MAFFIN
Anytime anywhere, Collaborative Research Environment

組織の壁を超える 利用者グループ概念の導入

～農林水産研究における新しい認証基盤～

農林水産技術会議事務局筑波事務所
(農林水産研究情報総合センター)
宮坂 和孝

本日の内容

MAFFIN
Anytime anywhere, Collaborative Research Environment

- **内容は「情報共有サービス」と「認証基盤」です**
  - 利用者の所属組織の内部・外部を問わない、非常に柔軟な情報共有サービスの事例紹介を行います
  - サービス実現に不可欠な認証基盤についても、詳しく紹介します
- **発表の流れ**
  1. はじめに(情報共有サービスについて)
  2. 農林水産研究情報総合センターについて
  3. 情報共有サービスの改善
     1. 現行システムの問題点
     2. 次期システムのコンセプト
     3. 認証基盤の実装
     4. 認証基盤を活用するアプリケーションの整備
  4. 今後の課題(認証連携時代に向けて)
  5. まとめ

MAFFIN
Anytime anywhere, Collaborative Research Environment

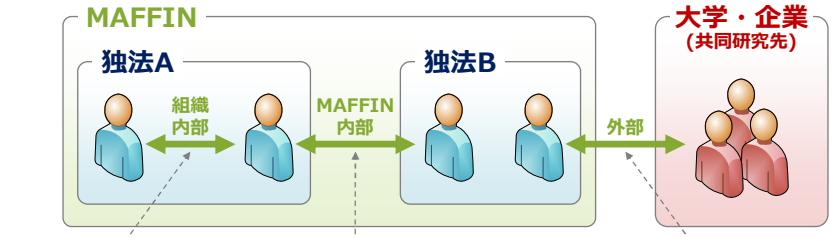
はじめに

情報共有サービスについて

情報共有サービスについて

MAFFIN
Anytime anywhere, Collaborative Research Environment

- **産学官の連携はますます重要に**
  - 緊密な連携には情報共有が不可欠
  - どうすれば外部組織との情報共有がスムーズに行えるのか
    - カギは認証とアクセス制限
- **内部利用者の情報共有パターン**



同一組織内部の利用者と
- 独法側導入グループウェア
- 電子メール
- メーリングリスト
- 研究データ交換システム

MAFFIN内の他の組織の利用者と
- 電子メール
- メーリングリスト
- 研究データ交換システム

他の組織の利用者と
- 電子メール
- メーリングリスト
- 研究データ交換システム

MAFFIN
Anytime anywhere, Collaborative Research Environment

農林水産研究情報総合センターについて

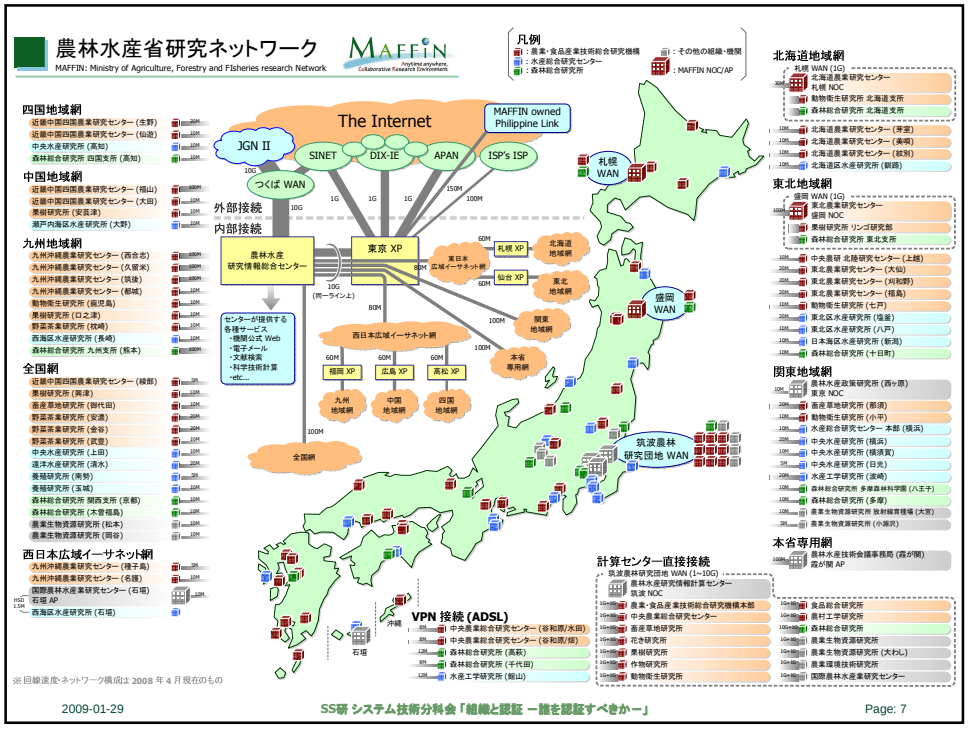
農林水産研究情報総合センターとは

MAFFIN
Anytime anywhere, Collaborative Research Environment

- **農林水産技術会議事務局筑波事務所が運営**
  - 国の機関、所在地つくば、30年以上の歴史(名称変更あり)
- **農林水産省研究ネットワーク(MAFFIN)を整備・運用**
  - 全国に展開する農林水産研究拠点を結ぶネットワーク
  - 「いつでも、どこからでも使える共同研究環境」の実現を目指す
    - "Anytime anywhere, Collaborative Research Environment"

ロゴにも記載

- **ネットワークから利用可能な各種サービスを運用**
  - 科学技術計算システム
  - ネットワークライブラリシステム
  - ネットワークサービスシステム
    - DNS、メール、利用者情報管理、情報共有サービス
  - AGROPEDIA(農学情報資源システム)など……



当センターの内部利用者

MAFFIN Anytime anywhere, Collaborative Research Environment

- **規模**
  - 約10,000人(うち研究者は約4,500人)
- **範囲**
  - 農林水産省の職員
  - 省の所管する独立行政法人の役職員と受け入れ職員
  - 省が推進する競争的資金による研究・プロジェクト研究等に参画する都道府県・大学・民間の研究機関の職員
  - etc...

※大学や企業の研究者でも当センターの「内部利用者」となることができます
参考: http://www.affrc.go.jp/PDF/news/pdf/news_no26.pdf
(ただし、一部のサービスは利用できない場合があります)

- **内部利用者特典**
  - 各種サービスが利用可能に
    - ネットワーク系サービス(メール、メーリングリスト、NAS、VPNなど)
    - 計算系サービス (スパコン、アプリケーションなど)
    - 図書館系サービス (文献複写依頼、オンラインジャーナルなど)

当センターの認証系システムの変遷

- **センター設立当初から認証情報は一元管理**
  - 古くはメインフレームの利用者管理から
  - 1993年に所属管理用の利用者管理データベースを作成
  - メールサーバが各地域に分散していた頃でも、認証情報はセンター側で集中管理して各サーバに反映
- **2000年度システムでの改善**
  - 利用者管理システムを導入
    - 利用者管理データベースのWebフロントエンド
  - LDAPを導入
    - メール、ネットワークストレージ(FTP/CIFS)などの認証を一元化
- **2004年度システムでの改善**
  - WebSSO(Cookie有効範囲内で利用可能なSSO)を導入
    - 各システムをシームレスに渡り歩けるようになった

2008年度システム更新

- **システム更新は4年に一度**
  - 稼働から2年が経過した時点で取りまとめる「中間評価報告書」の内容に基づいてシステム設計を行う
- **2008年度システムの更新経緯**
  - 2005.03 現行システム(2004年度システム)稼働
  - 2006.12 中間評価作業部会設置
  - 2007.04 中間評価報告書
  - 2007.09 システム設計作業部会設置
  - 2007.12 資料招請
  - 2008.05 意見招請
  - 2008.07 仕様書配布
  - 2008.09 入札・受注者決定
  - 2009.03 新システム稼働(予定)

大まかなシステム構想は
2006年夏頃~2007年秋頃に

MAFFIN
Anytime anywhere,
Collaborative Research Environment

現行システムの問題点

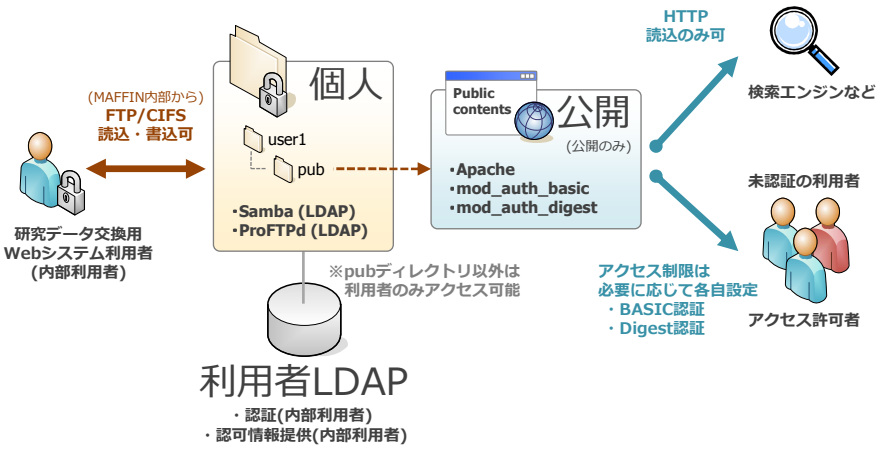
情報共有サービスの改善(1)

個人向け情報共有サービス

MAFFIN
Anytime anywhere,
Collaborative Research Environment

- **研究データ交換用Webシステム**
  - 概要
    - 個人用ネットワークストレージと連携したWebスペースの提供
  - 利用ケース
    - 研究者プロフィール・業績などのWeb公開
    - メールでは送信できない大容量データの引き渡し
  - 詳細
    - ファイルのアップロードは、FTPおよびWindowsファイル共有経由で、MAFFIN内部からのみ可能
    - 容量上限10GB
    - 個人用フォルダ内の公開用フォルダが自動的にWeb公開される
      - http://cse.*所属組織サブドメイン*.affrc.go.jp/*アカウント名*/
    - CGI スクリプトなどの設置・実行は不可能
    - アクセス制限は自前でBASIC認証などを設定する必要あり
      - WebSSOとは連携していない(Cookie盗聴防止のため)

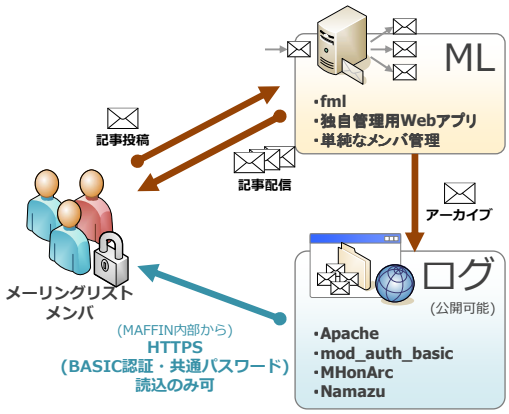
現行: 研究データ交換用Webシステム



グループ向け情報共有サービス

- **メーリングリストシステム**
  - 概要
    - 多人数による電子メールを介した共同作業を円滑に進めるための メーリングリスト機能の提供
  - 利用ケース
    - 研究・業務グループ内での情報共有
    - 学会・シンポジウムの事務局連絡先
    - メールマガジン発行
  - 詳細
    - メーリングリストマネージャはfml
    - 独自作成の管理用Webインタフェース
    - 過去記事Webアーカイブ
      - アクセス制限は、共通アカウントと共通パスワードによるBASIC認証(パスワード設定はWebインタフェースから行える)
      - ただし、MAFFIN外部からのアクセスは不可能

現行: メーリングリストシステム



問題点1: アクセス制限

- **アクセス制限の設定が難しい**
  - htpasswdコマンド、htdigestコマンドを使えない利用者が多い
  - そもそも.htaccessという名前のファイルを作れない利用者も多い
- **簡単なパスワードを設定しがち**
  - 設定したユーザ名・パスワードをメールなどで相手に伝える必要があるため、「わかりやすいパスワード」を設定してしまう
  - 相手から見ると、自分自身で設定したパスワードではないため、パスワードを覚えにくい
- **多人数でファイルを供覧する場合でも、一対のユーザ名・パスワードで済ませがち**
  - 全員にパスワードを割り当てて全員に連絡するのは面倒すぎる
  - 相手から見ると、「全員知っているパスワード」であるため、パスワードの機密意識が低くなる

問題点2: ファイルのアップロード

- **外部からファイルをアップロードできない**
  - システム構成上、アップロードできるのは内部利用者だけ
    - 研究データ「交換用」Webシステムなのに、実は「交換」できない
    - アップロード不能とした理由
      - 適切なアクセス制限が困難である
      - 「誰々がアップロードした」というログを残せない
      - CGIを許可するとセキュリティ管理が困難
- **ファイルをアップロードできないのは外部だけではない**
  - 内部利用者間のファイルの交換でも、お互いのファイルスペースに直接アップロードすることはできない

問題点3: 情報公開管理

- **公開してはいけない情報をうっかり公開してしまう**
  - 研究データ交換用Webサービスの公開用フォルダ
    - システム構成の問題
      - 個人のフォルダの中に公開用フォルダを配置する現行の構成
      - 機密性の高いファイルをうっかり置いてしまう可能性
    - 利用者の意識の問題
      - 「誰もアクセスしないだろう」という思い込み
      - アクセス制限を掛けずに著作権を侵害するようなコンテンツを公開領域に置いてしまう可能性
- **公開したい情報を公開できない**
  - メーリングリストの過去記事アーカイブ
    - システム側でアクセスを「MAFFIN内からのみ」にIPアドレスで制限
    - インターネットの検索にも引っ掛からない
    - 貴重な農林水産研究情報が埋もれてしまう

MAFFIN
Anytime anywhere,
Collaborative Research Environment

次期システムのコンセプト

情報共有サービスの改善(2)

次期情報共有サービスのコンセプト

MAFFIN
Anytime anywhere,
Collaborative Research Environment

- **コンセプト**
  - 「認証・アクセス制限・管理の強化」を行い、より柔軟なサービスを
- **具体的には:**

本日の発表の中心です

  - 認証範囲を広げる
    - 外部組織の利用者でも認証可能な、懐の深い認証システムを提供
    - 各自が常に「自分のアカウントとパスワード」で認証できる環境づくり
      - 多人数へのアクセス許可時でも共通パスワードは不要とする
  - アクセス制限(認可)設定インタフェースを使いやすくする
    - 簡単にアクセス制限を設定できるようWebインタフェースを整備
    - 利用者／利用者グループを基本としたアクセス制限を徹底する
      - 権限さえあれば、誰でもファイルをアップロードできるように
  - 情報公開管理機能を導入する
    - 公開したい情報をきちんと公開できるように
    - 意図しない公開はある程度抑止できるように

認証可能な利用者の範囲拡大

MAFFIN Anytime anywhere, Collaborative Research Environment

ほぼ誰でも認証対象にできる下地を作る

- メールアドレスをIDとする「外部登録利用者」区分を新設する


信頼はできないが、認証はできるように

	内部利用者	外部登録利用者
利用者となる資格	必要(かなり限定)	不要
ID	英数字3~31文字	メールアドレス
利用者情報	正確な情報(公文書申請)	偽名も可能(本人独自申請)
管理DBの構造	複雑	単純

IDとしてメールアドレスを採用することについて

- ○ 電子メールは広く普及しており、誰でも登録できる
- ○ 利用者が自分のIDを覚えやすい
  - 独自の外部登録利用者IDを割り当てても、たいてい忘れられる
- × IDに特殊記号が入るため、IDとして利用できないアプリもある
  - ただし、最近のWebアプリなどでは考慮されていることも多い
  - 特殊文字含有ID→アプリ側でのローカルIDへのマッピングなど

認証サービスの拡大

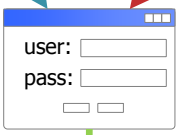
MAFFIN Anytime anywhere, Collaborative Research Environment

内部利用者・外部登録利用者に同じ使い勝手を提供

- 内部利用者・外部登録利用者を区別せず同一のインタフェースでログインできる認証環境を整備する


内部

外部



WebSSO
ログインなど

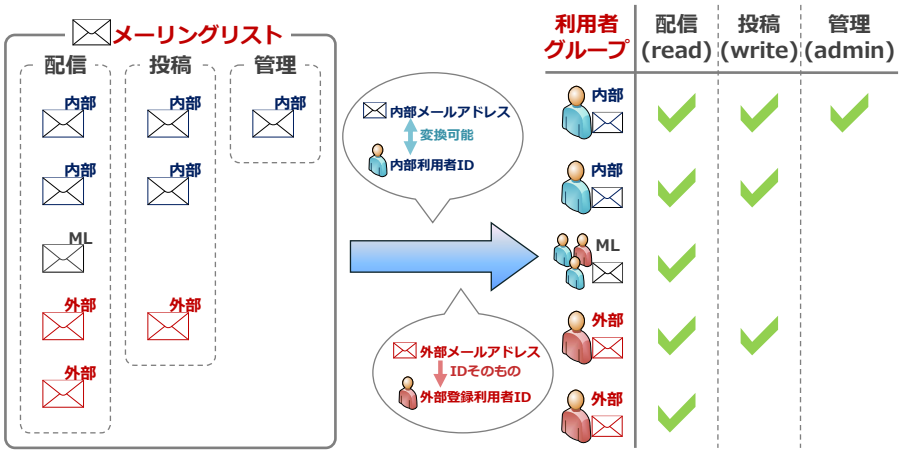
情報共有の相手が少人数なら、「外部登録利用者」区分の追加で認証・認可の問題は解決。

でも、相手が多人数の場合は?

情報共有サービス

利用者グループ概念の導入

- **既存のメーリングリストの捉え方を変える**
  - 「単なるメールアドレスの集合」から
    「認証可能な『利用者』の集合(利用者グループ)」へ



メーリングリストはグループとして優秀

- **基本的な権限が明確**
  - グループの中での各メンバの役割が決まっている
    - 配信対象者(≒いわゆる読込権限を保持)
    - 投稿権限者(≒いわゆる書込権限を保持)
    - 管理者
  - この役割を他の情報共有ツールに当てはめることにより、非常に自然な形で情報共有サービスを拡充できる
- **その他の良いところ**
  - 情報共有したい、という目的で集まったメンバから構成される
    - 単なる組織階層情報から切り出したグループとは趣向が異なる
  - メンバ管理の方法が確立されており、利用者も慣れている
  - 管理者への連絡手段(専用メールアドレス)が用意されている
  - すでに約2,500個のメーリングリストがMAFFINに存在
    - 「農林水産系の研究者グループ」という財産の継承

MAFFIN
Anytime anywhere, Collaborative Research Environment

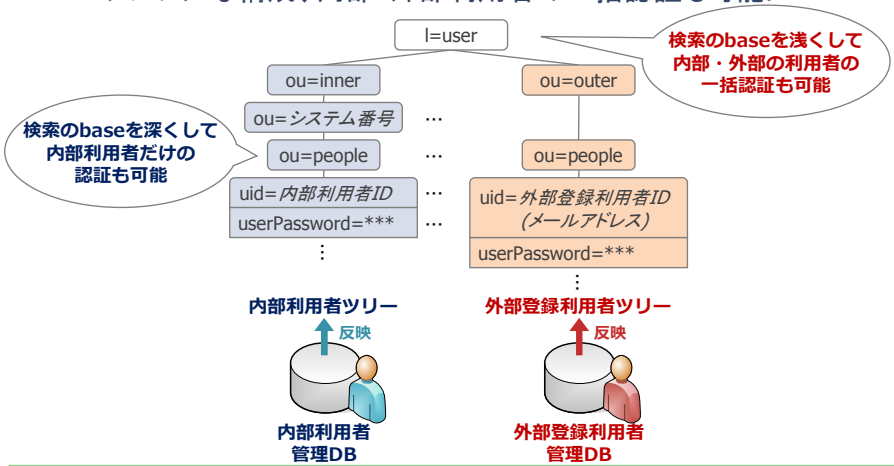
認証基盤の実装

情報共有サービスの改善(3)

利用者LDAP

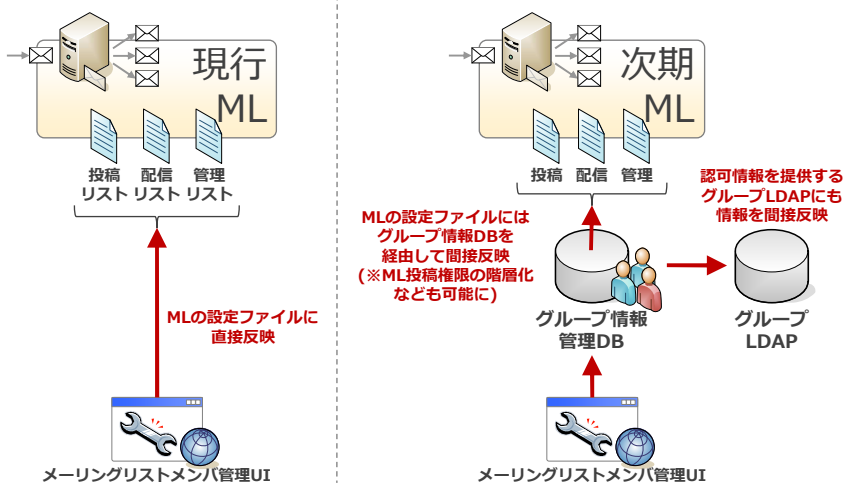
MAFFIN
Anytime anywhere, Collaborative Research Environment

- **情報共有サービスの認証基盤として、利用者 LDAPを構築**
  - LDAPに登録する情報は各DBからの二次情報
  - シンプルな構成、内部・外部利用者の一括認証も可能



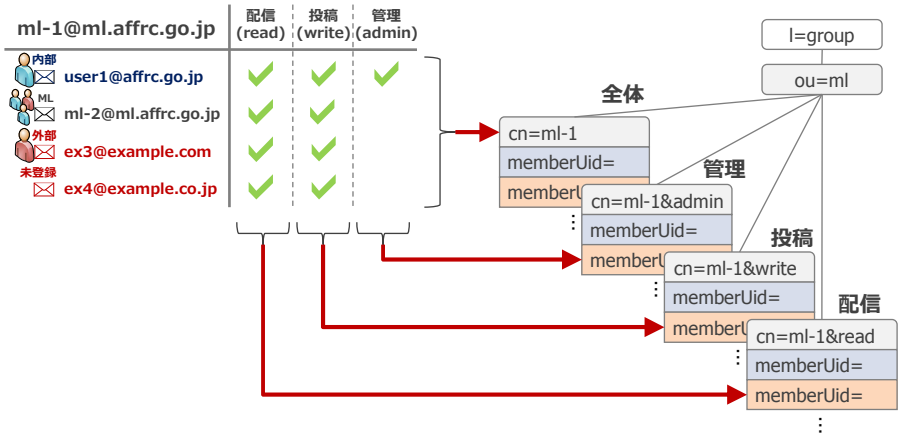
グループ情報管理データベース

- メーリングリストのメンバ情報を管理する
  - メンバ情報を利用した二次情報の作成元となる

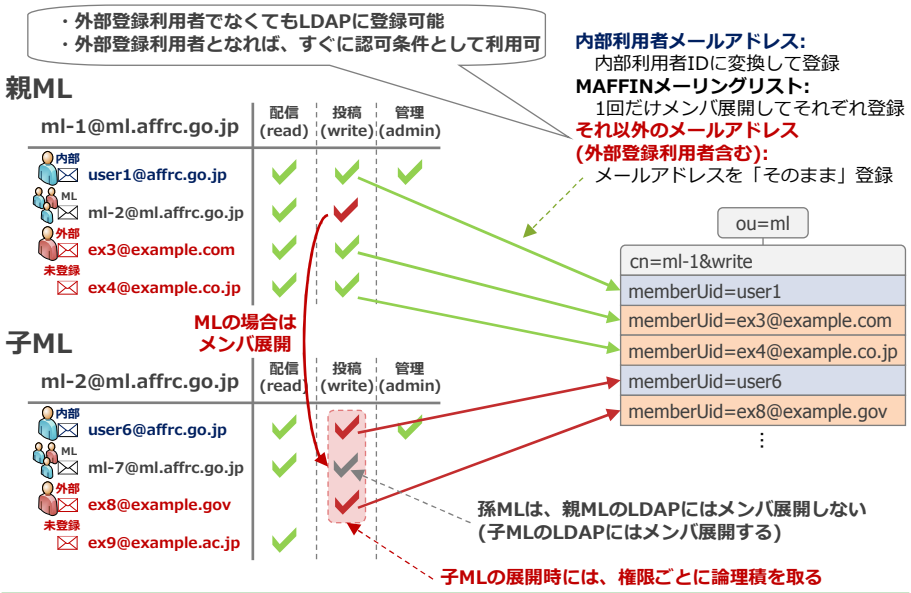


グループLDAP

- 情報共有サービスの認可基盤として、グループLDAPを構築
  - 1つのメーリングリストから4つのグループを生成
    - ML全体グループと、権限ごとのグループ(配信・投稿・管理)



メンバ情報のグループLDAPへの登録



特殊グループ: プリセットグループ

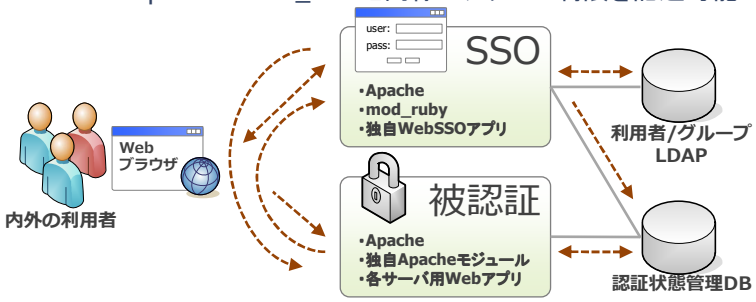
- **ある拠点/組織の利用者に対応するグループを提供**
  - 組織コード・住所コードを元にバッチ処理でグループLDAPに登録
  - 従来の「IPアドレス(拠点サブネット)」によるアクセス制限を代替
    - ネットワーク中心ではなく、利用者中心のアクセス制限を身近に

組織コード		住所コード	
階層1	階層2		
10265 (果樹研)		8 (つくば)	users.naro.fruit.tsukuba
10265		9 (盛岡)	users.naro.fruit.morioka
10265		10 (興津)	users.naro.fruit.okitsu
10265		11 (安芸津)	users.naro.fruit.akitsu
10265		12 (口之津)	users.naro.fruit.kuchinotsu
11402 (農環研)		4 (つくば)	users.niaes
11454 (JIRCAS)		58 (つくば)	users.jircas.tsukuba
11454		59 (沖縄)	users.jircas.okinawa
⋮	⋮	⋮	

users.naro.*** ⋮ users.naro.***
users.naro.fruit
users.naro
users.jircas

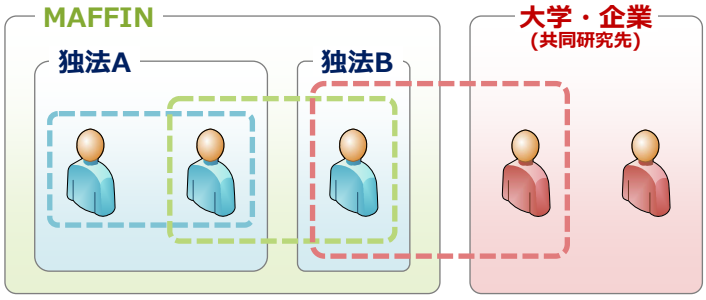
WebSSO

- **WebSSO機能も内部・外部の利用者に対応**
  - Cookieドメイン内で有効な独自方式のSSO
  - バックエンドは利用者/グループLDAP
    - 内部・外部の利用者を一括で認証可能
  - 被認証側のWebSSOクライアントはApacheモジュールとして提供
    - 認証・認可機能を含有
      - Apacheのmod_authと同様にアクセス制限を記述可能



ここまでのまとめ

- **この認証・認可基盤で実現できること**
  - 任意の利用者の認証
  - 任意の利用者のグループ化(組織の壁を超えても、何千人でも)
  - 利用者グループ情報の認可条件への利用



- **次は、認証基盤を利用する情報共有ツールの整備について**

MAFFIN
Anytime anywhere, Collaborative Research Environment

認証基盤を活用する アプリケーションの整備

情報共有サービスの改善(4)

追加アプリケーションの選定

MAFFIN
Anytime anywhere, Collaborative Research Environment

- **必要な機能の洗い出し**
  - 外部組織から接続できること
    - 現状ではHTTP上のサービス一択
  - MAFFINの認証基盤と連携できること
    - 可能な限りWebSSO、ダメならLDAPと連携
  - 権限として「アクセス不可」「読込」「書込」を設定できること
    - 「アクセス不可」権限は結構重要(実装していないWiki多し)
  - 権限として「誰でもアクセス可能」を設定できること
    - 「公開」は情報共有の延長線上に位置づけたい
  - アクセス制限設定インタフェースを統一できること
    - アクセス制限設定をPlain textで保存できるアプリだと都合がよい
- 
- **DokuWikiとWebDAV(Apache+mod_dav)を選定**
  - DokuWikiは「ACL完備」「DBいらず」な優秀アプリ
  - WebDAVは大容量ファイルの交換に対応するため導入

権限とアクセス制限の連動

- **初心者に優しく、上級者に便利に**
  - 初期設定で「安全、かつ十分便利に」使えるように

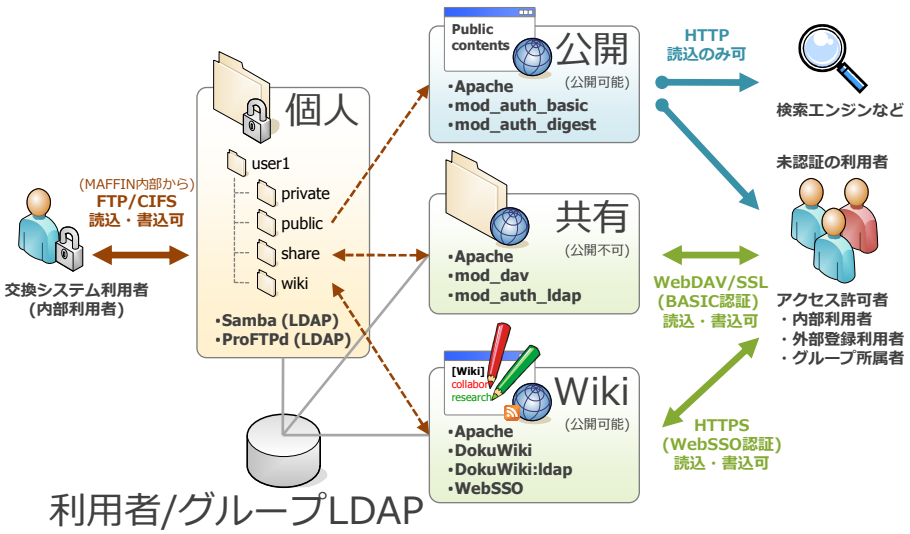
個人用 情報共有サービス
- 個人用Wiki
  - 読込: 本人のみ
  - 書込: 本人のみ
- 個人用共有フォルダ
  - 読込: 本人のみ
  - 書込: 本人のみ

グループ用 情報共有サービス
- ML用Wiki
  - 読込: 投稿グループ・配信グループ
  - 書込: 投稿グループ
- ML用共有フォルダ
  - 読込: 投稿グループ・配信グループ
  - 書込: 投稿グループ
- ML過去記事アーカイブ(読込のみ)
  - 読込: 投稿グループ・配信グループ

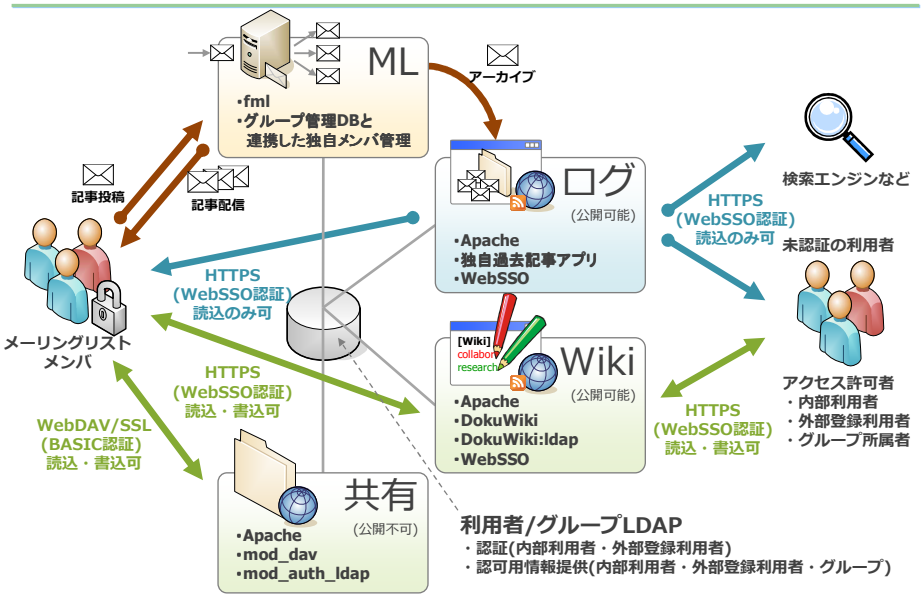
ML管理者グループは いずれのサービスも 無条件で読込・書込可能

  - Webから設定を行えば、どのようなアクセス制限でも可能に
    - 任意の利用者(内部利用者、外部登録利用者)
    - 任意のグループ(ML、プリセットグループ)

次期: 研究データ交換システム



次期: メーリングリストシステム



アクセス制限設定用インタフェース

- **Wiki、共有フォルダ、メーリングリスト過去記事アーカイブで、ほぼ同じ体裁のアクセス制限設定用インタフェースを用意**
  - このインタフェース以外からのアクセス制限設定は行えない

公開申請が承認されると、この「無効」が無くなる

- **組織の管理者による簡易公開制限が可能に**
  - 次期システムでの「公開」は、「不特定多数への閲覧権限付与」(未認証の利用者への閲覧許可)という意味
  - 上記以外は、「公開」ではないものとする
    - 人数の問題ではなく、認証の問題
    - 10,000人規模のグループへの閲覧権限付与は「公開」ではない

MAFFIN
Anytime anywhere, Collaborative Research Environment

今後の課題

認証連携時代に向けて

OpenIDへの対応

MAFFIN
Anytime anywhere, Collaborative Research Environment

- **OpenIDとは**
  - 簡易なWebSSO方式、URIがIDとなる
    - 世界的にIdP数が増加している
- **対応**
  - WebSSO機能にOpenIDのService Provider機能を組み込む
    - WebSSOに対応する全てのシステムがOpenID対応となる
- **実現できること**
  - MAFFINの情報共有サービス上でOpenIDをそのままIDとして利用するのは少し困難
  - パスワードをMAFFIN側に預けなくても良くなる効果はある
    - 外部登録利用者のパスワード管理の補助程度の効果
    - メールアドレスはOpenIDの属性情報から取得できるが、基本的に信頼できないため、メールアドレスの実在確認を行う必要がある
    - MAFFIN側ではOpenIDとメールアドレスの対応情報を保存

Shibboleth への対応

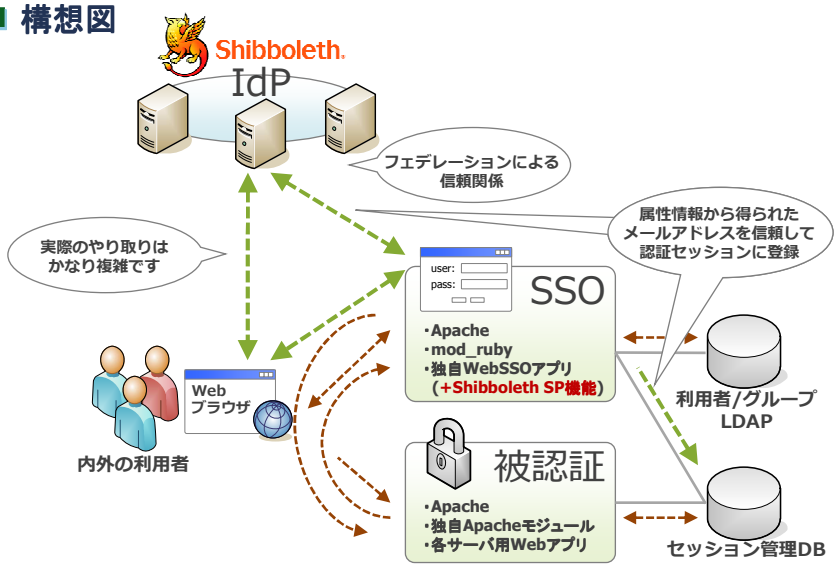
- **Shibbolethとは**
  - 組織間のID連携(フェデレーション)の一手段、SAMLベース
  - 欧米の学術機関で実績あり、日本ではUPKI Initiativeで実験中
- **対応**
  - WebSSO機能にShibbolethのService Provider機能を組み込む
- **実現できること**
  - 属性情報として取得できるメールアドレス情報を信頼すると……
    - 得られたメールアドレスをMAFFIN認証のIDに設定することで、外部登録利用者と同様に取り扱える
    - ➔利用者登録作業が不要に

かなりイレギュラーな使い方ですが……

  - もし学術系のフェデレーションに参加できれば……
    - この情報共有サービスのメインターゲットである学術系の利用者と、より手軽に情報共有を行うことが可能に
    - 組織間のID連携が実現した場合でも小回りの効くグループは有用

Shibboleth への対応

- **構想図**



MAFFIN
Anytime anywhere,
Collaborative Research Environment

まとめ

まとめ

MAFFIN
Anytime anywhere,
Collaborative Research Environment

- **利用者の所属組織の内部・外部を問わない、非常に柔軟な情報共有サービスを構築した(2009.3稼働予定)**
  - メールアドレスをIDとする「外部登録利用者」という区分を設け、ほぼ誰でも認証できる環境を整備した
  - 既存のメーリングリスト資産を活用することにより、内部組織・外部組織の利用者を含む農林水産系の研究者グループをLDAP上に表現することができた(認証・認可バックエンドの構築)
  - メーリングリストメンバの権限情報を活用することにより、自然な形でグループ向けの情報共有サービスを拡充できた
  - 今後は認証連携への対応を検討している
- **農林水産系の研究情報交換が活発になることを祈念します**