NET ASSIST
24/7 Guardian Deity

2023.9 #29

NEWS LETTER

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

#1 CDN特集～Cloudflareのご紹介～

Webサイトの表示速度と売上の関係性

普段スマートフォンやPCでWebサイトを閲覧するとき、表示が遅くていらいらする、ページ遷移の度に待つのがストレスになってページを閉じた、という経験はありませんか？
Amazonでは、「表示速度が0.1秒遅くなると、売り上げが1%減少する。1秒高速化すると10%の売り上げが向上する」という調査結果をだしています。
表示速度を上げることでコンバージョン率やGoogleの検索順位、売上にもつながってくるので、サイト運用者は優先して取り組みたい事項かと思います。
そこで今回はサイト表示速度改善の一つである「CDN（コンテンツ配信ネットワーク）」について説明するとともに、今年度より弊社で販売している「Cloudflare」のご紹介もいたします！

PICK UP!

CDNとは？

コンテンツ配信ネットワーク（CDN）は、エンドユーザーの近くでコンテンツをキャッシュする地理的に分散したサーバー群です。CDNを使用すると、HTMLページ、JavaScriptファイル、スタイルシート、画像、動画を含むWebコンテンツの読み込み速度を上げることができます。

CDNを利用するメリット

1. Webサイトのロード時間を改善

近くのCDNサーバーを利用してWebサイト訪問者の近くでコンテンツを配信することにより、ページのロード時間が短縮されます。訪問者は、読み込みが遅いサイトだと判断すると簡単に離れてしまう傾向が強いので、素早く遷移することが訪問者を長く留まらせるためにも重要です。

2.コンテンツの可用性と冗長性の向上

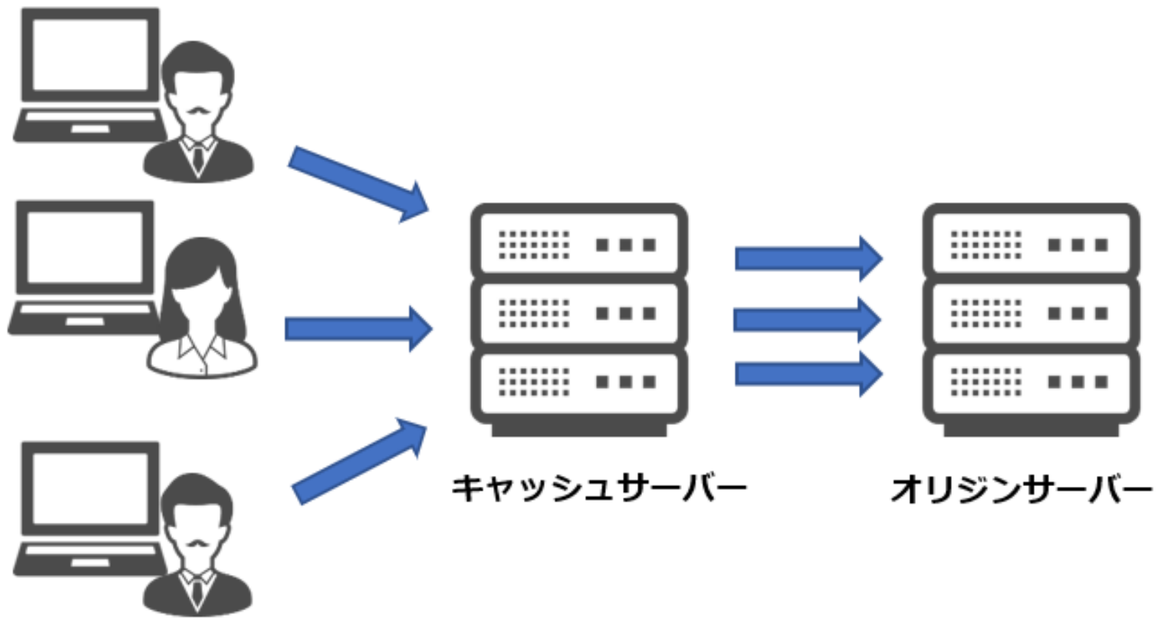
分散型という特性から多くのトラフィックに対応でき、そのほかのオリジンサーバーよりもハードウェア障害に耐えやすくなります。

3.Webサイトセキュリティの向上

DDos軽減やセキュリティ証明書などを提供することで、セキュリティ向上が期待できます。

CDNのしくみ

ユーザーが特定のサイトにアクセスする際、そのリクエストは世界中の複数地点に分散配置されたオリジンサーバーの内容・コンテンツを複製・保持したキャッシュサーバーで処理されます。ユーザーからのアクセスがオリジンサーバーに一極集中することはないため、サーバーおよびそのネットワークへの負荷が軽減され、よりスムーズなコンテンツが提供できます。
また、キャッシュサーバーは、地理的・ネットワーク的に各ユーザーにもっとも近いものが応答する仕組みです。そのため、よりスピーディーにコンテンツを届けることができます。



次ページへ

前ページより

Cloudflareとは？

2010年創業の米国企業で世界最大級のネットワークの一つです。100か国以上に合計275以上のデータセンターを構えています。（日本では東京・大阪・福岡・那覇にあり、今後も拡大予定です。）

Cloudflareには数百万のインターネットプロパティがあり、そのネットワークは毎日数万単位で成長しています。そして数百万のWebサイトのインターネットリクエストを処理し、平均で毎秒4600万のHTTPリクエストを提供しています。

Cloudflare[CDN]の特徴

従来のCDN機能である負荷分散/キャッシュに加えて、画像の最適化、Image Resizing（WebP変換）、専用ネットワークを利用できるという特徴があります。

また、セキュリティ対策としてWAF、DDos対策、Bot管理の機能が標準搭載されています。
CloudflareのみでCDN+画像最適化～セキュリティ対策まで対応することができるため、コスト最適化としても利用されることが多いです。

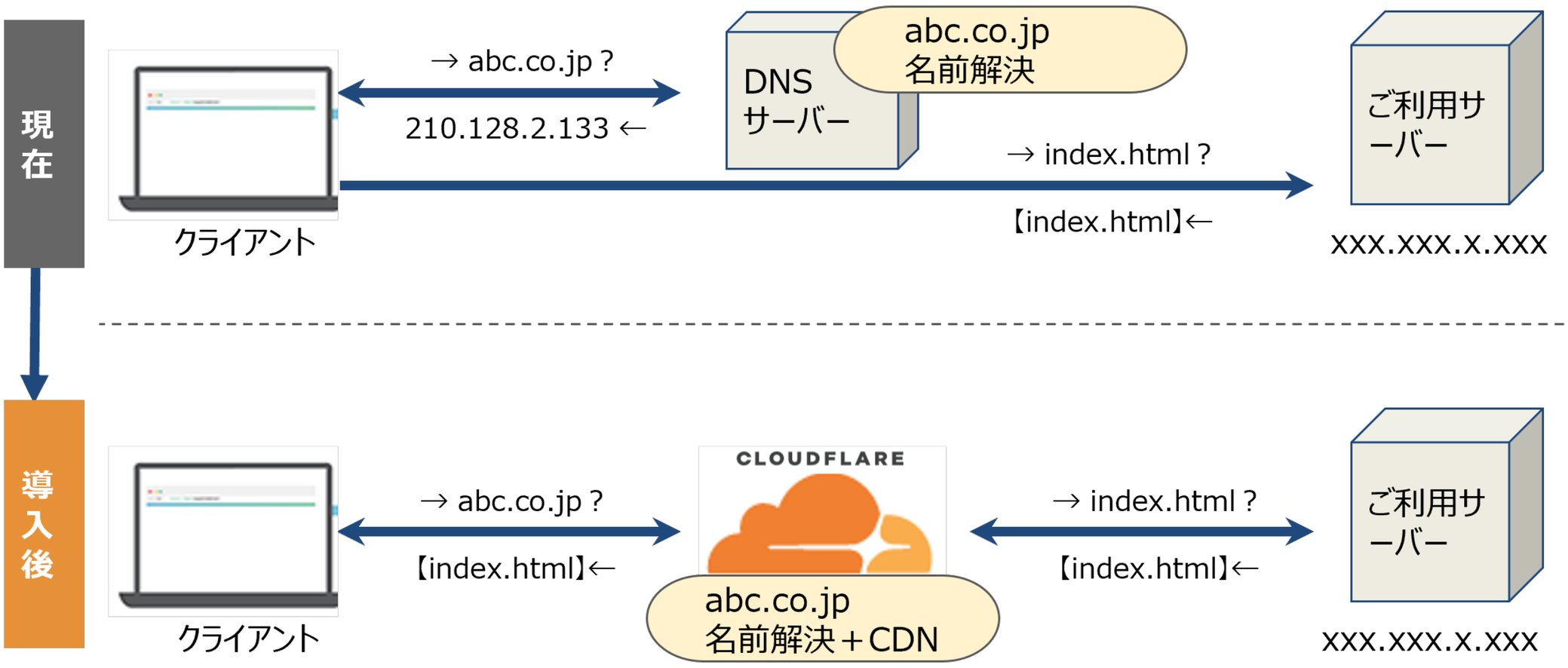
PICK UP!

Image Resizingとは

全画像のサイズ変更、品質調整、および画像のWebP形式への自動変換を行うことができる機能です。サーバー側の画像処理パイプラインを維持することなく、すばやく簡単に画像をサイトのレイアウトや訪問者の画面サイズに合わせることができます。

Cloudflare[CDN]の導入方法

DNSとして名前解決を行うことでオリジンサーバーの手前に配置します。



ネットアシストでは、本年度よりCloudflareの日本正規代理店である株式会社ドーモ社とパートナー提携いたしました。
機能の詳細説明や料金プランなどは担当営業より個別でご案内可能ですので、お気軽にお問い合わせください！

#2 情報セキュリティ白書2023を見てみよう（後編）

今月も8月号に続き、情報セキュリティ白書2023(※1)の内容をご紹介して参ります。
前号では、2022年に被害の多かったランサムウェアの事例などを抜粋してお伝えしました。
今回は趣向を変えて、「耳にしたことはあるけど、、、よく知らない」各省庁や警察のサイバー攻撃への政策・対策を抜粋してご紹介して参ります。

※1情報セキュリティ白書2023
独立行政法人情報処理推進機構（IPA）により2023年7月25日（火）に刊行された書籍です。
アンケートの回答に協力することでPDF版の入手も可能です。
独立行政法人情報処理推進機構(IPA)「情報セキュリティ白書2023」
https://www.ipa.go.jp/publish/wp-security/2023.html

デジタル庁の政策

デジタル庁は、デジタル社会形成の司令塔として、未来志向のDX（デジタル・トランスフォーメーション）を推進し、デジタル時代の官民のインフラを作り上げることを目指しています。

（1）情報システムの整備及び管理の基本的な方針

※https://cio.go.jp/sites/default/files/uploads/documents/digital/20211224_development_management_02.pdf

「情報システムの整備及び管理の基本的な方針」は、国の行政機関、地方公共団体その他の公共機関及び公共分野の民間事業者の関係者が効果的に協業できるように、情報システムの整備及び管理の基本的な方針を定めた文書を発行しています。

（2）常時リスク診断・対処（CRSA）実証事業

※https://www.digital.go.jp/policies/security/crsa

CRSAは、組織の情報セキュリティポリシー等で求められる情報セキュリティに関する統制目標（コントロール）と、情報システムの実際の状態とのギャップやリスクを可視化し、そのギャップの是正の対応を継続的に実施するプログラムです。

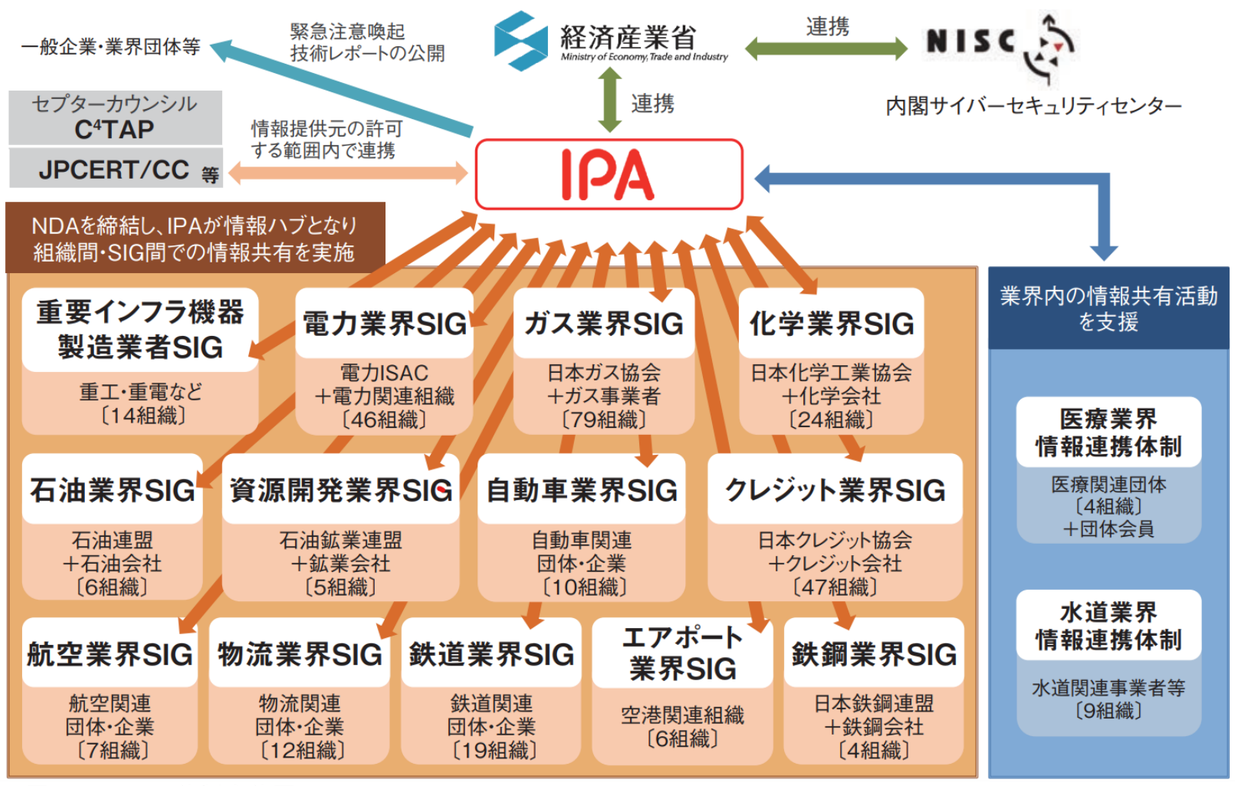
経済産業省の政策

経済産業省は、サイバー空間、フィジカル空間を統合した、サプライチェーン全体にわたるセキュリティ対策の強化に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施しています。

（1）J-CSIP（サイバー情報共有イニシアティブ）

※https://www.ipa.go.jp/security/j-csip/about.html

経済産業省の協力のもと、IPAでは2011年10月から、官民連携による標的型攻撃への対策を目的として、J-CSIPを運用しています。日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃の防御とその被害の低減を目指している。2023年3月末現在、IPAを情報の中継・集約点（情報ハブ）として15の業界から292の企業や業界団体（以下、組織）がJ-CSIPに参加しています。



■図1 J-CSIPの体制全体図
（出典）IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2023年1月～3月］」

（2）J-CRAT（サイバーレスキュー隊）

※https://www.ipa.go.jp/security/j-crat/about.html

経済産業省の協力のもと、IPAは2014年7月にJ-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan）を発足させました。J-CRATの目的は以下の通りです。

- **攻撃に気付いた組織における被害拡大抑止と再発防止**
- **標的型攻撃による諜報活動等の連鎖の遮断**

	2019 年度	2020 年度	2021 年度	2022 年度
相談件数	392 件	406 件	375 件	330 件
レスキュー支援件数	139 件	102 件	94 件	163 件
オンサイト支援件数	31 件	20 件	9 件	43 件

※一つの事案に対しての複数回のオンサイト対応を要した場合も、1 件として集計
■図2 J-CRATの活動実績

次ページへ

前ページより

総務省の政策

総務省は自らの役割を、社会経済活動を支える情報通信ネットワークの安全確保、及びサイバー空間を利用するすべての国民のサイバーセキュリティの向上を図ることとしており、2022年8月12日に「ICTサイバーセキュリティ総合対策2022」を公表しました。

(1) ICT サイバーセキュリティ総合対策2022※https://www.soumu.go.jp/main_content/000830903.pdf

サイバーセキュリティにおける総務省の役割とサイバーセキュリティを巡る最近の動向を踏まえ、「情報通信ネットワークの安全性・信頼性の確保」「サイバー攻撃への自律的な対処能力の向上」「国際連携の推進」及び「普及啓発の推進」の4点の施策の柱が掲げられています。2023年8月には、ICTサイバーセキュリティ総合対策2023も公表されました※https://www.soumu.go.jp/main_content/000895981.pdf

警察によるサイバー犯罪対策

警察では、サイバー空間をめぐる脅威に対処するため、2022年4月に警察庁に「サイバー警察局」を、関東管区警察局に「サイバー特別捜査隊」を新設しました。
サイバー警察局が、官民連携、人材育成等の基盤整備、各国との情報交換、サイバー事案の捜査指揮、高度な解析への技術支援等を担い、サイバー特別捜査隊は、国の捜査機関として重大なサイバー事案への対処、及び外国捜査機関との信頼構築や国際共同捜査への積極的参画等を担うとし、警察としてのサイバー事案の対処能力の強化を図っています。
また、2023年3月には「令和４年におけるサイバー空間をめぐる脅威の情勢等について」にて、様々なサイバー犯罪についての統計情報なども公表しています。※https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ここまで、各省庁や警察の政策・対策を見てきましたが、いかがでしたでしょうか？
発信している文書やメッセージが果たしてどこまで行き届いているのかは、疑問が残るところではありますが、国が本気で対策を講じたいと考えているのは明白です。

前編後編にわけてご紹介してきましたが、こちらはあくまでもほんの一部です。
是非実際に入手してご一読いただきたいと思います。
信憑性の高い情報を集め、できるところから適切に対策をとって参りましょう。

#3 セキュリティインシデント事例紹介

6月以降に発表された、最近のセキュリティインシデント事例をご紹介させていただきます。

スカパーJSAT株式会社

サーバーへの不正アクセスがあり対象となるファイルに、取引先の担当者および従業員等の個人情報が含まれていました。現在も調査中となっていますが、悪意ある第三者が同社子会社の従業員になりすまし、子会社のネットワークを経由して同社の社内サーバーにログインしたことに因るものであることが判明しています。

株式会社ジャックス

サーバーへの不正アクセスがあり、ランサムウェア「Elbie」に感染しました。そのためサーバーに記録していたファイルが暗号化されて使用できない状態になっていたとの事です。現時点では個人情報等が外部へ漏洩した痕跡はないと発表がありました。

株式会社富士ロジテックホールディングス

メールサーバー1台に不正アクセスがあり、同社メールサーバーから約3万件の迷惑メールが送信されていました。不正アクセス判明後に設定の強化を行い、迷惑メールの発信停止措置を既に行っているとの事です。

現在も様々なサービスで、不正アクセスや情報漏洩が続いているのが現状です。弊社では脆弱性診断やWAFなどのセキュリティソリューションもご提供していますので、ぜひお気軽にご相談ください。

NET ASSIST 24/7 Guardian Deity
株式会社 ネットアシスト
TEL 03-3985-6780
mail sales@netassist.ne.jp
web https://www.netassist.ne.jp