Tomorrow, Together

KDDI

おもしろいほうの未来へ。

au

サイバーセキュリティアニュアルレポート 2023

Cybersecurity Annual Report

KDDI VISION 2030

「つなぐチカラ」を進化させ、
誰もが思いを実現できる
社会をつくる。

Contents 目次

目次・編集方針……01
情報セキュリティ委員長メッセージ……02
サイバー攻撃・脅威動向……03
サイバーセキュリティへの取り組み……07
情報セキュリティガバナンス……09
セキュリティ強化に向けた施策……17
先端技術……26
セキュリティ事業への取り組み……33
グループ状況、第三者評価……36
KDDIグループの概要……37

編集方針

本レポートは、KDDIグループの情報セキュリティに関する活動をステークホルダーの皆さまへご紹介し、事業への信頼性を高めていただくことを目的に発行しました。

報告対象期間

本レポートでは、特に記載がない限り2023年9月末までの情報セキュリティに関する取り組みを対象としています。

参照した資料

経済産業省「情報セキュリティ報告書モデル」

WEBサイト

KDDI
https://www.kddi.com/

KDDI セキュリティポータル
https://www.kddi.com/corporate/kddi/public/security-portal/

KDDI サステナビリティ
https://www.kddi.com/corporate/sustainability/

研究開発（R&D）
https://www.kddi.com/corporate/r-and-d/

情報セキュリティ委員長メッセージ

当社は、KDDI VISION 2030として、「『つなぐチカラ』を進化させ、誰もが思いを実現できる社会をつくる。」をメッセージに掲げ、豊かなコミュニケーション社会の発展に向けてさまざまな事業に取り組んでいます。これらを進める上で課題となるのが情報セキュリティです。当社は、重要なライフラインを担う事業者の責任として、いつでも安定した通信サービスを提供するため、情報セキュリティを極めて重要な課題として位置付けています。

スマートフォンの普及やビッグデータ・AI技術の発展、企業のDX化の進展により、さまざまな情報を活用した新たなサービスが創出されていますが、これに伴い、情報セキュリティやプライバシーに関わるリスクも複雑化・多様化しています。また、ハッカー組織によるサイバー攻撃やサイバー犯罪などの活動も活発化し、その手法も日々高度化しています。

このような状況を踏まえ、当社では、不正アクセスや改ざん、標的型攻撃などのサイバー攻撃の脅威から電気通信設備を守るため、セキュリティエンジニアが24時間365日の体制で監視を実施するとともに、サイバー攻撃の分析や監視業務をAIで自動化する技術の導入を進めています。加えて、国内外のCSIRTなどの関連組織と連携し、脆弱性情報や攻撃動向などを収集・分析するなど、セキュリティ対策のさらなる強化に日々努めています。

また、KDDIグループでは、AIの開発と利活用を積極的に進めており、特に生成AIについては、全社横断の体制でその活用を推進しています。一方、AIの利活用は多様な分野に及ぶことから、各分野ごとにAIのもたらす便益やリスクが異なることにも留意し、ガイドラインなどを整備し、対応を進めています。

当社は、倫理・社会受容性、安全性および信頼性を確保するために、複雑化・高度化する新たな脅威への対応を進化させ続け、皆さまに安心してご利用いただけるサービスを提供してまいります。本レポートでは、こうした当社におけるセキュリティに対する取り組みを紹介していますので、是非、ご一読いただけると幸いです。

KDDI株式会社
取締役執行役員専務
CTO 技術統括本部長
兼 情報セキュリティ委員長

吉村 和幸

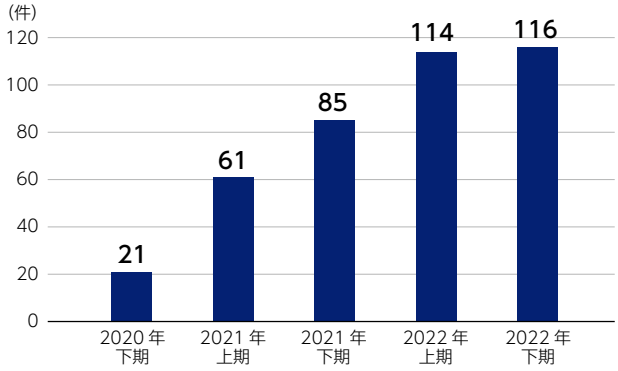
2020年4月　当社執行役員
　　当社技術統括本部長（現在に至る）
2020年6月　当社取締役執行役員
2021年4月　当社取締役執行役員常務
2022年6月　当社取締役執行役員専務（現在に至る）
2023年4月　当社CTO（現在に至る）

サイバー攻撃・脅威動向

1 今日のサイバー攻撃

企業や組織を標的としたサイバー攻撃の被害は絶えず続いており、警察庁の発表するランサムウェア被害の報告件数の推移は、右図にもある通り、セキュリティインシデントが年々増加傾向にあることがわかります。特に近年は、多種多様な製品の脆弱性を悪用する攻撃や攻撃を監視するシステムに検知されにくい手法を用いた攻撃などが増え、攻撃手法が高度化・巧妙化しています。さらに、サイバー攻撃を代行し報酬を得るビジネスモデルが確立され、企業のように複数部門に分かれた構成になっている攻撃者組織が確認されるなど、サイバー攻撃のビジネス化も進んでいます。

企業・団体等におけるランサムウェア被害の報告件数の推移（警察庁発表）

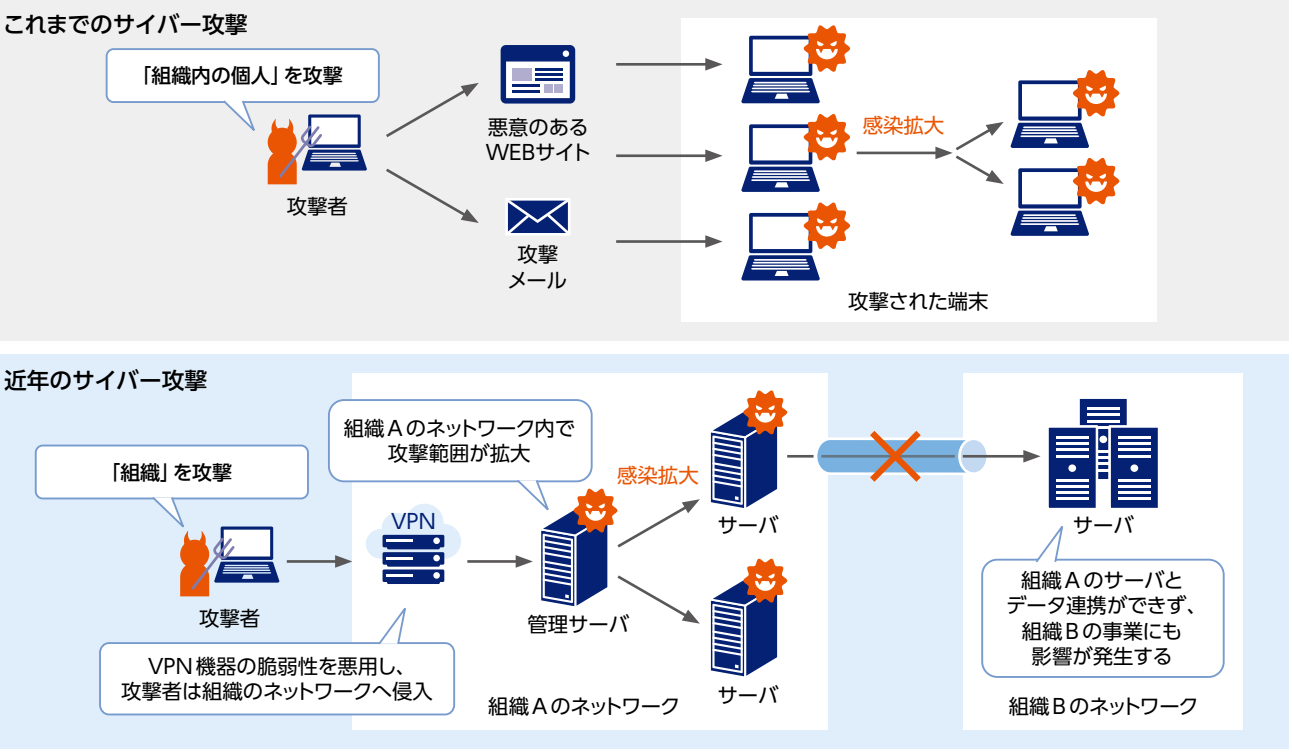


出典 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

組織を標的としたサイバー攻撃は、これまではインターネット上に公開・提供しているWEBサービスへの攻撃や、メールを用いた組織内の個人を標的とした攻撃が一般的でした。しかし、これに加え、VPN（Virtual Private Network）機器を標的とした攻撃や、セキュリティレベルの低いグループ会社や取引先を経由して標的の組織に侵入するサプライチェーン攻撃も増えています。そのため、サイバー攻撃の標的となる範囲が広がっているといえます。

攻撃者の侵入後の行動は多岐にわたりますが、ランサムウェア感染によるデータの暗号化と金銭要求は特に流行している手口です。ランサムウェア感染によって業務活動を停止せざるを得なくなる被害が国内外で報告されています。

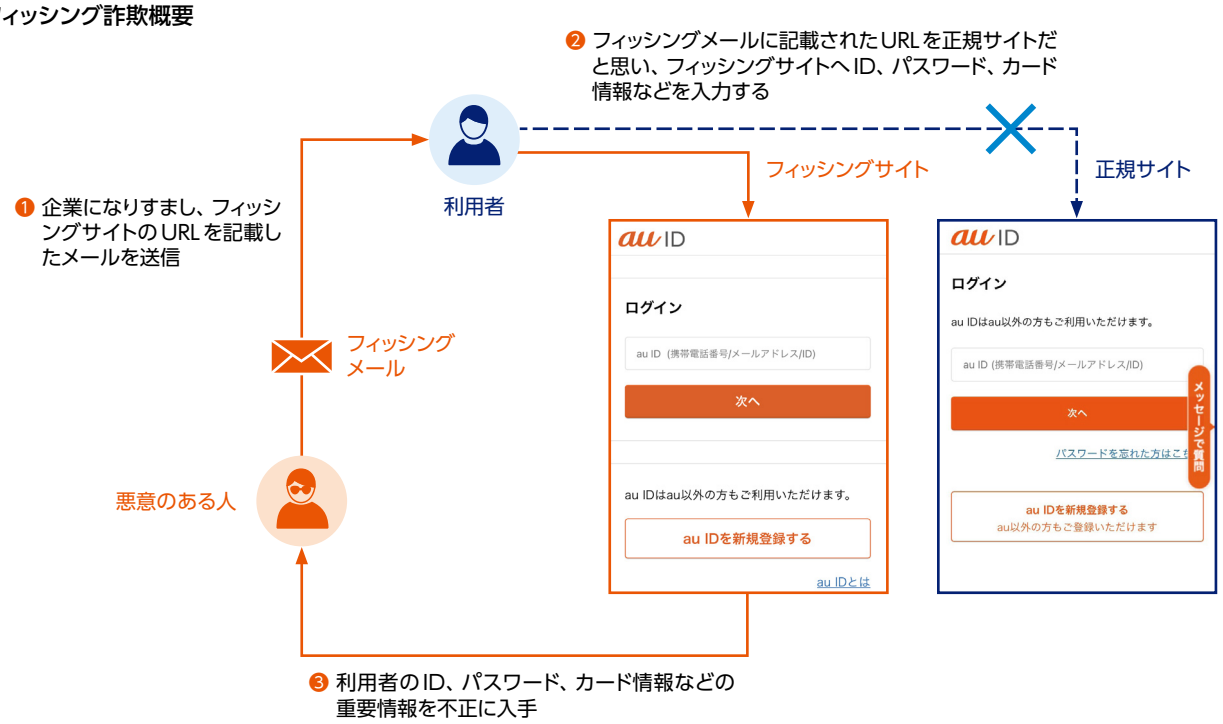
サイバー攻撃の変化



2 サービスの不正利用

企業や組織を標的としたサイバー攻撃に加え、個人のお客さまを狙ったフィッシング詐欺が社会問題化し、各種メディアでも取り上げられるようになりました。攻撃者は、実在する企業や有名なサービスを装ったEメールやSMSを送信し、お客さまを偽サイトに誘導する手法を用いて、認証情報やクレジットカード情報などの個人情報を盗み取っています。フィッシングサイトを用いた手口は年々巧妙になり、メールの文章や偽サイトは見た目だけでは偽物と判断することが難しくなっています。

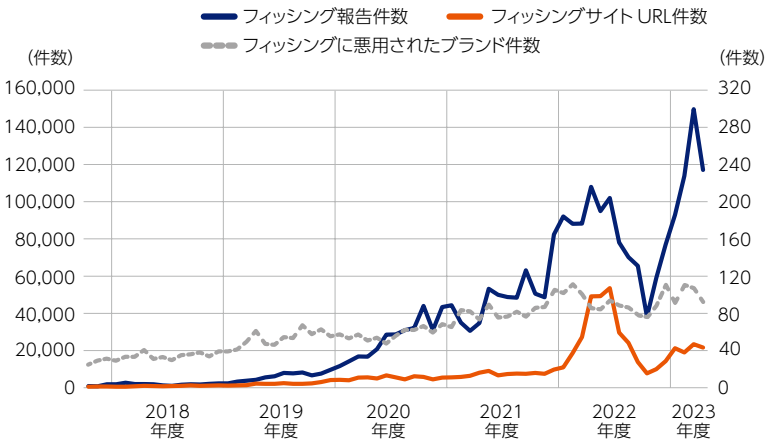
フィッシング詐欺概要



サイバー攻撃・脅威動向

さらに、スマートフォンに悪意のあるマルウェアをインストールさせ被害を引き起こす手口も常態化しています。お客さまがこうした手口に騙され個人情報を盗まれたり、マルウェアをインストールしたりすると、最終的には金銭的な被害を被ることになります。具体的な被害事例としては、キャッシュレス決済サービスやインターネットバンキングの認証情報が盗まれ、お客さまの口座から不正な送金が行われたり、ECサイトやゲームサイトで不正に利用されたりする被害が発生しています。これらの被害は、リアル店舗とオンライン上の両方で起こる可能性があります。警察庁や業界団体の発表によると、クレジットカードやインターネットバンキングの不正送金の被害はここ数年で急増しており、この背景にはフィッシング詐欺の増加があるとみられています。このため、デジタルサービスを提供する事業者においては、フィッシング詐欺などに起因する不正利用への対策強化が求められている状況です。

国内のフィッシング詐欺件数



出典 フィッシング対策協議会のデータから当社にて作成

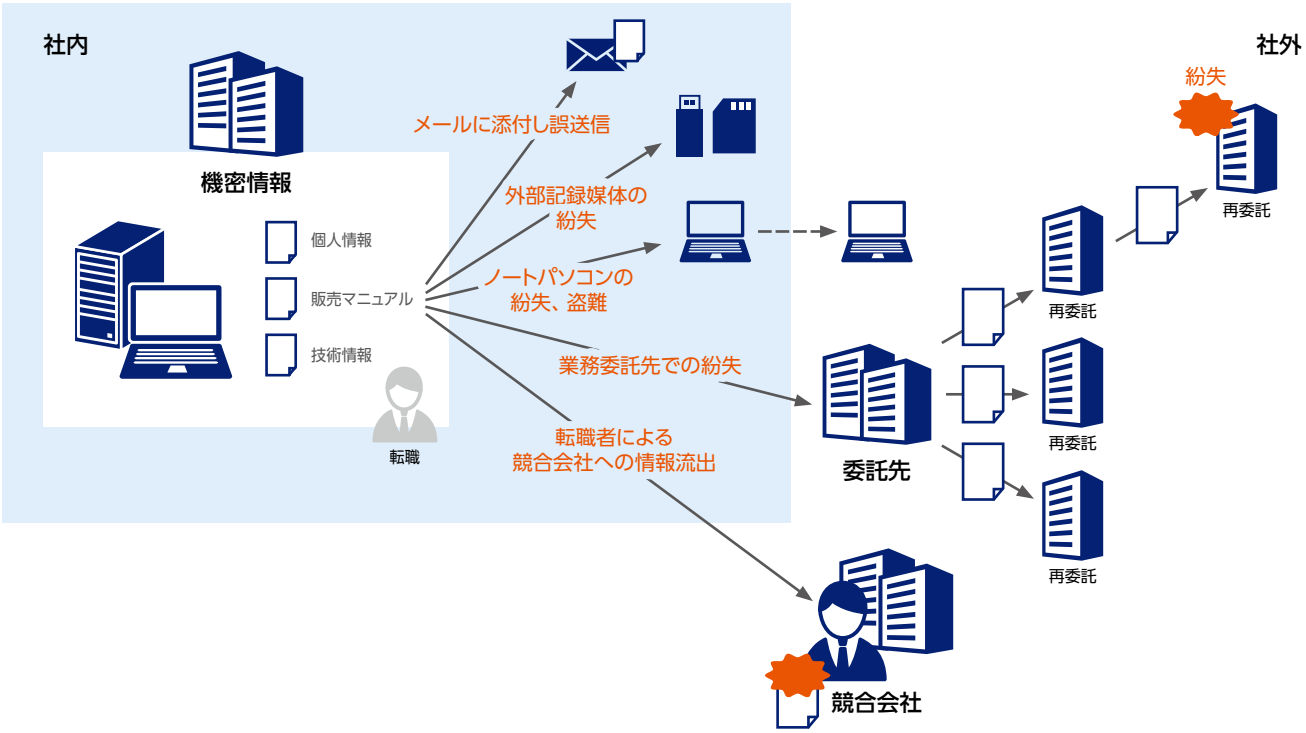
3 個人情報漏えい

企業が保有する個人情報においても漏えいリスクが高まっています。これはデジタル化の進展やテレワークの普及など、社会構造の変化が背景にあります。企業では初期投資や運用コストを削減するためにクラウドサービスの利用が一般的になっていますが、クラウドサービスの設定ミスを攻撃者に狙われ、データが外部に漏えいするリスクも高まっています。また、テレワークの普及により社員がセキュアでないネットワーク環境からアクセスすることが増えたこともリスクを高めています。さらに、人材の流動化による退職者からの情報流出リスク、業務委託先が個人情報を紛失したケース、企業の業務委託先社員が顧客情報を持ち出したケース、これらの事例からもリスクが身近に潜んでいることがわかります。政府の個人情報保護委員会の2022年度年次報告によれば、事業者の漏えい事案の報告が義務化されたこともあり、報告件数は前年度の1,042件から約4倍の4,217件※1に急増しています。

このように、企業の情報漏えいリスクに対しては、自社へのサイバー攻撃だけでなく、内部からの情報漏えいや、業務委託先を含むサプライチェーン全体のセキュリティ対策が急務の課題となっています。

※1 参考：個人情報保護委員会　令和4年度 年次報告の概要について　https://www.ppc.go.jp/files/pdf/050609_annual_report_gaiyou.pdf

機密情報漏えいのパターン

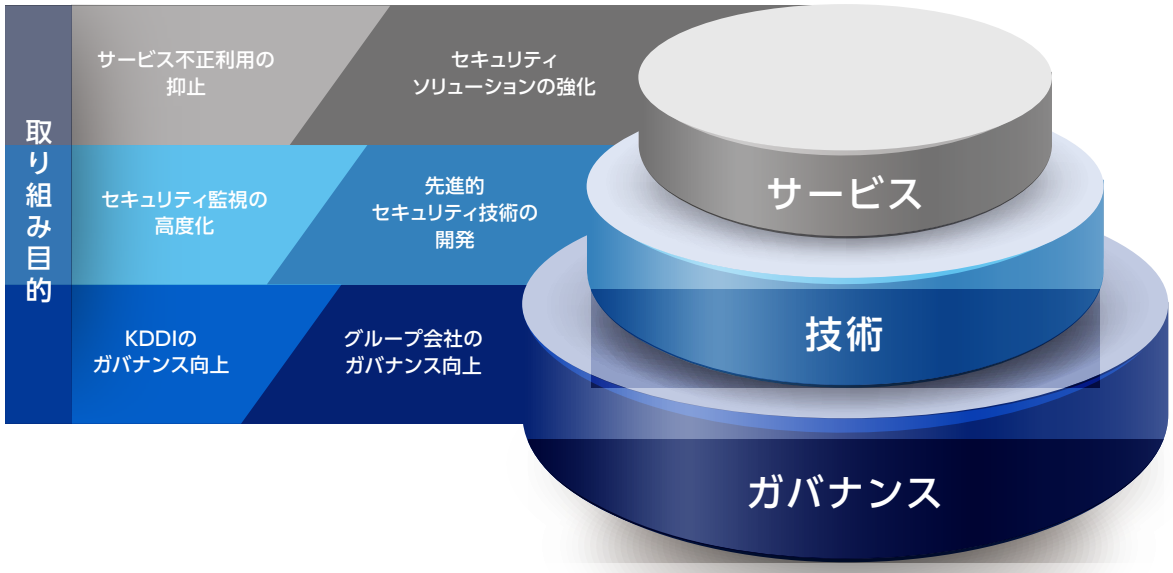


サイバーセキュリティへの取り組み

KDDIは、社会の情報基盤を支えるインフラ企業であり、公共の利益に資する役割を果たしています。そのため、お客さまの生活に直接関わることを強く認識し、使命として「いのち」「くらし」「こころ」をつなぐことを掲げています。この使命を達成するため、安心安全な通信の提供に向けた取り組みを積極的に推進しています。一方で、最近のデジタル社会の発展に伴い、サイバー攻撃も進化し、それによる重要な機密情報の外部流出やサービスの不正利用などの被害が世界的に増加していることも認識しています。これらのサイバー攻撃は、今や、自然災害や気候変動などに迫る大きなリスクとして位置付けられるようになっています。このような状況下で、KDDIはお客さまに安心安全な通信を提供するため、新たな攻撃手法に対しても対策を強化していくことが急務な課題となっています。

サイバーセキュリティ攻撃が激化する現状を受け、KDDIではサイバーセキュリティへの取り組みを一層強化していくべきと認識しており、ガバナンス、技術、サービスの三つの視点を重視し取り組んでいます。

サイバーセキュリティへの取り組み 三つの視点



	目的	取り組み
ガバナンス	KDDIのガバナンス向上	AIガバナンスの整備、ISMS運用のDX化
	グループ会社のガバナンス向上	グループ会社のセキュリティガバナンス強化
技術	セキュリティ監視の高度化	サイバー攻撃の予兆可視化、脅威情報プラットフォームの構築
	先進的セキュリティ技術の開発	情報分析によるC&Cサーバ検知、通信分野におけるソフトウェア部品表の活用検討 暗号化の世界最速処理、デジタルツインによるIoTセキュリティ基盤の構築
サービス	サービス不正利用の抑止	フィッシングサイト検知精度の向上、不正利用の検知高度化
	セキュリティソリューションの強化	セキュリティ事業への取り組み： マネージドトラストの提案・提供、セキュリティ対策の支援

企業がガバナンスを重視することは、リスクマネジメントの強化、コンプライアンスの確保、社会的責任の履行など、多くのメリットがあります。そのため、KDDIはセキュリティガバナンスの強固な土台を築き、KDDIグループ全体のガバナンスを向上させ、社会からの信頼を獲得することを目指しています。

また、セキュリティへの取り組みにおいて技術の向上は非常に重要であり、セキュリティ向上への貢献や支えとなる役割を担っています。KDDIでは、先進的なセキュリティ技術の開発に努め、セキュリティ向上や日々変化する脅威にも対応できるよう技術の礎を築いていきます。

KDDIが提供するサービスは、多くのお客さまに利用され、社会に大きな影響を与えるものです。そのため、サービスを守り、セキュリティを保つこともKDDIの社会的使命であると考えています。お客さまがサービスを安心して利用できるよう、最新の脅威に対応するための技術やノウハウを常に磨き、サービスの不正利用の抑止にも力を注いでいます。また、お客さまがセキュリティに関する問題を解決するための手段として、セキュリティソリューションやコンサルティングサービスも提供しています。

KDDIでは、セキュリティを最優先に対応すべき事項の一つと考え、安心安全な環境を提供するためにこれらの取り組みを進め、より良い未来を築いていくことを目指しています。

情報セキュリティガバナンス

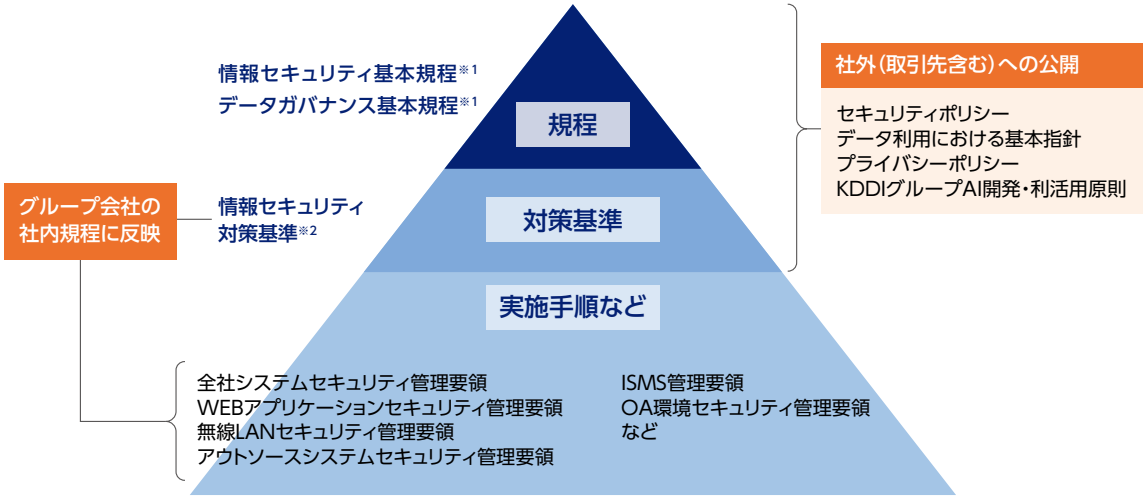
KDDIグループは、高度化・巧妙化が進むサイバー攻撃に対応するため、情報セキュリティに関するリスクマネジメントは非常に重要な課題と認識し、情報セキュリティガバナンスの強化に取り組んでいます。

この章では、KDDIの情報セキュリティガバナンス強化の取り組みとして、情報セキュリティに関するポリシー、情報セキュリティ体制、情報セキュリティマネジメントサイクル、情報セキュリティ監査、情報セキュリティ教育の概要について概説します。

1 情報セキュリティに関するポリシー

KDDIの情報セキュリティポリシーに関する社内文書は、3階層により構成されています。

第1階層に、情報セキュリティに関する基本方針を定めた「情報セキュリティ基本規程」、並びに、データガバナンスに関する基本的な方針を定めた「データガバナンス基本規程」を制定し、第2階層にそれを遵守するための対策基準、第3階層に実施手順などを制定しています。特に規程や対策基準において、お客さま情報や企業の機密情報を厳密に取り扱い、常に適切な防御措置を講じることで、お客さまや関係者からの信頼を得ることを目指しています。このため、社外公開版の「セキュリティポリシー」および「プライバシーポリシー」を策定し、遵守しています。



※1 安全・信頼性基準 別表第3情報セキュリティポリシー策定のための指針（総務省）、情報セキュリティポリシーサンプル改版（JNSA）などと対応
※2 電気通信分野における情報セキュリティ確保に係る安全基準（TCA）などと対応

セキュリティポリシー

KDDIは、情報の適切な管理を重要な経営課題として認識しており、情報セキュリティの確保に取り組んでいます。具体的には、情報セキュリティ管理体制の確立や情報セキュリティ対策の実施、社内規程の整備などを行っています。これらは、情報セキュリティに関する基本方針を定めた「セキュリティポリシー」の一環です。

▶ https://www.kddi.com/corporate/kddi/public/security/

データ利用における基本指針とプライバシーポリシー

KDDIは、さまざまなサービス・商品の提供などの事業活動を通じて、お客さまの体験価値向上や社会の持続的発展に貢献するため、お客さまのパーソナルデータを取得し利用することがあります。ここでいうパーソナルデータは、個人情報の保護に関する法律（以下、「個人情報保護法」といいます）で規定される個人情報に限らず、個人に関するデータを含みます。

その上で、KDDIは、パーソナルデータの重要性を認識し、その保護の徹底を図るために基本理念を明確化し、自らの行動指針を定めるものとして「データ利用における基本指針※1」を掲げています。また、KDDIはこの指針に基づき、パーソナルデータの取り扱いに関する方針として「KDDIプライバシーポリシー※2」を定めています。

※1 https://www.kddi.com/corporate/kddi/public/privacy-portal/
※2 https://www.kddi.com/corporate/kddi/public/privacy/

情報セキュリティガバナンス

生成AIに関するガバナンス

KDDIでは、AI（人工知能）を活用したお客さま体験価値のさらなる向上や社会の持続的発展に貢献するため、「KDDIグループAI開発・利活用原則」を策定しています。本原則では、セキュリティやプライバシー面のみならず、倫理・社会受容性やサービス提供者としての責任などを考慮した、KDDIグループにおけるAI開発者・AI利用者などが遵守すべき9つの原則を定めています。また、本原則に基づくAIサービス開発を実現するための対策要件を定めたガイドラインとして「AI開発ガイドライン」を策定するとともに、当該ガイドラインに基づくリスクアセスメントの活動を推進しています。KDDIグループでは本原則を軸としつつAIガバナンスを整備していくことで、AIサービスを利活用していくための基盤を構築し、生成AIをはじめとしたさまざまなAIの社内業務への組み込みを積極的に推進するとともに、それらの活動で得られた知見を踏まえ、AIの研究開発やお客さまへの安心安全なAIサービス提供を実現していきます。

▶ 2021年8月30日ニュースリリース
「KDDIグループAI開発・利活用原則」を策定　https://news.kddi.com/kddi/corporate/newsrelease/2021/08/30/5356.html
▶ 2023年5月25日ニュースリリース
社員1万人が「KDDI AI-Chat」の利用を開始　https://news.kddi.com/kddi/corporate/newsrelease/2023/05/25/6741.html

生成AI導入までの道
生成AI導入プロジェクト担当者対談

情報セキュリティ本部
セキュリティ管理部
佐々木 弘和

情報システム本部
スマートオフィスシステム部
平野 達矩

生成AIガバナンス整備に取り組むきっかけや、導入までにクリアにした課題があれば教えてください。

佐々木：KDDI社員の生産性向上や社内環境整備に携わっている情報システム本部が「攻めの領域」である一方、私の業務であるセキュリティガバナンスの整備は「守りの領域」と例えられます。この「攻」と「守」は本来であれば相反する領域なのですが、双方の共通認識として、「生成AIがビジネスに大きな影響を与え、ビジネス改革を生み出す」という点が合致していました。そのため、生成AIガバナンスの整備についても速やかに進めることができました。

平野：社内向けに生成AIを活用したサービスの検討を始めましたが、情報漏えいや著作権などのリスクもあり、情報システム本部だけで検討するのは難しいと感じていました。そのため、情報セキュリティ本部と連携し、想定されるリスクと対策について議論を重ねました。社内の利用者向けに利用ルールの策定や、普及啓発コンテンツの展開を実施することで、安全性と安心感を保証しつつ、サービスを開始することができたと考えています。

佐々木：KDDI社員の中には、生成AIをエンドユーザとして利用する人だけでなく、生成AIを自身のサービスに組み込んで提供するなどの発展的な利用をする人もいます。そういった人たちに生成AIのリスクを理解してもらい、正しく利活用してもらうためにも、普及啓発コンテンツではそれぞれの立場を踏まえた留意すべき事項を取り込みました。

今後、生成AIの発展とともに実施すべき施策や、展望があれば聞かせてください。

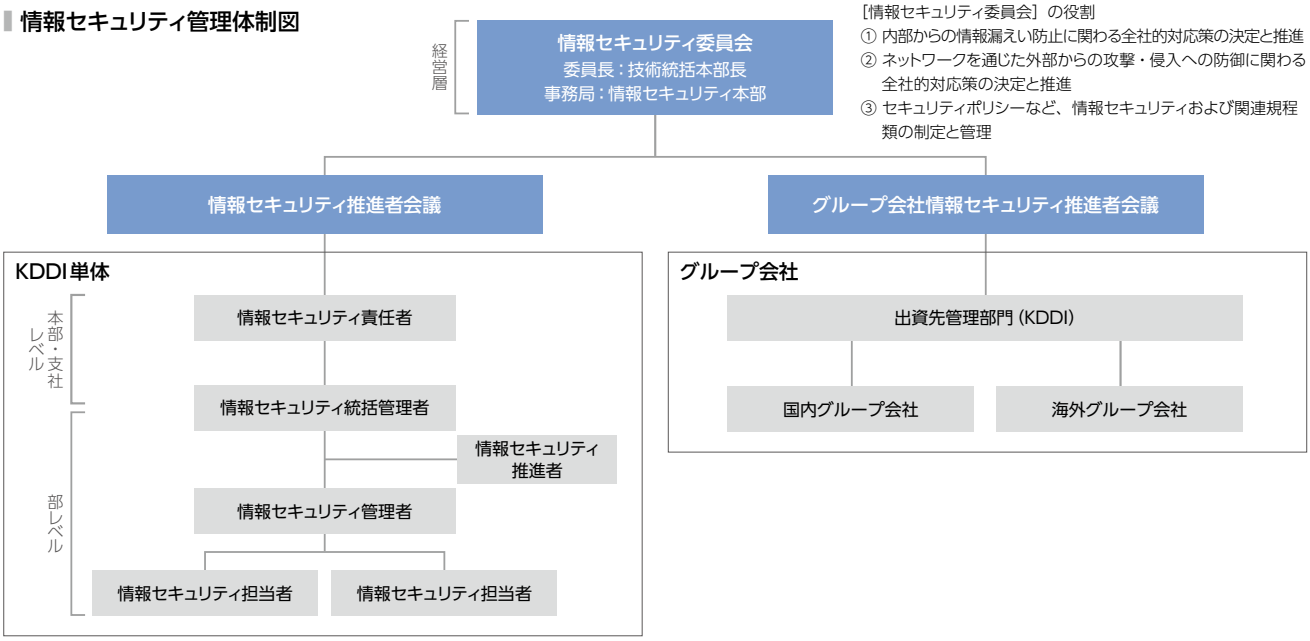
平野：生成AIは業務の生産性向上に大きく寄与できると考えています。今後もIT部門とセキュリティ部門で連携を深めながら、積極的に生成AIを活用した社内環境を整備していきたいと思います。

佐々木：今、社内ではさまざまな人が自然言語の対話型AIのみならずコード生成AIや画像生成AIなどを利用したり、自身のサービスに組み込んで利用しようとしていたりします。これらのさまざまなタイプの生成AIに対し、適切にリスク評価をできるようにし、KDDI社員が安心安全なサービスの利用・提供をできるようにすることが当面の課題です。ガバナンスを司る部門としては、利用者部門との連携をより密にし、お互い歩み寄ったルール作りを検討していきたいです。
また、世界的にAI利用におけるルール形成が進められているため、そういった動向を的確にキャッチし社内ルールに反映していくことで、KDDIが提供するAIサービスが社会的にも安心安全と認められるよう、努めていきます。

2 情報セキュリティ体制

KDDIは、経営層を委員長とし、営業、技術、コーポレートの各部門長を委員とする「情報セキュリティ委員会」を設置して、KDDIおよびKDDIグループ全体で統一的な情報セキュリティを確保しています。また、情報セキュリティ委員会に配属されたKDDIやグループ会社の各部門の代表者からなる「情報セキュリティ推進者会議」および「KDDIグループ情報セキュリティ推進者会議」を設置しています。この体制により、情報セキュリティの管理状況を的確に把握し、KDDIグループ全体で迅速に情報セキュリティを強化するための施策を展開することができるようにしています。また、各グループ会社でも、情報セキュリティ管理体制を整備し、情報セキュリティおよびサイバーセキュリティのリスク低減とその未然防止を図り、リスクの評価・分析および対策・対応を行っています。

情報セキュリティ管理体制図



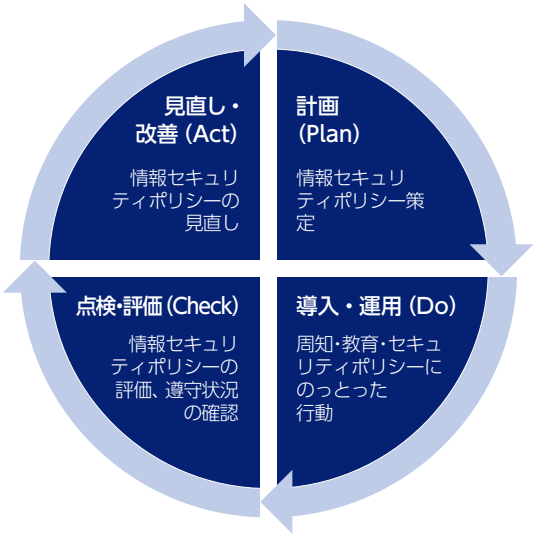
情報セキュリティガバナンス

3 情報セキュリティマネジメントサイクル

KDDIは、ISMS認証（ISO／IEC27001：2013）※1を取得しており、情報セキュリティマネジメントサイクルを導入しています。このサイクルでは、計画段階において情報セキュリティポリシーを策定し、以下の情報セキュリティマネジメント実施サイクル（PDCAサイクル）に従って、チェックや見直し、改善を実施しています。

※1 情報セキュリティに対する第三者適合性評価制度　情報セキュリティ全体の向上に貢献するとともに、国際的にも信頼を得られる情報セキュリティレベルの達成を目的とした制度

情報セキュリティマネジメントサイクルの概要

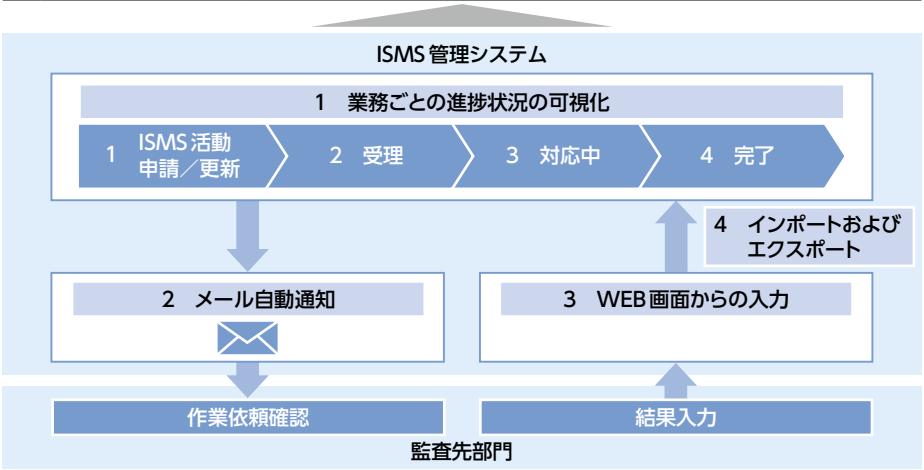


- **計画（Plan）**
  情報資産の洗い出しを行い、リスクや課題を整理し、組織や企業の状況に合った情報セキュリティ対策の方針を定めた情報セキュリティポリシーを策定する。
- **導入・運用（Do）**
  全社員に周知し、必要に応じて、研修などの教育を行う。社員が情報セキュリティポリシーにのっとって行動することで、目的とする情報セキュリティレベルの維持を目指す。
- **点検・評価（Check）**
  導入後の現場の状況や問題点、社会的な状況などを踏まえて、定期的に情報セキュリティポリシー自体を評価する。また、遵守されているかどうかの監査も行う。
- **見直し・改善（Act）**
  点検・評価の内容を参考にして、情報セキュリティポリシーの見直し・改善を行う。

ISMS活動では、さまざまな情報資産を保護するために、定期的にリスクを把握し、必要な対策を迅速に実施することが必要です。また、新たな脅威にも迅速に対応する必要があります。これらの活動は、各部署の担当者によって個別に管理されていましたが、技術の進歩や環境の変化により、担当者の負担が増える可能性がありました。そこで、ISMS管理システムを導入することで、情報資産を一元管理する共通データベース（DB）や業務プロセスの可視化による進捗管理が可能になりました。

今後は、段階的にデータを蓄積分析し、活用することで、業務内容や取り扱うデータに応じたパターン分けによるリスク評価を行います。これにより、効果的なリスク管理が実現されます。

	機能項目	機能概要・補足
1	業務ごとの進捗状況の可視化	申請・承認などのプロセスに応じた進捗状況の可視化が可能
2	メール自動通知	進捗に併せて、依頼メールなどの自動配信が可能
3	WEB画面からの入力	メニュー画面からの選択入力、内容確認が可能。また、入力漏れの検知も可能
4	インポートおよびエクスポート	情報資産台帳などのインポート／エクスポートが可能 また、インポート後にWEB画面からの更新も可能
5	活動状況・登録情報可視化	進捗に応じた活動状況の自動集計や、組織ごとの登録情報の可視化が可能



4 情報セキュリティ監査

KDDIでは情報セキュリティ関連規範の遵守と適切な運用を確認するために、以下の三つの監査を実施しています。

システムセキュリティ監査

KDDIでは、システムの構築または改修を行う場合、専門部署の監査担当者が「全社システムセキュリティ管理要領」に従っているかを調査します。監査では、セキュリティ管理要領に書かれた内容を実装レベルに細分化した「セキュリティ設計書」を使用します。監査項目は数百あり、要件を満たしていない場合は、システム構築担当に是正を求めます。監査で利用するセキュリティ管理要領やセキュリティ設計書については、最新のサイバー攻撃の手法などを踏まえて適宜改訂を行い、セキュリティレベルの向上に取り組んでいます。

セキュリティ監査の流れは下図の通りです。まず、システム化検討フェーズでは、セキュリティ設計書に基づいて書面や対面での監査を行います。システム開発フェーズではネットワーク脆弱性診断やWEB脆弱性診断などを実施し、リリース前に脆弱性に対する対策を講じます。さらに不正侵入検知システム（IDS）などのセキュリティ監視システムを導入し、検知した場合、すぐに対応可能な体制を整えています。システムリリース後、運用フェーズにおいてもセキュリティが適切に保たれていることを確認するため、適宜監査や点検を行っています。

セキュリティ監査の流れ

ISMS内部監査

KDDIは、ISMS認証の範囲にある各部門と関係各社に対し、「ISMS管理要領」と「統合ISMS内部監査手順」に従って、専門部門もしくは社内の組織から選出された監査員による監査を実施しています。このISMS内部監査ではKDDIが遵守すべき情報セキュリティ関連規範が適切に運用されているか、情報セキュリティ管理活動が計画的に実行されているか、またISMS活動が監査対象組織に浸透し有効に実施されているか確認し、準拠していない場合は是正を求めます。また、ISMS内部監査の実施結果およびISMS記録を分析した上でのISMS活動の有効性評価結果をマネジメントレビューで報告し、見直し、改善を行っています。

業務委託先監査

KDDIが業務の一部または全部を委託している場合、KDDIと同等のセキュリティレベルが適切に維持されていることを確認するため、年1回以上の頻度で業務委託先を監査し、管理体制を見直します。さらに、専門部門の監査員による業務委託先の特別監査も実施しています。KDDIは、顧客情報などの重要な情報を適切に保護するため、情報セキュリティに対する取り組みを一層強化していく考えです。

情報セキュリティガバナンス

5 情報セキュリティ教育

従業員のセキュリティ啓発・教育

KDDIでは、お客さまのデータや提供しているサービスをサイバー攻撃から守るために、セキュリティ人財育成プログラムを整備し、体系的なセキュリティ人財育成に取り組んでいます。本プログラムにおいて、社員の成長とキャリアの発展を重視しIPA（独立行政法人情報処理推進機構）が運営する国家資格「情報処理安全確保支援士（登録セキスペ）」の取得を積極的に促しており、専門的なトレーニングや学習支援の提供など資格取得に向けた準備をサポートしています。2023年4月時点でのKDDIグループにおける資格登録者数は274名と、国内有数の人数となっています。

情報処理安全確保支援士　資格登録者数　274名

※ IPA 公開名簿をもとに、勤務先名称「KDDI株式会社」と登録のあるものを抽出
※ 2023 年 4 月集計

人財育成は、社員の成長を促進し、企業のレベルの高さをアピールするための重要な取り組みです。資格取得者が増えることでKDDIの専門性と技術力が向上していくことを目的としています。その他、社員1万1千人を対象に階層別eラーニングおよび集合型の情報セキュリティ研修を実施し、社員のセキュリティ意識およびスキル向上に継続的に取り組んでいます。最新のサイバー脅威動向や情報漏えい事例、またそれらの対策について継続的に学習することで、情報セキュリティへの意識付けと、事故防止のためのスキル向上を図っています。

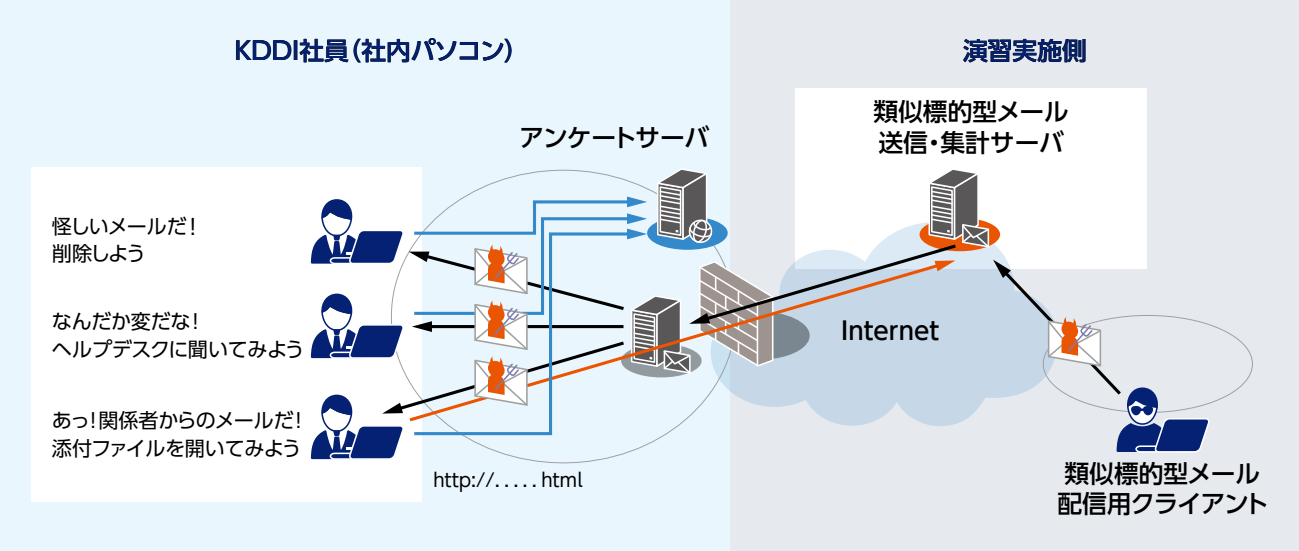
情報セキュリティ研修例

内容	対象者	実施方法
新入社員向け セキュリティ研修	新入社員	集合研修
セキュリティ基礎研修	全従業員	eラーニング
ライン長向け セキュリティ研修	ライン長	eラーニング／集合研修

インシデント対応演習

KDDIでは、万が一サイバー攻撃などのインシデントが発生した場合に、迅速かつ適切な情報共有方法やインシデント対応フローを確認するために、サイバー攻撃を模倣した標的型攻撃メール演習も定期的に実施しています。実際にインシデントが発生した場合には、インシデントの規模に応じて対策本部を設置し、関連部門と協力して適切な対応を進めます。そのため、演習ではセキュリティ関係部門だけでなく、システム関係部門や広報関係部門など、インシデントの発生源となる可能性がある部門や情報を外部に周知するための部門も自身の役割に合わせて演習に参加します。インシデント対応演習では、「シナリオ作成」「演習実施」「フィードバック・改善」というサイクルを継続的に行っています。本演習では、送信するメールの難易度や演習方法の改善を都度行いながら、社員のセキュリティリテラシーの継続的な向上を目指しています。

疑似標的型メール送信による演習例



❶ シナリオ作成

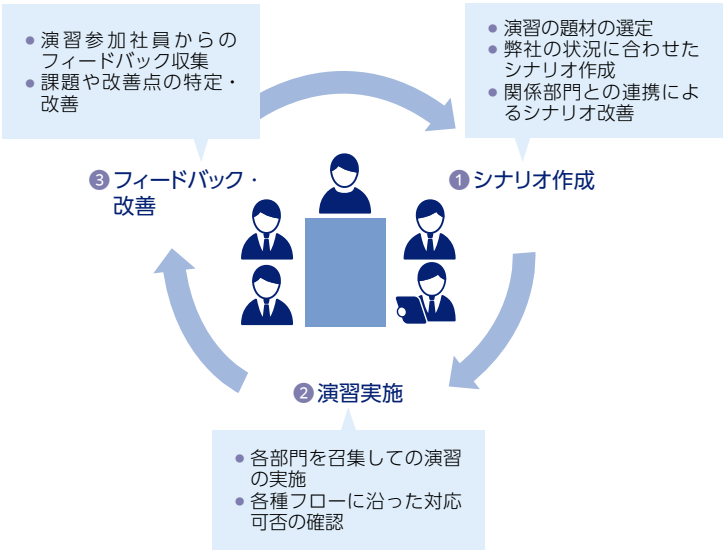
演習関係部門によるシナリオ作成を行います。シナリオ作成では、現在社会的に問題となっているランサムウェアなどの題材を使用して、演習を実施しています。作成したシナリオが実際に起こりうる状況を反映していることを確認するために、シナリオ上のインシデントの発生源となるシステム関係部門とも連携し、シナリオを改善していきます。

❷ 演習実施

各部門を招集し、実際にインシデントが発生したと仮定して、インシデント対応時のやりとりや各種対応を行います。このようにすることで、演習参加部門が予め定められたインシデント対応フローの中で役割を果たせるかを確認します。演習の実施では、実際の現場でのインシデント対応に合わせて、部門間の情報共有を遠隔で行うためにWEB会議を利用するなど、実践的な演習を行っています。

❸ フィードバック・改善

演習後、参加した社員からのフィードバックを集め、現在の課題や改善点を特定します。これらを改善し、さまざまな題材や多数の部門を対象にして、インシデント対応演習を継続実施することで、サイバー攻撃への対応能力を持続的に向上させることを目指します。



セキュリティ強化に向けた施策

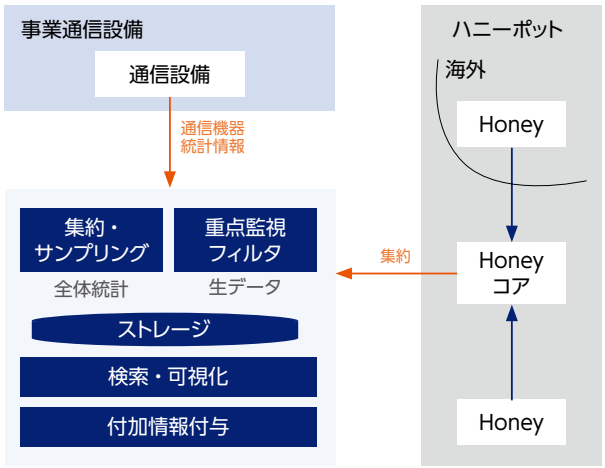
1 監視技術の高度化

お客さまから預かっている情報や取り扱う情報を守るため、常にサイバー攻撃を監視しています。監視システムには、さまざまなログやセキュリティ機器の検知情報を分析し、攻撃を予測する機能があります。また、情報発信を行う各種情報機関やセキュリティ研究機関、セキュリティ専門家からの情報を収集する機能も備えています。さらに、不審なアクセスがあった場合には、早期に検知・対応するためのパソコンやサーバへの監視機能も組み込まれています。これらの機能を活用するため、DXやAIの導入にも積極的に取り組んでいます。これにより、攻撃の兆候が見つかった場合には迅速に対応することが可能となっています。

■ 攻撃通信観測システム

KDDIでは、インターネット上の攻撃の傾向を把握し、攻撃の予兆を可視化することで、積極的な対策を行っています。これを実現するために、KDDIの通信網にはさまざまな通信設備やハニーポットが設置されており、その情報を集約・サンプリングし、相関的な分析を行っています。攻撃通信観測システムを使用することで、KDDIはセキュリティ監視業務において、KDDI網全体や法人のお客さまに対する攻撃の把握や予測が可能となっています。これにより、KDDIは自社および法人のお客さまに対して、通信会社ならではのサイバーセキュリティに関連する付加価値を提供しています。

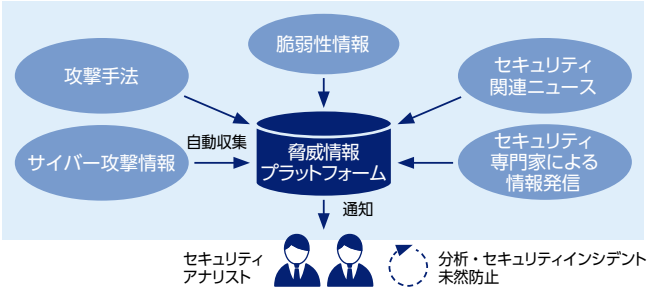
KDDIグループにて開発した攻撃通信観測システムの概要



■ 脅威情報プラットフォーム

サイバーセキュリティは急速に変化する領域であり、重大な脆弱性や攻撃コードが公開されると、迅速に対策を講じる必要があります。そのため、セキュリティ運用では最新の脆弱性情報を迅速に収集することが重要です。従来の方法では、セキュリティアナリストが手作業で情報を収集・分析し、優先順位を判断して社内に注意を喚起する必要がありました。しかし、2022年に開発した「脅威情報プラットフォーム」により、サイバー攻撃情報や攻撃手法、脆弱性情報、セキュリティ関連ニュース、セキュリティ専門家による情報発信を自動的に収集しています。

この脅威情報プラットフォームの利用により、セキュリティアナリストが行っていた情報収集作業が自動化され、セキュリティ運用の品質が向上し、セキュリティインシデントの未然防止につながっています。

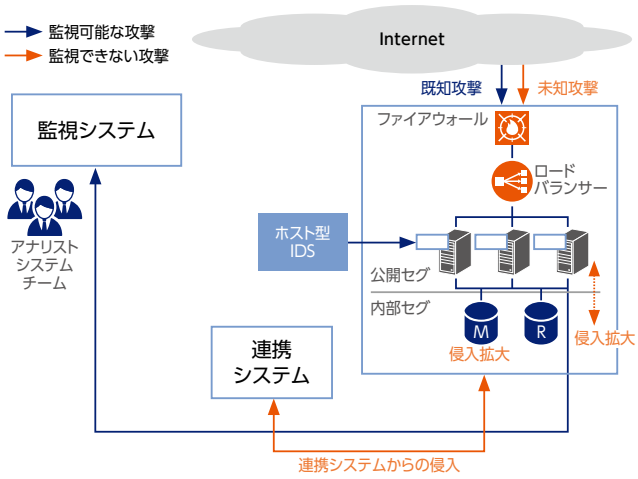


■ サーバ型EDR (Endpoint Detection & Response)

近年、サイバー攻撃が高度化し、巧妙化しています。このため、従来の境界型防御方法だけではサイバー攻撃を完全に防ぐことができず、「侵入前提」の対策が必要となっていました。さらに、攻撃者のリードタイムが短くなり、初期侵入から攻撃目的の達成までの時間が短くなっています。一方で、初期侵入から侵害検知までの時間が長くなっているため、侵害の早期検知と迅速な対応がセキュリティ運用において非常に重要になっています。こうした背景の中、多くの組織では従来のアンチウイルスソフトに加えて、セキュリティソリューションであるEDRを業務用パソコンおよびサーバへ導入し強力なAI技術と連携させることで、侵入してきた攻撃に迅速に対応できる環境を整備していきます。これにより、KDDI内外からの攻撃を検知することが可能となり、セキュリティ監視のレベルを向上させ、監視範囲を拡大することができます。また、セキュリティインシデントの未然防止やセキュリティインシデント対応の迅速化が可能となります。

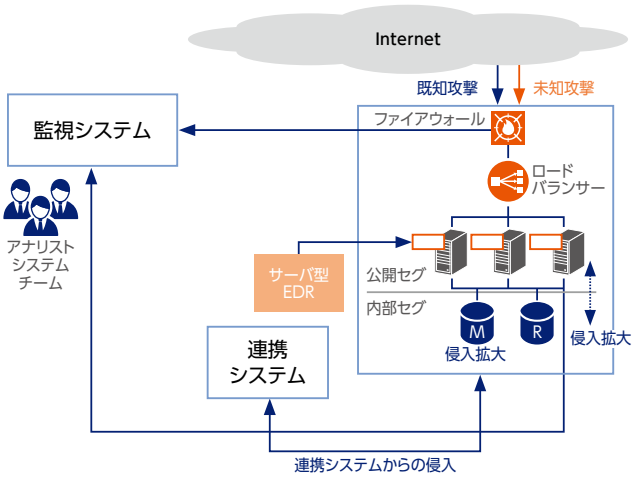
現状の課題

既知事象およびセキュリティインシデントのみを検知。侵入後の内部侵入などは検知できない。



対策内容

サーバ用EDRを導入し、ログを集約する。



セキュリティ強化に向けた施策

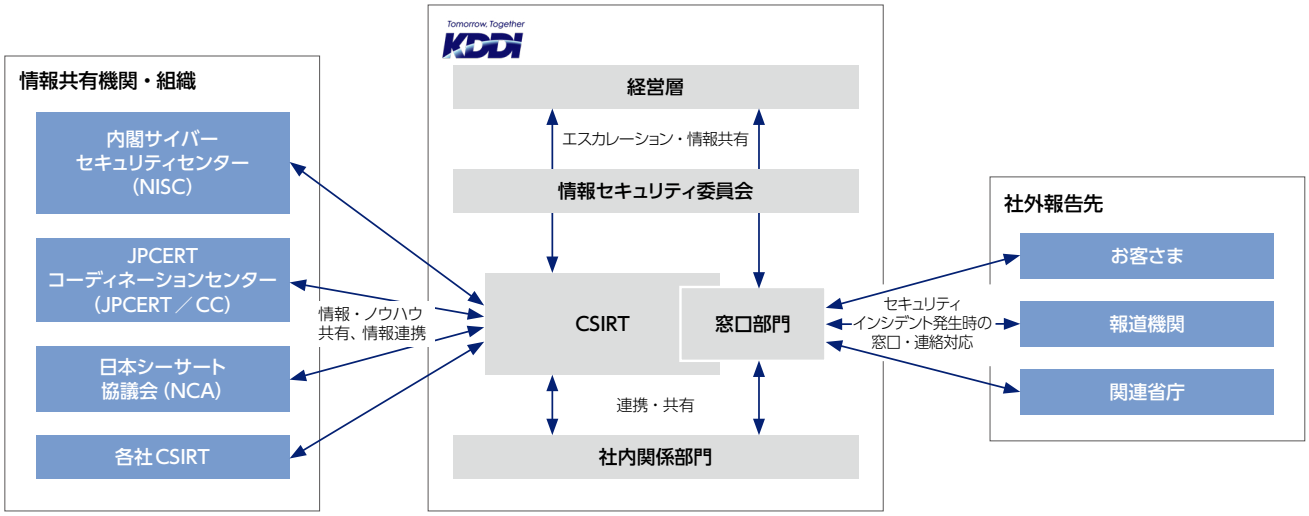
2 セキュリティ施策の紹介

CSIRTの取り組み

CSIRT (Computer Security Incident Response Team) は、組織内で発生したセキュリティインシデントに対応するための専門組織です。CSIRTは有事だけでなく、通常時から組織内外の調整や脅威動向・脆弱性情報の収集・分析を行い、的確なセキュリティインシデントへの対応体制を整備する役割を担っています。KDDIでは、2013年にCSIRTを設置しており、セキュリティインシデント発生時にはCSIRTが社内関係部署と協力して原因調査や証拠保全などを行い、事態収束に向けて社内の統制を確保しています。また、2018年からは外部組織であるKDDIデジタルセキュリティ※1との連携を開始しました。通常時には、セキュリティインシデントの予防のために、サイバー攻撃や脆弱性に関する情報収集を行います。さらに、内閣サイバーセキュリティセンター (NISC) やICT-ISAC、JPCERTコーディネーションセンター (JPCERT／CC) などの社外セキュリティ機関、FIRST (Forum of Incident Response and Security Teams) や日本シーサート協議会 (NCA) といったCSIRTのコミュニティとも緊密に連携しています。

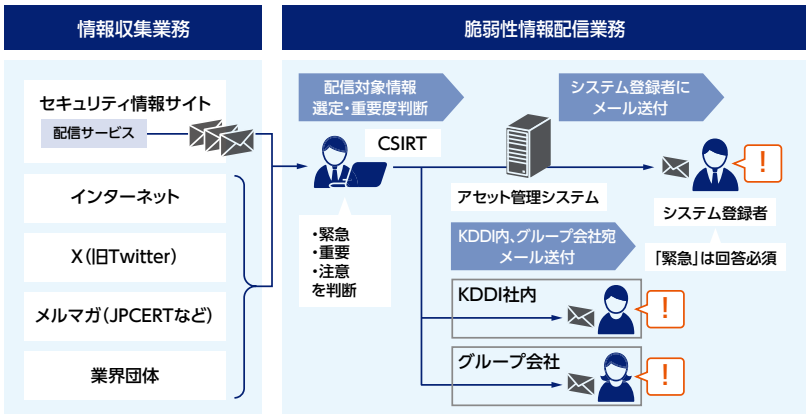
※1 KDDIデジタルセキュリティ株式会社 (KDSec) は、株式会社ラック (LAC) とKDDIが設立した会社で、情報セキュリティ分野のリーディング企業です。KDDIのICTソリューションとLACの高いセキュリティ分析力・技術力を組み合わせ、総合的なセキュリティソリューションを提供するとともに、KDDIグループのセキュリティ対策強化に取り組んでいます。

情報共有機関・社外報告先との連携体制図



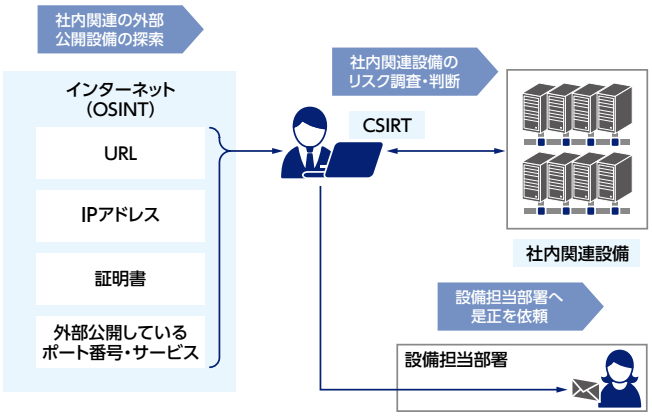
■ 脆弱性情報収集と配信

CSIRTでは、セキュリティ情報サイトや他の情報源から入手した脆弱性情報を社内のシステム構築担当および運用担当に展開し、各担当者に影響の有無を確認しています。もし影響がある場合には、結果をCSIRTに報告し、協力して対処策を実施しています。また2017年4月からは、全システムの構成情報を一元管理するサイバーセキュリティマネジメントシステムを導入しました。現在では、サイバーセキュリティマネジメントシステムを使用して是正対象となるシステムを自動的に判定し、該当するシステム構築担当および運用担当に脆弱性情報を直接配信しています。これにより、迅速かつ効率的な対応が可能となっています。



■ 外部からのアタックサーフェス調査・是正

CSIRTでは、DX推進の取り組みが進む組織において、攻撃の対象となる領域（アタックサーフェス）の拡大に伴い、特にVPN（Virtual Private Network）やRDP（Remote Desktop Protocol）をサポートする外部公開機器が攻撃者の標的とされる傾向があることを認識しています。これらの機器には脆弱性や管理不備が存在し、認証回避やパスワード情報の漏えいなどによる不正アクセスが大きな脅威となっています。実際に攻撃を受けた企業も報告されています。CSIRTでは、外部公開機器を悪用したサイバー攻撃のリスクを低減するために、攻撃者の視点で能動的な調査を行っています。通常の脆弱性診断では特定が難しいホストや管理不備があるホストを特定し、公開状態の見直しや設定不備の是正に取り組んでいます。具体的には、OSINT（Open Source Intelligence）などのインターネット上に一般公開されている情報、URLや証明書などを活用して、外部公開されている社内関連設備を探索します。この調査により、設備に対する攻撃リスクや管理状況を評価します。調査結果をもとに、リスクが高いホストに対しては迅速に是正対応を行い、攻撃者が外部公開機器を悪用できないように対策を実施しています。このように、CSIRTは、組織のセキュリティを強化し、企業が安全にDXを推進できるよう、積極的な対策を行っています。



■ セキュリティ監視への取り組み

KDDIでは、お客さまへ提供するサービスや情報を守るために、24時間365日セキュリティオペレーションセンター（SOC）にてセキュリティアナリストが不正なアクセスや改ざんなどを監視しています。この監視では、不正侵入検知システムやEDRなどからの情報を活用し、不審なアクティビティを検知しています。訓練を受けたセキュリティアナリストは、SIEM（Security Information and Event Management）を使用して、各セキュリティ監視機器から出力されるログを監視・分析し、攻撃の兆候を検知します。危険なセキュリティインシデントが検出された場合には、迅速にCSIRTおよび関係部門に連絡し、対処を指示します。また、内部不正に関しても、従業員が情報を不正に持ち出すなどの事象に対して監視を実施しています。これにより、お客さまのサービスや情報、社内の機密情報をさまざまなセキュリティ脅威から保護しています。

KDDIグループでは、セキュリティ業務に関連するさまざまなシステム（例：サイバーセキュリティマネジメントシステム、セキュリティ情報基盤）の内製開発にも注力しています。

セキュリティ強化に向けた施策

サイバーセキュリティマネジメントシステムは、各システムのアセット情報を管理し、アセットに関連する脆弱性情報の配信、各種対応状況のチケット管理を行います。サイバーセキュリティマネジメントシステムを導入することで、アセット管理の効率化を実現しています。また、セキュリティ情報基盤は、セキュリティ情報の収集、蓄積、調査、分析、可視化を目的としており、情報の一元化をしていることから、効果的なセキュリティ対策の実施を支援しています。

KDDIグループでは、内製開発によって技術を自社内に取り込むことで、より効率的で高品質な業務遂行を実現することにより、セキュリティ対策の強化とお客さまの信頼を確保しています。

■ DDoS攻撃への対策

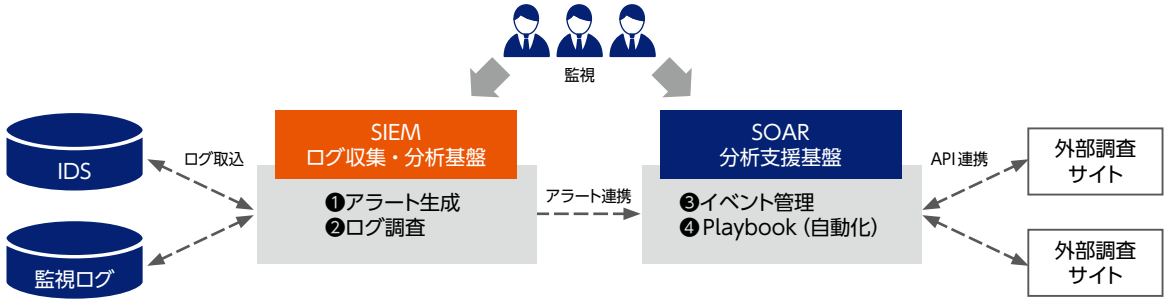
KDDIでは、DDoS攻撃（Distributed Denial of Service attack（分散型サービス妨害攻撃））に対処するためのシステムの開発と運用を行っています。攻撃を検知した場合、事前に設定されたルールに基づいて自動的に対処が行われます。ただし、必要に応じてKDDIデジタルセキュリティと通信設備の運用監視部門が連携し、対応策を実施します。DDoS対策においては、AIなどの技術に関する情報収集と検証にも積極的に取り組んでいます。これにより、最新の技術や手法を把握し、攻撃の特徴を迅速に検知して対応することが可能となっています。これらの取り組みにより、KDDIは通信ネットワークを保護し、安定的な電気通信サービスを提供することができています。DDoS攻撃によるサービスの停止や中断を最小限に抑え、お客さまに安心してご利用いただける環境を提供しています。

■ 高度なセキュリティ監視を支える技術開発

KDDIグループでは、事業用ネットワークやコーポレートネットワークをサイバー脅威から守るために、最先端技術を活用してセキュリティ監視システムの高度化に取り組んでいます。これには、SIEM（セキュリティインシデントおよびイベント管理）、SOAR（Security Orchestration, Automation and Response）、不正侵入検知システムなどの監視設備やシステムが活用されています。

サイバーセキュリティ分析支援基盤では、監視要員の高度な技術と監視プロセスの自動化を組み合わせることで、膨大なログを効率的に分析し、高品質なセキュリティ監視を実現しています。また、この分析支援基盤は、KDDI単体だけでなくKDDIグループ全体のセキュリティイベントを収集・分析するために、世界中のKDDIグループ会社に導入されています。これにより、KDDIグループ全体のセキュリティを確保しています。

KDDIグループは、最新のセキュリティ技術を活用し、セキュリティ監視システムの高度化と効率化を図ることで、お客さまのネットワークを確実に保護しています。また、グローバルな展開により、KDDIグループ全体のセキュリティを一元的に管理し、より安全な環境を提供しています。



データ分析による最新のサイバー攻撃情報を共有する強力なパートナーシップ

絶えず変化するサイバー攻撃に対して、KDDIの情報セキュリティ本部とKDDIデジタルセキュリティが共同で実際のデータからDDoS攻撃の傾向を分析し、情報共有する取り組みを推進しています。

KDDIデジタルセキュリティ　セキュリティ運用1部
牛田 敦（写真・左）
KDDIデジタルセキュリティ　セキュリティ運用1部
大石 暉（写真・中）
情報セキュリティ本部　システムセキュリティ部
三浦 雄大（写真・右）

どのような背景で、共同でDDoS攻撃を分析する取り組みを開始したのでしょうか？

KDDIは、各通信設備への大量のトラフィックデータを集約していますが、DDoS攻撃の分析に時間を割く人手が不足しているという課題を抱えていました。一方、KDDIデジタルセキュリティでは、主にKDDIに対するネットワーク経由でのサイバー攻撃を分析するアナリストの育成に力を注いでおり、双方の課題と要求が一致したことから、共同でデータ分析の取り組みを開始することになりました。また、KDDIデジタルセキュリティの強みである世の中の脅威情報を収集している知見を活かして、世間の攻撃情報と実際の検知データを絡めた定期レポートを作成し、双方で情報共有を行っています。

データ分析によるサイバー攻撃の傾向分析にどのようなメリットがあると考えていますか？

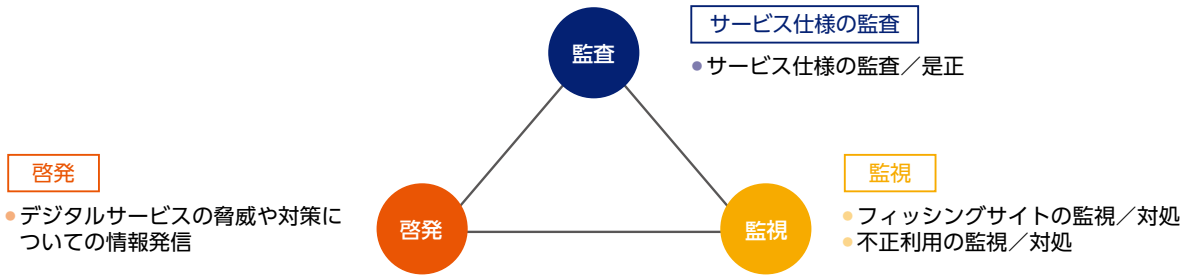
DDoS攻撃は最も古いサイバー攻撃手法の一つであり、「TCP SYN Attack」などは20年以上もの間、有効な攻撃で使われています。一方、現在は攻撃で利用されるポートが多岐にわたり、また、IoT機器を悪用したボットネットと思われるさまざまな送信元からの攻撃通信が観測されているため、攻撃を防御するのが困難な場合があります。
しかし、DDoS攻撃の傾向をデータ分析により把握することで、自動的に制御や対策の実施が可能となります。これにより、攻撃による被害の拡大を防止し、早期に復旧することができます。つまり、データ分析はDDoS攻撃を防御するために有用な手段であり、セキュリティ対策において欠かせない要素となっています。

今後の展望として、セキュリティに対してどのような取り組みを行っていく予定ですか？

DDoS攻撃手法のトレンドが日々変化していく中で、攻撃の全容が見え辛い通信も観測され始めてきました。こういった通信をアナリストが分析するために、高度な可視化技術を取り入れることで攻撃の全体像を掴み、適切なセキュリティ対策を実行していく予定です。

SSIRTの取り組み

SSIRT（Service Security Incident Readiness & response Team）は、NISCでも必要性が提起されている、サービスのデジタル化に伴う新たな脅威に対応するための組織です。当社では、2018年にSSIRTを結成し、デジタルサービス提供者としての新たなリスクに対処するため、専門知識を持ったチームが「サービス仕様の監査」「監視」「啓発」の三つの施策を軸に対策に取り組んでいます。さらに、この取り組みをKDDIグループ全体に拡大する活動も進めています。

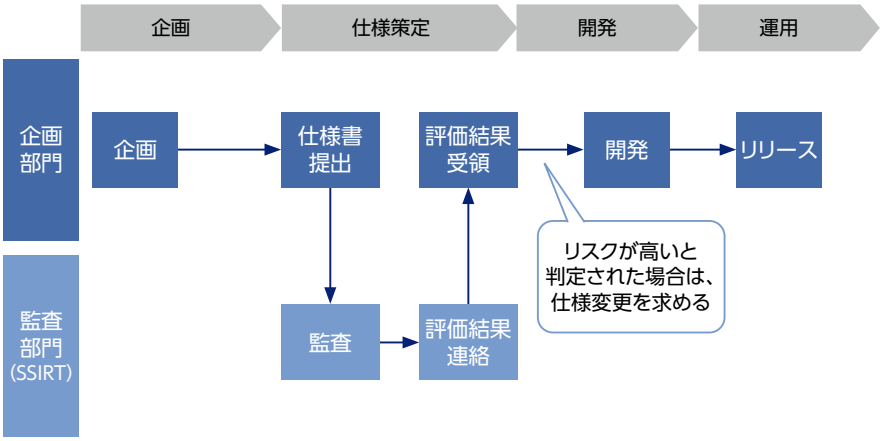


セキュリティ強化に向けた施策

デジタルサービスの不正利用への対策

■ サービス仕様の監査

SSIRTでは、新しいサービスの提供や機能の追加・変更を行う際に、事前にサービス仕様を監査しています。この監査により、サービス仕様の不備や悪用の可能性を特定し、お客さまが当社のサービスを安心安全に利用できるようにするため、仕様の修正や悪用リスクの軽減に取り組んでいます。



お客さまが安心して利用できるスマートフォンアプリの提供を目指して

スマートフォンの普及に伴い多種多様なアプリケーションが提供され、従来パソコンで行っていたことがスマートフォンでも利用できるようになり、人々の生活はますます便利になっています。しかし、スマートフォンには多くの個人情報が保存されており、常に持ち歩くことから、位置情報などの多数の情報の取得・蓄積が可能となっています。そのため、アプリケーションがスマートフォン内の情報にアクセスし、情報を取得されていることに不安を覚えることがあります。また、アプリケーションの脆弱性により、情報が漏えいする可能性もあります。

KDDIでは、お客さまがより便利にauのサービスを利用できるよう多くのアプリケーションを提供しており、先に述べた背景から、お客さまが安心して利用できるアプリケーションを提供することが必要だと考えています。

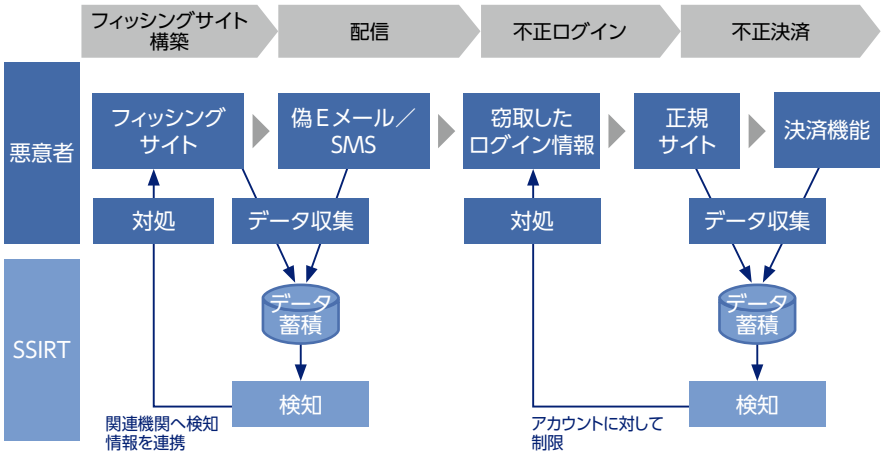
そのため、KDDIでは、スマートフォンアプリを開発・提供する際のガイドラインを全社規程として策定し、アプリケーションを公開する前に、脆弱性とプライバシーの監査を実施することを義務付けています。脆弱性の監査は一般社団法人日本スマートフォンセキュリティ協会（JSSEC）が発行している「Androidアプリのセキュア設計・セキュアコーディングガイド」やOWASP（Open Worldwide Application Security Project）が発行しているモバイルのセキュリティガイドラインに準拠した診断を行っています。また、プライバシーについては、総務省が発行しているスマートフォンプライバシーイニシアティブ（SPI）にのっとってプライバシーポリシーを作成し、さらに、SPIで推奨している第三者機関による審査を行っています。この審査では、プライバシーポリシーに記載されている通りデータを送信していることを確認し、取得するデータの透明性の確保を行っています。また、審査を実施するにあたり、専用の審査ツールを開発し審査を行っており、au Payマーケットで提供している3rd Party製のアプリケーションについても同様の審査を行っています。その結果、これまでの審査の累計数は13,000件を超えるものとなっています。

今後も、新たな脅威に備え、ガイドラインの改版を適宜行い、お客さまが安心して利用できるスマートフォンの提供を目指して取り組んでいきます。

サービス統括本部　サービス開発1部セキュリティ&プライバシーガイドライン監査担当　本間 輝彰

■監視

フィッシング詐欺への対策として、SSIRTでは二つの監視を行っています。一つは、「フィッシングサイトの監視」です。これはインターネットから得られる情報をもとにフィッシングサイトの発生を検知し、検知した場合には関連機関に連携し、お客さまがアクセスできないようにするなどの対処を行うものです。もう一つは、「不正利用の監視」です。システムのログなどの情報を分析し、ログインや決済が正規のお客さまによるものか、アカウント乗っ取りによる不正なものかを判定し、不正と判断した場合にアカウントに対する制限をかけるものです。SSIRTではこれらの監視を24時間365日体制で行い、お客さまが被害に遭わないよう対処にあたっています。また、日々データの分析や分析対象データの拡大などを行い、新たな不正の早期検知や検知精度向上に向けた監視機能の強化を進めています。



■啓発

フィッシング詐欺などの犯罪手口を当社WEBサイト上で公開し、デジタルサービスを利用する上でお客さまにご注意いただきたい事項や有効な対策を発信しています。また、フィッシング対策協議会や一般社団法人日本サイバー犯罪対策センター（JC3）などの外部団体と連携し、最新の手口や対策などの情報共有や対応能力の強化を進めています。

セキュリティ強化に向けた施策

安全なサービスを提供するための監査の取り組み
SSIRTメンバー対談

情報セキュリティ本部
システムセキュリティ部
西岡 幸来

情報セキュリティ本部
システムセキュリティ部
加藤 卓也

サービスの不正利用の最近の傾向を教えてください。

西岡：他人のオンラインアカウントへの不正ログインは、以前はパソコンでのインターネットバンキングなど一部のサービスを狙ったものでした。しかし、スマートフォンの普及によりオンラインで手軽に買い物や銀行振込などができるようになったことで、不正利用の被害も広がってきています。実在する組織になりすましたメールやSMSを使い、ログインに必要な情報を聞き出すフィッシング詐欺が悪意者の主な手口で、不正ログイン後は勝手に物品を購入したり不正に送金したりしていることが確認されています。

加藤：利用者がフィッシング詐欺に騙されてアカウント情報やパスワードをフィッシングサイトに入力してしまうと、悪意者はその情報をもとにログインできてしまいます。2段階認証コードの送付などによって不正ログイン対策をしているサービスもありますが、そのコードすらも騙されてフィッシングサイトに入力してしまうことで不正ログインを許してしまいます。

西岡：手口は日々巧妙になっています。企業も対策を行っているものの、それを乗り越えるような手口も考案されているのが現在の状況だと思います。
当社もau PAYやau PAYマーケットをはじめとした多様なサービスを提供しているため、このような被害とは無関係ではありません。それらへの対応としてフィッシングサイトや不正利用の監視を行っていますが、サービス自体を安全な仕様にするための取り組みとしてセキュリティ監査の対応も行っています。

どのようなことを意識して監査に取り組んでいますか？

加藤：サービス仕様の監査では、悪意者からの狙われやすさと悪用された場合の被害の大きさの二つを考慮して不正利用されるリスクの大きさを評価しています。また、一定以上のリスクが想定される場合には必要な対策案を考えてサービス企画部門に対策の強化を依頼します。セキュリティ対策は安全性と利便性がトレードオフの関係にありますが、安全性を第一に考えながらも私たちは可能な限り双方が両立することを目指すようにしています。

西岡：悪意者からの狙われやすさと被害の大きさは、悪意者が不正を働く手間と得られる利益との兼ね合い、言い換えると不正利用を実行するモチベーションそのものに依存するものとなります。そこで、悪意者のモチベーションが高まらないようにすることがポイントになりますが、それには画一的なルールを作り、監査によりルールに基づいて認証を追加したり利用できる金額を制限することがガバナンス上は有効です。ただ、サービスの不正利用対策において、これでは正規のお客さまの利便性を損ねてしまうのが難しいところです。

加藤：そこで私たちは画一的なルールではなく、ガイドラインのような一定の基準は定めつつも悪意者のモチベーションに着目した個別施策ごとにメリハリのある対策を推進しています。これには、国内や海外におけるサービスの不正利用の動向に精通している必要があるため、業界団体への参画や海外のニュース調査など、日々情報収集に努めています。

西岡：今後も、世の中の変化にあわせて悪意者の行動も変わっていくと考えられますが、常に変化を捉えながら安全で使いやすいサービスを提供していくことに貢献していきたいと思います。

3 ガバナンス強化への施策

グループセキュリティガバナンスの再構築

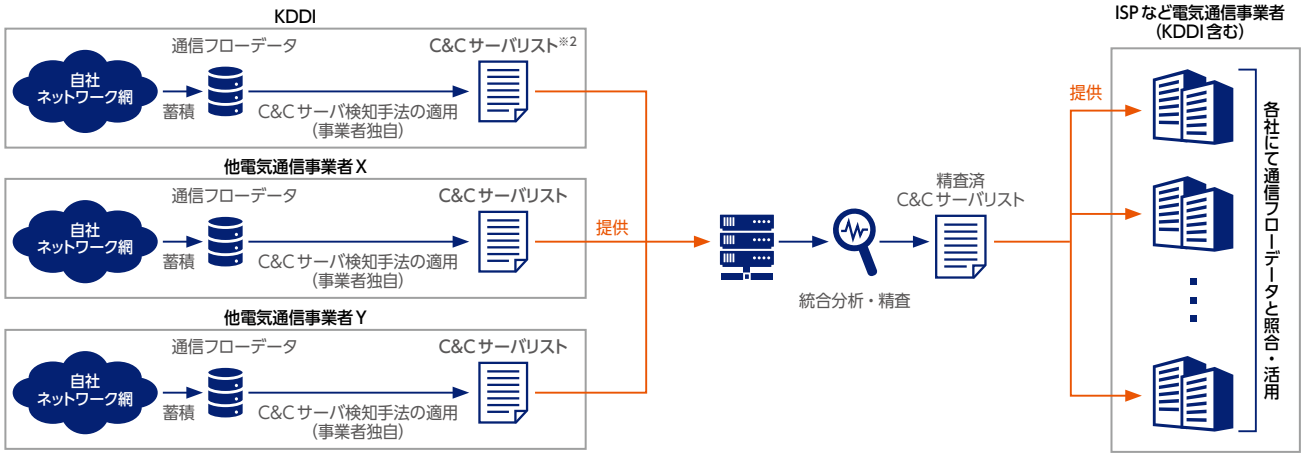
KDDIは、2011年度にグループ会社に対して「KDDIグループ情報セキュリティ共通基準」を制定し、各グループ会社に基準の達成を促しています。これにより、KDDIグループ会社のセキュリティレベルを向上させるとともに、情報セキュリティガバナンスの強化に取り組んでいます。また、グループ会社の増加に伴い、各社の事業形態や規模に合わせたセキュリティガバナンスの構築が求められています。そのため、2023年10月にKDDIグループ情報セキュリティ共通基準を改定し、各社が事業形態や規模に応じたセキュリティ体制を構築するための支援を行っています。これにより、グループ全体でのセキュリティ体制の統一と強化を図ることを目指しています。

1 C&Cサーバ検知事業

テレワークの増加をはじめとした社会情勢の変化によりIoT機器、スマートフォン、パソコンなどのインターネットに接続された端末がますます増加している昨今、端末をマルウェアに感染させDDoS攻撃やフィッシングに代表される情報窃取の踏み台として悪用するサイバー攻撃もその活動の規模を増しています。マルウェアに感染した端末にサイバー攻撃の指示を出す指令サーバは通称Command & Controlサーバ（以下C&Cサーバ）と呼ばれており、電気通信事業者であるKDDIとしては今後C&Cサーバへの適切な対処を進めていく観点から、主体的にC&Cサーバの活動状況を把握する必要があります。このような背景を踏まえ、KDDIでは複数の大手電気通信事業者などと連携し、2022年度から総務省より請負事業を受託し、自社ネットワークを流れるトラフィックのうちフロー情報※1と呼ばれるデータの大規模な分析によりC&Cサーバを検知する取り組みを行っています。

2023年度は2022年度の分析によって得られた知見や課題をもとに一層精緻にC&Cサーバを検知できるよう分析手法の改善を図るほか、KDDIを含む大手電気通信事業者が検知したC&Cサーバの情報を他事業者へ共有する取り組みにも協力することで、国内電気通信事業におけるセキュリティ対策を促進するとともに、KDDI情報通信ネットワークの安全・信頼性の確保に努めていきます。

※1 トラフィック内のコンテンツを除いた、送受信 IP アドレス・ポートやタイムスタンプなどの付随情報



※2 IP アドレス・ポート番号から構成され、通信の秘密には該当しません

データサイエンティストが切り拓くサイバーセキュリティ

私は、2023年4月より情報セキュリティの業務に携わっていますが、それまでは、KDDI総合研究所で5年半にわたり、データ分析・AIの研究に従事していました。C&Cサーバ検知事業プロジェクトは、自社通信フローデータを分析し、C&Cサーバである可能性が高いIPを絞り込むという取り組みで、研究所で携わっていた専門分野に親和性が高いものでした。しかし、実際に参画してみると、同じデータ分析でも、サイバーセキュリティ領域特有の課題があることに気づきました。

例えば、データセットの収集において、このIPがC&Cサーバであるかどうかというラベル情報を網羅的に取得することは極めて困難です。もちろん、こういった課題に対しては、半教師あり学習や教師なし学習といった機械学習アプローチが可能であり、今後検討を進めていく予定です。
また、違った側面からの取り組みも必要で、各通信事業者が構築しているラベル情報の共有や共通化を進めることで、プロジェクト自体の発展につながるだけでなく、各社の通信フローデータの分析に関する知見の獲得にもつながることを期待しています。

最終的には本プロジェクトを通じて社内のサイバーセキュリティに関連するデータ全般の分析力を会社全体で高め、KDDIのサイバーセキュリティ確立に寄与できればと考えています。

情報セキュリティ本部　セキュリティ管理部C&Cサーバ検知事業プロジェクト担当　美嶋 勇太朗

先端技術

2 SBOM導入に向けた実証事業

通信システム機能の高度化・多様化に伴い、その基幹ソフトウェア構成は多数のソフトウェア部品による複雑な組み合わせに変化してきました。一方で、ソフトウェア部品に対して悪意あるコード混入や脆弱性を狙ったサイバー攻撃などが発生しており、通信システムでも同様の攻撃被害を受けるリスクが顕在化しています。通信システム内のソフトウェア構成を把握できていない場合、脆弱性への迅速な対応が困難であるため、部品一覧やバージョン情報などをまとめたSBOM（Software Bill of Materials：ソフトウェア部品表）の重要性が急速に高まっています。

このような背景から、KDDIは総務省から「通信分野におけるSBOMの導入に向けた調査の請負」事業を受託し、KDDI総合研究所、富士通株式会社、日本電気株式会社、株式会社三菱総合研究所と、本事業に取り組む体制を構築しました。本事業では、SBOM活用により脆弱性などへの迅速な対応を実現するため、通信分野におけるSBOM導入に向けた技術面・運用面の課題の整理に取り組みます。

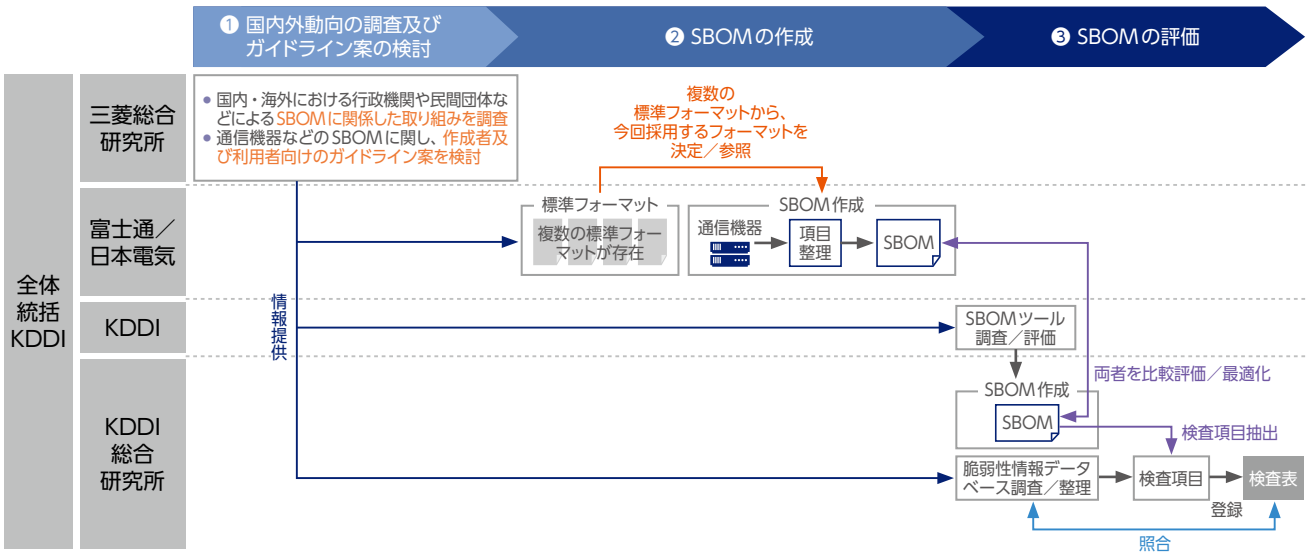
本事業では、通信分野におけるサイバーセキュリティ強化を目的として、KDDIが全体統括を担当し、各社が分担して、以下の❶～❸を実施します。

❶ 国内外動向の調査及びガイドライン案の検討（担当：三菱総合研究所）
国内における通信分野以外の分野でのSBOM活用事例及び欧米を中心とした諸外国の行政機関や民間団体などによるSBOMに関係した取り組みを調査します。また、通信分野におけるSBOMを作成及び利用する上での留意点の整理のため、作成者及び利用者向けのガイドライン案を検討します。

❷ SBOMの作成（担当：富士通／日本電気）
5GやLTEの無線アクセスネットワークやコアネットワーク向け通信機器を複数選定します。また、業界で提案されている標準フォーマットから実証事業で使用するフォーマットも決定した上で、「通信分野において着目すべき項目」を整理し、上記機器に対して抜け漏れがないよう網羅的に完成度の高いSBOMを作成します。

❸ SBOMの評価（担当：KDDI／KDDI総合研究所）
機能・精度・コストなどの観点から選定した複数のSBOM作成ツールを用いて、❷の機器に対するSBOMを作成します。また、ツールによるSBOMと❷にて作成したSBOMの比較により、精度評価を実施します。さらに、SBOMから脆弱性をチェックするための検査表を作成し、外部の脆弱性情報データベースとの照合により、SBOMを用いた適切な脆弱性管理方法の検証を実施します。

サイバーセキュリティを取り巻くさまざまな環境変化が予見される中、お客さまの生活を支える通信サービスを安定提供するために、今後もサイバーセキュリティ強化に向けた貢献に努めていきます。



3 Rocca-Sで世界最高速2Tbpsの性能を達成

超高速共通鍵暗号方式「Rocca-S」が世界最速となる2Tbpsの処理性能を達成

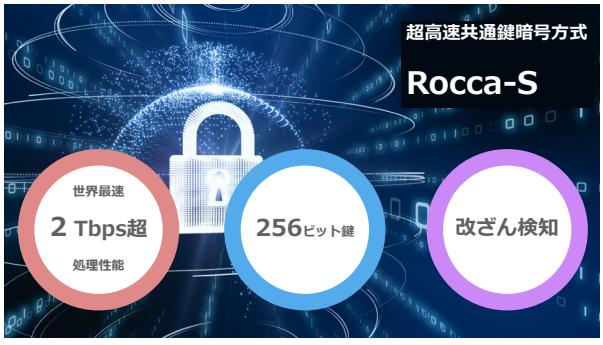
私たちが日常的にスマートフォンやパソコンを使ってインターネットを利用する際、その内容はほとんどの場合暗号化され、他人に見られないように保護されています。例えば、インターネット上で会員登録や問合せを行う際には、SSL／TLSという暗号技術が用いられ、個人情報などの入力内容が第三者によって見られないように保護されています。具体的な暗号化の例としては以下のようなものがあります。

- パスワードによるソフトウェアやハードディスク内データの暗号化
- 同じ電波を使っていても隣の人の通信内容を読み取れないWi-Fi通信の暗号化
- オンライン会員登録時の入力内容の暗号化
- オンラインショッピングサイトでの住所・氏名や決済情報の暗号化

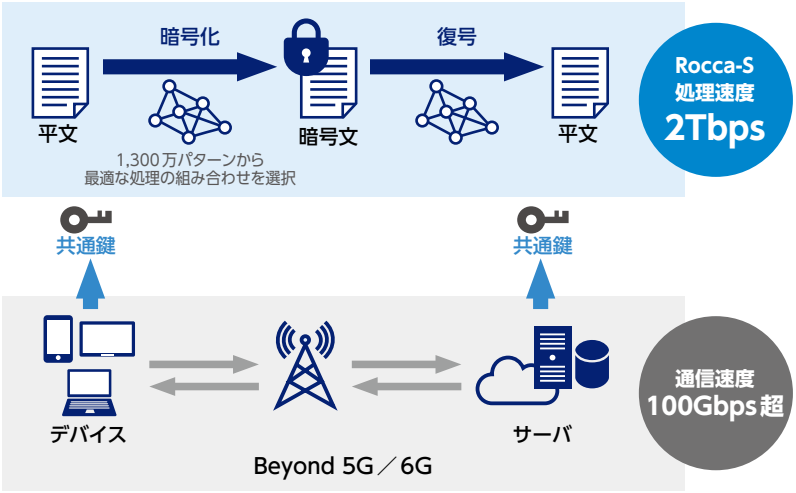
これまで、暗号技術によりさまざまなデータを保護してきましたが、5Gの次の世代であるBeyond 5G／6G時代には、新たな暗号技術が必要となります。その一つの課題は、Beyond 5G／6G時代の通信速度への対応です。現在の5Gの通信速度は最大でも10Gbps程度ですが、Beyond 5G／6Gでは100Gbpsを超える通信速度になるといわれています。現行の共通鍵暗号では、最大でも数10Gbps程度の処理性能にとどまっており、このままでは暗号化の処理が通信処理のボトルネックとなります。そのため、Beyond 5G／6Gの通信速度と同等あるいはそれ以上の処理性能を持つ共通鍵暗号が求められています。もう一つの課題は、量子コンピューターへの対応です。量子コンピューターは、量子力学の原理を用いて複数のデータを同時に処理し、現在のコンピューターでは時間がかかる複雑な計算も短時間で解く能力を持つコンピューターです。しかし、その登場により、RSA暗号を含む現行の公開鍵暗号は現実的な時間で破られる可能性が示されています。長らく量子コンピューターは理論上の存在とされ、実現は難しいといわれてきましたが、多くの組織での研究開発が進み、その実現可能性が高まっています。このような将来の状況を踏まえ、アメリカ国立標準技術研究所（NIST）は2016年に量子コンピューターに対する攻撃に耐えうる新しい公開鍵暗号を公募し、その標準化を進めています。共通鍵暗号についても、量子コンピューターに対する解読耐性を確保するため、鍵を長くする必要があります。現在は128ビットの鍵が一般的ですが、その2倍である256ビットの鍵が必要となると考えられています。鍵を長くすると暗号化の処理が遅くなるため、安全性と性能を両立する共通鍵暗号の開発が求められています。

そのため、KDDI総合研究所は兵庫県立大学と共同で、処理速度と対量子コンピューター耐性の両方を兼ね備えた新しい共通鍵暗号方式「Rocca-S」を開発しました。このRocca-Sを通じて、量子コンピューターへの耐性と処理速度という、二つの課題を同時に解決することが可能となりました。従来の暗号方式ではデータを順序立てて処理することで暗号化を行っていましたが、Rocca-Sでは複数の処理を同時に行うことで高速化を実現しました。具体的には、ハードウェア実装では2Tbpsを達成するとともに、市販のパソコンにおけるソフトウェア実装でも2023年8月現在の世界最速となる200Gbpsの速度を達成し、スマートフォンでも90Gbps以上の速度を記録しています。また、Rocca-Sは量子コンピューターによる解読に備えて256ビットの鍵に対応しており、現在知られている攻撃に対する安全性も確認済みです。さらに、データが途中で改ざんされていないかを検知する機能も備えているため、セキュリティ面でも大きな進歩を遂げています。

Rocca-Sの特徴



先端技術



Rocca-Sは複数ブロックを一括して並列処理し、各ブロックに対する演算処理量を均等にすることで、並列化による高速化の効果を最大限に引き出しています。また、撹はん処理に現行の標準暗号AESの部品を活用することで、サーバ、パソコン、スマートフォンに搭載されている専用のハードウェア命令（AES-NIなど）を用いた高速なソフトウェア実装が可能となります。

Rocca-Sは設計にあたっては、もととなるアイデアから導き出される1,300万通りもの構成候補を全て評価し、最適な方式を選定しました。数ヵ月にわたるコンピューターでのシミュレーションにより、1,300万通りの中から最も安全性が高い4つの候補を選び出しました。その上で、4つの候補を実際に実装して試験し、最も性能が高い候補をRocca-Sとして選定しました。2023年8月の時点では、Rocca-Sは世界最速の暗号方式として評価されており、その技術開発は総務省からも支援を受けています。今後はさらなる高速化を目指しつつ、実用化に向けた研究を加速させ、Rocca-SをBeyond 5G／6G時代の国際標準にすることを目指します。

暗号技術の最前線、高速化と安全性の両立を目指す研究者の挑戦

インフラの進化に伴い、なぜ高速な暗号が求められるのでしょうか？

福島：現在、5Gなどの通信システムでは、お客さまがやりとりするデータを暗号により保護しています。これまでは、暗号の処理性能が通信速度を上回っていたため、暗号の処理性能が問題となるケースは限られていました。しかし、2030年ごろにサービス開始が予定されている6Gでは、通信速度が大幅に向上することが見込まれています。その結果、現状のままでは、暗号の処理が追いつかなくなる可能性があります。そのため、暗号が通信性能の足を引っ張らないように、高速な暗号が必要となります。Rocca-Sは、ソフトウェア実装で200Gbps、ハードウェア実装で2Tbps超という、世界最速の性能を実現し、6Gで目標とする通信速度を大幅に上回っています。

世界最速のRocca-Sを設計するにあたり、苦労した点があれば教えてください。

仲野：暗号の設計においては、安全性が何よりも重要です。処理を減らすことで性能は向上しますが、その一方で安全性が低下する可能性もあり、性能と安全性を両立することは非常に難しい課題です。今回の研究開発では、他のものと比べ圧倒的に高速な暗号を作ることを目指しました。そのため、高速な暗号の1,300万通りもの候補を準備し、その全てについて安全性を検証しました。3ヵ月以上にわたりコンピューターを使って検証を続けた結果、わずか4つの安全性を満たす候補が見つかりました。内部構造を少し変更するだけで安全性や性能が大幅に変わるため、最適な候補を見つけるのに苦労しました。

Rocca-Sの安全性について、どのような検証が行われましたか？

仲野：既存の攻撃に対する安全性を、一つひとつ丁寧に検証しました。また、従来のコンピューターによる攻撃に加え、量子コンピューターによる攻撃に対しても安全であることを確認しています。

最後に、今後の展望について教えてください。

福島：今後は、Rocca-Sの国際標準化に向けて取り組み、KDDIの暗号を6G時代の標準暗号として、世界中で幅広く活用していただくことを目指します。引き続き、通信技術のさらなる進化や信頼性の向上に貢献できる研究開発を推進していきます。

KDDI総合研究所　セキュリティ部門　**仲野 有登**（写真・左）
KDDI総合研究所　セキュリティ部門　**福島 和英**（写真・右）

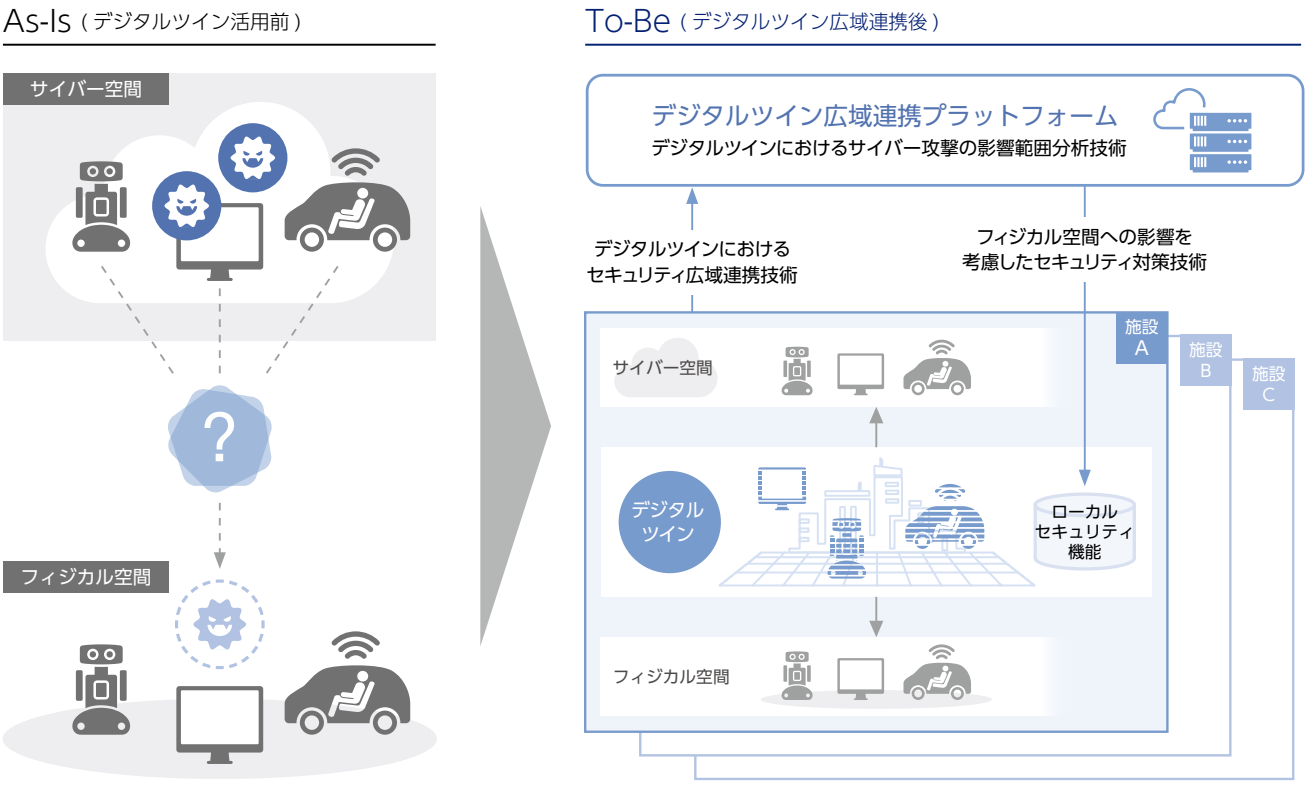
4 デジタルツインによるIoTセキュリティ基盤

Beyond 5Gの進展に伴い、サイバー空間とフィジカル空間が融合することが予想されます。これにより、サイバー攻撃の影響がフィジカル空間にも拡大し、その影響が増大する可能性があります。また、デジタルツイン技術の開発が進むことにより、フィジカル空間の状況をサイバー空間上で再現できるようになったことで、物体や人間の動きを分析し、シミュレーションすることが可能になっています。KDDIでは、このデジタルツインをサイバーセキュリティ対策に活用することで、フィジカル空間で発生したサイバー攻撃の影響を把握し、適切な対策を講じることができるよう研究開発を行っています。

現在では、IoT機器が社会全体に広く浸透し、重要なインフラを含む多くの場所で利用されています。このような状況下で、多数のIoT機器で共通して利用されているソフトウェアやハードウェアに悪用可能な脆弱性が発見された場合、それらがどの製品に組み込まれ、どの場所や状況で使われているかを把握することが重要となります。

しかし、現状では図1の左側のイメージ図のように、サイバー空間上で脆弱なネットワーク機器を見つけたとしても、それがどの製品に使用され、どこで使用されているかを特定するのは困難です。我々の研究では、図1の右側のイメージ図のように、さまざまな場所で構築・運用されるデジタルツインの広域連携プラットフォームを介してデジタルツインで再現したシミュレーション同士を連携させ、セキュリティ情報を共有します。そして、各デジタルツインが把握しているフィジカル空間の情報を用いて、危険なデバイスの存在を補足し、その影響を評価することで、適切な対策を行えるようなシステムの構築を目指しています。

図1 デジタルツインのセキュリティ活用により目指す世界



サイバー空間上の攻撃がどのフィジカル空間に影響を及ぼすか抽出が難しく、フィジカル空間への影響が拡大する恐れがある

デジタルツインの活用とその広域連携により、サイバー空間上の攻撃とフィジカル空間へのマッピングが可能になり、フィジカル空間への影響を最小化できる

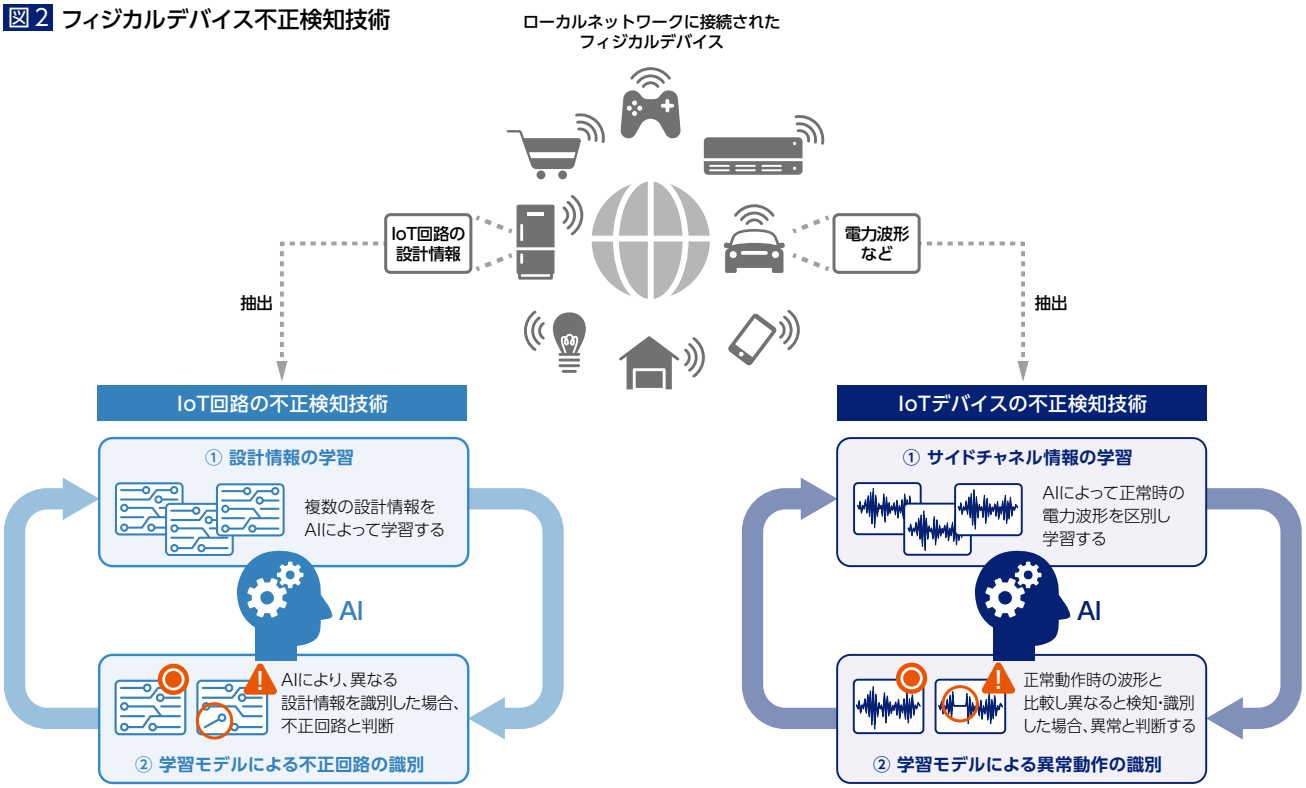
先端技術

この研究には、サイバー空間上の観測技術の高度化や、不正ICチップなどのハードウェアに関する脅威情報の把握、デジタルツインの活用・連携に関する検討、実環境での実証などのさまざまな研究課題があり、KDDI総合研究所を中心に、横浜国立大学、早稲田大学、芝浦工業大学の４研究機関が協力して研究開発を進めています。

Beyond 5G時代には広大なアドレス空間を持つIPv6の利用が一層進むと考えられており、サイバー空間上でのネットワーク機器の探索や脆弱な機器の発見が困難になります。また、脆弱性を持つネットワーク機器が発見された際に、それがどんな製品であるかを特定し、脆弱性の影響の大きさや取りうる対策を把握できるようにする必要があります。こういった、IPv6利用IoT機器の探索技術や、探索結果から機器の製品やバージョン情報などを特定し、当該機器の有する機能を把握可能にするデバイスプロファイリング技術などの研究開発を進めています。

近年、サプライチェーンセキュリティの問題として、不正なハードウェア部品の組み込みが懸念されており、不正な部品の検出や、それが組み込まれた製品の特定は重要な課題となっています。そこで、ICチップの回路情報から不正を検知する不正回路検知技術（図２左）や、IoT機器の動作時の電力波形などから不正な動作を検知する不正デバイス検知技術（図２右）の研究開発に加え、ハードウェア部品と製品の関係を保持するリポジトリを構築し、不正な部品が見つかったときにその影響が及ぶ製品を的確に把握可能にする取り組みを進めています。

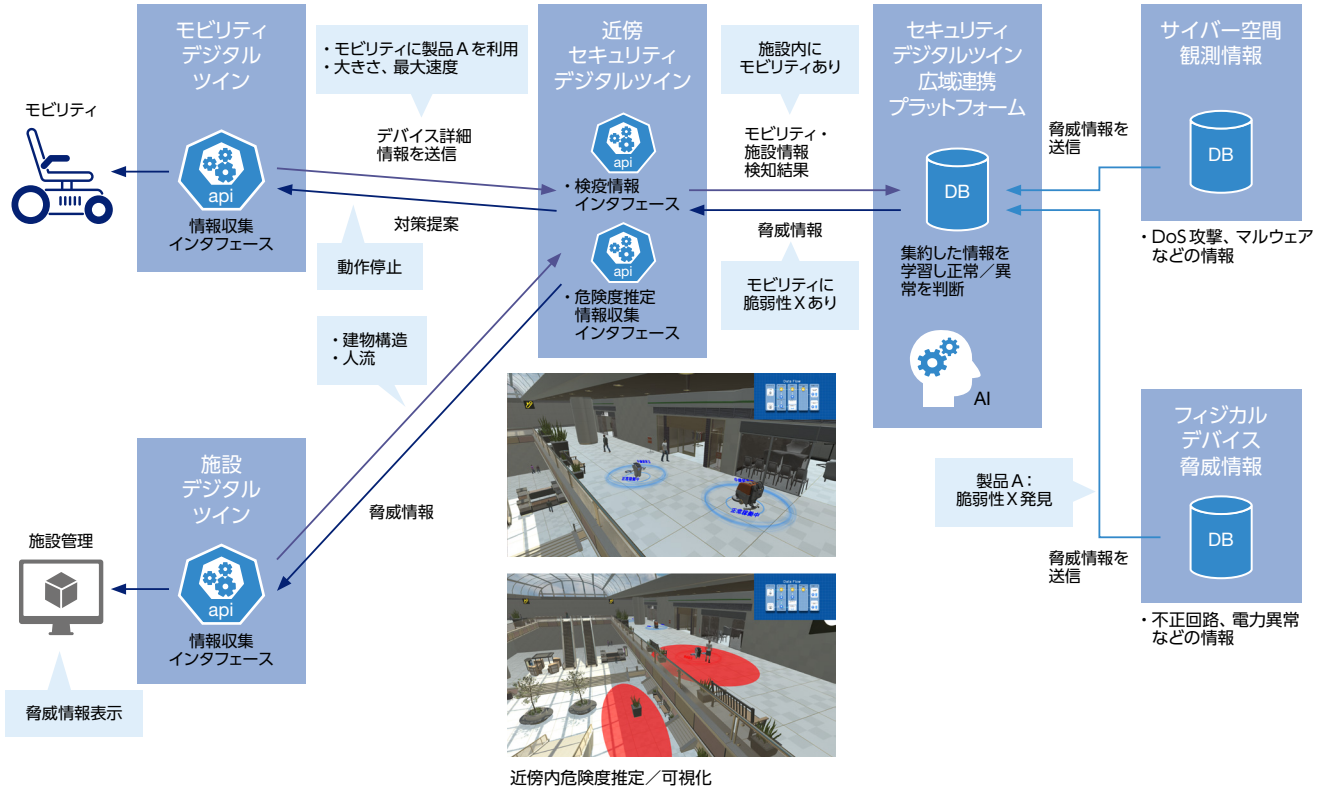
図２ フィジカルデバイス不正検知技術



こうした技術により把握した脅威情報をさまざまな場所のデジタルツインと共有し、セキュリティ対策に活用するためのプラットフォームとして現在開発中のプロトタイプの構成を示したものが図3です。脆弱なソフトウェアや不正なハードウェア部品が発見されたときに、それらが組み込まれた製品の情報を、セキュリティデジタルツイン広域連携プラットフォームと近傍セキュリティデジタルツインを介して多数のサービスデジタルツインと共有し、デジタルツイン上で捕捉、検知された該当製品の利用状況や周辺状況を踏まえた上で影響の大きさを評価し、適切な対応をとれるようにすることを目指しています。

例えば、通信機能の性能低下を引き起こす問題のあるネットワークコントローラが発見された場合に、それが組み込まれた製品の種別によっては対応の緊急性が低い場合がある一方で、ネットワーク制御される乗り物に組み込まれており緊急の対応が必要となる場合もあります。デジタルツインを活用することで、新たに発見された脆弱性情報や脅威情報の影響の大きさを、それらが影響を及ぼす可能性のある各現場の状況に応じて評価し、対策の優先順位付けや適切な対策手段の選択をサポートすることが可能となります。そのための情報連携、活用の仕組み作りを、この研究プロジェクトに参加している他の研究機関とともに進めています。

図3 デジタルツインによるサイバー・フィジカル連携セキュリティ基盤



セキュリティ事業への取り組み

1 マネージドトラスト

■ ゼロトラスト型セキュリティとは

テレワークの浸透・定着と軌を一にするように大きな注目を集めるようになったのが「ゼロトラスト」というセキュアな情報システム設計の考え方です。テレワークでは、ノートパソコンなど会社から貸与されたデバイスを持ち帰って、パブリックなインターネットから社内のネットワークに接続することも珍しくなくなりました。クラウドの活用も加速度的に広がり、従来の「境界防御モデル」でサイバーセキュリティを担保する、つまり社内外の境界上でセキュリティ対策を行い、社内ネットワークを安全に保つことを前提として情報資産をその中でのみ活用するという発想ではビジネスや業務が成り立たなくなってきています。ゼロトラストは社内ネットワークの内部と外部を問わず、全てのアクセスを都度検証することでセキュアな状態を保つというコンセプトで、次世代のあるべきセキュリティの考え方と注目されています。

KDDIでは働き方改革の一環として、2005年ごろから段階的に多様な働き方の実現に向けた取り組みを進めています。そうした中、在宅勤務・テレワークのデバイスやクラウドサービスの保護を目的に、2019年秋からゼロトラストの導入を検討し始めました。ところが、コロナ禍によって在宅勤務・テレワークを実施する社員が4倍となり、ビデオ会議の開催数は70倍以上と急激に増えたため、境界型のセキュリティでは業務に支障を来すようになりました。そこで計画を前倒しにして、ゼロトラストの全社展開を実施しています。

“利便性”と“セキュリティ”の両立を図って検討

計画前倒しで 全社（国内）展開へ
下期計画 1,000台 → 見直し後 14,000台

接続性／安定性の向上
接続断がなくなり、安心して商談に臨める環境

作業効率向上
軽快な動作で、出社時と同等の効率

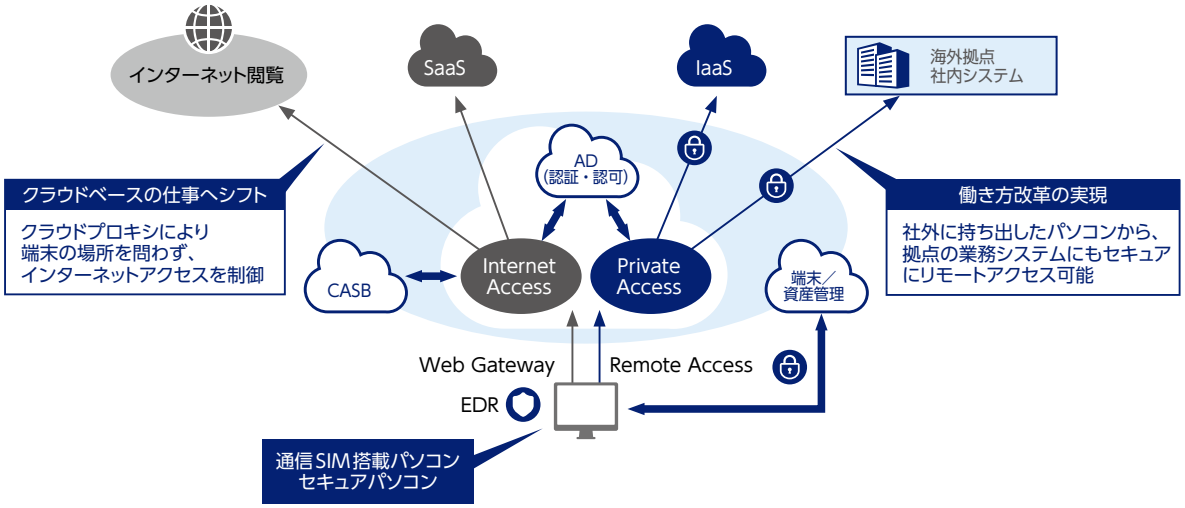
クラウドベースの仕事へシフト
場所を問わずどの端末でも業務可能

セキュリティ向上
万が一紛失したときにも遠隔管理ができ、安心

2020年11月からは全社合計1万3,800台に及ぶデバイスの導入・配布を開始し、2021年2月までに国内拠点のゼロトラストの導入を完了しました。クラウドソリューションを組み合わせることで迅速に導入ができ、テレワーク、オフィスワークを問わず、ストレスなく利用できるという効果が得られています。その後、国内で培ったノウハウをベースに、数年をかけてゼロトラストを海外現地法人にも導入を進め、22ヵ国49拠点へ海外展開をしました。

■KDDIのゼロトラストモデルの構成

LTE SIMを搭載したパソコン、FAT PCを中心に、ゼロトラストコンポーネントであるSWG、エンドポイントセキュリティ、CASB等のソリューションを搭載し、いつでもどこでもクラウド環境や社内リソースへセキュアに接続できる環境を実現しています。



■KDDIが提案する「マネージド ゼロトラスト」とは

KDDIでは、ゼロトラストを実現する上で必要となる「オペレーション」「クラウド・アプリ」「セキュリティ」「ID」「ネットワーク」「デバイス」という6つのコンポーネント別に多様な製品・サービスを揃えるとともに、これらを最適なかたちで組み合わせて、安心安全かつ多様な働き方をワンストップで支援します。

「マネージド ゼロトラスト」6つのコンポーネント

■国内外のお客さまのセキュリティ対策を支援

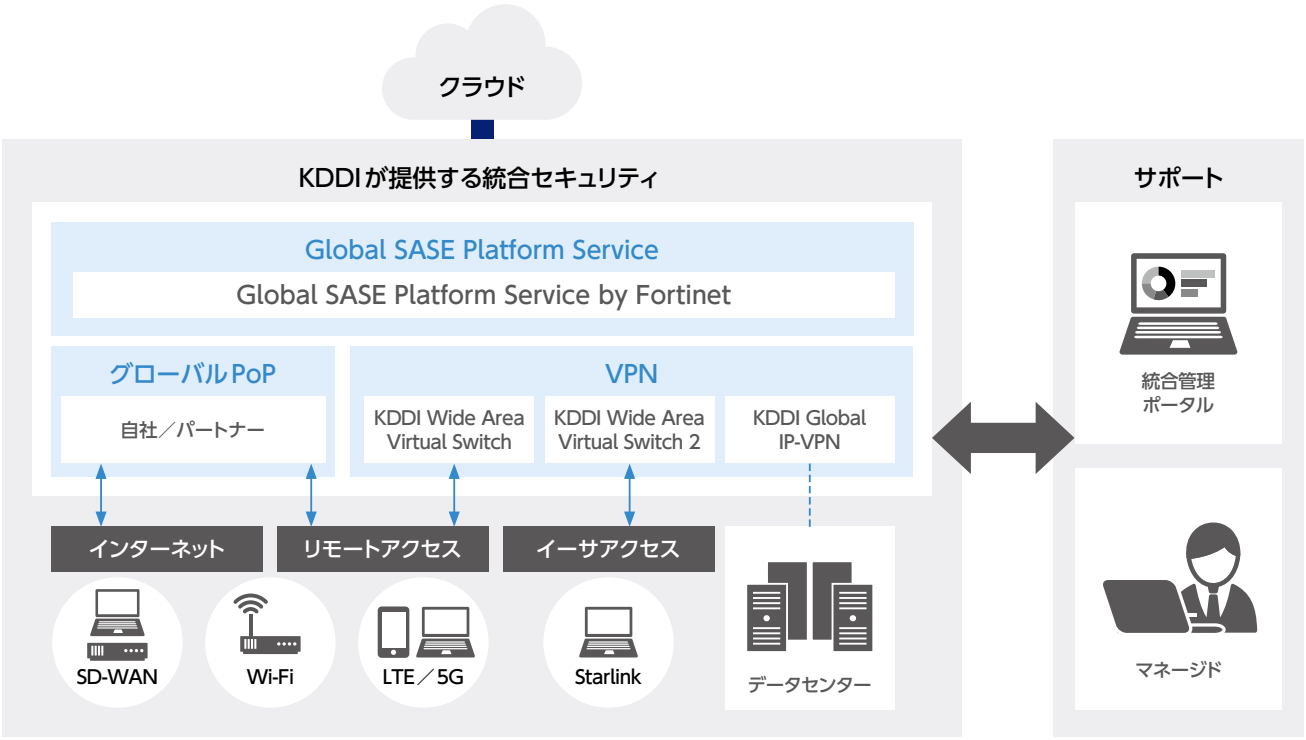
KDDIが社内で培ったノウハウを活かして、国内外問わず法人のお客さまのセキュリティ対策を、コンサルティングからシステムインテグレーション、運用支援までワンストップで支援します。

コンサルティング	システムインテグレーション	運用支援
企画・構想に関する策定支援	プロジェクトマネジメント推進	IT運用業務の代行
セキュリティ・クラウド移行などの調査・アセスメント	ネットワーク／クラウド／セキュリティコンポーネントの提供・設計・構築支援	ITヘルプデスク
海外法規制対応の支援		マネージドセキュリティサービス

セキュリティ事業への取り組み

■Global SASE Platform Service by Fortinet

国内外から高セキュリティなリモートアクセス環境を実現するほか、検討から導入、運用・保守までを国内外の拠点においてワンストップで提供します。主なセキュリティ機能として「セキュアWEBゲートウェイ」「ゼロトラストネットワークアクセス」次世代デュアルモード「クラウドアクセスセキュリティブローカー」「Firewall-as-a-Service」を展開します。



2 LACマネージドサービス

株式会社ラック（LAC）は、システムインテグレーションとサイバーセキュリティの豊富な経験と最新技術で、社会や事業のさまざまな課題を解決するサービスを提供しています。創業当初から金融系や製造業など日本の社会を支える基盤システムの開発に携わり、近年ではAIやクラウド、テレワークなど、DX時代に適した最新のITサービスも手掛けています。また、日本初の情報セキュリティサービス開始から25有余年にわたり、国内最大級のセキュリティ監視センターJSOC、サイバー救急センター、脆弱性診断、ペネトレーションテストやIoTセキュリティなど、常に最新のサイバー攻撃対策や事故対応の最前線に立ち、情報セキュリティ分野のリーディング企業としても成長を続けています。「KDDI セキュリティソリューション by LAC」は、KDDIと情報セキュリティでトップクラスであるLACのノウハウを融合し、コンサルティング、セキュリティ診断、セキュリティ監視・運用で、充実したセキュリティソリューションを提供します。

グループ状況、第三者評価

1 セキュリティ事故実績

情報セキュリティに関する重大事故の件数

KDDIは、グループ全体で情報セキュリティの強化に努め、情報セキュリティリスクの低減に取り組んでいます。

情報漏えいに関しては、故意・不注意に関わらず、就業規則に基づき厳正に対処することとしており、周知・徹底しています。

情報セキュリティに関する重大事故の件数

項目	バウンダリ	カバレッジ(2022年度)	単位	2018年度	2019年度	2020年度	2021年度	2022年度
外部からのサイバー攻撃に伴う電気通信サービスのサービス停止件数	単体	ー	件	0	0	0	0	0
外部からのサイバー攻撃に伴う個人情報流出件数				0	0	0	0	0
個人情報の漏えい件数				0	0	0	0	0

2 第三者評価・認証

ISMS 認証状況

KDDIグループでは、情報セキュリティに関連する第三者評価・認証に積極的に取り組んでいます。

情報セキュリティマネジメントシステム国際規格ISMS認証（ISO／IEC27001：2013）※1を取得した組織を持つ主な会社は、以下の通りです。

ISMS認証取得組織を持つグループ会社

KDDI株式会社

移動通信事業
沖縄セルラー電話株式会社
株式会社ソラコム

固定通信事業
中部テレコミュニケーション株式会社

コンテンツ・メディア事業
株式会社mediba

リサーチ・先端技術開発
株式会社KDDI総合研究所
株式会社KDDIテクノロジー

ネットワーク建設・運用・保守事業
KDDIエンジニアリング株式会社
日本通信エンジニアリングサービス株式会社※2

コンタクトセンター・ITソリューション事業
アルティウスリンク株式会社

セールス・マーケティング
KDDIまとめてオフィス株式会社※2
KDDIまとめてオフィス関西株式会社※2
KDDIまとめてオフィス中部株式会社※2
KDDIまとめてオフィス東日本株式会社※2
KDDIまとめてオフィス西日本株式会社※2

DX関連事業
アイレット株式会社
株式会社KDDIウェブコミュニケーションズ

KDDI直営店舗運営
KDDIプリシード株式会社

特例子会社
株式会社KDDIチャレンジド※2

その他
一般財団法人KDDIグループ共済会※2
KDDI企業年金基金※2
KDDI健康保険組合※2

海外グループ会社
KDDI EUROPE Ltd.
KDDI Deutschland GmbH
KDDI FRANCE SAS
KDDI HONG KONG LIMITED
KDDI Asia Pacific Pte Ltd
TELEHOUSE Deutschland GmbH
TELEHOUSE International Corp. of Europe Ltd. Paris Branch
Telehouse International Corporation of Europe Ltd.
TELEHOUSE BEIJING Co.,ltd
TELEHOUSE BEIJING BDA Co.,ltd
Mobicom Corporation LLC

※1 情報セキュリティに対する第三者適合性評価制度。情報セキュリティ全体の向上に貢献するとともに、国際的にも信頼を得られる情報セキュリティレベルの達成を目的とした制度
※2 KDDI株式会社のISMS認証適用範囲に含みます

KDDIグループの概要

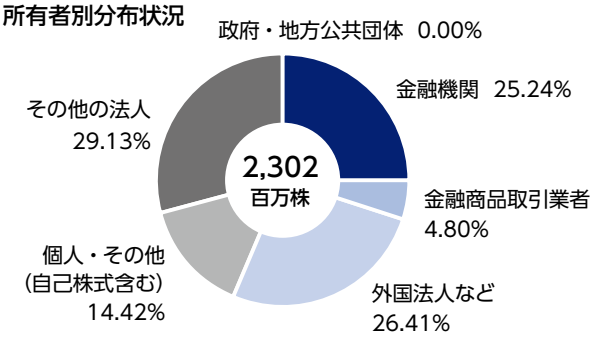
1 会社概要 (2023年3月31日時点)

社名	KDDI株式会社
創業	1984年6月1日 (KDDIは2000年10月 DDI、KDD、IDOの3社合併により発足)
事業内容	電気通信事業
本社所在地	〒102-8460　東京都千代田区飯田橋三丁目10番10号
本店所在地	〒163-8003　東京都新宿区西新宿二丁目3番2号
代表取締役社長 CEO	髙橋 誠
資本金	141,852百万円
社員数	49,659名 (連結ベース)

2 株式の状況 (2023年9月30日現在)

証券コード	9433
会社が発行する株式の総数	4,200,000,000株
発行済株式総数	2,302,712,308株
株主総数	429,078名

所有者別分布状況



大株主

氏名又は名称	所有株式数（株）	持株比率※1 (%)
日本マスタートラスト信託銀行株式会社（信託口）	342,866,800	16.37
京セラ株式会社	335,096,000	16.00
トヨタ自動車株式会社	253,094,600	12.08
株式会社日本カストディ銀行（信託口）	145,769,400	6.96
STATE STREET BANK WEST CLIENT - TREATY 505234	32,653,275	1.55
JPモルガン証券株式会社	25,097,071	1.19
SSBTC CLIENT OMNIBUS ACCOUNT	22,172,909	1.05
JP MORGAN CHASE BANK 385781	22,090,633	1.05
三菱UFJモルガン・スタンレー証券株式会社	19,647,001	0.93
STATE STREET BANK AND TRUST COMPANY 505103	18,533,969	0.88

※1 当社は、自己株式 208,402,549 株を保有しておりますが、上記大株主から除いております。持株比率は自己株式を控除して計算しております。なお、自己株式には役員報酬 BIP 信託が所有する当社株式（1,074,019 株）を含んでおりません。また、持株比率は小数点第三位を切り捨ての上、算定しています。

KDDI株式会社
KDDI CORPORATION
https://www.kddi.com/