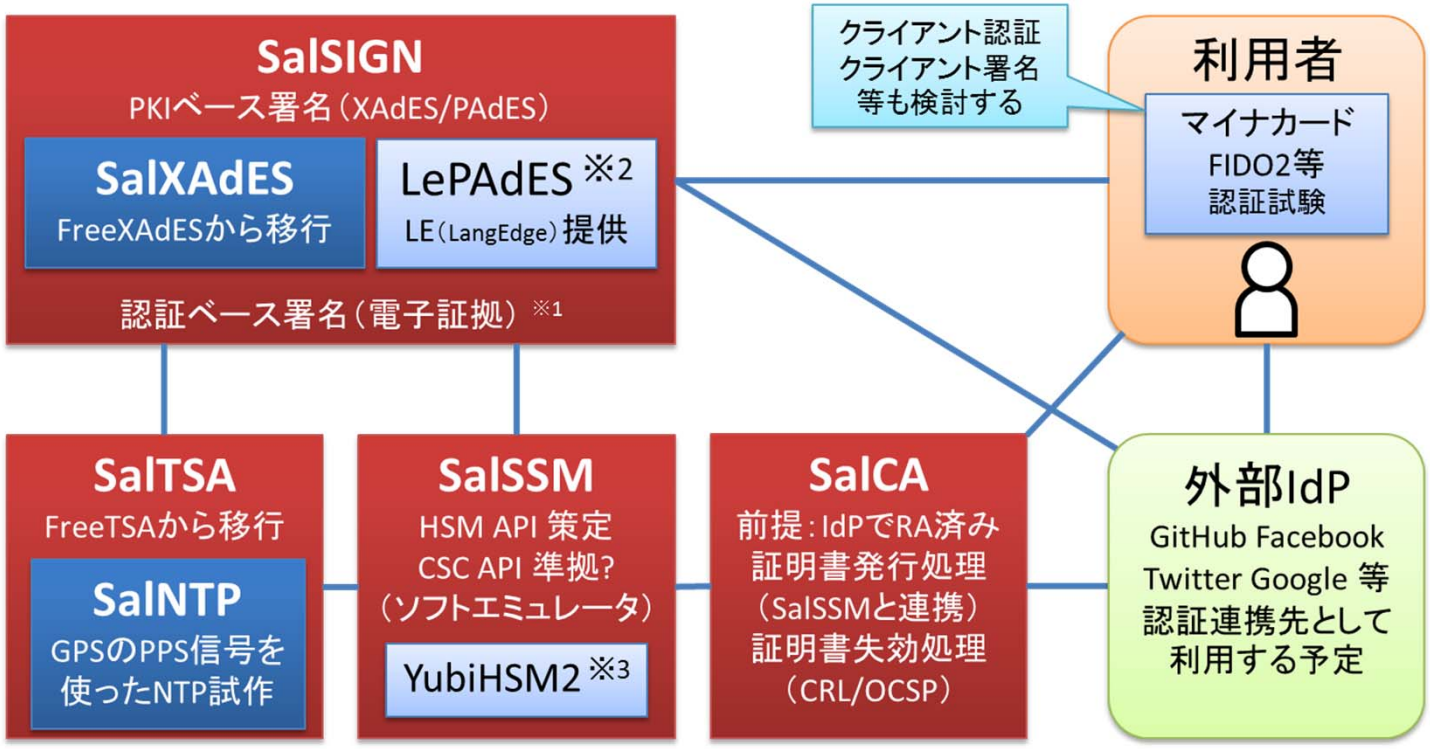
GitHub：ソース共有
https://github.com/OsSAL/

SlideShare：ドキュメント共有
https://www.slideshare.net/OsSAL-org/

サルプロ (オープンソース活動)

現在はほぼ @le_miyachi の個人活動。

将来的に共同開発者や別プロジェクトが増えると嬉しいなぁ。



※1 電子認証＋電子証拠ベースの米国型電子署名も試作してみる。
※2 さすがにPAdESのオープンソース化は難しいのでLE製品を…
※3 LE保有の安価なHSMのYubiHSM2も試してみる。

※4 ライセンスは全てMPLを予定。

署名系のサルプロ概要

➢ SalXAdES：XML長期署名ライブラリ

- 既存**FreeXAdES**から移行、現在JavaでXAdES-Tまで作成可能。

➢ SalTSA：RFC3161タイムスタンプサービス

- 既存**FreeTSA**から移行、 Ruby/PerlからOpenSSLを使う試験用。

➢ SalCA：試験用の認証局API

- クラウドHSMと連携可能な試験用認証局サービス。

➢ SalSSM (HSM)：秘密鍵管理API

- リモート署名で推奨されるHSMの試験用ソフト実装のサービス。
- 安価なHSMであるYubiHSM2も試してみる予定。

➢ SalSIGN：リモート署名API

- 上記プロジェクトを利用したリモート署名の試験用サービス。
- 外部IdPによる認証連携の機能も利用する。
- 認証ベース（ログ管理）の署名についても検討したい。
- PAdESライブラリはLE製品版を提供予定（署名は試験用のみ）。

SalMETA：メタ情報管理リポジトリ

➢ 文書やデータのメタ情報のバージョン管理

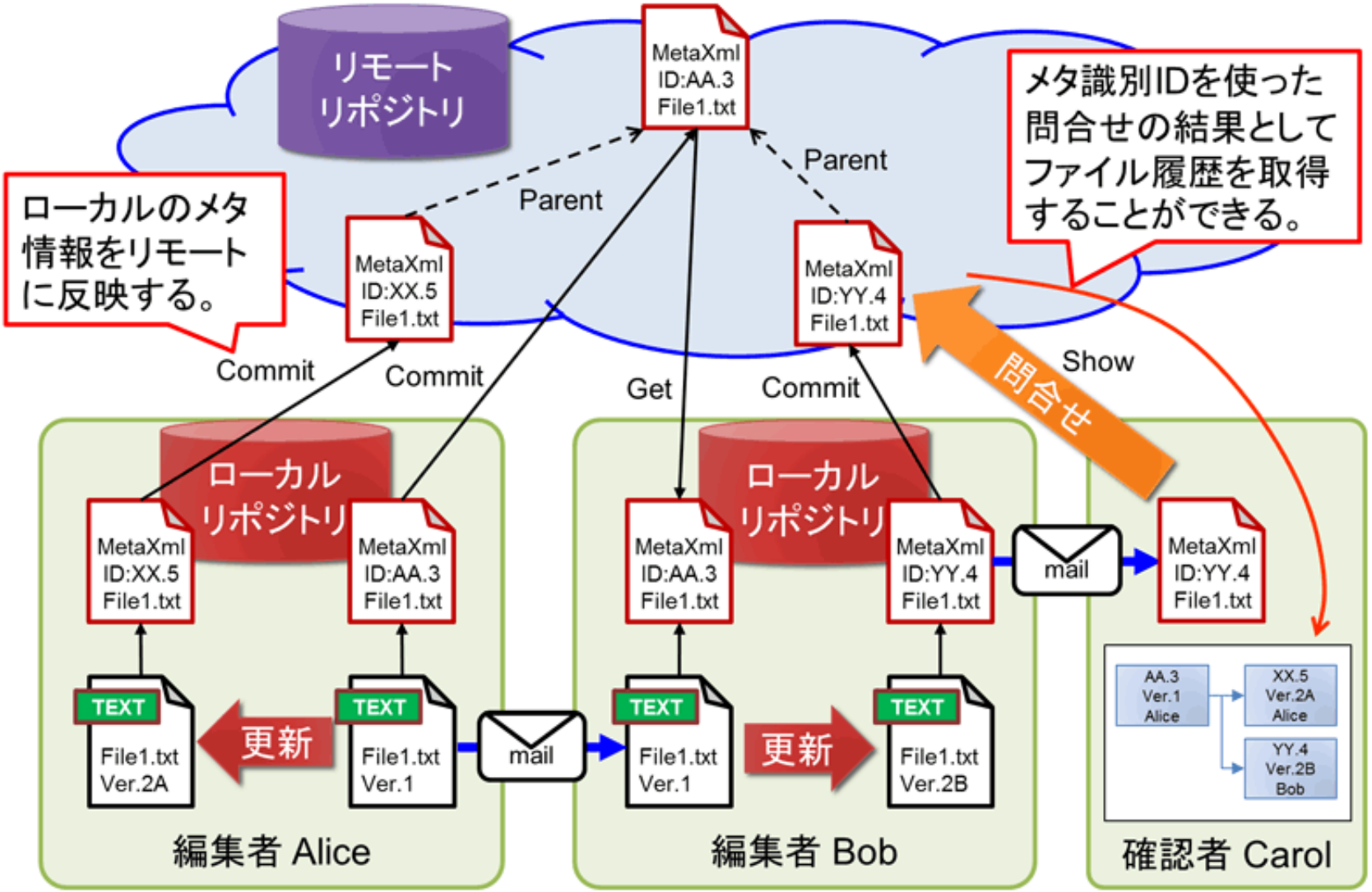
- 文書・データの本体は管理しない。
- 文書・データをハッシュ値等で識別してツリー化。
- ツリー自体は利用者が管理設定する。
- ハッシュツリーによりリンクして行く。
- 署名/タイムスタンプ/ブロックチェーン等の追加。

➢ Git（ソースのバージョン管理）のメタ情報版に近い

- Gitに対するGitHubのようにSalMETAのサービス化も可能。公開サービス以外にオンプレでも利用可能。
- 専用コマンドによりサービスにコミットして行く。

※ アジャイル開発で有用性を確認して行く予定。

SalMETA概要図


リモート
リポジトリ
MetaXml
ID:AA.3
File1.txt
メタ識別IDを使った
問合せの結果として
ファイル履歴を取得
することができる。
ローカルのメタ
情報をリモート
に反映する。
Parent
Parent
MetaXml
ID:XX.5
File1.txt
MetaXml
ID:YY.4
File1.txt
Commit
Commit
Get
Commit
Show
問合せ
ローカル
リポジトリ
ローカル
リポジトリ
MetaXml
ID:XX.5
File1.txt
MetaXml
ID:AA.3
File1.txt
MetaXml
ID:AA.3
File1.txt
MetaXml
ID:YY.4
File1.txt
mail
MetaXml
ID:YY.4
File1.txt
TEXT
File1.txt
Ver.2A
更新
TEXT
File1.txt
Ver.1
mail
TEXT
File1.txt
Ver.1
更新
TEXT
File1.txt
Ver.2B
AA.3
Ver.1
Alice
XX.5
Ver.2A
Alice
YY.4
Ver.2B
Bob
編集者 Alice
編集者 Bob
確認者 Carol

サルプロ詳細

サルオフ#2 以降で順次解説予定！

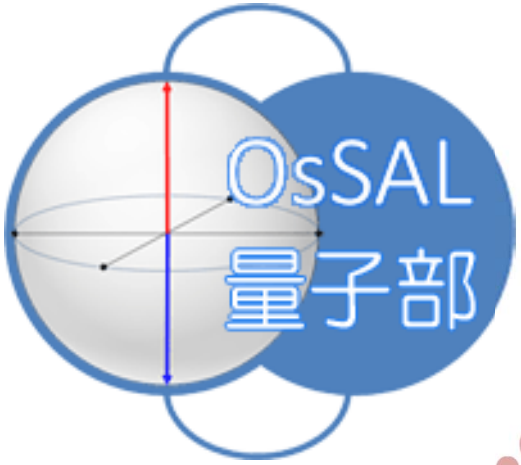
SalXAdES：XAdES-X-Long 検証編
SalSIGN：リモート署名実装してみた
SalMETA：メタ情報による文書追跡

とは言え空き時間に開発しているので、
気長にお付き合いください m(_ _)m

開発状況等はSlackで！（是非ご参加を！）

サル量子部

https://www.ossal.org/qc/



もう完全に
趣味
の世界ですw

署名/認証ラボ
OsSAL サルオフ
Open-src
Sign & Auth Labo

2019夏 に勉強会（**サル量子#1**）を開催予定

古典プログラマの為の量子プログラミング入門

第1部：関連数学と1量子ビット計算
第2部：量子ゲート型のプログラミング
第3部：量子アニーリング型のプログラミング

ショアのアルゴリズムもやります。

サルオフ#1

署名ブタ野郎は
認証先輩の夢を見ない

それではお楽しみください！

お願い：アンケートをお願いします。
お配りした紙にGoogleフォームのURL/QRコードがあります。
無記名で結構ですので6月26日(1週間)までに是非ご記入を！