PCI DSSセキュリティフォーラム

DX時代に求められるセキュリティ対策とPCI DSS準拠

2022年6月24日

NRIセキュアテクノロジーズ株式会社

コンサルティング第二事業本部

決済セキュリティコンサルティング部

セキュリティコンサルタント　日暮　一太

目次

自己・会社紹介

自己紹介：日暮　一太（ひぐらし　いちた）

所属・氏名	専門
■ **NRIセキュアテクノロジーズ株式会社** コンサルティング第二事業本部 決済セキュリティコンサルティング部 日暮　一太（ひぐらし　いちた） ■**連絡先** **higurashi@nri-secure.co.jp**	■**決済セキュリティ全般に関するコンサルティング・審査** 保有資格等 ◆CISA（公認情報システム監査人） ◆CISM（公認情報セキュリティマネージャ） ◆PCI QSA（PCI DSS認定審査員） ◆P2PE QSA（PCI P2PE/TSP認定審査員） ◆PCI CPSA（PCI CP認定審査員）
経歴	**プロジェクト**
■**2013年 4月　大手インターネットサービスプロバイダ入社** ～2019年1月　ネットワークの設計・構築・運用業務に従事 ■**2019年 2月　株式会社 野村総合研究所（NRI）入社** ■**2019年 2月　NRIセキュアテクノロジーズ株式会社出向** ～現在　　セキュリティコンサルティング事業に従事	■**決済セキュリティコンサルティング・準拠審査** ●3D secureシステムのコンサルテーション・審査 ●PCI DSS準拠コンサルテーション・審査 ●トークナイゼーションシステムのコンサルテーション・審査 ■**決済システムに対するコンサルティング** ●　クラウドにおけるリスク評価　等

会社情報

野村総合研究所（NRI）グループにおける情報セキュリティ専門の中核企業

社名	**NRIセキュアテクノロジーズ株式会社**（略称：NRIセキュア）		
会社所在地	本社　：東京都千代田区大手町 東京サンケイビル 横浜ベイオフィス　：神奈川県横浜市神奈川区 横浜ダイヤビルディング 北米支社　：米国カリフォルニア州アーバイン		
設立年月日	2000年8月1日　※サービス提供開始：1995年		
資本金	4.5億円		
株主	株式会社野村総合研究所		
代表取締役社長	柿木 彰		
取締役	池田 泰徳、建脇 俊一、西内 喜一、竹本 具城、山口 隆夫	監査役	坂田 太久仁
社員数	連結：621名、単体：520名		
NRIセキュアグループ会社	株式会社ユービーセキュア：東京都中央区 株式会社NDIAS　：東京都港区		
提供実績	官公庁、金融機関、流通、製造、製薬、通信、マスコミ など		
認証取得	ISO/IEC 27001認証取得　IS 75215 / ISO 27001		

主要な提供サービス・製品一覧

コンサルティング

リスクアセスメント
- セキュリティ対策状況可視化
- グローバルセキュリティアセスメント
- ファストセキュリティアセスメント
- MITRE ATT&CKを用いたサイバー攻撃対策の評価
- 暗号鍵の設計・運用に関する評価支援
- 電子決済セキュリティリスク評価
- セキュリティ対策レポート
- セキュリティ監査

リスクマネジメント
- セキュリティポリシー策定支援
- セキュリティガイドライン策定支援
- サプライチェーン・セキュリティコンサルティング
- クラウドセキュリティコンサルティング
- IoTセキュリティコンサルティング
- APIセキュリティコンサルティング
- マネージド脅威情報分析

法規制・ガイドライン準拠
- 産業用制御システム向けAchilles認証取得支援
- CIS Controlsによるサイバー攻撃対策の強化支援
- CIS Benchmarks を用いたシステム堅牢化支援
- NIST SP800-171準拠支援
- 医療情報ガイドライン準拠支援

PCI準拠支援
- **PCI DSS SAQ対応支援**
- **PCI DSS SAQ準拠パッケージ**
- **PCI DSS / P2PE / 3DS / CP / PIN Security 準拠支援/審査**
- **PCI DSS準拠／維持支援スキャン**
- **非保持化支援**

プロジェクト実行支援
- セキュリティ対策支援
- セキュリティ対策構想策定・システム化計画作成支援
- セキュリティ対策推進PMO
- 中長期計画策定支援
- ゼロトラスト・コンサルティング

セキュリティ組織支援
- 組織内CSIRT総合支援
- 組織内PSIRT向け支援
- セキュリティ・カウンセリング
- CIO / CISO支援

設計開発支援
- セキュア設計・開発ガイドライン策定支援
- セキュアアプリケーション設計レビュー
- ソースコード診断
- デジタルサービス向けリスク分析支援

セキュリティ事故対応
- セキュリティ事故対応支援
- PFIクレジットカード情報漏えい調査

セキュリティ訓練
- サイバー攻撃対応机上演習
- 工場向けセキュリティ教育・インシデント対応訓練プログラム
- 不審メール対応訓練
- レッドチームオペレーション
- ペネトレーションテスト

セキュリティ診断

セキュリティ診断
- Webアプリケーション診断
- プラットフォーム診断
- スマートフォンアプリケーション診断
- APIセキュリティ診断/APIセキュリティ設計レビュー
- ブロックチェーン診断
- コンテナ診断
- エンドポイントセキュリティ診断
- クラウド設定評価

IoT/OTセキュリティ診断
- OTネットワーク・アセスメント
- デバイス・セキュリティ診断

設計開発支援
- セキュア設計・開発ガイドライン
- セキュアアプリケーション設計レビュー
- ソースコード診断

サイバーアタックシミュレーション
- レッドチームオペレーション
- ペネトレーションテスト
- 不審メール対応訓練

SOC・マネージドセキュリティサービス

SOC（セキュリティオペレーションセンター）
- セキュリティログ監視（NeoSOC）

EDR・MDR（エンドポイント対策）
- マネージドEDR
- マネージドXDR powered by Cortex XDR from Palo Alto Networks
- マネージドEDR（Microsoft Defender for Endpoint）

OA・ワークプレイス環境 運用監視
- Zscaler Internet Access マネージドサービス
- Zscaler Private Access マネージドサービス
- Netskope Security Cloud 管理
- CATO Cloud運用支援
- マネージドセキュリティ powered by Prisma Access from Palo Alto Networks
- Palo Alto PAシリーズ管理
- セキュアインターネット接続

公開Web環境 運用監視
- クラウド型WAF管理（Imperva Cloud WAF）
- WAF管理
- 統合クラウドセキュリティマネージドサービス powered by Prisma Cloud from Palo Alto Networks
- Deep Security管理

セキュリティ製品・ソリューション

ID管理・認証
- Uni-ID Libra
- Uni-ID MFA
- **SecureCube Access Check**
- Cloud Auditor by Access Check
- Okta
- YubiKey

リモートアクセス
- CACHATTO

メール・Webセキュリティ
- m-FILTER MailAdviser
- Proofpoint
- Global Relay Archive
- Cofense

文書・ファイルセキュリティ
- クリプト便
- POSTUB
- Box
- FinalCode
- Contents EXpert / Digital Form
- Contents EXpert / XML Assist

エンドポイントセキュリティ
- PC Check Cloud
- TRUST DELETE prime
- Menlo Security
- マネージドEDR

クラウドセキュリティ管理
- Netskope
- Prisma Cloud
- Zscaler Internet Access マネージドサービス
- Zscaler Private Access マネージドサービス

リスク分析・可視化
- IntSights
- Recorded Future
- GR360
- RiskIQ
- ObserveIT
- Secure SketCH

脆弱性管理
- Contrast Security
- Vex
- komabato
- Qualys
- Fortify

IoT/OTセキュリティ
- SCADAfenceプラットフォーム

セキュリティ教育・研修

セキュリティ資格取得支援
- SANSトレーニング
- CISSP CBKトレーニング

セキュリティ人材育成
- セキュアEggs

ナビゲーション活動

国内外で政策提言や標準化活動、独自調査分析の公開を行い、業界の発展に貢献

NRI Secure Insight
企業における情報セキュリティ実態調査

NRIセキュアテクノロジーズ 発行
（2002年～、年刊）

ITロードマップ
情報通信技術は5年後こう変わる！

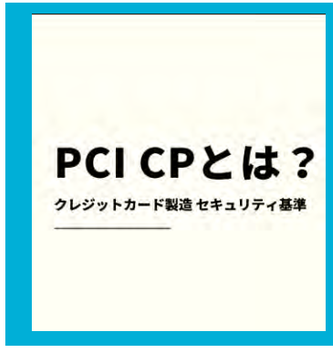
東洋経済新報社 発行
NRIセキュアテクノロジーズ、野村総合研究所 共著
（2016年～）

NRIセキュアレポート

NRIセキュアテクノロジーズ 発行
（2019年～、年2回刊）

ブログによる情報発信も実施

NRIセキュアブログ
：2022.06.22
『PCI DSS v4.0リリース情報｜その特徴とv3.2.1との差分、対応方針について解説』



NRIセキュアブログ
：2021.12.15
『PCI CPとは？クレジットカード製造時に求められるセキュリティ基準を解説』

決済セキュリティ分野におけるNRIセキュアテクノロジーズの強み

決済セキュリティに関わるあらゆるお客様の課題を解決可能

決済全般に精通

・QSA(PCI DSS, P2PE), 3DS Assessor, CPSA, QPAの5資格を保有し、カード決済領域を網羅
・電子決済（QR決済・スマホ決済・電子マネー等）の領域の支援可

豊富な実績とノウハウ

・規模、業種を問わず様々なお客様に対して決済セキュリティに対する豊富な支援実績
・国内トップクラスの豊富な知見

総合力

企画・設計・構築・運用・評価等様々なフェーズ、様々なレイヤ（インフラ・アプリ）での支援が可能

はじめに

DX（デジタルトランスフォーメーション）とは

- 経済産業省の定義によると

「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」

出典：経済産業省「デジタルトランスフォーメーションを推進するためのガイドライン」,
https://www.meti.go.jp/policy/it_policy/dx/dx_guideline.pdf

DX時代とは

- **デジタル・ディスラプターが台頭していることにより各業界の企業は従来のビジネスモデル、ビジネススピードではシェアを奪われるリスクにさらされている時代**
  デジタル・ディスラプター：デジタルテクノロジーを活用することにより既存のビジネスモデルを破壊する企業
- **Stripeに代表されるように、決済・金融の業界においても例外ではなく、生き残り戦略が不可欠**

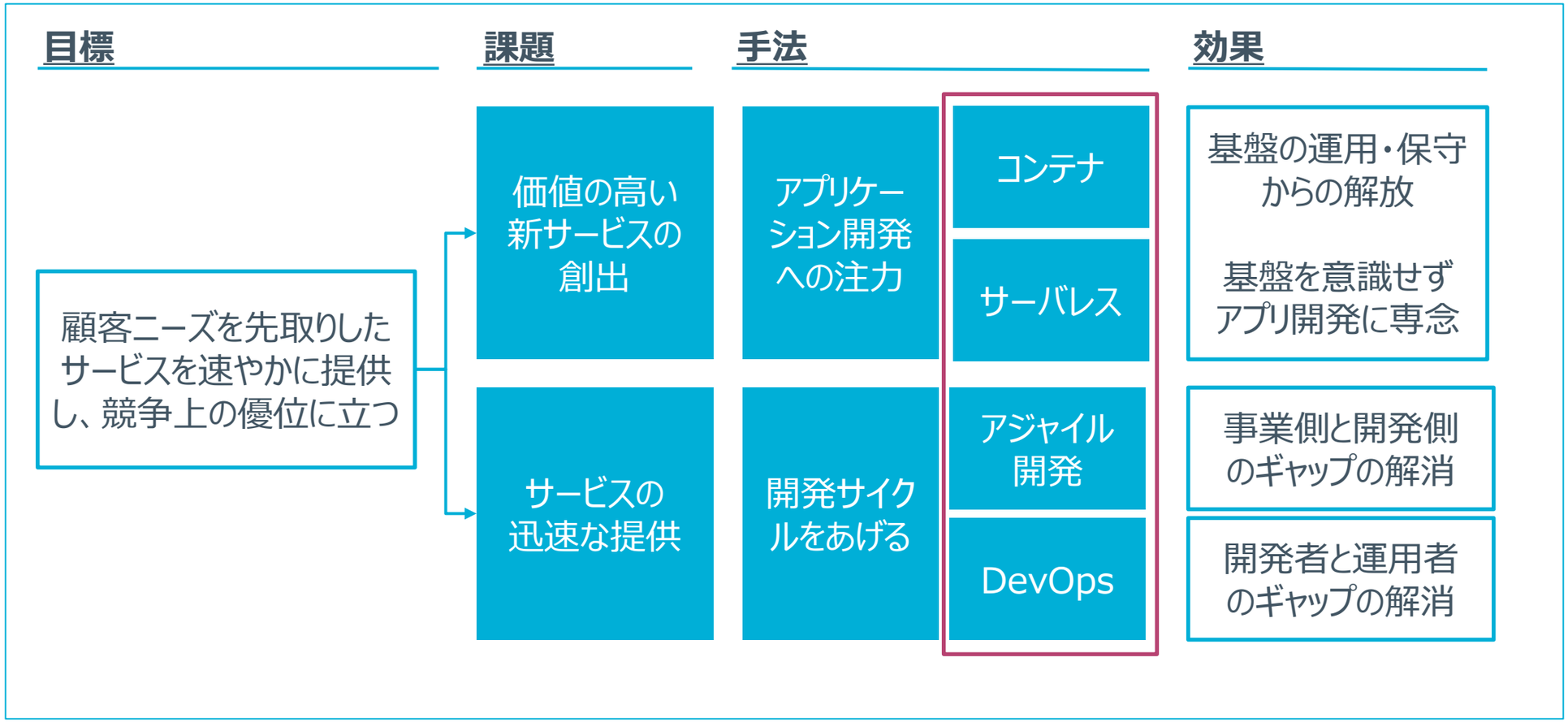
事例1：Amazon
インターネットの普及に伴い、商品売買の場がリアル店舗からECサイトへ拡大。Amazonの台頭は小売業界に大きなインパクトを与えた。

事例2：Netflix
オンラインのDVDレンタルサービスから、動画配信サービスを行う事業への転換を果たした。

事例３：Stripe
2011年創業の決済サービス企業。サービスのシンプルさと顧客の要望を満たす開発スピードの速さで、世界中にサービスを展開。ユニコーン企業として時価総額10兆円に。

DX時代で生き残るためには

- DX時代の課題は、「①価値の高い新サービスを、②迅速に提供すること」。
- そのためには、「アプリケーション開発にリソースを集中させ、開発サイクルをあげること」が重要。
- そして、そのためには「クラウド」と「標準化された開発手法」をいかに活用するかがカギ。



決済・金融におけるセキュリティの重要性

- 新サービスを開発することは重要である一方、決済・金融分野では<u>セキュリティは重要な経営課題</u>であるためセキュリティ対策は必須である。
- そのために以下の対応は必須であると考える。

サービスのリスク	サービスの穴を利用した攻撃は、システムでは対応できないため、サービスの企画段階で対策を行う必要あり
クラウドでのセキュリティリスク	情報資産をクラウドにおくため、外部からの脅威に常に晒されているため適切な対策を行う必要あり
開発におけるセキュリティリスク	・セキュリティ対策を後から実施することは難しく、また手戻りも発生するため設計・開発からセキュリティ対策を組み込む必要あり ・サプライチェーンへの対応

セキュリティを組み込みながら、高速なサービス開発を行い、安全・安心なシステムを提供していく必要がある。

DX時代に求められるセキュリティ対策

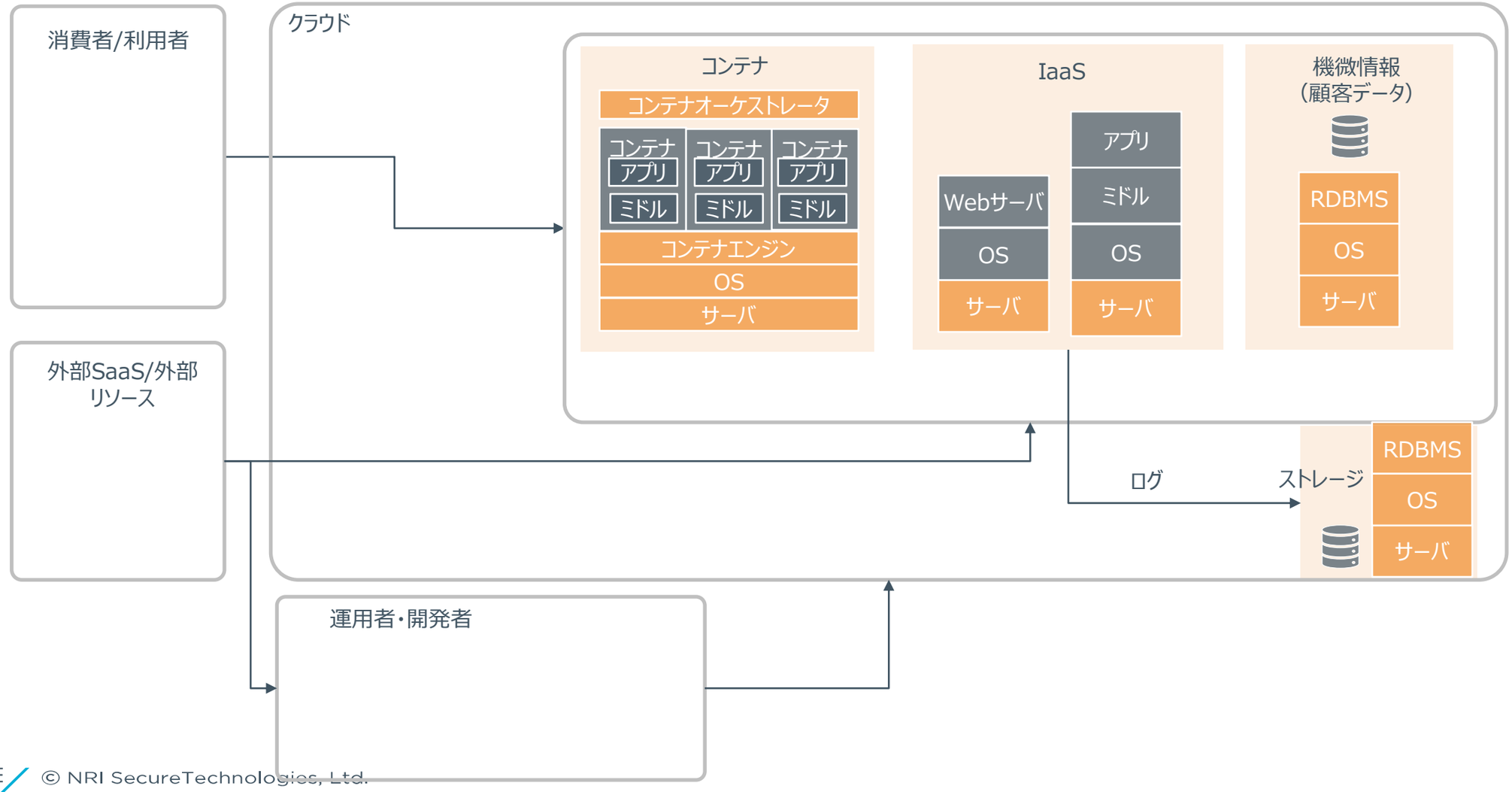
DX時代に必要なセキュリティ観点と課題

2つの観点と課題

観点	課題	
クラウドでのセキュリティ	クラウドサービス事業者の信頼性	サービス利用においては、機能や価格のみならず、セキュリティ面での対応状況など踏まえた選定が必要
	責任範囲の明確化	CSP側とユーザ側の管理/責任範囲を明確化したうえで、自社側にて対応する部分の明確化。加えて設定の確からしさのモニタリングが必要
	オンプレとは異なるセキュリティ設計・運用	従来のオンプレとは利用されている基盤技術が異なることから、オンプレとクラウドの違いを理解したうえでの設計が必要
開発におけるセキュリティ	開発サイクルの高速化・DevOpsへの対応	CI/CDを導入した開発サイクルへ追従するため、セキュリティテストの自動化が必要
	リモートワークでの開発への対応	リモートでの開発要求へ対応するため、従来のオフィスベースでの境界型防御から端末ベースでの保護が必要
	サプライチェーンリスクへの対応	オープンソースのライブラリの脆弱性確認や委託先からのソースコードの流出等への対応

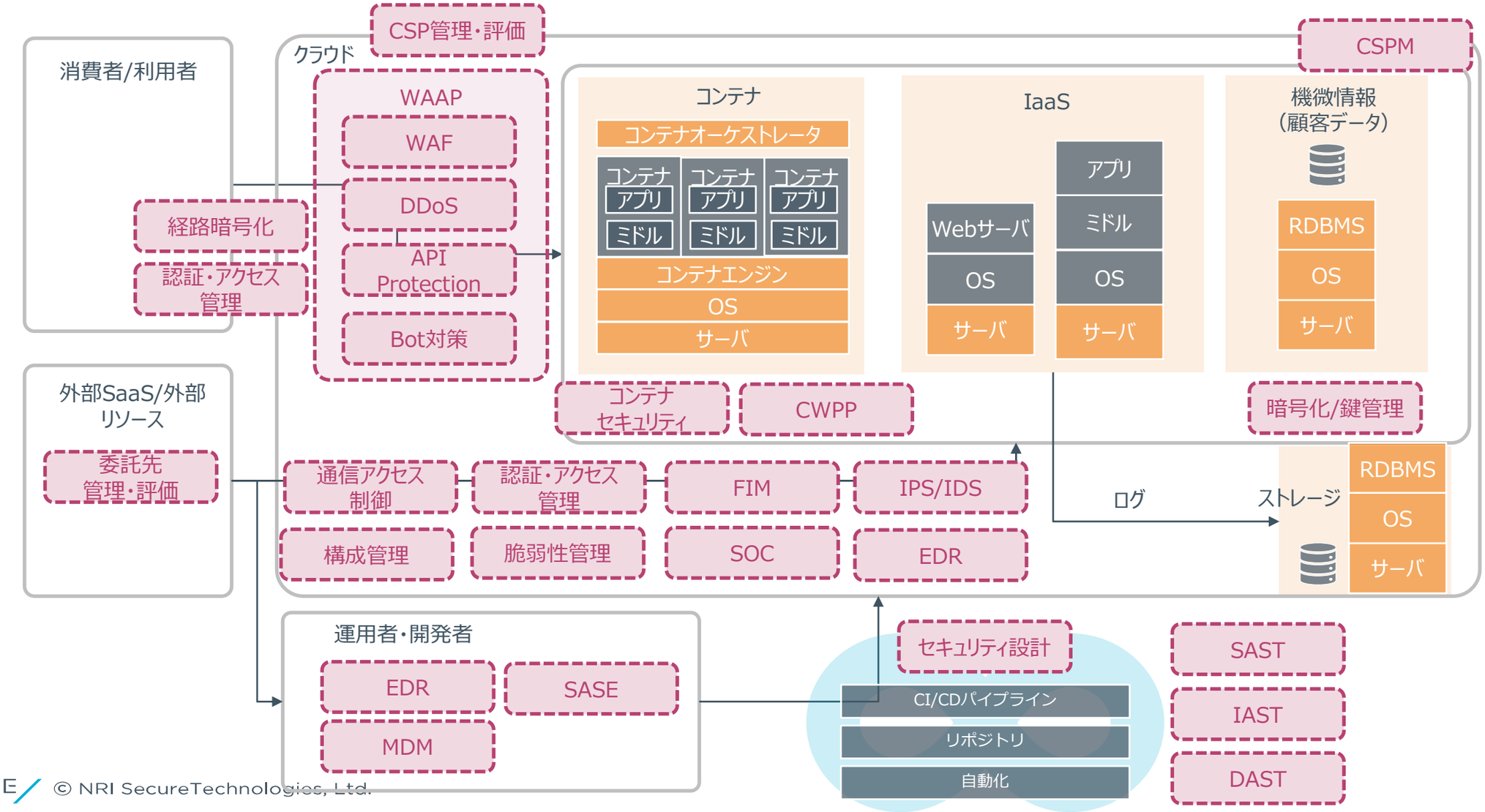
DX時代に求められるセキュリティ対策の全体像

システム例



DX時代に求められるセキュリティ対策の全体像

セキュリティの全体像(イメージ)

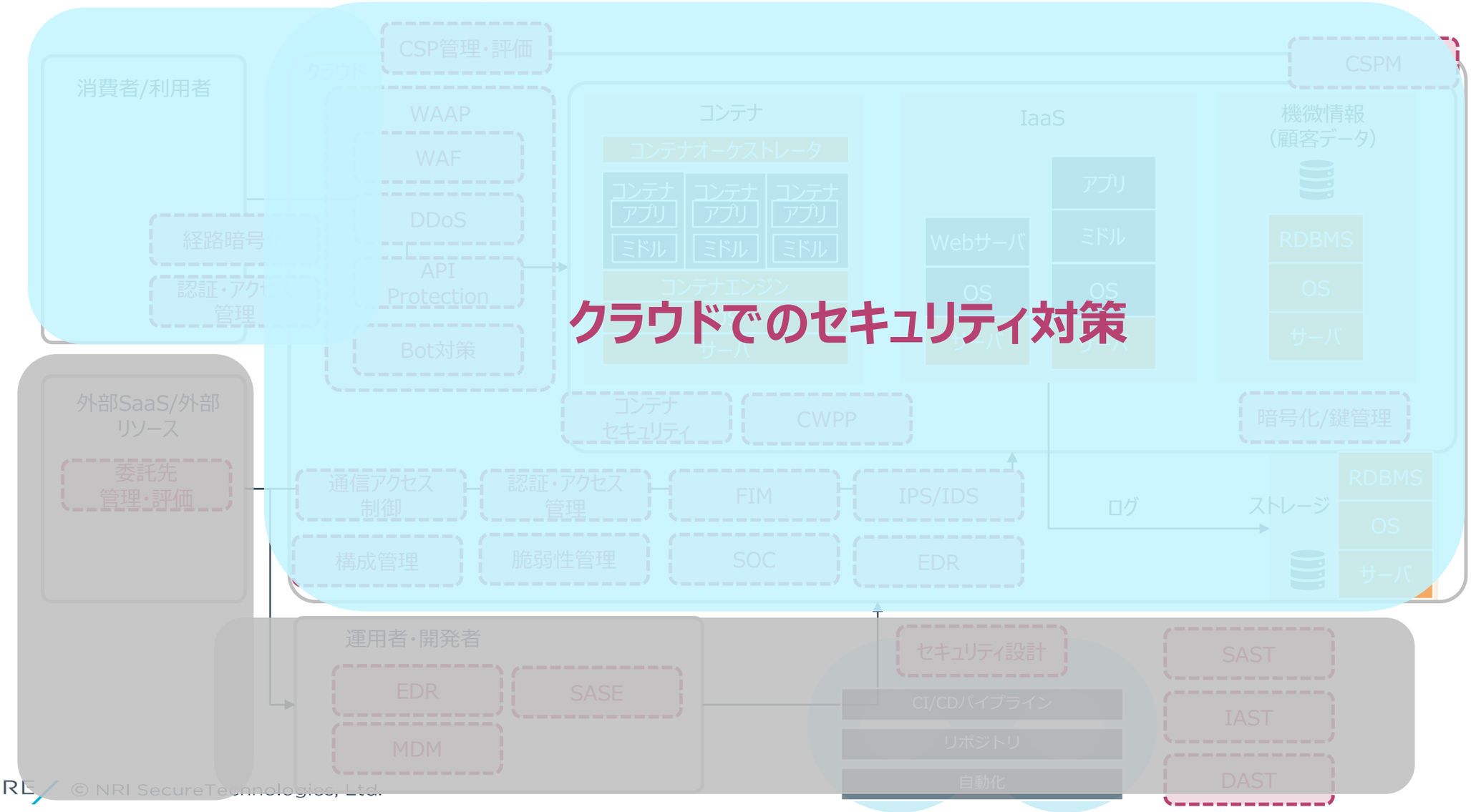


DX時代に求められるセキュリティ対策の全体像

セキュリティの全体像(イメージ)

DX時代に求められるセキュリティ対策の全体像

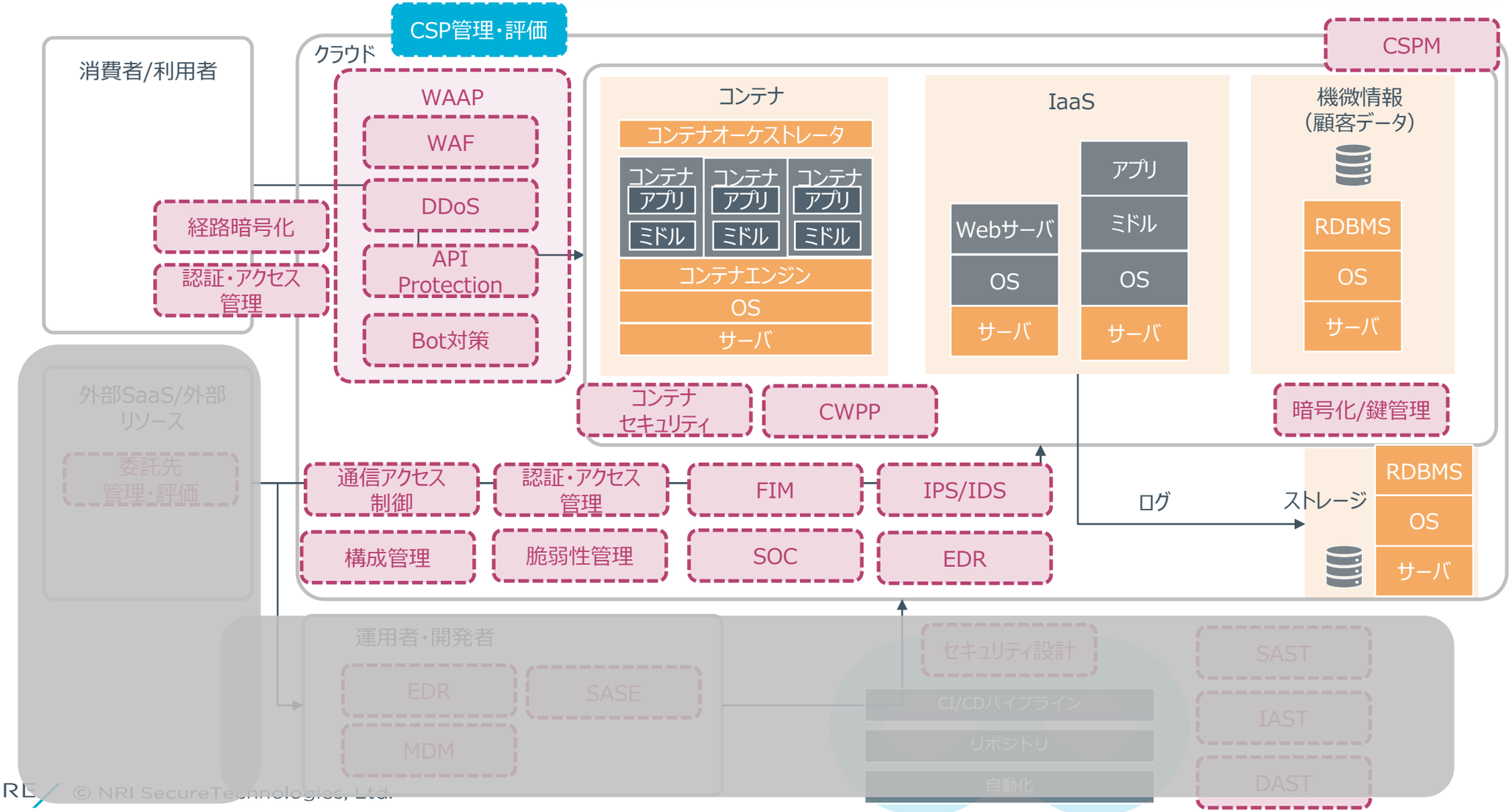
セキュリティの全体像(イメージ)



クラウドにおけるセキュリティ対策の重要なポイント①

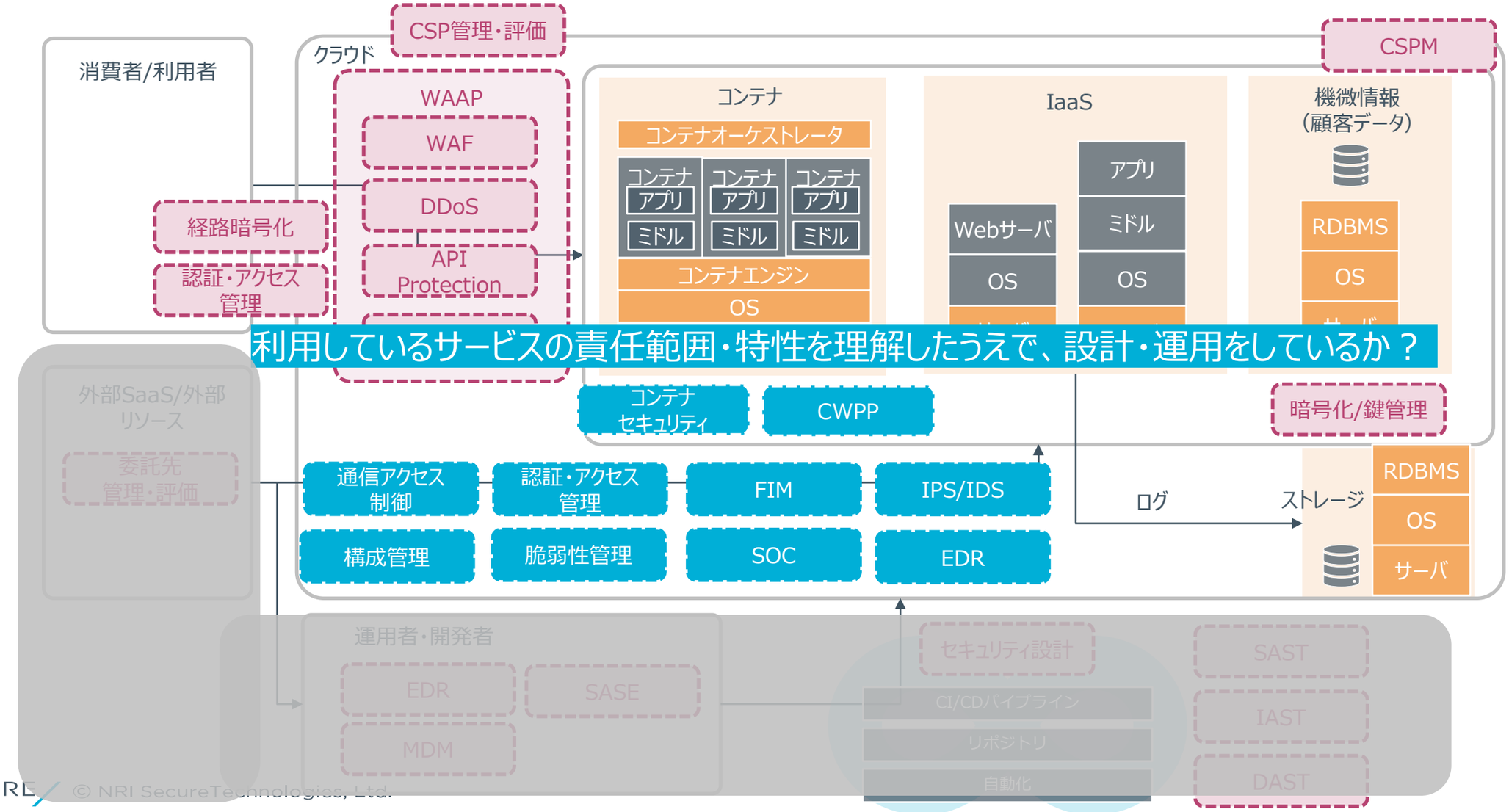
セキュリティの全体像(イメージ)

CSPが重要なデータを預けるに足る事業者であるかを確認したか？
コストやサービスの利便性だけで選んでいないか？



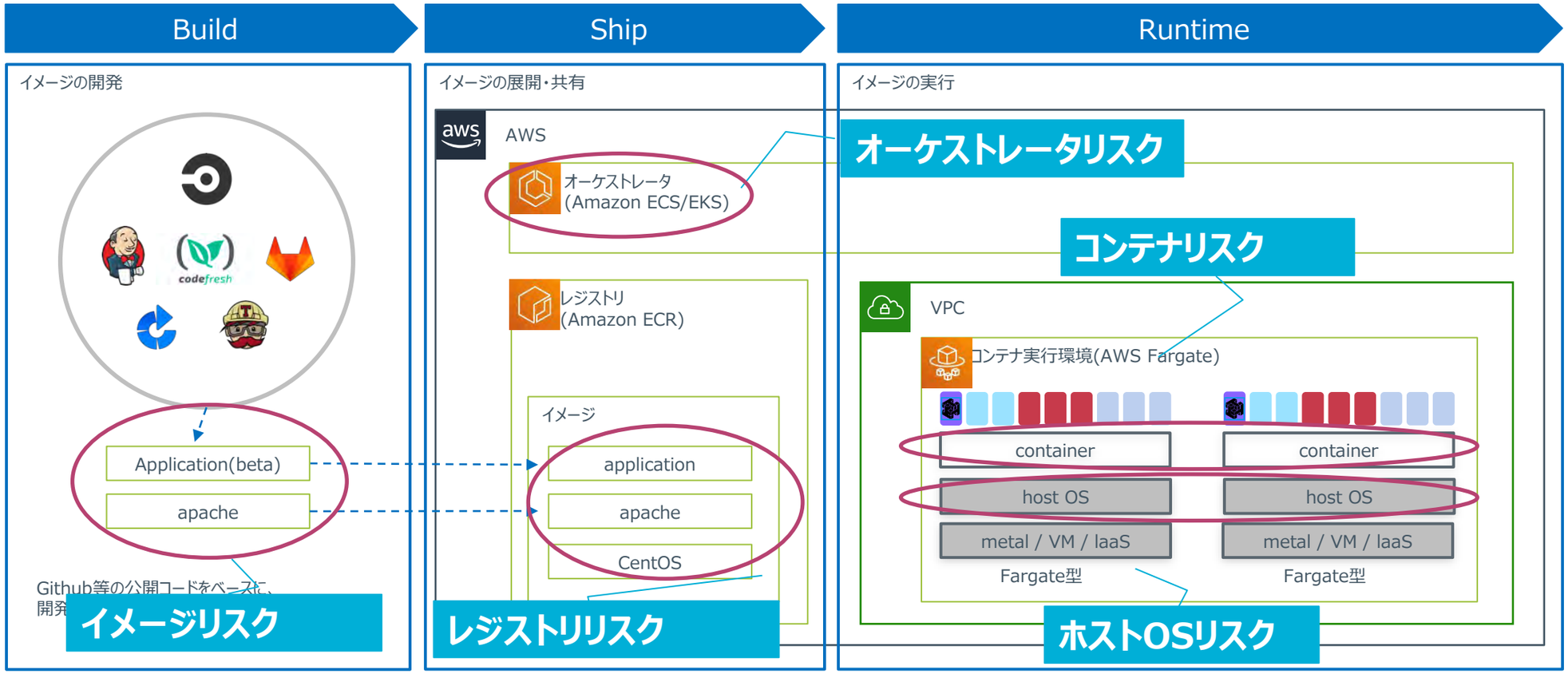
クラウドにおけるセキュリティ対策の重要なポイント②

セキュリティの全体像(イメージ)



クラウドにおけるセキュリティ対策の重要なポイント②’

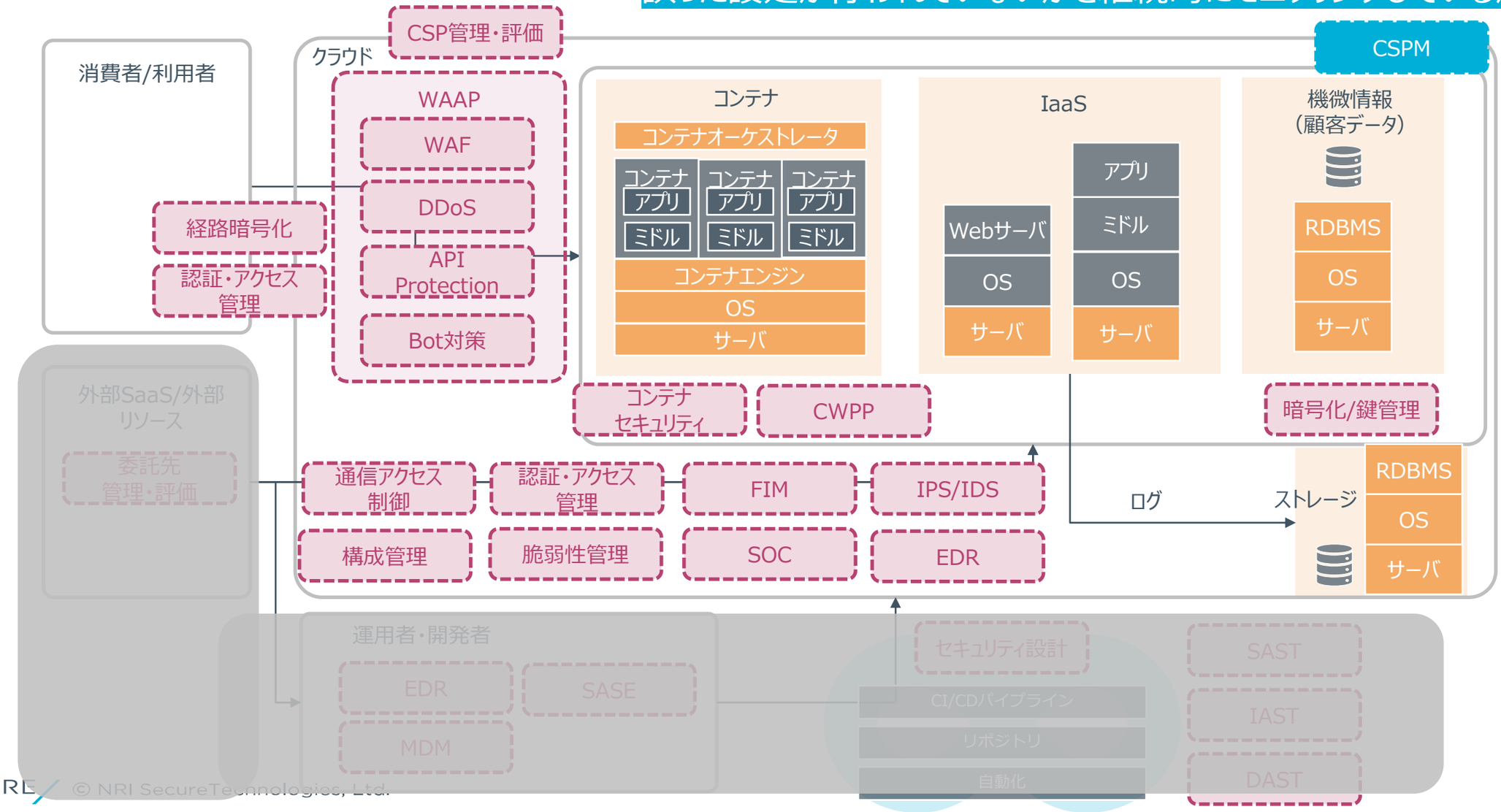
- **コンテナを利用した場合は、ビルドパイプライン全体を俯瞰した対策を行う**
  - コンテナを使うことで開発サイクルを高速化でき、アプリケーションの高頻度リリースを実現可能
  - 一方で、コンテナは複数の要素より構成されており、それぞれに潜むリスクを正しく理解する必要がある



クラウドにおけるセキュリティ対策の重要なポイント③

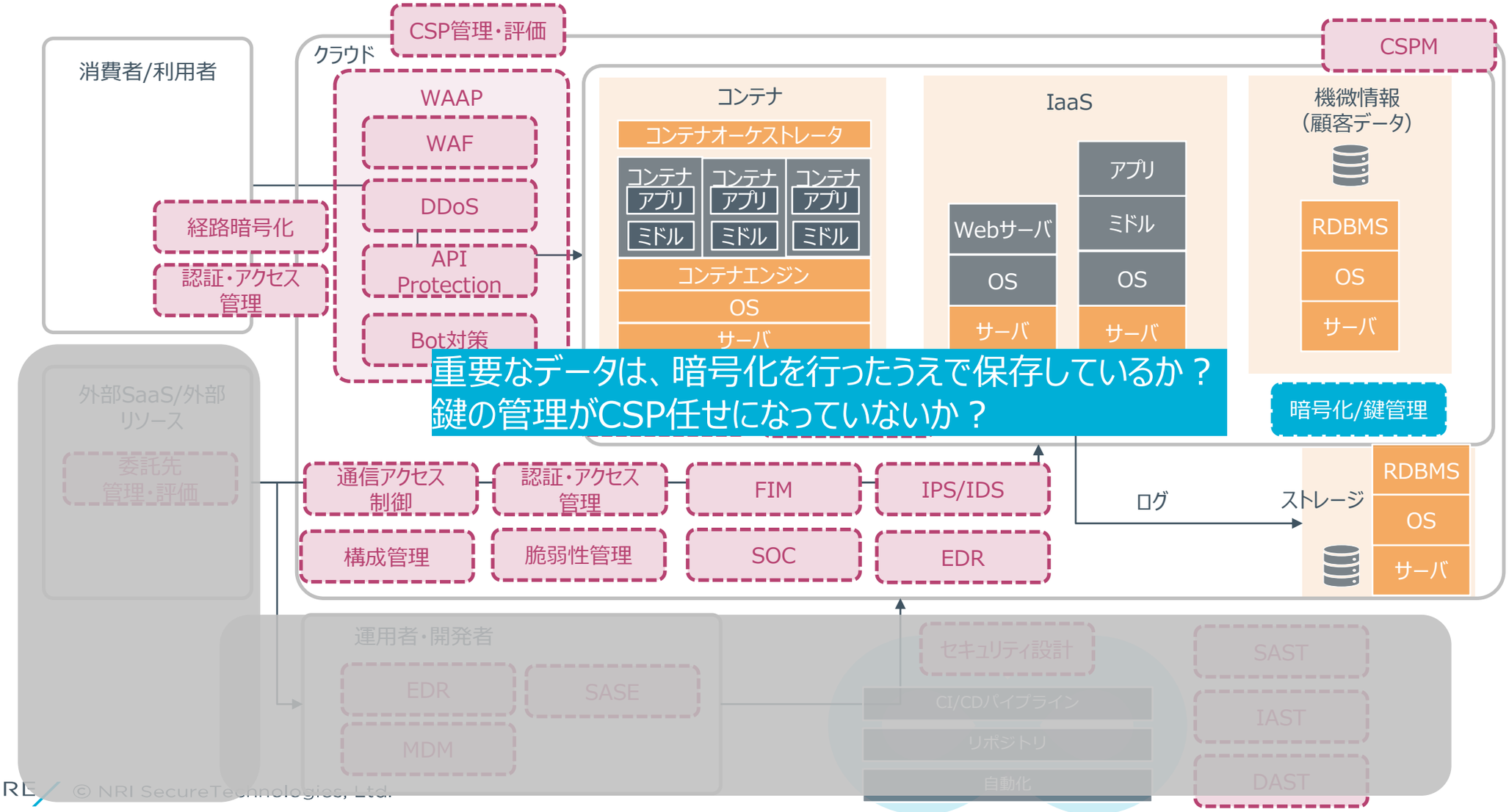
セキュリティの全体像(イメージ)

誤った設定が行われていないかを継続的にモニタリングしているか？



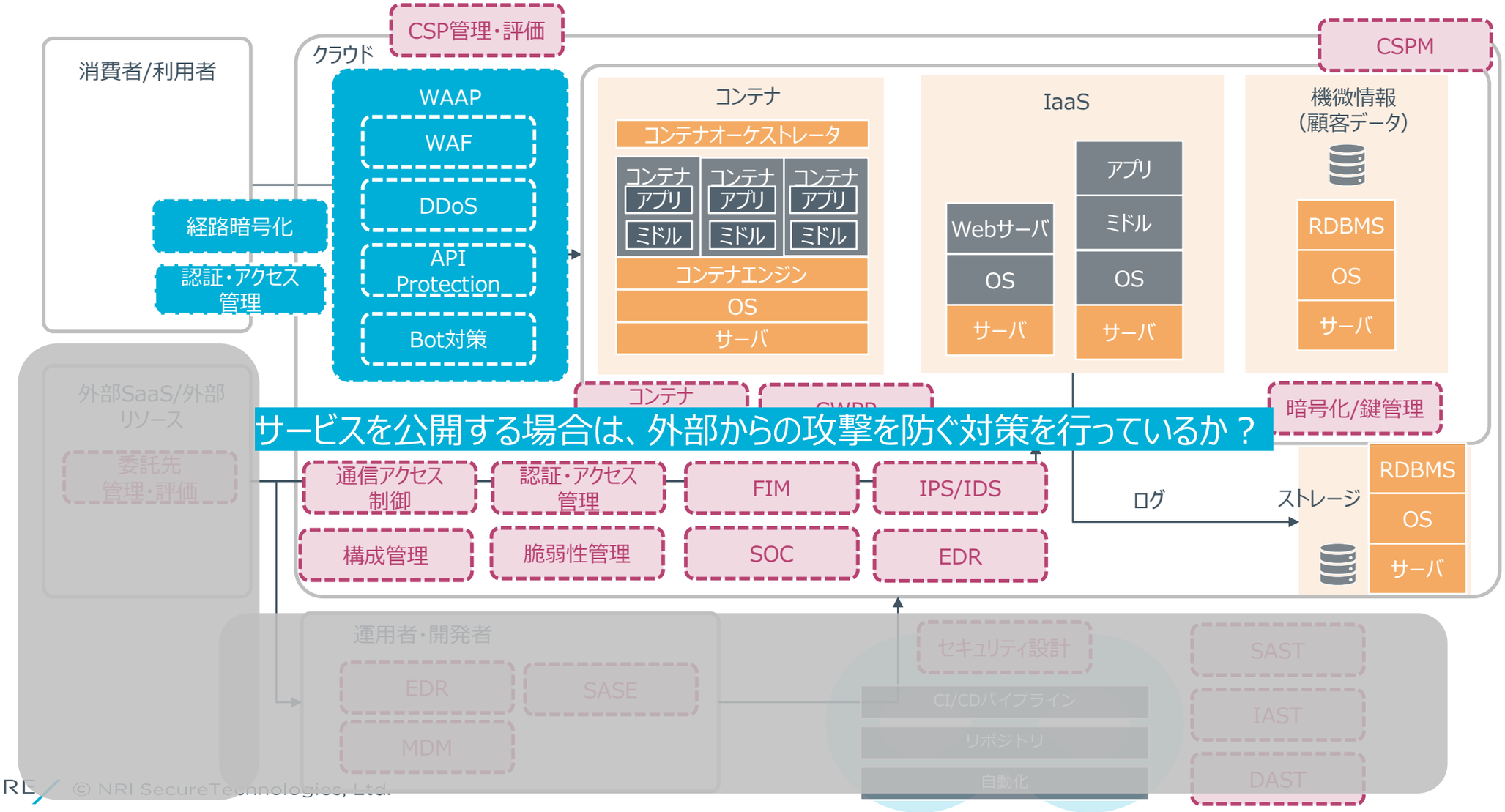
クラウドにおけるセキュリティ対策の重要なポイント④

セキュリティの全体像(イメージ)



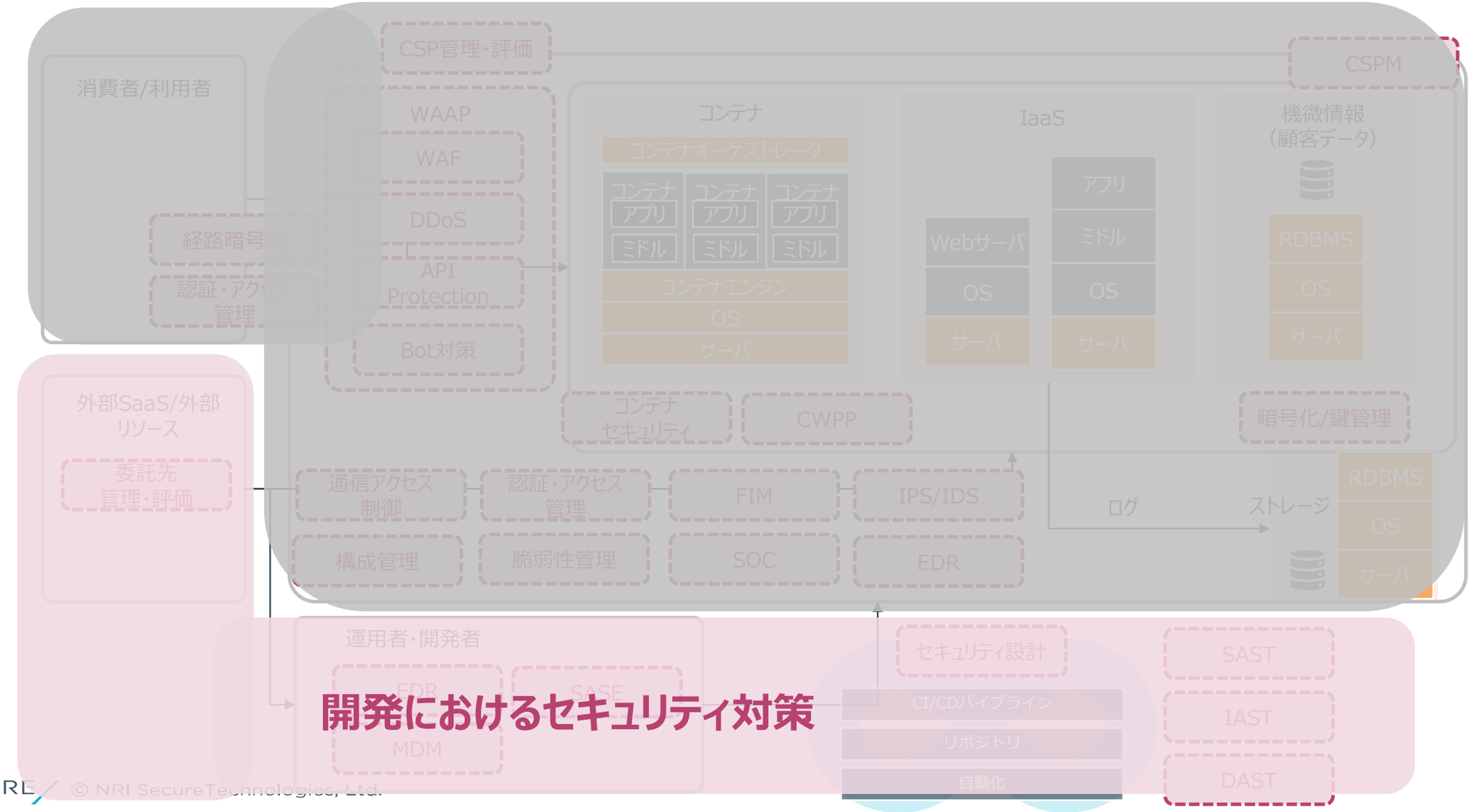
クラウドにおけるセキュリティ対策の重要なポイント⑤

セキュリティの全体像(イメージ)



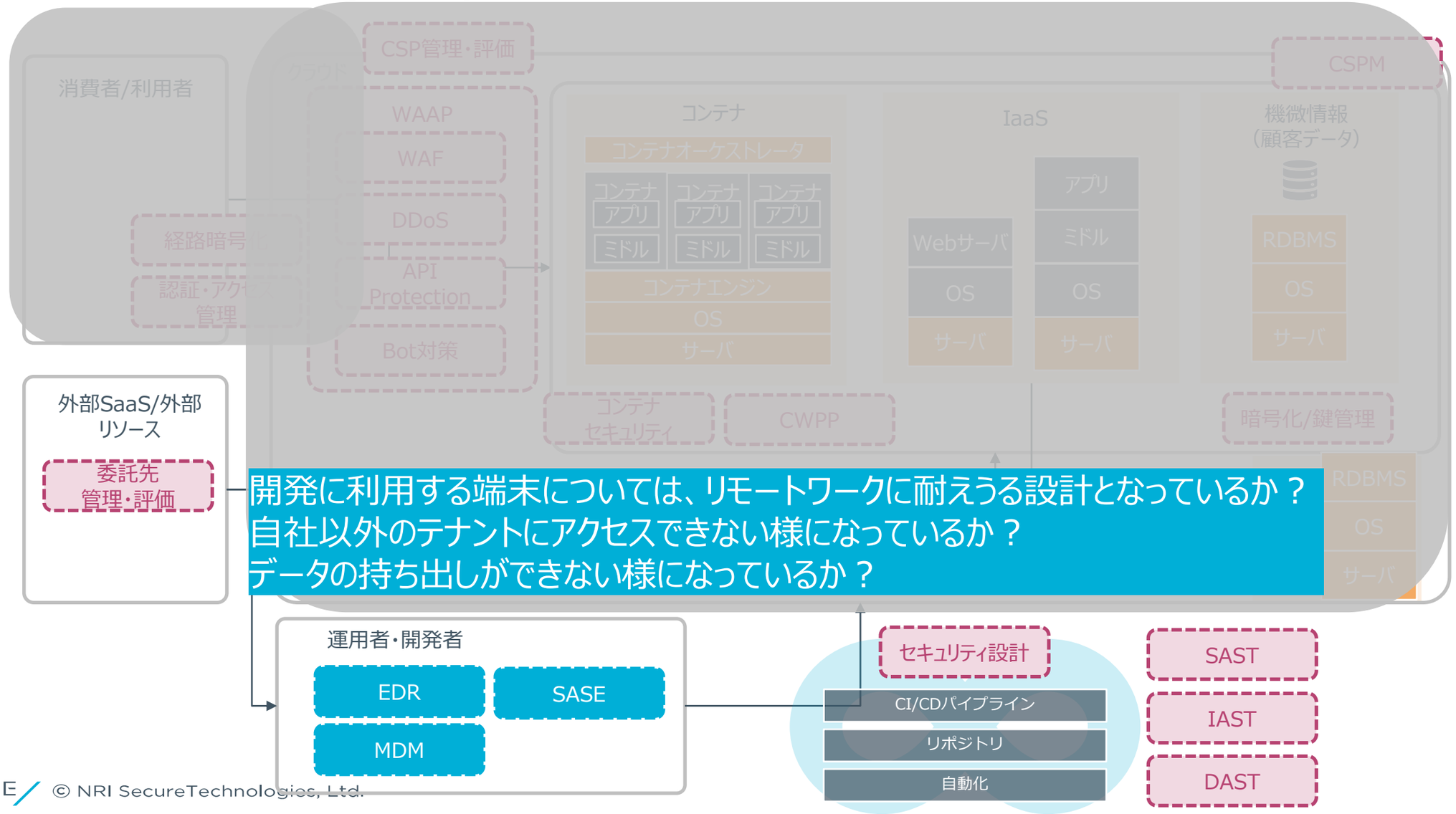
開発におけるセキュリティ対策の重要なポイント

セキュリティの全体像(イメージ)



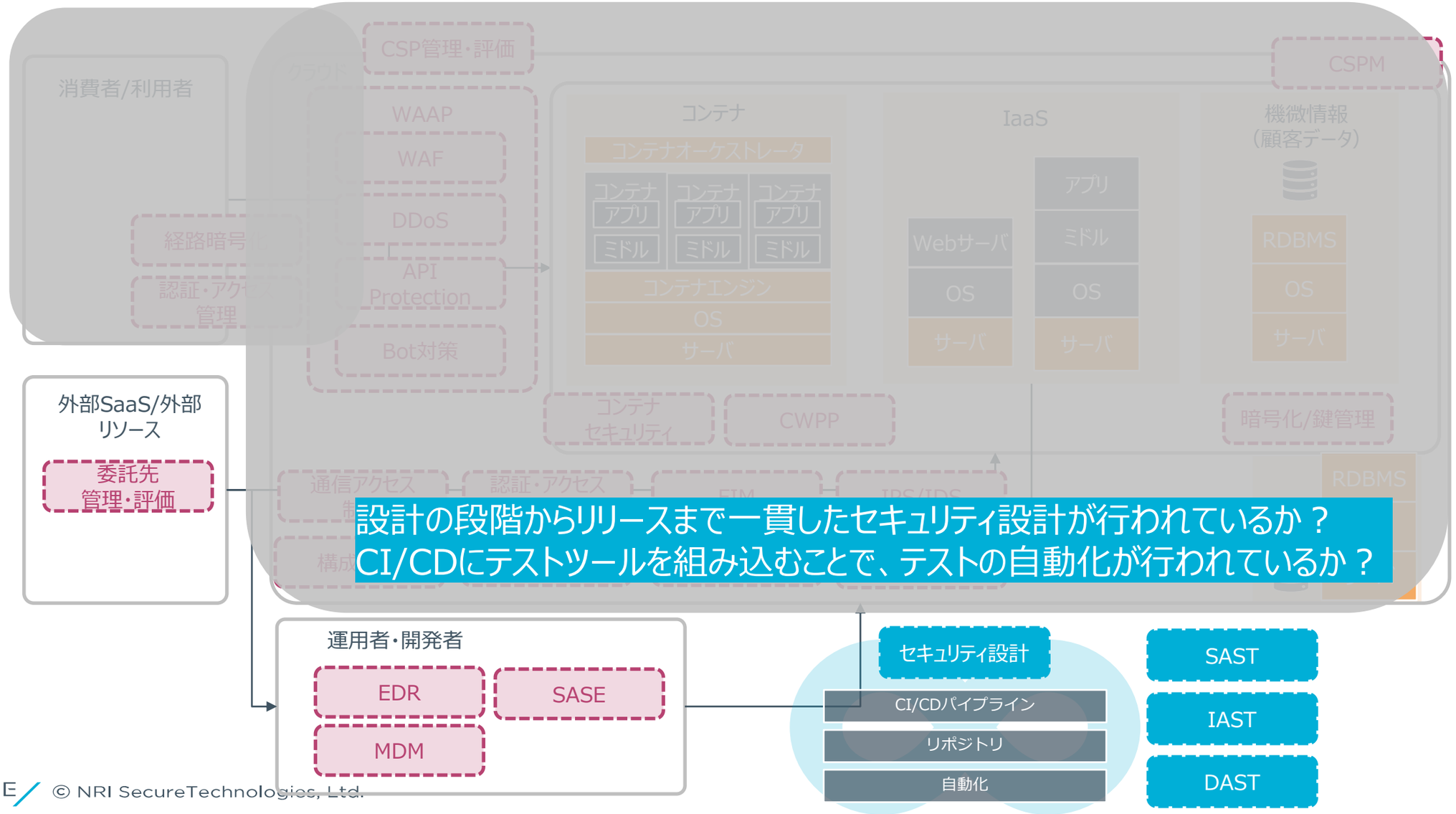
開発におけるセキュリティ対策の重要なポイント①

セキュリティの全体像(イメージ)



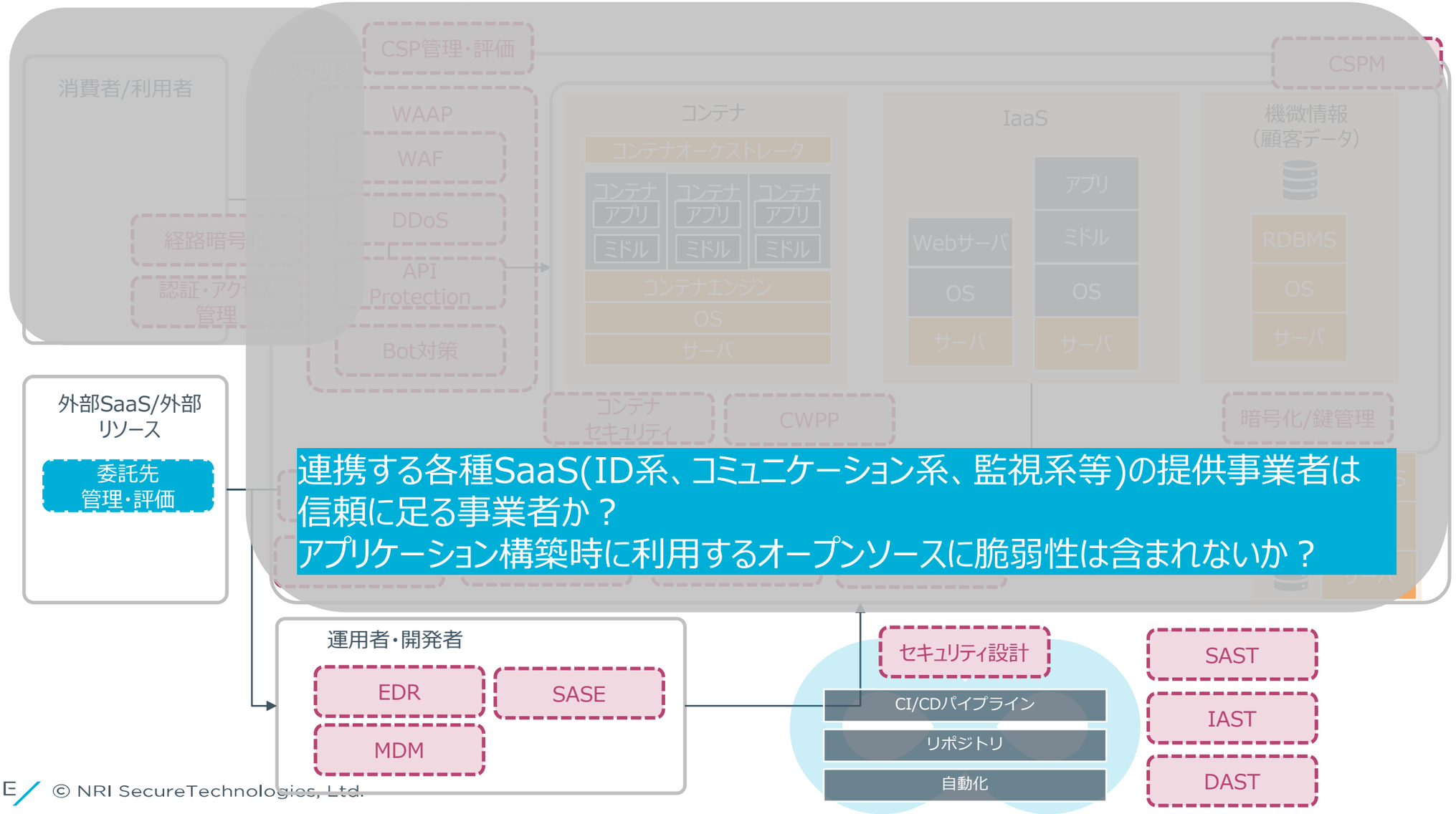
開発におけるセキュリティ対策の重要なポイント②

セキュリティの全体像(イメージ)



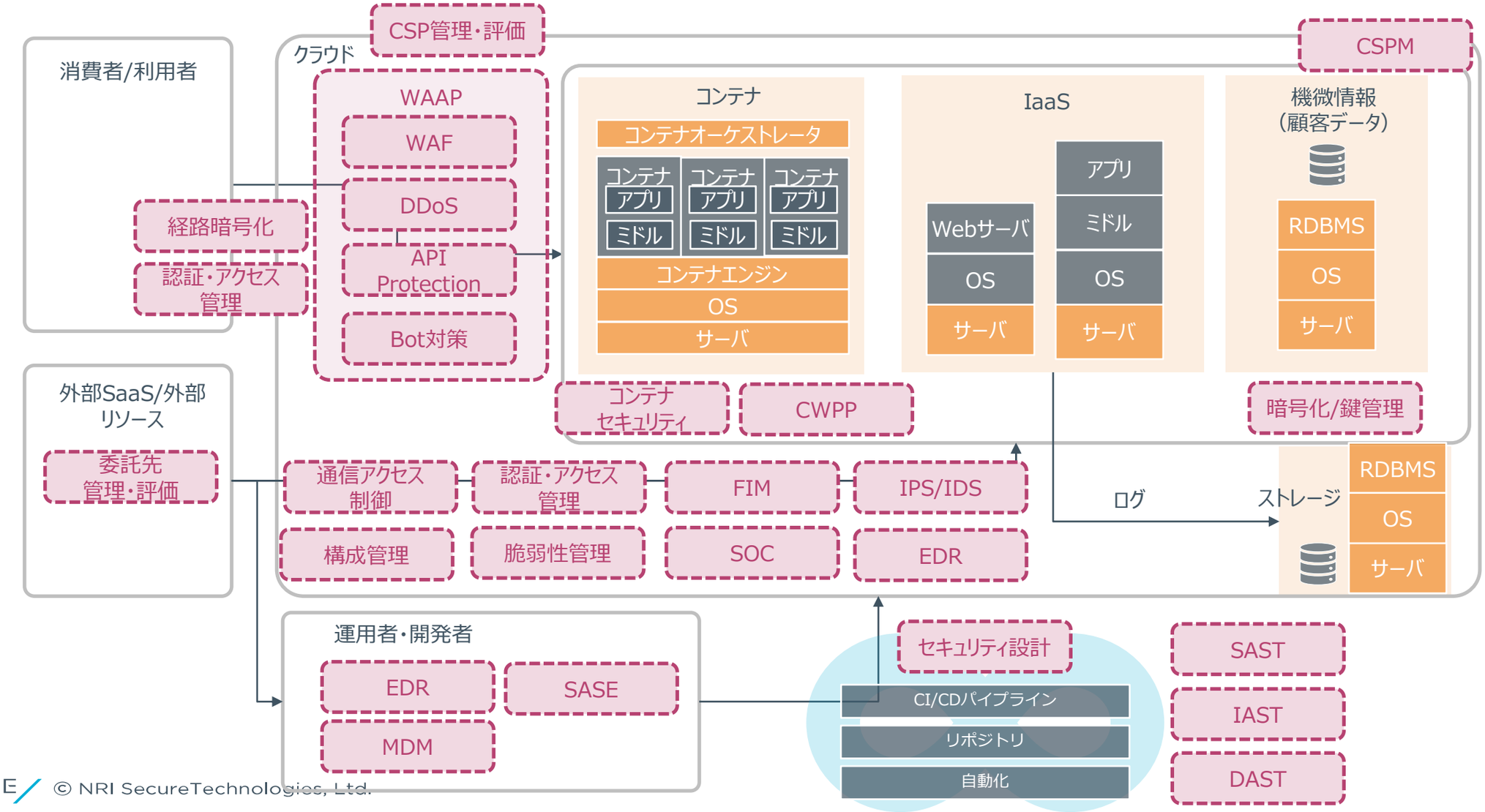
開発におけるセキュリティ対策の重要なポイント③

セキュリティの全体像(イメージ)



DX時代に求められるセキュリティ対策の全体像（再掲）

セキュリティの全体像(イメージ)



DX時代に必要なセキュリティ対策

- **クラウドでのセキュリティ対策**
  - クラウドサービス事業者の信頼性の確保
  - 責任範囲の明確化とモニタリング
  - オンプレとクラウドの違いを理解したうえでのセキュリティ設計・運用
- **開発におけるセキュリティ対策**
  - 開発サイクルの高速化・DevOpsへの対応
  - リモートワークでの開発への対応
  - サプライチェーンリスクへの対応

やるべき対策は多い。

自社の環境・サービスにあわせて、リスクベースで環境を評価して、

効果的な対策を優先度をつけて実行していく必要がある。

PCI DSS準拠におけるポイント

PCI DSS準拠におけるポイント

クラウド環境においてPCI DSS準拠する上で重要なこと

1 PCI DSS準拠対象スコープの明確化

利用するサービス・構成、およびPANの流れを明らかにしてPCI DSSスコープを明らかにすること。クラウドではコンポーネントが抽象化されているため、境界が不明瞭になっていることが多い。
境界になっているポイント・技術を洗い出すことが重要。

2 ユーザ側の責任範囲の明確化

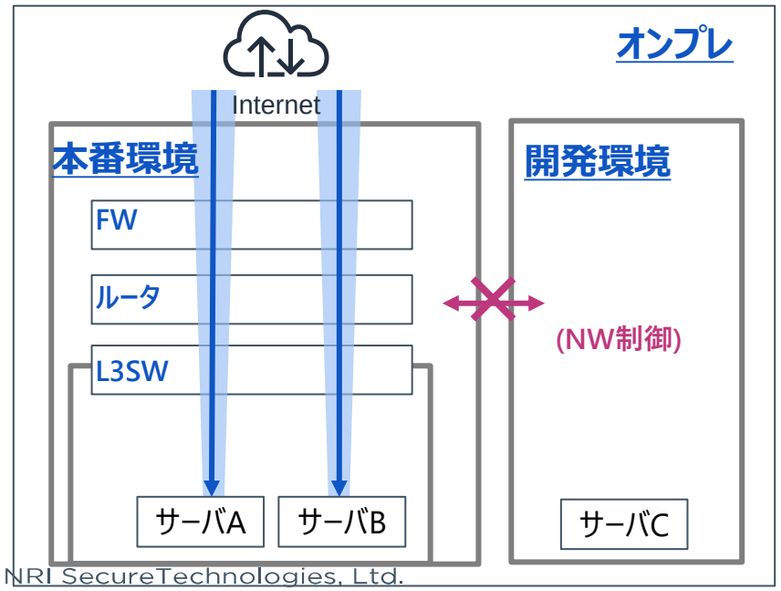
利用するサービス・構成が明確化された場合は、どのレイヤ（OS・ミドル・アプリ）までがユーザの責任範囲なのかを明らかにすること。
クラウド事業者によってはPCI DSS上の責任分界点が記載されたResponsibility Summaryが公開されているため必ず確認する必要がある。また、ユーザ側にて設定できる項目は確認する必要がある。

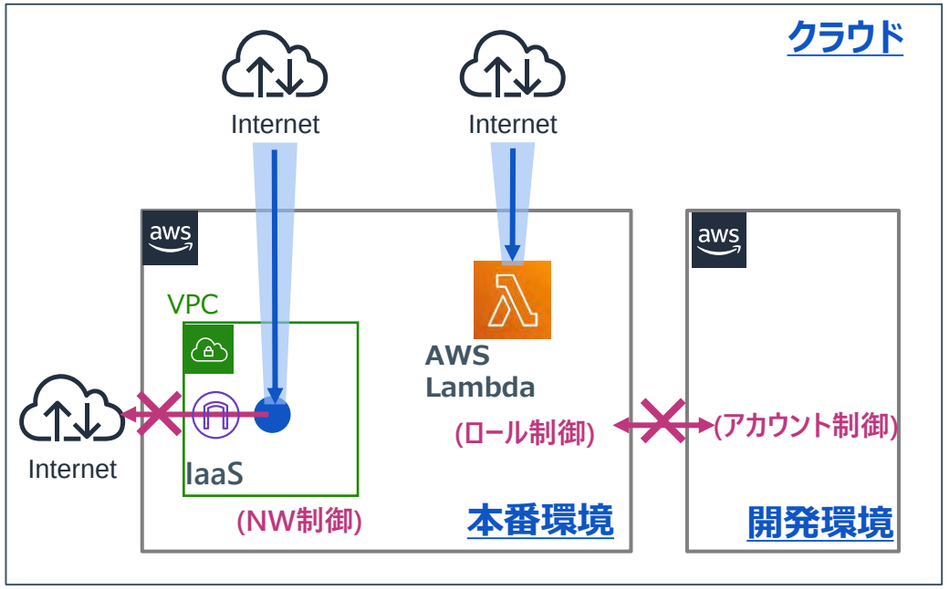
3 PCI DSS要件と利用されている技術の確認

スコープと責任範囲が明確化されたあとは、準拠を行うための技術的対策と要件のマッピングを行い、準拠性を確認する。

PCI DSS準拠におけるポイント①

- **PCI DSS準拠対象スコープの明確化**
  - 課題
    - 本番環境と開発環境が同一の契約（アカウント）に紐づいていることによるスコープの拡大
    - CDE（カード会員データ環境）とnon-CDEのコンポーネントが混在していることによるPCI DSSスコープが不明瞭になる
  - 対策
    - 本番環境と開発環境で別契約（別プロジェクト）とすることで、そもそも本番環境と開発環境を分離する
    - 従来のネットワークレイヤでのセグメンテーションのほかに、アプリケーションレイヤやアカウントレイヤ（IAM）レベルで環境分離を行う必要がある。





PCI DSS準拠におけるポイント②

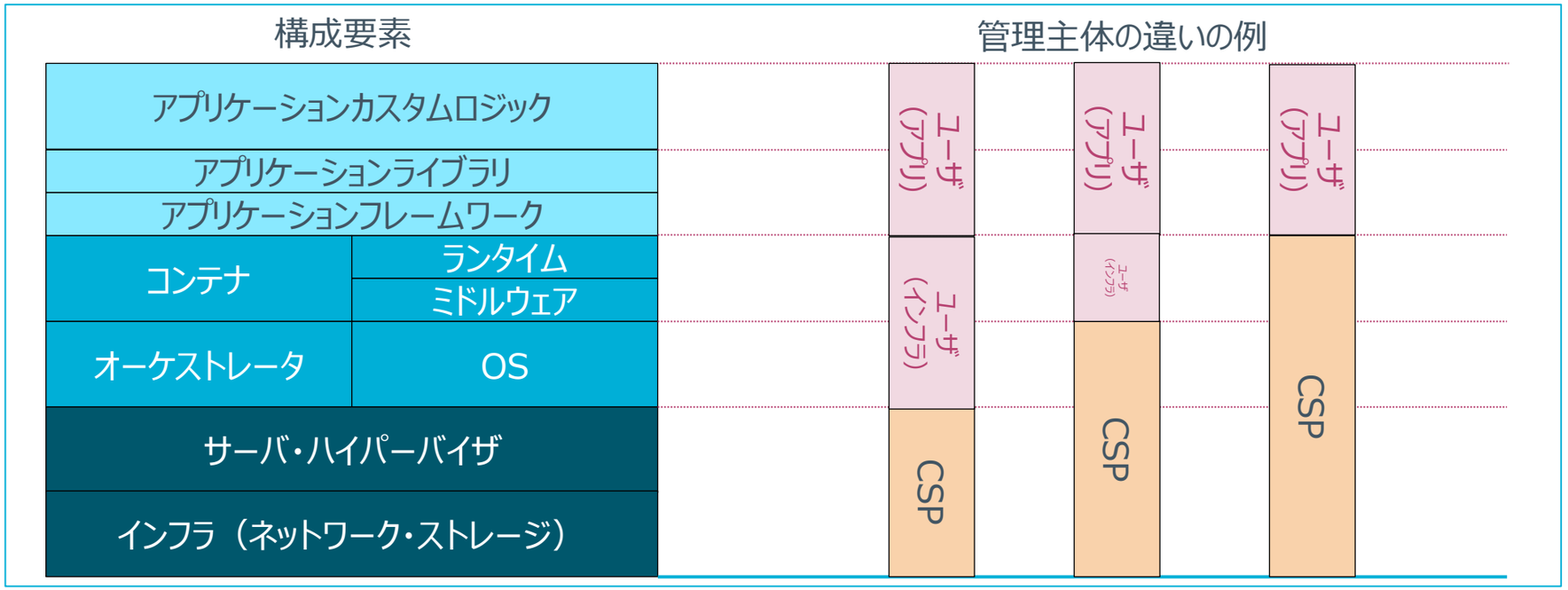
ユーザ側の責任範囲の明確化

課題

- 利用するサービス・環境の複雑化により、管理対象のOS、ソフトウェア、ライブラリの把握が困難なことに起因する脆弱性情報の収集漏れ

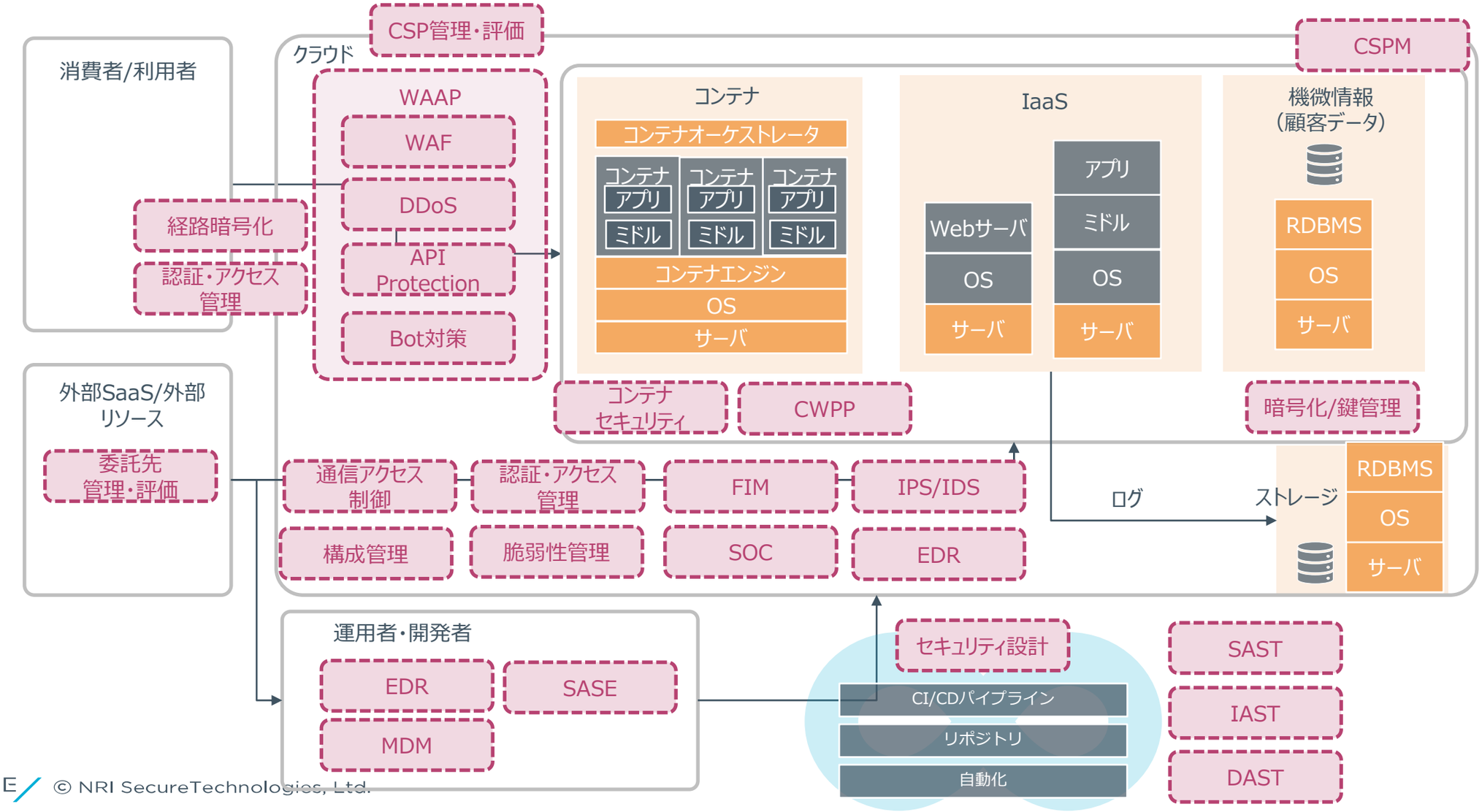
対策

- 責任範囲を明確化し、インベントリ管理および脆弱性情報の収集の自動化を行う



PCI DSS準拠におけるポイント③

PCI DSS要件と利用されている技術の確認



PCI DSS準拠におけるポイント③

PCI DSS要件と利用されている技術の確認

	v4.0	セキュリティ対策				
要件 1	ネットワークセキュリティコントロールの導入と維持	通信アクセス制御	認証・アクセス管理	SASE	MDM	セキュリティ設計・コンテナセキュリティ
要件 2	すべてのシステムコンポーネントに安全な設定を適用する	CSPM	構成管理			
要件 3	保存されたアカウントデータの保護	暗号化/鍵管理				
要件 4	オープンな公共ネットワークでの送信時に、強力な暗号化技術でカード会員データを保護する	経路暗号化	通信アクセス制御			
要件 5	悪意のあるソフトウェアからすべてのシステムおよびネットワークを保護する	EDR	CWPP	SASE	MDM	
要件 6	安全なシステムおよびソフトウェアの開発と維持	WAF	xAST	IPS/IDS	脆弱性管理	
要件 7	システムコンポーネントおよびカード会員データへのアクセスを、知る必要のある業務によって制限する	認証・アクセス管理				
要件 8	ユーザーの識別とシステムコンポーネントへのアクセスの認証	認証・アクセス管理				
要件 9	カード会員データへの物理アクセスを制限する					
要件 10	システムコンポーネントおよびカード会員データへのすべてのアクセスをログに記録し、監視すること	SOC				
要件 11	システムおよびネットワークのセキュリティを定期的にテストする					
要件 12	組織の方針とプログラムによって情報セキュリティをサポートする	委託先管理・評価	CSP管理・評価			

PCI DSS準拠におけるポイント（再掲）

クラウド環境においてPCI DSS準拠する上で重要なこと

1 PCI DSS準拠対象 スコープの明確化	利用するサービス・構成、およびPANの流れを明らかにして PCI DSSスコープを明らかにすること。クラウドではコンポーネントが抽象化されているため、境界が不明瞭になっていることが多い。 境界になっているポイント・技術を洗い出すことが重要。
2 ユーザ側の 責任範囲の明確化	利用するサービス・構成が明確化された場合は、どのレイヤ（OS・ミドル・アプリ）までがユーザの責任範囲なのかを明らかにすること。 クラウド事業者によってはPCI DSS上の責任分界点が記載されたResponsibility Summaryが公開されているため必ず確認する必要がある。また、ユーザ側にて設定できる項目は確認する必要がある。
3 PCI DSS要件と 利用されている技術の確認	スコープと責任範囲が明確化されたあとは、準拠を行うための技術的対策と要件のマッピングを行い、準拠性を確認する。

まとめ

まとめ

- **本日お伝えしたいこと**
  - DX時代になり、企業は生き残り戦略のため価値の高いサービスを迅速に提供することが重要
  - その中で、システムそのもの、またシステム開発の有り様が大きく変化している
  - DX時代のセキュリティ対策は、「クラウドでのセキュリティ」、「システム開発におけるセキュリティ」の2軸で検討する必要がある
  - PCI DSS準拠にあたっては、クラウドの特性と技術を理解しながら進めていく必要がある

NRIセキュアでは、安全・安心なIT社会を実現するために、日々技術と知見を磨き続けています。
セキュリティ対策について悩まれることがあれば、お客様と一緒に課題解決を図っていきます。
是非、一度ご相談ください。

NRI SECURE