「境界防御とゼロトラストネットワークってどういうこと？」

GSX
GLOBAL SECURITY EXPERTS

グローバルセキュリティエキスパート株式会社

常務取締役　西日本支社長

兵庫県警察サイバーセキュリティ対策アドバイザー

三木　剛

会社概要

- (株)ビジネスブレイン太田昭和を親会社として、サイバーセキュリティの黎明期に設立したサイバーセキュリティ専門企業
- 教育事業、コンサルティング事業、セキュリティソリューション事業、ITソリューション事業の4つの事業を展開

会社概要

会社名	グローバルセキュリティエキスパート株式会社
設立	2000年4月※1
代表者	代表取締役社長 青柳 史郎
資本金	541百万円　※23/6末
事業内容	情報セキュリティ・サイバーセキュリティの実装・運用支援をワンストップで提供する「コンサルティング事業」「ソリューション事業」と企業のセキュリティ水準向上を内面から支援する「教育事業」を展開
事業セグメント	サイバーセキュリティ事業（単一）
従業員数	144名　※23/6末
主要株主	(株)ビジネスブレイン太田昭和 兼松エレクトロニクス(株) (株)野村総合研究所

注釈 ※1：グローバルセキュリティエキスパートへの商号変更日を設立日として記載

役員一覧

代表取締役社長	青柳 史郎
代表取締役副社長	原　伸一
常務取締役	三木　剛
取締役	吉見　主税
取締役	中村　貴之
取締役	近藤　壮一
取締役	岡田　幸憲
取締役	上野　宣
取締役（監査等委員）	井上　純二
取締役（監査等委員）	古谷　伸太郎
取締役（監査等委員）	水谷　繁幸

加盟団体・資格

加盟団体	日本ネットワークセキュリティ協会（JNSA） 日本セキュリティオペレーション事業者協議会（ISOG-J） 情報セキュリティ教育事業者連絡会（ISEPA） 日本シーサート協議会（NCA） 金融情報システムセンター（FISC） 日本カード情報セキュリティ協議会（JCDSC） 情報セキュリティガバナンス協議会（ISGA） BCMSユーザーグループ（BCMSUG） 一般社団法人ソフトウェア協会（SAJ） 沖縄ITイノベーション戦略センター（ISCO） 日本CISO協会 日本コンピュータシステム販売店協会（JCSSA） サイバーセキュリティ人材キャリア支援協会（JTAG）
情報セキュリティマネジメント	認証基準：JIS Q 27001:2014(ISO/IEC 27001:2013) 認証登録番号：IS 71006
セキュリティサービス 基準適合サービスリスト登録	サービス登録番号：018-0029-10　情報セキュリティ監査サービス サービス登録番号：018-0029-20　タイガーチームサービス
システム監査/セキュリティ監査	システム監査企業台帳/情報セキュリティ監査企業台帳登録済
各種資格保有者	公認システム監査人 CIA CISA システム監査技術者 CISSP 情報セキュリティスペシャリストテクニカルエンジニア（IPA） 情報セキュリティアドミニストレータ米国公認会計士（CPA） 情報処理安全確保支援士 CEH（Certified Ethical Hacker） CND（Certified Network Defender） GICSP（Global Industrial Cyber Security Professional）

沿革

年月	概要	著名なサイバー犯罪史
1997年10月	・株式会社ギャブコンサルティングにて、タイガーチームサービス（侵入検査/模擬攻撃検査）の提供開始	
2000年４月	・株式会社ホスピタル・ブレイン昭和は、グローバルセキュリティエキスパート株式会社に商号変更	・東京ビューティセンター 3万人の情報インターネット流出
2005年12月	・情報セキュリティコンサルティング会社で最初のISO27001を取得	・Yahoo! BB 情報持ち出し 660万人の情報流用
2012年11月	・標的型メール訓練サービスの提供開始	・日本年金機構 不正アクセス 個人情報 約125万件流出
2016年５月	・EC-Councilセキュリティエンジニア養成講座の提供開始	
2017年８月	・Mina Secureの提供開始	・大阪大学 不正アクセス 8.1万件の個人情報流出
2017年８月	・兼松エレクトロニクス株式会社との資本業務提携	・Google+ 不正アクセス 50万件の個人情報流出
2018年11月	・企業と情報セキュリティ人材のマッチングサービス vCISOの提供開始 ・西日本支社の設置	・東京トヨタ 不正アクセス 310万件の個人情報流出
2019年10月	・西日本支社名古屋オフィスの開設	・ユニクロ gu不正アクセス 46万件の個人情報流出
2019年11月	・株式会社ＥＰコンサルティングサービス（ビジネスブレイン太田昭和グループ）から一部事業（ＩＴソリューション事業）を譲受ける	・7Pay設計ミス、不正アクセス サービス開始直後に廃止
2020年４月	・セキュリスト（SecuriST)® の提供開始	・三菱電機 不正アクセス 防衛情報、取引先口座の流出
2020年11月	・株式会社野村総合研究所との資本提携	・カプコン 不正アクセス 身代金要求型ウイルス感染
2020年12月		・ホンダ 不正アクセス 海外工場操業停止

事業ドメイン

コンサルティング事業

✓マネジメントコンサルティング

ポリシー体制整備、リスクアセスメント、CSIRT整備等

✓テクニカルコンサルティング

脆弱性診断(プラットフォーム/Webアプリ/設計書)

ペネトレーションテスト等

教育事業

✓企業向けセキュリティ訓練

標的型攻撃メール訓練、e-ラーニング、インシデント対応訓練

✓ セキュリティ教育講座

国際認定資格、GSXオリジナル

日本全国の企業の
セキュリティレベル向上を
支援する
4つの事業ドメイン
を展開

ITソリューション事業※

✓ITインフラ構築

✓バイリンガルSESサービス等

※事業譲受により2021/3期から開始

セキュリティ
ソリューション事業

✓セキュリティ製品の導入

SSE、SEG、EDR、SIEM、UEBA、WAF等

✓運用サービス

MDR、緊急対応サービス等

2つのビジネス

GSX
GLOBAL SECURITY EXPERTS

準大手・中堅・中小企業（エンドユーザ）

GSXの提供価値

セキュリティリスク対策に関するワンストップサービス

セキュリティ対策に必要な要素を
フルラインナップに備え、
ちょうど良いスペックで提供し
セキュリティノウハウを伝授

サービス内容

- 従業員教育
  セキュリティ人材育成
- 脆弱性診断
- 緊急対応
- コンサルティング
  (対策状況可視化)
- サイバーソリューション
  導入・運用と人材提供

IT企業・SIer

GSXの提供価値

セキュリティ教育・資格制度で
セキュリティ人材を育成

100万人以上いるIT人材に対し
セキュリティ教育を提供し
プラス・セキュリティ人材を創出

サービス内容

当社オリジナル SecuriST

- **国内発** 認定脆弱性診断士
- セキュアなWeb
  アプリケーション設計士
- ゼロトラストコーディネーター

EC-Council

- 国際的に著名なホワイトハッカー
  養成講座

CISSP

- 国際的に著名な情報セキュリティ
  マネジメント講座

実績一覧

脆弱性診断

20年に渡る業歴
3,000件以上
の診断実績
(業界を問わず)

標的型メール訓練サービス

年間約5,000組織
への実施実績
(業界を問わず)

セキュリティ監査

2,000件以上
の実施実績
(業界を問わず)

教育関連

中央省庁・独立行政法人・製造業
医療・エンタメを中心に、
実績多数

標的型攻撃対策ソリューション

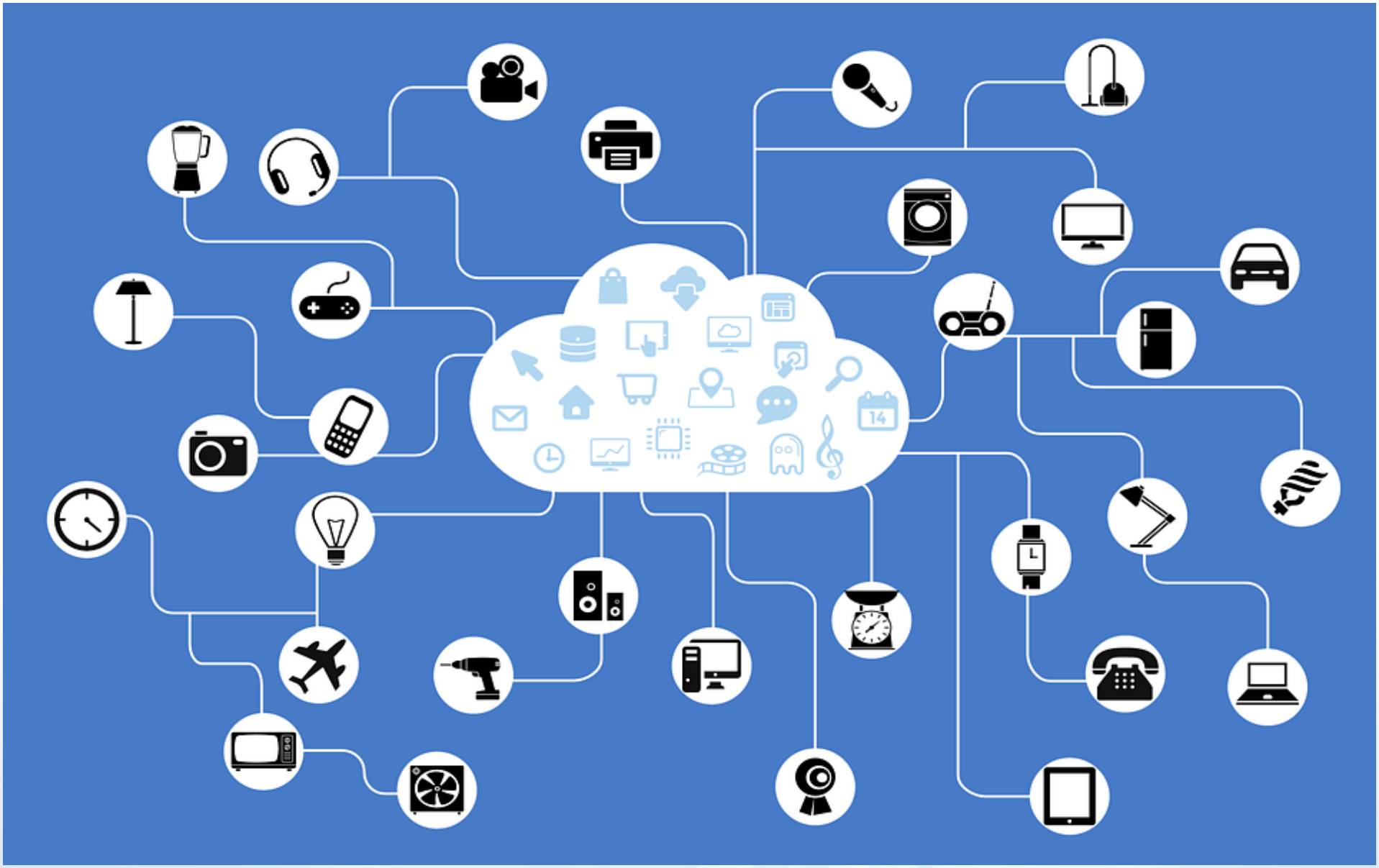
証券・保険・消費者金融・
製造業・エンタメ・独法・メディア
・防衛・人材・会計・Sierなどを
中心にサンドボックス・SIEMの導入

CSIRT関連

証券・カード・消費者金融・
石油・Sier・医療・電力・
スーパーゼネコン・製造業

インターネットの脅威

あらゆるモノと繋がるインターネット(IoT)



攻撃の目的と方法が変化してきている

愉快犯
自己顕示,見せしめ,嫌がらせなどが目的

目立つ攻撃
すぐに攻撃に気づき,対策を講じることができる

攻撃手法の巧妙化

目立たない攻撃
攻撃の発覚が遅れるため,被害の拡大長期化

2000年 → 2005年 → 2010年以降

KPMG/BT Taking the offensive: Disrupting Cyber Crime 2016
平成26年度 サイバー空間における脅威の情勢について

企業状況の変化

- **企業が急速にITの利活用**を始めた
- その結果、**価値のあるデータが散在**するようになった
- **テレワーク**で端末の管理が緩くなった

ネット環境とシステムが急拡大し、価値あるデータが散在

DXデジタルトランスフォーメーション

業務効率化
情報集約化
意思決定の迅速化
新規ビジネス創出

インターネットの相互接続

価値あるデータがクラウドへ

入出力端末の増加（出入口の増加）

犯人像の変化

- 攻撃手法や手口が一般化：犯罪インフラの発展
- **サイバー攻撃を「犯罪者」が金銭目的で行う**

サイバー犯罪の犯人達も、様々な立場、思惑があるが・・・

GSX
GLOBAL SECURITY EXPERTS

金銭目的

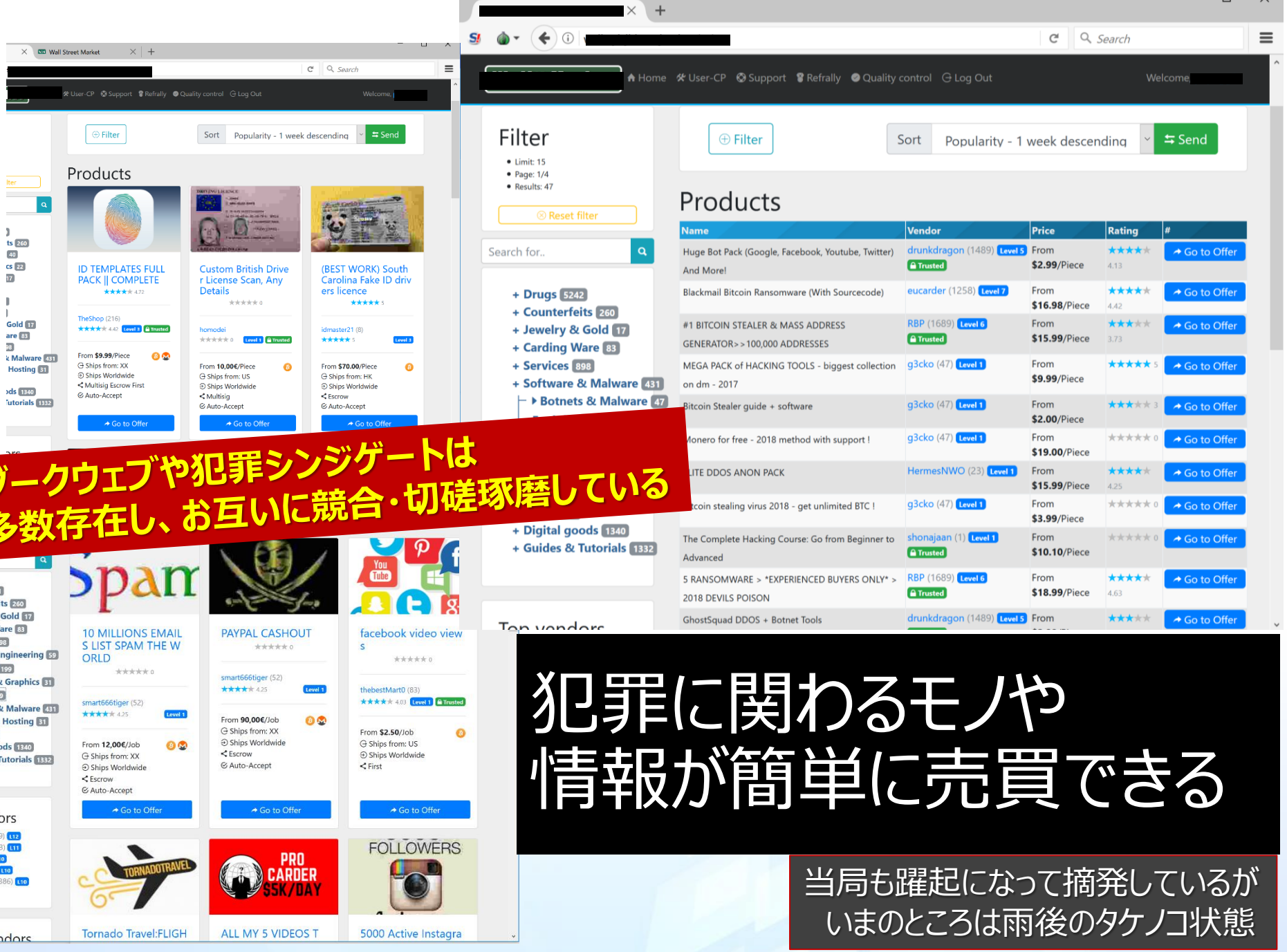
儲かる市場だと理解
組織化・**分業化**が進み
ブラックマーケットが成立

国営スパイ

ハクティビスト

アノニマスで有名

テロ/破壊活動



ダークウェブや犯罪シンジゲートは
多数存在し、お互いに競合・切磋琢磨している

犯罪に関わるモノや情報が簡単に売買できる

当局も躍起になって摘発しているが
いまのところは雨後のタケノコ状態

【実例】最新のマルウェアがワンクリックで購入できる

GSX
GLOBAL SECURITY EXPERTS

BROWSE CATEGORIES

Fraud	28434
Drugs & Chemicals	153543
Guides & Tutorials	10828
Counterfeit Items	5765
Digital Products	13065
Jewels & Gold	1250
Weapons	2402
Carded Items	2718
Services	5990
Other Listings	2735
Software & Malware	2178
Botnets & Malware	693
Botnets & Malware	693
Exploits	261
Exploit Kits	145
Security Software	473
Other	476

Search Results [Save Search]

★★ FREE ★ Blackshades 5.5.1 + Crack with SQL database ★ 2016 update ★★
Item # 42601 - Botnets & Malware / Botnets & Malware - Creatine.exe (6231)

Views: 29964 / **Bids:** Fixed price
Quantity left: Unlimited

Buy price
USD 0.00
(0.0000 BTC)

BlackShades RAT 5.5.1 + User Guide
Item # 22902 - Botnets & Malware / Botnets & Malware - shonajaan (11953)

Views: 32009 / **Bids:** Fixed price
Quantity left: Unlimited (5110 automatic items)

Buy price
USD 1.10
(0.0017 BTC)

[MS] [Account Stealer Pack] [Crack Pack] [%100 Working] Booters ~ Phishers ~ Cracking Tools [2016] + FREE GIFT
Item # 207268 - Botnets & Malware / Botnets & Malware - BestSales (9352)

Views: 2490 / **Bids:** Fixed price
Quantity left: Unlimited (1407 automatic items)

Buy price
USD 5.00
(0.0079 BTC)

サイバー犯罪の
サブスク化
（RaaS）
既に乱立状態

Comparative table of the information download speed of the attacked company							
Testing was made on the computer with a speed of Internet of 1 gigabit per second							
Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	**83,46 MB/s**	**Yes**	**Yes**	**Yes**	**1M 59S**	**19M 58S**	**1D 9H 16M 57S**
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

Only you decide during communication how much the encrypted company will pay you. You get the payment to your personal ewallets in any currency, after which you transfer us the percentage of the foreclosure amount.

LockBit 2.0 does not function in post-Soviet countries.

We cooperate only with experienced pentesters who are real professionals in such tools as Metasploit Framework and Cobalt Strike.

Cooperation terms and conditions are determined for each Customer individually.

With our help you can easily get more targets over the weekend than with any other affiliate program over the week.

LOCKBIT 2.0

Contact Us

Tox https://tox.chat/download.html

Tox ID Support

3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7

XMPP (Jabber) Support

598954663666452@exploit.im 365473292355268@thesecure.biz

企業を狙うサイバー犯罪の手口も体系化＆洗練されて共有化

GSX
GLOBAL SECURITY EXPERTS

実際にダークウェブで販売されている犯行シナリオのテキストのアジェンダ

1. 調査
2. 列挙分析
3. 犯罪シナリオの考慮
   3-1：脆弱性を悪用
   3-2：認証情報を悪用
   3-3：詐欺（ウイルス感染やフィッシングサイトへの誘導）
4. 初期潜入～偵察
5. 攻撃基盤の構築（陣地を作る）
6. 永続化（継続攻撃基盤の準備）
7. 情報の窃盗
8. 証拠隠滅とサービスの破壊
9. 脅迫

日本を取り巻く脅威

サイト改ざん

不正ログイン

不正アクセス

ランサムウエア

不正送金

内部犯行

負荷攻撃

標的型攻撃

攻撃手法が多様化しており、企業、個人として
どこまで対策すべきか頭を抱えている・・・

直近公表されたインシデント

9月28日　企業の健診結果を別企業へメールで誤送信 - **日大病院**
ワコールの海外子会社にサイバー攻撃 - 詳細を調査　**ワコールヨーロッパ**
9月27日　不正アクセスでスタッフの個人情報が流出した可能性、ハッシュ化PWも – **NHK**
セミナー参加者にメール誤送信、メアド流出 - **横須賀市**
事業者向けECサイトにサイバー攻撃 - **ソフトバンクC&S**
9月26日　セミナー案内メール、宛先に別人氏名誤送付 - **大阪府**
県立高校でメール誤送信、高校生活入門講座参加者のメアド流出 - **三重県**
9月25日　患者情報含む書類が所在不明 - **昭和大病院**
プレミアム付き商品券の発行事業でメール誤送信 - **唐津市**
9月22日　患者情報含むファイルがネット上で閲覧可能に - **日大板橋病院**
サポート詐欺で職員宅PCが遠隔操作 - **厚生中央病院**
9月21日　U-15選抜申込者の個人情報が閲覧可能に、フォーム設定ミスで - **INAC神戸**
サーバ侵害でキャンペーン応募者の個人情報流出の可能性 - **マルキユー**
シェアオフィスサイトが改ざん、顧客情報流出なし - **南海電鉄**
ボランティア登録した高校生宛のメールで誤送信 - **愛媛県**
9月20日　「新そばまつり」申込者の個人情報が閲覧可能に - **大石田町**
第三者が県立高PCを不正操作、偽警告にだまされ - **長野県教育委員会**
救急車出動先を知人にLINE送信、職員を懲戒処分 - **明石市**
9月19日　サーバに不正アクセス、個人情報10万件超が流出の可能性 - **マツダ**

引用：http://www.security-next.com

インシデントが発生する理由

外部からの攻撃

人的ミス

内部不正

現実問題としてもはや防ぐ事が不可能

ニュースに出てこないインシデント（事故）

ランサムウエア
ビジネスメール詐欺
システム、工場停止

これらは自社被害のためニュースになり難い
しかし情報漏洩よりもインパクト、企業リスクが大きい

私が目の当たりにしたインシデント

サイバーセキュリティにおける企業の最大のリスクは
「情報漏洩」よりも「事業継続の妨げ」にある

もはや経営課題でしかない

これからの対策は

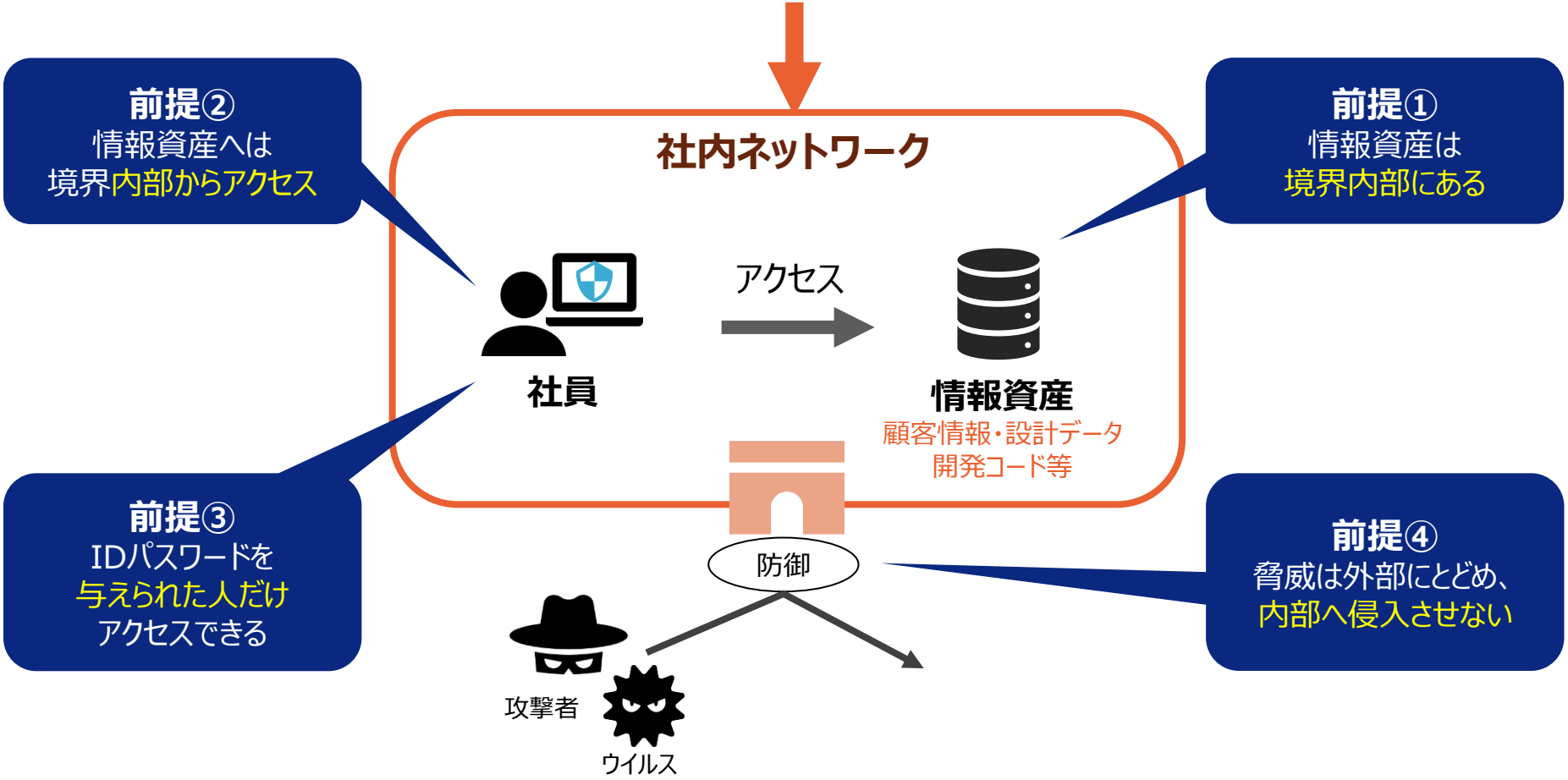
防御

素早い検知、素早い対応

ゼロトラストネットワークでは「社内は安全である」という前提の下で境界を守るセキュリティ対策ではなく、「全て信頼できない（ゼロトラスト）ことを前提として、全てのデバイスのトラフィックの検査やログの取得を行う」という性悪説に基づいたアプローチです。

境界防御の限界

これまでのセキュリティ対策は、**境界防御**でした。



「社内ネットワークの中は安全であり、信頼できる」という考え方

IT環境の3つの変化と今直面している課題

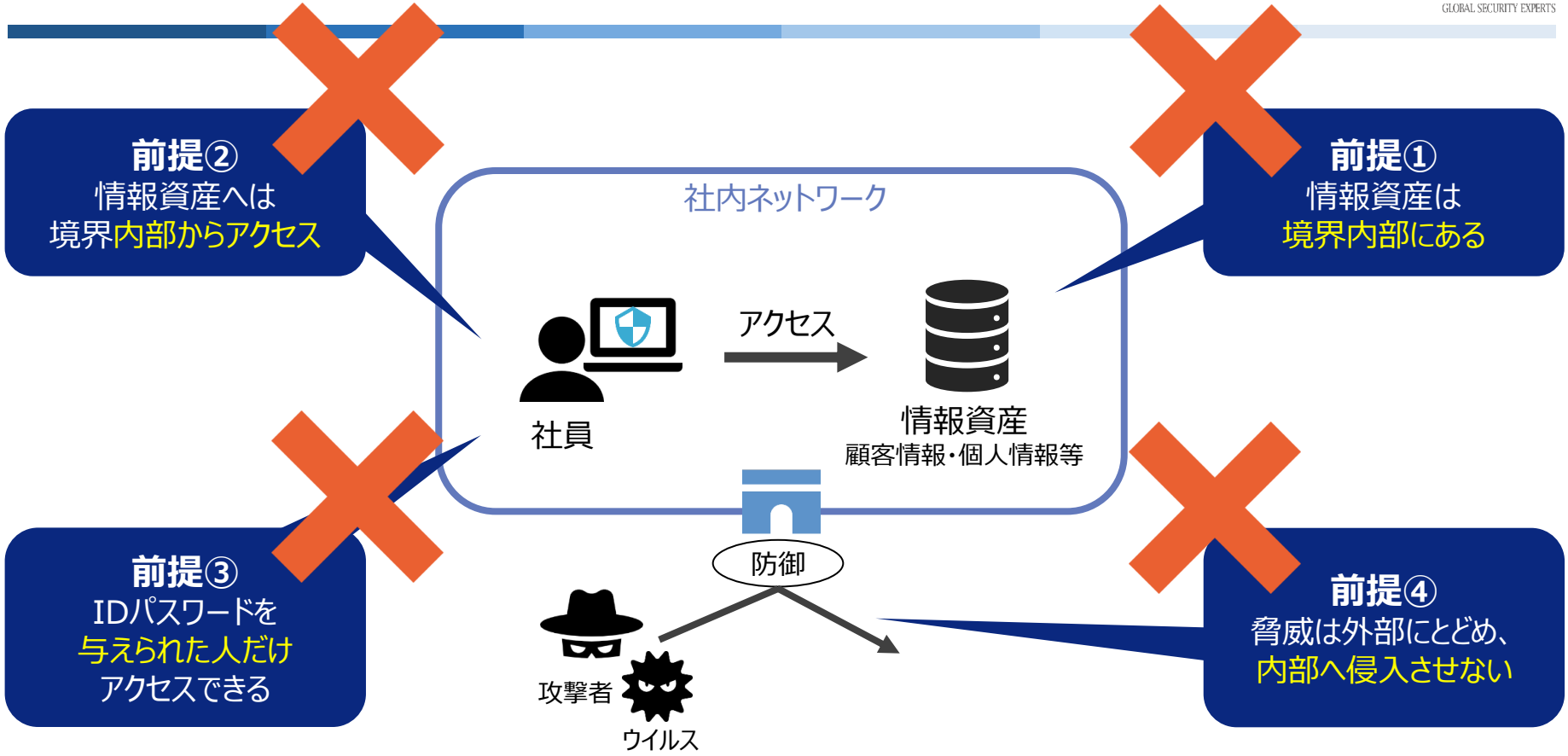
1. システムのクラウドサービスへの移行

2. 全てをインターネットで連携

3. サイバー犯罪の高度化/頻発化

境界防御だけで脅威に立ち向かうには限界がある

GSX
GLOBAL SECURITY EXPERTS



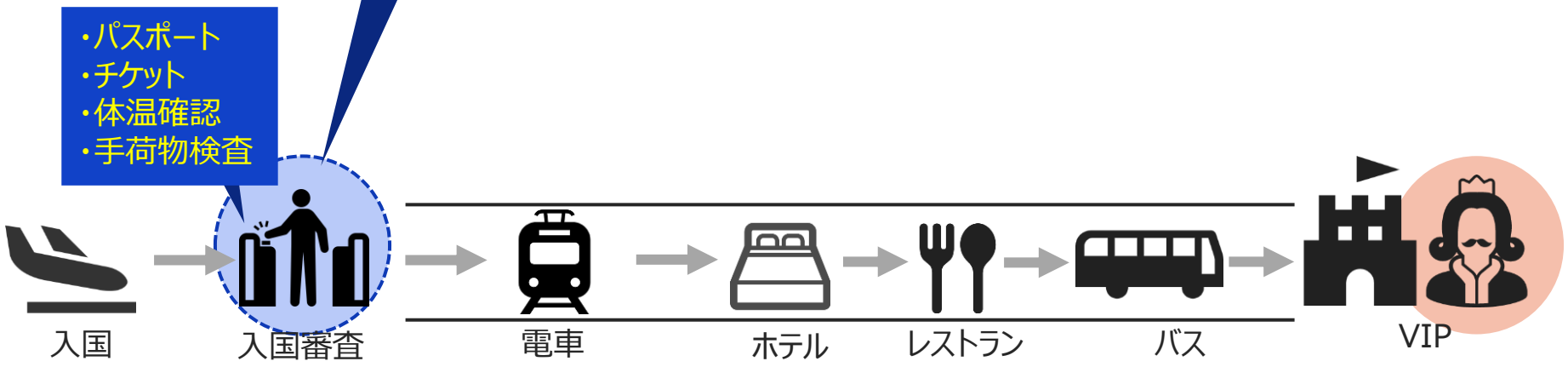
「社内ネットワークの中は安全であり、信頼できる」という考え方から
「信頼できるネットワークは存在しない」という考え方へ。
これがゼロトラストの根本となる考え方です。

1-3. 境界防御をたとえ話で理解する

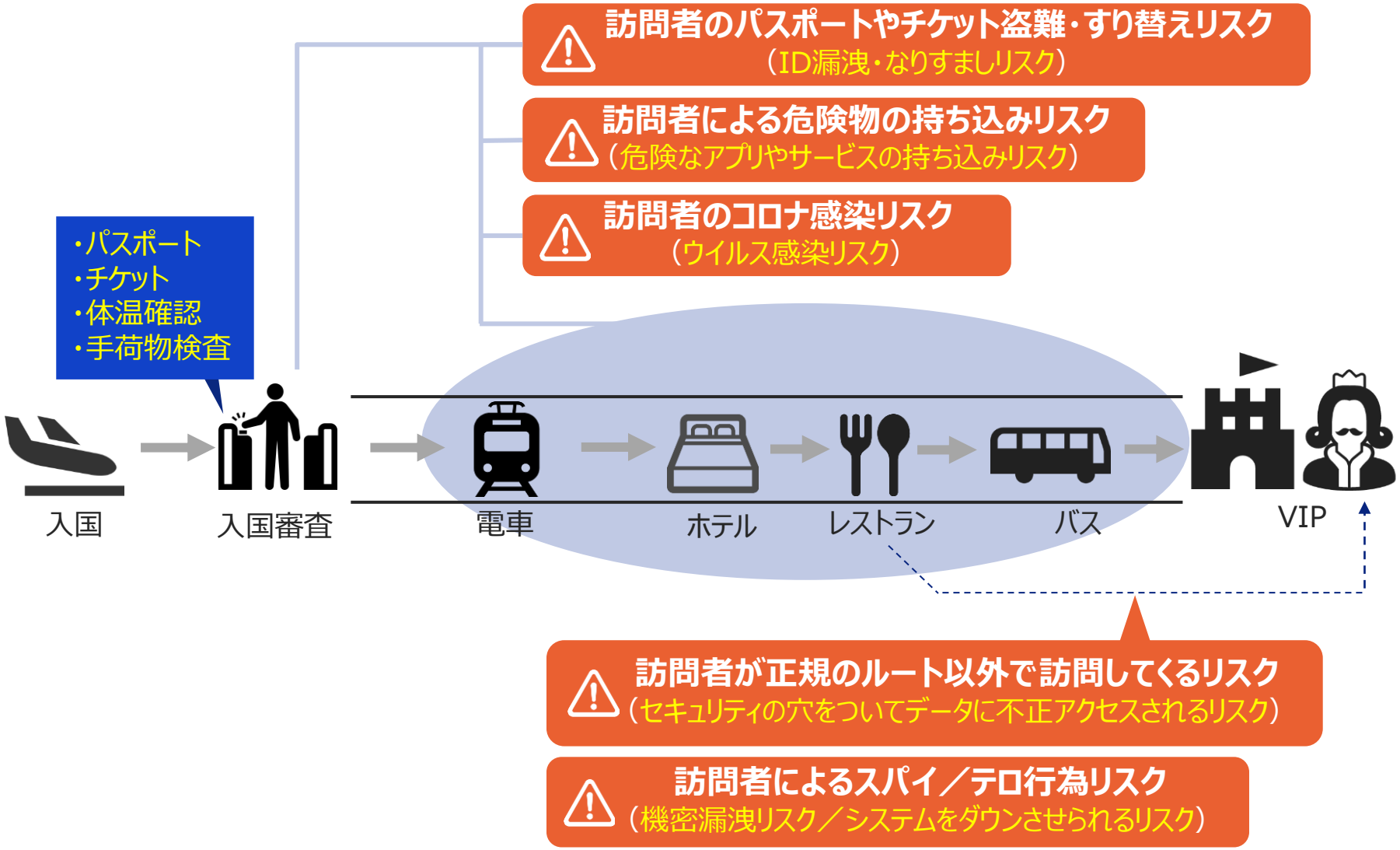
日本のVIPに会いに、外国人が来日した場合を想定してみましょう

VIPを守る視点から考えてみます

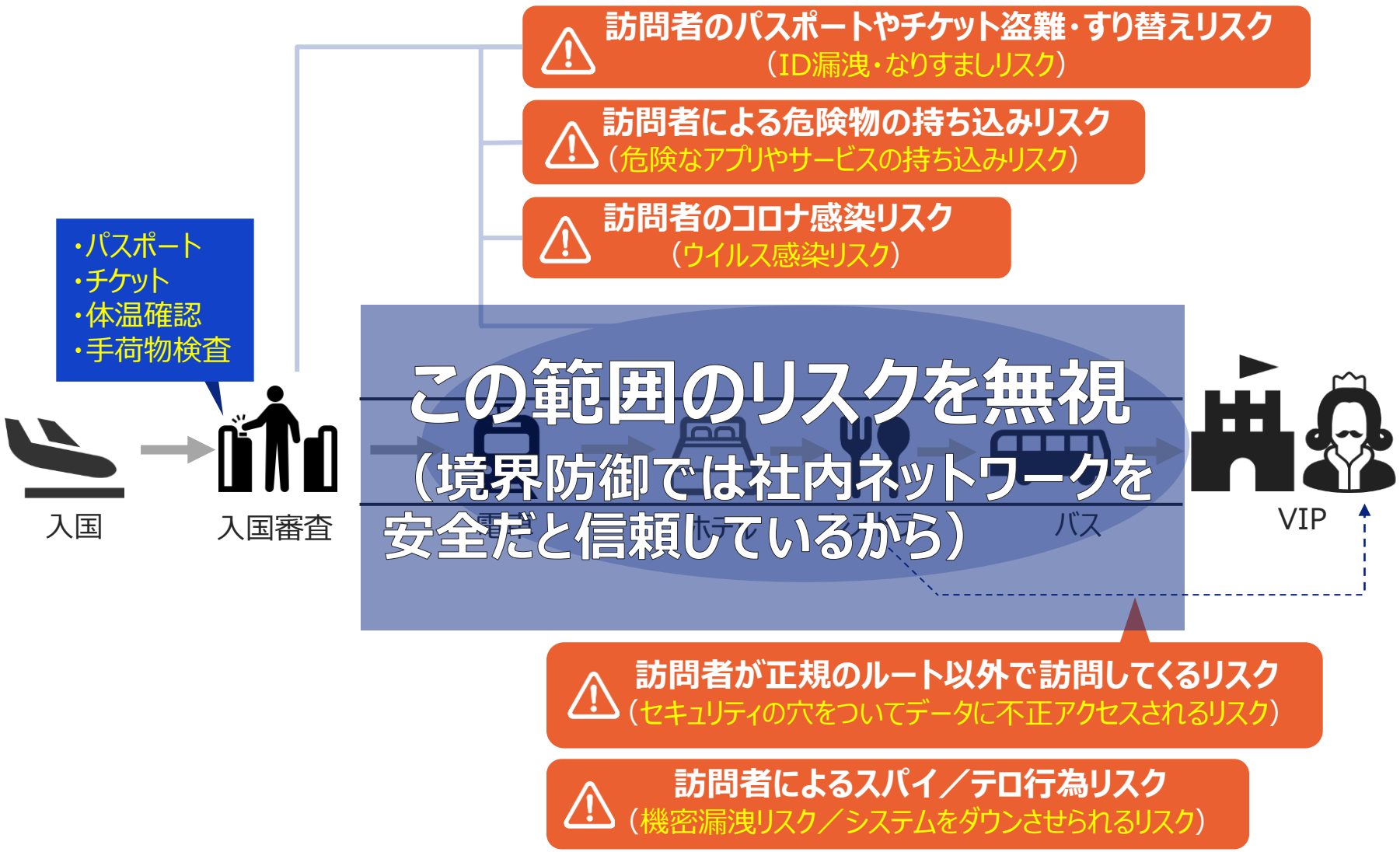
境界防御の考え方では、**一度でも安全確認していればOK**



1-3. 境界防御をたとえ話で理解する



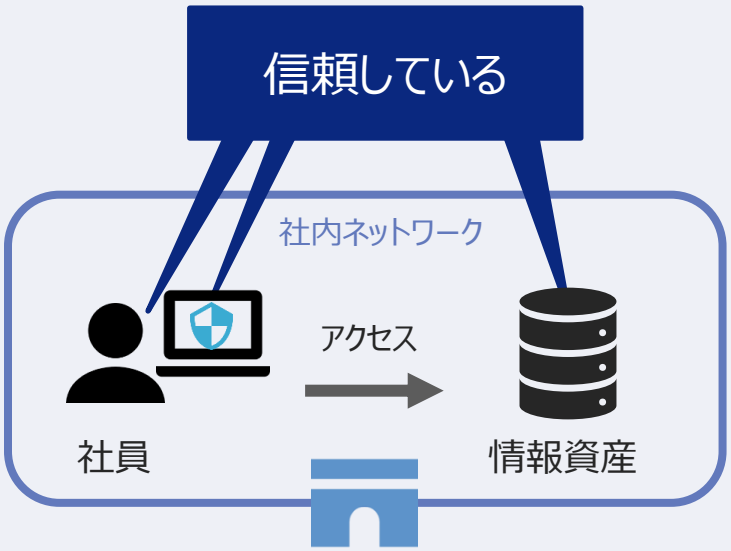
1-3. 境界防御をたとえ話で理解する



2-2. 境界防御とゼロトラストの比較

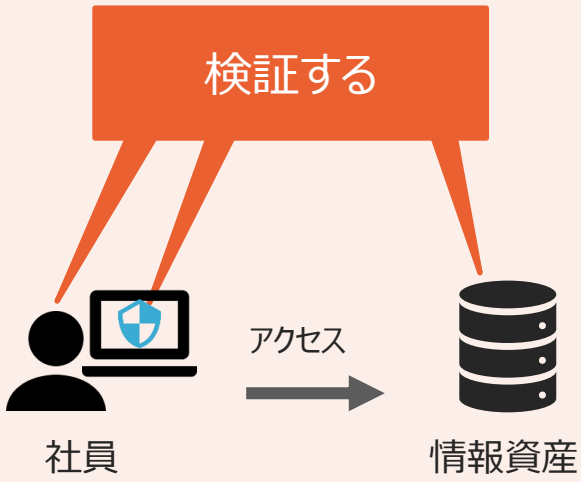
ゼロトラストとは、「無条件に信頼できるものは存在しない」という考え方。
これまでの「社内ネットワークの中は信頼できる」とする境界防御では限界があるため考案されました。

境界防御



**社内ネットワークを信頼しているため、
いったん境界内部に入ってしまえば、
様々な情報にアクセスできる**

ゼロトラスト



**社内ネットワークであっても、
社外ネットワークであっても
どちらも同じように”信頼しない”ため、
アクセスするたびに検証する**

2-3. ゼロトラストの7つの原則

アメリカ国立標準技術研究所

NIST（National Institute of Standards and Technology）は、科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関です。

SP800-207
Zero Trust Architecture

2021年8月 Final版が公開

https://csrc.nist.gov/publications/detail/sp/800-207/final

日本語版：https://www.ipa.go.jp/security/publications/nist/nist_publications.html#r2

SP800シリーズは、CSDが発行するコンピュータセキュリティ関係のレポートです。
米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書ですが、内容的には、セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応など、セキュリティに関し、幅広く網羅しており、政府機関、民間企業を問わず、セキュリティ担当者にとって有益な文書です。

2-3. ゼロトラストの7つの原則

GSX
GLOBAL SECURITY EXPERTS

NIST SP800-207

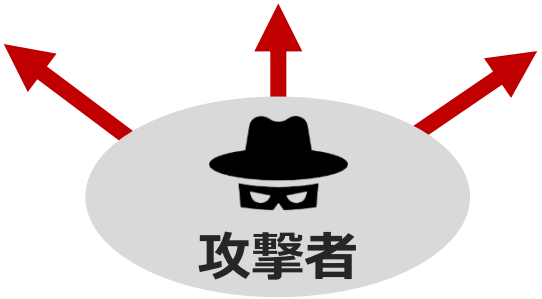
1. すべてのデータソースとコンピュータサービスを、**リソース**とみなす。
2. ネットワークの場所に関係なく、**すべての通信を保護**する。
3. リソースへのアクセスは、**セッションごとに許可／拒否を判断**する。
4. リソースへのアクセスは、**動的ポリシーで決定**する。
5. 正しくセキュリティが保たれるよう**すべてのデバイスを継続的に監視**する。
6. すべてのリソースの**認証と認可は、アクセスが許可される前に動的かつ厳密に実施**される。
7. 情報資産やネットワーク等の状態について、可能な限り**多くの情報を収集**し、**セキュリティを高めるために利用**する。

脅威と4つの検証ポイントの関係

アクセス元の脅威
- なりすまし（本人では無い）
- 端末がマルウェア感染している

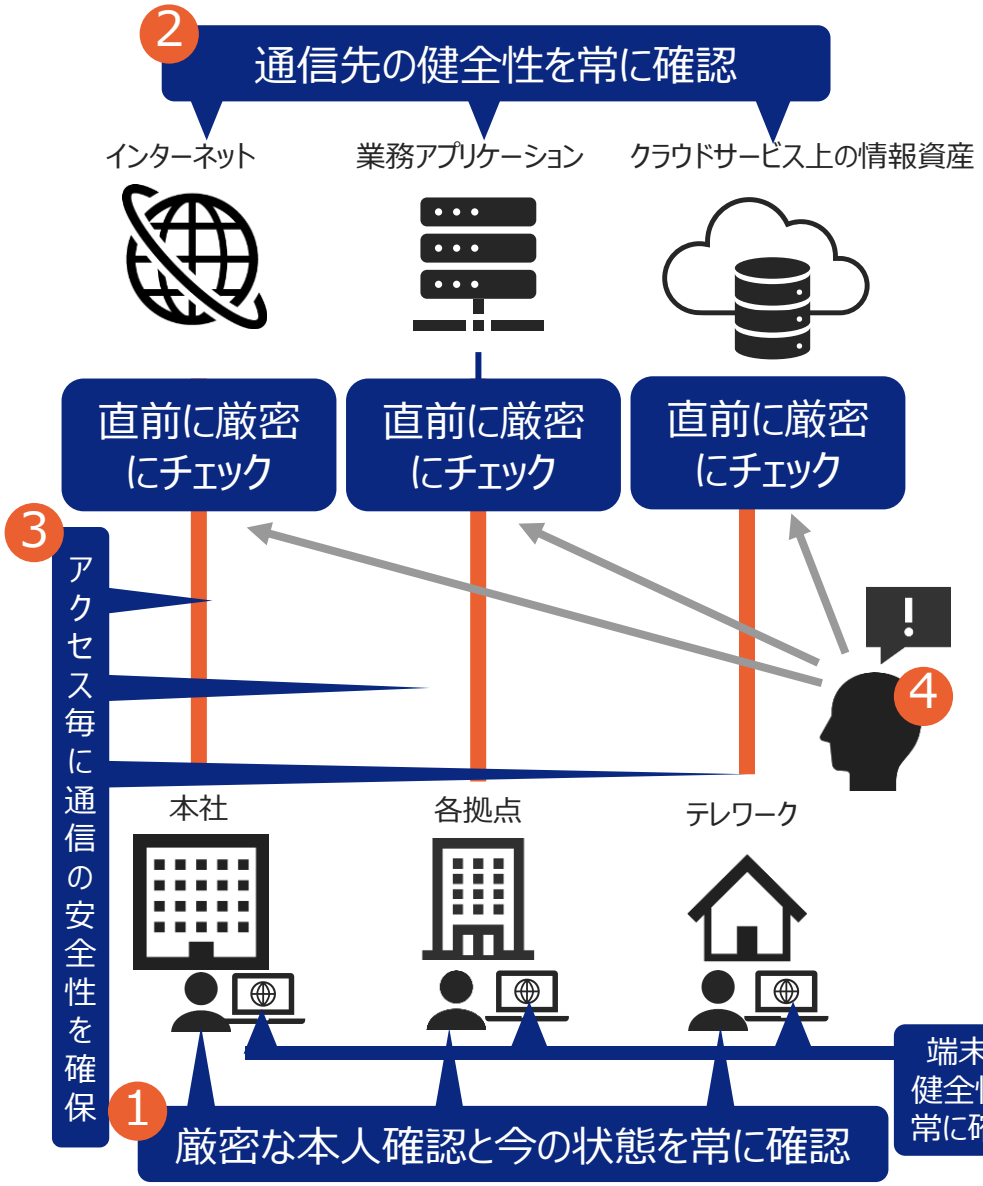
通信のやりとりの脅威
- 通信の盗聴や改ざん
- 通信のハイジャック
- 不正な経路

アクセス先の脅威
- 不正アクセス（情報漏えい）
- データの改ざん
- なりすまし（フィッシング）



2-6. ゼロトラストに必要な仕組を導入することで「できること」「わかること」

代表例



検証ポイント 1

高度な感染の検知と端末管理

なりすましの防止

巧妙なウイルスに感染していないか？
設定に問題がないか？
本当に本人がアクセスしてきているのか？

検証ポイント 2

シャドーITの抑制

業務サーバを常時管理

リスクの高いサービスを業務利用していないか？
サービス提供側の状況に変化が無いか？
業務サーバの状況が常に管理できているか？わかる

検証ポイント 3

どこでも業務アプリが使える

誰がどこでどのような通信をしているか常に把握

「誰が・どの情報に」アクセスしようとしているか？わかる
その信用度はどのくらいか？がわかる
どこからでも業務アプリやクラウドを安全に利用できる

検証ポイント 4

刻々と変わる状況を見える化 異変を早期検知

アクセス制御を動的に

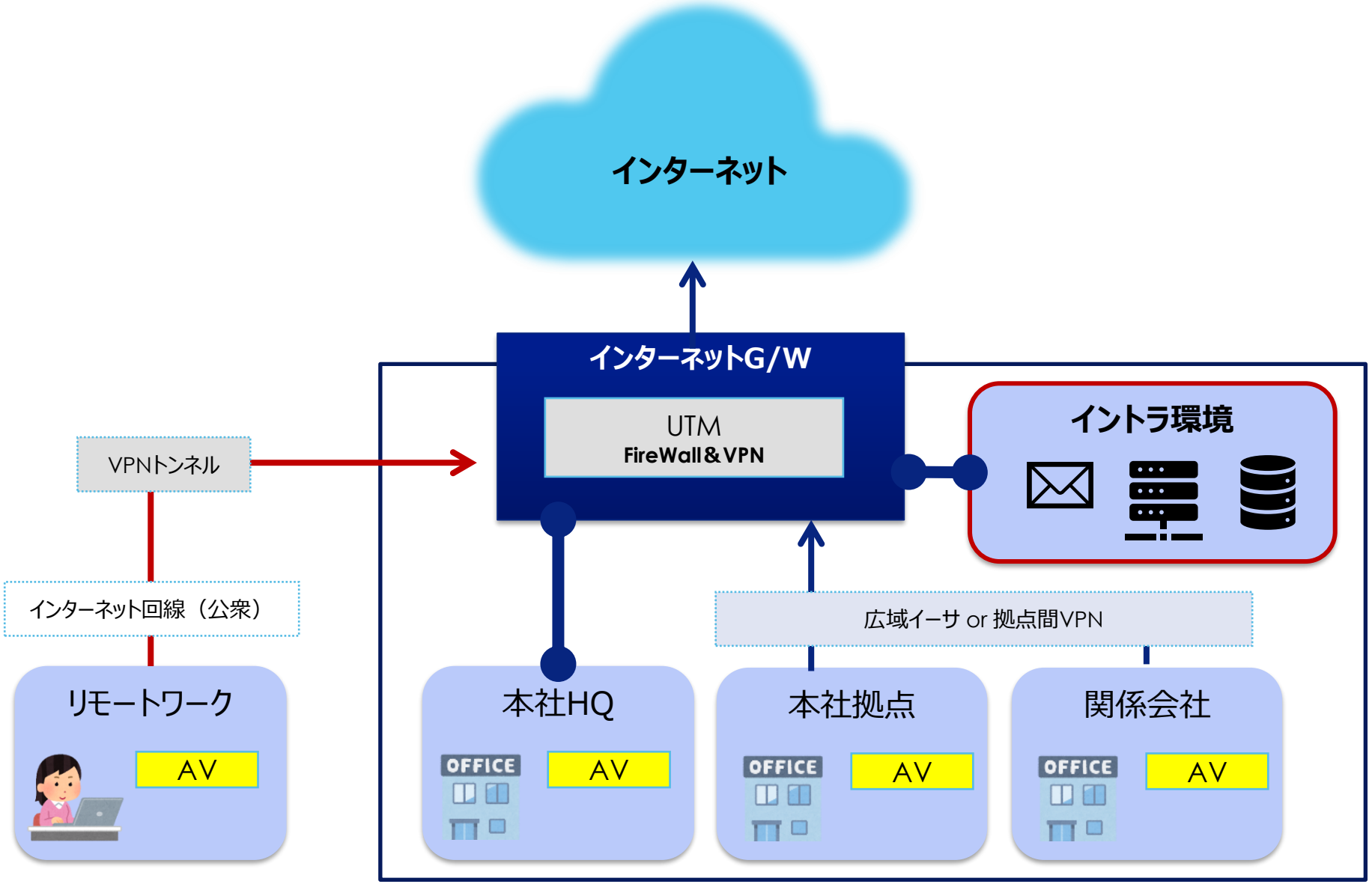
ログの統合管理と常時分析で状況を常時可視化できる
異変を早期にキャッチし、対応も迅速かつ的確
状況に応じた動的なアクセス制御が実現できる

1-4. 入門編のまとめ　さまざまな製品やサービスを組み合わせる

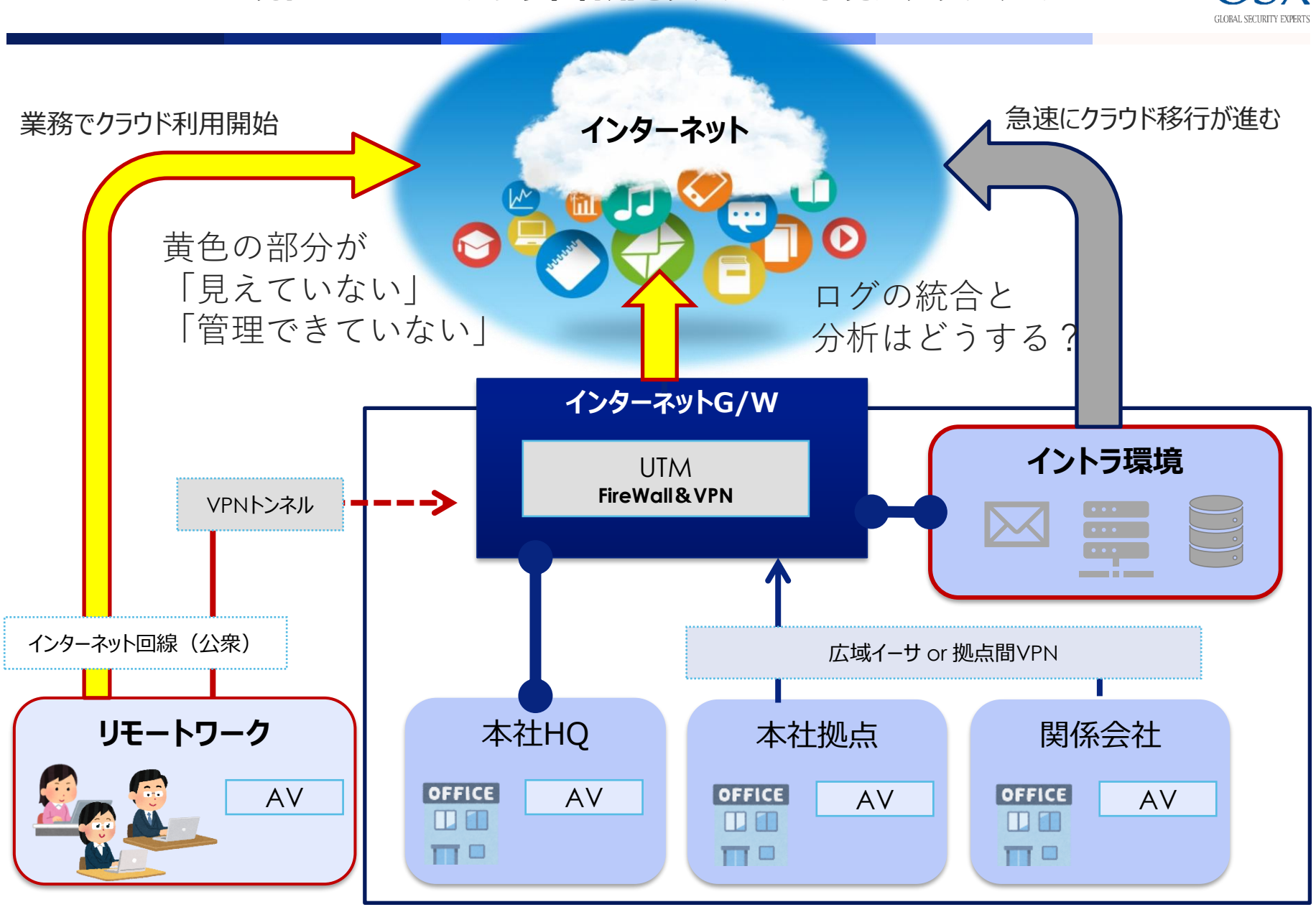
1つの製品やサービスですべての検証を行うことはできません。
複数の製品・サービスを組み合わせる必要があります。

		代表的な製品例
ID管理	**IDとアクセス制御の統合管理** （IAM / IDaaS：ID統合管理、および 詳細なアクセス制御と多要素認証＆シングルサインオン）	• Azure Active Directory • Okta Identity Cloud • Cisco Duo
ネットワーク制御	**認証とセッション別ネットワーク制御** （IAP：アイデンティティー認識型プロキシ） （SDP：ソフトウェアによる動的な境界制御）	• Zscaler Private Access • CATO Cloud • Google Identity-Aware Proxy
	インターネットアクセス制御 （SWG：SaaS型プロキシ＆Webフィルタ） （CASB：クラウド利用の制御）	• Zscaler Internet Access • Cisco Umbrella • CATO Cloud • Microsoft Could App Security
端末管理・制御	**端末の遠隔監視と事故対応** （EDR：端末の不審な挙動の検出と調査）	• Microsoft Defender for Endpoint • CrowdStrike Falcon • Cybereason EDR
	モバイル端末管理 （MDM：端末構成管理と、操作記録の取得） （MAM：端末のアプリケーション管理）	• Microsoft Intune • VMware Workspace ONE
状況監視	**Logの統合管理基盤** （SIEM：セキュリティ情報イベント管理）	• Splunk Enterprise Security • Azure Sentinel • Chronicle Security Analytics Platform
	ユーザーの行動分析/活動可視化基盤 （UEBA：ユーザーと端末の活動を自動で時系列に相関分析）	• exabeam

昔のネットワーク構成：10年前まではみなこの構成だった

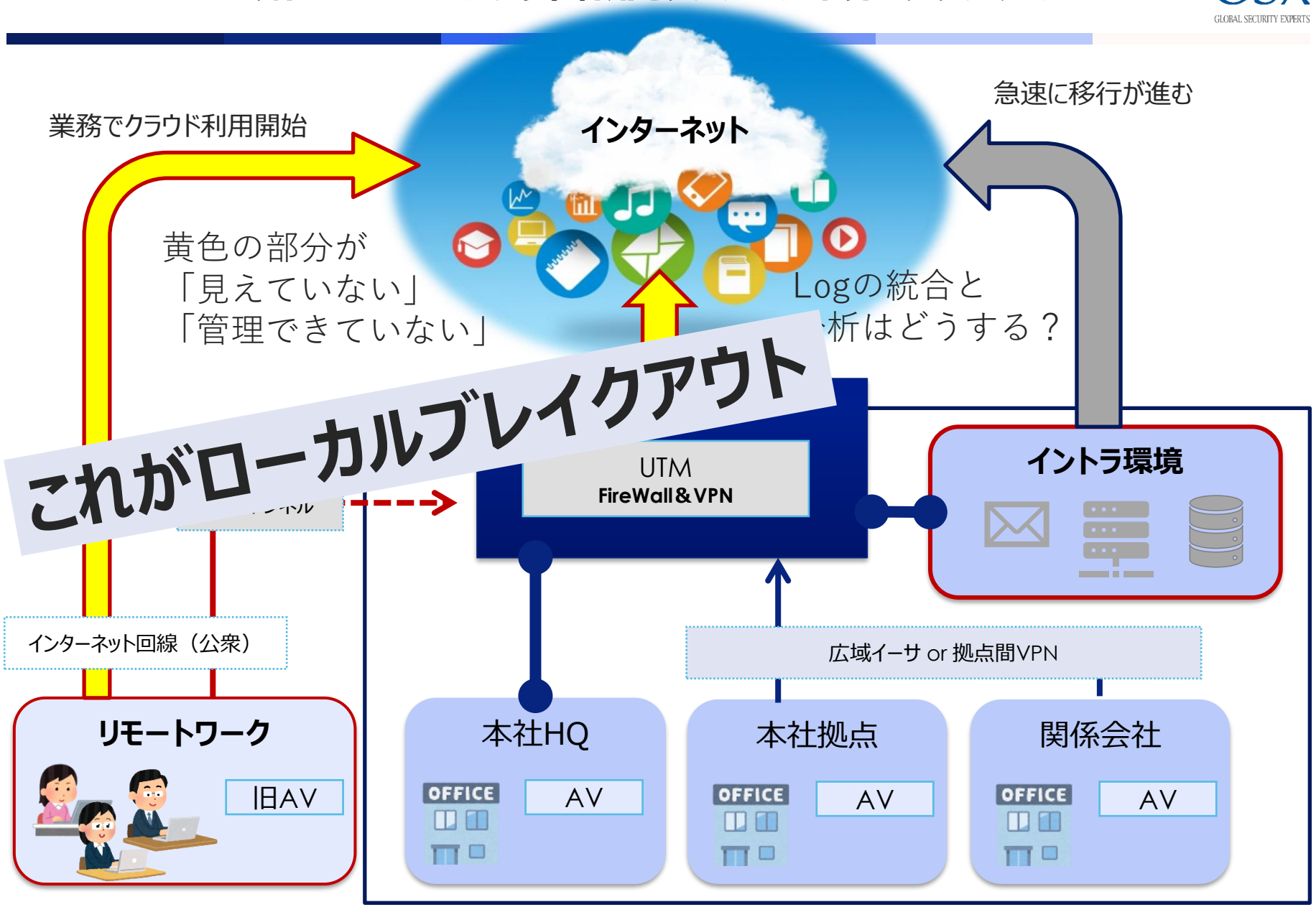


現在は… ⇒ クラウド利用とテレワーク環境がアタリマエに



現在は… ⇒ クラウド利用とテレワーク環境がアタリマエに

GSX
GLOBAL SECURITY EXPERTS



1．端末に問題がおきたら、分析も対処もできない

2．G/Wを通らないので、Web利用管理できない

3．会社の資産が管理しきれない

4．社員がオフィスに居ないので、目が届かない

クラウド利用とテレワーク環境でも安心して見えるように

GSX
GLOBAL SECURITY EXPERTS

業務でクラウド利用開始
クラウド利用を管理/可視化

インターネット

様々なログを自動解析し
ユーザー毎の行動に可視化
SIEM/UEBA

社外サービスも含めた全ての通信を可視化、制御
SWG/CASB

旧 G/W

UTM
FireWall＆VPN

VPNトンネル

イントラ環境

インターネット回線（公衆）

広域イーサ or 拠点間VPN

リモートワーク

端末の感染拡大を最
小限に留める
EDR

本社HQ
OFFICE
EDR

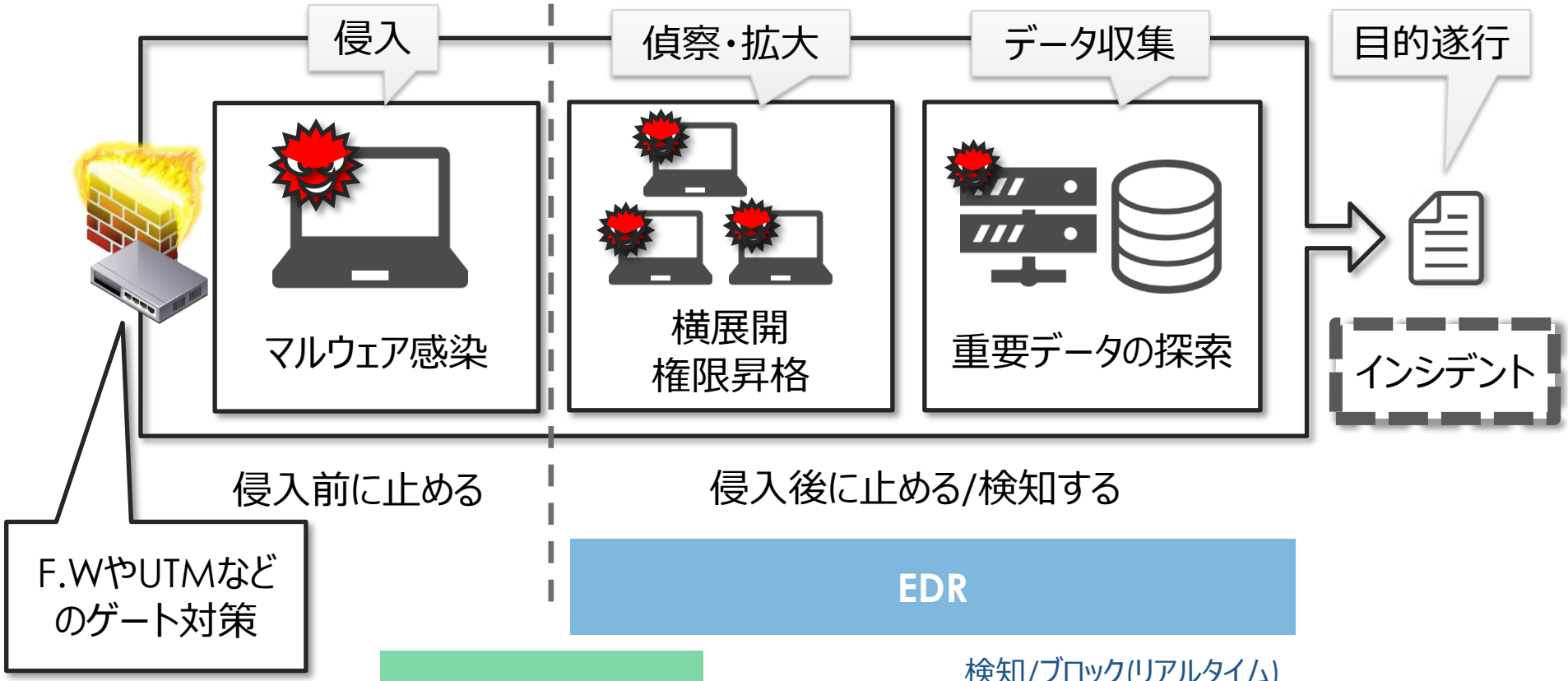
国内拠点
OFFICE
EDR

海外拠点
OFFICE
EDR

侵入されてからの「見えなかった動き」を可視化する

中の動きを可視化し、即応できる準備を

端末も「防御」から「検知・対処」へ



※**EDR**（Endpoint Detection & Response）
端末感染の検知・対処を行う仕組み

体制（CSIRT等）の構築

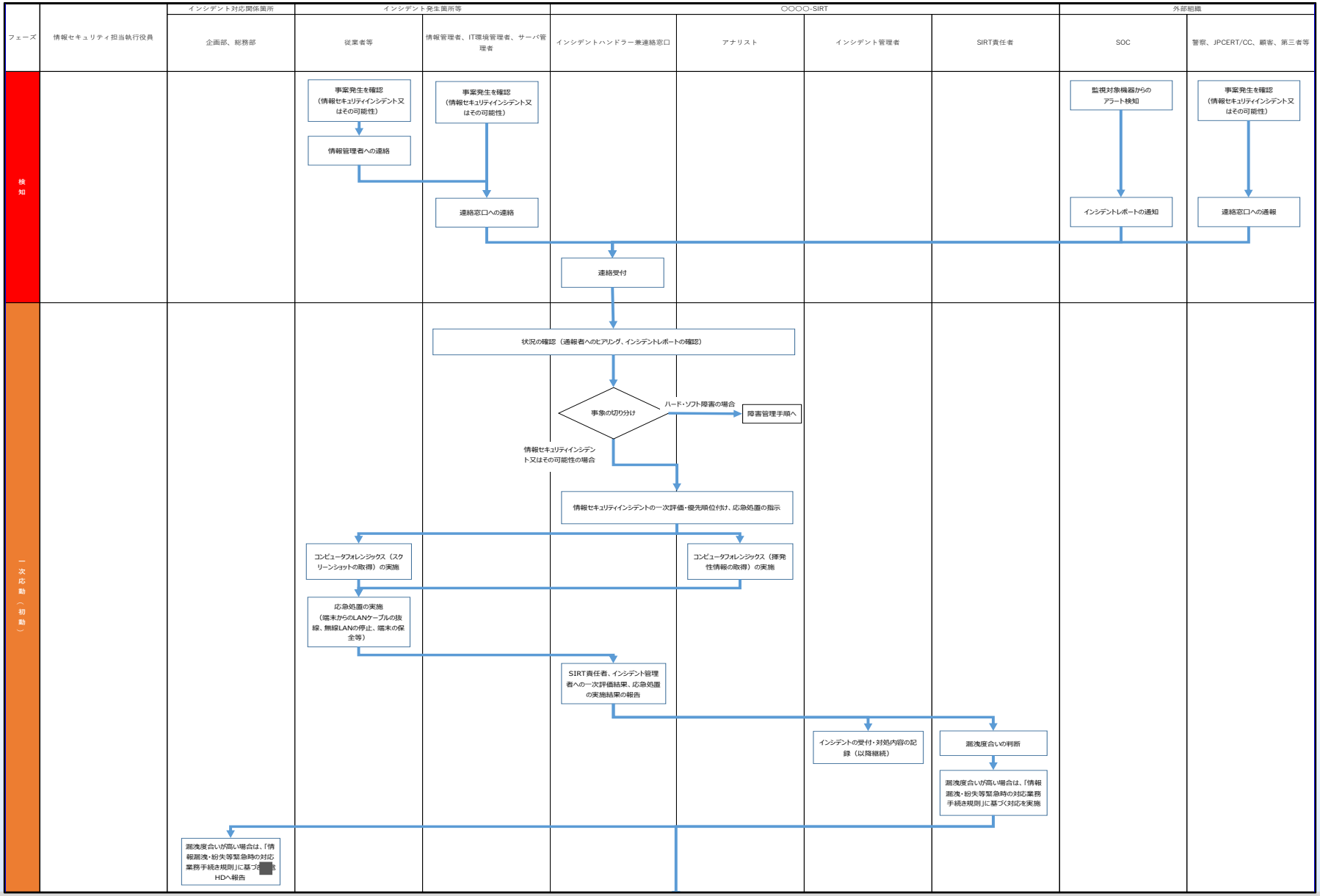
CSIRTのサービス・機能

【CSIRTのサービス・機能】

インシデント事後対応サービス	インシデント事前対応サービス	セキュリティ品質向上サービス
• セキュリティイベントの受付 • トリアージ • コンピュータ・フォレンジックス • マルウェア解析・ログ分析 • 内部連携 • 外部連携 • 被害拡大防止・復旧 • 経営層への報告 • 再発防止策の検討	• 脅威・脆弱性情報の収集 • セキュリティ技術動向調査 • 監視（セキュリティイベントの検知） • 脆弱性診断 • 外部コミュニケーション	• リスクアセスメント • セキュリティ監査 • 製品評価・認定 • 規程・ガイドライン・計画等の策定・維持 • セキュリティ教育・啓発 • サイバー訓練、演習

参照した指針・ガイドライン等
- 日本シーサート協議会「CSIRTスタータキット」
- 金融庁「「金融商品取引業者等向けの総合的な監督指針」
- 経産省「サイバーセキュリティ経営ガイドライン」
- 内閣サイバーセキュリティセンター「政府機関の情報セキュリティ対策のための統一基準（平成30年度版）」
- 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」

インシデント対応基本フロー



インシデント演習

実際のシナリオを用いて
事故時を想定したアクション、判断ポイントを確認

訓練参加者の例

**実際にインシデントを想定することで、どうアクション
すべきか、どう判断すべきかを確認できる**

**対応フローを確認することで、参加メンバーの
意識を高めることができる**

**組織変更によるフローの問題、ボトルネックを
発見、修正することができる（形骸化しない）**

自工会ガイドライン（JAMA2.0）

自工会/部工会・サイバーセキュリティガイドライン

JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.0 版

Japan Automobile Manufacturers Association, Inc.

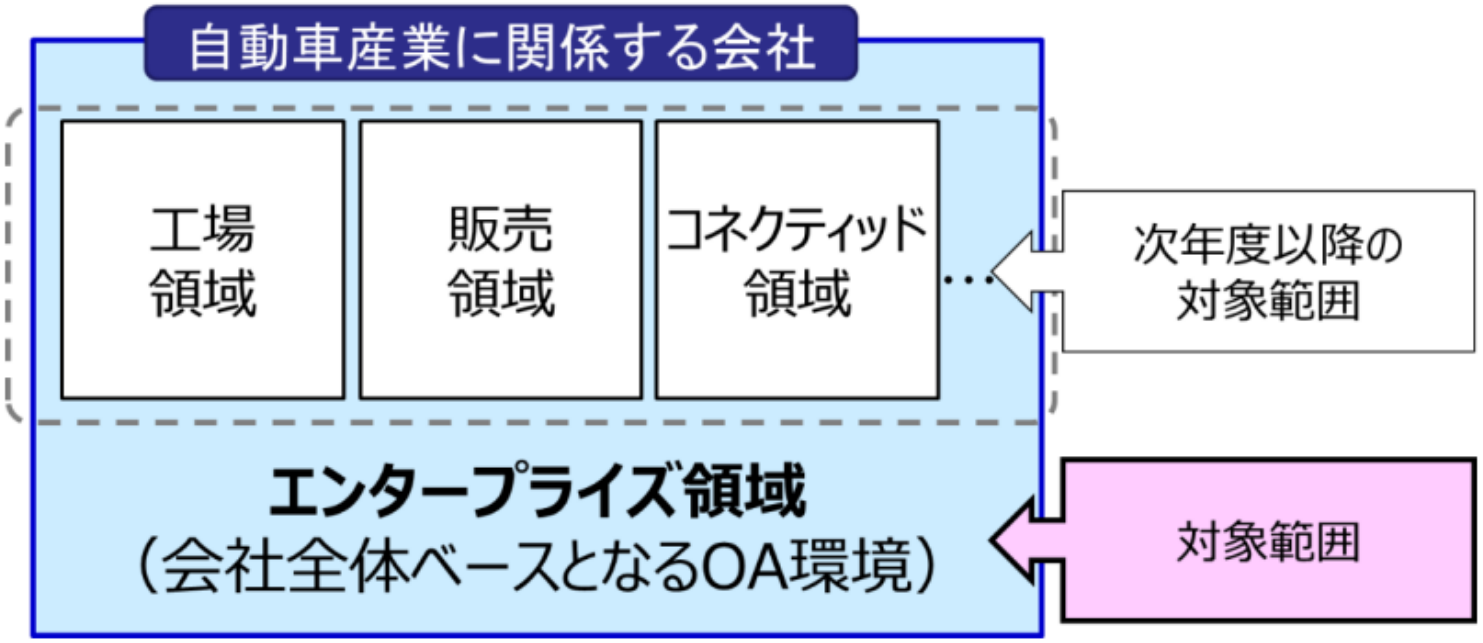
一般社団法人　日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

Japan Auto Parts Industries Association

一般社団法人　日本自動車部品工業会
IT 対応委員会
サイバーセキュリティ部会

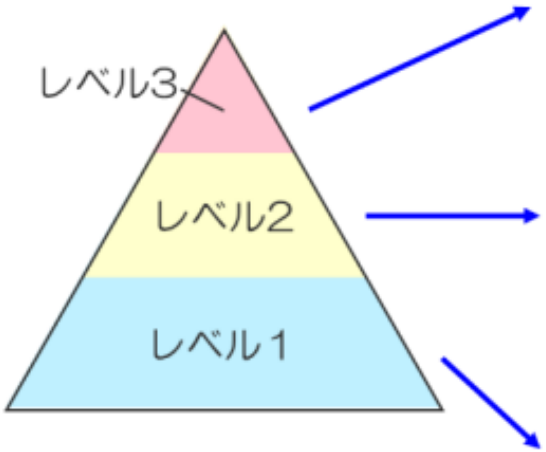
1 方針
2 機密情報を扱うルール
3 法令順守
4 体制(平時)
5 体制(事故時)
6 事故時の手順
7 日常の教育
8 他社との情報セキュリティ要件
9 アクセス権
10 情報資産の管理(情報)
11 情報資産の管理(機器)
12 リスク対応
13 取引内容・手段の把握
14 外部への接続状況の把握
15 社内接続ルール
16 物理セキュリティ
17 通信制御
18 認証・認可
19 パッチやアップデート適用
20 データ保護
21 オフィスツール関連
22 マルウェア対策
23 不正アクセスの検知
24 バックアップ・復元(リストア)

やはり体制とサプライチェーンにも言及されており、
どのガイドラインも求めるものはそう変わらない



＜図：自動車産業 CS ガイドラインの対象領域＞

CSIRT（OA）、FSIRT（工場）、PSIRT（製品）と対応領域を広げていく必要がある



レベル	定義	各レベルの達成を目指すべき会社
Lv3	現時点*で自動車業界が到達点として目指すべき項目　*2022年4月	・会社規模・技術レベルの観点で自動車業界を代表し牽引すべき立場の会社またはそれを目指す会社 ◆Lv1～3の全項目を達成
Lv2	自動車業界として標準的に目指すべき項目	以下のいづれかに該当する会社 ・サプライチェーンにおいて社外の機密情報（技術・顧客情報等）を取り扱う会社 ・自動車業界として重要な自社技術／情報を有する会社 ・相応の規模／シェアを有し、不慮の供給停止等により業界のサプライチェーンに多大な影響を及ぼし得る会社 ◆Lv1,2の全項目を達成
Lv1	自動車業界として最低限、実装すべき項目	・自動車業界に関係する全ての会社 ◆Lv1の全項目を達成

＜図：自動車産業 CS ガイドラインのセキュリティレベル定義＞

会社規模、取引状況、保持する情報によって求めるレベルを設定

					ること	
6 事故時の手順	同上	情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること	23	Lv2	情報セキュリティ事件・事故として扱う対象範囲を明確にし、周知していること	【規則】 ・下記対象範囲が明確になっていること ［明確にする内容］ -事件・事故として扱う事象 -事件・事故のレベル 【対象】 ・役員、従業員、派遣社員、受入出向者への周知
			24	Lv1	情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動、③調査・対応、④復旧、⑤最終報告
			25	Lv3	情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)は、定期的に確認され、必要に応じて、改定していること	【頻度】 ・１回／年及び、重大な事件・事故が発生した場合
			26	Lv1	マルウェア感染時の対応手順を定めている	【規則】 ・マルウェア感染時用の対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動、③調査・対応、④復旧、⑤最終報告
			27	Lv2	マルウェア感染時の対応手順は、定期的に確認され、必要に応じて、改定していること	【規則】 ・世間動向や攻撃のトレンドなどをふまえ、教育・訓練内容の見直しをすること 【頻度】 ・1回/年以上

インシデント対応手順は必須（Lv1）、周知（Lv2）、定期的な演習（Lv3）とレベル分け

セキュリティ対策の進め方

全職員の教育 ①

守る資産を把握 ②
リスクアセスメント
何を守るか？を明確にしリスクを見える化

対策ロードマップ

検知対処する仕組み ③
驚異を可視化する仕組の導入
（センサー/分析基盤/監視基盤）

体制構築 ④
脅威を早期に分析し、対処する
仕組の構築(社内体制)

①教育＆アウェアネス向上
階層別研修
標的型メール訓練
E-Learning
インシデント対応演習

②アセスメント
リスクアセスメント
脆弱性診断
ペネトレーションテスト
ロードマップ策定支援

③システム導入＆運用
EDR/MDR
SWG/CASB/SASE
SIEM/UEBA
緊急対応（フォレンジック）

④組織構築
セキュリティ人材育成
CSIRT/PSIRT/FSIRT
ポリシー作成/更新
運用チーム構築

まとめ

- 全職員の意識教育と事故を想定した訓練
- 防御から検知・対処への仕組み（ゼロトラスト）
- セキュリティ担当、専門部署（CSIRT）の設置

防御出来ないという想定のもと
直ぐに気づいてボヤで収束させる体制に

GSX

GLOBAL
SECURITY
EXPERTS

インシデント時にはこちらへご連絡下さい

緊急対応窓口：　119@gsx.co.jp

03-3578-9055