未来の原動機となるセキュリティ

豊かな社会をつくるIOWN（Innovative Optical and Wireless Network）時代のセキュリティR&Dを説明します．私たちはセキュリティを「人やアイデアを動かす」存在へ変えていきます．新しいセキュリティは人・組織・社会で多様なセキュリティモチベーションを解決し，アイデアや計算資源をダイレクトに仕事に変え，永く途切れなく保ちます．私たちはこれを，理論，データドリブン，コミュニケーションの3つを柱にした研究開発で実現します．

ひらた　しんいち
平田　真一[†1]　　たかはし　かつみ
高橋　克巳[†2]

NTT社会情報研究所　所長[†1]
NTT社会情報研究所[†2]

未来の原動機

私たちは30年以上にわたって通信と情報のセキュリティを考え続けてきました．暗号によってどことでも安全に通信ができるようになり，インターネットができました．セキュリティ対策によってどこにでも安全に情報を置くことができるようになり，Webやクラウドができました．ただし，セキュリティ対策によって私たちは日常を守れるようになりましたが，それでもセキュリティ脅威に不安を抱え，対策に腐心せざるを得ないことは見過ごせない問題です．

「IOWN（Innovative Optical and Wireless Network）時代」では，従来の限界を超えた情報通信技術により，さらなる豊かで満たされた生活が実現されます．私たちは，セキュリティをその原動機にしたいと考えています．

セキュリティの必要性は論を待ちません．セキュリティ・バイ・デザインの考え方が浸透しつつありますが，これはセキュリティが人や社会の健全な活動にそもそも必要だったことを示しています．他方，セキュリティコストやセキュリティ疲れという言葉も存在しています．健全な活動に必要なものが義務や苦労であってよいのでしょうか．私たちは，そうであってはならないと考えます．シンプルにセキュリティは明るい未来をもたらすべきです．

私たちは，セキュリティ技術が「必要だが難しい」現状を，以下のような考え方の研究開発で変えていきます．

・あらゆる業務や生活に幅広く役立つ（広範囲）
・アイデアや計算資源をダイレクトに仕事に変える（効率）
・途切れなく保つ（継続）

本稿はIOWN時代のセキュリティR&Dの考え方を，広範囲，効率，継続の観点から説明し，私たちが注力するセキュリティ技術を概説します（**図1**）．なお本稿で論じるセキュリティは，いわゆる情報セキュリティで，保安全般や治安は意図しないものの，プライバシや倫理といった周辺領域まで含めます．

セキュリティを広範囲に

これまでセキュリティは，ともすると「特定のシステムのセキュリティが破られない」ことと信じられてきました．私たちはセキュリティをあらゆる業務や生活に役立てられるものとするため，セキュリティ研究開発を対象とモチベーションの2点から広範囲なものに進化させます．

■広範囲1：セキュリティ対象

私たちは，セキュリティが守る対象を「特定のシステム」（情報資産）だけに限定せず，「企業・組織」「人」「社会」も含めたいと考えています．

・情報資産

セキュリティの対象は情報資産と呼ばれてきました．企業の顧客情報，販売情報，技術情報などがそれにあたります．情報資産の保護は，その記録・保存形態に依存するので，情報資産を収める形態も保護対象となります．代表的な形態には，ファイル，紙・ストレージ・伝送路等媒体，スマートフォン・コンピュータ等ハードウェアシス

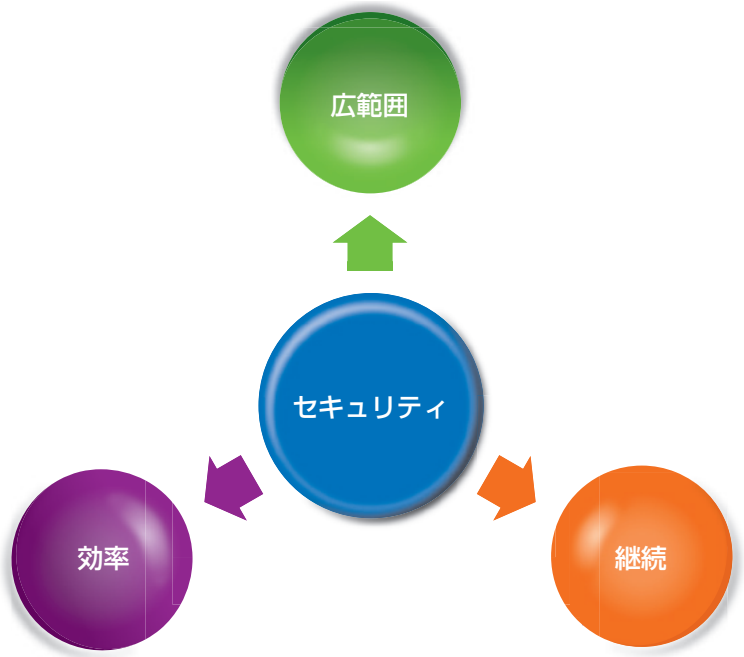

図1　IOWN時代のセキュリティR&Dの考え方

テム，電子メール・データベース・AI（人工知能）等ソフトウェアシステム，などがあり，そこにドローン・産業用ロボット等IoT（Internet of Things）機器らが加わっています．

・企業・組織への拡張

セキュリティの対象は，企業・組織の活動の変化に応じて大きく変化することが予想されます．例えば，情報資産の形態の確定が困難になります．情報資産は社外ストレージに置かれ，企業間取引によって別組織の管理下に置かれ，さらに調達や生産のサプライチェーンでは，ある意味他人が将来自社の情報資産をつくっているとみなせるでしょう．IoT機器の導入により，情報資産形態はさらに流動的になります．

・人への拡張

人を仮に情報資産の媒体とみなすと，かなり機密性の高い媒体といえます．気持ちが表情に出るという言葉がありますが，表情から顧客情報が漏れることはありません．他方，人は簡単に騙され，場合によっては裏切る存在でもあります．これに対して企業は研修や規則による対応を行っています．また，企業に限定されない人の活動の媒体にSNS投稿があります．SNSを介した情報事故は，漏洩，著作権侵害，さらに炎上などがあります．これに対しては，現在ほぼ個人の責任として放置されているのが実状です．人を対象とするセキュリティは，人をシステムとしてとらえた安全管理策では限界があります．

・社会への拡張

社会をセキュリティの対象にできるのかどうかは，確立した見解がないのが現状です．自動走行やモニタリングカメラのシステムは，社会レベルでシステム化が推進されているものです．これら「スマートシティ」には基本的なセキュリティの「約束事」（ポリシー）があるので，規模の問題はありますが，従来のセキュリティ対象の延長線上で考え得る問題です．他方，パンデミック対応はどうでしょう．接触確認アプリ等一部のものは明確なポリシー下で運用されましたが，多くのものの運用の「作法」は基本的に，自発的・自然発生的な情報のやり取りで合意され，社会全体が動いていると考えられます．この作法は倫理や慣習などと呼ばれるもので，その取り扱いには新しいアプローチが必要と考えています．

■広範囲2：セキュリティモチベーション

私たちはセキュリティが必要な理由（モチベーション）には，単なる情報漏洩だけにとどまらない幅広いインシデントの存在や，システム品質、法、倫理、慣習、社会目標などがあると考えました．

・インシデント

「情報漏洩を起こしてはならない」が，もっとも知られたモチベーションです．このモチベーションを核に，不正なアクセス，不正なソフトウェア，あるいは不正な入退室などのさまざまな脅威をふさぐ対応が行われるのは周知の事実です．しかし，私たちはこのインシデントを，「機密性・完全性・可用性の侵害」という考えにとらわれないことが重要だと考えています．例えば，プライバシがらみのインシデント（炎上）も注意すべきものです．これは情報漏洩ではなく，取得や利用目的の説明不足やルール違反によって生じるもので，セキュリティの周辺問題と考えられていました．では，AIの異常動作はどうでしょうか．AIの動作結果の内容は従来セキュリティの問題と考えられていませんでした．私たちは，対応すべき問題を，従来のセキュリティの枠で考えるのでなく，コンピュータがもたらす困りごと，プライバシやAIの問題にも拡張することが必要であると考えています．

・システム品質

システム開発におけるセキュリティは，重要インフラのような分野では高いレベルがあらかじめ要求され，セキュ

リティがモチベーションの一部になります．他方，セキュリティが暗黙の要求にとどまるシステムもあります．この場合ではセキュリティのレベルも暗黙のものとなり，対応は開発のコストとみなされてしまうこともあります．これは看過できない問題です．元来システムのセキュリティは必要なものなので，それがモチベーションから乖離するようであれば，その原因から根本的な解決が必要だと考えています．

・法律

法令遵守もセキュリティのモチベーションになります．日本では，サイバーセキュリティ基本法が国民にセキュリティの努力を求めています．企業にとっては，個人情報保護法の義務や不正競争防止法の前提としてセキュリティが求められます．私たちは，セキュリティ関連法制度を注視し研究開発に活かすだけでなく，制度のあり方の議論に関しても能動的であるべきだと考えています．

・倫理・慣習・社会目標

インシデントのおそれがなく，品質が一定に保たれ，さらに法に適合していても，セキュリティが必要だと感じる場合があります．それは，人々の中にある何らかの価値観やおそれに基づくもので，倫理や慣習や社会の目標などといった言葉で形容されます．私たちは，これらの存在をセキュリティのモチベーションの一部として取り扱うことを考えています．

原動機としてのセキュリティの効率

残念ながら業務のコストと考えられてきた可能性のあるセキュリティですが，私たちは新しくセキュリティの効率の概念を導入して，この状態を変えたいと考えています．効率とは，アイデアに関するものと，コンピュータ資源に関するものがあります．これらを最大限に活かしきるときに，セキュリティの効率は最大となります．

■効率1：アイデアをダイレクトに仕事に変えられる

アイデアの実現を邪魔しない，チャレンジの背中を押すセキュリティに取り組みます．アイデア実装時，セキュリティのための要件と実現方法の決定が必要になります．このプロセスの最小化が効率につながります．理想のイメージは，システムを開発したら，必要なセキュリティが意識せずビルトインされている状態です．要件の決定は通常，モチベーションで記載した要素すべて，インシデントの想定から法対応などの分析を経て行われます．実現方法の決定は，現実的にはセキュリティを一から構築することは少なく，用いる部品（ライブラリ）を調査して，そのセキュリティ機能を使うことで行われています．両プロセスの最小化，自動化に取り組みます．セキュリティの自動化は極めて困難なテーマですが，後述する理論アプローチ，データドリブンアプローチにより解決します．なお，セキュリティ要件と方法のベストカップリングを開発環境やユーザインタフェースとして提供できれば，この問題解決のショートカットになると考えられます．

■効率2：コンピュータ資源をダイレクトに仕事に変えられる

例えば現在のWebアプリケーションおいて，セキュリティ処理がオーバヘッドとなり，通信や画面表示が遅れるといったことはあまり考えられません．しかし，都市，交通等，社会インフラにかかわる大量のさまざまな機器がネットワークに接続されたIOWN時代では，それが無視できなくなると考えています．また，カーボンニュートラルの文脈においては，コンピュータや通信の資源を活かしきるセキュリティ処理が望まれます．私たちはIOWNオールフォトニクス・ネットワークに代表される最先端のハードウェアの特質を活かし，情報通信の体験を最大化するセキュリティに取り組みます．

セキュリティをより継続して

セキュリティは継続して保たれるべきです．セキュリティの攻撃と防御は連続的な情報処理技術の進展の上に乗っているため，継続的な研究開発を覚悟のうえ取り組んでいます．加えてセキュリティR&Dにおいて継続性が必要な理由があります．セキュリティ技術のコアは理論とデータです．前者の例に暗号が，後者の例にホワイトリスト・ブラックリストがありますが，それぞれに継続的な理論の積み上げ，データの積み上げが必要だからです．なおセキュリティ技術の連続性の一方，量子コンピュータという不連続な変化の到来も予測されています．私たちは継続を基本に，大きな変化にも耐える技術開発に取り組みます．

セキュリティ研究開発の新しい3つの柱

広範囲・効率・継続のセキュリティを実現していくために，私たちは次の3つの柱で研究開発を進めます（**図2**）．

■理論でセキュリティを保証する機構

暗号は適用したデータの機密性を理論的に保証します．理論的に安全が保証されたソフトウェアモジュールがあれば，そのモジュールにおけるセキュリティを心配する必要がなく，さらに理論的に安全なモジュールのみから，それらを正しく接続してシステムが構築できれば，そのシステム全体がセキュアと評価することができます．理論的に安全なモジュールを増やすことは，明らかにシステムのセキュリティ実現

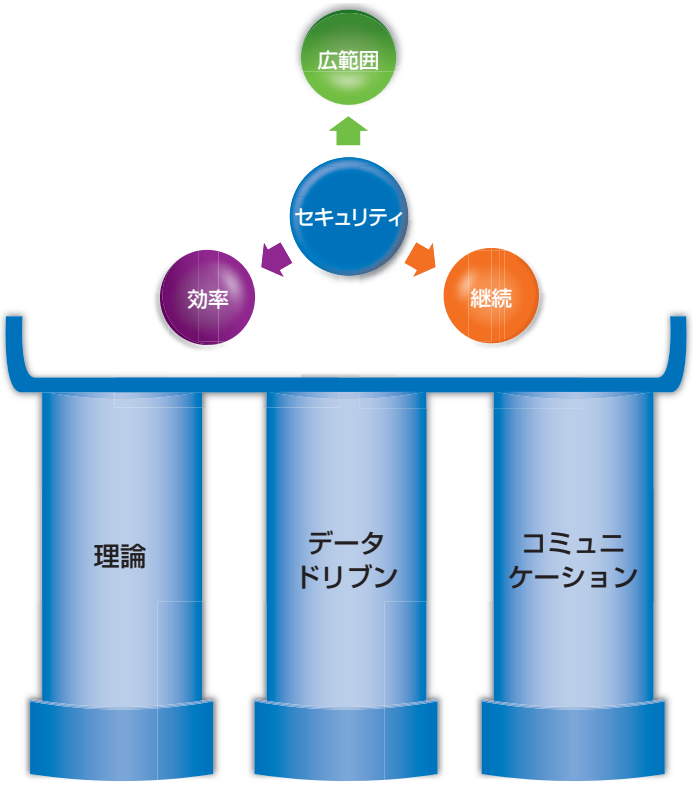

図2　セキュリティR&Dの3つの柱

に貢献します．セキュリティを保証する理論の代表は暗号ですが，暗号や暗号プロトコル，あるいはフォーマルメソッドなどを含む数学が基礎を成します．また，物理学にも着目しています．量子情報処理が実現されれば，新しい盗聴や偽造の防止が通信だけでなくデータ処理にも期待できます．

■データドリブンでセキュリティを保証する機構

すべての対象を理論的にセキュリティ保証することは難しく，あるものはデータドリブンに保証する必要があります．例えば複数の機器から構成されるインフラシステムであれば，構成するすべての機器に対して状態を記録し，リスクを評価するという考え方があります．この作業はそのサプライチェーンおよび運用の全体を通じて行います．この状態の記録がデータであり，その評価がデータドリブンと呼ばれるものです．評価結果の中で他の時間や環境でも利用できるものは，それを整形して再利用します．データドリブンは，インフラシステムだけでなく，任意のセキュリティ対象に関して適用可能な方法です．この再評価のためのデータを私たちはトラストデータと呼んでいます．トラストデータには，安全性に関してポジティブな評価もネガティブな評価も含みます．これらを使って，データドリブンなセキュリティ保証が可能になります．なおこのトラストデータは，全体的で絶対のものではなく，局所的かつ公平なものを志向しています．

■セキュリティの前提の合意を形成するコミュニケーション

理論とデータドリブンという継続的アプローチに加えて，私たちが新たに強く必要性を認識しているのが合意形成に関するコミュニケーションアプローチです．セキュリティ実施の前提となるポリシー等「決めごと」の決め方から検討する必要があると考えました．何をすれば安全なのか．何をすれば人々が不安なく活き活きと活動できるのか．「セキュリティモチベーション」を確定させる決めごとは，狭義セキュリティを，倫理・慣習・社会目標へ広げれば広げるほど，当事者間のコミュニケーションで合意形成することが重要と考えました．セキュリティの決めごとを当事者間で合意できる機構，および合意した決めごとどおりに運用が行われているかの評価ができる機構についての検討を進めていきます．

おわりに

IOWN時代のセキュリティR&Dの方向性を広範囲，効率，継続の考え方から再整理し，取り組む技術を理論，データドリブン，コミュニケーションの3軸で示しました．セキュリティに不安がない社会を，高い倫理観とテクノロジで実現していきます．

（左から）平田　真一/ 高橋　克巳

世の中のあらゆる情報を安全・公平に活用することにより多様な社会価値を創出し，誰もがその人らしく暮らせる豊かな社会を実現することをめざして研究開発を進めています．未来の原動機となるさまざまな技術にご期待ください．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab @ hco.ntt.co.jp