



サイバー攻撃は、 セキュリティ対策に取り組んでいる企業だけが知っている

認知しなければ分からないサイバー脅威とゼロ・トラスト (Zero Trust)のマインドセット

2019.12.06

グローバルビジネス本部

日本セキュリティビジネス戦略部門

陳 貞喜

目次

I. サイバー攻撃は、セキュリティ対策に取り組んでいる企業だけが知っている

II. 日本企業におけるセキュリティ・アプローチ

III. 「ビジネスを守る」の考え方

- データ中心のアプローチ
- ゼロ・トラスト

IV. まとめ



Company Overview

Founded 1997年 7月

CEO/Founder 李 錫雨 (リ ソグ)

Staff 230 人+ ※ 研究・開発および技術部門130人+(2019/07)

Located ソウル (韓国)

Overseas Branch 東京、ヒューストン、シンガポール


Overseas Network タイ、オーストラリア、ニュージーランド、マレーシア、インドネシア、イタリア、UAE、ウクライナ、キルギス 等々


Business Area 企業情報セキュリティ(web/データ/認証セキュリティ), IoT, Blockchain

Client 政府、官公庁、文教、一般企業、金融等 4,000カスタマー

Products データ暗号化プラットフォーム D'Amo
Webセキュリティソリューション WAPPLES
セキュリティ認証管理ソリューション ISign+
スマートカーセキュリティAutoCryptおよびIoT / blockchain


世界初


 クエリ変換装置利用
DB暗号化技術開発


 特性維持暗号化
データセキュリティ技術開発


 オープンソース基盤の
DB暗号化製品開発


韓国初

 RFC2510
公開鍵基盤製品開発

 データベース暗号化ソリューション
D'Amo


 スマートファクトリー・セキュリティソリューション
Penta Smart Factory Security


 インデックス・カラム暗号化開発


 SaaS型Webサイト・セキュリティサービス
Cloudbric


 スマートエネルギー・セキュリティソリューション
Penta Smart Energy Security


 KCDSA
デジタル署名システム開発

 コネクテッドカーセキュリティ・ソリューション
AutoCrypt

 マイナンバーセキュリティソリューション
MyDiamo

 日本市場へ
マイナンバーセキュリティソリューション提供

 POSセキュリティ・ソリューション

 鍵管理サーバのリリースおよび
韓国国内最高レベル「EAL 3 +」認証取得

 国内外
技術特許


83

 国内外
技術認証

58

 技術者
割合

60%

 製品関連
受賞

37



Asian Cyber
Security Vendor
of the Year



The First and Only
CCEAL4 Certified WAF



No.1 WAF Vendor
in the APAC Region



ICSA Labs
Certified WAF



Recognized on the
Gartner WAF
Magic Quadrant



SC Magazine Europe
Best SME Solution



PCI-DSS
Compliance



Hot Company in
Web Application
Security for 2016



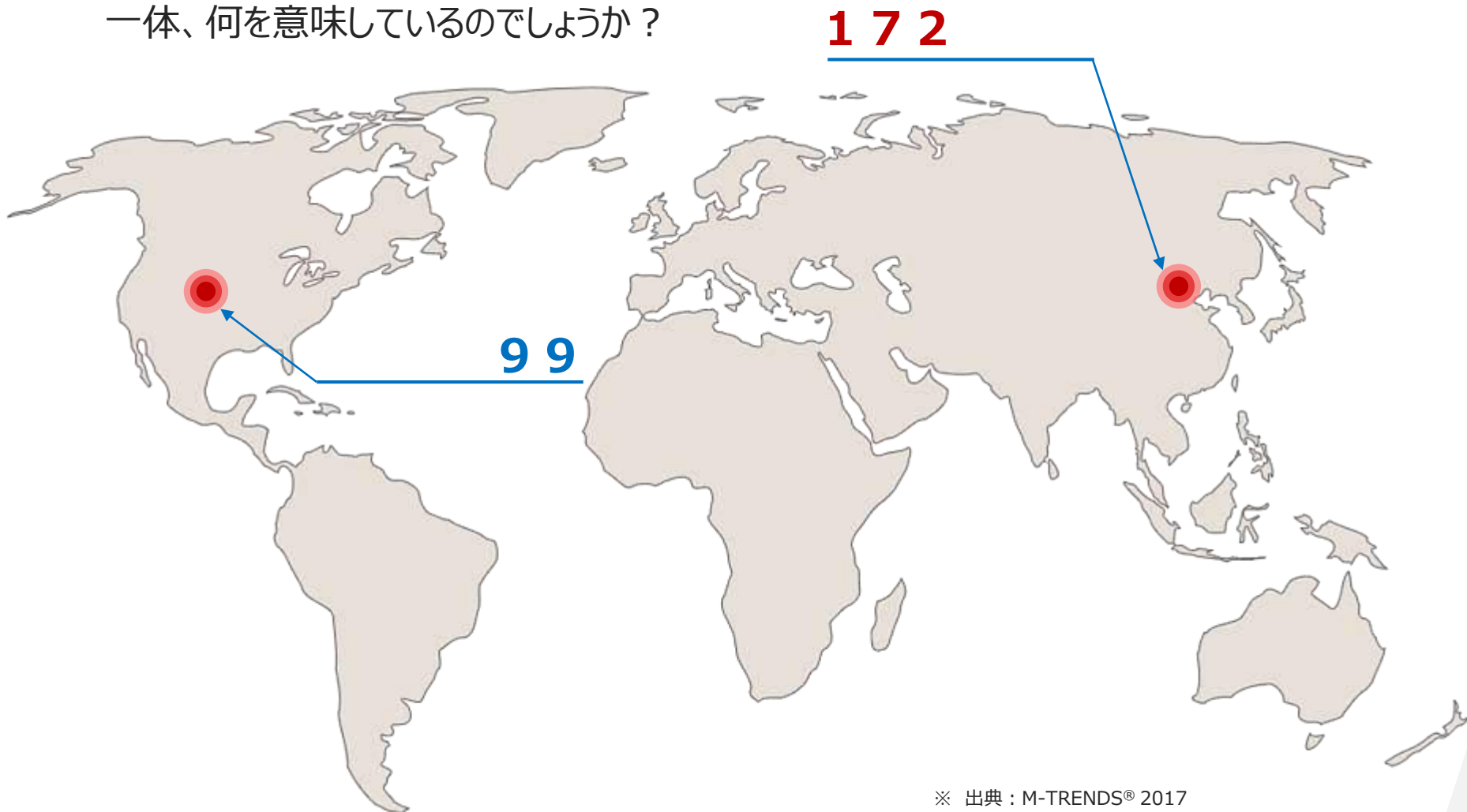
Cybersecurity Excellence
Awards Winner 2018

サイバー攻撃は、 セキュリティ対策に取り組んでいる企業だけが知っている

認知しなければ分からないサイバー脅威とセキュリティ概念

99と172

… **99**と**172**の数字。
一体、何を意味しているのでしょうか？



※ 出典：M-TRENDS® 2017

99と172

… 企業側でハッキングの攻撃を**認知する**までかかる時間

172日

アジア・パシフィック



99日

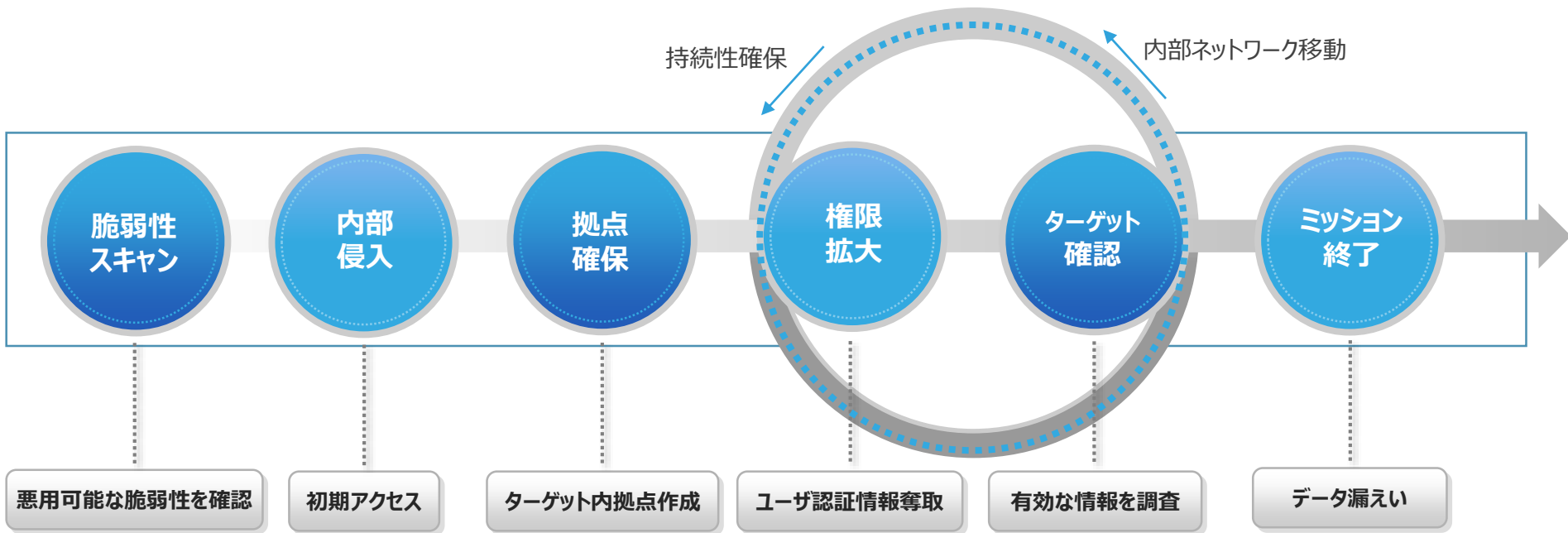
世界平均・アメリカ



※ 出典：M-TRENDS® 2017

サイバー攻撃のライフサイクル

Cyber Attack Lifecycle

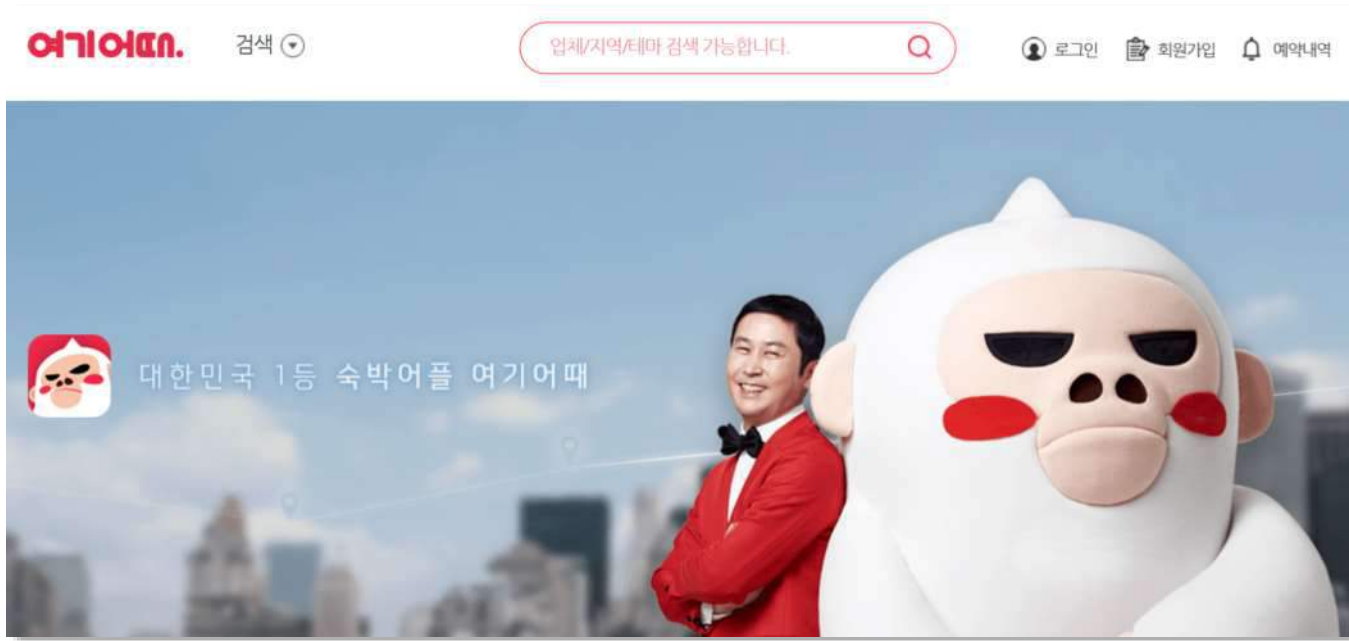


172日



○○○ホテルで楽しかった？事件 宿泊予約サイトのハッキング事件とその影響

事件発覚



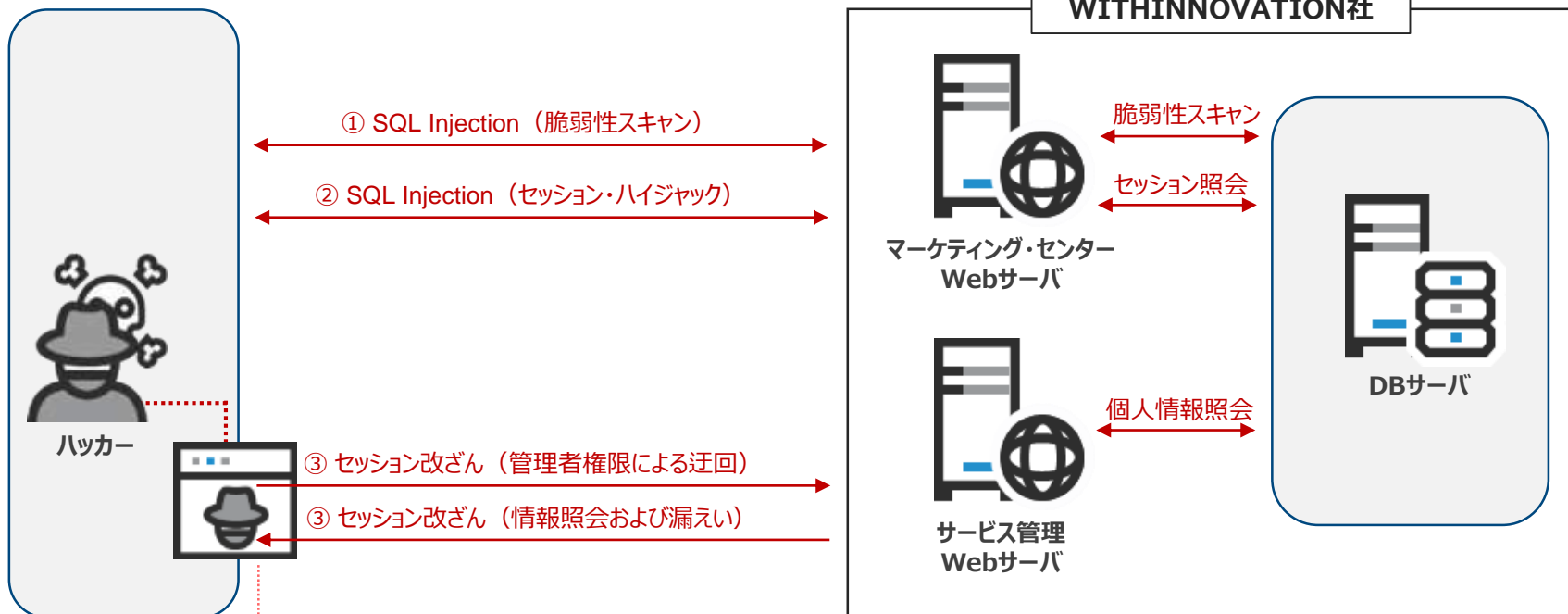
X月X日、○○○ホテルで、
楽しかった？全部知っているけど。笑

.....

同宿泊予約サイトをユーザに対し、
合計4,817件の脅迫性・性的メッセージが送られ、事件発覚

〇〇〇ホテルで楽しかった？ 事件 宿泊予約サイトのハッキング事件とその影響

事件後調査および原因



予約内訳の情報 → CSVファイル
提携店の情報 → EXCELファイル



サービス管理ページから管理者権限を利用し、会員情報を検索 **99万584件**の会員情報漏えい

3年9ヶ月間の最大93,014名の会員情報の流出

幻冬舎会員情報の流出事件

速報

幻冬舎のサイトから最大9万3000人の情報が流出、会員の指摘まで気づかず

根本 浩之 = 日経NETWORK

2018/01/15

日経NETWORK

目次一覧

シェア 17 | ブックマーク 2 | Pocket | ツイート | 保存する

幻冬舎は2018年1月15日、同社のウェブサイトから会員情報が流出したことを明らかにした。最大9万3014人のメールアドレス、ユーザーID、名前の情報が流出した可能性がある。

狙われたのは同社のWebサイトである「幻冬舎plus」。サイトに脆弱性が有り、そこを突かれて2013年11月12日から2017年8月18日までの間に会員登録した人について情報が流出した可能性がある。決済に使うクレジットカードや住所、電話番号などの情報は含まれていない。



1. 事件の概要

幻冬舎より運営されている「幻冬舎plus」への第三者による不正アクセスがあり、2013年11月12日から2017年8月18日までの3年9ヶ月の間、会員登録した最大93,014名のメールアドレス、ユーザーID、お名前（読み仮名含む）が漏えい



2. 事件の発覚

2017年12月27日、幻冬舎plusの会員からの連絡により発覚
会員登録時入力したメールアドレスへフィッシングメールが配信

3. 事件の原因

- ① 協力会社より、2017年3月30日に実施されたシステムのバージョンアップの際に発生した脆弱性に起因
- ② 2017年8月18日、パフォーマンス定価を検知し、調査した際に脆弱性を発見し、対応
→但し、その際に脆弱性が発生した期間に対し協力会社による不正アクセスの調査は実施されず

Apache Struts2脆弱性を突いた攻撃

日本事例

GMO-PG、Struts2脆弱性によるクレジットカード情報流出が確定

広田 望 = 日経コンピュータ

2017/04/05

日経コンピュータ

目次一覧

共有 0 | フックマーク | Pocket | ツイート | 保存する

GMOペイメントゲートウェイ（GMO-PG）は2017年4月5日、3月10日にApache Struts2の脆弱性を悪用され「情報漏洩の可能性がある」（GMO-PGのWebページ）としていた個人情報について、「不正に取得されたことが判明した」（同社）と統報を公開した。

GMO PAYMENT GATEWAY

2017年3月9日

GMOペイメントゲートウェイが運営するサイトにてApache Struts2の脆弱性を突いた攻撃により、クレジットカード番号および有効期限、セキュリティコードを含む、個人情報約72万件の漏えいが確認

- 東京都の都税クレジットカードお支払サイト
- 独立行政法人住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイト

韓国事例

日本経済新聞

2017年5月27日（土）

Web刊 | 速報 | ビジネスリーダー | マーケット | テクノロジー | アジア | スポーツ | マネー | ライフ | 新刊

トップ | 東アジア | 東南アジア | 南アジア | オセアニア | 中央アジアなど | ニュース | コラム

アジア > アジアニュース

アジア最新ニュースの掲載を始めました

ロッテがサイバー攻撃被害 THAAD配備で中国が報復？

2017/3/3 1:12

韓国 | 中国

共有 | 保存 | 印刷 | その他

【ソウル=加藤宏一】在韓米軍の地上配備型ミサイル迎撃システム（THAAD）の配備に対する中国の報復とみられる動きが相次いでいる。韓国のロッテ免税店のウェブサイトに

Apache Struts2の脆弱性を突き、自動化されたツールを利用し、韓国のWebサイトを改ざん

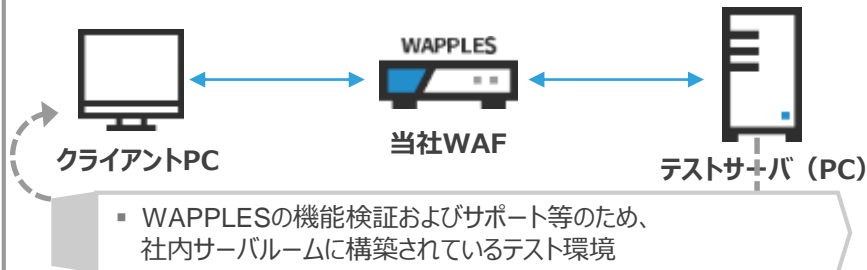


Apache Struts2脆弱性を突いた攻撃 Apache Struts2脆弱性を突いた攻撃



は?! テストサーバに Struts2の攻撃が来たって?

Struts2の攻撃が来たテスト環境構成



ルール名	発信元IP	国	URI
Request Header Filteri...	187.217.113....	🇩🇪	<未登録 Web サイト>/notFound.action
Request Header Filteri...	187.217.113....	🇩🇪	<未登録 Web サイト>/login.action
Request Header Filteri...	187.217.113....	🇩🇪	<未登録 Web サイト>/login.action
Request Header Filteri...	187.217.113....	🇩🇪	<未登録 Web サイト>/notFound.action

フィールド	値
ポリシー	0 検知なしに通過
ルール	Request Header Filtering
発信元IP	2.139.175.219
発信国	Spain
発信元IP	192.168.11.98:80
時刻	2017-03-27 19:12:09
Webサイト	未登録Webサイト
リクエストURI	/login.action
対応	エラーコード表示
危険度	0 (低)


```

Raw Data | Decoded Data
GET /login.action HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87
Safari/537.36
Host: 124.35.7.90
Accept: */*
Content-Type: multipart/form-data;
(#&#x002D;=&#x002D;login)OpnContext#@DEFAULT_MEMBER_ACCESS)
(#&#x002D;memberAccess?#&#x002D;memberAccess=&#x002D;#&#x002D;@container=#&#x002D;context
    
```

日本企業における セキュリティ・アプローチ

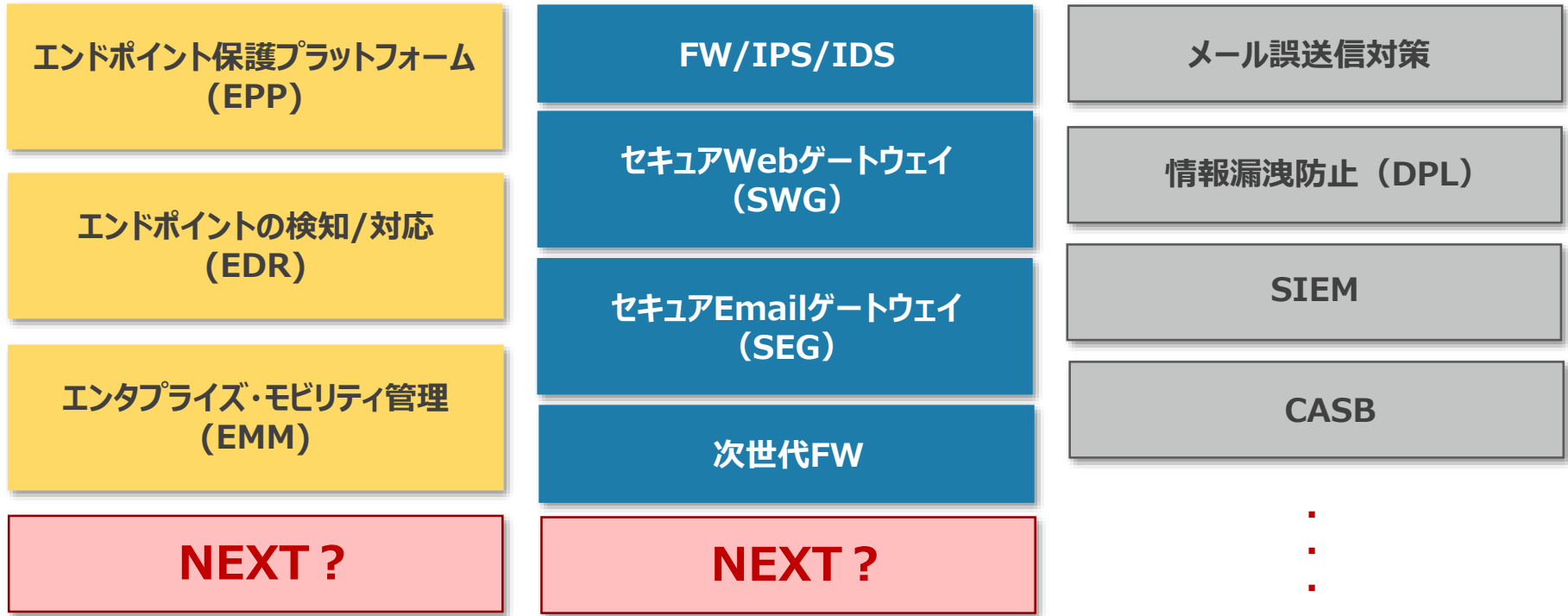


日本企業におけるセキュリティ アプローチ

Product-Centric Approach

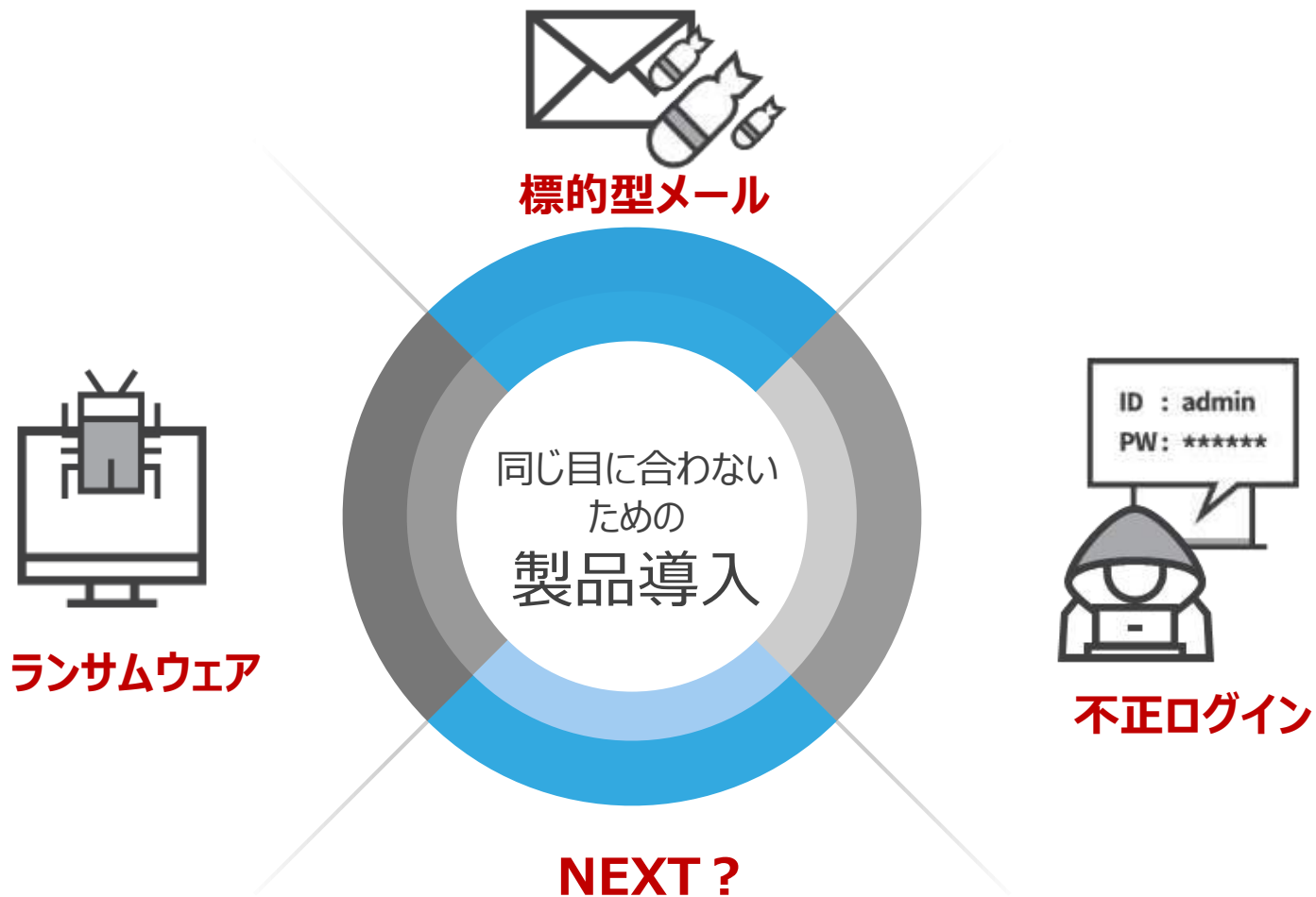
製品中心

日本企業におけるセキュリティのアプローチ



「**必要な製品は何か？**」という考え方で
製品を充足していくアプローチ

必要な製品は何か？ になってしまった要因：その1. 他社のインシデント



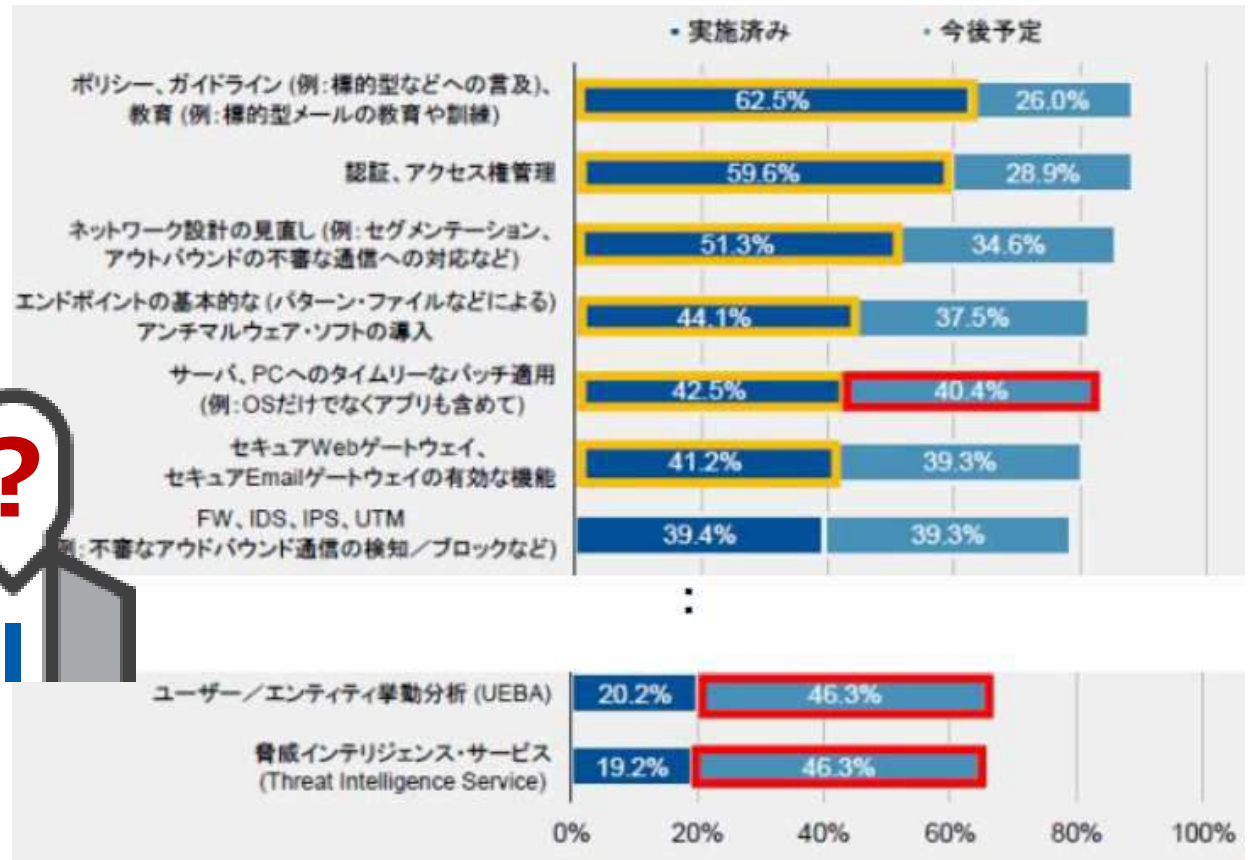
事件/事故をトリガーに騒ぎが繰り返されてきた歴史

必要な製品は何か？になってしまった要因：その2. 他社の動向

標的型攻撃やすり抜けるマルウェアへの対策の実施状況および予定

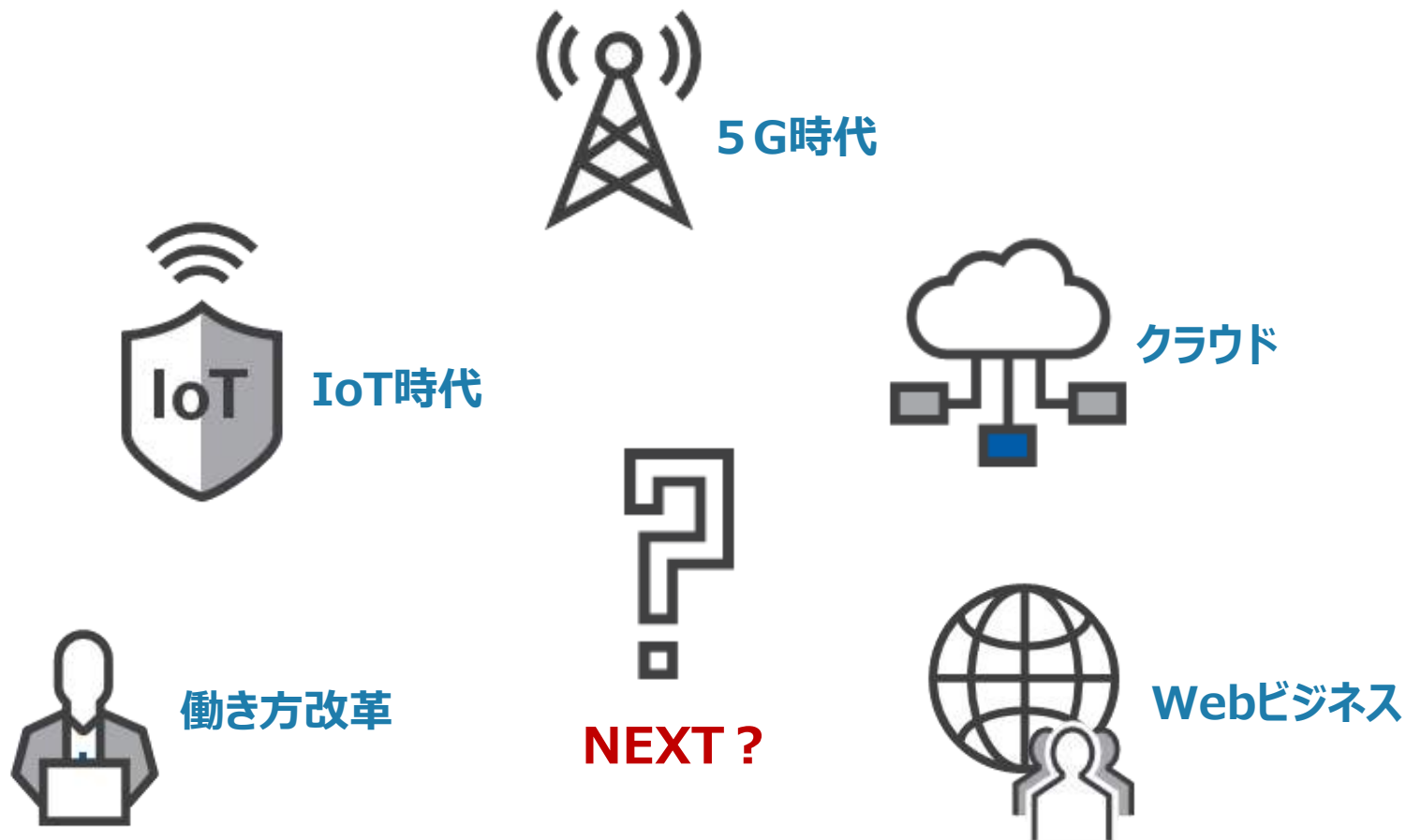
どの程度の企業が
この製品を導入しているか？

特に同業他社ではどうか？



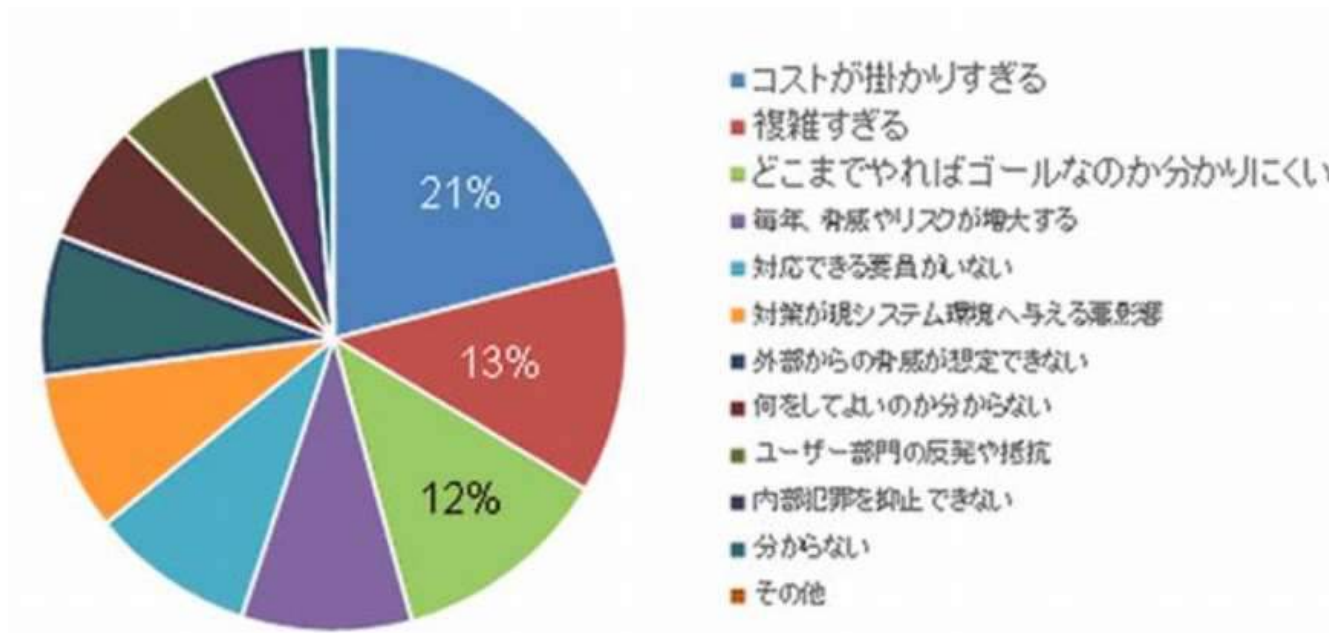
同業他社と同レベルの製品は導入しよう、という偏差值的思考

必要な製品は何か？になってしまった要因：その3. おかれている環境の変化



〇〇〇のセキュリティに必要な製品は？という考え方

それでも常に不安



セキュリティ 取り組み時 3大懸念点

- 21% コストが掛かりすぎる。
- 13% 複雑すぎる
- 12% どこまでやればゴールなのか分かりにくい

※ 出典：ガートナージャパン 調査結果（2016/07/04）

有効回答数515件（従業員2000人以上 253社、1000～1999人 108社、500～999人 154社）

情報セキュリティにおける企業側の悩み

●複雑

●費用対効果



●専門家の不在

「ビジネスを守る」の考え方

データ中心のアプローチ
ゼロ・トラスト



ビジネスを守る
セキュリティの取り組み方

Data-Centric Approach
データ中心

時代別セキュリティ・ニーズの変移

1980

1990

2000

2010

時代

PC



Network



Internet Biz



脅威

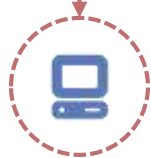
1990



ウイルス

感染 (infecting)

Personal Computer



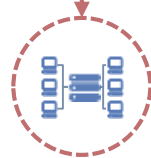
2000



ハッカー

侵入 (intruding)

Server System



2010



マルウェア ボット スпам 知られていない脅威

盗む (stealing)

Web Data



1990

2000

2010

2020

対策

アンチ
ウイルス

アンチウイルス
ソフトウェア

侵入防止

ネットワークファイアウォール
侵入検知システム
(Intrusion Detection System)
侵入防御システム
(Intrusion Protection System)

Webおよび
データ
保護

Webアプリケーション
ファイアウォール
データ暗号化・保護
データアクセス管理

時代別セキュリティ・ニーズの変移

1980

1990

2000

2010



時代

PC



Network



Internet Biz



Cloud + IoT



脅威

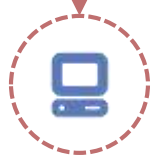
1990



ウイルス

感染 (infecting)

Personal Computer



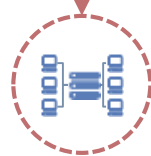
2000



ハッカー

侵入 (intruding)

Server System



2010



マルウェア ボット スпам 知られていない脅威

盗む (stealing)

Web Data



対策

1990



アンチウイルス
ソフトウェア

2000



ネットワークファイアウォール
侵入検知システム
(Intrusion Detection System)
侵入防御システム
(Intrusion Protection System)

2010



Webアプリケーション
ファイアウォール
データ暗号化・保護
データアクセス管理

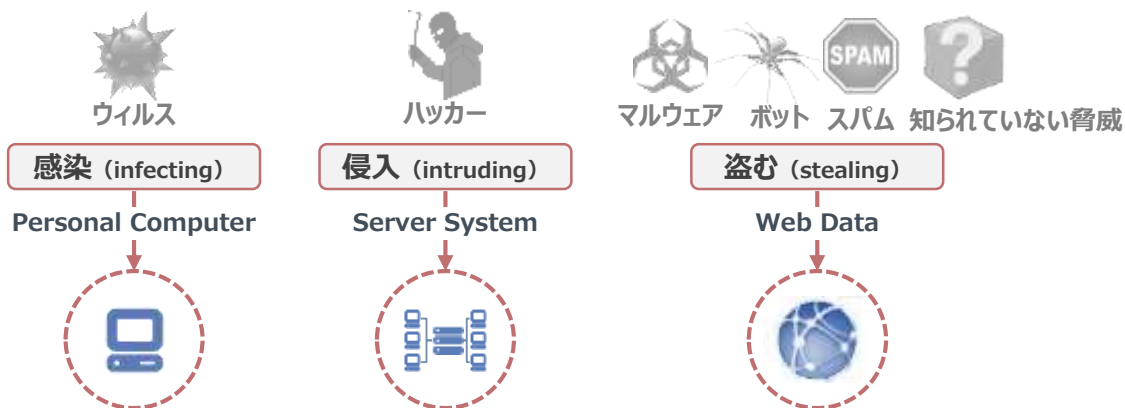
2020

時代別セキュリティ・ニーズの変移

Cloud + IoT



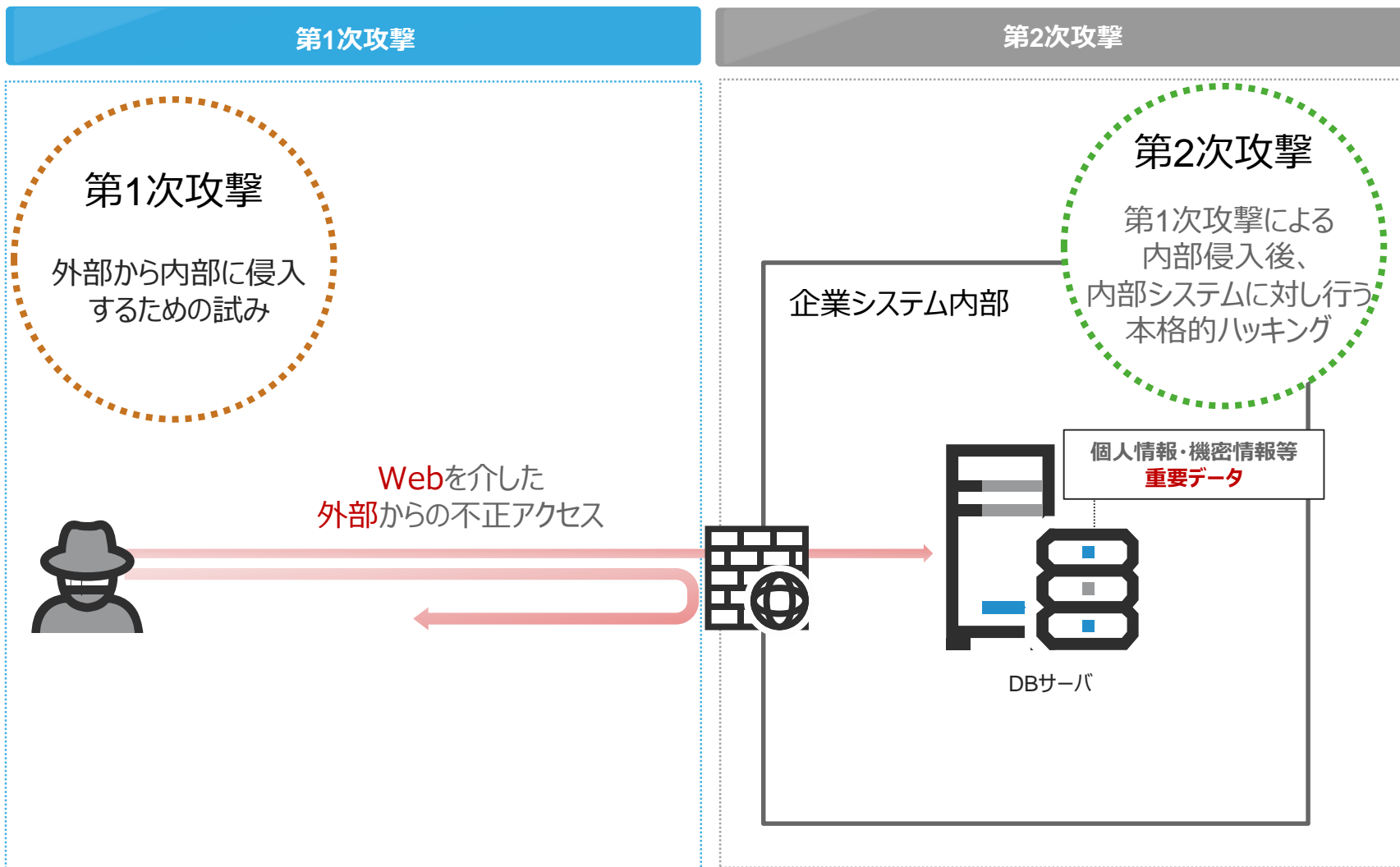
脅威



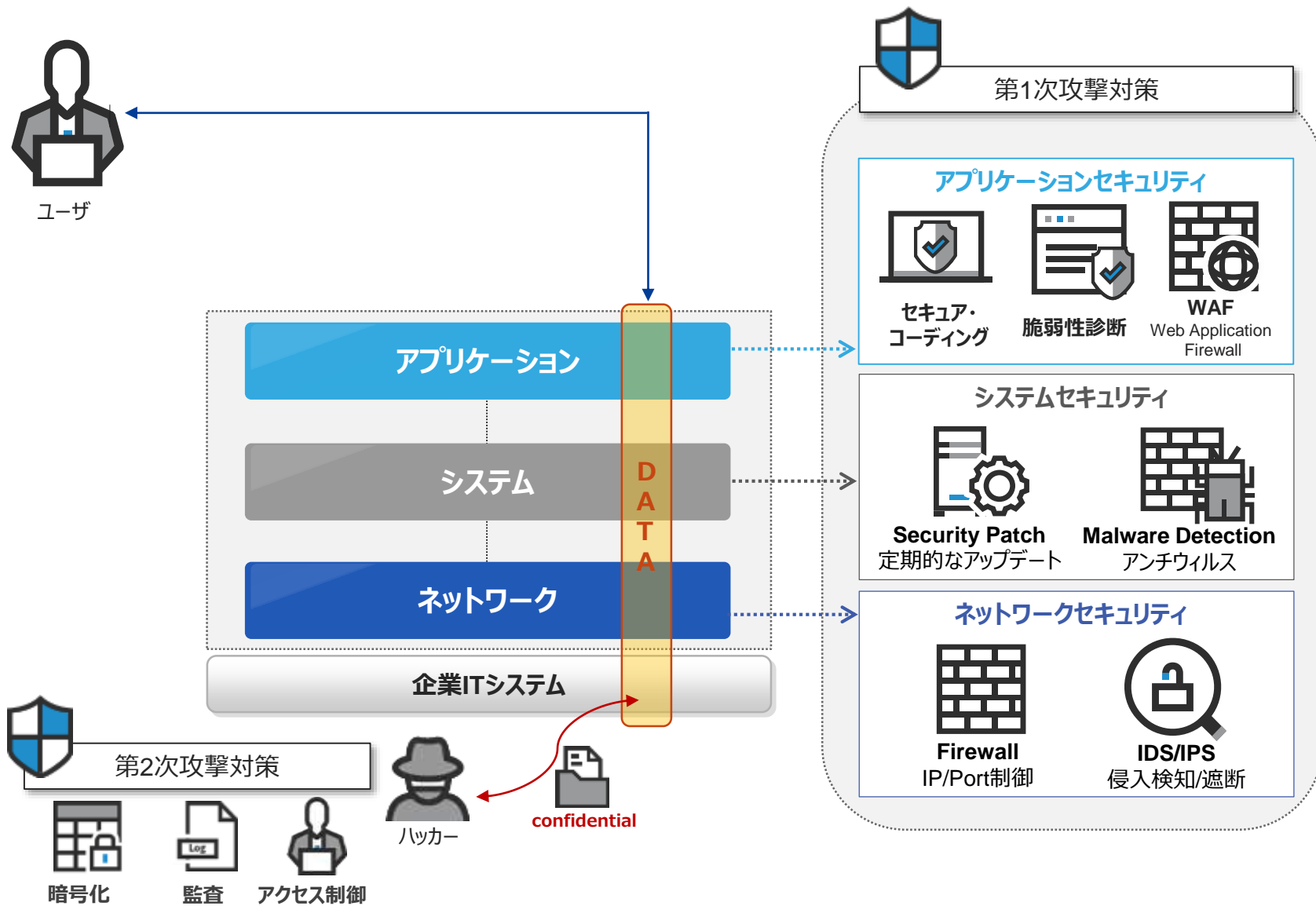
対策

「ビジネスを守る」のため、
守るべきデータは何であり、社内外のどこに存在し、どう扱われているのか

企業ITシステムへの脅威の分類



各脅威への対策および実情



Zero

Trust



米国OPMハッキング事件

Zero Trustの表舞台デビューの発端

概要

2015年4月に発生した、**米連邦人事管理局** (Office of Personnel Management : **OPM**) から連邦公務員および市民、**560万人分の指紋**情報を含む、**2,150万人分の個人情報**が漏洩した事件

詳細

- ディープ・パンダ(DEEP PANDA)とシェルクルー(Shell Crew)で知られるグループによる犯行
- 認証およびアクセスシステムの不備や古いバージョンのソフトウェア使用等**セキュリティ全般における不備**を指摘
- **暗号化対応ができていない、又はできない程古いシステム**の存在を確認
- **第3者によりUS-CERTへ通報し、US-CERTよりOPMへ情報漏洩について確認依頼**



OPM.GOV

2015年4月OPMハッキング事件について
同年6月、下院公聴会にて証言中の
キャサリン・アーチュレッタ長官

OPMハッキング事件

誰もを根拠なくして信じない

OPM ITセキュリティの責任者、ジェフ ワグナー(Jeff Wagner)

“

2014年第一次攻撃以降、第二次攻撃を準備していたとは想像すらしなかった。
第一次攻撃を受け、我々は、
システムをフォーマットし、リセットし、
そしてマルウェアと脆弱性を解消することで大忙しかった。

その時、第二次攻撃者は、
既に家に入っていた。

”

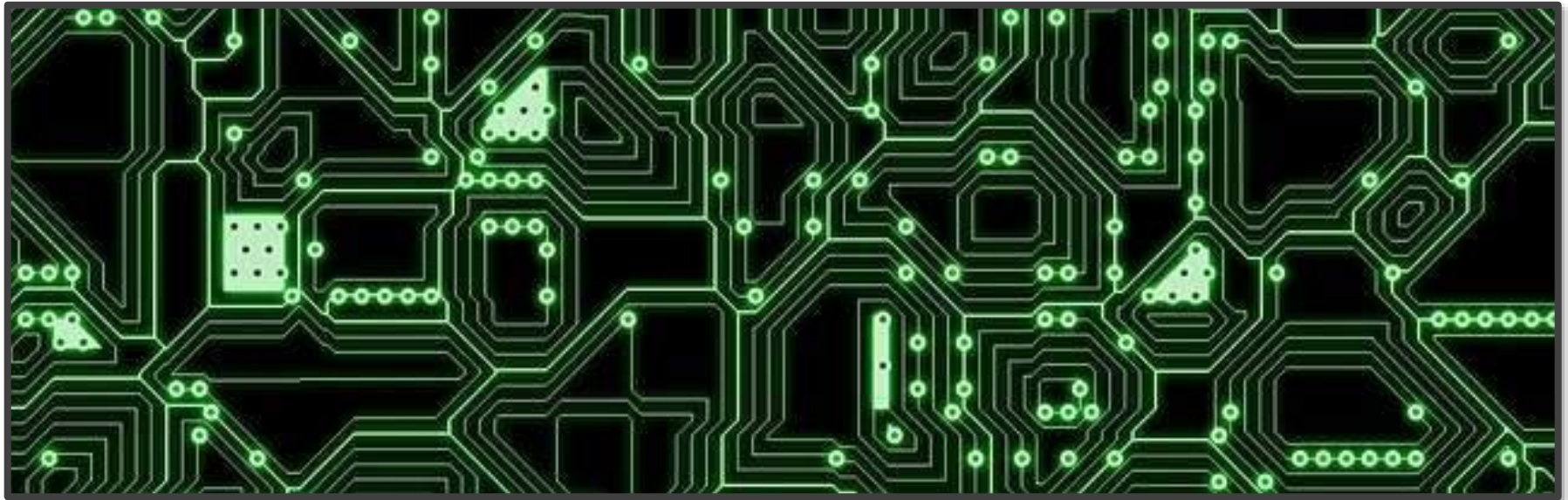
連邦政府機関のための提言およびレポート

Zero Trust

Inner Trust Model と Zero Trust Model

IT情報セキュリティモデルの比較

Zero Trust Modelの概念



Zero Trust Network、又はZero Trust Architectureで知られるZero Trust Modelは、2010年、米国の独立系リサーチ会社フォレスター・リサーチ(Forrester Research)の当時主席アナリストであった、ジョン・キンダーバグ(John Kindervag)により提言されたモデル

FORRESTER®

すべてを検証し、何も信頼しない

内部・外部すべて信頼できない前提で防御

データを中心としたネットワーク設計

Inner Trust Model

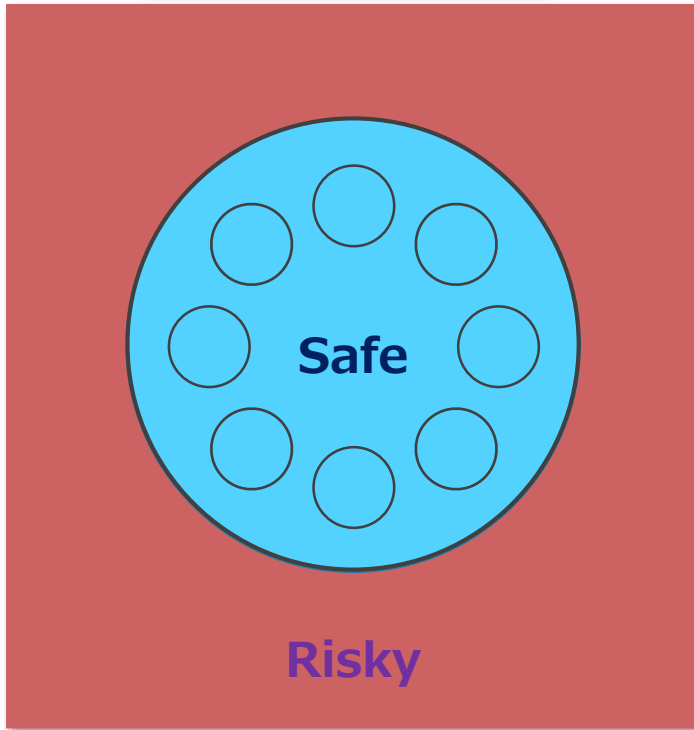
従来型セキュリティモデル
全ネットワークにおいて境界線
(Perimeter)を引き、内側へ
の侵入を防ぐための対策

Zero Trust Model

従来のInner Trust Modelの
概念をデータ個々に対し適用
Perimeterから
Micro-Perimeterへのシフト

Inner Trust Model と Zero Trust Model

Inner Trust Model



ネットワークの境界線(Perimeter)を基準に
外側にセキュリティを適用

内部への侵入を防御するモデル

システムの
前
侵入防止セキュリティがあることを
い

ネットワークとシステムを中心としたセキュリティ・ポリシー
内部侵入後データ漏洩対策等に不備

Zero Trust Model



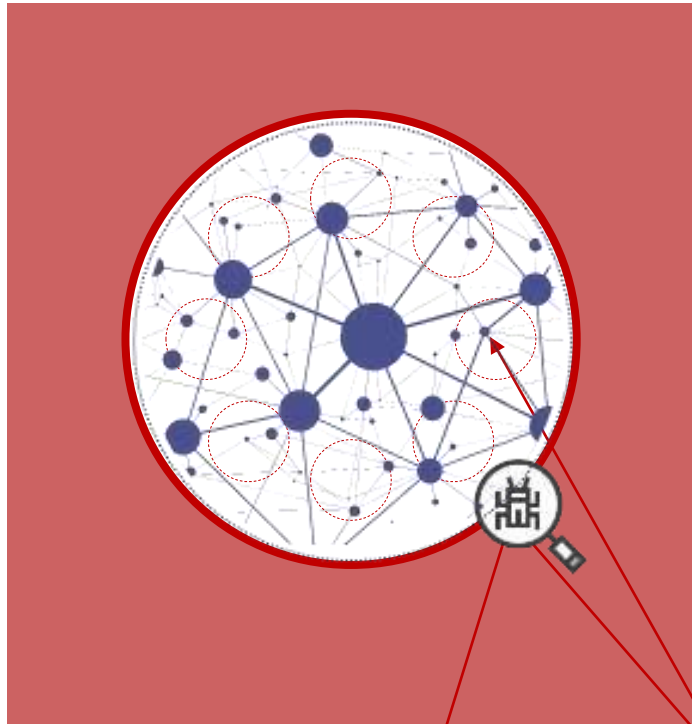
内部・外部すべて信頼できないを前提に防御

既存の境界線(Perimeter)の外側に

データ保護を
データ個々の境界線(Perimeter)に適用

Inner Trust Model と Zero Trust Model

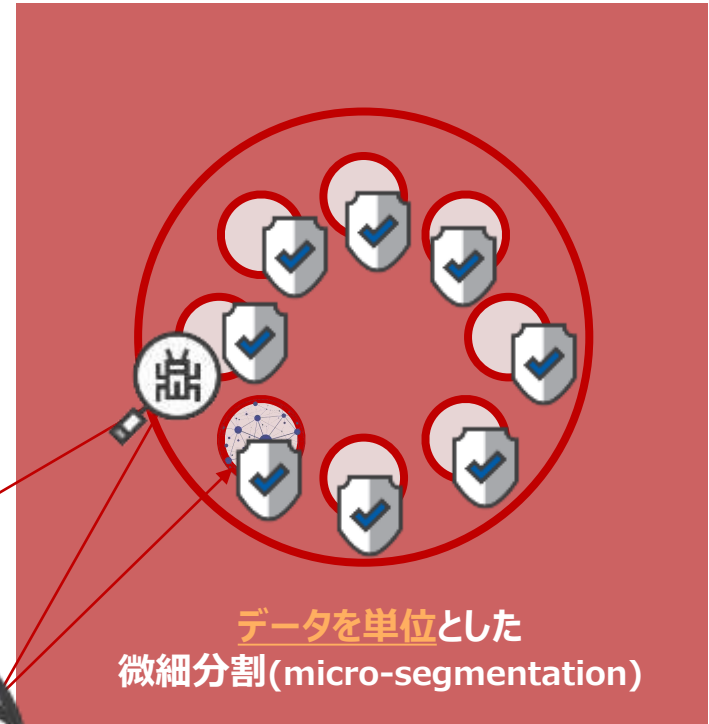
Inner Trust Model



一旦内部侵入後、**内部者としてデータ奪取**
内部者への権限過剰

境界線セキュリティ→失敗

Zero Trust Model



データを単位とした
微細分割(micro-segmentation)

粒子型境界線適用
(granular perimeter enforcement)

Inner Trust Modelで
ネットワークおよびシステムの境界線で適用した
セキュリティを微細分割の境界線に適用

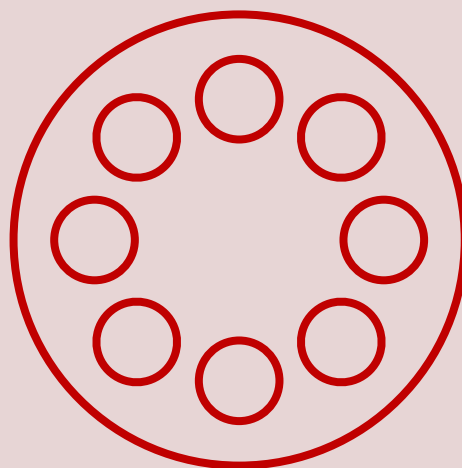
データ基準全領域防御



- ✓ Zero Trustを構成する技術概念
- ✓ Zero Trust実現のための5 Step
- ✓ Zero Trust概念が求められている環境としてのクラウドの適合性

Zero Trustを実現するには？

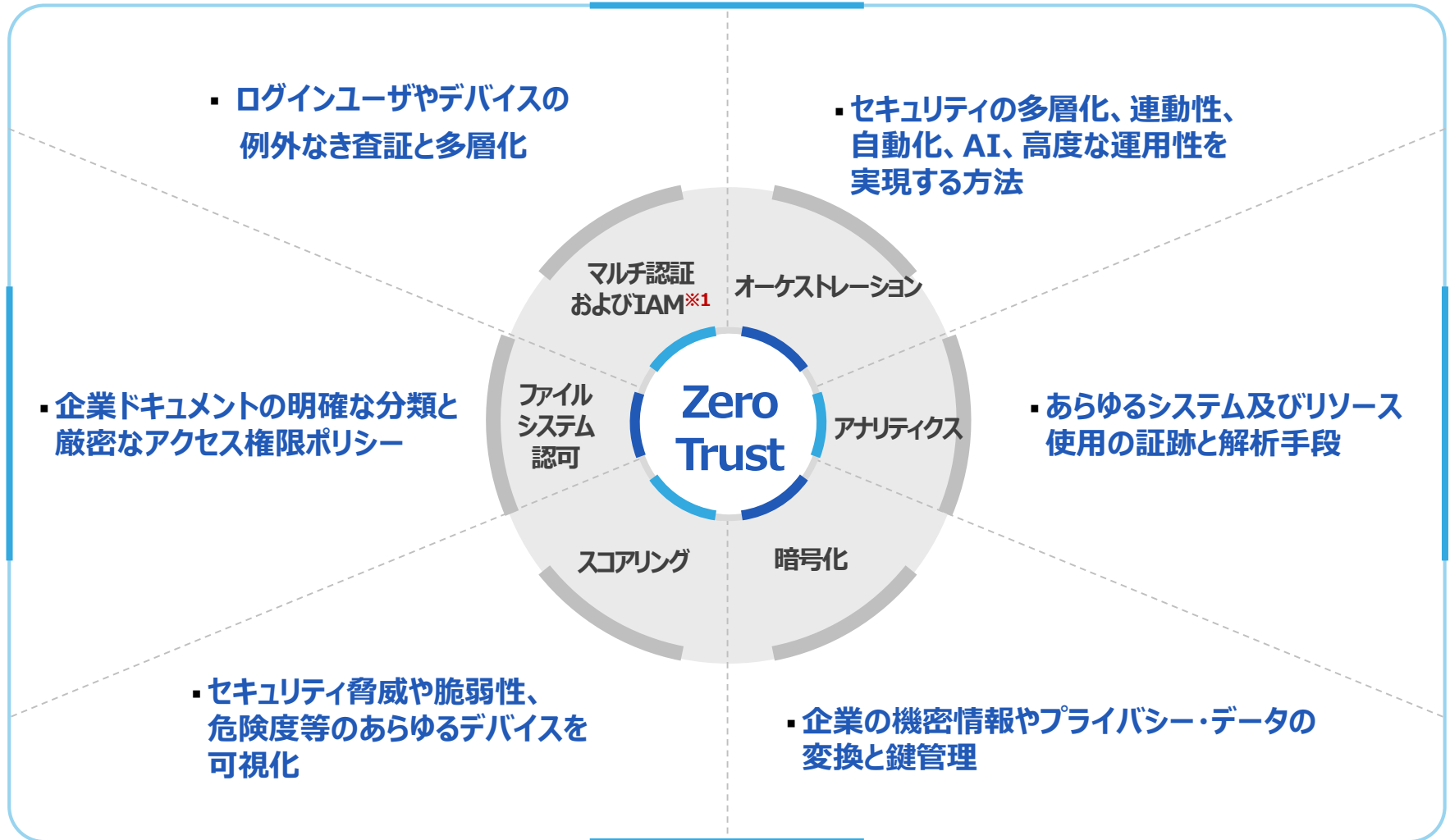
Zero Trust Modelの技術的基盤



企業IT環境を保護する目的

既存技術と管理プロセス等に依存

Zero Trust Modelの技術的基盤



※ 1 IAM : Identity and Access Management

Zero Trust Model実現のための5 STEP

5 STEP for Zero Trust Model

1. センサティブなデータの状況を把握

- **セキュリティの適用は、把握可能なデータのみ**
- 敵を知るより自らを知ることが先
- 把握後、ルール・ポリシーの整理も重要な作業である

- どこに格納されているのか？
- 頻繁にアクセスし利用する人は誰なのか？
- どのレベルのセンサティブさなのか？
- アウトソーシングのメンバーの内、頻繁にアクセスする人は誰なのか？

2. センサティブなデータのフローのマップを作成

- **データ・セキュリティは、格納データとフロー上データ両方を対象**
- **データ活用者と関係者を多く参照し詳細なマップを作成**
- 状況が把握できたデータに対し、どの時点で、どこから、どのように、どの経路で移動するのか、フローを把握し、マップのような形式で作成
- PCI-DSSの場合、必ずクレジットカードのデータ・フローのマップを作成

3. ネットワーク・トポロジーを設計

- Zero Trustのネットワーク・トポロジーは、全体のネットワークを貫通する取引のフローと利用者およびアプリケーションのアクセス方法により異なる

データを中心に、どのように、誰と共有、利用されたのかを考慮

企業の最も適したネットワーク・トポロジーとデータの外側の境界線(Micro-Perimeter)をどこで設定するか、どのような物理的・仮想的装置で分離、又は連携するかを決定

4. 自動化されたルール・ベースを作成

- 1～3のSTEPにて理想的なデータ・フローを把握済み
- 「必要な時のみ」データへのアクセス許可のためのルール
- **アクセス制御および管理・監視のルールとポリシーをデータの外側の境界線(Micro-Perimeter)に適用**
- ソースIP、受信元IP、ポート番号、プロトコルのみならず、ユーザのアプリケーションおよびユーザ認証についても理解は必須

5. 持続的に全環境を監査

- Zero Trustのコアは、**すべてのトラフィックを記録し監査すること**
- **今のステータスがベストだと信じない**

“
Zero Trustは、単純な技術ではなく、
プロセスであると同時に
企業が持たなければならないマインドセットである。
クラウドは、白いキャンバス紙のような空間であり、
クラウド環境へのシステム移行が活発である今こそ、
Zero Trustを始めるには完璧である
”

インフラストラクチャーの変革であるクラウド時代

既存のInner Trust Modelの考え方から
データを中心とした*Zero Trust Model*へ、マインドセットをシフト

Zero

Trust

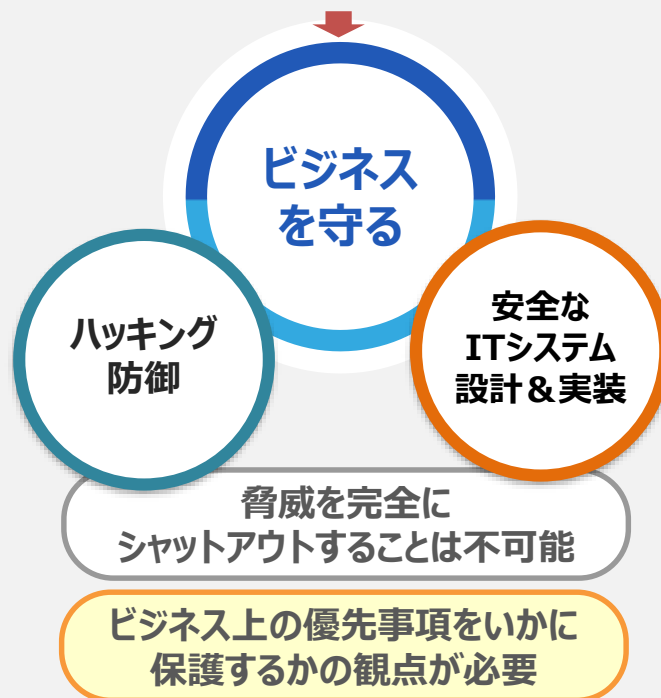
まとめ

「ビジネスを守る」



サイバー攻撃の高度化・巧妙化

従来型の予防策だけでは脅威から
ビジネスを守ることができない





アカウントビリティ

説明責任

tip



Why not Security? **ビジネスを守るための投資**

セキュリティ投資

Security Investment

- セキュリティは「コスト」として認識せずに、
ビジネスを守る事業継続性につながる「投資」として認識
- 「セキュリティへの投資」は、
企業イメージ向上および**お客様信頼**につながると認識



PentaSECURITY
enterprise · iot · blockchain

KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp



TU-Automotive Awards
Best Auto Cybersecurity
Product/Service 2019



Cybersecurity
Excellence Awards
Winner 2018



Hot Company in
Web Application
Security for 2016



SC Magazine Europe
Best SME Solution



Asian Cyber
Security Vendor
of the Year

Gartner

Recognized on the
Gartner WAF
Magic Quadrant



No.1 WAF
Vendor in the
APAC Region



ICSA Labs
Certified WAF



The First and Only
CCEAL4 Certified
WAF



PCI-DSS
Compliance