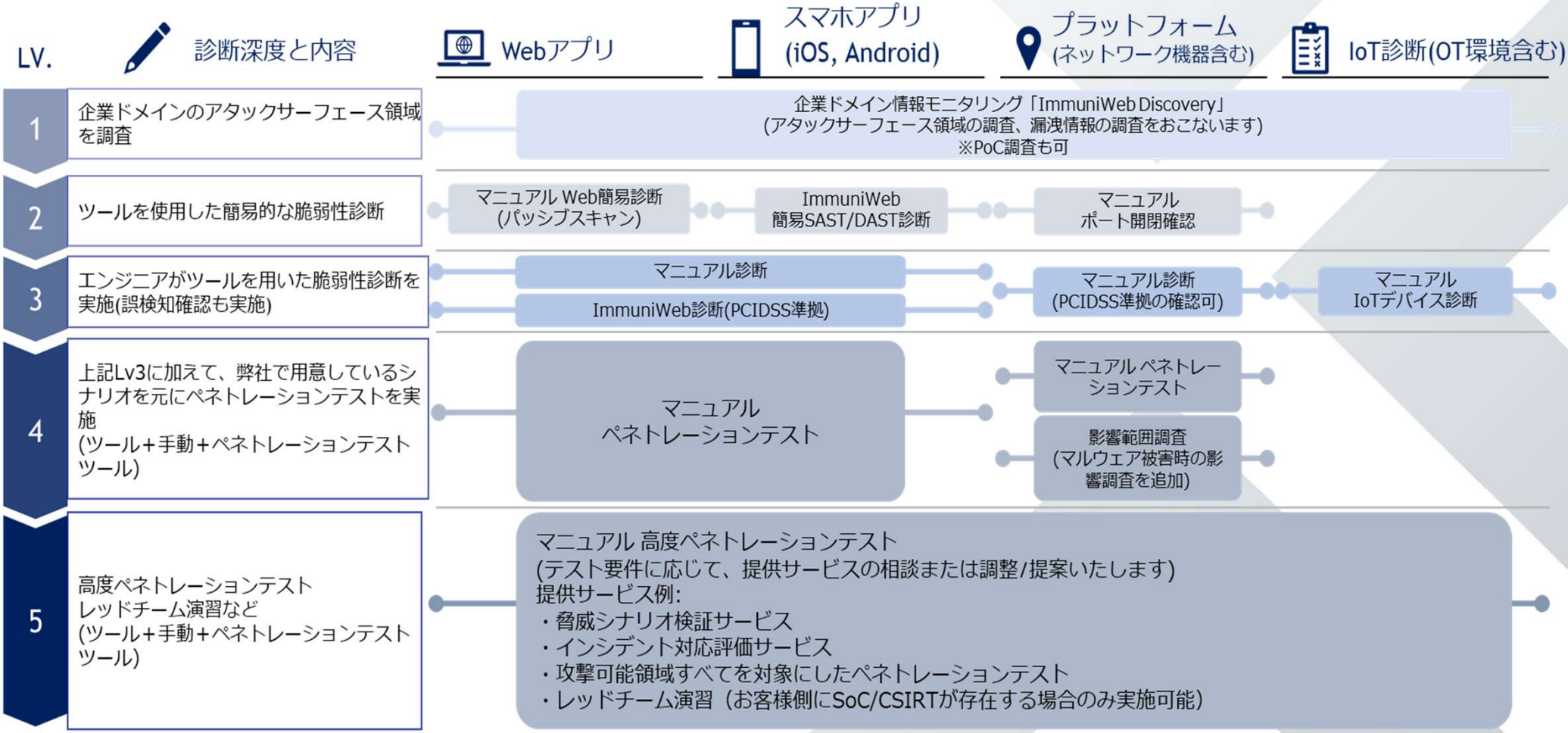
AIプラットフォーム脆弱性診断

ImmuniWeb

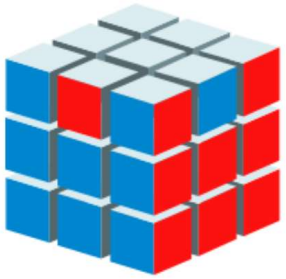
～セキュリティ　診断ソリューション～

セキュリティ　診断ソリューション

- 一般的な脆弱性診断は下記のLv.3が該当いたしますが、より高度な内容のセキュリティ検査にも対応致します



AIプラットフォーム脆弱性診断



ImmuniWeb®

Immuniwebは「IPA 情報セキュリティサービス基準適合サービスリスト」に掲載されています

インテリジェントな自動化とアクセラレーションのためのAI

ImmuniWebは、受賞歴のあるAIテクノロジーを活用して、面倒なタスクやプロセスのインテリジェントな自動化と加速を実現し、セキュリティの専門家を強化していますが、人間に取って代わるものではありません。

AIと人間の知能の相乗効果により、人々が人間の知性に真に値する高度なタスクのみを処理する場合、世界のアプリケーションセキュリティ市場で最も競争力のある価格で最高の品質を提供します。

AIプラットフォーム脆弱性診断　Immuniweb

海外での評価も高いAIプラットフォーム脆弱性診断サービスを2018年より国内初提供

第2世代
ツール＆HUMAN

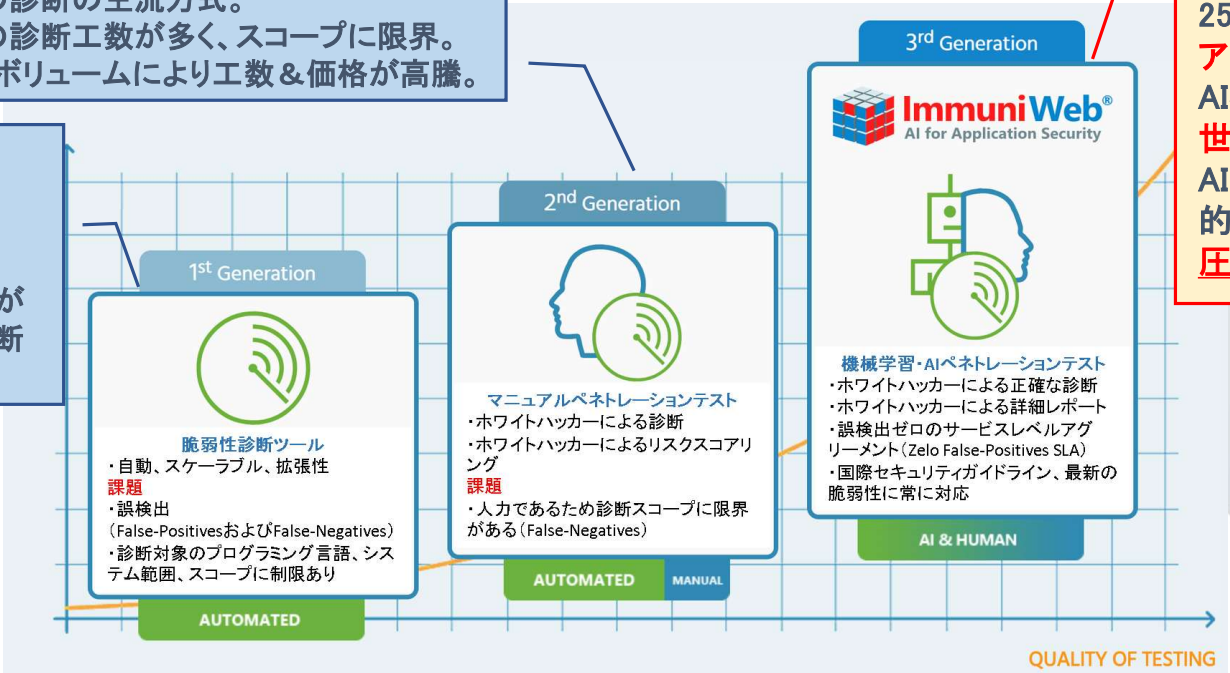
現在の診断の主流方式。
人力の診断工数が多く、スコープに限界。
サイトボリュームにより工数＆価格が高騰。

第1世代
ツール診断のみ

価格が安かったが誤検知が多く、SQLやXSSなどの診断不可など制限が多かった。

第3世代
AIプラットフォーム＆HUMAN

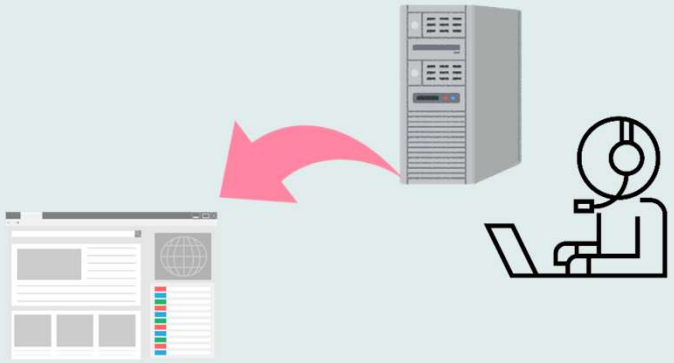
250台以上のインスタンスを組んで
アプリケーションを網羅的に診断。
AI機械学習により
世界中のガイドラインに準拠。
AIで対応困難なページはエンジニアに自動的にエスカーレーション。
圧倒的に優れたコストパフォーマンス。



AIプラットフォーム脆弱性診断　Immuniweb　イメージ

現行：他社の脆弱性診断

1台の診断マシンと1名～2名のエンジニア

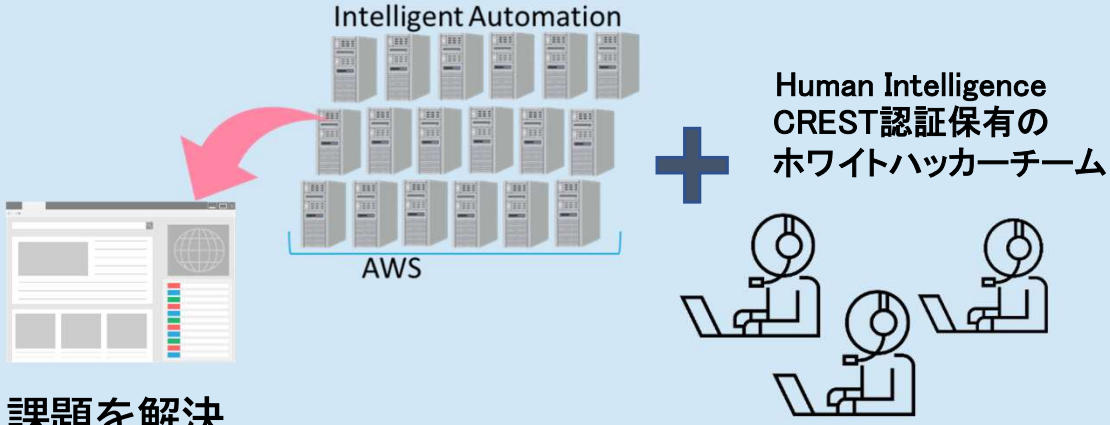


課題

★工数がかかるため、エンジニアの知見に頼る
全てのページを均等に検証している時間は無いので、
エンジニアの知見に頼る診断により工数を可能な限り削減。
★最新の情報までは蓄積出来ていない
常に最新のガイドラインやコードをエンジニアが学習する
わけにいかない。情報のタイムラグがある。
★1回の診断で時間もコストもかかりすぎる
サイトボリュームに応じて工数がかかる。

第3世代：AIプラットフォーム脆弱性診断

250台のマシン＋セキュリティスペシャリストのエンジニア



課題を解決

★AI×ホワイトハッカー
250台のマシンによる分散診断を用い、AIの優れた検査アルゴリズム
によって危険度の高い箇所を優先的に診断＆ホワイトハッカー（診断
スペシャリストエンジニア）のサポートにより誤作動、誤検知を防ぐ。
（結果をエンジニア検証して誤検知確認）
★12時間ごとに最新情報を蓄積
常に最新のガイドラインや攻撃コードをAIが機会学習しています。
★脆弱性診断はスピードが重要
最新の情報で素早く診断、素早く改修することが脆弱性診断では
重要となります。どんなに大きなサイトも8営業日で診断可能。

特長①　世界中のガイドラインを網羅

12時間ごとに最新ガイドラインをアップデートにより、常に最新情報での診断が可能！
OWAWSP Top10やSANSはもちろん、NIST・PCI DSS・HIPPAなどのガイドラインにも準拠。

国際セキュリティガイドライン	
米国	NIST (National Institute of Standards and Technology)
	FedRAMP (The Federal Risk and Authorization Management Program)
	ISACA (Information Systems Audit and Control Association)
英国	CREST (The Council of Registered Ethical Security Testers)
	UKAS (United Kingdom Accreditation Service)
欧州	EU GDPR (EU General Data Protection Regulation)
	TIBER-EU FRAMEWORK (Threat Intelligence-based Ethical Red Teaming)
金融業界	PCI DSS (Payment Card Industry Data Security Standard)
ヘルスケア	HIPAA (Health Insurance Portability and Accountability Act of 1996)
国際機関	ISO (International Organization for Standardization)
	ITU (International Telecommunication Union)

あらゆる最新の攻撃手法を網羅
OWASP (The Open Web Application Security Project), OWASP Top10, OWASP MOBILE Top10
SANS Institute, SANS Top25
CWE(Common Weakness Enumeration),MITRE
CVE(Common Vulnerabilities and Exposures),MITRE
Common Attack Pattern Enumeration and Classification (CAPEC),MITRE
ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge),MITRE
CVSS(Common Vulnerability Scoring System),FIRST
ITIL(Information Technology Infrastructure Library)

日本国内セキュリティガイドライン
内閣サイバーセキュリティセンター（NISC）
経済産業省(METI)
情報処理通信機構（IPA）
金融情報システムセンター（FISC）
日本コンピューターセキュリティインシデント対応チーム協議会（JP-CSIRT）
日本ネットワークセキュリティ協会(JNSA)

特長②　世界での高い評価と蓄積された実績

ImmuniWebサービス（スイス）は2015年に世界リリースされ数多くの金賞受賞！

40,390,000件以上
WEBアプリセキュリティテスト実績

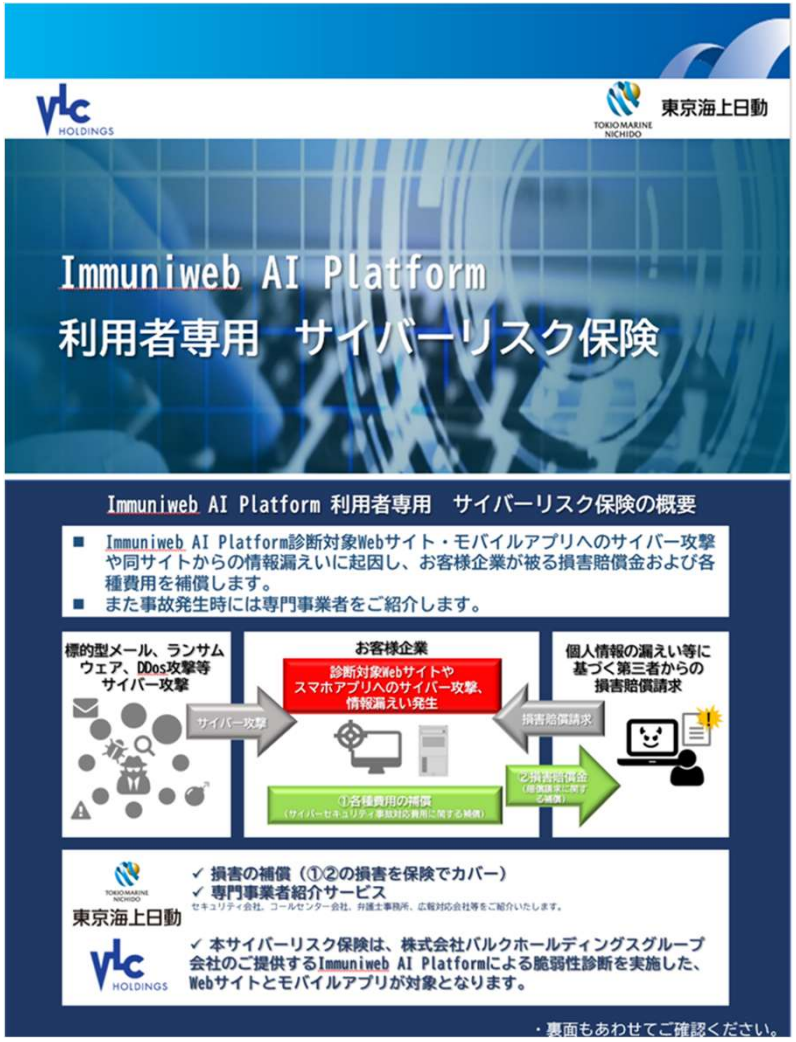
527,200件以上
モバイルセキュリティアプリテスト実績
OWASPMobileTop10Android, iOS対応

42,560,000件以上
サーバSSL TLS設定コンプライアンステスト実績。
PCIDSS、NIST、GDPR準拠チェック

915,100,000件以上
ドメインブランドテスト実績。フィッシングサイトや
ブランドの悪用をチェック

《世界で確実な評価を得ています》
2023年 SC Awards Europe 2023　セキュリティコンプライアンス遵守のためのベストツールとして採択
2023年 Globee Cybersecurity Awards 2023　“Asset Discovery & Management”部門にて金賞受賞
2023年 Cybersecurity Excellence Awards 2023
合計10部門にて革新的なAI技術をもちいたプラットフォームとして金賞受賞

特長③　サイバーリスク保険自動付帯



【賠償責任に関する補償】

損害賠償金・弁護士費用	第三者から損害賠償を受けた際の損害賠償金や弁護士費用等を補償します

【サイバーセキュリティ事故対応費用に関する補償】

不正アクセス等対応費用(※1)	①ネットワーク遮断費用：不正アクセス等またはそのおそれが発見されたことにより、ネットワークの遮断対応を外部委託した場合に支出する費用を補償します。 ②不正アクセス等有無確認費用：不正アクセス等またはそのおそれが発見されたことにより、不正アクセス等の有無を判断するために支出する費用をお支払いたします（※2）
原因・被害範囲調査費用(※1)	セキュリティ事故の原因もしくは被害範囲の調査または証拠保全のために支出する費用をお支払いたします。

※1：いずれの費用も事故発生から180日以内に支出した費用に限ります。
※2：不正アクセス等のおそれに基づき対応したにもかかわらず結果として不正アクセス等が生じていなかった場合、その不正アクセス等のおそれが外部通報によって発見された際に支出する費用に限ります(10%の自己負担あり)。
※3：別途、保険金をお支払しない場合（免責規定）がございます。詳細内容については、保険約款をご確認ください。

お支払できる保険金の上限額（1企業あたり）

賠償責任に関する補償 1,000万円			サイバーセキュリティ費用に関する補償 1,000万円	
損害賠償金	争訟費用	協力費用	不正アクセス等対応費用	原因・被害範囲調査費用

※この保険契約においてお支払いする保険金の額は、1企業に対しサイバーセキュリティ事故対応費用に関する補償でお支払いするすべての保険金を合算して、上記の支払限度額（保険期間中）1,000万円が限度となります。なお、本保険制度全体の総支払限度額は3億円となります。3億円を超えた場合には告知なく本制度は終了となります。

特長④　脅威インテリジェンス無償提供（付属診断）

【トレードマーク不正使用診断】

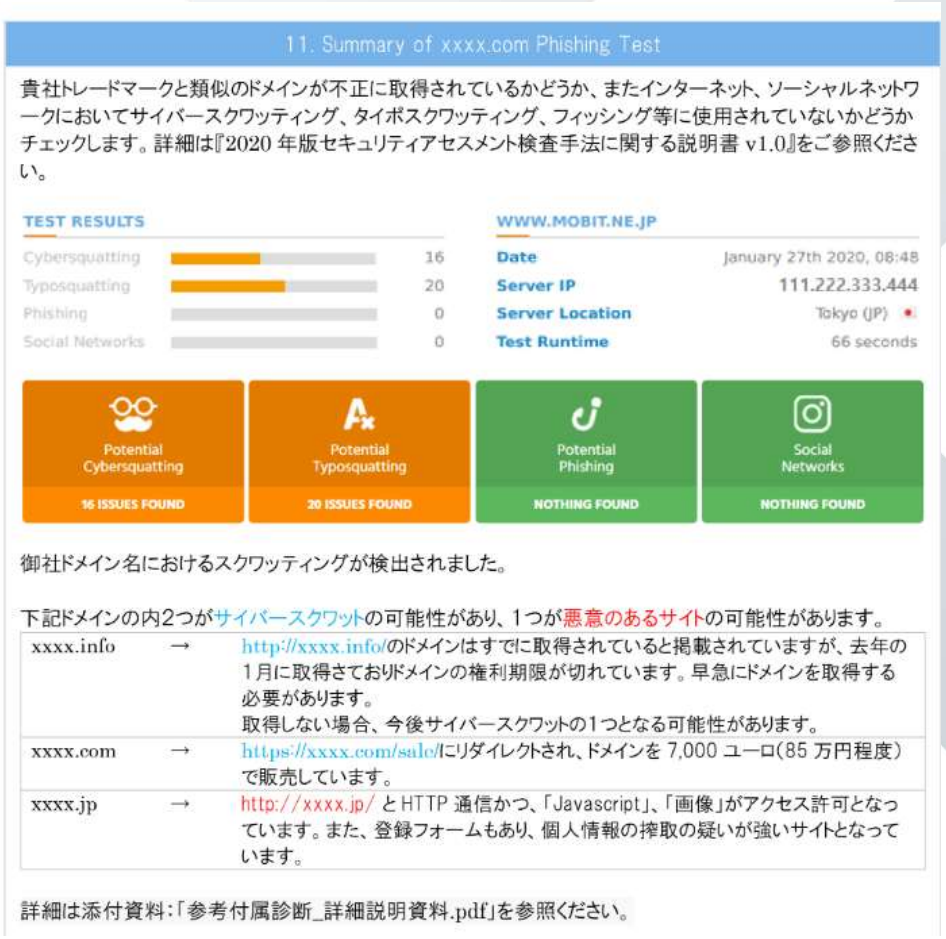
貴社トレードマークと類似のドメインが不正に取得されているかどうか、またインターネット、ソーシャルネットワークにおいてサイバースクワッティング、タイポスクワッティング、フィッシング等に使用されていないかどうかチェックします。

※診断スコープ

	サイバースクワッティングに関するリスク調査
1	Domains registered in different TLDs and owned by a third party
2	Domains imitating domain names or business identity and owned by a third party
	タイポスクワッティングに関するリスク調査
3	Domains with typos in body and owned by a third party
4	Domains with typos in body and TLD and owned by a third party
	フィッシングに関するリスク調査
5	Domains that try to visually impersonate your domain or brand and owned by a third party
6	Domains that contain phishing content targeting your domain or brand users
7	Domains that contain malicious content targeting your domain or brand users
	ソーシャルネットワークにおけるリスク調査
8	Twitter
9	Facebook
10	Google+
11	BitBucket
12	Github
13	YouTube

フィッシングサイトを特定するためのデータソース
Our proprietary network of web honeypots
Our proprietary network of email honeypots
Google Safe Browsing
PhishTank
CLEAN MX
OpenPhish

※報告書サンプル



11. Summary of xxxx.com Phishing Test

貴社トレードマークと類似のドメインが不正に取得されているかどうか、またインターネット、ソーシャルネットワークにおいてサイバースクワッティング、タイポスクワッティング、フィッシング等に使用されていないかどうかチェックします。詳細は『2020 年版セキュリティアセスメント検査手法に関する説明書 v1.0』をご参照ください。

TEST RESULTS

Cybersquatting	16
Typosquatting	20
Phishing	0
Social Networks	0

WWW.MOBIT.NE.JP

Date	January 27th 2020, 08:48
Server IP	111.222.333.444
Server Location	Tokyo (JP)
Test Runtime	66 seconds

Potential Cybersquatting — 16 ISSUES FOUND
Potential Typosquatting — 20 ISSUES FOUND
Potential Phishing — NOTHING FOUND
Social Networks — NOTHING FOUND

御社ドメイン名におけるスクワッティングが検出されました。

下記ドメインの内2つがサイバースクワットの可能性があり、1つが悪意のあるサイトの可能性があります。

xxxx.info	→	http://xxxx.info/のドメインはすでに取得されていると掲載されていますが、去年の1月に取得さておりドメインの権利期限が切れています。早急にドメインを取得する必要があります。 取得しない場合、今後サイバースクワットの1つとなる可能性があります。
xxxx.com	→	https://xxxx.com/sale/にリダイレクトされ、ドメインを 7,000 ユーロ(85 万円程度)で販売しています。
xxxx.jp	→	http://xxxx.jp/ と HTTP 通信かつ、「Javascript」、「画像」がアクセス許可となっています。また、登録フォームもあり、個人情報の搾取の疑いが強いサイトとなっています。

詳細は添付資料:「参考付属診断_詳細説明資料.pdf」を参照ください。

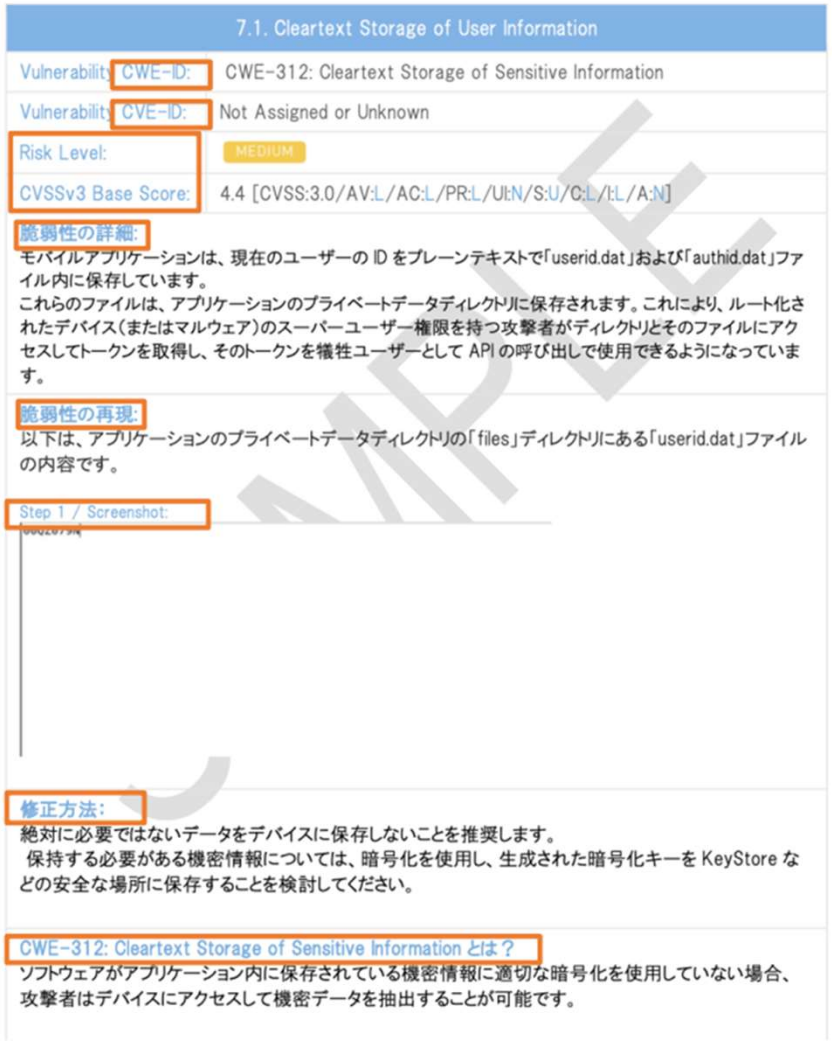
Immuniweb実績　～GLOBAL～

対象企業	対象インフラ	所在地
Israel Electric Corporation	発電所	イスラエル
Bank Leumi	銀行	イスラエル
Bank Hapoalim	銀行	イスラエル
Tel-Aviv stock exchange	株式市場	イスラエル
NATO	軍事機関	イスラエル
United Nations	国際連合および政府WEBサイト	スイス
Banca Stato	銀行	スイス
Swiss Quote	ネットバンク	スイス
ITU	国際電気通信連合	スイス
Telia	通信	スウェーデン
ARAB BANK	銀行	ヨルダン
Latvijas Banka	銀行	ラトビア
eBay	マーケットプレイス	USA

Immuniweb実績　～国内実績は1,200サイト以上～

企業	業種	ソリューション実績
官公庁	官公庁	Webアプリケーション・スマホアプリ
銀行	銀行	Webアプリケーション・スマホアプリ
証券会社	証券	Webアプリケーション・スマホアプリ
マーケティング会社	マーケティング	Webアプリケーション年間契約
消費財メーカー	消費財	Webアプリケーション・スマホアプリ
民間放送会社	放送	Webアプリケーション
電力会社	電力	Webアプリケーション
通信会社	通信	Webアプリケーション
物流会社	物流	Webアプリケーション
燃料製造会社	製造	TLPT　脅威ベースのペネトレーションテスト
計器製造会社	製造	Webアプリケーション・スマホアプリ・IOT機器のペネトレーションテスト
一般財団法人	財団法人	Webアプリケーション
金融系開発会社	情報サービス	Webアプリケーション・スマホアプリ
食品メーカー	製造	Webアプリケーション
地銀	銀行	Webアプリケーション・スマホアプリ・TLPT 脅威ベースのペネトレーションテスト

Immuniweb　報告書



7.1. Cleartext Storage of User Information

Vulnerability CWE-ID: CWE-312: Cleartext Storage of Sensitive Information

Vulnerability CVE-ID: Not Assigned or Unknown

Risk Level: MEDIUM

CVSSv3 Base Score: 4.4 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N]

脆弱性の詳細:
モバイルアプリケーションは、現在のユーザーの ID をプレーンテキストで「userid.dat」および「authid.dat」ファイル内に保存しています。
これらのファイルは、アプリケーションのプライベートデータディレクトリに保存されます。これにより、ルート化されたデバイス（またはマルウェア）のスーパーユーザー権限を持つ攻撃者がディレクトリとそのファイルにアクセスしてトークンを取得し、そのトークンを犠牲ユーザーとして API の呼び出しで使用できるようになっています。

脆弱性の再現:
以下は、アプリケーションのプライベートデータディレクトリの「files」ディレクトリにある「userid.dat」ファイルの内容です。

Step 1 / Screenshot:

修正方法:
絶対に必要ではないデータをデバイスに保存しないことを推奨します。
保持する必要がある機密情報については、暗号化を使用し、生成された暗号化キーを KeyStore などの安全な場所に保存することを検討してください。

CWE-312: Cleartext Storage of Sensitive Information とは？
ソフトウェアがアプリケーション内に保存されている機密情報に適切な暗号化を使用していない場合、攻撃者はデバイスにアクセスして機密データを抽出することが可能です。

CWE（Common Weakness Enumeration）共通脆弱性タイプ一覧
発見された脆弱性がどのような攻撃手法により活用されるのかを示します。脆弱性の修正方法を知る際に役立ちます。

CVE(Common Vulnerabilities and Exposures)共通脆弱性識別子
発見された脆弱性の共通番号を表示します。脆弱性の修正方法を知る際に役立ちます。

CVSS（Common Vulnerability Scoring System）共通脆弱性評価システム
発見された脆弱性がどの程度危険であるかをCritical,High,Middle,Lowの4種類で評価します。

脆弱性の詳細
発見された脆弱性がどのようなものであるか説明します。

脆弱性の再現
発見された脆弱性が誤検出でないことを確認するため、再現方法を示します。

スクリーンショット
発見された脆弱性の再現方法をキャプチャします。

修正方法
発見された脆弱性の修正方法を示します。

脆弱性によるリスクの説明
発見された脆弱性によるリスクに関して記述します。

Immuniweb　モバイルアプリケーション脆弱性診断

検証方法（iOS/Android）

- OWASP モバイルセキュリティテスト ガイド (MSTG)
- NIST SP 800-115 情報セキュリティに関するテクニカルガイド
- PCI DSS 情報補足: 侵入テスト ガイダンス
- モバイルおよびエンタープライズ向けのMITRE ATT&CK®マトリックス
- FedRAMP 侵入テスト ガイダンス
- ISACA による GDPR の監査方法

NIST　PCI Security Standards Council　FedRAMP　OWASP

モバイルアプリとバックエンドAPIのテスト

モバイルアプリケーション監査

- OWASPモバイルトップ10
- ソフトウェア構成分析
- 行動分析
- プライバシーリスク

モバイルバックエンドAPI監査

- OWASPトップ10
- CWE / SANSトップ25
- PCI DSS 6.5.1-6.5.10
- ビジネスロジックテスト

多くの脆弱性はバックエンドAPIから検出されます。弊社のモバイルアプリ診断ではバイナリ解析やネットワーク診断だけではなく、必ず動的テストを実施します。

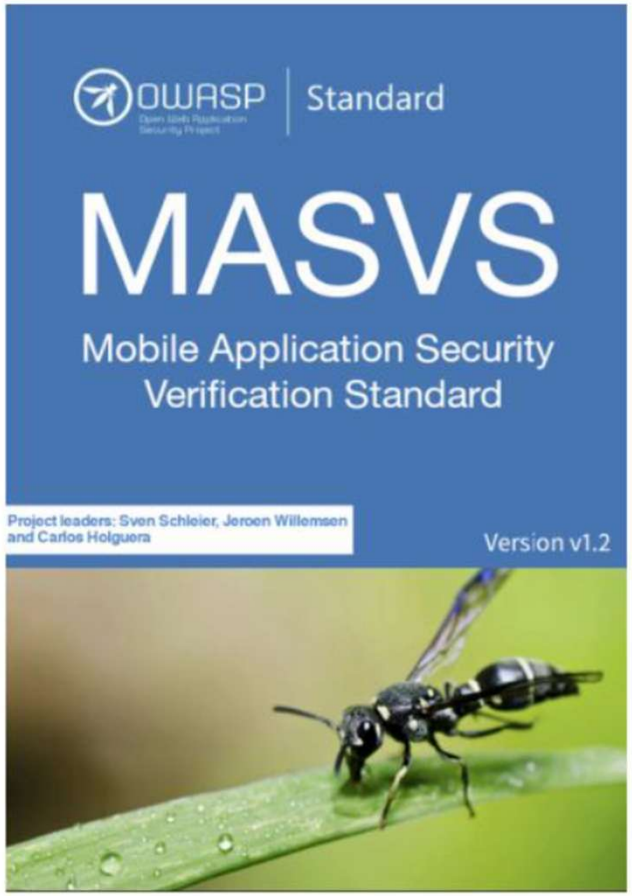
暗号化とプライバシーのテスト

- 機密データの漏洩
- 弱いネットワーク暗号化

- M1:不適切なプラットフォームの使用
- M2:安全でないデータ ストレージ
- M3:安全でない通信
- M4:安全でない認証
- M5:不十分な暗号化
- M6:安全でない承認
- M7:クライアントコードの品質
- M8:コード改ざん
- M9:リバースエンジニアリング
- M10:余計な機能

Immuniweb　モバイルアプリケーション脆弱性診断

OWASP Mobile Application Security Verification Standard
（モバイルアプリケーションのセキュリティ検証基準）



リバースエンジニアリングに対する耐性 - Android

ID	MSTG-ID	リバースエンジニアリングに対する耐性の要件	R
V8		動的解析と改竄の阻止	
8.1	MSTG-RESILIENCE-1	アプリはユーザーに警告するかアプリを終了することでルート化デバイスや脱獄済みデバイスの存在を検知し応答している。	✓
8.2	MSTG-RESILIENCE-2	アプリはデバッグを防止し、デバッガのアタッチを検知し応答している。利用可能なすべてのデバッグプロトコルを網羅している必要がある。	✓
8.3	MSTG-RESILIENCE-3	アプリはそれ自身のサンドボックス内の実行ファイルや重要なデータの改竄を検知し応答している。	✓
8.4	MSTG-RESILIENCE-4	アプリはそのデバイスで広く使用されるリバースエンジニアリングツールやフレームワークの存在を検知し応答している。	✓
8.5	MSTG-RESILIENCE-5	アプリは任意の方法を使用してエミュレータ内で動作しているかどうかを検知し応答している。	✓
8.6	MSTG-RESILIENCE-6	アプリはそれ自身のメモリ空間内のコードとデータの改竄を検知し応答している。	✓
8.7	MSTG-RESILIENCE-7	アプリは各防御カテゴリ(8.1から8.6)で複数のメカニズムを実装している。耐性は使用されるメカニズムのオリジナリティの量、多様性と比例することに注意する。	✓
8.8	MSTG-RESILIENCE-8	検知メカニズムは遅延応答やステルス応答を含むさまざまな種類の応答をトリガーしている。	✓
8.9	MSTG-RESILIENCE-9	難読化はプログラムの防御に適用されており、動的解析による逆難読化を妨げている。	✓
		デバイスバインディング	

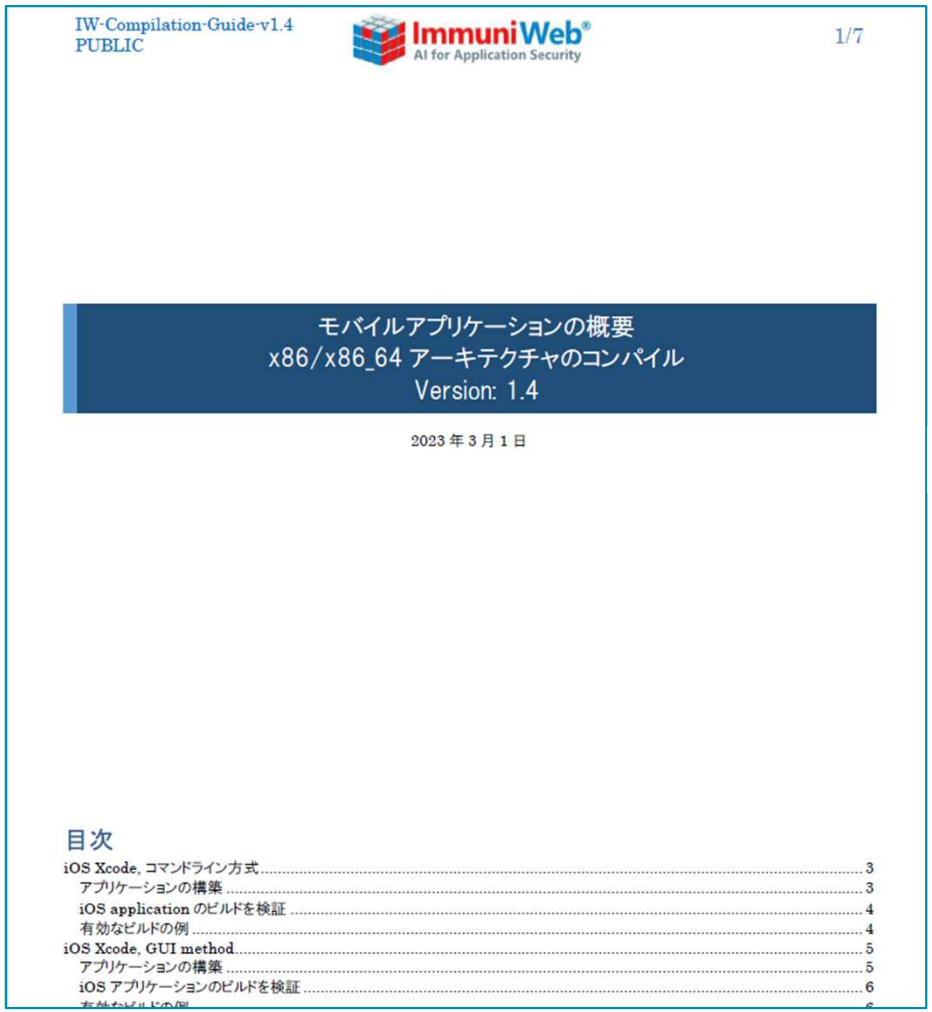
モバイルアプリケーションセキュリティ要件 - Android

ID	MSTG-ID	検証要件の内容	レベル 1	レベル 2
V1		アーキテクチャ、設計、脅威モデリング		
1.1	MSTG-ARCH-1	アプリのすべてのコンポーネントを把握し、それらが必要とされている。	✓	✓
1.2	MSTG-ARCH-2	セキュリティコントロールはクライアント側だけではなくそれぞれのリモートエンドポイントで実施されている。	✓	✓
1.3	MSTG-ARCH-3	モバイルアプリと接続されるすべてのリモートサービスの高次のアーキテクチャが定義され、そのアーキテクチャにセキュリティが対応されている。	✓	✓
1.4	MSTG-ARCH-4	モバイルアプリのコンテキストで機密とみなされるデータが明確に特定されている。	✓	✓
1.5	MSTG-ARCH-5	アプリのすべてのコンポーネントは提供する業務上の機能やセキュリティ上の機能の観点で定義されている。		✓
1.6	MSTG-ARCH-6	モバイルアプリとそれに関連するリモートサービスの脅威モデルが作られ、潜在的な脅威と対策を特定している。		✓
1.7	MSTG-ARCH-7	すべてのセキュリティコントロールは集約実装されている。		✓
1.8	MSTG-ARCH-8	暗号鍵が（もしあれば）どのように管理されるかについての明確な方針があり、暗号鍵のライフサイクルが施行されている。NIST SP 800-57 などの鍵管理標準に準拠することが理想的である。		✓
1.9	MSTG-ARCH-9	モバイルアプリの更新を強制するメカニズムが存在している。		✓
1.10	MSTG-ARCH-10	セキュリティはソフトウェア開発ライフサイクルのあらゆる部分で対処されている。		✓
V2		データストレージとプライバシー		
2.1	MSTG-STORAGE-1	個人識別情報、ユーザー資格情報、暗号化鍵などの機密データを格納するために、システムの資格情報保存機能が適切に使用されている。	✓	✓
2.2	MSTG-STORAGE-2	機密データはアプリコンテナまたはシステムの資格情報保存機能の外部に保存されていない。	✓	✓
2.3	MSTG-STORAGE-3	機密データはアプリケーションログに書き込まれていない。	✓	✓
2.4	MSTG-STORAGE-4	機密データはアーキテクチャに必要な部分でない限りサードパーティと共有されていない。	✓	✓
2.5	MSTG-STORAGE-5	機密データを処理するテキスト入力では、キーボードキャッシュが無効にされている。	✓	✓
2.6	MSTG-STORAGE-6	機密データはIPCメカニズムを介して公開されていない。	✓	✓
2.7	MSTG-STORAGE-7	パスワードやピンなどの機密データは、ユーザーインタフェースを介して公開されていない。	✓	✓
2.8	MSTG-STORAGE-8	機密データはモバイルオペレーティングシステムにより生成されるバックアップに含まれていない。		✓
2.9	MSTG-STORAGE-9	バックグラウンドへ移動した際にアプリはビューから機密データを削除している。		✓
2.10	MSTG-STORAGE-10	アプリは必要以上に長くメモリ内に機密データを保持せず、使用後は明示的にメモリがクリアされている。		✓
2.11	MSTG-STORAGE-11	アプリは最低限のデバイスアクセスセキュリティポリシーを適用しており、ユーザーにデバイスパスコードを設定することなどを必要としている。		✓
2.12	MSTG-STORAGE-12	アプリは処理される個人識別情報の種類をユーザーに通知しており、同様にユーザーがアプリを使用する際に従うべきセキュリティのベストプラクティスについて通知している。		✓
V3		暗号化		
3.1	MSTG-CRYPTO-1	アプリは暗号化の唯一の方法としてハードコードされた鍵による対称暗号化に依存していない。	✓	✓
3.2	MSTG-CRYPTO-2	アプリは実績のある暗号化プリミティブの実装を使用している。	✓	✓
3.3	MSTG-CRYPTO-3	アプリは特定のユースケースに適した暗号化プリミティブを使用している。業界のベストプラクティスに基づくパラメータで構成されている。	✓	✓
3.4	MSTG-CRYPTO-4	アプリはセキュリティ上の目的で広く非推奨と考えられる暗号プロトコルやアルゴリズムを使用していない。	✓	✓
3.5	MSTG-CRYPTO-5	アプリは複数の目的のために同じ暗号化鍵を再利用していない。	✓	✓
3.6	MSTG-CRYPTO-6	すべての乱数値は十分にセキュアな乱数生成器を用いて生成されている。	✓	✓

OWASPプロジェクトの一つであるMASVSを弊社でも検証の基準としています。
公開されたプロジェクトは以下にあります。
https://github.com/coky-t/owasp-mstg-ja

Mobile Security Testing Guideと合わせて活用することで診断に役立てています。
MASVSに基づきリバースエンジニアリングに対しての耐性も検証スコープに追加しています。
MASVSの検証深度は標準的なレベル1を採用しており、お客様からのご要望によってはレベル2の項目についても評価が可能です。

Immuniweb　モバイルアプリケーション脆弱性診断


IW-Compilation-Guide-v1.4
PUBLIC

ImmuniWeb®
AI for Application Security

1/7

モバイルアプリケーションの概要
x86/x86_64 アーキテクチャのコンパイル
Version: 1.4

2023 年 3 月 1 日

目次

モバイルアプリ診断の事前準備として対象アプリファイルをご準備いただく必要があります。iOSであればipaファイル、Androidであればapkファイルをご提供頂きます。

診断の形態としてシュミレータ上での診断と実機端末での診断の2種類があります。
弊社では基本的にシュミレータ上での診断形態を推奨しております。
診断にかかる期間が実機での診断と比べて短納期にすることが可能です。
（工数の減少に応じて費用も安価になります。）

シュミレータ（x86/x86_64アーキテクチャ）用にアプリファイルをコンパイルしていただく必要があるため、弊社からは左記のコンパイル手法説明書をお客様に配布しています。
⚠XcodeやAndroid Studioでの一例となります。開発環境によっては説明書通りにコンパイル出来ないこともございます。

クロスプラットフォーム（FlutterやReact Native）にて開発されたアプリでは指定のコンパイルが出来ない可能性が高いです。こちらのアプリケーションは実機端末での診断を実施します。

【コンパイル必須要件】
・x86及びx86_64アーキテクチャのシュミレーターにて起動する
・新しいOSバージョンにて稼働する
（Android 6以下、iOS10以下は診断対象外）
・HPKP（証明書のピン留め）の削除か無効化をする

ペネトレーションテスト

ペネトレーションテストとは？

ペネトレーションテスト（略称：ペンテスト）とは

日本においては「侵入テスト」を意味し、システム全体の観点でサイバー攻撃耐性がどのくらいあるかを試すテストです。悪意のある攻撃者が実行するような方法に基づいて、実践的にホワイトハッカーがシステムに侵入し、お客様から承諾の元、あらゆるハッキング技術やツールを使って脆弱な箇所に攻撃を行い、セキュリティ機能の回避または無効化を試みながらシステム内部へ侵攻出来るかをテストするものです。

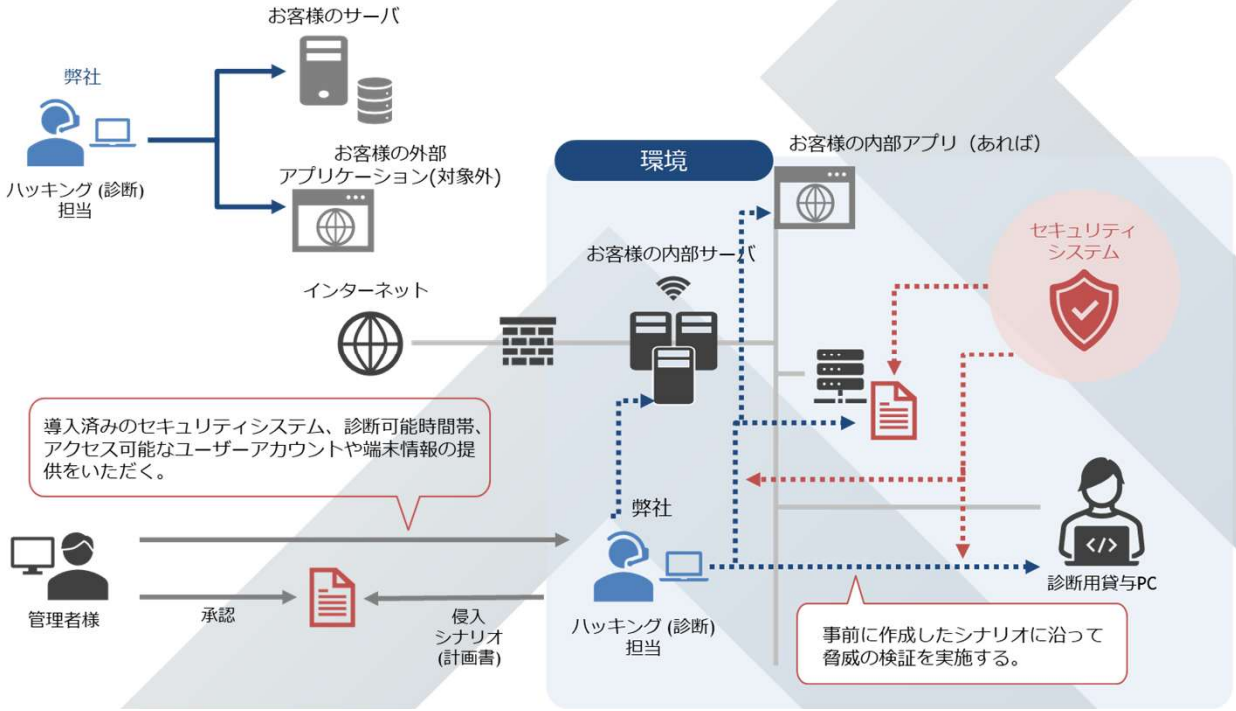
ペネトレーションテストと脆弱性診断の違い

両テストの違いは検証目的にあります。

ペネトレーションテスト：攻撃者がおこなう実際の侵入シナリオに基づいて脅威の検証をすることが目的。現実的に起こり得る脅威に対しての防御能力を測り改善に役立てることが可能です。

脆弱性診断：対象システムの存在する既知の脆弱性を洗い出すことが目的です。成立可能な脆弱性の発見自体を目的とし、システム単体の堅牢性を確認し改善することが可能です。

ペネトレーションテスト概念図



ペネトレーションテストの種類

ペネトレーションテストの種類

ペネトレーションテストの種類は、セキュリティの境界線に基づく外部からのテストと、内部からのテストに分類されます。
Zero Trust(ゼロトラスト)の視点から考えますと、外部だけでなく内部からのペネトレーションテストも重要と指摘されています。

種類	説明	診断方法
侵入影響範囲調査 (オリジナルペンテストパッケージ)	インターネットからアクセス可能な機器を突破し、社内ネットワークへの侵入が可能かどうかの外部侵入テストと外部からアクセス出来ない内部システムに対するペネトレーションテストを組み合わせた、セキュリティオリジナルパッケージテストになります。	リモート+オンサイト **(リモート調査は踏み台PCが必須)**
TLPT **(脅威ベースのペネトレーションテスト)**	上記侵入侵害調査に加え、ブルーチームテスト(多層防御能力)およびホワイトチームテスト(インシデントレスポンス能力)を評価します	リモート＋オンサイト

ペネトレーションテスト実施までの流れ

ステップ	説明
診断要望	お客様より「診断の目的」「診断対象」とネットワーク図をご提供頂きます
診断内容のご提案	上記診断要望とネットワーク図を弊社テスターチームが確認のうえ初期構想をご提案
ペネトレーション内容打ち合わせ	弊社ご提案内容とお客様要望のすり合わせをし、診断対象と診断方法等を決定します
診断計画書とお見積書のご提出	打ち合わせを基に、診断計画書とお見積書をご提出します
ご発注	ご発注書の発行とともに弊社内にて診断の準備に入ります

侵入影響範囲調査 ～オリジナルペンテストパッケージ～

攻撃者がインターネットからアクセス可能な機器を突破し社内ネットワークへの侵入が可能か？

＋

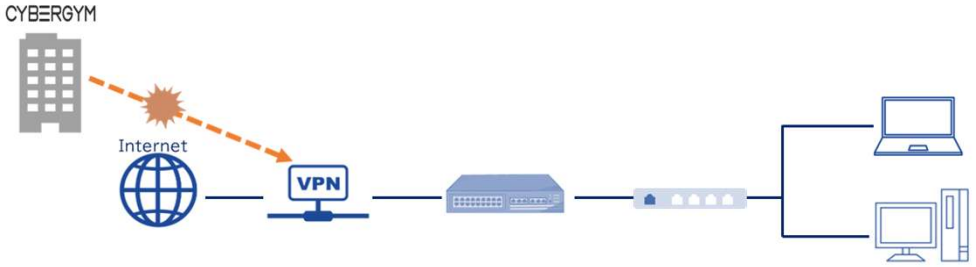
攻撃者が仮に内部侵入した場合に、水平・垂直展開のネットワーク侵害および情報を外部に持ち出すことが可能か？

外部侵入テスト

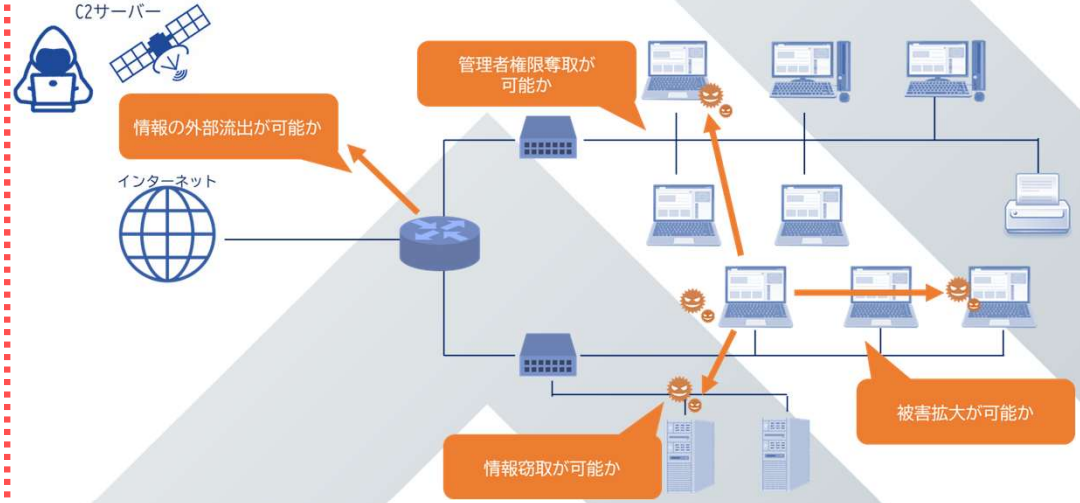
診断元端末：リモート端末

診断対象：外部に出ているネットワーク機器（VPN機器最優先）

実作業： ByPassスキャン、機器構成要素の脆弱性スキャン、
証明書の偽造など



内部影響範囲調査



TLPT ～脅威ベースのペネトレーションテスト～

ホワイトチームのインシデントレスポンス能力など多層防御能力を評価

	項目	目的	ポイント	対象
1	脅威インテリジェンス	脅威シナリオの調査や分析	保有するインフラにおいてどのような攻撃シナリオがあるかリスク要因の可視化	既知の脆弱性の調査 未知の攻撃手法のリスク可視化
2	ペネトレーションテスト	脅威シナリオに基づく侵入テスト	攻撃シナリオに基づいて脆弱性の網羅的なチェック	既知の脆弱性の発見
3	ブルーチームテスト	企業内に導入されているセキュリティ製品により攻撃の検知・ブロックが実現できているかをチェック	多層防御の観点により、セキュリティの堅牢性をチェック	既知の脆弱性への対応 未知の攻撃手法への対応可否
4	ホワイトチームテスト	セキュリティポリシー・インシデントレスポンス体制の成熟度をチェック	平時・有事の際の対応計画をチェック	セキュリティ運用ポリシーのレビュー
5	報告・環境修正	セキュリティ体制強化	各インフラの優先順位を検討しながらセキュリティ投資の意思決定	

☑既知の脆弱性の調査
☑既知の脆弱性・攻撃手法に対する多層防御能力の評価
☑実際の攻撃が生じた場合の防御・検知・修復能力を評価
☑未知の脆弱性・攻撃手法に対する防御・検知・修復能力を評価
例）ゼロデイ攻撃・ファイルレス攻撃・高度標的型攻撃などを想定

TLPT ～脅威ベースのペネトレーションテスト～

侵入経路①
アプリケーション
・コーポレートWEBサイト
・Eコマースサイト
・モバイル（iOS,Android）
・社内業務用アプリケーション
・WEBサーバ
・WAFバイパス

侵入経路②
エンドポイント端末
・既知の脆弱性
・AVのバイパス
・USBドロップアタック
・インターネット接続

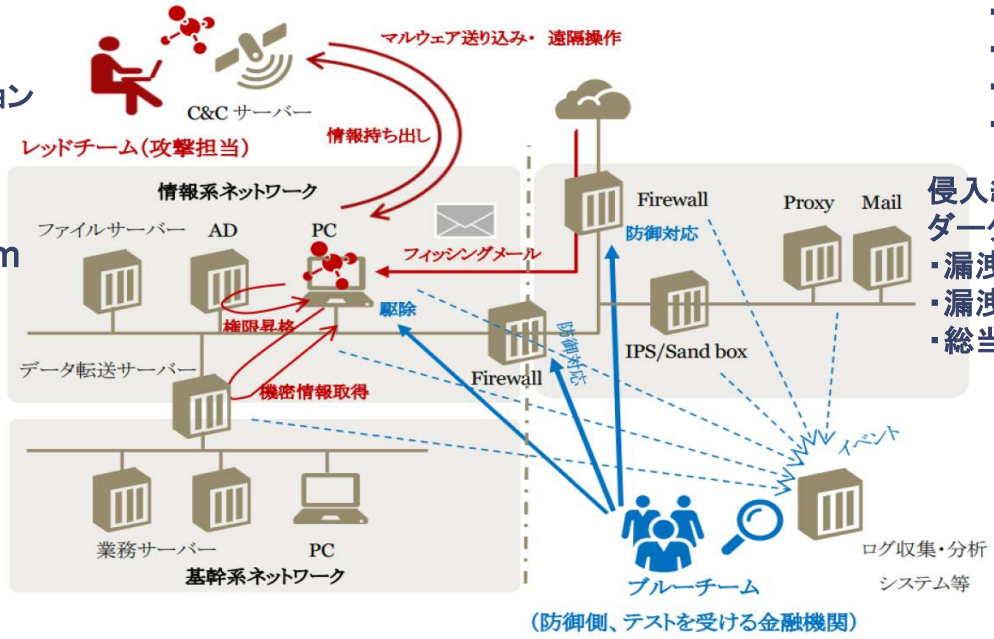
侵入経路③
メール
・既知の脆弱性
・標的型メール
・メールフィルタのバイパス

侵入経路④
ネットワーク
・既知の脆弱性
・FWのバイパス
・メールサーバ
・DNSサーバ

侵入経路⑤
無線接続IoT
・プリンタ
・空調システム
・IPカメラ

侵入経路⑥
重要インフラ
・OT
・SCADA/PLC
・センサー
・アクチュエータ

侵入経路⑦
ダークウェブ
・漏洩済みのID、パスワード
・漏洩済みのメールアカウント
・総当たり攻撃のヒントとなる情報



侵入経路と攻撃シナリオを選定しRED Teamによる侵入テストを実施します。

・水平、垂直展開等侵入拡大の調査

・セキュリティ製品の検知状況

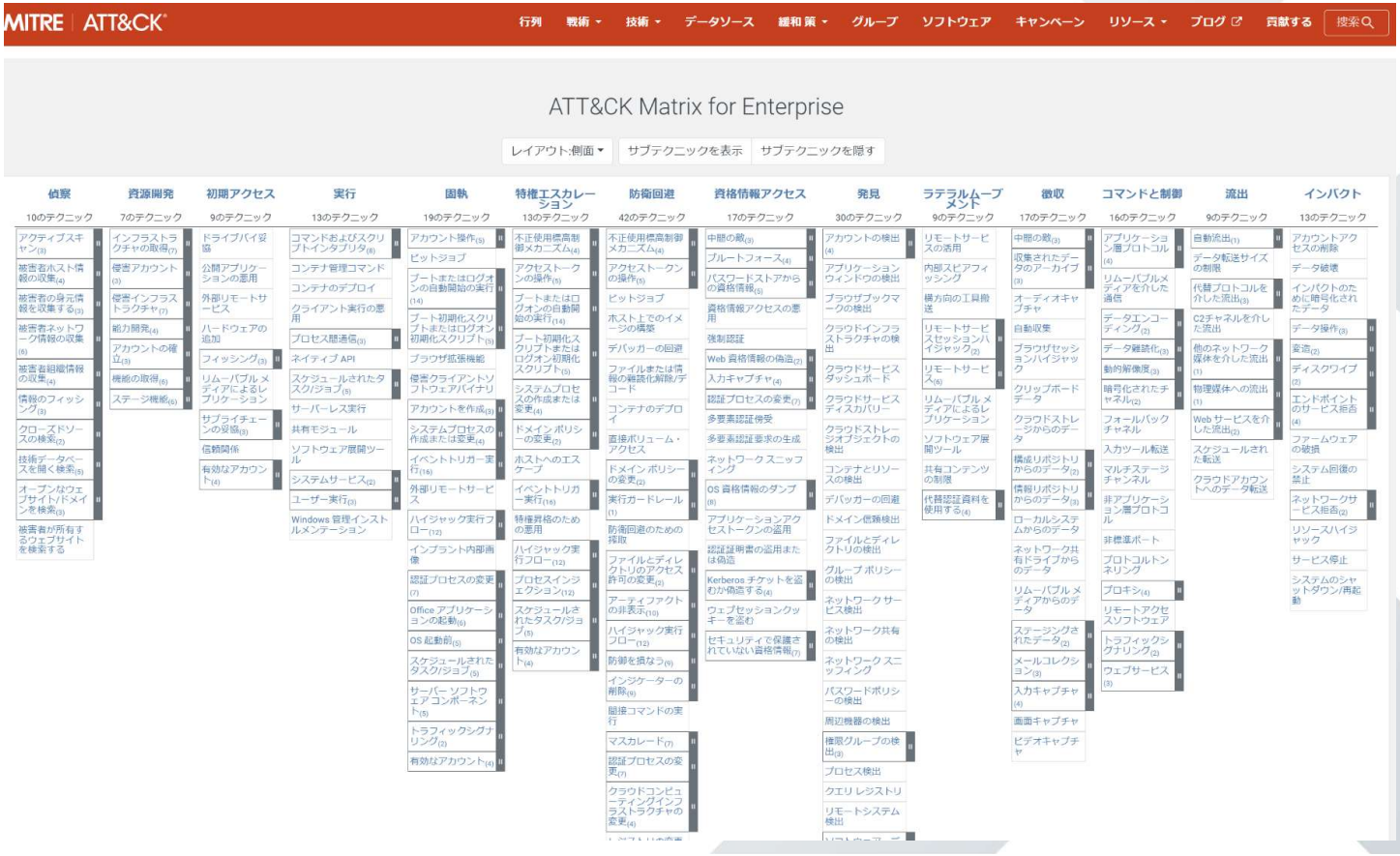
・インシデントレスポンス能力など
多層防御能力を評価

・ゼロトラストを前提に導入されているセキュリティ製品の設定、運用状況や多層防御の状態、インシデントレスポンス能力をテスト
・商用セキュリティ製品を導入済みであってもゼロデイ攻撃、ファイルレス攻撃、未知のマルウェアの検知は比較的困難
・高度標的型攻撃、DDoS、ブルートフォース攻撃（パスワードリスト攻撃・辞書攻撃・レインボーテーブル攻撃）などを想定
・制御システム（OT）、重要インフラ業界特有の深層システムの検査にも対応可能

TLPT　～脅威ベースのペネトレーションテスト　攻撃シナリオ～

MITRE ATT&CK

国際的に著名なサイバー犯罪組織と同様の攻撃手法（既知の攻撃・未知の攻撃）を用いたシステムストレステストを提供。
12段階の侵入項目に対して250項目以上の攻撃シナリオ（MITRE ATT&CKのガイドライン参考）から選定し調査いたします。



ペネトレーションテスト　報告書イメージ

総評

Strictly Confidential

2. 総評

High
2.67

3	High Risk	プラットフォーム[リモート]
2	Medium Risk	プラットフォーム[オンサイト]
3	High Risk	影響範囲調査

今回の各種診断における総合評価は「Medium-Risk」となります。
全体的に Medium-Risk が検出されており、一部では High-Risk も検出されております。

各セクションの結果を含め、ペネトレーションテスト対象に対し、下記観点で下記攻撃を試み、シナリオ達成を試行しました。

■シナリオ観点
①サイトのデータ改ざん・機密情報窃取
②ユーザーアカウントの奪取

■攻撃観点
①検出された脆弱性を用いた更なる攻撃
②脆弱性を組み合わせた攻撃
③Tool 診断では行えない攻撃

結果として、条件付きではありますが「なりすましログイン」を達成いたしました。
実態としては、ログイン後の TOP 画面のみ閲覧が可能ではありますが、TOP 画面に機密情報に類するデータがある可能性も考慮し、CVSS 値より Medium-Risk と評価しております。

※判定の定義
各検出項目の脅威度は CVSS v3.1 算出値から次のように割り振りしております。
None: 0 / Low: 0.1～3.9 / Medium: 4.0～6.9 / High: 7.0～8.9 / Critical: 9.0～10.0
総評での脅威度(Low～Critical)は次のように設定しております。
None: 0 / Low: 0.1～1.0 / Medium: 1.1～2.0 / High: 2.1～3.0 / Critical: 3.1～4.0

2

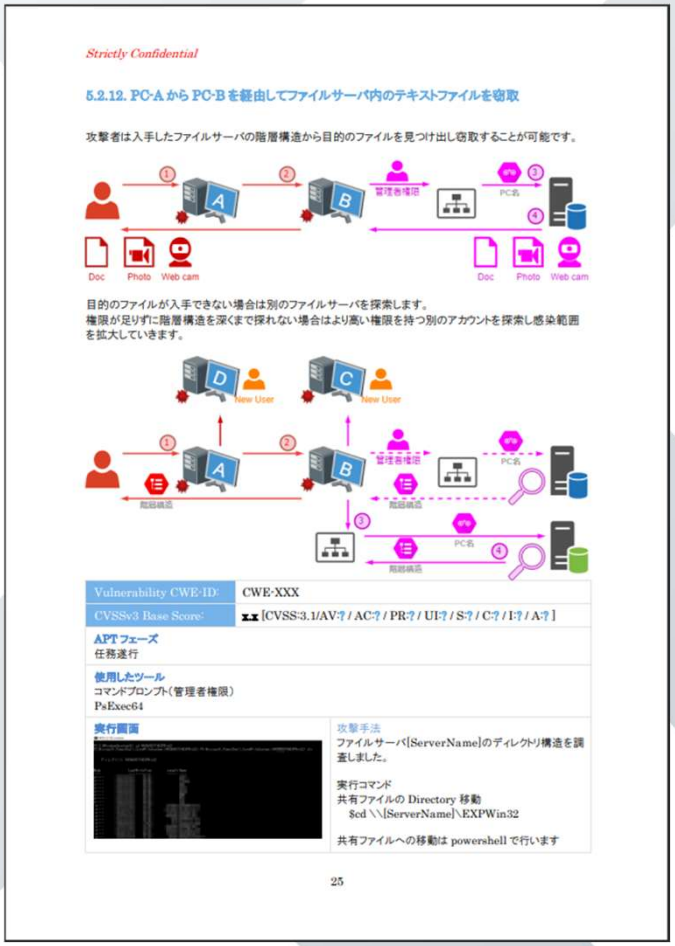
セクションサマリー

Strictly Confidential

4.3. 診断結果

7

詳細報告



Strictly Confidential

5.2.12. PC-A から PC-B を経由してファイルサーバ内のテキストファイルを窃取

攻撃者は入手したファイルサーバの階層構造から目的のファイルを見つけ出し窃取することが可能です。

目的のファイルが入手できない場合は別のファイルサーバを探索します。
権限が足りずに階層構造を深くまで探れない場合はより高い権限を持つ別のアカウントを探索し感染範囲を拡大していきます。

Vulnerability CWE-ID:	CWE-XXX
CVSSv3 Base Score:	xx [CVSS:3.1/AV:? / AC:? / PR:? / UI:? / S:? / C:? / I:? / A:?]
APT フェーズ 任務遂行	
使用したツール コマンドプロンプト(管理者権限) PsExec64	
実行画面	攻撃手法 ファイルサーバ[ServerName]のディレクトリ構造を調査しました。 実行コマンド 共有ファイルの Directory 移動 $cd \\[ServerName]\EXPWin32 共有ファイルへの移動は powershell で行います

25

ペネトレーションテスト及び脆弱性診断評価基準

➢ 評価基準

セキュリティの脆弱性を報告するために国際標準に準拠しています。

●Common Vulnerabilities and Exposures (CVE) Compatible
●Common Weakness Enumeration (CWE) Compatible
●Common Vulnerability Scoring System (CVSSv3)

共通脆弱性評価システムCVSS(Common Vulnerability Scoring System)は、米国インフラストラクチャ諮問委員会(NIAC: National Infrastructure Advisory Council)のプロジェクトで2004年10月に原案が作成されました。
その後、CVSSの管理母体としてFIRST(Forum of Incident Response and Security Teams)が選ばれ、2005年6月にCVSS v1が、2007年6月にCVSS v2が、2015年6月にCVSS v3。
そして最新のCVSS v4.0が2023年11月より公開されました。

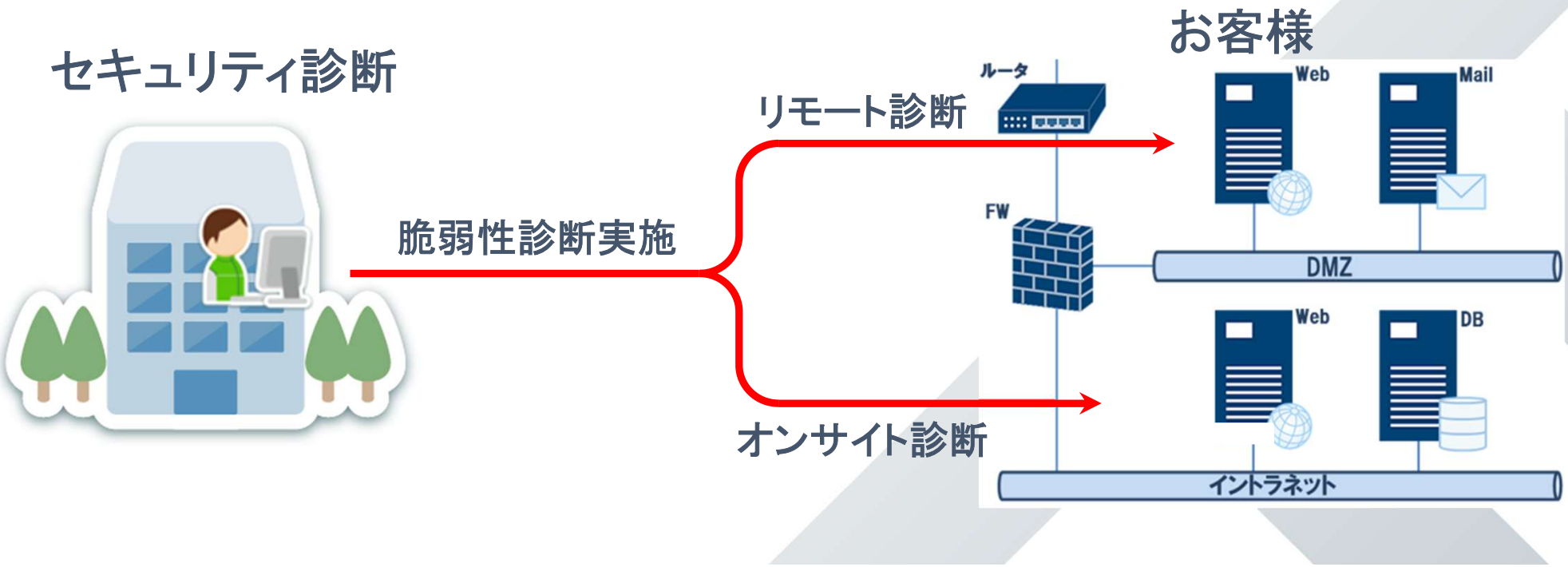
弊社ではアプリケーションの脆弱性の深刻度評価に関して、共通脆弱性評価システムCVSSv3 及び v4.0を採用しています。IoTや産業用制御システムなどITシステムに限らないリスク評価にCVSS v4.0を用います。
CVSSでは0-10までの点数による5段階の評価(None,Low,Medium,High,Critical)を行います。

	項目			レベルの選択			
攻撃難易度	1	AV	Attack Vector どこから攻撃可能か	Physical (P)	Local (L)	Adjacent (A)	Network (N)
	2	AC	Attack Complexity 攻撃条件の複雑さ	High (H)		Low (L)	
	3	PR	Priviledges Required 必要な特権レベル	High (H)	Low (L)	None (N)	
	4	UI	User Interaction 必要なユーザ関与のレベル	Required (R)		None (N)	
	5	S	Scope 管理権限の範囲	Unchanged (U)		Changed (C)	
攻撃の影響	6	C	Confidentiality 機密性（情報漏洩の可能性）	None (N)	Low (L)	High (H)	
	7	I	Integrity 完全性（情報改ざんの可能性）	None (N)	Low (L)	High (H)	
	8	A	Availavility 可用性（業務停止の可能性）	None (N)	Low (L)	High (H)	
合計値 None (0) / Low (0.1-3.9) / Medium (4.0-6.9) / High (7.0-8.9) / Critical (9.0-10.0)							

プラットフォーム診断

プラットフォーム診断

プラットフォーム診断（ネットワーク診断）とは、保有するサーバ/ネットワーク機器/端末などに対して、疑似攻撃を行い、稼働しているOSやミドルウェアに存在する情報漏えいや改ざん、設定不備、パッチの適用状況など様々なリスクを調査するサービスです。



プラットフォーム診断　診断項目

No.	診断項目	概要	
		調査・確認事項	主な脅威
1	ホストの存在確認 （ICMP パケットによるホストアップチェック）	対象サーバの存在を確認しました。主に ICMP パケットを利用して存在確認しました。	ICMP レスポンス状況によっては、攻撃者に攻撃の糸口を与える可能性があります。
2	ポートスキャン （TCP/UDP 全ポート）	対象サーバにおけるオープンポートを確認しました。	動作しているサービス状況が判明します。 不正侵入・攻撃を行う前の事前調査として行われます。
3	不要と思われるサービスの稼動	サービスの動作状況を確認しました。	セキュリティ上不要なサービスの動作は、攻撃者に攻撃の糸口を多く与えてしまいます。
4	稼動中のサービスからの情報取得	稼働しているサービスのバナー情報等を取得しました。	動作しているプログラムの特定等により、不正侵入等の攻撃に利用される可能性があります。
5	OS やアプリケーションソフトウェアの既知の脆弱性	OS のバージョンやセキュリティパッチの適用状況等を確認しました。	既知の脆弱性を利用した任意のコマンドの実行やサービス妨害攻撃を受ける可能性があります。
6	脆弱なパスワード設定	認証を伴うサービスに対して容易に推測可能なパスワードが設定されていないか確認しました。	パスワードが容易に推測可能な場合、なりすましにより不正にシステムにアクセスされる可能性があります。
7	脆弱性の知られている CGI スクリプトの存在	CGI スクリプトの存在確認及びバージョン等を確認しました。	既知の脆弱性を利用した任意のコマンドの実行やサーバの内部情報を取得される可能性があります。
8	アカウントポリシーの調査	アカウントロックアウト値などを取得できた場合設定値の妥当性を評価しました。	設定値に不備がある場合、パスワード推測攻撃が容易になったり、攻撃の成功確率が上がったりする可能性があります。
9	各種サービス(FTP サービス、SSH サービス等)の既知の脆弱性	各種サービスにおいて脆弱性の報告されている古いバージョンのソフトウェアが稼働していないか確認しました。	既知の脆弱性を利用した任意のコマンドの実行やサービス妨害攻撃を受ける可能性があります。
10	サービス運用妨害（DoS）の可能性	サービス運用妨害攻撃を実施できる可能性があるか確認しました。	提供しているサービスを停止または、アクセスすることが困難になる可能性があります。
11	サーバ設定上の問題	サーバ設定（書込権限やアクセス制御設定等）がセキュリティ的に妥当であるか確認しました。	セキュリティ的に不備がある設定の場合、不正侵入等の攻撃に利用される可能性があります。例）書込権限に不備がある場合、任意のファイルを作成されたりする可能性があります。

No.	診断項目	概要	
		調査・確認事項	主な脅威
12	プライベートアドレス漏えい	対象ホストからの応答にプライベートアドレス等が含まれていないか確認しました。	システムの内部ネットワーク情報が漏えいすることにより、不正侵入等の攻撃に利用される可能性があります。
13	DNS ゾーン転送の可否	DNS ゾーン転送を不特定のホストに許可しているか確認しました。	ドメイン内に存在すると思われるホストと利用用途を容易に特定することが可能となり攻撃対象が多くなります。
14	DNS 再帰的問い合わせの可否	DNS 再帰的問い合わせを許可している設定か確認しました。	DNS 再帰的問い合わせを許可している場合、DNS サーバの不正利用や他のサーバを攻撃する DDoS 攻撃に利用される可能性があります。
15	DNS ダイナミックアップデートの可否	DNS レコードをアップデート可能な設定であるか確認しました。	任意のレコード追加により悪意あるサイトに利用者を誘導することが可能です。
16	メール不正中継の可否	メールサーバのメール中継の設定状況を確認しました。	不正中継が可能な場合、スパムメールの送信などに利用される可能性があります。
17	メールサーバによるユーザ情報漏えい問題	メールサーバでユーザに許可しているコマンドやサーバの応答等を確認しました。	許可しているコマンド及びコマンドの応答結果によりシステムに登録されているユーザ情報を特定され、パスワード推測攻撃に利用される可能性があります。
18	Web サーバ上のデフォルトコンテンツの存在	システム導入時にインストールされるデフォルトコンテンツが存在するか確認しました。	デフォルトコンテンツに脆弱性があった場合、それを利用した不正侵入や、攻撃に利用可能な情報を取得される可能性があります。
19	不要なファイルの存在	不要なファイルが公開されていないか確認しました。	ファイルの情報から、攻撃者に攻撃の糸口を多く与えてしまいます。
20	Proxy 設定の不備	Proxy サーバの設定がセキュリティ的に妥当であるか確認しました。	セキュリティ的に不備がある設定の場合、Proxy サーバを他のシステムを攻撃する際の踏み台として利用される可能性等があります。
21	不適切な SSL サーバ証明書の利用	SSL サーバ証明書を取得して信頼できる証明書であるか確認しました。	SSL サーバ証明書に不備がある場合、サーバの実在証明ができず、利用者が悪意ある偽のサーバに誘導されても判断がつかず、利用者が誘導された偽のサーバに情報を送信してしまう可能性があります。
22	エラーメッセージによる情報漏えい	エラーメッセージが返るようなリクエストを送りエラーメッセージにサーバ内部情報等が含まれていないか確認しました。	サーバ内部情報等がふくまれている場合、取得した情報を不正侵入等の攻撃に利用される可能性があります。
23	ワーム感染の有無	既にワームに感染していないかを確認しました。	攻撃や不正侵入、サービス妨害に利用されている可能性があります。
24	バックドア検出　等	バックドアが既に仕組まれていないかなど様々な項目を確認しました。	バックドアがある場合、既に不正にシステムを利用されている可能性があります。

アセスメント1stのセキュリティソリューション群

バズワードに振り回されないセキュリティを！
自組織の現状をアセスメントで把握することでできるリスク・課題ベースで最適なセキュリティ投資と真のセキュリティインシデント対応力獲得を実現