NISC National center of Incident readiness and Strategy for Cybersecurity

新たな「サイバーセキュリティ戦略」について

内閣官房 内閣サイバーセキュリティセンター 副センター長
吉 川　徹 志

我が国におけるサイバーセキュリティ政策推進体制

内閣

内閣総理大臣

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 ｻｲﾊﾞｰｾｷｭﾘﾃｨ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術(IT)政策担当大臣(デジタル大臣)[注2]
東京オリンピック競技大会・パラリンピック競技大会担当大臣[※3]
有識者[※4]（８名；10名以下）

※3 平成27年７月22日付け内閣総理大臣決定により本部員に指定
※4 令和２年４月１日現在

閣僚が参画

遠藤　信博　日本電気株式会社取締役会長
小野寺　正　ＫＤＤＩ株式会社相談役
後藤　厚宏　情報セキュリティ大学院大学学長
中谷　和弘　東京大学大学院法学政治学研究科教授
野原佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英　東京都立大学法科大学院兼任教授
宮澤　栄一　株式会社デジタルハーツホールディングス取締役会長
村井　純　慶應義塾大学教授

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
ｻｲﾊﾞｰｾｷｭﾘﾃｨ対策推進会議（CISO等連絡会議）

整備基本方針作成等における緊密連携

デジタル庁[注1]

デジタル社会の形成に向けた司令塔としてデジタル改革を推進

連携

サイバーセキュリティ協議会

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

（事務局）

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ参与

政府関係機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

協力

＜重要インフラ所管省庁＞
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス、化学、クレジット、石油）
国土交通省（鉄道、航空、物流、空港）

＜その他関係省庁＞
文部科学省（セキュリティ教育）等

協力

閣僚本部員６省庁

警察庁（ｻｲﾊﾞｰ犯罪・攻撃の取締り）
デジタル庁[注1]（デジタル社会形成に向けた司令塔）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

（注1）デジタル社会形成基本法（令和３年法律第35号）、デジタル庁設置法（令和３年法律第36号）。（令和３年９月１日施行）

東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策（結果報告）

東京大会におけるサイバーセキュリティ対策

○ **リスクアセスメントの促進(事業者等が自主的に実施する取組)**
大会に関連する重要サービス事業者等を対象に、リスク評価の実施を依頼
（2016年から全６回）

○ **横断的リスク評価(NISCが検証する取組)**
競技会場や特に重要な事業者等を対象に、NISCが主体となって検証
（2018年から全５回）

○ **スポーツ関連団体に対する勉強会**
スポーツ関連団体を対象に、サイバーセキュリティに係る勉強会等を開催
（2017年から全17回）

○ **サイバーインシデント対応演習**
現下のサイバーセキュリティ情勢を踏まえたシナリオを用いた演習を実施
（2019年から全５回）

大会期間中の対策

○ **情報共有プラットフォームの運用**
関係組織間における脅威情報の共有等を迅速・効率的に行うための情報共有プラットフォーム（JISP）を運用。約350の関係組織がJISPを活用。

○ **サイバーセキュリティ対処調整センターの運用**
関係組織からの連絡に即応できるよう24時間態勢で運用。インシデント発生の際には、情報セキュリティ関係機関等と協力して、迅速にインシデント対処を支援。

東京大会へのサイバー攻撃に関する被害状況等

大会運営に影響を与えるようなサイバー攻撃は確認されなかった。

大会期間中の主なトピック（大会運営への影響なし）

○ **サイバー攻撃に関するSNS上の書き込み等**
大会関係組織に対するサイバー攻撃を呼びかけるSNS上の書き込み等を確認

○ **米国コンテンツ配信サービス企業における障害**
米国コンテンツ配信サービス企業においてシステムの不具合によるサービス障害が発生し、大会公式サイトを含む関係組織のwebサイトが一時的に閲覧不能になったことを確認（7/23 １時間程度）
本件に関しては、同企業からサイバー攻撃によるものではない旨の発表あり

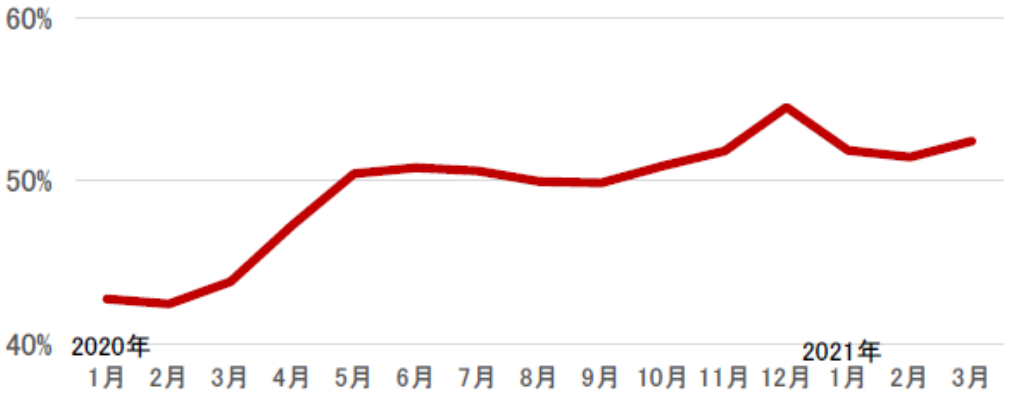
○ **不正な動画配信サイト**
開会式、各競技等の動画配信を装った複数の不正サイトを確認

動画配信サイトの検索結果

サイト接続後に案内される不正なアカウント登録画面

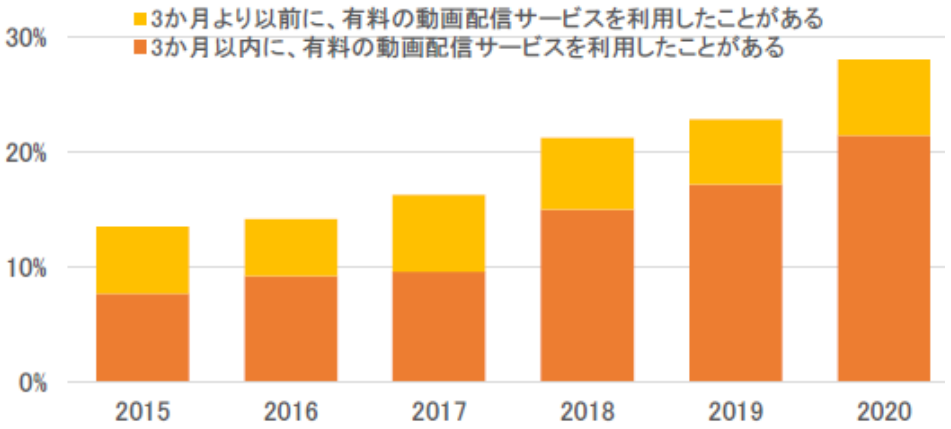
コロナ禍で拡大したデジタル活用

ネットショッピング利用率の推移



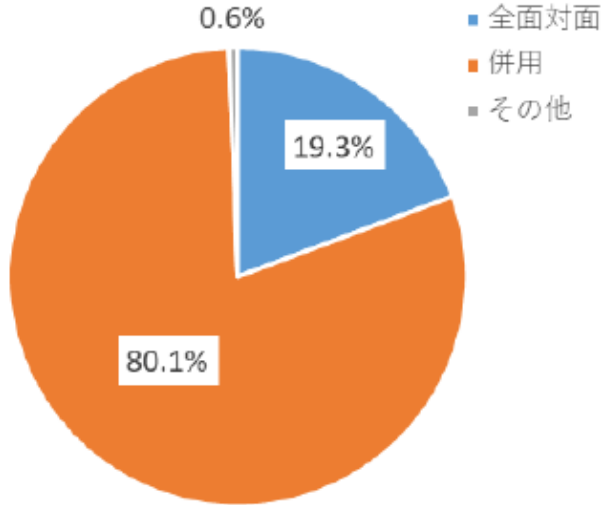
[出典]総務省「家計消費状況調査」を基に総務省作成（令和3年度情報通信白書）

有料動画配信サービス利用率の推移



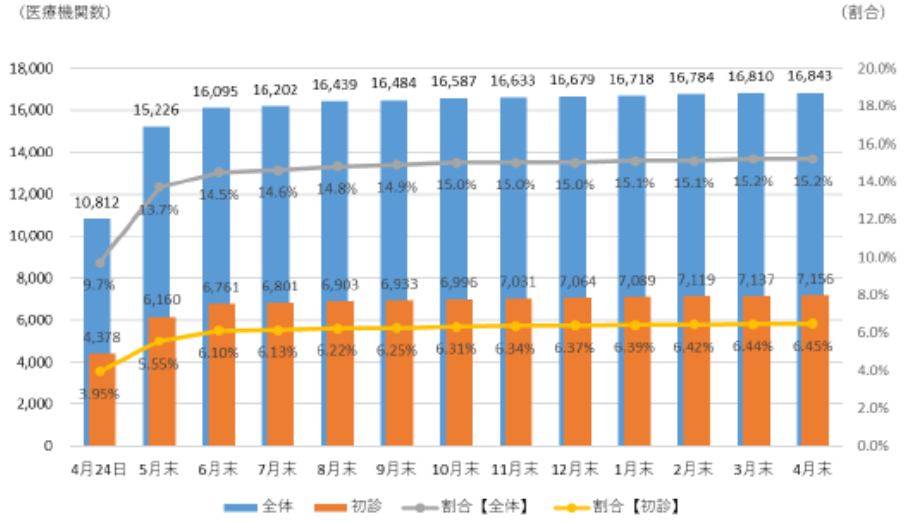
[出典]インプレス(2020)を基に総務省作成（令和3年度情報通信白書）

大学等における授業の実施方針



[出典]文部科学省（2020）「大学等における後期等の授業の実施方針等に関する調査」
を基に総務省作成（令和3年度情報通信白書）

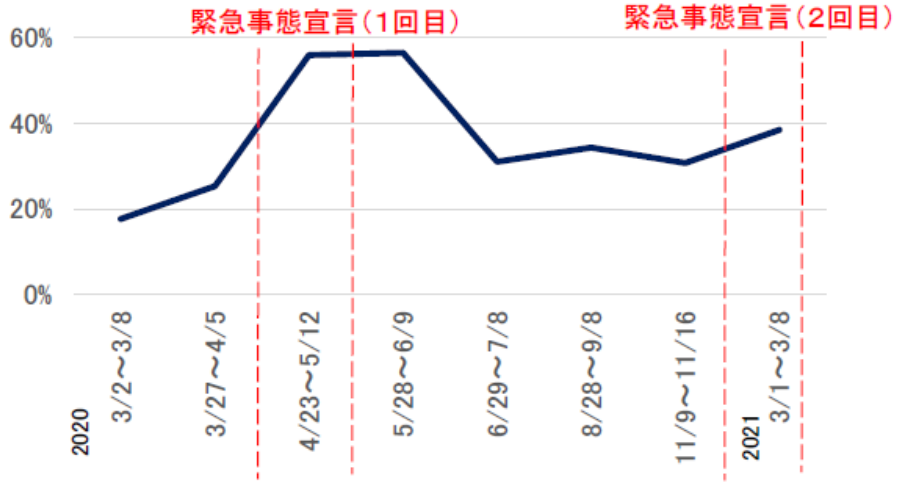
電話・オンライン診療の登録機関数



[出典]厚生労働省「第15回オンライン診療の適切な実施に関する指針の見直しに関する検討会」資料

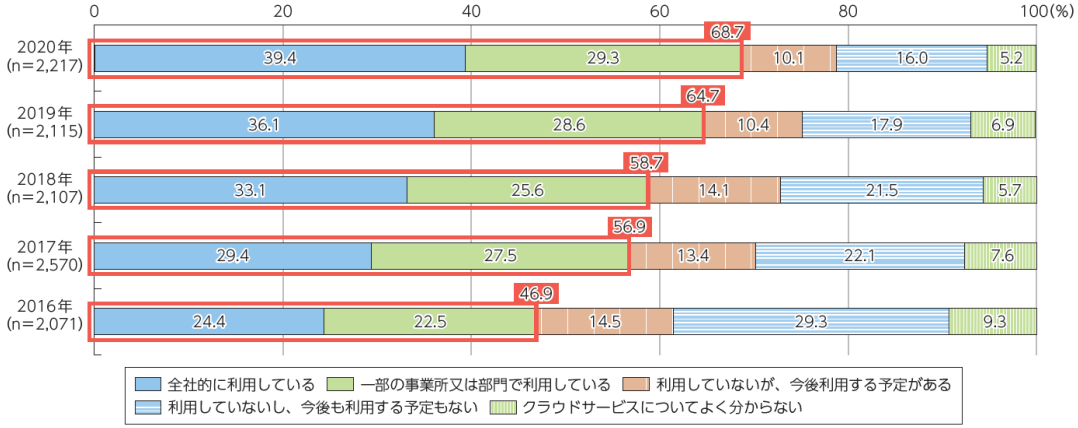
テレワークやクラウドサービスの普及を踏まえたサイバー攻撃

テレワーク実施率の推移



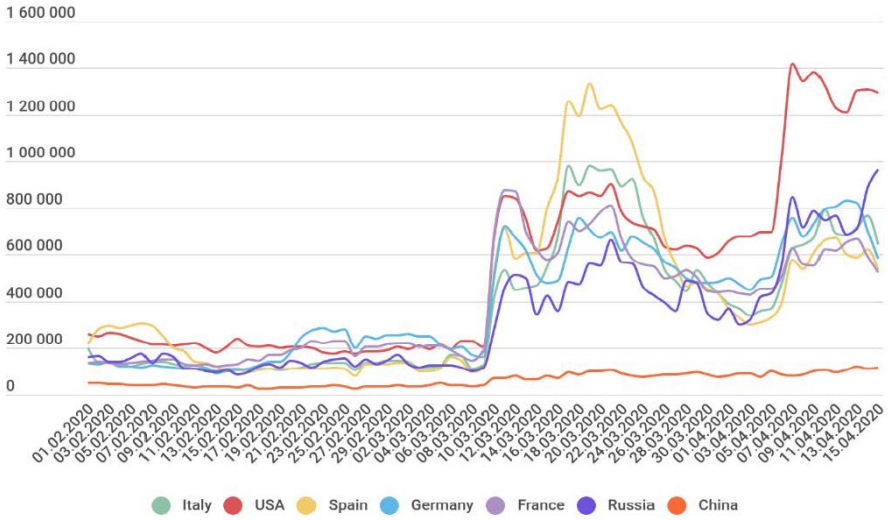
[出典]東京商工リサーチ「新型コロナウイルスに関するアンケート」調査（第 2～6、8、10 、14 回）を基に総務省作成（令和3年度情報通信白書）

クラウドサービスの利用状況の推移



[出典]総務省「通信利用動向調査」（令和3年度情報通信白書）

リモートデスクトップを狙った攻撃件数の推移



[出典]Kaspersky「Remote spring: the rise of RDP bruteforce attacks(2020/4/29)」
https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

クラウドサービスを標的とした外部脅威の推移

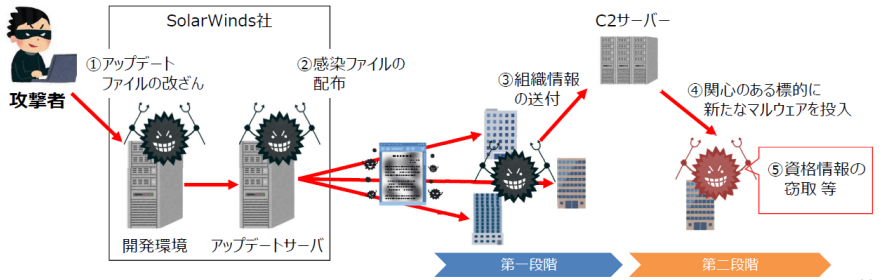
[出典]McAfee Labs COVID-19 脅威レポート（2020年7月）
https://www.mcafee.com/enterprise/ja-jp/assets/reports/rp-quarterly-threats-july-2020.pdf

大規模な影響のあった攻撃事案（サプライチェーン攻撃等）

SolarWinds Orion Platformのアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。
- 初期段階のマルウェアは、セキュリティサービスの検知を回避しつつ被害組織の情報をC2サーバーへ送信。**攻撃者が関心のある標的に対しては第２段階のマルウェアが投入**され、資格情報を窃取した上で、**米国政府内、政府間のやり取りを傍受していた可能性が指摘されている。**

◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

11

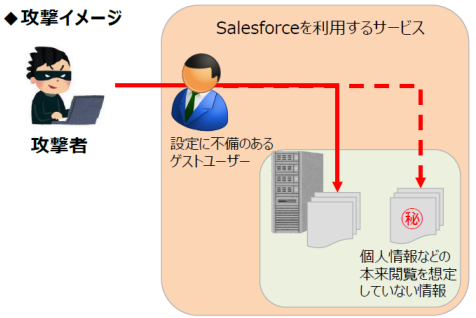
クラウドサービスの設定不備を原因とする不正アクセス

- 2020年12月25日、セールスフォース・ドットコムは、同社が提供するサービスにおける**ゲストユーザーに対する情報共有に関する設定が適切に行われていない場合、一部情報が第三者より閲覧できる**事象の発生を公表。また、**複数の国内事業者が本事象による不正アクセス及び個人情報漏えいの発生**を公表。
- 本サービスを組み込んだシステムがパッケージとして複数の顧客に提供され、同時に被害が発生したケースも。
- クラウドサービスを活用する際には、サービスの利用状況や各種設定の確認・見直しを行うなど、適切なセキュリティ対策を講ずることが重要。

◆不正アクセスがあったと公表した事業者等

- キャッシュレス決済サービス事業者
- サービス事業者
- クレジットカード事業者
- 小売事業者
- 玩具メーカー
- ガス事業者
- 地方自治体
- 独立行政法人　　他

◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

3

[出典]経済産業省 2021年4月2日第6回産業サイバーセキュリティ研究会資料

レジリエンス　～サイバー攻撃による米国石油パイプラインの操業停止～

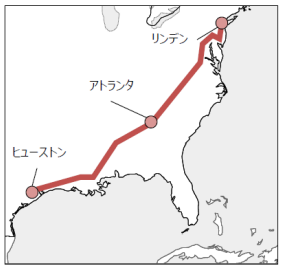
- 5月7日、**米石油パイプライン最大手のコロニアル・パイプライン**が**ランサムウェアによるサイバー攻撃**を受け、**全ての業務を停止**したと発表。直接の影響を受けたのはITシステムだが、**脅威を封じ込めるためにOTシステムをオフラインにし、全てのパイプライン運用を停止。**
- FBIはロシア系攻撃集団「ダークサイド」の関与を断定、同グループは「目的は金銭であり社会に影響を与えることは意図していない」と表明（※）。

※同グループは略取した身代金の一部を対価に開発したランサムウェアをグループ外の実行犯に提供するスキームを運用しており、実行犯がもたらした影響に同グループは関知しない、とのスタンス

コロニアル・パイプライン
メキシコ湾岸の製油所と米東部・南部を結ぶ全長8,850kmのパイプライン。
東海岸の需要の約半分にあたる１日約１億ガロンを輸送。

米運輸省による緊急措置の内容
影響を受ける１７州と首都ワシントン向けに
燃料を輸送する運転手の労働時間規制を一時的に緩和。

米CISAによる声明のポイント
CISAは、サイバーセキュリティ部門トップのGoldstein氏名で声明を公表。
・被害企業と関係官庁とともに本事案に対処中。
・ランサムウェアは組織の規模、セクターに関係なく直面する脅威。
・この種の脅威に晒されるリスクを減らすためサイバーセキュリティ体制を強化する措置を講じることを各組織に推奨。



コロニアル・パイプラインの
主要パイプライン（イメージ）

23

[出典]経済産業省 2021年6月4日第28回産業構造審議会総会資料

国家の関与が疑われるサイバー攻撃

外務報道官談話

米国による北朝鮮のサイバー攻撃に関する発表について（外務報道官談話）

平成29年12月20日
英語版 (English)

ツイート　シェア 0　メール

1　サイバー空間の安全は，我が国を含む国際社会の平和と繁栄を確保する上で極めて重要です。

2　こうした中，12月19日，米国は，本年5月の悪意あるプログラム「ワナクライ」を用いたサイバー攻撃が北朝鮮によるものであるとして，北朝鮮を非難する旨発表しました。

3　我が国は，サイバー分野を含む北朝鮮問題について米国を含む国際社会と緊密に連携してきており，北朝鮮に対する圧力を最大限まで高め，北朝鮮の政策を変えさせるとの観点からも，サイバー空間の安全の確保に向けた強い意思を示す今回の米国の発表を支持するとともに，我が国としても，「ワナクライ」事案の背後に，北朝鮮の関与があったことを非難します。

4　我が国としては，米国を始めとする国際社会と緊密に連携して，自由，公正かつ安全なサイバー空間の創出・発展のための取組を進めていきます。

外務報道官談話

中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）

令和3年7月19日
英語版 (English)

1 サイバー空間の安全は、我が国を含む国際社会の平和と繁栄を確保する上で極めて重要であり、先般、英国で行われたG7サミットでもこのことについて改めて確認されたところです。

2 こうした中、7月19日（現地時間）、英国及び米国等は、中国政府を背景に持つAPT40といわれるサイバー攻撃グループ等に関して声明文を発表するとともに、米国はAPT40の構成員4名を起訴しました。我が国としても、APT40は中国政府を背景に持つものである可能性が高いと評価しており、サイバー空間の安全を脅かすAPT40等の攻撃を強い懸念をもって注視してきています。今回の英国及び米国等の声明は、サイバー空間におけるルールに基づく国際秩序を堅持するとの決意を示すものであり、これを強く支持します。

3 我が国においても、先般、中国人民解放軍61419部隊を背景に持つTick（ティック）といわれるサイバー攻撃グループが関与した可能性が高いサイバー攻撃について発表を行いました。そして、今回のAPT40といわれるサイバー攻撃グループからの攻撃では、我が国企業も対象となっていたことを確認しています。

4 自由、公正かつ安全なサイバー空間という民主主義の基盤を揺るがしかねない悪意あるサイバー活動は看過できません。日本政府としては、これを国家安全保障の観点からも強く懸念すべきものであると考えており、断固非難するとともに、厳しく取り組んでいく考えです。

5 今後も、G7諸国を始めとする国際社会と緊密に連携して、自由、公正かつ安全なサイバー空間の発展のための取組を進めていきます。

※ 上記のほか、2018年12月には、「中国を拠点とするAPT10と」いわれるグループによるサイバー攻撃について」（外務報道官談話）を公表。

MEMO 警察のアトリビューションにより国家レベルの関与を明らかにしたサイバー攻撃事案

1　レンタルサーバ不正契約事件被疑者の検挙

中国共産党員の男（30代）は、平成28年９月から平成29年４月までの間、合計５回にわたり、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行った。警視庁公安部は、令和３年４月、同男を私電磁的記録不正作出罪・同供用罪で検挙した。

2　一連のサイバー攻撃に関与した背景組織の特定

本事件の捜査を通じ、警察では、同男が不正に契約したレンタルサーバが宇宙航空研究開発機構（JAXA）等に対するサイバー攻撃に悪用されたことを把握するとともに、同攻撃の実態解明の過程で、同一の攻撃者が関与している可能性が高いサイバー攻撃が約200の国内企業等に対して実行されたことを把握した。

本事件被疑者・関係者の供述をはじめ数多くの証拠を積み上げた結果、これらのサイバー攻撃がTickと呼ばれるサイバー攻撃集団によって実行されたものであり、このTickの背景組織として山東省青島市を拠点とする中国人民解放軍第61419部隊が関与している可能性が高いと結論付けるに至った。

3　被害企業等に対する注意喚起

警察では、これらのサイバー攻撃を認知後、被害企業等に対し、速やかに不正プログラムへの感染可能性や有効な対応策について個別に情報提供を実施した(注1)。

また、一連のサイバー攻撃は、日本製ソフトウェアのぜい弱性が悪用されたゼロデイ攻撃(注2)であったことから、このソフトウェアの開発企業と協力し、ぜい弱性の存在と有効な対応策について広く周知した。

[出典]令和３年警察白書

APT40に対してNISC・警察庁による注意喚起を実施

NISC 内閣サイバーセキュリティセンター　警察庁 National Police Agency

2021年７月19日

中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（注意喚起）

令和３年７月19日（現地時間）、英国及び米国等は、中国政府を背景に持つAPT40といわれるサイバー攻撃グループ等に関して、声明文を発表しました。

我が国政府としても、サイバー空間の安全を脅かすAPT40等の攻撃を強い懸念を持って注視してきており、７月19日、こうした悪意あるサイバー活動を断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話を発出しました。
（中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）
https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html）

今回のAPT40といわれるサイバー攻撃グループによるサイバー攻撃等では、我が国企業も対象となっていたことを確認しているところであり、内閣サイバーセキュリティセンターや警察では、引き続き国内外の関係機関と連携し、被害の未然防止及び拡大防止に向けて情報収集や対策等を進めてまいります。

こうしたサイバー攻撃にはさまざまな手法、手口がありますが、日頃から、不審なメールや添付ファイルは開かない、OSやプログラムのパッチやアップデートを可及的速やかに設定する等の基本的な留意事項を守りつつ、対象に応じた適切なサイバーセキュリティ対策を講じてください。また、実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

「サイバーセキュリティ戦略」（令和3年9月28日閣議決定）の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験
テレワーク、オンライン教育等の進展
- 厳しさを増す
安全保障環境
- **SDGｓ**への
デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**
に向けて行ってきた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも
- 不適切な利用は
国家分断、人権の阻害へ
- 官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

経済社会の活力の向上及び持続的発展

課題認識と方向性　ーデジタルトランスフォーメーションとサイバーセキュリティの同時推進 ー

- 本年9月に「デジタル庁」が設置され、デジタル化が大きく推進される絶好の機会。
  そのためにも、サイバー空間への信頼を醸成し、参加・コミットメントを得ることが重要。
- また、業務、製品・サービス等のデジタル化が進む中、サイバーセキュリティは企業価値に直結する営為に。
  「セキュリティ・バイ・デザイン」の重要性は一層増し、デジタル投資とセキュリティ対策の一体性は高まる。

⇨ デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進。

主な具体的施策

① 経営層の意識改革

→デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化・インセンティブ付けを行い、更なる取組を促進。

② 地域・中小企業におけるDX with Cybersecurityの推進

→地域のコミュニティの推進・発展、中小企業向けサービスの審査登録制度を通じ、デジタル化に当たって直面する知見や人材等の不足に対応。

③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

→Society5.0に対応したフレームワーク等も踏まえ、各種取組を推進。

- サプライチェーン：　産業界主導のコンソーシアム
- データ流通　　：　データマネジメントの定義、「トラストサービス」によるデータ信頼性確保
- セキュリティ製品・サービス：　第三者検証サービスの普及
- 先端技術　　：　情報収集・蓄積・分析・提供等の共通基盤構築

④ 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

→情報教育推進の中、「デジタル活用支援」と連携して、各種取組を推進。

国民が安全で安心して暮らせるデジタル社会の実現

課題認識と方向性 － 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保 －

- サイバー空間の**公共空間化**、**相互連関・連鎖の深化**、**サイバー攻撃の組織化・洗練化**。

国は、様々な主体と連携しつつ、①自助・共助による**自律的なリスクマネジメントが講じられる環境づくり**と、②持ち得る手段の全てを活用した**包括的なサイバー防御の展開**等を通じて、**サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築**し、国全体のリスク低減、レジリエンス向上を図る。

主な具体的施策（１）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築

- サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保
- 利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

- 政府機関・重要インフラ事業者等向けにクラウド利用の際に考慮すべきセキュリティルール策定
- ISMAPの取組等の民間展開による一定のセキュリティが確保されたクラウド利用の促進
- 信頼性が高く、オープンかつ使いやすい高品質クラウドの整備の推進

③ サイバー犯罪への対策

- サイバー空間を悪用する犯罪者やトレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等の摘発を推進し、実空間と変わらぬ安全・安心を確保
- 警察におけるサイバー事案対処体制の強化

④ 包括的なサイバー防御の展開

- サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化（対処官庁のリソース結集と連携強化、サイバーセキュリティ協議会等の関係機関との連携による官民連携・国際連携強化）
- 包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）

⑤ サイバー空間の信頼性確保に向けた取組

- 個人情報や知的財産を保有する主体への支援
- 経済安保の視点を踏まえたITシステム・サービスの信頼性確保（政府調達、重要なインフラ、国際海底ケーブル等）

国民が安全で安心して暮らせるデジタル社会の実現

主な具体的施策（２）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

- デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進。
- 情報と発信者の真正性等を保障する制度を企画立案し、普及を促進。ISMAP制度を運用し、民間利用の推奨。

主な具体的施策（３）経済社会基盤を支える各主体における取組

①　政府機関等

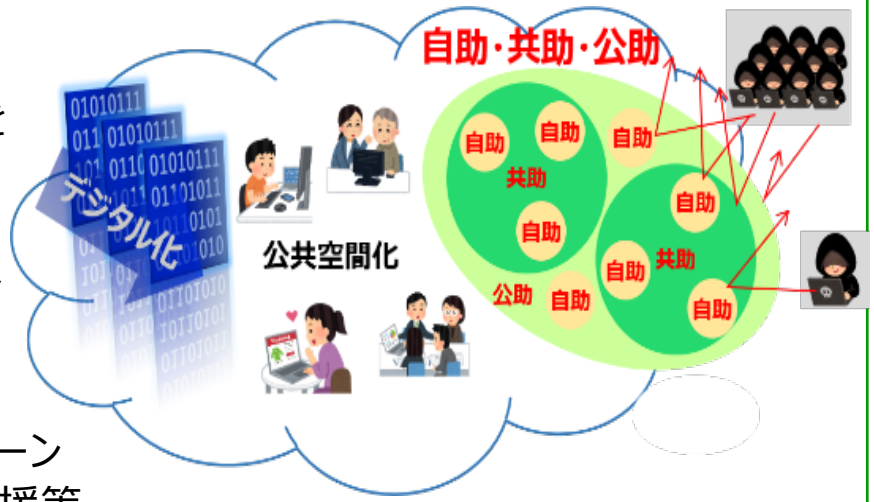
- 政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。

②　重要インフラ

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進。
- 地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度整備。

③　大学・教育研究機関等

- リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等。



主な具体的施策（４）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化

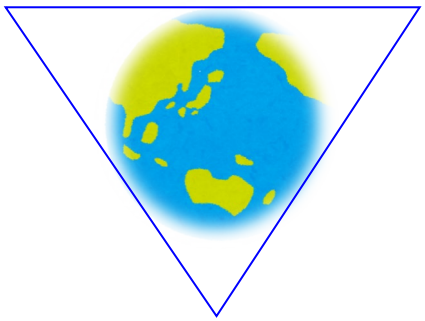
- 東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用。
- 平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化。

課題認識と方向性　－ 安全保障の観点からの取組強化 －

- 我が国をとりまく安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取等を企図したサイバー攻撃を行っているとみられている。
- 一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルール等をめぐる対立等に対して同盟国・同志国等が連携して対抗している。
- 加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある。

⇨ サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、以下を一層強化する。

「自由、公正かつ安全なサイバー空間」の確保



国際協力・連携

我が国の防御力・抑止力・状況把握力の向上

国際社会の平和・安定及び我が国の安全保障への寄与

主な具体的施策

① 自由・公正かつ安全なサイバー空間の確保

- サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）
  - 国際法の適用に関する議論・規範の実践の普及、サイバー犯罪に関する条約の普遍化等の推進
- サイバー空間におけるルール形成
  - 信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）や5Gセキュリティ等国際的な取組の進展を踏まえた我が国の基本理念に沿う国際ルールの策定

② 我が国の防御力・抑止力・状況把握力の強化

- サイバー攻撃に対する防御力の向上
  - 防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、自衛隊・米軍のインフラ防護の演習等の実施
  - 先端技術・防衛産業等のセキュリティ確保のための官民連携・情報共有等の強化
- サイバー攻撃に対する抑止力の向上
  - 相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応の活用、日米同盟の維持・強化
- サイバー空間の状況把握力の強化
  - 全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃の更なる実態解明の推進

③ 国際協力・連携

- 知見の共有・政策調整
  - 米豪印やASEAN等同志国との府省庁横断的・各府省庁における国際連携の重層的な枠組みの強化
- サイバー事案等に係る国際連携の強化
  - 国際サイバー演習の主導等による国際的なプレゼンスの向上
- 能力構築支援
  - 「基本方針」*に基づく産学官連携や外交・安全保障を含めたASEANを含むインド太平洋地域における取組強化

*「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」

新しい「サイバーセキュリティ戦略」のポイント（新旧比較）

➢ **基本法における３つの目的（※）を達成するための施策について、「Cybersecurity for All～誰も取り残さないサイバーセキュリティ～」という大きな方向性を示しつつ、デジタル改革やDXの進展に伴う課題、経済安全保障の懸念、国家の関与が疑われる攻撃の脅威の高まり等新たな脅威認識の下、国民目線、公助の取組強化の観点から新しい戦略を策定。**

（※）経済社会の活力の向上及び持続的発展 、国民が安全で安心して暮らせる社会の実現 、国際社会の平和・安定及び我が国の安全保障への寄与

	2018戦略	2021戦略
1 重点領域の拡大	○政府機関、重要インフラ事業者	○政府機関、重要インフラ事業者 ○サイバー関連事業者（主にクラウドサービス） ○知的財産、個人情報を扱う事業者
2 サイバー防御体制の強化	○多様な主体間の情報共有・連携の推進（サイバーセキュリティ協議会の設立） ○民間の参加・連携・協働の支援	○国主導による重大サイバー事案への対処（ナショナルサート機能の強化※１、警察庁サイバー局設置等） ○経済安全保障（ITインフラの信頼性確保） ※１ 情報集約～政策措置までの一体的推進を担う総合調整機能を強化 National CSIRT/CERT(Computer Security Incident Response Team / Computer Emergency Response Team)
3 サイバー抑止力の向上、国際連携の強化	○防御力・抑止力・状況把握力の強化（自衛隊等関係機関の強化） ○対外発信（脅威対象国、連携強化国は明記せず）	○外交安保上の優先度向上 ○防御力・抑止力・状況把握力の強化（妨げる能力の活用、外交的手段、刑事訴追） ○対外発信（脅威対象としての中※２露北、連携強化国として米豪印、ASEANの明記） ※２ JAXA等に対する攻撃に関し言及
4 社会のデジタル化への対応	○経営層、サプライチェーン対策	○経営層、サプライチェーン対策 ○子ども・高齢者のリテラシー対策
5 人材育成等	○人材：戦略マネジメント層の育成 ○研究：実践的開発の推進	○人材：戦略マネジメント層の育成（「プラスセキュリティ」知識※３の補充）高度専門人材の育成・確保 ○研究：実践的開発、AI、量子の対応具体化 ※３ セキュリティ専門家と協働するために、自らの業務にプラスして習得すべき知識

新しい「サイバーセキュリティ戦略」の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3　サイバー空間をとりまく課題認識

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜3つの方向性＞（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせるデジタル社会の実現	国際社会の平和・安定及び我が国の安全保障への寄与
１．経営層の意識改革 ２．地域・中小企業におけるDX with Cybersecurity の推進 ３．新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり ４．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	１．国民・社会を守るためのサイバーセキュリティ環境の提供 ２．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保 ３・４・５．経済社会基盤を支える各主体における取組 ①(政府機関等) ②(重要インフラ) ③(大学・教育研究機関等) ６．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用 ７．大規模サイバー攻撃事態等への対処態勢の強化	１．「自由、公正かつ安全なサイバー空間」の確保 ２．我が国の防御力・抑止力・状況把握力の強化 ３．国際協力・連携

横断的施策

研究開発の推進　／　人材の確保・育成・活躍促進　／　全員参加による協働・普及啓発

5　推進体制

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

「Cybersecurity for All」を踏まえた対応の強化

サイバー空間の課題認識

- あらゆる主体が参画する公共空間化
- サイバー・フィジカルの相互連関・連鎖の深化
- サイバー攻撃の複雑化・巧妙化
- 安全保障上の脅威の増大

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

個人		組織	
DXに向き合う**地方、中小企業、若年層、高齢者等**	目に見えないリスクと向き合う**個人・組織**	サイバー攻撃による**重要インフラ**停止、知財の窃取、金銭被害等の増大	**国家の関与**が疑われる攻撃

DXとサイバーセキュリティの同時推進

○デジタル改革と一体で：経営層の意識改革、地域・中小企業の取組促進
（経営インセンティブ、安価かつ効果的な支援サービス・保険の普及）

○誰も取り残さないリテラシーの向上と定着
（高齢者向けデジタル活用支援講習会との連携、GIGAスクール構想にあわせた普及啓発、サイバー防犯ボランティア）

安全保障の観点からの取組強化

○中露北からの脅威等を踏まえた外交・安全保障上のサイバー分野の優先度向上

○防衛省・自衛隊におけるサイバー防衛能力の抜本的強化

○「妨げる能力」、外交的手段や刑事訴追等を含めた対応、日米同盟の維持・強化

○国際協力・連携

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

○国民・社会を守るためのサイバーセキュリティ環境の提供
（産業横断的なサプライチェーン管理、サイバー犯罪対策、クラウドサービス利用のための対策の多層的な展開、経済安全保障の視点を含むサイバー空間の信頼性確保）

○深刻なサイバー攻撃から国民生活・経済を守る包括的なサイバー防御等の展開
（情報収集から対処調整、政策措置までの一体的推進の総合調整を担うナショナルサートの機能強化、政府機関・重要インフラ等の各主体のセキュリティ対策）

ご清聴ありがとうございました

https://www.nisc.go.jp