サイバーセキュリティ2021（１部 サイバーセキュリティに関する情勢）の概要

- サイバーセキュリティに関する情勢について、次期サイバーセキュリティ戦略※（以下「次期戦略」という。）の体系に沿って整理
- 次期戦略において、時代認識として整理している新型コロナウイルス感染症の拡大に伴う新たな生活様式の体現、デジタル経済の浸透やデジタル改革の推進といった経済社会の環境変化、安全保障環境の変化及び東京大会に向けて行われた官民の取組の活用等について内容の充実化を図りつつ、2020年度に政府機関、事業者、国民一般等において確認された国内外の主なサイバーセキュリティ事案等を併せて整理

※次期戦略が閣議決定された時点から効力を生じるものとする

経済社会の活力の向上及び持続的発展

新型コロナウイルス感染症拡大に伴う生活様式の体現

＜テレワークの利用拡大＞

・揺り戻しの動きは見られるものの、新型コロナウイルス感染症の拡大前よりも高い水準で推移。(2020年３月:8.9%、５月：20.4%、７月：16.9%、10月：16.0%)※1

＜ICT教育の推進＞

・「GIGAスクール構想」の推進状況として、当初2023年度までの整備の予定から、スケジュールを大幅に前倒し。

デジタル経済の浸透・デジタル改革の推進といった経済社会の環境変化、リスクの変容

＜DX推進に伴うセキュリティ対策＞

・経営層の意識について、経営会議等で審議・報告されるのは４割程度のまま推移※2しており、依然大きく進展せず、他国と比べても低水準。
・地域や中小企業は、人材課題等の制約が顕著であり、人材不足がセキュリティ対策の障害。（中小企業：42.8%、大企業：26.3%）※3
・サプライチェーンは他国以上に管理や対策は不十分。（物品調達先の対策が十分と回答した割合：（日本）24.0%、（米国：42.9%、（欧州）44.1%））※4
・我が国は他国と比べてDX推進に伴うセキュリティ対策の見直し状況は低い。(日本：21.7%、米国：73.7%、豪州：77.3%)※5

⇒「DX with Cybersecurity」をあらゆる面で推進

国民が安全で安心して暮らせるデジタル社会の実現

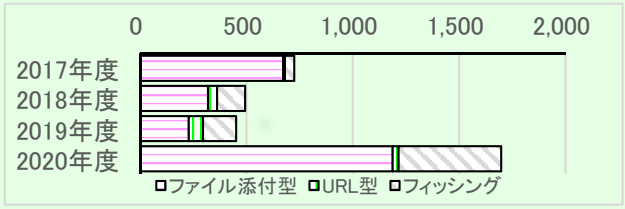
政府機関等に対する攻撃の高度化・巧妙化

政府機関において、マルウェア感染の疑いがある通信や標的型攻撃を引き続き検知しており、マルウェア感染の疑いがある通信は増加（図表１）。2020年度の不審メールはマルウェア「Emotet」により、ファイル添付型が大幅に増加。フィッシングも例年以上に増加傾向（図表２）。

図表１　政府機関における引き続き警戒を要する攻撃等の検知件数※6

年度	2018年度	2019年度	2020年度
マルウェア感染の疑い	111	55	245
標的型攻撃等	71	35	15

図表２　政府機関等に対する不審メールの傾向



サイバーセキュリティインシデント

・新型コロナウイルス感染症に乗じたサイバー攻撃
・DDoS攻撃による証券取引所の4日間にわたるシステムダウン（2020/8）
・電子決済サービスの口座への不正引出（2020/9）
・マルウェア「Emotet」による感染（2020/7以降）
・Netlogonの特権昇格が可能となる脆弱性を突いた攻撃（2020/8）等

国際社会の平和・安定及び我が国の安全保障への寄与

国外の動き（諸外国の国際動向）

米国
・バイデン政権の誕生（2021/1）
※国家安全保障戦略暫定指針において、サイバーセキュリティを最優先事項として位置づけ
・2021年度国防授権法により、ホワイトハウスにナショナル・サイバー・ダイレクターを新設予定

EU
・新たなサイバーセキュリティ戦略の公表（2020/12）
・サイバー攻撃に対する制裁措置の発動（2020, 2021）

英国
・「安全保障、防衛、開発及び外交政策の統合的見直し」の実施（2021/3）
サイバーエコシステムの強化、強靱かつ繁栄するデジタルUKの構築、自由・オープン・平和・安全なサイバー空間の推進等を柱とする新たなサイバー戦略を2021年に策定見込み

豪州
・サイバーセキュリティ戦略の公表（2020/8）
ビジョン：豪州市民、ビジネス、皆が依存する必要不可欠なサービスによってより安全なオンライン社会

中国
・グローバルデータセキュリティイニシアティブの発表（2020/9）

横断的施策

研究開発

・アカデミック研究が国際的に急成長しており、トップカンファレンス（IEEE Security&Privacy、ACM CCS、USENIX Security、NDSS）での論文投稿は、2000年と比較し、約４倍以上となる2,000本超が毎回投稿※7。
・国・産学をまたいだコラボレーションも活発化しており、デジタル化の進展に伴い、科学的基礎に基づく対策の重要性が高まる。

IT・セキュリティ人材

・デジタル化の進展に伴い、セキュリティ対策に当たる実務者層・技術者層の育成は一定の取組の進展が見られる一方で、ユーザ企業でのIT人材の不足傾向が拡大しており、セキュリティ人材も同様の傾向と想定
IT人材不足と回答した企業の割合※8：(2015年度)20.5% ⇒ (2019年度)33.0%
・我が国におけるユーザ企業のDX推進にあわせて、セキュリティ人材を確保するために、中長期的な観点からの人材育成のみならず、即戦力となる人材の流動性の向上やマッチングの機会の確保に取り組む必要がある

国民の意識・行動

・サイバー犯罪の検挙件数は増加の一途であり、情報セキュリティに関する事案として、高度な技術を使った攻撃だけでなく、標的型メール攻撃やビジネスメール攻撃等、心の隙を突くような古典的・比較的単純な攻撃も衰えていない
・一方で、これらの脅威を防ぐセキュリティソフトやサービス等での対策の実施状況は、個人・組織とも十分な水準に至っておらず、国民一人一人による着実な意識・行動の強化が必要な状況にある

※1　国土交通省「令和２年度テレワーク人口実態調査」（2021年3月19日）
https://www.mlit.go.jp/report/press/content/001391381.pdf
※2　（一社）日本システムユーザー協会「企業IT動向調査報告書」における複数年の調査結果を確認。
※3　(独)情報処理推進機構「2016年度 中小企業における情報セキュリティ対策に関する実態調査」（2017年8月8日）　https://www.ipa.go.jp/security/fy28/reports/sme/
※4　(独)情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017」(2017年4月13日)
https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html
※5　NRIセキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査2020」(2020年12月15日)
https://www.nri.com/jp/news/newsrelease/lst/2020/cc/1215_1
※6　既に攻撃手法に対応済みであるため攻撃としては失敗した通信、攻撃の前段階で行われる調査のための行為にとどまり明らかに対応不要と判断できる通信等を分析しノイズとして除去した上で、引き続き警戒を要するイベントについて集計
※7　“System Security Circus v2.0”（2021年5月7日）
http://s3.eurecom.fr/~balzarot/notes/top4_v2/
※8　(独)情報処理振興機構「人材白書2020」（2020年8月31日）
https://www.ipa.go.jp/jinzai/jigyou/about.html

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

１．経済社会の活力の向上及び持続的発展　～DX with Cybersecurityの推進～

昨年度の実績

- 経営層のサイバーリスクに対する意識改革により、組織能力の向上を図るため、サイバーセキュリティ経営ガイドライン・プラクティス集の普及啓発や、企業のサイバーセキュリティ経営実施状況の可視化ツールの開発を推進。
- 中小企業向けの安価かつ効果的なサービスの開発を目指し、（2019年度実証事業で得られた知見も活かしつつ）サイバーセキュリティお助け隊実証事業を実施。
- IoT機器やサプライチェーンの各構成要素について、信頼のチェーンを構築・維持することでIoTシステム・サービス及びサプライチェーン全体のセキュリティを確保することを目的とした各種研究開発、社会実装に向けた取組を推進。
- 子供たちのインターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者、教職員等に対する、学校等での現場での出前講座を実施。

評価

経営層の意識改革については、自社の競争力の源泉たるデジタルサービス等に内在するリスクの所在を適切に把握できるようにする観点から、引き続き必要な「プラス・セキュリティ」知識を補充できる環境整備を推進する。また、中小企業においても、知見や人材等のリソース不足を解消すべく、安価かつ効果的なセキュリティサービス・簡易サイバー保険の普及に向けた取組をさらに発展させる。加えて、あらゆる主体の相互連関・連鎖を自由に形成することで創出される新たな価値に対する信頼性を確保するために、課題の対処を継続して実施する。さらに、誰も取り残さないデジタル・セキュリティ意識の情勢と向上を図るため、サイバーセキュリティやインターネット利用における注意点に関する普及啓発の取組を推進する。

今年度の取組

- サイバーセキュリティ経営の普及啓発活動を行いつつ、適切な状況調査・フォローアップを行い、「プラス・セキュリティ」知識を補充できる環境整備に向けて、モデルカリキュラムの構築を推進する。
- 「共助」の考え方に基づく、地域のコミュニティづくりにおいて、ビジネスマッチングや人材の育成・マッチング、地域発のセキュリティソリューションの開発など地域による課題解決・付加価値を創出する場の形成及び展開を促進する。
- 先端技術・イノベーションの社会実装に向けて引き続き取り組むとともに、海外展開や国際標準化に向けた取組を実施する。
- 児童生徒への情報モラル教育（セキュリティを含む）や、教員等を対象とした研修を一層推進する。

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

２．国民が安全で安心して暮らせるデジタル社会の実現

昨年度の実績

- 政府機関等全体の情報セキュリティ対策の強化・拡充図るために策定した政府機関等の統一基準群に対し、近年のサイバーセキュリティ対策の動向等を踏まえ、次期統一基準群の改定骨子を策定。また、近年のサイバー攻撃事例や手法、最新の技術動向等を踏まえ、政府機関等とGSOC間における効果的かつ効率的な連携を可能とする機能を実装した第４期第一GSOCシステムの構築を実施。
- 重要インフラの防護の観点から、官民が一丸となって、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント及び対処態勢の整備、防御基盤の強化等第４次行動計画に基づく各取組を実施。
- 東京大会に向けて、重要サービス事業者を対象としたリスクマネジメントの促進やサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進。特に新型コロナウイルス感染症の拡大に伴う環境変化を踏まえたリスクの見直し、残留リスクが顕在化した場合の対処態勢の強化を推進。

評価

次期統一基準群の改定骨子の策定にあたり、各政府機関等との目指すべき情報セキュリティ対策の在り方について共通認識を得られた。また第４期第一GSOCシステムの構築により、政府横断的なサイバーセキュリティの強化が図られた。重要インフラの第４次行動計画に基づく取組については、引き続き推進するとともに、東京大会後に同計画の改定に向けた検討を行っていく。さらに、東京大会に向けた取組については、新型コロナウイルス感染症の拡大に伴う環境変化を考慮しながら、対処態勢の強化は図られており、大会直前まで可能な限り取組を推進することが必要である。

今年度の取組

- 統一基準群の改定を実施するとともに、改定後の統一基準群を踏まえた各政府機関等のセキュリティポリシー改定に係る支援等を実施。またGSOCシステムを着実に運用しつつ、デジタル庁における政府情報システムの統合・一体化を踏まえ、より効果的・効率的なGSOC監視の在り方の検討や必要な機能の強化を図る。
- 重要インフラの防護に関しては、第４次行動計画の改定に向けて、各取組に対する評価・見直し等を実施する。
- 東京大会に向けて、引き続きリスク対策を促進するとともに、サイバーセキュリティ対処調整センターの運用及び演習・訓練等を実施し、大会のサイバーセキュリティの確保に万全を期す。

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

３．国際社会の平和・安定及び我が国の安全保障への寄与

昨年度の実績

- 2019年G20大阪サミットで我が国が提示したDFFT（信頼性のある自由なデータ流通）に関し、2020年G20リヤド・サミットにおいても、デジタル経済とともに促進することの重要性を確認。また、国連政府専門家会合、国連オープン・エンド作業部会及びその他各種国際会議等での議論等を通じ、サイバー空間における法の支配を推進するため、国際的なルール及び規範作りに積極的に貢献。
- 国家の強靱性の確保のため、防衛省・自衛隊のネットワーク・インフラの防護の強化や先端技術・防衛関連技術の防護を実施。抑止力の向上として、サイバー防衛能力の抜本的強化に向けた取組を実施するほか、2021年３月の日米安全保障協議委員会等でサイバー分野における協力を一層強化することの重要性を確認。状況把握力の強化に向けて、情報収集・分析等を実施。
- 13の国・地域間、ASEAN諸国及び各種会合や協議会にてサイバー協議を実施し、国際協調・協力を推進。また、ASEAN加盟国とサイバー演習等を継続的に実施するほか、同志国とのオンラインサイバー演習等を実施。さらに、政府全体でASEANを中心とした発展途上国でのサイバーセキュリティ対策の向上に寄与するため、能力構築支援を実施。

評価

外国関係機関との緊密な連携を図り、自由・公正かつ安全なサイバー空間の確保に向けて取り組んでいる一方で、サイバー攻撃の脅威は多様化・複雑化していることから、引き続き外国関係機関との緊密な連携を図り、国際ルールや規範の着実な実践の推進や情報収集・分析力の強化及び能力構築支援によるサイバーセキュリティ対策の向上に積極的に取り組む必要がある。

今年度の取組

- 各二国間協議や国連などにおける多国間協議に参画し、国際法の適用や国際的なルール・規範づくりに積極的に関与する。
- 我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靱性を確保し、防御力、抑止力、状況把握力を高めていく。
- 世界各国との国際協力により、知見の共有・政策調整、平時からのサイバー脅威の情報の共有及び能力構築支援を推進する。

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

４．横断的施策

昨年度の実績

- 「サイバーセキュリティ研究・技術開発取組方針」に基づき、サプライチェーン・リスクに対応するためのオールジャパンの技術検証体制の整備、国内産業の育成・発展に向けた支援策の推進、攻撃把握・分析・共有基盤の強化、暗号等の基礎研究の推進及び産学官連携の研究・技術開発のコミュニティ形成に関して取組を実施。
- 人材の育成・確保を強化していくために、官民の様々な取組を集約するポータルサイトを構築し、試行運用を開始。また、サイバーセキュリティ人材の確保に向けて、戦略マネジメント層の育成・定着、実務者層・技術者層の育成、人材育成基盤の整備及び各府省庁における取組を推進。
- 「サイバーセキュリティ意識・行動強化プログラム」に基づき、サイバーセキュリティの普及啓発に係る状況を特徴づける事項について、継続的に収集しうる客観的なデータを収集・整理。またサイバーセキュリティ月間では、認知度の高いコンテンツ※とのタイアップを行い、標語ごとのポスター作成や普及啓発イベント動画のオンライン配信を行うなど、普及啓発活動を実施。

※ラブライブ！サンシャイン!!

評価

研究開発は「サイバーセキュリティ研究・技術開発取組方針」に基づき、継続して取組を推進する。また、サイバー攻撃の複雑化・巧妙化といった現状認識や実務者層・技術者層の育成に向けた資格・試験や演習、学び直しの促進等の取組の状況を踏まえ、「質」・「量」両面での官民の取組を一層継続・深化させ、社会全体で「DX with Cybersecurity」を推進する必要がある。さらに、「サイバーセキュリティ意識・強化プログラム」に基づき、引き続き取組を実施しつつ、新型コロナウイルス感染症の拡大等による環境変化を踏まえ、サイバーセキュリティの普及啓発におけるコンテンツの不断の改善を図ることが必要である。

標語ポスター
（例　パスワード関係、二要素認証関係）

普及啓発イベント動画の様子
（コンテンツの声優らによるセキュリティ講座）

今年度の取組

- 研究開発については、「サイバーセキュリティ研究・技術開発取組方針」に基づき、関係施策を実施する。
- 「プラス・セキュリティ」知識を補充できる環境整備の一環として、人材育成プログラムの需要と供給に係る対応を双方行い、市場の形成・発展を目指す。
- 普及啓発については、「サイバーセキュリティ意識・行動強化プログラム」に基づき、引き続き取組を推進するとともに、高齢者への対応を含め、プログラムの内容・効果の定期的な評価・見直しを実施する。

２部２章（主な昨年度の取組実績、評価及び今年度の取組）

５．推進体制

昨年度の実績

- 内閣サイバーセキュリティセンターを中心に、関係機関とのパートナーシップに基づく国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、国際担当者間の会合やIWWNでの分析レポートの情報発信により、総合的分析機能の強化を推進
- 戦略の趣旨を国内外の関係者に向け効果的に発信することを目的に、サイバーセキュリティ2020の冊子を制作。内閣官房及び関係府省庁において、戦略のカラー冊子やサイバーセキュリティ2020の冊子を活用するなどして、各種セミナーでの説明等を通じて、戦略等の発信を実施

サイバーセキュリティ戦略

サイバーセキュリティ2020

評価

戦略の国内外の関係者への更なる浸透を図るため、引き続き、取り組むことが重要。（一方で新型コロナウイルス感染症の拡大に伴う各種イベントの中止やオンライン開催への切替により、周知広報活動の機会が減少したことから、今後は実開催のみならず、イベントのオンライン開催を踏まえた従来とは異なる環境変化に柔軟に対応するため、電子版での配布を行うなど、様々な事業者は個人へ幅広く周知広報活動を実施する。）加えて、次期戦略が策定されることから、戦略のメッセージである「Cybersecurity for All ～誰も取り残さないサイバーセキュリティ～」を含め、我が国のサイバーセキュリティ政策の理解・浸透を広く行うことが必要不可欠であり、関係機関との一層の連携強化を図り、次期戦略及びサイバーセキュリティ2021の発信等に取り組むことが求められる。

今年度の取組

- 関係機関の一層の能力強化に向けては、既に構築している仕組みの機能向上を図るとともに、連携体制についても逐次見直しを実施する。
- また、全ての主体に関する自律的な取組を促進するため、引き続き、国内外の関係者へ戦略及びこれに基づく年次計画等の発信を行う。