携を推進してきた。グループ内の多様な事業や地域を横断する協力体制を築くにあたり、リスクベースマネジメントの考え方と共通言語となるフレームワーク（NIST Cybersecurity Framework）を導入。フレームワークの6つの機能、「統治」「特定」「防御」「検知」「対応」「復旧」の観点から、グループ全体でセキュリティの強化を進めている。また、NTTは米国国立標準技術研究所（NIST）に対し、コメント提出、ワークショップ参加、プラクティスやユースケースの共有を行うなどフレームワークの策定やアップデートに貢献している。NTTも会員となっている産業横断サイバーセキュリティ人材育成検討会の取り組みはNISTのウェブサイトにサクセスストーリーとして評価、掲載された。

世界各国の政府機関や産業界とも協力し、サイバーセキュリティの強化に向けた情報共有やコミュニティ形成、さらにはサイバー犯罪対策にも積極的に貢献している。米欧を中心に、各国政府や産業界と連携し、セキュリティ脅威情報やベストプラクティスの共有を進めるとともに、サイバー犯罪の無力化に向けた取り組みも推進してきた。欧州ではEC3（欧州サイバー犯罪対策センター）、米国ではNCFTA（全米サイバー犯罪科学訓練同盟）、日本ではJC3（日本サイバー犯罪対策センター）と協力し、脅威の特定から対応に至るまで、グローバルな視点での対策強化を進めている。

**米国との連携**

特に米国においては、2023年1月、NTTがアジア企業として初めて、米国政府の官民サイバーセキュリティイニシアティブ「共同サイバー防衛連携（JCDC）」のメンバーに正式加入した。JCDCは、2021年に米国サイバーセキュリティ・インフラセキュリティ庁（CISA）によって設立された官民合同の枠組みであり、サイバー防衛計画の策定、セキュリティ情報の融合、重要インフラ及び国家重要機能へのリスク低減を目的としている。

JCDCには、AT&T、Verizon、Lumen、Microsoft、Google、Cisco、Mandiant、Palo Alto Networksなどの大手通信企業やメガテック企業、主要セキュリティ企業が名を連ねるほか、米国政府のインテリジェンス関連省庁や、米国の友好国のサイバーセキュリティ関連機関も参加。NTTは、JCDCと連携することで得られるグローバルな専門知識とリソースを活用し、重要な情報ネットワークの保護やサイバーインシデント対応をより効果的に実施するとともに、JCDCメンバーとの情報共有を通じ、サイバーセキュリティの更なる強化を図っている。

NTTの島田明社長は当時、JCDCへの参加について、「これまでのCISA及び米国政府との協力・信頼関係をもとに、新たにJCDCに参加し、アジアからのユニークな視点を提供するとともに、NTTのリーダーシップ、セキュリティに関するグローバルな経験や幅広い専門知識を共有できることを光栄に思う。サイバーセキュリティを巡る状況はグローバル規模で不透明な時代が続くと予想されるが、私たちの日常生活を支える重要な社会インフラシステムを脅かすサイバー攻撃に対処するため、サイバーセキュリティの官民連携は、米国のみならず、国際的にも必要不可欠であると確信している」と述べている。

2025年には、米国政府と通信業界の情報共有機関であるCommunications-ISACに日本企業として初めて参画が認められた。

米国との協力は、研究開発の分野にも広がっている。NTTは2019年、シリコンバレーのパロアルトにNTT Research, Inc.（詳細につき、2節2項（2）参照）を設立し、サイバーセキュリティの強化につながる暗号技術等の研究を推進。さらに、2022年からはスタンフォード大学との共同研究を本格化させ、量子暗号技術やAIを活用した新たな脅威検知手法の開発に取り組んでいる。これらの技術は、NTTグループのセキュリティ対策の基盤を支えるとともに、最先端技術の実用化を加速させている。

**グローバルなマルウェア対策への貢献**

NTTグループは、国際的な脅威対策の一環として、2020年10月に発生したTrickBotマルウェア対策にも積極的に関与した。TrickBotは、米国大統領選挙への影響も懸念されるほど深刻なサイバー脅威であったが、NTTを含む世界のIT企業、ネットワークプロバイダー、法執行機関が協力し、その基盤を遮断し、拡散を抑えることで、マルウェアの広がりを防ぐことに成功した。

この対策において、NTTグループは独自の強みを発揮した。NTT Ltd.（当時）が運営するGTIC（グローバル脅威情報センター）やSOC（セキュリティオペレーションセンター）と、NTT研究所が連携し、世界規模のインターネットバックボーンのトラフィック分析を実施。マルウェアの拡散状況を正確に把握し、適切な対策を講じることで、この国際的な取り組みに貢献した。

## 4-2. NTTグループが守る

### （1）NTTセキュリティの設立とその歩み

**NTTセキュリティの設立**

デジタル社会の発展に伴い、サイバー攻撃はますます高度化・巧妙化し、企業や社会基盤を脅かす存在となっている。特に、通信インフラを支える企業にとって、グローバル規模でのサイバーセキュリティ対策の強化は喫緊の課題となっている。このような背景のもと、NTTはセキュリティ分野の専門性を強化し、統合的なサービスを提供する