資料６

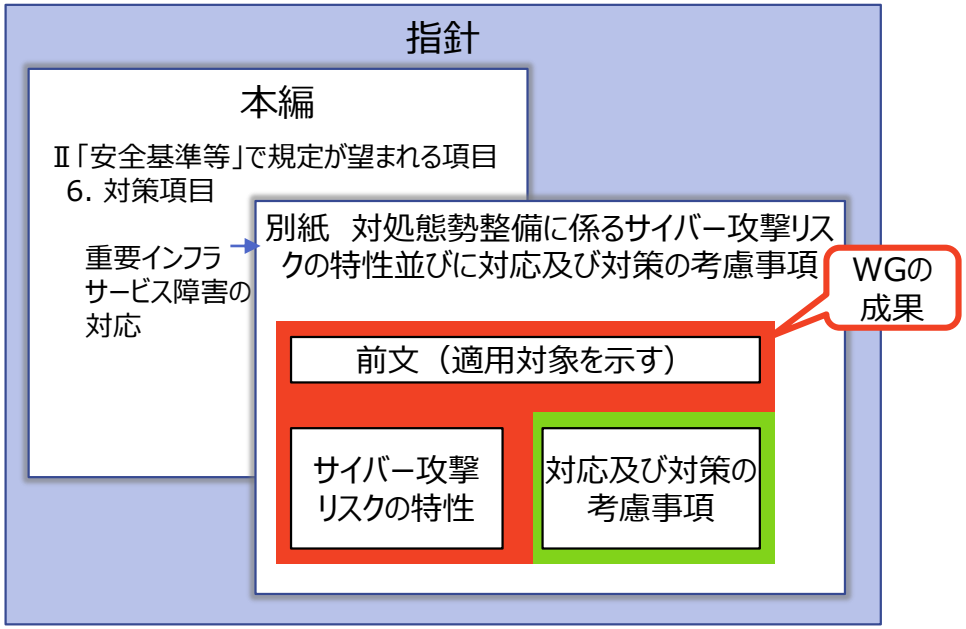
重要インフラサービス障害に係る対処態勢検討WGの検討結果について

２０１７年６月２７日

内閣サイバーセキュリティセンター
重要インフラグループ

重要インフラサービス障害に係る対処態勢検討WGの概要

重要インフラサービス障害に係るリスクに適切に対処するため、事業継続計画及びコンティンジェンシープランの策定・改定時に考慮されるべき「サイバー攻撃リスクの特性」等について調査検討を行うＷＧを設置し、４月より３回の会議を開催した。以下に記載の有識者がＷＧに参加し、「サイバー攻撃リスクの特性」の策定を行った。



WG開催スケジュール

第１回ＷＧ　2017年４月26日
　目的・目標のすり合わせ、金融分野における先導的取組の紹介（FISC）

第２回ＷＧ　2017年５月23日
　「サイバー攻撃リスクの特性」の草案を踏まえた議論

第３回ＷＧ　2017年６月15日
　「サイバー攻撃リスクの特性」の原案を確認

WG構成委員

主査	中島　一郎	早稲田大学研究戦略センター　特任教授
委員	阿部　克之	電気事業連合会　情報通信部長
委員	有村　浩一	一般社団法人ＪＰＣＥＲＴコーディネーションセンター　常務理事
委員	落合　正人	SOMPOリスケアマネジメント株式会社ERM事業部　部長
委員	中野　利彦	株式会社日立製作所サービス&プラットフォームビジネスユニット制御プラットフォーム統括本部セキュリティ推進室　室長
委員	中村　昌允	東京工業大学大学院環境・社会理工学院　特任教授
委員	野口　和彦	国立大学法人横浜国立大学 リスク共生社会創造センター　センター長兼大学院環境情報研究院　教授
委員	平田　真一	日本電信電話株式会社技術企画部門セキュリティ戦略　担当部長
委員	和田　昌昭	公益財団法人金融情報システムセンター　監査安全部長
委員	渡辺　研司	名古屋工業大学大学院工学研究科社会工学専攻　教授

WGにおける主な論点

＜サイバー攻撃リスクの特性＞

事業継続計画及びコンティンジェンシープランの策定・改定時に考慮されるべき「サイバー攻撃リスクの特性」の検討を行い、議論を踏まえ最終的に以下の７項目を策定した。各特性の詳細説明は別紙１記載のとおり。

・攻撃者の存在と多様な攻撃目的　・攻撃手口の高度化　・執拗な攻撃が行われる可能性
・同時多発的な攻撃が行われる可能性　・検知が困難な攻撃が行われる可能性
・急速な被害拡大に繋がる攻撃が行われる可能性　・誤った判断や対処を誘発する攻撃が行われる可能性

＜適用対象＞

コンティンジェンシープラン及び事業継続計画の名称や記載の範囲、発動のタイミング等は分野や事業者によって異なる場合があるため、「サイバー攻撃リスクの特性」を考慮すべき対象（適用対象）は各事業者において別紙１記載のフローの例を参考に検討を行うこととした。フローの例の中で「保安規程等に基づく対応」が行われるケースを挙げており、この対応への「サイバー攻撃リスクの特性」の適用要否がWGの中で論点となったが、最終的に別紙１記載のとおり、以下の整理としている。

「保安規程等に基づく対応は被害の低減及び抑制に着目した対応であり、一般的に被害の原因がサイバー攻撃であるか否かによって変わるものではない。一方、その対応にITが用いられる場合には、その対応自体がサイバー攻撃により機能しなくなる可能性を踏まえ、サイバー攻撃リスクの特性等を考慮することが期待される。」

（参考）第4次行動計画上の定義

＜コンティンジェンシープラン＞

重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ実行面から具体的に定めたもの（安全を確保するために重要インフラサービスの提供を停止するなどの対応についても含まれる。）

＜事業継続計画＞

機能保証の観点から、重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラサービスを許容可能な時間内に許容可能な水準まで復旧させることを目的として、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたもの。

別紙１．対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項（案）

次頁に示すサイバー攻撃リスクの特性及び対策の考慮事項は、重要インフラ事業者等がコンティンジェンシープラン及び事業継続計画を策定・改定する際に考慮されることを期待するものである。

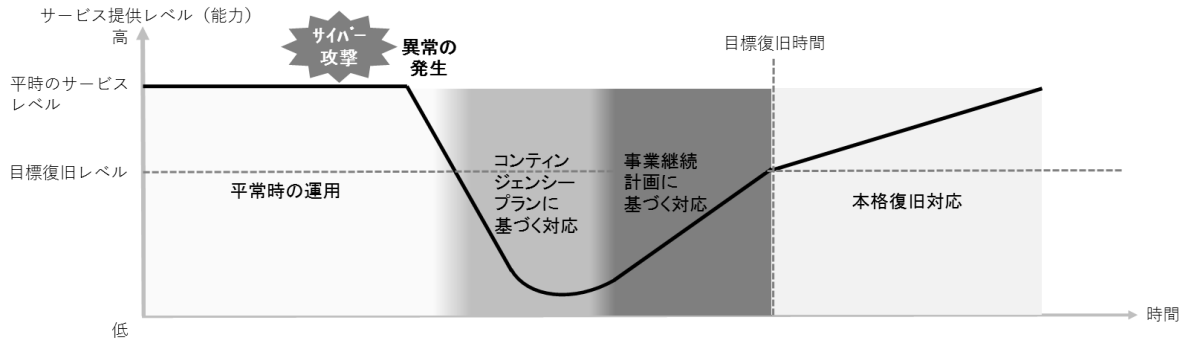
コンティンジェンシープラン及び事業継続計画の定義は指針本編記載のとおりであるが、これらの名称や記載の範囲、発動のタイミング等は分野や事業者によって異なる場合があるため、次頁の特性等を考慮すべき対象（適用対象）は各事業者等の状況に応じて検討されたい。

適用対象の検討の参考として、図１にサイバー攻撃の発生から復旧までのフローの例を示す。図１の例示（例１及び例２）はいずれもサイバー攻撃により異常が発生し、サービスレベルが時間の経過とともに低下した後、コンティンジェンシープランや事業継続計画に基づく対応を経てサービスレベルを復旧させる一連のプロセスを表したものである。

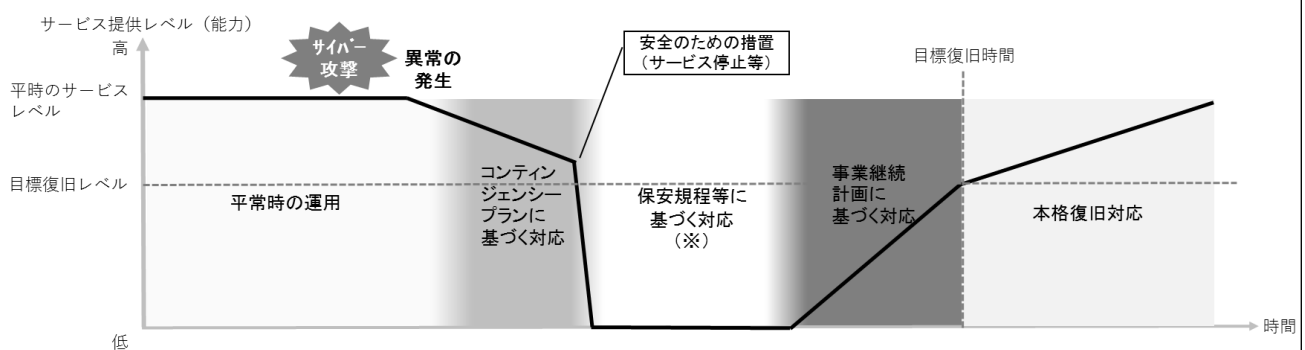
例１では、サービスの早期復旧を図るため早いタイミングで事業継続計画に基づく対応を開始している。一方例２では、安全のための措置として意図的にサービスを停止し、保安管理規程等に伴う対応を実施した後、事業継続計画に基づく対応を開始している。いずれの例においてもコンティンジェンシープラン及び事業継続計画は、次頁の特性等を考慮すべき適用対象となる。例２の保安規程等に基づく対応は被害の低減及び抑制に着目した対応であり、一般的に被害の原因がサイバー攻撃であるか否かによって変わるものではない。一方、その対応に IT が用いられる場合には、その対応自体がサイバー攻撃により機能しなくなる可能性を踏まえ、次頁の特性等を考慮することが期待される。

図１サイバー攻撃の発生から復旧までのフローの例（下記以外にも様々なフローが存在する。）

例1. サービスの早期復旧を図る場合



例2. 復旧作業開始前に保安規程等に基づく対応（災害・事故その他非常の場合の被害への対応）を行う場合



（※）保安規程等に基づく対応は被害の低減及び抑制に着目した対応であり、一般的に被害の原因がサイバー攻撃であるか否かによって変わるものではない。一方、その対応に IT が用いられる場合には、その対応自体がサイバー攻撃により機能しなくなる可能性を踏まえ、サイバー攻撃リスクの特性等を考慮することが期待される。

サイバー攻撃リスクの特性	対応及び対策の考慮事項
攻撃者の存在と多様な攻撃目的 サイバー攻撃は、自然災害等とは異なり、目的を持った攻撃者によって引き起こされる。その攻撃目的は、金銭・情報の窃取、主義・主張の表明、システム破壊によるサービスの停止等多様化している。組織的に計画されて行われる攻撃から内部犯行による攻撃まで、多様な攻撃者・攻撃目的に応じた様々な手法による攻撃が考えられるが、事前に攻撃者や攻撃目的を知ることは困難なケースが多い。	
攻撃手口の高度化 サイバー攻撃の手口は絶えず考え出され高度化している。新たな脆弱性を狙った攻撃のように現行技術をベースとした対策だけでは回避困難な攻撃や、事業者側が想定していない新しい手口で行われる攻撃等が考えられる。また、新しい手口で攻撃が行われた場合、その影響の度合や範囲を正確に把握できない可能性がある。	
執拗な攻撃が行われる可能性 サイバー攻撃は、その目的が達成されるまで執拗に行われる可能性がある。システム復旧の際、被害に遭う以前の状態に漫然と戻した場合にまた同じ攻撃が行われ被害を受けるケースや、システム復旧対応中に再度攻撃が行われるケース、攻撃への対処後にそれを回避する方法で再度攻撃が行われるケースも考えられる。また、インターネットに接続していないクローズド環境で運用される汎用性の低いシステムであっても、そのシステム仕様やシステム構成、内部ネットワーク等に関する情報を様々な手段で時間をかけて収集したうえで攻撃が行われるケース等も考えられる。	
同時多発的な攻撃が行われる可能性 サイバー攻撃では物理的な距離に関係なく、広範囲にわたるターゲットを同時に攻撃することが可能である。自組織の複数の拠点に同時に攻撃が行われるケースや、自組織のシステムとサプライヤーのシステムに同時に攻撃が行われるケース、メインシステムと非常用システムに同時に攻撃が行われるケース等が考えられる。	

サイバー攻撃リスクの特性	対応及び対策の考慮事項
検知が困難な攻撃が行われる可能性 サイバー攻撃に対して十分な検知策を講じていない場合、攻撃を認識できず長期間にわたり攻撃を受け続ける可能性がある。不正行為の検知に繋がるログを削除して回避しようとするケースや、実態とは異なる数値を表示して正常に動作しているように見せかけ不正行為を行うケース等も存在し、検知が遅れるほど被害が拡大する可能性が高くなる。また、攻撃を検知した以後も、攻撃者及び攻撃目的を特定するのは困難なケースが多い。	
急速な被害拡大に繋がる攻撃が行われる可能性 サイバー攻撃の被害は、攻撃を受けた箇所を起点にネットワークを介して急速に拡大する可能性がある。特定の端末に感染したマルウェアが同一組織内のネットワーク上にある別の端末に自身を複製することで被害が広がるケースや、外部委託先で発生したサイバー攻撃の被害が自社システムにまで広がるケース、自社システムが不正に操作され他社への攻撃に利用されることで自らが加害者の立場になってしまうケース等も考えられる。	
誤った判断や対処を誘発する攻撃が行われる可能性 サイバー攻撃によって、誤った判断や対処が誘発される可能性がある。例として、管理システムに実態と異なるアラートや数値を表示して判断を誤らせるケースや、障害対応時のシステム操作が意図しない動作を引き起こすようにシステムを不正変更（数値を上げる操作で数値が下がる、システム停止の操作でシステムが停止しない等）するケース等が考えられる。	