滋賀県警察サイバーセキュリティ情報

サイバーコネクトSHIG@

R５年度 No. 1

今、注目のサイバーセキュリティに関する情報をお届けします。

Cyber connect shig@

サイバー攻撃のリスクを減らす取組み実施中！

インターネットの「脆弱性」点検してみませんか？

点検：無料

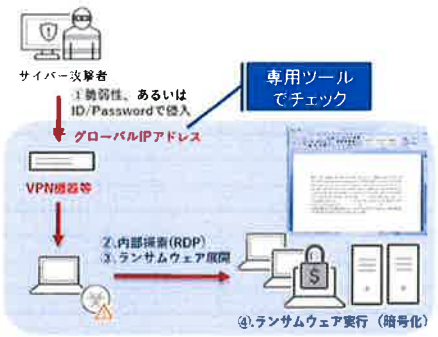
サイバー攻撃者は、インターネットを使って攻撃対象を常に探索しています。
VPN機器やWebサイトに脆弱性があると、不正に侵入され情報を盗み取られたりランサムウェアに感染したりします。また、第三者への攻撃の踏み台にされるなどの被害が発生します。
この種の脆弱性を未然に把握して、対処できれば被害のリスクを減らすことができます。
そこで、**滋賀県警では、立命館大学（サイバーセキュリティ研究室）のご協力を得て、県内事業者の方を対象に、インターネットの脆弱性点検を実施（試験実施）しています。**
費用は無料です。セキュリティ対策の一環としてぜひご利用ください。

【点検１】ランサムウェア侵入リスク診断

先着100社限定

VPN機器や公開しているポートを起点にランサムウェアに感染する事案が増加しています。
VPNはセキュリティの高い通信を行う手法ですが、機器に設定されたグローバルIPアドレスに脆弱性があると攻撃を受けてしまいます。グローバルIPアドレスが危険な状態で露出していないかどうかを確認することが重要です。

対象業者	・VPN機器を利用している業者 ・固定IPアドレスを契約し、サーバ等に設定している業者 ※滋賀県内事業者のみ
診断方法	グローバルIPアドレスが危険な状態で露出していないかを専用ツールを使って点検します。
必要なもの	グローバルIPアドレス　ネットワークに負荷は一切かかりません。



グローバルIPアドレスの確認方法は？
- **SSL-VPN装置については、導入業者にお問い合わせいただくか、Web管理コンソール等から閲覧する方法があります。**
- **グローバルIPアドレスについては、契約プロバイダやサーバ、ネットワーク等の導入業者にご確認ください。**

※この診断は、「トレンドマイクロ株式会社」と連携して実施しています。

【点検２】Webサイト脆弱性点検

随時実施中

公開されているWebサイトに脆弱性があると、侵入されたり改ざんされるおそれがあります。
Webサイト作成ソフトウェアの脆弱性には十分注意する必要があります。
深刻な脆弱性が発見されたWebサイトには、警察から注意喚起させていただいております。

対象業者	Webサイトを公開している業者 ※滋賀県内事業者のみ
点検方法	Webサイトのバージョンをチェックします。 （当面はWordPressで作成されたWebサイトに限ります。）
必要なもの	WebサイトURL

公開されているWebサイトURLを収集して専用ツールで点検しています。

申し込みはこちら（点検１、点検２）

※診断結果は、調査研究にも使用させていただきます。 個別の診断結果は公表しません。

上記の診断・点検は簡易的なもので、インターネットの安全性を保障するものではありません。
サイバー攻撃は日々進化していますので、サイバーセキュリティ対策もアップデートしていきましょう。

«CS情報SHIG@» スマートフォンのセキュリティ対策も確認しましょう。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表）

県警webページ →

https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html

滋賀県警察サイバーセキュリティ情報 RENEWAL

R５年度 No. 3

サイバーコネクトSHIG@

今、注目のサイバーセキュリティ・経済安全保障に関する情報をお届けします。

Cyber connect shig@

警察による経済安全保障の推進

● 日本の企業、研究機関等が保有する高度な技術情報等を、自国産業の強化や軍事技術への転用しようとする外国に狙われる可能性があります。

● 技術情報等の流出は、自社の損害だけでなく、取引先をはじめとする関連企業にも及ぶ上、日本の技術的優位性の低下を招くなど、日本の独立、生存及び繁栄に影響を与えかねません。

● 警察では、関係機関との連携を強化し、技術情報流出防止に向けた対策の一環として、企業やアカデミア等を訪問して過去の検挙事例などに基づく各種情報の提供等の、いわゆる「アウトリーチ活動」を展開しています。

滋賀県警察シンボルマスコット
けいたくん

情報流出の主な手口

サイバー攻撃

諜報工作

経済活動
学術研究

合法性・妥当性の濃淡の異なる様々な手法で秘密情報が狙われるように

✓ランサムウェア ✓標的型による攻撃 ✓マルウェア感染 ✓不正アクセス etc.	✓SNSによるｱﾌﾟﾛｰﾁ ✓多額の金銭謝礼 ✓脅迫・隠蔽工作 ✓ﾍｯﾄﾞﾊﾝﾃｨﾝｸﾞ etc.	✓共同研究 ✓大学間協定 ✓人材交流 ✓買収、合弁 etc.

«サイバーセキュリティ情報SHIG@»デマやフェイクニュースに注意してください。

滋賀県警察本部　警備第一課　077-522-1231（代表）

滋賀県警察サイバーセキュリティ情報 RENEWAL

R５年度 No. 4

サイバーコネクトSHIG@

今、注目のサイバーセキュリティ・経済安全保障に関する情報をお届けします。

cyber connect shig@

経済安全保障の推進

技術情報流出の事例紹介

近年の不正競争防止法違反の検挙事例

<事案の概要>

- 大手通信関連会社の日本人従業員が、外国情報機関員とみられる者から唆され、営業秘密を漏えい。
- 情報機関員とみられる者は道端で偶然を装い声を掛けて社員にアプローチ。

～ 個人への接近手口 ～

→ 道端で、見知らぬ外国の人に声をかけられる
→ 個人的に会おうと酒席へ誘われる
→ 「お礼」としてプレゼントやご馳走される
→ アクセス制限のある情報の提供をお願いされる

要注意

- 企業や大学等におかれましては、技術情報等の流出防止に向けた各種対策の推進をお願いします。
- 不審な動向や情報等を少しでも把握された場合は、警察に情報提供や相談をお願いします。

«サイバーセキュリティ情報SHIG@»デマやフェイクニュースに注意してください。

滋賀県警察本部 警備第一課 077-522-1231（代表）

滋賀県警察サイバーセキュリティ情報

サイバーコネクトSHIG@

R５年度 No. 5

今、注目のサイバーセキュリティに関する情報をお届けします。

Cyber connect shig@

DDos攻撃への対策について

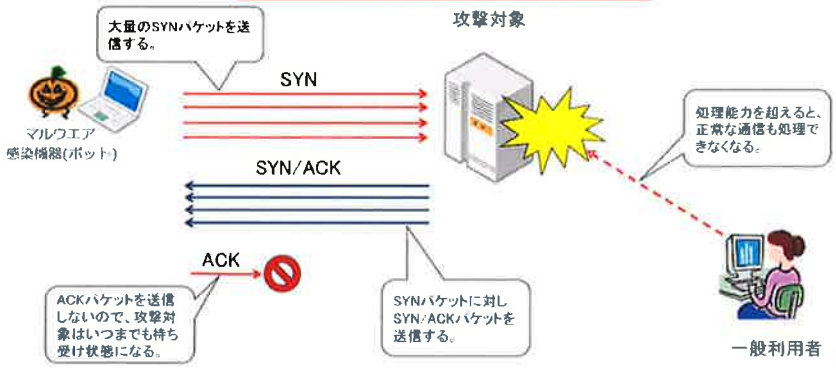
DDos攻撃とは

DDoS攻撃とは、攻撃者などが不正に操作した多数のパソコンなどから、攻撃目標に一斉に多量の問合せなどを行い、攻撃対象の反応が追いつかず利用できない状況にする攻撃。

最近のDDoS攻撃に見られる特徴と対策

特　徴

TCP(SYN)フラッド攻撃



★攻撃元IPアドレス

攻撃元となるIPアドレスは、

約99%が海外に割り当てられたIPアドレス

（約１%の国内IPアドレスは警察において対策を実施。）

★通信量の増加程度

最大で100Gbps程度の通信量の増加が確認。

★DDoS攻撃の手口（主なもの）

・TCP（SYN）フラッド
TCPの接続要求を行うSYNパケットのみを大量に送りつけて放置し「応答待ち状態」を大量に作り出す攻撃

・HTTPフラッド
標的に（大量の）HTTPリクエスト（データ送信要求）を送りつける攻撃。

このほか、Slow HTTP DoS攻撃※についても確認されているので注意が必要。
※　Slow HTTP DoS攻撃は、DoS攻撃の手口の一つであり、特定のTCPセッションを長期間継続することにより、Webサーバのセッションを占有してアクセスを妨害するもの。

対　策

脆弱性無料点検実施中

1　海外に割り当てられたIPアドレスからの通信の遮断
利用対象者が国内に限られるサイトの場合は、海外に割り当てられたIPアドレスからのアクセスを制限。

2　CDN、WAFの導入
CDNやWAFなどの通信量を制御するためのサービスを導入し、DDoS攻撃を防ぐため必要な設定を行う。

3　サーバ設定の見直し
同一IPアドレスからのアクセス回数を制限、タイムアウト設定を見直す。

※詳しくは
コネクトSHIG@No.1にて

≪CS情報SHIG@≫OSやアプリを最新のものに更新し、定期的にウイルスチェックしましょう。

滋賀県警察本部　サイバー犯罪対策課　警備第一課　077-522-1231(代表)詳細は県警webページで　→