サイバーセキュリティ報告書

2026年度版

目次

トレンドマイクロの使命

トレンドマイクロ株式会社（以下、当社）は、持続可能な社会にむけて、より安全な情報社会とお客さまの未来を創造する、サイバーセキュリティのグローバルリーダー企業です。当社は、「デジタルインフォメーションを安全に交換できる世界の実現」をコーポレートビジョンに掲げ、設立以来30年以上に渡り、一貫してサイバーセキュリティ分野に従事してまいりました。常に進化するデジタル技術や市場にいち早く対応したソリューションを継続して提供しお客さまの安全を守ると同時に、ビジョンを自己実現する取り組みを続けています。

企業のデジタルトランスフォーメーションが加速する中、リスクに備えながらいかに企業を持続的に成長させていくかを考えるうえでサイバーセキュリティはあらゆる企業にとっての経営課題になっています。

特に昨今の高度化したサイバー犯罪脅威の観点では、外部のリスクの大きさは常にダイナミックに変化しており、こうした外部のリスクの変化を的確に捉え都度的確に対応するために、通常のPDCAサイクルに加えてOODAのサイクルを定着させてリスクに備える体制が必須です。

当社の活動や保有する技術を「お客さまを守る、社会を守る」ことに活かしていくことが私たちの使命と考えています。例えば、当社のZero Day Initiativeでは、ソフトウェアなどの脆弱性をいち早く発見し、ソフトウェア／ハードウェアベンダーへ責任ある開示を行うことで、サイバー犯罪者の攻撃に備える取り組みを積極的に支援する活動を行っています。また、国内外の組織や警察機関とパートナーシップを締結し、世界各国で絶えず発生し続けるサイバー犯罪から社会を守る取り組みを行っています。

当社は、グローバル組織体制のもと、CIOがグローバルCISOを任命しガバナンス体制を構築しています。加えて、サイバーセキュリティは「リスクマネジメント」であるとの認識のもと、2012年に統合型リスクマネジメントチームを立ち上げ、国内ガイドラインへの対応を始め、国内特有のセキュリティ課題に対応できる体制も整えています。

当社では、BCMやBCPなど災害への対応、サプライチェーン・リスクマネジメント、インシデント対応、そしてSWATといわれるクライシスマネジメント体制など包括的にリスクを可視化し、定期的に経営層でレビューし適切な対応が迅速に取れる体制を構築しています。

当社は、これからもサイバーセキュリティ分野でお客さま、そして社会のデジタルライフサイクルを守っていくために、以下のように取り組んでまいります。

- 世界的に高まるセキュリティ・ファーストの要求に応え、お客さまおよび社会のセキュリティ・イノベーションの支援を通じて当社の企業ビジョンである「デジタルインフォメーションを安全に交換できる世界の実現」を目指す
- 重要な業界認証やコンプライアンス要件を確実に満たす当社の製品・ソリューション提供を通じ、お客さまおよび社会全体のセキュリティ向上に寄与
- 各地域の特性・地政学的特徴を踏まえたセキュリティ人財の育成、およびベストプラクティスの共有を実施

セキュリティ戦略および実践

当社は日本に拠点を置き日本の多くのお客さまにセキュリティ・ソリューションをご利用頂いている企業です。当社はそうした信頼にお応えするため、安心・安全に当社ソリューションをご利用頂くために当社自身のサイバーセキュリティ戦略を以下のように定義し、セキュアな企業活動を継続的に行えるように努力を続けています。

当社のビジネス戦略

当社は「デジタルインフォメーションを安全に交換できる世界の実現」という変わらぬ企業ビジョンの下で成長を続けています。このビジョンは、当社の製品やサービスの開発を推進するだけでなく、私たちのセキュリティおよびリスク管理のアプローチにも大きな影響を与えています。当社の製品やサービスは、企業、政府機関、重要インフラ企業、個人ユーザなど多様なグローバル顧客基盤によって利用されており、私たちのサイバーセキュリティ能力に対する絶対的な信頼が求められます。そのため、当社は内部および外部のコミュニケーションチャネルを通じて、戦略とリスク管理の実践を明確かつ効果的に伝え続けています。さらに、製品開発においては、クラウドベースおよびオンプレミスの提供能力のバランスを取り、お客様の多様で変化するニーズ、特にコンプライアンス要件に対応しています。このアプローチは、グローバルCISOの指導の下、「セキュリティ・バイ・デザイン」をデフォルトの開発プロセスとして取り入れ、全体的な企業リスク管理フレームワークと整合させています。これにより、最新のセキュリティ対策が開発、運用の各フェーズで適用され、お客様の信頼を高め、業界内での信頼性を向上させています。

サイバーセキュリティを支える３つの柱

当社は、世界中の脅威から顧客を保護する高度なプラットフォームを持つグローバルなサイバーセキュリティソリューションプロバイダーです。当社のセキュリティおよびリスク管理戦略は、企業ビジョンと完全に一致し、「人」、「プロセス」、「技術（セキュリティ施策）」という3つの基本的な柱に基づいて構築されています。

人

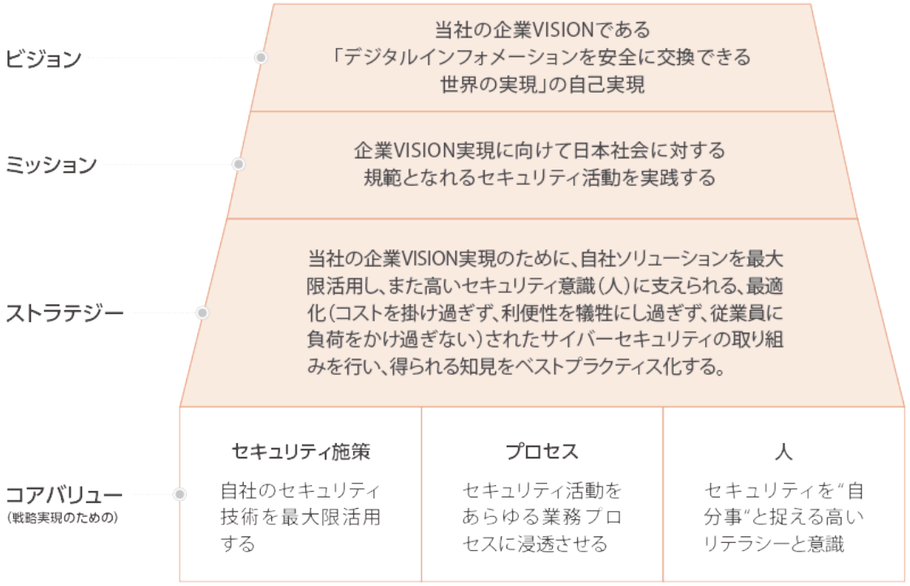
当社は30年以上前に「脅威防御の専門家」としてのコミットメントを宣言しました。この長年のコミットメントは企業ビジョンを支え、従業員の高いセキュリティリテラシーを生み出し、全体的なセキュリティ姿勢を自然に向上させ、全従業員向けの強力な教育プログラムによって強化されています。

プロセス

進化するサイバー脅威の状況やビジネス環境に対応するため、当社は従来の機能ベースの組織階層モデルから「目的ベースの非階層モデル」として社内で知られる「ラジアルウェブ」に変革しました。このモデルはトップダウンの意思決定構造を排し、部門を超えた従業員が積極的に協力し、必要な行動を迅速に実施できるようにします。この組織構造の変革により、当社は変化に迅速に適応し、持続可能な成長を達成し、お客様のニーズに長期的に対応できるようになります。

技術

当社は、従来の効果的なセキュリティ能力に加え、最近の生成AIブームの前からAIの力を活用しています。AI for SecurityおよびSecurity for AIを提供するプラットフォームを持ち、この技術は顧客の脅威検出および対応能力を向上させます。この技術の根幹には、バックエンドのセキュリティプロセスや世界中に広がる数百万のセンサーからのビッグデータ分析が含まれます。これにより、当社のプラットフォームとサービス提供の精度と運用の卓越性が向上し、潜在的なリスクやサイバー攻撃からの脅威を特定するのに役立ちます。
当社は、AI技術を開発および展開する企業として、これらの技術が倫理的で透明性があり、責任を持って使用されることを確保する責任を認識しています。



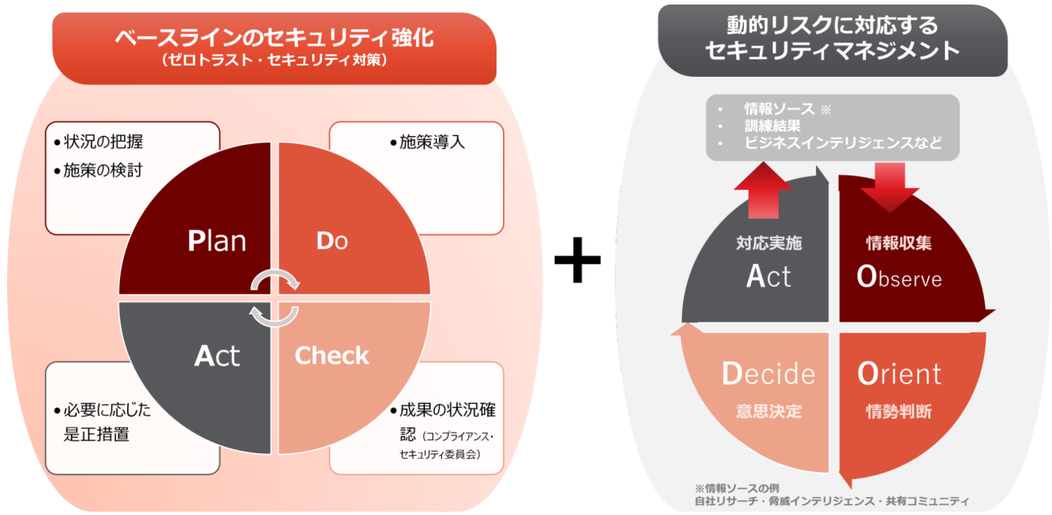
PDCAサイクル＋OODAループによる継続的なセキュリティ強化

当社は継続的なセキュリティ強化を目指したマネジメントサイクルに取り組んでいます。

当社では、計画→実施→効果測定→是正のPDCAサイクルを通してベースラインのセキュリティ強化を行い、コンプライアンス・セキュリティ委員会における経営層への報告と意思決定の場において定期的に確認しながら継続的な強化を続けており、働き方が多様化する中でリスクが大きくならないような対応を行っています。

また、サイバーセキュリティリスクは常に動的に変化していることをふまえて、上記PDCAサイクルに加えてOODAループを運用、自社リサーチや外部からの情報、ソフトウェアの脆弱性情報、訓練（レッドチームなど）結果を踏まえて必要に応じてリスクに対する素早い意思決定と対応の実施を行っています。

脅威インテリジェンスの社内活用の具体的な例として、当社業務に直接影響を及ぼす脅威情報の関係部署への連携が挙げられます。2024年末以降に国内の法人インターネットバンキング顧客を狙ったVishing（Voice Phishing）の増加が確認された事案では、当社においても影響が発生しうる脅威と判断し、当社スレットリサーチャーによりまとめられたVishing手口詳細を関係部門に展開し注意喚起を図りました。



セキュリティガバナンス体制

当社は、その企業構造（地域に根差すビジネスユニットと、全世界を支えるグローバルファンクションの組み合わせ）にベストフィットするセキュリティガバナンス体制を構築しています。

リスクマネジメント戦略

リスク管理の目的は、システム、データ、または運用に害を及ぼす前に、潜在的なセキュリティ脅威や脆弱性を特定、評価、および対処することです。リスクを体系的に評価し、適切なコントロールを実施することで、コンプライアンスを維持し、非公開情報および情報システムを保護します。

当社は、FedRAMP、PCI DSS、ISO 27001、ISO 27034-1、ISO 27014、ISO 27017などの国際的なサイバーセキュリティ標準に準拠した包括的なリスク管理プログラムを維持しています。コンプライアンスプログラムの完全なリストは、当社のトランスペアレンシーセンターでご覧いただけます。定期的なリスク評価を実施し、情報システム、非公開情報、またはビジネス運用の変更に応じて必要に応じて対応する認証フレームワークのリストを更新します。これらの評価は、資産および運用環境を徹底的に評価し、新たな脅威や進化する技術に対応するためにコントロールを適応させることを可能にします。

当社は、顧客からのセキュリティ脅威に関連する機密情報を「機密」として特定し、データの機密性および顧客のプライバシーを維持するための高度なセキュリティ対策で保護しています。さらに、顧客を保護するサービスインフラストラクチャの整合性および可用性を損なわないよう、包括的な復旧対策（事業継続管理）を実施および運用しています。 また、製品のソースコード、脅威に関連する研究開発、企業戦略情報などの情報は「管理対象非機密情報（CUI）」として特定され、適切に保護され、情報漏洩を防ぐためにアクセスが管理されています。

当社は、各サービスに関する重要な情報をビジネス影響分析（BIA）レポートに記録し、サービスの重要性に応じて最大許容中断期間（MTPD）、復旧時間目標（RTO）、および復旧ポイント目標（RPO）レベルを決定します。 事業継続計画（BCP）は、毎年または重大な変更が発生した場合に見直しおよび更新されます。

情報セキュリティポリシー

当社の情報セキュリティポリシーは、情報セキュリティ管理システム（ISMS）フレームワークに基づいて慎重に開発されています。これらのポリシーは各部門によって実施され、すべてのステークホルダーに明確に伝えられます。 継続的な改善を確保し、組織の有効性を高めるために、当社は定期的な管理レビューを実施しています。これらのレビューは、改善の領域を特定し、セキュリティ対策が堅牢で最新の状態を維持するのに役立ちます。これらのポリシーを遵守することで、機密情報を保護するだけでなく、組織全体にセキュリティ意識の文化を促進します。

役割、責任及び権限

サイバーセキュリティリスク管理は、社内のセキュリティチームの下で実施され、各関連部門が実行を担当します。

当社では、グローバルセキュリティガバナンスが2つの部門に分かれています。開発した製品およびサービスのセキュリティを監督するRDSecチームと、情報資産およびシステムのセキュリティを監督するInfoSecチームです。

新入社員は、採用された地域・国の法律または規制に従ってバックグラウンドチェックを受ける必要があります。役割やレベルに応じて、犯罪歴・教育・雇用の確認が行われることがあります。

全社員は、初期の雇用条件の一部として、機密保持／非開示および発明譲渡契約に署名する必要があります。さらに、採用時にセキュリティトレーニングを受け、毎年更新する必要があります。

監査

当社のFedRAMP、ISO 27001、ISO 27034-1、ISO 27014、およびISO 27017の証明書は、サイバーセキュリティリスク管理の複数の要素を含んでいます。監査レポートの分析結果をもとに、リスク管理戦略を洗練・改善・調整します。これにより、進化する脅威・ビジネス目標・および業界のベストプラクティスに対応しています。

当社は、財務、技術、人材などのリソースを効果的なサイバーセキュリティリスク管理のために戦略的に配分するために、これらのガイドラインに従っています。ビジネス目標に沿ってリスク管理を行うためのリソース配分を行うことで、当社の製品、サービス、および運用全体で堅牢なセキュリティ姿勢を維持しています。

サイバーセキュリティサプライチェーンリスクマネジメント

当社の情報セキュリティポリシーには、アウトソーシングポリシーおよびクラウドセキュリティポリシーが含まれています。これにより、他の組織によって処理される情報のセキュリティを維持するためのコントロールを実施し、サプライチェーンリスク管理に対応しています。

当社は、企業情報セキュリティポリシーの一部であるインシデント管理ポリシーを維持しています。当社のインシデント管理ポリシーは、インシデント監視および対応、セキュリティインシデントの報告、セキュリティ上の脆弱性の報告、ソフトウェアの不具合の報告、インシデントからの学びとして定義されています。インシデント管理手順におけるすべての関連当事者の責任と引き継ぎポイントには、サプライヤーも含まれます。

当社のセキュリティチームは、セキュリティレビューおよびリスク評価を通じて、サプライチェーンパートナーとの関係を維持するための審査プロセスを持っています。

サイバーセキュリティ施策

世界標準レベルのセキュリティ管理施策

当社のセキュリティ・ポリシーを、広く参照・推奨されている米国国立技術標準化研究所（NIST）が提唱するサイバーセキュリティ・フレームワーク（Cybersecurity Framework）を基に整理し、個々の管理施策に不足がないかを見直し、国際的にも高いレベルの標準に照らして十分なものを目指します。

危機管理体制

当社は2005年より、あらゆるリスクに対応するための危機管理スキームとして日本本社にSWATチームを発足しており、副社長２名を本部長としてクライシスマネジメント・プロセスを実践します。サイバーセキュリティリスクに関するリスクが顕在化した際にもこの危機管理体制に速やかに報告され、危機対応に対する意思決定を迅速かつ適切に行うために危機管理体制を発動します。

セキュリティ・インシデントについては当社のCSIRTであるTM-SIRTのスキームにより必要な外部コミュニケーションを速やかに実施する体制を敷いています。

また、リスクレベルが全世界に関わる事象においてはグローバルの危機管理体制と連携しながら全社を挙げて危機対応を行う体制を敷いています。

法令遵守

当社は、関連会社とともに、その核となる会社機能をさまざまな国々に分散し、国境を意識しない業務運営を行っています。そのため、法律や慣習は当社が事業を行う国ごとに異なっており、倫理規準もまたその事業環境により様々です。

当社は東京証券取引所（以下、「TSE」）に上場しており、日本において設立された会社として、日本の法律等はいうまでもなく、様々な法律、規則等の適用を受ける中で事業を行っています。日本におけるTSE規則、金融商品取引法および会社法に限らず、とりわけ利益相反の倫理的取扱い、十分かつ公平な開示および法令や、個人情報保護法、電気通信事業法に準ずる各種ルール等の遵守について広く義務を負っています。また、法人格を取得した国におけるその国の会社法の適用も受けています。

これを当社全体に周知徹底していくために、Code of Conduct（以下、「行動規範」）を定め、当社の業務行動規範の規準が当社およびその子会社（トレンドマイクログループ各社）のすべての取締役、役員および従業員の行動の根幹を成すルールとして浸透しています。

リスクの特定と対策

当社では、守るべき資産が侵害されてしまうリスクに関して、その発生要因（脅威源）別に定期的な見直しと可視化を行って、リスク対応が不十分な発生ルートのないように対策を都度強化しています。また、事案が発生してしまった場合の対応機能と危機管理体制を整備しており、事案によるお客さまへの影響を最小限にできるように体制を構築しています。

外部からの攻撃への対策

世界各国のセンサーから集められる脅威情報、連携外部団体などが提供する侵害兆候（IoC）などを最大活用し不正侵入行為に対する防御・検知を行います。

アカウント乗っ取りなどによる不正アクセスを防止するため多要素認証（MFA）などのセキュリティ施策の組み合わせによりリスクを低減します。不正アクセスを検知した場合は速やかにインシデント対応スキームが発動し、その影響に応じて適切に社内へのエスカレーションと危機下における対応方針の決定など重要な意思決定が行われます。重大な事案を認識した場合は速やかな法執行機関や外部関連機関との連携を行い正しく事件解決を目指します。

内部不正への対策

外部者による攻撃よりも防御が困難な内部者による情報の持ち出しに対する各種対策も実施しています。特に機械学習や深層学習を活用した「異常行動検知」や外部への情報持ち出しの導線をコントロールする施策、内部犯行が起こりにくい職場環境作りとその維持という３つの柱によって内部不正行為のリスクを低減します。

ミスなどによる意図せぬ事案への対策

後述する「安全なソフトウェア開発体制の構築」によってミスの起きにくいDevSecOps運用を目指す中でリスクの特定と対策を行っています。

製品セキュリティ

当社では、グローバルCISO配下の専門チームRD-Secを中心に安心して製品をお使い頂くための「セキュア・エンジニアリング」の実践と、作成されるソフトウェアの安全性を日本においても二重に確認して出荷するといった体制を構築し、安全性のさらなる強化のためにプロセス改善を続けています。

また当社が抱える脆弱性リサーチチームを中心とする脆弱性の早期発見と当社製品に脆弱性があった場合にPSIRTチームおよび、お客さま対応のエンジニアチームによる速やかで適切な対応ができるような体制を敷いています。

サプライチェーン・リスク対策

当社では、クラウド・AIサービスを含むサプライチェーン全体のリスク管理を重要な経営課題として位置づけています。情報セキュリティ審査プロセスの整備、サプライヤーへの倫理・サステナビリティ基準の要求、ソフトウェアサプライチェーンの安全性確保、そして生成AI利用に関する社内ガイドラインの策定を通じて、多層的なリスク対策を実施しています。

クラウドサービス・AIサービスの導入審査と分類管理

当社では、外部クラウドサービスやAIサービスの導入にあたり、情報セキュリティ部門（InfoSec）が主導する審査プロセスを設けています。導入サービスはリスクレベルに応じて分類され、特にAIサービスについては、ユースケースごとにAI特有のリスクを個別に評価・承認する仕組みとしています。審査にはCSA CAIQ（クラウドセキュリティアライアンスの評価アンケート）など、標準化されたセキュリティ・コンプライアンス評価に関する確認やセキュリティアーキテクチャレビューが含まれます。なお、AIツール・サービスについては、採用前に情報セキュリティおよびデータ取り扱いリスクを評価する審査・承認プロセスを経ることが全社共通で義務付けられており、機密情報の適切な保護を確認したうえで導入を進めています。

サプライヤーへの倫理・サステナビリティ基準の適用

当社はサプライヤー・ビジネスパートナーに情報セキュリティ要件、データプライバシー法令、現代奴隷制へのゼロ・トレランス方針の遵守を求めています。調達元には地理的リスクやセクター特性を考慮したリスク評価を定期的に実施し、ハードウェア製品のサプライヤー選定ではサステナビリティ基準を重視します。資産の識別・管理プロセスを整備し、アクセス権の失効処理、返却、顧客情報の安全な消去を確保しています。

生成AIサービスの安全利用に関するガイドラインの整備

生成AIの普及に伴い、当社ではサプライチェーンリスクの観点から社内での生成AI利用に関する明確なガイドラインを策定・運用しています。承認済みAIサービスのみを業務利用とし、業務外利用の禁止、データの匿名化、機密情報の管理徹底を義務付けています。さらに、全社員を対象として、責任あるAI利用・セキュリティ・プライバシーリスクに関する年次意識向上トレーニングを定期的に実施しています。

ソフトウェアサプライチェーンの安全性確保

製品・サービスを構成するサードパーティ製コンポーネントは、サプライチェーンリスクの重要な要素の一つです。当社では、製品・サービスに含まれるすべての第三者製コンポーネントを継続的にインベントリ管理し、NVD（米国国家脆弱性データベース）をはじめとする複数の脆弱性フィードと照合することで、脆弱性（CVE）をリアルタイムで検知する仕組みを運用しています（Software Composition Analysis）。検出された脆弱性はCVSSスコアに基づいて優先順位付けされ、重大度に応じたタイムラインで対処が義務付けられています。また、本番環境向けに構築されたすべてのコンテナイメージは、デジタル署名による検証を必須とするとともに、継続的な脆弱性スキャンの対象とされており、SLO（サービスレベル目標）内での対処が求められています。これらの取り組みを通じて、ソフトウェアのサプライチェーン全体にわたる安全性を確保しています。

インシデント対応

当社はセキュリティを専業としているため、セキュリティ・インシデントが発生した際に必要となる各種組織的機能・役割を全て自社に有しています。
また、お客さまおよび自社への影響の大きな事態に際してはセキュリティ事案か否かに関わらず、グローバル及び日本本社において危機管理体制を有しています。日本本社においてはSWAT（スワット）チームという呼称にて2005年よりあらゆる分類のリスクについて危機管理対応を行ってきています。

CSIRT

グローバルにおいては、TM-CSIRTという仮想型チームを構成してインシデントに関するPoC機能を持って活動しており、日本本社においては、TM-SIRTとして、一般社団法人日本シーサート協議会に加盟し各社CSIRTとの連携を含め必要な活動・対応を行っています。

また、リサーチャー、キュレーター、インベスティゲータといったCSIRTに求められる機能、組織的役割については当社のセキュリティ・サービスを提供する各部門が連携して担う役割をもって運用しております。

PSIRT

当社はソフトウェア製品の供給事業者であることから、自社製品に関する脆弱性の対応スキームを構築し製品をご利用頂いているお客さまへのリスクの最小化に努める活動を行っています。詳しくは後述の「安全なソフトウェア開発体制の構築」を参照ください。

事業継続マネジメント

当社はセキュリティ・プラットフォーマーとして世界中のお客さまに対してリアルタイムのセキュリティ・ソリューションを提供しているため、そうしたサービスが様々な原因（地政学リスク、災害リスク、サイバーリスク）により業務停止に陥ることのないように適切な事業継続マネジメントのもとで、継続性を維持するための仕組み、プロセスを導入し定期的な訓練を重ねています。

経営層への報告

コンプライアンス・セキュリティ・サステナビリティ委員会

日本本社においては半期ごとにセキュリティやサステナビリティを含むリスクについて可視化し現状と課題を明確にし、課題に対する適切な意思決定と改善アクションを行える体制を運用しております。また毎年２回、リスクレポートを作成し、各リスク領域の状況やその低減に関する取り組み内容などの詳細報告を経営層に対して行っております。

人材育成・トレーニング・訓練

人材育成

当社のセキュリティ戦略を支える柱の一つが高いセキュリティリテラシー、高いセキュリティ意識を持つ「人財」です。採用、導入教育、フォローアップ教育、定期的な教育を業務内容に関わらず実施し、戦略を支えるための大切な人財を維持していきます。また、新たな注目分野であるAIの活用にも力を入れており業務に応じた育成を行っています。

トレーニング・訓練

当社においても、新たな領域であるAIの活用が急務と考えています。当社では、業務改善および当社製品を利用したAIを守るためのセキュリティ（Security for AI）、そしてAIを利用したセキュリティの向上（AI for Security）双方の観点からトレーニングを提供し社員全体のAI利活用を支援しています。

また、サービス継続性の観点においては、重要なサービスプラットフォームに関してはサイバー攻撃以外の事態を想定した定期的な訓練を実施し緊急時に適切に事業継続が可能になるように努めています。

高度な人材育成

下記のような、論文発表・共同研究、国際イベント・カンファレンスでの発表など、社外に向けた活動を通じて社会全体に真に必要とされる高度な人材育成にも取り組んでいます。その活動の一部を以下に掲載いたします。

「EU Digital regulation and Cybersecurity」登壇

- 2025年6月18日オランダ経済省（NFIA）（および蘭日貿易連盟（DUJAT）主催のラウンドテーブル「EU Digital regulation and Cybersecurity」に登壇
- 最新の脅威動向を共有し、参加者（オランダに進出している、日本の金融機関、商社等）との意見交換が行われた

詐欺対策カンファレンスJapan2025（Anti-Scam-Conference-japan-2025）

- 国内詐欺動向解説カンファレンスの開催に協力
- 「日本における詐欺の現状 State of Scams in Japan」を講演

コンピュータセキュリティシンポジウム2025 (CSS2025) 講演

- CSS2025にて、香川大学・JC3・神奈川県警・千葉県警・トレンドマイクロ共同で「JC3の産学官連携推進に向けて」としてセッションを開催

https://www.iwsec.org/css/2025/program.html#4I3

香川大学 セキュリティ・キャンプ2025ミニ 講演

香川大学のセキュリティ･キャンプ2025ミニにて、フィッシング対策について以下2つの講演を担当

- 講演：フィッシング対策に係る産学官の共同研究について
- 講演：フィッシング詐欺の最前線と対策～JC3の取り組みと学生参加

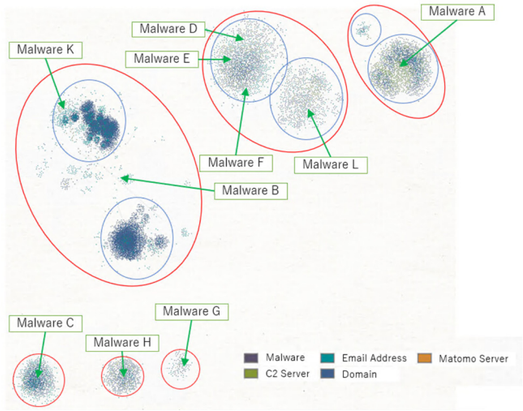
サイバーセキュリティ産学連携推進協議会（IAC3）JNSA-IAC3 第2回サイバーセキュリティセミナー 登壇

「民間企業の視点から見た産学官連携研究の価値」として以下内容について講演

- 企業が保有する脅威情報と研究への活用について
- IEEE DSC 2024 Best Paper Award受賞研究の紹介
- ビジネスへの還元と社会貢献について

「ACM DIGITAL THREATS: Research and Practive」に論文採択

- ACM (Association for Computing Machinery, 国際計算機学会) はコンピュータ分野で世界的に権威のある学会
- 偽ショッピングサイトへの転送を行うマルウェア間の関係性を分析
- 香川大学、神奈川県警、千葉県警での共同研究による成果



経済安全保障に関する対応

日本に本社を置く日本企業として日本政府の進める経済安全保障を念頭に対応体制の整備を進めています。

経済安全保障推進法に基づく基幹インフラ安定提供制度への対応体制整備

基幹インフラ事業者の皆様が当社製品を特定重要設備のセキュリティ確保のためにご利用の際に、構成設備の供給者に対して監督官庁から求められる、役員構成、株主構成、特定の外国政府との取引状況、及びリスク管理措置の情報の提供を行っております。また、「我が国の外部から特定社会基盤役務の安定的な提供を妨害しようとする主体」の攻撃から、安心して当社のクラウドサービス基盤を利用いただくために日本政府が推進しているISMAPの認証を取得し更新を継続しております。

政府公共機関･インフラ支援企業として自社の経済安全保障課題への対応

経済安全保障に関わるリスクを取り扱うための専門チームを中心に部門横断で新たに発生するリスクや規制に対し、迅速かつ適切に対応するためにサプライチェーンの対応チーム及びビジネス・セキュリティ・カウンシルの体制を整備しています。さらに、セキュリティ・バイ・デザインの思想に基づき、地政学リスクを考慮した製品・サービスの設計や当社製品の安全性・信頼性・透明性の確保を目的としたトランスペアレンシー・センターの活動を通して推進しております。

サイバーセキュリティ教育・文化形成の推進

経済安全保障の担い手である基幹インフラ事業者等を中心に自組織のデータおよびシステムを守る観点から事業自体を守ることで、国民および日本社会の営みを守る観点へ昇華させるリスクマネジメントとしてのサイバーセキュリティ教育および文化形成の推進をセキュリティ・ナレッジ&エデュケーションセンターの活動として行っております。

能動的サイバー防御法案を通じた政府・重要社会インフラ事業者への支援

- 経済安全保障推進法同様、重要電子計算機の供給者の届け出協力依頼への対応体制整備
- サイバーインフラ事業者としての脆弱性対応支援とSBOMを含むセキュリティ・バイ・デザインの推進
- 当社製品・サービスの利活用を通じたスレットハンティングおよびインシデント報告の実践支援
- サイバーセキュリティ協議会において、第一類構成員タスクフォースメンバーとして脅威情報の提供を通じて官民連携を継続支援

国産セキュリティ技術の振興活動を通じた経済安全保障の確保への貢献

- 日本サイバーセキュリティ産業振興コミュニティ（NCPC）への参画を通じて、日本で活躍するセキュリティ産業を強化・育成するための新たな枠組みを支援
- 一般社団法人サイバーリサーチコンソーシアム（CRC）への参画を通じて、国内民間サイバーセキュリティ企業の英知を結集し、個社ごとの取り組みも含め、解決困難な技術課題を会員の連携により解決し、我が国における安全保障の確保に寄与する先端的な重要技術の開発支援の取り組みを技術面から支援
- 特定非営利活動法人日本ネットワークセキュリティ協会の国産セキュリティ産業振興WGへの参画を通じて、経済産業省が2025年3月に公表した「サイバーセキュリティ産業振興戦略」を推進する為のイベント「国産セキュリティ推進フォーラム」への協力

サイバーセキュリティ啓発及び情報共有活動への貢献

「デジタルインフォメーションを安全に交換できる世界の実現」というコーポレートビジョンの元に、当社の活動や保有する技術を「お客さまを守る、社会を守る」ことに活かしていく為には、当社内だけの活動に閉じる事無く、社会全体のサイバーセキュリティ向上の取り組みに貢献していく事が必要です。
当社では各種団体活動を通して、ISAC（Information Sharing and Analysis Center）等の情報共有活動やサイバーセキュリティ啓発の為の活動に積極的に参加をしています。

	団体・組織名	主な取り組み
1	**特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）**	• 理事・幹事として運営に参画 • 社会活動部会 • 会員交流部会　国産セキュリティ産業振興ワーキンググループ • 教育部会　ゲーム教育WG／情報セキュリティ教育実証WG／教育部会産学連携プロジェクトメンバー
2	**一般財団法人日本サイバー犯罪対策センター（JC3）**	• 理事・幹事として運営に参画 • 事務局員（常駐）として各都道府県警からの研修生の受け入れ、研究テーマ設定指導、支援を担当 • 産官学連携による詐欺手口の分析や対策の研究 • 金融犯罪対策グループ副主査、各グループ配下におけるプロジェクト主査ならびに勉強会主査
3	**一般社団法人日本シーサート協議会**	• TM-SIRTとして参画
4	**一般社団法人日本IT団体連盟**	• サイバーセキュリティ委員会 ▪ DX with Cybersecurity分科会主査 ▪ 経済安全保障分科会 • 政策委員会委員
5	**フィッシング対策協議会**	• 運営委員として参画 • STC（STOP. THINK. CONNECT.）普及啓発WG／被害状況共有WG／詐欺サイト対処机上演習タスクフォースにおいて主査として活動
6	**サイバーセキュリティ協議会**	• 第一類、タスクフォース会合メンバーとして参加
7	**国家サイバー統括室**	• JISPの運営支援 • 大阪・関西万博の開催に向けてサイバーセキュリティに関する脅威情報の提供、講演を実施
8	**独立行政法人 情報処理推進機構（IPA）**	• 「情報セキュリティ10大脅威」選考委員
9	**一般社団法人ICT-ISAC**	• 国内外ISAC連携WGに参画
10	**一般社団法人ソフトウェア協会**	• 理事 • 政策・法務知財委員会委員 • Software ISAC • サイバーセキュリティ委員会

11	**一般社団法人オープンガバメント・コンソーシアム**	• WG1/2：「国・地方のネットワークの将来像」に係るWG • WG3：経済安全保障にそれぞれ主査として参画
12	**一般社団法人交通ISAC**	• 賛助会員として参画 • セキュリティマネジメント共有WG／IT-OT連携WG／脅威情報分析WG／事例共有WG／海事分野WG
13	**電力ISAC**	• テクニカル会員としてISACワークショップの企画実施
14	**一般社団法人日本コンピュータシステム販売店協会**	• 理事、コミュニティ委員会委員長、セミナー委員 • セキュリティ委員会、技術委員会、コミュニティ委員会
15	**一般社団法人 Generative AI Japan**	• 理事 • セキュリティ・ガバナンス研究会座長
16	**日本サイバーセキュリティ産業振興コミュニティ(NCPC)**	• 初期参加メンバーとして登録、立ち上げに向けて議論に参画
17	**一般社団法人サイバーリサーチコンソーシアム(CRC)**	• 賛助会員として加盟
18	**一般社団法人日本サイバーセキュリティ・イノベーション委員会(JCIC)**	• 理事兼研究員

具体的なサイバーセキュリティ施策

以下は、米国国立技術標準化研究所（NIST）が定めるガイドラインNIST SP 800-171［連邦政府外のシステムと組織における管理された非格付け情報の保護］に定められたセキュリティ管理施策ファミリーに沿った当社の管理施策実施状況についての説明となります。昨年度と同様にGlobal InfoSec主導によるゼロトラスト・セキュリティを基本施策とした、様々なセキュリティ強化の取り組みを実施しております。

今年度の新たな取り組みについては、表中で下線で表記しています。

意識向上と訓練	• Global-CISOがポリシー遵守の責任者で各組織・地域と連携して周知徹底を実施し、従業員への定期的な啓発・訓練を実施しています • セキュリティ及びコンプライアンスに関する全社オンライン研修や、模擬フィッシングメールによるセキュリティ演習を実施しています • メール誤送信防止のため、送信時の宛先や添付ファイルの確認を必須とする仕組みを設けており、新たにAIによる宛先と宛名のミスマッチを検知する仕組みを導入しました • 中途入社・新入社員向けの入社時トレーニングに、生成AI利用に伴う情報セキュリティリスクに関するコンテンツを含めました
監査と責任追跡性	• Global-CISO配下のInfoSec部隊がセキュリティ・モニタリングを「24時間×7日」で実施し、重要資産に関する管理監督責任者を設置し、追跡可能な措置を講じています • 製品開発部門管理の開発及び検証環境に対してGlobal InfoSecによる社内監査を実施しています • 社外向けWEBサイトの脆弱性診断について、実施結果の確認を社内監査の対象項目へ含め、実施状況の確認プロセスを厳格化しています
アクセス制御	• 重要資産のアクセスは役割に応じたアクセス制御方式（RBAC）および、多要素認証（MFA）を導入し不正アクセスを予防し、かつペネトレーションテストの結果などを踏まえて順次強化策を導入しています • 機械学習・深層学習を用いた不正アクセスの検知メカニズムを実装しています • サーバ及びネットワーク環境に対してより強固なアクセスコントロールを行うため、社内ITサービス運用や製品検証に伴う特定管理用プロトコル専用のゲートウェイサーバを導入しています • 検体解析及び一部の顧客サポート業務において、アクセス先を厳格に制限した専用VDIを導入しています • 業務用スマートフォン向けMDMの入替えを実施し、アプリケーションの利用や社内データの送受信へ厳格な制限を設けました • 国を跨ぐ社内業務用端末間の通信に制限を設けました • 社内ネットワークから生成AIサービスへのアクセスを監視し、一部の地政学的リスクが高いサービスへ制限を設けました • 各リージョン毎に固有のVisionOneテナントで行っていた運用をGlobal全体で一つのテナントへ集約し、アカウント管理や設定管理等を集約しました
構成管理	• 社内システムのソフトウェア開発ライフサイクル（SDLC）にセキュリティ観点を組み込んで運用しています（DevSecOps） • 各システムを保護するためのセキュリティ管理施策を自社製品・他社製品により導入し運用管理を行っています
識別と認証	• 各従業員の使用デバイス、アクセス可能なシステム、フォルダーを特定して管理しているアクセス権、デバイス、システム利用権限などを定期的および必要時に見直しています • 従来より強固な認証方式を利用可能な多要素認証サービスを再検討・導入しました • パートナー企業内当社向け業務委託環境において、ハードウェアトークンを使用した多要素認証を導入しています • パスキー認証を導入しました
インシデント対応	• GlobalおよびRegionにCSIRT組織を構築・運用しており、Global CSIRTはFIRSTに、日本のCSIRTは一般社団法人日本シーサート協議会（NCA）に加盟し外部連携を図っています • 社内業務環境における実践的なレッド・ブルーチーム演習を開催し、セキュリティ課題の洗い出しや対応フローの再確認、演習に関わるエンジニアの育成等を実施しています • Globalレッドチームにより全リージョンのオフィス、データセンター、クラウド環境を対象に、事前通告を行わないペネトレーションテストを実施しています
メンテナンス	• 業務システム、外部サービス向けシステムは脆弱性への対応を含めたメンテナンスを適時行っており、メンテナンス実施時には明確な手順に沿って実施しています
記録媒体保護	• 守るべき資産を記録した電子メディアと記録媒体および紙媒体についてはセキュリティ担保施策配下で管理しています。また、すべての記憶媒体を含むデバイス廃棄は廃棄後の復元ができないように破壊してから廃棄を行っています

人的セキュリティ	• 機密情報へのアクセス権限を新たに付与する際には情報管理責任者の責任において的確であるか判断を行っており、不要となったアクセス権等（退職、配置転換などによる）は速やかに抹消措置をとっています
物理的保護	• 一部の機密を扱う物理的領域への立ち入り権限は全従業員に与えず役割に応じて必要最低限の従業員にのみ付与しており、機密を扱う物理的領域は入退室ログ、監視カメラなどによって保護・管理しています • 日本本社移転に伴いオフィスビルゲート、オフィステナントエリア、オフィス内機密情報保管エリアの入退室の制御及び記録を開始し、社内情報システム部門管理のサーバ・ネットワークルーム、製品開発部門管理の開発及び検証環境等の機密情報保管エリアは完全分離の上監視カメラを設置しています
リスクアセスメント	• 重要資産を特定し、資産の負の影響度に応じたセキュリティ管理施策を実装し定期的に見直ししています • 社内外向けシステムの新規リリースに際し、Global InfoSecによるシステムアーキテクチャ及び運用プロセスのレビューを実施しています • クラウドサービス利用に際して、Global InfoSecによる事前レビューと承認を必須とするプロセスを導入しました • 社外へ公開しているウェブサイトに対して、サイトの変更時及び年に一度の脆弱性診断を実施しています
セキュリティアセスメント	• セキュリティ管理施策の有効性を定期的に見直しし、製品、サービス、社内業務システムについて早期の脆弱性発見、ハードニングなどに努めています。またセキュリティ管理施策の有効性についてのアセスメントと改善を実施しています • 社内セキュリティ演習及びレッドチームによるペネトレーションテストの実施結果に応じて、インシデント対応プロセスやセキュリティ施策の定期的な評価を実施しています • 情報セキュリティに関するリスクレポートを発行し、ベンチマークに基づく情報セキュリティリスクに対する評価値と近況について、半期毎にコンプライアンスセキュリティ委員会へ報告しています
システムと通信の保護	• 拠点間・テレワークを含め安全で暗号化された通信を実装し通信保護を徹底しています。またネットワーク構成はGlobal-CISOのガバナンス配下でセキュアな設計、構築、運用を実践しています • データセンターサーバラック内の電源をインテリジェントPDUへ移行し、これまでの機器単体の死活監視に加え各電源モジュール毎の電力使用状況の収集と死活監視を開始しています
システムと情報の完全性	• 顧客に対するサービスに関するシステムフローについては、常に最新状態を維持し、アタックサーフェスの見直しとリスクレベルの再査定等を実施しています • また組織内で自社開発のセキュリティ製品による必要なセキュリティ対策技術を実装しています • セキュリティソフトからの警告、およびネットワーク、アクセス監視による異常検知は24x7体制でGlobal-CISO配下のInfoSecチーム（SOC）で実施しておりアラートに対してリアルタイムでの対応を実施しています • 社内外システムに対して月次ならびに脆弱性のリスクレベルに応じた不定期のセキュリティパッチを適用しています • 当社が保有するGlobal IPアドレス帯に対し、社外より脆弱性並びにオープンポートの定期スキャンを実施しています

AIに対する取り組み

AI原則の採択

当社およびその関連会社は、AI技術を開発及び展開する企業としてのAIの責任ある使用のために、Bussiness Software Alliance および 米国国立技術標準化研究所（NIST）のガイダンスを踏まえ、Responsible Use of Artificial Intelligence (人工知能（AI）の責任ある使用)において、透明性の原則、公平性の原則、プライバシーの原則、説明責任の原則、安全性とセキュリティの原則、人間による管理の原則、社会的責任の原則、継続的改善の原則を当社およびその関連会社の取り組みの指針となるAI原則として採択し公開しています。

https://www.trendmicro.com/ja_jp/about/trust-center/privacy.html

AIガバナンスへの取り組み

AI Policyの制定

当社およびその関連会社は、AIの開発、導入、使用に関するすべての活動（以下、AIイニシアティブ）が、当社のコアバリューと一致するとともに、透明性を確保し、当社のステークホルダーの信頼を維持することを目的として、AI技術の開発、導入、使用にかかわる当社のすべての従業員、委託業者等に適用される Trend Micro - Artificial Intelligence (AI) Policy（以下、AIポリシー）を制定し関係者に周知しています。AIポリシーでは、AIの倫理的利用、プライバシーとセキュリティ、コンプライアンスおよび継続的な改善を確保するための指針等が示されるとともに、AI開発への総合的なアプローチを確保するための技術部門と非技術部門の協働や、ユーザ、顧客その他の利害関係者の意見を取り入れる有用性および必要性にも言及しています。また、研究開発向けのガイドラインおよび非研究開発向けのガイドラインを含んでいます。

AI Committeeの設置

当社は、AIイニシアティブを監督し、倫理コンプライアンスの観点からプロジェクトをレビューし、ガイダンスを提供するため、AI Committee（AI委員会）を設置しています。

プロジェクトをリードする者は、プロジェクトがAIポリシーに準拠していることを確認し、倫理上の懸念が生じた際にAI Committeeに報告する責任を負います。また、サードパーティのAIツールの利用に際しては、AI Committeeの審査を要し、従業員は承認されていないAIツールを使用することはできません。従業員は、AIシステムに関連する倫理的な懸念やインシデントをAI Committeeに報告しなければなりません。

「GENIAC-PRIZE」安全性領域 入賞

2025年度には、経済産業省と国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）が主催する、生成AI分野の研究開発・社会実装の促進を目指したNEDO懸賞金活用型プログラム「GENIAC-PRIZE」のテーマIII「安全性領域（生成AIの安全性確保に向けたリスク探索及びリスク低減技術の開発）」において3位に入賞いたしました。

※「AIエージェントにおける不正なツール実行リスクへの総合的な対策」の提案
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2026/pr-20260327-01.html

詐欺対策に関する取り組み

拡大する日本の詐欺被害

日本国内における詐欺被害は深刻さを増しています。警察庁の発表によると、令和7年の特殊詐欺の認知件数は27,832件、被害額は約1,423億円（前年比約98%増）に達し、過去最悪の水準となりました。特に警察官を装う「ニセ警察詐欺」の急増が被害拡大の主な要因となっています。また、SNS型投資・ロマンス詐欺の認知件数は15,168件、被害額は1,834億円（前年比約44.2%増）と引き続き深刻な状況が続いています。手口はますます巧妙化しており、20代・30代の若い世代への被害も急増しています。また、生成AIを悪用した新たな詐欺への懸念も一層高まっています。

政府は2024年6月に「国民を詐欺から守るための総合対策」を策定し、さらに2025年には「総合対策2.0」を策定して官民連携による詐欺対策を強化しています。

※出典：警察庁 令和7年における特殊詐欺及びSNS型投資・ロマンス詐欺の認知・検挙状況等について（確定値）

https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2025.pdf

当社の詐欺対策

当社では「AI技術の活用」「啓発活動」「詐欺対策のエコシステム構築」の3つの柱で社会問題である詐欺への対策を強化しています。

①AI技術の活用

2024年10月に個人向けの詐欺対策アプリ「トレンドマイクロ詐欺バスター」をリリースしました。このアプリでは以下のような最新技術を活用し、巧妙化する詐欺からユーザを保護します。

- 特殊詐欺やフィッシング詐欺の検出・対策
- ディープフェイクによるなりすましの防止
- SNSや広告の詐欺リスクをAIで検出

独自に開発したAI技術を活用し、テキスト・画像・動画を分析して詐欺の可能性を評価。ユーザへ適切なアドバイスを提供し、より安全な環境をサポートします。詐欺の手口や被害情報を体系的に整理し、AIが詐欺の意図を予測することで事前にリスクを回避できるよう設計されています。また、詐欺対策の専門チームが最新の脅威を継続的にリサーチし、より強力な対策を実現。「ウイルスバスターシリーズ」のフィードバックデータを活用し、独自の脅威インテリジェンスを強化。さらに、警察や金融機関と協力し、詐欺関連の情報を迅速に収集しています。これらの技術と情報を組み合わせ、詐欺検出技術をさらに進化させていきます。

②啓発活動の推進（警察・自治体との官民連携）

トレンドマイクロは特殊詐欺の入り口となる電話の対策機能を無償化し、全国の警察組織や地域の自治体と連携し、特殊詐欺対策アプリの普及と詐欺被害防止のための啓発活動に取り組んでいます。

- 特殊詐欺の入り口となる電話対策の普及に向け、2025年10月より「詐欺バスター」の詐欺・迷惑電話ブロック機能およびAndroid向け国際電話ブロック機能を無償化
- 2026年3月、詐欺電話・国際電話対策に特化した無償アプリ「詐欺バスター Lite」を「特殊詐欺対策アプリに係る警察庁推奨制度」において警察庁推奨アプリとしてリリース
- 警視庁より「特殊詐欺被害防止アドバイザー」を受嘱、700名のトレンドマイクロ社員及びサポートスタッフが資格を取得し、お客さまへのご案内体制を強化
- 全国47の都道府県警・警察庁と連携し、詐欺被害防止に関する啓発チラシの作成・配布や注意喚起動画の周知など、全国規模の啓発活動を推進
- 埼玉県さいたま市・神奈川県藤沢市・愛知県名古屋市・福岡県福岡市など12自治体と連携協定を締結し、地域における安心・安全なデジタル利用推進等に関する連携活動を展開

③詐欺対策のエコシステム構築

詐欺被害が世界中で拡大する中、各国の政府・金融機関・通信会社・プラットフォーム事業者が連携し、詐欺情報を共有するエコシステムの構築が進んでいます。日本においても、同様の取り組みが急務となっています。

当社は、国際的な詐欺対策団体「Global Anti-Scam Alliance（GASA）」の創設メンバーとして、国内での産官学連携による詐欺対策基盤の構築を目的に、2025年5月14日、「詐欺対策カンファレンス Japan 2025」を GASA、Google、Gogolookと協力して開催しました。

本カンファレンスには、政府・法執行機関・関連団体・学術機関の専門家に加え、プラットフォーム事業者やサイバーセキュリティ企業、各業界を代表するリーダーが参加。さらに、海外から官民連携の詐欺対策を推進するキーパーソンも招き、最新の詐欺の動向や対策、官民・民間連携の戦略について、実践的かつ建設的な議論を交わしました。

また、2026年6月には一般社団法人トラスト＆セーフティ協会から、日本におけるオンライン詐欺対策の抜本的強化に向けた「日本オンライン詐欺対策アライアンス（Japan Anti-Scam Alliance: JASA）」の設立準備開始とトレンドマイクロが設立支援パートナーとして協力することが発表されました。

当社は今後も、産官学の多様なパートナーと連携し、日本における詐欺対策エコシステムの構築に向けた取り組みをさらに推進していきます。

安全な開発体制の構築

当社のビジョンを実現するためには、お客さまの環境を守るための製品機能を強化していくだけでなく、製品自体および製品サプライチェーンのセキュリティも強化していくことも重要です。

開発体制

セキュリティを高める２つの組織

より安全性の高い製品を作るための組織として、RDSec部門とInfoSec部門を整備しています。

RDSec部門は開発プロセスのセキュリティを向上させることを、InfoSec部門は開発・運用環境のセキュリティを守ることを、それぞれ目的とした組織です。

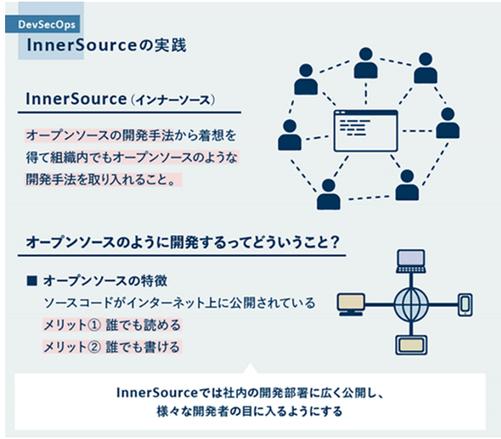
DevSecOps bibleの策定

開発プロセスのセキュリティ向上のために、「DevSecOps bible」と呼ぶ、ポリシー＆ベストプラクティス集を策定し、全ての開発メンバーがDevSecOps bibleに従って製品開発を行います。

DevSecOps bibleの見直しは適宜行われ、開発メンバーは誰でも新しいポリシーを提案することができるようになっています。

InnerSourceの実践

また、「InnerSource（インナーソース）」という取り組みも実践しています。インナーソースは、オープンソースの開発手法に着想を得た取り組みで、ソースコードを開発部門内に公開するというものです。



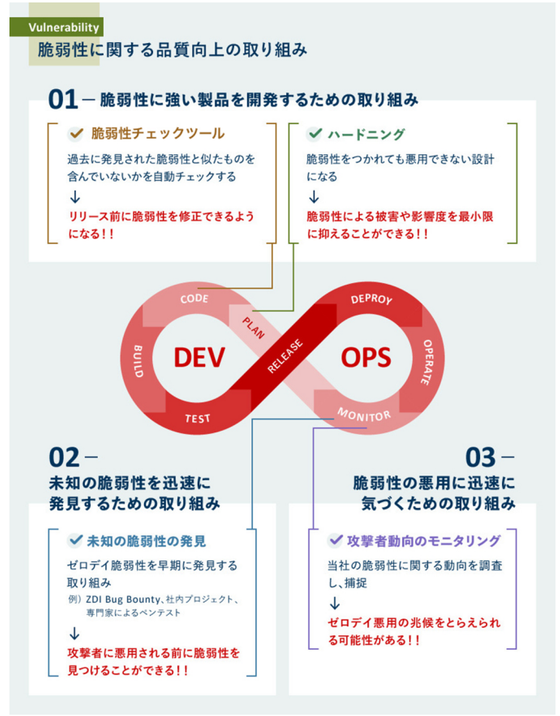
多くの開発者がソースコードを閲覧できるようになることで、サプライチェーン攻撃や内部犯行による不正なコードの挿入を発見できるようになり、製品セキュリティが向上します。それに加え、ナレッジの共有による工数の削減や開発力の向上も期待できます。

脆弱性に関する取り組み

脆弱性の早期発見と修正を実現するため、各種取り組みを実施しています。

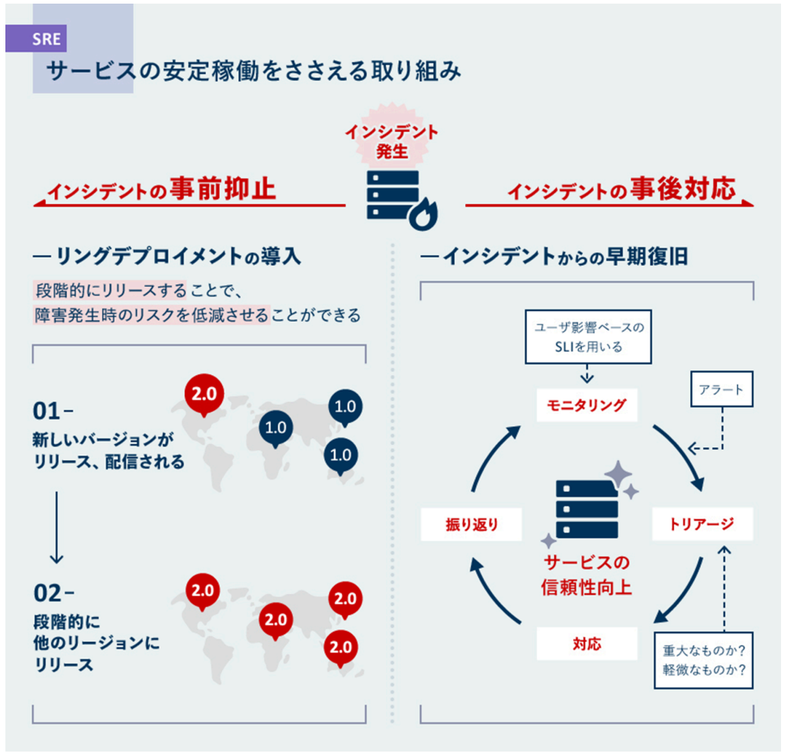
脆弱性対策の一環として、当社ZDI （Zero Day Initiative）のネットワークと知見を生かしたバグバウンティプログラムの実施や、社内セキュリティリサーチャによる脆弱性調査体制などを整えています。

当社製品で脆弱性が発見された場合は、JPCERT/CC（JPCERTコーディネーションセンター）と連携して適切な情報公開に努めています。



SaaS製品の信頼性向上に向けた取り組み

サイト・リライアビリティ・エンジニアリング（SRE）とは、スケールするシステムのサービス運用をエンジニアリングで改善してサービスの信頼性の確保とサービス成長のバランスをとる、Googleが提唱した方法論です。当社でもお客さまに安心してSaaS製品をご利用頂くために、日本及びグローバル全体でSREを導入し、SaaS製品の信頼性向上に取り組んでいます。



障害発生リスクの低減

リングデプロイメントと呼ばれる、新しいバージョンのソフトウェアリリースを段階的に行う方法を採用しています。

これは、新機能の提供を希望する国・地域からソフトウェアをリリースし、安定稼働を重視する国・地域でのソフトウェアリリースを遅らせるというソフトウェアリリース方法です。

この方法により、万が一、障害が発生しても影響範囲を限定することができます。

障害の早期発見・復旧

24時間365日、SaaS製品の稼働状況をモニタリングすることで、障害発生の早期発見が可能な体制となっています。

CPU使用率、メモリ使用率、ネットワークトラフィックなどのリソース状況をモニタリングするだけではなく、お客さまがSaaS製品を利用されるシナリオを想定してモニタリング対象や閾値を設定しています。

また、定期的に障害対応訓練を実施し、障害が発生しても早期に復旧できるように取り組みます。

セキュリティ・バイ・デザインの実践

製品自体のセキュリティ強化のため、セキュリティ・バイ・デザインの考えのもと、開発工程の全フェーズで製品セキュリティ向上のための施策を取り入れたセキュア開発ライフサイクルを定義しており、これは当社サービスのISO/IEC 27034-1（アプリケーションセキュリティ標準）認証取得の基礎となっています。

設計フェーズ

Threat Modeling（脅威分析）により他の手法では発見できない設計特有の問題を発見し解決に導きます。Threat Modelingは、リスクについて考えうるうえで役立つ抽象化された概念です。データフローや格納場所を整理してシステムをモデル化し、STRIDEを活用して脅威を探索します。例えば、プロセスがユーザからデータ入力を受け取る場合はどのような脅威が想定されるかを STRIDE に沿って検証します。

実装フェーズ

開発者によるコードレビューや静的コード解析ツールを用いて脆弱性検索を行います。検出されたケースを全て検証して影響のある項目を精査し、脆弱性の深刻度や成立条件などを確認します。

当社製品で使用しているサードパーティ製のモジュールに脆弱性がないか、外部ツールを用いて定期的に確認しています。

また、実行ファイルのビルド後に各種セキュリティフラグの確認を行い安全なファイルが生成されていることを確認します。

検証フェーズ

社内セキュリティ部門によるペネトレーションテストに加え専任のペネトレーションテストチームによる動的テストを行います。また、製品出荷前に各フェーズで実施されたセキュリティ検査への遵守状況のレビューを行っています。

それでも製品出荷後に脆弱性が発見・報告された場合に備え、PSIRT（Product Security Incident Response Team）および、お客さま対応のエンジニアチームによる速やかで適切な対応ができるように万全の体制を敷いています。

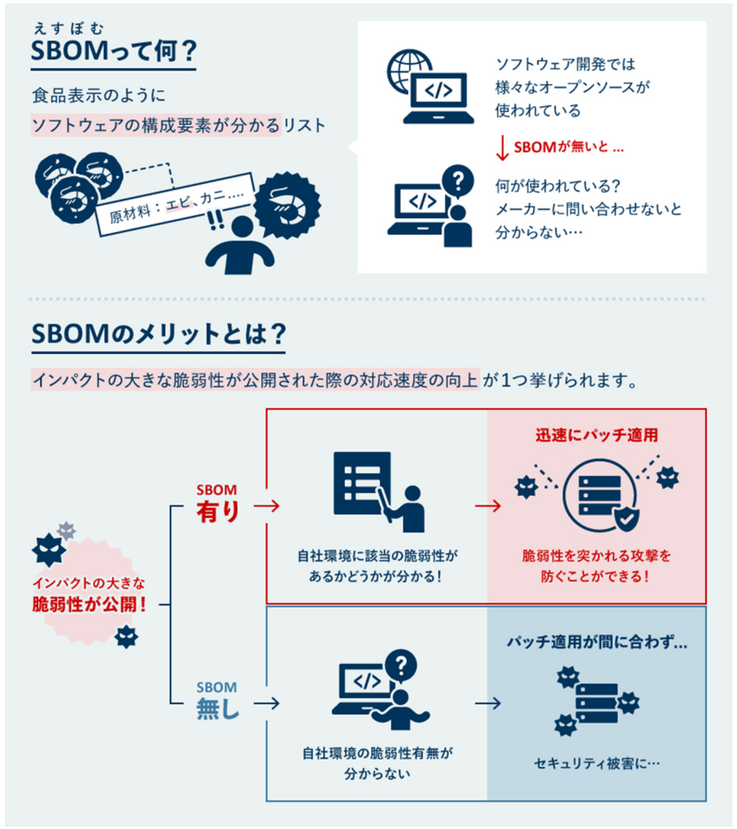
SBOMに関する取り組み

SBOMとは

ソフトウェア・サプライチェーンに存在する脆弱性特定に関して、ソフトウェアの開発組織と利用組織双方の課題を解決する仕組みの一つとして、SBOM（Software Bill of Materials）が注目されています。SBOMとはソフトウェア部品構成表のことで、ソフトウェアを構築する際のコンポーネントの詳細とサプライチェーンの関係性を含む正式な記録になります。SBOMはよく食品の包装に記載されている原材料の一覧と例えられ、ソフトウェア・サプライチェーンのトランスペアレンシー（透明性）とトレーサビリティー（追跡可能性）を確保する有効な手段とされています。アメリカでは相次ぐサプライチェーンに関連する被害事例の影響の大きさを鑑みて、NTIA（アメリカ合衆国国家電気通信情報管理庁）からSBOMの最小要素を定めた「The Minimum Elements For a Software Bill of Materials (SBOM)」が公表されるなど、SBOM提供の義務化に向けた動きが進んでいます。

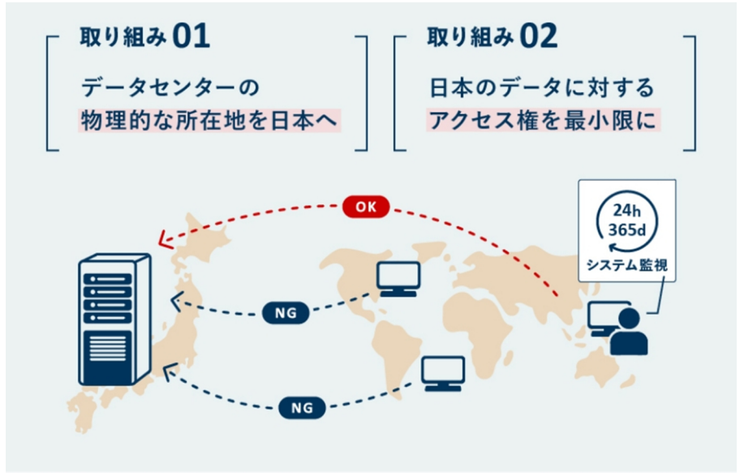
SBOM提供の体制について

当社のオンプレミス製品をご利用のお客様がSBOMの提供を必要とする場合、当社ではSBOMを個別に提供することが可能です。SaaSサービスに関しては、当社が定めた脆弱性対応プロセスに準じて適切な脆弱性対応を行うため、原則ご提供しておりません。



地政学リスクを考慮した製品・サービスの設計

安全保障に関する意識の高まりから、情報資産を保護するために国外への重要データの持ち出しを規制する機運が高まっています。これにより、製品設計時に「どこの国で運用されているか」、「顧客のデータはどこにあるのか」という地理的・地政学的な要素も十分に考慮する必要が出てきました。このような機運の高まりの中、当社でも「地政学的観点によるデータの取り扱い」は、安心して製品をご利用いただく上で欠かせない要素であると考えています。当社では、地政学リスクに関して以下のような２つの取り組みを行っています。



データセンターの物理的な所在地を日本へ

当社が提供しているSaaSサービスについて、サービスが稼働するデータセンターは、製品購入時に日本リージョンを選択した場合、物理的に日本国内で動作（一部以前から動作している製品は米国のデータセンターで動作）するように設計されています。当社では、自社のデータを意図しない形で取得されたり、想定外の使われ方をしないよう、物理的な所在地を日本中心とすることで、ガバメントアクセスの影響を最小限に抑えようとしています。

日本のデータに対するアクセス権を最小限に

従来実施していたアクセス権限の管理に加え、「日本でサービスをご契約いただいた方のデータは、アクセス権限を最小限に」するように見直しを行っています。

具体的には、日本のお客さまが利用する製品のデプロイや監視を行うLocal SRE（Site Reliability Engineering）チームや、24時間365日のシステムモニタリングを行う部署などにはサービスの運用に必要な権限を割り振りますが、アクセス権限の必要ない部署については、不必要なアクセス権限を与えないように設計を変更しています。

このようなアクセス分離を行った場合、保守サポートのスピードと効率性が低下するという影響も発生する可能性があります。しかし、地政学リスクを考慮した結果、デメリットを上回る恩恵があると当社では考え、現在このような設計変更に取り組んでいます。

トレンドマイクロにおける品質管理

トレンドマイクロは、サイバーセキュリティのグローバルリーダーとして、製品アップデートがお客様の業務に悪影響を与えないよう、多層的な品質管理プロセスを継続的に運用しています。すべての重要コンポーネント更新に対し、「開発」、「テスト」、「リリース」、「復旧」の4フェーズから構成されるセーフティネットを採用しています。

パターンファイルやルールのアップデート

パターンファイル、フィルタ、ルールなどのアップデートは、多くの製品・サービスで最も頻繁に更新されるコンポーネントであり、新たな脅威へのプロアクティブな保護を提供します。その性質と更新頻度から、リリース前のテストが非常に重要です。

- **開発**：パターンコードレビュー、脅威の網羅性確認、既知のOSおよびファイルとの照合を実施
- **テスト**：統合・パフォーマンス・検出・リグレッションテストに加え、社内環境への先行展開（ドッグフーディング）により本番品質を検証
- **リリース**：問題発生時に即時停止できる段階的展開でグローバルに配信
- **復旧**：リリース後に問題が発見された場合、迅速にロールバックできるメカニズムを整備

パターンファイルやルールのアップデート

パターンファイルほど頻繁ではありませんが、製品･機能更新時にも厳格な品質プロセスを実施しています。

- **開発**：BSODセーフティネットにより、ドライバ・コンポーネントの重大エラーを事前に検出し、自動的に無効化するメカニズムを実装
- **テスト**：包括的なテスト環境で主要な構成・シナリオを検証し、ドッグフーディングにより社内展開でグローバルリリース前の動作を確認
- **リリース**：社内展開・アーリーアダプター・一般提供・ミッションクリティカル環境の順でリングデプロイメントを実施。お客様側でもバージョン管理やスケジュール設定が可能
- **復旧**：リリース後に問題が報告された場合、該当アップデートを迅速に削除し、正常なバージョンまたは修正済みバージョンへ速やかに置き換え

これらのプロセスのほとんどは、業界標準を採用しており、いくつかは3rdパーティ（ISOなど）によって認定されています。

https://www.trendmicro.com/ja_jp/about/security-activity/quality-management.html

サイバーセキュリティ・イノベーション研究所

サイバーセキュリティはもはや専門家領域ではなく、事業に関わるすべての層の従業員（経営層、事業統括責任者、業務担当者）に求められる領域です。昨今ではDX（デジタルトランスフォーメーション）を推進するために必要な取り組みであると社会的にも認知が進んでいるところです。そのような社会的背景を受け、当社ではDX with Cybersecurityを目指す企業や日本政府などと積極的に情報を共有・交換しベストプラクティスを提供できる組織として、2021年1月1日付けでサイバーセキュリティ・イノベーション研究所を設立しました。

この研究所には、自らの製品の安全性をどのように担保できるかを追求する「トランスペアレンシー・センター」、脅威に関するインテリジェンスをどのようにお客さまに活用頂くかを追求する「スレット・インテリジェンス・センター」、そしてセキュリティ専門人材に加え、専門家ではない層の従業員もわかりやすく体系的にセキュリティの本質を学んで頂くための「セキュリティ・ナレッジ＆エデュケーションセンター」の３つのセンターを設置しています。

外部公開

当社では、「お客様に安心して製品をお使いいただくための環境整備」を担い、当社が提供するソリューション品質向上や開発プロセスの情報公開による透明性の確保、サプライチェーンリスクへの対応などを行います。

透明性に関するWebサイトの公開

近年は経済安全保障の懸念の高まりにより、製品の安全性や透明性に関するお問い合わせをいただく機会が増えています。この流れを受けて、当社では、2024年3月に当社のサービスの透明性に関する情報を掲載した専用のWebサイトを公開しております。

経済安全保障推進法の対応

2022年5月に成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（以下、経済安保推進法）」は４つの柱から構成されていますが、その柱の１つである「基幹インフラ役務の安定的な提供の確保（以下、基幹インフラ制度）」に関して、2024年5月17日から規律の適用が開始されました。

基幹インフラ制度は、国が定めた基幹インフラ事業（特定社会基盤事業）を導入する事業者（特定社会基盤事業者）に対して、重要設備（特定重要設備）の導入・維持管理等の委託をしようとする際に、事前に届出を行い、審査を受ける制度です。この事前審査では、「特定重要設備の供給者」および「構成設備の供給者」が審査の対象とされます。

そのため、特定社会基盤事業に関するシステムの導入において当社製品をご利用いただく場合、当社も事前審査に協力する必要があり、審査を迅速に・適切に行うことができるように、経済安保推進法の案件管理のためのシステムを構築し、対応しています。

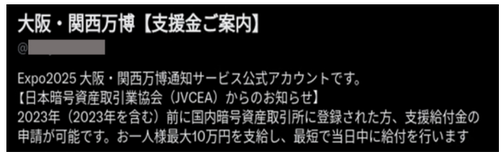
スレットハンティング調査

当社では長年にわたり、様々な国内外のイベント（スポーツ、文化、政治、国際イベントなど 例※1）開催時には特別体制を取りOSINTや独自の脅威のリサーチを積極的に行い、その過程で発見した脅威について協定、協力に基づき関係各所に脅威情報の提供を行っています。

2025年には、大阪・関西万博(2025年日本国際博覧会 Expo 2025 Osaka, Kansai, Japan)において特別体制を取り、「大阪・関西万博を想起させるドメイン取得とフィッシングサイト」、「SNSのおける偽アカウント」、「偽ショッピングサイト」、「チケット転売」や、攻撃者によるAI活用の可能性などを確認し、リサーチ結果を関係各所にタイムリーに提供しました。また、リサーチ結果の一部については、当社ブログを通じて広く注意喚起（※2）を行いました。

大阪・関西万博関連を装った不審サイト

※1 トレンドマイクロセキュリティブログ：SNS乗っ取り、不審メール、東京オリンピックを前に関連脅威が露見
https://www.trendmicro.com/ja_jp/research/21/g/analyzing-the-executable-urgent-damage-reports-regarding-cyberattacks-related-to-the-Tokyo-2020-Olympic-Games-exe.html



大阪・関西万博関連を装った偽SNSアカウント

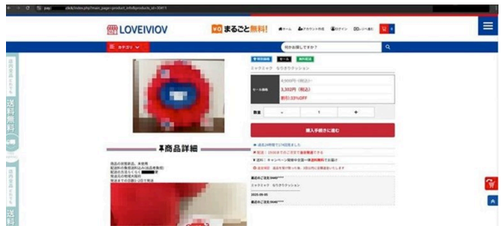
※2 トレンドマイクロ　Security Go:大阪・関西万博に便乗したサイバー犯罪の実態～大型イベントに潜む脅威と備え
https://www.trendmicro.com/ja_jp/jp-security/25/k/expertview-20251104-01.html

また、当センターではSEOポイゾニングなどを利用した偽ショッピングサイトへの誘導などについてもリサーチを行っており、直接万博を狙ったものではないものの、国際的なイベントという、注目、人気を集めるイベントゆえに、結果的に大阪・関西万博関連グッズを検索すると偽ショッピングサイトが検索エンジンの上位に表示されることで利用者が偽ショッピングサイトに誘導される事例も確認し広く注意喚起（※3）を行いました。

※3 トレンドマイクロ セキュリティブログ：偽ショッピングサイト：大阪・関西万博グッズの検索結果からの誘導を確認
https://www.trendmicro.com/ja_jp/research/25/i/fake-shopping-sites.html

万博関連グッズの検索結果で、偽サイトが上位に表示

※4:トレンドマイクロ プレスリリース：トレンドマイクロが大阪・関西万博の警察活動へ協力
https://www.trendmicro.com/ja_jp/about/newsroom/press-releases/2025/pr-20251114-01.html



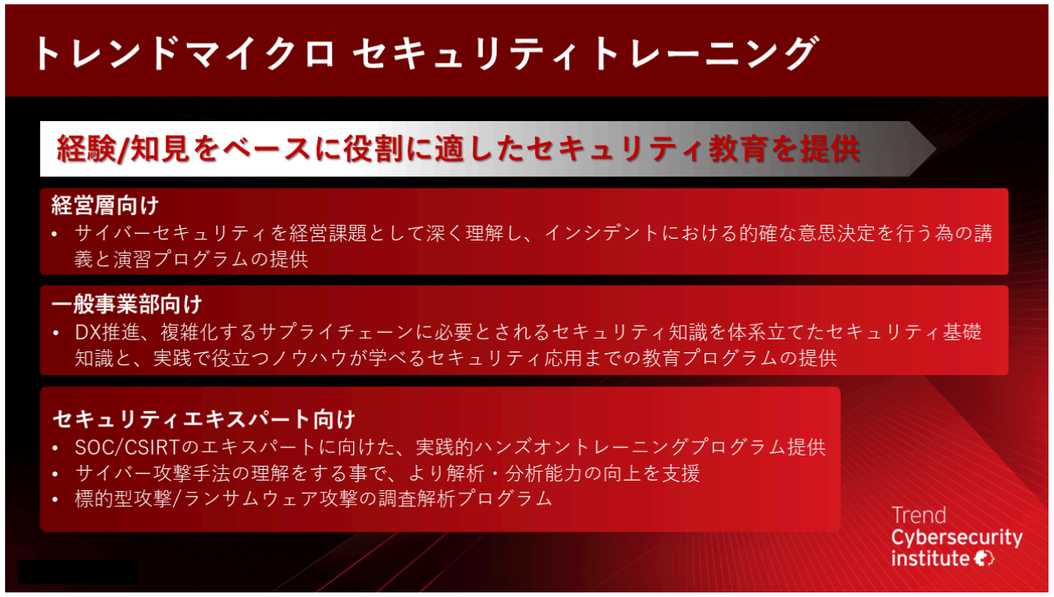
偽ショッピングサイトの例

※5: トレンドマイクロ プレスリリース：（東京オリンピックの事例）東京2020大会のサイバーセキュリティでNISCを支援～サイバーセキュリティの脅威情報提供により、NISCが当社に感謝状を授与～
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220310-01.html

これらのイベントに対するリサーチ活動、情報提供については、最新の手口を明らかにすることにより、脅威の防止、被害の最小限化に貢献したことが認められ関連組織より感謝状を授与いただくに至っています。

外部向けトレーニング

サイバーセキュリティにおける、解析技術、防御技術、調査技術などの技術的なプログラムはもちろんのこと、サイバーセキュリティを企業における経営の持続性における重要なファクターと位置づけ、危機管理、事業継続、リスク低減など「サイバーセキュリティ」=「リスクマネジメント」の視点で「サイバーセキュリティ」を事業継続性の組織課題としてとらえ対処するセキュリティナレッジトレーニングにも力を入れており、技術から社会全体におけるサイバーセキュリティの理解・普及まで幅広いトレーニングを提供しています。



図：当社 トレーニングプログラム概要

社会課題であるサイバーセキュリティ対策理解のため経営層向けトレーニングの推進

昨今サイバーセキュリティ被害は企業経営における事業継続性に直結することも多く、これらの課題を解決するためにサイバーセキュリティの理解、特にリスクマネジメントとしてのサイバーセキュリティの必要性、重要性、そして事業継続のあるべき姿を社会全体で実現していくために、経営層の役割が重要と考えています。そのため当社では、リスクマネジメント・モデルである「PDCAサイクル＋OODAループ」など当社でも実践している活動なども含め、企業全体でリスクマネジメントとして、サイバーセキュリティに取り組む必要性、方法論を経営層が理解し実践につなげるための経営層向けトレーニングに力を入れています。

以下に、当社が提供している経営層向けトレーニングの目的、内容の一部を掲載いたします。

■ 経営層向けトレーニング実施の目的

- 経営課題として考えるべきサイバーセキュリティを理解
- 経営層としてサイバーセキュリティに対する役割を理解
- 重要インシデント発生時の経営判断を行う為の共通の理解や認識を得る

■ 経営環境とセキュリティ

- PEST分析による現状のサイバー脅威の実情の把握
- 組織的分業化され高速化、巧妙化するサイバー攻撃の実態
- 自社が狙われる理由、ランサムウェアなどの被害例

■ 平常時のリスクの把握

- マクロ視点としての組織全体のセキュリティレベルの把握
- ミクロ視点としての事業、業務毎のビジネスインパクトを踏まえたリスクの把握

■ 平時の体制整備

- ビジネス（事業）戦略とサイバーセキュリティ戦略
- サイバーセキュリティにおける経営層のリーダーシップ
- サイバーセキュリティを「自分事化」する為の３線モデル

セキュリティを自分ゴト化する「３線モデル」

ガバナンスの効いた組織にするために提唱されているのが３線モデル。この「3つのディフェンスライン（three lines of defense）」は、COSO（Committee of Sponsoring Organizations of the Treadway Commission：トレッドウェイ委員会支援組織委員会）「内部統制の統合的フレームワーク」において示されている考え方で昨今の日本企業においても注目されているアプローチで日本企業でも導入が進んでいる。

第1のディフェンスライン（1線）
事業部門。自らの管轄するビジネス推進に伴って発生するリスクの発生源となりリスクに対するオーナーシップ（責任・意思決定・実践）を持つ立場

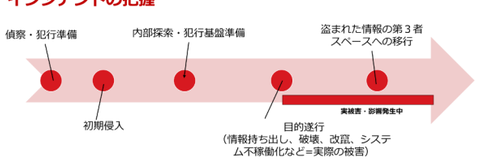
第2のディフェンスライン（2線）
リスクマネジメント、セキュリティ、IT、財務、法務およびコンプライアンス等を含む間接管理部門で、第１線をモニタリング、支援・助言・監督し、かつ組織横断的なリスクへのオーナーシップを持つ立場

第3のディフェンスライン（3線）
内部監査部門。1線および2線の行った業務を評価し、その適切性を保証するほか、必要な助言を提供する立場

出典：BUSINESS LAWYERS「三つの防衛線（3つのディフェンスライン）によるリスクマネジメント」 https://www.businesslawyers.jp/articles/783

■ インシデント発生時の判断

- 経営判断のためのインシデント発生段階の把握
- 事例を元にした判断事例と判断基準の理解

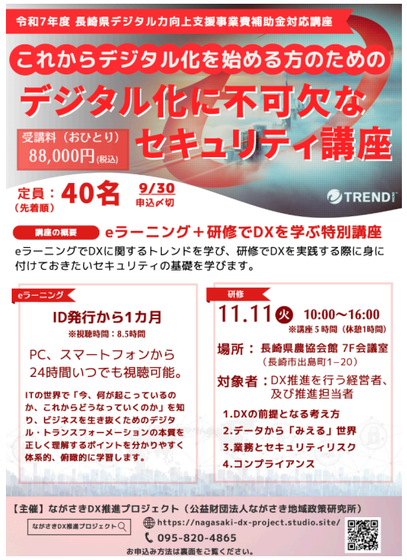


経営層は、インシデントの発生推移の、**どの段階か**を理解・把握する必要がある。
業務への影響発生前→**被害を最小化**することを優先する
業務への影響発生後→**影響の拡大を防ぐ**ことを優先する

これら、経営層主導のサイバーセキュリティを積極的に推進していらっしゃる企業・団体への本トレーニングを提供した実績の一部を以下に掲載いたします。

■ 長崎県様 デジタル力向上支援事業 『デジタル化に不可欠なセキュリティ講座』

- 令和7年度長崎県デジタル力向上支援事業費補助金対応のセキュリティ講座
- DXを安全に推進するためのIT基礎、配慮すべきセキュリティの講座



■ ANAホールディングス株式会社様 経営層自ら実施 事業継続や組織運営を踏まえたサイバーセキュリティインシデント演習

- 講義および「不測の事態における高度な判断」の必要性を経営層が実感できる演習を実施
- トレンドマイクロの執行役員 日本地域CISOである清水 智が自らの経験を元に講義を実施
- 同じ役員目線で実践的な講義を提供

事例公開ページ：
https://www.trendmicro.com/ja_jp/about/customer-stories/2025/ANA.html

技術的な対策、能力向上を推進する技術者向けトレーニング

防御の根幹となる技術面からサイバーセキュリティを支援するトレーニングプログラムについても引き続き提供しています。当社が支援したインシデントレスポンスの経験なども含め、攻撃者の手口を学ぶことにより、環境規制型攻撃などの気付くことが難しい攻撃に気付けるスキルを身に着けるためのThreat Hunting視点も取り入れたトレーニングや、防御策、そして実際に被害が発生した環境での調査方法など幅広い技術者向けトレーニングを提供しています。また、これらのトレーニング強化の一環として、積極的に経産省情報処理安全確保支援士の特定講習への登録を進めています。この度、新たに「Webサーバプロアクティブリスク対策トレーニング」が加わり、現在以下5つのプログラムが特定講習として登録されています。

インシデント調査トレーニング クライアント端末版
Windowsの機能や各種ツールまた弊社EDRを活用し、インシデント発生源、影響範囲等の調査と対処方法を学習します。

Webサーバプロアクティブリスク対策トレーニング
Webサーバの構成要素を把握したうえで、その脅威と対策を座学およびハンズオン形式で学習します。

標的型攻撃 対応・防御 トレーニング3日版
標的型攻撃対応・防御トレーニング5日版の内容を3日間に濃縮し集中的に学習可能なトレーニングです。

標的型攻撃 対応・防御 トレーニング5日版
標的型攻撃についての技術や手法を理解し、侵害されたネットワークの調査・解析を学習します。

ランサムウェア 対応 防御トレーニング
ランサムウェア攻撃の侵入から暗号化までのプロセスを座学と演習、ワークショップを交えて学習します。

セキュリティ認証

当社は、お客様に製品を安心してご利用頂けるように、必要なセキュリティ認証を原則として製品・サービス単位で取得しています。

取得済みの主なセキュリティ認証

個人情報保護

- **プライバシーマーク**

  プライバシーマーク制度（PrivacyMark System）は、事業者の個人情報保護の体制や運用の状況が適切であることを、<プライバシーマーク> というロゴマークを用いてわかりやすく示す制度です。当社は、日本産業規格「JIS Q 15001個人情報保護マネジメントシステム－要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備しています。

情報セキュリティ

- **SOC2 Type II**

  SOC（System and Organization Controls）報告書は、米国公認会計士協会（AICPA）の既存の Trust サービス基準（TSC）の監査基準審議会に基づく報告書です。セキュリティ、可用性、処理の完全性、機密性、プライバシーに関して組織の情報システムを評価することを目的としています。Type IIの監査は、当社のコントロールが時間を通じて効果的に機能していることを検証するものであり、特定の期間にわたる実際の運用に焦点を当てています。

  この継続的な評価は、当社がサービスの提供において一貫して高い基準を保っていることを保証します。

- **ISO®20000**

  脅威検出・レスポンスチームを通じて高品質のデータを確保することにより、当社はISO/IEC 20000-1:2018認証を取得しています。このISO規格には、組織がサービスマネジメントシステム（SMS：Service Management System）を確立、実施、維持、および継続的に改善するための要件が定められています。

- **ISO®20243**

  O-TTPS（Open Trusted Technology Provider™ Standard）としても知られており、情報通信技術（ICT）サプライチェーンにおける悪意のある改ざんや偽造コンポーネントのリスクを軽減することに重点を置いています。

- **ISO®27001、27014、27034**

  ISO/IEC 27001:2013は、セキュリティ制御を含む情報セキュリティマネジメントシステム（ISMS：Information Security Management System）の整備に焦点を絞った規格であり、製品の安全なオペレーションの実現を目的としています。この規格には2つの拡張機能があります。

  ISO/IEC 27014:2020は情報セキュリティガバナンスに関する基準で、ISO/IEC 27034-1:2011はアプリケーションセキュリティ管理策に関するガイドです。当社はセキュリティおよびプライバシーへの取り組みを示すことによって、この国際規格に基づくSaaS製品およびデータセンターが認定されています。

- **ISO®27017**

  クラウド製品のセキュリティとプライバシーに対する取り組みにより、当社はISO/IEC 27017:2015の認証を取得しています。この規格では、クラウドサービスのプロビジョニングと使用に関連する情報セキュリティ制御の指針が得られます。

- **ISMAP**

  政府情報システムのためのセキュリティ評価制度（ISMAP：Information system Security Management and Assessment Program）は、日本政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度です。当社のクラウドサービスがISMAPに登録されたことにより、これらのサービスが政府の求めるセキュリティ要件を満たしていると評価されました。

- **FedRAMP®**
  FedRAMP（Federal Risk and Authorization Management Program）は、クラウドサービスを対象とする米国連邦政府の調達要件に関する認証制度です。
  Trend Vision One for GovernmentとTrend Cloud One for Governmentを通して、物理環境、仮想環境、マルチクラウド環境にセキュリティを導入して、可視性、管理、検出、防御を一元化できます。

クラウド コンピューティング コンプライアンス基準カタログ

タイプ 2

Cloud Computing Compliance Controls Catalogue - Type 2

- **Cloud Computing Compliance Controls Catalogue（C5）- Type2**
  C5カタログ（Cloud Computing Compliance Controls Catalogue）Type 2はドイツ連邦政府の情報セキュリティ庁（BSI：Bundesamt für Sicherheit in der Informationstechnik）が導入した認証です。
  C5は、クラウドコンピューティングの現状把握、既存の標準に基づいた統一要件の提示、及び適合性の証明プロセスを包括しています。

- **PCI DSS Level 1 Service Provider**
  国際的なクレジット産業向けのデータセキュリティ基準（PCI DSS：Payment Card Industry Data Security Standard）では、クレジットカード情報を扱う組織はすべてクレジットカードのデータをPCIの基準に従って保護する必要があると規定されています。
  データのプライバシーとセキュリティへの取り組みの一環として、Trend Vision OneはPCI DSSの認定サービスプロバイダーです。

その他詳細については、以下のWEBサイトをご参照ください。
https://www.trendmicro.com/ja_jp/about/trust-center/compliance.html

インシデント発生状況

2025年度（2025年4月～2026年3月）の期間において発生したセキュリティ・インシデント※はございません。

※個人情報保護委員会への報告を行っているなど事業インパクトを有する重大なインシデントを対象としています。

サイバーセキュリティ経営ガイドライン対応

経済産業省が発行している「サイバーセキュリティ経営ガイドライン」Ver 3.0のサイバーセキュリティ経営の重要10項目について、本報告書内で言及されている箇所を記載しました。

No.	指示内容	本報告書内の該当箇所
指示(1)	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	セキュリティ戦略および実績
指示(2)	サイバーセキュリティリスク管理体制の構築	セキュリティガバナンス体制
指示(3)	サイバーセキュリティ対策のための資源（予算、人材等）確保	人材育成・トレーニング・訓練
指示(4)	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	リスクの特定と対策
指示(5)	サイバーセキュリティリスクに効果的に対応する仕組みの構築	サイバーセキュリティ施策
指示(6)	PDCAサイクルによるサイバーセキュリティ対策の継続的改善	PDCAサイクル＋OODAループによる継続的なセキュリティ強化
指示(7)	インシデント発生時の緊急対応体制の整備	インシデント対応
指示(8)	インシデントによる被害に備えた事業継続・復旧体制の整備	インシデント対応
指示(9)	ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策	サプライチェーン・リスク対策
指示(10)	サイバーセキュリティに関する情報の収集、共有及び開示の促進	サイバーセキュリティ啓発及び情報共有活動への貢献

■編集方針：

トレンドマイクロは、持続可能な社会にむけて、より安全な情報社会とお客さまの未来を創造する、サイバーセキュリティのグローバルリーダー企業であり、「デジタルインフォメーションを安全に交換できる世界の実現」をコーポレートビジョンに掲げ、常に進化するデジタル技術や市場にいち早く対応したソリューションを継続して提供しお客さまの安全を守ると同時に、ビジョンを自己実現する取り組みを続けています。本報告書は、お客さまをはじめステークホルダーの皆様に当社のサイバーセキュリティに掛る取り組みをご理解頂くとともに、そうした取り組みを通して安心・安全な日本社会の構築における一助となればと願っています。

■2026年度サイバーセキュリティ報告書　報告対象期間：2025年4月～2026年3月

■編集責任：

サイバーセキュリティ報告書編纂チーム（日本地域CISO、サイバーセキュリティ・イノベーション研究所、RFPサービスグループ、インフォメーションサービス本部、経済安全保障担当部門、開発チーム）

■発行履歴：

該当年次	発行日
2021年度版サイバーセキュリティ報告書	2021年8月3日
2022年度版サイバーセキュリティ報告書	2022年7月20日
2023年度版サイバーセキュリティ報告書	2023年7月1日
2024年度版サイバーセキュリティ報告書	2024年7月1日
2025年度版サイバーセキュリティ報告書	2025年7月1日
2026年度版サイバーセキュリティ報告書	2026年7月1日

BR-REPO-090

トレンドマイクロ株式会社

www.trendmicro.com

東京本社
〒160-0022
東京都新宿区新宿4-1-6
JR新宿ミライナタワー

大阪営業所
〒532-0003
大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13階

名古屋営業所
〒460-0002
愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7階

福岡営業所
〒812-0011
福岡県福岡市博多区博多駅前2-4-2
H1O博多駅前 305号室