資料2-3

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

行政機関から見た情報共有への期待

内閣官房　内閣サイバーセキュリティセンター(NISC)

令　和　４　年　６　月　２　０　日
サイバー攻撃被害に係る情報の共有・公表
ガ　イ　ダ　ン　ス　検　討　会

行政機関から見た情報共有への期待

【 サイバーセキュリティ戦略（令和３年9月28日閣議決定）】

（抜粋）

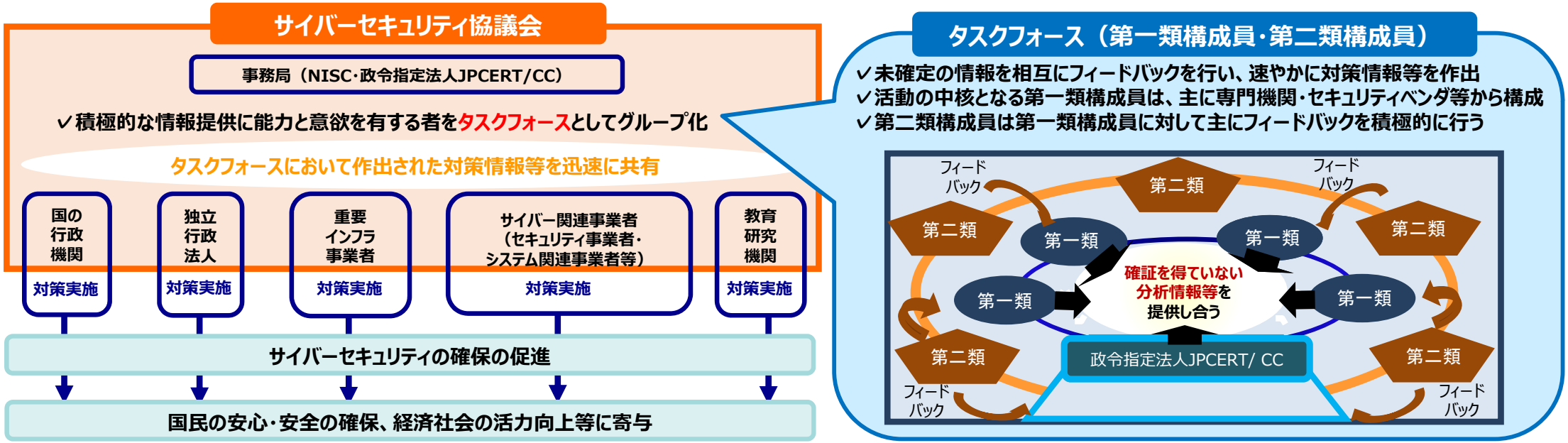
国は、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート（CSIRT/CERT）の枠組みを強化する。具体的には、対処官庁のリソース結集と連携強化を通じて対処能力の向上と対処に係る一体性・連動性を図るとともに、サイバー関連事業者との連携強化によって**組織・分野横断的に影響が波及し得る事案の情報収集や初動を含めた対処調整の迅速化を図る。**また、**サイバーセキュリティ協議会や**サイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する**専門機関をはじめとした情報共有体制間や海外関係機関との連携を一層推進する**ことで、官民間・国際間での情報共有と対処調整の円滑化を図る。

- **政府が有する情報に加えて、民間の組織・分野横断的な情報も収集・分析することで、我が国への攻撃動向等の把握につなげる。**
- **その結果、官民の多様な主体へのフィードバック（注意喚起等）が一層充実し、サイバー攻撃の被害の未然防止や拡大防止が図られ、我が国のサイバーセキュリティが向上。**

官民間の情報共有強化に向けた取組の現状

【サイバーセキュリティ協議会　概要】

・サイバーセキュリティ基本法の一部を改正する法律に基づき、平成31年４月にサイバーセキュリティ協議会が組織され、同年５月下旬から情報共有活動が開始されている。
・本協議会は、国の行政機関、重要社会基盤事業者、サイバー関連事業者等、官民の多様な主体が相互に連携し、より早期の段階で、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことなどを目的としている。
・令和３年度は60件の情報を取り扱い、これらの案件について、23回、対策情報等を作出し、広く公開等を実施。



・共有可能な情報が整理され、その理解が進むことにより、サイバーセキュリティ協議会に寄せられる情報も増えることを期待。
・その結果、対策情報等の作出が一層充実し、サイバーセキュリティ協議会におけるサイバー攻撃の被害の未然防止や拡大防止が図られ、我が国のサイバーセキュリティが向上。

政府によるフィードバックの取組の現状（注意喚起）

- 「サイバーセキュリティ戦略」（令和３年9月28日閣議決定）において、国が深刻なサイバー攻撃に対し、一体的に取り組むため「ナショナルサート機能の強化」を打ち出しているところ。
- 当該取組の一環として、サイバー攻撃事案の潜在的なリスクの高まり等昨今の情勢を踏まえ、本年２月以降、関係省庁が連携して、立て続けに注意喚起を発出。
- 今後も、政府機関、特にNISCに情報が集約されることを通じ、産業界等に適時、横断的に注意喚起を行い、被害の未然防止、再発防止のための対応を強化。

＜3月24日の注意喚起の例＞

令和４年３月２４日
経済産業省
総務省
警察庁
内閣官房内閣サイバーセキュリティセンター

現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）

昨今のサイバー攻撃事案のリスクの高まりを踏まえ、政府においては、２月23日に「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（※1）」、３月１日に「サイバーセキュリティ対策の強化について（※2）」注意喚起を行っております。

その後も、国内では、ランサムウェアによる攻撃をはじめとするサイバー攻撃事案の報告が続いており、また、エモテットと呼ばれるマルウェアの増加も見られるところです。また、米国では、３月21日に、バイデン大統領が、国内の重要インフラ事業者等に対して、ロシアが潜在的なサイバー攻撃の選択肢を模索しており警戒を呼びかける声明を発表するとともに、企業等に対してサイバーセキュリティ対策を強化する具体策を提示しています。

このような現下の情勢を踏まえ、政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、上記の**２月23日及び３月１日の注意喚起にある対策（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）の徹底**をあらためてお願いいたします。また、ランサムウェアやエモテットについては、これまで専門機関等において公表している情報・サイトを確認の上、対応を講じるようお願いいたします。あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して情報提供いただくとともに、警察にもご相談ください。

（以下、参考URL（略））

【参考】

※１） **２月23日、経済産業省より、「昨今の情勢を踏まえたサイバーセキュリティ対策の強化」（注意喚起）を発出。**（各企業・団体に対して、経営者のリーダーシップの下、脅威への認識を深め、リスク低減のための措置、インシデントの早期検知、インシデント発生時の適切な対処・回復を要請。）

※２） **３月１日、**トヨタ事案を踏まえ、**経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、NISCの連名により、「サイバーセキュリティ対策の強化」（注意喚起）を発出。**（政府機関や重要インフラ事業者を初めとする各企業・団体等に対策の強化を要請。）

※３） **4月25日、**長期休暇期間がサイバーセキュリティに与えるリスクに鑑み、**経済産業省、総務省、警察庁、NISCの連名により、「春の大型連休に向けて実施いただきたい対策」（注意喚起）を発出。**（政府機関や重要インフラ事業者を初めとする各企業・団体等に対策の実施を要請。）