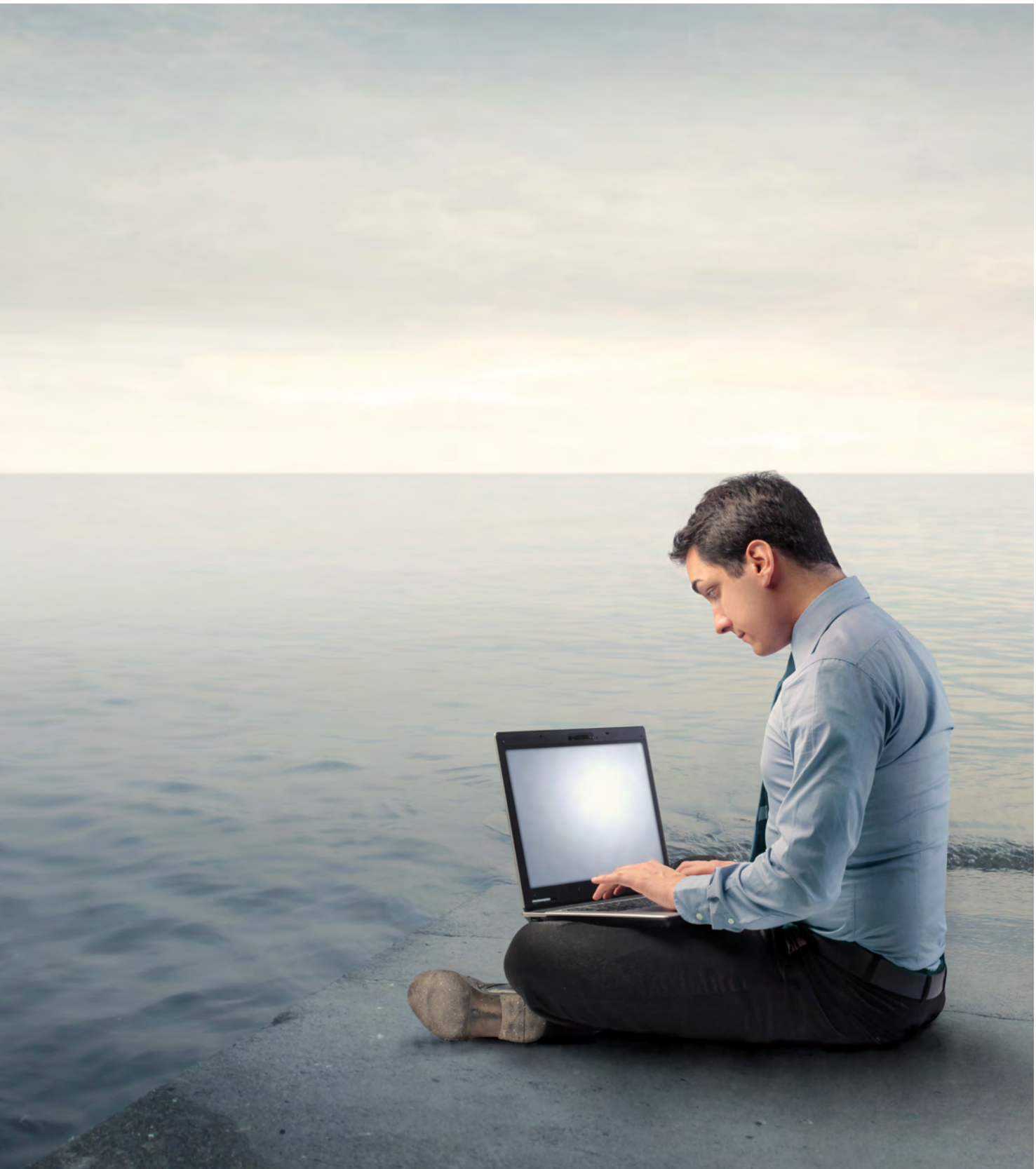
クラウド セキュリティー

ホワイトペーパー



概要

Software as a Service (SaaS)への関心が高まるにつれて、必然的にセキュリティー要件に対する新しいパラダイムが求められています。今までとは異なる外部の環境で顧客情報の転送、処理、管理が行われるため、その情報の保護を重視する必要があります。

ダッソー・システムズは、制御された幾層ものセキュリティー機能を確保するために、安全性をオンライン・ビジネス・エクスペリエンス・プラットフォームの開発および展開の中心に据えて、特に「Security in Depth (多層防御)」の概念を重視しています。

本書は、最も重要な資産であるお客様のデータを保護するためにダッソー・システムズが採用しているメソドロジーを紹介することを目的としています。本文書は、セキュリティー上のリスクを軽減するために利用されるメソドロジーや技術を概略的に説明することを目的としています。

SECURITY IN DEPTH

ダッソー・システムズのコンセプト「*Security in Depth*」で重視しているのは、あらゆる種類のリスクを軽減できる複数の独立した仕組みを配備することです。万が一、悪意ある行為をブロックできなかったとしても、すぐに脅威に発展することはなく、次に別の仕組みがブロックします。

ダッソー・システムズのオンライン 3Dエクスペリエンス・プラットフォームでは、業界の標準規格やベストプラクティスに可能な限り準拠し、特に以下を重視しています。

- ISO 2700x 標準規格、特に導入ガイド ISO 27002
- NIST 800 シリーズ
- 各種 OWASP ガイドライン
- CobIT フレームワーク

インターネット セキュリティー

幾層ものセキュリティーを配備し、意図したトラフィックやアクティビティのみをオンライン　プラットフォームで処理できるようにします。

受信するすべてのトラフィックを独立した仕組みでフィルタリングすることで、信頼性を保証し、脆弱性の連鎖がないことを確実にします。それに加え、インターネット規模のホスティング環境は分散 DoS 攻撃に堅牢です。ホスティング環境とお客様環境間で安全な通信チャネルが使用されるため、この機能が適用される場合は、送受信データの機密性と完全性が確保されます。

アプリケーション レベルのセキュリティー

ダッソー・システムズのオンライン・ソリューションでは、アプリケーション層に厳密なセキュリティー設計とレビュープロセスを施しています。開発および検証プロセスはセキュリティーに対する認識と対策を組み込んで設計されています。コードは、業界のベストプラクティスと推奨事項に適合し、社内外の部門による二段階レビューを受けています。OWASP が発行するリストの上位に掲がる脅威を重視し、アプリケーションのエコシステムに対しては、セキュア コーティングを補完する更なる安全性チェックを追加するために、ペネトレーションテストを一定の周期で実施します。スキャンプロセスを継続的に実施することで、アプリケーションの様々なモジュールを常に監視しています。

イン・クラウド・セキュリティー

ダッソー・システムズが提供するクラウド上では、クラウド上の他の要素に対する顧客環境の安全性(イン・クラウド・セキュリティー)を、さらに複数の独立したソリューション層を通して確実に保護します。ファイアウォールによるトラフィック制限を超えて、個々のユーザーが他のシステムから切り離されたインスタンス上で作業でき、このアプローチが顧客間のデータアクセスを保護しています。このような区画化もアプリケーション層でハードコーディングされています。

クラウド環境が区画の分割を実現できる構造になっていると、ネットワーク偵察行為やサイバー攻撃などの典型的なリスクも軽減されます。特にスニッフィングや IP スプーフィングを実行できない設計になっています。

仮想システムのセキュリティー

データやアプリケーションをホストする仮想システムは、運用環境へのリリース前に、セキュリティーの観点からの綿密な検査を受けます。この仮想システムに適用されているセキュリティー ライフサイクルは厳重に定められており、運用環境へのリリース後も高い水準でセキュリティーを維持できます。

ダッソー・システムズでは、一般的なセキュリティー保守対策(システム パッチの適用、サービス レビューなど)を越えて、攻撃を想定したシナリオを定期的に実行し、モデル システムの完全性とともに運用チームの反応もテストしています。不定期でも周期的に、これらのテストを実施することで、テスト結果の統合(因果解析)に効果を発揮します。

物理システムのセキュリティー

顧客データつまり知的財産（IP)は、人目につかないデータ センターで保管および処理されます。データ センターへのアクセスは許可されたスタッフのみに厳しく制限されます。
契約業者や訪問者がデータ センターを訪れる場合は、必ずスタッフが同行します。
データ センターへの入場者はすべて記録され、監査されます。
物理ストレージは、冗長構成ディスク、障害回復、バックアップの作成と復元などの方法で安全に保護されています。

セキュリティー テストとレビュー

情報セキュリティーは、ダッソー・システムズのお客様向けクラウド・ソリューションの開発工程に組み込まれています。これは、起こり得るすべての問題を特定し、共に対策に取り組んできた研究開発チームと情報セキュリティーチームの努力の結果です。

このような積極的なアプローチに加えて、単独テストを1 年に 1 回以上、またはプラットフォームの大幅な変更ごとに実施します。このテストでは、ハッカーと同じ手法を用いて各セキュリティー層に負荷をかけて侵入を試みます。

このようなセキュリティー対策は、グローバル規模の設計、実装、検証サイクルの一環として慎重に計画され、実施されています。

プラットフォームのセキュリティー対策だけでなく、役割ベースのアクセスもアプリケーション内で完全に制御でき、データの所有者は、粒度の細かいアクセス権を設定できます。

正当なライセンスを取得していなければアプリケーションにアクセスできないため、攻撃が表面化する可能性が最小限に抑えられます。TLS ベースのセキュリティーは、盗聴や中間者攻撃に対して有効で、接続の安全性を保証します。

SECURITY IN DEPTH のレイヤー構造

まとめ

ダッソー・システムズの Security in Depth は複数の独立した仕組みで設計されており、3Dエクスペリエンス・プラットフォームをクラウド上に展開する際のあらゆるリスクを軽減することを目的としています。ダッソー・システムズのオンライン・ビジネス・エクスペリエンス・プラットフォームは、セキュリティーを中心に据えて開発されているため、お客様は安心して当社の Saas プラットフォームをお使いいただけます。

用語集

メソドロジー

因果解析
不具合の発見後に、その原因と関係性を明確にするためのプロセス改善手法

OWASP

OWASP (Open Web Application Security Project)は、アプリケーションのセキュリティーに関するガイドラインを設定している国際的な団体。ウェブ アプリケーションが抱える重要なセキュリティー上の脆弱性を掲載したリストを発行。ウェブ セキュリティーにおける「代表的」な団体

サイバー攻撃

分散 DoS 攻撃

複数のネットワークに分散する大量のコンピュータが特定のシステムに対して一斉に接続要求を送る攻撃。ターゲットとされたシステムでは処理能力が追いつかず、機能停止状態に陥ります。

盗聴、ネットワーク スニッフィング

ネットワーク上を流れているデータを盗聴し、その内容を悪意ある目的で解析および利用する行為。主に中間者攻撃(別項参照)の手法を利用します。2 つのシステム間(主にクライアント/サーバー間)のトラフィックを盗聴できる特定のネットワーク構成をターゲットにします。

IP スプーフィング

攻撃者が自分の IP アドレスを偽装し、信頼できる相手からのトラフィックであるかのように見せかけて、攻撃対象システムに侵入する手法

中間者攻撃

正当なクライアントとサーバーの間の通信経路に悪意を持つホストを割り込ませる攻撃手法。明白な方法で正当な受信者にトラフィックが渡る前に、悪意を持つホストがデータを横取りします。横取りされたデータは解析され、悪意のある目的のために使用されます。

ネットワーク偵察行為

攻撃対象のネットワーク、システム、サービスのトポロジーを調査することを目的とした偵察行為。ネットワーク攻撃に先立って計画され、攻撃を準備するために行われます。

脆弱性の連鎖

あるシステム上の問題が他のセキュリティー層に影響を及ぼすような設計上および実装上の不具合

XSS

クロスサイト スクリプティング。アクセス制御を処理する際の欠陥(保安上の問題のあるコーディング方法など)を悪用して、アプリケーションを攻撃する手法。

保護

ペネトレーション テスト

ハッカーと同じ方法でシステムへの侵入を試みる一連のセキュリティー テスト。網羅的に実施されます。

セキュア コーディング

ウェブ アプリケーションに脆弱性が存在しないようにするためのルール、メソドロジー、フレームワークのサブセット。OWASP 標準に密接に関連します。

Security in Depth（多層防御）

複数の独立した仕組みによって情報を保護するセキュリティー概念。1 つの仕組みが破られても他の仕組みに影響が及ばないため、攻撃を排除しやすくなります。

システム パッチの適用

ベンダー推奨のパッチを適用することで、システムの全コンポーネントが確実に最新の状態になります。

TLS

ネットワーク通信の暗号化経路。安全性が保証されないメディア(インターネットなど)でのセキュアな通信を可能にします。

ダッソー・システムズの 3D エクスペリエンス・プラットフォームでは、12 の業界を対象に各ブランド製品を強力に統合し、各業界で必要とされるさまざまなインダストリー・ソリューション・エクスペリエンスを提供しています。

ダッソー・システムズは、**3D** エクスペリエンス企業として、企業や個人にバーチャル・ユニバースを提供することで、持続可能なイノベーションを提唱します。世界をリードするダッソー・システムズのソリューション群は製品設計、生産、保守に変革をもたらしています。ダッソー・システムズのコラボレーティブ・ソリューションはソーシャル・イノベーションを促進し、現実世界をより良いものとするためにバーチャル世界の可能性を押し広げています。ダッソー・システムズ・グループは 140 カ国以上、あらゆる規模、業種の約 19 万社のお客様に価値を提供しています。より詳細な情報は、**www.3ds.com**（英語）、**www.3ds.com/ja**（日本語）をご参照ください。

3DEXPERIENCE®

DASSAULT SYSTEMES | The 3DEXPERIENCE Company

南北アメリカ
Dassault Systèmes
175 Wyman Street
Waltham,
Massachusetts
02451-1223
USA

ヨーロッパ / 中東 / アフリカ
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay
Cedex
France

アジア太平洋
ダッソー・システムズ株式会社
〒141-6020
東京都品川区大崎 2-1-1
ThinkPark Tower