# 2018 年度 中南米 CSIRT 動向調査

一般社団法人 JPCERT コーディネーションセンター

2019 年 3 月 7 日

[ 目次 ]

[ 図表目次 ]

[ 略語表 ]

| 略語 | 名称 | 日本語訳/説明 |
|---|---|---|
| APWG | Anti-Phishing Working Group | フィッシング詐欺によるサイバー犯罪を撲滅するための非営利団体 |
| ATM | Automated/Automatic Teller Machine | 現金自動預け払い機 |
| BGP | Border Gateway Protocol | 通信経路制御プロトコル |
| C&C サーバ | Command and Control Server | コマンド&コントロール サーバ（遠隔からウイルス感染コンピュータに指示を送るサーバ） |
| CDCiber | Centro de Defesa Cibernetico | ブラジル防衛省の下部組織 |
| CDN | Content Delivery Network | コンテンツデリバリネットワーク |
| CERT.br | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil | ブラジルにおけるサイバーセキュリティ分野を管轄する組織 |
| CERT-MX | Centro Especializado en Respuesta Tecnologica de Mexico | メキシコのコンピュータインシデント緊急対応チーム |
| CGI.br | Comitê Gestor da Internet no Brasil | ブラジルにおけるプロジェクト決定事項を実施するための非営利組織 |
| CICTE | Inter-American Committee against Terrorism | 米州テロ対策委員会 |
| CIRT | Computer Incident Response Team | コンピュータインシデント対応チーム（CSIRT と同義） |
| CMM | Cybersecurity Capability Maturity | サイバーセキュリティ対策の成熟度 |
| CMU | Carnegie Mellon University | カーネギーメロン大学 |
| CPE | Customer Premises Equipment | 顧客構内設備（通信事業者との責任分界点） |
| CSIRT | Computer Security Incident Response Team | コンピュータセキュリティインシデント対応チーム（CIRT と同義） |
| CTIR.gov | Centro de Tratamento de Incidentes de Redes do Governo | DSIC の下部組織 |
| CT-Spam | Task Force on Spam | Spam メール対策タスクフォース |
| DDoS | Distributed Denial of Service | 分散型のサービス運用妨害 |
| DNS | Domain Name System | ドメイン名と IP アドレスの対応付けを行う仕組み |
| DoS | Denial of Service | サービス運用妨害 |
| DSIC | The Departamento de Segurança de Informações e Comunicações | ブラジル国家安全局の下部組織 |
| EB | Exabyte | エクサバイト（1,000 ペタバイト） |

| 略語 | 名称 | 日本語訳/説明 |
|---|---|---|
| FBI | Federal Bureau of Investigation | アメリカの連邦捜査局 |
| FIRST | Forum of Incident Response and Security Teams | 世界中の CSIRT の協力強化、情報共有を目的としたフォーラム |
| GCI | Global cybersecurity Index | ITU による調査レポート |
| GDP | Gross Domestic Product | 国内総生産 |
| GSI | The Gabinete de Segurança Institucional | ブラジルの国家安全局 |
| ICANN | Internet Corporation for Assigned Names and Numbers | インターネット資源をグローバルに調整する非営利組織 |
| IDRC | International Development Research Center | 国際開発研究センター |
| IoT | Internet of Things | モノのインターネット |
| IPA | Information-technology Promotion Agency | 独立行政法人情報処理推進機構 |
| ISO | International Organization for Standardization | 国際標準化機構 |
| ISP | Internet Service Provider | インターネットサービス事業者 |
| ITU | International Telecommunication Union | 国際電気通信連合 |
| IX | Internet Exchange Point | ISP やデータセンタ事業者などの相互接続点 |
| LACNIC | The Latin American and Caribbean IP address Regional Registry | ラテンアメリカとカリブ海地域のネットワーク資源管理を行う組織 |
| LRITF | Ley para Regular las Instituciones de Tecnología Financiera | 金融テクノロジー機関規制法 |
| NBSO | NIC BR Security Office | CERT.br の前身 |
| NGO | Non-Governmental Organizations | 非政府組織 |
| NIC.br | Núcleo de Informação e Coordenação do Ponto BR | CGI.br が所掌する事項の実施機関 |
| NTP | Network Time Protocol | 時刻同期プロトコル |
| OAS | Organization of American States | 米州機構 |
| RAT | Remote Administration Tool | リモートアクセスツール |
| RDP | Remote Desktop Protocol | リモートデスクトッププロトコル |
| RNP | Brazilian Research Network | ブラジル国立教育研究ネットワーク |

| 略語 | 名称 | 日本語訳/説明 |
|---|---|---|
| SEI | Software Engineering Institute | カーネギーメロン大学ソフトウエア工学研究所 |
| SIDA | Swedish International Development Cooperation Agency | スウェーデン国際開発協力庁 |
| SIP | Session Initiation Protocol | 音声や映像、テキストメッセージの交換を行うプロトコル |
| SNMP | Simple Network Management Protocol | ネットワーク管理プロトコル |
| SNS | Social Networking Service | ソーシャルネットワーキングサービス |
| SOC | Security Operations Center | セキュリティ監視センター |
| SSH | Secure Shell | 暗号化通信プロトコル |
| USB | Universal Serial Bus | コンピュータ等の情報機器に周辺機器を接続するための規格 |
| US-CERT | United States Computer Emergency Readiness Team | アメリカ国土安全保障省の国家サイバーセキュリティ実働部隊 |
| WARP | Warning, Advice and Reporting Point | LACNIC においてサイバーセキュリティを担当する組織 |

メキシコおよびブラジルの組織・法律の名称についてはそれぞれスペイン語、ポルトガル語を用いた正式な表記に従って記載している。

# 第1章　本調査の目的・背景

## 1－1　目的・背景

本調査の目的は中南米地域およびカリブ海諸国（以下、中南米）における CSIRT の活動およびサイバーセキュリティ戦略や関連法整備の状況等について、公開文書調査およびインタビューによる調査事業（以下、本調査）を実施し、当該地域におけるサイバーセキュリティ体制への理解を深めるとともに、今後のインシデント対応業務における参考となる知見を集めることである。

本調査の背景として、JPCERT/CC は世界中の CSIRT とのネットワークを有し連携を行っている。しかしながら中南米の CSIRT やサイバーセキュリティ専門家とは、インシデント対応における連携実績はあるもの、現状では他地域に比べて関係性が薄い。

今後のより密な関係構築および連携強化を図るために、各国の CSIRT 体制、活動内容やインシデント対応に係る国内外の連携はどの様なものがあるのかを把握することに重点を置き調査を進めた。

## 1－2　調査方法

まず先行調査として中南米全体におけるサイバーセキュリティ動向を調査し、各国を比較するうえでの分析視点の優先度付けと調査対象国の選定を行った。その後、次の 2 フェーズに分けて調査を進めた。

### 1－2－1　フェーズ 1　事前調査

インターネット等で入手した参考文献から次の各項目について情報を収集した。

① 当該国における National CSIRT の組織概要、活動状況および重大なセキュリティインシデント事例等
② 当該国政府が発行するサイバーセキュリティ戦略および関連法整備の状況
③ 中南米での CSIRT 間連携の活動の詳細

### 1－2－2　フェーズ 2　現地インタビュー

事前調査により定めた対象国、対象機関に対し、CSIRT の活動状況（組織、概要、サービス、規模）についてインタビューを実施し、事前調査結果と比較した。

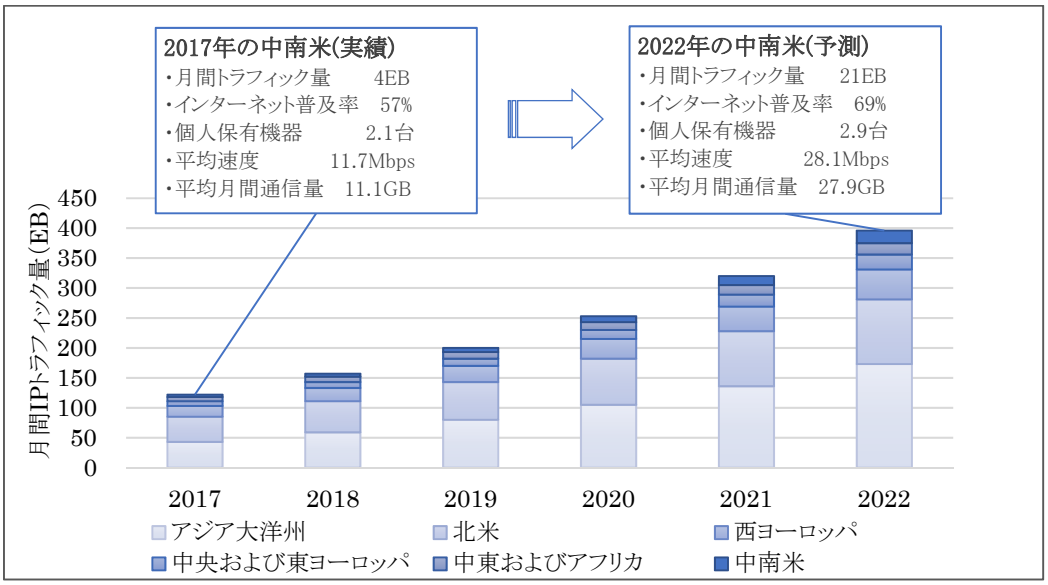
# 第2章　中南米地域のサイバーセキュリティに係る概要

## 2－1　現況概観

### 2－1－1　ユーザ数の増加と中南米地域のサイバーセキュリティ

世界のトラフィック量は IoT 関連を含むネットワーク機器の増加により、ますます増大することが予測されている。Cisco によると 2022 年には月間 IP トラフィック量が 396EB（エクサバイト）に達する見込みである。

中南米においては 2017 年には 57%であった居住者のインターネット利用率が 2022 年には 69%に増加し、一人当たりの保有デバイス数は、2.1 台（2017 年）から 2.9 台（2022 年）となる。2022 年のインターネット平均利用速度およびデータ通信量は、ともに 2017 年の約 2.5 倍に拡大する見込みである。（図 1）

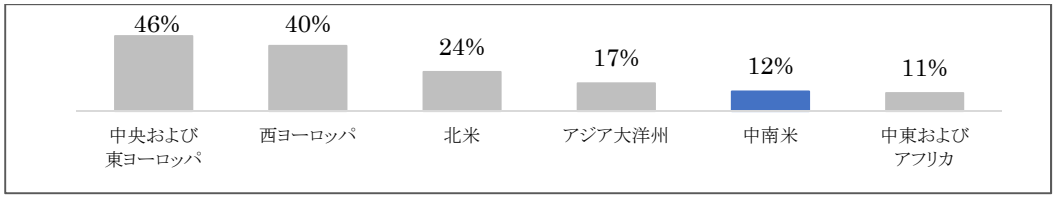



[図 1　全世界の IP トラフィックの成長と中南米におけるインターネット利用状況の予測]
出典：Cisco VNI Forecast and Trends, 2017-2022[1], VNI Forecast Highlights Tool[2]より作成

ユーザ層の拡大にともない、セキュリティや認証の安全性を高めたシステムの導入が進められているが、インターネットに接続された Web サーバ数に対する安全な Web サーバ数の割合を調べたデータを見ると、図 2 が示すように安全性が比較的高い中央および東ヨーロッパが 46%、西ヨーロッパが 40%であるのに対し、中南米においては 12%と他地域に比べてサイバーセキュリティ対策が遅れているのがわかる。

[1] Cisco: VNI Forecast and Trends, 2017-2022
(https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html)

[2] Cisco: VNI Forecast Highlights Tool
(https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html)

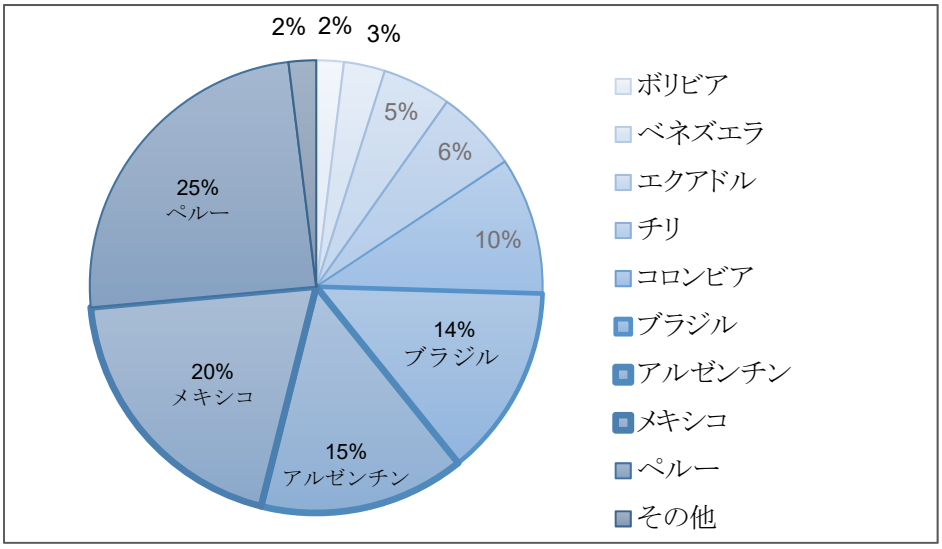



[図 2　地域ごとの Web サーバにおける安全な Web サーバの割合]
出典：Cisco ゼタバイト時代：トレンドと分析（2017 年 6 月）[3]より作成

## 2－1－2　中南米地域における顕著なセキュリティ脅威

サイバーセキュリティ対策が立ち遅れた地域においては、マルウエアの拡散、情報漏洩の発生や金銭的被害が多発するなどの影響が考えられる。ESET（サイバーセキュリティ企業）の調査では、中南米において、2016 年以前は企業を脅かす主要因がマルウエアであった。同社が、2017 年に中南米 15 カ国、2,500 以上の企業を対象に実施した調査では、ランサムウエアの被害が 2016 年に比べて 60%増加して、マルウエア被害の中でも突出し、ランサムウエアだけでも被害要因の最上位となった。

中南米において 2017 年に発生したランサムウエア被害の国別内訳では、ペルーが最上位であった。ペルーの人口はメキシコの約 4 分の 1 であるため、ペルーにおけるランサムウエアの被害件数が際立って多く、中南米地域内においても国ごとに被害状況に大きな差があることがわかる。（図 3）




[図 3　中南米におけるランサムウエア被害の国別内訳]
出典：ESET SECURITY REPORT Latinoamérica 2018[4]を翻訳

IoT などの技術革新により、これまで以上に数多くの機器が国境を越えて相互接続される現代においては、地理的に離れた場所から攻撃が行われることも多い。国際化するサイバー犯罪やサイバー攻撃に対抗するため、国際連携の必要性がこれまで以上に高まっている。

このような背景から、中南米を含む米州地域においてのサイバーセキュリティに関する国の枠を超えた組織的連携を強化する目的で OAS（後述）と LACNIC（後述）は 2013 年 5 月に Cyber Security Agreement

[3] Cisco: ゼタバイト時代：トレンドと分析（2017 年 6 月）
(https://www.cisco.com/c/ja_jp/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf)

[4] ESET: ESET SECURITY REPORT Latinoamérica 2018
(https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf)

を締結して、政府、民間部門、市民社会における連携を強化することで合意し、サイバーセキュリティ関連の様々な取組みを推進している。

## 2－2　OAS の概要

Organization of American States（米州機構、以下、OAS）は「1948 年に発足した米州における唯一の汎米国際機関で，同地域の諸問題の解決にあたる重要な国際機関」である[5]。近年では、米州各国での選挙監視活動等に重要な役割を果たしており、特に域内の民主化の確立、維持に取り組んでいる[6,7]。

### 2－2－1　設立目的

OAS の設立目的は次のとおりである。（外務省 Web サイト[7]より引用）

① 米州地域の平和と安全の強化
② 代表制民主主義の強化
③ 加盟国間の紛争の防止および平和的解決の確保
④ 侵略に対する共同行動
⑤ 加盟国間の政治的、法律的、経済的諸問題の解決
⑥ 共同的行動による加盟国間の経済的、社会的、文化的発展の促進
⑦ 極度の貧困の撲滅
⑧ 経済社会開発への資源分配を可能にするための通常兵器の制限の達成

### 2－2－2　加盟国

2019 年 2 月現在、35 カ国（アメリカ、カナダ、および全中南米 33 カ国）が正式加盟国とされている[8]。

69 カ国および EU が常任オブザーバー国とされており、日本は 1973 年 12 月に常任オブザーバー国となっている[9]。

### 2－2－3　活動概要

米州の平和と安全の維持、民主主義の擁護・促進、経済社会開発が主な活動目的であるが、1994 年 12 月に開催された米州サミットにおいて、OAS の活動の拡大・強化が合意され、上記各種活動を充実するほか、貿易の自由化、文化交流、汚職問題、テロ防止、通信・情報インフラの開発等、広範な分野での活動が期待されている[6]。

---

[5] OAS の設立は米州機構憲章に基づいているが、これが調印されたのが 1948 年、発効したのが 1951 年である。外務省の Web サイトではこの発効年を組織の設立年と捉えているが、OAS の Web サイトでは調印された 1948 年を正式な設立年として記載している。(http://www.oas.org/en/about/who_we_are.asp)

[6] OAS: Our History (https://www.oas.org/en/about/our_history.asp)

[7] 外務省: 米州機構（OAS）概要　(https://www.mofa.go.jp/mofaj/area/latinamerica/kikan/gaiyo.html)

[8] キューバは 1962 年の対キューバ制裁決議により、カストロ政権の OAS 参加を排除され、同年キューバ側も OAS 脱退を発表した。その後、2009 年に同決議を廃止する旨の決議が採択されたものの、キューバ側は復帰をしていない。（外務省米州機構（OAS）概要、3.加盟国(1)注）

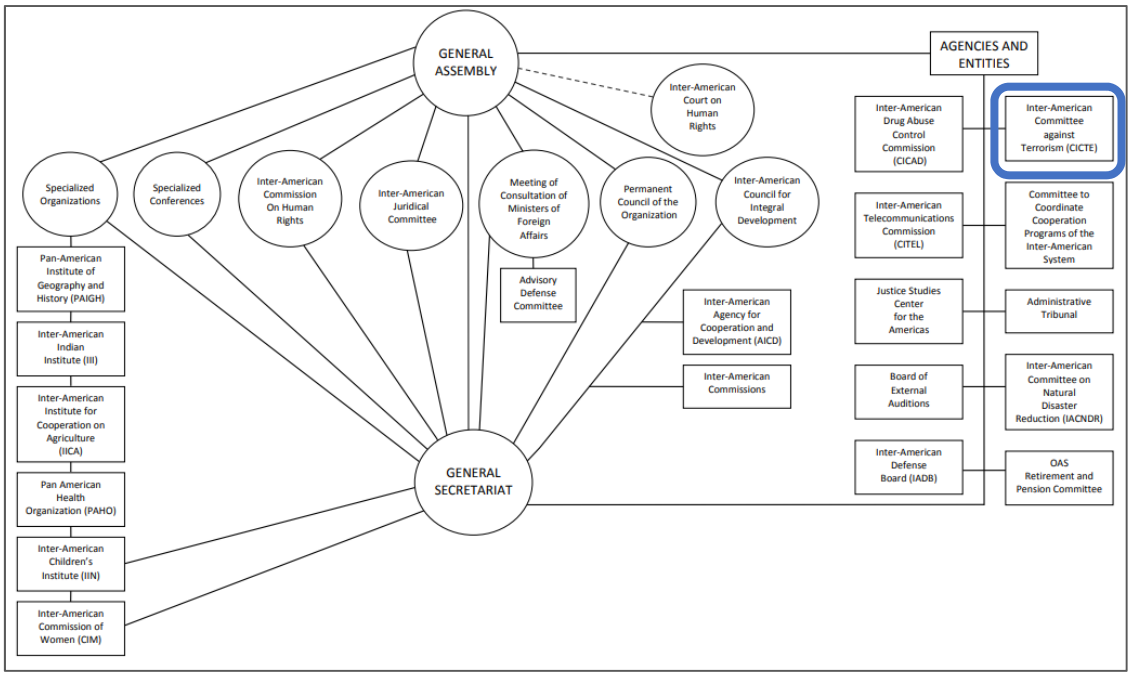
[9] OAS の Web サイトでの説明では、EU を含めて 70 のオブザーバーとして参加している旨記載されている。(https://www.oas.org/en/ser/dia/perm_observers/countries.asp)

## 2－2－4　OAS 組織構成

組織の目的を遂行するために次の組織体系がとられている。

① General Assembly（総会）
② Meeting of Consultation of Ministers of Foreign Affairs（外相協議会）
③ Councils（理事会）
④ Inter-American Juridical Committee（米州法律委員会）
⑤ Inter-American Commission on Human Rights（米州人権委員会）
⑥ General Secretariat（事務局）
⑦ Specialized Conferences（専門会議）
⑧ Specialized Organizations（専門機関）
⑨ Agencies and Entities（その他の主な機関）

Inter-American Drug Abuse Control Commission（米州麻薬濫用取締委員会）、Inter-American Telecommunication Commission（米州電気通信委員会）等に加えて、Inter-American Committee against Terrorism（米州テロ対策委員会、以下、CICTE）が設立されており、サイバーセキュリティに関する事項はテロ対策の一環として CICTE が所掌している。（図 4）




[図 4　OAS 組織構成および CICTE の位置づけ]
出典：OAS Organization of American States[10]

## 2－2－5　CICTE の活動

CICTE は OAS 加盟国をメンバーとして構成されており、毎年テロ対策の問題、評価方法や協力体制について協議や意思決定を行っている。2004 年の OAS 総会において、「サイバーセキュリティの脅威と戦うための米州の体系的戦略」について CICTE へ対応要請があった。これを受けて CICTE は OAS 加盟国の CSIRT 確立を支援し、CSIRT 間の情報連携やセキュリティ技術者に対する指導と支援を行っている[11]。

[10] OAS: Organization of American States (https://www.oas.org/legal/english/organigramaOEAeng.pdf)
[11] OAS: Cyber Security (https://www.sites.oas.org/cyber/en/pages/default.aspx)

2018 年から 2019 年のサイバーセキュリティ関連の活動計画には、OAS 加盟国に対するサイバーセキュリティ戦略整備支援、National CSIRT の設立や強化に係る支援、サイバーセキュリティに関する技術教育、ハッカソンやワークショップの企画運営を行うことが盛り込まれている[12]。

## 2－3　LACNIC の概要

The Latin American and Caribbean IP address Regional Registry（以下、LACNIC）は、ラテンアメリカとカリブ海地域の IP アドレス、AS 番号の割り当てや管理を行う組織である。（図 5）地域インターネットレジストリの 1 つとして、2002 年 10 月の ICANN 上海会議にて最終承認され、独立運用が始まった[13]。LACNIC と OAS は、政府、民間企業、市民社会間の連携を協調して強化促進することを目的として、サイバーセキュリティに関する公式な合意書を 2013 年 5 月 8 日に交わしている[14]。

LACNIC は毎年 5 月頃と 10 月頃にカンファレンスを開催しているが、5 月開催時には国際的非営利団体 Forum of Incident Response and Security Teams（以下、FIRST）の Regional Symposium と、10 月開催時には Technical Colloquia を会期中に併催するようになっている。

LACNIC が政府機関からの支援を得ているプロジェクトとしては、+RAICES Project（LACNIC 地域内にルート DNS サーバのコピーを展開するプロジェクト）、Frida Program（Regional Fund for Digital Innovation in Latin America and the Caribbean、ICT を使った地域発展に寄与する組織への資金支援）などがある。後者は International Development Research Center（国際開発研究センター、IDRC）を基に始まったプロジェクトで、のちに Swedish International Development Cooperation Agency（スウェーデン国際開発協力庁、SIDA）が支援に加わった。


[図 5　各地域のインターネットレジストリと LACNIC の管理範囲]
出典：APNIC "History of the Regional Internet Registries"[15]

[12] OEA CICTE: DRAFT WORK PLAN OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM FOR 2018-2019 (https://www.oas.org/en/sms/cicte/documents/sessions/2018/doc%208%20Plan%20de%20Trabajo%20CICTE01207E03.doc)

[13] JPNIC: LACNIC とは (https://www.nic.ad.jp/ja/basics/terms/lacnic.html)

[14] LACNIC: OAS and LACNIC Sign Cyber Security Agreement (https://www.lacnic.net/1672/2/lacnic/oas-and-lacnic-sign-cyber-security-agreement)

[15] APNIC: History of the Regional Internet Registries (https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/)

### 2－3－1　設立目的

設立目的はラテンアメリカとカリブ海地域の発展のためにオープンで安全なインターネット環境を推進することである。そのためにインターネットナンバーリソースの管理に加えて次の活動を行っている[16]。

① 他の組織とのトレーニング、協力、協調を通じて地域社会の能力開発
② 業界や国連のインターネットガバナンスフォーラムに関与する事による地域への貢献
③ さまざまな関係者を巻き込んだ参加型でボトムアップによるインターネットガバナンスの強化
④ 地域社会に係るインターネット標準の使用と展開促進
⑤ インターネットの発展に関する課題において、地域を永続的に主導

### 2－3－2　サービス提供範囲

ラテンアメリカおよびカリブ海地域の 33 カ国において 8,500 を超えるネットワーク事業者に対してインターネットナンバーリソースの管理等のサービスを提供している。

### 2－3－3　組織構成

運営責任者として理事が参加組織から選任される。またスタッフは次のとおり構成されている[17,18]。

① Strategic Relations Department
② Communications Department
③ Cooperation and Development Department
④ People Engagement Department
⑤ Administration and Finance Department
⑥ Services Department
⑦ Technology Area

Technology Area の担当者が Warning, Advice and Reporting Point（以下、WARP）というセキュリティインシデントを取り扱う組織を運営している。

### 2－3－4　LACNIC WARP の活動

サイバーセキュリティインシデント発生時の事態報告、LACNIC メンバー組織間（特に小規模な組織）での匿名情報仲介やセキュリティ事態の警告を通して管轄地域への調整を行い、サイバーセキュリティに関する課題を推進している[19]。具体的には以下の活動が行われている[20]。

① インシデント報告
LACNIC WARP の Web フォーム上からインシデントの分類（DoS、ブルートフォース、マルウエア、フィッシング、不正広告など）を選択し、その国における発生状況、緊急度を報告する。

[16] LACNIC: About LACNIC-Mission (https://www.lacnic.net/1004/2/lacnic/about-lacnic)
[17] LACNIC: Board of Directors (https://www.lacnic.net/1335/2/lacnic/board-of-directors)
[18] LACNIC: Staff (https://www.lacnic.net/1315/2/lacnic/staff)
[19] LACNIC News: LACNIC launches an incident response handling center (https://prensa.lacnic.net/news/en/cybersecurity/lacnic-launches-an-incident-response-handling-center)
[20] Lacnic warp (https://warp.lacnic.net/en/)

② 事例紹介
DoS 攻撃に活用される可能性をもった DNS サーバの設定修正の方法、技術支援した経緯、流行しているマルウエアの攻撃手法や予防策等の事例紹介をしている。

③ 人材育成
CSIRT の知識習得、強化や普及をはじめとして、DNS のセキュリティ対策、安全なルーティング方法などサイバーセキュリティに関する様々なトピックについての教材を作成している。また教育を活動地域の各国で実施している（2017 年は 3 カ国で CSIRT に関するワークショップを実施した)。

④ 統計情報の提供
LACNIC が管理するネットワーク上での攻撃例や通信状況のグラフを提供している。

- WARP へ報告された種類別のインシデント数、割合、発生源の表示
- LACNIC 管理のネットワーク上でのインシデント数や割合、ボットネット情報の表示

⑤ サイバーセキュリティ関連プロジェクト
ハニーネットワークを運用している。メキシコ、ウルグアイ、アルゼンチン、エクアドルに設置されたセンサーにより、地域で問題となる脅威を検出し、警戒を呼びかけている。

## 2－3－5　予算

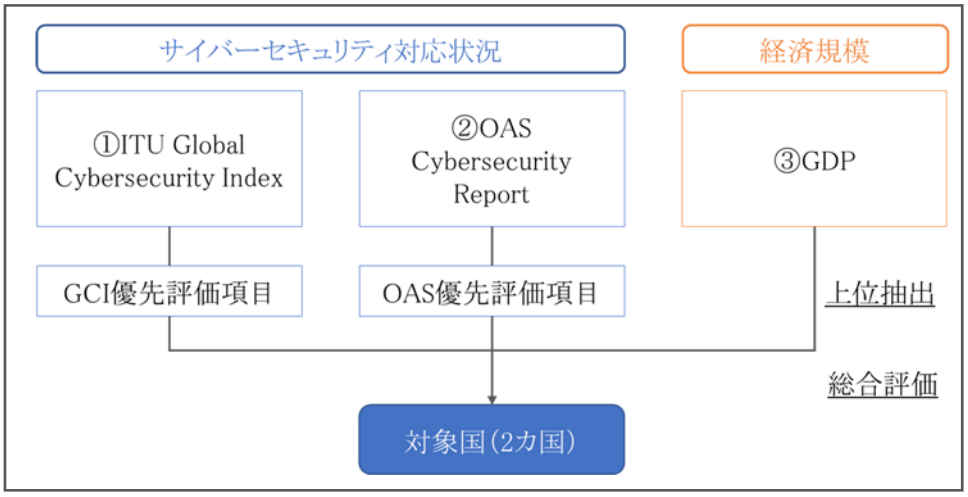
2018 年度予算の歳入は 7,997 千米ドルである。うち 95%を会員であるネットワーク事業者からの会費が占める[21]。

[21] LACNIC: Budget2018 (https://www.lacnic.net/2904/2/lacnic/budget-2018)

# 第3章　比較による各国の分析

本章では、中南米におけるより詳細なサイバーセキュリティの取組み状況を調査する、適切な対象国を選定するための検討を行う。選定にあたり、図 6 に示すように、中南米各国のサイバーセキュリティに対する対策状況を調査した報告書である①ITU の Global cybersecurity Index および②OAS の Cybersecurity report と、③各国の経済規模（GDP）を参照した。なお、サイバーセキュリティの対策状況に関する評価にあたっては、本調査の目的に合致する項目を選定し、優先評価項目を設定した。

①Global cybersecurity Index、②Cybersecurity report、③GDP の 3 つの指標からそれぞれ上位国を抽出し、それらの総合評価から本調査の対象国として 2 ヵ国を選定する。




[図 6　本調査の対象国選定フロー]

## 3－1　ITU “Global Cybersecurity Index”

### 3－1－1　概要

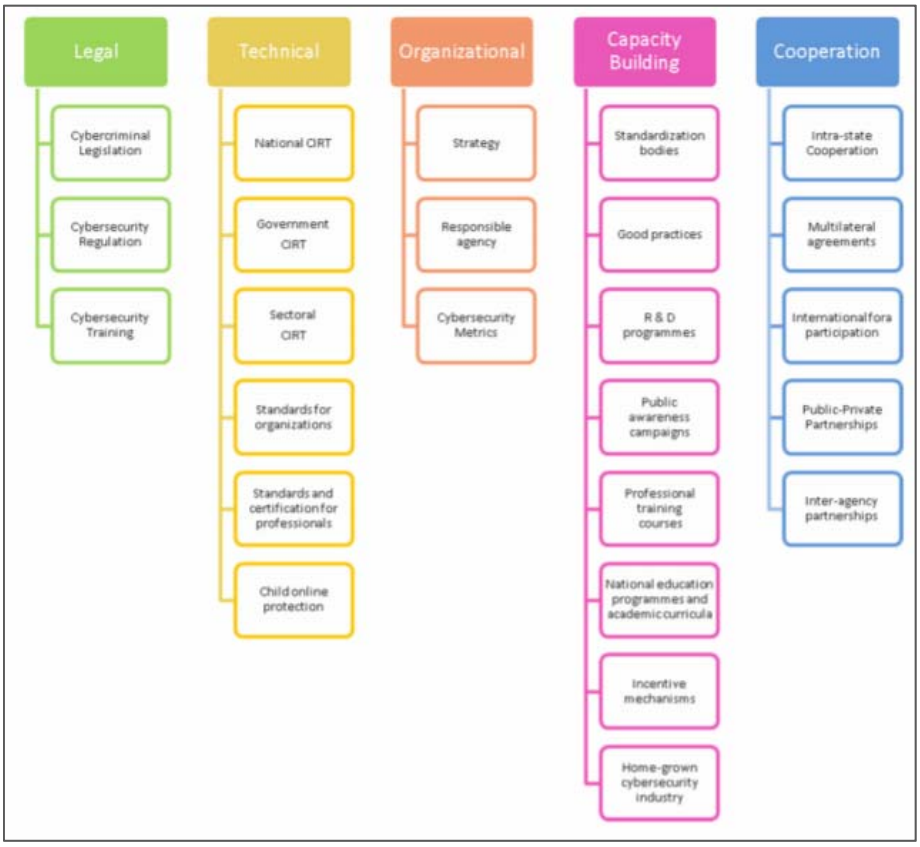
Global Cybersecurity Index（以下、GCI）は、ITU が 2017 年に 193 ヵ国の加盟国を対象にサイバーセキュリティ能力向上を目的として、各国の取組み状況を調査したレポートである。各国の取り組み状況を定量的に評価するため法律（Legal）、技術（Technical）、組織（Organization）、キャパシティビルディング（Capacity Building）、協力（Cooperation）の 5 つの評価軸を設け、それらの評価値を重みづけ平均して得られる GCI Score の数値により国別ランキングを導いている。概要は表 1 の通りである。

[表 1　Global Cybersecurity Index の数値評価-アメリカ地域より（参考）]
出典：ITU Global Cybersecurity Index 2017[22]

| Country | GCI Score | Legal | Technical | Organizational | Capacity Building | Cooperation |
|---|---|---|---|---|---|---|
| United States | 0.91 | 1 | 0.96 | 0.92 | 1 | 0.73 |
| Canada | 0.81 | 0.94 | 0.93 | 0.71 | 0.82 | 0.70 |
| Mexico | 0.66 | 0.91 | 0.89 | 0.48 | 0.68 | 0.34 |

[22] ITU: Global Cybersecurity Index 2017 (https://www.itu.int/pub/D-STR-GCI.01-2017)

各指標は、図 7 に示したそれぞれの小項目の評価値から算出される。




[図 7　Global Cybersecurity Index の評価軸の構成]
出典：ITU Global Cybersecurity Index 2017[23]

### 3－1－2　分析視点の優先度設定

本節では、GCI の評価結果を用いて、本調査の対象国を抽出するために、GCI の評価軸の中から本調査の目的に沿うものを優先評価軸として抽出する。

第 1 章にて述べた通り、本調査では「組織、体制の理解」に重点を置いている。そのため、対象国には「連絡窓口となる組織が整備されており、かつ定常的に活動していること」が必要となる。そこで、GCI のうち①国家 CIRT（National CIRT）および②所掌機関（Responsible Agency）を優先評価軸として抽出した。

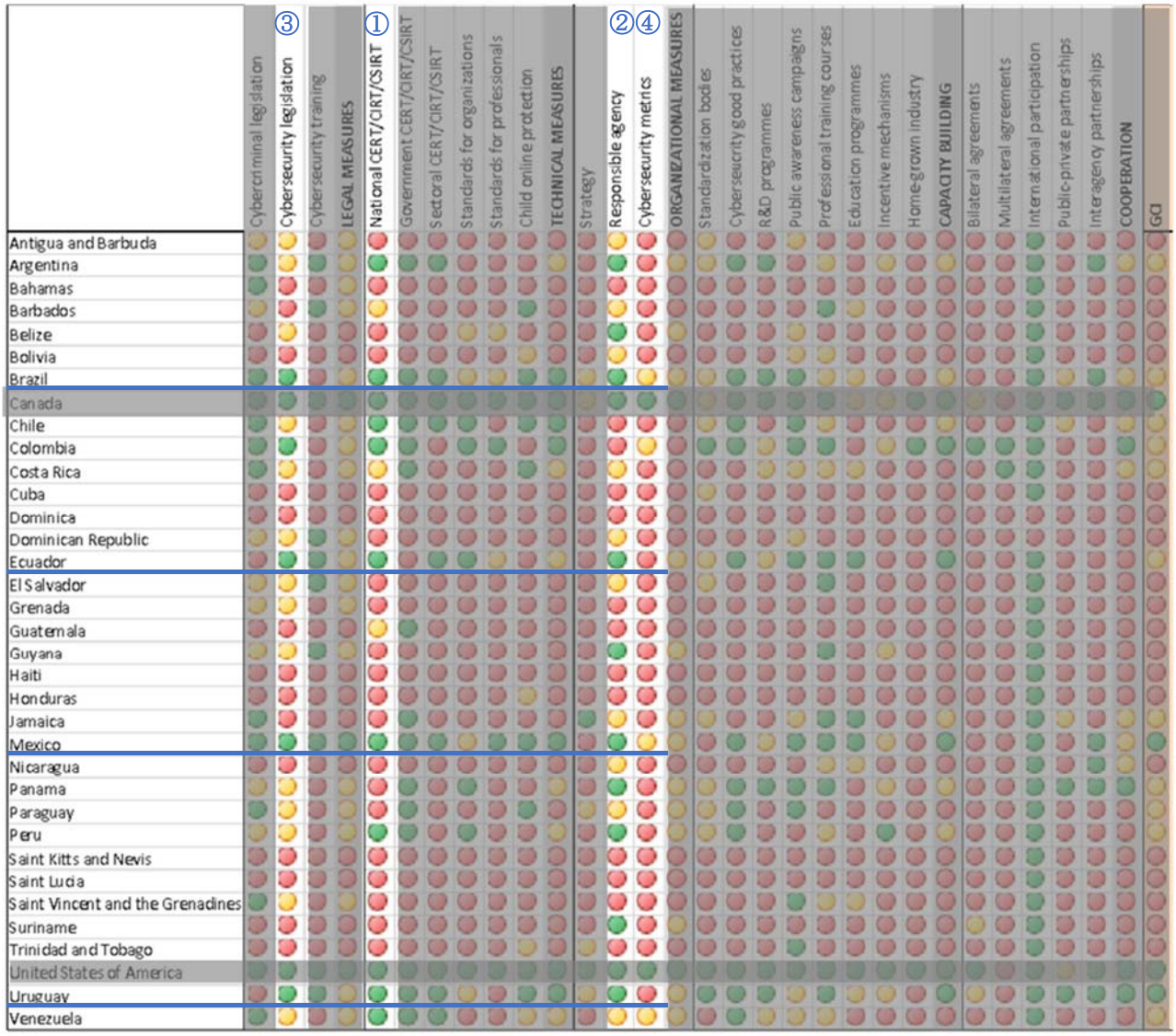
さらに、対象国のサイバーセキュリティに関する概況を把握するためサイバーセキュリティ戦略文書や関連法整備の状況等の公開文書調査を実施する必要がある。GCI のうち③法律（legislation）および④サイバーセキュリティ評価基準（Cybersecurity Metrics）を優先評価軸として抽出した。

### 3－1－3　分析結果

GCI には点数を各国比較するため、各評価軸を段階評価した一覧表が掲載されている。緑：高、黄：中、赤：低とする 3 段階で表示された各国のスコアを図に示す。これより、優先評価軸として選定した 4 つを参照すると、図 8 に示すとおり高い評価を得ている国はブラジル、エクアドル、メキシコ、ウルグアイ

[23] ITU: Global Cybersecurity Index 2017 (https://www.itu.int/pub/D-STR-GCI.01-2017)

の 4 か国となる。さらにこれらの国を比較すると、④評価基準（Cybersecurity Metrics）の評価によりメキシコ、ブラジルが中評価で、エクアドル、ウルグアイが低評価となっている。




[図 8　Global Cybersecurity Index のアメリカ地域評価結果]
出典：ITU Global Cybersecurity Index 2017[24]

## 3－2　OAS “Cybersecurity Report”

### 3－2－1　概要

Cybersecurity Report は、OAS が 2016 年に発行している、中南米のサイバーセキュリティの状態を包括的に整理したレポートである。Inter-American Development Bank（米州開発銀行）と OAS の共同研究であり、政府機関、重要インフラ事業者、軍、法執行機関、民間セクターおよび学術機関を対象に、オンラインでのアンケート、インタビュー、文献による調査を実施している。得られたデータは、英オックスフォード大学内に設けられた Global Cyber Security Capability Center（サイバーセキュリティ能力開発センター）が開発したサイバーセキュリティ成熟度基準に基づいて分析しまとめられている。同サイバーセキュリティ成熟度基準は政策と戦略　（Policy and Strategy）、文化と社会（Culture and Society）、教育

[24] ITU: Global Cybersecurity Index 2017 (https://www.itu.int/pub/D-STR-GCI.01-2017)

（Education）、法的枠組み（Legal Frameworks）、技術（Education）の 5 つの指標で構成され、各指標にはさらに細目を設け全体で 49 指標が設定されている。各指標に対する達成状況が 5 段階で表示され、各国のサイバーセキュリティ対策の成熟度の目安とすることができる。

各指標には GCI と同様に詳細な小項目が設けられている。評価軸の全体構成を図 9 に示す。


[図 9　Cybersecurity Report の評価軸]
出典：OAS 2016 Cybersecurity Report[25]

### 3－2－2　分析視点の優先度設

本節では、3-1 と同様に優先項目を設定した。

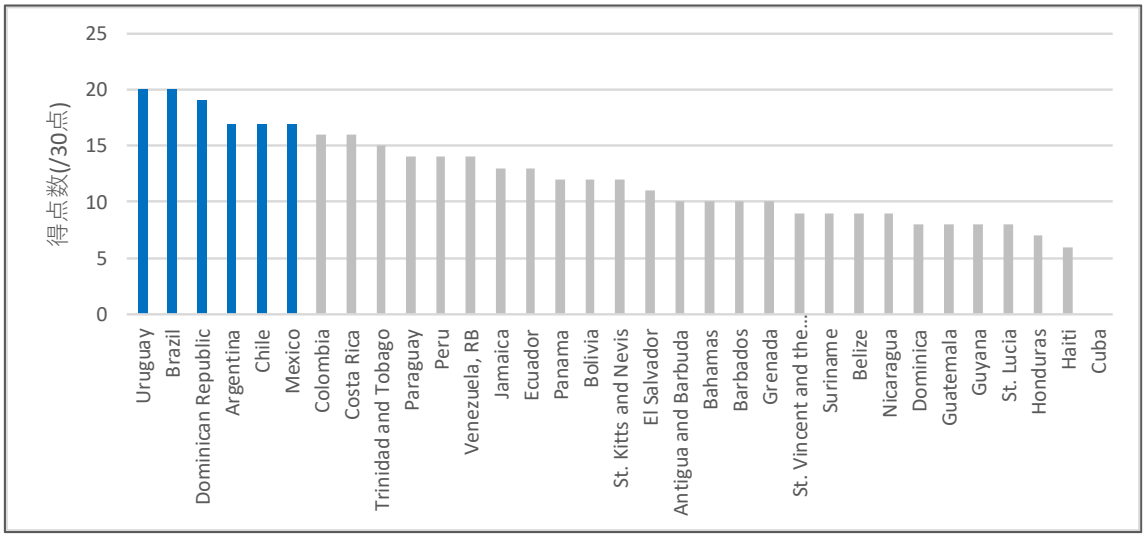
OAS 2016 Cybersecurity Report では、組織の活動状況を図る指標として、①Cybersecurity Coordinating Organization を、公開情報の充実度を図る指標として②Cybersecurity Legal Frameworks を優先項目として抽出した。

### 3－2－3　分析結果

Cybersecurity Report では、各国について評価項目に対して 5 段階の成熟度で評価する Country Profile を掲載している。本節では、優先項目に設定した①Cybersecurity Coordinating Organization の 2 項目と②

[25] OAS: 2016 Cybersecurity Report (https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf)

Cybersecurity Legal Frameworks の 4 項目の評価軸について、各項目 5 段階の得点方式で再評価を行った。再評価の結果 1 位はウルグアイとブラジルが同点、2 位はドミニカ共和国、3 位はアルゼンチンとチリとメキシコが同点となり、合計 6 ヵ国が調査対象として適するという結果が導かれた。




[図 10　Cybersecurity Report における評価結果の国別ランキング]
出典：OAS 2016 Cybersecurity Report[26]

[表 2　Cybersecurity Report における評価結果の上位国]
出典：OAS 2016 Cybersecurity Report[26] より作成

| 順位 | 国名 | ①Cybersecurity Coordinating Organizations | ②Cybersecurity Legal Frameworks | 合計 |
|---|---|---|---|---|
| 1 | ウルグアイ | 8 | 12 | 20 |
| 1 | ブラジル | 7 | 13 | 20 |
| 2 | ドミニカ共和国 | 3 | 16 | 19 |
| 3 | アルゼンチン | 5 | 12 | 17 |
| 3 | チリ | 4 | 13 | 17 |
| 3 | メキシコ | 6 | 11 | 17 |

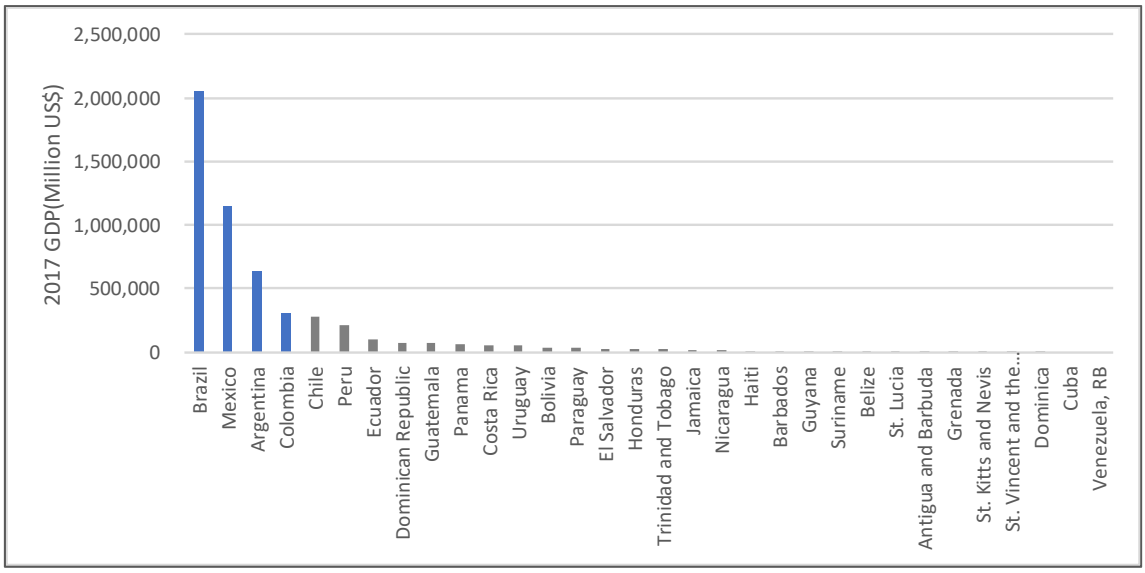
## 3－3　GDP
### 3－3－1　概要

世界銀行では、1960 年以降の世界各国の GDP の推計をインターネット上で公開している。当該 GDP データは米ドルで数値が記載されており、各国の比較が可能となっている。これより、公開データの中で最新年である 2017 年データを用いて中南米各国の GDP 比較を行い、経済規模の上位国を抽出する。

[26] OAS: 2016 Cybersecurity Report (https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf)

### 3－3－2　分析結果

中南米 32 カ国では約 5 兆 2,640 億米ドル の GDP があり、そのうち 1 位のブラジルが約 2 兆 555 億米ドル、2 位のメキシコが約 1 兆 1,499 億米ドル、3 位のアルゼンチンが約 6,376 億米ドル、4 位のコロンビアが約 3,092 億米ドルとなり、上位 4 か国で中南米の約 79%を占めていることがわかった。




[図 11　中南米における各国 GDP の比較]
出典：World Bank Open Data[27]より作成

### 3－4　分析結果の整理と本調査の対象国選定

上記の分析結果を一覧表に整理すると、アルゼンチン、ブラジル、チリ、コロンビア、ドミニカ共和国、エクアドル、メキシコ、ウルグアイの 8 ヵ国が上位国として抽出された。これらの結果を比較すると、サイバーセキュリティ対策状況を図る GCI と Cybersecurity Report の両方で抽出された国はブラジル、メキシコ、ウルグアイの 3 か国に絞られ、さらに経済規模を図る GDP を参照するとブラジル、メキシコが残る結果となった。

これより、先行調査において本調査の目的に合致する評価が高い国であり、かつ経済規模が大きい国と想定されるブラジル、メキシコを本調査の対象国として選定した。

[27] World Bank: World Bank Open Data (https://data.worldbank.org/)

[表 3　評価結果の比較]

出典：ITU GCI 2017[28]、OAS 2016 Cybersecurity Report[29]および World Bank GDP[30]データを基に作成

| 国名 | ITU Global Cybersecurity Index [評価数] | OAS Cybersecurity Report [評価順位（得点）] | GDP [億米ドル] |
|---|---|---|---|
| アルゼンチン | — | 3 位(17) | 6,376 |
| ブラジル | 高:3、中:1 | 1 位(20) | 20,555 |
| チリ | — | 3 位(17) | — |
| コロンビア | — | — | 3,092 |
| ドミニカ共和国 | — | 2 位(19) | — |
| エクアドル | 高:3、低:1 | — | — |
| メキシコ | 高:3、中:1 | 3 位(17) | 11,499 |
| ウルグアイ | 高:3、低:1 | 1 位(20) | — |

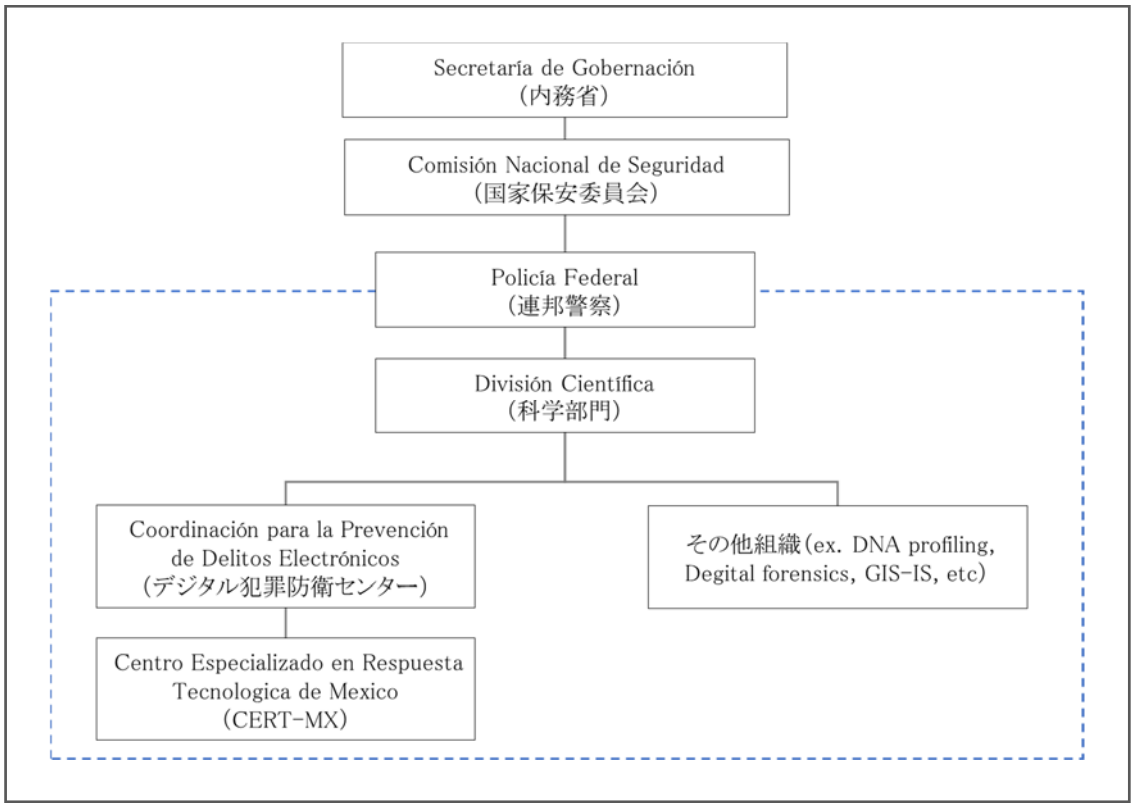
[28] ITU: Global Cybersecurity Index 2017 (https://www.itu.int/pub/D-STR-GCI.01-2017)
[29] OAS: 2016 Cybersecurity Report (https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf)
[30] World Bank: World Bank Open Data (https://data.worldbank.org/)

# 第4章　メキシコにおけるサイバーセキュリティに係る概要

本章の記載事項は、事前の文献調査および、2018 年 11 月に実施したメキシコ関係機関へのインタビューに基づくものである。

## 4－1　サイバーセキュリティ政策を所掌する省庁、公的機関

政府組織体制としては、Secretaría de Gobernación（以下、内務省）の傘下の Comisión Nacional de Seguridad （以下、国家保安委員会）の傘下に設立された Policía Federal（以下、連邦警察）の División Científica（以下、科学部門）が、サイバーセキュリティ政策を所掌している。また、防衛省配下の軍（陸軍、海軍）にも国防の観点からサイバーディフェンスを担う部門が存在する。




[図 12　サイバーセキュリティ政策に係る政府機関組織]
（インタビューを基に作成）

### 4－1－1　国家保安委員会

国家保安委員会は内務省の下部組織としてサイバーセキュリティも含む公共安全にかかわる政策の実行や州、地方公共機関との調整を行っている。

### 4－1－2　連邦警察科学部門

連邦警察における科学捜査部門であり、DNA 鑑定やサイバー犯罪を含む科学捜査を所掌しており、サイバー詐欺、フィッシング、児童ポルノなどのサイバー犯罪の取締を担当している。またアメリカの情報機関とも連携している。後述の CERT-MX は同部門の一部署という位置づけとなっている。

### 4－1－3　その他の公的機関

Coordinación para la Prevención de Delitos Electrónicos（デジタル犯罪防衛センター）は重要インフラの保護や監視を行っており、Instituto Federal de Acceso a la Información y Protección de Datos（情報・データ保護連邦研究所）は政府情報へのアクセス方法の管理や個人情報保護の促進等を行っている。

## 4－2　サイバーセキュリティ政策にかかる公的文書

### 4－2－1　政策、フレームワーク、アクションプラン、ガイドライン

#### 4－2－1－1　National Cybersecurity Strategy

① 策定された背景

2013 年－2018 年の国家開発計画（2013-2018 National Development Plan）に基づき 2017 年に National Cybersecurity Strategy が作成された。同戦略は、アプローチ可能な近代政府のための 2013 年－2018 年プログラム（2013-2018 Program for an Approachable and Modern Government）、2014 年―2018 年の国家公安プログラム（2014-2018 National Public Security Program）および、2014 年―2018 年国家安全保障プログラム（2014-2018 National Security Program）の達成に大きく貢献するものとされている[31]。

National Cybersecurity Strategy はメキシコが持続可能な発展をするために ICT の可能性を責任ある形で活用し、2030 年までにサイバー空間の脅威やリスクに対して耐性のある国になるというビジョンを確立するための文書として策定された。

② 記載概要

National Cybersecurity Strategy では戦略の目的と横断的なテーマを定義し、関係する利害関係者間のサイバーセキュリティに関する指標をそろえるために、戦略の実装、監視、評価のガバナンスモデルを示している。表 4 に示すように 5 つの戦略目標、3 つの基本原則が定義されており、戦略目標を達成するための 8 つの横断的な活動軸を定義している。

[表 4　National Cybersecurity Strategy における記載範囲]
出典: National Cybersecurity Strategy を基に作成

| 戦略目標 | 基本原則 | 分野横断的な活動軸 |
|---|---|---|
| ・社会と権利<br>・経済と改革<br>・公共機関<br>・公安<br>・国家安全保障 | ・人権の観点<br>・リスク管理<br>・分野をまたぐマルチステークホルダーの交流 | ・サイバーセキュリティ文化<br>・能力開発<br>・調整と共同活動<br>・ICT の研究、開発および改革<br>・標準化と技術基準<br>・重要インフラ<br>・法的枠組みと自己規制<br>・評価と観察 |

[31] Gov.mx: NATIONAL CYBERSECURITY STRATEGY
(https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf)

### 4－2－1－2　5 measures to strengthen cyber security for the stability of the Mexican Financial System

Secretaría de Hacienda y Crédito Público （大蔵公債省）により、金融システムにおける情報と処理の保護と攻撃に対する迅速な対応を可能とする目的で、2017 年 10 月 23 日に金融機関向けの対応方針が提示されている[32]。

## 4－2－2　白書、調査レポート

メキシコのサイバーセキュリティに関して公開されている調査レポートとしては、表 5 に示したものがあげられる。

[表 5　メキシコのサイバーセキュリティに関して公開されている主な調査レポート]

| タイトル | 発行年月 | 発行者 | 概要 |
|---|---|---|---|
| Perspectiva de ciberseguridad en México | 2018 年 6 月 | McKinsey& Company | メキシコにおけるサイバーセキュリティの動向 |
| Cybersecurity Market Analysis | 2018 年 1 月 | PROMEXICO | 世界的なサイバーセキュリティ流行状況やメキシコ国内における動向 |
| The State of Cybersecurity in Mexico: An Overview | 2017 年 1 月 | Wilson Center Mexico Institute | メキシコにおけるサイバーセキュリティの状況や分析結果 |

## 4－3　サイバーセキュリティに係る法制度

メキシコのサイバーセキュリティ犯罪に関する法律は、連邦刑法に含まれているため連邦警察が国家レベルでサイバー犯罪を調査する責任を負っている[33]。なお、金融犯罪、情報漏洩、テロ、誘拐、麻薬密売などのほかの犯罪に関しても連邦刑法で定められている。サイバー犯罪に関連する法令として以下が存在する[34]。

## 4－3－1　連邦刑法（Federal Criminal Code）

サイバー脅威に関連する特定の章が含まれており、許可なしに著作権で保護された素材を悪意ある方法で使用、複製、配布、保管、販売またはリースし金銭的利益を得た場合は刑事罰が科される。また公共サービスを破壊または妨害する犯罪も規制されている。

例えば、コンピュータシステムおよび機器への不正アクセスに関して、許可を受けていない者が、セキュリティ機構によって保護された状態のコンピュータシステムまたはコンピュータに含まれる情報を変更、

[32] Gov.mx: 5 medidas de fortalecimiento de la ciberseguridad para la estabilidad del Sistema Financiero Mexicano (https://www.gob.mx/shcp/articulos/conoce-los-5-principios-para-el-fortalecimiento-de-la-ciberseguridad-para-la-estabilidad-del-sistema-financiero-mexicano?idiom=es)

[33] The State of Cybersecurity in Mexico: An Overview (https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf)

[34] PROMEXICO: Cybersecurity Market Analysis (http://mim.promexico.gob.mx/work/models/mim/Resource/154/1/images/diagnostico-ciberseguridad.pdf)

破棄、または紛失させた場合の懲役や罰金について定められている（連邦刑法 211 条 1 項から 7 項[35]）。

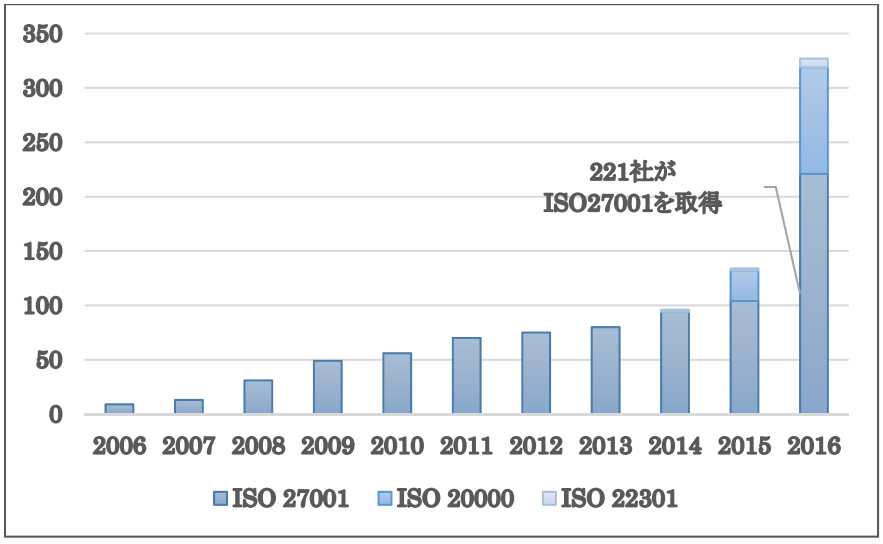
### 4－3－2　その他の法律

金融機関の法律にはクレジットカード情報に影響する行為への罰則があり、これに違反した個人データの取扱いをした場合には処罰される可能性がある。著作権、電話通信、電子商取引、電子署名等に関する法律による規制があり、2018 年 3 月には金融テクノロジー機関規制法（LRITF、通称：フィンテック法）も施行されている[36,37]。

## 4－4　政府 ICT システムに係るセキュリティ対策標準等

メキシコでは主要な政府組織に対して ISO 27001（情報セキュリティマネジメント規格）の準拠を求めている[38]。2017 年の National Cybersecurity Strategy では、「標準化と技術基準」に言及されており、今後、メキシコ独自の標準が策定される可能性がある。

民間企業においても、近年、IT 企業に対し契約上の要件として情報セキュリティマネジメントに関する一定の基準を満たしていることを求める傾向が強くなっており、社内外に情報セキュリティ対策を実施していることを証明する手段として、ISO27001 などの情報セキュリティに関する第三者認証の取得が一般化している。2016 年時点で 221 社（うち 73.3%が IT 企業）が ISO27001 を取得している[39]。（図 13）




[図 13　メキシコ民間企業におけるマネジメント認証取得状況]
出典: PROMEXICO Cybersecurity Market Analysis[39] より作成

[35] Informatica juridical: Art. 211 bis 1 al 211 bis 7 del Código Penal (https://www.informatica-juridica.com/codigo/codigo-penal-federal-mexicano-art-211-bis-1-al-211-bis-7/)

[36] JETRO:調査レポート中南米の制度改定動向 (https://www.jetro.go.jp/ext_images/_Reports/01/1a423d2c3421df7d/20170139.pdf)

[37] LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA :Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos に基づく 2018 年 3 月 8 日に発行された法令 (http://www.diputados.gob.mx/LeyesBiblio/doc/LRITF_090318.doc)

[38] ITU: CYBERWELLNESS PROFILE MEXICO (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Mexico.pdf)

[39] PROMEXICO: Cybersecurity Market Analysis (http://mim.promexico.gob.mx/work/models/mim/Resource/154/1/images/diagnostico-ciberseguridad.pdf)

## 4－5　主要 CSIRT：組織名、役割（業務内容）、体制

メキシコにおける主要 CSIRT としては、National CSIRT である CERT-MX、民間 CSIRT である SCITUM-CERT、学術系 CSIRT である UNAM-CERT が存在する。

### 4－5－1　CERT-MX

#### 4－5－1－1　概要

2010 年 6 月、連邦警察内のサイバーインシデント対応部署として Centro Especializado en Respuesta Tecnológica de México（以下、CERT-MX）が設立された。連邦警察科学部門の一部署という位置づけであり、CERT-MX 固有の設立根拠法はない。24 時間 365 日対応できる体制をとっており、主にインシデント対応を行うレスポンスチーム、啓発活動（SNS のリスク等）や情報収集および情報発信を行うインテリジェンスチーム、サイバー犯罪捜査・犯人逮捕も行う捜査チームの 3 つに分かれて活動している。

#### 4－5－1－2　主な活動内容

主な活動内容は次のとおりである[40]。

① サイバー犯罪行為の調査や防止活動によりサイバー攻撃の脅威を低減させる
② メキシコが扱う技術的基盤に不具合が生じていないことを監視する
③ 連邦レベルで認定された唯一の機関として国際的な警察機関と情報交換を行う
④ インターネット環境を 24 時間 365 日体制で監視する
⑤ CSIRT の国際フォーラム FIRST のコミュニティに参加する
⑥ ソフトウエア、ハードウエアに関わらず製造業者で発見された脅威について国際機関と情報交換を行う
⑦ 民間や公的機関におけるサイバーセキュリティの理解を促進するための活動を行う

### 4－5－2　SCITUM-CERT

#### 4－5－2－1　概要

民間企業である SCITUM 内の CSIRT である。SCITUM は、1998 年 3 月の設立で、国内最大手通信事業者 TELMEX のパートナーとしての強みを活かし、サイバーセキュリティに係るアセスメント、ソリューション提案、実装、運用、モニタリングといったコンサルティングから運用サービスまでを提供するメキシコ国内最大のマネージドセキュリティサービスプロバイダとして、メキシコ政府や国内外の民間企業からサイバーセキュリティ分野の業務を請け負っている。その中でも、サイバー攻撃の検知やマルウエア解析、注意喚起の発行など実際のインシデント対応に関わる部分を担うのが SCITUM-CERT であり、SOC によるモニタリング業務を 24 時間体制で行っている。アメリカ、コロンビア、ペルーの拠点にも人員が配置されている。

[40] Gov.mx: Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal (https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es)

#### 4－5－2－2　主な活動内容

主な活動内容は次のとおりである。

① 攻撃者グループの行動分析による地域的動向の可視化
② 流行している脅威情報の提供や被害内容の可視化
③ マルウエア解析を含む他機関との共同捜査
④ サイバーセキュリティ・インテリジェンス教育

### 4－5－3　UNAM-CERT

#### 4－5－3－1　概要

UNAM-CERT は、Universidad Nacional Autónoma de México（メキシコ国立自治大学、以下、UNAM）内の CSIRT である。UNAM は、1575 年に設立されたラテンアメリカで最も歴史ある大学（1821 年のメキシコ国独立よりも古い）であり、これまでに 3 名のノーベル賞受賞者を輩出している。現在の学生数は約 374,000 人。メキシコ国内に 45 キャンパス、海外に 20 キャンパスを有する。UNAM-CERT は、1991～92 年頃から活動を開始しているメキシコで最も古い学術系 CSIRT であり、当初はスーパーコンピュータの防衛を主目的として設立された。

#### 4－5－3－2　主な活動内容

主な活動内容は次のとおりである。

① 同大学保有の情報および国が保有している情報資産（メキシコ国内の約 75%の研究資料）の管理
② 情報取り扱いに関する内部規定に基づく、セキュリティポリシーの関する大学内における啓発活動
③ 人材育成として毎年 20～25 名を奨学金付きインターン（6 カ月）として受入れ

## 4－6　サイバーセキュリティ対策に係る連携体制

### 4－6－1　国内連携

メキシコ国内において、National CSIRT である CERT-MX を中心に、CERT-MX、SCITUM-CERT、UNAM-CERT がそれぞれ公共部門、民間部門、学術研究機関という活動領域で入手した情報（サイバー犯罪の動向、関係者、犯罪手口、対策方法等）について適宜、情報交換を行い、緊密な組織間連携を行っている。

主要な 3 つの CSIRT 以外の機関との連携も行われており、CERT-MX はサイバーディフェンスを担う軍（陸軍、海軍）に対する技術的支援やトレーニングを実施し、司法機関や立法機関に対しても、サイバーセキュリティに関する基礎的な研修を提供している。加えてメキシコのドメイン名、IP アドレス等を管理する非営利組織 NIC México とも必要に応じ連携している。また、SCITUM-CERT は民間 IT 企業や Instituto Politécnico Nacional（国立工科大学）とも連携をおこなっている。

### 4－6－2　中南米内連携

#### 4－6－2－1　OAS、LACNIC による域内連携の取り組み

CERT-MX は OAS の中南米連携プログラムに賛同しており、OAS が毎月開催する Web 会議のほか、情報交換や勉強会（アルゼンチン、コロンビア、ブラジル等が参加している）にも参加している。また、OAS 加盟国間で各国が得意分野の講師を派遣し、互いにトレーニングを提供し合う取り組みにも参加してい

る（主にトレーニングはワシントン DC でおこなわれている）。
LACNIC が開催する年次会合には、CERT-MX が参加することもあるが、基本的に LACNIC のメキシコにおけるカウンターパートは NIC México である。インターネットエクスチェンジ(IX)、ISP に関連する問題については、必要に応じ CERT-MX は NIC México と連携している。

#### 4－6－2－2　その他中南米内での連携

CERT-MX にとって最も繋がりが強いのは、米国である。アメリカの法務省、FBI、US-CERT 等の機関との情報交換を行っている。アメリカ以外ではメキシコと国の状況が似通っており、National CSIRT の規模も同等であるコロンビアとの関係が強く、トラフィック情報等の共有も行われている。

### 4－6－3　その他海外との連携

#### 4－6－3－1　CERT-MX による国際的枠組みへの参加

CERT-MX、SCITUM-CSIRT、UNAM-CERT に MNEMO CERT というインシデント対応センターを加えた 4 機関は、CSIRT の世界的な集まりである FIRST のメンバーとして国際連携可能な体制をとっている。また、スペインからも支援を得ている。

一方、SCITUM-CERT は、増加する SNS 上でのクレジットカード犯罪に関連したグループの活動（Facebook 上での特価販売を謳い文句にしたカード情報の入手、金融機関内部の者との結託や買い物ポイントを盗むケース等）について、INTERPOL（国際刑事警察機構）への捜査協力を行っている他、技術領域では Cisco（サイバーセキュリティ調査グループ Talos）、およびマイクロソフトと連携している。

#### 4－6－3－2　サイバー犯罪に関する条約への参加

サイバー犯罪に関する刑事実体法、刑事手続法および国際捜査協力に関する規定を含んだ世界初の包括的な国際条約として、2001 年 11 月に「サイバー犯罪に関する条約（Convention on Cybercrime）」が欧州評議会で採択された。欧州評議会はヨーロッパ諸国が、人権、民主主義、法の支配といった価値観の実現のために設置した国際機関である。

メキシコはオブザーバーとして欧州評議会に参加しているが、法律や規制の問題がありすべての条項を遵守することが困難という理由で批准していない 。

### 4－7　サイバーセキュリティに係る啓発活動、人材育成活動

メキシコ国内において CERT-MX、SCITUM-CERT、UNAM-CERT はそれぞれ収集した脅威情報の発信や啓発活動を行っている。個別の状況については次のとおりである。

#### 4－7－1　CERT-MX による活動

CERT-MX は啓発活動として、SNS での情報発信（Facebook、Twitter、YouTube、Instagram）やパンフレットの配布（中小企業向けのサイバーセキュリティに関する注意喚起を促すもの等）、また、教育機関を訪問しての講義（全国の教育機関等を訪問し、経営層、教師、父母、生徒などを対象に SNS 使用にまつわるリスクや ISO27001 の重要性について講義を実施。年間約 2,000 名以上が受講）を通じた啓発活動をしている。また、2017 年の National Cybersecurity Strategy に基づき、政府機関、学術機関、民

間企業（特に、重要インフラである銀行、電力、石油等の業界）のコミュニティを形成し、それぞれに対する注意喚起を行っている。

### 4－7－2　大学や技術機関による活動

教育機関により、ICT に係る各種コースが提供されており、一部オンラインでの受講も可能である。また、サイバーセキュリティ関連の認証資格も国際的に認知されている資格が取得可能なコースも存在する[41]。（図 14 は UNAM を含むサイバーセキュリティ関連コース）

Education and training in 2017

| Educational entity | Career/ Major |
|---|---|
| Instituto Politécnico Nacional | Maestría en Ingeniería en Seguridad y Tecnologías de la Información. |
| Universidad La Salle | Maestría en Ciberseguridad. |
| Universidad Autónoma de Nuevo León | Licenciatura en Seguridad en Tecnologías de Información |
| UNITEC | Maestría en seguridad de tecnología de información |
| UNAM | Diplomado en Ciberseguridad |
| Escuela de Inteligencia para la Seguridad Nacional del Centro de Investigación y Seguridad Nacional (ESISEN) | Varios |
| Universidad Internacional de la Rioja (UNIR) | Maestría en Seguridad Informática (Online) |
| Universidad Internacional de Valencia | Máster en Seguridad Informática (Online) |
| Instituto Tecnológico y de Estudios Superiores de Occidente | Ingeniería en seguridad informática y redes |

Most relevant cybersecurity certifications in Mexico

| | Institution | Certification |
|---|---|---|
| Security General Knowledge | ISACA | CISA, CISM, CRISC |
| | ISC | CISSP |
| | CompTIA | CompTIA A+, Security+ |
| Specialist | CompTIA | Network+ |
| | SANS | GIAC,GPEN, GWAPT |
| | SEC-Council: | CEH, CHFI |
| Product / Brand | CISCO | CCSP, CCNP, CCIP, CCDP |
| | RSA | Various |

[図 14　サイバーセキュリティに関する教育カリキュラムおよび、認証資格の提供例]
出典：PROMEXICO Cybersecurity Market Analysis[41]

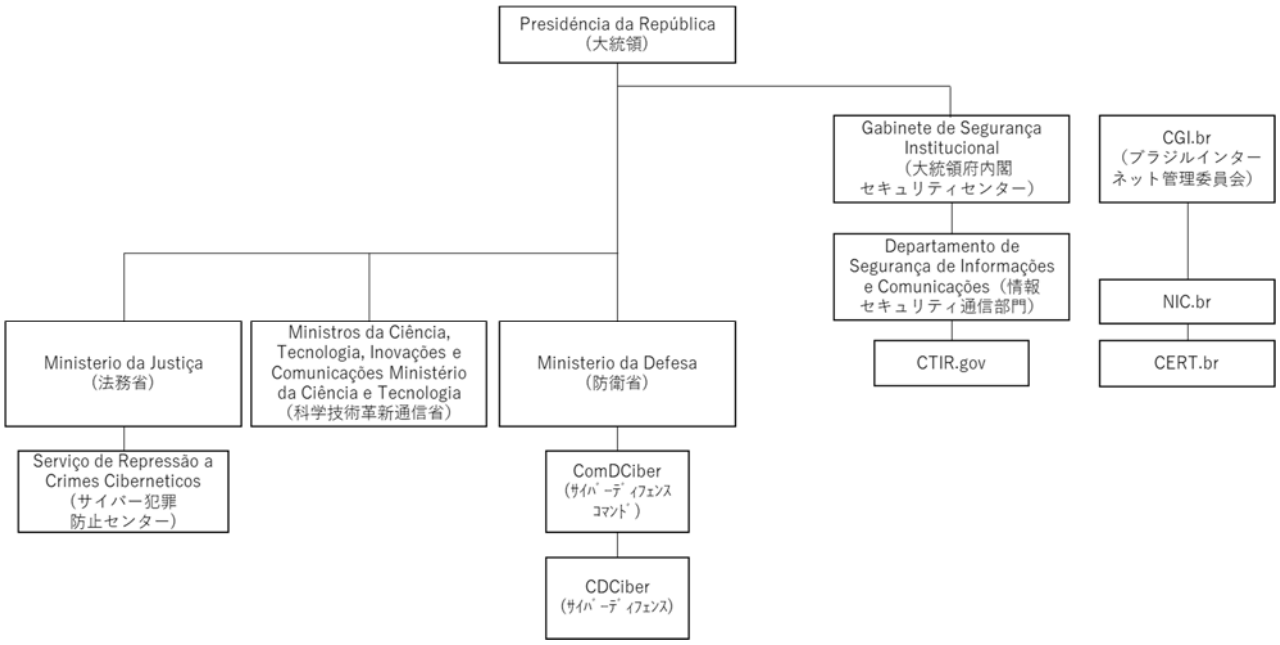
[41] PROMEXICO: Cybersecurity Market Analysis (http://mim.promexico.gob.mx/work/models/mim/Resource/154/1/images/diagnostico-ciberseguridad.pdf)

# 第5章　ブラジルにおけるサイバーセキュリティに係る概要

本章の記載事項は、事前の文献調査および、2018 年 11 月に実施したブラジル関係機関へのインタビューに基づくものである。

## 5－1　サイバーセキュリティ政策を所掌する省庁、公的機関

ブラジルのサイバーセキュリティ政策に関しては、政治的背景等を理由に、その対応責任の多くをブラジル国軍が担ってきていたという経緯がある。現在は、図 15 に示すとおり Ministros da Ciência, Tecnologia, Inovações e Comunicações（以下、科学技術革新通信省）や Ministerio da Justiça（法務省）といった複数機関が関与しているが、本分野を所掌する中心的な行政機関としては、依然として Ministerio da Defesa（以下、防衛省）があげられる。加えて、Gabinete de Segurança Institucional（以下、大統領府内閣セキュリティセンター）が、防衛の観点以外からサイバーセキュリティ政策を所掌する機関として防衛省ともにブラジルのサイバーセキュリティ政策を牽引している。具体的な組織としては、大統領府内閣セキュリティセンターの Departamento de Segurança de Informações e Comunicações（情報セキュリティ通信部門）、防衛省の Comando de Defesa Cibernética（以下、ComDCiber）および、Centro de Defesa Cibernética（以下、CDCiber）が特に重要な役割を担っている。




[図 15 サイバーセキュリティ政策に係る政府機関組織]
出典:ブラジル防衛省資料 CORDEIRO, MAJOR LUIS EDUARDO POMBO CELLES, and BRAZILIAN AIR FORCE. "CYBER ATTACKS: IS BRAZIL PREPARED?"およびサイバー空間に対する諸外国の施策動向調査より作成

### 5－1－1　防衛省

ブラジルの実務家が述べているように、「国家軍事・情報活動とも関連することの多い、サイバー空間における攻撃あるいは反撃戦闘のために用いられる軍事行動」を含むサイバー防衛と対比して、サイバーセキュリティを「先制的かつ抑圧的な行動であり、通常は、関係するシステムや人々が継続的に注意を払い、準備ができている状態を指す。またそのようにサイバー空間を守ろうとする個人や企業の個別の取

り組みのこと」と定義した上で、主にサイバー防衛の観点から防衛省が中心となって検討を進めている[42,43]。
防衛省の中でも、特に陸軍配下の ComDCiber と CDCiber が中心となり防衛分野におけるサイバーセキュリティ関連の活動を牽引している。CDCiber の方が設立は早く 2012 年 6 月より運用が開始され、最初の任務は国連持続可能な開発会議（Rio+20）の際のネットワーク防衛であった。一方、ComDCiber は、防衛分野のサイバー事業を体系的に計画・運営・管理するために 2016 年に設立され、National Cyber Defense Academy（国家サイバー防衛学校）でのサイバーセキュリティ人材育成を含む複数のプロジェクトを実施している[44]。

### 5－1－2　大統領府内閣セキュリティセンター情報セキュリティ通信部門

大統領府内閣セキュリティセンター情報セキュリティ通信部門は 2006 年 5 月、Presidential Decree No. 5772 により設立され、防衛省と共にサイバーセキュリティ政策を所掌しているが、2017 年 6 月の Interministerial Ordinance No. 91 により、改めて次の事項を所掌することが定義された[45]。

① 国家機密情報の取扱いに係る認証、評価
② 連邦行政機関における情報セキュリティポリシーおよび実施計画の策定
③ 連邦行政機関におけるサイバーセキュリティおよび機密情報を取り扱うインフラ整備に係る要件定義
④ 連邦行政ネットワークにおけるインシデント対応
⑤ 情報セキュリティに係る法規制の研究および提言
⑥ 情報セキュリティおよび国家機密情報取扱に係る国際的条約や枠組みの評価
⑦ 連邦行政機関における情報セキュリティポリシー実施計画の実施状況モニタリング

サイバーセキュリティ全般は防衛省が所掌しているが、国家機密情報の取り扱いや、連邦行政機関における情報セキュリティ、サイバーセキュリティについては、大統領府内閣セキュリティセンター情報セキュリティ通信部門が一定の役割を担っている。また、連邦行政ネットワークにおけるインシデント対応については、大統領府内閣セキュリティセンター情報セキュリティ通信部門の傘下に Centro de Tratamento de Incidentes de Redes do Governo （以下、CTIR.gov）が実施機関として存在する。

### 5－1－3　科学技術革新通信省

科学技術革新通信省は、2014 年 1 月に技術政策に関する優先取り組み施策を公表した。その最初の施策の一つとして、サイバーセキュリティ政策の策定を挙げ、民間部門のサイバーセキュリティ強化にも取り組むことを明らかにしている[43]。

[42] Deconstructing cyber security in Brazil: Threats and Responses (https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf)
[43] NISC（内閣サイバーセキュリティセンター）:サイバー空間に対する諸外国の施策動向調査 (https://www.nisc.go.jp/inquiry/pdf/shisakudoko_honbun.pdf)
[44] Diálogo: Brazilian Army Invests in Cyber Defense (https://dialogo-americas.com/en/articles/brazilian-army-invests-cyber-defense)
[45] DSIC: Missao do DSI Web サイト (http://dsic.planalto.gov.br/assuntos/missao-do-dsic)

## 5－2　サイバーセキュリティ政策にかかる公的文書

### 5－2－1　政策、フレームワーク、アクションプラン、ガイドライン

#### 5－2－1－1　サイバーセキュリティ戦略（2015-2018）（2015 年）

本文書の副題は「情報通信の安全保障戦略と連邦行政のサイバーセキュリティ」であり、2008 年 6 月の Normative Instruction GSI / PR 01/2008 を補完し、2015 年から 2018 年の 4 年間の戦略的目標を定めている[46]。現在、2019 年から 4 年間の戦略を新たに策定中である。CTIR.gov が調整役となり 20 の CSIRT が参加するワーキンググループを立ち上げ、議論が行われている。同ワーキンググループにおいては、特に大規模な事案に対する国家レベルでのインシデント対応戦略の策定と、重要インフラおよび政府機関のセキュリティ対策に焦点が当てられている。

#### 5－2－1－2　サイバー防衛政策（2012 年 12 月、防衛省）

本文書は、「戦略レベルにおけるサイバー防衛活動や、作戦・戦術レベルのサイバー戦争に関するサイバー防衛活動のガイドライン」として位置づけられている[47]。本文書は全ての軍関係者に適用される他、サイバー防衛およびサイバー戦争に参加する関係者も含まれるとされる。本政策では、次の 9 つの実施目的が規定されている[48]。

① 国防軍によるサイバー空間の効果的な利用確保、国家防衛の利益に対抗する利用の防止
② 防衛省内のサイバーセクターの業務を実施できる人材の育成
③ 首相府や他のセキュリティ関連部門との連携
④ サイバーセクターの運用方針の策定・改訂
⑤ 防衛省内の情報通信セキュリティマネジメントに貢献する手法の実行
⑥ サイバーセクターの需要を踏まえた 研究開発の実施
⑦ サイバーセクターにおける雇用に関する法律や規則を制定、基本原則の策定
⑧ オペレーション能力を確保するための軍事動員の取り組みへの協力、サイバーセクターの能力維持
⑨ 防衛省所掌範囲外のサイバーセキュリティに関連する連邦行政機関の情報資産に関するセキュリティ確保

### 5－2－2　白書、調査レポート

ブラジルのサイバーセキュリティに関して公開されている主な調査レポートとしては、表 6 に示したものがあげられる。

---

[46] Departamento de Segurança da Informação e Comunicações: ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES E DE SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL (http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf/view)

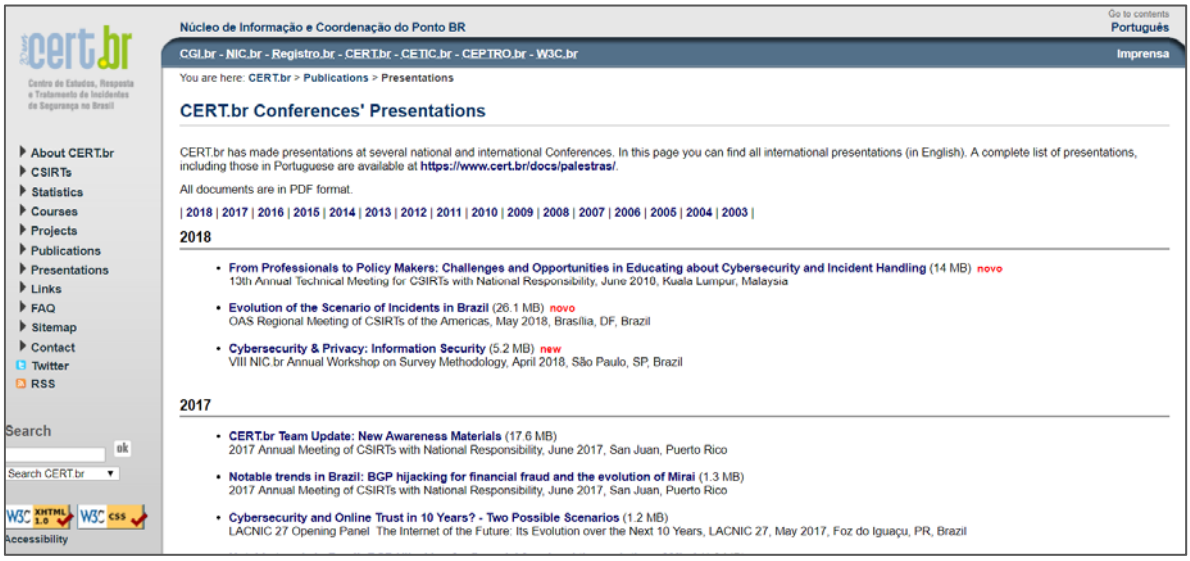
[47] NISC（内閣サイバーセキュリティセンター）:サイバー空間に対する諸外国の施策動向調査 (https://www.nisc.go.jp/inquiry/pdf/shisakudoko_honbun.pdf)

[48] Ministério da Defesa: POLÍTICA CIBERNÉTICA DE DEFESA (https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf )

[表 6　ブラジルのサイバーセキュリティに関して公開されている主な調査レポート]

| タイトル | 発行年月 | 発行者 | 概要 |
|---|---|---|---|
| Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015 | 2016 年 1 月 | トレンドマイクロ | ブラジルのサイバー犯罪アンダーグラウンドに関するレポート |
| Deconstructing Cyber Security in Brazil: Threats and Responses | 2014 年 12 月 | Igarapé Institute（ブラジルのシンクタンク） | ブラジルのサイバーセキュリティ政策に係る改善提案等 |
| Livro Verde de Defesa Cibernética–The Green Book of Cybernetic Defense | 2010 年 | ブラジル大統領府内閣セキュリティセンター情報セキュリティ通信部門 | ブラジルがサイバーセキュリティ対応能力を強化するための方策を経済、社会、政治など多面的視点から検討したもの |

また、CERT.br（後述）の Web サイトでも、図 16 に例示したように CERT.br が過去に作成した豊富なプレゼン資料を確認することができる。




[図 16　CERT.br のプレゼン資料ページ]
出典: CERT.br: Presentations at Conferences[49]

## 5−3　サイバーセキュリティに係る法制度

2008 年にサイバー空間の防衛を含む The National Strategy of Defense（国家防衛戦略）が制定された。その後、サイバー犯罪に対する警察による法執行を強化するため、2012 年 11 月に Azeredo Act – Law 12735/12329 と Carolina Dieckmann Act – Law 12737/12330 の 2 つのサイバー犯罪関連法案が可決された[50]。可決された 2 法案は、コンピュータや電子機器への不正アクセス、パスワードや暗証番号の不正

[49] CERT.br: Presentations at Conferences (https://www.cert.br/docs/presentations/)
[50] NISC（内閣サイバーセキュリティセンター）：サイバー空間に対する諸外国の施策動向調査 (https://www.nisc.go.jp/inquiry/pdf/shisakudoko_honbun.pdf)

取得、画像の無断流出、コンピュータウイルスの拡散など、ネットワーク上で行われるサイバー犯罪に関する国内初の法律である。

## 5－4　政府 ICT システムに係るセキュリティ対策標準等

サイバーセキュリティ対策標準として国際標準を反映した次の規範（Normative Instruction）が公式に定められている。

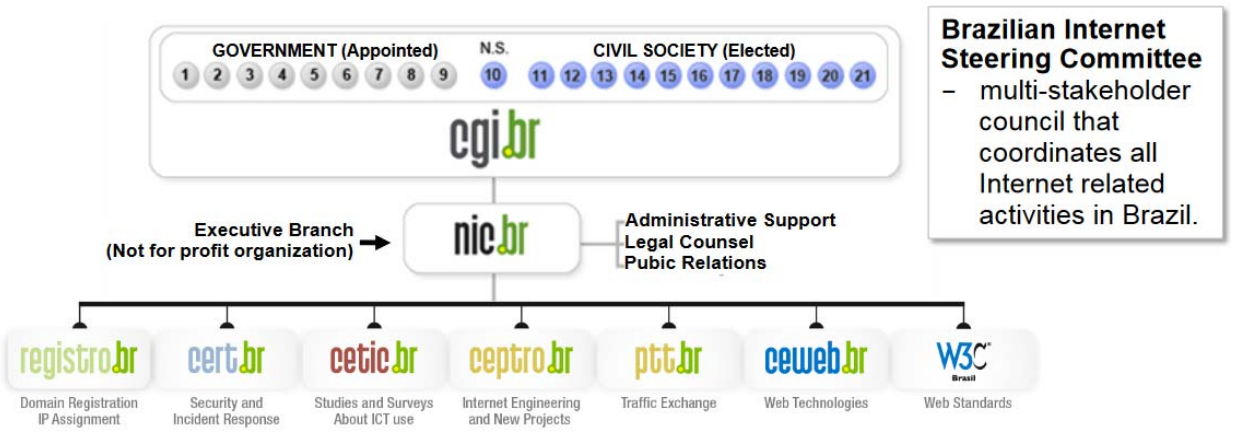
① Normative Instruction GSI no 1/2008
　連邦政府内における情報セキュリティマネジメント規範
② Normative Instruction GSI no 2/2008
　連邦政府実施機関における機密情報取り扱い規範
③ Normative Instruction GSI no 3/2008
　連邦政府実施機関における機密情報の暗号化アルゴリズムに関する規範

また、上記規範を補完するかたちで、連邦政府組織における専門家に対しては、次の資格およびトレーニングに係るガイドラインを定めている。

① Complementary Standard on. 17
　連邦政府組織における専門家を対象とした情報セキュリティ資格認定に係るガイドライン
② Complementary Standard on. 18
　直接的もしくは間接的に連邦政府事業に従事する専門家を対象とした情報セキュリティ関連トレーニングに係るガイドライン

## 5－5　主要 CSIRT：組織名、役割（業務内容）、体制図

ブラジルの National CSIRT は Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil（以下、CERT.br）である。防衛省や大統領府内閣セキュリティセンター情報セキュリティ通信部門とは直接の関係性がなく、CERT.br は Núcleo de Informação e Coordenação do Ponto BR（ブラジルネットワークインフォメーションセンター、以下、NIC.br）により運営管理されている。NIC.br は Comitê Gestor da Internet no Brasil（ブラジルインターネット管理委員会、以下、CGI.br）の傘下に位置づけられている。




[図　17　CGI.br が管轄する組織構成]
出典: CERT.br Team Update: New Awareness Materials[51]

[51] CERT.br Team Update: New Awareness Materials (https://www.cert.br/docs/palestras/certbr-natcsirts2017-2.pdf)

## 5－5－1　CGI.br

### 5－5－1－1　概要

CGI.br は、ブラジルにおけるすべてのインターネットサービスを一元的に調整・管理し、インターネットサービスの技術的品質向上、技術革新、普及促進等を担う委員会である。Ministério da Ciência e Tecnologia（旧通信科学技術省。現科学技術革新通信省）により Interministerial Ordinance No 147, of May 31st 1995 に基づき、1995 年 5 月に設立された。組織の役割は、2003 年に Presidential Decree No 4829, of September 3rd 2003 により改定されている。

CGI.br はインターネットに係る全ての取組みを所掌する委員会として、表 7 で示すとおり官民の代表者により構成されている。9 名は省庁など連邦政府から、残る 12 名は ISP や通信インフラ企業、NGO、学術機関といった市民組織から選出されている。科学技術革新通信省からの委員が全体の調整役を担っている。

[表 7　CGI.br の構成員]
出典: CERT.br Web サイトより作成

| 全体 | 分類 | 構成員 |
|---|---|---|
| CGI.br 構成員 | 政府組織（指定枠） 9 名 | ・ Ministry of Science and Technology (Coordination)　(1 名)<br>・ Presidential Cabinet (1 名)<br>・ Ministry of Communications (1 名)<br>・ Ministry of Defense (1 名)<br>・ Ministry of Development, Industry and Foreign Trade (1 名)<br>・ Ministry of Planning, Budget and Management (1 名)<br>・ National Telecommunications Agency (1 名)<br>・ National Council of Scientific and Technological Development (1 名)<br>・ National Forum of Estate Science and Technology Secretaries (1 名) |
| | 市民組織（選挙枠） 12 名 | ・ Internet Expert (1 名)<br>・ General Business Sector Users (1 名)<br>・ Internet Service Providers (1 名)<br>・ Telecommunication Infrastructure Providers (1 名)<br>・ Hardware and Software Industries (1 名)<br>・ Non-governmental Entity (4 名)<br>・ Academia (3 名) |

### 5－5－1－2　主な活動内容

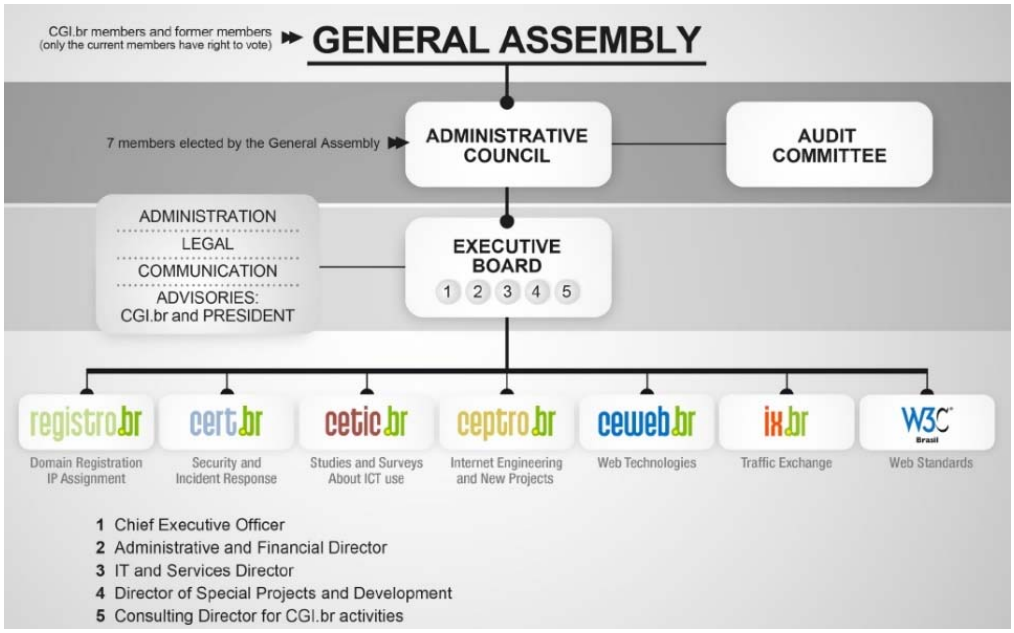
主な活動内容は次のとおりである。

① インターネットに係る政策、規制、技術標準等に関する提言
② インターネット利用に係る戦略・方針決定
③ ネットワークセキュリティに係る研究や技術標準化の促進
④ IP アドレスおよびドメイン名の割当管理
⑤ インターネットに係る各種統計等の情報収集および情報発信

## 5－5－2　NIC.br

### 5－5－2－1　概要

NIC.br は、CGI.br により意思決定されたプロジェクトを実施するための実施機関であり、ブラジル国内のインターネットサービスの調整・管理、技術的品質向上、技術革新、普及促進等を実際に行う非営利団体である。組織体としては、1999 年から活動を開始していたが、政府の承認を得た正式な設立は 2005 年である。CGI.br 同様 Interministerial Ordinance No 147, of May 31st 1995 が設立根拠法である。NIC.br のトップは 1995 年から今まで Internet Expert として CGI.br 委員に選出されている Demi Getschko 氏である。NIC.br の組織図を図 18 に示す。




[図 18　NIC.br の構成員]

出典: CERT.br: Evolution of the Scenario of Incidents in Brazil[52]

### 5－5－2－2　主な活動内容

主な活動内容は次のとおりである。

① REGISTRO.br（ネットワーク資源管理組織）によるドメイン名管理と IP アドレスの管理
② CERT.br によるサイバーセキュリティ分野の管理
③ IX.br（ネットワーク経路制御管理組織）によるインターネット相互接続点（Internet Exchange Point）やネットワーク経路制御番号（Autonomous System Number）の管理
④ その他組織を含めた下部組織の統括
⑤ ISP からのドメイン名登録管理料・使用料の徴収（ブラジルではインターネット黎明期にインターネット普及促進策として ISP 事業許認可が無料で取得できたその背景から、現在 5,000 以上の ISP が存在している）

[52] CERT.br: Evolution of the Scenario of Incidents in Brazil, p.5 (https://www.cert.br/docs/palestras/certbr-oas2018.pdf)

## 5－5－3　CERT.br

### 5－5－3－1　概要

CERT.br は、NIC.br の下で National CSIRT としてインシデントハンドリングから啓発活動や海外関連機関を含む連携強化まで、幅広い活動を行う。前身の NIC BR Security Office（以後、NBSO）が 1997 年 6 月に CGI.br により設立され、その後、2003 年 9 月に Presidential Decree No 4829（2003 年 9 月）に基づき CERT.br へ改組された。

### 5－5－3－2　主な活動内容

主な活動内容は次のとおりである。

① National CSIRT としてブラジル国内のインシデント統計情報の取りまとめ
② セキュリティ脅威とサイバー攻撃の動向に関する情報収集・分析および情報発信
③ サイバーセキュリティに関する国民の意識向上と対応能力の強化
④ 他機関との連携強化・促進
⑤ 新たな CSIRT 設立の支援

## 5－5－4　CTIR.gov

### 5－5－4－1　概要

CTIR.gov は、各行政組織に個別に設立された CSIRT 間の調整役として、政府組織内のコンピュータネットワークに係るインシデント対応、サイバー攻撃の動向の分析などを担う[53]。 2004 年末に活動を開始後、2006 年 5 月に Presidential Decree No. 5772 により大統領府内閣セキュリティセンター情報セキュリティ通信部門が設立されたことにともない、その下部組織 General Coordination for Incident Network（CGTIR）として設立された。その後、2009 年 11 月に Interministerial Ordinance No 56 によって CTIR.gov に改組された。

### 5－5－4－2　主な活動内容

主な活動内容は次のとおりである。

① インシデントの通知、分析、対応レポートを各政府機関に提供
② インシデント対応における関係者間の調整
③ サイバーセキュリティに関する注意喚起、統計情報を各政府機関に配布
④ サイバーセキュリティに関する啓発活動を各政府機関に実施
⑤ 他の CSIRT との連携

## 5－6　サイバーセキュリティ対策に係る連携体制

### 5－6－1　国内連携

CERT.br の前身である NBSO が 1997 年 6 月に設立された後、CSIRT（CAIS/RNP）が高等教育機関や研究機関の国立教育研究ネットワーク Brazilian Research Network（RNP）により、CERT-RS がリオグランデ・ド・スル州学術系ネットワークのために設立されたのに続き、1999 年には多くの大学や通信事業者等にも組織内に CSIRT を設立する動きが見られた。

[53] CTIR.gov: About CTIR Gov (https://www.ctir.gov.br/sobre-ctir-gov.html)

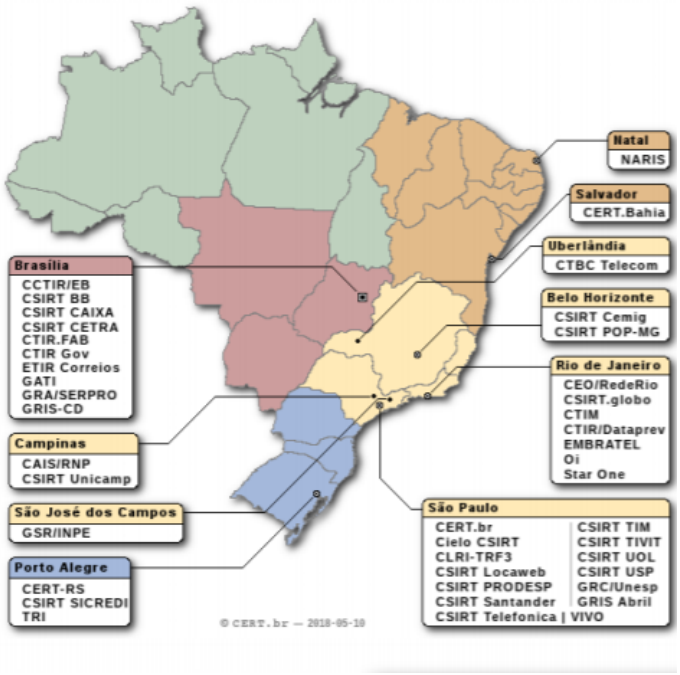
こうした背景から、2000 年に CERT.br は CSIRT 設立支援活動”CSIRT Development Program”を開始した。例えば、支援活動の一環として Carnegie Mellon University の Software Engineering Institute（SEI/CMU）認定コースである表 8 に示す 3 種類の技術トレーニングを CSIRT に対して提供している。

[表 8　CERT.br による技術トレーニングコース]
出典: CERT.br Web サイトより作成

| コース名 | 期間 | 費用 |
|---|---|---|
| Overview of Creating and Managing Computer Security Incident Response Teams (Overview)<br>（CSIRT の概要） | 1 日間 | R$ 1,100<br>（約 289 米ドル） |
| Fundamentals of Incident Handling (FIH)<br>（インシデントハンドリング基礎） | 5 日間 | R$ 2,800<br>（約 729 米ドル） |
| Advanced Incident Handling for Technical Staff (AIH)<br>（インシデントハンドリング上級） | 5 日間 | R$ 2,800<br>（約 729 米ドル） |

CERT.br による同支援活動の効果もあり、各省庁、陸軍、海軍、空軍、郵便局、通信事業者、クレジットカード業者、教育機関等にそれぞれの CSIRT が設立されており、2018 年 11 月時点でブラジル国内には、41 の CSIRT が存在する（公開情報に基づく数値。なお、業界単位のセクターCSIRT は存在していない）。

| Sector | CSIRTs |
|---|---|
| National - Any Brazilian Network | CERT.br |
| National – Federal Public Administration | CTIR Gov |
| Government | CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD |
| Energy | CSIRT Cemig |
| Financial | Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi |
| Telecom<br>ISP<br>Hosting | CSIRT Locaweb, CSIRT TIM, CSIRT TIVIT, CSIRT UOL, CSIRT Telefonica\|VIVO, CTBC Telecom, EMBRATEL, StarOne, Oi |
| Academia | CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI |
| Others | CSIRT.globo, GRIS Abril |

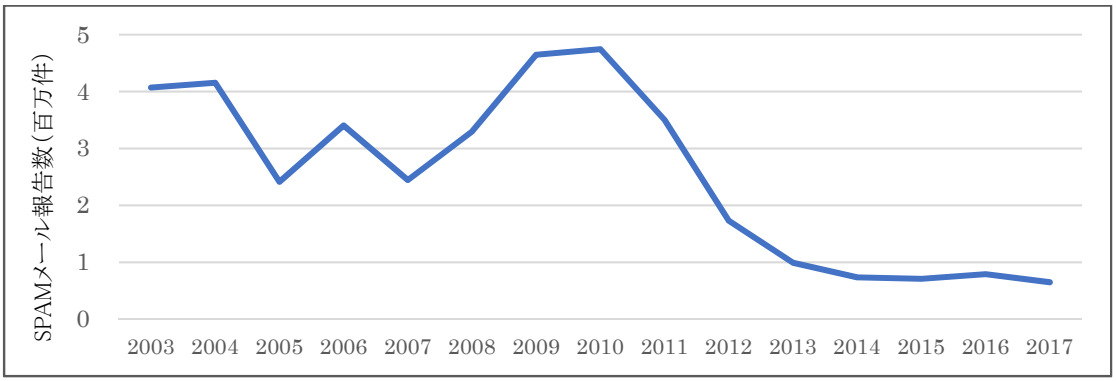



[図 19 ブラジル国内の各種 CSIRT]
出典: CERT.br: Evolution of the Scenario of Incidents in Brazil[54]

[54] CERT.br: Evolution of the Scenario of Incidents in Brazil, p 22 (https://www.cert.br/docs/palestras/certbr-oas2018.pdf)

CERT.br はこれら国内の CSIRT へ対する情報提供や技術支援を行っているほか、CSIRT 間の連携強化のための Brazilian CSIRT Forum（2012 年、2017 年、2018 年実施）という会議を開催する等、CSIRT 間の交流促進活動も積極的に実施している。また、CTIR.gov とは公式な合意文書は存在しないものの、定期的に連絡を取り合い密な連携を行っている。

国内連携における具体的成功事例としては、Spam メール対策があげられる。CERT.br、NIC.br、主要電話会社や主要 ISP が Spam メール低減を目的とした取り組みに関する公式な合意書を交わし、国内に対する Spam メール対策の必要性、改善効果や取り組み状況を周知した結果、2013 年以降 Spam メールに関する報告件数は大幅に減少した。




[図 20　ブラジルにおける Spam メール報告件数の減少状況]
出典: CERT.br: “Spams Reportados ao CERT.br por Ano[55]”より作成

## 5－6－2　中南米内連携

### 5－6－2－1　OAS、LACNIC による域内連携の取り組み

ブラジル国内には 27 ヶ所のインターネットエクスチェンジ(IX)があり、パラグアイやチリなどとの接続ポイントとして重要な位置を占めていることから、CERT.br は中南米域内での連携に積極的である。OAS や LACNIC 主催の定期会議へ参加し、ブラジルでの活動内容を共有している。例えば、LACNIC の定期会議では、新たな CSIRT 設立支援の知見を共有している。また、ブラジル国内の IP アドレス管理（IP allocation）を担っている NIC.br は LACNIC 設立（2002 年 10 月）よりも早く設立されたため、LACNIC 設立時に各種アドバイスを提供する立場でもあった。

### 5－6－2－2　その他中南米内での連携

ITU の Cybersecurity Index 2017 では、国際連携について十分な取組みが出来ていないと分析されているが、CERT.br はこれまでにウルグアイの CSIRT ANTEL（国営の通信事業者の CSIRT）やハイチの National CSIRT 等へ研修を提供している。より参加し易い交流の場づくりを試みるなど、OAS や LACNIC とは一線を画す形で、積極的に中南米内での連携促進に取り組んでいる。

また、2013 年 9 月 13 日、ブラジル国防省とアルゼンチン国防省がサイバーセキュリティ分野で提携（アルゼンチンからサイバーセキュリティの専門家をブラジルに派遣して、ブラジル CDCiber でサイバーセキュリティについて共同演習を行う）することを発表したとの報道があったように、国防省も他国との連携を図っている[56]。

[55] CERT.br: Estatísticas de Notificações de Spam Reportadas ao CERT.br (https://www.cert.br/stats/spam/)
[56] 情報通信総合研究所: ブラジルとアルゼンチン：サイバーセキュリティをめぐる協力 (http://www.icr.co.jp/newsletter/global_perspective/2013/Gpre2013112.html)

## 5－6－3　その他海外との連携

### 5－6－3－1　CERT.br による国際的枠組みへの参加

国際的枠組みへの参加状況は次のとおりである。

① FIRST フルメンバー
② Honey Research Alliance メンバー
③ Anti-Phishing Working Group Research Partner
④ APWG Research Partner
⑤ SEI Partner

### 5－6－3－2　サイバー犯罪に関する条約

ブラジルは、「サイバー犯罪に関する条約[57]」には署名していない[58]。

### 5－6－3－3　その他プロジェクトを通じた連携

Task Force on Spam（CT-Spam）という取組みでは、CGI.br による国内 Spam メール対策イニシアチブの指揮をとった一方、対外的な取り組みとして CERT.br が AusCERT（オーストラリア）および GOVCERT.NL（オランダ）と技術情報共有を実施した。また、CERT.br が主導する SpamPots というプロジェクトでは、CSIRT UNLP（アルゼンチン）、AusCERT（オーストラリア）、CERT.at（オーストリア）、CSIRT USP（ブラジル）、CLCERT（チリ）、CSIRT CIA（オランダ）、Cadia（オランダ）、Shadowserver Foundation（アメリカ）、TWCERT/CC（台湾）、CSIRT ANTEL（ウルグアイ）など世界 12 か国にセンサーを展開しており、各国から Spam メールを収集し分析している[59]。

## 5－7　サイバーセキュリティに係る啓発活動、人材育成活動

### 5－7－1　CGI.br および NIC.br による活動

ブラジルにおけるサイバーセキュリティに関する人々のリテラシーは高いとは言えない。このため、CGI.br および NIC.br がり会報や報告書の公開、啓発キャンペーン活動等に力を入れている[60]。

① 一般人や企業、団体を対象とした活動

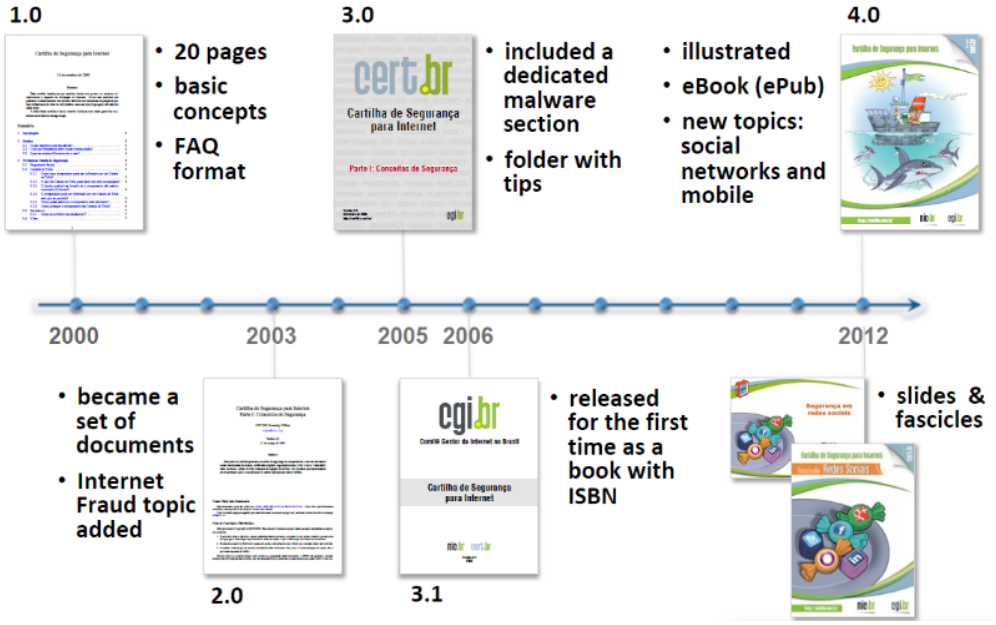
一般向けの啓発活動として、フェイクニュース、SNS 利用、インターネットバンキング等に関する注意喚起を目的に、学校向け（教師、生徒、保護者）の啓発用教材・資料を作成し配布している。また、ブラジルは国土が広いため、地方を対象とした活動については、地方の NGO 等とのパートナーシップに基づいて活動している。サイバーセキュリティに係る啓発活動に関心があるが、資料や教材を持っていない NGO や市民団体が多く、CERT.br が作成した資料が有効活用されている。加えて、コンピュータ教育を行う教師向けの研修教材を地方自治体と連携のもと作成したり、政府機関からの依頼に基づき用途に合った啓発資料を作成している。CERT.br がこれまでに作成してきた資料を図 21 に示す。

[57] 欧州評議会が 2001 年に発案した、個人情報保護とオンラインでの児童ポルノや著作権侵害を含むサイバー犯罪に関する対応を取り決める国際条約

[58] NISC（内閣サイバーセキュリティセンター）：サイバー空間に対する諸外国の施策動向調査 (https://www.nisc.go.jp/inquiry/pdf/shisakudoko_honbun.pdf)

[59] CERT.br: SpamPots Project (https://honeytarg.cert.br/spampots/)

[60] OAS: 2016 Cybersecurity Report (https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf)




[図 21　CERT.br の啓発活動教材]
出典: CERT.br: Evolution of the Scenario of Incidents in Brazil[61]

また、昨今の取組み例として、宅内設置ルータ等（以下、CPE）を調達する際の調達ガイドラインの作成がある。小規模な企業等は安価な CPE を購入する傾向があるが、安価な CPE にはソフトウエアのパッチ提供やアップデートがなされないケースが多い。製造・販売元も安価なパーツを組み立てて製品として販売しているだけで、各パーツの中身について理解が不十分なケースが多い。このため、The Messaging, Malware and Mobile Anti-Abuse Working Group（M3AAWG）や Latin American and Caribbean Anti-Abuse Working Group（LAC-AAWG）というプロジェクトと協力し、小規模企業向けに CPE を調達する際の調達ガイドラインを提供する等、認知向上に向けた活動を行っている。

② 専門家を対象とした活動

専門家向けの教育活動としては、技術情報の提供やトレーニング実施を含めた活動を行っており、これまで 800 名以上のセキュリティ専門家に対し、安全意識や対応能力向上に向けたトレーニングを行っている。また、ワールドカップやオリンピック等のイベント関係者に対する教育等も行っている。技術情報の提供事例としては、ネットワーク事業者向けの Web サイト（Best Current Practices Portal）があげられる。同 Web サイトでは、BGP ルーティング、アンチスプーフィング、CPE の管理、DDoS の抑制について事例や対応方法を紹介している。

[61] CERT.br: Evolution of the Scenario of Incidents in Brazil, p. 28 (https://www.cert.br/docs/palestras/certbr-oas2018.pdf)


[図 22　Best Current Practices Portal]
出典: NIC.br: Best Current Practices Portal[62]

③　ISP を対象とした活動

ISP 向けには、より専門的な情報提供を行っており、ハニーポットや Spam ポットを活用して把握したサイバー攻撃動向等を提供している（例えば、Telnet, SSH, RDP 等のポートに対するパスワード辞書攻撃、IoT ボットネットによる攻撃が増加しているといった観測・分析結果など）。また、CERT.br は外部から入手したスキャンデータ等を基に、DDoS 攻撃の踏み台となる脆弱な機器やサービスについての統計情報を定期的に収集する内部システムを保有している。Shadowserver Foundation（非営利のセキュリティ団体）や Team Cymru（非営利企業）などから、脆弱な DNS、SNMP、NTP サーバの数や、AS 番号と IP アドレス情報を入手し、CERT.br 側で分析を行い各 AS 管理業者に通知をしている。

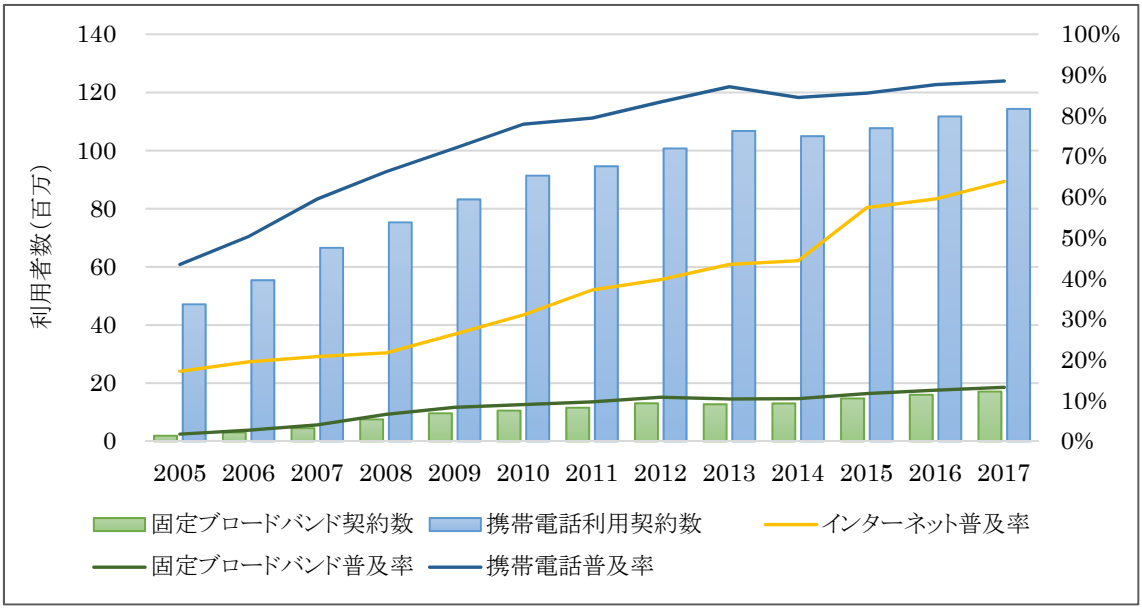
[62] NIC.br: Best Current Practices Portal (https://bcp.nic.br/)

# 第6章　各国におけるセキュリティ脅威の現状

## 6－1　メキシコにおけるセキュリティ脅威に係る日本との比較

### 6－1－1　インターネット利用者の増加状況

インターネット利用者は年々増加しており 2017 年時点でブロードバンド利用契約数は約 1,713 万件（メキシコ総人口の約 13%）および、携帯電話利用契約数は約 1 億 1,432 万件（メキシコ総人口の約 89%）、国内のインターネット利用者割合は約 64%である。（図 23）




[図 23　メキシコにおけるインターネット利用環境の推移]
出典: ITU Country ICT Data[63]より作成

### 6－1－2　サイバーセキュリティ被害の概況

メキシコ経済に影響を及ぼしたサイバーセキュリティ被害規模が 2016 年には 30 億米ドルを超えたとされており、メキシコの企業経営者のうち約 58%がサイバーセキュリティ対策に不安を持っているとの調査結果がある[64]。

### 6－1－3　IPA セキュリティ 10 大脅威との比較

日本でのサイバーセキュリティに係る脅威を把握する一つの指標として、IPA が毎年「情報セキュリティ 10 大脅威」を取りまとめている。

[63] ITU: Country Data (https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)

[64] PROMEXICO: Cybersecurity Market Analysis (http://mim.promexico.gob.mx/work/models/mim/Resource/154/1/images/diagnostico-ciberseguridad.pdf)

■「情報セキュリティ10大脅威 2018」

| 昨年順位 | 個人 | 順位 | 組織 | 昨年順位 |
|---|---|---|---|---|
| 1位 | インターネットバンキングやクレジットカード情報等の不正利用 | 1位 | 標的型攻撃による被害 | 1位 |
| 2位 | ランサムウェアによる被害 | 2位 | ランサムウェアによる被害 | 2位 |
| 7位 | ネット上の誹謗・中傷 | 3位 | ビジネスメール詐欺による被害 | ランク外 |
| 3位 | スマートフォンやスマートフォンアプリを狙った攻撃 | 4位 | 脆弱性対策情報の公開に伴う悪用増加 | ランク外 |
| 4位 | ウェブサービスへの不正ログイン | 5位 | 脅威に対応するためのセキュリティ人材の不足 | ランク外 |
| 6位 | ウェブサービスからの個人情報の窃取 | 6位 | ウェブサービスからの個人情報の窃取 | 3位 |
| 8位 | 情報モラル欠如に伴う犯罪の低年齢化 | 7位 | IoT機器の脆弱性の顕在化 | 8位 |
| 5位 | ワンクリック請求等の不当請求 | 8位 | 内部不正による情報漏えい | 5位 |
| 10位 | IoT機器の不適切な管理 | 9位 | サービス妨害攻撃によるサービスの停止 | 4位 |
| ランク外 | 偽警告によるインターネット詐欺 | 10位 | 犯罪のビジネス化（アンダーグラウンドサービス） | 9位 |

[図 24　IPA「情報セキュリティ 10 大脅威 2018 年」]
出典: IPA（独立行政法人情報処理推進機構）:情報セキュリティ 10 大脅威 2018[65]

メキシコのサイバーセキュリティに係る課題を整理するために、図 24 に示した IPA「情報セキュリティ 10 大脅威（組織向け）」と比較し、その現状およびメキシコに特有な事象について、表 9 のように整理した。

なお、情報セキュリティ 10 大脅威のうち、「8 位　内部不正による情報漏えい」については対象外とした。

[65] IPA（独立行政法人情報処理推進機構）:情報セキュリティ 10 大脅威 2018
(https://www.ipa.go.jp/security/vuln/10threats2018.html)

[表 9　メキシコにおける情報セキュリティ 10 大脅威との対比状況]
（IPA「情報セキュリティ 10 大脅威 2018 年」のランキングに、JPCERT/CC 調査内容を追加）

| 順位 | 「組織向け」10 大脅威 | メキシコの状況 |
|---|---|---|
| 1 | 標的型攻撃による被害 | • メキシコにおいても標的型攻撃が発生しており金融機関に対する被害が目立っている。事例として 2018 年 1 月にメキシコ外国貿易銀行で約 1 億 1,000 万米ドル（未遂との報道がある）[66]や 2018 年 5 月にメキシコ中央銀行の送金システムから 5 つの銀行を経由して約 1,500 万米ドルの不正送金被害[67]があった。金融機関独自のルールを設けることが重要と CERT-MX は考えている。 |
| 2 | ランサムウエアによる被害 | • ESET の報告書[68]によると、中南米域内でペルーに次ぐ被害件数（全体の 20%）であり、SCITUM-CERT でも流行している攻撃手口として懸念の声があった。 |
| 3 | ビジネスメール詐欺による被害 | • 件数は多くない様である。一方で CEO や CFO のメールアドレスとおぼしきアドレスからのフィッシングメール被害を SCITUM-CERT では確認している。また、CERT-MX は深刻なセキュリティ脅威の 1 位にフィッシング詐欺を挙げている。 |
| 4 | 脆弱性対策情報の公開に伴う悪用増加 | • 各 CSIRT 機関への訪問時には事例紹介がなかったが、NICT のレポート[69]によれば、2018 年 5 月に脆弱性の公開からわずか 1 週間後にそれを悪用した攻撃が観測されているが、攻撃元となったホストの一部にはメキシコのものも含まれていたことが分かっている。 |
| 5 | 脅威に対応するためのセキュリティ人材の不足 | • サイバーセキュリティネットワークや運用業務に関連する求人を満たすために、約 15 万人のトレーニングを受けた専門家が不足しているとされている[70]。<br>• UNAM-CERT では奨学金付きで受け入れたインターンが修了後に定着しない事も課題と認識していた。 |
| 6 | ウエブサービスからの個人情報の窃取 | • MNEMO CERT によるとユーザ名、パスワードやクレジットカード情報といった個人情報を詐取するためのフィッシングサイトが存在し、毎月 11%の割合で増加傾向にあると報告[71]されている。 |
| 7 | IoT 機器の脆弱性の顕在化 | • CERT-MX へのインタビューでは 2～3 年後の課題として IoT のセキュリティ対策を考えていた。<br>• CPE を中心として IoT 向けマルウエアの被害が深刻化している。IoT 機器向けマルウエア「Mirai」の亜種を利用したネットワークスキャンの発信源がメキシコであることをトレンドマイクロが確認しており[72]、感染機器の多くは SIP ポートが開いた家庭用ルータやネットワークカメラであった。 |

66 Fire Eye: APT38 Un-usual Suspects (https://content.fireeye.com/apt/rpt-apt38)

67 Bloomberg: Mexico Says Possible Bank Hack Led to Large Cash Withdrawals (https://www.bloomberg.com/news/articles/2018-05-13/mexico-says-possible-bank-hack-led-to-large-cash-withdrawals)

68 ESET: SECURITY REPORT Latinoamérica 2018 (https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf)

69 NICT（国立研究開発法人情報通信研究機構）: NICTER 観測レポート 2018 (https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf)

70 PROMEXICO: Cybersecurity Market Analysis (http://mim.promexico.gob.mx/work/models/mim/Resource/154/1/images/diagnostico-ciberseguridad.pdf)

71 MNEMO-CERT: Así puedes reducir el riesgo de robo de identidad (https://cert.mnemo.com/reducir-riesgo-robo-de-identidad/)

72 TrendMicro: 家庭用 GPON ルータの脆弱性を狙う「Mirai」の亜種、メキシコ発のネットワークスキャン活動で確認 (https://blog.trendmicro.co.jp/archives/17453)

| | | |
|---|---|---|
| | | ・ Mirai ボットネットのインフラを利用して仮想通貨のマイニングを行うキャンペーン（CryptoMirai と命名）を SCITUM-CERT がメキシコ国内で確認し注意を促している[73]。 |
| 8 | 内部不正による情報漏えい | 本調査では調査対象外とした。 |
| 9 | サービス妨害攻撃によるサービスの停止 | ・ 選挙期間中に野党の選挙公式サイトが DoS で一時停止する被害 が多くみられたとロイター通信が報じた[74]。。 |
| 10 | 犯罪のビジネス化（アンダーグラウンドサービス） | ・ ダークウエブで偽造カード読取機が販売されており、こうした不正ツールの拡散が懸念されている。また、CERT-MX は深刻なセキュリティ脅威の第 2 位にソーシャルメディア利用における課題を挙げており、SNS 上で売春の仲介や児童ポルノの売買が行われている。メキシコ国内の CSIRT は Facebook、Google、Twitter、Mega（オンラインストレージサービス事業者）等の企業、INTERPOL や EUROPOL 等と連携して対処している。<br>・ ダークウエブを通じて違法薬物が売買されており、国家安全保安委員会が取り締まっている[75]。 |

一方、上記の 10 大脅威に合致しない脅威として、個人情報の詐取、政治的ハッキング活動、ATM を利用したサイバーセキュリティ被害がある。

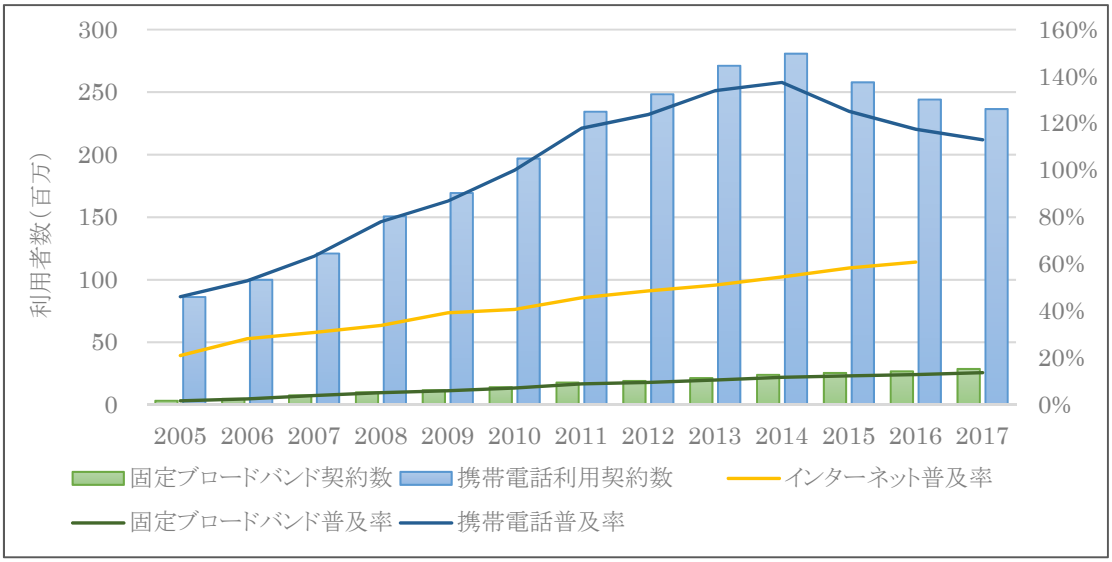
① 個人情報の詐取
ラテンアメリカ地域を起源とするマルウエア Dark Tequila[76]により、メキシコ国内のユーザが標的となって銀行の認証情報、個人情報や企業データが窃取されたケースがある。
② 政治的ハッキング活動
メキシコの Hacktivism（政治的ハッキング活動）では銀行の内部情報データベースから情報を盗むといった金融機関に対する活動が一例として確認されている。SCITUM-CERT では重要インフラに関する攻撃に発展する事を懸念している。
③ ATM を利用したサイバーセキュリティ被害
スペイン語圏が発祥とされている ATM を狙ったマルウエアが発見されている。また、亜種も確認されている。

## 6－2　ブラジルにおけるセキュリティ脅威に係る日本との比較

### 6－2－1　インターネット利用者の増加状況

インターネット利用者は年々増加しており 2017 年時点でブロードバンド利用契約数は約 2,867 万件（ブラジル総人口の約 14%）および、携帯電話利用契約数は約 2 億 3,649 万件（ブラジル総人口の約 113%）、国内のインターネット利用者割合は約 61%（2016 年時点）である。（図 25）

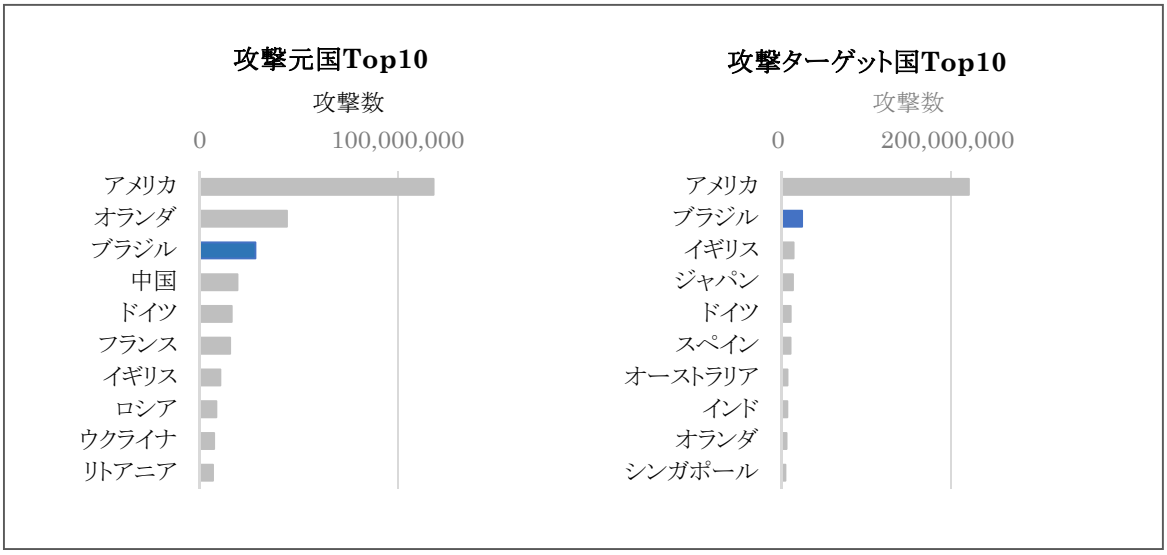
[73] SCIBLOG: Ataques asociados a criptomonedas en México (https://blog.scilabs.mx/ataques-asociados-a-criptomonedas-y-cryptomirai-en-mexico/)
[74] REUTERS: Cyber attack on Mexico campaign site triggers election nerves (https://www.reuters.com/article/us-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerves-idUSKBN1J93BU)
[75] Cronica.com: Hasta 15 tipos de drogas sintéticas se venden en México vía internet (http://www.cronica.com.mx/notas/2018/1083777.html)
[76] Kaspersky Lab: Kaspersky Lab、複雑な銀行系マルウェア「Dark Tequila」が 2013 年からメキシコを標的に活動していることを明らかに (https://www.kaspersky.co.jp/about/press-releases/2018_vir28082018)




[図 25　ブラジルにおけるインターネット利用環境の推移]
出典: ITU Country ICT Data[77]より作成

## 6－2－2　サイバーセキュリティ被害の概況

インターネットの普及にともないセキュリティ脅威も増加しており、アカマイ・テクノロジーズ（アメリカの CDN、クラウドセキュリティ企業）の報告書「インターネットの現状 / セキュリティ」（2017 年第 1 四半期）[78]によると、図 26 に示すとおりブラジルは世界のサイバー攻撃の標的となった国のランキングでアメリカに次ぐ 2 位、サイバー攻撃の発信元となった国としては 3 位となっている。




[図 26　サイバー攻撃元・ターゲット国]
出典: Akamai ［インターネットの現状］／セキュリティ（2017 年第 1 四半期）[78] より作成

[77] ITU: Country Data (https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)
[78] Akamai: akamai's [state of the internet] / security Q1 2017 report (https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf)

### 6－2－3　IPA セキュリティ 10 大脅威との比較

ブラジルのサイバーセキュリティに係る課題をするため、IPA による情報セキュリティ 10 大脅威（組織向け）と比較し、ブラジルの現状およびブラジルに特有な事象について、表 10 のとおり整理した。

なお、情報セキュリティ 10 大脅威のうち、「8 位　内部不正による情報漏えい」については、本調査では対象外とした。

[表 10　ブラジルにおける情報セキュリティ 10 大脅威との対比状況]
（IPA「情報セキュリティ 10 大脅威 2018 年」のランキングに、JPCERT/CC 調査内容を追加）

| 順位 | 「組織向け」10 大脅威 | ブラジルの状況 |
|---|---|---|
| 1 | 標的型攻撃による被害 | ・ 実際に、CERT.br に対してブラジル国内での深刻なセキュリティ脅威の上位 3 つについて質問したところ、第 2 位として金融機関をターゲットとする標的型攻撃があげられた。RAT、フィッシング、DNS スプーフィング等の複数手法で金融機関への攻撃が行われている。 |
| 2 | ランサムウエアによる被害 | ・ CERT.br に対してブラジル国内での深刻なセキュリティ脅威について質問したところ、DoS 攻撃、オンラインバンキングを悪用した詐欺被害、脆弱な IoT 機器に次ぐ第 4 位の脅威としてランサムウエアによる被害があげられた。特に小規模な企業や組織ではデータのバックアップを定期的に取っていない場合が多く、より深刻な脅威と捉えられている。 |
| 3 | ビジネスメール詐欺による被害 | ・ トレンドマイクロによれば、ブラジルは中南米で最大の Spam メール送信国であり、中南米の国が送信元となる Spam メールのうち、約 38%はブラジルから送信されていると分析されている[79]。 |
| 4 | 脆弱性対策情報の公開に伴う悪用増加 | ・ CERT.br へのインタビューでは何も言及がなかったが、脆弱性対策情報の公開に伴う攻撃が報道されている。例えば、NICT のレポート[80]によれば、ウエブサーバに存在する脆弱性を悪用するブラジルを起点とした攻撃が 2018 年 5 月に観測されているが、この動向が見られるようになったのは当該脆弱性が公開されてからわずか 1 週間後だったことが分かっている。<br>・ LACNIC のデータによると、ブラジルにおける 2017 年時点でのネットワークトラフィック内の不正行為割合としては、53.16%が調査目的としたポートスキャン（22/TCP, 25/TCP, 23/TCP が上位）であり、標的型攻撃の準備行為も含まれると考えられる。 |
| 5 | 脅威に対応するためのセキュリティ人材の不足 | ・ セキュリティ人材の不足はブラジルにおいても課題とされており、「5－7 サイバーセキュリティに係る啓発活動、人材育成活動」で説明したとおり、CERT.br も人材育成に係る活動に注力している（CSIRT 設立支援や専門家へのトレーニング提供等）。 |
| 6 | ウエブサービスからの個人情報の窃取 | ・ 仮想通貨投資サイト Atlas がハッキングされ、26 万件の個人口座残高、メールアドレス、電話番号等の情報が漏洩したとの報道がある[81]。 |
| 7 | IoT 機器の脆弱性の顕在化 | ・ CERT.br に対してブラジル国内での深刻なセキュリティ脅威の上位 3 つについて質問したところ、第 3 位に IoT 機器の脆弱性があげられた。Mirai などのマルウエアに監視カメラや CPE（上述のとおりセキュリティの穴となっていることが多い）といった IoT 機器が感 |

[79] TrendMicro: ブラジルが直面するサイバー犯罪の現状：従来型不正プログラム、スパムメール攻撃、アンダーグラウンド市場の急成長 (https://blog.trendmicro.co.jp/archives/7762)

[80] NICT: NICTER 観測レポート 2018 (https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf)

[81] COINTELEGRAPH: Brazilian Crypto Platform Atlas Quantum Reveals Data Breach Affecting 260K Customers (https://cointelegraph.com/news/brazilian-crypto-platform-atlas-quantum-reveals-data-breach-affecting-260k-customers)

| | | |
|---|---|---|
| | | 染することが懸念されている。ブラジルには 2014 年のワールドカップや 2016 年のオリンピック開催にあわせて多くの監視カメラが設置された背景もある。<br>・ また、横浜国立大学と BB ソフトサービス株式会社（BBSS）による共同研究「横浜国立大学・BBSS IoT サイバーセキュリティ 共同研究プロジェクト」（ハニーポットによるサイバー攻撃の観測システムを用い 192 カ国からの攻撃を観測するもの。実施期間：2017 年 6 月～2017 年 12 月）の結果によると、ブラジルは常に攻撃元の上位に入っている。<br>・ さらに、Mirai に感染の要因となる「ポート番号 23 または 2323 で telnet が動作している」、「ユーザ名、パスワードが初期値のまま動作している」という条件に該当する IoT 機器の数を調査した Flashpoint 社の調査報告[82]によると、該当する機器の多さで、ブラジルは第 2 位となっている（第 1 位はベトナム、第 3 位はトルコ）。<br>・ 2018 年に MikroTik 社のルータの脆弱性を狙ったゼロデイ攻撃によりブラジル国内で 200,000 台以上のルータがマイニングウイルス CoinHive に感染したと複数メディアで報道されている[83]。 |
| 8 | 内部不正による情報漏えい | 本調査では調査対象外とした。 |
| 9 | サービス妨害攻撃によるサービスの停止 | ・ CERT.br に対してブラジル国内での深刻なセキュリティ脅威の上位 3 つについて質問したところ、DDoS 攻撃が第 1 位にあげられた。小規模な企業や組織は対応が困難であることから、小規模な企業や組織にとって深刻な脅威と捉えられている。<br>・ また、ブラジルにおける 2017 年時点での不正なネットワークトラフィックの 26.41%が DoS/DDoS（IoT ボットネット型、DNS アンプ攻撃型が上位）攻撃パケットとなっている。<br>・ さらに、トレンドマイクロの報告書によれば、中南米における不正な URL の過半数（58%）はブラジル国内で提供されており、ブラジルが C&C サーバと大規模な情報収集型ボットネットの運用に関与する感染 PC の主な供給源であると分析されている[84]。 |
| 10 | 犯罪のビジネス化（アンダーグラウンドサービス） | ・ ブラジルにおけるサイバー犯罪の増加は、アンダーグラウンド市場の繁栄が一因になっている。トレンドマイクロの調査[85]によれば、Crime-as-a-Service と呼ばれる販売モデルで、誰もがサイバー攻撃のツール（ランサムウエアや改変版 Android アプリ等）を容易に入手できる。さらにツールの提供のみならず、サイバー犯罪を行うためのマルウエア開発やボットネット管理、クレジットカード情報盗難等のノウハウを教える有償トレーレングまで提供されている。<br>・ 例えば、アンチウイルスソフトを回避するため方法を含むマルウエアプログラミング技術について、200 レアル（約 51.16 米ドル）程度で、Skype によるオンラインサポート付きのトレーニングを受講できる。さらに、このようなツールの販売が、ダークウエブ上のみ |

[82] IPA （独立行政法人情報処理推進機構）:IoT とサイバーセキュリティ (https://www.ipsj.or.jp/topics/9faeag000000s7ly-att/20170602_tomita.pdf)

[83] TrendMicro: Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign (https://www.trendmicro.com/vinfo/vn/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign)

[84] TrendMicro:ブラジルが直面するサイバー犯罪の現状：従来型不正プログラム、スパムメール攻撃、アンダーグラウンド市場の急成長 (https://blog.trendmicro.co.jp/archives/7762)

[85] TrendMicro: Ascending the Ranks The Brazilian Cybercriminal Underground in 2015 (https://documents.trendmicro.com/assets/wp/wp-ascending-the-ranks.pdf)

| | | |
|---|---|---|
| | | ででなく、一般的な SNS サイトでもされる[86]といったサイバー犯罪者向け市場の一般化が最近では進んでいる。<br>・ トレンドマイクロが確認した事例では、「必要な機能を全て備えたオンライン銀行詐欺ツール」および「必要な C&C サーバとのネットワーク」といったサービスがレンタルで提供されている。また、YouTube チャンネルには、「銀行詐欺ツールのレンタル、またはソースコードの販売をいたします。9 つ以上の銀行に対応可能。バージョン 2016」などという宣伝文が記載されたケースも報告されている。 |

## 6－3　今後の連携可能性

メキシコにおいては、ATM 本体へ CD-ROM や USB ドライブを挿入しマルウエアを物理的に感染させる攻撃や、ブラジルにおいては、アンダーグラウンドサービスの拡大に伴うサイバー犯罪の一般化等、日本とは異なる様相の脅威も存在する。

その一方で、前述したように、日本におけるセキュリティ脅威と類似した課題をメキシコやブラジルも抱えていることがわかる。実際にメキシコの CERT-MX およびブラジルの CERT.br へ「最も深刻なセキュリティ脅威の上位 3 つをあげるとすれば何か？」と質問したところ、表 11 に示した回答を得ており、必ずしもメキシコ、ブラジルに特有のセキュリティ脅威がそれぞれの国内で目立っているわけではない。

[表 11　各国 National CSIRT に聞いた深刻なセキュリティ脅威トップ 3]
（インタビュー結果を基に作成）

| CERT-MX からの回答 | CERT.br からの回答 |
|---|---|
| **1.** フィッシング詐欺<br>**2.** ソーシャルメディア利用に関連する課題<br>**3.** 重要インフラに対する攻撃 | **1.** DDoS 攻撃<br>**2.** オンラインバンキングを悪用した詐欺被害<br>**3.** IoT 機器の脆弱性を狙った攻撃 |

また、各国とも National CSIRT が中心となりセキュリティ脅威に関する情報提供や、サイバーセキュリティ対応能力の向上、幅広い層への啓発活動、さらに国際的な連携の強化に取り組んでいる。メキシコの CERT-MX は警察組織の中に位置づけられ、他国の National CSIRT とは異なる権限を持つ点が特徴的である。その特色を活かし、国内 CSIRT との連携強化にイニシアチブを発揮している。

一方、ブラジルの CERT.br はインターネットの一般利用が始まった初期の段階から活動しており（1997 年に活動開始。なお、日本の JPCERT/CC の設立は 1996 年である）、国内のみならず中南米の域内連携の促進にも意識が高い。

冒頭第 1 章で述べたとおり、本調査の目的は今後のより密な関係構築および連携強化を図るために、各国 CSIRT の組織概要を把握することであったが、本調査の結果、日本とも類似するセキュリティ脅威を抱え、且つ、National CSIRT が積極的に活動しているメキシコ、ブラジルについては、今後の有益な連携可能性があると考えられる。

[86] THE ZERO/ONE:「サイバー犯罪大国」ブラジルの最新動向 (https://the01.jp/p0001819/)

# 第7章　まとめ

今回現地調査対象としたメキシコやブラジルの CSIRT には、組織の設立背景や活動内容に特色が見られた。例えば、現在活動する National CSIRT の多くは、政府内の情報通信系の省庁や、あるいは大統領・首相府直下のサイバーセキュリティ専門省庁の内部に設置されている。メキシコの CERT-MX のように警察の一部署として活動している組織は、世界でも珍しいと言える。犯罪捜査の一環としてサイバーセキュリティインシデント対応を行っているため、CSIRT 職員が犯人捜査や証拠の差押え、被疑者逮捕の権限を持っている点などを踏まえると、あくまで中立的なコーディネーションセンターとしての立場から技術的なサポートを行っている JPCERT/CC とはインシデントに対する意識やアプローチが大きく異なる。

また一方で、ブラジルでは 1990 年代前半から CSIRT の必要性が認識されていた。CERT.br は中南米地域だけでなく世界規模で見ても最も早く活動を開始した CSIRT の一つに数えられる。政情不安や経済危機などを抱える国が少なくない中南米地域では、政府内に CSIRT を設置したり、安定的に活動することが難しい国もあると推測されるが、そんな中でも LACNIC や OAS といったコミュニティを通して長年の CSIRT 運用の知見や技術を他国に対して提供しているブラジルのリーダーシップは、地域全体のサイバーセキュリティ分野での発展には必要不可欠である。

地域内での連携という観点で考えるとき、アジアやヨーロッパと比較して挙げられるのが使用されている言語の共通性が高い点である。中南米地域では、歴史的な背景から多くの国でスペイン語が公用語（の一つ）とされているため、他国間であっても比較的容易にコミュニケーションができる。言語の壁が低いため、LACNIC や OAS を通じた地域間連携も比較的活発に行われている模様だ。また、インシデント対応の観点では、ばらまき型メールなど言語を共有するがゆえに地域全域に蔓延してしまう脅威があるが、地域の CSIRT コミュニティがより密に情報連携をすることにより、そういった脅威に対しても効果的な対策を講じられるものと期待できる。

インタビューの中でメキシコ・ブラジルの CSIRT 担当者から聞いた、彼らが直面しているサイバー脅威を日本で確認されているものと比較したところ、地域特有の攻撃キャンペーンなどもいくつか見られたが、全体を通して言えばフィッシングや DDoS 攻撃など、日本でも継続的にみられる脅威と共通するものが多かった。日本で観測されているこうした攻撃の発信元が中南米地域の国の場合もあり、逆もまたしかりである。今回の現地調査で深めた信頼関係をもとに、さらなるインシデント対応の円滑化・効率化のため、中南米地域の各 CSIRT と連携を強化していくことが重要となる。