サイバーＢＣＰ策定と危機管理演習のすすめ

世界経済フォーラムが今年も年次総会（通称ダボス会議）に合わせ「グローバルリスク報告書 2019 年度版」を公表したが、この報告書によると、今後 10 年で発生の可能性が高いリスクの 5 番目に「サイバー攻撃」が挙げられた。昨年よりも 2 つ順位を下げたものの、「サイバー攻撃」による被害が日々報告されている現状を鑑みると、組織運営上、情報資産や情報システムを守るためにあらゆる対策の高度化が急務である。本稿ではサイバー攻撃に対する組織的対策の 1 つであるサイバーBCP（事業継続計画：Business Continuity Plan）策定とインシデント発生時の危機管理演習に焦点を絞り解説したい。

1．サイバー攻撃のインシデント事例

2018 年に発生したサイバー攻撃のインシデント事例を概観する。メディアで公表された事例のため大企業が中心であるが、実際に被害に遭っている企業等はその規模とは無関係であると考えられる。

■表１　2018 年に発生したサイバー攻撃のインシデント事例

時期	企業等	概　要	攻撃手法
1 月	コインチェック	同社が運営している仮想通貨取引所が不正アクセスを受け、約 580 億円分の仮想通貨（NEM）が流出。	不正アクセス
4 月	中央省庁	中央省庁から職員延べ約 2,000 人分のメールアドレスとログイン・パスワードが流出したことを内閣サイバーセキュリティセンターが発表。	不正アクセス
5 月	メニコン子会社	同社の通販サイトが不正アクセスを受け、顧客約 3,400 人分のクレジットカード情報が流出。不正利用による被害も確認された。	不正アクセス
6 月	森永乳業	同社の健康食品通販サイトが不正アクセスを受け、顧客約 9 万人分のクレジットカード情報が流出。不正利用被害が約 300 件確認された。	不正アクセス
8 月	台湾積体電路製造（TSMC）	台湾の主力工場がコンピューターウイルス（WannaCry 変種）に感染し生産が一時停止。最大 190 億円の売上高への影響が見込まれると発表。	マルウェア
9 月	テックビューロ	同社が運営している仮想通貨取引所が不正アクセスを受け、約 67 億円分の仮想通貨（ビットコイン、モナコイン等）が流出。	不正アクセス
9 月	British Airways	同社が会員に提供しているアプリの脆弱性が原因で、約 38 万人分の会員情報が流出。	不正アクセス
10 月	宇陀市立病院（奈良県）	電子カルテシステムがランサムウェアに感染し、1,133 人分の診療記録データが暗号化された。身代金は支払わず。	マルウェア

11 月	スクウェア・エニックス	同社のオンラインゲーム「ファイナルファンタジー14」のサーバーが DDoS 攻撃を相次いで受け、最大 20 時間の障害が発生。	DDoS 攻撃
12 月	ブルーチップ	買い物ポイントカードシステムのサーバーがランサムウェアに感染。ポイントの利用やポイントの残高照会ができない状態となった。	マルウェア

出典：各種報道機関・公開情報をもとに弊社作成

掲載したインシデント事例で使われた攻撃手法は「不正アクセス [1]」、「マルウェア [2]」、「DDoS 攻撃 [3]」の 3 つの手法であるが、攻撃者側はその他にも「ウェブサイト改ざん [4]」、「標的型攻撃 [5]」、「なりすまし [6]」等、さまざまな手法を駆使して攻撃を仕掛けてくる。警察庁の調査によれば「標的型攻撃」の 1 つである「標的型メール攻撃」の 97%は 2017 年に発生した WannaCry のような巧妙な「マルウェア」が仕込まれた「ばらまき型」であり、世界的な大企業ですら甚大な被害を受けている状況をみると、どんなに高度な対策を施しても、完全な防御は困難になりつつあると言わざるを得ない。

また、サイバー攻撃は実態社会における破壊や盗取などと同様の結果をもたらす一方で、攻撃者を特定し犯罪者や組織を法律に基づいて裁くことが難しいという厄介な特徴がある。政治的意思表示を主な目的とするハクティビストやテロリスト、ランサムウェアやフィッシング等の攻撃を駆使して金銭盗取を図る犯罪組織、軍事領域の「第 5 の戦場」と位置付けてサイバー軍を強化する国家など、さまざまな攻撃者が目的達成の手段としてのサイバー攻撃の有効性や必要性を認識しているのが現状であり、サイバー攻撃はますます予測不可能な領域に陥りつつある。

2. 進化するサイバー攻撃への対策の現状

サイバー攻撃の歴史は 1980 年代のハッキングにさかのぼり、当初はパソコンへのアンチウイルス製品の導入が対策の主流であった。1995 年の Windows95 の登場によりビジネスにおけるインターネットの利用が急拡大し、その状況を悪用した組織的サイバー犯罪が始まったことで、侵入検知システム（IDS）やファイアウォール等の侵入防止対策が施されるようになった。2000 年以降になると巧妙化するサイバー攻撃に対し侵入防止システム（IPS）、メールやウェブの無害化ソフト、ふるまい検知システム、アンチボット、サンドボックス等の導入が進むとともに、エンドポイントセキュリティ製品、クラウド型セキュリティサービス、モバイルデバイスのセキュリティ対策等も導入されつつある。

これらは技術的セキュリティ対策のトレンドであり、情報資産や情報システムを守るためには、複数のセキュリティ対策を組み合わせて、「入口対策（不正侵入を防ぐ）」、「内部対策（侵入後の被害拡大を防ぐ）」、「出口対策（情報資産の外部流出を防ぐ）」の 3 つの対策を総合的に実施する「多層防御」が不可欠である。

しかし、社会におけるテクノロジーの進化に伴い IoT デバイスは増える一方であり、それらの管理やセキュリティ対策がますます難しくなっている。また、攻撃者側が高度なハッキング・ツールを開発し攻撃が広範囲化・短時間化しており、技術的なセキュリティ対策だけでは完全に防御することが難しくなっている。

こうした状況を踏まえると、定期的なシステム構成の見直しや各システムへのセキュリティパッチ

の適用等を適切に行い、一番脆弱である従業員の教育（人的セキュリティ対策）を行うとともに、インシデントの発生を想定した BCP の策定や危機管理演習の実施（組織的対策）が重要である。

3．インシデント事例ごとの対応手順の解説

実際にサイバー攻撃を受けた場合の影響としては、「情報の漏えい（機密性）」、「システムの停止（可用性）」、「データの改ざん（完全性）」の 3 つがあるが、今回は「システムの停止（可用性）」についてどのような対応が必要となるか、下表の 3 つのケースごとの対応例を解説する。

システム	攻撃手法
（1）業務システム（経理システム・メールシステム等）	マルウェア
（2）顧客システム（e コマース、キャッシュレス決済サービス等）	DDoS 攻撃
（3）生産システム（MES[7]、PLC[8] 等）	マルウェア

⑴ ランサムウェア感染による業務システムの停止

マルウェアの一種であるランサムウェア感染により業務システムが停止した場合、次のような対応が必要である。

①インシデント対応（初動対応）

□感染拡大防止

感染しているパソコンやサーバーをネットワークから切り離す必要があるが、通常はすぐには感染範囲の特定が難しいことが多く、感染拡大防止のために、いったん全てのネットワークを切り離す。

□感染範囲と感染経路の特定

全てのパソコンやサーバーを対象に感染の有無を調査する。（その時点で通信ログ等から感染経路や攻撃手法等の原因が特定できれば、より早い復旧が可能である。）

□ランサムウェアの駆除

感染したパソコンやサーバーからランサムウェアを駆除する。

□データの復元

必要に応じて OS やアプリケーション等の再設定を行ったうえで、適切に保管しておいた直近のバックアップデータを使いデータを復元する。

□社内の情報共有

業務システム停止および復旧見込み等、社内に現状の共有を行い復旧までに必要な社内業務への対応方法や社外から問い合わせがあった場合の注意点等を指示する。

②原因調査･再発防止

セキュリティ会社等に依頼して通信ログ等の詳細な調査を行い、感染経路や攻撃手法等の原因を特定し、適切な再発防止策を講じることが大切である。

なお、ランサムウェアは身代金を支払ってもデータが戻る保証はなく、1 度支払うと再度標的となる可能性があるため、身代金を支払わないことが大切である。従って、前述の対応を行うためには次のような事前準備が重要である。

□適切なバックアップデータの取得

ランサムウェア対策で最も重要なのは、適切かつ定期的にバックアップデータを取得し、安全な方法で保管しておくことである。また、万一に備えデータの復元手順を確認しておくことが望ましい。

□重要業務の継続方法の検討

業務システムがランサムウェアに感染し停止した場合に備え、重要業務の継続方法を事前に検討しBCP を策定しておくことが必要である。

以上は、ランサムウェア感染により業務システムが停止した場合の対応例であるが、言うまでもなく感染防止策の方がより重要であり、前述の技術的セキュリティ対策に加え、標的型メール訓練等の定期的な従業員教育が不可欠である。

⑵ DDoS 攻撃による顧客サービスの停止

DDoS 攻撃により顧客サービスが停止した場合、以下のような対応が必要である。

①インシデント対応（初動対応）

□アクセス制御

同一 IP アドレスからのアクセス回数を制限する等して攻撃元の IP アドレスからのアクセスを一時遮断する。攻撃が海外から行われている場合には、日本以外の国からのアクセスを一時遮断するのも１つの方法である。

□代替手段による営業継続

代替手段により顧客サービスの提供を継続することが望ましいが、代替手段がない場合には、異なるドメインで新しいウェブサイトを立ち上げ早期の顧客サービス再開を図る。

□社内の情報共有

顧客サービスの停止および復旧見込み等、社内に現状の共有を行い復旧までに必要な社内業務への対応方法や社外から問い合わせがあった場合の注意点等を指示する。

□顧客への通知

メール等の方法が使えれば顧客サービス停止について状況や原因、復旧見込み等を顧客へ通知する。

②原因調査･再発防止

原因を調査し、再発防止および事業への影響を軽減する対策を講じることが大切である。

なお、DDoS 攻撃の原因は自社ではなく社外の攻撃者にあるため、事前の対策としては対策ツールの導入（WAF・IDS/IPS・UTM 等）やコンテンツ分散等が一般的であるが、ホームページの停止が事業に大きな影響を与える場合は、定期的な脆弱性診断を行うことに加えて、専門事業者が提供する「DDoS 対策サービス」の利用を検討することが望ましい。

⑶ マルウェア感染による生産ラインの停止

工場の制御システム（パソコンやサーバー等）がマルウェア感染したことにより生産ラインが停止した場合、次のような対応が必要である。

①インシデント対応（初動対応）

□感染拡大防止

感染している制御システムをネットワークから切り離す必要があるが、通常はすぐには感染範囲の特定が難しいことが多く、感染拡大防止のために、いったん工場の全ての制御システムを停止する。

□感染範囲と感染経路の特定

全ての制御システムを対象に感染の有無を調査する。（その時点で感染経路や攻撃手法等の原因が特定できれば、より早い復旧が可能である。）

□マルウェアの駆除

感染した制御システムからマルウェアを駆除する。

□制御システムの復旧

制御システムにプログラム等を再インストールし制御データ等の再設定を行う。

□停止期間の予測と供給継続方法の検討

感染範囲等の調査に基づき生産ラインの停止期間を予測する。また、生産停止によるサプライチェーンへの影響を最小限に抑えるため、停止期間中の手動による生産や代替拠点での生産、OEM 等、製品供給の継続方法を検討する。

□社内の情報共有と対応指示

生産ライン停止の影響や復旧見込み等を社内に共有するとともに、顧客への対応方針、受注制限や社外から問い合わせがあった場合の対応方法等を指示する。

□顧客への報告

納期に影響する可能性がある顧客を洗い出し、生産停止の状況報告と対応方針の説明を行う。

②原因調査・再発防止

制御システムのメーカーやセキュリティ会社等に依頼して感染経路等を特定し、適切な再発防止策を講じることが大切である。

なお、工場の制御システムはクローズドで外部から攻撃されることはないと考えがちであるが、本社の営業部門や購買部門と社内システムでつながっていたり、メンテナンス作業のためにパソコンや USB メモリ等を制御システムに接続することは日常的にあり得ることである。工場の制御システムは、本社の情報システム部門ではなく生産部門が管理していることが多く、全体像が把握されていない場合が多いので、まずは工場で使用している IT ネットワークや制御システムの全体像を把握しリスクを正しく認識することが事前の対策として重要である。

以上、（1）業務システム、（2）顧客システム、（3）生産システムの 3 つのケースについてシステム停止の対応例を記載したが、いずれのケースにおいても前述の項目に加えて次の 3 点についても参考にして頂きたい。

□対応要員や費用の確保

一時的にシステム関連の要員が多数必要になり超過勤務、休日出勤、他部門からの応援等が必要になるが、社内で十分な専門要員の確保が難しい場合には、IT ベンダーやセキュリティ会社に対応要員の派遣を依頼する必要がある。また、一連の対応には相応の費用が不可欠であり、経営者が迅速かつ適切に判断を行う必要がある。

□社外広報

社会的影響等を勘案し必要に応じてプレスリリース等を行い、影響の極小化に努める必要がある。

□警察等への通知

サイバー犯罪の被害に遭った場合には、速やかに所轄の警察や一般社団法人日本サイバー犯罪対策センター（https://www.jc3.or.jp/index.html）等へ通報する。

4. サイバーBCP と危機管理演習の必要性

前章でインシデントごとの対応について解説したとおり、インシデント対応はシステム担当による技術的な対応だけではない。肝心なことは、被害を最小限にするとともに、重要業務を継続することである。地震や台風などの大規模災害時の BCP（事業継続計画：Business Continuity Plan）を策定している企業は増えているが､サイバー攻撃を受けた場合の BCP を策定している企業はまだ少ない。災害時の BCP にもシステムの復旧対応が含まれるが、サイバー攻撃への対応は異なる。

大規模災害であればお客様やサプライチェーンも同時に被災している可能性があるが、サイバー攻撃の場合は自社のみが攻撃されていることが多く、その場合、復旧の遅れが直接信用の失墜、受注停止、売上減少等に繋がる可能性が大きい。また、サイバー攻撃を受けた場合、対応が遅れれば短時間に影響範囲が広がり被害が拡大する。被害拡大防止のためには、速やかに全面的なシステム停止という判断が必要となる局面もあり得るので、各組織の役割と責任、連携についてあらかじめ決めておく必要がある。そのうえで、優先すべき重要業務を継続するために必要な各組織の役割および対応手順をマニュアル化することが望ましい。BCP 策定の主な手順とポイントについて以下に解説する。

＜事業継続計画（BCP）とは＞

不測の事態などの発生により事業リソースが損傷を受け、通常の事業活動が中断した場合に、残存する能力で優先すべき業務を継続させ、許容されるサービスレベルを保ち、かつ許容される期間内に復旧できるように前もって代替リソースの準備を行ったり、災害時の対応方法や組織を規定したもの。

出典：『最新 リスクマネジメントがよ～くわかる本［第 2 版］』東京海上日動リスクコンサルティング株式会社著、秀和システム（2012 年）

⑴ 基本方針の策定

BCP の策定にあたっては、基本方針を定めておく必要がある。方針を定めることにより、経営者を巻き込んだ全社的対応が可能となる。

⑵ 重要業務の選定

非常時にはすべての事業を通常どおり実行することはできないため、最優先すべき業務に経営資源を集中させる必要がある。そのためシステムが停止した場合でも止められない重要業務を選定する。重要業務の選定には売上や収益だけでなく戦略の観点も必要であり、重要顧客への供給責任、今後拡大が見込まれる事業、人命の安全に関わる製品やサービス等自社のビジネスモデルに応じて選択することが重要である。

⑶ 被害想定

被害想定は想定シナリオのインシデントが発生した場合に、被害の範囲や影響を分析し、事業継続

までに要する時間や損害額、ビジネスへの影響を見積もることである。起こりうる最悪のケースを想定することで、実際の損害を覚悟した経営者の素早い決断が可能となる。

⑷ サイバーBCP におけるマニュアル作成

策定した BCP は文書化しておく。事前の対策や有事の対応を具体的な行動計画に落とし込むものであるが、インシデント発生時の対応についてはマニュアル化して関係者が内容を熟知しておく必要がある。

サイバーBCP におけるインシデント発生時対応マニュアルには以下のような項目が必要となる。

ａ.対策本部組織ごとの役割、責任者（不在時のルール）、指揮命令系統
ｂ.情報の集約方法（CSIRT への情報集約）
ｃ.社内外の連絡先一覧表
ｄ.緊急時対応手順・対応チェックシート（事例の原因調査、再発防止策を手順化しておく）

なお、インシデント発生時対応マニュアルは、定期的に人事異動や生産ライン、サプライチェーンの変更などビジネスの実態に合わせて修正する必要がある。またシステム停止に備え、対応手順や連絡先等は紙に印刷しておくことが大切である。

⑸ 危機管理演習

マニュアル作成後は、実効性の検証が必要となる。演習等により、実際にマニュアルどおりに対応が可能であるか、対応や連携に抜け漏れはないか等、課題の抽出を行う。また、緊急時にマニュアルをすべて読み込んで対応する余裕はないため、経営層を含む各対応組織が部門横断的に対応方針や手順を訓練で確認することによりインシデント対応力を高めることが重要である。人事異動も鑑みて、最低年１回の定期的な演習の実施が望ましい。

また、危機管理演習は、目的、参加メンバー、参加メンバーの習熟度等に応じたウォークスルー型やシミュレーション型等の方式で実施することが効果的である。

■表２　危機管理演習（例）

ウォークスルー型演習（手順確認演習）	
目的	マニュアルの実効性検証、課題の抽出
概要	部門単位で、作成したマニュアルを机上で読み合わせを行う。対応手順を確認し、マニュアルの実効性を検証する。抽出された課題によりマニュアルの修正を行う。
シミュレーション演習（机上型・リアルタイム型）	
目的	マニュアルの実効性検証、インシデント対応力の向上
概要	各部門および緊急対応組織で、シナリオに基づきインシデントの発生・検知から、初動対応、業務継続、部門間の連携、事態収束までの各フェーズの対応を討議する。主に部門、組織ごとの討議を行う机上型と、実際の事象経過に合わせて事務局よりさまざまな情報を付与し、各部門、組織が状況に応じた対応や意思決定を行うリアルタイム型がある。

5．おわりに

サイバー攻撃は、自然災害とは異なり悪意を持った攻撃者によって引き起こされるものである。攻撃手法は年々巧妙化し、攻撃ツールがアンダーグラウンドで売買されている状況の中、企業等がサイバー攻撃を完全に防ぐことは難しい。サイバー攻撃から自社の情報資産や情報システムを守るためには、サイバー攻撃により発生しうる被害を想定し、事業継続のための事前の対策と有事の対応計画を立てるとともに、日々の情報収集に基づく対策のアップデート、定期的な演習等によるインシデント対応力の向上を図ることにより、明日発生するかもしれない有事に備えることが重要である。

本稿が、貴社におけるリスクマネジメントの一助となれば幸いである。

[2019 年 3 月 12 日発行]

---

[1] 不正アクセス：アクセス権限を持たない者が、サーバーや情報システムに侵入すること。情報漏えいやシステム停止等の影響を及ぼす。
[2] マルウェア：不正な動作を行う目的で作成された、悪意あるソフトウェアやプログラムの総称。
[3] DDoS 攻撃：Distributed Denial of Service attack の略。複数のコンピューターから大量のアクセスを集中させることにより、相手のサーバーやネットワークをダウンさせる攻撃。
[4] ウェブサイト改ざん：第三者によりウェブサイトの内容が書き換えられる、またはウェブサイトにウイルス等を埋め込まれること。
[5] 標的型攻撃：特定の組織や情報を狙って、継続的に行われる攻撃。
[6] なりすまし：他人の ID・パスワードを盗用するなどして、ネットワーク上で正規のユーザーのふりをして活動をする行為。
[7] MES：Manufacturing Execution System の略。製造工程の状況把握、管理、作業者への指示や支援等を行う製造実行システム。
[8] PLC：Programmable Logic Controller の略。工場の自動機械を制御する装置。

TOKIO MARINE NICHIDO
東京海上日動リスクコンサルティング株式会社
ソリューション創造本部〔サイバーチーム〕
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23 階
Tel. 03-5288-6591　Fax. 03-5288-6590
http://www.tokiorisk.co.jp/