

サイバーセキュリティの新たなアプローチ

未知なる脅威、潜在的な危機を未然に防ぐには？

株式会社サムライズ
マーケティンググループ
ビジネスデベロップメントユニット
藤井義隆

サムライズのご紹介

2006年創業



サイバーセキュリティの新たなアプローチ

何が危険なのか？

従来のセキュリティのアプローチ

危険と判断されたものを排除する！

危険と判断できないものは察知できない！

察知するために更新され続ける必要がある

**検知するためのルールやシグニチャを
常に完全な状態にすることは難しい**

新たなアプローチとは？

危険と判断された **もの/事象** を検知しようとするのではなく、

それら が起こす **怪しい兆候を検知** する。

怪しい兆候とは・・・？

URL
IPアドレス

時間帯

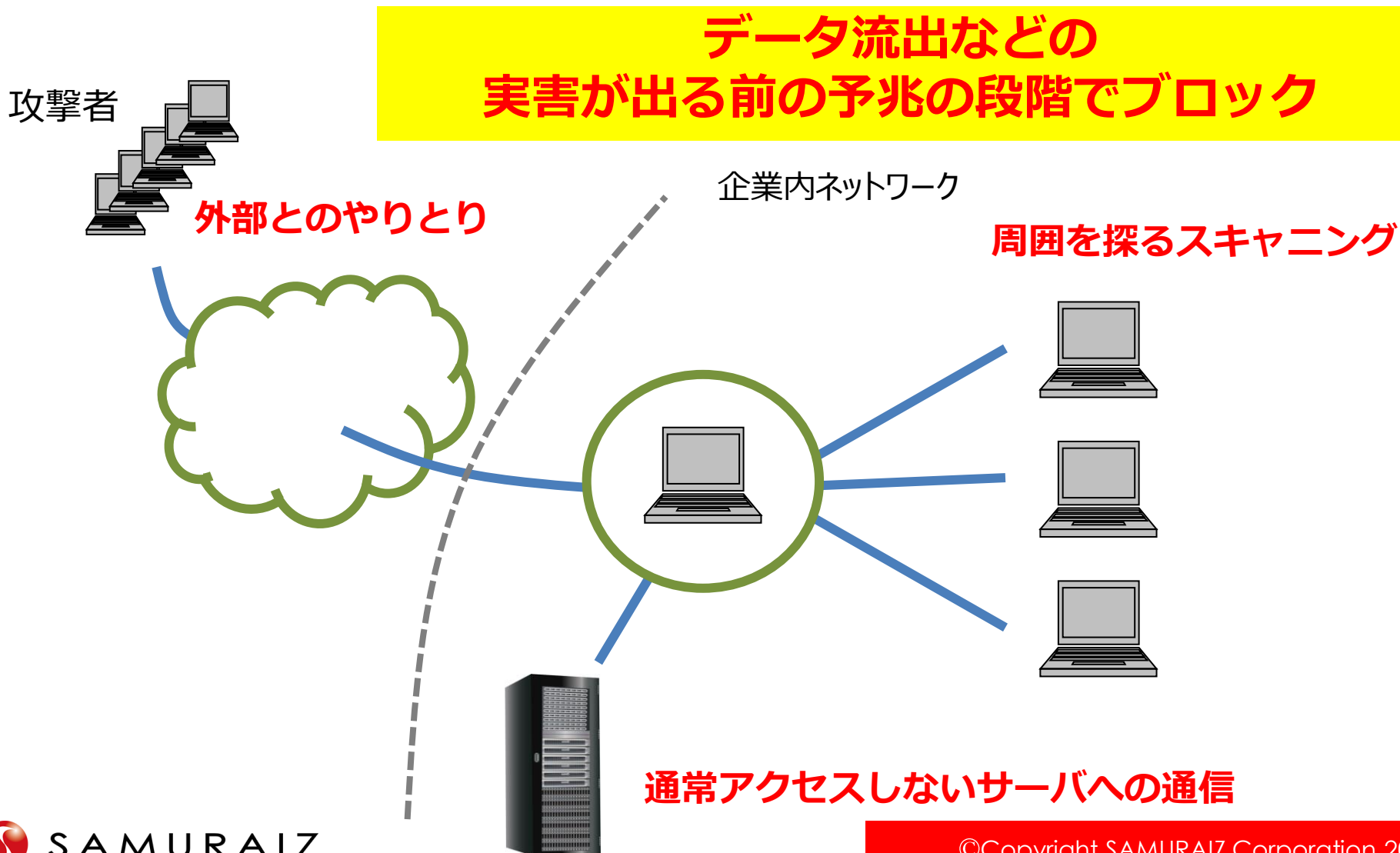
通常と合致しない異常な挙動

サーバー
アクセス

ポート
スキャン

検出パターン例

例えば、「マルウェア」



未知の脅威や潜在的な危機をブロックするのではなく、

遭遇してしまうことを前提として、
遭遇した結果起こる事象を検知するというアプローチ

**SIEMでは実現しえなかった
ネットワーク全体のリアルタイムな可視化**

セキュリティモニタリングソリューション

Darktrace Enterprise Immune System
Darktrace Industrial Immune System のご紹介

新たなアプローチを実現するために英国ダークトレース社が提供する、

セキュリティモニタリング用のアプライアンス製品

■ダークトレース社

数学者と政府情報機関のスペシャリストにより、2013 年英国ケンブリッジにて設立

英国ケンブリッジ、米国サンフランシスコを本拠点とし、21カ所にオフィスを展開

全世界で1,200社以上の導入実績、16,000以上の脅威を検出

人体が多様な外的や環境変化（感染、発病等）に対抗する仕組みを
ITセキュリティに応用している

Enterprise と Industrial に違いは？

Enterprise Immune System

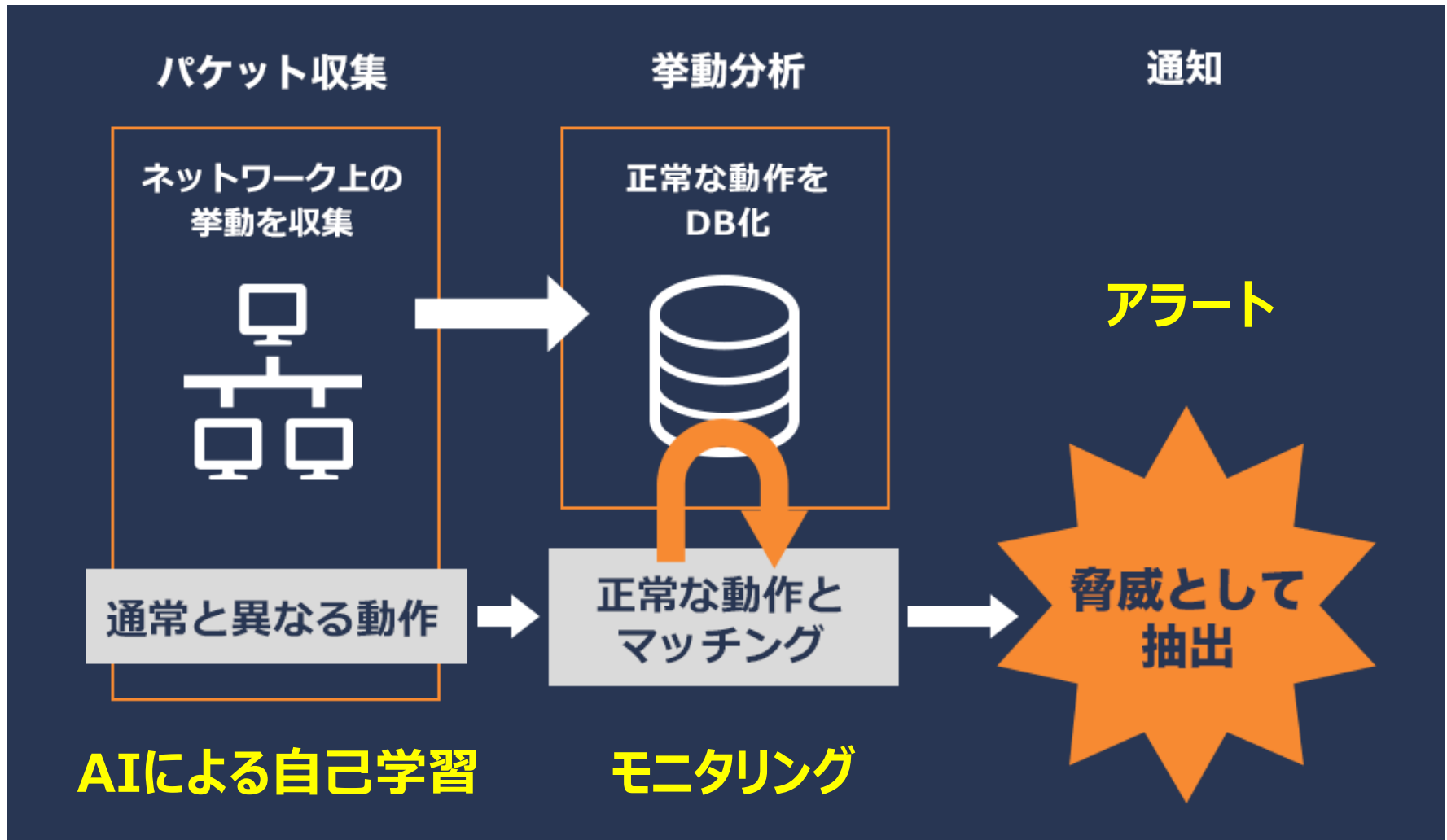
→ 通常の企業ネットワーク向け

Industrial Immune System

→ 制御系ネットワーク向け

- Enterprise Immune Systemの脅威検知対象をSaaSアプリケーションに拡大
 - SaaSアプリケーションに接続する各デバイスのログイン情報、データ通信およびダウンロード、アップデート情報を常に可視化することで、クラウド上の疑わしい振る舞いや異常な挙動のリアルタイム検知が可能になりました。
 - Salesforce.com、Box、Google Apps、Microsoft Office 365 については、ユーザーのやりとりを100%可視化することが可能

具体的には・・・。



Search for a device, subnet, IP or host...

Thu Sep 15 2016 / 18:33:00 +09:00

Home

Menu

Breach Log



Math / Device / Unusual Activity

Wed Sep 7, 18:33:26 - Thu Sep 15, 18:33:26

Tue Sep 13 20:09:01 mne-dc1-3.holdingsinc.com

Unusual Activity

Strength 72 % > 35 %

Mon Sep 12 19:23:01 Linux 434

Unusual Activity

Strength 95 % > 35 %

Mon Sep 12 19:18:01 dipssmith42.holdingscorp.com

Unusual Activity

Strength 67 % > 35 %

Model Breach Event Log

Mon Sep 12 2016, 19:18:01

All Events

Mon Sep 12, 19:18:01 dipssmith42.holdingscorp.com breached model **Math / Device / Unusual Activity**
Mon Sep 12, 19:18:00 **Unusual Activity 67.77%** due to Internal Data Transfer, Internal Connected Devices and Internal Connections to Closed Ports
Mon Sep 12, 19:17:46 dipssmith42.holdingscorp.com connected to mail-oc.holdingsinc.com [445]
Mon Sep 12, 19:17:45 dipssmith42.holdingscorp.com connected to cel12.holdingsinc.com [445]
Mon Sep 12, 19:17:37 dipssmith42.holdingscorp.com connected to File Server [445]

An increase in internal data accessed

Mon Sep 12, 19:17:25 dipssmith42.holdingscorp.com connected to File Server [445]
Mon Sep 12, 19:17:18 dipssmith42.holdingscorp.com failed to connect to 10.100.17.9 [445]
Mon Sep 12, 19:17:18 dipssmith42.holdingscorp.com failed to connect to 10.100.17.10 [445]
Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:16 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:13 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]
Mon Sep 12, 19:17:12 dipssmith42.holdingscorp.com connected to 10.100.17.8 [445]

An increase in the number of internal IPs connected to

Mon Sep 12, 19:17:11 dipssmith42.holdingscorp.com connected to File Server [445]
Mon Sep 12, 19:17:09 dipssmith42.holdingscorp.com connected to 10.100.17.28 [445]
Mon Sep 12, 19:16:13 dipssmith42.holdingscorp.com connected to Domain Controller [445]

com failed to connect to 10.10...

[com failed to connect to 10.100.17.10 [445]] Mon Sep 12, 19:17:17 dipssmith42.holdingscorp.com failed ...

Last 7 days

Wed Sep 7, 18:33:26

Thu Sep 15, 18:33:26

Models, highest score

Include acknowledged breaches

20%

Math / Device /
Unusual ActivityMath / User /
Unusual Credential
useMath / Unusual
ConnectivityMath / Network
Profile / Rare
connection from

DARKTRACE

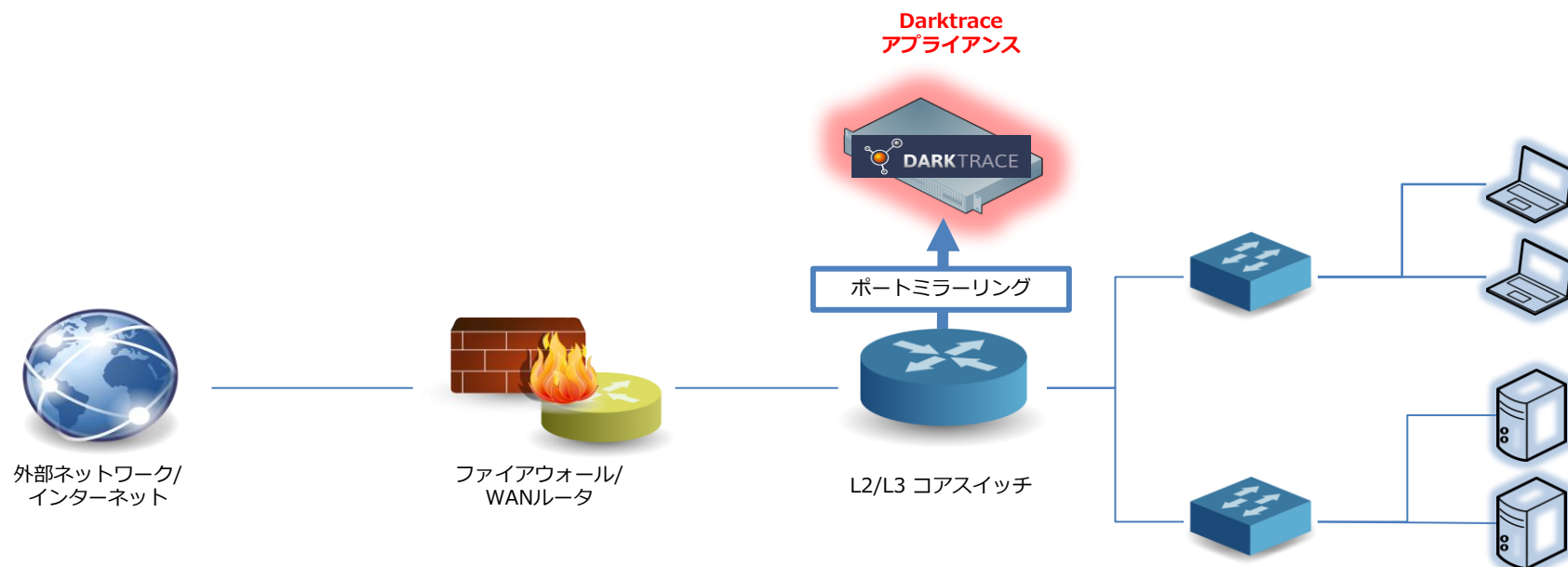
Enterprise Immune System の位置付け



- マルウェア/ランサムウェアをはじめとした未知の脅威対策
- 内部による脅威対策
- 内部統制の効果
- SIEMでは実現しえなかったネットワーク全体のリアルタイムな可視化

- 事前の定義を必要とせず、自己学習してモニタリングを開始
- 既存のセキュリティを否定するものではなく強化するもの
- システムの可用性に影響を与えない

- ポートミラーによるパケット収集
- 監視対象ノード数に応じたサーバー構成
 - S (1,000) 、M (10,000) 、X2 (35,000)
- 階層化構成による複数トポロジーの一括管理



監視対象：1,000ノード

月額：240,000円～

3週間のPoV（Proof of Value）

- ・3週間の無償トライアル
- ・毎週検出結果をご報告 & 脅威度の確認
- ・導入価値のご判断

お問合せ先：

**株式会社サムライズ
マーケティンググループ**

**〒141-0032 東京都品川区大崎1-6-4 新大崎勧業ビル10F
TEL: 03-5436-2044**

**Mail : darktrace_info@samuraiz.co.jp
<http://www.samuraiz.co.jp/darktrace>**

**<http://www.samuraiz.co.jp/>
<http://www.facebook.com/SamuraizCorp>**

記載されている会社名や製品ブランド名は各社の商標または登録商標です。

2016年10月18日（火） 15:30より

サムライズセミナールーム（エメラルドマウンテン）

http://www.samuraiz.co.jp/event/31_161018.html

ご清聴ありがとうございました。

※アンケート回収にご協力下さい。