



# 新たな攻撃に対する検知や防御に関する最新情報 「ビジネスを守る」企業ITセキュリティの在り方

攻撃者プロファイリングと今求められる投資

2018.02.16

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. 会社紹介

- 会社概要
- 開発およびビジネス沿革
- グローバルビジネス展開

## II. 攻撃者グループのプロファイリング

- 攻撃者プロファイリング
- 悪意あるコートのプロファイリング・プロセス
- Rifle CAMPAIGNタイムライン
- TTPプロファイリング
- ラザルス (Lazarus)
- ブルーノロフ (Bluenoroff)
- アンダリエル (Andariel)
- ラザルス・ブルーノロフ・アンダリエルの比較

## 目次

### III. 企業ITセキュリティ実態

- 99と172
- サイバー攻撃のライフサイクル

### IV. 時代別セキュリティニーズの変移

- 時代別セキュリティ・ニーズ
- IT技術発展による情報セキュリティの中心移動

### V. 企業ITセキュリティの考え方「ビジネスを守る」

- 「ビジネスを守る」の考え方
- これからの企業情報セキュリティに求められる6つの基本原則
- 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

### VI. まとめ

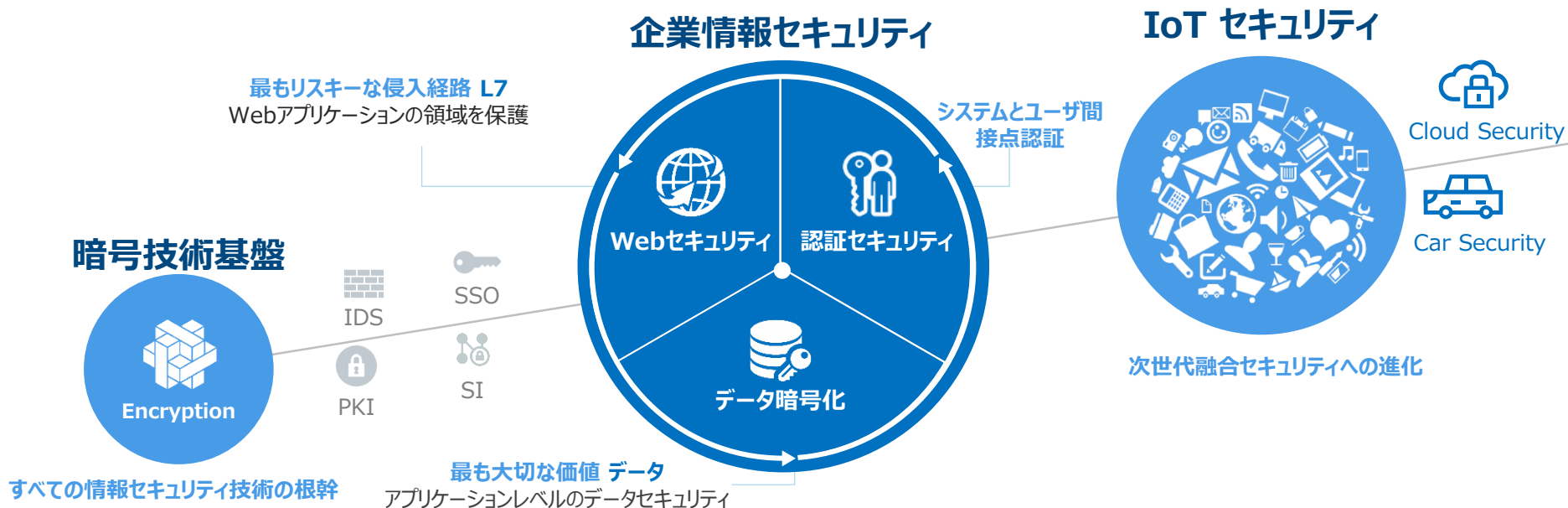
- 3年9ヶ月間の最大93,014名の会員情報の流出
- 安全なインターネットの基準、WAF
- ビジネスを守るための投資

# 会社紹介

# 会社概要 暗号化技術基盤の企業情報セキュリティの専門会社

**Penta** SECURITY は、企業情報セキュリティの専門会社です。

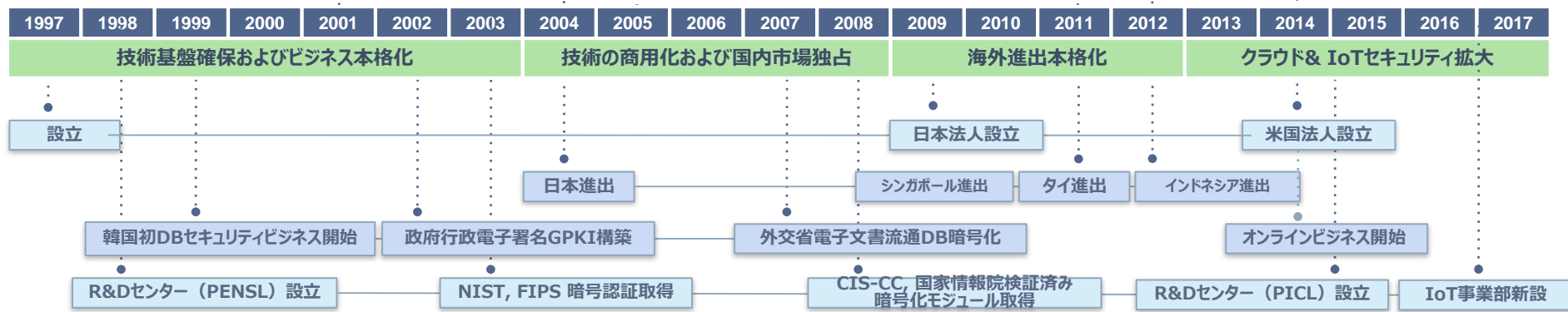
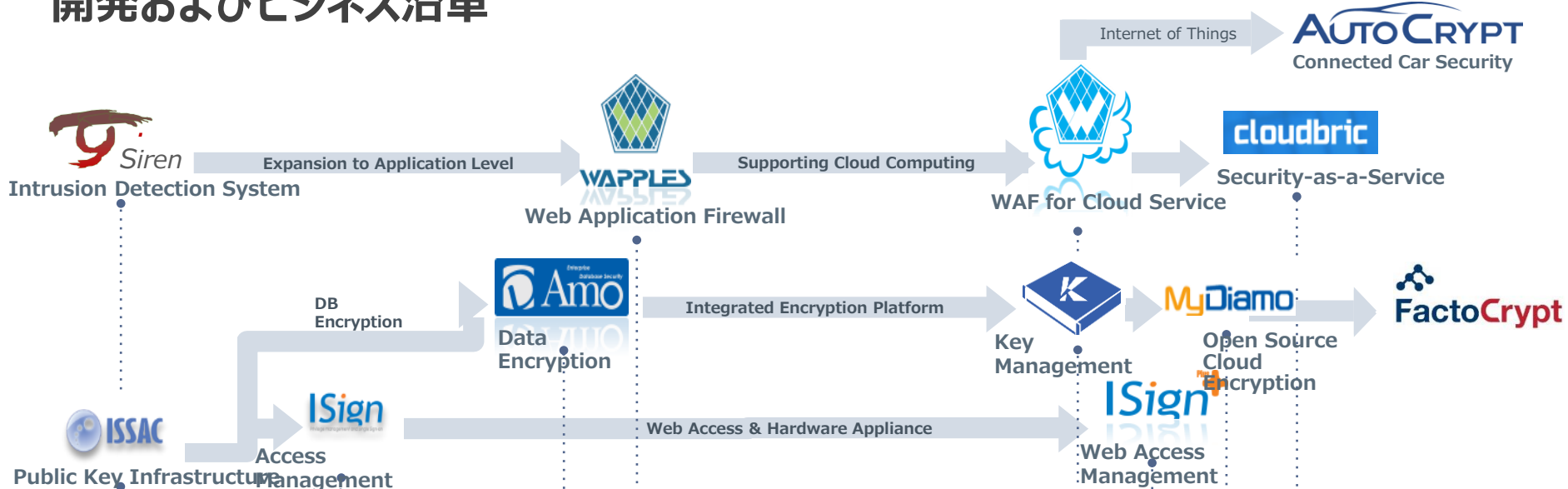
暗号化コア技術基盤に企業情報セキュリティの3つのポイントを実現し、次世代融合セキュリティへ



## Company Overview

<b>Founded</b>	1997年 7月	<b>Business Area</b>	データ暗号化/Webセキュリティ/認証セキュリティの企業情報セキュリティ
<b>CEO/Founder</b>	李 錫雨 (リ ソグ)	<b>Client</b>	政府、官公庁、文教、一般企業、金融等3,500カスタマー
<b>Staff</b>	250人+ ※ 研究・開発および技術部門150人+(2018/01)	<b>Products</b>	データ暗号化プラットフォーム <b>D'Amo</b> Webセキュリティソリューション <b>WAPPLES</b> セキュリティ認証管理ソリューション <b>ISign+</b> 自動車セキュリティ、IOTセキュリティ等次世代セキュリティ事業
<b>Located</b>	韓国ソウル		
<b>Overseas Branch</b>	日本法人 (東京) / 米国法人 (ヒューストン)		
<b>Overseas Network</b>	シンガポール、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		

# 開発およびビジネス沿革



**PENSL** Penta Security Technology Lab  
Asia Pacific No.1 Era Security

**PICL** Penta IoT Convergence Lab  
New Era IoT Security

ロセキュリティR&Dセンター

DEP  
Amo  
MyDiamo

WAF  
WAPPLES  
cloudbric

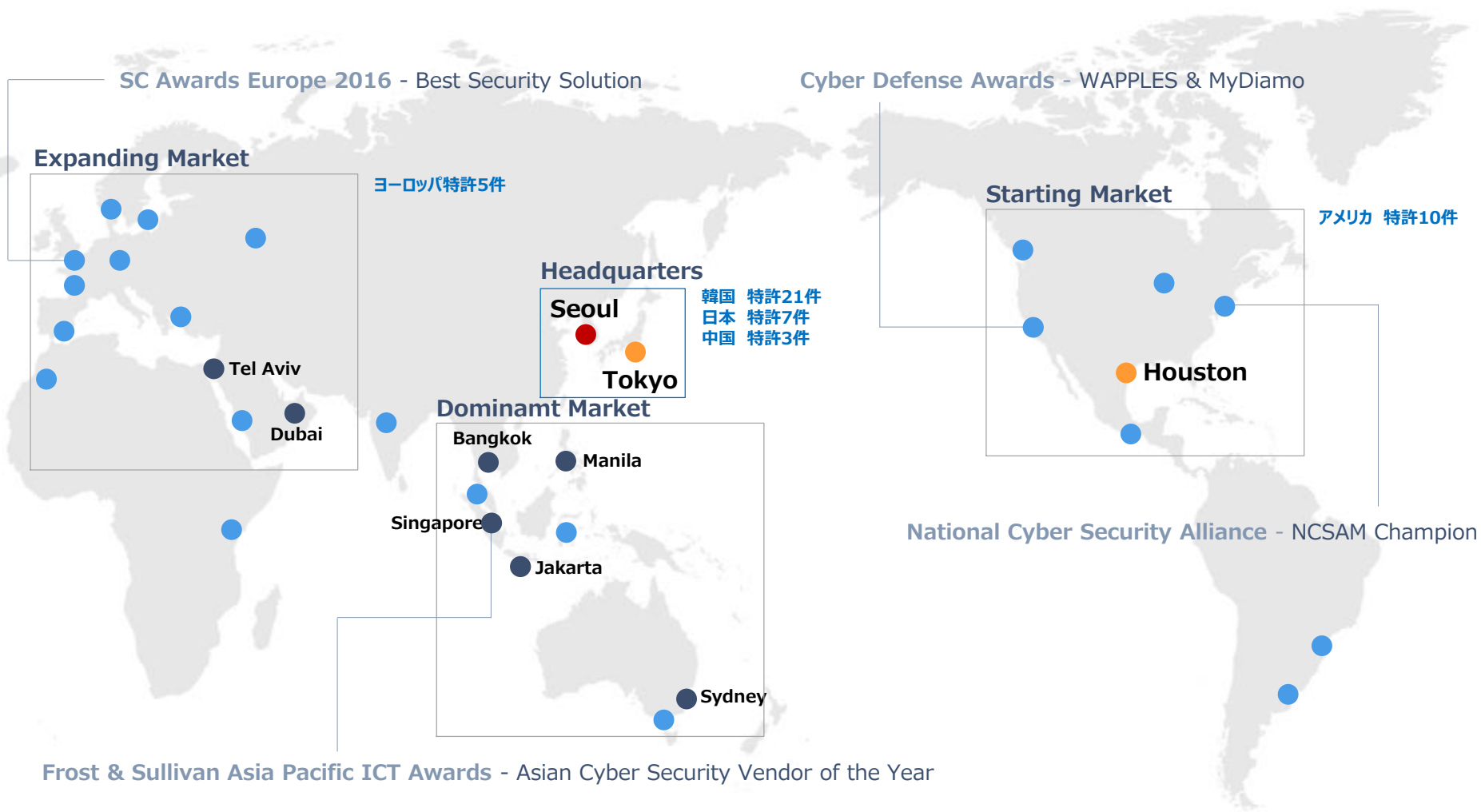
WAM  
ISign+

IoT  
自動車セキュリティ  
クラウド・セキュリティ・サービス  
セキュリティ・ウェブ・ゲートウェイ

自動車セキュリティ  
スマートシティ・セキュリティ・インフラ事業  
スマートファクトリー・プラント・セキュリティ事業

正品認証ソリューション

# グローバルビジネス展開 日本およびアメリカの現地法人、そしてグローバル・パートナーのネットワーク



- Headquarters
- Branch Office
- Sales & Services
- Government & Main Customers

# 攻撃者グループのプロファイリング

*TTP (Tactics, Techniques and Procedures) の分析*



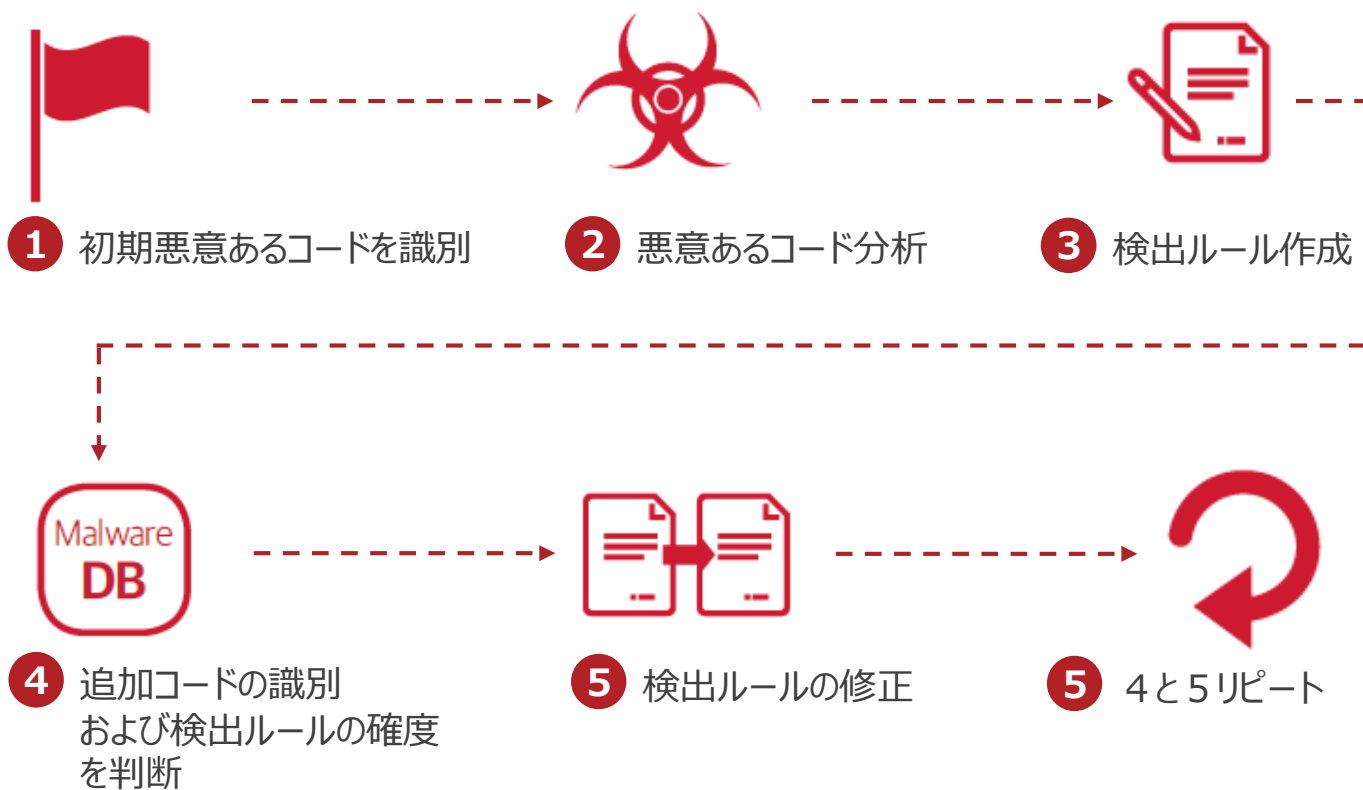


## 0. 攻撃者プロファイリング

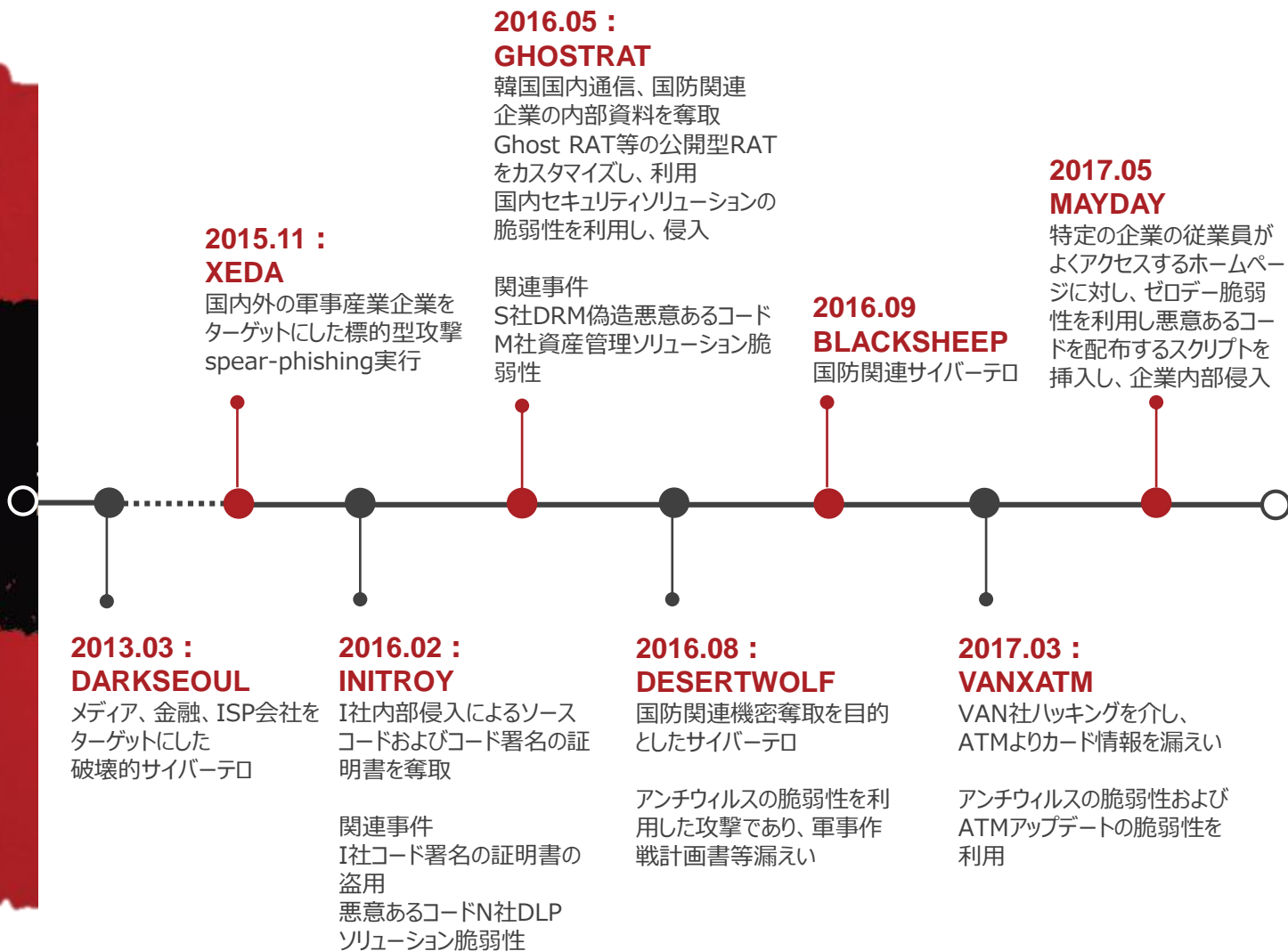
ハッキング事故および悪意あるコードを分析し、攻撃者を追跡することは、非常に難しく、特に近年のサイバー空間上組織的に行われるテロの場合、その根底に潜む攻撃者を探し出すことは言うまでもありません。そのため、多くの専門家らはインシデント全般にわたるTTP (Tactics, Techniques and Procedures) を分析し、攻撃者 (グループ) をプロファイリングします。

プロファイリングの結果は、**新たに発生するハッキング事故および悪意あるコードを分析する際に、攻撃予想シナリオおよび隠ぺい手法の把握に役に立ち、さらに攻撃ターゲットを予想でき、事前に体制を整え被害を最小限に抑えるかたちで対応可能に致します。**

# 悪意あるコードのプロファイリング・プロセス



# Rifle CAMPAIGNタイムライン



# TTPプロファイリング



## 戦略 (Tactics)

金融、IT企業、大手企業、軍事産業企業、国防等  
攻撃のターゲットは幅広いが、「国防」や「金融」の  
ような社会基盤施設を最終目標にする

- ターゲットのITインフラ環境および内部人事状況まで把握する徹底した下調べ
- 内部侵入後、継続的に悪意あるコードを送り込み、内部従業員PCおよびサーバに対し、追加攻撃を決行
- 内部情報の収集および分析後、最終的に機密情報の漏えいおよびシステム破壊

## 技術 (Techniques)

攻撃ターゲットへの侵入および侵入後内部拡散の  
ため、ゼロデー脆弱性を利用、Agent型で多数PC  
にインストールされるSWの脆弱性を利用

- 侵入後、拠点確保以降は、内部から外部へ設定したリバーストンネリングを介し、内部攻撃
- 拠点には攻撃者が開発したRATやバックドアをインストール
- Windows環境では攻撃のためのアカウント (SQLAdmin等) を追加し、RDP (Remote Desktop Protocol) 接続を利用
- WebShell等を利用し、C&Cサーバ確保

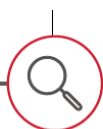
## 手順 (Procedures)

典型的なAPT攻撃を行い、内部侵入後、内部情報を収集し、選別し情報奪取  
MBR(Master Boot Record)破壊型悪意あるコードをテスト

### 1. 事前情報収集



### 3. 内部情報収集



### 5. システム破壊



### 2. 内部侵入



### 4. 機密データ漏えい





# 1. ラザルス (Lazarus)

- ・グローバル・セキュリティ業界により命名された代表的な危険グループ
- ・特定の国（北朝鮮と推測）が背景に存在するとみられ、技術力および組織力を持つ

## 推測される攻撃事例

2009年7月7日 DDos攻撃	2011年3月4日 DDos攻撃
2011年3月 金融機関内部システム破壊	2011年3月 複数のメディア内部システム破壊
2013年3月20日 DARK SEOULテロ	2014年11月 米国Sony Pictures攻撃

- ・韓国および米国FBI捜査結果、北朝鮮のサイバー攻撃組織による攻撃にみなされ、2016年Novettaにより発表されたOperation BlockbusterレポートにてTTPプロファイリング結果、一連の攻撃が同一攻撃者によるインシデントとして分析

2017年全世界的に影響を与えた、WannaCryランサムウェアの背景である疑い



# 1. ラザルス (Lazarus)

グループの攻撃パターンに変化有



悪意あるコードのプロファイリングの結果

攻撃ターゲットの選択基準

ラザルスと  
関連のある  
複数のグループにわけ、追跡

主に金融機関を攻撃ターゲットにする  
ブルーノロフ (Bluenoroff)

特に韓国国内でRIFLE文字列を利用する  
アンダリエル (Andariel)



## 2. ブルーノロフ (Bluenoroff)

### 推測される攻撃事例

2016年2月 ハンガリー 中央銀行のSWIFT不正取引事故

ポーランド金融監督院ホームページを介したWatering Hole攻撃

- ・グローバル金融機関を攻撃ターゲットとし、活動
- ・FireEye、Symantec、kaspersky、British Aerospace Systems等から背景にラザルスを指摘 → 2017年4月kasperskyによりラザルスと関連性を持つ新たなグループとして「ブルーノロフ」と命名し、Group-IBにより北朝鮮との関連性を公開

2017年1月金融機関の網分離ソリューションの脆弱性を利用し、内部網PCに悪意あるコードを挿入、以降WebDAV脆弱性 (CVE-2017-7269) を利用した、社内サーバへの攻撃事例が増加



### 3. アンダリエル (Andariel)

- ・ラザルスによる攻撃と推測される「2013年3月20日 DARK SEOULテロ」時の悪意あるコードの類似性を持ちながら、新種コードを作成し、2016年からグローバル金融機関および韓国国内金融機関の網分離ソリューションの脆弱性を突いた攻撃を実行しているブルーノフの攻撃パターンおよび方式に相違点がある



2014年を前後に、ラザルス組織がTTP（攻撃方式）の異なる2つのグループに分けられ、同時期に異なるターゲットに対し、攻撃を実行することから、「アンダリエル」と命名

- ・アンダリエルとブルーノフの根底には、ラザルスが存在するが、攻撃ターゲットおよび目的において差異があり、アンダリエルの場合、特に韓国に特化した攻撃手法を用いて、韓国企業および政府をターゲットにする



# ラザルス・ブルーノフ・アンドリエルの比較

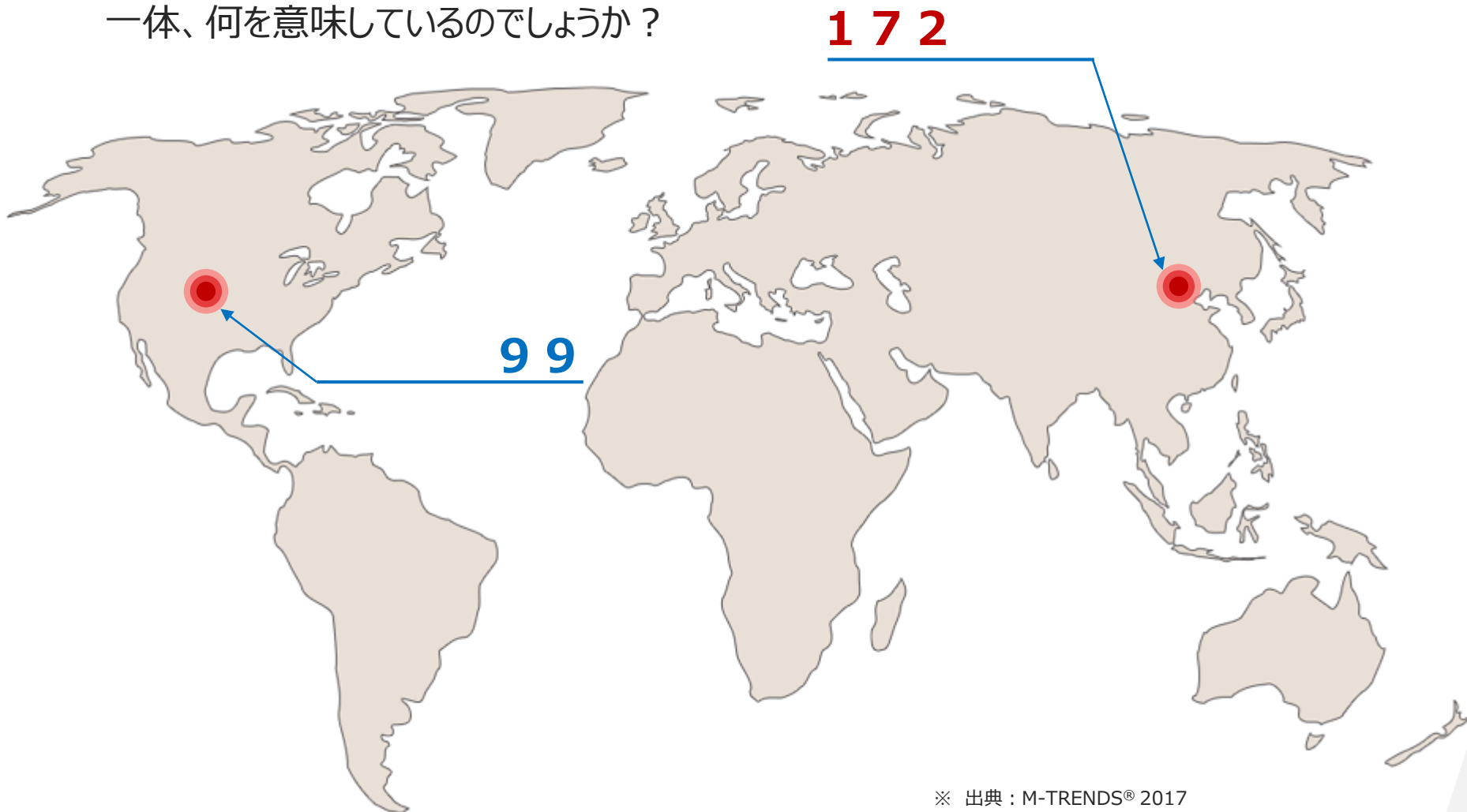


危険グループ	ラザルス	ブルーノフ	アンドリエル
攻撃ターゲット	政府、金融、メディア等	グローバル金融機関	韓国金融機関 韓国中小IT企業および大手企業 国防省、軍事産業企業
攻撃目的	社会的混乱	経済的利益 (SWIFT、ビットコイン等)	機密情報の奪取 経済的利益
主な活動時期	～最近	2015～	2014～
主な事故	(韓国) 7.7 DDos攻撃 (韓国) 3.4 DDos攻撃 (韓国) 3.20 サイバーテロ (米国) Sony Pictures攻撃 WannaCryランサムウェア	(バングラデシュ) 中央銀行 SWIFT不正取引事件 (ポーランド) 金融監督院 ホームページ改ざんおよび Watering Hole攻撃 (韓国) 網分離脆弱性攻撃	大手企業のデータ漏えい 国防省ネット侵入 VANおよびATMに悪意 あるコードの挿入

# 企業ITセキュリティ実態

## 99と172 (1/2)

... **9 9**と**1 7 2**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 (2/2)

… 企業側でハッキングの攻撃を**認知する**までかかる時間

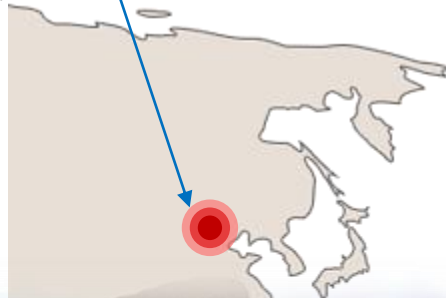
**172日**

アジア・パシフィック



**99日**

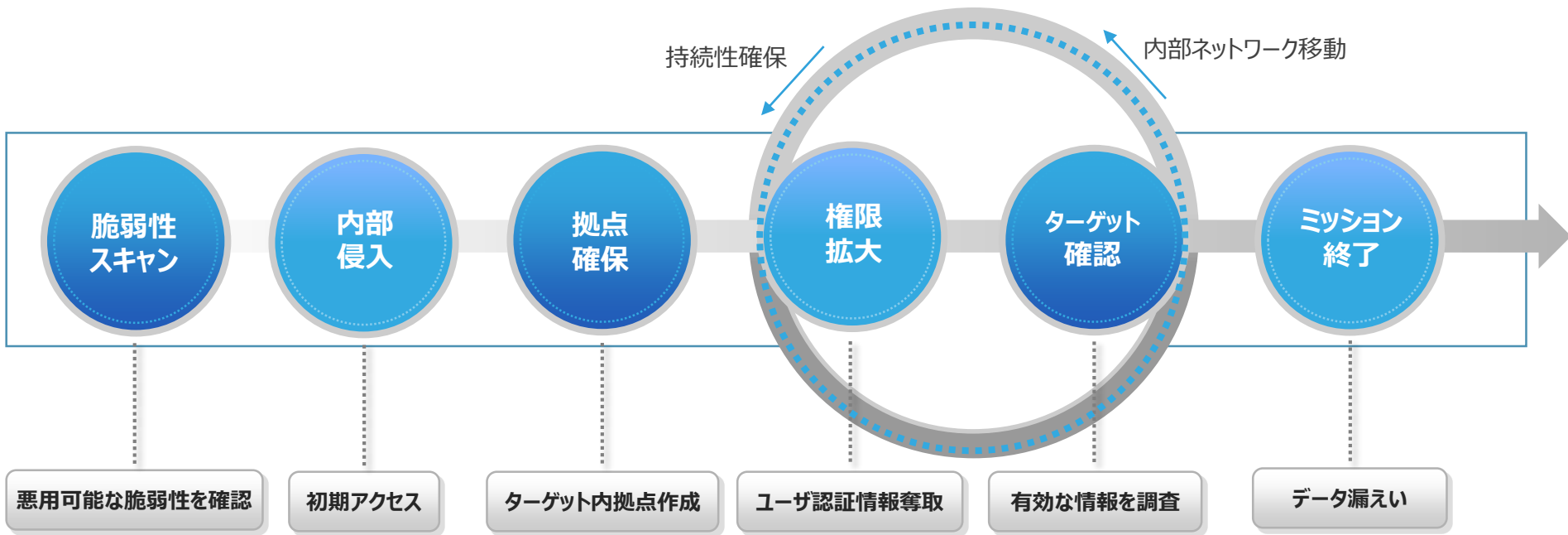
世界平均・アメリカ



※ 出典：M-TRENDS® 2017

# サイバー攻撃のライフサイクル

## Cyber Attack Lifecycle

















172日
















# 時代別セキュリティニーズの変移

# 時代別セキュリティ・ニーズ (1/3)













	1980s	1990s	2000s	+2010s
era	<p><b>PC</b></p> 	<p><b>Intranet</b></p> 	<p><b>WebBiz</b></p> 	<p><b>Cloud + IoT</b></p> 
threat	<p> virus</p> <p><b>infecting</b></p> <p>Personal Computer</p> <p></p>	<p> hacker</p> <p><b>intruding</b></p> <p>Server System</p> <p></p>	<p>    malware bots spam unknown</p> <p><b>stealing</b></p> <p>Web Data</p> <p></p>	<p></p>
recipe	<p><b>Anti Virus</b></p> <p>vaccine</p>	<p><b>Intrusion Prevention</b></p> <p>firewall IDS/IPS</p>	<p><b>Website Protection</b></p> <p>WAF</p>	

# 時代別セキュリティ・ニーズ (2/3)

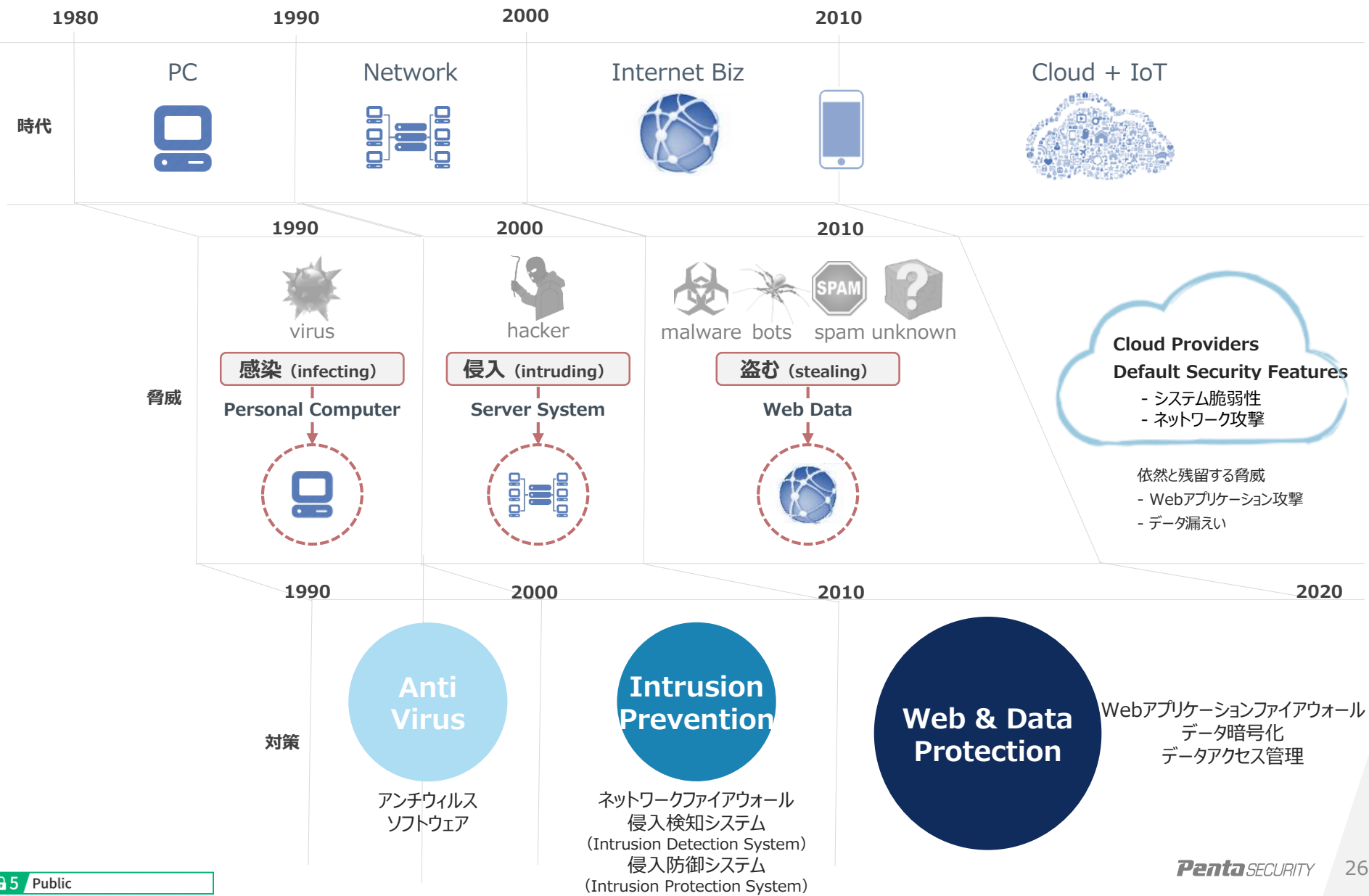
	1980s	1990s	2000s	+2010s
era	<p><b>PC</b></p> 	<p><b>Intranet</b></p> 	<p><b>WebBiz</b></p> 	<p><b>Cloud + IoT</b></p> 
threat	<p> virus</p> <p><b>infecting</b></p> <p>Personal Computer</p> 	<p> hacker</p> <p><b>intruding</b></p> <p>Server System</p> 	<p>    malware bots spam unknown</p> <p><b>stealing</b></p> <p>Web Data</p> 	<p>Cloud Service Security</p> <ul style="list-style-type: none"> <li>Anti Virus <input checked="" type="checkbox"/></li> <li>Intrusion Prevention <input checked="" type="checkbox"/></li> <li>Website Protection <input checked="" type="checkbox"/></li> </ul>
recipe	<p><b>Anti Virus</b></p> <p>vaccine</p>	<p><b>Intrusion Prevention</b></p> <p>firewall IDS/IPS</p>	<p><b>Website Protection</b></p> <p>WAF</p>	



# 時代別セキュリティ・ニーズ (3/3)

	1980s	1990s	2000s	+2010s
era	<p><b>PC</b></p> 	<p><b>Intranet</b></p> 	<p><b>WebBiz</b></p> 	<p><b>Cloud + IoT</b></p> 
threat	<p>virus</p>  <p><b>infecting</b></p> <p>Personal Computer</p> 	<p>hacker</p>  <p><b>intruding</b></p> <p>Server System</p> 	<p>malware bots spam unknown</p>  <p><b>stealing</b></p> <p>Web Data</p> 	<p>Cloud Service Security</p> 
recipe	<p><b>Anti Virus</b></p> <p>vaccine</p>	<p><b>Intrusion Prevention</b></p> <p>firewall IDS/IPS</p>	<p><b>Website Protection</b></p> <p>WAF</p>	<p><b>Data Encryption</b></p> 

# IT技術発展による情報セキュリティの中心移動



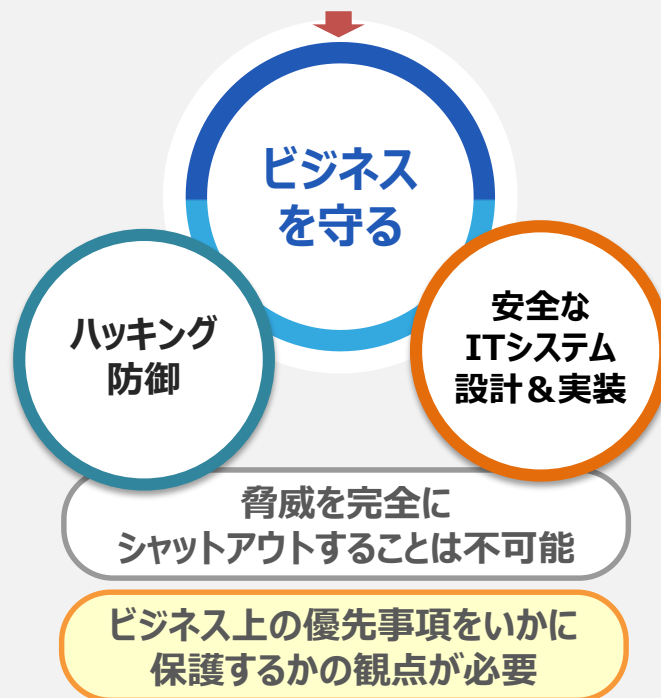
# 企業ITセキュリティの考え方 「ビジネスを守る」

# 「ビジネスを守る」の考え方



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



# これからの企業情報セキュリティに求められる6つの基本原則



Source: <https://www.flickr.com/photos/saxamnovelty/288741595/>

サイバー攻撃  
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

ビジネス  
を守る

## レジリエンス (Resilience)

- 新たな脅威に対抗するための「**抵抗力**」・「**復元力**」
- 被害の予防のみならず、被害発生を前提に「**検知**・**復旧の速度**」に重きをおく考え方

## レジリエンス 6つの基本原則

### 1. リスクベース思考

- 法律やISO等規格によるチェックリストは実効性に乏しい
- ビジネスに影響を及ぼす可能性のあるリスクを洗い出し対応および投資の優先順位を確定

### 2. ビジネスを守る

- インフラを守るのではなく、ビジネスを守るへ認識
- セキュリティと利便性のバランスを考慮

### 3. ファシリテーター

- ビジネス部門とのコミュニケーションを取り持つファシリテーターとして、ビジネス上メリットを考慮した上で判断

### 4. 情報フローを理解

- 情報を制御するのではなく、そのフローの仕組みを理解し、適切な対応を行う

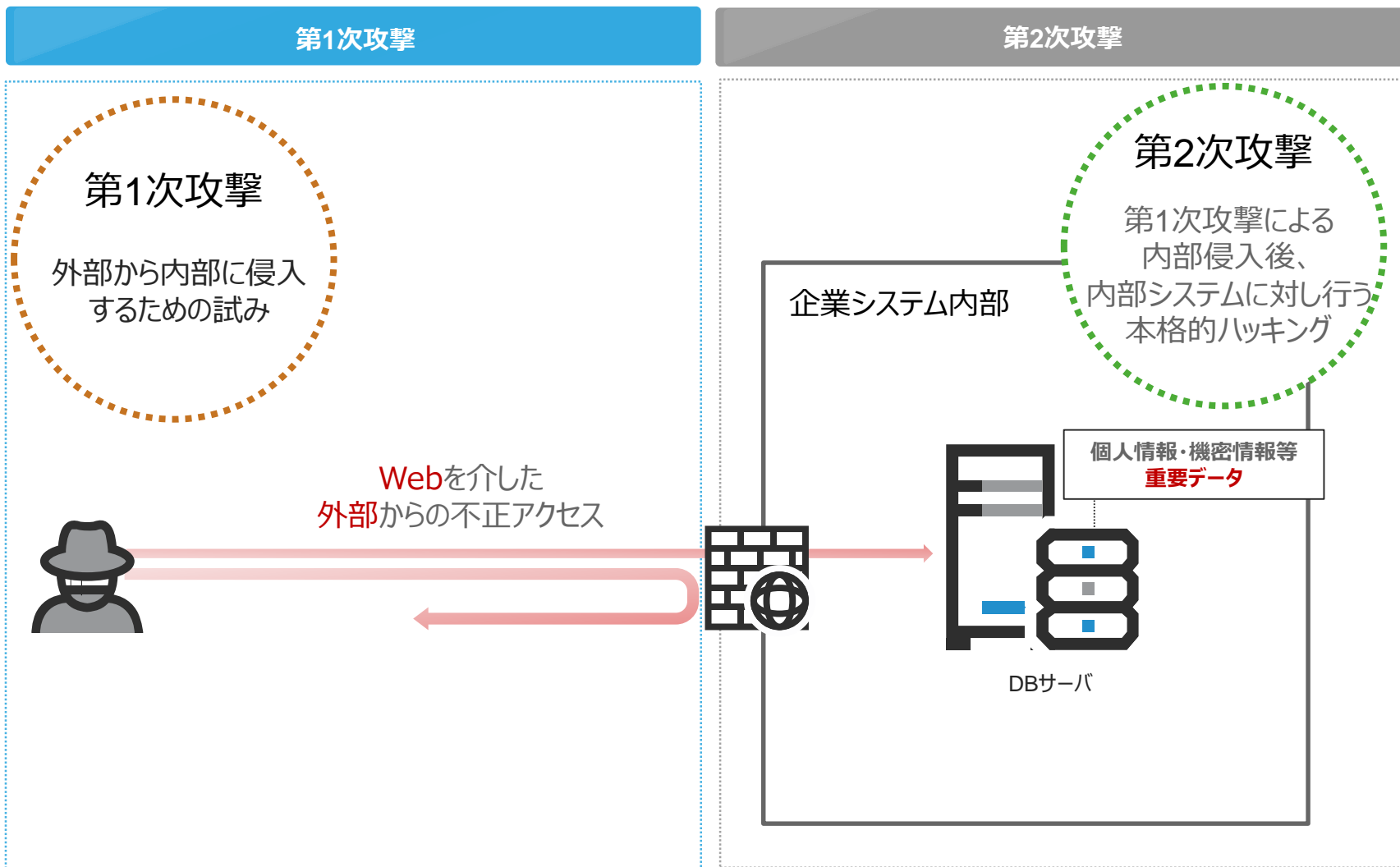
### 5. 技術限界を理解

- セキュリティ技術の限界を認めた上で、過信せずに運用・対応を行う

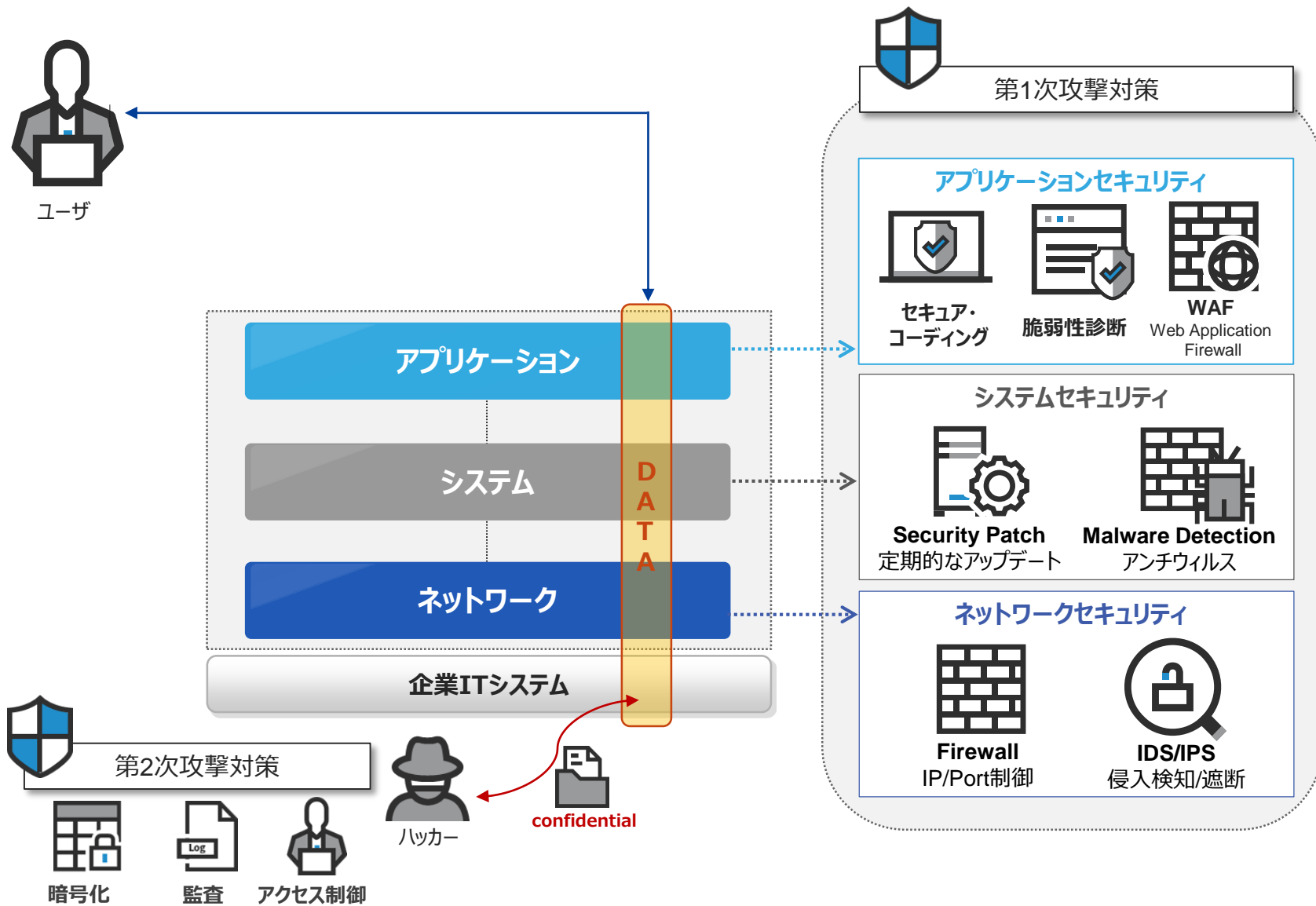
### 6. 被害は避けられない

- セキュリティ被害を完全に防ぐことは不可能であり、経営者も理解すべき
- 予防策+被害の迅速な検知・対応の体制確立

# 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



# まとめ



# 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」。サイトに脆弱性があり、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。



※ 出典： [http://itpro.nikkeibp.co.jp/atcl/news/17/011502952/?itp\\_leaf\\_cxpc&rt=nocnt](http://itpro.nikkeibp.co.jp/atcl/news/17/011502952/?itp_leaf_cxpc&rt=nocnt)

## 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

※ 出典： <http://www.gentosha.co.jp/news/n446.html>

# 安全なインターネットの基準、WAF



## OTA(Online Trust Alliance)

国際的非営利NGO団体 / オンライン信頼度評価機関  
毎年有名なWebサイトを対象に対し、セキュリティをチェック、  
安全なインターネット文化をリードしたWebサイトを選定

## OTHR (Online Trust Honor Roll) : オンライン信頼度優秀



## OTHR (Online Trust Honor Roll)

**選定対象** ■政府・メディア・金融・SNS等様々な分野の1,000サイト

**選定基準** ■2015年から**WAF使用有無**を重要な加点に指定

Webセキュリティ全般における最も重要な機能を提供するため、  
Webサイトの安全性に影響が大  
OTAは、今後のOTHR選定時WAF使用有無で加点をあたえる方針

企業戦略

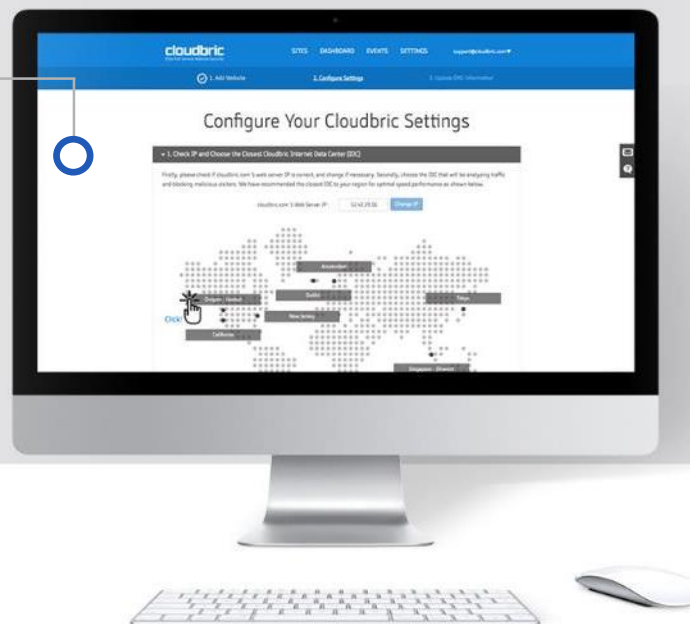
日本国内

海外戦略

# 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



## ■ お問い合わせ



### お電話でのお問い合わせ

03 - 5361 - 8201 (平日 10 : 00 ~ 18 : 00)

### メールでのお問い合わせ

[japan@pentasecurity.com](mailto:japan@pentasecurity.com)

### Webからのお問い合わせ

[www.cloudbric.jp](http://www.cloudbric.jp)



t h a n k   y o u

**Penta**SECURITY

**KOREA** Yeouido, Seoul [www.pentasecurity.co.kr](http://www.pentasecurity.co.kr) (HQ)  
**U.S.A.** Houston, Texas [www.pentasecurity.com](http://www.pentasecurity.com)  
**JAPAN** Shinjuku-Ku, Tokyo [www.pentasecurity.co.jp](http://www.pentasecurity.co.jp)