サイバー戦入門　その１０
～フェイクニュースと世論操作～

三村　守（防大情報工学科）

１　はじめに

ＬＩＮＥやＦａｃｅｂｏｏｋ等のソーシャルメディアあるいはＳＮＳ[1]は広く普及しており、個人の日常生活のコミュニケーションに欠かせないツールとなってきている。ソーシャルメディアは単純なメッセージのやり取りだけでなく、写真の共有、通話等の様々な便利な機能を有しており、電話やメールの代替手段としている利用者も少なくない。近年では、各国の多くの企業や政府機関でもソーシャルメディアの導入が進んでおり、単純な情報発信にとどまらず、マーケティングやビッグデータ解析に必要な情報源としても機能しており、ビジネスモデルの構築や政策を立案する上での重要な要素となっている。このように、非常に利便性が高く有用なソーシャルメディアには、機密情報の漏洩、個人情報の暴露、フェイクニュース等の様々な問題点も指摘されている。ソーシャルメディアで不用意に写真や個人情報を公開してしまうことで、学校や職場、氏名、交友関係等が暴露され、個人が特定されてしまうことも珍しくない。そのため、情報機関にとってソーシャルメディアは個人情報の宝庫であると言える。例えば２０１４年には、インターネット上に公開されたアルバムの写真から、米国に対するサイバー攻撃の実行犯と中国人民解放軍に所属する隊員の関係性が指摘されている[2]。また、ソーシャルメディア上でのニュースは信頼できないとの指摘もある。例えば、２０１１年の東日本大震災では、単なる誤報、科学的根拠がない信頼性に欠ける情報、特定の個人を貶めるためのデマ等の様々なフェイクニュースが確認されている。このようなフェイクニュースは例え真実ではなかったとしても、人々の行動や心理に何らかの影響を与える可能性がある。そのため、世論操作のための手段としても注目を集めるようになっている。特に、２０１６年の米大統領選では、フェイクニュースの拡散が選挙結果に影響した可能性が指摘されている[3]。このように、ソーシャルメディアはもはや兵器であり、政局を左右する可能性すら秘めている。そのため、フェイクニュースはもはやハイブリッド戦の主要な要素であり、その特徴と対策について十分に検討する必要がある。

そこで本稿では、ハイブリッド戦の一要素としてのフェイクニュースの概要について説明し、世論操作の現状を体系的に整理する。さらに、フェイクニュースに関する事例に基づき、各国の能力と現状について考察する。最後に、フェイク

---

[1] SNS (Social Networking Service)

[2] CrowdStrike (2014). PUTTER PANDA, CrowdStrike Intelligence Report

[3] Guess et al. (2019). “Less than you think: Prevalence and predictors of fake news dissemination on Facebook”

ニュースへの対策について述べる。

２　フェイクニュースの概要

（１）フェイクニュースの定義

フェイクニュースとは、主にソーシャルメディア等のインターネット上で拡散する真実ではない偽のニュース記事のことである。フェイクニュースの目的としては、プロパガンダ、広告、愉快犯等が挙げられる。プロパガンダ目的のフェイクニュースは、政府に関係する報道機関や出資を受けた企業や個人により、何らかの政治的な思想を誘導する目的で発信される。広告目的のフェイクニュースは主に経済的な利益を目的としており、ブログ記事のように一見して広告とは見分けがつかない巧妙なものも多い。これらのフェイクニュースは、明確な目的があるという点で愉快犯のフェイクニュースとは異なっている。このように、フェイクニュースという言葉は様々な背景で使用されている。ある調査会社のレポートでは、フェイクニュースを大手報道機関への批判と、信頼性が低い不確かなニュースに分類している[4]。先の２０１６年の米大統領選で勝利したドナルド・トランプ氏は、自身に不利なニュースを報じる大手報道機関をフェイクニュースと批判し、記者会見における質問を拒否したことで話題となった。この事例では、報じられるニュースの真偽よりも、むしろ大手報道機関への批判としての意味合いが強い。他方、フェイクニュースを問題視する市民団体や研究者にとっては、情報の真偽が議論の対象であり、真実に対する偽のニュースとしての意味合いが強い。本稿では、情報の真偽に着目し、「虚偽や疑わしい情報を信じ込ませるために、人々を欺いて誤解させる目的で意図的に作成あるいは出版された情報」をフェイクニュースとして取り扱う。

フェイクニュースに関する情報は、表１に示すとおり分類できる[5]。

表１：フェイクニュースに関する情報の分類

偽情報（Dis-information）	虚偽であり、個人、社会集団、組織、または国に危害を加えるために故意に作成された情報
誤情報（Mis-information）	虚偽であるが、危害を加えることを意図して作成されていない情報
不正情報（Mal-information）	現実に基づいた情報であり、個人、組織、または国に危害を加えるために使用される。

このうち本稿で扱うフェイクニュースは、個人、社会集団、組織、または国

[4] Data & Society (2018). “Dead Reckoning Navigating Content Moderation After Fake News”
[5] Council of Europe report (2017). “INFORMATION DISORDER :Toward an interdisciplinary framework for research and policy making”

に危害を加えるために作成される 偽情報および不正情報である。

（２）フェイクニュースの目的

フェイクニュースをその目的を基に分類すると、主に政治目的と金銭目的によるフェイクニュースに分類される。

政治目的のフェイクニュースは、政治家が人々の政治に関する信条や意見を変えるために作成される。実際の出来事に対する人々の視点は様々であり、その描写は解釈の仕方によって異なる。この描写を巧妙に記述することで、人々の視点を変化させ、実際の出来事をあたかも他の出来事のように見せかける。このような政治目的のフェイクニュースは、政敵や特定の個人を社会的に抹殺する用途で用いられることもある。週刊誌で報じられる政治家や芸能人のスキャンダル、あるいはソーシャルメディアでの炎上等がこれに類似している。サイバー攻撃を活用し、相手に不利となるような情報漏洩を引き起こす手法も確認されている。２０１６年の米大統領選では、Ｗｉｋｉｌｅａｋｓ[6]が民主党全国委員会幹部のメール約 19,000 件を暴露し、委員長が辞任する騒ぎとなった。同年のフランス大統領選においても、投票前にメールや内部文書が流出する事件が発生している。これらの事件においては、人々の行動に何らかの影響を与える目的で意図的に暴露された可能性が指摘されている。

金銭目的のフェイクニュースは、主に広告収入によって利益を得るために作成される。センセーショナルな見出しのコンテンツは人々の注意を引く傾向があり、そのようなニュースを配信するサイトには大量のアクセスがある。一般にインターネットにおける広告収入は、その閲覧数によって課金される。そのため、フェイクニュースを配信するサイトは、掲示される広告から直接的に多額の報酬を得ることが可能である。また、フェイクニュースが間接的な利益をもたらす場合もある。株価は景気に影響するニュースに敏感であり、ソーシャルメディアの影響を受けることが指摘されている。そのため、意図的に景気に影響を与え得るフェイクニュースを配信すれば、その株価変動により利益を得られる可能性もある。

（３）フェイクニュースの特徴

フェイクニュースには人々の興味を引いたり視点を変えようとしたりするため、表２に示すような特徴があることが指摘されている[7]。

---

[6] 匿名で政府、企業、宗教等に関する機密情報を公開するウェブサイトの一つ

[7] TrendMicro (2017). “The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public”

表２：フェイクニュースの特徴

分類	項目
見出し	①興味を引くための大げさな見出し
改ざんの痕跡	②正規ニュースメディアを詐称する不審なＷｅｂサイトのドメイン
	③スペルミスや不自然なレイアウト
	④不正に加工あるいは修正された写真、画像、動画等
根拠の欠如	⑤出版日の欠如
	⑥作成者、情報源、具体的なデータの欠如

見出しに関しては、一般に大げさな見出しは人々の興味を引き、クリックあるいはタップされやすい傾向がある。そのため、人々の目に触れる機会も増える。①は、フェイクニュースが人々の興味を引くために作成されているために生じる特徴である。②は有名な正規サイトのドメインに似せた偽のサイトを構築し、そこで配信するフェイクニュースの信頼性を向上させようとするものである。ニュースの閲覧する際にどこの出版社かを確認する人はいるものの、そのサイトが本当にその出版社のサイトであるかをわざわざ確認する人は少ない。③は正規の記事を加工する作業において、スペルミスやレイアウトの変更が不自然な形でフェイクニュースに残っているものである。④も同様の過程において、写真、画像、動画等に不自然な加工の痕跡が残っているものである。一般に正規のサイトであれば、このようなミスが生じる可能性は少ないものと考えられる。②～④は、そのフェイクニュースが正規の記事を改ざんして作成している可能性を示唆している特徴である。記事の出版日、作成者、あるいはその情報源や具体的なデータが記述されていない曖昧な記事も、フェイクニュースの可能性が考えられる。⑤～⑥は、記事に関する具体的な根拠がないことに起因する特徴である。

３　世論操作の手法

これまでに示したとおり、フェイクニュースは人々の興味を引きやすく、ソーシャルメディアはこれを配信するための最適な手段となっている。そのため、政府が世論操作のためにこれを活用するのは合理的である。このような政府主体の世論操作活動は、それと気づかれないように多数のソーシャルメディアのアカウントを用いて大々的に実施されている。このような特徴は、ルアーを本物の魚に見せかけて引く漁業の方式に類似していることからトローリングと呼ばれている。また、このように世論操作活動のために運用されるソーシャルメディアのアカウントはトロールと呼ばれる。トロールは、実際の人間により運用されている場合もあれば、プログラムにより自動応答するボットにより運用されている場合もある。

政府主体の世論操作活動は表３に示す４つの方式に分類できる[8]。

表３：政府主体の世論操作活動の方式

方式	説明	実施者
政府が直接実行する方式	政府が直接実施あるいは出資する。	有志、素人、専門職
政府が主導・調整する方式	政府が主導・調整するが直接実施しない。	支援者、有志
政府が扇動する方式	政府が一般市民の集団心理を刺激して扇動する。	不特定多数の一般市民
政府が容認する方式	政府が攻撃対象を名指しして助長する。	

表中の上位の方式ほど政府の関与が強く、下位の方式ほど関与が弱くなる。そのため、下位の方式ほど巧妙で世論操作活動の証拠が残りにくくなる特徴がある。

政府が直接実行する方式では、政府が直接的に世論操作活動のためのトローリングを実施、あるいは出資する。その実施者は、主に有志、素人あるいは専門職の職員であると考えられている。このようなトローリングは、中国、ロシア、トルコ等の情報開示が不十分とされる国々で広く実施されている。例えば、２０１７年のエストニアへのサイバー攻撃では、エストニアに対する誹謗中傷やサイバー攻撃の手法がソーシャルメディアで共有され、サイバー攻撃を促す書き込みも多数確認されている。

政府が調整する方式では、政府は直接的にトローリングを実施せず、外部の他の組織等に実施を委託する。その実施者は、主にその委託を受けた支援者や有志であると考えられる。例えば、ベネズエラのチャベス政権は、利害が対立する実業家の誹謗中傷のハッシュタグ[9]を用いて関連する投稿を集約し、支援者によるトローリングを調整したとされている。ハッシュタグは関連する投稿を容易に結びつけることが可能であり、これによりさらに投稿が加速される効果が期待できる。

政府が扇動する方式では、不特定多数の一般市民の集団心理を刺激し、扇動することで世論を誘導する。２０１６年の米大統領選では、トランプ氏はＴｗｉｔｔｅｒを巧みに活用し、集団心理を利用して選挙戦を有利に導いたとの指摘がある。

政府が容認する方式では、ただ攻撃対象を名指しして批判することで、攻撃してもよい雰囲気を醸成する。例えば、２０１５年に中国において、新疆ウイグル自治区での反テロ対策を取り上げた記事を執筆した仏ニュース紙の駐在記者が

[8] IETF Digital Intelligence Laboratory (2018). "State-Sponsored Trolling"

[9] ソーシャルメディアにて投稿を分類して検索を容易にするためのキーワード

「中国人の感情を傷つけている。」と名指しで批判されたことがある。その後、その駐在記者は期限切れとなる記者証の更新を行わないとの通告を受けている。このように、政府の権力が強い国家では、政府からの名指しでの批判が暗黙の圧力として機能する場合がある。

４　各国の世論操作部隊の現状

（１）ソーシャルメディアのメッセージの内容

オックスフォード大学の調査によると、各国のサイバー部隊のソーシャルメディアのメッセージの内訳は表４に示すとおりである[10]。

表４：各国のソーシャルメディアのメッセージの内訳

	フェイクアカウントの種類	政府支持メッセージの発信	反対勢力への攻撃	中立のメッセージの発信	トローリングや嫌がらせ
米国	人間、ボット、サイボーグ	○	○	○	○
中国	人間、ボット	○	○	○	○
ロシア	人間、ボット、サイボーグ	○	○	○	○
北朝鮮	人間	○	○		
韓国	人間、ボット	○	○		○

フェイクアカウントの種類については、「人間」、「ボット」、「サイボーグ」に分類されている。「人間」は、本物の人間により手動で運用されているアカウントである。「ボット」はプログラムにより自動的に運用されているアカウントであり、「サイボーグ」は人間がボットを活用して運用しているアカウントである。これらのアカウントを活用して発信されるメッセージに関しては、政府支持、反対勢力への攻撃、中立、あるいはトローリングや嫌がらせに分類される。このように、ある程度ソーシャルメディアが発達した国では、フェイクアカウントにより様々な世論操作活動のためのメッセージが発信されていることが確認できる。

（２）ソーシャルメディアの活用手法

ソーシャルメディアを運用するサイバー部隊は、政府のプロパガンダを広めるために様々な手法を活用する。同調査によると、各国のサイバー部隊のソーシャルメディアの活用手法は表５に示すとおりである[11]。

---

[10] Bradshaw et al. (2018). "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation"

[11] Bradshaw et al. (2018). "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation"

表５：各国のソーシャルメディアの活用手法

	独自コンテンツの作成	適正なコンテンツやアカウントの停止	ターゲッティング広告	検索エンジンの最適化
米国	○		○	○
中国	○	○		○
ロシア	○	○		
北朝鮮				
韓国				

独自コンテンツの作成には、フェイク動画、ブログ、メモ、写真、ニュースサイト等が含まれる。加えて情報開示が不十分とされる国々では、コンテンツの検閲や遮断も実施されていることが確認できる。これらの国々ではさらに、ソーシャルメディア上の適正なコンテンツやアカウントの停止処置もとられている証拠があるとしている。これらの手法は、国内で行使される場合もあれば、国外に対して行使される可能性もある。とりわけ、ロシアの諸外国への干渉（クリミア紛争、米大統領選、仏大統領選）については度々指摘されている。中国では国内での監視が非常に厳しく、国産ソーシャルメディアのＷｅＣｈａｔでのサイバー部隊の活動や、検索エンジンによる不都合なコンテンツの遮断も確認されている。例えば、「天安門事件」に関する情報が一切表示されないのは周知の事実である。また、特定層のみを対象としたターゲッティング広告も活用されている。ターゲッティング広告は、閲覧者の端末をトラッキング[12]技術により識別することで、その閲覧者の属性に応じた広告を表示させる手法である。検索エンジンの最適化は、検索結果の表示順位を様々な手法で操作することで、都合の良い情報を意図的に上位に表示させる手法であり、マーケティングにも活用されている。

５　フェイクニュースへの対策

（１）組織的な対策

このようなフェイクニュースや海外からの世論操作活動の脅威に対し、多くの国々では独自のアプリケーション、ポータルサイト、あるいは対策チームを構成している。政府による主な対策の例を表６に示す。

表６：政府によるフェイクニュースの対策の例

手法	対象
ファクトチェック	情報
防諜	人間
情報提供の推奨	
自発的活動の推進	

[12] 利用者の端末を識別して継続的に追跡する技術

最も基本的な対策は、その情報の真偽を確認するファクトチェックである。ファクトチェックはその情報の正確性や妥当性を検証する行為であり、事実検証あるいは事実確認とも呼ばれる。そのほかの対策は、情報ではなく主に国民等の人間を対象としたものである。防諜はカウンター・インテリジェンスとも呼ばれており、いわゆるスパイ活動への対策である。従来のカウンター・インテリジェンス活動としては、スパイ活動への対策が主な教育内容となっているが、このようなフェイクニュースによる世論操作活動にも留意すべきであろう。このように、フェイクニュースは従来のインテリジェンス活動を拡張する側面も備えている。情報提供の推奨は、フェイクニュースやそれに関連する活動を発見した場合には、情報提供を推奨する制度である。自発的活動の推進は、アストロターフィングと呼ばれており、政府が背後に隠れ、国民の自発的な活動に見せかけて主張を行う手法である。これらの対策手法では、ソーシャルメディア上のファクトチェックのための情報に着目したり、一般市民にそのような情報の提供を呼び掛けたりする場合もある。いくつかの国々では、政府による一般市民の自発的行動を装うためのアプリケーションやポータルサイトも確認されている。

（２）個人で実行可能な対策

個人において実行可能なフェイクニュースを見破るためのポイントは表７に示すとおりである[13]。

表７：フェイクニュースを見破るためのポイント

分類	項目
内容の確認	①見出しだけでなく内容も確認する。
	②ボットによる不自然な点がないか確認する。
	③記事の出版日、作成者、情報源および具体的なデータの有無を確認する。
他の記事との相互確認	④他のメディアの記事も確認して相互チェックする。
	⑤記事の裏付けとなる情報源を精査し、誤報を広めていないことを確認する。
	⑥記事の画像や動画が改ざんされていないか他の記事と相互チェックする。
	⑦信頼できる情報源を活用し、フィルターバブル[14]の影響を排除する。
専門家の活用	⑧著名な事実確認の専門家に相談する。

まずは基本的なことであるが、見出しだけでなく記事の内容をきちんと確認

[13] TrendMicro (2017). “The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public”

[14] 検索サイトにおいて利用者をトラッキングにより識別し、見たくない情報を遮断する機能

することである。その記事に記載されている内容が事実かだけでなく、書き方にボットの自動処理による不自然な点についても留意が必要である。また、記事の出版日、作成者、情報源および具体的なデータの記載の有無も真偽を確認するためには重要である。

次に、その記事と他の記事との相互確認を実施することが挙げられる。他のメディアにも同様の見出しの記事があるのであれば、その内容は概ね一致しているか？　記事の裏付けとなる情報源があるのであればその内容を確認し、誤った情報を広めていないか？　あるいはこれらの記事の画像や動画が改ざんされていないか？　これらの確認を実施するにあたっては、ターゲッティング広告や検索エンジン最適化の影響により、そもそも不都合な情報が遮断されていないかを確認することも重要である。

自身での確認が難しいようであれば、著名な事実確認の専門家に相談するという選択肢もあり得る。

これらは個人においても実施可能な対策の例であるが、自組織の人間やすべての国民がこれを完璧に実施するのは現実的ではない。これは、世の中で詐欺による被害が一向に減らないことからも明らかである。したがって、このような事項を教育しつつ、そのリスクを踏まえた組織的な対策が必要であると考えられる。

（３）OSINT の活用

情報の真偽を確認するファクトチェックに関しては、ＯＳＩＮＴ[15]と呼ばれる公開情報を利用した分析手法が注目されている。

例えば、２０１４年７月１７日に、マレーシア航空の１７便がウクライナ上空で撃墜された事件では、ロシアは関与を否定した。しかしながら、ベリングキャット[16]と呼ばれる有志のグループがＯＳＩＮＴを活用し、撃墜に用いられたミサイルの経路を特定した。これにより、ミサイルはロシアからウクライナに運搬され、撃墜に用いられたことが裏付けられた。彼らは、衛星画像、ドライブレコーダの映像、ＳＮＳ等の情報を丹念に分析し、画像や動画の撮影日時や地点を特定しました。特に、画像に映った背景や看板等の情報からその撮影地点を推定する、ジオロケーションと呼ばれる分析手法はしばしば用いられている。さらに、背景に映ったガソリンスタンドの看板のガソリン価格と実際の価格の推移を照合し、その動画の撮影日時を特定する手法や、車両のナンバーのみならず、傷の形状から個体を識別する等の高度な手法も用いている。

６　おわりに

本稿では、ハイブリッド戦の一要素としてのフェイクニュースの概要をについて説明し、世論操作の現状を体系的に整理した。また、フェイクニュースに関す

[15] Open Source Intelligence
[16] https://www.bellingcat.com/

る事例や各国の能力と現状について考察した。さらに、フェイクニュースに対する組織的な対策と個人で実行可能な対策について述べた。

１９９９年に提唱された「超限戦」は今や「ハイブリッド戦」に進化しており、正規戦以外にもサイバー戦、情報戦等のあらゆるドメインに影響が及んでいる。サイバー戦では不正アクセスによる機密情報の情報搾取やスタックスネットのようなマルウェアによる制御システムへの攻撃が注目されてきたが、ソーシャルメディアによる活動も本格化している。大統領選の結果をも左右するソーシャルメディアはもはや兵器であり、その特徴や影響については熟知しておく必要がある。

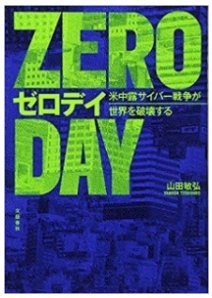
世界的なソーシャルメディアであるＦａｃｅｂｏｏｋでは、２０１６年の米大統領選でフェイクニュースを配信したことをきっかけとし、ファクトチェックの機能を強化している。この機能では、ファクトチェックのための複数のパートナー組織と情報を共有し、フェイクニュースと判定されたリンク、画像、動画等を配信されにくくし、シェアしようとした場合には警告を表示させる。このような機能の拡充によりその影響はある程度緩和される可能性もあるが、ファクトチェック機能を回避する試みも時間の問題であると考えられる。近年ではＡＩ技術の進歩により、自然なフェイク画像や動画の作成も可能となってきている。これを検知する手法にもやはりＡＩ技術が活用されており、まさにＡＩｖｓＡＩの時代となっている。

個人でソーシャルメディアを利用しないという選択肢は情報漏洩の対策にはなり得るが、大衆を対象とした世論操作活動の対策とはならない。カウンター・インテリジェンス等の具体的な対策を検討するためには、各ソーシャルメディアの特徴にも精通しておく必要があるものと考える。

付録１：おすすめの書籍

「おすすめのサイバーセキュリティの書籍はありますか？」と尋ねられる機会は多いのですが、一口にサイバーセキュリティと言っても、技術、国際政治（安全保障）、経営、法律、教育等の様々な側面があります。また、コンピュータになじみのある方とそうではない方では理解力にも差があるため、おすすめの書籍も異なります。そこで今回は、サイバーセキュリティ技術および安全保障に関する内容を中心に、なるべく一般的で役立ちそうな書籍をいくつか紹介したいと思います。

もっとも頻繁に受ける質問は、「サイバー攻撃で何ができますか？」という質問です。2020 年から小学校で必修となるプログラミングを経験していない方には、具体的にどのような脅威があるのかイメージするのは難しいと思います。



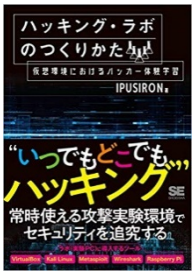
このようなＩＴの基礎知識がない方への入門書としては、山田敏弘氏の「ゼロデイ 米中ロサイバー戦争が世界を破壊する」がおすすめです。この本は、米国とイスラエルがイランの核燃料施設を攻撃するために共同開発したとされる「スタックスネット」やロシアの米大統領選への介入疑惑等、これまでのサイバー攻撃の事例を平易な用語でわかりやすく解説したものです。より広く最新の事例に関しては、David E. Sanger 氏の「The Perfect Weapon（邦題）サイバー完全兵器」もおすすめです。

サイバー攻撃を題材とした小説もヒントになります。数ある小説の名でもおすすめしたいのが、一田和樹氏の「原発サイバートラップ」です。最近ではサイバー攻撃を題材にしたドラマや小説もだいぶ増えてきましたが、現実離れした内容があることも否めません。この小説は日本周辺で発生したサイバーテロを題材としたものですが、技術的なチェックがしっかりとされていて現実味のある内容です。また、主人公が防衛大学校の卒業生ということで、皆さんにも親しみ易い内容です。現実とのギャップや登場人物のモデルを想像してみるのも面白いかもしれません。

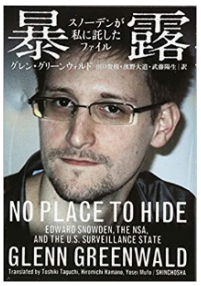
イメージがつかめると、「技術的な仕組みを学びたい。」との要望が聞かれるようになります。IT やセキュリティの分野には専門用語が多く、難解な用語のイメージができないという方におすすめなのが、みやもとくにお氏、大久保隆夫氏による「イラスト図解式 この一冊で全部わかるセキュリティの基本」です。この本ではよく目にする用語を中心に解説しており、手っ取り早く概要を理解したい方におすすめです。

セキュリティの概要を理解しても、実際に使ってみないと技術はなかなか身につかないものです。また、個人でできるセキュリティ対策も限られています。個人でできる対策を紹介した書籍としては、岩井博樹氏の「動かして学ぶセキュリティ入門講座」があります。この本では個人のＷｉｎｄｏｗｓパソコンでもできるセキュリ

ティ対策を、具体的にソフトをインストールして設定する手順を紹介しています。とりあえず自分の身くらいは自分で守れるようになりたいという方におすすめです。

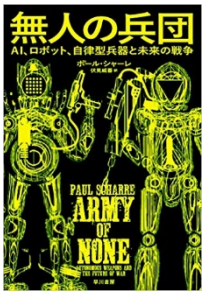


IT やセキュリティの素養があり、サイバーセキュリティを専門的に学びたいという方には IPSIRON 氏の「ハッキング・ラボの作り方 仮想環境におけるハッカー体験学習」がおすすめです。この本は模擬ハッキングを実際にやってみて、仕組みを学ぼうとするものです。まさに、「彼を知り己を知れば百戦殆うからず」ですね。サイバーセキュリティ技術者には高い倫理観が求められます。くれぐれも、この本で学んだ内容を悪用したり、仮想環境以外で実行したりして迷惑をかけることがないように注意しましょう。



最後に、安全保障により深く関連する書籍をいくつか紹介したいと思います。Glenn Greenwald 氏の「No Place to Hide、（邦題）暴露」は、米国のサイバースパイ活動や世界レベルの監視システムの存在をスノーデン氏が暴露したものです。本人による自伝「Permanent Record、（邦題）スノーデン自伝 消せない記憶」もあります。この事件は間違いなくインテリジェンス史に残る大事件でした。今日ではＳＮＳの普及もあり、個人を標的としたインテリジェンス活動の中心はますますサイバー空間にシフトしています。

そんなＳＮＳはもはや兵器であり、国家主体の世論操作活動に警鐘を鳴らすのは一田和樹氏の「フェイクニュース」です。ＡＩの発達で動画を含む精巧なフェイクニュースの作成は容易となり、真偽の判断はもはや困難です。大統領選の結果をも左右するＳＮＳは、ハイブリッド戦の重要な要素となりました。ユーゴ紛争でセルビアを悪者に仕立て上げた「戦争広告代理店」は、より洗練された国家によるＰＲ活動に進化しています。



ＡＩの発達は戦場も変えました。兵器の無人化が進み、その通信を支えるサイバーセキュリティ技術はますます重要となります。そんな未来の戦闘様相やＡＩに関する倫理的課題について網羅的に扱っているのは、Paul Scharre 氏の「Army of None、（邦題）無人の兵団」です。将来の指揮官にはこの本で描かれているように、現在よりもはるかに高速で複雑な意思決定が求められることになるのでしょう。

以上、サイバーセキュリティ関連の皆さんに役立ちそうな書籍を紹介させていただきました。

付録２：サイバーセキュリティ関連の情報源

「サイバーセキュリティ関連の情報はどうやって集めればよいか？」も同じく頻繁に受ける質問です。ここではいくつかのサイバーセキュリティ関連の情報源を紹介したいと思います。

サイバーセキュリティに関する最もタイムリーな情報源は、主要なソーシャルメディアの１つであるＴｗｉｔｔｅｒです。Ｔｗｉｔｔｅｒの内容はＷｅｂサイトからも参照することが可能であり、アカウントを持っていなくても以下のサイトからパソコンやスマートフォンで手軽に閲覧することができます。

・piyokango
https://twitter.com/piyokango/

・北河拓士
https://twitter.com/kitagawa_takuji/

・辻 伸弘 (nobuhiro tsuji)
https://twitter.com/ntsuji/

Ｔｗｉｔｔｅｒの他にも以下のようなサイトもあります。

・セキュリティホール MEMO
http://www.st.ryukoku.ac.jp/~kjm/security/memo/

これらのサイトを毎日チェックしておけば、新聞やテレビよりもはるかに迅速かつ効率的にサイバーセキュリティに関する情報を網羅することができると思います。新聞の切り抜きは不要です。Google で検索、あるいはブラウザで上記の URL を入力するだけです。通勤や空き時間に見出しをチェックするだけでも、この分野の最新の事情に精通することができると思います。

ある程度まとまって整理された情報が欲しい場合には、以下のサイトが非常に参考になります。

・piyolog
https://piyolog.hatenadiary.jp/

このサイトではサイバーセキュリティに関する比較的大きな事件を、図表を用いてわかりやすく解説しており、記述内容の根拠となる情報源も掲載しております。ある事件について詳しく知りたい場合や、その事件に関する報告資料等を作成する場合には、非常に参考になるサイトです。レスポンスも非常に速く、新聞やテレビで報道される頃にはすでにコンテンツが掲載されている場合がほとんどです。うまく活用し、部下に無用な報告を強いるのは控えましょう。

これらの情報源は特定の個人に強く依存しており、いつまでもタイムリーに情報が発信できるとは限りません。他の新しい情報源を活用したり、複数の情報源を使い分けたりするのも良いと思います。

以上、サイバーセキュリティ関連の情報源をいくつか紹介させていただきました。