

セキュリティ YOROZU 相談
サービス機能説明書 (Ver. 1.3)



2024 年 2 月

NTT コミュニケーションズ株式会社



目次

1.	はじめに.....	2
2.	サービス概要.....	3
2.1.	サービス概要	3
3.	サービス仕様.....	5
3.1.	セキュリティ相談窓口.....	5
3.2.	セキュリティメールマガジン配信サービス仕様.....	8
3.3.	Agent 衛生管理ツール（5 ライセンス初期バンドル）	10
3.4.	ヘルスチェックレポート（月次）	16
3.5.	Agent ライセンス追加（有償オプション）	18
3.6.	Web フィルタリング（有償オプション）	18
3.7.	情報漏えいリスク診断（任意活用）	21
3.8.	セキュリティチケット（個別見積り）	22
4.	前提条件・制限事項	22
4.1.	前提条件・制限事項.....	23
	改版履歴.....	24

1. はじめに

文書構成



2. サービス概要

2.1. サービス概要

2.1.1. セキュリティ相談窓口

「セキュリティ相談窓口」は、情報セキュリティに関する「困った」、「不安」、「知りたい」を解消するために、気軽に問合せができる相談窓口です。メール、電話で問合せをいただき、お問い合わせ内容やそれらの統計データをもとに当社のセキュリティエンジニアが回答します。

2.1.2. セキュリティメールマガジン配信

「セキュリティメールマガジン配信」は、週次でトレンド入りした時事情報や話題になっているトピックスをセキュリティと関連付けた記事、「重要なセキュリティの関心事をセキュリティのプロが分かりやすく解説した記事」などをメールマガジンとして配信します。

2.1.3. Agent 衛生管理ツール（5ライセンス初期バンドル）

「Agent 衛生管理ツール」は、Windows OS 端末に Agent を導入頂くことで、端末のインベントリ情報と端末操作履歴をログデータとして直近 90 日間分を常時収集・保管し、お客様からの問合せ対応やヘルスチェックレポート及び統計データ作成の基情報として活用します。

2.1.4. ヘルスチェックレポート（月次）

「ヘルスチェックレポート」は、Agent 導入済み Windows 端末から収集したインベントリ情報（OS 情報・ソフトウェア情報）と端末操作ログ（Web 接続ログ・ログオンログ・外部装置接続ログ）及びその統計データを基に、脆弱性を可視化した診断書としてレポートを月次で提供します。

2.1.5. Agent 衛生管理ツールのライセンス追加（有償オプション）

「Agent 衛生管理ツールのライセンス追加」は、初期バンドルされている 5 ライセンス（5 端末）以上の端末に Agent を追加導入されたい場合、有償オプションとしてライセンスをご提供します。

2.1.6. Web フィルタリング（有償オプション）

「Web フィルタリング」は、定型化したカテゴリ（セキュリティ・ギャンブル・出会い系・アダルト・ショッピングなど）に分類される Web サイトへ接続が出来ないようにしたいと希望される場合、有償オプションとしてサービスを提供します。

2.1.7. 情報漏えいリスク診断（任意活用）

「情報漏えいリスク診断」は、お申し込み時にご案内する簡易な「11 問の設問フォーム」に回答頂くことで、回答結果やその統計データをもとに社内の情報漏えいリスクを外部要因と内部要因の両面から分析評価し、リスク度を数値化した診断レポートを提供します。レポートには、総合評価と内外要因に対する簡易のアドバイスも付与します。

※情報漏えいリスク診断は、お客さまの任意による実施、およびセキュリティ YOROZU 相談窓口からのご案内をもとに実施となります。

2.1.8. セキュリティチケット（個別見積り）

「セキュリティチケット」は、お客様からの相談事に対し、個別での支援対応をご依頼頂く場合に、個別見積り内容に沿ってご購入頂くチケットです。

3. サービス仕様

3.1. セキュリティ相談窓口

3.1.1. セキュリティ相談

情報セキュリティに関する「困った」、「不安」、「知りたい」を解消するために、気軽に問合せができる相談窓口です。メール、電話で問合せをいただき、お問い合わせ内容やそれらの統計データをもとに当社のセキュリティエンジニアが回答します。



3.1.2. セキュリティ相談サービス仕様

本サービスでは、電話・メールにてセキュリティに関する相談にお答えします。

受付手段	連絡先	受付時間
電話	専用電話番号 (フリーダイヤル)	9:30～12:00 及び 13:00～17:30 ※土日祝日、年末年始(12/29～1/3)を除く
メール	専用メールアドレス	24 時間 但し、当社が相談内容の確認及び回答を送付する日時は、以下の通りです。 9:30～12:00 及び 13:00～17:30 ※土日祝日、年末年始(12/29～1/3)を除く

3.1.3. 想定している相談内容

本サービスで想定している相談内容は以下の通りです。

カテゴリ	相談内容の例
インシデントまたはインシデント疑い	<ul style="list-style-type: none"> • ウィルスに感染したかもしれません。どうすれば良いですか？ • 普段と違うこんな事象がありました。
脅威・脆弱性	<ul style="list-style-type: none"> • 情報配信記事を見ました。我が社が気を付けることはありますか？
不審なメール	<ul style="list-style-type: none"> • メールに添付された Word ファイルの「コンテンツの有効化」ボタンをクリックしてしまった。
ワンクリック請求	<ul style="list-style-type: none"> • アダルトサイトの登録完了画面(料金請求画面)が表示され、画面を消すことができません。
偽警告	<ul style="list-style-type: none"> • ウィルスに感染したという警告画面が出ていて消えません。ここに電話をかけるようにと電話番号も表示されています。
ランサムウェア	<ul style="list-style-type: none"> • ファイルが突然開けなくなった。拡張子も変わっている。 • 画面に「何が起こったのか?」、「料金の支払い方」が表示されている。

また、本サービスをご契約いただいたお客様は、以下の相談内容もお受けできます。(Agent 衛生管理ツールをインストール頂いているお客様に限ります)

カテゴリ	相談内容の例
PC 端末ログ調査	<ul style="list-style-type: none"> • 昨日退社した社員が機密データを持ち出した可能性があります。調べてもらえますか？
PC 端末ソフトウェア調査	<ul style="list-style-type: none"> • ○○というソフトウェアをインストールしている PC はありますか？ • このセキュリティパッチを適用していない PC はありますか？

3.1.4. 回答できない相談内容

本サービスで回答できない相談内容の場合、以下の相談窓口をご案内する場合があります。

カテゴリ	解決が期待できる相談窓口
契約に関するトラブル	<ul style="list-style-type: none"> ・ 消費者ホットライン ・ 国民生活センター
犯罪行為に関する被害届や捜査についての相談	<ul style="list-style-type: none"> ・ 都道府県警察本部のサイバー犯罪相談窓口
インターネット上での違法・有害情報に関する相談	<ul style="list-style-type: none"> ・ 違法・有害情報相談センター ・ インターネット・ホットラインセンター
フィッシングサイトの発見または被害に関する相談	<ul style="list-style-type: none"> ・ フィッシング対策協議会 ・ 警察庁 フィッシング 110 番

3.1.5. 注意事項

電話の場合：

- ・ ご相談は 1 回あたり 30 分以内を目安とさせていただきます。
- ・ ご相談内容によっては、折り返しのご連絡となる場合がございます。
- ・ サービス品質向上のため通話内容は録音させていただきます。

メールの場合：

- ・ メールを受信後、1 営業日以内を目途にご回答します。
- ・ 1 営業日を越える可能性がある場合は、別途ご連絡いたします。
- ・ ファイルを添付される場合は、セキュリティ YOROZU 相談窓口からファイルアップロードサイトをご案内しますので、セキュリティ YOROZU 相談窓口にご連絡ください。
- ・ フィルタリング設定をしている場合は、「ntt.com」ドメインを受信できるようにしてください。

3.2. セキュリティメールマガジン配信サービス仕様

3.2.1. 記事の選定について

本サービスでは以下のような記事を配信します。

① 主要検索エンジンで数多く検索されたトピックとセキュリティを関連付けた記事

週次で数多く検索されたトピックや世代別に今週話題となったキーワードなどを題材に、少しユーモアも盛り込みながら、トピックやキーワードに紐づくセキュリティの関心事を記事にしていきます。

② 重要なセキュリティの関心事をセキュリティのプロが分かりやすく解説した記事

直近で発生したセキュリティの関心事として、世間を騒がせている「Emotet」や「ランサムウェア」などに付いて、解りやすく解説すると共に、対策や事例などを交えて記事にしていきます。

③ 重要なセキュリティパッチの適用を促す記事

悪意のあるハッカーからのセキュリティ攻撃への備えとして重要な要素となる、OS やソフトウェアの緊急パッチ適用など、「適用を推奨する理由」、「適用しないとどうなるか」などを記事にしていきます。

3.2.2. 記事の内容（レベル感）について

本サービスでは以下のような内容(レベル感)で記事を記載します。

項目	内容
ボリューム(文字の量)	スマートフォンの画面でもサクッと読め、読み飽きない程度のボリューム
難易度	専門用語を避け(一般用語へ置き換え)、使う場合には解説を付ける
言葉遣い	親しみやすい言葉遣い・言葉選び

3.2.3. メールマガジンの配信タイミング

本サービスでは、「毎週水曜日 15:00 を目安」にメールマガジンを配信します。

3.2.4. メールマガジンの配信方法

本サービスでは、登録いただいたメールアドレスにメールを送付します。

送信者のメールアドレス： From: メルマガ配信専用アカウント

受信者のメールアドレス： To: メルマガ配信専用アカウント

Bcc: お客様のメールアドレス (メールリングリストを作成)

3.3. Agent 衛生管理ツール（5 ライセンス初期バンドル）

3.3.1. Agent 導入

ご契約頂いたお客様へ開通案内メールをお送りすると共に、メール本文に記載する URL から「Agent インストーラー」、「Agent アンインストール」、「インストール手順書」をダウンロードして頂き、以下の手順に沿って Agent を管理対象の Windows 端末にインストールして頂きます。

3.3.2. Agent インストール準備とインストール手順

Agent がクラウド上の管理サーバと通信を行う為、事前にルーター等のポート開放が必要になります。

※重要 開放して頂くポート番号 「TCP 80」「TCP 443」

ダウンロード頂いた「Agent インストーラー」を Windows 端末のデスクトップ上にコピー配置して頂き、「インストール手順書」に沿ってインストールを開始して頂きます。




インストールはデスクトップ上に配置したインストーラーをダブルクリックして頂くとインストールを開始します。

※Agent インストーラーのファイルサイズは、 50MB 程度です。


■注意事項

1. 既に何らかのIT資産管理ツールを導入済みのお客様は、専用アプリが相互干渉する為、本オプションをご利用いただけません。
※例：SKYSEA Client View、LanScope Cat、AssetView、IP-guard などのIT資産管理ツール
2. 対象のOSは、Windows OSの端末が前提となります。 MacOSやLinuxなどのOSの端末ではご利用いただけません。

■インストール前の準備と確認

3. Agentがクラウド上の管理サーバと通信を行う為、事前にルーター等のポート開放が必要になります。
※事前に開放して頂きたいポート番号 「TCP 80」「TCP 443」
4. 配布されたインストーラ（  XMPS_Agent_Manager_AIO.zip ） ZipファイルをWindows端末のデスクトップ上に配置して下さい。
5. Zipファイルをダブルクリックし、1つのファイル（  install.vbs ）と、1つのフォルダ（  AIO ）が格納されていることを確認して下さい。

■インストーラの実行

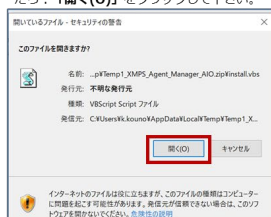
6. 上記5で確認したInstall.vbs（  install.vbs ）をダブルクリックし、次ページの手順に沿ってインストールを進めて下さい。
※インストールが完了するまで、端末の電源はシャットダウンしないようにお願いします。
※インストール中、次ページのステップで確認画面が表示されますので、手順に沿ってインストールを進めて下さい。



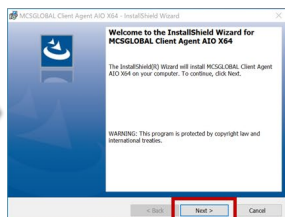
次ページの手順に沿ってインストールを進めて下さい。

■インストール進行中の画面とアクション

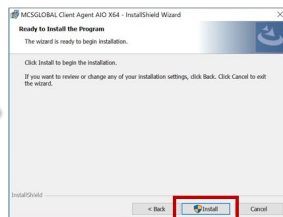
端末の設定内容によっては以下の画面が表示される場合があります。この画面が表示されたら、「開く(O)」をクリックして下さい。



この画面が表示されたら「Next」ボタンをクリックして下さい。



この画面が表示されたら「Install」ボタンをクリックして下さい。

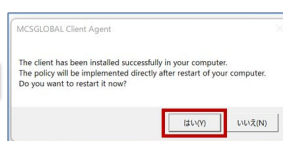


端末の設定内容によっては以下の画面が表示される場合があります。この画面が表示された場合、「はい」をクリックして下さい。

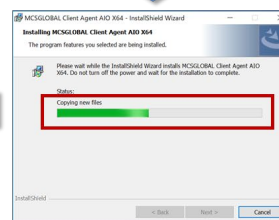


インストールが正常に完了した場合、画面下のタスクバーに「青色の盾の形をしたアイコン」が表示されます。
青色の盾のアイコンが表示されていれば、Agentインストールが成功しています。

以上でインストールは全て完了です。



この画面が表示されたらAgentインストールは完了です。最後に「今すぐに再起動を実行するか」を確認されますので、今すぐ再起動を実行する場合は、「はい」をクリックして下さい。ドキュメント作成など作業中や後からにしたい場合は、「いいえ」をクリックして下さい。

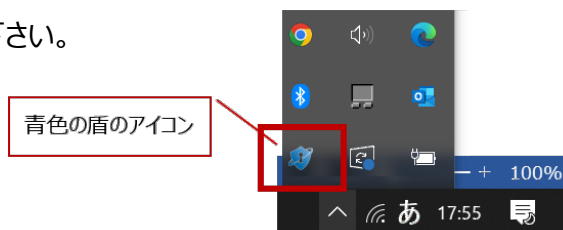


この画面が表示されると、インストールの進行状況がバー表示されます。
※進行中にWindows端末の電源シャットダウンは行わないで下さい。

3.3.3. Agent インストール完了確認

Agent インストールが正常に完了した場合、タスクバーに Agent のアイコンが表示されます。

タスクバーにアイコンが表示されていることを確認して下さい。



Agent インストール後、クラウド上の管理サーバと通信が開始され、月次でご提供する「ヘルスチェックレポート」を生成する為の、端末情報（インベントリ情報・各種操作ログ）が管理サーバにアップロード保管されます。

3.3.4. 対象 OS と端末性能要件

対象 OS は『Windows』に限ります。

「ヘルスチェックレポート」をご利用頂くための、Agent を導入する Windows 端末に求めるスペック要件を以下に示します。

項目	内容
CPU	Intel Core 2 Duo 2.4GHz 以上
メモリ	1GB 以上
HDD	100MB 以上
OS	Microsoft Windows 10 22H2、Microsoft Windows 11 22H2 windows server 2016、windows server 2019 windows server 2022
ブラウザ	Google Chrome 46.0.2490 ~ 103.0.5060.53 Mozilla Firefox 49.0 ~ Mozilla Firefox 101.0.1 Microsoft Edge 44~103.0.1264.37

3.3.5. 取得する操作ログの種類

Agent を導入した Windows 端末から、以下の各種操作ログを取得します。

※各端末の操作ログは 15 分間隔で収集（各端末から管理サーバへアップロード）します。

また、1 端末から収集する操作ログの容量は、MAX 1MB 程度となります。

※データ通信は、米国国立標準技術研究所（NIST）採用企画 AES 方式で暗号化しています。

項目	内容		
起動ログ	ユーザ ID	ログオンユーザ	部署名
	コンピュータ名	IP アドレス	MAC
	ドメイン名/ワークグループ	操作区分 ※1	実行時間
ログオンログ	ユーザ ID	ログオンユーザ	部署名
	コンピュータ名	IP アドレス	MAC
	ドメイン名/ワークグループ	操作区分 ※2	実行時間
Web 接続ログ	ユーザ ID	ログオンユーザ	部署名
	実行時間 ※3	開始時刻 ※3	終了時刻 ※3
	サイト名	サイト URL	ブラウザタイトル
	詳細 URL		
ソフトウェア操作 ログ	ユーザ ID	ログオンユーザ	部署名
	実行時間 ※3	開始時刻 ※3	終了時刻 ※3
	製品名	ファイル名	パス

	説明		
ファイル操作ログ	ユーザ ID	ログオンユーザ	部署名
	実行ファイル名	サイズ	作業区分 ※4
	元ファイルパス	元ファイル装置タイプ ※5	開始時刻
	ターゲットファイルパス	ターゲットファイル装置タイプ ※5	終了時刻
プリンタ出力ログ	ユーザ ID	ログオンユーザ	部署名
	プリンタ名	ファイル名	ページ
	スプールサイズ	開始時刻	終了時刻
外部装置監視ログ	ユーザ ID	ログオンユーザ	部署名
	ドライブ名	操作区分 ※6	装置タイプ ※7
	装置名	会社名	モデル
	操作時間		

※1 1:スタンバイモードの起動 2:スタンバイモードの停止 3:モニターオフ 4:モニターオン 5:バランス調整 6:高性能
7:節電 8:AC 電源供給 9:DC 電源供給 10:UPS 電源供給 11:バッテリー充電率 12:退席中モードの起動 13: 退席中モードの停止

※2 1:ログオン 2:ログオフ 3:Windows 起動 4:Windows 停止 5:スクリーンセーバースタート 6:スクリーンセーバーストップ 7:コンピュータロック 8:コンピュータロック解除 9:リモート接続 10:リモート切断

※3 開始時刻 = 接続を開始した時刻 終了時刻 = 接続を終了した時刻 接続開始から終了までの接続時間

※4 1:CREATE 2:DELETE 3:COPY 4:MOVE 5:RENAME 5:MODIFY

※5 0:NONE 1:HDD 2:FDD 3:REMOVAL 4:CD 5:REMOTE 6:RAMDISK 7:Portable Device

※6 1:Device Inserted 2:Device Removed 3:Device Exists

※7 1:USB 2:SATA 3:FileBackedVirtual 4:SCSI 5:ATA 6:ATAPI 7:IEEE1394 8:FIBRE
9:RAID 10:I-SCSI 11:SAS 12:SD 13:MMC 14:Virtual 15:UNKNOWN

3.3.6. 取得するインベントリ情報の種類

Agentを導入した Windows 端末から、以下のインベントリ情報を取得します。

※各端末のインベントリ情報は、1 時間間隔で前回収集情報との差分を収集（各端末から管理サーバへアップロード）します。

項目	内容		
ハードウェア情報	ユーザ ID	コンピュータ名	MAC アドレス
	部署名	項目 ※1	状態 ※2
	収集日付		
ソフトウェア情報	ユーザ ID	コンピュータ名	部署名
	製品名	会社名	バージョン
	状態 ※2	インストール日付	アップデート時刻
OS 情報 Windows アップ デート	ユーザ ID	コンピュータ名	部署名
	製品名	サービスパック/バージョン	収集日付
	セットアップ言語	Windows アップデート 名	関連情報
	種類 ※3	製品名	作成時刻

※1 1:プロセッサ 2:メモリ 3:ハードディスク 4:CD/DVD 5:LAN カード 6:ビデオカード 7:サウンドカード 8:モニタ
9:プリンター

※2 1:追加 2:削除 3:変更情報

※3 セキュリティ問題の修正プログラム

3.3.7. 操作ログの保管期間

Windows 端末から収集した操作ログは、最新(当日)から過去 90 日間分をサイクリックに最新化して保持します。

3.3.8. インベントリ情報の最新化と保管

対象端末から収集するインベントリ情報は、Agent 導入後の初回データ通信（対象端末から管理サーバへのアップロード）で収集した情報を起点に、以降更新があった差分データのみを定期的に自動アップロードし、最新のインベントリ情報として保持します。

3.3.9. 保管した操作ログの活用方法

対象端末から収集した過去 90 日間分の操作ログは、ヘルスチェックレポート生成時の基情報として、以下に示す視点で脆弱性観点、情報漏えいリスク観点で分析集計します。

項目	内容
起動ログ	いつ、誰(どのホスト)が、端末の電源を ON したか、他の端末からリモートデスクトップ (RDP) 接続されたか、切断されたかを確認することができます。
ログオンログ	いつ、誰(どのホスト)が、どのくらいの時間、ネットワークに接続していたかを確認することができます。
WEB 接続ログ	いつ、誰(どのホスト)が、どのくらいの時間、どの Web サイトに接続していたかを確認することができます。これにより悪意のある Web サイトや社内で禁止されている Web サイトへの接続有無を確認することができます。
ソフトウェア操作ログ	いつ、誰(どのホスト)が、どのくらいの時間、どのソフトウェアを起動して操作していたかを確認することができます。これにより情報漏えいに繋がるファイル交換ソフトの不正利用や、社内で許可されていないソフトウェアの利用などを確認することができます。
ファイル操作ログ	いつ、誰(どのホスト)が、どこに格納されていた、どのファイル进行操作(コピー持出し、ファイル名の変更、更新、削除)したかを確認することができます。これにより万が一情報漏えいが発生した際に、大元のファイルを起点に時系列に沿って証跡を確認することができます。
プリンタ出力ログ	いつ、誰(どのホスト)が、どのファイルを、どのネットワークプリンターで、何枚印刷したかを確認することができます。これにより万が一情報漏えいしたが発生した際に、大元のファイル名を基に紙ベースでの持出しを確認することができます。
外部装置接続ログ	いつ、誰(どのホスト)が、どの端末に、どのような外部記憶媒体 (USB メモリ、外部記憶媒体、光学メディアなど) を接続し、どのような操作をしたかを確認することができます。これにより万が一情報漏えいしたが発生した際に、大元のファイル名を基にデータ持出しを確認することができます。

3.4. ヘルスチェックレポート（月次）

3.4.1. ヘルスチェックレポートの内容

「ヘルスチェックレポート」には、対象端末にインストールされている Windows OS のバージョン、OS パッチの適用状況と共に、インストールされているアプリケーションの名称やバージョン情報が分類一覧化されています。これにより、Windows OS のパッチ未適用に起因する問題発生の可能性や障害発生、またサイバー攻撃を受けやすい脆弱性など、潜在的な問題を事前に特定することができます。

また、端末操作ログの中から、Web サイト接続ログや外部装置接続ログ、端末のログオンログなどから情報漏えいに繋がるリスクを可視化し、これらの結果及び統計データからコメントの付与と推奨対応策などを診断サマリとしてご提供します。

【サンプル】

ヘルスチェック（健康診断）サマリレポート



項目	結果	所見
OS脆弱性情報 Windowsアップデート情報		<p>管理対象端末4台の内、Windowsの緊急パッチ「Critical」が適用されていない端末が1台あります。 この端末に対するサイバー攻撃を踏み台として、企業全体・取引先へのリスク発生の可能性が高くなる為、早期のpatch適用を推奨します。 ※重要パッチ「Important」の適用推奨端末も3台あります。タイミングを回った適用を検討して下さい。 ※他の社内端末にもAgentを導入して調査可視化することを推奨します。</p> <p>緊急パッチ（Critical）：KB5025221＝特権昇格の脆弱性(CVE-2023-28252)、リモートコード実行の脆弱性(CVE-2023-28250、21554)の問題 ※リモートコードとは、攻撃者がインターネットなどのネットワークを通じてシステムや機器にアクセスし、悪意のあるコードを実行し、マルウェアの実行やシステムの乗っ取りなど、深刻な影響を与える危険性が有ります。</p>
ソフトウェア脆弱性情報 バージョン情報		<p>管理対象端末4台には、緊急「Critical」アップデートを必要とするような端末は有りませんが、最新化を推奨する高「High」レベルのソフトウェアが5つ存在します。最新Versionへのアップデートを検討して下さい。</p> <p>※脆弱性を有する古いVersionのソフトウェアを使用していると、不正なスクリプトの受信やSQLコマンドにより情報管理データベースが悪意のある第三者に操作される危険性が有ります。 ※メーラー：XXXXXXXXXXXXをインストールしている端末が有りますが、社内利用のメーラーを限定している場合はご確認下さい。</p>
記憶媒体接続注意情報 外部装置接続ログ		<p>「USBメモリスティック」の接続履歴が1件存在します。情報漏えいに繋がる記憶媒体の接続利用には注意が必要です。</p> <p>※その他、iPhoneを充電する為に接続したと思われる履歴が多数有ります。 iPhoneでもiTunesやAirdrop、icloudを使った情報転送は可能な為、PC接続による充電には注意が必要です。</p>
業務外・危険サイト接続確認 Webサイト接続ログ		<p>接続累計回数・接続累計時間ともに多く接続されているWebサイトは有りますが、全て業務に関する接続利用だと思われます。</p> <p>「不法（違法・著作権侵害・薬物利用など）に該当するサイト：0 「セキュリティ（マルウェア・フィッシング詐欺・DBD攻撃）に該当するサイト：0 「アダルト・フェティシズム」に該当するサイト：0 「出会い」に該当するサイト：0 「ギャンブル」に該当するサイト：0 「過激な表現（暴力組織・カルトなど）」に該当するサイト：0</p> <p>※一部、ゲーム関連サイトへの接続は見受けられるため、Webフィルタリングの検討や、コンピュータウイルスやハッキングなどの脅威から包括的にセキュリティ保護する統合脅威管理「UTM」などの導入を検討されることを推奨します。</p>
土日祝・深夜帯（22:00～5:00） ログオンログ（PC起動含む）		<p>2台の端末において、深夜帯での端末起動・ログオンが実行されています。 また、土日での端末起動・ログオンが多数見受けられます。</p> <p>※深夜帯での業務、および土日での出勤日など、社内規定や勤務表など、必要に応じて確認をしてみてください。</p>

【セキュリティYOROZU相談】

3.4.2. ヘルスチェックレポート項目（WindowsOS 脆弱性情報）

「Windows OS 脆弱性情報」は、対象端末にインストールされている Windows OS のセキュリティパッチ（KB）適用有無を確認し、適用されていない KB に内在するリスクを WSAS カタログと突合せを行う事で、脆弱性情報（Critical、Important、Medium、Low）として可視化します。

3.4.3. ヘルスチェックレポート項目（ソフトウェア脆弱性情報）

「ソフトウェア脆弱性情報」は、対象端末にインストールされている各種ソフトウェアのバージョンを基に、アップデート適用有無を確認し、適用されていないバージョンに内在するリスクを JVN の脅威情報と突合せを行う事で、脆弱性情報（Critical、High、Medium、Low）として可視化します。

3.4.4. ヘルスチェックレポート項目（外部装置接続状況）

「外部装置接続状況」は、対象端末の USB ポートなどに接続された外部機器のログを基に、情報漏えいに繋がる恐れのある記憶媒体（USB メモリスティック、外付けハードディスク、スマートデバイスなど）が接続利用された履歴を特定可視化します。

3.4.5. ヘルスチェックレポート項目（Web サイト接続閲覧状況）

「Web サイト接続閲覧状況 TOP30」は、対象端末で Web サイトへ接続したログを基に、サイトへの接続履歴を、接続累計時間・接続回数として集計し、業務に関係のない Web サイト閲覧や悪意のあるセキュリティリスクを伴う Web サイト接続を可視化します。

3.4.6. ヘルスチェックレポート（時間外 PC 端末使用状況）

「時間外 PC 端末使用状況」は、対象端末がログオンした履歴を基に、休日（土日祝）、および深夜帯（労働基準法で定められている 22 時～翌朝 5 時）に端末が起動・ログインされた実績を抽出し、就労時間外での隠れ残業や休日における端末の使用実態（在宅勤務時を含む）を企業内で確認することができるため、働き方改革や PC 端末の休日使用によるセキュリティリスク対策に活用できます。

3.4.7. ヘルスチェックレポートの送付方法

「ヘルスチェックレポート」は、毎月末（最終営業日）の最新情報を基に分類集計し、レポートに取り纏めます。お客様へのレポート提供は、ご準備が整い次第（翌月 5 営業日を目安に）、お客様へ準備完了通知メールをお送りすると共に、メール本文に記載する URL から当該ヘルスチェックレポートをダウンロードして頂きます。

3.5. Agent ライセンス追加（有償オプション）

3.5.1. Agent ライセンス追加

ご契約頂いたお客様に初期バンドルとして提供する Agent 衛生管理ツール 5 ライセンスを超えて追加で端末へインストールを希望される場合、有償オプションとしてライセンスを追加購入することができます。ライセンスの追加購入は、初期バンドルの 5 ライセンスとは別に、10 ライセンス以上から購入できます。

※例：追加 10 ライセンス以上は 1 ライセンスから加算できます（10 ライセンス、11～ライセンス）

3.6. Web フィルタリング（有償オプション）

3.6.1. Web フィルタリングの内容

Web フィルタリングは、業務に関係のない Web サイトや悪意のあるセキュリティリスクを伴う Web サイトへの接続アクションを、各種カテゴリに分類された脅威辞書と突合せを行うことで Web サイトへの接続許可、および接続拒否を実施するセキュリティ対策を有償オプションとしてご提供します。



3.6.2. Web フィルタリングのカテゴリ

本サービスは以下のカテゴリについてフィルタリングの対象とします。

不法	
違法と思われる行為	爆破予告、貯金通帳の売買、利用可能な携帯電話の売買など、インターネット上で情報の提供が違法とされる行為
著作権や商標権の侵害行為	著作権や商標権を侵害する可能性のある行為
児童ポルノ	18歳未満と思われる児童の性的な姿態や虐待などを写實的に描写したもの※1
違法と思われる薬物	違法薬物およびその利用を助長する情報※2
不適切な薬物利用	国内法では違法とされていない一般薬物の不適切な利用を助長する情報
自殺誘引	人を自殺に誘引・勧誘する情報

セキュリティ	
クラッキング	ウィルスの製造方法やネットワーク、コンピュータ、モバイル端末への不正侵入や不正使用に関連する情報
マルウェア	ウィルスやスパイウェア感染の恐れがあるサイト。 C&C（コマンド&コントロール）サーバーなどの不正攻撃サイト。※3
DBD攻撃	閲覧することにより、自動的にマルウェア（不正なプログラム）などをダウンロードさせられる恐れがあるサイト
フィッシング詐欺・ワンクリック詐欺	フィッシングサイトやクリックしただけで料金を請求される詐欺サイト※4
公開プロキシ	フィルタリング機能を回避する公開プロキシ
フィルタリング回避	フィルタリング機能を回避する目的ではないが、結果的にフィルタリング機能を回避してしまうサービス

アダルト・フェティシズム	
アダルト・ポルノ	性行為やヌードなど性的な描写、性風俗店、アダルトグッズ、アダルトゲームなどの情報
フェティシズム	身体や服装の一部分、または人間が身に付けるものに対する執着などいわゆるフェチの描写。盗撮とおもわれる画像や映像

出会い	
出会い	出会い系サイトや異性・同性の紹介、恋愛・交際を仲介するサービス

ギャンブル	
ギャンブル	競馬・オートレースなどの公営競技、カジノやその他ギャンブルに関わる情報。または金品などを対象に射幸心を煽るサービス
宝くじ・スポーツくじ	スポーツくじ・宝くじの販売や予想に関連する情報

過激な表現	
暴力組織・カルト	過激・暴力的な活動を行なう団体などの情報
グロテスク・ショッキング	拷問、虐待、傷害、暴行、死体、流血などの描写

※1：一般社団法人インターネットコンテンツセーフティ協会（ICSA）から児童ポルノのアドレスリストの提供を受け、該当するサイトを登録対象としております。

詳しくは一般社団法人インターネットコンテンツセーフティ協会のサイトを参照ください。

※2：一般的に合法（脱法）ドラッグと呼ばれるような指定薬物外で、所持・摂取・売買は禁止されていないが、麻薬と同様の効果を持つ類似薬物や物質も含まれます。

※3：管理者が意図せずウイルス感染しているサイトも含まれます。全てのウイルス感染サイトが網羅されているわけではありません。

3.6.3. Web フィルタリング時の表示画面

フィルタリング対象の Web サイトへ接続しようとした場合、以下の画面が表示されます。**サンプル画像**



3.6.4. Web フィルタリング対象の追加と削除

個別にフィルタリングする対象を追加（ブラックリスト登録）や、削除（ホワイトリスト登録）を希望される場合、月次で1回に限り、以下の方法で申請することができます。


※カテゴリ「不法」「セキュリティ」は、削除（ホワイトリスト）に指定することが出来ません。

※個別URLが多岐にわたる場合は、リストにてご提示ください。

フィルタリング追加・削除の連絡 → セキュリティ YOROZU 相談窓口へ、電話・Mail で連絡

セキュリティ YOROZU 相談窓口 → 申請書 → お客様で記載後、窓口に戻送して下さい。

フィルタリング対象の追加（ブラックリスト）、削除（ホワイトリスト）**申込書（サンプル）**

【セキュリティYOROZU相談】Webフィルタリング追加・削除申込書		
申込年月日	2023/	該当するカテゴリの追加・削除欄に「○」を選択して下さい。 
契約番号		
会社名		
申込者		
		削除 (White) 追加 (Black)
個別URL	http://	
個別URL	http://	
個別URL	http://	
個別URL	http://	
個別URL	http://	
※※個別URLの指定には、ワイルドカード「*」が利用できます。 例：*aaaa、aaaa* aa*aa		
アダルト・フェティシズム		
アダルト・ポルノ	性行為やヌードなど性的な描写、性風俗店、アダルトグッズ、アダルトゲームなどの情報	削除 (White)
フェティシズム	身体や服装の一部、または人間が身に付けるものに対する執着などいわゆるフェチの描写。盗撮とおもわれる画像や映像	
出会い		
出会い	出会い系サイトや異性・同性の紹介、恋愛・交際を仲介するサービス	
ギャンブル		
ギャンブル	競馬・オートレースなどの公営競技、カジノやその他ギャンブルに関わる情報。または金品などを対象に射幸心を煽るサービス	
宝くじ・スポーツくじ	スポーツくじ・宝くじの販売や予想に関連する情報	
過激な表現		
暴力組織・カルト	過激・暴力的な活動を行なう団体などの情報	
グロテスク・ショッキング	拷問、虐待、傷害、暴行、死体、流血などの描写	
※1：一般社団法人インターネットコンテンツセーフティ協会（ICSA）から児童ポルノのアドレスリストの提供を受け、該当するサイトを登録対象としております。詳しくは一般社団法人インターネットコンテンツセーフティ協会のサイトを参照ください。 ※2：一般的に合法（脱法）ドラッグと呼ばれるような指定薬物外で、所持・摂取・売買は禁止されていないが、麻薬と同様の効果を持つ類似薬物や物質も含まれます。 ※3：管理者が意図せずウイルス感染しているサイトも含まれます。全てのウイルス感染サイトが網羅されているわけではありません。		

3.7. 情報漏えいリスク診断（任意活用）

3.7.1. 情報漏えいリスク診断の内容

情報漏えいリスク診断は、お客様の任意のタイミング、または半年に1回を目安に社内における情報漏えいリスクの診断として積極的にご活用下さい。情報漏えいリスク診断は社内における外的要因リスクと内的要因リスクの両面から簡易的に診断し、リスク度の総合評価と共に、内的・外的要因に対する推奨対策をアドバイスします。

診断結果



情報漏えい発生リスク	66.8pt	リスクレベル	E
情報漏えい pt	リスクレベル	推奨事項	
75~100	F	重大な被害が発生する可能性が極めて高く、早急な脆弱性の特定と対策が必須	
60~74.9	E	重大な被害が発生する可能性が高く、早急な脆弱性の特定と対策が必要	
40~59.9	D	重大な被害がいつ発生してもおかしくない、脆弱性の特定と見直し検討が必要	
25~39.9	C	重大な被害がいつ発生してもおかしくない、脆弱性の特定と見直し検討が必要	
10~24.9	B	危険度は低いが、将来的な危険性を認識するための脆弱性の特定を推奨	
0~9.9	A	危険度は低い、現状問題が生じる可能性は低い。効果維持の継続が必要	

3.7.2. 利用方法

情報漏えいリスク診断を活用される場合、セキュリティ YOROZU 相談窓口にご連絡して頂くことで診断用のヒアリングポータル URL をメールでご連絡致します。受け取った URL にアクセスし、全 11 問の設問フォームより回答を入力して下さい。

ヒアリングポータル URL はこちら：<https://forms.office.com/r/kaAjvwNu2R>



4. 前提条件・制限事項

3.7.3. 診断書の送付方法

「情報漏えいリスク診断レポート」は、全 11 問の設問フォームより回答を入力頂いた後、診断結果としてレポートに取り纏めます。お客様へのレポート提供は、ご準備が整い次第（5 営業日後を目安に）、お客様へ準備完了通知メールをお送りすると共に、メール本文に記載する URL から情報漏えいリスク診断レポートをダウンロードして頂きます。

3.8. セキュリティチケット（個別見積り）

3.8.1. セキュリティチケットの内容

セキュリティチケットは、お客様からの相談事に対し、個別での支援対応をご依頼頂く場合に、個別見積り内容に沿ってご購入頂くチケットとなります。

4.1. 前提条件・制限事項

4.1.1. 前提条件・制限事項

- ・サービスをご利用頂けるエリアは、「日本国内の法人」が前提となります。
- ・サービス提供に用いる言語は「日本語」が前提となります。
- ・ヘルスチェックレポートをご利用頂く場合、Windows 端末に Agent 衛生管理ツールをインストールして頂く事が前提となります。
- ・ヘルスチェックレポートの提供は、月次提供（当月末〆、翌月 5 営業日までを目安に）となります。
- ・情報漏えいリスク診断レポートは、全 11 問に回答後、5 営業日後までを目安に提供します。
- ・Agent 衛生管理ツールを活用した各種サービスは、Windows OS の端末が前提となります。
- ・Agent 衛生管理ツールのご利用（インストール）は、他社製 IT 資産管理ツール未導入の端末が前提となります。※他社製資産管理ツールの例：SkySea、LANScope、AssetView など

改版履歴

バージョン	改版内容	日付
1.0	初版	2023/8/28
1.1	内容の修正	2023/12/27
1.2	内容の修正	2024/2/1
1.3	サービス名称変更/注意事項文言の修正	2024/2/20