資料１－４－２

NOTICE：4年間の取組と成果、課題

～ ナショナルサイバーオブザベーションセンターの取組 ～

2023/01/18

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
ナショナルサイバーオブザベーションセンター

NOTICEとNICTERの2つの通知を実施

Active Countermeasure

パスワード設定等に
不備のある機器

特定アクセス
による調査

NOTICE
National Operation Towards IoT Clean Environment

通知
(2019年4月より開始)

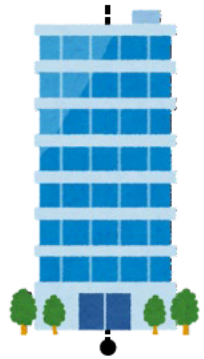
Passive Countermeasure

既にマルウェアに
感染している機器

ダークネット
による観測

NICTER

通知
(2019年6月より開始)

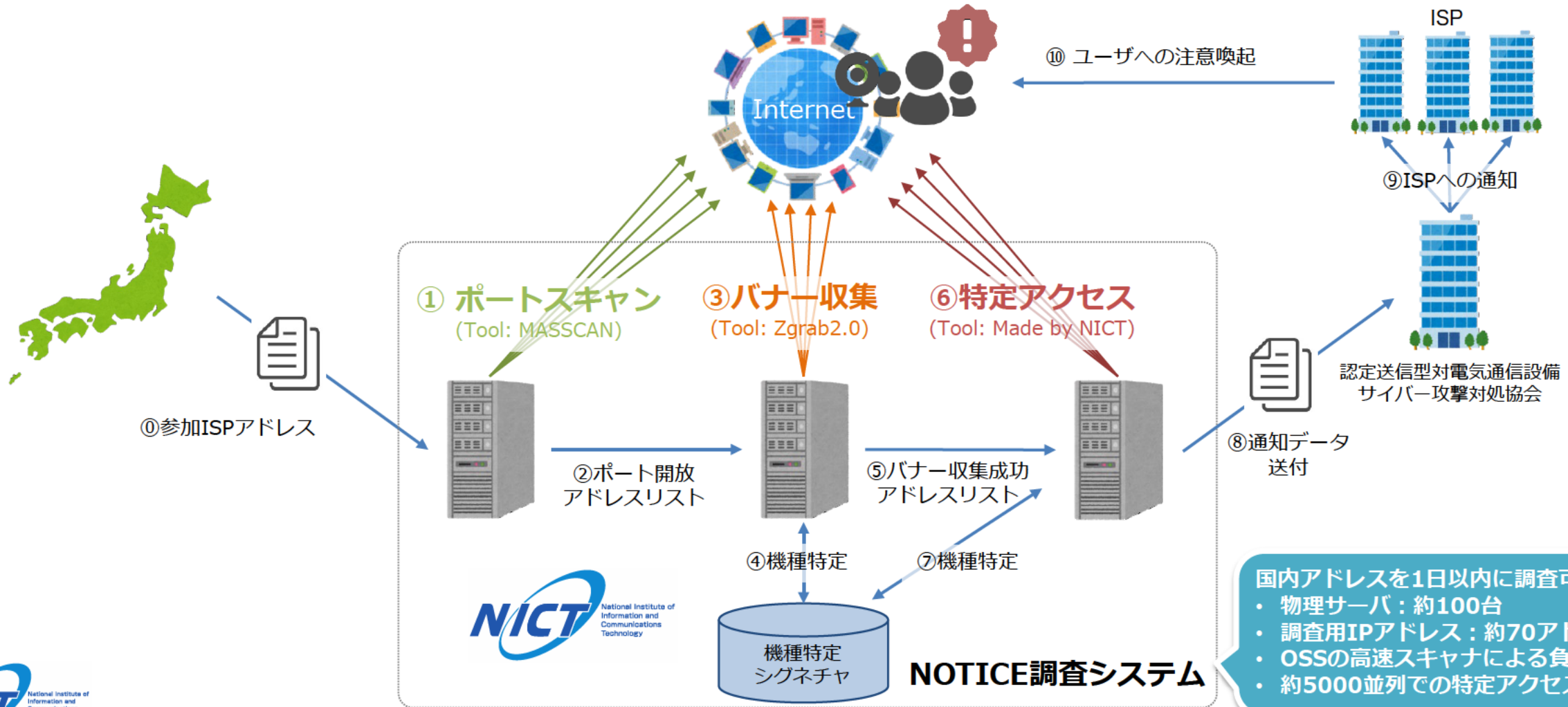


ISP

NICT National Institute of Information and Communications Technology

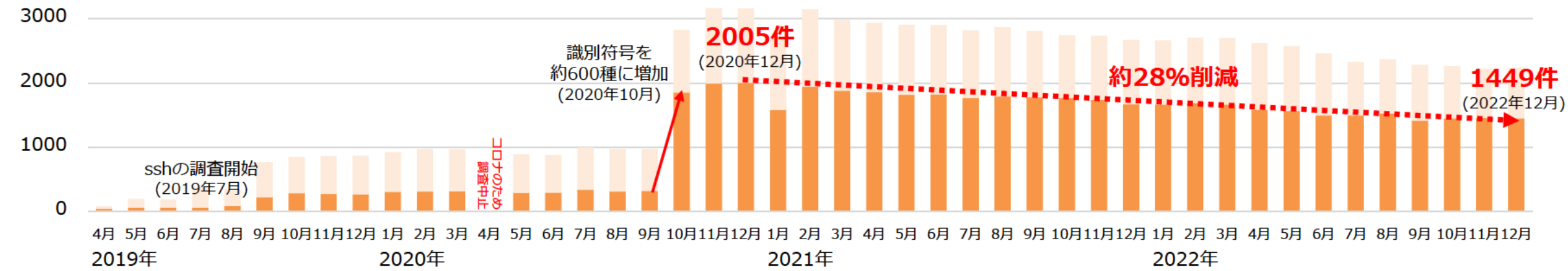
日本国内アドレスを1日以内に調査可能なシステムを構築

- **2019年4月：NOTICE調査＋ISP通知の開始**

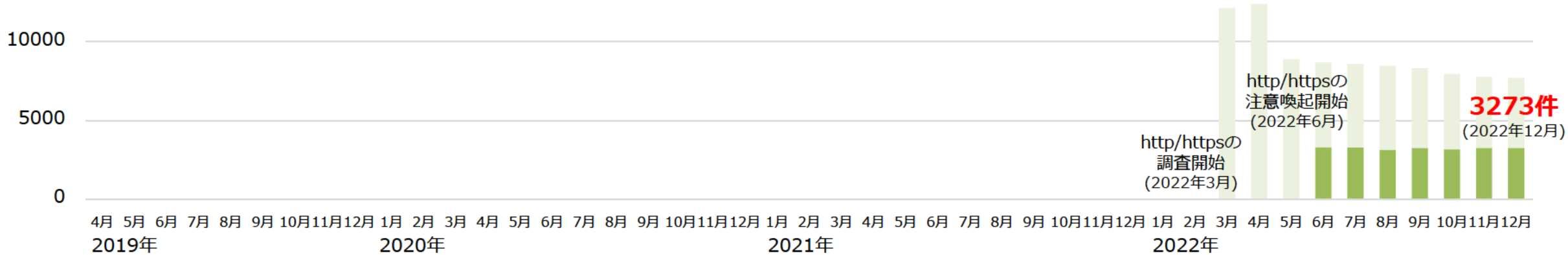


月1回の継続的な調査とISPへの通知を実施

- **Telnet/SSHに関して注意喚起対象数は約28%減少 (ピーク比)**
  - ✓ 新規ISPの追加や新たな機器が発見されるケースがあるため増加分も含む統計値であることに注意



Telnet/SSHの注意喚起対象数の推移(月毎)



HTTP/HTTPS(Basic認証/Digest認証)の注意喚起対象数の推移(月毎)

NICT National Institute of Information and Communications Technology

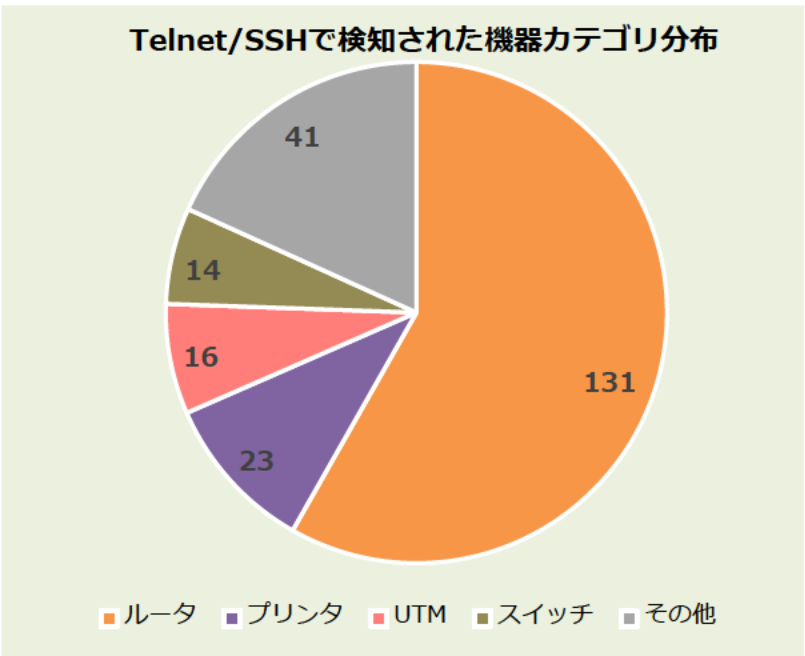
注意喚起対象数が0件まで減少したISPの事例

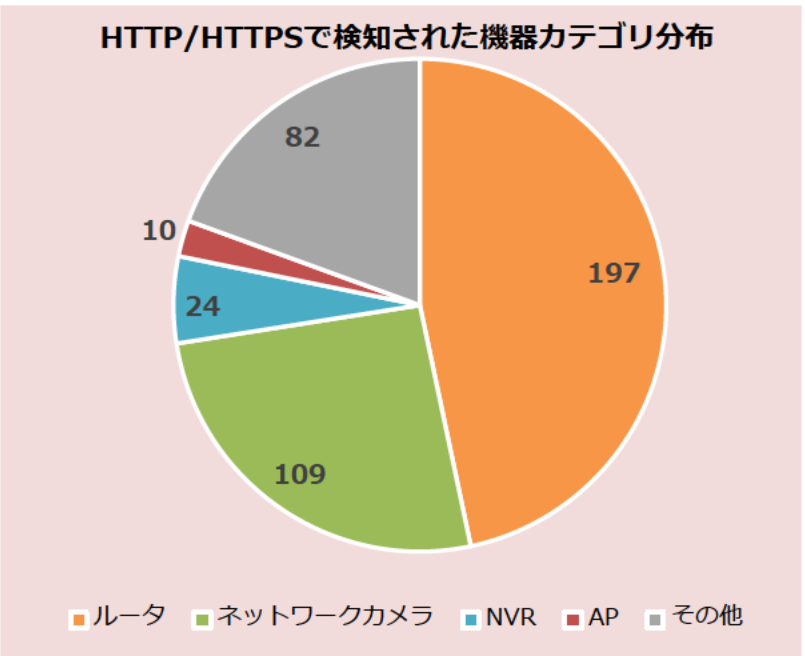
- **某ISP：Telnet/SSHに関してはほぼ全件対処完了**
  - ✓ 検知された契約者は**全て法人顧客**。メールでの注意喚起を実施
  - ✓ ISP内で通知データを顧客単位で紐づけて暦月管理し、対処状況を把握

某ISPのNOTICE通知グラフ

NOTICEで発見した機器の機種特定に成功(約600機種)

Telnet/SSH：　50ベンダ、計225機種
HTTP/HTTPS：83ベンダ、計422機種
を特定(2022年12月時点まで)





リフレクション攻撃の踏み台となる機器の情報提供を開始

- **リフレクション攻撃は大規模なDDoS攻撃(サービス妨害攻撃)で用いられる**
  - ✓ 2020年02月：2.3 Tbpsのリフレクション攻撃の発生をAmazonが報告
  - ✓ 2021年11月：3.47 Tbpsのリフレクション攻撃の発生をMicrosoftが報告

- **リフレクション攻撃に悪用される恐れのあるリフレクタ(踏み台)を調査し、2022年3月よりISPへ情報提供を開始。注意喚起実施に向けて調整予定**
  - ✓ 悪用されるプロトコルのうち、DNS、NTP、SSDPの3種のプロトコルの踏み台を調査

非公開情報	非公開情報	非公開情報

リフレクション攻撃の踏み台として悪用される恐れのある機器数の推移(各プロトコル、月毎)

ユーザ注意喚起無しでISPが直接対処した事例(1)

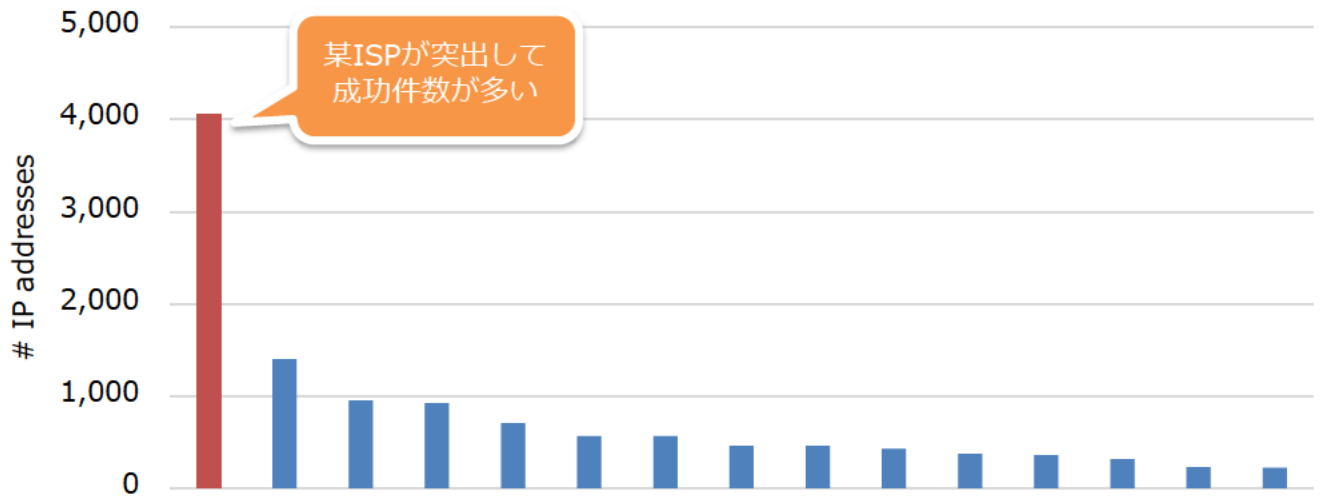
- **2019年9月：某ISPにある某社製ルータに特定アクセス成功・通知**
  - ✓ 通知数は約20件だが、ログイン試行が可能な機器が1700台以上、当該ISP内に存在
- **同月：当該ISPが調査した結果、ISP管理ルータ(マンション設置機器)と判明**
  - ✓ 管理用にOpen。設置時のパスワード変更の作業漏れで一部のルータがデフォルトで放置
- **～2019年11月：ISPでパスワード変更した結果、通知数0件に減少**
  - ✓ パスワード変更に合わせてログイン試行可能な機器1700台も設定変更され、悪用リスクを軽減

某社製ルータの注意喚起対象数の推移(月毎)

某社製ルータのログイン試行可能な機器数の推移(月毎)

ユーザ注意喚起無しでISPが直接対処した事例(2)

- **2022年3月：HTTP予備調査時に某ISP内で大量の機器にログイン成功**
  - ✓ バナー情報から4000台以上は全て同一機器だと推測し、ISPに通知
- **同月：当該ISPが調査した結果、ISP管理ルータ(顧客配布モデム)と判明**
  - ✓ 全て特定ベンダの機種(バージョン違い含む)であったため、ISPからベンダに修正を依頼
- **～2022年5月頭：ISPで修正ファームウェアの適用を実施し、対処完了**



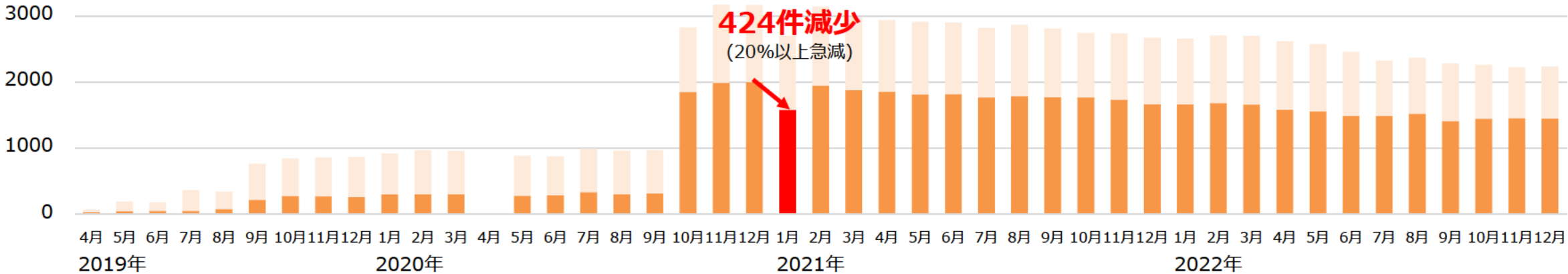
予備調査時(2022年3月)のISP別のhttp/https特定アクセス成功数

非公開情報

特定されたISP配布のルータシリーズ

毎月調査の変動から実際の不正アクセス発生を特定した事例

● 2021年1月：Telnet/SSHの検知数が急減



Telnet/SSHの注意喚起対象数の推移(月毎)

- **某ベンダの機器が調査と同じタイミングにインターネットから不正ログインされていたことで、調査の特定アクセスが失敗し、検知数が急減していたことが詳細分析によって判明**
  - ✓ 当該機器のデフォルトアカウントは同時ログインができない仕様のため、特定アクセスが失敗していた
  - ✓ 減少が見られたISPに協力を依頼し、実際の顧客の該当機器のログを調査した結果、インターネット上の機器から不正アクセスされていたログが発見されたため、各ISPに本事象について注意喚起を実施
  - ✓ 2021年2月からは元の水準に戻った

課題(1)：注意喚起対象外となっている機器への対処①

- **NOTICE調査の過程で見つかったパスワード設定等の不備以外のIoT機器の脆弱性の代表例：**
  - ✓ 脆弱なVPNルータの調査結果 (2021年4月当時)
  - ✓ ファームウェア解析により発見した脆弱性を報告(CVE取得数24件)

- **パスワード設定不備以外の脆弱性についても注意喚起対象とすべきではないか？**

ベンダ	脆弱性	影響を受けるバージョン
PaloAlto Networks	CVE-2019-1579	GlobalProtect SSL VPN 7.1.x < 7.1.19 GlobalProtect SSL VPN 8.0.x < 8.0.12 GlobalProtect SSL VPN 8.1.x < 8.1.3
Fortinet	CVE-2018-13379	FortiOS 6.0.0 - 6.0.4 FortiOS 5.6.3 - 5.6.7 FortiOS 5.4.6 - 5.4.12
Pulse Secure	CVE-2019-11510	Pulse Policy Secure 5.1R1 - 5.1R15 Pulse Policy Secure 5.2R1 - 5.2R12 Pulse Policy Secure 5.3R1 - 5.3R12 他

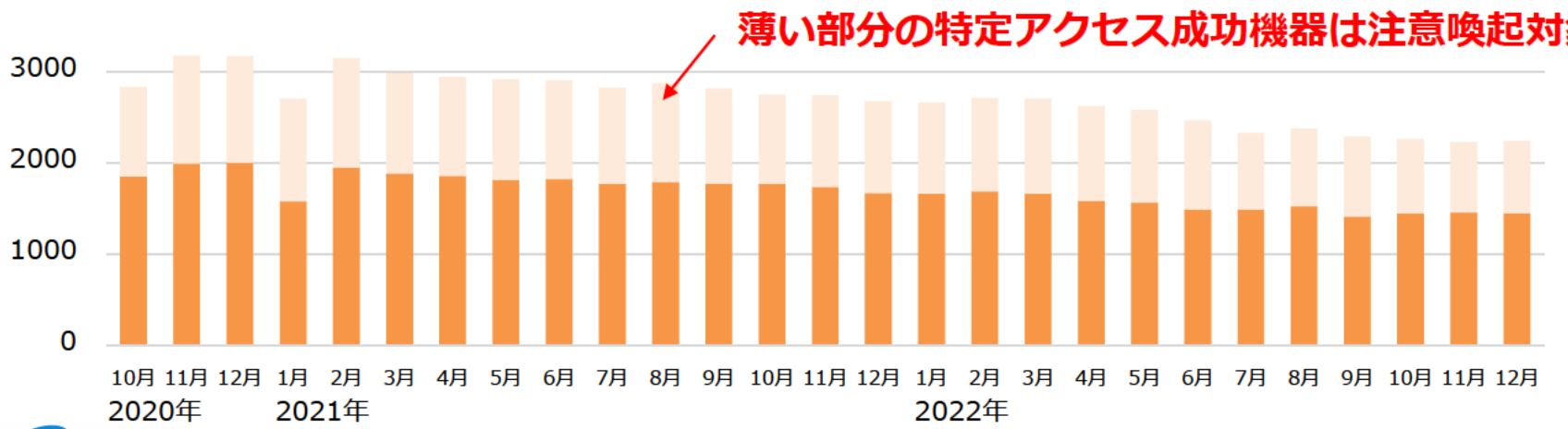
非公開情報

VPN脆弱性と影響を受けるバージョン機器の台数と機種分布

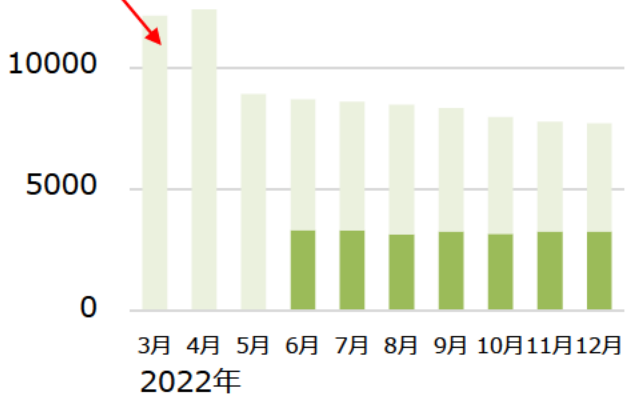
非公開情報

課題(1)：注意喚起対象外となっている機器への対処②

- **現状のNOTICEでは機種特定できない機器は注意喚起外**
  - ✓ 特定アクセスに成功した機器のうち約3割は機種特定が困難
- **機種特定の精度向上が一つの課題**
  - ✓ 様々なプロトコルのバナー情報を収集し特定に活用。実機検証によるシグネチャ作成。
- **ログイン可能な状態＝高リスクとして一律で注意喚起対象とすべきではないか？**
  - ✓ ユーザへの対処方法の案内についても検討が必要(各機器向けの対処マニュアルが作れない)



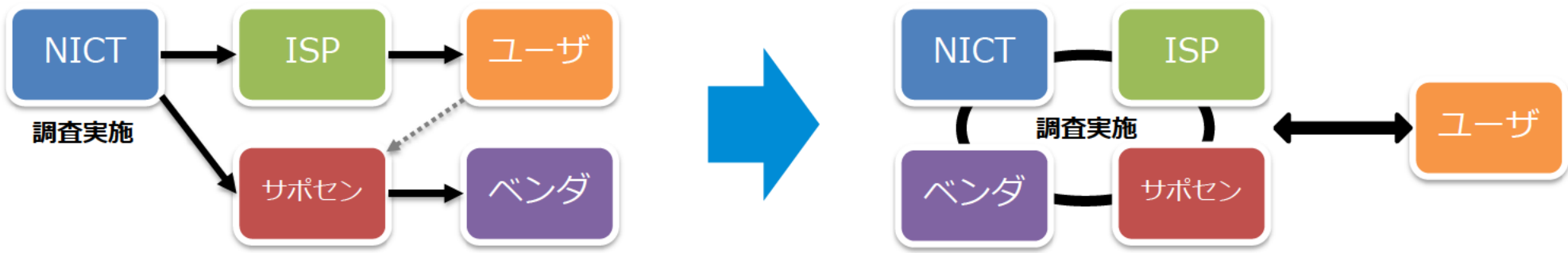
Telnet/SSHの調査結果の推移(月毎)



HTTP/HTTPSの調査結果の推移(月毎)

課題(2)：マルチステークホルダー・プロセスの実現

- **現状のNOTICE調査はNICT単独で実施しており、情報共有は限定的**
  - ✓ ISPはNICTから調査結果の通知のみを受け取る（NICT→ISP）
  - ✓ 機器ベンダはサポートセンターから問合せのみを受ける（サポセン→ベンダ）
- **各ステークホルダーが調査に主体的に関与できる体制構築が必要**
  - ✓ 各ステークホルダーが調査に関わることで迅速かつ詳細な情報共有が可能
  - ✓ ISP管理ルータの対応や、ベンダによる修正ファームウェアの提供など迅速な対処の実現
  - ✓ **IoT機器のセキュリティ確保に向けたマルチステークホルダー・プロセス**の実現



片方向な通知・問い合わせの運用体制

各ステークホルダーが直接関与する運用体制