

無料の自動更新か、 有料の証明書か。 SSL 証明書の選び方。

DV・OV・EV の違いと、2026 年から始まる「有効期間の短縮」への備え

Web サイト運営者・情報システム担当者向け / ibis studio



はじめに —— 「どれを選んでも、鍵マークは同じ」

「無料の証明書で十分なのでは？」

「有料との違いが、正直わからない」

「毎年の更新作業が、地味に手間」

SSL 証明書について、よくいただくご相談です。結論から言えば、暗号化の強度そのものは無料でも有料でも変わりません。

違いは「どこまで審査するか」と「何を保証するか」、そして「更新をどう回すか」です。

そして 2026 年 3 月から、証明書の有効期間が段階的に短くなり始めました。これまでのように「1 年に 1 回、手で更新」という運用は、数年のうちに成り立たなくなります。

選ぶ基準は「価格」ではなく「**サイトの性格**」と「**更新をどう回すか**」。

本書では、無料 (自動更新) と有料の違い、DV・OV・EV の認証レベル、そして 2026 年からの有効期間短縮への備えを、実務目線で整理します。

目次

1

そもそも SSL 証明書とは何を証明しているのか

暗号化と「実在証明」は別のもの

2

DV・OV・EV —— 3 つの認証レベル

審査の深さと、保証されるものの違い

3

無料 (自動更新) と 有料 の違い

Let's Encrypt と商用 CA の使い分け

4

2026 年から始まる「有効期間の短縮」

398 日 → 200 日 → 100 日 → 47 日

5

自動更新は「無料だけの特権」ではない

有料証明書でも ACME で自動化できる

6

主なブランドと、自動更新の対応状況

大手ほど一般販売では ACME 非対応

7

無料の証明書はどう成り立っているのか

寄付・スポンサー / 本業への導線 / 試用

8

「無料だから信頼性が低い」は成り立たない

有料で買っているのは審査・補償・サポート

9

サイト別・選び方の早見表

中小規模は DV で足りる / EV が要る場面

10

更新事故を防ぐ運用チェックリスト

中間証明書・監視・担当の明確化

SSL 証明書は「暗号化」と「実在証明」の 2 つを担う

証明書には役割が 2 つあります。混同されやすいのですが、選び方に関わるのは後者だけです。

① 通信の暗号化

ブラウザとサーバーの間の通信を暗号化し、盗み見や改ざんを防ぎます。

この強度は DV・OV・EV で差がなく、無料の証明書でも同じです。

② 運営者の実在証明

「このサイトを運営しているのは誰か」を認証局 (CA) が審査して保証します。

ここが DV・OV・EV で大きく異なり、証明書を選ぶ基準になります。

よくある誤解:「有料のほうが暗号が強い」は事実ではありません。

暗号方式 (RSA 2048bit / ECDSA など) と鍵長は同じで、ブラウザの鍵マークの見た目も同じです。

差が出るのは「審査の深さ」「保証」「サポート」「更新の運用」の 4 点です。

DV・OV・EV ―― 審査の深さで 3 段階

暗号強度は同じ。違うのは「誰であることを、どこまで確かめたか」です。

	DV (ドメイン認証)	OV (企業認証)	EV (拡張認証)
審査の対象	ドメインの保有のみ	ドメイン + 法人の实在	ドメイン + 法人 + 事業実態
審査方法	メール / DNS / ファイル設置	登記情報・電話確認など	OV + 第三者データベース照合
発行までの期間	数分～数時間	数日～1週間程度	1～2週間程度
証明書に載る情報	ドメイン名のみ	ドメイン + 組織名	ドメイン + 組織名 + 所在地
費用の目安 (年額)	0円～1万円台	3万～8万円台	8万～15万円台
自動発行	可能	一部可能	不可 (審査が必須)

注意: かつて EV 証明書は「アドレスバーに緑色の社名が出る」ことが最大の利点でしたが、
主要ブラウザは 2019 年以降この表示を廃止しました。現在の EV の価値は「見た目」ではなく、
審査の厳格さそのものと、証明書の内容を確認する取引先・監査への説明材料にあります。

無料 (自動更新) と 有料 —— 本当の違いは 4 つ

比較項目	無料 (Let's Encrypt 等)	有料 (商用 CA)
認証レベル	DV のみ	DV / OV / EV から選べる
暗号強度	同じ	同じ
有効期間	90日 (2026年内に短縮予定)	最長 200日 ※2026年3月15日以降
更新方法	ACME による自動更新が前提	手動 または ACME 自動更新
損害補償	なし	あり (数千万～数億円規模)
サポート	コミュニティのみ	電話・メールでの問い合わせ窓口
組織名の記載	なし	OV・EV なら記載される
向いている用途	個人・検証環境・情報サイト	企業サイト・EC・業務システム

判断の軸:「サイトの規模」と「訪問者が運営者を確認めたがるか」。

中小規模のサイトは、EC を含めて無料 (DV) で十分です。決済自体は決済代行会社の画面で行われ、カード情報が自社サーバーを通らない作りが一般的だからです。判断が変わるのは、規模が大きく、運営者の実在そのものが信用の前提になるサイト —— 金融機関や公的機関などです。

2026 年から、証明書の有効期間が段階的に短くなる

業界標準 (CA/Browser Forum) の決定により、最大有効期間が段階的に短縮されます。

398 日

～2026年3月14日
従来の期間

200 日

2026年3月15日～
年1回では回らない

100 日

2027年3月15日～
年4回の更新が必要

47 日

2029年3月16日～
手動運用は事実上不可

➡ 更新の回数は増え、手作業の限界が先に来る

これが意味すること

- ・2029 年には、年 7～8 回の更新が必要になる。手作業では現実的に回らない
- ・EV・OV であっても、証明書の「取得」は自動化せざるを得なくなる
- ・いま手動更新しているサイトは、更新の自動化を前提に組み直す時期に来ている

「自動更新 = 無料証明書」ではない

自動更新の仕組み (ACME) は、無料の証明書のために作られたものですが、いまは主要な商用 CA も対応しています。

「有料 = 手動更新」という思い込みは、すでに実態と合っていません。

A 無料 DV + 完全自動更新

Let's Encrypt 等を ACME クライアントで自動更新。費用ゼロ・人手ゼロ。

情報サイト・検証環境・個人サイトに最適。

B 有料 OV + 自動更新

商用 CA の ACME 対応を使う。組織名の記載と補償を得ながら、更新は自動。

企業サイト・EC の現実的な最適解になりつつある。

C 有料 OV / EV + 手動更新

従来からの運用。期間短縮に伴い更新頻度が上がるため、

担当者の負担と失念リスクが年々大きくなる。

主な証明書ブランドと、ACME 自動更新の対応状況

有効期間が短くなるほど「自動更新に対応しているか」が選定基準になります。

ブランド	提供元	主な種別	費用	ACME 自動更新
Let's Encrypt	ISRG (非営利)	DV	無料	対応 (標準)
ZeroSSL	ZeroSSL	DV	無料～	対応
Google Trust Services	Google	DV	無料	対応
FujiSSL	フジプレミアムサービス	DV / OV	有料	対応
Sectigo	Sectigo (旧 Comodo)	DV / OV / EV	有料	一部対応
GlobalSign	GMOグローバルサイン	DV / OV / EV	有料	法人向け (Atlas)
DigiCert / GeoTrust	DigiCert	DV / OV / EV	有料	一般販売は非対応
セコムトラストシステムズ	セコム	OV / EV	有料	非対応
サイバートラスト	サイバートラスト	OV / EV	有料	非対応

見落としやすい点: 大手ブランドほど、一般向けの販売では ACME に対応していません。
「有名なところで買えば自動更新できる」とは限らないため、更新の自動化を重視するなら
対応ブランドから選ぶか、法人向けの管理プラットフォーム (GlobalSign Atlas 等) を検討することになります。

※ 2026年9月時点。販売代理店によって取り扱い・対応状況が異なる場合があります。

無料の証明書は、どうやって成り立っているのか

「タダより高いものはない」と身構える前に、収益の出どころを知っておくと判断しやすくなります。

寄付・スポンサー

Let's Encrypt

非営利団体 ISRG が運営。
収益を得ておらず、原資は
スポンサー企業の寄付。
Google / AWS / Microsoft /
Mozilla / Cisco / Shopify など

本業への導線

ZeroSSL / Google

営利企業だが証明書では
儲けていない。
ZeroSSL は 3 枚まで無料の
フリーミアム。Google は
クラウド利用につなげる

上位プランへの試用

一部の商用 CA

期間限定の無料 DV を配る。

実質的に試用版で、OV・EV・
ワイルドカードへの
アップセルが目的

なぜ企業が寄付するのか: HTTPS が普及したほうが、自社に得だからです。
ブラウザ事業者は Web 全体の安全性が上がる。クラウド・CDN は顧客の HTTPS 化の障壁が下がる。
EC プラットフォームは数百万の顧客サイトに証明書を配る必要があり、自前で調達するより安い。
道路や信号機に共同出資しているのに近い構図です。

※ スポンサー一覧は ISRG 公開情報 (2026年9月時点) による。

「無料だから信頼性が低い」は成り立たない

証明書が信頼されるかどうかは、支払った金額ではなく「ブラウザのルート証明書ストアに入っているか」だけで決まります。

ここに入るには、Apple・Microsoft・Google・Mozilla が定める監査を毎年通り続ける必要があります。

無料でも同じ基準

WebTrust 等の監査は、無料か有料かに
関係なく同じものを受けます。

Let's Encrypt は世界の HTTPS サイトの過半数に証明書を発行しており、
規模では最大手です。

では有料で何を買っているのか

証明書そのものではなく、
「人手のかかる作業」と「約束」です。
審査・補償・サポートは、いずれも人と原資が必要で、自動化できません。

有料で得られるもの

無料では提供できない理由

OV・EV の審査

登記確認や電話確認は人手が必要で、自動化できない

損害補償

保険であり、支払いの原資が要る

サポート窓口

問い合わせに対応する人を置く必要がある

Let's Encrypt が DV しか発行しないのは、思想というより構造上の必然です。すべて自動化しないと無料では配れず、OV・EV は自動化できないためです。

サイトの性格から選ぶ ―― 早見表

サイトの種類	推奨	理由
情報発信のみのサイト (ブログ・メディア・コーポレート)	DV (無料)	暗号化が目的。実在証明までは求められない
中小規模の EC サイト (決済代行を利用)	DV (無料)	カード情報は決済代行の画面へ。自社サーバーを通らない
問い合わせフォームのある 企業サイト	DV (無料)	暗号化されていれば足りる。社名表示が必要なら OV
検証・開発環境	DV (無料)	費用をかけず自動更新で十分
大規模 EC・会員制サービス (自社で決済情報を保持)	OV	組織名を示し、補償を備える。監査で問われることも
金融機関・公的機関 証券・保険・行政サービス	EV	運営者の実在そのものが信用の前提になる

※ 費用はあくまで目安です。ワイルドカード (*.example.com) やマルチドメイン対応は別途加算されます。

迷ったときの基準: 一般的な企業サイトや中小規模の EC であれば、無料 (DV) で問題ありません。
有料を検討するのは「社名を証明書に載せたい」「補償が必要」「取引先や監査に説明する」場合です。

更新事故を防ぐ —— 運用チェックリスト

1

中間証明書を必ず一緒に設置する

最も多い事故。ブラウザは中間証明書をキャッシュするため、手元の PC では正常に見え、他の環境や API 連携だけが失敗する —— 極めて気づきにくい形で壊れる。

2

設置後は「外部から」検証する

自分のブラウザで確認するだけでは不十分。openssl s_client などですerverが返すチェーン全体を確認する。

3

有効期限を監視する仕組みを持つ

カレンダーの登録だけでは担当者の異動で失われる。期限を自動で検知し、複数人に通知が届く形にしておく。

4

秘密鍵の取り扱いを決めておく

パーミッションは 600・root 所有。メールやチャットで送らない。
作業後は一時ファイルを確実に削除する。

5

更新後の切り戻し手順を用意する

旧証明書を消さずに残し、設定ファイルをバックアップしてから切り替える。
問題が出たら即座に戻せる状態にしておく。

まとめ

- 暗号の強度は無料でも有料でも同じ。違うのは「審査の深さ」と「保証」。
- 一般的な企業サイトや中小規模の EC は無料 (DV) で十分。EV が要るのは金融機関などに限られる。
- EV のアドレスバー緑色表示は 2019 年以降廃止済み。価値は審査の厳格さにある。
- 2026 年 3 月から有効期間が 200 日へ。2029 年には 47 日。手動更新は限界を迎える。
- 有料証明書でも ACME で自動更新できる。「有料 = 手動」はもう古い。
- 最多の事故原因は中間証明書の設置漏れ。設置後は必ず外部から検証する。
- 無料でもブラウザの監査基準は同じ。有料で買っているのは審査・補償・サポート。

証明書の選定・更新作業・監視の仕組みづくりまで、まとめてご相談いただけます。