SasaL（ササエル）

AIペネトレーションテストサービス
ご紹介資料

2020年3月

扶桑電通株式会社

企業存続の脅威となるサイバー攻撃に備える

昨今、働き方改革やWebテクノロジーの発達により、ネットワークシステムの複雑化やアクセスするデバイスの多様化が進んでおります。

それに伴い攻撃手法も多様化し、Webアプリ・スマホアプリの設計や開発の不備を利用したサイバー攻撃が後をたちません。

個人情報漏えいインシデント概要

	2017年		**2018年**
漏えい件数	386件	↗	**443件**
想定損害賠償総額	1,914億2,742万円	↗	**2,684億5,743万円**
一件当たり平均想定損害賠償額	5億4,850万円	↗	**6億3,767万円**

NPO日本ネットワークセキュリティ協会「2018年情報セキュリティインシデントに関する調査結果」

1件あたりに換算すると、賠償額は約6億3千万円になり、中小企業以下であれば企業の存続を脅かすほどの金額といえます。

また、財務的に体力のある大企業であったとしても、サイバー攻撃により個人情報などが漏洩したことによる**経営責任**、**社会的信用の失墜とその回復にかかるコスト**を想像すると、**企業経営に著しい影響を与えることは必至**となります。

つまり**企業規模を問わず、サイバー攻撃対策は企業活動に必須の取り組み**といえます。

ペネトレーションテストとは

ペネトレーションテストは、テスト対象の企業/組織に応じて**様々なサイバー攻撃手法を講じて、システムなどへの侵入を試みることでセキュリティレベルを評価する取り組み**で、2018年5月には金融庁から「諸外国の『脅威ベースのペネトレーションテスト』に関する報告書」が公表されたことから、急速に関心が高まっている。

また、内閣府サイバーセキュリティセンターでは、2020年東京オリンピック・パラリンピック競技大会までに、**全ての独立行政法人に対してペネトレーションテストを行う**としているなど、その重要性がクローズアップされている。

セキュリティ診断（脆弱性診断）とペネトレーションテストの違い

脆弱性診断は**脆弱性を発見する事を目的**としています。診断を定期的に行い、脆弱性を発見して修正するというのが通常の流れとなります。テスト対象のサーバやシステムに対して、特定のコマンドを送信してOSやアプリケーションのバージョンなどの情報を取得し、どういった脆弱性を持っているのかを確認します。

ペネトレーションテストは、脆弱性診断に加え**存在する脆弱性を悪用された時に、どの程度影響があるのか**まで**攻撃者の視点で検証**することになります。そのため、ペネトレーションテストの方が、よりスキルの高いエンジニアが必要になります。

	セキュリティ診断	ペネトレーションテスト
目的	脆弱性を網羅的に洗い出すこと	**攻撃者の目的が達成されてしまうかを確認するために、必要な脆弱性を発見・評価・検証すること**
アプローチ	ベースラインアプローチ	**リスクベースアプローチ**
方式	Web、ネットワークなど、システムを構成する要素をセキュリティ規格などに照らし、安全性を確認	**サイバー攻撃を模して、攻撃目標が達成できるかを試行**
報告内容	個別の脆弱性リスト	**攻撃シナリオと検証結果**

SasaL AIペネトレーションテストサービス

お客様が実施したいテスト内容に応じて、
最適なペネトレーションテストサービスをご提案致します。

公開サーバ・アプリケーションテスト

外部Webサーバ診断
外部メールサーバ診断
外部アプリケーションサーバ診断
サーバSSL/TLS設定テスト
モバイルアプリケーションテスト

ネットワークプラットフォームテスト

内部ネットワークシステム
内部ネットワークプラットフォーム
オーダーメイドのセキュリティ検査
大規模ネットワーク診断

リモートペネトレーションテストサービス

- ✓ アプリケーション・プロダクトに対するテスト
- ✓ ホワイトハッカーによる正確な診断レポート
- ✓ 誤検出ゼロのサービスアグリーメント（Zero False-Positives SLA）
- ✓ 最新の国際ガイドライン、最新の脆弱性、最新の攻撃手法に常に対応

脅威ベースのペネトレーションテスト

TLPT（Threat Led Penetration Testing）

- ✓ 侵入シナリオの網羅的な調査
- ✓ Red Team（イスラエル・スイス・台湾・日本）による侵入テスト
- ✓ 実際のIT・OT環境に対して、または模擬環境に対してあらゆる攻撃手法を実施

リモートペネトレーションテストサービス

従来のペネトレーションテストにおける問題点

- 各社の様々なツールを組み合わせて診断するため費用が高騰する。
- 人力診断のためスコープに限界があり、長期間を要す。
- 非常に高いスキルをもった人材が世界的に不足している。
- 診断対象のプログラミング言語、システム範囲、スコープに制限有り。

第一世代
診断ツールによる自動検査

第二世代
ホワイトハッカーが
診断ツールなどを
一部手動で検査

SasaL AIペネトレーションテストサービス

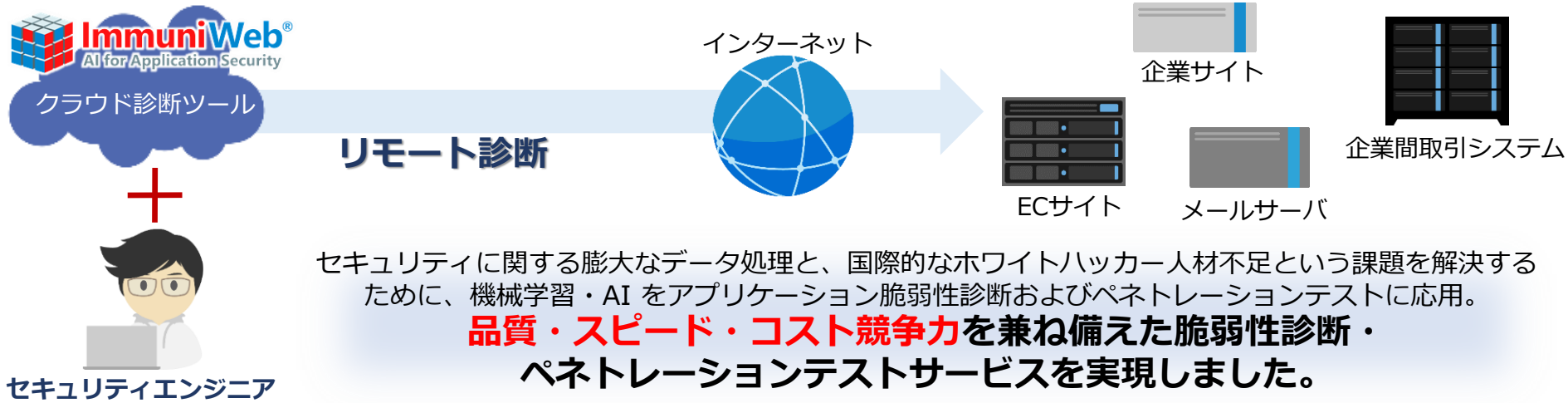
第3世代のセキュリティ診断

機械学習・AIペネトレーションテスト

ImmuniWeb® AI for Application Security × ICTコンビニサービス

- 世界各国の法制度・ガイドラインに準拠（NIST、GDPR、PCIDSS、HIPAAなど）
- 国際的な脆弱性規格に準拠（CVE、CVSSなど）
- ハッカーの攻撃手法を網羅（OWASP Top10、CWE/SANS Top25など）

- 過去の膨大な診断データから、**AIが最適な診断アルゴリズムを算出**
- ハイスペックのクラウドマシンを160以上並行で稼働させ、**短時間で高速、網羅的なテストを実現**
- **AIを使い高速でサイトマップを構築**
  お客様環境のレスポンスから、適度に負荷分散することが可能



セキュリティに関する膨大なデータ処理と、国際的なホワイトハッカー人材不足という課題を解決するために、機械学習・AI をアプリケーション脆弱性診断およびペネトレーションテストに応用。

品質・スピード・コスト競争力を兼ね備えた脆弱性診断・ペネトレーションテストサービスを実現しました。

ImmuniWebセキュリティ検査の実績

世界最高レベルの高品質と実績

WEBサーバセキュリティテスト実績

40,390,000件以上

GDPRおよびPCI DSSコンプライアンスについてWebサイトをチェックし、CMSおよびCSPセキュリティをテストし、Webサーバーの強化とプライバシーを確認します。

サーバSSL TLS設定テスト実績

42,560,000件以上

PCI DSS要件、HIPAAガイダンス、およびNISTガイドラインへの準拠についてSSL / TLSセキュリティと実装をテストします。

モバイルアプリテスト実績

527,200件以上

モバイルアプリケーション（iOS、Android）のセキュリティとプライバシーをテストし、OWASP Mobileトップ10およびその他の弱点を検出します。

ドメインブランドテスト実績

10,170,000件以上

商標やブランドを悪用しようとする「ブランドサイバースクワット」「タイポスクワッティング」「フィッシングサイト」等をチェックします。

他社セキュリティ診断との比較

	国内競合他社	SasaL AIペネトレーションテストサービス
診断費用の見積方法	**1リクエストあたり（動的ページ数）** **費用例：300ページで¥9,000,000～¥27,000,000** ¥30,000～¥90,000/1リクエスト	**1ドメインあたり** **費用例：¥1,700,000/1ドメイン**
両社の比較	**エンジニアの経験とカンによりある程度の診断優先順位がつけられるが、クオリティには差が出る。網羅性は保証できない。**	**網羅的なテストが可能なため、他社ツールで検出できない脆弱性が検出可能。セカンドオピニオンとしても有効。**
WEB見積範囲	**WEBアプリのみの検査で上記価格。WEBサーバとAPIは別見積。**	**WEBアプリ・WEBサーバ・APIをすべて含んで上記価格**
モバイル見積範囲	**モバイルアプリのみの検査でも、WEBページより高額になる場合が多い。バックエンドWEBアプリ、WEBサーバ、APIは別見積**	**iOS(またはAndroid）アプリ+バックエンドWEBアプリ+WEBサーバ・APIをすべて含んで上記価格**

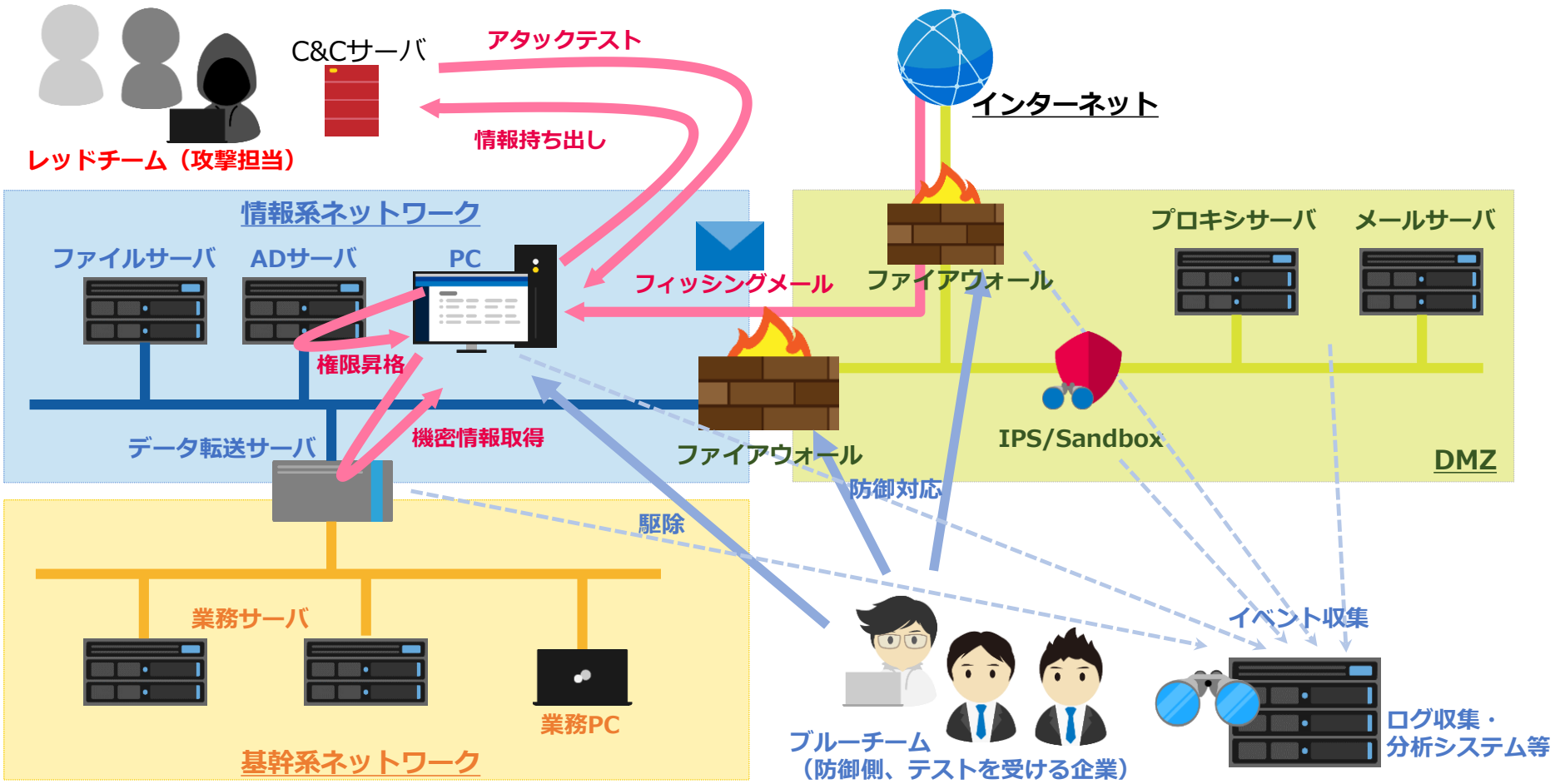
リモートペネトレーションテストサービスの流れ

初回訪問	概要ご説明
要件定義	セキュリティ診断の目的・スコープ・スケジュール
お見積り	診断対象のWEBサイトドメインを指定 診断対象のWEBサーバを指定 診断対象のモバイルアプリを指定（iOS、Android）
ご発注	発注書の受領・契約書の締結
診断開始	テスト中、IPS、WAF、アプリケーションにテスト用IPアドレスのアクセス許可 指定ドメインの全ページに対して、148項目の侵入手法を検査、国際脆弱性規格に準じて報告書作成 SQLインジェクション検査に伴うメール送付の了承
報告書送付	診断開始から2週間以内に報告書（日本語）を送付 侵入テストの手法、各種準拠する国際ガイドライン、脆弱性の箇所と修正方法などを記載
報告会開催	発見された脆弱性の説明 全社的な年間セキュリティ診断計画の策定 再診断の実施（別途見積）

診断期間の目安は2日～8日間。ご発注から報告書まで2週間～3週間という圧倒的な短期間で実施いたします。

脅威ベースのペネトレーションテストサービス ～ネットワークインフラテスト～

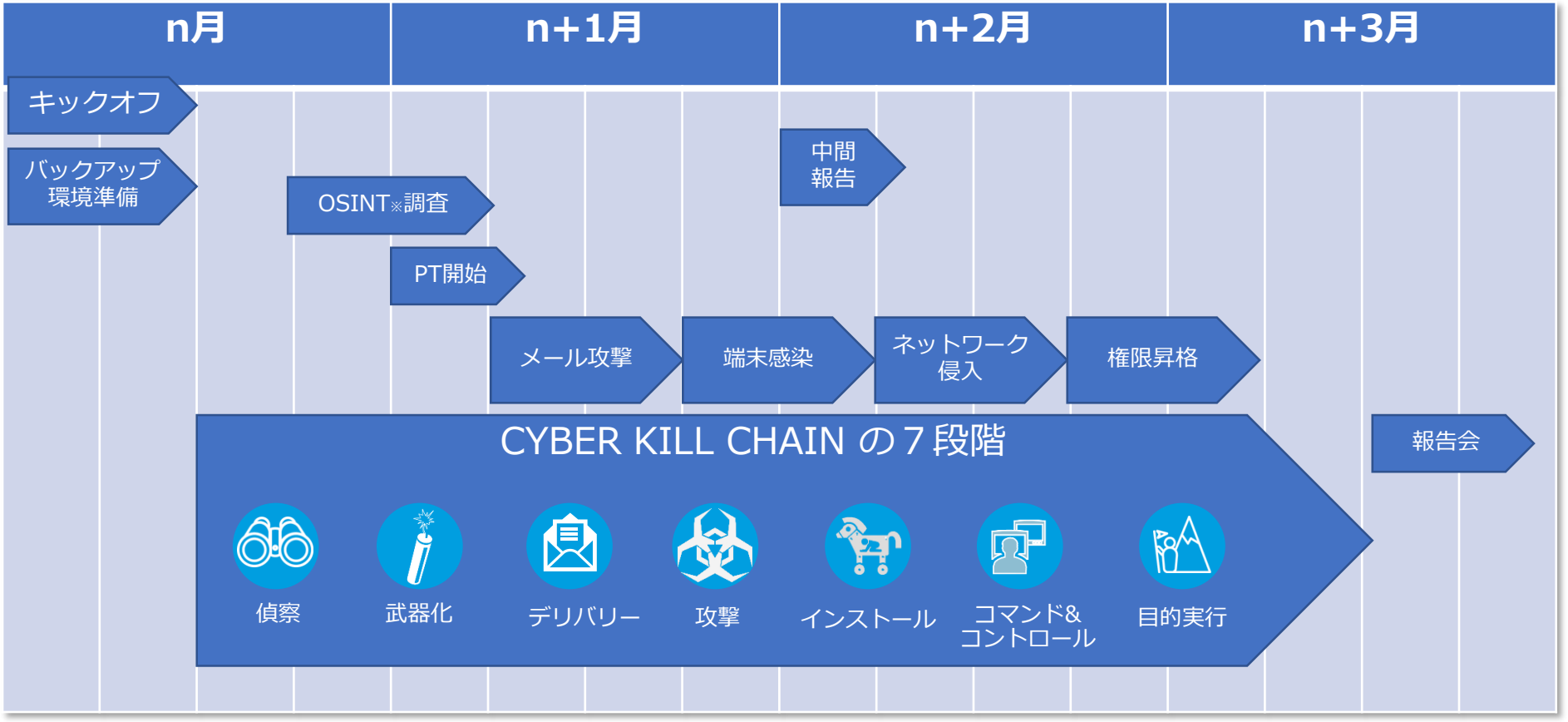
お客様が晒されている脅威やシステム・ネットワークの特性を考慮し、どのような脅威シナリオが成立しうるのかを検討します。
脅威シナリオに沿って、Red Teamにより擬似的な攻撃を仕掛けることで、既存のセキュリティ対策が有効に機能しているか検証し対策の不足や設定の不備等を調査いたします。
また、発生するアラートや記録されるログをもとに適切に対処できるか検証し、対応手順の不備や抜け漏れ等を洗い出すことができます。
マルウェアなどに感染した場合を想定し、PC端末が汚染された場合に水平展開・垂直展開が可能かどうかのシミュレーション等も行います。 ※実際にマルウェアをお客様システムに投入することはありません。



例）大企業向けペネトレーションテストの要件定義

項目	内容
時期	2019年10月以降　　期間　　約3カ月
ターゲット例	①　メールサーバ（ゴール：メールサーバに保管されているメールを閲覧する） ②　重要情報が保管されたサーバ（ゴール：サーバに保管されているファイル内容を確認する。顧客情報・技術情報など） ③　WEBサーバ・アプリケーションサーバ、データベース等アクセス（ゴール：アクセス権限の取得） ④　ルータ、FWなどのネットワーク機器のアクセス権限取得 ⑤　ネットワーク図の獲得
プロジェクト進行	テストのスタート １．疑似標的型メールの送付 ・疑似標的型メールを送付するメンバーのリストは、予め提供（もしくはブラックボックス） ・上記とは別に、メールに添付されたファイル／URLにアクセスするメンバーを準備（速やかに足場を作るため。任意） ・疑似攻撃メールを送付する際、ＢＣＣに窓口担当のアドレスを入れる（メール内容把握のため） ２．端末への感染 ３．水平展開 ４．垂直展開（権限昇格） ５．目的達成 ※貴社セキュリティチームによる検知、防御、インシデントレスポンスを実施。
侵入方法	ブラックボックステスト→グレーボックステスト（プロジェクトの各段階で多層防御の条件を緩和） OSINT、パスワードリスト、レインボーテーブルの利用可能。
対象環境	グループ国内のネットワーク ※テスト不可の拠点へはアクセスしない（条件は貴社より提示） 端末数　〇万IP程度　　端末：Windows,Mac　サーバ：Windows, Linux　データベース：mySQL等 メールアドレス〇名程度
対象組織	貴社より対象組織を指定
実施時間	日本の営業時間内での対応も可能
報告会	• 週次で実施内容と今後の予定を報告。 • 最終報告会（詳細と総括）を実施。 • 報告レポートは英語版と日本語版
報告レポート内容	• 調査方法 • 調査対象 • 侵入の時系列レポート • 脆弱性の報告 • 脆弱性の修正方法の明示
注意事項	• バッファオーバーフローに関するルール（サービス停止やCPU、メモリなどのリソースを圧迫するような操作） • ブルートフォースに関するルール（同一IDのログイン試行回数制限等） • テスト時に不審な攻撃を見つけた場合は対処可能とする。 • テストによりサーバのダウンやアカウントロックが発生した場合は連絡する
免責事項	別途契約書で定義

例）大企業向けペネトレーションテストの要件定義

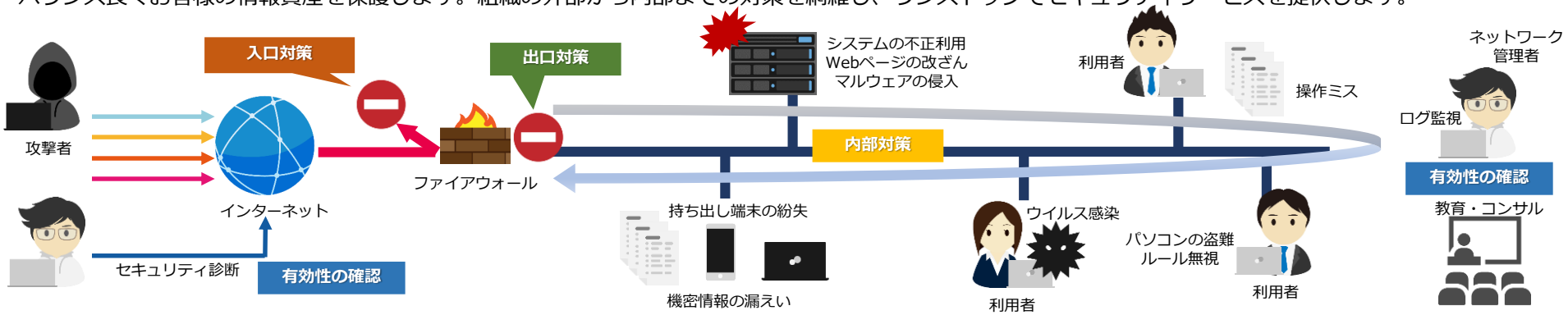


プロジェクト　7名体制×３カ月
報告書納品（英語・日本語）
報告会開催（英語・日本語各１回）
週次での進捗会議（メール・ビデオ会議もしくは訪問）

※OSINT (open source intelligence) … 一般に公開され利用可能な情報を情報源に機密情報等を収集する手法を指します。例えば、トップに対するインタビュー記事や企業のプレスリリース、書籍、インターネット情報等を合法的に調べて分析することにより、一見断片的なデータから、意味を持った情報が得ようとする手法

ICTコンビニサービス　セキュリティソリューションマップ

扶桑電通ICTコンビニサービスのセキュリティソリューションは日々巧妙化しつつある標的型サイバー攻撃、不正アクセス、情報漏洩などのあらゆる脅威からバランス良くお客様の情報資産を保護します。組織の外部から内部までの対策を網羅し、ワンストップでセキュリティサービスを提供します。



入口対策

標的サイバー攻撃、不正アクセス対策などによる内部ネットワークへの侵入を防ぐ対策です。外部からの不正侵入を防御します。

サイバー攻撃対策

次世代ファイアウォール	Palo Alto PAシリーズ	パロアルトネットワークス
	フォーティゲート	FORTINET

WEB/メールセキュリティ

標的型メール対策	Deep Discovery EmailI nspector	トレンドマイクロ
クラウドサービスの保護	HENNGE ONE	HENNGE
	Online Service Gate	Soft bank

不正侵入検知・防御対策

IPS/IDS	Palo Alto PAシリーズ	パロアルトネットワークス
	フォーティゲート	FORTINET
不正侵入の認証強化	NetAttest EPS	ソリトンシステムズ

ウイルス・スパム対策

ウイルス侵入防止	Palo Alto PAシリーズ	パロアルトネットワークス
	CloudGen Firewall	Barracuda
スパムメール防御	Email Security Gateway	Barracuda

出口対策

企業の重要な情報を外部感染による外部への流失を防ぐ対策です。内部から外部への情報流出を監視し、情報漏洩のリスクを最小化することによる多層防御します。

情報漏洩対策

メール誤送信防止	FENCE メール誤送信対策サービス	富士通
ゲートウェイ型メール暗号	FENCE-Mail For Gateway	富士通
DNSで危険サイト対策	Soliton DNS Guard	ソリトンシステムズ
多要素認証	Smart OnID	ソリトンシステムズ

標的型攻撃対策

Webフィルタリング	Palo Alto PAシリーズ	パロアルトネットワークス
	i-Filter	デジタルアーツ
	Cisco WSA	Cisco
次世代ファイアウォール	Palo Alto PAシリーズ	パロアルトネットワークス
	フォーティゲート	FORTINET

ウイルス対策

ウイルス漏出防止	iNetSec	富士通
不正な外部通信の検知	Palo Alto PAシリーズ	パロアルトネットワークス
不正アクセス対策	InterScan Web Security as a Service™	トレンドマイクロ

内部対策

組織のセキュリティポリシーに沿って不適切な行為を制限することによる機密情報を守る対策です。不正アクセスを早期発見させ、機密情報の漏洩を未然に防ぎます。

ポリシー運用

標的型攻撃対策	Palo Alto PAシリーズ	パロアルトネットワークス
	フォーティゲート	FORTINET
	Deep Security	トレンドマイクロ
ネットワーク暗号ルータ	IPアクセスルータ Si-Rシリーズ	富士通
	フォーティゲート	FORTINET
IT資産管理	SKYSEA Client View	Sky
	Systemwalker Desktop Patrol	富士通
内部不正対策	Lanscope CAT	エムオーテックス

運用管理

ID統合管理	LDAPManager	富士通
データ消去	HDD破砕	扶桑電通

ウイルス対策

エンドポイントウイルス対策	ESET Endpoint Protection	ESET
	TrendMicro Apex One™	トレンドマイクロ
ネットワークウイルス対策	iNetSec シリーズ	富士通

データ保護

保存データ暗号化	AssetView	ハンモック
働き方・テレワーク	Soliton SecureAccess	ソリトンシステムズ

不正アクセス検知

不正侵入検知・遮断	iNetSec SF	富士通
	TiFRONT	日本ダイレックス
ネットワーク接続認証	NetAttest LAP	ソリトンシステムズ

有効性の確認

セキュリティの有効性を見える化する対策です。各種のセキュリティ対策診断やログ管理などを通じて、セキュリティの脆弱性や情報漏洩のリスクを早期発見、対策をサポートします。

セキュリティ診断

サイバーセキュリティ対策	ペネトレーションテスト	扶桑電通
Webセキュリティ診断	アプリケーション診断	扶桑電通
総合リスク診断クラウド	security-risk,jp	ソリトンシステムズ

教育・コンサルティング

セキュリティトレーニング	CYBERGYM	扶桑電通
セキュリティコンサルティング	セキュリティレベル現状調査	GSX
セキュリティ体制構築	CSIRT構築・運用を支援	ソリトンシステムズ

ログ解析・監査

高速ログ分析	Soliton NK	ソリトンシステムズ
ログ管理・IT資産管理	OnDemand シリーズ	ソリトンシステムズ

不正アクセス監視

不正ファイル解析・検知(仮想環境構築)	Deep Discovery Analyzer	トレンドマイクロ
標的型攻撃・ゼロデイ攻撃対策	Deep Discovery Inspector	トレンドマイクロ

IoTセキュリティ

サイバー攻撃対策(デバイス)	Trend Micro IoT Security	トレンドマイクロ
標的型攻撃対策	DeepDiscovery Inspector	トレンドマイクロ
IoT機器対策	IoTセキュリティ診断サービス	ソリトンシステムズ


ICTコンビニサービス