Web アプリケーションを突いた攻撃（専門的にはバッファーオーバーフロー、
SQL インジェクション、デレクトリートラバーサル、クロスサイトスクリプティングなど）

「DoS/DDoS 攻撃」は、防御の確実性を担保できないので、ここでは対象外。

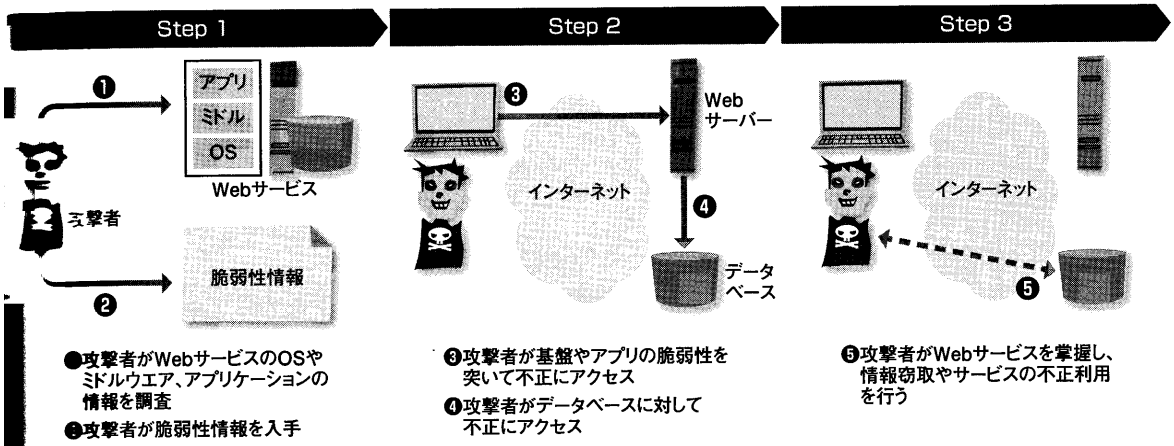

図5 Webサイトへの不正アクセスの流れ

Web サーバーからデータベースサーバーへのアクセスについては、データベースに接続可能な専用の API を使ったものだけを許可すべきでしたが、そうした設定になっていませんでした。本来ならば要件定義や設計時にデータへのアクセスルートを特定・整理し、その**アクセス制限（いつ、どのアカウントで、どの目的で、どうアクセスさせるか）**を決めて設定する必要がありました。

重要データへのアクセスの監視については、データベースで利用するプロトコルと実行するコマンドを監視するように設計する必要がありました。この企業では、通常利用するアカウントからの通信だけを監視していました。その結果、不正アクセスを見逃してしまいました。こうした「特殊だが重要な例外」の監視要件は、**後工程の設計では簡単に追加できません**。

セキュリティインシデント発生時の影響分析を行う際には**「CIA」**が重要な観点になります。CIA とは機密性（Confidential）、完全性（Integrity）、可用性（Availability）の頭文字を取った略称で、それぞれがセキュリティの構成要素となります。三つの観点でインシデント発生時の企業への影響を考え、どれだけの対応が必要かを導き出します。

機密性（C）の観点では「システムで利用・保管するデータが漏えいした場合にどういった影響があるか」を分析します。影響に応じて、データ漏えいを防ぐための施策を設計する必要があります。完全性（Ｉ）の観点では「システムのデータが破壊・改ざんされた場合の影響」を分析します。それに応じてデータが破壊

されたり、利用不可になったりした場合の施策を設計します。可用性（A）については「セキュリティインシデントでシステムが利用できなくなった場合に、どのユーザー、システムに影響するか」を分析します。サービス継続性をどれくらい維持する必要があるかを考慮して対策を設計しますo

米NIST（米国国立標準技術研究所）は、サイバーセキュリティ対策のコア要素は**「特定」「防御」「検知」「対応」「復旧」の五つ**で構成されると定義しています。これらの要素を総合的に実施することで、セキュリティリスクへの対策を戦略的に行えます。

しかし昨今は、マルウエア対策ソフトの定義ファイルやセキュリティパッチが更新される前にサイバー攻撃が行われる**「ゼロデイ攻撃」**、社員や協力会社が情報を盗み出す**「内部犯行」**といった様々な種類のインシデントが実際に起こっています。

次に、セキュリティ対策の構成を俯瞰的に見るための考え方を紹介します。重要なのが「レイヤー」を意識することです。レイヤーは、大きく**「アプリケーション」「ミドルウエア」「OS」「ネットワーク」の四つ**に分類されます。それぞれのレイヤーで**特定、防御、検知、対応、復旧**といった要素を意識して、セキュリティ対策を設計します。

表2 想定すべきサイバーセキュリティの脅威

ISO/IEC 27005:2008で挙げられた脆弱性の例からサイバー攻撃の脅威に関する項目を抽出し、八つの分類に整理した

脅威分類	想定される主な脅威
(1) システムの脆弱性を突く攻撃	• Webアプリケーションの脆弱性 • システム基盤の脆弱性 • ネットワーク基盤の脆弱性
(2) 不正アクセス	• サーバーおよびネットワークへの侵入 • 未承認の端末や媒体の不正接続 • DoS/DDoS攻撃 • ブルートフォース攻撃などによる特権昇格
(3) メール攻撃	• ウイルス付きメール攻撃 • URL付きメール攻撃
(4) マルウエア	• Webアクセス経由のマルウエア感染 • 記憶媒体経由のマルウエア感染
(5) 改ざん	• データやログの改ざん • プログラムの改ざん
(6) なりすまし	• アカウントの奪取
(7) 情報持ち出し	• メール経由での情報持ち出し • 正常な通信（HTTPSなど）による情報持ち出し
(8) 通信の盗聴	• ネットワークパケットの盗聴 • 攻撃者のサーバーによる端末通信の傍受

表4 セキュリティ対策の技術要件

要件定義時にこうしたセキュリティにかかわる要件を洗い出す

項目	詳細項目
標準構成	構成管理、変更管理など
アカウント管理	アカウント管理手法、申請、ポリシーの設定、発行・削除、モニタリング、棚卸しなど
アクセス制御	境界制御の実施、権限の割り当て、重要データの分離、モニタリング、棚卸しなど
マルウエア対策	アプリケーション制御、ネットワーク制御など
脆弱性管理	脆弱性診断、脆弱性管理実装、脆弱性情報の評価など
データ保護	データ保護実装、棚卸し、変更管理、モニタリングなど
ログ管理	時刻同期、モニタリング、保管・保護、監査など
バックアップ	バックアップの方針、バックアップの取得、保管・保護、テストの実施など

ブルートフォース（総当たり）

〜〜〜〜〜〜〜〜〜〜〜〜

Brute-force attack

ブルートフォース攻撃とは、暗号やパスワードを解読、解析するための手法のひとつである。 考えられる全ての暗号鍵を自動化されたプログラムによってひたすら入力し、復号化プログラムによって、暗号が意味のある文字列になるかどうかを試行錯誤しながら調べて行く方法。

〜〜〜〜〜〜〜〜〜〜〜〜

表3 抜け漏れを防ぐフレームワーク

要件定義		特定	防御	検知	対応	復旧
基本機能	アカウント管理	アカウント管理対象の特定	アカウント統制	アカウント監視	アカウント停止	アカウント復旧
	認証	認証対象の特定	認証	認証監視	認証の停止	認証の復旧
	アクセス制御	アクセス制御対象の特定	アクセス制御	アクセス監視	アクセスの遮断	アクセスの復旧
	データ保護	データ保護対象の特定	データ保護	データ改ざん・漏洩範囲の調査	データ改ざん・漏洩対処	データの復旧
	バックアップ	バックアップ対象の特定	バックアップ取得	バックアップ監視	バックアップ復元	システムの復旧
共通機能	標準構成	標準構成の特定	構成管理	構成監視	構成復元	標準構成の復旧
	脆弱性管理	脆弱性情報の特定	脆弱性管理	脆弱性診断・監視	脆弱性暫定対処	脆弱性監査・報告
	マルウエア対策	マルウエア情報の特定	マルウエア遮断	マルウエア監視	マルウエア駆除・封じ込め	マルウエア感染対象の復旧
	ログ管理	ログ管理対象の特定	ログ取得・保管	ログ監視	ログ調査・分析	ログ監査・報告

基本設計（アプリ）		特定	防御	検知	対応	復旧
基本機能	アカウント管理	アカウントの申請・登録	アカウントポリシー統制	アカウント棚卸・利用監視	アカウントの無効化	アカウントの有効化
	認証	認証方式・対象の定義	ID・端末・生体による認証	ログイン監視	ログインの無効化	ログインの有効化
	アクセス制御	役割の定義	役割によるアクセス制御	アクセス状況の監視	アクセス権限の無効化	アクセス権限の有効化
	データ保護	暗号化方式の定義	通信・処理の暗号化	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化
	バックアップ	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化
共通機能	標準構成	プログラム構成の把握	プログラム構成管理	プログラム構成監視	モジュールの復元	プログラム構成の復旧
	脆弱性管理	プログラムの脆弱性の把握	セキュアコーディング	アプリケーション診断	プログラム修正・パッチ適用	バージョンアップ
	マルウエア対策	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化	要件定義の詳細化
	ログ管理	ログ出力要件の定義	アプリケーションログ出力	アプリケーションログ監視	アプリケーションログ調査・分析	アプリケーションログ監査・報告

米 NIST のガイドライン「SP－800－63－B」では、**パスワードの定期変更や複数文字種の組み合わせの強制は非推奨**としています。「長さや複雑さを要求しても、ユーザーは‘‘Passwordl！’’などの推測されやすいものを選択してしまう」「定期変更を強制すると、変更のたびに‘‘先頭か末尾に付けた数字を変えていく”といった安易なルールで対応してしまう」といった要因により、推測の難易度には寄与しないと考えるからです。

表2 セキュリティ脅威の分類

分類			詳細項目
大	中	小	
人為的脅威	意図的脅威	脆弱性を突く攻撃	Web アプリケーションの脆弱性（バッファオーバーフロー、SQL インジェクション、ディレクトリートラバーサル、クロスサイトクリプティングなど）、システム基盤の脆弱性（ミドルウエア、OS プラットフォームなど）、ネットワーク基盤の脆弱性
		不正アクセス	サーバーおよびネットワークへの侵入、未承認端末の不正接続、未承認媒体の不正接続、リスト型アカウントハッキング、DoS/DDoS、ブルートフォース攻撃、特権昇格
		メール攻撃	ウイルス付きメール攻撃、URL 付きメール攻撃
		マルウエア	既知のマルウエア、未知のマルウエア
		改ざん	プログラム改ざん、データ（静的）・ログ改ざん、データ（動的）改ざん、コンフィグ改ざん
		情報持ち出し	内部者による電子媒体・紙媒体・ネットワーク経由の情報の不正持ち出し
		盗難	紙媒体の盗難、電子記憶媒体の盗難、機器の盗難
		データ復元	リサイクル、廃棄されたディスクの復元、トラッシング
		なりすまし	アカウントの奪取、権利の偽造
		通信の盗聴	ネットワークパケットの盗聴、電話・音声の盗聴
		構内侵入	建物や管理室などへの物理的侵入
		盗み見	ショルダーハック
		物理破壊	機器の破壊、情報資産の破壊
	偶発的脅威	ヒューマンエラー	置き忘れによる紛失・棄損、配送時紛失・棄損、メール /FAX/ 郵便物の誤送信、システム設定ミス、システムの誤操作
		障害	ハードウエア障害 / ソフトウエア障害、OS・サービスダウン、メンテナンス不備（容量超過など）
環境的脅威		災害	水害、洪水、汚染、大気現象（台風、落雷）、火災、地震、火山活動、ちり・ほこり
		社会インフラの損失	空調・水道設備の破損、停電、通信遮断
		放射線による外乱	電磁放射、熱放射、電磁パルス

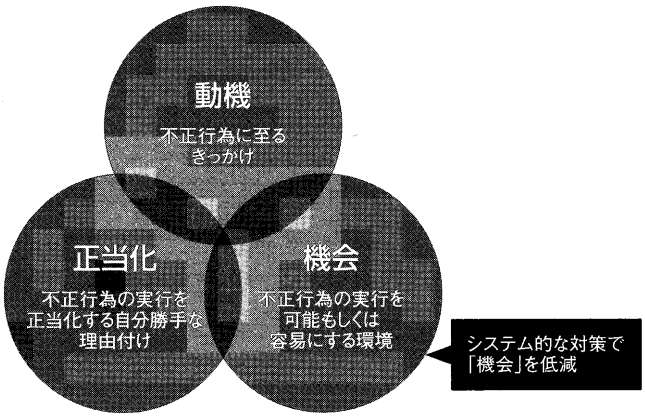

図4 内部不正の3大要因

組織犯罪研究者のドナルド・R・クレッシー氏が提唱した

一方、残りの一つの要因である機会は、人の心理とはあまり関係がありません。内部不正に対してシステム的な対策を打つべきなのは、ここです。**機会がなければ内部不正は成立しません。**IT システムを利用して不正行為をできない、やらせない環境にいかに近づけるか、これが IT エンジニアが上流工程でやるべき内部不正対策となります。

脅威の識別の具体的な方法としては、「**STRIDE(ストライド)手法**」が知られています。米 Microsoft が策定したソフトウエア開発における一般的なアプローチですが、IoT における脅威の識別としても有効です。想定される脅威を、「なりすまし（Spoofing）」「改ざん（Tampering）」「否認（Repudiation）」「情報の漏洩・意図しない開示（Information disclosure）」「DoS 攻撃（Denial of service）」「権限昇格（Elevation of privilege）」の 6 つに分類します。STRIDE はこれらの頭文字をとったものです。

最後のステップの（5）脅威の評価では、製品の故障分析などで一般的に用いられている FTA（Fault Tree Analysis）手法や、FTA をサイバー攻撃の分析に応用した ATA（Attack Tree Analysis）手法を用いて、脅威が発現する具体的な条件や、攻撃手段を検証します。攻撃の手段を抽象度の高いものからより詳細な手段へツリー構造で分解し、そのリスクの度合いを分析する手法です。

分解した攻撃手段の影響の大きさは、「潜在的な損害（Damage potential）」「再現可能性（Reproductivity）」「攻撃利用可能性（Exploitability）」「影響ユーザー（Affected users）」「発見可能性（Discoverability）」という 5 つの指標を用いて評価します。それぞれの頭文字をとって「**DREAD(ドレッド)**」と呼ばれています。