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2022

Cybersecurity Annual Report 2022

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

01　目次・編集方針

02　情報セキュリティ委員長メッセージ

03　サイバーセキュリティ動向

05　情報セキュリティガバナンス

10　セキュリティ施策（サイバー攻撃対策）

14　セキュリティ施策（個人情報保護対策）

16　セキュリティ施策（サービス不正利用対策）

17　研究開発の推進

21　法人のお客さま向けセキュリティソリューション

24　第三者評価・認証

25　KDDIグループの概要

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2022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、これに対する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で自動化する技術開発を進めています。また、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。

当社は、複雑化・高度化する新たな脅威への対応を進化させ続けることで、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いきます。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
兼 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）

サイバーセキュリティ動向

近年、セキュリティ技術の進化、並びに、フレームワーク、法規制の整備が進んでいますが、一方でサイバー攻撃手法の高度化・巧妙化も著しく進んでおり、攻撃と対策の応酬の繰り返しが続いています。

企業のセキュリティ投資は年々増加し、多様なセキュリティ対策が導入されていますが、大規模な個人情報漏洩、経営を脅かす機密情報漏洩、ランサムウェア感染による事業停止など、世間を騒がすセキュリティ事案は後を絶ちません。また、必ずしも高度な手法を用いていないサイバー攻撃、パッチを当てていない機器の悪用や、暗号化されていない情報の外部への流出、パスワード・ID漏洩によるインシデントなど、「厳密に管理すれば防げていたはず」の事案も国内外を問わず数多く発生している状況です。

攻撃の進化と必要な防御策

サイバー攻撃の歴史を振り返ると、2000年代初頭までは、主に個人を狙ったコンピュータウイルス、ワーム、マクロ型ウイルス、トロイの木馬などの端末に入り込んで予期せぬ動作を引き起こす種類の攻撃が多く、世間を騒がせて自己満足を得ることがサイバー攻撃の主な目的となっていました。一方で、法人を狙った攻撃も発生し始め、未公表の脆弱性を利用したゼロデイ攻撃による被害も散見されるようになりました。このような攻撃への対応としては、端末防御のためのパーソナルファイアウォールやアンチウイルスなどのエンドポイント対策が主体となっていました。

2010年代になると特定の企業や政府をターゲットにした標的型攻撃が発生し始め、サイバー攻撃による被害がより深刻化していきました。代表的な例として、標的型メールを契機としたウイルス感染で個人情報が漏洩した、日本年金機構の年金管理システムへのサイバー攻撃が挙げられます。このような標的型攻撃への対応としては、不審メールを分離するメールアイソレーションや、DDoS・各種インジェクション攻撃を防ぐためのNGFW／IDS／ISP／WAFなどの境界型防御が有効であり、エンドポイント対策と合わせて実施する必要があります。

近年の攻撃の特徴と必要な防御策

2010年代後半からは、ランサムウェア攻撃、暗号資産（仮想通貨）を発掘するクリプトジャッキング、ダークウェブによる攻撃ツールの流通化などによって、サイバー攻撃が金銭取得などを目的として産業化していく傾向がより強まってきました。また特定の団体・国家などが政治・信念を主張する際の道具として利用されたり、知的財産の窃取や諜報活動の手段として用いられるようになりました。被害の規模もさらに拡大を続け、2017年に猛威を振るったランサムウェアWannaCryは、ファイル共有プロトコルSMBv1の脆弱性を悪用することで、150ヵ国30万台のPCに感染、国内大手企業においても工場の生産停止や取引先との受発注システムの停止などの被害が発生しました。このような自動感染活動により広がるランサムウェアなどの攻撃に対しては、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あるゼロトラスト防御が有効な考え方となります。

グローバルな社会課題

セキュリティ対策の需要が増えるなか、日本だけではなく、世界的にセキュリティ人材の不足が問題となっています。（ISC）[2]の報告※1によりますと、2021年に世界では272万人、日本では4万人のセキュリティ人材が不足しているとされています。

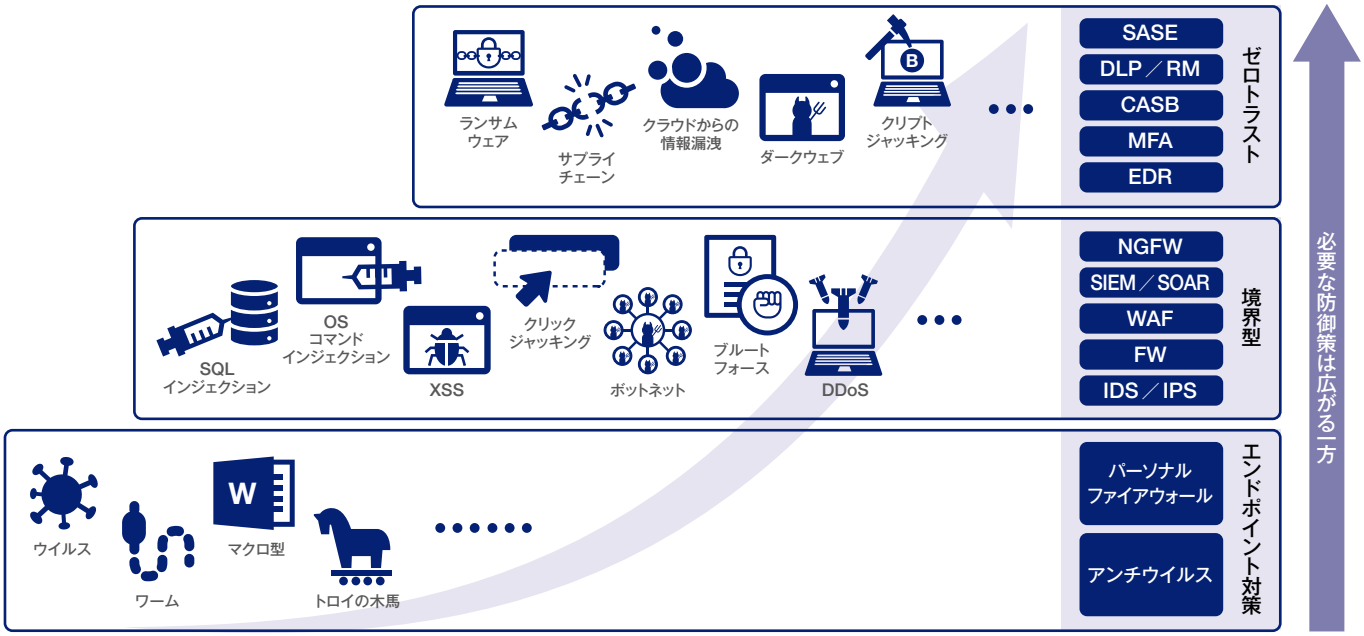
一方で、重要インフラによるICT技術の活用（デジタルトランスフォーメーション）やIoTの浸透により、サイバー攻撃は現実世界との関わりが以前より深くなってきており、人命や重要インフラの運営に 関わるサイバー攻撃※2も発生している状況です。

このように近年のサイバー攻撃は高度化・巧妙化が進み、その影響も極めて深刻化しており、サイバー攻撃から重要インフラなどの被害を防ぐために、社会全体の課題として、人材育成を含めたセキュリティ対策に取り組む必要があります。

※1 "A Resilient Cybersecurity Profession Charts the Path Forward - (ISC)² CYBERSECURITY WORKFORCE STUDY-", 2021,
https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

※2 人命や重要インフラの運営に関わるサイバー攻撃事例

2019年7月	米アラバマ州の病院がランサムウェア攻撃によって8日間全てのコンピュータが使用不能に陥った。その結果、分娩室にある胎児の心拍が監視できなくなり、その間に誕生した新生児が重度障がいになり、9ヵ月後に死亡した。
2020年9月	ドイツ、デュッセルドルフ大学病院がランサムウェア攻撃を受け、緊急搬送が必要な患者が予定搬送先から30km以上も離れた別の病院に搬送されることになり、治療が遅れたことで、その後死亡が確認された。
2021年5月	パイプラインを運営する米コロニアル・パイプライン社がサイバー攻撃を受け、数日操業停止になった。その結果、ガソリン供給が停止し、社会的な混乱が発生、ガソリンの平均価格の上昇にもつながった。



情報セキュリティガバナンス

高度化･巧妙化が進むサイバー攻撃への対応として、KDDIグループは情報セキュリティに関わるリスクマネジメントを極めて重要な課題として位置付け、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。本章では、KDDIの情報セキュリティ推進体制を始め、情報セキュリティ社内規程、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紹介します。

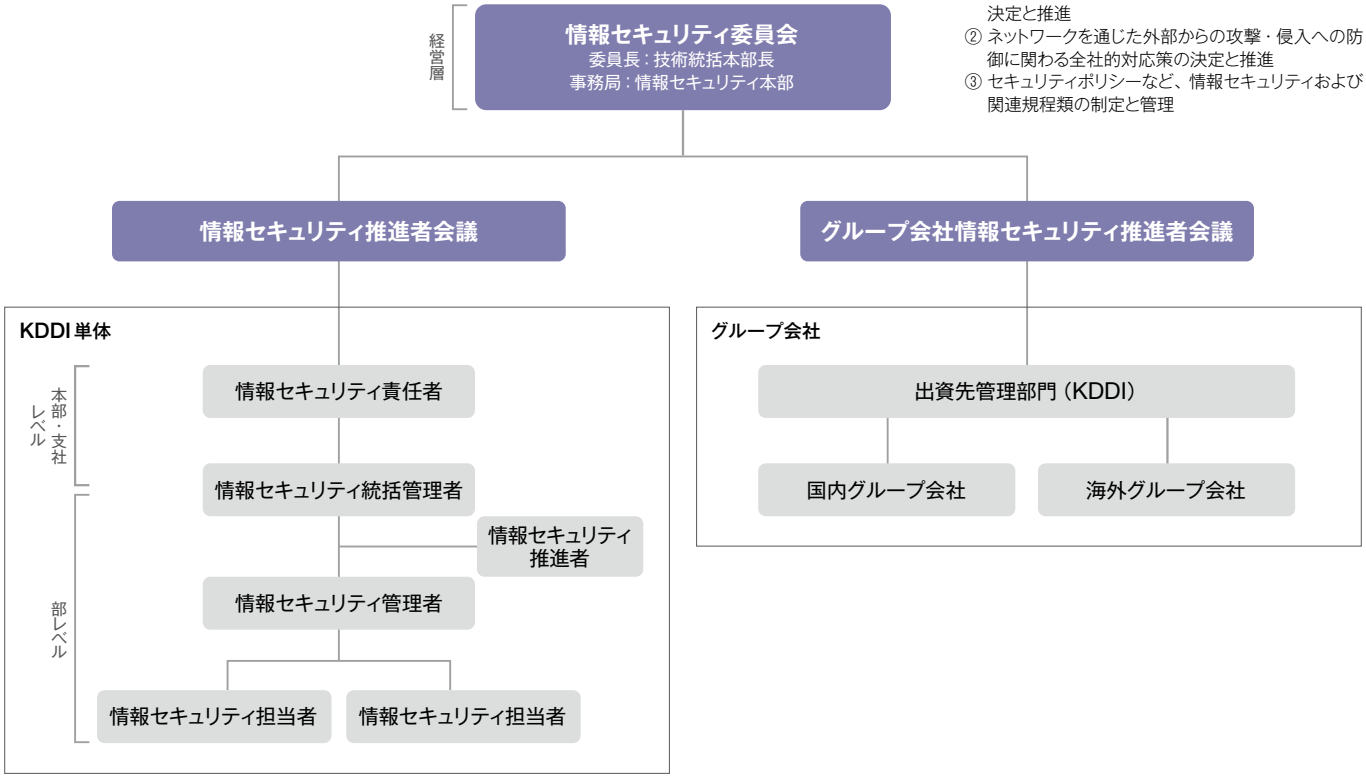
1 情報セキュリティ推進体制

KDDIおよびKDDIグループ全体での統一的な情報セキュリティの確保を目的に、技術統括本部長を委員長とし、経営層および営業・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」を設置しています。

また、情報セキュリティ委員会の配下に、KDDI単体および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するとともに、情報セキュリティ強化のための各種施策をグループ全体に迅速に展開できる体制を整備しています。

また、各グループ会社においても、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に関するリスク低減とその未然防止を図り、リスクに対する評価･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



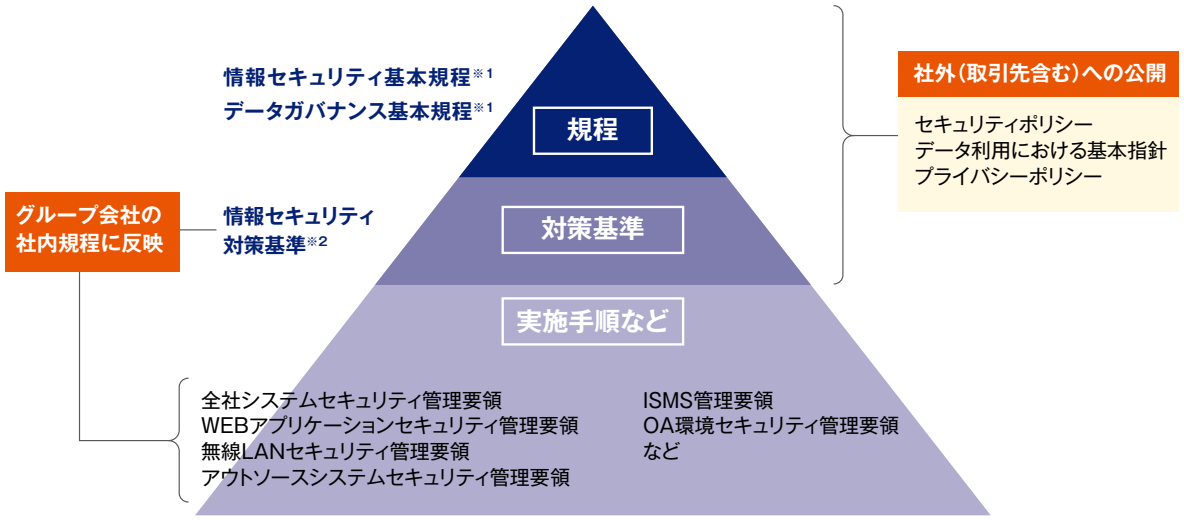
［情報セキュリティ委員会］の役割
① 内部からの情報漏洩防止に関わる全社的対応策の決定と推進
② ネットワークを通じた外部からの攻撃・侵入への防御に関わる全社的対応策の決定と推進
③ セキュリティポリシーなど、情報セキュリティおよび関連規程類の制定と管理

2 情報セキュリティ社内規程

KDDIの情報セキュリティに関する社内文書は、下図に示す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・対策基準においては、お客さま情報ならびに会社の機密情報を厳密に取り扱うとともに、情報漏洩リスクなどに対して、常に適切な防御措置を講じることにより、お客さまならびに関係者の信頼を得るため、社外公開版として「セキュリティポリシー」「プライバシーポリシー」を定め、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

社外（取引先含む）への公開

セキュリティーポリシー

KDDIは情報に対する適切な管理を重要な経営課題として認識し、情報セキュリティを確保するために、情報セキュリティ管理体制、情報セキュリティ対策の実施、情報セキュリティに関する社内規程の整備など、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」を定めています。

▶ 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に、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。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、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。KDDIは、本指針に基づき、パーソナルデータの取り扱いに関する方針として、「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/

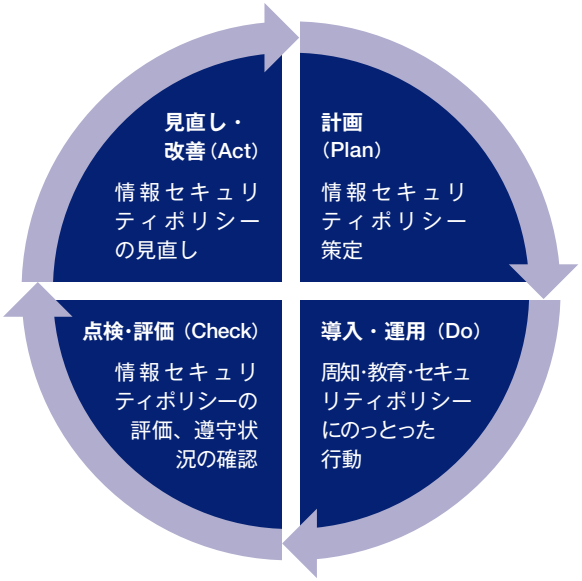
情報セキュリティガバナンス

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として、計画段階において情報セキュリティポリシーを策定するとともに、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）に従い、チェック・見直し・改善を図っています。

※1 ISMS認証（ISO／IEC27001：2013）。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。

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などが遵守され、適切に運用されているかを確認するため、以下3つの監査を実施しています。

システムセキュリティ監査

電気通信設備を新たに設置、改修する場合に、「全社システムセキュリティ管理要領」に遵守しているかどうか、専門部門の監査担当者によって監査を実施します。

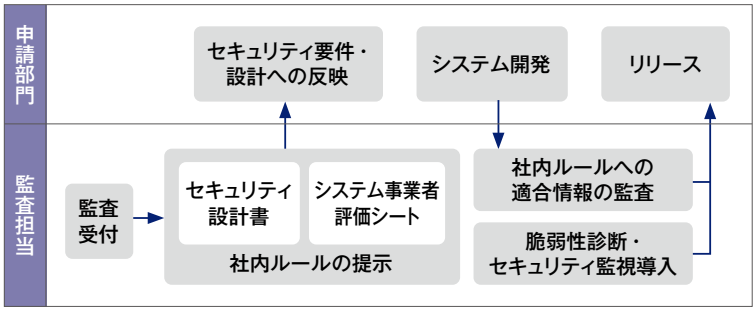
監査には、セキュリティ管理要領に記載された内容を一問一答の表形式にしたセキュリティ設計書を使用します。数百項目の監査要求事項があり、必須の要求事項に準拠していない場合は、システム構築担当に是正を求めます。

事業スピードが加速する中、短期間でリリースするシステムの増加や、過去に監査したシステムの機能追加・設備更改により、再監査を含む監査対象システム数は年々増加傾向にありますが、日々の業務改善やツールの整備を進めることで、効率的に対応しています。

セキュリティ監査の業務フローは右図の通りです。まず、事前問診票でシステムの構成を確認します。次に、セキュリティ設計書による書面の監査を実施します。

書面の監査の結果を踏まえ、リリース前にはネットワーク脆弱性診断、WEB脆弱性診断などを実施し、また不正侵入検知装置（IDS）などによるセキュリティ監視の仕組みを導入します。

セキュリティ監査の業務フロー



ISMS内部監査

KDDI ISMS認証範囲の各部門および関係各社に対し、「ISMS管理要領」および「統合ISMS内部監査手順」に従い、専門部門もしくは社内各組織より選出された監査担当者によって監査を実施しています。

ISMS内部監査ではKDDI ISMSで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、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ています。

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、改善を図っています。

業務委託先監査

KDDIが業務の全部または一部を委託している場合には、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に、年1回以上の頻度で業務委託先への監査を行い、管理体制の見直しなどを実施しています。また、これに加え専門部門の監査担当者による業務委託先特別監査も実施しています。

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では全従業員を対象に、eラーニングによるセキュリティ教育を毎年実施しています。最新のサイバー脅威動向や情報漏洩事例、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。

また、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。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。

その他にも、新入社員全員を対象とした情報セキュリティ基礎研修、ライン長を対象としたセキュリティマネジメント研修など、階層別にセキュリティ教育を行い、セキュリティ事故防止に向けた取り組みを進めています。

情報セキュリティガバナンス

セキュリティ専門人材の育成

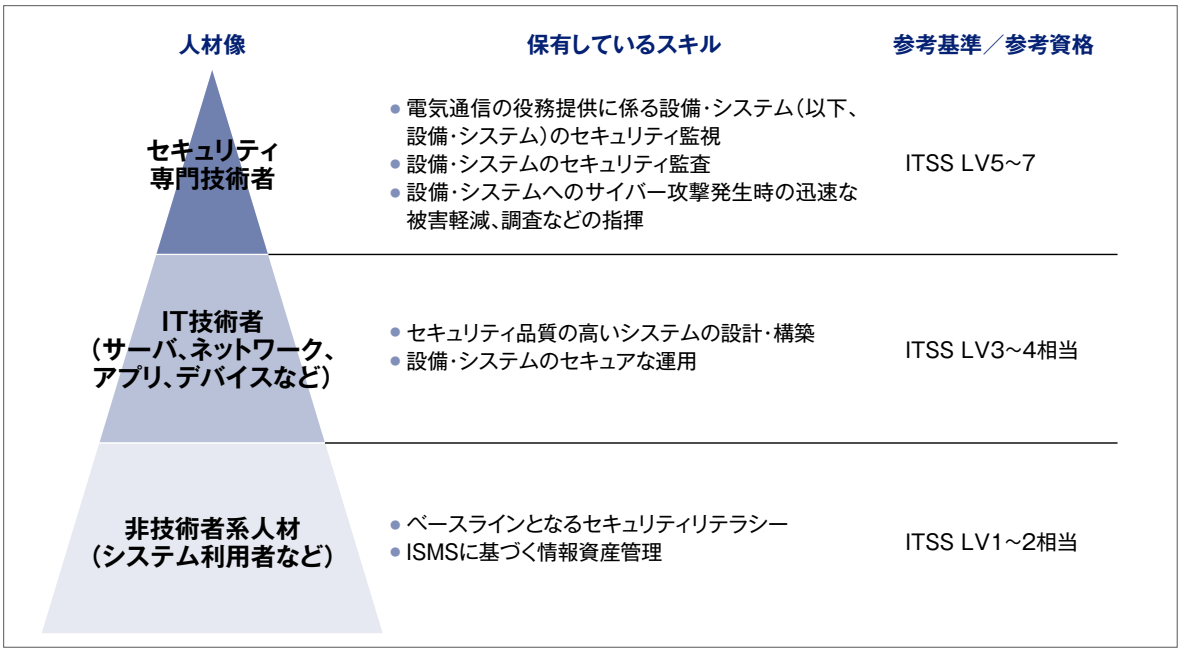
お客さまのデータや提供しているサービスをサイバー攻撃から守るために、サイバーセキュリティに係る人材の育成も必要となります。KDDIでは各階層に分け、体系的な育成にも取り組んでいます。

セキュリティを専門にする技術者は、社外専門機関のセキュリティトレーニングプログラムに参加し、セキュリティの専門性の向上を図るとともに、未知の攻撃やインシデントに対応するため、日々の実践・演習の中でプロフェッショナルとしてのスキル深化を図っています。

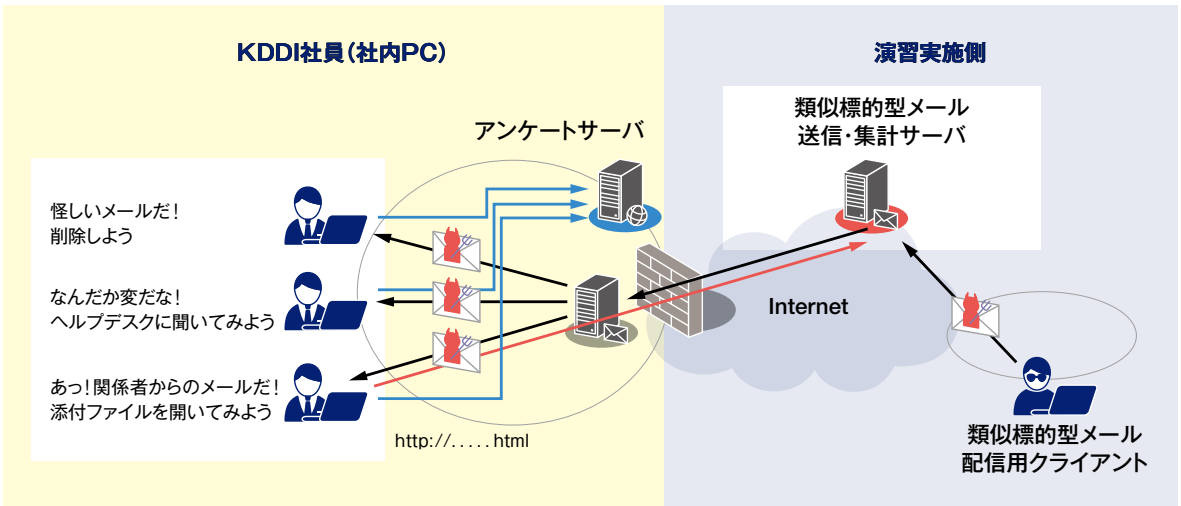
また、社内の人材育成プログラムを整備し、この中でIPA（独立行政法人情報処理推進機構）が運営する国家資格「情報処理安全確保支援士（登録セキスペ）」の取得を促しており、KDDIの資格登録者数は国内有数の人数となっています。

さらに、定期的にサイバー攻撃に対応するための演習を社内で実施しています。各演習の実施結果と参加社員からのフィードバックの収集・分析などを通して、社員のセキュリティ意識およびサイバー攻撃対応能力の維持・向上に努めています。

セキュリティ人材に求められるスキルと参考基準



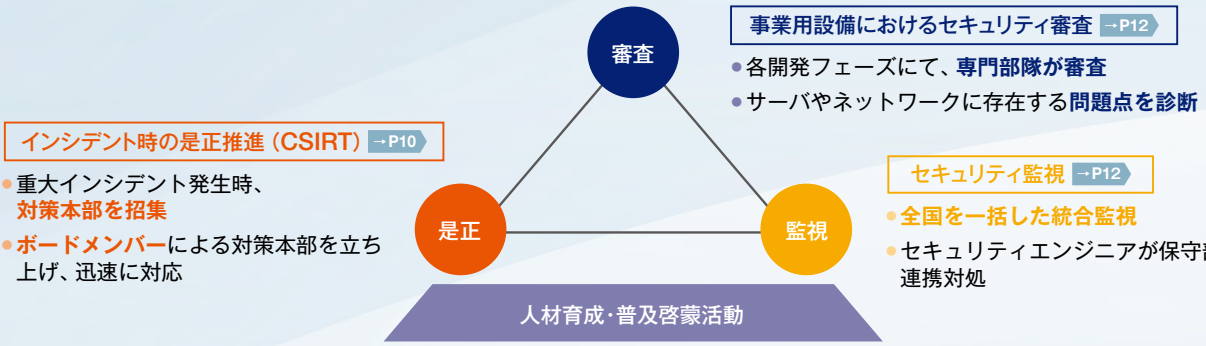
疑似標的型メール送信による演習例



セキュリティ施策（サイバー攻撃対策）

KDDIでは、サイバー攻撃に対する対策として「インシデント時の是正推進（CSIRT）」、「事業用設備におけるセキュリティ審査」、「セキュリティ監視」の3施策を柱としてセキュリティ対策の継続的な強化に努めています。

本章では3施策の具体的な取り組みについてご紹介します。



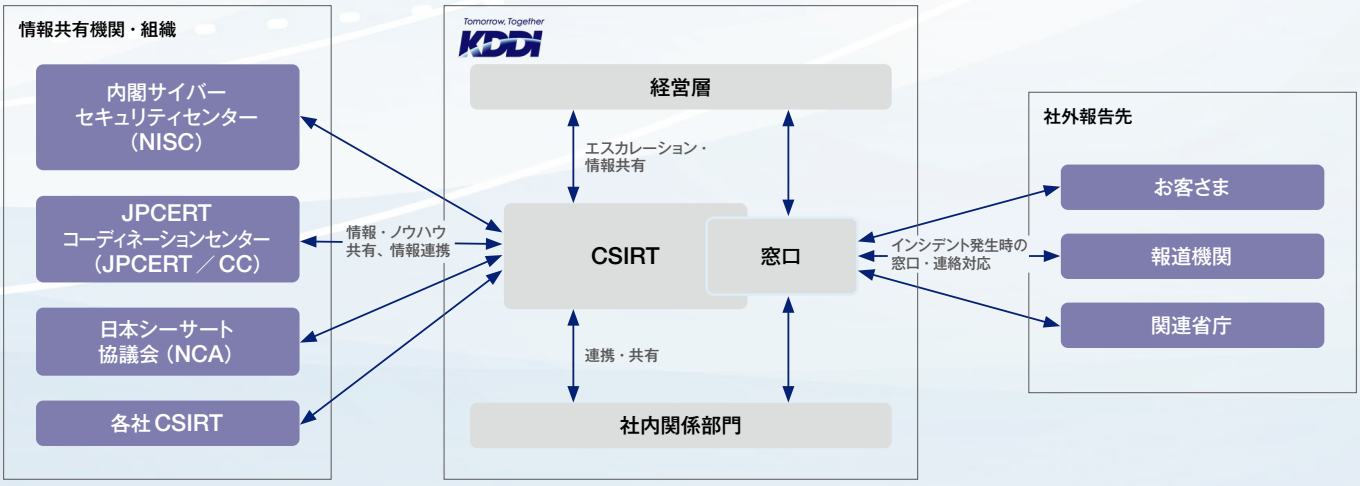
インシデント時の是正推進（CSIRT）

CSIRTとは

CSIRTとは、組織内をコーディネートしてセキュリティインシデント対応を行うための専門組織の通称であり、KDDIでは2013年にKDDI-CSIRTを設置しており、2018年からKDDIデジタルセキュリティ※1もKDDI-CSIRTに加え活動を行っています。

インシデントが発生した際は、KDDI-CSIRTが社内関係部署と連携し、原因調査や証拠保全などを行い、事態収束に向けた社内の統制を行います。また、平時はセキュリティインシデントの予防のため、サイバー攻撃や脆弱性などに関するさまざまな情報収集を行うとともに、内閣サイバーセキュリティセンター、ICT-ISAC、JPCERT／CCなどの社外セキュリティ機関、およびCSIRTのコミュニティであるFIRST（Forum of Incident Response and Security Teams）や日本CSIRT協議会にも参加し、緊密な組織間連携を行っています。

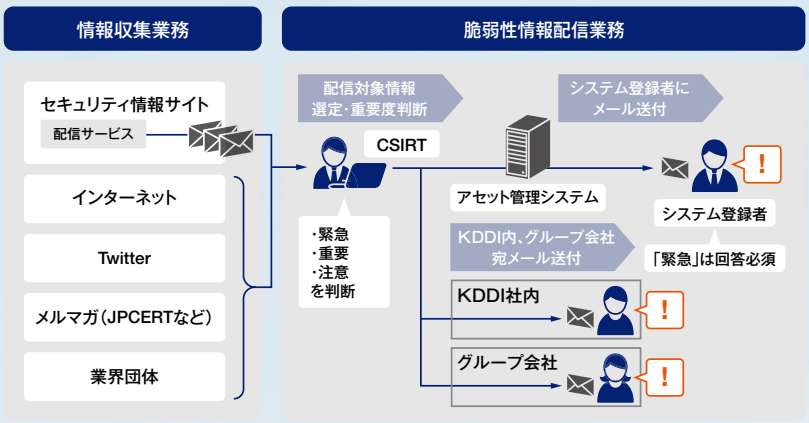
※1 KDDIデジタルセキュリティは、情報セキュリティ分野のリーディング企業である株式会社ラック（LAC）とKDDIが設立した会社で、KDDIのICTソリューションとLACの高いセキュリティ分析力・技術力を融合させることで、総合的なセキュリティソリューションをお客さまに提供するとともに、KDDIグループのセキュリティ対策強化に取り組んでいます。



セキュリティ施策（サイバー攻撃対策）

CSIRTの活動<脆弱性情報収集と配信>

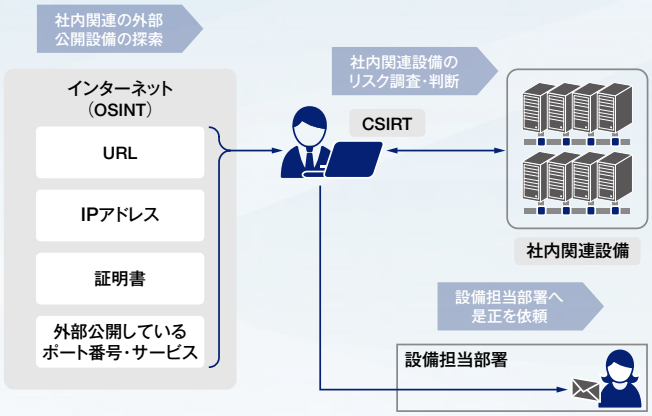
セキュリティ情報サイトなどから入手した脆弱性情報をKDDI-CSIRTから全社に展開し、システムへの影響有無を確認しています。影響がある場合にはKDDI-CSIRTに結果を報告させ、協力して対処を行っています。また、全システムの構成情報を一元管理するアセット管理システムを構築し、是正対象となるシステムを自動で判定し、該当するシステム構築担当／運用担当に直接、脆弱性情報の配信を行っています。



外部からのアタックサーフェス調査・是正

企業のIT資産は年々拡大しており、これに併せて攻撃の対象として狙われる領域（アタックサーフェス）も増加しています。特に、近年のリモートワークの増加に合わせ、自宅から企業のネットワーク環境へ接続するためにRDP（Remote Desktop Protocol）やVPN（Virtual Private Network）をサポートする外部公開機器が急増しており、攻撃者は、管理が不十分な外部公開機器を悪用することで、企業内のネットワークに侵入しようとします。

KDDI-CSIRTでは、外部公開機器を悪用する攻撃者の攻撃リスクを低減するため、URLや証明書といったインターネット上に一般公開されている情報であるOSINT（Open Source Intelligence）などを利用して、外部公開されている社内関連設備を探索し、攻撃者に悪用されるサービスやコンテンツを誤って公開していないかなど、設備に対する攻撃リスクや管理状況を調査して、速やかに是正を図ることで、攻撃者が外部公開機器を悪用できないように対処を行っています。



事業用設備におけるセキュリティ審査

KDDIでは、サービスをお客さまに安全に提供するために、設備調達時におけるセキュリティ対策を適切に講じるように努めています。安全かつ信頼性の高いネットワーク確保のために、5Gのセキュリティ強化が重要とされ、本年3月末に、5G SAシステムを対象とした国のセキュリティガイドラインを定めており、KDDIも定期診断・監査時における社内規程の改訂を行い対応しました。

社内規程では、一般的なシステムに共通するセキュリティ対策に加えて、5G SAシステム特有のセキュリティ対策の要件を定めています。規程を基準とするセキュリティ監査を実施することで、内部からの情報漏洩リスク、および外部からの攻撃リスクなどに対する対策の実施状況を確認し、高いリスクが存在すると判断された場合は是正対応を行います。

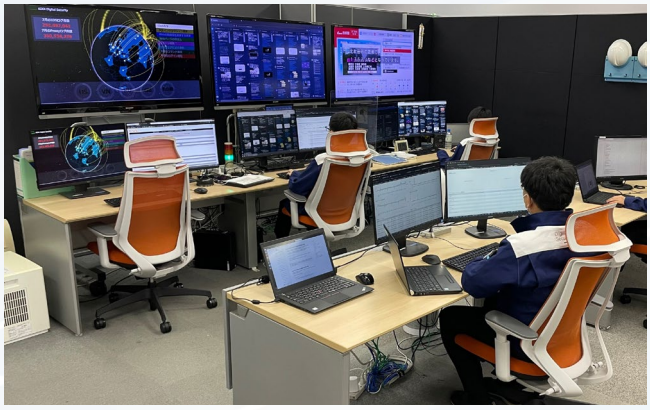
今後もKDDIでは、定期的に機器調達時の社内規程を見直し、必要なセキュリティ対策をアップデートしていくことで、安全なサービスの提供に努めていきます。

セキュリティ監視

KDDIでは、お客さまへ提供しているサービスや情報を守るために、セキュリティオペレーションセンター(KDDI-SOC)にて、セキュリティアナリストが24時間365日不正なアクセスや改ざんなどの監視を実施しています。

専門的な訓練を受けたセキュリティアナリストは、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、膨大なログの中から攻撃の兆候を見つけ出し、そこから不正アクセスや改ざんなどの危険なインシデントを発見した場合、CSIRTおよび社内の関係部門へ迅速に連絡を行い、対処を指示します。

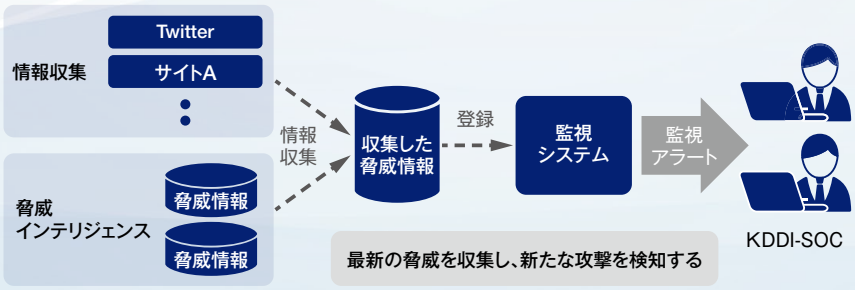
また近年、標的型メールなどからOA環境へ不正に侵入し、企業の重要情報を入手するケースが増えています。KDDIではSIEM／SOARやEDRなどを導入し、不審なアクティビティ監視し対処を実施しています。さらに、従業員が不正に情報を持ち出すなどの内部不正についても、日々監視を実施しており、お客さまのサービスや情報、そして社内の機密情報をさまざまなセキュリティの脅威から保護しています。



継続的な脅威情報収集

KDDI-SOCでは、最新のセキュリティ脅威に対応するため日々情報収集を行っています。情報収集は、公開されている情報やTwitterなどから収集しているだけでなく、脅威インテリジェンス情報も活用し情報を収集しています。

収集した情報からセキュリティ監視に有効となりそうなものは、監視システムへ登録され、最新脅威も検知できるように、継続的な収集を実施しています。



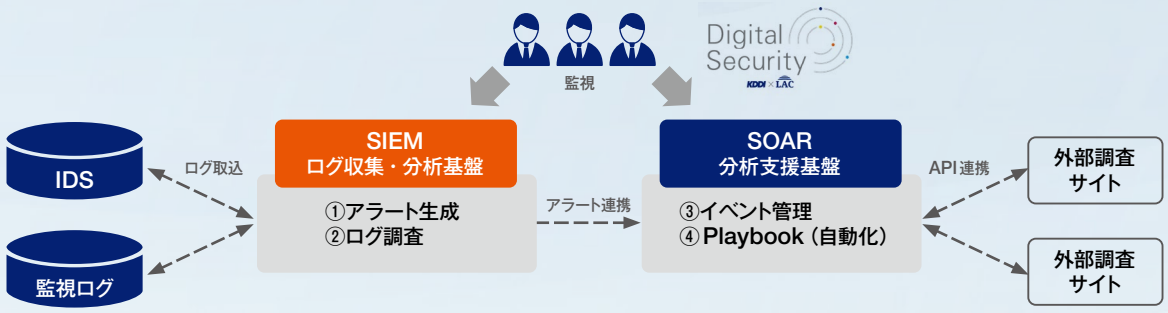
セキュリティ施策（サイバー攻撃対策）

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、最先端技術を応用して、セキュリティ監視システムのさらなる高度化に努めています。

SIEM、SOAR、IDSなど監視設備・システムを応用したサイバーセキュリティ分析支援基盤を用いて、高度な技術を持つ監視要員による判断と監視プロセスの自動化を組み合わせることで、膨大なログを効率良く分析し、高品質なセキュリティ監視を行っています。

サイバーセキュリティ分析支援基盤では、KDDI単体だけではなく、世界中のKDDIグループ会社に導入しているSIEMで収集されたセキュリティイベントの収集・分析を行い、全世界のKDDIグループのセキュリティを確保しています。



DDoS対策

DDoS攻撃に関しても、対処するためのシステムの開発・運用を行っています。

攻撃を検知した場合には、所定のルールにのっとり、自動で対応を行いますが、必要に応じてSOCと通信設備の運用監視部門が連携して対応を行います。

これにより、KDDIの通信ネットワークを保護し、安定的な電気通信サービスの提供を可能としています。

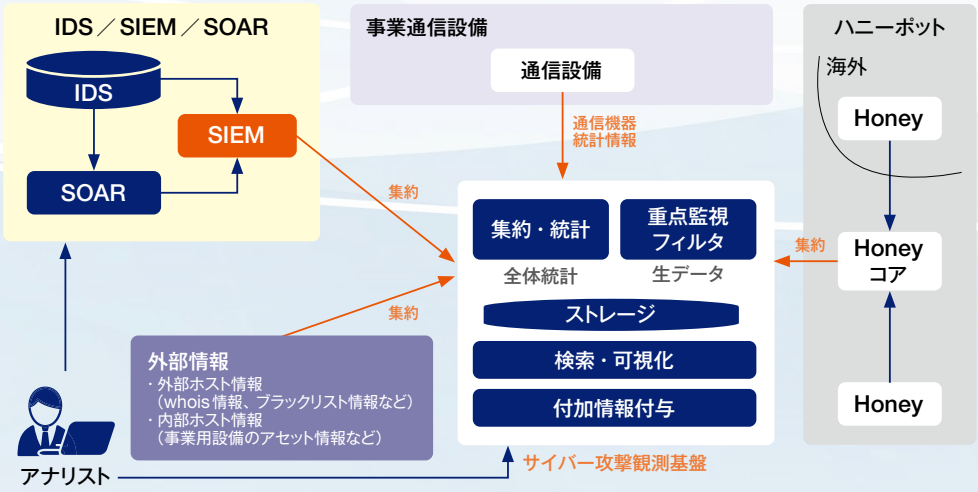
セキュリティ高度化システムの開発

サイバー攻撃は、組織化・複雑化・巧妙化・高速化が進んでいます。こうしたサイバー攻撃に対応するため、最先端技術・業界トレンドの調査・分析・評価を行い、KDDIで応用できる技術を取り入れ、セキュリティオペレーションに使用するシステムの開発を行っています。

KDDIグループにて開発したセキュリティオペレーションシステムの一例

- **KDDI通信網を通した攻撃通信の観測システム**

攻撃傾向の把握、攻撃の予兆を示す挙動を可視化し、プロアクティブに対処を図っていくため、KDDI通信網に設置する多種多様な監視機器の情報を集約・サンプリングした上、相関的に分析し、KDDI網全体への攻撃の把握・予測を行っています。



セキュリティ施策（個人情報保護対策）

KDDIはさらなる適正なお客さま情報の取り扱いを目指し、社内組織の整備、第三者による評価の実施、お客さまによるプライバシー管理機能の提供、サービス導入前のプライバシー影響評価（PIA）の導入などの対応を実施しています。

社内体制の整備

KDDIは、個人データ利活用に向けた整備・運用を担う組織として、データガバナンス室を設立しました。 また、プライバシー・データガバナンスに係る意思決定機関として、代表取締役社長を議長とするデータガバナンスボードを設置し、プライバシー保護などに関する取り組みに関して、審査･承認を行う体制を構築しています。

組織	データガバナンス室
	↓ 事務局
承認・審議機関	データガバナンスボード（議長：代表取締役社長）
役割	●データ利用中長期戦略の立案 ●データガバナンス戦略の立案および施策実施 ●国内外プライバシー法制への対応 ●プライバシーガバナンス社内浸透活動

第三者による評価の実施

KDDIのデータ活用の取り組みに関して、適切なデータの取り扱いとなっているかどうかを、第三者の視点からのご意見をいただき、お客さまの体験価値向上・社会の持続的発展をより一層推進するべく、さまざまな領域の有識者から構成されるアドバイザリーボードを設置しています。

アドバイザリーボードの議論内容については、プライバシーポータルでも公開※1しています。

参考：（アドバイザリーボード委員 2022年9月5日時点）

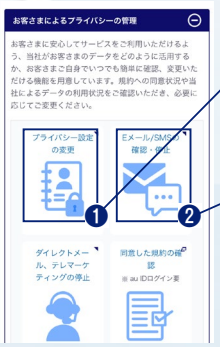
森田 朗　一般社団法人 次世代基盤政策研究所 代表理事【座長】
沢田 登志子　一般社団法人 ECネットワーク 理事
宍戸 常寿　東京大学大学院 法学政治学研究科 教授
篠原 治美　株式会社 シーピーデザインコンサルティング／公益社団法人 日本消費生活アドバイザー・コンサルタント・相談員協会
森 亮二　英知法律事務所 弁護士

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

お客さまによるプライバシー管理機能の提供

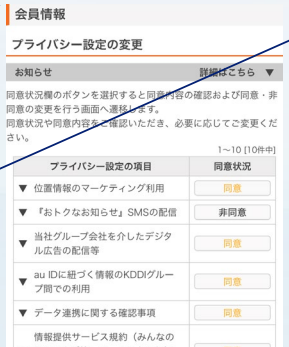
前述の「プライバシーポータル」を提供し、お客さまがよりわかりやすくかつ容易にお客さま自身に関する情報の取り扱いについてアクセスできるような機能を提供しています。

プライバシーポータル



ダッシュボードによる動線一元化

❶ プライバシー設定の変更画面



データ利用の同意・非同意の設定変更が可能

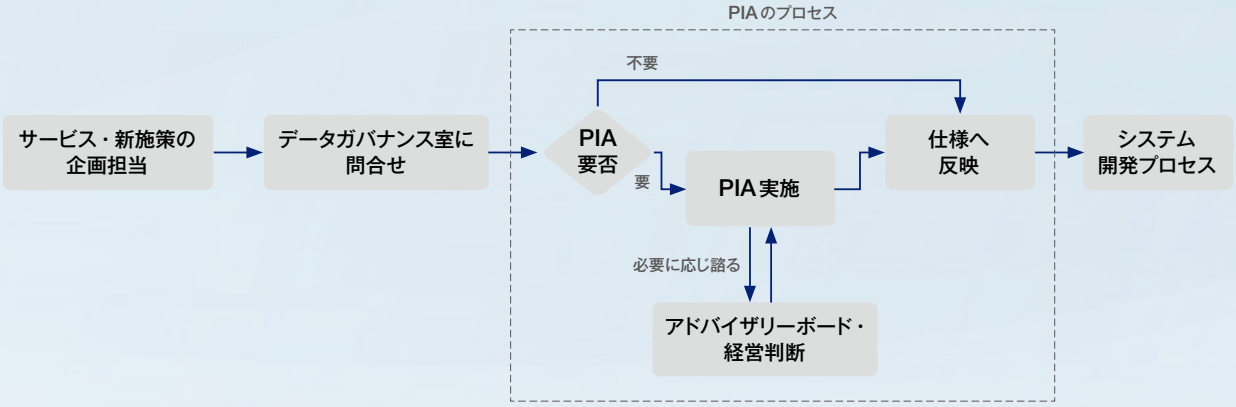
❷ メルマガなどの停止

メルマガなどの停止導線を集約

セキュリティ施策（個人情報保護対策）

プライバシー影響評価（PIA）

業務プロセスにPIAを組み込み、新規サービスの企画検討時にリスク評価が実施できるよう業務フローを導入しています。



AIを安心安全に開発、利活用するための取り組み

KDDI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 総合研究所の協力のもと、「KDDI Accelerate 5.0」の一環として、「KDDIグループAI開発･利活用原則※1」を2021年8月30日に策定しました。KDDIグループは本原則に基づく社内の啓発活動を通じて、お客さまに安心してサービスをご利用いただけるよう、AIの研究開発、利活用を推進しています。

※1 KDDIグループAI開発・利活用原則（https://www.kddi.com/corporate/kddi/public/ai_principles/）

セキュリティ施策（サービス不正利用対策）

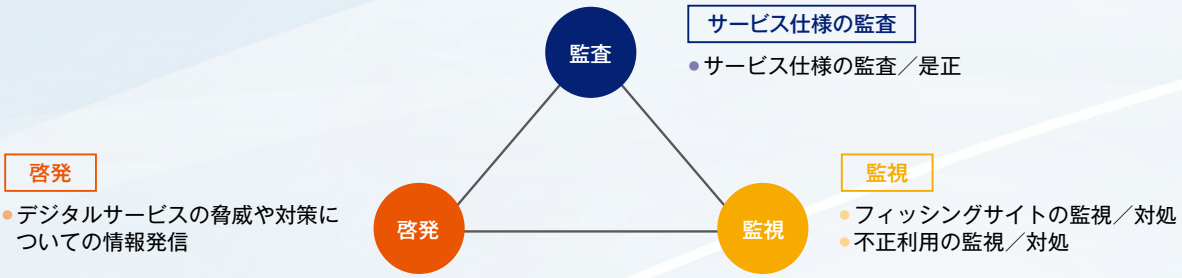
SSIRTの取り組み

SSIRT（Service Security Incident Readiness & response Team）とは、サービスのデジタル化により発生した新たな脅威に対応する体制として、内閣サイバーセキュリティセンター（NISC）でもその必要性が議論されている組織であり、KDDIではいち早く取り入れてKDDI-SSIRTを2018年に組成しています。

最近では、スマホ決済サービスの普及に伴い、生活が便利になる一方で、金銭目当ての悪意のある者が正規利用者になりすまして不正行為を働く隙を狙っています。

このような不正行為により発生する被害が事業者のサービス仕様の不備に原因がある場合、そのサービスが終了に追い込まれるリスクもあります。

こうしたデジタルサービス提供者としての新たなリスクに対して、専門知識を持ったSSIRTが対策に取り組んでいます。本章ではSSIRTが取り組んでいる「サービス仕様の監査」、「監視」、「啓発」の3施策の取り組みについてご紹介します。



サービス仕様の監査

SSIRTでは、新たにサービスを提供する際や機能を追加･変更する際に、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される可能性を洗い出し、お客さまにKDDIサービスを安心・安全にご利用いただけるよう、仕様の是正や悪用リスクの低減に取り組んでいます。

監視

フィッシングサイトの監視

ここ数年、不正行為を行う目的で、実在する企業やKDDIを装ったEメールやSMSを送り、本物そっくりなフィッシングサイトへ誘導することで、お客さまのパスワードや個人情報などを窃取するフィッシング詐欺が急増しています。

このようなフィッシング詐欺への対策としては、以前からの迷惑メール対策だけでなく、フィッシングサイトの発生を監視する取り組みも行っています。発見したフィッシングサイトは、関連機関と連携して、お客さまが被害に遭わないよう対処に取り組んでいます。

不正利用の監視

SSIRTでは、フィッシング詐欺などにより正規利用者のアカウントを乗っ取る不正な行為に対して、24時間365日監視する体制を整備して対応にあたっています。お客さまが被害に遭わないよう、さらなる強化を進めています。

啓発

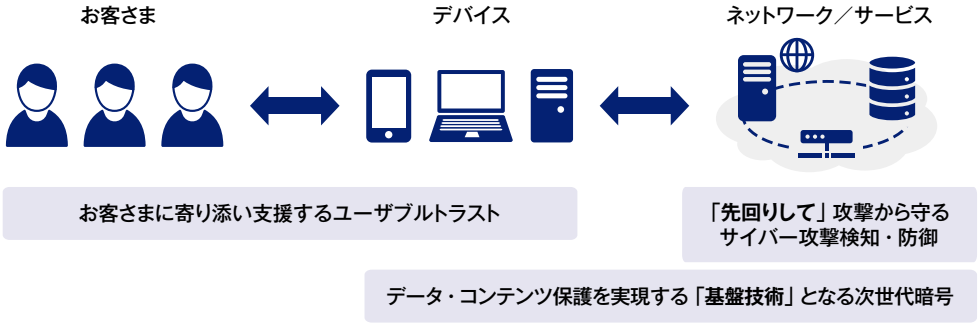
フィッシング詐欺などの犯罪手口をKDDIホームページ上で公開し、デジタルサービスを利用する上でお客さまにご注意いただきたい事項や有効な対策を発信しています。また、業界を超えた複数のインターネット企業などが協力して、年に一度、お客さまの啓発を行うイベント「サイバー防災」にも、その趣旨に賛同して毎年参画しています。少しでも多くのお客さまにデジタルサービスの脅威や対策を知っていただきたいという思いのもと、引き続き分かりやすい情報発信に取り組みます。

研究開発の推進

KDDI 総合研究所における研究開発

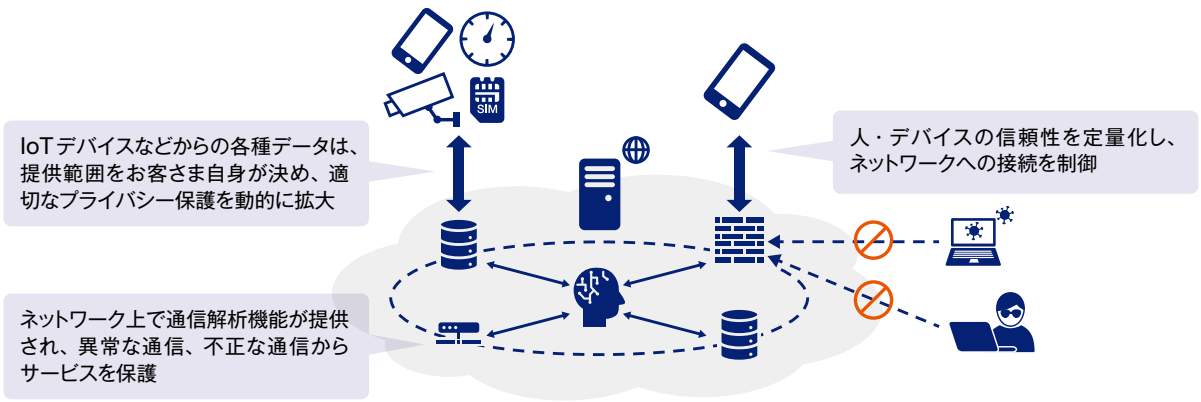
KDDIは、B5G／6G時代に向け、通信を使ったサービスにおけるあらゆる脅威に対し、最適な対策を実現するための研究開発を行っています。KDDI総合研究所セキュリティ部門における研究開発の取り組みを下図に示します。ユーザブルトラストは、人の心理や行動分析に基づくセキュリティ対策やお客さまの選好を考慮したプライバシー保護技術を含みます。サイバー攻撃検知・防御技術に関しては、セキュリティビッグデータをAIで効率的に解析することで、攻撃に先回りした対策を実現します。また、次世代暗号技術に関しては、B5G／6G時代を見据えた超高速・大容量に対応した共通鍵暗号、量子コンピュータ時代に対応する耐量子計算機暗号の研究開発を進めています。

KDDI 総合研究所セキュリティ部門における研究開発



ネットワークの信頼性を高める技術として、サービスを利用する人やデバイスの信頼性を定量化し、信頼関係に基づいてネットワークへの接続を制御する技術により不正利用者の侵入を阻止する機構および高度なトラフィック解析技術により新しい種類のデバイスに対しても的確に異常・不正通信を検出して遮断などの適切な制御を可能とする機構について、取り組みを進めています。さらに、ネットワークを構成する機器の信頼性を担保するために、サプライチェーンにおけるハードウェアの検証ならびに検証結果の共有を実現する情報共有基盤の実証実験を行っています。また、データの利用をお客さまが制御できる技術は、プライバシーを保護するための重要な機能であり、プライバシーバイデザインの観点からは、共通的な機能として通信ネットワーク上で利用されることが望まれます。通信ネットワークにおいてデフォルト機能として利用可能となることで、各サービスにおいて、お客さまの同意とプライバシープリファレンスに基づいた適切なプライバシー保護手段を適用することが可能となるため、適切なデータ利用が実現できます。下図に示すように、これらの技術を、通信ネットワーク上の各サービスに対してシームレスに適用可能とすることで、より広範囲で統一的なセキュリティ・プライバシー対策を提供することを目指します。

セキュリティ・プライバシー機能を内包するセキュリティ基盤



AIを活用した攻撃検知ならびに防御技術の研究開発も進めています。WEBセキュリティ対策技術の高度化を目指したWarpDriveプロジェクトにおいては、大量のWEBアクセス情報を収集・蓄積し、国内のセキュリティ研究機関8組織が協力して分析・研究を行う基盤を構築・運用して、数々の有望な成果を創出しました。今後も、セキュリティビッグデータの蓄積と協業を両輪で進め、B5G／6GにおけるAIを活用したサイバーセキュリティ対策の研究開発を進めます。また、膨大な数のハードウェア・ソフトウェアの安全性を効率的に検証するために、AIを積極的に活用していきます。一方、導入したAIが新たな脆弱性を生まないために、AIへの攻撃対策も重要な課題として取り組んでいます。AIそのものに対する攻撃は、近年急速な進歩を遂げており、AIの判定を巧妙にすり抜けるようなマルウェアの作成方法なども具体化が進んでいます。AIの利活用が進むにつれて、攻撃による脅威の顕在化が予想されるため、その対策技術についても研究開発を推進していきます。さらにAIを有効活用するために、統合分析に活用できる高機能で高速な次世代型準同型暗号の改良も進めています。

耐量子計算機暗号の安全性評価

B5G／6G時代を見据えた新世代の暗号アルゴリズムの研究開発も継続的に実施しています。

インターネットをはじめとする情報通信システムの安心・安全を支える基盤技術である公開鍵暗号技術は、ネットショッピングやICカードなどで日常的に利用されています。しかし近年、大規模な量子コンピュータの登場により、暗号解読の大幅な性能向上が見込まれます。今後は量子コンピュータに対しても安全性を確保できる公開鍵暗号（耐量子計算機暗号）が必要とされています。米国では、アメリカ国立標準技術研究所が主導する耐量子暗号の標準化プロジェクト（NIST-PQC）において、耐量子計算機鍵暗号の選定が進められています。

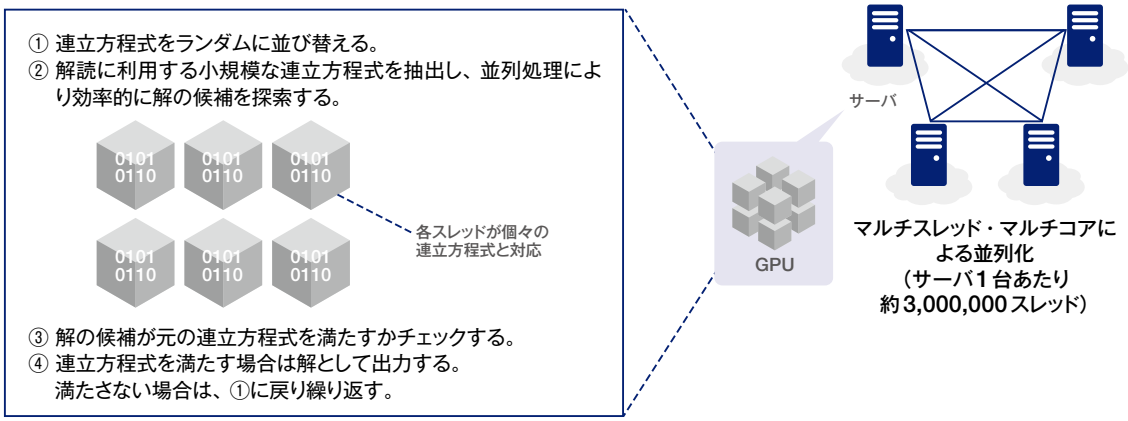
KDDIは、2022年2月、暗号解読コンテスト「decodingchallenge.org」において、550次元のSyndrome Decoding問題（以下SD問題）を、世界で初めて解読しました。SD問題は、NIST-PQCの最終候補に選定されたClassic McEliece暗号を含む符号暗号の安全性の根拠となっています。耐量子計算機暗号として符号暗号を利用する際、安全な次元の大きさを決定するために、解読可能な次元の限界を知ることが重要です。550次元のSD問題は、同コンテスト全体を通じ、これまで解読された問題の中で、解読に最も大きな計算量を必要とする問題です。問題の解読にあたり、解読アルゴリズム処理やデータ構造を最適化するとともに、GPUサーバ1台あたり約300万のマルチスレッド・マルチコア並列化を実施しました。その結果、通常の解読アルゴリズムに対し、226倍の処理速度を達成し、550次元のSD問題の解読に13日で成功しました。

研究開発の推進

解読アルゴリズムの概要を図の①～④に示します。解読の対象となる連立方程式は大規模であるため、直接解読することは極めて非効率的です。そのため、方程式をランダムに並べ替え、解読に利用する小規模な連立方程式を抽出します。ここで、GPUによる並列計算を活用し、各スレッドで異なる連立方程式を解き、解の候補を絞り込んでいきます（①～②）。次に、絞り込まれた解の候補が、元の連立方程式を満たすかどうかをチェックします（③）。もし、連立方程式を満たす場合は、その解の候補を正しい解として出力します。連立方程式を満たさない場合は、①に戻り処理を繰り返します。

本成果は、耐量子計算機暗号として符号暗号を利用する際に、安全な次元の大きさを決めるための非常に重要な情報となります。

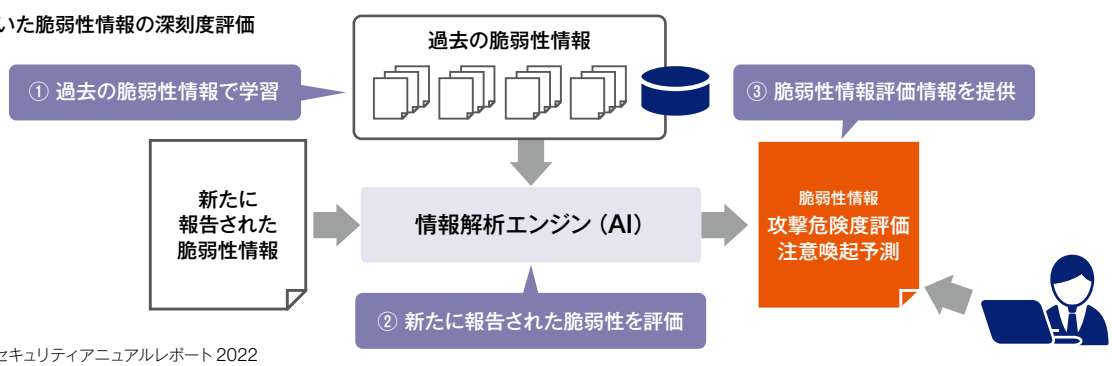
解読アルゴリズムの概要



脆弱性対応支援

サイバー攻撃は、ソフトウェアのバグなどに起因するシステムの脆弱性を突いて行われるものも多く、新たに発見された脆弱性へのセキュリティパッチの適用などの対処を怠っていると深刻なサイバー被害につながる恐れがあります。しかしながら、年間で発見される脆弱性の数は20,000件程度もあり、脆弱性の深刻度を0から10の数値で表すCVSS（Common Vulnerability Scoring System）スコアで「緊急」に該当する9以上の脆弱性に絞っても年間2,000件以上あります。このため、次々と発見される脆弱性の詳細情報を収集してその内容や影響の有無を把握し、適切な対処を講じることが困難になっています。そこでKDDIでは、脆弱性に関する情報収集とその分析を自動化するための研究を進めており、その成果として開発した分析システム（名称：Vuldate）を用いて、一般社団法人ICT-ISAC（情報通信分野の事業者によるサイバーセキュリティ関連情報の共有や分析を目的に設立された組織）の会員企業向けの情報提供を2022年6月から開始しています。Vuldateの動作の流れを図の①～③に示します。まず、過去の脆弱性情報を学習データとして分析モデルを構築し、AI情報解析エンジンに取り込みます（①）。新しい脆弱性が報告された際には、その脆弱性を突くための攻撃コードが作成される可能性の高さを示す「攻撃危険度評価」と、注意喚起の対象となるかどうかの「注意喚起予測」に関するAIによる脆弱性評価情報を示すとともに、当該脆弱性に関連する情報をインターネット上のニュースサイトやSNSサイトから自動収集・整理して提供し、情報システム担当者による脆弱性対応の判断をサポートします（②～③）。脆弱性への迅速な対処によるセキュリティ向上は、社会全体で取り組まなければならない課題であり、KDDIは、VuldateのICT-ISACへの提供などを通じて、安心安全な情報社会の実現に貢献しています。

機械学習を用いた脆弱性情報の深刻度評価



お客さまに寄り添い、的確な対策を実現するユーザブルセキュリティ

KDDIは、セキュリティの事故や被害を防止する重要な対策のポイントとして、お客さまの行動にも注目しています。設計時の期待通りに機能すればセキュリティ事故を防げるシステムであっても、設定や利用手順を誤ってしまうと、事故や被害が起きてしまいます。セキュリティの観点で、システムを適切に利用できるか否かは、お客さまのリテラシーや利用する状況など、複数の要因が関係します。そして、こうした複雑な状況では、注意喚起や適切な利用手順を画一的に提示する取り組みは、事故の防止に限界があります。

そこで、お客さまのリテラシーやシステムを利用する状況に応じて、システムの安全な利用を、負担なく叶えることを目指して、サービスを利用するお客さまに寄り添ったセキュリティ技術の研究を行っています。具体的には「お客さまの理解」と「適切なセキュリティ対策行動を引き起こす仕掛け」の研究に取り組んでいます。

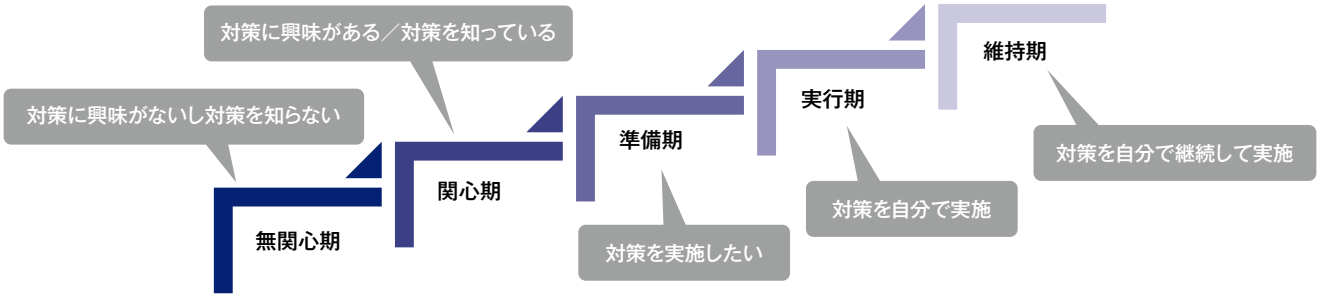
「お客さまの理解」の研究の一例として、下図に示す「セキュリティ行動変容ステージモデル」の研究があります。これは、健康分野で用いられる行動変容ステージを参考に、セキュリティ対策への関心や普段の対策状況といった態度の違いを「無関心期」から「維持期」の5つに定義したものです。この研究成果は、お客さまの状態を正確に把握・分類可能にするとともに、セキュリティ対策への態度を、より望ましい状態（図中では右上の方向）に向上する要因を解明する研究に寄与します。その他、適切なセキュリティ対策行動を実際にとっているか否かの実態を、限られた質問数で高精度に推定する心理尺度を作成する研究にも取り組み、その成果は、難関国際会議であるSOUPS 2022に採択されました※1。

「適切なセキュリティ対策行動を引き起こす仕掛け」の研究については、上記の研究成果を通じて把握するお客さまの状態に応じて、セキュリティ対策やリスク回避を効果的に促す方法や注意を喚起する手段の実用化を目指しています。これまでに、パソコンのOSの更新を対象に、更新通知の文言、画面のデザインおよび通知のタイミングを最適化する技術を検証し、有効性を確認しました。

こうした研究を通じて、負担が少なく、お客さまの納得感を伴って、的確なセキュリティ対策を実現する技術の実現を目指していきます。

※1 https://www.kddi-research.jp/topics/2022/062801.html

セキュリティ行動変容ステージモデル



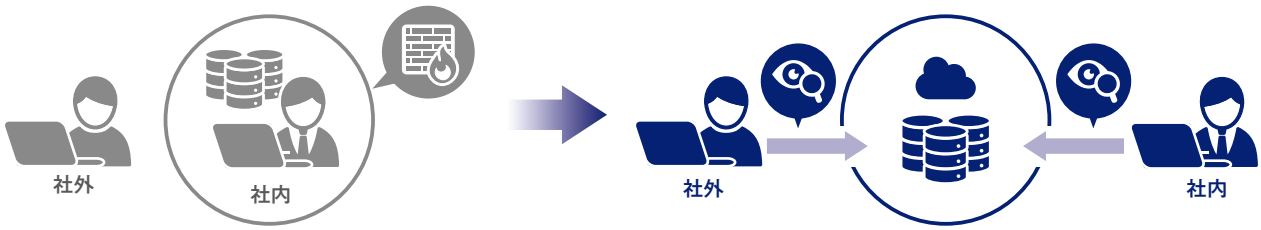
法人のお客さま向けセキュリティソリューション

マネージド ゼロトラスト

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。

「働き方」が柔軟になり、「働く場所」も分散



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

セキュリティアセスメント

「セキュリティアセスメント」や「脆弱性診断・ペネトレーションテスト」によって、セキュリティ上の課題・リスクを可視化し、改善に向けた対策計画策定の支援を行います。ゼロトラスト構築にあたり、情報収集・選別が困難、何から着手すればよいかわからないなどのお悩みに対し、「ゼロトラスト成熟度アセスメント」によって、ゼロトラスト対応状況を可視化、対策の優先度や実施後の効果を、短期間（1ヵ月程度）・無償で定量評価します。

セキュリティアセスメント

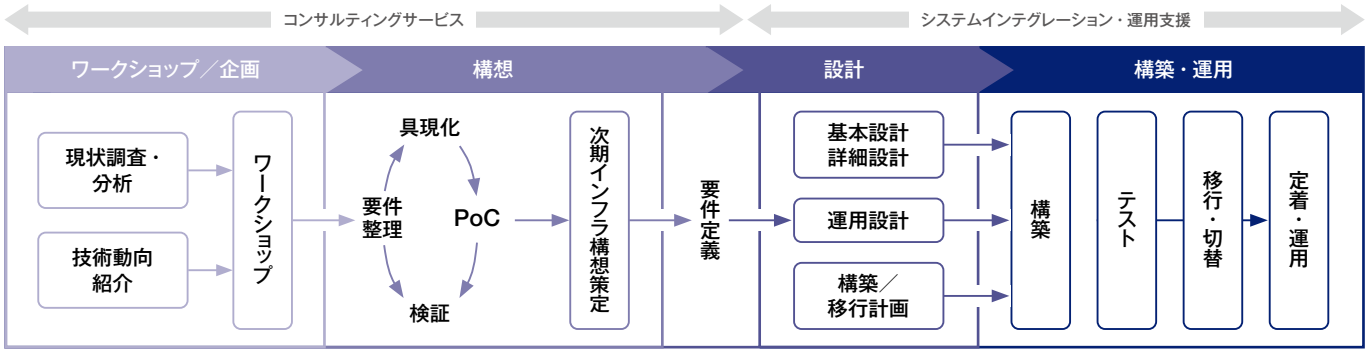
企業の体制、インフラ、運用、物理的対策などの全体を鑑みたセキュリティの脅威を調査（レポートの提供を含む）

脆弱性診断・ペネトレーションテスト

ITインフラや、WEBアプリケーションなど、ネットワーク機器に対し疑似攻撃を実施し、脆弱性があるかどうかの調査

コンサルティングサービス

ゼロトラストの導入はITインフラ環境全体の見直しです。段階を踏んで具体的な構想策定を支援するコンサルティングサービスメニューを用意しています。目指す姿を見据えて、具体的な構想策定を支援します。



導入後の運用もワンストップで支援

従業員からの問合わせやクラウドのアップデートに合わせたチューニング、セキュリティ運用など、導入後の負荷もKDDIがトータルでサポートします。

お客さま業務サポートで管理業務を支援

支援内容

- ヘルプデスクアウトソース（エンドユーザからの各種お問い合わせを一元受付）
- アカウント、デバイスの管理
- 設定作業代行

システム・サービス運用で運用の安定化・効率化を支援

支援内容

- サービスデスク（管理者からのサービス一元受付）
- システム、サービス監視
- 障害通知、復旧対応
- 可視化、レポーティング
- 設定作業代行（ポリシー・パラメータ設定、各種コンソール代行）

セキュリティ運用で脅威対策を支援

支援内容

- ログ監視とリスク分析
- セキュリティ改善
- セキュリティ通知
- インシデント対応（特定デバイスやアカウントの隔離、遮断、レポート）

KDDI セキュリティソリューション by LAC

LAC（株式会社ラック）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ラック社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。

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（ISO／IEC27001）認証※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

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
株式会社KDDIエボルバ

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まとめてオフィス西日本株式会社※2
KDDIまとめてオフィス東日本株式会社※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

※1 ISMS認証（ISO／IEC27001：2013）。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認証適用範囲に含む。

KDDIグループの概要

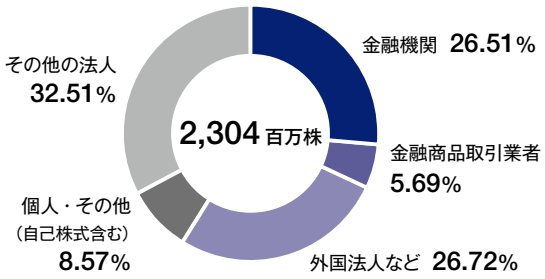
会社概要（2022年3月31日時点）

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社合併により設立）
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	髙橋 誠
資本金	141,852百万円
従業員数	48,829名（連結ベース）

株式の状況（2022年3月31日時点）

証券コード	9433
発行可能株式総数	4,200,000,000株
発行済株式総数	2,304,179,550株
株主数	341,622名

所有者別分布状況



大株主

氏名または名称	所有株式数（株）	議決権比率※1（%）	持株比率※2（%）
日本マスタートラスト信託銀行株式会社（信託口）	357,949,400	16.13	15.53
京セラ株式会社	335,096,000	15.10	14.54
トヨタ自動車株式会社	316,794,400	14.28	13.74
株式会社日本カストディ銀行（信託口）	130,021,300	5.86	5.64
STATE STREET BANK WEST CLIENT - TREATY 505234	31,085,775	1.40	1.34
バークレイズ証券株式会社	28,453,600	1.28	1.23
三菱UFJモルガン・スタンレー証券株式会社	24,555,562	1.11	1.06
JPモルガン証券株式会社	23,590,296	1.06	1.02
STATE STREET BANK AND TRUST COMPANY 505103	22,595,124	1.02	0.98
JP MORGAN CHASE BANK 385781	21,868,304	0.99	0.94

※1 議決権比率は、自己株式（85,058,340株：2022年3月31日時点）を除いて算定しています。また、役員報酬BIP信託口および株式付与ESOP信託口が所有するKDDI株式（3,920,592株：2022年3月31日時点）は議決権を有する株式に含めて算定していますが、KDDIは同株式における議決権を行使しないものとしています。なお、議決権比率は小数点第三位を四捨五入の上、算定しています。
※2 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/