あんしん安全で持続可能な社会を実現するために、私たちはセキュリティ監視基盤の構造改革と AI の活用により、サイバー攻撃からの防御力を高めてきました。
To realize a safe, secure, and sustainable society, we have enhanced our defenses against cyberattacks by reforming our security monitoring infrastructure and adopting the use of AI.

技術が進化するにつれて人々の生活は変わってきました。
With the evolution of technology, the lives of people have changed.

電話は普及に 35 年、インターネットは 7 年、一方で生成 AI はわずか 2 カ月で世界を席巻しました。
While the telephone and Internet took 35 and 7 years, respectively, to become widespread, generative AI took only 2 months to take the world by storm.

同様に、フィッシング詐欺や DDoS 攻撃などのサイバー攻撃は、急速に高度化・巧妙化しており、防御側にもそのスピードへの対応が求められています。
Similarly cyberattacks such as phishing scams and DDoS attacks are rapidly becoming more sophisticated and complex, necessitating defensive countermeasures and actions.

通信が社会の重要な構成要素の一つである中で、サイバー攻撃の早期検知と迅速な対処を行うためのセキュリティ監視は、私たちセキュリティエンジニアに課せられた重要課題です。
Because communication is a vital component of society, security monitoring for the early detection of and rapid response to cyberattacks is a critical task for security engineers.

セキュリティ監視の課題は三つ
Security monitoring entails three challenges.

第一に時間――新規に監視対象となるログの収集から分析までに要する時間が長く、攻撃者に隙を生まないため初動対応を迅速化する必要があります。
The first relates to time.
To prevent attackers from exploiting time gaps, a faster initial response is required from the time of collecting new logs to analyzing them.

第二にデータのつながり――複数のシステムからログを収集し、データの相関分析によってつながりを可視化する必要があります。

The second relates to data connections.
Logs need to be collected from multiple systems, and data correlation analysis is required to visualize the connections.

第三に予測と精度――兆候を疑い、攻撃の確証に近づくための分析は、人手中心の分析となり精度に限界があったため、分析ロジックの構築により更なる攻撃検知の強化が必要になっています。
The third relates to prediction and accuracy.
Analyses to identify suspicious signs and confirm attacks rely heavily on manual effort, limiting precision. Building analytical logic is essential to further strengthen attack detection.

これらの課題を解決するために、私たちはセキュリティ監視基盤を刷新しました。
To address these issues, we have overhauled our security monitoring infrastructure.

まず、国内最大級の顧客基盤と多様なサービスを前提に、ログの収集から分析までを再設計。 ログ収集・加工・蓄積のパイプライン作成の大部分を自動化し、新規ログ収集にかかる時間を大幅に短縮。
First, we redesigned the entire process from log collection to analysis, based on our massive customer database and diverse services. We automated the creation of most of the pipelines for log collection, processing, and storage, thereby significantly reducing the time required for new log collection.

さらに、AI による高度な不正検知ロジックを独自に導入。 社内の複数のシステムから収集した多種のログを用いて、これまで点で捉えていたデータを、攻撃者の行動シナリオとして線で見えるようにデータのつながりを可視化。 また、未知・亜種の振る舞いにも敏感に反応し、兆候を早期に捉える予測と、過検知を抑える精度の向上を両立させています。
Furthermore, we introduced proprietary AI-based logic for threat detection.
Using diverse logs collected from multiple internal systems, we visualized data connections, transforming previously isolated data points into the behavioral scenarios of visible attackers.
This approach enables the predictive detection of early signs by rapidly responding to unknown and variant behaviors, and accuracy is improved, thereby suppressing false positives.

私たちサービス＆ネットワークセキュリティ対策室では、新たな脅威への対策立案から開発、監視運用までを一括して対応。

Our Service and Network Security Office handles all aspects of cyber security, from planning countermeasures against new threats to development and monitoring operations.

SOC（Security Operation Center）による 24 時間 365 日の監視で、インシデント把握、影響調査、攻撃分析、要因の特定・対処をワンストップで迅速に実施しています。
Through 24/7 year-round monitoring by our Security Operations Center (SOC), we rapidly execute incident identification, impact assessment, attack analysis, root cause determination, and remediation in a single streamlined process.

監視の改革により、AI が兆候を拾い、分析の見取り図を提示。SOC アナリストはその見取り図をもとに仮説を立て、分析し意思決定します。 アナリストと AI の役割分担によって、対応のスピードと質を同時に高めることができるようになりました。
Through monitoring reform, the AI detects signs and presents an analytical overview. SOC analysts then formulate hypotheses according to the overview, analyze the data, and make decisions. By the division of roles between analysts and AI, we can improve both response speed and quality simultaneously.

ログ収集から分析までの時間を従来比で最大 80%短縮したことで、初動対応の迅速化を実現
By reducing the hours from log collection to analysis by up to 80%, we have achieved faster initial response times.

また、AI の活用により、膨大なログの中から不正を見抜く検知率も約 2 倍に向上。
Furthermore, AI utilization has doubled the rate for detecting and identifying anomalies within vast log volumes.

一連の作業時間を圧縮できたことで、生まれたリソースをより高度な脅威分析や対策の検討へとシフトし、セキュリティ運用の質を高めることが可能になりました。
By compressing the hours required for these tasks, freed-up resources can be shifted toward more advanced threat analysis and countermeasure planning, thereby enhancing the quality of security operations.

このセキュリティ監視の仕組みは”as a Service”として、社内へ展開中です。
This security monitoring framework is currently being deployed “as a Service” within the company.

高速に多様なログを検索できる仕組み、可視化された分析結果、AI による分析の知見は、全社的なセキュリティ監視力をさらに高める基盤として育てています。
The abilities to rapidly search diverse logs, visualize analytical results, and acquire AI-driven analytical insights are being cultivated as a foundation for further enhancing company-wide security monitoring capabilities.

脅威は日々姿を変え、連鎖し、広がります。私たちの改革は、技術的なアップデートだけではありません。
Threats constantly evolve, chain together, and spread. Our reform goes beyond technical updates.

ステークホルダーと密に連携して脅威情報を共有し、予防的な措置を『先回りして』講じます。
お客様からの信頼、そして事業への影響から社会インフラを守り抜くために、私たち自身が強く連携すること――それがあんしん安全で持続可能な社会を支える鍵だと考えています。
We collaborate closely with stakeholders to share threat intelligence and proactively implement preventive measures. To safeguard the trust of our customers and protect critical business infrastructures from disruptions, we ourselves must collaborate strongly—this is the key to supporting a safe, secure, and sustainable society.