資料35－２

令和３年度補正予算及び令和４年度予算案における総務省サイバーセキュリティ関係事項

令和４年１月

サイバーセキュリティタスクフォース事務局

令和3年度補正予算及び令和4年度予算案における総務省サイバーセキュリティ関係事項

事業	令和3年度予算額（円）	令和3年度補正予算額（円）	令和4年度予算（案）額（円）	新規/継続
（1）サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証 大規模化が懸念されるサイバー攻撃に、電気通信事業者が積極的に対処できるようにするため、フロー情報分析によるC&Cサーバ検知技術の実証等を実施。	ー	18.0億	ー	新規
（2）サイバーセキュリティ演習環境の拡充 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に対する実践的な対処能力を持つセキュリティ人材育成のための演習を高度化するため、そのシステムなどの演習環境の拡充を図ることで、高度化されたサイバーセキュリティ演習を安定的に実施可能とし、我が国全体のサイバーセキュリティ対応能力を強化。	ー	11.7億	ー	新規
（3）地域セキュリティコミュニティ強化支援事業 産学官連携による地域に根付いたセキュリティコミュニティ(地域SECUNITY(セキュニティ))を形成し、その取組をセミナー、インシデント演習等を通じて支援。	ー	ー	0.4億	新規
（4）ナショナルサイバートレーニングセンターの強化 NICTに設置した「ナショナルサイバートレーニングセンター」において、巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材等を育成。	12.0億	ー	11.9億	継続
（5）サイバーセキュリティ統合知的・人材育成基盤の構築 サイバーセキュリティ情報の国内での収集・蓄積・分析・提供や、社会全体でのサイバーセキュリティ人材育成のための共通基盤をNICTに構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力を向上。	7.0億	ー	7.0億	継続
（6）IoTの安心・安全かつ適正な利用環境の構築 国内のインターネットに接続されたIoT機器のうちサイバー攻撃に悪用されうる脆弱なIoT機器を調査し、当該機器の利用者に個別に注意喚起を行うプロジェクト「NOTICE」等を実施。	12.8億の内数	ー	11.4億	継続

（１）サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証（18.0億円(R3補正））

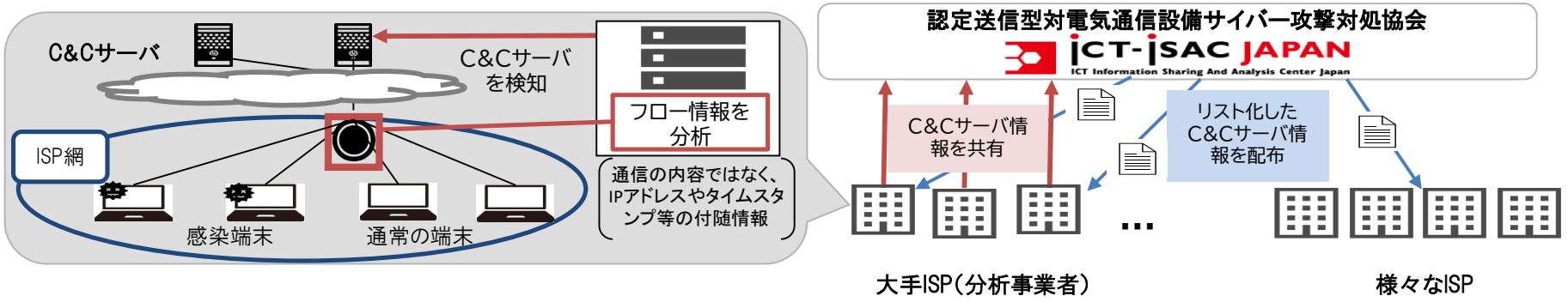
＜資料35-1【１】情報通信ネットワークの安全性・信頼性の確保①＞

サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

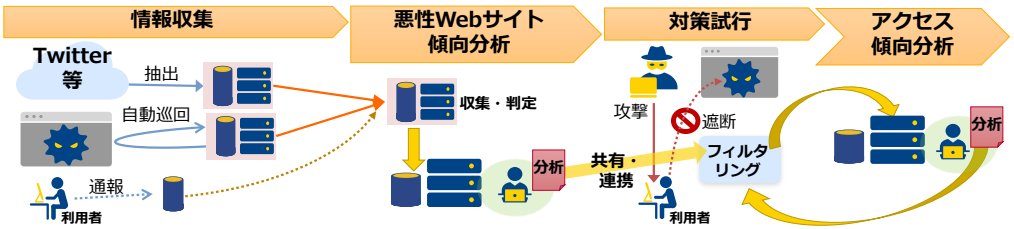
■ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が技術的手法を活用して効率的・積極的に対処できるようにするため、①フロー情報分析によるC&Cサーバ検知技術の実証、②悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ技術の円滑な導入のための実証を実施。

①フロー情報分析によるC&Cサーバ検知技術の実証

※C&C(Command and Control)サーバ：各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

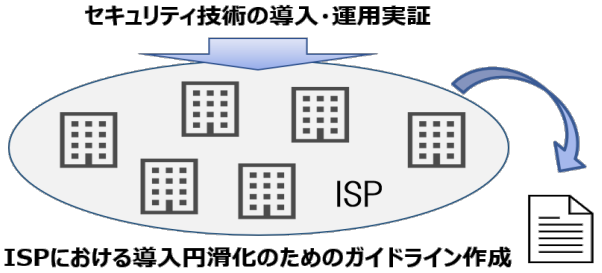


② 悪性Webサイトの検知技術・共有手法の実証



※悪性Webサイト：IDやパスワードなど個人情報の窃取に使用される、正規の金融機関等に偽装したWebサイト（フィッシングサイト） など

③ ネットワークセキュリティ技術の導入実証



※ ネットワークセキュリティ技術：BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC 等

①フロー情報分析によるC&Cサーバ検知技術の実証

■ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が積極的に対処できるようにするため、フロー情報の分析を通じて、サイバー攻撃の指令元であるC&Cサーバを検知する技術の実証を行う。具体的には、電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を実施予定。

（※）フロー情報：通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報

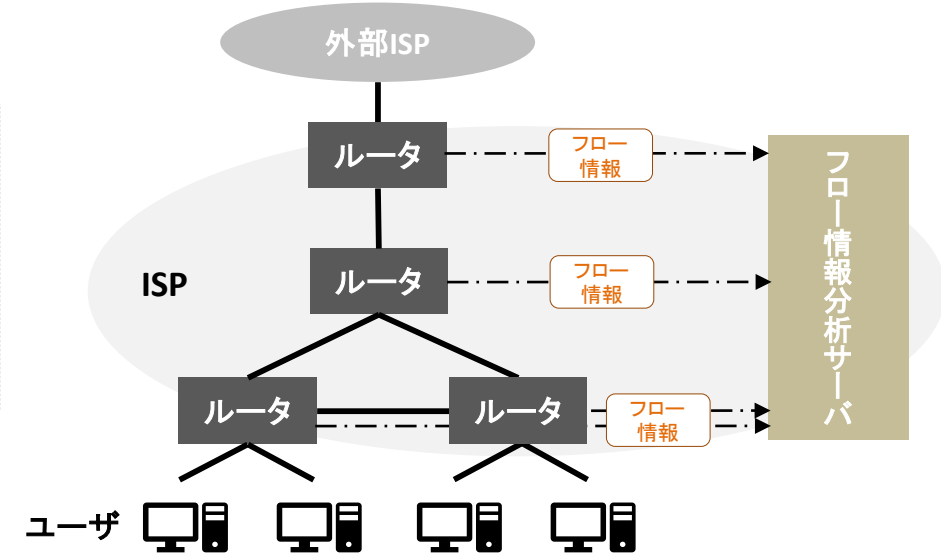
C&Cサーバ：Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータ

■ なお、有識者による研究会において、昨年11月に通信の秘密に係る法的整理を実施。

1）フロー情報の収集・蓄積

- ISPのネットワーク内の各所に設置されているルータから、当該ルータを通過するユーザの通信トラフィックに係るデータの一部（IPアドレス、ポート番号等）を収集・蓄積する。

※大手ISP等においては、通信の傾向を把握し、ネットワークの設計や輻輳対策、DDoS攻撃対策等に活用するべく、平時からフロー情報の収集を行っており、これをC&Cサーバ検知に活用する。



2）フロー情報の分析・C&Cサーバの検知

- 踏み台となる感染端末を用いたサイバー攻撃においては、複数の感染端末が共通の相手方（＝標的、C&Cサーバ等）と通信を行ったり、共通のふるまい（例えば、同種・同サイズのパケットを同時期に大量送信する等）をすることから、フロー情報の中からこうした通信の特徴を抽出し、C&Cサーバの検知を行う。

（参考）「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」第四次とりまとめ（2021年11月24日公表）の概要

（1） 平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知について

→ 正当業務行為として許容される

〈考え方〉

ISPが平時において、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IP アドレス等のフロー情報を収集・蓄積・分析して未知のC&Cサーバを検知することは、必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報をC&Cサーバ検知以外の用途で利用しない場合に限り、正当業務行為として許容される。

（2） フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有について

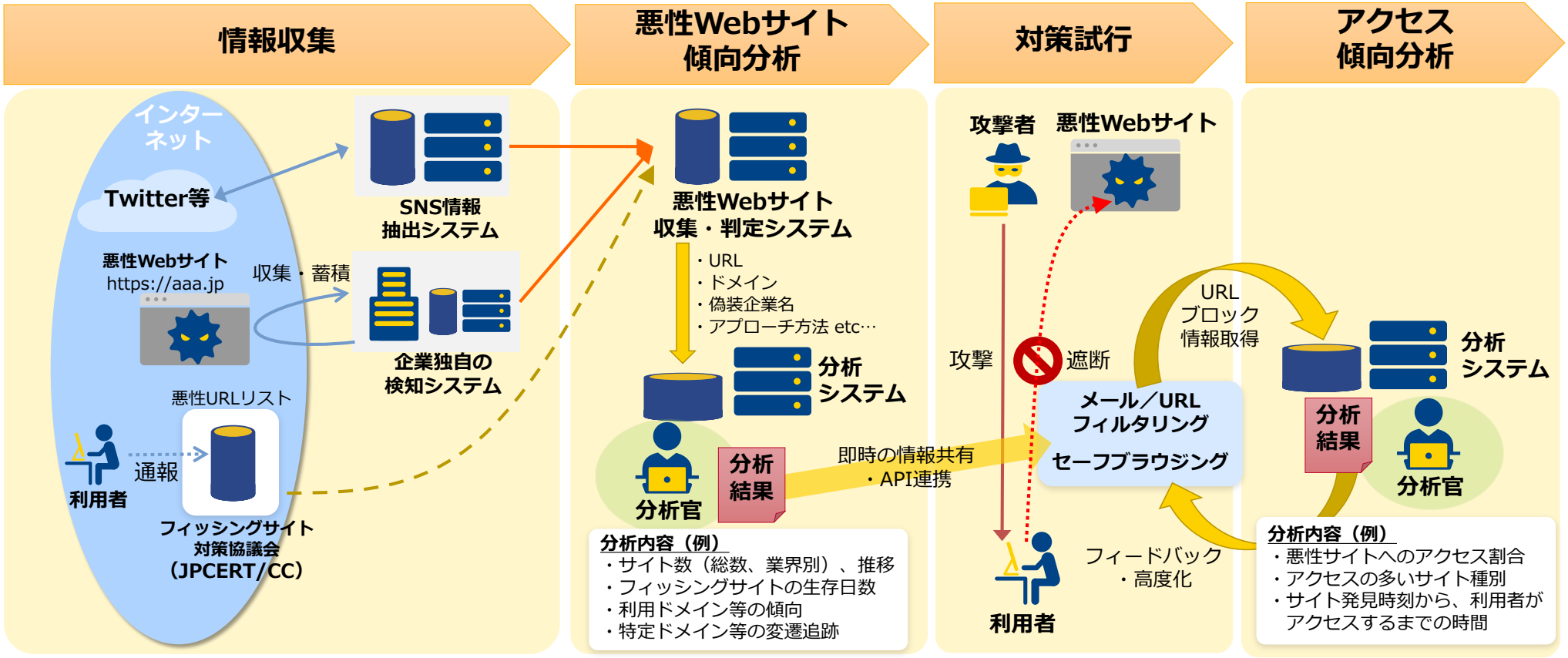
→ 通信の秘密の保護規定に抵触しない

〈考え方〉

一のISPが、（1）の取組により得られたC&Cサーバに関する情報（IPアドレス、ポート番号）を取りまとめてリスト化したものを、サイバーセキュリティ対策を行うために適切な事業者団体等に提供することは、通信の秘密の保護規定に抵触しない。

②悪性Webサイトの検知技術・共有手法の実証

■ SNS等への投稿、企業独自の悪性Webサイト検知システム、また利用者による通報等をもとに、自動巡回による機械的処理を活用して悪性Webサイト情報の収集・分析を行い、利用者の被害実態把握および課題について整理し、悪性Webサイトを検知する手法の有効性実証、検知結果を活用し継続的な対策を講じるための必要事項を整理する実証事業を行う。



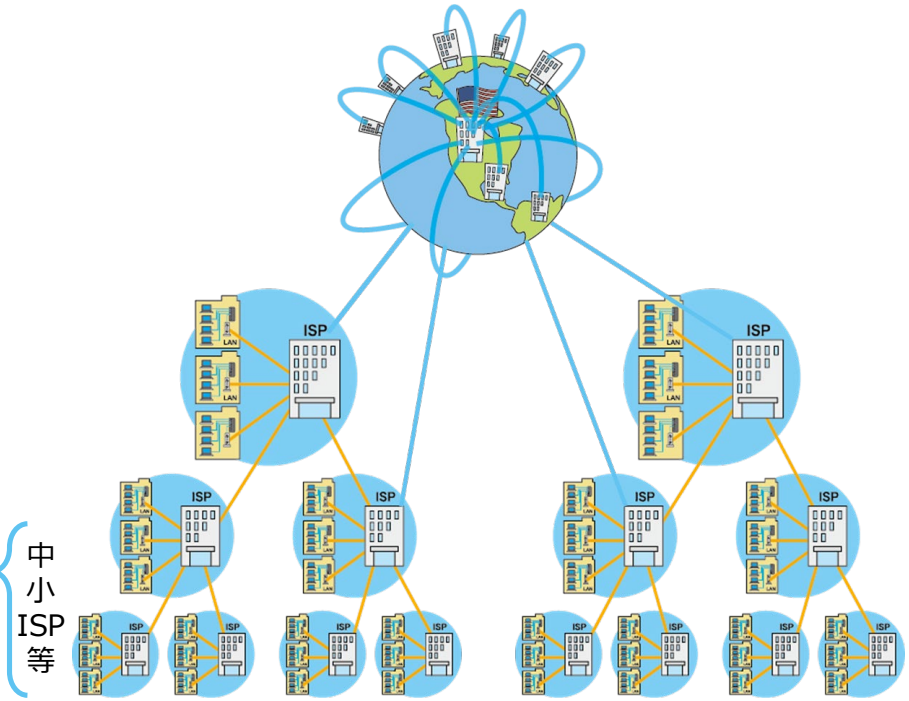
自社偽装サイト検知の仕組みの各種企業への提供、URLフィルタリング・迷惑メール対策・セーフブラウジングの高度化およびJPCERTと連携し悪性Webサイトのテイクダウンに貢献

③ISPにおけるネットワークセキュリティ技術の導入実証等

- インターネットの一部の脆弱な仕様を悪用するサイバー攻撃に対しては、電子認証技術を活用したネットワークセキュリティ技術が国際標準化*されており、それらを実装することで通信ネットワーク側で抑え込むことが可能。
  *例: BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC等がIETFでRFC化されている。
- これらの実装には、各ISP等が管理する通信ネットワークに、対応ソフトウェア・ハードウェアを組み込み、継続運用していく必要があるところ、国内においては以下のような事情もあり、いまだ普及率が上がらないのが実情。
  - ✓ 通信ネットワークの再構築を要するとともに、導入後は電子認証技術の運用に関する知見や能力が求められる。
  - ✓ ユーザが、各ISPを選定する際、対策状況が分からない・判断が難しいなど、ISPが苦労して導入・運用しても競争優位に繋がるか不透明。
  - ✓ ネットワークセキュリティ技術の実装に関する特段の規制も存在しない。
- 本事業では、中小ISP等の通信ネットワークを実証環境とし、ネットワークセキュリティ技術の導入実証を実施。得られた知見等に基づき、ISPにおける導入円滑化のためのガイドラインを作成するとともに、対策を実装したセキュアな通信ネットワークがユーザから評価される仕組みの在り方検討等を進める。

- ネットワークセキュリティ技術の導入実証（想定される対象技術: RPKI, DNSSEC, DMARC等）
- 実証結果に基づき:
  - ISPにおける導入円滑化のためのガイドラインを作成
  - セキュアな通信ネットワーク・ISPがユーザから評価される仕組みの在り方検討 等

- インターネットの一部の脆弱な仕様を悪用するサイバー攻撃に対する、通信ネットワーク側での積極的対処を推進
- 自律・分散・協調のもと、我が国サイバー空間の安全性と信頼性の強化とユーザの保護を実現



Resource Public-Key Infrastructure

– IPアドレスやAS番号といった番号資源（Number Resource）の割り振り／割り当てをリソース証明書で証明する。

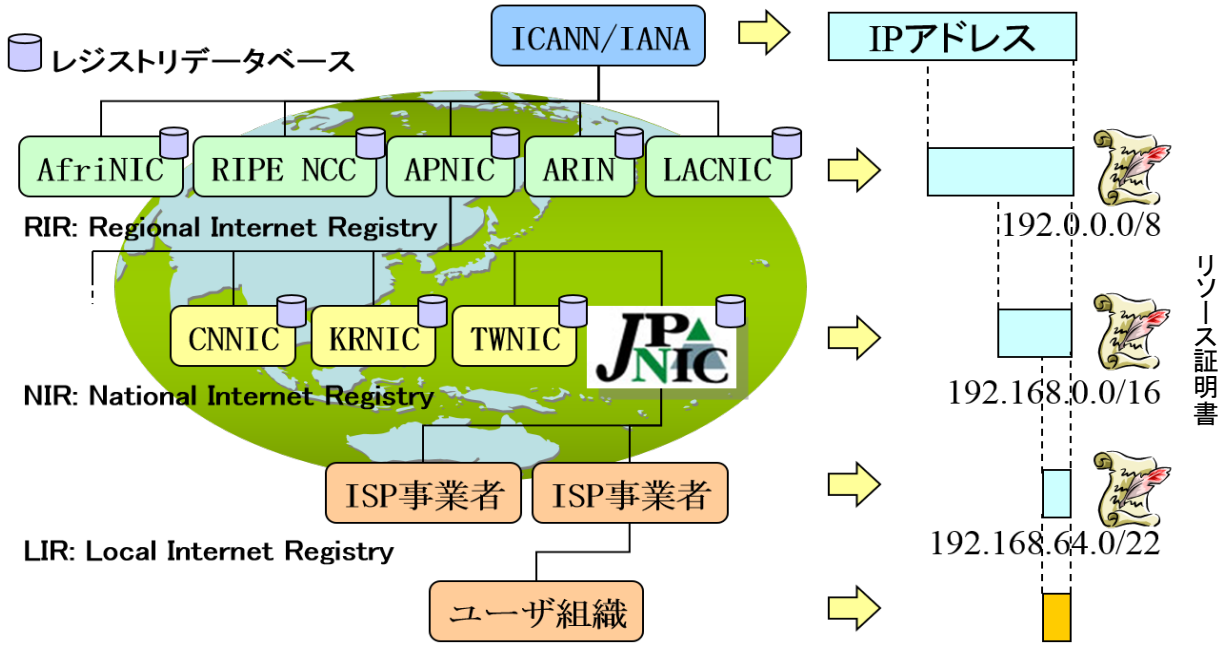
IPアドレスが正しいものかを確認できる

↓

BGPの経路情報が正しいかどうかを確認できる

↓

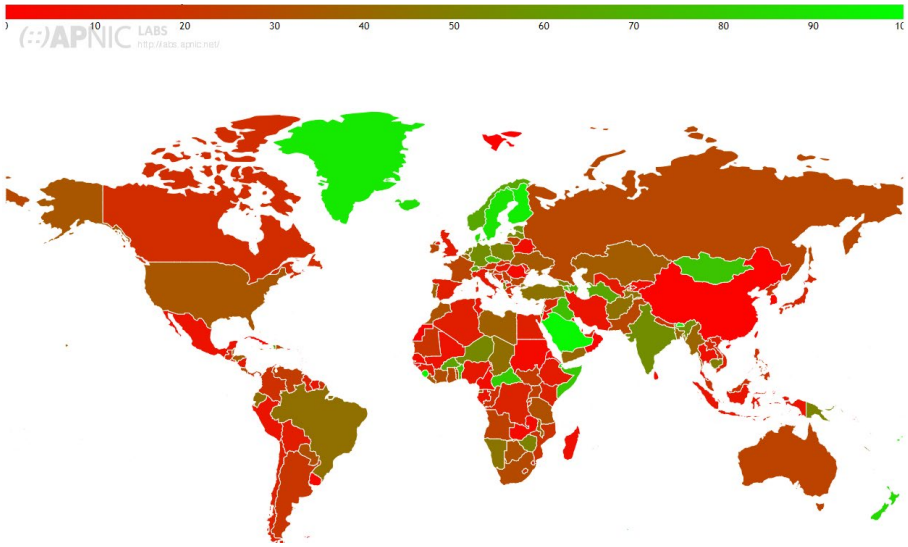
IPアドレスの不適切な利用を検知するために利用できる



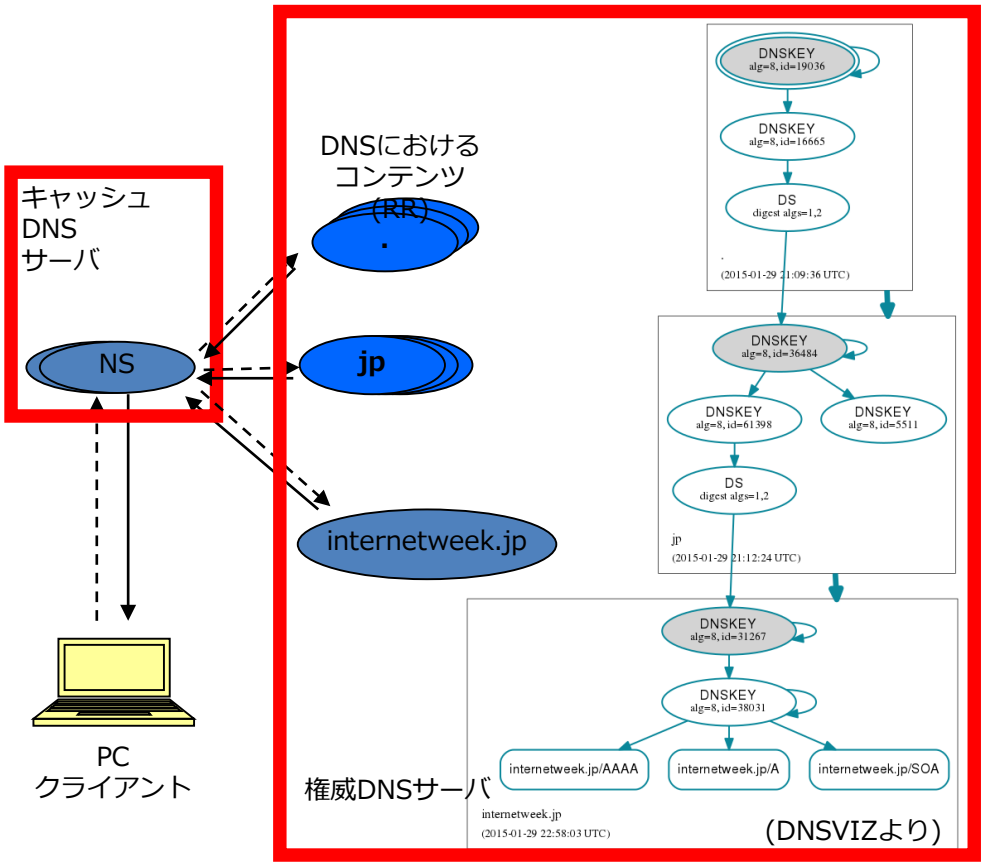
出所: 総務省 サイバーセキュリティタスクフォース（第30回）JPNIC説明資料「情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向について」
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html

（参考） DNSSECの概要

- 権威DNSサーバのコンテンツ（内容）を署名鍵（秘密鍵）で署名することによりDNSキャッシュサーバ側でそのコンテンツが正当であるかの判定ができる。
- DNSのツリー構造の中に署名鍵情報（公開鍵）を登録することによりDNSの中に閉じて解決が可能。
- 但しルートの署名鍵情報についてだけは別途正当性の確認が必要。



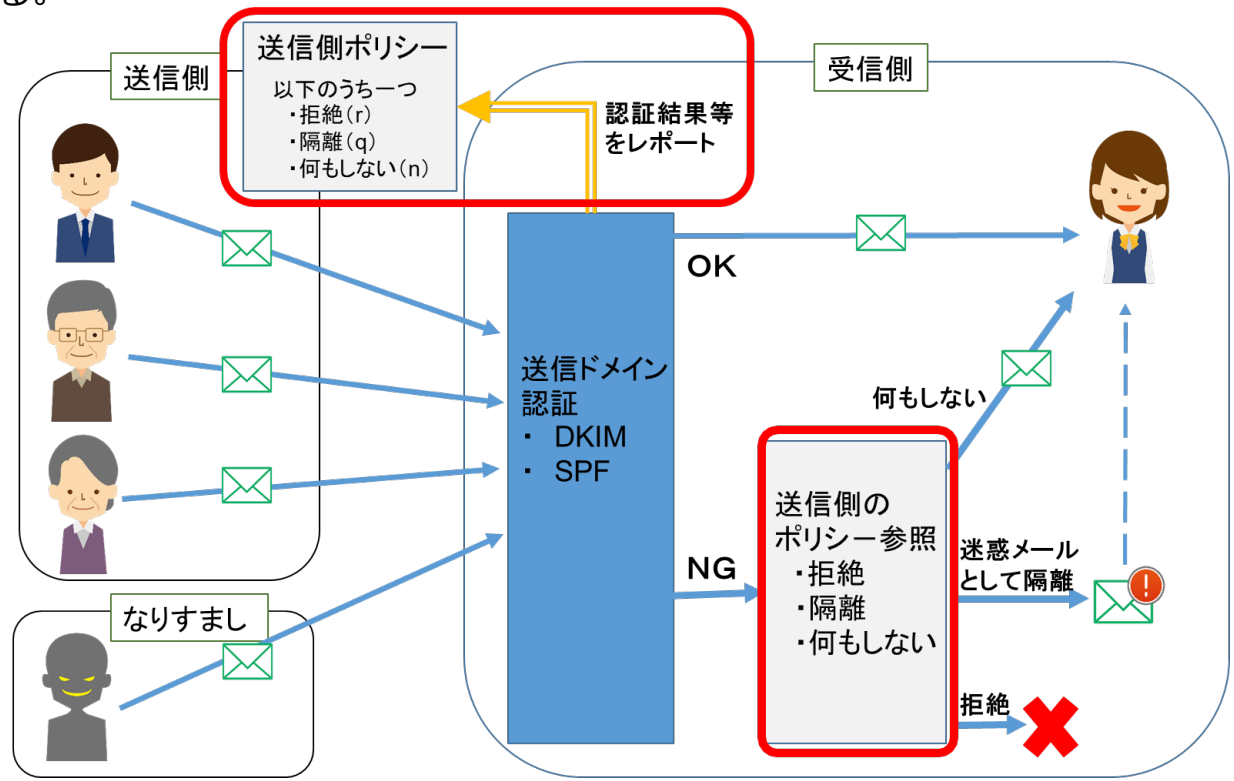
世界のValidation状況 (APNIC Labsによる計測結果より)



出所: 総務省 サイバーセキュリティタスクフォース（第30回）JPNIC説明資料「情報通信ネットワークの将来像とセキュリティ技術に関する標準化を巡る議論の動向について」
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html

（参考）DMARCの概要

1. ドメイン管理者において、当該ドメイン名義で送信される電子メールに関して、受信時のドメイン認証が失敗した場合の取り扱い方針を宣言するとともに、後記3.記載のレポートの送付先メールアドレスを公開する。
2. 電子メールの受信サーバ側で、ドメイン認証（DKIM、SPF）を行った上、認証に失敗した電子メールにつき、1.の取り扱い方針も踏まえ、以下のいずれかの処理をする。
   - ○ 何もしない :そのまま受信者に届ける
   - ○ 隔離　　:認証に失敗した旨を付して隔離する（迷惑メールとして扱う）
   - ○ 拒絶　　:受信サーバから削除する（受信者は存在を認識しない）
3. 受信サーバ側は、送信ドメイン管理者の指定した送付先メールアドレスに対し、2.の認証結果に関するレポートを送付する。



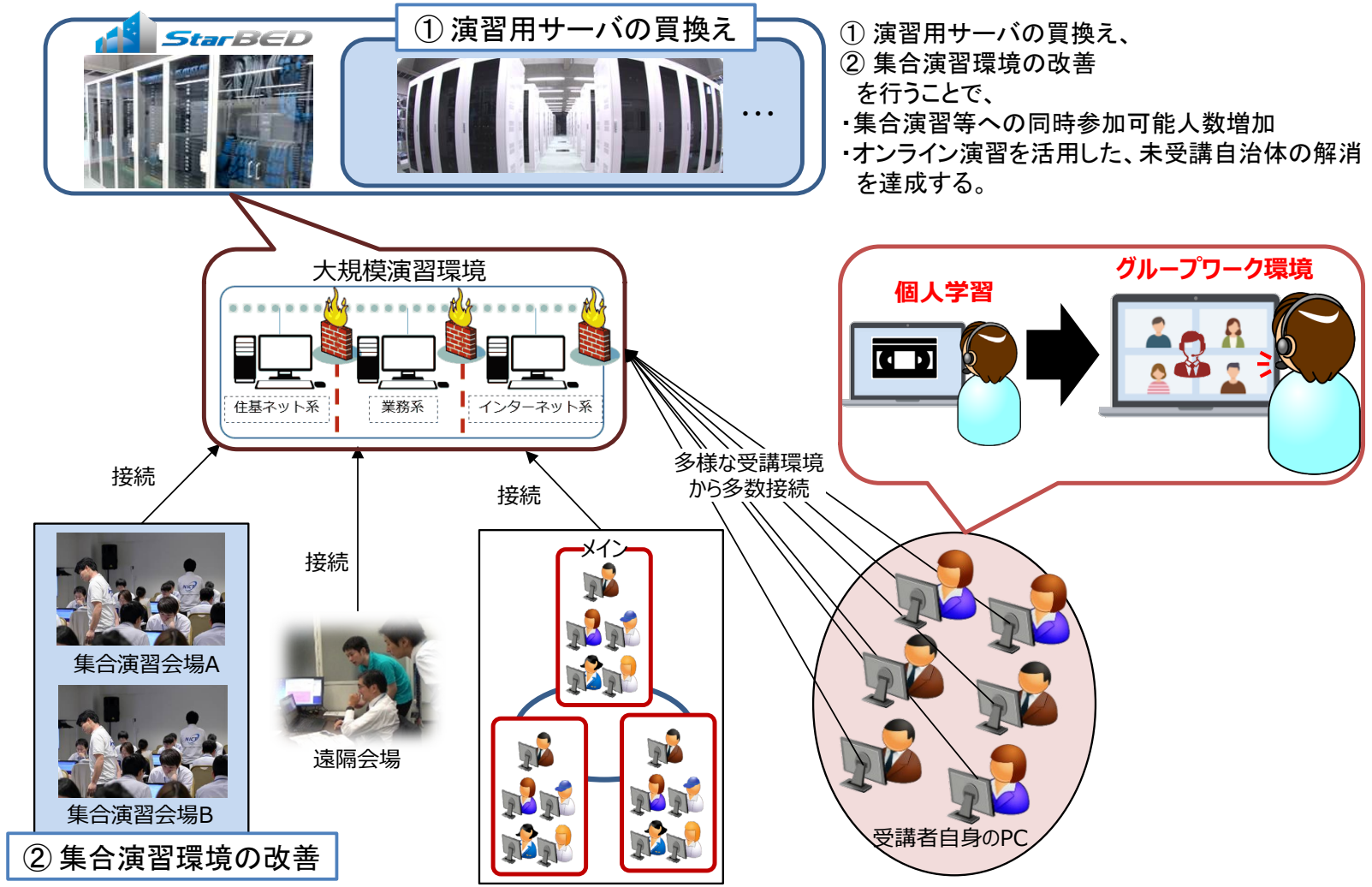
出所: 総務省「送信ドメイン認証技術等の導入に関する法的解釈について」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html

（２）サイバーセキュリティ演習環境の拡充
（11.7億円(R3補正)）

＜資料35-1【３】人材育成＞

サイバーセキュリティ演習環境の拡充

■ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に対する実践的な対処能力を持つセキュリティ人材育成のための演習を高度化するため、そのシステムなどの演習環境の拡充を図ることで、高度化されたサイバーセキュリティ演習を安定的に実施可能とし、我が国全体のサイバーセキュリティ対応能力を強化。

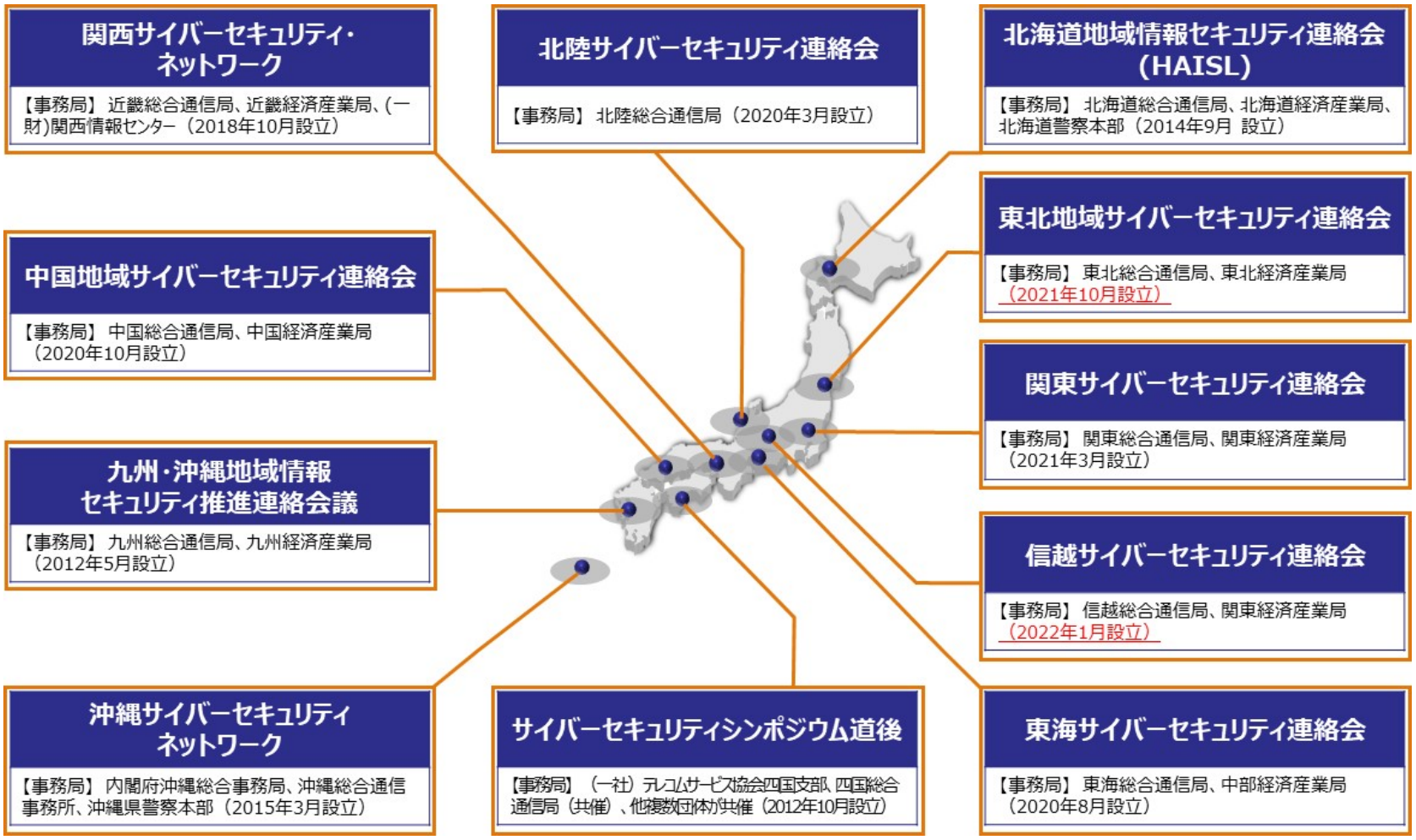


（３）地域セキュリティコミュニティ強化支援事業
（0.4億円（R4））

＜資料35-1【５】普及啓発＞

地域セキュリティコミュニティ強化支援事業

■ 大都市圏を除く各地域ではセキュリティに関する人材育成、普及啓発等の機会が十分でないことから、産学官連携による地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））を形成し、その取組をセミナー、インシデント演習等を通じて支援する。



（４）ナショナルサイバートレーニングセンターの強化
（11.9億円(R4)）

＜資料35-1【３】人材育成＞

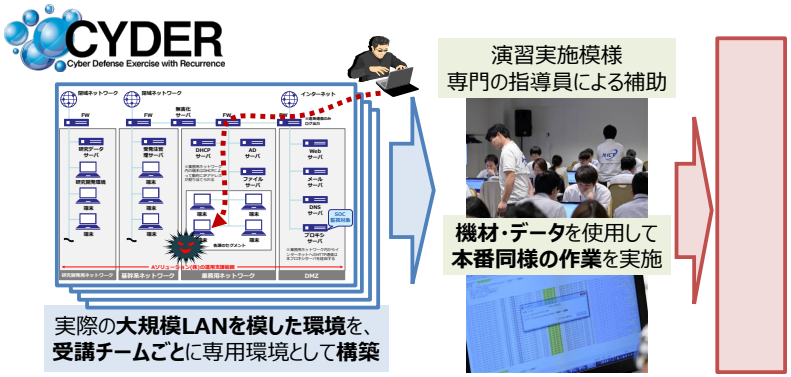
ナショナルサイバートレーニングセンターの強化

■ 巧妙化・複雑化するサイバー攻撃に対し、国立研究開発法人情報通信研究機構（NICT）に設置した「ナショナルサイバートレーニングセンター」において、実践的な対処能力を持つセキュリティ人材等を育成し、我が国のサイバーセキュリティを強化する。

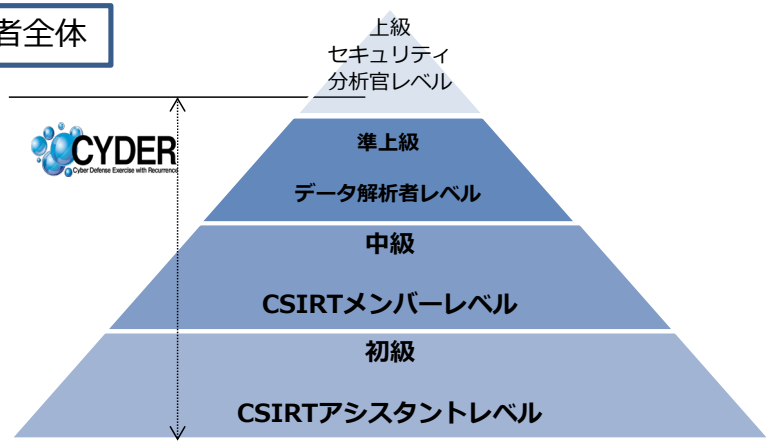
①CYDER（実践的サイバー防御演習）

国の行政機関、地方公共団体、独立行政法人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実践的サイバー防御演習（CYDER）を実施。

※オンライン受講環境を令和３年度より本格稼働。



運用者全体

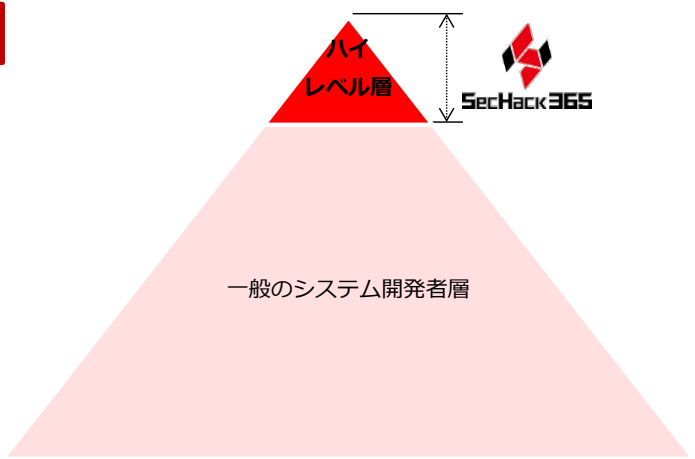


※CSIRT：Computer Security Incident Response Team

②SecHack365（若手セキュリティイノベータの育成）

25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材を育成。

開発者全体

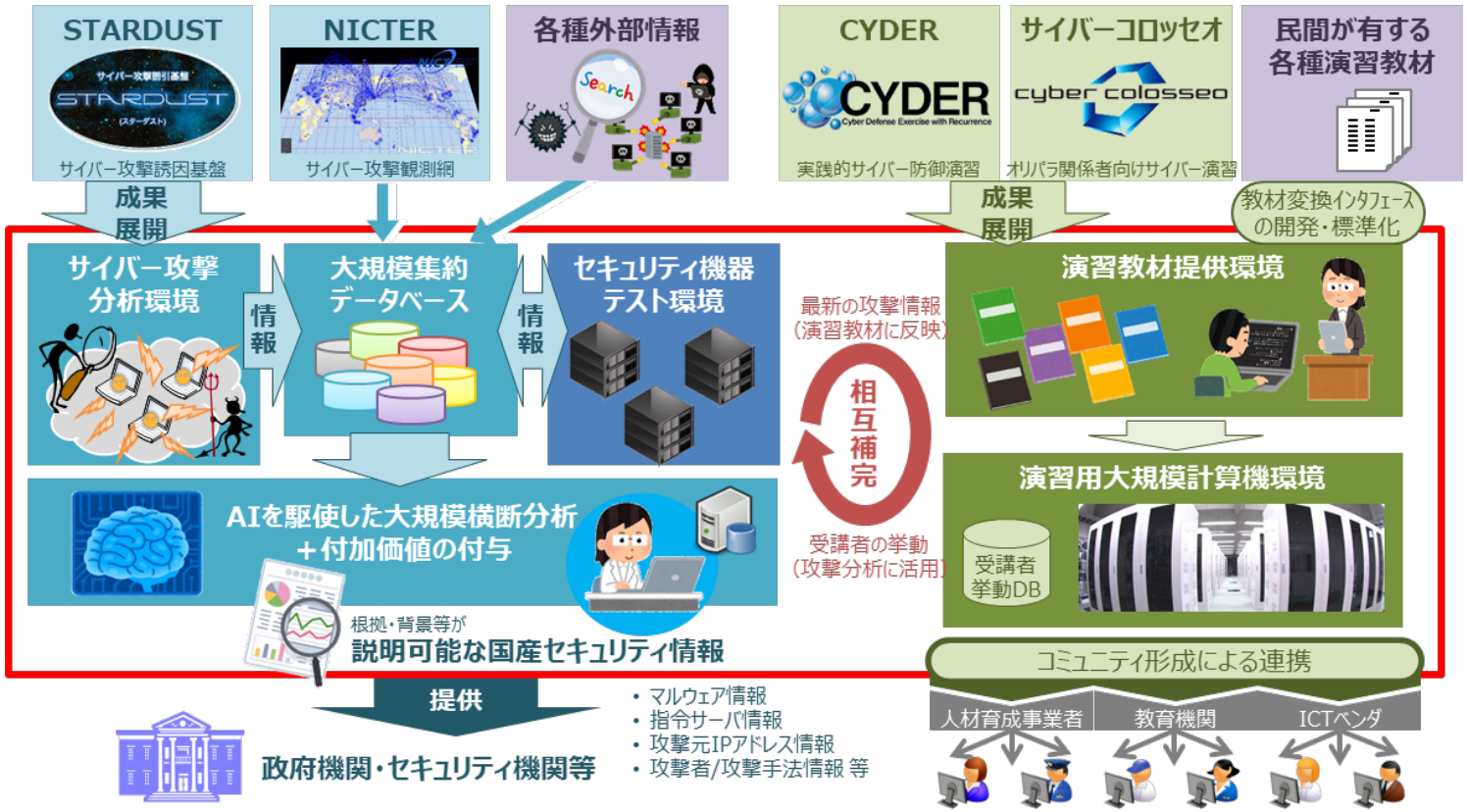


（５）サイバーセキュリティ統合知的・人材育成基盤の構築（7.0億円（R4））

＜資料35-1【４】「統合知的・人材育成基盤（CYNEX）」の構築＞

サイバーセキュリティ統合知的・人材育成基盤の構築

■ サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤をNICTに構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力の向上を図る。



次のとおり活用可能な基盤をNICTに構築。

- **国産セキュリティ情報の収集・蓄積・分析・提供**
  幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。
- **セキュリティ機器テスト環境**
  国産のセキュリティ機器・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。
- **高度解析人材の育成**
  収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。
- **人材育成のための基盤提供**
  NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自立的な人材育成を推進。

（６）IoTの安心・安全かつ適正な利用環境の構築
（11.4億円(R4)）

＜資料35-1【１】情報通信ネットワークの安全性・信頼性の確保①②、
【３】人材育成、【５】普及啓発＞

IoTの安心・安全かつ適正な利用環境の構築

■ 電波を使用するＩｏＴ機器が急増し多様化するとともに、それらに対するサイバー攻撃の脅威が増大していることから、ＩｏＴに係る様々なセキュリティ対策の強化やＩｏＴの適正な利用環境の構築に向けたリテラシーの向上を図ることで、国民生活や社会経済活動の安心・安全の確保等を実現する。

① IoTセキュリティ対策の推進

国立研究開発法人情報通信研究機構法に基づき国内のインターネットに接続されたIoT機器のうちサイバー攻撃に悪用されうる脆弱なIoT機器を調査し、当該機器の利用者に個別に注意喚起を行うプロジェクト「NOTICE」を実施する。

② 5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

5Gネットワークやその構成要素及びサービスについて、ソフトウェア及びハードウェア両面の技術的検証を通じ、各構成要素におけるサプライチェーンリスク対策を含むセキュリティを総合的かつ継続的に担保する仕組みを整備する。

※ ソフトウェアに関する技術的検証については、令和３年度で終了。

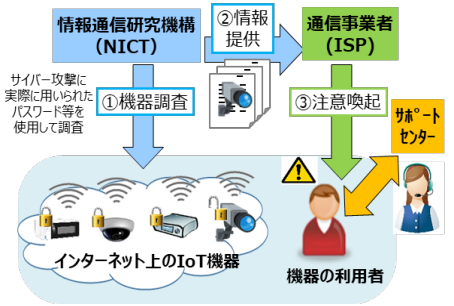
③ 地域におけるIoTセキュリティ対策の強化

地域のコミュニティや企業、教育機関等と連携して、IoTセキュリティに関して活躍可能な人材を自立的に育成していくためのエコシステムの確立に向けた実証を行う。

④ 無線LANのセキュリティ対策の強化

無線LANを安心・安全に利用するため、利用者・提供者双方におけるセキュリティ対策状況調査やガイドライン策定を行うとともに、周知・啓発活動を推進する。

①IoTセキュリティ対策の推進



②5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発