戦略的イノベーション創造プログラム（SIP）

【日本電信電話】

1－1　サーバ機器の改変を常時検知して重要インフラを保護

真贋判定技術

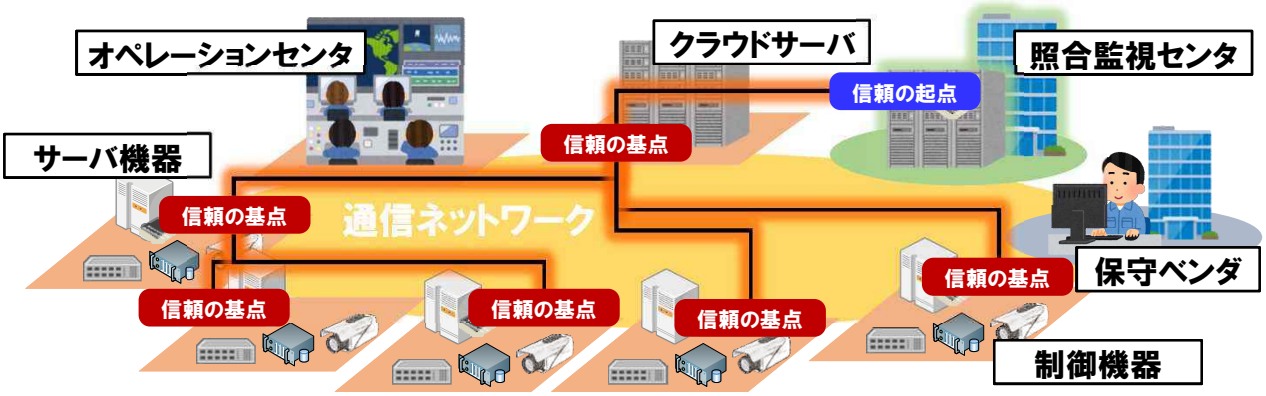
システムの不正な改変を常時検知して、バックドア通信などの異常な動作を阻止します

特長

① **システムの不正な改変の常時監視と記録保護**
システムの改変事実を常時検知して、改変に起因する異常な動作を阻止します（リアルタイム監視・防御技術）。
本技術の動作検査、及び監視記録の破壊対策等により安全確実な監視が可能です（セキュアレコーディング技術）。

② **効率的かつ確実かつ簡単な導入・運用**
本機能に必要な設定は機器間で安全に共有でき、かつ多くの機器で構成されるシステムにも効率的に導入できます（セキュアコンフィグレーションシェアリング技術）。
機器のソフトウェア構成等に応じて、本機能に必要な設定を自動調整できます（自動コンフィグレーション技術）。

導入イメージと差異化ポイント（高いサイバー攻撃耐性を備えた“きめ細かな完全性証明技術”を実現）



安全確実な改ざん検知
世界標準の最新セキュリティチップ（TPM2.0）と暗号技術を駆使して、監視記録の不正な改変などを検知し、安全確実な監視機能を実現

大規模システム全体の監視
数百～数千台レベル、1台あたり数十万の大量ファイルからなるサーバ機器に対応し、設備全体の真贋を判定可能にする「信頼の連鎖」を実現

ライフサイクル全体を監視
サーバ機器の起動から運用に至るまで、リアルタイムにソフトウェアの完全性を監視

実用化・事業化に向けた計画

	2017年度	2018年度	2019年度	2020年度～
研究成果普及	事業者提案	技術検証	試験導入 ⇒ 商用導入	
	先行導入実績をフィードバックしつつ導入拡大		重要インフラ分野展開（個別SI型）	
さらなる展開施策		OA系等の重要インフラ分野以外にも展開		既存製品連携によるソリューション化
			設備共用型による導入を実現	認証制度／照合監視センタサービス

戦略的イノベーション創造プログラム（SIP）　【日本電信電話】

1－1　サーバ機器の改変を常時検知して重要インフラを保護

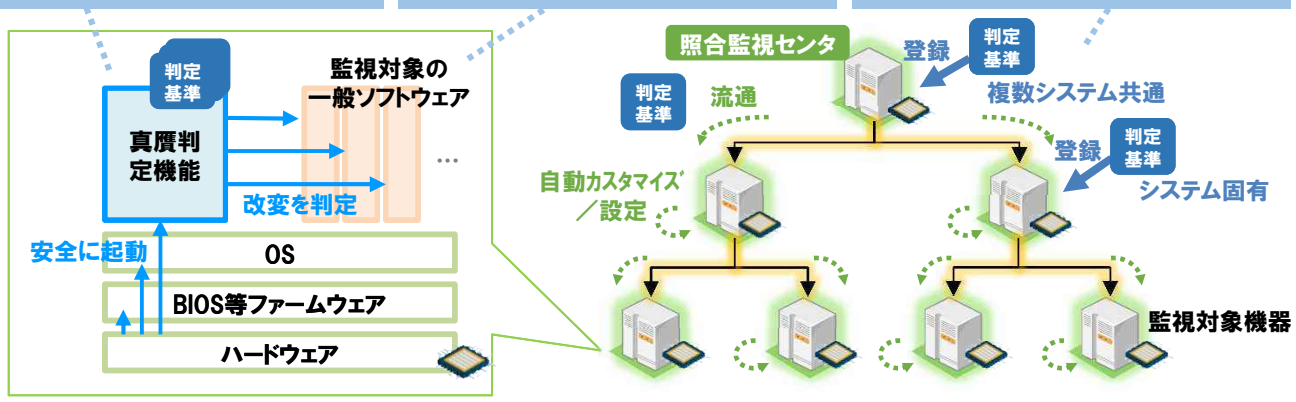
本研究開発テーマの背景

機器の配送、導入、保守を契機とした人為的改変や高度なマルウェアなどによって、バックドアを持つ不正な機器が重要インフラに混入するリスクが高まっています。特に、日本国内では東京2020オリンピック・パラリンピック競技大会に向けてそのような脅威がさらに高まると予測されており、2020年には、ファイアウォールを導入するような従来の追加型セキュリティ対策だけでなく、重要インフラ設備自体のセキュリティ強度を根本から高める新技術が必要な時代が到来すると考えられます。

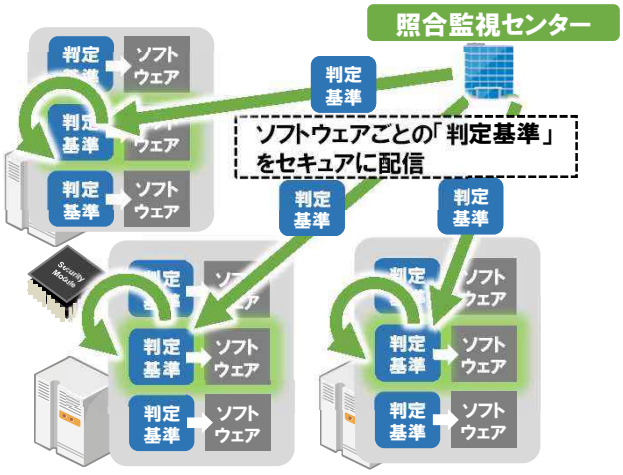
本技術の動作概要

3つの特長

真贋判定機能を安全に起動　**判定基準と比較して改変を判定**　**判定基準の安全な取得・自動設定**



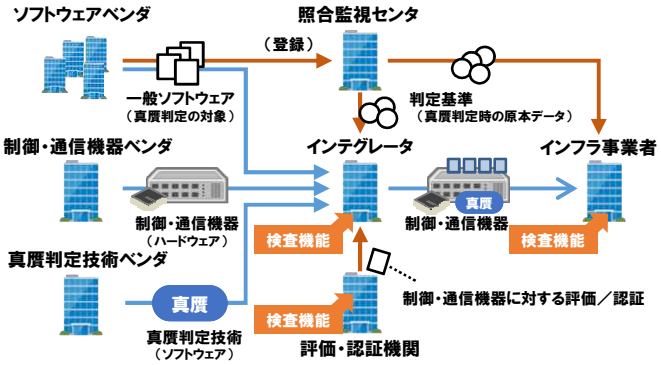
大規模システムの安全なアップデートが可能です



ソフトウェアごとの「ルール」に基づく自動設定

信頼の連鎖によって判定基準を共有し、機器ごとの差異には判定基準の自動設定で対応できます。

サプライチェーン上での検査機能を提供します



制御通信・機器の導入プロセスにおける検査

上記のような制御・通信機器のサプライチェーンにおいて、「インテグレータ」「インフラ事業者」「評価・認証機関」のそれぞれが、真贋判定技術が正しく導入され、かつ制御・通信機器の改変がないことを検査できます。

既存技術との比較

	本技術	A社製品	B者製品	C社製品
監視記録の保護	○	×	×	×
大規模システムへの導入のしやすさ	○	△	×	-
リアルタイム監視	○	△	△	×
改変ファイルの実行阻止	○	×	×	×