

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



目次

1.	ダッ	シュボードマニュアル 4
1.	1.	ダ ッシュボードログイン4
1.	2.	ダッシュボード (グローバルトレンド) 5
1.	3.	概要報告
1.	4.	漏洩詳細 11
1.	5.	漏洩対応履歴 15
1.	6.	処理必要リスト
1.	7.	処理完了リスト 16
1.	8.	レポート17
	CSV	形式のレポート 18
	PDF	形式のレポート 19
2.	管理画	回面マニュアル
2.	1.	ダッシュボードログイン 20
2.	2.	管理画面 21
2.	3.	マイ ページ22
2.	4.	私の会社
	(1)	基本情報

(2)	ドメイン	25
(3)	業界	26
2.5	5.	ドメイン管理者リスト	26
(1)	ユーザー作成	26
(2)	アクション	27
2.6	5 .	定期レポートリスト	30
2.7	' .	緊急レポートリスト	32
3. 🖈	対策力	ゴイドライン	35

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「<u>dashboard.darkwebcheck.jp</u>」へアクセス
- B) ID/パスワードを入力してログイン

	Welcome to Darkwebch	eck!
Email		
Dasswor	4	
1 033000	A	

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。

👸 DarkWebCheck	Y
⑦ローバルトレンド	グローバルマルウェア攻撃トレンド
ドメイン漏洩レポート ヘ	Japan
(概要報告	
[2] 漏洩詳細	
🛄 漏洩対応履歴	
文書/メール漏洩検出 ヘ	
▶ 処理完了リスト	
🖸 処理必要リスト	

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。

🎽 DarkWebCheck	
	Critical ▲ ア攻撃トレンド
ドメイン漏洩レポート ヘ	Japan
🕒 概要報告	
[] 漏洩詳細	

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。

🦉 DarkWebCheck	• ×	ユーザーガイド	
⊕ 20-лингок	グローバルマルウェア攻撃トレンド		
ドメイン深法レポート	Japan		
④ 根要報告		TOP 20 👔	站式表 件款
C 原皮訂編		イルウェア感染液	μ
□ 漏決対応履歴	in the second	44 🕒 Japan	6.5M-4830
文書/メール環境検出 へ	A A A A A A A A A A A A A A A A A A A	1 📀 Brazil	140.2M+37.48

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「<u>1.9 レポート</u>」の 項をご参照ください。

🦉 DarkWebCheck		ב-₩-₩/¥ Φ L₩-₽9720-¥ D
⊕ 10-100FU2F	グローバルマルウェア攻撃トレンド	
ドメイン深油レポート	● Japan	
ြ 标要報告		TOP 20 ? 將北太 件款
C BRIN		OPD/SER
🔲 漏洩対応蔵歴		44 Japan 6.5M-4830
文書/メール環境検出 へ		1 🔞 Brazil 140.2M+37.4K

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。

TOP 20 ? マルウェア感染数	略式表 件数
44 🔵 Japan	6.5M-4930
1 📀 Brazil	140.2M+37.4K
2 🔮 USA	109.8M +7.4K
3 📀 India	86.6M+9.4K
4 🦰 Indonesia	55.3M +7.5K
5 C Türkiye	41.4M+10.6K

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。

各国の感染詳細 ランサムウェア組織活動レート		(1) 🔮	LockBit	(2) 🤨	被害対象国	(3)	0
	LockBit	48	Victim Site	er delse over	🎒 USA 1024 🌔	France	150
	BlackCat (ALPHV)	11	Detection Date	2024-06-24 21:44:48	United Kingd 140 🌔	italy	126
	Ransomhub	9	Industrial Sector	IT Services	🛑 Germany 121 (🍝)	Canada	116
	8BASE	9			😨 Spain 90 📀	Brazil	61
Total 84	CLOP	7			💮 Australia 58 🤶	India	57

(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。

=	Juan com	~			ユーザーフ	ガイド く	レポートダウンロード	ł
די	カ ウント漏洩 152件	I	Eメール漏洩 2件		ドキュメント漏洩	7件	感染したデバイス 6件	
リスクス	コアレベル							?
		A	<u>`</u>	ف	\$	(: <u>)</u>		
		緊急	/	注意	/	安全		

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。

🦉 DarkWebCheck	Jran.com	~								ユーザーガイド	Φ	レポートダウンロード	۵
⊕ <i>9</i> 0- <i>1</i> 1.11+122+	7	アカウント漏決	8 1621≑			EX-ル潮洩 2件		ドキュメント漏洩 7件		感染	したデバイス 6	件	
ドメイン漏洩レポート ヘ	リスクスコアレベリ	L					7	社員アカウントの漏洩					7
○ 概要報告 ○ 振波詳細													
L. 漏洩対応履歴			>	ġ	>				(P	I		152	
文書/メール漏決検出 ヘ		20.46		11.0		双圭			新規調波	解決済み	対応中	合計	
▶ 処理完了リスト													



・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。



・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。



・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。

🦉 DarkWebCheck	(innear	~								ユーザーガイド	Ģ	レポートダウンロード	۵
🌐 σα-πικευγκ	Ph	1ウント漏洩	152件			EX-ル渥渡 2件		ドキュメント漏洩 7件		感染	したデバイス	61=	
ドメイン深浅レポート ヘ							1						-
() 概要報告	リスクスコアレベル						3	社員アカウントの漏洩					0
(2 mtare		•				\sim		-					
🛄 漏洩対応履歴		A No	>	. С .	>	(<u>;</u>)			(19	9		152	
文書/メール 漏洩検出 ヘ				100.000					新規漏洩	剰決済み	封站中	合計	
☑ 処理完了リスト													



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**

8月 202	24					< >	漏洩件数 Type	新規漏洩	再漏洩	合計
8	月	火	水	木	金	±	E アカウント潮波 分 マルウェア感染	0	0	0
4	5	6	7	1 8	2 9	3 10	אגעאייב 🛐	0	0	0
11 18	12 19	13 20	14 21	15 22	16 23	17 24	お知らせ お知らせは現在ありません。	対応件数 対応した履歴	はありません。	
25	26	27	28	29	30	31				

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

IP: 122177 22311 : 0 (1)	UTX III NO LE		^	地図 航空写真	
user	password At http://www.	stealer_path	stealer_type	배년로 이신리 기장군 개성	
IP: 2221.284-200.5) 💿 (1)			~	Ben Bar	
				dong-do 84	(橋川)市 양주시 ウィジョンブ (議取府)市 의정된시
					高陽市 100 100 고양시 Bukhansan の National Park SEDグ +
	漏洩履歴の詳細時	题 (2)		Go.gle	マロラジ クリー ソウル特別市 -トカット 地球デビスを認知をMobility 利用ス

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。



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。

·**白**· 注意

緊急

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。



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

漏洩対応	むの推移						?
024-08-13	2024-08-14	2024-08-15	2024-08-16	2024-08-17	2024-08-18	2024-08-19	2024-08-20

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

期間別対応状況			?
Туре	本日の対応	月間累積対応	対応累計合計
€ アカウント漏洩	0	0	0
✓ マルウェア感染	0	0	0
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	0	0	0

「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。

漏洩部	+和"育致 (1)		(2)	(3)	(4)		(5)	_
	全体	◇ 制制波沢 ◇ ~ 制制波択	全てのリスク	◇ 全てのステータス	🗸 全ての漏気タイプ 🗸	 一致するIDまたに 	む(スワード	検索 Q
	リスクスコア	アカウントロ	初回漏洩日	直近漏洩日	漏洩タイプ	重複漏洩件数	対応状態	対応完了日
	0 60%	and a distance	2016-09-01	2024-08-10	e 🗅 😓	37	① 新規調度	9
	0 60%	AV075-715-0555-4575	2021-12-13	2024-07-30	🖹 🚹 🛠	158	① 新規漏洩	8
	0 60%	communication activity	2021-12-11	2024-07-25	🖹 🖸 😓	18	① 新規漏決	
	0 64%	lana a sel d'anne ann	2022-06-15	2024-07-20	E 🖸 😣	37	① 新規漏洩	-
	0 60%	naron's all nómenn	2016-09-01	2024-07-16		38	① 新規調波	-
	0 60%	anna an that an ann	2018-04-01	2024-07-08	E 🖸 🕁	18	① 新規漏洩	8
	0 60%	a million and	2024-01-29	2024-07-07	目 🖸 🕁	6	① 新規漏洩	
	0 60%	und a glace and	2024-01-29	2024-07-07	E 🖸 🛠	5	① 新規漏洩	φ.
	0 60%	Hence Mile account	2018-04-01	2024-07-06	E D 🛠	14	① 新規漏洩	2
	0 60%	CANADA CANADA AND AND AND A	2023-08-28	2024-07-06	目 🖸 🚸	9	① 新規漏決	2
	0 60%	o no rocano com	2021-12-13	2024-07-05	E 🖸 🛠	31	① 斯規漏決	8
	0 60%	and the second	2023-08-28	2024-06-29	e 🖸 🛠	5	① 新規漏決	8
対応	解決 (6)						1 2	3 4 4

(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。

漏洩対 (1)	応履歴の照会	(2)							? (3)
管理者	and the second V	対応期間	2024-07-01	~	~ = 2024-07-05	~	今日	1週間	検索
(1)	管理者	: 対象ド	メインを選択	てします。					
(2)	対応期間	:検索対	す象の期間を	を入力し	ます。				
(3)	検索	: (1) (2	<mark>2)</mark> で設定した	を条件で	た検索を行いま	す。			
	検索結果は以一	F「B) 期	間別対応の	変化/対	応詳細履歴	」に表示	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。

	r 古 亦 小	2	担当者	1877 (S. 12)	Pharlos T
别间加水	一心の変化	•	対応期間	2024-07-10 ~	2024-07-17
	\wedge		タイプ別対応件数		
				0	
				1	
02401-10 02401-	1 reading reading reading read	15 024.01.16 024.01.11	אגעדעב 🚹	57	
1 ² 1 ²	v v v v	\$v° \$v°	合計	58	
ت خر ر د					
对心言	牛种 腹 歴				
No	דאלילת	URL	漏洩タイプ	漏洩日	対応日
1	er face seler	-	D & E	2024-03-28	2024-07-17
					Þ

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。

処理必要リスト 19 ?	文章/水-小道宗(1) v キーワード道宗(2) v Search (3) 検索 Q
Keyword: */iran.com (4) Re: (지환지교에스캔씨) 인전국제공항공사 DDAN API 문서 진달 드립니다. (4) Keyword: */iran.com [CJ스큠신고] RE: ATTACHED INVOICE WITH PAYMENT S	Re: [지란자교에스앤씨] 인천국제공항공사 DDAN API 문서 전달 드립니다. (5) 표준:
Keyword: #Jiran.com GR@TABLE_VAVBV0_1020.XLS	안녕하세요 지런지교예스앤씨 양용훈입니다. 유선으로 요청주신 DDAN API 문서 전달 드립니다. Deep Discovery Analyzer API 소개 마지막 페이지의 주의사항을 꼭 확인 부탁드립니다. 문 의사항 있으신 경우 연락 부탁드립니다. 김사합니다 Original Message From :
● Keyword: #Jiran.com jiransecunty_MobileKeeper_对答么准서.pdf	The second seco
■ Keyword: #/iran.com 매입전자세금계산서목록(1_1053).xls	A Design of the second seco
keyword: #jran.com 모바일키퍼_브로셔.pdf	(a) which is the probability of the second state of the second
♣ Keyword: #jran.com 매입친자세균계산서목록(1_1053).xls	and the state of the second state of the state state of the
e Keyword: #Jiran.com 9월 매입전자세금계산서목록(1_1053).xls	該当腸決内容の詳細を記載してください。 (6) (7) 処理完了とする (8) 関連なしとする

(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。

処理完了リスト 1	全ての開い	囲性(1) v 文志パイ-ル道奈(2) v キーフード道奈(3) v Search (4)	検索 Q
Keywort: #Jiran.com	(5)	MEMBER.xlsx 還浅日: 2024-05-14	(6)
		57М8	
		▲ 書合 ゼロダークなゴから現代される満成文金をダウソロードする場合、春田世市にマルウエアに感染するリスクがあります。したがって、 に仮想マタン環境で文書をダウソロードするか、他の必要ななキュリティ対像を開いた上でファイルを描くことをお勧めします。また、 繋する時にはサンドボックス環境で変行してください、文書にマルウエアが含まれている考点でも、リスクを最小原に加えることがで	史全のため 文書を開 さます。
		該当憲決内容の詳細を記載してください。 (7) (8) 3メント修正 (9)関連な	らしとする

- (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。

👸 DarkWebCheck	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■
⊕ グローバルトレンド	グローバルマルウェア攻撃トレンド
ドメイン漏洩レポート ヘ	Japan
(概要報告	
[] 漏洩詳細	
漏洩対応履歴	

0.00
(2)
3) ~
4) ~

- (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

Welcome back! 🗦	•
Email Address	
Password	
	Sign In

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。

				ŻA _ ,∞träthire	krog v
MY PAGES P# マイページ	私の会社 🔆			Q Search Compa	ny Name
PAGES	All 1				
🖽 私の会社	ID	会社名	従業員数	作成日	アクション
 ♀ ♀ ▶ ↓ ポート管理 ∨ 	FETRIC THOM SERVICE	지원지교	900	2024-08-14 14:08:46	Ľ

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。

👸 DarkWebCheck				ZA jsecuritytödarkva	eboteckiju 🗸 🗸
MY PAGES P_{\$} マイページ	私の会社 🔶		KOR JPN ENG	Q Search Compa	ny Name
PAGES	All 1				
田 私の会社	ID	会社名	従業員数	作成日	アクション
ペ ドメイン管理者管理 ✓	489040000 IIA4800 JA2888 S	1.52.7	900	2024-08-14 14:08:46	Ľ
₿ レボート管理 ッ					

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。

) ∂arkWebCheck				Z_A jsecurity@darka	webcheck,p 🗸
my pages 🎗 マイベージ	私の会社 🤸			契約管理者 Sign Out	
PAGES	All 1				
111 私の会社	ID	会社名	従業員数	作成日	アクション
 ペ ドメイン管理者管理 ~ ペ レポート管理 ~ 	100.4451/h446.5520(00.00)	শ্বস	900	2024-08-14 14:08:46	Ľ

2.3. マイページ

マイページ 🤧	
SETTINGS 全基本情報	(1) 基本情報 D(メール) 「エー・」。@www.comment

(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。

SE	パスワード変更	×
	新しいパスワード*	
		キャンセル 保存
L		ドヤンセル 保存

2.4. 私の会社

私の会社 、 (2)		(1)	Q Search Compar	ny Name
All 1				
ID	会社名	従業員数	作成日	アクション
		900	2024-08-14 14:08:46	(3) 🕜

(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。

会社詳細情報 🔆	
SETTINGS	基本情報
() 基本情報 (1)	<u> 今</u> 注人
▲ 業界 (3)	지난지고
	従業員数
	900
	保存

(1) 基本情報

会社詳細情報 🔆	
SETTINGS	基本情報
() 基本情報	
● ドメイン	会社名
四 業界	시킨 사 교
	従業員数
	900
	保存

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。

SETTINGS ① 基本情報	ドメイン		
● ドメイン	ドメインリン	21	
界業 24	ドメイン	作成日	アクション
	(frantioon)	2024-08-14 14:16:5	51 =Q
	契約リスト ドメインを選択す	「る時に契約期間を確認できます。	
	ドメイン	契約開始	契約終了
	liran.com	2024-08-14 00:00:00	2025-01-31 00:00 00
	キーワード ドメインを選択す	する時にドメインキーワードを確認できぇ	キーワード追加ます。
	ドメイン	キーワード	承認ステータス
	TIST COTT	(Incol)	ACTIVE

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。

Domain Keyword Modal	×
ドメイン*	
jiran.com	
キーワード*	
承認ステータス*	
リクエスト	×
	キャンセル保存

(3) 業界

2.5. ドメイン管理者リスト

ドメイン管理	者!	ノスト	*	Q, Search User	Name (1)	- ユーザー作成
All 1						
ID	名前	所属会社	ログイン有効化	権限	会員登録日	2) アクション
sjølp200ggraf.com		지난지교	true	ドメイン管理者	2024-08-16 11:30:2	3 ピ 🖞

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。

名前*	
名前	
ID*	
Email	
Password*	
Password	
会社の選択*	
사람위프	3
ログイン有効化*	

(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。

SETTINGS	基本情報
○ 基本情報	ID(メール)
<u>Ⅲ</u> 会社	sjwig200@igne.toc.m
	名前
	ログイン有効化
	一時的なロジインコートを使用せずに水統的なハスワートを設定できます。
	パスワードリセット
	保存

<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。

パスワード変更	×
新しいパスワード*	
	キャンセル保存

■会社

対象の管理者の会社情報の確認、変更が行えます。

ユーザー設定 🦂	•		
SETTINGS C 基本情報	会社		会社作成
Ⅲ 会社	所属会社		
_		会社名	アクション
		ierby electricit	=0, 🗇
	ドメイン 会社選択するとドメインが確認	できます。	
	会社名	ドメイン	アクション
		No Data	

<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。

	Q, d
	SEARCHES
TINC	deroestrivezt
-	

・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>

所属会社

会社名		アクション
darkwebcheck		<u>=</u> α 🛍
ドメイン		ドメイン追加
会社選択するとドメインが確認できます。		
会社名	ドメイン	アクション
darkwascheck	j rankozini	団

・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。

CEADOUEO			
SEARCHES			
jran.com			

・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。

定期レポートリスト 🔆				+ 定期	ルポート生成
All 1					
ID	ID(メール)	ドメイン	DATE_TYPE	作成日	アクション
CARLENDER DE CARLENDER SOCIET ESTENSE SOCIET	darthoghane was	[access]	WEEK ()	2024-08-16 11:30:52	C 🖻

・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。

調査期間設定*		
2) 毎週	~ 月	~
ドメインユーザー*		
(3) уваанного дражеству со др		~
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。	
jimm.com (JP)		
inan.com い⊳ (6)タイトル*		

段落	~	в	Ι	\mathcal{O}	:=	1=	A≞ ∖	A A	[~]	<u>A</u>	~	A	~	<u></u>		:
こんにちば 当社のDai います。 [調査期間 す。	ま、「Dar rkWebのi :{{INVE	kWel 常時盟 STIG	bCh 告視 ATIC	eck」 クラウ DN_P	です クドセ PERIC	t。 ナービ DD}}]	スをこ にモニ	「利用 :タリ	いけ	ただ ブさ	き、	あ	りカ 容を	*とう :レポ	ごっ	- 2
内容をご 引き続き、	電認いたた お客様の	Eき、 D情報	道 し キ	」な対	応や	対策を確何	をお願 呆する	いい ため	たし に最	まで	す。 を尽	<ι	ょ	す。		
フッター内容	*															
フッター内容	*	в	I	0	:=	1	A⁼ .	~ A1	[~	A	~	A	~	111		:

- (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、フッダ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。

緊急レポートリスト 🤆			+ 緊	急レポート生成
All 1				
ID	ID(メール)	FX7 >	作成日	アクション
THE STREET BALLAND CONTRACT		period a	2024-08-28 08:50:49	് 🖞

・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) テンプレート	
韓国語 英語 日本語	
<mark>2)</mark> ドメインユーザー*	
vasumoto(%(security.cn.)p	~
3)cc	
	追加
No Data	
4) 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る	ます。
jman.com (JP)	
<mark>5)</mark> タイトル*	
and the second sec	

	~	В	Ι	Ø	:=	1-2-	A⁼	~	AI ~	A	~	A	~		:
フッター内容*															
印弦	~	в	Ι	O	:=	1 <u>-</u> 2 <u>-</u>	A⁼	~	~ 1A	<u>A</u>	~	A	~	<u>-</u>	÷

(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

