Verona

不正サイトを自動ブロック！

企業を守る Webフィルタリング

AMIYA

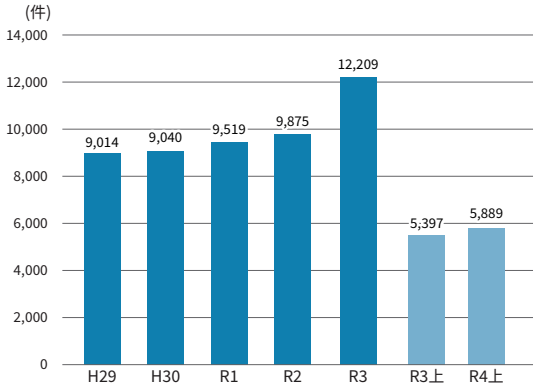
Index

01 はじめに サイバー攻撃の脅威

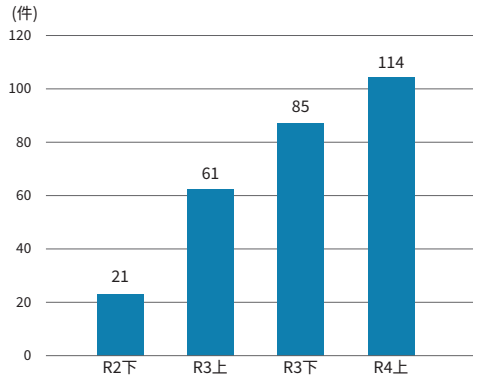
サイバー攻撃が猛威を振るっています。警察庁が発表した「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」では、サイバー犯罪検挙は年々増加しており、令和4年も増加傾向が続いていることが明らかになっています。

特にランサムウェアの被害件数の増加は止まるところを知らず、規模や業種を問わない様々な企業で多大な被害が出ています。

サイバー犯罪の検挙件数の推移



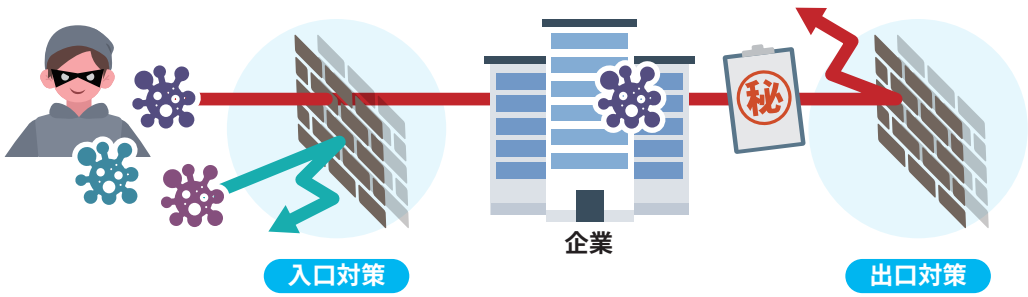
ランサムウェア被害の報告件数の推移



（参照：警察庁「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf）

これまでのサイバー攻撃は、企業内のサーバを狙った外部からの直接的な攻撃が主流であったため、ファイアウォール、IDS/IPS等の「外部からの不正アクセスを防ぐ」ことを目指した「入口対策」が有効でした。しかし、近年サイバー攻撃は多様化しており、標的型攻撃によるランサムウェアをはじめとしたマルウェアへの感染や、社員の不用意なWebアクセスによってPCを乗っ取られ、攻撃者の外部サーバ（C&Cサーバ）への通信によって内部から情報を盗まれるといった攻撃手法が増加しています。このような状況下で注目を集めているのが、「出口対策」です。

「出口対策」とは、万一攻撃者に企業内部に侵入され、内部の情報にアクセスされたとしても、外部にデータを流出させなければ被害を最小限に抑えることができる、という考え方に則った対策のことです。



代表的な「出口対策」が「Webフィルタリング」です。Webフィルタリングは、悪意あるWebサイトなどをデータベース化しておき、クライアント端末からそれらのサイトへの通信をブロックすることで、情報流出を防ぐ対策のことです。本書では、Webフィルタリングについて、どんな効果・種類があるのかなど、詳しく紹介していきます。

02 Webフィルタリングとは

Webフィルタリングとは、インターネットへのアクセスを制限するための機能です。
あらかじめ設定された条件に従って、望ましくないWebサイト等へアクセスしようとした際に、自動的にアクセスを禁止します。
企業では、主に次の目的で使用されます。

1 業務効率化

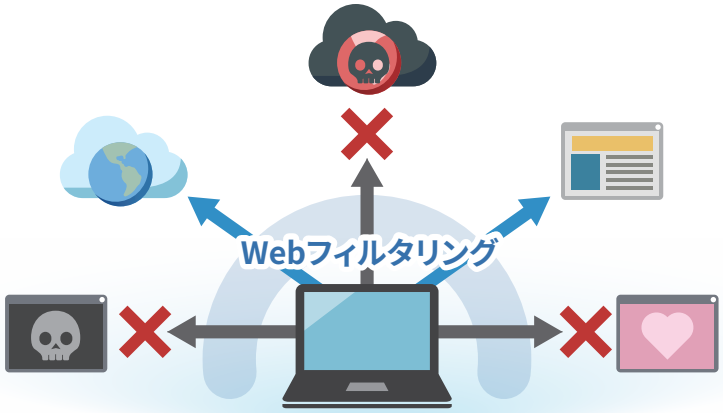
インターネット上には多くのWebサイトが存在していますが、業務中に仕事と関係のないWebサイトを閲覧すると、生産性が落ちることになります。業務上不要なWebサイトの閲覧を禁止することで、業務に集中できる環境を整備し、業務の効率化を図ることができます。

2 内部統制の強化

SNSやクラウドストレージなど、外部の送信先を限定することで、従業員による不適切な投稿や内部不正による情報の持ち出しを防止できます。また、従業員のWebアクセスも可視化できるため、不正行為の抑止効果もあり、内部統制を強化できます。

3 サイバー攻撃対策

攻撃者が用意したサイトにアクセスしてしまい、コンピュータがマルウェアに感染したり、詐欺サイト等にアクセスをしてコンピュータ内のデータを盗まれたり、といったサイバー攻撃の被害を防ぐことができます。また、コンピュータが攻撃者に乗っ取られた場合、遠隔操作のためのC&Cサーバとの通信もブロックすることができるものもあるため、広範なサイバー攻撃に対応できます。



これまでWebフィルタリングは、業務効率化や内部統制の強化の目的での導入が進んできました。

しかし、前述の通りサイバー攻撃が猛威を振るっている近年では、サイバー攻撃対策として利用される側面が強くなってきています。

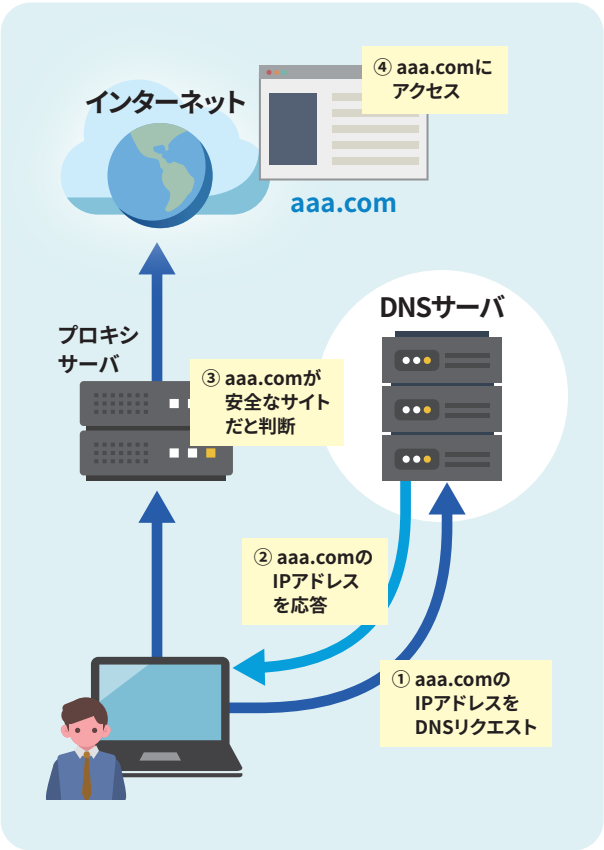
03 「プロキシ型」と「DNS型」

Webフィルタリングの提供形態として「プロキシ型」と「DNS型」の2つが代表的です。

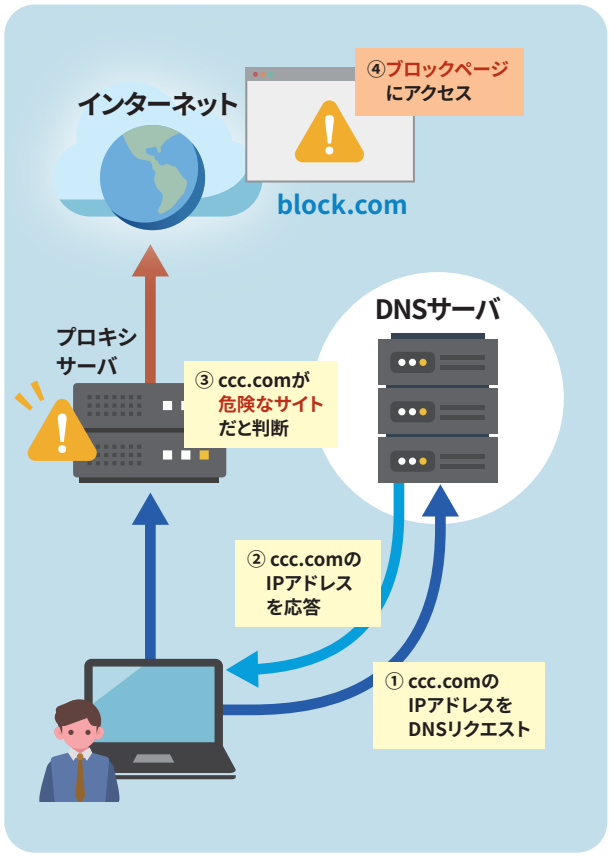
プロキシ型

webトラフィックがプロキシ経由となり、プロキシでURLチェックなどのアクセス制御を行います。

安全なサイトの場合



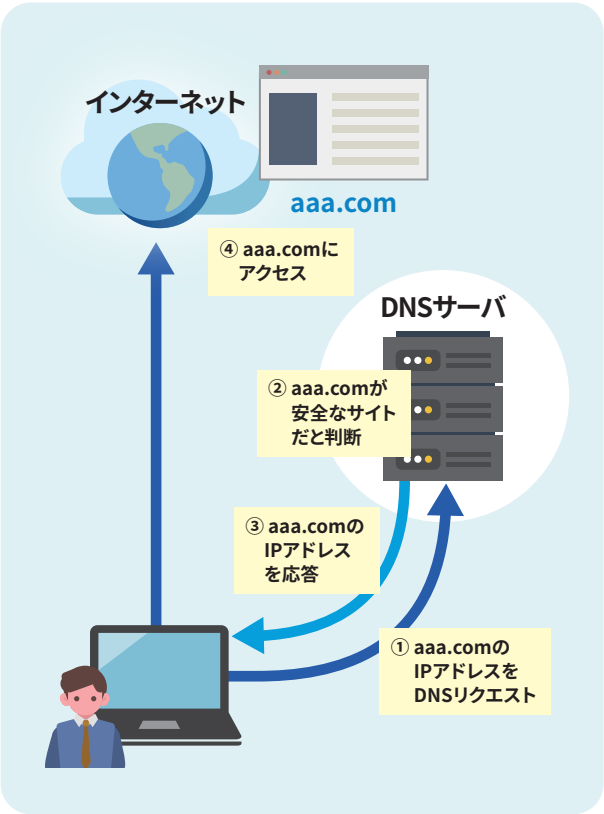
危険なサイトの場合



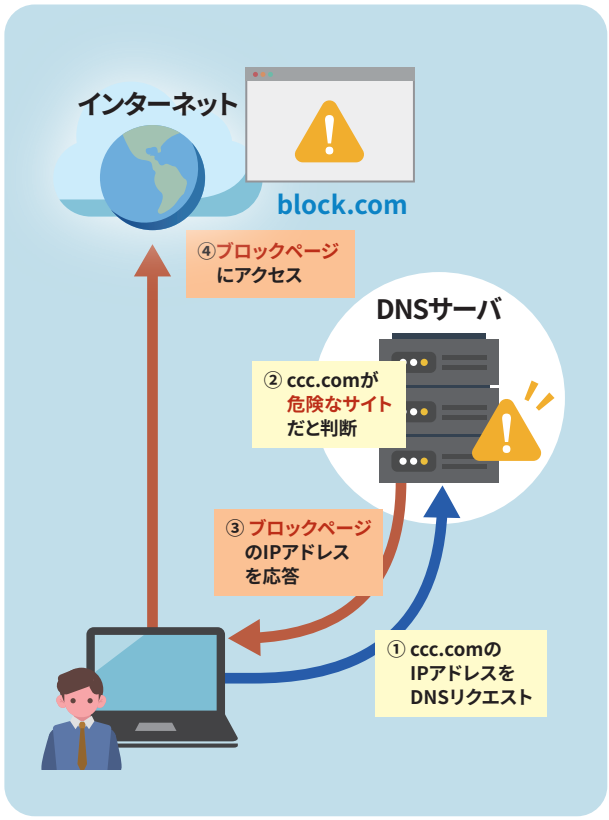
03 「プロキシ型」と「DNS型」

DNS型 エンドポイントからのDNSリクエストに対してクエリを返すことによって
アクセス制御を実施します。

安全なサイトの場合



危険なサイトの場合



「プロキシ型」と「DNS型」の違い

一つの大きな違いは、アクセス時のフィルタリング方式です。「プロキシ型」はURL単位の詳細なアクセス制御ができますが、「DNS型」はあくまでドメイン単位で危険度を判定するため、URLベースでの詳細な制御はできません。
しかし、その分「プロキシ型」はURL単位での管理が必要となるため運用が大変ですが、「DNS型」だと運用負荷が減ります。

URL
Uniform Resource Locator

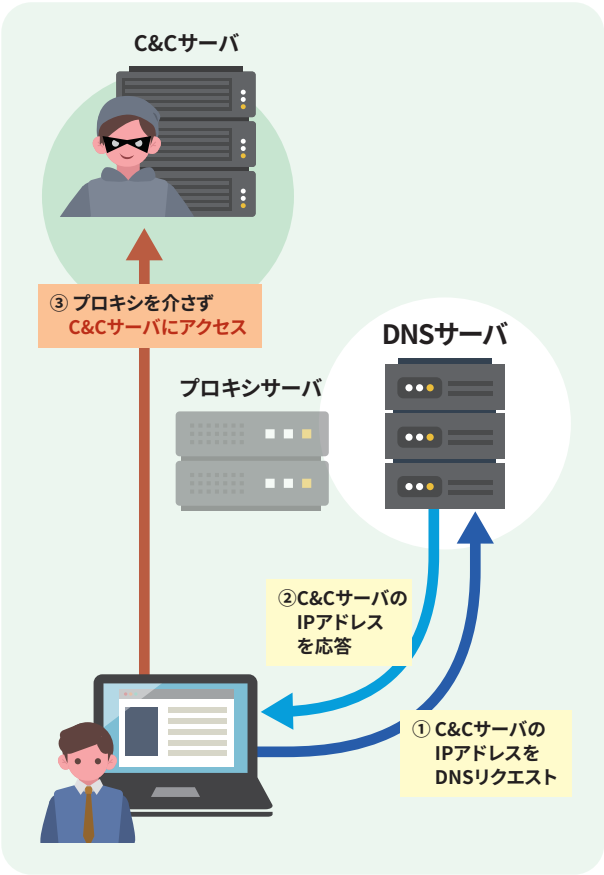
https://www.aaa.com/about/

ドメイン
DNS=Domain Name System

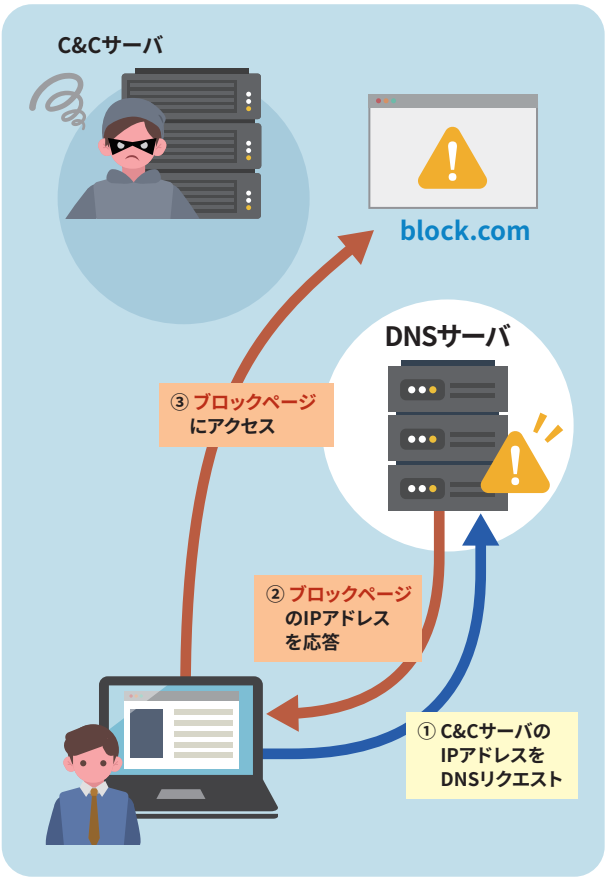
04 「プロキシ型」と「DNS型」サイバー攻撃対策に最適なのは?

URL単位での綿密なアクセス制御が可能な「プロキシ型」ですが、サイバー攻撃対策目的で利用する場合は問題点があります。なぜなら、危険なアクセス先はWebサイトだけではないからです。
例えば、ランサムウェアは、C&Cサーバを使用して攻撃者のプラットフォームと通信をしながら攻撃が進行します。しかしながら、「プロキシ型」がフィルタリングできるのはWebの通信のみであるため、これらのC&Cサーバとの通信を遮断することができません。
一方で、「DNS型」であれば、Webの通信だけでないあらゆる通信をフィルタリングできるため、幅広い悪性の通信を遮断することができます。そのため、サイバー攻撃対策目的でWebフィルタリングを実施する場合、「DNS型」が最適であるといえます。

プロキシ型



DNS型

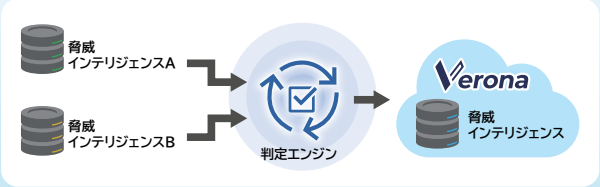


05 Veronaの DNSセキュリティサービス

VeronaのDNSセキュリティサービスは、サイバー攻撃対策に最適なDNS型のフィルタリングサービス。働く場所やVPNのON/OFFを問わず、セキュアなインターネットアクセスを実現します。

独自の脅威インテリジェンス

独自エンジンにより収集した200万以上のレピュテーション情報をベースに、独自の脅威インテリジェンスを構築。
迅速なアップデート対応により、既知・未知を意識することなく高精度な検知を実現します。



有害ドメインへのアクセスをブロック

ここが
ポイント!

働く場所を選ばない これからのセキュリティ

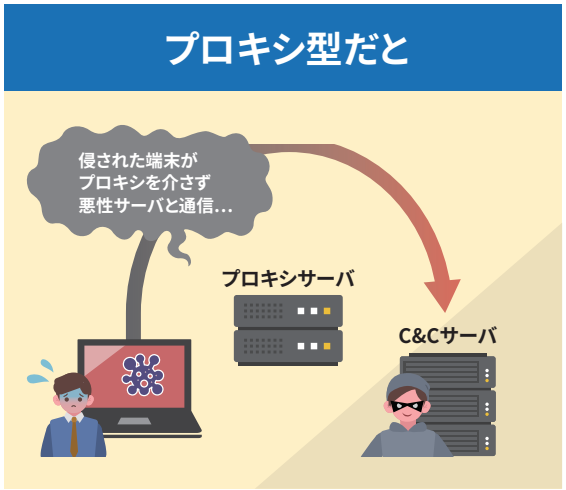
Veronaなら、フィルタリングとリモートアクセスを一つのエージェントで実現可能。
統一されたネットワークセキュリティを提供します。

05 VeronaのDNSセキュリティサービス「DNS型」だからこその強み

VeronaのDNSセキュリティサービスには、「DNS型」だからこその強みが。

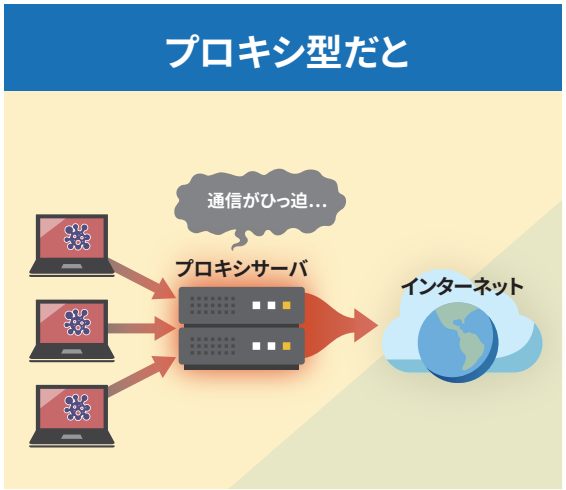
サイバー攻撃対策に

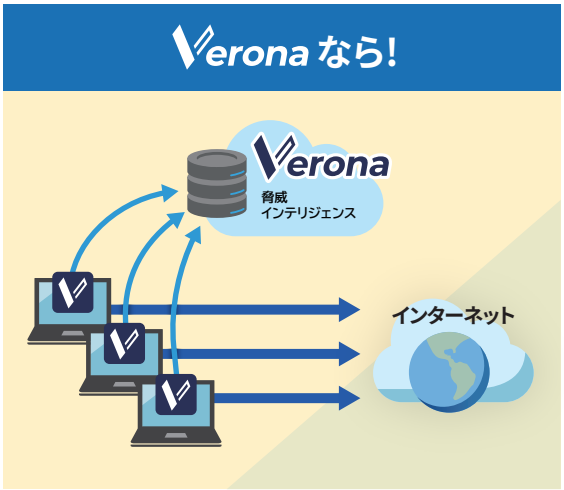
端末にインストールしたエージェントが脅威インテリジェンスにアクセス。
端末が攻撃者に乗っ取られても、不審な通信をブロックすることができます。



通信パフォーマンスを落とさない

DNSでフィルタリングした後には端末が直接インターネットにアクセス。
プロキシ型のフィルタリングと異なり、通信ボトルネックが発生しません。





05 VeronaのDNSセキュリティサービス 強固なセキュリティをかなえる 3つのフィルタリング

1 カテゴリフィルタリング

組織のポリシーに合わせて、3つのカテゴリフィルタを選択可能。
業務に不必要なサイト、危険なサイトへのアクセスを防止します。

セキュリティレベル →

Category	Security	Enterprise	Family
マルウェア配布サイト	●	●	●
疑わしい SSL 証明書を使用したサイト	●	●	●
C&C サーバ	●	●	●
ペイロード配布サイト	●	●	●
フィッシングサイト	●	●	●
トラッキング、ハッキングサイト	●	●	●
クリプトジャッキング	●	●	●
DDoS などのアタッカー	●	●	●
人種差別		●	●
暗号資産マイニング		●	●
DoH		●	●
VPN		●	●
プロキシ		●	●
賭博		●	●
アダルト			●
爆発物、危険物			●
出会い系サイト			●
薬物			●
海賊版配布			●
詐欺			●

05 VeronaのDNSセキュリティサービス 強固なセキュリティをかなえる 3つのフィルタリング

2 許可・ブロックリスト機能

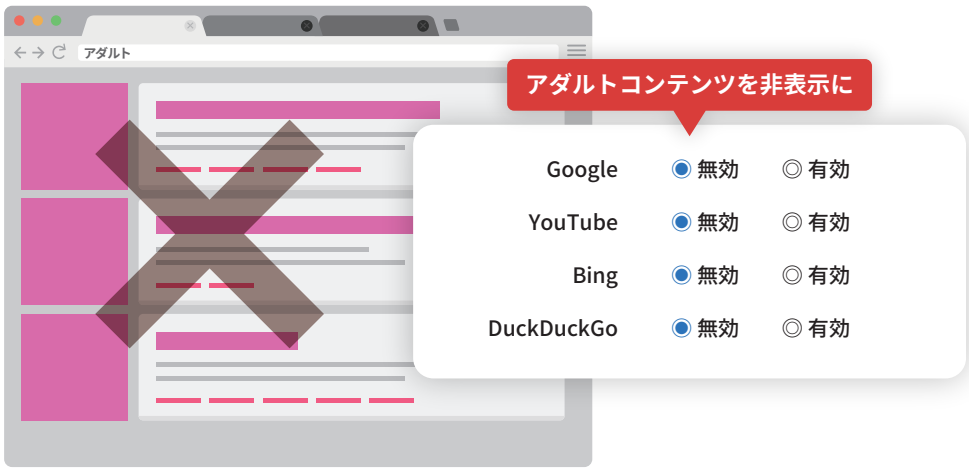
個別ドメインに対して、許可/ブロックを設定可能。
カテゴリフィルタリングでカバーできないフィルタ設定を提供します。

許可リスト
yahoo.co.jp
google.co.jp
amiya.co.jp
all-cloud.jp.
alog.app

ブロックリスト
yaaaho.co.jp
gogle.co.jp

3 セーフサーチ機能

サイト検索においてアダルトコンテンツなどを強制的に非表示に。
検索エンジンごとに個別設定が可能です。



06 おわりに サイバー攻撃対策に万全はない

本書では、サイバー攻撃の「出口対策」として、Webフィルタリングについて、どんな効果・種類があるのかなどを紹介してきました。Webフィルタリングの中でも「DNS型」のフィルタリングは特にサイバー攻撃対策効果が高く、様々な悪性の通信をブロックすることが可能になります。

しかしながら、サイバー攻撃が猛威を振るう現在、その被害を最小限に抑えるには、「入口対策」、「出口対策」のみならず、侵入されてから目的達成までに至る段階で、いかに早期に検知し対処できるかどうかに重点を置いた「内部対策」を実施することが重要です。

ログマネジメントソリューション

ALog

サーバアクセス市場 国内シェア 16年連続 No.1 2006～2021

そこで紹介したいのが、網屋の「ALog」です。「ALog」は、多様なITシステムのログをエージェントレスで自動集約・運用監視するログマネジメントソリューション。ログを収集・監視することで、サイバー攻撃を受けている事実をいち早く検知し、早期の対応により被害を最小限に抑えることを可能にします。また、特許を取得した独自のログ翻訳変換・整形技術をはじめとした、ログ管理の「むずかしいをカンタンに」する技術により、専門知識やノウハウがなくとも、高度なログ活用を実現。サイバー攻撃対策だけでなく、内部不正対策や監査報告など、あらゆるビジネスの課題を解決します。

さらに、2023年2月に待望のクラウド版「ALog Cloud」をリリース。ALogシリーズのよさはそのまま、動作環境の準備・運用不要でログ管理をスタートできるようになりました。

Verona

Veronaはゼロトラストセキュリティを実現するクラウド管理型ゼロトラストサービスです。
場所を選ばない、統一されたネットワークセキュリティを実現します。

お問い合わせ先

株式会社網屋
ネットワークセキュリティ事業部
TEL：03-6822-9995　E-mail： infra-sales@amiya.co.jp

詳しい製品概要資料はこちら

開発元

株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/