# データの保護と
# システムの安全性維持

（株）大和ソフトウェアリサーチ

# Agenda

* 会社概要
* DSRが提案するPCIDSS準拠の範囲
* カード会員データの保護
  * 暗号化
  * アクセスコントロール、監査ログ
* システムコンポーネントの安全性の維持＆管理
  * システムコンポーネントの安全性確保
  * 適用範囲の違い ⇒ FireWall、IPS/IDS、WAF
  * 攻撃の検知方法
  * 最近の攻撃 『 アノニマス 』

# 1. 会社概要

【会社名】　株式会社大和ソフトウェアリサーチ

【代表者】　代表取締役社長　竹末 圭五

【所在地】　本社：東京都千代田区麹町1丁目5番2号

TEL：03-3262-8558（代表）　FAX：03-3262-8867

システムサービスセンター：千葉県茂原市緑ヶ丘3丁目17番1号

TEL：0475-25-8111（代表）　FAX：0475-25-8130

【設立日】　1969年 7月 3日

【資本金】　4億450万円

【従業員数】　148名（2012年4月1日）

【認定資格】　情報セキュリティマネジメントシステム：ISO/IEC27001：2005認証
（対象事業所：システムサービスセンター）

品質マネジメントシステム：ISO9001：2008認証
（対象事業所：本社　）

プライバシーマーク：JIS Q 15001:2006

【主要株主】　大興電子通信株式会社

株式会社大和総研

株式会社大和証券グループ本社 他

【取引銀行】　三井住友銀行、三菱東京ＵＦＪ銀行、みずほコーポレート銀行　他

【Ｕ Ｒ Ｌ】　http://www.dsr.co.jp

# はじめに：変化＆増大化するサイバー攻撃の状況

## ◇ 攻撃の内容が犯罪化の傾向

従来、サイトへの攻撃は悪戯や興味本位での侵入と言った内容でしたが、昨今は、『機密情報の入手』『情報の改竄』『サービス機能の停止』と言った、明らかに悪意を持った犯罪化したアクセスが増えています。

➪標的型攻撃（APT）
➪アノニマス集団による攻撃

狙われる企業・団体も、政府や公共機関に止まらず、国家的な安全性に関係するサイトであったり、一般社会へ与える影響の大きな企業を狙ったりという傾向にあります。

サービスを提供する側としては、被害に遭ってしまってからユーザーへ謝罪しても、全く、意味がありません。如何に未然に防ぐかと言う点に注力した取り組みが必要です。

IPAでも日常業務の中で、自衛手段としての取り組みを喚起しています。

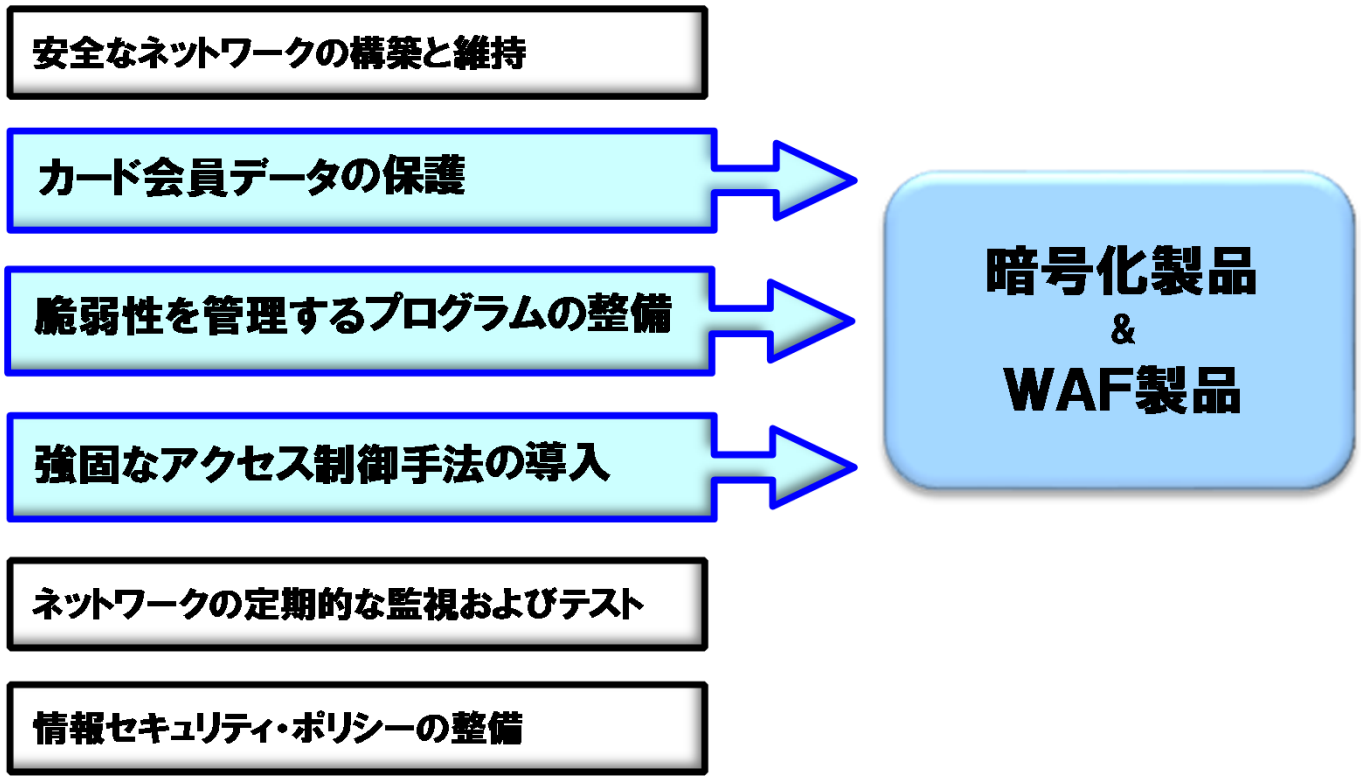
（１）取り扱う組織情報の重要度、機密度を精査する

（２）企業の社会的責任と事業継続性の観点から、相応の対策を選択することが重要

（３）グループ企業や連携している組織では、統制されたポリシーと対策が必要

# 2. DSRのPCIDSS要件準拠に向けたソリューション

◇ DSRが提供するPCIDSS要件（目的）を準拠するソリューションの分野



# クレジットカードデータの保護

# 暗号化製品～D’Amo

# 3. データ保護のPCIDSS準拠に向けた取り組み

## ◇ 暗号化製品【D'Amo （ディアモ】 が対応する要件は 3及び7になります

| 要件3 及び7でのサポート項目 | サポート状況 |
|---|---|
| 3.5.2 暗号化キーの保存場所と形式を最小限にし、安全に保存する。 | |
| 3.5.2.a システム構成ファイルを調査し、キーが暗号化された形式で保存され、キー暗号化キーがデータ暗号化キーとは別個に保存されていることを確認する。 | ✓ |
| 3.6.5 キーの完全性が弱くなったとき（たとえば、平文キーの情報を持つ従業員が業務から離れる場合）またはキーが危険にさらされている疑いがあるときに必要とみなされる、キーの破棄または取替。キーの破棄または取替とは、たとえば、アーカイブ、破棄、または廃止（あるいはこれらのすべて）である。 | |
| 3.6.5.a キー管理手順で、キーの完全性が弱くなった場合にキーの破棄が要求されることを確認する。 | ✓ |
| 3.6.5.b キー管理手順で、危険にさらされたことがわかっている、またはその疑いがあるキーの取替が要求されていることを確認する。 | ✓ |
| 3.6.5.c 破棄された、または取り替えられた暗号化キーを保持する場合、そのキーが暗号化処理で使用されないことを確認する。 | ✓ |
| 7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下の項目を含める必要がある。 | |
| 7.1.1 特権ユーザ IDに関するアクセス権が、職務の実行に必要な最小限の特権に制限されていることを確認する。 | ✓ |
| 7.1.2 特権の付与が、個人の職種と職能に基づいていることを確認する（「役割ベースのアクセス制御」（RBAC）とも呼ばれる）。 | ✓ |
| 7.1.4 自動アクセス制御システムによるアクセス制御が実装されていることを確認する。 | ✓ |
| 7.2 複数のユーザが使用するシステムコンポーネントで、ユーザの必要性に基づいてアクセスが制限され、特に許可のない場合は「すべてを拒否」に設定された、アクセス制御システムを確立する。 アクセス制御システムには以下の項目を含める必要がある。 | |
| 7.2.1 アクセス制御システムがすべてのシステムコンポーネントに実装されていることを確認する。 | ✓ |
| 7.2.2 職種と職能に基づいて個人に特権を付与するように、アクセス制御システムが構成されていることを確認する。 | ✓ |
| 7.2.3 アクセス制御システムに「すべてを拒否」がデフォルト設定されていることを確認する。 | ✓ |

# データベースセキュリティソリューションのご紹介

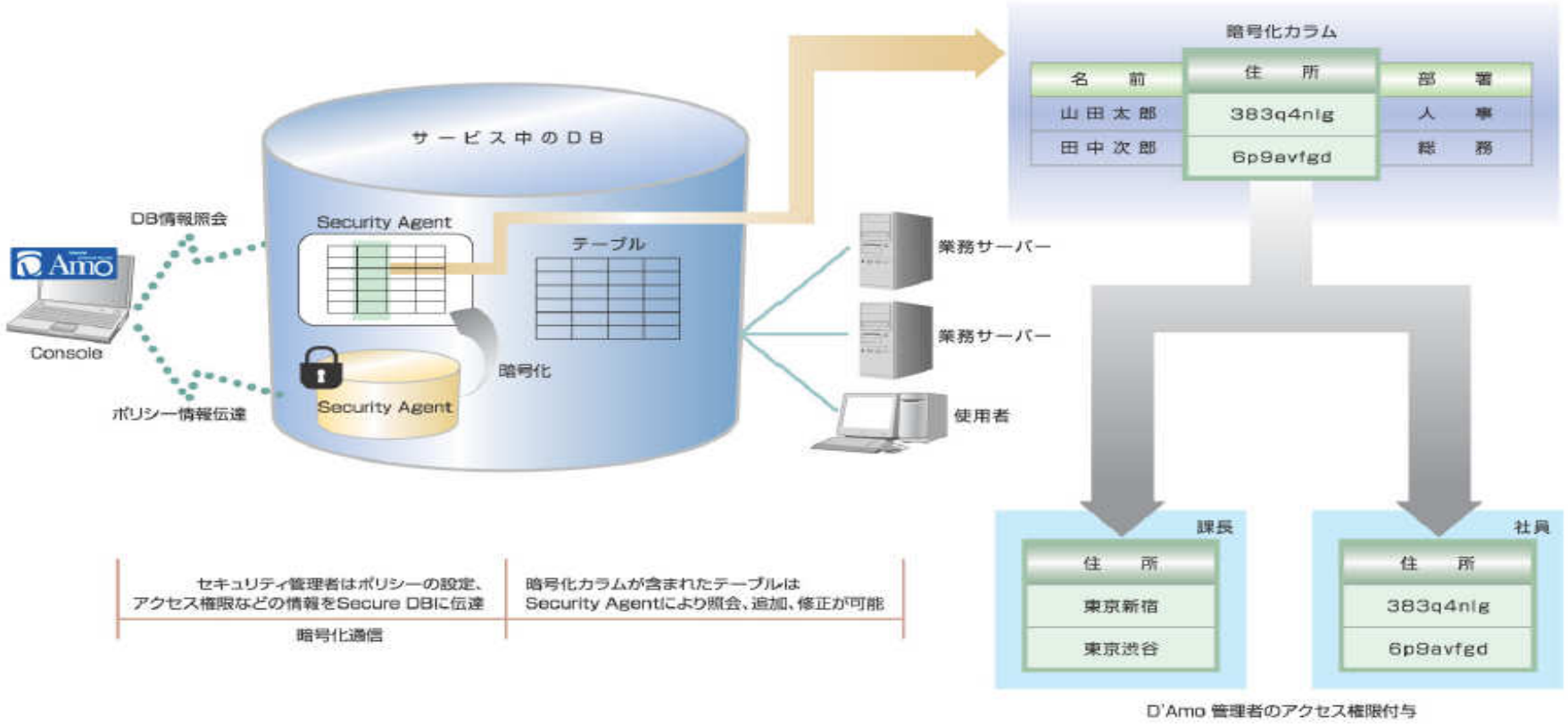
## 統合DBセキュリティソリューション
## 『D‘Amo（ディアモ）』


- ✓ DB内のデータを**カラム単位で選択して暗号化**
- ✓ DBアカウント/IP/応用プログラム/時間帯別/MACアドレスなど
  **DB全体または暗号化カラムへのアクセスコントロール**
- ✓ 非暗号化カラムもカラム単位で**監査ログ取得可能**
- ✓ 暗号化カラムに対する**保護機能を提供**
- ✓ **迅速な設置**によるシステムの統合：インストール製品
- ✓ 複数のDBを1台のD'Amoコンソールで**統合管理**


**D' Amo（ディアモ）は,応用プログラムの修正なしにDBのデータをカラム単位で暗号化し
アクセスコントロール、監査を実装できる統合DBセキュリティソリューションです。**

# D'Amoの機能

**D'Amoは、コンソールとセキュリティエージェントで構成します。**



# 導入事例(1)

## 【ニッセイアセットマネジメント株式会社様】
## 適用業務:投資運用業務

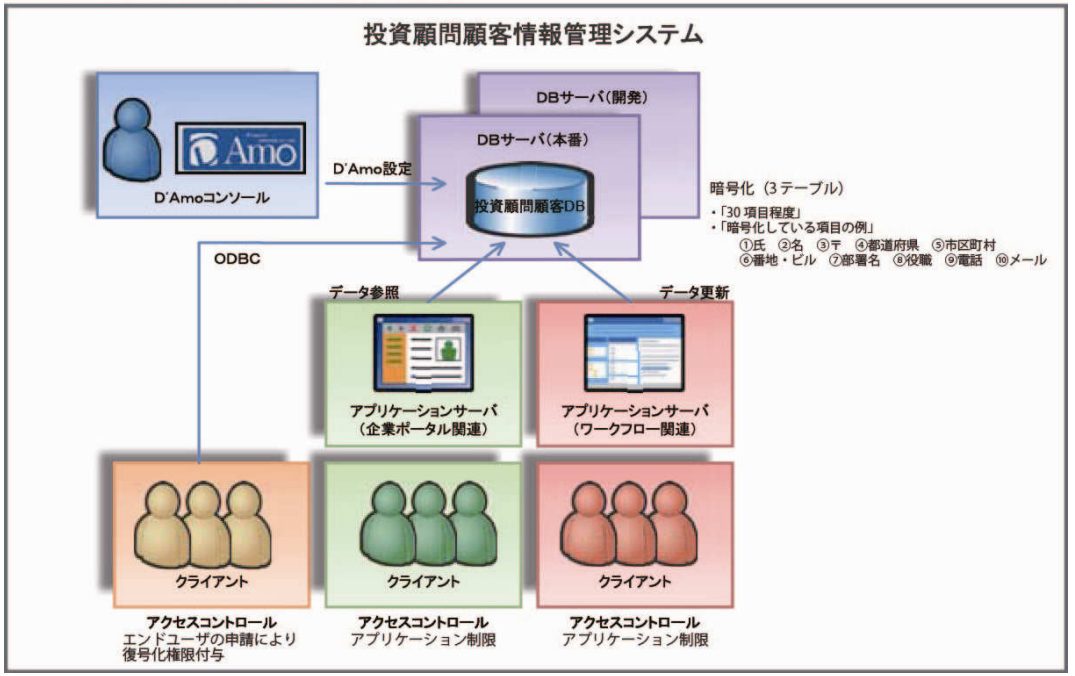
### 導入前の問題点

1. 顧客情報を統合して社内データベースで管理する事により、更なるセキュリティ強化が必要になった
2. データベースのセキュリティ対策において「暗号化」「ログ監視」をおこなう為には、アプリケーションなどの再開発など、コストと時間をかけなければならなかった

### 導入後の効果

1. アプリケーションの再開発などを必要としない為、短期間での導入に成功
2. 暗号化、ログ監視、アクセスコントロールにより非常に高いセキュリティ対策を実現
3. 低価格での導入が可能だった為、当初予算より大幅なコスト削減に成功

▼D'Amo導入システム構成図



# 導入事例(2)

## 【学校法人東京農業大学様】
## 適用業務:学事基幹システム

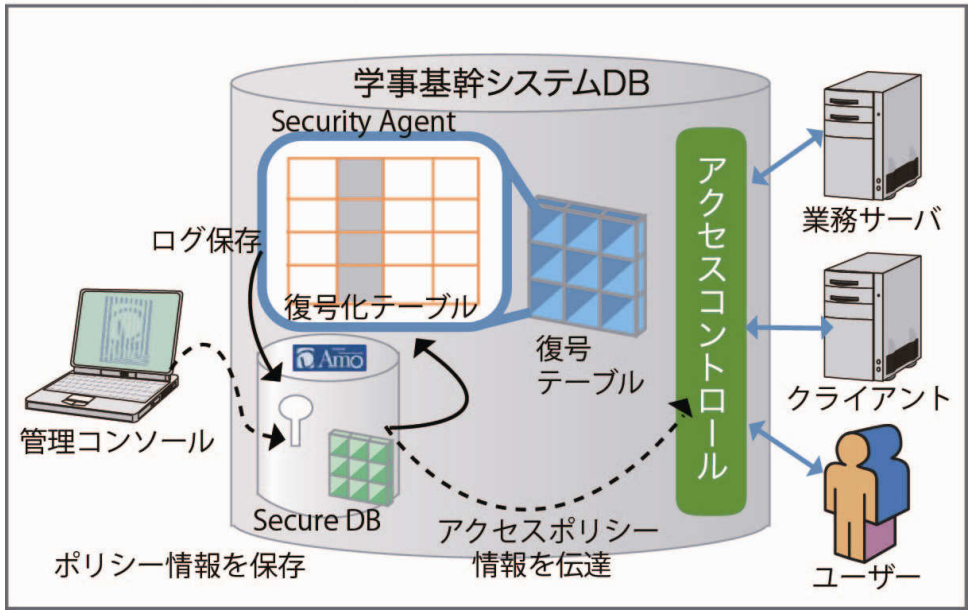
### 導入前の問題点

①個人認証、データベースユーザ認証、アプリケーションにおけるきめの細かいアクセスコントロールリストなどをすでに実施し運用中。個人情報の保護のためデータベースに対するセキュリティ対策を実施したいと考えていた。
②すでにアプリケーションレベルでのきめ細かなアクセスコントロールは実施しているが、Microsoft Accessなどでのより多角的なデータベースの有効活用において、利便性と迅速な対応を維持したまま、いかにより高度なセキュリティ対策を講じるかが課題となっていた。

### 期待される効果(現在進行中)

①IPやサイト単位でのアクセス制御を行うことにより、より細かい対策が可能に
②データベース自体の監査情報およびその統計情報が確認できる
③アプリケーションの変更が必要なく、導入が容易である
④暗号化を実装することにより、外部・内部からの漏えいに対する高度な対策が可能に

▼ D'Amo導入アーキテクチャ



# システムコンポーネントに対する安全性の維持＆管理

# 4. システム安全性のPCIDSS準拠に向けた取組

| 要件6.6　Webアプリケーションファイアウォールの推奨される能力 | WAPPLESのサポート状況 |
|---|---|
| カード会員のデータ環境のシステム構成要素に関する、適用可能なすべての PCI DSS 要件を満たす。 |  |
| 少なくとも OWASP トップ 10 または PCI DSS 要件 6.5 で特定されている、関連のある脆弱性に対する脅威に、適切に（アクティブなポリシーまたはルールによって定義）対処する。 |  |
| Web アプリケーションへの入力を調査し、アクティブなポリシーまたはルールや、実行されたログアクションに基づいて応答（許可、ブロック、アラート）する。 |  |
| データ漏えいの回避 – Web アプリケーションからの出力を調査し、アクティブなポリシーまたはルールや、実行されたログアクションに基づいて応答（許可、ブロック、マスク、アラート）する機能が備わっている。 |  |
| ポジティブとネガティブの両方のセキュリティモデルの実装。ポジティブモデル（「ホワイトリスト」）では、許可する動作、入力、データ範囲などを定義し、定義されていないものはすべて拒否します。ネガティブモデル（「ブラックリスト」）では、許可しないものを定義します。これらのシグネチャと一致するメッセージはブロックされ、シグネチャと一致しない（「ブラックリストに掲載」されていない）トラフィックは許可されます。 |  |
| HTML（Hypertext Markup Language）、DHTML（Dynamic HTML）、CSS（Cascading Style Sheets）などの Web ページコンテンツと、HTTP（HypertextTransport Protocol）、HTTPS（Hypertext Transport Protocol over SSL）などのコンテンツの送信基盤となるプロトコルの両方を調査する（HTTPS には、SSL だけでなく、TLS による HTTP も含まれます）。 |  |
| Web サービスが公共のインターネットに公開されている場合は、Web サービスのメッセージの調査。HTTP に加え、通常、これにはドキュメント指向モデルと RPC 指向モデル両方のSOAP（Simple Object Access Protocol）と XML（eXtensible Markup Language）が含まれます。 |  |
| Web アプリケーションとの間でのデータ転送に使用されるすべてのプロトコル（独自または標準的なもの）またはデータ構造（独自または標準的なもの）が、メッセージフローの他のポイントで調査されない場合、これらを調査する。 |  |
| WAF 自体を標的とした脅威を防ぐ。 |  |
| SSL または TLS ターミネーションに対応する。または、暗号化された送信内容を復号化してから調査できる位置に配置されている。調査エンジンの手前で SSL が終端しない限り、暗号化されたデータストリームは調査されません。 |  |

# PCI DSS適合証明についての報道資料

## PCI DSSの適合証明取得


| | WAPPLES-100 Type 2 | WAPPLES-1000 Type 2 |
|---|---|---|
| アプライアンス | 1U Rack type | 2U Rack type |
| CPU | Single Intel 2.4 GHz Quad Core | Dual Intel Xeon 2.33 GHz Quad Core |
| Memory | 4GB | 8GB |
| HDD | 500GB | 500GB |
| Throughput | 最大500 Mbps | 最大2 Gbps |
| TPS | 7000 | 20000 |
| NIC | 10/100/1000 BaseTX (8ポート) | 10/100/1000 BaseTX (8ポート)<br>1000 BaseSFP (2ポート)<br>1000 BaseTX (2ポート)<br>オプティカルバイパス (オプション) |

### ☆ 報道資料（2009年12月）

WAPPLESがこのたびPCI DSS（Payment Card Industry Data Security Standard：PCIデータ・セキュリティ基準）適合証明を取得いたしましたことをお知らせします。

このたびの適合証明取得において、WAPPLESは**PCI DSSのバージョン1.2、要件6.6オプション2**を満たしました。また、すでにPayment Card Industry Security Standards Council（PCI SSC：PCIセキュリティ基準協議会）承認のQualified Security Assessors Company（QSAC：認定審査機関）であるテュフラインランドジャパン株式会社（www.jpn.tuv.com）が実施している100種類以上のテストにも合格しています。

WAPPLESは製品開発の段階からPCIDSS準拠に向けて取り組み、規格がVer.1.2という早い時期で、既に適合証明を取得しています

適合証明書

TÜVRheinland

証明書番号： AK 50170567 0001

試験報告書番号： 12606696 002

保有者： ベンタセキュリティ システムズ株式会社
〒100-0013東京都千代田区霞が関3-3-2
新霞ヶ関ビル18F

製品： Web アプリケーションファイアウォール

識別： WAPPLES Model 100, 1000, 2000, 5000
バージョン 3.0 R11
試験報告書記述の設定による

認証に使用した技術基準： PCI DSS v.1.2 要件6.6オプション2

この適合証明書は、上記製品の試験サンプルが上述の技術基準に適合していることを証明するものです。この証明書は上記製品の量産品すべての適合を証明するものではありません。またテュフラインランドの適合性マークの使用は許可されません。

発行年月日
2009 年 12 月 9 日

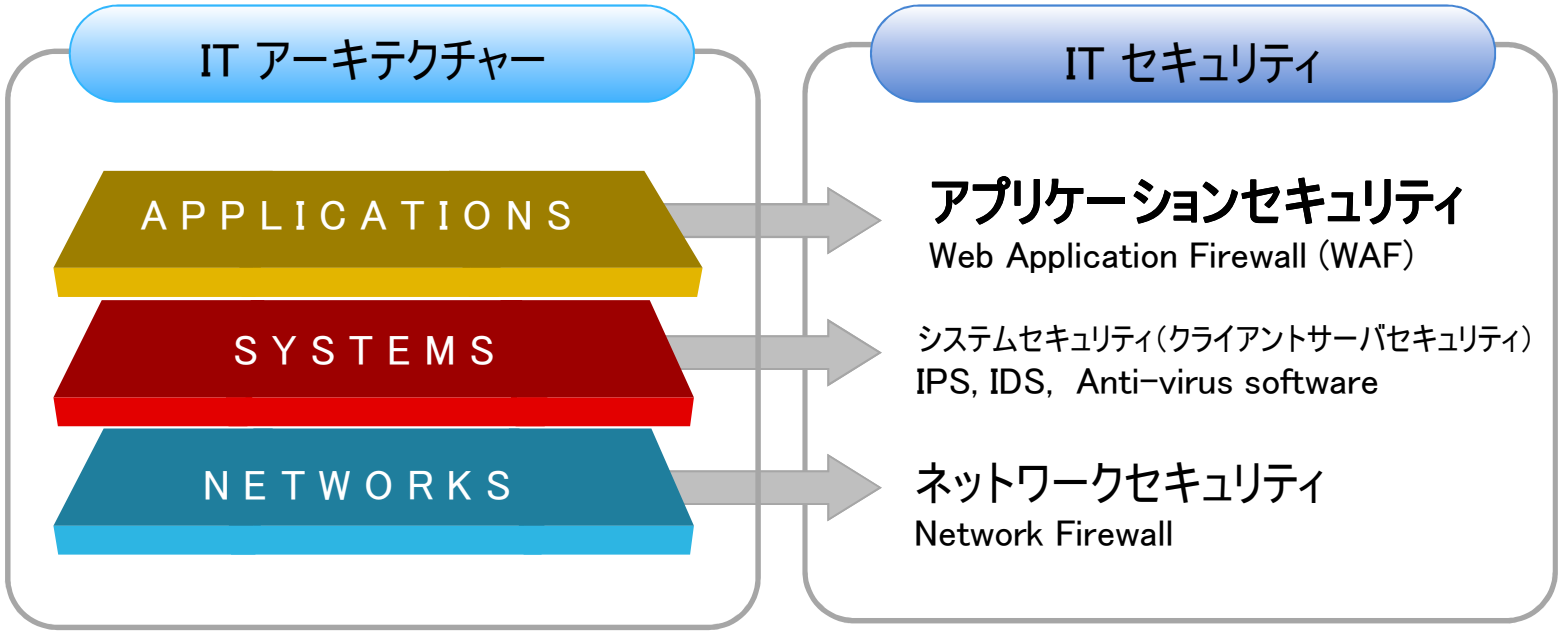
製品認証機関
Dipl.-Ing. R. Keller
ランドルフ ケラー

テュフ・ラインランド・ジャパン株式会社
TÜV Rheinland Japan Ltd. - Yokohama 222-0033 - JAPAN

# システムコンポーネントの安全性

## 安全なITシステムをつくるには

ITアーキテクチャで分割されているそれぞれのレイヤ―ごとに、適切なセキュリティを実装することが望ましいです。1つのレイヤ―が他のレイヤ―までもカバーするようなセキュリティ実装の仕方は望ましくありません。



# WAFの守備範囲

## WAFだけがWebアプリケーションの脆弱性に完璧に対応できる

OWASPが発表したWebアプリケーションの脆弱性について、確実に防御できるのはWAFだけとなります。

| OWASP Top 10 Application Vulnerabilities for 2010 の脆弱性 | Firewall | IPS/IDS | WAF |
|---|---|---|---|
| 1.インジェクション（SQLインジェクション、OSインジェクション等） | × | △ | ○ |
| 2.クロスサイトスクリプティング | × | △ | ○ |
| 3.不完全な認証とセッション管理 | × | △ | ○ |
| 4.危険な直接的オブジェクト参照 | × | × | ○ |
| 5.クロスサイトリクエストフォージェリ（CSRF） | × | × | ○ |
| 6.セキュリティ設定の間違い | × | × | ○ |
| 7.安全ではない暗号保管 | × | × | ○ |
| 8.URLアクセス制限の不備 | × | × | ○ |
| 9.安全ではない通信 | × | ○ | ○ |
| 10.安全ではないリダイレクトとフォワード | × | × | ○ |

# WAPPLES主要機能&特徴

- **多様なウェブセキュリティ機能を提供**
  - **ルールベース(ロジック分析エンジン:日本で特許を取得)**によるウェブ攻撃を検知、遮断
  - アクセスコントロール
  - 攻撃に対し多様な対応を提供
- **個人情報流出防止及びコンテンツ保護**
  - マスキング処理によりクレジットカード番号流出防止
  - 不適切単語の自動変換機能を搭載
- **便利な強力な管理ツールを提供**
  - 各種情報を22種類のチャートで表示
  - 設定ウィザードにより容易にセキュリティポリシーを設定
- **多様なウェブ環境をサポート**
  - 暗号化通信(SSL)の内容を検査
  - 冗長化構成をサポート(アクティブ-アクティブ、アクティブスタンバイ)
- **安定したサービス提供のためにトラブル対応機能を提供**
  - 自己診断機能(Watchdog)
  - バイパスモード
  - 監査機能

WAPPLES

# 検知方法の違いによる長所&短所

## ブラックリストとホワイトリスト

事前にリストアップされた接続は全て遮断する／事前にリストアップされた接続のみ許可する

## シグネチャベースのパターンマッチングとは？

基本はブラックリストタイプで、過去に認識された攻撃リクエストのパターン（シグネチャ）をデータベース化し、リクエストの内容をシグネチャと比較することで攻撃検知を行う手法です。

※ ブラックリストもホワイトリストも、事前にリストへ登録された内容に対してのみ有効であり、未知の接続や新たな接続には有効ではありません。シグネチャベースも含めて、常にリストの定期的な更新が必要です。

## ルールベース（ロジック分析エンジン）とは？

予め**プログラミングされた26（現時点）種類の攻撃検知エンジンの集まり**です。このロジック分析により、**未知の攻撃へも対応出来ます**。更に個々が独立することで処理の高速化と運用の簡素化を実現しています。

## クレジットカード番号を識別できるか？

一見ランダムに生成されていそうなクレジットカード番号は、実は発行会社により番号の作り方が定められている

| | クレジットカード番号 | 他社製 | WAPPLES |
|---|---|---|---|
| 1 | 2123-4214-1232-7584（発行会社のルールに基づいた番号） | 検知できない | 検知 |
| 2 | 1111-2222-3333-4444（ランダムに入力したもの） | 検知できない | 検知しない |

※WAPPLESはクレジットカード番号の作り方（生成ロジック）を認識しており、クレジットカード番号であると判断することが可能です。

# アノニマス攻撃について

## 1. アノニマス（Anonymous）によるサイバー攻撃

6月25日、世界的ハッカー集団・アノニマス（Anonymous）により日本の重要Webサイトが立て続けに攻撃を受けました。（財務省、裁判所、JASRAC、民主党、自民党、知的財産高等裁判所、国土交通省関東整備局霞ヶ浦河川事務所など）
アノニマスは、特定の目的をやり遂げるため、特定されたターゲットを狙うと意味では標的型攻撃に該当するとも言えます。

## 2. アノニマスの攻撃ツール＆手口

アノニマス(Anonymous)がDDos攻撃を行う際に使っているという「HOIC（High Orbit Ion Cannon）」ツールです。
このツールのもっとも強力な機能は、「Booster」であります。
**シグネチャーベース製品だと、Boosterによってランダムに生成されたリクエストには対応できず、どれだけシグネチャーを登録すればやり切れるかも不明であります。（シグネチャーベースのWAFの根本的限界とも言われています。）**

## 3. 防御方法の一例

**WAPPLESのロジック分析エンジンにより、様々のDos系攻撃が持っている動きの特徴を取り入れたリクエストの時間差による対応（MayblockTimeの実装）にてランダムで生成されるリクエストにも対応できます。**



株式会社大和ソフトウェアリサーチ
アウトソーシング事業本部

〒102-0083
東京都千代田区麹町1-5-2
tel:03-3262-8558
e-mail:outsales@dsr.co.jp