「サイバー攻撃対策ソリューション」の主な取り扱い製品・サービス

コンサルティング	
CSIRT構築支援	CSIRT構築支援サービス
ログ分析シナリオ策定支援	ログ分析シナリオ策定支援サービス
現状分析	サイバー攻撃現状分析サービス
	標的型攻撃対策評価サービス ～レッドチームによる評価～
教育・訓練	標的型メール訓練サービス
	サイバーインシデント対応演習サービス
システム構築	
マルウェア対策・ランサムウェア対策	次世代マルウェア対策製品 CylancePROTECT
	次世代エンドポイントセキュリティ製品 パロアルトネットワークス Traps
	マルウェア対策アプライアンス FireEye
	Trend Micro Deep Discovery Inspector
	Web分離・無害化ソリューション Menlo Security Web Isolation Service
	ホワイトリスト型マルウェア対策 McAfee Application Control
標的型攻撃対策・不正アクセス対策	次世代ファイアウォール パロアルトネットワークス PAシリーズ
	次世代ファイアウォール Juniper Networks SRXシリーズ
	UTMアプライアンス Fortinet FortiGateシリーズ
	Webアプリケーションファイアウォール SecureSphere
	SaaS型WAF/DDoS対策 Imperva Incapsula
	DNS/DHCPアプライアンス Infobloxシリーズ
	秘文 Data Encryption/秘文 Device Control
	拡散活動検知ソフトウェア
	活文 メールゲートウェイ
	Blue Coat シリーズ
脆弱性対策	セキュリティ診断サービス
	Trend Micro Deep Security
	オープンソースの脆弱性対策ソリューション Black Duck Hub
DDoS攻撃対策	次世代型DDoS防御専用アプライアンス A10 Networks Thunder TPS
パスワードリスト攻撃対策・不正送金対策	認証強化ソリューション Entrust IdentityGuard
	指静脈認証システム 静紋
ログ分析	SIEMアプライアンス McAfee SIEM
	マシンデータ利活用基盤ソリューション Splunk
	サイバー攻撃分析サービス
運用支援	
CSIRT運用支援	CSIRT関連サービス
	ログ分析レポート
	マルウェア感染調査サービス
不正アクセス監視	マルウェア監視サービス
	DDoS監視サービス
インシデント対応	セキュリティインシデント緊急対応サービス
	セキュリティエキスパートサービス

詳細はホームページをご覧ください。http://www.hitachi-solutions.co.jp/cybersecurity/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/cybersecurity/

S15K-19-06 | 2018.04

HITACHI
Inspire the Next

サイバー攻撃対策ソリューション

株式会社 日立ソリューションズ

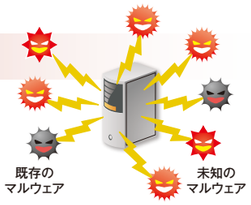
多様化するサイバー攻撃への悩みや課題を コンサルティングからシステム運用・監視までトータルにサポートします。

サイバー攻撃は、日々、高度化、巧妙化しており、単一の対策では防ぐことが難しくなってきています。
日立ソリューションズの「サイバー攻撃対策ソリューション」は
標的型攻撃、マルウェア、DDoS※1攻撃に加え、リスト型攻撃、オンライン不正送金などの
最新のサイバー攻撃に有効な対策を複合的に組み合わせた最適なソリューションを提供します。

課題　多種多様化するサイバー攻撃に対して、企業のセキュリティ対策の見直しが急務です

最新のサイバー攻撃への対策ができていない

- 未知の脆弱性やマルウェアにどう対策したらよいかわからない
- ファイアウォールやIPS※2だけでは、ネットワークセキュリティとして大丈夫か不安



サイバー攻撃に対して、組織的な取り組みができていない

- セキュリティインシデントに対応する組織を作りたい
- 社員のセキュリティ意識を向上させたい

何から対策をしたらよいのかわからない

- セキュリティは強化したいが、何から対策をしたらよいのかわからない
- 現状の対策状況を把握し、不足点を洗い出したい

対策のポイント　最新のサイバー攻撃に有効な対策を複合的に組み合わせて提案します

Point 1　多層防御での対策

単一の製品導入による対策ではなく、複数のセキュリティ対策を組み合わせることで、強固なセキュリティ対策を実施

Point 2　侵入されることを前提にした対策

攻撃の被害を最小限にするために、防御だけでなく、検知、分析、対処までのトータルな対応が重要

Point 3　新たな脅威への継続的な対策

定期的に対策状況の見直しを実施し、新たな脅威への対策を継続的に実施

※1 Distributed Denial Of Service：複数の中継コンピュータから一斉にパケットを送信し、サーバーへ負荷を与え、サービスを低下させることを目的とした攻撃　※2 Intrusion Prevention System：侵入防止システム　※3 Computer Security Incident Response Team：コンピュータやネットワーク上におけるセキュリティ攻撃や脅威に対処する組織　※4 Security Information and Event Management：サーバーやネットワーク機器、セキュリティ関連機器、各種アプリケーションから集められたログ情報に基づいて、異常があった場合に管理者に通知したり、その対策方法を知らせたりする仕組み

ソリューションの特長

計画からシステム設計・構築、運用・監視まで、トータルに対応

お客様に最も有効な施策は何かをコンサルティングするサービスから、対策システムの設計・構築、運用・監視まで、トータルに提案します。

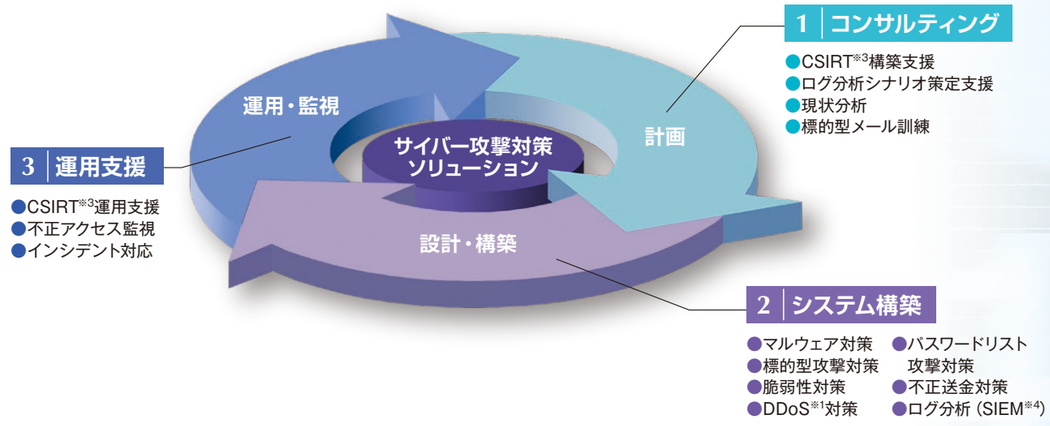
特定の製品ではなく、お客様に最適な製品・解決策を提案

お客様の現在の業務内容やセキュリティ対策状況、守るべき重要情報の内容、予算を考慮し、最適なセキュリティ対策を実現します。

従来のセキュリティ対策では防ぎきれない最新のサイバー攻撃に対応

高度化するマルウェアやDDoS※1攻撃など、あらゆるサイバー攻撃に対する最適なソリューションを提供し、セキュリティリスクを低減します。

ソリューションの体系と概要



計画
1 コンサルティング

サイバー攻撃対策コンサルティングは、日立グループでのノウハウ・知見を活用したCSIRT※3構築支援から、SIEM※4導入における分析シナリオの策定支援、マルウェアの感染調査まで、お客様のサイバー攻撃対策における現状の課題を明確にし、マネジメントとシステムの両面でセキュリティ強化を支援します。

設計・構築
2 システム構築

サイバー攻撃対策システム構築支援サービスは、お客様の運用体制、リソース等、お客様の実情に合った最適なシステムを提案し、構築を支援します。高度化するマルウェアや標的型攻撃、DDoS※1攻撃などに対応するため、様々な製品・サービスを組み合わせた最適なソリューションを提供します。

運用・監視
3 運用支援

サイバー攻撃対策運用支援サービスは、CSIRT※3運用に必要な脆弱性情報の提供や不正アクセス監視によるサイバー攻撃の可視化からインシデント発生時の調査、復旧対応まで、日々のサイバー攻撃対策の運用を幅広く支援します。