NET ASSIST News Letter

サーバー・セキュリティサービスが築く、信頼と安心を情報発信する

News Letter

2026.03
vol.58

NET ASSIST
24/7 Guardian Deity

TOPICS

※TOPICSの各タイトルをクリックすると該当の記事へ飛びます

NEWS TOPICS 1

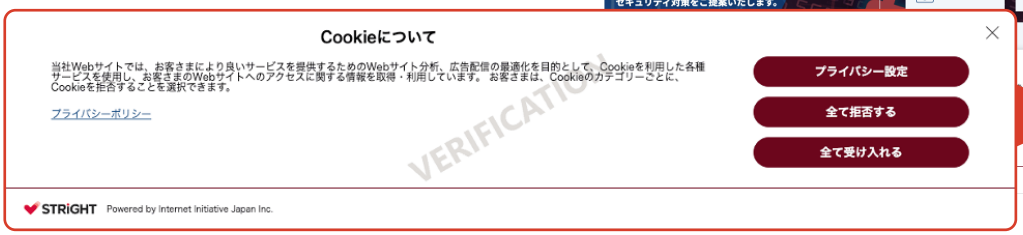
信頼されるサイト運営の新常識、Cookie同意管理ツール「STRiGHT」

Webご担当者様が今、最も注目すべき「プライバシー保護とCookie（クッキー）対策」について、新サービスのご紹介を交えてお届けします。（特別な無料キャンペーンもご用意しております！最後までご覧ください。）

なぜ今、Cookie対策が必要なのか？

Webサイトを閲覧した際にブラウザに保存される「Cookie」は、アクセス解析やログイン情報の保持に欠かせないデータです。

しかし近年、世界的なプライバシー保護規制の強化により、Cookieを収集・活用する際には、サイト利用者の適切な同意を得ることが強く求められるようになっています。



1 法規制の強化

欧州のGDPRだけでなく、日本でも2022年施行の「改正個人情報保護法」により、トラッキング等に対する同意取得が明確に義務化されました。

2 ブラウザの対応

SafariやFirefoxに続き、Google ChromeもサードパーティCookieを段階的に廃止する予定です。

3 ユーザー意識の変化

利用者の約7割がデータの使われ方に不安を感じており、強引に同意を迫るデザイン（ダークパターン）への批判も高まっています。こうした背景から、法規制に対応しつつユーザーの信頼を勝ち取る「CMP（Cookie同意管理ツール）」の導入が、Webサイト運営の必須条件になりつつあります。

オールインワンのCookie同意管理ツール「STRiGHT（ストライト）」

弊社が提供を開始した「STRiGHT」は、これらの課題を一挙に解決する高機能なCMPツールです。

STRiGHTの3つのポイント

Point 1

世界中の規制にこれひとつで対応

日本はもちろん、GDPR（欧州）やCCPA（米国カリフォルニア州）など、各国の規制に合わせた表示設定が可能です。

Point 2

「誠実なデザイン」で信頼性アップ

日本はもちろん、GDPR（欧州）やCCPA（米国カリフォルニア州）など、各国の規制に合わせた表示設定が可能です。

Point 3

圧倒的なコストパフォーマンス

月額換算9,800円（税別）の低コスト（※DAUU 500,000までの場合）で、外部送信スキャンや多言語対応などの充実した機能をご利用いただけます。

※DAUUは日次平均ユニークユーザー数です。

ご提供価格（税抜）

	ベーシックプラン	カスタムプラン
プラン内容	・オプトインバナーのみ　・カラーを自由に指定可能 ・表示位置を自由に指定可能　・日本語のみ対応	・バナーの種類が選択可能　・カラーを自由に指定可能 ・バナー文言を自由に指定可能　・表示位置を自由に指定可能 ・法域／年齢制限／多言語対応
初期費用	¥200,000～	¥400,000～
年間費用（DAUU 500,000まで）	¥117,600／年	

オプション　サポートプラン

プラン内容	・IIJへのお問い合わせ代行 ・ストライトの設定変更（バナーの種類変更／カラー変更／バナー文言変更／表示位置変更／法域変更／年齢制限変更／多言語対応変更） ※ベーシックプランの場合はカラー変更と表示位置変更のみ可 ・バナーが表示できなくなった等の調査
サポートプラン ※月2時間まで	¥240,000／年 受付時間：10:00～19:00（土日祝、弊社が定める休日を除く）

STRiGHTの初期費用

通常20万円～

無料キャンペーン!!

申込期限 4/1（水）～6/30（火）

※本キャンペーンは、導入実績としてWebサイト等への掲載にご協力いただける企業様が限ります。

導入はネットアシストにお任せください

STRiGHTは、画面を覆い隠さないスマートなバナー表示など、サイトのユーザー体験（UX）を損なわない設計が可能です。導入にあたっては、Cookieのスキャンや、プランに応じたバナー作成、タグのサイト実装まで、弊社にお任せいただけます。

「今使っているCMPツールが高い！」「自社のサイトは対策が必要？」「どのプランが最適？」などの疑問がございましたら、ぜひお気軽にお問い合わせください。

NEWS TOPICS 2

情報セキュリティ10大脅威2026

2026年1月29日、IPA（情報処理推進機構）より「情報セキュリティ10大脅威　2026」が公開されました。こちらは、前年に発生した社会的影響の大きいセキュリティ事故や攻撃事例をもとに、専門家の審議・投票を経て選出された“いま本当に警戒すべき脅威”をまとめたものです。

本記事では、その中から一部を抜粋し、ポイントをわかりやすくご紹介いたします。

情報セキュリティ10大脅威2026（個人）

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	7年連続10回目
インターネット上のサービスへの不正ログイン	2016年	11年連続11回目
インターネットバンキングの不正利用	2016年	4年ぶり8回目
クレジットカード情報の不正利用	2016年	11年連続11回目
サポート詐欺（偽警告）による金銭被害	2020年	7年連続7回目
スマホ決済の不正利用	2020年	7年連続7回目
ネット上の誹謗・中傷・デマ	2016年	11年連続11回目
フィッシングによる個人情報等の詐取	2019年	8年連続8回目
不正アプリによるスマートフォン利用者への被害	2016年	11年連続11回目
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	2019年	8年連続8回目

参考：IPA「情報セキュリティ10大脅威 2026」

※個人向け10大脅威では、IPAからの公開では順位の記載をせず、50音順で並べています。これは、順位の低い脅威への対策が疎かになることを懸念してのことです。
順位に関わらず自身に関係のある脅威に対して対策を行うことが大切です。

情報情報セキュリティ10大脅威2026（組織）

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

参考：IPA「情報情報セキュリティ10大脅威2026」

今回は「AIの利用をめぐるサイバーリスク」が初選出され、いきなりの3位にランクインしております。AIが社会におよぼす影響の大きさを物語る順位となりました。また、「ランサム攻撃による被害」、「機密情報を狙った標的型攻撃」、「内部不正による情報漏洩等」は11年連続でランキングに入りました。

それでは、「組織」向け脅威のランキングから、上位3つを抜粋してご紹介いたします。

1位 ランサム攻撃による被害

概要

ランサム攻撃とは、「ランサムウェア」と呼ばれるマルウェアに感染させ、PCやサーバーのデータを暗号化し、業務の継続を困難にした上で、データを復旧することと引き換えに、金銭を要求する攻撃です。
近年では、ネットワークを介して感染を拡大させるタイプのランサムウェアも登場しており、企業や組織全体に甚大な被害を与えるケースが増えています。

手口

・VPN機器やOSの脆弱性を悪用し、ネットワークからランサムウェアに感染させる。
・メール・WEBサイトからランサムウェアに感染させる。

事例

大手飲料メーカーでランサムウェア攻撃により一時生産が止まり、製品が店頭から消えることで、一般消費者にも影響を与える事例がございました。

対策

- **パッチ管理**：修正プログラムを適用し、OSやソフトウェアを常に最新の状態にアップデートしておく。
- **従業員教育**：不審なメールの添付ファイルやURLをクリックしないよう周知するとともに、定期的に訓練を行う。
- **バックアップ**：重要なデータを定期的にバックアップし、オフラインで管理する。
- **多層防御の実施**：ファイアウォール、アンチウイルスソフト、侵入検知システムなど、複数の防御層を設ける。

2位 サプライチェーンや委託先を狙った攻撃

概要

関連企業や取引先の中から、セキュリティ対策が脆弱な組織を最初の標的とし、そこを踏み台として本来の標的を攻撃する手口です。
他にも、ソフトウェア会社やサービスプロバイダーなどを経由して、ターゲットに侵入するパターンもございます。

手口

・セキュリティ対策が比較的弱い関連会社や委託先を踏み台として侵入し、本来の標的である企業・組織へ不正アクセスを行う。
・ソフトウェア開発元を攻撃し、正規のソフトウェアやパッチにマルウェアを埋め込み、利用者を感染させる。

事例

通販大手が大規模なサイバー攻撃を受け、倉庫管理や物流に関わるシステムが停止したことで、そのサービスを利用していた他社や消費者にも影響が広がりました。

対策

- **通常のセキュリティ対策**：セキュアなネットワーク環境の構築、セキュリティソフトの使用、パスワードの複雑化等、自社でできる対策を確実に行う。
- **サプライチェーンリスクの徹底管理**：自社だけでなく、サプライチェーン全体の状況を把握し、関連会社に対しても対策を徹底するよう要請する。

3位 AIの利用をめぐるサイバーリスク

概要

AIの利用をめぐるサイバーリスクは、情報漏洩リスク、攻撃手法の高度化によるリスク(フィッシングメールの高度化、マルウェアの自動生成、ディープフェイクによるなりすまし等)がございます。
「利用するリスク」と「利用されるリスク」があることが特徴です。

手口/原因

・生成AIに入力した情報が、社外システムにより学習・ログ保存・分析される場合、情報漏洩となる可能性がある。
・生成AIを使用することで、これまでより本物に近いメールを送付し、攻撃対象を偽サイトに誘導する。

事例

現時点では、具体的な事例はございません。

対策

情報漏洩対策

・機密性の高い情報をAIに送る際は、データのマスキングを行う。
・無料版ではなく、エンタープライズ版を利用する。

AIを使用した攻撃対策

・不審なメールの添付ファイルやURLをクリックしないよう周知するとともに、定期的に訓練を行う。

NEWS TOPICS 3

2025年度 セキュリティインシデント動向まとめ

2025年度に入ってからも、国内ではサイバー攻撃や情報漏えいなどのセキュリティインシデントが相次いで発生しています。
そこで今回は2025年4月1日以降に日本国内で公表された事例を整理し、どのような攻撃が多く発生しているのか、またどのような被害が生じているのかを解説します。
自社の対策を見直すヒントとして、ぜひご覧ください。

日本におけるセキュリティインシデント件数

2025年に公表されたセキュリティインシデントは、合計165件にのぼりました。これは約2日に1回の頻度で発生している計算となり、サイバー攻撃は決して他人事ではなく、どの企業にも起こり得る身近な脅威であることが分かります。また、個人情報の漏えい件数は約2,000万件に達しました。

業種別ではサービス業が最多となっており、業種を問わず被害が拡大している状況です。

CSC「企業のセキュリティインシデントに関する調査レポート2025」 >

セキュリティインシデントの一覧（※一部）

2025年4月1日以降に公表された主な事例は、以下の通りです。

発生日時（公表日を含む）	会社名	攻撃種類	狙われた箇所/原因
2025年4月15日	IIJ	不正アクセス	ソフトウェアの脆弱性
2025年4月24日	PR TIMES	不正アクセス	管理者画面への不正アクセス（使われていないIPからの侵入）
2025年6月10日	楽待	不正アクセス	Webサーバの脆弱性
2025年6月27日	審調社	ランサムウェア攻撃	ネットワーク機器の脆弱性
2025年8月8日	駿河屋	不正アクセス	監視ツールの脆弱性
2025年8月24日	アクリーティブ	ランサムウェア攻撃	ファイアウォールの設定ミス
2025年8月29日	ハウステンボス	不正アクセス	VPN機器からの侵入
2025年9月29日	アサヒグループホールディングス	ランサムウェア攻撃	ネットワーク機器からの侵入
2025年10月17日	JR九州	不正アクセス	詳細は調査中
2025年10月19日	アスクル	ランサムウェア攻撃	VPN機器からの侵入
2025年11月4日	日本経済新聞社	不正アクセス	業務用PCにウイルス感染
2025年11月14日	東海大学（委託先）	ランサムウェア攻撃	詳細は調査中
2025年11月26日	ジモティー	不正アクセス	開発環境で不正コードが混入
2026年2月9日	日本医科大学 武蔵小杉病院	ランサムウェア攻撃	VPN機器からの侵入
2026年2月13日	ワシントンホテル	ランサムウェア攻撃	詳細は調査中

このように、2025年度のインシデントは業種を問わず発生しており、不正アクセスおよびランサムウェア攻撃が中心となっています。

特に目立つのは、VPN機器やファイアウォールなどのネットワーク機器を起点とした侵入や、Webサーバおよび各種ソフトウェアの脆弱性を悪用した事例です。

事例紹介

実際に公表された事例の中からいくつかを取り上げ、その概要と影響について見ていきます。

事例① JR九州 不正アクセス

参考：JR九州「サイバー攻撃によるグループ会社従業員の個人情報漏えいの可能性について」

概要

JR九州グループ会社のネットワーク環境に対する不正アクセスが発生し、従業員情報が漏えいした可能性があることが判明しました。

経緯

2025年10月17日、グループ会社ネットワークへの不正アクセスをセキュリティツールが検知しました。
防御対応を実施しましたが、その後の調査で情報流出の可能性が判明しました。

流出の可能性がある情報

・従業員、派遣スタッフ、退職者の氏名
・会社付与メールアドレス
・PCログインID
対象者数：14,638名

事例② ジモティー 不正アクセス

参考：ジモティー「弊社利用システムへの不正アクセスに関する調査結果のご報告」

概要

株式会社ジモティーにおいて、本番環境とは分離された社内開発環境（dev環境）に対する不正アクセスが発生しました。
社内調査の結果、一部の個人情報が外部からアクセス可能な状態であったことが判明し、漏えいの可能性があるとして公表されました。

経緯

2025年11月26日、開発環境の一部でマルウェア感染を含む不正アクセスの兆候を検知しました。
その後、速やかにアクセス遮断措置を実施しました。
調査の結果、開発環境に保存されていた一部データが外部から閲覧可能な状態であったことが確認されました。

流出の可能性がある情報

・問い合わせ履歴
・従業員および社外協力者の氏名、メールアドレス

まとめ

2025年に入り、サイバー攻撃は本番環境だけでなく、開発環境や委託先環境、さらにはネットワーク機器にまで及ぶなど、攻撃対象が多岐にわたっています。また、Webサイトやネットワーク機器の脆弱性を悪用するなど、侵入経路も年々多様化・高度化しています。
ネットアシストでは、WAF、IDS／IPS（EDR機能付き）、脆弱性診断、Webサイト改ざん検知など、お客様の環境や課題に応じた最適なセキュリティ対策の導入支援を行っております。
現状対策の見直しや新規導入をご検討の際は、弊社営業担当者までお気軽にお問い合わせください。

・WAF　・IDS／IPS（EDR機能付き）　・脆弱性診断　・Webサイト改ざん検知