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 2024

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

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2025年1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/

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/

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、ランサムウェア攻撃の増加、国家を背景とした攻撃の拡大などサイバー攻撃の洗練化・巧妙化が一層進展しております。

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日の体制で監視を行うとともに、サイバー攻撃の分析や監視業務をAIで自動化する技術を導入し、最新の攻撃手法の把握やAIを活用した検知技術の強化に継続的に取り組んでいます。これにより、サイバー攻撃によるサービスへの被害を最小限に抑え、お客さまに安心してサービスをご利用いただけるよう努めています。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。

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
執行役員専務
CTO コア技術統括本部長
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
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
2023年4月　当社CTO
2024年4月　当社CTO コア技術統括本部長（現在に至る）
2024年6月　当社執行役員専務（現在に至る）

サイバー攻撃・脅威動向

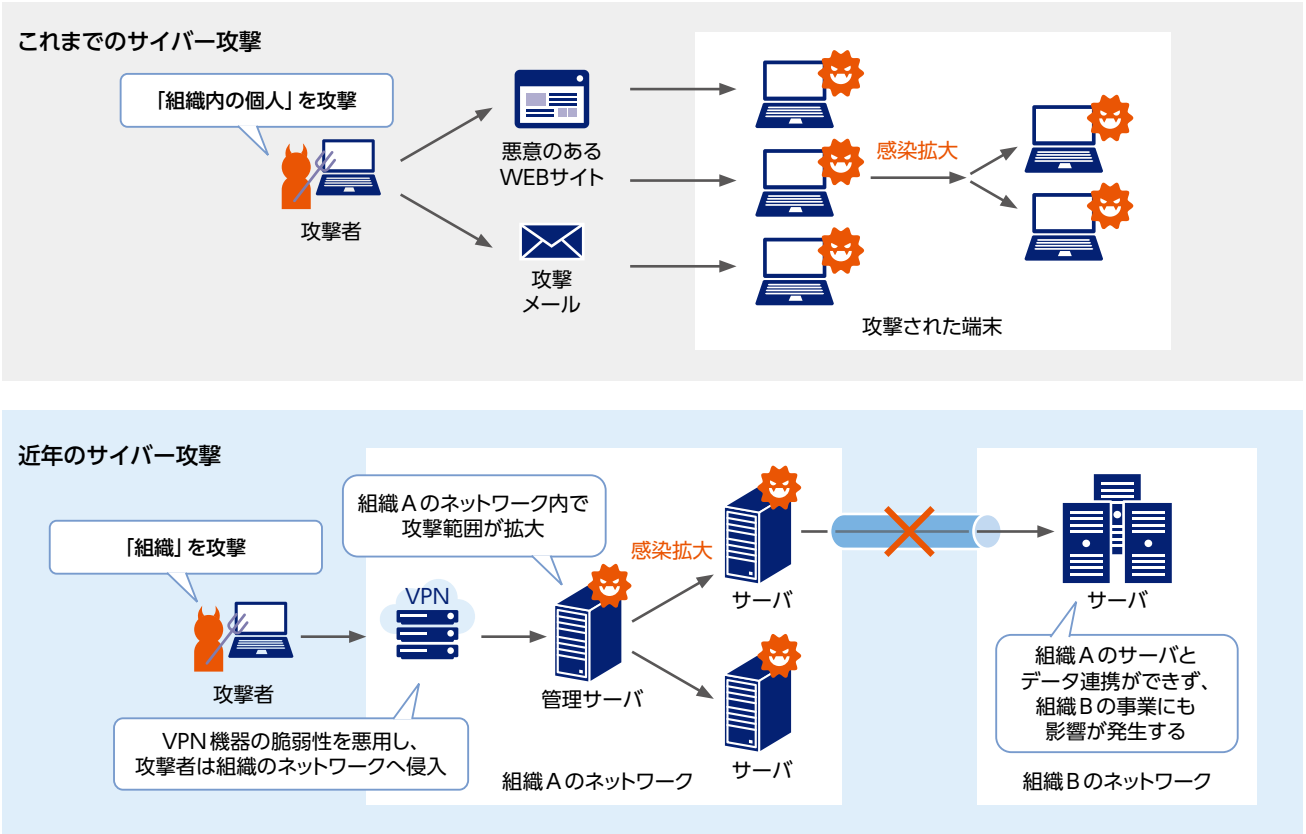
1 今日のサイバー攻撃

組織を標的としたサイバー攻撃の被害の報告は後を絶たず、警察庁の報告によると2023年のランサムウェア感染被害件数は197件（2022年は230件）と依然として高い水準で推移しており、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は、国内外で報告されています。

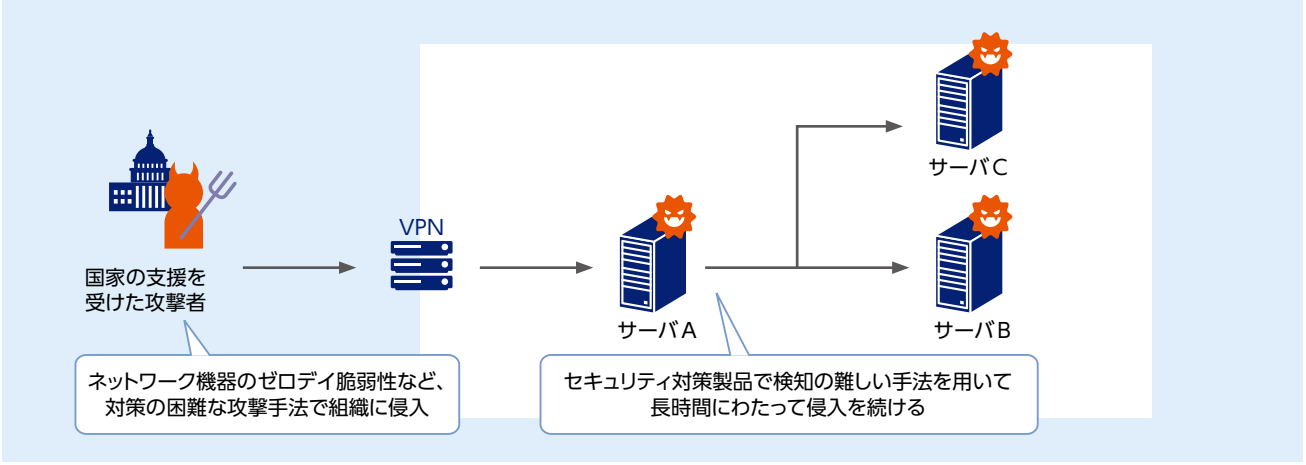
組織を標的としたサイバー攻撃は、これまではインターネット上に公開・提供しているWEBサービスへの攻撃や、メールを用いた組織内の個人を標的とした攻撃が一般的でした。これに加えて、VPN（Virtual Private Network）機器を標的とした攻撃や、セキュリティレベルの低い組織（グループ会社や取引先）を経由して標的の組織に侵入するサプライチェーン攻撃も増えており、サイバー攻撃の標的となる範囲は広がっています。

さらに近年は、国家を背景とする攻撃者およびその活動に関する注意喚起が国内外の政府組織から発出され、既に多くの組織が被害に遭っていること、攻撃者は標的組織への侵入を長期間にわたり維持するためにセキュリティ対策製品での検知が困難な攻撃手法を用いることが報告されています。組織を守るためには高度かつ巧妙なサイバー攻撃への対応がこれまで以上に重要となってきています。

サイバー攻撃の変化



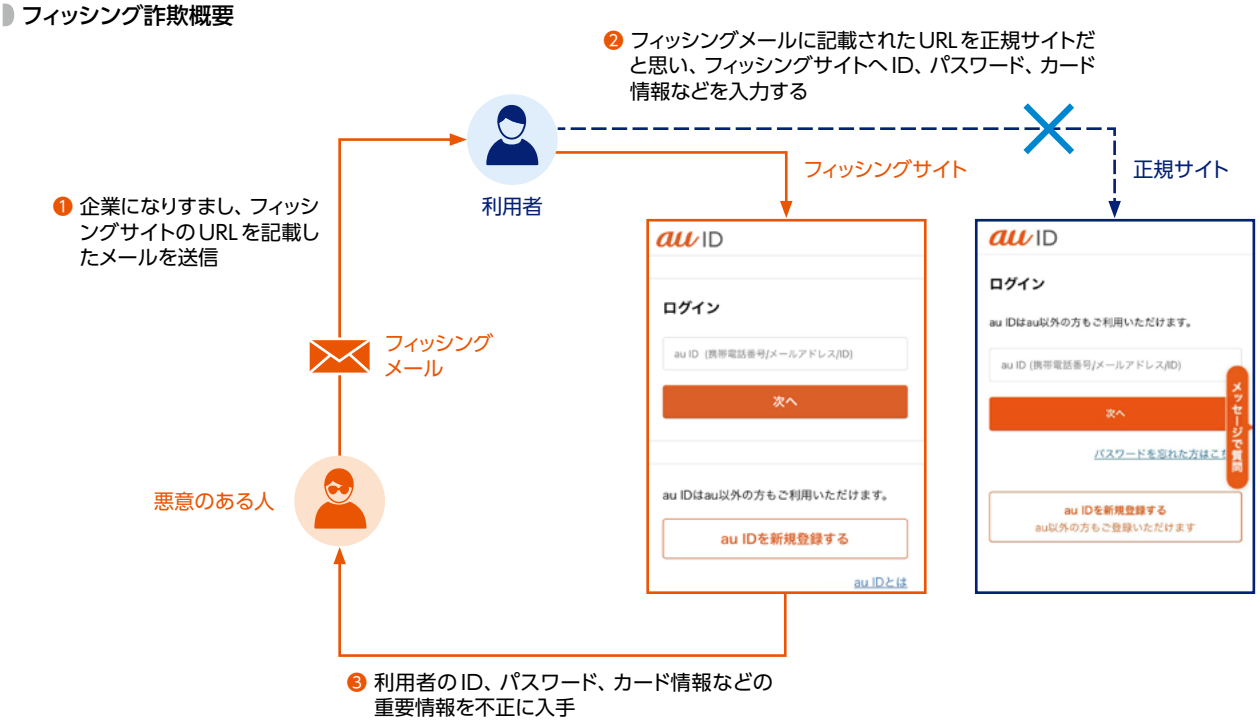
国家の支援を受けた攻撃者の活動



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。

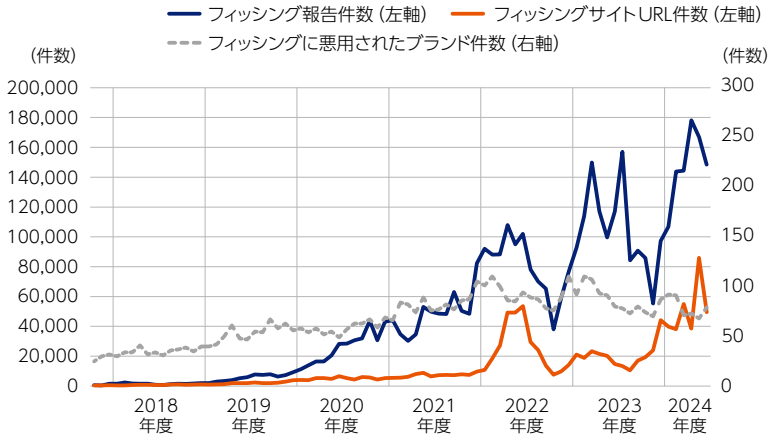
フィッシング詐欺概要



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受けることになります。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額は過去最高を記録した2023年以降も依然として高い水準が続いており、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。また、近年では、「闇バイト」と呼ばれるSNSなどでの犯罪実行者の募集も増加しており、こうした犯罪が今後も活発化していくことが想定されます。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

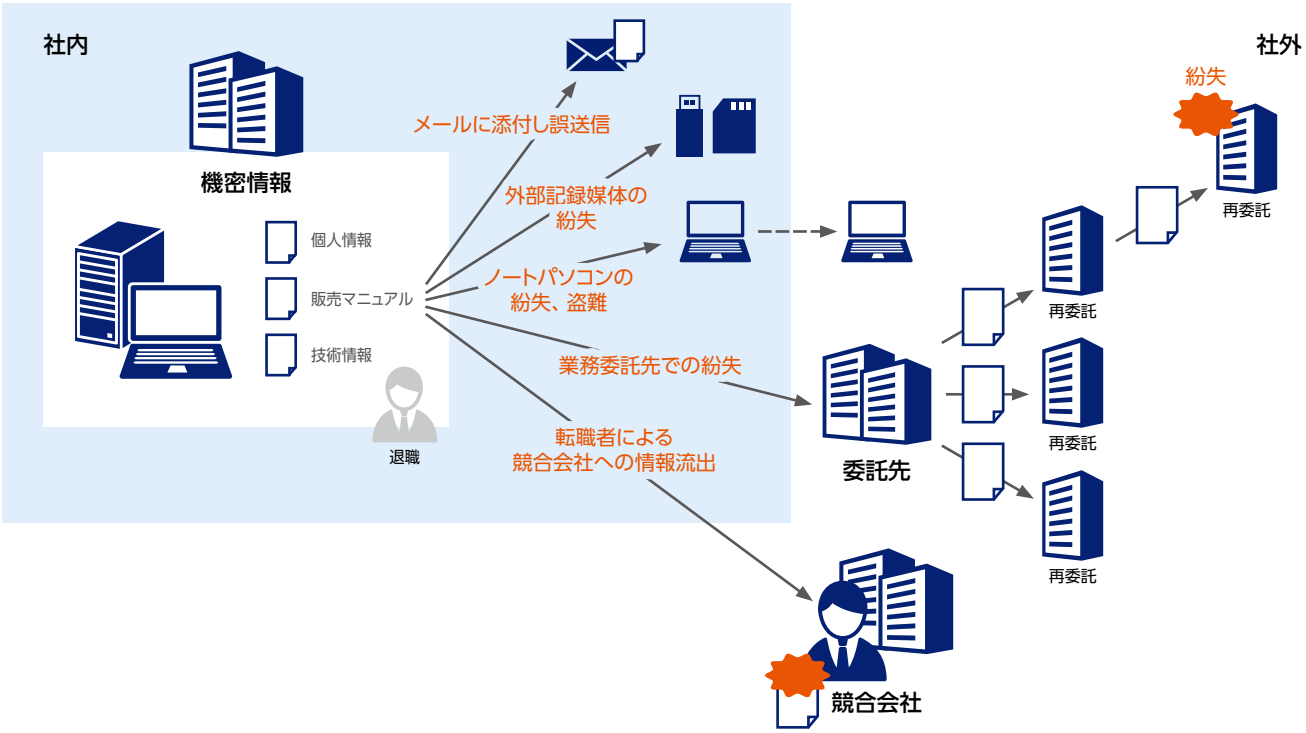


※ 出典：フィッシング対策協議会のデータから当社にて作成

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。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。

企業の機密情報漏えいのパターン

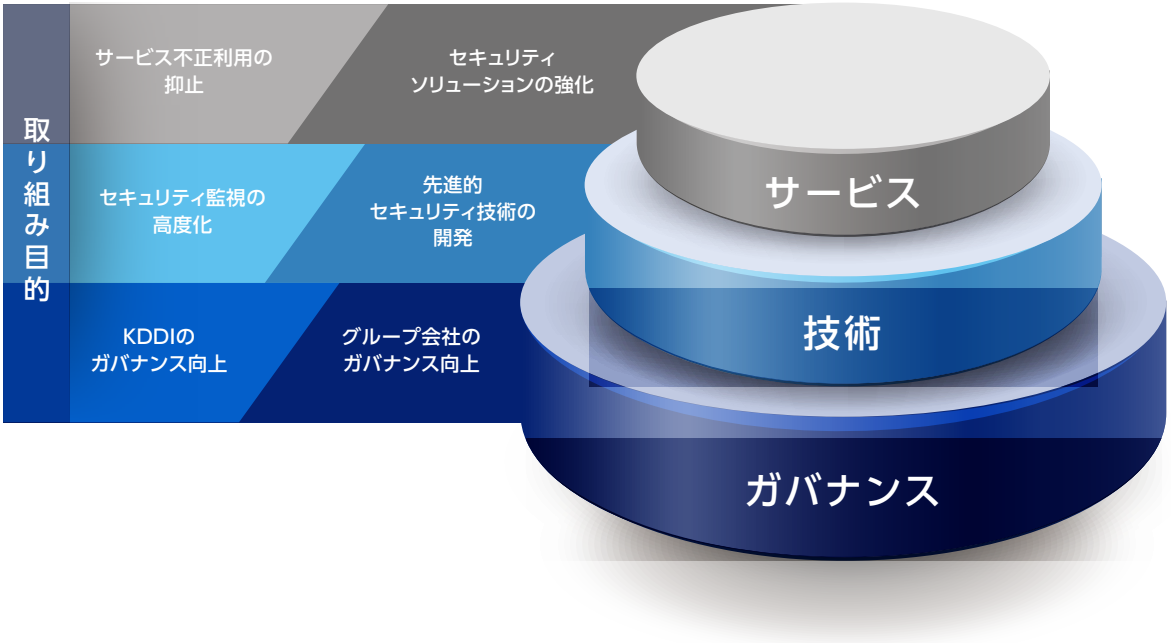


サイバーセキュリティへの取り組み

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、サイバー攻撃が進化する中で、特にランサムウェアによるデータ損失や企業の業務停止、さらにはそれによる信頼性の低下などが、個人や企業に対して重大な影響を及ぼす可能性があることを深く認識しています。これらのサイバー攻撃は、今や、自然災害や気候変動などと同様に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	ポリシー、体制、規程、マネジメント、監査、教育
	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	DDoS攻撃の可視化による防御力向上、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	SBOM導入に向けた実証事業 超高速共通鍵暗号方式「Rocca-S」の処理性能向上
サービス	サービス不正利用の抑止	フィッシングサイト・不正なサービス利用の監視、お客さま啓発 ログイン認証×生成AI（kCAPTCHA）
	セキュリティソリューションの強化	KDDIマネージドセキュリティサービス、SL商品

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ひとつと考え、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

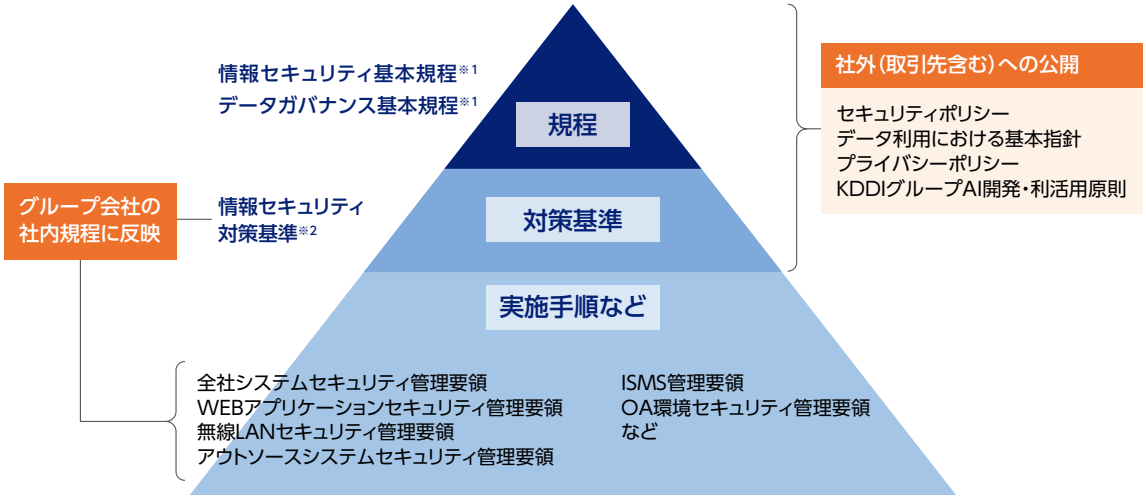
KDDIグループは、高度化・巧妙化が進むサイバー攻撃に対応するため、情報セキュリティに関するリスクマネジメントは非常に重要な課題と認識し、情報セキュリティガバナンスの強化に取り組んでいます。

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）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/

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。

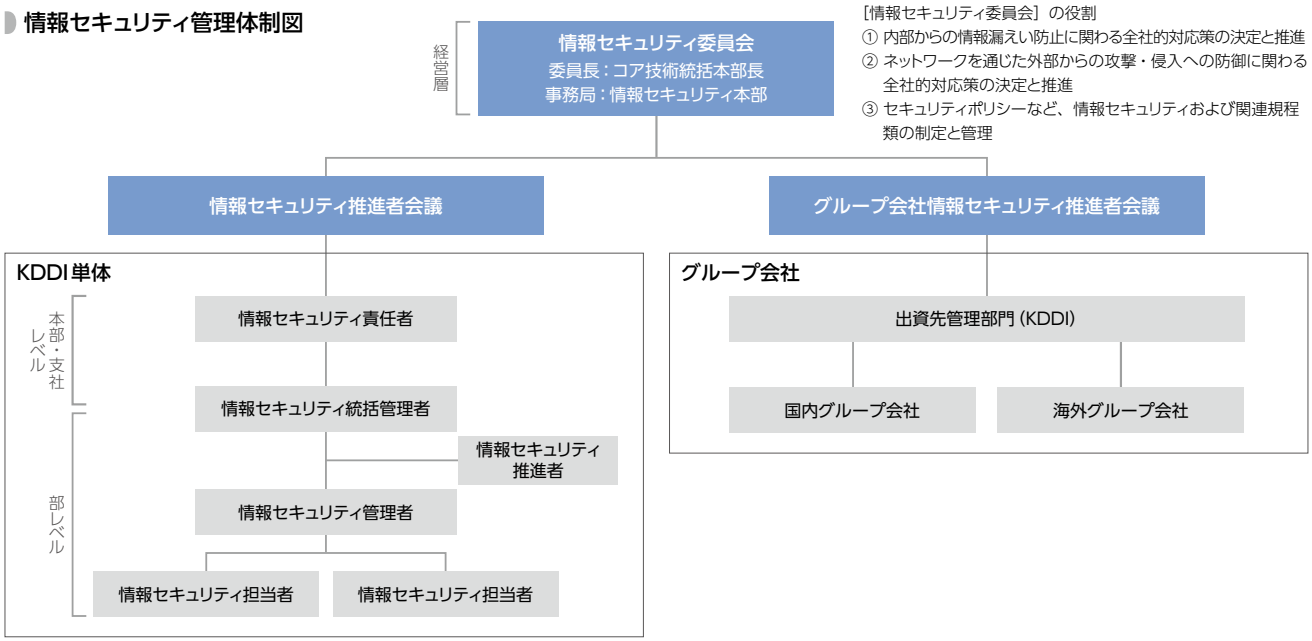
▶ 2021年8月30日ニュースリリース
「KDDIグループAI開発・利活用原則」を策定　https://news.kddi.com/kddi/corporate/newsrelease/2021/08/30/5356.html
▶ 2023年5月25日ニュースリリース
社員1万人が「KDDI AI-Chat」の利用を開始　https://news.kddi.com/kddi/corporate/newsrelease/2023/05/25/6741.html
▶ 2024年3月18日ニュースリリース
ELYZAとKDDIグループ、生成AIの社会実装に向け資本業務提携を締結　https://news.kddi.com/kddi/corporate/newsrelease/2024/03/18/7333.html

情報セキュリティガバナンス

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「グループ会社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

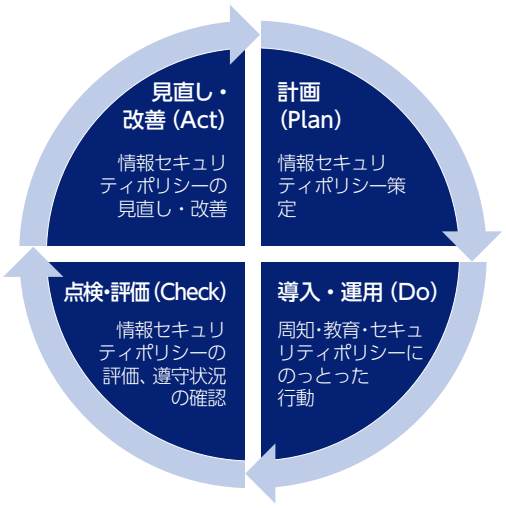


3 情報セキュリティマネジメントサイクル

KDDIは、ISMS認証（ISO／IEC27001：2013）※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。

※ 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

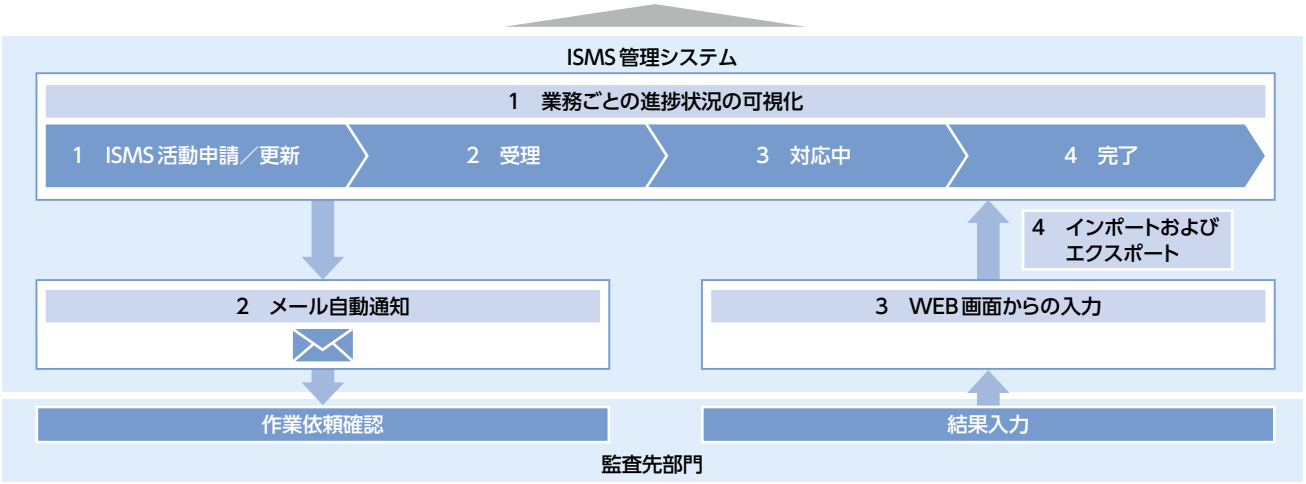


- **計画 (Plan)**
  情報資産の洗い出しを行い、リスクや課題を整理し、組織や企業の状況に合った情報セキュリティ対策の方針を定めた情報セキュリティポリシーを策定する。
- **導入・運用 (Do)**
  全社員に周知し、必要に応じて、研修などの教育を行う。社員がセキュリティポリシーにのっとって行動することで、目的とする情報セキュリティレベルの維持を目指す。
- **点検・評価 (Check)**
  導入後の現場の状況や問題点、社会的な状況などを踏まえて、定期的に情報セキュリティポリシー自体を評価する。また、遵守されているかどうかの監査も行う。
- **見直し・改善 (Act)**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



情報セキュリティガバナンス

4 情報セキュリティ監査

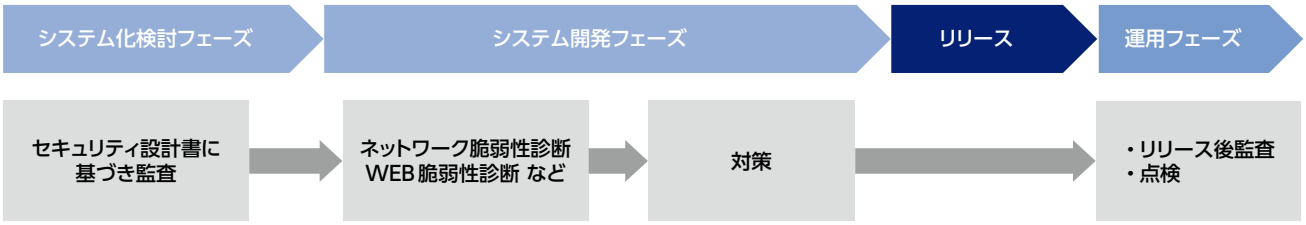
KDDIでは情報セキュリティ関連規範の遵守と適切な運用を確認するために、以下の3つの監査を実施しています。

システムセキュリティ監査

KDDIでは、システムの構築または改修が「全社システムセキュリティ管理要領」に従って適切に実施されているかを専門部署の監査担当者が監査します。この監査では、セキュリティ管理要領で規定された要件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）やEDR（Endpoint Detection and Response）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の情報資産を取り扱う業務の一部または全部をKDDIが委託している場合、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、「情報セキュリティ対策基準」に基づき、年1回以上の頻度で業務委託先を監査しています。さらに、重要度の高い業務委託のなかから毎年選定し、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。

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。2024年10月時点でのKDDIグループにおける資格登録者数は309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　309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
※ 2024 年 10 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／ 情報セキュリティ推進者向けセキュリティ研修	ライン長／情報セキュリティ推進者	eラーニング／集合研修

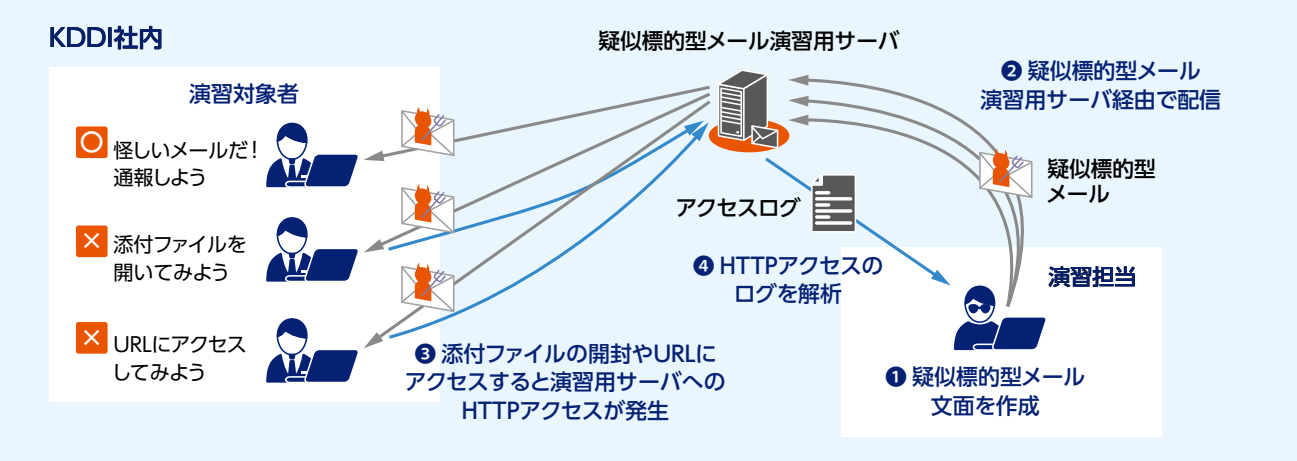
標的型攻撃メール演習

KDDIでは、全社員を対象に標的型攻撃メール演習を年に数回実施しています。本演習では、標的型攻撃メールに対する意識を高め、実際の攻撃に対する防御力を向上させることだけでなく、攻撃メールが届いた際に適切な判断を社員一人ひとりが行えるかの確認も併せて実施しています。

なお、演習を形骸化させないために、毎回メールの内容を変更することや習熟度に応じてKPIの指標も見直しながら対応を進めています。

また、演習結果は都度各部門へフィードバックしており、攻撃メール受信時の対応について意識向上を図っています。

情報セキュリティガバナンス



インシデント対応演習

KDDIでは、セキュリティインシデント発生時に迅速かつ適切な情報共有や対応フローを確認することを目的に、インシデント対応演習を実施しています。インシデントが発生した際には、規模に応じて対策本部を設置し、関連部門と協力して対応を進めるため、演習にはセキュリティ部門だけでなく、システム担当部門や広報担当部門も自身の役割に合わせて参加します。演習に取り組むにあたり、「シナリオ作成」「演習実施」「フィードバック・分析・改善」というサイクルを継続的に行っています。

❶ シナリオ作成

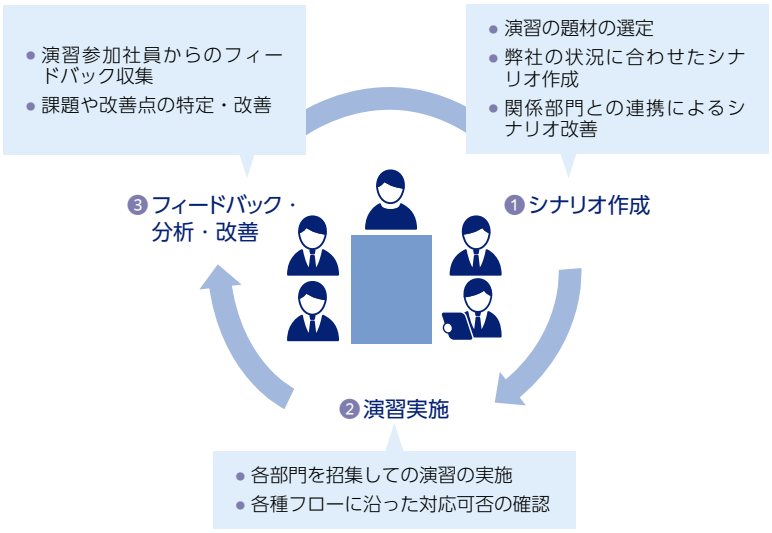
ランサムウェア感染などのテーマを決めて演習シナリオを作成します。作成したシナリオが実際に起こりうる状況を反映していることを確認するために、演習シナリオ内で侵害されるシステムの担当部門とも連携します。

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、参加部門が予め定められた対応フローの中で役割を果たせるか確認します。また、社内外への情報共有の連絡内容や、プレスリリース内容の検討など、実際のインシデント対応のシチュエーションに合わせた実践的な演習を行っています。

❸ フィードバック・分析・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 ガバナンス向上への取り組み

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。

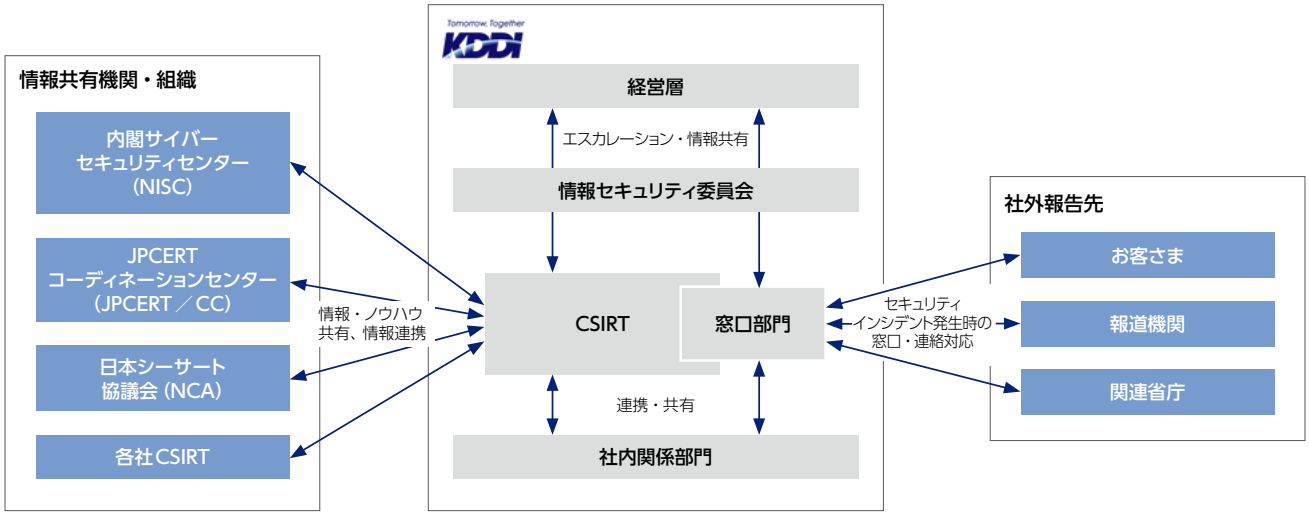
2 サイバー攻撃に対する取り組み

CSIRT体制

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。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※との連携を開始しました。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。

※ 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

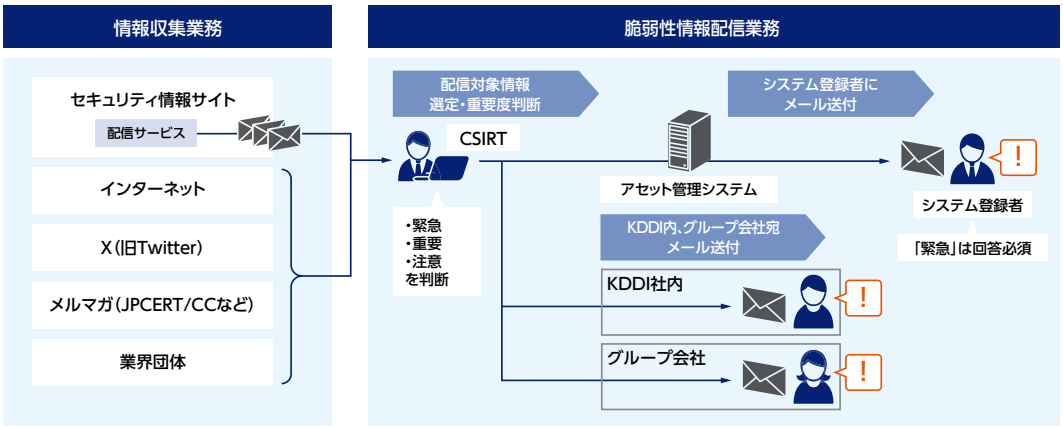
情報共有機関・社外報告先との連携体制図



セキュリティ強化に向けた施策

● 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。

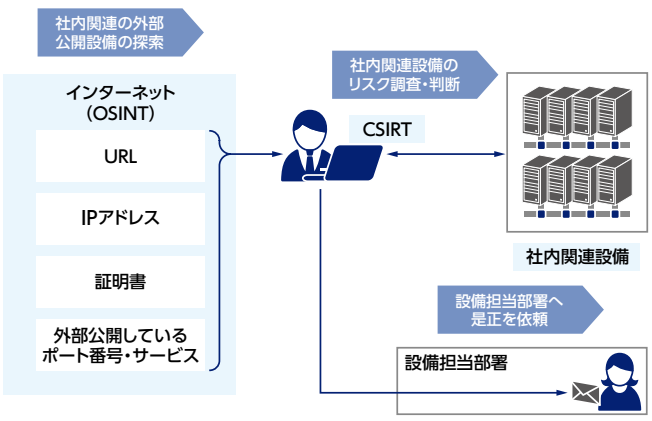


● 外部からのアタックサーフェス調査・是正

近年、インターネット上でさまざまな新たなサービスが展開されていることに伴い、サイバー攻撃の対象となる領域（アタックサーフェス）も拡大しています。特にこの領域の中で、VPN（Virtual Private Network）、RDP（Remote Desktop Protocol）、SSH（Secure Shell）といったリモート通信をサポートする外部公開機器が攻撃者の標的になっています。これらの機器に脆弱性や管理不備が存在すると、認証回避やパスワード情報の漏えいなどを起因とした不正アクセスによる大きな影響が発生し、実際に攻撃を受けた企業も報告されています。

KDDI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、防御側の視点だけではなく、攻撃者視点から能動的な調査を実施しています。この能動的な取り組みにより、通常の脆弱性診断では特定が困難なホストや、管理が不十分なホストの検出が可能となっています。

具体的な実施策としては、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やURL、証明書情報などを活用して、外部に公開されている社内関連設備を探索します。この探索で関連ホストが確認された場合、攻撃リスクや管理状況の評価を行います。リスクが高いと判定された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、KDDIでは攻撃者の視点によるアタックサーフェス調査を取り入れることで、外部公開されている社内の脆弱な機器を網羅的に特定し、組織全体のセキュリティ強化を図っています。

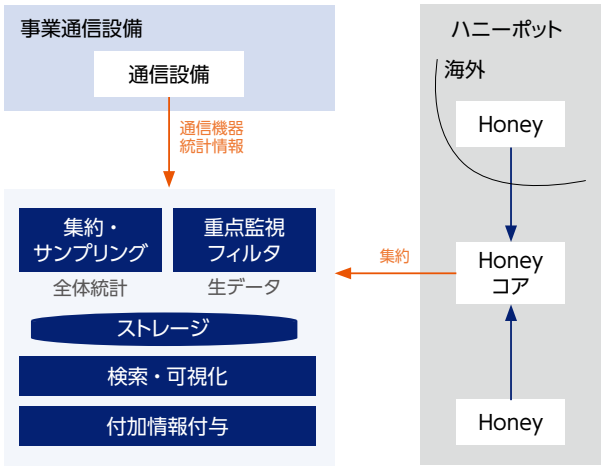
監視技術の高度化

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。

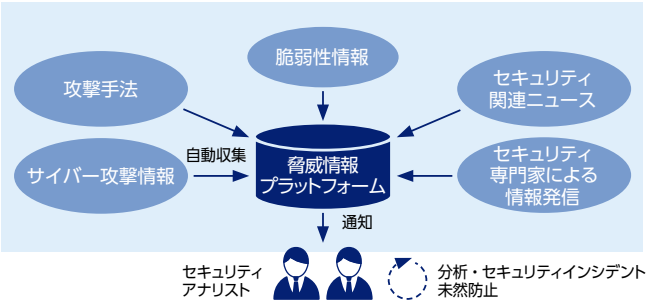
KDDIグループにて開発した攻撃通信観測システムの概要



● 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。2023年3月に開発した「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。



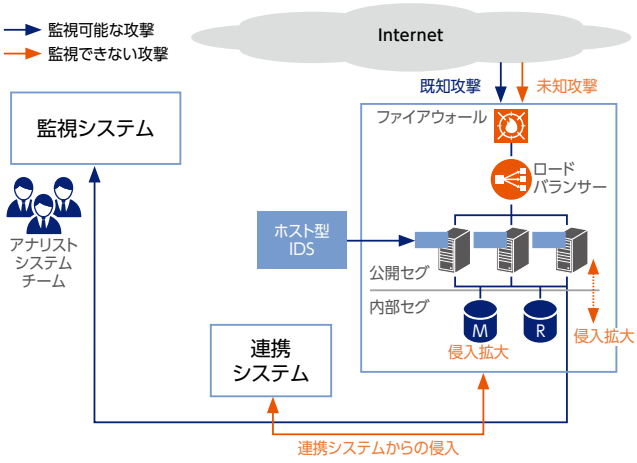
セキュリティ強化に向けた施策

● サーバ型EDR

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サーバ型EDR (Endpoint Detection and Response) 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。

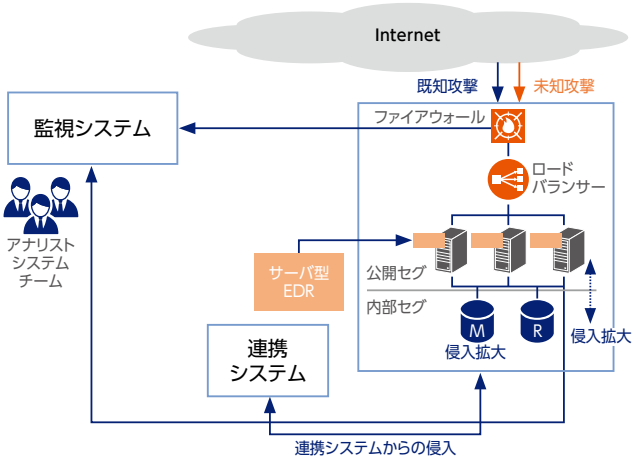
現状の課題

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

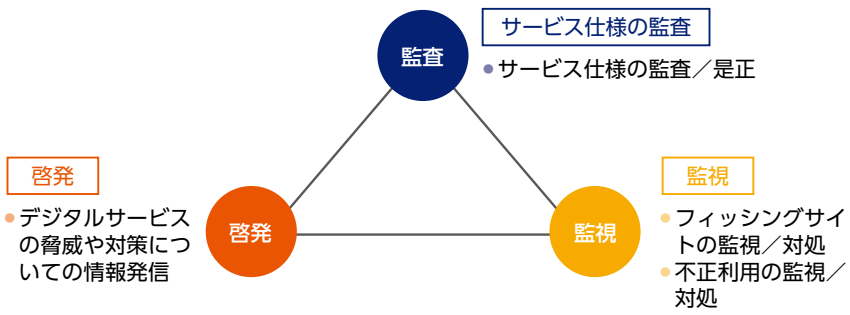
サーバ型EDRを導入し、ログを集約する。



3 サービス不正に対する取り組み

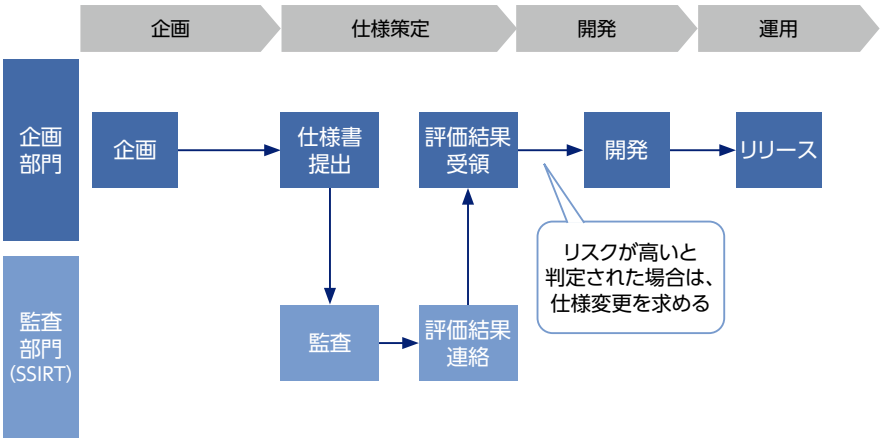
SSIRT体制

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3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。



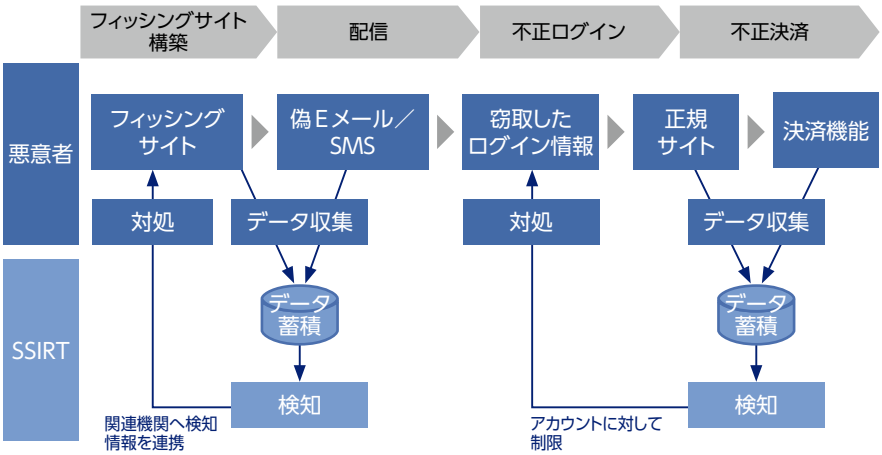
● サービス仕様の監査

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。



● フィッシングサイト・不正なサービス利用の監視

フィッシング詐欺への対策として、SSIRTではふたつの監視を行っています。ひとつは、「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。もうひとつは、「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。



● お客さま啓発

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。

先端技術による情報セキュリティの開発・研究

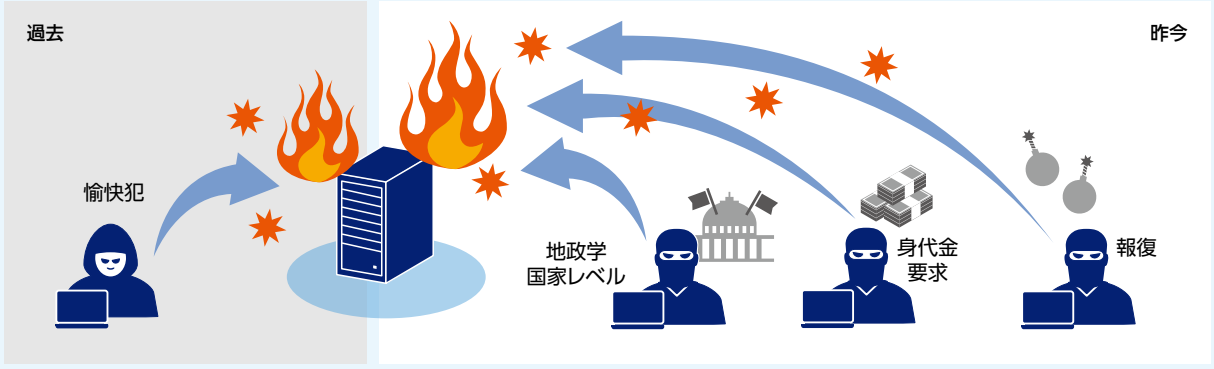
日々進化し深刻な脅威となっているサイバー攻撃に対応するため、KDDIでは先端技術を活用した情報セキュリティ対策に注力しています。生成AIや機械学習などの革新的な技術を取り入れ、より強固なセキュリティ体制の構築を目指しています。本章では、KDDIが取り組んでいる先端技術を用いたセキュリティ施策について紹介します。

先端技術

1 DDoS攻撃の可視化による防御力向上の試み

KDDIでは、DDoS攻撃（Distributed Denial of Service attack（分散型サービス妨害攻撃））の可視化プロジェクトに取り組んでいます。DDoS攻撃とは、特定のサーバやネットワークに大量のデータを送りつけて、正常な通信を妨げる攻撃のことです。DDoS攻撃の市場は、過去数年で大きく変化しています。以前は、主に愉快犯による攻撃が多くを占めていましたが、現在では、身代金を要求する経済的利益を狙った攻撃や、特定の国や政府機関を標的にした政治的な目的を持つ攻撃が増加しています。この変化に伴い、攻撃手法もより高度化しています。

DDoS攻撃市場の変化



なぜ可視化なのか

現在のシステムでは、KDDIのネットワークに対する攻撃のみが検知できていますが、攻撃の高度化が進み、発生状況が見えにくいのが現状です。そこで、KDDIでは新たなDDoS対策として、攻撃の「可視化」を進めています。

可視化によって、以下のような情報が明らかになります。

- **新規攻撃の発生状況:** 新たに発生する攻撃をリアルタイムで把握できます。
- **特定ターゲットへの攻撃:** どのシステムが狙われているかを明確に把握できます。
- **攻撃の詳細の把握:** 攻撃の変化や不正活動の確認が可能になります。

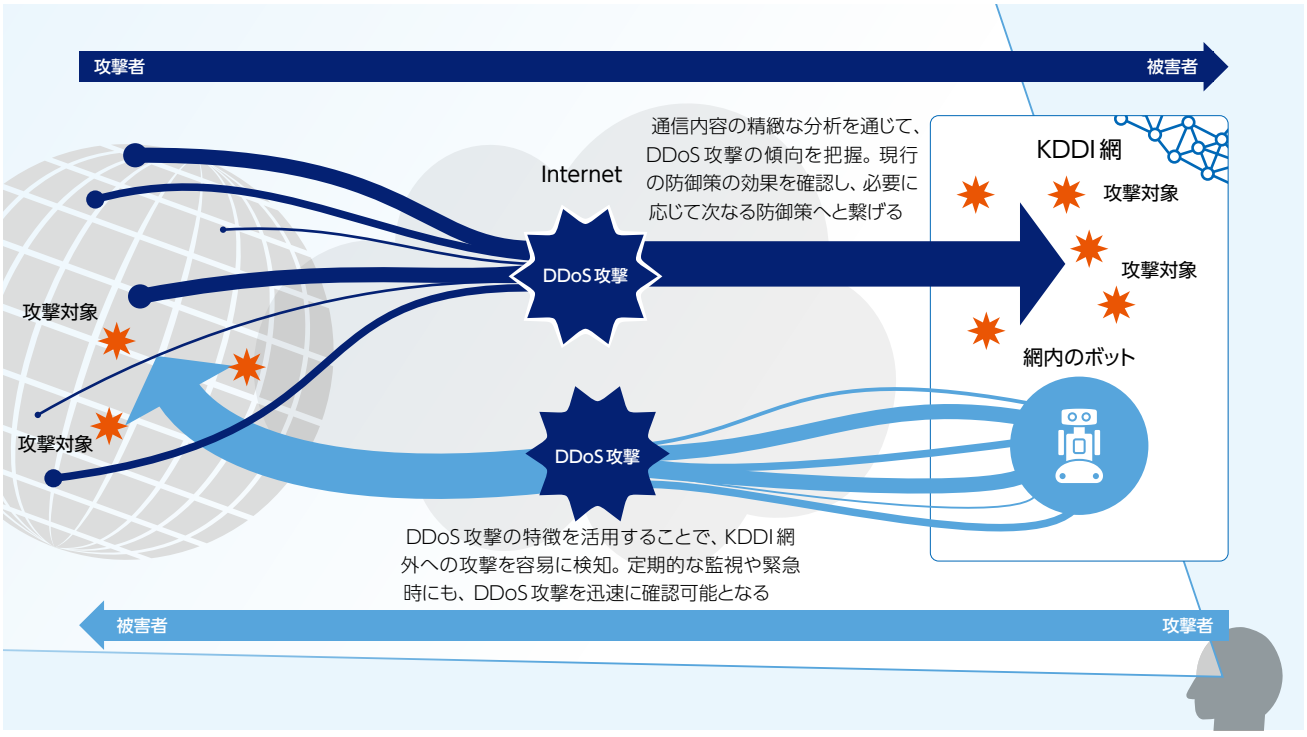
攻撃者の手法が年々進化するDDoS攻撃に対応するため、実際の攻撃の発生情報を調査し、防御方法を検証するとともに、生成AIや可視化を行い攻撃の分析を進めています。

これまでは単に攻撃の発生を確認し、特定の攻撃に対する防御が可能でしたが、特定のネットワーク宛の攻撃を可視化することで、攻撃以外の異常な挙動や不正なアクセスを試みる通信も観測できるようになりました。

DDoS攻撃の可視化による効果

KDDIのネットワークで発生しているDDoS攻撃を可視化することで、攻撃の発生状況を量でしか把握できなかったものが、時系列で情報が得られるようになります。これにより、事前に攻撃の挙動を調査し、防御方法に役立てることが可能です。また、攻撃によっては実際の攻撃の予兆が見られることもあり、これらはKDDIのDDoS対策システムに活用されます。

DDoS攻撃の可視化



DDoS攻撃の可視化を通じて、これまで確認が難しかった攻撃状況を把握できるようになります。DDoS攻撃に限らず、全体の攻撃状況を把握することが可能です。さらに、攻撃に加担している状況を観測することや、AIが生成した攻撃の特徴の有効性を確認することもできます。

これらの可視化の取り組みを通じて、KDDIは新たなDDoS対策装置の開発と運用に取り組んでいます。

サイバー攻撃に立ち向かう DDoS攻撃の可視化プロジェクトの取り組み

DDoS攻撃は、一般的に想像されるサイバー攻撃とは少し異なります。攻撃手法について言及すると、マルウェアを利用した不正侵入やサービスの脆弱性を突く不正利用と比べ、非常に単純な攻撃であることが特徴です。要するに、「何でもいいから大量に通信を流してシステムをダウンさせよう」というのがDDoS攻撃の本質です。

一方で、対策が簡単かというと、実際には奥が深く、攻撃であると判断する基準やその対策については非常に難しいサイバー攻撃となります。

私の所属する部署では、DDoS攻撃からKDDIの通信網を守るためのシステムを企画・開発から運用・保守までを実施しています。その一環として、本誌に掲載しているDDoS攻撃の可視化と、並行して進めているDDoS攻撃に対する検知・対策の高度化に取り組んでいます。

本施策は、3年ほど前に「3年後のDDoS攻撃市場の変化予想とそれに向けた対策は何か」という議題から発展しました。これに基づき、対策ポイントの特定や方法の検討を行い、DDoS攻撃の可視化施策を進めています。高度な攻撃に対して漏れなく、過剰に対応しないことを方針としDDoS攻撃の検知・対策の高度化施策に取り組んできました。

最も困難だったことは、DDoS攻撃を正しく判断することでした。前述の通り、DDoS攻撃は単純でありながら、その判断が難しい攻撃です。しかし、課題から目を背ければお客さまや事業への影響につながる一方、詳細に分析しようとすると「通信の秘密を守る」という制約に直面します。さらに、通信量は日に日に増加し、数Tbpsもの膨大なデータ量となるため、目検・手作業で分析を行い、攻撃を判断するということは非常に困難です。

このような状況で悩んだ結果、その膨大なデータを分析するために統計的分析や機械学習のツールを導入し、分析者の工数削減が可能となりました。正直なところ、自身にネットワークやセキュリティの知識だけでなく、統計学や機械学習も求められるとは思いもしませんでしたが、優秀な上司や同僚、また協力してくれたメンバーのおかげで乗り越えることができました。

既に運用しているDDoS攻撃の可視化に加え、現在進行中のDDoS対策の高度化を完遂することで、KDDIのサイバーセキュリティをより強固なものにします。そして、KDDIのサービスやネットワークを利用される皆さまに、今後も安心を提供できるよう努めていきます。

情報セキュリティ本部 システムセキュリティ部 北沢 尭宏

2 kCAPTCHAによる不正検知の取り組み

kCAPTCHA（ケイキャプチャ）は生成AIの活用で従来よりも視認性の高い認証画像を利用したログイン認証技術です。KDDIでは、高度化するサイバー攻撃の動作を検知・防止するため 2024年11月12日からkCAPTCHAをau IDログイン認証に導入しました。

KDDI総合研究所で開発されたこの技術は、近年の生成AIなどの先端技術の悪用によるインターネットへのサイバー攻撃が高度化に対応するために研究・開発されました。これまでサイバー攻撃への対策としては「ゆがんだ文字を読み取る」「ある題材の描かれた画像を探す」など「機械（コンピュータープログラム）には解けないが、人間には解ける問題を出す」ことで、機械からの攻撃を防ぐことを目的としたCAPTCHA（キャプチャ）がログイン認証時などによく用いられています。

しかし、生成AIを使った技術の進歩により機械の回答能力が向上しており、従来型のCAPTCHAでは十分に不正なログインを防御できなくなっています。昨今ではログイン認証時に出題する問題が複雑化しており、利用者が回答する際にも判別しづらくなっています。生成AIを使った新たな時代の攻撃はWEBサイトを運営するさまざまな企業にとって深刻な脅威となっています。

kCAPTCHAは生成AIなど高度化する機械攻撃を高精度に検知可能にするために研究・開発されました。kCAPTCHAによって機械攻撃を検知し対策をとることで、なりすましやフィッシング詐欺、サービスの乱用など事業継続を妨げるさまざまな不正アクセスを防ぐことができるようになっています。

金融サービスのログイン画面	電子商取引サイトの購入手続き	生成AI・検索	オンラインフォームの送信時	SNS
なりすましやフィッシング詐欺などの攻撃を抑制し、お客さまを被害から守ります	自動操縦攻撃による不正決済を未然に防ぎます	高価なサーバ設備を攻撃から守ります	いたずらや迷惑行為などによる送信を抑制し、コスト削減を実現します	ボットによるクロールなどの大量アクセスからサイトを保護しコンテンツを守ります

kCAPTCHAの特徴

kCAPTCHAは、生成AIなどの先端技術とKDDI総合研究所で開発した独自技術を組み合わせて作られています。主な特徴としては以下のようなものが挙げられます。

（1）生成AIなど高度化する機械攻撃に対する検知精度の向上

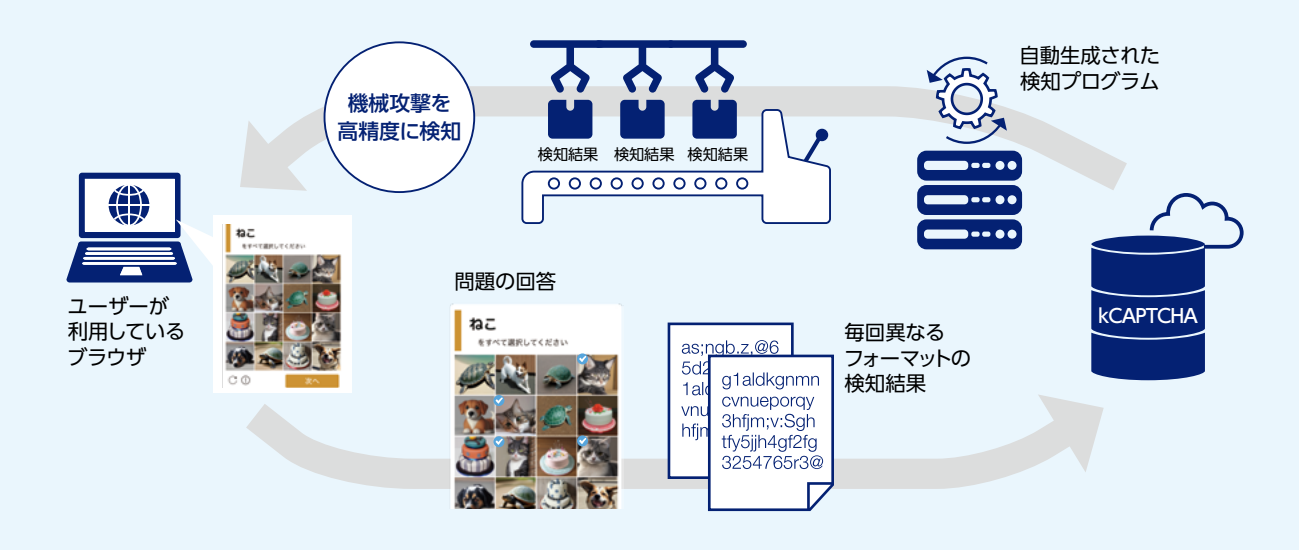
ログイン認証時に出題する問題の難易度のみに依存せず、問題を解く過程で行われる動作をもとにした検知により、従来では発見できなかった機械攻撃を高精度に検知します。

（2）検知プログラムの自動生成による不正な攻撃への対抗強化

kCAPTCHAでは検知プログラムの高度化により、従来のCAPTCHA製品では難しかった生成AIなどを使った機械攻撃への対抗を強化しています。（注）特許第7451464号

(3) 生成AIの活用による認証時のユーザビリティ改善

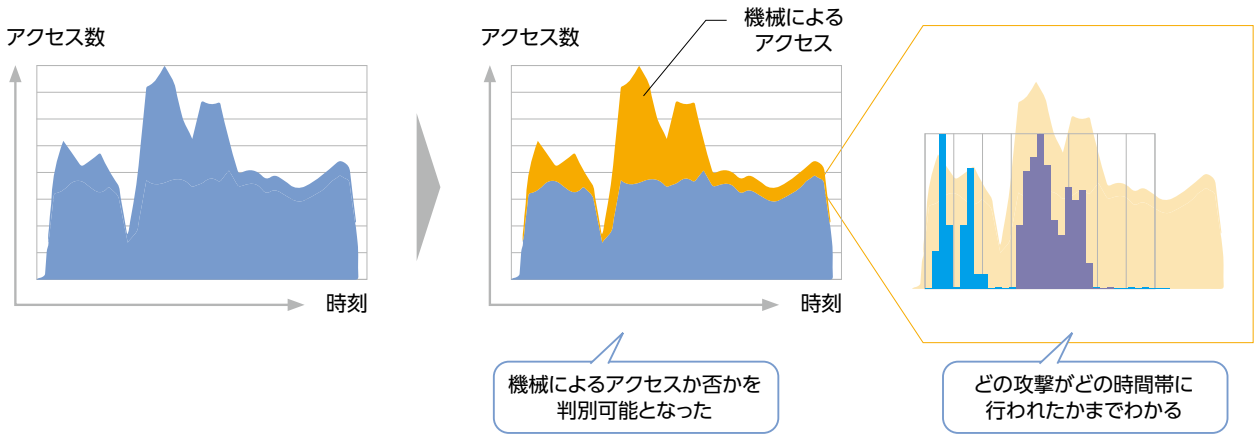
kCAPTCHAでは、ログイン認証時に出題する画像を表示する場合、生成AIの活用で、高解像度かつ視認性が高い画像を生成します。これにより利用者に判別しやすく不快感の少ない画像を提示することができるようになりました。



kCAPTCHAの効果

KDDIでは、kCAPTCHAの導入によりこれまでのCAPTCHAでは発見できなかった機械攻撃を発見することに成功しました。以下のグラフではこれまでユーザーアクセスの集中だと考えられていたアクセスの増減のうちオレンジ色の部分が機械攻撃であることが判明、アクセスの集中と考えていたものの大半が攻撃であったことも判明しています。

kCAPTCHAではさらにこれらの攻撃が具体的にどのように行われたかまで分析ができるようになり、下の水色と紫色の棒グラフのようにどの攻撃がどの時間帯に行われたかまでわかるようになりました。



kCAPTCHAの今後

サイバー攻撃の高度化に伴い、お客さまが実施すべきセキュリティ対策も多様化しています。KDDIとKDDI総合研究所は、本技術や、本技術を運用するノウハウを提供するため、将来的な「kCAPTCHA」の法人のお客さまへの販売も含め、社会のサイバーセキュリティ対策の向上と、お客さま体験価値の向上の両立に向けて取り組んでいきます。

パーソナルシステム本部 ライフデザインプラットフォーム部
亀山 和真

KDDI総合研究所
田淵 純一

お客さまを守る×利便性を両立する技術はどう生まれたか

今回開発されたCAPTCHA技術の背景について教えてください。

亀山：au IDログインでは、歪んだひらがなを読ませるCAPTCHAを導入していましたが、お客さまから「ひらがながうまく読めず、何度も間違えてしまう」というフィードバックが寄せられていました。一方で、攻撃を防ぐためにはセキュリティの強化も不可欠であり、二重の課題に直面していました。そこで、お客さまの利便性を高めながら、セキュリティも強化するCAPTCHAの改善ができないかと、KDDI研究所へ相談したのがきっかけです。

田淵：研究所で調査を進めてみると、CAPTCHAにはさまざまな課題があることが分かりました。特に解決すべき課題だったのは、人間が解ける問題と生成AIが解ける問題の境界が曖昧であることです。そのため、「問題が解けるかどうか」で人間と生成AIを判別しようとすると、難しい問題を出さざるを得なくなります。これでは、セキュリティを強化しても、お客さまにとって使いにくく、不便を強いる結果になってしまいます。

亀山：そのため、お客さまに難しい問題を解かせることや、複雑な操作を強いることを避けるべき、と話していましたね。

田淵：そうですね。そこで、研究所では自動操縦を行うブラウザ攻撃に注目しました。さらに、研究所で取り組んでいる通信を守るための暗号技術の開発経験を活かし、その知識を検知プログラムへ応用することで、偽装を見破る方法を思いつきました。

亀山：攻撃の検知手法については、研究所のメンバーとともに多くのアプローチを試しました。その結果、他のシステムでは検知できなかった攻撃を見破ることができるようになり、この検知技術をCAPTCHAとしてさまざまなサイトで利用できる形にしたのが今回の製品です。

今後、利用者はこのようなkCAPTCHAの問題を解く機会は増えるのでしょうか？

田淵：いいえ、お客さまが実際にkCAPTCHAの問題を解く機会はほとんどありません。kCAPTCHAでは、問題を出す前に行う攻撃の検知技術が大幅に進化しています。何度もアクセスした程度では問題が表示されることはありません。ほとんどのお客さまは一度も問題を目にすることなく、安全にサービスを利用できると考えています。

亀山：攻撃の検知精度が非常に高いため、リリース前の試験で問題を表示させることが難しかったです。

田淵：これもkCAPTCHAの特長のひとつですね。

亀山：ほとんど目にすることがないということ自体がユーザー体験の向上に繋がっていると感じています。この安全性と使いやすさのバランスを取ることで、私たちはより多くのユーザーに安心してサービスを提供していきたいと考えています。

3 SBOM導入に向けた実証事業

通信分野において、オープンソースソフトウェア（OSS）の利用が急速に普及拡大しており、ソフトウェアは多数のOSS等による複雑な組合せへと変化しています。また、通信インフラの長期運用性によって、新旧様々なバージョンのソフトウェアが混在している状況です。そのため、ソフトウェアのバージョン管理を含む構成管理が煩雑になっています。このような事情を踏まえ、ソフトウェアに脆弱性が発見された際の対応を迅速化するため、通信分野においてもソフトウェア部品等を一覧化したSBOM（Software Bill of Materials）が注目されています。

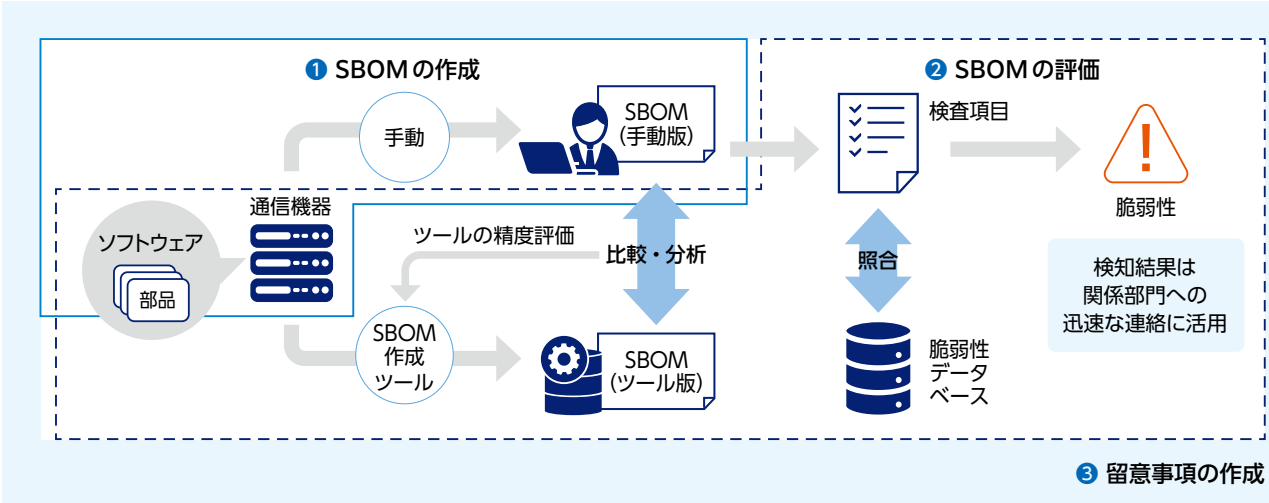
そこで、KDDIでは、2023年度に総務省から「通信分野におけるSBOMの導入に向けた調査の請負」事業を受託し、KDDI総合研究所、富士通株式会社、日本電気株式会社、株式会社三菱総合研究所とともに、❶～❸の分担により、通信分野へのSBOM導入に向けた実証事業を実施しました。

❶ SBOMの作成（担当：富士通／日本電気）
通信事業者が実際に使用または使用予定の通信機器を選定し、SBOM作成ツールから出力したSBOMを基に、ソースコード等を確認しながら手動追記して、抜け漏れの無い網羅的な「手動版SBOM」を作成しました。

❷ SBOMの評価（担当：KDDI ／ KDDI総合研究所）
SBOM作成ツールとして有償ツール２つと無償ツール４つを選定し、そのうち３つのSBOM作成ツールを用いて、❶の機器に対する「ツール版SBOM」を作成し、「手動版SBOM」との比較・分析により、精度評価を実施しました。更に、「手動版SBOM」記載の検査項目を用いて、脆弱性データベースとの照合により、脆弱性情報をどの程度検知できるかを検証しました。

❸ 国内外動向の調査及び留意事項の作成（担当：三菱総合研究所）
SBOMに関連した国内外動向調査として、主な国と分野及び要件・基準と手順・方法について、主要な事例の全体像を整理しました。更に、通信分野において、SBOMの作成、共有、活用プロセスに基づき章構成を体系化し、SBOMの費用対効果に関するKPIや通信分野の要求に対応した主な留意事項を項目レベルで整理しました。

SBOM導入に向けた実証事業の全体概要



我が国の通信分野において、脆弱性管理のための手法としてのSBOMの有効性を検証するとともに、通信事業者が実際にSBOMを運用・導入していく上での課題等を整理しました。更に、2024年度は、我が国の通信分野におけるSBOM導入に向けた留意事項を整理するため、同じ体制のもと本事業に取り組んでいます。

SBOM導入の現状と未来への道筋

このプロジェクトが社会に与える影響や貢献について教えてください。

SBOMは、2021年に出された米国の大統領令をきっかけとして、近年注目されるようになったソフトウェア部品表の新技術です。それ以降、海外では、米国を中心にして、SBOMを導入・活用するためのガイドラインやガイダンスが発表されています。日本国内でも、経済産業省が「ソフトウェア管理に向けたSBOMの導入に関する手引」を公開しています。その中でも、SBOMの取組みは政府調達や自動車分野、医療機器分野で先行しています。一方、通信分野では、SBOM導入が十分進んでいるとは言えず、通信機器ソフトウェアを対象とした場合の課題や有用性はまだわかっていない状況でした。本実証事業では、実際の通信機器ソフトウェアに対し、SBOMを作成・評価を実施することにより、SBOM作成、SBOM共有取得、SBOMによる脆弱性管理の観点でそれぞれ課題を抽出しました。このプロジェクトにより、通信業界におけるSBOM導入の課題を整理し、今後の普及に向けた留意事項を明確にすることを目指しています。本実証事業の成果報告として、総務省のサイトにて公開しています。

SBOM技術の導入によって、どのような実務的な課題が解決されると考えていますか？

OSS（オープンソースソフトウェア）を活用した製品開発は通信分野でも進んでいるため、実務ではどのOSSが含まれているかを把握することが難しい状況になっています。SBOMを活用すれば従来よりも製品に含まれているOSSの把握が容易になり、脆弱性管理やライセンス管理のスピードアップやコスト削減につながります。ライセンス管理については、SBOMの導入により、ライセンス違反のリスクを低減することが可能です。ただし、ソフトウェアのライセンス違反のほとんどは、その対象の企業が大きな損害を被るだけで影響は限定的になると思います。一方、ソフトウェアの脆弱性はサイバー攻撃の標的となり、世界的に大規模なセキュリティインシデントを引き起こし、社会的に大きなインパクトを与えかねません。そのため、ソフトウェアの脆弱性管理はセキュリティ上の重要な課題であり、SBOMの導入により、その課題解決が期待されています。

事業が完了した後、SBOMはどのように発展していくと考えていますか？　SBOM実証事業が企業のセキュリティ文化に与える影響についてお考えをお聞かせください。

SBOMは現在、過渡期にあり、多くの課題を抱えている状況ですが、今後発展していく技術です。実際、SBOMの標準フォーマットは現在もメジャーバージョンアップが行われていますし、SBOMツールは精度向上も含め進歩しています。そのため、本実証事業が完了した時点で、通信分野においてSBOMが導入されるには課題が残っており、広く普及する段階には至っていません。重要なシステムや脆弱性管理が必要不可欠な領域で限定的に導入が検討される、くらいにとどまると思われます。しかしながら、SBOMに関する取組みは世界的に進行中であり、特に海外における規制動向によっては、日本でも急速に状況が変わる可能性があります。本実証事業は2024年度も継続しており、我が国の通信分野におけるSBOM導入に向けた留意事項を整理しています。世の中の情勢が変化し、通信事業者や通信機器ベンダがSBOMを導入する必要が出てきた場合には、後れを取らずに着手できるよう参考にしていただけるような留意事項を作成していきたいと考えています。

サプライチェーンの取引先との信頼関係を構築しつつ、自社の設備に含まれるOSSを把握することで、セキュリティのスピードアップやコスト削減につなげていくセキュリティ文化が醸成されていくことを期待しています。

情報セキュリティ本部 セキュリティ管理部 太田 陽基

4 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。

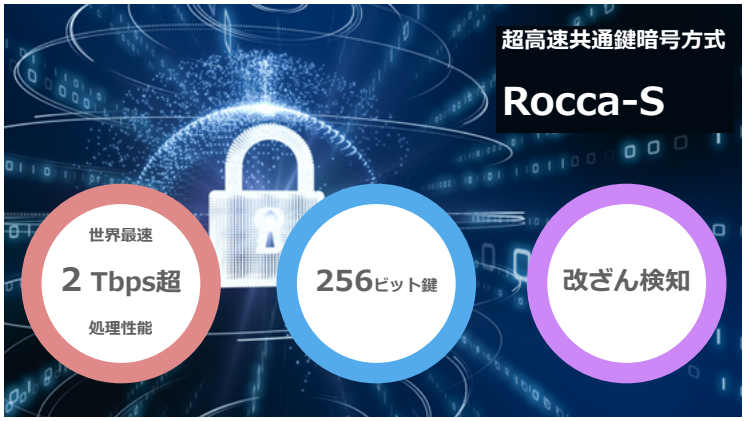
- パスワードによるソフトウェアやハードディスク内データの暗号化
- 同じ電波を使っていても隣の人の通信内容を読み取れないWi-Fi通信の暗号化
- オンライン会員登録時の入力内容の暗号化
- オンラインショッピングサイトでの住所・氏名や決済情報の暗号化

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。そのひとつの課題は、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。もうひとつの課題は、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、ふた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2024年11月時点の世界最速と

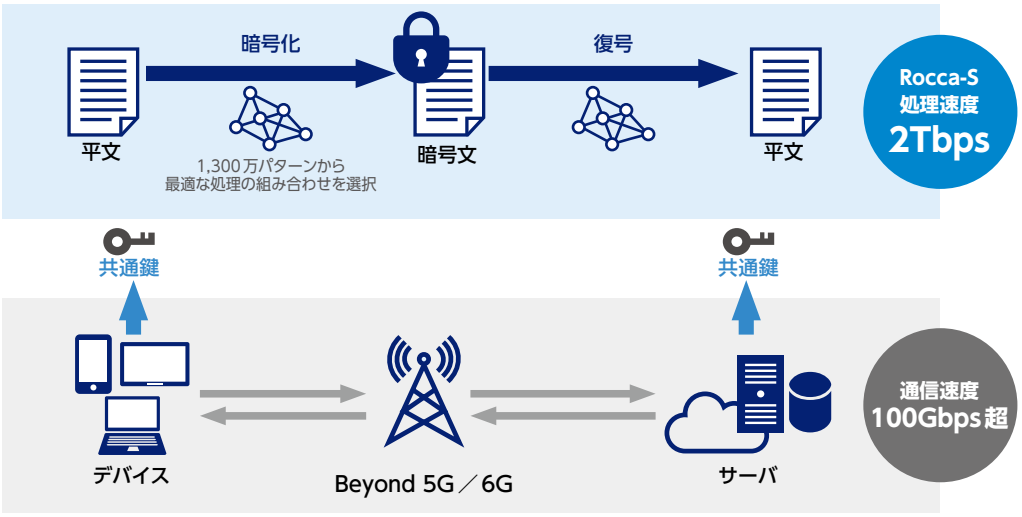
なる200Gbpsの速度を達成し、スマートフォンでも100Gbps以上の速度を記録しています。また、Rocca-Sは量子コンピューターによる解読に備えて256ビットの鍵に対応しており、現在知られている攻撃に対する安全性も確認済みです。さらに、データが途中で改ざんされていないかを検知する機能も備えているため、セキュリティ面でも大きな進歩を遂げています。

Rocca-Sの特徴



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の設計にあたっては、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。2024年11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。

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

セキュリティ事業への取り組み

1 セキュリティ事業への取り組み

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、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、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
当初計画 1,000台 → 見直し後 1万3800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

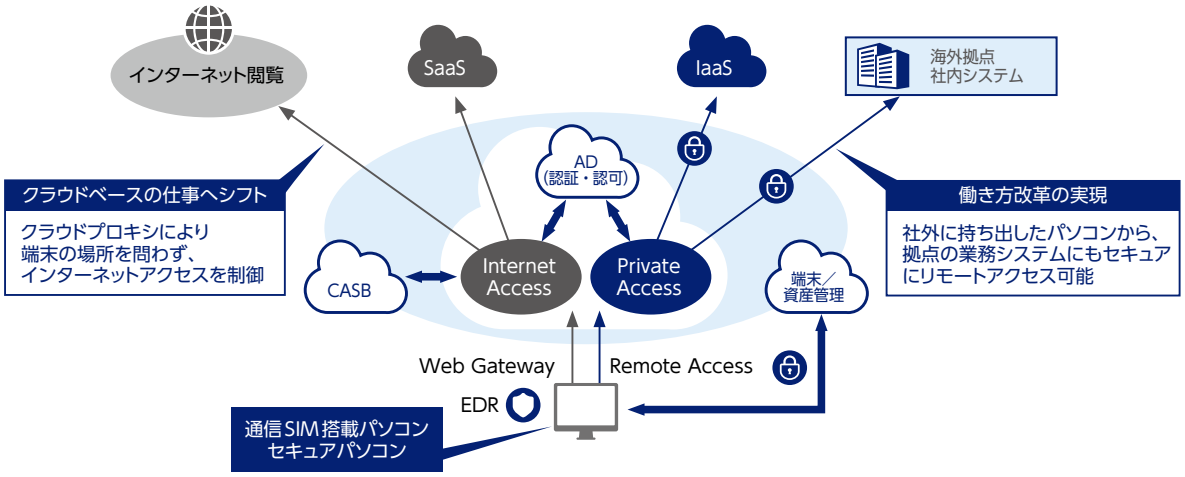
全社合計1万3,800台に及ぶデバイスの導入・配布を開始し、国内拠点のゼロトラストの導入を完了しました。クラウドソリューションを組み合わせることで迅速に導入ができ、テレワーク、オフィスワークを問わず、ストレスなく利用できるという効果が得られています。その後、国内で培ったノウハウをベースに、数年をかけてゼロトラストを海外現地法人にも導入を進め、22ヵ国49拠点へ海外展開をしました。

セキュリティ事業への取り組み

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、ゼロトラストコンポーネントであるSWG (Secure Web Gateway)、エンドポイントセキュリティ、CASB (Cloud Access Security Broker) ※など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。

※ キャスビー・従業員のクラウドサービスの利用を監視、適切なセキュリティ対策を行うソリューションのこと



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

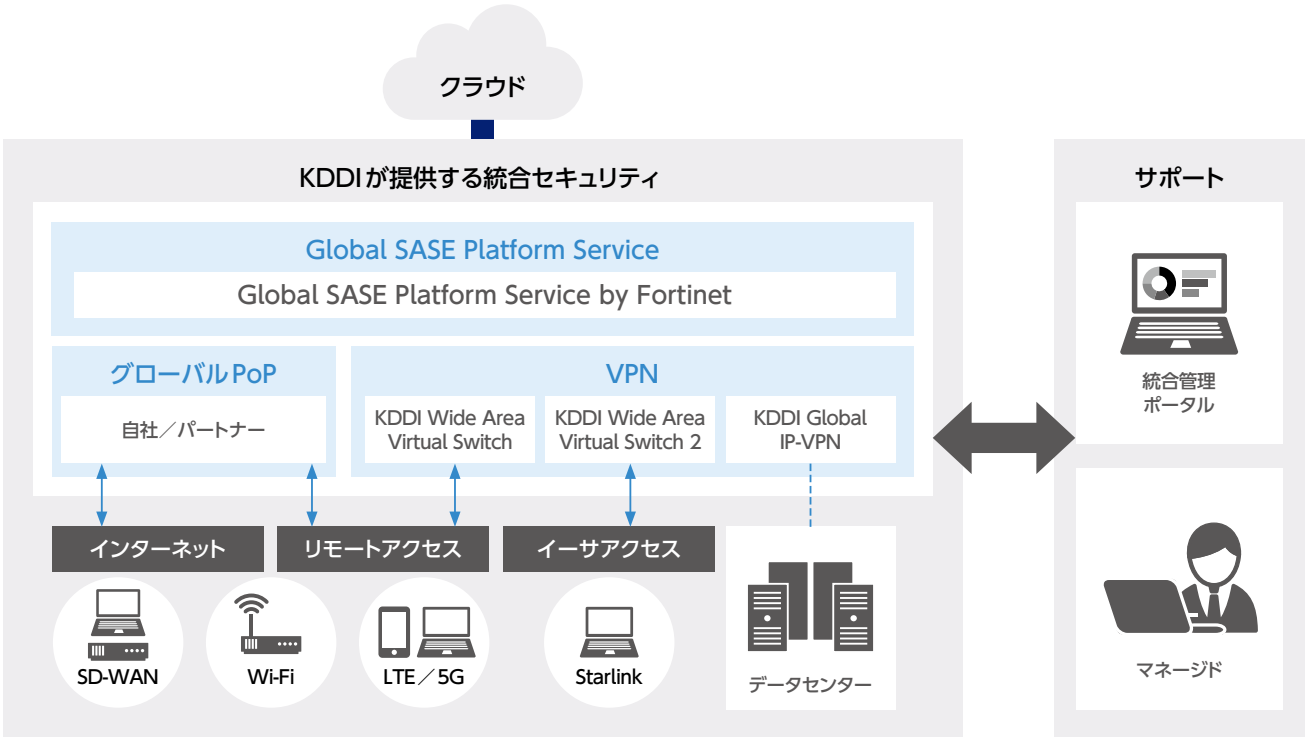
● 国内外のお客さまのセキュリティ対策を支援

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

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 KDDIマネージドセキュリティサービス

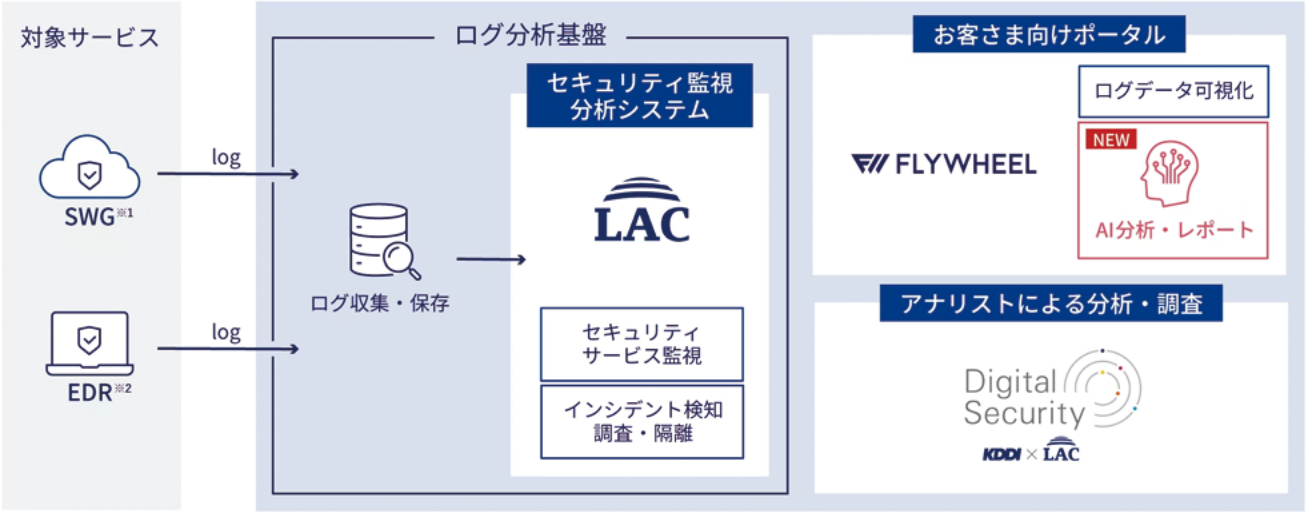
KDDIマネージドセキュリティサービスとは、WAKONX（ワコンクロス）を構成するサービスとして、KDDIのログ分析基盤とLACがこれまでに蓄積したインテリジェンス情報を標準提供、LACの知見をベースとする高度・高品質なログ自動分析エンジンを活用し、お客さまのゼロトラスト環境に必要なセキュリティ監視・運用を提供するサービスです。セキュリティログの監視・通知・対処を行い、複数のセキュリティサービスから収集される膨大なログに対し、ひとつの基盤で自動分析することでインシデント発生の早期検知、セキュリティアナリストによる分析・アドバイスを受けられます。

2024年6月より、生成AIを活用してセキュリティ要約レポートを自動作成する機能を標準機能として追加しました。本機能の追加により、セキュリティサービスのアラートの状況や傾向が可視化されるほか、生成AIが自動作成したアラート情報の要約レポートが提供可能になり、セキュリティ対策の迅速化・効率化を支援します。KDDIのグループ会社であるフライウィールが提供するデータ活用プラットフォーム「Conata」が、複数のセキュリティサービスから収集される膨大なログを分析し、アラート状況を可視化します。また、アラート状況の要約レポートを生成AIが自動作成します。アラート状況や要約レポートは、お客さま任意のタイミングでダウンロード可能です。アラート状況の要点を明確化することで、セキュリティリスクの傾向・状況などの現状把握と、改善策の検討を支援します。

セキュリティ事業への取り組み

KDDIマネージドセキュリティサービス

ログ分析基盤とLACのノウハウが入った自動分析エンジンを活用し、お客さまのゼロトラスト環境に必要なセキュリティ監視・運用を提供



※1 SWGはSecure Web Gatewayの略称です。Zscaler、Cisco Umbrellaが対象サービスとなります
※2 EDRはEndpoint Detection and Responseの略称です。Microsoft Defender for Endpoint、Crowdstrike Falconが対象サービスとなります

WAKONX

「WAKONX」は、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。」の実現に向け、日本のデジタル化をスピードアップするというコンセプトから生まれたブランドであり、機能群を有する生成AI時代のビジネスプラットフォームです。「WAKONX」を通じて、最適化したネットワークの設計・構築から、大規模計算基盤による企業間データの蓄積・融合・分析を行います。また、生成AIが組み込まれたサービスやソリューションを各業界に最適化して提供することで、法人のお客さまの事業成長と社会課題の解決を支援していきます。

KDDIが推進するセキュリティの未来：生成AIによる要約レポート機能の導入

KDDIが提供するマネージドセキュリティサービス（以下MSS）に新たな機能として生成AIを活用したセキュリティ要約レポートの自動作成機能が加わりました。

Q1: MSSの新機能リリースに向けたプロジェクトが始まった背景やきっかけは何ですか？

福岡：私たちは2021年から「日々のセキュリティ状況をお客さまに代わって把握し、有事の際にはサイバーセキュリティの専門家に全てお任せできる」KDDIマネージドセキュリティサービスを提供していますが、さらなるサービスの顧客価値向上が求められている状況にありました。

高橋：企業のデジタル化が進む一方で、サイバー攻撃も増加しており、対策の手間を軽減するために自動化が求められていました。サービス企画を担当している私は、この流れに乗り、生成AIを活用することでより効率的なサービスを提供しようと考え、生成AIによる要約レポート機能の導入検討が始まりました。

Q2: このプロジェクトで直面した最も大きな課題は何でしたか？

福岡：MSSの顧客価値向上のため、お客さまの本質的な課題を解決することです。サービスを利用されるセキュリティ管理者さまの業務把握から仮説を立て、「日々のセキュリティのアラート状況や傾向をスピーディーに把握したい」「有事の際には対応～報告レポートまでセキュリティの専門家に任せたい」というニーズに対し生成AIを活用することで解決できると道筋を立てました。

林：それに伴い、より多くの企業にサービスを活用してもらうために、ターゲットとなる顧客像を一新しました。企業のセキュリティに関わる担当者や管理者だけでなく、実際に導入を決定する責任者やステークホルダーが何を知りたいのかにも焦点を当て、お客さまの声を直接ヒアリングするなど、開発担当としてお客さまへの提供価値にこだわりました。

高橋：開発における納期の厳しさも課題でした。当初は生成AIを使用した機能のリリースのみが決まっている状態でした。加えて通常の開発であればリリースまで1年くらい要しますが、半年後のリリースということもあり、納期も非常に短く、通常の開発よりも急ピッチで進める必要がありました。

Q3: 課題を克服するためにどのようなアプローチを取りましたか？

高橋：私たちは、進行中の変更や改善にも迅速に対応できる段階的な改善手法を導入し、企画と開発の迅速化に努めました。特に、一緒に開発を進めていたフライウィールというKDDIグループ会社との定期的なミーティングを設け、意見や認識齟齬をなくすよう努めました。また、開発チームと密に連携し、設計段階からフィードバックを得ることで、品質を確保するよう心がけました。

Q4: サービスの将来の展望について教えてください。

林：将来的には、生成AIを活用してさまざまな製品のログを関連付けて相関分析できる機能や、アナリストと同等レベルの分析を可能とする機能を充実させ、より高度なセキュリティプラットフォームを構築したいと考えています。また、KDDIが持つさまざまな法人サービスとセキュリティをかけ合わせていくことも視野に入れています。これらにより、お客さまが安心してデジタル環境を活用できるよう支援していきたいです。

左：ビジネスデザイン本部 DXプロジェクト推進部 **福岡 千紗**
中：プロダクト本部 ネットワークサービス企画部 **高橋 遼平**
右：ソリューション推進本部 システム技術部 **林 優太**

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・不注意にかかわらず、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	2023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停止件数	単体	ー	件	0	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	0
個人情報の漏えい件数				0	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または2022）※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

AI研究開発・SaaS事業
株式会社ELYZA

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
KDDIアジャイル開発センター株式会社
株式会社KDDIウェブコミュニケーションズ
株式会社フライウィール

教育事業
株式会社ディジタルグロースアカデミア

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
KDDI Sonic-Falcon株式会社※2

海外グループ会社
KDDI America, Inc.※3
KDDI EUROPE Ltd.
KDDI Deutschland GmbH
KDDI FRANCE S.A.S.
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
KDDI Myanmar Co., Ltd.

※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
※3 情報セキュリティ評価「TISAX」認証を取得

KDDIグループの概要

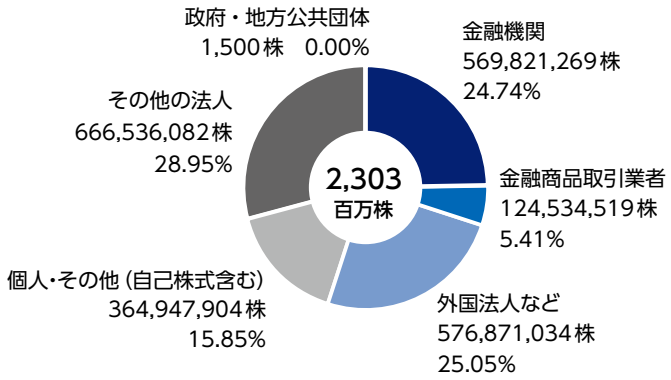
1 会社概要 (2024年3月31日時点)

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3丁目10番10号
本店所在地	〒163-8003　東京都新宿区西新宿2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	61,288名 (連結ベース)

2 株式の状況 (2024年9月30日時点)

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	553,939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)	持株比率※ (%)
京セラ株式会社	335,096,000	16.61
日本マスタートラスト信託銀行株式会社 (信託口)	329,737,800	16.35
トヨタ自動車株式会社	203,294,600	10.08
株式会社日本カストディ銀行 (信託口)	151,660,150	7.52
STATE STREET BANK WEST CLIENT - TREATY 505234	34,982,875	1.73
STATE STREET BANK AND TRUST COMPANY 505001	27,785,923	1.37
JPモルガン証券株式会社	27,562,048	1.36
STATE STREET BANK AND TRUST COMPANY 505103	22,479,000	1.11
JP MORGAN CHASE BANK 385781	21,308,669	1.05
SMBC日興証券株式会社	20,231,235	1.00

※ 当社は、自己株式175,121,584株を保有していますが、上記大株主から除いています。持株比率は自己株式を控除して計算しています。なお、自己株式には役員報酬BIP信託が所有する当社株式 (952,188株) を含んでいません。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/