L-011

ネットワークにおけるCell Wall（細胞壁）モデルの提案

Proposal of the cell wall model in a network

吉村 真弥† 奥野 拓†
Shinya Yoshimura Taku Okuno

1．はじめに

動物細胞のガン細胞に対する免疫系治療は一定の成果を得ている。しかしガンの転移を完全に抑制する免疫システムは研究途上である。また動物細胞のガン細胞は転移しても植物細胞のガン細胞は転移しないことが知られている。この違いは動物細胞にはない細胞壁を植物が持っているからと考えられている。

同様に情報システムの中で免疫系を考えた場合、完全に自己と非自己を区別できないという要件の複雑さのため、効果的な免疫系のセキュリティモデルがない。そこで本稿ではガン細胞の転移をさせない植物の細胞壁に着目し、情報システムにおいてウィルスや不正アクセスからの影響を受けにくい新たなセキュリティモデルを Web サーバーのアクセスに限定して提案する。

2．ガンの転移と免疫系

ガンの転移とは原発腫瘍から離脱したガン細胞が、遠く離れた組織や臓器に移動し、新たにガン細胞のコロニーを形成することである。ガン細胞が原発腫瘍から遠く離れた組織や臓器に転移するプロセスを示す。①ガン細胞が腫瘍から離脱。②上皮組織を区切るバリアーである基底膜を破損。③周囲の組織へ浸潤。④血管やリンパ管に侵入。⑤血液やリンパ液の流れで遠隔へ運ばれる。⑥再び血管やリンパ管から組織に浸潤する。⑦増殖して新たなコロニー（転移巣）を形成。このようにガン細胞は臓器の機能や免疫システムを破壊することによって個体を死においやる。[1]

このプロセスは分散システムにおけるウィルスの増殖と非常に酷似している。ガン細胞をウィルスや悪意のある攻撃者と想定すれば、転移はウィルスの蔓延、踏み台行為と見なすことができる。細胞の免疫システムと同じく情報セキュリティは転移を防ぐ使命を持っている。

ここで免疫システム（免疫系）とは自己と非自己を認識して非自己を排除するシステムを指している。ガン細胞も一種の異物（非自己）であるから、そこに注目して免疫力を高め、ガン細胞を封じ込めることが、免疫療法の基本的な考え方である。

情報セキュリティの世界においてもこのようなアプローチで様々なソリューションが提案されている。（例アンチウィルスソフト）だが自己と非自己を情報セキュリティの世界で完全に認識するのは難しい。それは自己と非自己を認識できることの複雑さのためと考えられる。[2] アンチウィルスソフトは定義ファイルにない未知のウィルスを検知できず、悪意のある攻撃者に乗っ取られたサーバーの検知も難しい。そこで本稿ではガン細胞の転移から別アプローチの免疫モデルを導出し、Web サーバーに限定したアクセスとして適用した。

† 北海道大学情報科学研究科

3. セキュリティのための Cell Wall モデル

一般的に複雑な構造を持つものの方が壊れやすい。動物は体内に多種多様な器官を持つが、植物の器官は花、葉、茎、根のみである。大部分の動物は失った器官を再生できないが、植物では同じ器官が複数あり、葉や花が虫に食べられても植物の生命にはほとんど影響しない。同じように植物にもガン細胞が発生するが、植物の細胞は細胞壁で固定されているため、ガン細胞が他の場所に転移できない。それは強固な細胞壁が転移要素を阻止しているからである。その反面、細胞の柔軟性と流動的な動きを犠牲にしており、柔軟性を犠牲にして構造体を強固にする道を歩んだのが植物といえる。ここで情報システムを細胞と見なすと従来のセキュリティモデルは柔軟性を維持する代償として複雑さを内包する Cell membrane（細胞膜）モデルであると考えられる。これを踏まえて、複雑さを持たず、強固な細胞壁を有する Cell Wall（細胞壁）モデルを提案する。（図 1）

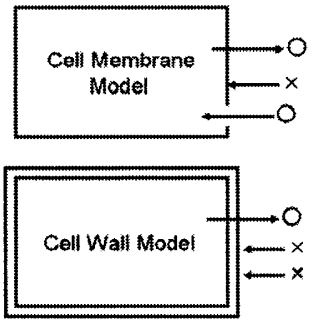

図 1: 従来の Cell Membrane モデルと Cell Wall モデル

このモデルは単純である。入力を内部から外部のみとする。実際には SYN パケットを遮断するファイアウォールを配置することに相当する。従来の Cell Membrane モデルではインバウンドの通信が許可されていることに違いがある。このため DMZ へのサーバーの配置や、要件により異なるファイアウォールの通信ポートを開放しなければならないという複雑さを内包している。例えば DMZ と LAN 内部の通信用の実装を別途作りこむ複雑さがある。また特定の通信ポートの開放では実装の手間だけではなく、その回避として 80（HTTP）、443（SSL）番ポートのみを使う処理の乱立競合などの問題を抱えている。次に外部からの接続要求を一切遮断した Cell Wall モデルは内部での複雑さを内包しておらず簡潔である。ただし外部との双方向通信ができなくなる問題がある。そこで Cell Wall モデルの Web アクセスにおける通信は図 2 のように考える。

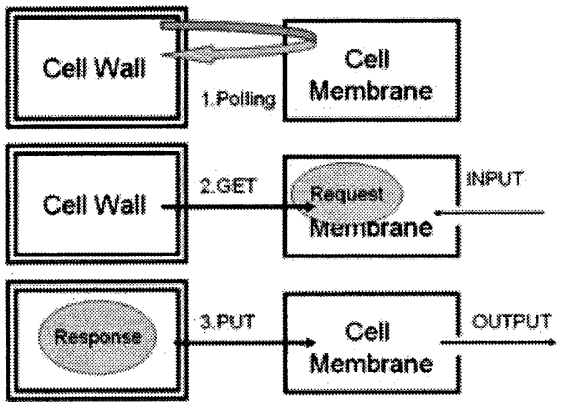

図 2: Cell Wall モデルによる Web アクセス

1.Polling では Cell Membrane サーバーにある Request を一定間隔でポーリングし確認している。2.GET では Cell Membrane サーバーにある Request があった場合、それに応じた要求を 3.PUT で返している。このアクセスであれば細胞壁を固定しながらも通信することが可能となる。つまりプル型のリクエストのみで双方向通信と同様の処理が実現できることが示している。セキュリティモデルとしてのメリットは、まずモデルへのインバウンドの通信がすべて拒否されることから能動型ウィルスによる転移防止が可能となる。また、すべてアウトバウンドでの通信で行われ、同時にプロキシ経由の対応も可能なので基本的には匿名通信となる。これによりウィルスは汚染されたサーバーから次の攻撃対象を定めることができず、攻撃者は通信先を知ることが容易ではない。そしてこれらを多重化することで侵入脅威をさらに軽減できる。

このモデルとアクセス手法では対応できない点もある。まず Cell Wall モデル同士の通信はできないので Cell Membrane サーバーが必要となることである。次に提案の起点である細胞壁の信頼性と要求（図 2 の Request 部分）の改ざんである。ただし中継として一度 Web サービスでリクエストを公開するので汚染データ（例 バッファオーバーフロー、クロスサイトスクリプティング）のチェックは通常の構成に比べて容易であると予想される。実装においては、この 2 点にのみ注意すれば良い。したがってこのモデルは現在の複雑さによる手間を大幅に軽減する可能性を秘めている。

4. 評価

このモデルを使って HTTP プロトコルで情報公開を実装した。システム構成図を図 4 に示す。モデル間通信には Web サービスを用いた。Cell Membrane サーバーとして機能させるために HTTP リクエスト公開型 Web サービスを配置する。これによりクライアントであるブラウザからの HTTP リクエストを随時公開する。Cell Wall モデルの中には Web サーバーを配置するが、そのままだとリクエストの確認ができないためローカルに Web サーバーと外部通信のポーリング機能を持つデーモンプログラムを一つ実装した。興味深いのがすべての SYN パケットを防ぐよう設定されたファイアウォール内の Web サーバーに結果的にはアクセスできている点であり、従来の方法とは別な方法により実現されたことになる。また実装面の問題としてはパフォーマンスとポーリングの頻度である。パフォーマンスはポーリングの頻度に応じて上昇するのでポーリングの頻度が多ければ定常的に帯域に負荷がかかる。また HTTP ではコンテンツのダウンロードの際にリンクが多いと明らかにパフォーマンスが落ちる。これは Cell Wall モデル内部へその都度リクエストが発生していたからである。また一部のコンテンツが表示できない場合がある。これは表示の際にクライアントに見える Cell Membrane サーバーにコンテンツが移動しているために発生している。

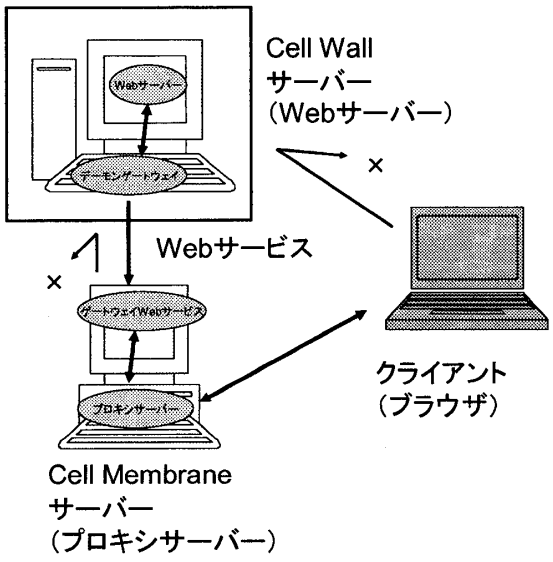

図 4: 検証システム構成図

また詳細は省くがセキュリティの評価としても、クローズドネットワークにて OS にパッチを当てずにこの構成を構築し、CodeRed、Nimda 等のウィルス、クロスサイトスクリプティング等の一般的な攻撃を行ったが、Cell Membrane サーバー、クライアントは感染しても Cell Wall モデル内のサーバーは無事であった。このことから Web サーバーの実現手法としては有効であると考えられる。

5. おわりに

細胞壁から導き出した Cell Wall モデルを提案し、免疫系としてセキュリティの向上が期待できることを示した。

一方で見方を変えればファイアウォールの内部へのアクセス手段にもなり得る。本稿では結果的にセキュリティを高めていることを実証したにすぎない。今後はこの成果の一般化してソフトとして公開する予定である。

6. 参考文献

[1] 松本邦夫，中村敏一，“21 世紀のガン治療”，“ http://www.kringle-pharma.com/”

[2] Dipankar Dasgupta, “An Artificial Immune System as a Multi-agent Decision Support System”, IEEE International Conference, San Diego, pages 3816--3820, 1998.