NTT EAST

おまかせサイバーみまもり

「知らなきゃ損！
おまかせサイバーみまもりの便利な使い方」

2025年12月

目次

1. 本セミナーの目的のご説明(3分)

2. 脅威の最新動向と対策(10分)
脅威の最新動向と対策:ランサムウェアの事例と対策を解説

3. おまかせサイバーみまもりサービス概要 (10分)
サービス概要説明:おまかせサイバーみまもりのサービス概要
導入後の運用紹介:セキュリティサポートデスクでのインシデント対応事例の紹介、設定変更等の運用対応について

4. サービス活用のコツ(20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
レポート解説:レポートの見方の解説
駆け込み窓口紹介:駆け込み窓口の概要説明
利用ガイドの紹介
よくある問合せ、対応内容:FAQの紹介、セキュリティサポートデスクのご案内

5. 最後に(10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、導入初期に感じやすい不安や疑問を解消し、安心してサービスをご利用いただくことを目的としています。
さらに、主催者側の思いとして、契約者の皆様とのコミュニケーションを活性化し、サービス改善に努める取り組みの一環として開催しております。

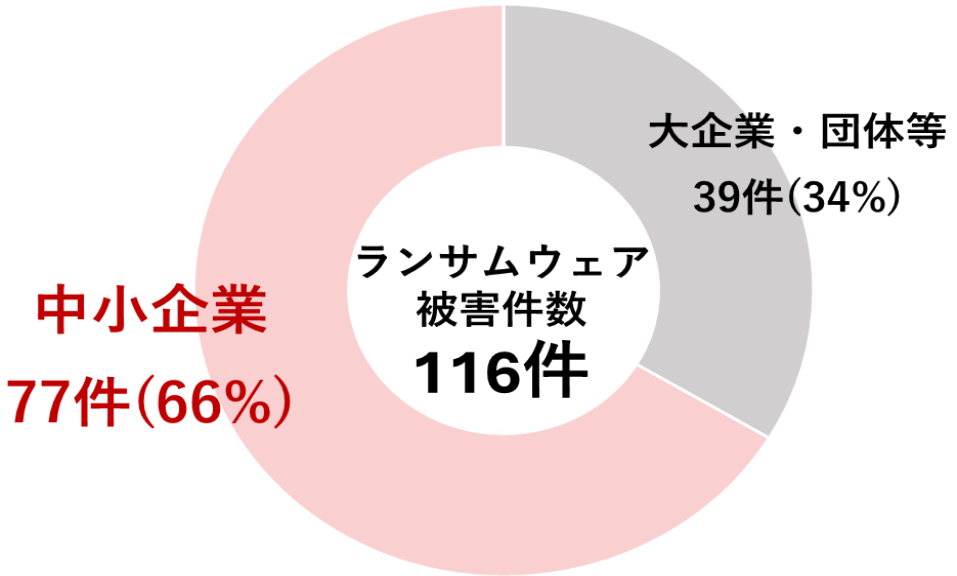
具体的には、サイバー攻撃の最新動向や、本サービスがどのようにリスクを低減するかを事例を交えて紹介し、導入後の運用イメージを明確にします。
さらにサービスの仕組みや特徴をわかりやすく解説し、日常業務における効果的な活用方法をご紹介させていただきたいと考えております。

契約者の皆様がサービスの価値を最大限に引き出し、安心・安全な環境を構築できるようサポートすることが本セミナーの狙いとなります。

2. 脅威の最新動向と対策

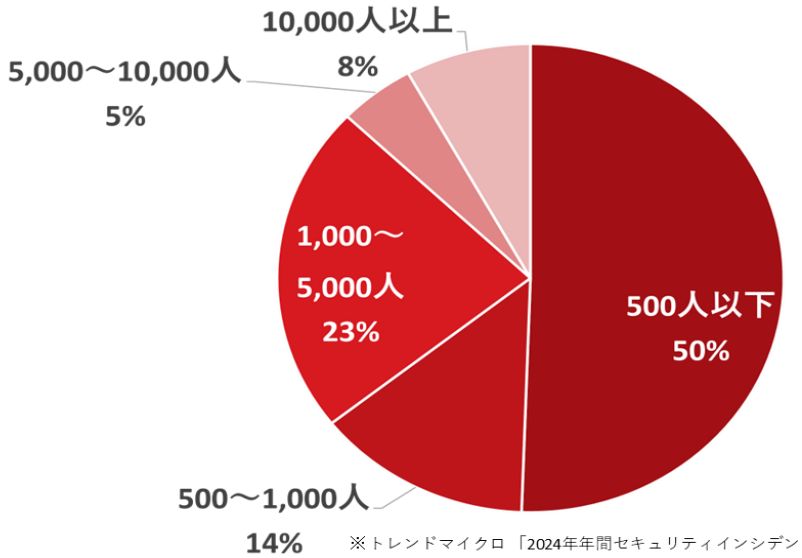
なぜ中小企業が狙われるのか

ランサムウェア被害の企業・団体等の規模別報告件数



※警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」

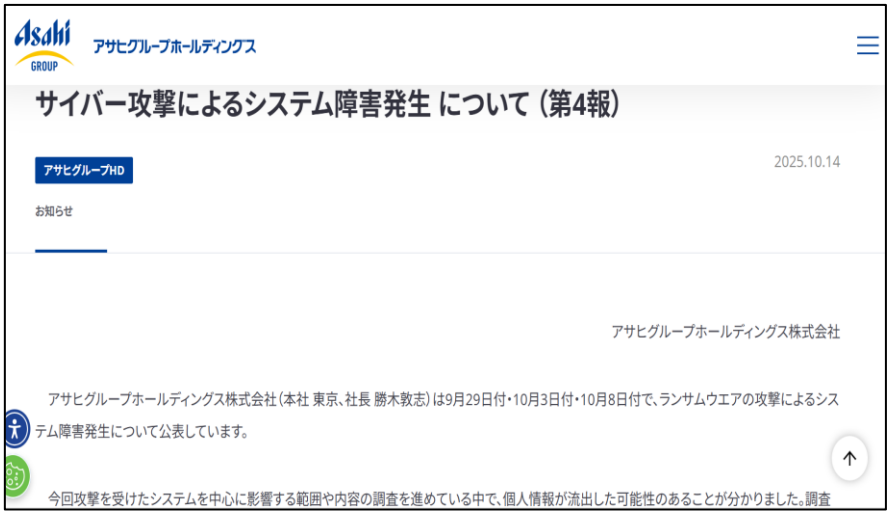
2024年の国内組織における
ランサムウェア被害の従業員規模別内訳



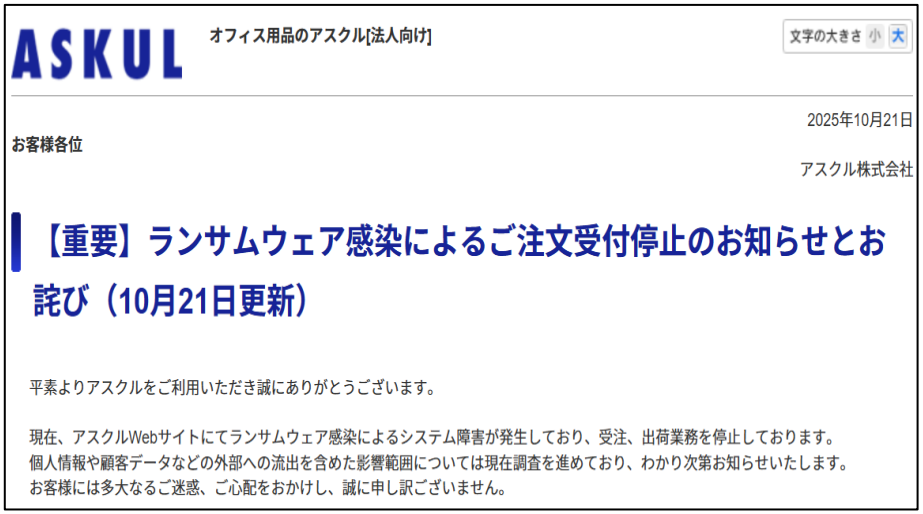
※トレンドマイクロ「2024年年間セキュリティインシデントを振り返る」

ランサムウェア被害が続出

9/29にアサヒグループホールディングス様で、10/19にASKUL様でランサムウェア被害が発生



サイバー攻撃によるシステム障害発生 について（第4報）｜ニュースルーム｜アサヒグループホールディングス

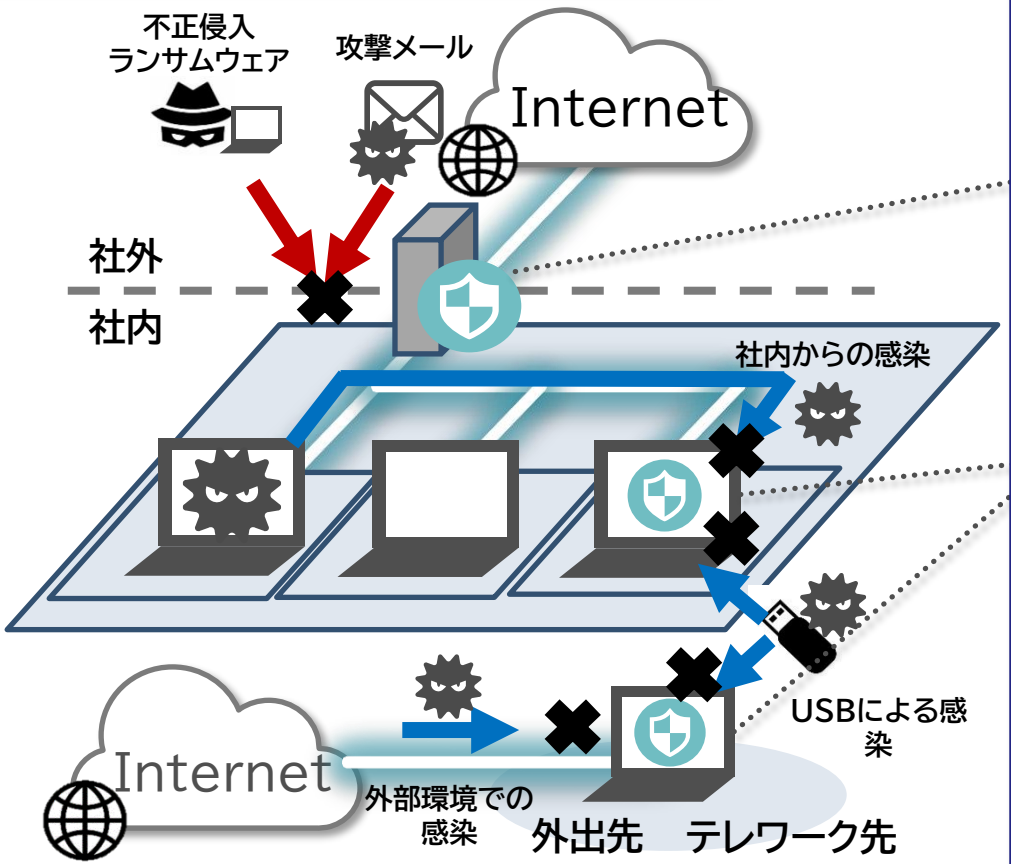


【ASKUL】お知らせ詳細 - オフィス用品の通販 アスクル

3. おまかせサイバーみまもり サービス概要

おまかせサイバーみまもりとは

中小企業へのサイバー攻撃と必要な対策



おまかせサイバーみまもりセキュリティパッケージ

出入口対策（UTM） おまかせサイバーみまもり

社内外の通信を監視し不審な通信を遮断

外部からの不正通信やメールによる攻撃、
不審なWebページとの通信から守ります！

端末対策（EPP+EDR） おまかせアンチウイルスEDRプラス

PC端末の感染防御、感染後の早期検知

端末に到達するサイバー攻撃を防御！
感染を早期検知し、侵入経路や感染範囲を
分析・感染からの復旧をサポート！

セキュリティサポート

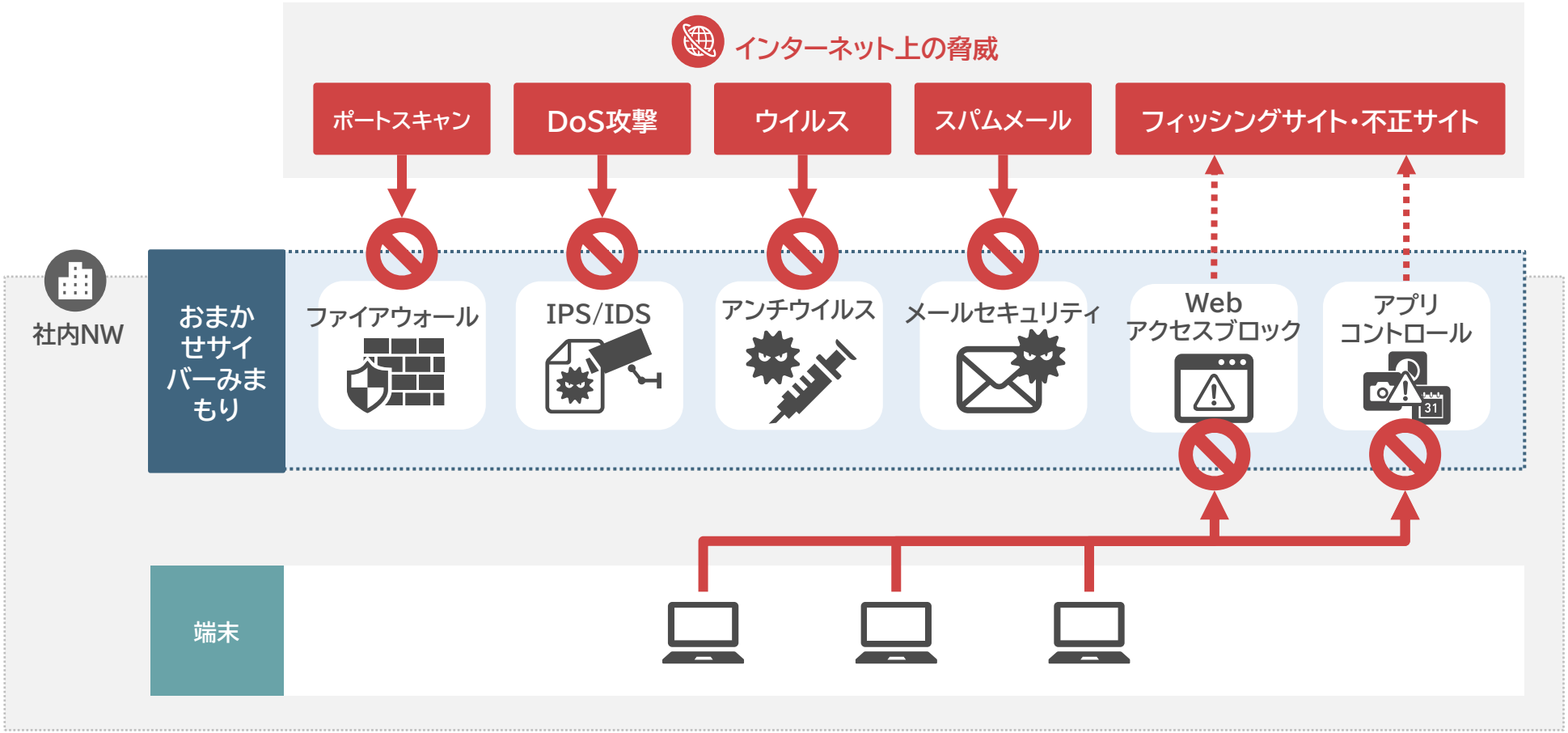
統一的なセキュリティ相談窓口

日々の運用監視、設定変更
異常検知時のアラート通知連絡
サイバーインシデント時の支援

必要な対策をパッケージ化したオールインワンサービス

おまかせサイバーみまもりとは

「おまかせサイバーみまもり」は、社内ネットワークとインターネットの間で行われる通信を常に監視し、不正なアクセスや脅威を検知することで、社内ネットワークの安全性を守ります。



おまかせサイバーみまもりの動き①

インターネットからの脅威に対するセキュリティ

インターネット経由の攻撃

不正アクセス

ポートスキャン
サーバに対してパケットを送信して、解放されているポート番号を調べる行為。
脆弱性の有無などを把握し、攻撃の準備に利用される。

DoS攻撃
コンピュータから一斉に大量のリクエストを送信し、サーバに負荷をかけてWebサービスやサイトを接続不可の状態にする攻撃。

ワーム
マルウェアをほかの端末に拡散させる動きをするプログラム

ネットワークレベルの保護

ファイアウォール機能
送信元のIPアドレスやポート番号などの情報から、その通信を許可するかどうかを判断し、内部ネットワークへの侵入を防ぐ。

サーバOS／ミドルウェアレベルの保護

IPS/IDS機能
サーバやネットワークの外部との通信や、内部での不正な通信を検知・防御する。

おまかせサイバーみまもりの動き②

社内からWebサイトを安全に利用するための機能

不正サイトへのアクセス対策

Webサイトアクセスブロック
不正と判断されたサイトへのアクセスをブロックする機能。
不正プログラムによる感染やフィッシング詐欺の被害を未然に防止する。

ポリシー違反対策

URLフィルタリング
社内ポリシーに基づき、
不正ではないが業務上不要なWebサイトへのアクセスを制限する。

アプリケーション利用制限
社内ポリシーに基づき、
不正ではないが業務上不要なアプリケーションの利用を制限する。

悪意のあるサイト

不正と判断された
Webサイトの利用

ポリシー違反

社内ポリシーに反した
Webサイトの利用

社内ポリシーに反した
アプリケーションの利用

おまかせサイバーみまもりの動き③

メールを安全に利用するための機能

メール経由の攻撃

メールセキュリティ

送信元の情報（メールアドレス、ドメイン、IPアドレス等）とブラックリストとの突合による
ブロック機能や、本文の解析によってスパム判定されたメールの削除や隔離を行う。

マルウェアの添付

本文中の不正サイトへのリンク

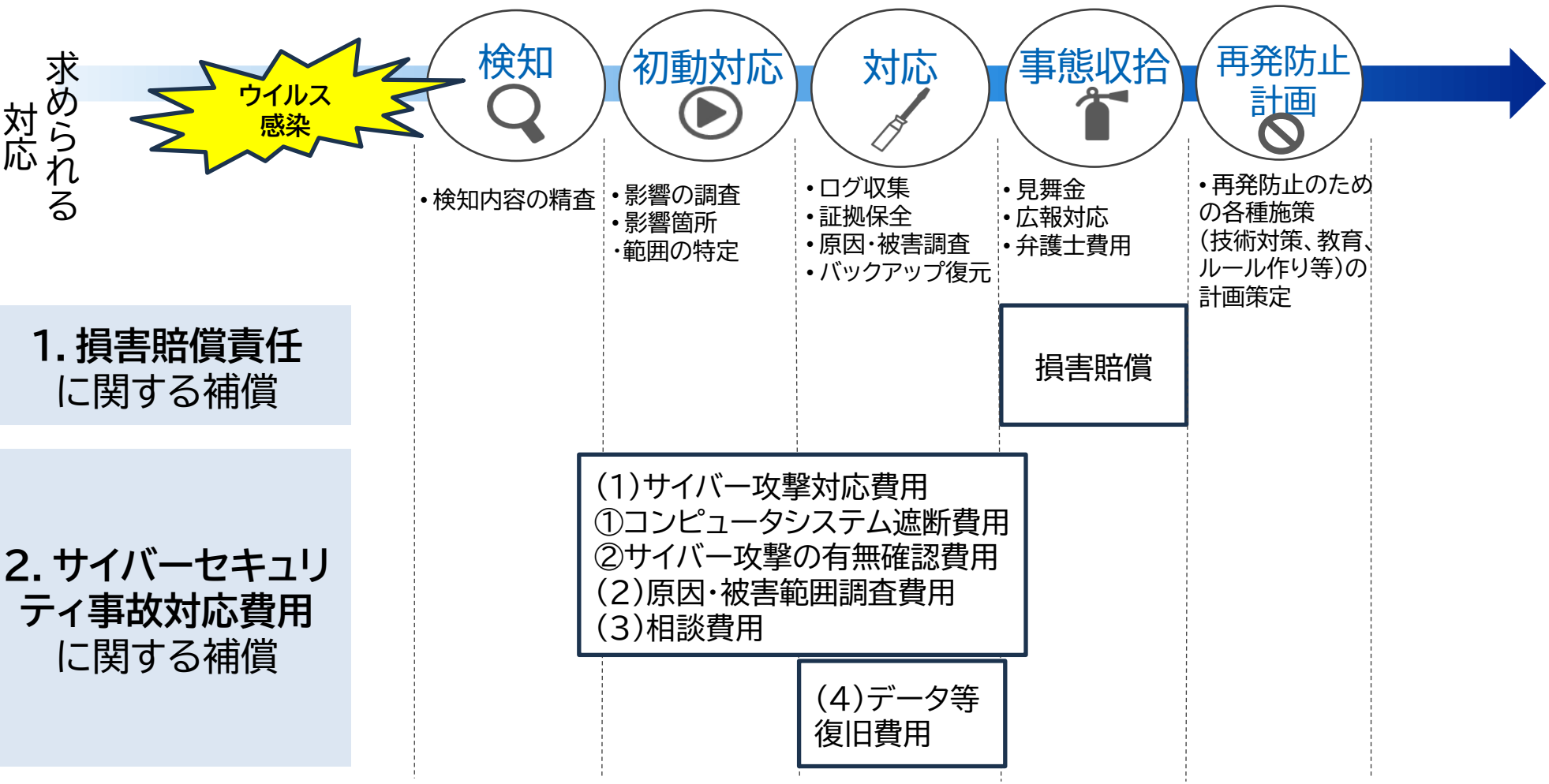
サイバー保険のご案内

- **有事の際も安心！サイバー保険付帯**
  - 全プラン、タイプに自動的に保険が付帯
  - サービス価格は据え置き。別途、保険料の支払いも不要

補償金額	最大200万円		
補償ステータス	初動対応	対応	事態収拾
補償内容	・影響調査 ・初動対応	・原因調査 ・データ復旧	・損害賠償 ・訴訟対応

サイバー保険 補償イメージ

サイバー攻撃を受けた場合に、「損害賠償責任」と「サイバーセキュリティ事故対応費用」に関する損害を補償※1します



※1:サイバー攻撃によって生じた実際の損害額を、本保険で全額カバーするものではございません。

セキュリティサポートデスク

- **セキュリティのプロによる運用サポート！**
  - 不正な通信を見つけたらプロからメール・電話で連絡、解決支援
  - 分からないことはプロの目線から支援

NTT EAST

Cloud Edge

セキュリティ
サポートデスク

セキュリティの
プロが運用

・不正通信の常時監視（24時間365日）
・遠隔でのウイルス駆除や復旧支援
・検知内容をレポート報告

遠隔サーバとの通信	不正Webへの通信	セキュリティサポート件数
5.4万件 （1社あたり1.9件）	10百万件 （1社あたり360件）	1.5万件

セキュリティサポート事例①

C&Cサーバへの通信ログを検知

対応事例

・業種　　:出版・印刷業(従業員20-30名)
・発生日時　:2017年9月26日
・発生内容　:C&Cサーバへの通信(計1,146回)
・感染端末　:1台(WindowsXP)

発生事象

実際のお客様の通信ログ（突然C2サーバへ接続開始）
10:12:22 □92.168.1.11□http://＊＊＊＊rzy8823l68me.net/account.asp?qu=cmd□
10:11:59 □92.168.1.11□http://＊＊＊＊siebabanahujtr.org/login.asp□
10:11:43 □92.168.1.11□http://＊＊＊＊siebabanahujtr.org/login.asp□
10:11:21 □92.168.1.11□http://＊＊＊＊rzy8823l68me.net/account.asp?qu=cmd□
10:09:45 □92.168.1.11□http://＊＊＊＊siebabanahujtr.org/login.asp□

お客様へのインシデント発生状況のご説明

- 外部からお客様の端末を遠隔操作するサーバに通信が発生していることを説明(C&Cサーバ通信の説明)
- 該当の通信が身に覚えがあるか確認　→　お客様は身に覚え無し

被疑端末の特定

- 不正通信が発生している端末のIPアドレスをお客様に伝え、被疑端末を特定
- 端末がOSサポートが切れているWindowsXPであることが発覚

対応方法コンサル

- 被疑端末をネットワークから切り離し(LANケーブル抜去)
- 端末のウイルス対策ソフト(他社製品)によるフルスキャンを推奨

⇒C&Cサーバへの通信停止を確認

アフターコール(後日電話応対)

- 対処後はC&Cサーバへの通信が発生していないことを連絡
- サポート対応後、困ったことや不明なことがないかヒアリング
- サポートセンタからの連絡を受け、改めてセキュリティリスクを認識し、該当WindowsXP端末を廃棄

セキュリティサポート事例②

UTM導入後、業務上アクセスするサイトへの接続ができなくなった・・・

①

新しく見ようとしたサイトがブロックされてしまった・・・

②

困ったときはセキュリティサポートデスクに相談だ！

③ 《サポートデスク対応》

①お客さまコンソール画面よりURLフィルタ項目を確認
⇒危険なサイトや業務に不要なサイトへのアクセスをブロックするために、指定したブロックするURLカテゴリに該当したため、アクセスができなくなったことが判明

④

②お客様の用途を確認後、URL許可リストに追加する設定変更を即座に実施

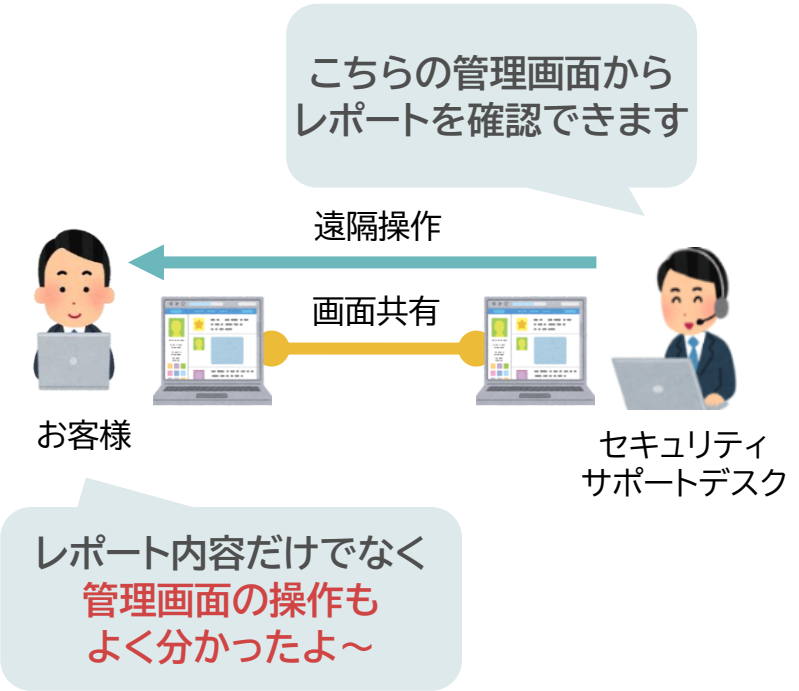
安全な通信・サイトであることを確認し、
即座に設定変更対応

セキュリティサポート事例③

受領した月次レポートを削除してしまい、内容が確認できなくなってしまった

月次レポートの内容について問い合わせを頂いたが、
送付済みのレポートファイルは削除していた

お客様の端末に**リモートで接続**し、
管理コンソール画面を操作することで、レポート内容、
確認方法の説明を実施



レポート内容の説明だけでなく、管理コンソール画面の操作もサポートします！

4. おまかせサイバーみまもり 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。

①

②

① ブラウザを開きお客様管理コンソール(https://clp.trendmicro.com/Dashboard?T=N7oD2)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。

※「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」メールより、お客様ご自身で設定する必要がございます。

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。

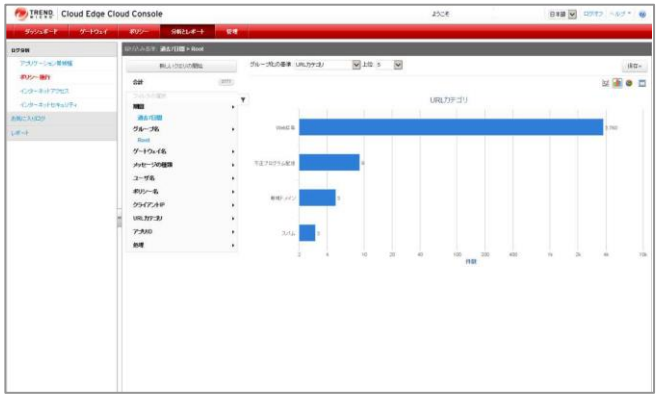
管理コンソールのトップページに遷移します。

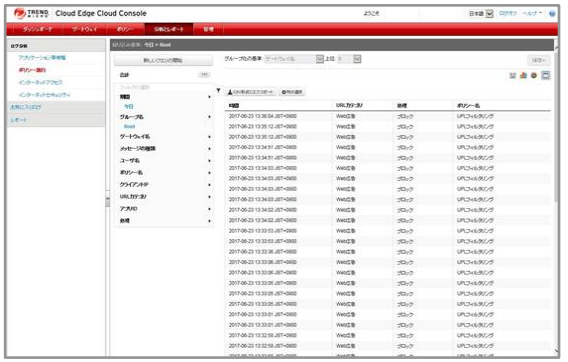
管理コンソール

ログ分析機能

ポリシー施行

- 「ポリシー施行」では、URL指定によるアクセス制御機能や、アプリケーション指定によるアクセス制御機能の検知状況を確認することができます。
- ポリシー施行にカテゴライズされる機能は、主に**お客様の業務に不要なURLへのアクセスやアプリケーション利用を制限**する機能です。





月次レポートには表示されない項目毎にアプリケーションの利用状況を確認し、業務改善訴求へつなげよう！

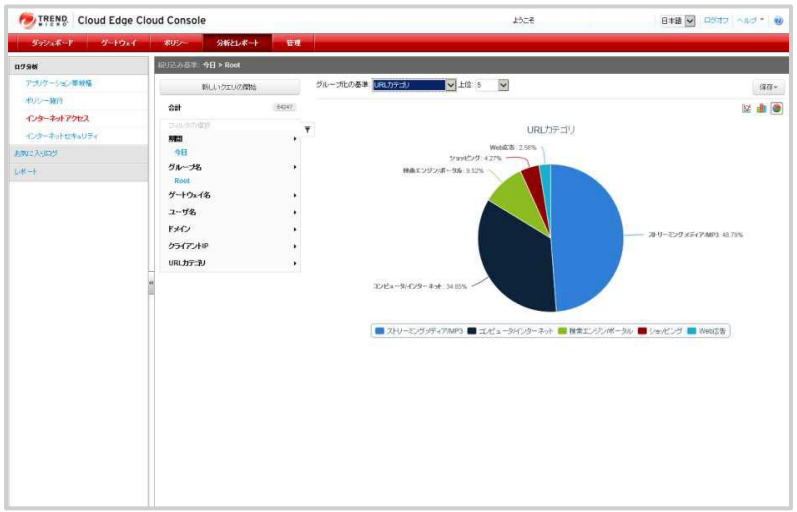
いつどのURLがブロックされたか詳しく知りたい場合に活用しよう！

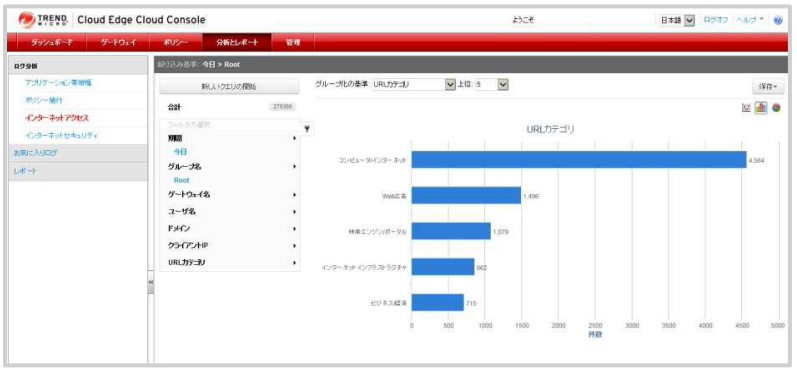
管理コンソール

ログ分析機能

インターネットアクセス

- 「インターネットアクセス」では、**おまかせサイバーみまもりを通してアクセスしたWebサイトに関する情報を確認**することができます。
- 「いつどの端末からどのサイトにアクセスしたのか」という情報までは知ることができません。





もし業務に必要ないカテゴリに頻繁にアクセスしていたら、業務内容や機器設定の見直しを行おう！

デモンストレーション

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）

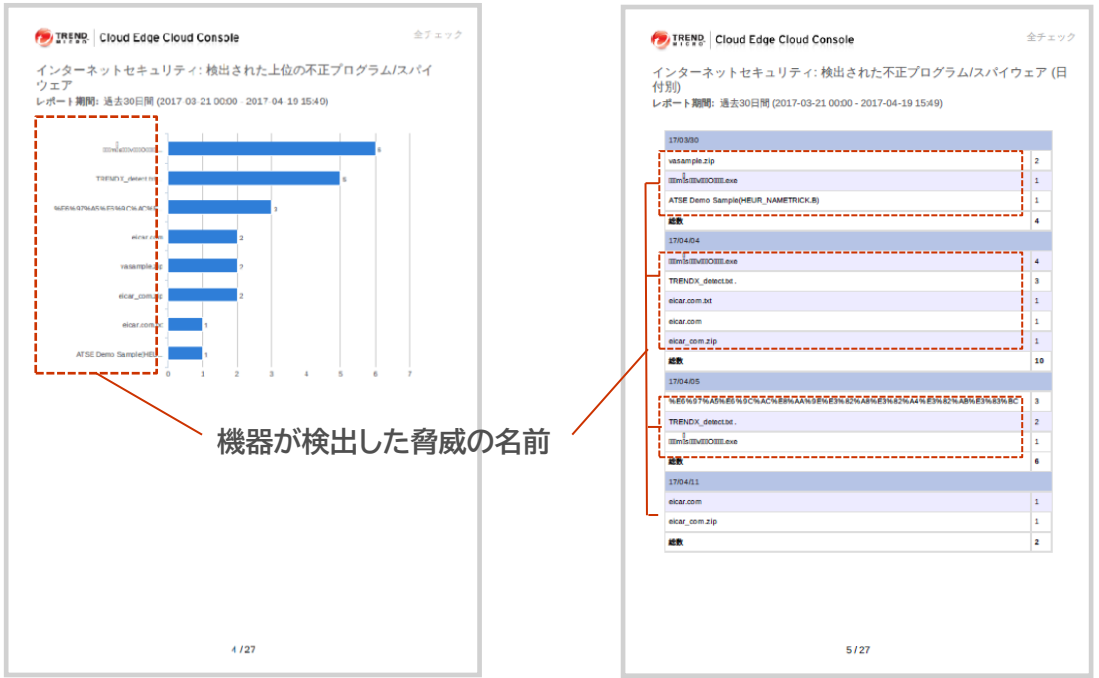
・お客様へのレポート配信で脅威の侵入や不正サイトへのアクセスのブロック状況を見える化

・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

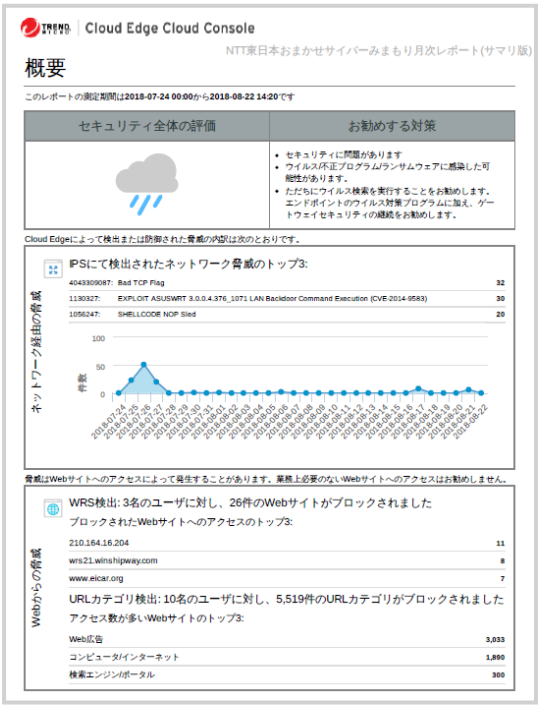


機器が検出した脅威の名前

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



月次レポート解説書

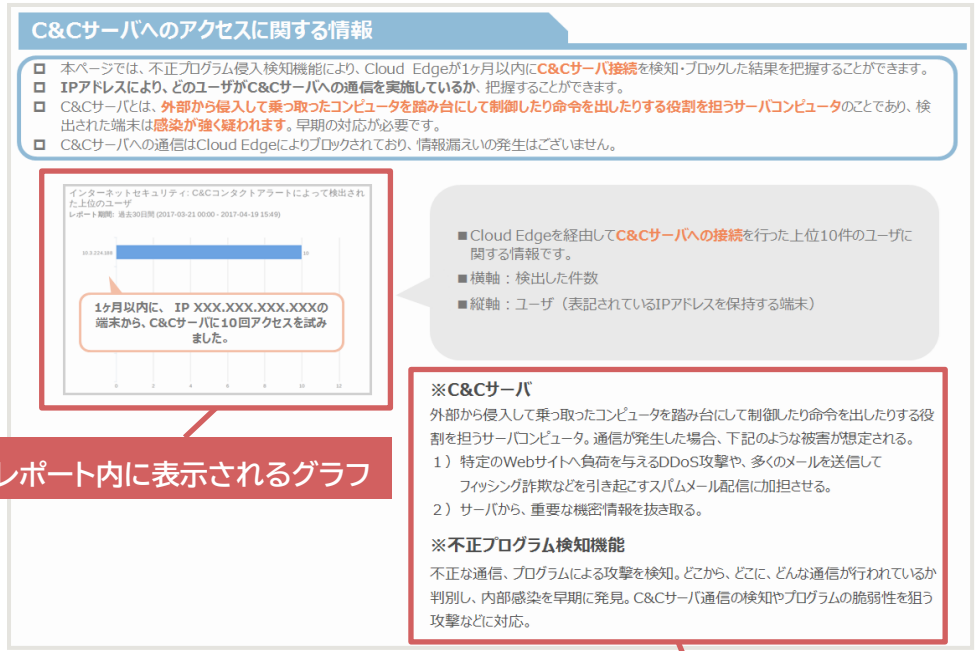
レポート解説書（一部抜粋）

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

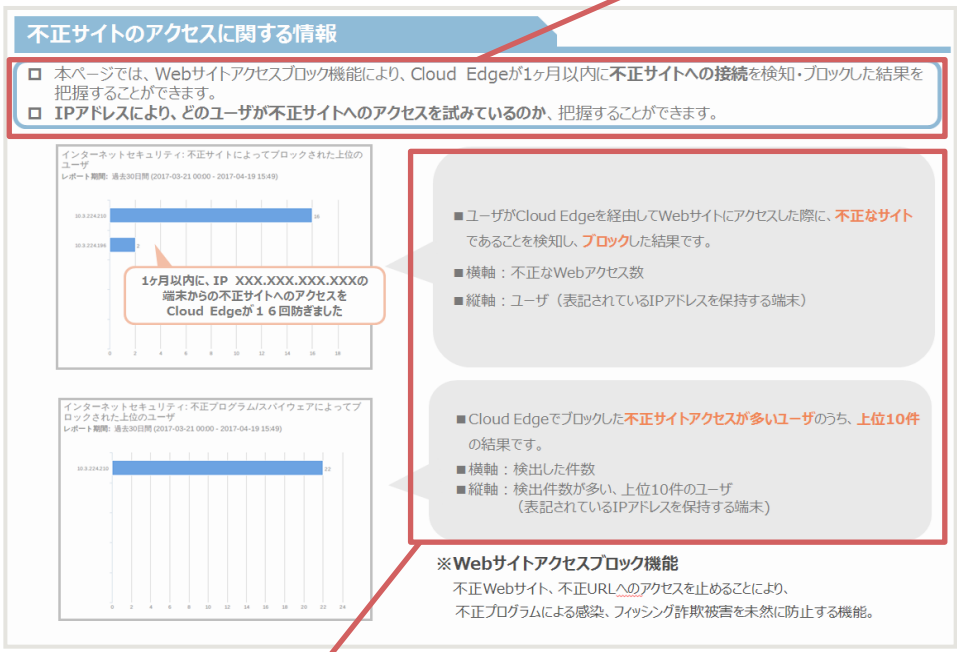
◆ C&Cサーバへのアクセス検出に関する説明



レポート内に表示されるグラフ

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



グラフの読み方

おまかせセキュリティ事故駆け込み窓口のご案内

- 情報セキュリティ事故に遭遇した際、被害を最小限に抑制する、事故発生の原因を解析する、事故発生前の状態に復旧するなどのサポートを行う窓口です。
- NTT東日本のサービスをご利用いただいていないお客さまでもご利用いただけます。

**セキュリティ事故発生時に
まずご相談いただける窓口です**

※同意書に同意いただいた後に、電話番号が表示されます。

セキュリティサポートデスク　問い合わせ先

セキュリティサポートデスク　電話での問い合わせ

- 電話番号は、ご契約者様のご契約状況に応じた上記いずれかの番号が、開通時に郵便で送付される重要事項説明書に記載されています。

項目	内容
受付時間	電話　：9:00-21:00
受付方法	電話によるお問合せ
有人受付及び 対応時間	9:00～21:00（365日） • 21:00以前に対応開始し、応対が21:00になっても終了していない場合は、問い合わせ対応が完了するまで対応 • 受付時間外に電話をお掛けいただいた場合は、翌日折り返し

セキュリティサポートデスク　Webフォームからの問い合わせ

- https://business.ntt-east.co.jp/support/cybermimamori/#anc-request
  『その他のお問い合わせ、変更依頼』>『設定変更・その他のお問い合わせについて』からご連絡いただけます。
- フォームの「お問い合わせの種別」は「設定変更・その他のお問い合わせについて」を選択してください。
- Webでのお問合せの際は、ご契約開始時にメールでお知らせしております、「ログインID」をご用意下さい。ご契約確認に必要となります。

FAQ

よくある質問

- おまかせサイバーみまもりでのよくある質問についてまとめています。お問い合わせの前に一度ご確認ください。

質問	回答
おまかせサイバーみまもりの専用BOXに固定IPアドレスを割当てたい（または変更したい）のですが、設定方法を教えてください。	固定IPアドレスの設定方法は、おまかせサイバーみまもりIPアドレス設定変更マニュアルを参照して下さい https://my.ebook5.net/ntteast-pamphlet/ip-address-manual/
• メールのセキュリティ警告が出るようになったので対処方法を教えてください。 • 証明書インストール方法を教えてください。	契約者管理コンソール（Cloud Edge Cloud Console)より証明書をダウンロードし、PC等のクライアント端末にインストールしてください。 https://my.ebook5.net/ntteast-pamphlet/certificate-install-manual/
おまかせサイバーみまもり専用BOXがオンラインか確認するにはどうしたらよいですか。	オンラインの場合、前面「Cloud Consoleに接続」横のLED（CloudEdge100 の場合のみ背面「12V DC」右下のLED）が「緑点灯」します。

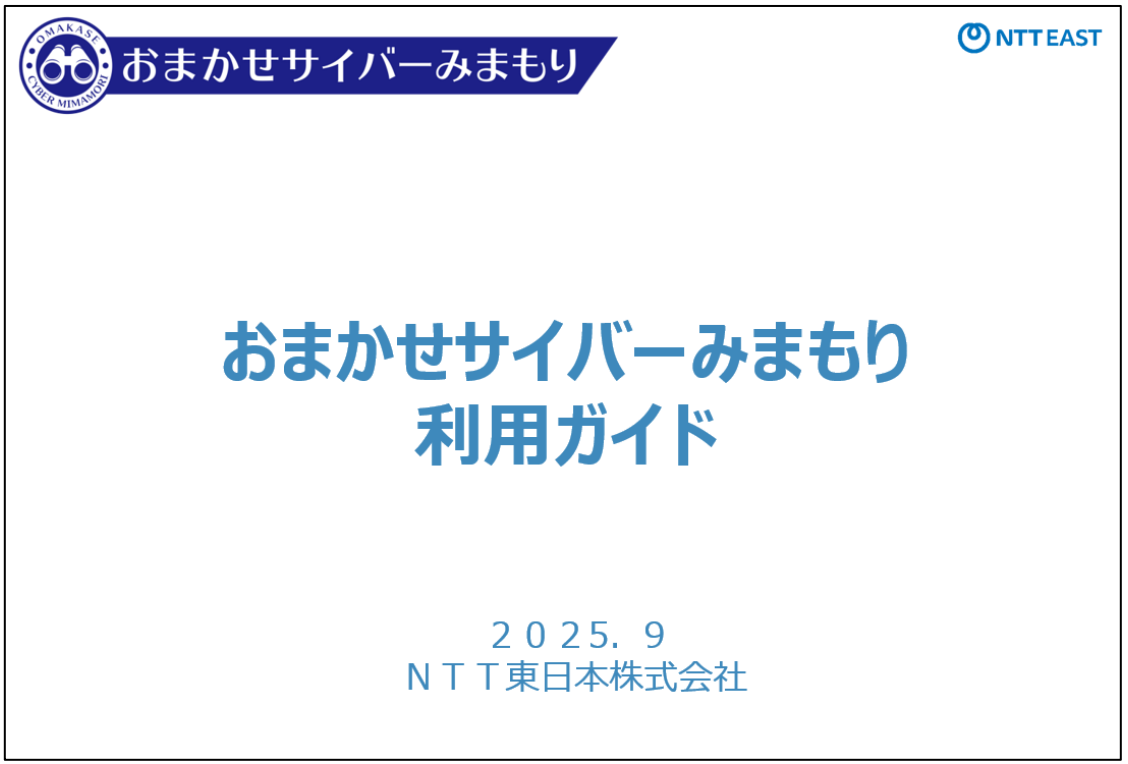
その他のよくある質問

- その他のよくある質問については、以下のリンクからご確認ください。

https://faq.ntt-east.co.jp/kb/ja/サービス一覧/ネットワークセキュリティ/おまかせサイバーみまもり

利用ガイドのご紹介

当サービスでは、契約者向けに「サービス概要」「トラブル時の対応方法」「サポート体制」などをまとめた**利用ガイド**を、2025年9月に公開しております。
このガイドは、万が一トラブルが発生した際に「どうすればよいか分からない」という不安を解消し、**安心してサービスをご利用いただけるよう利便性の向上を目的に作成**しています。ぜひご活用ください。



利用ガイドのURL
https://my.ebook5.net/ntteast-pamphlet/user-guide/

参加者からのご質問に対する回答

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-request
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いております。 ※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処のアドバイスをしております。
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ってしまった。 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%防げるものではございませんので、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、ランサムウエ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て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っている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。