戦略的イノベーション創造プログラム（SIP）　【富士通】

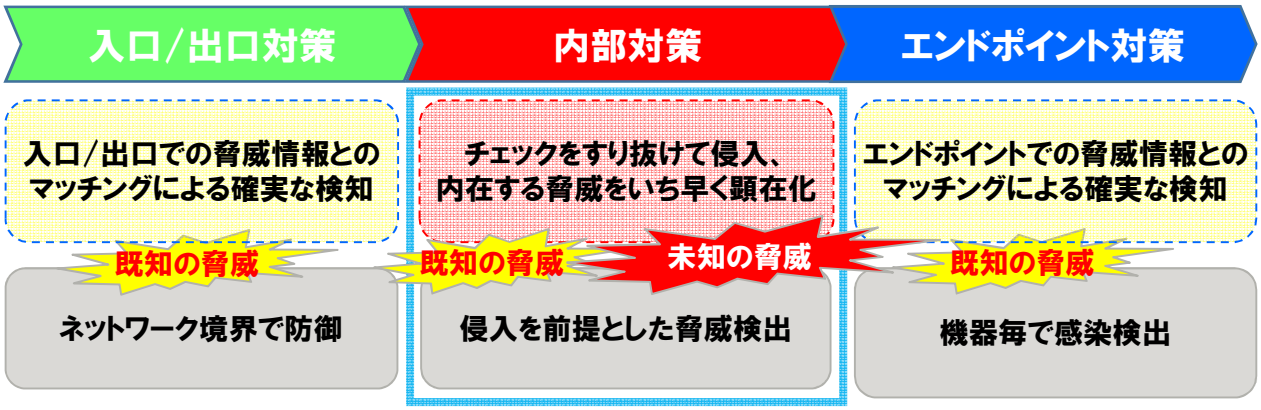
1－2　内在する脅威の早期顕在化にて業務影響を最小化

動作監視解析技術

既存のセキュリティ対策をすり抜けた内在する脅威をいち早く顕在化させ、脅威を監視・分析する高スキル業務を支援

■ 入口/出口脅威対策等を補完（多層で防御）する内部対策技術

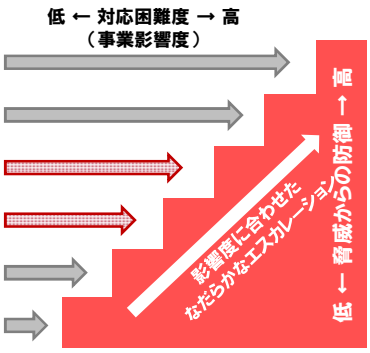
入口/出口対策、エンドポイント対策をすり抜けた内在する脅威の顕在化スピードをアップさせ、脅威レベルがエスカレーションされる前に捕獲する多層対策技術



■ 脅威を監視・分析する高スキル業務を支援

内在する未知の脅威の増加に伴い、Level-2/3の高スキル業務も増加
Level-1技術者にてLevel-2/3の業務ができるようシステムにて支援

脅威検知レベル（定義）		対策判断者	対策の観点
Level-5	業務サービスの異常検知	事業責任者 経営者	事業継続（BCP）
Level-4	業務システム全体の健全性阻害の検知	リスク委員会 （CISO）	システムの健全化
Level-3	内部ネットワークにおける異常拡散（侵入深化）の検知（ex. C&Cの対策）	CSIRT	システムの安定化
Level-2	外部ネットワークとの異常通信（C&Cサーバ通信）の検知（ex. C&Cの存在、情報漏洩）	セキュリティエキスパート（SOC）	影響範囲の特定
Level-1	内部ネットワークにおける通信変化を検知 （ex. C&C通信の可能性と対象領域）	ネットワークオペレータ（NOC）	被害の特定・除去
Level-0	外部ネットワークからのセキュリティ脅威の通知 （ex.アタック発生）	ツール（機器）	被害の特定・除去



■ 既存技術との違い

大規模ネットワークにおいて事前学習を必要としない数理モデルを適用

技術要素	既存技術	本研究テーマ技術
検知手法	過去挙動との差分	他機器挙動との差分
検知モデル	機械学習（事前学習要）	数理モデル（事前学習不要）
適合ネットワーク	小規模～大規模	大規模
監視対象通信	ネットワーク毎の監視	旧機器～仮想化混在に対応

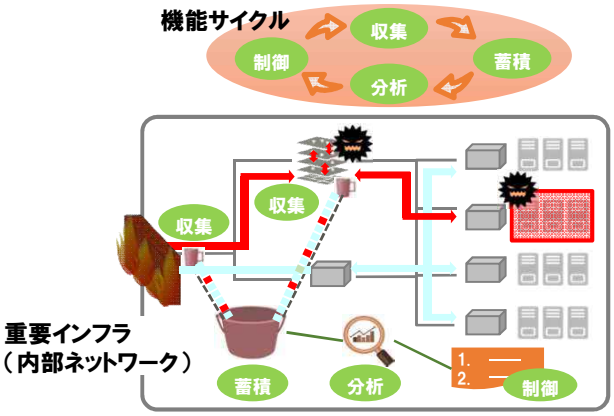
戦略的イノベーション創造プログラム（SIP）　【富士通】

1－2　内在する脅威の早期顕在化にて業務影響を最小化

動作監視解析技術

既存のセキュリティ対策をすり抜けた内在する脅威をいち早く顕在化させ、脅威を監視・分析する高スキル業務を支援

内部対策の機能サイクルと配備



技術ポイント

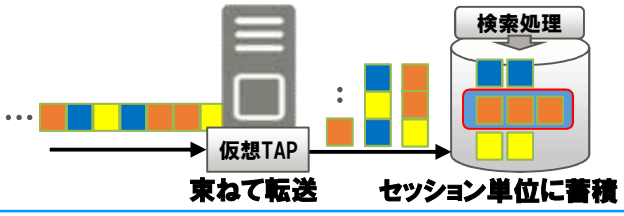
物理/仮想が混在する大規模ネットワークにおいて収集、蓄積、分析、制御の4機能サイクルを実現

① 仮想ネットワークから10Gbpsの高速でキャプチャするTAP収集技術
② 100Gbps対応高速・大容量蓄積技術
③ 事前学習を必要としない数理モデルによる分析技術
④ 脅威対策の高スキル業務を支援する制御技術

仮想ネットワークから通信を高速キャプチャ・蓄積する技術

収集　蓄積

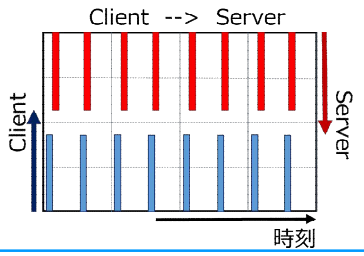
- 仮想スイッチへのアドオン技術により、高速パケットをキャプチャ、複数のパケットを束ねて転送することで仮想スイッチの輻輳回避
- セッション単位でのディスク書込み・読込みにより高速アクセスを実現



正常通信の中に紛れた不審な通信を検出する解析技術

分析

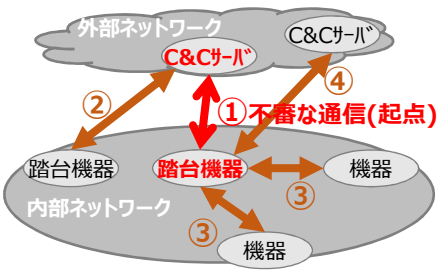
- 通信の規則性に着目（右図）、送受信相手の種類や取次状況を指標化、正常通信との識別性能を向上
- 独自の閾値調整手法（特許出願中）により、即時性の向上と精度低下の抑制を両立
- 既存セキュリティ技術で見過ごされていた、不審な通信の特定に成功（NEDO、富士通、NII　2019年11月29日プレス発表）



システムにて影響調査範囲を自動抽出

制御

- 不審な通信と相関関係にある通信をシステムにて分析・可視化することで脅威拡散被害の調査範囲を抽出し、オペレータの調査稼働を軽減



①検知した不審な通信（1次脅威）
②C&Cサーバとの通信（2次脅威）
③踏台機器との通信（2次脅威）
④SBY C&Cサーバとの通信（2次脅威）

製品展開予定

製品化予定：収集／蓄積技術 2019年度、分析／制御技術 2020年度

問合せ先：ネットワークソリューション事業本部　044-280-9861　fj-ci-procontact@dl.jp.fujitsu.com