Vol.2021-CSEC-95 No.23
Vol.2021-SPT-45 No.23
Vol.2021-EIP-94 No.23
2021/11/9

ビジネス・インテリジェンス（情報収集）の考察

内田勝也[†1]

概要：孫子は「戦わずして人の兵を屈するは善の善なる者なり」とあるが，サイバーセキュリティでは，事前の情報収集を行い，その対応を行うことが，該当する．　即ち，事前に適切な対応を行う仕組みの構築が，「戦わずに，攻撃をあきらめさせることになる.」　大規模な対応であれば，『地政学的考察』が必要だが，ここでは，サイバーセキュリティ情報の収集・分析を行い，その対応を示すことを試みた．　いくつかの事例を示し，その対応を考える．

キーワード：インテリジェンス，マルウェア，拡張変異，事前対応，孫子

Review for Business intelligence

Katuya UCHIDA[†1]

Keywords:

1. はじめに

1.1　インテリジェンスとは

かつて，国内では，インテリジェンスを「諜報」と呼んでおり，太平洋戦争時代には特殊な言葉として使われていたが，最近は，地政学の関連で言われることが多い．また，インフォメーションと対で考えることが多い．

サイバーセキュリティ分野の言葉でも同じであるが，関係者により，異なる定義をしていることが多い．インテリジェンス分野でも，同じだが，ここでは，インフォメーションとインテリジェンスを以下のように定義する．

- **インフォメーション**（Information）：日本語では『**情報**』と訳され，観察，報告，噂，画像，音声，映像や他の資源を含むあらゆる種類の素材（Material）で，未だ評価・加工されていないもの
- **インテリジェンス**（Intelligence）：インテリジェンスは，インフォメーションを収集，編集・加工，統合・分析・評価・解釈し，報告した成果物（プロダクト：報告書）と定義する．

これら２つの言葉の関係は，情報処理システムと考えことも可能で，情報処理（業務処理）システムでは，必要な情報を入力（収集）し，編集・加工，保存，分析等を行い報告書を作成している．

インテリジェンスでは、業務組織を対象にした「ビジネス・インテリジェンス」分野の考察も行われているが、ここでは，更にビジネス・インテリジェンスの一部の一部として，「**サイバーセキュリティ分野**」のインテリジェンスを考察した．

サイバーセキュリティでは，第三者の悪意（サイバー攻撃等）を考える必要があり、一般の地政学が地球全体を想定した「**グローバルな地政学**」に対し，「**ローカルな地政学**」と想定した．

ローカルな地政学で，インテリジェンスを考えると，

《インテリジェンス ＋ インフォメーション》

を中心に捉えることが，サイバーセキュリティ分野では適切だと感じている．

本来のインテリジェンスでも，収集情報の 90%以上は公開情報からの収集と言われており，一次情報の収集が重要であるといわれているが．今回のサイバーセキュリティ分野では，自組織でのインシデントを除き，多くはマスコミ等の**二次情報**だが，特に，一次情報なのか，二次情報なのかの問題は少なかった．

1.2　インテリジェンスとサイバーセキュリティ

サイバーセキュリティ分野でインテリジェンスでは，まず浮かぶ言葉は、孫子の

戦わずして人の兵を屈するは善の善なる者なり

である。

この言葉から感じるのは，『百戦百勝』が最適な戦法ではなく，戦わないこと，あるいは，攻撃されないことが望ましいことになる．

それは，百戦百勝でもあっても，敵だけでなく，味方も被害を受けることになり，資産の毀損や負傷者だけでなく，最悪の場合，死者がでる可能性もある．

現実の世界でも，被害を受けない方法を採用することを考えることが可能であろう．その一例として、侵入犯罪の防止がある。図表 1-1 は，警察庁の 2020 年の侵入犯罪の調査結果だが，**全体の 52%の**侵入盗が**無施錠が原因で発生**しており，**無施錠とガラス破りでは，80%**近くに達する．

無施錠だけでも無くすことができれば，侵入犯罪の半分を減らせ，ガラス破りを含めれば 80%近くの侵入犯罪を防ぐことができる．

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

Vol.2021-CSEC-95 No.23
Vol.2021-SPT-45 No.23
Vol.2021-EIP-94 No.23
2021/11/9

	総数	無施錠	ガラス破り	合計	割合(%)
一戸建て	16,316	8,620	4,860	13,480	82.6
共同住宅（３Ｆ以下）	4,083	2,127	905	3,032	74.3
共同住宅（４Ｆ以上）	1,900	870	247	1,117	58.8
合　計	22,299	11,617	6,012	17,629	79.1

図表 1-1 2020 年 侵入犯罪の脅威 [1]

サイバーセキュリティでも，同様で，「事前対応ができれば，インシデントの削減」は可能である．そのための１つの方法として，全くゼロから考えるのでなく，過去のインシデントをグループ化し，その延長として対応することを考えた．

1.3　サイバーセキュリティにおける事前対応

事前対応としては，プログラム作成時やウェブ構築時に対応することも考えられるが，

(1) バグバウンティ（バグ報奨金制度：Bug bounty）

「Hack the Pentagon」とも呼ばれ，2016 年 4 月から約１ヶ月間，事前に公募したホワイトハッカーにより，米国防総省のウェブの脆弱性を報告させ，発見・報告された脆弱性は，138 件あり，その脆弱性に応じ，報償金を支払う仕組みを構築した．現在では，1,000 社を越える企業等が実施しているが，国内ではあまり普及していない．

(2) インシデントの分析及び推測

過去に発生したインシデント情報の収集･分析を行い，将来を推測することを考えた．

歴史は繰り返すという言葉があるが，インシデントが常に自分の周りで発生している訳ではないが､インシデントを繰り返さないことが業務遂行に大切な要件であろう．

2. 収集情報を基に何を考えるか？

2.1 インテリジェンスの目的

サイバーセキュリティ事件・事故は，既に半世紀程度になり，最近は更に多くのインシデントが発生しており，多くの組織が被害を受けている．

本来，情報収集目的は，情報の収集・分析だけでなく，その分析情報が将来のサイバーセキュリティ事故・事件の対応に役立たせる必要があると考えている．

事前対応の重要性は，前述した「バグバウンティ」を考えても，サイバーセキュリティ分野での重要性は同じであり，個別のインシデントを考えるのでなく，関連するインシデントのグループ化により，対応すべき内容も明確になる．

前述した様に，サイバーセキュリティでは，自組織内でインシデントが発生する可能性は低く，多くの場合，二次情報[a]だと考えている．

収集した情報を基に，分析を行うが，基本的には，

① 収集情報（インシデント）が，自社で発生する可能性があるのか？

② 収集情報が，**拡張変異**[b]する可能性があるか？

等を考える必要があるが，今回は，インシデントを技術面から分析するのでなく，現象面を中心に過去のインシデントのグループ化を試み，サイバーセキュリティ技術はあまり必要がなかった．

3. 事例を考える

実際に発生したインシデントを取り上げ，インシデントの原因（遠因）やどの様なインシデントに拡大するか等の考察を行った．

3.1 機能拡張：　ランサムウェア（Ransomware）

基本機能が時間の経過等に伴い，機能が拡張され，また，従来は，コンピュータ・ウイルスの一種である『トロイの木馬』ウイルスから，『ランサムウェア』と呼ばれるようになった．ランサムウェアは，ランサム（身代金：Ransom）とソフトウェアを組み合わせた造語で，一種のマルウェアで，感染したコンピュータをロックする，ファイルを暗号化し，コンピュータ使用を不可能にするとし，元に戻すには，金銭（身代金）を要求した．　最近は，金銭の支払い以外にも，いくつかの要求を行っている．

(1) AIDS ウイルス（トロイの木馬）[c]

1989 年，スイスで AIDS（後天性免疫不全症候群）国際学会が開催され，その出席者や欧米金融機関のシステム部門責任者等に，約 2 万枚のフロッピー（ラベルには「**AIDS Information Introductory Diskette（エイズ・ウイルス情報入門）**」とあった）が送付され，『AIDS ウイルス』とか，『AIDS Trojan』と呼ばれた．パソコンを約 90 回起動すると，ハードディスクの内容を暗号化し，海外口座に 378 米ドル送金する旨の送金指示書を作成した．ただ，暗号は「共通鍵暗号」を使っていたため，暗号鍵はウイルス内に含まれており，ファイルの復元プログラムが作成され，犯人も逮捕された．

(2) ソフトウェアの脆弱性放置　WannaCry[3]

ネットワーク化の進展は，感染拡大も進展させ，単体での感染がネットワークを介して大きな事故／感染に拡大したが，感染拡大の要因は，**最新のソフトウェアへの未更新**であった．

(3) 二重恐喝（Double-Extortion Ransomware）Maze[4]

サイバー攻撃は，最も安易な金融犯罪で，直接的に殺人を行うこともないため，犯罪組織にとって格好の標的になっている．

a マスコミ等からの間接情報

b **拡張変異**：　報告者の**造語**．コンピュータの環境の変化，単独システムがネットワークに接続され，機能的には同じであるが，ネットワーク化されたため，機能が拡張される等とした

c 国内にも数枚が送られ，その 1 枚を使って，1990 年 6 月 感染実演を含めて，学会発表を行い，学会誌（日本セキュリティ・マネジメント学会）に，研究資料[2]とした

Vol.2021-CSEC-95 No.23
Vol.2021-SPT-45 No.23
Vol.2021-EIP-94 No.23
2021/11/9

データの暗号化と共に，支払いを拒否すれば，盗取した情報を公開すると脅迫した

(4) **四重脅迫**（Quadruple Extortion Services）[5]

組織内への恐喝だけでなく，更に，外部への脅迫を行うランサムウェアも発見されている．

従来の手口である；①ファイルの暗号化，②機密情報の公開 に加え，③企業のサービスを停止する（DoS攻撃），④取引先や顧客等に攻撃を連絡し，ハッキングされたことを伝える

3.2 電子メール詐欺（BEC: Business E-mail Compromise）

海外取引先や自社経営者などになりすまし，偽の電子メールを使い，偽の口座に入金をさせる詐欺．

特に海外との取引のある企業等は，海外のサイバーセキュリティ情報の収集が重要になる．

(1) 米国連邦捜査局（FBI：Federal Bureau of Investigation）

アメリカ合衆国の司法省傘下にある FBI は，サイバーセキュリティ分野でも積極的に情報発信を行っており，BEC に関しては，既に 2014 年から情報提供をしている[6][7]．

(2) 国内 セキュリティベンダーブログ

2016 年 1 月 国内のセキュリティベンダーは，BEC に関し，米国の被害状況を説明したブログ[8]を公開した．

(3) 国内での被害事例 3.8 億円の被害

2017 年 8 月～9 月 大手航空会社は，偽メールに従い，変更された偽の口座に，合計で約 3.8 億円を振込む BEC 被害受けた．

BEC 詐欺は，前述のように，2014 年から FBI（英語）の報告や国内セキュリティベンダーの情報等もあり，適切なインシデント体制が確立しており，これらの調査・分析報告が，当該部門へ報告され，口座変更等の重要情報の取扱手順が確立していれば，防ぐことができたインシデントと言える．

3.3 バックドア挿入の巧妙化

現在，多くの機器は，ソフトウェア（実行モジュール）が組み込まれているが，**『バックドア』**が組み込まれていた場合，検出できない可能性が高い

(1) マルウェア機能の挿入

1983 年 Ken Thompson は，『バックドア』を挿入した C コンパイラーを作成した． この C コンパイラーは，Thompson もユーザとして，ログインできた．彼は，チューリング賞の受賞講演（Reflections on trusting trust）で，C コンパイラーにバックドアがあることを公開したが，初期の C コンパイラーは，この機能が残っていたと言われている[9][10]．この『バックドア』はウイルスとかマルウェアとは呼ばれなかったが，**自己増殖機能**があった

(2) バックドアの挿入

電子会議システムの利用中に利用者アカウントを一時停止する事案が発生した[11]．

この件では，会議システム利用者**『Data owner』**と会議システム提供者**『Custodian』**の関係と考えられるが，Custodian の **CEO は母国のセキュリティ・ポリシーに従う制約**があり，この行為は今後も継続される可能性があるが，ソフトウェアの脆弱性への対応を適切に実施しいており，問題はないとの指摘[12]もあるが，全く異なる課題である．

(3) 政府による利用禁止報告

2021 年 9 月 22 日 リトアニア国防省は 8 月の調査で、セキュリティ上の重大なリスクが明らかになったため、国民に中国製スマートフォンの購入を控え、既に保有している場合は早急に処分すべきと公表した．中国のスマホ各社は指摘が適切でないと言っている．[13]

政府・自治体，民間企業や個人も，個人情報だけでなく，機密情報管理が重要になっており，今回の様な問題に関するポリシー等が不正に流出していないかの監視やガイドラインを国として考える必要がある[14]．

3.4 報復型攻撃

(1) 主義主張型ウイルス

1987 年 イスラエル ヘブライ大学で発見されたコンピュータ・ウイルスは，13 日の金曜日に発病（有害機能を実行）し，更に，感染した実行プログラムを 13 日の金曜日に実行すると，プログラムが削除された

(2) ハッカー（ハッカー集団）による報復

法的には問題なくとも，個人や国家・組織への恨みを買うような行為が引き金になり，攻撃された事案

① 2011 年 グローバルにゲームを提供している企業に一人のハッカーが**自社のゲームソフトを改ざん（ジェイルブレイク）した理由**で，米国で訴訟したことが契機で，ハッカー集団（？）と思われる集団により，ゲームの利用者情報や企業情報が漏えいした[15]

② 独裁的国家の**最高指導者の暗殺計画**を描いた**コメディ映画**の作成・公開により，ハッカー攻撃を受け，未公開映画を含め，組織が持つ，ほぼ全ての機密情報が漏えいした[16]．

3.5 虚偽申請（セキュリティ・ポリシー違反）

個人情報を含めた機密情報をツールやソフトウェアがどの様に処理しているかの判断をすることは，簡単ではないが，継続的な監視や調査が必要で，セキュリティ違反が発見されれば，情報を公開する必要がある．

(1) カナ漢字変換ソフト

2014 年 2 月 中国製カナ漢字変換ソフトでは，入力さ

Vol.2021-CSEC-95 No.23
Vol.2021-SPT-45 No.23
Vol.2021-EIP-94 No.23
2021/11/9

れた文字情報を中国にある自社サーバーに送付しており,パソコンとスマートフォン向けの両方で行われていた[17]

(2) 電子会議システムでのセキュリティ・ポリシー違反

会議システム提供者が，CEO は母国規制（セキュリティ・ポリシー）に従うことになっており，当該政府の規制に反する参加者がいたため,サービス提供を会議中に停止した[11]

3.6 攻撃の自動化・拡大化 （DoS 攻撃／DDoS 攻撃）

高速道路のアクセス集中と同じような現象がサイバーセキュリティにもあり，この攻撃方法として，**DoS 攻撃**（Denial of Service attack／サービス妨害攻撃）や**DDoS 攻撃**（Distributed Denial of Service attack）と呼ばれるものがある．

(1) DoS 攻撃

1994 年 12 月 ケビン・ミトニックは，サンディエゴ・スーパーコンピュータ・センターに DoS 攻撃の一種（SYN フラッド攻撃）を行った． センター勤務の下村努の協力で，FBI は彼を逮捕した

(2) DDoS 攻撃（手作業での埋込み）

2010 年 3 月 国内掲示板に韓国から,『**F5 アタック**(キーボードの F5 キーを押して攻撃を行う)』攻撃があった

(3) DDoS 攻撃（自動的な埋込み）

2001 年 7 月 脆弱性をもったプログラムに，ネットワーク経由で，マルウェア（「Code Red」）を挿入し，多数の感染プログラムを利用して，DDoS 攻撃を行う予定であったが，プログラムミスがあり，実施できなかった

なお，不特定多数のコンピュータ等から，目的とするサーバーなどにパケットが送られることにより,サーバーの処理能力を超える量のパケットが送られ，DDoS 攻撃と同じ現象である『**アクセス集中**』が発生する．新型コロナウイルスワクチン接種では,住民が複数の端末を使って，一斉にアクセスをしたため，一部の自治体では，アクセス集中が発生し，ワクチン接種の登録処理ができなくなった．

3.7 地政学的事案

被害国の行動が，攻撃国の政治的な課題を刺激したことが原因で,被害国に大きな被害が発生した.しかしながら,攻撃国は，当然ながら，自国による攻撃を否定している

(1) エストニアへの大規模サイバー攻撃 【青銅の夜】

2007 年 04 月 首都タリン中心部にあった『ソ連記念碑』（戦勝記念碑）を郊外の軍人墓地に移転したため，複数の大手銀行や政府,ニュースサイトがサイバー攻撃を受け，システムがダウンした．ピーク時には銀行カードや携帯電話も作動しなくなったが,ロシアは関与を否定した

(2) シンガポールテレコム（Singtel）での通信障害

2016 年 12 月 Singtel のファイバーブロードバンドサービスが停止した． Singtel はハーウェイのルーターを利用しており，そのバックドアを利用され，被害を受けたと多くのシンガポール人は考えており,中国からのサイバー攻撃がその原因と考えている．しかしながら、Singtel は機器故障と公表した．

中国からの攻撃が原因だと考える理由には,シンガポールと台湾の共同軍事訓練が行われたことによる報復だと考えている

これら 2 事案では，二国間の関係が政治的に悪化し，軍事的な攻撃でなく,攻撃者を判断し難いサイバー攻撃が仕掛けられたものと考えられる。

4. 終わりに

4.1 今後の課題

インシデントグループを，

インシデント A，インシデント B と考えると，

① A，B 共に過去のインシデント

② A は過去，B は今後可能性のあるインシデント

③ A，B 共に将来発生のインシデント

の 3 種類の組合せが考えられれる．

今回は①のみを対象としており，発生したインシデントをグループ化できれば事例を作成でき，**技術的セキュリティ知識はほぼ必要がなかった**.

今後，②や③の検討を行う必要があるが，セキュリティ技術よりは，想像力が必要と考えられ，一人で考えるのではなく，グループで自由な意見を提出・議論を行う，いわゆる『ブレーンストーミング』的検討が必要だと考えている．

謝辞 本報告書作成に以下の方々に貴重なご意見を頂き，厚くお礼を申し上げます.

- 情報セキュリティ心理学研究会への参加の方々
- 九州大学 リカレント講座：SECKUN 推進者：小出洋教授，藤岡福資郎氏

参考文献

[1] 警察庁，侵入犯罪の脅威 ～侵入窃盗の侵入手口，https://www.npa.go.jp/safetylife/seianki26/theme_a/a_d_1.html

[2] 内田勝也他，コンピュータ・ウイルスについて，pp91-100，1991 年 1 月，第 4 号，日本セキュリティ・マネジメント学会

[3] カスペルスキー．ランサムウェア「WannaCry」とは，https://www.kaspersky.co.jp/resource-center/threats/ransomware-wannacry

[4] Fireeye，MAZE - 新たなランサムウェア，2020.08.20，https://www.fireeye.com/blog/jp-products-and-services/2020/08/maze-ransomware.html

[5] 岩沢明信，ランサムウェア，4 重の脅迫で攻撃力 広がる企業の被害，2021.07.30，日本経済新聞，https://www.nikkei.co

Vol.2021-CSEC-95 No.23
Vol.2021-SPT-45 No.23
Vol.2021-EIP-94 No.23
2021/11/9

m/article/DGXZQOUC25CMN0V20C21A5000000/

[6] the Internet Crime Complaint Center (IC3), 2014 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2014_IC3Report.pdf

[7] Katie Stewart, 6 Years of Tracking BEC - What does the data show?, 2020.02.15, https://certifid.com/6-years-of-tracking-bec-what-does-the-data-show/

[8] Ryan Flores／品川暁子，企業から金銭をだまし取る，ビジネスメール詐欺「BEC」が増加中，2016.01.27，https://blog.trendmicro.co.jp/archives/12808?_ga=2.238534279.681487240.1633986267-499067792.1631580451

[9] 藤田昭人，Unix 考古学 Truth of the Legend, 2017, ドワンゴ

[10] 藤田昭人，Ken Thompson のチューリング賞授賞記念講演，2017，https://github.com/asciidwango/TruthOfTheLegend/blob/master/unix-archaeology-2017.pdf

[11] Zoom，人権活動家のアカウント一時停止　中国政府要請，2020 年 6 月 12 日，https://www.nikkei.com/article/DGXMZO60279220S0A610C2000000/

[12] 日商エレクトロニクス，Zoom の一連のセキュリティ・脆弱性の問題についてまとめ，https://zoom.nissho-ele.co.jp/blog/etc/security-issues.html

[13] BBC News, Lithuania urges people to throw away Chinese phones, 2021.09.22, https://www.bbc.com/news/technology-58652249

[14] 内田勝也他，サイバーセキュリティにおけるナショナルセキュリティの検討分科会 最終報告書，GLOCOM 六本木会議，https://www.infosecpsychology.com/seminar/CySec_FINALRep.pdf

[15] 小林伸也，誰が，なぜ？　史上最悪規模・ソニー個人情報流出事件を時系列順に整理，2011.05.06，ITmedia，https://www.itmedia.co.jp/news/articles/1105/06/news052.html

[16] 前田典彦，ソニーピクチャーズへのサイバー攻撃　解析で見えた，企業が知っておくべき脅威とは，ダイヤモンドオンライン，2015.01.09，https://diamond.jp/articles/-/64834

[17] 日本経済新聞，ネット入力情報を無断送信　漏洩の恐れ，https://www.nikkei.com/article/DGXNASDG2600W_W3A221C1CC0000/

[18] 小谷賢，インテリジェンス，2012 年，筑摩書房

[19] 上田篤盛，武器になる情報分析力，2019 年，並木書房