News Release

総務省
MIC 北海道総合通信局

経済産業省
北海道経済産業局

Hokkaido Prefectural Police
北海道警察

道内における
サイバーセキュリティの現状と対策について

2021年7月

北海道地域情報セキュリティ連絡会（HAISL）

北海道総合通信局
北海道経済産業局
北海道警察

１．道内におけるサイバーセキュリティの現状とHAISLについて

２．HAISLによる主なサイバーセキュリティの取組

（参考）政府におけるサイバーセキュリティ対策

１．はじめに

◆ 政府では、インターネットの急速な利用拡大など我が国社会や国民生活のＩＴ化が進展する中で、**不正アクセス事案の発生やコンピュータウイルスの蔓延など情報セキュリティに関わる問題への危機感の高まり**を受け、これまでに「サイバーセキュリティ基本法」制定（2014年）、「サイバーセキュリティ戦略本部」・「内閣サイバーセキュリティセンター（NISC）」設置（2015年）、「サイバーセキュリティ戦略」策定（2018年）等、様々な取組を推進。

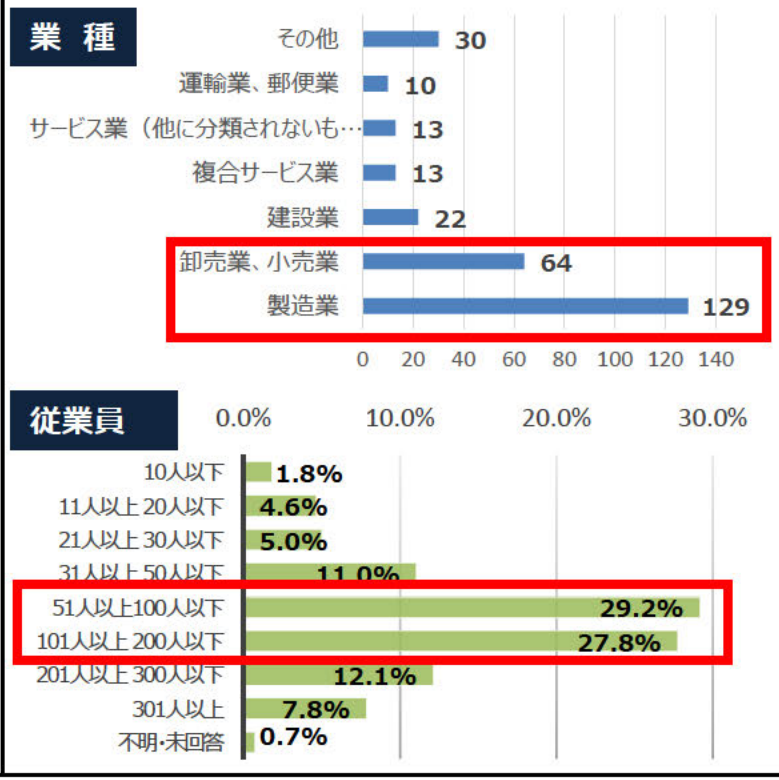
◆ 道内では、**北海道総合通信局・北海道経済産業局・北海道警察の3機関が連携した「北海道地域情報セキュリティ連絡会（HAISL）」の活動を通じ、北海道における情報セキュリティ意識の向上、情報セキュリティ対策の促進および人材の育成に向けた環境整備を実施。**

◆ **このような状況において、新型コロナウイルスの感染拡大に伴い、テレワークの導入など、ITインフラの整備を進める企業が増加**しており、企業規模を問わず、**サイバー攻撃の高度化等に伴うリスク・被害も増大していくことが予想されることを踏まえ、中小企業等のサイバーセキュリティに関するリテラシー向上が必要**。

◆ DX促進と併せて、サイバーセキュリティ対策が求められることから、当該3機関では、今後、**HAISLの更なる強化・拡充を通じ、道内におけるサイバーセキュリティに関する機運醸成・理解向上等を強力に推進**していく。

1-2-1. 道内中小企業におけるサイバーセキュリティ対策の現状

- 北海道経済産業局では、道内中小企業のサイバーセキュリティ対策への理解度を把握するとともに、対策レベルに合わせた支援方法の検討を行うための情報を収集することを目的として、アンケート調査を実施した。

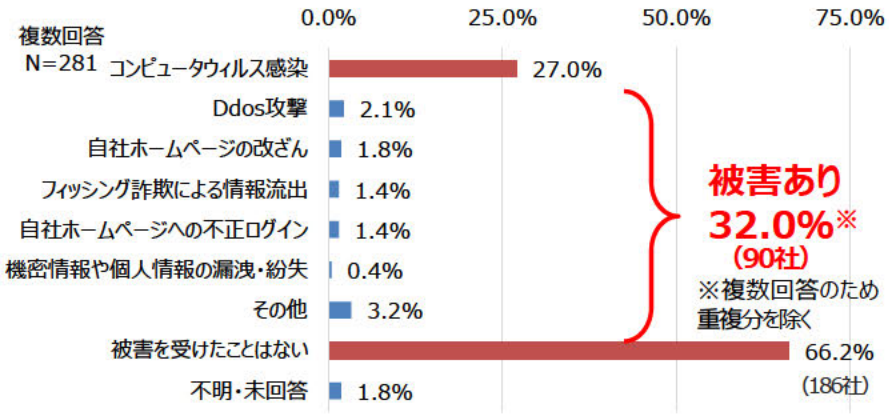
調査対象	TSRに登録されている道内中小企業のうち、製造業・非製造業それぞれ売上上位500社
調査方法	郵送（調査票）およびインターネット調査（専用webサイト）
調査期間	2020年9月～10月
回答率	281社 ／ 1,000社（28.1%）
回答企業の属性 (N=281)	

【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』

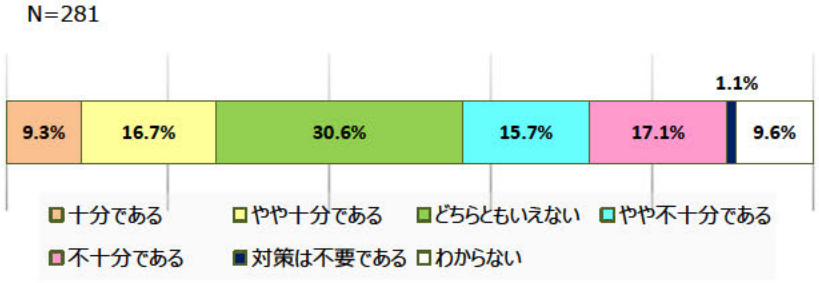
1-2-2. 調査結果

- 3割以上（32.0%）がサイバー攻撃の被害に遭っている
- 9割以上の企業がウイルス対策ソフトを導入済み
- 対策を行うことができる人材が不足するとともに危機意識が低いことが課題

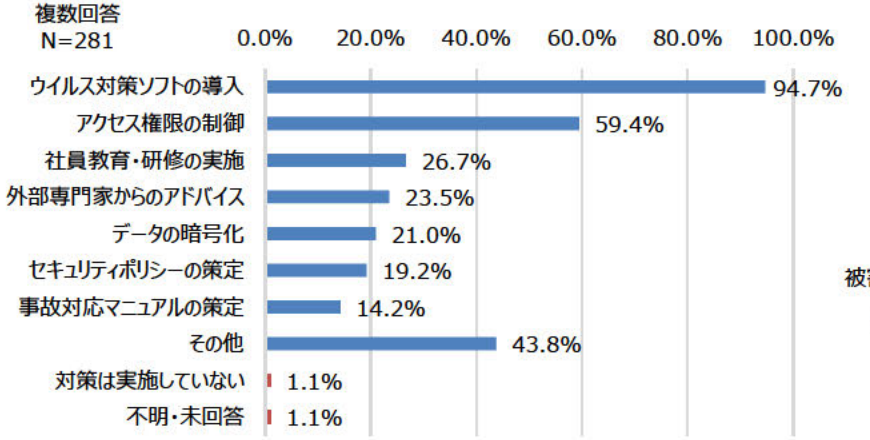
Q：貴社が受けたことのあるサイバーセキュリティ被害は？



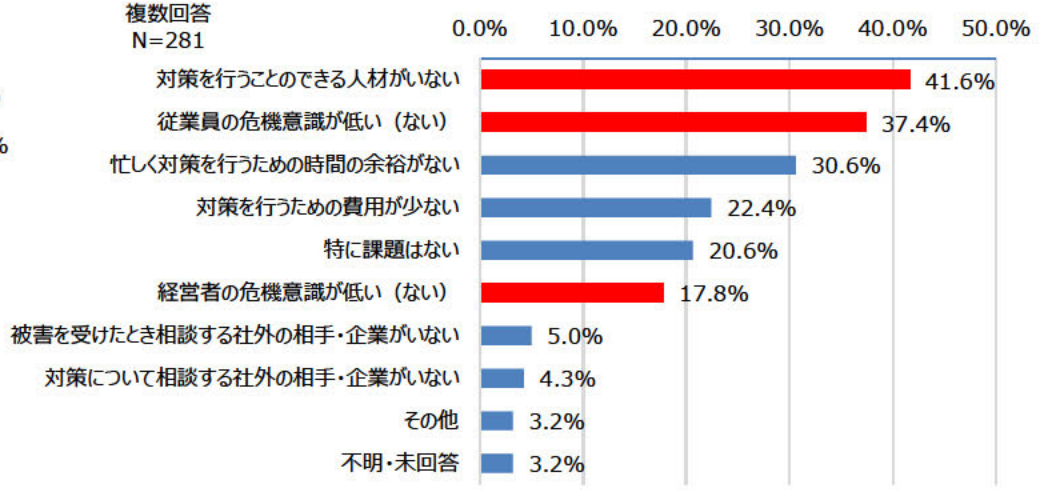
Q：サイバーセキュリティ対策について、現在の対応で十分だと感じていますか？



Q：実施済みのサイバーセキュリティ対策は何ですか？



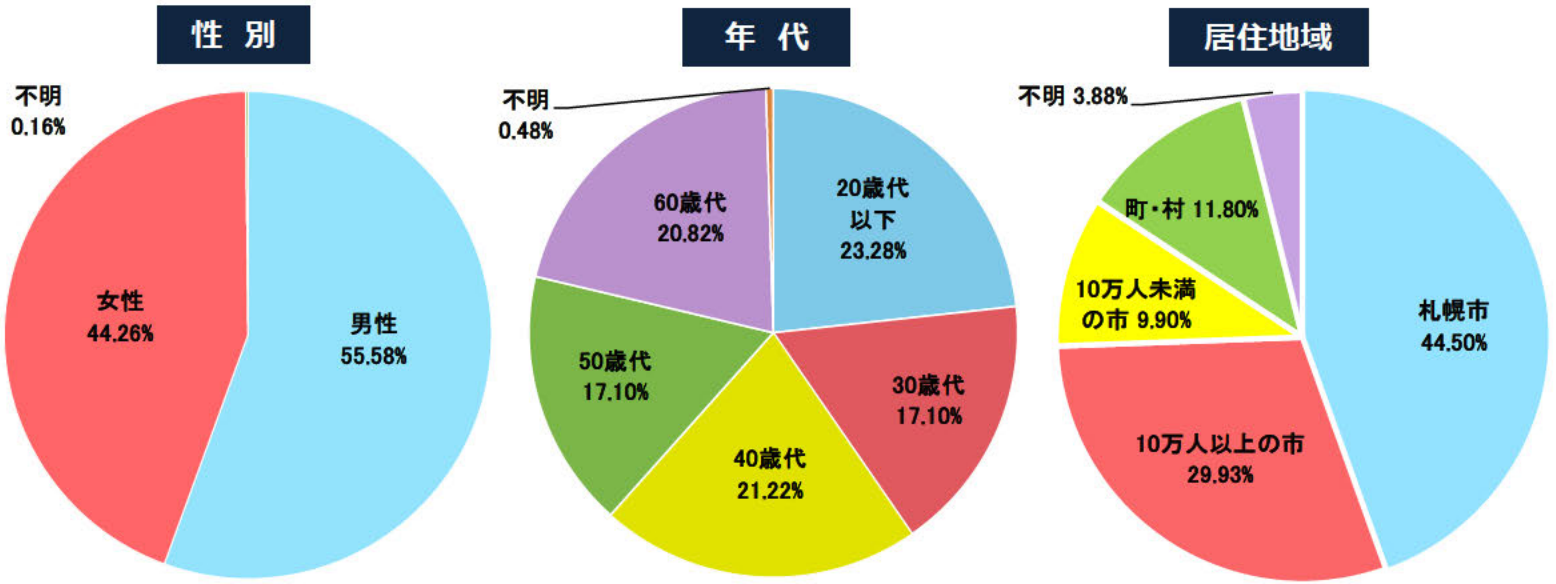
Q：サイバーセキュリティに関する課題は？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』

1-2-3. 警察活動等に関する道民の意識調査

- 北海道警察では、犯罪や事故のない安心して暮らせる北海道の実現に向けて、北海道警察の重要課題や主要施策について、道民の意識を調査してニーズを把握し、各種施策に反映させることを目的として、調査を実施した。

調査対象	北海道に居住する運転免許更新者
調査方法	調査票の配布
調査期間	2020年7月
回答率	1,263人 ／ 1,279人（98.75%）
有効回答者の構成	

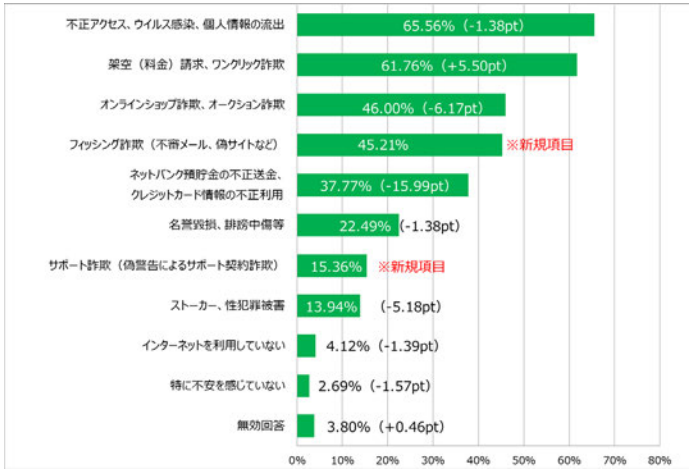
【出典】警察活動等に関する道民の意識調査結果 北海道警察

1-2-4. 調査結果

- 不正アクセス、ウイルス感染による個人情報流出をはじめ、架空請求など、身近な犯罪への不安が多い
- 警察による犯罪検挙のほか、地域、企業、学校等との連携強化による被害防止対策が期待されている

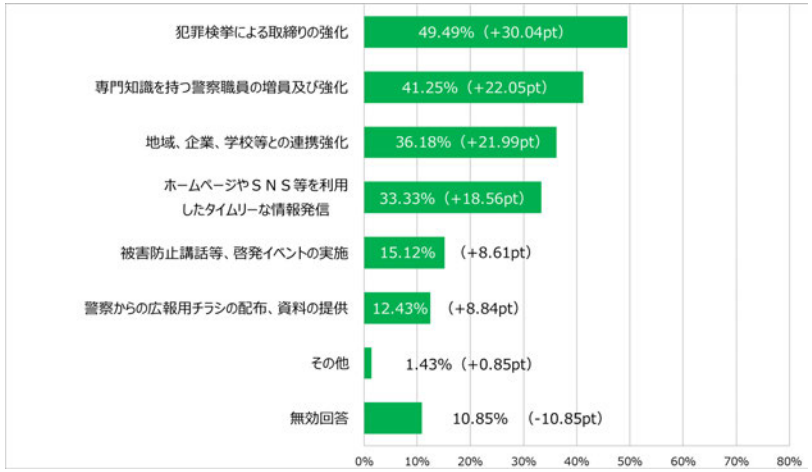
・インターネット空間で、不安に感じる犯罪や被害は何ですか。（複数回答）

※（　）内の数値は、前回（H30）調査時と比較したもの



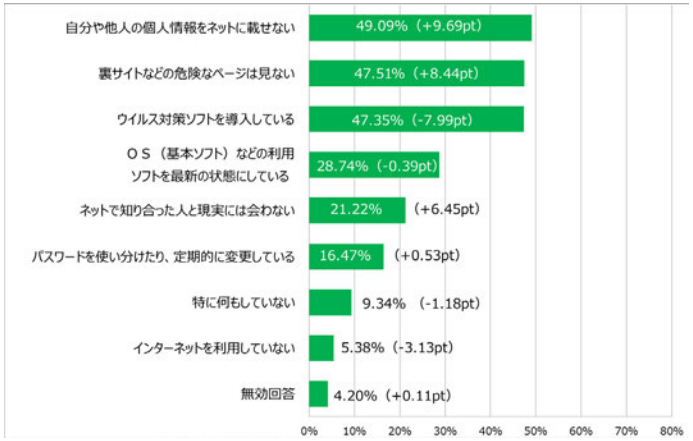
・インターネット空間の安全を守るため、警察にどのような活動を期待しますか。（複数回答）

※（　）内の数値は、前回（H30）調査時と比較したもの



・インターネット空間での犯罪被害に遭わないために、どのような対策をしていますか。（複数回答）

※（　）内の数値は、前回（H30）調査時と比較したもの



【出典】警察活動等に関する道民の意識調査結果 北海道警察

1-3. まとめ（アンケート調査結果）

①サイバーセキュリティに対する意識の低さ

道内の中小企業のサイバーセキュリティに対する意識の低さが明らかとなった。意識の低さは、経営層、従業員に共通しているが、従業員の意識が高まったとしても、**経営層がサイバーセキュリティ対策の重要性を認識しない限り、対策に必要な人員の配置やコストの負担は行われない**ことから、より重要なことは経営層の意識を高めることにある。

②セキュリティ人材の不足

セキュリティ対策のレベルにかかわらず、**企業においてセキュリティの知識を持った人材が不足**している。一方で、セキュリティ教育に対するニーズは幅広い年代層に潜在しており、**セキュリティ人材の育成・確保のためには年齢や立場にとらわれない学習機会を提供していくことが必要**。

③連携による対策が求められている

北海道警察本部が実施したアンケート調査結果によると、警察に期待されることとして、取締りの強化、専門知識を持つ警察職員の配置、強化に次いで、地域、企業、学校等との連携強化が上げられてることから、今後、**産学官がそれぞれの得意分野で協力するサイバーセキュリティ対策が必要**と考えられる。

1-4-1. 北海道地域情報セキュリティ連絡会（HAISL）によるサイバーセキュリティ対策の取組

Hokkaido Area Information Security Liaison

- 2014年9月、**総合通信局、経済産業局、道警察の3機関が連携し、全国に先駆けて「北海道地域情報セキュリティ連絡会（HAISL）」を発足。**道内の情報セキュリティ推進機関として、普及啓発や人材育成等を実施。
- 2020年度は、サイバーリスクの理解促進に向けた取組を展開したほか、**大学・高専等と連携した人材育成プロジェクト「SC4Y」の始動**など、HAISLの取組を強化・拡充してサイバーセキュリティ普及を強力に推進。

【HAISL事務局】

総務省 北海道総合通信局 × 経済産業省 北海道経済産業局 × Hokkaido Prefectural Police 北海道警察

産学官による地域コミュニティとして、企業経営者・セキュリティ担当者、支援機関等を対象とした情報セキュリティに関する意識の喚起や、情報セキュリティ技術・セキュリティマネジメント能力向上に向けた機会を提供することにより、セキュリティ意識の向上や人材育成を実施。

【会長】北海道大学　高井教授
【参加機関】49企業・団体等
【設立】2014年9月

普及啓発

☆情報セキュリティセミナー

中小企業等におけるサイバーリスクに対するリテラシー向上を目的に、DX with Cybersecurityに関する講演のほか、セミナーでは初となるサイバー攻撃演習を実施。（'20/12/1）

人材育成

☆Security College for Youth(SC4Y)

複数の道内教育機関等と連携し、学生向け教育カリキュラムを試行。

（勉強会：'20/8/29、'20/11/28、'21/2/10、'21/2/28）

道内中小企業のサイバー対策の現状

道内全域対象の初の実態調査

4割以上（41.6%）「経営者等の危機意識が低い」

3社に1社（90社）サイバー攻撃の被害

専門人材不足が浮き彫り **41.6%**（117社）「対策できる人材がいない」

1-4-2. 北海道地域情報セキュリティ連絡会（HAISL）

Hokkaido Area Information Security Liaison

- 現在、事務局も含めて49機関が参画。2014年9月発足時（28機関）より順次拡大中。

2021.7.1現在（49機関）

カテゴリ		主な機関
産	団体等	北海道IT推進協会、北海道インターネットカフェ等防犯連絡協議会、北海道サイバーテロ対策協議会、札幌銀行協会、北海道信用金庫協会、北海道防犯協会連合会、社会インフラ企業情報連絡会、テレコムサービス協会北海道支部、北海道ITコーディネータ協議会、北海道クレジットカード犯罪対策連絡協議会 【10】
	企業	日本赤十字社北海道支部、北海道ソフトウェア技術開発機構、北海道総合通信網、HBA、HDC、トレンドマイクロ、さくらインターネット、日本システム機器、富士通、エスアイピー、ピットクルー、アライドテレシス、インターネットイニシアティブ、大日本印刷、東日本電信電話（NTT東日本） 【15】
学	大学	北海道大学、小樽商科大学、北海道科学大学、北海道情報大学、北海学園大学、千歳科学技術大学、札幌市立大学、室蘭工業大学、名寄市立大学、釧路公立大学、北見工業大学 【11】
	その他	苫小牧工業高等専門学校、函館工業高等専門学校、北海道ハイテクノロジー専門学校、北海道情報専門学校 【4】
官	国	北海道総合通信局、北海道経済産業局、北海道警察 【3】
	自治体	北海道、北海道教育庁、札幌市、札幌市教育委員会 【4】
個	コミュニティ等	LOCAL、北海道情報セキュリティ勉強会【2】

1-4-3. 広報関係

- 事務局機関の各HPのほか、HAISL独自にちらし配布やFacebookにおける情報配信を実施中。

【HAISLへの入会について】

HAISLは現在、産学官の49機関によって構成されています。
入会希望は、企業、団体、個人を対象として随時受け付けており、入会料、年会費等は無料となっております。
会に入会することによって、事務局からサイバーセキュリティに関する最新の情報やHAISLが開催するセキュリティ関連のイベント情報等が提供されます。入会をご希望される場合は下記事務局までお問い合わせください。

問合せ先
総務省北海道総合通信局サイバーセキュリティ室　TEL：011-709-2311(内線4767)
経済産業省北海道経済産業局地域経済部製造・情報産業課　TEL：011-709-2311（内線2566）
北海道警察サイバーセキュリティ対策本部　TEL：011-251-0110（内線2976）

事務局機関HP等

【出典】北海道地域情報セキュリティ連絡会（HAISL）～Facebook～
https://www.facebook.com/haisl0929

【出典】北海道警察～サイバーセキュリティ取組紹介～
https://www.police.pref.hokkaido.lg.jp/info/seian/cyber-bouhan-hiroba/activity/activity.html

【出典】北海道経済産業局～IT・情報政策-情報セキュリティ～
https://www.hkd.meti.go.jp/information/it/security.htm

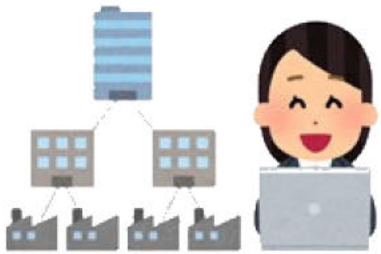
1-5. 北海道中小企業サイバーセキュリティ支援ネットワーク（Cyber-道net）

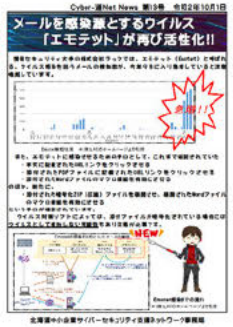
- 中小企業支援に関わる機関等が相互連携し、道内中小企業に対してサイバーセキュリティの意識醸成に資する情報提供等を通じて、健全かつ安心安全なサイバー空間で事業活動が行えるよう支援するため、2017年7月に北海道警察を事務局として発足。

構成機関名
（一社）北海道商工会議所連合会
北海道商工会連合会
北海道中小企業団体中央会
札幌商工会議所
(株)北海道ソフトウェア技術開発機構
（公財）北海道中小企業総合支援センター
（一財）さっぽろ産業振興財団 【札幌中小企業支援センター】
（一社）北海道IT推進協会
経済産業省 北海道経済産業局 【製造・情報産業課】
北海道 【中小企業課】
札幌市 【商業・金融支援課】
北海道警察 【サイバーセキュリティ対策本部】

情報発信

理解しやすい内容で、タイムリーに発信





▲メルマガ情報（2020.10.1配信）

セミナー等の企画、開催

企業のレベルに合わせたセミナーの定期的な開催

▲2021年２月開催（オンライン）
◀2020年２月開催

１．道内におけるサイバーセキュリティの現状とHAISLについて

２．HAISLによる主なサイバーセキュリティの取組

（参考）政府におけるサイバーセキュリティ対策

2．サイバーセキュリティ対策の取組

- コロナ禍におけるオンライン化、デジタル化などのDXの推進に伴い、外部からサイバー攻撃を受けるリスク増大。
- HAISLおよび各事務局機関では、道内中小企業向けにサイバーセキュリティ対策の促進や担い手となる人材育成強化を図るために以下の取組を実施予定。

【サイバーセキュリティ人材の育成】

①人材育成プロジェクト「SC4Y」

- HAISLとサイバーセキュリティ分野に携わる複数の教育機関が連携した「人材育成プロジェクト(SC4Y)」による学生を対象としたサイバーセキュリティ人材の育成・確保に向けた勉強会等を実施

②セキュリティ・ミニキャンプ

- 次代を担う日本発で世界に通用する若年層の情報セキュリティ人材を発掘・育成するため、産業界、教育界を結集した講師による「セキュリティ・ミニキャンプ」を実施

【周知・広報活動】

③サイバーセキュリティに関するセミナー等の開催

- HAISL会員を対象とした連絡会や一般公開型セミナーの開催
- サイバーセキュリティフォーラムの開催
- 啓発、注意喚起資料の作成・発信

【演習・実証】

④実践的サイバー防御演習「CYDER」

- 国の機関、指定法人、独立行政法人、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習(CYDER)を実施

⑤サイバーセキュリティ対策実証モデル構築

- 中業企業がかけられる現実的なコストで効果的なセキュリティ対策を行うための実証を行う

2-1. ①_2021年度人材育成プロジェクト【SC4Y】

- 北海道警察では、HAISLとサイバーセキュリティ分野に携わる複数の教育機関が連携し、新たに「人材育成プロジェクト（SC4Y）」を立ち上げ、学生期からのサイバーセキュリティ人材の育成・確保に向けた取組を試行。

サイバーセキュリティを学ぶ上で、何から手をつければ良いのか分からない
セキュリティ対策に必要な基本的知識や技術が足りなかった
体系的にセキュリティを学べるような研修機会がない・・・

参加した学生

学ぶ意欲がある学生は多いその意欲を潰さないよう、学ぶ機会を提供することが肝要なのでは・・・

●Security College for Youth(SC4Y）の始動

北海道大学、（一社）LOCAL、公立千歳科学技術大学、北海道情報大学、苫小牧工業高等専門学校、北海道ハイテクノロジー専門学校、北海道地域情報セキュリティ連絡会（総通局、経産局、道警）

- 今後、社会の様々な分野で活躍する学生、青年層に、サイバーセキュリティに関する知見、技術を体系的に身につけてもらう
- 将来のセキュリティリーダー、ホワイトハッカーになり得る人材の発掘と育成
- 知見・技術のある青年層を輩出することによる社会全体のセキュリティ対処能力の底上げ

■オンライン勉強会
①'21/5/22（土）
②'21/6/26（土）
③'21/8/28（土）

定期的な勉強会の実施
（段階的に知識を身につける）

競技会の開催
（研鑽した力を試す）

■競技会
Micro Hardening
'21/10/2（土）

まとめ学習
（反省・教訓を今後に生かす）

2-2. ②_2021年度セキュリティ・ミニキャンプ【HAISL】

- 経産省・IPAでは、学生に対して情報セキュリティに関する高度な技術教育を実施し、次代を担う情報セキュリティ人材を発掘・育成するため、「セキュリティ・キャンプ」事業を2004年から開始。全国大会を首都圏で毎年1回、2013年に開始された地方大会を毎年各地で10回程度開催。
- 北海道においても、（一社）LOCAL等が主催団体となり2014年から毎年開催しており、2021年度も開催予定。

【参考：2020年度開催実績】

★実施団体：一般社団法人LOCAL

・名称：セキュリティ・ミニキャンプin北海道2020
・日時：2020年11月7～8日@北海道大学
・主催：LOCAL、北海道大学、セキュリティ・キャンプ協議会、IPA
・共催等：北海道経済産業局、HAISL（総通局・経産局・道警）
・内容：サイバーセキュリティに関する一般講座、座学・演習など
・参加人数：13名

『CTF形式で学ぶ Cプログラムの脆弱性』
灰原 渉　氏（室蘭工業大学・LOCAL学生部）
セキュリティ競技であるCTFには、プログラムの脆弱性を見つけて攻撃する、Pwnと呼ばれる分野があります。この講義では、Pwnの問題を解くことで、Cプログラムに潜む脆弱性について理解を深めます。

『クライアント & サーバアプリケーションセキュリティ入門』
岸谷 隆久　氏（株式会社イエラエセキュリティ）
現代のスマートフォンやパソコン向けの多くのアプリケーションは、インターネットを介してサーバとの通信を行いながら動作することが一般的です。本講義では演習用アプリケーションを題材に、動作の解析や通信内容の調査を行ってアプリケーションセキュリティについて考えます。

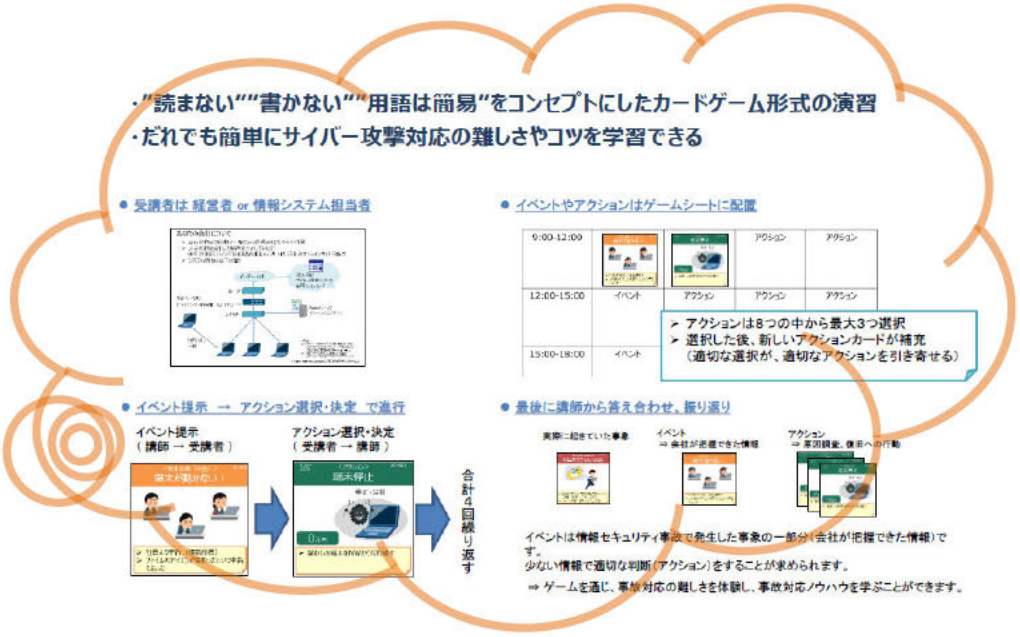
【引用】情報処理推進機構HP「未踏／セキュリティ・キャンプ」https://www.ipa.go.jp/jinzai/camp/2020/minicamp2020_hokkaido.html
セキュリティ・キャンプ協議会HP「セキュリティ・ミニキャンプin北海道2020」https://www.security-camp.or.jp/minicamp/hokkaido2020.html

2-3. ③-1_2021年度「北海道地域情報セキュリティセミナー」の開催【HAISL】

- 北海道地域情報セキュリティ連絡会（HAISL／事務局：北海道総合通信局、北海道経済産業局、北海道警察）では、コロナ禍でのDX進展に伴うサイバーセキュリティの重要性や企業が取り組むべきセキュリティ対策を紹介することを目的に、「北海道地域情報セキュリティセミナー」（仮称）を開催予定。

【参考：2020年度開催実績】

- 日時：2020年12月1日（火）　13時30分から16時30分
- 形式：オンライン開催（YouTube配信／参加無料）
- 対象：HAISL会員、企業の経営者・サイバーセキュリティ担当者、支援機関　等
- 主催：北海道地域情報セキュリティ連絡会（HAISL）
- 共催：経済産業省北海道経済産業局、(株)道銀地域総合研究所、NTT東日本(株)
- 最大同時視聴数：90名

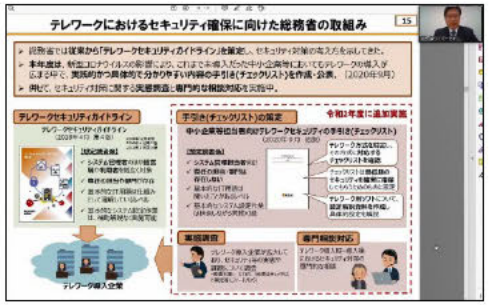


2-3. ③-2_2021年度「サイバーセキュリティフォーラム北海道」の開催【北海道総合通信局】

- 北海道総合通信局は、北海道地域情報セキュリティ連絡会と連携し、北海道におけるサイバーセキュリティの人材育成、サイバーセキュリティレベルの強化を目的に、コロナ禍におけるサイバーセキュリティ政策の最新動向やセキュリティ対策などを紹介する「サイバーセキュリティフォーラム北海道」(仮称)をサイバーセキュリティ月間に開催予定。

【参考：2020年度開催実績】

日時：2021年3月4日(木曜日)　14時30分から17時30分
配信方法：YouTube（参加無料）
主催：総務省北海道総合通信局
共催：北海道地域情報セキュリティ連絡会
後援：サイバーセキュリティ戦略本部、北海道、北海道警察サイバーセキュリティ対策本部、北海道経済連合会、
国立研究開発法人情報通信研究機構、北海道テレコム懇談会



総務省 サイバーセキュリティ統括官　田原講師

「テレワークにおけるセキュリティ確保に向けた総務省の取組み」の説明模様

立命館大学 情報理工学部セキュリティ・ネットワークコース教授　上原講師

「テレワークによるリスク」の説明模様

2-3. ③-3_啓発、注意喚起資料の作成【北海道警察】

- 北海道警察では、サイバーセキュリティ対策に関する広報啓発資料を作成、各種媒体を通じて効果的な情報発信を継続実施

一般向け
啓発資料

中高生向け啓
発資料

啓発チラシの作成

北海道警察防犯情報発信室（@HP_seian）
https://twitter.com/HP_seian

QRコード
（Twitter）

Twitterを利用した広報

QRコード
（YouTube）

https://www.youtube.com/playlist?list=PLHnOH6YL-Ou02_DRX5APRgEOx4ukBqbpE

YouTube「サイバーセキュリティ講座」

QRコード
（ホームページ）

https://www.police.pref.hokkaido.lg.jp/info/seian/cyber-bouhan-hiroba/main/information.html

道警ホームページ
「サイバーセキュリティひろば」

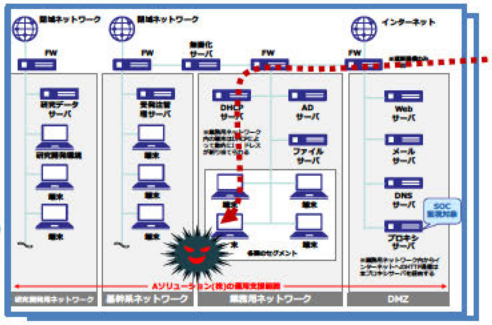
2-4. ④_実践的サイバー防御演習（CYDER）【北海道総合通信局】

CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、国の機関、指定法人、独立行政法人、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習(CYDER)を実施。
- 受講者は、チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験。
- ※2018年度：年間107回･2,666名受講／2019年度：年間105回･3,090名受講／2020年度：年間106回･2,648名受講

演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

機材･データを使用して**本番同様の作業**を実施

インシデント（事案）対処能力の向上

2021年度の全国の実施計画

コース名	演習方法	レベル	受講対象者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	４７都道府県	６５回	7月～翌年２月
B1		中級	システム管理者･運用者（主体的な事案対応 ｾｷｭﾘﾃｨ管理）	地方公共団体	全国１１地域	２１回	9月～翌年２月
B2				地方公共団体以外	東京･大阪･名古屋･福岡	１３回	11月～翌年２月
C		準上級	セキュリティ専門担当者（高度なセキュリティ技術）	全組織共通	東京	2回	翌年1月～2月
オンラインA	オンライン演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	（受講者職場等）	随時	１１月～翌年２月

←**新規開設**

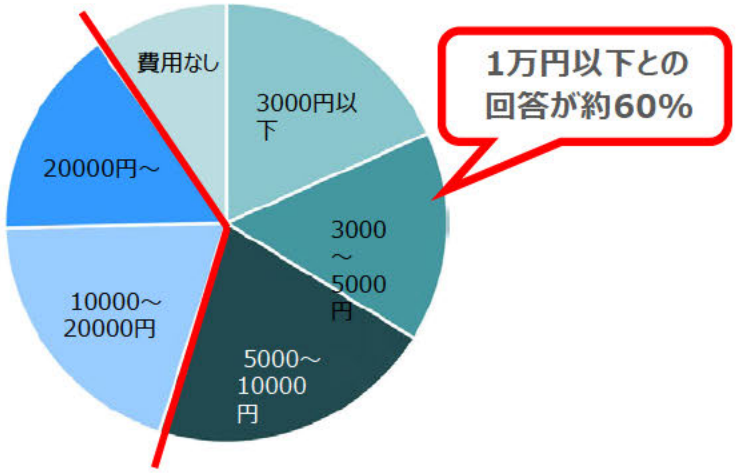
2021年度の北海道内の実施計画

コース名	開催地	実施時期
A	札幌市	１０月１４日
A	釧路市	１１月５日
B１	札幌市	１１月２５日
オンライン A	受講者職場など	１１月～翌年２月

2-5. ⑤_サイバーセキュリティ対策実証モデル構築【北海道経済産業局】

- 北海道経済産業局では、中小企業がかけられる現実的なコストで効果的なセキュリティ対策について実証を行う。
- また、攻撃に関連するシナリオをもとに、自社が狙われた時のインパクトおよびインシデントへの対処についてシミュレーションを行うことで既存の対応体制、連絡調整、復旧手順などにおける課題を洗い出す。
- それら成果についてオンラインセミナーで発表する場を設ける。

＜今後セキュリティ対策にかける月額費用見込み＞



（出典）サイバーセキュリティお助け隊事業 成果報告書
https://www.ipa.go.jp/files/000091309.pdf

1．企業実証モデル

- UTMの導入により、脅威を入口でシャットダウン
- 不正アクセスのログを監視　等

2．シミュレーションの実施

- 実証企業にとって脅威となるサイバー攻撃に関するシナリオを策定。
- シナリオに基づき、社内で以下を検討。

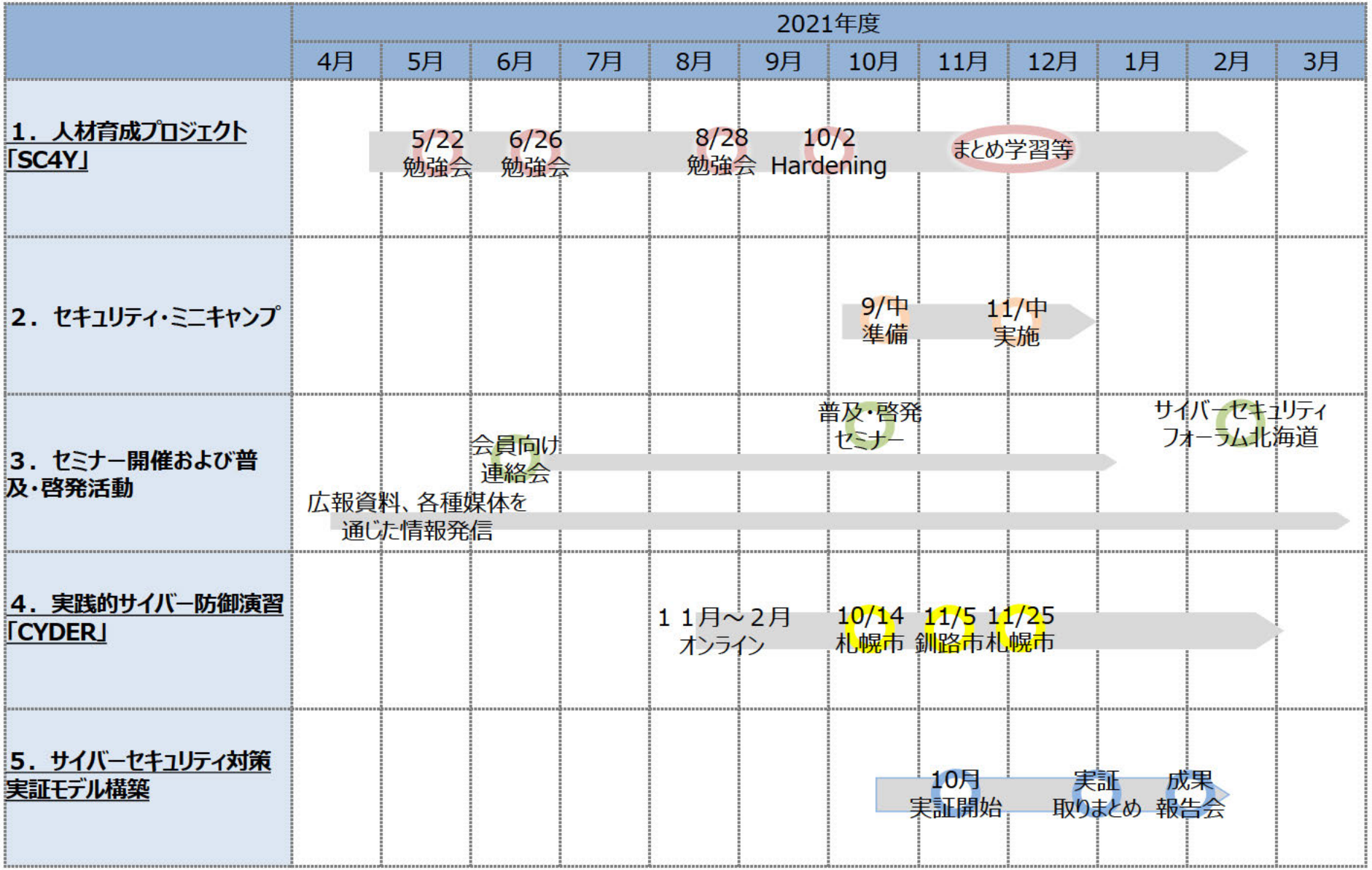
✓ サイバー攻撃による被害を未然に防ぐために必要な事前準備および社内体制
✓ 被害を受けたことも想定し、速やかに復旧を行うための手順

3．実証結果の横展開

- 1．および2．の成果を広く普及させ、実証企業以外におけるサイバーセキュリティ対策構築の参考と資するためにオンラインによる成果発表会を実施する。

2021年度_全体スケジュール（予定）

参考



１．道内におけるサイバーセキュリティの現状とHAISLについて

２．HAISLによる主なサイバーセキュリティの取組

（参考）政府におけるサイバーセキュリティ対策

サイバーセキュリティ戦略（2018戦略　平成30年7月27日閣議決定）

- 我が国のサイバーセキュリティに関する基本的な立場等と諸施策の目標および実施方法を国内外に示すものとして「サイバーセキュリティ基本法」に基づいて策定。

1　策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2　サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3　本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

4　目的達成のための施策

経済社会の活力の向上及び持続的発展

～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 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
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5　推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

【出典】『サイバーセキュリティ戦略』（2018年7月27日サイバーセキュリティ戦略本部）

政府のサイバーセキュリティ推進体制

- サイバーセキュリティ戦略本部の事務局であるNISCを中心に関係機関の一層の能力強化を図るとともに、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担う。

【出典】『サイバーセキュリティ戦略』（2018年7月27日サイバーセキュリティ戦略本部）