第64回諜報研究会

インターネットと社会のかかわり史

2025年3月22日

（株）IT企画　才所敏明

Mail：toshiaki.saisho@advanced-it.co.jp
Web：http://www.advanced-it.co.jp/
Facebook：https://www.facebook.com/toshiaki.saisho

経歴・活動内容

1970年4月～1994年12月　東京芝浦電気（東芝）・情報システム部門

技術開発・研究部門の計算機利用環境（ハード・ソフト・ネットワーク）の整備・高度化
技術開発・研究業務における先進的計算機利用技術の社内導入・指導・支援
＜インターネット：米国で発明、日本でも実証実験開始、東芝イントラネット構築推進＞

1995年1月～2007年9月　東芝・セキュリティ技術研究開発部門

セキュリティ技術センター長として、セキュリティ技術開発・事業支援活動推進
国プロの企画・提案推進、受託PJの指揮・指導
＜インターネット：商用サービス開始、急速な発展・多くの課題、国プロ研究開発推進＞

2007年10月　(株)IT企画を設立

［現職］(株)IT企画　代表取締役社長
事業支援活動（顧問・相談役）：ZenmuTech、System7
研究開発活動：中央大学研究開発機構、九州大学大学院

活動技術分野：
暗号・認証、秘密分散、本人確認技術（バイオメトリクス）、
電子メールセキュリティ、IoTシステム、ビッグデータ、AI、
暗号資産セキュリティ、ブロックチェーン技術、安心・安全な社会基盤
＜サイバー・フィジカル社会の安心・安全のための研究開発推進＞

 3

諜報研究会とのかかわり

(1)テクノインテリジェンスへの寄稿

①「暗号と社会のかかわり史」　2016年11月
http://www.npointelligence.com/Techno-Intelligence/Theme-C/Theme17(Cipher)/theme17.html

②「暗号と社会のかかわり史（その2）」　2017年7月
http://www.npointelligence.com/Techno-Intelligence/Theme-C/Theme17(Cipher)/theme17_2.html

③「暗号と社会のかかわり史（その3）」　2018年8月
http://www.npointelligence.com/Techno-Intelligence/Theme-C/Theme17(Cipher)/theme17_3.html

④「暗号と社会のかかわり史（その4）」　2019年10月
http://www.npointelligence.com/Techno-Intelligence/Theme-C/Theme17(Cipher)/theme17_4.html

(2)第31回諜報研究会での講演　2020年5月23日
「暗号と社会のかかわり史」
https://www.advanced-it.co.jp/2016_wp/wp-content/pdf/20200523angoV6.pdf

 4

本日のお話

インターネットと社会のかかわり史

補足説明1：サイバー攻撃について

補足説明2：インターネットと諜報活動

インターネットと社会のかかわり史

1．発明・実装（1961年～1984年）

2．日本上陸（1984年～1992年）

3．商用サービス開始（1992年～2002年）

4．社会基盤化（2002年～）

●3分

1．発明・実装（1961年～1984年）

(1)パケット通信の発明

＊1961年、アメリカのユタ州でテロにより3ヶ所の電話中継基地が破壊された

➔この事件により軍用回線も一時的に完全停止

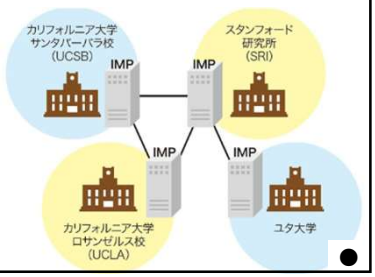
➔アメリカの国防総省は核戦争時に従来の電話網はまったく役に立たなくなると考え、新たな通信システムの研究に着手

＊アメリカ空軍のシンクタンクであるランド研究所の
ポール・バランが提唱（1962年に内部提示・1964年に最終提案）

➔パケット通信

(2)ARPANETの構築（世界最初のパケット通信網）

＊1969年に米国防総省のARPAが構築
（Advanced Research Projects Agency）
当初の基本プロトコルは
NCP（Network Control Protocol）
カリフォルニア大学：IBM360
スタンフォード大学研究所：SDS940
カリフォルニア大学ロサンゼルス校
：SDS SIGMA 7
ユタ大学：DEC PDP-10



●

(3)TCP/IPの発明

＊ヴィントン・サーフ氏とロバート・カーン氏によって発明、1974年5月仕様公開
タイトルは、「A Protocol for Packet Network Intercommunication」

＊TCP/IPは、パケット通信網を利用し、送信先へメッセージを送付するための、メッセージを一定のサイズに分割し、宛先の指定、メッセージを合成する順序を示す通し番号等の制御情報を含むヘッダの仕様を定めたもの

＊1981年9月に、TCP/IPがRFC（IETF）として文書化
TCPは「端末間の接続」、IPは「通信経路の選択・転送」

➔TCP/IP

(4)Ethernetの開発

＊米ゼロックスのパロアルト研究所（PARC）において、ロバート・メトカーフを中心に発明(1973年)、1974年にEthernetの公開実験に成功

＊その後、インテル社とDEC社が開発に加わり、1979年に3社の頭文字を取ったDIX仕様が制定（このDIX仕様が現在のEthernetで使われている仕様の元）

＊ローカルエリアネットワーク (LAN) 構築に使用されるネットワークプロトコル
このプロトコルにより、複数のデバイスがネットワーク経由でデータパケットを交換し、通信することが可能

(5)TCP/IPの標準実装

＊標準実装された最初のOSは、1983年に公開された
4.2BSD（Berkeley Software Distribution）と呼ばれるUNIX

＊BSD版UNIX：カリフォルニア大学バークレー校が
1977年にAT&Tのソースコードを元に開発し、配布を開始（大学等に急速に普及）

➔UNIX

(6)ARPANETが最初のインターネット
（現在のインタネットと同等の技術によるネットワーク）

＊DARPAがARPANETの開発プラットフォームにBSD版UNIXを採用、
DARPAの支援を受け、TCP/IPの実装を含む4.2BSDが開発され、1983年リリース

＊1983年に、ARPANETのプロトコルがNCPからTCP/IPへ移行

＊1983年に、ARPANETから軍事部門が切り離され、大学間を結ぶネットワークへ

＊1984年10月に、ARPANET接続拠点は1000を超えた

➔DARPAがインターネットの発明およびその普及を強力に推進

➔DARPA

（1961年～1984年）

主要なサイバー社会の事故・事件

1978年　初の迷惑メール（スパム）
DEC営業責任者がARPANET全ユーザ（393名）へ
DEC-10の宣伝メール

1981年　初のコンピュータウイルス“Elk Cloner”（AppleII）
50回目の起動で「詩」を朗読！

1983年　初のトロイの木馬“ARF-ARF”（IBM PC）
DOS ディスクのディレクトリを「ソート」する
➔ディスク上のすべてのファイルを削除し、
画面をクリアして、ARF – ARF と表示

●12分

2．日本上陸（1984年～1992年）

(1)JUNET（Japan University Network）の構築・稼働

＊1984年、東京工業大学、慶應義塾大学、
東京大学のコンピュータ（VAX/UNIX）を
電話回線経由接続、UUCPを利用したメール交換が可能に
➔日本最初のインターネット、JUNETが稼働

➔東芝の状況

＊1985年、電気通信事業法施行。
JUNET構築・拡大にもモデム利用が可能に。

●

（1984年～1992年）

(2)InetClubの設立

＊1985年、JUNET運用側（村井氏）からの、インターネットの産業界での
活用可能性についての実証実験への協力要請を受け、参加決定

＊1987年、国際科学技術通信網利用クラブInetClub発足（会長：石田氏）

➔メールの利用は実験の範囲に限定
（郵便事業を圧迫しかねないと危惧され、
業務使用は郵政省の許可を得られず）

＊1988年、企業・大学・公的機関のメンバによる
WIDE（Widely Integrated Distributed Environment）プロジェクト発足

＊1991年、米国でインターネットの商用利用が解禁

＊1994年、InetClub解散（1992年に、日本でISPが営業開始）

●

（1984年～1992年）

主要なサイバー社会の事故・事件

1985年　世界初のコンピュータウイルス“Brain”

ソフトウェアの販売会社を経営する兄弟
違法コピーにより感染、 感染ソフトを起動した場合に、
著作権者の連絡先が表示、ワクチン接種が必要な場合は
会社へ連絡するようなメッセージを表示

1988年　世界初のインターネットワーム“Morris”
損害を与える意図で書かれたのではなく、
インターネットの大きさを測る目的
➔1つのコンピュータに複数回にわたって侵入し、それぞれ
の侵入で起動されたプロセスがマシンに負荷を与え、
数千台のマシンを利用不可能な状態

1989年　日本初の国産ウイルス“Christmas”
感染後，12月25日が来るのをじっとパソコン内で待ちかまえ
12月25日になったらメッセージで驚かせる

収集ウイルス消滅事件＊ ●

（1984年～1992年）

1989年　世界初のランサムウェア/トロイの木馬” PC Cyborg“
　　フロッピーのラベルには「エイズ・ウイルス情報入門」
　　➔PCの起動回数が90回程度を越えるとすべてのファイル名を暗号化
　　PC Cyborg社の口座へ378ドルを送金する送金指定書を印刷
　　送金すると復号するプログラムが送られてきた

1991年　大量感染のブートセクタウイルス“Michelangelo”（500万台感染）
　　3月6日にコンピュータを起動した場合にのみウイルス感染
　　ハードディスク上のすべてのデータがでたらめな文字列で上書き

＜マルウェアの分類＞
　ウイルス
　　他のファイル、プログラムに寄生して自己増殖するプログラム
　ワーム
　　単体のプログラムのみで実行、自己増殖できるプログラム
　　ネットワークを介して他のコンピュータに侵入する
　トロイの木馬
　　有用なプログラムを装い、コンピュータに侵入するプログラム
　　単体のプログラムだが、自己増殖はしない　➔ウイルス感染ルート例 ●20分

3. 商用サービス開始（1992年～2002年）

(1)日本のISPが営業開始
＊1992年、AT&T Jensがインターネット接続サービス SPIN開始（UUCP）
＊1993年、IIJ がインターネット接続サービス開始（UUCP、専用線IP接続サービス）
➔2024年10月時点で、インターネット接続サービス事業者（ISP）は34社

(2)インターネットの個人利用の時代へ（研究者・技術者とは異なる一般の利用者）
＊インターネットのキラー・アプリ:①インターネットメール、②Webサービス
＊インターネット利用者（個人）の急増　アクセス端末（PC、スマホ）の普及
➔インターネット利用率、パソコン普及率、携帯電話・スマホ普及率推移

(3)インターネットメールの課題:送信者の匿名性
＊従来の利用者は限られた組織の研究者・技術者、
利用者の認証機能なしでも問題なし
➔不特定多数の利用者の時代になると、利用者の匿名性が大きな課題に
➔匿名性を皮肉った格言

＊インターネットメールの爆発的増大と膨大な数の迷惑メール
➔迷惑メールの量・割合の推移 ●

（1992年～2002年）

(4)WWW（World Wide Web）の登場

＊1991年、CERNのTim Berners-Leeが開発

欧州原子核研究機構（CERN）：世界最大規模の素粒子物理学の研究所
研究に関連するドキュメントやデータの研究者仲間との共有のために考案
当初は、テキストベースのブラウザ（東芝からアクセスし、可能性を確認）
HTML（HyperText Markup Language）もTim Berners-Leeが開発

(5)ブラウザの登場

＊1993年、NCSAがMarc Andreessen開発のブラウザMosaicを公開

NCSA：米国立スーパーコンピュー応用研究所

＊東芝として1990年代当初に訪問、解析結果の可視化技術・ソフトの調査

社内技術部門における解析ソフトの結果の画像表示ソフト調査の一環

＊1994年、モザイク・コミュニケーションズ

(Mosaic Communications Corporation) 設立
同年11月にネットスケープコミュニケーションズに社名変更

➔初期のブラウザの系譜＊

（1992年～2002年）

(6)Webサービスの普及

＊最初のWebサイト：世界では、1991年8月にスイスの欧州原子核研究機構が公開

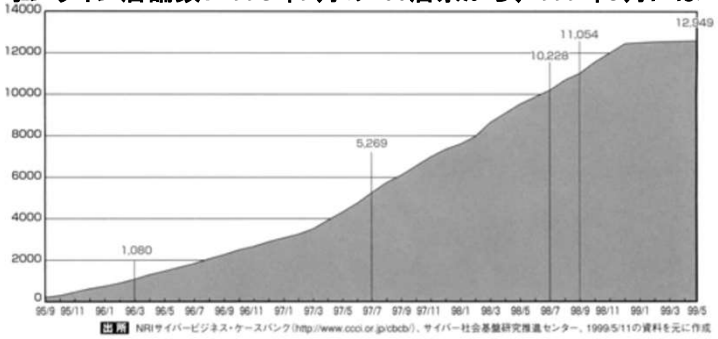
日本では、1992年9月に高エネルギー加速器研究機構（KEK）が公開

世界のWebサイト数：1995年には数万だったが、2002年ごろには数千万へ

＊最初のECサイト：世界では、アメリカのNet Market（1994年）

日本では、楽天の前身であるエム・ディー・エムが楽天市場（1997年：13店舗）

日本のオンライン店舗数：1995年9月の200店余から、1999年3月には12,549店へ



出典 NRIサイバービジネス・ケースバンク（http://www.cci.or.jp/cbcb/）、サイバー社会基盤研究推進センター、1999/5/11の資料を元に作成

1997年：楽天市場がスタート （ECモールの出現） https://netshop.impress.co.jp/node/4478

2023年：店舗数は455万を超えた

（1992年～2002年）

主要なサイバー社会の事故・事件

1994年　本格的な迷惑メールが出現
法律事務所が移民手続きサービスの宣伝のため、
大量にメールを送信するソフトウエアを開発し迷惑メールを大量送信

1995年　世界初のマクロウイルス：WORD“Concept”、1996年EXCEL“Laroux”
マクロ機能を利用し、新しいファイルの作成、ファイルの送信、
データの破壊、テキストの移動、ハードドライブのフォーマットなどを行う

1999年　急速・大量に拡散の
WORDマクロウイルスOutlookメールワーム“Melissa”
Wordのテンプレートに感染し、そのWordで開いた文書ファイルに感染
Melissaに感染したファイルを開いたユーザがOutlook97/98を使っている
場合には、アドレス帳に登録されているユーザに対して
Melissa感染ファイル添付したメールを自動送信（数日で10万台以上感染）

●

（1992年～2002年）

1999年　自治体による初めての大規模な個人情報流出
京都府宇治市住民基本台帳データ漏えい事件
MOディスクによる持ち出し、名簿業者がインターネット上で販売

2000年　日本の中央省庁のHP（Webサイト）改ざん（不正アクセス）
科学技術庁のHPが改ざん
＊日本人をののしり、ポルノサイトへ誘導
＊南京大虐殺をめぐる抗議文へ改ざん
多くの中央官庁やその関係団体のサイトが同様の抗議文へ改ざん

➔HP改ざんの手口例

2001年　WindowsのWebサーバー（IIS）のセキュリティホールを利用して侵入、
自己増殖するワーム“CodeRed”
マイクロソフトの IIS Webサーバが動作するコンピュータを攻撃
（35万台以上のサーバが感染）
感染先を求めて無差別に接続要求を出すため、多くのサーバが高負荷、
インターネットのトラフィックも急増、どのサイトへもつながりにくい状態へ

➔2000年前後の東芝のセキュリティ関連国プロ＊

●30分

（2002年～）

4．社会基盤化（2002年～）

(1)2002年に、インターネット人口普及率が50%を超えた！

➔インターネットが日本のサイバー社会の基盤の地位を確立し更に発展フェーズへ

➔インターネット利用率、パソコン普及率、携帯電話・スマホ普及率推移

(2)クラウドサービスの出現・発展

1997年　南カリフォルニア大学の教授ラムナト・チェラッパが
クラウドコンピューティングという概念を提唱

2006年　Amazonが企業向けのクラウドサービス「Amazon EC2/S3」の提供を開始

2008年　Googleが「Google Cloud Platform」を提供開始

2010年　Microsoftが「Microsoft Azure」を提供開始

2018年　クラウド・バイ・デフォルト原則：政府が情報システムを調達する際は、
クラウドサービスの利用を第一候補として、その検討を行う

➔クラウドの利用状況の推移

●

（2002年～）

(3)Webサービスによるオンライン店舗の急増

インターネット利用者の急増とともに、オンライン店舗も急増（2023年455万店舗）

➔多くのオンライン店舗が、多くの利用者の登録情報（名前、住所、・・・）を管理

➔オンライン店舗やECモール（Webサイト）への攻撃が多発

➔主要なサービスの利用者数＊

多発したWebサイトからの個人情報の漏洩事件

2005年　クラブツーリズムおよび静岡新聞の個人情報漏洩事件
（不正アクセスにより、約9万人分および約4万人分の顧客情報）

2010年　サミーネットワークスの個人情報漏洩事件
（不正アクセスにより、約173万人分）

2014年　ベネッセの個人情報流出事件（流出した顧客情報は最大で3504万件）
DBシステム管理を担当していた外部事業者のエンジニアが不正に持ち出し

2023年　LINEヤフー利用者の個人情報・通信情報を含む情報の漏洩（約51万件）
共通の認証基盤を利用する韓国のNAVER Cloud株式会社の委託先企業
の従業員が所有するパソコンにマルウェアに感染したことが原因

2024年　積水ハウスの 顧客や従業員など29万人分の個人情報が漏えい
サーバの脆弱性を利用され、SQLインジェクション攻撃を受けた

➔EC市場の拡大と個人情報漏洩件数推移

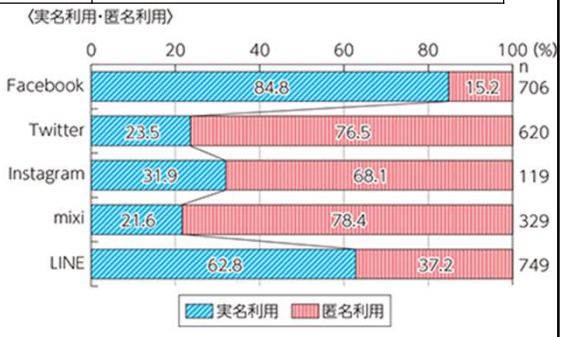
●

（2002年～）

(4)Social Network Serviceが次々とサービス開始

開始時期	主要SNS	国内月間アクティブ利用者数
2004年	mixi	2800万人（最新HP上で公表）
2007年	YouTube（日本）	7000万人（2020年10月）
2008年	Facebook（日本）	2600万人（2019年7月）
	Twitter（X）（日本）	4500万人（2017年10月）
2010年	Instagram（日本）	3300万人（2019年6月）
2011年	LINE	9400万人（2022年12月）

https://lab.kuas.ac.jp/~jinbungakkai/pdf/2018/p2018_01.pdf
https://programming-shikiho.com/major-sns-lists/



SNSの利用は
匿名による利用が主流

誹謗・中傷やフェイクニュース、無責任な発言・いいねの氾濫

（2002年～）

多発した誹謗・中傷事件

1998年　お笑い芸人のスマイリーキクチさん、20年以上、1989年の「女子高生コンクリート詰め殺人事件」の実行犯、というデマで誹謗中傷を受けた
(2008年、特に悪質な書き込みを行った17歳から45歳の男女18人が一斉検挙)

2005年　学校裏サイトによる誹謗中傷で女子学生が退学
（元同級生とその両親を相手取り、2008年に200万円の慰謝料を求める民事訴訟を提訴）

2011年　女優の春名風花さんが、9歳の頃から10年間、SNS等で誹謗中傷を受けた
（2018年10月にプロバイダに発信者の情報開示を求める訴訟を提訴。1年後開示命令。）

2019年　あおり運転を行い、さらに車から降車後、暴行を加えるという事件の共犯者（同乗者）、というデマで女性が誹謗中傷を受けた
(女性は情報を拡散した元市議会委員に110万円の損害賠償を求めて提訴、東京地裁は33万円の支払いを命じた)

2020年　女子プロレスラーの木村花さん、「テラスハウス」での言動に対し、誹謗中傷受け自殺　➔総務省：違法・有害情報相談センターの相談受付状況

2024年　日本で初めて、SNSの「いいね」が中傷投稿に当たると確定。
杉田議員は2018年に、ジャーナリスト伊藤詩織さんの性的被害に対し、名誉を侵害するようなツイート25件に対して、「いいね」押した。

（2002年～）

主要なサイバー社会の事故・事件

2004年　日本でフィッシングメール（JCB、VISAのクレジットカード番号等を入力させるサイトへの誘導メール）
➔標的型攻撃手口例

2005年　日本で標的型攻撃メール（外務省職員を詐称して、ウイルス付きWordファイル添付のメールが複数の官公庁へ）

2007年　エストニアがロシアから大規模なDDoS攻撃、政府機関、銀行が機能停止
8万台のPCが乗っ取られ構築されたボットネットからの攻撃
➔DDoS攻撃手口例

2009年　大企業（JR東日本・ホンダ・ローソン・京王グループ等）のWebサイト改ざん
正規のWebを改ざんし不正サイト「gumblar.cn」へ誘導し、
無差別にウイルスをダウンロードさせるドライブ・バイ・ダウンロード攻撃

2012年　政府機関を狙った水飲み場攻撃
Web サイト「47行政ジャーナル」が標的となり乗っ取られ、
特定の組織に属する人物がサイトを閲覧した際にウイルス感染が発生

（2002年～）

2015年　日本年金機構の個人情報流出事件（125万件の年金情報が流出）
「『厚生年金基金制度の見直しについて（試案）』に関する意見」という件名の標的型攻撃メールが発端

2016年　最大規模のDDoS攻撃
Akamaiのサービス上のセキュリティブログKrebs On Securityを攻撃
38万台のIoT機器（ボットネット）による分散型サービス妨害攻撃（DDOS）
（「ミライ」（Mirai）ウイルスのソースコードがインターネットにて公開された）

2019年　三菱電機がAPT攻撃を受け防衛情報を含む情報が流出
サーバのログが改ざんされていて、攻撃は数年前から行われていた可能性

2022年　ランサムウェア攻撃を受けトヨタ自動車の全工場がライン停止
トヨタ自動車は国内全14工場28ラインを停止
部品仕入れ先の協力企業・小島プレス工業がサイバー攻撃を受けたため
データを人質にして「身代金」を要求する「ランサムウェア」の手口
その間に約1万3,000台の自動車の生産が止まった

2022年　ランサムウェア攻撃を受け春日井リハビリテーション病院5万人分の電子カルテが暗号化、閲覧不可に
VPNの脆弱性から電子カルテ等の保管サーバーにランサムウェア攻撃
復旧に数千万の費用と4か月余りを要した

（2002年～）

社会基盤としてのインターネットの課題

①インターネットの課題：匿名性
＊サイバー社会のセキュリティを強化し，
サイバー社会での無責任な利用者の多さ、
サイバー社会の犯罪者・攻撃者優位の現状を改善することが必要
＊そのための重要な対策の一つが，
サイバー社会に参加する利用者の確実な本人確認と，
様々な活動における利用者の匿名性と特定・追跡性の両立

②インターネットの課題：個人情報の集中管理
＊個人情報・プライバシー情報のクラウド上での集積を削減し、
犯罪者・攻撃者の活動を抑制、被害を最少化することが必要
＊そのための重要な施策の一つが、
個人情報・プライバシー情報の自己利用制御の推進

➔推進中の研究開発テーマ
「安心・安全なブロックチェーンサービス基盤（SSBSI）」 ●45分

補足説明1：サイバー攻撃について

The Internet's founders saw its promise
but didn't foresee users attacking one another ... Vinton G. Cerf
（インターネットの創始者たちはその可能性を認識していたが、
ユーザが互いに攻撃し合うことは予見していなかった。）

1. 主要なサイバー攻撃

2. サイバー攻撃の目的

3. 主要なサイバー攻撃主体

●

主要なサイバー攻撃

1. マルウェア
   ウイルス，ワーム，トロイの木馬
2. ランサムウェア
   暗号化ランサムウェア，ロッカーランサムウェア，ドックスウェア
3. ゼロデイ攻撃
   マルウエア/ランサムウェア対策ソフトがリリースされる前の攻撃
4. 標的型攻撃（標的型メール・水飲み場）（vs　ばらまき型攻撃）
   攻撃対象（標的）の状況を調査の上、なりすまし攻撃
5. サプライチェーン攻撃
   攻撃対象（標的）と取引のある組織経由の攻撃
6. DoS/DDoS攻撃（サービス妨害攻撃）
   攻撃対象（標的）のサーバやネットワークへ高負荷をかけて
   サービスを妨害する攻撃
7. APT攻撃（Advanced Persistent Threats）
   特定の組織や個人を狙った長期間にわたる巧妙なサイバー攻撃

サイバー攻撃の目的

PA：自己顕示欲
愉快犯的な犯行や自身が持つ技術力を見せつけたいといった自己顕示欲を満たす目的のもの

PB：金銭の収奪
個人・組織のシステム・情報・サービスを人質にとったり、攻撃予告による脅迫により、金銭を要求するもの

PC：機密情報を窃取
特定組織の機密情報を窃取する産業スパイなど組織犯罪に類するもの

PD：政治的な主張
攻撃を通じて、政治的な主張を行うことを目的とするもの

サイバー攻撃

主要なサイバー攻撃主体

EA：愉快犯や悪意のある個人 ➔ PA：自己顕示欲、PB：金銭の収奪

EB：サイバー犯罪組織 ➔ PB：金銭の収奪

➔サイバー攻撃ビジネスのエコシステム（分業化）

EC：産業スパイ ➔ PC：機密情報を窃取

ED：ハクティビスト ➔ PD：政治的な主張

Anonymous（アノニマス）、KILLNET（キルネット）

EE：国家支援組織 ➔ PC：機密情報を窃取、PD：政治的な主張

➔ 補足説明2：インターネットと諜報活動 へ

●50分

諜報活動

補足説明2：インターネットと諜報活動

1．サイバー攻撃による諜報活動

APT（Advanced Persistent Threats）攻撃

情報を盗むことが主な目的であり、

データの改ざんやサーバのっとりのケースも

長期的に情報を入手する目的のため、

攻撃・侵入・活動していることに気づかれない工夫

2．OSINT（Open Source Intelligence）による諜報活動

秘密ではない、様々の公開情報の収集・分析による、諜報活動

インターネットの普及とともに発展

●

諜報活動

サイバー攻撃による諜報活動
APT攻撃の被害事例

2009年 「Operation Aurora」

「オーロラ攻撃」「オーロラ作戦」などとも呼ばれるAPT攻撃事件。中国のElderwoodグループが中心になって実行された攻撃。ゼロデイ攻撃によりトロイの木馬を仕込む手口で、30社以上が被害に遭い、メールのアカウントやパスワードなどを盗まれている。

2010年 「イランの核開発施設の被害」

アメリカとイスラエルが「Stuxnet」と呼ばれるマルウェアを使い、イランの核開発施設を攻撃した事例。この結果、ウラン濃縮に用いる遠心分離機が壊れ、イランにおけるウラン濃縮化技術の開発が遅れた。

2011年 「防衛関連産業の被害」

世界中の防衛企業がAPT攻撃を受け、アメリカやイスラエルのほか、日本の三菱重工も被害を受けた。原子力発電プラントやミサイルの開発研究所などを標的とされていた。標的型攻撃メールによる侵入、外部から制御し機密情報などを盗み出す手口。

2015年 「日本年金機構の情報漏えい事件」

日本年金機構が攻撃され、約125万人分の個人情報が漏えいした事件。標的型メール攻撃が3回にわたって送られていたことが分かった。同事件は、日本においてAPT攻撃の脅威が広く知られるきっかけとなった。警視庁が2018年5月20日に、時効を迎えた日本年金機構の情報流出事件の操作を打ち切り、事実上真相解明を断念。

諜報活動

2017年「WannaCry」（Microsoft Windowsを標的としたワーム型ランサムウェア）

北朝鮮との関係を疑われるLazarus Groupの関与が指摘されている。同グループは2009～2012年の「トロイ作戦」や2014年のソニー・ピクチャーズへの攻撃で知られる。またWannaCry同様、2015年にベトナムのTien Phong Bankが100万ドルを盗まれた事件や2017年に台湾の遠東国際商業銀行が6000万ドルを盗まれたと報じられた事件など、近年は金融機関を狙った活動が顕著で、APT38との関係も指摘されている。

2020年 「日本の電機メーカーへの大規模サイバー攻撃」

三菱電機がAPT攻撃を受けた。この攻撃は、まず脆弱性を利用したゼロデイ攻撃で子会社の端末へ侵入し、ネットワーク上で拡散、クラウドサービスや関連サーバにログインし、個人情報や機密情報を窃取。

マルウェアに感染したと疑われる端末は130台以上で、端末のメモリー内で活動するファイルレスマルウェアという手法が用いられており、最初の感染から検知するまでに3カ月以上を要した。

採用応募者情報や従業員情報、技術資料といった情報に加えて、安全保障上の機微な情報が流出した可能性があると防衛省により発表。この安全保障に影響を及ぼす可能性のある流出情報は59件にのぼるとされている。

諜報活動

サイバー攻撃による諜報活動
主要な国家支援組織

APT28　別名：Fancy Bearなど。

APT28は、ロシアの軍参謀本部情報総局（GRU）に紐づけられる脅威グループで、少なくとも2004年から活動している。特に有名なのは、2016年の米国大統領選挙において、民主党のクリントン陣営や民主党関連機関・個人を狙ったサイバー攻撃を通じて情報漏洩などを行い、選挙に干渉した点。これについては、米国政府が詳細な調査レポートを公表。

APT41　別名：MISSION2025，Wicked Pandaなど。

APT41は、中国に支援されていると見られるサイバー諜報グループであり、同時に金銭目的の活動も行っている。少なくとも2012年から活動しているとされ、医療、通信、テクノロジー企業などを標的とすることで知られている。

Lazarus Group

Lazarus Groupは、北朝鮮の工作・諜報機関である軍偵察総局（RGB）に関連づけられる脅威グループで、少なくとも2009年頃から活動している。別名はLabyrinth Chollima、Guardians of Peaceなど。2014年に起こったSony Pictures Entertainmentへの大規模なサイバー攻撃に携わった。

諜報活動

OSINTによる諜報活動とは

1. HUMINT（Human Intelligence）
   a. 報告
   b. 尋問
   c. スパイ活動

2. SIGINT（Signals Intelligence）
   a. COMINT（Communications Intelligences）
      電子通信情報を収集（傍受）し分析
   b. ELINT（Electronic Intelligence）
      レーダー、通信、無線送信などの電波を収集し分析

3. OSINT（Open Source Intelligence）
   a. 学術論文などの公開された情報
   b. ニュース・新聞・メディア放送など
   c. Internet上の公開情報

諜報活動

OSINTによる諜報活動　第１世代

(1)第一次世界大戦時のフランス

敵国が自国の（＝オープンソースの）報道を有利に利用できることを前提で、憲兵隊の防諜活動の組織化を行っていた。

(2)第二次世界大戦時の米国

1941年に、CIA（中央情報局）の前身であるOSS（Office of Strategic Services、戦略情報局）が開設した際から、OSINTを取り入れていた。

OSSの調査分析部門は、世界中から何十もの新聞、雑誌、新聞の切り抜き、ラジオ放送のレポートを収集し、敵に関する重要な情報をまとめていた

OSSはこれらの情報から、ナチスの新しい戦艦や航空機の画像などを取得していて、それらは入念に照合されまとめられ、OSSがナチスの軍事作戦を含む様々な状態を評価するために使用されていた。

第二次大戦までのOSINTは第１世代で、敵の意図に関する戦略的情報を得るために、敵国の放送を分析するなどの外国メディアの物理的な検索と分析が主なもの。米国ではCIAが管轄していたForeign Broadcast Information Service（FBIS）などの機関が主に担当し、その主なタスクはドキュメントの検索と翻訳・収集された資料の内容分析。

諜報活動

OSINTによる諜報活動
第２世代（デジタルOSINT）

(1)急速に発展したインターネットにより、1990年代後半からOSINTの情報源は、インターネット上のデータへ。

(2)米国では2005年、FBISに代わってオープンソースセンター（OSC）という組織が創設され、「デジタルOSINT」として専門の研究を行うようになり、これがOSINTの第２世代の始まりに。

(3)第二世代OSINT（デジタルOSINT）の主要な情報源

- Webで公開されている情報やニュース記事
- GitHubなどのソースコード共有や会話の場所
- SNS
- 脆弱性データベース
- 公開されている既存の脆弱性のPoC

  脆弱性を突いてシステムを攻撃するプログラムを作成し、実際に攻撃が成功することを実証すること
- ゼロデイ攻撃に関する公開された情報

諜報活動

＊2022年：親ロシア派の地元ジャーナリストが8月8日に
メッセージアプリ「Telegram」に投稿した写真

写真にワグネルの拠点が写っていたせいで、拠点の所在地が露見したようだ。後に写真は削除されたが、その1枚には住所が写り込んでいた。ウクライナ軍は、この情報を利用、数日後、ワグネルの拠点はウクライナ軍によってがれきの山と化した。

＊2022年：ウクライナのニュース番組の映像

新ロシア派のOSINT集団がウクライナのニュース番組の映像を使って、キーウにある軍需工場の場所を特定した。この工場は後にロシア軍のミサイル攻撃を受け、3人の民間人が亡くなった。

＊2023年：ロシア軍の兵士がSNSにアップロードした写真

ロシアによるウクライナ侵攻では、2023年1月2日（現地時間）にロシア軍の兵士がSNSにアップロードした写真を基に、ウクライナ軍がロシア軍の正確な位置を把握して高機動ロケット砲システム（HIMARS）による攻撃に利用したというケースが報告されている。

●

諜報活動

ベリングキャット（Bellingcat）
オランダに本拠を置く調査報道機関

オランダに本拠を置く調査報道機関（2014年設立）

ウェブサイトやSNSで公開されている情報を収集・分析するオープン・ソース・インテリジェンスを特徴（ハッキングや秘密の情報源は使わない方針）

ウクライナ東部紛争の最中に起きた2014年のマレーシア航空17便撃墜事件で、親ロシア派が9K37ブーク地対空ミサイルを旅客機に誤射してしまったことを解明し、これが公的国際捜査機関による起訴につながったことで注目された。

2018年の元ロシア人二重スパイのセルゲイ・スクリパリ暗殺未遂事件では、公開情報や内部告発者から提供されたデータも活用して、関与したロシア連邦軍参謀本部情報総局（GRU）工作員チームを割り出した。

2020年のアレクセイ・ナワリヌイ暗殺未遂事件では関与したロシア連邦保安庁（FSB）工作員チームの割り出しをしている。

また、2022年ロシアのウクライナ侵攻にについても、戦争法違反である捕虜・民間人への虐待・残虐行為について調査・報道をしている。（ブチャの虐殺、ウクライナ人捕虜への残虐行為を行ったグループの特定、ウクライナの住宅・民間インフラへの精密誘導ミサイル攻撃を管理するロシア軍部隊と兵士33人の特定など）

●

諜報活動

OSINTによる諜報活動
これからのOSINT（第３世代）

(1)OSINTの情報収集と分析プロセスのほとんどが自動化（AI応用）

＊自動的データ収集

世界中で生成されるデータの量は 2025年までに 175 ゼタバイト
（10億テラバイトまたは1兆ギガバイト）に増加すると予想

＊高度なパターン認識　＊予測分析

(2)国家安全保障における活用の動き

＊米国 国家情報長官室・CIA 2024-2026年のOSINT戦略

Goal: Coordinate Open Source Data Acquisition and Expand Data Sharing
Goal: Establish Integrated Open Source Collection Management
Goal: Drive OSINT Innovation To Deliver New Capabilities
Goal: Develop the Next-Generation OSINT Workforce and Tradecraft

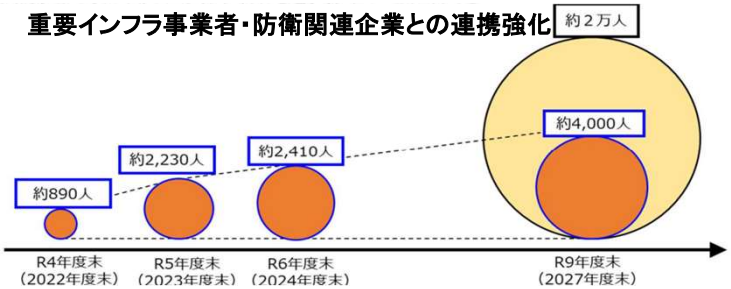
＊「オープンソースから得られる情報と
諜報機関が収集する情報の立場が逆転した」

（2024年5月の米国防情報局・リックマン副長官の発言）

OSINTによる諜報活動　日本では？

防衛力整備計画（令和4年 12 月 16 日　閣 議 決 定）より

- 体制の大幅な拡充 サイバー専門部隊を約4，000人
（サイバー関連業務を含む総サイバー要員約20，000人）
- 高度人材の確保・育成 システム通信・サイバー学校への改編 など
- 専門能力の高度化 同盟国・パートナー国との連携、
共同訓練の実施（米、英、豪、NATO等）
- スレット・ハンティング機能の強化 など
- 自衛隊の能力を生かした国全体のセキュリティ強化への貢献
重要インフラ事業者・防衛関連企業との連携強化



https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/siryou7-4.pdf

終

（ご清聴、ありがとうございました）

2025年3月22日

（株）IT企画　才所敏明
Mail：toshiaki.saisho@advanced-it.co.jp
Web：http://www.advanced-it.co.jp/
Facebook：https://www.facebook.com/toshiaki.saisho

●70分