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

2026.06
vol. 61

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

貴社のウェブサイトは安全ですか？ IPA「安全なウェブサイトの作り方」のご紹介

ウェブサイトに潜む脅威とIPA資料のご紹介

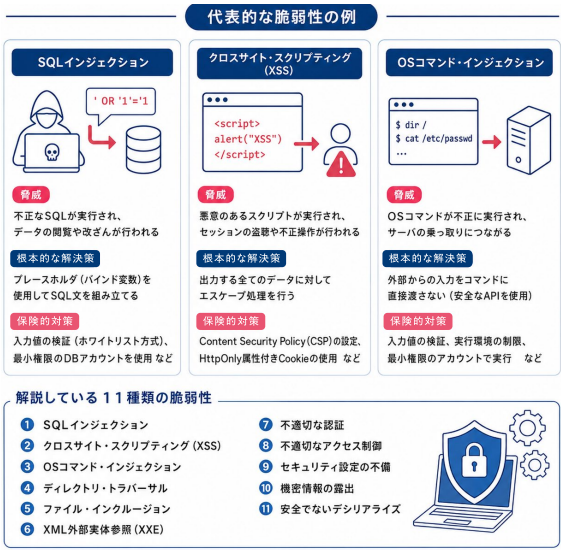
昨今、サイバー攻撃の手口はますます巧妙化し、企業にとってウェブサイトのセキュリティ対策は喫緊の課題となっています。そこで今回は、独立行政法人情報処理推進機構（IPA）が公開しているガイドライン「安全なウェブサイトの作り方」をご紹介いたします。

本資料は、IPAへ届出件数の多い脆弱性や、攻撃による影響度が大きい脆弱性を取り上げ、適切なセキュリティを考慮したウェブサイトを作成するための手引きとして広く活用されています。

11の脆弱性とチェック項目

本資料では、「SQLインジェクション」や「クロスサイト・スクリプティング」、「OSコマンド・インジェクション」といった代表的な11種類の脆弱性について、発生しうる脅威や根本的な解決策、保険的対策が詳しく解説されています。また、資料の巻末には「ウェブアプリケーションのセキュリティ実装チェックリスト」が付属しています。

このリストには、「SQL文の組み立ては全てプレースホルダで実装する」や「ウェブページに出力する全ての要素に対して、エスケープ処理を施す」などの具体的な実施項目が明記されており、自社サイトのセキュリティレベルを確認・見直すための指標として役立ちます。

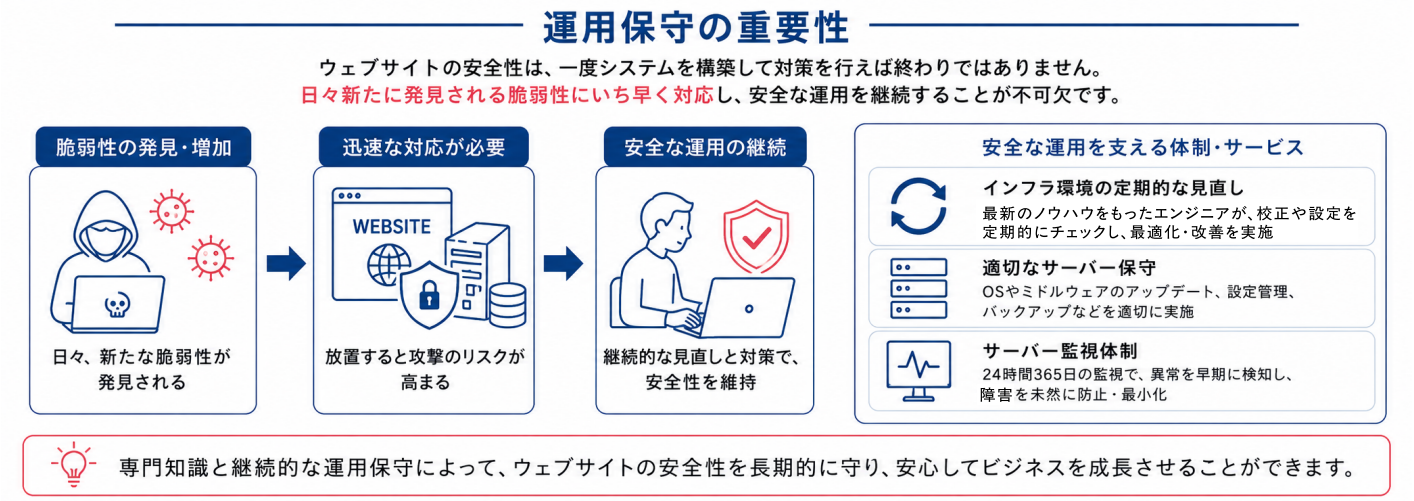


セキュリティ対策の課題と運用保守の重要性

しかし、実際にチェックリストを確認してみると、「専門的すぎて現在の自社の実装状況が把握できない」「自社にセキュリティエンジニアがおらず、適切な対策ができているか不安」といったお悩みを抱える企業様も少なくありません。

ウェブサイトの安全性は、一度構築して対策を行えば終わりではありません。

日々新たに発見される脆弱性にいち早く対応し、安全な運用を継続するためには、最新のノウハウを持ったエンジニアによるインフラ環境の定期的な見直しや、適切なサーバー保守・監視体制が必要不可欠です。



セキュアなサイト構築と運用保守はネットアシストにお任せください

「現在の自社サイトにセキュリティリスクが潜んでいないか不安だ」「クライアントに納品するウェブサイトの安全性をしっかりと担保したい」とお考えのサイトご担当者様や、制作会社のディレクターの皆様、まずは、現状のシステムにおけるリスクを可視化することから始めてみませんか？ネットアシストでは、OSやミドルウェア、Webアプリケーションなどに対して様々な疑似攻撃を試行し、潜在的な問題点を発見する「脆弱性診断（セキュリティ診断）」サービスを提供しております。

お客様の環境やご予算に合わせて、自動ツールによる診断や、手動でのより精密な診断など、柔軟なプランをご用意しています。ご興味ございましたら営業までお気軽にお問い合わせください。

サービス名	価格	内容
SecurityBlanket Standard(自動)	100,000円	1FQDN一回の診断ライセンス ページ制限なし
SecurityBlanket 365(自動)	390,000円	SecurityBlanket Standardの 年間ライセンス
SecurityBlanket Advance(自動＋手動)	660,000円 ＋手動診断URL追加	報告会、再診断を含む
SecurityBlanket Pro(手動)	980,000円	手動診断10URL、プラットフォーム 診断31P、報告会、再診断を含む
	30,000円	11URL以降の追加費用（1URLあたり）

NEWS TOPICS 2

相次いで発見されるLinux・Nginxの深刻な脆弱性

2026年5月、LinuxおよびNginxにおいて、重大な脆弱性が立て続けに報告されました。いずれもサーバー運用に大きな影響を及ぼす可能性があり、迅速な確認と対策が求められています。

① Linuxカーネル脆弱性「Copy Fail」

「Copy　Fail（CVE-2026-31431）」は、Linuxカーネルに存在する権限昇格の脆弱性です。一般ユーザー権限からroot権限を取得できる可能性があり、多くのLinuxディストリビューションに影響すると報告されています。特に問題視されているのは、下記3点です。

- 2017年以降のLinuxカーネルに広く影響
- 公開済みのPoC（攻撃コード）が存在
- 一部では実際の悪用も確認

② Linuxカーネル脆弱性「ssh-keysign-pwn」

さらに、Linuxカーネルでは「ssh-keysign-pwn（CVE-2026-46333）」と呼ばれる脆弱性も公開されました。この脆弱性では、一般ユーザー権限から、下記を読み取られる可能性があるとされています。

- SSH秘密鍵
- /etc/shadow
- root権限相当の機密情報

③ Nginxでリモートコード実行（RCE）の脆弱性

Webサーバーソフトウェアとして広く利用されているNginx　において、リモートコード実行につながる可能性のある脆弱性「CVE-2026-42945」が報告されました。特定のrewrite設定環境下で、外部から細工されたHTTPリクエストを送信されることで、下記の問題に発展する可能性があります。

- サービス停止
- メモリ破壊
- 条件次第で任意コード実行

近年は、脆弱性公開後すぐに攻撃コード（PoC）が出回るケースも多く、「あとで対応する」が大きなリスクにつながります。そのため、《自社環境に脆弱性が存在しないか確認する》、《セキュリティアップデートを迅速に適用する》、《継続的に監視・運用する》といった継続的なセキュリティ対策が重要になっています。

ネットアシストでは、《脆弱性診断サービス》、《セキュリティアップデートサービス》をご提供しております。Linuxサーバーはもちろん、Windowsサーバーを含めたセキュリティ対策についても、お気軽にご相談ください。

NEWS TOPICS 3

SSL証明書更新申請についてのお知らせ

いつもお客様ポータルをご利用いただきありがとうございます。SSL証明書につきまして、通常「お客様ポータル」より発行・更新の申請をいただいておりますが、SSL証明書の有効期限短縮と自動化対応の関係で、一部証明書にて更新ステータス変更のための「編集」ボタンをクリックできない場合がございます。（上記は仕様変更に伴う改修作業の影響のため、一時的なものになります）

SSL証明書の更新自動化の詳細なご案内はこちら

対象のお客様

対象のSSL証明書をご利用のお客様については、更新確認メールに送付する形でExcelの申請書を送付しております。（同じSSL証明書であっても環境によって改修作業の要否が異なるため、お手数ですが送付ファイルの有無にて判断をお願いいたします）

Excelでの更新方法

シート内の必要事項をご記入いただき、弊社管理部門（kanri@netassist.ne.jp）までご返送くださいませ。

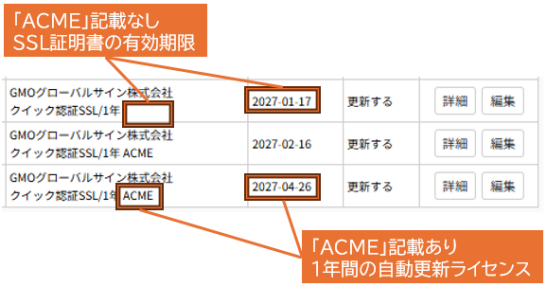
また、自動化対応の関係上、表示される「有効期限」は下記2種類ございます。有効期限前には更新確認のメールをご案内しておりますが、申請の際に混同しないようご注意をお願いいたします。

①SSL証明書種別に「ACME」の記載がない場合

弊社よりご提供している、「SSL証明書自体の有効期限」が表記されます。自動更新対応前もしくは自動更新未対応のSSL証明書です。（有効期限短縮の影響を受けます）

②SSL証明書種別に「ACME」の記載がある場合

弊社よりご提供している「1年間の自動更新ライセンスの有効期限」が表記されます。ライセンスの期限内であれば自動的に更新され続けるため、SSL証明書自体の有効期限は表示しておりません。（有効期限短縮の影響を受けません）



ACME（Automatic Certificate Management Environment）［自動証明書管理環境］とは

証明書の管理を自動化するためのプロトコルです。ACME機能を利用することで、SSL証明書更新の一部手続きを自動化できるようになります。

- 鍵ペアの作成
- CSRの作成・認証局への送信
- ドメイン名利用権の検証
- 証明書の設定・更新

SSL証明書の仕様変更に対応できるよう今後も改修を進めて参りますので、ご不明点等ございましたら各営業担当までお気軽にお申し付けください。

現場のプロ目線で
国産クラウドを深堀り!
さくらのクラウドを"活かす情報"が、ここにある。
さくらのクラウドラボ by NET ASSIST
サイトを見る

NET ASSIST 24/7 Guardian Deity × SAKURA internet
ネットアシストはさくらインターネットの最上位パートナーとして、
豊富な運用ノウハウと実践的な技術力を活かした支援体制を確立しています。

NET ASSIST 24/7 Guardian Deity
株式会社ネットアシスト
〒171-0022　東京都豊島区南池袋3-13-5 池袋サザンプレイス 7F
https://www.netassist.ne.jp/