|  |  |
| --- | --- |
| ***注意事項****：（巻末に詳細を記述* ***必ずお読みください****）*  本番環境に対し、インターネット経由でのセキュリティ診断の実施をご希望の場合、必ず**弊社診断機器からの通信経路の確保**をお願いいたします。この際、IPアドレスによるアクセス元規制や、攻撃検知時に通信を遮断する機器が存在すると、診断結果に影響を与えますので、事前の設定変更の必要がございます。**運用ご担当者とご調整**頂けますようお願いいたします。  注意事項の一覧は巻末 10.実施にあたっての注意事項 をご覧ください。 | 記入日　    年  月  日  記入者 |

|  |  |
| --- | --- |
| お客様社名 |  |

1. **診断対象システムの概要　(可能な範囲でご記入願います)**

|  |  |
| --- | --- |
| システム正式名称 |  |
| システムの利用目的 |  |
| 診断実施環境 | 本番環境  開発環境 　 保守環境 　 その他（     ）  ※開発環境や保守環境での診断を推奨致します。 |
| 開発言語 |  |
| リリース時期 | リリース済み  リリース前 （リリース年月     年  月） ※予定込み |

1. **診断対象のURLまたはIPアドレス　(必須)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No | URLまたはIPアドレス | ホスト名 | OS | Webサーバ, | APサーバ | フレームワーク | DBサーバ |
| (例) | http://www.nri-secure.co.jp | www.nri-secure.co.jp | RedHat Enterprise Linux 6.9 | Apache- 2.2.15-59.el6 | tomcat6- 6.0.24-105.el6\_8 | Struts 2.5.10 | MySQL 5.7 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |

※製品/バージョンについて、パッケージインストールの場合は、パッケージのマイナーバージョンまでご記入願います。  
　(例：rpm -q apacheの出力等)

1. **診断用ログインID・パスワード　(認証があるアプリケーションでは必須)**

|  |  |  |  |
| --- | --- | --- | --- |
| No | ログインID | パスワード | 権限 |
| １ |  |  |  |
| ２ |  |  |  |
| ３ |  |  |  |
| ４ |  |  |  |
| ５ |  |  |  |

※必ず5つご用意ください。5つ用意できない場合は別途担当者にお問い合わせください。

※所属グループによって閲覧できる情報や権限が異なるアプリケーションの場合は、グループや会社が異なるIDを含めるようにしてください。  
　(A社 → B社への成りすましの可否の診断に利用します。)

※同じグループに属する場合でも、権限によって利用できるメニューが異なるアプリの場合は、各権限のIDを含めるようにしてください。  
　(一般ユーザ → 管理者ユーザへの成りすましの可否の診断に利用します。)

1. **診断対象に関するヒアリング事項　(必須)**

Q1. 診断対象IPアドレスの運営組織について該当する物を選択してください。

自社管理  
 外部委託 (ホスティング)  
 外部委託 (クラウドサービス)

Q2. 前項Q1で「外部委託 (ホスティング)」または「外部委託 (クラウドサービス)」を回答された場合は、以下の事項にもご回答ください。外部委託先の情報をご回答ください。

1. 委託先：（     ）

例）　Amazon Web Service (AWS)、Microsoft Cloud(Azure)、Google Cloud、IIJ GIO など

2. 利用している委託先によっては、セキュリティ診断の際に事前申請が必要な場合があります。事前申請が必要か、また既に申請が完了しているかご回答ください。

事前申請が不要  
　 事前申請が必要（ 申請済み、 未申請）

※AzureおよびGoogle Cloudに対するセキュリティ診断の事前申請は不要となっています。

　【参考】

- Azure: https://learn.microsoft.com/ja-jp/azure/security/fundamentals/pen-testing  
- Google Cloud: https://support.google.com/cloud/answer/6262505?hl=ja

　※AWSに対するセキュリティ診断では、事前申請が必要となる場合がございます。診断対象サービスが下記参考リンク中の「許可されたサービス」に該当しない場合には、事前申請が必要となります。詳細はAWSへご確認ください。

【参考】

- AWS: https://aws.amazon.com/jp/security/penetration-testing/

※その他の委託先についての事前申請の必要有無は、お手数ですが貴社でご確認ください。

1. **事前に準備していただく資料　(可能な範囲でご提供願います)**

セッション管理に関する基本設計書 (または事前ヒアリング)  
 認証 (ログイン) に関する基本設計書 (または事前ヒアリング)  
 診断対象画面一覧  
 画面遷移図  
 ネットワーク構成図  
 Webサーバの公開ディレクトリおよびファイル一覧 (例：公開ディレクトリ上でのlsコマンドやdirコマンドの出力等)

1. **診断実施日時 (必須)**

|  |  |  |  |
| --- | --- | --- | --- |
| 実施日付 | 実施時刻 | 延長可否 | 延長時連絡 |
| 年   月   日  ～    年   月   日 | 開始時刻   時   分  ～  終了時刻   時   分 | 可　不可 | 連絡不要  連絡必要  連絡不通時の対応　続行　中止 |

|  |  |
| --- | --- |
| 予備日 | 年   月   日 |

1. **実施体制（必須）**

* 本シートにご記入いただいた個人情報につきましては十分注意の上取扱い、セキュリティ診断に関するお客様へのご連絡、お客様からのお問合せ・ご相談への対応以外の目的には使用いたしません。
* 個人情報の訂正・消去を希望される場合は、弊社担当営業宛て、その他個人情報についてのお問い合わせにつきましては下記までご連絡下さい。  
  NRIセキュアテクノロジーズ株式会社：personal@nri-secure.co.jp

|  |  |  |  |
| --- | --- | --- | --- |
| 会社 | 氏名 | 部署名 | 当日の連絡先 |
| お客様 |  |  | １：  ２： |
|  |  |  | １：  ２： |
|  |  |  | １：  ２： |
| お客様関係会社 |  |  | １：  ２： |
|  |  |  | １：  ２： |
| その他関係会社 |  |  | １：  ２： |
|  |  |  | １：  ２： |

|  |  |  |  |
| --- | --- | --- | --- |
| 会社 | 氏名 | 部署名 | 当日の連絡先 |
| 当社 | 藤原 健 | テクニカルアセスメント事業部 | １：050-3032-1288 ２：090-4814-9761 |
| 千葉 祐司 | テクニカルアセスメント事業部 | １：050-3085-0180 ２：070-2186-4841 |
| 野村 琳汰朗 | テクニカルアセスメント事業部 | １：050-3173-0987 ２：070-8849-7072 |
| 藤谷 知季 | テクニカルアセスメント事業部 | １：050-3173-4855 ２：070-8683-7002 |
| 王 サン | テクニカルアセスメント事業部 | １：050-3032-1289 ２：090-6715-4798 |
| 大熊 百馨 | テクニカルアセスメント事業部 | １：080-5497-8551 |
| 北澤 拓郎 | テクニカルアセスメント事業部 | １：050-3204-4374 ２：080-5075-4057 |

**備考欄**

　オンサイトでの診断実施の場合は当日所在場所をご記入ください。

　その他、ご連絡事項等ありましたらご記入ください。

|  |
| --- |
|  |

**重大な脆弱性が発見された場合の措置**

重大な脆弱性が発見された場合の連絡先をご記載ください。通常は電話連絡とさせていただいております。

|  |  |  |
| --- | --- | --- |
| 連絡 | 連絡手段 | 連絡先 |
| 必要  不要 | E-mail  電話 | １：  ２： |

**診断開始、終了時の連絡**　(通常はE-mailでの連絡とさせていただいております)

|  |  |  |
| --- | --- | --- |
| 連絡 | 連絡手段 | 連絡先 |
| 必要  不要 | E-mail  電話 | １：  ２： |

**報告書の送付先**

|  |  |  |
| --- | --- | --- |
| 氏名 | 所属 | E-mailアドレス |
| １：  ２： | １：  ２： | １：  ２： |

1. **その他 (貴社オフィスやコンピュータセンター等のオンサイトの診断時のみご記入ください)**

**診断実施時の立会人の連絡先**

|  |  |  |
| --- | --- | --- |
| 氏名 | 所属 | 当日の連絡先 |
|  |  |  |

**サーバ設置施設(コンピュータセンター)に関する情報**

|  |  |
| --- | --- |
| 実施場所 | 家屋外からの弊社担当者への連絡 |
| 施設名：     　　（  階     号室）  入退館申請 ：必要 不要  機材持込手続き：必要 不要 | 携帯電話使用可  　備付電話で可　（番号     ）  　連絡不可 |

**機材準備等**

|  |  |  |  |
| --- | --- | --- | --- |
| HUB/SWITCH | LANケーブル | 電源タップ | その他 |
| 持込不要  　お客様側準備  　NRIセキュア準備 | 持込不要  　お客様側準備　（  本）  　NRIセキュア準備（  本） | 持込不要  　お客様側準備　　（  本）  　NRIセキュア準備　（  本） |  |

**NRIセキュア診断端末用ネットワーク情報**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 機材 | 診断機用のIPアドレス注 | ネットマスク/デフォルトゲートウェイ | DNSサーバアドレス (必要な場合) | 疎通可能対象 （2．診断対象のNo.） |
| 2台 | IPアドレス：   ．   ．   ．  IPアドレス：   ．   ．   ． | ネットマスク ：   ．   ．   ．  デフォルトゲートウェイ：   ．   ．   ． | ．   ．   ． | No. |
| 2台 | IPアドレス：   ．   ．   ．  IPアドレス：   ．   ．   ． | ネットマスク ：   ．   ．   ．  デフォルトゲートウェイ：   ．   ．   ． | ．   ．   ． | No. |
| 2台 | IPアドレス：   ．   ．   ．  IPアドレス：   ．   ．   ． | ネットマスク ：   ．   ．   ．  デフォルトゲートウェイ：   ．   ．   ． | ．   ．   ． | No. |

（注）弊社が診断時に持ち込む、診断機用で利用するIPアドレスです。診断対象機器と同一セグメントで未使用のアドレスをご記入願います。  
セグメントが複数に分割されている場合は、全てのセグメントについて、診断機用IPアドレスをご記入願います。  
デフォルトゲートウェイは必要な場合のみご記入願います。

1. **システムに関する事前ヒヤリング事項　(可能な範囲でご記入願います)**

診断対象システムについて以下の質問事項にご回答願います。診断の精度向上に繋がりますのでご協力のほどお願いいたします。  
なお、診断対象システムにログイン認証が無い場合、もしくはログインに必要な認証情報を保持していない場合はQ11以降をお答え願います。

Q1. パスワードを連続して間違えた場合に該当アカウントを利用不能にする(ロック)機能はありますか？  
ある場合、何回連続してパスワードを間違えた場合にロックされますか？  
また、一定時間経過後にロックをシステムで自動解除する方式の場合、何分で解除されますか ?

はい (ロック回数：  回、ロック時間：    分)  
 いいえ

Q2. ログインIDの発行方式をお知らせください。

連番 (例: A00001、A00002、A00003)  
 ランダム (例: abq83456、bhy83124、ioq33234)  
 ユーザが設定する (ユーザIDを選べる)  
 メールアドレス・社員番号等の他の情報をログインIDとしている (利用している情報：     )  
 その他 (     )

Q3. 一定時間アクセスがなかった場合にログイン情報を無効にする(セッションのタイムアウト)機能はありますか？  
ある場合、何分でセッションが無効になりますか？

はい (タイムアウト時間：    分)  
 いいえ

Q4.データベースにパスワードを格納する際、暗号処理はありますか？ (平文のまま格納していない)  
ある場合、暗号学的ハッシュ処理か、可逆暗号処理の何れを利用していますか？

はい (ハッシュ処理を利用)  
 はい (可逆暗号を利用)  
 いいえ

Q5. 前項Q4で「はい (ハッシュ処理を利用)」以外を回答した場合、Q8へお進みください。  
ハッシュ処理の際、何らかの文字列を付加していますか？ (ソルト値を利用している)

はい   
 いいえ

Q6. 前項Q4で「はい (ハッシュ処理を利用)」以外を回答した場合、Q8へお進みください。  
ハッシュ処理の際、繰り返しハッシュ処理を行っていますか？ (ストレッチング処理を行っている)

はい   
 いいえ

Q7. 前項Q4で「はい (ハッシュ処理を利用)」以外を回答した場合、Q8へお進みください。  
ハッシュ処理に利用しているアルゴリズムをご記入ください

MD5  
 SHA-1  
 SHA-2 (SHA-224、SHA-256、SHA-384、SHA-512)  
 その他 (     )

Q8. パスワードに有効期限を設定していますか？ (一定期間経過時に強制変更する機能を実装していますか？)

はい (有効期限：  ヶ月)  
 いいえ

Q9. パスワード変更の際、ユーザが以前に使用したパスワードの再使用を制限していますか？

はい (過去何回分までの再使用を制限：  回)  
 いいえ

Q10. システム側で初期パスワードをユーザに付与する仕様の場合にご回答ください。  
初回ログイン時にユーザによるパスワード変更を強制していますか？

はい   
 いいえ  
 システム側で初期パスワードを付与していない

Q11. システムのサポートブラウザの種類・バージョン情報をお知らせください。

(     )

例: Microsoft Internet Explorer 11以降、Google Chrome 54 以降

Q12. クレジットカードに関連する情報を処理するシステムの場合にご回答ください。  
ユーザから入力されたクレジットカード情報について、自社/カード会社/決済代行会社が行う本人確認方式として「クレジットカード番号」「有効期限」の確認以外のものがあれば以下から選択してください。

3Dセキュアによる認証  
 セキュリティコードによる認証  
 何らかの本人属性の検証 (カード名義人、配送先情報など)  
 なし

Q13. クレジットカードに関連する情報を処理するシステムの場合にご回答ください。  
以下のクレジットカードに関連する情報から、データベース等システムに保管しているものを選択してください。  
また、クレジットカード番号に関しては、保管する際の暗号化の有無についても回答してください。

クレジットカード番号 (暗号化：有・無)  
 セキュリティコード (CVS2/CVV2/CID等、カードの裏面等に記載されている3～4桁のコード)  
 暗証番号  
 クレジットカードに関連する情報を保管していない

Q14. 診断対象の環境にWAF (Web Application Firewall) を導入されていますか？  
導入している場合、プロダクト/サービス名をお知らせください。

はい (プロダクト/サービス名：     )  
 いいえ

Q15. 診断対象システムの構築においてCMS (コンテンツ管理システム) を利用していますか？  
利用している場合、プロダクト名、バージョン、利用プラグイン名をお知らせください。(複数記述可)

はい (プロダクト名：     　バージョン：      　プラグイン名：     )  
 いいえ

Q16. 診断対象システムにおいてユーザがファイル（画像、文書等）をアップロードできる機能はありますか？  
ある場合、悪意のあるファイルのアップロードを検知する仕組み（アンチウイルス、IDS/IPS等）を導入していますか？

はい（何らかの検知機構を　導入している　導入していない）  
 いいえ

Q17. 診断対象システムにおいてユーザがファイル（画像、文書等）をアップロードできる機能がある場合、GhostscriptあるいはGhostscriptに依存するソフトウェア（ImageMagick等）を利用していますか？  
利用している場合、バージョンをお知らせください。  
(本項はGhostscriptの深刻な脆弱性（CVE-2021-3781）の影響確認のための質問です)

はい (バージョン：     )　※例: Ghostscript/GhostPDL 9.50  
 GhostscriptあるいはGhostscriptに依存するソフトウェアを利用していない。

Q18. 診断対象システムにおいて、大量不正ログイン試行に対して特別なリスク低減策を取っていますか？  
以下に例を挙げますので該当するものがあれば選択してください。  
(本項は近年問題となっている "リスト型アカウントハッキング" のリスク評価のための質問です)

ログイン試行数、ログイン失敗数の異常増の検知  
 ユーザが普段とは異なる環境からログインする場合の検知  
 攻撃利用疑義IPをブロックする仕組み、または手順の整備  
 不正ログイン被害疑義アカウントを保護する仕組み、または手順の整備（例: アカウントの強制ロック、強制パスワード変更）  
 一時的に認証を強化する仕組み（例: ログインフォームへのCAPTCHA追加）  
 一時的に重要処理を行う機能を凍結する仕組み（例: ポイント交換機能の一時停止）  
 休眠アカウントの凍結・削除  
 その他（     ）

Q19. 診断対象システムにおいてOSとしてLinux/Unixを採用している場合、標準採用しているShellはBash (Bourne again shell) ですか？  
Bashの場合、バージョンをお知らせください。  
(本項はBashの深刻な脆弱性、通称“ShellShock”の影響確認のための質問です)

はい (バージョン：     )　※例: bash-4.1.2-15.el6\_5.2  
 Linux/Unixを利用していない、またはShellにBashを採用していない

Q20. 診断対象システムにおいてOSとしてLinux/Unixを採用している場合、利用しているCライブラリはglibc (The GNU C Library) ですか？  
glibcの場合、バージョンをお知らせください。  
(本項はglibcの深刻な脆弱性、通称“GHOST”の影響確認のための質問です)

はい　（バージョン：     )　※例: glibc-2.12-1.149.el6\_6.5  
 Linux/Unixを利用していない、またはCライブラリにglibcを採用していない

Q21. 診断対象システムにおいて、Javaベースのログ出力用ライブラリApache Log4jを採用している場合、log4j-coreの利用バージョンをお知らせください。  
※log4j-coreの存在有無は、ビルドツール (Maven、Gradle等) で依存ライブラリを確認するほか、プロジェクトにおいて "log4j-core-\*.jar" の名称に合致するファイルを検索することで確認可能です。  
(本項はApache Log4jの深刻な脆弱性、CVE-2021-44228の影響確認のための質問です)

はい　（バージョン：     )　※例: log4j-core-2.14.1  
 Apache Log4jを採用していない、またはApache Log4j のlog4j-coreを利用していない

Q22. 診断対象システムにおいて、Spring Framework (またはその派生フレームワーク)を採用している場合、Spring Frameworkの利用バージョンをお知らせください。  
(本項はSpring4Shellの深刻な脆弱性、CVE- 2022-22965の影響確認のための質問です)

はい　（バージョン：     )　※例: Spring Framework 5.3.0  
 Spring Frameworkを採用していない

Q23. 前項Q22で「はい」と回答し、ご記載のプロダクトのバージョンが「Spring Framework5.3.17以前」、「Spring Framework 5.2.19以前」、  
「Spring Framework5.1.x」、「Spring Framework5.0.x」もしくは「4系以前のプロダクト」を採用している場合、該当する項目をお知らせください。

実行環境のJDK（Java Development Kit）またはJRE（Java Runtime Environment）のバージョンが9以上である  
 スタンドアロン版Apache Tomcat（10.0.19以前、9.0.61以前、または8.5.77以前）をサーブレットコンテナとして採用している  
 WARファイルとしてパッケージ化し、実行環境へ展開している  
 spring-webmvc または spring-webflux を依存関係にもつ

1. **実施にあたっての注意事項（必ずお読みください）**
   * + - インターネット経由での実施をご希望の場合、弊社診断機器のIPアドレスから診断対象機器へのアクセス経路を確保して頂く必要があります。  
         弊社FNCサービスをご利用の場合も、サービス申込者の責任において当該作業の実施をお願いします。
       - 本サービスの実施にあたり、FW（ファイアウォール）やIDS（侵入検知システム）の設定変更など、お客様のシステムへの何らかの変更作業が生じる場合があります。その際は、サービス申込者の責任において当該作業の実施をお願いいたします。
       - インターネット側から診断を実施する場合に、弊社で利用するIPアドレスは以下の通りです。

➢113.157.195.208/28 ➢113.157.217.178～179 ➢118.238.8.48/28 ➢118.238.210.75　➢133.250.179.86～90

* + - * 診断対象システムにメール送信機能が含まれる場合、診断の一環として弊社の診断用メールサーバ宛にメールを送信する場合があります。  
        診断で利用するメールサーバのドメインは以下の通りです。

➢ @wa.red-infra.jp ➢ @nri-secure.co.jp

メールの送受信を特定のドメインに制限している場合は上記ドメインを許可するようにお願いいたします。

* + - * IDS/FW/その他の監視システムが導入されている場合、本サービスの実施によって、検知ログが大量に出力される可能性があります。監視運用への悪影響を防ぐため、事前に関係者に周知の上、「診断作業中は監視を停止する」、「監視の除外設定をする」、「アラートを無視する」といった措置をお願いいたします。
      * IDS/FW/その他の監視システムにおいて、攻撃を検知した際に攻撃元のIPアドレスからの通信を遮断する機能が有効になっている場合があります。これらに該当する機能が有効になっている場合には、診断実施前に解除をお願いします。
      * 正しい検査結果を得るためには診断作業時に対象機器が正常に動作していることが必要です。そのため、診断作業の前後で対象機器の再起動を行っていただくことを推奨いたします。
      * 正しい検査結果を得るためには診断作業時に対象アプリケーションの各機能に正常にアクセス可能であることが必要です。そのため、データ処理を前提とする機能においては、診断の前に最低限度必要なデータ投入をお願いいたします。
      * 診断開始時点で対象システムの診断準備が整っていない場合、予定している診断作業が期間内に終了しない可能性がございます。診断に必要なデータの投入、対象画面への疎通確認など、診断開始前までに診断作業のご準備をお願いいたします。  
        また診断実施開始の5営業日前より、対象システムへのアクセスが可能か、対象画面へのアクセスが可能か、必要なデータが揃っているかを確認させていただく場合があります。
      * 正しい検査結果を得るために、診断期間中に機器・アプリケーションの設定/更新/入替はお控えください。どうしても必要な場合、弊社診断担当者までご連絡ください。
      * サービス申込者が正当に所有権又は使用権を有さない第三者のシステム（ASPシステム等）を、第三者の了承無く本サービスの診断対象とすることはできません。この場合、当該第三者から直接、本サービスに申し込んで頂く必要があります。
      * 診断対象としてご指定頂くIPアドレスはサービス申込者により正当な権限に基づき管理されているものであることを前提とします。

また、本サービスでは擬似攻撃を行うため、稀に診断対象機器やその経路上にあるネットワーク機器に予想外の影響を及ぼす場合があります。  
下記注意事項についてご理解のほど、よろしくお願いいたします。

* + - * 診断作業が継続できない何らかの問題が発生した場合、診断作業を中断する場合があります。
      * 対象システムのリソース（CPU/HDD/メモリ）に余裕が無い場合、対象システム内のネットワーク機器に不具合がある場合など、動作状況によっては対象システム群の全部または一部の機能停止、もしくは対象システム群が提供するサービスの停止等の事態を引き起こすおそれがあります。診断作業時は対象システムの通常のご利用を停止していただくか、サービス停止の発生を前提とした調整及び措置をお願いいたします。
      * 診断作業を通じてデータの作出・更新・削除が複数回発生します。特に利用時にシステム管理者等へのメール送信を伴う機能が存在する場合、大量にメールが送信される場合があります。
      * 擬似攻撃を行うことでシステムの運用に影響が出ることに関して弊社が責任を負うものではありません。

# **その他**

その他、診断にあたっての特記事項等、診断担当者への連絡事項があればご記入ください。

以上