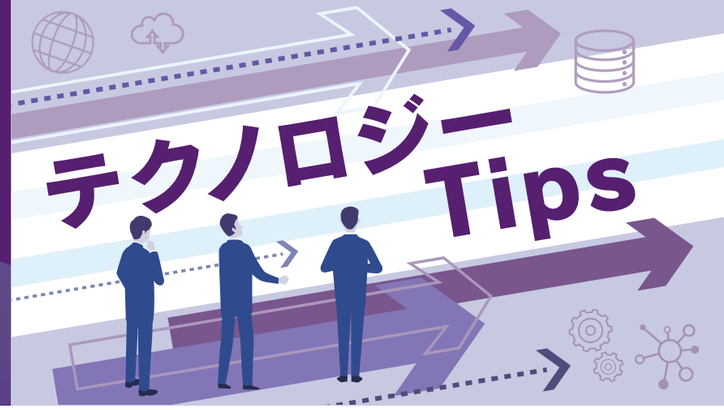
今こそ知りたい Tech Tips!
vol.22 (Ver2.0)

2025年 情報セキュリティ10大脅威

IPA(独立行政法人情報処理推進機構)のWebサイトを参考に、2025年の情報セキュリティのリスクトピックスを整理します。

2024 年、社会的に影響が大きかったセキュリティ上の脅威について「10 大脅威選考会」の投票結果に基づいたTOP10を知り、対策を徹底しましょう!



2025年の脅威ランキング

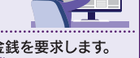
		初選出年	連続/通算
1	ランサム攻撃による被害	2016年	10年連続 10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続 7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続 8回目
4	内部不正による情報漏えい等	2016年	10年連続 10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続 10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続 5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃(DDoS攻撃)	2016年	5年ぶり 6回目
9	ビジネスメール詐欺	2018年	8年連続 8回目
10	不注意による情報漏えい等	2016年	7年連続 8回目

上位にランクインした脅威と、数年ぶりにランクインし、昨年被害が大きく増加した脅威について、攻撃手口、対策、被害にあってしまった時の対応を詳しく説明します!

1 ランサム攻撃による被害

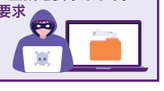
ランサムウェアとは、PCやサーバーなどの端末に感染し、データの暗号化や窃取を行い、金銭を要求する悪質なソフトウェア(マルウェア)の一種です。近年では、サービスとして提供されるランサムウェア(RaaS)や、データを暗号化せずに窃取のみを行う「ノーウェアランサム」といった手口も確認されています。

攻撃手口
- ●ソフトウェアの脆弱性を悪用したネットワークからの感染
- ●不正アクセスによるネットワークからの感染
- ●ウェブサイトやメールを介した感染(添付ファイル、不正なリンクなど)



脅威と影響

攻撃者は、以下のような脅迫を組み合わせて金銭を要求します。
- ●データの暗号化と復元を条件とした金銭要求
- ●窃取した機密情報の公開
- ●DDoS攻撃によるサービスの妨害
- ●感染した事実の利害関係者への通知



対策

組織として以下の対策を行うことが重要です。
- ●インシデント対応体制の整備 ●情報セキュリティ対策の実施
- ●多要素認証の導入 ●不審なソフトウェアの実行
- ●添付ファイルの開封を避ける ●適切なバックアップの実施

被害時の対応
- ●原則として身代金は支払わない
- ●適切な報告・連絡・相談を行う
- ●復旧業者の選定は慎重に行う、または復号ツールを活用する

2 サプライチェーンや委託先を狙った攻撃

企業間の「ビジネス上の繋がり」や、ソフトウェア開発における「ソフトウェアの繋がり」を悪用した攻撃です。取引先や委託先、ソフトウェアの提供元などを経由して、最終的な標的となる組織に間接的に侵入を試みます。

攻撃手口

セキュリティ対策が強固な組織でも、サプライチェーン上の脆弱な部分を突かれることで、機密情報の漏えいやサービスの停止、信用の失墜などの被害を受ける可能性があります。

脅威と影響
- ●取引先や委託先を攻撃し、標的組織の機密情報を窃取
- ●ソフトウェアやサービスにマルウェアを仕込み、標的組織に感染させる
- ●システム運用などを請け負う事業者を攻撃し、顧客にマルウェアを拡散させる

対策

①組織全体で
- ●インシデント対応体制の整備
- ●取引先や委託先のセキュリティ対策状況の確認
- ●セキュリティ評価サービスの活用 ●契約時のセキュリティ要件の明確化
- ●納品物のセキュリティ検証 ●情報セキュリティ認証の取得と維持

②委託先・取引先との連携
- ●連絡プロセスの確立 ●相互のセキュリティ対策状況の確認・監査
- ●公的機関の情報共有

3 リモートワーク等の環境や仕組みを狙った攻撃

リモートワークの普及に伴い、自宅などオフィス外から社内システムにアクセスする環境を狙ったサイバー攻撃が増加しています。

攻撃手口

VPN機器やリモートワーク用端末の脆弱性を悪用され、マルウェア感染や情報漏えい、不正アクセスなどの被害が発生する可能性があります。その結果、業務停止や遅延、信頼失墜などの深刻な影響が生じます。

脅威と影響
- ●リモートワーク用製品の脆弱性や設定ミスを悪用した攻撃
- ●アカウント情報の不正利用による侵入
- ●リモートワーク用端末へのマルウェア感染
- ●Web会議への潜入

対策

●従業員
- ●情報セキュリティ対策の基本を遵守
- ●組織のセキュリティポリシーに従う
- ●家庭用ネットワーク機器のセキュリティ対策

●組織
- ●インシデント対応体制の整備
- ●リモートワークのセキュリティポリシー策定
- ●セキュリティ対策を施したリモートワーク環境の導入
- ●従業員へのセキュリティ教育 ●多要素認証の導入

4 分散型サービス妨害攻撃(DDoS攻撃)

複数のコンピュータを不正に操作して、標的となるサーバーに大量のアクセスを集中させ、サービスを停止させる攻撃です。

攻撃手口

ウェブサイトの閲覧遅延やサービス停止を引き起こし、組織の事業活動や人々の日常生活に大きな支障をきたす可能性があります。

脅威と影響
- ●ボットネットを利用した大量アクセス
- ●制御パケットやUDPパケットを大量に送信するフラッド攻撃
- ●標的サーバーに応答を集中させるリフレクション攻撃
- ●DNSサーバーに負荷をかけるDNSランダムサブドメイン攻撃
- ●DDoS攻撃代行サービスの利用

対策

●ウェブサイト運営
- ●CDNの利用 ●WAF ●IDS/IPS ●DDoS対策サービスの導入
- ●システムの冗長化 ●ネットワークの冗長化
- ●代替サーバーの用意 ●公開サーバーの設定見直し
- ●IoT機器の脆弱性対策 ●IT資産の把握と対策

●サービス事業者
- ●公開サーバーの設定見直し ●IoT機器の脆弱性対策
- ●IT資産の把握と対策

本情報は、IPA(独立行政法人 情報推進機構 https://www.ipa.go.jp/)のWebサイトを参照し、参考にした情報です。またランキングを含めた情報は、以下のサイトに掲載のPDFを参考に編集させていただいております。https://www.ipa.go.jp/security/10threats/10threats2025.html

今年初めて7位ランクインした「地政学的リスクに起因するサイバー攻撃」について、詳しく説明しておきましょう。

Q ん？まず、「地政学」ってなんだ？？最近、よく目にするけど!?

A 地政学とは、地理的な条件が国家の政治や経済、
軍事戦略に与える影響を分析する学問のことだよ。整理してみましょう。

1. 地政学の基本的な考え方

地理的条件の重要性

国の位置や地形、気候、資源などは、その国の行動や国際関係に大きな影響を与えるんですよ。
例えば、海に囲まれた島国は、海洋資源や貿易ルートの確保をとても大事にするよね!?
また、資源が豊富な国は、その資源を巡って他の国との関係が複雑になることもあります。

国家の戦略

各国は、自分たちの地理的な条件を考えて、安全保障や経済発展のための戦略を立てています。
例えば、国境を接する国との関係や、貿易ルートの確保、資源の獲得などが重要な課題になります。

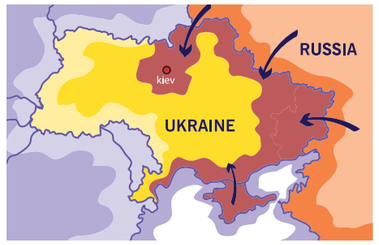
国際関係

地政学は、国家間の関係を理解するのにとても役に立つよ。
最近注目されている学問だね!
地理的な要因が、紛争や協力関係の背景にあることが多いことが窺い知れますね。

では、少し、最近の事例についても触れてみましょう。

❶ ウクライナ情勢

ウクライナは、ロシアとヨーロッパの間に位置していて、重要な地政学的な要衝なんです。ロシアはウクライナを自分たちの勢力圏に留めようとしていますし、ヨーロッパはウクライナを自分たちの陣営に取り込みたいと考えています。
だから、ウクライナ情勢はロシアとヨーロッパの対立を象徴する出来事になっているんです。



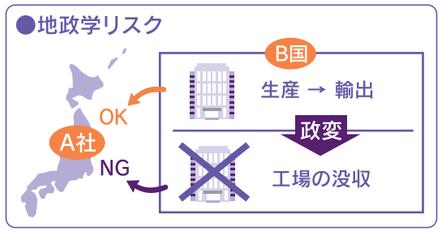
❷ 日本のエネルギー安全保障

日本は資源が少なく、エネルギーのほとんどを輸入に頼っています。だから、中東からの石油や天然ガスの安定供給を確保することがとても重要な課題なんです。
そして、シーレーン（海上交通路）の確保は日本にとって生命線とも言えるんですよ。

地政学リスクについても簡単にふれておくね！地政学リスクってのは、世界の政治的な問題や争いが原因で、会社が損しちゃったり、困ったりする可能性のことなんだ！

例えば、こんな例を考えてみよう。

A社は、海外のB国に工場を持っていて、
そこで作った製品を日本に輸入しているとするね。
ある日B国で「政変」が起きて、新しい政府がA社の工場を没収しちゃった！
A社は工場を失って製品を作れなくなり、大損害を被ってしまう。
さらに、B国からの輸入が止まったことで、
日本でその製品が買えなくなって消費者も困るよね…



では本題です。「地政学的リスクに起因するサイバー攻撃」について説明します。

政治的な対立や報復を目的としたサイバー攻撃を行う国家が存在します。これらの国家は、競争優位性を確保するために他国の機密情報を窃取したり、外貨を獲得するためにサイバー攻撃を行ったりします。特に、経済制裁を受けている国家がサイバー攻撃で金銭を得ると、制裁の効果が薄れてしまう可能性があります。そのため、組織としては、これらの攻撃に備えて常に対策を強化することが重要です。

攻撃手口

- DDoS攻撃によるサービス妨害
- ランサムウェアによる業務停止や情報窃取
- フィッシングによるアカウント情報等の窃取
- ソーシャルエンジニアリングによる情報収集やマルウェア拡散
- 誹謗中傷やデマによる情報操作

対策

組織

- 地政学的リスクの情報収集
- インシデント対応体制の整備
- 多要素認証の導入
- バックアップの実施
- 従業員への地政学やセキュリティ教育実施

個人

- パスワードの適切な管理
- 不審なメールやリンクへの注意
- 自身の個人情報やスマホ
- パソコンなどの管理
- 不審なアプリ
- 海外サーバーへの注意

まとめるね！

国家戦略としてのサイバー攻撃は、高度な技術と潤沢な資金が基盤です。攻撃の標的は、政府機関、電力や交通、医療機関や施設など、生活の基盤インフラ、その国の主要産業や関連する大企業・中小企業まで、多岐にわたります。被害は甚大で、国民の生活、国家の安全保障、経済に深刻な影響を与えるに至ります。さらに、これらの攻撃は国家戦略の一環として目的を達成するまで数年かかったとしても、時間・労力・資金を惜しまず続くことになります。長期的かつ、国際的な協力体制の構築やセキュリティへの対策が必要とされます。まさに「人間とAIの関係」について世界のトップリーダーが議論しているのも、地政学リスクへの対策の1つです。

2025年もさらにセキュリティ脅威は増すばかりです！
AIやクラウド、インターネットに接続したり、
インターネット上の情報を閲覧、収集する機会は
さらに増していきます。パソコン、スマホ、ネットワーク、
インターネットを使う人、使う組織すべてに、
「セキュリティの義務」があると考えましょう。