

テクノロジーと災害

—セキュアな超スマート社会(Society 5.0)に向けて—

加 藤 将 貴

目 次

1. はじめに
2. サイバー犯罪の情勢
3. サイバー空間における脅威の類別
4. 超スマート社会(Society5.0)とサイバー攻撃

1. はじめに

世界中でサイバー攻撃が増加している。サイバー攻撃の対象は個人、企業、国家などあらゆる範囲にわたり、容易に国境を超え、被害もデータの破壊や金融資産の詐取といった従来のケースに留まらない。2010年にはイランの核燃料濃縮施設の遠心分離機を破壊するといった物理的被害をも引き起こしているのである。最早、サイバー攻撃はコンピュータの中だけに閉じられたものではない。一方、社会はサイバー空間とフィジカル空間とを高度に融合させる、超スマート社会(Society5.0)^①へと移行しつつあり、サイバー攻撃への対処は尚以て重要性を増すだろう。

本稿では、我が国におけるサイバー犯罪の情勢を確認した後、現在主流となっているサイバー攻撃の種類や被害事例について概観し、新たな社会として到来する超スマート社会(Society5.0)におけるサイバー攻撃について示唆を得ることを目的とする。

2. サイバー犯罪の情勢

我が国ではサイバー犯罪⁽²⁾を「コンピュータ・電磁的記録対象犯罪」「コンピュータネットワーク利用犯罪」「不正アクセス禁止法違反」の3類型に分類しており、匿名性が高い、証拠が残りにくい、時間・場所の制約が少ないといった特徴を持つ犯罪である。近年のサイバー犯罪について警察庁から公表されている「サイバー空間をめぐる脅威の情勢等について」を引照しながら情勢を把握する。

表1はサイバー犯罪検挙件数の推移と内訳を示したものである。サイバー犯罪は増加傾向にあり、2018年（平成30年）中のサイバー犯罪検挙件数は9,040件と過去最多であった。手口も年々巧妙化している。

表1 サイバー犯罪検挙件数の推移と内訳

年次（西暦）	2014	2015	2016	2017	2018	2018上	2019上
年次	H26	H27	H28	H29	H30	H30上	R01上
不正アクセス禁止法違反	364	373	502	648	564	181	182
不正指令電磁的記録に関する罪 コンピュータ・磁的記録対象犯罪	192	240	374	355	349	164	175
児童買春・児童ポルノ法違反	1,741	1,881	2,002	2,225	2,057	1,010	1,136
詐欺	1,133	951	828	1,084	972	531	464
著作権法違反	824	593	586	398	691	191	118
上記以外の罪種	3,651	4,058	4,032	4,304	4,407	2,174	2,168
合計	7,905	8,096	8,324	9,014	9,040	4,251	4,243

※上は上半期の数

出所：警視庁「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について 統計データ」[online] <https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（最終閲覧 2019年12月31日）

表2は不正アクセス禁止法違反の検挙件数の推移を示したものである。2018年（平成30年）中の不正アクセス禁止法違反の検挙件数は564件であり、2017年（平成29年）と比較すると減少したが、近年の特徴である仮想通貨交換業者等への不正アクセス等による不正送信事犯は、認知件数が169件、被害額が約677億3,820万円相当と大きな被害となっている。

表 2 不正アクセス禁止法違反の検挙件数の推移

年次（西暦）	2014	2015	2016	2017	2018	2018上	2019上
年次	H26	H27	H28	H29	H30	H30上	R01上
検挙件数	364	373	502	648	564	181	182

※上は上半期の意

出所：警視庁「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について 統計データ」[online] <https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（最終閲覧 2019 年 12 月 31 日）

表 3 は不正指令電磁的記録に関する罪及びコンピュータ・電磁的対象犯罪の検挙件数推移を示したものである。不正指令電磁的記録に関する罪及びコンピュータ・電磁的対象犯罪は電磁的記録不正作出・毀棄等、電子計算機損壊等業務妨害、電子計算機使用詐欺及び不正指令電磁的記録作成等について罰するものである。2018 年（平成 30 年）中の検挙件数は 349 件（うち、不正指令電磁的記録に関する罪の検挙件数は 68 件）となっており、2016 年（平成 28 年）に急増したが、その後、微減となっている。コンピュータ・ウィルスは不特定多数に被害が及ぶことも多く、また被害者が知らぬ間に加害者になってしまうこともある点が特徴である。

表 3 不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙件数の推移

年次（西暦）	2014	2015	2016	2017	2018	2018上	2019上
年次	H26	H27	H28	H29	H30	H30上	R01上
不正指令電磁的記録に関する罪	28	45	58	75	68	36	13
電子計算機使用詐欺	108	157	281	228	188	93	124
電磁的記録不正作出・毀棄等	48	32	24	39	84	33	33
電子計算機損壊等業務妨害	8	6	11	13	9	2	5
合計	192	240	374	355	349	164	175

※上は上半期の意

出所：警視庁「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について 統計データ」[online] <https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（最終閲覧 2019 年 12 月 31 日）

表4、表5はインターネットバンキングに係る不正送金事犯の発生件数と被害額の推移を示したものである。サイバー犯罪も時代により傾向があり、数年前に被害が大きかったインターネットバンキングの不正送金については、セキュリティ対策が進んだこともあり件数・被害額共に大幅に減少傾向にある。

表4 インターネットバンキングに係る不正送金事犯の発生件数の推移

年次（西暦）	2014	2015	2016	2017	2018	2018上	2019上
年次	H26	H27	H28	H29	H30	H30上	R01上
発生件数	1,876	1,495	1,291	425	322	212	182

※上は上半期の意

出所：警視庁「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について 統計データ」[online] <https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（最終閲覧 2019年12月31日）

表5 インターネットバンキングに係る不正送金事犯の被害額の推移

年次（西暦）	2014	2015	2016	2017	2018	2018上	2019上
年次	H26	H27	H28	H29	H30	H30上	R01上
被害額（百万円）	2,910	3,073	1,687	1,081	461	373	165

※上は上半期の意

出所：警視庁「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について 統計データ」[online] <https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（最終閲覧 2019年12月31日）

警察庁ではサイバー犯罪に対する取組として「警察におけるサイバーセキュリティ戦略」に基づいて、セキュリティ人材の育成や被害防止対策の推進等を進めていくとしている。

3. サイバー空間における脅威の類別

サイバー攻撃は多様化しており、更に時代によってトレンドが大きく変化する。IPA（情報処理推進機構）は2006年から毎年、情報セキュリティに係る10大脅威を公表している。表6は2019年版の情報セキュリティ10大脅威であり、組織を対象とした脅威と、個人を対象とした脅威に分けて、サイバー空

間における脅威をランク付けしている。

表 6 10 Major Security Threats 2019 – Threat Ranking

Threats for Individuals	Rank	Threats for Organizations
Unauthorized Use of Leaked Credit Card Information	1	Advanced Persistent Threat
Phishing Fraud for Personal Information	2	Business E-mail Compromise
Malicious Smartphone Application	3	Financial Loss by Ransomware
Extortion of money by E-mail etc.	4	Emergence of Attacks Exploiting Supply Chain Weaknesses
Cyberbullying and Fake News	5	Information Leakage by Internal Fraudulent Acts
Internet Fraud by Fake Warnings	6	Business Service Outage Caused by Denial of Service Attacks
Unauthorized Use of Internet Banking Credentials	7	User Information Leakage from Services on Internet
Unauthorized Login to Services on Internet	8	Exposure of IoT Device Vulnerability
Financial Loss by Ransomware	9	Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information
Improper Management of IoT Devices	10	Unintentional/Accidental Information Leakage

出所：IPA「10 Major Security Threats 2019 ～ 10 Major Security Threats for Organizations ～
～ Apply the best security measure depending on the ever-changing situation」より

各脅威の要略については以下の通りである。

【Threats for Individuals（個人を対象とした脅威）】

RANK1 Unauthorized Use of Leaked Credit Card Information（クレジットカード情報の不正利用）

キャッシュレス社会の進展と共に、更に被害の拡大が予測される脅威である。キャッシュレスは用いられる場面が飛躍的に拡大しているが、多くがクレジットカード情報と紐付いている。そのため、攻撃者は端末をウィルス感染させたり、フィッシングサイトに誘導して、被害者自身にクレジットカード情報を提供させる等の手法で情報を詐取する。

RANK2 Phishing Fraud for Personal Information（フィッシングによる個人情報 の詐取）

有名企業や内部のシステム管理者を装う形でフィッシングメールを送信し、フィッシングサイトへ誘導することで、アカウントやパスワード、クレジットカード情報等を入手。情報はダークウェブで売買されたり、不正ログインなどに使用される。世界最大のECサイトであるAmazonをかたったものや、大学を標的としたフィッシングの被害が確認されている。

RANK3 Malicious Smartphone Application（不正アプリによるスマートフォン利用者への被害）

不正なアプリケーションを端末にインストールさせ、端末内の情報の窃取や、第三者への攻撃の踏み台とされるケースである。攻撃者が用意したサイトへ誘導し、不正アプリケーションをインストールさせる手法だけではなく、公式マーケットに不正アプリケーションを公開し、被害者に安全なものであると誤認させインストールさせる手口が存在する。宅配業者をかたった不正アプリケーションのインストール誘導や、スマートフォンの動画撮影機能、カメラ機能、録音機能等を使用者の意図しない形で不正利用する被害が確認されている。

RANK4 Extortion of money by E-mail etc.（メール等を使った脅迫・詐欺の手口による金銭要求）

アダルトサイトを閲覧している映像を拡散するといった脅迫や、有料サイト料金の架空請求によって、金銭等を騙し取る手口である。周囲への相談がしにくいセクストーションを利用したり、ダークウェブに出回っている被害者の情報を入手して脅迫を行うなど、手口が巧妙化している。

RANK5 Cyberbullying and Fake News（ネット上の誹謗・中傷・デマ）

SNS等の普及により、フェイクニュースの発信や他人への誹謗・中傷が大きな問題となっている。明確な悪意によるものだけではなく、情報モラルやリテラシーの低さから、起こりうる状況を想定できずに発信されるものも数多くあり、経済的損失や事件に繋がるケースが後をたたない。

RANK6 Internet Fraud by Fake Warnings(偽警告によるインターネット詐欺)

端末に偽の警告画面を表示させ利用者の不安を煽ることで、不必要なソフトウェアやサポートの購入等に繋げ、金銭を騙し取る手口である。その際に取得される個人情報やクレジットカードの情報は、更に不正利用されるなど、二次被害の拡大に繋がる。

RANK7 Unauthorized Use of Internet Banking Credentials (インターネットバンキングの不正利用)

攻撃者が不正取得した情報からインターネットバンキングへログインし、不正送金することで、金銭的被害が生じるものである。他の手口と同様に実在する企業や金融機関をかたった E-mail や SNS 等により、フィッシングサイトへ誘導する手口だけではなく、端末をウィルス感染させ自動不正送金させる手口も確認されている⁽³⁾。

RANK8 Unauthorized Login to Services on Internet (インターネットサービスへの不正ログイン)

Brute force attack や Joe account attack 等の攻撃やウィルス感染により ID やパスワードが漏洩し、インターネットサービスにログイン、不正利用がなされるものである。被害者が気づかないこともあり、対応が遅れるほど被害が拡大する。

RANK9 Financial Loss by Ransomware (ランサムウェアによる被害)

E-mail やウェブサイト、OS の脆弱性を利用して端末をランサムウェアに感染させ、データの暗号化や端末をロックする手法である。復旧させることと引き換えに、攻撃者が被害者に金銭を要求し、被害者が支払いに応じると経済的損失も生じる。

RANK10 Improper Management of IoT Device (IoT 機器の不適切な管理)

IoT 機器への不正アクセスや脆弱性を利用した攻撃により、機器の乗っ取りや情報取得、DDoS 攻撃の踏み台となってしまう脅威である。IoT 機器の中にはパスワード変更やファームウェア更新がされないまま、放置されているものも存在し、その数も急激に増加していることから被害の拡大が予想される。

【Threats for Organizations（組織を対象とした脅威）】

RANK1 Advanced Persistent Threat（標的型攻撃による被害）

E-mailに含まれる添付ファイルやウェブサイトから、端末をウィルス感染させたり、クラウドサービスやウェブサーバーへの不正アクセスにより取得した認証情報を利用することで、機密・知財情報等の重要情報を窃取する脅威である。事業継続に大きな影響を及ぼす可能性があり、企業や官公庁への標的型攻撃が度々確認されている。

RANK2 Business E-mail Compromise（ビジネスメール詐欺による被害）

取引先になりすました請求書の偽装や、経営者等へのなりすまし、窃取メールアドレスを不正利用して相手を信じ込ませるなどの手口で、攻撃者へ送金させるものである。海外での事例が多く見られたが、近年日本においてもビジネスメール詐欺が確認されている。

RANK3 Financial Loss by Ransomware（ランサムウェアによる被害）

個人と同様にE-mailやWebsite、OSの脆弱性を利用して端末をランサムウェアに感染させ、端末や事業継続に必要なデータをロックするものである。攻撃者は復旧に金銭を要求し、被害者が支払った場合には経済的な損失も被る。

RANK4 Emergence of Attacks Exploiting Supply Chain Weaknesses（サプライチェーンの弱点を悪用した攻撃の高まり）

サプライチェーン内の業務委託組織のうち、セキュリティ対策不足がある組織へのサイバー攻撃を足がかりとして、そこから連鎖して委託元組織にも被害が及ぶ脅威である。委託先組織のセキュリティ対策を検討したとしても、再委託や再々委託があると更に管理が困難となる。

RANK5 Information Leakage by Internal Fraudulent Acts（内部不正による情報漏えい）

組織内部の悪意を持った従業員や元従業員により、機密情報や重要情報が外部に漏洩することがある。外部からの不正アクセス等と異なり、正規のアクセス権で情報入手している場合には、セキュリティ対策強化での防衛が難しい。

RANK6 Business Service Outage Caused by Denial of Service Attacks (サービス妨害攻撃によるサービスの停止)

ボットネットやリフレクター攻撃等により、対象組織のサービスに高負荷をかけることで、機能停止やレスポンス遅延といった損害を引き起こすものである。

RANK7 User Information Leakage from Services on Internet (インターネットサービスからの個人情報の窃取)

インターネットサービスの脆弱性を悪用し、個人情報やクレジットカード情報を窃取するものである。

RANK8 Exposure of IoT Device Vulnerability (IoT 機器の脆弱性の顕在化)

IoT 機器の脆弱性を利用して DDoS 攻撃の踏み台にしたり、機能を不正利用したりするケースが確認されている。数が膨大であり、セキュリティ対策が不十分な機器も存在するため、IoT 機器を対象としたサイバー攻撃は増加傾向にある。

RANK9 Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information (脆弱性対策情報の公開に伴う悪用増加)

開発ベンダー等により公開された脆弱性情報を悪用し、対策パッチが適用される前に攻撃をするものである。広く使用されているソフトウェアである場合、同様の手口で攻撃できることから被害が拡大する可能性がある。

RANK10 Unintentional/Accidental Information Leakage (不注意による情報漏えい)

業務用端末の紛失や、情報取り扱い者の不注意等による重要情報の漏えいである。規定の策定や、インシデント発生時の対応について、事前に検討しておく必要がある。

個人を対象とした脅威については、「Unauthorized Use of Leaked Credit Card Information (クレジットカード情報の不正利用)」や「Phishing Fraud for Personal Information (フィッシングによる個人情報の詐取)」に代表される個人資産を狙ったものが多数を占める。2018 年版における 1 位は「インターネットバンキングやクレジットカード情報等の不正利用」という分類であったが、手口の多様化に伴って 2019 年版からは「インターネットバンキングの不正利

用」「クレジットカード情報の不正利用」「仮想通貨交換所を狙った攻撃」「仮想通貨採掘に加担させる手口」「フィッシングによる個人情報等の詐取」の5つに細分化されている。

組織を対象とした脅威については、外部からの脅威が多いのは確かであるが「Information Leakage by Internal Fraudulent Acts（内部不正による情報漏えい）」と「Unintentional/Accidental Information Leakage（不注意による情報漏えい）」といった、内部脅威がランクインしている点にも注意しなければならない。

4. 超スマート社会（Society5.0）とサイバー攻撃

サイバー空間と実空間との融合が進展する中、サイバー攻撃の脅威は実空間にも及んでおり、既に多くの物理的実害が発生している。中でも世界に大きな衝撃を与えたものは W32.Stuxnet によるイラン原子力施設攻撃であろう。W32.Stuxnet は世界で初めて産業用システムに物理的実害をもたらしたマルウェアである。W32.Stuxnet はゼロデイ脆弱性^④を利用して拡散し、イランの原子炉施設に物理的にダメージを与えたのである。一般に産業用システムはサイバー攻撃から守るために stand-alone で運用されるが、W32.Stuxnet は USB flash drive 経由で感染し stand-alone のコンピュータに侵入^⑤したのである。W32.Stuxnet は Siemens の SCADA における WinCC/PCS7 を標的とし、核燃料施設のウラン濃縮用遠心分離機を破壊したことから、マルウェアによる産業システムの攻撃可能性を実際に示したものとして衝撃を与えたのである。

人類は社会構造を狩猟社会（Society1.0）、農耕社会（Society2.0）、工業社会（Society3.0）、情報社会（Society4.0）と変化させてきた。今後は人工知能（AI）や IoT 等のテクノロジーによって、5 番目の社会構造である超スマート社会（Society 5.0）へシフトすると予測されている。超スマート社会（Society 5.0）とは、第 5 期科学技術基本計画によれば「必要なもの・サービスを、必要な人に、必要な時に、必要なだけ提供し、社会の様々なニーズにきめ細やかに対応でき、あらゆる人が質の高いサービスを受けられ、年齢、地域、言語といった様々な

違いを乗り越え、活き活きと快適に暮らすことのできる社会」とされる。様々なテクノロジーが活用され、サイバー空間と実空間とが密接に融合していくことから、同時にサイバー攻撃の脅威も深刻化していくことが予測される。しかし、サイバー攻撃への対処を含むセキュリティ対策は、それ自体が利益を生まないことから、保険的な意味合いで捉えられることが多く、利便性や経済的利益の追求に比べ後回しにされがちであった。超スマート社会（Society5.0）へのシフト前夜である現時点でこそ、社会全体でその意義を再確認すべきであろう。

参考文献

出口雅史（2017）「重要インフラを標的とするサイバー攻撃と国際安全保障への影響」『中央大学政策文化総合研究所年報』20,pp.71-85, 中央大学政策文化総合研究所

インターネット資料

警視庁「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」
<https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>（最終閲覧 2019 年 12 月 31 日）

IPA「10 Major Security Threats 2019 ～ 10 Major Security Threats for Organizations ～ ～ Apply the best security measure depending on the ever-changing situation」
<https://www.ipa.go.jp/files/000076989.pdf>（最終閲覧 2019 年 12 月 31 日）

注

- （1）第5期科学技術基本計画（2016年～2020年）において目指すべき未来の姿として提唱がなされた。
- （2）警察庁によれば「インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等、情報技術を利用した犯罪」とされる。
- （3）認証方式の改善等、被害予防により、2017年上半期と2018年上半期を比較した場合、被害件数は横ばいであるものの被害額は減少した。
- （4）Microsoft Windows Shortcut ‘LNK/PIF’ Files Automatic File Execution Vulnerability (BID 41732)
- （5）感染すると rootkit のインストールや Mcshield.exe, avguard.exe を停止させ、検知を遅らせる。