7C-03

# 遠隔操作によるサイバー攻撃の被害報告とその対策

今野 陽子 †

財団法人独立書人団 †

## 1 はじめに

サイバー空間におけるデータ活用が普及する一方で，情報保護の為の新たな課題に直面した．直近4年間，身近なところで発生した被害は遠隔操作を応用したものであり，未だ解決に至っていない．その技術的側面を整理し，物理的や身体的な影響を提示して，人工知能やデータサイエンスを通しての考え方を見出す．

本研究では，近年のデータ活用状況とサイバー攻撃に関する動向(2 章)，実際に起きた被害事例(3 章)，それらに対する対処方法(4 章)，利用されている技術の調査・分析(5 章)について説明する．それらによって想定される問題を提示し，人工知能の技術開発に携わってきた経験からの考えを考察する(6 章)．

## 2 背景 ーサイバー攻撃の動向

サイバーセキュリティとは，コンピュータやネットワークに構築された仮想空間上のセキュリティのことである．近年のサイバー攻撃の動向として，特にマルウェアによる被害が拡大している．攻撃の対象は無差別型，標的型がある．感染経路は特定 Web サイトの閲覧，メールに添付されたファイルのダウンロードによるものがある．感染した端末からは情報が搾取され，データ改ざんの修復の見返りとして金銭が要求されるケースがある．

ネットワークカメラやミリ波イメージングなどのレーダーセンサによるモニタリング技術が浸透する一方で，位置情報と映像によるプライバシー侵害が懸念される．それらを利用した情報搾取が報告される．[1]

無線 LAN の閲覧，接続機器の特定，端末間を接続する機能が複数あり，設定が容易である．[3]

情報保護のため，これらを管理・規制するための法律が複数策定されている．電波法，個人情報保護法，が挙げられる．

## 3 被害事例

PC 端末あるいはサーバーがオンラインの時，接続グループからのログインによって，またはパスワード設定前の初期段階に接続され，資格情報の登録により随時接続可能な端末に設定される(図 1)．また，特定のフォルダが配置されて，対象機器の未使用中のアプリケーションがバックグラウンドで実行された場合のログが出力される(図 2)．必ずとは限らないが，別の管理者ユーザの登録，Bluetooth の有効化，モバイルホットスポットによるテザリング，端末間の同期設定が行われる場合がある(図 3)． 計算機資源の分割や設定変更が起きることは，技術者にとって重要な問題である．

図 1. 登録された資格情報マネージャーの画面


| | 配置されるパス |
|---|---|
| 1 | C:¥ $SysReset |
| 2 | C:¥ $WinREAgent |
| 3 | C:¥ $WINDOWS.~BT |
| 4 | C:¥ Intel |
| 5 | C:¥ PrefLogs |
| 6 | C:¥ ProgramData |
| 7 | C:¥ Users¥ パブリック |
| 8 | C:¥ Users¥ default |

表 1. 配置されるファイルのパス(例)

汎用資格情報とは，PC に保存されるユーザのログイン情報の一種であり，リモートデスクトップに利用する．[4] 汎用資格情報のログが最初に発見されたのは 2016 年で，PC 所持者が設定したものではなかった．ログインにはパスワードが必要であるが．2019 年から，遠隔地にいる人物の音声に，まるで携帯電話から話しかけるように流れるようになった．これらは電界強度の測定から，電波を利用した音声であると判明し，水中，上空(航空機)に及んだ．2021 年から，組織内の文書と類似内容のファイルが，知らない間に組織ポータルに置かれるケースが発生した．一連の出

Example of Damage Caused by Remote Access Cyberattocks and the Measures
†Yohko Konno: Dokuritsushojindan

来事の発生場所は，特定のプログラムの開発現場から始まり，住居，複数の組織に，時間帯は年中24時間に影響が拡大した．


図 2. 同期設定

## 4　対処方法

端末やサーバーなどのシステムに，前述のような意図しない設定変更が確認された場合，個人や組織内で設定変更を監視しブロックする方法と，接続グループに対して管理や規制を促す方法がある．

前者について，特に以下の対処方法が求められる．

A) 対象機器オペレーティングシステム(対象と想定される媒体)のログインパスワードの設定方法を強化．(都度変更．生体認証など)
B) 機器やネットワークを特定する ID やアカウント情報の設定方法を強化．
C) 資格情報の登録の機能を無効化．(コンピュータの管理のサービスの項目の停止と無効化)
D) 配置されたファイルを除外し使用不可にする．
E) 権限や同期などを本来の目的の設定に戻す．
F) 現象と対策を共有する．

しかしログイン時の情報をキーロガーなどによって取得される場合，侵入を回避することは難しい．接続グループに対して停止を説得する場合には，合意が図れない状況において，外部組織のシステムへの介入は不可能に近いため，専門の国家機関に証拠と併せて技術的背景，解決方法を相談するのが相応しいと考えている．数十回の調査報告を経て，専門家に相談可能な体制が整えられたことは進展である．

## 5　遠隔操作の利用技術

長期に及ぶ事象の観測から，侵入される目的は，監視，奪取，抑圧に整理できる(表 2)．リモートアクセスを導入するためには，法律の遵守が大切である．電磁波強度を表す 1V/m とは，金属平板を平行に 1m 離して 1V の電圧をかけた時，板の間に生じる電磁界の大きさである．表 3 の状況下において，昆虫や小動物が屋内で亡くなった．

## 6　関連する問題と要因について

サイバー攻撃の観点から，遠隔から残された不正アクセス履歴をもとに，受けた被害の整理を行った．一方的な攻撃に対して，解決のためには，証拠の有無ではなく，個人のセキュリティに対するリテラシーの向上，および社会的な観点で捉えた議論の推進，両方が必要であると認識するに至った．現在も継続的に，利用技術の解明と対策について取り組んでいる．その一環として電波受信機を応用した測定方法を検討している．

データサイエンティストの素養を持つ人材を求めるベンチャービジネス，人工知能技術の開発を推進する環境では，それらに関心を持つ人，人材を勧誘する人が集まった．3 章で紹介した状況が未だ停止に辿り着かないのは，社会実装の理念を共有できないためである．新しい連携の価値を模索し開拓する一方で，人材育成の体制を，徹底的に社会から学ぶ姿勢が大切である．これが組織の課題を解決する一助となると考える．

A) 情報システムの保守運用
B) モニタリング／センシングデータに対する価値の考え方
C) 安全性を優先する考え方
D) 公共のための技術を育てる姿勢

| | 事象項目 | 監視 | 奪取 | 抑圧 |
|---|---|---|---|---|
| 1 | システム侵入・システム出入り | ● | | |
| 2 | 機能の設定変更 | | ● | |
| 3 | 接続・画面監視 | ● | | ● |
| 4 | 情報搾取・情報漏洩 | | ● | ● |
| 5 | 改ざんと共有・配信 | | ● | ● |
| 6 | 実在人物なりすましメールアドレス | | ● | ● |
| 7 | 盗聴 | ● | | |
| 8 | 盗撮 | ● | | |
| 9 | 遠隔から音声で伝達・依頼 | | | ● |
| 10 | 脳内音声技術（思考盗聴） | ● | | |
| 11 | 電磁波照射 | | | ● |

表 2. 観測される事象と接続グループの目的

| | 電子機器　観測項目 | 電界強度 [V / m] |
|---|---|---|
| 1 | 通常・屋内外　(電気カーペット有無) | 0.03　～　0.06 |
| 2 | PC，無線LAN，携帯電話　利用 | 0.05　～　0.20 |
| 3 | テレビ　接近 | 0.10　～　0.20 |
| 4 | 電子レンジ　接近 | 0.20　～　3.00 |
| 5 | 電波音声関係　侵入 | 1.50　～　14.00 |
| 6 | 感電　(体調不良・しびれ・痛み) | 1.00　～　20.00以上 |
| 7 | 屋外　歩行時 | 1.00　～　3.00 |

表 3. 電界強度の測定結果(機種 SATO-TECH EMS-831SD)

## 参考文献

[1] 防衛基盤整備協会，中国のサイバー攻撃の実態(2017)