アタックツリーを用いた動的セキュリティレベル制御方式の研究

アタックツリーを用いた動的セキュリティレベル制御方式の研究

DYNAMIC SECURITY LEVEL ANALYSIS METHOD USING ATTACK TREE

加藤祐也
Yuya KATO
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

Most companies carry out security countermeasures against maximum-security risks based on countermeasure cost. However, maximum security is costly and low availability. Therefore, it is important to consider the optimum security level. Since the risk varies according to the external environment that changes sequentially, it is necessary to dynamically change the optimum security level. In this paper, we propose a concept for dynamically analysis the security level in cyberspace. In addition, we propose a method to dynamically change the security countermeasures by calculating risks using attack tree. Furthermore, we showed the usefulness of the proposed method.
***Key Words** : Dynamic, Risk, Security Assessment, Cyberspace*

１．はじめに

企業には顧客や従業員の個人情報，企業独自の手法やノウハウなど様々な情報が存在している．これらの情報の漏洩は企業に多大な損失を発生させるため，各企業では情報セキュリティマネジメントシステム(以降 ISMS)を導入しリスクマネジメントを行っている[1]．ISMS では一定の算出法でリスクを算出し，一般的にリスクの高い状態を想定しそれに対応する高いレベルのセキュリティ対策を実施する[2]．しかしセキュリティ対策の実施にはソフトの導入費や人件費などのコストが発生し，その値はセキュリティレベルの高さに応じて高価になる．

またセキュリティ対策はその情報資産の可用性や利便性の低下，仕事内容の複雑化や仕事効率の低下など従業員に負担を与える．さらに高すぎるセキュリティレベルの維持はセキュリティによる疲労度がたまり，逆に企業内のセキュリティ意識低下を発生させる[3]．

これらのことからセキュリティを考慮する際にはより高いセキュリティレベルの対策を行うのではなく，リスクに応じて最適なセキュリティ対策を考慮すべきである．

最適なセキュリティレベルを考慮する際，周囲に脅威が存在する場合としない場合でリスクの値は変化する．つまりもっとも最適なセキュリティ対策は逐次変化するリスクに応じてセキュリティ対策を動的に変化させることである．これにより常に脅威が存在すると仮定する場合より可用性等を向上させることが可能である．この考え方はダイナミックセキュリティと呼ばれ提案されている[4][5][6]．

ダイナミックセキュリティでは特に物理空間に存在する脅威に対して焦点を絞り，動的にセキュリティ対策を変化させる手法が多く提案されている．しかしサイバー空間に存在する脅威に対しては深く議論されていない．

そこで本論文ではサイバー空間に存在する脅威に焦点を当てた動的セキュリティレベル制御手法のコンセプトを提案する．またこのコンセプトで実現する手法としてアタックツリーを用いた動的セキュリティレベル制御方式を提案する．

２．関連研究

（１）既存のリスク分析手法

現在セキュリティ対策のために提案されている分析手法は幾つか存在する．その中の一つにアタックツリーによる脅威の分析法が存在する[7]．

この手法は攻撃を受ける対象がどのように攻撃されるのかツリー状に細分化していくことで脅威を分析する．この分析は作成したサブゴールごとに対策とコストを考えて行う対策を決定できるが時間変化で細分化しているわけではなく範囲ごとの細分化のため動的な分析には適していない．

オフィス空間において場のセキュリティを考慮したリスクアセスメントもまた同様に提案されている[8]．この

手法は物理空間とサイバー空間を合わせて一つの場として考え，そこに存在するリスクを RBS 手法によって 27 の要素に抽出し分析している．この手法ではリスクへの対策として軽減，回避，需要，転嫁をそれぞれ行っているが，これらは発生することを前提にした対策がメインであり，発生前に予防するためのセキュリティ対策について詳しく考慮されていない．

これらの既存の分析手法ではリスクが逐次に変化することが考えられていない．そのため変化するリスクを分析するためには別の方法を考える必要がある．

（２）既存の動的なサイバーセキュリティ対策

リスク分析を動的に行う手法は主流ではないが，サイバー空間でセキュリティ対策を動的に変更している手法はいくつか存在する．

認証方式の一つであるリスクベース認証はそのうちの一つである[9]．この方式は IP アドレスやブラウザ等の情報が普段と違う場合に追加の認証を行うことでセキュリティ対策を強化している．つまりブラウザ情報等をもとにリスクの値を考慮して対策を動的に変化させていると言える．

またハイブリッド・クラウド環境でセキュリティレベルを動的に変更する手法も提案されている[10][11]．この手法はデータを分散保管する際に分散するクラウドの種類や数を，データの価値に応じて動的に変更する手法である．つまりデータの価値をもとに情報漏洩時のリスクを考え，動的にセキュリティレベルを変更しているということができる．

これらの手法は特定の攻撃に対する動的な対策手法ではあるが，そのリスクの分析手法はその攻撃に特化しておりサイバー攻撃全般への応用をおこなうことはできない．

（３）物理空間での動的なセキュリティ対策

物理空間においては動的にセキュリティレベルを変更する手法が幾つか提案されている．

その一つに脅威の位置によって対策を変更する手法が存在する．この手法では情報資産からの距離によって発生する可能性のある脅威が変化することに着目し，脅威との距離によって別のセキュリティ対策を行う．このコンセプトはダイナミックセキュリティと呼ばれている．

ダイナミックセキュリティではトレードオフである情報セキュリティの 3 要素を，動的に変化させることで可用性と機密性の両立を目指している．脅威が付近に存在しない場合には可用性を上げて機密性を下げ，近づくにつれて機密性を上げていく．常に脅威の存在を検知しリスクを計算することで最適なセキュリティレベルを維持している．

ダイナミックセキュリティはサイバー攻撃にも対応できると考えられているが，実際に対応させるには脅威の検知方法などの問題があり具体的な内容を議論されていない．そのため今回はサイバー空間で動的にリスクを分析し最適なセキュリティ対策を策定する手法を提案する．

３． 提案手法

（１）ダイナミックセキュリティの 3 工程

ダイナミックセキュリティには脅威の検知，リスクの評価，セキュリティレベルの制御の 3 つの工程が必要である．その 3 つの工程をサイバー空間に当てはめた結果を図 1 として示す．

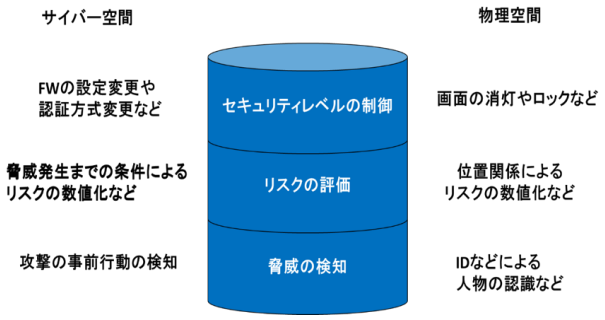

図1 サイバー空間でのダイナミックセキュリティのコンセプト

サイバー空間では攻撃の事前行動による脅威の検知，脅威発生までに必須となる条件の発生率などによるリスクの評価，動的なセキュリティ対策変更によるセキュリティレベルの制御の 3 つの工程によってダイナミックセキュリティを実現する．

（２）脅威の検知

サイバー空間において物理空間のように脅威が周囲に存在することを判断することは難しい．しかしサイバー攻撃には事前に行う行動がある場合があり，その事前行動を検知することは可能である．例えばポートスキャンは不正アクセスなどの事前行動だといえる．今回はそのことに注目し，事前行動があとどの程度残っているのかによって脅威が存在するかどうかを判断し，擬似的に脅威の検知を行う．

サイバー攻撃には突然発生するものや事前行動の検知がむずかしいものも存在する．このような攻撃は常に脅威が周囲にいることと同じであると言える．そのためセキュリティレベルは常に高く維持する必要がある．一方でまだ複数の事前行動が必要で，それらが検知されていないならリスクは限りなく低いためセキュリティレベルを下げることができる．

また脅威が周囲にいる可能性を考える際に，外部の環境は一つの指標となる．新製品の開発などを行った後にはその企業へのサイバー攻撃は増えると考えられるし，オリンピックなどのイベントを行っている場合や脆弱性が発見された場合にもサイバー攻撃が増えることがわかっている．このような直接脅威とはかかわらない要素も脅威の存在する可能性を引き上げる要因となる．

（３）リスクの評価

サイバー空間においてリスクの評価は，リスクを発生させる脅威となる行動が発生し成功する確率である．つまり，不正アクセスなどの損失が発生する行動を攻撃者がどの程度行うのか，それがどの程度成功するのかを確率的に計算する．そのため事前行動が存在する行動は，それが終わるまで行動が発生しないためリスクの値が小さくなる．

リスクの確率計算には事前行動を含めた攻撃者の行動ごとに行動発生率と行動成功率を定義する必要がある．

行動発生率とは，その行動を攻撃者が行う際の行いやすさである．その行動が法的に制限されている場合や深い専門知識が必要な場合には発生率は減少する．しかし知識がなくても行うことが可能である場合や見返りが大きい場合には行動発生率が大きくなる．

行動成功率は情報資産を持つ企業側に依存する確率であり，セキュリティ対策による防御を示している．セキュリティ対策を行っていない場合，攻撃者が行動を起こすとその行動は必ず成功するため行動成功率は 1 となる．一方で強固な対策を行っていれば行動の成功率が低下する．

この行動発生率と行動成功率，さらに事前行動が発生し成功する確率を全て掛け合わせることでその行動が実際に発生して情報を抜き取られるリスクの値を確率で表現できる．

（４）セキュリティレベルの制御

サイバー空間においてセキュリティレベルを動的に変更するには事前に複数のセキュリティ対策を用意し，どのタイミングで変更するのか考えなければならない．セキュリティレベルを上昇させるタイミングは，事前行動が起きて，リスクが増加したタイミングである．しかしそれを元に戻すタイミングは難しい．物理空間では脅威が周囲に存在する間だけセキュリティレベルを上げることができたが，サイバー空間では脅威が立ち去ることがないためそれは不可能である．そこで事前行動の結果攻撃者が得た情報を無意味なものにすることでセキュリティレベルを元に戻すタイミングを決定する．

例えばポートスキャンで開いているポートの情報を抜き取られた場合，使用しているポートを変更することでセキュリティレベルを下げる．

このことからサイバー空間のセキュリティレベルは物理空間よりも下げるタイミングがシビアであるといえる．

攻撃者が事前行動も含めて，行動によって情報を取得できる確率が上がった行動に対してセキュリティ対策は行う．つまり発生した事前行動の次に来る行動への対策を行うと上手くいく．この時の情報取得の確率はリスクの値と同じものである．

（５）ダイナミックセキュリティで対応すべき脅威

セキュリティ対策を行う場合何に対して対策するのか明確にする必要がある．関連研究のオフィス空間のリスクアセスメントでは脅威を 27 の要素に分けて対策を考えている．この中からサイバー空間に存在する脅威であるか，外部から不定期に発生する脅威であるか，動的に対策すべき脅威であるかを考慮してダイナミックセキュリティで対応すべき脅威か判断した．その結果ダイナミックセキュリティで対応すべき脅威は次の表 1 に存在する 8 つであるといえることがわかった．

表 1 サイバー空間で対応すべき脅威一覧

ウイルスの感染	情報資産やそれにアクセス可能な機器へコンピュータウイルスを感染させること
不正アクセス	許可したユーザ以外による情報資産へのアクセス
盗聴	通信路上で許可した人物以外が情報を得ること
改ざん	情報資産を不正に書き換えること
なりすまし	不正に権限を得ること
DoS 攻撃	メモリなどの負荷を上げることでサービスを停止させること
不正コピー	許可していない人物に情報をコピーされること
フィッシング	偽サイトなどへ情報を入力させること

この表 1 では直接企業に損失を発生させるような脅威のみを挙げている．そのため標的型攻撃のような，これらの脅威を発生させるためのサイバー攻撃については記載していない．

ダイナミックセキュリティを実際に行うためには，ここに挙げた脅威についてそれぞれ脅威の検知，リスクの評価を行って,セキュリティ対策を変更する必要がある．

４．アタックツリーを用いた動的セキュリティレベル制御方式

上記で述べてきたサイバー空間での動的にセキュリティレベル制御を実現するために，今回アタックツリーを用いた動的セキュリティレベル制御方式を提案する．この手法では既存のアタックツリーの作り方を変化させ，動的な脅威分析に利用できるようにして，そのアタックツリーを用いてリスクの評価を行っていく．

（１）アタックツリーを利用した脅威の検知

脅威の検知には脅威の事前行動を検知することが必要である．しかし事前行動からどの攻撃に繋がるのか瞬時に判断することはできない．そのためセキュリティ対策を行う前に脅威と事前行動の関係を分析しておく必要がある.今回は分析のためにアタックツリーを用いている．

今回作成したアタックツリーは脅威を種類で分けるのではなく，事前行動，事後行動というように時系列順に

攻撃者の行動を並べて分けていく．

基本となるアタックツリーを図 2 として示す．この図では赤い丸で攻撃者の行動を，青い四角形で攻撃に必要な情報や攻撃の結果得られる情報を示している．

図 2 を見ると攻撃者の行動の前に情報が存在している．これはその行動を行うために必要な情報を示している．また攻撃者の行動の後に情報が来ている場合はその行動

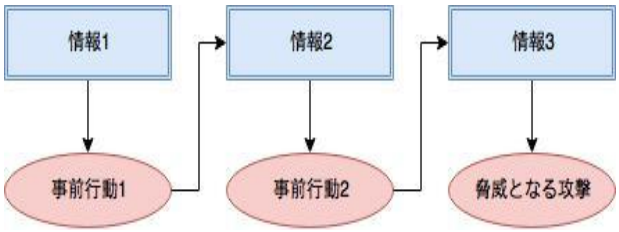

図 2 基礎となるアタックツリー

の結果得られることを示している．また攻撃や情報へ繋がる矢印が複数存在する場合には，いずれかの行動，または情報によって矢印の先の情報や行動が可能であることを示している．

さらに攻撃を行う場合に複数の行動が必須になる場合もある，そのような場合には AND 回路を使用することで問題なく対応できる．具体的な攻撃を当てはめると図 3 のようになる．

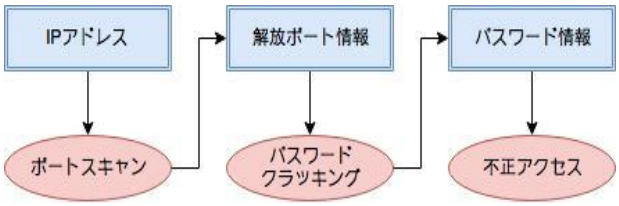

図 3 アタックツリーの使用例

このように書くことで不正アクセスの事前行動がパスワードクラッキングであり，そのパスワードクラッキングの事前行動にポートスキャンが存在することが一目瞭然である．

実際の事前行動の検知にはいくつか方法が存在するが，効果的なものとしては，既存のセキュリティソフトや FW，IDS，IPS による検知，またそれらやサーバのログ分析が考えられる．ネットワーク上の行動は発生前に検知することは難しいが発生後にはログを残すことが多いため行動の検知は可能である．

（2）アタックツリーによるリスクの評価

上記で脅威の事前行動にどのようなものが存在するのか判断できるようになった．ではこの時のリスクの値を求める．前述の通りリスクの値を求める前に行動ごとに行動発生率と行動成功率を設定する必要がある．

例えば図 2 の例の場合どのようにリスクを求めるのか図 4 を用いて説明する．

	事前行動1	事前行動2	攻撃
行動発生率	a	b	c
行動成功率	A	B	C
情報取得率 ＝リスクの値	A’=A × a	B’=B × b × A’	C’=C × c × B’

図 4 リスク計算の例

この図 4 では行動ごとの行動発生率と行動成功率からそれぞれの情報取得率を求める方法を示している．この図 4 の A’の値はすなわち図 2 でいう情報 2 が攻撃者に盗まれる可能性を示している．事前行動 2 の B’も同様に情報 3 を得る確率である．

もしも事前行動が並列に存在する場合，つまり攻撃に必要な情報を得る手段である事前行動が，複数存在する場合，それらの中で最も情報取得率が高いものが情報を得る確率となる．その値を攻撃行動の発生率，成功率と掛け合わせる．その他の計算結果は必要ない．

AND 条件が存在する場合，例えば図 2 の情報 2 と情報 3 の両方が脅威の事前行動となる場合には，図 4 の事前行動 2 に対して A’を掛け算しない．その代わりに攻撃に B’だけではなく A’も掛け算して計算する．

（3）事前行動発生時のリスク変化

リスクの値の計算法を今まで示したが実際に事前行動を検知した場合にどのように変化するのかを図 5 として示す．

	事前行動1	事前行動2	攻撃
行動発生率	a -> 1	b	c
行動成功率	A -> 1	B	C
情報取得率 ＝リスクの値	A’ = A × a = 1	B’=B × b × A’	C’=C × c × B’

図 5 事前行動 1 検知時のリスクの値

この図 5 は今までの図 4 の状態から事前行動 1 を検知した場合のリスクの値の変化を示している．もうすでに検知した事前行動は情報を取得されたと考えるため A’の値が 1 に変化する．確率が 1 になることから A’を今まで掛けていた B’やその先の C’のリスクの値が上昇する．

このようにリスクの値が変化したため動的にセキュリティ対策を変更する．

（4）セキュリティ対策の動的な変更

上記でリスクの値が上昇することは示した．この時ある一定のボーダーを考えておき，リスクの値がそれを上回った場合に対策を変更する．

セキュリティ対策を強化した場合には，その行動の行

動成功率が減少する．それによってリスクの値を減少させることで，安全な状態を維持する．

変更するセキュリティ対策は発生した行動以降のものであり，かつリスクの値の変化したものとなる．ここでは事前行動 2 と攻撃の 2 つとも当てはまる．どちらの行動の対策を行っても脅威のリスクの値を減少させることができるため，変更した場合の利用者の可用性の低下が少ない方の対策を選択する．しかしこれは複数の脅威を総合して考えた場合例外も存在する．

セキュリティレベルを低下させるには一旦情報のリセットを行う必要がある．この場合利用者への通知などが必要となることから簡単には戻すことはできない．しかし常にその対策を行っている場合に比べて可用性が向上していることは間違いない．

５．具体的な例

ここでは不正アクセスを脅威として想定した場合を例に何が発生したらどのように変化させるのか，実際にセキュリティ対策が動的に変化可能なのかを述べる．

今回の想定する情報資産は外部からの入力が発生しないシンプルな Web サーバである．また今のところ外部環境は至って平穏であり，周辺の機器や物理空間から権限情報が漏れることはないとしておく．

（１）不正アクセスに関わるアタックツリーの作成

不正アクセスに関わるアタックツリーから今回のサーバに関わりのある部分を抜粋したものを図 6 として示す．

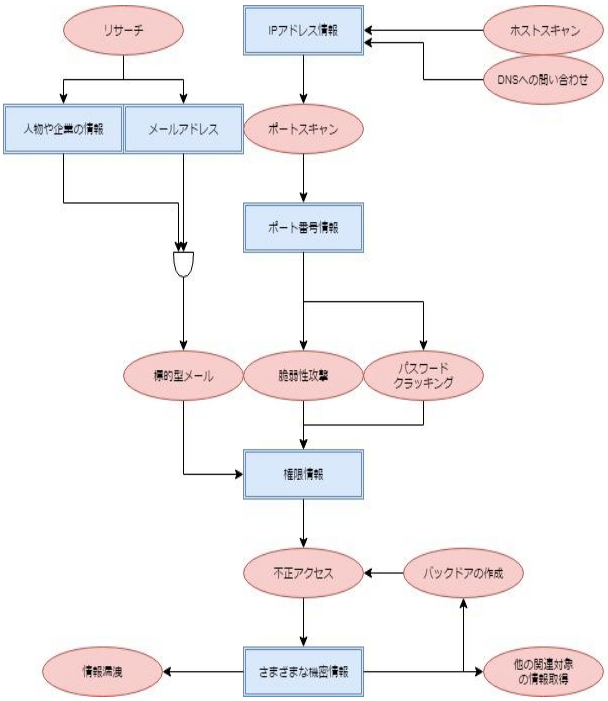

図 6 調整したアタックツリー

この図 6 において標的型メールとはサーバの管理者を対象とした攻撃を想定している．また今回は不正アクセスを防ぐことを目的としているため不正アクセス以降の行動は大きく分類している．さらにバックドアはセキュリティ対策を低く戻す場合に必要な要素であることから不正アクセスの対策を変更するまで考慮しない．

（２）リスク計算に必要な要素の定義

リスクの計算には行動発生率と行動成功率が必要である．行動発生率は企業ごとに異なるため，過去のデータから決定する．今回は過去のデータが存在しないため，行動の行いやすさを 4 段階に分けて設定している．情報系の知識が無くても誰でもすぐ行える行動は 1，ソフト等の利用をすれば誰でもできる行動はや行っても問題にならないものは 0.8, 大学で学ぶレベルの情報系の知識が必要な行動や行うと問題になる行動は 0.5, 情報系の中でも高度なハッキング知識が必要である場合や行うと大きな問題となる行動は 0.3 として定めた．

今回はリスクの値をどの程度まで許容するのかのボーダーを 40%と設定し，この値を超えた場合セキュリティ対策を行う．この値は企業やその情報資産の価値によって変わるため一概に一定の値を決めることはできない．

（３）セキュリティ対策の策定

不正アクセスの事前行動が起こる前の段階でのセキュリティ対策は以下のように設定する．

セキュリティ対策が難しいものや効果が薄いもの，重要度が低い行動には対策を行わない．具体的にはリサーチ，ホストスキャン，DNS への問い合わせの行動は対策を行わない．

事前行動が判断できないが重要度の高い行動は常に一定の対策を行う．具体的にはポートスキャンと標的型メールである．ポートスキャンの対策としては ICMP パケットの遮断，標的型メールの対策としてはサーバログイン用 PC でのメールアクセス禁止を行う．

事前行動が検知可能であり複数のセキュリティ対策が考えられる行動は，複数のセキュリティ対策を想定する．具体的にはパスワードクラッキング，脆弱性攻撃，不正アクセスが該当する．パスワードクラッキングの対策はセキュリティレベルが低い対策として同一 IP からの ssh 失敗が 100 回続いた場合の同日の接続禁止，高いレベルの対策として同一 IP からの失敗が 3 回続いたら同日の接続禁止とする．脆弱性攻撃の対策としては，低いレベルの対策として一日ごとのソフトアップデート確認，高いレベルの対策として確認の頻度を増やし脆弱性がふさがるまで利用を停止する．不正アクセスの対策は低いレベルの対策として telnet の禁止と ssh ポートの変更を行う．高いレベルの対策としてはサーバ内部で別の認証を追加で行う．

このようにセキュリティ対策を想定した上で，事前行動がなにも発生していない場合には一番セキュリティレベルの低い対策を行っておく．

（４）事前行動発生前のリスク

事前行動が起きていない段階でリスクの値がどのようになっているのか図 7 として示す．

	リサーチ	ホストスキャン	DNSへの問い合わせ	ポートスキャン
行動発生率	1	0.8	1	0.8
行動成功率	1	1	1	0.4
リスクの値	1	0.8	1	0.32×1 =0.32
	標的型メール	脆弱性攻撃	パスワードクラッキング	不正アクセス
行動発生率	1	0.3	0.8	0.5
行動成功率	0.1	0.1	0.8	0.8
リスクの値	0.1×1 =0.1	0.03×0.32 =0.01	0.64×0.32 =0.20	0.4×0.20 =0.08

図 7 事前行動発生前のリスク

この段階ではリスクが 40%を超えているものは存在しないためセキュリティ対策は変更しない．現在不正アクセスまでの経路で確率が最も高いものはパスワードクラッキングである．

（５）事前行動発生後のリスクと最適な対策の選定

事前行動としてポートスキャンを検知した場合のリスクを図 8 として示す．

	リサーチ	ホストスキャン	DNSへの問い合わせ	ポートスキャン
行動発生率	1	0.8	1	0.8
行動成功率	1	1	1	0.4
リスクの値	1	0.8	1	1
	標的型メール	脆弱性攻撃	パスワードクラッキング	不正アクセス
行動発生率	1	0.3	0.8	0.5
行動成功率	0.1	0.1	0.8	0.8
リスクの値	0.1×1 =0.1	0.03×1 =0.03	0.64×1 =0.64	0.4×0.64 =0.26

図 8 ポートスキャン発生時のリスク

この図 8 を見るとパスワードクラッキングの確率が 64%となり 40%を大きく超えている．そのためパスワードクラッキングの対策を先程決めた高いレベルの対策に変更する．

事前行動として標的型メールを検知した場合のリスクを図 9 として示す．

	リサーチ	ホストスキャン	DNSへの問い合わせ	ポートスキャン
行動発生率	1	0.8	1	0.8
行動成功率	1	1	1	0.4
リスクの値	1	0.8	1	0.32×1 =0.32
	標的型メール	脆弱性攻撃	パスワードクラッキング	不正アクセス
行動発生率	1	0.3	0.8	0.5
行動成功率	0.1	0.1	0.8	0.8
リスクの値	1	0.03×0.32 =0.01	0.64×0.32 =0.20	0.4×1 =0.4

図 9 標的型メール発生時のリスク

図 9 では不正アクセスのリスクが 40%以上となっている．このため不正アクセスのセキュリティ対策を高いレベルの二段階認証に変更する．

最後に使用しているソフトに脆弱性が存在した場合について考える．その時のリスクを図 10 として示す．

	リサーチ	ホストスキャン	DNSへの問い合わせ	ポートスキャン
行動発生率	1	0.8	1	0.8
行動成功率	1	1	1	0.4
リスクの値	1	0.8	1	0.32×1 =0.32
	標的型メール	脆弱性攻撃	パスワードクラッキング	不正アクセス
行動発生率	1	0.8	0.8	0.5
行動成功率	0.1	1	0.8	0.8
リスクの値	0.1×1 =0.1	0.8×0.32 =0.26	0.64×0.32 =0.20	0.4×0.26 =0.10

図 10 脆弱性発見時のリスク

図 10 の場合リスクが 40%を超えているものは存在しないため対策は変更しない．

今回は脆弱性が発見されたことにより，その攻撃を試す人が増えると考えられる．そのことから行動発生率が上昇している．また脆弱性が対応されるまでは行動成功率が 100%となると言える．なおこの行動成功率は脆弱性対応されたバージョンにアップデートした段階でもとに戻ると考えられる．

６．考察

今回不正アクセスを対象に３つの事前行動を検知した場合にセキュリティ対策がどう変化するのか具体的に数値計算を行った．その結果検知した事前行動によって違ったセキュリティ対策を行った．これは動的に最適なセキュリティ対策を選ぶことができているといえる．そして常にセキュリティレベルが高い対策を行うよりもシステムの可用性，利便性が上昇していることは明らかである．これは不正アクセスだけで考えても，認証回数が２倍になることから判断できる．

しかし今回は脆弱性発見などの外部環境の変化を具体的に計算で判断せず，管理者の主観で判断した．そのため完全自動化で動的にセキュリティ対策を変更するようなことは未だできないだろう．

また今回は一つの脅威について様々な事前行動を想定したが，他の脅威と複合して発生した場合の最適な対策がどのようになるのか，ネットワーク単位で管理する場合に複数の情報資産を共通で守るためにはどうするのかなどが検証不足である．これらを検証することによってネットワーク単位などで最適な対策を導き出すことができるようになるだろう．

７．結論

本論文では，今まで物理空間しか考慮されていなかったダイナミックセキュリティの考え方をもとに，サイバー空間において動的にセキュリティレベルを変更する新しいダイナミックセキュリティのコンセプトを提案した．また具体的にサイバー空間で動的にセキュリティレベルを変更する手法としてアタックツリーを利用してリスクを計算し，セキュリティ対策を行う手法を提案した．この手法を使うことで今まで問題であったセキュリティレベル固定化による可用性や利便性，パフォーマンスの低下などを多少なりとも改善できるであろう.しかし可用性などを数値的に表現することが困難なことからどの程度の効果が発揮されるのか判断が難しいという問題も未だ残っている．

今後この手法を改善するためには，複数の情報資産が存在する場合，複数の脅威が存在する場合，ネットワーク単位での対策を行う場合などの状況で効率的なセキュリティ対策選択を行う方法を考えていく必要がある．

また，動的なセキュリティという分野全体において，可用性の存在は大きなポイントとなる．この可用性の数値化は必ず考えなければならないだろう．

謝辞：本研究を進めるにあたり，ご指導頂いた指導教員の金井敦教授に感謝致します．また，日常生活で私の研究を行うモチベーションを維持してくれた情報ネットワーク・セキュリティ研究室のメンバーに感謝します．

参考文献

1) "情報マネジメントシステム認定センター," 一般財団法人日本情報経済社会推進協会, [Online]. Available: https://isms.jp/isms.html. [Accessed 5 2 2018].
2) NTT コミュニケーションズ, 新・情報セキュリティ対策ガイドブック―.com Security Master, NTT コミュニケーションズ, 2004.
3) K. N. K. H. T. H. Y. S. A. K. Shigeaki Tanimoto, "A Concept Proposal on Modeling of Security Fatigue Level," IEICE Technical Report.
4) 本間博礼, "人物フォーメーションを考慮した危険度定量化手法," 2014年度暗号と情報セキュリティシンポジウム, 2014.
5) 牧. 谷. 佐. 金. 米田翔一, "動的リスク評価に基づくセキュリティ場モデルの提案," プロジェクトマネジメント学会 2013 年度春季研究発表大会, 2013.
6) 榎本真也, "ダイナミックに制御する情報漏洩対策システムの検討," 第 11 回情報科学技術フォーラム(FIT2012)講演論文集, 2012.
7) B. Schneier, "Attack Trees," Dr. Dobb's Jounal, 1999.
8) 谷. 佐. 金. 米田翔一, "オフィス空間における場のセキュリティを考慮したリスクアセスメント," 第 13 回情報科学技術フォーラム(FIT2014), 2014.
9) A. O. N. B. Lior Golan, "System and method for risk based authentication". Patent US20050097320A1, 5 5 2005.
10) 金. 谷. 佐. 梶浦悠生, "ハイブリッド・クラウドにおける動的セキュリティ制御基盤法式," IEICE Technical Report, 2014.
11) S. U. A. K. S. T. H. S. Yuuki Kajiura, "An Approach to Selecting Cloud Services for Data Storage in Heterogneous-multicloud Environment with High Availability and Confidentiality," IEEE Twelfth International Symposium on Autonomous Decentralized Systems, 2015.