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

2026.02
vol.57

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

なぜSSL証明書の有効期間は短縮されるのか？

近年、個人情報保護法や各国のプライバシー規制が強2026年3月以降、SSL証明書の有効期間が段階的に短縮される方針が決定されました。今回は、SSL証明書が「47日」という短い期間になる理由と、その背景についてご紹介します。

SSL証明書とは？

SSL証明書は、Webサイトの通信を暗号化し、安全に運用するうえで欠かせない仕組みです。証明書が設定されていない場合、ブラウザに警告が表示され、利用者に不安を与えてしまうことがあります。

さらに、通信が暗号化されない状態では、第三者による通信内容の盗聴や改ざんが行われる可能性があり、個人情報やパスワードなどが盗まれるリスクも高まります。

有効期間短縮の背景

Webサイトと安全な通信を実現するための国際標準規格を定める団体、CA/Browser Forum（認証局・ブラウザベンダー等で構成）により、サーバ証明書の有効期間を短縮する方針が決まりました。

この決定は、認証局（CA）をはじめとする関係各社による投票で可決されており、主要なブラウザベンダーであるGoogle、Microsoft、Mozilla、Apple なども賛成票を投じています。なお、可決には全体の2/3以上の賛成が必要とされています。

（出典：Ballot SC-081v3: Introduce Schedule of Reducing Validity and Data Reuse Period
《証明書有効期間およびデータ再利用期間短縮のスケジュール導入》）

有効期間短縮の目的（なぜ短くするのか）

有効期間短縮の目的は、主に以下の3点です。

1 セキュリティリスクへの迅速な対応

暗号技術の脆弱性発見や、秘密鍵の漏洩などが発生した場合、証明書は速やかに失効・再発行が必要になります。有効期間が短くなることで更新頻度が上がり、万が一のインシデント発生時でも影響範囲を限定しやすくなります。

2 証明書情報の最新化

証明書にはドメインや組織情報が含まれるため、短期間で更新されることで、古い情報のまま運用され続けるリスクを低減できます。

3 更新の自動化促進

有効期間が短くなることで更新頻度が増え、手動更新による運用は現実的ではなくなります。自動更新を導入することで、更新忘れや対応漏れを防ぎ、安定した運用につなげることができます。

SSL証明書の有効期間変更スケジュール

以下の通り、段階的に短縮される予定です。

期日	最大有効期間
～2026年3月14日	398日（約13カ月）
2026年3月15日～	200日（約6.5カ月）
2027年3月15日～	100日（約3カ月）
2029年3月15日～	47日（約1.5カ月）

※47日となった背景として、「31日（最も長い月＋15日（30日の半分）＋1日（余裕）＝47日）」とし、実際の運用で耐えられる現実的な上限として決まりました。

当社の対応

SSL有効期間の短縮に伴い、各社ではACMEを活用した「SSL更新の自動化」対応が進んでいます。
ネットアシストにて現在管理しているSSL証明書、および今後新規取得されるSSL証明書についても、対象サーバへの自動更新対応を順次進めてまいります。自動化にあたっては、以下の対応を実施します。

- 対象サーバへのSSL更新自動化ツールのインストール／設定
- 証明書の自動更新が正常に完了しているかの監視
- 更新失敗時の迅速な検知と復旧対応

SSL更新自動化ツールの導入に関するご案内メール

弊社で保守しているサーバにつきましては、SSL更新自動化ツールの導入可否を順次確認しております。下記日程にてご案内メールをお送りしておりますので、ご確認ください。

・2025/12/18：【重要】SSL証明書更新自動化ツール導入のご案内／株式会社ネットアシスト

・2026/01/14：《再送》【重要】SSL証明書更新自動化ツール導入のご案内／株式会社ネットアシスト

ご不明な点がございましたら、担当営業までお気軽にお問い合わせください。
また、証明書更新の自動化をご検討中の場合も、ぜひご相談ください。

NEWS TOPICS 2

年度切り替えに向けたITインフラの見直しチェックポイント

皆様は、ITインフラの見直しを定期的に実施されていますでしょうか。昨今はセキュリティインシデントの増加により、これまで以上に対策の重要性が高まっています。加えて、従来通りシステムダウンに備えた可用性の確保も欠かせません。

こうした状況を踏まえ、ITインフラは定期的に見直し、現状に合った対策へ更新していくことが重要です。そこで今回は、年度切り替えに向けたITインフラの見直しチェックポイントをご紹介します。

見直しチェックポイント

1. 退職者や異動者のアカウント削除はできているか?
2. サーバー構成やスペックが適切になっているか?
3. セキュリティ対策が万全になっているか?
4. 障害・インシデントに対応できる体制が整っているか?
5. 運用が属人化しているサーバーがないか?

次に、1〜5について具体的に解説していきます。

1 退職者や異動者のアカウント削除はできているか?

退職者や異動者のアカウントを放置すると以下の3つのリスクが考えられます。多忙な中ではありますが、リスクを避けるためにも、退職者や異動者のアカウントは確実に削除することを推奨いたします。

退職者や異動者のアカウントを放置するリスク

- リスク1 不正アクセスの原因となる
- リスク2 情報漏洩のリスクが高まる
- リスク3 無駄なコストがかかる

2 サーバー構成やスペックが適切になっているか

サポート期限が切れたOSを利用していないか、またバックアップの設定に漏れがないかをご確認ください。サポートが終了したOSを使用するとセキュリティインシデントにつながる可能性があるため、該当する場合は速やかな切り替えを推奨いたします。

サポート切れOSを使用するリスク

- リスク1 セキュリティの脆弱性
- リスク2 ソフトウェアの互換性
- リスク3 サポートの欠如

バックアップが適切に取れない場合のリスク

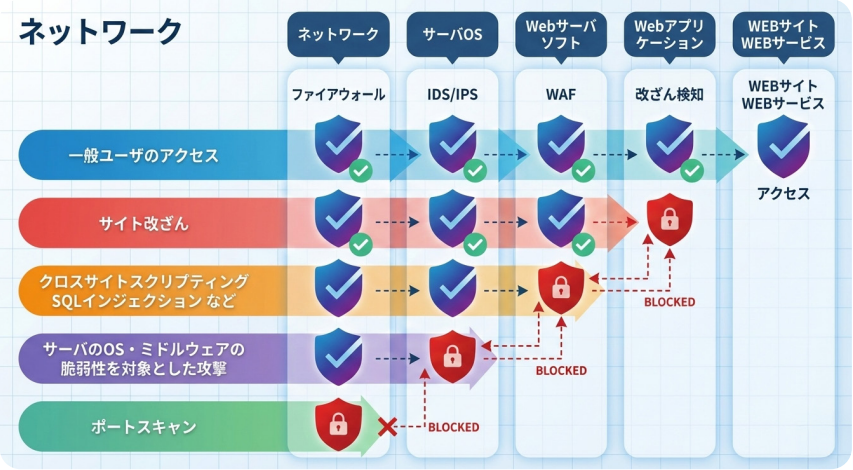
- リスク1 復旧までに時間がかかる
- リスク2 営業活動に支障がでる可能性がある

システムがダウンする原因は、人的ミス、システム障害、災害、外部からの攻撃等があり、完全に防ぐことは不可能です。
バックアップが適切に取れているかを、今一度確認することを推奨いたします。

3 セキュリティ対策が万全になっているか

近年、セキュリティインシデントが急増しており、何らかの対策は必須といっても過言ではございません。

ファイアウォール（主にネットワークを保護）、IDS/IPS（主にOS/ミドルウェアを保護）、WAF（主にアプリケーションを保護）のようなセキュリティ製品の導入はお済でしょうか？



その他、セキュリティを万全にするには、脆弱性対策が必要です。脆弱性を放置することがセキュリティインシデントに繋がるからです。
そのため、脆弱性管理を行い、OSやソフトウェアを最新の状態にアップデートすることが重要です。また、近年、脆弱性診断を実施する企業様が増えております。
まだ脆弱性診断をされていない企業様は、安心、安全であることを維持し続けるために、定期的な診断をしてみてはいかがでしょうか？

4 障害・インシデントに対応できる体制が整っているか

障害やインシデントが発生した際の対応体制が整っていない企業様では、復旧に時間がかかり、事業への影響が長期化してしまうリスクがございます。インシデント対応では、一刻も早い問題解決が求められます。そのため、事前に準備をしておくことが重要です。

インシデントにより想定される被害の例

- 対応人件費、原因調査や復旧のための外部委託費
- 攻撃者による不正送金や金銭要求
- 事業停止による機会損失

5 運用が属人化しているサーバーがないか

サーバーの運用が属人化してしまうと、「特定の担当者がいなければ業務が回らない」状態になってしまいます。
中には、”ひとり情シス”と呼ばれる社内IT業務のほとんどをひとりが担っているケースもございます。IT業務の負担は年々増え続けており、これでは、いつか破綻することは目にみえています。主な原因は以下になります。

属人化がすすむ原因

- 属人化により、「その人しか知らない設定」「本人だけが覚えているルール」が存在する。
- 忙しいので業務マニュアルを作成する時間がない。
- 人員を追加しようにも人材育成に時間がかかる。

どれも早期に解決することが難しい問題ですが、業務が回らなくなる前に、外部リソースの活用も含めて、対策を実施されることを推奨いたします。

まとめ

ネットアシストでは、24時間365日のサーバーの監視・運用・保守代行サービスに加え、サーバーの構築やお引越し、セキュリティ製品のご提案が可能です。
ITインフラをチェックし課題事項がでてきた際は、ぜひ当社にご相談ください。

NEWS TOPICS 3

CEO詐欺（社長なりすまし）メールにご注意

最近、以下のようなメールを受信していないでしょうか？昨年末より、実在する企業及びその代表者を騙る「CEO詐欺（社長なりすまし）」メールが急激に増加しております。実際に弊社や、弊社サービスをご契約いただいているお客様を名乗る詐欺メールも確認されており、本件に関するお問い合わせ・ご相談も多数いただいております。

メールの場合

新規のプロジェクト対応のため、新しいLINEのワークグループを作成してください。

なお、グループへの他メンバーの追加については、私が参加した後にこちらで対応しますので、現時点では追加不要です。グループ作成が完了しましたら、参加用のQRコードを生成のうえ、本メールへの返信にてご共有ください。

私がQRコードから参加次第、当該グループ上で今後の業務調整を進めていきます。お手数をおかけしますが、よろしくお願いいたします。

株式会社〇〇　代表取締役△△

LINEの場合

●●（振込先）に▲▲円の振込をお願いします。
緊急で対応が必要なプロジェクトのため、社内手続きは後回しで構いません。

※弊社から個別にLINEグループの作成をお願いすることはございませんので、ご注意ください。

弊社のお知らせ｜「当社や当社代表を騙った迷惑メールにご注意ください」

これら詐欺メールは代表者の名前や、「緊急」「返信不要」などの言葉で判断力を鈍らせることが目的です。決裁権限を持つ経営層からの緊急業務命令を装っているため、通常のフローを外れた対応であっても確認する間を与えない狡猾な手口であり、実際に数百万～数千万円を騙し取られる被害も発生しております。

主なターゲット

CEO詐欺の主なターゲットとなるのは、下記の部署やその担当者です。

CEO
詐欺の主なターゲットとなるのは、下記の部署やその担当者です。

経理部/経理担当者
送金の権限を持つため、最も直接的なターゲットになりやすいです。

人事部/人事担当者
送金ではなく「社員名簿」「連絡先」等、データ窃盗としてのターゲットになります。

新入社員
業務理解や注意力が不足しており、上司の指示に従いやすいため、詐欺の標的になりやすいです。

詐欺被害を防ぐには

多くの企業では、コーポレートサイトに代表者の名前・メールアドレス・主要取引先が公開されており、これらを悪用した標的型の詐欺メール事態を完全に防ぐことは不可能です。詐欺メールの中には開封しただけでウイルスに感染する危険なものもあり、1人の社員がたった1回、間違えて攻撃メールを開いてしまうだけで、取引先や顧客の情報が漏洩する危険があります。

こうした被害を防ぐには、社員1人1人が「送信者のメールアドレス」や「依頼内容、文体」等でなりすましの兆候を見抜き、不自然なメールは開封しないようリテラシーを高めることが大切です。弊社では、そのようなご要望にお応えするため、**標的型メール訓練サービス「情報漏えい防ぐくん」**をご用意しております。ご興味がございましたら、ネットアシスト営業担当者までお気軽にお問い合わせください。