

# WideAngle プロフェッショナルサービス

## リスクスコアリング サービス仕様書

オーナー	NTT コミュニケーションズ株式会社 M&S 部セキュリティサービス部門
バージョン	1.14
日付	2024 年 11 月 28 日

WideAngle を利用するお客さまが対象です。

# 目次

1. はじめに.....	4
2. サービス概要.....	5
3. サービス仕様.....	6
3.1. サービス構成.....	6
3.2. 提供区分.....	6
3.3. 提供メニュー.....	7
3.4. 提供条件.....	7
3.5. 提供機能.....	8
3.5.1. サマリーレポート.....	8
3.5.2. 詳細レポート.....	9
3.5.3. リスク対策の推奨サービスレポート.....	12
3.5.4. レポートに関する問い合わせ.....	12
3.5.5. 診断レポート解説.....	12
3.6. スコア算出の仕組み.....	13
3.7. サービス品質.....	14
3.8. 提供地域.....	14
4. お客さま事前同意・制限事項.....	15
4.1. サービスの価格.....	15
4.2. お申し込み.....	15
4.2.1. 申込方法.....	15
4.2.2. 申込書.....	15
4.3. 標準開通日.....	16
4.4. 開通案内・配布同梱物.....	16
4.5. 受付業務.....	17
4.6. 工事・故障通知.....	18
4.7. 請求方法.....	18
4.8. 重要説明事項.....	19
4.8.1. ライセンスについて.....	19
4.8.2. 品質について.....	19
4.8.3. アクセス回線について.....	19
4.8.4. 最低利用期間.....	19
4.8.5. 料金について.....	19
4.8.6. 提供中止.....	20
4.8.7. 契約の成立.....	20
4.8.8. 契約の解除.....	20

4.8.9. 免責 .....	20
4.8.10. サービスの廃止 .....	20
<b>4.9. 留意事項 .....</b>	<b>21</b>
4.9.1. ご利用について .....	21
4.9.2. 注意事項について .....	21
<b>5. お問い合わせ連絡先 .....</b>	<b>22</b>
<b>改訂履歴 .....</b>	<b>23</b>

記載されている会社名や製品名は、各社の商標または登録商標です。

## 1. はじめに

WideAngleはNTTコミュニケーションズが提供する総合リスク マネジメント サービスのブランドです。

WideAngleプロフェッショナル サービス（略称：WideAngle PS）では、セキュリティ専門家の有する高度なナレッジやテクノロジーを、コンサルティング、インシデント レスポンス、脆弱性診断および脆弱性マネジメントといったカテゴリーでお客さまに提供します。

近年のサイバー攻撃の巧妙化や悪質化に伴い、企業のCISO・CIOにおいては増加するサイバー攻撃やグローバル化に伴う海外拠点への対応などが急務となっています。その一方、企業のIT 部門ではノウハウやリソースの不足等により、サイバー攻撃からの脅威に十分な対応ができていないのが現状です。

WideAngle PSはリスクの可視化、対策の検討、実施までのフェーズで必要なノウハウを提供することで、企業における迅速なセキュリティ対策の検討や導入、お客さまのセキュリティ向上を実施します。

リスクスコアリングはWideAngle PSの「CSIRT支援ソリューション」の1つです。攻撃者視点で、自社及びサプライチェーン全体の脆弱性が外部からどのように見えているかを把握し、継続的にモニタリングすることで、その結果「攻撃されにくい環境を維持し続ける」ことを可能にするソリューションです。

本書は、リスクスコアリングのサービス提供機能、利用条件、および注意事項などについて記述したものです。機能名や画面、メール文面は、予告なく変更される場合があります。

## 2. サービス概要

リスクスコアリングは、サイバーセキュリティリスククレイティングの「SecurityScorecard (SSC)」を利用したサービスです。ドメインをインプットに情報を収集して、セキュリティ対策状況を自動でスコアリングし、対策に有効な NTT コミュニケーションズの商材を併せてレポートします。

### スコアリングの流れ

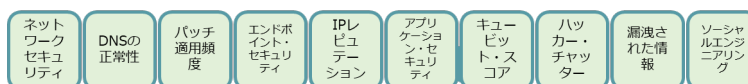
#### ▶ 調査対象のドメイン入力

調査対象のドメイン名をSSCスコアリングシステムに入力

#### ▶ データ収集と解析（常時情報収集実施）

Internet上の公開情報やハニーポット、マルウェア解析情報などを常時収集しており、調査対象のドメイン名をもとに、SSC社の持つデータと必要な場合はデータ追加収集により情報を解析

#### ▶ 10の検査項目によりスコアリング実施



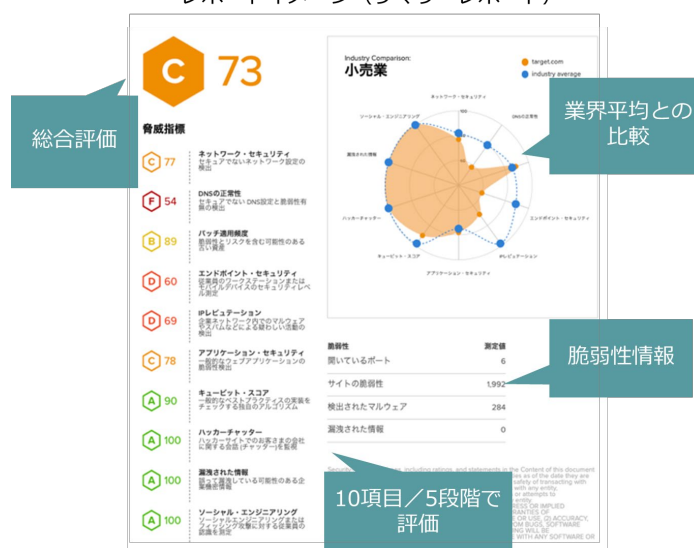
#### ▶ 全体スコアリングの実施

AからFまで分かりやすい指標でスコア化



SecurityScorecard

レポートイメージ（サマリーレポート）

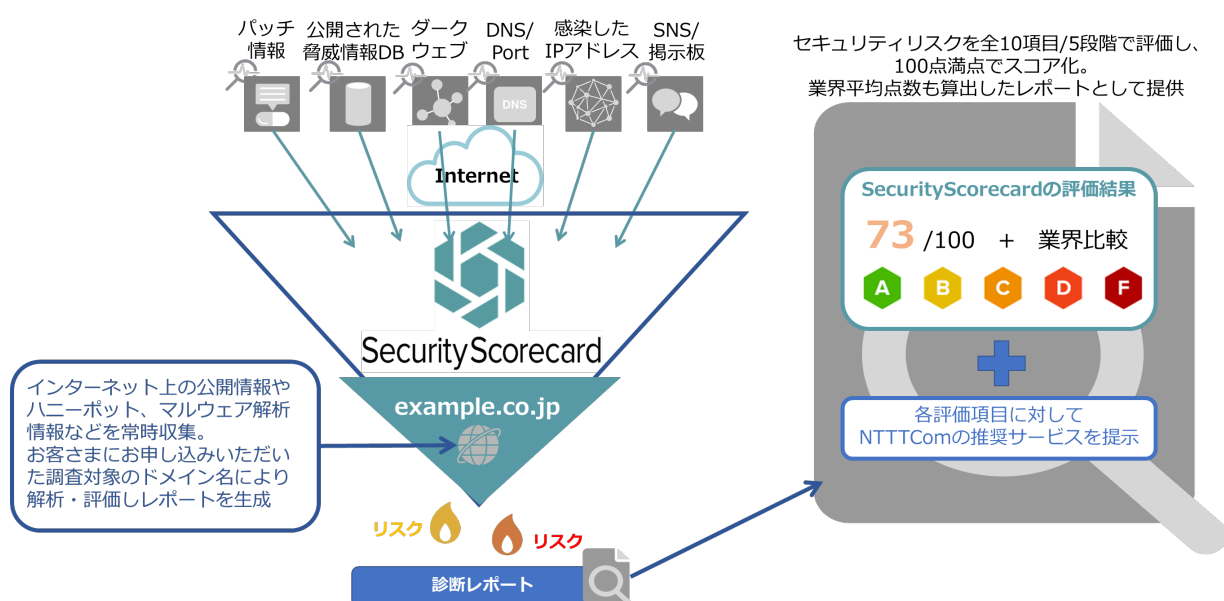


## 3. サービス仕様

### 3.1. サービス構成

当社にて、SecurityScorecard のポータル画面を操作して調査対象のドメインを入力します。

SecurityScorecard にて、そのドメイン情報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。当社にてその評価レポートと各評価項目に対しての推奨サービスを提示します。



### 3.2. 提供区分

SecurityScorecard のライセンスはサービス側（NSJ）が保有し、お客さまへライセンスの提供は行いませんので、お客さまにて SecurityScorecard のポータル画面を操作することはありません。サービス側で操作しお客さまへレポート提示します。

オプションの診断レポート解説にて、レポート結果の解説やアドバイスをを行います。

### 3.3. 提供メニュー

基本サービスが診断レポートの提示、オプションサービスが診断レポートの解説やアドバイスを行う診断レポート解説です。

区分	メニュー	内容	調査対象ドメイン数	サポート期間
プラン (基本サービス)	無料トライアル	<ul style="list-style-type: none"> <li>セキュリティリスクスコア結果の要約レポートを提供します（SSCのサマリーレポート）</li> <li>対策となるお勧めNTTComサービス例も提供します</li> <li>レポートの見方、サービスに関する問い合わせは、レポート提示からサポート期間内で受け付けます</li> <li>※サマリーレポートの項目についての具体的な内容は、スポット診断や定期診断を実施していただくことで確認できます。</li> </ul>	1ドメイン	1カ月
	スポット診断	<ul style="list-style-type: none"> <li>セキュリティリスクスコア結果の詳細レポートを提供します（SSCのサマリーと詳細レポート）</li> <li>対策となるお勧めNTTComサービス例も提供します</li> <li>レポートの見方、意味に関する問い合わせは、レポート提示からサポート期間内で受け付けます</li> </ul>	10ドメイン	3カ月
	定期診断	<ul style="list-style-type: none"> <li>スポット診断を定期的（毎月）に実施します。</li> <li>対策となるお勧めNTTComサービス例も提供します</li> <li>レポートの見方、意味に関する問い合わせは、契約期間中受け付けます。ただし結果に関連する内容は過去3回分までです</li> </ul>	10ドメイン	契約期間
オプション	診断レポート解説	<ul style="list-style-type: none"> <li>レポート結果の内容について解説、専門的アドバイスを行います。以下のチケットメニュー以外は個別相談です。 <ul style="list-style-type: none"> <li>✓ 2チケット：解説のみ</li> <li>✓ 3チケット：解説とヒアリング、専門的アドバイスと実施報告書</li> </ul> </li> </ul>	-	契約期間

### 3.4. 提供条件

- サービス区分は、プラン（基本サービス）とオプションがあり、オプションだけ新規で申し込むことはできません。
- 3つのプランは、同時に複数申し込みません。1契約で1つのプランのみお申し込みとなります。
- オプションメニューは、プランの“無料トライアル”には同時申込できません。“スポット診断”または“定期診断”に同時申込できます。
- 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。
- 3つのプランのプラン変更はできません。（ex. スポット診断から定期診断へのプラン変更）新たに新規申込をしていただきます。
- 無料トライアルやスポット診断後に、オプションの診断レポート解説を申し込む場合は、新たに新規申込で、スポット診断または定期診断をお申し込みいただき、そのオプションとして診断レポート解説をお申し込みいただきます。診断レポート解説のみのお申し込みはできません。
- 定期診断は、毎月1日～10日の間に診断レポートを送付します。

- 定期診断の変更申込した場合は、ご希望変更日が 1 日～10 日のものは、変更日当月のレポートから変更内容を適用します。
- 定期診断を廃止申込した場合は、廃止月のレポート未提出の場合は廃止日直前の診断レポートを送付します。
- 定期診断の最低利用期間は 1 年です。
- 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。無料トライアル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等、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。
- 日本語を含むマルチバイト文字をサポートしています。また日本語ドメインから英語ドメインにリダイレクトされているものは、そのリダイレクト先のドメインが表示されます。日本語ドメインのままリダイレクトされないものは、日本語のドメインとしてレポートに表示されます。（日本語.jp など）
- リダイレクト設定をしているドメインの場合は、リダイレクト先のドメインに対してのみ診断を行います。
- 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します。
- 無料トライアルは、原則 1 社につき 1 回のお申し込みに限ります。

### 3.5. 提供機能

#### 3.5.1. 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～F）のランクと 100 点満点の点数で行います。また同業種の平均も示します。各カテゴリは次の内容です。



セキュリティカテゴリ	概要	詳細説明
ネットワーク・セキュリティ	セキュアでないネットワーク設定の検出	例としては、オープンアクセスポイント、SSL証明書の安全性や設定の誤りなどの脆弱性の悪用、適切なセキュリティ対策の欠如に起因するデータベースの脆弱性やセキュリティホールなどがあります。
DNSの正常性	セキュアでないDNS設定と脆弱性有無の検出	OpenResolver構成などの複数のDNS構成設定、およびDNSSEC、SPF、DKIM、DMARCなどの推奨構成の存在を測定します。
パッチ適用頻度	脆弱性とリスクを含む可能性がある古い資産	組織がオペレーティングシステム、サービス、アプリケーション、ソフトウェア、およびハードウェアにタイムリーにパッチを当てているか否かを観察します。
エンドポイント・セキュリティ	従業員のワークステーションまたはモバイルデバイスのセキュリティレベル測定	組織のラップトップ、デスクトップ、モバイルデバイス、およびその組織のネットワークにアクセスするすべての従業員デバイスに関連する保護を指します。
IPレピュテーション	組織ネットワーク内でのマルウェアやスパムなどによる疑わしい活動の検出	独自のシンクホールシステムで、世界中のコマンドアンドコントロール（C2）インフラストラクチャから数百万のマルウェア信号を取り込みます。その後、感染した受信IPアドレスが処理され、IPアドレスの複数のストリームを通じ、そのIPアドレスが帰属する組織を特定します。
アプリケーション・セキュリティ	一般的なウェブアプリケーションの脆弱性検出	検出された脆弱性の例には、クロスサイトスクリプティング（XSS）またはSQLインジェクション攻撃が含まれます。
キュービット・スコア	一般的なベストプラクティスの実装をチェックする独自のアルゴリズム	Cubitスコアファクターは、公開されている管理ポータルに関連する重要なセキュリティと構成の問題のコレクションを測定するSecurityScorecard独自の脅威インジケーター。
ハッカーチャッター	ハッカーサイトでお客さまの会社に関する会話（チャッター）を監視	アクセスが困難なフォーラムやプライベートハッカーフォーラムなど、アンダーグラウンドチャッターの複数のストリームからの通信を継続的に収集。
漏洩された情報	誤って漏洩している可能性のある組織機密情報	キーロガー、データベースダンプ、その他の情報リポジトリを介して抜き取られる機密情報を識別。漏洩データまたは関連するメールアドレスを所有する組織を特定し、漏洩した情報が原因で組織がセキュリティインシデントに直面する可能性を評価します。
ソーシャルエンジニアリング	ソーシャルエンジニアリングまたはフィッシング攻撃に対する従業員の認識を測定	SNSアカウント、個人金融アカウント、悪用可能なマーケティングリストなどに従業員が組織アカウントを使用するなど、ソーシャルエンジニアリングされるリスクをはらんださまざまな要素を識別します。

### 3.5.2. 詳細レポート

サマリーレポートの 10 項目のカテゴリを、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。

エビデンス情報が詳細レポートに記載されない項目があります。お客さまからの要望により提示します。

セキュリティカテゴリ	重大度	項目
ネットワーク・セキュリティ	高	Certificate Is Revoked Network Attached Storage Device Exposed Product Running Vulnerable Log4j Version SSL/TLS Service Supports Weak Protocol TOR Server Detected UPnP Accessible
ネットワーク・セキュリティ	中	Apache CouchDB Service Observed Apache Cassandra Service Observed Cobalt Strike C2 server detected DNS Server Accessible Elasticsearch Service Observed FTP Service Observed HTTP Proxy Service Detected IMAP Service Observed Industrial Control System Device Accessible IP Camera Accessible LDAP Server Accessible LDAP Server Allows Anonymous Binding Microsoft SQL Server Service Observed Minicraft Server Accessible MongoDB Service Observed MySQL Service Observed Networking Service Observed OpenVPN Device Accessible Oracle Database Server Accessible POP3 Service Observed PostgreSQL Service Observed PPTP Service Accessible Printer Detected Pulse Connect Secure VPN Product Observed RDP Service Observed Redis Service Observed rsync Service Observed SMB Service Observed SOAP Server Accessible SOCKS Proxy Service Detected

セキュリティカテゴリ	重大度	項目
ネットワーク・セキュリティ	中	SSH Software Supports Vulnerable Protocol SSH Supports Weak Cipher SSH Supports Weak MAC Telnet Service Observed VNC Service Observed
	低	Apple AirPort Device Detected CDN Used Certificate Is Expired Certificate Is Self-Signed Certificate Lifetime Is Longer Than Best Practices Certificate Signed With Weak Algorithm Certificate Without Revocation Control Embedded IOT Web Server Exposed Mobile Printing Service Detected MySQL Server Running with Empty Password Product Potentially Impacted by CVE-2022-41040 & CVE-2022-41082 Product Potentially Impacted by PowerShell Remoting RCE Remote Access Service Observed TLS Service Supports Weak Cipher Suite ※
セキュリティカテゴリ	重大度	項目
DNSの正常性	中	Malformed SPF Record SPF Record Contains a Softfail without DMARC SPF Record Found Ineffective SPF Record Missing
パッチ適用頻度	中	Critical-Severity CVSS v3.0 Service Vulnerability in Last Observation Critical-Severity CVSS v3.0 Vulnerability Patching Cadence End-of-Life-Product End-of-Service Product High-Severity Vulnerability in Last Observation Low-Severity Vulnerability in Last Observation Medium-Severity Vulnerability in Last Observation Vulnerability observed in most recent scan
	低	High Severity CVEs Patching Cadence High-Severity CVSS v3.0 Service Vulnerability in Last Observation High-Severity CVSS v3.0 Vulnerability Patching Cadence Low Severity CVEs Patching Cadence Low-Severity CVSS v3.0 Service Vulnerability in Last Observation Low-Severity CVSS v3.0 Vulnerability Patching Cadence Medium-Severity CVEs Patching Cadence Medium-Severity CVSS v3.0 Service Vulnerability in Last Observation Medium-Severity CVSS v3.0 Vulnerability Patching Cadence
エンドポイント・セキュリティ	高	Outdated Operating System Observed Outdated Web Browser Observed
	低	Browser Average Age Indicates Older Versions
セキュリティカテゴリ	重大度	項目
IPレピュテーション	高	Malicious botnet C2 server detected Malicious Scan Detected Malicious TOR Exit Node Detected Malware Detected Potentially Vulnerable Application (PVA) Installation Ransomware infection detected Ransomware Infection Trail Detected
	中	IP on blacklist due to malicious Activity Known compromised or Hostile Host Mirai Botnet Traffic Detected SMTP Server on Unusual Port
	低	Active CVE Exploitation Attempted Adware Installation Adware Installation Trail Anonymous Open Proxy Attack Detected DOS Attack Attempt Detected Malicious TOR Relay/Router Node Detected Malicious User Agent Detected Malware Controller Observed Malware Infection Malware Infection Trail Potentially Vulnerable Application Installation (PVA) Trail Products Susceptible To Ransomware Exploits Exposed Unsolicited Commercial Email

セキュリティカテゴリ	重大度	項目
アプリケーション・セキュリティ	高	November 2022 OpenSSL 3.X vulnerability detected Redirect Chain Contains HTTP Session Cookie Missing 'HttpOnly' Attribute Session Cookie Missing 'Secure' Attribute Vulnerable VMWare ESXi Server Detected Website communicates with payment provider Website References Object Storage Websocket requests contain sensitive fields or PII
	中	High Severity Content Management System vulnerabilities Identified Insecure channel exposes sensitive information Low Severity Content Management System vulnerabilities Identified Medium Severity Content Management System vulnerabilities Identified Non-standard links detected:Unsafe File Transfer Protocol
セキュリティカテゴリ	重大度	項目
アプリケーション・セキュリティ	低	Browser logs contain debug Messages Certificate key is smaller than recommended size Content Security Policy Contains Broad Directives Content Security PolicyContains 'unsafe-*' Directive Content Security Policy(CSP) Missing ※ Critical-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation High-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation Insecure HTTPS Redirect Pattern Link redirects to insecure website Low-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation Medium-Severity CVSS v3.0 Content Management System Vulnerability in Last Observation Non-standard links detected: Contact information displayed Non-standard links detected: Local file path exposed Server certificate issued by country on denylist Server error detected Server with Expired Certificate Contacted Site does not enforce HTTPS Site Does Not Use Best Practices Against Embedding of Malicious Content Site emits visible browser logs Site fails to load page components Site links to insecure websites Site may use WebSockets to send user data Site receives data over Websockets Site requests data over insecure channel Unsafe Implementation Of Subresource Integrity Web application potentially vulnerable to Spring4Shell Website Hosted on Object Storage Website Does Not Implement HSTS Best Practices Website does not Implement X-Content-Type-Options Best Practices
セキュリティカテゴリ	重大度	項目
キュービットスコア	高	Ransomware-Susceptible Remote Access Services Exposed
ハッカーチャッター	高	Domain Advertised as Ransomware Victim
	中	Alleged Breach Incident
漏洩した情報	中	Cleartext password exposed Credentials at Risk Email exposed Exploit Attempt Detected Password hint exposed Security question and answer exposed Social Security number Exposed
	低	Attempted Information Leak Credentials at Risk (Historical) Employer exposed IP address exposed
ソーシャルエンジニアリング	低	Exposed Personal Information Exposed Personal Information(Historical)

### 3.5.3. リスク対策の推奨サービスレポート

詳細レポートの詳細項目に対して、リスク低減対策に有効なサービスや対応を提示します。

### 3.5.4. レポートに関する問い合わせ

レポートに関する問い合わせ受付の条件です。

項目	内容
お問い合わせ受付内容	<ul style="list-style-type: none"> <li>サマリーや詳細レポートの内容</li> <li>対策となるサービスの概要</li> </ul>
お問い合わせ対象外	<ul style="list-style-type: none"> <li>対策についての提案（提案のお問い合わせ先をご案内します）</li> <li>レポート結果の解説やアドバイス（オプションの診断レポート解説で行います）</li> </ul>
お問い合わせ期間	<ul style="list-style-type: none"> <li>レポート提示からお問い合わせ受付までの期間に制限があります。期間はお申し込みプランにより異なります。</li> </ul>

### 3.5.5. 診断レポート解説

診断レポート結果の内容について解説し、お客様環境を踏まえたアドバイスを行います。

#### ① 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）
- お申込みいただいたドメイン（10 ドメインまで）が対象です。

#### ② 提供内容

- 診断レポートの解説：2 チケット（2 時間程度）
- 診断レポートの解説とアドバイス：3 チケット（2～4 時間程度）
  - ✓ 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
- その他（個別相談）

#### ③ 提供条件

- 解説やアドバイスはリモート会議での対応とさせていただきます。
- リモート会議は 1 回実施としますが、解説とアドバイスをお申し込みの場合は、1 回（2 時間）で終わらない場合は 2 回目を実施させていただく場合もあります。
- 事前にお申し込みいただいたチケット数の内容を提供します。

- ・ お申し込みいただけるチケット数は2チケットまたは3チケットです。4チケット以上をご希望の場合は事前にご相談ください。
- ・ お申し込みいただいたドメイン数に関係なく最大 10 ドメインまで2チケットまたは3チケットで対応します。
- ・ お客さまのご要望内容によっては、追加のお申し込みが必要になります。
- ・ チケットの有効期限はスポット診断の場合は3カ月、定期診断の場合は契約期間内になります。
- ・ お客さま環境のヒアリングでは、お客さま情報の提示が必要になります。
- ・ サービス導入を見据えた具体的な提案（見積作成など）や導入サポートは行いません。各販売担当にて対応します。
- ・ 診断レポートの解説やアドバイスは日本語対応のみです。
- ・ お申し込み後の返金・キャンセルは受け付けません。
- ・ ご利用開始後のオプションに関する連絡は、wa-rs@ml.ntt.com で実施します。

#### ④ 提供の流れ

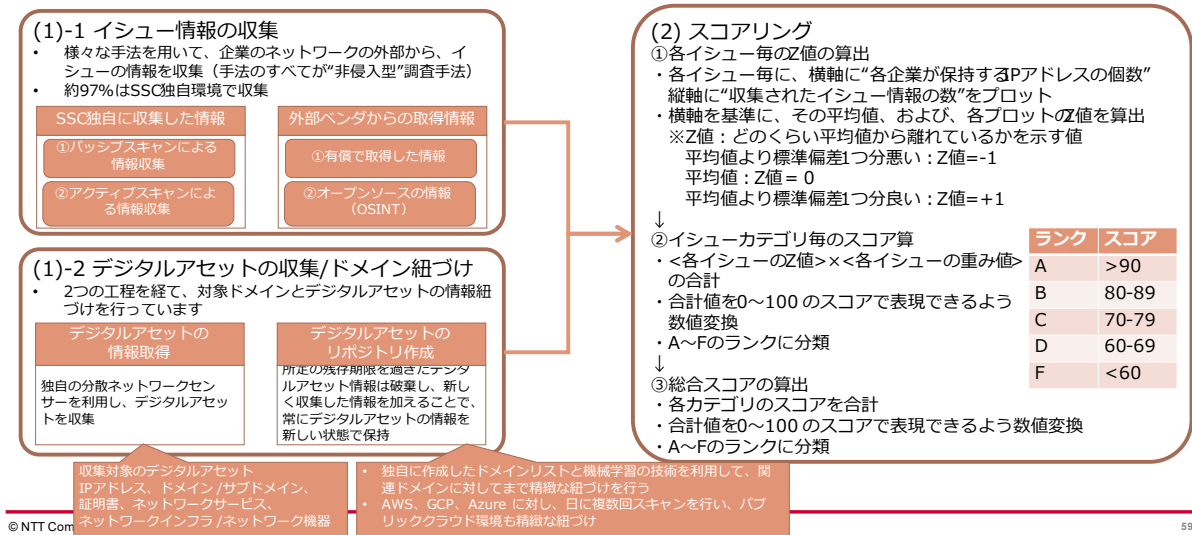
- ・ 診断レポートの送付先に営業が含まれる場合は、日程確認メールをお客さまと営業併せて送付します。



### 3.6. スコア算出の仕組み

SecurityScorecard のスコア算出は大きく 3 つの工程から成り立っており、精緻なスコアを迅速に計算

/表示させるために固有の技術を利用、工程の自動化に努めているため、精緻なスコアをタイムリーに提示可能です。



### 3.7. サービス品質

本サービスは、お客さまへレポートを提示する、もしくは、診断レポートの解説やアドバイスを提供するものであり、SLA は定めません。

### 3.8. 提供地域

日本契約を対象とし診断対象のドメイン利用地域に制限はありません。また、情報収集するサーバの場所を指定することはできません。

## 4. お客さま事前同意・制限事項

### 4.1. サービスの価格

スポット診断プラン、定期診断プランのレポートサービスは、診断対象のドメイン数により価格が決定します。オプションの診断レポート解説は、チケット数により価格が決定します。

スポット診断プラン、診断レポート解説はご利用月に一括料金請求とし、定期診断プランは月額料金とします。

### 4.2. お申し込み

#### 4.2.1. 申込方法

- 新設、変更、廃止の申込は、申込内容のパターンによって、申込方法が異なります。
- Web サイトからのお申し込みの場合は、NTTCom の法人向けモバイル・ICT サービス注文サイト「ドコモビジネスオンラインショップ」から注文します。
- 申込書でお申し込みの場合は、当社営業担当または、ドコモビジネスコンタクトセンターに注文します。

申込パターン	備考	Webサイト (ドコモビジネスオンラインショップ)	申込書
新設	診断プラン全て（無料トライアル/スポット診断/定期診断）対応します。	●	●
変更	診断プランが定期診断の場合のみ、変更申込対応しています。	-	●
廃止	診断プランが定期診断の場合のみ、解約時は廃止申込が必要です。 診断プランが、無料トライアル/スポット診断の場合は廃止申込は不要です。サポート期間終了をもって廃止扱い（解約）とします。	-	●
簡易変更	診断プランが定期診断の場合のみ、契約者情報の変更に対応します。	-	●

#### 4.2.2. 申込書

新設、変更、廃止の申込内容は次の項目とします。ご契約者情報の変更（譲渡/改称/継承等）は、サービス共通簡易変更申込書で対応します。



STEP (区分)	申込項目	申込単位	値	新設	変更	廃止	契約管理	保守管理
ご契約者情報	契約番号 (N番)	契約	N+数字9桁	-	●	●	●	●
	契約者名	契約	文字列	●	●	●	●	●
	契約者住所	契約	文字列	●	●	●	●	●
	契約担当者名	契約	文字列	●	●	●	●	●
	契約者電話番号	契約	数字、ハイフン要	●	●	●	●	●
	メールアドレス	契約	文字列	●	●	●	●	●
	請求書送付先 (会社名、住所、担当者名、電話番号、メールアドレス)	契約	文字列	●	-	-	●	-
商品情報	お申込日/ご利用開始希望日	契約	年月日	●	●	●	●	●
	診断プラン	契約	無料トライアル/スポット診断/定期診断	●	-	-	●	●
	診断レポート言語	契約	日本語/英語	●	●	-	●	●
	診断ドメイン数量	契約	1~10	●	●	-	●	●
	診断ドメイン情報 (01~10個)	ドメイン	文字列0~255文字 (ex. ntt.com)	●	●	-	●	●
	診断レポート解説チケット数	チケット	0~9999 (申し込みは2以上)	●	●	-	●	●
	レポート送付先メールアドレス	契約	文字列	●	●	-	●	●
	開通案内兼レポート用パスワード	契約	半角英数字8~10桁 (半角文字の英小文字、英大文字、数字の3種類の文字をすべて利用)	●	●	-	●	●
	レポート送付先営業 (会社名、担当者名、メールアドレス)	契約	文字列	●	●	-	●	●

### 4.3. 標準開通日

標準開通日は次の日程です。当社が申込を受理し、不備が無いことを確認された時点から起算した日数となります。尚、当日 15 時を過ぎた場合は翌営業日受付の扱いとなります。

申込種別	申込項目	標準開通日	納期の条件
新設		12営業日	オプションの診断レポート解説は、解説の日程調整等の最初の連絡をする日は、開通後から3営業日以内とします。
廃止	・ 定期診断のみ	5営業日	
変更	・ 定期診断のドメイン数や、対象ドメインの変更 ・ 定期診断のレポート言語の変更 ・ 定期診断の診断レポート解説追加	12営業日	オプションの診断レポート解説は、解説の日程調整等の最初の連絡をする日は、開通後から3営業日以内とします。

### 4.4. 開通案内・配布同梱物

- ・ 新設申し込み、変更申し込みの場合に開通案内を発行します。
- ・ 廃止申し込みの場合は開通案内等を行いません。
- ・ 開通案内と診断レポートは、別々に送付します。(定期診断の場合は、2回目以降は診断レポートのみ送付します)
- ・ 送付物は、開通案内が BOX、診断レポートが NTT コミュニケーションズの Biz ストレージファイルシェアサービスを利用して送付します。次の手順でファイルを受領していただきます。
  - ① お客さまへ送信元が次のメールアドレスからメールが届きます
    - (ア) 開通案内 : [wa-customer@ntt.com](mailto:wa-customer@ntt.com)
    - (イ) 診断レポート : Biz Storage File Share <admin@sharestage.com>



- ② お客さまは、メール本文の URL をクリックして、BOX または Biz ストレージファイルシェアサービスの Web サイトへアクセスします
- ③ ファイルダウンロードには、申込書に記載のパスワードを入力します
- ・ 各プランで送付するものは次のものです。

送付物	プラン	無料トライアル 新設	スポット診断 新設	定期診断 新設	定期診断 変更	定期診断 定期レポート
開通案内（ご利用内容のご案内）		●	●	●	●	-
診断レポート（サマリーレポート）		●	●	●	-	●
診断レポート（詳細レポート）		-	●	●	-	●
診断レポート（リスク対策の推奨サービスレポート）		●	●	●	-	●
診断レポート解説の実施報告書 ※1		-	○	○	○	-

※ 1 診断レポート解説の実施報告書は診断レポート解説（オプション）で 3 チケットをお申し込みのお客さまのみ実施後に送付します。

- ・ 診断レポートのファイル名は、次の命名規則です。  
日本語の場合
  - ① サマリーレポート\_契約番号\_診断ドメイン情報通し番号\_YYYYMM  
(ex. サマリーレポート\_N123456789\_01\_202107)
  - ② 詳細レポート\_契約番号\_診断ドメイン情報通し番号\_YYYYMM  
(ex. 詳細レポート\_N123456789\_01\_202107)
- 英語の場合
  - ③ summary\_契約番号\_診断ドメイン情報通し番号\_YYYYMM  
(ex. summary\_N123456789\_01\_202107)
  - ④ detailed\_契約番号\_診断ドメイン情報通し番号\_YYYYMM  
(ex. detailed\_N123456789\_01\_202107)
- ・ リスク対策の推奨サービスレポートは、次の命名規則です。  
日本語のみ      リスク対策の推奨サービスレポート\_バージョン番号  
(ex. リスク対策の推奨サービスレポート\_ 1.00)

## 4.5. 受付業務

- ・ サポートデスクにて、お客さまからのお問い合わせを受け付けます。

窓口業務	受付時間	手段	内容
お問い合わせ受付	平日(年末年始除く) 9:00~17:00	メール 電話	<ul style="list-style-type: none"> <li>レポートの内容に関する問い合わせ</li> <li>申込内容の変更に関する問い合わせ</li> </ul>

- 受付の対応目標値（SLO）は次の値とします。
  - ① メールでの受付は、営業日の 24 時間以内に返信します
  - ② 電話での受付は、応答率 80%以上とします
- お問い合わせには次の情報が必要です。この情報が一致することをもって、正当な権限に基づくお問い合わせや申請であることを認証します。正当な権限のないお問い合わせや申請は受け付けられません。

認証に必要な情報	例	備考
契約番号（N番）	N+数字9桁	開通案内のご案内に記載しています。
契約者名（会社名）	〇〇株式会社	お申し込みの契約者名（会社名）です。

- お問い合わせ受付は、営業担当からも受け付けますが、お客様からか営業担当からか確認します。

## 4.6. 工事・故障通知

- 計画工事の通知は、お客さまへのレポート提出に影響がある場合にのみ、事前にサポートサイトに掲載します（お客さまがサポートサイトにてメール通知設定された場合は、掲載時にメール通知されます）。
- 緊急工事や故障の通知は、お客さまへのレポート提出に影響がある場合にのみ、提出予定日が過ぎる前にサポートサイトに掲載します（お客さまがサポートサイトにてメール通知設定された場合は、掲載時にメール通知されます）。

## 4.7. 請求方法

- 本サービスでは、単独の契約番号（N 番）を発行し、その N 番あてに請求します。
- 利用料が 0 円の項目は表示されません。
- 税区分は、月額料金は合算、一括請求は個別の計算を行います。
- 例：請求書表示項目イメージ  
 スポット診断 x 3 ドメイン、定期診断 x 5 ドメイン、診断レポート解説 x 2 チケットの場合  
 ※定期とスポット診断の同時申込はできなので、仕様上両方表示はないので、イメージです。

ご利用料金内訳名	金額（円）	税区分	ご利用期間等のお知らせ
[Wide Angle リスクスコアリング]			
定期診断利用料	100,000	合算	7月ご利用分です。診断ドメイン数は5です
スポット診断料	240,000	合算	
診断レポート解説料	160,000	合算	
消費税等	***		

## 4.8. 重要説明事項

重要事項を記載します。その他利用規約の内容を遵守いただきます。

### 4.8.1. ライセンスについて

本サービスは、SecurityScorecard 社のサービスを利用していますが、SecurityScorecard 社とお客さまとの間に契約関係は生じません。

### 4.8.2. 品質について

本サービスは、SLA（Service Level Agreement）を規定しません。

### 4.8.3. アクセス回線について

本サービスの診断レポートは、メールでダウンロードサイトを通知しお客さまにダウンロードしていただきます。メールやファイルを受領するためのインターネット回線については、お客さまにてご準備ください。回線にかかる費用（ISP 料金を含む）は、本サービスとは別に発生し、ご利用になった通信会社から利用料金が請求されます。

### 4.8.4. 最低利用期間

定期診断プランは、最低利用期間を 1 年とします。この期間内に解約の場合は、残りの期間の利用料分を違約金としていただきます。

### 4.8.5. 料金について

- 本サービスの料金は利用規約 別紙 1 料金表に記載します。
- 本サービスのメニューの内、定期診断プランは月額料金とし、スポット診断プランと診断レポート解説は利用開始月に一括料金の請求とします。定期診断プランについて、同一月内に利用の開始及び契約の解除があった場合は、当該月の利用料は発生します。

- 定期診断プランを利用開始した最初の月の翌月以降に、サービスの数量の変更があった場合、当該月の月末時点の契約内容に基づいて料金が発生いたします。
- 契約の解除およびサービスの廃止があった月の月額料は、契約解除および廃止した時点の数量をもとに当該月の利用料を計算いたします。
- 契約解約日が含まれる月の全てのメニューの料金について、日割り計算はいたしません。
- お客さま都合により本サービス開通日までにご利用のご案内をお受取になれなかった場合は、本サービスの料金の返還はいたしません。

#### 4.8.6. 提供中止

当社は、災害・広域停電・インターネット障害・パンデミック等の事態が発生し、本サービスを提供することが困難な場合は本サービスの一部又は全部の提供を中止することがあります。

#### 4.8.7. 契約の成立

契約の成立は、お客さまからお申し込みを頂いた日をもって成立するものとさせていただきます。ただし、そのお申し込みに不備がある場合等、お承りできない事があります。また、お承りのご連絡は、ご利用開始時に通知する『ご案内』をもって代えさせていただきます。

#### 4.8.8. 契約の解除

お客さまが本サービスの利用規約に記載のお客さまの義務の規定に違反したとき、当社は契約を解除することがあります。

#### 4.8.9. 免責

- 当社は本サービスを現状有姿で提供するものであり、契約者は、当社が本サービスについて正確性、実現性、市場性、有用性、特定目的適合性、有効性を保証するものではないことを了承し、契約者の責において本サービスを利用するものとします。
- 当社は、本規約の変更等により契約者が本サービスを利用するにあたり当社が提供することとなっている設備、端末等以外の設備、端末等の改造又は変更（以下、この条において「改造等」といいます。）を要する場合であっても、その改造等に要する費用については負担しません。

#### 4.8.10. サービスの廃止

- 無料トライアル、スポット診断は、サポート期間またはオプションの実施期間終了をもって廃止扱いとします。

- 定期診断は、お客さまからの廃止申込により本契約は終了し廃止されます。

## 4.9. 留意事項

### 4.9.1. ご利用について

- 本業務では公開情報からお客さまの脅威となる情報を抽出分析して提供します。提供する情報は情報源、内容を含めて精査して精度を高めておりますが、古い情報や誤った情報を含むことがあります。また、脅威情報の検出については全ての脅威を検出することを保証するものではありません。
- 本資料で記載の調査手法・項目については攻撃手法や外部環境の変化、技術的要因、効率性の改善等の理由により変更する場合があります。同様に情報源、モニタリング対象についても NTT コミュニケーションズの判断によって変更する場合があります。
- 本業務内で提供する各種推奨事項の実行はお客さまの判断・責任において行われるものとします。
- 本業務で実施する調査手法や情報源は原則開示しません。
- 各種調査結果は状況に関して保証や意見表明などを行うものではありません。
- 本業務の中で発生した著作物に関する著作権は NTT コミュニケーションズに帰属します。お客さまの内部使用に限って利用は可能ですが、関連会社以外の第三者に配布・公開はできません。

### 4.9.2. 注意事項について

- 送付物は、送信元が "Biz Storage File Share <admin@sharestage.com>" からメール通知が届きますので、このドメインからのメールが受信でき、かつこのドメインからファイルがダウンロードできるようにしてください。
- 送付物をダウンロードする際のパスワードは、お申し込み時にお客さまに記載いただいたものを使用し当社から通知は致しません。また、定期診断プランで変更申込された場合は、それ以降の定期診断レポートをダウンロードする際のパスワードは、すべて変更申込時にお客さまが記載したパスワードを利用します。パスワードをお忘れの場合は、本サービスのサポートデスクまでお問い合わせください。
- 定期診断プランで診断ドメイン数を変更する場合は、当該月の月末時点の契約内容に基づいて料金が発生しますので、標準納期で対応可能な暦月の最初の平日を指定してください。
- 違約金発生期間は、当該契約のご利用開始日から起算します。
- 違約金は、当該契約の解約があった時点の月額料金を元に違約金発生期間末日までの未払い期間で計算します。
- 同業者様からのお申し込みはお断りすることがあります。あらかじめご了承ください。

## 5. お問い合わせ連絡先

本サービスのお問い合わせについては、ベストエフォートで対応しており、お問い合わせ内容により、翌営業日対応となることがあります。

内容	受付窓口	連絡先	受付時間
お申し込みWebサイト	NTTComの法人向けモバイル・ICTサービス 注文サイト 「ドコモビジネスオンラインショップ」	<a href="https://www.onlineshop.docomobusiness.ntt.com/">https://www.onlineshop.docomobusiness.ntt.com/</a>	24時間365日
ご利用開始前の サービスのお問い合わせ	ドコモビジネスコンタクトセンター	電話：0120-003300	平日(年末年始除く) 9:00～17:00
ご利用開始後の サービスのお問い合わせ	セキュリティアドバイザーセンター	電話：0120-525-279 E-Mail：wa-rs-support@ntt.com お問い合わせフォーム： <a href="https://support.ntt.com/wideangle-rs/inquiry/search">https://support.ntt.com/wideangle-rs/inquiry/search</a>	平日(年末年始除く) 9:00～17:00
料金に関するお問い合わせ	ビリングカスタマセンタ	電話：0120-047-128 <a href="https://www.ntt.com/b-charge">https://www.ntt.com/b-charge</a>	平日(年末年始除く) 9:00～17:00
サービス情報サイト	NTTComお客さまサポートサイト	<a href="https://support.ntt.com/wideangle-rs">https://support.ntt.com/wideangle-rs</a>	24時間365日
リスク対策の推奨サービスのお問い合わせや提案要望	NTTComお客さまサポートサイト	<a href="https://support.ntt.com/wideangle-rs">https://support.ntt.com/wideangle-rs</a> お問い合わせ>新規お申し込み・ご契約について	24時間365日

## 改訂履歴

バージョン	主な変更	日付
1.00	初版作成	2021 年 7 月 5 日
1.01	3.5.2 詳細レポートの項目更新 3.5.5 提供条件の記載一部修正、チケットの有効期限を追加 5 お問い合わせ連絡先にサポートサイトの情報を追加	2021 年 11 月 4 日
1.02	3.4 提供条件にリダイレクト設定しているドメインについて追加 3.5.5 診断レポート解説の対象範囲が 10 ドメインまでであることを追加 4.6 工事故障通知方法についてメール通知からサポートサイト掲載に変更	2021 年 12 月 3 日
1.03	3.4 提供条件に nslookup で DNS 情報取得できることを追加 3.5.2 詳細レポート項目の更新 3.5.5 提供条件の記載一部修正、提供フローの日程の変更 4.4 開通案内と診断レポートが別々送付に変更、リスク対策の推奨サービスレポートのファイル命名規則を記載 4.7 請求書の表示変更	2022 年 4 月 4 日
1.04	3.4 無料トライアルの提供条件を複数回はお断りさせていただくという記載をお申し込み 1 回限りと変更 3.5.2 詳細レポート項目の更新 4.2.1、5 法人コンタクトセンタの名称と連絡先と受付時間を変更 4.4 リスク対策の推奨サービスレポートのファイル命名規則を変更 5 お問い合わせ連絡先の変更	2022 年 7 月 1 日
1.05	4.2.1 ICT Business Mall で新設申込時のオプション受付対応可	2022 年 7 月 12 日
1.06	3.3 無料トライアルの内容記載変更 3.4 複数回の変更申込について記載 3.5.2 詳細レポート項目の更新 4.2.2 開通案内兼レポート用パスワードの英大文字は必須を削除	2022 年 12 月 8 日
1.07	3.5.5 診断レポート解説の説明時間と回数の記載変更 4.4 リスク対策の推奨サービスレポートの送付は、定期診断は新設時のみから毎月に変更	2023 年 4 月 3 日
1.08	3.5.2 詳細レポート項目の更新	2023 年 5 月 18 日
1.09	4.2.2 開通案内兼レポート用パスワードルールの変更 4.7 10 月請求（9 月利用分）から消費税の個別計算を合算に変更 5 ICT Business Mall の URL 訂正 5 料金に関するお問い合わせ先の連絡先メールアドレスを URL に変更	2023 年 11 月 15 日
1.10	3.5.2 詳細レポート項目の更新	2023 年 12 月 22 日
1.11	3.5.1. サマリーレポートの更新	2024 年 4 月 9 日

	3.5.2 詳細レポート項目の更新 3.5.5 診断レポート解説項目数の更新 3.6. スコア算出の仕組みの更新	
1.12	3.5.2. 詳細レポート項目の更新 4.2.1. 申込方法の ICT Business Mall 名称変更 5. お問い合わせ連絡先の更新	2024 年 6 月 4 日
1.13	3.5.2. 詳細レポート項目の更新	2024 年 10 月 11 日
1.14	3.5.2. 詳細レポート項目の更新、エビデンス情報が詳細レポートに記載されない項目の印※を削除	2024 年 11 月 28 日