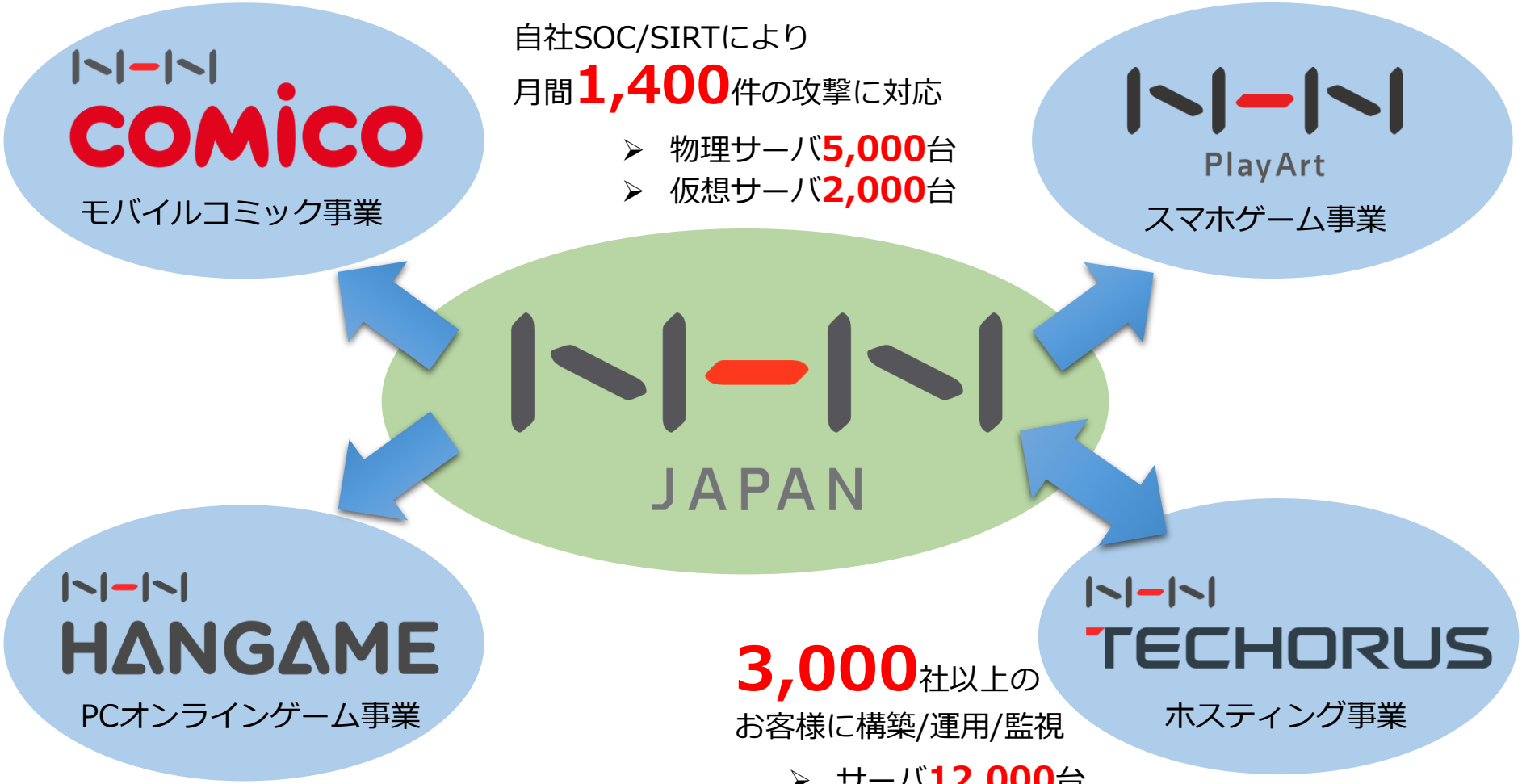
# PCI DSS準拠のための データベースアクセス管理の要点

※ 当日の講演内容と、同一にならない場合がございますので、あらかじめご了承下さい

NHN JAPAN株式会社
Aegis Wall事業部

# NHN JAPANグループについて

## グループとホスティングサービスを守るノウハウをお客様へ

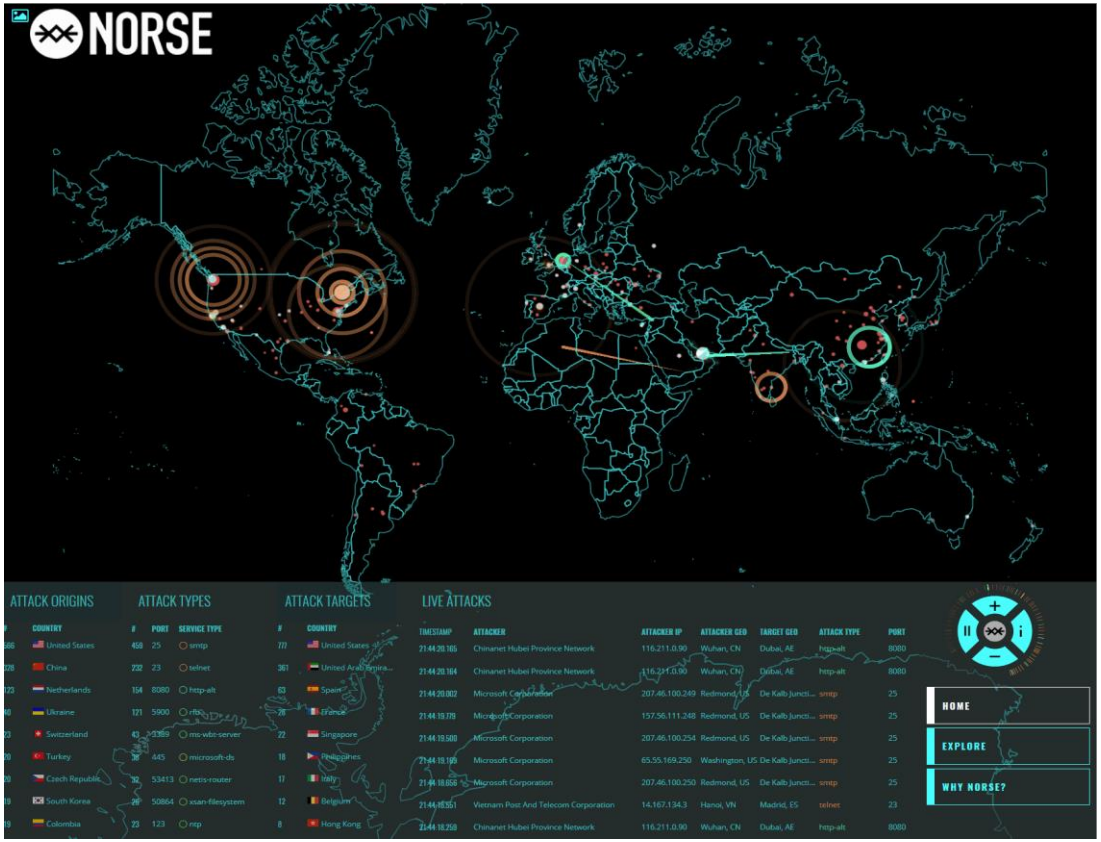


# 本日のアジェンダ

1. 情報資産を守るために
2. 特権ID管理の重要性
3. PCI DSS準拠のポイント(技術的対策)
4. Aegis Wallのご紹介

# 1. 情報資産を守るために

- サイバー攻撃の大半はオリジナルで日々進化を続けている
- パターンマッチングやふるまい検知で防げるのは
  ブラックマーケットで販売された中古品の攻撃パターンのみ




Norse社 IPViling Live http://map.norsecorp.com/


標的型攻撃

DDoS攻撃


IoT機器の悪用

# 1. 情報資産を守るために

| 偵察 | 侵入 | 調査 | 実行 |
| --- | --- | --- | --- |
|  |  |  |  |
| 侵入経路を探す | 内部に侵入する | 情報資産に接近 | 資産の窃取/破壊 |

攻撃手段がどんなに進化しても、
「偵察」→「侵入」→「調査」→「実行」という攻撃の手順
(サイバーキルチェーン)は変わらない

# 1. 情報資産を守るために


攻撃手段がどんなに進化しても、
「偵察」→「侵入」→「調査」→「実行」という攻撃の手順
(サイバーキルチェーン)は変わらない

# 目的達成のために通るポイントはいつも1つ

内部不正


**特権ID & パスワード**

情報資産


サイバー攻撃

高度化

低コスト

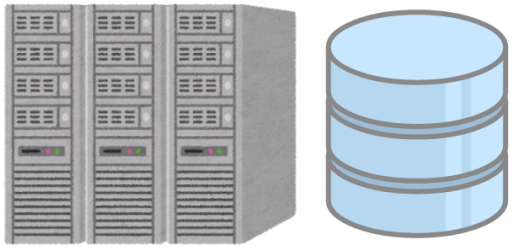
ゴールデンチケット攻撃
管理者アカウント乗っ取り

# 特権IDとは

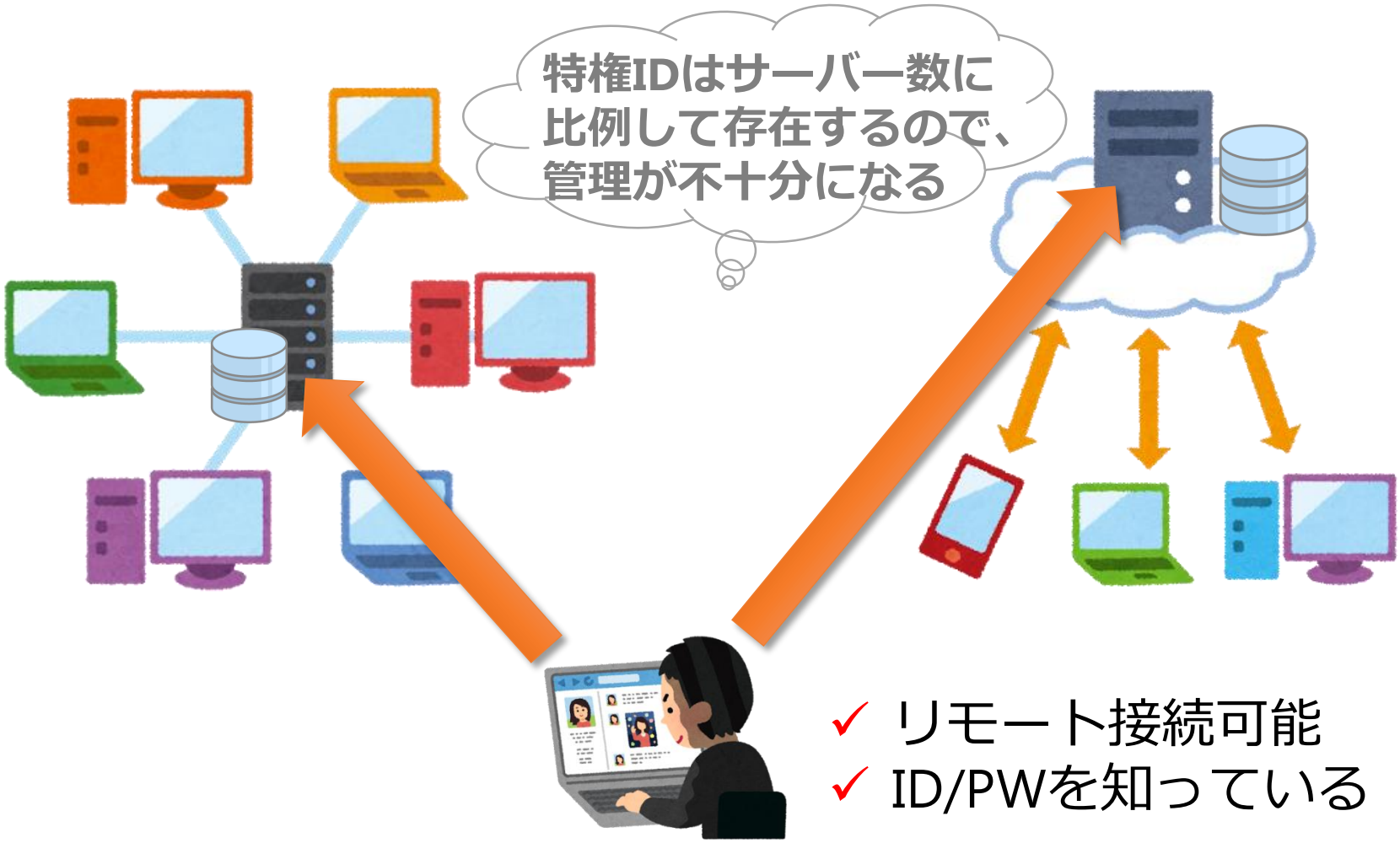
システムの維持･管理のために利用するID
起動/停止、設定変更などあらゆる操作が可能な権限

- Unix/Linux：root
- Windows：administrator
- DBMS：sys, sa

など



## 実態その1：担当者の異動・退職後も利用可能




- ✓ リモート接続可能
- ✓ ID/PWを知っている

# 実態その2：デフォルトのIDとパスワードを使用

機器によってはハードコードされている場合も…

ID: admin
PW: admin

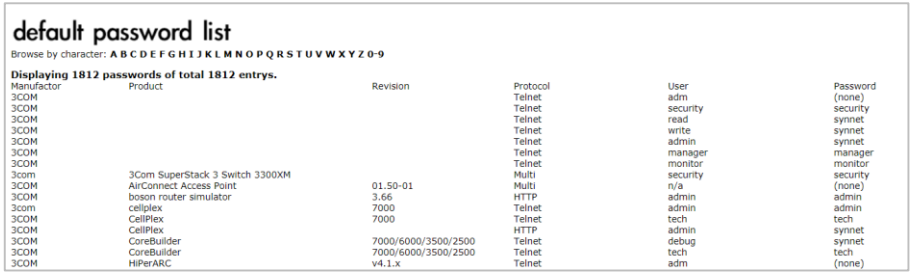
ID: root
PW: default

…etc

**侵入さえできれば簡単にログイン**

**内部からしかアクセスできないので…と保留**

各種機器のデフォルトパスワードまとめサイト
http://www.defaultpassword.com/



default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

**Displaying 1812 passwords of total 1812 entrys.**

| Manufactor | Product | Revision | Protocol | User | Password |
|---|---|---|---|---|---|
| 3COM | | | Telnet | adm | (none) |
| 3COM | | | Telnet | security | security |
| 3COM | | | Telnet | read | synnet |
| 3COM | | | Telnet | write | synnet |
| 3COM | | | Telnet | admin | synnet |
| 3COM | | | Telnet | manager | manager |
| 3COM | | | Telnet | monitor | monitor |
| 3com | 3Com SuperStack 3 Switch 3300XM | | Multi | security | security |
| 3COM | AirConnect Access Point | 01.50-01 | Multi | n/a | (none) |
| 3COM | boson router simulator | 3.66 | HTTP | admin | admin |
| 3com | cellplex | 7000 | Telnet | admin | admin |
| 3COM | CellPlex | 7000 | Telnet | tech | tech |
| 3COM | CellPlex | | HTTP | admin | synnet |
| 3COM | CoreBuilder | 7000/6000/3500/2500 | Telnet | debug | synnet |
| 3COM | CoreBuilder | 7000/6000/3500/2500 | Telnet | tech | tech |
| 3COM | HiPerARC | v4.1.x | Telnet | adm | (none) |

## 実態その3：共通のIDとパスワードを使用

外部委託業者

システム管理者

システム開発者

サーバーエンジニア

誰が操作しているか
分からない

**特にDBの特権IDは権限のスイッチが
できないため、個人識別が難しい**

## 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 |

# 3. PCI DSS準拠のポイント(技術的対策)

## ①個人認証

✓識別/認証の強化

**要件8に対応**

## ②アクセス制御

✓権限の最小化

**要件7に対応**

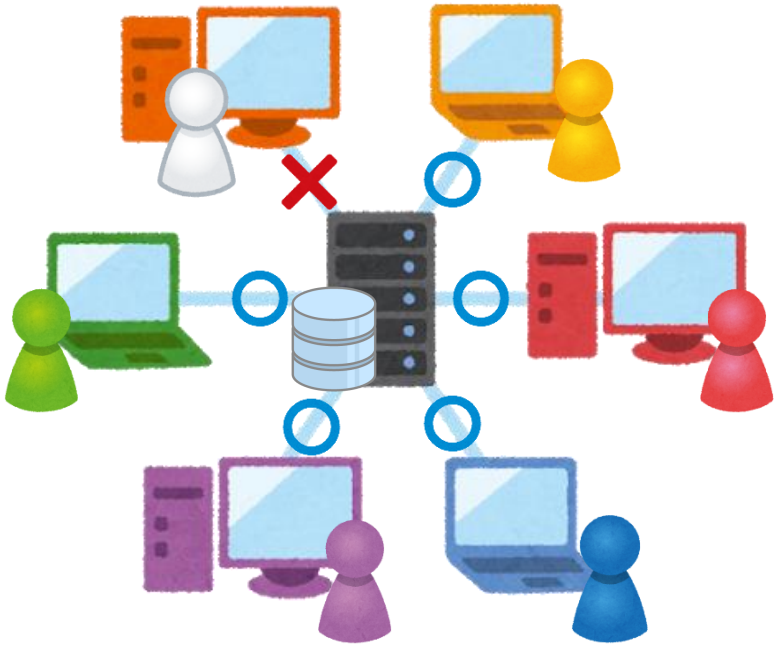
## ③ログ記録

✓不審な操作の検知

**要件10に対応**

## ①個人認証 (要件8)

- **識別/認証の強化**
  - 多要素/多段階の認証
  - ユーザー個人を一意のIDで識別
  - パスワード設定/変更の管理

## ①個人認証 (要件8)

- **識別/認証の強化**
  - 多要素/多段階の認証
  - ユーザー個人を一意のIDで識別
  - パスワード設定/変更の管理

ワンタイムパスワード


生体認証

端末/入室による管理


複数の認証を組み合わせることで権限窃取のリスクを軽減
CDE(カード会員データ環境)へのアクセス時は必須要件に

## ①個人認証 (要件8)

- **識別/認証の強化**
  - 多要素/多段階の認証
  - ユーザー個人を一意のIDで識別
  - パスワード設定/変更の管理

| ユーザー | ID | IPアドレス | プロトコル | アプリ | アクセス権 |
|---|---|---|---|---|---|
| taro | root | 192.168.137.1 | SSH | Tera Term | ○ |
| | | 103.5.142.1 | SSH | Tera Term | × |
| | sys | 192.168.137.1 | DBMS | SQL Plus | × |
| masako | root | 192.168.137.1 | SSH | Putty | × |
| | sys | 192.168.137.1 | DBMS | SQL Plus | ○ |

OSでは個人ユーザーを作成して特権IDにスイッチさせる運用が可能だが、
DBでは権限のスイッチができず、共有ID使用が避けられない場合がある

AD認証などと連携し、個人を一意に識別した形で管理する

## ①個人認証 (要件8)

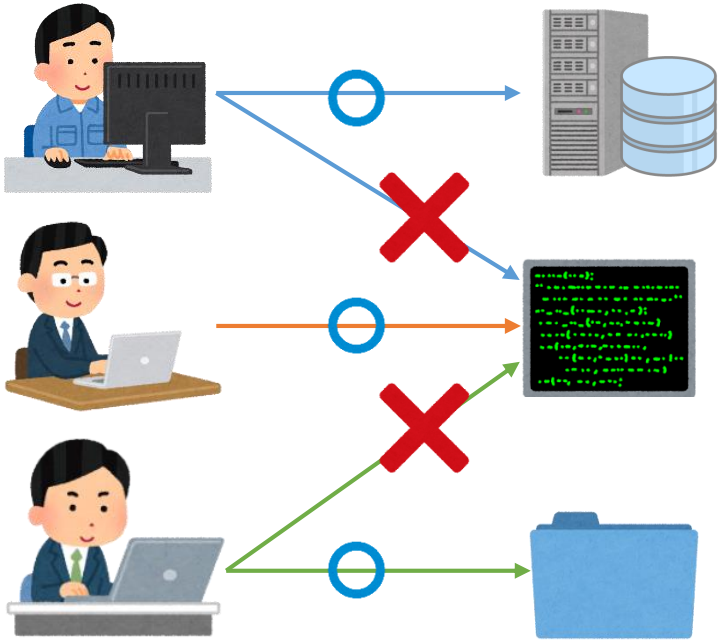
- **識別/認証の強化**
  - 多要素/多段階の認証
  - ユーザー個人を一意のIDで識別
  - パスワード設定/変更の管理

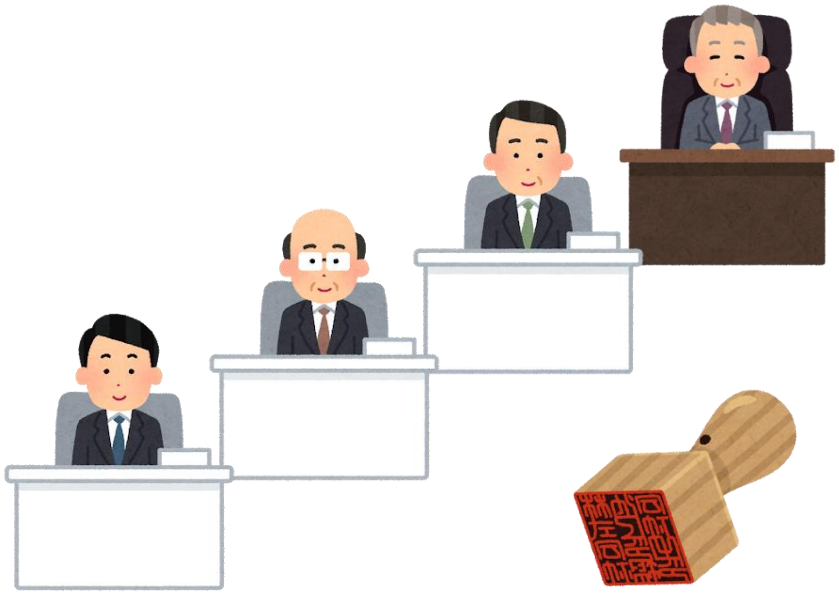

- パスワードの複雑性(7文字以上、数字/英字の両方を含む)
- これまでに使用した最後の4つのパスワード/フレーズと同じものを使用しない

- 初回使用後にパスワードをリセットする
- 90日に1回はパスワードを変更する
- 6回以上のパスワード失敗でアカウントをロックする
- リモートアクセスは使用期限を設定する

## ②アクセス制御 (要件7)

- **権限の最小化**
  - 個人の職務範囲に基づくアクセス権付与
  - 文書化された申請/承認による利用制限
  - デフォルトは「すべてを拒否」





## ②アクセス制御 (要件7)

- **権限の最小化**
  - 個人の職務範囲に基づくアクセス権付与
  - 文書化された申請/承認による利用制限
  - デフォルトは「すべてを拒否」

| ユーザー | サーバー | プロトコル | アクセス権 |
|---|---|---|---|
| インフラ担当者 | Webサーバー | SSH | ○ |
| | DBサーバー | SSH | ○ |
| | | DBMS | × |
| DBA | DBサーバー | SSH | × |
| | | DBMS | ○ |

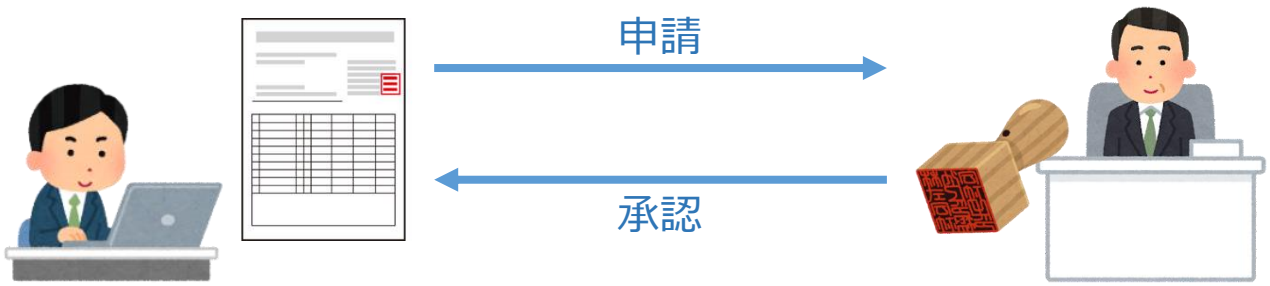
インフラ担当者はサーバーのメンテナンスのみ、DBAはDBの管理のみ

個人の職務範囲を定義し、それに応じた権限を付与

## ②アクセス制御 (要件7)

- **権限の最小化**
  - 個人の職務範囲に基づくアクセス権付与
  - 文書化された申請/承認による利用制限
  - デフォルトは「すべてを拒否」

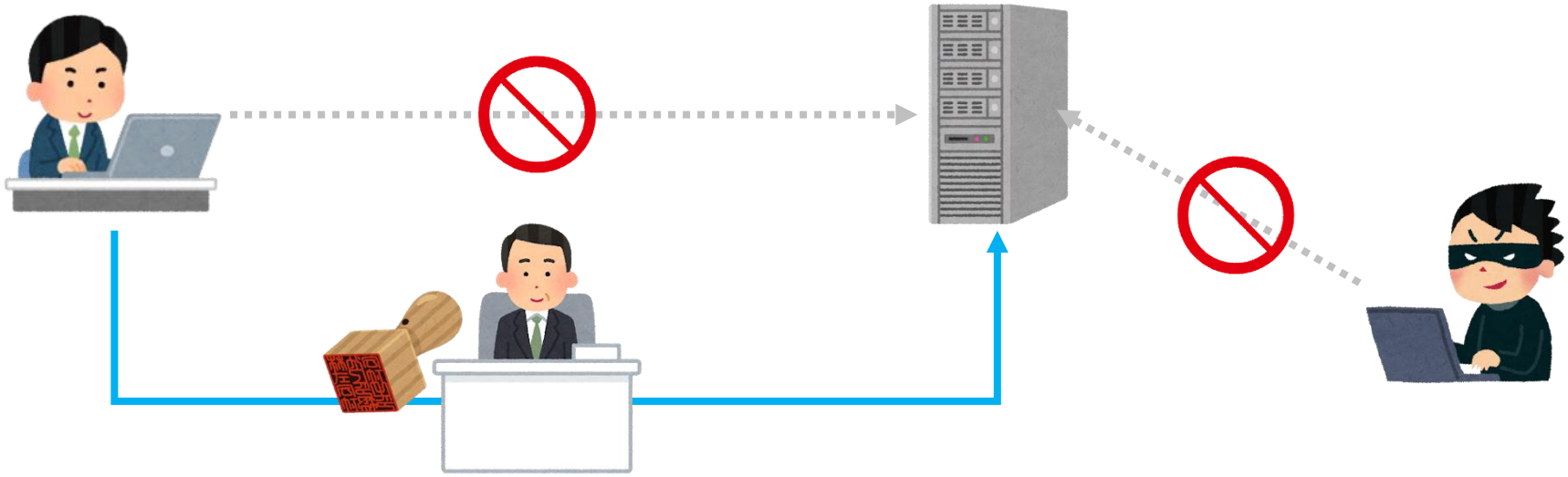
| ユーザー | ID | サーバー | プロトコル | 作業日時 |
|---|---|---|---|---|
| taro | root | WEBサーバー | SSH | 2018/03/30 09:00-12:00 |
| masako | sys | DBサーバー | DBMS | 2018/03/31 17:00-19:00 |




無制限の利用を禁止することで権限悪用のリスクを軽減

## ②アクセス制御 (要件7)

- **権限の最小化**
  - 個人の職務範囲に基づくアクセス権付与
  - 文書化された申請/承認による利用制限
  - デフォルトは「すべてを拒否」



職務や必要に応じた許可のないアクセスをすべて禁止

## ③ログ記録 (要件10)

### ■ 不審な操作の検知

- 個人を特定した形でアクセス/操作内容を正確に記録
- 申請→承認を経た正当な業務と識別
- 監査ログへのアクセスの記録と保護

誰が

どこへ

いつ

| 順番 | ユーザーID | 接続ID | IPアドレス | アプリケーション | サービス名 | サーバーIP[ポート] | 接続時刻 | 接続終了時刻 |
|---|---|---|---|---|---|---|---|---|
| 2 | taro | root | 192.168.137.4 | MySQLWorkbench.exe | MySQL_192.168.137.3_3306(2) | 192.168.137.3:3306 | 2018-03-01 12:04:31 | 2018-03-01 12:05:16 |
| 1 | taro | root | 192.168.137.4 | MySQLWorkbench.exe | MySQL_192.168.137.3_3306(2) | 192.168.137.3:3306 | 2018-03-01 12:04:31 | 2018-03-01 12:05:17 |

どこから

| 動作 | 順番 | コマンド | コマンド数 | 結果サイズ | 結果 | 要求時刻 |
|---|---|---|---|---|---|---|
| 遮断 | 22 | delete from tbl_areas where id=8 | 1 個 | 348 Byte | DENY COMMAND(DBSAFER) | 2018-03-01 12:05:06 |
| 許可 | 21 | SELECT * FROM db_customer.tbl_areas | 1 個 | 287 Byte | Run Complete | 2018-03-01 12:05:00 |
| 許可 | 20 | SELECT * FROM db_customer.tbl_credit_card_numbers | 1 個 | 60.5 KB | Run Complete | 2018-03-01 12:04:49 |
| 遮断 | 19 | delete from tbl_areas where id=8 | 1 個 | 359 Byte | DENY COMMAND(DBSAFER) | 2018-03-01 12:04:40 |
| 許可 | 18 | SHOW SESSION VARIABLES LIKE 'version_compile_os' | 1 個 | 232 Byte | Run Complete | 2018-03-01 12:04:33 |
| 許可 | 17 | USE `db_customer` | 1 個 | 16 Byte | Run Complete | 2018-03-01 12:04:31 |
| 許可 | 16 | SHOW SESSION VARIABLES LIKE 'lower_case_table_names' | 1 個 | 232 Byte | Run Complete | 2018-03-01 12:04:31 |
| 許可 | 15 | SELECT current_user() | 1 個 | 74 Byte | Run Complete | 2018-03-01 12:04:31 |

何を

どうした

## ③ログ記録 (要件10)

### ■ 不審な操作の検知

- 個人を特定した形でアクセス/操作内容を正確に記録
- 申請→承認を経た正当な業務と識別
- 監査ログへのアクセスの記録と保護

誰が


どこへ

いつ

| 順番 | ユーザーID | 接続ID | IPアドレス | アプリケーション | サービス名 | サーバーIP[ポート] | 接続時刻 | 接続終了時刻 |
|---|---|---|---|---|---|---|---|---|
| 2 | taro | root | 192.168.137.4 | MySQLWorkbench.exe | MySQL_192.168.137.3_3306(2) | 192.168.137.3:3306 | 2018-03-01 12:04:31 | 2018-03-01 12:05:16 |
| 1 | taro | root | 192.168.137.4 | MySQLWorkbench.exe | MySQL_192.168.137.3_3306(2) | 192.168.137.3:3306 | 2018-03-01 12:04:31 | 2018-03-01 12:05:17 |

**個人の特定 (特権を含む)**

どこから

**時刻の同期**

| 動作 | 順番 | コマンド | コマンド数 | 結果サイズ | 結果 | 要求時刻 |
|---|---|---|---|---|---|---|
| 遮断 | 22 | delete from tbl_areas where id=8 | 1 個 | 348 Byte | DENY COMMAND(DBSAFER) | 2018-03-01 12:05:06 |
| 許可 | 21 | SELECT * FROM db_customer.tbl_areas | 1 個 | 287 Byte | Run Complete | 2018-03-01 12:05:00 |
| 許可 | 20 | SELECT * FROM db_customer.tbl_credit_card_numbers | 1 個 | 60.5 KB | Run Complete | 2018-03-01 12:04:49 |
| 遮断 | 19 | delete from tbl_areas where id=8 | 1 個 | 359 Byte | DENY COMMAND(DBSAFER) | 2018-03-01 12:04:40 |
| 許可 | 18 | SHOW SESSION VARIABLES LIKE 'version_compile_os' | 1 個 | 232 Byte | Run Complete | 2018-03-01 12:04:33 |
| 許可 | 17 | USE `db_customer` | 1 個 | 16 Byte | Run Complete | 2018-03-01 12:04:31 |
| 許可 | 16 | SHOW SESSION VARIABLES LIKE 'lower_case_table_names' | 1 個 | 232 Byte | Run Complete | 2018-03-01 12:04:31 |
| 許可 | 15 | SELECT current_user() | 1 個 | | Run Complete | 2018-03-01 12:04:31 |

何を

どうした

## ③ログ記録 (要件10)

### ■ 不審な操作の検知

- 個人を特定した形でアクセス/操作内容を正確に記録
- 申請→承認を経た正当な業務と識別
- 監査ログへのアクセスの記録と保護

| 順番 | ユーザーID | 接続ID | IPアドレス | アプリケーション | サービス名 | サーバーIP[ポート] | 接続時刻 | 接続終了時刻 |
|---|---|---|---|---|---|---|---|---|
| 2 | taro | root | 192.168.137.4 | MySQLWorkbench.exe | MySQL_192.168.137.3_3306(2) | 192.168.137.3:3306 | 2018-03-01 12:04:31 | 2018-03-01 12:05:16 |
| 1 | taro | root | 192.168.137.4 | MySQLWorkbench.exe | MySQL_192.168.137.3_3306(2) | 192.168.137.3:3306 | 2018-03-01 12:04:31 | 2018-03-01 12:05:17 |


| 動作 | 順番 | コマンド | コマンド数 | 結果サイズ | 結果 | 要求時刻 |
|---|---|---|---|---|---|---|
| 遮断 | 22 | delete from tbl_areas where id=8 | 1 個 | 348 Byte | DENY COMMAND(DBSAFER) | 2018-03-01 12:05:06 |
| 許可 | 21 | SELECT * FROM db_customer.tbl_areas | 1 個 | 287 Byte | Run Complete | 2018-03-01 12:05:00 |
| 許可 | 20 | SELECT * FROM db_customer.tbl_credit_card_numbers | 1 個 | 60.5 KB | Run Complete | 2018-03-01 12:04:49 |
| 遮断 | 19 | delete from tbl_areas where id=8 | 1 個 | 359 Byte | DENY COMMAND(DBSAFER) | 2018-03-01 12:04:40 |
| 許可 | 18 | SHOW SESSION VARIABLES LIKE 'version_compile_os' | 1 個 | 232 Byte | Run Complete | 2018-03-01 12:04:33 |
| 許可 | 17 | USE `db_customer` | 1 個 | 16 Byte | Run Complete | 2018-03-01 12:04:31 |
| 許可 | 16 | SHOW SESSION VARIABLES LIKE 'lower_case_table_names' | 1 個 | 232 Byte | Run Complete | 2018-03-01 12:04:31 |
| 許可 | 15 | SELECT current_user() | 1 個 | 74 Byte | Run Complete | 2018-03-01 12:04:31 |

承認完了文書の一覧　D：DBMS　T：TERMINAL　I：IM　U：USER　10

| | 文書番号 | 文書種類 | 稟議タイトル | 申請者 | 稟議申請日 | 承認日 | 状態 |
|---|---|---|---|---|---|---|---|
| D | BA-20180521-000001 | アクセス稟議 | DBMSアクセス申請：テスト1 | ユーザーA | 2018-05-21 13:18:26 | 2018-05-21 16:58:52 | 進行 |
| T | BS-20180521-000001 | コマンド稟議 | TERMINALコマンド申請：テスト2 | ユーザーA | 2018-05-21 13:36:07 | 2018-05-21 16:38:58 | 却下 |

作業と承認完了のログを突合して、業務の正当性を証明

## ③ログ記録 (要件10)

### ■ 不審な操作の検知

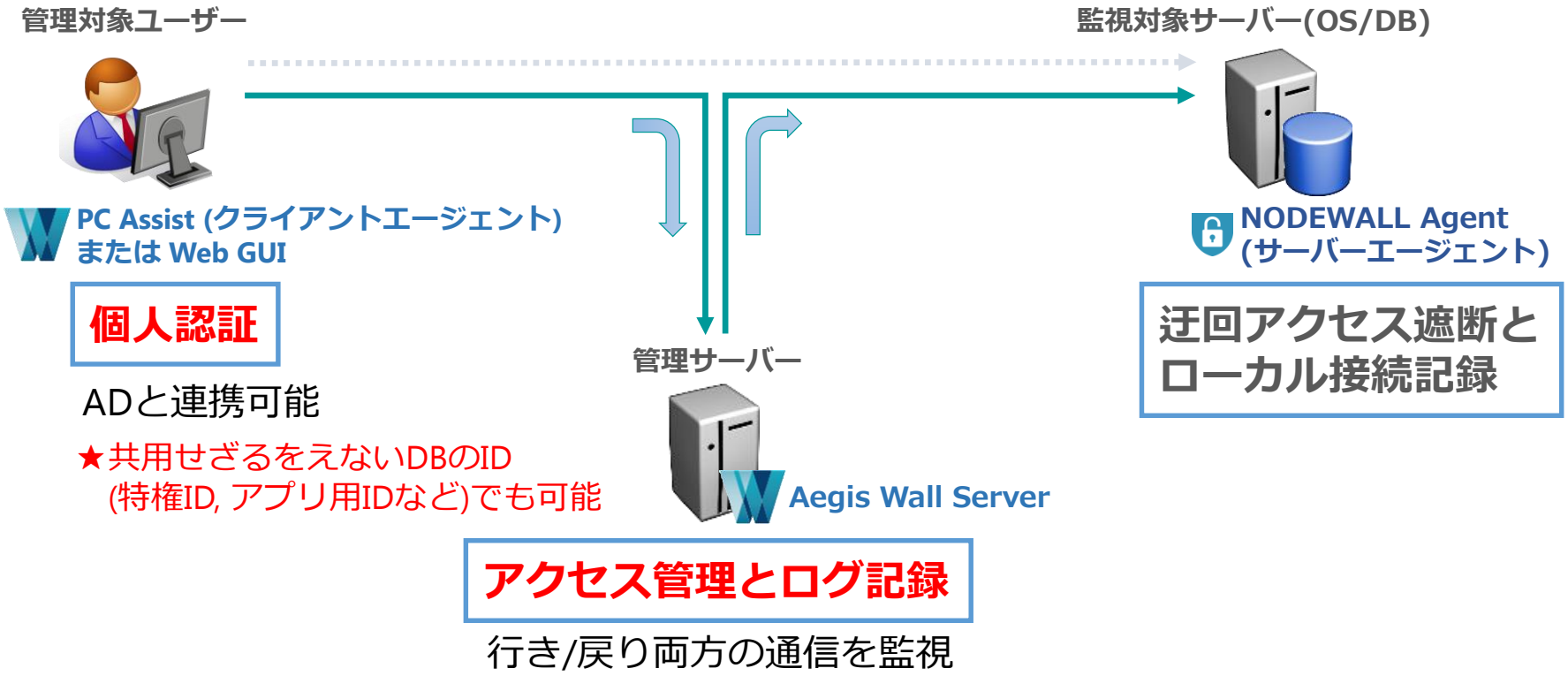
- 個人を特定した形でアクセス/操作内容を正確に記録
- 申請→承認を経た正当な業務と識別
- 監査ログへのアクセスの記録と保護


- 監査ログへのアクセス権限の管理
- 監査ログへのアクセス/操作の記録
- ログファイルの保護
- ログファイルの安全なバックアップ
- ログファイルの整合性の監視

監査ログ変更による不正アクセスの証拠隠滅を防ぐ

# Aegis Wallの設計思想

ソフトウェア制御によるゲートウェイ構成により、
**監視対象サーバーへの負荷ゼロ**で、**厳密な個人認証**に基づく
**DB/サーバーOSのアクセス管理/ログ記録**が可能



# Aegis Wallが提供するソリューション

## ログ記録 Log Auditor

1. 操作端末の認証情報から**個人を一意のIDで特定**
2. いつ/誰が/何をしたか、正確で分かりやすいログ
3. リモートアクセスの**GUI操作を動画で記録**
4. 多種/大量のサーバーのログを**一元管理**

## アクセス管理 Access Controller

1. コマンドの種類やテーブルなど**細かな制御**
2. OTP(ワンタイムパスワード)による**二段階認証**
3. 重要データの**マスキング**
4. 申請/承認**ワークフロー**による制御

# 4. Aegis Wallのご紹介

# 4. Aegis Wallのご紹介

## 国内

2015年3月～ 国内で10社以上に導入

| | | | |
|---|---|---|---|
| NHN Japanグループ | インターネット | 1,000人以上 | 監査（ITGC）対応 |
| 霧島酒造 | 製造 | 500人以上 | 内部統制（委託業者管理） |
| 国境なき医師団 | NPO | 100人以下 | 情報漏えい対策 |
| （非公開） | インターネット | 1,000人以上 | 内部統制（J-SOX対応） |
| （非公開） | 信用金庫 | 1,000人以上 | 内部統制（金融庁検査対応） |
| （非公開） | 地方銀行 | 1,000人以上 | PCI DSS対応 |
| （非公開） | 製造 | 1,000人以上 | 内部統制（J-SOX対応） |
| （非公開） | アパレル | 1,000人以上 | 内部統制（J-SOX対応） |
| （非公開） | ASP事業者 | 100人以下 | ユーザーの内部統制対応 |
| （非公開） | 旅行代理店 | 500人以下 | PCI DSS対応 |
| （非公開） | インターネット | 500人以下 | 内部統制（委託業者管理） |
| （非公開） | 人材派遣 | 1,000人以上 | 内部統制 |
| （非公開） | データセンター | 100人以下 | 監査（SOC2)対応 |
| （非公開） | 地方公共団体 | 1,000人以上 | 内部統制 |

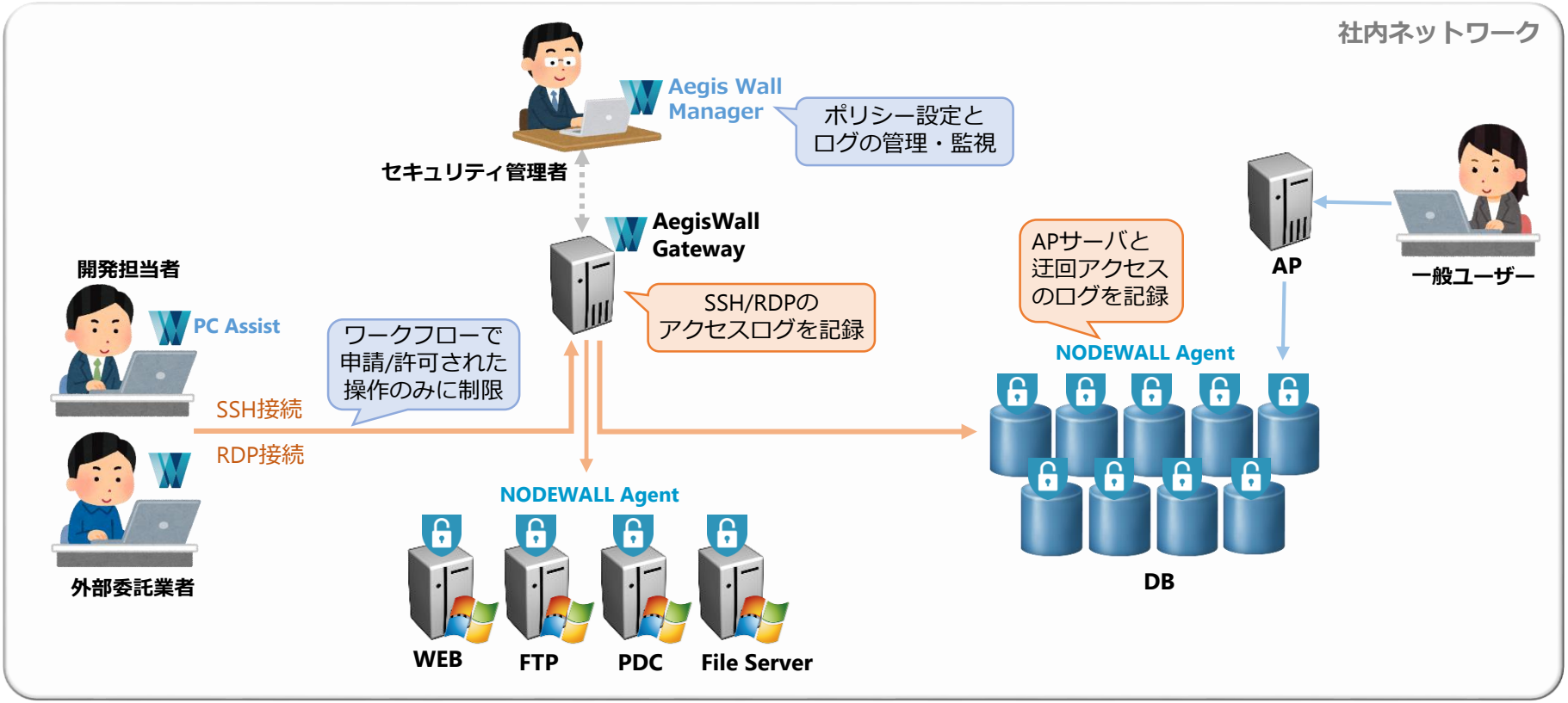
## 海外

2004年～ 韓国の1,000以上の企業・政府機関で導入

| 政府・自治体 | 製造 | 金融 | 情報・通信 | 小売 |
|---|---|---|---|---|
| ソウル特別市 | 現代自動車 | 釜山銀行 | 三星SDI | イーマート |
| 国家情報院 | ルノー三星自動車 | 農協銀行 | 郵政事業情報センター | 現代デパート |
| 金融決済院 | ロッテ製菓 | メットライフ生命 | 新世界I&C | GSリテール |
| 国税庁 | LG | ハナSKカード | | ピザハット |
| 防衛事業庁 | | ウリ投資証券 | | |

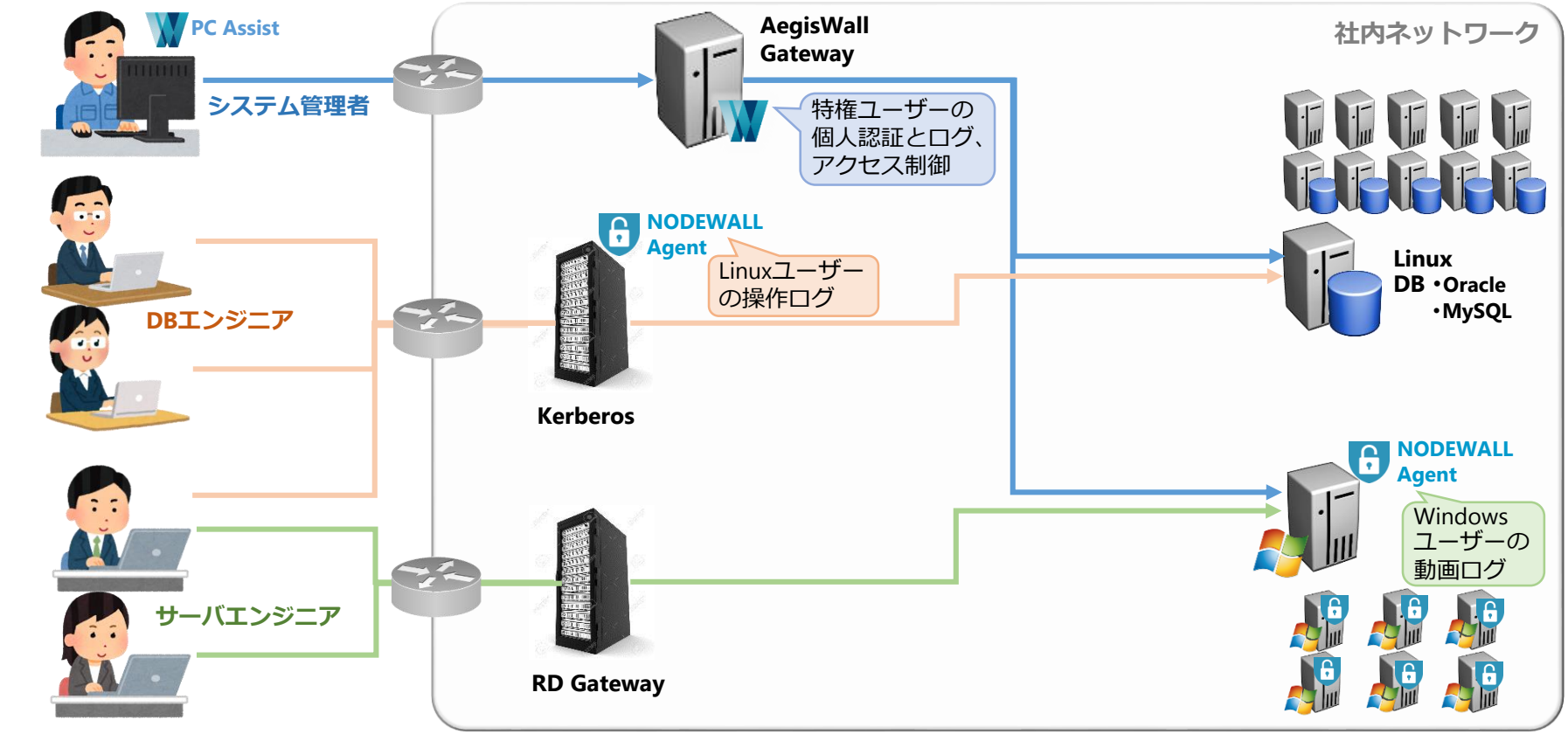
# 内部統制の強化（信用金庫）

| | |
|---|---|
| 導入目的 | 金融庁検査に備えて、DBとWindowsサーバの個人を識別したログを記録するため<br>アクセス権の申請・承認業務のシステム化 |
| 環境・構成 | Windowsサーバ＋DB監視<br>Gatewayで特権ユーザーの操作内容、NODEWALLで一般ユーザーのアクセスを監視 |
| 選定ポイント | RDP接続の動画ログを記録できる他社製品と比べて安価<br>ワークフローを含めたアクセス制御とコマンド制御まで1製品だけでカバー |



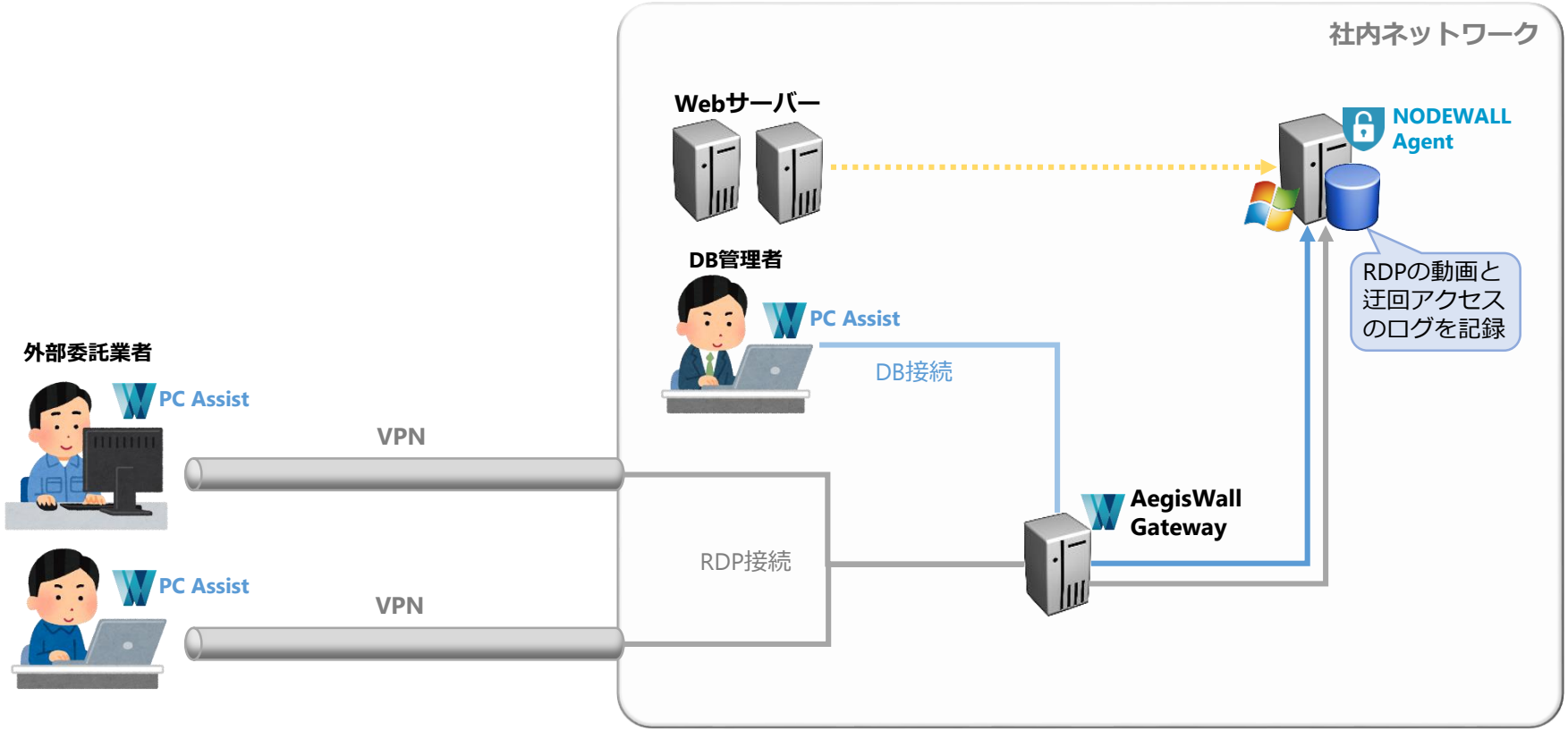
# 大規模システムの監視（NHN Japan グループ）

| | |
|---|---|
| 導入目的 | IT全般統制に対応するため、内部の証跡記録を行う |
| 環境・構成 | Linux/Windows合わせて3,000台のサーバーを監視<br>Gatewayで特権ユーザー操作、NodewallでLinux/Windowsサーバーへのアクセスを監視 |
| 選定ポイント | アクセスログ管理ポイントの一元化による監査対応の効率化 |



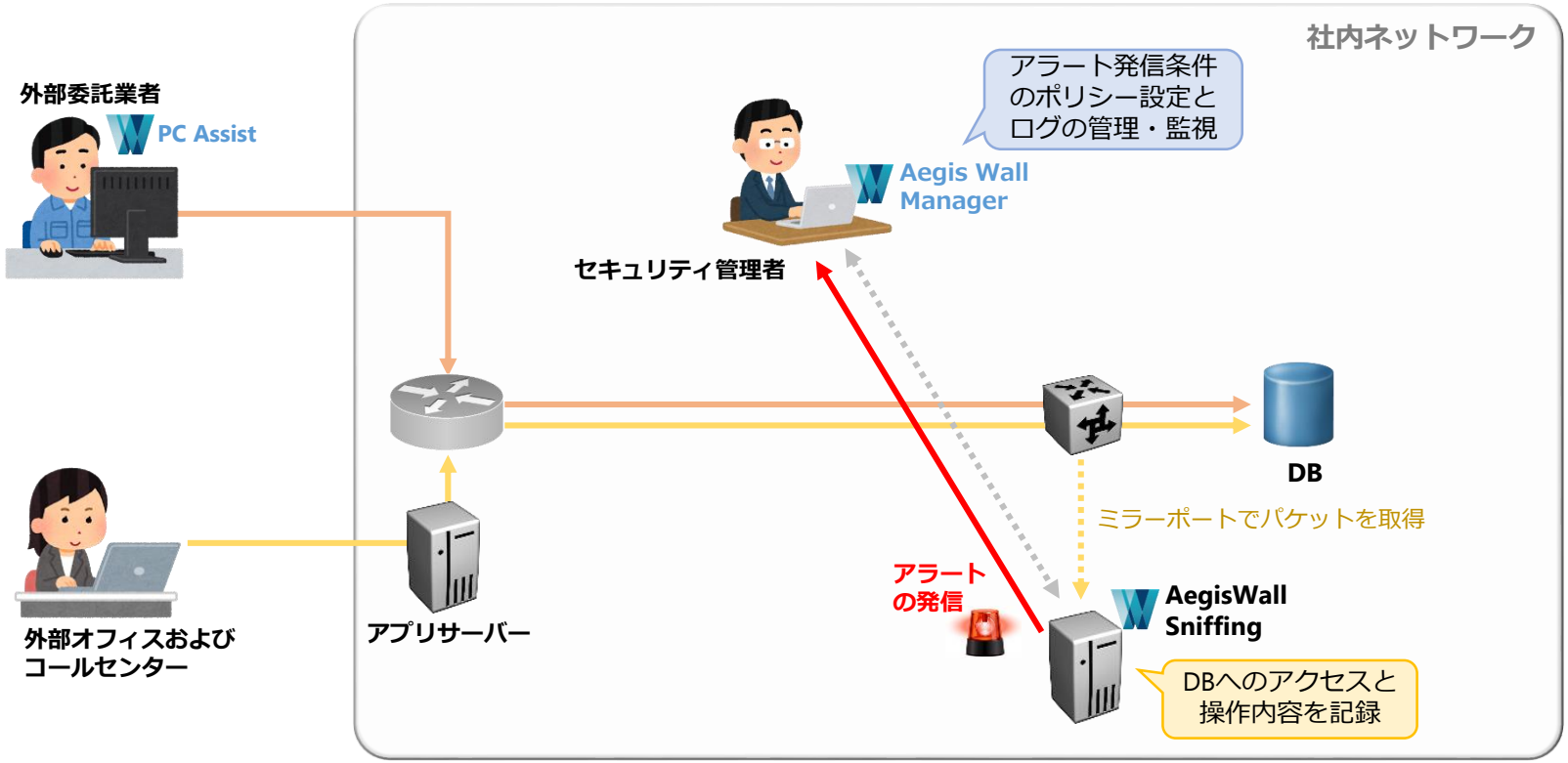
# 委託業者の管理（霧島酒造）

| | |
|---|---|
| 導入目的 | 内部統制強化の一環で、外部委託業者からのリモートアクセスを監視するため |
| 環境・構成 | DB監視<br>Gatewayで特権ユーザーの操作内容を監視 |
| 選定ポイント | 安価でテキストログ/動画の記録、レポート作成までカバー可能<br>複数事業者からの作業申請・承認の管理にワークフロー機能が有用 |



# 不正操作の検知（国境なき医師団）

| | |
|---|---|
| 導入目的 | 委託元から要求されたセキュリティ要件を満たすため（アクセスログの記録） |
| 環境・構成 | アプリケーションサーバ＋DB監視<br>DBへの直接アクセス、およびWEBサーバ⇔DB間の通信をSniffing構成で監視 |
| 選定ポイント | DBへの操作内容に基づいたアラート発信が可能<br>ホスティングサービスのサポート体制への満足度 |



# お問い合わせ窓口

**NHN JAPAN株式会社**
**Aegis Wall事業部**

**TEL**：03-6263-1830
**MAIL : dl_aegiswall@nhn-japan.com**

**https://aegis-wall.com**

イージスウォール　検索