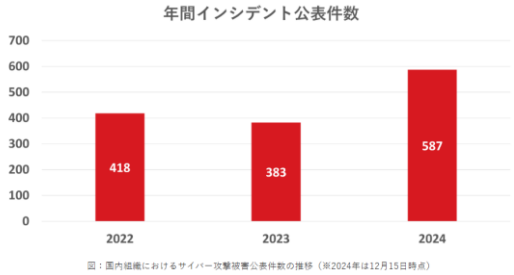
ZeroDarkweb on iDC

御社のホームページ、セキュリティ対策していますか？

Webサイトへのサイバー攻撃は増加傾向にあります。その対象は大企業から関連会社、取引先を含めた中小企業に広がっています。

サイバー攻撃被害の公表件数は過去最大に！

2024年に国内法人組織より公表されたセキュリティインシデントの総数は587件で、2023年の383件に対し大きく増加しました。
2024年の件数を平均すると一日当たり、1.7件の被害が公表されており、毎日どこかで1～2組織がサイバー攻撃被害を公表している状態にあります。



図：国内組織におけるサイバー攻撃被害公表件数の推移（※2024年は12月15日時点）

二次被害の増加！

2024年のインシデント公表件数が増えた最も大きな理由は、サイバー攻撃の二次被害の増加です。2024年の二次被害の合計件数は213件であり、全体の36.3%、つまり三分の一以上がこの二次被害であったことがわかります。

トレンドマイクロ　メールマガジンより
https://www.trendmicro.com/ja_jp/jp-security/24/l/expertview-20241223-01.html

SSL対応だけでは不十分！

SSL対応によりホームページの真正性が保証され、通信が暗号化されるため盗聴を防ぐことができますが、Webサイトへの不正アクセスを防ぐことはできません。
もし不正アクセスされてしまうとWebサイトから重要なデータが盗み取られたり、改ざんされたりするだけでなく、大事な取引先へ二次被害を与えてしまうリスクがあります。

特に ECサイト（オンラインショップ）は、Webスキミングや改ざんによる情報漏洩が多発しています。

ダークウェブに情報が流れていないか調査することができます。

よくあるサイバー攻撃

SQLインジェクション

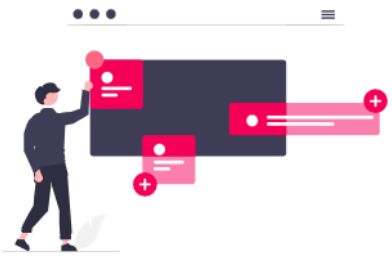
問い合わせフォームや検索フィールドなど命令文を入力し、データベースへ不正にアクセス、重要データを抜き出したり、書き換えたりする攻撃

クロスサイトスクリプティング XSS

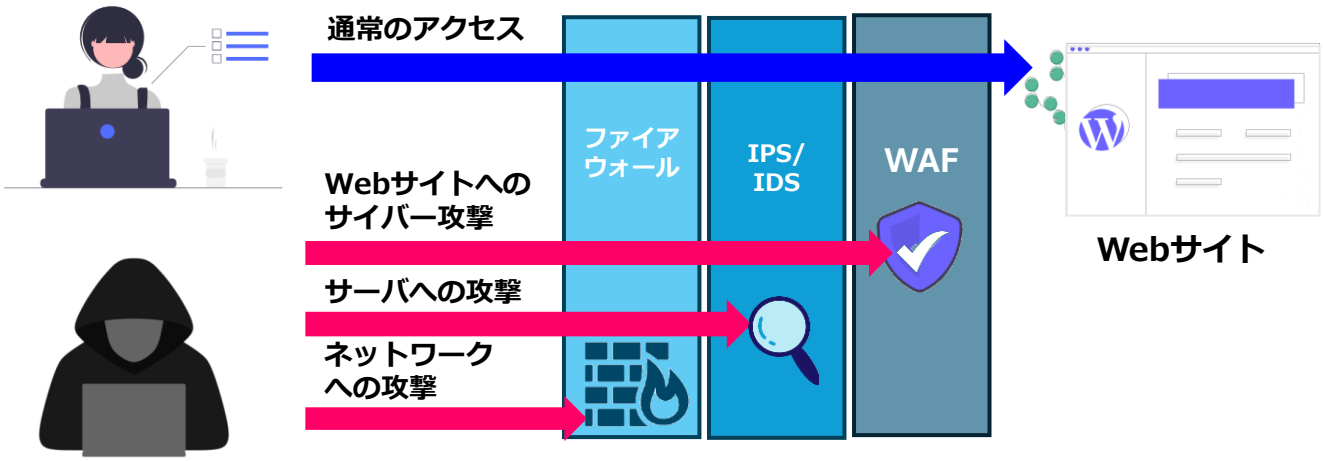
入力フォームなどを改ざんし、ユーザ情報や機密情報を盗み出したり、Webサイトを乗っ取る攻撃

ディレクトリトラバーサル

公開されたファイル名から、非公開のファイル名を推測し、機密情報にアクセスしたり削除したりする攻撃



これらのサイバー攻撃は、通常のWebアクセス（ http / https ）を利用して行われるため、ファイアウォールでは防げません。



ファイアウォールはネットワーク攻撃を遮断する装置またはソフトウェア
IPS/IDSはネットワークやサーバへの不正アクセスを検知し防御するシステム

近年、国内でもWebサイトへの不正アクセスにより個人情報などの重要データが流出する事件が多発しています。更には、それを外部から指摘されて初めて気づくケースも多くあります。

情報漏洩は企業や組織にとって事業存続にかかわる重大なリスクです。セキュリティ対策は先手必勝！早めの対策をお勧めします。

サテライトオフィスの情報漏洩調査サービス For Zero Darkweb

情報漏洩自動検知

被害状況レポート

強いセキュリティ体制を構築

Darkwebとは？

Darkwebは、GoogleやYahooなどの一般的な検索では表示されることがなく、専用のツールやブラウザからでないとアクセスできないWebサイトです。Darkwebでは仮想通貨を使った銃や禁止薬物の取引から、マルウェアやランサムウェアなどの悪性プログラムの開発および販売、そして個人情報や企業のアカウント情報、機密情報などを販売しています。

日本企業の流出現況

2023年1月、Zero Darkwebは日本の大手企業100社を対象にDarkweb情報流出調査を実施した結果、合計流出件数45.3万件、1,000件以上の機密文書がDarkwebに流出され、販売されている企業は54社で本当に深刻な状況です。

ダークウェブ情報漏洩によるリスク

外国からのマルウェア・ランサムウェアの攻撃やエモテットメールのようなサイバー攻撃によって情報が流出されてしまうと、企業・組織にとって信頼を失ってしまいます。個人情報を取り扱う企業様は定期的な調査や監視が必須であり、放置してしまうと大きな損失を発せさせるリスクがあります。

ZeroDarkwebの機能

ZeroDarkwebは、ダークウェブに流出したIPアドレス、文書、ハッキングデバイス情報の調査を行い、レポートを提供します。

機能詳細

流出した情報を常時自動検知

ZeroDarkwebのエンジンが、指定したドメインの漏洩情報を常に調査委、漏洩したメールアドレスやパスワードを報告します。

攻撃される可能性があるIPアドレスを調査

Darkweb流出したIPアドレスは今後の攻撃対象になりやすいです。いつどのパソコンから流出したのか確認できます。

漏洩・対応状況をリアルタイムで確認

管理ページで漏洩状況・対応状況をリアルタイムに確認できます。通常の監視から流出や攻撃があったときの対策になります。

ドメイン単位でお申し込み

機能	詳細	標準価格（税抜・年額） 設定・管理費込み
ZeroDarkweb on iDC	メールアドレスやパスワード、IPアドレス、文書の漏洩状況を調査します	□100名以下: ¥510,000 □100名以上: ¥990,000

※ZeroDarkwebはサテライトオフィスのサービス

株式会社 イシマル

https://www.ishimaru.ne.jp

□長崎本社　：長崎市田中町587-1　Tel:095-834-0330　Fax:095-834-0331
□佐世保支店：佐世保市卸本町8-2　Tel:0956-26-1400　Fax:0956-33-2328
□島原支店　：島原市前浜町甲74-1　Tel:0957-63-0735　Fax:0957-64-4353
□北九州支店：北九州市小倉北区熊本１丁目13-5　Tel:093-923-1400　Fax:093-923-1408

お問い合わせ先：