日本年金機構サイバー攻撃事案における サイバーキルチェーン分析

森 滋男[†1]　天野 純一郎[†1]　岡田 周平[†1]　桑田 雅彦[†1]
大坪 雄平[†1]　水越 一郎[†1]　後藤 厚宏[†1]

概要：2015 年に発生した日本年金機構のサイバー攻撃事案をサイバーキルチェーン（Cyber Kill Chain）にしたがって分析を行ったので紹介する．サイバーキルチェーンは，標的型攻撃に対して，インテリジェンス主導のコンピュータ・ネットワーク防御を行うためのツールである．本分析によって，同手法を用いることにより，様々なサイバー事案を標準的手法で分析するとともに，国内はもとより国際的なインテリジェンス共有を容易ならしめる可能性のあることが分かった．本稿では，また，標的型攻撃以外のサイバー攻撃や，サイバー犯罪，サイバー不正に対する新たなキルチェーンの策定についても論じる．

キーワード：キルチェーン，インテリジェンス

Analysis on Cyber Incident of Japan Pension Service based on Cyber Kill Chain

Shigeo Mori[†1]　Junichiro Amano[†1]　Shuhei Okada[†1]　Masahiko Kuwata[†1]
Yuhei Otsubo[†1]　Ichiro Mizukoshi[†1]　Atsuhiro Goto[†1]

Abstract: This paper is to introduce the analysis based on the Cyber Kill Chain about the cyber incident that the Japan Pension Service suffered in May 2015. The Cyber Kill Chain is a tool for intelligence-driven computer network defense against APTs (Advanced Persistent Threats). The analysis reveals the possibility to standardize the method of analyses of the various cyber incidents and to help sharing the intelligence domestically and internationally by using the kill chain. The paper also discusses the possibility of creating alternative kill chains for non-APT cyber attacks or even cyber crimes and cyber misconducts.

Keywords: Kill Chain, Intelligence

1. はじめに

2015 年 5 月に発生した日本年金機構に対するサイバー攻撃では，約 125 万件もの個人情報が流出するという非常に大きな被害が発生した．本事案については，本格的な原因究明のための調査が行われ，日本年金機構自身のみならず，厚生労働省，および，サイバーセキュリティ戦略本部からも報告書が公表された [1][2][3].

国が管理する重要な業務における事案であり，国民に対しての説明責任を果たし，国民の信頼を回復するために，このように手厚い報告を行ったものと思われる．これら報告書は，多くの企業や組織で教訓として（自社／自組織は大丈夫か）活用されるであろう．また，万一，今後同様なインシデントが発生した場合には，本事案にならった報告書が作成されるかもしれない．そのような二次利用や，そもそもの事案に対する理解を促進するためには，標準に準拠して分析しておくと良いのではないだろうか.

また，説明責任を果たし，信頼を回復すべき相手は国内だけではない．インターネットは世界がつながった空間である．インターネット上で活動し，利便性を享受し，利益を得ていくためには，世界に対して説明し，世界から信頼を得なければならないと考える．したがって，国際標準に準拠することが有効である.

日本年金機構事案のような標的型攻撃を分析するにあたっての国際的な標準として，サイバーキルチェーン（Cyber Kill Chain）がある．本稿では，サイバーキルチェーンを利用しての日本年金機構事案の分析を紹介するとともに，かかる標準的分析手法の充実と活用について提案する.

2. サイバーキルチェーンとは

サイバーキルチェーンとは，米国ロッキードマーチン社が提唱しているもので，標的型攻撃における攻撃者の一連の行動を，軍事行動になぞらえて示したものである [4].

具体的には，①偵察，②武器化，③デリバリ，④エクスプロイト，⑤インストール，⑥コマンド&コントロール（C2），⑦目的実行，の 7 段階を定義しており，攻撃者はこれらの行動を鎖のように順次実行していく.

各段階の定義（拙訳）を以下に示す.

第 1 段階：偵察

攻撃目標の調査，特定，および，選定であり，メールア

†1 情報セキュリティ大学院大学
Institute of Information Security

ドレス，広報，または，特定の技術に関する情報にかかわる，議事録やメーリングリストなど，インターネット上のウエブサイトを徘徊するなどの行為である．

第 2 段階：武器化

脆弱性を悪用する遠隔操作型トロイの木馬を，配送可能な運搬手段に組み込むこと，典型的には「武器化ツール」と呼ばれる自動化ツールを使用して行う．武器の配送可能運搬手段としては，Adobe PDF や Microsoft Office 文書などの，クライアントアプリケーションのデータファイルが使用されることが増えている．

第 3 段階：デリバリ

武器を攻撃目標の環境に転送すること．ロッキードマーチン社のコンピュータ・インシデント対応チーム（LM-CIRT）による 2004 年～2010 年の観測によると，三大主要武器配送媒介物は，電子メールの添付ファイル，ウエブサイト，USB メモリである．

第 4 段階：エクスプロイト

武器が攻撃対象コンピュータに配送されたのち，脆弱性を悪用し，侵入プログラムを発動させること．多くの場合，脆弱性の悪用は，アプリケーションや OS の脆弱性を悪用するものであるが，より単純に，ユーザ自身の弱さに付け込んだり，プログラムを自動実行させるような OS の機能を濫用することもある．

第 5 段階：インストール

遠隔操作型トロイの木馬，または，バックドアを攻撃対象システムにインストールすることにより，攻撃者は当該環境の中に，永続性を確保する．

第 6 段階：コマンド&コントロール（C2）

典型的には，感染したコンピュータは，指揮命令を受ける経路を確立するために，インターネット上の指揮サーバに対して，信号通信を発信しなければならない．特に APT のマルウエアは，自動的な活動を行うよりも，手動の対話を必要とする．ひとたび指揮命令経路が確立されると，侵入者は攻撃目標の環境内において，「キーボードに手を載せているような」操作が可能となる．

第 7 段階：目的実行

6 までのフェーズを進捗して初めて，侵入者は本来の目的を達成するための活動を行うことができるようになる．典型的には，目的は情報漏えいであり，その場合は，情報の収集，暗号化，対象環境からの持ち出しを行うことになるが，データの改ざんや，データを使えなくすることが目的である場合もある．あるいは，侵入者は，他のシステムを侵害したり，ネットワーク内を横移動するための踏み台として利用したかっただけであるということもあり得る．

一方，防御者側については，攻撃者行動のそれぞれの段階に対して，i)検知，ii)拒否，iii)妨害，iv)減殺，v)欺瞞，vi)破壊の 6 種類の対応を定義している．防御者は攻撃者行動の鎖のどこか一箇所を断ち切ることで，攻撃者が最終目的を果たすのを妨げることができるわけであるが，この理論の本質は，最後の段階ではなく，極力早い段階で断ち切ることにより，攻撃者の行動の選択肢を狭め，それによって防御のチャンスを高めるという点にある．サイバー攻撃は，攻撃者が場所・時・手段を選べるので攻撃者優位とよく言われるが，キルチェーンを用いることでそれを逆転し得る可能性があるというのが，本理論の主張するところである．

すなわち，攻撃者は，前述のとおり，①～⑦の行動を順次実行しなければならない．もし，防御側の対策によっていずれかの行動が阻止されたら，その対策を迂回する方法を考えなければならない．例えば，標的型メールがブロックされて不着になったら，異なるアドレスから送信してみる．着信したけれど誰も開封してくれなかったら，もっと多数の受信者宛に送ってみる，あるいは，メールの文面を変えてみる，などである．このように攻撃者はいくつか失敗をするものであるが，それを防御者が全く気付かなかったとしたら，攻撃者は何度でも試行錯誤を繰り返すことができ，徐々に段階を進んで最終目的に辿り着くことができる．しかしながら，防御者が攻撃者の失敗を検知し，その前の段階の行動を特定し，それに対し速やかに対策を行えば，攻撃者は対策が行われた段階に戻って迂回を行わなければならなくなる．このようにして攻撃者の選択肢が狭まっていくわけである（図 1）．

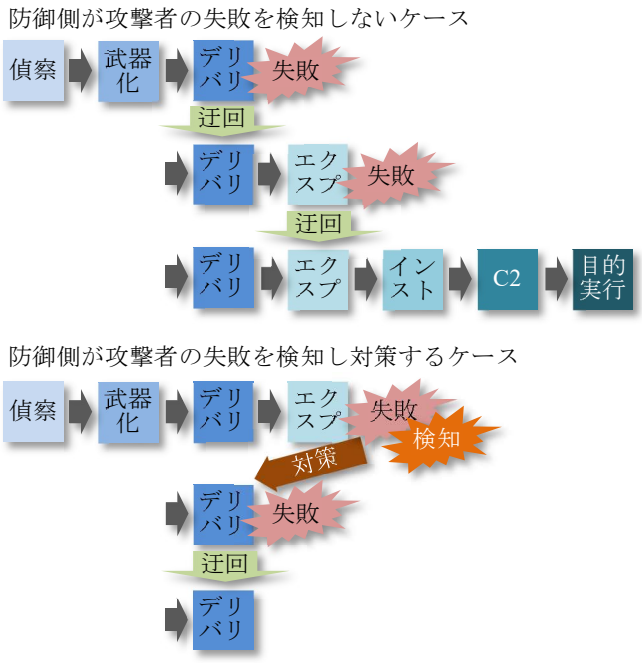

図 1　防御側の対応による攻撃者の選択肢

このような，攻撃者行動の分析に基づく防御の方法を，本理論では「Intelligence-driven Computer Network Defense（インテリジェンス主導型ネットワーク防御）」と呼んでい

る．

ただし，このような防御を行うためには，実際に観測された事象から，侵入の事実を描写し得る最小単位の情報を取り出し，集めて，分析を行う必要がある．本理論では，そのような情報を「Indicator（指標）」と呼んでいる．例えば標的型メールを受け取った場合であれば，その標的型メールの発信者，発信元アドレス，メール表題，メール本文などが，それぞれ Indicator となる．

3. 年金機構事案について

2015 年 6 月 1 日，日本年金機構は，職員の端末に対する外部からのウイルスメールによる不正アクセスによって，同機構が保有している個人情報の一部が外部に流出したことが 5 月 28 日に判明した旨，発表した．流出した情報は約 125 万件に及んだ．流出した個人情報を悪用しての不正行為が行われたとの報道はないが、年金機構を騙り「キャッシュカードのデータを元通りにする」などと言ってカードを預かり預金を不正に引き出すなど、事案に便乗した詐欺事件が発生したことが報道された．

このように国民生活に多大なる影響を与える事案が発生したことを重く受け止め，厚生労働大臣は，6 月 4 日，一連の事案についての原因究明と再発防止策を検討させるため，厚生労働省，および，日本年金機構から独立した第三者による検証委員会「日本年金機構不正アクセス事案検証委員会」を設置した．日本年金機構自身も，同機構理事長を委員長とし，役職員，および，外部委員からなる「不正アクセスによる情報流出事案に関する調査委員会」を設置した．また，サイバーセキュリティ戦略本部においても，サイバーセキュリティ基本法第 25 条第 1 項第 3 号に規定された「国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む）」に基づく報告を行うべく，内閣サイバーセキュリティセンター（NISC）と協力して作業に着手した．

かかる経緯を経て，2015 年 8 月 20 日，3 つの組織（厚生労働大臣が設置した委員会，日本年金機構自身の委員会，および，サイバーセキュリティ戦略本部）から調査報告書が公表された．サイバーセキュリティ戦略本部が，その報告書の中で「本文書には，NISC の対処能力を推知しうる情報が含まれるが，今般発生した事案の重大性に鑑み，可能な限り実態解明のための情報開示を行い，説明責任を果たす観点から取りまとめたものである」と述べるほど，詳細で力の入った報告書である．

これらの報告書から，以下の経緯が判明した．日本年金機構では，個人情報を取り扱う社会保険オンラインシステムを中心とした基幹系ネットワークと，一般的事務処理を行い，インターネットメールやインターネット Web 閲覧などの利用も可能な機構 LAN システムを中心とした情報系ネットワークが，ネットワークレベルで分離されており，両ネットワーク間をデータが行き来することはない(図 2)．サイバー攻撃を受けたのは情報系ネットワークであり，本来，基幹系ネットワークにしか存在しないはずの個人情報が，サイバー攻撃によって流出することはありえないはずであった．にもかかわらず個人情報が流出したのは，ネットワーク分離の方針にかかわらず，情報系ネットワーク上に大量の個人情報が保存されていたためである．

日本年金機構では，機構 LAN システム上での事務処理上必要な個人情報を，外部記憶媒体を介して社会保険オンラインシステムからコピーして情報系ネットワーク上に保存することが認められている．その場合，情報系ネットワーク上では個人情報に暗号化やパスワード付与などの保全措置を行い，事務処理上の必要が済んだ時には速やかに削除するよう，ルールが定められている．しかしながら，これらのルールは必ずしも遵守されておらず，保存措置のない個人情報が，必要以上に大量に，情報系ネットワーク上に存在する状態になっていた．サイバー攻撃は，これらの情報を流出させたものである．サイバー攻撃が基幹系システムに侵入したという形跡は確認されていない．本来であれば，基幹系から情報系に個人情報をコピーする必要のないよう基幹系上で業務が完結するようにシステムを構築する，あるいは，情報系ネットワーク上の個人情報がルールどおりに保全されているかどうか点検を行う，等の措置をとるべきであり，それらの対策を怠ったという点において，情報セキュリティのマネジメントに課題があったと言えよう．

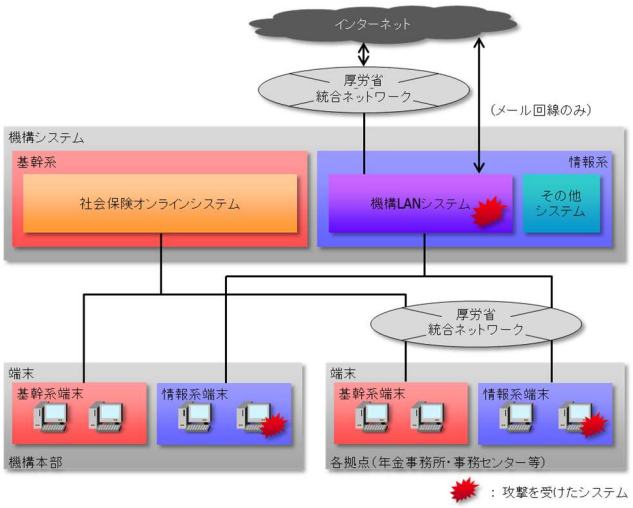

図 2　日本年金機構のシステム構成イメージ
（厚生労働省報告書を参考に作成）

このように，本事案は，サイバー攻撃によって情報が流出させられたという側面に加え，ネットワーク分離という，重要情報を漏えいさせないための抜本的な対策を導入していながら，それを生かせなかった情報セキュリティマネジメントの問題という側面を持つ事案であったが，今回は情

報セキュリティマネジメント面には目をつむり，一つのサイバー攻撃事案として分析を進める．

4. 年金機構事案のサイバーキルチェーン分析

4.1 年金機構事案の発生事象

サイバーキルチェーンを用いて分析を行うには，実際に観測された事象から，侵入の事実を描写し得る最小単位の情報，Indicator を取り出す必要がある．しかしながら，本事案については詳細な報告書が公開されているとはいえ，そこまで微細な情報が公表されているわけではない．Indicator とは，前述のとおり，例えば標的型メールを受け取った場合であれば，その標的型メールの発信者，発信元アドレス，メール表題，メール本文などである．それらのすべてが入手できているわけではないので，もう少し大きな単位，例えば，「標的型メールを受信した」というレベルの情報を使用する．この分析においては，そのような情報を「発生事象」と呼ぶことにする．

表 1 は前述の 3 報告書をもとに，発生事象を抽出し，時系列に記載したものである．

表 1　日本年金機構事案の時系列発生事象

#	発生日	発生事象
1	4 月 22 日	厚労省年金局および地方厚生局あてに標的型メール
2	↑	添付ファイルを開封
3	↑	端末感染
4	↑	C&C との通信開始
5	↑	NISC が検知，2 時間後に遮断（ただし、サブドメイン単位で URL 遮断）
6	5 月 8 日	機構の 2 公開アドレスに標的型メール
7	↑	1 名がリンク（外部のオンラインストレージサービス）をクリック
8	↑	不正プログラムがダウンロードされ端末感染
9	↑	C&C との通信を開始
10	↑	個人アドレス情報流出（報告書に明記無いが，発生したと推定される）
11	↑	NISC が検知，4 時間後に抜線
12	↑	機構 LAN でも URL ブロックを実施
13	↑	検体解析を依頼（解析結果は「特定のサイトにファイルを取得しに行くタイプのもので感染端末から情報を発信することはない」）
14	↑	当該 URL へのアクセスをモニタリング開始
15	↑	職員に注意喚起
16	↑	厚労省側でもドメイン単位で URL をブロック
17	5 月 18 日	101 名の個人アドレス宛に標的型メール
18	↑	送信アドレスを受信拒否登録
19	↑	別アドレスから 17 通の標的型メール
20	↑	3 名が添付ファイルを開封
21	↑	端末感染
22	↑	C&C との通信は URL ブロックのため失敗
23	↑	メールから検体は採取したが、感染には気付かず
24	5 月 19 日	2 名の個人アドレス宛に標的型メール
25	↑	送信アドレスを受信拒否登録
26	↑	別アドレスから 1 名の個人アドレス宛に標的型メール
27	↑	誰も開封せず
28	5 月 20 日	5 公開アドレス宛に標的型メール
29	↑	1 名が添付ファイルを開封
30	↑	端末感染

表 2　サイバーキルチェーン分類結果

#	攻撃者	防御者						
	段階	段階	検知	拒否	妨害	滅殺	欺瞞	破壊
1	3							
2	4							
3	5							
4	6							
5		6	✔	✔				
6	3							
7	4							
8	5							
9	6							
10	7							
11		6			✔			
12		6		✔				
13								
14		6	✔					
15		4				✔		
16		4		✔				
17	3							
18		3		✔				
19	3							
20	4							
21	5							
22		6		✔				
23								
24	3							
25		3		✔				
26	3							
27								
28	3							
29	4							
30	5							

31	↑	C&C との通信開始
32	↑	ディレクトリサーバの管理者権限奪取
33	↑	他の 26 台の端末に感染拡大
34	↑	C&C との通信開始
35	↑	共有フォルダ内のファイルを流出
36	↑	メールから検体は採取したが､感染には気付かず
37	↑	検体解析をセキュリティ会社と NISC に依頼
38	↑	新たな C&C の URL 見つかったが、ブロックせず
39	5 月 22 日	NISC が不審な通信を検知
40	↑	抜線し、拠点のインターネット接続を遮断
41	5 月 23 日	別拠点で NISC が不審な通信を検知
42	↑	抜線し、拠点のインターネット接続を遮断

31	6							
32	7							
33	5							
34	6							
35	7							
36								
37								
38								
39		6	✔					
40		6			✔			
41		6	✔					
42		6			✔			

4.2 発生事象の分類

次に，これら発生事象が，攻撃者の行動なのか，防御者の行動なのか，第何段階の行動なのか，また，防御者の行動であれば，検知，拒否，妨害，減殺，欺瞞，破壊のどの種類に属する行動なのか，を考察した．分類結果を表 2 に示す．

なお，何も記載のないところは，攻撃者の行動にも，防御者の行動にも当てはまらないものである．

4.3 分類結果の分析

上記の分類により，以下の点が判明した．

1) 本事案において観測された攻撃者の行動は、すべてサイバーキルチェーンのいずれかの段階に分類可能であった．
2) 本事案において観測された防御者の行動が，サイバーキルチェーンの段階，および，種別に分類可能であった．

上記より，実際に発生した事案から発生事象を抽出し，サイバーキルチェーンモデルにしたがって分類することにより，攻撃者行動の分析，および，防御者行動の分析を標準化しうるものと考える．

以下，それぞれについて，詳しく述べる．

4.3.1 攻撃者行動分析の標準化

表 2 に示したとおり，本事案の攻撃者の行動がサイバーキルチェーンのいずれかの段階に分類できている．また，その行動が，

- 3→4→5→6，3→4→5→6・・・と繰り返している．
- 6 に失敗したらまた 3 に戻って繰り返している．
- 段階を飛ばしたりはしていない．
- 繰り返した結果，最終的に 7 に到達している．

というように，標的型攻撃の典型的な行動に則っていることが良く分かる．このように，観測された攻撃者の行動をサイバーキルチェーンの段階に紐づけて示すことにより，それぞれの事象がどの段階に属するかという標準化された情報が付与される．すなわち，標準化された手法で分析し，標準化されたフォーマットで分析結果を表現できるということである．

これによって，当該インシデントが理解しやすいものとなるので，これを情報として共有する際にも，共有先での理解を促進するものと考える．

また，このような標準化された分析は，分析結果を二次利用する，すなわち，分析結果を教訓として生かす，あるいは，分析結果を蓄積して統計的に分析するなどの場合にも，より有効な二次利用を可能にするものと考える．

なお，このように，攻撃者の行動を分かりやすく記述するという目的のためであれば，Indictor レベルで記述しなくとも，発生事象による記述でも有効であると考える．それ以上の考察を加えたいとき，すなわち，攻撃者は誰であったのか，あるいは，同じ攻撃者が他の組織を攻撃していないか，といったことを究明したいときには Indicator レベルの情報を共有することも検討すればよいと考える．

4.3.2 防御者行動の標準化

防御者行動については，段階に加え，検知・拒否・妨害・減殺・欺瞞・破壊の対応種別という標準化情報が付与される。この，分析手法の標準化，表現フォーマットの標準化によって，理解，および，情報共有の促進に寄与するであろうことは，攻撃者行動分析のケースと同様である．

防御者行動の分析に関しては，加えて，

ア）防御者行動に対する評価の妥当性

イ）課題抽出の網羅性

ウ）課題に対する対応策の適切性

についても，より説得力ある形で分析結果を提供できるものと考える．サイバー攻撃事案の報告において，防御者側の行動に関する記述は，攻撃者行動の記述よりも，さらに重要である．起きたという事実以上に，どのように守ろうとしたのか，何が失敗（あるいは不十分）だったのか，次に起きないようにどのような対策をしているか，が重要視され，したがって，上記の 3 点が十分に納得性ある形で盛り込まれる必要があるのである．

ア）防御者行動に対する評価の妥当性

サイバーキルチェーンによって分析を標準化することにより，防御者行動が攻撃者行動を食い止めるのに有効であったかどうかが端的に示される．表 2 の 22 番の行動で防御者が第 6 段階の拒否に成功している．これにより，攻撃者が 19 番から 21 番にかけて 3→4→5 と進んできたものの，第 6 段階に進むことができず，24 番で再び第 3 段階に戻った．ここでは防御者の第 6 段階の防御策は有効であったと言える．しかしながら，4 番，9 番，31 番，34 番では攻撃者の第 6 段階行動を阻止できておらず，したがって，防御者の第 6 段階の防御策は成功率が高いとは言えない，と評価できる．

イ）課題抽出の網羅性

課題抽出という観点では，防御者が取った行動（防御者が予め取っておいた行動＝防御策が取った行動を含む）がすべて記載されているのであるから，課題を抽出することも容易である．一方，記載されることが期待されていたにもかかわらず記載されなかった行動，すなわち，有効でなかった対策も明らかになる．

実際のところ，表 2 の防御者行動を集計すると，第 3 段階が 2 件，第 4 段階が 2 件，第 6 段階が 9 件の合計 13 件である．第 6 段階は最後の砦であり，ここでの防御に失敗すると，攻撃者が第 7 段階（目的の実行）に移ることができる．サイバーキルチェーンの本質は，より早い段階で攻撃者行動を検知・拒否等することにより，攻撃者行動の選択肢を狭め，攻撃が成功する可能性を下げることであると第 2 節で述べた．この集計から判断すると，第 3・第 4・第 5 段階の対策が不十分であったか，対策はしてあったものの十分に有効ではなかった，などの課題が抽出されるものと考える．

ウ）課題に対する対応策の適切性

課題に対する対応策という点でも，例えば，第 3 段階で検知できたものの拒否できなかったとしたら，対策としては拒否が可能となるものを検討する，など，理に適った対策を立案できる．換言すると，立案した対策が理に適っていることを示すのが容易である．なお，本事案では第 3・第 4 段階の行動は拒否に成功しているので，上の例は当てはまらない．

このように，サイバーキルチェーンを使用し分析を標準化することにより，防御者行動についての報告内容を，より分かりやすく，妥当性・網羅性・適切性という観点からも説得力のあるものにすることができると考える．

なお，これらの評価は，あくまでも，公表された報告書から読み取ることのできた発生事象のみに基づいて評価したものである．公表されていない事象が存在した場合には評価の妥当性を欠くかもしれないが，本稿は，分析の手法について述べているものであって，年金機構事案を評価することが目的ではないことをお断りしておく．

4.3.3 サイバーキルチェーン分析の限界

日本年金機構事案は，冒頭に述べたように，極めて詳細な報告がなされた稀有な例である．詳細な報告があったので，今回，筆者らのような第三者でもサイバーキルチェーンを使用して分析することができた．しかし，日々発生するインシデントを，公開された情報のみから第三者がサイバーキルチェーン分析を行うことには，困難が伴うものと推測する．したがって，是非にも当事者側にてサイバーキルチェーンを使用して分析し，その結果を公表してもらいたいものであるが，分析結果を公表するということは，防御側の弱点をかなり具体的に述べることになってしまう．したがって，その弱点が対策により克服されてからでないと公表できないなど，タイムリーな公表を妨げる要素となる可能性がある．

では，弱点部分を隠して公表したらどうなるか．サイバーキルチェーン分析は，発生事象を論理的につなげていく分析である．意図的に一部の事象を伏せれば，論理的なつながりを欠く分析となり，理解しやすさを大幅に損ねるものと思われる．場合によっては，何らかの事象がそこに隠されていると気づかれてしまうであろう．

5. 関連事例

サイバーキルチェーンなどの標準に基づいた分析が分かりやすさと，その結果としての情報共有の促進につながっている事例を，一件挙げておく．2015 年 12 月に発生したウクライナ電力網へのサイバー攻撃による広域停電事案に関して，2016 年 3 月 18 日に，E-ISAC（電力業界のセキュリティ情報共有組織）が SANS Institute と共同で報告書を公開した[5]．この中で，攻撃過程が ICS サイバーキルチェーンにしたがって分析されているのである．

ICS サイバーキルチェーンとは，SANS Institute が提唱する，ICS（Industrial Control System：産業制御システム）を対象とするサイバー攻撃のキルチェーンモデルである．本稿で紹介しているサイバーキルチェーンとは段階の構成などが異なっている．筆者らはこの報告書を読んでみたが，ICS になじみの薄い我々にも分かりやすい内容となっている．

本件も，ウクライナにおける国家的な重大インシデントであり，国際的に情報共有し，理解を得る必要があったものと思われるが，ICS サイバーキルチェーンという標準化されたスキームにしたがって分析した報告書を公開することによって，多くの人が理解し関心を持つこととなり，その目的を大いに果たしたものと考える．

6. サイバーキルチェーンの多様化

第 4 節で，標的型攻撃事案においてはサイバーキルチェーンが有効な標準手法であると述べた．また，第 5 節では，

ICS へのサイバー攻撃事例において ICS サイバーキルチェーンが有効であった事例を紹介した．サイバー攻撃は標的型攻撃だけではない．国家的に重大と見なされる可能性のある攻撃パターンをとってみても，Web サイトの改ざん，DoS／DDoS 攻撃（サービス拒否攻撃／分散型サービス拒否攻撃），Web サイトからの情報漏えい，システムダウンなど多岐にわたる．また，実際のところ，サイバー攻撃だけが国家重大インシデントとは限らない．内部者による不正やサボタージュでも，重大なインシデントは発生しうる．

これら様々なパターンの攻撃に対して，それぞれキルチェーンモデルを策定する必要があるのではないかと考える．それにより，異なるパターンの攻撃についてもキルチェーンモデルという同じ考え方に基づいた分析が可能となり，異なるパターン間での比較や統計的分析が容易に行えるようになる可能性がある．

その一方で，キルチェーンモデルを策定するのは，標準化が目的であるので，あまりにも多種多様なキルチェーンが乱立してしまっては意味がない．しかし，その点に関してはさほど悲観する必要はないであろう．本稿で紹介しているサイバーキルチェーンにおいても，最終の第 7 段階：目的の実行では，様々な攻撃目的を取り扱うことができる．第 1～第 6 段階を省略できないパターンの攻撃であれば，最終目的が何であれ，一つのモデルで様々な攻撃に適用可能なのである．他のキルチェーンモデルの策定においても，このような柔軟性を念頭に置くことで，いたずらにキルチェーンモデルの数が増大することを防げるのではないかと考える．

7. まとめ

サイバー攻撃は多様化している．目的ひとつ取ってみても，金銭目的の攻撃や，前述ウクライナ停電事案のようなテロ行為，さらには，何らかの攻撃のための踏み台とするための攻撃もある．日本年金機構事案も踏み台であった可能性は否定できない．今後，物理テロと連動したサイバー攻撃が発生する懸念もある．サイバー攻撃が国民生活や，場合によっては生命に影響する恐れがある．

このような中，サイバー攻撃対策を効率的・効果的に進めるためには，インテリジェンスに基づいたプロアクティブな対策が必須である．また，攻撃者がグローバル化している以上，インテリジェンスもグローバル，すなわち国際的に共有されたものでなければならない．国際的なインテリジェンス共有の枠組みに加わるためには，国際的インテリジェンス共有にかかわる貢献と，責任能力の所在を明らかにしなければならないであろう．国家重大インシデント発生時のアカウンタビリティ（説明責任）は，そのような責任能力の一部である．

アカウンタビリティを適切に果たすためには，インシデントについて報告する際の標準準拠が必要であり，標的型攻撃事案においてはサイバーキルチェーンが有効であると考える．

本稿では，実際に日本年金機構のサイバー攻撃事案を題材にサイバーキルチェーンを用いた分析を試みた．その結果，分析手法の標準化が可能となり，分かりやすさ，二次利用の容易さ，および，防御行動に関する妥当性・網羅性・適切性の明確化に貢献できることを示せたと考える．この結果をもとに，標的型攻撃以外のパターンの攻撃についても，必ずしも外部からの攻撃とは限らず内部からの攻撃も含めて，キルチェーンモデルを策定することの可能性について考察した．

一方で，4.3.3 で示した，サイバーキルチェーンを用いた分析を公表した場合の，防御側課題が明確になりすぎてしまう点については，サイバーキルチェーン分析の優位性を損なわない範囲で機微な情報を守る手法の検討が必要と考えられる．

以上

参考文献

[1] “不正アクセスによる情報流出事案に関する調査結果報告について”
http://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.files/press0820.pdf,（参照 2016-08-06）

[2] “検証報告書”
http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf,（参照 2016-08-06）

[3] “日本年金機構における個人情報流出事案に関する原因究明調査結果”
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf,（参照 2016-08-06）

[4] “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf,（参照 2016-08-06）

[5] “Analysis of the Cyber Attack on the Ukrainian Power Grid”
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf,（参照 2016-08-06）