サイバーセキュリティ2018の全体概要

資料２－３

平成30年７月25日
サイバーセキュリティ戦略本部決定

項目	主な施策例
1. 経済社会の活力の向上及び持続的発展	
1.1 新たな価値創出を支えるサイバーセキュリティの推進	
(1) 経営層の意識改革	・官民の連携による、経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催【NISC】
(2) サイバーセキュリティに対する投資の推進	・サイバーセキュリティ保険の普及、情報開示・共有を促進するためのモデル事業の検討【総務省及び経済産業省】
(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化	・セキュリティ製品・サービスの有効性検証、レーティングを実施できる環境整備の検討【経済産業省】
1.2 多様なつながりから価値を生み出すサプライチェーンの実現	
(1) サイバーセキュリティ対策指針の策定	・「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定【経済産業省】
(2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築	・中小企業を含むサプライチェーン全体を守ることに活用できる「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装の推進【内閣府】
(3) 中小企業の取組の促進	・中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」への登録を促すことによるセキュリティレベル向上の促進【経済産業省】
1.3 安全なIoTシステムの構築	
(1) IoTシステムにおけるサイバーセキュリティの体系の整備と国際標準化	・「IoTセキュリティガイドライン」を様々な産業分野の標準仕様等への反映に向けた普及、国際的展開に向けた活動【総務省及び経済産業省】
(2) 脆弱性対策に係る体制の整備	・パスワード設定に不備のある機器の調査、IoT機器に対する脆弱性対策に関する実施体制の整備【総務省】
2. 国民が安全で安心して暮らせる社会の実現	
2.1 国民・社会を守るための取組	
(1) 安全・安心なサイバー空間の利用環境の構築	・ソフトウェア等の脆弱性に関する情報を利用者に提供【経済産業省】 ・情報通信ネットワークの変化、新たなサービス提供に伴い社会・経済に生じ得るリスク源の評価、情報通信ネットワークに関連するハードウェア、ソフトウェアの市場動向及び技術開発動向等についての調査【NISC、総務省、経済産業省】 ・仮想通貨交換業者におけるサイバーセキュリティの強化に向け、実効性のある自主規制機能の確立を促進【金融庁】
(2) サイバー犯罪への対策	・取締り・捜査に必要な専門的知識・技能の習得のための各種研修の実施【警察庁及び法務省】
2.2 官民一体となった重要インフラの防護	
(1) 行動計画に基づく主な取組	・第４次行動計画に基づき、リスクマネジメントの推進、安全基準等の改善・浸透、深刻度評価基準、官民の枠を超えた訓練・演習の実施、制御系システムのセキュリティ対策等を推進【NISC及び重要インフラ所管省庁】
(2) 地方公共団体のセキュリティ強化・充実	・地方公共団体職員を対象とした集合研修・eラーニングを実施、セキュリティポリシーに関するガイドラインを随時更新【総務省】 ・緊急時対応訓練の支援及びCSIRT※1の連携組織の設立【総務省】
2.3 政府機関等におけるセキュリティ強化・充実	
(1) 情報システムのセキュリティ対策の高度化・可視化	・政府機関情報システムのサイバー攻撃等に関する情報を収集・分析し、分析結果を各政府機関等へ適宜提供【NISC】
(2) クラウド化の推進等による効果的なセキュリティ対策	・政府機関におけるクラウドサービス利用状況の調査及び課題の把握、新たな政府のプライベート・クラウドとしての整備計画の策定【NISC及び総務省】
(3) 先端技術の活用による先取り対応への挑戦	・サイバー攻撃による高い耐性を有する情報システム基盤の情報技術について、政府機関等での活用可能性を検証【NISC】
(4) 監査を通じたサイバーセキュリティの水準の向上	・政府機関、独立行政法人等への監査・ペネトレーションテストの実施【内閣官房】
(5) 組織的な対応能力の充実	・政府機関におけるサイバー攻撃に係る対処要員の能力等の強化を図るため、研修や実践的サイバー防御演習(CYDER)を実施【NISC及び総務省】
2.4 大学等における安全・安心な教育・研究環境の確保	
(1) 大学等の多様性を踏まえた対策の推進	・自律的かつ組織的に取り組むべきサイバーセキュリティ対策についての検討、サイバーセキュリティに関するガイドライン等の策定【文部科学省】
(2) 大学等の連携協力による取組の推進	・サイバー攻撃に関する情報や共通課題、事案対応の知見等を共有するための手法を検討【文部科学省】
2.5 2020年東京大会とその後を見据えた取組	
(1) 2020年東京大会に向けた態勢の整備	・「サイバーセキュリティ対処調整センター」の構築を推進、横断的リスク評価の実施【NISC】
(2) 未来につながる成果の継承	・大会後も各種施策は適用範囲を拡大して引き続き推進し、整備した仕組み、その運用経験及びノウハウはレガシーとして、以降の我が国の持続的なサイバーセキュリティの強化のために活用【NISC】
2.6 従来の枠を超えた情報共有・連携体制の構築	・ISAC※2を含む既存の情報共有の推進【NISCおよび関係省庁】
(1) 多様な主体の情報共有・連携の推進	・サイバーセキュリティに関する施策の推進に係る協議を行うための協議会創設に向けた検討【NISC】
(2) 情報共有・連携の新たな段階へ	・積極的に情報の共有に貢献する参加者が評価される環境整備に向けた検討【NISC】
2.7 大規模サイバー攻撃事態等への対処態勢の強化	・関係府省庁、重要インフラ事業者等と連携した初動対処訓練の実施【内閣官房】

項目	主な施策例
3. 国際社会の平和・安定及び我が国の安全保障への寄与	
3.1 自由、公正かつ安全なサイバー空間の堅持	・ハイレベルの会談・協議等を通じ、サイバー空間における我が国の利益が達成されるよう、戦略的な取組を推進【NISC】
(1) 自由、公正かつ安全なサイバー空間の理念の発信	・各二国間協議や多国間協議に参画し、我が国の意見表明や情報発信を実施【NISC及び外務省】
(2) サイバー空間における法の支配の推進	・サイバー空間における国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映させるよう取組を推進【NISC及び外務省】
3.2 我が国の防御力・抑止力・状況把握力の強化	
(1) 国家の強靱性の確保	・サイバー攻撃対処を行う部隊の能力の向上、自らの活動が依存するネットワーク・インフラの防護の強化、自衛隊の任務保証に関係する主体との連携の深化【防衛省】
(2) サイバー攻撃に対する抑止力の向上	・内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進【内閣官房】
(3) サイバー空間の状況把握の強化	・諸外国関係機関との情報交換等国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を継続的に実施【警察庁、法務省】
3.3 国際協力・連携	・各国機関との連携、国際会議への参加、我が国での国際会議の開催等を通じ、我が国の情報セキュリティ人材が海外の優秀な技術者等と研鑽を積む場を増やす取組の実施【NISC】
(1) 知見の共有・政策調整	・国際的な会議の場等を活用し、二国間協議に加え，各国とのサイバーセキュリティ分野における関係を強化【NISC及び外務省】
(2) 事故対応等に係る国際連携の強化	・インシデント対応演習等を通じ、各国との情報共有・インシデント発生時の国外との情報連絡体制を整備【NISC】
(3) 能力構築支援	・ASEAN等における能力構築を政府一体的に支援【NISC及び関係各省】
4. 横断的施策	
4.1 人材育成・確保	・人材育成施策について、施策間の連携の強化、横断的かつ継続的に人材育成施策の全体像が把握できるよう「見える化」を推進【NISC】
(1) 戦略マネジメント層の育成・定着	・戦略マネジメント層育成に向けて、必要な知識・スキルを身に着けるための試行的取組を検討【NISC】
(2) 実務者層・技術者層の育成	・「ナショナルサイバートレーニングセンター」を通じ実践的サイバー防御演習（CYDER）の実施【総務省】 ・セキュリティ技術コンテスト「SECCON 2018」の普及・広報支援【経済産業省】
(3) 人材育成基盤の整備	・発達の段階に応じた情報セキュリティを含めた情報活用能力を培う教育の推進、教員等を対象とした研修を実施【文部科学省】
(4) 各府省庁におけるセキュリティ人材の確保・育成の強化	・体制の整備・人材の拡充、一定の専門性を有する人材の育成等、政府部内のセキュリティ人材の充実に係る諸施策をより一層推進【NISC】
(5) 国際連携の推進	・人材育成に取り組む大学や公的機関等の研究・教育プログラムに係る基準や諸外国との連携方策について検討【NISC】
4.2 研究開発の推進	
(1) 実践的な研究開発の推進	・IoT機器のセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術等を開発【内閣府】
(2) 中長期的な技術・社会の進化を視野に入れた対応	・「サイバーセキュリティ研究開発戦略」について、目下の課題を解決すべく、融合領域の研究動向についての調査等を検討【NISC】
4.3 全員参加による協働	・「サイバーセキュリティ月間」をはじめとし、サイバーセキュリティに関する各種イベント等の開催や情報発信等を通じ普及啓発活動を推進【NISC】
5. 推進体制	・関係機関の一層の能力強化、サイバーセキュリティに関する自律的な取組の促進及び国内外への積極的な情報発信【NISC】

※1 Computer Security Incident Response Teamの略（シーサート）。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。

※2 Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。