様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 5 月 20 日現在

研究種目：基盤研究(B)
研究期間：2007～2009
課題番号：19300015
研究課題名（和文）　開かれた計算環境におけるケーパビリティに基づくアクセス制御

研究課題名（英文）　Capability-based access control for open computing environments

研究代表者
新城 靖（SHINJO YASUSHI）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：00253948

研究成果の概要（和文）：本研究は、開かれた計算環境において、ケーパビリティに基づくアクセス制御の実現方式を明らかにした。ケーパビリティとは、アクセス対象の識別子とアクセス権を併せ持ったものである。ケーパビリティの性質を活用して、一般利用者は管理者の手を患わせることなく自分の持つアクセス権の一部を他の利用者に渡すことを様々な環境で実現した。具体的には、電子メール、Web、TCP/IP 接続、無線 LAN 接続で実現した。

研究成果の概要（英文）：In this research, we have clarified the implementation methods of capability-based access control in open computing environments. A capability means a pair of the identifier to a target object and access rights to the object. By making use of characteristics of capabilities, we have enabled regular users to pass a part of their access rights to other users without administrators' efforts in various environments. These environments include the e-mail system, the web, TCP/IP connections, and wireless LAN connections.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	2,400,000	720,000	3,120,000
2008 年度	1,900,000	570,000	2,470,000
2009 年度	1,400,000	420,000	1,820,000
年度			
年度			
総　計	5,700,000	1,710,000	7,410,000

研究分野：計算機科学
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：情報セキュリティ, アクセス制御, ケーパビリティ, 権限委譲, 電子メール Spam 対策, World Wide Web, TCP/IP 接続, 無線 LAN 接続

１．研究開始当初の背景

アクセス制御は、暗号と並び、高いセキュリティを実現し安全で安心な社会を築くために重要な技術である。現在利用されているアクセス制御は、アクセス制御リストに基づくものが主流である。アクセス制御リスト (Access Control List, ACL) とは、利用者やそのグループを主体として、主体とその主体

が可能な操作を列挙したものである。アクセス制御リストに基づく方式は、ファイル・システムにおけるアクセス制御では現在主流であり、Microsoft Windows では、直接的に利用できる。Unix 系のオペレーティング・システムが採用しているファイルのモードも、アクセス制御リストを簡素化したものに分類される。World Wide Web でも、アクセス制御リストは、一般的に使われている。

アクセス制御リストに基づくアクセス制御は、閉ざされた計算環境では有効に機能する。閉ざされた計算環境とは、利用者の集合をあらかじめ明確に定義できるような計算環境のことである。たとえば、構成員が明確な学校や企業などの組織、および、家庭で利用するような計算環境である。この場合、全ての利用者が計算環境に事前に登録されており、利用者名とパスワード、または、公開鍵などがきちんと管理されている。

閉ざされた計算環境に対して、開かれた計算環境とは、利用者の集合があらかじめ明確に規定できないような計算環境である。たとえば、ある時刻に公園に集まっている利用者にのみサービスを提供できるような計算環境が考えられる。また、閉ざされた 2 つの組織ＡとＢがあった時、それぞれの組織の構成員の一部だけが参加するような共同プロジェクトを行いたいことも多い。この場合、プロジェクトの参加者は、プロジェクトの進行状況によりしばしば変化する。このように、利用者の集合が必ずしも常に特定できないような計算環境も開かれた計算環境に含めることにする。開かれた計算環境においても、アクセス制御は重要である。しかしながら、現在主流のアクセス制御方式であるアクセス制御リストに基づく方式は、開かれた環境では、次のような問題が生じる。

・利用者管理の手間が増大する。特にアクセス可能な期間を限定した時に増大する。
・アクセス権の一部を委譲することが難しい。

たとえば、Web ページに対するアクセス制御では、しばしばページごとに利用者管理(利用者名とパスワードの登録) を行う必要が生じる。この方法は、アクセス制御すべきページの数が増えた時に、うまく動作しなくなる。無線 LAN に対するアクセス制御でも、来訪者があった場合に問題が生じる。訪問期間中に限りアクセスを可能にしたい場合、アクセス制御リストに基づく方法では、来訪時に利用者登録を行い、帰宅後に即座に削除する必要がある。この方法では利用者管理の手間が増加する。来訪者の利用者登録を行わず、固定的な利用者が自分の利用者名とパスワードを来訪者に教えたとすると、しばしば無線 LAN アクセス以外の過大な権限を譲渡することになる。

２．研究の目的

本研究の目的は、開かれた計算環境において、効率的なアクセス制御を実現することである。この方法として、ケーパビリティに基づくアクセス制御を用いる。ケーパビリティとは、オブジェクトの識別子とアクセス権を併せ持ったものである。ケーパビリティを持った主体のみがオブジェクトを利用できる。ケーパビリティには、制限されたケーパビリティを定義し、それを他の主体に配布できるという性質を持つ。この性質を活用し、従来のアクセス制御リストに基づく方式における問題点を解決する。すなわち、管理者による利用者管理の手間がなく、かつ、アクセス権の一部を委譲できるようなアクセス制御の仕組みを実現する。

３．研究の方法

本研究課題を達成するためには、次の２つが必要となる。

・ケーパビリティを安全に受け渡しする仕組みを構築する。
・ 個々の対象に対して、操作、ケーパビリティの形式、アクセス制御の対象から利用する仕組みを提供する。

本研究では、次のようなものを対象としてケーパビリティに基づくアクセス制御を実現した。

(1) 電子メール
(2) Web ページ
(3) TCP/IP 接続
(4) 無線 LAN 接続

４．研究成果

本研究の第１の成果は、電子メールを対象としてケーパビリティに基づくアクセス制御を実現したことである（論文 [6]）。電子メールでは、現在、spam メール(迷惑メール)が問題になっている。既存のメールリーダの大きくは、spam フィルタと呼ばれるプログラムが内蔵されており、spam メールを自動的に判定し、除去する機能がある。しかし、spam フィルタは完全ではないので、誤検知により正当なメールを spam メールとして分類する危険性がある。本研究では、この誤検知を防ぐためにケーパビリティに基づくアクセス制御を用いる。まず、spam フィルタを迂回する権利を、ケーパビリティとして実現する。正しいケーパビリティを持ったメールは、直接利用者の受信箱に届けられるため、決して spam フィルタで落とされることはない。提案方式を、Mozilla Thunderbird で実装した。

さらに、ケーパビリティを配布するためのツール Capability Basket を QtRuby により実装した。これらは、Windows、Linux、および、MacOSX で動作する。Capability Basket には、インスタント・メッセンジャ Skype を用いて安全にケーパビリティを送受信する機能を設けた。

本研究の第２の成果は、既存の保護 Web ページに対して外付けでケーパビリティに基づくアクセス制御を実現したことである（論文 [5]）。既存の保護 Web ページの多くは、利用者名とパスワード等で利用者認証を行い、その結果を利用してアクセス制御リストに基づくアクセス制御を行っている。このため、そのようなページをアクセスできる権限を他の利用者に渡すことは困難である。本研究では、Castor と呼ばれるプロキシ・サーバを用いて、そのような保護されたページに対して外付けでケーパビリティに基づくアクセス制御を実現した。Castor では、利用者は、パスワード等の機密情報を隠したまま他の人に保護されたページをアクセスできる権限を渡すことができる。また、より制限されたケーパビリティとして、アクセス回数や期間を限定することもできる。Castor は、Ruby 言語、および、Java 言語を用いて実装されている。Web ブラウザとしては、SSL に対応した任意のものを用いることができる。

本研究の第３の成果は、TCP/IP 接続を対象としてケーパビリティに基づくアクセス制御を実現したことにある（論文 [2]）。工場やホームセキュリティ・システム等の組み込み機器から構成されるネットワークにおて、TCP/IP により機器間の通信がなされることが多い。そのような環境で自社製品だけでは機能が不足した時には他社が開発した機器を接続する必要がある。他社製品を全面的に信頼することはできないので、他社製品がアクセスできる機器を制限したい。この時、アクセス制御リストに基づくアクセス制御を用いると、既存の機器の設定を全て現場で変更することがあり、大きな手間がかかる。この問題を解決するために、内部機器をアクセスする権利をケーパビリティとして表現し、特定の外部機器にケーパビリティを配布するという方式を実現した。この方式では、現場ではなく環境が整ったオフィスでケーパビリティを生成し、外部機器の開発者にファイル等の安全な方法で渡す。外部の機器は、TCP/IP で内部の機器に接続する時に、ケーパビリティを提示する。内部の機器は、受け取ったケーパビリティの電子署名を確認し、正当なものであればこれを受け入れ、そうでなければアクセスを拒否する。このようにして、外部の機器は必要な範囲で内部の機器にアクセスできる。この方式は、Linux において動的リンク・ライブラリを置き換える形で実装した。このため、元の TCP/IP を用いるプログラムを一切改変することなく利用できる。

本研究の第４の成果は、無線 LAN の接続においてケーパビリティに基づくアクセス制御を実現した点にある（論文 [1]）。既存の方式の多くは、アクセス制御リストに基づくアクセス制御を用いているので、利用者登録の作業が発生する。このことは、出張先の無線 LAN を一時的に使いたい時に、利用者登録の手間が大きくなるという問題がある。本研究では、無線 LAN へ接続する権利をケーパビリティとして表現し、他人に受け渡し可能にする。この結果、既に無線 LAN へのアクセス権を持っている利用者から持っていない利用者へ管理者に手間をとらせることなくアクセス権を受け渡すことが可能になる。無線 LAN のアクセスの場合、問題になることは、不正利用が行われた時に誰が行ったかを追跡する必要があることである。本研究では、この問題を解決するために、制限されたケーパビリティの考え方を用いた。他の人にケーパビリティを渡す時には、自分が持っているケーパビリティをそのまま渡すのではなく、それを元に新たに制限されたケーパビリティを生成して渡す。万一不正に利用された場合には、ケーパビリティを生成した人が誰に渡したかを追跡する。この方式は、既存のネットワーク・スイッチ専用機、および、Linux が動作するサーバにおいて利用可能にした。ケーパビリティの受け渡しには、10 桁程度の乱数による識別子を用いた。

以上４つの環境においてケーパビリティに基づくアクセス制御を実現した。この結果、開かれた環境においては、ケーパビリティに基づくアクセス制御が有効であることを確認できた。得に、制限されたケーパビリティの考え方が、有用であることがわかった。また、ケーパビリティに基づくアクセス制御を実現する時に、パスワード・ケーパビリティと呼ばれる、乱数を用いる方法が有効であることが確認された。ケーパビリティを安全に受け渡す方法としては、電子メール用には、capability Basket、保護された Web ページ用には、Castor を開発した。

今後の課題は、ケーパビリティに基づくアクセス制御の適応範囲をさらに広げることである。まず電子メールでは、メーリング・リストへ投稿する権利をケーパビリティとして表現したいと考えている。Web ページに対するアクセス制御では、複数の Castor を相互接続してケーパビリティの受け渡しを実現したいと考えている。TCP/IP による接続では、通信路が安全であることを仮定している。今後は、通信路が安全ではない環境でも利用可能にしたいと考えている。　また、現

在はアプリケーション毎に個別にケーパビリティに基づくアクセス制御を実現してきた。今後は、フレームワークやライブラリを用意して、より簡単にケーパビリティに基づくアクセス制御を利用できるようにしたいと考えている。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 15 件）

[1] 馬渕充啓，高田真吾，小沢健史，豊岡拓，松井慧悟，佐藤聡，新城靖，加藤和彦：″利用者間で接続権限を受け 渡し可能なネットワーク制御機構の実現″，情報処理学会論文誌，Vol.51, No.3, pp.974-988 (2010)．査読有.

[2] Mitsuhiro Mabuchi, Yasushi Shinjo, Koji Hasebe, Akira Sato, Kazuhiko Kato: ″CapaCon: Access Control Mechanism for Inter-Device Communications through TCP connections″, ACM Symposium on Applied Computing (SAC2010), pp.706-712 (2010)．査読有.

[3] 高田真吾,金子直矢,齋藤剛,佐藤聡，新城靖，中井央，板野肯三：″UPKI 認証連携基盤を用いたWebアクセス制御″，情報処理学会研究会報告 2010-IOT-8-38, 6 pages (2010)．査読無.

[4] 高田 真吾，佐藤 聡，新城 靖，中井央，板野 肯三：″認証デバイスを用いたOSの起動・終了制御″，情報処理学会論文誌，Vol.50, No.3, pp.1043-1052 (2009)．査読有.

[5] 馬渕充啓，池嶋俊，川崎仁嗣，吉野純平，松井慧悟，新城靖，佐藤聡，上川大介，加藤和彦：″CaStor：Web資源に対するケーパビリティの管理・配布を行う Web サーバ″，情報処理学会論文誌，Vol.50, No.8, pp.1856-1869 (2009)．査読有.

[6] Yasushi Shinjo, Keigo Matsui, Takuya Sugimoto, and Akira Sato: ″An Anti-Spam Scheme Using Capability-Based Access Control″, 5th IEEE LCN Workshop on Security in Communication Networks (SICK) (SICK 2009), pp.907-914 (2009)．査読有.

[7] 高田真吾，佐藤聡，新城靖，中井央，板野肯三：″認証デバイスを用いたOSの起動・終了制御システムにおける起動時間の短縮″，情報処理学会研究会報告 2009-IOT-004-27, pp.155-160 (2009)．査読無.

[8] 馬渕充啓，小沢健史，高田真吾，豊岡拓，松井慧悟，佐藤聡，新城靖，加藤和彦：″持ち込み PC を対象としたネットワーク利用許可権限の委譲を可能にするアクセス制御メカニズムの実現″，情報処理学会研究会報告 2009-IOT-004-31, pp.179-184 (2009)．査読無.

[9] Mitsuhiro Mabuchi, Yasushi Shinjo, Akira Sato, and Kazuhiko Kato: ″An Access Control Model for Web-Services that Supports Delegation and Creation of Authority″, The 7th International Conference on Networking (ICN'08), pp.213-222 (2008)．査読有.

[10] 杉本卓哉，新城 靖，松井慧悟，佐藤聡，中井 央，板野肯三：″電子メールに対するケーパビリティに基づくアクセス制御の実装″，第70回情報処理学会全国大会講演論文集,3ZB-1, 2ページ (2008)．査読無.

[11] 高田真吾，佐藤 聡，新城 靖，中井央，板野肯三：″USB トークン認証を用いた OS の安全な起動制御″，第 70 回情報処理学会全国大会講演論文集,2Y-7, 2ページ (2008)．査読無.

[12] 馬渕充啓，池嶋俊，川崎仁嗣，吉野純平，松井慧悟，新城靖,佐藤聡，加藤和彦：″既存の Web 資源に対するケーパビリティの管理・配布を行うサーバの実現″，情報処理学会研究会報告 2008-OS-107-6, pp.41-48 (2008)．査読無.

[13] 松井慧悟，新城 靖，杉本卓哉，佐藤聡，中井 央，板野肯三：″ケーパビリティに基づくアクセス制御のためのケーパビリティ管理機構″，第70回情報処理学会全国大会講演論文集,3ZB-2, 2ページ (2008)．査読無.

[14] 高田真吾，佐藤聡，新城靖，中井央，板野肯三：″認証デバイスを用いた OS の安全な起動制御″，情報処理学会研究会報告 2008-IOT-001-14, Vol.2008, No.37, pp.77-82 (2008)．査読無.

[15] 金子 直矢,新城 靖,佐藤 聡,中井 央,板野 肯三：″インスタントメッセンジャを用いたネットワークファイルシステムの実現″，情報処理学会コンピュータシステム・シンポジウム (ComSys2008),ポスターセッション, 2ページ (2008)．査読無.

〔その他〕

ホームページ等
http://www.softlab.cs.tsukuba.ac.jp/

６．研究組織
(1)研究代表者
新城 靖（SHINJO YASUSHI）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：00253948

(2)研究分担者
佐藤 聡（SATO AKIRA）
筑波大学・大学院システム情報工学研究科・講師
研究者番号：90285429