# 再考、エンドポイントセキュリティ

# ~インシデント発生時に慌てないための要諦~



エバンジェリスト 内山 史一

#### **Profile**

#### 名前:

内山 史一(うちやま ふみかず)

#### 所属/役職:

株式会社インフォメーション・ディベロプメント サイバー・セキュリティ・ソリューション部 / iD-SIRT / エバンジェリスト

#### 主な略歴:

- 大手金融機関でNWインフラ管理やNW更改プロジェクトに参画
- セキュリティ企業で不正アクセス監視業務に従事
- 大手金融機関のCSIRT支援 現在、当社のセキュリティサービス企画・インシデントレスポンスに従事

#### 認定:

CISSP、PMP、情報処理技術者(ネットワーク、セキュリティ)



会社名

株式会社インフォメーション・ディベロプメント

本計所在地 東京都千代田区五番町12-1 番町会館

2019年 4月1日 (IDホールディングス 1969年10月20日) 設立 代表者 代表取締役計長 山川 利雄

4億円(2019年4月1日現在)

従業員数 1,752名(2019年3月31日現在)

株式会社IDホールディングス(持株会社)

東京証券取引所 市場第一部 証券コード:4709

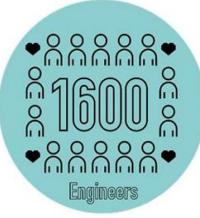
資本金

上場

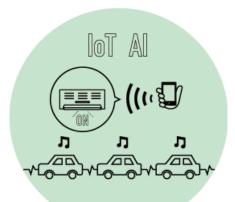


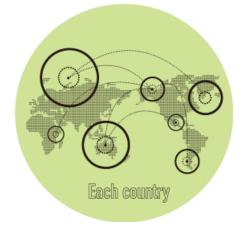
### IDとは









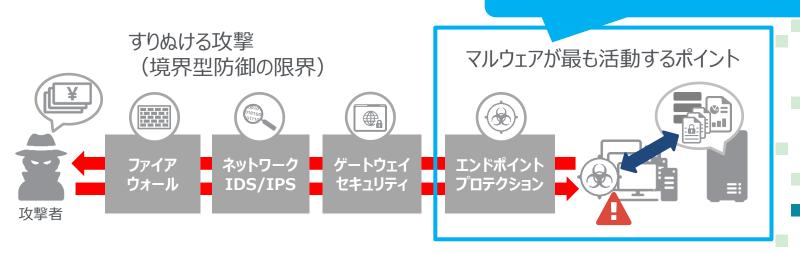




### Concept

# エンドポイントセキュリティの再定義

#### 本日のお話はここです

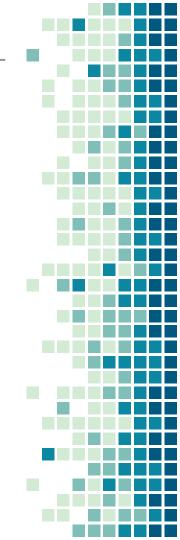


### Agenda

- 1. 変わる、エンドポイントセキュリティの役割
- 2. なぜ?変化が求められるのか

3. セキュリティ担当者の心配事

4. 有事に慌てないための勘所と備え



#### 1. 変わる、エンドポイントセキュリティの役割

2. なぜ?変化が求められるのか

3. セキュリティ担当者の心配事

4. 有事に慌てないための勘所と備え

8

#### エンドポイントセキュリティのイメージ



- ✓ デバイスはPCやサーバ
- ✓ 基本的にデバイスは社内



✓ 既知のマルウェア防御

# エンドポイントセキュリティ=ウイルス対策ソフト

#### 変わる、エンドポイントセキュリティの役割



- ✓ 多様なデバイス
- ✓ 社外利用シーンの増加
- ✓ サーバは境界の外にも



- ✓ 既知のマルウェア防御
- ✓ 未知のマルウェア防御
- ✓ 不審な挙動や攻撃の防御
- ✓ 脆弱性攻撃の防御
- ✓ 資格情報の保護
- ✓ HDD暗号化の修復

### 変わる、エンドポイントセキュリティの役割





# 多様なデバイスと利用シーンをカバーする 多層化されたセキュリティ機能

- ✓ 脆弱性攻撃の防御
  - ✓ 資格情報の保護
- ✓ HDD暗号化の修復

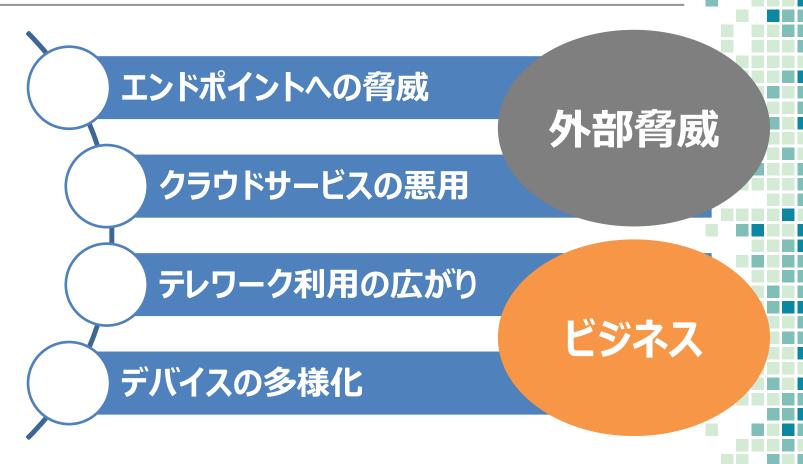
1. 変わる、エンドポイントセキュリティの役割

2. なぜ?変化が求められるのか

3. セキュリティ担当者の心配事

4. 有事に慌てないための勘所と備え

### 変化が求められる背景



# エンドポイントへの脅威 (1/3)

ばらまき型攻撃



高度標的型攻擊

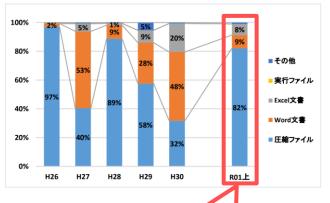


**TARGETING** 

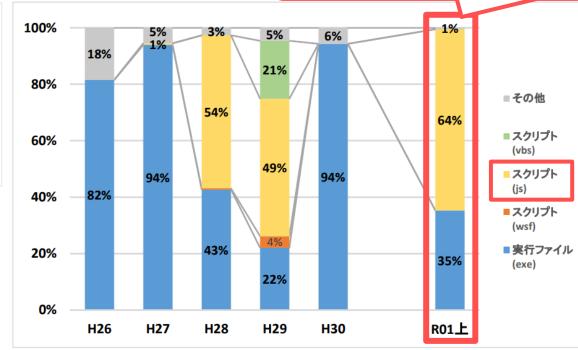
### エンドポイントへの脅威 (2/3)

#### JavaScript を圧縮した添付ファイルが多い

添付の中身は.js H29以来の**半数越えの64%** 



添付ファイル形式は 圧縮ファイルが多数 前年32%→**82%** 



出典:警察庁 | 令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01\_kami\_cyber\_jousei.pdf

### エンドポイントへの脅威 (3/3)

#### 従来型のウイルス対策では検知が難しい攻撃

July 8, 2019

Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack

Microsoft Defender ATP Research Team

Windowsの正規システムツールを悪用し、 トロイの木馬「Astaroth」に感染させる

そこにあるもので攻撃を実行する

Living off the land(環境寄生)

.lnk含むZipが添付されたフィッシングメール

Process hollowing

containing a .Ink file with misleading file name. When clicked, the .Ink file runs a BAT command-line that runs WMIC.

WMIC downloads an XSL file that h

WMIC downloads an XSL file that hosts an obfuscated JavaScript, which runs WMIC again.

email with URL to an archive file

WMIC once again downloads an XSL file that hosts an obfuscated JavaScript, which uses the Bitsadmin, Certutil, and Resort tools for the next steps.

Multiple instances of Bitsadmin download encoded payloads.

Certutil decodes the downloaded payloads.

Regsvr32

One of the decoded payloads is run with Regsvr32 tool and runs a second DLL, which in turn reflectively loads a third DLL This DLL decrypts and injects another DLL into Isserinit.

The DLL that's loaded into
Userinit is a proxy that reads,
decrypts, and reflectively loads a
final DLL, which is the infostealer Astaroth

Userinit

wMIC

Download

XSL file

JavaScript

WMIC Download XSL file JavaScript

Bitsadmin

Bitsadmin

Download

Certutil

Decode

Payloads

DLL Reflective DLL Astaroth loading

Astarothに感染

Process injection

出典: Microsoft | Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/

#### クラウドサービスの悪用

#### 正規サービスを悪用し検知回避を狙う

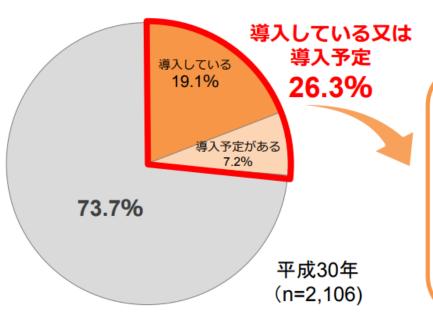


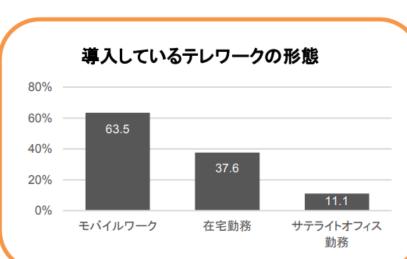
出典: LAC | DropboxをC2サーバとして悪用する、日本を狙った新たなマルウェアを確認https://www.lac.co.jp/lacwatch/people/20180925 001704.html

AWSやGCPをC2サーバとして利用する攻撃も確認されている

### テレワーク利用の広がり (1/2)

#### テレワークの導入状況(企業)



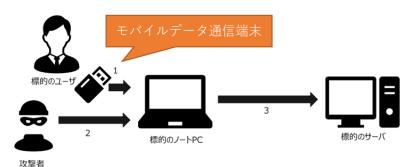


出典:総務省 | 平成30年通信利用動向調査の結果

http://www.soumu.go.jp/johotsusintokei/statistics/data/190531 1.pdf

### テレワーク利用の広がり (2/2)

#### モバイル端末のマルウェア感染



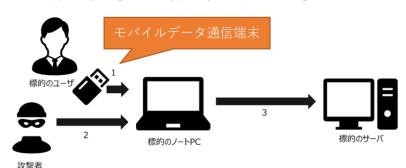
出典: Secureworks | 日本国内でモバイルデータ通信端末経由のマルウェア感染事案が増加https://www.secureworks.jp/resources/at-portable-connection-devices-spreading-malware





## テレワーク利用の広がり (2/2)

#### モバイル端末のマルウェア感染

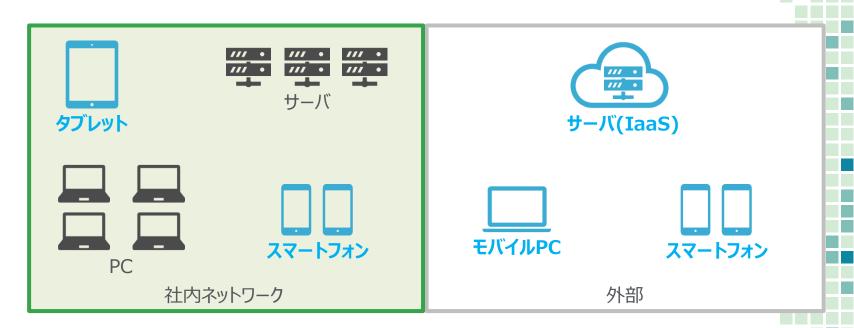


出典: Secureworks | 日本国内でモバイルデータ通信端末経由のマルウェア感染事案が増加 https://www.secureworks.jp/resources/at-portable-connection-devices-spreading-malware



#### デバイスの多様化

#### ネットワークに接続するデバイスの増加



#### 攻撃対象可能な領域が拡大

### エンドポイントセキュリティも変わらなくてはならない

背景	自組織における懸念事項		想定されるリスク
エンドポイントへの脅威	✓ Windowsの <b>正規管理ツールを使った</b> 攻撃 の発生	I j	女撃に気づきにくい
クラウドサービスの悪用	✓ パブリッククラウドサービスを悪用した攻撃 の発生		感染後の迅速な対応がで ない
テレワーク利用の広がり	<ul><li>✓ 社内NW接続時と比較して相対的にセキュ リティレベルが低い環境での利用</li><li>✓ 監視していないモバイル端末がマルウェア感 染</li></ul>	唇	感染端末の社内NW接続
デバイスの多様化	<ul><li>✓ NW接続デバイスが増加し、<b>攻撃対象可能</b> な領域が拡大</li><li>✓ セキュリティ対応組織の守る範囲が拡大</li></ul>		2キュリティ対応組織の負 市増大

#### エンドポイントセキュリティも環境変化に対応しなくてはならない

1. 変わる、エンドポイントセキュリティの役割

2. なぜ?変化が求められるのか

3. セキュリティ担当者の心配事

4. 有事に慌てないための勘所と備え

### セキュリティ担当者の心配事



#### 社員

- ✓ ひっかかりやすい人がいる
- ✓ 感染端末の利用者がつかまらない
- ✓ 途中で外出してしまう



#### エンドポイントの構成管理

- ✓ 把握できていない端末がある
- ✓ 感染端末の所在が不明
- ✓ 脆弱なSWをもつ端末が不明



#### セキュリティ対応組織

- ✓ マルウェアの通信先の封じ込み に時間を要する
- ✓ 感染の疑いがある端末を調査 する労力が大きい



#### モバイル

- ✓ 外部で持出しPCが感染しても 気づけない
- ✓ スマートフォンのマルウェア感染

### 心配事はつきないが・・・これは避けたい

✓進行中の攻撃に気づけない

✓マルウェア感染のアウトブレーク



1. 変わる、エンドポイントセキュリティの役割

2. なぜ?変化が求められるのか

3. セキュリティ担当者の心配事

4. 有事に慌てないための勘所と備え

### 基本が一番大事

✓守るものは何か

✓脅威は何か

✓どのように検知・対応するか



### ガイドラインからのアプローチ (1/4)

- ✓ サイバーセキュリティ経営ガイドライン
- ✓ NIST Cybersecurity Framework
- ✓ ISMS (ISO/IEC27001, 27002)

### **✓CIS Controls**

- 米国の公的機関やセキュリティ企業等が共同開発した、NIST CSF や ISMSに並びグローバルで普及するフレームワーク
- サイバー攻撃対策にフォーカスし、**具体的な技術対策**が示されている

### ガイドラインからのアプローチ (2/4)

#### CIS Controls™

#### Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

#### **Foundational**

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

### Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

出典: CIS | CIS Controls V7 https://learn.cisecurity.org/control-download

### ガイドラインからのアプローチ (2/4)

#### CIS Controls™



#### Basic

- Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- Maintenance, Monitoring and Analysis of Audit

- ①ハードウェア資産のインベントリとコントロール
- ②ソフトウェア資産のインベントリとコントロール
- ③継続的な脆弱性管理
- ④管理権限のコントロールされた使用
- ⑤モバイルデバイス、ラップトップ、ワークステーション およびサーバに関するハードウェアおよびソフトウェア のセキュアな設定
- ⑥監査ログの保守、監視および分析

出典: CIS | CIS Controls V7 https://learn.cisecurity.org/control-download

## ガイドラインからのアプローチ (3/4)





#### Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit

#### **Foundational**

- 7 Email and Web Browser Protections
- Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

- 12 Boundary Defense
  - . ⑧マルウェア対策
- 14 Controlled Access Based on the Need to Know
- 5 Wireless Access Control
- 16 Account Monitoring and Control

#### **Organizational**

- 17 Implement a Security Awareness and Training Program
  - ion Software
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

出典: CIS | CIS Controls V7 https://learn.cisecurity.org/control-download

### ガイドラインからのアプローチ (4/4)

CIS Control 8: マルウェア対策

サフ゛コントロール	コントロールタイフ°	
8.1	<b>集中管理</b> されたアンチマルウェアソフトウェアを活用する	
8.2	アンチマルウェアとシグネチャが <u>更新されている</u> ことを確認する	
8.3	オペレーティングシステムの <u>悪用防止機能</u> を有効にする/ <u>悪用防止</u> <u>技術</u> を適用する	
8.4	取り外し可能な <u>メディアのアンチマルウェアスキャン</u> を構成する	
8.5	デバイスがコンテンツを <u>自動実行しない</u> ように設定する	
8.6	アンチマルウェアロギングを <b>集中管理</b> する	
8.7	<b>DNSクエリ</b> のロギングを有効にする	
8.8	<b>コマンドライン監査</b> ロギングを有効にする	
	出典:CIS   CIS Controls V7	

### ガイドラインからのアプローチ (4/4)

#### CIS Control 8: マルウェア対策

サフ゛コントロール	コントロールタイフ°				
8.1	<b>集中管理</b> されたアンチマルウェアソフトウェアを活用する				
8.2	アンチマルウェアとシグネチャが <u>更新されている</u> ことを確認する				
8.3	オペレーティングシステムの悪用防止機能を有効にする/悪用防止 技術を適用する				
8.4	攻撃者の「Living off the land (環境寄生)」に対し、				
8.5	ロギングはイベントの発生方法・内容・状況の把握を容易にする				
8.6					
8.7	<b>DNSクエリ</b> の で有効にする				
8.8	<b>コマンドライン監査</b> ロギングを有効にする				

### エンドポイントセキュリティも変わらなくてはならない

背景	自組織における懸念事項		想定されるリスク
エンドポイントへの脅威	✓ Windowsの <b>正規管理ツールを使った</b> 攻撃 の発生	I I	文撃に気づきにくい
クラウドサービスの悪用	✓ パブリッククラウドサービスを悪用した攻撃 の発生		感染後の迅速な対応がで きない
テレワーク利用の広がり	<ul><li>✓ 社内NW接続時と比較して相対的にセキュ リティレベルが低い環境での利用</li><li>✓ 監視していないモバイル端末がマルウェア感染</li></ul>	垣	感染端末の社内NW接続
デバイスの多様化	<ul><li>✓ NW接続デバイスが増加し、<b>攻撃対象可能</b></li><li><b>な領域が拡大</b></li><li>✓ セキュリティ対応組織の<b>守る範囲が拡大</b></li></ul>		2キュリティ対応組織の負 市増大

#### エンドポイントセキュリティも環境変化に対応しなくてはならない



#### **MVISION ePO**

シンプルなクラウドベースの SaaS管理サービス



#### **MVISION Endpoint**

統合された管理を備えた Windows 10の高度な拡張防御機能

# **MVISION**



#### **MVISION EDR**

強力な脅威の検出、調査、 および対応の簡素化



#### **MVISION** Mobile

他デバイスと同様、iOSと Androidを集中管理し、防御

#### 多層化された統合型セキュリティ

# **MVISION**





機械学習 Fileless脅威の検知 データのロールバック パスワード盗難防止



機械学習 アプリケーションの動的隔離 シグニチャベースの マルウェア検知 ホストIPS ファイアウォール Webコントロール スクリプトベースの 脅威保護(AMSI連携)



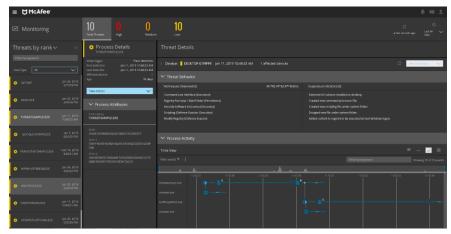
機械学習 振る舞い分析 - Device Safety

- Network Safety - App Safety



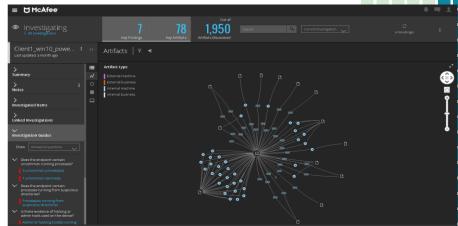
### 検知から恒久対応まで支援する MVISION EDR

#### EDR機能



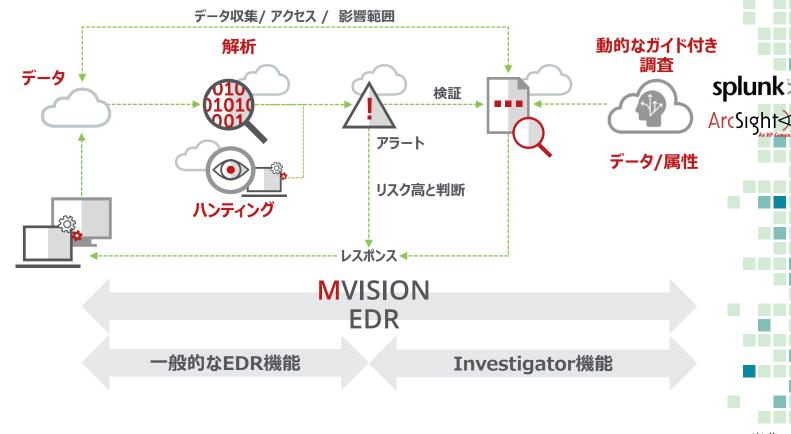
- ✓ エンドポイントの動作を解析し脅威検知
- ✓ NW隔離、ファイル削除、プロセス停止等 のレスポンス機能を提供
- ✓ マルウェアの挙動をタイムラインで可視化

#### Investigator機能

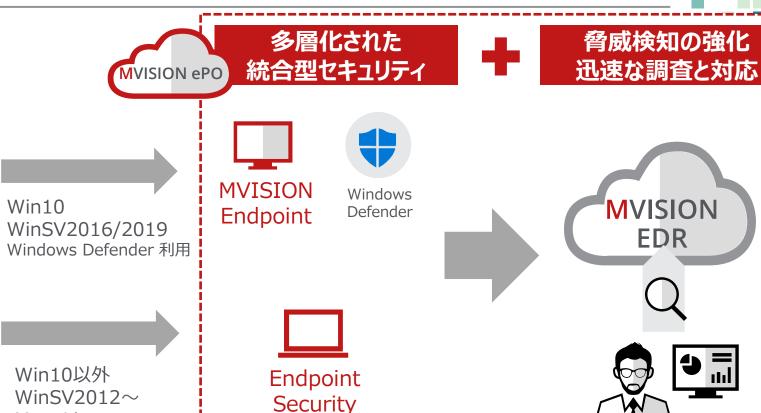


- ✓ エンドポイントのスナップショットデータを基に 更なる詳細な調査・解析が可能
- ✓ エキスパートガイド機能による分析作業の 自動補助

### MVISION EDIPおけるレスポンスイメージ



### 目指すべきエンドポイントセキュリティの姿



McAfee

もしくは 他社製品 (既知の対策)

Mac, Linux

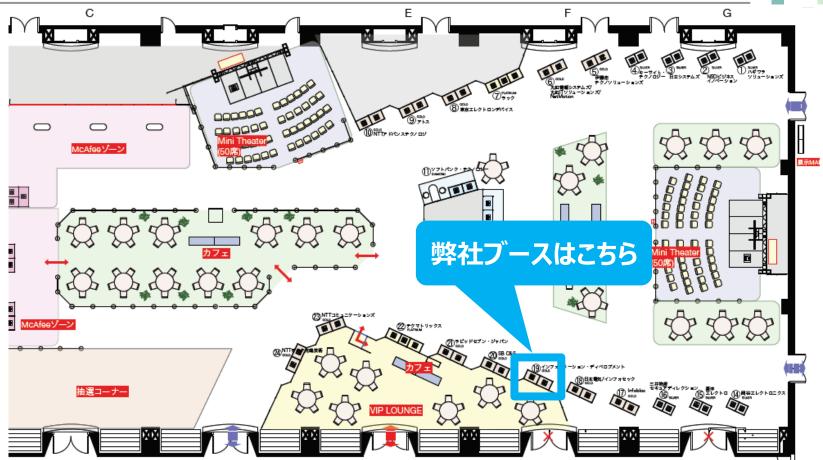
### 本日のまとめ

✓ エンドポイントセキュリティには、 **多様なデバイスと利用シーン**を
カバーする **多層化されたセキュリティ機能**が求められています。

✓ 変化が求められる背景には、外部脅威への対応とビジネス環境の変化があります。

✓ 有事に備えるため、構成管理等の基本コントロールと環境変化に対応したセキュリティ機能の実装が重要です。

### 弊社ブースのご案内



# ご清聴有難うございました

