2

情報収集・インテリジェンス

情報セキュリティ演習教材 第2回

株式会社　日立製作所
サイバーセキュリティ技術本部
セキュリティ人財統括センタ

目 次

1. インテリジェンスとは

情報セキュリティ演習教材 第2回

1-1 インテリジェンス＝諜報活動

●「インテリジェンス※１」とは、主に国家の安全保障を目的に、外国の軍事・政治・経済等に関する情報を収集し分析・評価する活動を指す。

●単に情報を集めるのではなく、情報の正確性、重要度を考慮して、分析・評価を行う点に重きがおかれている。

● 様々なインテリジェンスの例

- OSINT(オシント、Open-Source INTelligence)
  新聞・雑誌・書籍・インターネット等で公開されている情報を対象とする
- HUMINT(ヒューミント、HUMan INTelligence)
  有識者や重要な情報に接触できる人物から情報を収集する。
- IMINT(イミント、IMagery INTelligence)
  偵察衛星や偵察機によって撮影された画像を分析することにより情報を得る。
- SIGINT(シギント、SIGnals INTelligence)
  通信や電子信号を傍受することにより情報を得る。

※スパイなどの秘密かつ非合法な手段を用いるイメージがあるが、多くは合法的な手段を用いた活動であると言われている。

※１：インテリジェンス(intelligence)には、知性や知能といった意味もある。

1-2 OSINT(オシント)

●OSINT(オシント、Open-Source INTelligence)は、公開情報を基にした情報収集活動であり、国家の安全保障のみならず、サイバーセキュリティの分野でも着目されている。

● セキュリティ分野でのOSINT活用例

- GoogleやFacebook、Twitter等の情報の継続的観測
  一般的なSNSやWebベースの情報の観測
  SNSで現在注目、炎上している話題の調査(ex.Yahoo!のリアルタイム検索)
- SHODAN/CENSYS等のIoT情報の観測
  インターネットに接続されているデバイスの情報の調査

➡ 本教材では、OSINTの基本となる、質の高い情報収集について学びます。

※参考情報：OSINT関連の情報サイト
https://i-sight.com/resources/101-osint-resources-for-investigators/

２．質の高い情報を収集するには

2-1 情報収集において留意すべき視点

情報の種類	・一次情報およびファクト(事実)や客観的情報(統計)を重視 ・意見や見解は、発信者から判断
発信者の信頼性	・誰(どの組織)が発信した情報か ・発信者の専門性
発信者の立場	・マスコミの報道情報はバイアスがかかっていることが多い ・発信者の立場におけるメリット・デメリットを考える
環境・前提	・前提となる対象分野の専門的な知識 ・多数からのチェックされているか

2-2 視点１：情報の種類

情報の種類	・一次情報およびファクト(事実)や客観的情報(統計)を重視 ・意見や見解は、発信者から判断

- **一次情報およびファクト(ファクト)を重視する**
  - ファクト(事実)や、実際の観測に基づく統計情報等を集めること。
- **ファクト(事実)と仮説(意見や見解)を区別する**
  - 事実であるという根拠がない情報は、仮説として扱うこと。
- **知識・理論**
  - 知識や理論は、背景となる技術分野の成熟性による。
  - セキュリティは、まだまだ未成熟な分野であるため、確立された理論が少ないことに注意すること。

2-3 視点２：発信者の信頼性

発信者の信頼性	・誰(どの組織)が発信した情報か ・発信者の専門性

- **公的機関**
  - 政府機関、自治体等の公的機関。一般に信頼性が高い
  - 専門性については有識者が適切に関与している場合とそうでない場合がある
- **非営利団体**
  - 標準化団体等、公平な立場で情報を提供している
- **民間団体**
  - 共通の営利目的、競合団体との対立軸等のバイアスがあることに注意
- **民間企業**
  - 製品の宣伝等、企業の営利目的の影響を受ける
- **個人**
  - 個人の力量に依存するので、個別に判断する

2-4 視点３：発信者の立場

発信者の立場	・マスコミの報道情報はバイアスがかかっていることが多い ・発信者の立場におけるメリット・デメリットを考える

- **マスコミ・メディアの報道情報はバイアスがかかっていることに注意**
  - より世間の注意を引くニュース性の高い情報を報道する傾向がある
    例：「特定の事件に着目」→「類似の事件を多数報道」→「類似事件が増加しているように錯覚する」
- **発信者の立場からメリットがあるか**
  - 情報の内容が、発信者にとってメリットがある場合は、差し引いて考える
  - メリットがない場合は、信頼できる可能性が高い
- **著名な専門家であっても常に正しいとは限らない**
  - 専門家には間違ったことを言えないというプレッシャーがあり、無難な発言をしてしまう可能性がある
  - 専門家の発言を、メディアが部分的に切り取って報道することがある

2-5 視点４：環境・前提

環境・前提	・前提となる対象分野の専門的な知識 ・多数からのチェックされているか

- **情報を正しく理解するためには、対象分野の専門知識が必要**
  - 常に関連知識の習得に努力する必要がある
  - 自身の対象分野の理解度を客観的に認識すること
- **情報の認知度・公開範囲**
  - より多くの有識者の目に触れ、チェックされた情報は、信頼性が高い
- **書籍の読み方**
  - 最初の「謝辞」から、著者の所属するコミュニティが推測できる
  - 参考文献のリストから、書籍の記載内容や著者の視野の広さがわかる
  - (ある程度専門知識がある場合)自分で、同じ内容の書籍を書くと、どのような章構成となるかを考え、比較する(著者の意図や趣向についての気づきをえる)
  - 雑誌等は、広告の有無を見て、その分を差し引いて解釈する
    例：A製品の広告が載っている→A製品の評価記事は良く書かれているはず

参考 サイバーセキュリティ動向を知るための情報源(例)

#	情報源	内容
1	IPA 情報セキュリティ10大脅威 https://www.ipa.go.jp/security/vuln/10threats2021.html	毎年、有識者による投票により決定。主観的であるが、マクロな動向を把握することができる
2	JPCERT/CC http://www.jpcert.or.jp/	収集したインシデント情報等を、Weekly Reportや四半期レポートとして公開。
3	警察庁 サイバー犯罪対策プロジェクト http://www.npa.go.jp/cyber/	半期毎に、サイバー空間における脅威の情勢等の報告あり。警察庁が運営しているセンサー及び実犯罪に関する統計に基づき、速報性は低いが傾向への言及あり。
4	一般財団法人日本サイバー犯罪対策センタ(JC3) https://www.jc3.or.jp/index.html	サイバー犯罪に関する注意喚起情報が具体的に展開されている。海外機関との連携も行う。
5	IPA サイバー情報共有イニシアティブ（J-CSIP） https://www.ipa.go.jp/security/J-CSIP/index.html	様々な業界にわたる参加組織により共有された攻撃情報等について３か月毎に報告。攻撃の手口に関する解説情報も公開されている。
6	NICT NICTER http://www.nicter.jp/	ダークネットに送信されるパケットの観測を通して、攻撃対象のTCP/UDPポートや発信国の情報を知ることができる。
7	Piyolog http://d.hatena.ne.jp/Kango/	個人のブログであるが、的確かつ迅速な情報収集により、セキュリティ専門家もまとめサイトとして活用している。(2017年総務大臣奨励賞)
8	F-secure blog http://blog.f-secure.jp/	海外動向にも通じた専門家が自分の言葉で発信しているサイト。主観的であるが、先進的な動きに関するヒントが含まれいている。

・JVN等、脆弱性情報DB等や、市場調査等の間接的なものは対象外としている。
・ISAC等団体内のみでの情報共有や、情報発信の少ないサイトは対象外としている。