



「月次レポートから読み解く！
今すぐ見直したい
おまかせサイバーみまもりの設定ポイント」

2026年9月18日

目次

1. 本セミナーの目的のご説明(3分)

2. サマリーレポートの解説(5分)

毎月のサマリーレポートをわかりやすく読み解く方法

3. 管理コンソールを用いたサービス活用(25分)

サマリーレポートの内容を管理コンソールから確認し、セキュリティ対策の設定変更を実施

4. ダッシュボードの解説(5分)

ダッシュボード：見方、検証環境にてデモンストレーションを実施

5. 最後に(15分)

アンケート再周知、質疑



1. 本セミナーの目的のご説明



目的

本日はセミナーにご参加いただきありがとうございます。

本セミナーは、「おまかせサイバーみまもり」をご契約いただいたお客様を対象に、導入初期に毎月お届けしているサマリーレポートの見方を理解し、セキュリティ対策の設定見直しに活用いただくことを目的としています。

サマリーレポートには、検知した脅威や通信の状況など、お客様のセキュリティ対策を考えるうえで重要な情報が記載されています。一方で、レポートのどこを確認し、その内容をどのように日々の運用や設定変更につなげればよいか、分かりにくい場合があります。

本セミナーでは、サマリーレポートの基本的な見方や確認すべきポイントを解説するとともに、管理コンソールを用いて、レポートから把握した内容を具体的な設定の確認・見直しにつなげる方法をご紹介します。

さらに、ダッシュボード画面の見方についても、デモンストレーションを交えながら分かりやすく解説します。

サマリーレポートを有効活用し、お客様自身でセキュリティ対策の状況を把握するとともに、より安心・安全な環境の構築につなげていただくことが、本セミナーの狙いとなります。



2. サマリーレポートの解説

月次レポート

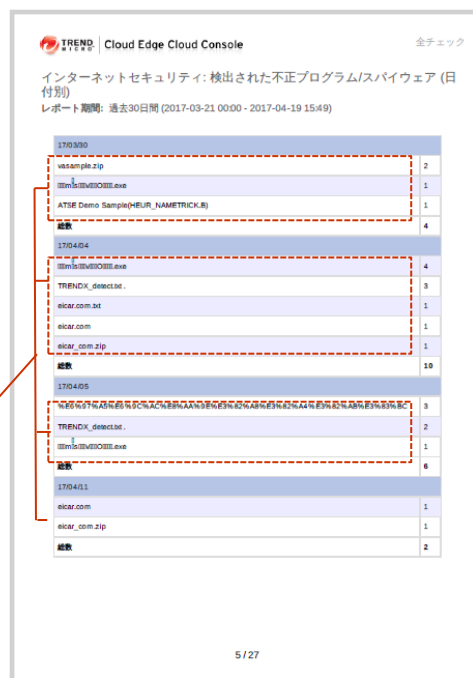
月1回、メールにてお客様へのレポート配信を行っております。

レポートイメージ(抜粋)

- ・お客様へのレポート配信で脅威の侵入や不正サイトへのアクセスのブロック状況が見える化
- ・視覚的に状況を把握することにより、必要なセキュリティ対策が明らかになります
- 具体的な脅威名と検出件数に関するグラフ
- 各脅威が検出された件数と日付に関するグラフ



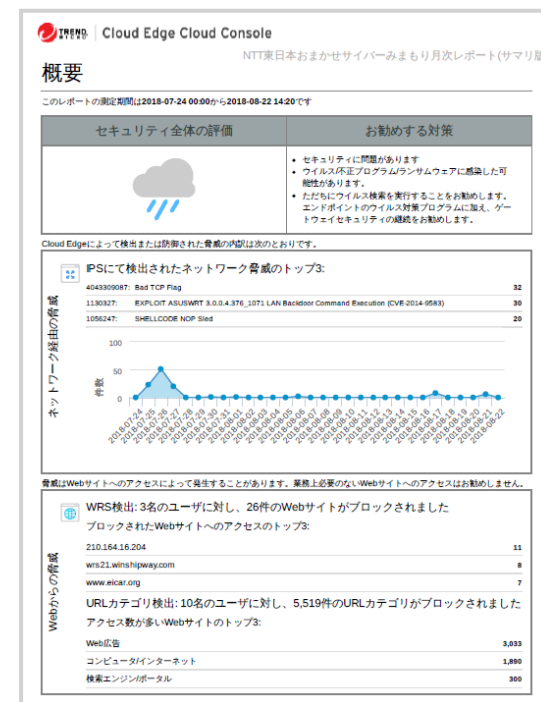
機器が検出した脅威の名前



サマリレポート(2018年9月~提供)

・セキュリティ対策状況の評価が一目でわかる

サマリレポートも合わせて提供



レポートのポイント

- 月次レポートを基に設定を変更することも可能です。今後のセミナーではおまかせサイバーみまもりの設定のポイントについて取り上げて解説させていただく予定です。

ポリシー施行: URLフィルタによってブロックされた上位のサイト
レポート期間: 過去30日間 (2017-03-21 00:00 - 2017-04-19 15:49)



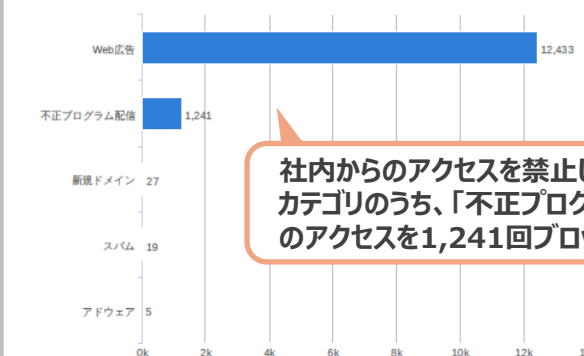
1ヶ月以内に、社内から
www.XXXX.comというサイトに、16
回アクセスを試み、ブロックしました。

■ URL指定によるアクセス制御機能によってブロックされた上位のWebサイトに

関する情報です。

- 横軸：検出した件数
- 縦軸：URL/IPアドレス

ポリシー施行: ブロックされた上位URLカテゴリ
レポート期間: 過去1か月間 (2017-11-01 00:00 - 2017-11-30 23:59)



社内からのアクセスを禁止しているURL
カテゴリのうち、「不正プログラム配信」へ
のアクセスを1,241回ブロックしました。

■ URL指定によるアクセス制御機能によってブロックされた上位のURLカテゴ

リに関する情報です。

- 横軸：検出した件数
- 縦軸：カテゴリ名

※新規ドメイン

トレンドマイクロ社が実施するWebサイトの安全性評価において「未評価」の場

合に新規ドメインカテゴリのWebサイトと認識されます。

月次レポート解説書

レポート解説書(一部抜粋)

レポートの内容をよりお客様に理解していただけるよう、レポート解説書を別途提供

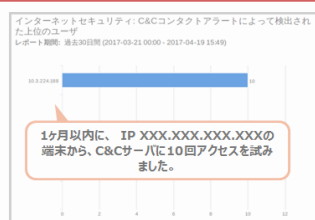
【掲載場所】 <https://my.ebook5.net/ntteast-pamphlet/report-guide/>

概要や対策説明など

◆ C&Cサーバへのアクセス検出に関する説明

C&Cサーバへのアクセスに関する情報

- 本ページでは、不正プログラム侵入検知機能により、Cloud Edgeが1ヶ月以内に**C&Cサーバ接続**を検知・ブロックした結果を把握することができます。
- IPアドレスにより、どのユーザが**C&Cサーバへの通信**を実施しているか、把握することができます。
- C&Cサーバとは、外部から侵入して乗っ取ったコンピュータを踏み台にして制御したり命令を出したりする役割を担うサーバコンピュータのごとであり、検出された端末は**感染が強く疑われます**。早期の対応が必要です。
- C&Cサーバへの通信はCloud Edgeによりブロックされており、情報漏えいの発生はございません。



- Cloud Edgeを経由して**C&Cサーバへの接続**を行った上位10件のユーザに関する情報です。
- 横軸: 検出した件数
- 縦軸: ユーザ (表記されているIPアドレスを保持する端末)

※C&Cサーバ

外部から侵入して乗っ取ったコンピュータを踏み台にして制御したり命令を出したりする役割を担うサーバコンピュータ。通信が発生した場合、下記のような被害が想定される。

- 1) 特定のWebサイトへ負荷を与えるDDoS攻撃や、多くのメールを送信してフィッシング詐欺などを引き起こすスパムメール配信に加担させる。
- 2) サーバから、重要な機密情報を抜き取る。

※不正プログラム検知機能

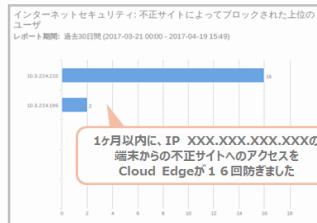
不正な通信、プログラムによる攻撃を検知。どこから、どこに、どんな通信が行われているか判別し、内部感染を早期に発見。C&Cサーバ通信の検知やプログラムの脆弱性を狙う攻撃などに対応。

検知した機能やキーワードの説明

◆ 不正サイトへのアクセス検出に関する説明

不正サイトのアクセスに関する情報

- 本ページでは、Webサイトアクセスブロック機能により、Cloud Edgeが1ヶ月以内に**不正サイトへの接続**を検知・ブロックした結果を把握することができます。
- IPアドレスにより、どのユーザが**不正サイトへのアクセスを試みているのか**、把握することができます。



- ユーザがCloud Edgeを経由してWebサイトにアクセスした際に、**不正なサイト**であることを検知し、**ブロック**した結果です。
- 横軸: 不正なWebアクセス数
- 縦軸: ユーザ (表記されているIPアドレスを保持する端末)

- Cloud Edgeでブロックした**不正サイトアクセスが多いユーザのうち、上位10件**の結果です。
- 横軸: 検出した件数
- 縦軸: 検出件数が多い、上位10件のユーザ (表記されているIPアドレスを保持する端末)

※Webサイトアクセスブロック機能

不正Webサイト、不正URLへのアクセスを止めることにより、不正プログラムによる感染、フィッシング詐欺被害を未然に防止する機能。

グラフの読み方



3. 管理コンソールを用いたサービス活用

管理コンソール

- Cloud Edge Cloud Console(以降CECC)は、開通時にメールにて送付したID/Passを利用してログインすることにより、専用BOX(Cloud Edge)の脅威の検知状況および、アプリケーション利用制限・URL指定によるアクセス制御機能等のポリシー設定機能の検知状況をお客さまご自身で把握いただくことができます。

NTT 東日本

登録情報を入力してください

アカウント:
[入力欄]

パスワード:
[入力欄]

[パスワードのリセット \(パスワードをお忘れの場合\)](#)

☒ アカウント名を記憶する

アカウントをまだ取得していない場合 [今すぐ登録](#)

- ① ブラウザを開いてお客様管理コンソールにアクセスします。「アカウント」「パスワード」を入力し、「ログイン」をクリックします。

※ お客様管理コンソールのURLおよび「アカウント」は、「新規アカウント発行のお知らせ」メールに記載。「パスワード」は、「新規アカウント発行のお知らせ」メールにて、お客様ご自身で設定する必要があります。

TREND MICRO Licensing Management Platform Powered by TREND MICRO

ようこそ Demo100No33Time1 | ログアウト

登録済みの製品/サービス ユーザ登録情報 サポート情報

登録済みの製品/サービス

+ キーの入力

サービスプラン名	製品/サービス	シート/ユニット	ライセンス種別	開始日	有効期限	アクション
おまかせサイバーまもり Standardプラン	Cloud Edge 50	シート/ユニット	製品版	2017/06/19	自動更新	コンソールを開く
おまかせサイバーまもり セキュリティパッケージプラン(アンチEDRプラス)	Worry-Free Co-Managed XDR for Endpoint	1 シート/ユニット	製品版	2017/06/19	自動更新	コンソールを開く

有効期限内 間もなく期限切れ 有効期限切れ

- ② 製品/サービスに Cloud Edge と記載がある行の「コンソールを開く」をクリックします。

- ③ 2ページに示したCECCのトップページに遷移します。

この後デモとしてご紹介する内容

管理コンソールを用いたサービス活用方法について、次の3点を動画を交えてご説明

①管理コンソールの使い方

- ・サマリーレポートの内容を管理コンソールのログ分析から確認
- ・「いつ」、「どの端末」から、「どこへアクセス」し、「どう対処した」かを把握

②業務改善の検討

- ・セキュリティ初期設定をご説明のうえ、様々なアクセス制御のポリシールールをご紹介
- ・①の把握し内容をもとに、業務改善を検討

③ブロックされた後の「次の一手」

- ・不正プログラム等をブロックした内容を管理コンソールのログ分析から確認
- ・本サービスの範囲に留まらず、「次の一手」として何を実施すべきかをご説明

管理コンソールの使い方(1/2)

①セキュリティプロファイルの「**Webレピュテーション**」によるアクセス制御結果を確認

- ブロック時の挙動 : 警告画面表示
- サマリーレポート : 「不正サイト」の項目から全体傾向を把握
- 管理コンソール : **ログ分析 > インターネットセキュリティ**から詳細を確認



管理コンソールの使い方(2/2)

②ポリシーールの「**URLカテゴリフィルタ**」によるアクセス制御結果を確認

- ブロック時の挙動 : 警告画面表示
- サマリーレポート : 「不正サイト」の項目から全体傾向を把握
- 管理コンソール : **ログ分析 > ポリシー施行**から詳細を確認



セキュリティ初期設定(1/2)

基本的なセキュリティ対策機能はあらかじめ有効になっており、そのままでも安心してサービスをご利用いただくことが可能です。

初期設定の詳細について公式HPでも公開しております。[セキュリティ初期設定 | ebook5](#)

お客様の利用環境に合わせ「**何をつかって良いか**」を定めることで、セキュリティリスクの低減や業務効率の向上につなげることが可能

セキュリティ機能（初期値）

機能名		機能概要	初期値	初期値詳細	変更可能範囲
ポリシー ルール	アプリケーションコントロール	アプリケーションの利用制限を行う機能。日本独自のアプリケーションを含む1,000 以上のアプリケーションをサポート	有効	カテゴリ：ピアツーピアのみ ブロック（Bittorrent、Share EX2、WinMX、Winny等）	カテゴリまたは個別アプリケーション単位で設定変更可能
	URLフィルタリング	不正Webサイト、不正URLへのアクセスを止めることにより不正プログラムによる感染、フィッシング詐欺被害を未然に防止	有効	カテゴリ：インターネットのセキュリティのみブロック（ハッキング、フィッシング等）	カテゴリ単位で設定変更可能
	ファイアウォール	攻撃のみをブロックし、適切なアプリケーショントラフィックだけを通過する機能	無効	—	有効・無効での設定変更 IPアドレス・ポート番号等の指定による許可・ブロック設定
	セキュリティ検索除外	業務でセキュリティを除外したい端末等を指定することで、おまかせサイバーみまもりのセキュリティ検索の対象から外すことが可能	無効	—	セキュリティ検索を除外したいIPアドレス、ネットワークアドレスを設定
許可/ブロックリスト (URL及びIPアドレス)		URLまたはIPアドレスを指定し、アクセス許可されたカテゴリから、特定のサイトのみをブロック（ブラックリスト）したり、ブロックしたカテゴリから、特定のサイトのみをアクセス可能（ホワイトリスト）とする。	設定なし	—	①ファイアウォール個別許可設定 ②URL/IP アドレスの許可 ブロックリスト 登録可能なポリシー数は基本無制限だが、URL の許可 ブロックは合計で最大 100 件まで

セキュリティ初期設定(2/2)

「**セキュリティ上の脅威からどう守るか**」を定めることが可能であり、
基本的には機能有効のままご利用頂くことを推奨

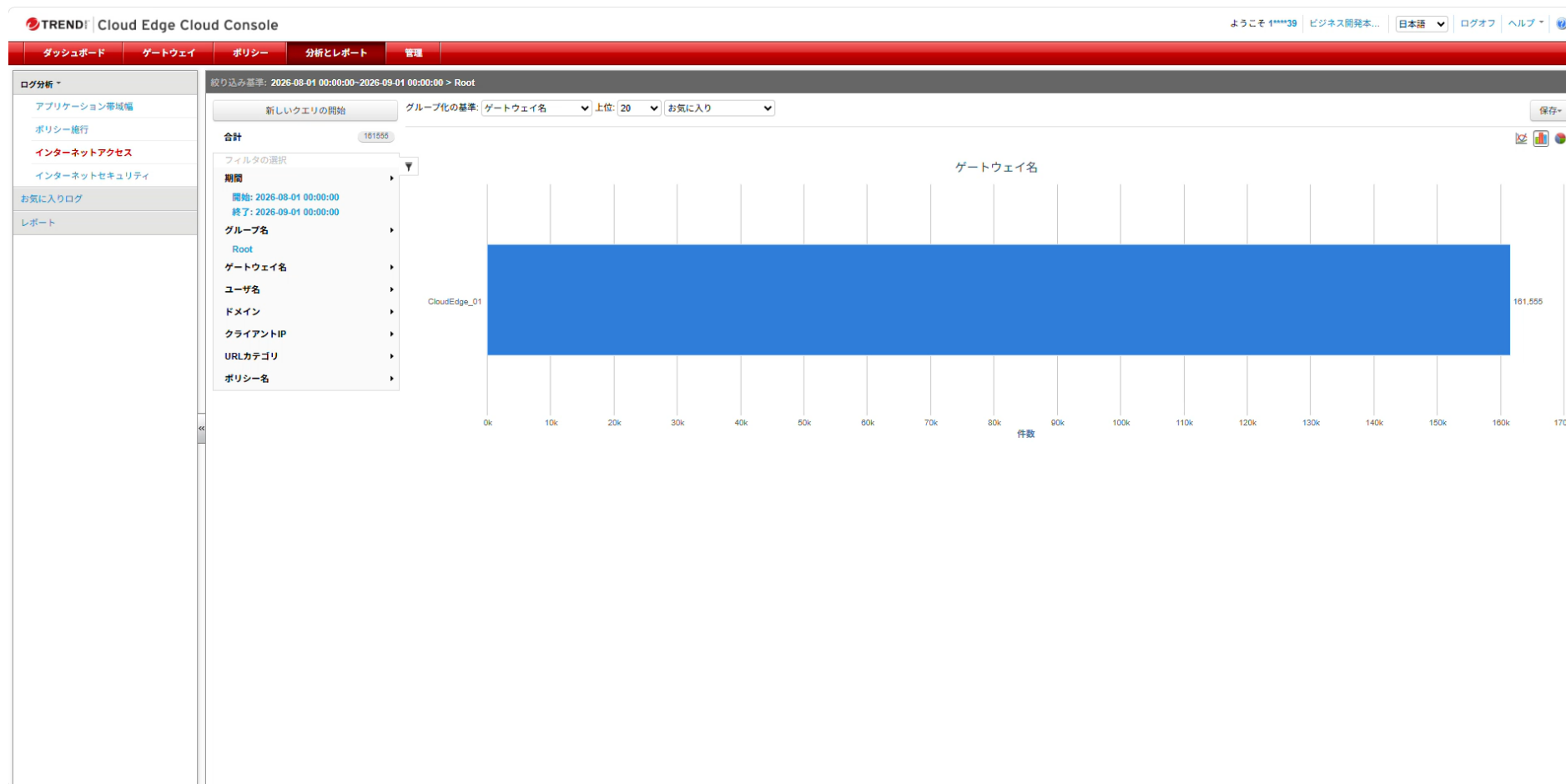
セキュリティ機能（初期値）

機能名		機能概要	初期値	初期値詳細	変更可能範囲
セキュリティ プロファイル	IPS	「不正侵入防御システム」の略称で、ポリシールールで許可されたトラフィックを調べ侵入する脅威、セキュリティホールなど悪意ある攻撃がないかを確認し、ブロック	有効	検出時の処理：ブロック	変更不可
	不正プログラム対策	不正な通信、プログラムによる攻撃を検知。どこから、どこに、どんな通信が行われているか判別し、内部感染を早期に発見。C&C サーバ通信の検知、Shellshock など脆弱性を狙う攻撃などに対応	有効	スマートスキャン、機械学習型検索が有効	無効に変更可能（不正プログラム疑いのあるファイルを削除しない）
	不正プログラム対策	メールにウイルスが添付されていないか検査。ウイルスが検出されたら駆除	有効	添付ファイルは削除され、メールの件名に[ウイルス駆除済み]を付与し、お客様へ送信	無効に変更可能（メール添付ファイルの不正プログラム対策を行わない）
	機械学習型検索	不正プログラム検索（パターンマッチング）で検出されない未知の不審なファイルが見つかった場合に、その特徴情報をトレンドマイクロへ送信し、脅威・安全の統計情報をもとに脅威であるかの判断を行う機能	有効	添付ファイルは削除され、メールの件名に[ウイルス駆除済み]を付与し、お客様へ送信	無効に変更可能（不正プログラム疑いのある添付ファイルを削除しない）
	スパムメール対策	メールの受け取り手に許諾なく送ってくる宣伝やいやがらせ、マルウェアなどを含んだメールを検出し、メールの件名に[スパムメール]を付与	有効	メールの件名に[スパムメール]を付与し、お客様へ送信	無効に変更可能（スパムメールの検出を行わない）
	例外リスト	特定のメールアドレスに対してメールセキュリティ対策の例外化が可能	設定なし	—	許可もしくはブロックさせたい送信者のメールアドレスを登録可能
	パスワード付きアーカイブの警告	パスワードが付与されたZipファイルなどについてメール受信者に注意を促す。メールの本文に警告文を付与	有効	メールの本文に警告文を付与し、お客様へ送信	無効に変更可能（パスワード付きアーカイブファイルのあるメールに注意喚起を行わない）
	POP3S/SMT PS/IMAPS 復号	暗号化されたメールプロトコル(POP3S、SMTPS、IMAPS)に対してもメールセキュリティ対策を実施する。適切にメールセキュリティ対策を実施するためには端末に証明書のインストールが必要	有効	サーバとの接続にSSL/TLSを用いるメール通信を検査	無効に変更可能（POP3S/SMTPS/IMAPS通信は検査除外）
セキュリティ プロファイル	Webレピュテーション	接続前にサイトの危険度（評点）を問い合わせし、そのサイトが「危険性のある Web サイト」と評価された場合に、その接続リクエストをブロック（ドロップ）する機能	有効	セキュリティレベル：中 不正なコンテンツを含むサイト：ブロック	変更不可
	HTTPS復号	HTTPS (HTTP over SSL/TLS)で暗号化された通信を検査する。暗号化された通信を検査するためには、端末に指定の証明書をインストールしていただく必要がある	無効	—	有効に変更可能（HTTPS接続の通信も検査する）

業務改善の検討(1/2)

●ポリシールールを用いた業務改善の流れの一例

- ①アクセス先などの利用状況を、管理コンソールの「インターネットアクセス」より把握
- ②アクセス先のURLカテゴリや、頻度、時間帯等でフィルターを行うことで分析
- ③実際の通信内容を調査のうえ、アクセス制御の可否を検討。**必要に応じてブロックを実施**



業務改善の検討(2/2)

●設定変更に関わる各種留意事項

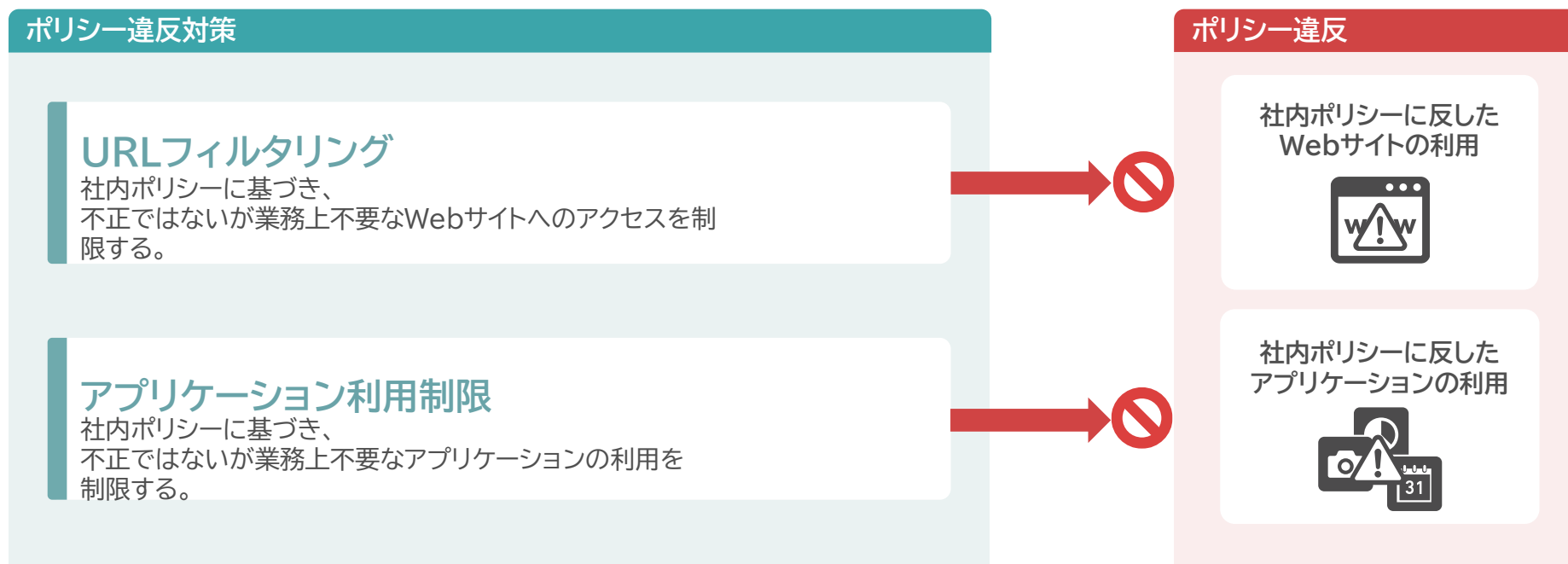
・強固なセキュリティ制限と業務利便性のバランス

→ 制限による業務影響、制限すべき範囲や方法を検討

そのために、管理コンソールを用いることで利用状況を把握・分析することも可能

●設定変更イメージ

・セキュリティサポートデスクに申請いただくことで、代わって設定を行うことも可能



ブロックされたあとの「次の一手」

■不正プログラム等がブロックされた後の対応

- ①検知レポートを確認
- ②管理コンソールから詳細なログを読み解く
- ③必要に応じて、端末のウイルススキャンや、追加のアクセス制御の検討

生成者:	9066033
生成日:	2026-09-01 01:46
レポート期間:	過去1か月間 (2026-08-01 00:00 - 2026-08-31 23:59)
インターネットセキュリティ: 不正プログラム/スパイウェア検出の傾向	3
インターネットセキュリティ: 検出された上位の不正プログラムファイル	4
インターネットセキュリティ: 検出された不正プログラムファイル (日付別)	5
インターネットセキュリティ: 不正サイトが検出された上位のユーザ	6
インターネットセキュリティ: 不正プログラムが検出された上位のユーザ	7
インターネットセキュリティ: 検出された不正サイト (日付別)	8
インターネットセキュリティ: 検出された上位の不正サイト	9
インターネットセキュリティ: ランサムウェアが検出された上位のユーザ (Webチャネル)	10
インターネットセキュリティ: 検出されたランサムウェア (Webチャネル/日付別)	11
インターネットセキュリティ: 検出された上位のランサムウェア (Webチャネル)	12
インターネットセキュリティ: ランサムウェアがブロックされた上位のユーザ (メールチャネル)	13
インターネットセキュリティ: ランサムウェアが検出された上位のユーザ (ネットワークチャネル)	14
インターネットセキュリティ: スパムメール対策によって検出された上位のユーザ	15
インターネットセキュリティ: マイナンバーがフィルタで検出された上位のユーザ	16
インターネットセキュリティ: メールの機械学習型検索によって検出された上位のユーザ	17
インターネットセキュリティ: C&Cコールバックが検出された上位のユーザ	18
インターネットセキュリティ: 上位のIPS検出	19
インターネットセキュリティ: IPSによって検出された上位のユーザ	20
インターネットセキュリティ: IPS検出 (日付別)	21

まとめ

管理コンソールの使い方から、詳細な通信内容进行分析する方法、ブロック後の対応をご説明

①管理コンソールの使い方

- ・サマリーレポートの内容を管理コンソールのログ分析から確認
- ・「いつ」、「どの端末」から、「どこへアクセス」し、「どう対処した」かを把握

②業務改善の検討

- ・セキュリティ初期設定をご説明のうえ、様々なアクセス制御のポリシールールをご紹介
- ・①の把握し内容をもとに、業務改善を検討

③ブロックされた後の「次の一手」

- ・不正プログラム等をブロックした内容を管理コンソールのログ分析から確認
- ・本サービスの範囲に留まらず、「次の一手」として何を実施すべきかをご説明



4. ダッシュボードの解説



参加者からのご質問に対する回答 (2025年12月4日開催)

質問・回答①

No.	質問	回答
1	管理コンソールやレポート解説書のURLをもう一度教えてください。	管理コンソール利用マニュアルや月次レポート解説書につきましては、以下のおまかせサイバーみまもり サポート情報 ページに掲載しております。 https://business.ntt-east.co.jp/support/cybermimamori/#anc-manual
2	管理コンソールのデバイスリストに、会社の備品以外のデバイスが表示された場合、対象デバイスをブロックする方法はございますか？	対象デバイスのIPアドレスもしくはMACアドレスを指定してブロックすることが可能です。 具体的な設定方法については、セキュリティサポートデスクへご相談、ご依頼ください。 ■お問い合わせ、変更依頼 https://business.ntt-east.co.jp/support/cybermimamori/#anc-inquiry
3	管理コンソールから、ログを採取(ダウンロード)する場合に条件などはありますか？ たとえば、指定した期間のログを取得する といった場合に、ログが残っているのは何日間(何件)まで やダウンロードできるサイズはどのくらいまで など	ログの保持期間は最大62日間です。管理コンソール上で指定した期間のログをダウンロードできますが、取得可能なのは過去62日以内のデータとなります。また、一度にダウンロードできる上限は5,000件となります。
4	ログ分析、インターネットアクセスを見る際、上位20がMAXになっており、もう少し増やすには何か設定ありますか？	UIの仕様上、上限20件となっております。より詳細な分析をしたい場合、ユーザ名や期間を細分化して表示してください。
5	月次レポートの検出された不正サイトに自社HPのURLが表示されるのですが、HPの何を変更すれば不正サイトではなくなりますか？	判定理由は「SSL証明書の期限切れ」などが考えられます。 まずはHPのSSL証明書の期限のご確認を実施してください。 誤判定の場合は、トレンドマイクロ社への訂正申請も可能です。詳細はセキュリティサポートデスクへご相談ください。
6	いつ、どの端末がどのサイトへアクセスしたかのログは採られていないとのこと。オプション追加で解決できるでしょうか。	おまかせサイバーみまもりで保持しているログは、専用BOXのセキュリティ機能(不正プログラム対策、IPS等)でのブロックログ、メールセキュリティ機能でのスパム判定のログ、ポリシー設定でのブロックログ等となります。端末ごとにブロックされていない通信(Webサイトへのアクセス履歴等)は記録しておりません。 どの端末がどのサイトへアクセスしたかのログを取得されたい場合にオプションはご用意がございません。 なお、どのサイトへアクセスしたのかは、アクセス単位のログとして保持しておりませんが、統計情報として保持しています。 分析とレポート>インターネットアクセス より確認することが出来ます。

質問・回答②

No.	質問	回答
7	月次レポートの他に、インシデントが検知された場合は、即時に何らかの連絡があるのでしょうか。	C&Cサーバとの通信検知時にメールまたはお電話にてご連絡をさせていただきます。 ※C&Cサーバ(Command and Controlサーバ)とは、マルウェアやボットネットを遠隔操作するために攻撃者が利用するサーバのことです。
8	業務時間帯に動画サイトへのアクセスを禁止するポリシーを作成し適用したところ、自社のホームページにアクセスできなくなった	自社HPの一部コンテンツが「動画カテゴリ」に分類されている可能性があります。アクセスが必要なサイトを「許可リスト」へ追加することで対応可能です。 詳細はセキュリティサポートデスクへご相談ください。
9	インシデント発生時はサポートデスクでも検出でき、対応等のアドバイスも即時にいただけるのでしょうか？	セキュリティサポートデスクでは、C&Cサーバとの通信検知時の確認や初動対応のアドバイスをしています。
10	おまかせサイバーを導入したらレピュテーションリスク観点から閲覧できるサイトが見れなくなりました。 ホワイトリストで都度追加はしているが、不特定多数存在すると思われるのでもう少し柔軟に対応できるようにできないか。	「許可リスト」や「カテゴリ単位の許可」「時間帯別ポリシー」など柔軟な運用が可能です。業務に必要なサイトはまとめて許可リスト登録することもできます。 詳細はセキュリティサポートデスクへご相談ください。
11	フィッシングサイトのURLサイト付きのメールを受信した場合、メールの受信がブロックされるのか もしくは、URLのアクセスがブロックされるのか教えて下さい。	おまかせサイバーみまもりの初期設定では、メール自体をブロックすることではなく、メールの件名にタグ付けをいたします。フィッシングサイトのURLへのアクセスは、Webフィルタリング機能でブロックする機能はございますが、100%防げるものではありませんので、フィッシングには十分ご注意ください。

質問・回答③

No.	質問	回答
12	おまかせアンチウイルスEDRプラスを適用している端末が、ランサムウェアに被害にあい暗号化されてしまった場合、どのように回復を図るのでしょうか？	EDRプラスを導入している端末がランサムウェア被害で暗号化された場合、まずEDRの機能で感染端末をネットワークから隔離し、拡散防止を図ります。 なお、暗号化されたファイルは基本的に復号できないため、バックアップデータからのリストアが最も確実な復旧方法となります。 復旧後はOSやソフトウェアのアップデート、EDRポリシーの見直しなど再発防止策を実施します。
13	おまかせサイバーみまもりの利用から数年経過し、専用BOXの最新機種への交換に申込させていただき、最新機種をお送りいただきました。まだ交換していないのですが、本体を繋ぎ変える他に管理コンソールから設定などもする必要がありますか？また設定方法など、わからないことがあればサポートセンターで教えていただけますか？	通常は本体交換のみで設定は完了します。ただし固定IPアドレスの設定有理の場合やLAN2、LAN3のポートをご利用になられている場合は、管理コンソールからの機器設定が必要になります。 設定方法や交換手順は以下のマニュアルで確認でき、セキュリティサポートデスクよりご説明・サポートしますのでご安心ください。不明点やトラブル時は、遠慮なくセキュリティサポートデスクへご連絡ください。 ■専用BOX設置マニュアル https://my.ebook5.net/ntteast-pamphlet/cloud-edge-manual/
14	IPSを検知した場合は、具体的にどういう対策を取ったらいいのでしょうか？	IPSで検知された際は、通信自体はブロックされておりますので、端末を特定し業務に必要な通信かどうかを判断いただきます。 誤検知により必要なサイトにアクセスできない場合などは、セキュリティサポートデスクにご連絡いただければ、対応いたします。 不明点やトラブル時は、遠慮なくセキュリティサポートデスクへご連絡ください。
15	ポリシールールについて設定できるようですが、詳しい設定マニュアルはございますか？	ポリシールール等の設定は可能です。設定変更が必要な際は設定変更シートを

質問・回答④

No.	質問	回答
16	5年程度前から契約していますが、サイバー保険も自動的に付与される理解で良いですか？	おまかせサイバーみまもり契約者は、追加申込不要でサイバー保険が自動付帯されています。
17	EDRプラスへ変更するにはどのような手続きをおこなえばよろしいでしょうか。	弊社の営業担当または以下の窓口までご連絡いただき、お申込みください。 ■お電話でのお問い合わせ フリーダイヤル 0120-116-032 ■Webお問い合わせフォーム https://form.business.ntt-east.co.jp/?formId=pf3792inq
18	お取引先様とのメールのやり取りで、添付ファイル・URLの有無にかかわらず[SPAM]がついたりつかなかったりしますが、原因は何ですか？	[SPAM]タグは、メールセキュリティ機能により送信元アドレス、本文内容、添付ファイルやURLの有無など複数の要素を総合的に判定して自動付与されます。添付やURLがなくても本文や構成がスパムの特徴に近い場合、タグが付くことがあります。また、判定ルールは定期的に更新されるため、同じ取引先でもタイミングによって判定が変わる場合があります。誤判定が疑われる場合は、セキュリティサポートデスクへご相談ください。
19	5年経過し新しい機種への交換が終わったのですが、すぐにEDR機能を付けることは可能ですか？	すぐにEDR機能(EDRプラス)を追加で申し込みいただくことが可能です。弊社の営業担当または以下の窓口までご連絡いただき、お申込みください。 ■お電話でのお問い合わせ フリーダイヤル 0120-116-032 ■Webお問い合わせフォーム https://form.business.ntt-east.co.jp/?formId=pf3792inq

質問・回答⑤

No.	質問	回答
20	レポートの中でポリシー行:適用された上位のユーザはどういう意味ですか？	「ポリシー行:適用された上位のユーザ」とは、一定期間内にセキュリティポリシー(Webフィルタリングやアクセス制御など)が最も多く適用されたユーザ(端末)をランキング形式で表示したものです。 この項目を見ることで、 ・どのユーザ(端末)が頻繁にポリシーによる制限やブロックを受けているか ・業務上、アクセス制限が多いユーザや、セキュリティリスクの高い行動をしているユーザを把握できる ・ポリシー設定の見直しや、業務に必要なサイトの許可リスト追加など、運用改善の参考になる というメリットがあります。 詳細な定義や見方は「レポート解説書」に記載されていますので、必要に応じてご参照ください。 ■レポート解説書 https://my.ebook5.net/ntteast-pamphlet/report-guide/
21	月次レポートに不正プログラム検出などが毎月何も表示されていないが、これは何も脅威にさらされていないという認識でよろしいでしょうか	月次レポートに「不正プログラム検出」などの項目が毎月何も表示されていない場合、該当期間中に脅威(ウイルス感染やマルウェア等)が検知されていない状態と考えて問題ありません。 ただし、レポート設定期間や専用BOXがオフラインとなってしまうなど運用状況によっては月次レポートに表示されないこともございますので、ご不明な点はサポートデスクまでご相談ください。



参加者からのご質問に対する回答 (2026年2月26日開催)



質問・回答①

No.	質問	回答
1	管理コンソールにしばらくログインしていないとパスワードが無効になってパスワードのリセットを毎回おこなっています。そのような仕様なのでしょうか？	2～3か月間、管理コンソールへのログインが行われなかった場合に、自動的にパスワードが無効化され、再発行(リセット)が必要となるような仕様はございません。詳細な確認が必要な場合は、管理コンソールのURLおよびログインIDを添えて、セキュリティサポートデスクへご相談ください。
2	今回のパワーポイントをダウンロード等で提供してほしい。	以下の「おまかせサイバーみまもり サポート情報」ページ内、【より便利にご利用いただくために(設定マニュアル、活用情報)】に掲載しております。本ページには、セミナー資料のほか、利用ガイドなどサービスをより効果的にご利用いただくための各種資料を掲載しております。ぜひご確認のうえ、ご利用ください。 https://business.ntt-east.co.jp/support/cybermimamori/
3	サポート詐欺について、PCの画面にウイルスに感染しましたなどの警告画面が出た場合、表示された電話番号に連絡せず、すぐに110番しましょうと警察からビラがありますが、このような時の初動対応としてはPCのシャットダウンでよろしいですか。	PCにウイルス感染の疑いがある場合は、被害拡大防止のため、まず当該PCをネットワークから切り離し、利用を中止してください。画面に表示される電話番号には安易に連絡しないようにしてください。 その後、発生時刻や症状、直前の操作内容を可能な範囲で整理・記録のうえ、速やかに情報システム部門またはセキュリティ担当窓口へ連絡し、指示に従って対応してください。 証拠保全の観点からPCのシャットダウンは控えてください。
4	ポリシーの設定方法を教えてください。	設定変更については、セキュリティサポートデスクへご相談、ご依頼ください。 ■お問い合わせ、セキュリティ設定の変更 https://business.ntt-east.co.jp/support/cybermimamori/#anc-inquiry
5	フレッツ光クロスBizの導入を検討しています。おまかせみまもりサービスはクロスBizでも対応されているのでしょうか。	おまかせサイバーみまもりは、フレッツ 光クロス Biz に対応しております。以下のページに、おまかせサイバーみまもりの仕様情報を掲載しておりますので、記載されているスループットをご参照のうえ、最適なプランをご選択いただければと存じます。 https://business.ntt-east.co.jp/service/securitypackage/service.html#anc-device

質問・回答②

No.	質問	回答
6	ウィルス感染が疑われた際、初動としてはLANケーブルを抜きPCのシャットダウンは行わないが正しいでしょうか？	PCにウィルス感染の疑いがある場合は、被害拡大防止のため、まず当該PCをネットワークから切り離し、利用を中止してください。その後、発生時刻や症状、直前の操作内容を可能な範囲で整理・記録のうえ、速やかに情報システム部門またはセキュリティ担当窓口へ連絡し、指示に従って対応してください。
7	お勧めのポリシーをまとめた資料はあるでしょうか？	現時点におきましては、おすすめのポリシー設定を取りまとめた資料のご用意はございません。
8	先ほど例に出たポルノサイトを禁止するためどんな設定すればいいのでしょうか。	以下のページの「セキュリティ設定の変更」より、設定変更ファイルをダウンロードしてください。ダウンロード後、“①-4【シート2】URLフィルタリング詳細設定”シート内の項番A「アダルト」について、一括でON、またはカテゴリ配下のジャンルごとに個別でONに設定してください。そのほか必要事項をご記入のうえ、セキュリティサポートデスクへメールにてご相談・ご依頼ください。 ■お問い合わせ、セキュリティ設定の変更 https://business.ntt-east.co.jp/support/cybermimamori/#anc-inquiry
9	運用面のご質問ですが、機器のログを確認しているとパケットのバイパスが頻発しております。何が起因しているのか、バイパスすることに問題があるのか確認頂くことは可能でしょうか？	本件につきましては、個別事象であり、詳細な確認が必要なケースと認識しております。お手数ですが、ログインIDを添えてセキュリティサポートデスクへご相談ください。
10	毎月送られてくるセキュリティ対応状況と検知状況のレポートですが、不正侵入検知や不正プログラム検知、ランサムウェア検知の数値は他と比べて多いのか少ないのか知りたい	セキュリティ対応状況および検知状況のレポートでは、全UTM機器(約30,000台)における検知状況を件数として集計・表示しています。そのため、月ごとの件数を30,000で割っていただくことで、検知件数が多いか少ないかの判断材料としてご活用いただければと思います。
11	フィッシングと思しきメアドを逐一ブラックリストに入れてますが、意味ありますか？ 魑(いたち)ごっこでは？	同一送信元からの再送防止や被害拡大の抑止には有効です。一方で、攻撃者は送信元を頻繁に変更するため、単体では魑ごっこになりがちです。他のメール対策や利用者教育と組み合わせると運用することが重要です。

質問・回答③

No.	質問	回答
12	スパムメールではないものもスパムと表示されて受信するメールがありますが、管理画面で何か対応できますでしょうか	〔SPAM〕タグは、メールセキュリティ機能により送信元アドレス、本文内容、添付ファイルやURLの有無など複数の要素を総合的に判定して自動付与されます。添付やURLがなくても本文や構成がスパムの特徴に近い場合、タグが付くことがあります。誤判定が疑われる場合は、セキュリティサポートデスクへご相談ください。
13	機器交換のメールが届きましたが、新旧で機器に違いはあるのでしょうか。 また交換時の設定に対応できない場合はリモートで作業していただけると伺っていますがサポートへ連絡すればOKでしょうか。	機器交換に伴う新旧機器の違いにつきましては、主にスループット(処理性能)の向上がございしますが、提供しているセキュリティ機能自体に差はございません。従来どおりのセキュリティ機能をご利用いただけます。 また、固定IPアドレスの設定など現地での対応が必要な作業を除き、基本的にセキュリティ設定は自動的に引き継がれます。セキュリティに関する設定を追加・変更したい場合は、サポートデスクで対応いたしますのでご連絡ください。
14	先日、Microsoftのデスクトップ版のコパイロットが不正URLを拾って表示してしまうという不具合があったと思いますが、AIが拾ってくる不正URLもブロックできますか？	AI(Copilotなど)が取得した URL に対する通信であっても、当該通信がWebレピュテーションによる不正URLに該当した場合には、Cloud Edge において、処理(通信のブロック、または監視)が行われます。
15	複数拠点で契約していますが、毎月のレポートは一つ送られてきます。全ての拠点を網羅したレポートでしょうか？	おまかせサイバーみまもりの月次レポートは、契約ID単位で作成・送付されます。そのため、複数拠点でご契約いただいている場合でも拠点ごと(契約IDごと)のレポートとなります。
16	新旧機器というのは初耳なのですが、機器が新しいのか古いのか？の判断はどうしたらよいでしょうか。	ご利用期間の長いお客さまより順次交換のご案内メールを送付しております。交換をご希望のお客さまは、メールの案内に従いお申込みください。



参加者からのご質問に対する回答 (2026年6月23日開催)

質問・回答①

No.	質問	回答
1	zoomやteamsで設定変更のサポートを受けられますか？ 電話とメールだけだと不便なので、今後teams等でやり取りできるようにしていただきたいです。	zoomやteamsでのサポート対応は実施しておりません。 今後のteams等でのサポート対応については検討をさせていただきます。
2	本日の資料をホームページへ掲載されるとのことです、そのホームページのURLを教えてください。	以下の「おまかせサイバーみまもり サポート情報」ページ内、【より便利にご利用いただくために(活用情報)】に掲載しております。本ページには、セミナー資料のほか、利用ガイドなどサービスをより効果的にご利用いただくための各種資料を掲載しております。ぜひご確認のうえ、ご利用ください。 https://business.ntt-east.co.jp/support/cybermimamori/
3	事故にあった際に対応を相談できる窓口があるとのことですが、どこで知ることができますか。	おまかせセキュリティ事故駆け込み窓口のHPはこちらになります。 https://business.ntt-east.co.jp/content/adlp/cybersecurity_sodan/
4	以下、2点質問があります。 ①サービス導入によって、不正ではないメールをブロックしている可能性はあるでしょうか。 ②現在、管理コンソールのアクセス権を持っていませんが、管理コンソールへのアクセス権があると、どのような操作が可能になるでしょうか。	①おまかせサイバーみまもりの初期設定では、メール自体をブロックすることではなく、メールの件名にタグ付けをいたします。 ②以下のような情報を確認することができます。 ・各セキュリティ機能のブロック状況(ブロックした機能及び脅威の名前やURLなど) ・URL指定によるアクセス制御機能にて接続をブロックしたURLの情報 ・アプリケーション利用制限機能にて利用をブロックしたアプリケーションの情報 など
5	開設時の資料が見つからない場合、どちらに相談すればいいですか	サービス開通日にメールにてご指定のメールアドレスに送付しておりますので、メールをご確認ください。 メールが見当たらない場合は、ご契約さま向けお問い合わせフォーム、もしくはセキュリティサポートデスクまでご連絡ください。 ■お問い合わせフォーム https://business.ntt-east.co.jp/support/cybermimamori/#anc-inquiry

質問・回答②

No.	質問	回答
6	ウイルス対策ソフトとの相性・親和性を知りたい。	おまかせサイバーみまもりはネットワークの出入り口を監視するのに対して、ウイルス対策ソフトは端末自体のセキュリティを向上します。どちらかを入れるのではなく、併用して多層防御されるのが望ましいと考えます。
7	以前、ウェブフィルタリングの機能で、HTTPSの通信がブロックできない不具合がありました。	「おまかせサイバーみまもり」において、TLS1.3に対応したブラウザの通信がブロックできない事象につきまして、本事象を改善するファームウェアの配信し、修正しております。 詳細は以下URLお知らせ欄2025.9.10の記事を参照してください。 https://business.ntt-east.co.jp/support/cybermimamori/#anc-info
8	事務所内で設定されているwifiにアクセスした時のみ、こちらの見守りサービスによって守られているという認識で間違えないですか？(PCに詳しくなくすみません)	例えばおまかせサイバーみまもりの配下に無線アクセスポイントが設置されていれば、おまかせサイバーみまもりを経由しますので、おまかせサイバーみまもりによって守られております。
9	複数台運用しておりますが、総合的に管理できる管理画面などはありませんでしょうか。	ダッシュボード画面よりご契約いただいている複数台のおまかせサイバーみまもりを管理いただけます。
10	固定電話への迷惑通信を遮断することができますか	おまかせサイバーみまもりにおいては固定電話への迷惑通信の遮断機能はございません。
11	CloudSandBOXとの連携はどうなっているのでしょうか？ESETでのクラウドサンドボックスと同じなのでしょうか？	おまかせサイバーみまもりのクラウドサンドボックスは「UTM(Cloud Edge)」側のサンドボックス機能であり、主にメールの不審な添付ファイルを仮想環境上で実際に動作させて脅威判定します。ESETのクラウドサンドボックス(端末エージェントが未知のファイルをクラウド解析する方式)とは役割が異なります。

質問・回答③

No.	質問	回答
12	本内容はEDRプランのみが対象ですか。	本セミナーの内容はおまかせサイバーみまもりを中心に説明をさせていただきました。
13	外出先でもおまかせサイバーみまもりが使える方法はあるのでしょうか。	おまかせサイバーみまもりの専用ボックスを外出先にご持参いただくことでご利用は可能です。ただし、固定IPアドレスの設定など、外出先のネットワークに設定を合わせていただく必要がございます。
14	cloudedgeとウィルスバスターは連携できるのでしょうか？	現状、Cloud Edge(専用ボックス)とウィルスバスターの連携機能はございません。
15	毎月メールでいただくレポートについて「どの状態であれば問題ないと判断できるのか」という基準が分からず、判断に悩むことがあります。特にIPSの検出は比較的頻繁に発生しており、検出内容が誤検知なのか、それとも実際に対応が必要な脅威なのかを判断することが難しい状況です。レポートを確認する際の着眼点や、どのような基準でリスクを評価・判断すればよいのかといった、実務的な観点についてもご説明いただけると、大変参考になります。(今後別のセミナーでご説明の機会があると大変助かります)	ご意見いただきありがとうございます。月次レポートを読み解き、設定のポイントをお伝えするセミナーを企画しております。
16	不審なメールが届くことがあります。どのような対応がされているのでしょうか。	おまかせサイバーみまもりのメールセキュリティ機能においては、メール自体をブロックすることではなく、メールの件名にタグ付けをいたします。

質問・回答③

No.	質問	回答
17	デモ画面では、ギャンブルをブロックしておりましたが、ブロックするカテゴリは、ある程度、事前に登録されているのでしょうか。ギャンブルやアダルトなどは、事前にこちらが設定しなくてもブロックされるのでしょうか	ギャンブルやアダルトは初期設定でブロックはしておりません。初期設定では、ピアツーピアのみブロックをしております。 詳細は以下のセキュリティ機能設定の初期値を参照してください。 https://my.ebook5.net/ntteast-pamphlet/security-default/
18	コンソールに久々にログインを試みたところ、以下のメッセージが表示されました。「お使いのモバイルデバイスからGoogle認証システムアプリを使用してTrendAI™ SaaS製品用の確認コードを取得し、そのコードを入力してログインしてください。」 PCでログインしておりまして、Google認証システムの他にログイン方法はございますか？	二要素認証を設定されていないでしょうか。もしログインができない場合は、お手数ですがセキュリティサポートデスクまでご連絡いただけますでしょうか。 ■お問い合わせフォーム https://business.ntt-east.co.jp/support/cybermimamori/#anc-inquiry
19	この1か月で1端末の異常を検知することができたが、異常通知のタイミングを設定が可能であるかを知りたい。	C&C通信のアラートに関するお話かと存じます。本アラートは検知が発生したタイミングで通知される仕組みのため、通知タイミングを任意に変更することはできません。
20	他社製のUTMとの違いはありますか？	一般的なUTMは機器・ライセンス提供が中心ですが、おまかせサイバーみまもりは24時間365日のセキュリティ監視とサポートデスク対応をセットで提供しています。 また、C&C通信などの脅威を検知した際には、メールや電話による通知を実施します。 マルウェア感染が疑われる場合は、遠隔での調査・駆除支援や復旧サポートを受けられます。



参加者からのご質問に対する回答 (2026年9月18日開催)

質問・回答①

No.	質問	回答
1	管理コンソールにログインするユーザーIDとパスワードがわからない場合はどこに問い合わせればよいでしょうか	セキュリティサポートデスクへお問い合わせください。 ユーザーIDをお伝えします。 パスワードのリセットは、以下のフォームより依頼可能です。 https://business.ntt-east.co.jp/support/cybermimamori/#anc-inquiry 『パスワードリセット・メールアドレス変更』よりご連絡いただけます。
2	管理コンソールのログ分析機能で、ユーザー名がPC名のもので表示されるものがあります。PC名で表示させる方法を教えてください	以下の条件をすべて満たす場合にコンピュータ名(PC名)で表示されます。IPアドレスで表示されている端末は、いずれかの条件を満たしていない可能性が高いと考えられます。 ・PCなどのデバイスがIPアドレスをDHCPで取得している ・DHCP Discoverパケットが専用BOXを通過している ・DHCP DiscoverパケットにHostname情報が含まれている
3	初期設定では、ファイアウォールが無効のまま提供されているのはなぜですか	デフォルトで有効とした場合、正常な通信へも影響が生じる可能性があるため、ファイアウォール機能を無効の状態ですべてサービス提供させていただいています。
4	停電後、専用BOXが再起動を繰り返します。対処方法を教えてください	本件につきましては、個別事象であり、詳細な確認が必要なケースと認識しております。 お手数ですが、セキュリティサポートデスクへご相談ください。
5	複数の拠点におまかせサイバーを設定しています。管理コンソールへのログインは拠点ごとに設定しなければいけないでしょうか	複数拠点の管理コンソールへのログインIDを統合できます。 方法については、セキュリティサポートデスクへお問い合わせください。
6	IDを統合することで、複数拠点に同じポリシーを配信できますか	IDを統合すると、同じ設定を配信することが可能になります。
7	同一内容のセミナーは今後、開催予定はありますか	2026年度中に同一内容のセミナーの開催を予定しております。

質問・回答②

No.	質問	回答
8	セキュリティポリシーは初期設定のまま使用しても大きな問題はございませんか	当社で推奨するセキュリティ設定をデフォルト設定として提供させていただいております。 利用環境に応じて設定をご確認ください。
9	機器の交換に関して、自身での交換が難しい場合の対応はどうしたらいいでしょうか	交換作業の際、専用BOXのIPアドレス設定等、不明な点があれば、セキュリティサポートデスクでサポートさせていただきます。 また、現在のセキュリティ設定は引継ぎされます。
10	おまかせサイバーみまもり月次レポートにて、報告された内容について原因を調査したい	本件につきましては、個別事象であり、詳細な確認が必要なケースと認識しております。 お手数ですが、セキュリティサポートデスクへご相談ください。
11	一部の社員にフィッシングメールが毎日数十通届くようになった。対策を教えてください	メールセキュリティ機能を見直していただくことで、受信数を低減できる可能性があります。 具体的な設定方法等につきましては、セキュリティサポートデスクへお問い合わせください。
12	LINEやInstagram、X、Facebook等を設定上ブロックしていますが、ブラウザ経由だとアクセスできたり、リンクから経由では接続できます。設定に問題がありますか	ブロックの設定に不足がある可能性がありますので、セキュリティサポートデスクへご相談ください。
13	今回のセミナーの内容を動画配信することはできますか	動画の公開予定はありません。同内容のセミナーを2026年度中に開催予定ですので、ぜひご参加ください。
14	月次レポートの冒頭で、検知したセキュリティ脅威の状況を天気予報で表しているが、こちらの掲載目的を教えてください	天気表示によりお客様のリスク状況を直感的に把握できるようにしています。

質問・回答③

No.	質問	回答
15	おまかせサイバーみまもりのStandardプランを利用しています。会社支給のスマートフォンを20台配布予定です 会社のネットに接続する場合はおまかせサイバーみまもりの上位グレードに変更したほうが良いでしょうか	接続機器が増えることでインターネットへの通信接続が遅い状況があれば、より高いスループットでのご利用が可能なGigaプランへの変更をご検討いただければと思います。 プラン変更につきまして弊社の営業担当または以下の窓口までお問い合わせください。 ■お電話でのお問い合わせ フリーダイヤル 0120-116-032
16	ポリシー施行のログの処理ブロックでポリシー名は表示されているのですが、接続しようとしたURLアドレスを調べることは出来ますか	URL全体は確認はできませんが、接続先のドメインを確認することが可能です。
17	ChatGPTなどの生成AIサービスについて、 機密情報漏洩防止の観点から社員の利用を抑制するためのフィルタリング設定は可能でしょうか	生成AIサービスの通信を制御することは可能です。 具体的な設定方法についてはセキュリティサポートデスクでサポートさせていただきます。
18	メールセキュリティはIPv6対応していますか	2026年10月現在、IPv6には対応しておりません。
19	セグメントを分けたいのですが、現在は単一セグメントしか接続できないのでしょうか	おまかせサイバーみまもりには、セグメントを分ける機能がありません。 ルーター等で、VLAN機能を使用してセグメントを分ける必要があります。 おまかせサイバーみまもりでは、VLAN通信もセキュリティ検査することができます。
20	おまかせサイバーみまもりを利用してもウイルス対策ソフトは必須でしょうか	端末を保護するウイルス対策ソフトとの併用を推奨します。 おまかせサイバーみまもりはネットワークの出入り口を監視するのに対して、ウイルス対策ソフトは端末自体のセキュリティを向上します。どちらかを入れるのではなく、併用して多層防御を行うことが望ましいと考えます。
21	購入したウイルスバスターは重複しますか	おまかせサイバーみまもりとは、主な保護対象が異なるため、基本的に併用できます。 なお、おまかせサイバーみまもりはネットワークの出入り口を監視するのに対して、ウイルス対策ソフトは端末自体のセキュリティを向上します。

質問・回答④

No.	質問	回答
22	10Gbps回線の引き込みを検討しております。おまかせサイバーみまもりで10Gbps回線に対応しているプラン、機器等はございますでしょうか	2026年10月現在、10Gbps回線に対応したプランはありません。
23	専用BOXのスループットが最大1Gbpsだと、10Gbps回線利用する場合などにはボトルネックになると思いますが、おまかせサイバーみまもりに代わるサービスの提供予定はありますでしょうか	2026年10月現在、提供予定はありません。