主な取り扱い製品・サービス

Plan	
BCPコンサルティング	サイバー攻撃対応BCP策定コンサルティング
	CSIRT構築支援サービス
	CSIRT構築・運用支援サービス
	CSIRT要員基本教育
リスク分析	サイバー/制御現状分析サービス
	SHIELD セキュリティコンサルティングサービス
Do	
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 パロアルトネットワークス Traps
	拡散活動検知ソフトウェア
	標的型攻撃対策ソフトウェア FFRI yarai
	秘文 Data Encryption
	Trend Micro Deep Security
	McAfee Application Control
	産業用PC向けセキュリティ 制御向け yarai
	デコイサーバー
Web改ざん防止	Tripwire Enterprise IT変更管理ソリューション
	Trend Micro Deep Security
	フィッシング・不正送金対策 PhishWallシリーズ
	Webアプリケーションファイアウォール SecureSphere
	SiteGuard
	SaaS型WAF/DDoS対策 Imperva Incapsula
	SecureBrain Web改ざんチェックGRED
DoS/DDoS 攻撃対策	高速ロードバランサー A10 Networks Thunder/AXシリーズ
	DefensePro
	SaaS型WAF/DDoS対策 Imperva Incapsula
	Akamai
標的型攻撃対策	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
	マルウェア対策アプライアンス FireEye
	標的型サイバー攻撃対策システム Trend Micro Deep Discovery Inspector
	サンドボックス製品 Fortinet FortiSandbox
	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
	McAfee Network Security Platform
	Blue Coatシリーズ
	InterSafe
	i-FILTER
	DNS/DHCPアプライアンス Infobloxシリーズ
	SHIELD Webセキュリティ・オンデマンドサービス BlueCoatクラウドサービス
	ウェブ分離・無害化ソリューション Menlo Security Web Isolation Service
	活文 メールゲートウェイ
	SandBlast
	m-FILTER
	IronPort
	GUARDIANWALL
	SHIELD メールセキュリティ・オンデマンドサービス
	Application Container Platform
運用・監視	SHIELD マネージドセキュリティサービス
	SHIELD セキュリティリスク管理サービス
予兆検知	マシンデータ利活用基盤ソリューション Splunk
	McAfee SIEM
	IBM Qradar
	統合セキュリティログ分析システム ArcSight
	ファイルサーバ専用アクセスログ収集システム VISUACT
	拡散活動検知ソフトウェア
	標的型サイバー攻撃対策システム Trend Micro Deep Discovery Inspector
Incident対応	
緊急対応	SHIELD リモートインシデント対応支援サービス
	FalconStor社製品利用 ディザスタリカバリソリューション
バックアップ対策	レプリケーション&フェイルオーバーソフトウェア Double-Take
	大規模クライアント・バックアップソリューション HPE Connected Backup
	JP1/VERITAS
	バックアップ統合化ソリューション CommVault Simpana
	安心バックアップサービス
原因分析	サイバー攻撃分析サービス
	マルウェア感染追跡ソフトウェア Cisco AMP
	Cybereason
復旧	セキュリティエキスパートサービス
	SHIELD クラウドCSIRTサービス
Check	
ランサムウェア対策	サイバー攻撃分析サービス
	脆弱性管理支援サービス
Web改ざん防止	SHIELD Webセキュリティ・オンデマンドサービス
	SHIELD クラウドWAFサービス
標的型攻撃対策	SHIELD メールセキュリティ・オンデマンドサービス
内部不正対策	SHIELD PCマネジメント・オンデマンドサービス
Action	
ランサムウェア対策	サイバーインシデント対応演習サービス
	標的型メール訓練サービス
	情報セキュリティ教育サービス
ネットワーク脆弱性可視化	RedSeal
CSIRT構築	CSIRT構築ソリューション
脅威情報収集	SHIELD グローバルインテリジェンスサービス
脆弱性チェック	セキュリティ診断サービス
	マルウェア感染調査サービス
	情報セキュリティ 現状分析サービス
	サイバー攻撃対策状況分析サービス
	標的型攻撃対策評価サービス
	SHIELD セキュリティ診断サービス
	SHIELD セキュリティ健康診断サービス

最新の情報は当社ホームページをご覧ください。

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/cyberbcp/

S17S-20-03 | 2019.03

HITACHI
Inspire the Next

サイバー攻撃対応BCPソリューション

株式会社 日立ソリューションズ

マルウェアなど高度化するサイバー攻撃に特化したBCP*の策定、セキュリティ対策、監視運用、復旧まで、トータルに事業継続を支援します。

＊BCP：事業継続計画（Business continuity plan）

情報システムや制御システムを狙った標的型のサイバー攻撃は、
高度化するマルウェア・ランサムウェアが利用されるため、気づかないうちに被害が拡大してしまい、
重要な情報の漏洩やシステム破壊といった事業の存続に関わる被害が発生します。
サイバー攻撃被害を想定したBCPでは、災害やパンデミックの際の情報システムや
ITインフラを対象としたBCP（IT-BCP）とは異なる対応が求められます。

「IT-BCP（災害・パンデミック）」と「サイバー攻撃対応BCP」の違い

		災害・パンデミック	サイバー攻撃
1	標的企業・団体	不特定である	標的型が多い
2	考慮する視点	被害者視点	被害者・加害者視点
3	リスク低減対策	リスク低減が困難	リスク低減が可能
4	被害状況把握	気づきやすい	気づきにくい
5	復旧開始タイミング	即時	原因究明後
6	体制の違い	原因調査部隊不要	原因調査部隊必要

サイバー攻撃を想定したBCP対応のポイント

サイバー攻撃被害を想定したBCP策定においては、「被害の発生時期や状況が分かりにくい」「原因究明に時間がかかる」など、サイバー攻撃の特性を踏まえたBCPを事前に策定・運用する必要があります。

1 リスク（重要情報など）の洗い出し、検討

2 情報漏洩、踏み台サーバーなど加害者的視点での考慮

3 再攻撃に対応できる仕組みの考慮によるリスク低減

4 早期発見のための監視

5 原因究明後の適切な復旧

6 CSIRT*による原因究明と対策立案

＊CSIRT：Computer Security Incident Response Team

ソリューションの特長

1. 経験豊富な専門家がBCP策定に向けたコンサルティングを実施

サイバー攻撃に対するBCP策定に関して経験豊富なコンサルタントが、ISO27001などのリスクアセスメントを基準にした「サイバー攻撃対応BCP策定コンサルティング」を提供します。サイバー攻撃を受けた際の事業への影響のリスク分析を行い、対策・運用・検証に関する計画の策定や、インシデントが発生した場合のBCP発動タイミング、攻撃分析体制、業務再開手順、業務復旧手順の策定を行います。

2. BCPに沿ったセキュリティ対策システム・サービスを幅広く提供

策定したBCPやリスク分析結果に基づき、サイバー攻撃を受けた際に、事業への影響が大きいシステムに対するセキュリティを実現します。標的型攻撃やランサムウェアへの対策に効果的なシステム・サービスなどに加え、セキュリティ教育や訓練サービスなども幅広く提供可能です。

3. 24時間365日体制でインシデント発生を早期発見、現地で復旧を支援

運用は、セキュリティアナリストが常駐するSOC*がサポートします。ファイアウォールなどのネットワーク機器からPC、サーバーなどのエンドポイントまで含めて24時間365日体制でお客さまシステムのセキュリティ運用監視を行います。セキュリティインシデントを早期に発見し、迅速な原因究明と対策の実行、事業継続をサポートします。

＊SOC：Security Operation Center

PDCAサイクルで支援

経験豊富な
コンサルタントが支援

特有の判断基準や行動基準を考慮したBCP策定やマルウェア感染対策、24時間365日の総合監視など、お客さまの規模・予算に応じた事業継続計画の策定・運用をトータルで支援します。