

ASM サービス

Attack Surface Management

無償簡易調査 キャンペーン実施中

※キャンペーンは一定数に達しましたら終了します

調査範囲
(検知件数のみ)

- ☒ 攻撃可能性の高い脆弱性
- ☒ 外部公開されたログインページ / 認証プロンプト
- ☒ 漏洩アカウント
- ☒ 発見された IT 資産

Attack Surface Management 簡易調査報告書

調査結果

調査対象ドメイン: ist-software.co.jp

発見されたリスク

ソフトウェア等の脆弱性

対応の優先度が高いと思われる脆弱性の件数 ☐ 件

※下記の観点で検出されました。

・既に攻撃が検出されている

・攻撃コード(PoC)が公開されている

・リモートから攻撃可能

漏洩アカウントを利用した不正ログインのリスク

公開されたログイン画面、またはログインプロンプト ☐ 件

アカウント漏洩件数 ☐ 件

発見された IT 資産

ホスト名 IP アドレス オープンポート ソフトウェア

311 87 16 32

コメント

対応の優先度が高いと思われる脆弱性、また、不正ログインのリスクが発見されましたので、詳細な調査をお勧めします。

以上

Attack Surface Management の必要性

JPCERT/CC

ランサムウェアによる攻撃や

不正アクセスを防ぐため JPCERT/CC では以下の対策を呼び掛けています

ー 01

インターネットなど外部から接続可能なシステムの点検

- 外部から接続可能なシステムの棚卸し
- 製品およびシステムのファームウェアおよび稼働ソフトウェアのバージョン確認
- 深刻な脆弱性への修正対応の検討およびサポート終了製品の代替移行検討

ー 02

攻撃対象の最小化、認証強化、検知強化の検討

- 適切なアクセス制御による許可制限、不要なアカウントの棚卸しの検討
- 初期パスワードの変更、二要素認証などを用いた認証強化の検討
- 認証ログや通信ログの監視や確認などによる不審挙動の早期検知の検討

経済産業省が

「ASM (Attack Surface Management) 導入ガイドンス ～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」

を取りまとめました (2023年5月29日付で公表)

※出典 <https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html>



ー 製品に関するお問い合わせはこちらまで

株式会社ISTソフトウェア

※プライム市場上場アイネットグループ

株式会社 IST ソフトウェア

ソリューション事業本部 SP 事業部 営業部

☎ 03-5480-6711

✉ security-sales@ist-software.co.jp

〒144-8721 東京都大田区蒲田 5-37-1 ニッセイアロマスクエア 13F

URL <https://www.ist-software.co.jp/>

サービス詳細はこちら



20230623CAN