WideAngle プロフェッショナルサービス
リスクスコアリングのご紹介

2024年08月27日

NTTコミュニケーションズ株式会社

WideAngleとは

「WideAngle」 はNTT Comが提供する グローバル統一の総合セキュリティサービスブランドです

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

- プロフェッショナルサービス
- マネージドセキュリティサービス

WideAngleという名称には、標的型攻撃など未知の脅威に世界がさらされる中、
広い視野でリスクを見通し、より安心・安全な社会を志す開拓者でありたいという思いを込めています。
NTT Comは、WideAngleブランドのもと総合リスク マネジメント サービスを積極的に展開し、
マネージド セキュリティ サービス プロバイダー（以下MSSP）のグローバル トップ プレイヤーを目指します。

セキュリティ状況を把握することの必要性

このようなお困りごとはありませんか

自社セキュリティレベルの把握

・自社のセキュリティ対策の改善や今後の対応方針を決めたい

・セキュリティ対策といっても何から対策すればいいか分からない

・簡単に安くセキュリティ対策を始めたい

・効率的にセキュリティ対策を行いたい

取引先のセキュリティの把握または報告

・サプライチェーンのセキュリティレベルを把握し管理したい

・委託先、取引先のセキュリティレベルを確認しておきたい

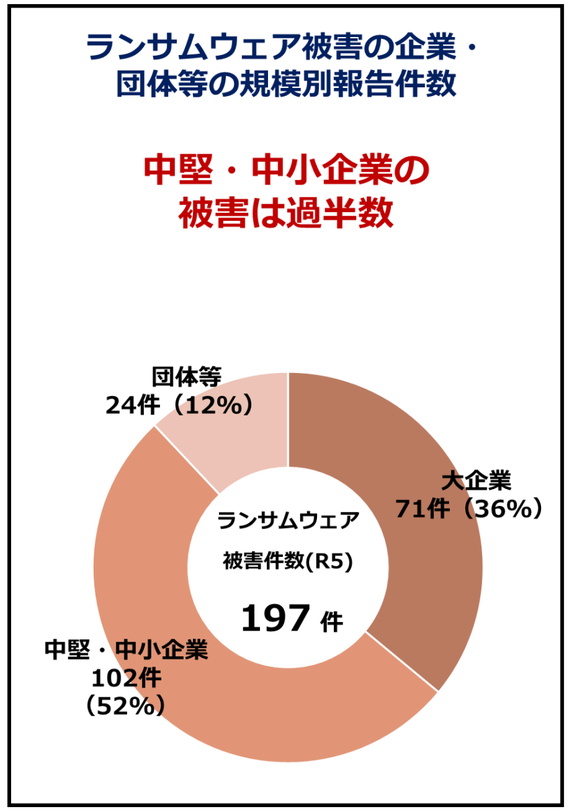
セキュリティ脅威の実情

企業規模にかかわらずセキュリティ製品を導入していればセキュリティ対策は十分だと考えている企業は多く存在します。しかし攻撃者はサプライチェーン全体を偵察し弱点をついてくるため、企業規模にかかわらず対策不足の企業が狙われるケースがあります。狙われたサプライチェーンの企業の中には、実際に攻撃を受けていても気づけていないケースも数多く存在しています。

IPA 情報セキュリティ10大脅威(年代別)

セキュリティ脅威（組織）	2024年	2023年	2022年	2021年	2020年
ランサムウェアによる被害	1位	1位	1位	1位	5位
サプライチェーンの弱点を悪用した攻撃	2位	2位	3位	4位	4位
内部不正による情報漏えい	3位	4位	5位	6位	2位
標的型攻撃による機密情報の窃取	4 位	3位	2位	2位	1位
修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	5位	6位	7位	-	-
不注意による情報漏えい等の被害	6位	9位	10位	9位	7位
脆弱性対策情報の公開に伴う悪用増加	7位	8位	6位	10位	14位
ビジネスメール詐欺による金銭被害	8位	7位	8位	5位	3位
テレワーク等のニューノーマルな働き方を狙った攻撃	9位	5位	4位	3位	-
犯罪のビジネス化（アンダーグラウンドサービス）	10位	10位	-	-	-

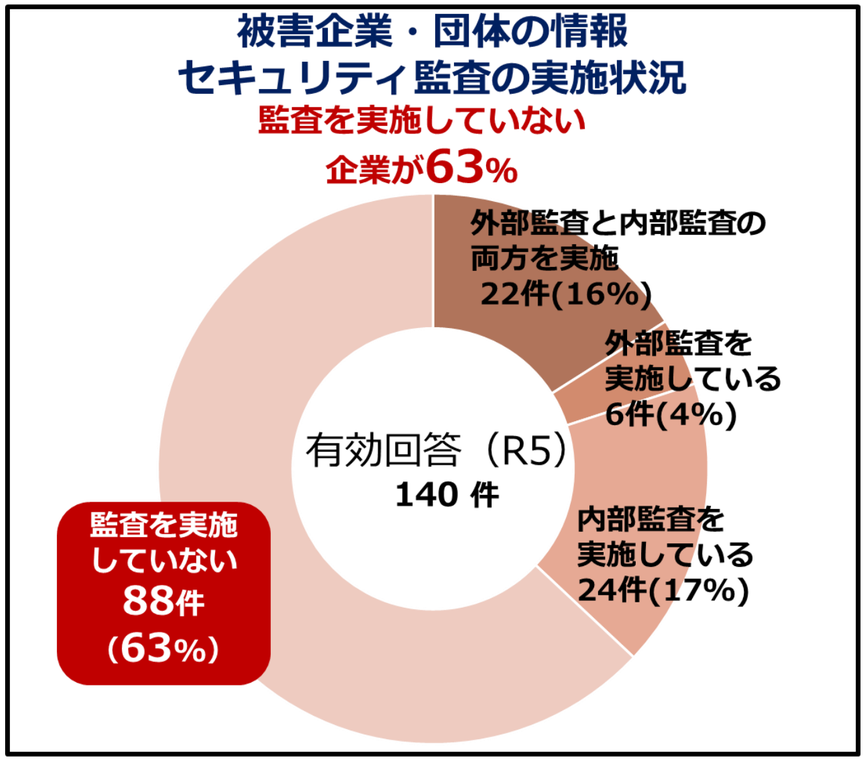
出典: IPA『情報セキュリティ10大脅威』2020～2024年版をもとに作成

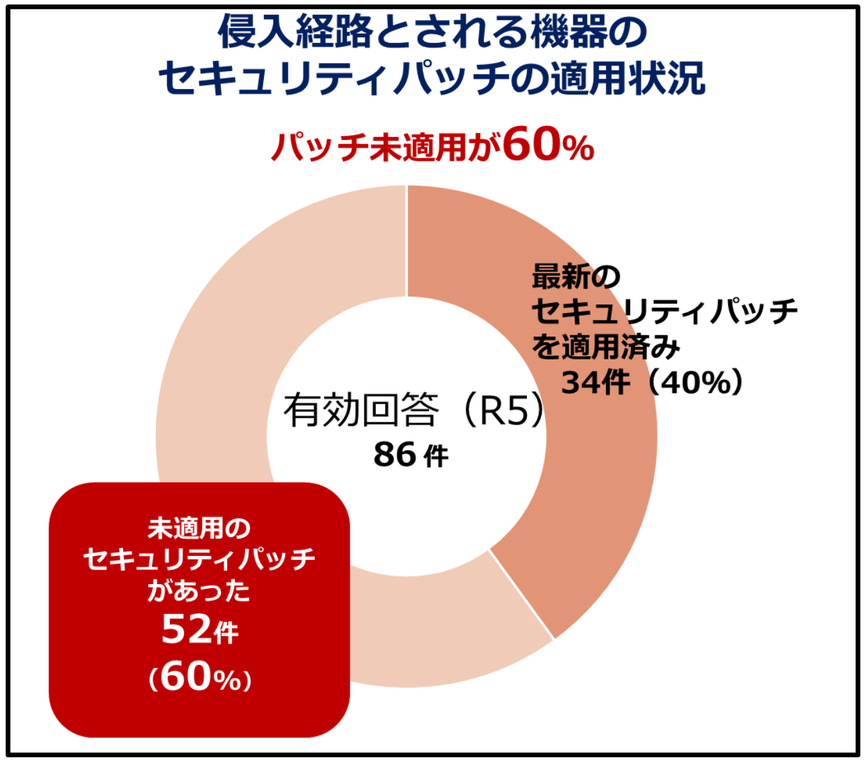


出典:警察庁　令和５年におけるサイバー空間をめぐる脅威の情勢等について

昨今の被害状況

- 被害を受けた企業の63%はセキュリティの監査を行っていないと回答しています。
- 侵入経路とされる機器に対してセキュリティパッチを適用していないとの回答は60%となっています。





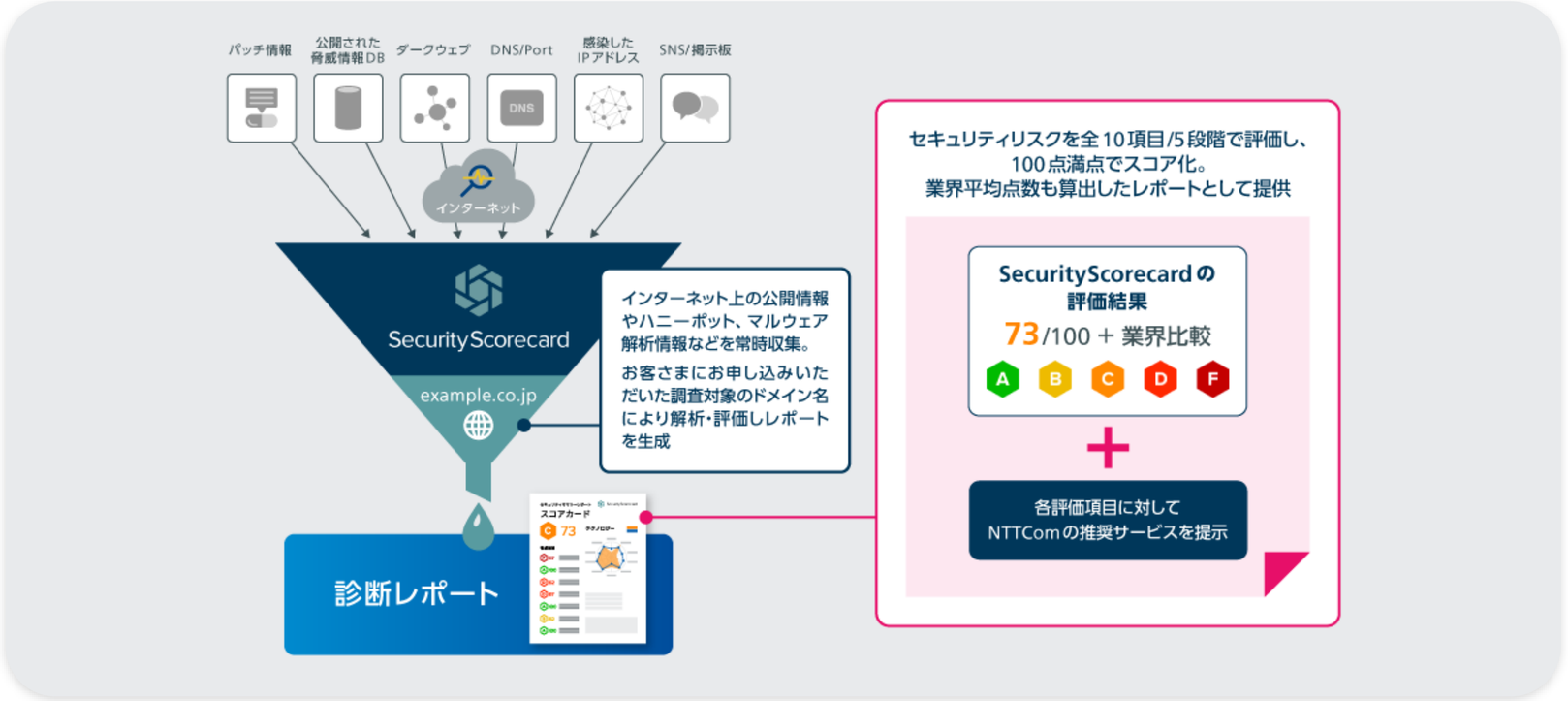
出典:警察庁　令和５年におけるサイバー空間をめぐる脅威の情勢等について

リスクスコアリングで安価に自社のセキュリティリスクを認識し、必要な対策は何かを把握できます。

WideAngle プロフェッショナルサービス
リスクスコアリングとは

サービス概要

- リスクスコアリングは、「Security Scorecard社」のサイバーセキュリティリスクレイティングを利用したサービスです。
- お客様のドメインに紐づくインターネット上の公開情報を自動で定期的に収集・分析して評価レポートを生成します。
- 評価レポートの各評価項目に対して、リスク低減に有効な対策案や推奨サービスを掲載した推奨サービスレポートを提供します。



※お客さまにてSecurity Scorecardのポータル画面を操作することはありません。

提供内容

選べるプランをご用意。「定期診断」「スポット診断」をそれぞれお求めやすい価格で提供します。
診断対象のドメイン数により価格が決定します。

	定期診断	スポット診断
診断レポート提供回数	毎月	1回
提供価格（1ドメインあたり）	2万円（税込2.2万円）／月	8万円（税込8.8万円）／回
診断レポート内容	詳細レポート＋サマリーレポート	詳細レポート＋サマリーレポート
リスク対策の推奨サービスレポート	○	○
お問い合わせサポート期間	契約期間	3カ月
診断レポート解説（オプション）お申し込み	○	○

提供内容（定期診断）

定期診断では毎月、セキュリティスコア結果の詳細レポート＋サマリーレポートと、対策サービスレポート、問い合わせサポートを提供します。毎月診断レポートのスコアを確認することで、セキュリティリスクの推移を把握することができ、対策状況の確認に活用することができます。

サマリーレポート＋詳細レポート＋リスク対策の推奨サービスレポート（初月1回）

＋

お問い合わせサポート

レポートについて不明な点があればお問い合わせ可能!

＋

診断レポート解説（オプション）

診断レポート結果の解説やお客さまの環境を踏まえたアドバイスを提供します。

※定期診断の最低利用期間は１年です。

提供内容（スポット診断）

スポット診断ではセキュリティスコア結果の詳細レポート＋サマリーレポートと、対策サービスレポート、３カ月間のお問い合せサポートを提供します。詳細レポートでは、サマリーレポートの10項目のカテゴリよりもさらに、詳細な項目レベルまで掲載。具体的なセキュリティリスク箇所を示しているため、より詳細に分析が可能です。

提供機能①（サマリーレポート）

10項目のカテゴリ評価と総合評価を、5段階（A～D,F）のランクと100点満点の点数で行います。
また業界平均との比較グラフで、自社のセキュリティ対策レベルが一目で分かります。

以下の様な業種区分で相対評価が可能です!

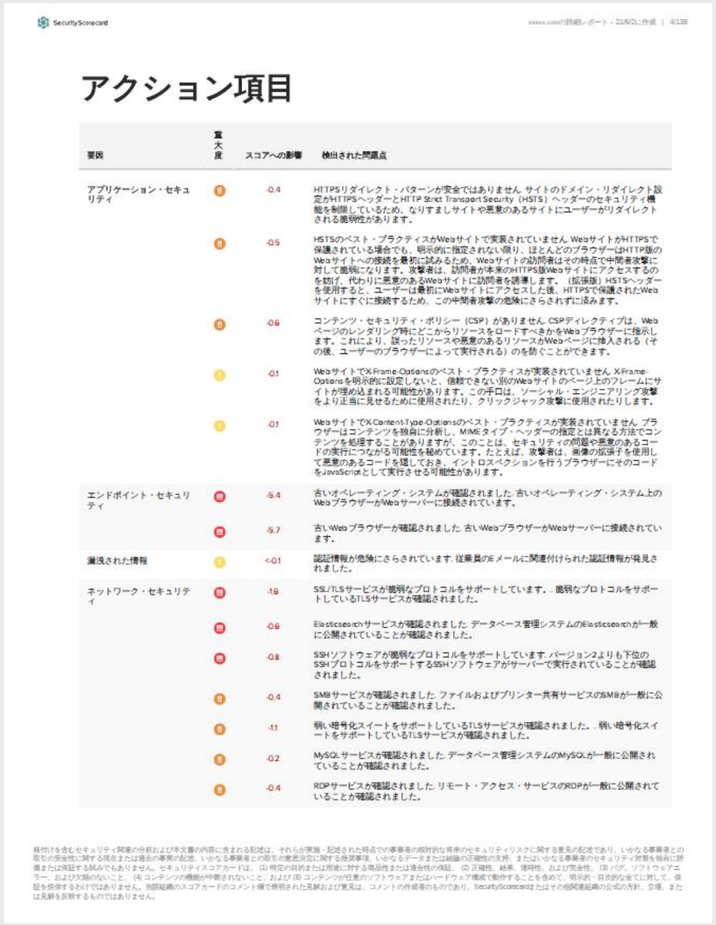
小売業　テクノロジー　金融業　食料品

医薬　エネルギー　建設業　教育

など

提供機能②（詳細レポート）

10項目の診断カテゴリを、約153項目に分類し高（High）/中（Medium）/低（Low）の詳細項目レベルで具体的なセキュリティリスク箇所を示します。



SecurityScorecard

xxxxx.comの詳細レポート - 21/6/2に作成 | 4/138

アクション項目

要因	重大度	スコアへの影響	検出された問題点
アプリケーション・セキュリティ	B	-0.4	HTTPSリダイレクト・パターンが安全ではありません サイトのドメイン・リダイレクト設定がHTTPSヘッダーとHTTP Strict Transport Security（HSTS）ヘッダーのセキュリティ機能を制限しているため、なりすましサイトや悪意のあるサイトにユーザーがリダイレクトされる脆弱性があります。
	B	-0.5	HSTSのベスト・プラクティスがWebサイトで実装されていません Webサイトがhttpsで保護されている場合でも、明示的に指定されない限り、ほとんどのブラウザーはHTTP版のWebサイトへの接続を事前に試みるため、Webサイトの訪問者はその特定の中間者攻撃に対して脆弱になります。攻撃者は、訪問者が本来のHTTPS版Webサイトにアクセスするのを妨げ、代わりに悪意のあるWebサイトに訪問者を誘導します。（拡張版）HSTSヘッダーを使用すると、ユーザーは最初にWebサイトにアクセスした後、HTTPSで保護されたWebサイトにすぐに接続するため、この中間者攻撃の危険にさらされずに済みます。
	B	-0.6	コンテンツ・セキュリティ・ポリシー（CSP）がありません CSPディレクティブは、Webページのレンダリング時にどこからリソースをロードすべきかをWebブラウザーに指示します。これにより、誤ったリソースや悪意のあるリソースがWebページに挿入される（その後、ユーザーのブラウザーによって実行される）のを防ぐことができます。
	I	-0.1	Webサイトで X-Frame-Optionsのベスト・プラクティスが実装されていません X-Frame-Optionsを明示的に設定しないと、信頼できない別のWebサイトのページ上のフレームにサイトが埋め込まれる可能性があります。この手口は、ソーシャル・エンジニアリング攻撃をより正当に見せるために使用されたり、クリックジャック攻撃に使用されたりします。
	I	-0.1	Webサイトで X-Content-Type-Optionsのベスト・プラクティスが実装されていません ブラウザーはコンテンツを独自に分析し、MIMEタイプ・ヘッダーの指定とは異なる方法でコンテンツを処理することがありますが、このことは、セキュリティの問題や悪意のあるコードの実行につながる可能性を秘めています。たとえば、攻撃者は、画像の拡張子を使用して悪意のあるコードを隠しておき、イントロスペクションを行うブラウザーにそのコードをJavaScriptとして実行させる可能性があります。
エンドポイント・セキュリティ	C	-5.4	古いオペレーティング・システムが確認されました 古いオペレーティング・システム上のWebブラウザーがWebサーバーに接続されています。
	C	-5.7	古いWebブラウザーが確認されました 古いWebブラウザーがWebサーバーに接続されています。
漏洩された情報	I	<-0.1	認証情報が危険にさらされています 従業員のEメールに関連付けられた認証情報が発見されました。
ネットワーク・セキュリティ	C	-1.6	SSL/TLSサービスが脆弱なプロトコルをサポートしています。 脆弱なプロトコルをサポートしているTLSサービスが確認されました。
	C	-0.6	Elasticsearchサービスが確認されました データベース管理システムのElasticsearchが一般に公開されていることが確認されました。
	C	-0.8	SSHソフトウェアが脆弱なプロトコルをサポートしています バージョン2よりも下位のSSHプロトコルをサポートするSSHソフトウェアがサーバーで実行されていることが確認されました。
	B	-0.4	SMBサービスが確認されました ファイルおよびプリンター共有サービスのSMBが一般に公開されていることが確認されました。
	B	-1.1	弱い暗号化スイートをサポートしているTLSサービスが確認されました。 弱い暗号化スイートをサポートしているTLSサービスが確認されました。
	B	-0.2	MySQLサービスが確認されました データベース管理システムのMySQLが一般に公開されていることが確認されました。
	B	-0.4	RDPサービスが確認されました リモート・アクセス・サービスのRDPが一般に公開されていることが確認されました。

格付けを含むセキュリティ関連の分析および本文書の内容に含まれる記述は、それらが実施・記述された時点での事業者の相対的な将来のセキュリティリスクに関する意見の記述であり、いかなる事業者との取引の安全性に関する現在または過去の事実の記述、いかなる事業者との取引の意思決定に関する推奨事項、いかなるデータまたは統論の正確性の支持、またはいかなる事業者のセキュリティ対策を独自に評価または保証する試みでもありません。セキュリティスコアカードは、(1) 特定の目的または用途に対する商品性または適合性の保証、(2) 正確性、結果、適時性、および完全性、(3) バグ、ソフトウェアエラー、およびウイルスのないこと、(4) コンテンツの機能が中断されないこと、および (5) コンテンツが任意のソフトウェアまたはハードウェア構成で動作することを含めて、明示的・目的的な全てに対して、保証を提供するわけではありません。当該組織のスコアカードのコメント欄で表明された見解および意見は、コメントの作成者のものであり、SecurityScorecardまたはその他関連組織の公式の方針、立場、または見解を反映するものではありません。

SecurityScorecard

xxxxx.comの詳細レポート - 21/6/2に作成 | 6/138

B 82 アプリケーション・セキュリティ

Web Application Vulnerability モジュールでは、ホワイトハットCVEデータベースやブラックハット・エクスプロイト・データベース、主要な検索エンジンによってインデックス付けされた機密性の高い検出結果などの方法で特定された、悪用される可能性のある既知の問題に基づく脅威インテリジェンスが使用されます。このモジュールは、複数の公開データセットやサードパーティ・フィードに加え、社内開発されたインデックス作成/集計エンジンからもデータを取り込みます。今後Webアプリケーションのセキュリティ侵害が起こる可能性はスコアに基づいて判断され、既存の改ざんコードの有無が調べられます。脆弱なアプリケーション、古いバージョン、アクティブな改ざんの存在は、全般的な格付けを計算するために使用されます。

重大度「高」	重大度「中」	重大度「低」	プラス要素
Application Securityの重大度「高」の問題はありません	HTTPSリダイレクト・パターンが安全ではありません 1 HSTSのベスト・プラクティスがWebサイトで実装されていません 3 コンテンツ・セキュリティ・ポリシー（CSP）がありません 3	Webサイトで X-Frame-Optionsのベスト・プラクティスが実装されていません 2 Webサイトで X-Content-Type-Optionsのベスト・プラクティスが実装されていません 2	Webアプリケーション・ファイアウォール（WAF）が検出されました 2 **情報提供目的** サプリンス整合性の実装が安全ではありません 3 Webサイトで X-XSS-Protectionのベスト・プラクティスが実装されていません 3

Webサイトで X-Frame-Optionsのベスト・プラクティスが実装されていません

-0.1 スコアの影響

X-Frame-Optionsを明示的に設定しないと、信頼できない別のWebサイトのページ上のフレームにサイトが埋め込まれる可能性があります。この手口は、ソーシャル・エンジニアリング攻撃をより正当に見せるために使用されたり、クリックジャック攻撃に使用されたりします。

説明
X-Frame-Options HTTP応答ヘッダーを使用すると、ページを「<frame>」、「<iframe>」、または「<object>」の形式で表示することをブラウザーに許可するかどうかを指定できます。サイトはこれを使用して、そのサイトのコンテンツが他のWebサイトに埋め込まれないようにすることで、クリックジャック攻撃を回避できます。

推奨事項
「DENY」または「ALLOW-FROM」ディレクティブを使用して、このWebサイトからの応答に次のヘッダーのいずれかを追加します。X-Frame-Options: DENY' X-Frame-Options: ALLOW-FROM https://example.com/'

2件の検出結果

ドメイン	初期URL	最終URL	リクエスト・チェーン	分析	前回確認日
xxxxx.com	https://xxxxx.com/	https://OOO.□□□.com/?tenant=aaaaaaaaaaaa	https://△△△.xxxxx.com/ https://OOO.□□□.com/?tenant=aaaaaaaaaaaa	Header missing	2021/3/31 22:58:37
証拠：					
xxxxx.com	https://xxxxx.com/	https://xxxxx.com/	n/a	Header missing	2021/3/24 16:23:08
証拠：					

HTTPSリダイレクト・パターンが安全ではありません

-0.4 スコアの影響

サイトのドメイン・リダイレクト設定がHTTPSヘッダーとHTTP Strict Transport Security（HSTS）ヘッダーのセキュリティ機能を制限しているため、なりすましサイトや悪意のあるサイトにユーザーがリダイレクトされる脆弱性があります。

格付けを含むセキュリティ関連の分析および本文書の内容に含まれる記述は、それらが実施・記述された時点での事業者の相対的な将来のセキュリティリスクに関する意見の記述であり、いかなる事業者との取引の安全性に関する現在または過去の事実の記述、いかなる事業者との取引の意思決定に関する推奨事項、いかなるデータまたは統論の正確性の支持、またはいかなる事業者のセキュリティ対策を独自に評価または保証する試みでもありません。セキュリティスコアカードは、(1) 特定の目的または用途に対する商品性または適合性の保証、(2) 正確性、結果、適時性、および完全性、(3) バグ、ソフトウェアエラー、およびウイルスのないこと、(4) コンテンツの機能が中断されないこと、および (5) コンテンツが任意のソフトウェアまたはハードウェア構成で動作することを含めて、明示的・目的的な全てに対して、保証を提供するわけではありません。当該組織のスコアカードのコメント欄で表明された見解および意見は、コメントの作成者のものであり、SecurityScorecardまたはその他関連組織の公式の方針、立場、または見解を反映するものではありません。

リスクスコアリング実例からよく発見されるリスク項目

本サービスをお申込みいただいた診断結果の傾向です。

対象ドメイン：　136
対象期間　　：　2023年7月～8月
スコア結果　：

カテゴリ	スコア平均
総　合	
ネットワーク	**８０(B)**
DNSの正当性	８７
パッチ適用頻度	８６
エンドポイント	９８
IPレピュテーション	９８
アプリケーション	**７４**
キューピット・スコア	１００
ハッカーチャッター	１００
漏洩された情報	１００
ソーシャル・エンジニアリング	１００

スコア平均が低かった2つのカテゴリにおいて、
多かった脆弱性の項目トップ５

ネットワークのカテゴリ

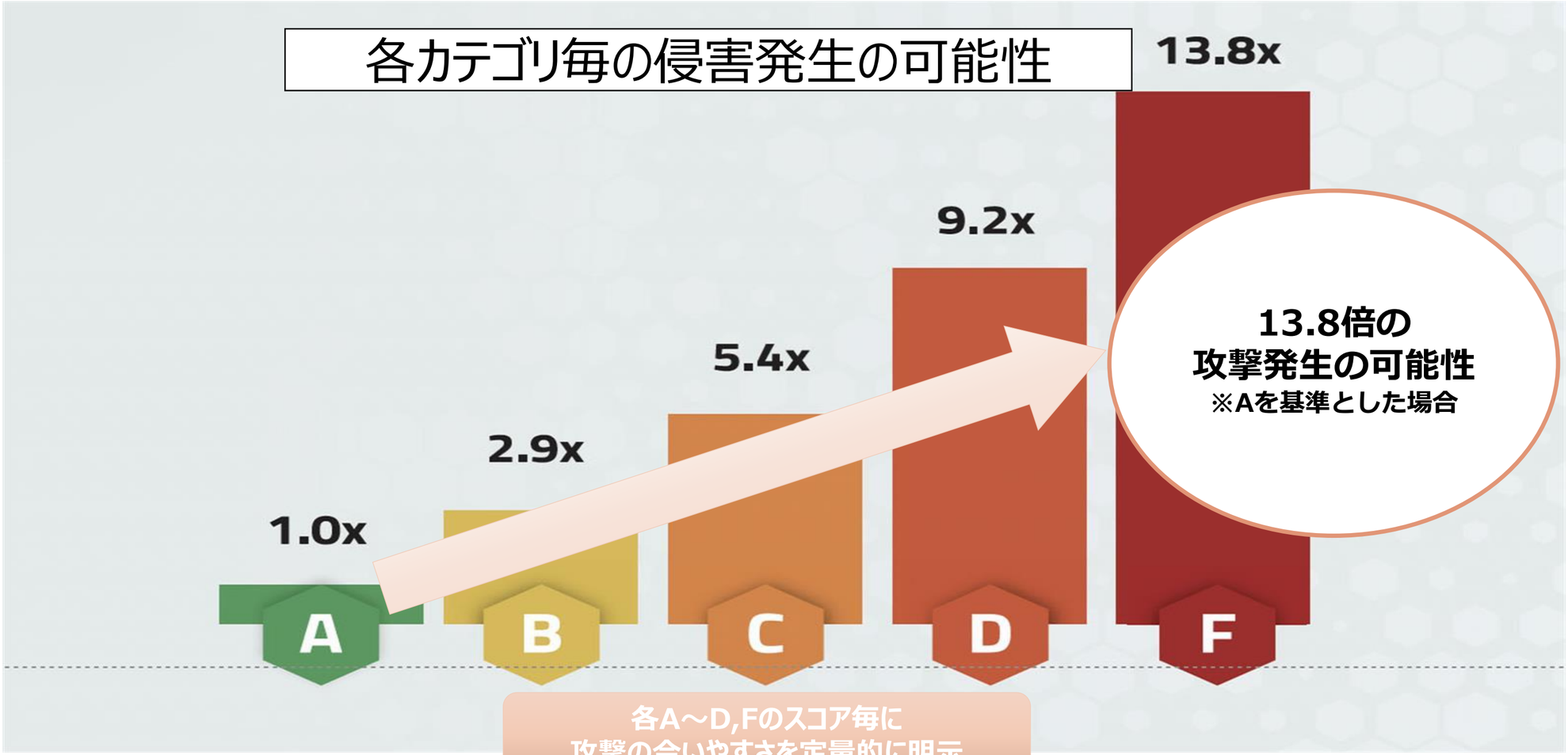
順位	項目
1	SSL/TLS サービスが脆弱なプロトコルをサポート
2	TLS サービスは弱い暗号スイートをサポート
3	証明書は自己署名されています
4	証明書の有効期限が切れています
5	失効管理のない証明書

アプリケーションのカテゴリ

順位	項目
1	コンテンツ・セキュリティ・ポリシー（CSP）がない
1	X-Frame-Options が推奨設定になっていない
3	X-Content-Type-Optionsが推奨設定になっていない
4	HSTSが推奨設定になっていない
5	HTTPSが適用されていない

攻撃されにくい環境を目指す重要性

SecurityScorecard社では、100点満点のスコアと合わせて、「A～D,F」の5段階のスコアを提示します。
それぞれのスコアで、「攻めづらさ」を定量的に判断することが可能です。



出典：サイバーセキュリティスコア（https://www.virosafe.no/cyber-security-score）

将来的に『サイバー攻撃を受ける可能性との相関性』をスコアで提示

提供機能③（リスク対策の推奨サービスレポート）

詳細レポートの各項目に対して、リスク低減対策に有効なサービスや対応をNTTコミュニケーションズオリジナルのリスク対策の推奨サービスレポートにて提示します。
必要な対策が簡単に分かるため、セキュリティ改善にすぐに活用できます。

重大度	項目	概要	対策案	推奨サービス
高	詳細レポートの各項目を記載します。 例） Certificate Is Revoked 証明書が失効しています	左記の項目について説明を記載します。 例）サーバの証明書がなんらかの理由で失効していることが確認されました。ウェブブラウザなどのTLSクライアントは証明書が失効しているサーバに対しての接続を拒否します。	左記項目について必要な対策案を提示します。 例）サービスを利用していない場合は証明書を廃止します。そうでない場合は認証局（CA）に連絡して新しい証明書の発行を手配してください。	NTTコミュニケーションズの具体的な推奨サービスを提示します。

NTTコミュニケーションズ
オリジナルの対策レポートを提供！

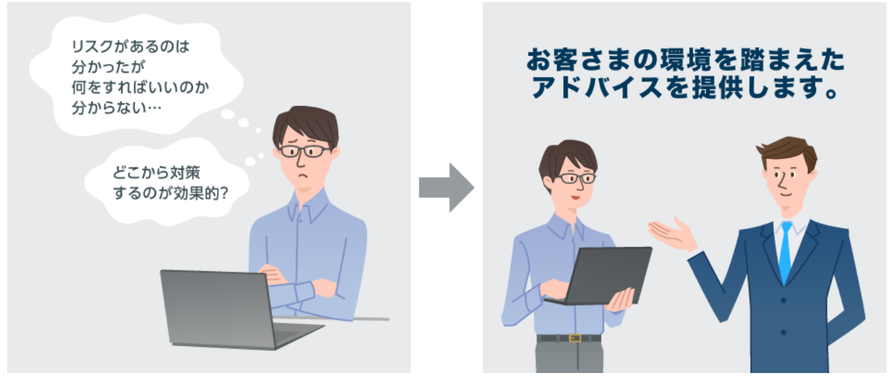
上記の様に詳細レポートで表示される重要度（高・中・低）の各項目について一覧で提供します。

提供機能④（診断レポート解説　※オプション）

オプションとして診断レポート解説がお申し込み可能です。

■対象範囲

・診断レポートの内容に関する解説と専門的アドバイスを提供します。
（10種類の診断カテゴリに分類された全項目）
・お申し込みいただいたドメイン（10ドメインまで）が対象です。
・10ドメインを超える場合はオプション契約が別途必要です。



■提供内容

項目	概要	所要時間	料金
診断レポートの解説	診断レポートの内容について解説を行います。	2時間程度	2チケット
診断レポートの解説とアドバイス	• 診断レポートの解説とお客さま環境のヒアリング • 診断レポート結果に対する専門的アドバイス • 実施報告書の提出	2～4時間程度	3チケット
個別相談	お客様の要件に個別に対応します。	相談	個別見積

※診断レポート解説（オプション）は80,000円（税込88,000円）/チケットです。２チケットからお申し込みいただけます。

オプション機能のご契約例(定期診断)

■**10ドメイン**を対象に**定期診断**と**診断レポートの解説オプション**を申し込む場合の請求料金

	単価	数量	料金
定期診断	20,000円/ドメイン(税込22,000円)	10	200,000円(税込220,000円)/月
診断レポートの解説	80,000円/チケット(税込88,000円)	2	160,000円(税込176,000円)
合計			360,000円(税込396,000円)

■**11ドメイン**を対象に**定期診断**と**診断レポートの解説オプション**を申し込む場合の請求料金

	単価	数量	料金
申込書1枚目			
定期診断	20,000円/ドメイン(税込22,000円)	10	200,000円(税込220,000円)/月
診断レポートの解説	80,000円/チケット(税込88,000円)	2	160,000円(税込176,000円)
申込書2枚目			
定期診断	20,000円/ドメイン(税込22,000円)	1	20,000円(税込22,000円)/月
診断レポートの解説	80,000円/チケット(税込88,000円)	2	160,000円(税込176,000円)
合計			540,000円(税込594,000円)

※オプションの料金につきましては1回あたりの料金となります

申込方法

本サービスのお申し込みは担当営業にお問い合わせください。

Web（ドコモビジネスオンラインショップ）からもお申し込みが可能です。
https://www.onlineshop.docomobusiness.ntt.com/TOPページから、
キーワードから探すを選択いただき「リスクスコアリング」と入力をお願いします。

※ドコモビジネスオンラインショップはお客さまご自身での注文のみ受け付けます。
※標準開通日は**12営業日**です。

その他、本サービスの提供条件などは、ドコモビジネスオンラインショップにも掲載しております。

参考）注意事項

- 定期診断の1回目およびスポット診断のレポートは、ご利用開始日に提供します。定期診断では、2回目以降は毎月1～10日の間に診断レポートを提供します。なお納期は通常12営業日です。
- 変更申込は、プランが”定期診断”の場合のみ対応しています。変更できる内容は、調査対象のドメイン、オプションメニューの追加です。
- 複数回の変更申込は受付をお断りさせていただく場合があります。
- 診断レポートは、レポート作成時点の最新情報で評価します。よって、定期診断の場合、先月から当月の間の情報での評価ではありません。無料診断やスポット診断同様に、毎月、レポート作成時点の最新情報で評価します。
- レポートの言語は、日本語または英語の選択ができます。
- Gmail、Hotmail、Yahoo!メールや、通信キャリア・ISP（インターネットサービスプロバイダー）が提供するメールドメインは診断対象外となります。また、診断対象ドメインが別のドメインのサブドメインとなっている場合など、一定の条件に該当する場合には診断対象外とさせていただくことがあります。
- 診断対象ドメインは、nslookupでDNS情報が取得できるものとします。
- 無料トライアルプランは、申込者が管理するドメインであることを当社が認めたものに限ります。具体的には、申込者のメールアドレスのドメインが診断対象になります。また、原則1社につき１回のお申し込みに限ります。

参考）WideAngle リスク診断サービスの特徴

	リスクスコアリング	サイバー保険付き脆弱性診断
利用シーン	セキュリティリスク対策について現状を把握したい	特定の自社システムのセキュリティリスクを無くしたい
利用方法	ドメイン情報の提示	対象システムをヒアリングして見積 実施内容の擦り合わせ
調査対象	ドメイン情報からハッカーと同じ手法で調査できる範囲 （自動化）	自社の特定のシステム （Webアプリ/サーバ/NW機器など）
調査範囲	広範囲	お客さま指定
提供期間	スポット（問合せ3ヶ月） 定期（月次レポート）	定期的（スポット）な実施 （1年に1回など）
価格（税別）	スポット：8万円/ドメイン 定期： 2万円/ドメイン	約40万円～
特徴	• 外部から見える脆弱性をスコア化 • 業界平均と比較 • お客さま環境への負荷がかからない調査方法	• サイバー保険を無償で自動付帯 • 高い品質・培ったスキルによる診断実績 • 充実したセキュリティ対策フォロー • 的確な診断報告書の提示

参考）市場ニーズと対策

まずは現状のセキュリティリスクを認識し、必要な対策は何かを把握することが重要です。
セキュリティリスクを可視化するニーズは市場でも高まっており、市場分析ではセキュリティスコアリングサービスの成長率（CAGR）が19.7%と非常に高い予測結果がでています。

順位	「組織」向け脅威	初選出年
1	ランサムウェアによる被害	2016年
2	サプライチェーンの弱点を悪用した攻撃	2019年
3	内部不正による情報漏えい等の被害	2016年
4	標的型攻撃による機密情報の窃取	2016年
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年
6	不注意による情報漏えい等の被害	2016年
7	脆弱性対策情報の公開に伴う悪用増加	2016年
8	ビジネスメール詐欺による金銭被害	2018年
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年

出典：IPA「情報セキュリティ10大脅威2024[組織]」

RANK	品目	2019年度実績（百万円）	2025年度予測（百万円）	CAGR（%）
1	SBOM/脆弱性管理サービス	800	10,500	53.6
2	**セキュリティスコアリングサービス**	**3,300**	**9,700**	**19.7**
3	スレットインテリジェンスサービス	4,800	13,300	18.5
4	電子認証サービス(運用管理サービス)	500	1,300	17.3
5	レッドチーム演習/ ペネトレーションテストサービス	1,600	4,100	17.0

出典：富士キメラ総研
2023ネットワークセキュリティビジネス調査総覧（市場編）

本サービスでは簡単に自社や関連会社のセキュリティレベル・情報資産が狙われるリスクを可視化し、対策案を提供します。

参考）提供内容（無料トライアル）

無料トライアルではセキュリティスコア結果のサマリーレポートと、対策サービスレポート、１カ月間のお問い合せサポートを提供します。無料トライアルの場合、調査ドメイン数は１ドメインまでで、お申し込みいただいたメールアドレスのドメインのみです。

※無料トライアルは、複数回申込がある場合はお断りさせていただくことがあります。