



【infoCMSご契約者様限定】

Webサイトのセキュリティをチェック！ 検索結果にも影響？ 安全な通信について解説

株式会社インフォネット

2023.6.21

本日のスケジュール

■ 開催概要

日時：2023年6月21日(水) 14:00～14:30

内容：Webサイトのセキュリティをチェック！

～検索結果にも影響？「安全な通信」について解説～

主催：株式会社インフォネット

■ タイムスケジュール

- ・ 14：00～14：05 はじめに
- ・ 14：05～14：20 Webサイトのセキュリティをチェック！
～検索結果にも影響？「安全な通信」について解説～
- ・ 14：20～14：30 質疑応答

Contents

目次

- はじめに
- **サイトのセキュリティ対策のポイント**
- SSLとは？
- SSL証明書の種類
- SSLに関するよくあるご質問
- まとめ
- 質疑応答

サイトのセキュリティ対策のポイント

サイトのセキュリティ対策には「外部対策」と「内部対策」がある

攻撃されることを未然に防ぐ

外部対策



- **WAF (Web Application Firewall)**
サイトにアクセスする通信の発信元・宛先を監視するサービス。不正な発信元からのアクセスを検知した際、通信を遮断する。
- **IDS/IPS (不正侵入検知・防御サービス)**
不正な通信内容を検知し、アラートを発報する(IPS)
不正な通信内容を検知し、通信を遮断する(IDS)

など

攻撃された際の被害を抑える

内部対策



- **reCAPTCHA**
フォームのスパム対策
- **改ざん検知**
サイトの更新内容を監視するサービス
- **暗号化通信(SSL化対応)**
サイトの通信を暗号化するサービス

など



攻撃される前、された後両方に備えておくことが重要

Contents

目次

- はじめに
- サイトのセキュリティ対策のポイント
- **SSLとは？**
- SSL証明書の種類
- SSLに関するよくあるご質問
- まとめ
- **質疑応答**

SSLとは？

そもそもSSLとは？

SSL

Secure Socket Layer

SSL (Secure Socket Layer) とは、インターネット上でデータを暗号化して送受信する仕組みのひとつです。クレジットカード番号や、一般に秘匿すべきとされる個人に関する情報を取り扱うWebサイトで、これらの情報が盗み取られるのを防止するため、広く利用されています。また、SSLは暗号化に加え、電子証明書により通信相手の本人性を証明し、なりすましを防止するなど、今日のインターネットの安心・安全を支えています。

参照元 (総務省) : https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_structure_13.html

③SSLとは？

SSL化するとどうなる？

1 サイトの通信が暗号化される

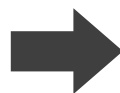


クレジットカード情報や個人情報を含む通信が暗号化される

2 URLの先頭がhttpsになり、暗号化されたWebサイトであると示される

SSL化していないサイト

http



SSL化したサイト

https

HyperText Transfer Protocol Secure

全ページSSL化することのメリット

1 Googleの検索結果で優遇される

・2014年：Google検索セントラルブログより

セキュリティは Google の最優先事項です。Google は、デフォルトでの強力な HTTPS 暗号化など、業界をリードするセキュリティを Google サービスに導入することに力を注いできました。

(中略)Googleはランキング シグナルとして HTTPS を使用することにしました。

参照元 (Google) : <https://developers.google.com/search/blog/2014/08/https-as-ranking-signal?hl=ja>

➡SSL化されたサイトを検索上優遇すると明言

➡ GoogleのSEO検索評価で優遇されるサイトの例



スマートフォン対応済のサイト

スマホ利用者増加により、モバイルサイトがSEO検索評価の軸になっている



全ページSSL化済のサイト

セキュリティ対策済みのサイトとして高評価になる

Contents

目次

- はじめに
- サイトのセキュリティ対策のポイント
- SSLとは？
- **SSL証明書の種類**
- SSLに関するよくあるご質問
- まとめ
- **質疑応答**

SSLブランドについて

インフォネット取り扱いSSLブランド

- Rapid SSL
- Global Sign
- DigiCert
- RapidSSL・ワイルドカード

その他SSLブランド(一部)

- ジオトラスト
- サイバートラスト
- セコムパスポート
- セキュアコア
- Let's Encrypt など

※その他ブランドの場合はお客様側にて取得頂き、弊社側で証明書の設置となります

自社サイトに合わせたブランド選択する

SSL証明書の認証の種類

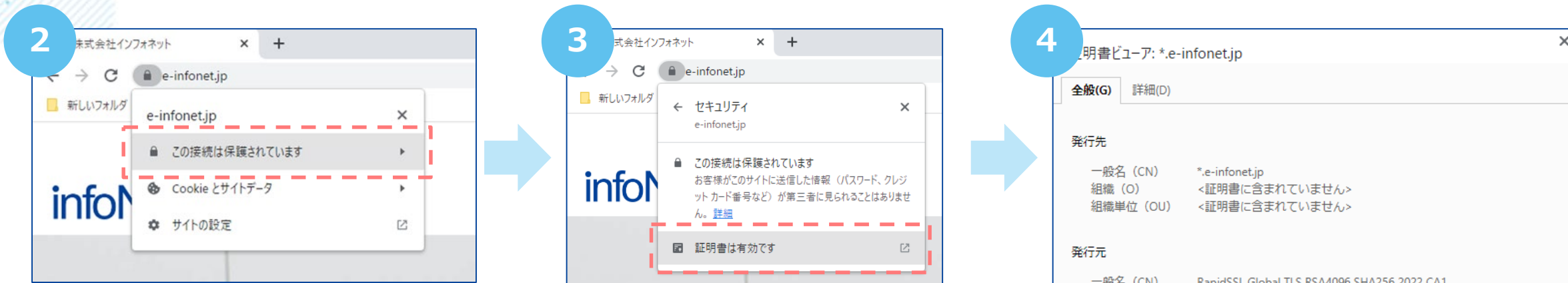
SSL認証タイプは3つ存在する

	ドメイン認証	企業実在認証	EV認証
認証レベル	★☆☆	★★☆	★★★
認証項目	ドメイン名の利用権	ドメイン名の利用権 組織の法的実在性	ドメイン名の利用権 組織の法的・物理的実在性 組織の運営 承認者・署名者の確認
特長	価格が安い スピード発行可能 個人事業主の取得可能	証明書情報に組織名 Webサイトの信頼性アップ	証明書情報に組織名と登記簿の会社法人等番号が記載 フィッシング詐欺対策

※インフォネットサーバに証明書を設置する場合はドメイン認証タイプとなります

SSL証明書の認証の種類

SSL証明書の種類や有効期限を確認する方法



- ① Google chromeでサイトにアクセス
- ② URL左の🔒マークをクリックし、「この接続は保護されています」を選択する
- ③ 「証明書は有効です」を選択する
- ④ 発行日や有効期限を確認できる

Contents

目次

- はじめに
- サイトのセキュリティ対策のポイント
- SSLとは？
- SSL証明書の種類
- **SSLに関するよくあるご質問**
- まとめ
- 質疑応答

Q : SSL化していないとどうなる？

A : 「セキュリティ保護されていない」旨の警告表示が出る可能性がある

サイトにアクセスした時、こんな表示を見たことはありませんか？



ユーザーから見ると……

「なんか怪しい会社なのかな……？」
「アクセスして大丈夫なのかな……？」
「情報が盗まれたら嫌だからアクセスやめよう」



サイトにアクセスされず
離脱してしまい、
機会損失につながる

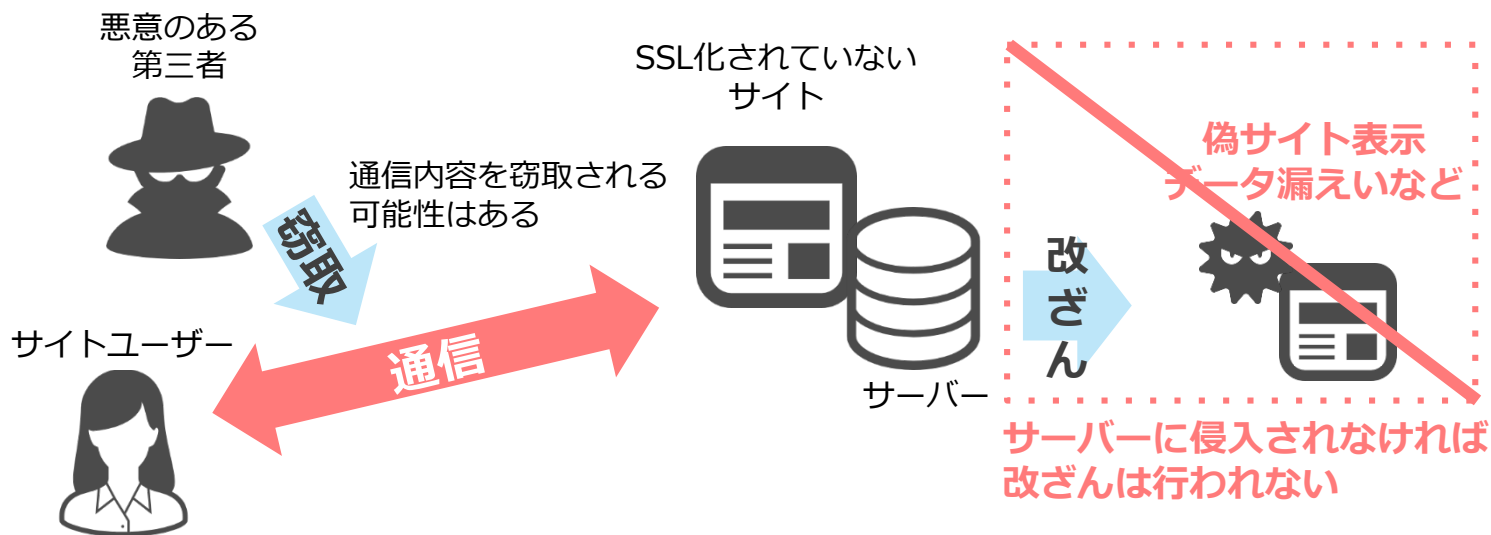


現在は必須で警告が出るわけではないが、仕様変更の可能性あり
➡未対応であれば、早めのSSL化がおすすめ

Q : SSL化しないとサイトを改ざんされる？

A : SSL化未対応でもサイトは改ざんされない

SSL化を行っていない場合、問い合わせフォームの内容やクレジットカード情報を盗み見られる可能性があります。しかし、サイトの改ざんはサーバ側に侵入しない限り行われません。



サイト改ざんのリスクに対しては、WAFや改ざん検知などの別対策が必要

Contents

目次

- はじめに
- サイトのセキュリティ対策のポイント
- SSLとは？
- SSL証明書の種類
- SSL化していないとどうなる？
- よくあるご質問
- **まとめ**
- 質疑応答

まとめ

サイトのセキュリティをチェックし、適切な対策を講じよう



サイトによって対策すべきセキュリティリスクはさまざま。
安心して利用できるサイトをつくるためにも、自社サイトの状況を確認しよう

次回以降のウェビナー予定

6月・7月のウェビナー予定

1 6月22日(木) 14:00~14:45

今すぐ対応したい！

Google Analytics4移行後のWeb解析ポイントを解説

Universal Analytics(UA)の計測停止がいよいよ2023年6月末に迫り、今後アクセス分析を行うためにはGoogle Analytics4(GA4)への移行が不可欠です。本セミナーでは、6月の移行前に準備しておくべきこと、移行後に対応すべきことなど、移行に伴う対応スケジュールについて改めて解説します。

