RICOH

ユーザーマニュアル Ver1.0

RICOH

目次

1　はじめに

表示	説明
本文中の青文字+下線	ハイパーリンク（ページ誘導）です。

- 管理者様はご使用前に本書を最後までよくご確認の上でご利用ください。
- お客様データの消失による損害、その他本サービスおよび使用説明書の使用または使用不能により生じた損害については法令上賠償責任が認められる場合を除き、当社は一切その責任を負えませんので、あらかじめご了承ください。
- お客様が追加、修正した情報、パスワードの管理についてはお客様にてお願いいたします。
- お客様がご利用の ISP（インターネット サービス プロバイダー）や NTT 回線のトラブル及びメンテナンス時には本サービスをご利用いただけない場合があります。
- 本機器の機器管理画面を操作する際の Web ブラウザは Google Chrome もしくは FireFox の最新版をご利用ください。

2　おことわり

- 本資料の内容の一部または全てを無断で複写することは禁止されております。
- 本資料の内容は事前の予告なく変更されることがあります。
- 変更した設定による影響については責任を負いかねますので、ご了承ください。

RICOH

3　ゲートウェイセキュリティパック Lite「サイバー脅威レポートサービス」とは

- お客様宅に設置しているFortiGate（ゲートウェイセキュリティパック Lite 専用機器）のログ（1ヶ月間分）を調査・分析したPDF形式のレポートをポータルサイトに公開します。お客様には毎月1日にメールでその旨ご案内します。
  ※但し、回線不具合やシステム不具合があった場合はこの限りではありません。

  [レポート掲載内容 例]
  - 分析結果の概況
  - 重要度の高い事象に対する分析結果と対策
  - その他の事象に関する分析結果

3-①　サイバー脅威レポートの送付先

送付アドレスはお申込時にご提示いただいたメールアドレスを登録します。
FortiGate導入後にメールアドレスの変更をご希望の場合は、設定変更申請にてメールアドレス変更申請をお願いします。

3-②　サイバー脅威レポートのポータルサイト

サイバー脅威レポートはポータルサイトからレポートを確認いただけます。尚、ポータルサイトにもこれまで送付したレポート（最大1年分）、参考資料、FAQなどが掲載されていますので、必要に応じてご活用ください。

ポータルサイトURL	：https://portal.riskadvisor.jp/
ログインID	：サービス提供開始時のご案内メールに記載
PW	：サービス提供開始時のご案内メールに記載
画像認証数字	：ポータルサイトに表示されている数字を入力

RICOH

3-③　サイバー脅威レポート記載内容の補足

サイバー脅威レポートに記載している内容について補足します。

＜分析状況の概況に関する補足＞

1　分析結果の概況

1.1　はじめに

この報告書では、お客様にて設置・導入されている以下の製品が期間中に検出した情報をもとに、1 項にて分析結果の概況を、また、2 項および 3 項にて、重要度の高い事象とその他の事象に分けて、それぞれの分析結果の詳細を記載しております。

報告対象のセキュリティ製品	報告対象期間
FortiGate	2017 年 9 月 1 日～2017 年 9 月 30 日

なお、本サービスではお客様内部の端末の識別に際し、あらかじめ個々の端末に割りふられる IP アドレス（端末の識別番号）を用いております。本文中に表記されている IP アドレスから対象端末を特定する方法については 4 項をご参照ください。

1.2　分析結果の概況

本項では、分析結果の概況を一覧で表示しております。それぞれの評価結果の詳細につきましては、各項目の詳細参照先をご確認ください。

項番	検知内容	評価基準	詳細参照先
1	重要度の高い事象 2 件		2 項
2	外部からのウイルスによる攻撃 3 件 上記のうち、ブロック済みの件数 3 件		3.1 項
3	外部からの不正侵入の試み 4 件 上記のうち、ブロック済みの件数 4 件		3.2 項
4	セキュリティリスクの高い Web ページの閲覧試行件数 50 件 上記のうち、ブロック済みの件数 50 件		3.3 項
5	4 以外に閲覧を制限している Web ページの閲覧試行件数 51 件 上記のうち、実際に閲覧した件数 30 件		3.4 項
6	迷惑メールの受信件数 18 件		3.5 項

評価基準について

 報告対象のセキュリティ製品では注意が必要な事案は検知されませんでした。

 報告対象のセキュリティ製品で注意が必要な事案が検知されました。

 報告対象のセキュリティ製品で対策が必要な事案が検知されました。

「1.2 分析結果の概況」の各項目における、雨曇晴判定の基準は以下の通りとなります。

- 2. 外部からのウイルスによる攻撃件数

  検知件数＝ブロック件数　→　晴

  検知件数＞ブロック件数　→　雨

- 3. 外部からの不正侵入の試み件数
  検知件数＝ブロック件数　→　晴
  検知件数＞ブロック件数　→　曇り

- 4. セキュリティリスクの高い Web ページの閲覧試行件数
  検知 0 件　→　晴
  検知件数＝ブロック件数　→　曇り
  検知件数＞ブロック件数　→　雨

- 5. 4 以外に閲覧を制限している Web ページの閲覧試行件数
  閲覧試行件数＝0 件　→　晴
  閲覧試行件数＞0 件　→　曇り

- 6. 迷惑メールの受信件数
  検知件数＝0 件　→　晴
  検知件数＞0 件　→　曇り

RICOH

＜外部からの不正検知結果に関する補足＞

3.2　外部からの不正侵入の検知結果

報告期間中に検知された不正侵入の試みは以下の通りです。

外部からの不正侵入による攻撃件数	4 件
内、ブロック済みの件数	4 件

上記において不正侵入による攻撃件数が 0 件の場合、または、攻撃件数に対しブロック済みの件数が下回っている場合には、IPS（不正侵入防御）の機能の設定に置いて、不正侵入の検知またはブロックの機能が無効となっている場合が考えられますので、念のため機器の設定内容の確認をお奨めします（確認方法につきましてはサービス提供元の Web サイトより手順書（手順書 No.07）をダウンロードいただき、ご確認ください）。

また、上記において、ブロックされていない不正侵入が確認された場合でも、業務上使用されているアプリケーションによる正常な通信が誤検知されている可能性も含まれます。本報告書では、ブロックされていない不正侵入のうち特に重要度の高い事象については 2 項に記載しています。

それ以外の事象も含め、比較的注意が必要なものについては、件数が多い端末から順に最大 5 台分について端末の IP アドレスと攻撃手法（シグネチャ名）を以下に記載しております（該当する事案が検知されなかった場合は表示されません）。IP アドレスから対象端末を特定する方法については 4 項を参照ください。また、攻撃手法の詳細を確認する方法については、本サービス提供元の Web サイトの FAQ を参照ください。

端末の IP アドレス :192.168.1.79

シグネチャ名	件数
MS.MSXML3.Same.Origin.Policy.Bypass	4

- FortiGate については、以下メーカーWeb サイトから攻撃方法（シグネチャ）の詳細情報が確認できます。

Fortinet 社　FortiGuard Encyclopedia（英語）
https://fortiguard.com/encyclopedia

3-④　FAQ

Q：月次レポートに「ヒアリング調査」とありますが、どのようなヒアリングを実施すればよろしいでしょうか。

A：レポート内の検知履歴に検知日時、送信元・送信先の IP アドレスを掲載しています。まずは、該当する PC やサーバの使用者に、検知日時に操作していたかどうかを確認してください。可能であれば、サイバー脅威レポートサービスポータルの資料ダウンロードページから IP アドレスの所有者情報の確認方法をダウンロードし、URL などの情報を確認し、該当する URL にアクセスしたかどうかを PC やサーバの使用者に確認してください。

Q：同じ内容の通知メールが多数通知される場合に、通知を止める方法はありますか。

A：FortiGate で検知されたリスク種別に基づき、FortiGate の設定画面で下記に従って設定を変更してください。尚、各機能の設定を変更することによって感染リスクが高まる可能性がありますので、その点をご留意の上、実施してください。

＜FortiGate（FortiOS-5.4.x）の場合＞

- アンチウイルス：「セキュリティプロファイル」＞「アンチウイルス」から、アクションを「ブロック」に変更
- IPS：「セキュリティプロファイル」＞「侵入防御」から該当するシグネチャ（攻撃手法名）の設定を「ブロック」または「検知のみ」に変更
- Web フィルタ：「セキュリティプロファイル」＞「Web フィルタ」から該当する URL をホワイトリストとして追加
- アンチスパム：「セキュリティプロファイル」＞「アンチスパム」から該当する送信元メールアドレスをホワイトリストとして追加

Q：通知メールや月次レポートにおける「対策方法」に、「ネットワークから切り離したうえで、シャットダウンや再起動をせずに」と記載されている場合がありますが、なぜシャットダウンや再起動をしてはいけないのですか。

A：端末の情報の保存する場所は、メモリとディスクの 2 種類があります。このうち、メモリは再起動やシャットダウンを実施することで情報が消去されますが、セキュリティインシデントが発生した後の事後解析において、メモリに保存されている情報が必要となる場合があるため、シャットダウンや再起動はしないことをお奨めしています。

RICOH

3-⑤　参考情報　セキュリティ攻撃について（外部リンク集）

■近年のセキュリティ脅威の流行

- 情報セキュリティ 10 大脅威 2022（IPA より引用）
  https://www.ipa.go.jp/security/vuln/10threats2021.html
- 情報セキュリティ 10 大脅威 2021（IPA より引用）
  https://www.ipa.go.jp/security/vuln/10threats2021.html
- 情報セキュリティ 10 大脅威 2020（IPA より引用）
  https://www.ipa.go.jp/security/vuln/10threats2020.html
- 情報セキュリティ 10 大脅威 2019（IPA より引用）
  https://www.ipa.go.jp/security/vuln/10threats2019.html
- 情報セキュリティ 10 大脅威 2018（IPA より引用）
  https://www.ipa.go.jp/security/vuln/10threats2018.html

■マルウェア関連

- メールの添付ファイルの取り扱い 5 つの心得（IPA より引用）
  https://www.ipa.go.jp/security/antivirus/attach5.html
- ボット対策について（IPA より引用）
  https://www.ipa.go.jp/security/antivirus/bot.html
- マルウェアとは（JNSA より引用）
  https://www.jnsa.org/ikusei/03/08-01.html
- マルウェア対策（JNSA より引用）
  https://www.jnsa.org/ikusei/03/08-01.html

■不正侵入(IPS)関連

- 知っていますか？脆弱性 （ぜいじゃくせい）（IPA より引用）
  https://www.ipa.go.jp/security/vuln/vuln_contents/index.html
- クロスサイト・スクリプティング（IPA より引用）
  https://www.ipa.go.jp/security/vuln/vuln_contents/xss.html

■迷惑メール関連

- メールの添付ファイルの取り扱い 5 つの心得（IPA より引用）
  https://www.ipa.go.jp/security/antivirus/attach5.html
- 迷惑メールへの対策（JNSA より引用）
  https://www.jnsa.org/ikusei/02/06-02.html

RICOH

Fortinet®、FortiGate®、FortiCare®、FortiCloud、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です

Google および Google Chrome™ ブラウザは Google Inc.の商標です。

Mac OS は、米国および他の国々で登録された Apple Inc.の商標です。

Firefox、Thunderbird は Mozilla Foundation の商標です。

Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

Microsoft、Windows、Windows 10、Internet Explorer、Windows Live、Excel および Outlook Express は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

Microsoft Corporation のガイドラインに従って画面写真を使用しています。
その他の製品名、名称は各社の商標または登録商標です。