Syngula | Save you from cyber attacks

Cyber Rescue 概要資料

株式会社Syngula
2021年8月

企業情報

株式会社シングラ　Syngula Co., Ltd.

代表取締役
沼田　智博

所在地
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

事業内容
デジタルマーケティング事業　グローバルマーケティング事業

設立日
2013年8月29日(8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とは

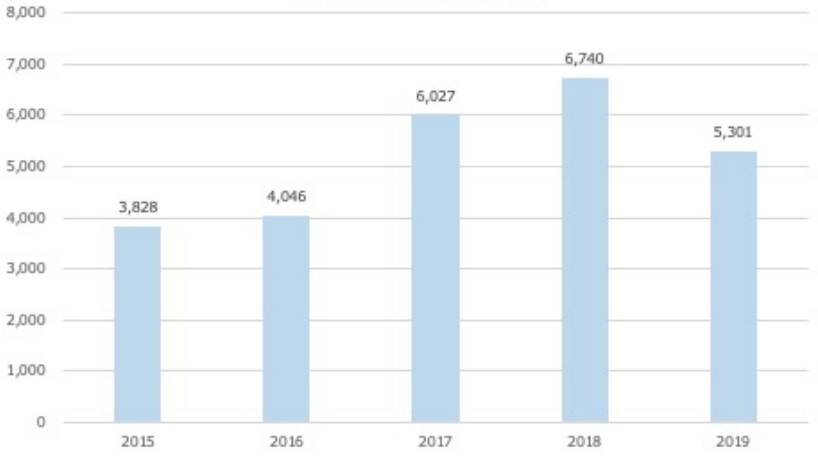
サイバーセキュリティとは

近年、企業や官公庁、研究機関等の組織を標的としたサイバー攻撃は増加し続けており、2020年3月の警視庁調査では、2019年の標的型メールは5301件にのぼります。

標的型攻撃の中でも特にAPT（高度で持続的な脅威）攻撃は、標的とする組織に合わせてカスタマイズしたマルウェアを用いたり、ゼロデイ脆弱性を悪用したりするため、既存のセキュリティ対策では完全に防御することが難しくなってきています。

加えて、最近では標的とする組織を直接狙わず、その取引先や関連会社、工場などを踏み台にして攻撃する「サプライチェーン攻撃」も増えており、大手・中堅企業のみならず、中小企業においても適切な備えが不可欠となっています。

標的型メール攻撃件数の推移



警視庁調査データを参考に弊社作成

サイバー犯罪の拡大と防御策の需要

サイバー犯罪はデジタル社会の成長と共に年々増加しており、また多様化/深刻化しています。

警視庁調査データを参考に弊社作成

Synqula

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。

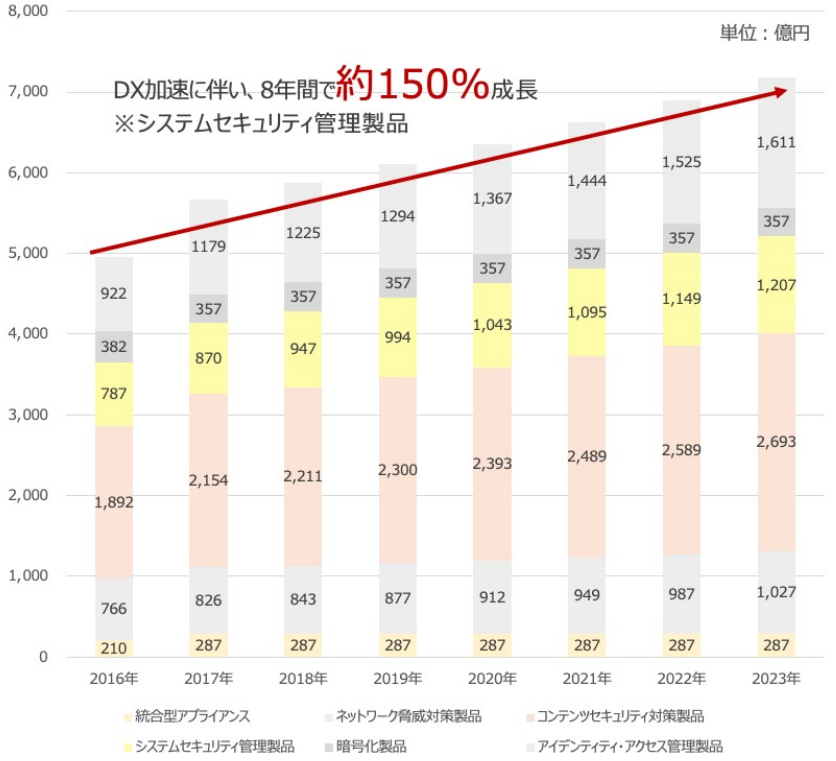
脆弱性診断＋侵入テストを基軸とした当社のサイバーセキュリティサービスによって企業のデジタル課題を解決いたします。

Syngula

サイバーセキュリティの市場性（ニーズ推移）

サイバーセキュリティ市場規模推移

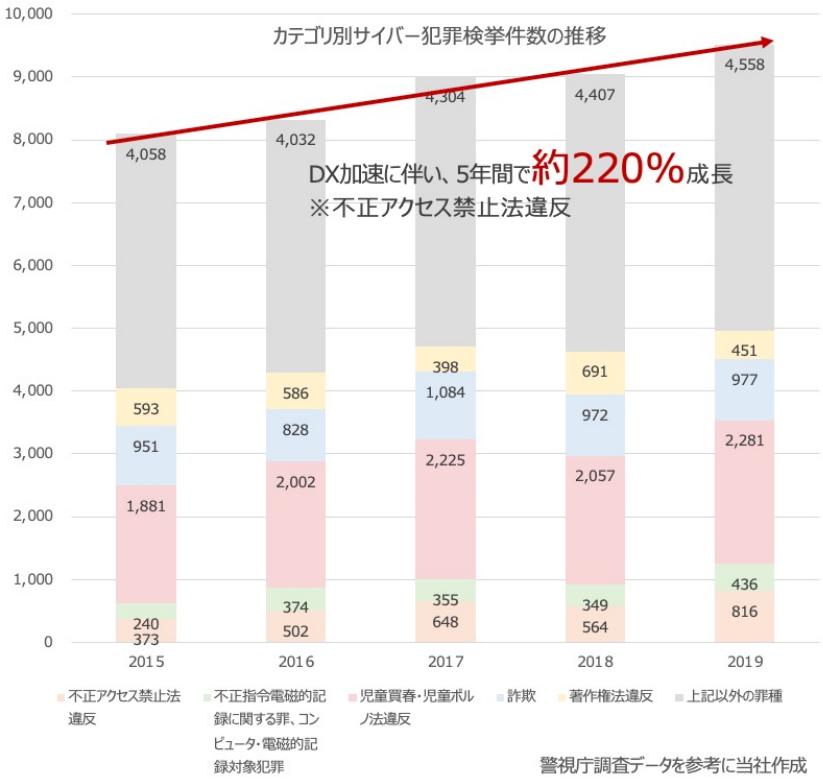
深刻化するサイバー攻撃を背景に、市場に求められる需要は拡大を続けています。



日本ネットワークセキュリティ協会「サイバーセキュリティ市場」を参考に当社作成

サイバー犯罪の被害状況推移

サイバー犯罪はデジタル社会の成長と共に年々増加しており、また多様化/深刻化しています。



警視庁調査データを参考に当社作成

Synqula

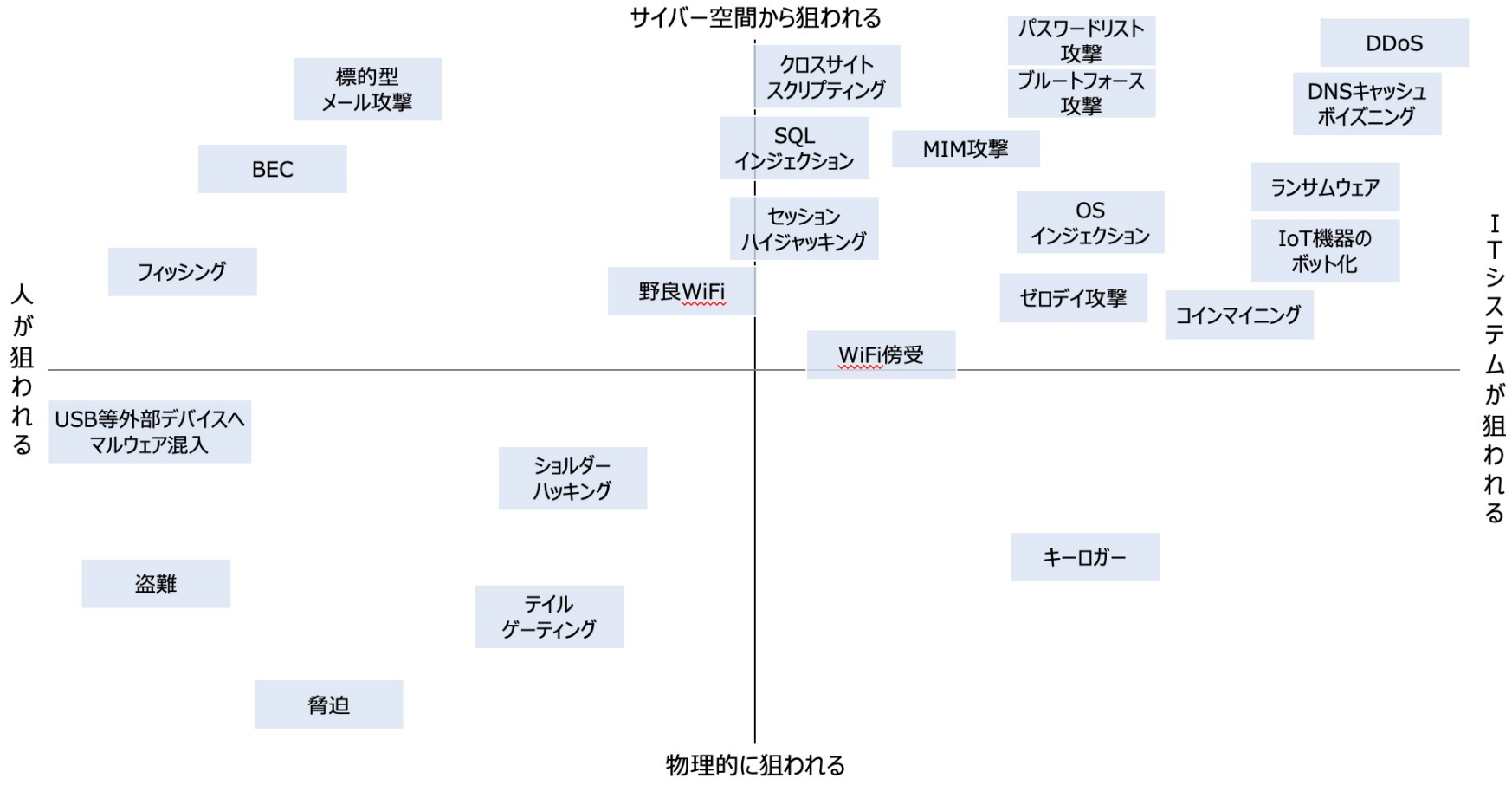
危機体系におけるサイバークライシス

大分類	中分類		小分類	結果を生じうる事象（脅威）の例
環境に起因する脅威	災害		• 自然現象による災害	地震、火災、風水害、落雷、動物害、温度・湿度異常
	障害		• 設備障害	停電、瞬断、施設内火災、漏水、空調機器の故障、入退出管理装置の故障、監視カメラの故障
			• ハードウェア障害	メモリ障害、ディスク障害、CPU障害、電源装置障害、ケーブル劣化、メモリやディスクの容量オーバー
			• ソフトウェア障害	OSやアプリケーションの潜在的なバグ・過負荷等による異常
			• ネットワーク障害	回線障害(専用回線・公衆回線の障害)、通信事業者(接続局、ISP、NOC、IDC等)内での障害、通信機器障害、構内配線の障害
人に起因する脅威	意図的	外部不正	• WEB改ざん	脆弱性
			• 情報漏えい	マルウェア感染
			• 情報滅失	ランサムウェア感染
			• 不正アクセス	SQLインジェクション、OSコマンドインジェクション、フィッシング、パスワードクラック
			• サービス妨害	DoS/DDoS攻撃
			• ソーシャルエンジニアリング	ソーシャルハッキング
			• 盗聴	ネットワーク盗聴
		内部不正	• システムの不正利用	不正なデータ操作、機密情報の不正な閲覧
			• データの不正持ち出し	機密情報の不正持ち出し、データの意図的な外部送信
			• システムの破壊	データを破壊するマルウェアのインストール
	偶発的		• 操作ミス	メール誤送信、マルウェア付きメールの開封、重要データの消去、意図しないシステム停止
			• 遺失・紛失	持ち出し媒体の置き忘れ、管理不備による媒体の紛失
			• 不適切な廃棄	廃棄した媒体からの復元
			• 許可されない機器・媒体・プログラムの持ち込み	マルウェアに感染した機器を社内ネットワークに接続
			• 意図しない情報公開	Webサーバの設定不備による重要データの流出
			• 任務怠慢	既定の捜査の実行忘れ

サイバークライシス

Syngula

サイバーセキュリティの手法とターゲット



Synqula

主なサイバー攻撃における検知および対策ソリューション

●検知ソリューション

代表的な攻撃方法	対策								
	セキュアコーディング	セキュリティパッチ	脆弱性診断	ID管理	スクラビングセンター	DDoS緩和装置	Fire Wall	IDS/IPS	WAF
不正な通信による攻撃（Dos/DDoS攻撃）		○	○		○	○	○	○	
不正アクセスによる攻撃				○			○	○	○
マルウェアによる攻撃		○	○				○		
脆弱性を突いた攻撃	○	○	○					○	○

●対策ソリューション

セキュアコーディング SOLインジェクション、クロスサイトスクリプティングなどの脆弱性を生まない開発手法

セキュリティパッチ ソフトウェア開発元（Microsoftなど）から脆弱性対策のために提供される更新プログラム

脆弱性診断 アプリケーションやその基盤となるOSなどに脆弱性が残っていないかを検査するテスト

スクラビングセンター おもにクラウドサービスで、DDoS攻撃パケットなどを除去し正当な通信だけを通すサービス

DDoS緩和装置 オンプレミス（自社環境）またはプロバイダサイドに設置し、DDoS攻撃パケットを廃棄する装置

Fire Wall 通過してはいけない通信を阻止する装置、通過させるかどうかの判断基準として、IPアドレスベースのものから、アプリケーションの種類を判断するものまである。

IDS/IPS Intrusion Detection System/ Intrusion Protection System(侵入検知/防御システム)

WAF Web Application Firewall(アプリケーションの脆弱性を突いた攻撃を防ぐFirewall)

サイバークライシスによる企業の損失

企業資産の喪失や事業の停止

コインチェック株式会社における仮想通貨流出事例

2018年1月26日、コインチェックが保持している仮想通貨のうちNEM（ネム）建ての顧客資産が、クラッキングにより取引所から外部に送金され、さらに別口座に移転されてほぼ100%流出してしまう事態が発生した。

同社はユーザーに対して580億円の損失補償を実施。

企業イメージの低下

ソニー株式会社における顧客情報流出事例

2011年4月21日、サイバー攻撃により、ソニー株式会社と株式会社ソニー・コンピュータエンタテインメントが7700万件以上の顧客情報を漏えいした。システムの脆弱性をついたサイバー攻撃で、情報漏えいによる被害は2兆円以上とされている。さらにイメージダウンを恐れたソニーは、被害の情報公開を遅らせたことも発覚し、批判を集める結果にもなった。

企業価値や株価の毀損

カプコン株式会社における機密情報流出事例

2020年11月9日、「RAGNAR LOCKER」を名乗るグループによって機密情報が盗み取られ、盗み取ったデータと引き換えに身代金を要求される。2020年11月16日時点で、およそ35万件の個人情報が流失した可能性があると発表した。

株価は16%下落となった。

その他取引への影響

ソフトバンク株式会社における機密情報流出事例

2013年5月27日、同社が運営するWebサーバに対して外部から不正アクセスがあり、顧客情報の流出が判明したと発表した。これは4月23日17時頃、同社が契約している決済代行会社よりクレジットカード情報の流出懸念について連絡があり、これを受けて同日直ちに同サーバを用いたサービスの申し込みの停止およびデータベースサーバ内に保存されていたクレジットカード情報の削除を行ったというもの。調査の結果、不正アクセスを受けたサーバには最大146,701件にのぼる顧客のクレジットカード情報があり、うち2011年3月7日から2013年4月23日に申し込みを行った109,112件が流出したとされる。流出した情報にはカード名義人名・カード番号・カード有効期限・セキュリティコード・申込者住所が含まれていた。

Syngula

相次ぐ大手企業の不正アクセス・セキュリティー事故

マッチングアプリOmiai、個人情報10年保存「見直し検討」

6/8(火) 11:00 配信 3

朝日新聞 DIGITAL

主なマッチングアプリの個人情報保存期間は……

画像は運営会社提供

	サービス開始	利用者数	退会後の個人情報の保存期間
Omiai	12年2月	累計600万人	10年間
Tinder	12年8月	4.3億回以上（世界累計ダウンロード数）	3カ月間
ペアーズ	12年10月	累計1千万人以上	非公表
タップル	14年5月	687万人	90日間
ゼクシィ縁結び	15年4月	累計150万人	非公表
with	16年3月	累計450万人	3年間

【表】主なマッチングアプリの個人情報保存期間は…

ネット上で恋人や結婚相手を見つけるマッチングアプリ大手「Omiai（オミアイ）」で5月、退会者を含めた利用者の運転免許証などの画像データ約171万件が流出した恐れが発覚した。こうしたアプリは年齢確認が必須で、運営会社は身分証明書データの送信を利用者に求めている。流出すれば悪用される危険性が高い個人データを、各社は退会後、いつまで保存しているのか、主なマッチングアプリに尋ねると、思わぬ違いも浮かび上がった。

【写真】「Omiai」のウェブページ

オミアイは、会員情報を管理するサーバーが不正アクセスを受け、免許証・健康保険証・パスポートなどの画像データが流出した恐れがある。この中には退会者の情報も含まれていた。退会後も10年間は個人情報を保存していたためだ。また、これらのデータは暗号化処理をしていなかったという。

鹿島もキーエンスもサイバー恐喝被害、身代金を支払ったらダメか

2021.5.10

11件のコメント

吉野 次郎
日経ビジネス記者

印刷　クリップ

4月末以降、鹿島建設やキーエンスの海外拠点での被害が相次いで発覚するなど、インターネットで恐喝を受ける企業が急増している。恐喝に使われるコンピューターウイルスは「ランサム（身代金）ウエア」と呼ばれる。感染するとパソコンやサーバー内のデータが使えなくなり、元に戻す見返りに「身代金」を要求するメッセージが画面に表示される。

特に1年半前から被害が急増しているのが「暴露型ランサムウエア」だ。データを使えなくするだけでなく、データを大量に盗み出して一部をネットで公開。「残りを公開されたくなかったら身代金を支払え」と脅してくる。今回、鹿島やキーエンスは盗まれたデータの一部がネットにさらされたことで、被害が発覚した。

相次ぐ大手企業の不正アクセス・セキュリティー事故

三菱電機に「隠密型」攻撃　再び被害、中国系ハッカーか

有料会員記事

編集委員・須藤龍也　2020年11月20日 16時19分

再びサイバー攻撃を受けた大手総合電機メーカーの三菱電機

三菱電機 が再び、大規模な サイバー攻撃 に見舞われた。昨年6月に発覚した攻撃では、「BlackTech」（ブラックテック）という中国系 ハッカー 集団の関与が浮上した。同社では今回も中国系集団による攻撃との見方を強めているが、同じ集団かどうかは現時点で分かっていない。

三菱電機にまたサイバー攻撃、取引先の口座８千超流出 →

これらの集団はいずれも企業の機密情報を狙った「スパイ」目的とみられ、インテリジェンス（情報収集・分析）に詳しい専門家の多くは、中国政府や軍の意向を受けた ハッカー との見方で一致している。

カプコン サイバー攻撃 金銭要求の「ランサムウェア」

2020年11月12日 18時19分

大阪のゲームソフト会社のカプコンがサ
られるマルウェアー悪意を持ったプログ
ファイルを徹底的に暗号化し、身代金を
サイバー攻撃であることが分かりました

CAPCOM

2020年11月16日
大阪市中央区内平野町三丁目1番3号
株式会社カプコン
代表取締役社長 辻本 春弘
（コード番号：9697 東証第1部）

不正アクセスによる情報流出に関するお知らせとお詫び

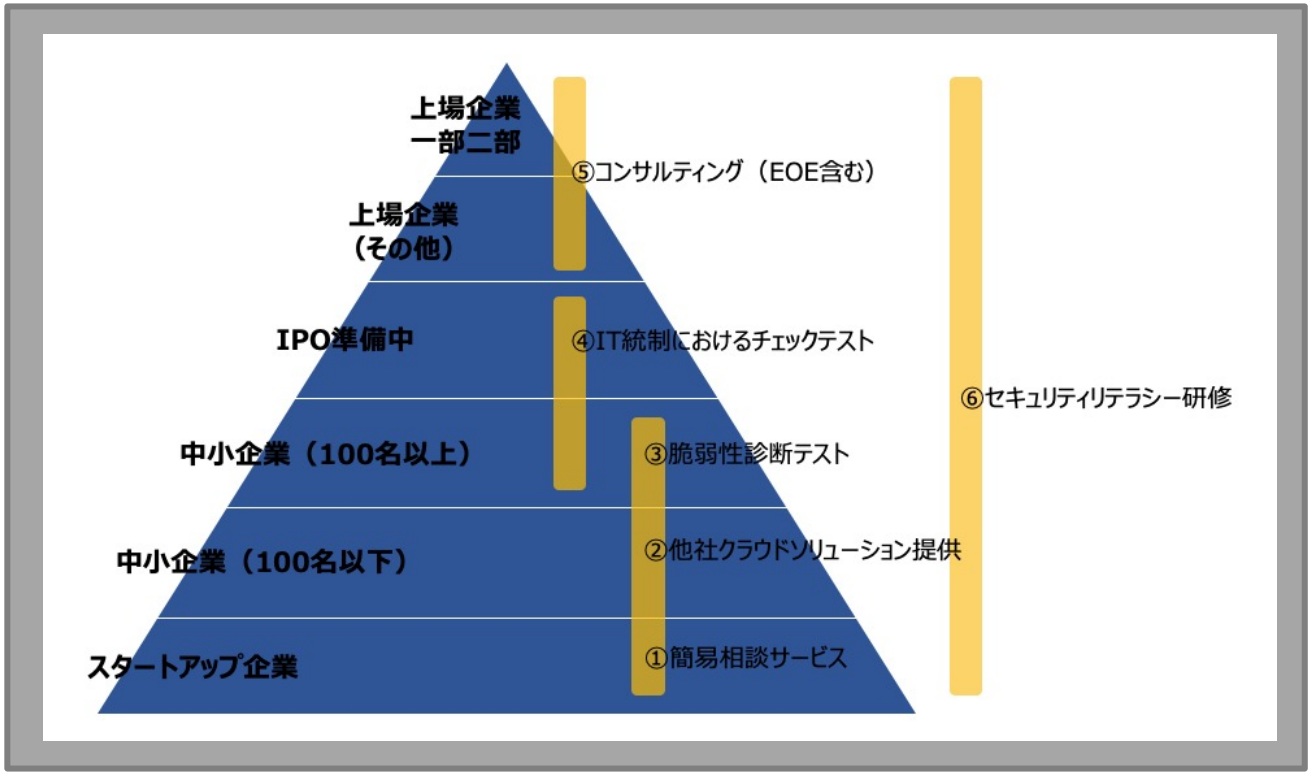
株式会社カプコンは、第三者からのオーダーメイド型ランサムウェアによる不正アクセス攻撃を受け、当社グループが保有する個人情報流出の発生を確認いたしました。
また、この攻撃により、当社が保有している個人情報・企業情報が流出した可能性があることを確認しましたので、「2. 流出の可能性がある情報」にて併せてお知らせいたします。
なお、現時点ではコンテンツ開発や事業遂行において支障はございません。
お客様はじめ多くのご関係先にご迷惑とご心配をおかけしておりますことを、深くお詫び申しあげます。

02 Cyber Rescueの概要

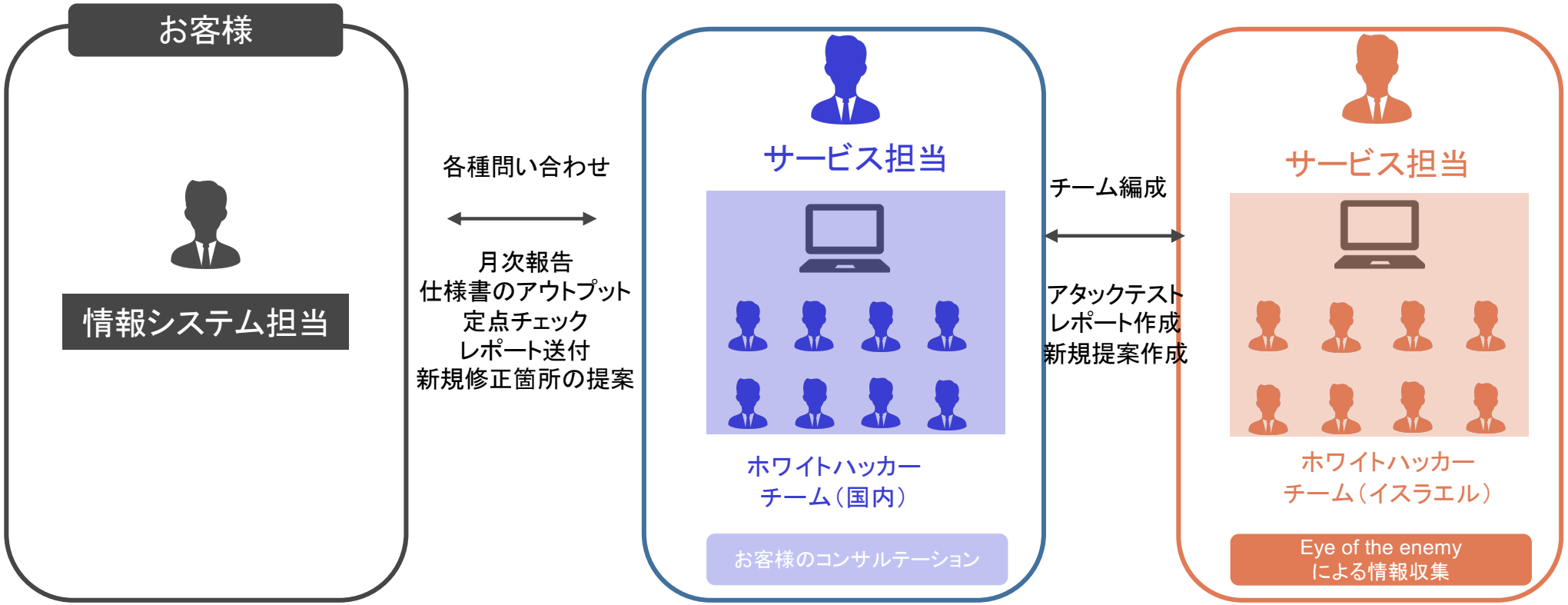
Cyber Rescueとは

サイバーセキュリティコンサルティングサービス

クライアントニーズに沿った適切なソリューションを提供します。



Cyber Rescueの体制



弊社チームの強み

最高技術顧問　“Code name 大佐”

グローバルに活躍し日本を代表する
ホワイトハッカーが最高技術顧問に就任

実績豊富な
ホワイトハッカーによる診断

完全成果報酬での
サービスを保有

コンサルティング
サービス一体型

他社との競合優位性

③より実践的な視点から精緻な調査を行い、有意な情報を提供

●脆弱性診断＋侵入テスト

「**現在課題**」「**攻めの調査**」

セキュリティエンジニア中心の他社とは違い、優秀なホワイトハッカーによる調査分析により、「突破」を前提にした課題箇所の明確化

●保守運用

「**将来課題**」「**守りの実装**」

脆弱性診断サービス会社が対応できない、「**課題解決**」**に向けた具体的打ち手を提案、実現**していくことが可能です。

実施内容事例

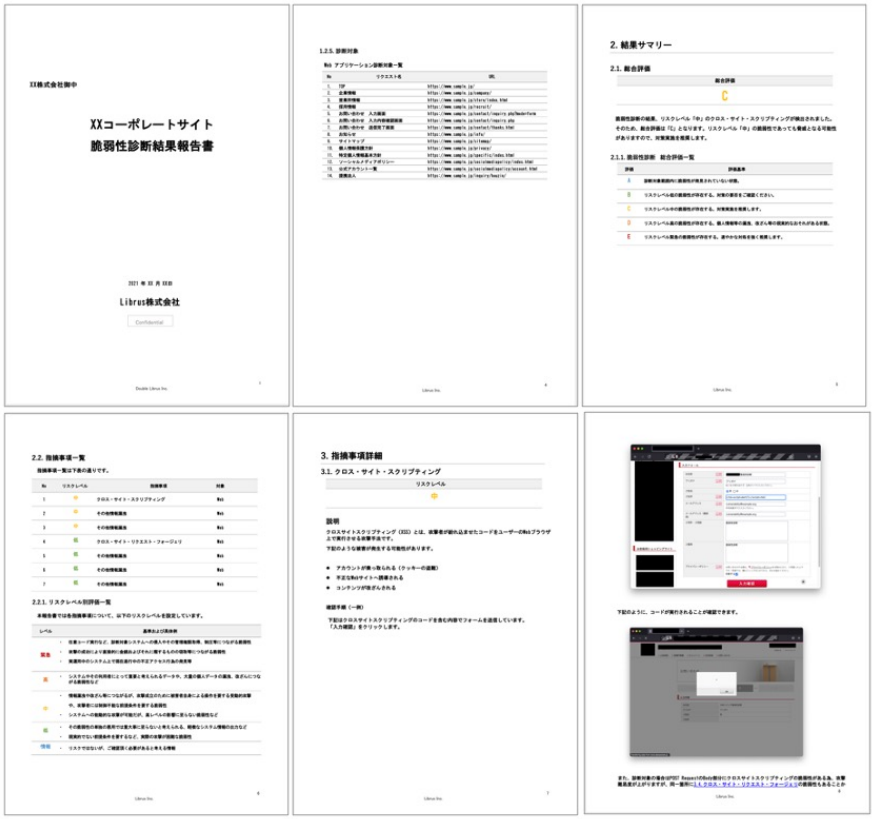
01 ログを活用したクラッキング率調査から、
下記「**思想**」に基づき、攻撃されやすい箇所の特定および解決策の提示

不正アクセスを	不正アクセスされることを前提とした
「事前対策/予防する」	**「順応する」**
思想	**思想**

02 サイバー犯罪等既存会社が重視するコア領域に加え、例外的or通常対象外とされる非コア領域調査、問題箇所特定および解決策の提示

03 セキュリティ課題の解決知見を用いて、調査分析結果から、解決方法を提案

成果物イメージ



Synqula

①② Cyber Rescue Light

①簡易シミュレーションアタック

簡易シミュレーションアタックを行い、現状の簡易セキュリティホールを把握します。

Red Flag：緊急性が高い
Yellow Flag：緊急性は高くないが早めに対応しほうがいい

```
<meta name="author" content='                              >
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({
'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.
getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=
true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.
parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-5CKHVS');</
script>
<!-- End Google Tag Manager -->
<meta property="og:title" content=                              >
<meta property="og:type" content="website">
<meta property="og:url" content='
<meta property="og:image" content=
```

②他社クラウドソリューション

サイバーセキュリティクラウドソリューションを提供します。

企業の課題に合わせたソリューションを組み合わせることで多層防御のセキュリティを構築します。

他社クラウドソリューション例：

Cybereason EDR

SentinelOne™

DDH
DIGITAL DATA HACKING

etc…

③脆弱性診断テスト“完全成果型サイバーセキュリティコンサルティングサービス”

お客様が抱える課題

1 事業継続性の観点等からサイバーセキュリティに本格的に取り組みたいが、大手サービスベンダーは費用が高すぎる

2 サービスベンダーの技術力が見極められない

3 信用度の低いサービスベンダーに依頼することで、情報流出や経済的/時間的な損失が懸念される

お客様にとってはサイバーセキュリティに関する情報が圧倒的に不足しており、極めてアンフェアな状態です。これによって適切なサービスベンダー選定が難しく、大きな課題であると考えます。

弊社の“完全成果型サイバーセキュリティコンサルティングサービス”をご提案いたします

弊社がご提案する解決策と選ばれる理由

弊社のご提案内容

システム脆弱性の指摘1点につき、50万円（税抜）の成果報酬、特に重要な脆弱性に関しては指摘1点につき、60万円（税抜）の成果報酬のみ発生

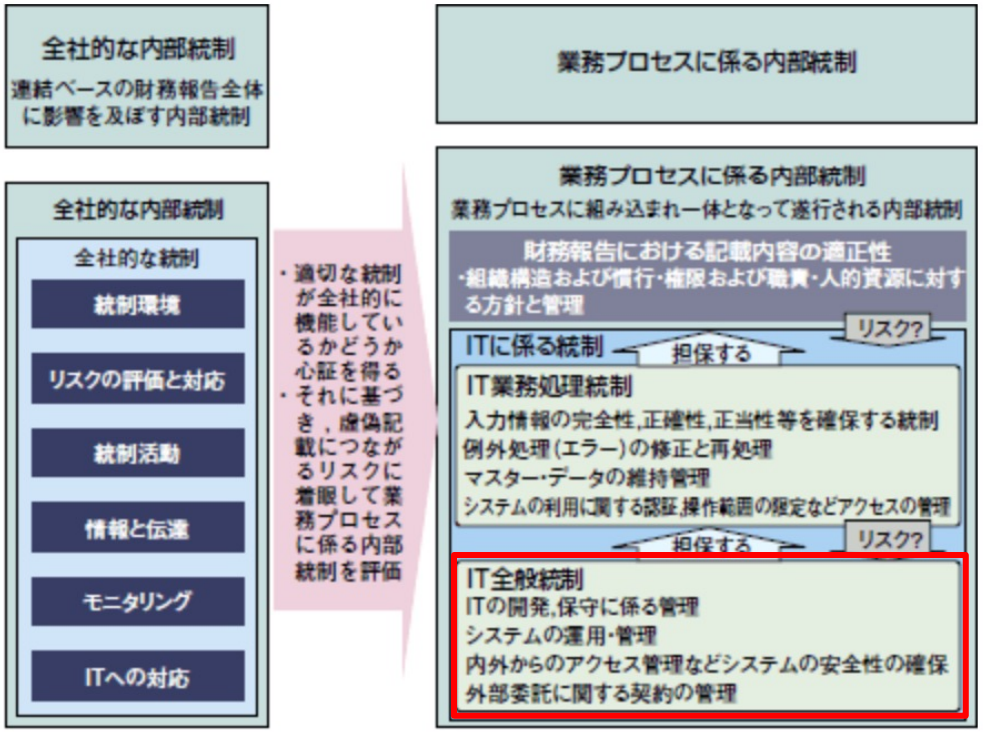
完全成果報酬だから、着手金なし

上限ミニマム200万円（税抜）から発注できるから、予算管理上も安心

年度別の定期検診で、最先端のサイバーセキュリティも定期的にキャッチアップ可能

④IT統制におけるチェックテスト

IPO準備中・IPO後の企業向けのセキュリティ対策です。



ITへの対応

・経営者は、ITに関する適切な戦略、計画等を定めているか。

・経営者は、内部統制を整備する際に、IT環境を適切に理解し、これを踏まえた方針を明確に示しているか。

・経営者は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びITを用いた統制の利用領域について、適切に判断しているか。

・ITを用いて統制活動を整備する際には、ITを利用することにより生じる新たなリスクが考慮されているか。

・経営者は、ITに係る全般統制及びITに係る業務処理統制についての方針及び手続を適切に定めているか。

⑤Cyber Rescue

サイバーレスキューとは？

1 シミュレーションアタック

2 セキュリティホールの解決

3 定点チェック（Eye of the enemyの活用）

システム管理・サイバーセキュリティリスク管理実態をヒアリングしつつ、現状を把握します。シミュレーションアタックを行い、組織の環境内に潜在する脆弱ポイントを捜索し、一社一社の環境にフィットしたオーダーメイドのセキュリティサービスを提供します。

サイバーセキュリティに関するコンサルティングサービスを提供します。

Eye of the enemyとは

諜報活動や偵察活動により収集された機密情報をもとに、実際に利用される攻撃手段やワークフローを模倣し、シミュレーション攻撃を繰り返しながら、監視巡回するプラットフォームです。

⑦セキュリティリテラシーコンサルティング

業務の負荷なく社員のサイバーセキュリティの意識を強化し、情報漏えいのリスクを減少させます。

コンテンツ例

フィッシングメールの知見例

漫画によるコンテンツ

脆弱性診”概要（1/2）

脆弱性診断:脆弱性診断専用のツールやホワイトハッカーの手動によってシステムの脆弱性を診断するサービスです。当社では下記の項目をベースに脆弱性診断を実施いたします。

#	脆弱性診断項目			診断手法	
	診断対象	リスク概要	脆弱性診断有効度/重要度	診断種別	
				ツール診断	手動診断
1	SQLインジェクション	DBサーバへのアクセスを不正に実行されてしまいます。 これにより、ウェブサイトからの情報漏洩、改竄等の危険性があります。	必須	●	●
2	コマンドインジェクション	サーバ内のOSのコマンドを不正に実行されてしまいます。 これにより、ウェブサイトからの情報漏洩、改竄等の危険性があります。	必須	●	●
3	クロス・サイト・スクリプティング	サイトをまたがって不正な要求を送り、ユーザが意図していないスクリプトを実行させられてしまいます。 その結果、例えば偽ページを表示することが可能になり、フィッシング詐欺などに悪用されてしまいます。	必須	●	●
4	クロス・サイト・リクエスト・フォージェリ	サイトをまたがって不正な要求を送り、ユーザが意図していない操作を実行させられてしまいます。 例えば、ユーザが意図しないままオンラインショップで買い物をさせられたりしてしまいます。	必須	●	●
5	クロス・サイト・トレーシング	ウェブのヘッダ情報を不正に読み出されてしまいます。 これにより、他の脆弱性を利用して管理者や他のユーザに成りすまされてしまいます。	低	●	
6	スクリプト（SQL含む）の実行	許可していないスクリプトを実行されてしまうため、情報の漏洩やウェブサイトの改竄を許してしまいます。	高	●	
7	XMLインジェクション	XMLデータにスクリプト等を混入して攻撃されてしまいます。 これにより、ウェブサイトからの情報漏洩、改竄等の危険性があります。	低		●
8	パラメータ改竄	パラメータを不正に改竄されてしまいます。その結果、管理者や他のユーザに成りすまされてしまいます。	高	●	
9	CRLFインジェクション （HTTPヘッダインジェクション）	動的にHTTPヘッダを生成する機能の不備を突いてヘッダ行を挿入することで不正な動作が発生し、セッションハイジャック、XSS等につながる可能性がある攻撃を受ける危険性があります。	中	●	●
10	パストラバーサル （ディレクトリ・トラバーサル）	ウェブサーバ内のファイルを閲覧されることにより、ウェブサーバ攻撃の足がかりとされてしまいます。	中	●	●
11	SSIインジェクション	SSIコマンドを不正に実行されてしまいます。 これにより、ウェブサイトからの情報漏洩、改竄等の危険性があります。	低	●	
12	LDAPインジェクション	LDAPコマンドを不正に使用されてしまいます。 これにより、ウェブサイトからの情報漏洩、改竄等の危険性があります。	低	●	
13	リモートファイルインクルージョン	プログラムの中で別ファイルを参照するコードがあった場合に、実際に参照すべきファイルとは別のファイルやデータを読み込ませて、本来意図しない不正なデータ処理を実行されます。 システム上に脆弱性がある場合、ファイルインクルードで攻撃されることで、ユーザーIDやパスワードが漏洩し、システムの乗っ取りなどを引き起こす可能性があります。	中	●	●
14	認証制御の不備	サーバーのセッション管理等により正常なログイン処理を介さずにログイン後の画面にアクセスされてしまうため、成りすましや情報漏洩の危険性があります。（セッションジャック等）	必須		●
15	認可制御の不備	セッション情報が推測しやすい値の場合、攻撃者は正しい値を推測し、管理者やユーザに成りすますことができます。 また認可が不適切だと、アクセス権限の高いコンテンツや機能へのアクセスを認めてしまいます。 これにより、攻撃者が他のユーザや管理者に成りすます危険性があります。	高		●

脆弱性診断概要（2/2）

脆弱性診断:脆弱性診断専用のツールやホワイトハッカーの手動によってシステムの脆弱性を診断するサービスです。当社では下記の項目をベースに脆弱性診断を実施いたします。

#	脆弱性診断項目			診断手法	
	診断対象	リスク概要	脆弱性診断有効度/重要度	診断種別	
				ツール診断	手動診断
16	セッション管理の不備	セッション・クッキーが類推可能な簡単なものであったり、セキュアでない通信経路で送られた過程で盗まれたりすると、セッション自体が盗まれる可能性があります。 これにより、個人情報が盗まれたり、コンピュータに侵入されたりする危険性があります。	必須		●
17	セッション期限が不適切	セッション期限が不適切である場合、ユーザのセッション情報を盗用しやすくなり、攻撃者が管理者やユーザに成りすますことができます。	高	●	
18	セッションの固定	攻撃者が任意のセッション情報を使って管理者やユーザに成りすますリスクがあります。	高	●	
19	セッションの盗難	SSL等を使用して暗号化をしていない場合、攻撃者はセッション情報を容易に取得することができ、管理者やユーザに成りすますことができます。	高	●	
20	オープンリダイレクト	信頼できるウェブサイトから悪意あるウェブサイトにユーザを誘導し、フィッシング攻撃でユーザー情報を盗まれる危険性があります。	中		●
21	クリックジャッキング	見えない透明化したリンクを、ユーザが見ているサイトに被せて表示し、意図したリンクとは別のURLへ遷移させられてしまいます。 そのリンク先に悪意のあるスクリプトが埋め込まれていた場合、予期しなかった挙動や、情報漏洩の危険性があります。	中		●
22	ディクショナリアタック	管理者や他のユーザに成りすまされてしまう危険性があります。	中	●	
23	その他情報漏洩	機微情報や脆弱性に関する情報が記載されている状態になっています。	中		●
24	バッファ・オーバフロー	アプリケーションの予期しないデータを送り、アプリケーションを異常終了させられてしまいます。 これにより、ウェブサーバのサービスを停止させられたり、ウェブサーバを乗っ取られる危険性があります。	中	●	
25	DDoS攻撃	サービスを利用できなくすることで嫌がらせをされたり、攻撃をやめることと引き換えに金銭を要求されるリスクがあります。 また、ライバル企業の依頼で同業者のサービスに攻撃を仕掛けて「あのサービスはつながらなくて使えない」といった風評被害を誘発させられるリスクがあります。	中		●

侵入テスト概要（1/2）

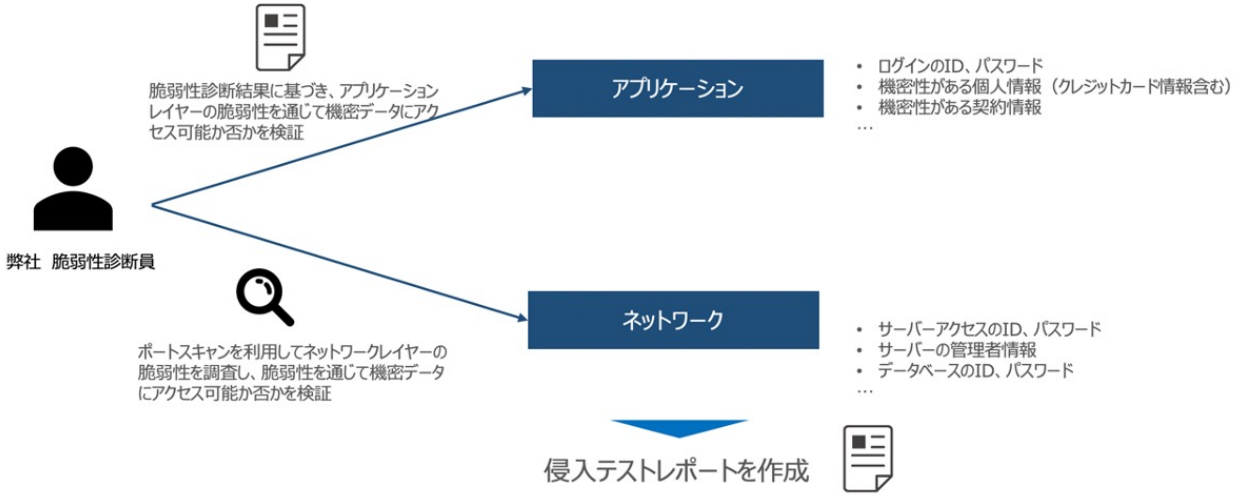
侵入テスト:外部からシステムに侵入し、コンピュータやネットワークの脆弱性を通じて、機密性があるデータ（個人情報、サーバ情報等）にアクセスが可能か検証するテストです。

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



侵入テスト概要（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。

料金表

①簡易相談サービス	40万円/1回
②クラウドソリューション提供	10万円～/月
③脆弱性診断テスト	200万円～/1回
④IT統制におけるチェックテスト	100万円～/1回
⑤コンサルティング（EOE含む）	300万円～/月
⑥リテラシーコンサルティング	10万円～/月

※上記金額はMinの金額であり都度お見積もりさせていただきます。

thank you

https://www.syngula.co.jp/

〒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