

標準サービス

セキュリティ監視

- リモートアクセス装置より出力される、リモートアクセスの利用記録をセキュリティ分析システムに集約し、サイバー攻撃事例をもとに開発された分析ルールにより自動分析します。
- お客様環境でアクセスログを取得・保管されていない場合は、万が一の事態に備え、送信いただくアクセスログをT S設備にて6ヶ月間保管します。
- ※ お客様宅内のリモートアクセス装置を監視対象とする場合、対象装置にてT S設備へアクセスログを転送頂くための設定を投入いただく必要があります。
- ※ T Sリモートアクセスサービスをご利用の場合、お客様側での導入作業は不要です。

不審アクセスの検知と通知

- 不審アクセスを検出した場合には、検出内容および対処方法を含む警報を発報します。
- 警報は、不審アクセスの内容に応じて、即時/日次/週次で発報します。
- 警報の発生はメールにて通知いたします。警報の内容は、機密性確保のため、Webポータルに掲載いたします。

Webポータル

- 不審アクセスの警報や月次レポートをいつでもご確認いただけます。
- 多要素認証により機密性を確保しております。



月次レポート (サンプル)

- リモートアクセス装置の安全度、当月に発報した警報の内容、リモートアクセスのご利用実績を月次で報告いたします。
- お客様がご利用のリモートアクセス装置に脆弱性が判明した場合には、対策方法とともにお知らせいたします。

安全度評価

2. 監視結果サマリ

安全度
B

・対処が必要な不審アクセスが検出されています。
・VPN装置の管理状態は良好です。

< 安全度の評価 >
指標 I 警報の発生状況

○ 良好	B	B-	A
△ 要対処	C	B	B

× 危険 △ 要対処 ○ 良好

指標 II VPN装置の管理状態

○ 良好	B
------	---

1. 警報の発生状況

評価	種別	1アカウントあたり	数値	個別評価
要対処	1) 不審アクセス件数	0.1	0.4	29
	2) ログイン試行件数	100	25	10,267

II. VPN装置の管理状態

評価	種別	基準値	状態	個別評価
良好	1) ファームウェアの脆弱性対策	実施済	○ 未実施	○
	2) アカウント管理技術 (IP制限/アカウント数)	0	47	○

警報の発生状況 / リモートアクセスの利用傾向

3. 当月に発生した警報と推奨対策

(1) 不審ログインの発報件数

不審なアクセスと思われるログインの発生状況は下表のとおりです。推奨対策をご参照いただき、対処をお願いいたします。
(警報の詳細は「6. (1) 警報の一覧」に掲載しております)

< 警報の内訳 >

種別	No	検知内容	警報
不審ログイン	1	勤務時間外からのアクセス	27
	2	指定地域外からのアクセス	2
	3	多重ログイン	0
	4	長時間アクセス	0
	5	未承認アカウントによるアクセス	0

(推奨対策)

No	検知内容	推奨対策
1	1 勤務時間外からのアクセス ① 利用者の本人のアクセスであるか、確認してください。 ② 以下の記録を確認してください。 (発生/日時/時間帯/作業)	
2	2 指定地域外からのアクセス ① 作業場所を確認してください。 ② アクセス元からのIPアドレスを確認してください。 ③ 対象アカウントのパスワードをリセットしてください。	
3	3 多重ログイン ① 利用者の本人のアクセスであるか、確認してください。 ② 本人からのアクセスと認識できない場合は、変更してください。	
4	4 長時間アクセス ① 作業場所を確認してください。 ② 利用者の本人のアクセスであるか、確認してください。 ③ 以下の記録を確認してください。 (発生/日時/時間帯/作業)	
5	5 未承認アカウントによるアクセス ① 対象装置にて発行されたアカウントであるか、確認してください。 ② お客様にて発行されたアカウントである場合は、アカウント数(警報の数)と、装置側で発行されたアカウント数(検知数)を照合してください。	

脆弱性情報

5. ご利用機器に関する脆弱性情報

(2) 脆弱性情報と推奨対策

種別	発生数	件名	種別
1	1	FortiOS SSL-VPNに、任意のコードが実行される脆弱性が発生	110

1. 対象となる製品

項目	内容
製品名	FortiGate-VM (Fortinet) 製品
主な利用環境	FortiGate-VM (Fortinet) 製品
脆弱性のあるバージョン	FortiGate-VM (Fortinet) 製品

2. 対策方法

区分	内容
個人対策	FortiGate-VM (Fortinet) 製品の更新
推奨対策	SSL-VPN機能の無効化

3. (参考) 詳細情報

項目	内容
脆弱性の概要	① 本件 脆弱性により、遠隔サーバ(権限制限を課せられる)に脆弱性がある ② 本件 脆弱性はネットワーク越しに悪用可能である ③ 本件 脆弱性を修正するパッチが提供されていない
脆弱性の影響	FortiGate-VM (Fortinet) の FortiGate-VM (Fortinet) の脆弱性
脆弱性の情報(注)	CVE-2022-48131に該当する脆弱性
参考URL	https://www.fortinet.com/ja/2022/02/20220210vm

記載されている会社名、製品名およびサービス名称は各会社の商標または登録商標です。記載内容は2023年10月現在のものです。記載された仕様は予告なく変更する場合があります。



株式会社トヨタシステムズ

TEL : 050-3142-7889 Mail : helpdesk01@tns.toyotasystems.com

URL : <https://www.toyotasystems.com>



2019年第1版