Penta SECURITY

WAFとデータベース暗号化の役割

ペンタセキュリティシステムズ株式会社
代表取締役社長　桜田仁隆

January 22nd , 2014

IPA発表「2013年版 10大脅威　身近に忍び寄る脅威」

タイトル	説明	ペンタの対応
第1位　クライアントソフトの脆弱性を突いた攻撃	クライアントソフトの脆弱性を悪用されることにより、ウイルスに感染したり、システム内の情報が窃取されるなどの被害の可能性があります。	
第2位　標的型諜報攻撃の脅威	政府機関や宇宙航空産業への攻撃が報道され、機密として扱われている政府関連情報や特殊技術情報の流出が疑われています。	○
第3位　スマートデバイスを狙った悪意あるアプリの横行	個人情報を収集する手口がより巧妙化しています。	
第4位　ウイルスを使った遠隔操作	ウイルスに感染したPCは、これまでもスパムの送信やDDoS攻撃のために悪用されてきました。	
第5位　金銭窃取を目的としたウイルスの横行	2012年からは国内のインターネットバンキングでも同様の手口による被害が確認されだしています。	
第6位　予期せぬ業務停止	システムのクラウド化が進む中、2012年は、レンタルサーバー企業において人為的ミスによる大規模障害が発生しました。	
第7位　ウェブサイトを狙った攻撃	ウェブサイトを狙った攻撃は、旧来から認識されている脅威ですが、残念ながら被害が後を絶ちません。ウェブサイト内の個人情報窃取や、ウェブサイトの改ざんによるウイルス配布など、組織や個人ユーザーに影響を及ぼす脅威です。	◎
第8位　パスワード流出の脅威	オンラインサービスの増加に伴い、ユーザーが複数のパスワードを管理する必要が生じています。その結果、同一のID/パスワードを使い回すユーザーが多くなり、一つのウェブサイトでパスワードが漏えいすることで、複数のウェブサイトで成りすましの被害に遭ってしまいます。	○
第9位　内部犯行	内部の人間による故意の情報漏えいや不正操作による被害が報告されています。	○
第10位　フィッシング詐欺	フィッシング詐欺によってインターネットバンキングのパスワードを奪われると、知らないうちに口座から預金を引き出されてしまう恐れがあります。	○

75% のハッカーはWeb
アプリケーションを狙っている。

Gartner

93% 過去2年、

セキュア―ではない

Webアプリケーションを介して

ハッキングされていた。

Ponemon Institute

サイト改ざん、前年の2倍のペースで増加る「脆弱性」と「アカウント」

警察庁は、ウェブサイトの改ざんが前年の2倍を上回るペ-るとして、注意を呼びかけている。

同庁によれば、2013年1月以降にウェブサイトの改ざんが大きく分けると、「脆弱性が悪用されるケース」「FTPアられるケース」の2種類だという。

前者は、ブログシステムなど「CMS」に存在する既知の脆もので、1月から2月にかけて多数確認された。既存ファイではなく、不正なファイルがあらたに設置されるケースが在する旧バージョンの利用者が被害に遭った。

一方4月以降は、サイトのトップページに外部サイトへ誘導するiframeタグを挿入する改ざんが目立っているという。「FTP」のパスワードが窃取されたことにより不正アクセスが行われた事例が数例確認された。

同庁では、CMS利用の有無を確認し、利用している場合は利用バージョンの

Web改ざんの次の段階、ドライブ・バイ・ダ

日本IBMは26日、世界10拠点のIBMセキュリティー・オペレーション・センター月～6月）のインターネットセキュリティ情報に基づき、主に国内の企業環境に影響年上半期Tokyo SOC 情報分析レポート」を発表した。

ドライブ・バイ・ダウンロード攻撃は前期比4倍に

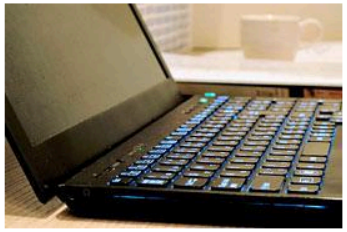
まず指摘されたのは、ドライブ・バイ・ダウンロード攻撃の急増についてだ。改ウェアがダウンロード・感染されてしまう攻撃で、今期の件数は3972件。前期（24.2倍に増加している。昨今、Webサイトの改ざん事例が多数報告されているが、次の段階と言えるもので、報告通り、多くのWebサイトが実際に改ざんされている

攻撃の手口として、前期まではAdobe製品の脆弱性を突いたものが大半だったが、増。前期の308件（全体の32.3%）だったのが、今期は3192件（80.4%）と、件

特に2013年1月～3月に多発。CMSやWebアプリケーション・フレームワークのが多発したころとちょうど重なるという。グローバル・テクノロジー・サービス事

ユーザーに被害を及ぼす「ウェブサイト改ざん」 気づかず「放置」した企業の責任は？

弁護士ドットコム：ニュース一覧
2013年10月18日(金)19時00分配信



ユーザーに被害を及ぼす「ウェブサイト改ざん」 気づかず「放置」した企業の責任は？
弁護士ドットコム

「企業のウェブサイトがこっそり改ざんされるケースが増えている」。警察庁サイバーテロ対策技術室がこう注意を呼びかけている。ウェブサイトの改ざんはその企業にダメージをもたらすだけではない。そのサイトを訪れたネットユーザーにも深刻な被害を与える恐れがあるので、注意が必要だ。

同庁サイバーテロ対策室によると、今年1～2月のウェブサイト改ざんはサイトに「犯行声明」を置くなど、明らかに改ざんされたことが分かるケースが多かった。しかし、5～6月の改ざん事例は「サイトの外見上変化がない」「閲覧者が気づかないまま悪意あるサイトに誘導される」「誘導されると不正プログラムに感染するおそれがある」など、新たな特徴が出てきているという。

不正プログラムに感染すると、ネットバンキングの口座番号やパスワードなどが盗まれる可能性があるほか、偽のウイルス対策ソフトを購入させるための誘導メッセージが出たり、コンピュータを使うために300ドル支払えといった「身代金」を要求されるケースもあるという。

【特集】改ざん
- 「Fuck-JP.html」……9月18日、複数のウェブ改ざんが確認され始め
- 「9月18日」にサイバー攻撃が急増の可能性
- 改ざんされたWebサイト閲覧によるマルウェア感染に注意

情報処理推進機構（IPA）およびJPCERTコーディネーションセンター（JPCERT/CC）は6日、ウェブサイト改ざん等のインシデントの急激な増加を受け、ウェブサイト運営者および管理者に対し、改めて点検と備えを呼びかけた。

ウェブ改ざん被害の推移（JPCERT/CCへの報告による）

ウェブ改ざん等の発見、被関する連絡先

JPCERT/CCによると、ウェブサイト改ざんの被害件数が2013年6月、7月には1,000件を越えるなど、急激な増加が見受けられるという。2年は7月の400件弱が最高だったが、2013年は5月に505件、6月に1028件、7月に1106件、8月件となっており、今年に入って大きく被害が拡大していることが分かる。IPAへの届出も同じく増見られ、2013年6月、7月には、「今月の呼びかけ」で注意喚起が行われている。

昨今増加しているウェブサイトへの攻撃の代表的な例は、「ウェブサイトの管理端末への侵入るウェブサイト改ざん」「パスワードリスト攻撃」「ソフトウェアの脆弱性を狙った攻撃」「SQLインジョン攻撃」などがあり、攻撃手法も多様化している。

今アクセスしているWebサイトは安全なんでしょうかという話

山本 一郎｜個人投資家
2013年6月6日 21時13分

コメントを見る(0件)

山本一郎です。偽名ではありませんので安全です。

ところで、このところネットにおけるセキュリティ問題について報道される機会が増えていますが、今年になってから企業や団体等のホームページが改ざんされる事件も増加傾向にあるようです。

ウェブサイト改ざん事案の多発に係る注意喚起について（PDF書類　警察庁）

:が「Web改ざん」の被害拡大につい

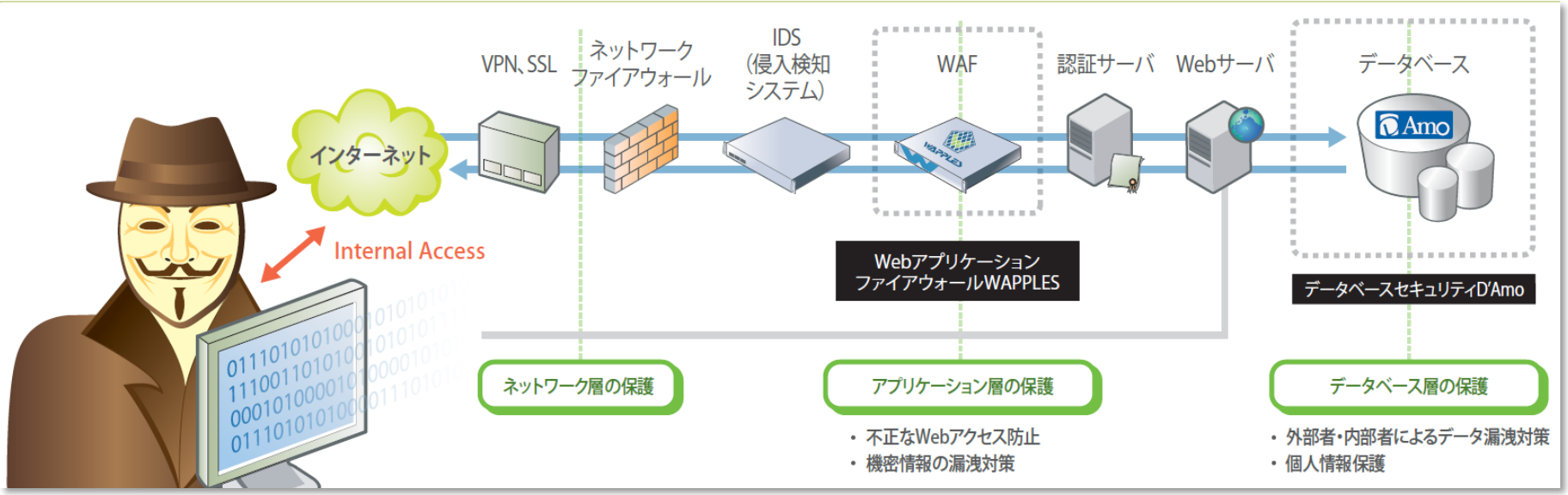
2013年7月 4日

推進機構(IPA)は、6月26関等のWebサイトの改ざて、サイト閲覧者のパソする可能性が高まっていいる。

発生しており、6月に入っが多いと思われる企業等受けたことが報じられてんにより、サイトを閲覧しンの脆弱性を利用され、閲覧しただけでウィルスに感染する可能性があると指摘している。

Webサーバの保護やデータベースの暗号化
は非常に重要な防犯対策です。

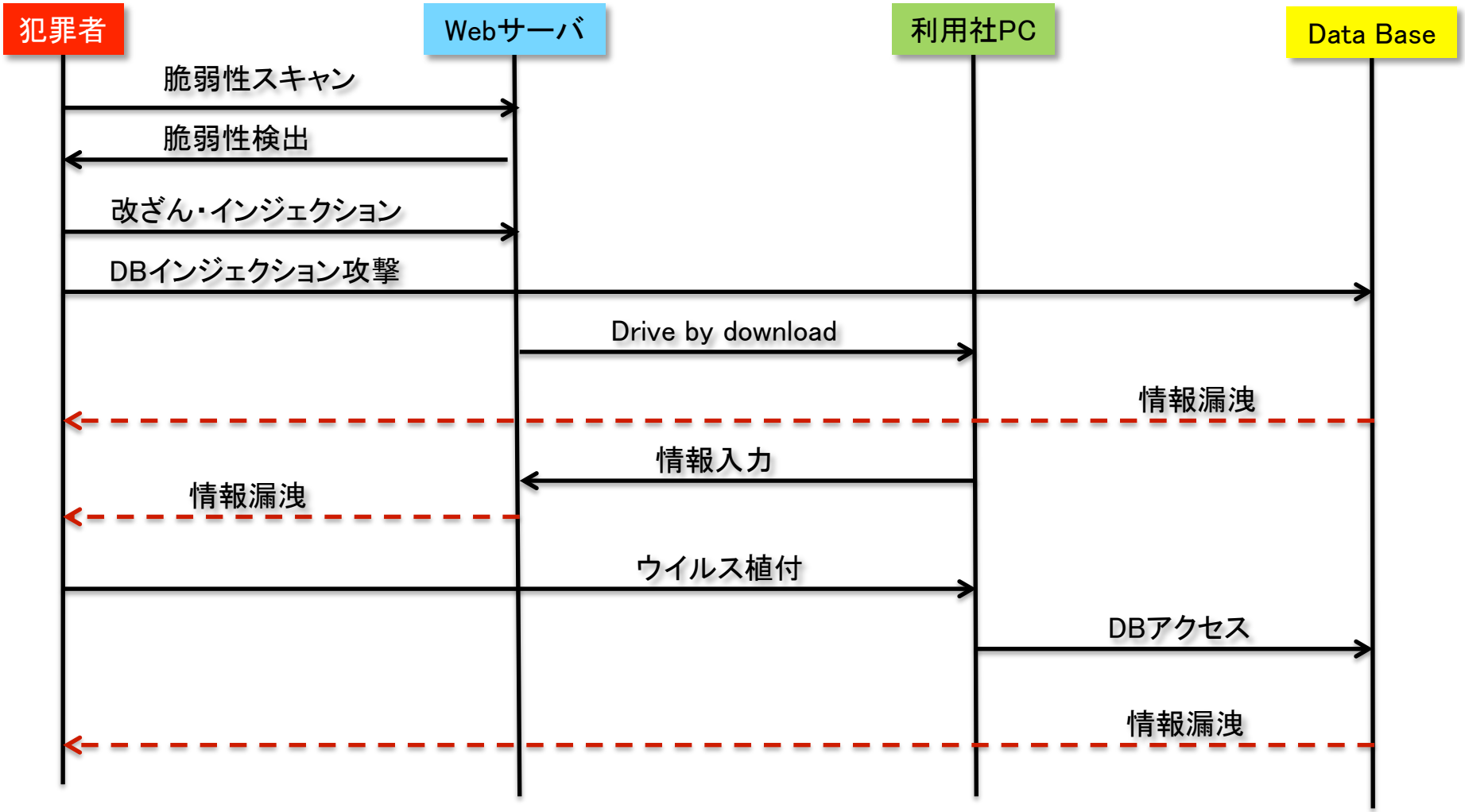
情報セキュリティ



**** DLP(data loss preventionあるいはdata leak prevention)システムを導入し全ての侵入経路に対しモニタリングをすることは可能だが、この方法はとても<u>コストが高くつき運用が難しい</u>ため、**システム上複雑な侵入経路がある場合管理から外れてしまい安全ではない状態で運用されることが多々ある** (Global Data Leakage Report, 2009, infowatch)*

1. 重要なデータへの不正なアクセスや情報の露出のような脆弱性に対しての対策としては、OS、ネットワーク、アプリケーション、DBなど、各領域に適したセキュリティソリューションを実現することが必須
   1) 加えて、アカウント管理、認証、権限管理などにわたり、全社的認識が要

犯罪手口の確認


犯罪者
Webサーバ
利用社PC
Data Base
脆弱性スキャン
脆弱性検出
改ざん・インジェクション
DBインジェクション攻撃
Drive by download
情報漏洩
情報入力
情報漏洩
ウイルス植付
DBアクセス
情報漏洩

情報セキュリティの領域

Data Privacy & Security

データベース層の保護

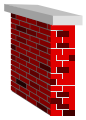
Web Application Firewall

アプリケーション層の保護

Secure OS & Anti Virus

システム・ＯＳ層の保護

Firewall, VPN, SSL



ネットワーク・レベルの保護

ネットワーク・レベルやシステムOSに偏った
情報セキュリティ対策の現状

シグネチャ型WAFの限界

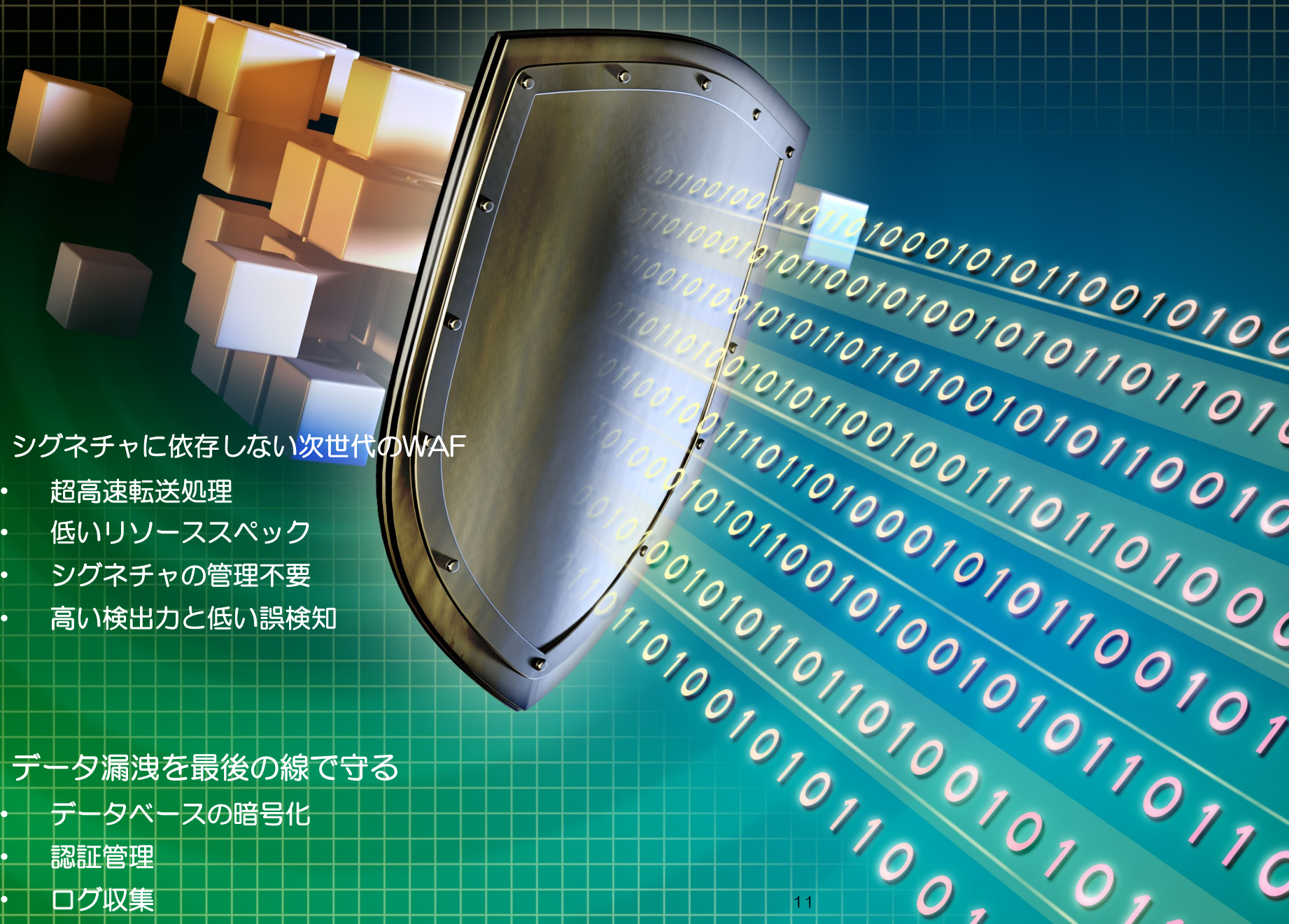
- シグネチャに無いもの条件は検出出来ない
  - シグネチャが比較検知方式である性質上、ホワイトでもブラックでも、リストに無いものには対応出来ない。
  - 非存在であるため不可知

- パフォーマンスの経年劣化
  - シグネチャ型のWAFはパケット単位でデータを参照するため、仕組み上シグネチャの増加とともに、参照回数が増加しデータベースの成長と反比例して、パフォーマンスは劣化致します。

- 誤検知のリスク
  - シグネチャでは1ビットのズレが誤検知を引き起こすため、非シグネチャ型と比べ、どうしても誤検知率は高くなります。
  - 検知率を高めるためには、より詳細なシグネチャが必要となり、パフォーマンス劣化へと、悪循環へと入っていきます。

- 仮想環境への負担
  - WAFをクラウドサービス等に実装した際には、ユーザトラフィックだけでなく、シグネチャの増加するために、同等のパフォーマンスを担保するため、プラットフォーム要件を改善する必要があります。必然的にコストが増えてまいります。

ペンタセキュリティだけが出来ること

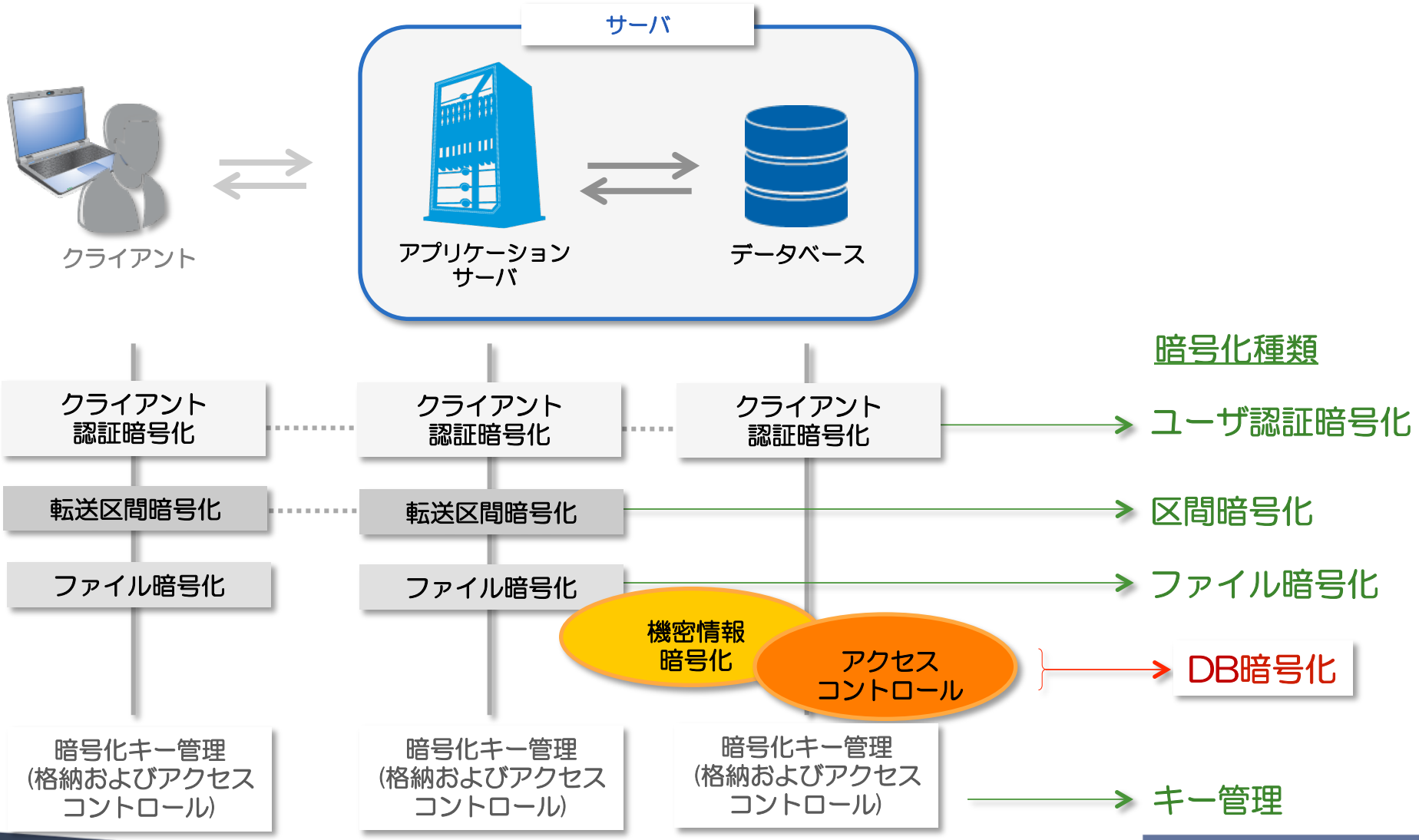


- シグネチャに依存しない次世代のWAF
  - 超高速転送処理
  - 低いリソーススペック
  - シグネチャの管理不要
  - 高い検出力と低い誤検知

- データ漏洩を最後の線で守る
  - データベースの暗号化
  - 認証管理
  - ログ収集

暗号化ソリューション種類

ユーザ認証暗号化 / 区間暗号化 / ファイル暗号化 / DB暗号化



暗号化ソリューションの選定

暗号化ソリューションの重要な選定は暗号化機能に加え、アクセス制御や監査そしてキーの管理が重要となります。

キー管理

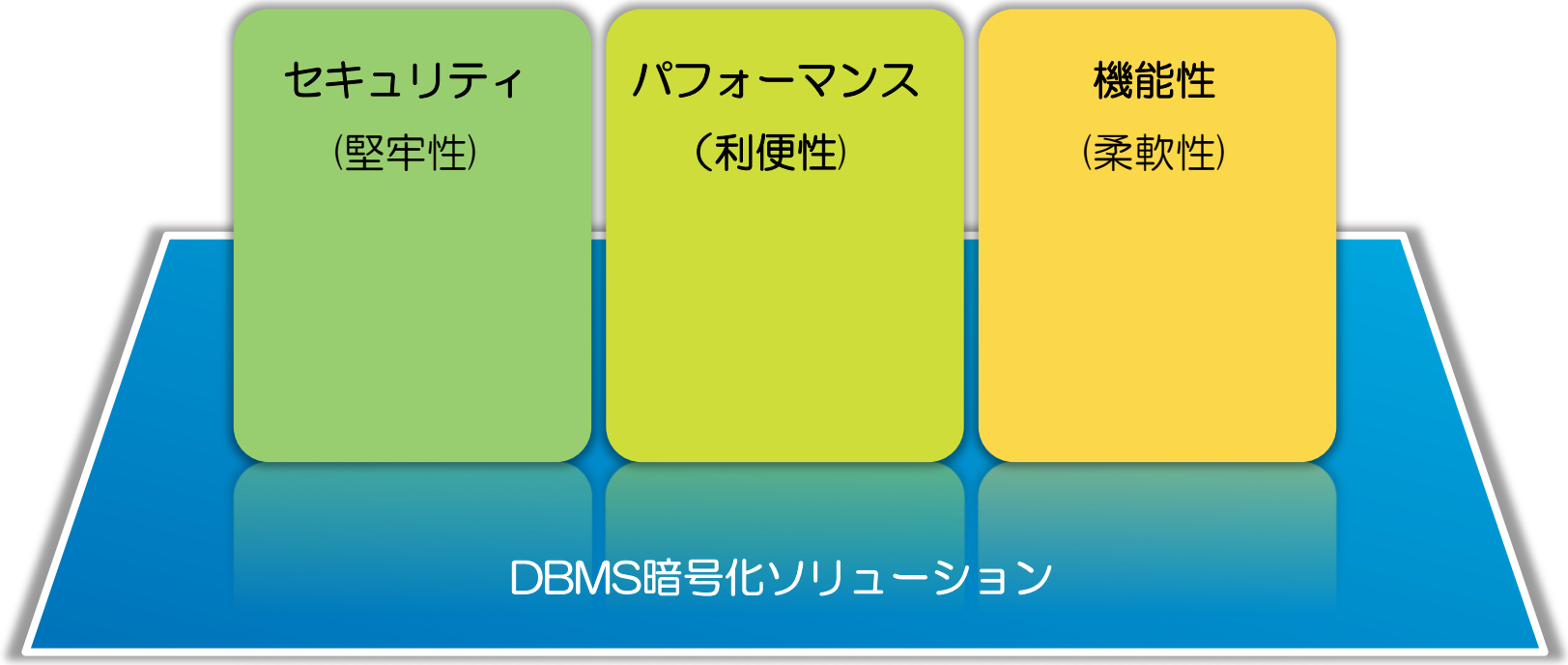
暗号化、アクセスコントロール、
監査、キー管理の
トータルソリューション

セキュリティ
ソリューション
DB暗号化

DB暗号化製品の選定

暗号化ソリューションの選定にはセキュリティ(堅牢性)やパフォーマンス(利便性)、機能性(柔軟性)が重要な要素となります。

1. DB暗号化ソリューションの導入は、本来の機能であるセキュリティ機能だけでなく、導入前後のパフォーマンス劣化、その他管理者のため機能等を全て加味して判断されます。
   →DAmoはデータベースのトータルセキュリティソリューションです。



ペンタセキュリティの優位性

❑ エンジンレベルの暗号化ソリューション

セキュリティ	● DB管理者(DBA)とセキュリティ管理者の権限分離 ● 暗号化カラムに対しDBアカウントおよびIPごとのアクセスコントロール ● ログの偽造および改ざんの防止機能 ● 暗号化カラムに対し監査機能
パフォーマンス	● 重要データに対し「選択的」カラム単位の暗号化 ● 暗号化データに対し順次維持およびインデックス検索対応
機能性	● アプリケーションに対しての独立性 ● 重要データに対し「選択的」カラム単位の暗号化 ● 暗号化データに対し順次維持およびインデックス検索対応 ● アプリケーションに対しての独立性 ● 認証情報(パスワードなど)の暗号化のためのハッシュ対応

護らなければいめないのは

t h a n k y o u

Penta SECURITY

Penta Security Systems K.K.
Ascend Akasaka Bldg. 3F, 3-2-8 Akasaka, Minato-Ku, Tokyo 107-0052 Japan
Tel. 81-3-5573-8191 Fax. 81-3-5573-8193 / www.pentasecurity.co.jp