Hewlett Packard Enterprise

サイバーセキュリティ重点事項について

日本ヒューレット・パッカード株式会社
サイバーディフェンスエバンジェリスト
塩屋通宏

2017年2月18日

自己紹介

在日米軍施設の情報システム部員として勤務

国家公務員ではなく、国家に雇用される者

「国防」を体験して分かった、真のセキュリティとは？

塩屋さんが在日米軍で働いていた時期は、ちょうど国際紛争が起きた時期だった。紛争地域はもちろん、米軍基地でもテロ対策などの警戒レベルが高まり、さまざまなセキュリティ対策が行われたそうだ。

「大統領をトップとして、非常に統率が取れたセキュリティ対策ができていました。もちろん国と企業では、規模もミッションも異なりますが、企業のトップである経営陣としても、ここから学べることは多いと思っています」（塩屋さん）

塩屋さんが国防に関わる中で感じたセキュリティ対策のポイントは次の5つだ。各項目について塩屋さんに解説してもらった。

塩屋さんは在日米軍施設に勤務していたそうだ

1. 守るべきものが明確であること
2. リスクと脅威は明確で、段階的であること
3. 脅威のレベルに対し、それぞれに対策があること
4. 行動や判断をする際に、正しい情報を根拠としていること
5. 責任者が明確であること

ITmedia 掲載記事より
http://www.itmedia.co.jp/enterprise/articles/1609/26/news003.html

Hewlett Packard Enterprise

イノベーションとビジネス

イノベーションは、以前にもましてビジネスの成功のカギとなっています。

もう、後戻りはできない。
（より速く、より便利に、より良いサービス）

Hewlett Packard Enterprise

ITイノベーションがビジネスイノベーションを引き起こす。

ビッグデータ

IoTやAI

新しいビジネス

リモートワーク

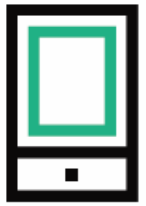
2003

ソーシャルメディア

2006

クラウドコンピューティング

2007



スマートフォン

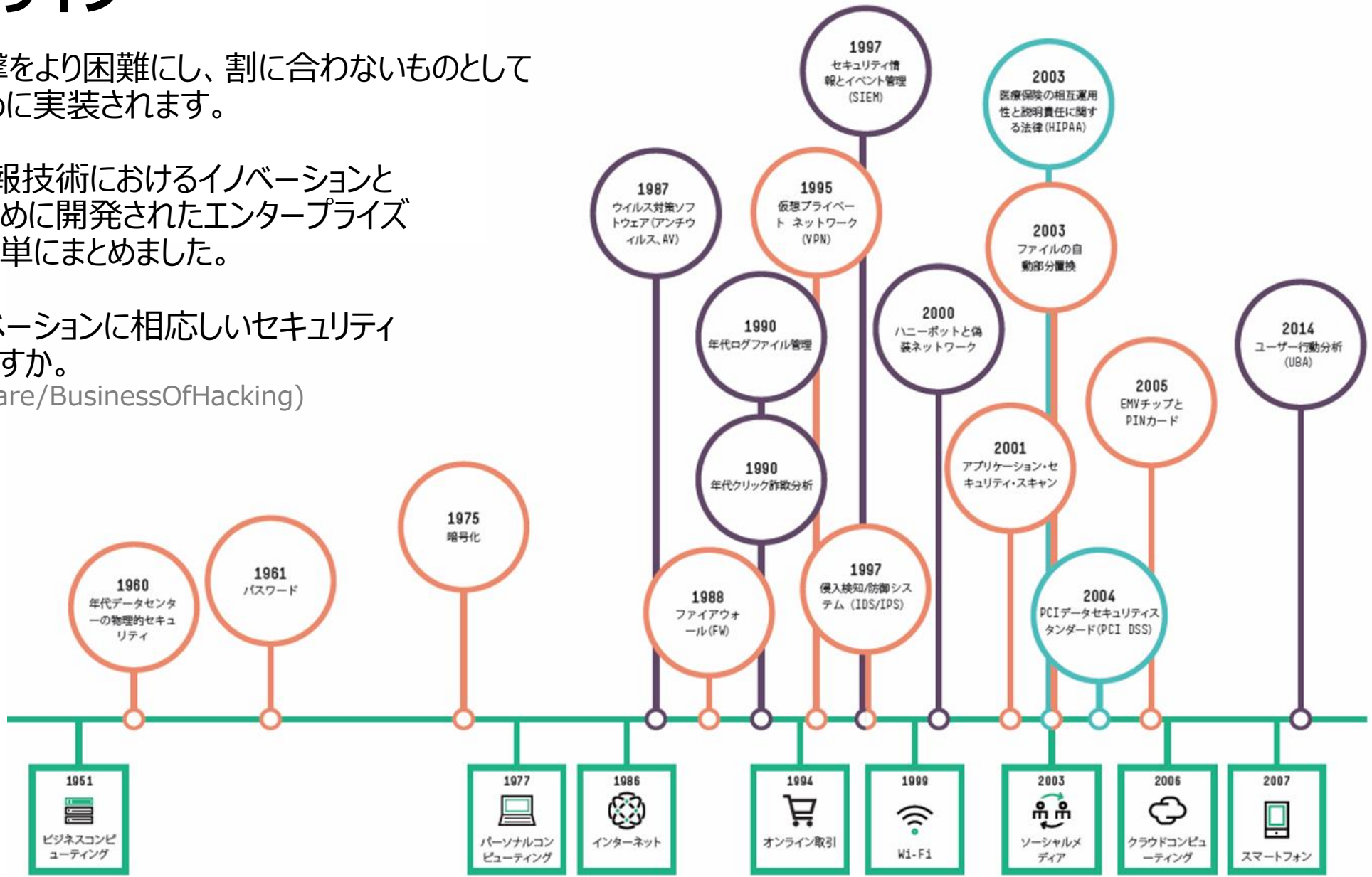
Hewlett Packard Enterprise

撃退のタイムライン

セキュリティ技術は攻撃をより困難にし、割に合わないものとして攻撃者を撃退するために実装されます。

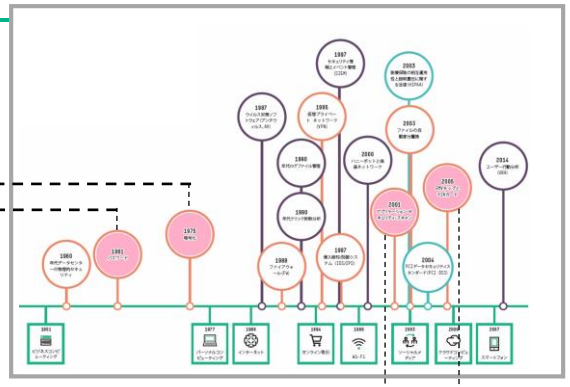
このタイムラインは、情報技術におけるイノベーションとサイバー攻撃撃退のために開発されたエンタープライズセキュリティの歴史を簡単にまとめました。

自社のビジネスのイノベーションに相応しいセキュリティ警備を用意できていますか。
（出典　hpe.com/software/BusinessOfHacking）



Hewlett Packard Enterprise

撃退のタイムライン と 現在



1961

パスワードの導入

現在

組織の67%が強固なパスワードの方針を制定。

***UBM, Most Effective Security Technologies and Practices, 2016年5月。*

1975

暗号化の導入

現在

65%がデータ暗号化を使用。

***UBM, Most Effective Security Technologies and Practices, 2016年5月。*

2001

アプリケーションセキュリティスキャンの導入

現在

モバイルアプリケーションの75%に、重度のまたは重大な脆弱性が少なくとも一つ存在

***HPE, 2016 Cyber Risk Report, 2016年2月*

2005

EMVチップおよびPINカードの導入

現在

EMVカードはスワイプカードの4倍以上価格で販売できます。

***HPE, The Business of Hacking, 2016年5月*

Hewlett Packard Enterprise

イノベーションのスピードにセキュリティは対応できているのか?

Yes & No

ビジネスのイノベーションには、サイバー攻撃の脅威が必ず付きまといます。

セキュリティ対策が、「イタチごっこ」、「エンドレス」といわれる理由です。

Hewlett Packard
Enterprise

裏のビジネス vs. 表のビジネス

（ハッキングビジネス）

Hewlett Packard
Enterprise

地下経済に潜む攻撃者から、

私達の情報を完全に護ることはできるのか?

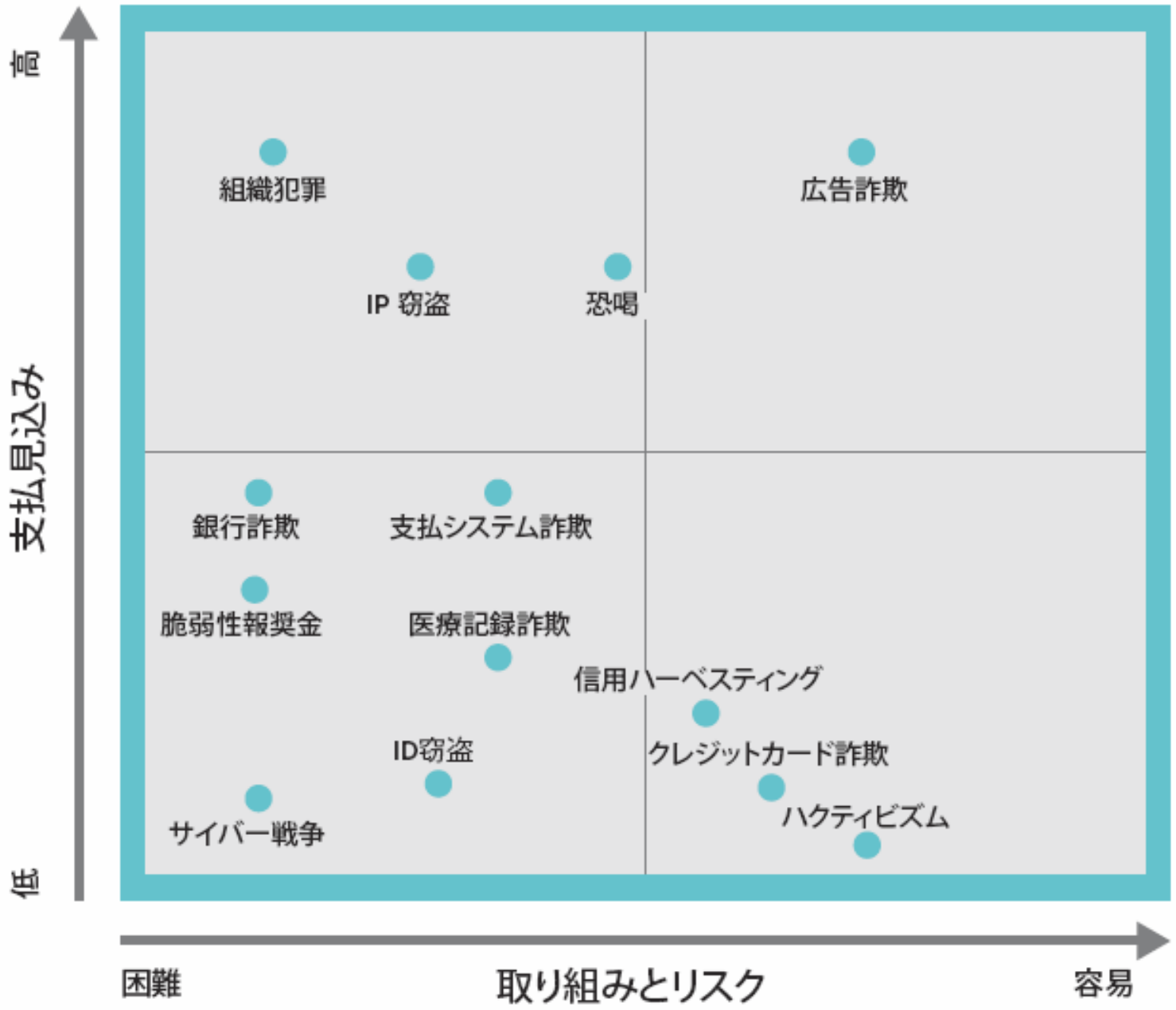
12兆

全世界のブラックマーケット年間市場規模（円）

ハッキングというビジネスが完成されている。

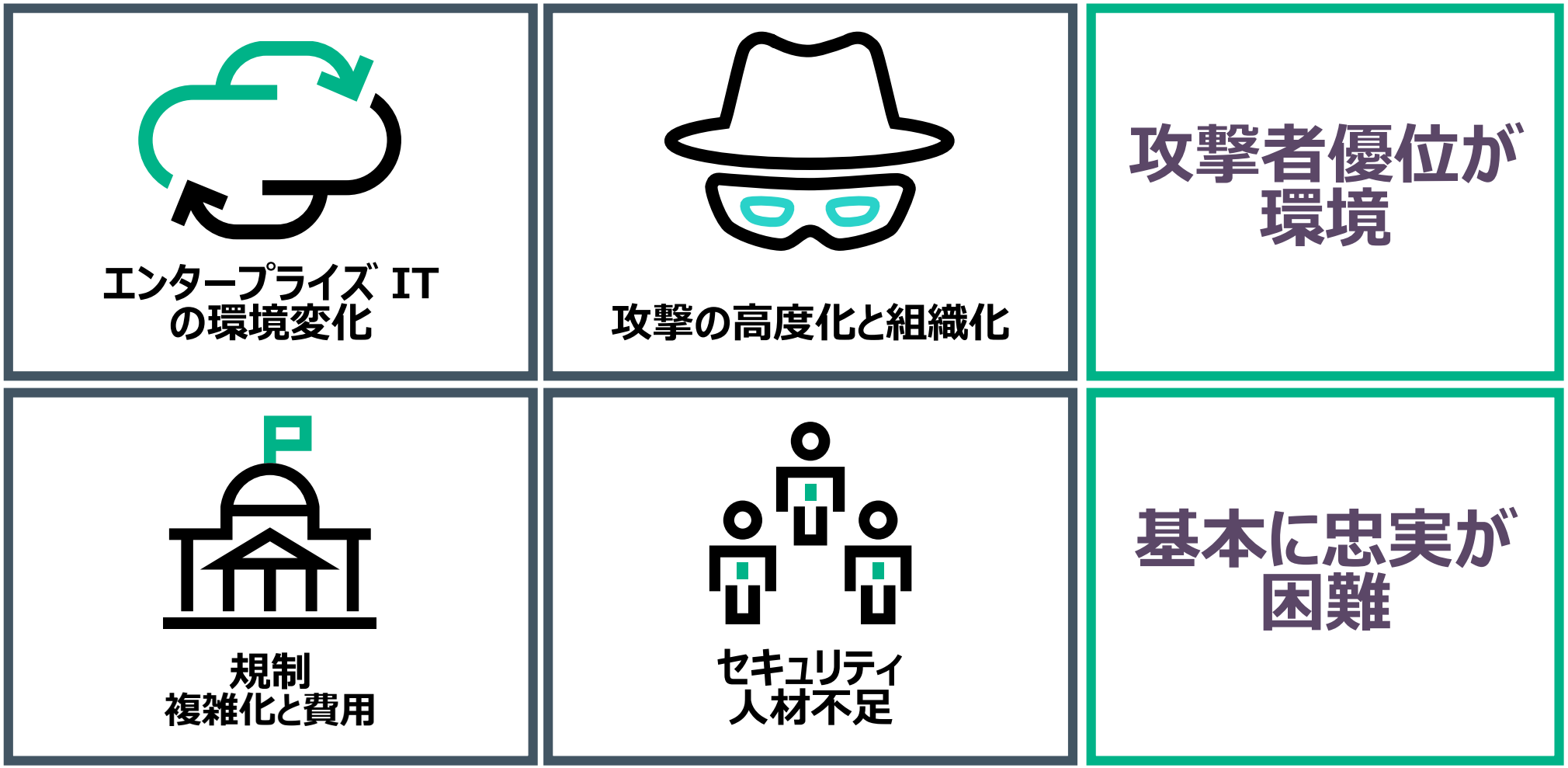
出典:
Ponemon Institute: Enterprise Security Benchmark Survey, November 2012

Hewlett Packard Enterprise



Hewlett Packard Enterprise

「攻撃者を完全に排除することは難しい」と言われている



Hewlett Packard
Enterprise

攻撃者たちから私達の情報を完全に護ることはできるのか?

No & Yes

多くのセキュリティベンダー、セキュリティの専門家は、攻撃者有利と判断。

セキュリティ事故が起こることを前提に対策する必要がある。

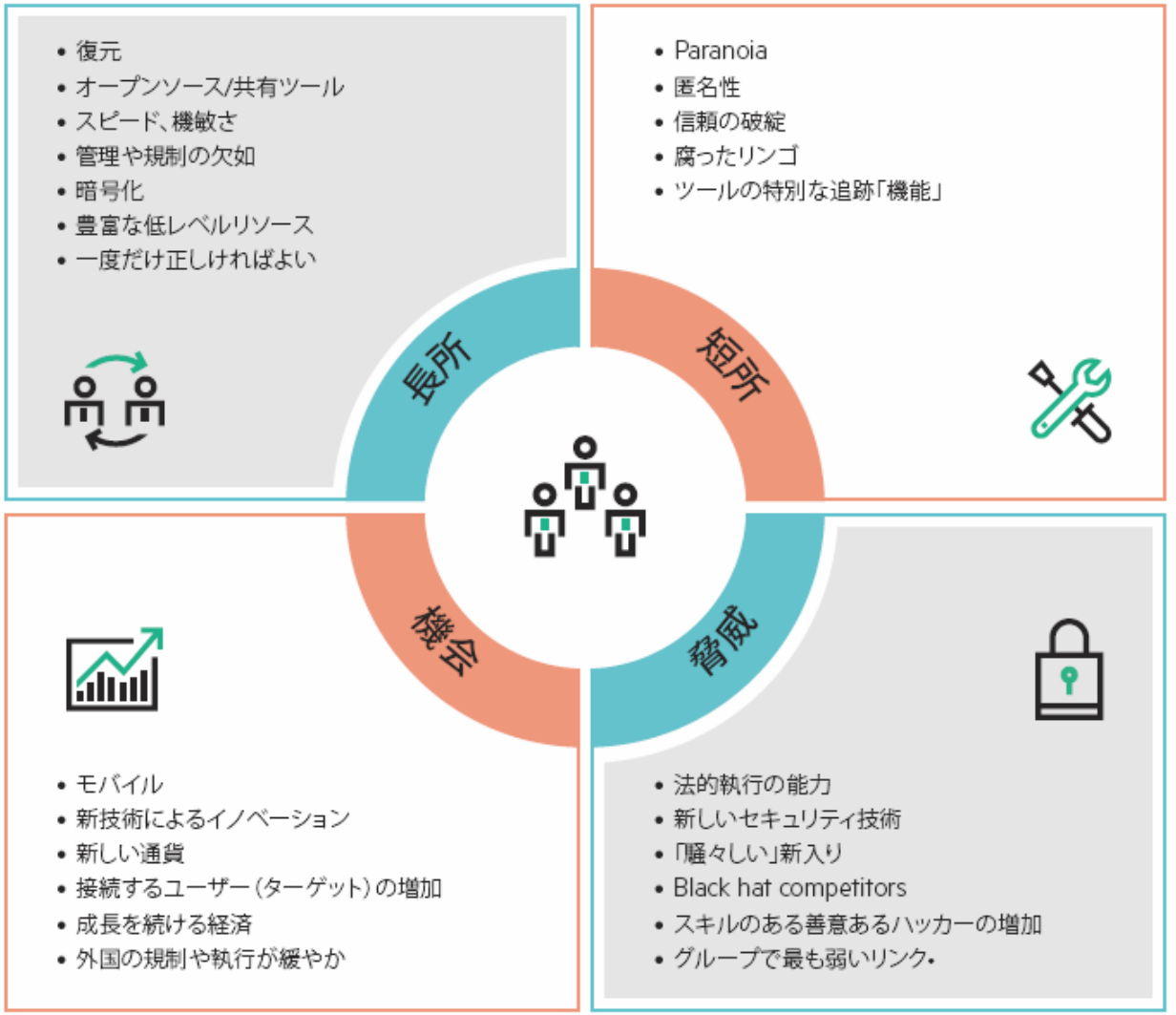
ハッキングビジネスに対抗するために

Hewlett Packard
Enterprise

ハッキングビジネスの研究で、

企業は攻撃者に対抗できるのか？

ハッキングビジネスのSWOT分析



Hewlett Packard Enterprise

ビジネスの目標

Hewlett Packard
Enterprise

アプリケーションは、現在、サイバー攻撃者によって企業や組織の機密データにアクセスできる最も簡単ルート

75

モバイルアプリケーションから脆弱性が見つかる割合（%）

標的の候補を減らす

229-205

2013-2014　　2015-2016

情報漏えいが発覚するまでの平均日数

情報入手までの時間を増やす

Hewlett Packard Enterprise

ハッキングビジネスに対する対抗策はあるか?

Yes & No

裏経済、裏組織を研究することでセキュリティ事故のリスクは低くすることが可能。

サイバーディフェンス重点事項

Hewlett Packard
Enterprise

当たり前、知っている、基本的な事が、

サイバーディフェンス重点事項

最も価値のある
モノ: **データ**

狙われる場所：
アプリケーション

対処するためには：
セキュリティログ

Hewlett Packard
Enterprise

データの暗号化、アプリケーションのリスク管理、ログ分析の仕組みの導入はできていますか？

Yes & No

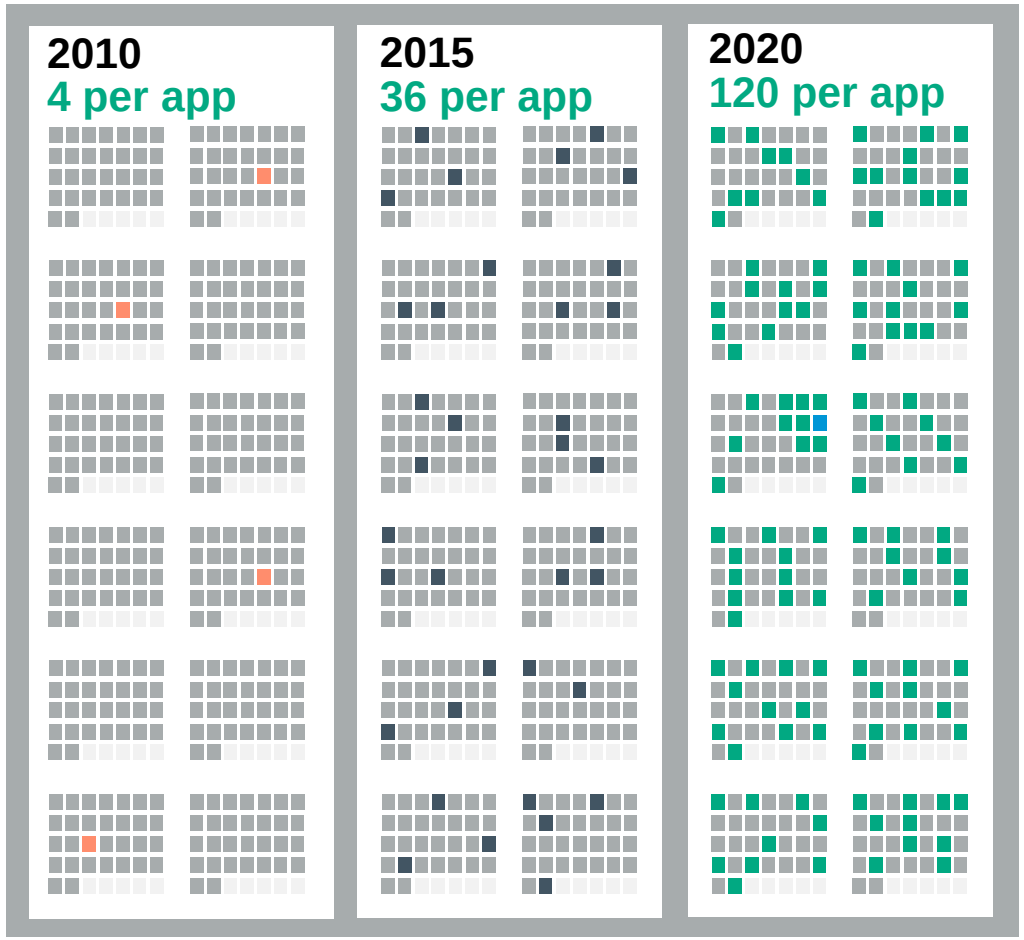
60%以上の企業や組織では、サイバーディフェンス重点事項の対策済み

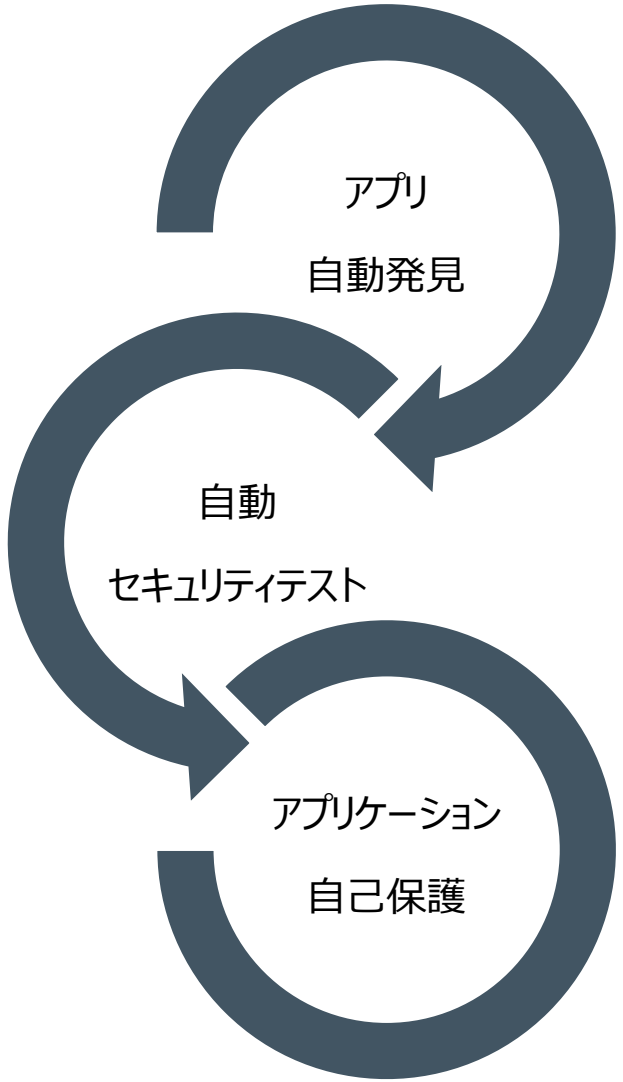
課題は、フレームワークとその拡張性

Hewlett Packard Enterprise

インテリジェンスを利用して、継続的にアプリケーションの穴を監視

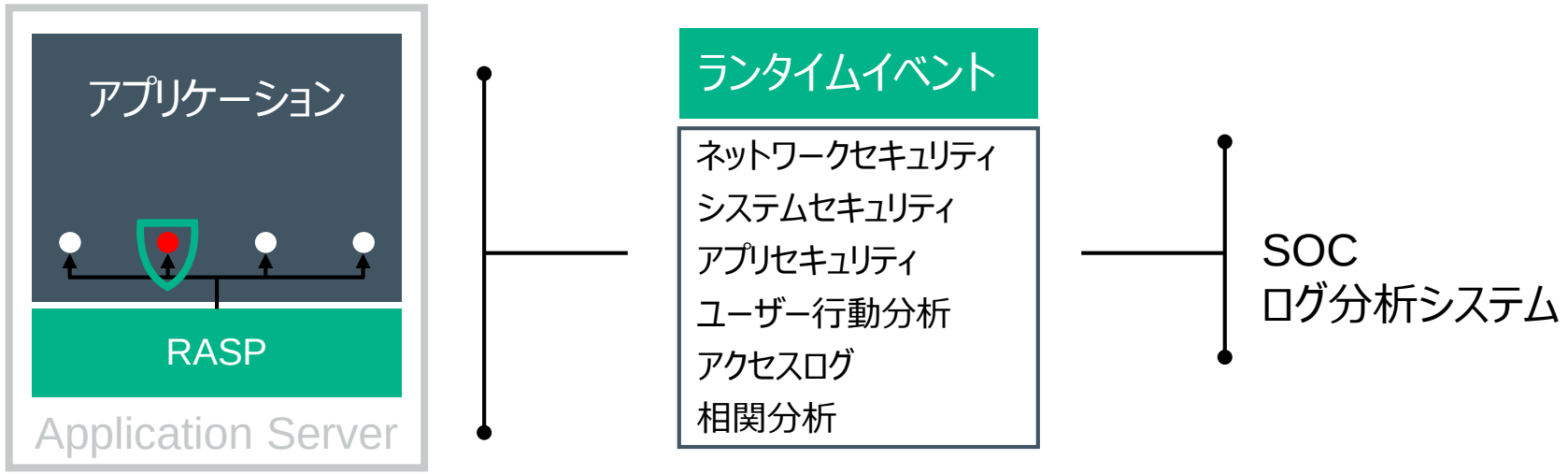
年間アプリケーションリリース回数





Hewlett Packard Enterprise

アプリケーションが不正なアクセス、情報漏えいを検知・報告・遮断



アプリケーションから情報漏えいを防ぐ技術

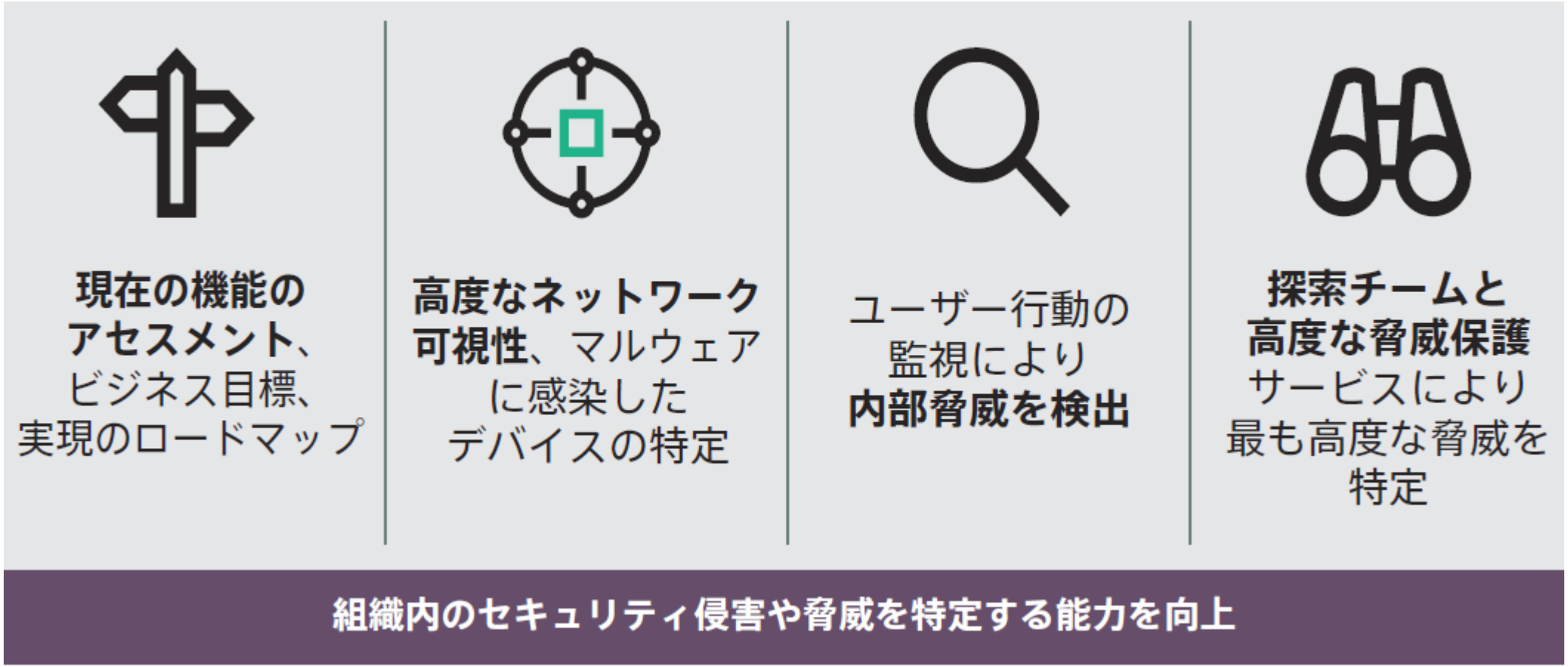
セキュリティ情報収集のフレームワーク

セキュリティリサーチ

- 脅威情報提供
- 年次リスクレポート
- 攻撃者情報レポート
- セキュリティブログやSNS
- セキュリティインテリジェンス

Hewlett Packard
Enterprise

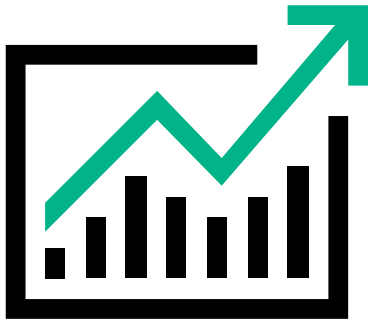
脅威は組織外部からではなく、内部にも潜む



Hewlett Packard Enterprise

SOCからインテリジェントSOCへ
データ分析と人による分析が必須

リアルタイム監視

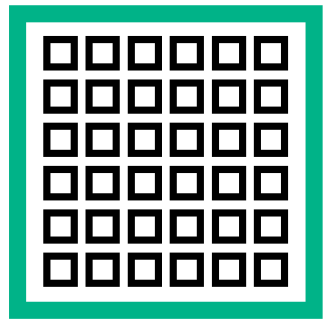


- SOCの基盤
- セキュリティイベントの視覚化
- 既知の脅威検知
- **異常行動情報**を利用して検知時間を短縮
- **75% のSOC**は異常行動情報による時間短縮はできていない

調査

- 現時点までの**基準値**を利用して正常値を把握
- 異常行動の理解と**攻撃の危険性**を理解

Hunt



- 上級セキュリティアナリストは、**行動分析**、機械学習、セキュリティイベント情報により正常値以外に注目
- 正常ではないパターン、異常な行動の検出により**未知の脅威** を発見する能力

Hewlett Packard Enterprise

ハッカーの論理

無視をする／過信する／経験不足

攻撃する
感覚

対応する
直観力

判断する／ミスをする／疲弊する

企業・組織の論理

Hewlett Packard
Enterprise

まとめ

まとめ：サイバーディフェンスの重点

–セキュリティ対策やリスク管理は、イノベーションが起こる限り終わりがない活動

–ユーザー、アプリケーション、データを如何に護るか

–セキュリティインシデントのリアルタイム監視体制を如何に構築できるか

–人が、最大の脅威であり、人が最高の防御壁である

Hewlett Packard
Enterprise

ご清聴、
ありがとうございました。

Michihiro.shioya@hpe.com