- ☐ Security Consulting
- ☐ Security Assessment
- ☑ Managed Security

Managed Security Service

セキュリティ監視サービス

三井物産セキュアディレクション株式会社

〒103-0013 東京都中央区日本橋人形町1丁目14番8号 JP水天宮前ビル6階
TEL : 03-5649-1961（代表）

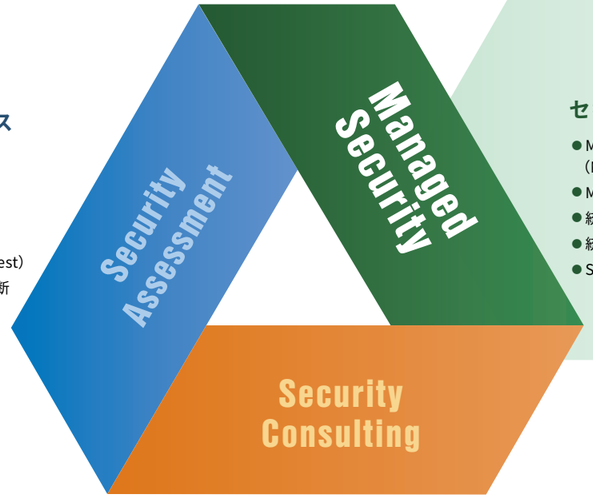
https://www.mbsd.jp/

Part No. AS11-1001-2503

24時間365日脅威を逃さない、
今求められるサイバー防御

Services

MBSDの事業は3サービスを軸として提供しています。



セキュリティ診断サービス

- Webアプリケーション診断
- ネットワーク診断
- スマホアプリ診断
- ペネトレーションテスト
- TLPT（Threat Led Penetration Test）
- AIシステムに対するセキュリティ診断
- 要塞化支援
- IoT診断
- ゲーム診断
- OT診断

セキュリティ監視サービス

- MBSD Managed Security Service（MBSD-SOC）
- Microsoftセキュリティ監視
- 統合ログ監視・Advanced SOC
- 統合ログ環境構築支援
- Security Force

セキュリティコンサルティングサービス

- リスクアセスメント
- セキュリティ組織運用支援
- サイバーBCP/BCM対策構築運用支援
- CSIRT構築・運用支援
- シンクタンクコンサルティング
- AIセキュリティ対策アドバイザリー
- その他のサービス

24時間/365日の監視を通じ、経験豊富なSOCアナリストによる常時監視体制で、迅速かつ正確な問題解決が可能

SOCアナリストが大量のアラートから重要度の高いものを抽出し検査することで、早期発見と迅速な対応を支援

長年培ったMicrosoft製品の知見を活用し、DefenderやAzure Active Directoryなどの環境全体を監視・運用サポート

この小冊子では、当社の具体的なソリューションを通じて、貴社の成長を力強く支えるための セキュリティ監視サービスをご紹介します。

MBSD Managed Security Service（MBSD-SOC）

MBSD Managed Security Service（MBSD-SOC）は、当社指定製品の監視・運用をSOCアナリストが24時間365日体制で代行し、攻撃検知時の分析から適切なオペレーションまで一元的にサポートするサービスです。SOCアナリストが大量のアラートから緊急性の高いものを抽出して通知し、有人監視やアラートログ分析、多角的なインシデント判定、危険度に応じた通知を提供します。また、監視対象デバイスやサービスの稼働状況を把握し、問題発生時には迅速な解決を支援します。

セキュリティ運用ではシグネチャの自動・手動更新やチューニング、緊急時のカスタムシグネチャ作成で最新の脅威に対応し、適切なポリシー調整によりお客様の負荷軽減を図ります。専用Webポータルでアラート状況や月次報告書を閲覧でき、アラートログは3ヶ月間保管します。さらに、オプションで月次報告書へのコメント追加やお客様のご要望に応じたカスタムシグネチャ作成、ログの保管期間延長を提供し、柔軟で高度なセキュリティ運用を実現します。

特長

多角的な解析による通知精度の向上

- MBSD-SOCは、セキュリティアナリストが「パケットペイロード解析」や「レスポンス分析」など多角的にアラート分析を行います。一般的なSOCサービスでは行っていない深堀分析により、本当に確認が必要な攻撃アラートのみを通知します。

お客様環境に合わせた対応製品の監視ポリシー最適化

- MBSD-SOCでは専門知識がないと判断の難しい誤検知判断などのポリシーチューニングも代行し、お客様環境にあわせた最適なポリシーを設定/維持します。

当社カスタムシグネチャによる攻撃検知率アップ

- MBSD-SOC独自のカスタムシグネチャによりメーカーのシグネチャだけでは検知できない攻撃にも対応します。

セキュリティアナリストによる安心の24時間365日対応

- セキュリティアナリストが24時間365日お客様のネットワークを監視します。サポート窓口（電話、メール）も24時間365日対応ですので、夜間・休日もご安心ください。

20年以上の信頼と実績

- MBSD-SOCは、2001年からセキュリティ監視サービスを提供しています。20年以上にわたってサービスを提供し続けてきた、知識と経験を基に高品質な監視サービスを実現します。

監視対象

UTM機器監視サービス対応製品

- Fortinet FortiGateシリーズ
- Palo Alto Networks PAシリーズ

IDS / IPS 監視サービス対応製品

- Trellix Network Security IPSシリーズ
- Trend Micro Deep Security

WAF 監視サービス対応製品

- F5 BIG-IP Advanced WAF
- F5 NGINX App Protect
- Cloudflare
- F5 XC WAAP

SASE 監視サービス対応製品

EDR 監視サービス対応製品

監視対象は、今後随時拡張していく予定です。

Microsoftセキュリティ監視

Microsoft関連製品監視サービスは、お客様のMicrosoftセキュリティ製品環境におけるセキュリティアラートを、MBSD-SOCの熟練したセキュリティアナリストが24時間365日体制で監視するサービスです。このサービスでは、Microsoft　Defender for Endpoint（MDE）を中心に、Defender for Identity（MDI）やAzure Active Directory（IDP）などの製品環境全体を対象に、認証やエンドポイント活動の監視を行います。

万が一の場合、端末隔離やID/パスワードのロックといった初動対応から、恒久的な対策までを提供し、柔軟かつ包括的にサポートします。また、ヘルプデスクが24時間365日体制で電話・メール対応を行い、専用Webポータルを通じてインシデント状況の閲覧が可能です。さらに、オプションサービスではアラートログ保管期間の1年間延長が利用可能で、お客様の運用負担を軽減しながら、効率的なセキュリティ管理を実現します。

Microsoft セキュリティ 監視サービス 対応製品 PRODUCTS

- **MDE監視（Microsoft Defender for Endpoint）**
  インシデントモニタリング、一次分析、緊急対処を24時間365日行い、高危険度の際には即時端末隔離を実施します。
- **MDI監視（Microsoft Defender for Identity）**
  インシデント監視と通知に加え、重大度の高い場合にはIDロックを適用します。
- **IDP監視（ID Protection / Azure Active Directory）**
  重大インシデント発生時にパスワードリセットを行い、不具合の認知時には迅速な通知を実現します。

サービス対応製品は、今後随時拡張していく予定です。

Service Details

サービス内容

	対象製品	分類	運用項目	提供時間	サービス内容
標準サービス	MDE監視（Microsoft Defender for Endpoint）	セキュリティ監視	インシデントモニタリング	24時間365日	24時間365日のセキュリティアナリストによるインシデント監視・分析
			インシデント一次分析		
			インシデント緊急対処		危険性が高いインシデントの場合は端末隔離を実施
			インシデント通知		高危険度の場合は電話・メール通知
			インシデント二次分析	平日日中帯	お客様からのお問い合わせに応じて二次分析を実施
	MDI監視（Microsoft Defender for Identity）	セキュリティ監視	インシデントモニタリング	24時間365日	24時間365日のセキュリティアナリストによるインシデント監視・分析
			インシデント分析		
			インシデント通知		
			インシデント緊急対処（IDロック）		重大度Highのインシデントの場合は、特定の条件を満たした場合にMBSD-SOCの判断で該当のIDロックを実施
	IDP監視（ID Protection / Azure Active Directory）	セキュリティ監視	インシデントモニタリング	24時間365日	24時間365日のセキュリティアナリストによるインシデント監視・分析
			インシデント分析		
			インシデント通知		
			インシデント緊急対処（PWリセット）		重大度High（またはHigh相当）のインシデントの場合は、該当のIDのPWリセットを実施
	製品の不具合対応			24時間365日	Microsoft 365 DefenderコンソールやAzureポータルへのアクセス不可、長時間に及ぶログ取得失敗など、MBSD-SOCにて不具合を認知できた場合に通知
	ヘルプデスク	お問い合わせ		24時間365日	電話・メールによるセキュリティに関する問い合わせ受付/回答
		Webポータル			インシデント検知状況を専用のWebポータルに掲載
	アラート・ログ保管			-	検知インシデントのログを3ヶ月間保
オプションサービス	月次報告書			1回/月	MDEのインシデント検知状況を月次報告書にまとめて報告
	検知アラートログ保管期間の延長（1年間）			-	検知アラートログの保管期間を延長（1年間）

特長

セキュリティアナリストの解析による通知精度の向上

- セキュリティアナリストがMicrosoft対応製品のログ分析を行い、本当に確認が必要なインシデントのみを通知します。

お客様環境に合わせたMicrosoft対応製品の設定最適化

- セキュリティアナリストがお客様環境に最適なMicrosoft対応製品の設定を行います。

緊急度が高いインシデントの端末隔離やIDロック

- 緊急度の高いインシデントを検知した場合は、セキュリティアナリストが24時間365日体制で端末隔離やIDロックなどを行います。

セキュリティアナリストによる安心の24時間365日対応

- セキュリティアナリストが24時間365日お客様のネットワークを監視します。サポート窓口（電話、メール）も24時間365日対応ですので、夜間・休日もご安心ください。

20年以上の信頼と実績

- MBSD-SOCは、2001年からセキュリティ監視サービスを提供しています。20年以上にわたってサービスを提供し続けてきた、知識と経験を基に高品質な監視サービスを実現しています。

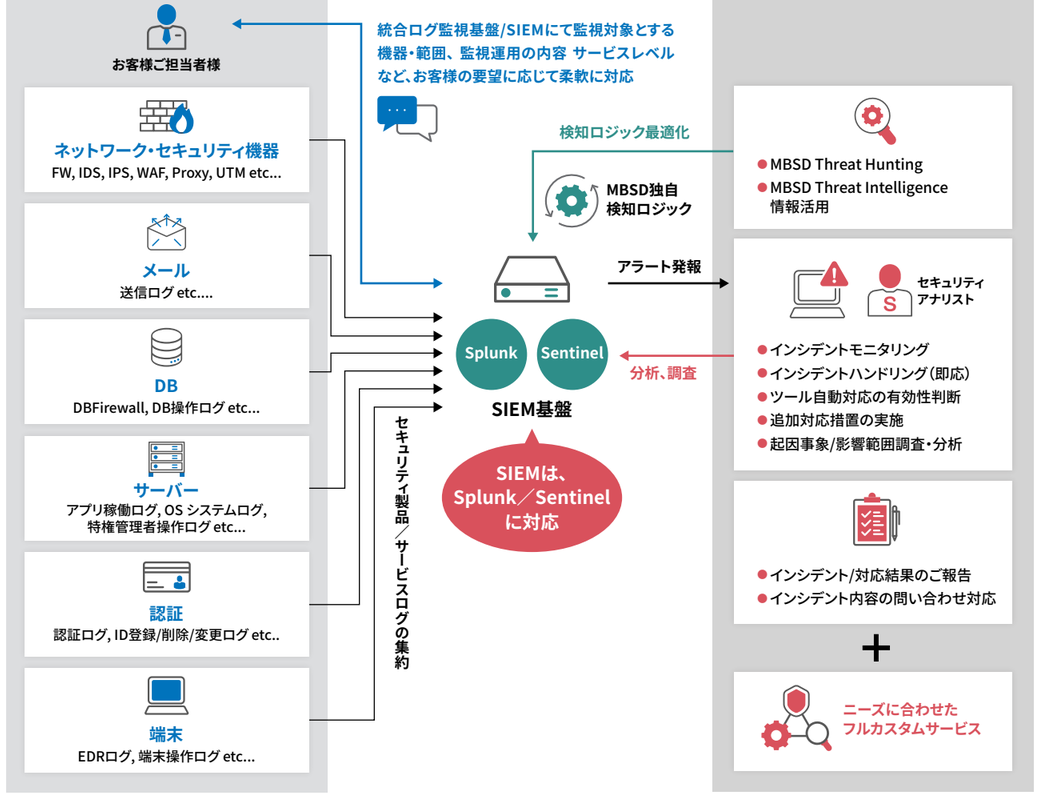
統合ログ監視・Advanced SOC

統合ログ監視・Advanced SOC（ASOC）サービスは、ご利用中のシステムのログやセキュリティ製品・サービスからのアラート情報をお客様専用の情報分析基盤（SIEM）に集約し、経験豊富なセキュリティアナリストが24時間365日体制で監視を行うサービスです。本サービスは、お客様のニーズに応じたフルカスタム対応が可能で、監視対象や範囲、運用内容・サービスレベルの柔軟な調整に加え、可視化や特定の事象検知を目的とした独自の検知・分析ルールの作成・加工にも対応しています。

また、情報分析基盤で集約したデータを加工し、お客様が必要とする情報を一目で確認できるカスタムダッシュボードの作成・提供が可能です。さらに、重大インシデント発生時のインシデントレスポンスサービスなど、複数のサービスを組み合わせたワンストップのパッケージ提供も行っており、包括的なセキュリティ支援を提供します。

Service Details

サービス内容



特長

お客様ニーズに合わせたフルカスタム

- 監視対象とする機器・範囲、監視運用の内容・サービスレベルなど、お客様の要望に応じて柔軟に対応します。

検知・分析ルールの作成/加工

- 可視（見える）化や、発見（検知）したい事象など、目的等に応じ、その実現のため、独自の検知・分析ルールの作成のご相談を承ります。

カスタムダッシュボードの作成・提供

- 情報分析基盤に集約した情報を加工し、お客様が知りたい情報を一目で確認可能なダッシュボードの作成、提供が可能です。

ワンストップ提供

- 万が一、重大インシデントが発生した場合におけるインシデントレスポンスサービスなど当社の複数サービスを組み合わせたパッケージ提供も可能です。

Service Delivery Process

サービス提供フロー

統合ログ環境構築支援

統合ログ導入コンサルティング・環境構築支援サービスは、自社のログやセキュリティ製品・サービスから発生するアラート情報をSIEM（Security Information and Event Management）に統合し、セキュリティ耐性向上や監視合理化を目指すお客様向けのプロフェッショナルサービスです。

複数のセキュリティ製品やアプリケーションから得られるログやアラートを効果的に管理・分析するために、導入前の検討・準備からSIEM基盤の構築・運用までを支援します。SIEM導入の方針は決まっているが進め方が不明な場合や、既に導入済みでも活用が不十分な場合、MBSDのコンサルタントが課題や環境を丁寧にヒアリングし、統合ログ環境により実現したい将来像への到達をサポートします。

Service Details
サービス内容

- 何から手を付けてよいか解らない
- 専門家のアドバイスが欲しい
- 当社のベストプラクティス提案が欲しい

【統合ログ導入コンサルティング】サービスで全体をサポート

- 収集対象のログ整理は済んでいる
- とりあえずSIEMを入れてみたけど利活用ができていない

【統合ログ環境構築支援】サービスで要件定義から設計・構築完了までをサポート

- 現状把握
- 必要なログ情報の整理
- 製品選定支援
- PoC支援

要件定義	設計・構築
お客様ヒアリング	基本・詳細設計
要件定義	基盤構築・ログ取込
	システム・運用テスト

特長

統合ログ導入 コンサルティングサービス

- SIEMの導入方針は決まったものの、どんなログを集めればやりたいことが実現できるのかわからない場合でもMBSDのコンサルタントにお任せいただければ、ヒアリングを通してお客様のイメージを具現化し、必要なプロセスの洗い出しと実現をサポートさせていただきます。

統合ログ環境構築 支援サービス

- 統合ログ環境の構築に必要なステップの策定から構築までをワンストップでご支援します。

Service Delivery Process
サービス提供フロー

ご提案～ご成約 → **サービス提供**

初回お打合わせ	ヒアリング	ご要望と提案内容のすり合わせ	全体提案と合意形成	ご支援開始
●背景/課題ヒアリング ●解決・実現したいゴールイメージ ●スケジュール感 ●ご予算	●NDAの締結 ●QAディスカッション ●ヒアリング ・ご要望や課題 ・構成概要	●提案素案提示 ●ご要望・スケジュール ・ご予算等のすり合わせ	●正式提案書のご提出 ●正式御見積書のご提示 ●全体提案への合意 ●ご成約	

Security Force

“Security Force”は当社が有するセキュリティスペシャリスト/アナリストチームです。長年セキュリティリスクに立ち向かってきた経験と、セキュリティ専門家としての知見を基に、様々なセキュリティインシデントに関するご相談や解析をサポートいたします。

当社が長年にわたり培ってきたセキュリティリスクに対する知見のすべてを活用し、お客様に降りかかるあらゆるセキュリティリスク、インシデントに対して、最適なセキュリティ人材リソースを提供いたします。インシデントが発生してしまった際の対応支援はもちろん、APT（Advanced Persistent Threat）による攻撃予告対策や、マルウェアによる暗号化被害など、さまざまな状況に対応可能なスペシャリスト人材のアウトソースサービスです。

※「Security Force」は三井物産セキュアディレクション株式会社の商標登録です。

01 インシデント対応支援 SERVICE

インシデント対応支援サービスは、ランサムウェア感染、Web改ざん等のサイバー攻撃被害が発生した際や、被害が懸念される場合に、セキュリティスペシャリスト/アナリスト（Security Force）が、初動対応の支援や原因調査を実施するサービスです。
当社が培ってきたセキュリティ対策のノウハウとセキュリティスペシャリスト/アナリストによって管理、遂行される最高品質のインシデント対応により迅速な問題解決をご提供いたします。
サービスはお客様からの申告を基にスタートさせていただき、状況のヒアリングを含め、調査のスコープを確定させていただくところから、実際の調査作業、最終結果のご報告、恒久対策のアドバイスまで、一連のインシデント対応フローをワンストップでご提供可能なサービスです。

特長

対象機器や環境に制限を設けないサービス提供体制

- 調査対象を特定のサービスや、機器、環境等に限定する事なく、どのような環境でもサービスを提供可能です。

経験豊富なセキュリティスペシャリスト/アナリストによる作業

- 様々なインシデントと現場を経験してきたセキュリティスペシャリスト/アナリストがインシデントの内容、状況に即した対応方法をスピーディに検討し、実施内容をご提案します。

柔軟な調査範囲

- 調査期間は、インシデントの内容・進行の度合い、セキュリティ対策の実施状況、調査可能なログや保全データのサイズにも依存しますが、早期の報告の必要性が高いケースなどでは、想定される攻撃シナリオに応じて調査対象を絞った調査を行い、短期間での結果見通しをご提示する等の柔軟な調査計画を立てることが可能です。

02 不正トランザクション検知 SERVICE

不正トランザクション検知（機械学習・AIモデル構築支援）サービスは、お客様環境で収集された大量のデータ（ログ情報やネットワークトラフィック情報、センサー情報等）を、機械学習モデルを活用し解析することにより、これまで見つけることができなかった脅威を発見、検知することを目的としたテクニカルコンサルティングサービスです。
当社のSecurity Force（セキュリティスペシャリスト/アナリスト）が、お客様の持つ大量かつ多様なデータを分析し、お客様が抱えた課題（問題の発見や異常の検知）解決のために必要なアルゴリズムや、機械学習（Machine Learning）モデルの構築を支援します。
既存のセキュリティ製品やサービスではこれまで発見することができなかった、お客様ビジネスやサービス特有のビジネスロジック問題に対してアプローチすることで、セキュリティリスクの高い事象の発見や異常な振る舞いをリアルタイムで検知し、セキュリティ上のリスクを軽減することが可能になります。

特長

ビッグデータ解析技術とサイバーセキュリティ技術・知見の融合

- 決済情報等の大量なビジネスロジックログを使ったビッグデータ解析技術/機械学習アルゴリズム
- ネットワークログ分析、認証ログ分析等のサイバーセキュリティ分析の技術
- IoA/IoC等のThreat IntelligenceやDarkweb情報等に代表されるサイバーセキュリティ情報

などを、多角的なアプローチを組み合わせ、高度な不正検知の仕組みを提供します。

お客様向け完全オリジナル実装

- 独自のRating技術を実装するなど、お客様のサービス/システムに即した、完全オリジナルの検知システムを実装・構築することが可能です。

多様な導入実績

- 大手オンライン決済サービスの不正決済検知フィードバックループへの実装や、大手ポイントサイトでの不正利用検知など、継続的なサービスの性能改善にご活用いただいている実績もあり、確かな品質のサービスが提供可能です。

Security Force

03 ダークウェブ モニタリング SERVICE

各企業が保有するシステムやWebサイトの脆弱性や、アクセスに必要なID/パスワード（クレデンシャル）の漏えい有無について、当社はダークウェブ上の情報を監視します。当社独自ツールを含む複数の手法を活用し、ダークウェブを含むウェブ上から脅威情報（脆弱性情報やクレデンシャル情報など）を監視し、発見時には迅速に通知を行います。
ダークウェブ監視にはノイズが多く含まれるため、当社の専門監視チームが情報を精査し、適切な情報のみをお客様に通知します。また、ご要望に応じて、お客様のIT部門向けにダークウェブモニタリングツールのインターフェースへのアクセスを提供し、直接モニタリングや調査を行うことも可能です。

当社のセキュリティアナリストは豊富な脅威情報の調査・分析経験を基に、重要な情報をモニタリングし、漏えい情報が見つかった場合にはその詳細を調査して報告します。事前に対象となる企業名やサービス名のリストを受け取り、これに基づいて定常的な監視を行うほか、短期（1～3か月）のプロジェクトとして情報漏えいチェックを実施することも可能です。
このサービスは、お客様のセキュリティ体制を強化し、漏えいリスクの早期発見と対応を支援します。