

DBSC早春セミナー

～ 個人情報保護法改正と越境問題 ～

企業紹介①

“NHNテコラスが提供するクラウド移行・運用支援とセキュリティ対策”

2022.3.2

NHN テコラス株式会社

マーケティング本部 Aegis Wall事業推進部

李 敏碩

目次

- 最新の情報セキュリティ事情
- クラウドシフトを支えるNHNテコラスのサービス
- 企業ガバナンス確保と特権IDアクセス管理のセキュリティソリューション『Aegis Wall』

最新の情報セキュリティ状況

「デジタルトランスフォーメーション（DX）」

サプライチェーン・

ニューノーマルな働き方・内部不正

→ 「ゼロトラスト」

個人情報保護法の改正

PCI DSS v4.0初版リリース

地政学的不安要素

2021年のサイバー犯罪検挙数は1万2275件 - 前年比25%増

- 2021年のサイバー犯罪検挙数は1万2257件と1万件の大台を突破し、前年の1.25倍へ拡大
※速報値
- 2017年以降、9000件台で緩やかに増加してきたが、2021年は目立って増加
- オンラインバンキングにおける不正送金は件数も被害額も減少
- 一方、ランサムウェアの被害報告増加
業種別では「製造業」・「卸売、小売業」・「サービス業」・「建設業」の順

※令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）：
警察庁、[R4.2.10掲載]
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

機密情報の悪用事例

【コンピュータウイルス・不正アクセスの届出事例 [2021年上半期 (1月~6月)]】

IDとパスワードによる認証を突破された不正アクセス	31	24%
身代金を要求するサイバー攻撃の被害	30	23%
脆弱性や設定不備を悪用された不正アクセス	24	19%
サプライチェーンに関するインシデント	23	18%
コンピュータウイルスの検知・感染被害	14	11%
その他	6	5%
合計	128	

- ・ ID やパスワードの管理不備や強度不足により認証を突破された事例や、脆弱性やセキュリティ設定の不備を悪用された事例が多い
- ・ 業務委託先サーバへの侵害や、SaaS (Software as a Service) 基盤利用時の設定不備による情報漏洩など、自組織のシステム管理者や利用者だけでは直接の対策が難しいサプライチェーンに関するインシデントの届出も

※「コンピュータウイルス・不正アクセスの届出事例 [2021年上半期 (1月~6月)]」より
：独立行政法人情報処理推進機構 セキュリティセンター、2021年8月23日
<https://www.ipa.go.jp/security/outline/todokede-j.html>

「情報セキュリティ10大脅威 2022」を公開

順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
↑ 3位	サプライチェーン の弱点を悪用した攻撃	4位
↓ 4位	テレワーク等の ニューノーマルな働き方 を狙った攻撃	3位
↑ 5位	内部不正 による情報漏えい	6位
6位	脆弱性対策情報の公開に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

※「情報セキュリティ10大脅威 2022」より
：独立行政法人情報処理推進機構、2022年1月27日更新
<https://www.ipa.go.jp/security/vuln/10threats2022.html>

2022年4月に改正個人情報保護法が施行

国内で改正個人情報保護法の全面施行（令和4年4月1日より）

- **本人の権利強化**

- **データ利活用の促進**

- **法人への報告義務、罰則・罰金大幅に強化**

漏えい等が発生し、個人の権利利益を害するおそれがある場合に、

委員会への報告及び本人への通知を義務化

命令への違反：30万円以下⇒1億円以下

個人情報データベース等の不正提供：50万円以下⇒1億円以下

虚偽報告：無罰則⇒50万円以下

- **越境移転など法の域外適用**

※「令和2年改正個人情報保護法について」より
：個人情報保護委員会（PPC）
<https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/>

「PCI-DSS v4.0」改訂のポイント

1. 6つの目標・12のセキュリティ要件はそのまま維持の方向
2. セキュリティ強化のための要件追加・更新

例：

- リスク管理プロセスのより明確化
- 組織に指針提供の為のリスクアセスメント要件更新
- サービスプロバイダー向け要件追加
- クラウドサービスの要件への取り組み

PCI DSS準拠のポイント(技術的対策)

■ アクセス管理の要件

要件7	カード会員データへのアクセスを業務上の必要範囲内に制限すること
要件8	コンピュータにアクセスする利用者ごとに個別のIDを割り当てること
要件9	カード会員データへの物理アクセスを制限する

■ ネットワーク監視の要件

要件10	ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること
------	--

その他、参考

「DX時代における企業のプライバシーガバナンスガイドブック (ver1.2)」策定

経済産業省・総務省

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000140.html

「金融分野におけるサイバーセキュリティ強化に向けた取組方針」アップデート (Ver. 3.0)

金融庁

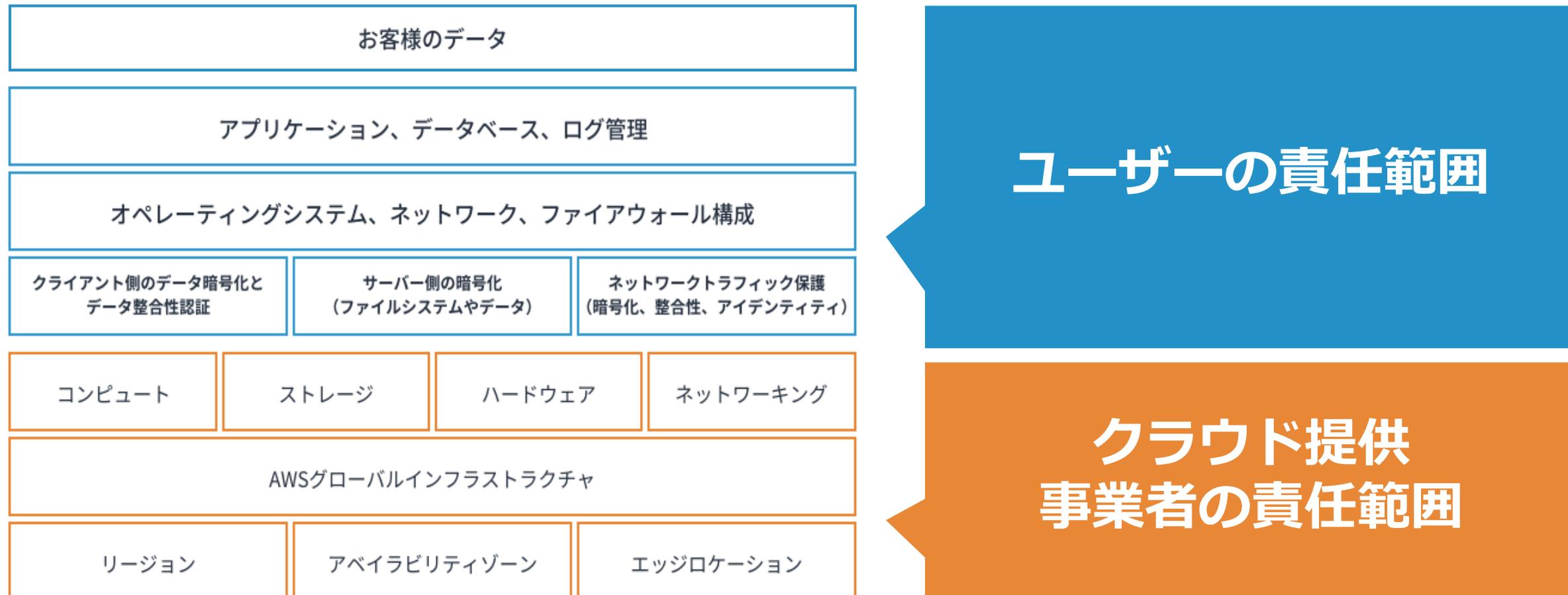
<https://www.fsa.go.jp/news/r3/cyber/torikumi2022.html>

クラウドサービスの利活用とセキュリティ

なぜクラウドサービス？

- 数多のサービスから必要なサービスを選び、必要な時に、必要な分だけ、利用することが出来る
- 初期費用をかけず、すぐに初めて、すぐにやめることもできる
- **設備やハードウェア面の各種セキュリティ基準をクラウド事業者側が準拠**している

クラウドにおいて責任範囲に応じた対応が必要

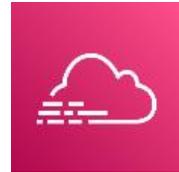


- クラウドのサービスを理解したうえでケースに応じて対応が必要
 - アップデートの多いクラウドサービスをすべて理解するには学習コストがかかる
 - インシデント発生時に素早い対応に不安がある

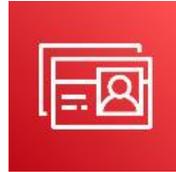
出来ることはたくさんある



AWS Trusted Advisor



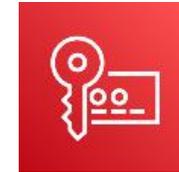
AWS CloudTrail



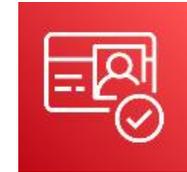
AWS Directory Service



AWS Identity and Access Management (IAM)



AWS Key Management Service (AWS KMS)



Amazon Cognito



AWS Firewall Manager



AWS Audit Manager



Amazon Inspector



AWS Secrets Manager



AWS Security Hub



AWS Shield



Amazon Cloud Directory



AWS Artifact



AWS Certificate Manager (ACM)



AWS CloudHSM



Amazon GuardDuty



AWS Network Firewall



Amazon Macie



AWS WAF



AWS Single Sign-On



AWS Resource Access Manager



Amazon Detective



AWS Signer

どうすればいい？

- 数多のサービスから必要なサービスを選び、必要な時に、必要な分だけ、利用することが出来る
- 初期費用をかけず、すぐに初めて、すぐにやめることもできる
- 設備やハードウェア面の各種セキュリティ基準をクラウド事業者側が準拠している

**クラウドのセキュリティ・ガバナンス強化するには
何から取り掛かればいいのか？**

NHN テコラス株式会社

クラウド、データセンター、データサイエンス。

合理的なITインフラ、プロフェッショナルサービスとデータ活用により新しいビジネスの創造を支援します。

会社名	NHN テコラス株式会社（英表記：NHN Techorus Corp.）
代表者	代表取締役社長 白倉 章照
代表番号	03-5155-0111
所在地	・本社 〒105-6322 東京都港区虎ノ門一丁目23番1号 虎ノ門ヒルズ森タワー22階 ・大阪オフィス 〒530-0002 大阪府大阪市北区曾根崎新地1-13-22 御堂筋フロンティア1階
設立	2007年4月
資本金	21億円
事業内容	ITインフラ・ソリューション事業
社員数	169名（2021年6月現在）

グローバル展開のNHNグループにおける
クラウド中核事業会社



AWS最上位パートナーランク

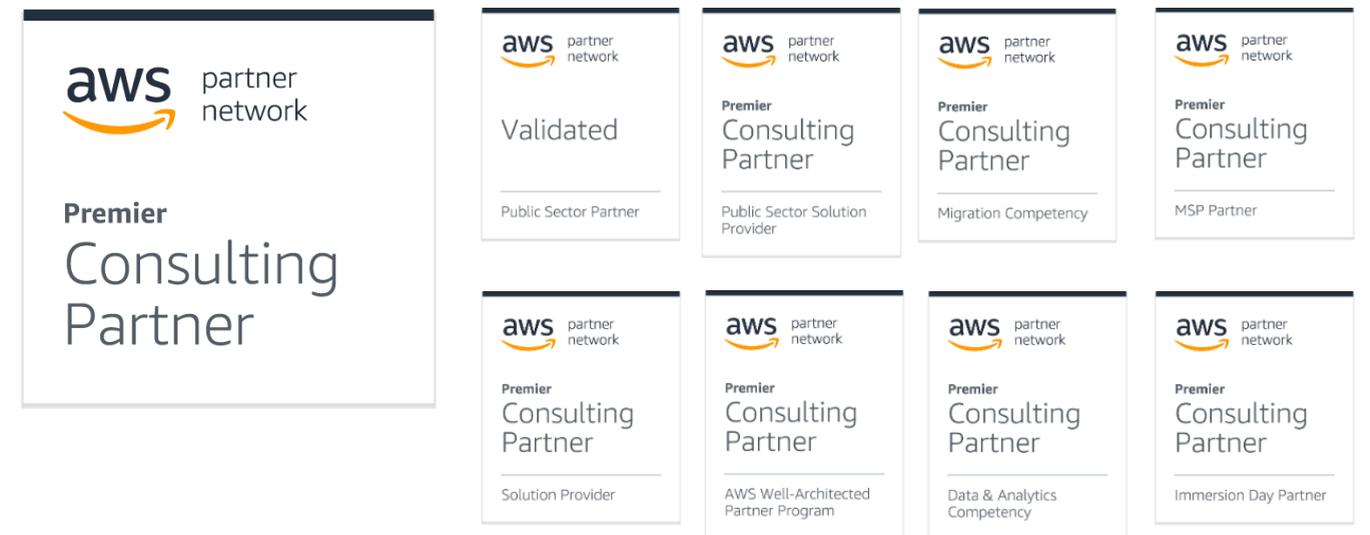
AWSパートナーネットワークの最上位 AWSプレミアコンサルティングパートナー

【AWSコンピテンシー】

- データと分析のコンサルティングコンピテンシー
- 移行のコンサルティングコンピテンシー

【パートナープログラム】

- マネージドサービスプロバイダー
- Well Architected
- APN Immersion Day
- AWS ソリューションプロバイダープログラム
- AWS 公共部門パートナー
- AWS ソリューションプロバイダー



AWS総合支援サービス C-Chorus



AWSの素晴らしさはそのままに
コスト削減と利便性向上という付加価値を

リセールサービス

- ・ 料金割引
- ・ 技術サポート
- ・ クラウド保険等

AWSを安く安全に

マネージドサービス

- ・ 導入、移行支援
- ・ 技術支援、コンサルティング
- ・ 運用管理代行、継続的最適化
- ・ エンジニア作業代行
- ・ セキュリティ、ガバナンス対策

必要な時に
必要なご支援を



2千契約
以上

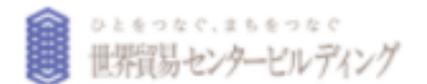
ソリューション・特定業種向け

- ・ 機械学習、ビッグデータ
- ・ ネットワーク
- ・ for 公共・教育機関
- ・ for モバイルゲーム
- ・ for スタートアップ企業

・ 特定領域
・ 特定業種向け

導入実績

様々な業種・業態のお客様にご利用いただいています



C-Chorusのマネージドセキュリティ

クラウド上で稼働するシステムのセキュリティ対策を支援します



ニーズに合わせて選べるセキュリティサービス

プロフェッショナルサービス



AWSセキュリティの ベストプラクティス

AWSサービスを活用しWell-Architected Frameworkに基づいたセキュリティの最適化やログの集中管理など総合的なセキュリティ対策を提案

Aegis Wall



特権ID管理・データベース監査

特権IDユーザーのアクセス管理の効率化を実現。不正アクセスや内外からの情報漏洩対策、特権ID管理に必要な機能を提供。個人情報保護法やISMS認証など企業ガバナンス対応をサポート。

Webアプリケーション脆弱性診断



専門家による脆弱性診断評価

セキュリティ専門家が様々な観点からWebアプリケーションに対する脆弱性診断評価を行い、Webアプリケーションの安全性を徹底的に調査します。

BLUE Sphere



クラウド型WAF

Webサービスの攻撃を防ぐWAF機能をはじめ、DDoS攻撃の防御やWebサイトの改ざん検知をまとめて導入できます。

WafCharm



AWS WAF自動運用支援

AWS WAFの自動運用サービス。AIによって攻撃パターンを学習しルールを最適化するため、新規の脆弱性対応を手軽に実現できます。

Workload Security※



多層防御・脆弱性対策

多層防御・脆弱性対策を提供するクラウド型のセキュリティサービスの導入、構築、運用を支援します。

※旧称：Deep Security as a Service

Well-Architected レビュー

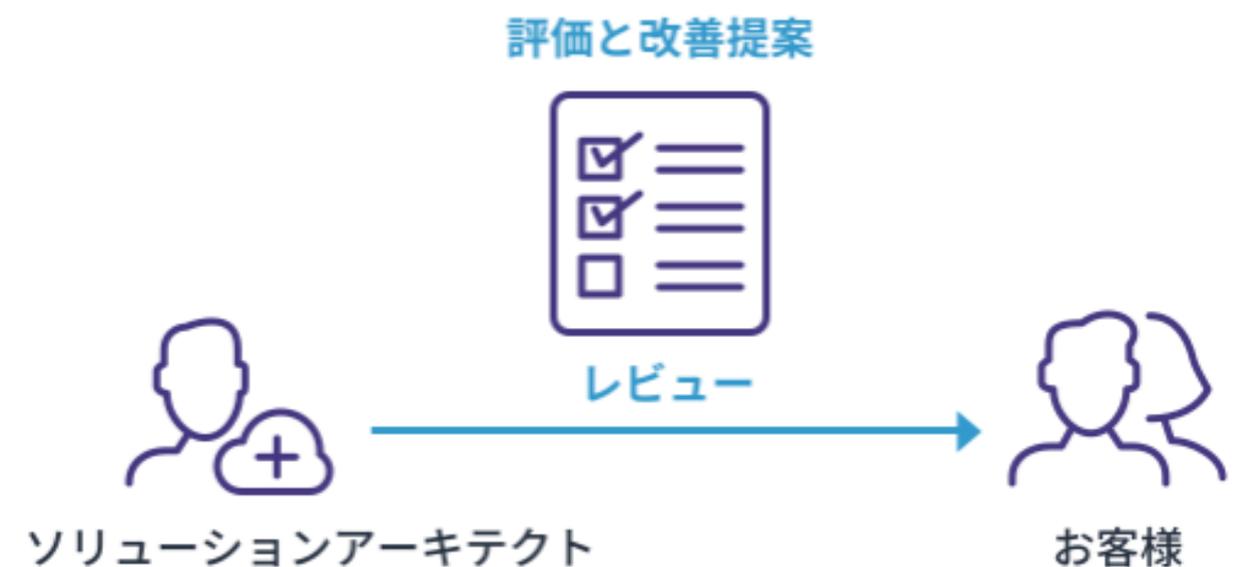
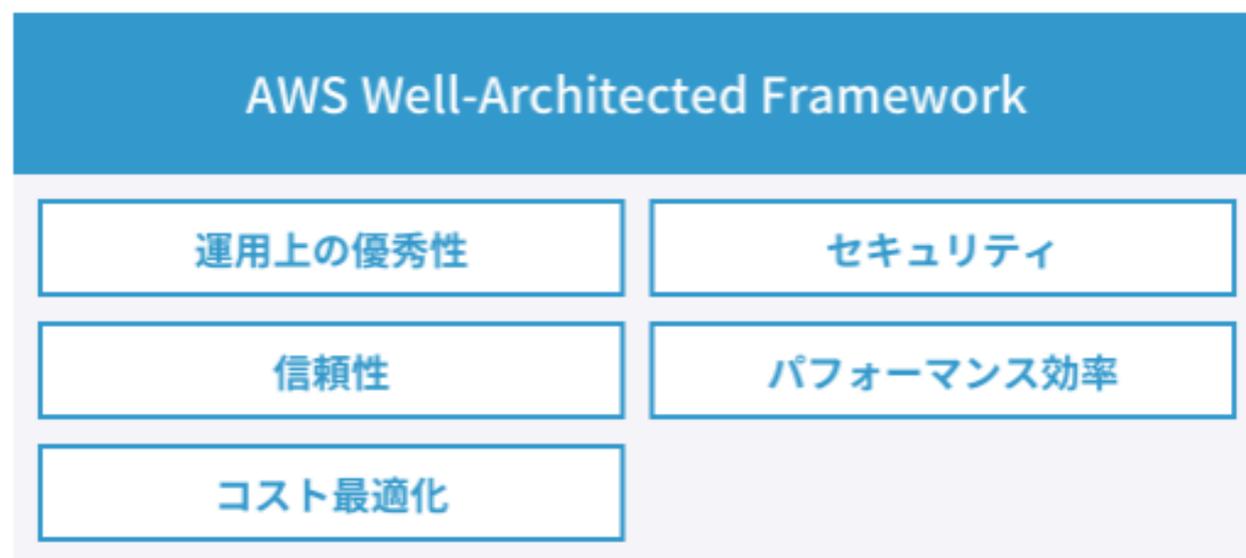
AWS 利用のベストプラクティス実践フレームワークに基づいたワークロードの診断・監査

AWS 稼働状況の診断・監査サービス

AWS Well-Architected Frameworkに基づいてお客様のAWS上でのワークロードの診断・監査を実施し結果をレビューします。AWSの定めるフレームワークに準拠した第三者レビューにより改善項目やその手法についてアドバイスを受けることができ、より最適な環境の実現に役立ちます。

レビューは AWS 公式の Well-Architected Toolに加え、300項目以上の自動精査が可能な当社ツールなどを利用することで、データに基づいたワークロードの評価レポートを提出します。

ソリューションアーキテクトがレビュー会を実施し、レポートとともに改善機会を特定のうえで、その手法やプロセスについて支援します。



セキュリティソリューション『Aegis Wall』

特権アクセス管理・データベース監査ソフトウェア

— Aegis Wallの3大機能

特権ユーザー・アクセス管理

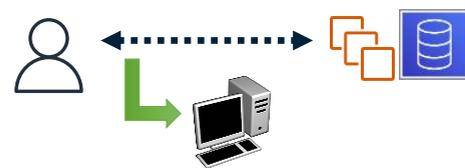
- PC/WEB AgentのIDで**使用者個人を特定**
- ワンタイムパスワードによる二段階認証も可



共有ID/PWで利用されていて
個人識別できないことが多い

ログ管理

- いつ・誰が・何をしたかを正確に記録
- 検索や**動画によるセッション再現**も可能
- 各種レポートの用意



パケットキャプチャ方式で
パフォーマンス負荷0%

アクセス・コマンド権限制御

- 正規ユーザー以外のアクセスを遮断
- テーブル・カラム単位での制御が可能
- ワークフローで作業申請を効率的に管理



- クエリ・コマンドなどユーザーの操作内容に対するルール設定、マイナンバーなどの重要データの**マスキング**も可能



DBからの戻り値を
マスキング

***** ← 0123456

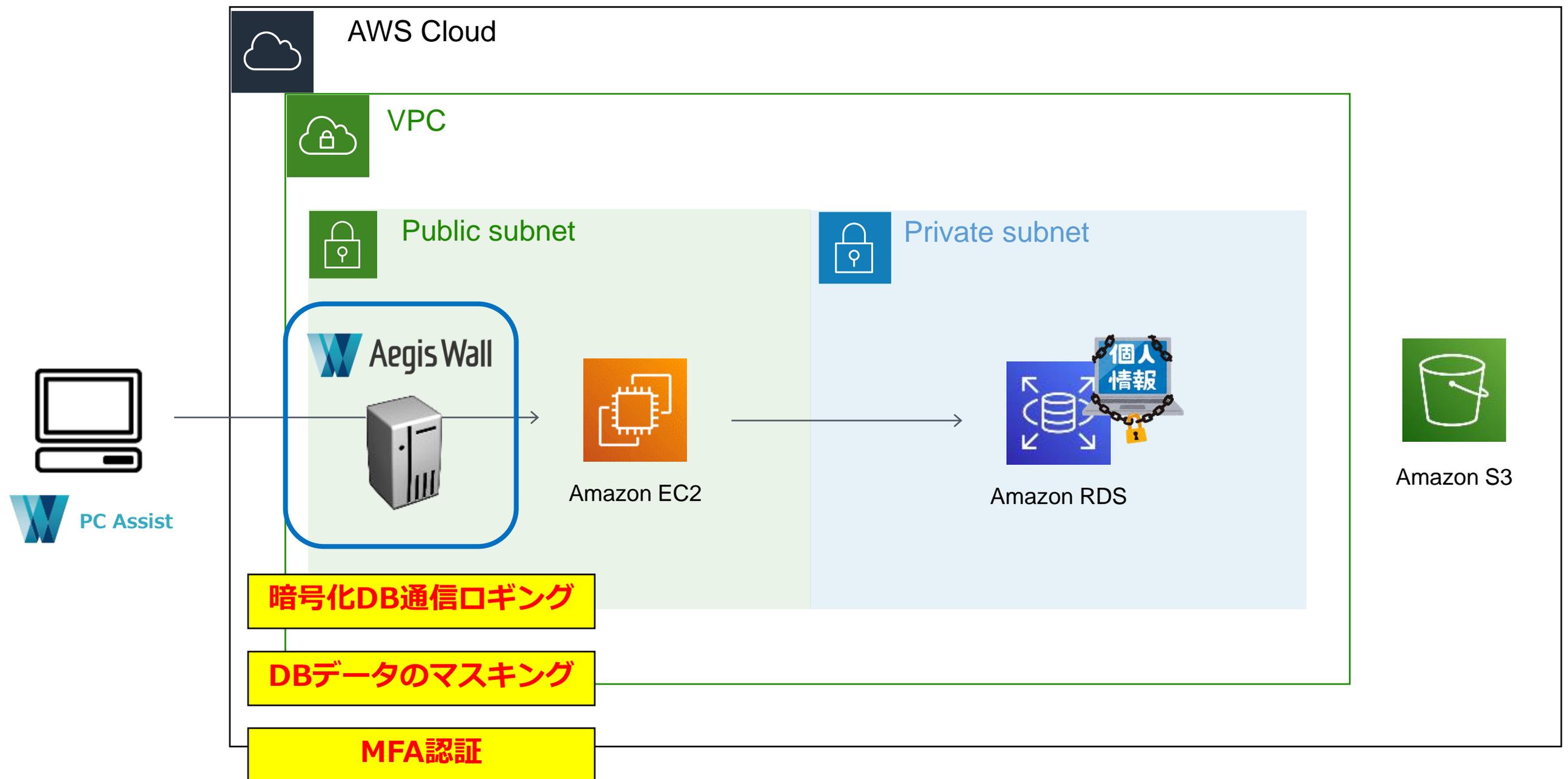


Aegis WallはAWSの技術検証レビューを通過した
認定ソフトウェアです。

ハイブリッド環境でも、Aegis Wallであれば一元管理が可能

ゼロトラスト時代に、簡単かつ安価に始められるセキュリティソリューション

セキュリティソリューション『Aegis Wall』



- 不正アクセス可能性の減少、DBや機微情報にアクセスする作業者の心理的安心感
⇒ **万が一の大事に至りにくい、システム・作業者負担減らす**

Aegis Wall事例

プロシューマー・ハピネス
FANCOM 株式会社ファンコミュニケーションズ様

セキュリティ強化施策の一環で、 ログの抜け漏れ防止や監査作業の効率化を検討

- セキュリティに関して第三者機関の監査を受けており、監査のためにデータの整理が課題に・・・
 - 誰がいつアクセスをしてどのような操作をしたかを記録し、メールで送信
 - メール送信の際の書式が統一されていないので、監査項目の抜け漏れが発生
 - データの整理にも時間がかかる
 - エンジニアの安全性を担保する「守る」ために明確な記録を残したい

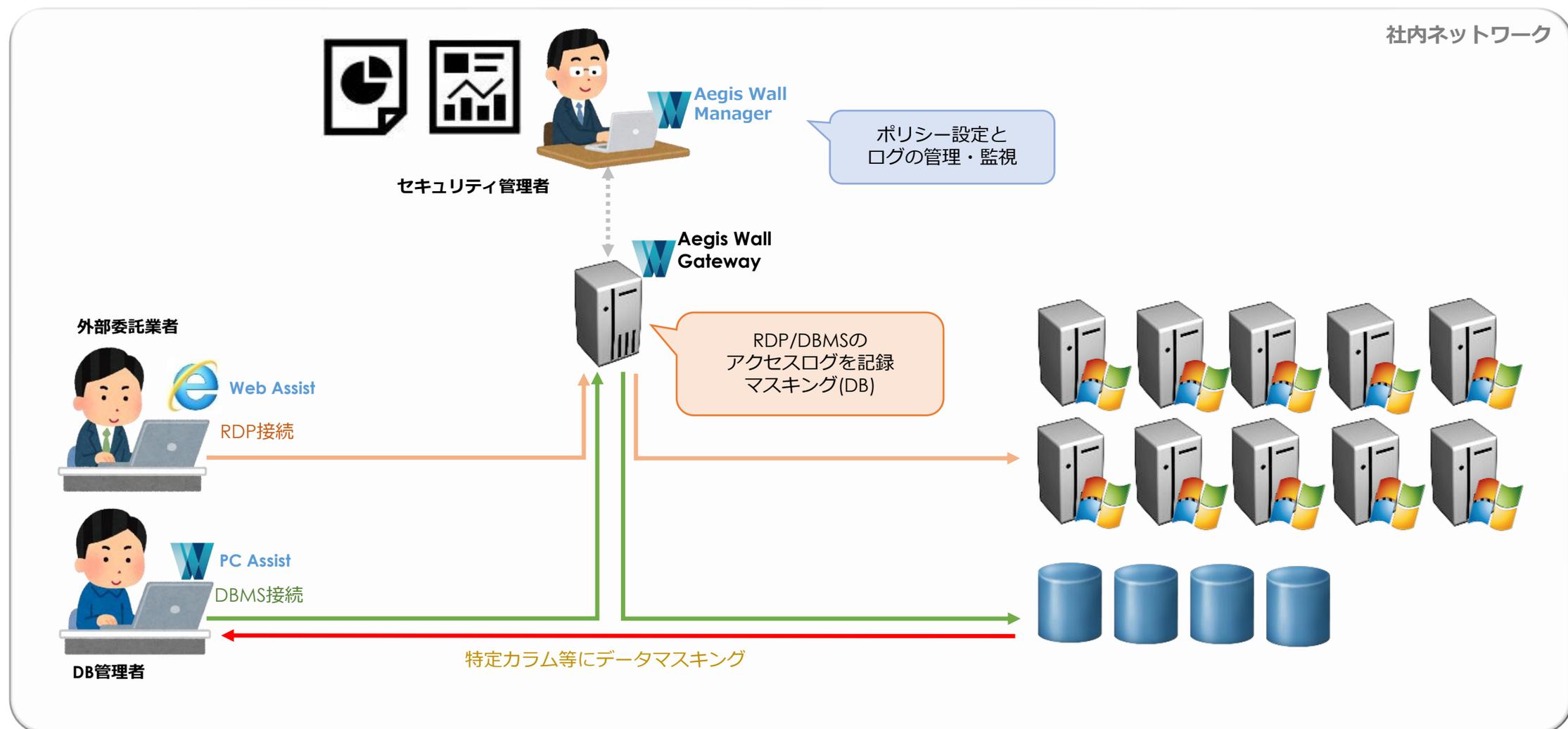
そこで、Aegis Wallのログ管理を利用



Aegis Wall事例

内部統制の強化（地方官庁 様）

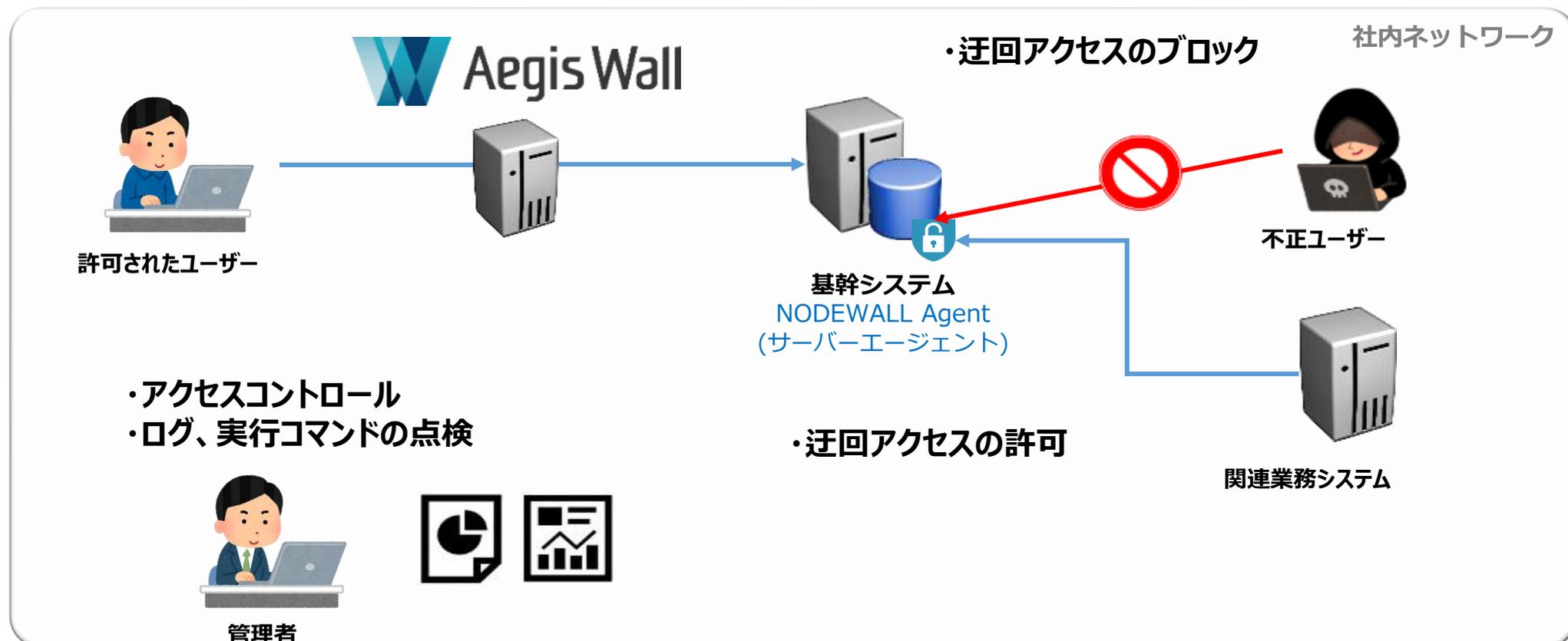
導入目的	ITガバナンス強化の一環として、サーバールームに出入するベンダーの作業内容のログを記録し、アクセス可能なデータの範囲を必要最小限に制限する
環境・構成	DB4台 + Windowsサーバ80台 WindowsサーバはWeb Assistを使用してエージェントレスでの運用
選定ポイント	コマンド単位での権限制御、データマスキングによる個人情報保護など、他社のログ記録やアクセス管理製品ではカバーできない機能を備えていたこと



Aegis Wall事例

セキュリティ強化と内部統制監査対応（ユニチカ株式会社 様、製造業）

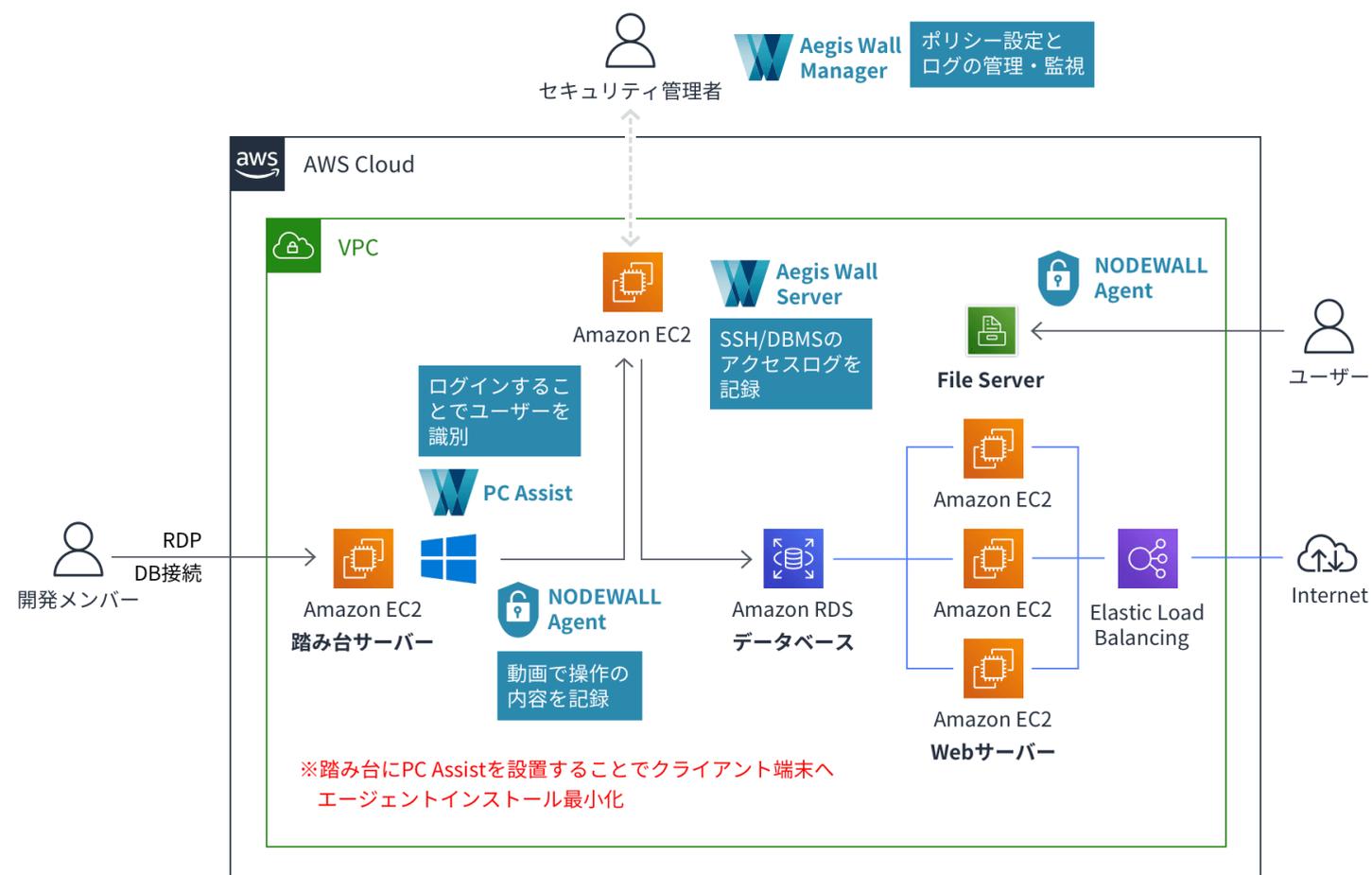
導入目的	グループ全体で約3,700人の従業員の業務を支える基幹システムのセキュリティ強化、および内部統制監査に対応するための、アクセス管理・ログ管理の重要性を感じた為
環境・構成	Windowsサーバー数十台+DB数台（順次、拡大中） Gatewayでサーバー・DBのログ記録と監視部門毎職務に応じたアクセス制限とレポート
選定ポイント	・コストと納期 ・アクセス経路を問わず個人特定し、管理ができる点 -2ヶ月以内という短期間での導入が可能 -管理画面操作・レポート出力が簡単



Aegis Wall事例

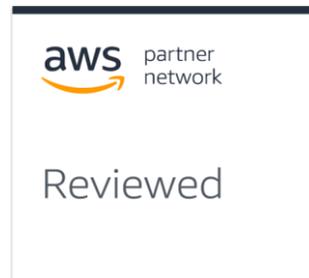
AWS環境の監査対応（株式会社HANATOUR JAPAN 様、旅行業）

導入目的	上場に伴う外部監査対応と内部統制強化の為、AWS上に構築された、DBとファイルサーバーへのアクセス・作業内容を記録・管理するため
環境・構成	DB 10台、File Server 1台 データベースサーバーリモート接続とファイルサーバー1台へのファイルアクセスを監視
選定ポイント	AWS環境の基本となる踏み台構成に適した設計 導入前評価と導入後運用へのサポートの迅速さと機能・監視対象の将来的拡張性



Aegis Wall for Cloud リリース記念キャンペーン

Aegis WallはAWSの技術検証レビュー通過ソフトウェア



Aegis WallはAWS上に展開するワークロードの、セキュリティ、信頼性、運用の優秀性に関するリスクを検証する技術検証レビューであるAWSファンデーションショナルテクニカルレビュー (FTR)を通過しました。

Aegis Wall
AWS上の特権ユーザーによるアクセス管理ソフト
リリース記念キャンペーン

**導入オプション
サービス無料**

期間限定 2022年3月31日まで

The banner features an illustration of a person sitting on a server rack, working on a laptop. A large red padlock is shown on the screen, symbolizing security. The background is a light blue gradient with gears and a cloud.

Aegis Wall for Cloud リリース記念キャンペーン 導入オプションサービス無料	
監視対象サーバへのエージェント設置	Aegis Wallセキュアゲートウェイの監視対象ホストへエージェント導入作業を代行
踏み台サーバへのエージェント設置	踏み台サーバへのエージェントインストールおよびAegis Wallサーバとの疎通/動作確認
特権アカウント情報登録代行	Aegis Wallシステムへの特権アクセスユーザ情報登録作業を代行
追加ハンズオントレーニング	ご担当者変更時等、Aegis Wallに関するハンズオントレーニングを実施

ご提供ライセンス※1例	標準価格 単年(12ヶ月)契約プラン
Small ~ 5ホスト	¥300,000
Medium ~ 10ホスト	¥600,000
Large ~ 15ホスト	¥900,000

お客様よりのお引合い・お声

1.7倍↑

※21年6月～12月
弊社調べ(20年同期比)

製品導入に関する引合い・相談数

- ・ クラウド移行、クラウド運用に絡んだセキュリティ対策
- ・ オンプレオンリーでも特権アクセス管理の対策

約80%

※21年度、弊社顧客満足度
アンケート結果

重要データへのアクセス、システム管理者・開発者など 特権アクセスを管理の導入を検討する割合

- ・ 利用環境問わず共通する割合
- ・ クラウド移行などと合わせた全体ルール策定と合わせて検討



DX、災害・感染症対策、法整備・認識変化による

クラウド化・リモートワーク普及...

ゼロトラストリスクとアクセス管理・認証の見直し

まとめ

- デジタルトランスフォーメーション（DX）の推進には、クラウドの利活用が不可欠
- パブリッククラウドでも様々なセキュリティ対策が可能
→ 「ゼロトラスト」対策を安く、早く
- **NHN テコラスがクラウド化の
セキュリティ・ガバナンス強化を支援します**
- **特権アクセス管理・DB監査の『Aegis Wall』も
是非お試しください！**

セキュリティ対策など
お気軽にご相談ください

本日の講演資料をご希望の方は
DBSC事務局または、下記までご連絡いたします

NHN テコラス株式会社

マーケティング本部 Aegis Wall 事業推進部

TEL. 03-6263-1830

MAIL: sales-info@ml.nhn-techorus.com

<https://nhn-techorus.com/c-chorus/aegis-wall/>