我が国におけるサイバーセキュリティ政策について

内閣官房
内閣サイバーセキュリティセンター(NISC)
中溝和孝
2025年３月10日

サイバー攻撃の変遷

■ サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大している。

サイバー攻撃の巧妙化・深刻化

公開サーバへの攻撃

ウェブサーバ・外向けサービスへの大量送信　等

エストニア・2007年

ウェブサイト等の停止

IT系システムの侵害

情報システム内部への侵入・暗号化
（主に既知の脆弱性を悪用）

WannaCry・2017年
コロニアルパイプライン・2021年
大阪急性期・総合医療センター・2022年

システム障害
身代金要求

有事に備えた重要インフラ等への侵入

最深部・制御系システムに至る高度な侵入能力
（ゼロデイ脆弱性の積極活用など）
高度な潜伏能力
（システム内寄生戦術(Living-off-the-Land)など）

ウクライナ・2015年/2022年等
Volt Typhoon・2023年

インフラ機能停止

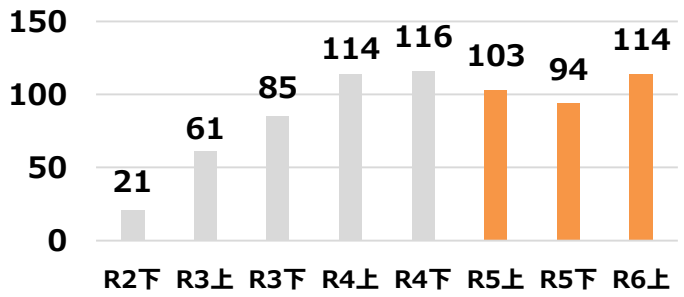
サイバー攻撃関連通信や被害の量

NICTが観測したサイバー攻撃関連通信数（※）の推移

※NICTの観測用IPアドレス約29万に届いたパケットの数。

（出典）国立研究開発法人情報通信研究機構「NICTER観測レポート2023」を基に作成

企業・団体等におけるランサムウェア（※）被害の報告件数の推移



※データを暗号化して身代金を要求するマルウェア。

（出典）警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について（2024年９月19日）」を基に作成

2024年のサイバーインシデント

○…国内　□…海外

○ 親ロシア派ハクティビストによる日本への攻撃示唆（2024年２月）

NoName057(16)等のハクティビストグループが犯行を示唆する投稿。日本及び日本の組織に対する攻撃を実施したと主張。

○ 鹿児島県医療生活協同組合 国分生協病院のシステム障害（2024年３月）

ランサムウェア攻撃により、画像管理サーバに障害が発生し、救急及び一般外来の受入について一部制限を実施。

○□ 太陽光発電施設へのサイバー攻撃（2024年５月）

コンテック社製太陽光発電計測監視装置の脆弱性(2021年以降複数存在)を悪用され、約800台がサイバー攻撃を受け、インターネットバンキングの不正送金に悪用されていたことが判明。

○ JR東日本のシステム障害（2024年５月）

「モバイルSuica（スイカ）」や、インターネット予約サービス「えきねっと」などで５月10日午後5時半ごろからアクセスしづらい状況が発生し、同10時ごろには大部分が復旧。運行への影響はなかった。通常とは異なるアクセスが多数検知されており、サイバー攻撃を受けたと判断。

○ DMM Bitcoin社からのビットコイン流出（2024年５月）

暗号資産交換業者DMM Bitcoin社において、利用者から預かっているビットコイン4,502.9BTC（約294,000,000ドル）が流出する事案が発生。

○ ニコニコサービスへのサイバー攻撃（2024年６月）

ニコニコサービスを運営する角川がランサムウェア攻撃を受けサービスが停止したほか、「Black Suits」により脅迫を受け、データ（1.5TB）が公開された。

○□ CrowdStrike社製ソフトウェアに起因するWindowsの障害（2024年７月）

米国CrowdStrike社のソフトウェアが原因でWindowsがブルースクリーン状態になり、使用できなくなる状況が世界的に発生。米マイクロソフト社の推定では全世界で850万台の端末で影響を受けた。鉄道、航空、金融をはじめとする多くの企業で業務に支障が生じた。

○ JAXAへの不正アクセス事案（2024年７月）

外部からJAXA内の業務用イントラネットの管理用サーバーに不正アクセスが行われた可能性があった旨を公表。

○ 重要インフラへのDDoS攻撃事案（2024年12月～2025年１月）

JAL、三菱UFJ銀行、みずほ銀行、りそな銀行、三井住友カード及びNTTドコモなどに対してDDoS攻撃があり、各社のシステムやサービスに障害が発生。

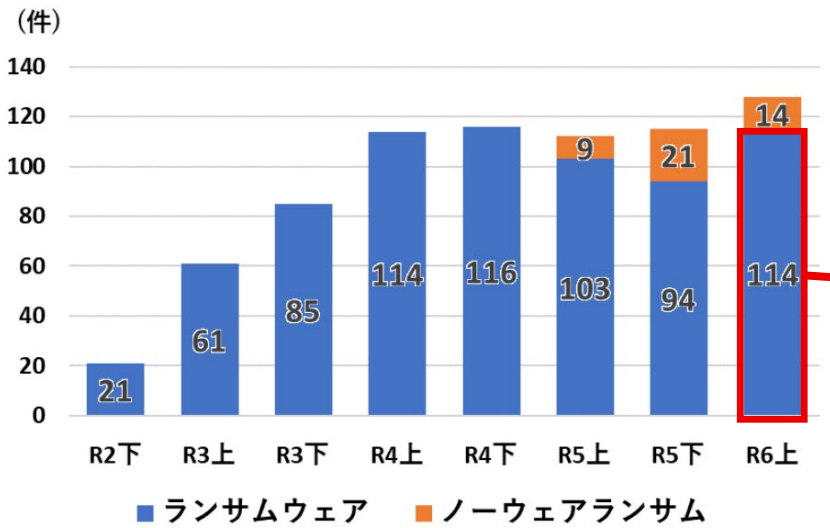
※2025年2月4日、DDoS 攻撃への対策について（注意喚起）（https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf）

企業が受けるサイバーリスク：ランサムウェア

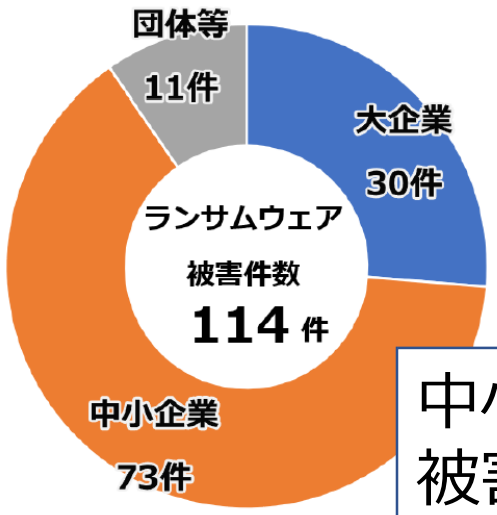
ランサムウェア

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可にし、その**解除と引換えに金銭を要求**する。
- 企業のサービスが停止する、個人情報が漏えいするなどの甚大な被害に繋がることもある。
- 2024年(令和6年)上半期に全国の都道府県警察から警察庁に報告があった件数は**114件**であり、前年と同じく高い水準で推移。
- 被害件数(114件)の内訳は、**大企業が30件（26%）**に対して、**中小企業は73件（58%）と過半数**。

企業・団体等におけるランサムウェア被害の報告件数の推移



ランサムウェア被害の被害企業・団体等の規模別報告件数（令和6年上半期）



中小企業の
被害が過半数

出典：警察庁「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について（2024年９月19日）」

最近のサイバー事案

国家関連の攻撃グループによるサイバー攻撃

- 2025年１月、NISC及び警察庁は、2019年頃から、中国の関与が疑われるサイバー攻撃グループ「MirrorFace」（ミラーフェイス）が、我が国の個人や組織に対し、情報窃取を目的としたサイバー攻撃を行っている旨公表し、MirrorFaceによるサイバー攻撃の手口や、攻撃の検知策と緩和策を解説した注意喚起を発出した。

- 2024年12月、警察庁は、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）と連名で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）が、DMM Bitcoinから当時約482億円相当の暗号資産を窃取したことを特定した旨公表した。
- 同日、NISC、警察庁及び金融庁は、標的となり得る組織・事業者向けに、TraderTraitor による暗号資産窃取等の手口の例や、リスク低減のための対処例・緩和策を解説した注意喚起を発出した。

令和７年１月８日
警察庁
内閣サイバーセキュリティセンター

MirrorFace によるサイバー攻撃について（注意喚起）

警察庁及び内閣サイバーセキュリティセンターでは、2019 年頃から現在に至るまで、日本国内の組織、事業者及び個人に対する、以下のサイバー攻撃キャンペーンが、「MirrorFace」（ミラーフェイス）（別名、「Earth Kasha」（アース カシャ））と呼ばれるサイバー攻撃グループによって実行されたと評価しています。

1 2019 年から 2023 年にかけて、主に我が国のシンクタンク、政府（退職者含む）、政治家、マスコミに関係する個人や組織に対し、不正なプログラム（マルウェア）を添付したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されました。（以下「攻撃キャンペーンA」とします。）
2 2023 年頃から、インターネットに接続されたネットワーク機器に対し、ソフトウェアのぜい弱性を悪用して標的ネットワーク内に侵入するサイバー攻撃が確認されました。主な標的は我が国の半導体、製造、情報通信、学術、航空宇宙の各分野でした。（以下「攻撃キャンペーンB」とします。）
3 2024 年６月頃から、主に我が国の学術、シンクタンク、政治家、マスコミに関係する個人や組織に対して、マルウェアをダウンロードするリンクを記載したメールを送信してマルウェアに感染させ、情報窃取を試みるサイバー攻撃が確認されています。（以下「攻撃キャンペーンC」とします。）

令和６年 12 月 24 日
警察庁
内閣サイバーセキュリティセンター
金融庁

北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃について
（注意喚起）

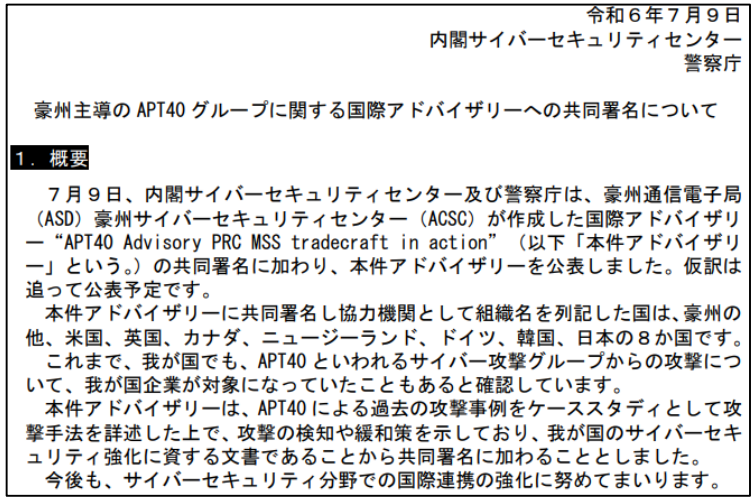
本日（令和６年 12 月 24 日）、警察庁、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）は連名で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）が、暗号資産関連事業者「株式会社 DMM Bitcoin」から約 482 億円相当の暗号資産を窃取したことを特定したと公表しました。

TraderTraitor に関しては、米国では令和４年４月 18 日に、FBI、米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）及び米国財務省の連名で注意喚起が行われています。また、TraderTraitor は、北朝鮮当局の下部組織とされる「Lazarus Group」（ラザルスグループ）の一部とされていますところ、Lazarus Group については、我が国でも同年 10 月 14 日に、金融庁、警察庁及び内閣サイバーセキュリティセンターの連名で「「ラザルス」と呼称されるサイバー攻撃グループ」として既に一度注意喚起を行うなど、累次にわたり注意喚起が行われている状況にあります。

最近のサイバー事案（つづき）

国家関連の攻撃グループによるサイバー攻撃（つづき）

- 2024年７月、NISCは、中国の国家的な支援を受けるサイバー攻撃グループである「APT40」による過去の攻撃事例を参考として攻撃手法を説明した上で、攻撃の検知手法や緩和策を提言する国際アドバイザリー（注意喚起）に共同署名し、公表。
（日・米・英・加・豪・NZ・独・韓が署名）



令和６年７月９日
内閣サイバーセキュリティセンター
警察庁

豪州主導の APT40 グループに関する国際アドバイザリーへの共同署名について

１．概要

７月９日、内閣サイバーセキュリティセンター及び警察庁は、豪州通信電子局（ASD）豪州サイバーセキュリティセンター（ACSC）が作成した国際アドバイザリー“APT40 Advisory PRC MSS tradecraft in action”（以下「本件アドバイザリー」という。）の共同署名に加わり、本件アドバイザリーを公表しました。仮訳は追って公表予定です。

本件アドバイザリーに共同署名し協力機関として組織名を列記した国は、豪州の他、米国、英国、カナダ、ニュージーランド、ドイツ、韓国、日本の８か国です。

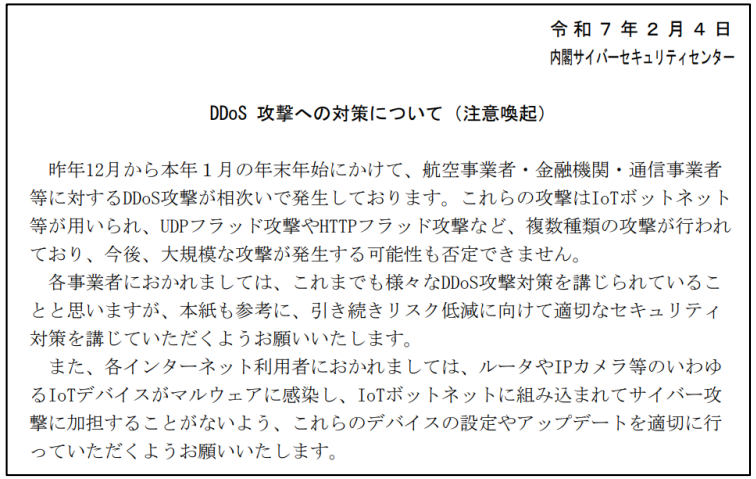
これまで、我が国でも、APT40 といわれるサイバー攻撃グループからの攻撃について、我が国企業が対象になっていたこともあると確認しています。

本件アドバイザリーは、APT40 による過去の攻撃事例をケーススタディとして攻撃手法を詳述した上で、攻撃の検知や緩和策を示しており、我が国のサイバーセキュリティ強化に資する文書であることから共同署名に加わることとしました。

今後も、サイバーセキュリティ分野での国際連携の強化に努めてまいります。

重要インフラ等へのDDoS攻撃事案

- 昨年末から本年１月の年末年始にかけて、複数の重要インフラ等を対象としたDDoS攻撃が発生し、一部サービスに支障が出るなどの影響が生じたことなどを受け、本年２月に、DDoS攻撃に対する具体的なリスク低減に向けたセキュリティ対策を含む注意喚起を公表。



令和７年２月４日
内閣サイバーセキュリティセンター

DDoS 攻撃への対策について（注意喚起）

昨年12月から本年１月の年末年始にかけて、航空事業者・金融機関・通信事業者等に対するDDoS攻撃が相次いで発生しております。これらの攻撃はIoTボットネット等が用いられ、UDPフラッド攻撃やHTTPフラッド攻撃など、複数種類の攻撃が行われており、今後、大規模な攻撃が発生する可能性も否定できません。

各事業者におかれましては、これまでも様々なDDoS攻撃対策を講じられていることと思いますが、本紙も参考に、引き続きリスク低減に向けて適切なセキュリティ対策を講じていただくようお願いいたします。

また、各インターネット利用者におかれましては、ルータやIPカメラ等のいわゆるIoTデバイスがマルウェアに感染し、IoTボットネットに組み込まれてサイバー攻撃に加担することがないよう、これらのデバイスの設定やアップデートを適切に行っていただくようお願いいたします。

今後のサイバーセキュリティ対策強化の方向

＜国家安全保障戦略（抜粋）　（令和４年12月16日閣議決定）＞

サイバー安全保障分野での対応能力の向上

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

具体的には、**まずは、**最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを**常時評価**し、政府機関等の脅威対策やシステムの脆弱性等を**随時是正するための仕組みを構築する。**その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、外交・防衛・情報の分野を始めとする政府機関等のシステムの導入から廃棄までのライフサイクルを通じた**防御の強化、政府内外の人材の育成・活用の促進等を引き続き図る。**

その上で、**武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。**

そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

(ｱ) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

(ｲ) 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

(ｳ) 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。これらの取組は総合的な防衛体制の強化に資するものとなる。

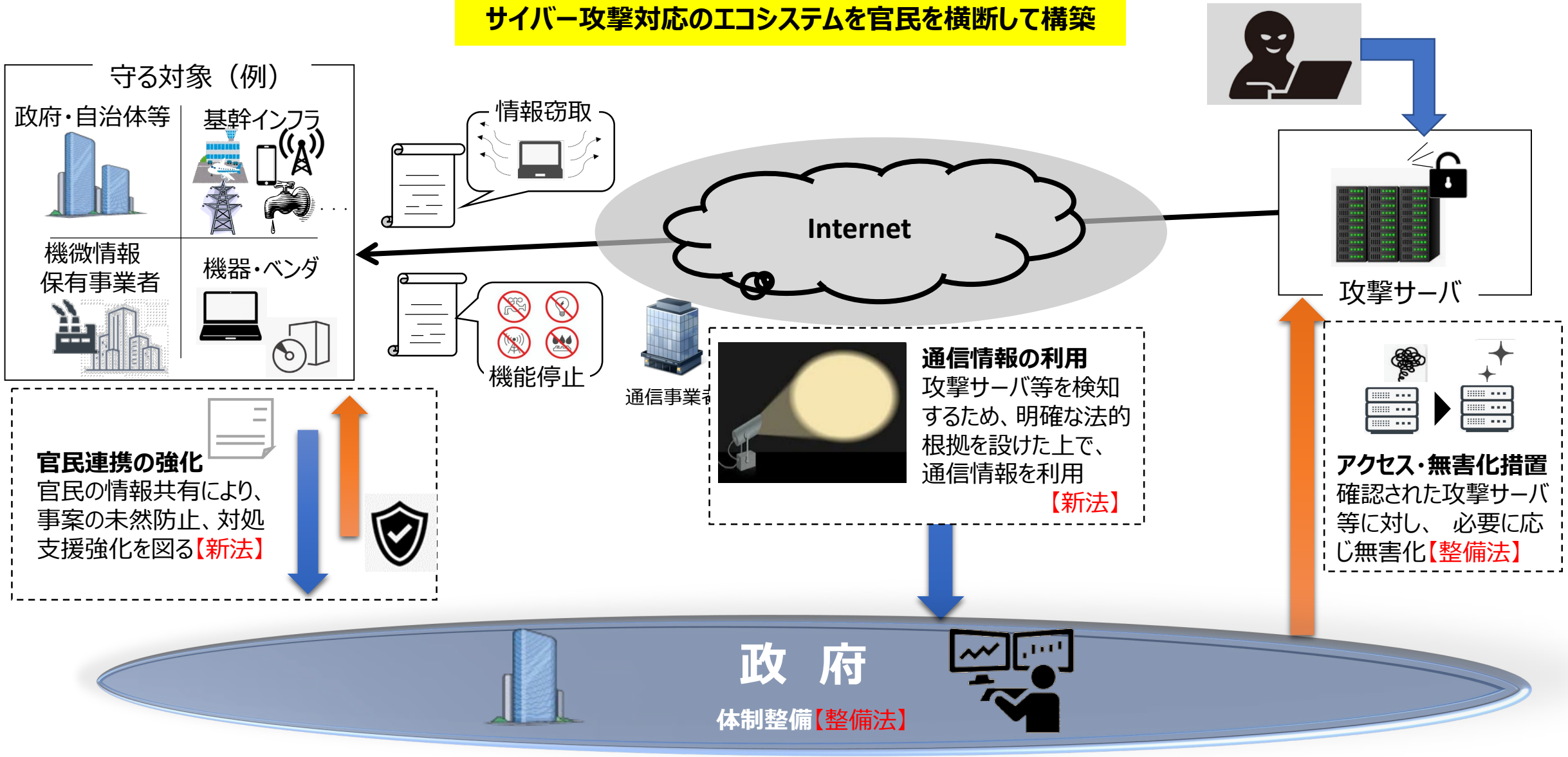
また、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化する。

さらに、同盟国・同志国等と連携した形での情報収集・分析の強化、攻撃者の特定とその公表、国際的な枠組み・ルールの形成等のために引き続き取り組む。

法案の全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。

全てのステイクホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを官民を横断して構築



重要電子計算機に対する不正な行為による被害の防止に関する法律案 及び 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案　概要

趣　旨

● 国家安全保障戦略（令和４年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④***NISC*の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。

● 国家安全保障戦略に掲げられたこれら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、サイバー安全保障分野での対応能力の向上に向けた有識者会議を開催（令和６年６月７日～11月29日）、「サイバー安全保障分野での対応能力の向上に向けた提言」を取りまとめ。

→　これらを踏まえ、「新法」及び「整備法」として必要な法制度を整備。

概　要

官　民　連　携　（新法）

- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告
- 情報共有・対策のための協議会の設置
- 脆弱性対応の強化

通信情報の利用　（新法）

- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得
- （同意によらない）通信情報の取得
- 自動的な方法による機械的情報の選別の実施
- 関係行政機関の分析への協力
- 取得した通信情報の厳格な取扱い
- 独立機関による事前審査・継続的検査　等

→ 分析情報・脆弱性情報の提供等

アクセス・無害化措置　（整備法）

- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等

（警察官職務執行法改正）

- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・在日米軍が使用するコンピュータ等の警護（権限は上記を準用）

等

（自衛隊法改正）

組織・体制整備等　（整備法）

- サイバーセキュリティ戦略本部の改組　（サイバーセキュリティ基本法改正）
- サイバーセキュリティ戦略本部の機能強化　（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設　（内閣法改正）　等

施行期日

公布の日から起算して１年６月を超えない範囲内において政令で定める日　等

今後のサイバーセキュリティ対策強化の方向

＜国家安全保障戦略（抜粋）　（令和４年12月16日閣議決定）＞

サイバー安全保障分野での対応能力の向上

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

具体的には、**まずは、**最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを**常時評価**し、政府機関等の脅威対策やシステムの脆弱性等を**随時是正するための仕組みを構築する。**その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、外交・防衛・情報の分野を始めとする政府機関等のシステムの導入から廃棄までのライフサイクルを通じた**防御の強化、政府内外の人材の育成・活用の促進等を引き続き図る。**

その上で、**武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。**

そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

(ｱ) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

(ｲ) 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

(ｳ) 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。これらの取組は総合的な防衛体制の強化に資するものとなる。

また、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化する。

さらに、同盟国・同志国等と連携した形での情報収集・分析の強化、攻撃者の特定とその公表、国際的な枠組み・ルールの形成等のために引き続き取り組む。

NISCの取組の強化

■ 2024年７月以降、NISCは**体制を抜本的に強化**（幹部職員増強、定員倍増）。

■ サイバーセキュリティ戦略及び国家安全保障戦略を踏まえ、**セキュリティ監視、民間との対話、国際連携の強化に向けた施策を順次実施中**。

①セキュリティ監視強化

・**横断的アタックサーフェスマネジメント（ASM）事業の運用開始**（2024年７月から順次実施）

全ての府省庁(26府省庁)に加え、全ての独立行政法人(87法人)と一部の指定法人(９法人)を対象として、攻撃者の視点に立って、インターネットに公開されているサーバやネットワーク機器などの状態を網羅的に調査・評価し、脆弱性等を随時是正。

※国家安全保障戦略において、「政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する」とされている。

②民間企業との連携強化

・**「サイバーセキュリティの確保に向けた企業経営層向け意見交換会」の開催**（2024年７月）

大臣出席の下、様々な分野の企業等の経営層（約200名）が参加（経団連と共催）。昨今のサイバー情勢や最近の事例を紹介しつつ、我が国のサイバーセキュリティの強靱化のためには、経営トップのリーダーシップによる対策の着実な実施が重要であることなど、企業経営層と問題意識を共有。

③国際連携の強化

・**脅威検知等のためのベストプラクティスへの共同署名**（2024年８月）

検知が困難とされるシステム内寄生戦術（Living Off The Land。マルウェア（不正なソフトウェア）ではなく被害システムの正規のツールを使うことで監視・検知を回避する手法。）への技術的な対策を紹介するベストプラクティス集に共同署名（米・英・加・豪・NZ・星・韓・蘭）。

・**エッジデバイスのための緩和戦略への共同署名**（2025年２月）

エッジデバイスを標的とした攻撃が増加していることを踏まえ、リスク緩和のための７つの戦略を提供する国際文書に共同署名（日・米・英・加・豪・NZ・韓・蘭・チェコ）。

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について

社会全体へのDXの浸透や、AI・量子技術等の進展により、急速に変化するサイバー空間をめぐるリスクに対応するため、「サイバーセキュリティ戦略」（特にサイバーセキュリティ2024における「特に強力に取り組む施策」）及び「サイバー安全保障分野での対応能力の向上に向けた提言」等を踏まえ、現行制度下において喫緊に取り組むべき事項について検討し、対処方針を示す。

サイバーセキュリティ2024（特に強力に取り組む施策）

- 政府機関や重要インフラ等の対処能力の向上
- サプライチェーン・リスクへの対応強化
- DXを推進・支援する取組の強化
- 欧米主要国をはじめとする関係国との連携の一層の強化

等

サイバー安全保障分野での対応能力の向上に向けた提言（横断的課題等）

- 政府機関や重要インフラ事業者等の対策強化
- サイバーセキュリティ人材の育成・確保
- 中小企業や地域における対策強化
- 国産セキュリティ製品・サービスの供給強化
- 被害組織の負担軽減（報告様式一元化）

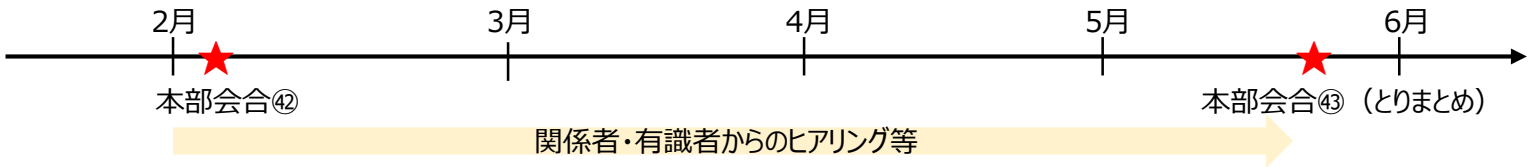
等

検討事項（案）

- 政府機関・重要インフラ事業者等の対応能力の向上
- 社会全体のサイバーセキュリティ確保
  - 官民連携の強化
  - セキュアバイデザイン・セキュアバイデフォルト原則等を踏まえた対策強化
  - 中小企業のサイバーセキュリティ対策の促進
- 国際連携の一層の強化
- 横断的施策の推進
  - サイバーセキュリティ人材の育成・確保
  - 我が国のサイバーセキュリティ技術の研究開発・活用及び産業振興・育成（研究開発・社会実装の推進等）

年次計画への反映
中長期的課題の整理

今後のスケジュール



サイバー攻撃　今、そこにあるリスク～経営トップがすべきこと～

被害を予防するため、企業経営層に知っておいていただきたいサイバーセキュリティの要点を、短い動画10本で紹介。

https://security-portal.nisc.go.jp/guidance/for-executives/
https://www.youtube.com/watch?v=4k7WFjqn9F0&list=PLfDHJFHUbJOI8s-xOgpieyE5hgsI3rPpF

事例で学ぶサイバーリスクマネジメント ～経営トップがすべきこと 実践編～

経営層向けコンテンツ第二弾。具体的な事例を盛り込み、
対策へのヒントを３本の動画で紹介。

https://security-portal.nisc.go.jp/guidance/executives2/index.html
https://www.youtube.com/watch?v=jufdymQufEY&list=PLfDHJFHUbJOJkWm7UAqxdHByb3wPmIvnS

セキュリTT兄弟のサイバーセキュリティパンフレット

中小企業向けの基本的なサイバーセキュリティ対策を、分かりやすい漫画風にまとめたパンフレット。
自由にダウンロードし、印刷・配布も可能。

https://security-portal.nisc.go.jp/guidance/pamphlet2025.html

インターネットの安全・安心ハンドブック中小企業等向け抜粋版

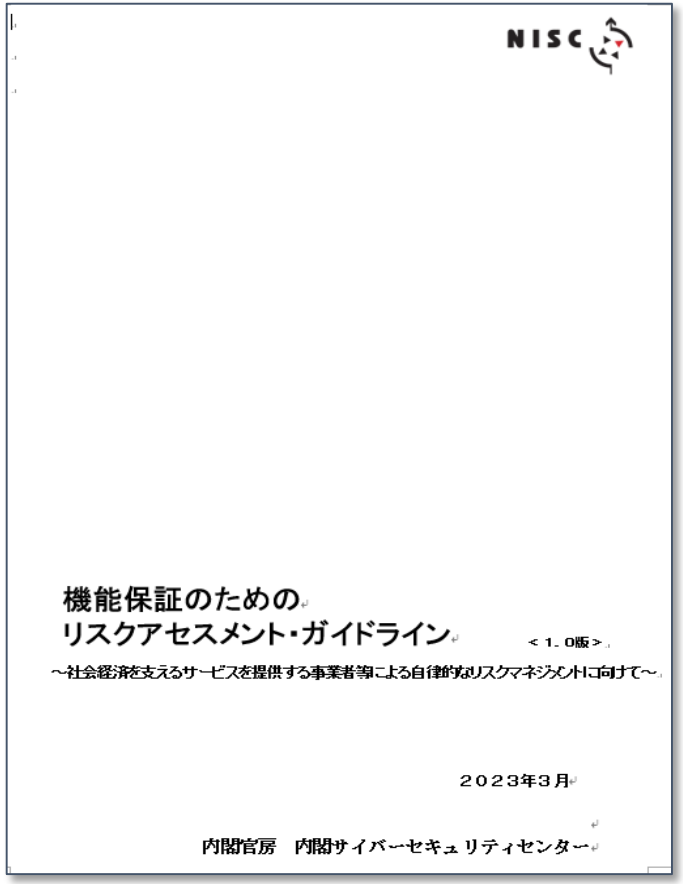
「インターネットの安全・安心ハンドブック」から中小企業向けの要素を抜粋した冊子。

https://security-portal.nisc.go.jp/guidance/handbook.html

サイバー攻撃から企業を守るために。リスクアセスメントの実施に向けて

- リスクアセスメントは自組織のリスクを把握するサイバーセキュリティに係わる第１歩の取組です。
- リスクアセスメントの重要性を認識しながらも、具体的にどのように進めたらよいかが分からないなどの理由により、実施できていない事業者等も多く存在しており、リスクアセスメントの考え方や実施方法がしっかりと定着しているとは言い難い状況です。
- NISCでは、こうした状況を踏まえ、情報セキュリティに係るリスクアセスメントの実施方法についての具体的な手順を含む基礎的なフレームワーク(*1)を提供しています。サイバー攻撃から企業を守るために、経営層主導のリスクアセスメントの実施に向けて、是非ご活用ください。

(*1) https://www.nisc.go.jp/policy/group/cyber/policy.html　よりダウンロード可能

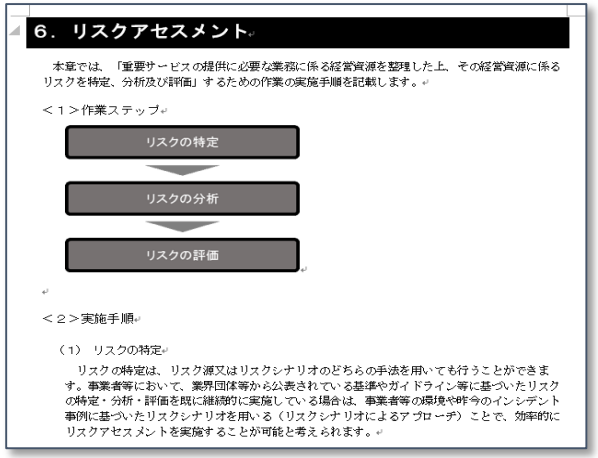

NISC

機能保証のための
リスクアセスメント・ガイドライン　＜１.０版＞

～社会経済を支えるサービスを提供する事業者等による自律的なリスクマネジメントに向けて～

2023年3月

内閣官房　内閣サイバーセキュリティセンター


6．リスクアセスメント

本章では、「重要サービスの提供に必要な業務に係る経営資源を整理した上、その経営資源に係るリスクを特定、分析及び評価」するための作業の実施手順を記載します。

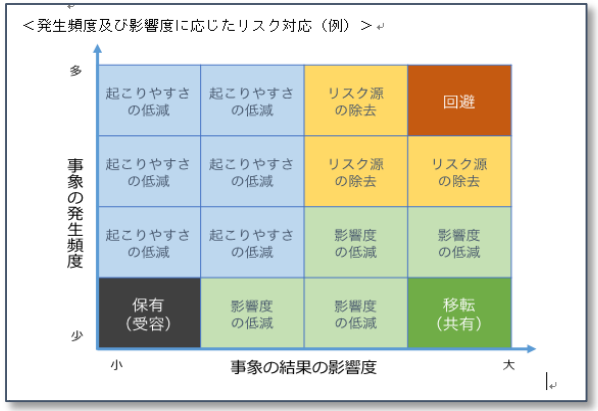
＜１＞作業ステップ

リスクの特定
リスクの分析
リスクの評価

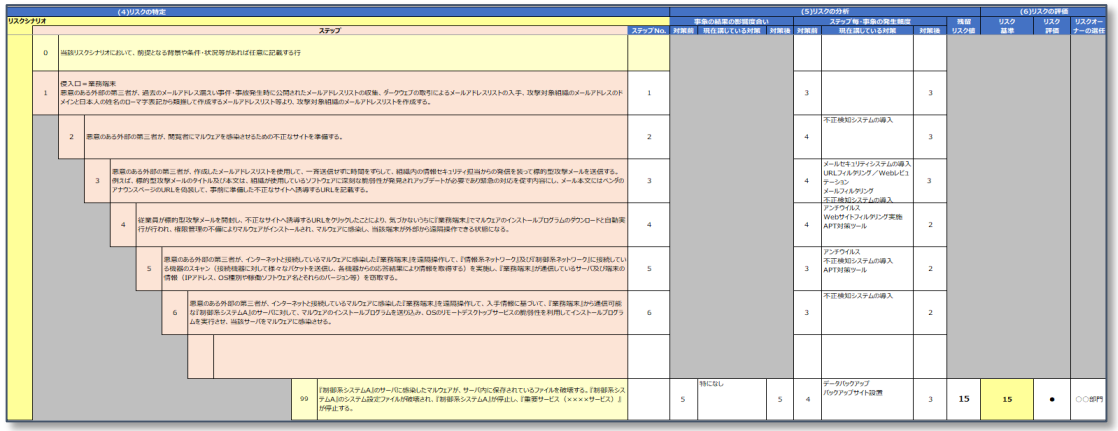
＜２＞実施手順

（１） リスクの特定

リスクの特定は、リスク源又はリスクシナリオのどちらの手法を用いても行うことができます。事業者等において、業界団体等から公表されている基準やガイドライン等に基づいたリスクの特定・分析・評価を既に継続的に実施している場合は、事業者等の環境や昨今のインシデント事例に基づいたリスクシナリオを用いる（リスクシナリオによるアプローチ）ことで、効率的にリスクアセスメントを実施することが可能と考えられます。


＜発生頻度及び影響度に応じたリスク対応（例）＞

事象の発生頻度 ↑多	小			大 事象の結果の影響度
多	起こりやすさの低減	起こりやすさの低減	リスク源の除去	回避
	起こりやすさの低減	起こりやすさの低減	リスク源の除去	リスク源の除去
	起こりやすさの低減	起こりやすさの低減	影響度の低減	影響度の低減
少	保有（受容）	影響度の低減	影響度の低減	移転（共有）


(4)リスクの特定 / (5)リスクの分析 / (6)リスクの評価

リスクシナリオ	ステップ	ステップNo.	(5)リスクの分析 事象の結果の影響度合い 対策前	現在講じている対策	対策後	ステップ毎・事象の発生頻度 対策前	現在講じている対策	対策後	残留リスク値	(6)リスクの評価 リスク基準	リスク評価	リスクオーナーの設定
0	当該リスクシナリオにおいて、前提となる背景や条件・状況等があれば任意に記載する行											
1	侵入口＝業務端末 悪意のある外部の第三者が、過去のメールアドレス漏えい事件・事故発生時に公開されたメールアドレスリストの収集、ダークウェブの取引によるメールアドレスリストの入手、攻撃対象組織のメールアドレスのドメインと日本人の姓名のローマ字表記から類推して作成するメールアドレスリスト等より、攻撃対象組織のメールアドレスリストを作成する。	1				3		3				
2	悪意のある外部の第三者が、閲覧者にマルウェアを感染させるための不正なサイトを準備する。	2				4	不正検知システムの導入	3				
3	悪意のある外部の第三者が、作成したメールアドレスリストを使用して、一斉送信かつ巧妙な手口で、組織内の情報セキュリティ担当からの発信を装って標的型攻撃メールを送信する。 例えば、標的型攻撃メールのタイトルや本文では、組織が使用しているソフトウェアに深刻な脆弱性が発見されアップデートが必要であり緊急の対応を促す内容にし、メール本文にはヘンタイのアナウンスページのURLを仕込んで、事前に準備した不正なサイトへ誘導するURLを記載する。	3				4	メールセキュリティシステムの導入 URLフィルタリング／Web レピュテーション メールフィルタリング 不正検知システムの導入	3				
4	従業員が標的型攻撃メールを開封し、不正なサイトへ誘導するURLをクリックしたことにより、気づかないうちに『業務端末』にマルウェアのインストールプログラムのダウンロードと自動実行が行われ、権限管理の不備によりマルウェアがインストールされ、マルウェアに感染し、当該端末が外部から遠隔操作できる状態になる。	4				4	アンチウイルス Webサイトフィルタリング実施 APT対策ツール	2				
5	悪意のある外部の第三者が、インターネットと接続しているマルウェアに感染した『業務端末』を遠隔操作して、『情報系ネットワーク』及び『制御系ネットワーク』に接続している機器のスキャン（接続機器に対して様々なパケットを送信し、具体機器からのOS等結果により情報を取得する）を実施し、『業務端末』が通信しているサーバ及び端末の情報（IPアドレス、OS種別や稼働ソフトウェアおよびそれらのバージョン等）を窃取する。	5				3	アンチウイルス 不正検知システムの導入 APT対策ツール	2				
6	悪意のある外部の第三者が、インターネットと接続しているマルウェアに感染した『業務端末』を遠隔操作して、入手情報に基づいて、『業務端末』から通信可能な『制御系システムA』のサーバに対して、マルウェアのインストールプログラムを送り込み、OSのリモートデスクトップサービスの脆弱性を利用してインストールプログラムを実行させ、当該サーバをマルウェアに感染させる。	6				3	不正検知システムの導入	2				
99	『制御系システムA』のサーバに感染したマルウェアが、サーバ内に保存されているファイルを破壊する。『制御系システムA』のシステム設定ファイルが破壊され、『制御系システムA』が停止し、『重要サービス（×××サービス）』が停止する。		5	特になし	5	4	データバックアップ バックアップサイト設置	3	15	15	●	○○部門

リスクアセスメントの実施方法や手順等、疑問・ご不明な点がございましたら、下記までお気軽にお問合せください。

＜担当＞
内閣官房　内閣サイバーセキュリティセンター
対処・外部連携ユニット　リスクマネジメントチーム
メール：riskassess2020-ot4yi@cyber.go.jp

ご清聴ありがとうございました

https://www.nisc.go.jp