

クラウドサービスにおけるセキュリティ設計

NECソリューションイノベータ株式会社 岩本 博文

DXにおけるセキュリティ

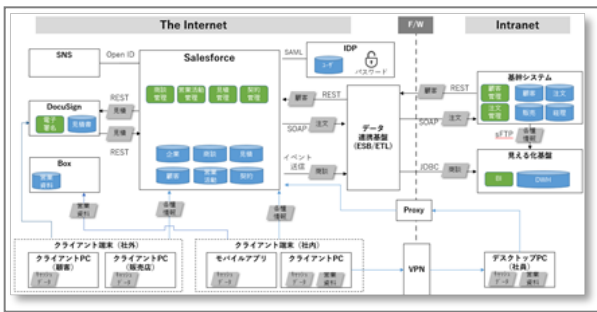
- DXによりオンプレミスからクラウドサービスへとシステムの移行が加速
- 利便性が高まる半面、設定ミス等による情報漏洩も発生
- DXを進めるためには、クラウドにおけるセキュリティの考え方を理解し、正しく設計・実装を行う必要がある

手法・ツールの適用による解決

- クラウドとオンプレからなる仮想システムを設計し、STRIDEによる脅威分析を実施
- 分析結果から退職者によるアクセスや自動バージョンアップ、ベンダーリスクなどクラウドならではの脅威を抽出し、セキュリティ設計を実施

アプローチ

1. 仮想システム設計



- ・ 見積から注文までをシステム化
- ・ SaaSとオンプレミスのハイブリッド構成

3. 差異結果整理

差異整理結果 (Information Disclosure)

- ・ ゼロデイ攻撃への対応リードタイムはベンダーに依存する
- ・ 退職者や私有デバイスによる不正アクセスが発生しうる

	クラウドサービス	オンプレミス
■ 第三者	・ クラウドサービスに接続する機器の脆弱性不備 ・ クラウドサービスとシステム間の通信経路 ・ クラウドサービスとシステム間の通信経路 ・ クラウドサービスとシステム間の通信経路	・ VPNの脆弱性についてインターネットに侵入し、システムに不正アクセス ・ クラウドサービスとシステム間の通信経路 ・ クラウドサービスとシステム間の通信経路
■ ベンダー(管理者)	・ 業務目的外でデータを第三者に提供 ・ 退職者/異動者のアカウントによるアクセス ・ 物理記憶媒体の窃盗	・ 業務目的外でデータを第三者に提供 ・ 退職者/異動者のアカウントによるアクセス ・ 物理記憶媒体の窃盗
■ 社員(管理者)	・ 業務目的外でデータを第三者に提供 ・ 退職者/異動者のアカウントによるアクセス ・ 社内コミュニケーションツールの投稿による、開示範囲外の社員への情報公開	・ 業務目的外でデータを第三者に提供 ・ 退職者/異動者のアカウントによるアクセス ・ 社内コミュニケーションツールの投稿による、開示範囲外の社員への情報公開
■ 社員(一般社員)	・ 業務目的外でデータを第三者に提供 ・ 退職者/異動者のアカウントによるアクセス ・ 社内コミュニケーションツールの投稿による、開示範囲外の社員への情報公開	・ 業務目的外でデータを第三者に提供 ・ 退職者/異動者のアカウントによるアクセス ・ 社内コミュニケーションツールの投稿による、開示範囲外の社員への情報公開

- ・ クラウドとオンプレミスに関するものを抜粋し差異を整理

外部からのアクセスやベンダーとの責任分界点がポイントとなる

2. 脅威分析

脅威分析結果 (Information Disclosure)

Element	Where	Who	How	C	I	A
Information Disclosure (情報漏洩)	Salesforce	第三者	ゲストユーザに対する権限設定不備により非公開情報が開示される	○		
			クワイアタイム間やシステム間の通信を傍受する	○		
			公開された脆弱性をベンダーが対応する前に攻撃される	○	○	○
		サーバやストレージなどの物理媒体を窃盗し、データを採取する	○	○	○	
ベンダー (管理者)		業務目的外でデータを第三者に開示する	○			
		退職者もしくは異動者にアカウント・権限が付与されたままとなり不正アクセスが行われる	○	○	○	
社員 (管理者)		業務目的外でデータを第三者に開示する	○			
		退職者もしくは異動者にアカウント・権限が付与されたままとなり不正アクセスが行われる	○	○	○	

- ・ 「顧客情報」に関する脅威分析を実施

情報漏洩に関するリスクが特に多い

4. セキュリティ設計

セキュリティ設計 (Information Disclosure)

- 退職者 / 異動者によるアクセスを抑制するためにアカウントの権限を実施
- 製品固有のセキュリティ設定に関しては、知識習得やベンダー等のコンサルを活用

Element	Where	Who	How	対策
Information Disclosure (情報漏洩)	Salesforce	第三者	ゲストユーザに対する権限設定不備により非公開情報が開示される	<ul style="list-style-type: none"> サービス知識の習得 ベンダー等のコンサル活用
			公開された脆弱性をベンダーが対応する前に攻撃される	<ul style="list-style-type: none"> 通信の暗号化 サービスのセキュリティ対策の確認
			サーバやストレージなどの物理媒体を窃盗し、データを採取する	<ul style="list-style-type: none"> サービスのセキュリティ対策の確認
			業務目的外でデータを第三者に開示する	
ベンダー (管理者)		退職者もしくは異動者にアカウント・権限が付与されたままとなり不正アクセスが行われる	<ul style="list-style-type: none"> アカウントの早期削除 / 権限削除 アクセス監視 	
社員 (管理者)		退職者もしくは異動者にアカウント・権限が付与されたままとなり不正アクセスが行われる		
社員 (一般)		退職者もしくは異動者にアカウント・権限が付与されたままとなり不正アクセスが行われる		
			私用デバイスを用いたアクセス	<ul style="list-style-type: none"> 運用マニュアルの徹底 アカウントの早期削除

- ・ クラウドにのみ存在する脅威のセキュリティ対策を検討

認証強化やサービス側の対策状況の確認が必要

考察

- 多要素認証等の認証強化策や退職に伴うアカウント棚卸等の運用設計は必須
- バージョンアップ時の影響確認が必要。ベンダー等の外部コンサル活用も効果的
- 信頼できるベンダーと契約すべく、契約前のセキュリティ対策状況の確認も有効

今後の取り組み

- オンプレミス特有の脅威やセキュリティの整理
- コストと損失を考慮したセキュリティ設計のレベル分け
- 実業務への分析結果適用