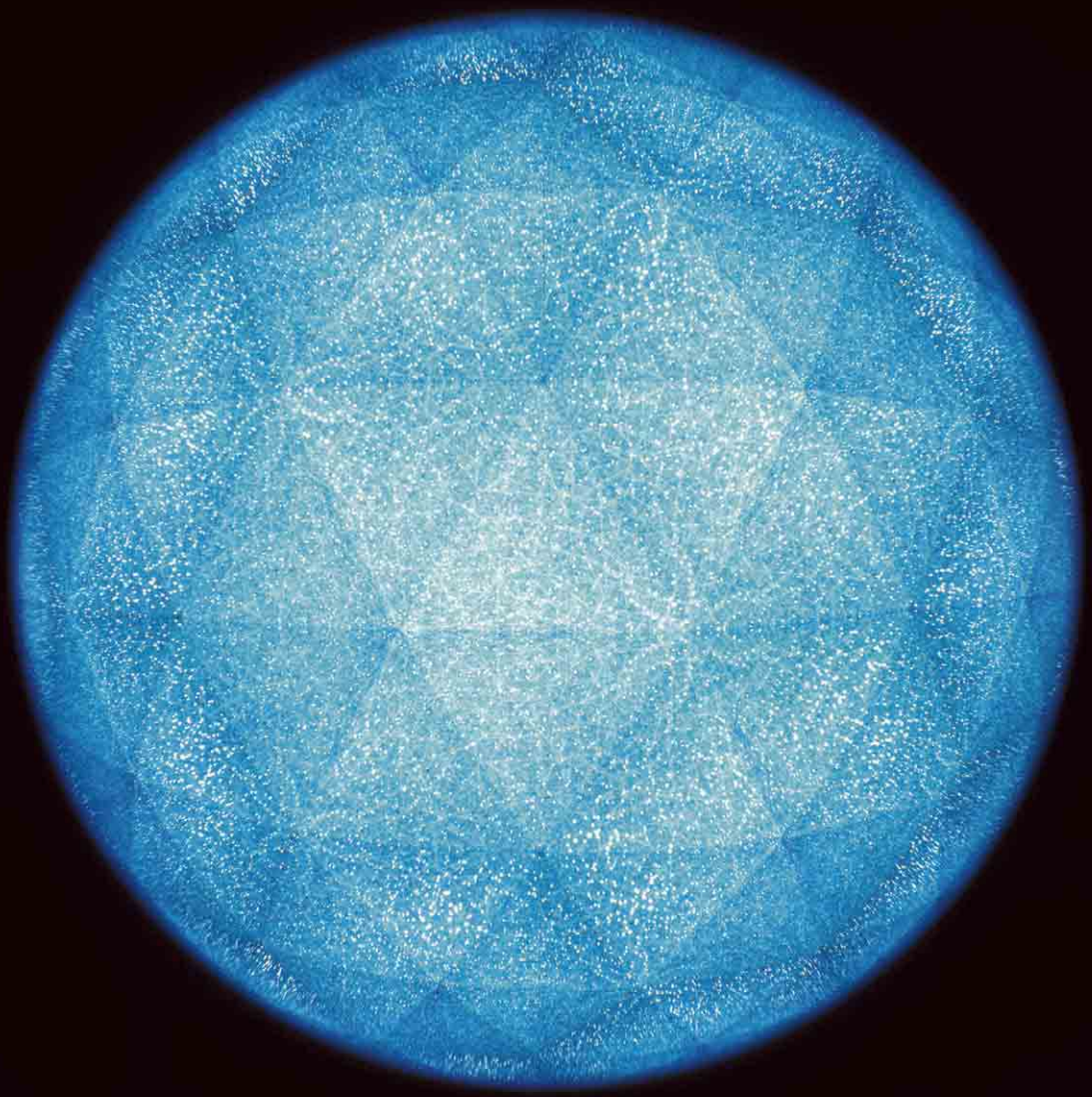
Deloitte.
デロイト トーマツ



サイバー
インテリジェンス サービス

サイバー インテリジェンスを
活用した脅威への対応

デロイト トーマツ リスクサービス株式会社

サイバー
インテリジェンスを活用し
企業を狙った
サイバー脅威に対応

近年、企業を狙ったサイバー攻撃（標的型攻撃等）の被害が急増しています。これらの攻撃は、価値の高い情報資産（技術・生産・個人情報等）の窃取・破壊・風評被害等を目的として行われ、その対策は企業にとって重要な課題となっています。また、攻撃の高度化により、従来型のインターネット境界を中心とした対策のみでは、これらの攻撃に対処することは大変困難な状況です。デロイト トーマツ グループは、各国デロイトのCyber Intelligence Center（以下：CIC）のサイバー インテリジェンスを活用し、クライアントを狙うサイバー攻撃に対応したセキュリティ脅威分析サービスを開始します。

サイバー インテリジェンス センター（CIC）とは

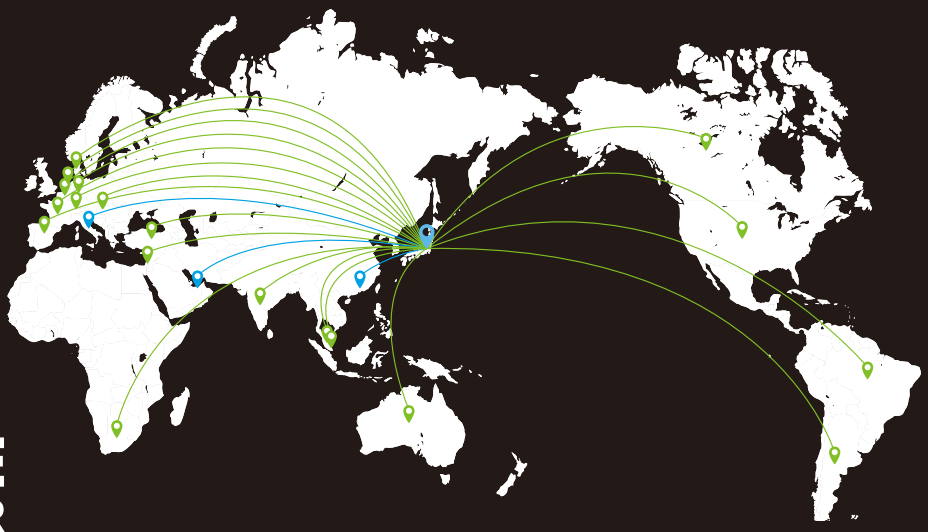
- サイバー インテリジェンスを活用し、クライアントのインフラストラクチャをサイバー攻撃から守ります。
- 世界20ヶ国以上に拠点を構え、グローバル規模のサービスを提供します。

サイバー インテリジェンス センター（CIC）の特長

- 各国で収集・分析した非常に高度なサイバー インテリジェンスを提供します。
- 境界デバイスだけでなく、Proxy・DNS・エンドポイントセキュリティ製品等も分析対象とし、クライアントのインシデントレスポンス工数を低減します。

デロイトメンバーファーム各国のCIC

各国CICとのシームレスな連携により、
グローバルにビジネス展開されている
クライアントをサポート



CYBER
INTELLIGENCE
CENTER

※準備/計画中を含み20カ国以上で展開中

サイバー インテリジェンス サービス

サイバー インテリジェンス サービスは
右記2つのサービスから
構成されています

Threat Intelligence and Analytics (TIA)

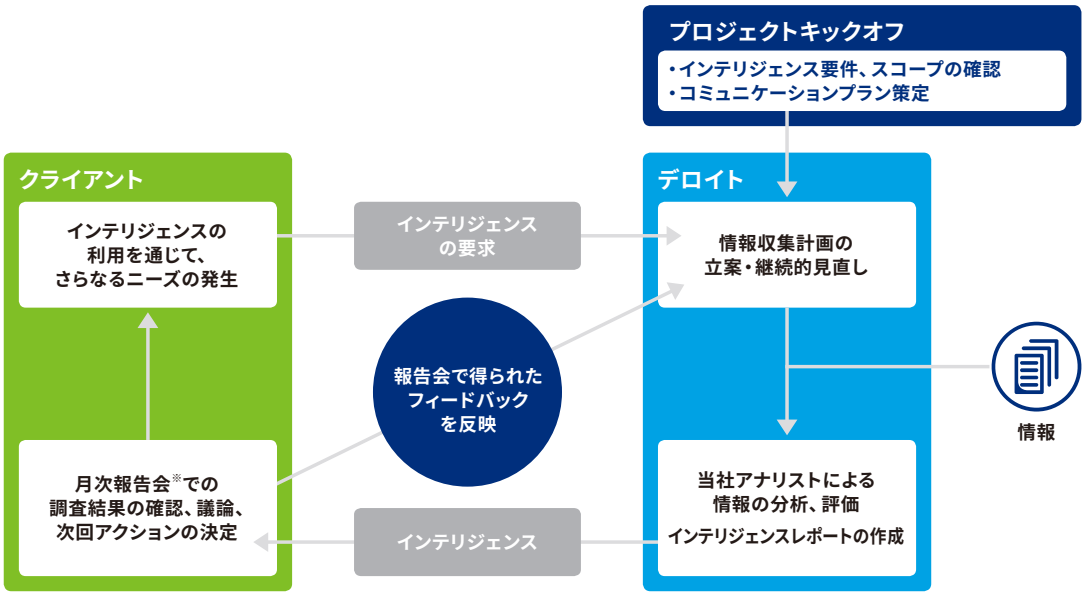
クライアントのビジネス環境に対応したインテリジェンスの提供

TIAの特長

- クライアント固有のリスクをダークネット、ディープウェブといった通常の手法ではアクセス困難なネットワークから能動的に収集し、分析結果をレポートとして提供します。
- ソーシャルメディアにおけるアクティビティやアカウント間のリンクを分析することで、クライアントのブランドに悪影響を及ぼす可能性の高いユーザー・グループを特定し、調査を行います。
- 対面での報告会を実施し、分析結果の報告を行うとともに、クライアントから分析結果に対するフィードバックをいただくことで、収集・分析計画を修正し、よりクライアントのニーズに合ったインテリジェンスを提供します。
- 新たな脅威への検知精度を高めるため、セキュリティ対策製品に取り込み可能なインテリジェンス情報（IPアドレス、ドメイン名等のIOC※）を提供します。

※IOC = Indicator of Compromise（サイバー攻撃の兆候・痕跡）

インテリジェンスサイクルに基づく能動的な収集・分析



※月次以外にも、必要に応じ随時確認・利用可能

Threat and Security Monitoring (TSM)

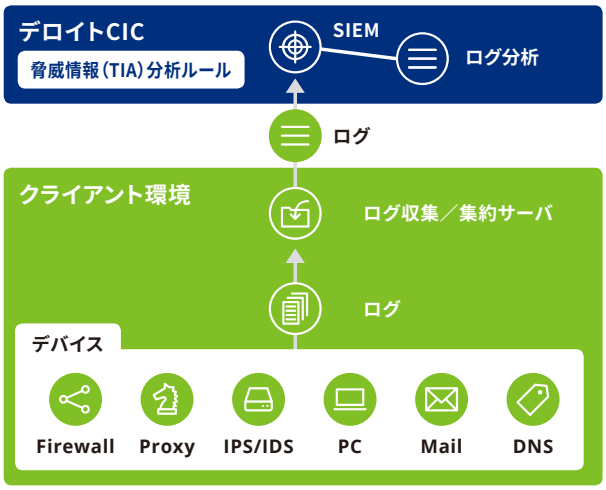
24時間365日のセキュリティ脅威分析サービス

TSMの特長

- TIAのインテリジェンスをもとに、インダストリーまたはクライアント固有のビジネスリスクとサイバーリスクとの関連性を踏まえた高度な分析サービスを提供します。
- クライアントのアセット情報を能動的に収集・更新することで、分析精度を常に高いレベルで維持します。
- 特定のベンダーやテクノロジーに依存しない、最適なセキュリティソリューションを活用します。
- インダストリー毎の脅威分析レポート、TAP（Technical Acceleration Pack）を配信します。
- セキュリティ インシデント発生時には、専任のインシデント コーディネータが収束まで対応します。

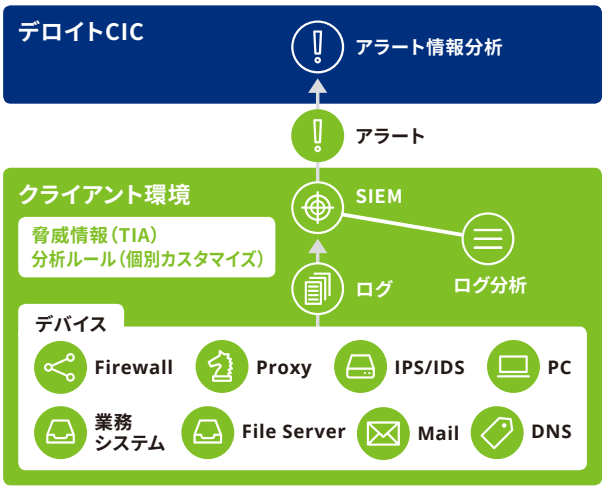
Standard / Premiumの2種類のサービス

Standard スタンダード



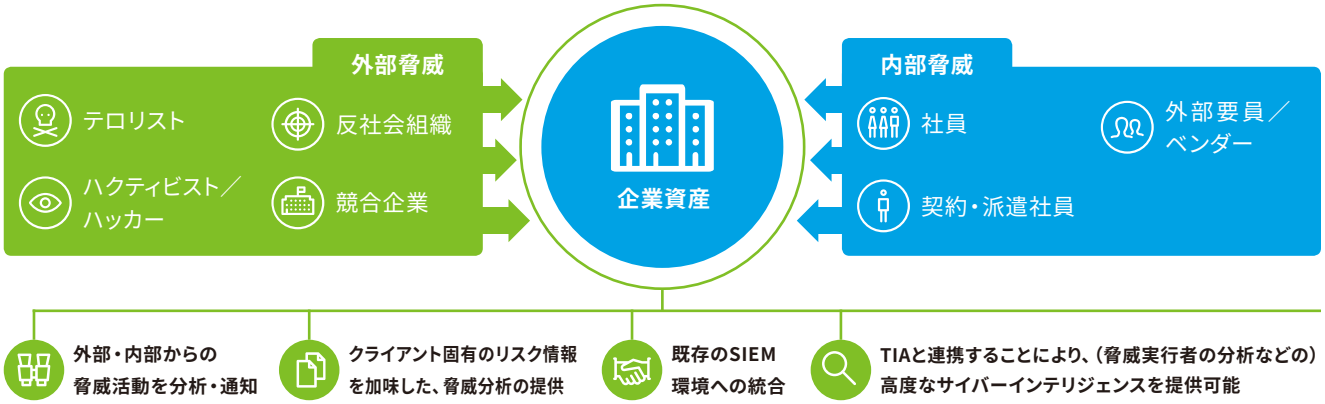
Firewall、IDSといった境界デバイスだけでなく、クライアントの様々な機器のログを収集・分析することで、従来型のアプローチでは発見が困難なサイバー脅威を検知。

Premium プレミアム



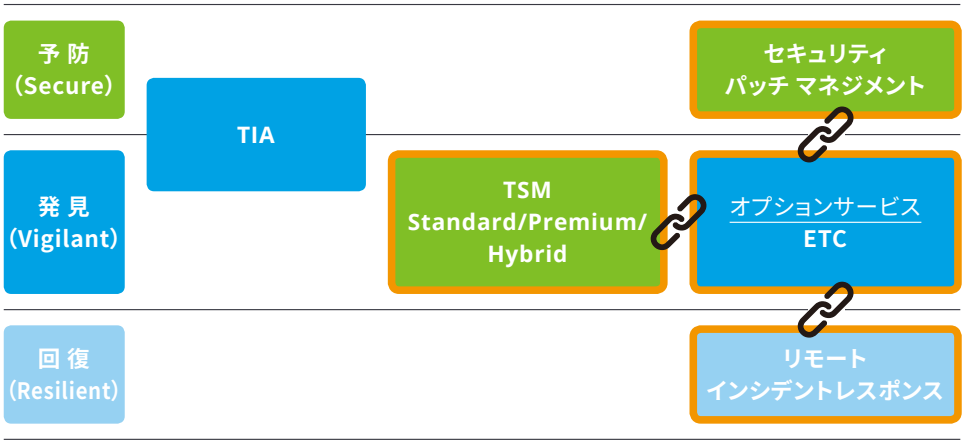
クライアントのシステム（オンプレミス環境）にSIEM製品を導入し、外部への持ち出しが困難なログを分析。
サイバー脅威や内部不正といったクライアント固有のリスクを発見し、CSIRTと連携することで、インシデント対応を全面的に支援。

Threat and Security Monitoring



TSMはエンドポイント対策をご提供する オプションサービスEndpoint Threat Control (ETC)をご用意しております

サイバー インテリジェンス サービス構成



TSMは各オプションサービスを追加することにより、「発見(Vigilant)」だけでなく、「予防(Secure)」・「回復(Resilient)」の範囲に対してもサポート可能となります。

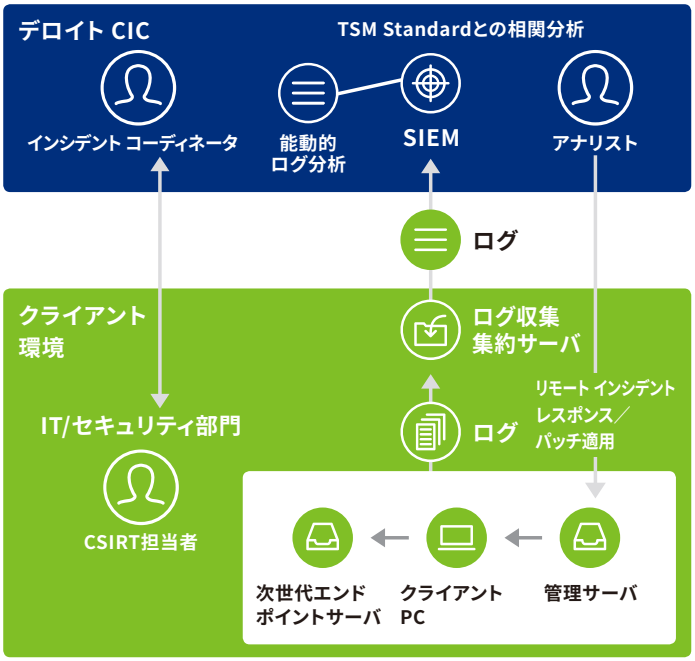
TSM+ETCではエンドポイントと SIEMによる統合分析サービスをご提供します

Threat and Security Monitoring
+ Endpoint Threat Control

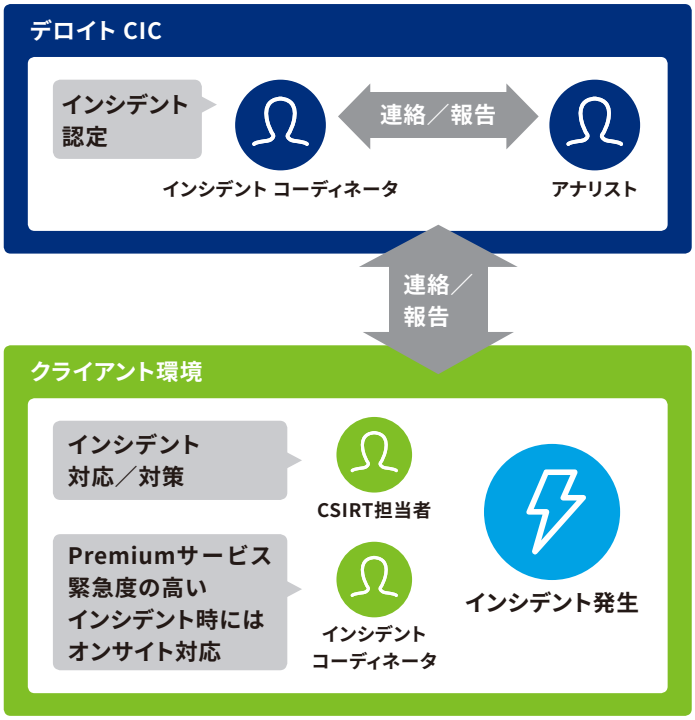
特色

- 複数ベンダーの次世代エンドポイント セキュリティ製品に対応したエンドポイント セキュリティ分析サービスを提供。
- エンドポイント製品のアラートと他機器のログを相関分析することで、感染経路や影響範囲を分析。
- インシデント発生時の対応(調査・回復・影響範囲特定)をCICのアナリストがリモートから支援。
- マルウェア感染の原因であるパッチマネジメントの支援サービスを提供。

構成概要図



TSMにおけるインシデントの発生から収束までの流れ



インシデント発生

インシデント設定

インシデント対応／対策

インシデント収束

- クライアントもしくはCICアナリストが、インシデント発生をインシデント コーディネータに申告する。

- インシデント コーディネータが内容を精査し、インシデント レスポンスの必要有無を判断する。

- インシデント コーディネータがクライアントに連絡し、インシデント レスポンスの支援を行う。
- 緊急度の高いインシデント時にはオンサイトにて対応（Premiumサービス）。
- フォレンジック等、高度な技術支援が必要な場合はオプションサービスにて提供する。

- クライアントとインシデント コーディネータは、インシデント対応完了を確認する。
- インシデント コーディネータは再発防止策のアドバイスを行う。

Deloitte.
デロイト トーマツ

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300
名古屋　〒450-6337　愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋　Tel:052-565-5950

2017.01_0063