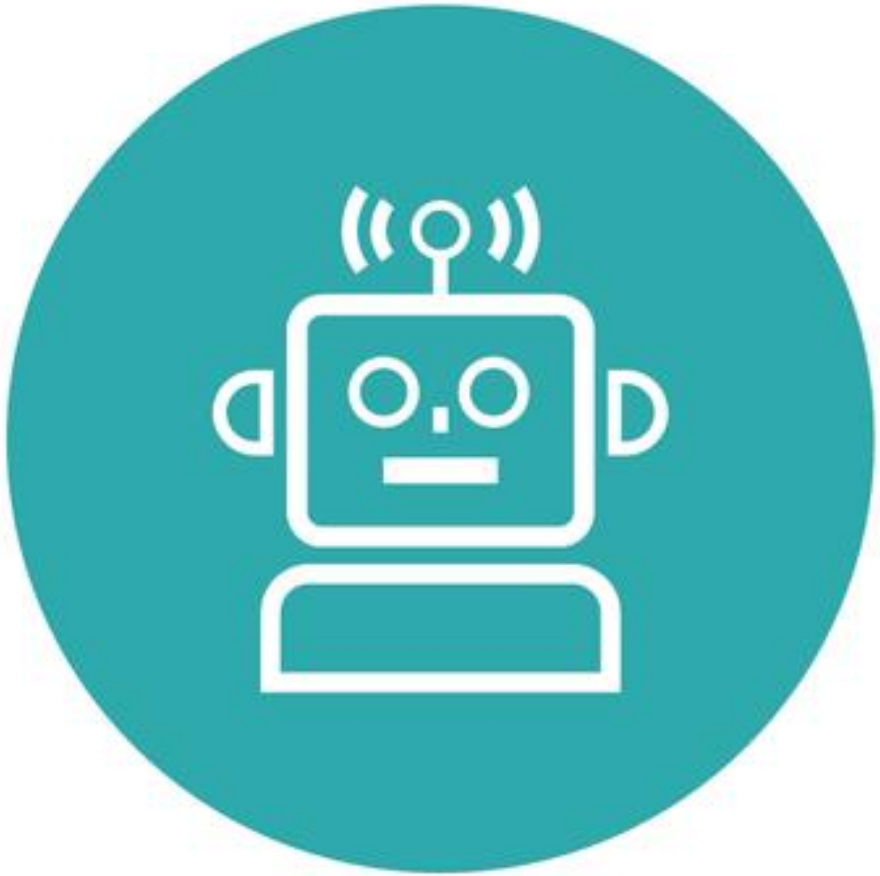
Deloitte.
デロイト トーマツ



新たなビジネス拡大、そこにはサイバーリスクが必ず・・・

これからのサイバーセキュリティを巡る動向と対策の方向性

デロイト トーマツ リスクサービス株式会社
2017年10月24日

講演の概要

高度情報化社会においてビッグデータの利活用やマイナンバーの民間利用は、新たなビジネスチャンスともいわれている。

その反面、サイバー攻撃や個人情報漏えいは最優先に取組むべきリスクである。

サイバーセキュリティを巡る動向と対策の方向性について 、印刷事業者の様々なビジネスシーズ＆チャンスを踏まえて概説する

Agenda

攻撃はどのように行われているのでしょうか？

皆さまはどのような情報をどのようにもっていますか？

どのように対応しましょうか？

攻撃はどのように行われているのでしょうか？

サイバースペースにおける犯罪は日々多様化・高度化しています

インターネット環境の変化

潤沢な資金を持ち組織化された攻撃が世間を騒がす一方で、下記のような環境から、サイバー犯罪は参入障壁の低いビジネスとなり今後も高度な攻撃が増加することが予想されます。

- 攻撃手法のコモディティ化
- ブラックマーケットの拡大
  - 脆弱性・攻撃手法の売買
  - 個人情報の売買
  - ボットネット（ウイルス感染PC）の売買 等
- ローリスク・ハイリターン
- 国境を越えた活動が可能

犯罪者の環境

スマートフォンに代表される携帯型情報端末の普及により、常時インターネットに接続できることが日常になりつつあります。

次のような環境の変化は、利用者にとって便利な反面、犯罪者にとっても都合のよいものとなっています。

- インターネットのコモディティ化
- インターネットビジネスの拡大
- PC等の高性能化
- モバイル端末の利用拡大
- インターネット利用における啓蒙の遅れ

【参考】サイバー攻撃事件の現況

サイバー攻撃事件が日常的なものに・・・（1）

■ 米国A証券への攻撃　【標的型攻撃】

- 米国A証券が2009年にAurora攻撃の被害を受けていたことが、米国のセキュリティ企業が2011年3月にAnonymousによって攻撃を受けた際に発覚
- Aurora攻撃とはInternet Explorerのゼロデイ脆弱性を悪用したAPT攻撃であり、Googleが被害をブログで公表したことで知られている

■ 米国B銀行グループへの攻撃　【システムの脆弱性】

- 2011年6月に、米国のB銀行グループが不正アクセスを受け、顧客情報（顧客名、クレジットカード番号、連絡先）が漏洩したと発表
- 北米で発行したクレジットカードのうち、約1%の会員に影響があった
- なお、クレジットカードの顧客が利用するホームページのURLに顧客の口座番号が埋め込まれる仕様となっており、犯行グループは総当り的にアクセスし大量の口座番号の入手に利用された

■ 国内C地方銀行の顧客への攻撃　【フィッシング】

- 2011年7月に全国の地方銀行で、顧客に対するスパイウェアや金融機関を装ったメールにより、インターネットバンキングのパスワードが盗まれたり不正な振り込みが行われる事件が発生

【参考】サイバー攻撃事件の現況

サイバー攻撃事件が日常的なものに・・・（2）

■ **国内D銀行　【内部犯行】**

- 日本D銀行のATMの保守管理業務を通じて不正にカード情報を再委託先の従業員が入手し、偽造カード作成していた
- 作成した偽造カードを利用して被害者の口座から現金を引き出していた

■ **国内E会社　【サイバー攻撃】**

- ポイントサービスにおいて、利用者以外の第三者による不正ログインがあり、ポイントが他社のギフト券に交換される被害が発生した
- 特典交換サービスを停止し、利用者に対してパスワードの変更を呼びかけた

■ **国内F会社　【サイバー攻撃】**

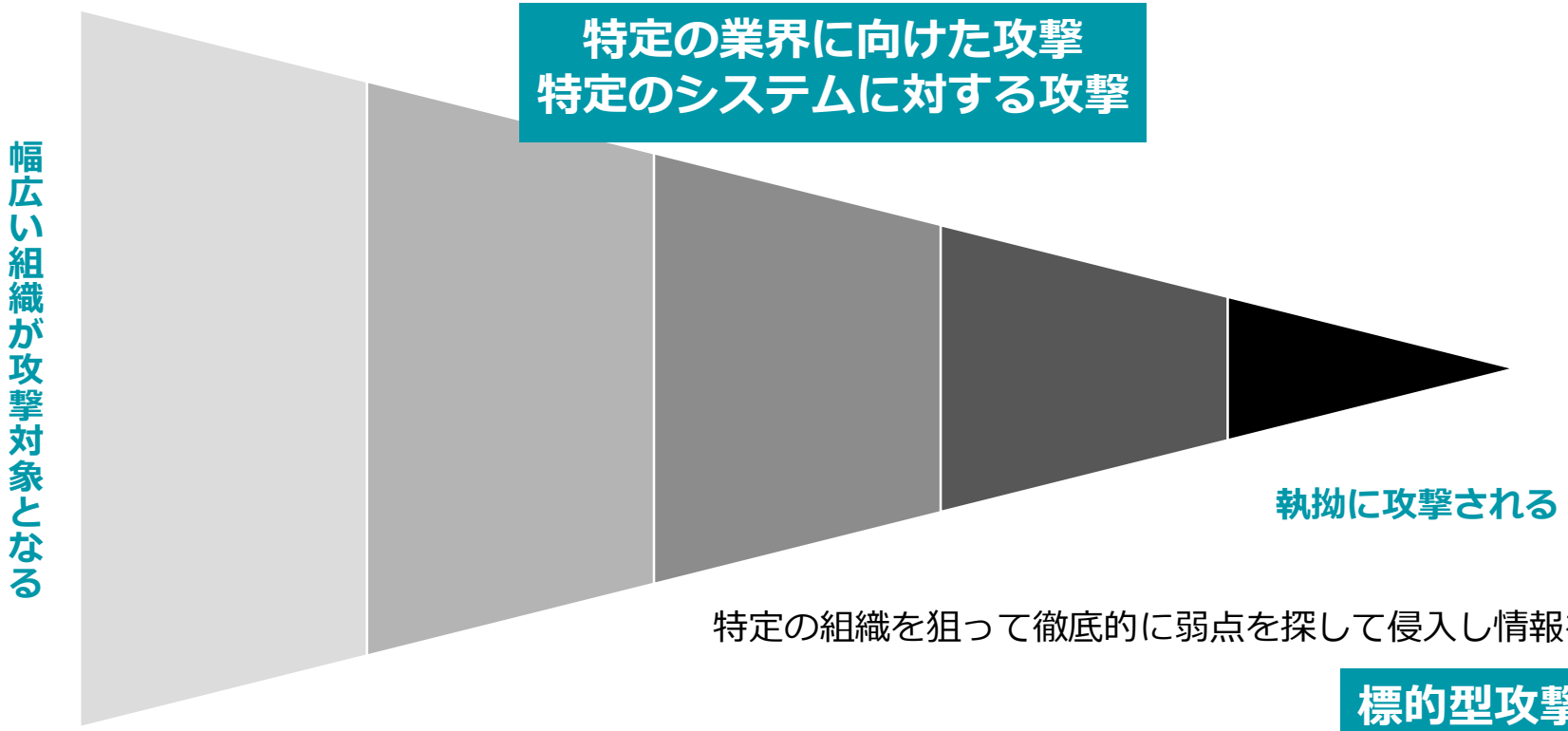
- IDと暗号化されたパスワード100万件以上が第三者に搾取された
- 利用者に対してパスワードの変更を呼びかけた

ニュースになっている標的型攻撃はほとんど標的型攻撃ではありません

無差別攻撃から標的型攻撃まで

無差別攻撃

多くの組織でできていない対策を狙った攻撃により情報を搾取等する



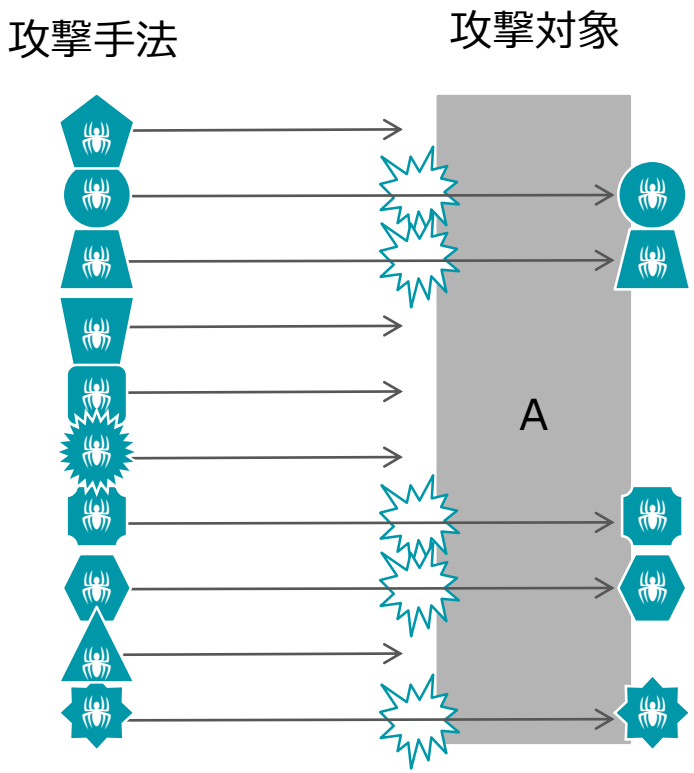
特定の組織を狙って徹底的に弱点を探して侵入し情報を搾取等する

標的型攻撃

狙われたら侵入されます

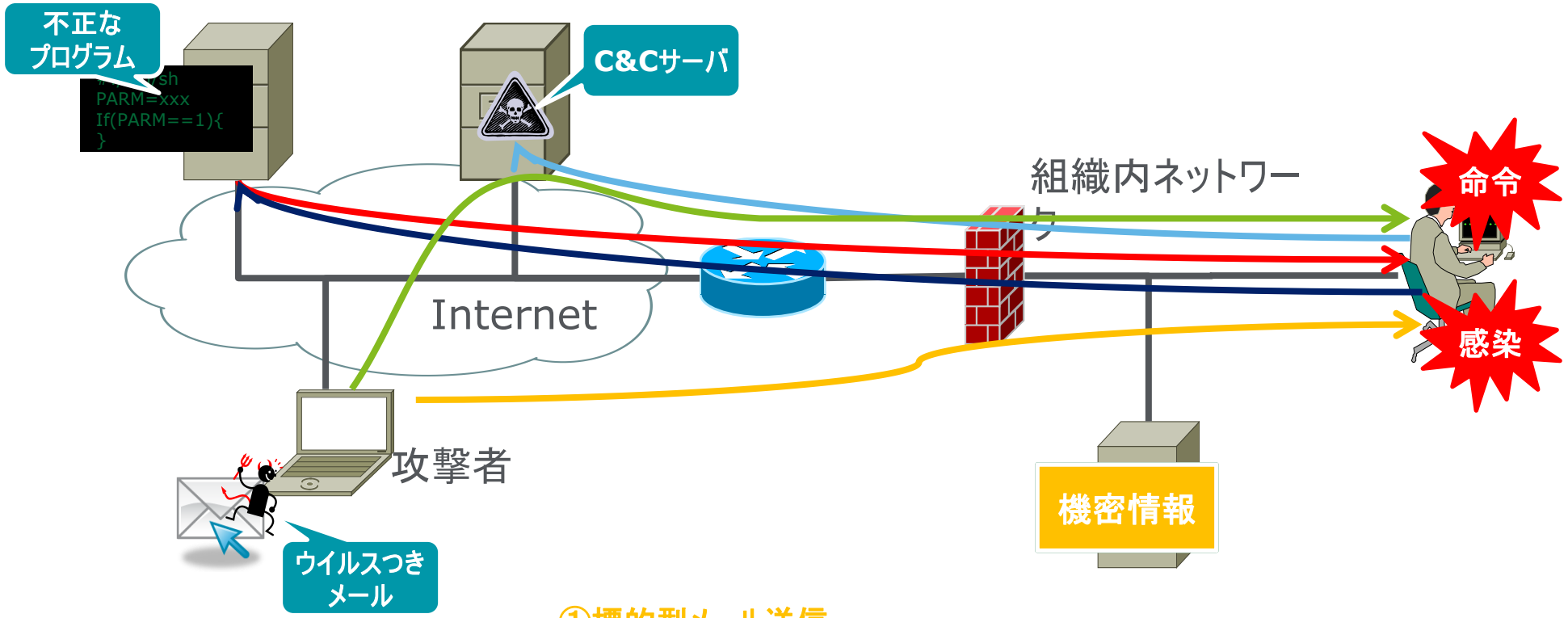
狙われたら最後？　標的型攻撃の恐怖

1. 未知の脆弱性をつく攻撃は常に存在します。
2. 人間の不注意はなくせません。
3. 狙われたら侵入を防ぐことは難しいと思ってください。



あらゆる手段を使って目的を達成しようとします

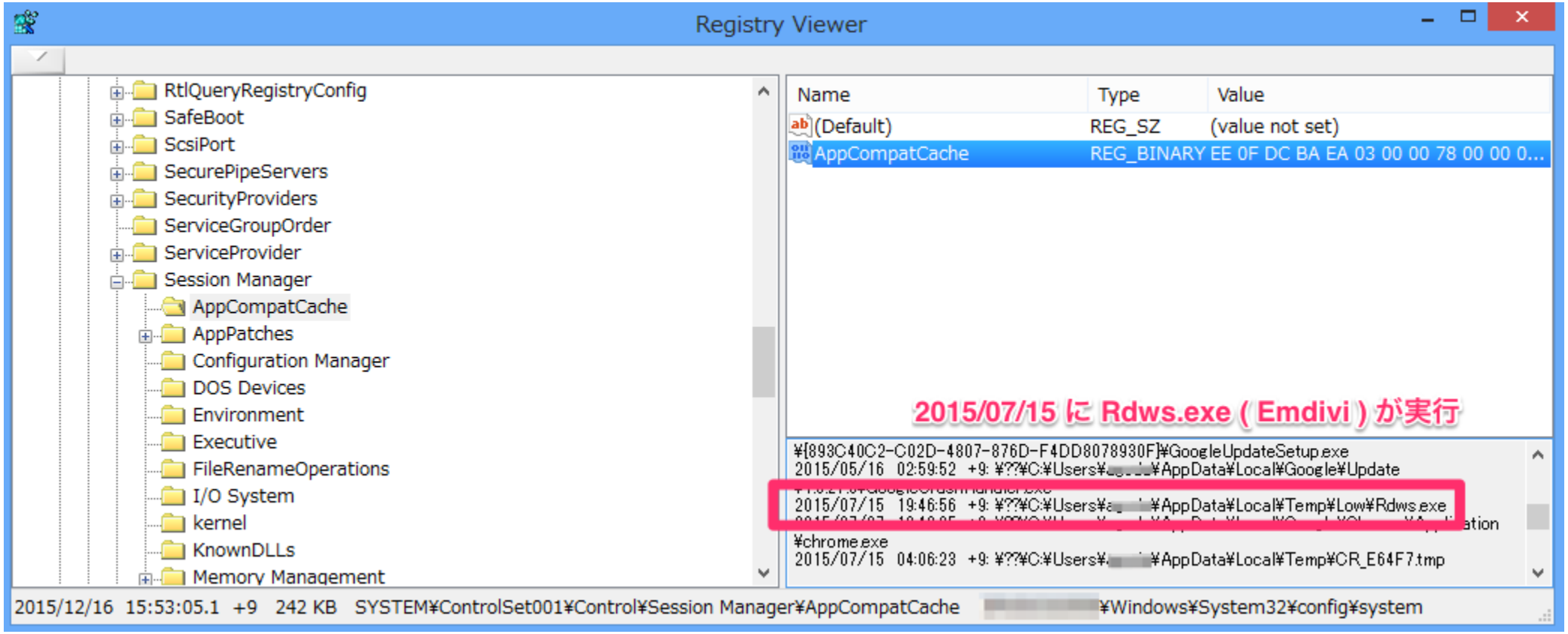
標的型攻撃による攻撃手法例



①標的型メール送信
②組織内で感染し更なる不正プログラムを要求
③不正プログラムをダウンロード
④C&Cサーバ等攻撃者の用意した外部サーバと接続
⑤外部サーバ経由で指令が送信される
⑥組織内の機密情報等が漏えいする

空白の時間（１）

侵害時の痕跡



空白の時間（2）

ウイルス対策ソフト対応時

OnAccessScanLog.txt

```
3319  2015/07/22  22:09:53  EXTRA.DAT の検出シグネチャ数 ..... =  なし
3320  2015/07/22  22:09:53  EXTRA.DAT の検出シグネチャ名 ..... =  なし
3321
3322  2015/07/23  22:26:09  エンジンのバージョン ..... = 5700.7163
3323  2015/07/23  22:26:09  AntiVirus  DAT バージョン ..... =  7870.0
3324  2015/07/23  22:26:09  EXTRA.DAT の検出シグネチャ数 ..
3325  2015/07/23  22:26:09  EXTRA.DAT の検出シグネチャ名 ..... =  なし
3326  2015/07/24  12:58:09  削除  NT AUTHORITY\SYSTEM C:\Windows\system32\wbem\wmiprvse.exe
      C:\Users\[redacted]\AppData\Local\Temp\Low\Rdws.exe Artemis!2345AE36972F (トロイの木馬)
3327
3328  2015/07/25  4:53:53  エンジンのバージョン ..... = 5700.7163
3329  2015/07/25  4:53:53  AntiVirus  DAT バージョン ..... =  7871.0
3330  2015/07/25  4:53:53  EXTRA.DAT の検出シグネチャ数 ..... =  なし
3331  2015/07/25  4:53:53  EXTRA.DAT の検出シグネチャ名 ..... =  なし
3332
3333  2015/07/26  0:49:52  エンジンのバージョン ..... = 5700.7163
3334  2015/07/26  0:49:52  AntiVirus  DAT バージョン ..... =  7872.0
3335  2015/07/26  0:49:52  EXTRA.DAT の検出シグネチャ数 ..... =  なし
3336  2015/07/26  0:49:52  EXTRA.DAT の検出シグネチャ名 ..... =  なし
3337
```

2015/07/24 にウイルス対策ソフトが対応

多くの企業はRansomwareの感染を経験している

ランサムウェアの脅威

感染PCからアクセスできるファイルが暗号化され、利用できなくなる。

要求された「身代金」を支払うことによる金銭的な被害が発生する。

https://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/ransomware/index.html

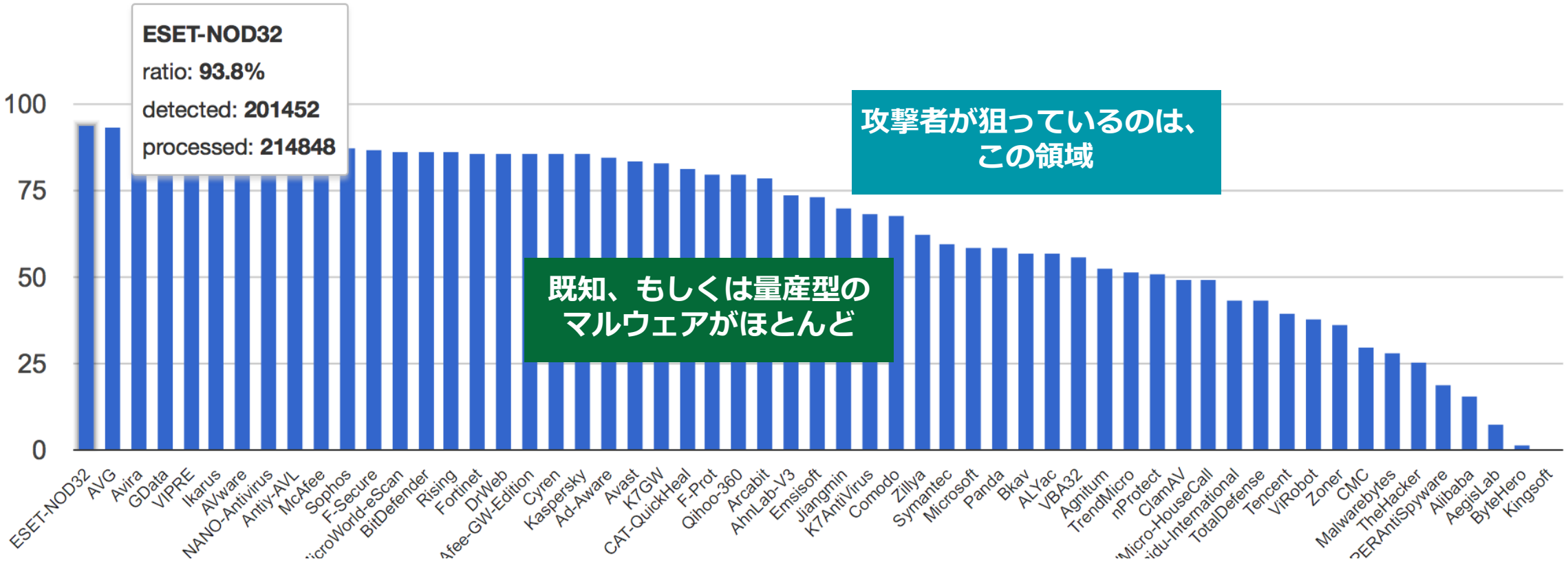
具体的な被害

- 大企業でも意外とランサムウェアに感染した経験がある。
- 多くの場合は、バックアップから復旧させることにより大事には至っていない。

ウイルス対策ソフトですべてを防げません

全てを未然には防げない

2016年12月のマルウェア検知状況 / Age 0～30日



※Virustotal.com の統計情報を集計

皆さまはどのような情報をどのようにもっていますか？

今後、重要なデータはますます増えていくと思います

Personal Data

Security Data

Credit Card Data

Location Data

Client Data

System Control Data

マイナンバーは様々なデータと連携する

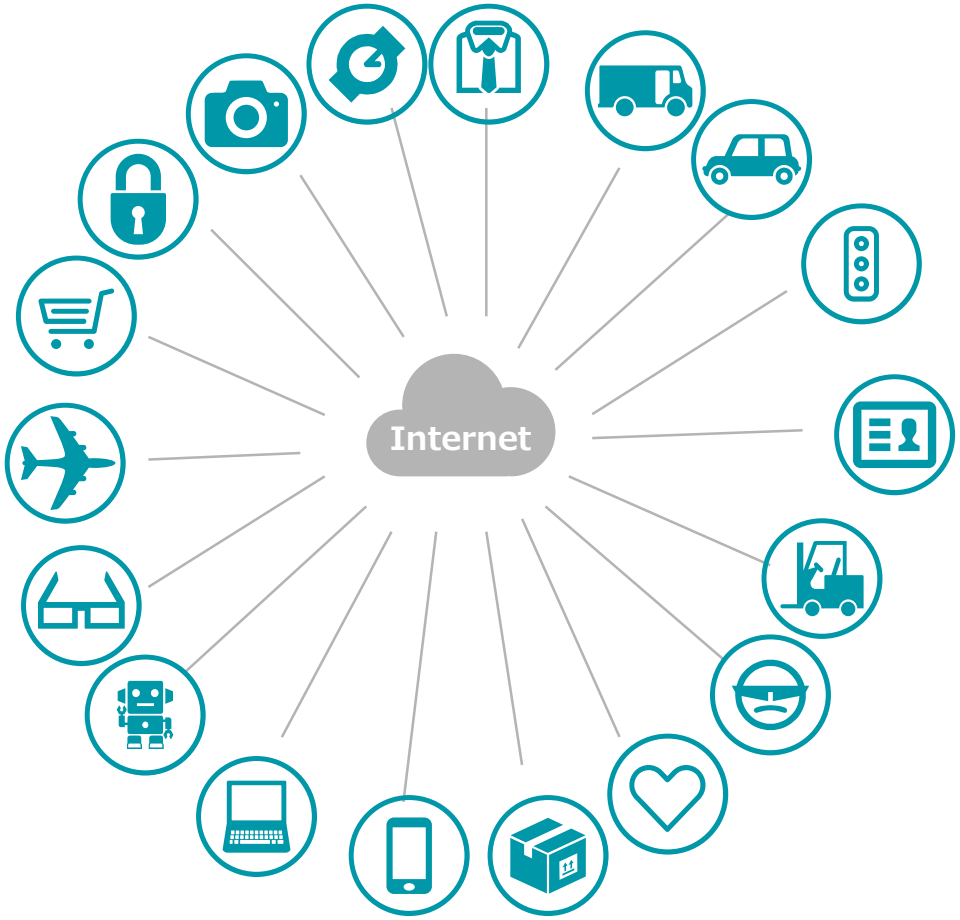
マイナンバー

マイナンバー制度

個人や企業にナンバーが付与され、
様々なデータと紐付けられることで
利便性が向上する
その半面、漏洩してしまった場合は、
事件・事故に巻き込まれたり
プライバシーが侵害されるリスクがある

つながるものはすべてが攻撃対象となる

Internet of Things



考えられるリスク

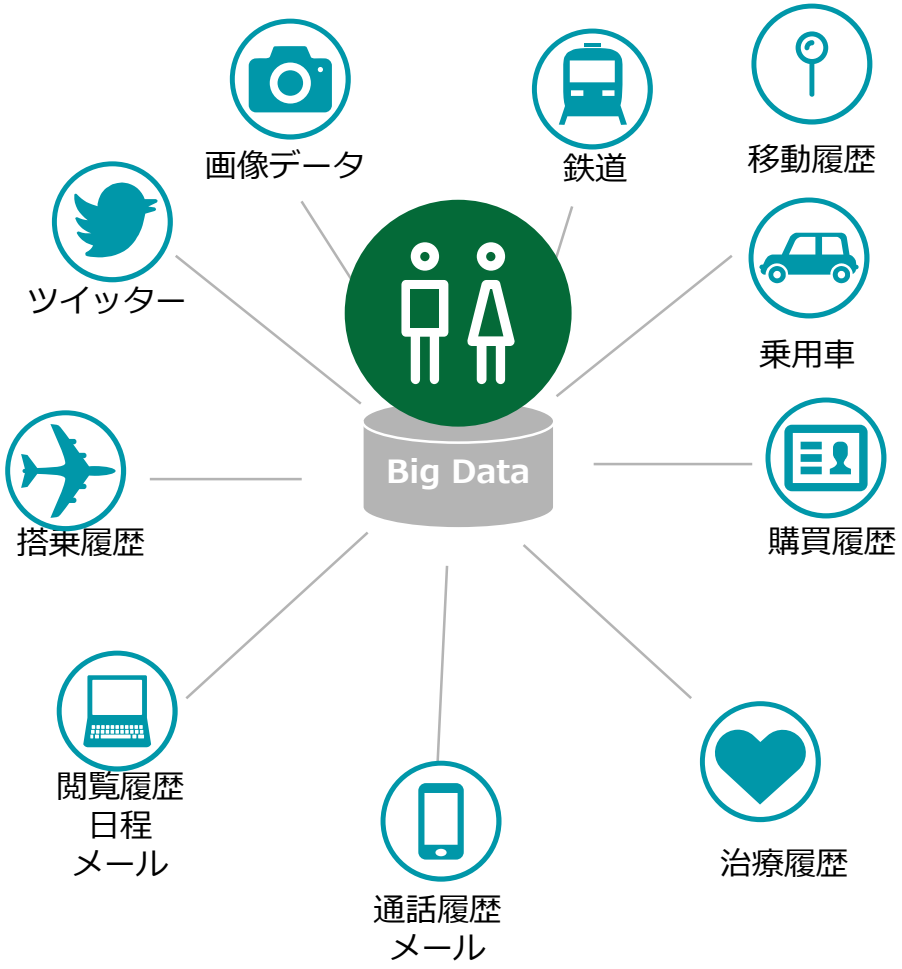
システム停止
誤作動
情報搾取

どこからでも
インターネットにつながっている「もの」に
攻撃ができる

それが直接狙われなくても
踏み台として利用されることもある

インターネット上で自らのプライバシーをどのように守るべきか？

Big Data



技術進歩

センサー技術の進歩
ストレージの容量の拡大
情報処理技術の進歩

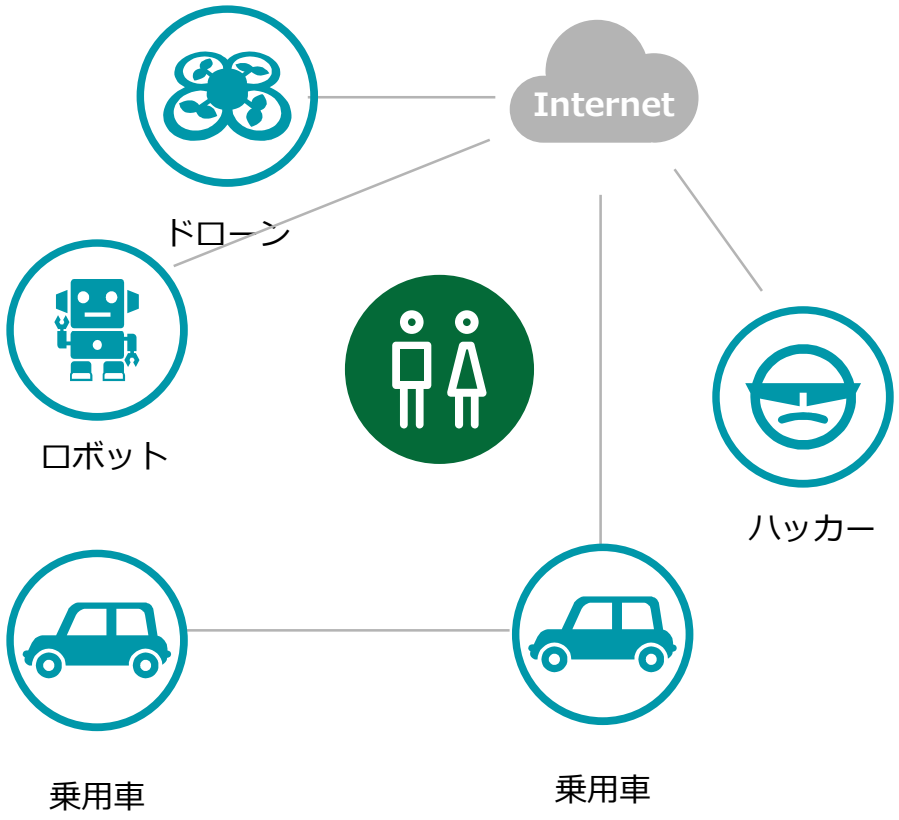
新たな付加価値が見出されるかもしれない。

プライバシー上の懸念

自分についての情報が蓄えられ、紐付けられ
想定もしていない人に
想定もしていない目的で
利用されているかも知れない

自律移動する機械と人間が物理的な空間を共有する

Autonomous control



従来の産業ロボットの安全管理

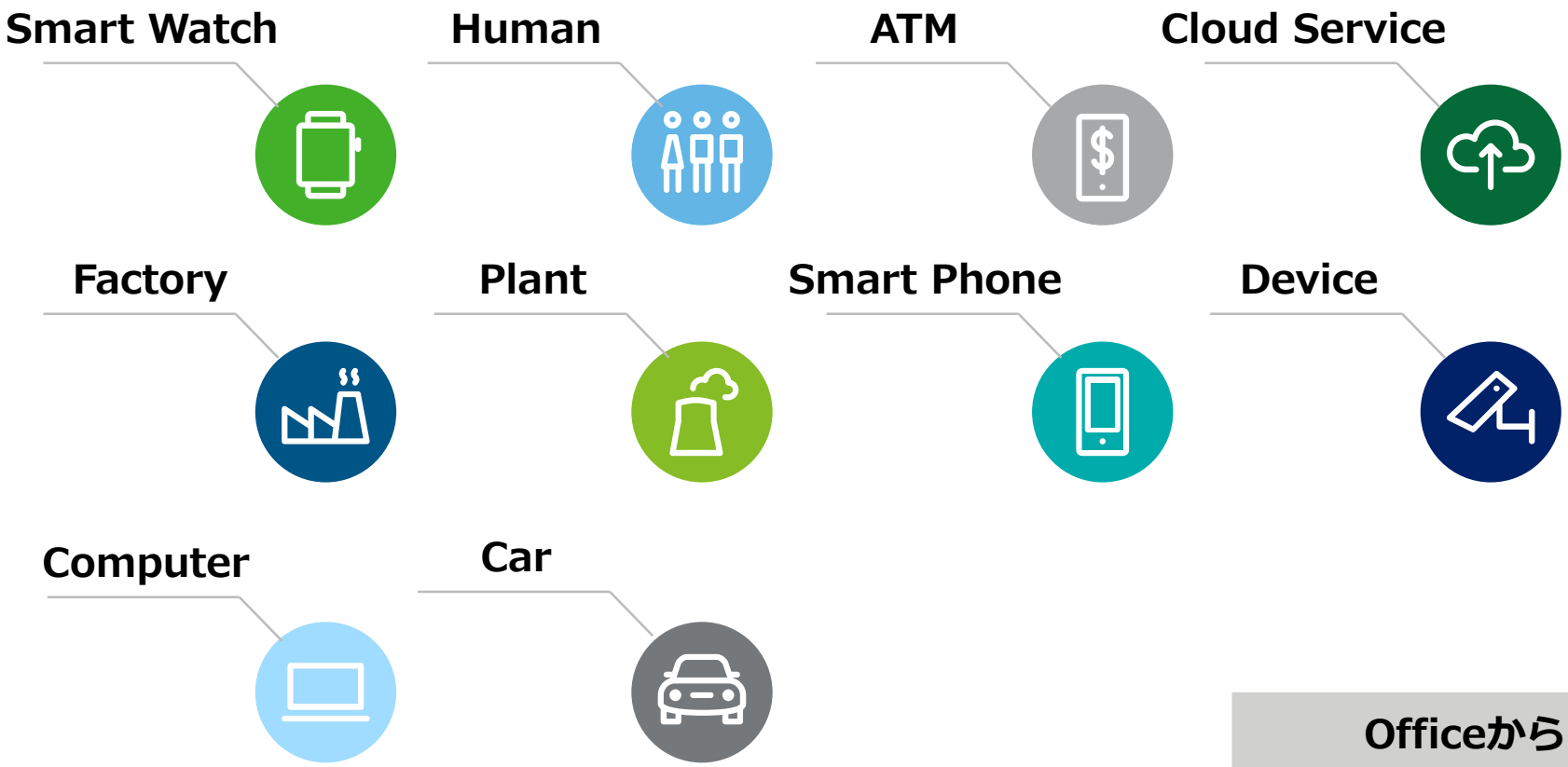
稼動部分への人の立ち入り制限

自立移動する機械の安全管理

？？？

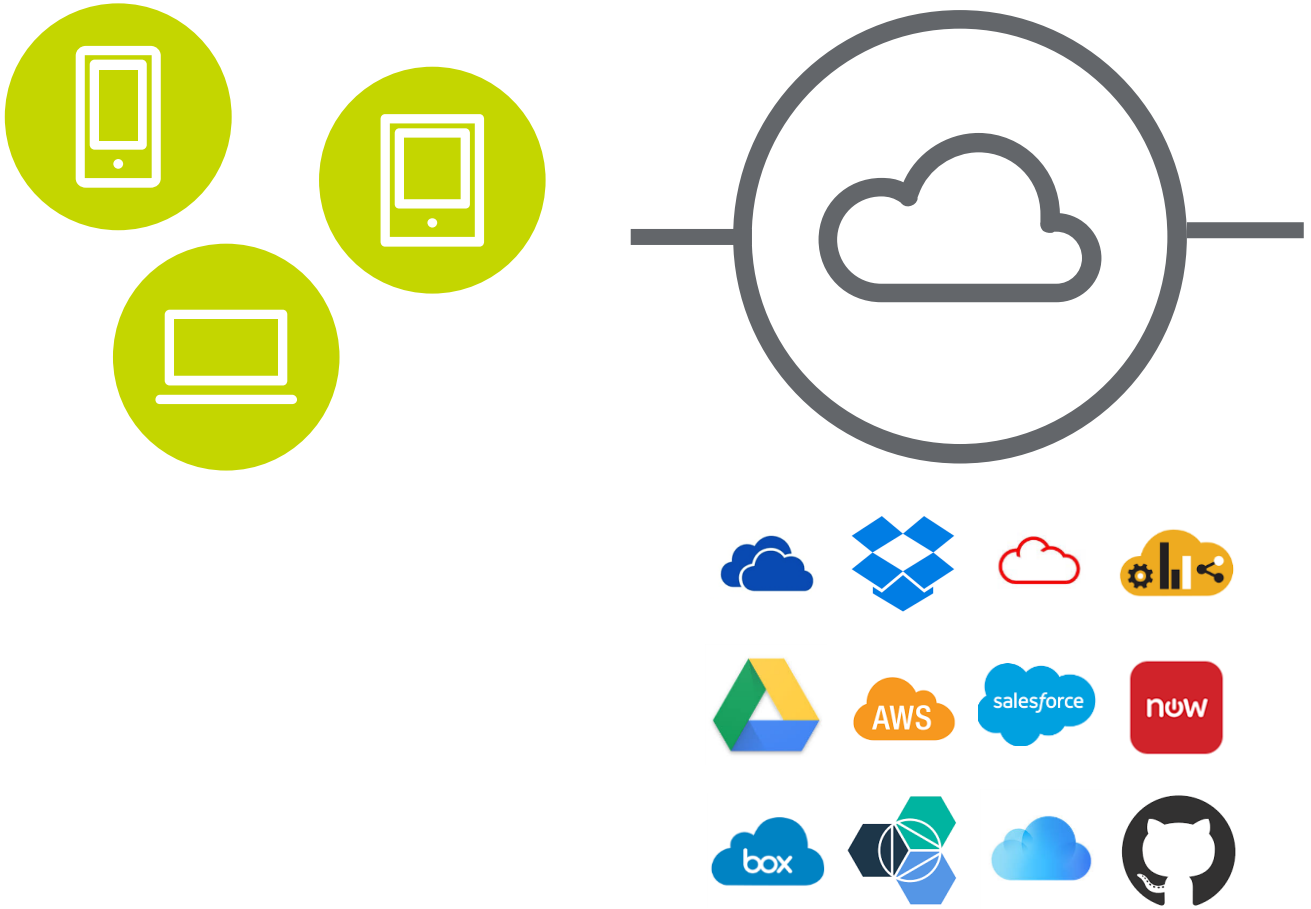
自律移動する機械と人間が物理的な空間を共有する

Securityの対象領域は広がっています



OfficeからDevice, Plantまで

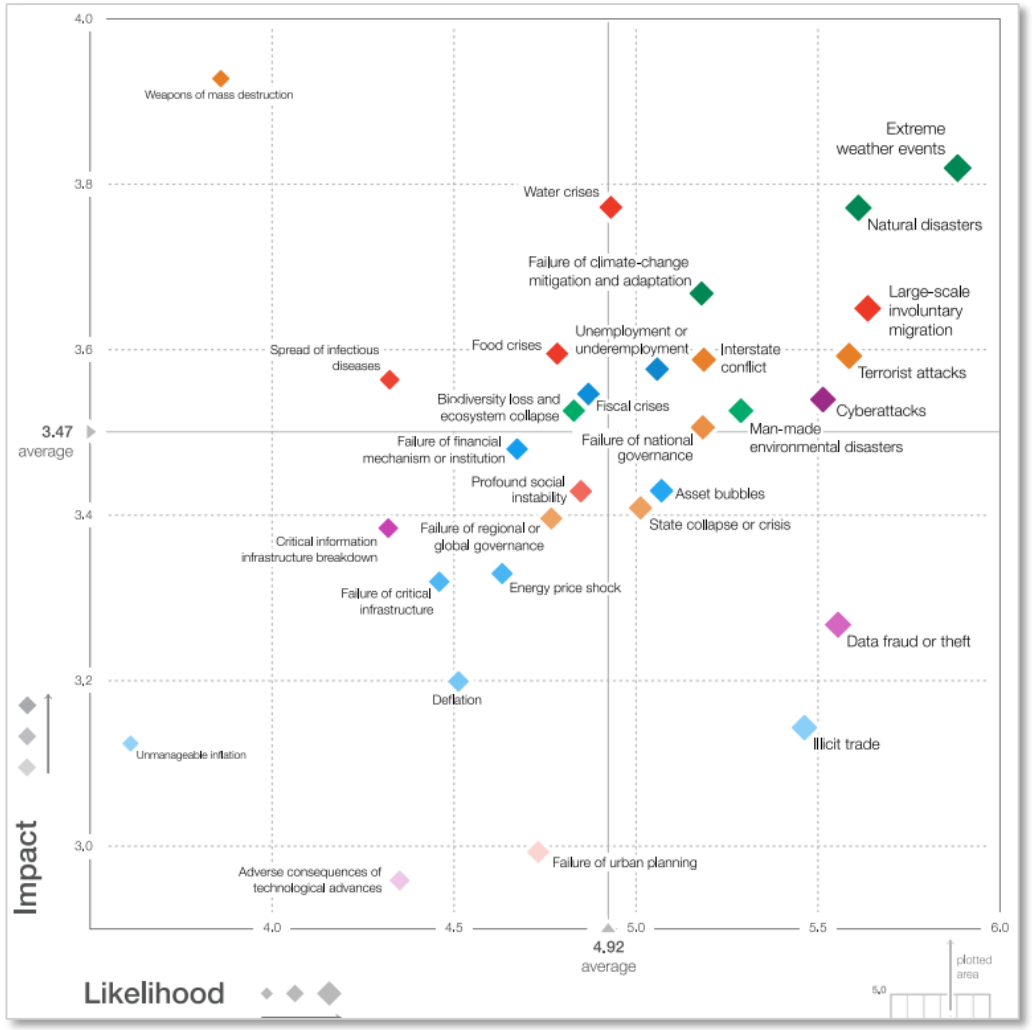
パブリック・クラウドの利用はさらに広がるでしょう。



- Mail
- Document
- Presentation
- Calculator
- Archive

どのように対応しましょうか？

サイバーセキュリティ対策はリスクマネジメントの一分野である



Extreme weather events

Water crisis

Natural disasters

Large-scale industrial migration

Large-scale industrial migration

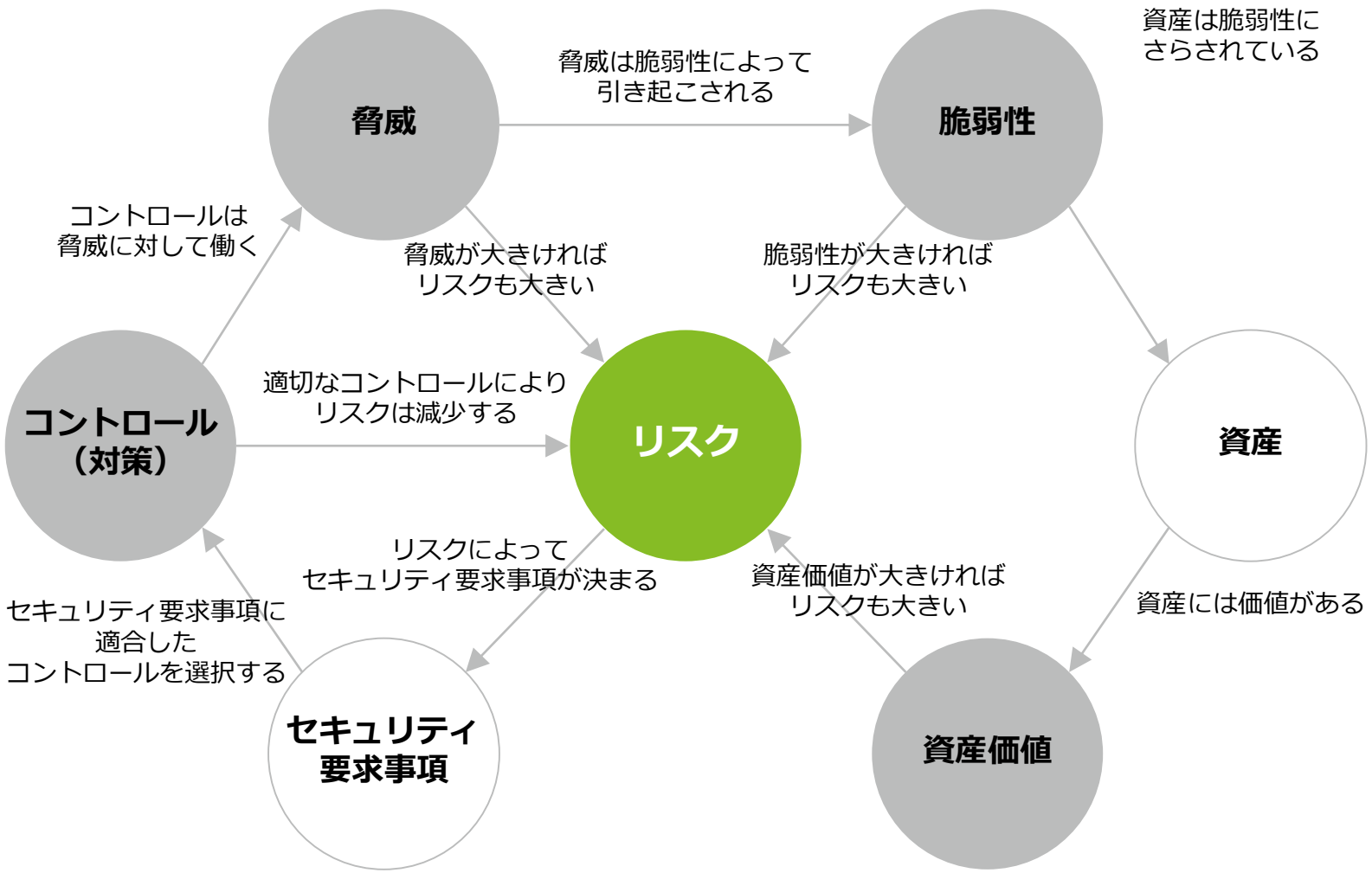
Cyber attacks

Data fraud or theft

World Economic Forum
The Global Risks Report 2017 12th Edition

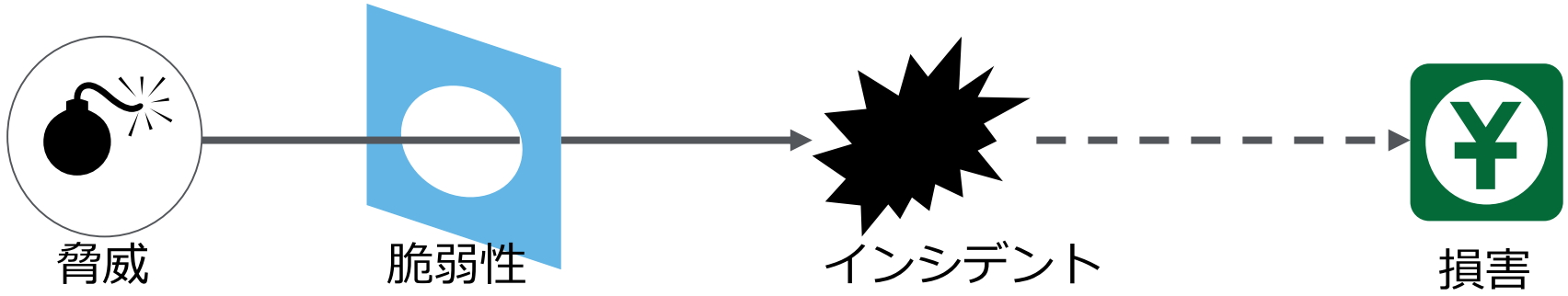
http://www3.weforum.org/docs/GRR17_Report_web.pdf

20年前の話を思い出してみましょう（えっ、学生だった？）



ISO/IEC TR 13335-3 1998　Guideline for the Management of IT Security

リスクマネジメントの考え方をもう一度思い出そう



予防的対策　　**発見的対策**

対策

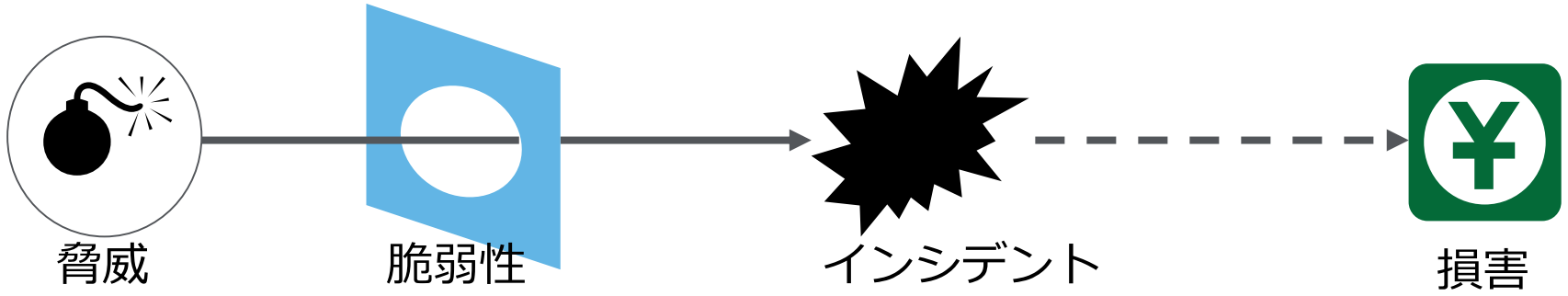
抑止	予防	検出	回復

主に**発生可能性**の低減　　**損害**の低減

最終的に損害をミニマム化するために

バランスを考慮した最適なセキュリティ対策が必要

身近なものにたとえてみよう

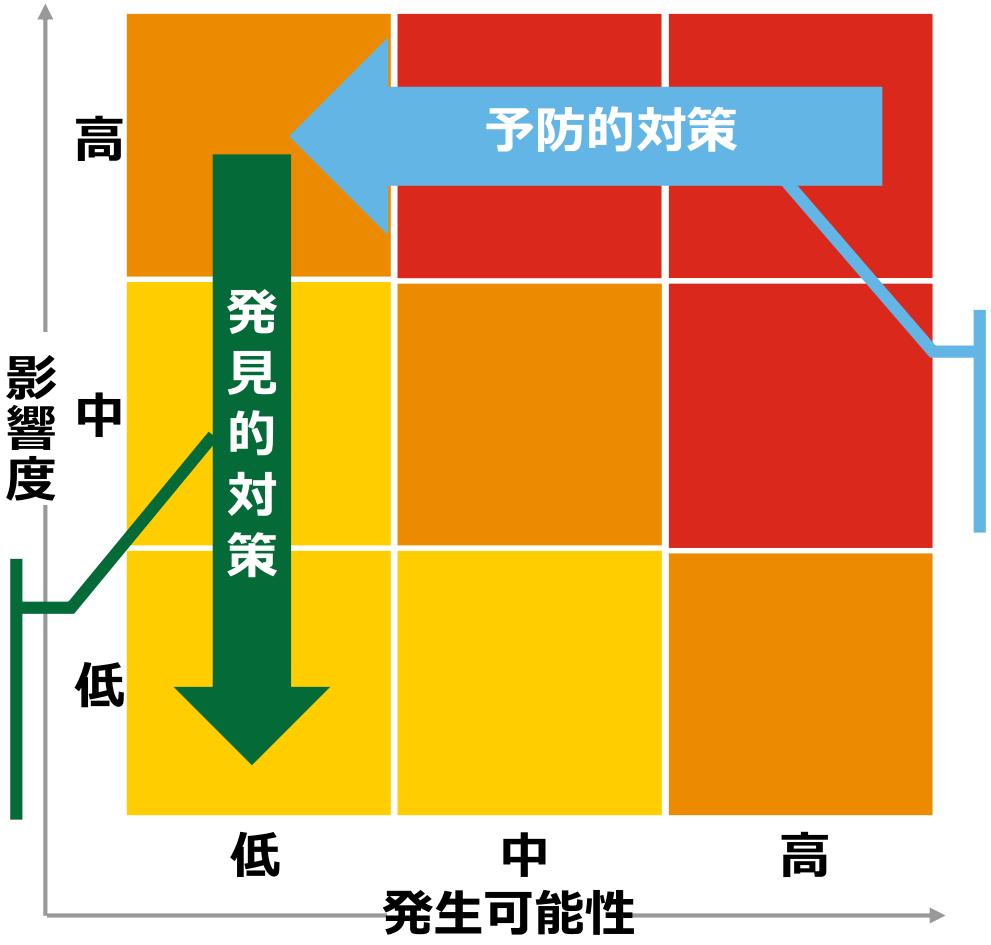


	脅威	脆弱性	インシデント		損害
	泥棒がいる	施錠をしていない窓	泥棒による住居侵入		現金の持ち出し
対策	抑止	予防	検出	回復	
	見回り活動	施錠	侵入警報機	駆けつけ警備	損害保険

最終的に損害をミニマム化するために

バランスを考慮した最適なセキュリティ対策が必要

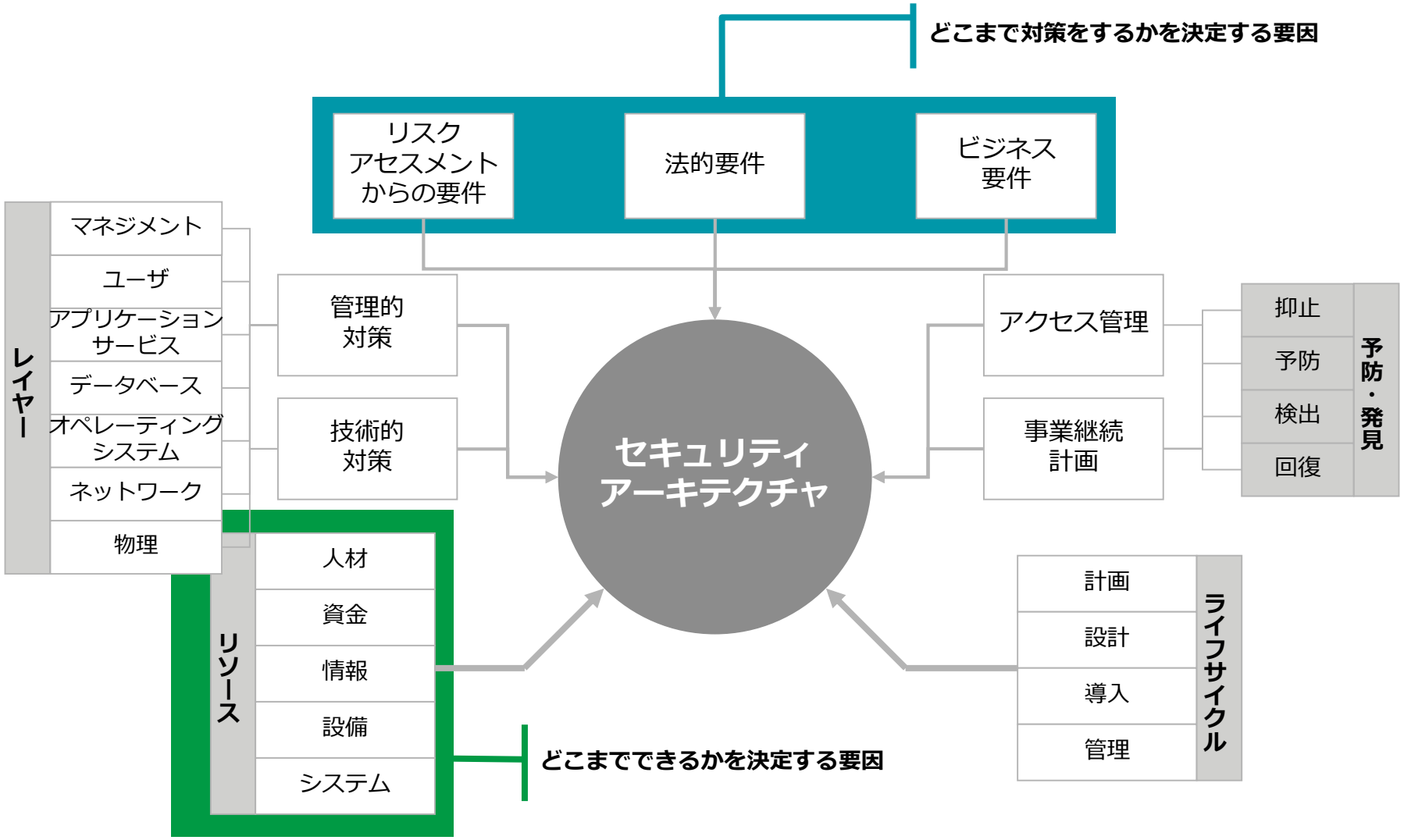
どういう場合に予防的対策を重視し、どういう場合に発見的対策を重視すればよいのか？



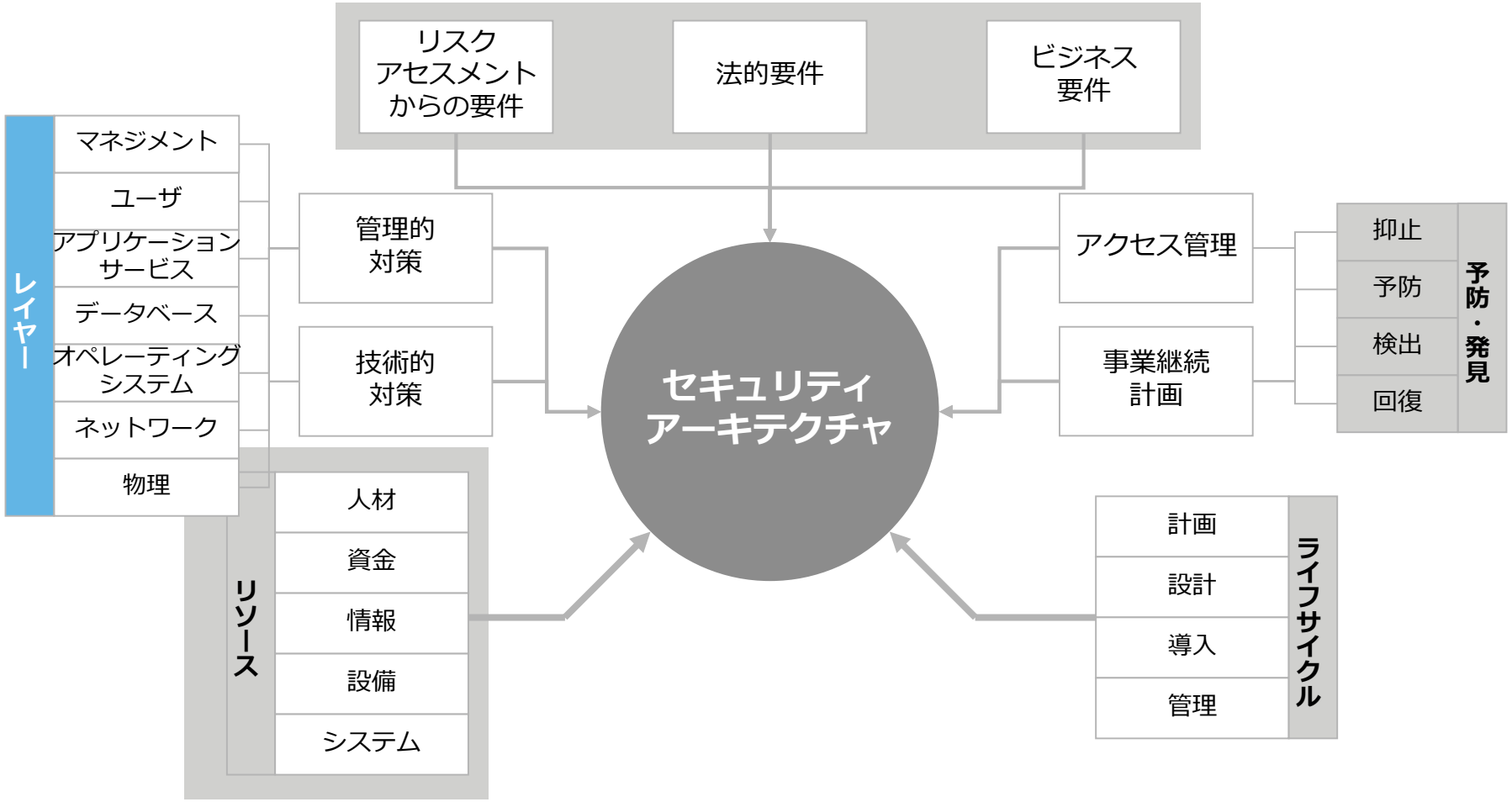
発生可能性が高いリスクについては、リスクが発現しないように、予防的な対策を重視すべきです。

リスクが発生した場合の影響度が大きいリスクについては、リスクが発現したとしても、影響が大きくならないように、早く発見し、対応するといった事後的な対策が重要となります。

どうやってセキュリティ対策を決めるかは簡単ではありませんが、考え方は昔からかわりません

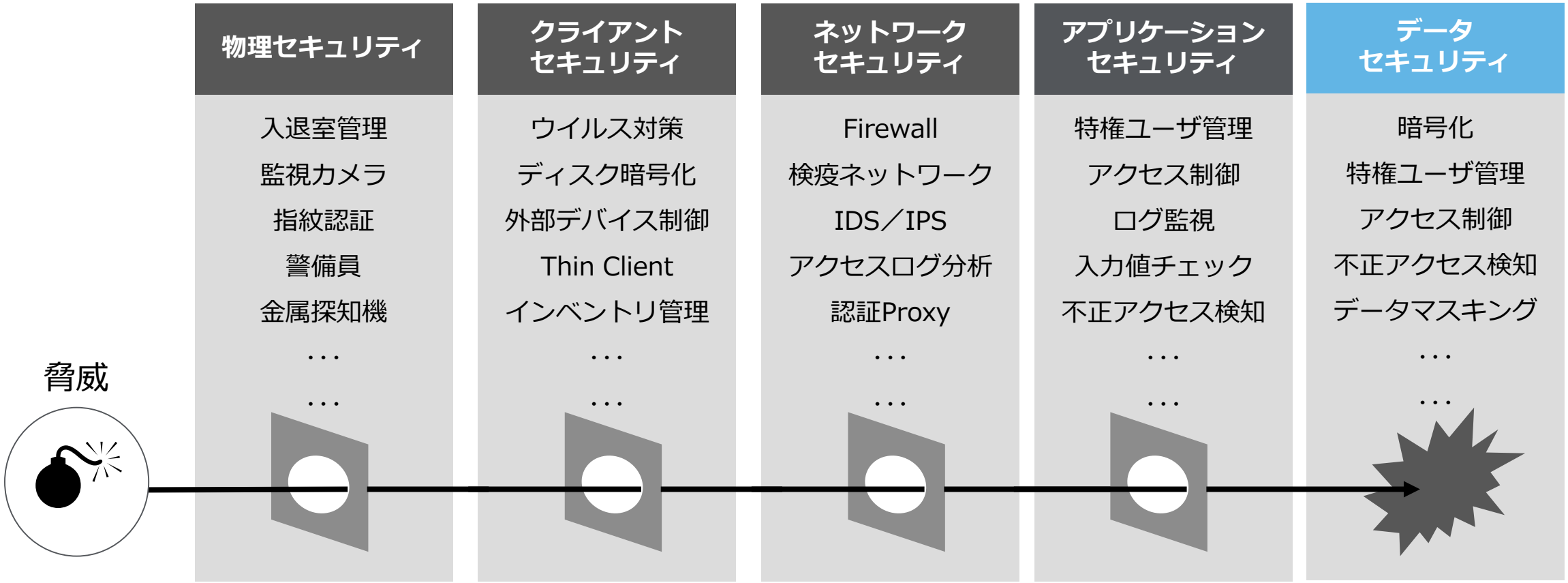


セキュリティ対策は多層的に考える必要があります



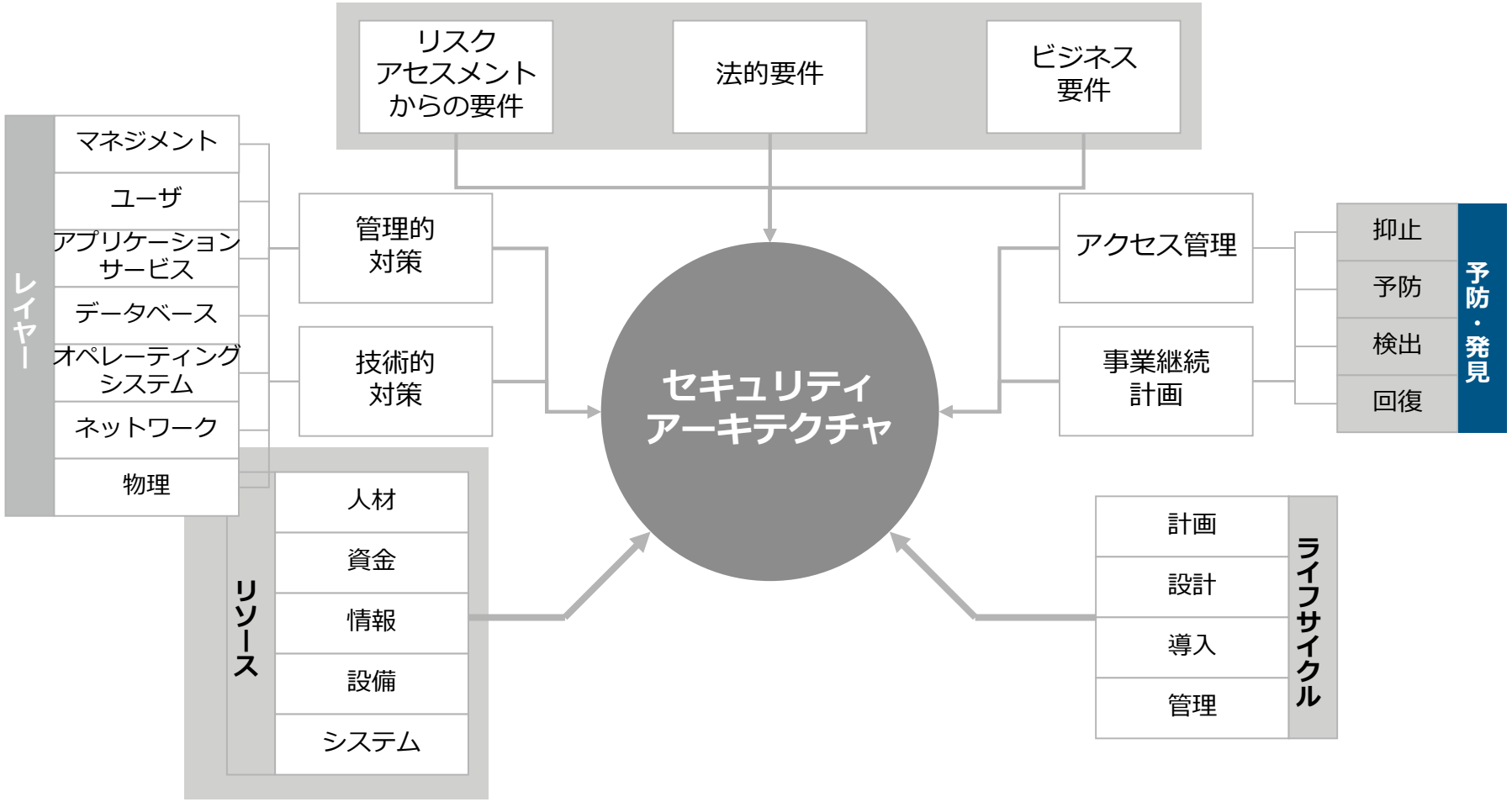
セキュリティ対策は多層的に考える必要があります

情報漏えいを考えた場合

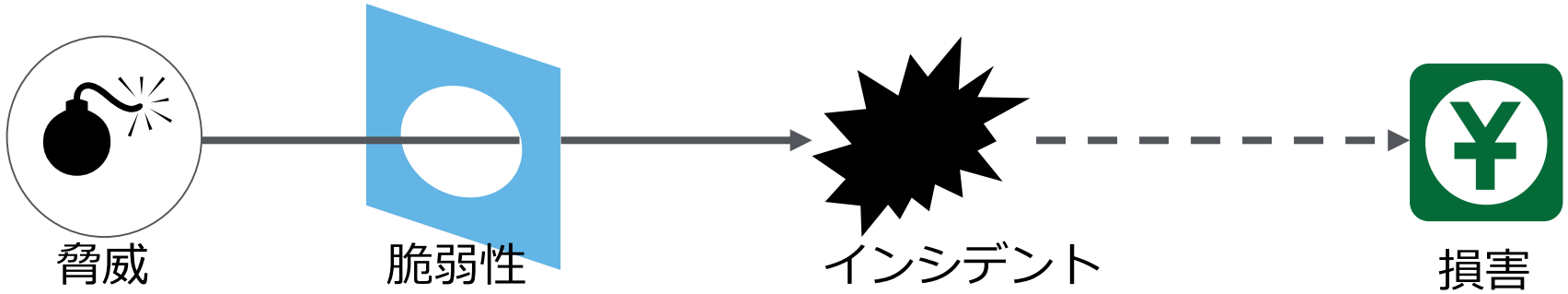


特定の製品の導入で解決する問題ではありません。

予防と発見に分けて考えるのはセキュリティ対策の考え方の王道です



予防と発見に分けて考えるのはセキュリティ対策の考え方の王道です



- Need to Know
- Least Privilege

- SOC

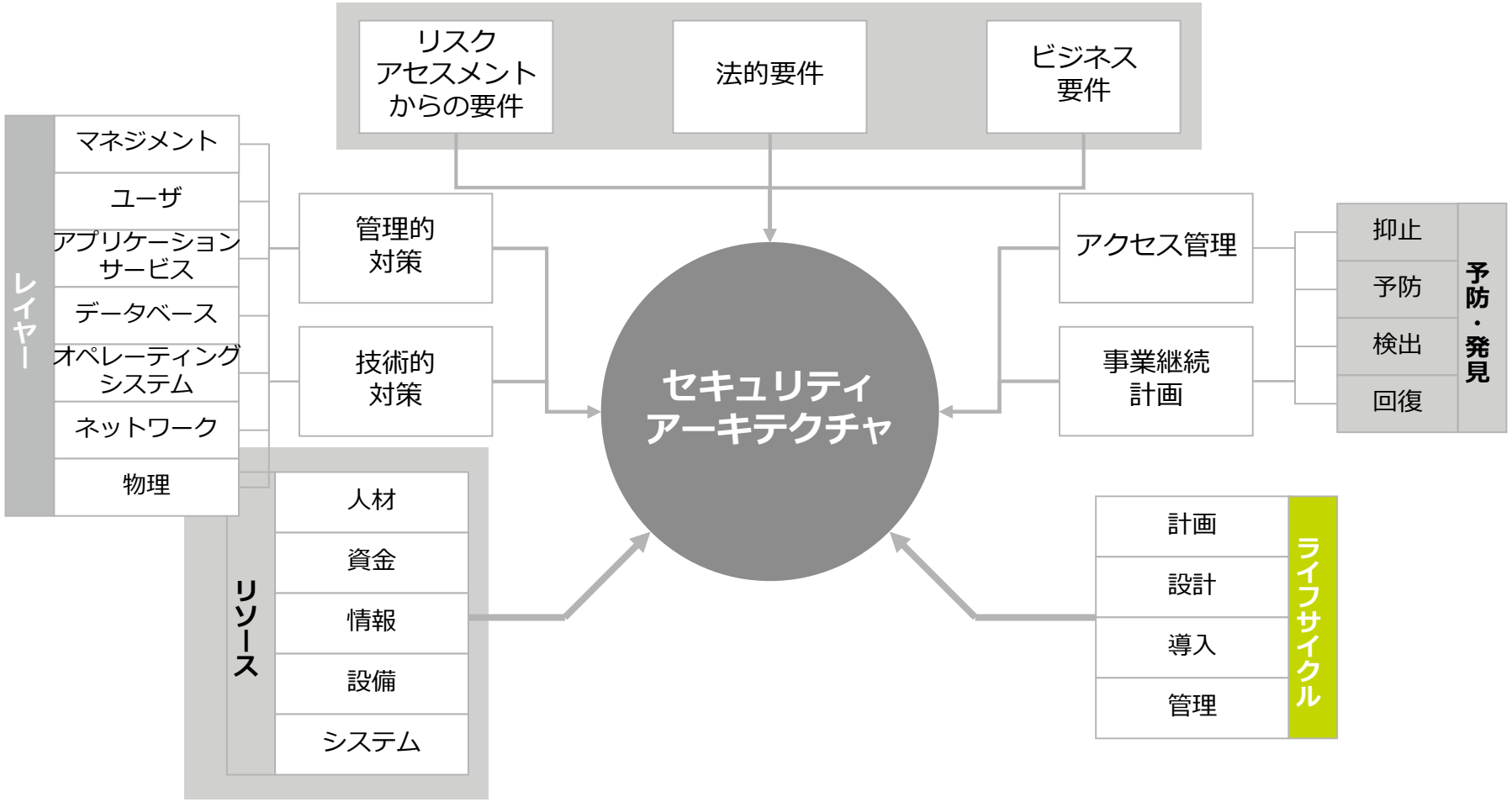
- CSIRT

予防的対策

- MFA

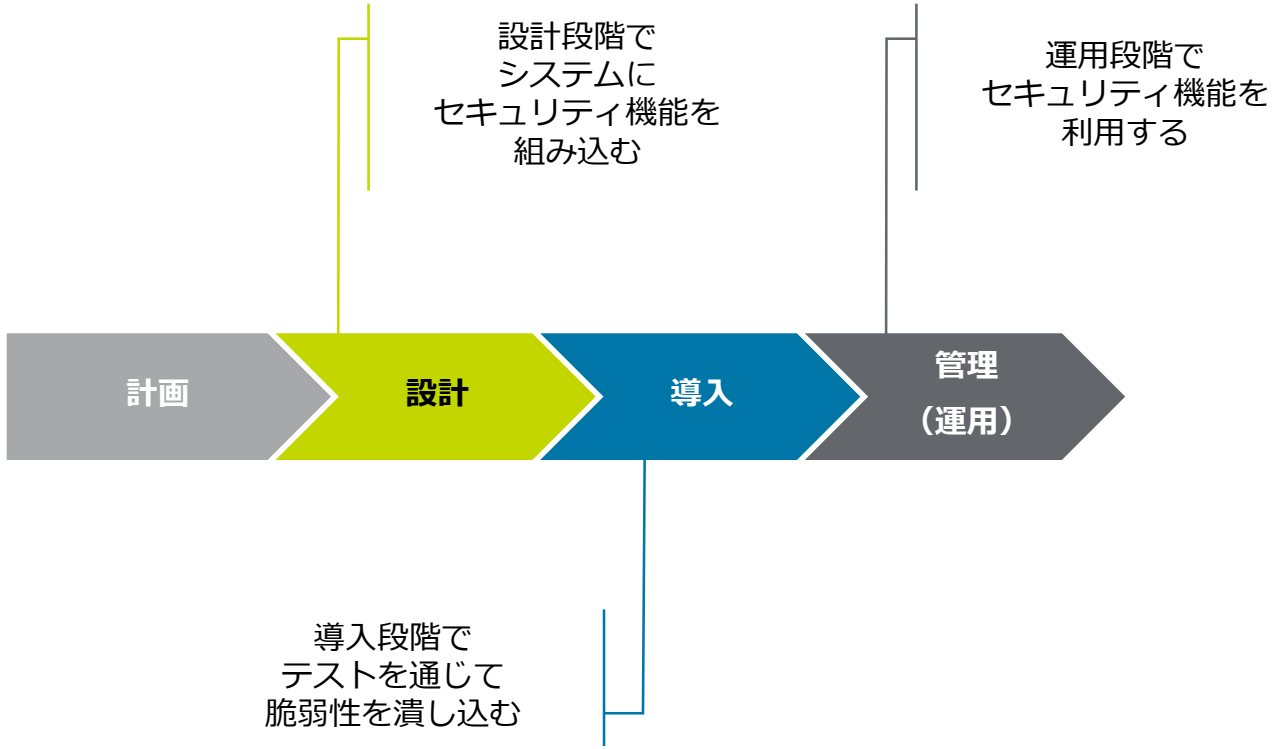
発見的対策

できる限り上流でリスクを減らすことが重要となります



できる限り上流でリスクを減らすことが重要となります

IoT時代はSecurity by Designの重要性が増します



ライフサイクル全体で考える必要があります。

運用に頼りがちであるが、上流で対策ができるのであれば、コストは下がります。

また工場や設備等の場合は、

連続稼働が前提で、仕様変更がオペレーションの品質に影響が及ぶ可能性が高いため、

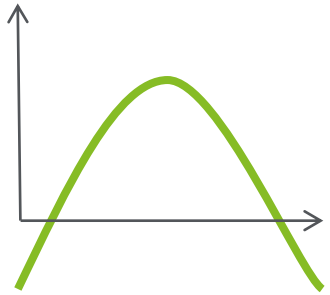
設計段階で必要なセキュリティ機能を実装し、

導入段階でテストを通じて脆弱性を潰し込み、

運用段階までに、セキュアなシステムを作り込むことの重要性が高まってきています。

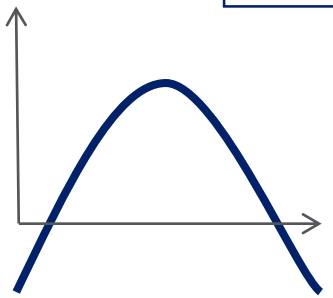
リスクとコスト、短期利益と長期利益を考える必要があります

理想的なセキュリティ対策にこだわり、業務効率が落ち、利益が増えないようでは本末転倒です。



情報セキュリティリスク　効率性

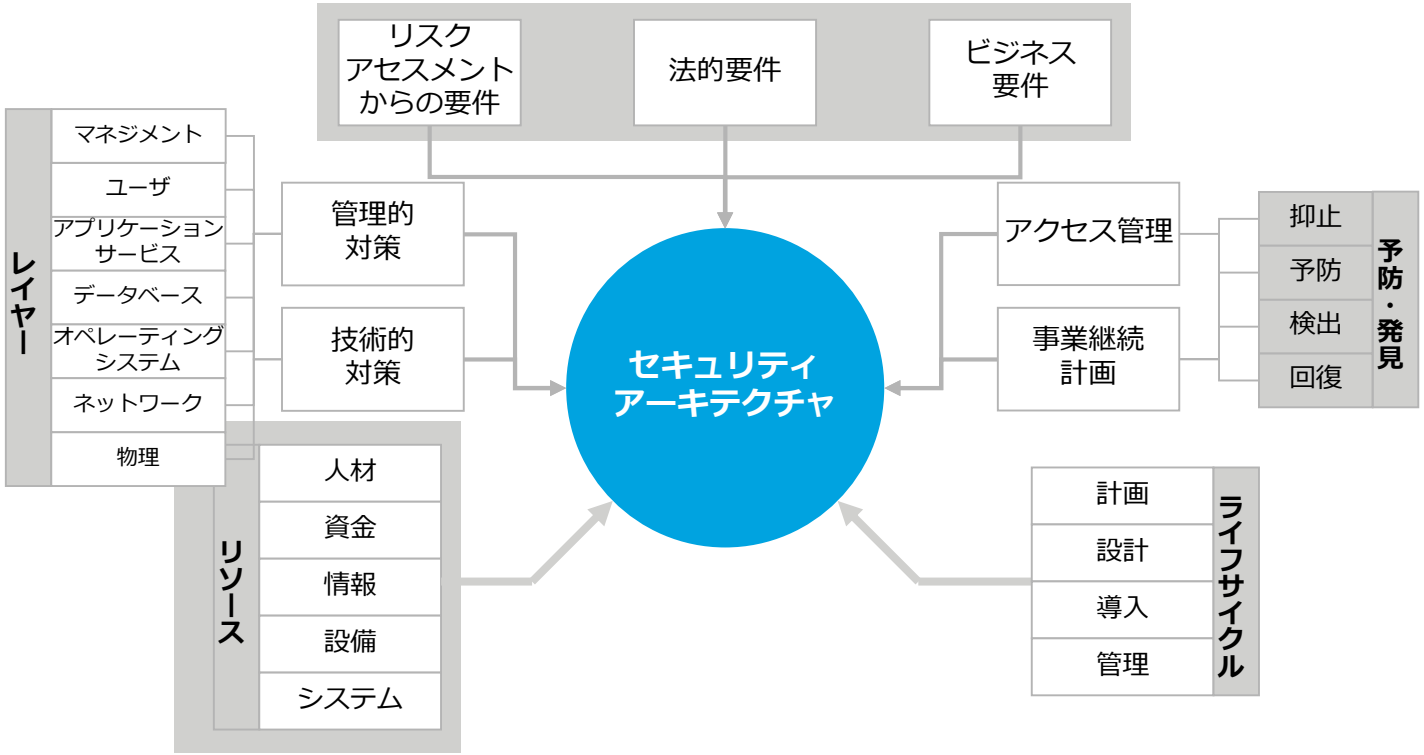
短期的な利益にこだわり、セキュリティ対策をおざなりにしていると、事故が起こった場合の損害は非常に大きくなることは、覚悟しておく必要があります。

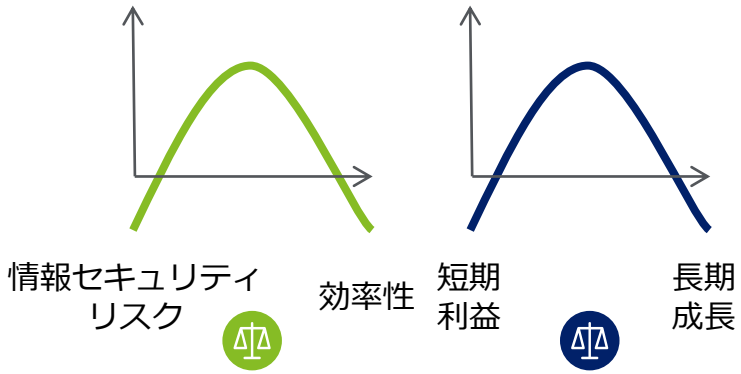


短期利益　長期成長

新しい技術の導入により、セキュリティ対策自体が効率化するのであれば、新しい技術は積極的に取り入れていくべきです。

セキュリティ対策の最適解の求め方は・・・

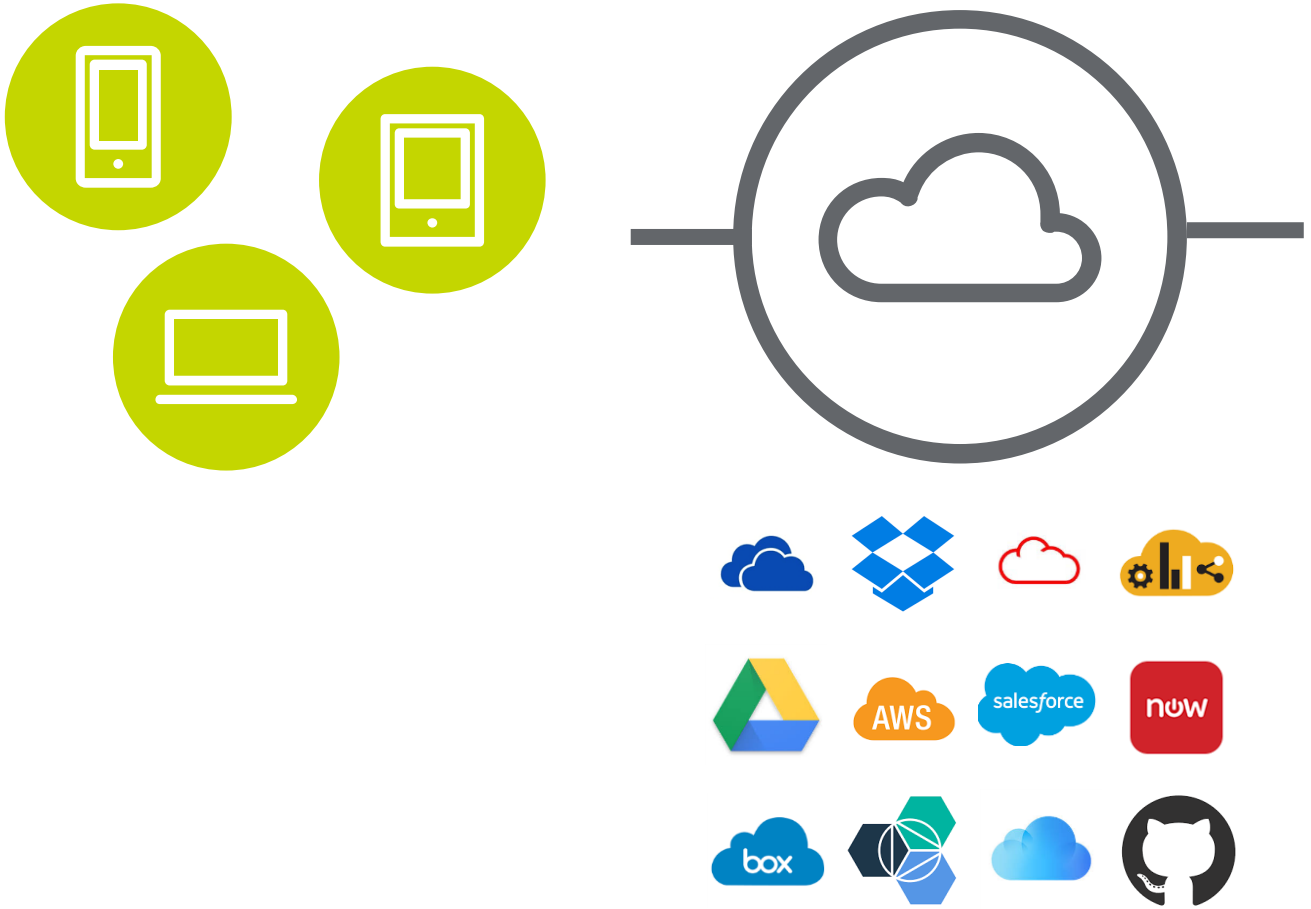




論理的に考えて、最後は芸術的に決める必要があります

中小企業は大企業ほどセキュリティ対策をする技術もお金もありませんが

クラウドの活用を考えましょう



- Mail
- Document
- Presentation
- Calculator
- Archive

具体的にはどのように手段がとれますか？

解決する技術も増えています

Endpoint Detection and Response

Endpoint Security with artificial intelligence

Data Diode

Cloud Access Security Broker

Computer Incident Response Team

Deception

Security Information and Event Management

Red Team Operation

Cyber Intelligence

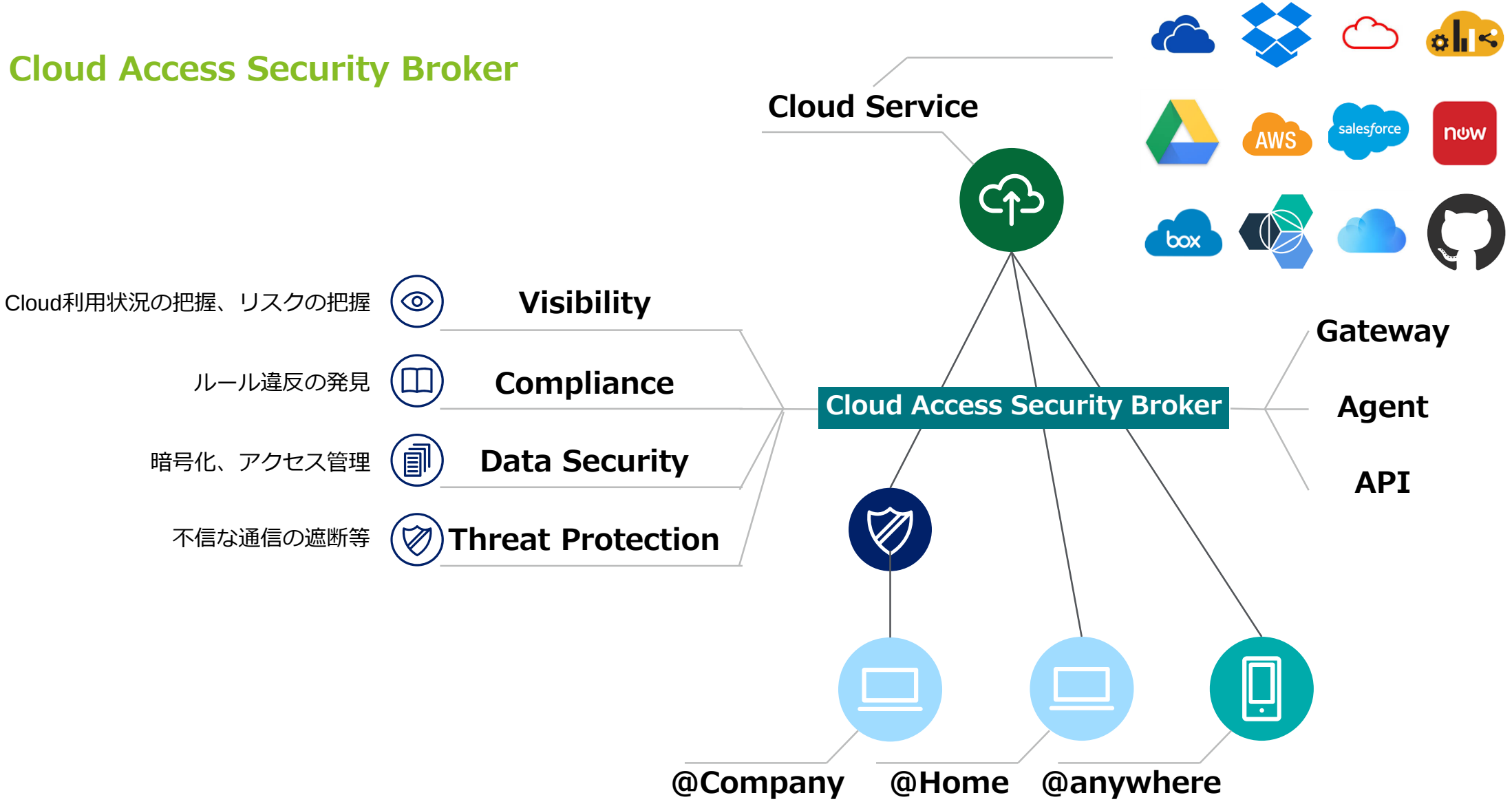
DevSecOps

Indicators of Compromise

User and Entity Behavior Analytics

クラウド利用時の新しいセキュリティ対策手法

Cloud Access Security Broker



まとめ

基本に戻ってよく考えてみよう

セキュリティの対象は増え、それを解決する技術も増えているが基本は同じです

Endpoint Detection and Response

Endpoint Security with artificial intelligence

Data Diode

Cloud Access Security Broker

Computer Incident Response Team

Deception

Security Information and Event Management

Red Team Operation

Cyber Intelligence

DevSecOps

Indicators of Compromise

User and Entity Behavior Analytics

システムが変わっても、新しいデバイスができても

リスク分析が重要

制御システム、自動車、スマートフォン、クラウドなどに対するセキュリティもリスク分析をすれば自ずからやるべき対策が見えてくるはずです。

セキュリティに対する新しい技術や概念に対しては

新しい技術や概念の積極的な活用を考えることが重要です。

セキュリティに対する新しい技術や概念は

- 新しい技術に対応をしているかもしれません
- 既存の技術よりも効率的に実施することが可能かもしれません

Endpoint Detection and Response

Endpoint Security with artificial intelligence

Data Diode

Cloud Access Security Broker

Computer Incident Response Team

Deception

Security Information and Event Management

Red Team Operation

Cyber Intelligence

DevSecOps

Indicators of Compromise

User and Entity Behavior Analytics

リスクにうまく対応できる組織が生き残ります

ビジネスの拡大には新しい技術の活用が不可欠です。

新しい技術の活用により、リスクもまた大きくなります。

そのリスクにうまく対応できるかどうかでビジネスが成功するかどうかがきまります。

チャレンジなき成功はない

ただ、チャレンジをするだけでは成功できない

リスクにうまく対応することが成功への道です

ご静聴ありがとうございました

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームであるデロイト トーマツ合同会社およびそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（ www.deloitte.com/jp ）をご覧ください。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクアドバイザリー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500®　の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

IS 669126 / ISO 27001

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited