DarkWebCheck

ユーザーマニュアル

文書バージョン 1.0.0

最終修正日 2025-2-14

JSecurity
All for Japan Security

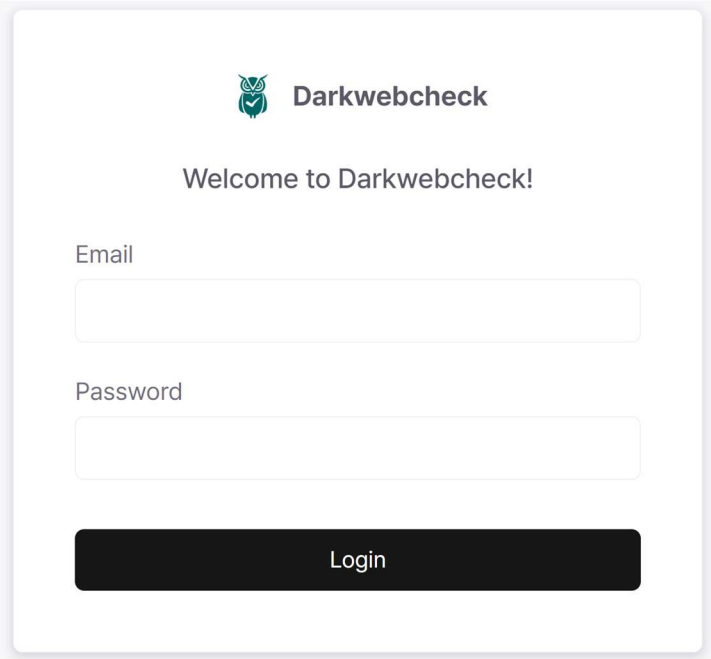
目次

1.　ダッシュボードマニュアル

1.1. ダッシュボードログイン

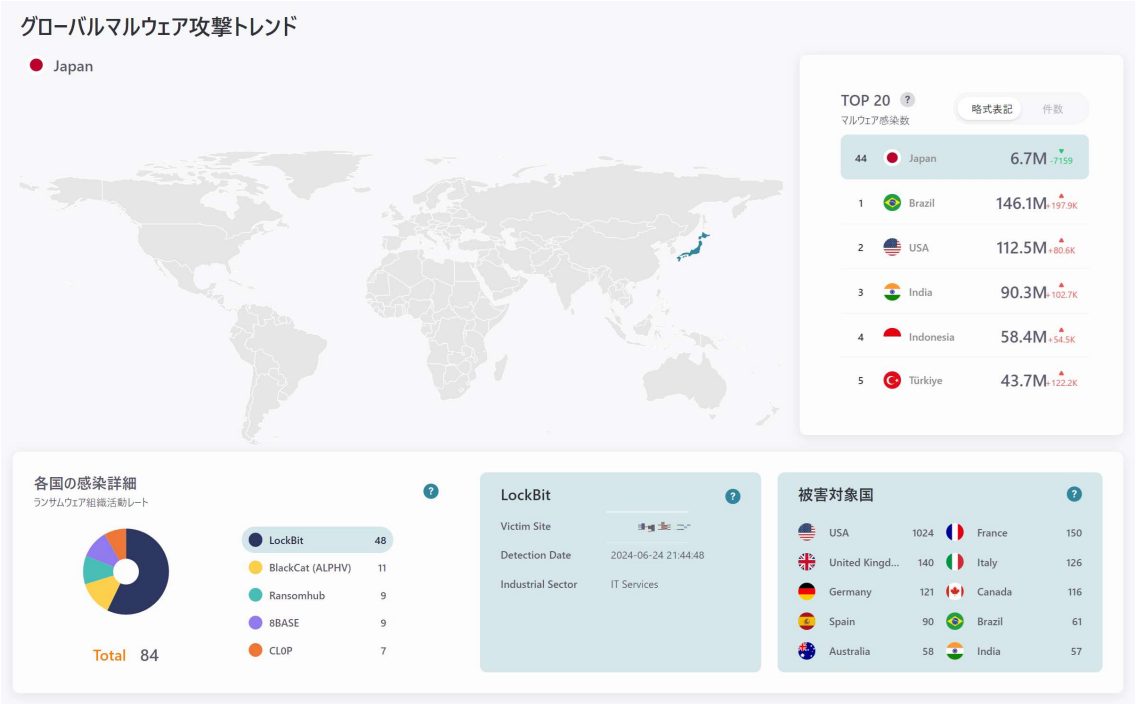
A)　ウェブブラウザから「dashboard.darkwebcheck.jp」へアクセス

B)　ID/パスワードを入力してログイン

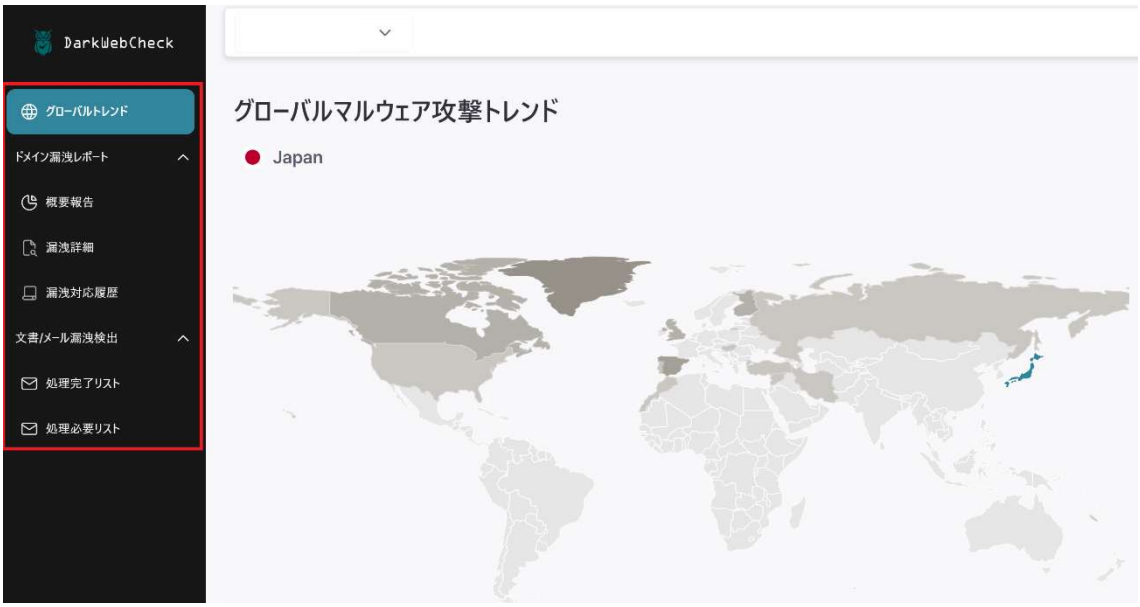


1.2. ダッシュボード (グローバルトレンド)

世界中で進行中のサイバー攻撃グループの攻撃状況について分析情報を見ることができます。



A) **左段メニュー** ： 選択したメニューに移動します。

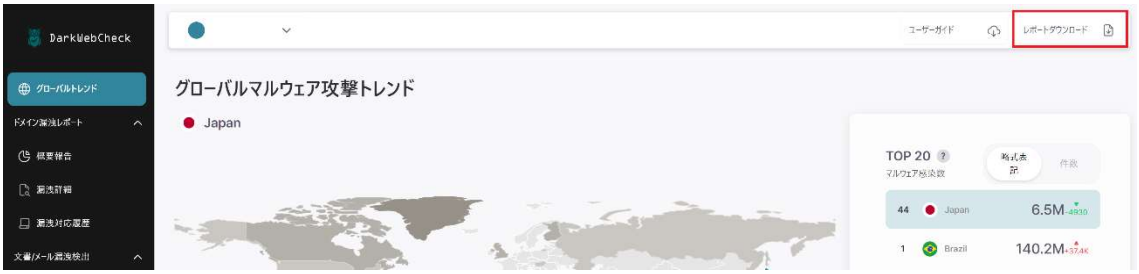


B) **左下メニュー** ： 言語設定を変更します。

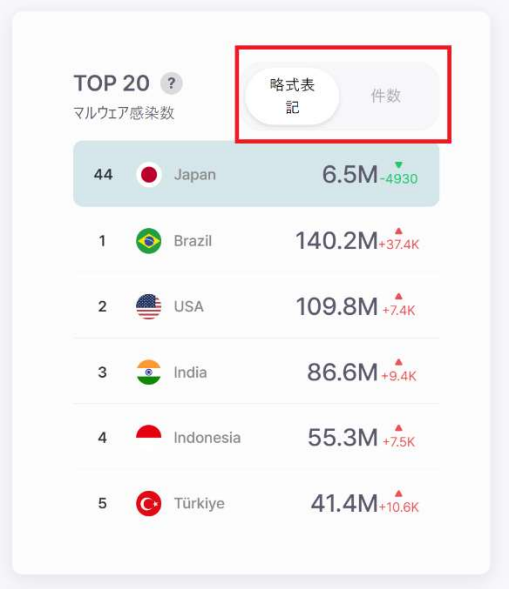
C) **ドメイン選択/ログアウトプルダウン** ： 対象のドメインを選択/ログアウトします。

D) **ユーザーガイド** ： ユーザーマニュアルをダウンロードします。

E) **レポートダウンロード** ： レポートをダウンロードします。レポートの詳細については「1.9 レポート」の項をご参照ください。



F) **TOP 20** ： 世界中で発生しているマルウェア攻撃のケースをまとめて、上位 20 カ国の攻撃状況情報とユーザーの国に関する状況情報を表示します。詳細を表示したい国をクリックすると、下のエリアにアクティビティ分析情報が表示されます。



赤枠のトグルボタンより「略式表記」と「件数(精算表示)」を切り替えることができます。

G) **各国の感染詳細** ： F) の「**TOP 20**」で選択された国で活動しているサイバー攻撃グループの状況を分析して表示します。

(1) 各国の感染詳細 ： 選択した国で発生した攻撃をサイバー攻撃グループ別に分類し、攻撃率を表示します。

(2) (1) で選択したランサムウェア組織の最新の攻撃対象情報です。

(3) 被害対象国 ： (1) で選択したランサムウェア組織のターゲットとなった国のリストと各国の被攻撃件数を表示します。

1.3. 概要報告

ダッシュボードを使用して企業内の独自のセキュリティ状態をすばやく把握し、効率的に対応計画を立てることができるように、ダークウェブ監視情報を分析して各種情報を表示します。

A) **全体漏洩件数** ：

対象ドメイン全体の漏洩件数が確認できます。

見出しはそれぞれ以下の件数を表示しています。

・アカウント漏洩 ：漏洩が確認できたユーザーのアカウント件数

・E メール漏洩 ：漏洩が確認できた E メールアドレスの件数

・ドキュメント漏洩 ：漏洩が確認できたドキュメントの件数

・感染したデバイス ：マルウェア感染による漏洩が確認できたデバイスの件数

B) **リスクスコアレベル** ： 漏洩時点、パスワードの過去の変更履歴など、ダークウェブに情報漏洩があった企業の内部情報を総合的に分析します。計算されたリスク情報漏洩レベルの値に基づいて、情報漏洩レベルを段階的に表現します。これにより、事後対応を通じて追加的な攻撃被害を防ぐことがで

きます。

緊急

・Info stealer のようなマルウェアに感染した端末がある恐れがあります。システムとデータを調査し、その他の漏洩がないかどうか確認の上、全ての認証情報を変更または削除する必要があります。

注意

・情報漏えいやデータベースハッキングより、アカウント情報、文書、電子メールなどの情報がダークウェブやディープウェブに流出している恐れがあります。

安全

・認証情報の漏洩やマルウェア感染などの異常な動作が検出されていない状態、または過去の情報漏洩について対応し終えている安全な状態です。

C) **社員アカウントの漏洩** ： モニタリングによって検出された企業内情報漏洩をまとめて示します。毎日午前中に収集された情報を分析して新規に漏洩した情報かどうかを整理し、管理者が対応を進めた漏洩件、被害ユーザーが対応完了した処理完了件数を分類して表示します。該当件を押すと、その件数を詳細に集めて確認することができます。
漏洩が確認されたアカウントの情報と対応状況が表示されます。
各ステータスのアイコンをクリックすると、詳細情報を示すページへ遷移します。

新規あるいは未対応の漏洩アカウント件数です。

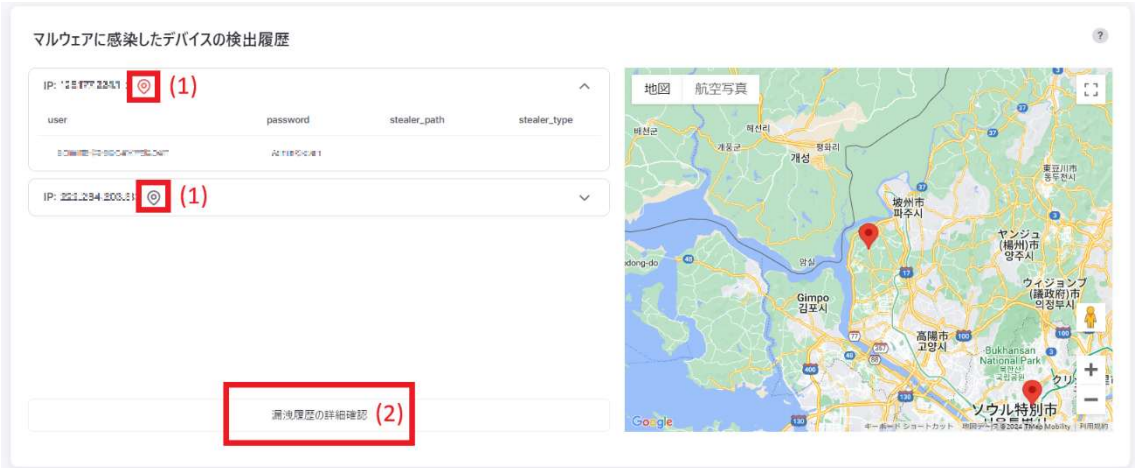
現在対応中の漏洩アカウント件数です。

対応済みの漏洩アカウント件数です。

D) **ウェブカレンダー**

DarkWebCheck からの主要なお知らせが表示されるカレンダーです。カレンダーの日付をクリックすると各漏洩タイプの対応履歴と対応状況がウィンドウ右側に表示されます。

E) **マルウェアに感染したデバイスの検出履歴**



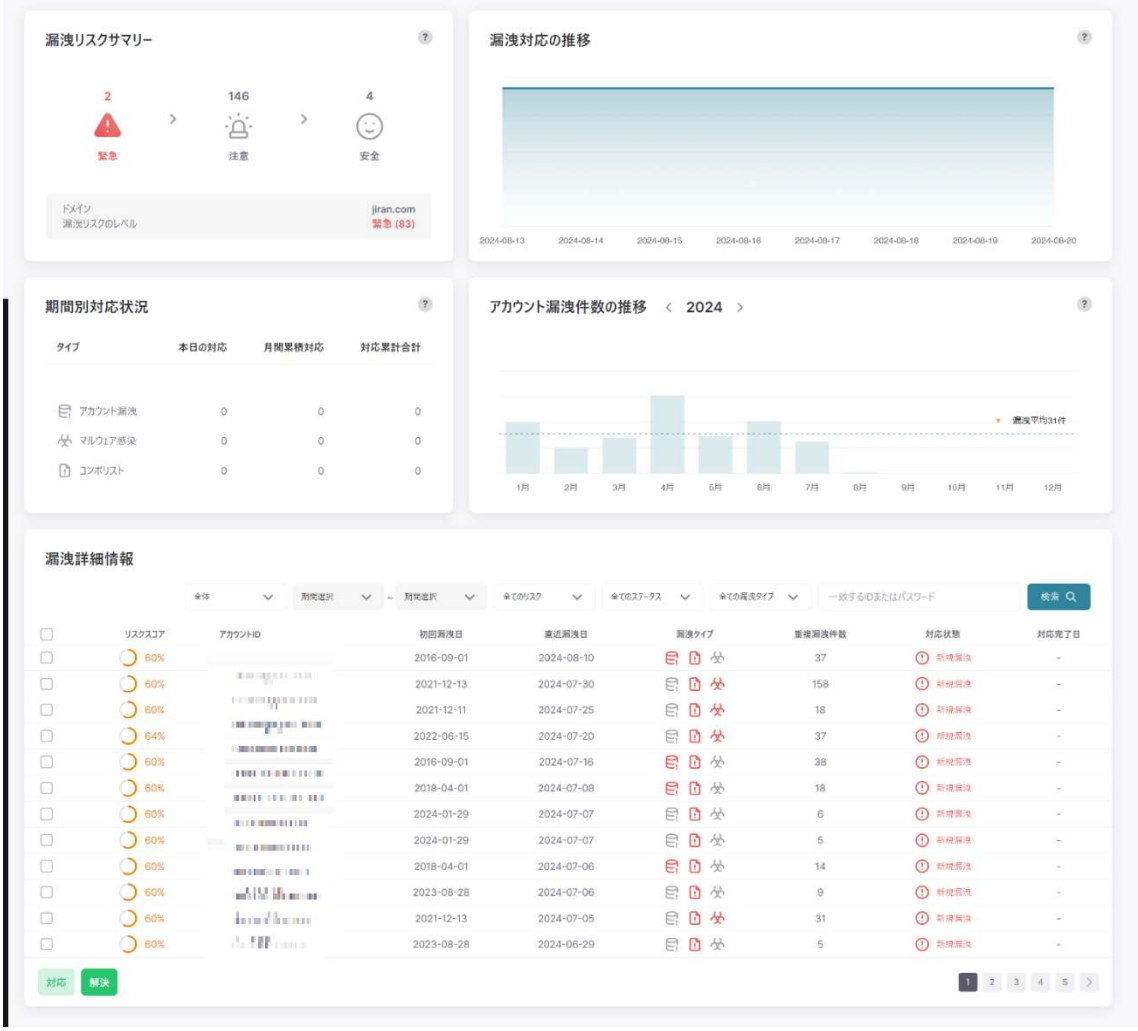
組織内のデバイスがマルウェアに感染した場合、そのデバイスの場所と、マルウェアが保存されているパス(stealer_path)が表示されます。

(1) の位置情報アイコンをクリックすると右側のマップウィンドウで対象の場所が拡大表示されます。

(2) の「漏洩履歴の詳細確認」をクリックすると「漏洩詳細」の画面へ遷移し漏洩への対処が可能です。各対処の操作については「漏洩詳細」の項をご参考ください。

1.4. 漏洩詳細

漏洩詳細履歴メニューでは、実際にドメインの漏洩事故に対応する管理者が対応できる機能が集約されています。



A) **漏洩リスクサマリー**： 漏洩リスクレベルで表される緊急度は、現在選択されているドメイン漏洩件数の平均リスクレベルを意味します。各アイコンをクリックすると画面下部の「漏洩詳細情報」のウィンドウに各リスクのリストが表示されます。

緊急

Info stealer などのマルウェアに感染したデバイスが存在する恐れがあります。漏洩した情報は悪用される恐れがあるため至急対応する必要があります。セキュリティ担当者は組織の全システムとデータを調査し、さらなる漏洩がないかの確認を行い、すべての認証情報を変更または廃棄する必要があります。

注意

情報漏洩やデータベースハッキングより、ダークウェブやディープウェブにアカウント情報、ドキュメント、E メールなどの情報が流出しています。これにより、アカウントへの不正アクセスや個人情報の不正利用の恐れがあります。

安全

漏洩された認証情報やマルウェア感染などの異常な動作が検出されていない、または過去に漏洩した情報への対応が完了している、安全な状態です。

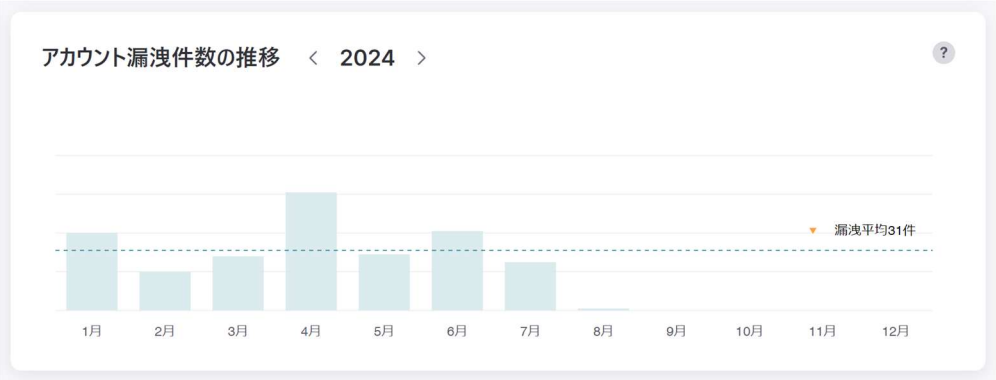
B) **漏洩対応の推移**

アカウントの漏洩/マルウェア感染/コンボ(ID とパスワードのペア)の漏洩に対応した履歴の状況を過去 1 週間分まとめて表示できます。

C) **期間別対応状況**

「漏洩詳細情報」のページで対処を行った各インシデントの対応履歴が確認できます。
各インシデントタイプ別に当日/当月/累計の対応数をそれぞれ示しています。

D) **アカウント漏洩件数の推移**



対象のドメインにおける年度ごとの各月漏洩被害件数と年間平均漏洩件数を示しています。

E) **漏洩詳細情報**

管理者は、対応メニューを通じて企業内の漏洩被害者に対する措置を通知することができます。

(1) インシデントの検索期間を指定します。「全体」では全期間が対象となり「直接入力」では右側プルダウンより期間を指定いただけます。

(2) インシデントのリスクレベルを指定します。「リスクレベル全体」では全レベルが対象となります。

(3) インシデントの対応状態を指定します。「対応段階全体」では全状態が対象となります。

(4) インシデントの漏洩タイプを指定します。「漏洩タイプ全体」では全てのタイプが対象となります。

(5) アカウント名の語句検索ができます。

(6) 「対応」を押下すると選択したインシデントについて DarkWebCheck へ対応リクエストが

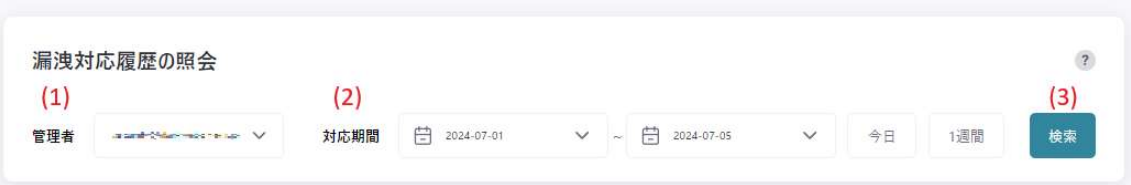
送付され、DarkWebCheck 内部の担当者による対処が行われます。「解決」を押下すると選択したインシデントは「解決済み」ステータスへ変更されます。

1.5. 漏洩対応履歴

対象のドメインの漏洩への対応履歴が確認できます。

A) **漏洩対応履歴の照会**

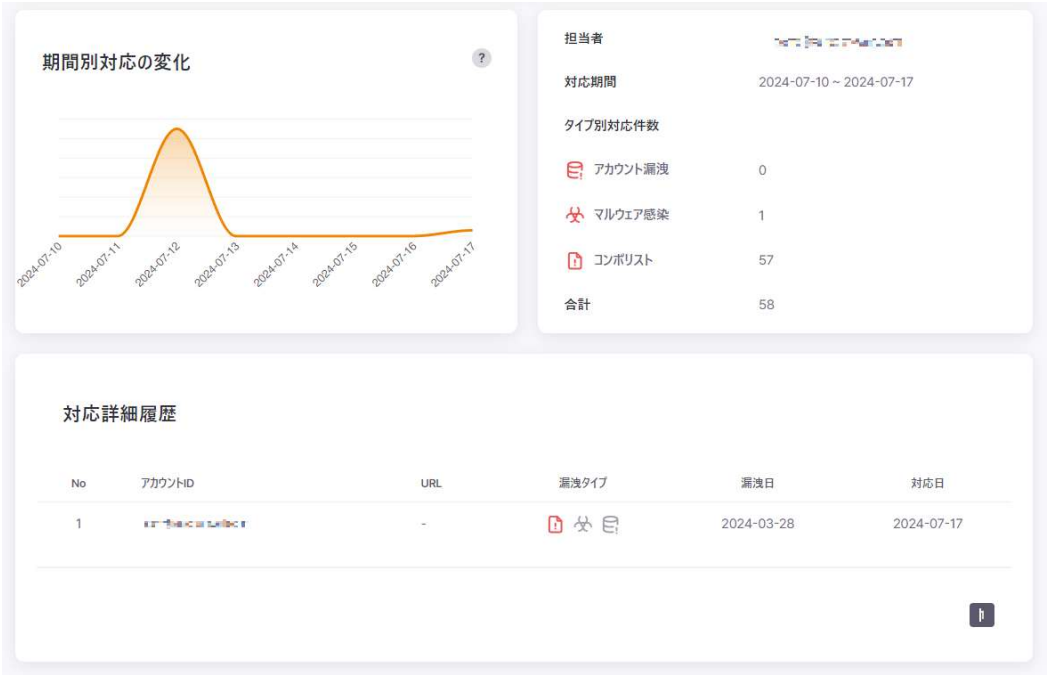
ドメインごと、期間ごとに管理者が対応した漏洩件数の詳細を確認できます。



(1) 管理者　　：対象ドメインを選択します。
(2) 対応期間　　：検索対象の期間を入力します。
(3) 検索　　：(1) (2)で設定した条件で検索を行います。
検索結果は以下「B) **期間別対応の変化/対応詳細履歴**」に表示されます。

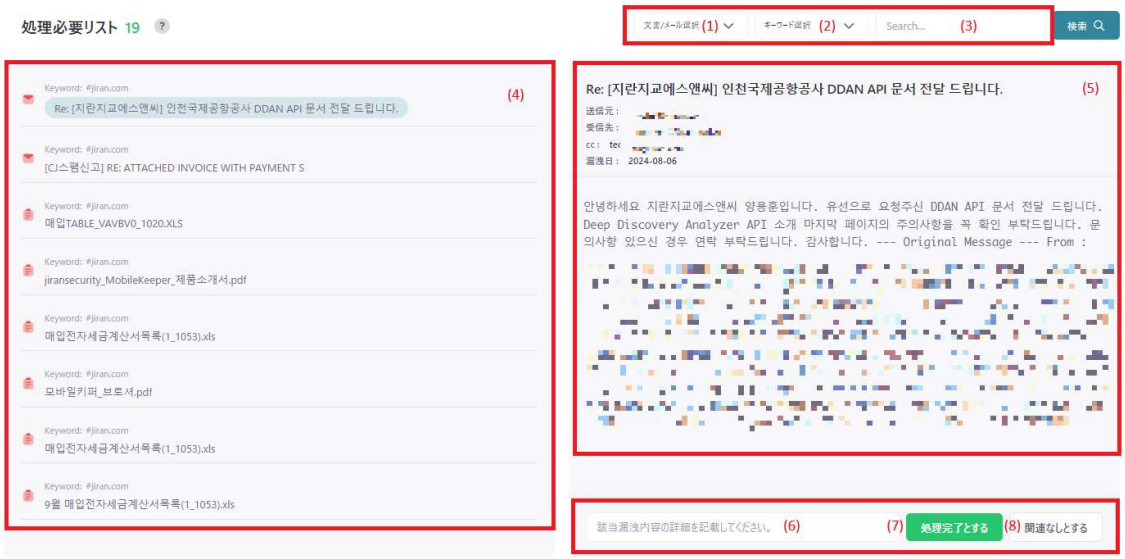
B) **期間別対応の変化/対応詳細履歴**

「A) **漏洩対応履歴の照会**」で設定したドメインと期間において、管理者が何件の漏洩件数に対応したかについてのグラフおよび統計情報を確認できます。



1.6. 処理必要リスト

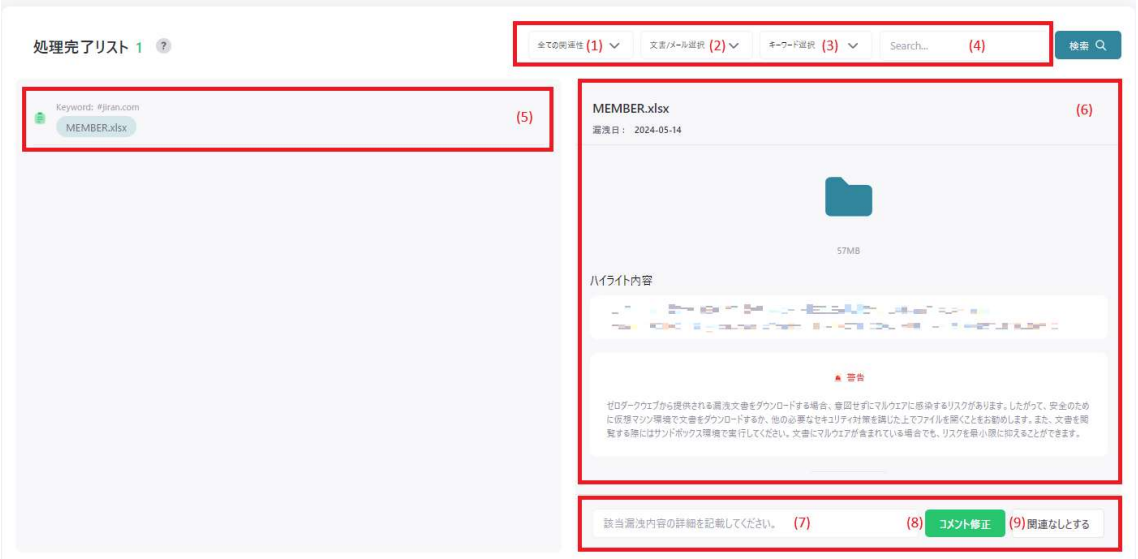
管理者が流出したメールや文書を確認し、機密情報が含まれているかを確認して、適切な対応措置を取るためのメニューです。このメニューを通じて、管理者は流出した情報の重大性を評価し、必要に応じて追加調査を依頼したり、セキュリティ強化のための措置を実施したりすることができます。



(1) プルダウンから文書/メールのフィルタリングができます。
(2) プルダウンからキーワードを選択しフィルタリングができます。
(3) キーワードを入力し検索することができます。
(4) 処理が必要な漏洩のリストが表示されます。
(5) (4)でクリックした漏洩の詳細が表示されます。
(6) 漏洩内容の詳細などに関するメモを保存いただけます。
(7) 対象の漏洩が「処理完了」のステータスとなり「処理完了リスト」へ移動します。
(8) 対象の漏洩が「関連なし」のステータスとなり「処理完了リスト」へ移動します。

1.7. 処理完了リスト

漏洩したメールや文書に対するレビューと必要な対応措置が完了した項目がリスト表示されます。このメニューを通じて、管理者はすべてのレビューおよび対応が完了した流出事件を追跡し、その処理状況を把握し、将来同様の事件が発生した場合に参考にすることができます。



(1) プルダウンから関連性の有無のフィルタリングができます。
(2) プルダウンから文書/メールのフィルタリングができます。
(3) プルダウンからキーワードを選択しフィルタリングができます。
(4) キーワードを入力し検索することができます。
(5) 処理が完了した漏洩のリストが表示されます。
(6) (5)でクリックした漏洩の詳細が表示されます。
(7) 漏洩内容の詳細などに関するメモを保存いただけます。
(8) (7)で入力いただいたメモを保存します。
(9) 対象の漏洩が「関連なし」のステータスとなります。

1.8. レポート

以下赤枠の箇所よりドメインごとのレポートをダウンロードいただけます。

(1) 過去から当日までの全期間を選択します。
(2) レポートの対象期間を設定します。
(3) レポートの対象ドメインを設定します。
(4) ダウンロード形式を CSV、PDF から選択します。

CSV 形式のレポート

CSV 形式のレポートの各見出しの定義は以下の通りです。

TYPE	インシデントタイプを表示します。 CL (Credential Lookout) は「アカウント漏洩」を、CB (Combo Binder) は「コンボリスト」を、CDS (Compromised Data Set) は「マルウェア感染」を意味しています。
HOST	漏洩した ID/PW でログイン可能なサービスの URL を表示します。

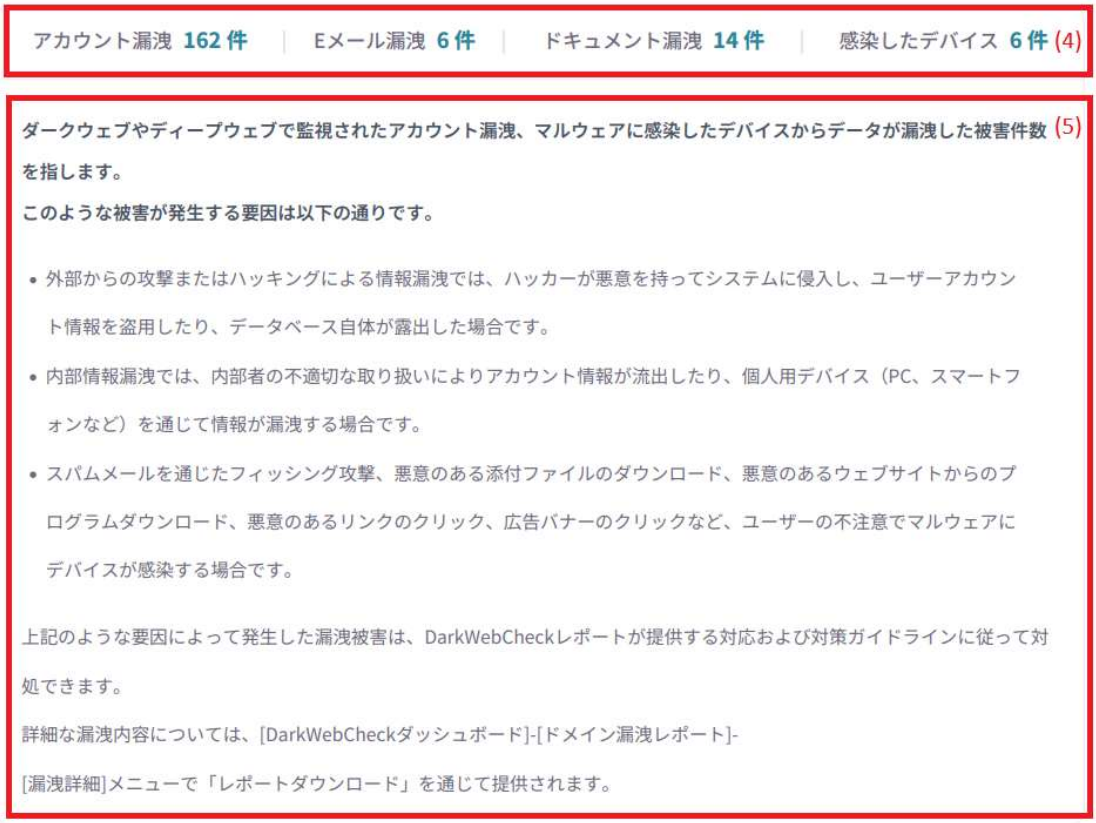
	マルウェア感染による漏洩の場合に表示されます。
user	情報が漏洩したユーザーID を表示します。
domain	漏洩が発生した契約ドメイン名が表示されます。
leaked_from	漏洩元のソースや場所を表示します。
leaked_date	漏洩が発生した日付を表示します。
ip	対象の IP アドレスを表示します。 マルウェア感染による漏洩の場合に表示されます。
username	コンピュータにログインする際に設定されたユーザー名を表示します。 マルウェア感染による漏洩の場合に表示されます。
computername	対象のコンピュータ名を表示します。 マルウェア感染による漏洩の場合に表示されます。
password	漏洩したパスワードを表示します。

PDF 形式のレポート

(1) リスクスコアレベルとスコアの数値を表示します。リスクスコアレベルは「緊急」、「注意」、「安全」に分かれており、「緊急」はスコア 76~100、「注意」は 17~75、「安全」は 1~16 のスコアに該当し、スコアは漏洩されたアカウントのリスクとドキュメントやメールの漏洩有無に基づいて計算されます。

(2) 登録されている会社名、対象ドメイン、直近の漏洩日が表示されます。

(3) 検知内容に基づいて、被害状況や対処方法に関する総評が表示されます。



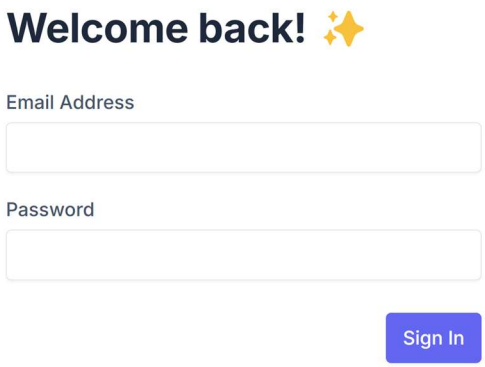
(4) 漏洩内容ごとに件数が表示されます。
(5) (4) の漏洩が発生する要因および対策が表示されます。

2. 管理画面マニュアル

2.1. ダッシュボードログイン

A) ウェブブラウザから「backoffice.darkwebcheck.jp」へアクセス

B) ID/パスワードを入力してログイン



2.2. 管理画面

A) 左段メニュー

選択したメニューへ移動します。

B) 言語設定

KOR(韓国語)、JPN(日本語)、ENG(英語)への変更が可能です。

C) ログイン情報

ログインアカウント情報の確認、およびサインアウトを行うことができます。

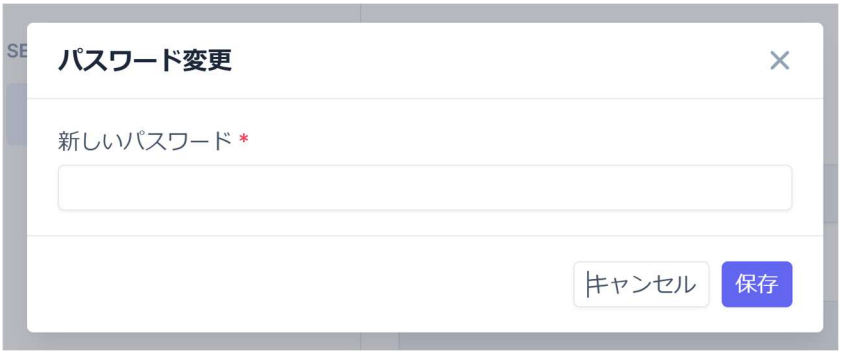
2.3. マイページ

(1) 基本情報

登録を行っている ID 名および名前が表示されます。

(2) パスワード

設定したパスワードのリセットを行うことができます。



2.4. 私の会社

(1) 会社名からフィルタリングを行うことができます。

(2) ID、会社名、従業員数、作成日(会社情報登録日)がご確認いただけます。

(3) 「アクション」のアイコンを押下いただくと、以下「会社詳細情報」のページへ遷移します。

(1)　基本情報

会社名および従業員数が表示され、従業員数に関しては数値の変更、保存ができるようになっています。

(2)　ドメイン

追加したドメインのリストおよび検査対象とするキーワードをご確認いただけます。
また赤枠の「アクション」のアイコン>「キーワード追加」を押下いただくと、監視対象のキーワードを新規追加いただけます。

(3)　　業界

2.5. ドメイン管理者リスト

ドメイン管理者およびそのプロパティ情報をご確認いただけます。

(1) ユーザー作成

「ユーザー作成」のボタンを押下すると新規管理者作成のための情報入力画面へ遷移します。

(2) アクション

アクション列の編集ボタンを押下すると対象の管理者のプロパティ情報の編集画面に遷移します。

■基本情報

対象の管理者の基本情報の確認、変更が行えます。

＜基本情報＞

・ログイン有効化

対象の管理者のログイン可否をご設定いただけます。

＜パスワード＞

・パスワードリセット

対象の管理者のパスワードを再設定いただけます。

■会社

対象の管理者の会社情報の確認、変更が行えます。

＜所属会社＞

・会社作成

対象の管理者の所属会社を設定いただけます。

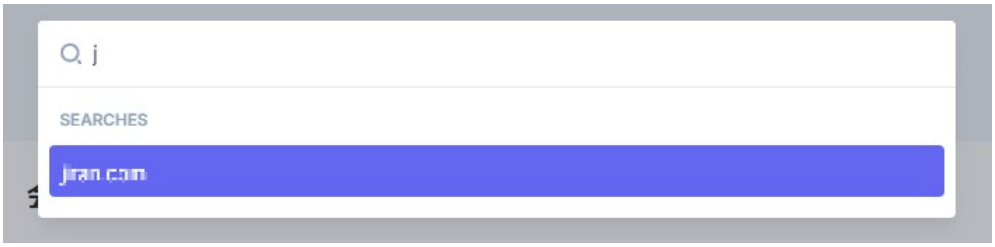
・アクション

編集ボタンを押下すると下部の「ドメイン」欄でドメインの追加、削除が行え、削除ボタンを押下すると所属会社を削除いただけます。

＜ドメイン＞

・ドメイン追加

「所属会社」の項目で選択中の会社に対しドメインを割り当てることができます。



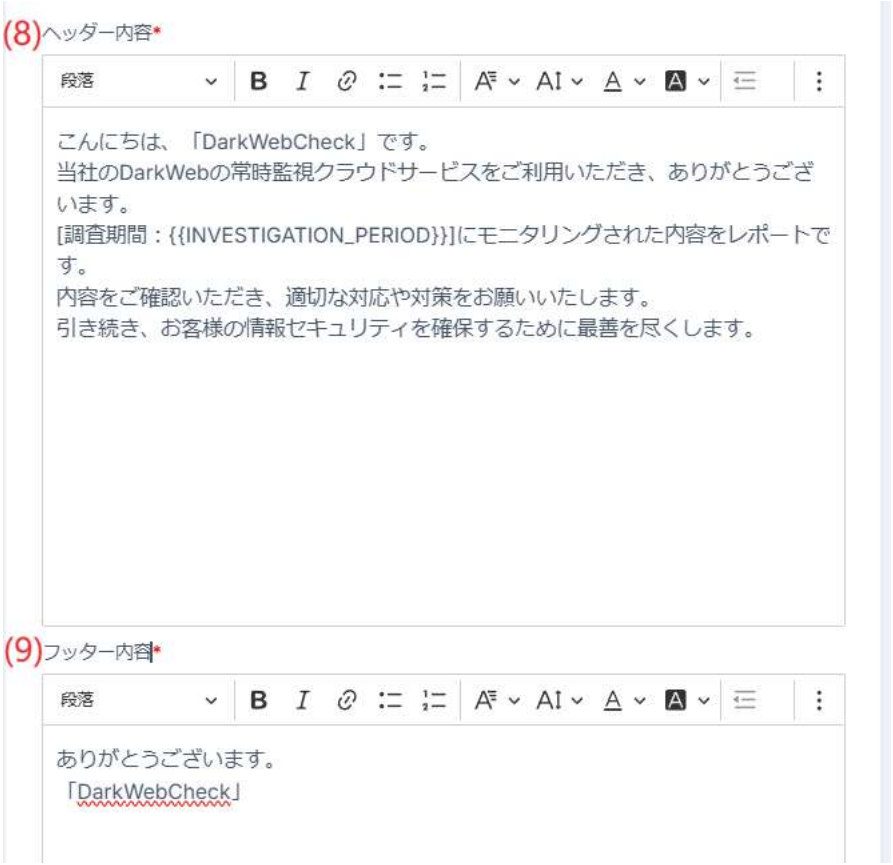
・アクション
ゴミ箱ボタンを押下いただくと「所属会社」の項目で選択中の会社からドメインの割当を解除することができます。

2.6. 定期レポートリスト

定期レポートの作成、および作成した定期レポートの確認が可能です。

・定期レポート生成
新規定期レポートの作成画面に遷移します。


テンプレート
(1)
韓国語
英語
日本語
調査期間設定*
(2)
毎週
月
ドメインユーザー*
(3)
cc
(4)
追加
No Data
(5)ドメイン*
レポート送信時は国家コードに基づいた言語で送信されます。
(6)タイトル*
「DarkWebCheck」定期レポート
(7)変数リスト
• {{INVESTIGATION_PERIOD}} → INVESTIGATION PERIOD



(1) 各言語ごとのテンプレートを選択します。
(2) 調査期間を指定します。
(3) ドメインユーザーを指定します。
(4) レポートの CC を指定します。
(5) レポートの対象となるドメインを指定します。
(6) レポートのタイトルを指定します。
(7) 下記(8)、(9)のヘッダー、フッター内で使用可能な編集が表示されます。
(8) レポートに挿入するヘッダーが入力できます。
(9) レポートに挿入するフッターが入力できます。

・アクション

編集ボタンで対象のレポートの編集、ゴミ箱ボタンで削除がそれぞれ可能です。

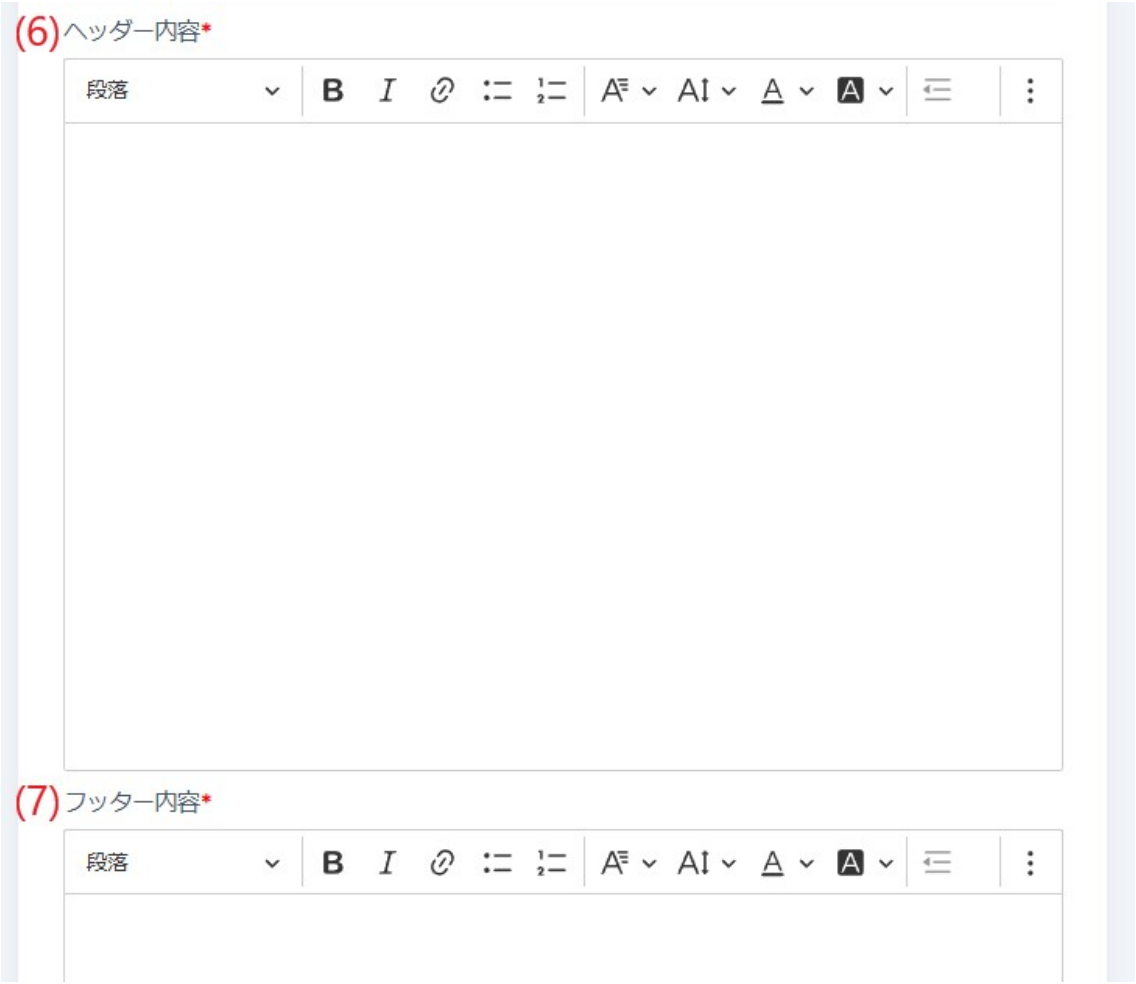
編集メニューの各項目は上記「定期レポート生成」と同様です。

2.7. 緊急レポートリスト

緊急レポートの作成、および作成した定期レポートの確認が可能です。

・緊急レポート生成

新規緊急レポートの作成画面に遷移します。



(1) 各言語ごとのテンプレートを選択します。
(2) ドメインユーザーを指定します。
(3) レポートの CC を指定します。
(4) レポートの対象となるドメインを指定します。
(5) レポートのタイトルを指定します。
(6) レポートに挿入するヘッダーが入力できます。
(7) レポートに挿入するフッターが入力できます。

・アクション
編集ボタンで対象のレポートの編集、ゴミ箱ボタンで削除がそれぞれ可能です。
編集メニューの各項目は上記「緊急レポート生成」と同様です。

3. 対策ガイドライン

DarkWebCheck における各漏洩タイプ別の対策ガイドラインは以下の通りです。

■ **漏洩タイプ：アカウント漏洩、コンボリスト**

- 漏洩した ID のパスワードを新しく設定する必要があります。
  - 最低 8 文字以上大文字、小文字と一緒に数字、特殊文字を使用し、複雑なパスワードを使用する必要があります。
  - すでに漏洩したパスワードは再び漏洩する可能性が高いです。これまで使用したことのないパスワードへ変更する必要があります。
- すでに漏洩したパスワードが再度漏洩した場合

  一度でも漏洩したパスワードは、ハッカーの間で伝播され共有され続けます。

  既に変更措置を取ったパスワードであっても、定期的に変更することをお勧めします。

  必ず、これまで使用したことのないパスワードを使用してください。

■ **漏洩タイプ：Infostealer**

- PC にインストールされているマルウェアを削除する必要があります。
  - 「漏洩詳細」のページの[Stealer_path]の項に表示される、マルウェアがインストールされたパスを確認します。
  - ウイルス対策ソフト等を使用してマルウェアを削除します。（ウイルス対策プログラムと OS の最新化は必須になります。）
  - 必要に応じて組織のセキュリティ担当者とマルウェアに対応してください。
- 漏洩した ID のパスワードを新しく設定する必要があります。
  - 少なくとも 8 文字以上の大文字、小文字とともに数字、特殊文字を使用して複雑なパスワードを使用する必要があります。
  - 一度漏洩したパスワードは再び漏洩する可能性が高いです。これまで使用したことのないパスワードを使用する必要があります。
- 予防措置
  - 怪しい URL へ接続しないようにする
    - 接続が必要な場合は事前に安全確認を行う

      → Google 透明性レポート
  - 開発元が不明な怪しいソフトウェアを使用しない
  - OS とソフトウェアを常に最新の状態に保つ
  - ウイルス対策プログラムを使用し、定期的に更新する


JSecurity
All for Japan Security