推薦論文

PKIの証明書失効に必要な通信量の確率論的評価

田中直樹[†] 飯野陽一郎[†]

公開鍵認証基盤（PKI）では，Certificate Revocation List（CRL）を使って，証明書の失効を確認する方法が提案されている．CRL は Certificate Authority（CA）ごとに発行されるが，検証者は全 CRL のうちの必要な CRL だけを取得すればよいこと，および 1 度取得した CRL を保存しておくことで，同一の CRL の取得はたかだか 1 度ですむことにより，CRL 取得に必要な通信量が減ることが期待される．本稿では，PKI での主な証明書の失効方式である完全 CRL 方式と δ-CRL 方式について，確率論的な取扱いにより，検証者が同一の CRL の取得をたかだか 1 度しか行わない場合の通信量の理論式を導いた．その評価結果から，検証者が必要な CRL だけを取得することで通信量が下がるのは，認証頻度が CRL の発行頻度と CA 数の積に比べて十分低い領域に限られ，認証頻度がそれより高い領域では，通信量はすべての検証者がすべての CRL を取得するのと同等で，Entity 数の 2 乗に比例することが分かった．また，δ-CRL 方式については，認証頻度が十分大きい場合には，通信量を最小化する base-CRL と δ-CRL の発行間隔の比が CA の数とは無関係に決まることを示す．

Volume of Communications Necessary for Certificate Revocation in PKI Estimated Based on Probability Theory

Naoki Tanaka[†] and Yoichiro Iino[†]

In Public Key Infrastructure (PKI), it is proposed that a verifier checks a validity of certificate by Certificate Revocation Lists (CRLs) issued by Certificate Authorities (CAs). A verifier obtains only a necessary part of CRLs and, by preserving CRLs once obtained, a verifier needs not obtain the same one more than once. Therefore CRL is expected to reduce the volume of communications necessary for certificate revocation. In this paper, for full-CRL and δ-CRL methods, we take into account the fact that one CRL is obtained by one verifier at most once and we derive the volume of communications necessary for certificate revocation based on probability theory. The result shows that the effect that a verifier obtains only a necessary part of CRLs reduces the volume of communications only when the frequency of authentications is sufficiently lower than the product of the frequency of CRL issuances and the number of CAs. When the frequency of authentications is higher than the product, the volume of communications becomes comparable to that in the case that all verifiers obtain all CRLs and is proportional to the squre of the number of all entities. Furthermore, for the δ-CRL method, it is proved that there exists an optimal ratio between a frequency of base-CRL issuances and a frequency of δ-CRL issuances independent of the number of CAs if the frequency of authentications is high enough.

1. はじめに

公開鍵認証基盤（Public Key Infrastructure，PKI）では，証明書の有効期間内に，entity が秘密鍵を紛失した場合や，漏洩させた場合には，ある秘密鍵の持ち主がある ID の entity であることが成立しなくなるので，証明書の失効を行う必要がある．証明書発行者（Certificate Authority，CA）は，その場合には，失効された証明書の証明書番号を検証者に通知する．以下では 1 つないし複数の失効された証明書の証明書番号を失効情報と呼ぶ．失効情報を通知する最も簡単な方法は，証明書が失効されると同時に，その失効情報を検証者全員に通知する方法である．しかし，この方法には以下の大きく 2 つの問題がある．

† 株式会社ソニー・コンピュータエンタテインメント
Sony Computer Entertainment Inc.

本論文の内容は 2003 年 7 月のコンピュータセキュリティ研究会にて報告され，CSEC 研究会前主査 により情報処理学会論文誌への掲載が推薦された論文である．

問題 1 検証者は認証することのない entity の証明書の失効情報まで受け取ることになる．

問題 2 証明書失効の発生は予測不可能なので，検証者は常時失効情報を受け取れるようにすることが必要になる．

これらの問題に対して，検証者が認証で必要になったときに必要な失効情報を取得する方法が提案されている．それを，ここでは便宜上，オンライン型，オフライン型の 2 つに分けて説明する．

オンライン型では，失効情報は専用のサーバで管理されていて，検証者は entity の認証時に，その証明書の失効を，サーバに問い合せて確認する．この場合，entity の認証がつねに entity，検証者，サーバの 3 者間の処理になるため，認証の応答性や，可用性の確保が困難になる．本稿では以降，この方法は取り扱わない．オンライン型には Online Certificate Status Protocol（OCSP）[1]，Naor らの方式[2]，Certificate Revocation System（CRS）[3] などがある．

これに対してオフライン型では，失効情報は失効されかつ有効期限前である証明書の番号のリスト，Certificate Revocation List（CRL）として CA から発行され，検証者がアクセス可能な Repository と呼ばれるサーバで公開される．検証者は 1 度取得した CRL を保持しておくと，次に新たな CRL が発行されるまでは，保持している CRL を使って証明書の失効を確認できるので，entity の認証を entity と検証者の 2 者間で処理できる．CRL の詳細は，たとえば X.509 [4] や RFC3280 [5] で規定されている．CRL の代表的な運用方式としては，完全 CRL 方式，δ-CRL 方式がある．

完全 CRL 方式 CRL に失効情報として，CRL の発行時点で，失効されていてかつ有効期間内であるすべての証明書の番号を含める方式である．このような CRL を，以下では完全 CRL と呼ぶ．この場合，完全 CRL の発行間隔が短くなると，新旧の完全 CRL 間の差分が小さくなり，このような CRL を発行のたびに取得するのは効率的ではないという問題がある．

δ-CRL 方式 比較的長い時間間隔で，base-CRL と呼ばれる完全 CRL と同じ情報を含む CRL を発行し，base-CRL の発行の間では，δ-CRL と呼ばれる base-CRL より短い発行間隔の CRL を発行する方式である．δ-CRL には base-CRL の発行以降に，新たに失効されかつ有効期限前である証明書の番号だけが含まれる．これによって，発行間隔が短くなった場合の完全 CRL 方式の問題を緩和している．

PKI 運用でシステム全体に発生する通信量について考える．CRL のサイズは，おおよそ失効された証明書の数，すなわち entity 数と証明書の失効頻度の積，に比例する．CRL は認証頻度が高ければすべての検証者が取得するので，最悪の場合，CRL 取得に必要な通信量は，entity 数と検証者数と証明書の失効頻度の積に比例する．これに対して，認証自体に必要な通信量は，entity 数と entity の認証頻度の積に比例する．特に entity どうしが PKI で認証を行う場合には，entity 数と検証者数は一致し，CRL 取得に必要な通信量は entity 数の 2 次に比例するのに対して，認証自体に必要な通信量は entity 数の 1 次に比例する．entity 数は非常に大きくなりうるので，前者の通信量が支配的になる場合，ネットワークの通信容量をユーザ数に比例するように確保すれば足りるとする現在の見積りでは問題が生じうる．我々はこの点に注目し，本稿では CRL 取得に必要な通信量の見積りを行い，entity 数の 2 次に比例する振舞いがどのように現れるかを調べる．

National Institute of Standards and Technology（NIST）による PKI の運用に必要な通信量の見積り[6] では，検証者が entity を認証する際に，一定の割合で CRL を取得すると仮定して，通信量を見積もっている．しかし，この方法では，同一の CA に属する entity を複数回認証する場合には，同一の CRL を複数回取得することになり，同一の CRL の取得はたかだか 1 回ですむ効果を取り入れることができなかった．また，entity を認証する回数（認証頻度）に対する CRL 取得に必要な通信量を考えると，認証頻度が十分大きくなった場合は，entity 数の 2 次に比例する通信量を再現するが，その振舞いがどの程度の認証頻度から顕著になるかは明らかでなかった．

本稿では entity どうしが認証を行う場合に，認証を行う entity が同一の CRL をたかだか 1 回しか取得しないことを確率論的に扱う方法を示す．それに基づいて，完全 CRL 方式および δ-CRL 方式で，CRL 取得に必要な通信量の認証頻度への依存性を評価し，entity 数の 2 次に比例する振舞いがどのように現れるかを明らかにする．

全体の構成は次のとおりである．はじめに本稿での評価モデルと評価項目，すなわち完全 CRL 方式，δ-CRL 方式での CRL 取得に必要な通信量を定義する．次に，評価項目の理論式の導出を説明する．つづいて理論式の評価と考察を行い，最後に本稿での結果をまとめる．

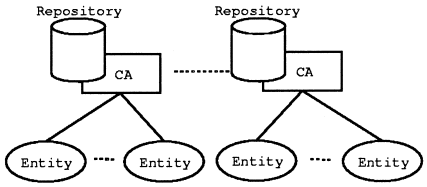

図 1 評価モデルの概要
Fig. 1 Overview of model.

2. 評価モデルと評価項目

2.1 評価モデル

評価モデルを**図 1** に示す．複数の証明書発行者（CA）と，各 CA に付随する形で Repository が存在し，CA から証明書を発行された entity が複数存在する構成である．それぞれの CA には，一定の数の entity が属し，entity の証明書の失効情報は，各 entity が属する CA が管理する．CA は，失効情報を CRL として発行して Repository に置く．改竄を防ぐために CRL には CA の電子署名が付加される．したがって，CRL の正当性を検証するためには CA の公開鍵が必要になる．CA の公開鍵と CA の関係も，証明書によって保証するために，CA が階層構造を構成し，上位の CA が下位の CA に対して証明書を発行する．ただし，CA は通常の entity よりも秘密鍵の管理を厳重に行っていると考えられるので，CA の証明書の失効は entity の証明書の失効に比べて十分に低い頻度でしか発生しないと仮定する．これにより，CA が階層構造を構成する場合であっても，CA の証明書の失効確認に必要な上位の CA が発行した CRL の取得で発生する通信量は，entity の証明書の失効確認に必要な CRL の取得で発生する通信量に比べて無視できる．したがって，CRL の取得に必要な通信量を考えるうえでは，図 1 のように，CA が階層構造を構成しないモデルで評価を行うことができる．

証明書は，認証を行う entity（以下では，検証者と呼ぶ）が認証を行うたびに，認証される entity（以下では，単に entity と呼ぶ）から送られる．entity の証明書から証明書を発行した CA，および対応する CRL の置かれている Repository を特定できるので，検証者は Repository から直接 CRL を取得できるものとする．検証者は CRL を用いて証明書が失効されていないことを確認した後，entity が対応する秘密鍵を持つことを確認することで，entity を認証する．

またこの評価モデルでは検証者はすべての entity を一様に認証するため，すべての CA の発行する CRL を同等の確率で取得する．これは現在一般的なサーバの認証と比べて強い仮定だが，対等な entity どうしの認証では妥当である．現在一般的なサーバの認証では，サーバは検証者すなわちクライアントをあらかじめ想定し，クライアントに便利な CA（たとえば日本のクライアント向けのサーバなら日本の CA）から証明書を取得することができる．しかし，entity どうしの認証では，entity の持つ証明書は検証者とは無関係に選ばれるからである．

2.2 通信量の定義

ここでは，完全 CRL 方式と δ-CRL 方式での，CRL 取得に必要な通信量を定義する．

完全 CRL 方式での CRL 取得に必要な通信量 システム全体で全検証者が全 Repository から取得するすべての完全 CRL のサイズの総情報量を，単位時間（1 日）あたりで平均した値（ビット数）とする．L_{CRL} で表し，単位は [bit/day] である．

δ-CRL 方式での CRL 取得に必要な通信量 システム全体で全検証者が全 Repository から取得するすべての base-CRL と δ-CRL のサイズの総情報量を，単位時間（1 日）あたりで平均した値（ビット数）とする．$L_{deltaCRL}$ で表し，単位は [bit/day] である．

3. 理論式の導出

ここでは 2.2 節で定義した通信量の理論式を導出する．はじめに導出に必要なパラメータの定義と，必要な仮定を示す．次に導出方法を説明する．以降では CRL に含まれる失効された証明書 1 つあたりの情報（1 つの失効した証明書の番号）を項目と呼ぶ．

3.1 パラメータの定義

評価に必要なパラメータを以下に定義する．

- p ：1 つの証明書が 1 日に失効される平均回数（失効発生頻度）[回/day]
- N ：entity 数 [個]
- k ：CA の個数 [個]
- q ：1 entity が，1 日に認証される平均回数（認証頻度）[回/day・個]
- T_C ：完全 CRL 方式での完全 CRL，および，δ-CRL 方式での δ-CRL の発行間隔 [day]
- T_B ：δ-CRL 方式の base-CRL の発行間隔 [day]
- L ：証明書の有効期間 [day]
- l_{sn} ：CRL の項目 1 つあたりのビット数 [bit]
- l_{sig} ：CRL の項目数によらない要素（CA の電子署名や，発効日など）のビット数 [bit]

3.2 仮　　定

理論式を導くうえで必要な評価モデルで説明した以外の仮定を示す．

(1) 証明書の失効は，失効発生頻度 p の Poisson 過程に従って発生する．
(2) 認証は，認証頻度 q の Poisson 過程に従って発生する．
(3) 各 entity は有効な証明書を 1 つだけ持ち，証明書が失効すると，すぐに代わりの証明書を取得する．
(4) すべての entity は同等に認証を行う（検証者となる）．
(5) 証明書有効期間 L はすべての証明書で同一とする．
(6) 証明書の有効期限切れは時間的に一様に発生する．
(7) 完全 CRL 方式での完全 CRL，δ-CRL 方式での δ-CRL は発行間隔 T_C で定期的に発行される．
(8) δ-CRL 方式での base-CRL は発行間隔 T_B で定期的に発行される．
(9) base-CRL の発行間隔 T_B は，δ-CRL の発行間隔 T_C の整数倍である．
(10) 各 CA には，同数（N/k）ずつの entity が属する．

3.3 導出のポイント

完全 CRL 方式，δ-CRL 方式の通信量の理論式を導出するうえでのポイントを説明する．

3.3.1 定常状態での完全 CRL，base-CRL の項目数

完全 CRL，δ-CRL 方式の base-CRL の項目数は，無限に大きくなるのではなく，ある時間経過後には，ある一定の数で定常状態になると考えられる．なぜならば，仮定 1 から，CRL にはつねに一定数の証明書番号が新たに加わり，仮定 6 から CRL に含まれる証明書番号のうちの一定数が有効期限切れで CRL から抜けるので，両者がバランスして一定になるからである．

図 2 を参照しながら，定常状態の項目数を導出する．定常状態の CRL の項目数を $N_{stable}(N,L,p,k)$ とする．1 つの CA について，1 日に失効される証明書数は Np/k なので，1 日に $N_{stable}(N,L,p,k)$ に追加される項目数は Np/k である．また，有効期限が切れるために 1 日に $N_{stable}(N,L,p,k)$ から除外される項目数は，$N_{stable}(N,L,p,k)/L$ である．定常状態では $N_{stable}(N,L,p,k)$ は変化しないので，新たに加わる項目数と除外される項目数は等しい．

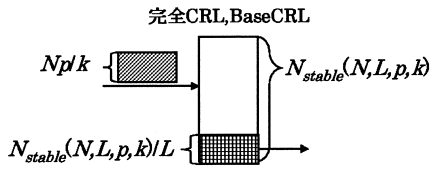

図 2 定常状態の完全 CRL，base-CRL の項目数
Fig. 2 Number of records in a full-CRL and a base-CRL schemes in a static state.

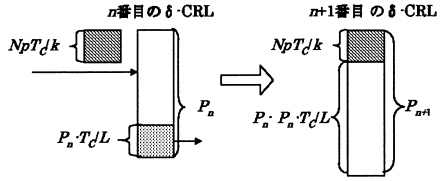

図 3 $n, n+1$ 番目の δ-CRL の項目数
Fig. 3 Number of records in n-th and $n+1$-th δ-CRLs.

$$\frac{Np}{k} = \frac{N_{stable}\,(N,L,p,k)}{L} \tag{1}$$

式 (1) を $N_{stable}(N,L,p,k)$ について解くと，定常状態の CRL の項目数は，以下で与えられる．

$$N_{stable}\,(N,L,p,k) = \frac{NpL}{k} \tag{2}$$

3.3.2 base-CRL の発行から n 番目の δ-CRL の項目数

δ-CRL には，ある base-CRL の発行時点以降に，新たに失効されかつ有効期限前である証明書の番号が含まれる．base-CRL の発行以降に，n 番目に発行された δ-CRL の項目数を P_n とする．1 つの CA について δ-CRL の発行間隔 T_C の間に新たに失効される証明書の数は NpT_C/k である．また，P_n 個の項目のうち，T_C の間に $P_n \cdot T_C/L$ 個は有効期限切れで δ-CRL に含まれる必要はなくなる．したがって，**図 3** に示すように，$n+1$ 番目の項目数 P_{n+1} は，P_n に，NpT_C/k を加え，$P_n \cdot T_C/L$ を削除したものとなり，以下の関係式が成り立つ．

$$P_{n+1} = P_n + \frac{NpT_C}{k} - \frac{P_n \cdot T_C}{L} \tag{3}$$

初項 $P_0 = 0$ として式 (3) を解くと，一般項 P_n は以下の式で与えられる．ただし，n の範囲は $1 \le n \le T_B/T_C - 1$ である．

$$P_n = \frac{NpL}{k}\left\{1 - \left(1 - \frac{T_C}{L}\right)^n\right\} \tag{4}$$

3.3.3 検証者がある CA に属する entity をある時間に 1 回以上認証する確率

完全 CRL 方式，δ-CRL 方式のいずれの場合も，検証者は CRL が発行された後に初めてある CA に属す

る entity を認証するときだけ，その CA の発行した CRL を取得すればよい．その後は，CRL が再度発行されるまで同一の CRL を再取得する必要はない．したがって，ある検証者がある CRL を取得する確率は，その CRL を発行した CA に属する entity を CRL の発行間隔の間に 1 回以上認証する確率に等しい．

仮定 2 より認証頻度は q であり，また 1 つの CA に属する entity 数は N/k なので，1 つの CA に属する entity を認証する回数の期待値は Nq/k 回となる．検証者数が N なので，時間間隔 T［day］の間に，ある検証者がある CA に属する entity を認証する回数の期待値は qT/k 回になる．一般に，ある時間間隔に平均 λ 回発生する事象の発生回数 X の確率分布は，Poisson 分布 $P(X) = \lambda^X \cdot e^{-\lambda}/X!$ に従うことが知られている．したがって，ある検証者が，ある CA に属する entity を認証する回数は，$\lambda = qT/k$ とした Poisson 分布に従うと考えられる．このことから，ある検証者が，T の間に，1 回以上ある CA に属する entity を認証する確率 $P(X \geq 1)$ は，$P(X)$ の X が 1 から ∞ までの和として，以下で与えられる．

$$P(X \geq 1) = \sum_{X=1}^{\infty} P(X) = 1 - P(0)^{-\frac{qT}{k}} \quad (5)$$

3.4 通信量の理論式の導出

3.4.1 L_{CRL} の導出

完全 CRL 方式では，1 つの CA が 1 回に発行する CRL のサイズ l_{CRL} は，式 (2) の CRL の項目数と CRL の項目 1 つあたりのビット数 l_{sn} の積，および項目数によらない要素のビット数 l_{sig} の和であり，以下で与えられる．

$$l_{CRL} = N_{stable}(N, L, p, k) \cdot l_{sn} + l_{sig} \quad (6)$$

発行間隔 T_C の間に，検証者がある CA に属する entity を 1 回以上認証するときに，その CA の発行した CRL を取得する必要がある．したがって，L_{CRL} は式 (5) で $T = T_C$ とした確率で l_{CRL} を全 CA 数，全検証者数について和をとってから時間平均することにより，以下の式で与えられる．

$$\begin{aligned} L_{CRL} &= k \cdot N \cdot P(X \geq 1)\Big|_{T=T_C} \cdot l_{CRL} \cdot \frac{1}{T_C} \\ &= \frac{1}{T_C}\left(NpL \cdot l_{sn} + k \cdot l_{sig}\right) \cdot N \\ &\quad \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \end{aligned} \quad (7)$$

3.4.2 $L_{deltaCRL}$ の導出

δ-CRL 方式の通信量は，base-CRL 取得に必要な通信量と δ-CRL 取得に必要な通信量からなる．前者を $L_{baseCRL}$，後者を L_{delta} と表すと，次式が成立する．

$$L_{deltaCRL} = L_{baseCRL} + L_{delta} \quad (8)$$

1 つの CA が 1 回に発行する base-CRL のサイズ $l_{baseCRL}$ は，式 (6) と同様に，以下で与えられる．

$$l_{baseCRL} = N_{stable}(N, L, p, k) \cdot l_{sn} + l_{sig} \quad (9)$$

base-CRL の発行間隔 T_B の間に，検証者がある CA に属する entity を 1 回以上認証するときに，その CA の発行した base-CRL を取得する必要がある．したがって，$L_{baseCRL}$ は，式 (5) で $T = T_B$ とした確率で $l_{baseCRL}$ を全 CA，全検証者について和をとってから時間平均したものであり，以下の式で与えられる．

$$\begin{aligned} &L_{baseCRL} \\ &= k \cdot N \cdot P(X \geq 1)\Big|_{T=T_B} \cdot l_{baseCRL} \cdot \frac{1}{T_B} \\ &= \frac{1}{T_B}\left(NpL \cdot l_{sn} + k \cdot l_{sig}\right) \cdot N \cdot \left(1 - e^{-\frac{qT_B}{k}}\right) \end{aligned} \quad (10)$$

最新の base-CRL の発行以降に，n 番目に発行された δ-CRL のサイズ $l_{delta}(n)$ は，式 (4) の δ-CRL の項目数 P_n と CRL の項目 1 つあたりのビット数 l_{sn} の積，および項目数によらない要素のビット数 l_{sig} の和であり，以下の式で与えられる．

$$l_{delta}(n) = P_n \cdot l_{sn} + l_{sig} \quad (11)$$

δ-CRL の発行間隔 T_C の間に，検証者がある CA に属する entity を 1 回以上認証する場合だけ，その CA の発行した δ-CRL を取得する必要がある．したがって，L_{delta} は，式 (5) で $T = T_C$ とした確率で $l_{delta}(n)$ を全 CA，全検証者について和をとってから時間平均（$1 \leq n \leq T_B/T_C - 1$ で整数 n について和をとり，T_B で割る）したものであり，以下の式で与えられる．

$$\begin{aligned} &L_{delta} \\ &= k \cdot N \cdot P(X \geq 1)\Big|_{T=T_C} \cdot \sum_{n=1}^{\frac{T_B}{T_C}-1} l_{delta}(n) \cdot \frac{1}{T_B} \\ &= \frac{1}{T_B} \sum_{n=1}^{\frac{T_B}{T_C}-1} \left[\frac{NpL}{k}\left\{1 - \left(1 - \frac{T_C}{L}\right)^n\right\} \cdot l_{sn} \right. \\ &\quad \left. + l_{sig}\right] \cdot k \cdot N \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \end{aligned} \quad (12)$$

したがって，式 (8) により $L_{deltaCRL}$ は以下の式で表される

$$\begin{aligned} L_{deltaCRL} &= \frac{N}{T_B} \cdot A \cdot \left(1 - e^{-\frac{qT_B}{k}}\right) \\ &\quad + \frac{N}{T_B} \sum_{n=1}^{\frac{T_B}{T_C}-1} F(n) \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \end{aligned} \quad (13)$$

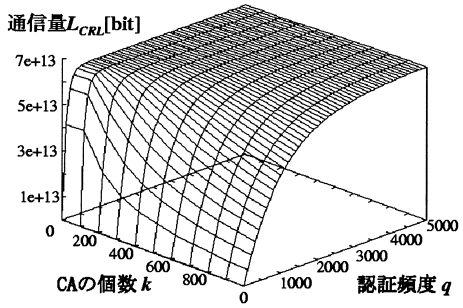

図 4 完全 CRL 方式での CRL 取得に必要な通信量
Fig. 4 Volume of communications necessary for obtaining full-CRLs.

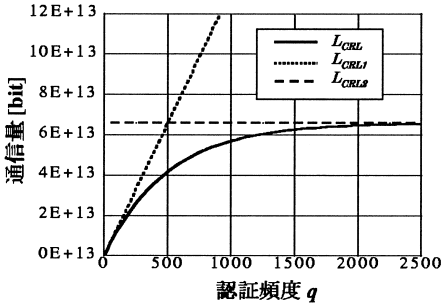

図 5 認証頻度に対する L_{CRL}，L_{CRL1}，L_{CRL2}
Fig. 5 $L_{CRL}, L_{CRL1}, L_{CRL2}$ with regard to the frequency of authentication.

ただし，$A = NpL \cdot l_{sn} + k \cdot l_{sig}$，$F(n) = NpL\{1 - (1 - T_C/L)^n\} \cdot l_{sn} + k \cdot l_{sig}$ とした．

4. L_{CRL}，$L_{deltaCRL}$ の評価と考察

完全 CRL 方式，δ-CRL 方式での CRL 取得に必要な通信量 L_{CRL}，$L_{deltaCRL}$ の評価と考察を行う．

4.1 パラメータ

評価で用いたパラメータを以下に示す．

- entity 数 $N = 3{,}000{,}000$ [個]
- 失効発生頻度 $p = 0.1/365$ [回/day]
- 証明書の有効期間 $L = 365$ [day]
- 完全 CRL，δ-CRL の発行間隔 $T_C = 1$ [day]
- CRL の項目 1 つあたりのビット数 $l_{sn} = 72$ [bit]
- CRL の項目数によらず一定な要素のビット数 $l_{sig} = 728$ [bit]

N，p，L，T_C，l_{sn}，l_{sig} は，参考文献 6) と同一の値を用いた．

4.2 L_{CRL} の評価と考察

図 4 は，認証頻度 q，CA の個数 k を変化させたときの完全 CRL 方式での L_{CRL} を示す．

図から L_{CRL} は，q の小さい領域での q への依存性の大きい振舞いと，q の大きい領域での q への依存性の小さい振舞いの 2 つからなることが予想される．実際，q の小さい極限では $qT_C/k \ll 1$ であるので，式 (7) の L_{CRL} で $e^{-qT_C/k} \cong 1 - qT_C/k$ としたときの近似式 L_{CRL1} は，以下の式で与えられる．

$$L_{CRL1} = \frac{N}{k}\left(NpL \cdot l_{sn} + k \cdot l_{sig}\right) \cdot q \qquad (14)$$

同様に，q の大きい極限では $qT_C/k \gg 1$ であるので，式 (7) の L_{CRL} で $e^{-qT_C/k} \cong 0$ としたときの近似式 L_{CRL2} は，以下の式で与えられる．

$$L_{CRL2} = \frac{N}{T_C}\left(NpL \cdot l_{sn} + k \cdot l_{sig}\right) \qquad (15)$$

図 5 は，CA の個数 $k = 500$ に固定して，q を変化させたときの L_{CRL}，L_{CRL1}，L_{CRL2} を示したものである．L_{CRL1} が q の 1 次に比例しているのは，q が十分小さく同一の CA に属する entity を複数回認証する確率が小さいので，検証者が entity を認証するたびに CRL を Repository から取得することを表している．また，L_{CRL2} は q を含まず，q に非依存である．これは，q が十分大きい場合，検証者はすべての CA に属する entity をほぼ確実に 1 回以上認証することになり，すべての CA で発行されるすべての CRL を取得することを表している．

このように L_{CRL} は，q の小さい極限での q の 1 次に比例する漸近的な振舞いと，q の大きい極限での q に依存しない漸近的な振舞いの 2 つからなる．そして，それぞれの振舞いが支配的な領域は，おおよそ L_{CRL1} と L_{CRL2} の値が等しくなる認証頻度 q で切り替わる．式 (14)，(15) より，$L_{CRL1} \cong L_{CRL2}$ として，q について解くと，以下の関係式が得られる．

$$q \cong \frac{k}{T_C} \qquad (16)$$

このことは，認証頻度 q が CRL の発行頻度と CA の個数の積 k/T_C とほぼ等しいときに 2 つの振舞いが交差することを示している．

図 6 は CA の個数 k と認証頻度 q の平面が式 (16) によって，L_{CRL1} と L_{CRL2} のそれぞれの振舞いの支配的な 2 つの領域に分割されることを示したものである．図 6 の領域 $1(q < k/T_C)$ では，L_{CRL1} の q の 1 次に比例する振舞いが支配的である．この領域では，CRL の発行頻度より認証頻度の方が小さく，検証者はすべての CA の発行した CRL を取得しなくてすむ．そのため，CRL を CA ごとに発行して，検証者がそのうち必要なものだけを取得できるようにすることが，CRL 取得に必要な通信量を下げるために有効に働いている．一方，領域 $2(q > k/T_C)$ では，L_{CRL2} の q に依存しない振舞いが支配的である．この領域で

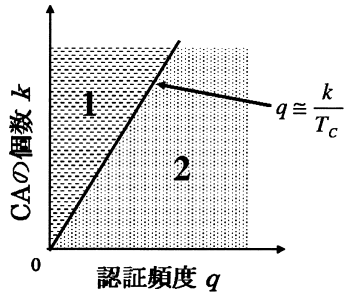

図 6 完全 CRL 方式で CRL 取得に必要な通信量の 2 種類の q 依存性のそれぞれが支配的な領域
Fig. 6 Schematic diagram in the plane of k and q of two dominant q-dependences of volume of communications necessary for obtaining full-CRLs.

は，CRL の発行頻度に対して認証頻度の方が大きく，すべての CA に属する entity を 1 回以上認証するため，検証者はすべての CA の発行した CRL を取得する．したがってこの領域では，CRL を CA ごとに発行して，検証者がそのうちの必要なものだけを取得できることは，CRL 取得に必要な通信量を下げるために有効に働いているとはいえない．特に式 (15) から分かるように，領域 2 では CRL 取得に必要な通信量は entity 数の 2 次に比例する．

認証頻度 q を一定にすると，式 (15) から図 6 の領域 2 での CRL 取得に必要な通信量 L_{CRL} は，CA の個数 k に比例することが分かる．また，CA が k（> 1）個の場合でも，各 CA がそれぞれに CRL を発行するのではなく，全 CA 分を 1 つの CRL にまとめて 1 つの CRL 発行機関が発行することで，CRL 取得に必要な通信量 L_{CRL} の中の実効的な CA の個数を 1 にすることができる．これらのことから，CA の個数 k，CRL の発行間隔 T_C，認証頻度 q が与えられ，それが図 6 の領域 2 に属する（$q > k/T_C$）場合，k 個の CA がそれぞれに CRL を発行するよりは，むしろ全 CA の分を 1 つの CRL にまとめて発行する方が，CRL 取得に必要な通信量 L_{CRL} を低くすることができることが分かる．

CA の個数 k を一定にすると，式 (16) から CRL の発行間隔 T_C を小さくすることで，図 6 の領域 1，つまり CA ごとに CRL を発行することが有効な q の範囲（$0 < q < k/T_C$）を広げることができる．しかし $T_C^{'} < T_C$ に対して，式 (7) より，$L_{CRL}\big|_{T_C^{'}} > L_{CRL}\big|_{T_C}$ となる．したがって，CRL の発行間隔を小さくすることで領域 1 を広げることは可能であるが，同一の認証頻度での通信量はむしろ大きくなってしまう．

4.3 $L_{deltaCRL}$ の評価と考察

完全 CRL 方式と同様に，δ-CRL 方式での CRL 取得に必要な通信量 $L_{deltaCRL}$ は，認証頻度 q の小さい極限での q に依存する振舞いと，q の大きい極限での q に依存しない振舞いの 2 つからなる．実際に，q の小さい極限では $qT_C/k \ll 1$，$qT_B/k \ll 1$ であるので，式 (13) の $L_{deltaCRL}$ で $e^{-qT_C/k} \cong 1 - qT_C/k$，$e^{-qT_B/k} \cong 1 - qT_B/k$ としたときの近似式 $L_{deltaCRL1}$ は，以下で与えられる．

$$L_{deltaCRL1} = \frac{N \cdot q}{k}\left\{A + \frac{T_C}{T_B}\sum_{n=1}^{\frac{T_B}{T_C}-1} F(n)\right\} \tag{17}$$

同様に，q の大きい極限では $qT_C/k \gg 1$，$qT_B/k \gg 1$ であるので，式 (13) の $L_{deltaCRL}$ で $e^{-qT_C/k} \cong 0$，$e^{-qT_C/k} \cong 0$ としたときの近似式 $L_{deltaCRL2}$ は以下の式で与えられる．

$$L_{deltaCRL2} = \frac{N}{T_B}\left\{A + \sum_{n=1}^{\frac{T_B}{T_C}-1} F(n)\right\} \tag{18}$$

したがって，式 (17)，(18) から $L_{deltaCRL}$ は q の小さい極限での q の 1 次に比例する漸近的な振舞いと，q の大きい極限での q に依存しない漸近的な振舞いの 2 つからなる．また，それぞれの振舞いが支配的な領域は，おおよそ $L_{deltaCRL1}$ と $L_{deltaCRL2}$ が等しくなる認証頻度 q で切り替わる．

$L_{deltaCRL1} \cong L_{deltaCRL2}$ として，$\sum F(n)/A = x$ とすると，次式が得られる．

$$q \cong \frac{k}{T_B} \cdot \frac{1+x}{1+\frac{T_C}{T_B}x} \tag{19}$$

$x \geq 0$，$0 < T_C/T_B \leq 1$ なので，$T_C/T_B \leq (1 + x \cdot T_C/T_B)/(1+x) \leq 1$ である．したがって，式 (19) の q について

$$\frac{k}{T_B} \leq q \leq \frac{k}{T_C} \tag{20}$$

が成立する．このことから，δ-CRL 方式の場合は，q の 1 次に比例する $L_{deltaCRL1}$ の振舞いが支配的な領域は，完全 CRL 方式の場合よりもさらに認証頻度の低い領域に限られることが分かる．

図 7 は，認証頻度 q と CA の個数 k の値の組 (k, q) を，例として (100, 100)，(80, 30)，(50, 10) にしたときの base-CRL の発行間隔 T_B と CRL 取得に必要な通信量 $L_{deltaCRL}$ の関係を示している．いずれの場合も，$L_{deltaCRL}$ は T_B の増加にともない減少し，その後再び増加しているので，$L_{deltaCRL}$ が最小になる最適な base-CRL の発行間隔が存在することが予想

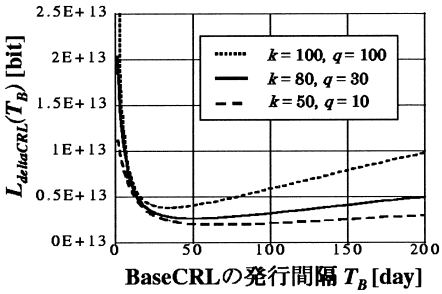

図 7 base-CRL の発行間隔と δ-CRL 方式の通信量の関係
Fig. 7 Volume of communications for obtaining base- and δ-CRL with regard to the interval of base-CRL issuances.

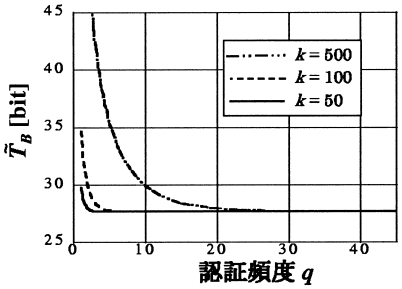

図 8 認証頻度と最適な base-CRL の発行間隔 ($L = 365, T_C = 1$) の関係
Fig. 8 Optimal interval of base-CRL issuance with regard to the frequency of authentication at ($L = 365, T_C = 1$).

される．

δ-CRL 方式で任意の k と q の値で，$L_{deltaCRL}$ が最小になる最適な base-CRL の発行間隔 T_B^* が存在する理由は以下のとおりである．式 (8) から $L_{deltaCRL}$ は base-CRL の寄与 $L_{baseCRL}$ と δ-CRL の寄与 L_{delta} からなり，それぞれは時刻 $t = 0$ で発行される base-CRL と，時刻 $t = 0$ から $t = T_B$ の間に T_C の間隔で発行される δ-CRL について，同一の CRL はたかだか 1 回だけ取得されるという条件で，取得されたもののサイズの和を時間平均した（T_B で割った）ものである．

$T_B = T_C$ では δ-CRL が発行されないので，$L_{deltaCRL}$ は式 (10) の $L_{baseCRL}$ で $T_B = T_C$ としたものと一致する．$T_B > T_C$ では，$L_{baseCRL}$ は T_B の増加とともにほぼ T_B に反比例して減少する（base-CRL を T_B の間に取得する確率の変化が $1/T_B$ よりも小さいことは容易に示される．また T_B が証明書の有効期間 L に比べて十分小さい間は，base-CRL 発行以降 T_B の間に新たに失効する証明書数は少ないので，δ-CRL と base-CRL のサイズの関係は $l_{deltaCRL}(n) \ll l_{baseCRL}$ であり，$L_{deltaCRL}$ への L_{delta} の寄与は $L_{baseCRL}$ に比べて小さい）．このため，$T_B > T_C$ でも T_B が小さい間は，$L_{deltaCRL}$ は減少する．一方 T_B が大きいときには，base-CRL の寄与は T_B に反比例して消え，$L_{deltaCRL}$ は主に L_{delta} で決まる．以下で示されるように，base-CRL 発行から（L に比べて）十分大きい時間の後に発行される δ-CRL のサイズ $l_{deltaCRL}(n)$ は，漸近的に base-CRL のサイズ $l_{baseCRL}$ に近づく．したがって，$T_B \to \infty$ で $L_{deltaCRL}$ では，式 (12) で $l_{deltaCRL}(n)$ をその漸近的なサイズ $l_{baseCRL}$ とした L_{delta} に一致し，再び $T_B = T_C$ での $L_{deltaCRL}$ を与える．このため，時刻 $T_B = T_C$ から $T_B = \infty$ の間に，$L_{deltaCRL}$ が最小になる $T_B = T_B^*$ が存在する．

δ-CRL のサイズ $l_{deltaCRL}(n)$ は，漸近的に base-CRL のサイズ $l_{baseCRL}$ に近づくことは次のようにして分かる．T_B が証明書の有効期間 L よりも大きい場合を考えると，$L < t < T_B$ なる時刻 t で発行された δ-CRL には，base-CRL 発行以降に発行された証明書に対応する項目だけが含まれる．さらに $L \ll t < T_B$ とすれば，時刻 0 で δ-CRL の項目数が 0 であったという初期値の影響も失われるので，この δ-CRL に含まれる項目数は定常状態で失効されている証明書数と同数，つまり時刻 0 で発行された base-CRL の項目数と同じになる．これは $n \to \infty$ で $l_{deltaCRL}(n) = l_{baseCRL}$ が成り立つことを意味するが，式 (9) と (11) から容易に確かめられる．

仮定 9 より T_B は T_C の整数倍であるが，最初にこの条件を無視する．式 (13) の $L_{deltaCRL}$ で $F(n)$ についての和と T_B についての偏微分を解析的に計算して，$L_{deltaCRL}$ を最小にする $T_B = \tilde{T}_B$ を，$\partial L_{deltaCRL}/\partial T_B = 0$ を満たす T_B として求める．ただし，この方程式を解くために，Newton-Raphson 法による数値計算を用いた．**図 8** に k が 1，50，100，500 の場合に，$\tilde{T}_B$ と q の関係を示す．図より q が十分大きい場合は，$\tilde{T}_B$ は k の値とは無関係にある一定の値（図 8 では，27.7 日）に収束することが確認できる．したがって，δ-CRL 方式では，q が十分大きい場合には，k とは無関係に T_B^* が存在すると予想される．次に，δ-CRL 方式では q が十分大きい場合は k とは無関係に T_B^* が存在することを証明する．base-CRL の発行間隔 $T_B = T$ のときの δ-CRL 方式での CRL 取得に必要な通信量を $L_{dletaCRL}|_{T_B=T}$ と表す．base-CRL の発行間隔が最適であるとき，すなわち $T_B = T_B^*$ のとき，以下の不等式が成り立つ．

$$L_{deltaCRL}\big|_{T_B=T_B^*} - L_{deltaCRL}\big|_{T_B=T_B^*+T_C} < 0 \tag{21}$$

$$L_{deltaCRL}\big|_{T_B=T_B^*} - L_{deltaCRL}\big|_{T_B=T_B^*-T_C} < 0 \tag{22}$$

式 (21)，(22) の左辺は，以下で与えられる．

$$\begin{aligned}
&\frac{N}{T_B^*+T_C}\left\{\frac{T_C}{T_B^*}\cdot A\cdot\left(1-e^{-\frac{qT_B^*}{k}}\right)\right.\\
&\quad+\frac{1}{T_B^*}\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\cdot\left(1-e^{-\frac{qT_C}{k}}\right)\\
&\quad+A\cdot\left(-e^{-\frac{qT}{k}}+e^{-\frac{q(T_B^*+T_C)}{k}}\right)\\
&\quad\left.-F\left(\frac{T_B^*}{T_C}\right)\left(1-e^{-\frac{qT_C}{k}}\right)\right\}
\end{aligned} \tag{23}$$

$$\begin{aligned}
&\frac{N}{T_B^*-T_C}\left\{\frac{T_C}{T_B^*}\cdot A\cdot\left(1-e^{-\frac{qT_B^*}{k}}\right)\right.\\
&\quad+\frac{1}{T_B^*}\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\cdot\left(1-e^{-\frac{qT_C}{k}}\right)\\
&\quad+A\cdot\left(-e^{-\frac{qT}{k}}+e^{-\frac{q(T_B^*-T_C)}{k}}\right)\\
&\quad\left.-F\left(\frac{T_B^*}{T_C}-1\right)\left(1-e^{-\frac{qT_C}{k}}\right)\right\}
\end{aligned} \tag{24}$$

式 (23)，(24) を，$e^{-\alpha\frac{qT_C}{k}}$ (α：定数) に依存する項と，依存しない項に分けると，以下の式が得られる．

$$\begin{aligned}
&\frac{N}{T_B^*+T_C}\left\{\frac{T_C}{T_B^*}\left\{A+\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\right\}\right.\\
&\quad\left.-F\left(\frac{T_B^*}{T_C}\right)+\mathcal{O}\left(e^{-\alpha\frac{qT_C}{k}}\right)\right\}
\end{aligned} \tag{25}$$

$$\begin{aligned}
&\frac{N}{T_B^*-T_C}\left\{\frac{T_C}{T_B^*}\left\{A+\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\right\}\right.\\
&\quad\left.-F\left(\frac{T_B^*}{T_C}-1\right)+\mathcal{O}\left(e^{-\alpha\frac{qT_C}{k}}\right)\right\}
\end{aligned} \tag{26}$$

式 (25), (26) で，q を十分大きくすると，$\mathcal{O}(e^{-\alpha\frac{qT_C}{k}}) \cong 0$ となるので，式 (21)，(22) は各項に共通な $NpL\cdot l_{sn}$ を取り除くと以下で与えられる．

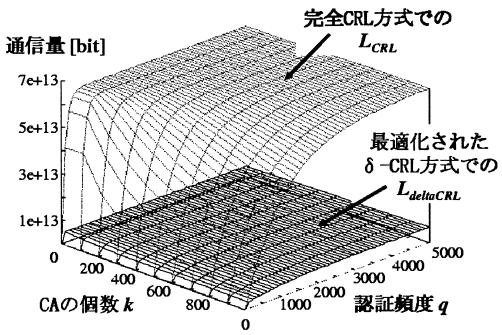

図 9 完全 CRL 方式と，最適化された δ-CRL 方式の CRL 取得に必要な通信量

Fig. 9 Volume of communications necessary for obtaining CRLs in full-CRL and optimized δ-CRL schemes.

$$\begin{aligned}
&\frac{T_C}{T_B^*}\left\{1+\sum_{n=1}^{\frac{T_B^*}{T_C}-1}\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\}\right\}\\
&\quad-\left\{1-\left(1-\frac{T_C}{L}\right)^{\frac{T_B^*}{T_C}}\right\}<0
\end{aligned} \tag{27}$$

$$\begin{aligned}
&\frac{T_C}{T_B^*}\left\{1+\sum_{n=1}^{\frac{T_B^*}{T_C}-1}\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\}\right\}\\
&\quad-\left\{1-\left(1-\frac{T_C}{L}\right)^{\frac{T_B^*}{T_C}-1}\right\}<0
\end{aligned} \tag{28}$$

式 (27)，(28) は，T_B^*/T_C と L/T_C を変数とする関数についての不等式 $f_1(T_B^*/T_C, L/T_C) < 0$ と $f_2(T_B^*/T_C, L/T_C) < 0$ の形式である．このことと T_B^* が T_C の整数倍であるという仮定から，式 (27)，(28) を同時に満たす T_B^*/T_C は一意に定まるので，ある 1 変数の関数 f により $T_B^*/T_C = f(L/T_C)$ の形式に表される．つまり，q が十分大きい場合は，T_B^*/T_C は L/T_C によって一意に定まり，かつ CA の個数に無関係である．

図 9 は，4.1 節のパラメータを用いて，base-CRL の発行間隔を図 8 での最適な発行間隔から $T_B^* = 28$ [day] にした場合に，δ-CRL 方式での CRL 取得に必要な通信量 $L_{deltaCRL}$ を示したものである．本来ならば，T_B^* は，任意の q，k に対して定まる値であるが，実際のシステムでは，検証者が認証を行う頻度，すなわち q は予測不可能なのでシステム側で決めることは難しい．したがって，q が十分大きい場合に $L_{deltaCRL}$ を最小化する T_B^* をとることが適当である．これを以下では最適化された δ-CRL 方式と呼ぶことにする．

図 9 から，完全 CRL 方式と最適化された δ-CRL 方式では，CRL 取得に必要な通信量に差があること

が分かる．認証頻度が十分大きく，CRL 取得に必要な通信量が認証頻度 q に依存しない領域（完全 CRL 方式では式 (15)，δ-CRL 方式では式 (18) で表される領域）では，たとえば，認証頻度 $q = 5000$，CA の個数 $k = 1000$ の場合，最適化された δ-CRL 方式での通信量は完全 CRL での通信量のおよそ 1/10 になる．

5. ま と め

PKI での主な証明書の失効方式である完全 CRL 方式，δ-CRL 方式について，CRL 取得に必要な通信量の理論式を検証者が同一の CRL の取得をたかだか 1 度しか行わないことを確率論的に取り入れて導いた．

その評価結果から，完全 CRL 方式，δ-CRL 方式での CRL 取得に必要な通信量は，認証頻度が CRL の発行頻度と CA 数の積より十分小さい領域での認証頻度に比例する振舞いと，認証頻度が CRL の発行頻度と CA 数の積より十分大きい領域での認証頻度には依存せず，Entity 数の 2 次に比例する振舞いに分かれる．そして，CRL を CA ごとに発行して，検証者がそのうちの必要とする CRL だけを取得することで通信量が下がるのは，認証頻度の十分低い領域に限られることを示した．

さらに δ-CRL 方式では，認証頻度が十分大きい場合に，通信量を最小化する最適な baseCRL の発行間隔と δ-CRL の発行間隔の比が，証明書の有効期間と δ-CRL の発行間隔の比から一意に定まり，それは CA の個数とは無関係であることを示した．

参 考 文 献

1) Malpani, A., Galperin, S., Myers, M., Ankney, R. and Adams, C.: RFC 2560: X.509 Internet public key infrastructure online certificate status protocol — ocsp (June 1999).
2) Naor, M. and Nissim, K.: Certificate revocation and certificate update, *Proc. 7th USENIX Security Symposium*, San Antonio, Texas (Jan. 1998).
3) Micali, S.: Efficient certificate revocation, Technical Memo MIT/LCS/TM-542b, Massachusetts Institute of Technology, Laboratory for Computer Science (Mar. 1996).
4) ITU: ITU-T Recommendation X.509 Authentication Framework, Technical Report X.509 (2000).
5) Housley, R., Ford, W., Polk, W. and Solo, D.: RFC 3280: Internet X.509 public key infrastructure certificate and Certification Revocation List (CRL) profile (Apr. 2002).
6) Berkovits, S., Chokani, S., Furlong, J.A., Geiter, J.A. and Guild, J.C.: Public Key Infrastructure Study: Final Report, MITRE Corporation for NIST (Apr. 1994).

(平成 15 年 10 月 6 日受付)
(平成 16 年 10 月 4 日採録)

推 薦 文

本論文では，PKI での主な証明書の失効方式である完全 CRL 方式とデルタ CRL 方式について，CRL 取得に必要な通信量の理論式を確率論的に導出している．同様の評価として米国 NIST による評価があるが，同一の CA に属する entity を複数回認証する場合に，同一の CRL の取得はたかだか 1 回ですむにもかかわらず複数回取得していた．PKI 運用に必要なシステム全体の通信量を評価することは，安全な電子社会を支える PKI を設計するうえで大変重要であり，この課題に対して実情に即した理論的アプローチを行った点，さらに得られたデータに対して優れた理論的考察を行っている点がとくに評価できるので，論文として推薦したい．

（CSEC 研究会前主査　岡本栄司）

田中　直樹

平成 13 年横浜国立大学大学院工学研究科人工環境システム学修士課程修了．同年ソニー（株）入社．コンピュータセキュリティの研究開発に従事．

飯野陽一郎

平成 9 年東京大学理学系研究科物理学専攻博士課程修了．平成 10 年ソニー（株）入社．コンピュータセキュリティの研究開発に従事．