Digital Shift EXPO 2020

ＡＷＳ公開用サーバー
運用事例から考えるセキュリティ対策と費用バランス

株式会社エクストランスＣＳ

執行役員　営業部部長：山口　成彦

2020年12月10日

会社概要

社名	株式会社エクストランスＣＳ
設立年月日	昭和53年4月1日
代表者	丹羽　直樹
事業内容	サーバーホスティング クラウド設計構築
所在地	大阪市西区新町1－28－11
従業員数	7名　※グループ全体43名
所属グループ	株式会社エクストランス
売上高	エクストランスＣＳ　1.4億円 ※エクストランスグループ全体 ６億円（2019年度）

ホスティング　マネージド

AWS　設計構築 24/365監視運用

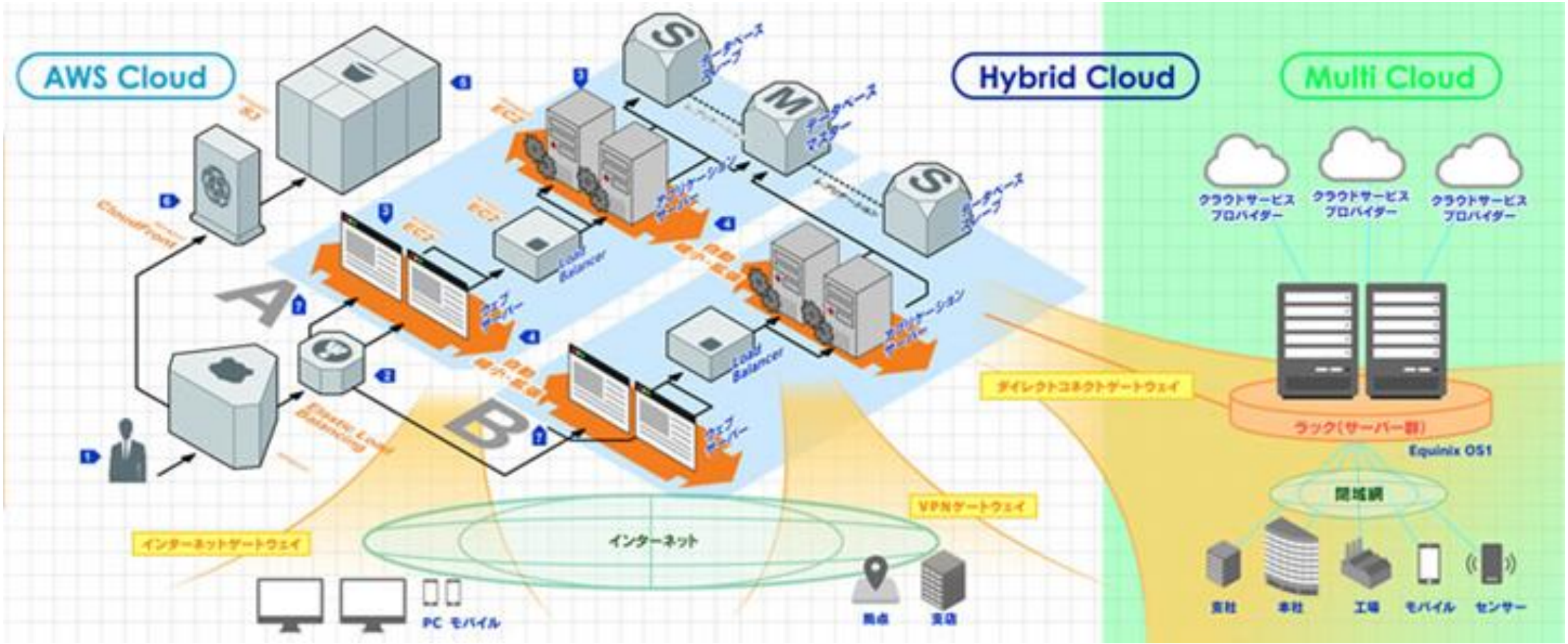
aws partner network

Standard
Consulting
Partner

【運用実績】6,000サービス以上

クラウド
設計・構築・サポート

AWS／ハイブリッド／マルチクラウド



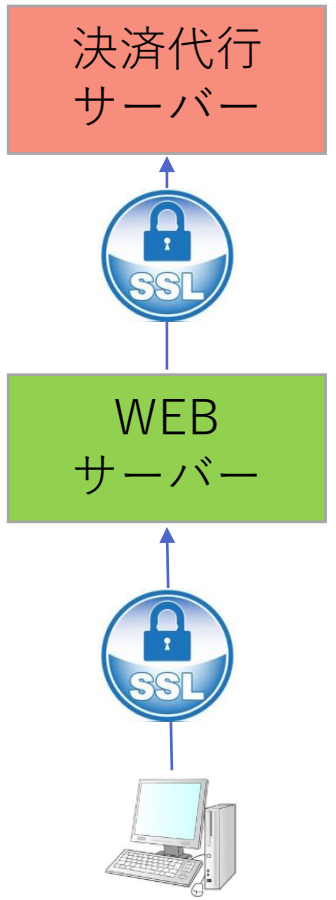
事例①　～ECサイト～

クレジットカード番号漏洩疑惑発覚後、AWSクラウドへ移行

※ Trend Micro Cloud One - Workload Security™
(旧製品名称 Trend Micro Deep Security as a Service ™) 利用

【クレジットカード番号漏洩疑いの状況】

ECサイト



データ伝送(API)型

クレジット
番号入力画面

URL：自社ドメイン

インシデント内容

【不正プログラムの埋込】

一時的に暗号化がとかれたクレジット番号が取得され他社サーバに転送されていた

【コンテンツ側の課題】

漏洩 疑い

クレジット決済代行会社からカード番号漏洩の疑い

クレジットカード取扱停止？

認識 誤り

自社ＷＥＢサーバーではクレジット番号は取り扱っていないという認識

伝送方式？

対処 不明

クレジット番号を取り扱いにはＰＣＩＤＳＳ基準に沿った運用が必要

PCIDSS準拠？

【コンテンツ側での対応】

漏洩	疑い	フォレッジング調査 ※クレジットカード会社指定事業者 日本:3社	100万円～
認識	誤り	クレジットカード番号 伝送方式	リンク（画面遷移） 方式に変更
対処	不明	セキュリティ専門会社に相談したい ↓ コストがあわない	セキュリティを強化し ECサイトを一日でも早く再開したい ↓ インフラ部の提案

【インフラ側の課題】

安全	セキュリティ	再発防止？
設備	クラウド	高負荷対策？
保守	マネージド	運用見直し？

【AWSクラウドへWEBシステムを移行】

プログラム改修をほぼ行わず高負荷対応とセキュリティ向上を考慮したAWS構成

POS基幹系

一括保守

ルータ
マネージドサービス

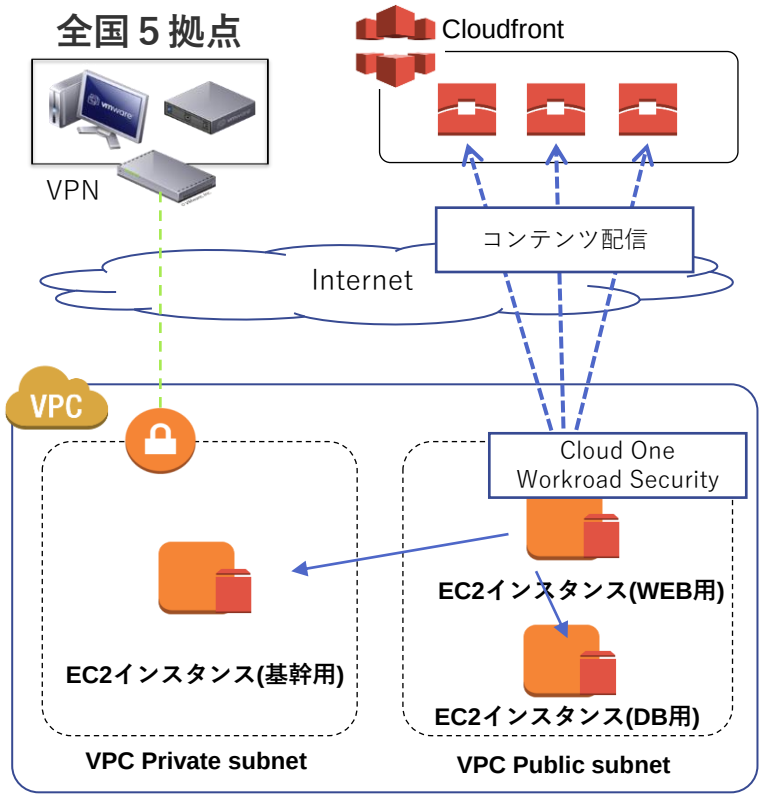
24時間365日
障害対応

Sale時
サーバー負荷

クラウド
マネージドサービス

スケールアップ

ECサイト



クラウド
マネージドサービス

月間１２TBデータ転送量
負荷分散

アクセス
負荷分散

C1WS(旧:DSaaS)
マネージドサービス

Agentアップデート
チューニング
障害／レポート通知

侵入防御

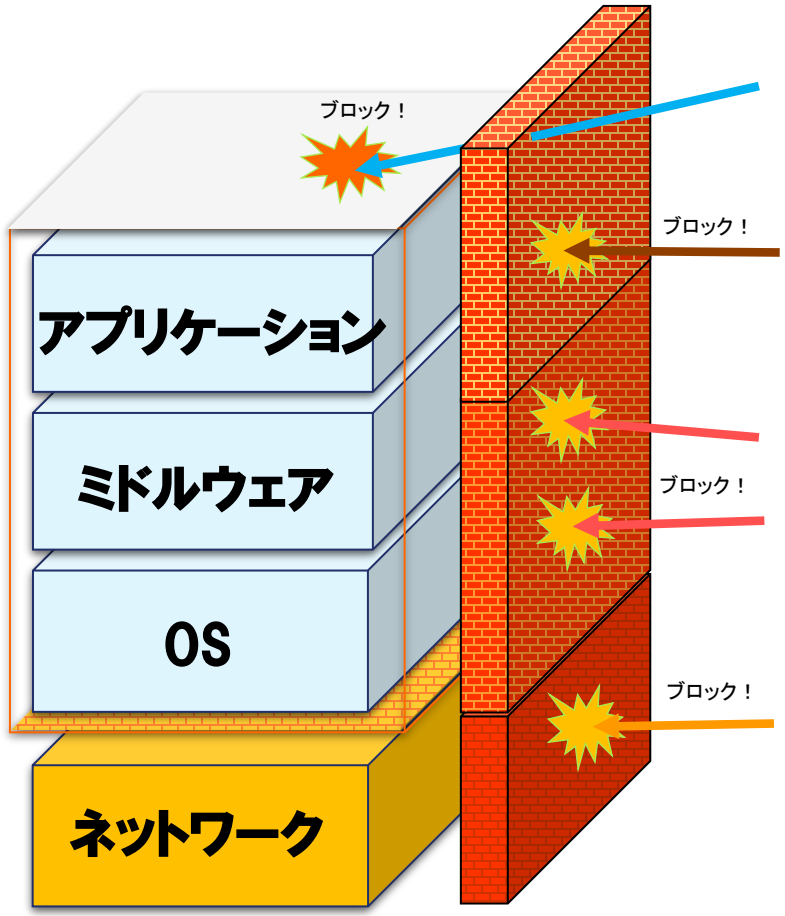
クラウド
マネージドサービス

スケールアップ

Sale時
サーバー負荷

【セキュリティ強化】

WEBアプリケーションへの攻撃を考慮しDeepSecurityを設定



サーバへの攻撃

- サーバを狙った攻撃
- ファイル改ざん
- ルートキットの設置
- サーバへの不正アクセス

ブロック！

Webアプリへの攻撃

- WEBアプリケーションの脆弱性を狙った攻撃
- SQL/OSコマンドインジェクション
- クロスサイトスクリプティング
- Cookie、パラメータ改ざん

ブロック！

OS・Webシステムへの攻撃

- DoS攻撃等の不正アクセス攻撃
- Apache、IIS等の脆弱性を狙った攻撃

ブロック！

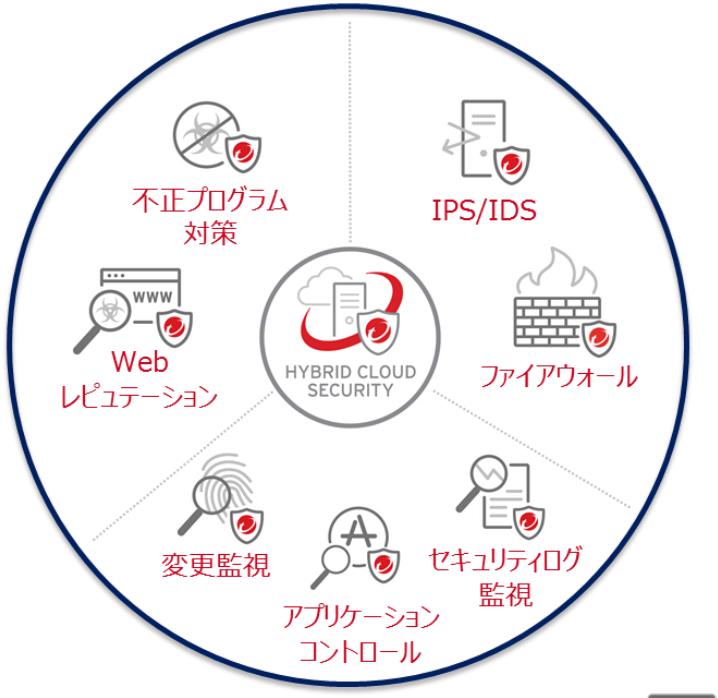
ネットワークへの攻撃

- ネットワークを利用した攻撃
- ポートスキャン
- IP/ポート制御

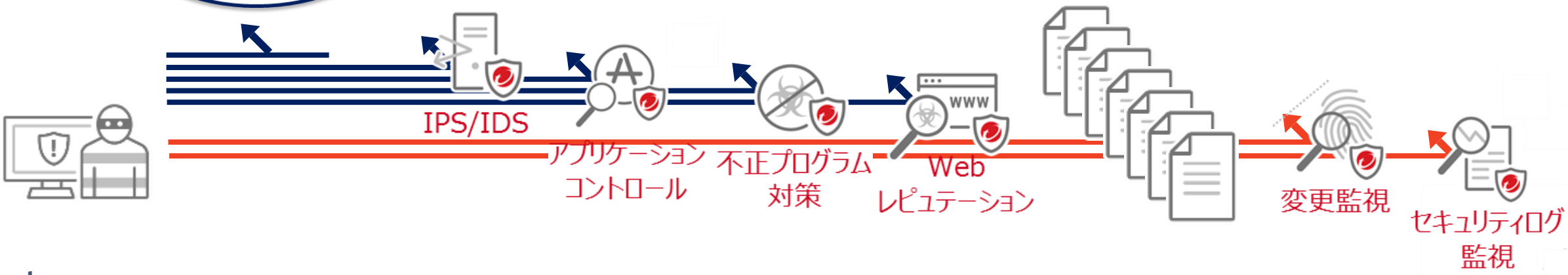
提供ツール/サービス	
WAF	Trend Micro Cloud One - Workload Security™ (旧:DeepSecurity as a Service) Webアプリケーションの脆弱性
IPS (IDS)	OS/Middlewareの脆弱性 ウィルス対策 アプリケーション実行 改ざんの検知
AWS（VPC）	セキュリティグループの設定 ネットワークアクセスコントロールリストの設定

【セキュリティ対策と対応機能】

Trend Micro Cloud One - Workload Security™　(旧:DeepSecurity as a Service)



セキュリティ対策	対策項目	Deep Security 対応機能
ウィルス対策	公開サーバー側のウィルス感染防止	不正プログラム対策
脆弱性対策	脆弱性への攻撃を検知・ブロック	IPS（侵入防御）
	脆弱性の把握と修正パッチ適用	IPS（侵入防御）の推奨設定
自社で攻撃に気付く対策	サーバーやシステムのフィル改ざん検知	システム上の変更監視
	セキュリティログによるサーバー異常の検知	セキュリティログ監視
	不正プログラムの侵入を検知・ブロック	不正プログラム対策
	サーバーを狙った攻撃通信の検知	IPS（侵入防御） ホスト型ファイアウォール
	サーバに設置された遠隔操作ツールの検知	IPS（侵入防御） Webレピュテーション



xtrans cs

【AWS構築運用＋セキュリティ費用】

		初期費用	月額費用
提案中	**WafCharm** WafCharm(ワフチャーム） 攻撃パターンをAIで学習し、WAFのルールを最適化させる自動運用サービス	10,000円 ＋ AWS WAF設定費用	エントリー 5,000円 ビジネス 50,000円 エンタープライズ 95,000円 ※リクエスト数によって変動
	C1WS（旧製品名：Deep Security as a Service） **Professionalプラン** ライセンス＋ FW、ウィルス対策、脆弱性対策、 ファイル／レジストリ監視、 セキュリティログ監視 **マネージドサービス** ２４時間３６５日運用保守	200,000円	40,000円
	AWS設計／構築・運用 **設計／構築** EC2×2 RDS×１ CloudFront等 **運用** ２４時間/365日 クラウドマネージド	500,000円	90,000円 ＋ AWS費用

その他

フォレッジング調査費用
※クレジットカード会社指定事業者

初期1,000,000円～

※参考価格

xtrans cs

事例②　～会員サイト～

モバイルアプリ、WEBサイトのコード診断おこなった
WEBサイトのAWS構成例

※株式会社ブロードバンドセキュリティ社　　スマホアプリ、AP、外部脆弱性診断

【AWSクラウドでの提供サービス】

お客様サイト

スマホアプリ

脆弱性診断

- スマホアプリ診断
- API診断
- WEB診断

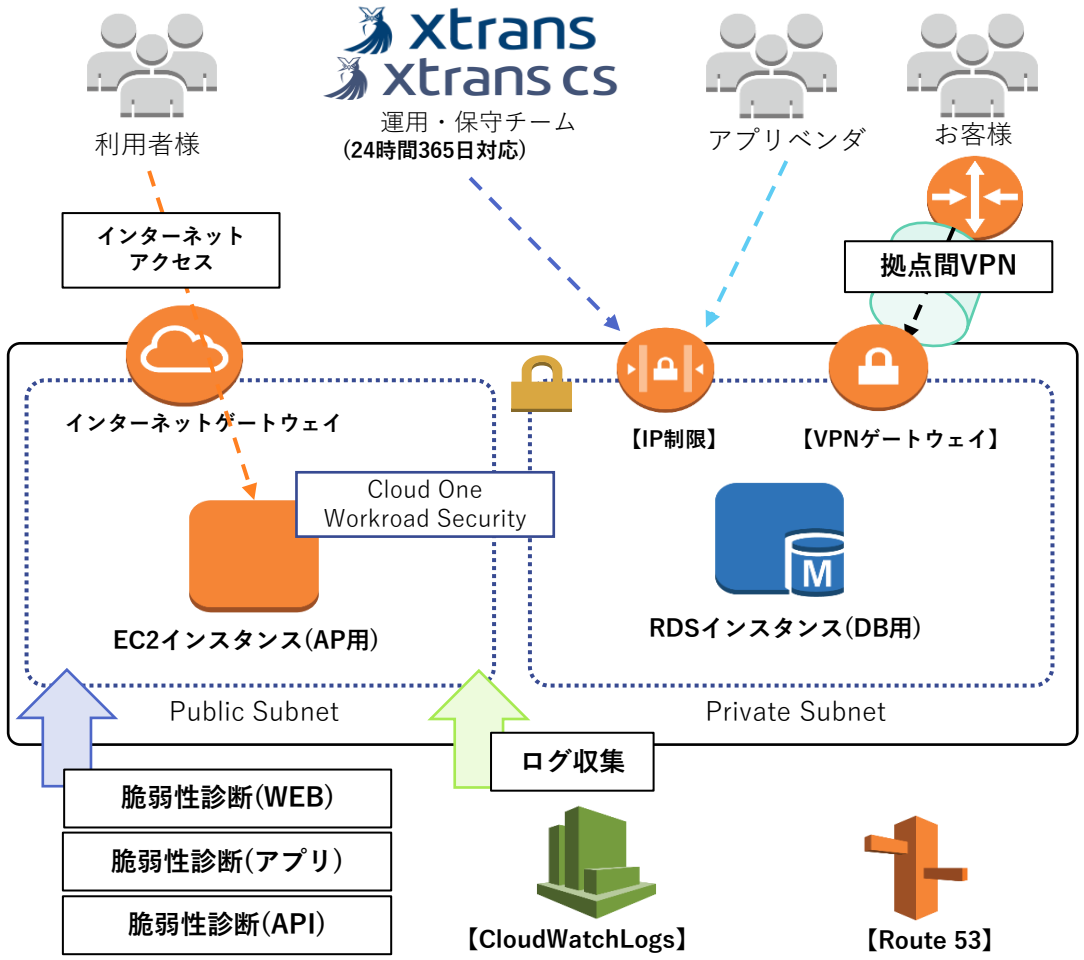
侵入防御

- C1WS(旧:DSaaS)マネージドサービス

Agentアップデート
チューニング
障害／レポート通知

接続制御 → クラウドマネージドサービス

24時間365日監視運用



【ホワイトハッカーの教え】

まずは診断

【株式会社ブロードバンドセキュリティ社　スマホアプリ診断】

スマホアプリ診断

アプリケーションそのものの診断

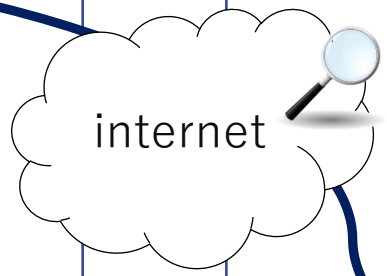
診断担当者

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

API診断

スマホアプリ ⇔ サーバ間の通信の診断

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

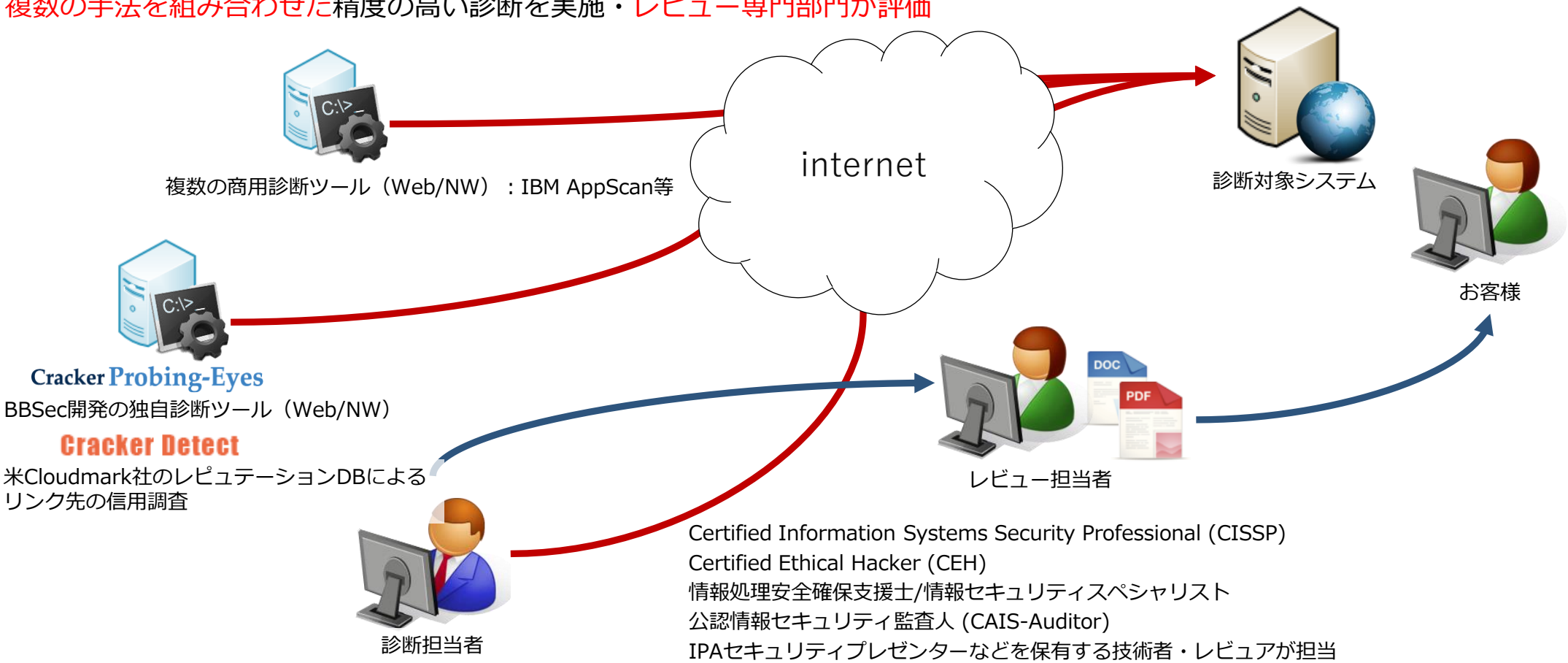
API通信

APIサーバ

【株式会社ブロードバンドセキュリティ社　外部脆弱性診断】

外部脆弱性診断　SQAT A＆P（Web＋NetWork）

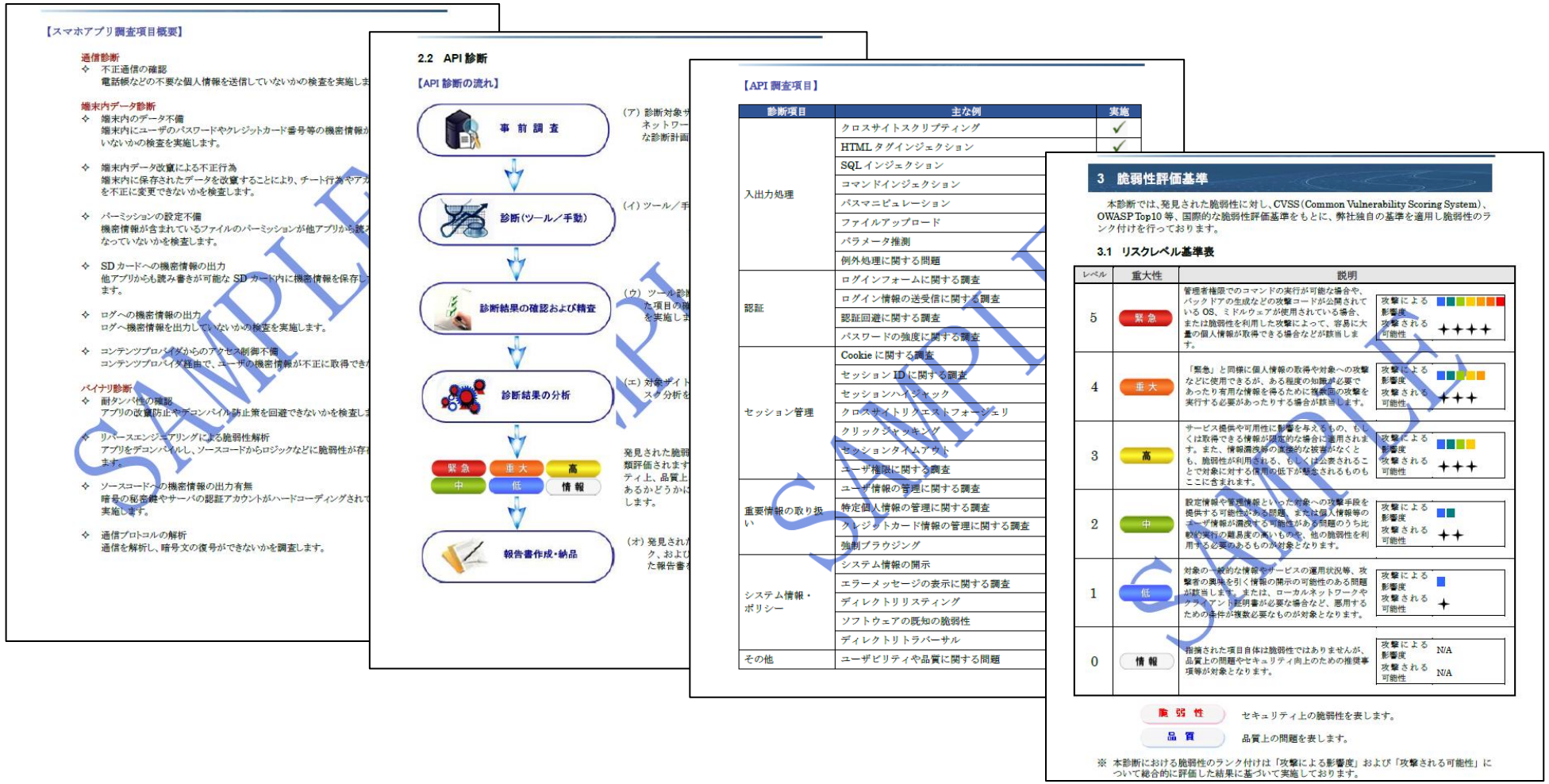
複数の手法を組み合わせた精度の高い診断を実施・レビュー専門部門が評価



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

【レビュー専門家と診断結果報告会】

検出された**脆弱性の概要・再現手法・リスク・対策方法**を詳細に報告



【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ま
- 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 → (ア) 診断対象サ ネットワー な診断計画

診断(ツール／手動) → (イ) ツール／手

診断結果の確認および精査 → (ウ) ツール診 た項目の を実施しま

診断結果の分析 → (エ) 対象サイト スク分析を

緊急 / 重大 / 高 / 中 / 低 / 情報

報告書作成・納品 → (オ) 発見され ク、およ た報告書

発見された脆弱 類評価されます ティ上、品質上 あるかどうかに します。

【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。	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。

【AWS公開サーバーにおけるセキュリティ費用】

		初期費用	月額費用
C1WS（旧：：Deep Security as a Service）			
Professionalプラン FW、ウィルス対策、脆弱性対策、ファイル／レジストリ監視、セキュリティログ監視	**マネージドサービス** ライセンス ＋ ２４時間３６５日運用保守	200,000円	40,000円
AWS設計／構築・運用			
設計／構築 EC2×1 RDS×１	**運用** ２４時間365日 クラウドマネージド	300,000円	60,000円 ＋ AWS費用

BBsec社　脆弱性診断
スマホアプリ脆弱性診断 初期500,000円～ （OS単位）
API診断 （１APIリクエスト）
外部脆弱性診断 別途要相談

xtrans cs

ご清聴いただき有難うございました。