Constant Monitoring Service

DarkWeb監視代行サービス

DarkWebCheck

（ダークウェブチェック）

ドメイン情報さえあれば
DarkWebの常時監視代行ができます

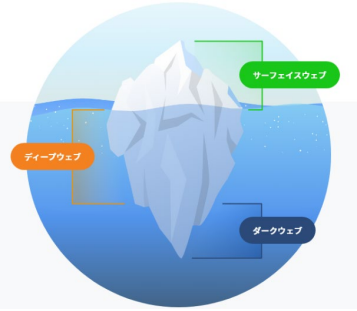
DarkWeb監視代行サービス

DarkWebCheck

JSECURITY

DarkWebCheck

DarkWebとは



DarkWebは漏洩・搾取された情報の取引が行われているWebサイトです

DarkWebでは漏洩された企業及び個人情報や、
マルウェアやランサムウェアなどの不正ツールが取引されています。
攻撃の材料や手段も売買できるDarkWebは、企業や個人にとって大きな脅威となります。

DarkWeb上で公開されている情報と漏洩時の脅威

アカウント情報

組織のアカウント情報（ID、パスワード等）です。悪用された場合、なりすましによる不正アクセスが可能となり組織内の重要情報の漏洩に繋がります。また、メールアカウント情報の場合は、なりすましによる組織内情報漏洩に繋がります。

Eメール情報

組織のアカウントを利用して送受信されたメールです。
メール情報が漏洩した場合は、取引先を装った悪意のある攻撃を受けたり、機密情報や顧客情報の流出に繋がります。

ドキュメント情報

PDF・図面等のドキュメント情報です。 知的財産などの重要なデータが含まれている場合、競合他社が悪用して組織の競争優位性を弱体化させるなどの問題に繋がります。

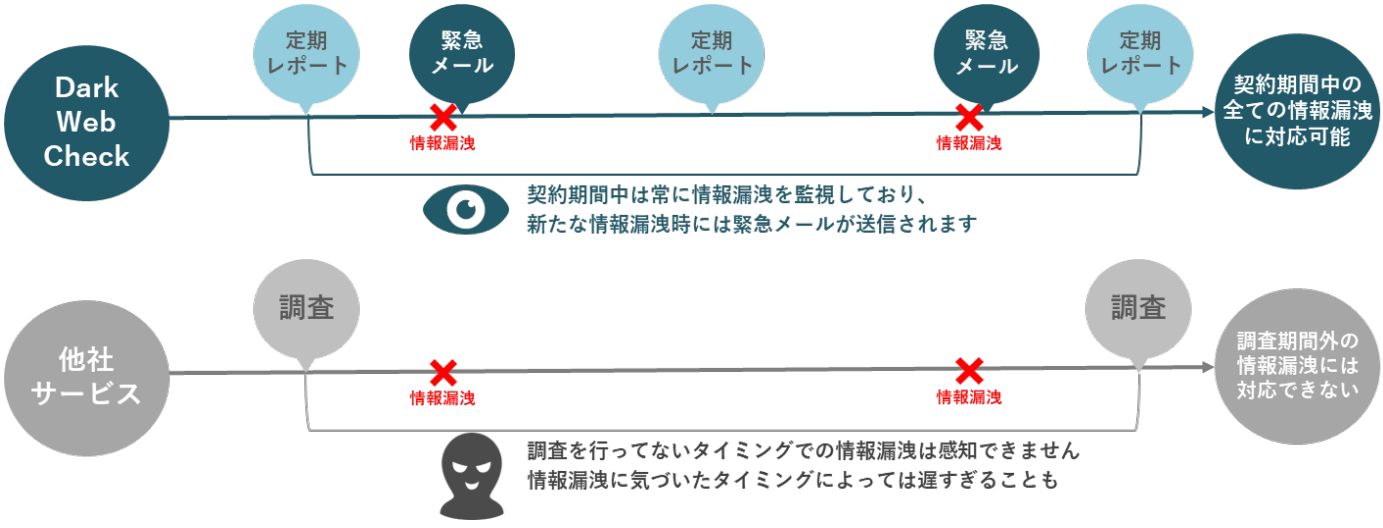
顧客への情報流出 | **事業の中断** | **売上機会損失** | **顧客への二次被害**

DarkWebでの情報漏洩を放置してしまうと重大な問題に発展してしまうリスクがあります

DarkWebCheckとは

DarkWebの情報漏洩を常時監視代行するサービスです

DarkWeb上の情報は常に変化します。
あなたの会社の機密情報は、昨日まではなくても今日には漏洩しているかもしれません。
新たに情報漏洩が発生した場合にお知らせする緊急メールや、毎月状況をお知らせする定期レポートがあります。DarkWebCheckは常にDarkWebの監視を続けます。



サービス導入プロセスについて

1 **ドメイン数、オプションを決定**
ドメイン数は従量課金制となり、詳細レポートのオプションもあります。

2 **申込書を記入後、お申し込み**
・**当月末営業日**から定期レポート配信…**当月20日まで**にお申込みいただいた場合。
・**翌月末営業日**から定期レポート配信…**当月21日以降**にお申込みいただいた場合。
※当該20日が土日祝の場合はその直前の営業日が基準となります。

3 **定期レポートを確認、新たな情報漏洩があった時は緊急メールを確認**
通常の定期レポートに加え、新たな情報漏洩時には緊急メールを翌営業日に配信、
情報漏洩に対してスピーディな対策が可能です。

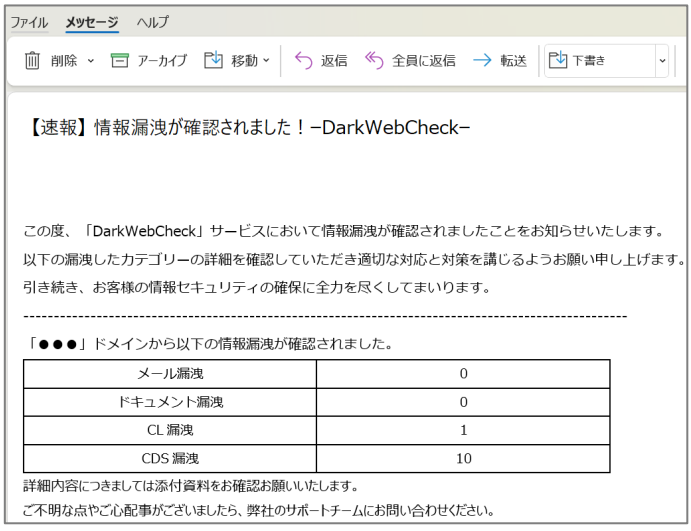
4 **対策案の適応**
レポートを元に様々な対策を行うことが可能です。
DarkWebにある情報は日々更新されますので**継続して調査をしていくことが大切です。**

サービス１. 定期レポートについて

毎月末営業日に現在の漏洩状況を報告するサービスです

今DarkWeb上にある情報にどの程度まで対応できているかがわかります。
DarkWeb上にあるすべての情報漏洩をなくすことはできませんが、
現在の状況がリスクをコントロールできているかどうかがわかります。

サービス２. 緊急メールについて


ファイル　メッセージ　ヘルプ
削除　アーカイブ　移動　返信　全員に返信　転送　下書き

【速報】情報漏洩が確認されました！−DarkWebCheck−

この度、「DarkWebCheck」サービスにおいて情報漏洩が確認されましたことをお知らせいたします。
以下の漏洩したカテゴリーの詳細を確認していただき適切な対応と対策を講じるようお願い申し上げます。
引き続き、お客様の情報セキュリティの確保に全力を尽くしてまいります。

「●●●」ドメインから以下の情報漏洩が確認されました。

メール漏洩	0
ドキュメント漏洩	0
CL 漏洩	1
CDS 漏洩	10

詳細内容につきましては添付資料をお確認お願いいたします。
ご不明な点やご心配事がございましたら、弊社のサポートチームにお問い合わせください。

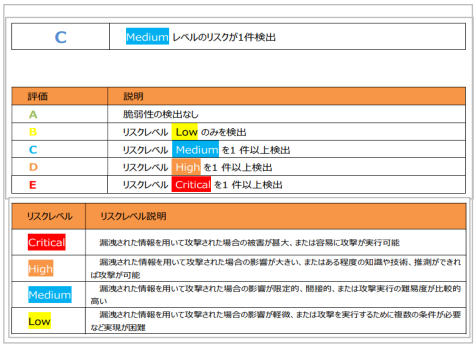
新たな情報漏洩があった場合にはメールを利用して翌営業日にスピーディにお知らせします

翌営業日に情報漏洩がわかるので迅速な対応により被害を最小限にできます

アカウント情報が漏洩していたら…
すぐにパスワードを変更、なりすましの被害を防ぐことが可能です。

侵害されたデバイスのIPがわかったら…
ネットワークから取り除くなどの対策が可能です。

サービス３. 詳細レポート（オプション）

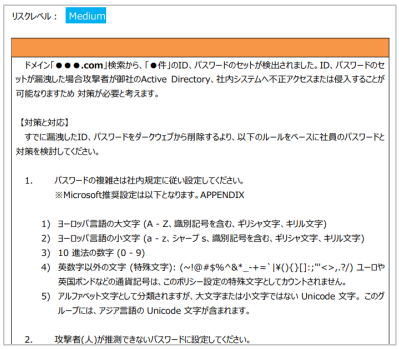


C	Medium レベルのリスクが1件検出

評価	説明
A	脆弱性の検出なし
B	リスクレベル Low のみを検出
C	リスクレベル Medium を1 件以上検出
D	リスクレベル High を1 件以上検出
E	リスクレベル Critical を1 件以上検出

リスクレベル	リスクレベル説明
Critical	漏洩された情報を用いて攻撃された場合の被害が甚大、または容易に攻撃が実行可能
High	漏洩された情報を用いて攻撃された場合の影響が大きい、またはある程度の知識や技術、推測ができれば攻撃が可能
Medium	漏洩された情報を用いて攻撃された場合の影響が限定的、間接的、または攻撃実行の難易度が比較的高い
Low	漏洩された情報を用いて攻撃された場合の影響が軽微、または攻撃を実行するために複数の条件が必要など実現が困難

<リスクレベル>



リスクレベル： Medium

ドメイン「●●●.com」検索から、「●件」のID、パスワードのセットが検出されました。ID、パスワードのセットが漏洩した場合攻撃者が御社のActive Directory、社内システムへ不正アクセスまたは侵入することが可能なりますため 対策が必要と考えます。

【対策と対応】
すでに漏洩したID、パスワードをダークウェブから削除するより、以下のルールをベースに社員のパスワードと対策を検討してください。

1. パスワードの複雑さは社内規定に従い設定してください。
※Microsoft推奨設定は以下となります。APPENDIX

1) ヨーロッパ言語の大文字 (A - Z、識別記号を含む、ギリシャ文字、キリル文字)
2) ヨーロッパ言語の小文字 (a - z、シャープ s、識別記号を含む、ギリシャ文字、キリル文字)
3) 10 進法の数字 (0 - 9)
4) 英数字以外の文字 (特殊文字): (~!@#$%^&*_-+=`|¥(){}[]:;"'<>,.?/) ユーロや英国ポンドなどの通貨記号は、このポリシー設定の特殊文字としてカウントされません。
5) アルファベット文字として分類されますが、大文字または小文字ではない Unicode 文字。このグループには、アジア言語の Unicode 文字が含まれます。

2. 攻撃者(人)が推測できないパスワードに設定してください。

<詳細レポートの例>

情報漏洩の状況を報告書形式でレポートすることも可能です

リスクレベルを元にした報告書なので社内を巻き込んだ対応への判断材料にできます

各項目について危険度・攻撃難易度を評価し、リスクレベルを決定しています。

※リスクレベルは、情報漏洩のみでリスクを判定する国際基準は存在しないため弊社独自の判定基準に沿って判定いたします

単独でのDarkWebの調査は困難です。だからこそ代行サービスを。

スキル

Darkwebへアクセスするためには必要なTorブラウザは悪性コードや不法的な要素が含まれている可能性があるため、**ブラウザの設置すらリスクがあります。**
Torブラウザでアクセスしたとしても、漏洩された情報を探すことは一般な知識では不可能で特殊なソフトウェア（以下S/W）が必要となります。

負担

自社でS/Wを購入して運用する場合、大手企業の場合S/Wライセンス費用だけで年間約1,000万円以上かかります。エンジニアの工数も加味すると最低でも**年間約2,000万円以上はかかる計算です。**

コスト

専門会社に依頼する場合には、**スポットで約500～1,000万円、年間で約1,500～4,000万円かかります。**
さらにDarkWeb上の情報は常に入れ替わるので**継続した調査が必要です。**

サービス形態について

プラン	内容
基本プラン	定期レポート＋緊急メール
追加オプション	詳細レポート

※ご希望に合わせて調査対象ドメインを追加購入することが可能です。
※詳細レポートは1ドメインあたり1レポートとして提供致します。

できるだけコストをかけずに情報漏洩を調査したい
基本プラン
自社で５個のドメインを持っているため、すべてのドメインを調べたい
基本プラン＋4ドメイン追加
メインのドメインを調査、さらに社内向けに調査結果をレポートで報告したい
基本プラン＋詳細レポート

1ドメインからお申込み可能です
調査対象のドメインに対して
毎月の定期レポートと
情報漏洩発生時の緊急メールが
受け取ることが可能です

調査したいドメインの数だけ追加も可能です。
ボリュームディスカウントもあります。

調べたい情報量に応じてフレキシブルにプランが組めます。必要な分だけお支払いなので無駄がありません。

開発元
JSECURITY
株式会社 JSecurity
東京都港区浜松町2-4-1 世界貿易センタービルディング 南館17階
TEL: 03-4567-2823 FAX:03-4567-2824
E-mail：sales@jsecurity.co.jp
URL：https://www.jsecurity.co.jp