**サイバーセキュリティ経営ガイドラインも推奨 今こそ求められている「サイバー攻撃に対応したBCP」**

ZDNet Japan Ad Special 2018年03月02日 15時00分

https://japan.zdnet.com/pickup/hisol\_201802/35115091/

[PR]サイバー攻撃による事業停止が大きなリスクになっている。最近のサイバー攻撃にはかつての常識が通用しないことがほとんどだ。特にビジネスに与えるインパクトが桁違いに大きくなった。

**サイバー攻撃で事業停止。なぜBCPは発動されないのか?**

　サイバー攻撃による事業停止が大きなリスクになっている。最近のサイバー攻撃にはかつての常識が通用しないことがほとんどだ。特にビジネスに与えるインパクトが桁違いに大きくなった。WebサイトやECサイトといったITシステムが止まるだけでは済まないケースもある。ときには製品を製造するラインやサプライチェーンそのものまで止まってしまう。

　記憶に新しいのは、昨年、国内で大きな被害をもたらした脅威であるWannaCryだろう。データを暗号化して身代金を要求するランサムウェアと呼ばれる脅威だが、Windowsファイル共有の脆弱性を突いて自己増殖するウイルスのような性質をもっていた。感染力と感染スピードが高く、インターネット閲覧用のPCだけでなく、社内システムを管理するPCや生産整備を管理するPCにも感染を広げた。この結果、生産やサービス提供を一時的に停止する企業が多発したのだ。

　なかには海外の製造拠点や研究拠点での感染が発端となったケースもあった。製造設備や検査機器へのセキュリティパッチ適用が遅れ、そこから日本国内の業務システムへと感染が広がった。脅威に国境線がないことをまざまざと見せつけた格好だ。

　ビジネスへのインパクトが桁違いに大きくなった背景には、いくつかの理由が考えられる。まず、脅威が高度化・巧妙化したことだ。ITだけでなく医療機器や制御系システム、IoT機器などにまで対象が広がったことも大きい。また、こうした機器はパッチ適用が難しいことも影響している。しかし、最も大きな理由が考えられる。それは、対策のための発想が根本的に変わったのに、それに合わせた対策ができていないことだ。

　実際、こう思ったことはないだろうか。「サイバー攻撃で事業が止まるほどの事態が起きたのに、なぜBCP(Business Continuity Planning: 事業継続計画)は発動されないのか？」。サイバー攻撃リスクはいまや経営課題だ。だが、それが事業継続の計画を実行する事態として捉えられていないのだ。

**「サイバーセキュリティ経営ガイドライン」でBCP関連項目が追加**

　BCPは、パンデミックや自然災害が発生したときに備える対策だ。事業が停止する事態に陥ったときどう復旧させ事業を継続させていくかの手順が書かれている。一方、サイバーセキュリティは、サイバー攻撃の発生に備える対策が中心だ。インシデントと呼ばれる緊急事態の発生に迅速に対応していくためのさまざまな対策を行う。

　一般的には、このようにBCPとサイバーセキュリティ対策は異なるものとして考えられている。IT-BCPという言葉もあるが、これはBCPをITの側面でどう整備するかを指した言葉だ。しかし、サイバー攻撃はいまや事業継続を左右する経営課題だ。そうであるなら、本来サイバーセキュリティ対策を含めたBCPが必要になるはずだ。

　逆に言えば、BCPとサイバーセキュリティが同じ経営課題として統合的に把握されていないことが、被害の拡大につながっている要因だと考えられないだろうか。

　例えば、BCPでは、災害によるシステムダウンやデータ消失に備えて、災害対策(DR)サイトを構築する。だが、現在のサイバー攻撃はネットワークを介してDRサイトのデータをも破壊してしまう。実際、WannaCryの被害事例のなかには、バックアップ対象のデータが暗号化され、そのデータが暗号化されたままDRサイトにバックアップされ、復旧が不可能になったケースがある。従来のBCPでは現在のサイバー攻撃に耐えられないのだ。

　また、BCPの復旧手順や推進体制も、現在のサイバー攻撃に耐えられるようには設計されていない。従来の手順では、ウイルスなどに感染したPCは、ネットワークから隔離して駆除したのち再接続するという流れだった。しかし、現在は、ネットワーク内部に脅威が潜伏するため、再接続した段階で再び感染してしまう。

　災害対策本部も、訓練のなかでこうしたサイバー攻撃を受けたときの対応を想定していない。専門的な知識をもった人材も少ない。攻撃を受けてから「どこに何を連絡すればいいかわからない」というBCPの初動すらできないケースも少なくない。

　つまり、サイバー攻撃で事業が停止してもそれに対応するBCPがないのが大きな問題なのだ。組織全体でサイバー攻撃に対応したBCP対策を講じる重要性は日増しに高まっている。実際、経済産業省が公表し、多くの企業が参考にしている「サイバーセキュリティ経営ガイドライン」では、昨年の改訂版のVer 2.0で、新たにリスク対応策（防御・検知・分析）の実施やインシデント発生時の復旧体制の整備についての項目が追加された（同書P.11、P.14）。

**サイバーセキュリティ経営ガイドラインも推奨 今こそ求められている「サイバー攻撃に対応したBCP」 - (page 2)**

ZDNet Japan Ad Special 2018年03月02日 15時00分

[PR]サイバー攻撃による事業停止が大きなリスクになっている。最近のサイバー攻撃にはかつての常識が通用しないことがほとんどだ。特にビジネスに与えるインパクトが桁違いに大きくなった。

**サイバー攻撃に対応したBCPソリューションが登場**

　では、どのようにしてサイバー攻撃に対応したBCPを構築していけばよいのか。BCPもサイバーセキュリティ対策も全社的な取り組みが求められ、予算規模が大きく、カバー範囲も多岐にわたる。BCPとサイバーセキュリティに関する専門的な知識やスキルも必要だ。実際に被害の現場に立ち会ってみないとわからないノウハウや経験の蓄積もある。

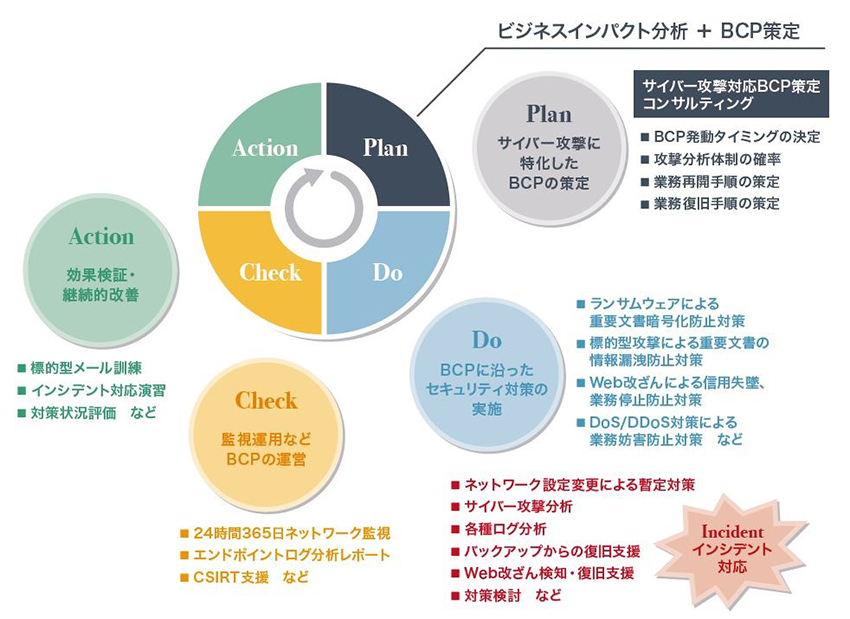
　そのような中、サイバー攻撃に対応したBCPソリューションが登場した。日立ソリューションズと日立システムズが提供を開始した「サイバー攻撃対応BCPソリューション」だ。

　サイバー攻撃対応BCPソリューションは、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するソリューションだ。PDCAサイクルに沿って、サイバー攻撃に特化したBCPの策定(Plan)、BCPに沿ったセキュリティ対策の実施(Do)、監視運用などBCPの運営(Check)、BCPの効果検証・継続的改善(Action)を行い、事業継続を支援する。特徴は大きく3つある。

　1つめは、BCP策定に向けたコンサルティングだ。経験豊富なセキュリティスペシャリストが、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」を提供する。また、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度に応じたセキュリティ対策を提供する。

　2つめは、ネットワーク機器からエンドポイントまでの統合的な運用監視だ。セキュリティアナリストが常駐するSOC（Security Operation Center）から、ネットワーク機器の24時間365日監視や、インシデントの迅速な原因究明と対策の実行を行う。

　3つめは、事業継続のサポートだ。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連携して、顧客をサイバー攻撃から守り、有事の際の原因調査・再発防止策提案までを含めて事業継続をサポートする。

[[](https://japan.zdnet.com/image/l/storage/35115091/storage/2018/02/28/56a4463dc36a191ee345fa39954f0128/hisol_35115091_img01.jpg)ソリューション概要図](https://japan.zdnet.com/image/l/storage/35115091/storage/2018/02/28/56a4463dc36a191ee345fa39954f0128/hisol_35115091_img01.jpg)  
※クリックすると拡大画像が見られます

　ソリューションを活用することで、サイバーセキュリティ経営ガイドライン Ver 2.0で指示されている項目を効率よく導入していくことが可能になる。

**ソリューションの目玉「サイバー攻撃対応BCP策定コンサルティング」**

　こうしたBCPとセキュリティが融合したトータルソリューションはこれまでほぼ存在しなかった。必要性の高さは認識され始めていたものの、実際に提供するための知識やノウハウ、体制を有するベンダーは限られてしまうためだ。

　例えば、セキュリティの専門ベンダーならBCPコンサルティングまでを提供しようとすると、BCP分野に強いコンサルタントが必要になる。一方、BCPコンサルティングに強みを持ったベンダーは具体的なセキュリティ製品やサービスに強いセキュリティスペシャリストが必要になる。BCPとセキュリティが違うものと認識されていたように、それぞれに強みを持った人材も分かれていたのが実情なのだ。

　そこで、サイバー攻撃対応BCPソリューションでは、日立ソリューションズと日立システムズの強みを統合させた。両者はもともと日立グループの総合力を生かしたセキュリティ関連の製品とサービスを展開しており、BCPにもセキュリティにも強かった。

　その強みが特に発揮されているのが「サイバー攻撃対応BCP策定コンサルティング」だ。コンサルティングは「事業への脅威分析」と「サイバー攻撃対応BCP策定」の2つのフェーズに分けられており、サイバー攻撃に特化した事業リスク分析と優先度に応じた対策や行動基準の作成を行う。作業期間は最短3ヵ月から可能だ。

　一般に、BCPコンサルティングは全社的な取り組みになることが多い。そのため、期間も長く、費用も高額になりがちだ。一方、セキュリティコンサルティングは、ソリューションの導入がメインのため、BCP導入で使われるビジネスインパクト分析などの手法が利用されないことが多い。

　サイバー攻撃対応BCP策定コンサルティングは、こうした課題を解消している。人材不足などでBCP策定が未着手の中堅中小規模の企業でも要件に柔軟に対応した低価格なBCP対応を実現することが可能だ。また「IEC62443」などの制御システムのセキュリティマネジメントシステムに準拠したコンサルティングも行う。

　サイバー攻撃による事業停止リスクを正しく把握するためには、サイバーセキュリティだけのアプローチやBCPだけのアプローチでは不十分だ。サイバーセキュリティ経営ガイドラインが訴えるように、サイバーセキュリティに対応したBCPが今求められている。