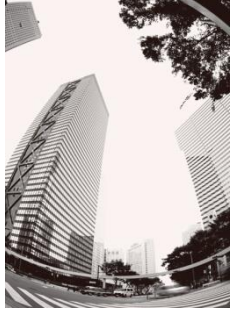




GSX
GLOBAL SECURITY EXPERTS

PCIDSSセキュリティフォーラム　2013
～PCIDSSへの効率的な対策を探る～

セキュリティインシデントからビジネスを守る

～セキュリティインシデントの教訓を踏まえた効果的なセキュリティ対策とは～

2013年7月10日

日本カード情報セキュリティ協議会（JCDSC）

グローバルセキュリティエキスパート株式会社

代表取締役　相原　秀明

GSXのご紹介

社　名	**グローバルセキュリティエキスパート株式会社（GSX）**		
設　立	**2000年4月**	資本金	**2億7000万円**
事業所	**東京本社　東京都港区西新橋1-2-9　日比谷セントラルビル21F**		

1997.10	株式会社ギャブコンサルティングにて、タイガーチームサービス（侵入検査/模擬攻撃検査）の提供開始
2000.04	グローバルセキュリティエキスパート株式会社設立（ギャブコンサルティングより営業譲渡）
2001.04	Webアプリケーション検査サービスの提供開始 個人情報保護基本法（現 保護法）に関するコンサルティングサービスの提供開始
2002.10	英国規格協会よりアソシエイトコンサルタント会社として認定される ISMS認証取得支援コンサルティングサービスの提供開始
2002.11	本社事業所がBS7799/ISMSを取得、タイガーチームサービスも ISO9001 を取得
2005.12	情報セキュリティコンサルティング会社で最初の ISO27001 を取得
2006.01	内部統制（日本版SOX法）コンサルティングサービスの提供開始
2006.07	デザイン＆インテグレーション・システム診断サービスの提供開始
2010.10	クラウドシステム検査の提供開始
2011.04	クラウドセキュリティ監査サービスの提供開始
2011.07	GSXスマートフォンセキュリティスイートの提供開始
2011.12	APT（標的型）攻撃耐性評価の提供開始
2012.07	スマートデバイス安心導入運用サービスを提供開始
2012.11	標的型メール訓練サービスの提供開始
2012.11	EAGLE TEAM SERVICE の提供開始
2013.01	アドバンステクノロジーサービスを新設

情報セキュリティコンサルタント会社
国内最初の ISO27001 取得
（*2005*年*12*月）

タイガーチームサービス
ISO9001取得
（*2002*年*11*月）

イーグルチームサービス
（*2012*年*11*月提供開始）

GSXのビジネス・ドメイン

▼　GSXでは、情報セキュリティのノウハウに基づいたサービスをご用意しています。

危機の時代にも強い情報セキュリティ

- 標的型メール訓練サービス
- APT(標的型)攻撃対策セキュリティスイート
- 次世代ファイアウォール
- イーグルチームサービス
- 情報セキュリティレベル診断
  - ・タイガーチームサービス
  - ・レベル診断サービス
- 情報セキュリティ対策可視化
- 技術対策支援
- セキュリティ事故対応
- セキュリティ監査
- セキュリティ教育
- 統合ID管理システム構築支援
- 統合ログ管理システム構築支援
- 各種認定取得（ISMS、Pマーク、PCIDSS）
- セキュリティ業務アウトソーシング　など

情報システムに係わるマネジメント力をレベルアップさせる

- 情報システムリスク評価支援
- ITSMS、ITガバナンスアセスメント
- 情報システムリスクソリューション
  - ・アクセス管理
  - ・変更管理
  - ・ネットワークセキュリティ　など
- ITマネジメント向上支援
- システム監査
- 各種認証取得（ISO20000、9001、FISC　他）
- スマートデバイス安心導入・運用サービス

など

リスクマネジメントが堅牢な企業を創出する

- 統合リスク管理（ERM）診断／構築支援
- BCMS診断／構築支援
- 内部統制構築支援
- 受託会社の内部統制[86号監査(旧18号監査）]対応
- ISO22301認証取得支援
- BCM(事業継続管理)教育、BCMS整備支援
- 各種認証取得（ISO14001、10002　他）など

サイバー攻撃とは

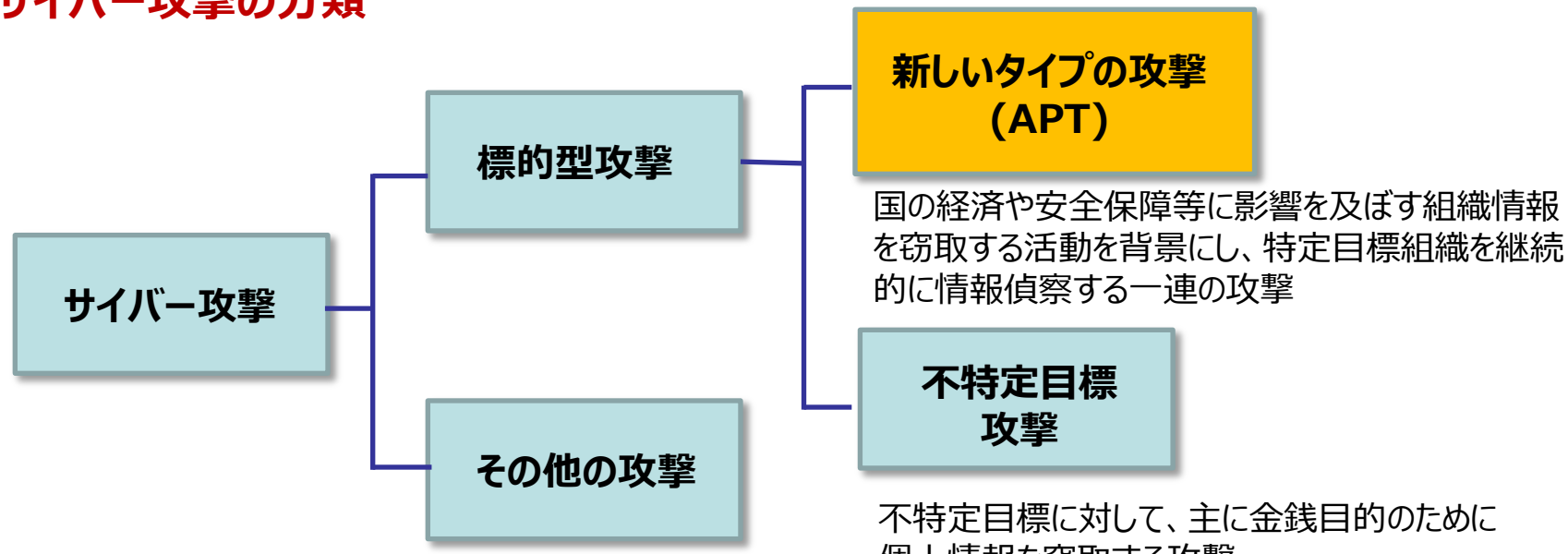
サイバー攻撃とは

サイバー空間を経由して、サイバー空間の企業利用を標的として行われる攻撃。
下記のような目的で行われる。
・コンピュータ環境/インフラストラクチャーの混乱、機能停止、破壊および悪意のある制御
・コンピュータ上に格納されている情報の改ざんおよび窃取

米国NISTにおける定義

サイバー攻撃の分類

APT: Advanced Persistent Thread



国の経済や安全保障等に影響を及ぼす組織情報を窃取する活動を背景にし、特定目標組織を継続的に情報偵察する一連の攻撃

不特定目標に対して、主に金銭目的のために個人情報を窃取する攻撃

DDos攻撃、ホームページ改ざん等

サイバー攻撃の変遷と組織への影響

サイバー攻撃は日々、変遷している。

2000年頃からの攻撃の特徴：
攻撃しやすい公開されている
サーバ等を狙った攻撃

- WHO：単独の攻撃者（スクリプトキディ、クラッカー）、愉快犯
- WHY：いたずら、自己顕示
- WHAT：Webサイト改竄等
- HOW：**大量無差別攻撃**

2005年頃からの攻撃の特徴：
特定組織の公開サーバ等を
狙ったより高度な攻撃

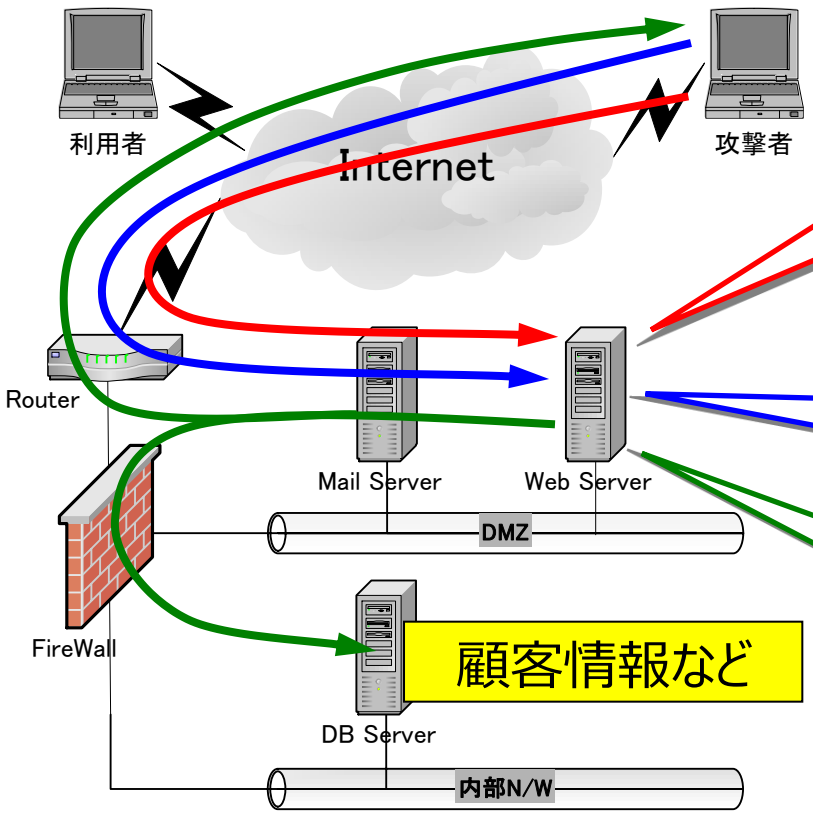
- WHO：組織化された攻撃者
- WHY：金銭目的
- WHAT：Webサイトからの情報搾取（クレジットカード情報）等
- HOW：**標的型攻撃**

2010年頃からの攻撃の特徴：
攻撃の難しい非公開の内部
サーバ等を狙った攻撃

- WHO：犯罪組織（w/潤沢な資金）
- WHY：金銭目的
- WHAT：内部サーバからの情報搾取（知財や軍事・政治上の機密情報）等
- HOW：**新しいタイプの攻撃（ＡＰＴ）**

攻撃のタイプが進化するにつれて漏洩する情報の価値が高まり、賠償金額など、補償も高額となってきている。

一般的（古典的）な攻撃の流れ



①情報収集フェーズ

Webアプリケーションの動作を確認し、セッション情報（※）等を収集する

②侵入フェーズ

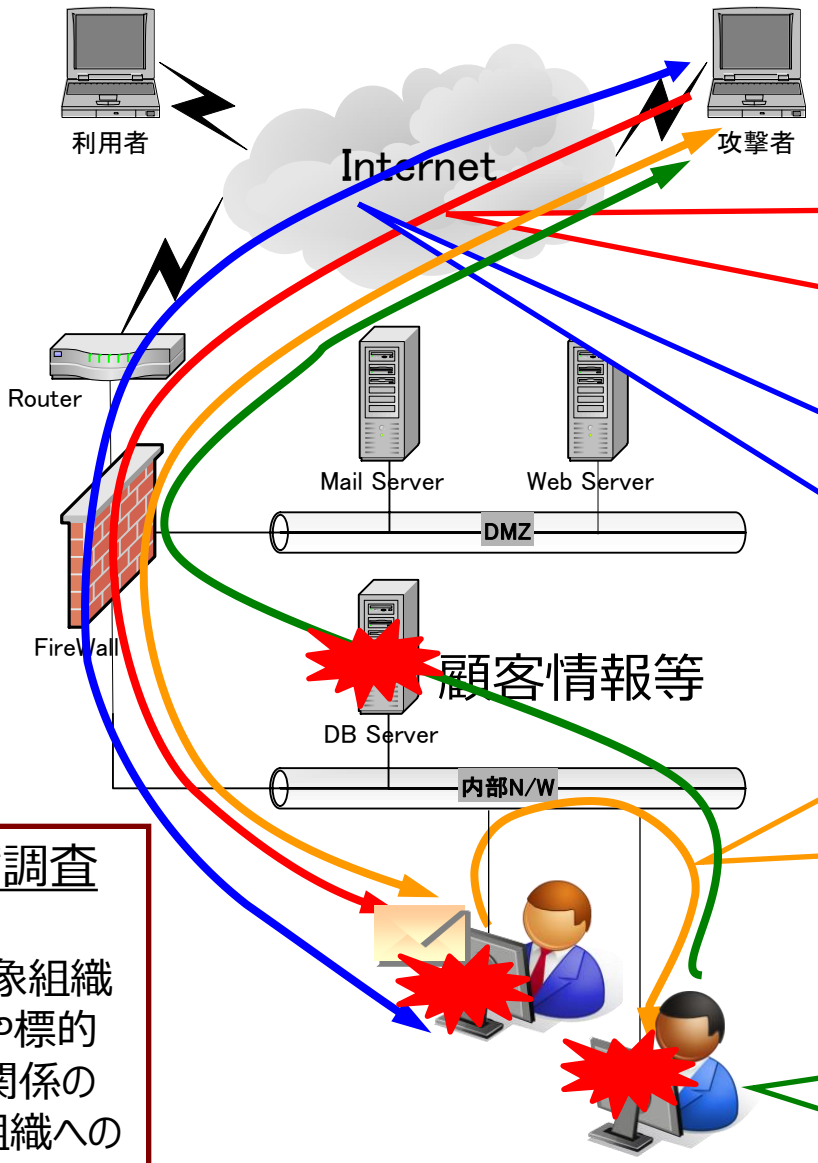
上記①の情報を基に侵入（攻撃）を試みる

③目的遂行フェーズ

情報の取得、情報の改ざん、不正プログラムの設置等

※Webサーバに接続しているユーザの状態を管理する為の情報

新しいタイプの攻撃の流れ



①予備調査段階
攻撃対象組織の調査や標的組織に関係のある別組織への攻撃実施

②初期潜入段階
組織内の特定ユーザに対して関係者を装ったメールを送る（標的型メール攻撃）。添付ファイルを開くことで、ファイルに仕込まれたマルウエアに感染する。

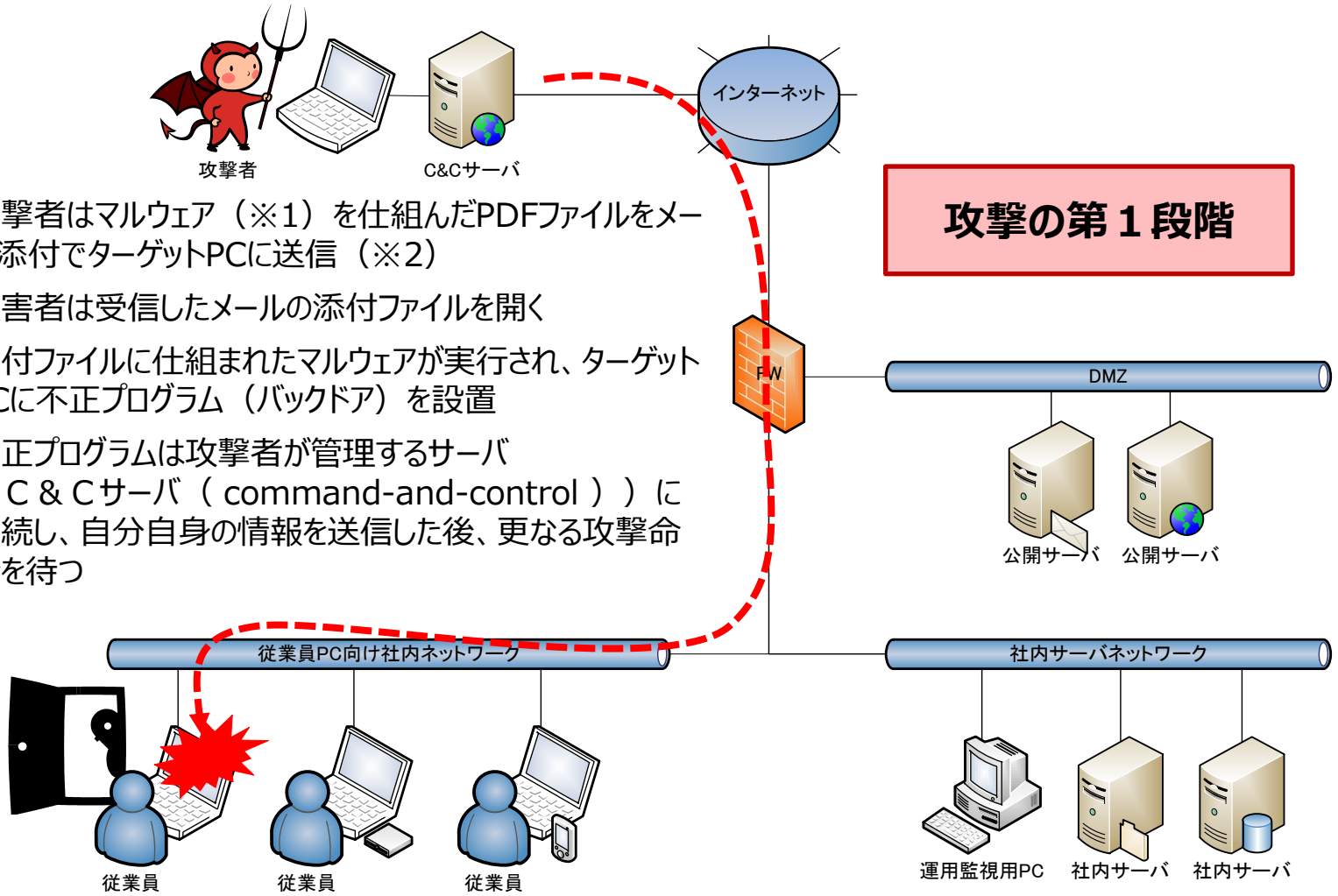
③攻撃基盤構築段階
マルウエアが更なるマルウエアをダウンロードすることでバックドアとなり、外部との通信経路を確立する。
攻撃者はリモートからターゲットをコントロールできる状態となる。

④システム調査／内部侵害段階
内部システムから情報を探す。潜伏期間は数週間から数ヶ月。組織に合わせたマルウエアの更新や上位の特権を段階的に取得する。

⑤攻撃最終目的遂行段階
情報の取得及び攻撃者への送付、情報の改ざんまたは不正プログラムの設置等

新しいタイプの攻撃事例（シナリオ①）

今回の事件に至る可能性があると推測されるシナリオは以下の通り。

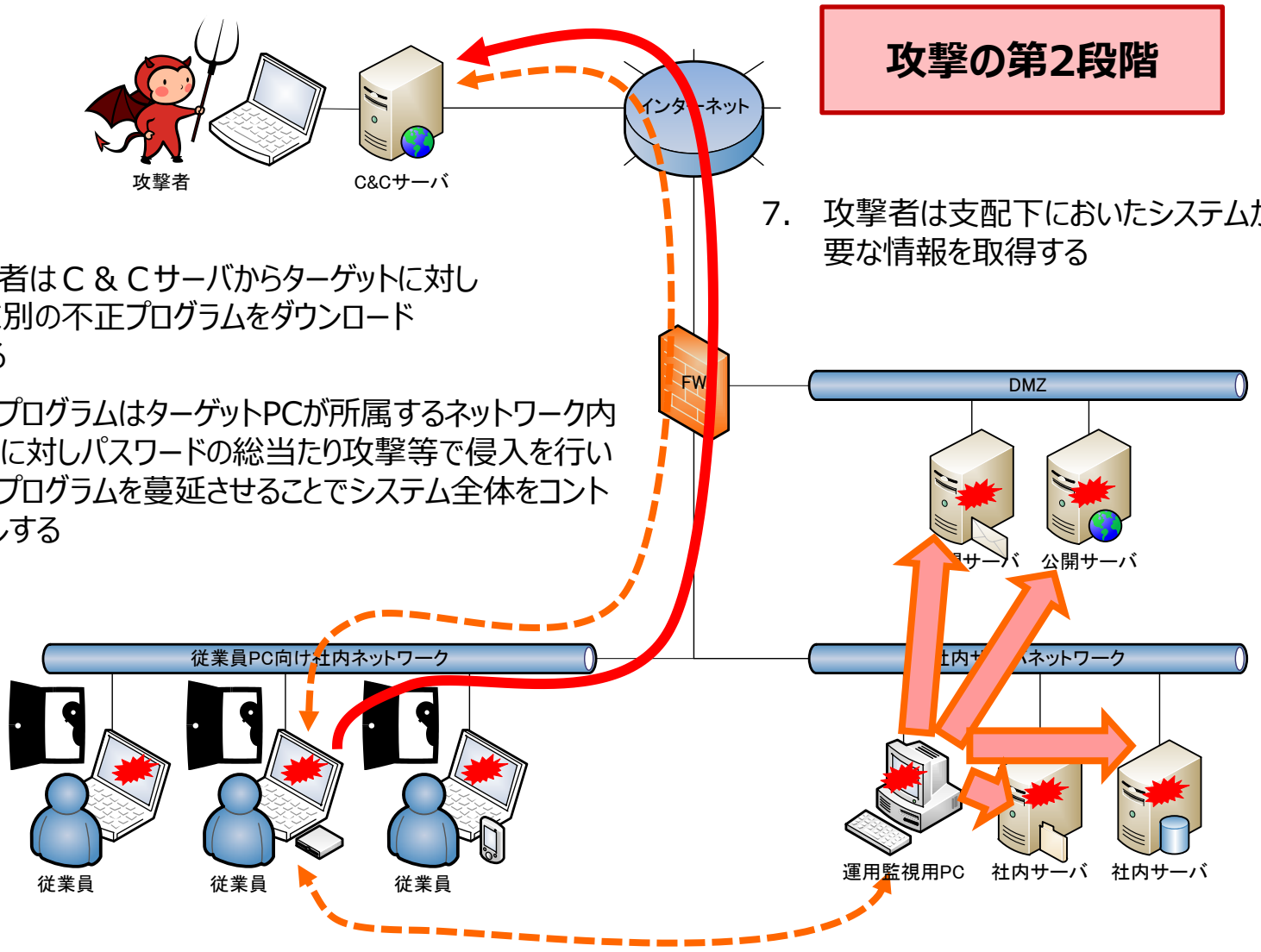


攻撃の第１段階

1. 攻撃者はマルウェア（※1）を仕組んだPDFファイルをメール添付でターゲットPCに送信（※2）
2. 被害者は受信したメールの添付ファイルを開く
3. 添付ファイルに仕組まれたマルウェアが実行され、ターゲットPCに不正プログラム（バックドア）を設置
4. 不正プログラムは攻撃者が管理するサーバ（Ｃ＆Ｃサーバ（ command-and-control ））に接続し、自分自身の情報を送信した後、更なる攻撃命令を待つ

※1：不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアの総称。
※2：フィッシングサイトへのアクセス、内部犯行によるウイルス持込み（USB経由）の可能性も考えられます。

新しいタイプの攻撃事例（シナリオ②）



攻撃の第2段階

5. 攻撃者はＣ＆Ｃサーバからターゲットに対しさらに別の不正プログラムをダウンロードさせる

6. 不正プログラムはターゲットPCが所属するネットワーク内のPCに対しパスワードの総当たり攻撃等で侵入を行い不正プログラムを蔓延させることでシステム全体をコントロールする

7. 攻撃者は支配下においたシステムから必要な情報を取得する

新しいタイプの攻撃事例（得られた教訓）

事件の発端は、マルウェアが添付ファイルとして仕込まれたメールを社員が開いたことから始まった

- PCのアンチウィルスソフトでマルウエアを検知できなかった。
- 社員に対するセキュリティ意識の啓発活動が必要。

攻撃者が営利目的の為に必要とする情報を持つ特定の企業に対して継続的かつ執拗に行われた攻撃

- 従来通りのセキュリティ予防対策だけでは防ぎきれない可能性を示唆。
- 点検に関しても従来のようなシステム監査や脆弱性診断を単発的に組み合せるだけでは不十分。

まとめ

- 新しいタイプの攻撃は、年々増加しており被害も大きくなっている。
- 新しいタイプの攻撃は、今までのアンチウイルスソフトやファイアウオールでは防げない。
  → **新しい防御対策が必要**
- 社員が標的、社員一人一人のセキュリティ意識が大切
  → **社員への新たなセキュリティ教育が必要**

具体的な対策3つのポイントとは？

ＧＳＸが考える具体的な対策ポイントとして、以下の３つを推奨しています。

1 【 現状調査 】

自組織内にマルウェア感染があるのか、もしくは実際にマルウェアが侵入した場合の耐性を把握する。

- **Bot感染調査**
- **Botシミュレーション…**

2 【 入口対策 】

マルウェア感染そのものを防ぐ、あるいは感染リスクを低減するための対策。

- **標的型メール訓練**
- **IDS/IPS**
- **ペネトレーションテスト**
- **Webアプリケーションファイアウォール**
- **…**

3 【 出口対策 】

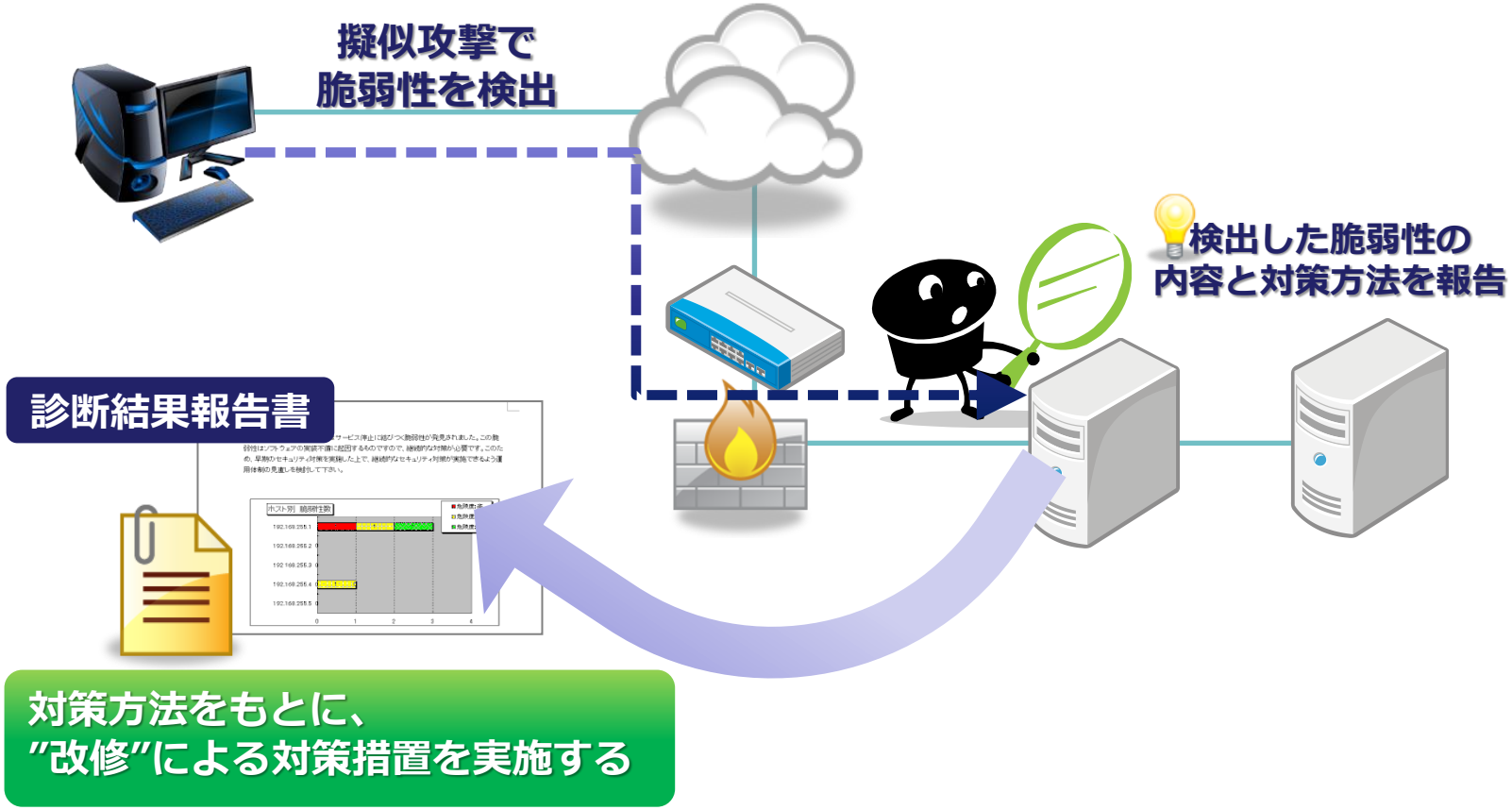
マルウェアに感染してしまった場合でも、その通信(≒情報流出)を水際で防ぐための対策。

- **次世代ファイアウォール(NGFW)**
- **標的型攻撃対策　専用機器…**

高度化、そして増加し続ける、標的型攻撃への対策は、
上記のポイントを踏まえながら、複合的・多層的な対策が重要！！

ペネトレーションテスト（脆弱性診断サービス）とは？

ネットワークシステム/Webアプリケーションに対して、擬似攻撃を実施し、その脆弱性を検出、その対策方法をご報告するサービス



TIGER TEAM SERVICE とは？

GSX専門エンジニアが実施する、高度な脆弱性診断サービス
(専門エンジニアが手動オペレーションで診断します)

TIGER TEAM SERVICEの歴史

1997年～　システム監査の一環として、脆弱性診断サービスを開始
(**「タイガーチーム」として商標登録**)

2001年　Webアプリケーション脆弱性診断サービスを開始

2002年　ISO9001(QMS)を認証取得

ネットワークおよびIT技術の変遷に伴い、
常にサービスメニューを拡張

IP V6対応 プラットフォーム診断(ペネトレーションテスト)
クラウドシステム向けの脆弱性診断
スマートフォン端末向け脆弱性診断
スマートフォン向けWEBサイト/API向け脆弱性診断　など

TIGER TEAM SERVICE メニュー

豊富な診断メニューの中から、ご要望に応じたセキュリティ診断サービスをご提供しています。
(どんな診断が必要かどうか、ご相談/ご提案に応じています)

◆プラットフォーム診断

サーバOSやサービスパックの脆弱性
各種サービスプログラムの脆弱性
アカウント・パスワードの脆弱性
サーバ設定に関する脆弱性
＊ サーバ外部より診断します

◆Webアプリケーション診断

Webプログラミングの脆弱性

最も基本的な診断メニュー

◆データベース診断

セキュリティパッチの脆弱性
アカウント・パスワードの脆弱性
ロールベースアクセスの脆弱性
運用上の脆弱性

◆サーバ設定診断

サーバOSやサービスプログラムの脆弱性
アカウント管理、ログ管理の脆弱性
＊ サーバにログオンして診断します

◆ファイアーウォール設定診断

アクセスポリシーの脆弱性
管理機能の脆弱性
アクセスポリシーの妥当性

◆無線LAN診断

無許可アクセスポイントの探索
暗号化強度の解析

◆パスワード解析

パスワード強度の解析
＊ パスワードファイルを入手し解析にかけます

◆クラウド(仮想化)システム診断

ゲストOSの脆弱性
仮想マシン間での脆弱性
ハイパーバイザーの脆弱性

◆スマートフォン向けセキュリティ診断

スマートフォン向けWEBサイト/API診断

スマートフォン端末のセキュリティ診断

TIGER TEAM SERVICE の特長

1 高レベルの脆弱性診断サービスを実現

GSXの専門エンジニアが手動オペレーションによる診断を実施します。診断ツールやASPサービス等の診断手法では実現できない、高レベルの診断(網羅性と検出精度が高い*)をご提供します。

【網羅性】診断項目に抜けやモレがないこと
【検出精度】未検出(検出すべき脆弱性を検出できない)と、誤検出(脆弱性ではないものを誤って検出)

2 診断時の安全性を最大限に優先

診断が原因でサーバ等に影響を与え、サービス停止や業務の中断などが発生しない様、安全性を充分に考慮した診断手法と最大限の人的注意を払いながら診断を実施しています。

3 認証規格に裏付けられた品質(QMS & ISMS)

品質の認証規格であるQMSをベースとしたスキームを構築することで、個々のエンジニアの力量に依存せず、チームとして常に高品質の診断をご提供することが出来ます。
また同時に情報セキュリティ管理に関するISMSついても認証を取得しています。診断対象情報や診断結果の管理についても厳重なセキュリティ管理を実施しています。

プラットフォーム診断について

二重診断による高精度な診断

専門コンサルタントによる手動オペレーション診断および商用診断ツールによる診断をそれぞれ実施し、非常に高い診断精度を実現しています。 手動オペレーションでは、複数の脆弱性を組合わせた攻撃など、診断ツールと比較して、実際のハッカーの攻撃手法に近い視点による高度な診断を実施します。

ブラックボックス方式

実際のハッカーと同じ視点でブラックスボックス方式のテストを実施します。(対象がサーバもしくはルータ・FWなどのネットワーク機器のいずれであっても、IPアドレスをご指定頂くだけで診断が可能です。)

安全性への配慮

充分なインターバルをとった作業、目視での異常検知と負荷調整などにより、診断時の障害発生について、最大限に配慮した診断を実施します。

診断項目

主に以下の項目を情報収集、診断致します。(約5000項目) ※DoS診断についてオプションにて実施可能です。

OSの脆弱性チェック	バックドアのチェック	推測可能なパスワードのチェック
ミドルウェアの脆弱性チェック	ウイルス感染チェック	通信の盗聴可否のチェック(暗号化)
アプリケーションの脆弱性チェック	バックドアのチェック	第三者中継(SPAM)のチェック
データベースの脆弱性チェック	証明書の有効性チェック	サンプルスクリプトの有無のチェック

Webアプリケーション診断について

手動オペレーションによる高度な診断

専門コンサルタントによる手動オペレーション診断で高度な診断を実施します。 (プラットフォーム診断と比較すると、手動オペレーションと商用診断ツールの精度/網羅性に大きく乖離があることから、手動オペレーションを基本としています。)

※ただしお客様のご希望や、内容・状況により、診断ツールを併用した診断についても対応可能です。

安全性への考慮

充分なインターバルをとった作業、目視での異常検知と負荷調整、システムへの影響を考慮した診断により、診断に起因する障害発生について、最大限に配慮します。

診断項目　右記(ツール及びWAFとの対比含む)

手動オペレーションによる診断は網羅性と検出精度がもっとも高く、診断結果に基づいたソースコード改修を実施できればもっとも高いセキュリティレベルを実現できます。

※右記の診断項目で、3種とも"○"の項目であっても、検出精度自体は手動オペレーションによる診断が最も高いと言えます。
(例：右記で3種とも"○"となっているクロスサイトスクリプティング等)

	手動	診断ツール	WAF
セッション管理の不備	○	×	×
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	○	○	△
クロスサイトスクリプティング	○	○	○
SQLインジェクション	○	○	○
OSコマンドインジェクション	○	○	○
ディレクトリトラバーサル	○	○	○
XMLインジェクション	○	○	○
SSIインジェクション	○	○	○
XPathインジェクション	○	○	○
XQueryインジェクション	○	○	○
LDAPインジェクション	○	○	○
MXインジェクション	○	○	○
HTTPレスポンス分割	○	○	○
リモートファイルインクルード	○	×	△
通信の暗号化	○	○	○
証明書の不備	○	○	△
Refererによる情報漏洩	○	○	△
ユーザID等の調査	○	×	×
詳細なエラーメッセージ	○	×	×
拡張子偽装	○	×	×
コメント・デバッグ情報	○	○	×
アプリケーション固有の問題	○	×	×
フォーマットストリング	○	○	×
バッファオーバーフロー	○	○	△
DNSリバインディング(ガラケー固有)	○	×	△

TIGER TEAM SERVICE 実施ステップ

主な脆弱性診断サービスの流れとなります。ご要望に応じて、各種特別対応を行うことも可能です。

事前調整 & 内容確認書作成	診断	速報	結果分析/報告書作成	報告会	*脆弱性検出箇所の改修確認
診断期間や対象などを決定。内容を確認書として作成します。	営業時間の平日10:00～17:00で診断します。 ご要望に応じ、夜間・深夜・休日などにもオプション対応が可能です。	診断中に緊急度の高い脆弱性が発見された場合、速報としてご連絡します。	診断結果を、“報告書”として取りまとめます。	専門エンジニアが内容をご説明する報告会を開催します。	脆弱性が検出された場合のオプションとして、検出された脆弱性の改修チェックを行います。

報告書及び診断内容確認書の記載内容

診断内容確認書

①診断の概要
-診断対象、診断日程、診断環境、
診断手法　等
②連絡先
(診断開始/終了連絡、緊急連絡)
-GSX側 診断技術者の連絡先情報
-お客様側 窓口担当者の連絡先情報

◆ お客様情報

総合窓口（■検査連絡窓口）	所属			
	ご担当者名			
	住所			
	電話番号		FAX 番号	
	E-mail			
技術担当者（■検査連絡窓口）	所属			
	ご担当者名			
	住所			
	電話番号		FAX 番号	
	E-mail			
技術担当者（■検査連絡窓口）	所属			
	ご担当者名			
	住所			
	電話番号		FAX 番号	
	E-mail			

◆ グローバルセキュリティエキスパート側

総合窓口	所属	事業開発部		
	担当者名	船橋　良輔		
	電話番号	03-3457-1900	FAX 番号	03-3457-6565
	E-mail	rfunabashi@glbex.com		
技術担当者	所属	タイガーチームサービス事業部		
	担当者名	XXXX		
	電話番号	03-3457-1900	FAX 番号	03-3457-6565
	E-mail	XXXX@glbex.com		

◆ 検査対象台数及び検査日程

検査		検査内容	数量	日程
■	I	インターネット経由の検査(侵入検査)	2 台	
□		インターネット経由の検査(DoS 検査)	台	
□	II	内部ネットワーク経由の検査（侵入検査）	台	
□		内部ネットワーク経由の検査（DoS 検査）	台	
□	III	RAS への侵入検査	回線	
□	IV	モデム探査	回線	
■	V	Web システム検査	XXX パラメータ	2012 年 XX 月 XX 日 -XX 日
		Web システム検査 for スマートフォン		10:00 - 17:00
□	VI	パスワード強度検査	アカウント	
□	VII	データベース検査	インスタンス	

◆検査情報（V） － Web システム検査

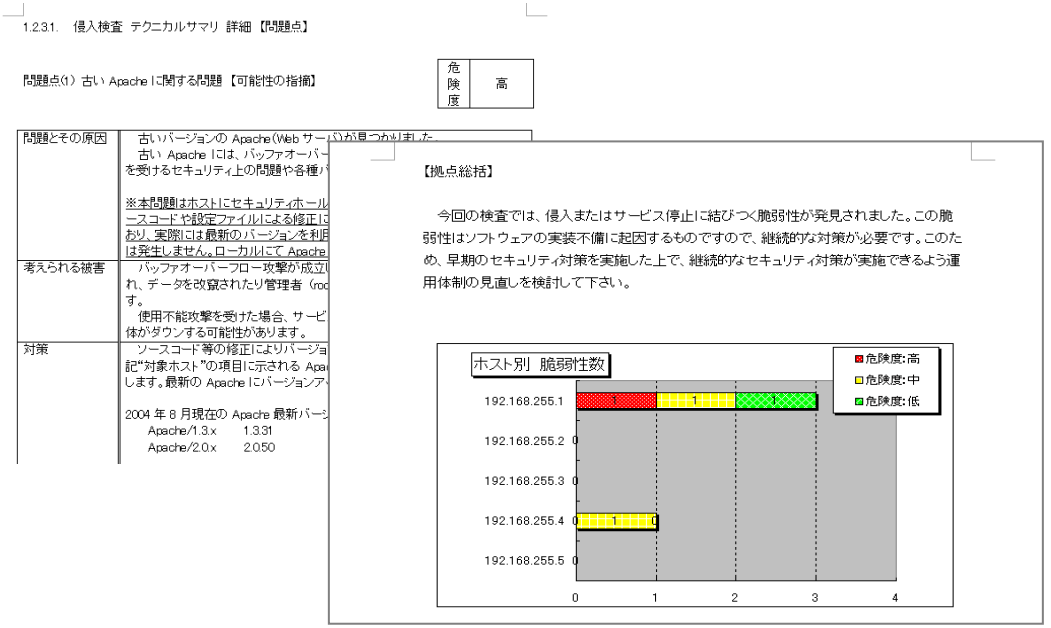
No.	名称	対象 URL	備考
1		http://XXXXXXXXXXXX	
	合計	X サイト	

◆ 特記事項

・検査日の検査開始前及び終了時に、検査担当者より開始及び終了のご連絡を致します。
・検査では、「tiger.team.service」で始まるアカウント名の「gmail.com」ドメインのメールアドレスを登録します。検査終了後に当該アカウントによる登録データを削除していただくようお願い致します。
⇒例：tiger.team.service.dcm1@gmail.com, tiger.team.service.dcm2@gmail.com 等
・複数回のログイン失敗によりアカウントをロックアウトする仕様の場合、事前にご連絡下さい。

診断結果報告書書

①診断の概要
-診断目的、診断対象、診断日程
診断環境、診断手法
②診断結果総評
③指摘事項
-危険度評価
「高」、「中」、「低」の三段階表示
-問題点とその原因（詳細記述）
脅威の内容、緊急性
-考えられる被害、対策、関連情報、リスク、
対策
-診断対象サーバ毎の事象のまとめ　等



1.2.3.1.　侵入検査 テクニカルサマリ 詳細 【問題点】

問題点(1) 古い Apache に関する問題 【可能性の指摘】

危険度	高

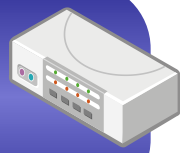
問題とその原因	古いバージョンの Apache(Web サーバ)が見つかりました。 古い Apache には、バッファオーバー を受けるセキュリティ上の問題や各種バ ※本問題はホストにセキュリティホール ースコードや設定ファイルによる修正に おり、実際には最新のバージョンを利用 は発生しません。ローカルにて Apache
考えられる被害	バッファオーバーフロー攻撃が成立 れ、データを改竄されたり管理者（roo す。 使用不能攻撃を受けた場合、サービ 体がダウンする可能性があります。
対策	ソースコード等の修正によりバージョ 記"対象ホスト"の項目に示される Apa します。最新の Apache にバージョンア 2004 年 8 月現在の Apache 最新バージ Apache/1.3.x　1.3.31 Apache/2.0.x　2.050

【拠点総括】

今回の検査では、侵入またはサービス停止に結び つく脆弱性が発見されました。この脆弱性はソフトウェアの実装不備に起因するものですので、継続的な対策が必要です。このため、早期のセキュリティ対策を実施した上で、継続的なセキュリティ対策が実施できるよう運用体制の見直しを検討して下さい。

WAFの位置づけ（外部公開サーバへの対策）

セキュリティアプライアンス



脆弱性診断＆改修

プラットフォーム

FW(ファイアウォール)

IPS(侵入防止装置)

プラットフォーム脆弱性診断と改修

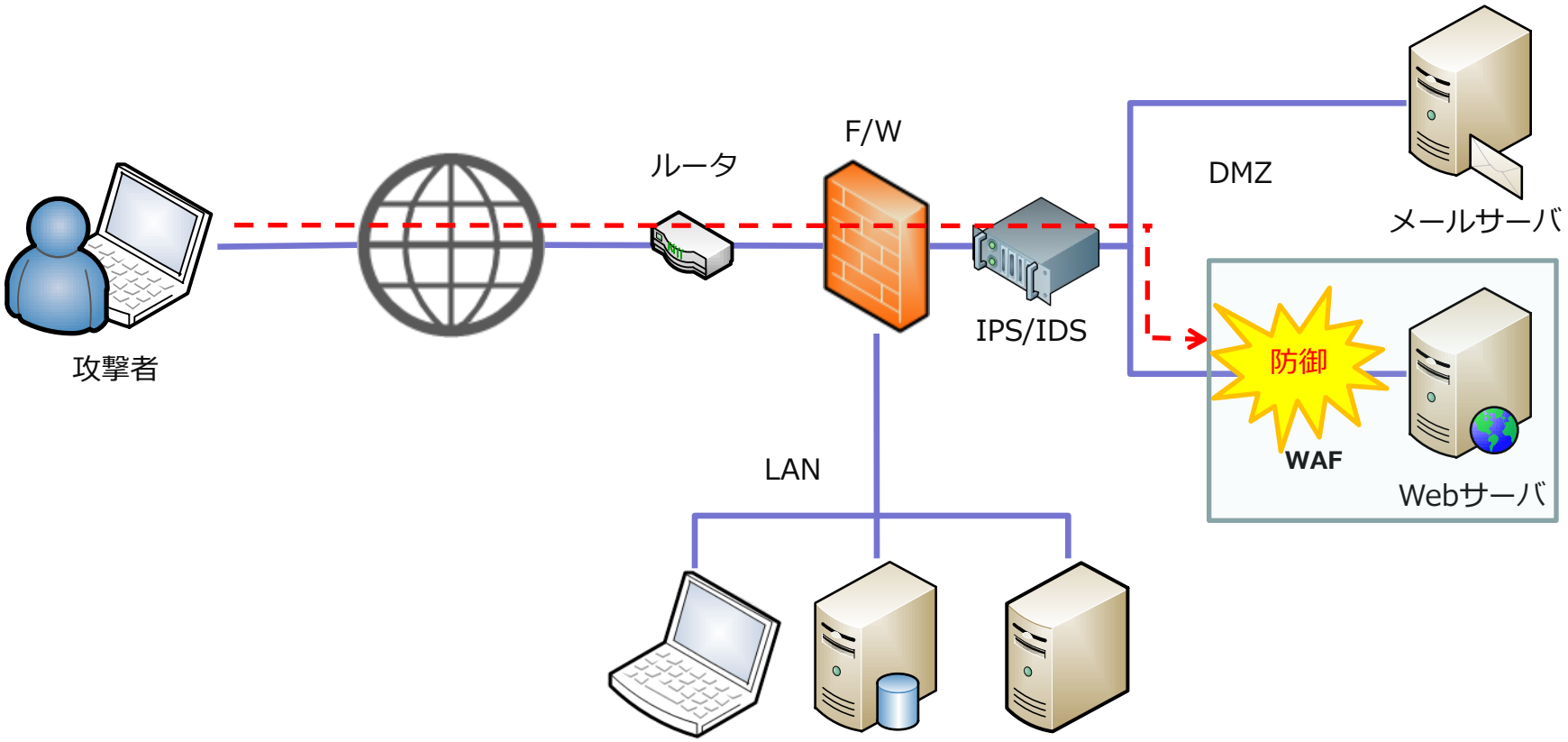
Webアプリケーション

WAF(Webアプリケーションファイアウォール)

Webアプリ脆弱性診断と改修

WAFとは？

WAF（Web Application Firewall）は、Webアプリケーションを介した不正アクセスを防ぐための専用ハードウェア(またはソフトウェア）です。WAFはWebアプリケーションの通信内容を取得・管理することで不正アクセスを防御することが可能です。



WAFが必要とされる背景①

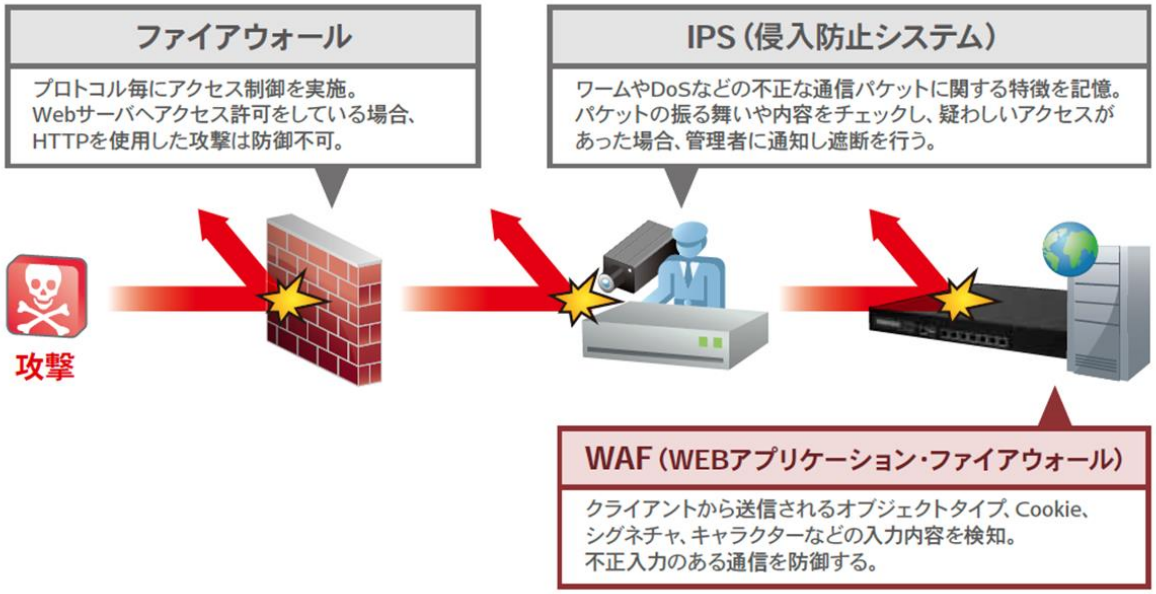
Webアプリケーションの脆弱性を悪用した攻撃は増大し、巧妙さを増しています。

攻撃例

脆弱性	SQLインジェクション	クロスサイトスクリプティング
攻撃手法	Webサーバーが使用しているデータベースを外部から不正に操作し、データベースの内容を書き換え、意図しないデータをWebに表示させたりする。	動的にWebページを生成するアプリケーションに、悪意を持ったスクリプト(命令)を埋め込み、偽ページの表示などを可能にする。これにより偽ページにユーザがだまされて、個人情報などを攻撃者に送ってしまう。
リスク	• 個人情報の流出 • クレジットカードの流出 • 情報の改ざん・消去	• 個人情報の流出 • クレジットカードの流出 • Cookieデータの盗聴
被害	➢ 損害賠償 ➢ 社会的信用の失墜 ➢ 売上減 ➢ 巨額の復旧費	➢ 損害賠償 ➢ 社会的信用の失墜 ➢ 売上減 ➢ 巨額の復旧費

WAFが必要とされる背景②

既存のセキュリティ製品として認知されている、FW・IPS/IDSではWebアプリケーションに対する攻撃は防御できません。この為、安全なWebサイトの運用にWAFの導入が注目されています。

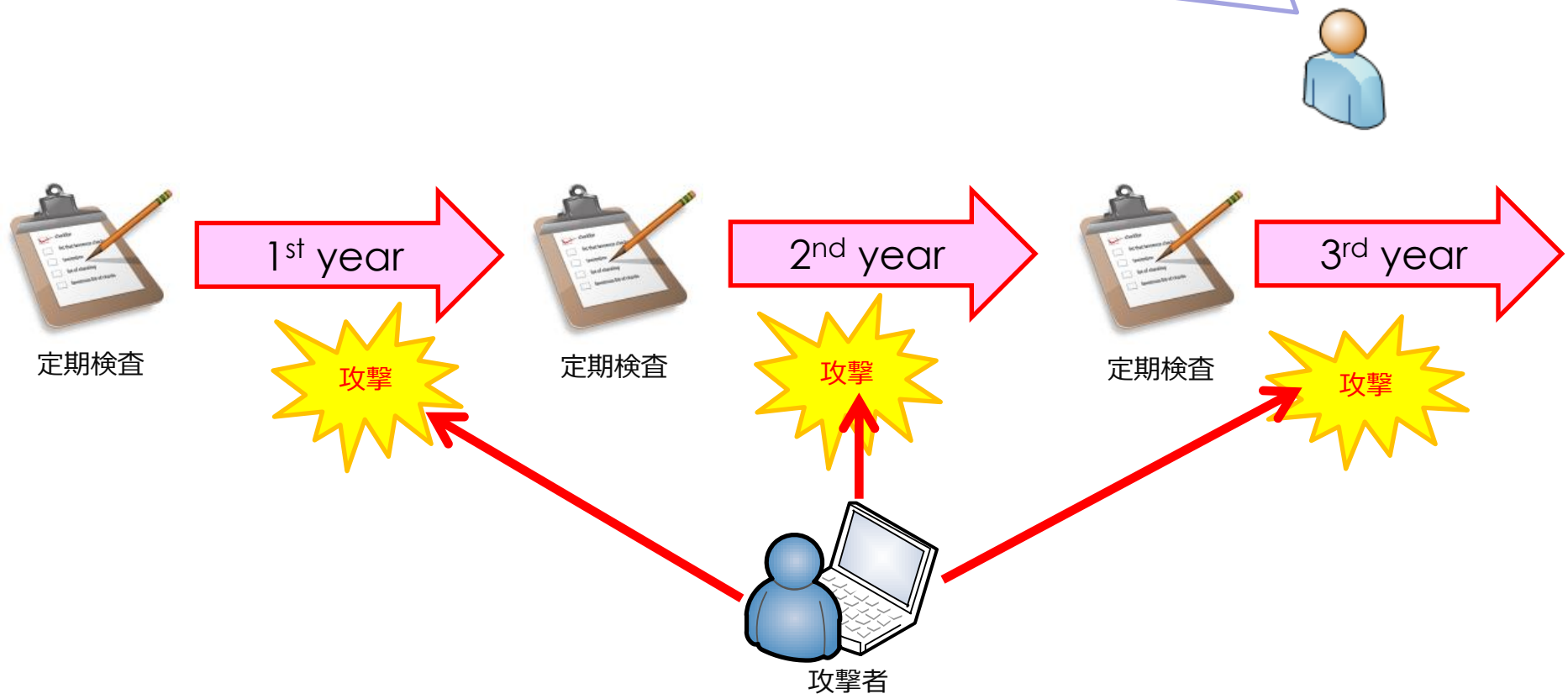


セキュリティ製品	防御・監視対象	防御・監視内容
FireWall	ネットワーク（TCP/IP）	IPアドレス、ポート番号によるアクセス制御
IPS, IDS	OS, ミドルウェア（DB, SMTP, DNS等）	不正な通信パケットの検知、遮断
WAF	Webアプリケーション	不正な入力内容を遮断

WAFが必要とされる背景③

タイガーチームサービス事業部へのご相談例から

毎年定期的な脆弱性検査を受けているが、検査終了時から次回の検査までの間に新種の攻撃を受けるリスクを低減する方法はないか・・・。



WAFが必要とされる背景④

タイガーチームサービス事業部へのご相談例から

脆弱性診断を受けて、多くの脆弱性が確認されたが、対策するためのコストが厳しい、せめてクリティカルな問題だけでも低コストで対処する方法はないだろうか・・・

危険度：高

SQLインジェクション
クロスサイトスクリプティング

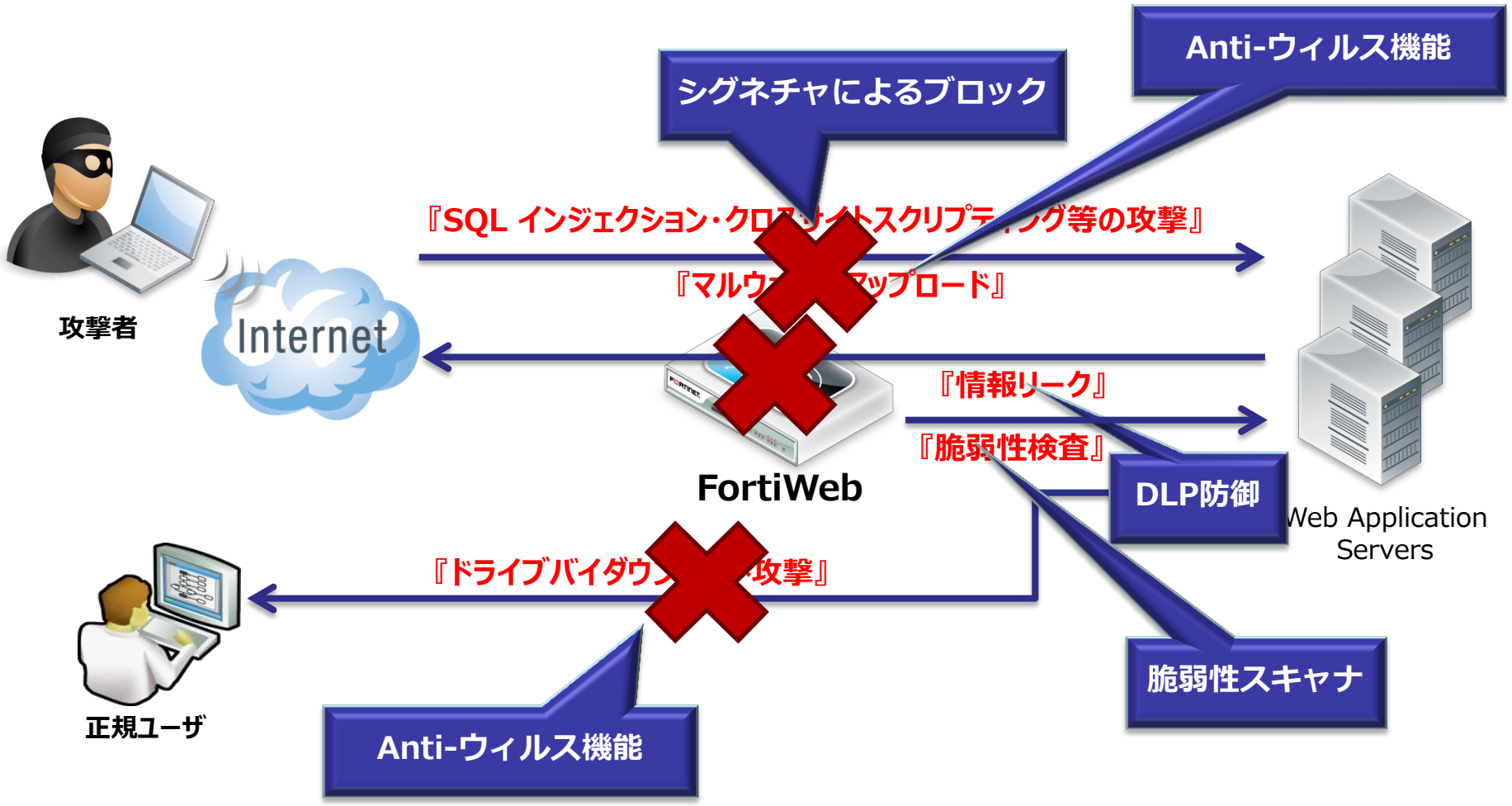
危険度：中

HTTP非暗号化
エラーメッセージ分析によるID推測

危険度：低

プログラムエラー情報の露出

Fortiweb の特長



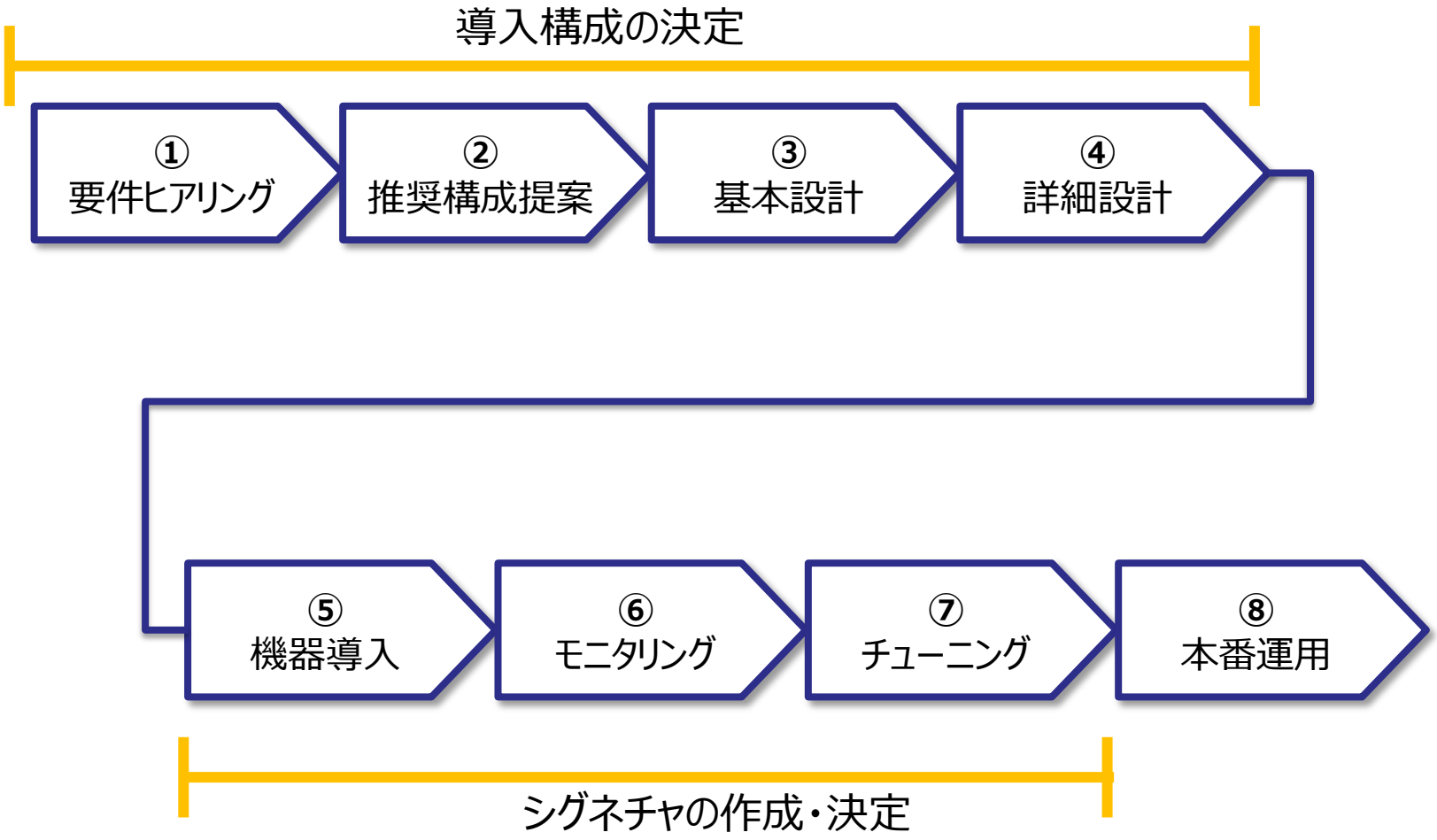
様々な攻撃からWebアプリケーションを保護

- 以下の攻撃からWebアプリケーションを守ります。

クロスサイト スクリプティング	アウトバウンドデータ漏洩	アクセス レート コントロール
SQLインジェクション	HTTPリクエスト スマグリング	スキーマ ポイズニング
セッション ハイジャック	リモートファイル インクルージョン	XMLパラメータ改変
Cookie改変/ポイズニング	エンコーディング攻撃	XML不正侵入防御
クロスサイト リクエスト	アクセス制御破壊	WSDLスキャン
フォージェリ（CSRF）	強制ブラウズ	再帰ペイロード
コマンド インジェクション	ディレクトリ トラバーサル	外部エンティティ攻撃
リモートファイル インクルージョン	サイト偵察	バッファオーバーフロー
形状改変	検索エンジン ハッキング	DoS
Hiddenフィールド操作	ブルートフォース ログイン	

WAF 導入イメージ

- 保護対象となるWebサイトやネットワーク環境の大きさにもよりますが、導入までおおよそ２ヶ月前後かかります。



グローバルセキュリティエキスパート株式会社

〒105-0003
東京都港区西新橋1-2-9　日比谷ｾﾝﾄﾗﾙﾋﾞﾙ21Ｆ
Tel　：03-3507-1360（代）
Fax　：03-3507-1361

URL　：http://www.gsx.co.jp

E-mail：tiger@gsx.co.jp