SYGNIA

# サイバーセキュリティ体制の強化

2022 SC awards EUROPE WINNER BEST SECURITY TEAM

以下を受賞しています

Gartner FORRESTER

# サイバーセキュリティ体制の強化

クライアントが深刻なセキュリティ侵害を封じ込め、修復し、自社の防御を固めることを手助けしてきたSygniaの広範囲にわたる経験は、クライアントがセキュリティ体制の大きな、短期間で成果が出る改善を実現し、自社の既存のセキュリティ投資のROIを最大化し、同時に自社の戦略的なセキュリティ上の長期目標の達成を加速できることを示しています。

Sygniaの体制強化サービスにより、クライアントは、自社のサイバーレジリエンスとサイバーリスクを大幅に軽減するための詳細な道筋を包括的に理解することができます。

## 実績のある利益

- サイバー攻撃に対する組織のレジリエンスを総合的かつ全体論的に理解する
- 現実に生じている攻撃において組織に対して使用される可能性がある攻撃ベクトルを修復することを明らかにし学ぶ
- 優先され、実用的な一連のサイバーセキュリティ強化イニシアティブを受け取る
- 既存のセキュリティ投資のROIを最大化する
- 戦略的かつ戦術的で、全社的なサイバーセキュリティの目標の達成を加速する
- 侵害とダメージのリスクを大幅に削減する

## 組織の真のサイバーセキュリティ体制を知る最速の道

Sygniaの体制強化サービスは、わずか数週間で大きなインパクトを出せるように設計されており、効率的な3つのステップからなるプロセスで行われます。

### ステップ1：発見

ステップ1は、業務とITシステムの両方を見直すことから始まります。組織の事業の背景、組織体制、重要な資産とプロセスを理解します。ITシステム、ネットワークアーキテクチャーやセキュリティスタックなどの技術環境も見直します。続いて、脅威アクターの戦術、技法と手順を模擬する、実践的かつ敵対的なシミュレーションがネットワークに適用されます。Sygniaの敵対的なシミュレーションに埋め込まれているのは、Sygniaの脅威研究グループとSygniaのインシデント対応チームから得た脅威アクターの戦術に対する最新の知見です。セキュリティシステムの構成ミス、設計の欠陥および悪用できる脆弱性が特定されます。

**Sygniaは複雑性を乗り越え、経営陣に優先される明快かつ戦略的なサイバーロードマップを提供します。**

## ステップ2：分析

ステップ2では、組織の能力をSygniaのベストプラクティスと比較の上、分析を行います。当社では、NISTやISOなどの国際規格から業界内のベストプラクティスを注意深く選び、当社の広範囲にわたる最前線での経験を有効させました。Sygniaは、組織の真の能力を評価するための、インパクトの大きい攻撃シナリオを開発しています。

このシナリオでは、敵対者が、組織に対してその目標を具現化できるであろう方法をストレステストします。組織が、各シナリオを防止、検出、対応さらに復旧できるかとその方法を特定しています。その結果は、セキュリティギャップ、強みや改善の機会などの組織の現在のセキュリティ体制の正確かつ詳細な状況を描くのに使用されます。

### 01 インフラストラクチャーとシステムのセキュリティ

| CATEGORY | STATUS |
|---|---|
| Infrastructure Management and Administration | |
| Patch Management | |
| Workstation Security | |
| Server Security | |
| Storage Infrastructure | |
| PaaS \ SaaS Security | |
| Virtualization | |
| Outsourced IT Administrative Privileged Access | |
| Helpdesk Practices | |

### 02 ネットワークセキュリティ

| CATEGORY | STATUS |
|---|---|
| Secure Network Architecture | |
| Secure Management of Network Devices | |
| Remote Access: Site to Site | |
| Remote Access: Client to Site | |
| Remote Access: Terminal Emulation | |
| Mobile Device Management | |
| Network Access Control | |
| Wireless Security | |
| Secure Internet Browsing | |

### 03 アプリケーションとサービスのセキュリティ

| CATEGORY | STATUS |
|---|---|
| Email Services | |
| Application Management and S-SDLC | |
| Business Critical Application | |
| Customer Support Practices | |

### 04 アイデンティティとアクセス管理

| CATEGORY | STATUS |
|---|---|
| Secure Privileged Identity | |
| Privileged Access Management | |
| Identity Lifecycle Management | |
| Central Identity Directory | |

### 05 データ保護

| CATEGORY | STATUS |
|---|---|
| Information and Data Security Strategy | |
| DLP | |
| DRM for Sensitive Information | |
| Disaster Recovery | |
| Backup Infrastructure | |
| Databases and Repositories | |

### 06 検出と対応

| CATEGORY | STATUS |
|---|---|
| Network Visibility | |
| Application and User Visibility | |
| Host Visibility | |
| Endpoint Investigation and Response Tool Kit | |
| Threat Intelligence | |
| Incident Management | |
| IR Organization & Competence | |

### 07 セキュリティの統治

| CATEGORY | STATUS |
|---|---|
| Security Organization in Corporate Governance | |
| Security Operating Model | |
| Strategy, Policies & Procedures | |
| Risk Management | |
| Supply Chain & 3rd Parties | |
| Asset Management | |
| Configuration & Change Management | |
| Security Assessment & Testing | |
| HR Security | |
| Business Continuity Management | |

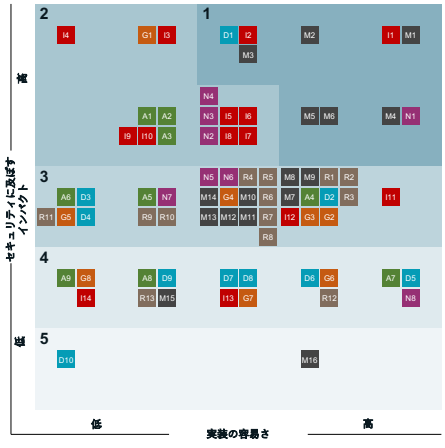
Aligned with best practices　Partially aligned　Substantial gaps

## ステップ3：戦略的および戦術的な推奨事項

ステップ3では、Sygniaは、インパクトと実装のしやすさで優先付けされた実用的なデータ解析と取り組みを開発し、統合しています。 Sygniaは、セキュリティギャップだけでなく、戦略的および技術的なレベル両方で組織が対策を講じる必要がある特定のステップを特定しています。

例えば、Sygniaは、組織の現在の強みや防御を固める機会、主要な戦略的知見、そして推奨の行動計画を備えたロードマックなどの戦略的な概要を用意しています。

Sygniaは、セキュリティチームに対して詳細かつ視覚的なギャップ分析を提供しており、ここには、組織の現在のサイバーでの強みと弱みと改善の分野が図解されています。詳細かつ優先される取り組みには、実装の成功を保証するのに必要な粒度が備わっています。検出と対応、アイデンティティとアクセス管理、データ保護、アプリケーションのセキュリティ、セキュリティの統治、ネットワークセキュリティやITインフラストラクチャーなどすべてのサイバーセキュリティの分野を対処しています。




**取り組みの柱**

- I# インフラストラクチャーとシステムのセキュリティ
- N# ネットワークとセキュリティ
- A# アプリケーションとサービスのセキュリティ
- M# アイデンティティおよびアクセス管理
- D# データ保護
- R# 検出と対応
- G# セキュリティの統治

Sygniaの推奨事項は実用的かつ合理的で、インパクト主導型です。Sygniaのアプローチは、クライアントの既存のセキュリティスタックを最適化する方法を常に第一に考えています。追加投資が必要な場合は、組織が直面するセキュリティ上の課題を幹部の方が容易に理解できるように設計された詳細なロードマップで正当化できます。

## 行動を起こすのは今なのです

サイバー防御は、多くの場合想定より実用にほど遠いものですが、攻撃者と防御者の非対称性を逆転することができます。組織は、サイバー攻撃に対する自組織のレジリエンスへの完全な明らかにするため体制の評価から始めるべきです。サイバーセキュリティ上の強みが特定され、悪用可能なギャップが明らかにされます。決定的なギャップは、攻撃者に悪用される前に直ちに埋められます。そして、組織は戦略的な体制強化ロードマップの実装へと進み、サイバーレジリエンスにおける劇的な改善を達成します。

**平均して、推奨事項の75%以上が、クライアントの既存のセキュリティスタックを活用しています**

# SYGNIAの優位性

### A-チームのみを編成

Sygniaは、広範囲にわたるサイバー戦争と企業におけるセキュリティの経歴をもつ熟練したA-チームのみを編成しています。Sygniaの広範なインデント対応と企業のセキュリティに関する経験は、前提となる防御構造とサイバー防御を最大化するのに必要な戦術など、当社の体制評価と強化の中に埋め込まれています。

### 技術的な優越

Sygniaチームは、どのようなITまたはセキュリティスタックを備えたいかなる環境下でも、クラウド、アプリケーション、CI/CD、OT、モバイル、iOTや従来型のネットワークインフラストラクチャーなどどのようなドメインでも効果的に体制を評価します。

### 実用的かつインパクト主導型

Sygniaの推奨事項は実用的かつ合理的で、インパクト主導型です。当社のチームは、クライアントの既存のセキュリティスタックの最適化を常に第一に考え、セキュリティに係る支出をできるだけ有効に使うようにしています。Sygniaは、複雑さを乗り越え、経営陣に、優先される、明快かつ戦略的なロードマップを提供します。

### SYGNIAの優位性
### 脅威研究チーム

グローバルな脅威アクターとその戦術に関する最新の研究成果は、Sygniaの敵対的シミュレーションとベンチマークに組み込まれており、堅牢な体制評価を保証します。

**Forbes**

**サイバーセキュリティデルタフォースとして広く認知されている…(Sygnia)**は、攻撃への対応速度と決断力で名声を築き、フォーチュン誌「働きがいのある会社」ランキングにランクインした企業が自社のサイバーレジリエンスを構築するのを支援しています。

# 実行中のSygniaの体制強化：ユースケース

## 戦略的な評価

Sygniaは、組織の現在のサイバー態勢を評価し、レジリエンスを強化するための戦略的なロードマップを策定し、完全な分析を行っています。

## 侵害後

Sygniaは、組織への主要なサイバー攻撃に続いて、完全な体制評価を実施し、関連する脅威の全範囲に対してクライアントのネットワークを強化するための詳細なロードマップを提供しています。

## セキュリティに係る支出の最適化

Sygniaは、体制分析を優先付けし、組織のセキュリティ予算を検証し最適化するために使用できる詳細な強化ロードマップを提供しています

## クラウドへの移行

計画されたITインフラストラクチャーのクラウドへの移行前に、Sygniaは完全なクラウドセキュリティフレームワークを提供しています。Sygniaは、クラウドへの移行に続き、クラウドのセキュリティを評価し検証します。

## ベンチマークと業界同業者の比較

現在のセキュリティ上の強みと弱みは業界のセキュリティ「フレームワークに関連して評価され、典型的な業界同業者のスコアと比較されます。

## 合併買収（M&A）

Sygniaは、買収完了前に、デューデリジェンスの不可欠な部分として、対象企業の完全な体制分析を行います。

## 規制遵守

Sygniaは、組織の既存のセキュリティ対策、コントロールと能力を規制要件と比較してチェックします。

## デジタルトランスフォーメーション

Sygniaは、組織の幅広いITエコシステム内部の重要な製品やアプリケーションのサイバーレジリエンスを評価し、固有の弱みを洗い出します。

Sygnia はサイバーコンサルティングとインシデント対応を行う会社で、世界中の組織にインパクトの大きいサービスを提供しています。Sygniaは、自社のクライアントと協力して、脅威に迅速に対応し、レジリエンスを積極的に強化します。当社の折り紙付きの実績、コミットメントと思慮分別により、Sygniaはセキュリティチーム、上級幹部、およびフォーチュン誌「働きがいのある会社」ランキングにランクインした企業を含め世界中の大手企業の取締役会の信頼を勝ち得ています。

TEMASEK　ISTARI　Temasek社およびISTARI Collectiveメンバー

## 24時間365日のインシデント対応

インシデントの疑いですか？今すぐお電話を +1-877-686-8680 | 詳細はwww.sygnia.coにアクセスしてください

SYGNIA