Vol.2015-CSEC-71 No.2
2015/12/4

多層防御モデルの実装における攻撃者行動の考慮について

星　智恵[†1]　　内田勝也[†2]

概要：サイバー攻撃への防御策として多層防御の有効性について取り上げられることが増えてきているが、セキュリティ対策機器の導入による境界型の防御策にとどまっているケースがある。多層防御を実現するには、攻撃者の最終目的を実行させないことが肝要である。本稿では攻撃者の行動を考慮した多層防御の検討について考察する。

キーワード：多層防御, スイスチーズモデル,ジャーニーマップ,

Cyber attacker’s behavior considerations for Defense in Depth implementation

TOMOE HOSHI[†1]　KATSUYA UCHIDA[†2]

Abstract: Defense in depth has become popular for cyber-attack. However, some case remain at the level of perimeter security. Defense in depth is not let you carry out the purpose of the attacker by various measures. This report introduce the consideration of defense in depth from the behavior of the attacker.

Keywords: Defense in Depth, Swiss cheese model, journey map

1. はじめに

企業や政府機関を狙ったサイバー攻撃の増える一方であり、攻撃内容についても深刻度を増している。増加するサイバー攻撃に対抗するため、数多くの組織、機関でセキュリティ対策の取組が進んでいる。

ところが、攻撃は不正アクセス、ウイルス感染、情報の改ざん、サービス不能等多岐にわたることからも、セキュリティ対策には万全は存在せず、攻撃に対する複数のセキュリティ対策の組み合わせによりリスクを低減する方法がとられることが一般的であり、このような複数対策の組み合わせは「多層防御」と呼ばれるが、多層防御の「層（レイヤー）」の基本的な考え方に対する誤解や､防御策が技術･機能中心に採用される等のセキュリティ設計上の課題がある。

そこで本稿では、多層防御の基本的な考え方を整理したうえで、攻撃者行動から層となる行動を洗い出し機器に加えて運用を考慮する防御策設計のフレームワークについて考察する｡攻撃者行動を意識したセキュリティ対策の企画、設計、導入、運用を行うことで、組織内のセキュリティ人材育成やインシデント対応力向上につなげることを効果として考える。

2. 多層防御のモデルと採用時の課題

2.1 多層防御の考え方

多段階対策の考え方として 2 種のモデルを紹介する。

(1) スイスチーズモデル

英国マンチェスター大学心理学教授の James Reason により提唱された組織事故発生リスクを抑制、軽減するための考え方であり、危険要因（ハザード）と事故による損害発生に至るまでの間に設計する複数の防御策をスイスチーズの穴に見立てて、穴の重なりにより事故発生の可能性がふさがれるとしている。防御策の例としては、設備、物理的バリア等のハード的防護機能だけでなく、コンプライアンスやポリシー整備等のソフト的防護機能が例示されている。

また、本モデルでは組織的な活動の中における事故発生の原因は個人のみにあるのではなく職場要因さらには、組織要因にあるとの考え方をベースとしている。

セキュリティ対策の観点からもリスク軽減の手法として有効であり、防御策に対しての継続的な監視と運用により効果が現れる。継続的な監視運用が必要である事由は事故発生のリスクに対して完全な防御策は存在せず、穴は防御策の採択後にも未知のものが生じる可能性や、一度あいた穴が前述の組織要因等により移動することもあるためである。したがってセキュリティ対策の観点では、危険とリスクを適切に評価と多層にわたる防御策の実装と事故発生時の分析による再発防止策の検討が有効である。

†1 ネットワンシステムズ（株）
NetOne Systems Co., Ltd.
†2 情報セキュリティ大学院大学
Institute of Information Security

ⓒ2015 Information Processing Society of Japan

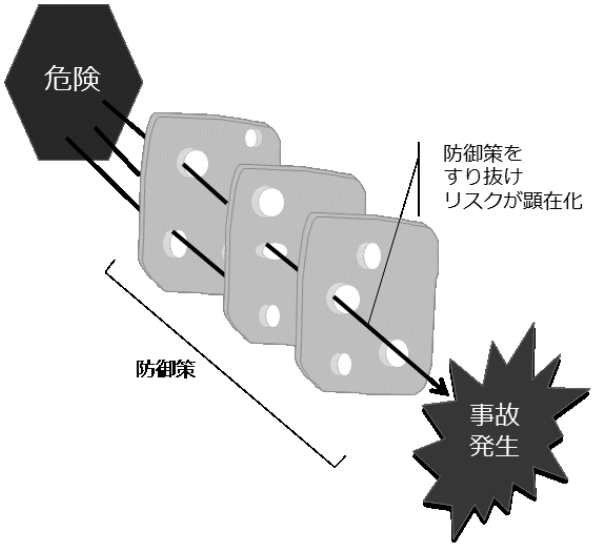

図 1　スイスチーズモデル解説図

(2) **Defense in Depth**

多層防御の英訳として使用されることの多い「Defense in Depth」は、もともとは軍事用語であり米国防省の定義によると「敵攻撃力の緩和及び積極的な弱体化、敵の初期偵察による布陣の全体像把握の阻止、並びに指揮官による我が予備兵力の戦術展開可能を意図した相互支援防御陣地の配置をいう。」(XX)とある。この配置は、中世期ヨーロッパの築城設計に利用されている。つまり何重にもわたる城壁や防御策を突破しないと城の最奥部分に到達することができないという戦略である。この戦略により城の最奥部分に到達するまでに攻撃の軍勢は疲弊し防衛側は反撃に転じることが可能となる。さらに様々な攻撃に対する防御を行うために異なる技術、戦略を採用することで防御効果をあげていく。

セキュリティ対策の観点でも複数のセキュリティ対策を組み合わせることで攻撃を無効とさせることができる。セキュリティ対策を米国安全保障局（NSA）が提唱する多層防御戦略では、対策の要素として、「人的要素」「技術要素」「運用要素」の異なる要素をあげている。

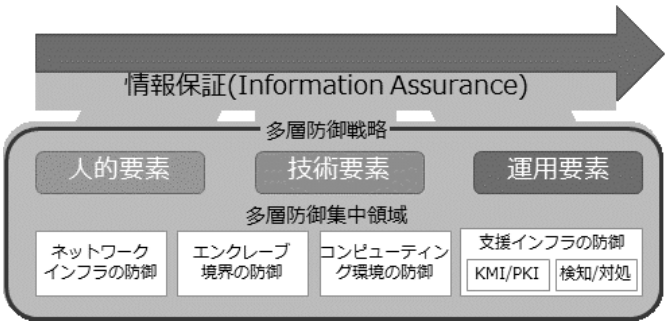

図 2　米国家安全保障局（NSA）の多層防御モデル

情報保証（Information Assurance）における多層防御では、ひと、技術及び運用の融合をコアとしており防御策の階層化によりリスク低減を実現することとしており、各要素には以下の対策が含まれる。

(1) **人的要素**

・Policies & Procedures（方針及び手順）
・Training & Awareness（訓練及び気づき）
・System Security Administration （システムセキュリティ管理）
・Physical Security（物理的セキュリティ）
・Personnel Security（人的セキュリティ）
・Facilities Countermeasures（施設セキュリティ対策）

(2) **技術要素**

・IA Architecture（情報保証アーキテクチャ）
・IA Criteria（情報保証クライテリア、）
・System Risk Assessment（システムのリスク評価）

(3) **運用要素**

・Security Policy（セキュリティポリシー）
・Certification and Accreditation（認証）
・Security Management（セキュリティ管理）
・Key Management（暗号鍵管理）
・Readiness Assessment（リリース前評価）
・ASW&R（攻撃の検知、アラートおよび対応）
・Recovery & Reconstitution（復旧。再構成）

さらに、攻撃のタイプにより１次、または２次防衛ラインでの防御策を例示しており攻撃タイプに応じて防衛策の層を計画することを表している。

表 1　多層防御の例

Class of Attack	First Line of Defense	Second Line of Defense
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

2.2 多層防御モデルのまとめ

スイスチーズモデル、Defense in Depth のいずれの考え方も攻撃タイプを意識した複数の防衛策を組み合わせた多層防御を実装することが、セキュリティ対策として有効であると示唆される。

が、セキュリティ対策の設計の段階で「層（レイヤー）」の基準については特に定めがない。これは組織によってネットワーク、システム構成や運用体制は千差万別であることから多層防御を採用する組織自身がどのような攻撃にさ

ⓒ2015 Information Processing Society of Japan

らされているのかを考慮したうえで攻撃タイプに応じた防御策を設計する必要があると考えられる。

多層防御の設計においては､組織が利用する IT サービス全般を俯瞰的に評価することが必要である。その結果としてネットワーク、サーバ、クライアントといった機器毎に対するセキュリティ対策を組み合わせた場合、同様の機能を持つ製品の購入や導入後運用が煩雑になるといった課題を解決することにつながるためである。

3. 攻撃者行動に基づく多層防御の提案

3.1 攻撃者行動の考察による「層（レイヤー)」の検討

組織にとっての重要な資産、サービスを攻撃者から防御する、あるいは攻撃をいち早く検知するためには、攻撃者がどのようなプロセスで目的を果たそうとするかを考察することで有効な打ち手をとることができる。

(1) 標的型攻撃の出口対策

近年、攻撃手法として知られるようになった「標的型攻撃」の対策としても外部からの攻撃を入口で防ぐ入口対策としてファイアウォールや侵入検知システム(IDS)、ウイルス対策ソフトによる検知といった攻撃者が侵入した時点で対処する防御策では十分ではないとして、仮に脅威となるウイルスソフト等のマルウェアが組織内に侵入してしまったとしても、侵入したウイルスの活動を遮断、封じ込めすることで攻撃者の目的である情報の窃取を回避させるという「出口対策」の有効性が取り上げられている。出口対策は攻撃者がどのような手法と行動をとるかという観点で検討を行った事例である。

表 2 標的型攻撃の各段階の攻撃内容

段階	攻撃内容	特徴
攻撃準備段階	(1) 攻撃対象に関連のある組織への攻撃 ・メール情報の窃取など	対象組織への初期潜入を成功させるため、ソーシャルエンジニアリングのためのメール文面や送付先を収集。
初期潜入段階	(1) 各種初期攻撃 ・標的型攻撃メール添付ウイルス ・ウェブ改ざんによるダウンロードサーバ誘導 ・外部メディア(USB 等)介在ウイルスなど	入口の対策をすり抜け、システム深部に潜入。 素早く次の段階へ移行。 攻撃手法は使い捨て。
攻撃基盤構築段階	(1) バックドア(裏口)を使った攻撃基盤構築 ・ウイルスのダウンロードと動作指示 ・ウイルスの拡張機能追加 ・システム内部への攻撃基盤構築	構築した攻撃基盤は発見されない。 構築した攻撃基盤は再利用される。
システム調査段階	(1) 組織のシステムにおける情報の取得 (2) 情報の存在箇所特定	時間をかけて何度もしつこく行う。
攻撃最終目的の遂行段階	(1) 組織の重要情報の窃取 (2) 組織情報（アカウント等）を基に、目標を再設定	何度も攻撃を行うため情報窃取。 組織への影響を与える情報窃取。

(2) ジャーニーマップの活用

マーケティングの領域でも、購買や選択といった活動に対して顧客行動を時系列にマップし行動内容を分析することで、顧客ニーズを分析する手法があり、設定したペルソナが､「カスタマージャーニーマップ」と呼ばれる。例えば「海外旅行をする」という顧客の目的に対して、ステージを分割し、それぞれのステージで実行される顧客行動の整理と関心や意識を明確にし、マーケティング担当者は提供サービスや機能を企画、デザインしていく。

表 3 海外旅行を目的とした行動リスト

ペルソナ	郊外分譲マンションに居住する家族 子供２人（10 歳、8 歳）
ステージ	顧客行動
計画前	家族会議 カレンダーチェック ママ友情報交換 前回の写真閲覧 メルマガ
計画･情報収集	レビューや写真チェック 店舗でハナシを聞く 空き状況をチェック 逐次相談 カタログ集め 旅行ムック購入 経験者に電話で質問
予約	予約商品の確認 旅程の確認 変更・キャンセル条件確認 出発までの ToDo 確認 支払方法選択 予約完了確認 電話予約 店舗予約
準備・出発・移動中	おしゃべり ネットで現地情報収集 宿泊先、渡航先の新しいレビューチェック
旅行中・観光・宿泊先	写真撮影、共有 現地旅行会社訪問 コメント投稿、共有 観光地、便利情報をアプリで取得、利用
旅行後	商品レビュー、振り返り Photobook アンケート お土産渡し おしゃべり コメント投稿、共有 SNS 写真投稿

カスタマージャーニーマップは顧客の視点から顧客が目的を果たすまでの全容を概観することで、行動への影響を与える要因を明らかにするという効果がある。例えば、

各ステージでの関心事は何か、どのようなタッチポイント（接点）が存在するのか。といった状況に対して提供者側に期待する行動は何かといった点について打ち手を打つのである。

顧客と攻撃者では立場は大きく異なるが、攻撃者が目的を果たすためにどのような行動をとるのかを理解することで、ステージを「層（レイヤー）」として見立てることが可能となり攻撃者の行動における関心事や成果を妨げるための打ち手を打つという方策がとれる。

3.2 攻撃行動とリスク管理行動

攻撃行動に対して防御する側は攻撃行動に対してとりうるリスク管理策の検討と検討結果の可視化を行うことがリスク対応状況の可視化とインシデント発生時の初動対応と早期復旧に効果的である。

(1) サイバーセキュリティリスク管理機能

サイバーセキュリティリスクを低減するための防御策の特定と優先順位づけの考慮で用いられる機能として米国国立標準技術研究所（National Institute of Standards and Technology）が策定したサイバーセキュリティフレームワークで採用されているフレームワークコアを紹介する。

表 4　サイバーセキュリティフレームワークコアの定義

リスク管理機能	定義
特定	システム、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深める。
防御	重要インフラサービスの提供を確実にするための適切な保護対策を検討し、実施する。
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し、実施する。
対応	検知されたサイバーセキュリティイベントに対処するための適切な対策を検討し、実施する。
復旧	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを復旧するための適切な対策を検討し、実施する。

3.3 有効性の検討

以上の考察の有効性を検証するため、攻撃者行動の洗い出しと、洗い出した行動のマップ化と攻撃対象とするリソースを書き出した。

(1) 標的型攻撃の行動マップの作成

標的型攻撃をしかける攻撃者の行動を時系列で整理した。侵入行動についてはメールに添付されたマルウェア感染を発端とする情報収集とバックドア作成による情報の窃取というシナリオを想定した。

・攻撃者の目的

特定の企業に対して、その企業が保有する重要情報を窃取し闇で販売したい。

・攻撃者の行動

① 偵察
② 侵入（外部セグメント）
③ 侵入（内部セグメント）
④ 侵入（機密セグメント）
⑤ 感染/潜伏
⑥ 情報の窃取

既述の通り、多層防御戦略としては、人、技術、運用の三要素を考慮する必要があるが、NSA の定義における人的要素では組織体制や人材スキル等の攻撃行動の影響が少ない項目であるため、技術要素、および運用要素の２種に着目することとした。

運用のフィールドを明記しておくことにより防御策検討においいて技術、製品機能だけでなく運用において必要なアクションを明確にした。

表 5　攻撃者行動マップサンプル

攻撃者の目的（特定の企業に対して、その企業が保有する重要情報を窃取し闇で販売したい。）		偵察	
情報漏えい	攻撃名称、脅威と脆弱性（メールによるマルウェア配布を行う標的型攻撃）	ターゲットとなる組織の情報を収集する	
	攻撃対象となる IT リソース	外部公開情報 日常やりとりされるメール通信	
サイバーセキュリティリスク管理機能		製品/技術・サービス	
		技術	運用
特定	リスクアセスメント	N/A	N/A
防御	アクセス制御 境界セキュリティ データセキュリティ 保護技術	N/A	N/A
検知	異常・イベント監視 高度なモニタリング	N/A	N/A
対応	分析 対応計画	N/A	N/A
復旧	復旧計画・改善（再発防止）	N/A	N/A

(2) システム脆弱性を狙う直接攻撃の行動マップの作成

同様にシステム、ネットワークやウェブアプリケーションの脆弱性を悪用した直接的な攻撃のシナリオに沿って行動マップと対策の検討を行った。

その結果、標的型攻撃では有効な対策を検討することができなかった「偵察」のステージに対してもネットワークセキュリティ対策としてポートスキャン対策やファイアウォールログの検知等のリスク管理機能が列記される結果となった。

(3) 検討結果からの考察

本結果を元に企業のセキュリティ推進組織のメンバと自社におけるセキュリティ対策の評価についてのディスカッションを行った。1

1 インタビューを行ったのは、流通系情報子会社の情報セキュリティ推進組織の担当者　3 名

ⓒ2015 Information Processing Society of Japan

その結果、フレームワークとしての評価について以下のような意見が寄せられた。

- 侵入されても被害を出さないようにするためには攻撃対象に対して複数防御策が有効だが、ログ分析のように共通である技術要素がある。
- 第１次防衛ラインであるファイアウォールは相変わらず重要な位置づけで直接の攻撃を受けた際に消耗させることが防御策として有効ではないか。
- 米国企業でハッカーが採用される意味がわかった。
- 特定の攻撃に対して、どこまでの対応ができているのかを段階で確認し、上位層に説明することができるのは良い。
- イベント監視やログ分析のシナリオとして攻撃者行動をとりいれた分析について見直しをしたい。

また、課題意見としてはアクション項目の詳細度合に関する意見が多くかわされた。

- 運用に関するアクションはあまり詳細でないのでもう少し具体的な項目に紐づける必要がある。
- 認証については特権管理やユーザアカウント管理といった運用によるアクションがあるので細分化した方が良い。

また、標的型攻撃についての攻撃者行動のディスカッション中、当初偵察行動についての対策を「N/A」としたところ、「グループ企業からの不審メールに対する照会、情報収集等の活動を行っていることは攻撃者の偵察行動を妨げるアクションにならないか」といった質問が上がるなど、現状のセキュリティ対策に対して攻撃者の行動を理解するといった視点での意見があがった。

以上のディスカッション結果から攻撃者の行動を軸とした多層防御のフレームワークはセキュリティ対策の設計に際して有効であると考える。

4. まとめ

本稿では、多層防御を企業が実装する際に攻撃者行動を中心として防御策を検討する施策についての考察を行った。多層防御については、従来型の堅牢な（同種の）境界（セキュリティ機器）を幾重にも張り巡らせる境界型防御との区別が曖昧にとられることがあるが、新たな攻撃手法や人為的なミス等によるインシデントに対する段階的な防御策を実装するには、技術だけでなくセキュリティ運用と継続的なマネジメントが必須である。

防御策を検討する際に、相手である攻撃者も人であり、ねらいがあって攻撃をしてくるのだということを意識しながら防御策を設計、導入することは、インシデント発生の検知、証跡管理や初動対応といった諸々のセキュリティ運用活動につながることが期待される。

一方で、運用要素に対するアクション項目は、より具体的なプラクティスを指定する必要があると考えられるため、ISO/27000 シリーズや PCI DSS といったセキュリティ基準を参考に関連付けについての検討を進めていきたい。

参考文献

1) 菊池 浩, スイスチーズモデルと情報セキュリティ,防衛調達研究, 第三巻 第二号,(2009)
2) 菊池 浩, 情報セキュリティにおける多層防衛戦略について, 防衛調達研究, 第一巻 第二号,(2007)
3) 独立行政法人情報処理推進機構セキュリティセンター,「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂 2 版, p.15-16,
https://www.ipa.go.jp/files/000017308.pdf
4) 米国安全保障局(NSA),Defense in Depth
https://www.nsa.gov/ia/_files/support/defenseindepth.pdf
5) 米国国立標準技術研究所（NIST）,重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0 版,(2014) ,
https://www.ipa.go.jp/files/000038957.pdf
6) カスタマージャーニーとは？
http://ecbible.net/contents-marketing/customer-journey 2015 年 11 月 9 日アクセス
7) マーク・スティックドーン, ヤコブ・シュナイダー, THIS IS SERVICE DESIGN THINKING., ビー・エヌ・エヌ新社,（2013）

ⓒ2015 Information Processing Society of Japan

付録　A.1 検討結果からの考察で使用した攻撃者行動マップ

攻撃者の目的（特定の企業に対して、その企業が保有する重要情報を窃取し闇で販売したい。）		偵察		侵入（外部セグメント）		侵入（内部セグメント） 境界型防衛ライン	
情報漏えい	攻撃名称、脅威と脆弱性（メールによるマルウェア配布を行う標的型攻撃）	ターゲットとなる組織の情報を収集する		個人宛メール中に不正サイトへのアクセスを誘導するURLやウイルス添付		メールを受領した個人がウイルスに感染し重要情報、および格納場所を収集	
	攻撃対象となるITリソース	外部公開情報 日常やりとりされるメール通信		個人宛メール		業務用サーバ ファイルサーバ USBデバイス	
サイバーセキュリティリスク管理機能		主な製品/技術・サービス 技術	運用	主な製品/技術・サービス 技術	運用	主な製品/技術・サービス 技術	運用
特定	リスクアセスメント	N/A	N/A	脆弱性検査	標準 ガイドライン	脆弱性検査	標準 ガイドライン
防御	アクセス制御 境界セキュリティ データセキュリティ 保護技術	N/A	N/A	ファイアウォール Ｗｅｂセキュリティ メールフィルタリング アンチウイルス	ネットワーク接続ポリシー セキュリティ監査	認証技術 統合ID管理 DBセキュリティ	ネットワーク接続ポリシー セキュリティ監査
検知	異常・イベント監視 高度なモニタリング	N/A	N/A	ログ管理・分析 Webセキュリティ ファイアウォール IDS	CSIRT/SOC	ログ管理・分析 ファイアウォール アンチウイルス	CSIRT/SOC
対応	分析 対応計画	N/A	N/A	電子証明書	運用手順	被害セグメント分離	運用手順
復旧	復旧計画・改善（再発防止）	N/A	N/A	N/A	N/A	N/A	CSIRT（対応組織）

攻撃者の目的（特定の企業に対して、その企業が保有する重要情報を窃取し闇で販売したい。）		侵入（機密セグメント） 境界型防衛ライン		感染/潜伏		攻撃者目的の実行	
情報漏えい	攻撃名称、脅威と脆弱性（メールによるマルウェア配布を行う標的型攻撃）	メールを受領した個人がウイルスに感染し重要情報、および格納場所を収集		バックドア、ボットを仕掛ける		情報を盗み出す	
	攻撃対象となるITリソース	データベース ファイルサーバ		業務利用PC スマートデバイス 各種サーバ		データベース 重要データ	
サイバーセキュリティリスク管理機能		主な製品/技術・サービス 技術	運用	主な製品/技術・サービス 技術	運用	主な製品/技術・サービス 技術	運用
特定	リスクアセスメント	脆弱性検査	標準 ガイドライン	N/A	標準 ガイドライン	N/A	標準 ガイドライン
防御	アクセス制御 境界セキュリティ データセキュリティ 保護技術	認証技術 統合ID管理 DBセキュリティ	ネットワーク接続ポリシー セキュリティ監査	アンチウイルス デバイス・端末管理	ウイルス対策ポリシー セキュリティ監査	データ暗号化	セキュリティ監査
検知	異常・イベント監視 高度なモニタリング	ログ管理・分析 ファイアウォール アンチウイルス	CSIRT/SOC	アンチウイルス （ログ分析） デバイス・端末管理	CSIRT/SOC	DLP エンドポイント （ログ分析） 通信監視	CSIRT/SOC
対応	分析 対応計画	被害セグメント分離	運用手順	サンドボックス 被害セグメント分離	運用手順	フォレンジック	運用手順
復旧	復旧計画・改善（再発防止）	N/A	CSIRT（対応組織）	N/A	CSIRT（対応組織）	N/A	CSIRT（対応組織）

ⓒ2015 Information Processing Society of Japan