次世代ＩＰインフラ研究会
セキュリティＷＧ（第３回）議事要旨（案）

１　日　時：平成１７年2月１７日（木）１６：００～１８：００
２　場　所：総務省　低層棟１階　共用会議室１
３　出席者：
〔ＷＧ構成員〕
新井構成員、飯塚構成員（サブリーダー）、歌代構成員、内田構成員、笠原構成員、加藤幹之構成員、加藤佳実構成員、桑子構成員、笹木構成員、佐々木構成員（グループリーダー）、篠田構成員、武智構成員（與儀代理）、手塚構成員、永瀬構成員、南浮構成員、藤谷構成員、星澤構成員（池田代理）、松島構成員、森構成員
〔ゲストスピーカー〕
村上シニアコンサルタント
〔総務省〕
有冨総合通信基盤局長、江嵜電気通信事業部長、金谷電気通信技術システム課長、吉田情報セキュリティ対策室長
〔事務局〕
秋本データ通信課調査官、山路データ通信課課長補佐

４　議　事
松下電器産業　加藤佳実構成員より、資料ＷＧ３－１（ネット家電のインターネット接続に伴うセキュリティの確保について）に沿って説明があった。主な意見は以下のとおり。

○：「SPREAD」は、Telecom-ISAC と JNSA が中心となって、昨年 6 月に立ち上げたものだが、情報家電を含めた検討はなされていない。他社や団体間でどのように連携を取っていくべきかについて話が出ている。

○：ホームゲートウェイは、複数メーカーの機器が接続されることは想定されており、なるべく標準的な技術に対応するように検討されている。ただ、各社独自の味付けもあり、すべてメーカーの機器に完全に対応することは難しいと思う。

○：情報家電はソフトウェアではなく、PL 法が適用されるため、メーカーやベンダーの敗訴する率が高くなる。どこまでセキュリティを講じれば免責されるかについて安易なガイドラインを作ってしまうと、ガイドラインを作った組織や団体も賠償責任を負うことになりかねないため、あまり緩めない方がいいのではないか。現時点では１万年に１回の確率で故障すると思われているようなことが、来年には１年に１回起こるような事態も考えられるので、確率論ではない別の切り口で検討することが必要。

続いて、日立製作所手塚構成員より、資料ＷＧ３－２（情報家電機器認証技術）に沿って説明があった。主な質疑は以下のとおり。

○：外部から情報家電を立ち上げることが出来るようにするためには、情報家電が常に電源 ON にしている必要があるが、京都議定書の関係もあり省エネ対策が必要。また、ＰＣは通信をしているときランプが光るなど気付きやすいと思うが、情報家電では潜り込まれたら気付かないのではないか。知らないうちに通信分、待機分の電力料金を支払うことになるので、その旨を重要事項として知らせるべきではないか。

○：不正侵入対応としてゲートウェイを置いて、家庭内の情報家電を守るという議論がある。現状では、家をみると殆ど家電の電源が入っており、それが一般的と思うが、省エネも検討しなければならない。

○：リモートメンテナンスを考える場合、数百万、数千万の個々の情報家電が同時にデータのダウンロードを行うことは可能なのかという問題もある。個々の機器で難しいということであれば、ゲートウェイに蓄積するなどの方法も考えないといけない。

○：情報家電にオープンアーキテクチャが入ってくるのは課題。これまでは自社独自で作り、責任分担も明確だったが、これからは情報家電に載るソフトのアップデート等をダウンロードでやるのか、それともソフトを配る方法で対応するのかは課題。これは情報機器一般にあてはまることで、それらと合わせて考えることが必要。

○：オープンアーキテクチャだから危ないというわけではない。リバースエンジニアリングを使って悪さをする者もおり、仕様が分かるのは全てだめと考えてもいいと思う。

○：家庭のネットワークを１つの固まりとして考え、ホームゲートウェイで外部と内部を分けるという考え方もある。ホームネットワークをクローズにしてしまい、家庭のネットワークを安全にする方法や、エンド－エンドで家庭内の個々の機器まで入り込む方法などもあり、議論し相場観を合わせる取り組みも必要。

○：認証をきちんとやらないといけないことは事実だが問題もある。個々の機器ごとに認証するようになると、ロケーションの情報などメートル単位で正確に把握できるようになり、個人情報プライバシーも問題になる。

○：脆弱性は、オープンアーキテクチャだけの問題ではない。OS を含め機器認証は重要であるが、機器認証に統一的な ID が必要かどうかについては、今後、検討し

ていくべき。

○：識別番号は、機器と機器が違うということを判別するだけで、真性なデバイスか、ソフトが動いているかということとは別と思う。

続いて、ゲストスピーカーのラック村上氏より、資料ＷＧ３－３（セキュリティベンダの情報家電セキュリティに対する取り組み）に沿って説明があった。主な質疑は以下のとおり。

○：情報家電のトラヒックの問題に関連して、銀行の大規模オンラインシステムでは、何百台ものサーバを起動する際、いきなり主幹電源を入れるようなことはせず、少しずつ立ち上げていき、全体を立ちあげる。情報家電自体が持つべき対策なのか、又は情報家電を運用していく仕組みの中での対策とするのかは議論が分かれるところではある。

○：ネットワークのサーバ検査や企業イントラネットの PC の脆弱性検査などは、今までは一子相伝のようなところもあったが、最近はマニュアル化に努めている。しかし、サーバや PC の脆弱性検査については、整備が進みつつあるが、家電は家電の特異性があるので、誰もが出来るというようなところまでは出来ていない。

○：ホームネットワークは外部から守るだけではダメで、内側を向いている IDS や、家電が異常な動作をしだしたら、それを切り離すということをやることも必要。家電を入れるときの検疫というような一過性のものではなく、常にチェックするようなアプローチが必要。

○：どこまでエラーが許されるのかという許容範囲のようなものが通常の家電でも存在するはず。情報家電も、どこまでが PL 法の許容範囲内なのかある程度考えておかなければならない。

○：情報家電について議論する際は、ユーザーの声をどれくらい反映しているのかという問題がある。メーカーも消費者も女性を入れる必要があるのではないか。

○： 災害時、電話回線は（回線が）集中してダウンしないように徐々に復旧させていくが、情報家電が数多く普及すると、難しいのではないか。トラヒックが急増したときにそれを別のところに貯めておくような仕組みについて通信業界全体で考えてほしい。

○：脅威に関して、すべて同じ基盤の上でシステムを構成すると、システム自身の脆弱性が増すので、１つのネットワークに全てが依存することのないような方策を

考えるべきではないか。

○：停電復旧後に大量のトラヒックが発生するという話について、ホームゲートウェイが、情報家電から外部向けのトラヒックを隔離するという対策もあり得るのではないか。

以上