HITACHI
Inspire the Next

News Release

2018年1月30日
株式会社日立システムズ
株式会社日立ソリューションズ

企業の事業継続を支援する「サイバー攻撃対応 BCP ソリューション」を提供開始

BCP 策定からセキュリティ対策の実施、監視運用、復旧までをトータルにサポート

株式会社日立システムズ(本社:東京都品川区、代表取締役 取締役社長:北野 昌宏、／以下、日立システムズ)と株式会社日立ソリューションズ(本社:東京都品川区、代表取締役 取締役社長:柴原 節男／以下、日立ソリューションズ)は、サイバー攻撃に備え、企業の事業継続を支援する「サイバー攻撃対応 BCP※1 ソリューション」を本日から提供開始します。

本ソリューションは、両社の強みであるセキュリティ関連の製品・サービスを生かし、サイバー攻撃に特化したBCPの策定からBCPに沿ったセキュリティ対策の実施、監視運用、復旧までをトータルにサポートし、企業の事業継続を支援するものです。

本ソリューションの中でも、このたび新たに提供を開始する「サイバー攻撃対応 BCP 策定コンサルティング」は、情報セキュリティの国際的な規格である ISO27001 のリスクアセスメントを基準にしており、金融・公共・産業などのさまざまな業種で両社が約 20 年にわたり行ってきたセキュリティ対策や、IT-BCP 対応の知見を生かし、企業の業態や予算に応じた BCP の策定を支援します。

また、BCP に沿ったセキュリティ対策の実施から監視運用、復旧までのプロセスにおいても、適切なセキュリティ対策のシステムやサービスの提供、Security Operation Center(SOC)によるネットワーク機器やエンドポイントの 24 時間 365 日の運用監視など、約 2,000 名のセキュリティスペシャリストによる多様なサービスを提供します。

※1:Business Continuity Plan の略。企業が自然災害や大火災、サイバー攻撃などを受けた場合に、被害を最小限にとどめ、早期復旧を図るために、平常時や緊急時の事業継続するための方法・手段を取り決めておく計画のこと。

図 1. サイバー攻撃対応 BCP ソリューションの概要

■背景

昨今、サイバー攻撃は高度化・多様化が著しく、完全に防御することが難しくなっています。サイバー攻撃によって社内・組織内にマルウェアが侵入すると、管理者が気付かないうちに被害が拡大し、そのまま原因究明と対策ができない場合は、業務停止にまで進展する可能性があります。

そのため、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、災害やパンデミック対策とは異なるサイバー攻撃の特性を踏まえた BCP を事前に策定・運用することが喫緊の経営課題となっています。

■「サイバー攻撃対応 BCP ソリューション」の主な特長

本ソリューションは、サイバー攻撃に特化した BCP の策定(Plan)から BCP に沿ったセキュリティ対策の実施(Do)、監視運用などの BCP に沿った運営(Check)、BCP の効果検証・継続的改善(Action)までをトータルにサポートし、事業継続を支援するものです。

（1）経験豊富なセキュリティスペシャリストが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 策定に関して豊富なコンサルテーション経験を持つエンジニアが、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。お客さまの業態や予算に応じた BCP を短期間で策定します。

本コンサルティングでは、サイバー攻撃を受けた際の事業への影響範囲とリスクの洗い出しを行います。そのうえで、優先度を考慮したリスク低減対策、運用・効果検証に関する計画を策定します。さらに、インシデントが発生した場合の BCP 発動契機、分析・復旧へ向けた体制、業務再開に必要な手順を整備し、システムがダウンした場合に備え、段階的に業務復旧を行う BCP を策定します。

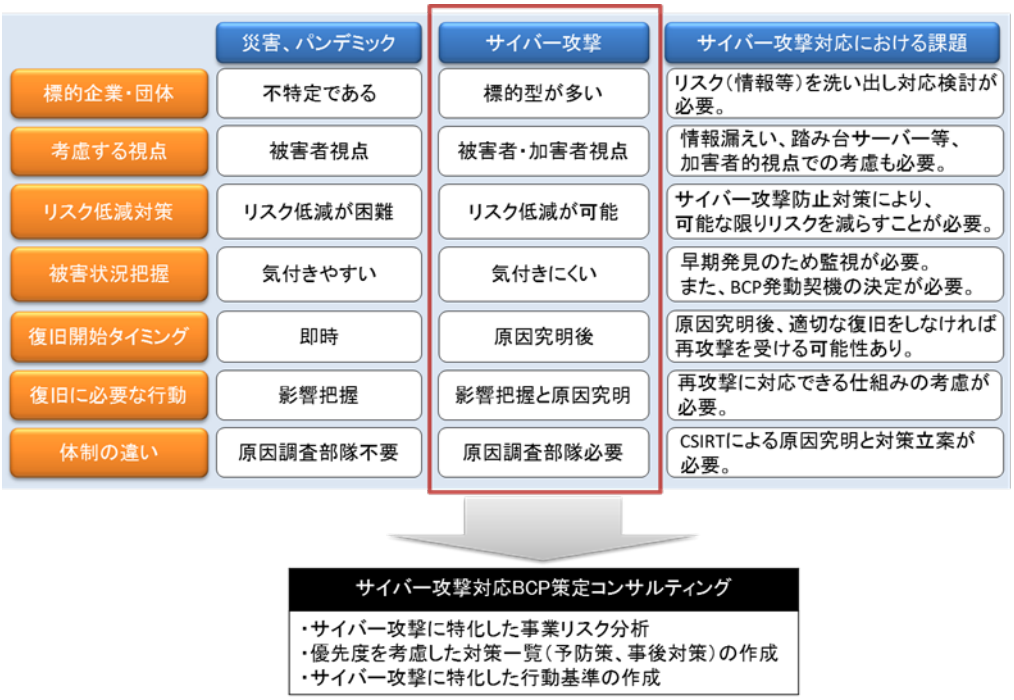

図 2. サイバー攻撃向け BCP 策定におけるポイント

(2)BCPに沿ったセキュリティ対策システムや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、事業上の影響が大きいシステムへのセキュリティ対策を実現します。標的型攻撃やランサムウェアへの効果的な対策として、各種システムやサービスの提供に加え、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)ネットワーク機器からエンドポイントまでを統合的に運用監視

BCPのライフサイクルで重要な役割を果たす日頃の運用においては、セキュリティアナリストが常駐するSOCからサポートします。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うことにより、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。

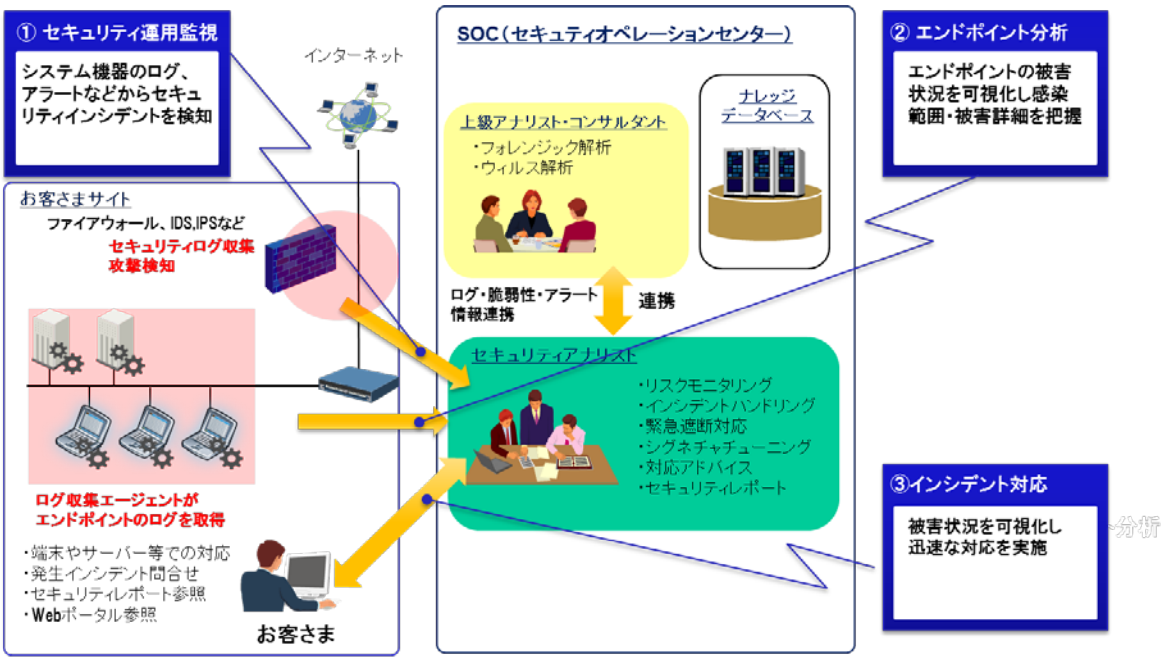

図3. 運用監視のサポート体制

(4)豊富なセキュリティスペシャリストを結集し、お客さまの事業継続をサポート

BCPの策定支援からBCPに沿ったセキュリティ対策の実施、運用監視、有事の際の原因調査・復旧支援、再発防止策の提案まで、約2,000名の公的資格や業務経験を保持したセキュリティスペシャリストやホワイトハッカーが、お客さまをサイバー攻撃から守り、事業継続をサポートします。

■価格

個別見積もり

■提供開始時期

2018年1月30日

■ソリューション紹介ホームページ

株式会社日立システムズ：https://www.hitachi-systems.com/solution/t01/shield/cyberbcp.html

株式会社日立ソリューションズ：http://www.hitachi-solutions.co.jp/cyberbcp

■商品・サービスに関するお問い合わせ先

株式会社日立システムズ

ホームページ：https://www.hitachi-systems.com/form/contactus.html

Tel：0120-346-401（受付時間：9 時～17 時/土・日・祝日は除く）

株式会社日立ソリューションズ

ホームページ：https://www.hitachi-solutions.co.jp/inquiry/

Tel：0120-571-488（受付時間：9 時～17 時/土・日・祝日は除く）

■報道機関からのお問い合わせ先

株式会社日立システムズ

担当部署：CSR本部 コーポレート・コミュニケーション部

担当者：杉山、藤原

TEL：03-5435-5002（直通） E-mail：press.we@ml.hitachi-systems.com

株式会社日立ソリューションズ

担当部署：経営企画本部 広報・宣伝部

担当者：安藤

Tel：03-5479-5013 Fax：03-5780-6455 E-mail：koho@hitachi-solutions.com

以上