社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－MBL－28　(1)
2004／3／4

ユビキタスネットワークにおける超分散サービスとセキュリティに関するアーキテクチャ（RiSSA)の提案

岸本了造、川越恭二、柴田史久，川合誠

立命館大学理工学部

あらまし
　将来のユビキタスネットワークの研究としてすでに世界中で数多く研究されている。しかし、それらの研究は、無線ネットワークだけの研究であったり、一部サービスの研究を行っているのみで、全体アーキテクチャの研究は行われていない。
　本論文はユビキタスネットワーク全体のアーキテクチャの提案を行う。まず、全体のアーキテクチャを超分散と位置づける。無線レイヤの構造を超分散のアドホックネットワークとし、サービスやセキュリティにおいても超分散環境のアスペクト指向ソフトウエアに基づいたサービス及びセキュリティのプラットホームを提案する。サービスに関してはサービス開発時および運用時にアスペクト指向の導入を行う。セキュリティに関しては超分散の IDS や Web 攻撃対策、ウイルス撃退を対象とする。

RiSSA Network Architecture based on Security and Services

Ryozo Kishimoto, Kyoji Kawagoe, Fimuhisa Shibata, Makoto Kawai
Ritsumeikan University, College of Science and Technology

Abstract
　In this papper, RiSSA Network Architecture based on Security and Services Platform is proposed. There are three layers in RiSSA Network Architecture. The first layer is the mobile network composed of the physical layer, datalink layer and IP network layer. The second layer is the aspect-oriented broker for security and services. The third layer is service layer.
　In this paper, the network construction technique, the handover processing, and the access control technique using geography information is also proposed.

１．はじめに

　現在、インターネットは本来の意味での社会のインフラストラクチャとして、行政、企業活動、市民生活にとってはなくてはならないものになっている。将来は、自動車や家庭ロボット、無線 IC タグといった極めて膨大な端末がネットワークに接続され、多様なサービスが提供されることが期待されている。そのため、各国において、将来のユビキタスネットワークの研究が行われている。
　ユビキタスネットワークの研究として、２つの分野において研究が進められている。１つは、広域無線ネットワークの研究で、第 4 世代の移動通信ネットワークやアドホックネットワークに代表される無線 LAN の研究である。[1],[2],[3],[4]
　もう１つの研究分野は、無線ネットワークの上で提供される情報システムや情報サービスの研究で、現在の Web アプリケーションの次世代のサービスとしての Web サービスの研究開発であったり、JXTA に代表される分散オブジェクト指向に基づく研究などが行われている。
　しかし、現在のインターネットの状況は大きな脆弱性をはらんでいる。それは、不正アクセスや

コンピュータウイルス、ワームといったネットワークや情報システム、情報サービスに対する攻撃である。今年１月にも Mydoom といったワームが発生し、過去最大の被害を与えている。これらワームの出現により、以前であれば、自社の LAN をネットワークの脅威から防御すればよかったが、WAN 上におけるワームの攻撃により、LAN を防御することが大変困難になりつつある。更に、WAN において誰がワームを防御するのかも明らかでない。従来ならば、新たなサービスに対応し、そのトラフィック設計に見合ったネットワークを提案するものであったが、様相は一変した。セキュリティこそが最大の課題になりつつある

本論文はユビキタスネットワーク全体のアーキテクチャの提案を行う。まず、全体のアーキテクチャを超分散と位置づける。無線レイヤの構造を超分散のアドホックネットワークとし、サービスやセキュリティにおいても超分散環境のアスペクト指向ソフトウエアに基づいたサービス及びセキュリティのプラットホームを提案する。

本論文ではまず２章で、全体のアーキテクチャを提案し、次に、3 章で、物理層、データリンク層、ネットワーク層を含む GeoNet と Geo IP を提案する。4 章では、セキュリティアーキテクチャを提案し、最後に、５章では、サービスアーキテクチャとその一部の技術について提案する。

２．ユビキタスネットワークアーキテクチャ RiSSA の提案

図１にユビキタスネットワークにおけるサービ

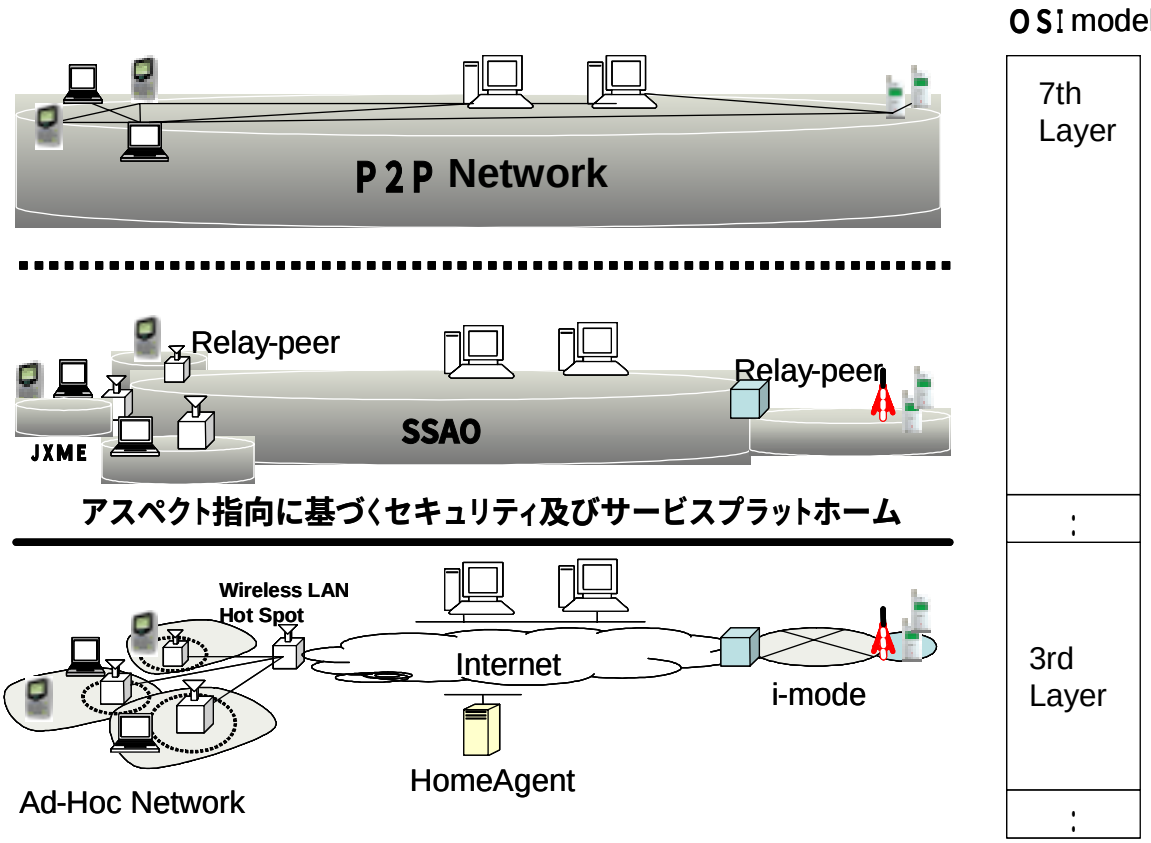

図 1　ユビキタスネットワークにおけるサービス　　とセキュリティアーキテクチャの提案

スとセキュリティアーキテクチャの提案を示す。
ネットワークアーキテクチャは、大きくは、3つの階層に大別される。下位のレイヤは、物理層、データリンク層及びネットワーク層を含むもので、移動透過性として、マクロモビリティ、マイクロモビリティ及びアドホックモビリティを実現している。また、ネットワークはGPSなどから取得出来る位置情報を基本にネットワークアーキテクチャが実現されている。
第2番目の階層は、アスペクト指向ソフトウエアに基づくセキュリティとサービスのプラットホームで、広域ネットワークにおいてセキュリティとサービスをアスペクトあるいは分散オブジェクトとして提供するためのプラットホームである。セキュリティとサービスを提供するための仕組みが提供されている。
第3番目の階層は、情報サービスそのものの階層である。

3．GeoNet及びGeoIPの提案

従来の無線ネットワークは基地局からの電波が及ぶ範囲を一つのネットワークとして扱っていた。つまり，基地局の配置位置がそのまま無線ネットワークの性質を決定してしまい，柔軟な設計が困難であった．しかし，地理情報を元にネットワークを定義できれば，基地局に依存しない柔軟なネットワークを構築が可能となる．

3.1 GeoNetの提案

地理を物理的な尺度で区切った地域範囲を Geo Net と呼ぶ．Geo Net には一対一に対応する Geo Address が割り当てられている．
Geo NetはGISデータによって定義されるので，従来のネットワークの構成のように基地局（以下AP）の電波が届く範囲が１つのネットワークになるといった制約がまったくない．また，Geo Netはそれぞれが意味を持つネットワークであり，利用形態によって柔軟にカスタマイズすることが可能である．

(1) Geo Address

移動体端末(以下MN)が取得する情報は，その時MNが存在する地理的要因と非常に密接な関係がある．しかし，IPアドレスは端末の論理的な位置を示すものであり，物理的な位置を示すものではない．この問題を解決するために，GISを用いIPアドレスに物理的な位置情報という性質を付加する．このIPアドレスをGeo Addressと呼ぶ．Geo AddressはMNの物理的な位置に依存するIPアドレスである。

(2) Basic GeoNet

Basis Geo Netはすべての Geo Net の基盤となる基本的なネットワークである。Basis Geo Net の特徴は複数の AP を含み, それらの AP が 1 つの FA(Foreign Agent)の管理下に置かれていることである。また，この AP の IP アドレスはすべて Basis Geo Address と一致している必要がある。あらゆる Geo Net はこの Basis Geo Net の上に構築される。

3.2 GISを用いた無線ネットワーク網の構成

図2にGISを用いた無線ネットワーク網の構成を示す。

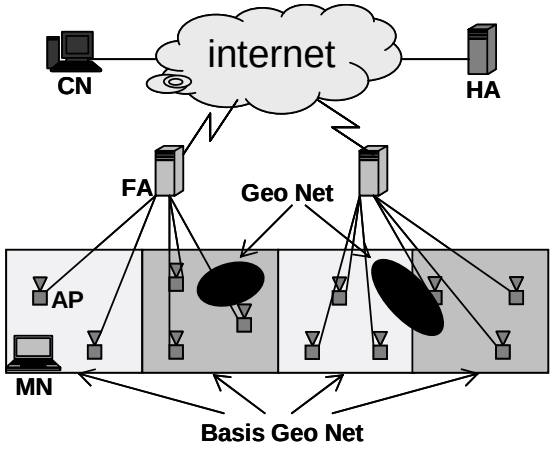

図2　地理情報を考慮した無線ネットワーク網

3.3 GeoIPの提案

Geo IPはIPアドレスにMNの現在位置の情報を加味することで，Mobile IP[5]やCellular IP[6]より，柔軟な通信を可能とする移動透過プロトコルである。IPアドレスは端末の位置を表すといった，特定の意味を内包する識別子ではない．しかし，MNが移動先でAd-Hoc Networkを構築しそのネットワーク内，もしくは周辺のコミュニティに限定した通信を行う場合には，MNの位置や所属するコミュニティを何らかの手法で把握できなければ適正な情報配信は不可能である．Geo IPではGISを用いてこの問題解決する．GISデータで定義されたある限定範囲とIPアドレスが一対一に対応すればIPアドレス自体に地理情報を付加することができる．また，エリアで使用すべきIPアドレスも容易に取得可能となる。

４　セキュリティアーキテキチャの提案

4.1　現在のセキュリティ

広域ネットワークを利用した新たなサービスを提供する場合、ネットワークセキュリティを考慮せずに提案することは困難である。

日々、多くの攻撃や不正アクセスが報道されている。そのため、現在、LAN を守るために、多くのセキュリティ対策や技術が導入されている。しかし、現在のセキュリティ対策や技術で不正侵入などを防ぐのは困難である。

図 3 に、クラッカーがネットワークに不正侵入する侵入・攻撃の全体の流れを示す。クラッカーは、様々な攻撃手法を使って攻撃する。これらの攻撃の中で、多くの攻撃が LAN だけでなく、WAN をも攻撃する。

4.2　ネットワーク型コンピュータワームの出現

特に、大きな脅威はネットワーク型コンピュータワームの出現である。コードレッド（Code Red）と呼ばれるワームが 2001 年 7 月 13 日に発見された。コードレッドは、WindowsNT/2000 上の IIS サーバのバッファオーバーフローの脆弱性を攻撃して、Web ページを改ざんして、ワームをネットワーク上で拡散し、最後に、ＤＤｏＳ攻撃を行う。コードレッドは、プロバイダのサーバや米国ホワイトハウスのサイトのみ攻撃し、一般利用者のパソコンは攻撃しない。コードレッドは、サーバのセキュリティホールを狙う初めてのネットワーク型コンピュータワームであり、セキュリティホールの怖さを示した。

ニムダは、2001 年 9 月に発見され、翌日には、2 万台を超えるコンピュータが感染した。ニムダは、最初は、Web サーバのセキュリティホールを攻撃する。その後、Web ページを改ざんして、Web ページを閲覧にきた利用者を利用して、感染メールをネットワーク上で拡散する。ニムダのメカニズムは、コードレッドのメカニズムとウイルス感染型ワームのメカニズムを有している。

これらのネットワーク型コンピュータワームでは、大量のパケットが広域インターネットに流され、インターネットは使用不能に陥る。更に、インターネットでなくてはならないルーDNS サーバやプロバイダのサーバが攻撃され、メールサービスや Web サービスが利用できなくなる。

一見、一般利用者に無関係に見えるが、ルート DNS サーバが攻撃されると、すべての利用者が被害に合う事になる。2003 年に発生した MS ブラスタは、クライアントパソコンが対象となった。感染すると、自動的に電源がシャットダウンされた。

ニムダは、コードレッドより更に強力な攻撃をしかける。それは、一般の利用者を悪用して、利用者がネットワーク上のホームページを閲覧すると、利用者のパソコンに侵入する。その後、メールを拡散しながら、パソコンの内部データを破壊する。そのため、コードレッドより悪い被害を社会に与えた。

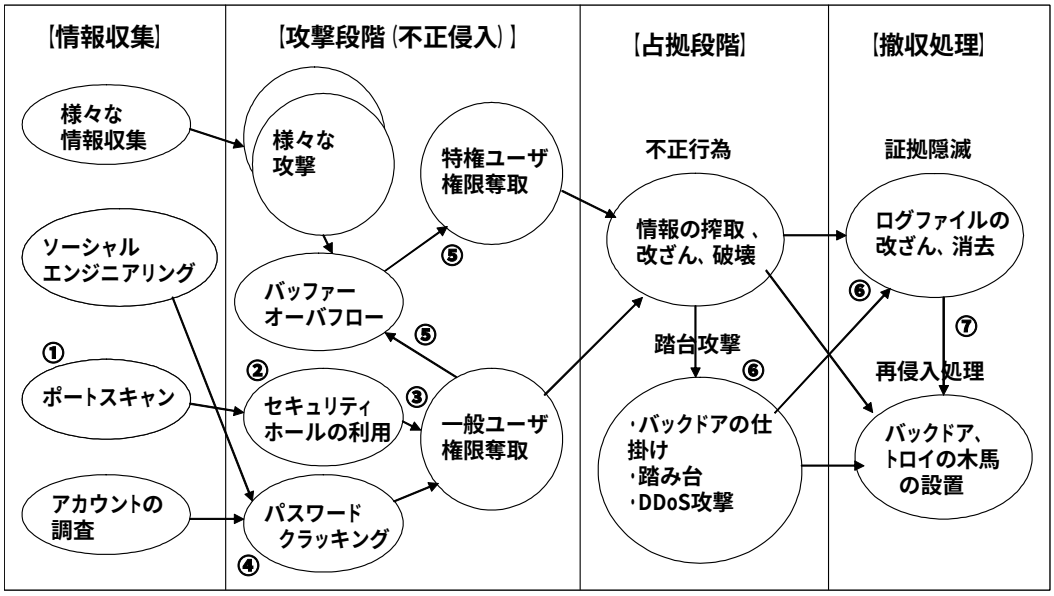

図 3　4 階段に分かれた不正侵入

ニムダの攻撃は、図 4 に示すように、２つの段階を有しており、最終的に WAN および一般利用者に大打撃を与えた。
【攻撃の第１段階：ホームページの改ざんと感染】
【攻撃の第２段階：メールから感染する】

4.3　セキュリティアーキテクチャの提案
ネットワークの脅威や攻撃から WAN を防御するため、セキュリティアーキテクチャとして以下の２つの機能を有する SSAO(Security and Service Platform based on Aspect-Oriented Software)を提案する。

(1) 不正アクセスやワームを駆除するメカニズム、
(2) サービス提供時にセキュアなサービスを提供するメカニズム

(2)の機能は、5 章で提案するセキュアなサービス提供機能で、(1)の機能は、以下に提案する。

【１】おとりによるワームの検出システム
①おとりサーバでの異常検知法によるワーム検出、
②おとりサーバの広域インターネットにおける配備

【２】新種ワームソフトウエアの分析システム
①新種ワームソフトウエアの分析システム
新種ワームソフトウエアの分析
（例えば、CodeRed の場合）
①バッファーオーバーフロー
②ランダム IP アドレスに基づくワームの広域網への拡散、
③DDoS による攻撃
②分析に基づくワクチンのウイルス追尾システム

【３】新種ワームの広域インターネットでの拡散状況の常時計測システム
①ワームの IP パケットのトラヒック増減の異常検知法による測定、
②ワームの拡散モデルに基づく拡散地域の特定

【４】ワクチンの広域インターネットにおける追跡技術システム
①ワクチンの広域インターネットでの追跡技術、
②拡散地域の特定

不正アクセスやワームを駆除するメカニズムでは、ワームなどの異常検知技術がキーとなる。図 5 にＳＯＭ（自己組織化マップ）を用いた異常検知技術の実験結果を示す。

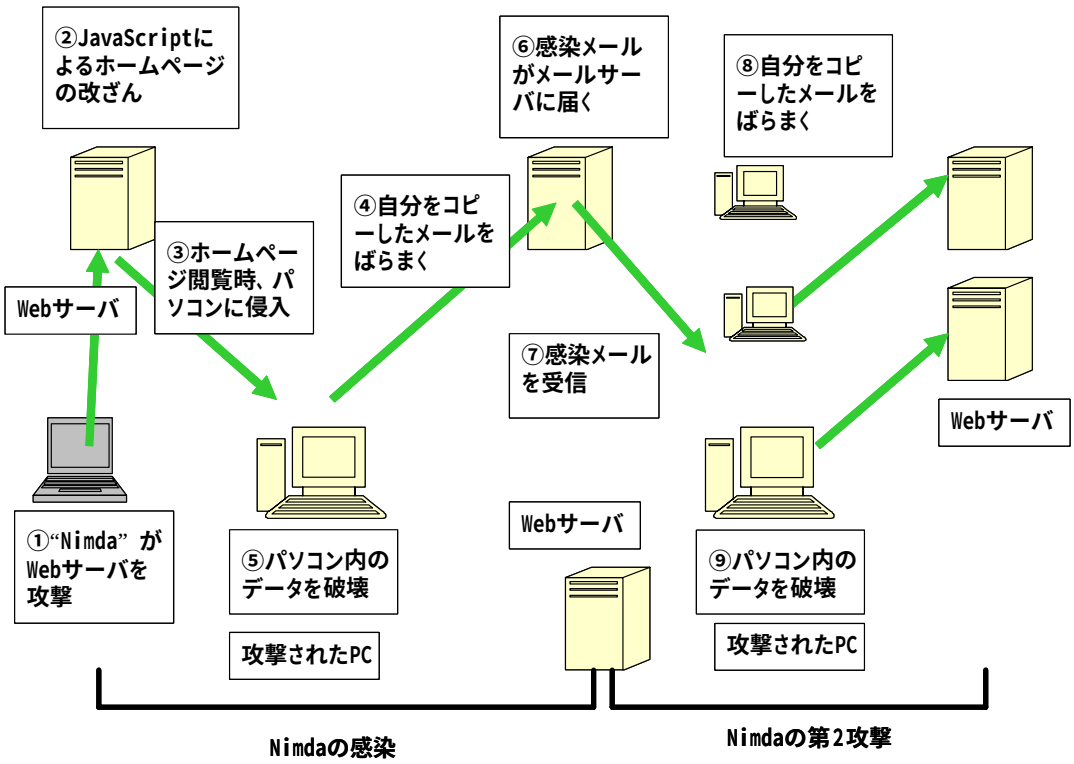

図４　ニムダの感染メカニズム

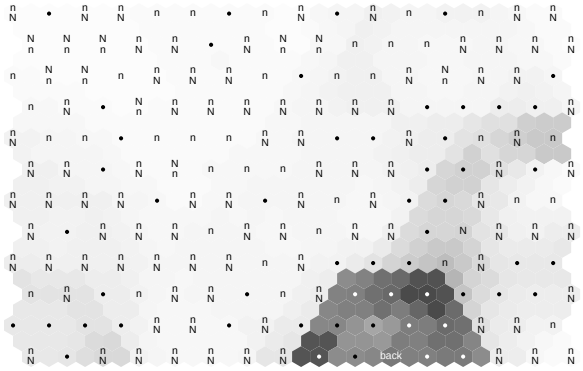

図５　ＳＯＭ（自己組織化マップ）を用いた異常検知技術の提案

５　アスペクト指向に基づいた Web サービス開発の提案

5.1 リスク分析に基づく UML を用いた開発技法

前章で、インターネットにおけるセキュリティリスクについて述べたが、この章では、それらをふまえて、リスク分析に基づく UML を用いた開発技法の提案を行う。

開発者は、開発するアプリケーションにおける情報資産を洗い出し、その情報資産が持つ価値を明確にすることが必要である。そして、その情報資産に対する様々な脅威から保護されるべきであると判断した場合には、対策を講じる必要がある。

以下の過程でリスク分析を行う。

１）情報資産の分析
２）人の分析
３）脅威の分析
４）脆弱性の分析
５）リスク評価
６）対策の策定
７）対策の評価（実装後）

5.2　リスク分析からＵＭＬへの連携

上記のリスク分析を基に、セキュアなシステムを開発するための分析・設計を行うわけであるが、分析・設計には UML を用いる。標準の UML にはセキュリティに関する視点は含まれていないが、本論文では、リスク分析に基づくセキュリティ・ビューから UML を記述することにより、セキュアな開発ができることを述べるのが目的である。

以下、リスク分析から UML への連携について述べる。

5.3　アスペクト指向に基づくＵＭＬの拡張

標準の UML だけでは Web アプリケーションを開発するのに十分とは言えない。UML には標準の UML モデルで十分な表現ができないときに、独自にステレオタイプを追加することで UML を拡張する手段として、UML プロファイルというものがある。これを利用したものに、ジム・コナレン氏によって提唱された WAE for UML（Web アプリケーションのための UML 拡張）というものがある。これは、Web に特有なアーキテクチャの要素を他の部分と同じようにモデル化できるようにするために、Web アプリケーションの Web ページ同士の関連や、それらによって構築される Web ページをクラスとしてみなし、制約とタグ付き値を持ついくつかのステレオタイプを定義することによって、アプリケーション全体のモデル化を計るものである。

本論文では、セキュアなアプリケーション全体のモデル化を行うため、これを基に、セキュリティを考慮したステレオタイプを定義する。

このＵＭＬの拡張では、クラッカーの機能をスーパークラスとして定義する。オブジェクト指向ソフトウエアでは、通常のサービスをオブジェクトのクラスと定義し、クラスでは表現できないものをスーパークラスとして定義する。このスーパークラスという概念は、アスペクト指向の概念の一部を実現する技法である。アスペクトとは、様相という意味で、複数のオブジェクトにまたがる機能を実装する。本来、アスペクト指向技法をより実装するには、AspectJava のようなアスペクト指向言語を用いることが有用である。本論文では、ネットワークの攻撃や脅威をアスペクトとして実装することを提案するものである。

5.4　クラッカーを UML に実装する技法の提案

本論文では、有用性を明らかにするため、Web サイトでの e-ショッピングの書籍購入の例を示す。

オブジェクト指向による情報サービスの分析・設計・実装を行う場合、UML を用いて実装する。まず、分析段階でのユースケース図の構成を提案する。

○分析段階のユースケース図

アクターに、リスク分析における人の分析で洗い出した人（リスクの主体）を、クラッカーを含め図 6 のように表記に加え、それを基に分析する。アプリケーションの通常の利用をするアクターを

ユーザとし、クラッカーをメインとするリスクの主体アクターのスーパークラスとする。リスク分析の際に洗い出したリスクは、リスクの主体アクターに関するユースケースとして表記する。

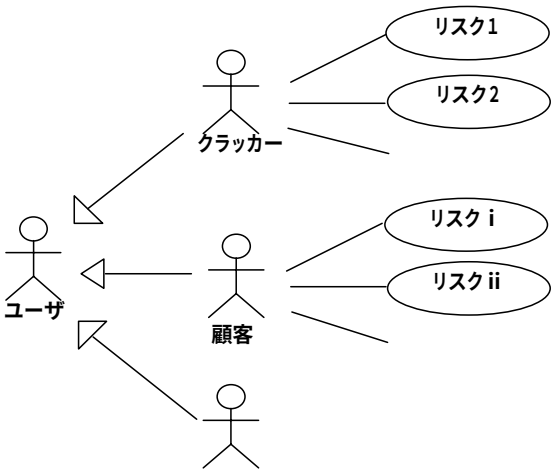

図 6　リスクに関するユースケース図の提案

5.5 システムの実装

最後に、システムを実装的な側面から表記する。「書籍を検索する」ユースケースに関するコンポーネント図は以下の図 7 のようになる。

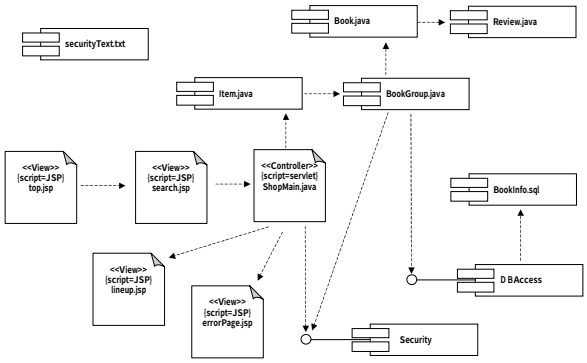

図 7　「書籍を検索する」に関係するコンポーネント図

全てのユースケースに対して、上記のようにコンポーネント図作成し、それを基に実装を行った。なお、ここまで分析・設計・実装といくつかの表や図を用いたが、流れを示すことを目的としたため簡略に示しているが、実際の開発においては、より多く、詳細に記述する必要がある。また、ここで用いた以外の種類の図も表記する必要がある。

5.6 システムの評価

実装した Web アプリケーションが、正常に動作するかの確認を行った。その中で、本論文の重要な課題であるセキュリティ、すなわち開発した Web アプリケーションに対して、策定した対策で脆弱性を抑え、リスクが減少しているかどうかの評価を以下に述べる。

評価法を、対応するアプリケーションの各箇所に試し、正常な結果が出るか確認した。

一例として、クロスサイト・スクリプティングにおける脆弱性の排除を、以下表 1 に示す。

表 1　クロスサイト・スクリプティングに対する対策の評価法

対策名	サニタイジング（XSS）
対策検証箇所	検索結果表示画面 レビュー表示画面 登録情報確認画面 注文情報確認画面
対策検証方法	<S>TEST</S>の文字を入力フォームに入力する。
脆弱性が残っていた場合	~~TEST~~と表示される。
正常な結果	<S>TEST</S>と表示される。

以下、検索結果表示画面における脆弱性の排除を示す。まず、検索フォームに図 8 のようにスクリプトを入力し、「検索」ボタンをクリックした。

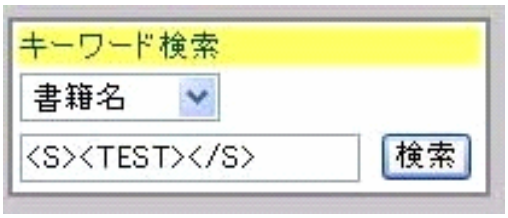

図8　検索入力フォーム

アプリケーションが検索を終えた後の画面は以下の図9のようになった。

図9　検索結果画面

検索結果の表示は以下の図10ようになっており、入力フォームに入力した文字と同じ文字がキーワードの部分に表示され、正常な結果が得られたと言える。故意に脆弱性を残して実験を行った場合は、図11のように表示された。以上より、検索結果表示画面における脆弱性は排除されていることが確認できた。同様に、各対策検証箇所でチェックを行い、脆弱性の排除を確認した。

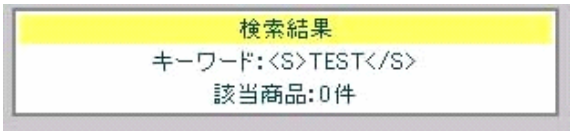

図 10　正常な検索結果

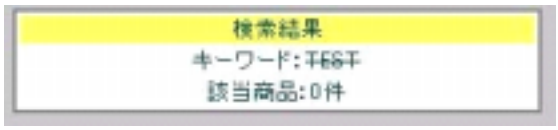

図 11　不正な検索結果。

6.　まとめ

本論文では､ユビキタスネットワークにおけるモバイルネットワーク及びサービスとセキュリティアーキテクチャを提案した。セキュリティを当初から組み込むようなネットワーク提案は以前なら考えられなかった。しかし、インフラストラクチャとしてのネットワークは、社会のあらゆるサービスを実現するプラットホームである。攻撃が厳然として存在するならば、セキュアな環境が求められる。そのセキュアな環境は情報技術やネットワーク技術に従来とは異なった機能を要求する。一例として、ソフトウエア科学は従来、ソフトウエアの品質、経済性などに重点が置かれてきたが、さらにセキュアなソフトウエア科学が必要となる。

参考文献

[1] Young-Bea Ko, and Nitin H. Vaidya, ”Location-Aided Routing (LAR) in Mobile Ad Hoc Networks” Mobicom 1998
[2] Brad Karp and H.T.Kung “GPSR:Greedy Perimeter Stateless Routing for Wireless Networks” (2000) Proc.Mobicom’00.
[3] Stefano Basani, Imrich Chalamtac, Violet R. Syrotiuk and Barry A. Woodward “A Distance Routing Effect Algorithm for Mobility””(1998) Mobicom 98.
[4] 斉藤忠夫，立川啓二，“新版移動通信ハンドブック” (2001) オーム社
[5] James D. Solomon, 寺岡文男，井上淳 “詳解 Mobile IP 移動ノードからのインターネットアクセス” (1998) プレンティスホール出版
[6] A. Campbell, J. Gomez, C-Y. Wan, Z. Turanyi, A. Valko, "Cellular IP," Internet Draft, draft-valko-cellularip-01.txt. (1999)