InternetWeek 2004 チュートリアル

WebDAV

～そのプロトコルと実装／実用面からのアプローチ～

2004年12月2日

WebDAV Resources JP
宮本 久仁男(Kunio Miyamoto)
wakatono@todo.gr.jp

Agenda

- WebDAV概論
- DAVと類似のプロトコルリモートファイル操作
- WebDAVの実装
- WebDAVをどう使う？～実用への提案～
- いいことばかりじゃありません ～WebDAVの問題点
- WebDAVセキュリティの基本
- WebDAVの利用を制限するには
- まとめ

WebDAV概論

•WebDAVのはじまり
•WebDAVの背景〜RFC2291〜
•WebDAVの基本仕様〜RFC2518〜
•バージョニング拡張〜DeltaV / RFC3253〜
•最近RFC化された拡張〜RFC3648
•その他の拡張〜DASL, BIND, ACL〜

3

WebDAVって何？

- WebDAVとは…
  - Web経由でアクセス可能なリソースを操作するための規格
  - 拡張でバージョン管理とかについても規定
  - 多分、**一般ユーザはこんなの知らなくても使えます**
- WebDAVを知らなきゃいけないのは…
  - サーバ／クライアントその他関係するものの開発者
  - サーバ管理者
  - トラブル対応者

4

WebDAVのはじまり(1/2)

- WebDAVという言葉が最初に出てきたのは？
  - 知る限りはRFC2291の文中で初出
    Requirements for a Distributed Authoring and Versioning Protocol for the World Wide Web
  - ほんとに概念（というか理念）だけ
  - プロトコルはRFC2518が基本
    - HTTP Extensions for Distributed Authoring -- WEBDAV
    - リソース（後述）を操作する。
    - ファイル操作（open/read/write/mkdir/unlink/stat/lock）相当のものが規定される

WebDAVのはじまり(2/2)

- 拡張仕様も順次規定
  - バージョン管理:RFC3253
    Versioning Extensions to WebDAV
  - コレクション（後述）内のファイルの並び替え:RFC3648
    Web Distributed Authoring and Versioning (WebDAV) Ordered Collections Protocol
  - アクセスコントロール：RFC3744
    Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol
  - 検索（DASL）、名前空間のバインド（シンボリックリンクみたいなもの／BIND）についてはInternet Draftで規定（順次RFC化されるものと思われる）。

WebDAVってどんなもの？

- WebDAVは特定のソフトウェア／実装をさすものではなく、プロトコルである
- プロトコルとしては、HTTP1.1を拡張
  - 但し、RFC3253については「バージョン管理の方式」を一般化した文書として読むことも可能

WebDAVの背景～RFC2291～(1/2)

- 以下のものについて定義（まずは必要なものの定義から）
  - 部分書き込み(Partial Write),リンク(Links)
    - 従来のHTTPおよびHTMLの仕様でカバー
  - コレクション(Collections),リソースの多様性(Variants), プロパティ(Properties) ,ロック(Locking),名前空間操作(Name Space Manipulation),セキュリティ(Security)
    - RFC2518ではじめて定義
  - バージョン管理(Versioning)
    - RFC3253ではじめて定義

WebDAVの背景～RFC2291～(2/2)

- 予約(Reservations)
  - プロパティおよびプロパティ検索／編集につながってくる
- 未処理のソースの検索(Retrieval of Unprocessed Source)
  - DASLにつながってくる
- 国際化(Internationalization)
  - 今もって問題になっている…

WebDAVの基本仕様 ~RFC2518(1/8)

- RFC2518で規定している範囲
  - 扱うものと状態（4つの概念）
  - 扱う方法と扱った結果（メソッドとステータスコード）
    - リクエストヘッダやエンティティについても定義
      - XMLエレメントなど、エンティティで使うものも定義
  - セキュリティ上の留意事項
    - 認証方法などについても言及
      - 例：暗号化なしの環境でベーシック認証は推奨しない

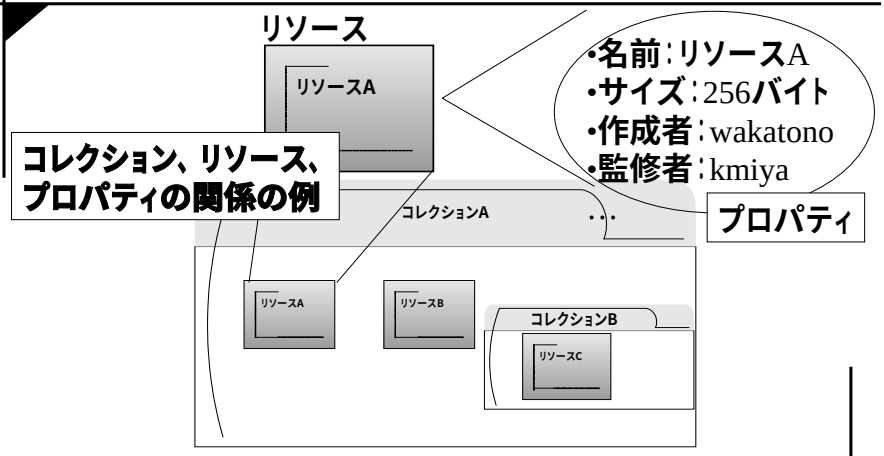
WebDAVの基本仕様~RFC2518(2/8)

- リソース(Resource)
  - WebDAVでの操作対象となるもの。
  - ファイルシステムにおける「ファイル」にあたるもの
  - PUTで作成し、DELETEで削除
  - COPYで複製を、MOVEで移動を行う
- コレクション(Collection)
  - ファイルシステムにおける「ディレクトリ」にあたるもの
  - 複数のリソース情報を含むリソース
  - MKCOLで作成、DELETEで削除
  - COPYで複製を、MOVEで移動を行う
    - 所属するメンバも同様に操作される

WebDAVの基本仕様~RFC2518(3/8)

- プロパティ(Property)
  - リソースやコレクションの情報（メタデータ）
    - 例：作者、編集者、作成／更新日時
  - ライブプロパティ（システムで付与するもの）と デッドプロパティ（ユーザが付与するもの）の2種類
  - PROPFINDで取得、PROPPATCHで変更
    - ライブプロパティはPROPPATCHで変更不可
- ロック(Lock)
  - 概念というよりは、状態というのが正しい
  - LOCKでロック、UNLOCKでロック解除

WebDAVの基本仕様 ~RFC2518(4/8)



WebDAVの基本仕様 ~RFC2518(5/8)

- WebDAVで規定されたメソッド(RFC2518の範囲)

メソッド	機能
PROPFIND	プロパティの取得
PROPPATCH	プロパティの変更
MKCOL	コレクションの作成
COPY	コレクションを含むリソースおよびプロパティの複製
MOVE	コレクションを含むリソースの移動
LOCK	コレクションを含むリソースのロック
UNLOCK	コレクションを含むリソースのロック解除
OPTIONS	既存のメソッドとかわらない
GET	既存のメソッドとかわらない
HEAD	既存のメソッドとかわらない
POST	既存のメソッドとかわらない
PUT	リソースの作成
DELETE	リソースの削除
	コレクションおよびそのコレクションに含まれるリソースの削除

WebDAVの基本仕様 ~RFC2518(6/8)

- WebDAVで規定・拡張されたステータスコード(RFC2518の範囲)

表2 新設／拡張されたステータスコード

値	ステータス	意味	新設／拡張
102	Processing	リクエストは受け付けたが、まだ処理が終わっていない	
207	Multi-Status	複数のステータスを持つ	
422	Unprocessible Entity	リクエストの書式は正しいが、その内容が間違っている	新設
423	Locked	リソースはロックされている	
424	Failed Dependency	とあるリクエストに関連したリクエストが失敗したため、リクエストの依存関係が保てない	
507	Insufficient Storage	記憶領域が不足している	
200	OK	PROPPATCH が成功した（PROPPATCH）	
201	Created	リソース／コレクションが作成された（MKCOL, PUT）	
		コピーが成功した（コピー先は新規作成）（COPY）	
		移動が成功した（移動先のリソース等は新規作成）（MOVE）	
204	No Content	リソース／コレクションの削除が成功した(DELETE)	
		コピーが成功した（コピー先は既存のリソース）（COPY）	
		移動が成功した（移動先のリソース等は既存）（MOVE）	
		ロック解除された（UNLOCK）	
400	Bad Request	ロック解除の時に指定したロックトークンが不正なものだった(UNLOCK)	
403	Forbidden	サーバ側の設定で、コレクション作成を許していない。(MKCOL)	
		認証設定などで、許可されていないURLの下にコレクションを作成しようとした(MKCOL)	拡張
		コピー元とコピー先は同一。(COPY)	
		何らかの理由でプロパティを変更できなかった(PROPPATCH)	
		移動元と移動先が同じである。(MOVE)	
404	Not Found	プロパティが見つからない(PROPFIND)	
405	Method Not Allowed	すでに存在する名前のコレクションを作ろうとした。(MKCOL)	
409	Conflict	読み取り専用のプロパティなど、変更できないプロパティを変更しようとした（PROPPATCH）	
		存在しないコレクションの下にリソースやコレクションを作ろうとした。(MKCOL, PUT, COPY,MOVE)	
		例：http://localhost/DAV の下にDAV2 というコレクションがない状態で http://localhost/DAV/DAV2/DAV3 を作ろうとした。	
412	Precondition Failed	指定したリソースがロック可能な状態ではないか、サーバが lockinfo XML エレメントの要求を満足できなかった。	
		プロパティの内容を保持できなかった、もしくは Overwrite ヘッダの値が F である。(COPY,MOVE)	
415	Unsupported Media Type	MKCOL のリクエストボディが受け付けられないものだった。(MKCOL)	

WebDAVの基本仕様 ~RFC2518(7/8)

- DAV Compliant Class(1/2)
  - RFC2518ではClass1, Class2について規定
    - Classは独立に規定される
      - 例：Class2は、Class1 + LOCK,UNLOCKだが、後に規定されるClassは別にClass2を含む必要はない
  - RFC3253で、さらに細かい規定
    - もはや細かすぎて追いきれてません…

WebDAVの基本仕様 ~RFC2518(8/8)

- DAV Compliant Class(2/2)

バージョニング拡張 〜DeltaV / RFC3253〜(1/7)

- WebDAVのV (Versioning) に関する拡張
  - DeltaVとも呼ばれる
    - 現在も (当然) 活動中
  - RFC3253にて規定
    - 多くのメソッド規定＆拡張
      - 新しく規定されたメソッドの数はRFC2518より多い(!)
        - » メソッド発行時の条件がより厳密になり、条件を満たす時と満たさない時の挙動もより細かくなった
    - ステータスコードについても同じ

バージョニング拡張
～DeltaV / RFC3253～(2/7)

- 増えたメソッド
  - VERSION-CONTROL
  - REPORT
  - CHECKOUT,CHECKIN,UNCHECKOUT
  - MKWORKSPACE
  - UPDATE
  - LABEL
  - MERGE
  - BASELINE-CONTROL
  - MKACTIVITY
- 拡張されたメソッド
  - 過去に規定されたメソッドのほぼすべてが影響を受ける
  - さらに、LOCKをサポートするかしないかで、RFC3253を実装する上での複雑さも増す

バージョニング拡張
～DeltaV / RFC3253～(3/7)

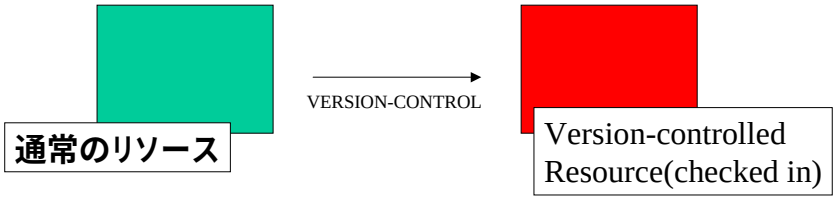
- RFC3253の中で複数のバージョン管理方式について規定
  - Basic, Advanced, Server Side, Client Sideに関するおおざっぱな分類
  - RFC3253準拠のバージョン管理は、その中に書かれてるすべてを満足する必要はない。
    - Subversionは現にサブセットだが、分類としてはAdvanced Client Workspace（後述）のようになる（と思う…）

バージョニング拡張
～DeltaV / RFC3253～(4/7)

- **バージョニングに関するおおまかな分類**
- Basic Versioning Features
  - Core-Versioning, Basic-Server-Workspace, Basic-Client-Workspace
- Advanced Versioning Features
  - **上記**Basic-* **に、以下の機能が追加される**
    - **コレクションバージョニング**
    - **構成のバージョニング**
    - **ベースラインリソースのサポート**
    - **アクティビティのサポート**

バージョニング拡張
～DeltaV / RFC3253～(5/7)

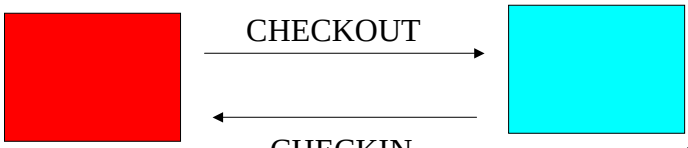
ものすごく単純なバージョン管理(1/2)



- VERSION-CONTROL**メソッドにより、リソースがバージョン管理されている状態に変化（一方通行）**
- **実際には、当該リソースの状態が変わるだけでなく、ヒストリリソースが作られたりと付随する処理は多くある**
- **最初からバージョン管理可能なリソースを扱うことを前提にしている**
  Subversion**では、**VERSION-CONTROL**メソッドは実装されていない**

バージョニング拡張
～DeltaV / RFC3253～(6/7)

ものすごく単純なバージョン管理(2/2)



Version-controlled Resource(checked in)

Version-controlled Resource(checked out)

- チェックアウトされたリソースが編集／変更可能
- チェックアウト先は実装に依存
  - サーバサイド（サーバサイドワークスペース）
  - クライアントサイド（ワーキングコピー）
    - 実際には、サーバサイドにもワークスペースは作成される
- 実際には、チェックイン時にヒストリリソースの量が増えたりする

バージョニング拡張
～DeltaV / RFC3253～(7/7)

- バージョニングをサポートしないクライアントのための仕様もこの中に含む
  - オートバージョニング(Auto Versioning)
    - 通常、チェックアウトやチェックインその他の処理を明示的に発行することで可能なバージョン管理操作を、PUTなどの操作が発行されるとそれにともなった一連の処理を実施する
  - 細かいバージョン管理は厳しい
    - 例：REPORTメソッドの結果（ログ）が閲覧できない
    - 記録形式によっては容量が…

Ordered Collection ～RFC3648～(1/2)

- RFC3648
  - Web Distributed Authoring and Versioning (WebDAV) Ordered Collections Protocol
    - **要はコレクション内のメンバの並びの制御**
  - **具体的には**ORDERPATCH**メソッドを規定**
  - **コレクション内のメンバの並びを決める。→たとえば**PROPFIND**発行時に、どのような規則でメンバー一覧が返るかに影響**

最近RFC**化された拡張** ～RFC3648～(2/2)

```
>> Request:

ORDERPATCH /coll-1/ HTTP/1.1
Host: example.org
Content-Type: text/xml; charset="utf-8"
Content-Length: xxx

<?xml version="1.0" ?>
<d:orderpatch xmlns:d="DAV:">
  <d:ordering-type>
    <d:href>http://example.org/inorder.ord</d:href>
  </d:ordering-type>
  <d:order-member>
    <d:segment>two.html</d:segment>
    <d:position><d:first/></d:position>
  </d:order-member>
  <d:order-member>
    <d:segment>one.html</d:segment>
    <d:position><d:first/></d:position>
  </d:order-member>
  <d:order-member>
    <d:segment>three.html</d:segment>
    <d:position><d:last/></d:position>
  </d:order-member>
  <d:order-member>
    <d:segment>four.html</d:segment>
    <d:position><d:last/></d:position>
  </d:order-member>
</d:orderpatch>
>> Response:

HTTP/1.1 200 OK
```

- **前提は、**three.html, four.html, one.html, two.html**という**4**つのリソースがこの順番で並んでいる。**
- two.html **をまず** first (**先頭**) **に配置**
- One.html **を次に** first (**先頭**) **に配置**
  →one.html, two.html **という順序に**
- Three.html **を**last (**最後**) **に配置**
  →one.html, two.html, three.html**という順序に**
- Four.html**を**last (**最後**) **に配置**
  →one.html, two.html, three.html, four.html **という順序に**

ACL〜RFC3744

- 2004年5月にRFCとなる
- 以下のようなものを定義
  - 制御する権限
  - アクセス制御のためのプロパティ
  - Access Control List(ACL)評価方法
  - 既存のメソッドに対する拡張
  - ACLメソッドの定義
  - その他必要と思われる事項
    - 書式とかサンプルとかその他もりだくさん

ACLリクエストの例

```
ACL /top/container/ HTTP/1.1
Host: www.example.com
Content-Type: text/xml; charset="utf-8"
Content-Length: xxxx
Authorization: Digest username="fielding",realm="users@example.com", nonce="...",
          uri="/top/container/", response="...", opaque="..."

<?xml version="1.0" encoding="utf-8" ?>
  <D:acl xmlns:D="DAV:">
    <D:ace>
      <D:principal>
        <D:href>http://www.example.com/users/esedlar</D:href>
      </D:principal>
      <D:grant>
        <D:privilege><D:read/></D:privilege>
        <D:privilege><D:write/></D:privilege>
      </D:grant>
    </D:ace>
    <D:ace>
      <D:principal>
        <D:property><D:owner/></D:property>
      </D:principal>
      <D:grant>
        <D:privilege><D:read-acl/></D:privilege>
        <D:privilege><D:write-acl/></D:privilege>
      </D:grant>
    </D:ace>
    <D:ace>
      <D:principal><D:all/></D:principal>
      <D:grant>
        <D:privilege><D:read/></D:privilege>
      </D:grant>
    </D:ace>
  </D:acl>
```

esedlar

オーナ

全員

- <D:ace>〜</D:ace>で囲まれた部分がアクセス制御の定義のブロックにあたる
  - 今回の例では3つ
- <D:principal>〜</D:principal>で囲まれた部分が「誰に対して権限を与えるか」の定義
- <D:grant>〜</D:grant>で囲まれた部分で「どんな権限を与えるか」の定義
- 今回は以下のような権限を与えている
  - http://www.example.com/users/esedlarで特定可能なユーザに読み書きの権限を
  - オーナにはACLの読み書きの権限を
  - 誰もが読み出しをできる権限を

その他現在規定されつつあるもの

- DASL(DAV Search and Locating)
  - リソース検索のための規定
  - SEARCHメソッドの規定
- BIND
  - 名前空間のバインディング（対応付け）のための規定
  - BINDメソッドの規定

独自のWebDAVプロトコル？(1/2)

- Exchangeでサポートされるメソッドがある
  - BCOPY, BMOVE, BPROPPATCH,BPROPFIND,BDELETE
  - Bは“Batch”（バッチ）の略
  - 複数のリソースに対するリクエストを一括で処理する
    - リクエストボディに（XML形式で）処理内容を記述する

独自のWebDAVプロトコル？(2/2)

- MicrosoftはBで始まるメソッドの標準化を提案
  - でも却下
- その後、BATCHメソッドについての議論がにわかに盛り上がる
  - その後しぼんだけど…
- 基本的にはMicrosoft Exchange Serverでのみサポートするが、Proxyソフトウェアでもサポートしているものがある
  - 筆者はSquidのソースコードを読んでて知りました
    - squid-2.5.STABLE3/src/enum.hに、
      METHOD_COPY,METHOD_GETなどと並んで
      METHOD_BCOPY, METHOD_BMOVE,etc... などが…

DAVと類似のプロトコル(?)

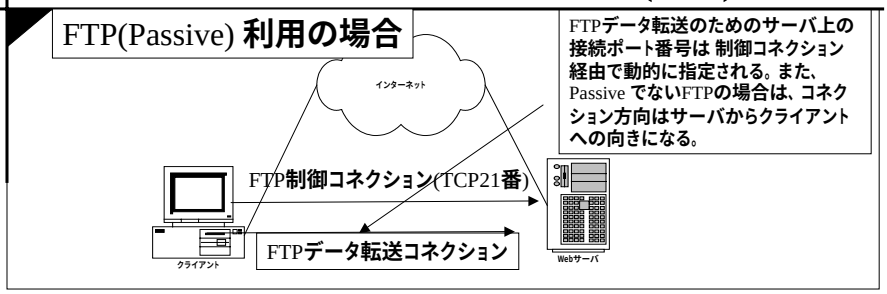
ファイル操作とかオーサリングとか

DAVと類似のプロトコル ～リモートファイル操作(1/6)

- 機能が似てる？リモートファイル操作
  - WebDAV以前～FTPとか(Web)NFSとか
  - FTPとの比較は取りざたされる
  - NFSとの比較もやっぱり取りざたされる
  - WebNFSとは「同じに見られた」(泣)

- じゃ、実際はどうなんだろう？

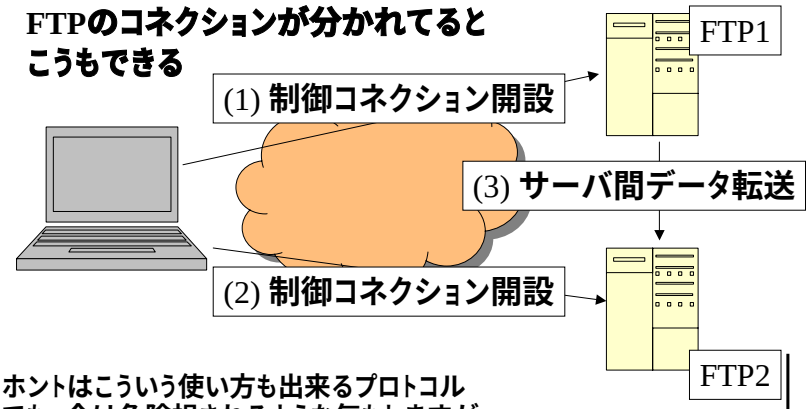
DAVと類似のプロトコル ～リモートファイル操作(2/6)



- FTPデータ転送のためのサーバ上の接続ポート番号は 制御コネクション経由で動的に指定される。
- Passive でないFTPの場合は、コネクション方向はサーバからクライアントへの向きになる。

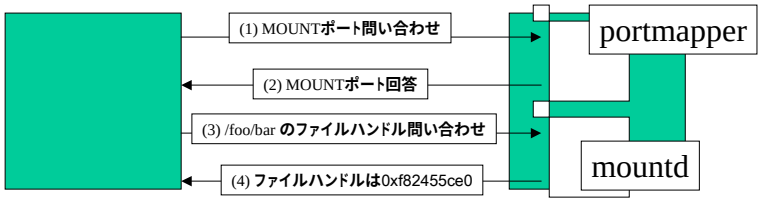
DAVと類似のプロトコル ～リモートファイル操作(3/6)

FTPのコネクションが分かれてるとこうもできる



- ホントはこういう使い方も出来るプロトコル
- でも、今は危険視されるような気もしますが…

DAVと類似のプロトコル ～リモートファイル操作(4/6)

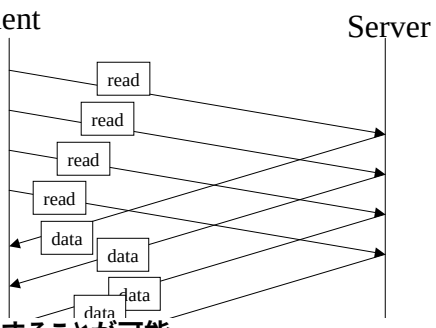


NFS Client　　NFS Server

- portmapperとmountdの2つのプロセスが介在
- NFSv3ではmountプロトコルは必要なし

DAVと類似のプロトコル ～リモートファイル操作(5/6)

NFSにおけるread



- Readを複数同時に発行することが可能
- ブロック単位のI/Oであり、途中からの再開が可能
- 基本的には、TCP/2049もしくはUDPによるデータ転送

DAVと類似のプロトコル ～リモートファイル操作(6/6)

- DAVとの比較をまとめると…
- FTP
  - よくつかわれて、枯れてはいるが…
    デザインが若干（？）古い
  - コネクションの消費もさることながら、（絞れるとはいえ）複数のポートを確実に使う
    - サーバ（＆サーバを収容するネットワーク）の管理が面倒
- NFS
  - LAN向きだがWANには不向き
  - 商用UNIXでもWANでのNFS使用を保証していなかった時期が
    - 今は知らない…
- WebNFSは？
  - 単にNFSクライアントがWebブラウザ（HotJava）というだけ

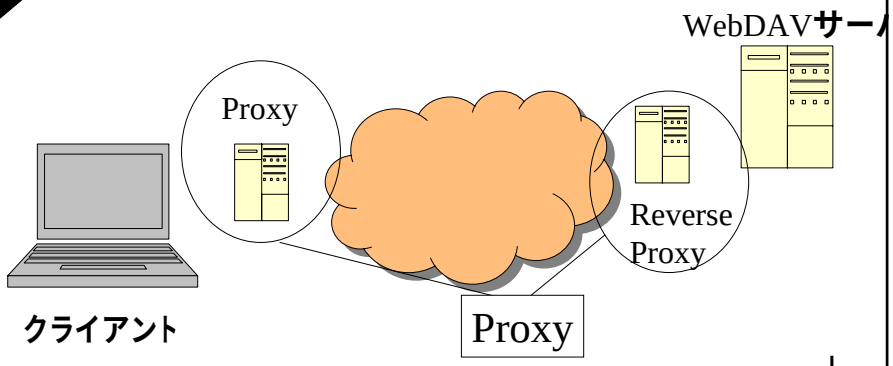
DAVと類似のプロトコル ～オーサリング

- WikiとBlogとWebDAVと～どう違う？
  - 語感が似てる？
- Wikiは思想・概念から実装に展開されている。
  - 利用者に「見える」ページオーサリングのコラボレーションという点からアプローチを行なう
  - Wikiに関する標準化も最近走りはじめたとかなんとか
    - http://lab.lolipop.jp/fswiki/wiki.cgi/wikistandard
- Blogは「結果的に」そう呼ばれてるように見える
  - http://kotonoha.main.jp/weblog/000125_google.html
- DAVは概念を実現するために仕様化、そして実装に展開されている
  - コラボレーションというのは意識されてはいるが、その結果出来上がる内容（PUT等で扱われるエンティティの解釈）についてはその仕様の中で取り扱わない
- …上記はあくまで私見です（汗）
  - 何がいいとか悪いとかいう話ではありません（！）

WebDAVの実装

サーバとクライアントとProxy

DAVに関連する コンポーネント種別（？）



- サーバ、クライアント、Proxyの3種類が存在
  - Proxyは通常のHTTP Proxyとは区別されない

WebDAVの実装（サーバ編）

- いろいろ出て来てます。
- 定番はApache,IISあたりでしょうか？
  - 伏兵でSubversion. Catacombあたりも

WebDAVのサーバ実装(1/2)

- フリーソフトウェア・オープンソースソフトウェアな実装
  - Apache 1.3 + mod_dav 1.0.3
  - Apache 2.0 (mod_dav を含む)
  - Subversion
  - Catacomb
  - Apache Tomcat
  - Zope
- 他にもいろいろ…

WebDAVのサーバ実装(2/2)

- 商用製品での実装
  - Microsoft IIS5.0以降
  - Xythos WebFile Server
  - Microsoft Exchange Server 2000 以降
    - BCOPY,BMOVE, BPROPPATCHなど、独自のメソッドも実装

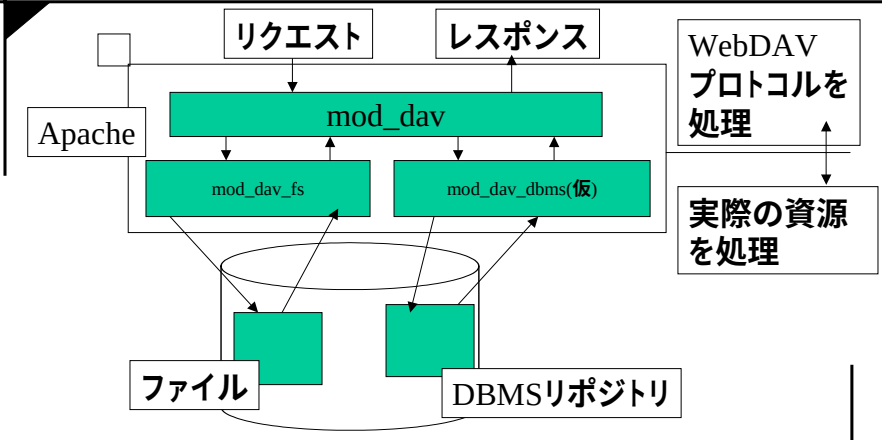
Apache 1.3 + mod_dav 1.0.3

- もっとも安定しているWebDAV実装の1つ
- mod_davの作者はGreg Stein
  - 現在のApache Foundation の Chair
- DAV Compliant Class 1,2 をサポート
- この組み合わせでRFC2518をサポート
  - 拡張仕様も考えてはいた痕跡
    - DAVParamパラメータの設定で拡張モジュール（別途用意）の設定を実施する構造
      - Oracle 9i IFS はこれでパラメータ設定
  - すでにメンテナンスベース
  - 新しいプロトコルサポートは行われない「はず」

Apache2(1/2)

- 配布物にmod_davを含む
  - mod_davとmod_dav_fsの2つに分離
  - mod_davはプロトコル処理を担当
  - mod_dav_fsはリポジトリへの物理アクセスを担当
- DAV Compliant Class1,2をサポート
- RFC2518をサポート

Apache2(2/2)



Apache2.1

- mod_davが持っている機能をさらに細分化
  - mod_davとmod_dav_lockに分解
  - Lock処理の外出し
- Subversionのリポジトリもロックが可能に
  - 実際ロックに関する前処理と後処理がどこまでできてるかはチェックできてませんが…

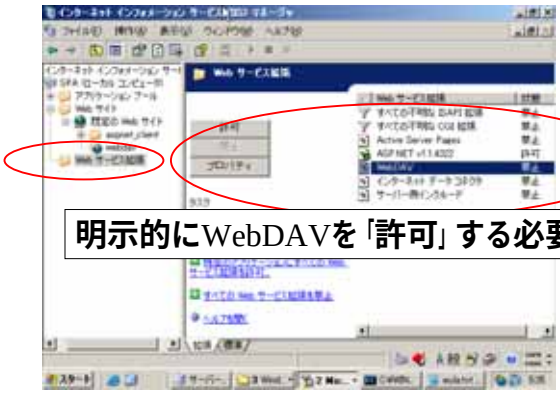
Microsoft IIS5.0〜(2/2)

- Windows 2000,Windows XP, Windows Server 2003 **にて使用可能**
  - IIS5.0(Windows 2000), IIS5.1(Windows XP), IIS6.0(Windows Server 2003)
- WebDAV**サーバとしても使用可能**
- **認証ユーザでの権限で**WebDAV**アクセスが可能**
  - Apache**だと、認証ユーザとファイルシステムへのアクセス権限は独立**
- NTFS**の機能である**ACL**を設定することでアクセス制御が可能**

Microsoft IIS5.0〜(1/2)

- IIS5.1**までと**IIS6.0**の管理**UI**が変わった**
  - IIS5.1**までは、仮想ディレクトリで書き込みやディレクトリ参照を許可すると「**WebDAV**アクセスを許可」していた**
  - IIS6.0**では明示的に「**WebDAV**を許可」しないと機能が有効にならない**

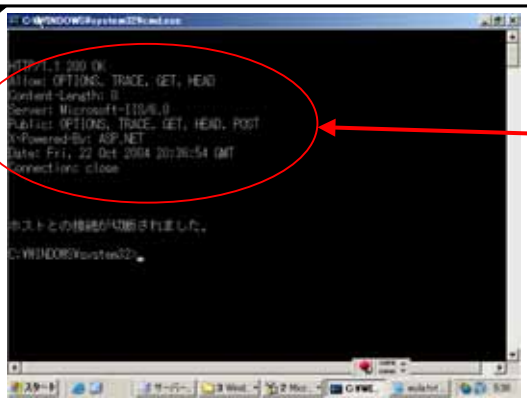
IIS6.0の場合



明示的にWebDAVを「許可」する必要がある

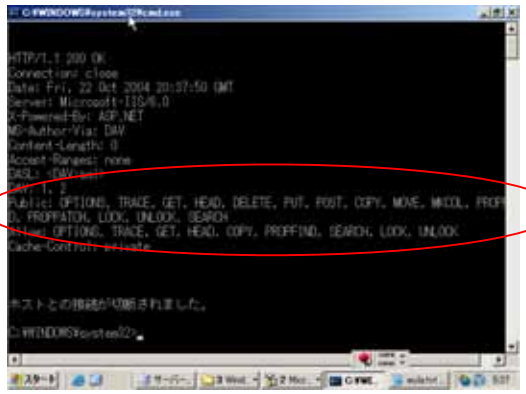
- **ここで許可されない場合、個別の仮想ディレクトリでの設定は無効**

WebDAVを許可しない場合のOPTIONS結果



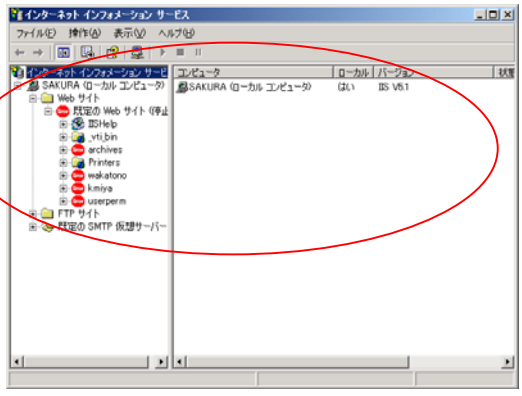
- **参照系のメソッドのみ現れる**
- **その他は陰も形もなし**
- **IISの管理UIでWebDAVを単に許可すると不思議なことが…**

WebDAVを許可した場合のOPTIONS結果



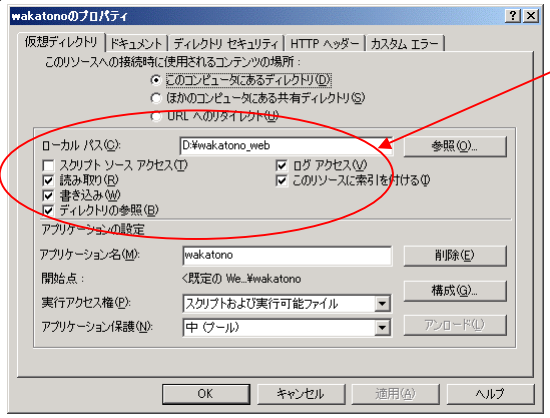
- **単に許可しただけだが使えるメソッドが増えている**
- LOCK,UNLOCK,PROPFINDなどは典型
- PROPFINDはバグのような気がする…

IIS5.1の場合のWebDAV許可？



- **どこにもいない**

IIS5.1までは仮想ディレクトリ設定でWebDAV許可



- 仮想ディレクトリごとに設定するだけ

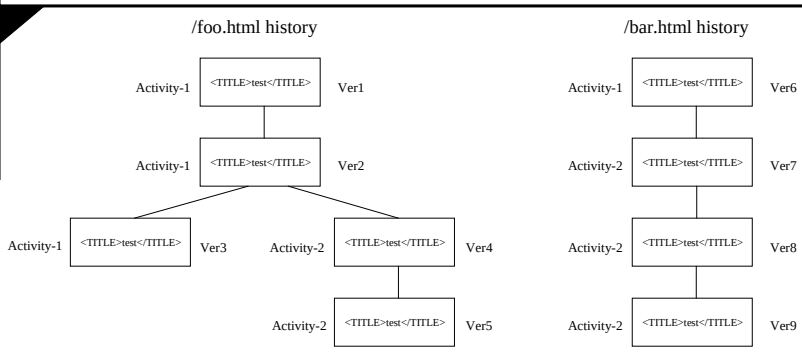
Subversion(1/6) ～概要

- もともとはCVSの後継として開発される
  - svnserveを使うことで、単独で使用可能
- Apache2と組み合わせることで、RFC3253に規定された機能を使うことが可能
  - mod_dav_svnを用いる
  - 拡張アクセス制御はmod_authz_svnを用いる
- RFC2518中、DAV Compliant Classは1
- RFC3253的にはAdvanced Versioning Featureを実装
  - RFC2518の範囲のクライアント実装でも、Auto Versioning を有効にすることでアクセス可能
    - でも効率は悪い

Subversion(2/6)
～バージョン管理の概要

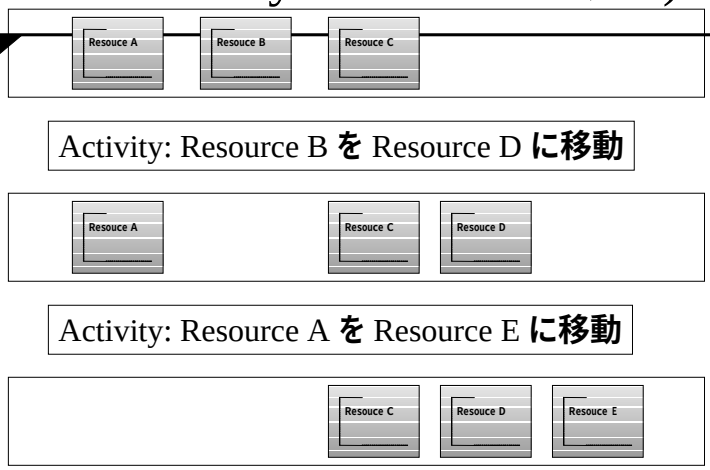
- DeltaVによるバージョン管理を踏襲
  - DeltaVで規定されたバージョン管理の1つを実装している（多分）
  - Apache2と組み合わせるとよくわかる
    - 某書籍で説明したのはこの内容
  - DeltaVとは…WebDAVのバージョン管理拡張だけど、内容を見るとバージョン管理に関する標準化とも解釈できる

Subversion(3/6)
Activityというもの（DeltaVより）

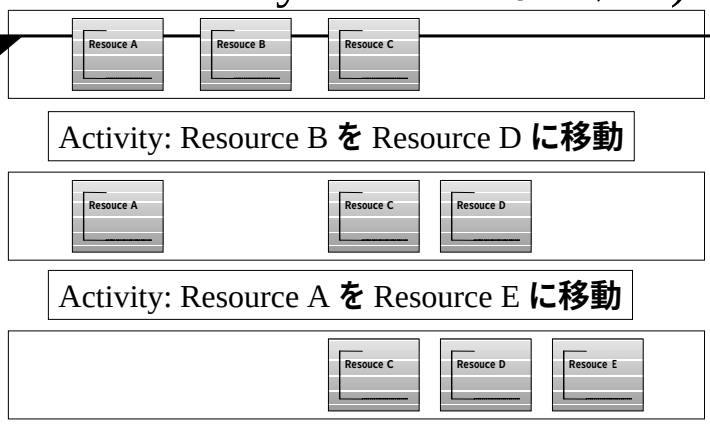


- リソースの変更を組(Set of changes)で扱うためのリソース
  - バージョン管理はされない。

Subversion(4/6)
Activityとバージョン (1/3)

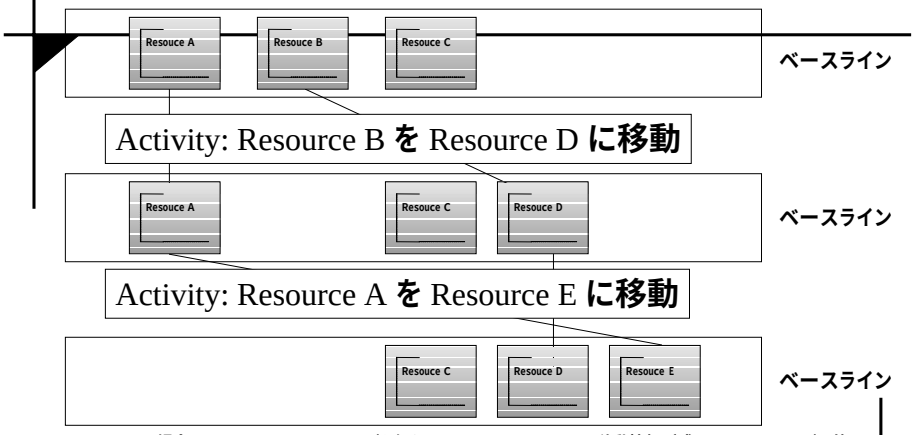


Subversion(5/6)
Activityとバージョン (2/3)



- CVSの場合:Resource A,Bのトラッキングは不可
  (ファイル内容のバージョン管理しか実施しない)

Subversion(6/6) Activityとバージョン(3/3)



- DeltaVの場合、ResourceD,Eのトラッキングを行なうと、ActivityにA,Bからの移動情報が残るためトラッキング可能
- リソースの組をベースラインとして管理していることも大きな利点

Catacomb

- Sung Kim氏によるDASLの実装
  - SEARCHメソッドの実装
  - cadaverの最新版で検索に対応
  - メタデータ(プロパティ)検索および、全文(リソースそのものの内容)検索が可能
  - Cadaverから使用可能
- リポジトリをDBMS(MySQL)上に持つ
- RFC2518的にはDAV Compliant Classは1,2
- RFC3253のBasic Versioning Featureも実装されている
  - この場合、クライアントはcadaverを用いる
  - Cadaverの最新版ではversion,checkout,checkinコマンドなどが使える

アクセス制御機能を備えた WebDAVサーバ

- WebDAV RBAC(Role Based Access Control)
  - アクセス制御機能を有するWebDAVの開発
    http://www.ipa.go.jp/security/fy15/development/dav_rbac/index.html
    http://rbac.igel.co.jp/index.php?WebDAV%20RBAC
    - IPAの事業の一環として実施された
- RBACメソッドを実装
  - 内容を見るとACLに酷似

WebDAVのクライアント実装(1/2)

- フリーソフトウェア・オープンソースソフトウェアな実装
  - Cadaver
  - davtool
  - PerlDAV
  - DAVExplorer、
  - DAVManager
  - sitecopy
  - jEdit + WebDAVプラグイン
  - Eldav
  - Argon
  - 他にもいろいろ…

WebDAVのクライアント実装(2/2)

- 商用製品での実装
  - Webフォルダ
  - Adobe Acrobat 5以降
  - その他…

cadaver(1/2)

- コマンドラインWebDAVクライアント
- FTPライクな操作性
- DASLやDeltaVにも一部対応
  - Catacomb向けの拡張機能
- i18n対応はパッチで…
  - NECの吉山氏によるパッチが存在

cadaver(2/2)

- CによるWebDAVクライアント実装
  - http://www.webdav.org/cadaver/ より入手可能
  - 最新は0.22.2 (2004/10/23時点)
  - FTPライクな操作性
  - Install も容易
  - 実行例→
  - パッチもいろいろ
    - WebDAV RBAC クライアントも

```
$ cadaver http://localhost/davauth/
Looking up hostname... Connecting to server... connected.
Authentication required for editor on server `localhost':
Username: wakatono
Password:
dav:/davauth/> ls
Listing collection `/davauth/': succeeded.
        .htaccess                305  Nov 28 11:36
        DAVSec.txt              7533  Nov 28 11:32
        DAVSec.txt~             7659  Nov 28 11:32
        DAVSec_.lzh            13880  Nov 28 11:32
        FIG.txt                 1155  Nov 28 11:32
        FIG.txt~                 284  Nov 28 11:32
        davsec20011126.lzh     14821  Nov 28 11:32
dav:/davauth/> quit
Connection to `localhost' closed.
```


davfs2

- Catacomb の Sung Kim氏による実装
- Linuxのファイルシステムモジュールとして実装
  - DAVクライアントである
- DAVサーバ上の領域をファイルシステムとして操作可能
  - Codaモジュールに依存
    - Codaモジュール内のルーチンを使用
  - LKM(Loadable Kernel Module)として導入可

davtool

- Catacomb の Sung Kim氏による実装
- -mオプションでメソッドを指定可能
  - 無指定時はGETを指定したことになる
  - -m PROPFIND
- リクエストボディを指定することが可能
  - -i オプションでリクエストボディの格納されたファイル名を指定
- Depthヘッダ, Content-Typeを指定可能
  - それぞれ-dオプション,-tオプションで指定可能

ARGON

- 日本製のクライアントライブラリ
  - Neon →Argon というのが名前のもと
  - IPAのオープンソースソフトウエア活用基盤整備事業に応募、テーマ採択される
    - 住友電工情報システム㈱によるプロジェクト
    - http://www.sei-info.co.jp/IPAHP/JP/indexJ.html
  - クライアントライブラリとサンプルから成る
    - C++のライブラリとして実装
  - DeltaV,DASL,ACLなどにも対応している

Webフォルダ(1/2)

- Windows 98SE以降で使用可能
  - Windows98でも使えるが付加コンポーネントが必要
- Windows XPでは複数のWebDAVサーバへのアクセスのためのしくみを搭載
  - WebフォルダとWebClientサービス
    - WebClientサービスで不具合頻発（後述）
- 容易にリソースやコレクションの操作可能
- 一部 Internet Explorer と共有する部分があり、不具合も
  - キャッシュを溜め込みすぎると不具合頻発

Webフォルダ(2/2)

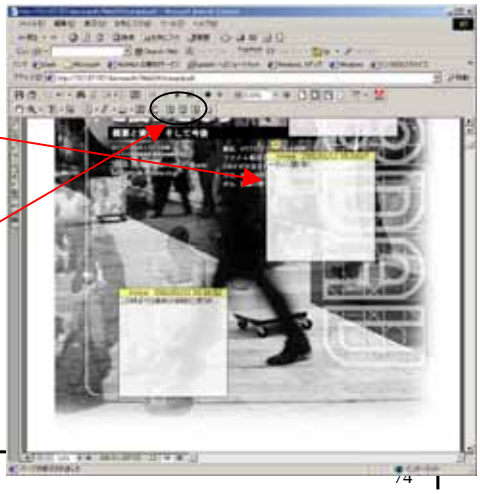
- Windows における WebDAVクライアント実装
- 実行例

Adobe Acrobat 5以降(1/2)

- オンライン注釈のデータをWebDAVサーバ上に置くことが可能
- ボタン一発で注釈データのアップロード／ダウンロードが可能
- URLの扱いに不備があり、トラブルも
  - WebDAVサーバのURLを指定する際にURLの最後に / がないとうまく処理されない

Adobe Acrobat 5以降(2/2)

- 例えば…
  - Acrobat 5のオンライン注釈機能
  - WebDAV経由で注釈をアップロード可能



その他の実装（Proxy編）

- Squid
  - RFC2518レベルは対応
    - Microsoft Exchange Server 2000 の独自メソッド（BCOPYなど）にも対応している
  - RFC3253以降はメソッドを追加して対応
    - 但し20個まで
  - ACLの設定で、簡単なファイアウォールにも
    - かけすぎると大変なことに
  - リクエストのサイズ制限には注意
    - デフォルトは1MB

その他の実装（Proxy編）

- 商用Proxy
  - 結構対応しているようだ
    - 例えばMS製品では、Microsoft Proxy 2.0 から対応
  - ただ、古すぎるものは対応してない可能性大
    - オープンソースなProxyではパッチで対応しているものもあるが、入れ替えた方が吉
  - 私自身はCacheFlowとF5 Networksの装置で確認

WebDAVをどう使う？ ～実用への提案

- その1:どこでもオフィスのコンポーネント
  - Microsoft Office, OpenOffice.orgはWebDAVに対応している
  - WindowsもWebフォルダ使えばOK
  - UNIXもcadaverなりJavaのクライアントを使えばOK
  - KDEでもKonquerorでWebDAVサポート
- その2:自由度の高いWebオーサリング
  - メジャーなWebオーサリングツールはおおよそ対応
    - Dreamweaver, Homepage Builder, GoLive
- その3:分散開発支援
  - Subversionを使うことで、HTTPを経由しての構成管理

増える商用サービス

- IIJドキュメントエクスチェンジサービス
  - http://www.iij.ad.jp/service/system/IIJ-DX.html
- AirTriQサービス
  - http://www.airtriq.jp/
- インターネットディスク
  - http://internetdisk.jp/
- 商用サービスは、WebDAV以外のところで工夫している会社が多い
  - Web経由の管理UI設置、その他管理のためのコマンドの作成、etc...
- その他いろいろ…

いいことばかりじゃありません ～WebDAVの問題点

いいことばかりと言うわけではない

79

いいことばかりじゃありません ～WebDAVの問題点

- 国際化の問題とその対処
  - 文字化けしちゃって…
- Webフォルダでのトラブルと対処
  - 何を疑う？
- Windows XP SP2をあてたら認証NGに
- ユーザ権限設定（UNIX限定）と対処
  - 誰が書いてもnobody権限…

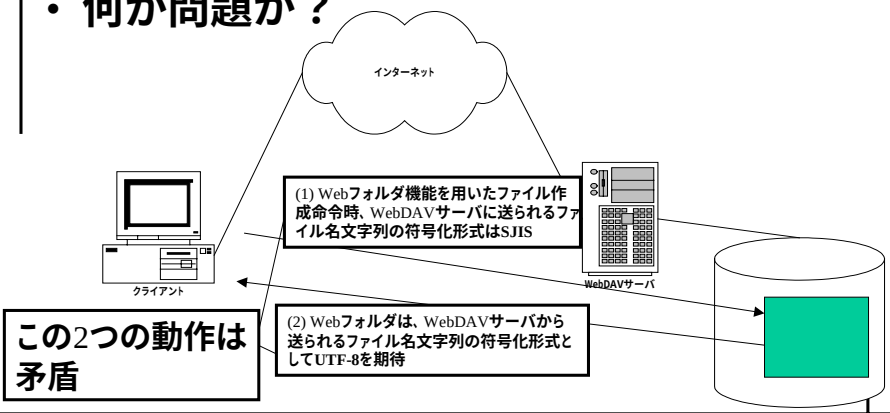
80

国際化の問題とその対処 ～文字化けしちゃって…(1/5)

- mod_encodingである程度は解決できる
- リクエストURIの部分をUTF-8化
  - もともとはクライアントのリクエストURIのEncodingに難ありなものがあったためこういう操作が必要
  - ヘッダは操作しない
- ダイジェスト認証に難あり
  - URLの書き換えを実施するため、クライアントで計算したダイジェスト(CP932ベースのURI)とサーバサイドで計算したダイジェスト(UTF-8ベースのURIをもとに計算)があわない

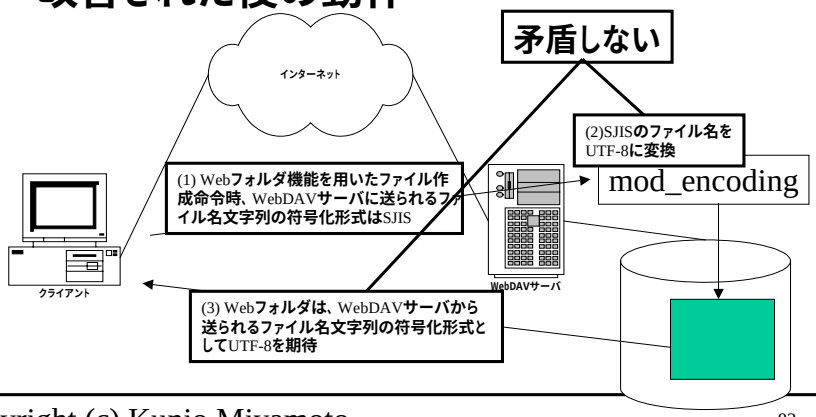
国際化の問題とその対処 ～文字化けしちゃって…(2/5)

- 何が問題か？



国際化の問題とその対処 ～文字化けしちゃって…(3/5)

- 改善された後の動作

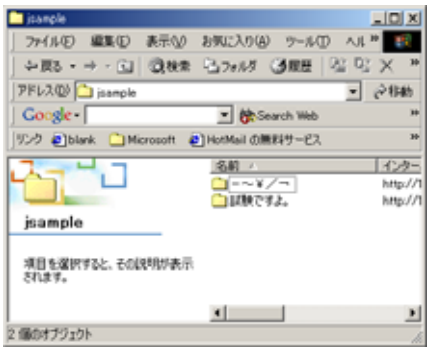


国際化の問題とその対処 ～文字化けしちゃって…(4/5)

- 改善前
  - 「ー～￥／¬」というファイル名をDAV経由で作成すると化けた＆以後アクセス不可

国際化の問題とその対処 ～文字化けしちゃって…(5/5)

- 改善後
  - 使えるようにはなった。
  - Sambaからのアクセスも可能



Webフォルダでのトラブルと対処

- 何を疑う？
  - 疑うのは何箇所かある
    - Internet Explorer のキャッシュ溜め込みすぎ？
    - WebClientサービス動いてない？
    - OfficeのSRあててる？
  - 私の場合はキャッシュを消して解決できた
    - そんなにキャッシュに溜め込むなという話も…

Windows XP SP2でのトラブル

- ベーシック認証が使えなくなった
  - WebDAVリダイレクタの改修なので、WebClientサービスを有効にしてる場合に影響
  - レジストリ操作で回避可能
    http://www.microsoft.com/japan/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx#EFAA
    - あんまりお勧めしませんが…

ユーザ権限設定（UNIX限定）と対処

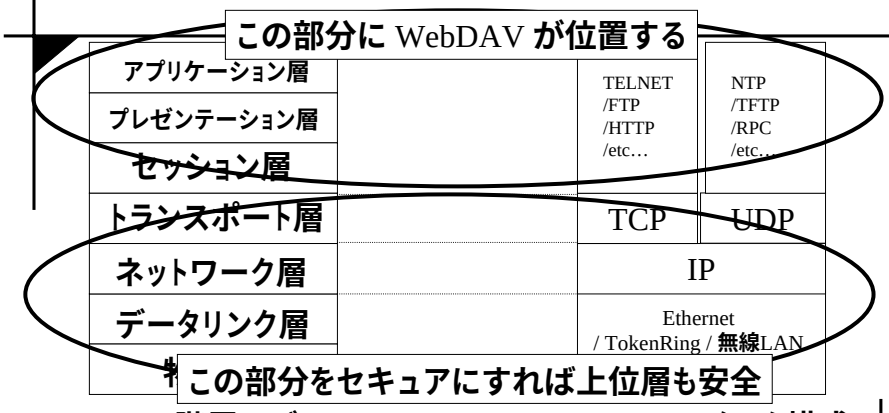
- mod_suid2を利用
  - 中満英生氏(http://www.bluecoara.net/)による
  - アクセスURLによるユーザ権限切替を実施
- mod_ruidを利用
  - http://websupport.sk/~stanojr/projects/mod_ruid/
  - mod_suid2をベースにした改良版
  - Linux専用
- 吉山氏のパッチを利用
  - 詳細はWebDAV-JP MLのアーカイブやWebDAV Resources JPに
    - http://begi.net/webdav/
    - http://webdav.todo.gr.jp/

WebDAVセキュリティの基本

基本はいっしょ

89

WebDAVセキュリティの基本



OSI 7階層モデル　　TCP/IP のスタック構成

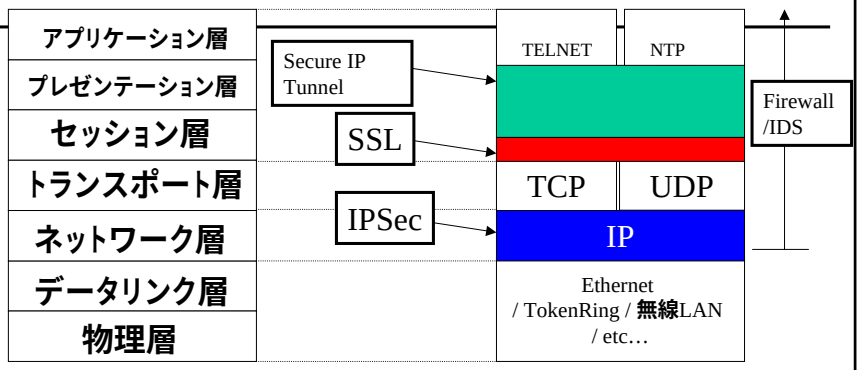
Webサーバセキュリティの考え方が流用可

90

セキュリティ確保の方法

- Firewall / IDS の導入（コネクション自体を切断／拒絶）
  - 不要なサービスの遮断
  - 侵入検知
- 通信内容の暗号化（盗聴を無効化）
  - 通信レイヤごとにいろんな方法がある
    - レイヤ2（データリンクレベル）
      - WEP（無線LAN）
    - レイヤ3（ネットワークレベル）
      - IPSec ,etc…
    - レイヤ4 and above（アプリケーションレベル）
      - SSL / Secure IP Tunnel (SSH / Zebedee) / SOCKS / etc…

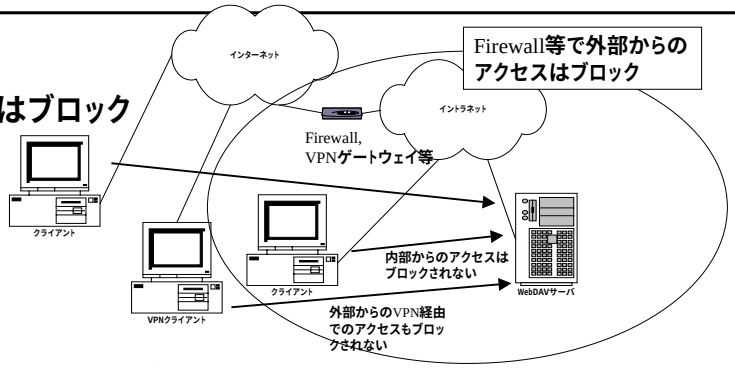
各セキュリティ実装の位置関係



OSI 7階層モデル　　TCP/IP のスタック構成

ところが…

外部からはブロック



- リクエストがレイヤ3やレイヤ4レベルで通過してしまった（セキュアなネットワークの内部で何らかの不正アクセスが試行される）場合、WebDAVサーバの認証／アクセス制限のみが頼り

DAVを不正に使われないために

- VPNクライアントや鍵の管理を厳重に
  - 大基本
- **Firewall を過信しない**
  - フィルタはフィルタ
  - 正しい形式のリクエストにはFirewall / IDS は無効
  - 破られてもその後でブロック可能なように
- **考えられる脅威を把握する**
  - 適切な設定を施す
  - 各メソッドの動作を把握して
  - 適切なユーザに適切な認証を

DAVで考えられる脅威の把握

- DAVやWebサーバの特性／公開文書等から得られる情報
  - http://www.webdav.org/ 等から情報は取得可
- DAVアクセスで発行されるメソッドの動作
  - 注意しておかないととんでもないことに
- 適切なユーザに適切な権限を付与
  - 認証にも気をつけて。
- Apache での例を次ページ以降で

対策

- メソッドの制限（全メソッド）
  - <Limit>, <LimitExcept>等を活用
    - 利用方法は後述
- クォータの設定(PUT,COPY)
  - ディスクフルの被害を局所的にとどめる
- ファイル等のパーミッション変更 (PUT,COPY,MOVE,MKCOL,DELETE)
  - HTTPプロセスの実行権限で操作できないように
  - WebDAV経由で操作できなくなる諸刃の剣
- ロックデータベース削除(LOCK)

適切な認証／制限

メソッドの適切な制限

- 先述のメソッドの動作を把握した上で、適切な制限を
  - Writeをともなうメソッド、PROPFINDについては制限をかけた方が好ましい
- 次ページ以降で Apache における制限例

制限の設定(1/2)

- <Limit>ディレクティブを利用
  - 明示的にメソッドを指定した制限に利用
- 例

```
<Location /davauth>
        DAV     on
        AuthUserFile     /home/kmiya/htpwd/user.pwd
        AuthGroupFile    /dev/null
        AuthName         DAVhome
        AuthType         Basic
        <Limit PROPFIND>
            Require user wakatono
        </Limit>
</Location>
```

PROPFINDについて
ユーザwakatonoに対して
認証を求める

制限の設定(2/2)

- <Limit>ディレクティブを利用
  - 複数のメソッドを指定可能
- 例

```
<Location /davauth>
        DAV     on
        AuthUserFile     /home/kmiya/htpwd/user.pwd
        AuthGroupFile    /dev/null
        AuthName         DAVhome
        AuthType         Basic
        <Limit PUT DELETE PROPFIND PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
            Require user wakatono
        </Limit>
</Location>
```

RFC2518で追加されたメソッド
および、PUT,DELETEを制限

効率的な制限の設定(1/2)

- <Limit>ディレクティブの欠点
  - 新しいメソッドが追加された時、それを明示的に指定追加する必要がある
    - 例：RFC3253で策定されたMKACTIVITY, CHECKIN他の新メソッドを利用する機能をApacheに追加した場合はそれらを指定する必要あり。
- <LimitExcept>ディレクティブの利用
  - 指定した「以外」のメソッドについて制限

効率的な制限の設定(2/2)

- <LimitExcept>ディレクティブを利用
  - 複数のメソッドを指定可能
- 例

```
<Location /davauth>
    DAV     on
    AuthUserFile     /home/kmiya/htpwd/user.pwd
    AuthGroupFile    /dev/null
    AuthName         DAVhome
    AuthType         Basic
    <LimitExcept GET HEAD OPTIONS>
       Require user wakatono
    </LimitExcept>
</Location>
```

GET,HEAD,OPTIONS
「以外」のメソッドを制限

安全な認証のために(1/4)

- ベーシック認証の危険性
  - 盗聴に対して非常に脆弱
  - それ以前に、WebDAVでは利用を推奨しない
- 例

```
PROPFIND /davauth HTTP/1.1
Accept-Language: ja, en-us;q=0.2
Content-Type: text/xml
Translate: f
Content-Length: 380
Depth: 1
User-Agent: Microsoft Data Access Internet Publishing Provider DAV 1.1
Host: tripmachine
Connection: Keep-Alive
Authorization: Basic d2FrYXRvbm86d2FrYXBhc3M=

<?xml version="1.0" ?>..<propfind xmlns="DAV:">
(略)
```

IDとパスワードが MIME Encodeされてるだけ

ベーシック認証時に流れる電文

安全な認証のために(2/4)

- ベーシック認証の危険性
  - Authorization ヘッダの内容をデコードしてみる

Authorization ヘッダの内容

```
$ mimencode -u
d2FrYXRvbm86d2FrYXBhc3M=
wakatono:wakapass
```

ID:パスワードの組み合わせ

安全な認証のために(3/4)

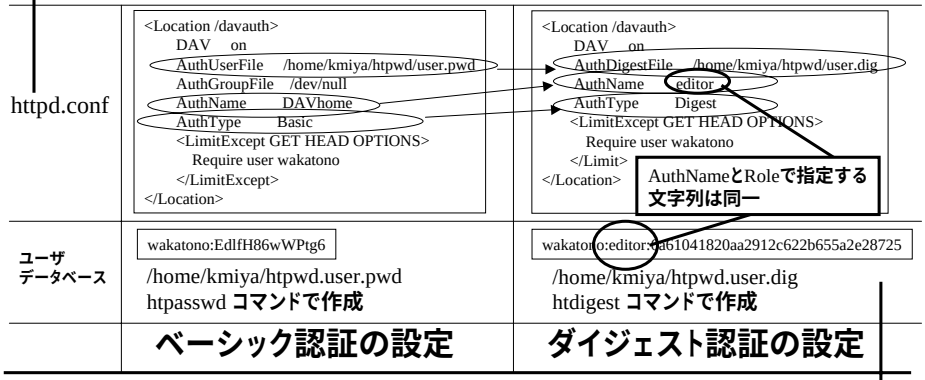
- ダイジェスト認証
  - RFC2069で規定
  - RFC2518では、実装は必須のもの
  - 直接IDとパスワードを送るかわりに、パスワードのダイジェストとIDを送る
    - 同じパスワードでも、ダイジェストの内容は毎回変わる
  - Apache 1.3.8以降,IIS5以降 で利用可能
    - Apache2は標準、Apache 1.3.x では experimental

安全な認証のために(4/4)

- Apacheでのダイジェスト認証利用のために
  - インストール＆設定
    - Experimental ではあるが、Apache1.3.x では問題なく利用可
    - ベーシック認証しかできないクライアントのために、mod_bolというモジュールは有用。
- 注意
  - 使うクライアントはダイジェスト認証に対応してる？
  - mod_encodingを使ってる場合は認証失敗する可能性
  - ベーシック認証を使うならば、通信路をセキュアに
    - SSLなどで保護しておけばまだ安心（でも油断は出来ない）
    - コンテンツを読まれる以上に被害甚大（消されるとかDoSとか）

Apacheでダイジェスト認証(1/2)

- 設定



Apacheでダイジェスト認証(2/2)

- 設定 (ユーザデータベースの作成)
  - htdigest コマンドを使用する
  - 新規データベース作成の例

```
$ /usr/local/apache/bin/htdigest  -c user.dig sample wakatono
Adding password for wakatono in realm sample.
New password:
Re-type new password:
$ cat user.dig
wakatono:sample:7d7dd82a166d8278f415c9333e0641b5
$
```

ダイジェスト認証の実例

- 認証文字列は全て異なる（パスワードは同一）

WebDAVの利用を制限するには ～Proxyの活用～

シームレスであるために起こりうる
事故を防ぐ
そして「覚えのない」制限の原因を探る

WebDAVの特徴

- DAVではじめて規定されたメソッド
  - MKCOL, COPY, MOVE, PROPFIND, PROPPATCH
- DAVではじめて規定されたヘッダ
  - Destination, Depth, If, ...
- 以前からあるメソッドだが、あまり実装されていなかったもの
  - PUT, DELETE

WebDAVの何を制限するか?

- メソッドを制限
  - 書き込みに関連したメソッドをProxyが許可しない
- リクエストのサイズを制限
  - 基本的には、ファイルを送るなどの行為が発生しなければ、メガバイト級の大きなサイズのリクエストは発生しないだろう

…どうやって？

ProxyでWebDAVの使用を制限

- Squidでこれらの制限は可能
  - ACLを活用（メソッド制限）
  - リミットを設定（リクエストやヘッダサイズ制限）
    - request_body_max_size（デフォルト10MB）
    - request_header_max_size（デフォルト10kB）
  - ヘッダはあまり細かく制御できない
    - ユーザエージェントの種類くらい
- 次ページに設定例を示します

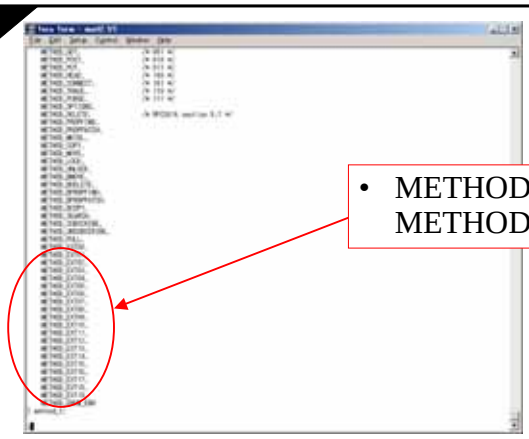
Squidでの設定例

```
# HTTPPORT,PUT_METHODという名前のACLを
# 定義
acl HTTPPORT port 80
acl PUT_METHOD method PUT
（中略）
#80番ポートに対するPUTを禁止
http_access deny PUT_METHOD HTTPPORT
```

逆の悩み～制限した覚えないのに

- Squidを使ってSubversionやCatacomb使って…
  - 使えないorz
- 理由は？
  - 単純に対応していない
    - Squid-2.5 STABLE7, Squid-3.0 PRE3のどちらもバージョニング拡張には対応していない
  - 例えば、以下のような感じでメソッドを追加
    extension_methods VERSION-CONTROL MKACTIVITY CHECKOUT MERGE CHECKIN MKWORKSPACE UPDATE LABEL REPORT
  - 追加可能なメソッドは20個まで
    コード上の制限（たぶん拡張可能）

Squidのコードの上は？ (Squid3 PRE3)



- METHOD_EXT00～ METHOD_EXT19が拡張領域

まとめ
～結局WebDAVはいいの悪いの？

- 普及の度合いは？
- 使いどころと注意点
- そして今後の課題

普及の度合いはどうだろう

- 普及が進んでるのか進んでないのかわからない
  - WGも停滞気味という噂
- 実装はもう広く配布されている
  - Microsoft製品にバンドルされている（いろいろ）
    - 特にWindows
    - 後には引けない（多分MS的にはこんなところ）
  - IPP(Intenret Printing Protocol), WebDAVという感じか？

使いどころと注意点

あくまで私見ですが…

- WAN経由の共同作業には便利
  - ファイル共有がLANと同じ感覚で可能
  - LANとWANで同じインタフェースで作業可能
  - NFSなどとくらべるとネットワークにかかる負担は大きい（特にwrite時）
- LOCKを活用しよう
  - 更新の時には必ずリソースをLOCKしよう
- セキュリティ上の考慮は必須
  - HTTPと同様だが、writeが出来る分デンジャラス
  - 組織内からの情報漏洩のパスの1つにもなりうる

今後の課題

- 利用促進
  - まだDAVは歴史が浅い
    - 1999年2月がRFC2518のリリース（5歳10ヶ月）
  - よく使われるようになれば、改善も早い（だろう）
    - がんばりましょう（オレもがんばりますが…）
- 何はなくともURI表記の国際化
  - 特にURI名前空間の国際化については深刻
    - 表現方法がいくつもあるが、DAVでこれというのが決まっていない
      - URL Encoding Style, UTF-8, CP932（論外）, etc...
- クライアントでの国際化対応
  - 実装でカバーするのも案

参考資料(1/6)

- WebDAV Resources
  - http://www.webdav.org/
- WebDAV Resources JP
  - http://webdav.todo.gr.jp/
- Subversionによるバージョン管理（日本語訳）
  - http://subversion.bluegate.org/
- Microsoft WebDAV の発行
  - http://www.microsoft.com/JAPAN/developer/library/jpiis/core/wcwbdav.htm

参考資料(2/6)

- WebDAV入門―ダヴとXMLがつくる情報共有の未来
  - ISBN: 4883092208
- WebDAVシステム構築ガイド ーApache／IIS／Subversion／Jakarta Slide
  - ISBN: 4774119113
- Webdav: Next-Generation Collaborative Web Authoring
  - ISBN:0130652083（洋書）

参考資料(3/6)

- 次世代プロトコルWebDAVの可能性 ［前編］［中編］［後編］
  - http://www.atmarkit.co.jp/flinux/special/webdav/webdav01a.html 〜
- WebDAV時代のセキュリティ対策 ［前編］［後編］
  - http://www.atmarkit.co.jp/flinux/special/webdav02/webdav01a.html 〜
- UNIX USER 2003年11月号
  - WebDAVファイル共有 最新事情

参考資料(4/6)

- Subversionによるバージョン管理（日本語訳）
  - http://subversion.bluegate.org/
- Subversionによるバージョン管理（@IT記事）
  - http://www.atmarkit.co.jp/flinux/special/webdav03/webdav02a.html

参考資料(5/6)

- [Subversion]CVSユーザのための Subversionガイド
  - http://d.hatena.ne.jp/wakatono/20040307#p2
- [Subversion]なんでCVSじゃいけないの？ ／なんでCVSなんか踏襲するの？
  - http://d.hatena.ne.jp/wakatono/20040311#p6

参考資料(6/6)

- WebDAV RBAC
  - http://rbac.igel.co.jp/index.php?WebDAV%20RBAC
- ARGONプロジェクト – neon WebDAVライブラリの拡張
  - http://www.sei-info.co.jp/IPAHP/JP/indexJ.html