WebDAV システムのセキュアな設定・運用に関する調査

調査報告書

(フィジビリティスタディ編)

平成 15 年 4 月

情報処理振興事業協会

セキュリティセンター

1. 本編の概要……1

2. WebDAV を利用した情報共有の想定 ……2

2.1. 委員会における電子文書の共有 ……2
2.2. ユーザおよび利用形態の想定……3

3. 想定システムにおける要件 ……5

3.1. ユーザ管理機能に関する要件……5
3.1.1. システム全体および複数の委員会の管理……6
3.1.2. 各委員会内部の権限の管理 ……7
3.2. アクセスコントロールモデルの検討 ……8
3.2.1. アクセスコントロール情報の管理 ……8
3.2.2. ファイルシステムのセマンティクス……8
3.2.3. その他の検討事項……9

4. アクセスコントロール機構の検討 ……10

4.1. アクセスコントロールアーキテクチャの動向……10
4.2. アクセスコントロールアーキテクチャの検討……11
4.2.1. 検討対象 ……11
4.2.2. アクセスコントロール ……12
4.2.3. 認証 ……12
4.2.4. 属性の継承 ……13
4.3. 国際化に関する問題……14

5. ユーザ管理アプリケーション開発に向けて……15

5.1. 開発の有効性 ……15
5.1.1. Apache の管理 ……15

5.1.2. ACL Principal の管理 16
5.1.3. Protected プロパティの管理 16
5.1.4. ACE プロパティの制御とファイル空間管理 16
5.2. 技術的な問題点 17

1. 本編の概要

本調査では、セキュアな WebDAV システムについて、その利用を促進するために設定方法を総括する調査を行うとともに、ソフトウエア開発が必要と考えられるアクセス権管理機能を中心としたフィジビリティスタディ等を行い、今後の技術開発の必要性についての検討を示す。[1]

「フィジビリティスタディ編」においては、セキュアな WebDAV システムを円滑に利用するために必要な機能の抽出を行う。特に、アクセスコントロールアーキテクチャとユーザ管理アプリケーションに注目し、それらの要件を提示する。

対象読者としては、WebDAV のアクセスコントロール機能ソフトウエアおよびアクセスコントロール管理ソフトウエアの設計者・開発者を想定している。

本編の記述の概要を以下に示す。

- まず委員会形式のグループでの WebDAV を用いた情報の共有および作成のモデル化を行い、それらを基に要求仕様を整理する。
- さらに、WebDAV におけるアクセスコントロール仕様の策定動向を考慮して、この要件に適合する WebDAV のアクセスコントロールアーキテクチャを提示する。
- 最後に、ユーザ管理アプリケーションの開発について提案を行い、その有効性と技術的な問題についても言及する。

[1] 本調査は、調査主体である情報処理振興事業協会セキュリティセンター（IPA/ISEC）が、株式会社 SRA 先端技術研究所に委託して平成 14 年度に実施した。

2. WebDAV を利用した情報共有の想定

この章では、セキュアな WebDAV システムの利用像を具体的に検討するために、ひとつの例として委員会における電子文書共有を想定し、その利用像から情報共有システムにおける機能要件の抽出を行う。

2.1. 委員会における電子文書の共有

ここでは、政府および関連する組織、団体における各種委員会での文書作成に WebDAV を利用することを想定する。以下では、対象とするグループを「委員会形式のグループ」もしくは単に「委員会」と呼ぶ。

委員会形式のグループにおける文書の作成は、従来一般には、委員会を構成するメンバが数度にわたりミーティングを行い、作成した文書を郵便、ファックス、電子メールなどを用いてバッチ形式で配布し、変更するプロセスを繰り返す形で進められている。この方法には同時に最新の文書を見ることができず、更新箇所や更新者の管理が困難である等、不便な点が多くあり、協同作業を進める上で効率的とは言い難い。

ここでは物理的に遠隔地で活動する各委員が、ネットワーク上で文書を共有し協同して作成するプロセスを効率よくかつ安全に支援するために WebDAV を用いることを検討していく。

2.2. ユーザおよび利用形態の想定

以下のようにユーザおよび委員会を想定する。

（1） ユーザはいずれかの委員会に所属する。

（2） 委員会は、下表の 4 つの役職のいずれかに該当するユーザより構成される。

表 2-1 ユーザの役職と人数の想定

役職	想定人数
委員長	１名
事務局代表責任者	１名
委員	１０名から２０名程度
事務局担当者	若干名

（3） ユーザの所在地は各地に分散している。

（4） ある委員会を構成するユーザは固定されない。ユーザの参加、脱退などが適宜行われる。

また、システムにおけるユーザおよび委員会の取扱いについては、以下を想定する。

（5） ユーザは委員会が取り扱う議題・項目についての専門家および事務担当者であり、必ず しもコンピュータ及びコンピュータネットワーク等についての専門的な技術や知識を持つとは限らない。

（6） システム上には複数の委員会が存在しうる。

（7） システムにおいて委員会は、論理的なグループとして存在するだけでなく、ユーザなどの主体と同様に取扱い可能とする。データの操作を行う際の権限の移譲もグループに対して行われる。

（8） 委員会における役職と、共有する文書の取り扱いの権限を以下のように規定する。

表 2-2　権限と役職の関係

権限	役職
文書の所有	委員長
文書の管理	事務局代表責任者
文書の閲覧	委員会を構成する全ユーザ
文書の更新	事務局担当者、および、委員会において選任された者

（9） システム上の委員会自体の維持に関する権限を以下のように規定する。

表 2-3　委員会全体に関する権限

権限	役職
委員の登録・削除	事務局担当者
文書更新可能者の登録	事務局担当者

3. 想定システムにおける要件

この章では、想定するシステムにおける要件を、特にアクセスコントロールの実現に必要な要件に絞って検討する。

委員会内に限定された文書の共有を行うためには、情報が送受される通信路を暗号化し、ユーザの認証機構を実現する必要がある。WebDAV における通信を暗号化する方法については本調査報告の「設定・運用ガイド編」において既に述べたので、ここでは取り扱わない。

以下では、想定システムにおけるアクセスコントロールの実現に必要な機能について、まずユーザ管理機能に関する要件を抽出し、次にアクセスコントロールモデルの検討を行う。

検討をより具体的なものとするため、以下ではシステムで利用する Web サーバに Apache 2.0 の利用を想定する。

3.1. ユーザ管理機能に関する要件

想定するシステムの円滑な運用のためにはユーザ管理機能が必要となる。ユーザ管理機能における要件は、次の 2 つに整理される。

- システム全体および複数の委員会の管理
- 各委員会内部の権限の管理

以下、それぞれについて述べる。

3.1.1. システム全体および複数の委員会の管理

システム全体および複数の委員会の管理とは、委員会に対して権限を移譲するための措置を行うことを指す。以下、この管理を行う者をシステム管理者と呼ぶこととする。システム管理者は、特定の委員会には属さない。

システム管理者の作業は個々の委員会運営とは直接的な関連を持たない。この作業は最小限に留めることが望ましい。

システム管理者が行う作業には次のようなものがある。

1. 委員会のためのファイル空間の提供
2. 委員会の文書の管理者の登録
3. 委員会の文書の所有者の設定
4. 委員会をグループとして登録
5. 委員会を構成するものの登録
6. 委員会のグループの削除
7. 委員会を構成するのもの削除および追加
8. アクセスコントロールのための HTTP メソッドの管理者への開放

これらの作業は、システムの利用を開始する段階で必要となる。このため、事務局担当者ではなくシステム管理者が行うことが適当である。（ただし、委員会の構成人員に関する変更の権限を、システム管理者から各委員会に委譲する場合には、上記の項目 5 についてはシステム管理者の作業から外し、委員会事務局担当者の作業項目とすることを検討すべきである。）

また、これらの作業のほとんどは、想定する Web サーバ Apache 2.0 に関する設定に対して変更を加えるものであり、WebDAV のファイル空間に関する設定を変更する作業は少ない。

よって、高度な専門知識を持たないシステム管理者が、これらの初期設定作業を行うためには、Apache 2.0 自体の設定を変更する GUI ツール、もしくは容易に利用可能な CUI ツールが必要となる。これらは、Web サーバの設定を補助するツールであるため、通常の Web アクセスとは独立したアクセス方法を提供する必要がある。Web ツール以外で実装することも可能である。

システム管理者による操作はネットワークセキュリティの確保された状態での通信を前提としている。システム管理者によるアクセスは、サーバと同じ部屋、同じビル、および隣接したビルなど、物理的に他者の盗聴、妨害などを受けない場所から行うことを前提とする。

委員会のための WebDAV 空間の設定に関しては、WebDAV プロトコルを介して設定を行うツールが必要となる。この際の WebDAV の設定はプロトコル階層において下位のプロトコルに依

存する。このため、WebDAV の設定は下位のプロトコルのセマンティクスに影響されない形式で提供すべきである。特に Web サーバ自体の設定はファイルシステムなどの OS の機能に依存することに注意が必要である。

WebDAV で与えた許可が下位のファイルシステムのパーミッションにより無効になる事態、すなわち WebDAV データとファイルシステムの不整合については回避する必要がある。

3.1.2. 各委員会内部の権限の管理

各委員会の運営は事務局担当者が行う。事務局担当者は委員会の文書管理を行う以外に、次の操作を行う。

1. 文書更新可能者の選任に伴うアクセスコントロールの設定
2. 委員会を構成するものの異動に伴うグループメンバの追加および削除

事務局担当者は、担当する委員会に属するので、項目 1 の WebDAV 空間のアクセスに関する設定の変更については、WebDAV 経由のアクセスコントロール設定のメカニズムをシステムより提供する必要がある。

項目 2 のメンバ（Web ユーザ）の増減にともなう設定の変更は、想定する Web サーバ Apache 2.0 の Basic 認証に関する設定の変更と関連しうる。Web サーバ自体の設定の変更が必要となるため、システム管理者に権限を移譲することが望ましい。

3.2. アクセスコントロールモデルの検討

ここでは、まず WebDAV におけるアクセスコントロールの管理について検討する。その後、WebDAV が提供するファイル空間に存在するファイルおよびディレクトリの操作に関するファイルシステムのセマンティクスと、実際の委員会の運用に関するアクセスコントロールモデルについて検討を行う。

3.2.1. アクセスコントロール情報の管理

本調査報告「現状調査編」においても触れたように、WebDAV においてコンテンツを格納する文書やフォルダはリソースと呼ばれるオブジェクトである。また、そのリソースに関する情報は全てプロパティで管理されている。プロパティはオブジェクトの属性を記述したオブジェクト、つまりメタオブジェクトとして表現される。

したがって、アクセスコントロールに関する情報は、WebDAV との整合性を考慮にいれ、各リソースに対応したプロパティの一部として管理することが望ましい。

3.2.2. ファイルシステムのセマンティクス

委員会を構成する者はそれぞれ異なるコンピュータネットワーク環境を利用する。ファイルシステムはそれぞれのコンピュータに依存した機能を提供しているため、WebDAV においてはファイルシステムに関する規定は未定である。ここでは、委員会の運営に対応したファイルシステムのセマンティクスを検討する。

複数のユーザで階層的なファイルシステムを利用する場合の重要のファイルシステムセマンティクスとして以下の取扱いについて検討しなければならない。

- ディレクトリ作成時の上位のディレクトリ属性の継承
- ファイル作成時のディレクトリからの属性の継承

想定する委員会における文書の共有については、以下の性質をあげることができる。

- 全ての文書の所有者は委員会の委員長
- 全ての文書の管理者は事務局の代表
- 全ての文書は委員会の委員および事務局員が閲覧可能
- 全ての事務局員は文書の更新が可能

これらの性質を考慮すると、これらの値は、変更が不可能な WebDAV プロパティとしてディレクトリ作成時およびファイル作成時に継承するのが自然だろう。

想定する委員会における協同作業では、ファイルの更新者は事務局担当者と選任された者である。選任は、文書の作成を委嘱した者に対してのみ、動的にファイルのアクセス権を拡張することで実現できる。このアクセス権の変更については、ファイルの所有者およびファイル管理責任者のみに許可し、ファイルのアクセスコントロール設定に関しての一貫性を保つ。

既述したように、WebDAV 上のファイルシステムのセマンティクスは下位のファイルシステムに依存すべきではない。よって、ファイルのアクセスの許可／不許可は下位のファイルシステムではなく、WebDAV が提供するアクセスコントロールのレイヤで完全に行わなければならない。アクセスコントロールのレイヤにおいて許可されたが、実際のファイル I/O で許可されないということが発生してはならない。

3.2.3. その他の検討事項

その他、アクセスコントロールに関連しシステムに必要となる機能を以下に挙げる。

- アクセス権限に変更を行った際の記録（誰が、いつ、どのよう操作を行ったかのアクセスログ）を残す機能
- 現在の設定状況および現在可能な操作の両方を対で表示するインタフェース機能
- ユーザに提供する非可分な操作（アトミックトランザクション）を細分化せずに提示する機能

4. アクセスコントロール機構の検討

この章では、想定する文書共有システムにおけるアクセスコントロールアーキテクチャに関して検討を行う。

4.1. アクセスコントロールアーキテクチャの動向

既存のアクセスコントロール機構のうち、調査時点において WebDAV システムで利用可能なものを以下に挙げる。

- Basic 認証などの HTTP の authentication に基づくユーザ識別を利用した、ファイル空間へのアクセスコントロール
- HTTP メソッドの制限
- OS のファイルシステムに依存したアクセスコントロール

これらのアクセスコントロール機構については、次のような問題点を指摘できる。

- 提供されるアクセスコントロール機能が貧弱である。
- 設定を変更する際に Web サーバ自体の設定を変更する必要があり、サーバ管理に不慣れなユーザには作業負荷が大きい。
- 設定ミスがセキュリティホールの原因となる可能性がある。
- OS 等の下位レイアに依存した機能を用いるため、システムの汎用性が損なわれる。
- 下位のファイルシステムやオペレーティングシステムのユーザ概念から独立したアクセスコントロールの機構を提供している実装はほとんど存在しない。

このような理由から、オペレーティングシステム等の下位レイヤへの依存度が低く、高い抽象度を持ち、高機能なアクセスコントロール機構の開発が必要となっている。

最も有望なアクセスコントロール機構としては、WebDAV の拡張仕様である WebDAV アクセスコントロールプロトコル仕様（WebDAV ACL）があげられる。

WebDAV ACL 仕様の詳細については本調査報告の「現状調査編」で既に触れた。調査時点においては、この仕様はドラフトの段階にあり、近い将来に標準となることが期待される。

4.2. アクセスコントロールアーキテクチャの検討

4.2.1. 検討対象

WebDAV ACL 仕様をベースとしたアクセスコントロールプロトコルを採用したアーキテクチャの開発について検討を行う。

ACL ベースのアクセスコントロールメカニズムを実装した WebDAV サーバは調査時点においては存在しないが、ACL の採用を視野に入れた開発は、今後の Web アーキテクチャとの整合性を考えればごく自然なアプローチと言える。WebDAV アクセスコントロールプロトコルでは、アクセスコントロールデータが WebDAV のプロパティとして管理される。このため、特別な管理機構の開発は必要とされず、WebDAV が提供する機能に矛盾しない純粋な拡張として実装が可能であり、開発作業が容易になることが予想される。

しかしながら、ACL 仕様については今後大きな変更があり得る点に注意が必要であり、特に詳細に関しては依然曖昧な記述や未定義の部分が多くある点については十分に考慮する必要がある。Web サーバとの整合性についても、明白な課題ではあるが議論が進められていない。

このような理由により、ACL 仕様に基づきアプリケーションシステムを作成する上では、いくつかの実装上の問題点を解消し、アプリケーションに依存した制約条件を導入することも必要となると考えられる。

開発するシステムについては、Web サーバとして Apache 2.0 を用い、ユーザ認証は同ソフトウエアが提供する Basic 認証を利用するものと想定する。

WebDAV のアクセスコントロールは、Apache 2.0 のユーザ認証の結果を基本的な Principal として使用している。さらに、それぞれのリソースへのアクセスは、HTTP メソッドを介して行われるため、WebDAV のアクセスコントロールは下位の HTTP メソッドの実行に関する許可情報を利用することになる。更に実装上、リソースが OS レベルではファイルとして表現される場合には、その OS 特有のファイルパーミッションによるアクセスコントロールが WebDAV のセマンティックスと独立に適応されてしまう可能性も考慮しておかなければならない。

これらの議論に基づいた、認証およびアクセスコントロールのアーキテクチャに関する検討を以下に示す。特に実装に依存する WebDAV サーバのファイルシステムセマンティクスについても検討を加えた。

以下に記述する WebDAV のコレクションの階層構造と委員会構造の対応づけ、および構造の上下関係を利用した権限の継承、ACL の権限委譲を適宜行うことにより、委員会の管理セマンティックスを WebDAV の世界で表現することが可能になる。

4.2.2. アクセスコントロール

WebDAV におけるアクセス権は Principal であるユーザ、グループとアクセスするリソースのメタデータであるプロパティとの比較によって決定される。つまり、アクセスコントロールは、実際にはリソースのプロパティの参照と比較、更新によって行われる。このため、アクセスコントロールの設定および検索は、WebDAV メソッドとして提供されている PROPFIND, PROPPATCH および ACL メソッドで操作することができる。

しかし、ACL で Protected プロパティとして指定されているプロパティの変更には他の変更方法を用意しなければならない。また、ユーザの認証は Apache 2.0 の認証に基づくことからも ACL とは別のレイヤでのアクセスコントロールも考慮しなければならない。

これらの議論から、4 つのレイヤで異なるアクセスコントロール機構を提供する必要がある。

1. Apache のレイヤでの Basic 認証をベースとした HTTP メソッドの制限
2. ACL Principal の管理
3. ACL 以外の方法による Protected プロパティの設定
4. WebDAV のレイヤでのＡＣＥプロパティの制御

4.2.3. 認証

WebDAV における認証については、以下の 2 つの問題を解決する必要がある。

1. グループ概念の作成
2. 作成者および管理者という概念の作成

Apache の Basic 認証には、グループの概念が存在しないため、基本的な Principal はユーザに基づくものとする。そのユーザとグループとの関連付けは ACL の設定によって記述される。

すなわち、ユーザのアクセスコントロールは Apache 2.0 の Basic 認証で獲得されたユーザ名と ACL で宣言された Principal との関連付けが行われ、その Principal に対して ACL の Principal による判定機構が働くことによって行われる。

この場合、この Principal に対応するユーザの記述は Apache が提供するアクセス可能な Web 空間の外に格納しなければならない。逆に、Principal の定義を WebDAV および ACL で設定可能とすることはセキュリティ上安全性を著しく可能性があり、回避しなければならない。

4.2.4. 属性の継承

次に属性の継承について述べる。現実世界の委員会等の階層構造をもつ組織は、上位の性質は下部組織、もしくは構成メンバ全体がデフォルトで獲得するものとするのが自然である。この機能の実現は、WebDAV が持つアクセスコントロールリストの継承プロパティ（Inherit Property）を活用することにより自動的な設定の継承が可能になる。さらにファイルシステムのもつ制限によりこの機能を補完することで効果的に行うことができると考えている。

WebDAV にはファイルの所有者（owner）という概念は存在するが、管理者という概念が存在しない。例えば、リソースの所有者を示す DAV:owner プロパティは Protected プロパティであるため、PROPPATCH リクエストによって変更することができない。このことはリソースの所有者を直接的に変更することができないことを意味する。

このような問題を回避するために、ある委員会の WebDAV 空間を指定した際、最上位のコレクション、またはファイルのプロパティは、下位のコレクションおよびファイルに継承されるプロパティとして定義する。継承されたプロパティは個々には変更することはできないため、一貫性の確保を容易に実現することができる。また、それぞれの委員会を示す WebDAV のグループを作成し、グループに対して権限を設定することにより作業の効率化をはかるとともに、グループへの加入・脱退をもってそれぞれの委員会への参加、脱退を表現する。さらに、Protected プロパティが一般に変更できないことから、このプロパティを変更する手段を提供することによって管理者の概念を表現することができる。

具体的には、各委員会グループの最上位のコレクションに対し、グループおよび管理者について

（1）保護されたプロパティ(Protected Property)として定義

（2）文書管理者はそれぞれのコレクションの write 特権を委譲される

（3）同一委員会のファイル、コレクションはこのプロパティを継承

の対応をとっていく。このことにより、グループおよび管理者の権限の一貫性を保つことが可能となる。

4.3. 国際化に関する問題

WebDAV では HTTP メソッドに XML データを添付することで、細かな操作を実現している。アクセスコントロールでは対象を URI で識別しているため、この XML データに対しては国際化された URI を与えることを検討する必要がある。

XML においては UTF-8 によるエンコーディングが標準とされている。しかしながら、URI の国際化に関しては多数の課題がある。調査時点においては IETF に国際化 URI のワーキンググループが設立されてはいるが、今後の動向については不明な点が多い。

したがって、アクセスコントロールの国際化に関しては、将来の動向に注意を払う必要はあるものの、現時点の WebDAV システムの利便性を向上させることを狙うユーザ管理機能の開発においては、検討対象から外すことが適当であると考える。

5. ユーザ管理アプリケーション開発に向けて

この章では、前章までの検討を踏まえ、WebDAV を用いた文書共有システムの運用上有用なユーザ管理アプリケーションを開発する必要性、および開発にあたっての技術的な課題について述べる。

5.1. 開発の有効性

ユーザ管理アプリケーションの機能を実現するためには以下の 4 つのレイヤを制御する必要がある。

1. Apache のレイヤでの Basic 認証をベースとした HTTP メソッドの制限
2. ACL Principal の管理
3. ACL 以外の方法による Protected プロパティの設定
4. WebDAV のレイヤでの ACE プロパティの制御

ここでは、これらの機能を管理するアプリケーションの実現可能性について述べる。

5.1.1. Apache の管理

以下では、Apache 2.0 の Basic 認証をベースとした HTTP メソッドを制限するための高度な設定ツールの実現についての検討を行う。

これらの設定は、通常は Apache 2.0 の設定ファイルを編集して設定を行う。円滑な運用を実現するためには、システムが扱いやすい独自の GUI 環境または簡便な CUI 環境を提供することが望ましい。

これは Apache 2.0 が稼動するシステム（特に GUI 環境）に依存するため、任意の WebDAV サーバの設定には利用できないが、高度な技術・知識を持たない運用者やシステム管理者にとっては必須のツールと言える。本システムにおけるシステム管理者は非常に限られたユーザとな

り、委員や事務局担当等の一般ユーザのクライアントプログラムには影響し無いため、容認される範囲の選択だろう。

5.1.2. ACL Principal の管理

先に述べたように、Apache 2.0 の Basic 認証の結果として得られたユーザ名と ACL で設定する Principal のマッピングに基づきアクセスコントロールが行われる。この Principal の定義ファイルは、セキュリティ上は、Apache 2.0 が通常のクライアントに提供する Web 空間内に配置された操作可能なオブジェクトとして提供されるべきではない。したがって、Principal の設定は設定ファイルなどの形態で実現し、通常の WebDAV の変更作業とは別の手段で変更できる環境を提供することが望ましい。

5.1.3. Protected プロパティの管理

Protected プロパティは仕様上 ACL の機能を利用して変更することはできない。本調査で提案するユーザ管理ツールでは、この Protected プロパティを活用することでシステムを実現するものである。したがって、ACL とは別の経路を利用した方法で Protected プロパティを設定、変更する手段が必要になる。

5.1.4. ACE プロパティの制御とファイル空間管理

ACE プロパティの制御とファイル空間管理の設定は、XML 構文のデータの作成により操作可能ではあるが、これは実現可能性が乏しい。

システムにおける管理者を表現するためには Apache 2.0 の設定ファイルや Protected プロパティの変更をもって行うということはすでに述べた。更にプロパティとして表現されるオブジェクトやユーザの状態に基づき、該当オブジェクトのプロパティを変更することが必要となるケースは容易に想定される。この場合の変更作業は、PROPFIND→LOCK→PROPPATCH という一連のメソッドの処理により実現される必要がある。これら粒度の細かいオペレーションからなる複合オペレーションを人手で行うことは一般に難しく、誤りも混入しやすい。

そこで、WebDAV のプロパティに働きかける複合的な処理を提供する XML プロシージャを提供し、ユーザの付加を軽減することが必要である。

これらは、Web ブラウザを用いた提供可能である。実際には、Java プログラムなど、可能な限りクライアント環境に依存しない形態で実装することが望まれる。

これらのプログラムについては HTML、Java アプレット、その他スクリプト言語などでシュガーコーティングし、Web ブラウザ経由での操作を可能とすることや、あるいは、代表的なブラウザの Plug-in として開発することも可能である。

5.2. 技術的な問題点

WebDAV のアクセスコントロールを実現し、その設定を行う機能を有するソフトウエアを開発する上では、大きな問題は無いが、いくつかの未解決の問題が残されている。ここでは先にも触れた、WebDAV を Apache 2.0 の一部として提供する場合の実装から生じる問題点について述べる。

先に想定したシステムにおけるアクセスコントロール機能においては、Basic 認証は WebDAV でなく Apache 2.0 により行われる。また、一部の HTTP メソッドの利用の制限も WebDAV のアクセスコントロールではなく、実際には Basic 認証のレベルで行われる。WebDAV の基本的な機能は下部のレイヤの制約を無条件に仮定しているため、上位レイヤで許可を与えたリクエストが実行時エラーを引き起こすことが容易に想像される。このような、同様の意味をもつ制御が異なるレイヤで独立に可能である性質は、アクセスコントロールの全体としての一貫性の喪失として表面化する可能性がある。

この一貫性問題に対応するためには、注意深く選択されたマニュアルおよびそれを基に作られたシュガーコーティングされたコマンドセットなどの運用上の対処や、WebDAV のプロパティと Apache 2.0 の設定ファイルの一貫性の問題を発見するようなツールが必要となる。 また、委員会の文書を保管しているリソースの所有者が既にその委員会に存在しない場合など、上位の意味的な整合性を機械的にチェックする機構も、意味的な不整合により現実の業務におよぼす障害を防ぐために必要となるのは明白である。