ソリューションカタログ

Sophos Security Services Retainer

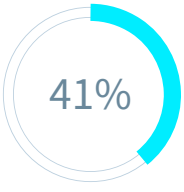
先を見越した準備と、確実なデジタルフォレンジックおよびインシデント対応 (DFIR) により、防御を強化し、リスクを低減します。

Sophos Security Services Retainer は、リスクを低減し、レジリエンスを強化する予防的なセキュリティサービスを提供します。また、攻撃が発生した場合でも、DFIR を迅速に利用できるようにします。

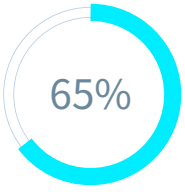
現代の脅威には、より強固なサイバーレジリエンスが求められている

多くの組織は、攻撃を受ける前にセキュリティポスチャを強化し、インシデントが発生した際に効果的に対応することに苦慮しています。AI によって高度化および高速化する脅威への対策には継続的な備えが不可欠です。しかし、セキュリティチームは日常的な運用業務に追われており、十分な対応体制を維持することが困難になっています。燃え尽き症候群や時間の制約により、先を見越した計画策定やインシデントへの備えを継続的に維持することは容易ではなく、その結果、攻撃を受ける隙が生じる可能性があります。サイバー攻撃者による行動は、多くの場合、通常の業務時間外に発生します。そのような状況では、セキュリティチームは迅速な対応を迫られますが、攻撃の封じ込めや排除に必要な情報やリソースが十分に揃っていないことも少なくありません。脅威の高度化や AI を悪用した攻撃の増加が進むなか、絶え間ない業務負荷に対応しながら、インシデントへの備えと対応のための能力を維持することが大きな課題となっています。

数字が示す事実

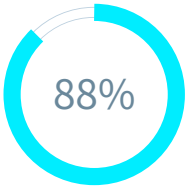


燃え尽き症候群により組織のレジリエンスが低下したと報告した IT 専門家およびサイバーセキュリティの専門家の割合。[1]



既知または未知のセキュリティ上の脆弱性が原因で、ランサムウェア攻撃の被害を受けたことを報告した組織の割合。[2]

Sophos DFIR チームが調査した事例における、攻撃者の滞留時間の全体的な中央値。[3]



営業時間外に展開されたランサムウェアのペイロードの割合。[4]

特長

- 予防的なサービスを活用して防御の弱点を特定し、**サイバーレジリエンスを強化します。**
- 侵害が発生した場合、脅威を評価、阻止、無力化するための**専門的な DFIR を確実に実行できるようにします。**
- 世界最高クラスのセキュリティテスターやインシデント対応者の支援によって、**社内のリソースを拡充します。**
- 固定料金で利用できるテストサービスを定期的に実施することで、**予防的なセキュリティ運用へ移行し**、セキュリティ体制の成熟度の向上とサイバーレジリエンスの強化を図ります。
- 規制当局による監査の前に、テストを通じて問題を洗い出し、**コンプライアンス対策を強化します。**
- より強固な防御体制とオンコールの DFIR により、**サイバー保険の契約条件を改善します。**

Sophos Security Services Retainer

Sophos Security Services Retainer は、予防的なサービス、プロフェッショナルサービス、DFIR サポートを、利用しやすい単一のサブスクリプションに統合したものです。柔軟なサービスユニットモデルを通じて、組織はテスト、アセスメント、インシデント対応準備、各種プロフェッショナルサービスを優先度に応じて計画的に利用できます。これにより、脆弱性や運用上の課題を明らかにし、セキュリティ防御を強化できます。

インシデント発生時には、このリテーナー契約により、経験豊富な DFIR 専門家への迅速なアクセス、事前に定義されたインシデント対応の SLA、事前に交渉および割引された緊急対応の時間単価が適用され、対応の遅れや不確実性を排除します。これにより、サイバーセキュリティに対するバランスの取れたアプローチを実現でき、攻撃への備えを整えるとともに、インシデント発生時には最も必要とされるタイミングで、安心感、明確性、専門家による支援を提供を得ることができます。

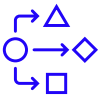
リテーナーに含まれるサービス

レベル / カテゴリ	レベル 1	レベル 2	レベル 3	レベル 4
含まれるサービスユニット (SU) の数	2	15	35	65
SU の追加購入	可	可	可	可
SU から DFIR の作業時間への変換	不可	可	可	可
DFIR 作業時間の追加購入	可	可 (事前に交渉された割引料金)	可 (事前に交渉された割引料金)	可 (事前に交渉された割引料金)
DFIR リテーナーを組み込み	いいえ	はい	はい	はい
テクニカルサポートの優先対応	はい	はい	はい	はい
プロフェッショナルサービスコミュニティへのアクセス	はい	はい	はい	はい
サービス連携担当	いいえ	いいえ	はい	はい
経営幹部向け年次ブリーフィング *	いいえ	いいえ	はい	はい
年次パスワードクラッキング演習 *	いいえ	いいえ	いいえ	はい

^ レベル 1 のお客様は、スタンドアロンの DFIR リテーナーを購入できます。このリテーナーでは、DFIR に対する SLA の保証と Sophos DFIR の作業時間について事前に交渉および合意済みの割引料金を受けることができ、予防的なサービス向けのサービスユニットを購入できます。

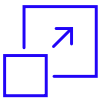
* リクエストに応じて提供

Sophos Security Services Retainer の内容



プリペイド型サービスユニットによる運用の柔軟性
各リテーナーレベルには、予防的サービスとプロフェッショナルサービスとの引き換えに利用できる一定数のサービスユニットが含まれています。これにより、年間を通じてサービスの利用計画を立てることができ、組織は自社のニーズを満たし、レジリエンスを強化できます。必要に応じて、サービスユニットを Sophos DFIR の作業時間に変換することも可能です。

予防的なサービスおよびプロフェッショナルサービスへの広範なアクセス。
テスト、アセスメントなどの専門家主導のサービス提供など、予防的なサービスとプロフェッショナルサービスの包括的なカタログにアクセスできます。カタログに掲載されている各サービスは明確に定義されており、それぞれにサービスユニット数が設定されています。



SLA が保証された DFIR リテーナーを標準提供。
上位レベルには、初動対応およびエンゲージメント開始に対する SLA が保証された DFIR リテーナーが含まれます。また、Sophos DFIR の追加時間については、
事前に交渉された割引料金が適用されるため、重大なセキュリティインシデント発生時のコストに関する不確実性を軽減できます。

世界最高クラスのセキュリティ専門知識へのアクセス。
本サービスは、経験豊富なセキュリティテスター、プロフェッショナルサービスコンサルタント、DFIR の専門家によって提供されます。これらの専門家は、新たな攻撃者の行動やセキュリティのベストプラクティスについて、実務に基づいた深い知識と洞察を備えています。このチームは、Sophos X-Ops の脅威リサーチャー、脅威ハンター、セキュリティアナリストによって支えられています。

セキュリティライフサイクル全体に対応
Security Services Retainer は、予防的なサービス、プロフェッショナルサービス、DFIR サービスを 1 つのサブスクリプションに統合しており、簡単に購入して利用できます。組織は、複数のリテーナーや契約を個別に管理する負担をかけることなく、攻撃への備え、予防、対応にわたって、グローバルなセキュリティリーダーの包括的な能力を活用できます。

サービスユニットの使用方法は以下が含まれます。

- 外部侵入テスト
- 内部侵入テスト
- ワイヤレスネットワーク侵入テスト（本サービスは日本では提供していません）
- Web アプリケーションセキュリティアセスメント
- セキュリティポスチャの評価
- 机上訓練
- Sophos Endpoint、Sophos XDR、Sophos MDR の導入
- Sophos Firewall の導入
- Sophos MDR オンボーディング支援
- 詳細なオプション一覧については、サービスカタログ を参照してください。

計画、準備、対応をもっとスマートに

現代の脅威に対処するには、個別のサービスや断片的なリテーナー契約だけでは不十分です。Security Services Retainer は、先を見越した準備と Rapid Response を単一のサブスクリプションに統合しており、組織がセキュリティポスチャの計画、優先順位付け、および継続的な強化を柔軟に進めることができるように支援します。

プリペイド型のサービスユニット、専門家主導のサービスへの広範なアクセス、DFIR の保証により、このセキュリティサービスリテーナーは、事前の準備からインシデント発生後の対応に至るまで、あらゆる局面における不確実性を解消します。ソフォスと連携することで、複雑化し、予測困難さを増す脅威環境の中で、リスクの低減、レジリエンスの強化、そして迅速かつ確実な対応を実現することが可能になります。

業界からの評価

ソフォスはセキュリティテストにおいて認定されており、その技術力、プロセス、ガバナンスが検証されています。

英国国立サイバーセキュリティセンター (NCSC) より、CIR インシデント対応サービスプロバイダーとして認定されており、CIR Enhanced および CIR Standard の両方の認定を取得。

DEFCON Wireless Capture the Flag において 3 年連続で優勝 (ソフォスのテスターは現在、このコンペティションの運営にも参画しています)。

ドイツ連邦情報セキュリティ庁より、インシデント対応業務における信頼できるパートナーとして認定。

Sophos Red Team のメンバーが持つ幅広い専門知識を示す認定資格。

日本の経済産業省より、サービスの信頼性および運用成熟度に関する基準を満たしているとして認定。

詳細については、https://www.sophos.com/ja-jp/services/security-services-retainer を参照してください。

1 - ソフォス：サイバー脅威への警戒がもたらす人への負荷：サイバーセキュリティの燃え尽き症候群への対処 2025 年版
2 - ランサムウェアの現状 2025 年版 - ソフォス
3 - Sophos アクティブアドバーサリーレポート 2026 年版
4 - Sophos アクティブアドバーサリーレポート 2026 年版

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2026-06-15 BR-JA (MP)