Synqula | Save you from cyber attacks

サービス概要資料

株式会社シングラ
2023年3月

株式会社シングラ　Syngula Co., Ltd.

代表取締役

沼田　智博

所在地

本社：東京都品川区西品川1-1-1　住友不動産大崎ガーデンタワー9F TUNNEL TOKYO

海外現地法人：シンガポール / ベトナム

事業内容

デジタルマーケティング事業・セキュリティ事業・グローバルマーケティング事業

設立日

2013年8月29日(10期)

資本金

1,000万円

01 サイバーセキュリティの概要と現状

サイバーセキュリティの目的

サイバーセキュリティに関する取り組みの目的はリスク管理の高度化と企業ブランド/IRの向上（=企業価値の保全/向上）です。

企業が抱える主なリスク一覧

リスク項目	内容
カントリーリスク	政治経済、地政学関連のリスク：金融危機、為替変動、原材料や原油高の高騰、財政難、海外諸国の政治情勢など
自然災害リスク	地震、風水害、その他災害の発生、疫病蔓延等の発生など
財務リスク	資金流動性リスク：資金調達のコスト変動、資金ショートの発生 信用リスク：取引先の倒産、未回収債権の発生、 市場リスク：保有資産の価格変動、株価下落など
ガバナンスリスク	本社機能不全、子会社/海外拠点のガバナンス不足、買収後の事業統合不全など
法務・規制リスク	法改正や業界基準の変更、知的財産侵害、環境法規制、法令遵守違反、訴訟等による損失など
労務リスク	人材不足、人件費高騰、ハラスメント問題、過労問題、その他労使問題など
ブランドリスク	風評被害/不買運動の発生など
製品/サービスその他オペレーショナルリスク	社員の不正もしくは過失による損失、リコール、設備事故の発生、サプライチェーンの寸断など
情報リスク	サイバー攻撃、ウイルス感染、情報漏洩、システムダウン、情報逸失

企業のDXが加速したことにより、事業継続における**最大のリスク課題**の1つになりました。

サイバーセキュリティ対策の充実によるメリット

【守りの観点】

事業継続性をゴールとしたリスク管理の高度化（リスクの可視化、対応方針の策定等）

DXの加速に伴い、サイバーリスクが経営における重要なリスク課題となっています。その対策の第一歩として脆弱性診断/侵入テストによる**サイバーリスクの可視化/定量化**と対応策の策定が求められます。

【攻めの観点】

IR/企業ブランド/事業の信頼性向上

自社のサイバーリスクを明確に定義し、対策実施及びIR関係その他公的な資料で報告することで、**ステークホルダーの信頼性向上**、ひいては**IR改善**につなげることが可能となります。

脆弱性診断＋侵入テストを基軸とした当社のサイバーセキュリティサービスによって企業のデジタル課題を解決いたします。

セキュリティ10大脅威 2023

順位	組織	昨年順位
1位	**ランサムウェアによる被害**	1位 →
2位	**サプライチェーンの弱点を悪用した攻撃**	3位 ↑
3位	標的型攻撃による機密情報の窃取	2位 ↓
4位	**内部不正による情報漏えい**	5位 ↑
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位 ↓
6位	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**	7位 ↑
7位	ビジネスメール詐欺による金銭被害	8位 ↑
8位	脆弱性対策情報の公開に伴う悪用増加	6位 ↓
9位	不注意による情報漏えい等の被害	10位 ↑
10位	犯罪のビジネス化（アンダーグラウンドサービス）	**NEW**

引用：IPA「情報セキュリティ10大脅威2023」

昨年までの傾向同様、組織においては
外部脅威がより多く上位を占める結果となりました。
特に注視すべき傾向は以下です。

①ランサムウェアによる被害が3年連続1位

②新たな手口の報告：暗号化のみならず窃取した情報を公開すると脅す「二重脅迫」、DDoS攻撃を仕掛ける、被害者の顧客や利害関係者へ連絡するとさらに脅す「四重脅迫」

ランサムウェアの感染経路は多岐にわたるため、
ウイルス/不正アクセス/脆弱性対策と多層の対策が必要となっています。

相次ぐ不正アクセス・セキュリティー事故

規模・業界に関わらず、情報を持つすべての企業・団体がサイバー攻撃の対象となっています

「クレカ情報が漏えい」とする詐欺に注意　メタップス不正アクセス問題に便乗

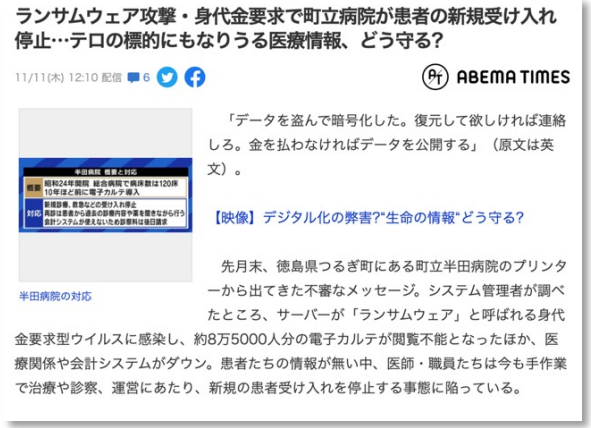
2022年03月03日 16時45分 公開　[ITmedia]

印刷　226　Share　B!　3　3

メタップスペイメントへの不正アクセスによりクレジットカード情報が流出した問題に便乗し、カード情報を盗もうとする詐欺メールやSMSが出回っているとして、ローソン銀行は3月2日、注意喚起した。

■ フィッシングメール例
「お客さまのクレジットカード情報が漏えいしている可能性がございます。カード情報（クレジットカード番号、有効期限、暗証番号、セキュリティコード、ID・パスワード等）をご入力いただきご確認ください！」
「あなたのカードが不正に使用されています。至急カードを停止しますので、カード情報（クレジットカード番号）、有効期限、暗証番号、セキュリティコード、ID・パスワード等）を教えてください！」

■ 一般社団法人日本クレジット協会「フィッシング詐欺に遭わないための注意事項」



ランサムウェア攻撃・身代金要求で町立病院が患者の新規受け入れ停止…テロの標的にもなりうる医療情報、どう守る?

11/11(木) 12:10 配信　6　ABEMA TIMES

半田病院の対応

「データを盗んで暗号化した。復元して欲しければ連絡しろ。金を払わなければデータを公開する」（原文は英文）。

【映像】デジタル化の弊害?"生命の情報"どう守る?

先月末、徳島県つるぎ町にある町立半田病院のプリンターから出てきた不審なメッセージ。システム管理者が調べたところ、サーバーが「ランサムウェア」と呼ばれる身代金要求型ウイルスに感染し、約8万5000人分の電子カルテが閲覧不能となったほか、医療関係や会計システムがダウン。患者たちの情報が無い中、医師・職員たちは今も手作業で治療や診察、運営にあたり、新規の患者受け入れを停止する事態に陥っている。

取引先にサイバー攻撃でトヨタ国内全工場停止"ランサムウェア"とは？解説

3/1(火) 23:30 配信　17　テレ朝news

All Nippon NewsNetwork(ANN)

トヨタ自動車は1日、車の内装や外装の部品を製造する取引先企業がサイバー攻撃を受けたため、国内にある全ての工場を停止しました。攻撃されたのは『小島プレス工業』。サイバー攻撃は、身代金要求型の"ランサムウェア攻撃"とみられます。
されたことで、被害が発覚した。

▲不正アクセス・個人情報流出　**▲システムダウン・事業困難**　**▲情報窃取・事業の一時停止**

弊社では毎月最新の事故事例や脆弱性に関する情報をアップデートしています。
詳しくはこちらからお問い合わせください。

サイバークライシスによる企業の損失

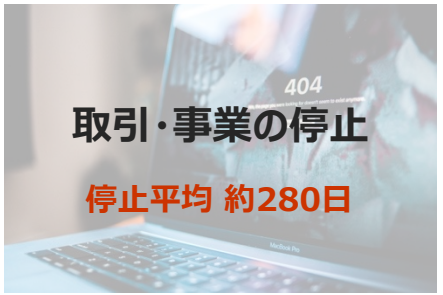
サイバー攻撃は、もはやどんな企業も避けることは困難と言われ、

インシデントが発生した際の対応・未然の取り組みによって被害を最小限に抑えることができるかが

企業としての信用やイメージに関わる重要なポイントです。

カプコンにおける事例では顧客情報約35万件の流出の可能性が公表され、株価16%の下落を招いた。

コインチェックにおいて顧客資産が外部に送金される被害が発生し、顧客への損害賠償は580億円に上った。



インシデントの調査や復旧のため、日本企業のサービス・事業の停止は平均8ヶ月に及ぶとされている。

このほか**業務負荷の増加**、**風評被害**、**自社を踏み台とした他社への被害拡大**など一度のインシデントで被る損失は甚大です。

(出典) JNSA インシデント損害額調査レポート 2021年版

02 CYBER RESCUE 概要

CYBER RESCUE立ち上げの背景

創業以来の事業

デジタルマーケティング領域における
顧客ビジネスの成長をサポート

【 DX・広告・ECコンサルティング 】

×

近年のニーズ顕在化

事業継続性や企業IRの向上を
セキュリティ領域からサポート

【 診断・研修・セキュリティコンサルティング 】

「 企業の『攻め』と『守り』を双方向から強力に支援したい 」

CYBEIRESCUE は生まれました

CYBER RESCUEのビジョン

高い技術力とグローバルの目線で
社会価値を創造する
“Total Cyber Security Service”

ネットワーク力を活かし、国内外で強固なチーム・パートナーシップを構築

▽スペシャリストによる監修

最高技術顧問 ”Code name 大佐”

元海外特殊部隊。
国防のセキュリティに携わるなど豊富な実績を保有。
国際的に活躍するホワイトハッカー。

▽グローバルパートナー

WHITE - HAT LTD

イスラエル政府公式サービスプロバイダーであり、銀行・保険・航空宇宙・エネルギー業界のサイバーセキュリティ企業最大手。アメリカ国防の総務庁ペンタゴンのサイバーセキュリティコンサルティングを担当。

▽グローバルパートナー

viettel security

国防省傘下ベトナム軍隊工業通信グループ(ベトテル＝Viettel) のセキュリティ・カンパニー。

CISSP、Comp TIA Security+、CCIE、CEH、など国際的なセキュリティプロフェッショナル資格を持つエンジニアが揃い、世界一のホワイトハッカーも所属。

ベトナム最大手であるこのVCSの日本国内でのサービス取扱いは日本法人で初。

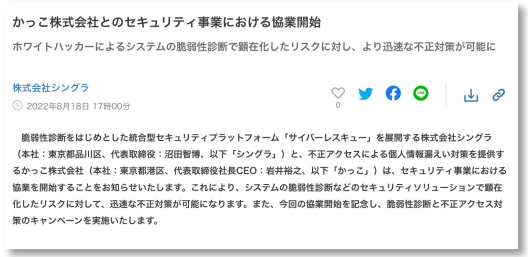
【日本初】シングラ、アジアのTOPセキュリティベンダーViettel Cyber Security社のサービス提供を開始

日本国内全体のサイバーセキュリティレベル底上げの実現を目指す

株式会社シングラ
2023年6月1日 11時00分

株式会社シングラ（本社：東京都品川区、代表取締役：沼田智博、以下シングラ）はベトナム最大手のサイバーセキュリティ企業Viettel Cyber Security社（所在地：ベトナム ハノイ、以下VCS）のセキュリティソリューション提供を開始したことをお知らせいたします。VCSの日本国内でのサービス取扱いは日本法人で初となります。

▽協業リリース（一部）

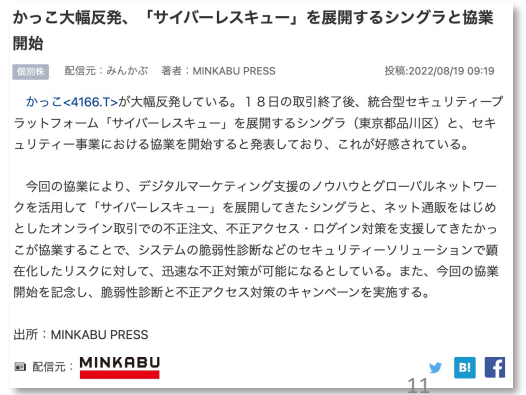


かっこ株式会社とのセキュリティ事業における協業開始

ホワイトハッカーによるシステムの脆弱性診断で顕在化したリスクに対し、より迅速な不正対策が可能に

株式会社シングラ
2022年8月18日 17時00分

脆弱性診断をはじめとした統合型セキュリティプラットフォーム「サイバーレスキュー」を展開する株式会社シングラ（本社：東京都品川区、代表取締役：沼田智博、以下「シングラ」）と、不正アクセスによる個人情報漏えい対策を提供するかっこ株式会社（本社：東京都港区、代表取締役社長CEO：岩井裕之、以下「かっこ」）は、セキュリティ事業における協業を開始することをお知らせいたします。これにより、システムの脆弱性診断などのセキュリティソリューションで顕在化したリスクに対して、迅速な不正対策が可能になります。また、今回の協業開始を記念し、脆弱性診断と不正アクセス対策のキャンペーンを実施いたします。



かっこ大幅反発、「サイバーレスキュー」を展開するシングラと協業開始

個別株　配信元：みんかぶ　著者：MINKABU PRESS　投稿:2022/08/19 09:19

かっこ<4166.T>が大幅反発している。１８日の取引終了後、統合型セキュリティープラットフォーム「サイバーレスキュー」を展開するシングラ（東京都品川区）と、セキュリティー事業における協業を開始すると発表しており、これが好感されている。

今回の協業により、デジタルマーケティング支援のノウハウとグローバルネットワークを活用して「サイバーレスキュー」を展開してきたシングラと、ネット通販をはじめとしたオンライン取引での不正注文、不正アクセス・ログイン対策を支援してきたかっこが協業することで、システムの脆弱性診断などのセキュリティーソリューションで顕在化したリスクに対して、迅速な不正対策が可能になるとしている。また、今回の協業開始を記念し、脆弱性診断と不正アクセス対策のキャンペーンを実施する。

出所：MINKABU PRESS

配信元：MINKABU

ネットワーク力を活かし、国内外で強固なチーム・パートナーシップを構築

CIO 足立 照嘉 （TERUYOSHI ADACHI）

英国のサイバーセキュリティ・サイエンティスト、テック起業家、ベストセラー作家。

サイバーセキュリティ企業の経営者として20年以上の経験を持ち、ロンドン・ニューヨーク・東京での起業・買収・売却を経験。日本を代表する企業経営層からの信頼も厚い。また、英国政府によるサイバーセキュリティ戦略立案へのアドバイザリなども提供。

研究者としては、サイバーリスク管理と意思決定に関する論文の執筆や、京都大学、大阪大学などでの研究プロジェクト参画、また、世界ランキング8位（2023年度 QS世界大学ランキング）のUCL（ユニバーシティ・カレッジ・ロンドン）に研究員として就任予定。
サイバーセキュリティ関連技術への投資や経営参画なども行なっており、投資先の米国サイバーセキュリティ企業はユニコーン企業へと成長。また、英国大手金融機関やAIスタートアップの顧問のほか、EV（電気自動車）メーカーのCTOも兼任している。
英国政府主催イベントでの基調講演やジェトロ主催による欧州各都市や全米主要都市での講演、J-WAVEラジオやTBSラジオなどへの出演やNHKでのテレビ番組監修のほか、雑誌・ウェブへの寄稿により啓発を行なっている。
『サイバー犯罪入門』『3分ハッキング』『GDPRガイドブック』、これまでの著書全てがAmazonランキングで1位を獲得しているベストセラー作家でもある。

令和元年度サイバーセキュリティに関する総務大臣奨励賞に、
トヨタ自動車、東京海上、NTT、NHKなど日本を代表する企業各社様からの推薦でノミネート
マサチューセッツ工科大学スローン経営大学院 Executive certificate in Cyber Security
大阪大学大学院工学研究科元共同研究員

ソリューションマップ

CYBERESCUE

	攻撃からの防御	早期検知・被害軽減	インシデント対応
ネットワーク	**プラットフォーム診断・ペネトレ** ネットワーク環境のセキュリティを把握	**SOC ・ IPS/IDS** 攻撃・不正侵入を検知	**デジタルフォレンジック** 攻撃された際の 法的根拠となる証拠保全や 被害の特定
Web アプリケーション ・ スマホアプリ	**脆弱性診断** Webサイト・サービスの セキュリティレベルを把握	**WAF ・ DDos攻撃対策** Webサイト・サービスへの攻撃防御	**サイバー保険** インシデント発生時の保険による補償
エンドポイント	**IoT診断** ネットワーク機器のセキュリティを把握	**EDR ・ 簡易EDR** 端末内の脅威検知・隔離	**個人情報保護** 端末内の個人情報検出・管理
その他	**サイバーセキュリティコンサルティング・アドバイザリー** リスクアセスメント・教育研修・ワークショップ・法令対応・CSIRT構築/運用支援 など継続的な支援		

完全成果型脆弱性診断

成果単価	システム脆弱性*の指摘1点につき、50万円（税抜） 特に重要な脆弱性の指摘1点につき、60万円（税抜） ※予算の上限設定可能
着手金	なし
診断対象	Webアプリケーション

*5段階のリスクレベル
緊急/高/中/低/情報で
優先度の高いものからご報告します。

セカンドオピニオンとしてのご利用や
定期運用の場合、コストを抑えることが
可能です。

プロジェクト型脆弱性診断

診断対象や納期、ご予算感に合わせてお見積もり・ご提案いたします。

- Webアプリケーション診断
- スマホアプリケーション診断
- ソースコード診断
- ネットワーク診断
- IoT診断

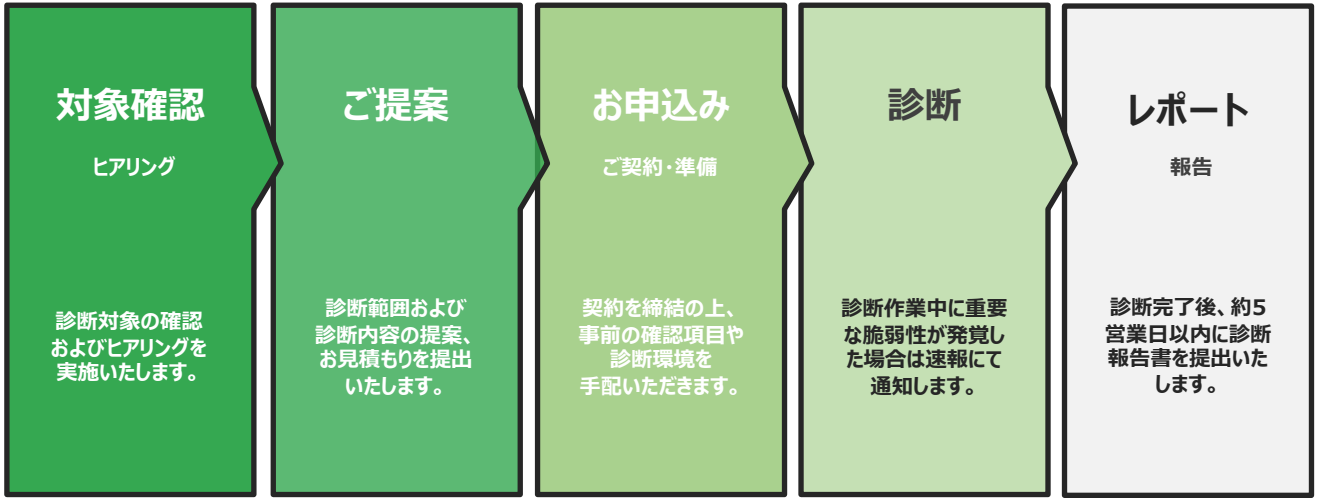
サービスの大規模改修やローンチ時など
網羅的な診断をご希望の場合、
プロジェクト型を推奨しております。

他社サービスとの比較

	CYBERESCUE	A社	B社	C社
診断手法	◎ ツール診断＋ ホワイトハッカー による手動診断	○ セキュリティエンジニアに よる手動診断	○ セキュリティエンジニアに よる手動診断	△ ツール診断
料金体系	完全成果型 50万円～/件	300万円～/回	-	100万円
アウトプット	具体的な対策・想定 リスクを記載した調査 報告書	具体的な対策・想定 リスクを記載した調査 報告書	診断結果報告書	ツール診断結果のみ
保守運用	対応可能	対応可能	要相談	不可
ペネトレーションテスト	脆弱性診断と 並行して実施可能	別途プラン	対応なし	対応なし
診断以外のサービス	CSIRT構築 研修サービスなど 内部セキュリティ支援	-	CSIRT構築 研修サービスなど 内部セキュリティ支援	-

脆弱性診断 - 導入フロー

脆弱性診断/成果報酬型脆弱性診断



※アプリケーションの規模やネットワーク環境によって前後する可能性がございます。

ペネトレーションテスト

対象のシステムに対して、攻撃者が情報搾取や改ざん、妨害などの攻撃が達成できるか検証する事を目的としています。
目的達成のため脆弱性の検査や実行可能な攻撃コードの検証を実施します。

ペネトレーションテストと脆弱性診断の比較

	ペネトレーションテスト	脆弱性診断
目的	■攻撃者の目的(情報搾取や改ざん、妨害など)が達成できるか検証 ■目的達成のための脆弱性の検査や実行可能な攻撃コードの検証	■脆弱性を網羅的に洗い出し検査
評価	■実際のサイバー攻撃同様に、攻撃目的が達成可能か検証	■IPAなどのセキュリティ規格を基準に検査・分析・評価
報告	■シナリオと攻撃検証結果・システムリスク評価	■個々の脆弱性に対する危険度評価とリスト化
網羅性	■なし	■あり
スキル	■脆弱性の活用	■脆弱性の指摘

ペネトレーションテスト概要（1/2）

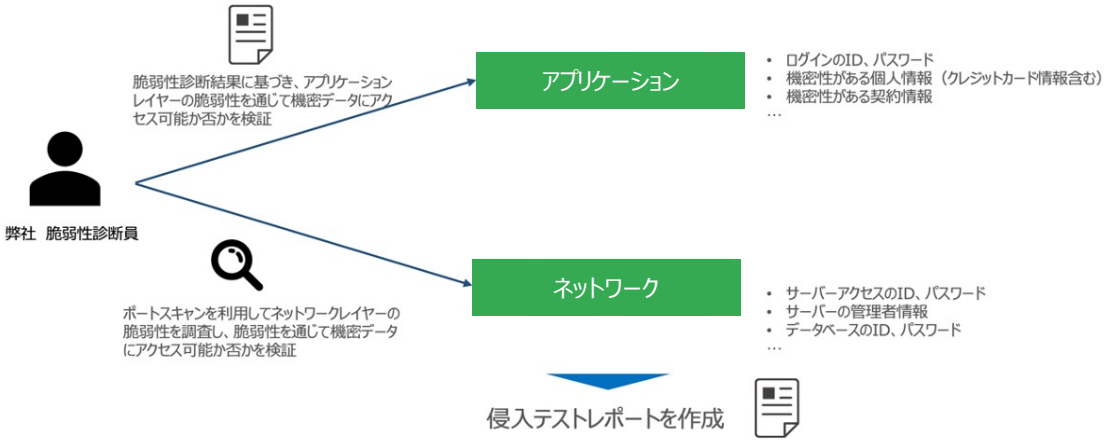
侵入テスト:外部からシステムに侵入し、コンピュータやネットワークの脆弱性を通じて、機密性があるデータ（個人情報、サーバ情報等）にアクセスが可能か検証するテストです。

侵入テストの種類：当社ではブラックボックステスト＋外部侵入テストとして実施することを推奨いたします。

①	ホワイトボックステスト	テスト対象のシステムの内部の構造を把握した上で、企業様に合わせた内容で行うテスト ※企業様から、予め各種情報を頂戴し、それに応じて対応させていただきます
②	ブラックボックステスト	テスト対象のシステムの内部構造は考慮せずに、外部から把握できる機能を検証するテスト ※企業様から、事前に情報を受領せず、対応させていただくテストとなります
③	外部侵入テスト	攻撃者がシステムの外部（第三者）から攻撃してくることを想定したテスト
④	内部侵入テスト	システムの内部にすでに攻撃者が侵入しているまたは社員が侵入することを想定したテスト

対象サイトのアプリケーション及びネットワークのレイヤーの脆弱性を通じて、機密性があるデータ（個人情報、サーバ情報等）にアクセスが可能か、検証させていただくことを想定しております。
なお、検証は下記の原則に沿って実施いたします。

- サーバーの停止や遅延を発生させないようにすること
- データの更新・削除を実施しないこと
- 基本的に機密性があるデータを当社内のPCに保存せず、一時保存しても診断が完了した時点に素早く削除すること



ペネトレーションテスト概要（2/2）

侵入テストのシナリオ事例紹介

#	実施レイヤー	侵入の前提条件	事例概要
1	アプリケーション	Webアプリケーションのログインフォームに SQLインジェクションの脆弱性がある ※各サイトの脆弱性診断によって上記を検証	下記のSQL文字列を入力して送信し、不正にログインが可能かを確認します。 1' or '1' = '1 不正ログインが成功した場合、ログイン後のページに入り、個人情報ページ、契約ページ等機密情報が入っているページを閲覧できるかを確認します。
2		Webアプリケーションの入力フォームにコマンドインジェクションの脆弱性がある ※各サイトの脆弱性診断によって上記を検証	下記のコマンドを入力して送信し、実行可能かを確認します。 cat /etc/passwd sleep 10 コマンドが実行できた場合、サーバー側のOSアカウントのパスワード情報を取得します。
3		WebアプリケーションがPHPで実装されており、入力フォームにコードインジェクションの脆弱性がある場合 ※各サイトの脆弱性診断によって上記を検証	下記のコードを入力して送信し、実行可能かを確認します。 phpinfo() system('id') コマンドが実行できた場合、 • phpinfo()では、サイトのPHPの構成情報（バージョン情報、どういったライブラリが有効になっているか等）を取得しています。 PHPのバージョン脆弱性を調査した上で、侵入シナリオを作成します。 • system('id') では、PHPのsystem関数を用いてPHPの実行ユーザ（OS上のアカウント）の情報を取得しています。
4	ネットワーク	sshポート(22)が開放している場合 ※ポートスキャンによって上記を検証	パスワード攻撃（ブルートフォースアタック）を実施して不正にログインできないか確認します。 不正ログインが成功した場合、サーバーに関連するアカウントやファイル情報を閲覧できるかを確認します。
5		MySQLポート(3306)が開放している場合 ※ポートスキャンによって上記を検証	パスワード攻撃（ブルートフォースアタック）を実施して不正にログインできないか確認します。 不正ログインが成功した場合、データベースのテーブル情報を閲覧できるかを確認します。
6		Apacheポート(443,80)が開放している場合 ※ポートスキャンによって上記を検証	Apacheの脆弱性の一種 Remote code execution （RCE)の脆弱性を確認します。 Remote code execution の脆弱性がある場合、Reverse Shellの実行が可能かを確認します。 実行可能な場合、Reverse Shellによってサーバーシェルを奪取し、サーバーに関連するアカウントやファイル情報を閲覧できるかを確認します。

■コンサルティング契約 - ご支援例

【中～大規模プロジェクト】

①リスクアセスメント支援
事業にクリティカルなリスクの洗い出しやその実現性の確認など、
ISMS内でも重要なリスクアセスメントを支援。

②セキュリティリスク分析
ISMSでは把握できない細かいリスクについて分析。
運用フロー等を直接ヒアリングし、内在的なリスク洗い出しを支援。

③セキュリティ規程類見直し
セキュリティに関わる規程などに不足点や見直し支援。
例：クラウド利用ルール、リモートワークルール、など

④CSIRT構築支援
セキュリティインシデントが発生した時の対応フロー明確化、
構築後の運用支援。

【小規模プロジェクト】
・セキュリティ訓練（サイバーセキュリティ演習、標的型攻撃メール訓練、インシデントハンドリングフローチェック
・管理者/従業員向け情報セキュリティ研修

■アドバイザリー契約

貴社既存プロジェクトに対するサポートとして、お打ち合わせや他チャットツールによる弊社知見の共有や質疑応答、方針アドバイスなどの支援。
セキュリティエンジニアやセキュリティマネジメント担当者などの知見をもとに疑問点や懸念点の解消をお手伝いいたします。

コンサルティングサービス（解決策の策定例）

リスク事項と解決策			解決策における優先順位/ステップ		
カテゴリ	解決策	想定効果	第一ステップ	第二ステップ	第三ステップ以降
本業/サプライチェーン（子会社/投資先企業）に対するサイバー攻撃	ホワイトハッカーによる脆弱性診断と保守開発	高		●	
	サイバーセキュリティツールの導入	中			●
	セキュリティ規定、ガイドライン作成	高	●		
	CSIRTの構築	高		●	
内部によるプロフェッショナル情報/取引先企業の不正利用	不正監視ツールの導入	高			●
	社内研修の強化	中			●
	社内ルールの徹底,ファイル加工など	低			◌
プロフェッショナルによるオペレーショナルリスク	社内研修の強化	中			●
			貴社のサイバーセキュリティ/デジタルリスクマネジメントを包括的に調査、理解しつつ、成果物をご提供するフェーズ。	規定類やガイドラインを整備した上で技術面の調査と予防/即時対応の体制構築を行うフェーズ。	ツール導入や社内教育などを通じて、デジタルリスク管理体制を仕上げるフェーズ。

コンサルティング実績

実績1

規模：～100名
内容：社内文書の整備・作成

開業時セキュリティマネジメントに関する文書やフロー整備を支援
各文書修正案を作成、リスクアセスメントのフローを中心に見直し セキュリティ対策の過不足を俯瞰して助言・支援

管轄省庁への質疑応答時セキュリティ専門の知見で支援
管轄省庁主導のセキュリティ演習参加時、インシデント発生時の対応フロー整備を支援、対応フローの見直しを支援

実績2

規模：~500名
内容：ISMS取得コンサルティング CSIRT構築支援

インシデントの定義、エスカレーションフローの確立、ISMS委員（CSIRT体制メンバー）への教育、専門的な知見が必要な場合の緊急連絡先（弊社）の設置

その後のPDCAとして、実際に起きたインシデントの際の報告から是正処置までの一連の流れをレビューし改善点等を指摘

貴社のニーズに合わせて小規模～中規模プロジェクト単位でのご支援が可能です。

アドバイザリープラン例

初期のアドバイザリーにて課題の洗い出し、情報資産の把握などを行い、
貴社へ適したソリューションをご提案させていただきます。（アドバイザリー契約は3ヶ月～のご提供となります）

項目	プランA	プランB	プランC
定例会議	月4時間 ※1	月2時間 ※1	なし
チャット対応	月5トピック	月5トピック	月5トピック
料金	月額50万円(税別)	月額30万円(税別)	月額20万円(税別)
対応範囲	・セキュリティ全般に関するご相談 プロダクトのセキュリティ対策、リスクアセスメント試算、セキュリティ規定　など		
支援対象外	文書作成、法令に関する助言 ※1※2		

※1 1回あたりの時間、頻度に関しては調整可能
※2 文書レビューは対応範囲内となりますが、頻度により別途お見積りとなる場合もございます

スタートアップ向けセキュリティアドバイザリー

専任の担当がいない　監査法人や営業先から診断実施を求められている　何から始めればいいかわからない

投資ラウンドにおいてセキュリティに課題感をお持ちのスタートアップ企業様向けに

業界20年以上の専門家ら監修で【個社ごとのテーラーメイド】のアドバイザリープランをご提案します

	セキュリティアドバイザリー(スタートアッププログラム)
提供メニュー	①セキュリティ全般に関するQAチャット対応 ②Webアプリケーションの定期簡易診断 ③月1回の定例 ④セキュリティ事例・脆弱性情報の定期アップデート　など
料金	月額20万円(税別)～
備考	・ご契約期間：３か月～ ・メニュー組合せとご予算によってお見積りいたします

▼簡易診断サンプル

簡易診断結果報告書

診断実施日	
対象サービス/サイト	
URL	
総合評価一覧	A・・・診断対象範囲内に脆弱性が発見されていない状態。 B・・・リスクレベル低の脆弱性が存在します。対応の要否をご確認ください。 C・・・リスクレベル中の脆弱性が存在します。対応実施を推奨します。 D・・・リスクレベル高の脆弱性が存在します。個人情報の漏洩や、改ざんなど具体的な恐れがある状態です。 E・・・リスクレベル緊急の脆弱性が存在します。速やかな対処を強く推奨します。
総合評価	D

NO.	リスクレベル	指摘事項
1	D	クリックジャッキング攻撃から防御するためのX-Frame-Optionsヘッダーが設定されていません。 他のドメインのサイトからの読み込みを制限したい場合は、この設定を行ってください。
2	D	htaccessファイルを使用して、Apache Web サーバー ソフトウェアの構成を変更し、Apache Web サーバー ソフトウェアが提供する追加の機能を有効または無効にすることができます。.htaccessファイルがアクセス可能ではない状態になっていることを確認してください。
3	C	次のディレクティブは、ワイルドカードソースを許可、広く定義されています。script-src、style-src、img-src、connects-src、frame-src、font-src、media-src、object-src、manifest-src、worker-src、prefetch-src、form-action、Webサーバー、アプリケーションサーバー、ロードバランサーなどの、CSPヘッダー設定が適切にされていることを確認してください。
4	B	タイムスタンプがWEBまたはアプリケーションサーバーによって露見しています。
5	B	cache-controlヘッダーが正しく設定されていないか欠落しているため、ブラウザーとプロキシがコンテンツをキャッシュできます。

※簡易診断となっておりますので、本診断との結果は異なる可能性がございます。
※あくまでも診断実施日の状態を示したものであり、将来的な安全性を保証するものではございません。
※診断結果に基づく設定変更アドバイス、手動診断については、脆弱性診断（本診断）の対象となります。

アドバイザリー実績

実績1

規模：～20名
事業概要：流通動産産取引プラットフォーム

課題：事業拡大とともに今後の上場を視野に入れる中、セキュリティ対策に取り組むためのリソース不足

プラン：セキュリティアドバイザリー
（スタートアッププログラム）

提供内容
・セキュリティ事例・脆弱性情報の
定期アップデート（月次）
・月に一度簡易診断 および 定例報告
・チャットQ&A対応

実績２

規模：～90名
事業概要：多言語化サービス提供

課題：セキュリティ担当者の業務負荷によって自社のセキュリティ課題が不明瞭

プラン：セキュリティアドバイザリー

提供内容
・セキュリティ事例・脆弱性情報の
定期アップデート（月次）
・チャットQ&A対応

実績3

規模：～150名
事業概要：IT系人材サービス

懸念点：脆弱性診断は過去実施済み。保有しているサービスが多く予算の兼ね合いもあるため、簡易診断の定期プランにニーズあり

プラン名：簡易診断サブスクリプション

提供内容
・セキュリティ事例・脆弱性情報の
定期アップデート（月次）
・簡易診断
（回数無制限、5営業日以内に結果報告）
・チャットQ&A対応

主要取引先

全日本空輸グループ各社
日本放送協会（NHK）
花王株式会社
株式会社セブン銀行
株式会社長谷工コーポレーション
富士急行株式会社
湘南美容クリニックグループ
株式会社ポニーキャニオン
ビックローブ株式会社
NTTデータ先端技術株式会社
株式会社オプト

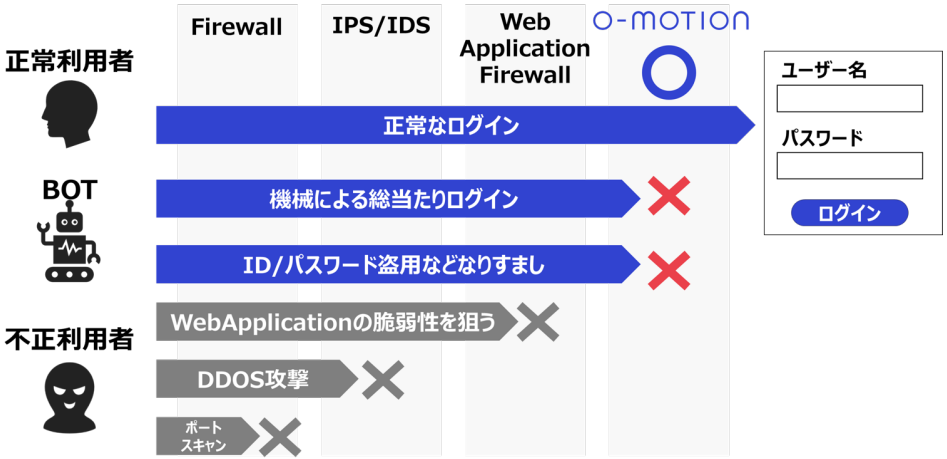
きらぼしテック株式会社
株式会社はてな
株式会社セプテーニ
GMOクラウド株式会社
株式会社船井総合研究所
ネットイヤーグループ株式会社
金融機関
官公庁
地方自治体
大学・教育機関
Etc.

Appendix

提携サービス：不正アクセス検知サービス「O-MOTION」

不正アクセス検知サービス O-MOTION

- WEBサイトにアクセスしたユーザーの操作情報、デバイス情報等をリアルタイムに分析
- 他人のなりすましを識別し、不正アクセスから生じる不正行為を防止



■特徴

- ◆ 証券会社・銀行が採用
- ◆ 脆弱性がなくても発生するBot・なりすましアクセスを検知
- ◆ 端末特定技術で特許取得

■防止できる被害

- 個人情報漏洩
- 不正送金
- ポイントの不正取得/交換

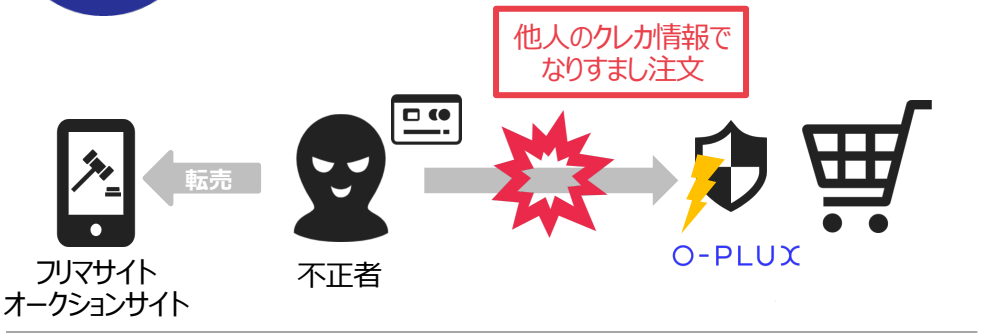
▶ 左記被害による ブランドイメージ棄損

期間限定導入キャンペーン実施中：トライアル無料/初期費用無料/月額費用2ヵ月無料
※先着5社限定

提携サービス：不正注文検知サービス「O-PLUX」

不正注文検知サービス O-PLUX

ECにおける代金未払い等の不正注文を独自の審査モデルでリアルタイムに検知するSaaS型サービス



■特徴

- 4年連続不正注文検知サービス導入実績No.1
- 20,000サイト以上の不正注文情報を共有
- ECカートと連携多数
- CSVによる連携システム改修をせずに導入も可能
- 月額3万円から利用可能（トライアルプランもあり）

■防止できる被害

チャージバック	初回限定商品の不正取得
後払い未払い	悪質な転売
ポイントの不正取得	代引き受取拒否

お問い合わせ

株式会社シングラ
サイバーレスキュー 営業担当

TEL　　：03-6420-0517
e-mail：security_cr@syngula.co.jp
Web　：https://www.syngula.co.jp/

Syngula

〒141-0033 東京都品川区西品川1丁目1－1
住友不動産大崎ガーデンタワー9階 TUNNEL TOKYO