

CTC Engineer's Insight #4

CTCが挑んだ、現場で効く金融ITセキュリティ
— 運用・検証・生成AI活用から攻撃トレンド対処まで

セキュリティ運用の勘所

伊藤忠テクノソリューションズ株式会社

金融セキュリティ技術部

小谷 陽

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

自己紹介



小谷 陽

Yo Odani

CTC・金融セキュリティ技術部
主任

<プロフィール>

- 出身:新潟県
- 理学部院卒(アルバイトでプログラマーをした経験からITの道へ)
- 新卒CTC入社 インフラ系エンジニアとして構築案件を中心に担当
- 2011年より顧客システムのインフラ運用業務に従事
- 2018年より別顧客システムのセキュリティ運用業務に従事
 - 脆弱性管理、セキュリティパッチ適用業務、CSIRTの一員としてインシデント対応、SOC連携などを担当
- 2024年より現職、CTCの金融事業のお客様へセキュリティ製品・サービスの提案・提供の推進活動に従事

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

お伝えしたいこと

- CSIRTの役割である「インシデント対応」における運用のイメージ
- セキュリティ運用における重要な事：相互理解

本日のアジェンダ

ここ数年、サイバー攻撃の手口がますます高度化し、企業のセキュリティ体制にもより強固な対応が求められています。その中でも、“運用”こそがセキュリティを支える最前線であり、最も重要な部分です。

本日は、現場のリアルな視点から、セキュリティ運用における勘所についてご紹介します。

1 セキュリティ運用の説明

CSIRTとSOCの役割と連携体制

2 セキュリティ運用の一例

実際の現場での対応フロー

3 運用改善

継続的な改善活動とAI活用

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

1

セキュリティ運用の説明

CSIRTとSOCの役割と連携体制

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CSIRTとSOCの関係

セキュリティ監視対象

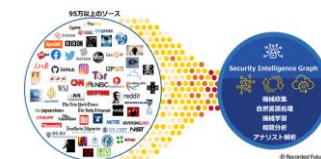


調査・対応

CSIRT



CTC-MSS
SOC



脅威インテリジェンス

攻撃情報照合

セキュリティ
ログ収集

サイバー攻撃分析基盤
(SIEM)

- ・セキュリティログ分析
- ・相関分析
- ・アラート検知



デバイス
エンジニア

- ・デバイス維持管理
- ・緊急時の通信遮断
- ・製品サポート連携



セキュリティ
アーキテクト

- ・高度サイバー攻撃分析
- ・分析基盤開発/メンテナンス
- ・監視ストラテジー



セキュリティ
アナリスト

- ・サイバー攻撃監視
- ・詳細ログ分析
- ・24時間365日
- ・緊急時オペレーション

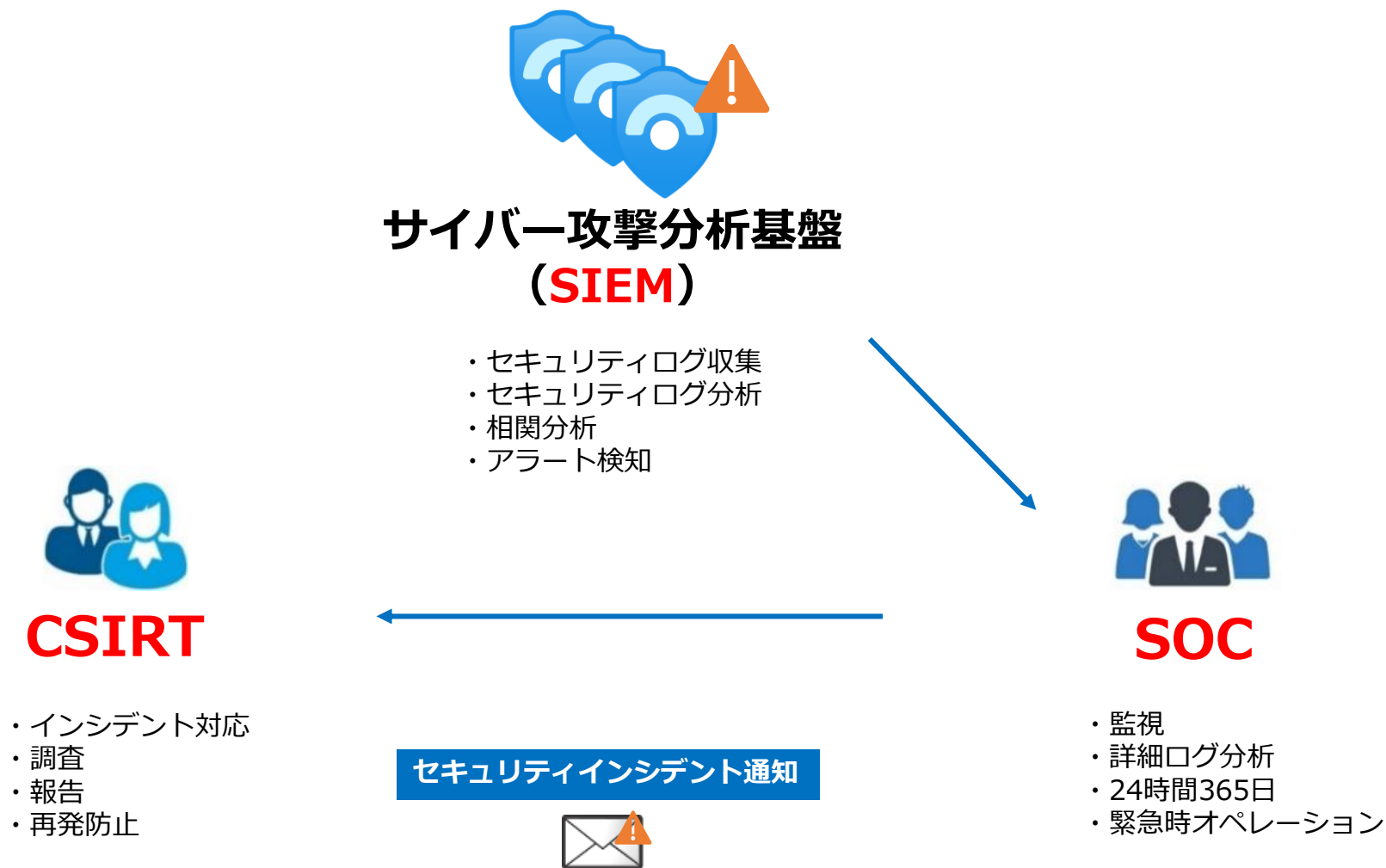
セキュリティインシデント通知



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CSIRTとSOCとSIEMの関係



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CSIRTとSOC

CSIRT

Computer Security Incident Response Team

- ・ インシデント対応の総合調整
- ・ 報告と復旧方針の策定
- ・ 関係部署との連携
- ・ 再発防止策の立案

CSIRTは組織全体の司令塔として機能します。

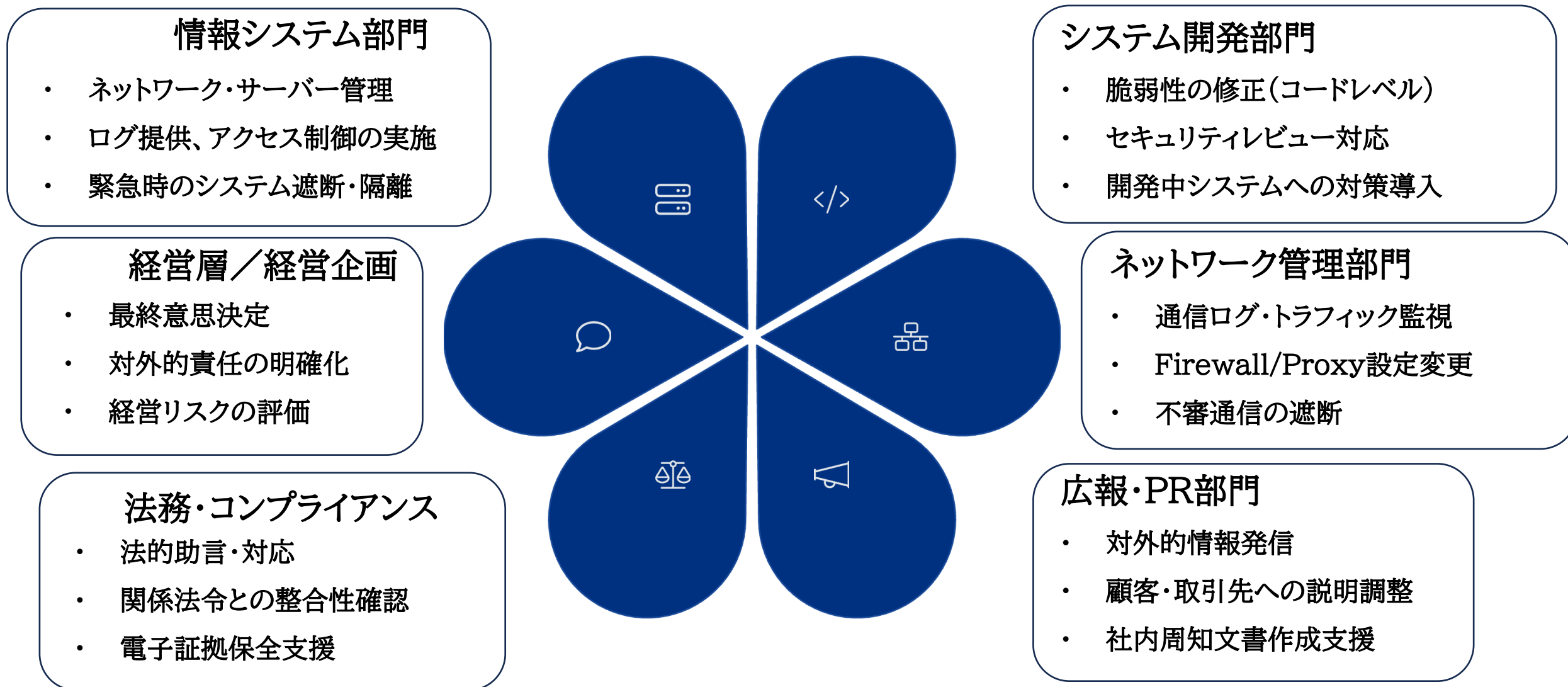
SOC

Security Operation Center

- ・ 日々のセキュリティ監視
- ・ アラートの初期分析
- ・ 脅威の検知と判断
- ・ エスカレーション

SOCは24時間365日の最前線で活動しています。

CSIRTと関連部門



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CSIRTが司令塔、SOCが最前線だとすれば上記のような組織が多方面にわたり防御に携わります。

本日のお話は



※本日のお話はサイバーセキュリティフレームワークでは「検知」～「対応」に基本的には該当します。

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

2

セキュリティ運用の一例

実際の現場での対応フロー

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

セキュリティ運用の一例（エンドポイント）

実際の運用現場がどのように動いているのか、サンプルとして下記のようなストーリーをご紹介します。

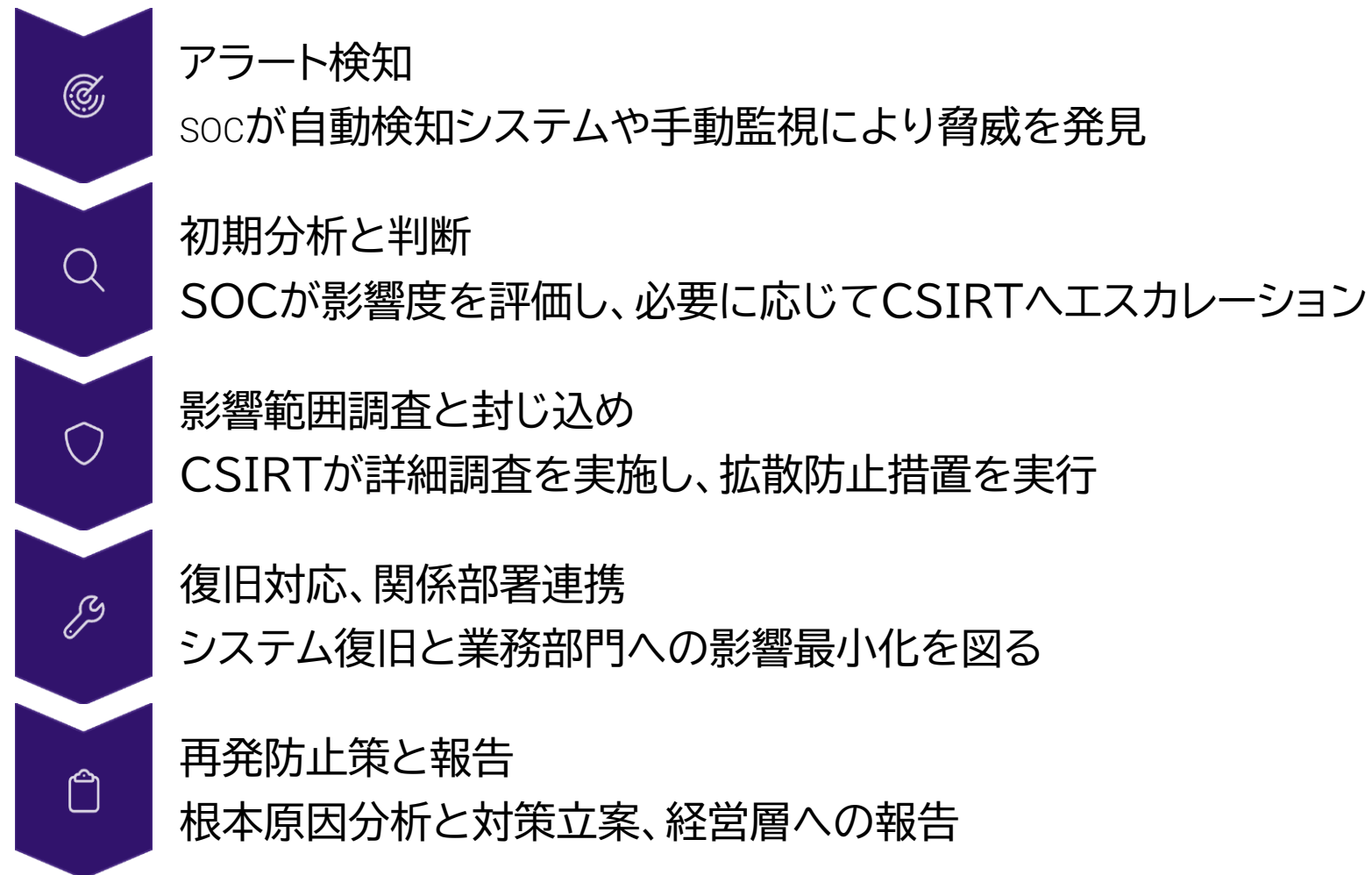
- 1 — アラート確認
 エンドポイントのログではEPP/EDRのようなアンチマルウェア製品のログが日々大量に出力されています。またエンドポイントからインターネットへの通信のログも大量にSIEMで分析されています。
- 2 — 不審通信の検知
 ある端末から国外の不審なサーバーへの通信が記録されました。C2通信の疑いがあります。
- 3 — 詳細分析
 SOCはその端末のログ、プロセス、通信先などを確認し、不審なプログラムが実行されていたことを突き止めます。
- 4 — エスカレーション
 これは”本物”のインシデントと判断され、CSIRTへエスカレーション。CSIRTはその端末を隔離し、影響範囲の調査を進めます。

こうした対応には、アラートへの反応速度と分析の精度、そして判断力が求められます。

無限の未来と、幾千のテクノロジーをつなぐ。

インシデント対応フロー

CSIRTとSOCが連携し、以下のフローでインシデントに対応します。



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

セキュリティ運用の一例（Web攻撃）

- 1 アラート確認
外部からWebサーバへの通常ではない通信を多数確認
- 2 不審通信の検知
DDoS攻撃やセキュリティスキャン関連の通信を除外し、Webサーバ内まで到達している通信を検知
- 3 詳細分析
SOCは上記情報からCSIRTへエスカレーション
CSIRTはセキュリティインシデント疑いとして関係部署と共同して調査
- 4 判断ならびに振り返り
アプリケーションサーバのログなどを分析した結果侵害が無かったことを確認
IPSやWAFを通過した状況を確認して製品ベンダーに確認
再発時の検知手段を検討してSIEM/SOCに反映

無限の未来と、幾千のテクノロジーをつなぐ。

他部署との認識・立場の違い

業務部門の視点

「サービスは止められない」

- ・ 業務継続性を重視
- ・ 利便性の確保
- ・ コスト(セキュリティ対応が追加コストになるケースも多々)

SOC/CSIRTの視点

「リスクを重く見て早急な対応を要請」

- ・ セキュリティレベルの維持
- ・ リスクの最小化
- ・ ガバナンス

⚠ このように、“業務の継続性”と“セキュリティの厳格さ”のバランスを巡って、意見が食い違うことがあります。

業務部門との認識の違いもありますが、運用部門ともやはり似たような違いが発生します。

インシデントの重大度評価や対応基準を、事前にすり合わせておくことが、運用の安定化には欠かせません。

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

3 運用改善

継続的な改善活動とAI活用

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

運用改善の取り組み

日々の運用の中で実施している改善活動についてご紹介します。

アラートチューニング

誤検知を減らし、本当に重要なアラートに集中するため、検知ルールの調整を継続的に行っています。特にSIEM製品の検知ルール最適化は重要な改善ポイントです。

手順書整備・品質向上・自動化対応

対応フローを標準化し、誰が対応しても同じ品質を確保するため、手順書やナレッジの整備に力を入れています。分析結果や判断ロジックを明文化し、属人化を防止します。また有事の際の連絡先一覧や連絡フローの最新化も重要になってきます。

無限の未来と、幾千のテクノロジーをつなぐ。

部門間の連携強化

先ほどの課題にも触れましたが、他部署との共通認識の形成は改善活動の一環として重要です。



標準化

「重大度定義」「エスカレーションルール」「報告レベル」などをドキュメント化し、全社で共有しています。



定期的な共有

セキュリティ委員会やレビュー会議で定期的に共有・更新を行い、認識を統一しています。



協調体制

これにより、緊急時にも迷わず協調して動ける体制を作ります。

部門間の連携強化により、インシデント対応の効率性と効果が向上します。
共有方法も重要です。組織が大きい場合は入社時ガイダンスのような場で取り組みを知ってもらう必要がありますし、リリースレビューのような場では必ずセキュリティ有識者も承認フローに組み込むなどのルール化も必要です。

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

最新化とAI活用への移行

脅威情報の変化に即応するため、脅威インテリジェンスの活用や、新しい攻撃手法への対応力強化も行っています。

AIアシスタントの活用

近年では、SIEM製品にAIアシスタントが搭載される動きが加速しています。

- 自然言語での質問対応
- クエリ作成の自動化
- ログ探索の効率化
- 分析業務の高速化
- アラートのトリアージ

私たちも今後、AIを活用した“AI SOC”の実現に向けて、積極的に技術習得を進めていかなければならないと感じています。

AIを有効活用するために、AIを知り、AIにシステムを知ってもらうことが重要になってくると考えています。

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

まとめ

セキュリティ運用の勘所について、現場の実践的な視点からご紹介させていただきました。

運用体制の確立

CSIRTとSOCの役割分担と連携体制の構築が基盤となります。インシデント発生時に協力を仰ぐ関係部署も巻き込むことが重要です。

継続的な改善

アラートチューニング、プレイブック整備、部門間連携の強化が重要です。部門間連携では、共通認識の醸成、相互理解の推進が重要です。

技術の進化への適応

AI活用による”AI SOC”の実現に向けた取り組みが求められています。AIのことを知る、AIに運用対象のシステムを知ってもらうことが重要になると思います。

セキュリティ運用は、技術と人、そして組織の連携によって成り立っています。皆様の組織でも、これらの勘所を参考に、より効果的なセキュリティ運用体制を構築していただければと思います。

CSIRTとSOCの関係

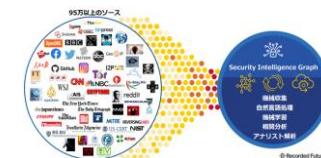
セキュリティ監視対象



調査・対処

CSIRT

CTC-MSS
SOC



脅威インテリジェンス

攻撃情報照合



サイバー攻撃分析基盤 (SIEM)

- ・セキュリティログ分析
- ・相関分析
- ・アラート検知



デバイス
エンジニア

- ・デバイス維持管理
- ・緊急時の通信遮断
- ・製品サポート連携



セキュリティ
アーキテクト

- ・高度サイバー攻撃分析
- ・分析基盤開発/メンテナンス
- ・監視ストラテジー



セキュリティ
アナリスト

- ・サイバー攻撃監視
- ・詳細ログ分析
- ・24時間365日
- ・緊急時オペレーション

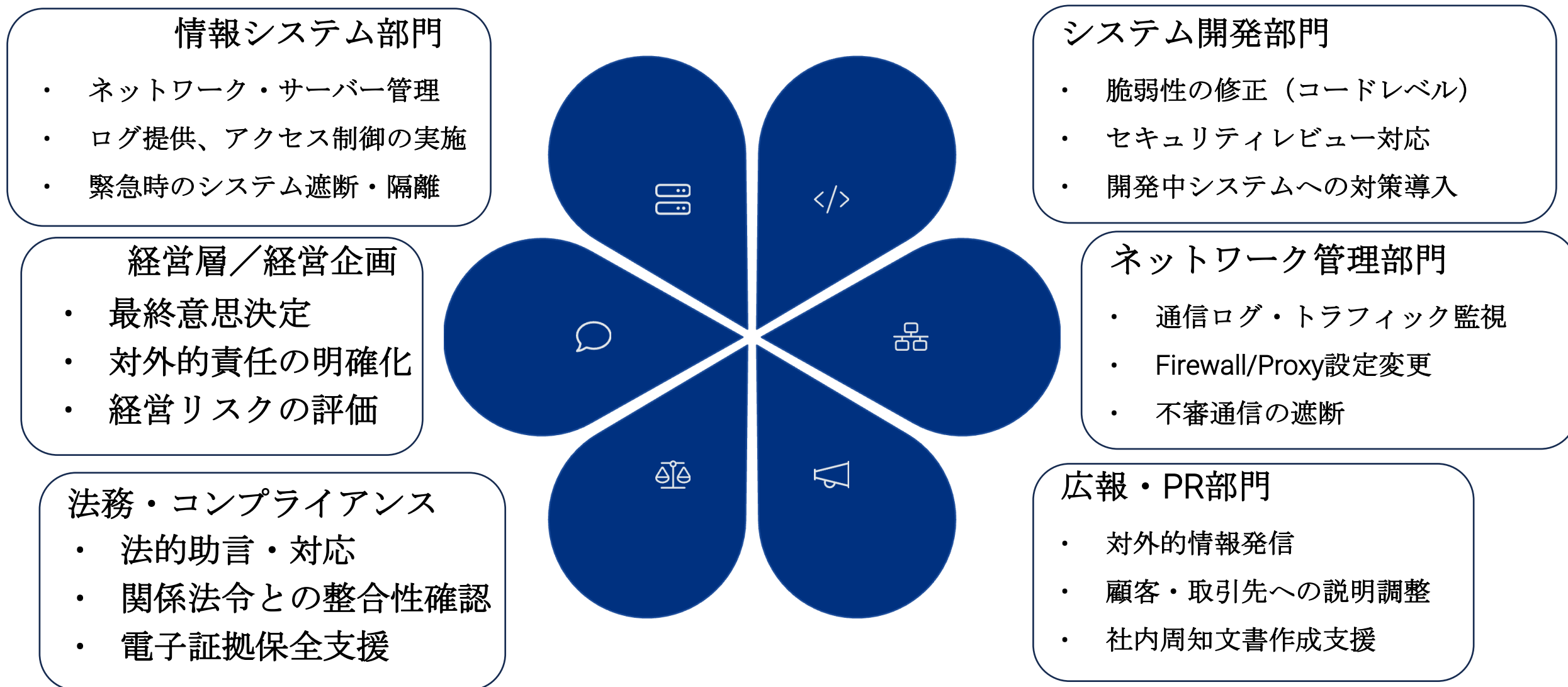
セキュリティ
ログ収集

セキュリティインシデント通知

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CSIRTと関連部門



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CSIRTが司令塔、SOCが最前線だとすれば上記のような組織が多方面にわたり防御に携わります。

まとめ

セキュリティ運用の勘所について、現場の実践的な視点からご紹介させていただきました。

運用体制の確立

CSIRTとSOCの役割分担と連携体制の構築が基盤となります。インシデント発生時に協力を仰ぐ関係部署も巻き込むことが重要です。

継続的な改善

アラートチューニング、プレイブック整備、部門間連携の強化が重要です。部門間連携では、共通認識の醸成、相互理解の推進が重要です。

技術の進化への適応

AI活用による”AI SOC”の実現に向けた取り組みが求められています。AIのことを知る、AIに運用対象のシステムを知ってもらうことが重要になると思います。

セキュリティ運用は、技術と人、そして組織の連携によって成り立っています。皆様の組織でも、これらの勘所を参考に、より効果的なセキュリティ運用体制を構築していただければと思います。

部門間の連携強化

先ほどの課題にも触れましたが、他部署との共通認識の形成は改善活動の一環として重要です。



標準化

「重大度定義」「エスカレーションルール」「報告レベル」などをドキュメント化し、全社で共有しています。



定期的な共有

セキュリティ委員会やレビュー会議で定期的に共有・更新を行い、認識を統一しています。



協調体制

これにより、緊急時にも迷わず協調して動ける体制を作ります。

部門間の連携強化により、インシデント対応の効率性と効果が向上します。

共有方法も重要です。組織が大きい場合は入社時ガイダンスのような場で取り組みを知ってもらう必要がありますし、リリースレビューのような場では必ずセキュリティ有識者も承認フローに組み込むなどのルール化も必要です。

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

まとめ

セキュリティ運用の勘所について、現場の実践的な視点からご紹介させていただきました。

運用体制の確立

CSIRTとSOCの役割分担と連携体制の構築が基盤となります。インシデント発生時に協力を仰ぐ関係部署も巻き込むことが重要です。

継続的な改善

アラートチューニング、プレイブック整備、部門間連携の強化が重要です。部門間連携では、共通認識の醸成、相互理解の推進が重要です。

技術の進化への適応

AI活用による”AI SOC”の実現に向けた取り組みが求められています。AIのことを知る、AIに運用対象のシステムを知ってもらうことが重要になると思います。

セキュリティ運用は、技術と人、そして組織の連携によって成り立っています。皆様の組織でも、これらの勘所を参考に、より効果的なセキュリティ運用体制を構築していただければと思います。

最新化とAI活用への移行

脅威情報の変化に即応するため、脅威インテリジェンスの活用や、新しい攻撃手法への対応力強化も行っています。

AIアシスタントの活用

近年では、SIEM製品にAIアシスタントが搭載される動きが加速しています。

- ・ 自然言語での質問対応
- ・ クエリ作成の自動化
- ・ ログ探索の効率化
- ・ 分析業務の高速化
- ・ アラートのトリアージ

私たちも今後、AIを活用した“AI SOC”の実現に向けて、積極的に技術習得を進めていかなければならないと感じています。

AIを有効活用するために、AIを知り、AIにシステムを知ってもらうことが重要になってくると考えています。

AI for SIEMの話でしたが、SIEM for AIというのも今後我々が考えないといけないキーワードになってくると考えています。

無限の未来と、幾千のテクノロジーをつなぐ。

まとめ

セキュリティ運用の勘所について、現場の実践的な視点からご紹介させていただきました。

運用体制の確立

CSIRTとSOCの役割分担と連携体制の構築が基盤となります。インシデント発生時に協力を仰ぐ関係部署も巻き込むことが重要です。

継続的な改善

アラートチューニング、プレイブック整備、部門間連携の強化が重要です。部門間連携では、共通認識の醸成、相互理解の推進が重要です。

技術の進化への適応

AI活用による”AI SOC”の実現に向けた取り組みが求められています。AIのことを知る、AIに運用対象のシステムを知ってもらうことが重要になると思います。

セキュリティ運用は、技術と人、そして組織の連携によって成り立っています。皆様の組織でも、これらの勘所を参考に、より効果的なセキュリティ運用体制を構築していただければと思います。

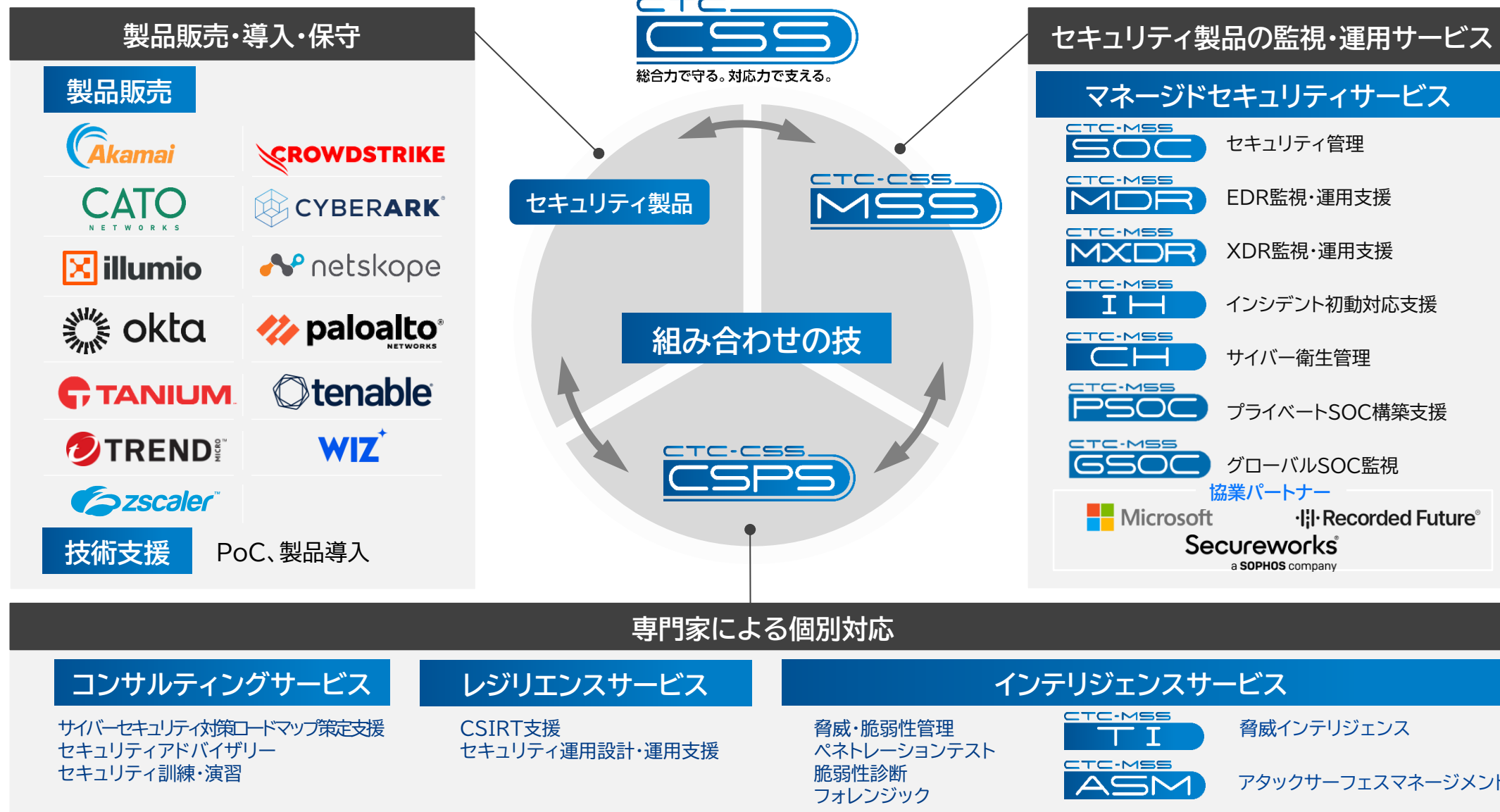
CTCサービスのご紹介



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CTC セキュリティビジネスの全体像



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

サイバーセキュリティサービス ポートフォリオ



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

ご清聴ありがとうございました



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

無限の未来と、
幾千のテクノロジーをつなぐ。

CTC Financial Services Group

