BBSec診断サービス
スマホアプリ診断サービス

ICMS-SR0326 / JIS Q 27001

018-0039-20

10470048(06)

株式会社ブロードバンドセキュリティ

xtrans cs

便利で安全なネットワーク社会を創造する BroadBand Security, Inc.

SQAT®サービスの優位性

SQAT®は当社の登録商標です。登録商標第5146108号

SQAT®サービスの優位性

SQAT® A&P (Software Quality Analysis Team Attack & Penetration) サービスは「システムの弱点をあらゆる視点から網羅する」「正確かつ客観性の高いレポートをする」「お客様にわかりやすく説明する」が特徴です。お客様は、すべての問題部位と脆弱性のポイントの把握、リスクに対する明確な理解、具体的な対策立案のヒントを得ることが出来ます。

01 QUALITY

数多くのシステムに対する脆弱性診断やペネトレーションテストの経験を保有するセキュリティ技術者（情報セキュリティスペシャリスト・CISSP・CEHなど）による手動/ツール検査を実施いたします。また、OWASP TOP10, ASVS, Testing Guide/NIST SP 800シリーズ/IPA 安全なWebサイトの作り方などの「標準」を踏襲した、網羅性の高い内容で診断いたします。診断結果は、画像つき再現手順や検出個所一覧、トレンドと対象システム特有のリスクを分析した結果と対策方法を記載した報告書にお纏めいたします。

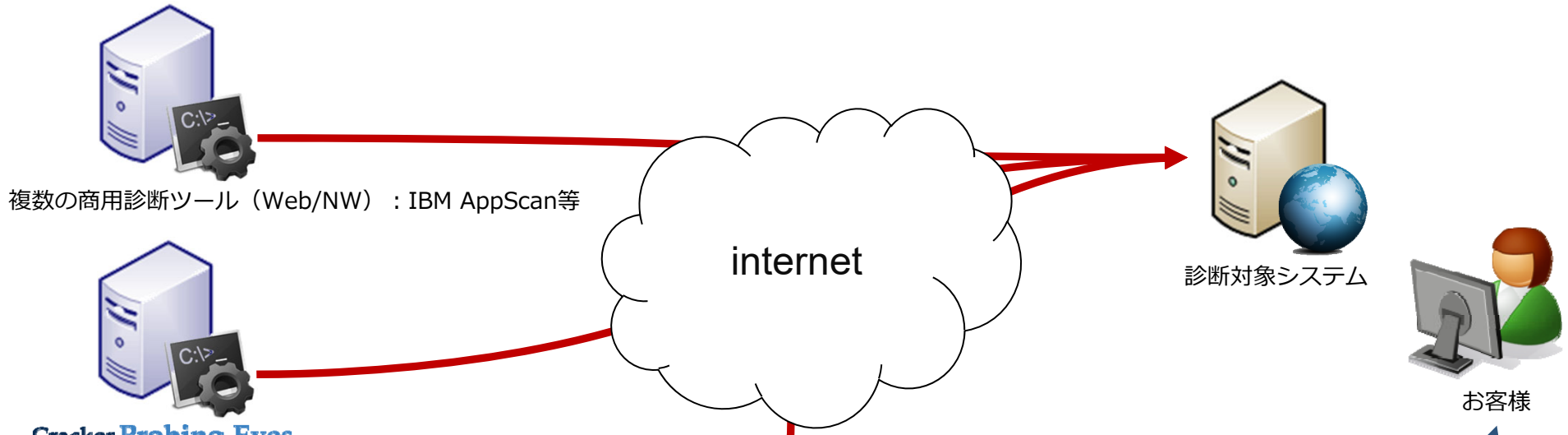
02 COMMUNICATION

診断を実施する技術部門だけでなく、報告書のレビューを専門とする部門や、診断を効率的に実施するためのツール開発を行う部門が、各役割に集中する体制を整えています。診断前のご相談などは、技術同席にてお伺いさせていただきます。また、BBSecポータルをご利用いただくことで、スケジュール・進捗状況の確認や依頼・お問い合わせのステータス管理など、コミュニケーションを円滑に図ることが可能です。なお、ポータルについては、回答遅延が発生しないよう、専用のサポートデスクが対応いたします。

03 SUPPORT

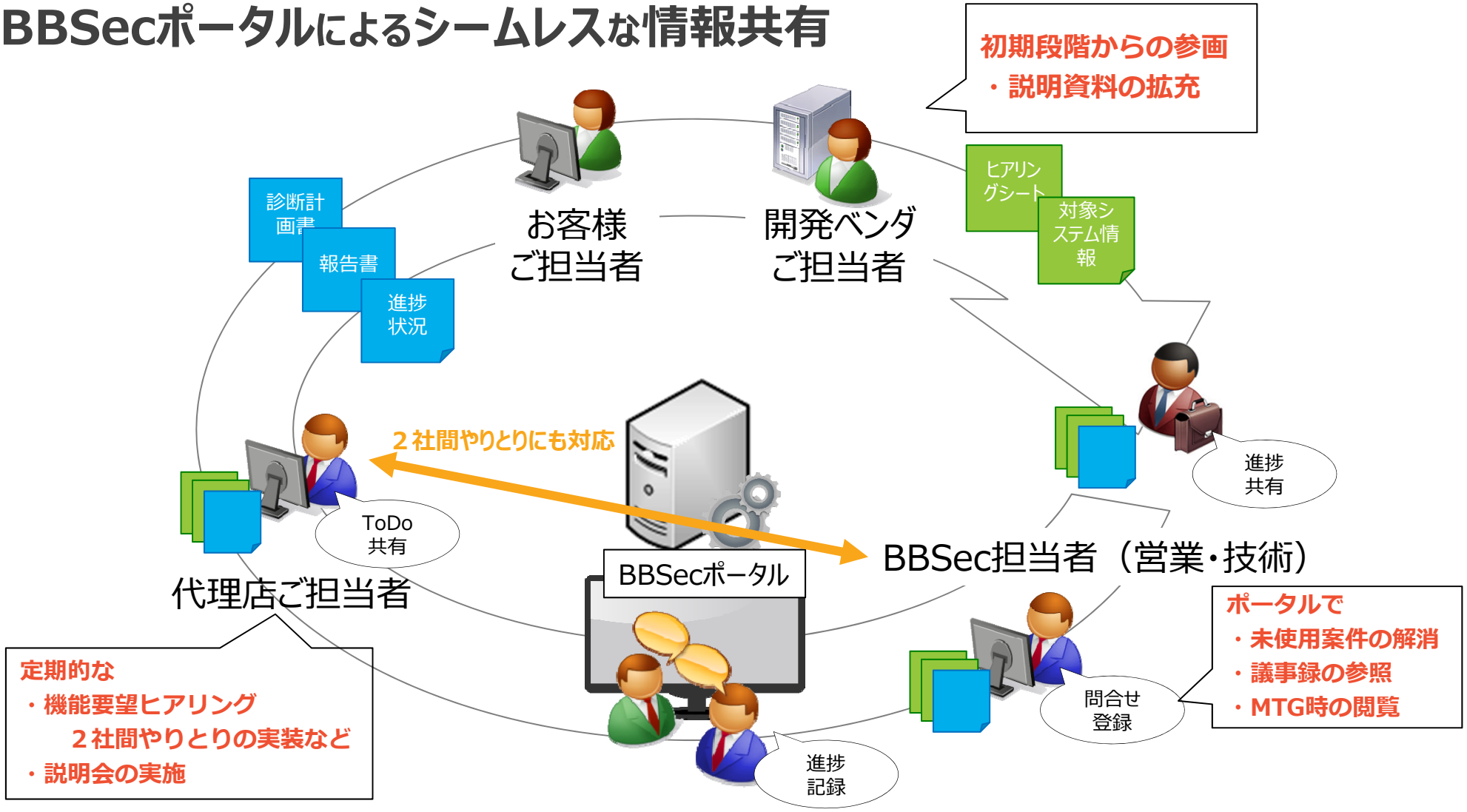
診断結果に関するお問い合わせは、診断実施後もBBSecポータルより承っております。診断結果の報告会は、弊社技術者（実担当者や技術責任者）が貴社へお伺いし説明、質疑応答いたします。
また、報告書納品日から３ヶ月間は、再診断を無償（リモート診断）でご提供いたします。
その他、定期的・継続的な保守に適した自動診断・改竄検知、ソースコード検査などのメニュー（有償）も用意しております。弊社担当営業までご連絡ください。

複数の手法を組み合わせ精度の高い診断を実施・レビュー専門部門が評価



Certified Information Systems Security Professional (CISSP)
Certified Ethical Hacker (CEH)
情報処理安全確保支援士/情報セキュリティスペシャリスト
公認情報セキュリティ監査人 (CAIS-Auditor)
IPAセキュリティプレゼンターなどを保有する技術者・レビュアが担当

BBSecポータルによるシームレスな情報共有



問い合わせ対応・再診断、関連サービスによる保守・サポート

問い合わせ対応・再診断

診断結果に関するお問い合わせは、診断実施後もBBSecポータルより承っております。また、報告書納品日から３ヶ月間は、再診断（リモート診断）を無償＊1でご提供いたします。

＊１：再診断が有償となるサービスもございますので、担当営業までお問い合わせください。

デイリー自動診断＆改竄検知

1日1回、インターネット越しにお客様サイトの脆弱性をチェックする自動診断サービス「Cracker Probing-Eyes」と、1日に複数回、お客様サイトを巡回し改竄を検知するサービス「Cracker Detect」により、基本的なセキュリティ対策・保守を低コストでご提供します。

ソースコード診断ツール

アプリケーションのソースコードをインターネット経由でアップロードするだけで、ソースコードの脆弱性と品質の診断を行える品質分析自動ツールです。お客様のオフィスから、任意のタイミングで依頼が可能なため、時間が切迫した開発現場での品質分析に大きなメリットをもたらします。

セキュリティ・セミナー

貴社のシステム開発を外注する際に、開発要件に何を組み込むべきか？担当者のお悩みに対して技術者が説明します。よくある脆弱性とその対策、シフトレフト、DevSecOps について、発注側がおさえておくべき事項について解説します。

SQAT®特徴まとめ

外部脆弱性診断のみサービス提供するのではなく、様々な情報セキュリティ対策の観点から、サービス・ソリューションを組み合わせ、お客様にとって最適解をご提案するのが、BBSec SQAT®サービスの特徴です。

例えば

- ☑ 開発中の状況からでも診断を開始したいが・・・

⇒ソースコード診断で入力値に対する安全化の不備を先に検出＋開発後に動的診断

- ☑ ユーザの書き込みに不正リンク（マルウェア等）が無いか・・・

⇒自動クローリング＋レピュテーションＤＢによる不正リンクの検出

- ☑ 診断で見つかった脆弱性を具体的に直す箇所が・・・

⇒ソースコード診断＋外部診断の両面による部位特定（GlassBoxサービス）

外部脆弱性診断
- SQAT® A&P（Web+Network） -

サービス全体の流れ

① ご提案・説明/依頼/打ち合わせ
- ヒアリング（時期・諸条件・対象）
- 概要説明（期間・フロー）
- 診断実施計画の提示
- 診断対象（追加/更新/削除）の相談

⇒ 「ヒアリングシート」

② 診断対象一覧の受領・内容の確認

③ 診断対象の提示・了承/見積/ご契約
- 推定診断期間の提示

⇒ 診断対象一覧の共有

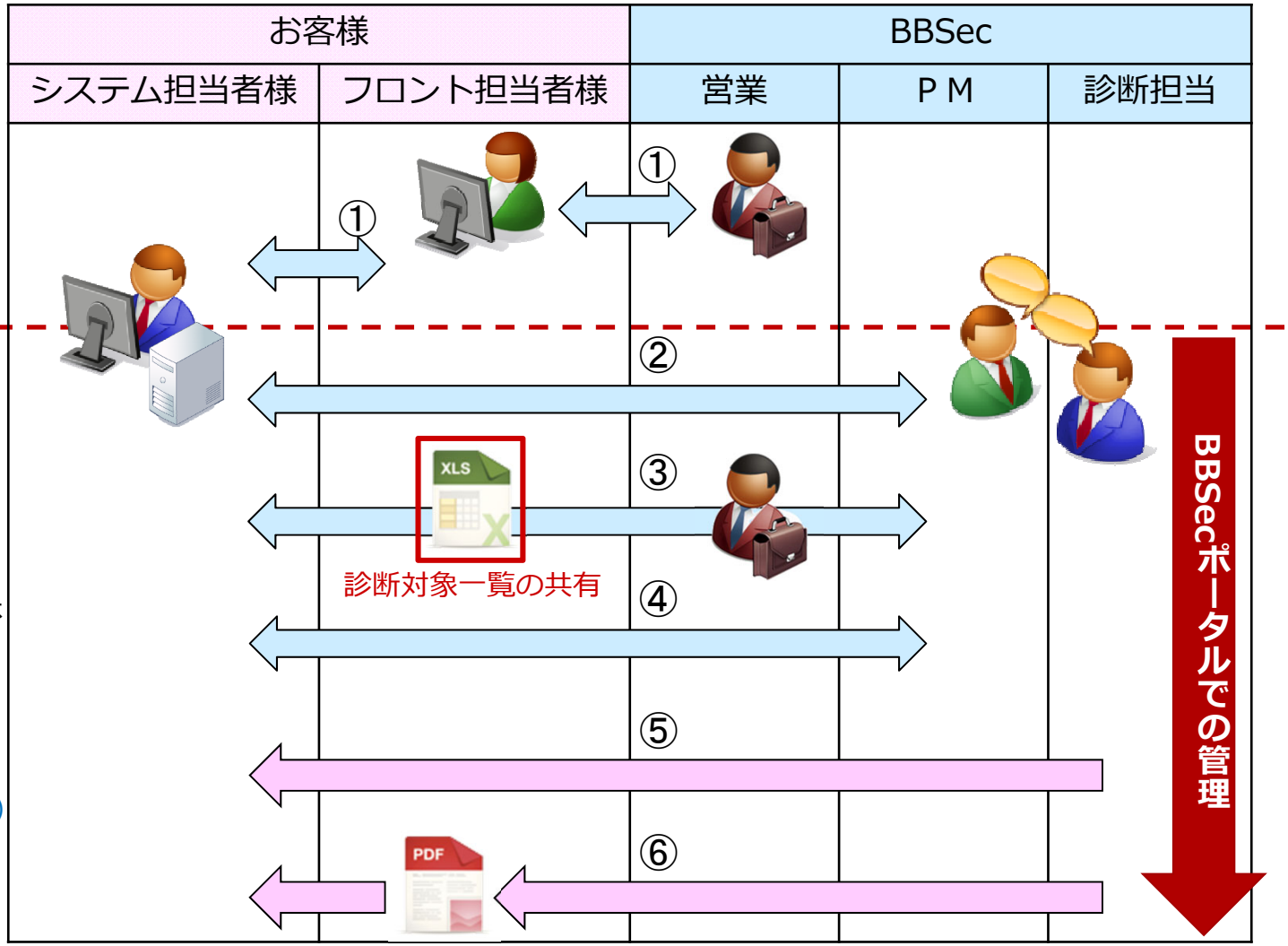
④ 診断実施計画（期間・納期）の提示

⇒ 「診断実施計画書」

⑤ 脆弱性診断の実施
- 診断期間の相談（検出内容により）
- 報告書納期の相談（検出内容により）

⑥ 報告書の提示・納品

⇒ 脆弱性診断報告書



診断の流れ（Web＆NW）

診断前準備・調査

予備調査 → クローリング → 対象システムの機能分析（Point）

Webシステムへの事前調査（クローリング）を実施し、診断対象機能・リクエストの選定と検査手法を検討します。
手動による調査は、機械的な判断では見落としてしまう画面遷移・分岐にも対応できるメリットがあります。
また、NW診断対象への正常疎通・経路を確認します。

診断実施＊1

脆弱性診断 → 複数ツールによるスキャン → ホワイトハッカーによる擬似攻撃 → ペネトレーションテスト＊2（Point） → エビデンス取得リスク評価

複数の商用ツール（IBM AppScan 等）や、自社開発の脆弱性診断ツール（Cracker Probing-Eyes 等）を用いて、システム全体の脆弱性・問題部位を洗い出します。
手動による診断は、数年以上の経験を持ったセキュリティエンジニアが、業界標準および弊社独自の手法により擬似攻撃を行います。もちろん最新の攻撃手法・シグネチャにも対応しています。
また、オーディット専門部門が、対象システムの特性に応じたリスクを評価します。

報告書作成～報告会

報告書作成 → BCPに対するリスク評価（Point） → トレンドにもとづく脅威評価（Point） → 報告会

レビュー専門部門が、対象システムの利用範囲や環境を考慮し、組織の事業継続リスクの評価を行います。また、昨今のセキュリティ事象や傾向を加味したリスク分析結果にもとづき、脅威を評価します。とくに攻撃の大流行・法改正などの大きなイベント（例：GDPR）については、別途トピックスを掲載します。
診断・解析を担当したエンジニアが報告会を実施、質疑応答にも対応いたします。

診断保守

結果報告後の対応 → 再診断 → 自動診断ツール CPE/CD＊3

報告書提出後３ヶ月間は指摘内容・対策についての質問をお受けします。また、脆弱性の改修箇所に対する再診断も実施します。
ほか、定期的・継続的な保守に適した自動診断・改竄検知ツールも用意しています。

＊１：重大な問題点を検出した場合は「速報」として随時ご報告いたします。
＊２：ご依頼がある場合、検出した脆弱性を用いてシステムへの侵入を試みます。
＊３：有償のメニューとなりますので、弊社営業担当までご連絡ください。

Webアプリケーションの機能・遷移をエンジニアが手動で詳細調査

	サイト名	画面数	禁則事項			
	テストサイト	15				
			23		49	

対象	機能名	画面名	URL	TYPE	パラメータ名	備考
	ログイン画面		https://www.example.com/			
○	ログイン画面	ログイン	https://www.example.com/login.form	Body	username	
				Body	password	
				Body	login-form-type	
○	ログイン後トップ	トップ	https://www.example.com/menu.do?type=1	URL	type	
○	ログイン後トップ	ナビゲーション（開発）	https://www.example.com/bbsecnavi1/postLogin.do?actionId=001&_token=147193950476038446284488888 2	URL	actionId	ユーザアカウント：開発権限でのみアクセス可能
				URL	_token	
○	ログイン後トップ	ナビゲーション（ユーザ）	https://www.example.com/bbsecnavi2/postLogin.do?actionId=001&_token=147193952561351037553970865 3	URL	actionId	
				URL	_token	
	ログイン後トップ	パスワード変更	https://www.example.com/passwd			
◎	パスワード変更	パスワード変更する	https://www.example.com/passwd.form	Body	old	完了形
				Body	new	
				Body	new2	
○	ナビゲーション（開発）	番号検索 > 検索	https://www.example.com/navi1/addr_kensaku.do	Body	searchPattern	ユーザアカウント：開発権限でのみアクセス可能
				Body	polNo	
				Body	_search	
				Body	_token	
○		検索結果	https://www.example.com/navi1/search/kekka.do?first=true&word=test	URL	first	最初のページ
				URL	word	
				Body	_token	
○		検索結果 > ページ遷移	https://www.example.com/navi1/search/kekka.do?page=2&word=test	URL	page	
○		検索結果 > ページ遷移	https://www.example.com/navi1/search/kekka.do?last=true&word=test	URL	last	最後のページ
	お問い合わせ	お問い合わせ	https://www.bbsec.co.jp/inquiry/			
○		送信	https://www.bbsec.co.jp/inquiry/send.php	Body	name	完了形
				Body	email	
				Body	text	
				Body	_token	
	資料請求	資料請求	https://www.example.com/siryo/			
○		確認	https://www.example.com/siryo/kakunin.do	Body	name	
				Body	email	
				Body	text	
				Body	_token	
◎		完了	https://www.example.com/siryo/kanryo.do	Body	name	完了形

機能・画面・URL・パラメータ・値・アクセス時の留意事項を、リクエスト単位で事前調査し、棚卸しを実施します。規模の相互認識を合わせ、診断対象の抜け漏れを防止します。

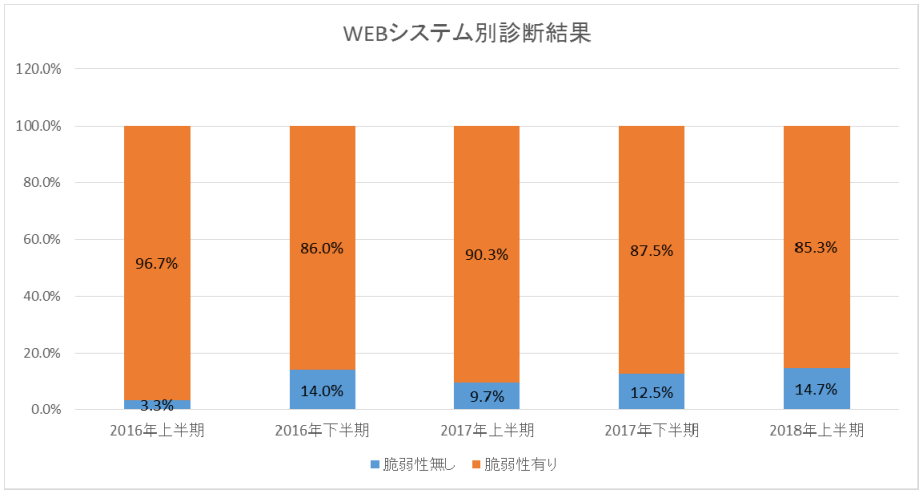
Webアプリ（API）診断項目概要

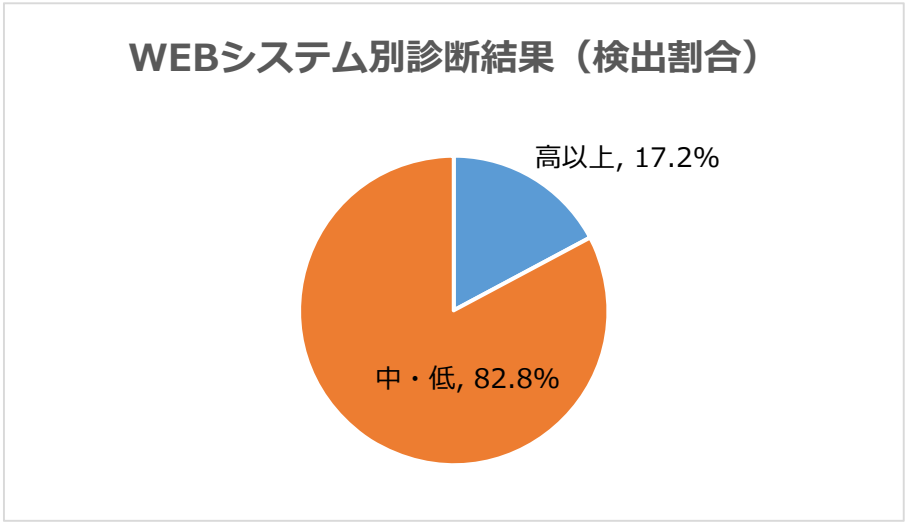
診断項目	主な例 *1:標準では実施しない項目		
入出力処理	クロスサイトスクリプティング	HTMLタグインジェクション	SQLインジェクション
	コマンドインジェクション	パスマニピュレーション	ファイルアップロード機能に関する調査
	パラメータ推測	例外処理に関する問題	オープンリダイレクト
	CRLFインジェクション	バッファオーバーフロー*1	XML外部エンティティ参照
認証	ログインフォームに関する調査	ログイン情報の送受信に関する調査	認証回避に関する調査
	パスワードの強度に関する調査	復元可能なパスワード保存	認証トークンに関する調査
セッション管理	Cookieに関する調査	セッションIDに関する調査	セッションハイジャック
	セッションフィクセーション	クロスサイトリクエストフォージェリ	セッションタイムアウト
	ユーザ権限に関する調査	ー	ー
重要情報の取り扱い	ユーザ情報の管理に関する調査	特定個人情報の管理に関する調査	クレジットカード情報管理に関する調査
	キャッシュ制御に関する調査	強制ブラウジング	GDPR関連に関する調査
システム情報・ポリシー	システム情報の開示	エラーメッセージの表示に関する調査	ディレクトリリスティング
	ソフトウェアの既知の脆弱性	クリックジャッキング	デフォルト設定に関する調査

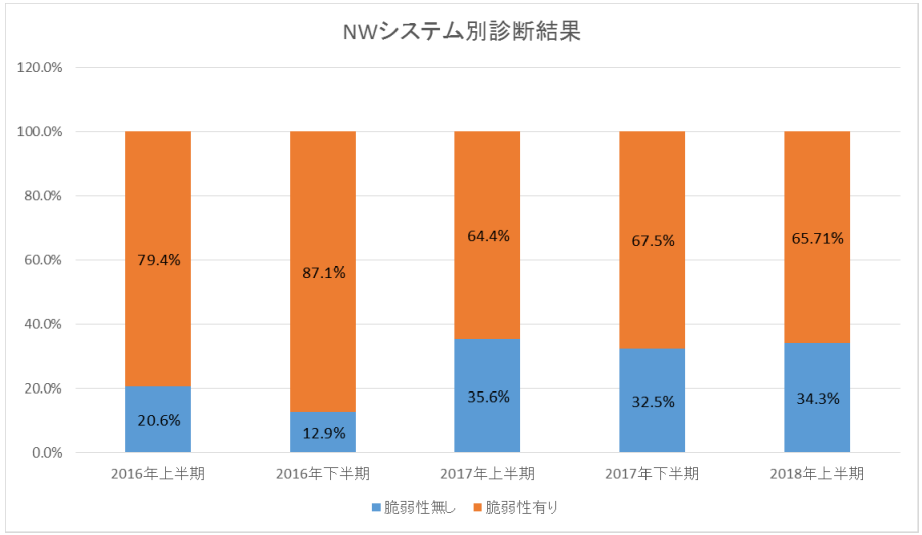
ネットワーク診断項目概要

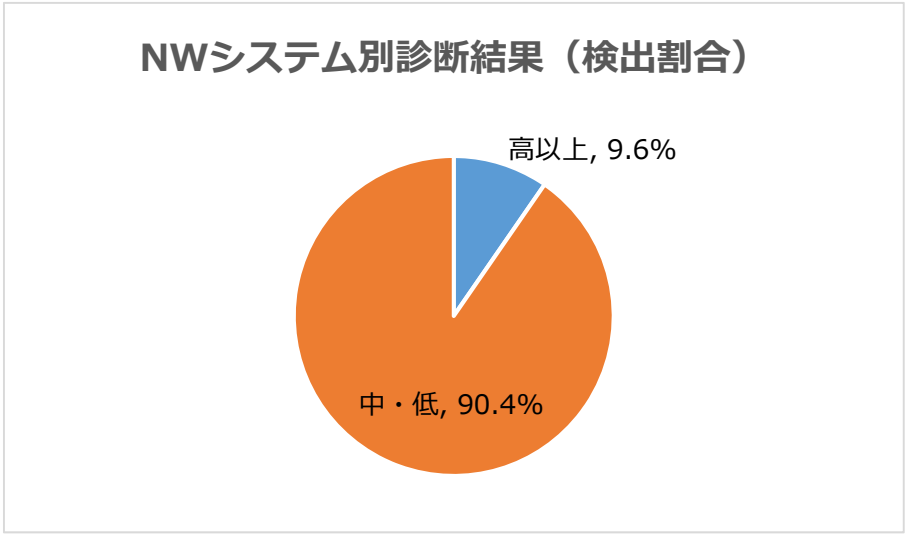
診断項目	主な例		
ホストのスキャン	TCP、UDP、ICMPでのポートスキャン	実行中のサービスの検出	ー
ネットワークサービスの脆弱性	DNSに関する調査	メールサーバに関する調査	FTPに関する調査
	RPCに関する調査	ファイル共有に関する調査	SNMPに関する調査
	SSHサーバに関する調査	データベースサーバに関する調査	その他サービスに関する調査
Webサーバの脆弱性	Webサーバの脆弱性	Webアプリケーションサーバの脆弱性	許可されているHTTPメソッド
各種OSの脆弱性	Windowsの既知の脆弱性	Solarisの既知の脆弱性	各種Linuxディストリビューションの既知の脆弱性
	その他各種OSの既知の脆弱性	ー	ー
悪意あるソフトウェア	バックドアの調査	P2Pソフトウェアの調査	ー
ネットワーク機器の脆弱性	各種ルータ機器の既知の脆弱性	各種FW機器の既知の脆弱性	ー
その他	その他ホスト全体の調査	ー	ー

脆弱性検出の統計情報（検出割合）



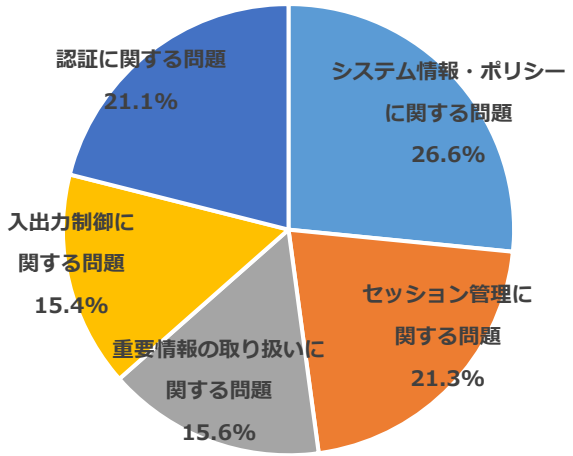






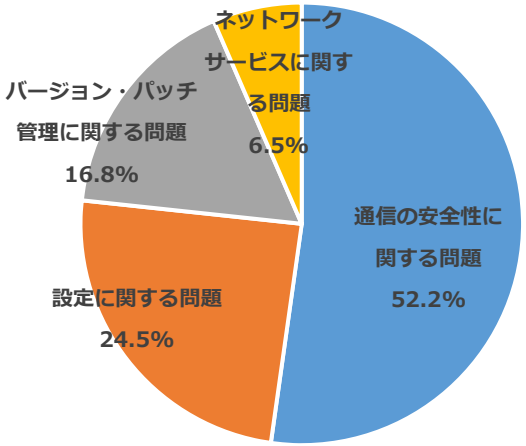
脆弱性検出の統計情報（ハイリスク脆弱性）

Webアプリケーション



診断項目	主な例		
入出力処理	クロスサイトスクリプティング	SQLインジェクション	パスマニピュレーション
認証	パスワード強度に関する問題	不正操作による認証回避	アカウント情報の表示
セッション管理	不適切な権限管理	セッションフィクセーション	セッションハイジャック
重要情報の取り扱い	強制ブラウジング	クレジットカード情報管理に関する問題	キャッシュ制御の不備
システム情報・ポリシー	既知の脆弱性が存在するバージョンのOS/アプリケーション	システム情報の表示	ディレクトリリスティング

ネットワーク



診断項目	主な例		
通信の安全性に関する問題	推奨されない暗号鍵の許容	推奨されないSSL/TLS方式の許容	FTPサービスの検出
認証に関する問題	推測が容易なBasic認証アカウントの検出	アクセス制御が不適切な認証機構の検出	アクセス制御の不備
設定に関する問題	設定変更されていない初期アカウントの検出	脆弱性が存在するリモートデスクトップサービス検出	SMB共有へアクセスが可能な問題
バージョン・パッチ管理に関する問題	サポートの終了したバージョンのOS/アプリケーション	Windows SMBにおける任意コード実行を含む複数の脆弱性	既知の脆弱性が存在するバージョンのOS/アプリケーション

レポートサンプル-1

診断レポートのイメージをサンプルとして抜粋いたします。

1 診断概要

1.1 診断対象

システム名称	△△システム
診断対象 Web アプリケーション	http://sample.sample.com/
診断対象ネットワーク	xxx.168.0.1 xxx.168.0.2

1.2 診断環境

診断場所
- 弊社診断ルーム

診断元 IP アドレス
- 218.223.4.224/27
- 218.223.6.0/24
- 218.40.57.166～190
- 59.159.217.195～196

1.3 診断担当者

リーダー : ○○、△△
Web アプリケーション脆弱性診断 : ○○、△△
ネットワーク脆弱性診断 : ○○、△△

1.4 診断期間

2018 年○月△日 ～ 2018 年○月■日

2 診断手法

2.1 システム脆弱性診断手法概要

診断対象として提示されたホストに対し、インターネットを経由したア
ステム脆弱性診断を行いました。

【診断の流れ】

事前調査
診断(ツール／手動)
診断結果の確認および精査
診断結果の分析
報告書作成・納品

(ア) 診断対象サイトの構造や
ネットワークの構造調査
な診断計画を策定します。

(イ) ツール／手動による診断

(ウ) ツール診断／手動診断
た項目の確認、精査（過
を実施します。

(エ) 対象サイトの性質を考
スク分析を実施します。

発見された脆弱性は、最
分類評価されます。

(オ) 発見された脆弱性の説明
ク、および推奨対策につ
た報告書を作成、納品い

本診断は、あらかじめ期間を指定し、その期間中に起こりうる事象を常
「一定期間監視型」ではなく、突発的に調査を行い、そこから情報を収集す
の調査方法を採用しています。そのため、調査実施後システムに変更が発生
見された脆弱性が適用されない場合もありますのでご了承ください。

○○株式会社 様

2.2 システム脆弱性診断サマリ

【Web アプリケーション調査項目概要】

診断項目	主な例
入出力処理	クロスサイトスクリプティング
	HTML タグインジェクション
	SQL インジェクション
	コマンドインジェクション
	パスマニピュレーション
	ファイルアップロード
	パラメータ推測
	例外処理に関する問題
認証	ログインフォームに関する調査
	ログイン情報の送受信に関する調査
	認証回避に関する調査
	パスワードの強度に関する調査
セッション管理	Cookie に関する調査
	セッション ID に関する調査
	セッションハイジャック
	クロスサイトリクエストフォージェリ
	クリックジャッキング
	セッションタイムアウト
	ユーザ権限に関する調査
重要情報の取り扱い	ユーザ情報の管理に関する調査
	クレジットカード情報の管理に関する調査
	強制ブラウジング
システム情報・ポリシー	システム情報の開示
	エラーメッセージの表示に関する調査
	ディレクトリリスティング
	ソフトウェアの既知の脆弱性
	ディレクトリトラバーサル
その他	ユーザビリティや品質に関する問題

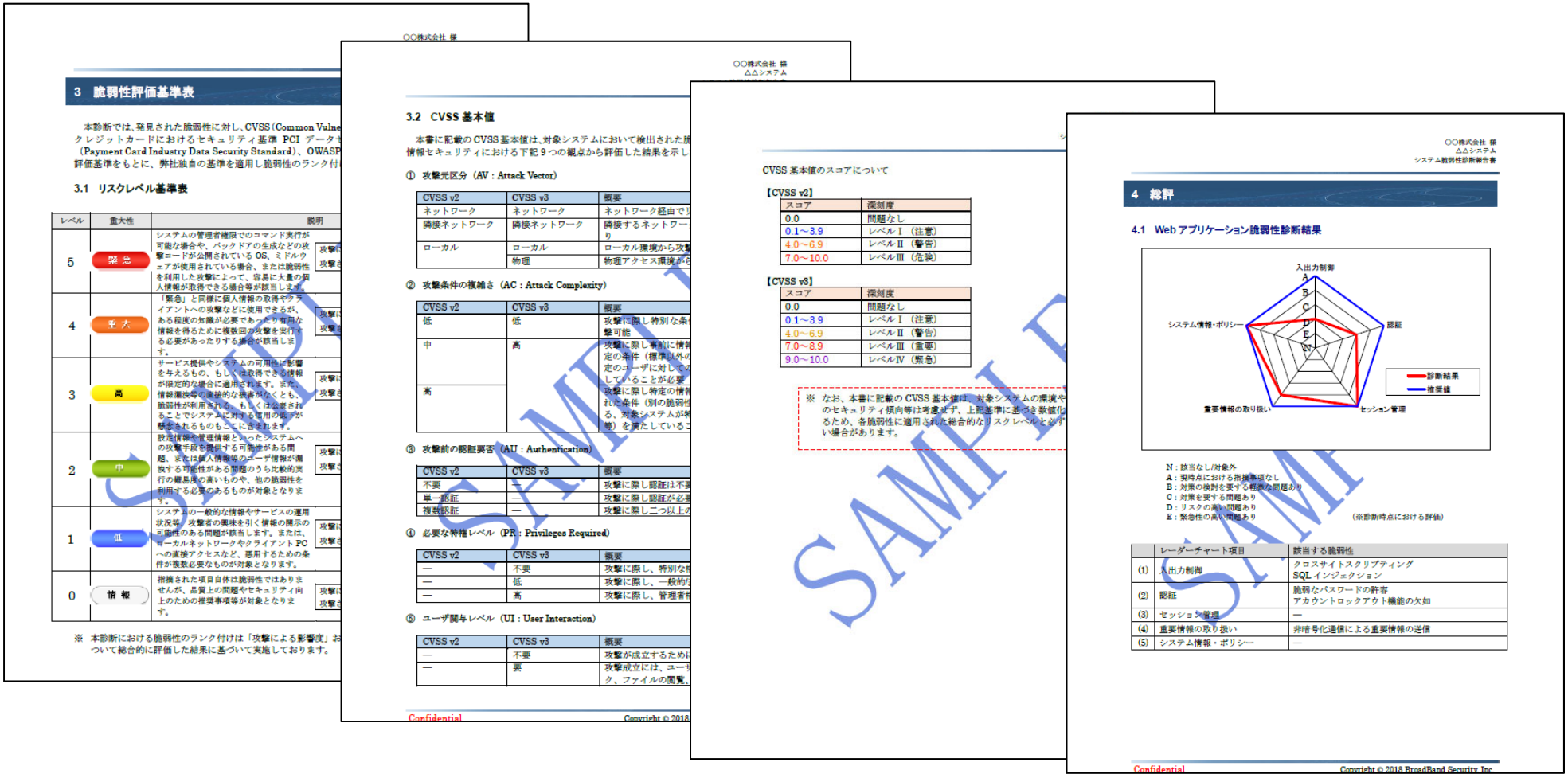
○○株式会社 様
△△システム
システム脆弱性診断報告書

【ネットワーク調査項目概要】

診断項目	主な例	実施
ホストのスキャン	TCP、UDP、ICMP でのポートスキャン	✓
	実行中のサービスの検出	✓
ネットワークサービスの脆弱性	DNS に関する調査	✓
	メールサーバに関する調査	✓
	FTP に関する調査	✓
	RPC に関する調査	✓
	ファイル共有に関する調査	✓
	SNMP に関する調査	✓
	SSH サーバに関する調査	✓
	データベースサーバに関する調査	✓
	その他サービスに関する調査	✓
Web サーバの脆弱性	Web サーバの脆弱性	✓
	Web アプリケーションサーバの脆弱性	✓
	許可されている HTTP メソッド	✓
各種 OS の脆弱性	Windows の既知の脆弱性	✓
	Solaris の既知の脆弱性	✓
	各種 Linux ディストリビューションの既知の脆弱性	✓
	その他各種 OS の既知の脆弱性	✓
悪意あるソフトウェア	バックドアの調査	✓
	P2P ソフトウェアの調査	✓
ネットワーク機器の脆弱性	各種ルータ機器の既知の脆弱性	✓
	各種ファイアウォール機器の既知の脆弱性	✓
	その他各種ネットワーク機器の既知の脆弱性	✓
その他	その他ホスト全体の調査	✓
ご希望時のみ実施する調査	サービス運用妨害（DoS）攻撃	—
	総当り（Brute Force）攻撃	—

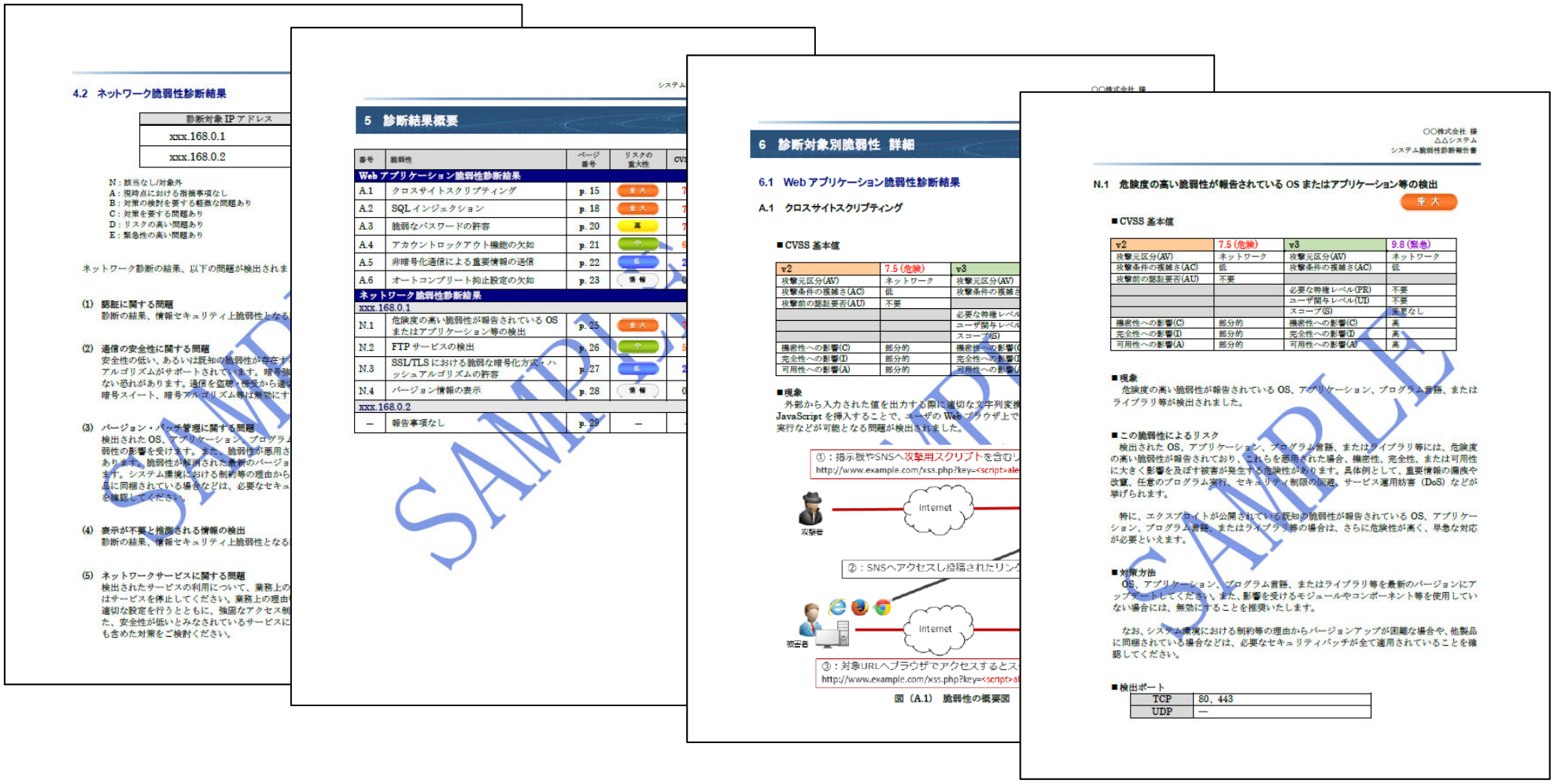
レポートサンプル-2

診断レポートのイメージをサンプルとして抜粋いたします。



レポートサンプル-3

診断レポートのイメージをサンプルとして抜粋いたします。



4.2 ネットワーク脆弱性診断結果

診断対象 IP アドレス
xxx.168.0.1
xxx.168.0.2

N：該当なし/対象外
A：現時点における指摘事項なし
B：対策の検討を要する軽微な問題あり
C：対策を要する問題あり
D：リスクの高い問題あり
E：緊急性の高い問題あり

ネットワーク診断の結果、以下の問題が検出されま

(1) 認証に関する問題
診断の結果、情報セキュリティ上脆弱性となる

(2) 通信の安全性に関する問題
安全性の低い、あるいは既知の脆弱性が存在す
アルゴリズムがサポートされています。暗号強
ない恐れがあります。通信を盗聴・改変から適
暗号スイート、暗号アルゴリズム等は無効にす

(3) バージョン・パッチ管理に関する問題
検出された OS、アプリケーション、プログラム
弱性の影響を受けます。また、脆弱性が悪用さ
あります。脆弱性が解消された最新のバージョ
ます。システム環境における制約等の理由から
品に同梱されている場合などは、必要なセキュ
を確認してください。

(4) 表示が不要と推測される情報の検出
診断の結果、情報セキュリティ上脆弱性となる

(5) ネットワークサービスに関する問題
検出されたサービスの利用について、業務上の
はサービスを停止してください。業務上の理由
適切な設定を行うとともに、強固なアクセス制
た、安全性が低いとみなされているサービスに
も含めた対策をご検討ください。

5 診断結果概要

番号	脆弱性	ページ番号	リスクの重大性	CVS
Web アプリケーション脆弱性診断結果				
A.1	クロスサイトスクリプティング	p. 15	重大	7
A.2	SQL インジェクション	p. 18	重大	7
A.3	脆弱なパスワードの許容	p. 20	高	7
A.4	アカウントロックアウト機能の欠如	p. 21	中	5
A.5	非暗号化通信による重要情報の送信	p. 22	低	2
A.6	オートコンプリート抑止設定の欠如	p. 23	情報	0
ネットワーク脆弱性診断結果				
xxx.168.0.1				
N.1	危険度の高い脆弱性が報告されている OS またはアプリケーション等の検出	p. 25	重大	7
N.2	FTP サービスの検出	p. 26	中	5
N.3	SSL/TLS における脆弱な暗号化方式・ハッシュアルゴリズムの許容	p. 27	低	2
N.4	バージョン情報の表示	p. 28	情報	0
xxx.168.0.2				
—	報告事項なし	p. 29	—	

6 診断対象別脆弱性 詳細

6.1 Web アプリケーション脆弱性診断結果

A.1 クロスサイトスクリプティング

■CVSS 基本値

v2	7.5 (危険)	v3	
攻撃元区分(AV)	ネットワーク	攻撃元区分(AV)	
攻撃条件の複雑さ(AC)	低	攻撃条件の複雑さ	
攻撃前の認証要否(AU)	不要		
		必要な特権レベル	
		ユーザ関与レベ	
		スコープ(S)	
機密性への影響(C)	部分的	機密性への影響	
完全性への影響(I)	部分的	完全性への影響	
可用性への影響(A)	部分的	可用性への影響	

■現象
外部から入力された値を出力する際に適切な文字列変換
JavaScript を挿入することで、ユーザの Web ブラウザ上で
実行などが可能となる問題が検出されました。

図（A.1） 脆弱性の概要図

○○株式会社 様
△△システム
システム脆弱性診断報告書

N.1 危険度の高い脆弱性が報告されている OS またはアプリケーション等の検出

重大

■CVSS 基本値

v2	7.5 (危険)	v3	9.8 (緊急)
攻撃元区分(AV)	ネットワーク	攻撃元区分(AV)	ネットワーク
攻撃条件の複雑さ(AC)	低	攻撃条件の複雑さ(AC)	低
攻撃前の認証要否(AU)	不要		
		必要な特権レベル(PR)	不要
		ユーザ関与レベル(UI)	不要
		スコープ(S)	変更なし
機密性への影響(C)	部分的	機密性への影響(C)	高
完全性への影響(I)	部分的	完全性への影響(I)	高
可用性への影響(A)	部分的	可用性への影響(A)	高

■現象
危険度の高い脆弱性が報告されている OS、アプリケーション、プログラム言語、またはライブラリ等が検出されました。

■この脆弱性によるリスク
検出された OS、アプリケーション、プログラム言語、またはライブラリ等には、危険度の高い脆弱性が報告されており、これらを悪用された場合、機密性、完全性、または可用性に大きく影響を及ぼす被害が発生する危険性があります。具体例として、重要情報の漏洩や改竄、任意のプログラム実行、セキュリティ制限の回避、サービス運用妨害（DoS）などが挙げられます。

特に、エクスプロイトが公開されている既知の脆弱性が報告されている OS、アプリケーション、プログラム言語、またはライブラリ等の場合は、さらに危険性が高く、早急な対応が必要といえます。

■対策方法
OS、アプリケーション、プログラム言語、またはライブラリ等を最新のバージョンにアップデートしてください。また、影響を受けるモジュールやコンポーネント等を使用していない場合には、無効にすることを推奨いたします。

なお、システム環境における制約等の理由からバージョンアップが困難な場合や、他製品に同梱されている場合などは、必要なセキュリティパッチが全て適用されていることを確認してください。

■検出ポート

TCP	80、443
UDP	—

脆弱性・リスク評価基準

検出された脆弱性に対して 「攻撃による影響度」と「攻撃される可能性」について総合的に評価し、危険度を５～１までに分類、問題箇所の事象・リスク・対策方法を解説いたします。

	リスクレベル		解説
現象・リスク・対策方法を解説	5	緊急	システムの管理者権限でのコマンド実行が可能な場合や、バックドア生成などの攻撃コードが公開されているOS・ミドルウェアが使用されている場合、または脆弱性を利用した攻撃によって、容易に大量の個人情報の取得や改竄が可能な場合などが該当します。
	4	重大	「緊急」と同様に個人情報の取得やクライアントへの攻撃などに使用できるが、ある程度の知識が必要であったり有用な情報を得るために複数回の攻撃を実行する必要があったりする場合が該当します。
	3	高	サービス提供やシステムの可用性に影響を与えるもの、もしくは取得できる情報が限定的な場合に適用されます。また、情報漏洩等の直接的な被害がなくとも、脆弱性が利用される、もしくは公表されることでシステムに対する信用の低下が懸念されるものもここに含まれます。
	2	中	設定情報や管理情報といったシステムへの攻撃手段を提供する可能性がある問題、または個人情報等のユーザ情報が漏洩する可能性がある問題のうち比較的実行の難易度の高いものや、他の脆弱性を利用する必要のあるものが対象となります。
	1	低	システムの一般的な情報やサービスの運用状況等、攻撃者の興味を引く情報の開示の可能性のある問題が該当します。または、ローカルネットワークやクライアントPCへの直接アクセスなど、悪用するための条件が複数必要なものが対象となります。
現象を解説	0	情報	指摘された項目自体は脆弱性ではありませんが、品質上の問題やセキュリティ向上のための推奨事項等が対象となります。

外部脆弱性診断　SQAT® A&P（Web+Network）

当社の診断事例を記載いたします。

年間延べ5,000システム以上の脆弱性診断（ペネトレーションテスト含む）を実施しています。
高いセキュリティ基準が求められる金融業においては、直近の過去3年間で延べ約500社、約18,000システムに対する診断実績がございます。

業種	対象組織	規模	利用ケース
官公庁	海上保安庁	約40リクエスト	一般利用者向け電子計算機システムに対して、外部脆弱性診断を定期的（年2回）に実施
官公庁	人事院	約10IPアドレス	インターネット接続サービス安全・安心マーク制度の基準準拠のために外部脆弱性診断を定期的に実施（当社は同制度の認定診断ベンダー）
官公庁	特許庁	約40IPアドレス	内部ネットワークおよびインターネット公開システムに対し脆弱性診断を実施
公益・特殊・独立行政法人	某一般財団法人	約20リクエスト 約15IPアドレス 約５API	試験受験申込サイトに対して、外部脆弱性診断を定期的（年2回～3回）およびシステム更改時に実施
公益・特殊・独立行政法人	某国立研究開発法人	約50リクエスト	研究課題管理システムのセキュリティ担保およびリスク評価のため外部脆弱性診断を活用
公益・特殊・独立行政法人	某公益財団法人	約70リクエスト	助成財団向け業務支援系システムの安全性確認・維持のため定期的（2年に一度）に外部脆弱性診断を実施
金融・保険業	某保険会社	約200リクエスト 約10IPアドレス	GDPR対応に更改したシステムの状況確認のために脆弱性診断を実施

診断事例・実績

外部脆弱性診断　SQAT® A&P（Web+Network）

業種	対象組織	規模	利用ケース
金融・保険業	メガバンク （某大手銀行）	約1000リクエスト 約100IPアドレス	メガバンクおよび傘下のグループ銀行のシステムについて「Webサイトシステム」および「外部サービス」のセキュリティに関する検査として脆弱性診断を定期的（毎年）に実施
金融・保険業	某銀行	約300リクエスト 約20IPアドレス	PCI DSS準拠のための脆弱性スキャン・ペネトレーションテストを実施（Web：年1回、NW：年4回）
金融・保険業	某銀行	約200リクエスト	同行ホームページ、ローン審査申込機能、口座開設機能等に対しセキュリティ維持のため外部脆弱性診断を定期的に活用
金融・保険業	複数信用金庫	約500リクエスト	グループ信用金庫（約50社）に対し、金融庁発行のセキュリティ指針/ガイドライン/基準遵守を目的とした脆弱性診断実施
金融・保険業	某外資系保険会社	約100リクエスト 約60IPアドレス	米国親会社のセキュリティポリシーで要求される基準を満たすために外部脆弱性診断を定期的（年1回）に実施
金融・保険業	某信用金庫	約200リクエスト 約30IPアドレス	複数の一般利用者向けWebサイト（ネットバンキングシステム）および外部接続サーバに対して、外部脆弱性診断を定期的に実施
金融・保険業	某協同組合連合会	約300リクエスト 約10IPアドレス	一般利用者向けインターネット共済加入および各種手続ページのセキュリティ対策の一環として外部脆弱性診断を定期的（年1回）に実施
金融・保険業	某決済業務代行会社	20000リクエスト以上 3000IPアドレス以上	決済代行を行う各種企業との連携システムやネットワークのセキュリティリスク評価および安全性確保のため、新規構築～機能追加の都度、外部脆弱性診断を実施

診断事例・実績

外部脆弱性診断　SQAT® A&P（Web+Network）

業種	対象組織	規模	利用ケース
金融・保険業	大手証券会社	約600リクエスト 約200IPアドレス	一般利用者向けWebサイトおよび内部インフラに対して、外部/内部脆弱性診断を実施
金融・保険業	大手金融グループ	約1000IPアドレス	PCI DSS準拠のための脆弱性スキャン・ペネトレーションテストを実施（NW：年4回）
金融・保険業	某カード会社	約200IPアドレス	PCI DSS準拠のための脆弱性スキャン・ペネトレーションテストを実施（NW：年4回）
金融・保険業	某信託銀行	約500IPアドレス	FEPシステム含む、複数の重要役割を持つシステムのセキュリティチェックに脆弱性診断を活用
商業	某ECサイト運営会社	約500リクエスト 約30IPアドレス	オンラインショッピングサイトと周辺システムに対して、外部/内部からの脆弱性診断を定期的（年１回）に実施
情報・通信業	某ITソリューション会社	約300リクエスト	ソリューション開発したWebサイトに対してサービス提供前のセキュリティチェックに活用
製造業	某鉄鋼会社	約1000リクエスト	社内業務システムに対して、機能拡充前に現状のセキュリティリスク可視化に脆弱性診断を活用
情報・通信業	某ゲーム会社	約300リクエスト	ゲーム関連のコミュニティサイトに対して、新規構築～機能追加の都度、外部脆弱性診断を実施
情報・通信業	某システム開発会社	約300IPアドレス	PCI DSS準拠のための脆弱性スキャン・ペネトレーションテストを実施（NW：年4回）
電気・ガス業	某ガス会社	約2000リクエスト 約150IPアドレス	グループ全体で保有するWebサイト/インフラに対して、定期的な脆弱性診断を実施。また、対象システムの重要度に応じたペネトレーションテストを実施

スマホアプリが抱えるリスク

スマホアプリはWEBアプリと比べて下記のような独自のリスクを抱えています。

A) 重要情報の取り扱い

スマホアプリでは「電話帳・メール・通信ログ・位置情報（GPS）・決済情報・利用履歴」といった、WEBアプリよりも多くの重要情報が扱われる。

B) クライアント端末側での情報保持

WEBアプリでは、サービス提供者が管理可能なサーバ側で情報を保持していたが、スマホアプリはユーザ端末側に情報が保持される。サーバ側は OS・サービスへのパッチ適用、Firewall 等のセキュリティソリューションで守れたが、ユーザ端末の保護はユーザに依存する。

C) クライアント・サーバ間の通信

WEBアプリでは、一般に普及しているブラウザ（Chrome, Safariなど）でアクセスするが、スマホアプリでは独自開発された機能でアクセスする。常時電源オンかつインターネットに常時接続された状態である。

過去に発見された脆弱性の事例

✓ Skypeの脆弱性

内容：チャット履歴や個人情報を含む端末内ファイルが、他のアプリからアクセス可能な状態になっていた
原因：ファイルパーミッションの設定不備
参考：http://www.itmedia.co.jp/enterprise/articles/1104/19/news025.html

✓ GREEの脆弱性

内容：端末内に保管されたユーザ情報が、他のアプリからアクセスできる状態になっていた
原因：独自開発したブラウザ（WebView)の脆弱性
参考：http://jvn.jp/jp/JVN99192898/

✓ mixiの脆弱性

内容：「友人の発言」が、他のアプリからアクセスできる状態になっていた
原因：アクセス制御ができないSDカード領域への機密情報の保管
参考：http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-000078.html

① アプリケーションそのものの診断（スマホアプリ診断）
② スマホアプリ ⇔ サーバ間の通信の診断（API診断）
をご提供いたします。

① スマホアプリ診断

診断担当者

実機を使用し、以下（例）に関する診断を実施します。
- 個人情報、決済情報など重要情報の取り扱い
- アプリによる端末情報の不正送信
- 端末に保有された情報へのアクセス制御、暗号化
- リバースエンジニアリングによる詳細な分析

② API診断

診断担当者

プロキシツールを使用し、以下（例）に関する診断を実施します。
- コマンドインジェクション、SQLインジェクション
- API不正操作による改竄、なりすまし、情報漏洩
- 認証・セッション機構に対する不正操作
- 不正なHTTPメソッドによる影響

API通信

APIサーバ

※Android、iOSともに多数の診断実績がございます。

ご準備・ご提供のお願い

A) スマホアプリファイル（IPA/APK）

稼動するスマホアプリファイルをご提供ください。アプリのソースコードをご提供いただく必要はございません。アプリ操作のためにアカウントが必要である場合は、あわせてご提供ください。
また、スマホアプリの仕様によっては、弊社端末のUIDを事前にご登録いただく場合がございます。

B) API電文仕様書（正常リクエスト・レスポンスのサンプル）

API診断をご依頼の際は、API電文仕様書および正常リクエスト・レスポンスのサンプルの提示をお願い致します。サンプルのAPI電文仕様書もご用意しておりますので、参考にされる場合は、お申し付けください。

C) サーバへのアクセス許可

スマホアプリがサーバと通信する場合（API診断を実施しない場合でも）は、弊社診断元IPアドレスからのアクセス許可をお願いします。診断元IPアドレスはヒアリングシートに記載しております。

D) ヒアリングシート

ご連絡先や診断種別・対象情報などを記入済みのヒアリングシートの提出をお願い致します。

診断の観点（スマホ&API）

【スマホ診断】

総務省が提言する「関係事業者向け スマートフォン利用者情報取扱指針」で示された6つの基本原則を考慮し、JSSEC セキュアコーディングガイド、OWASP Mobile Top10に基づきセキュリティ診断を実施します。

【API診断】

APIサーバに対するリクエスト/レスポンスを検証、攻撃者と同じ観点であるブラックボックステスト・疑似攻撃による検証を行います。OWASP Top10などの標準を網羅することはもちろんのこと、最新の脆弱性に対応したシグネチャによる検証も行います。

スマホ診断・API診断とも、発見された脆弱性に対し、CVSS（Common Vulnerability Scoring System）、OWASP Top10、CWE等、国際的な脆弱性評価基準をもとに、弊社独自の基準を適用し脆弱性のランク付けを行います。
診断によって洗い出された問題点は一つ一つ誤検知・過検知を取り除くとともに、対象システムの特性や攻撃の難易度等によりリスク評価を行います。
また、お客様の業種やシステム環境、保持している情報の種類等、他の要因も考慮したリスク分析により、どの問題部位に修正を施すべきかどうかを正確に確認することができます。

スマホアプリ診断 診断項目

実機を使った動的解析とAPK（Android）・IPA（iOS）ファイルの静的解析を実施します。
基本的には攻撃者と同じ観点であるブラックボックステストを実施します。

大項目	中項目	
プラットフォーム種別	Androidアプリ	iOSアプリ
通信診断	**不正通信の有無**（不要な情報の送信・意図しないサーバとの通信）	
	重要情報の送信における不備（個人情報・ID/パスワード・決済情報）	
	SSL/TLS暗号化通信の検証（証明書・暗号化方式）	
端末内データ診断	**データ保持における不備**（File, Database等での平文保持）	
	データ改竄による不正行為（チート・課金回避）	
	ログへの重要情報の出力（個人情報・ID/パスワード）	
	パーミッションの設定不備	ー
	SDカードへの機密情報の出力	ー
バイナリ診断（プラチナプランのみ）	**アプリ間連携・共有機能のアクセス制御不備**	ー
	WebView関連の問題点の有無	
	難読化・耐タンパー性の確認	
	プロトコルの解析（HTTP以外）	
	リバースエンジニアリングによる解析（ソースコード・ロジック）	

API診断 診断項目

SOAT® for Smartphone

APIサーバに対するリクエスト/レスポンスを検証・疑似攻撃による検査を実施します。
基本的には攻撃者と同じ観点であるブラックボックステストを実施します。

大項目	中項目	
入出力処理	クロスサイトスクリプティング	SQLインジェクション
	コマンドインジェクション	パスマニピュレーション
	パラメータ推測	例外処理に関する問題
	オープンリダイレクト	CRLFインジェクション
認証	ログイン・認証処理に関する調査	パスワードの強度に関する調査
セッション管理	セッションID・トークンに関する調査	セッションハイジャック・固定化
	クロスサイトリクエストフォージェリ	アカウントの権限に関する調査
重要情報の取り扱い	個人情報・決済情報などの管理に関する調査	
	キャッシュ制御に関する調査	強制ブラウジング
システム情報・ポリシー	システム情報の開示・エラーメッセージの表示	
	ディレクトリリスティング	ソフトウェアの既知の脆弱性

診断の流れ（スマホアプリ＆API）

SOAT® for Smartphone

診断前準備・調査＊1

予備調査 → クローリング → 対象APIの機能分析（Point）

ご提供頂く電文仕様書を元に事前調査（クローリング）を実施し、診断対象APIの機能・リクエストの選定と検査手法を設定いたします。手動での詳細な確認によって、機械的な判断では見落としてしまう処理の分岐にも対応いたします。

診断実施＊2

脆弱性診断 → 複数ツールによるスキャン → ホワイトハッカーによる擬似攻撃 → バイナリ解析＊＊（Point） → エビデンス取得リスク評価

商用/自社開発ツールを用いて、対象APIおよびスマートフォンアプリの脆弱性・問題部位を洗い出します。
数年以上の経験を持ったエンジニアが、業界標準および弊社独自の手法を用いて擬似攻撃/解析を行います。
オーディット専門部門が、対象システムの特性に応じたリスクを評価いたします。
＊＊バイナリ解析は「スマホアプリ プラチナ診断」をご依頼の場合に実施いたします。

報告書作成～報告会

報告書作成 → BCPに対するリスク評価（Point） → トレンドにもとづく脅威評価（Point） → 報告会

レビュー専門部門が、対象システムの利用範囲や環境を考慮し、組織の事業継続リスクの評価を行います。また、昨今のセキュリティ事象や傾向を加味したリスク分析結果にもとづき、脅威を評価します。
実際に診断・解析を担当したエンジニアや上級エンジニアが報告を行い、質疑応答にも対応いたします。

診断保守

結果報告後の対応 → 再診断＊3 → ソースコード診断 CPE Core ＊3

報告書提出後３ヶ月間は、指摘内容・対策についての質問をお受けいたします。また、修正いただいた指摘内容の再診断も実施いたします。
その他、弊社サービス「Cracker Probing-Eyes Core」でのソースコード診断も合わせてご検討ください。

＊１：API診断をご依頼の場合のみ実施いたします。
＊２：重大な問題点を検出した場合は「速報」として随時ご報告いたします。
＊３：有償のメニューとなりますので、弊社営業担当までご連絡ください。

API診断

SOAT® for Smartphone

機能・URL・パラメータ・値・留意事項をAPIリクエスト単位で調査し、仕様外の操作が行えないか検査します。また、Webアプリケーションと同様に、各種インジェクション攻撃に対して脆弱か、セッションが適切に管理されているか等を検査します。

API電文仕様書のサンプル

エントリポイントURL

テスト環境	https://bbsec.co.jp/api/

共通HTTPヘッダー

HTTPリクエストヘッダ		
key	value	詳細
X-BBSEC-ACKEY	以下の値をコロン:で連結した値 App123456789:リクエスト時間(UNIX time)	API認証で使用するデータ リクエスト時間がサーバ日時と60秒以上ずれていると認証エラーを返す。
X-BBSEC--SECKEY	以下の値をコロン:で連結しSHA256でハッシュ化した値(16進数表現) App123456789:リクエスト時間(UNIX time):[共有鍵]	API認証するためのハッシュ サーバ側でもアプリキーに対応する共有鍵で同様のハッシュ値を生成し、一致しなければ認証エラーを返す。
X-BBSEC--SESSION-ID	ログインAPIで取得したセッションID	セッションIDの有効期限が切れていた場合はエラーとなる。
CLIENT-PLATFORM	iosまたはandroidのいずれか	プラットフォームの識別子として値をセットする
CLIENT-OS-VER	例)　[iOS]9.0.2 [Android]5.0	OSバージョン（文字列） AndroidはBuild.VERSION_RELEASEの値
CLIENT-APP-VER	例)　1.0.0	アプリバージョン（文字列） AndroidはBuildConfig.VERSION_CODEの値

共通JSONレスポンス

status	0 ・・・ 正常終了 101 ・・・ 認証失敗 201 ・・・ パラメータ不正 202 ・・・ リクエスト時間不正 301 ・・・ リクエスト件数が一定量超過 401 ・・・ セッションIDが有効期限を過ぎている 999 ・・・ 予期しないエラー	全API共通 各API専用のレスポンスコードは各APIで800番台に定義する

通信診断

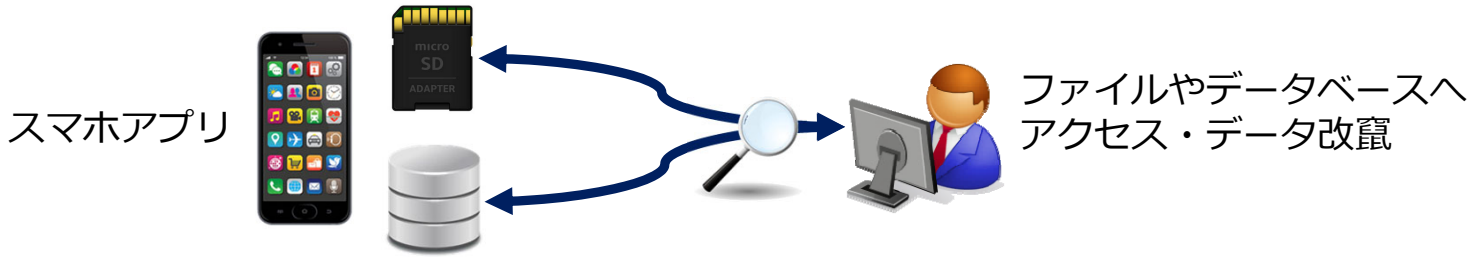
内容	不正通信の有無	電話帳などの不必要な個人情報の送信や、不正なサーバに対する通信が発生していないかを検査
	重要情報の送信における不備	重要情報を送信する際に、非暗号化などの安全でない通信方法が用いられていないかを検査
	SSL/TLS暗号化通信の検証	SSL/TLS通信で用いるサーバ証明書を適切に検証しているかを検査
手法	スマホアプリの通信をProxyでキャプチャし内容を調査する	
使用ツール	Burp Suite / Fiddler / Wireshark 等	

診断イメージ

端末内データ診断

内容	データ保持における不備	端末内のファイルやデータベースに、パスワードや個人情報などのデータを平文で保存していないことを検査
	データ改竄による不正行為	端末内のデータを改竄することによって不正行為（チート、残高の偽装、課金の回避など）が行えるかを検査
	ログへの重要情報の出力	ユーザの個人情報/機密情報がログに出力されていないかを検査
	パーミッションの設定不備	重要情報を含むファイルが他アプリからアクセスできるパーミッションになっていないかを検査　※ Androidのみ対応
	SDカードへの機密情報の出力	他アプリからアクセス可能なSDカード内へ重要情報を保存していないかを検査　※ Androidのみ対応
手法	アプリを動作させることによって生成される端末内データの内容や保持方法、設定状況を調査する	
使用ツール	SSH 等	

診断イメージ

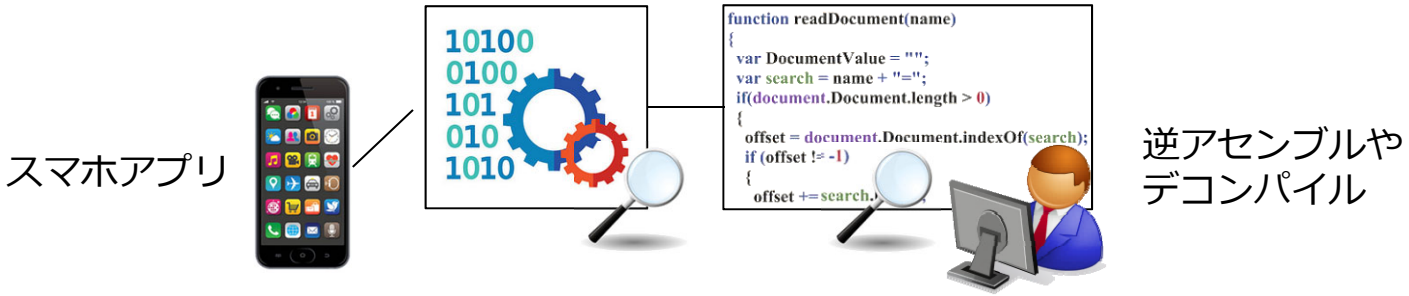


スマホアプリ診断（バイナリ診断）

バイナリ診断 ※プラチナプランのみ対応

内容	アプリ間連携・共有機能のアクセス制御不備	重要情報に対し意図せず他アプリから不正にアクセス可能かを検査
	WebView関連の問題点の有無	WebView機能による情報漏洩の有無や、他アプリとの連携における不備を検査
	難読化・耐タンパー性の確認	アプリのデコンパイル可否や難読化の有無などを検査
	プロトコルの解析（HTTP以外）	プロトコル自体に脆弱な要素が存在しないかを検査
	リバースエンジニアリングによる解析（ソースコード・ロジック）	ロジックの不備による脆弱性や暗号化ロジック・鍵の解析、隠し機能隠しURLの存在などを検査
手法	逆アセンブル・リバースエンジニアリングによって得られたコードを調査する	
使用ツール	IDA Pro / dex2jar 等	

診断イメージ



脆弱性・リスク評価基準

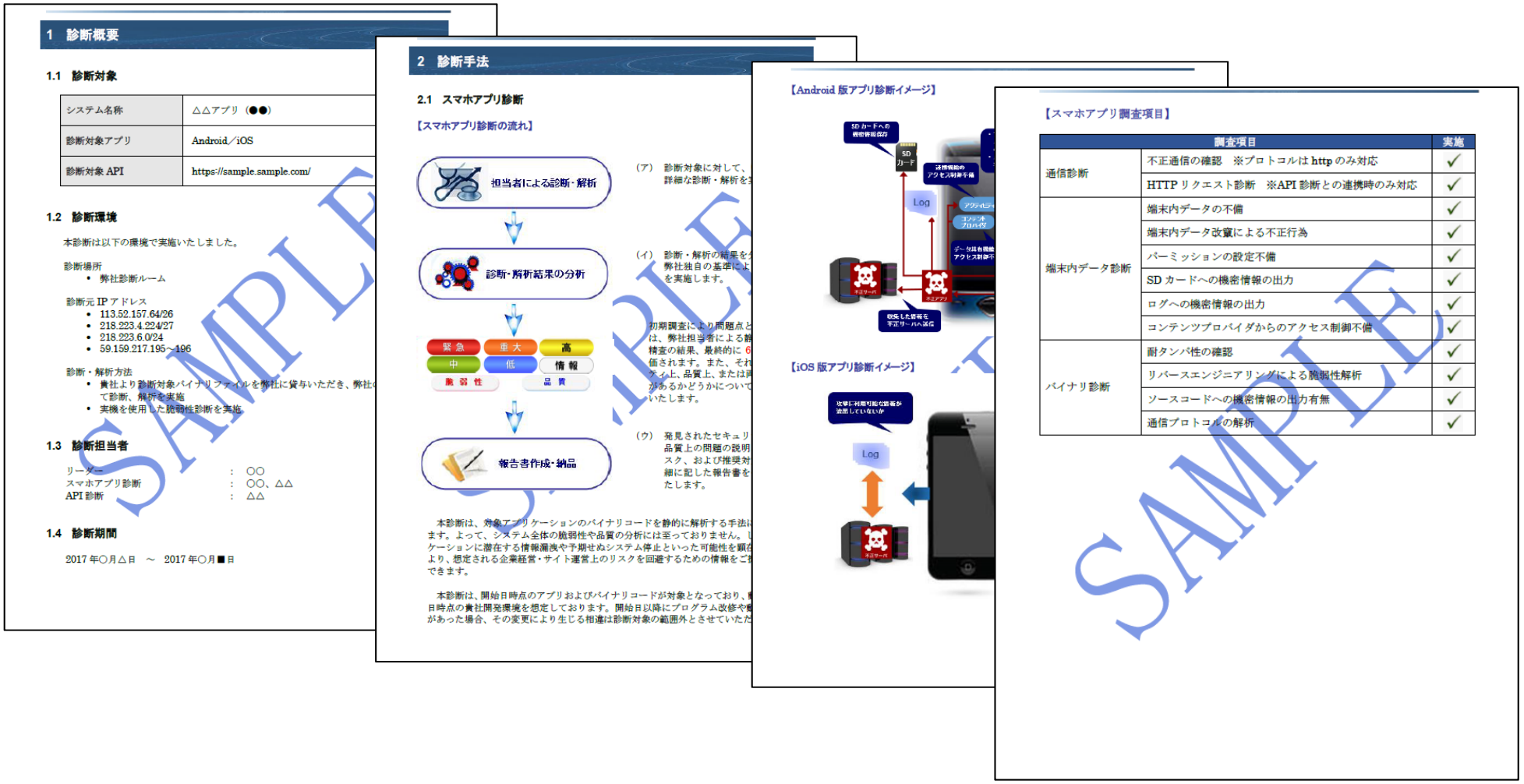
検出された脆弱性に対して 「攻撃による影響度」と「攻撃される可能性」について総合的に評価し、危険度を５～１までに分類、問題箇所の事象・リスク・対策方法を解説いたします。

	リスクレベル		解説
現象・リスク・対策方法を解説	5	緊急	システムの管理者権限でのコマンド実行が可能な場合や、バックドア生成などの攻撃コードが公開されているOS・ミドルウェアが使用されている場合、または脆弱性を利用した攻撃によって、容易に大量の個人情報の取得や改竄が可能な場合などが該当します。
	4	重大	「緊急」と同様に個人情報の取得やクライアントへの攻撃などに使用できるが、ある程度の知識が必要であったり有用な情報を得るために複数回の攻撃を実行する必要があったりする場合が該当します。
	3	高	サービス提供やシステムの可用性に影響を与えるもの、もしくは取得できる情報が限定的な場合に適用されます。また、情報漏洩等の直接的な被害がなくとも、脆弱性が利用される、もしくは公表されることでシステムに対する信用の低下が懸念されるものもここに含まれます。
	2	中	設定情報や管理情報といったシステムへの攻撃手段を提供する可能性がある問題、または個人情報等のユーザ情報が漏洩する可能性がある問題のうち比較的実行の難易度の高いものや、他の脆弱性を利用する必要のあるものが対象となります。
	1	低	システムの一般的な情報やサービスの運用状況等、攻撃者の興味を引く情報の開示の可能性のある問題が該当します。または、ローカルネットワークやクライアントPCへの直接アクセスなど、悪用するための条件が複数必要なものが対象となります。
現象を解説	0	情報	指摘された項目自体は脆弱性ではありませんが、品質上の問題やセキュリティ向上のための推奨事項等が対象となります。

報告書サンプル 1

SOAT® for Smartphone

検出された脆弱性の概要・再現手法・リスク・対策方法を詳細にご報告します。



1 診断概要

1.1 診断対象

システム名称	△△アプリ（●●）
診断対象アプリ	Android／iOS
診断対象 API	https://sample.sample.com/

1.2 診断環境

本診断は以下の環境で実施いたしました。

診断場所
- 弊社診断ルーム

診断元 IP アドレス
- 113.52.157.64/26
- 218.223.4.224/27
- 218.223.6.0/24
- 59.159.217.195～196

診断・解析方法
- 貴社より診断対象バイナリファイルを弊社に貸与いただき、弊社にて診断、解析を実施
- 実機を使用した脆弱性診断を実施

1.3 診断担当者

リーダー　：　○○
スマホアプリ診断　：　○○、△△
API 診断　：　△△

1.4 診断期間

2017 年○月△日　～　2017 年○月■日

2 診断手法

2.1 スマホアプリ診断

【スマホアプリ診断の流れ】

担当者による診断・解析

診断・解析結果の分析

緊急　重大　高　中　低　情報　脆弱性　品質

報告書作成・納品

【Android 版アプリ診断イメージ】

【iOS 版アプリ診断イメージ】

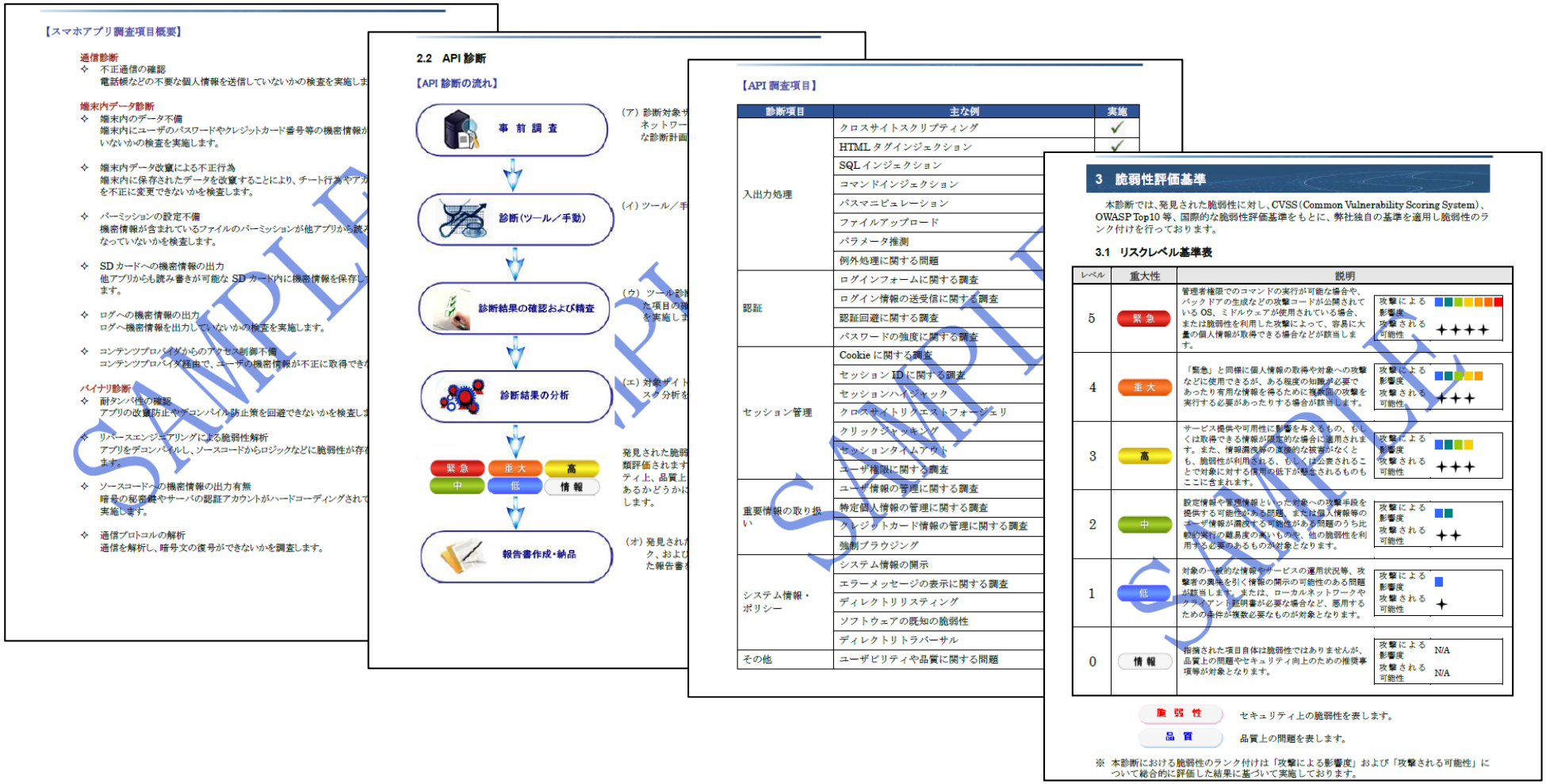
【スマホアプリ調査項目】

調査項目		実施
通信診断	不正通信の確認　※プロトコルは http のみ対応	✓
	HTTP リクエスト診断　※API 診断との連携時のみ対応	✓
端末内データ診断	端末内データの不備	✓
	端末内データ改竄による不正行為	✓
	パーミッションの設定不備	✓
	SD カードへの機密情報の出力	✓
	ログへの機密情報の出力	✓
	コンテンツプロバイダからのアクセス制御不備	✓
バイナリ診断	耐タンパ性の確認	✓
	リバースエンジニアリングによる脆弱性解析	✓
	ソースコードへの機密情報の出力有無	✓
	通信プロトコルの解析	✓

報告書サンプル 2

SOAT® for Smartphone

検出された脆弱性の概要・再現手法・リスク・対策方法を詳細にご報告します。



【スマホアプリ調査項目概要】

通信診断
- 不正通信の確認
  電話帳などの不要な個人情報を送信していないかの検査を実施しま

端末内データ診断
- 端末内のデータ不備
  端末内にユーザのパスワードやクレジットカード番号等の機密情報が
  いないかの検査を実施します。
- 端末内データ改竄による不正行為
  端末内に保存されたデータを改竄することにより、チート行為やア
  を不正に変更できないかを検査します。
- パーミッションの設定不備
  機密情報が含まれているファイルのパーミッションが他アプリから読
  なっていないかを検査します。
- SD カードへの機密情報の出力
  他アプリからも読み書きが可能な SD カード内に機密情報を保存し
  ます。
- ログへの機密情報の出力
  ログへ機密情報を出力していないかの検査を実施します。
- コンテンツプロバイダからのアクセス制御不備
  コンテンツプロバイダ経由で、ユーザの機密情報が不正に取得でき

バイナリ診断
- 耐タンパ性の確認
  アプリの改竄防止やデコンパイル防止策を回避できないかを検査し
- リバースエンジニアリングによる脆弱性解析
  アプリをデコンパイルし、ソースコードからロジックなどに脆弱性が存
  ます。
- ソースコードへの機密情報の出力有無
  暗号の秘密鍵やサーバの認証アカウントがハードコーディングされて
  実施します。
- 通信プロトコルの解析
  通信を解析し、暗号文の復号ができないかを調査します。

2.2 API 診断

【API 診断の流れ】

事前調査
診断(ツール／手動)
診断結果の確認および精査
診断結果の分析
緊急 重大 高 中 低 情報
報告書作成・納品

【API 調査項目】

診断項目	主な例	実施
入出力処理	クロスサイトスクリプティング	✓
	HTML タグインジェクション	✓
	SQL インジェクション	
	コマンドインジェクション	
	パスマニピュレーション	
	ファイルアップロード	
	パラメータ推測	
	例外処理に関する問題	
認証	ログインフォームに関する調査	
	ログイン情報の送受信に関する調査	
	認証回避に関する調査	
	パスワードの強度に関する調査	
セッション管理	Cookie に関する調査	
	セッション ID に関する調査	
	セッションハイジャック	
	クロスサイトリクエストフォージェリ	
	クリックジャッキング	
	セッションタイムアウト	
	ユーザ権限に関する調査	
重要情報の取り扱い	ユーザ情報の管理に関する調査	
	特定個人情報の管理に関する調査	
	クレジットカード情報の管理に関する調査	
	強制ブラウジング	
システム情報・ポリシー	システム情報の開示	
	エラーメッセージの表示に関する調査	
	ディレクトリリスティング	
	ソフトウェアの既知の脆弱性	
	ディレクトリトラバーサル	
その他	ユーザビリティや品質に関する問題	

3 脆弱性評価基準

本診断では、発見された脆弱性に対し、CVSS（Common Vulnerability Scoring System）、OWASP Top10 等、国際的な脆弱性評価基準をもとに、弊社独自の基準を適用し脆弱性のランク付けを行っております。

3.1 リスクレベル基準表

レベル	重大性	説明	
5	緊急	管理者権限でのコマンドの実行が可能な場合や、バックドアの生成などの攻撃コードが公開されている OS、ミドルウェアが使用されている場合、または脆弱性を利用した攻撃によって、容易に大量の個人情報が取得できる場合などが該当します。	攻撃による影響度 ✦✦✦✦ 攻撃される可能性
4	重大	「緊急」と同様に個人情報の取得や対象への攻撃などに使用できるが、ある程度の知識が必要であったり有用な情報を得るために複数回の攻撃を実行する必要があったりする場合が該当します。	攻撃による影響度 ✦✦✦ 攻撃される可能性
3	高	サービス提供や可用性に影響を与えるもの、もしくは取得できる情報が限定的な場合に適用されます。また、情報漏洩等の直接的な被害がなくとも、脆弱性が利用される、もしくは公表されることで対象に対する信用の低下が懸念されるものもここに含まれます。	攻撃による影響度 ✦✦✦ 攻撃される可能性
2	中	設定情報や管理情報といった対象への攻撃手段を提供する可能性がある問題、または個人情報等のユーザ情報が漏洩する可能性がある問題のうち比較的実行の難易度の高いもの、他の脆弱性を利用する必要のあるものが対象となります。	攻撃による影響度 ✦✦ 攻撃される可能性
1	低	対象の一般的な情報やサービスの運用状況等、攻撃者の興味を引く情報の開示の可能性のある問題が該当します。または、ローカルネットワークやクライアント証明書が必要な場合など、悪用するための条件が複数必要なものが対象となります。	攻撃による影響度 ✦ 攻撃される可能性
0	情報	指摘された項目自体は脆弱性ではありませんが、品質上の問題やセキュリティ向上のための推奨事項等が対象となります。	攻撃による影響度 N/A 攻撃される可能性 N/A

脆弱性　セキュリティ上の脆弱性を表します。
品質　品質上の問題を表します。

※ 本診断における脆弱性のランク付けは「攻撃による影響度」および「攻撃される可能性」について総合的に評価した結果に基づいて実施しております。

報告書サンプル 3

SOAT® for Smartphone

検出された脆弱性の概要・再現手法・リスク・対策方法を詳細にご報告します。

API 診断の結果、対象システムにおいて、「重大」リスクを含む複数の脆弱性が検出されました。これら脆弱性が悪用された場合、アクセス制限の回避、機密情報や個人情報の漏洩、なりすましによる不正操作、サービス運用妨害（DoS）攻撃、システム停止等の危険性があります。

(1) 入出力制御に関する問題
診断の結果、情報セキュリティ上脆弱性となる問題は特に検出されて

(2) 認証に関する問題
診断の結果、情報セキュリティ上脆弱性となる問題は特に検出されて

(3) セッション管理に関する問題
対象システムにおいて、クロスサイトリクエストフォージェリ（CSRF）れています。この脆弱性が悪用された場合、本来意図していない処理（削除）を実行される恐れがあります。推測が困難な文字列（トークン）画面制御を導入することを推奨します。

(4) 重要情報の取り扱いに関する問題
診断の結果、情報セキュリティ上脆弱性となる問題は特に検出されて

(5) システム情報・ポリシーに関する問題
サポートの終了した OpenSSL および脆弱性が存在するバージョンの A ました。特に検出された OpenSSL のバージョンは既にサポートが終了 に発見された脆弱性への対策が困難です。早急に脆弱性対策が施された プデートするか、システム環境における制約等の理由からバージョンア には、必要なセキュリティパッチが全て適用されていることを確認して

加えて、本来公開すべきでない情報が外部より閲覧可能です。不用意な 撃者に、攻撃に有用な情報を提供する原因となるため、セキュリティ上 情報セキュリティの最善策である「Need-to-Know（知る必要）」の原則 アクセス管理を実施してください。

4.3 システム脆弱性診断結果に対する所見

対象システムには API において、リスクレベルの高い脆弱性が複数存在し ティ上の不備を意図的に利用した攻撃の影響を受ける危険性があります。また 断においては、軽微リスクではあるものの、重要情報の漏洩につながる危険性 出されています。

検出された脆弱性に関しては、悪用された場合に影響範囲の拡大が懸念され しを行い、下記の対応を実施することが推奨されます。

- 重要情報の取り扱いに関する対策の見直し、改善
- バージョン・パッチ管理の徹底
- セッション管理の見直し、改善

昨今、ミドルウェアに存在する脆弱性や不要に公開された安全性の低いサ た攻撃が活発化しており、既知の脆弱性が存在するバージョンのミドルウェ と、キャンペーンと称した無差別かつ集中的な攻撃の対象となる可能性があ

例えば、2017 年 2 月に公表された WordPress の REST API の処理に起因す ンツ改竄攻撃や 2017 年 3 月より被害が確認されている Apache Struts 2 の脆 部からの不正アクセスのような被害を受ける危険性があるため、システムに ミドルウェアは常に最新版を利用する、必要なセキュリティパッチがすべて適 をご確認ください。

サイバー攻撃は近年益々増加の傾向にあり、攻撃手法も複雑化しております 切な情報セキュリティ対策の導入は急務となっており、その中でも個人情報 扱うシステムにおいては、攻撃に対して堅牢なシステムを構築、維持すること 結論として、「高」リスク以上の脆弱性につきましては早急に修正することを す。また、その他の脆弱性や指摘事項についても、情報セキュリティのさらな に、リスクレベルや影響度に応じた適切な対策を実施してください。但し、対 ムの運用に影響を及ぼす可能性があるため、対応に際してはシステム管理責 必要と考えられます。

なお、特定の事由により段階的な対処法を採用される場合には、関連するリ し、当該リスクが顕在化した場合の対応計画を策定・実施することが重要と

また、システムの改修時等に限らず、セキュリティポリシーの踏襲および定 により、今後とも継続的にシステム全体の安全性を確認することを推奨いた

5 診断結果概要

番号	脆弱性
スマホアプリ診断結果	
Android	
S.1	デバッグログへの重要情報の出力
S.2	重要情報の平文保存
S.3	難読化について
iOS	
S.4	重要情報の平文保存
API 診断結果	
A.1	サポートが終了したバージョンの OpenSSL 使用の可能性
A.2	脆弱性が存在するバージョンの Apache 使用の可能性
A.3	ディレクトリリスティング
A.4	クロスサイトリクエストフォージェリ
A.5	バージョン情報の表示
A.6	不適切な例外処理
A.7	公開不要と推測されるファイルの検出
A.8	サーバ設定に関する推奨事項

6 診断結果詳細

6.1 スマホアプリ診断結果

6.1.1 Android

S.1 デバッグログへの重要情報の出力

脆弱性 品質 低

■CVSS 基本値

v2	2.6（注意）	v3	3.7（注意）
攻撃元区分(AV)	ネットワーク	攻撃元区分(AV)	ネットワーク
攻撃条件の複雑さ(AC)	高	攻撃条件の複雑さ(AC)	高
攻撃前の認証要否(AU)	不要		
		必要な特権レベル(PR)	不要
		ユーザ関与レベル(UI)	不要
		スコープ(S)	変更なし
機密性への影響(C)	部分的	機密性への影響(C)	低
完全性への影響(I)	なし	完全性への影響(I)	なし
可用性への影響(A)	なし	可用性への影響(A)	なし

■現象
本アプリは、デバッグログに API の URL やアクセスキー、token 情報を出力しています。

診断にて取得した結果エビデンス

図 1 token 情報の出力

セキュリティ診断におけるリスク

システムに対する負荷

API診断では、診断対象システムに対し、10アクセス/秒を超える負荷を与えない範囲で実施いたします。DoS攻撃（サービス運用妨害）に該当する項目は実施いたしませんが、診断対象システムに内在する問題により、サービス停止等の影響が発生する可能性がございます。

万が一、システムからの応答がなくなったり、遅延が発生したり、あるいは何らかの異常が認められた場合には、診断を停止し至急ご連絡いたします。

データのバックアップ

脆弱性診断においては細心の注意を払って検査を実施いたしますが、不測の事態が発生した際に、データの削除・変更が発生する可能性がございます。とくに、システムに内在する脆弱性によっては、診断の影響として意図しないデータの登録・更新・削除が起こりえます。

万が一、そのような事態が発生した場合でもデータの復旧を実施できるよう、脆弱性検査開始前に、対象システムのデータのバックアップを忘れずに実施してください。

よくあるご質問

Q：重要情報を扱わないアプリですが、セキュリティ診断を受ける必要はありますか？

A：開発に用いたライブラリが、意図しないサーバに対して不正通信していたというアプリも存在します。また、貴社アプリが攻撃の踏み台となることもありうるため、リリースや機能追加の際には、セキュリティ診断を受診されることを推奨します。

Q：API診断を実施しない場合、アプリ通信先サーバ側のデータバックアップは不要ですか？

A：API診断を実施しない場合であっても、アプリからの通信によってサーバ側のデータに対して改竄やデータ不整合を発生させる可能性はございます。不測の事態への対応として、セキュリティ診断を受診される際は、データバックアップをとることを推奨します。

Q：診断期間はどれくらいですか？

A：アプリの機能・複雑さにもよりますが、ノーマル診断の場合、診断５営業日、報告書作成５営業日、プラチナ診断の場合は、診断１０営業日、報告書作成７営業日が平均的なスケジュールとなります。

Q：診断の結果報告会に開発ベンダを同席させても良いですか？

A：もちろん問題ありません。運用側・開発側がともにセキュリティを意識、対策されることが、最も良い形であると考えます。

お問い合わせは下記までお気軽にご連絡願います。

エクストランスCS株式会社

TEL:06-6537-5222

E-Mail:rental@xtrans-cs.jp

営業：山口、宮田